



## **Cisco Video Surveillance Management Console Administration Guide**

Release 7.2

### **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-27092-07

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

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

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

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

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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

*Cisco Video Surveillance Management Console Administration Guide*  
© 2012-2013 Cisco Systems, Inc. All rights reserved.



# CONTENTS

## **Preface** vii

Overview vii

Related Documentation vii

Obtaining Documentation, Obtaining Support, and Security Guidelines vii

---

## **CHAPTER 1**

### **Overview** 1-1

Overview 1-2

Co-Located and Stand-Alone Server Configurations 1-2

Feature Summary 1-3

Requirements 1-4

Understanding Cisco Video Surveillance Software 1-5

Logging In 1-7

    Changing the Cisco VSM Management Console Password 1-8

Configuring the Server Ethernet Ports 1-9

    Default Ethernet Interface Settings 1-9

    Network Settings in a Virtual Machine (OVA File) Installation 1-9

    Supported Ethernet Port Configurations 1-10

    Using DHCP 1-11

---

## **CHAPTER 2**

### **Using the Initial Setup Wizard** 2-1

---

## **CHAPTER 3**

### **Monitoring a Cisco Video Surveillance Server** 3-1

System Summary 3-2

- Device List 3-3
- Mediaout Statistics 3-6
- Recordings 3-8
- Streams 3-10
- Installed Packages 3-11
- Logs 3-12
- System Trends 3-14
- Hardware Status 3-18
  - Viewing System Status 3-18
  - Viewing Hardware Status 3-19
  - Viewing RAID and Physical Drive Status 3-20
- Audit Logs 3-23

---

**CHAPTER 4**

- Administration 4-1**
  - System Setup 4-1
    - Services 4-1
    - Network 4-3
    - Date and Time 4-5
    - Reset Password 4-7
    - Language Settings 4-8
    - Security 4-9
  - Media Server 4-11
    - SNMP Trap Destination 4-11
  - Maintenance 4-13
    - Log Level 4-13
    - Server Upgrade 4-15
    - Backup 4-17
    - Restore 4-20
    - Manage Drivers 4-21

Support Report 4-23

Restart Services 4-24

Reboot Server 4-25

Shut Down Server 4-25

---

**CHAPTER 5**

**Camera View 5-1**

---

**APPENDIX A**

**Related Documentation A-1**

---

**APPENDIX B**

**Revision History B-1**





## Preface

---

Revised: September 13, 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 services.

## Related Documentation

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

## Obtaining Documentation, 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, page 1-2](#)
- [Co-Located and Stand-Alone Server Configurations, page 1-2](#)
- [Feature Summary, page 1-3](#)
- [Requirements, page 1-4](#)
- [Understanding Cisco Video Surveillance Software, page 1-5](#)
- [Logging In, page 1-7](#)
- [Configuring the Server Ethernet Ports, page 1-9](#)

# Overview

The Cisco VSM Management Console is used by system administrators to perform infrequent server administration tasks, such as initial server setup, backups, system software upgrades, and log monitoring.

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

The Management Console is also used to enable the following services:

- **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**—A service 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**

After a server is added to the Operations Manager configuration, the Management Console can only be used to activate or deactivate the Operations Manager (VSOM) service. Use the Operations Manager to activate or deactivate other services, such as the Media Server. See the [“Services” section on page 4-1](#) for more information.

**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.

## Co-Located and Stand-Alone Server Configurations

The Operations Manager and Media Server services can run on the same server, or separate servers. The following combinations are supported.

- **Stand-alone Operations Manager and Media Servers**—The Operations Manager and each Media Server is run on a separate server. The Operations Manager server does not run the Media Server service.
- **Co-located**—The Operations Manager and a single Media Server are enabled on the same server. The following rules apply:
  - The co-located Media Server can only be a primary Media Server (co-located Media Servers do not support other HA roles such as Standby or Redundant).
  - Failover or Redundant Media Servers cannot be associated with the co-located primary Media Server (only a long term storage (LTS) server can be associated with the co-located primary Media Server).
  - The co-located Media Server do not support the same number of cameras as a stand-alone server.

- The co-located Operations Manager does not support the same number of Media Servers as a stand-alone Operations Manager.

## 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 <b>Setup Wizard</b> guides you through the process to enable the server services such as the (Media Server and Operations Manager), configure network settings, define the system time (or NTP server), and other basic settings.	<a href="#">System Setup, page 4-1</a>
Monitoring	Use the <b>Monitor</b> 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.	<a href="#">Monitoring a Cisco Video Surveillance Server, page 3-1</a>
Administration	Use the <b>Administration</b> pages to enter basic system set up properties, define the log levels, upgrade the server software and device drivers, backup or restore the server configuration, define SNMP trap destinations, view the SNMP MIBs, and other tasks.  <b>Note</b> Beginning in Release 7.2, most Media Server configurations are performed using the Operations Manager user interface).	<a href="#">Administration, page 4-1</a>
Restart or shutdown the server	Use the buttons in the top right to restart, reboot or shut down the server.	<ul style="list-style-type: none"> <li>• <a href="#">Restart Services, page 4-24</a></li> <li>• <a href="#">Reboot Server, page 4-25</a></li> <li>• <a href="#">Shut Down Server, page 4-25</a></li> </ul>
View Video	View video from a single Cisco Video Surveillance camera.	<a href="#">Camera View, page 5-1</a>

# Requirements

The Cisco Video Surveillance Management Console requires the following.

**Table 1-2**      **Requirements**

Requirement	Requirement Complete? (✓)
<p>A PC or laptop with the following:</p> <ul style="list-style-type: none"> <li>• Windows 7 (32-bit or 64-bit) or Windows 8 (64-bit)</li> <li>• Minimum resolution of 1024x768</li> <li>• You must log in with a standard Windows user account. Logging in with a Guest account can prevent video streaming and result in an error to be displayed in the video pane: “Cannot create RTSP connection to server. Check network connection and server health status.”</li> </ul> <p>See the <a href="#">Cisco Video Surveillance Monitoring Workstation Performance Baseline Specification</a> for the complete baseline performance specifications for a video surveillance monitoring workstation.</p>	<input type="checkbox"/>
<p>The Internet Explorer (IE) web browser.</p> <p><b>Windows</b></p> <ul style="list-style-type: none"> <li>• Windows 7 supports IE 9 or 10.</li> <li>• Windows 8 supports IE 10, desktop version (the Metro version of IE 10 is not supported).</li> </ul> <p>See the <a href="#">Cisco Video Surveillance Monitoring Workstation Performance Baseline Specification</a> for the complete baseline performance specifications for a video surveillance monitoring workstation.</p>	<input type="checkbox"/>
<p>A physical or virtual Cisco Video Surveillance 7.x server installed in the network where the other Cisco Video Surveillance components are deployed.</p> <ul style="list-style-type: none"> <li>• Physical Servers: <ul style="list-style-type: none"> <li>– (Systems pre-installed with Release 7.2) See the <a href="#">Cisco Physical Security UCS Platform Series User Guide</a> for more information.</li> <li>– (Systems pre-installed with Release 7.0.0 or 7.0.1) See the <a href="#">Cisco Physical Security Multiservices Platform Series User Guide</a> for more information.</li> </ul> </li> <li>• Virtual Machines—See the <a href="#">Cisco Video Surveillance Virtual Machine Deployment and Recovery Guide for UCS Platforms</a> for instructions to install the server software .ova image as a virtual machine (VM).</li> </ul>	<input type="checkbox"/>
<p>At least one static IP address used to access the server. The address will be assigned to the Eth0 or Eth1 port.</p> <ul style="list-style-type: none"> <li>• 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).</li> <li>• See the “<a href="#">Configuring the Server Ethernet Ports</a>” section on page 1-9</li> </ul>	<input type="checkbox"/>
<p>Complete the Media Server initial configuration (including network settings) using the Setup Wizard.</p> <p><b>Note</b> Adding a Media Server directly to the Operations Manager configuration without completing the Management Console <b>Initial Setup Wizard</b> will cause the Media Server to use the Operations Manager IP address (instead of the hostname).</p>	<input type="checkbox"/>

Table 1-2 Requirements (continued)

Requirement	Requirement Complete? (✓)
Verify that only one interface is enabled and active on the server configured with the Operations Manager service (including co-located servers). <b>Note</b> Although the Management Console UI allows enabling both interfaces when the Operations Manager service is running, this configuration is not supported.	<input type="checkbox"/>
Verify that the Operations Manager server hostname resolves to only one (correct) address. <b>Note</b> Dual-homed/NAT server configurations are not supported on any server running the Operations Manager service (including co-located servers). Dual-homed/NAT server configuration is supported only for stand-alone Media Servers.	<input type="checkbox"/>
Each Media Server and Operations Manager must run the same versions of the <i>system software</i> and device <i>driver packs</i> . See the “ <a href="#">Understanding Cisco Video Surveillance Software</a> ” section on page 1-5 for more information.	<input type="checkbox"/>

## 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	<p><i>System Software</i> denotes the Cisco VSM software, including Media Server, Operations Manager, Management Console, and Cisco Video Surveillance Safety and Security Desktop clients.</p> <ul style="list-style-type: none"> <li>The Operations Manager and all associated Media Servers must run the same software version.</li> <li>See the “<a href="#">Server Upgrade</a>” section on page 4-15 for upgrade instructions.</li> </ul> <p>To repair or restore the Cisco VSM server software, see the <a href="#">Cisco Video Surveillance Manager 7.0 Recovery Flash Drive guide</a>.</p>
OVA image (for VM installations)	<p>OVF template files are used to install the server software as a virtual machine (VM) on a supported Cisco Unified Computing System (UCS) platform.</p> <ul style="list-style-type: none"> <li>OVA template files are downloaded from the Cisco website.</li> <li>The file format is .ova. For example: <code>Cisco_VSM-7.2.0-331d_ucs-bc.ova</code></li> <li>See the <a href="#">Cisco Video Surveillance Virtual Machine Deployment and Recovery Guide for UCS Platforms</a> for instructions to install the .ova image and perform the initial VM setup.</li> <li>After the VM setup is complete, use the Management Console to complete the configuration.</li> </ul>

Table 1-3 Cisco Video Surveillance Software Types (continued)

Software Type	Description
USB Recovery Disk image	<p>Use the USB Recovery Disk image to create a Cisco VSM 7 Recovery Flash Drive (for example, on a USB stick). The recovery disk can be used do the following:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> </ul> <p>See the <a href="#">Cisco Video Surveillance Manager Flash Drive Recovery Guide</a> for more information.</p>
Device <i>firmware</i>	<p>Device <i>firmware</i> 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.</p> <p>See the “Upgrading Camera and Encoder Driver Firmware” section of the <a href="#">Cisco Video Surveillance Operations Manager User Guide</a> for instructions to upgrade Cisco device firmware, or refer to the device documentation.</p>
Device <i>driver packs</i>	<p>Device <i>driver packs</i> are the software packages used by Media Servers and the Operations Manager to interoperate with video devices, such as cameras. Driver packs are included with the Cisco VSM software, or may be added to a server at a later time to add support for new devices or features.</p> <ul style="list-style-type: none"> <li>• Install new driver packs to add support for additional devices.</li> <li>• Upgrade existing driver packs to enable support for new features.</li> </ul> <p><b>Note</b> We strongly recommend upgrading driver packs using the Operations Manager interface. This allows you to upgrade multiple servers at once. Driver packs must be upgraded to the same version on each server where the Media Server and Operations Manager services are enabled or a driver pack mismatch error occurs. Templates cannot be revised when a driver pack mismatch error is present.</p> <ul style="list-style-type: none"> <li>• To upgrade drivers using the Operations Manager, see the “Driver Pack Management” section of the <a href="#">Cisco Video Surveillance Operations Manager User Guide</a>.</li> <li>• To upgrade using the Management Console, see the “Manage Drivers” section on page 4-21.</li> </ul>
Language Packs	<p>Language packs can be added to display the VSM user interfaces in non-English languages. Language packs are added using the <b>Server Upgrade</b> page of the Cisco VSM Management Console. You must upgrade the language packs on all servers in your deployment.</p> <p>See the <b>Server Upgrade</b> section for more information.</p>

# 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 on your Windows computer.  
See the “Requirements” section on page 1-4 for supported versions.
- 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: <b>http://192.168.0.200/vsmc/</b>
Virtual Machine: Cisco Unified Computing System (Cisco UCS) platform	The Cisco VSM server includes two network ports with the following default configuration: <ul style="list-style-type: none"> <li>• Eth0 port—static IP address 192.168.0.200</li> <li>• Eth1 port—DHCP</li> </ul> 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 <a href="#">Cisco Video Surveillance Virtual Machine Deployment and Recovery Guide for UCS Platforms</a> for more information.

- Step 3** Enter the Cisco VSM Management Console password.

Platform	Server Address
Physical server —Cisco Multiservices Platform (Cisco MSP)	<ul style="list-style-type: none"> <li>• The default username <b>localadmin</b> is read-only and cannot be changed.</li> <li>• The default password is <b>secur4u</b>.</li> </ul>
Virtual Machine—Cisco USC platform	<ul style="list-style-type: none"> <li>• The default username <b>localadmin</b> is read-only and cannot be changed.</li> <li>• A new password is entered during the VM setup.</li> </ul> See the “Changing the Default Password” section of the <a href="#">Cisco Video Surveillance Virtual Machine Deployment and Recovery Guide for UCS Platforms</a> 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 2-1).
- 

## 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 services enabled on the server.

Refer to the following topics for more information.

- [Default Ethernet Interface Settings, page 1-9](#)
- [Network Settings in a Virtual Machine \(OVA File\) Installation, page 1-9](#)
- [Supported Ethernet Port Configurations, page 1-10](#)
- [Using DHCP, page 1-11](#)

**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 4-3 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 “[Using the Initial Setup Wizard](#)” section on page 2-1). At least one of these interfaces must be 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 your 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 and Recovery Guide for UCS Platforms](#) 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. [Table 1-4](#) summarizes the supported configuration depending on the running services.

**Table 1-4** Supported Ethernet Configurations

Server Services	Ethernet Port Configuration
Co-located system (Operations Manager and Media Server hosted on the same server)	<p>Only one interface can be enabled (static or DHCP). The other interface must be disabled. Verify that the Operations Manager server hostname resolves to only one (correct) address.</p> <p><b>Note</b> Only one interface should be enabled and active on the server. Dual-homed/NAT server configurations are not supported on any server running the Operations Manager service.</p> <p><b>Note</b> The Media Server must be added to the browser-based Operations Manager configuration to access the network settings.</p>
Operations Manager-only system	<p>Only one interface can be enabled (static or DHCP). The other interface must be disabled. Verify that the Operations Manager server hostname resolves to only one (correct) address.</p> <p><b>Note</b> Verify that only one interface is enabled and active on the server. Dual-homed/NAT server configurations are not supported on any server running the Operations Manager service.</p>
Media Server-only system	<p>At least one Ethernet port must be enabled. The following combinations are supported:</p> <ul style="list-style-type: none"> <li>• Both interfaces configured static.</li> <li>• One interface static and the other disabled.</li> <li>• One interface configured static and the other DHCP.</li> </ul> <p><b>Note</b> Dual-homed/NAT server configuration is supported only for stand-alone Media Servers.</p>

### Usage Notes

- At least one static interface must be configured.
- See the [“Using DHCP” section on page 1-11](#) for information regarding DHCP interfaces.
- See the [“Network” section on page 4-3](#) 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 4-24](#).

## 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 4-3](#).

### 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

# Using the Initial Setup Wizard

---

Complete the following procedures to set up a Cisco Video Surveillance server the first time you log on to the Cisco VSM Management Console.

Refer to the following topics for more information.

- [Accessing the Setup Wizard, page 2-1](#)
- [Usage Notes, page 2-1](#)
- [Completing the Setup Wizard, page 2-1](#)
- See also [System Setup, page 4-1](#)

### 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 1-7](#) and [Default Ethernet Interface Settings, page 1-9](#)).

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 service.
- 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 server services to restart, if the setting is modified. 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** Select the *Services* that will run on the server, and click **Next**.

See the “[Services](#)” section on page 4-1 for more information.

**Step 2** Select the date and time settings, and click **Next**.

See the “[Date and Time](#)” section on page 4-5 for more information.

**Step 3** Enter the *Network* settings and click **Next**.

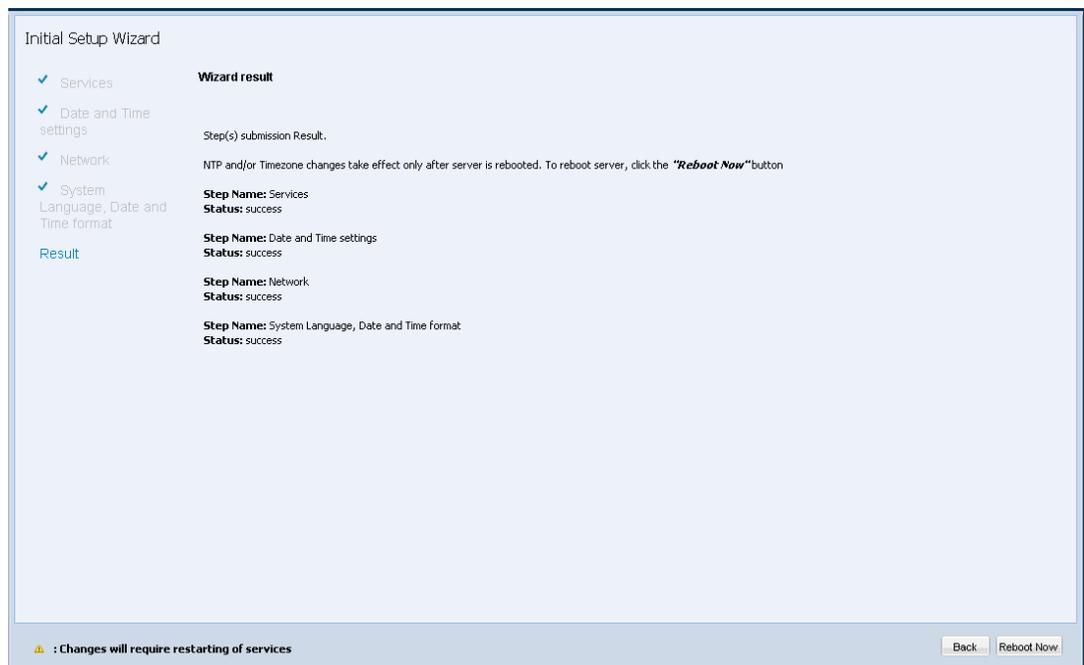
See the “[Network](#)” section on page 4-3 and the “[Configuring the Server Ethernet Ports](#)” section on page 1-9 for more information:

**Step 4** Enter the *System Language, Date and Time Format* settings and click **Next**.

See the “[Language Settings](#)” section on page 4-8.

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

**Figure 2-1** Wizard Result



**Step 6** Click **Reboot 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 4-9](#)—create and install a custom SSL certificate, if required (a self-signed certificate is used by default).
- [System Setup, page 4-1](#)—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](#)” section on page 4-11—manage Media Server attributes such as SNMP trap destinations.
- “[Maintenance](#)” section on page 4-13—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.
-





## 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, page 3-2](#)
- [Device List, page 3-3](#)
- [Mediaout Statistics, page 3-6](#)
- [Recordings, page 3-8](#)
- [Streams, page 3-10](#)
- [Installed Packages, page 3-11](#)
- [Logs, page 3-12](#)
- [System Trends, page 3-14](#)
- [Hardware Status, page 3-18](#)
- [Audit Logs, page 3-23](#)

# 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
Platform Origin Type	(VM installations only)
Platform Origin SubType	(VM installations only)
Platform Origin Version	(VM installations only)
Server Model	The server model. For example, <i>CIVS-MSP-IRU</i> is a Cisco Multiservices Platform server that requires 1 rack unit.
BIOS Version	The system BIOS version number.
Number Of CPU	The number of CPUs in the Linux system.
Number of Logical Cores	The number of processing cores in the system.
Processor Model Name	The processor model. For example: Intel(R) Core(TM)2 Duo CPU E4300 @ 1.80GHz
Total Physical Memory	The total amount of physical memory.
Total Swap Memory	The total amount of memory available for paging.
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.
Fiber Channel Port Name	Servers with FC card only.
Fiber Channel Port ID	<b>Note</b> The Cisco Physical Security UCS series servers do not display the status of FC port-0.
Fiber Channel Port Link State	
Fiber Channel Port Type	<b>Note</b> The Cisco Physical Security UCS series servers require a service restart to see updated FC link status..
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, network ports or storage.

**Table 3-1** System Summary

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 Video Surveillance server, but only one instance of Operations Manager is used to manage all of the Media Servers. See the <a href="#">“Feature Summary” section on page 1-3</a> for more information. To enable or disable Operations Manager on a server, see the <a href="#">“Services” section on page 4-1</a> .
Service Status	Displays the aggregate status of the services running on the server and the status of the corresponding components.  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 1-7](#)). 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 Media Server.

### Procedure

**Step 1** From the **Monitor** tab, expand the **Media Server** menu and click **Device List**.



**Step 2** Select a device type from the Device Filter menu ([Figure 3-1](#)):

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

**Step 3** Click **Search Now**.

**Step 4** Use the column headings to sort the results.

[Table 3-2](#) describes the available device information:

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 <i>true</i> or <i>false</i> .
IP Address	IP cameras and encoders	The network address of the device. <b>Note</b> 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 <i>true</i> or <i>false</i> .
Security	All devices	Indicates if the network communication is <i>secured</i> or <i>unsecured</i> .
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 <a href="#">Cisco Video Surveillance Operations Manager User Guide</a> for more information.
Device UID	All devices	The unique ID assigned to each device. See the <i>Cisco Video Surveillance API Programming Guide</i> located on the Cisco Developers Network (CDN) for more information on using the device UID.
Encoder IP/Hostname	Analog Cameras	The IP address or hostname of the encoder associated with the analog camera. Click the encoder address to view device details in a pop-up window ( <a href="#">Figure 3-1</a> ).

Figure 3-1 Device List

The screenshot shows the 'Device List' interface. At the top, there is a 'Device Filter' dropdown set to 'Analog Cameras' and a 'Search Now' button. Below this is the 'Analog Camera List' table. The table has columns for Name, Vendor, Model, PTZ Supp..., Motion Dete... Supp..., Secu..., Num... of Reco..., Admin State, Device UID, and Encoder IP/Hostname. Eight rows of camera data are visible, all with 'Generic' as the vendor and '10.104.183.160' as the encoder IP. A red arrow points to the 'Encoder IP/Hostname' column of the first row. A pop-up window titled 'Associated encoder details for wowza\_1' is overlaid on the table, displaying the following information: IP/Hostname : 10.104.183.160, Device UID : d293emFtdGVzdF9lbmNvZGVy, Model : civs-aenc-8P, Port Type : VIDEO, and Port Number : 1. A 'Close' button is at the bottom of the pop-up.

Name	Vendor	Model	PTZ Supp...	Motion Dete... Supp...	Secu...	Num... of Reco...	Admin State	Device UID	Encoder IP/Hostname
wowza_1	Generic	generic_analog	false	false	secur...	0	disab...	a8f88831-a098...	10.104.183.160
wowza_2	Generic	generic_analog	false	false	secur...	0	disab...	d939d342-b8ee...	10.104.183.160
wowza_3	Generic	generic_analog	false	false	secur...	0	disab...	eba20b19-1106...	10.104.183.160
wowza_4	Generic	generic_analog	false	false	secur...	0	disab...	5f4ad8dd-ce79...	10.104.183.160
wowza_5	Generic	generic_analog	false	false	secur...	0	disab...	8254e83a-f795...	10.104.183.160
wowza_6	Generic	generic_analog	false	false	secur...	0	disab...	c039890f-ef32...	10.104.183.160
wowza_7	Generic	generic_analog	false	false	secur...	0	disab...	ca149fdd-fa1c...	10.104.183.160
wowza_8	Generic	generic...							10.104.183.160

# Mediaout Statistics

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

From the **Monitor** tab, expand the **Media Server** menu and click **Mediaout Statistics**.



Select either the [Mediaout Summary](#) or the [Mediaout Detail](#) radio button.

## 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 3-3](#) describes the summary information.

**Table 3-3** *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.

## Mediaout Detail

**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 3-10](#) 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 3-4).

**Table 3-4** *Mediaout Connection Details*

Item	Description
Connection Type	The network protocol used to deliver video (RTSP or HTTP).
Device Name	The camera name. Click an entry to view additional camera details, such as the camera make and model, IP address, PTZ and motion detection support, and the number of recording associated with the camera.
Stream 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.).
Sub Session Type	The format used for video recording, compression, and distribution. For example H.264 is used for high-definition video and internet streaming.
IP Address	The destination network address for the video stream.
Up Time (in Seconds)	The number of seconds that the Media Server has been sending the video stream to the endpoint.
Transport	Transport protocol used for the stream (TCP or UDP).
Port	Port on the server from which the stream is being sent.
Average Throughput (in Bps)	Average bandwidth used by the stream, in bytes per second.
Average FPS	Average frames per second send in the stream.
Lost Frames	Number of frames dropped by the stream.
Lost RTP	Number of RTP packets dropped by the stream.

# 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, expand the **Media Server** menu and click **Recordings**.
- Step 2** Select a camera from **Device Name** (or select **All** to display information for all cameras).
- Step 3** Click **Go**.
- Step 4** Review the information (Table 3-5).

**Table 3-5** Recordings Information

Item	Description
Recording Name	Unique ID of the recording.
Device Name	The camera name. Click an entry to view additional camera details, such as the camera make and model, IP address, PTZ and motion detection support, and the number of recording associated with the camera.
Stream Name	Unique ID of the camera video stream. Click the name to display stream properties, including the camera admin state, transport type and video configuration details (resolution, codec, etc.).
Type	Recording types include the following: <ul style="list-style-type: none"> <li>• Regular—The recording is configured as a regular archive, which runs for a set duration</li> <li>• Loop—The archive is configured as a loop archive, which repeats contains data for a set duration</li> </ul>
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: <ul style="list-style-type: none"> <li>• CONFIG</li> <li>• RUNNING</li> <li>• SHELVED</li> <li>• PAUSED</li> <li>• FAILED</li> </ul>

**Table 3-5 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: <ul style="list-style-type: none"> <li>• notaclip (the recording is a system recording and was not saved as a clip).</li> <li>• native</li> <li>• mp4</li> <li>• bwm</li> <li>• bwx</li> </ul>
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: <ul style="list-style-type: none"> <li>• mpeg4</li> <li>• JPEG</li> <li>• h264</li> </ul>
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, expand the **Media Server** menu and 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 3-6](#) describes the information that the list provides.

**Table 3-6 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, <i>720p</i> 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 3-6 Streams Information (continued)**

Item	Description
Secured	If <i>True</i> , 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.

## Installed Packages

The **Installed Packages** window displays the services enabled on the server.

This window also displays the Additional Driver Packs installed on the server. These driver packs enable cameras and encoders driver on the server.



### Tip

See the [“Server Upgrade”](#) section on page 4-15 for instructions to update and manage the installed software packages. See the [“Manage Drivers”](#) section on page 4-21 to update the *driver packs* used by Media Server and Operations Manager to interoperate with video devices.

### Procedure

- 
- Step 1** From the **Monitor** tab, click **Installed Packages**.
- Step 2** Use the column headings to sort the results.
-

# 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 4-13](#).

**Procedure**

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

- Step 1** From the **Monitor** tab, click **Logs**.
- Step 2** Select a **Service**, such as the **Operations Manager** (VSOM) or **Media Server**.
- Step 3** Select a service or process from the **Search** menu. The options correspond with the selected service.

**Table 3-7 Log Options and Descriptions**

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

Table 3-7 Log Options and Descriptions (continued)

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

- Step 4** (Optional) Enter search text in the *Text Pattern* field to display only the log lines that includes that text.
- Step 5** Select the number of lines to display.  
The system can display the most recent 500 or 1000 entries.
- Step 6** (Optional) Select the *refresh (30 sec)* check-box to automatically perform the search every 30 seconds.
- Step 7** Click **Search Now** to display the log records. The results are displayed from the most recent log entry.

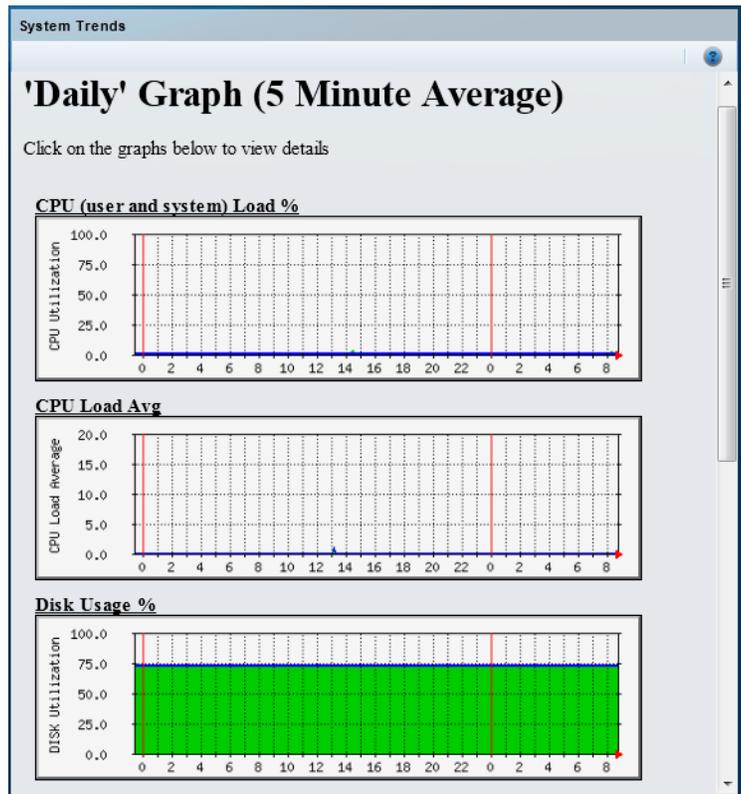
# System Trends

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 3-2](#).

Refer to the following topics for more information:

- [Viewing Current Reports, page 3-15](#)
- [Viewing Historical Reports, page 3-15](#)
- [Understanding Graph Data and Colors, page 3-16](#)

**Figure 3-2** System Trends



### Viewing Current Reports

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

**Table 3-8** 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 %	Green Displays the CPU resources that are consumed by user applications, as a percentage of total CPU capacity. Blue Displays the CPU resources that are consumed by system operations, as a percentage of total CPU capacity.
Disk Usage %	Green Displays the amount of used disk space, as a percentage of total disk capacity.
Traffic Analysis	Displays the amount of incoming and outgoing network traffic, in bytes per second.
Physical Memory Usage %	Displays the percentage of physical memory being used.
Swap Memory Usage %	Displays the percentage of Swap memory being used.

### Viewing Historical Reports

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

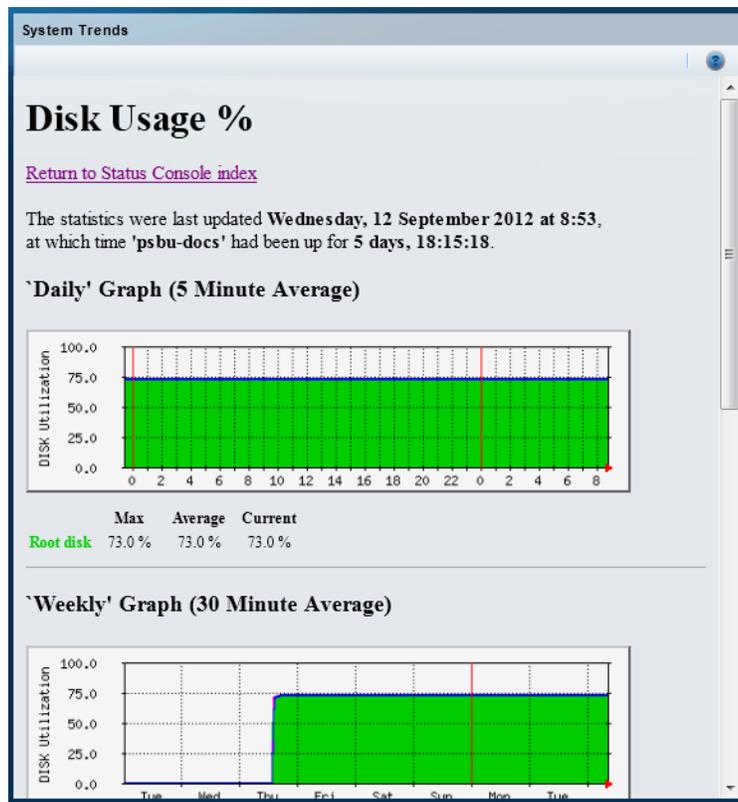
- Daily graph—Provides information for the past 32 hours, calculated by averaging values every 5 minutes. The information in this graph is the same as the default page (see the “[Viewing Current Reports](#)” section on page 3-15).
- Weekly graph—Provides information for the past 8 days, calculated by 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 3-16 for more information.

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

**Figure 3-3** 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 3-9 describes the information provided by each report:

**Table 3-9 Data and Line Color Descriptions**

<b>Color</b>	<b>Description</b>
<b>CPU (user and system) Load %</b>	
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.
<b>CPU Load Avg</b>	
Green	Displays CPU load average on the server.
<b>Disk Usage %</b>	
Green	Displays the amount of disk space, as a percentage of total disk capacity.
<b>Traffic Analysis</b>	
Green	Displays the amount of incoming network traffic, in bytes per second.
Blue	Displays the amount of outgoing network traffic, in bytes per second.
<b>Physical Memory Usage %</b>	
Green	The percentage of used physical memory, excluding buffers and cached.
<b>Swap Memory Usage %</b>	
Green	The percentage of used Swap memory.

# 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 3-18](#)
- [Viewing Hardware Status, page 3-19](#)
- [Viewing RAID and Physical Drive Status, page 3-20](#)

## 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 3-10](#) for descriptions of each field.

**Table 3-10** 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 3-11](#) for descriptions of each field.

**Table 3-11** 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

The RAID Status page (Figure 3-4) displays information if a RAID is installed on a Cisco Multiservice Platform that includes an LSI MegaCLI compliant RAID controller. This page also lets you silence alarms that occur when a RAID failure occurs or when the RAID array is rebuilding, and generate a debug package.

### Procedure

- 
- Step 1** Select **Hardware Status**.
- Step 2** Select **RAID** from the drop-down menu and click **Go**.
- Step 3** Select a *Virtual* drive to display information about the associated physical drives (see Figure 3-4).
- Step 4** Click a virtual or physical drive number to display additional drive details in a pop-up window.

Table 3-12 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 3-12 RAID Drive Status**

Field	Description
Alarm 	<p>The alarm icon  is displayed if an alarm occurs for one or more physical drives.</p> <ul style="list-style-type: none"> <li>View the physical drive(s) that caused the alarm.</li> <li>Click <b>Silence Alarm</b> to silence the RAID controller alarm.</li> </ul> <p>The timestamp is updated for virtual drives only.</p>
Virtual Drives	<p>The RAID drives configured on the server. The possible states are:</p> <ul style="list-style-type: none"> <li><i>Optimal</i>—the RAID is working normally</li> <li><i>Degraded</i>—one or more RAID drives are missing or not operational but is still operating with reduced performance</li> <li><i>Offline</i>—two or more RAID drives are missing or not operational, making the RAID inoperable.</li> </ul>
State	<p>The current drive status.</p> <ul style="list-style-type: none"> <li><b>Missing</b>—Provides information when a hard drive is not detected.</li> <li><b>Rebuild</b>—Provides information when hard drive is rebuilding.</li> <li><b>Optimal</b>—Provides information when a hard drive is rebuilt and operating.</li> </ul>
Alarm Timestamp	<p>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.</p> <p>The timestamp is updated for virtual drives only.</p>

**Table 3-12 RAID Drive Status (continued)**

Size	The amount of storage available on the drives.
Number of Drives	The number of physical drives.
Access Policy	Read/Write access to the drive.
<b>Physical Drive Information</b>	
Physical Drives	Physical drives are listed by their physical location. For example: <i>Sx</i> =the slot and enclosure number.  <b>Note</b> 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: <i>Online</i> , <i>Spun Up</i> , or <i>Rebuilding</i> .
Alarm Timestamp	The time when a non-optimal condition was recognized. A timestamp is displayed only if the drive is in an alarm state and has not rebuilt successfully or been replaced.  The timestamp is updated for virtual drives only.
Slot Number	The physical slot location in the server.  For example, 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.
Media Error Count	The number of errors that occurred when reading, writing, or accessing data on the hard drive.  These errors are usually related to the drive platters (media) and related mechanism.
Other Error Count	All other hard drive behaviors, such as failed commands, the drive resetting or needing to be reset, and any other error not included in the Media or Predictive error counts.
Predictive Error Count	Predictive errors are similar to SMART errors, which indicate possible future failure of the drive to the hard drive or RAID controller.
Raw Size	The size of the disk drive.

Figure 3-4 shows a sample RAID Status page. A Virtual Drive is selected to show the physical drives.

Figure 3-4 RAID Status

The screenshot displays the RAID Status page. At the top, there is a 'Status for:' dropdown menu set to 'RAID' and a 'Go' button. Below this is the 'RAID Status' section, which contains a table with columns: Virtual Drive, State, Alarm Timestamp, Size, Number Of Drives, and Access Policy. The table shows two virtual drives, both in an 'Optimal' state with a size of 11,999 GB and 12 drives each.

Below the RAID Status is the 'Physical Drives' section, which contains a table with columns: Physical Drive, State, Alarm Timestamp, Slot Number, Media Error Count, Other Error Count, Predictive Failure Count, and Raw Size. The table lists 10 physical drives (E0:S0 to E0:S9), all in an 'Online' state.

A modal window titled 'Physical Disk Detail' is open, showing detailed information for the selected physical drive (E0:S0). The details include:

- Name : E0:S0
- State : Online
- Enclosure Device Id : 0
- Device Id : 1
- Slot Number : 0
- sequence Number : 2
- Media Error Count : 0
- Other Error Count : 0
- Predictive Failure Count : 0
- Last predictive Failure Event Sequence number : 0
- PD Type : SATA
- Raw Size : 931.512 GB [0x74706db0 Sectors]
- Non Coerced Size : 931.012 GB [0x74606db0 Sectors]
- Coerced Size : 930.390 GB [0x744c8000 Sectors]
- Firmware State :
- Connected Port Number : 0(path0)
- Inquiry Data : JPW9K0HD2DGSXLHitachi HUA722010CLA330 JP4OA3EA
- FDE Capable : Not Capable
- FDE Enable : Disable
- Secured : Unsecured
- Locked : Unlocked
- Foreign State : None
- Device Speed : 3.0Gb/s
- Link Speed : 3.0Gb/s
- Media Type : Hard Disk Device

# 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

## Administration

---

The Administration tab includes the following topics:

- [System Setup, page 4-1](#)
- [Media Server, page 4-11](#)
- [Maintenance, page 4-13](#)
- [Restart Services, page 4-24](#)
- [Reboot Server, page 4-25](#)
- [Shut Down Server, page 4-25](#)

## System Setup

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:

- [Services, page 4-1](#)
- [Network, page 4-3](#)
- [Date and Time, page 4-5](#)
- [Reset Password, page 4-7](#)
- [Language Settings, page 4-8](#)
- [Security, page 4-9](#)

## Services

Use the *Services* setting to activate or deactivate services running on the server. At least one service must be enabled.

Services include features such as the Media Server and/or Operations Manager. When the server is added to the Operations Manager configuration, those services are available to the system and you can configure additional service settings.

For example, when a server running the Media Server service is added to the browser-based Operations Manager, you can configure the Media Server partitions and high-availability role. The Media Server can also be used for camera and video processing.

### Activating and Deactivating Services

The Management Console interface can be used to activate or deactivate services according to the following:

- After a server is added to the Operations Manager configuration, the Management Console can only be used to activate or deactivate the Operations Manager (VSOM) service. Use the Operations Manager to activate or deactivate other services, such as the Media Server.
- The Media Server service cannot be activated or deactivated using the Management Console after the server is added to the Operations Manager configuration.
- You can deactivate the Operations Manager (VSOM) service even if the Media Server is running on the same server or if the Operations Manager is managing other Media Server. The Operations Manager (VSOM) will stop managing the Media Servers and associated cameras, so that another Operations Manager can take ownership of these Media Server and associated cameras and start managing them.

### Disassociate a Server

Click the **Remove** button to disassociate the server and all server services from the Operations Manager (Figure 4-1). This allows the server (and running services) to be added and managed by a different Operations Manager.

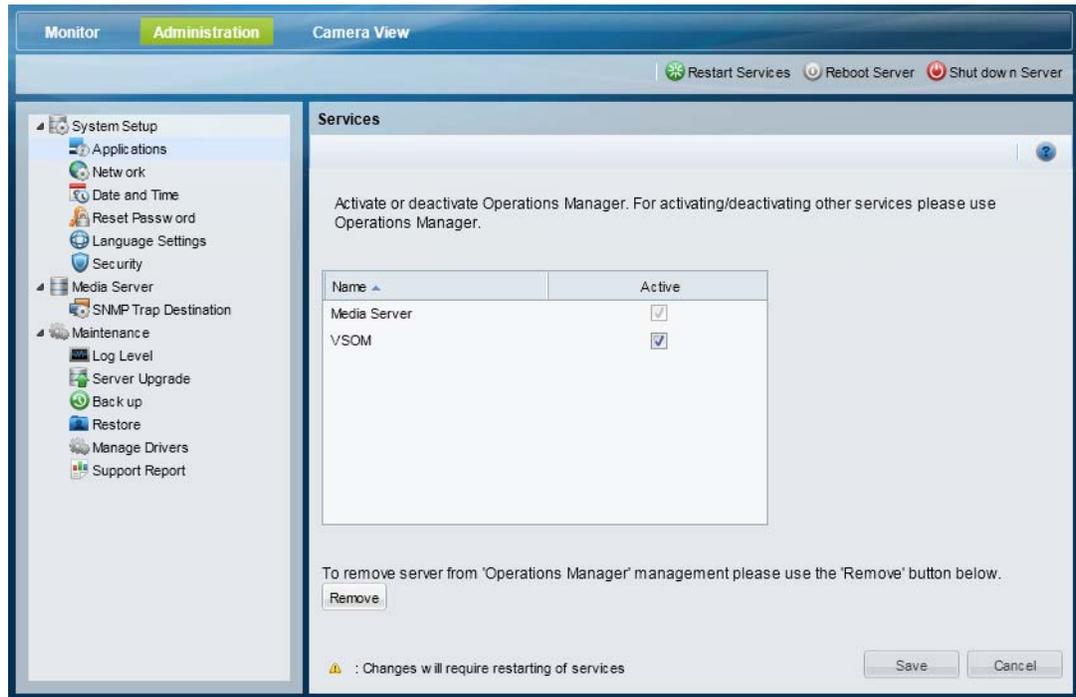
### Understanding Co-Located Servers

- 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.

### Procedure

- 
- Step 1** Click the **Administration** tab and then click **Services** (Figure 4-1).
- Step 2** Select or de-select the following services (Figure 4-1).
- **Media Server**—Enables the Media Server service for camera hosting and video processing.
  - **VSOM**—Enables the browser-based Cisco VSM Operations Manager administration and configuration tool.
- Step 3** Click **Save**.
- Step 4** Restart the system services, if prompted.
-  Changes require you to restart server services and log back in.
  - Restarting services can take up to 90 minutes or more depending on number of devices managed by the Operations Manager and Media Server. Installed products will be offline during this time.

Figure 4-1 Services



### Related Topics

- [Logging In, page 1-7](#)
- [Feature Summary, page 1-3](#)
- [Configuring the Server Ethernet Ports, page 1-9](#)
- [Restart Services, page 4-24](#)

## Network

The *Network* settings (Table 4-1) 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 1-9](#) for information regarding the Ethernet port settings used to support the services 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.
- Multiple DNS servers are not supported.

VSM 7 allows configuring more than one DNS server in the Cisco VSM Management Console. However, VSM 7 does not preserve the order in which they are used, which can result in a Configuration Mismatch error in VSOM in some cases. If this situation occurs, perform the Repair Configuration procedure to clear the error. To avoid this situation, configure only one DNS server for VSM 7 deployments.

- Operations Manager-only systems can include one static interface and one DHCP interface.

**Table 4-1 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)	<p>Select one of the following options based on the enabled server services. See the <a href="#">“Configuring the Server Ethernet Ports”</a> section on page 1-9 for more information.</p> <ul style="list-style-type: none"> <li>• <b>Static IP</b>—if selected, you must also enter the <b>IP address</b> and <b>Subnet Mask</b> for the interface.</li> <li>• <b>DHCP</b>—the IP address, Default Gateway, DNS Servers, and Search Domain(s) are disabled and will be defined by a DHCP server. See the <a href="#">“Using DHCP”</a> section on page 1-11.</li> <li>• <b>Disable</b>—disables the interface.</li> </ul> <p><b>Note</b> At least one interface must be set to static for proper functioning of the system.</p> <p><b>Note</b> Multiple DNS servers are not supported.</p>
Default Gateway	(Disabled when DHCP is enabled) Enter the IP address of the default gateway and click <b>Add</b> .
DNS Servers	<p>(Optional: Disabled when DHCP is enabled) Enter one domain name service (DNS) server.</p> <p><b>Note</b> If the Operations Manager address entered in the <a href="#">“Services”</a> section on page 4-1 is a hostname, a DNS server is required for Media Servers to resolve the associated IP address.</p> <p><b>Note</b> Multiple DNS servers are not supported.</p> <p>To add a DNS entry, enter the IP address in the entry field and click <b>Add</b>. To remove an entry, highlight the IP address and click <b>Remove</b>.</p>
Search Domain(s)	(Optional, Disabled when DHCP is enabled) Enter the domain name to search in the entry field and click <b>Add</b> . To remove an entry, highlight the domain and click <b>Remove</b> .

### Procedure

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

- Step 2** Edit the network settings described in [Table 4-1](#).
- 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 4-1](#)).
- 

#### Related Topics

- [Logging In, page 1-7](#)
- [Configuring the Server Ethernet Ports, page 1-9](#)
- [Restart Services, page 4-24](#)

## 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.



#### Note

The *Date and Time* settings (in the Management Console) are disabled after the Media Server is added to the Operations Manager configuration.

---

#### 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 services hosted by the server.

- **Operations Manager-only servers**
  - Always use the **NTP** server option (see [Table 4-2](#)).
  - 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**
  - The *Date and Time* settings (in the Management Console) are disabled after the Media Server is added to the Operations Manager configuration. 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 than 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 4-2 Time Mode Settings**

Mode	Settings
Manual	Select the date, time and time zone for the server.
NTP	(Recommended) Click <b>Add</b> 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 4-2):
- 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 username *localadmin* cannot be changed.

### Procedure

To reset the currently configured password, do the following:

- 
- Step 1** Click **Administration > 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 4-15.

### Procedure

- Step 1** Click the **Administration** tab and then click **Language Setting**.
- Step 2** Enter the *Language Settings* ([Table 4-3](#)).
- 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 4-3** *Language Settings*

Setting	Description
<b>System Language</b>	Select a supported language for the user interface text.
<b>Date Format</b>	<p>Select the date format displayed in system messages, alerts, and other generated information.</p> <p>For example, <b>MM/DD/YYYY</b> means that dates will appear as month, day, and year.</p> <ul style="list-style-type: none"> <li>d, dd = day</li> <li>M = Month</li> <li>y = year</li> </ul>

**Table 4-3** Language Settings (continued)

<b>Time Format</b>	<p>Select the time format displayed in system messages, alerts, and other generated information.</p> <p>For example, <b>h:mm:ss tt</b> means that the time will be displayed as hours, minutes, and seconds, and include the AM/PM notation.</p> <ul style="list-style-type: none"> <li>• h = hour</li> <li>• m = minute</li> <li>• s = second</li> <li>• tt = A.M. or P.M.</li> <li>• h/H = 12/24</li> </ul> <p><b>Note</b> Select <b>hh</b>, <b>mm</b>, <b>ss</b> to display the leading zero (or <b>h</b>, <b>m</b>, <b>s</b> if the display leading zero should not be displayed).</p>
<b>Calendar</b>	<p>Select the day that should be considered the first day of the week.</p> <p>For example, <b>Monday</b>.</p>

## 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 4-2](#)).

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 4-9
- [Installing the .pem Certificate](#), page 4-10

### 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 [“Backup” section on page 4-17](#)). 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 4-10](#).

## 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*.

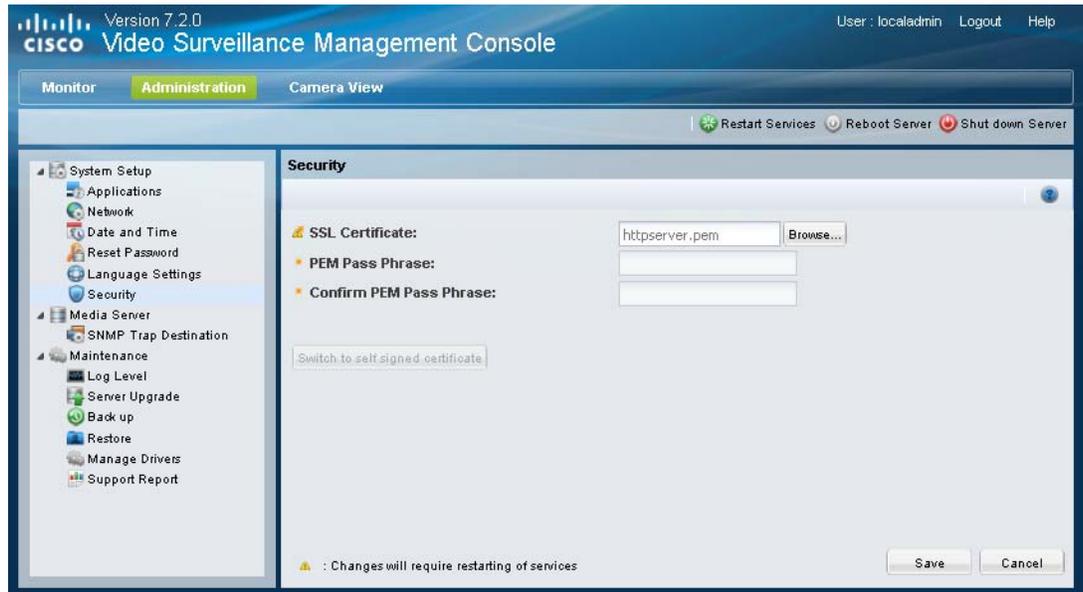
**Step 4** Click **Save**.

**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 4-2 Security



## Media Server

Use the Media Server options to manage the following attributes:

- [SNMP Trap Destination, page 4-11](#)



### Note

- The Media Server options are only available on servers running the Media Server service. See the [“Services” section on page 4-1](#) for instructions to enable or disable the Media Server.
- Use the browser-based Operations Manager to revise the Network Ports, Storage, Recording and Miscellaneous settings, if necessary.

## SNMP Trap Destination

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



### Note

- To view the supported traps and descriptions, click the link [“Click here to view the VS Event MIB file”](#).
- Cisco Video Surveillance supports SNMP version 2 (Inform)
- Running a third-party trap receiver on a Cisco Video Surveillance host is not supported.

### 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 **Add** 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 **Delete**.

---

**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 destination.

---

### (Optional) Change the SNMP Read Only Community String

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




---

**Note** The default string is a randomly generated value created during installation. You can change this string if necessary.

---



---

**Step 1** Enter a new read only community string.

**Step 2** Click **Save**.

---

# Maintenance

- [Log Level, page 4-13](#)
- [Server Upgrade, page 4-15](#)
- [Backup, page 4-17](#)
- [Restore, page 4-20](#)
- [Manage Drivers, page 4-21](#)
- [Support Report, page 4-23](#)
- [Restart Services, page 4-24](#)
- [Reboot Server, page 4-25](#)
- [Shut Down Server, page 4-25](#)

## 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 3-12](#) 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 4-14](#) for more information.
- **Operation Manager**—select ERROR, WARN, INFO, DEBUG, or TRACE.
- **Management Console**—select ERROR, WARN, INFO, DEBUG, or TRACE.

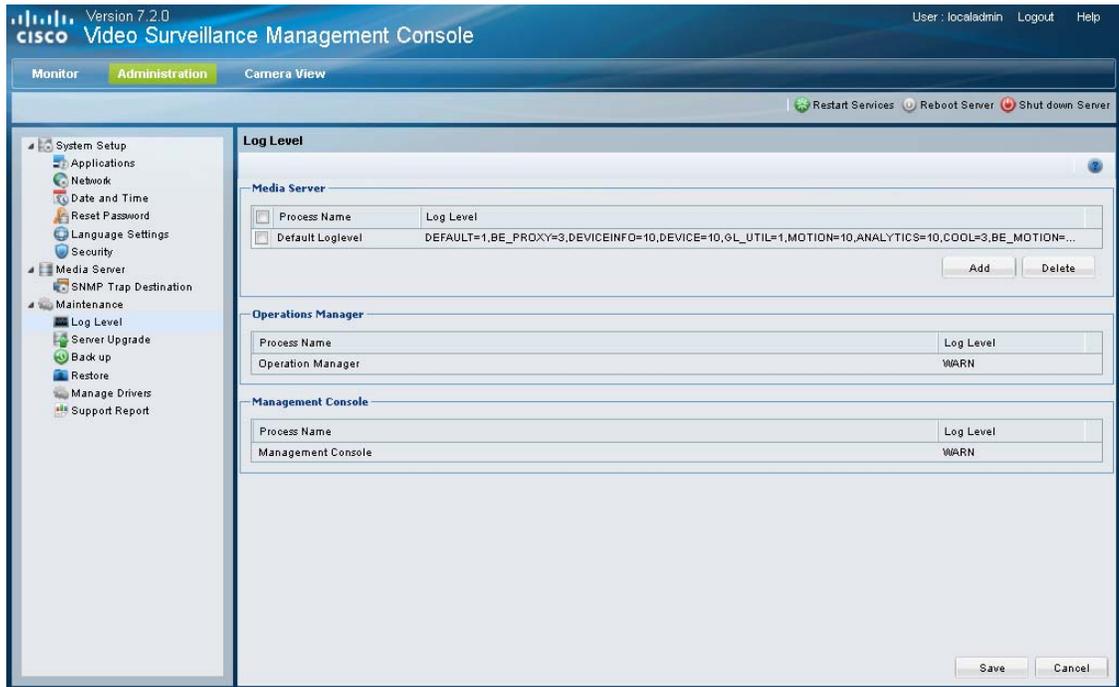


---

**Note**

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

Figure 4-3 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 **Add** to create a new log level entry.
- Step 2** Select the Process Name in the entry field. You can also enter the Process Name or edit a selected name.
- 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 **Monitor > Logs** to view the log information. See the “[Logs](#)” section on page 3-12.



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

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

## Server Upgrade

The Cisco VSM server software upgrade file is a `.zip` file that includes all required software packages for the Cisco Media Server, Operations Manager, Management Console, Cisco Video Surveillance Safety and Security Desktop client and other components.

Installing the `.zip` file upgrades all components and ensures that all packages are running the required versions.

Refer to the following topics for more information:

- [Upgrading Language Packs, page 4-16](#)
- [Usage Notes, page 4-16](#)
- [Upgrading a Linux Red Hat Server From Release 7.0.0 to 7.0.1, page 4-16](#)
- [Recovering From a Failed Upgrade, page 4-16](#)
- [Upgrade Procedure, page 4-17](#)



**Tip** See the “[Understanding Cisco Video Surveillance Software](#)” section on page 1-5 for a summary of the different software components.

### 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 7.2](#) for instructions to upgrade Cisco device firmware.
- In rare scenarios, a PC workstation firewall can cause the upgrade process to fail. If this occurs, temporarily disable the workstation firewall software until the upgrade is complete.
- The server upgrade process automatically restarts server services. See the “[Restart Services](#)” section on page 4-24 for more information.
- Installation is supported only if the RAID is in a non-bad, non-failed state.

### Upgrading a Linux Red Hat Server From Release 7.0.0 to 7.0.1

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



#### Tip

Open the **Monitor > System Summary** page to determine the server “OS Type”.

- 
- Step 1** Use an SSH client to access the Cisco VSM server and log in as *localadmin* user.
- Step 2** Enter the following command to update the date that the root user password was last set, where *date* is the current date in *yyyy-mm-dd* format:

```
[localadmin@linux:~]# sudo chage -d date root
```

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

---

### Recovering From a Failed Upgrade

If the upgrade fails or is interrupted, an error message (“work order file exists”) may appear when you attempt to perform the upgrade again. This can be caused by a corrupted file, or if a RPM package is missing from the .zip file. To complete the upgrade, you must manually delete the `upgradeinput` file from the upgrade directory, as described in the following steps.

- 
- Step 1** Use an SSH client to access the Cisco VSM server and log in as *localadmin* user.
- Step 2** Navigate to the `/usr/BWhttpd/upgrade/server/` directory.
- Step 3** Use **sudo** to delete the `Upgradeinput` file. For example:
- ```
[localadmin@linux:~]# sudo rm /usr/BWhttpd/upgrade/server/upgradeInput
```
- Step 4** Re-download the upgrade file, making sure that the upgrade package is complete.

**Step 5** Continue to the [“Upgrade Procedure”](#).

---

### Upgrade Procedure

---

**Step 1** Download the server software file.

- Navigate to the [Cisco Video Surveillance Manager download page](#) and select **Video Surveillance Media Server Software**. Select the correct release and follow the on-screen instructions.
- See the [Release Notes for Cisco Video Surveillance Manager, Release 7.2](#) for more information on downloading software and the packages included in a release.

**Step 2** Complete the [“Upgrading a Linux Red Hat Server From Release 7.0.0 to 7.0.1”](#) section on page 4-16, if necessary.

**Step 3** Select **Administration > Server Upgrade**.

**Step 4** 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 5** Click **Start Upgrade**.

**Step 6** 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 7** Wait for up to 90 minutes for the operation to complete and the server to restart.



**Note** If the upgrade fails, see the [“Recovering From a Failed Upgrade”](#) section on page 4-16 and the [“Upgrading a Linux Red Hat Server From Release 7.0.0 to 7.0.1”](#) section on page 4-16.

---

**Step 8** Re-login in the server when the login screen appears.

**Step 9** 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).

---

## Backup

Use the following procedures to backup and restore configuration data for the services running on the server, such as the Media Server and Operations Manager.

We recommend backing up the server services on a regular basis to ensure data is not lost in the event of a hardware failure. Backups are also used to restore the configuration when upgrading or moving to a new system.

- [Usage Notes, page 4-18](#)
- [Backup File Format, page 4-18](#)

- [Backup Procedure, page 4-18](#)
- [Restore, page 4-20](#)

### Usage Notes

- Backups include services on the current server only, and do not include data from other servers.
- Backups do not include video files. Use the high-availability feature to back up video files, as described in the [Cisco Video Surveillance Operations Manager User Guide](#).
- Configuration data includes user-configured settings, such as camera configurations. Historical data includes all user entered data *plus* logs and events.
- Automatically scheduled backups are not supported using the Management Console. Use the Operations Manager interface to schedule recurring backups. See the [Cisco Video Surveillance Operations Manager User Guide](#) for more information.
- 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 4-9](#) for more information.

### Backup File Format

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

**Table 4-4 Backup File Formats**

| Backup Data           | Format                                                                                                                                                      |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Config and Historical | <b>VSMS_<i>HostName</i>_yyyyMMdd_HHmms.DbBackup.tar.gz</b><br><b>Example:</b> VSMS_vsm-server_20121126_105943_1.0.62.DbBackup.tar.gz                        |
| Config Only           | <b>VSMS_<i>HostName</i>_yyyyMMdd_HHmms.configOnlyDbBackup.tar.gz</b><br><b>Example:</b><br>VSMS_vsm-server_20121126_103509_1.0.62.configOnlyDbBackup.tar.gz |

- *HostName*—the host name of the server running the service.
- *yyyyMMdd\_HHmms*—the date and time when the backup file was created.

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

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

### Backup Procedure



#### Note

We highly recommend backing up all services when any major configuration changes are made. Backups ensure the system data can be restored to the present state, if necessary.

|               | Field                                                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------|--------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Select Services                                        | Select the services to be backed up, such as the <b>Operations Manager</b> or <b>Media Server</b> . All services are selected by default.<br><br>A separate backup file is created for each service. You can restore services individually as described in the <a href="#">“Restore” section on page 4-20</a> .                                                                                                                                                                                                                             |
| <b>Step 2</b> | Backup Options                                         | <ul style="list-style-type: none"> <li>• <b>Configuration Only</b>— includes user-configured settings, such as camera configurations.</li> <li>• <b>Configuration Plus Historical Data</b> —includes all user entered data <i>plus</i> logs and events.</li> </ul>                                                                                                                                                                                                                                                                          |
| <b>Step 3</b> | Transfer backup file on server                         | Saves the backup file to the server being backed up.<br><br><b>Tip</b> After the file is saved to the server, you can download the file to a local drive.                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Step 4</b> | Transfer backup file to FTP server                     | Saves the file to an FTP server.<br><br>Enter the server address, file path where the file will be saved, username and password.                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Step 5</b> | Transfer File                                          | Click <b>Transfer File</b> to initiate the backup and save the file to the selected server location.<br><br>Once completed, the file is displayed under “Manage Backup Files”. <ul style="list-style-type: none"> <li>• VSOM=Operations Manager service backup.</li> <li>• VSOM=Media Server service backup.</li> </ul> See the <a href="#">“Backup File Format” section on page 4-18</a> for more information.<br><br><b>Note</b> This Operation happens in background. For progress details, please refer to the Management Console logs. |
| <b>Step 6</b> | Download the backup file to a local disk, if necessary | To restore a backup, the file must be located on a local disk or FTP server.<br><br>If saving the file to the current server (not the FTP server): <ol style="list-style-type: none"> <li>Wait for the backup file to appear in the “Manage Backup Files” list.</li> <li>(Optional) Select a backup entry and click <b>Download</b>. You can download one file at a time.</li> </ol><br><b>Note</b> Files saved to an FTP server can be restored directly from the FTP server.                                                              |

Figure 4-4 Backup

The screenshot shows the Cisco Video Surveillance Management Console Administration interface. The main content area is titled "Server backup" and contains the following sections:

- Backup data when the server is first configured, or after any subsequent configuration changes. The backup file can then be used to restore the server to a previously configured state.**
- Select Services:**  Media Server  VSOM
- Backup Options:**  Configuration Only  Configuration Plus Historical Data
- Transfer backup file on server** (selected)
- Transfer backup file to FTP server** (unselected)
  - FTP server:
  - File path on FTP server:
  - FTP Username:
  - FTP Password:
- Transfer File** button
- Manage Backup Files** table:
 

| File Name                                                                        | Date                | Size (Kb) |
|----------------------------------------------------------------------------------|---------------------|-----------|
| <input checked="" type="checkbox"/> VSOM_psbu-docs_backup_20130712_103553.tar.gz | 07/12/2013 10:35:57 | 782.61    |
| <input type="checkbox"/> VSMS_psbu-docs_20130712_103551_1.0.71.DbBackup.tar.gz   | 07/12/2013 10:35:53 | 32.03     |
- Delete** and **Download** buttons
- Last Backup Status** log window:
 

```
CONFIG_AND_HISTORY backup started for services : [vsom, vsom]
===== vsom =====
making backup to file VSMS_psbu-docs_20130712_103551_1.0.71.DbBackup.tar.gz ...
Getting VSOM files ...
Cleaning up source and tar files
Grooming backups greater than 30 days old from /usr/BW/httd/root/httdocs/download/ ... done
backup completed successfully
```

## Restore

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



### Note

- Restoring a backup requires the server services to restart.
- Backups for each service can be restored one at a time. Perform multiple restore operations to restore multiple services.
- 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 4-9 for more information.

### Procedure

|               | Field                                                                  | Description                                                                                                                                                                                                                                                                                    |
|---------------|------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Select Services                                                        | Select the service to be restored. You must restore each services individually.<br><b>Note</b> A separate backup file is created for each service as described in the “Backup” section on page 4-17.                                                                                           |
| <b>Step 2</b> | Restore System Configs                                                 | Restores all system configurations such as network settings, language settings, date time, log level, SMTP, and the enabled services.                                                                                                                                                          |
| <b>Step 3</b> | Use file on PC                                                         | Click <b>Browse</b> and select a <code>.tar.gz</code> backup file.<br><b>Tip</b> Files saved to the server must be downloaded to a local drive. See the “Backup” section on page 4-17 for instructions.<br><b>Note</b> See the “Backup File Format” section on page 4-18 for more information. |
| <b>Step 4</b> | Use file on FTP                                                        | Restores a file that was saved on an FTP server.<br>Enter the server address, file path and file name where the file is located, username and password.                                                                                                                                        |
| <b>Step 5</b> | <b>Restore.</b>                                                        | Click <b>Restore</b> to initiate the restore process. <ul style="list-style-type: none"> <li>• The server services will automatically restart.</li> <li>• Click <b>Yes</b> to confirm and continue.</li> </ul>                                                                                 |
| <b>Step 6</b> | Wait for the operation to complete and the server services to restart. | A success message appears when the operation is complete and the services have restarted.                                                                                                                                                                                                      |
| <b>Step 7</b> | 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 or features.

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



#### Tip

See the “Understanding Cisco Video Surveillance Software” section on page 1-5 for descriptions of the different software types.



#### Note

We strongly recommend upgrading driver packs using the Operations Manager interface. This allows you to upgrade multiple servers at once. Driver packs must be upgraded to the same version on each server where the Media Server and Operations Manager services are enabled. The Management Console interface described in this section allows you to upgrade the driver packs for the current server only. Using the Management Console, you must log in to each server to upgrade the drivers.

### Usage Notes

- Driver packs must be upgraded to the same version on each server where the Media Server and Operations Manager services are enabled. For example, if your deployment includes a stand-alone 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.
- Driver packs can be upgraded but not downgraded.
- 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 4-5).
- See the [Release Notes for Cisco Video Surveillance Manager, Release 7.2](#) 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 7.2](#) 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** Upload the new driver pack software file to the server.
- a. Click **Add**.
  - b. In the pop-up window, click  icon and select a valid `.zip` driver pack file from a local or network disk. For example: `dp_cisco-2.0-16d_7.2-331d_sles10-sp1.zip`
  - c. Click **Upload** and wait for the upload to complete.  
The driver pack status is “Not Installed”.
- Step 4** (Optional) Click the **Detail** icon  to display important information about the release, and the impact of upgrading to the new driver pack (Figure 4-5).
- Step 5** Install the driver pack file on the server.
- a. Select a driver pack from the list.
  - b. Click **Install**.

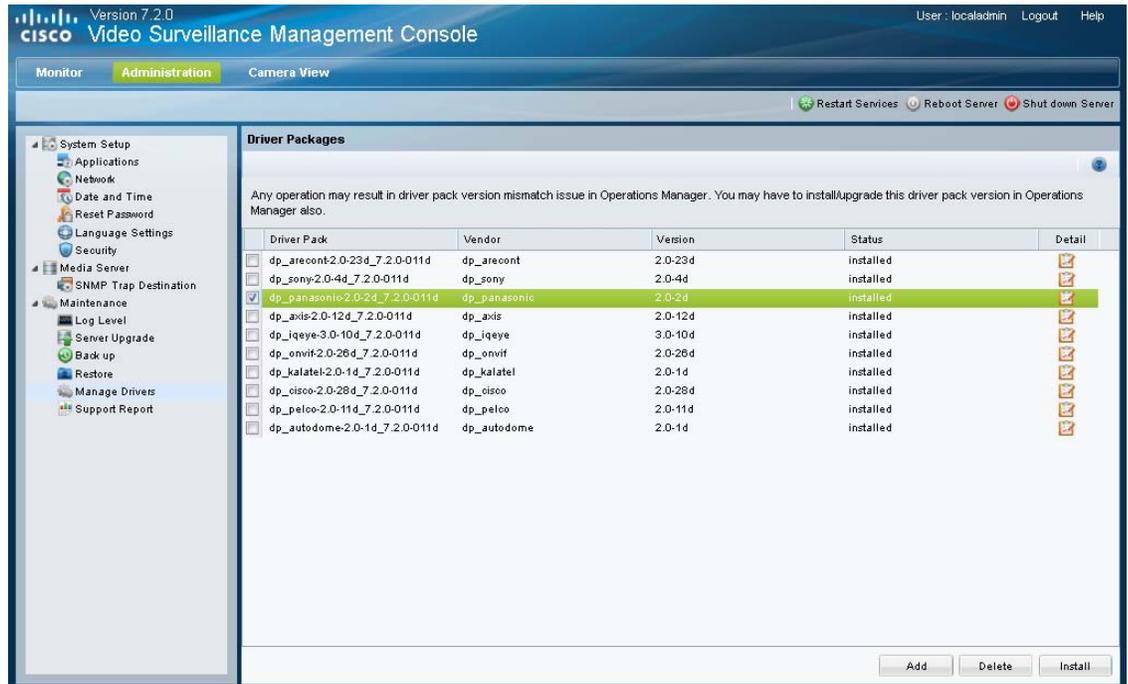


#### Caution

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

- Step 6** Complete these steps for each server that hosts a Media Server or Operations Manager.
- (Recommended) Use the Operations Manager interface to upgrade multiple servers at once. Driver packs must be upgraded to the same version on each server where the Media Server and Operations Manager services are enabled.
  - (Alternative) Log in to the Management Console for each server and upgrade the driver pack software to the same version.

Figure 4-5 Manage Drivers

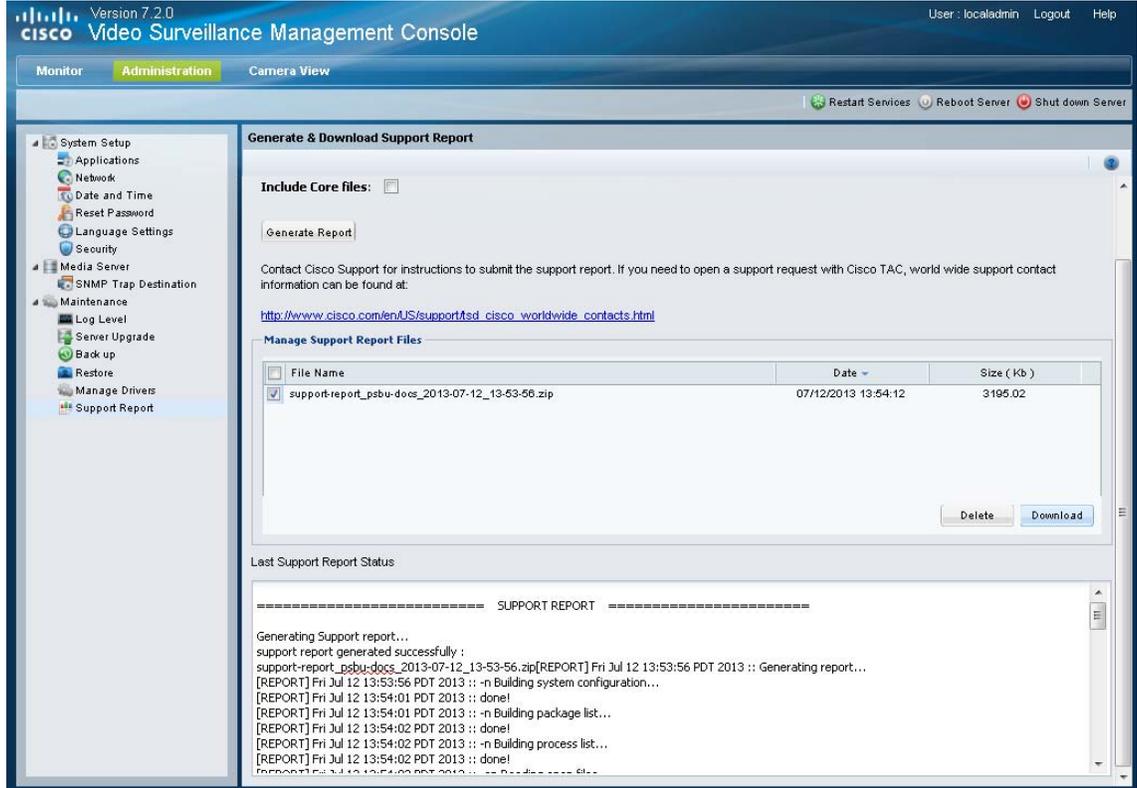


## Support Report

### Procedure

- Step 1** (Optional) Select **Include Core Files** to generate core files on the system. This is useful if any Media Server processes crashed at runtime.
- Step 2** Click **Generate Report** to create a new support report (as a .zip archive file).
- Step 3** Select a report entry and click **Download** to save the .zip file to a local drive.
- Step 4** 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](http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html)

Figure 4-6 Support Report



## Restart Services

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

- Changes to 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.
- 

## Shut Down Server

Use **Shut down 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 **Shut down 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.
-





## CHAPTER 5

# 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 1-7](#)).
- Step 2** Click **Camera View** ([Figure 5-1](#)).
- 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 5-1** Camera View



## APPENDIX **A**

### Related Documentation

---

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

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





# APPENDIX **B**

## Revision History

---

Last Revised: August 2013

**Table B-1**      *Revision History*

| Release       | Document Revision Date | Change Summary                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Release 7.0.0 | October, 2012          | Initial draft.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Release 7.0.0 | February, 2013         | <ul style="list-style-type: none"><li>Revised the <a href="#">“Creating a Custom Certificate in .pem Format (Example)”</a> section.</li><li>Added information about virtual machine installation requirements (OVA image) to the <a href="#">“Overview”</a> section, including requirements for network and password settings.</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Release 7.0.1 | February, 2013         | <ul style="list-style-type: none"><li>Various minor edits and feature enhancements. See the <a href="#">Release Notes for Cisco Video Surveillance Manager</a> for more information.</li><li>Added support for multiple Media Servers in a co-located configuration. See the <a href="#">“Co-Located and Stand-Alone Server Configurations”</a> section.</li><li>“Mediaout Ports” renamed “Network Ports”.</li><li>Added the “Device UID” field to the <a href="#">“Device List”</a>.</li><li>Added a “Silence Alarm” button to the <a href="#">“Viewing RAID and Physical Drive Status”</a> page.</li><li>Added Virtual Disk and Physical Disk details to the <a href="#">“Viewing RAID and Physical Drive Status”</a> page.</li><li>Added the ability to view and download multiple backup and report files to the <a href="#">“Backup”</a> and <a href="#">“Support Report”</a> section on page 4-23 pages.</li><li>Backup files are saved to the server being backed up, or to an FTP server. Saved files can be downloaded to a local PC drive. See the <a href="#">“Backup”</a> section on page 4-17.</li><li>Physical and Swap memory usage graph stats are shown in percentage instead of absolute data. See the <a href="#">“System Trends”</a> pages.</li></ul> |

**Table B-1**      *Revision History (continued)*

| <b>Release</b> | <b>Document Revision Date</b> | <b>Change Summary</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Release 7.2.0  | August 2013                   | <ul style="list-style-type: none"><li>• Applications are now “services” that can enabled or disabled on the server. See the <a href="#">“Services” section on page 4-1</a>.</li><li>• Additional options and logs available in the <a href="#">“Logs” section on page 3-12</a>.</li><li>• All services can be backed up and other changes to the <a href="#">“Backup” section on page 4-17</a> and <a href="#">“Restore” section on page 4-20</a>.</li><li>• Most Media Server settings were removed and are now managed using the Operations Manager. See the <a href="#">“Media Server” section on page 4-11</a>.</li><li>• Additional minor changes, edits and updates.</li></ul> |