



Cisco Video Surveillance Operations Manager User 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-27060-07

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. 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 Operations Manager User Guide, Release 7.2
©2012- 2013 Cisco Systems, Inc. All rights reserved.



Preface

Revised: June 17, 2014

This document, the *Cisco Video Surveillance Operations Manager User Guide* provides an overview of Cisco Video Surveillance Operations Manager Release 7.2, including basic procedures that should be performed when you first start to use the system, and detailed information about advanced features and configurations.

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.



Tip

See [Related Documentation](#) for more information and links to Cisco Video Surveillance documentation.



CONTENTS

Preface iii

Related Documentation iii

Obtaining Documentation, Obtaining Support, and Security Guidelines iii

CHAPTER 1

Overview 1-1

Operations Manager Feature Summary 1-2

Requirements 1-4

Main Elements of the User Interface 1-6

Summary Steps: Basic Configuration 1-8

Summary Steps: Advanced Configuration 1-16

Logging In and Managing Passwords 1-18

Logging In 1-18

Default User Accounts and Passwords 1-19

Changing Your Password 1-19

Changing Another User's Password 1-20

Understanding Cisco Video Surveillance Software 1-21

Installing Licenses 1-23

Usage Notes 1-23

License Part Numbers 1-24

Displaying License Information 1-24

Obtaining and Installing Licenses 1-25

Deleting Licenses 1-25

Using Find 1-27

CHAPTER 2

Viewing Video 2-1

Understanding the Video Viewing Options 2-2

Operations Manager Requirements 2-3

Using the *Monitor Video* Page 2-3

Selecting a Multi-Pane "View" 2-4

Controlling Live and Recorded Video 2-7

Overview 2-8

Viewing Live Video 2-9

Viewing Recorded Video 2-12

Creating, Viewing and Managing Video Clips	2-17
Creating a Repeat Segment	2-23
Using Record Now	2-24
Using the Pop-Up Menu	2-25
Understanding Video Pane Border Colors	2-27
Using the Smooth Video Options When Viewing Live Video	2-27
Synchronizing Video Playback in Multiple Panes	2-29
Using Pan, Tilt, and Zoom (PTZ) Controls	2-32
Clip Search (View, Download and Delete MP4 Clips)	2-36
Viewing a Thumbnail Summary of Video Archives	2-39
Using Thumbnail Search	2-41

CHAPTER 3

Configuring Video Viewing Options 3-1

Creating Pre-Defined Views	3-2
Setting the Default View	3-8
Configuring Video Walls	3-10
Enabling Record Now	3-12

CHAPTER 4

Adding Users, User Groups, and Permissions 4-1

Overview	4-1
Understanding Roles, Groups and Users	4-2
Understanding the System-Defined User Roles, Groups and Accounts	4-3
Understanding Permissions	4-4
Example Roles For Different Types of Users	4-7
Defining User Roles	4-8
Adding User Groups	4-10
Adding Users	4-13
Adding Users from an LDAP Server	4-15
LDAP Usage Notes	4-15
Upgrade Requirements	4-15
LDAP Server Settings	4-16
LDAP Search Filter Settings	4-20
LDAP Configuration Examples	4-20
LDAP Configuration Procedure	4-23

CHAPTER 5

Creating the Location Hierarchy 5-1

Overview	5-2
Summary Steps	5-2

Understanding <i>Permission-Based</i> and <i>Partition-Based</i> Resources	5-3
Simple Deployments (User Access to All Devices and Resources)	5-4
<i>Permission-Based</i> Resources: Limiting User Access to Devices	5-4
Examples: Locations in Simple vs. Large Deployments	5-7
Understanding a Camera's Installed Location Vs. the Pointed Location	5-9
Creating and Editing the Location Hierarchy	5-10
Impact of Device Location Changes on Alerts	5-11
Deleting a Location	5-11

CHAPTER 6
Configuring Servers 6-1

Requirements	6-2
Summary Steps to Add or Revise a Server	6-3
Server Settings	6-4
General Information Settings	6-4
Medianet	6-4
Services	6-5
Access Information Settings	6-5
Hardware Information Settings	6-6
Network Information	6-7
NTP Information	6-8
Adding or Editing Servers	6-10
Overview	6-10
Pre-Provisioning Servers	6-11
Prerequisites	6-11
Adding or Editing a Single Server	6-11
Importing or Updating Servers Using a CSV File	6-13
Deleting a Server	6-18
Bulk Actions: Revising Multiple Servers	6-19
Viewing Server Status	6-22
Resetting the Server Device State	6-23
Repairing the Configuration or Restarting the Server	6-23
Operations Manager Advanced Settings	6-24
SMTP Management Settings	6-24

CHAPTER 7
Configuring Media Server Services 7-1

Overview	7-2
Requirements	7-2

Summary Steps to Add, Activate, and Configure a Media Server 7-3

Media Server Settings 7-4

Accessing the Media Server **Advanced** Settings 7-4

High Availability Options 7-5

Partition Settings 7-5

Storage Management Settings 7-6

Media Server Properties 7-6

Viewing Media Server Status 7-8

CHAPTER 8

Adding and Managing Cameras 8-1

Overview 8-3

Understanding Network and Analog Cameras 8-3

Requirements 8-3

Summary Steps 8-4

Viewing Cameras 8-5

Viewing a List of Supported Cameras 8-7

Manually Adding Cameras 8-8

Overview 8-9

Manually Adding a Single Camera 8-12

Importing or Updating Cameras or Encoders Using a CSV File 8-17

Discovering Cameras on the Network 8-22

Understanding Discovery and Auto-Configuration 8-22

Understanding Camera Conflicts 8-24

Enabling the Auto Configuration Defaults for a Camera Model 8-25

Discovering Non-Medianet Cameras on the Network 8-28

Cameras Pending Approval List 8-30

Discovering Medianet-Enabled Cameras 8-32

Adding Cameras from an Existing Media Server 8-38

Adding Cameras From a 6.x or 7.x Media Server 8-38

Adding Unknown Cameras During a Media Server Synchronization 8-39

Blacklisting Cameras 8-40

Blacklisting a Camera 8-40

Viewing Cameras in the Blacklist 8-41

Removing a Camera From the Blacklist 8-41

Editing the Camera Settings 8-42

Accessing the Camera Settings 8-42

General Settings 8-45

Streaming, Recording and Event Settings 8-49

Using Custom Video Quality Settings 8-55

Image Settings	8-57
Configuring the High Availability Options for a Camera or Template	8-58
Deleting Cameras	8-59
Changing the Camera or Encoder Access Settings (Address and Credentials)	8-61
Viewing Camera and Encoder Status	8-63
Configuring Camera PTZ Controls, Presets, and Tours	8-65
PTZ Requirements	8-66
PTZ Camera Configuration Summary	8-67
Defining the User Group PTZ Priority	8-69
Using Camera PTZ Controls	8-70
Configuring PTZ Presets	8-71
Configuring PTZ Tours	8-73
PTZ Advanced Settings	8-76
Configuring Motion Detection	8-77
Motion Detection Overview	8-78
Motion Detection Settings	8-79
Configuring Motion Detection	8-80
Enabling Motion Detection on All Existing Cameras (Bulk Actions)	8-82
Replacing a Camera	8-83
Bulk Actions: Revising Multiple Cameras	8-85

CHAPTER 9
Defining Schedules 9-1

CHAPTER 10
Adding and Editing Camera Templates 10-1

Overview	10-2
Creating or Modifying a Template	10-3
Creating a Custom Template for a Single Camera	10-5
Configuring Video Recording	10-7
Configuring Continuous, Scheduled, and Motion Recordings	10-7
Using <i>Advanced Events</i> to Trigger Actions	10-11
Configuration Overview	10-12
Configuration Summary	10-12
Trigger and Action Descriptions	10-13
Configuring Soft Triggers	10-15
Configuring Multicast Video Streaming	10-18

CHAPTER 11
Adding Encoders and Analog Cameras 11-1

Overview	11-2
----------	------

Pre-Provisioning Encoders and Analog Cameras	11-3
Requirements	11-4
Adding External Encoders and Analog Cameras	11-5
Bulk Actions: Revising Multiple Encoders	11-11
Using “Split Model” Multi-Port Multi-IP Encoders	11-13

CHAPTER 12

High Availability 12-1

Overview	12-2
Requirements	12-2
Summary Steps	12-3
Understanding Redundant, Failover, and Long Term Storage Servers	12-4
Understanding Failover	12-7
Define the Media Server HA Role and Associated Servers	12-9
Configuring the Camera Template HA Options	12-12
Configuring the <i>Redundant</i> and <i>Failover</i> Options	12-12
Archiving Recordings to a Long Term Storage Server	12-16
Defining the <i>Recording Options</i>	12-20
Viewing the Server HA Status	12-22

CHAPTER 13

Monitoring System and Device Health 13-1

Understanding Events and Alerts	13-2
Overview	13-2
Event Types	13-4
Triggering Actions Based on Alerts and Events	13-4
Monitoring Device Health Using the Operations Manager	13-5
Health Dashboard: Viewing Device Health Summaries	13-6
Device Status: Identifying Issues for a Specific Device	13-8
Understanding the Overall Status	13-8
Understanding Device Status	13-10
Viewing Device Error Details	13-13
Health Notifications	13-14
Reports	13-16
Create a Report	13-16
Delete a Report	13-16
Synchronizing Device Configurations	13-17
Overview	13-17
Viewing Device Synchronization Errors	13-19
Understanding Device Configuration Mismatch Caused by Media Server Issues	13-20

	Repairing a Mismatched Configuration	13-21
	Manually Triggering a Media Server Synchronization	13-22
	Device Data That Is Synchronized	13-22
	Synchronization During a Media Server Migration	13-23
	Viewing the Server Management Console Status and Logs	13-24
	Understanding Jobs and Job Status	13-25
	Viewing Job Status and Details	13-25
	Understanding Job Status	13-27
	Viewing All Jobs in the System	13-28
	Viewing Audit Logs	13-31
CHAPTER 14	Revising the System Settings	14-1
	General System Settings	14-1
	Password Settings	14-2
CHAPTER 15	Software Downloads and Updates	15-1
	Downloading Cisco SASD and the Cisco Review Player	15-1
	Downloading the Workstation Profiler Tool	15-2
	Downloading Software, Firmware and Driver Packs from cisco.com	15-2
	Accessing the Management Console	15-2
	Downloading Documentation	15-2
	Upgrading Cisco Camera and Encoder Firmware	15-3
	Installing and Upgrading Driver Packs	15-8
CHAPTER 16	Backup and Restore	16-1
	Backing Up and Restoring the Operations Manager Configuration	16-2
	Performing Backups	16-3
	Backup Settings	16-3
	Backup File Format	16-4
	Disk Usage for Backups	16-5
	Restoring an Operations Manager Backup	16-5
	Deleting a Backup File	16-6
	Backing Up the Media Server Configuration	16-6
	Backing Up Recordings	16-7
APPENDIX A	Related Documentation	A-1
APPENDIX B	Revision History	B-1



CHAPTER 1

Overview

The Cisco VSM Operations Manager is a browser-based configuration and administration tool used to manage the devices, video streams, archives, and policies in a Cisco Video Surveillance deployment.

The Operations Manager interface is enabled when the Operations Manager service is enabled on a Cisco Video Surveillance server (see the [Cisco Video Surveillance Management Console Administration Guide](#) for more information).

Refer to the following topics for a summary of the main Operations Manager capabilities, configuration features, and other information.

Contents

- [Operations Manager Feature Summary, page 1-2](#)
- [Requirements, page 1-4](#)
- [Main Elements of the User Interface, page 1-6](#)
- [Summary Steps: Basic Configuration, page 1-8](#)
- [Summary Steps: Advanced Configuration, page 1-16](#)
- [Logging In and Managing Passwords, page 1-18](#)
- [Understanding Cisco Video Surveillance Software, page 1-21](#)
- [Installing Licenses, page 1-23](#)
- [Using Find, page 1-27](#)

Operations Manager Feature Summary

The following table summarizes the main Operations Manager features.

Table 1-1 **Feature Summary**

Feature	Description	More information
Manage physical devices	Add, configure and monitor the cameras, servers, s, and encoders that provide live and recorded video.	<ul style="list-style-type: none"> • Configuring Servers, page 6-1 • Adding and Managing Cameras, page 8-1 • Adding and Managing Cameras, page 8-1
Manage server services	Configure, enable or disable server services, such as the Media Servers that manage video playback and recording.	<ul style="list-style-type: none"> • Configuring Media Server Services, page 7-1 • Operations Manager Advanced Settings, page 6-24
Monitor video	View live and recorded video, save video clips, search thumbnail summaries of recorded video, use the camera, Pan, Tilt and Zoom (PTZ) controls, or configure pre-defined video Views and Video Walls.	<ul style="list-style-type: none"> • Viewing Video, page 2-1 • Configuring Video Viewing Options, page 3-1
Define recording and event policies	Create recording schedules, define event-triggered actions, configure motion detection, and other features.	<ul style="list-style-type: none"> • Configuring Continuous, Scheduled, and Motion Recordings, page 10-7 • Configuring Camera PTZ Controls, Presets, and Tours, page 8-65 • Configuring Motion Detection, page 8-77 • Using Advanced Events to Trigger Actions, page 10-11

Table 1-1 **Feature Summary (continued)**

Feature	Description	More information
Monitor system and device health	View a summary of system health for all devices, or device status, alerts and events.	Monitoring System and Device Health, page 13-1
Backup and restore	Backup the system configuration, and optionally include historical data (such as alerts). You can also backup recorded video to a separate server.	<ul style="list-style-type: none">• Backup and Restore, page 16-1• Archiving Recordings to a Long Term Storage Server, page 12-16




Requirements

Cisco VSM Operations Manager requires the following.

Table 1-2 **Requirements**

Requirements	Requirement Complete? (✓)
<p>At least one Cisco Video Surveillance server must be installed on the network.</p> <ul style="list-style-type: none"> At least one Media Server and Operations Manager must be enabled. The Media Server and Operations Manager services can be enabled on a single physical server (co-located) or on separate servers. Multiple Media Servers can be hosted by a co-located Operations Manager, or a stand-alone Operations Manager. See the Cisco Physical Security UCS Platform Series User Guide for instructions to install a physical server. See the Cisco Video Surveillance Virtual Machine Deployment and Recovery Guide for UCS Platforms for instructions to install a virtual machine. See the Cisco Video Surveillance Management Console Administration Guide for instructions to enable the Media Server and Operations Manager applications. 	<input type="checkbox"/>
The IP address or hostname of the Operations Manager.	<input type="checkbox"/>
A valid Cisco VSM Operations Manager username and password.	<input type="checkbox"/>
The server IP address and password if stand-alone Cisco Media Servers are deployed.	<input type="checkbox"/>
<p>At least one camera physically installed and connected to the network.</p> <ul style="list-style-type: none"> See the camera documentation for instructions to install the camera. You can also install network or analog cameras. Analog cameras require a video encoder to enable network connectivity. <p>Tip You can pre-provision cameras by adding them to the Operations Manager before they are available on the network. See the “Pre-Provisioning Cameras” section on page 8-10.</p>	<input type="checkbox"/>
<p>All the server hostnames 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).</p> <p>All edge devices (such as cameras and encoders) must be added to a server using a local (non-NAT) addresses.</p>	<input type="checkbox"/>

Table 1-2 Requirements (continued)

Requirements	Requirement Complete? (✓)
<p>A PC or laptop with the following:</p> <ul style="list-style-type: none"> • Windows 7 (32-bit or 64-bit) or Windows 8 (64-bit) • Minimum resolution of 1280x1024 • You must log in with a standard Windows user account. Logging in with a Guest account can prevent video streaming and result in an error to be displayed in the video pane: “Cannot create RTSP connection to server. Check network connection and server health status.” <p>See the Cisco Video Surveillance Monitoring Workstation Performance Baseline Specification for the complete baseline performance specifications for a video surveillance monitoring workstation.</p>	
<p>The Internet Explorer (IE) web browser.</p> <p>Windows</p> <ul style="list-style-type: none"> • Windows 7 supports IE 9 or 10. • Windows 8 supports IE 10, desktop version (the Metro version of IE 10 is not supported). <p>32-bit or 64-bit</p> <ul style="list-style-type: none"> • The IE 32-bit version can display a maximum of 4 video panes (for example, in a 2x2 layout). • The IE 64-bit version can display a maximum of 16 video panes (for example, in a 4x4 layout). <p>See the Cisco Video Surveillance Monitoring Workstation Performance Baseline Specification for the complete baseline performance specifications for a video surveillance monitoring workstation.</p>	
<p>The Cisco Multi-Pane client software installed on the PC.</p> <ul style="list-style-type: none"> • The Multi-Pane client is an Active X client that enables video playback and other features. • You will be prompted to install Multi-Pane client the first time you log in to the Operations Manager, or if you are using a the 64-bit Internet Explorer (IE) web browser for the first time. Follow the on-screen instructions if prompted. • You will also be prompted to install the required Microsoft .Net 4.0 component, if necessary. If your workstation does not have Internet access, the .Net 4.0 installer can be downloaded from http://www.microsoft.com/en-us/download/details.aspx?id=17718. • You must have administrative privileges on the PC workstation to install the software. <p>Note By default, all video monitoring using Internet Explorer 10 is performed using the 32-bit Cisco Multi-Pane client software. To enable 64-bit browser monitoring in Windows 7 or 8 using IE 10, see the Cisco Video Surveillance Monitoring Workstation Performance Baseline Specification.</p>	

Main Elements of the User Interface

All windows include a basic set of links and features, as described in [Figure 1-1](#).



Tip

See the [“Summary Steps: Basic Configuration”](#) section on page 1-8 for instructions to add and configure a basic set of devices.

Figure 1-1 Main User Interface Elements



- | | |
|----------|---|
| 1 | <p>Feature tabs:</p> <ul style="list-style-type: none"> • Monitor Video—View live and recorded video from up to four panes. See the “Viewing Video” section on page 2-1. • Cameras—Add, configure and modify video surveillance cameras, templates and encoders. See the “Adding and Managing Cameras” section on page 8-1. • Users—Manage user accounts and access permissions, including access for LDAP users. See the “Adding Users, User Groups, and Permissions” section on page 4-1. • System Settings—Configure system attributes, including system settings, Media Servers, locations, schedules, software licenses, Video Walls, and other attributes. • Operations—Links to documentation, desktop monitoring software, logs, Reporting and Health features, and the Cisco VSM Management Console. |
| 2 | <p>Find—Search for devices and attributes (see the “Using Find” section on page 1-27).</p> |
| 3 | <p>Location Hierarchy—Allows you to organize devices, resources, and access permissions according to the locations in your deployment. See the “Creating the Location Hierarchy” section on page 5-1.</p> |

4	Devices, users, or other attributes available for the selected location.
5	Action buttons. For example, Thumbnail Search , Clip Search or Add Cameras . The buttons vary depending on the screen.
6	Video Monitoring panes or configuration window. The fields and contents of the main window vary depending on the feature you are accessing.
7	Views—(Monitor Video window) Select a blank layout or pre-defined <i>View</i> (set of video panes). See the “Selecting a Multi-Pane “View”” section on page 2-4 .
8	Connection—Defines if the Operations Manager is receiving real time status updates (from the ActiveMQ service).
9	Help —Opens the online help system that contains this document. For more information and additional documentation, refer to the Help links in the Operations tab.
10	Logout—Click to log out of the Cisco VSM Operations Manager.
11	Username—Displays the username for the currently logged in user. Tip Click the username to change your password. See the “Changing Your Password” section on page 1-19 .

Summary Steps: Basic Configuration

Complete the following steps to create a basic configuration. A basic configuration allows you to verify that basic system components and devices are online, configured, and working properly.

Table 1-3 **Summary Steps: Basic Configuration**


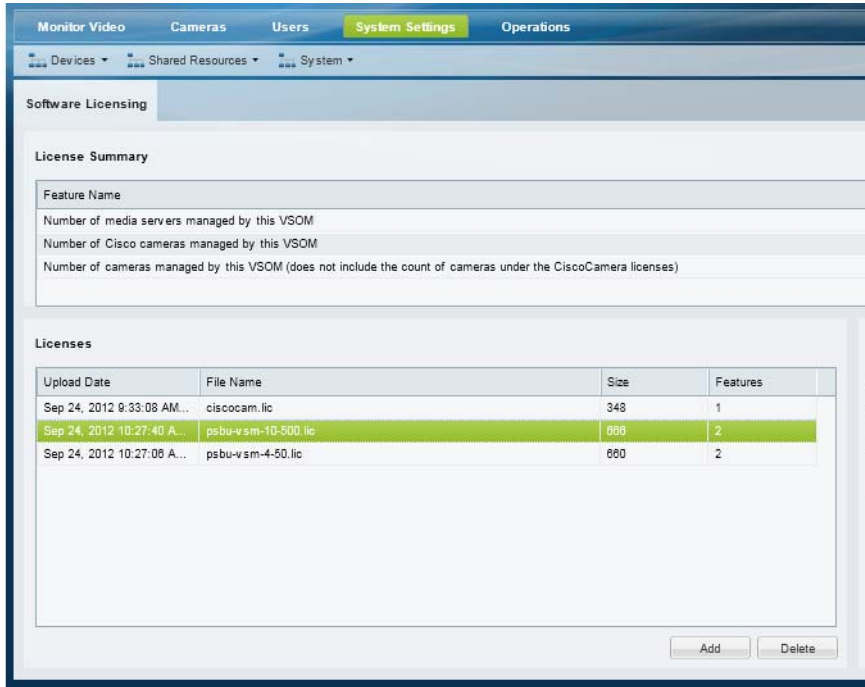
	Task	Description
Step 1	Log on to the Cisco VSM Operations Manager.	<p>See the “Logging In and Managing Passwords” section on page 1-18.</p> 
Step 2	Install the system licenses.	<p>Purchase and install a license for each Media Server and non-Cisco camera added to your deployment. See the “Installing Licenses” section on page 1-23.</p> 

Table 1-3 Summary Steps: Basic Configuration (continued)


Task	Description
Step 3 Revise the system settings.	<p>Revise the default user password properties, record storage rules, backup file rules, and other settings.</p> <p>Tip The default settings are sufficient for a basic setup, but you should review and revise the settings to meet the needs of your deployment.</p>  <p>For example:</p> <ol style="list-style-type: none"> Choose Settings > System Settings. Revise the following properties, as necessary: <ul style="list-style-type: none"> General System Settings, page 14-1 Password Settings, page 14-2 <p>See the “Revising the System Settings” section on page 14-1 for more information.</p>

Table 1-3 Summary Steps: Basic Configuration (continued)

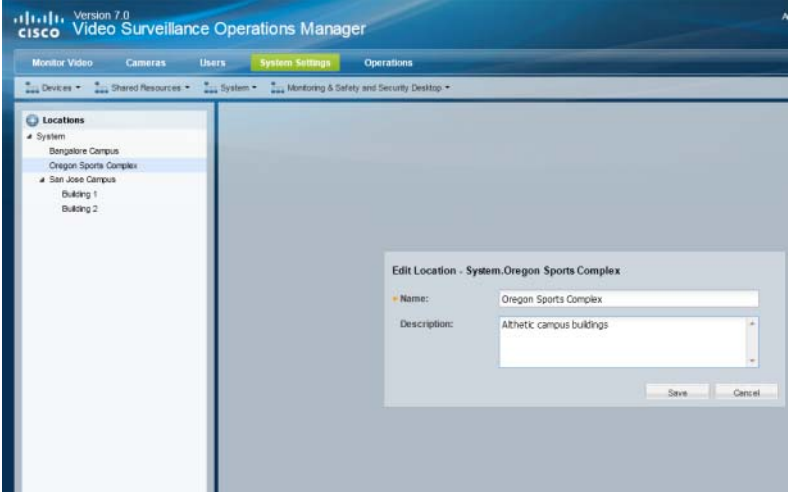
	Task	Description
Step 4	Create at least one location.	<p>Define the locations that are assigned to devices (such as cameras) user groups, and policies. Locations allow administrators to restrict user access to the cameras, policies, and data (such as alerts) required by the user's role. For example, a security guard can have access to view video at a specific location, but not to configure the camera properties.</p>  <ol style="list-style-type: none"> Select Locations from the System Settings menu. Click Add. Enter the location name and press <i>Enter</i>. <p>See the “Creating the Location Hierarchy” section on page 5-1 for more information.</p>

Table 1-3 Summary Steps: Basic Configuration (continued)




Task	Description
Step 5 Create at least one user account.	<p>Create the user accounts and access permissions that restrict the locations and tasks available to a user. For example:</p> <p>Create a User Role</p> <p>The Role defines the access permissions for different types of users. Roles are assigned to User Groups.</p> <ol style="list-style-type: none"> Select Users. Select the Roles tab . Click Add. Enter the basic settings (see Table 4-5). Select the Role permissions (see Table 4-2 and Table 4-3). Click Create. <p>See the “Defining User Roles” section on page 4-8.</p> <p>Create a User Group</p> <p>User Groups allow you to create groups of users. The access Role for the User Group grants those access permissions to all users in the group.</p> <ol style="list-style-type: none"> Select the User Groups tab . Click Add. Enter the group settings, including the Role that defines the access permissions for the group (see Table 4-6). Click Create. <p>See the “Adding User Groups” section on page 4-10.</p> <p>Create a User Account</p> <p>The User account defines the username and password. Users gain access permissions through the User Group assignments. A user can be assigned to multiple groups, and gains the combined access permissions of all groups.</p> <ol style="list-style-type: none"> Select the User tab . Click Add. Enter the basic user settings (see Table 4-7). Add the user to one or more user groups. <ul style="list-style-type: none"> Click Add under the User Groups box. Select one or more user groups from the pop-up window. Select OK. Click Create. <p>See the “Adding Users” section on page 4-13.</p> <p>See also the “Adding Users, User Groups, and Permissions” section on page 4-1 for more information.</p>

Table 1-3 Summary Steps: Basic Configuration (continued)

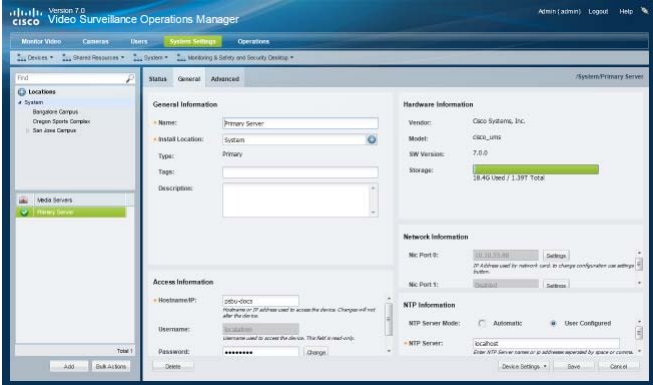
	Task	Description
Step 6	Add at least one Media Server.	<p>Add a Media Server and camera.</p> <p>A Media Server is an application that runs on physical Cisco Video Surveillance server, and provides video streaming, recording and storage for the cameras associated with that server. You must add the Media Server to the Operations Manager configuration to communication between the applications.</p>  <ol style="list-style-type: none"> Click System Settings. Click Media Servers. Click Add. Enter the basic server settings and click Add. Click Save. <p>See the “Viewing Media Server Status” section on page 7-8 for more information.</p>

Table 1-3 Summary Steps: Basic Configuration (continued)

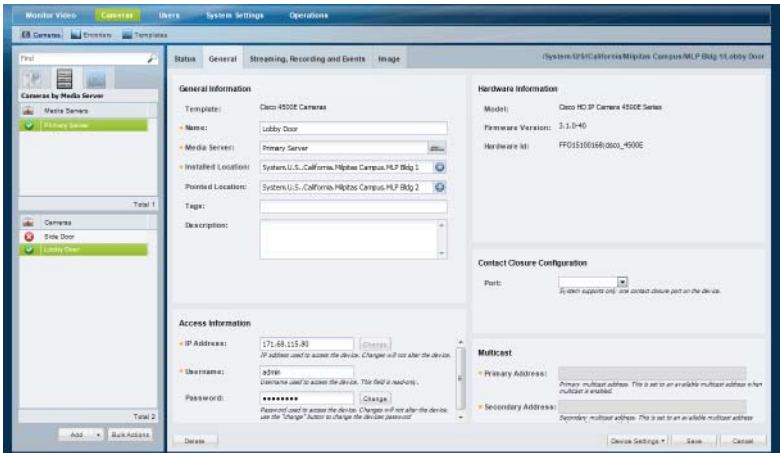
Step 7	Task	Description
	Add at least one camera.	<p>The surveillance video camera must be installed on the network.</p> <p>Note Although cameras can be pre-provisioned (added before they are installed on the network), you should add at least one installed camera to the basic configuration to verify network connectivity, video monitoring, and other features.</p>  <ol style="list-style-type: none"> Click Cameras. Click Add. Select the camera type: <ul style="list-style-type: none"> IP Camera—networked IP camera Analog Camera—analog camera are attached to an encoder to provide network connectivity and digitize the analog video. See the Adding Encoders and Analog Cameras, page 11-1 for more information. Enter the basic camera settings and click Add. <p>See the “Manually Adding a Single Camera” section on page 8-12 for more information.</p>

Table 1-3 Summary Steps: Basic Configuration (continued)

	Task	Description
Step 8	View video from the camera to verify that the system is working properly.	<p>View the live or recorded video from the camera to verify that the settings are correct and that the devices are available on the network.</p> <p>See the “Controlling Live and Recorded Video” section on page 2-7 for more information.</p>

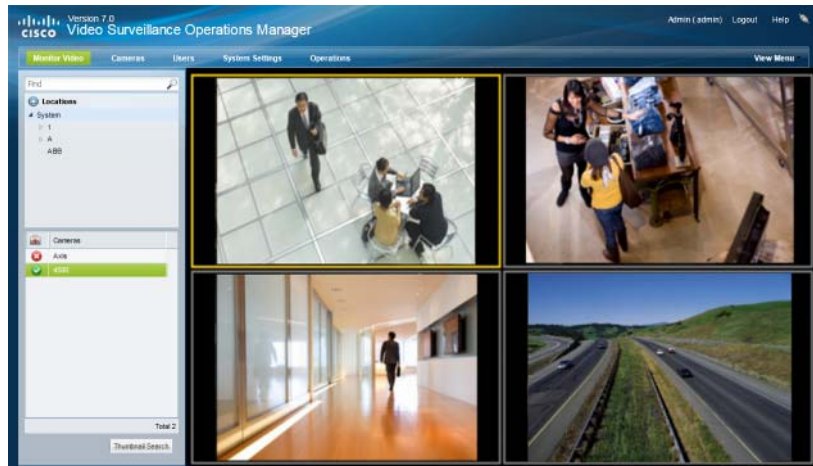
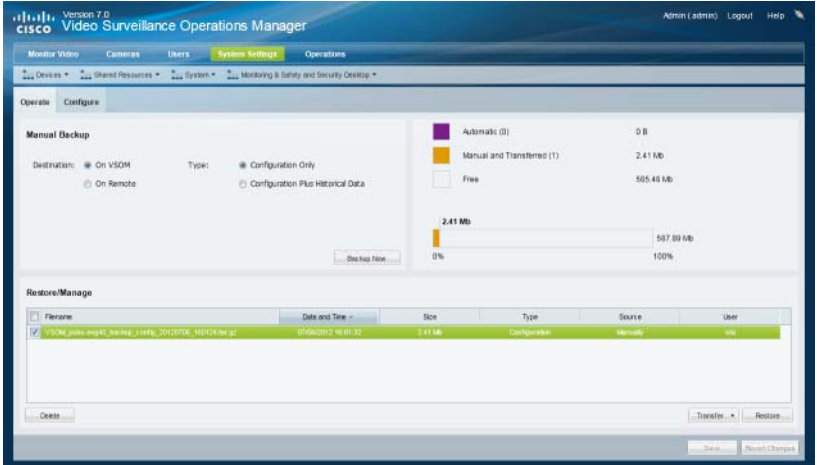



Table 1-3 Summary Steps: Basic Configuration (continued)

Task	Description
Step 9 Backup the Operations Manager configuration and other data, or create an automatic backup schedule.	<p>See the “Backup and Restore” section on page 16-1 for more information.</p>  <p>Tip We highly recommend that you also back up the Media Server application data using the Cisco Video Surveillance Management Console interface. The Media Server application backup is separate from the Operations Manager backup and includes critical server settings and data necessary to restore the system in the event of a hardware failure. See the “Backing Up the Media Server Configuration” section on page 16-6 for more information.</p>
Step 10 Troubleshoot problems or verify the system and device status.	<p>See the “Monitoring System and Device Health” section on page 13-1 for more information.</p> 

Summary Steps: Advanced Configuration

After completing the basic configuration, you can utilize advanced features, as summarized in [Table 1-4](#).



Note

[Table 1-4](#) describes a sub-set of options available in the Cisco Video Surveillance deployment. Review the other topics in this guide for additional features and configuration instructions.

Table 1-4 *Summary Steps: Advanced Configuration*

	Task	Description
Step 1	Create a more sophisticated location hierarchy to reflect the needs of your deployment.	See the “Understanding Permission-Based and Partition-Based Resources” section on page 5-3 .
Step 2	Add additional users (or add LDAP servers to authenticate users from other systems).	<ul style="list-style-type: none"> • Adding Users, User Groups, and Permissions, page 4-1 • Adding Users from an LDAP Server, page 4-15
Step 3	Add additional Media Servers and configure the high availability options.	<p>High availability servers provide redundant or failover support for the Primary Media Server.</p> <p>Long Term Storage servers can back up recordings and remove them from the Primary Media Server.</p> <ul style="list-style-type: none"> • Configuring Media Server Services, page 7-1 • High Availability, page 12-1
Step 4	Create camera templates.	<p>Templates define configurations that can be applied to multiple cameras.</p> <p>See the Adding and Editing Camera Templates, page 10-1.</p>
Step 5	Add additional cameras.	<p>You can import cameras from a file or discover them on the network.</p> <ul style="list-style-type: none"> • Importing or Updating Cameras or Encoders Using a CSV File, page 8-17 • Discovering Cameras on the Network, page 8-22 • Adding Cameras from an Existing Media Server, page 8-38
Step 6	Configure camera recordings.	<p>Configure cameras to record in a continuous loop, on a recurring schedule, or both.</p> <p>See the “Configuring Continuous, Scheduled, and Motion Recordings” section on page 10-7</p>

Table 1-4 **Summary Steps: Advanced Configuration (continued)**

Step 7	Configure additional camera and monitoring features.	<ul style="list-style-type: none">• Configuring Camera PTZ Controls, Presets, and Tours, page 8-65• Configuring Motion Detection, page 8-77• Creating Pre-Defined Views, page 3-2• Configuring Video Walls, page 3-10• Enabling Record Now, page 3-12
Step 8	Define the system events that trigger actions.	<p>Use <i>Advanced Events</i> to trigger an immediate one-time action when a specified event occurs. For example, when motion starts or a contact is closed, the system can trigger an alert, aim the camera to a PTZ preset position, or trigger an action on an external system.</p> <p>See the “Using Advanced Events to Trigger Actions” section on page 10-11 for more information.</p>

Logging In and Managing Passwords

- [Logging In, page 1-18](#)
- [Default User Accounts and Passwords, page 1-19](#)
- [Changing Your Password, page 1-19](#)
- [Changing Another User's Password, page 1-20](#)

Logging In

To log in to the Cisco Video Surveillance Operations Manager:

-
- Step 1** Launch the 32-bit or 64-bit version of Internet Explorer on your Windows computer.
See the [“Requirements” section on page 1-4](#) for more information.
- Step 2** Enter the Operations Manager URL or IP address.
- Step 3** Enter your username and password.
- Step 4** Select a Domain:
- Choose the default “localhost” if your account was created using the Operations Manager.
 - Select an alternative domain if instructed by your system administrator.
- Step 5** Enter a new password, if prompted.
You must enter a new password the first time you log in, or when your password periodically expires.
- Step 6** If prompted, complete the on-screen instructions to install or upgrade the Cisco Multi-Pane client software on your computer.
- This application is an Active X client that enables video playback and other features.
 - Video will not play unless the Cisco Multi-Pane client software is correctly installed.
 - If using the 64-bit version of Internet Explorer, you will be prompted to install the 64-bit version of the Cisco Multi-Pane client, if necessary.
 - You must have administrative privileges on the PC workstation to install the software.
 - You will also be prompted to install the required Microsoft .Net 4.0 component, if necessary. If your workstation does not have Internet access, the .Net 4.0 installer can be downloaded from <http://www.microsoft.com/en-us/download/details.aspx?id=17718>.

**Note**

You must log in with a standard Windows 7 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.”

Default User Accounts and Passwords

The Operations Manager includes two default users: the super-admin account and an operator account.

Table 1-5 *Default User Accounts*

Default Account	Default Username and Password	Access Privileges
admin	username: admin password: admin	<i>Super-admin</i> privileges with full rights to configure, view and manage all system settings and features.
operator	username: operator password: operator	Ability to view live and recorded video, control PTZ movements, push views to a Video Wall, and export recordings.

You are prompted to change the default passwords the first time you log in.

Changing Your Password

To change your password, click your username in the top right corner of the browser ([Figure 1-2](#)).



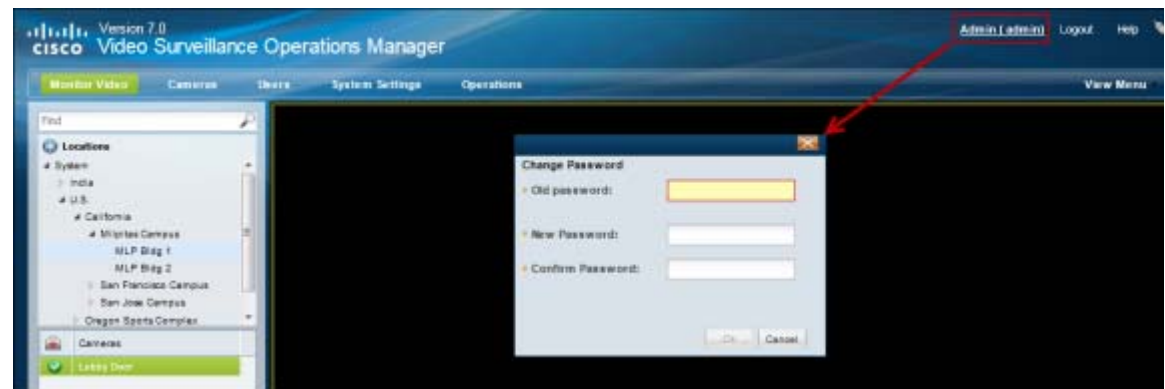
Note

Users from external systems (LDAP servers) cannot change their password using the Cisco VSM Operations Manager.

If you forgot your password, contact your system administrator and ask them to create a new password (you will be prompted to change it when you log in).

- Step 1** Log in to the Operations Manager (see [Logging In](#) [Figure 1-1](#)).
- Step 2** Click your username in the top right ([Figure 1-2](#)).
- Step 3** Enter your current password.
- Step 4** Enter and re-enter a new password.


Figure 1-2 *Changing Your Password*



Changing Another User's Password

To change another user's password, you must belong to a User Group with permissions to manage *Users & Roles*.

Procedure

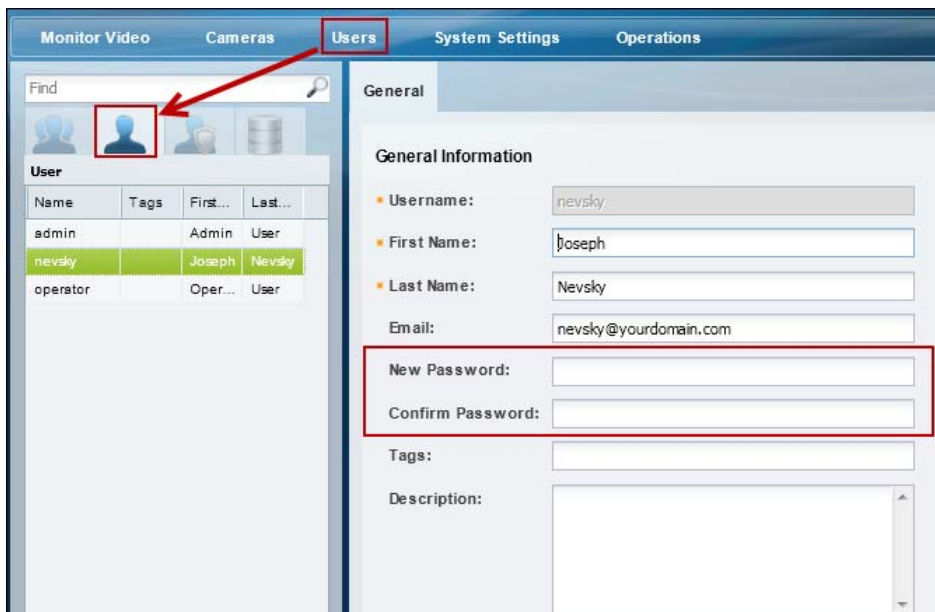
- Step 1** Select **Users**, and then select the **User** tab  (Figure 1-3).
- Step 2** Highlight a username.
- Step 3** Enter and re-enter a new password in the password fields.

**Note**

The user is required to change the password the first time they log in.

See the [“Adding Users, User Groups, and Permissions”](#) section on page 4-1 for more information

Figure 1-3 Changing a User Password



Name	Tags	First...	Last...
admin		Admin	User
nevsky		Joseph	Nevsky
operator		Oper...	User

General

General Information

Username: nevsky

First Name: Joseph

Last Name: Nevsky

Email: nevsky@yourdomain.com

New Password:

Confirm Password:

Tags:

Description:

Understanding Cisco Video Surveillance Software

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

Table 1-6 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. The Operations Manager and all associated Media Servers must run the same software version.</p> <ul style="list-style-type: none"> Use the Management Console to update <i>System Software</i>, as described in the Server Upgrade section of the Cisco Video Surveillance Management Console Administration Guide (go to Operations > Management Console to launch the browser-based interface or see your system administrator for login information). To repair or restore the Cisco VSM system software, see the Cisco Video Surveillance Manager 7.0 Recovery Flash Drive guide.
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"> OVA template files are downloaded from the Cisco website. The file format is .ova. For example: <code>Cisco_VSM-7.2.0-331d_ucs-bc.ova</code> See the Cisco Video Surveillance Virtual Machine Deployment and Recovery Guide for UCS Platforms for instructions to install the .ova image and perform the initial VM setup.
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"> Repair: reinstalls the Operating System files and partitions without erasing video files stored on the server. You must backup the Cisco VSM database before using the recovery image, and then restore the database after the recovery process is complete. This action also preserves the RAID configuration. Factory Restore: Restores the server to its factory default settings, reinstalls the operating system, and clears and reconfigures the RAID. This action deletes all data, configurations, software and video files from the appliance, and then reinstalls the operating system and Cisco VSM software. Perform this procedure only if necessary. <p>See the Cisco Video Surveillance Manager Flash Drive Recovery Guide for more information.</p>

Table 1-6 Cisco Video Surveillance Software Types (continued)

Software Type	Description
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 (as described in the “Upgrading Cisco Camera and Encoder Firmware” section on page 15-3).</p> <p>Firmware for other manufacturers is upgraded using a direct connection (refer to the device documentation).</p>
Device <i>driver packs</i>	<p>Device <i>driver packs</i> are the software packages used by Media Server and 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"> • Install new driver packs to add support for additional devices. • Upgrade existing driver packs to enable support for new features (System Settings > Driver Pack Management). See the “Installing and Upgrading Driver Packs” section on page 15-8 for instructions. <p>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 can also be used to upgrade the driver packs for a single server at a time.</p> <ul style="list-style-type: none"> • <i>Driver pack</i> versions must be the same on the servers that host the Media Server and Operations Manager or a <i>driver pack mismatch</i> error. Templates cannot be revised when a <i>driver pack mismatch</i> error is present.

**Tip**

For information about supported software releases, and how to locate device or system software, see the [Release Notes for Cisco Video Surveillance Manager, Release 7.2](#).

Installing Licenses

A license must be purchased and installed for each Media Server and non-Cisco camera added to your deployment.

Review the following topics for more information.

- [Usage Notes, page 1-23](#)
- [License Part Numbers, page 1-24](#)
- [Displaying License Information, page 1-24](#)
- [Obtaining and Installing Licenses, page 1-25](#)

Usage Notes

- Licenses are installed in the Operations Manager only (not on the individual Media Servers).
 - Licenses can only be installed on a single instance of Operations Manager.
 - The same license file cannot be installed more than once on the same Operations Manager.
 - Do not rename the license file before installing it on the Operations Manager. Use the original file name only.
- You must purchase and install a license for each Media Server and non-Cisco camera added to your deployment.
- A license for 10,000 Cisco cameras is included by default (you do not need to purchase and install an additional license for Cisco cameras).
- Licenses are cumulative: each additional license is added to the capacity of existing licenses. For example, if you initially installed a license for 100 non-Cisco cameras, you can purchase an additional license for 200 cameras to support a total of 300 non-Cisco cameras.
- The maximum number of devices in a system is 200 Media Servers and 10,000 cameras. This including Cisco and non-Cisco devices.
- Soft deleted cameras are included in the camera license count. See the [“Device Status: Identifying Issues for a Specific Device” section on page 13-8](#) for more information.
- Installed licenses are included in the Operations Manager backup and restore archives. We recommend backing up Operations Manager data after installing new licenses (or anytime major changes are performed). If the license file is installed after the backup is performed, the license file is not backed up and not available to be restored. You must re-install the missing license file. See the [“Backup and Restore” section on page 16-1](#) for more information, including how to configure scheduled backups.

License Part Numbers

For a summary of the Cisco VSM licenses, see the [Release Notes for Cisco Video Surveillance Manager](#). Multiple camera and Media Server licenses can be included in a single license file. For example, a single license file might include support for 25 additional cameras and two additional Media Servers. See the “[Displaying License Information](#)” section on page 1-24.

Displaying License Information

Select **System Settings > Software Licensing** to view information about each installed license, and a summary of all installed licenses (Figure 1-4).

Figure 1-4 **Software Licensing**

License Summary

Feature Name	Devices	Used	Available
Number of media servers managed by this VSOM	14	1	13
Number of Cisco cameras managed by this VSOM	10000	1	9999
Number of cameras managed by this VSOM (does not include the count of cameras under the CiscoCamera licenses)	550	0	550

Licenses

Upload Date	File Name	Size	Features
Sep 24, 2012 9:33:08 AM	ciscocam.lic	348	1
Sep 24, 2012 10:27:40 AM	psbu-vsm-10-500.lic	666	2
Sep 24, 2012 10:27:08 AM	psbu-vsm-4-50.lic	660	2

License Details

File Name: psbu-vsm-10-500.lic
 Upload Date: Sep 24, 2012 10:27:40 AM -0700
 Size: 666

Feature Name: Number of media servers managed by this VSOM
 Devices: 10

Feature Name: Number of cameras managed by this VSOM (does not include the count of cameras under the CiscoCamera licenses)
 Devices: 500

1	The <i>License Summary</i> displays the total number of Cisco cameras, non-Cisco cameras and Media Servers that can be managed by the current Operations Manager. The total number of device licenses used and available is also shown. Note Up to 200 Media Servers and 10,000 cameras can be managed by the system, although you can install more than that number of licenses.	3	Licenses for additional Media Servers and non-Cisco cameras.
2	The license for Cisco cameras (included).	4	Highlight a license name to display information about the license file, such as the upload date and the number of devices enabled by the license.

Obtaining and Installing Licenses

To install a license, purchase the license and obtain the license file, then upload the file to Operations Manager.

Procedure

-
- Step 1** Purchase additional licenses:
- Determine the part number for the license you want to purchase. See the “[License Part Numbers](#)” section on page 1-24.
 - Purchase the licence by contacting your Cisco sales representative or any Cisco reseller. For more information, visit <http://www.cisco.com/en/US/ordering/index.shtml>.
 - When the purchase is complete, you are issued a Product Authorization Key (PAK) in paper form, or in an email message.
- Step 2** Obtain the license file:
- Locate the Product Authorization Key (PAK) created with the purchase.
 - In a Web browser, open the Cisco Product License Registration Web page.
<http://www.cisco.com/go/license/>
 - Follow the onscreen instructions to complete the form and enter the Product Authorization Key (PAK). When you are done, a license file with the extension `.lic` is sent to your email address.
 - Transfer the file to the drive of the PC used for the configuration.
- Step 3** Install the license file in Cisco VSM:
- Log in to the Operations Manager.
 - Select **System Settings > Software Licensing** (Figure 1-4).
 - Click **Add** and select the license file located on your local drive.
 - Click **Save** to install the file and activate the additional capacity.



Tip The additional capacity is available immediately. You do not need to restart the server or take additional steps.

Deleting Licenses

Deleting a license will reduce the number of cameras and Media Server supported in your Cisco Video Surveillance deployment.

You cannot delete a license if the number of licenses devices will be less than the number added to the Operations Manager. View the number of licenses *Used* to verify that the license can be removed (see the “[Displaying License Information](#)” section on page 1-24).

Procedure

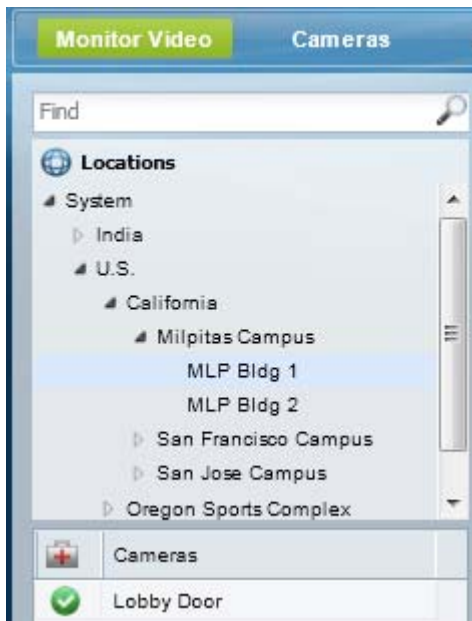
To remove a license:

-
- Step 1** Select **System Settings > Software Licensing**.
- Step 2** Highlight a license entry and click **Delete** ([Figure 1-4](#)).
- Step 3** Click **Yes** to confirm.
-

Using Find

Enter a term or name in the *Find* field to quickly locate cameras, Media Servers, users, or other Cisco VSM attributes. The *Find* field is located at the top of the left column (Figure 1-5) and dynamically locates any item in the open window (not just for the location selected).

Figure 1-5 Find




For example, open **Cameras** and then enter a name of a camera. The results are displayed below the *Find* field, and is dynamically updated to display even partial matches. The example in Figure 1-6 shows the results of a partial search: entering “Lo” returns the camera “Lobby Door”.

Figure 1-6 Find Results



Tip

Click the  icon to clear the *Find* entry and return to normal view. All entries are displayed.



CHAPTER 2

Viewing Video

The following topics describe how to view live and recorded video using a supported Cisco Video Surveillance application, such as the Cisco Video Surveillance Safety and Security Desktop (Cisco SASD) application or the Cisco VSM Operations Manager.

Contents

- [Understanding the Video Viewing Options, page 2-2](#)
- [Operations Manager Requirements, page 2-3](#)
- [Using the Monitor Video Page, page 2-3](#)
- [Selecting a Multi-Pane “View”, page 2-4](#)
- [Controlling Live and Recorded Video, page 2-7](#)
 - [Overview, page 2-8](#)
 - [Viewing Live Video, page 2-9](#)
 - [Viewing Recorded Video, page 2-12](#)
 - [Creating, Viewing and Managing Video Clips, page 2-17](#)
 - [Using Record Now, page 2-24](#)
 - [Using the Pop-Up Menu, page 2-25](#)
 - [Understanding Video Pane Border Colors, page 2-27](#)
 - [Synchronizing Video Playback in Multiple Panes, page 2-29](#)
 - [Using Pan, Tilt, and Zoom \(PTZ\) Controls, page 2-32](#)
- [Viewing a Thumbnail Summary of Video Archives, page 2-39](#)
 - [Using Thumbnail Search, page 2-41](#)

Understanding the Video Viewing Options

Live and recorded Cisco Video Surveillance video can be viewed using a Cisco-provided application, as summarized in [Table 2-1](#), or a third-party application that supports ActiveX controls.

Table 2-1 *Summary of Cisco Video Viewing Options*

Viewing Tool	Application	Description	Documentation
Desktop monitoring application	Cisco Video Surveillance Safety and Security Desktop (Cisco SASD)	<ul style="list-style-type: none"> Allows simultaneous viewing of up to 16 cameras. Create Video Matrix windows for display in separate monitors. View Video Walls. Create unattended workstations. View and manage alerts. View cameras, video, and alerts based on a graphical map. 	Cisco Video Surveillance Safety and Security Desktop User Guide Tip Go to Operations > Software to download and install the application.
Web-based configuration and monitoring tool	Cisco Video Surveillance Operations Manager (Operations Manager)	<ul style="list-style-type: none"> Allows simultaneous viewing of multiple video panes: <ul style="list-style-type: none"> View up to 4 cameras with the 32-bit version of Internet Explorer. View up to 16 cameras with the 64-bit version of Internet Explorer. Create the Views and Video Walls available in the desktop Cisco SASD application. Configure the camera, streams and recording schedules. 	Cisco Video Surveillance Operations Manager User Guide
Desktop video clip player	Cisco Video Surveillance Review Player (Cisco Review Player)	Simple player used to view video clip files.	Cisco Video Surveillance Review Player Tip Go to Operations > Software to download and install the application.
Web-based server console	Cisco Video Surveillance Management Console (Cisco VSM Management Console)	Provides basic viewing features for a single stream (Stream A) from a single camera.	Cisco Video Surveillance Management Console Administration Guide

Operations Manager Requirements

See the following to monitor video using the browser-based Operations Manager:

- “Requirements” section on page 1-4
- See the [Cisco Video Surveillance Monitoring Workstation Performance Baseline Specification](#) for the complete baseline performance specifications for a video surveillance monitoring workstation.

Using the *Monitor Video* Page

Open the **Monitor Video** window to view video using the Cisco VSM Operations Manager.

Procedure

Step 1 Log on to the Cisco VSM Operations Manager.



Note See the “[Logging In](#)” section on page 1-18. You must belong to a User Group with permissions for *View Live Video* or *View Recordings*.

Step 2 If prompted, complete the on-screen instructions to install or upgrade the Cisco Multi-Pane client software on your computer.



Note This application is an Active X client that enables video playback and other features. Video will not play unless the Cisco Multi-Pane client software is correctly installed.

Step 3 Click **Monitor Video**.

Step 4 (Optional) Select **View Menu** to select a video grid of multiple cameras.

- **Select**—select a blank layout.
- **Select Views**—select a pre-defined *View*.

See the “[Selecting a Multi-Pane “View”](#)” section on page 2-4 for more information.

Step 5 Expand the location tree and drag a camera from the list onto a viewing pane.



Tip Enter a partial or complete camera name in the *Find* field to display matching cameras.



Tip You can also select a video pane by clicking in it, and then double-click the camera name.

Step 6 See the “[Controlling Live and Recorded Video](#)” section on page 2-7 to use the video playback controls.

Selecting a Multi-Pane “View”

To view video from more than one camera, select an option from the **View Menu**, as described in [Table 2-1](#):

Figure 2-1 Video Layouts

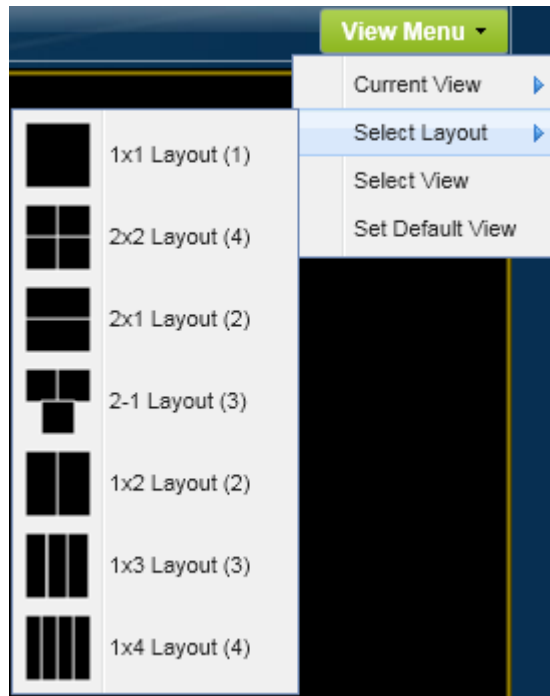


Table 2-2 View Menu

Menu	Purpose	Description
Select Layout	Blank layouts	Choose Select Layout to select a blank layout (Figure 2-1), and then select cameras for each pane.
Current View	Save or reset the currently displayed layout.	<ul style="list-style-type: none"> Choose Current View > Save As to save a layout or <i>view</i> under a new name. Enter a name and location for the view. <p>Tip Views can be assigned to the same location as the cameras, or to a higher level location. The new <i>View</i> appears under the Select View menu. Views are displayed in both the Operations Manager and Cisco Video Surveillance Safety and Security Desktop (Cisco SASD) application.</p> <ul style="list-style-type: none"> Choose Current View > Reset to reload the last view or layout and discard any changes.

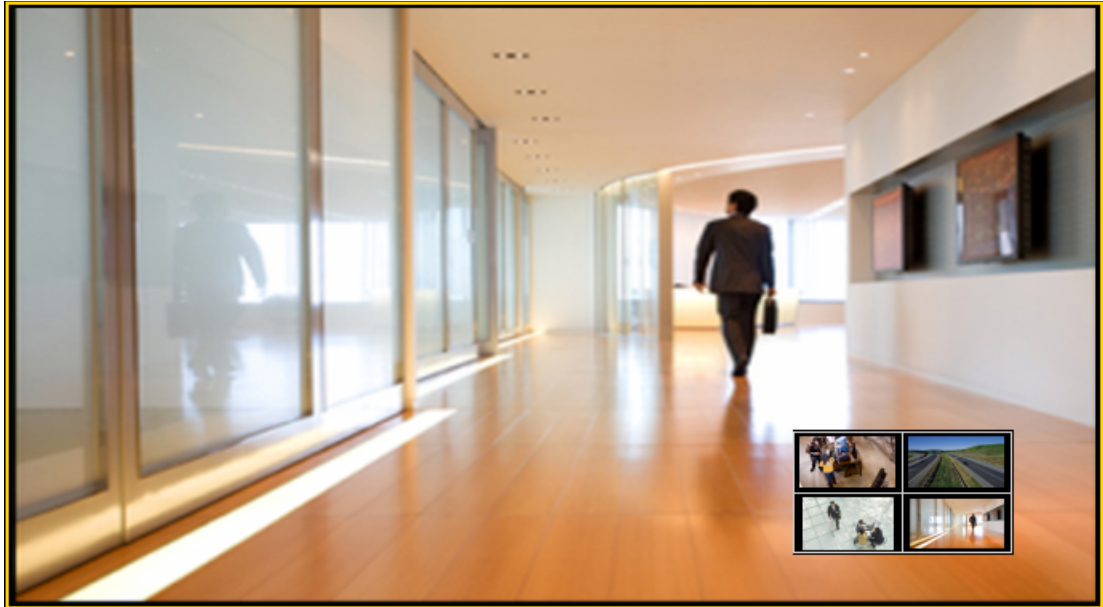
Table 2-2 **View Menu (continued)**

Menu	Purpose	Description
Select View	Display pre-defined views	<p>Choose Select View to select a pre-defined multi-pane view. <i>Views</i> can be configured to rotate video from multiple cameras to provide a virtual tour of a building or area. The video panes can (optionally) rotate video from different cameras to provide a virtual tour of a building or area.</p> <p>See the “Creating Pre-Defined Views” section on page 3-2.</p>
Set Default View	Define the view that is automatically loaded	<p>The Default View is defined by each user and is automatically loaded when they click Monitor Video.</p> <ol style="list-style-type: none"> 1. Create one or more Views as described in the “Creating Pre-Defined Views” section on page 3-2. 2. Select View Menu > Set Default View. 3. Select a View from the pop-up window and click Select. <p>Note The Default View is saved as a cookie in the browser and is unique to each user/PC. The Default View is not displayed if using a different workstation.</p> <p>See the “Setting the Default View” section on page 3-8 for more information and usage notes.</p>

**Tip**

- To change the video in a *View* pane, drag and drop a camera name onto the pane.
- *Views* can be accessed using either the browser-based Operations Manager or the Cisco Video Surveillance Safety and Security Desktop (Cisco SASD) application. The Operations Manager can display a maximum of 4 video panes using the 32-bit version of Internet Explorer, and up to 16 panes when using the 64-bit version. Cisco SASD can display up to 16 panes.
- Double-click a video pane to fill the screen with that video ([Figure 2-2](#)). A preview of the other video panes is shown in a smaller grid at the bottom of the screen. Double-click the video pane again to return the grid to normal size.

Figure 2-2 *Enlarge a Video Pane*



Controlling Live and Recorded Video

Each video viewing pane in a Cisco Video Surveillance monitoring application supports the following controls and features.

The features available on your workstation depend on the following:

- The camera and system configuration.
- Your user account access permissions.
- The features supported by the video monitoring application.

Contents

Refer to the following topics for more information.

- [Overview, page 2-8](#)
- [Viewing Live Video, page 2-9](#)
- [Viewing Recorded Video, page 2-12](#)
- [Creating, Viewing and Managing Video Clips, page 2-17](#)
- [Using Record Now, page 2-24](#)
- [Using the Pop-Up Menu, page 2-25](#)
- [Understanding Video Pane Border Colors, page 2-27](#)
- [Using the Smooth Video Options When Viewing Live Video, page 2-27](#)
- [Synchronizing Video Playback in Multiple Panes, page 2-29](#)
- [Using Pan, Tilt, and Zoom \(PTZ\) Controls, page 2-32](#)

Overview

To view live and recorded video, log on to the monitoring application and drag and drop camera names onto the available viewing panes (you can also select a pane and double-click the camera name). Use Views to view multiple panes in a single window.

For example, [Figure 2-3](#) shows a multi-pane view using the Cisco Video Surveillance Safety and Security Desktop (Cisco SASD) application.

Figure 2-3 Multi-Pane View using the Cisco Video Surveillance Safety and Security Desktop



Each viewing pane includes various controls that allow you to do the following:

- Switch between live and recorded video.
- Select the playback timespan.
- Pause, play, or skip forward and back.
- Create and save video clips from recorded video
- Mute or un-mute the audio (if available).
- Synchronize the playback of multiple recordings.
- Control the Pan Tilt and Zoom (PTZ) movements of a camera (if supported by the camera).
- Additional options are available by right-clicking the image. Options include synchronizing multiple viewing panes, recording live video, expanding the image to fill the screen, creating a snapshot image, and configuring smooth video options to improve playback performance when network performance is poor.

**Note**

The available controls depend on the camera model and system configuration. For example, pan-tilt-zoom (PTZ) controls are available only on cameras that support PTZ. Recording options are available only if the camera is configured to record video. Synchronized playback is available for recorded video (not live video). See your system administrator for more information.

Viewing Live Video

Live video is displayed by default when you log in to the viewing application. [Figure 2-4](#) summarizes the controls available in each viewing pane.

**Tip**

To control the playback in multiple video panes, `Shift-Click` or `Ctrl-Click` to select the panes. The borders of all selected panes turn to orange. Controls and actions performed in one pane also affect the other selected panes. To deselect panes, select a single pane, or use `Shift-Click` or `Ctrl-Click` to deselect the panes

**Note**


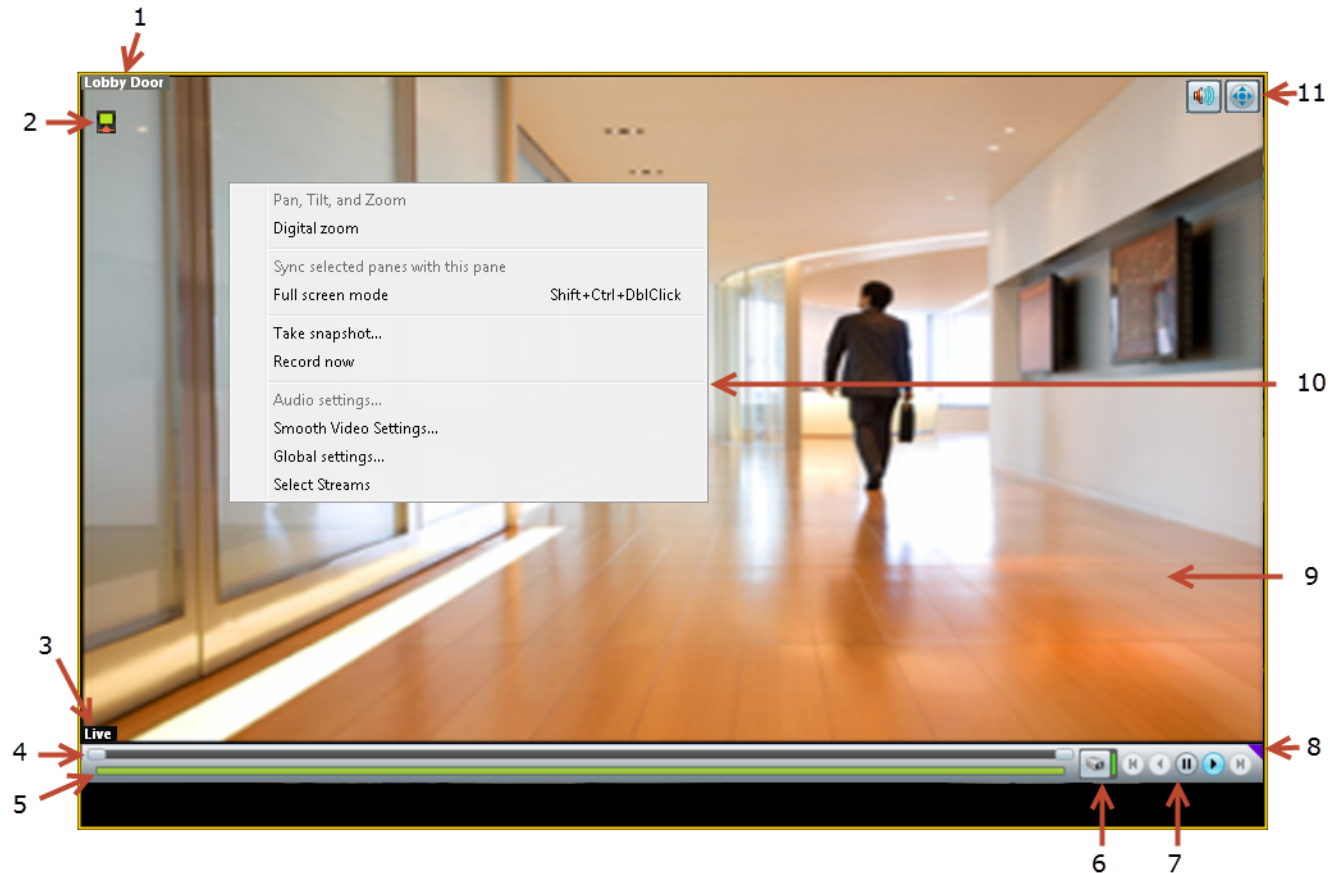













- Live video may be delayed 1-2 seconds. Live video can be further delayed if the smooth video option is enabled. See the [“Using the Smooth Video Options When Viewing Live Video”](#) section on [page 2-27](#) for more information.
- *Soft-deleted* cameras (shown with a  icon) are cameras that were removed from the system but still allow access to the camera's recorded video. You cannot display live video from *soft-deleted* cameras.
- The control bar and audio icon will not display if your workstation monitor is set to 16-bit color setting. Change your monitor *color* setting to 32-bit.

Figure 2-4 Video Pane Controls



1	Camera name—The source of the displayed video.
2	Indicates the quality of the primary live video stream. If the live video quality is poor,  , an alternative secondary or iFrame video stream can be automatically applied. See the “Using the Smooth Video Options When Viewing Live Video” section on page 2-27 for more information.
3	Indicates live or recorded video (recorded video displays a time stamp such as 4/2/2012 1:20:35:615 PM).
4	Range Bar—Used with recorded video (see the “Viewing Recorded Video” section on page 2-12 for more information).
5	Seek—Used with recorded video to choose a playback time (see the “Viewing Recorded Video” section on page 2-12 for more information).
6	The green  icon indicates live video. Click the icon to switch to the recorded view  .
7	Live video playback controls. <ul style="list-style-type: none">  —Pause the video playback.  —Play the video forward at normal speed. Note The other playback controls are used with archived video only. See Figure 2-5 on page 2-13 for more information.
8	 —Click the triangle to pin the control bar to the screen, or auto-hide the bar when the cursor is moved. Note The control bar and audio icon will not display if your workstation monitor is set to 16-bit color setting. Change your monitor <i>color</i> setting to 32-bit.

9	Video image.
10	<p>Camera menu.</p> <p>Right-click the image to open the menu and select an option. Options not supported by the camera are disabled (shown in gray). See the “Using the Pop-Up Menu” section on page 2-25 for more information.</p>
11	<p>Control icons.</p> <ul style="list-style-type: none"> —Audio. The audio icon appears if the camera supports audio. Click the icon to enable  or mute  live audio volume. This control does not affect recorded video. —PTZ. Click to enable  or disable  the Pan, Tilt and Zoom (PTZ) controls. See the “Using Pan, Tilt, and Zoom (PTZ) Controls” section on page 2-32. — See the “Synchronizing Video Playback in Multiple Panes” section on page 2-29. <p>Note The control bar and audio icon will not display if your workstation monitor is set to 16-bit color setting. Change your monitor <i>color</i> setting to 32-bit.</p>

Additional Information

Refer to the following topics for additional options:

- [Using Record Now, page 2-24](#)
- [Using the Pop-Up Menu, page 2-25](#)
- [Using the Smooth Video Options When Viewing Live Video, page 2-27](#)
- [Synchronizing Video Playback in Multiple Panes, page 2-29](#)
- [Using Pan, Tilt, and Zoom \(PTZ\) Controls, page 2-32](#)

Viewing Recorded Video

You can view recorded video from a continuous loop, for a motion event, or from a video clip. The camera must be configured to support each of these options, and you must have access to a video viewing application that supports these functions (some applications are used for viewing only).

For example, a camera can be configured to record the following:

- Continuous recordings that include video from a set amount of time, such as the past 60 minutes.
- Motion event recordings that are triggered whenever a motion event occurs. Video is recorded when the motion occurs, and for a configured number of seconds before and after the event. Use a video viewing application (such as the Cisco Video Surveillance Safety and Security Desktop) to view motion event video.



Tip

To control the playback in multiple video panes, press **Shift-Click** to select multiple concurrent panes, or **Ctrl-Click** to select individual panes. The borders of all selected panes turn to orange. Controls and actions performed in one pane also affect the other selected panes. To deselect panes, select a single pane, or use **Shift-Click** or **Ctrl-Click** to deselect the panes

Usage Notes




- Multi-pane video clips can also be saved to your desktop and played using the Cisco Video Surveillance Review Player.
- If the Record Now feature is enabled, right-click the image and choose **Record Now** to record live video.
- If a camera is *soft-deleted*, you can still access the camera's recorded video but cannot display live video. Recordings are retained on the system until removed according to the recording retention settings.
- Click the  icon to toggle between live and recorded video. The  icon appears when recorded video is displayed.
- The first time you select a camera's recorded video, the playback begins slightly behind the live (current) time. When you toggle between live and recorded, recorded video returns to the previously selected timestamp.

Figure 2-5 describes the main recording features and controls.

Figure 2-5 Viewing Recorded Video



1	Camera Name—Source of the recorded video.
2	Indicates the video quality, which can be affected by network and system performance. The icon turns red if the video quality is poor  . <p>Note This icon is for informational purposes only when displayed with recorded video (the Smooth Video options do not apply).</p>
3	Pop-up menu options. See the “Using the Pop-Up Menu” section on page 2-25.
4	Timestamp for the currently displayed video image. For example: 7/12/2012 4:08:39:886 AM . <p>Note Changes to Live when live video is displayed.</p>
5	Range Bar—The span of video to work with. <ul style="list-style-type: none"> The entire <i>range bar</i> represents the entire span of available recorded video. Slide the <i>range bar</i> selectors to shorten the range (see below). The lower (green) <i>seek bar</i> represents the selected range (see below).

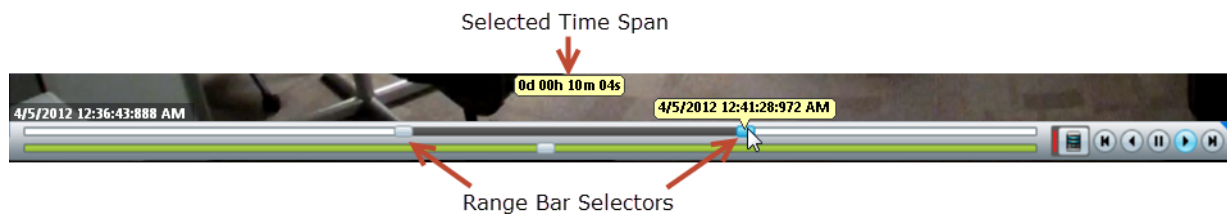
- 6** Range Bar selectors—Drag the *range bar* selectors to narrow the timespan of video you want to review.

For example, drag the selectors to create a 10 minute range. You can then drag that range left or right to the appropriate place in the recorded span.

In the following example, the entire range of recorded video is selected (the *range bar* selectors are to the far right and left). To display the timestamps, click a selector.



Click and drag the *range bar* selectors to choose a shorter period of time. In the following example, the *range bar* selectors are used to select approximately 10 minutes of video. Drag the selected range left or right to locate the desired range of recorded video.

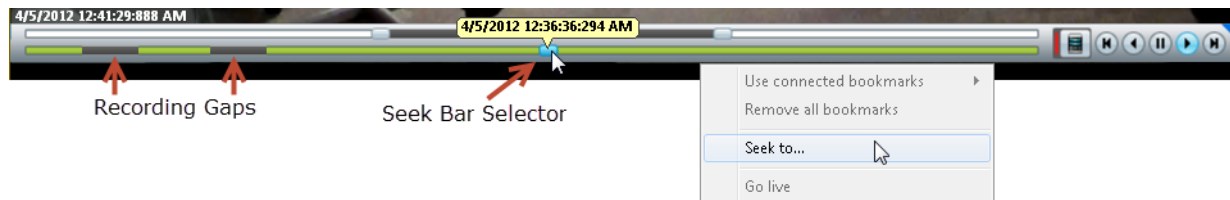


Tip The green *seek bar* represents the selected span. If the span in the top *range bar* is 10 minutes, then the green *seek bar* represents 10 minutes of video. Slide the *seek bar* selector to choose the playback time (see below).

Tip Double-click a *range bar* selector to playback the video from the beginning of that range.

- 7** Seek Bar —Represents the video range, and is used to select a playback time.

For example, if the *range* is 10 minutes, then the *seek bar* represents 10 minutes of video.



Tip Right-click the *seek bar* and select **Seek to...** to select a specific date and time.

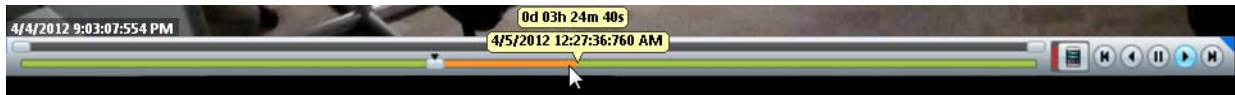
Note Gaps in the recorded video are shown in gray. Recording gaps occur if there is a manually-triggered Record Now session, if recording was manually stopped, if recording was stopped by a schedule, or if video was unavailable due to network connectivity issues, device malfunctions, or other events.

- 8** Seek Bar selector—Drag the selector to play video from the selected time (as indicated by the timestamp).

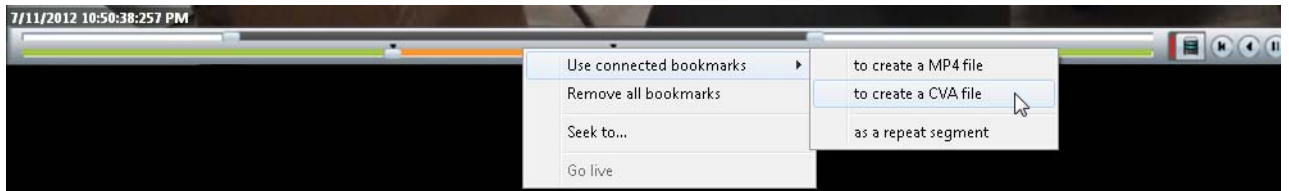
Note When you move the scroll bar for a video pane that is synchronized, that pane becomes the new synchronization master pane. The other synchronized panes play video according to the master pane. See the [“Synchronizing Video Playback in Multiple Panes”](#) section on page 2-29.

- 9 Bookmarks—Create bookmarks to save a video clip or a repeating segment (see below).

To create a bookmark, *Ctrl-Click-drag* the *seek bar*. The bookmark span is shown in orange.





- 10 Bookmarks menu—Right-click the *seek bar* to display the bookmark menu. You can save the bookmarked video as a clip in one of the supported formats, remove all bookmarks, or create a repeating segment.



See the following for more information:

- [Creating, Viewing and Managing Video Clips, page 2-17](#)
- [Creating a Repeat Segment, page 2-23](#)






- 11 Indicates live or recorded video. Click the icon to switch between live and recorded video.

-  —Live video is displayed.
-  —Recorded video is displayed.



Tip The first time you select a camera's recorded video, the playback begins slightly behind the live (current) time. When you toggle between live and recorded, recorded video returns to the previously selected timestamp.

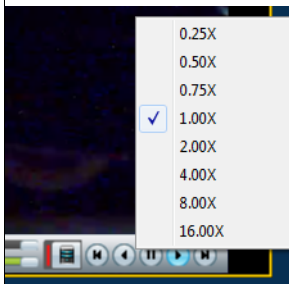
- 12 Recorded video playback controls.







-  —Step Reverse button—(Archived video only) Pauses the playback and steps back one frame at a time.
-  —Play Reverse button—(Archived video only) Plays the video archive in reverse at normal speed.
-  —Pause button—Pause the video playback.
-  —Play Forward button—Play the video forward at normal speed.
-  —Step Forward button—(Archived video only) Pauses the playback and steps forward one frame at a time.

Variable Speed Playback

Right-click the Play Reverse  or Play Forward  button to play the video slower or faster.



For example, select **0.50X** to play the video at half speed (forward or reverse). Select **4.00X** to play at 4 times the normal rate (forward or reverse).

-
- 13**  —Click the triangle to pin the control bar to the screen, or auto-hide it when the cursor is moved.
- Note** The control bar and audio icon will not display if your workstation monitor is set to 16-bit color setting. Change your monitor *color* setting to 32-bit.
-
- 14** Camera feature icons. For example:
-  or  —Audio is supported by the camera and enabled or disabled in the viewing pane.
 -  —The synchronization icon appears in video panes that play synchronized video. See the [“Synchronizing Video Playback in Multiple Panes”](#) section on page 2-29.
- Note** The PTZ icons are enabled only for live video.
- Note** The control bar and audio icon will not display if your workstation monitor is set to 16-bit color setting. Change your monitor *color* setting to 32-bit.
-

Creating, Viewing and Managing Video Clips

Video clips can be created in multiple formats for playback using the Cisco VSM Review Player, or a third party player.



Note Timestamps are not displayed in 3rd-party video viewers. Use the Cisco Review Player to display timestamps (see the [Cisco Video Surveillance Review Player User Guide](#) for more information).

This section includes the following topics:

- [Supported File Formats](#), page 2-17
- [MP4 Video Clip Usage Notes](#), page 2-18
- [Creating Video Clips](#), page 2-18
- [Viewing and Downloading MP4 Clips](#), page 2-21

Supported File Formats

Cisco Video Surveillance supports the creation and playback of the following video formats:

Table 2-3 Video Clip File Formats

File Format	Description
MP4	<p>A standard video file format that is playable on most computers and useful for sending to 3rd parties. MP4 clips support a single video pane and can include audio (CVA/CVX files do not support audio). MP4 clips are saved on the server for 7 days and must be downloaded using the Select Streams and Clips menu or the or Clip Search option.</p> <p>Notes</p> <ul style="list-style-type: none"> • MP4 clips are automatically deleted from the server 7 days after creation. Download the clips to a local drive if necessary (see the “Viewing and Downloading MP4 Clips” section on page 2-21). • MP4 audio playback is supported only with the Cisco VSM Review Player or VLC media player. • Use the Cisco VSM Review Player to save MP4 files in the tamper proof MPX format. See the Cisco Video Surveillance Review Player User Guide for more information.
CVA	<p>Cisco video archives (CVA) can include multiple video panes that synchronize to the same time. CVA files can only be opened in applications that support the CVA format (such as the Cisco Review Player).</p> <p>CVA files do not support audio playback.</p>
CVX	<p>A tamper proof CVA file. CVX files require a password that is entered when the file is created. You must enter the password to open and view the video file. CVX video playback will shut down if the file is tampered with.</p> <p>CVX files do not support audio.</p>



Tip You can also right-click a video pane and select **Take Snapshot** to save a still image in BMP, JPEG, PNG, and TIFF formats. See the [“Using the Pop-Up Menu”](#) section on page 2-25 for more information.

MP4 Video Clip Usage Notes

MP4 clips are saved on the server. Review the following notes to manage the server-side clips.



Note

CVA/CVX clips are downloaded immediately and not stored on the server.

- MP4 clips are automatically deleted after 7 days.
- MP4 clips require that the clipping repository be selected on the Media Server associated with the camera. See the [“Partition Settings” section on page 7-5](#).
- If using the Operations Manager browser interface, you can also use **Clip Search** to view, download and delete MP4 clips saved to the server. See the [“Clip Search \(View, Download and Delete MP4 Clips\)” section](#).
- You can create up to five MP4 clips at a time per Media Server.
- Users can only delete their own clips. Users that belong to a User Group with *Camera* permissions can also delete other users’ clips.
- If the clipping fails, see your system administrator for assistance.
- MP4 clips play automatically in the pane when downloaded. The clips can also be viewed using the Cisco VSM Review Player or VLC media player.

Creating Video Clips

To create video clips, create a bookmark span and select the file format, as described in the following procedure.

Requirements

- You must belong to a User Group with *Export Recordings* permissions to create, view or download video clips.
- The Media Server hard disk volume must have sufficient disk space to create the video clip or the operation will fail. See your system administrator for more information.

Procedure

Step 1 Select a video pane from the viewing application (such as Cisco SASD or Operations Manager).




Tip

To create a multi-pane clip in the CVA format, press *Shift-Click* to select multiple concurrent panes, or *Ctrl-Click* to select individual panes.

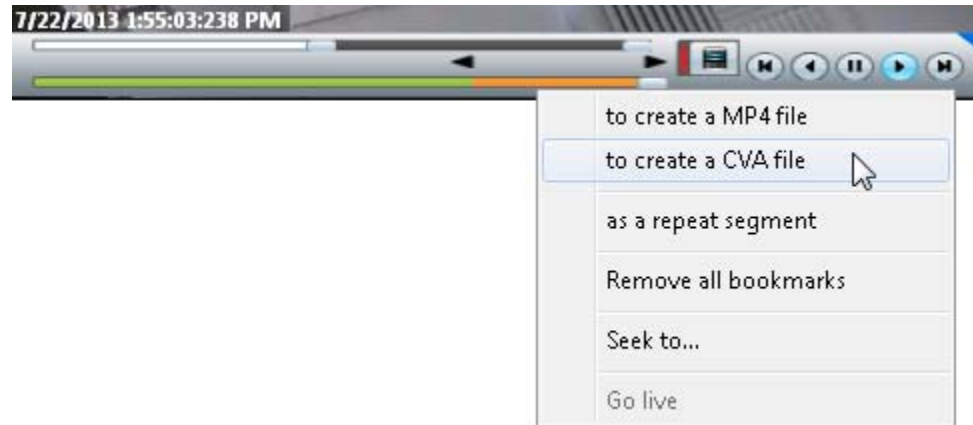
Step 2 In the green *seek* bar, *Ctrl-Click* and drag the mouse cursor to create a bookmark span. The bookmark span is shown in orange ([Figure 2-6](#)).



Tip

In recording mode , you can also right-click the image and choose **Select Clip Range** from the pop-up menu (see the [“Using the Pop-Up Menu” section on page 2-25](#)). A 10 minute clip range is automatically selected starting from current thumb position, and the range bar is automatically scaled to 1 hour.

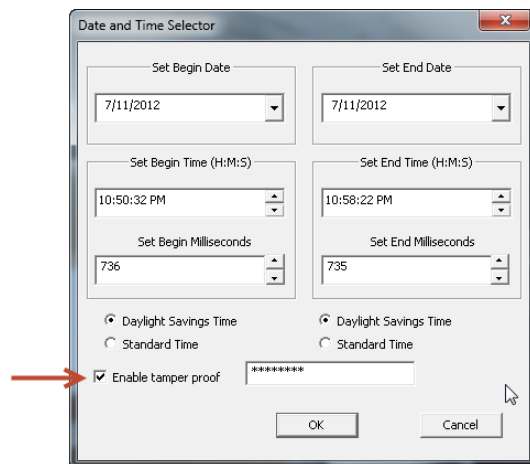
Step 3 Right-click the bookmark and select an option to create a file in the desired format ([Figure 2-6](#)).

Figure 2-6 *Creating a Video Clip*

Step 4 Save the file:

CVA/CVX files

- a. (Optional) Revise the start and end date and time (Figure 2-7). Enter a time between 30 seconds and 4 hours (the range cannot include more than one codec and the start time must be before the end time).

Figure 2-7 *CVA Clip Settings*

- b. (Optional) Select **Enable tamper proof** and enter a password to create a password-protected CVX file.
- c. Click **OK**.
- d. Select a location on a local disk and click **Save**.
- e. Wait for the clip to be generated and downloaded. Video streaming is paused during CVA/CVX clip generation.

MP4 clips

- a. (Optional) Revise the start and end date and time (Figure 2-8). Enter a time between 30 seconds and 4 hours (the range cannot include more than one codec and the start time must be before the end time).

Figure 2-8 *MP4 Clip Settings*

- b. (Optional) Enter a clip name that identifies the recording on the server (Figure 2-9). For example, if you enter “My 4500 Camera” then the clip selection will be “My 4500 Camera__1347005138141”. If blank, the default name is “My Clip__system-timestamp”.
- c. (Optional) Select or deselect **Record Audio** (if the camera supports audio recordings) to include or exclude audio. Audio playback is supported only with the Cisco VSM Review Player or VLC media player.
- d. Click **OK** to save the clip to the server.



Tip

Right click the image and select **Get clip status** to view the current status: In-Progress, Completed or Failed. Use the **Clip Search** option to view, download, delete and manage MP4 clips saved on the server.

- Step 5** Download and play the clip as described in the “[Viewing and Downloading MP4 Clips](#)” section on page 2-21.

Viewing and Downloading MP4 Clips

You can right-click a video pane and choose **Select Streams and Clips** to save and play MP4 clips. The clip remains on the server for 7 days after it was created.



Tip

If using the Operations Manager browser interface, you can also use **Clip Search** to view, download and delete MP4 clips saved to the server. See the “Clip Search (View, Download and Delete MP4 Clips)” section.



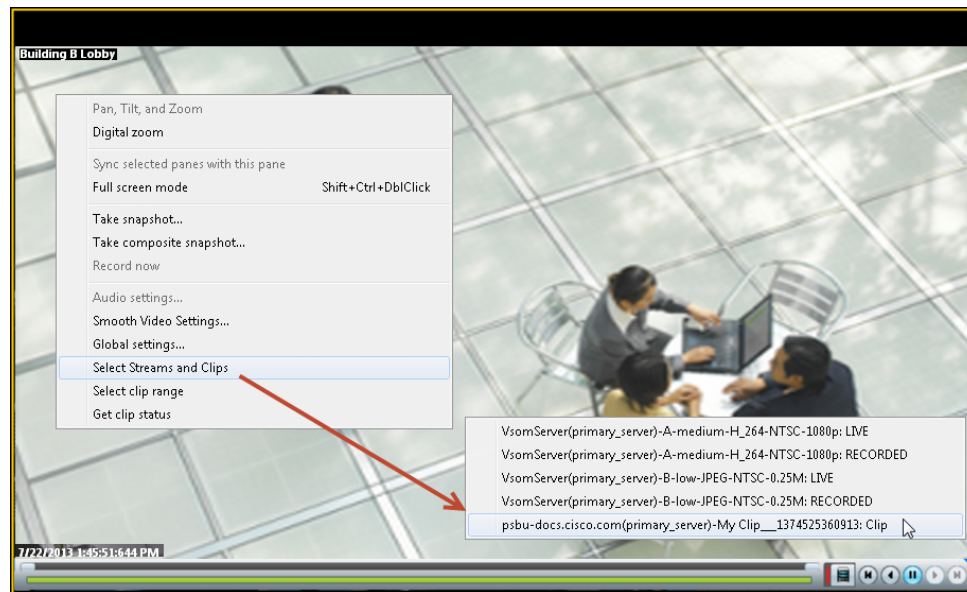
Note

See the “MP4 Video Clip Usage Notes” section on page 2-18 for more information.

Procedure

- Step 1** Right-click the video pane and choose **Select Streams and Clips** (Figure 2-9).
- Step 2** Select the *Clip* file.

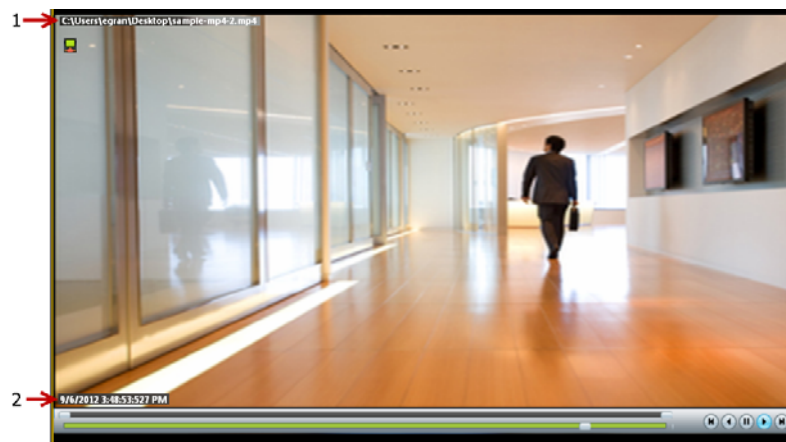
Figure 2-9 Accessing a MP4 Clip



Note

Clips are automatically deleted from the server after 7 days.

- Step 3** Enter a file name and location.
- Step 4** Click **Save** and wait for the clip to download.
- Step 5** The clip will automatically play in the pane the first time it is downloaded (Figure 2-10). To view the clips again, use a viewing application such as the Cisco Review Player.

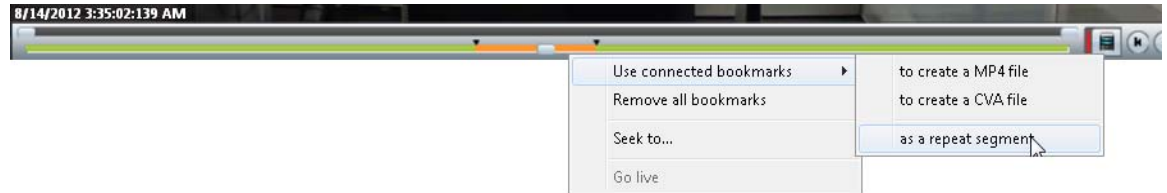
Figure 2-10 *MP4 Clip Viewing Pane*

1	MP4 file name and location	2	Timestamp for currently displayed image.
----------	----------------------------	----------	--

Creating a Repeat Segment

A *repeating segment* is a range selected on a recording that plays continuously in a loop. When the end of the segment is reached, playback starts over from the beginning of the segment. The video segment loops indefinitely until you cancel the segment or seek video outside the selected range (seeking inside the selected range does not cancel the segment).

Figure 2-11 Create a Repeating Segment



Note

Repeating segments are used with recordings only.

Procedure

- Step 1** *Ctrl-Click-drag* the *seek bar* in a recording to create a bookmark (Figure 2-11).
The bookmark span is shown in orange.
- Step 2** Right-click the *seek bar* and select **as a repeat segment**.
- Step 3** (Optional) Enter a specific start and end date and time.
- Step 4** To cancel the segment, right click the segment and choose **Remove all Bookmarks**.
You can also click on the seek bar outside the selected range.

Using Record Now

To manually trigger recording of a live video stream, right-click the image and choose **Record Now**.

Requirements

- The Record Now option must be enabled for the camera configuration in the Operations Manager.
- Your use account must include access permissions to view recorded video.
- You can record video from the live primary video stream only.

Usage Notes

- Audio is not recorded.
- Video is recorded for a system-defined length of time (the default is 5 minutes).
- The recording is retained on the system according to the event retention settings for the camera. For example, if the camera's event recordings are retained for 30 days, then the Record Now recordings will also be available for 30 days. When the retention time is exceeded, the recording is automatically deleted (see the [“Creating, Viewing and Managing Video Clips”](#) section on page 2-17 to save the video to a separate file).

Procedure


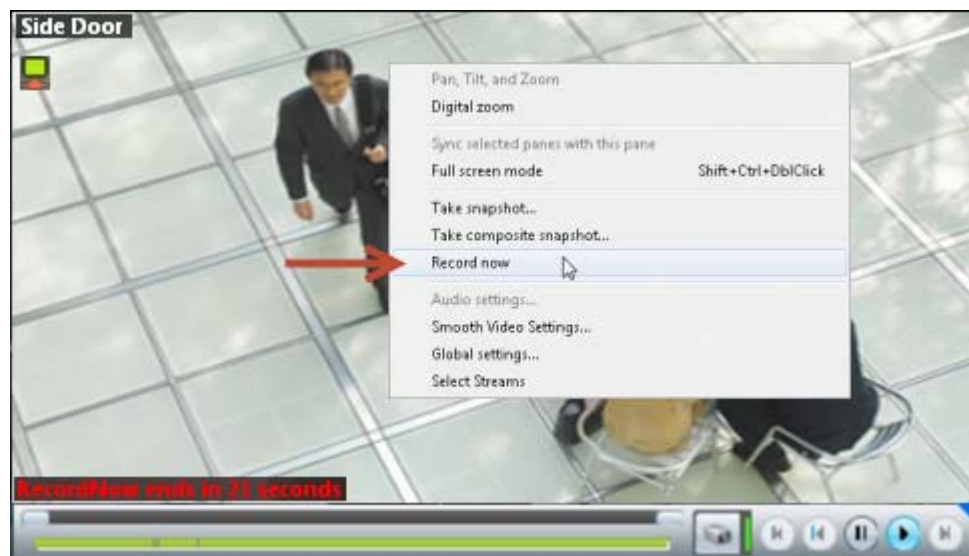
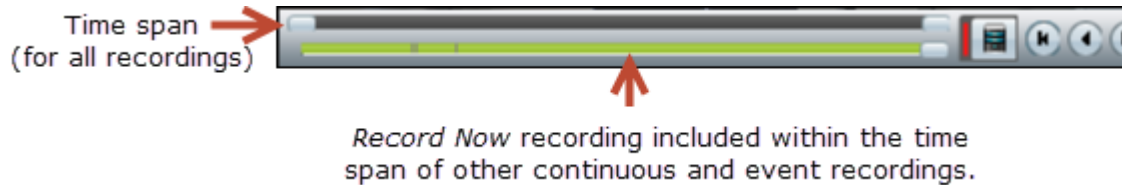
- Step 1** Log in to the video viewing application and select a camera.
- Step 2** Choose live video  (see the [“Viewing Live Video”](#) section on page 2-9).
- Step 3** Right click the image and choose **Record Now** (Figure 2-12).
 - The recording is performed in the background. You can continue to use the other playback controls.
 - The recording status is displayed in red text (Figure 2-12) when the recording time nearly complete.

Figure 2-12 *Record Now*

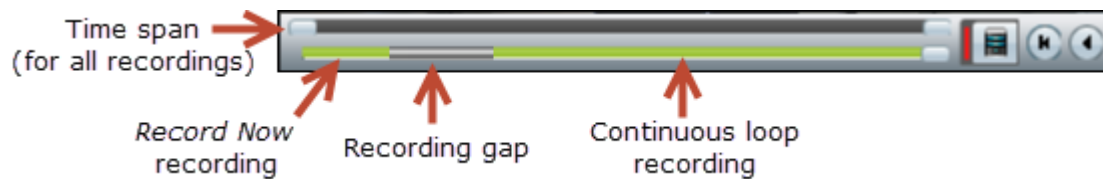


Step 4 To view the recorded video, review the following notes.

- Record Now clips are available from the primary stream only. Right click the image and choose **Select Streams and Clips** to view the recorded primary stream (disabled if the pane is synchronized).
- If the video is within the time span of other recorded video, there is no separate indication of the Record Now video. You can access the video as described in the [“Viewing Recorded Video” section on page 2-12](#)).



- If the Record Now video is older than the continuous loop, the gap between the recording times is shown in gray:



Note

When the event retention time is exceeded, the Record Now recording is automatically deleted. To save the recording, see the [“Creating, Viewing and Managing Video Clips” section on page 2-17](#).

Using the Pop-Up Menu

Select a video pane and right-click on the image to open a menu with the following options (see [Figure 2-4 on page 2-10](#)).

Table 2-4 Camera Pop-Up Menu (Right-Click the Video Image)

Camera Menu Item	Description
Pan, Tilt, and Zoom	(Live video only) Open the PTZ preset list that allows you to quickly adjust the camera view. See the “Using Pan, Tilt, and Zoom (PTZ) Controls” section on page 2-32
Digital zoom	Digitally enlarges the image to zoom in on a specific area. Double click the enlarged image to use a window-in window view. Adjust the viewing area in the small window to define the portion of enlarged video to display.

Table 2-4 Camera Pop-Up Menu (Right-Click the Video Image) (continued)

Camera Menu Item	Description
Sync selected panes with this pane	<p>Synchronizes the playback from multiple video panes to the same time.</p> <ul style="list-style-type: none"> After a pane is synchronized, the menu item changes to Remove this pane from sync. To synchronize additional panes, right-click an un-synchronized pane and select Add selected panes to sync. <p>See the “Synchronizing Video Playback in Multiple Panes” section on page 2-29.</p>
Full screen mode	<p>Enlarges the video image to fill your display screen.</p> <p>Tip To exit, press ESC, or right-click and choose Full screen mode again.</p>
Take snapshot	Saves a snapshot of a single video pane (<i>excluding</i> control icons, timestamps and other information) in BMP, JPEG, PNG, or TIFF format.
Take composite snapshot	Saves a snapshot of all panes in a multi-pane layout (<i>including</i> control icons, timestamps and other information) in BMP, JPEG, PNG, or TIFF format.
Record now	<p>(Live video only) Immediately begins recording video.</p> <p>See the “Using Record Now” section on page 2-24 for more information.</p> <p>Note The Record Now option must be enabled in the camera configuration.</p>
Audio settings	(Cameras with audio support only). Opens a window used to adjust video playback volume and balance.
Smooth video settings	<p>(Live video only) Creates a smooth video playback if the playback is choppy or delayed due to network or other performance issues.</p> <p>See the “Using the Smooth Video Options When Viewing Live Video” section on page 2-27.</p>
Global settings	Provides settings that apply to all video panes. For example: <i>UI transparency</i> and <i>zoom video to fit the pane</i> .
Select Streams and Clips	<p>Allows you to select the live and recorded video streams (primary or secondary) supported by the camera.</p> <p>Note <i>Select Streams and Clips</i> is disabled when the pane is synchronized. See the “Synchronizing Video Playback in Multiple Panes” section on page 2-29 for more information.</p>
Select clip range	<p>(Archive video only) Selects a 10 minute clip range starting from current thumb position. The range bar is automatically scaled to 1 hour.</p> <p>See the “Creating, Viewing and Managing Video Clips” section on page 2-17 for more information.</p>
Get clip status	Shows the current status of MP4 clips: In-Progress, Completed or Failed.

Understanding Video Pane Border Colors

The color that surrounds a video pane indicates the status of the video in that pane. For example, when you click anywhere in a video pane, the pane becomes active and the border changes to orange. The controls and actions performed apply to the active pane.

Table 2-5 describes the meaning of each color.

Table 2-5 Video Pane Border Colors

Color	Description
Gray	The pane is not highlighted. All panes have a gray border by default.
Orange	The pane is selected as the active pane, and the controls and actions apply to that pane. If multiple panes are selected as active panes, the controls and actions performed on one pane apply to all active panes.




Using the Smooth Video Options When Viewing Live Video

If live video playback is choppy due to network or other performance issues, use the **Smooth video settings** to automatically do the following:

- Create a video data buffer (in seconds) that delays live playback while video data is cached. Live video can then be played back smoothly despite network delays between the camera, Media Server, and workstation.
- Automatically switch to a different stream if the live video quality is poor.

Icon Colors

The video quality icons in each pane indicate the following:

- Green  indicates everything is fine.
- Yellow  indicates that the client workstation has detected the play back is not smooth.
- Red  indicates a severe adverse situation. Action will be taken to correct the situation, such as switching to secondary stream or iFrame streaming.

Usage Notes

- The *Smooth Video Options* are available only for live video on non-PTZ cameras (the *Smooth Video Options* are automatically disabled on PTZ cameras).
- The settings are applied to all non-PTZ cameras and are persistent for the current PC workstation. For example, the settings will remain if you log out and back in, or view a different camera and then return to the current camera.
- The settings also apply to the non-PTZ cameras when using the Cisco Safety and Security Desktop (SASD) application and the Cisco Video Surveillance Management Console.
- The Smooth Video options are disabled if you manually select a stream (right-click a video pane and choose **Select Streams and Clips**). The pane will display the selected stream even if the video quality is poor (the video will *not* automatically switch to the Smooth Video alternative stream). To cancel the manually selected stream and re-enable the Smooth Video settings, reload the view or drag and drop the camera again.
- If a video stream is selected from a redundant media server, the Smooth Video option is disabled (the camera will not use a secondary stream even if the video quality icon is red).

Procedure





-
- Step 1** Right-click a live video image to open the pop-up menu.
- Step 2** Select or deselect **Enable Smooth Video for Live non-PTZ Camera** to enable the smooth video options.
- Step 3** (Optional) Enter the **Preroll Buffer Size in Seconds** to define the number of seconds that live video will be delayed.

Video data is saved in a cache on your PC to avoid pauses caused by network bandwidth and other issues. We recommend a value between 1.5 and 3 seconds.






Caution

We strongly recommend that the **Preroll Buffer** be disabled (enter **0** or leave the field blank) since streaming delays can cause a potential security risk. We recommend that you address the network bandwidth or performance issues causing the delays. Use the **Preroll Buffer** only when significant stuttering occurs and a network resolution is not available.

- Step 4** Use the **Smooth Video Options** to define an alternative video stream that will be used if video quality is poor despite the smooth video buffer (video quality is indicated by the  icon on the live viewing pane).
- **Secondary Stream**—(Only if configured on the camera) If the live video quality is poor , the secondary video stream is used. Secondary streams typically present a lower-quality image that requires less bandwidth and processing.
 - **I frame only**—If the live video quality is poor , then only the iFrame video is displayed. iFrame video reduces the bandwidth requirement to correct the situation.
 - **None**—If the live video quality is poor , no change is made and the selected stream is displayed even if it results in choppy or paused playback.



Note

- These options are not used if the video quality is *acceptable*  or if the icon is yellow (*intermediate*) . The selected stream is displayed normally.
 - A down arrow  is displayed when the secondary or iFrame stream is applied.
 - If an alternative stream is applied, the settings remain until you close and reopen the video source (camera).
-

Synchronizing Video Playback in Multiple Panes

To synchronize video playback from multiple panes, select multiple panes, right-click the pane that defines the master time, and choose **Sync Selected Panes With This Pane**. All panes will play video from the same date and time.

Usage Notes


- All panes will play forward when synchronization begins, even if one or more of the panes was playing in reverse.
- Synchronization for recorded video is performed only if the time in the selected panes overlap. If the time for a video pane does not overlap with the master pane, the pane is excluded from synchronization.
- When you move the scroll bar for a video pane that is synchronized, that pane becomes the new synchronization master pane. The other synchronized panes play video according to the new master pane.
- If the seek controls are used to search video, the other synchronized panes pause until the seek completes, then continue to display video that is synchronized with the new master pane time.
- You can switch the synchronized panes between live and recorded video.
- To remove a pane from the synchronized playback, right-click the pane and choose **Remove This Pane From Sync** to remove it.
- To add un-synchronized panes, right-click the pane and choose **Add selected panes to sync**.
- The **Select Streams and Clips** menu item is disabled when a pane is synchronized.
- When 16 video panes are synchronized, some live video panes may appear to be not synchronized if the video stream is configured for the following:

Format	Resolution	Framerate
JPEG	640x480	30 fps
H-264	1920x1080	30 fps

Figure 2-13 describes the main synchronization attributes.

Figure 2-13 Synchronized Playback of Recorded Video



- | | |
|---|--|
| 1 |  —The synchronization icon appears in the video panes that display synchronized video. |
| 2 | The timestamp for synchronized video is the same. |
| 3 | Roll over a synchronized pane to display the playback controls. Changes to any pane are mirrored by the other panes. |
| 4 | Unsynchronized panes can continue to display live or recorded video.
To add a pane to the synchronized group, right-click the pane and select Add selected panes to sync . |

Procedure

To play recorded video from multiple video panes synchronized to the same time, do the following:

- Step 1** Select a layout or pre-defined view from the **View** menu.
- Step 2** *Shift-click* or *Control-click* to select multiple video panes for synchronization.
The selected panes are displayed with a light yellow border.

Step 3 Right-click a video pane and select **Sync Selected Panes With This Pane** from the menu.
The selected pane becomes the master pane.


Step 4 (Optional) To remove a pane from the synchronized group, right-click the pane and choose **Remove This Pane From Sync**.




Note The pane continues to play video from the same timestamp, but the video can be stopped or altered without affecting the other panes.

Step 5 (Optional) To add un-synchronized panes, right-click the pane and choose **Add selected panes to sync**.

Using Pan, Tilt, and Zoom (PTZ) Controls

Cameras that support pan, tilt and zoom (PTZ) movements display a PTZ icon .

- To pan and tilt, *left-click* the image (the movement icons  appear) and drag the mouse right, left, up and down.
- To zoom, hold down the left mouse button and use the scroll wheel to zoom in and out



Tip

To use a USB joystick, see the [“Calibrating a Joystick for Windows 7”](#) section on page 2-34.

In addition, PTZ presets allow the camera to quickly jump to a preset position. For example, a PTZ preset could zoom in on a doorway, or pan to the opposite end of a parking lot. PTZ presets can be triggered using a mouse, joystick or automatically triggered event.



Note

Cameras can also be configured with PTZ tours that automatically cycle between PTZ preset positions. You can interrupt the tour using the PTZ controls, and the tour will resume after a set amount of time. See your system administrator for more information.

Figure 2-14 summarizes the controls and information available on each PTZ camera viewing pane.

Figure 2-14 Camera PTZ Controls



1	Selected Camera	3	PTZ Enabled/Disabled Icon (click to toggle)
2	PTZ is available in Live mode only	4	PTZ Preset Menu (right-click to access)

Usage Notes




- PTZ movements are available only when viewing live video.

- PTZ can only be enabled for a single video pane if multiple panes are displayed. See the [“Using PTZ Controls When Multiple Video Windows are Displayed”](#) section on page 2-35.
- You must also belong to a user group with *Perform PTZ* permissions.
- PTZ commands are available only if the primary Media Server is functional. If the Primary server goes down, or is not available on the network, PTZ commands will not function even if video is still being delivered by a redundant server (if configured).

Procedure

To control a camera's PTZ movement or trigger a PTZ preset position, do the following:

-
- Step 1** Display the live video from a PTZ-enabled camera:
- a. Click **Monitor Video**.
 - b. Expand the location tree and select the camera.
 - c. Highlight a video pane and double-click a camera name.


- Step 2** Verify that the PTZ controls are enabled:
-  —PTZ controls are supported by the camera and enabled in the viewing pane.
 -  —PTZ controls are disabled. Click the  icon to enable PTZ controls.



Note If a higher-priority user is using the PTZ controls, the PTZ controls remain locked and you cannot control the PTZ movements until released by the higher priority user.

- Step 3** To move the camera position, use the following controls.

Using a Mouse

- Pan and Tilt—*Left-click* the image and drag the mouse () right, left, up and down.
- Zoom—Hold down the left mouse button and use the scroll wheel to zoom in and out.

Using a USB Joystick

- Pan—move the joystick bar horizontally.
- Tilt— move the joystick bar vertically.
- Zoom —twist the joystick.



Tip See the [“Calibrating a Joystick for Windows 7”](#) section on page 2-34 for information to set up a USB joystick for the first time.

- Step 4** (Optional) Select a PTZ preset position.

Using a Mouse

- *Right-click* the image and choose **Pan, Tilt, and Zoom** and then **Presets** ([Figure 2-14](#)).
- Choose a preset to move the camera to the defined position.

Using a USB Joystick

- Press the joystick button that corresponds to the PTZ preset number.

- For example, joystick button 1 triggers PTZ preset 1, joystick button 2 triggers PTZ preset 2, etc.
-

Calibrating a Joystick for Windows 7

To use a USB joystick to control PTZ camera movements, connect the joystick to a USB port on the client PC and calibrate the device for Window 7. You can use the software and instructions included with the joystick, or use the built-in Windows calibration utility, as described in the following procedure.

Procedure

- Step 1** Install and configure the USB joystick according to the manufacturer instructions.
- See the device documentation for more information.
 - The manufacturer may also include a calibration utility that can be used instead of the built-in Windows utility.
- Step 2** In Windows 7, calibrate the device using the **Game Controllers** control panel.
- a. Select **Control Panel** from the **Start** menu.
 - b. Select **Hardware and Sound**.
 - c. Select **Devices and Printers**.
 - d. Double-click **Game Controllers**.
 - e. Highlight the joystick device and click **Properties**.
 - f. Click **Calibrate** in the pop-up window.
 - g. Follow the on-screen instructions to complete the process.



Tip

You can also use the Windows search function: choose **Search** from the **Start** menu and enter “*set up USB game controllers*” to open the *Game Controllers* control panel. Highlight the joystick icon and click **Calibrate**. Follow the on-screen instructions to complete the process.

- Step 3** Click **Finish** or **OK** to close the windows.
-

Using PTZ Controls When Multiple Video Windows are Displayed

When multiple viewing panes are displayed, only a single pane can have PTZ controls enabled at a time (Figure 2-15). This prevents a USB joystick from affecting more than one pane.




- The pane with PTZ enabled displays a  icon. The  icon indicates that PTZ controls are disabled.
- Click the disabled icon  to enable the controls for a pane (and disable the controls for the other panes).
- If a pane does not display an icon, then the camera does not support PTZ movements.

Figure 2-15 PTZ Controls in a Multi-Pane View



1	PTZ enabled viewing pane	3	PTZ not supported by camera (no icon)
2	PTZ disabled viewing pane		


Note

PTZ movements are available only when viewing live video.


Tip

If multiple browser windows are used to display video, joystick PTZ commands will affect the enabled PTZ pane in each browser window.

Clip Search (View, Download and Delete MP4 Clips)

Select **Clip Search** from the **Monitor Video** window (Figure 2-16) to view, download and delete MP4 clips saved to the server.



Tip

You can also create and download clips by right-clicking a video pane. See the “[Viewing and Downloading MP4 Clips](#)” section on page 2-21.



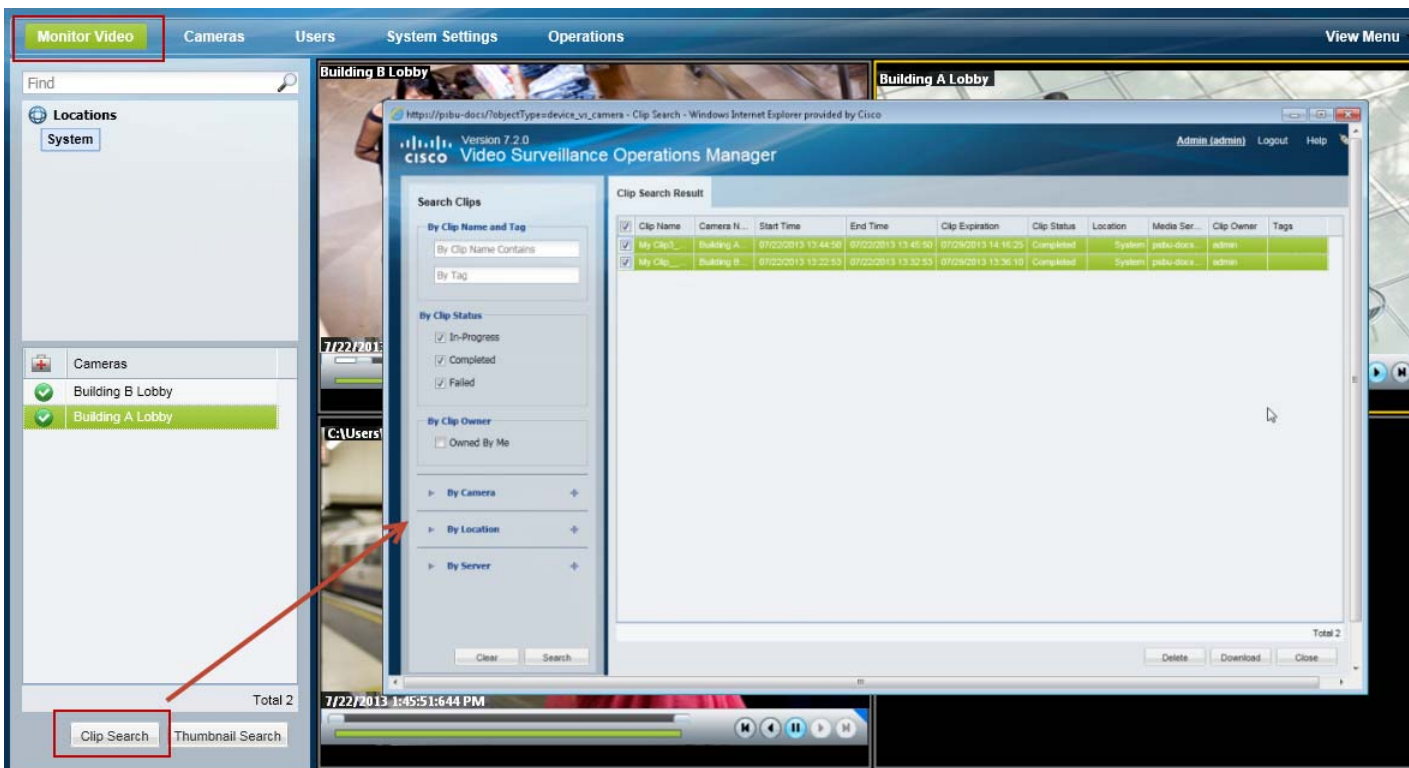
Note

Review the “[MP4 Video Clip Usage Notes](#)” section on page 2-18 before you begin.

Procedure

Step 1 From the **Monitor Video** page, click **Clip Search** to open the Clip Search window (Figure 2-16).

Figure 2-16 Clip Search Window



Step 2 (Optional) Use the filters to search for specific clips (Table 2-6):



Tip

Click **Search** without filters to display all available clips.

Step 3 Click **Search**.

Step 4 Review information about the clips.

Table 2-7 Video Clip Information

Field	Description
Clip Name	The clip name entered when the clip was created. The default is “My Clip” if no name is entered.
Camera Name	The camera name where the clip originated.
Start Time	The start timestamp for the clip.
End Time	The end timestamp for the clip.
Clip Expiration	The date/time when the clip will be deleted from the server.
Clip Status	In-Progress, Completed or Failed
Location	Location of the cameras where the clip originated.
Media Server	The Media Server that manages the camera video where the clip originated.
Clip Owner	The user that created the clip.
Tags	Tags associated with the clip (blank in Release 7.2)

Step 5 (Optional) To download a clip, select a clip and click **Download**.



Note Only a single clip can be downloaded at a time.



Note If an “HTTP 400 Bad Request” error appears, it may be due to the Internet Explorer (IE) settings. In IE, go to **Tools > Internet Options > Advanced** and select “**Use HTTP 1.1**”. Also deselect “Use HTTP 1.1 through proxy connections”. Next, click the **Connections** tab, choose the **LAN settings** button and select “**Automatically detect settings**”.

- a. Click **Continue** and accept the security certificate when the Internet Explorer web browser prompts you to proceed to the secure page. This prompt appears only once for each Media Server.
- b. Select one of the following options:
 - **Open**—Plays the file using your default video player.

- **Save** —Saves the file to the default location using a default filename.
- **Save As**—Enter a new filename and select a location on the local disk.
- **Save and Open**—Saves the file to the default location using a default filename, and then plays the clip using your default video player.

Step 6 (Optional) To permanently delete a clip from the server, select one or more clips and click **Delete**.

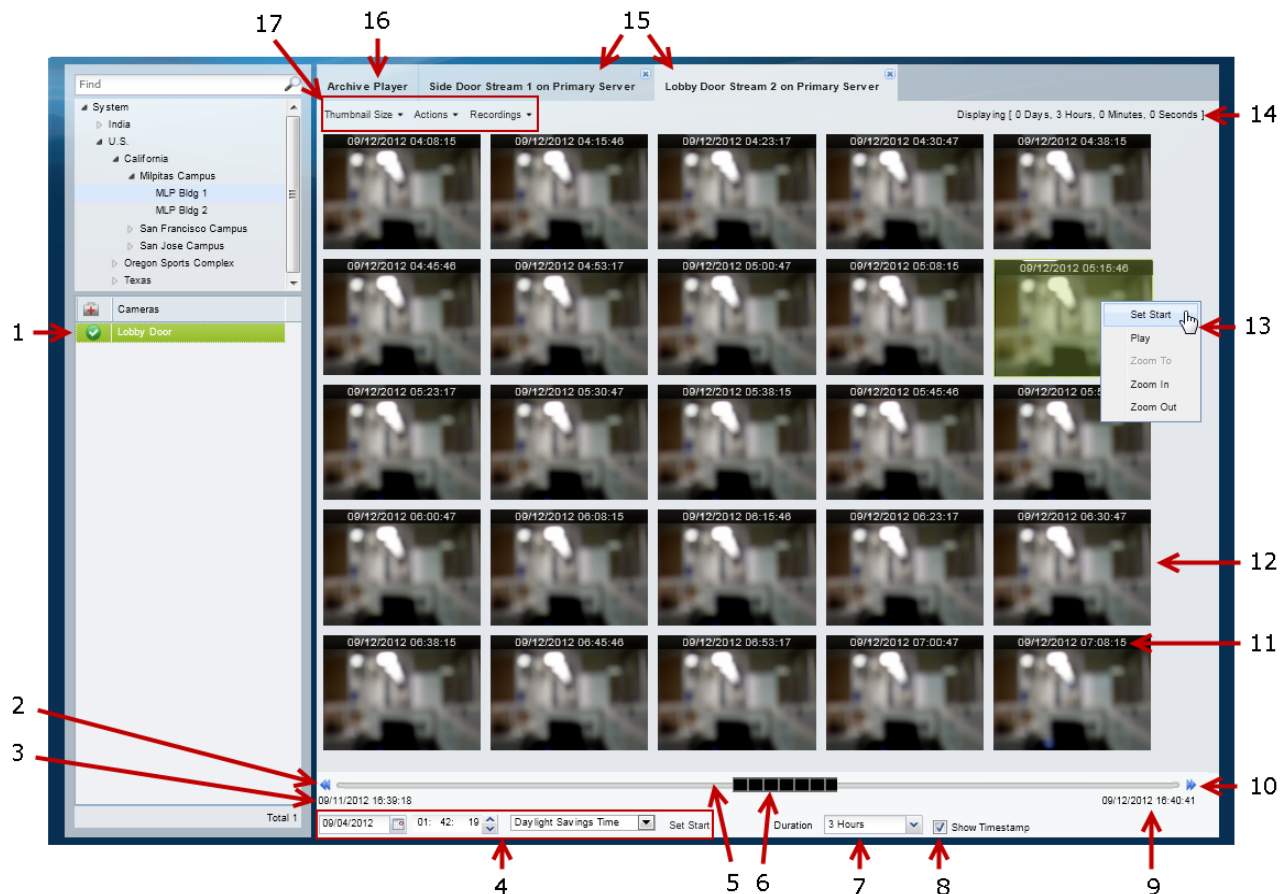
**Note**

Only the server file is deleted. Any clips previously downloaded to a local disk are not affected.

Viewing a Thumbnail Summary of Video Archives

Use *Thumbnail Search* to quickly locate specific scenes or events in recorded video. Thumbnails are an alternative way to search through recorded video without fast-forwarding or rewinding. [Figure 2-17](#) provides an overview of the search and display controls. See the “Using Thumbnail Search” section on [page 2-41](#) for step-by-step instructions.

Figure 2-17 Thumbnail Window



1	Selected Camera	<p>Select a location and double-click a camera name to display a thumbnail summary of recorded video for the camera.</p> <ul style="list-style-type: none"> Use the Recordings menu to select a camera stream. Cameras are displayed as tabs along the top of the window. Double-click multiple cameras to open a tab for each camera. Double-click an archive to play video in an <i>Archive Player</i> tab.
2	Skip back	Skip back by the Duration time increment (see #7). This icon is disabled if the entire archive is selected.
3	Archive start time	<p>The start date and time for the entire video archive.</p> <p>See #4 to select a new start time, or right-click a thumbnail and choose Set Start.</p>

4	Set Start Time	The start date and time for the first thumbnail (in the top left corner of the window pane). To change the start thumbnail, select a new date and time and click Set Start . Tip You can also select a thumbnail image and select Actions > Set Start to set the start time to a specific thumbnail (or right-click the thumbnail image and select Set Start).
5	Timeline	Timeline representing the entire video archive.
6	Start time slider	The slider represents the Duration setting relative to the length of the entire archive. If the Duration setting is for the entire archive, the black slider covers the entire time line and cannot be moved. To use the slider, choose a Duration that is less than the entire archive time and drag the slider to a different start time (the time is displayed above the slider). Release the mouse button to choose the new time.
7	Duration	Choose the time span for the displayed thumbnails. The top left thumbnail displays an image from the beginning of the time span and the bottom left thumbnail displays an image from the end of the time span. The number of thumbnails and the intervals between them depend on the size of the Forensic Search window and the thumbnail size that you choose from the Thumbnail Size menu.
8	Show Timestamp	Check this check box to show the date and time displayed at the top of each thumbnail.
9	Archive end time	End date and time for the entire video archive.
10	Skip forward	Skip forward by the Duration time increment.
11	Timestamp	Displays the date and time for each thumbnail. Select the Show Timestamp check box to turn timestamps on or off.
12	Video thumbnails	Thumbnails are displayed for the time span that is selected in the Duration drop-down menu. Use the Thumbnail Size menu to display larger or smaller thumbnails.
13	Actions Menu	Right click a thumbnail to select an option from the Actions menu (see #17).
14	Display length	The duration of the displayed thumbnails.
15	Camera tabs	A tab is displayed for each selected camera. Click the Recordings menu to select an available camera stream or recording.
16	Archive Player tab	An Archive Player tab plays video when you select a thumbnail and select Actions > Play (or right-click a thumbnail and click Play).

17	Menu Selections	<p>Thumbnail Size—select a smaller size to display more thumbnails for the displayed video duration. Select a larger size to display fewer thumbnails.</p> <p>Recordings—select a video stream or recording.</p> <p>Actions—choose one of the following options:</p> <p>Note You can also right-click a thumbnail to access the Actions (see #13).</p> <ul style="list-style-type: none"> • Set Start—Sets the selected thumbnail as the first thumbnail in the range. (Tip: to select a specific date and time as the start time, use the menu at that appears beneath the thumbnails as described in #4 “Thumbnail Start Time”). • Play —Plays the video from the selected thumbnail in an <i>Archive Player</i> tab. <ul style="list-style-type: none"> – You can also double-click a thumbnail to play video. – Playback begins from the start timestamp. If a start timestamp is not available, the next available frame is displayed. • Zoom To—Set the beginning and ending thumbnail for the display. Shift-click or Ctrl-click to select multiple thumbnails and choose Zoom To from the Actions menu. The first frame in the selected thumbnails becomes the new start time. The last frame in the selected thumbnails becomes the new end time. • Zoom In—Decreases the displayed thumbnail duration to the next available duration value. If no frames are selected, the start time does not change. If one frame is selected, that frame becomes the start time. If more than one frame is selected the frame closest to the beginning of the archive becomes the start time. Zoom in is not available when the minimum duration is set. • Zoom Out—Increases the duration of the displayed thumbnail duration to the next available duration value. The start time remains the same. For example, if the Duration is 3 hours, choose the Zoom Out option to increase the Duration to approximately 6 hours. If the start time plus the duration would exceed the length of the archive, the start time will be adjusted to the archive’s end time minus the duration. Zoom out is not available when the maximum duration is set.
----	--------------------	---

Using Thumbnail Search

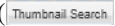
Summary Steps

To view a thumbnail summary of a camera’s recordings:

1. Select **Monitor** and click **Thumbnail Search** (Thumbnail Search) to open the forensic search tool in a separate window (Figure 2-17).
2. Select a location and double-click a camera name.
3. Use the tools described in Figure 2-17 to locate specific video.
4. Select a different stream from the **Recordings** menu.
5. Double-click a thumbnail to play the video. You can also select a thumbnail and select **Play** from the **Actions** menu.
6. See the “Detailed Procedure” for more information.

Detailed Procedure

Step 1 Click **Monitor**.


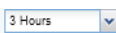


Step 2 Click **Thumbnail Search** () to open the forensic search window ([Figure 2-17](#)).

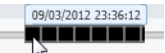
Step 3 Select a location and double-click a camera name.

The camera name appears as a tab at the top of the thumbnail display. You can select multiple cameras to open multiple tabs.

Step 4 Use the controls described in [Figure 2-17](#) to refine the search.

For example:

- To change the first thumbnail in the display, select a date and time from the menu below the thumbnails () and click **Set Start**. The thumbnail for the selected date and time is displayed in the top left corner (you can also right-click a thumbnail and choose **Set Start**).
- Choose the **Duration** () of the thumbnail display. For example, choose **1 Hour** to display thumbnails for a single hour. The default is **Entire Archive**.
- Click the skip icons to skip back  or forward  by the *Duration* time. For example, if the *Duration* is 1 hour, click the skip buttons to skip forward or back by 1 hour.

- Click and drag the slider  to a new start time.
 - The slider date and time appears when the slider is selected.
 - Release the mouse button to refresh the thumbnail display with the time displayed above the slider.



Note

The slider length represents the thumbnail duration relative to the entire length of the archive. The gray time line equals 100 percent of the archive. The black slider covers the entire time line if the selected Duration is Entire Archive (default).

- Choose a **Thumbnail Size** to enlarge or reduce the size of each thumbnail. Larger sizes display fewer thumbnails, and each thumbnail represents a greater time span.

Step 5 (Optional) Further refine your search by choosing one or more thumbnails and choosing one of the following options in the **Actions** menu.



Tip

You can also right-click a thumbnail to access the **Actions**.

- **Set Start**—Sets the selected thumbnail as the first thumbnail in the range (you can also select a specific date and time using the Set Start menu below the thumbnail display).
- **Play** —Plays the selected thumbnail video in an *Archive Player* tab.
 - You can also double-click a thumbnail to play video.
 - Playback begins from the start timestamp. If a start timestamp is not available, the next available frame is displayed.

- **Zoom To**—Set the beginning and ending thumbnail for the display. Shift-click or Ctrl-click to select multiple thumbnails and choose **Zoom To** from the **Actions** menu. The first frame in the selected thumbnails becomes the new start time. The last frame in the selected thumbnails becomes the new end time.
- **Zoom In**—Decreases the displayed thumbnail duration to the next available duration value. If no frames are selected, the start time does not change. If one frame is selected, that frame becomes the start time. If more than one frame is selected the frame closest to the beginning of the archive becomes the start time. Zoom in is not available when the minimum duration is set.
- **Zoom Out**—Increases the duration of the displayed thumbnail duration to the next available duration value. The start time remains the same. For example, if the Duration is 3 hours, choose the Zoom Out option to increase the Duration to approximately 6 hours.

If the start time plus the duration would exceed the length of the archive, the start time is set to the end of the archive minus the duration.

Zoom out is not available when the maximum duration is set.



CHAPTER 3

Configuring Video Viewing Options

Refer to the following topics to configure the viewing options that can be accessed using the Cisco Video Surveillance Safety and Security Desktop application, the Cisco VSM Operations Manager, or other supported video viewing applications.



Tip

For instructions to view video using the Cisco Safety and Security desktop application, see the [Cisco Video Surveillance Safety and Security Desktop User Guide](#).

Contents

- [Creating Pre-Defined Views, page 3-2](#)
- [Setting the Default View, page 3-8](#)
- [Configuring Video Walls, page 3-10](#)
- [Enabling Record Now, page 3-12](#)

Additional Documentation

- [Configuring Camera PTZ Controls, Presets, and Tours, page 8-65](#)
- [Configuring Motion Detection, page 8-77](#)
- [Editing the Camera Settings, page 8-42](#)
- [Adding and Editing Camera Templates, page 10-1](#)

Creating Pre-Defined Views

Use Operations Manager to create *Views* that can be displayed in either Operations Manager or the Cisco Safety and Security desktop application. You can create *Views* in one of the following ways:

- [Saving a Basic View, page 3-2](#)—Quickly create and save a View with up to four video panes using the **Monitor Video** page.
- [Creating Rotating Views, page 3-4](#)—Create *Views* with more than four video panes. View can include static panes that always display video from a specific camera, or rotating panes that rotate the video from multiple camera sources. For example, a View might include 3 video panes that rotates the video from 8 cameras to provide a virtual tour of a building, and a static pane that always displays video from a specified camera.

Saving a Basic View

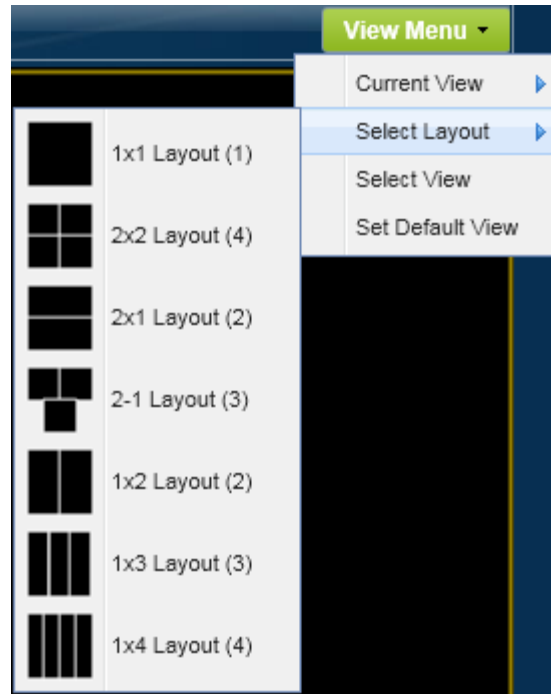
You can create a basic *View* by saving a layout in the **Monitor Video** page. The panes in a basic *View* are static and do not rotate. Views can be accessed using either Operations Manager or the Cisco Safety and Security desktop application.

**Tip**

Operations Manager can display *Views* with up to four video panes. To create *Views* with more than four panes for use by the Safety and Security desktop application, see the [“Creating Rotating Views” section on page 3-4](#).

Procedure

- Step 1** Log on to the Operations Manager.
You must belong to a User Group with permissions for *Views*.
- Step 2** Click **Monitor Video**.
- Step 3** Click **View Menu > Select Layout**.
- Step 4** Select a blank *Layout* from the list.
- Step 5** Drag and drop cameras from the camera list in the left column to the available video panes.
- Step 6** Save the layout as a new View.
 - a. Choose **Current View > Save As** from the **View Menu** ([Figure 3-1](#)).

Figure 3-1 Video Layouts

- b. Enter a name and *Access Location*.
 - Views can be assigned to the same location as the cameras, or to a higher level location.
 - Only users assigned to a user group with this location can access the View.
- c. Click **Save**.

Step 7 Verify that the new View appears under **View Menu > Select View**.

Creating Rotating Views

The **Views** feature allows you to create *Views* with up to 16 video panes (Figure 3-2). The panes in a View can be static (always display the video from a single camera, or rotate video from multiple cameras). For example, you can create a virtual tour of all *Lobby Doors* that rotates the video from 8 cameras between 3 panes while a 4th *static* pane always shows the rear door.

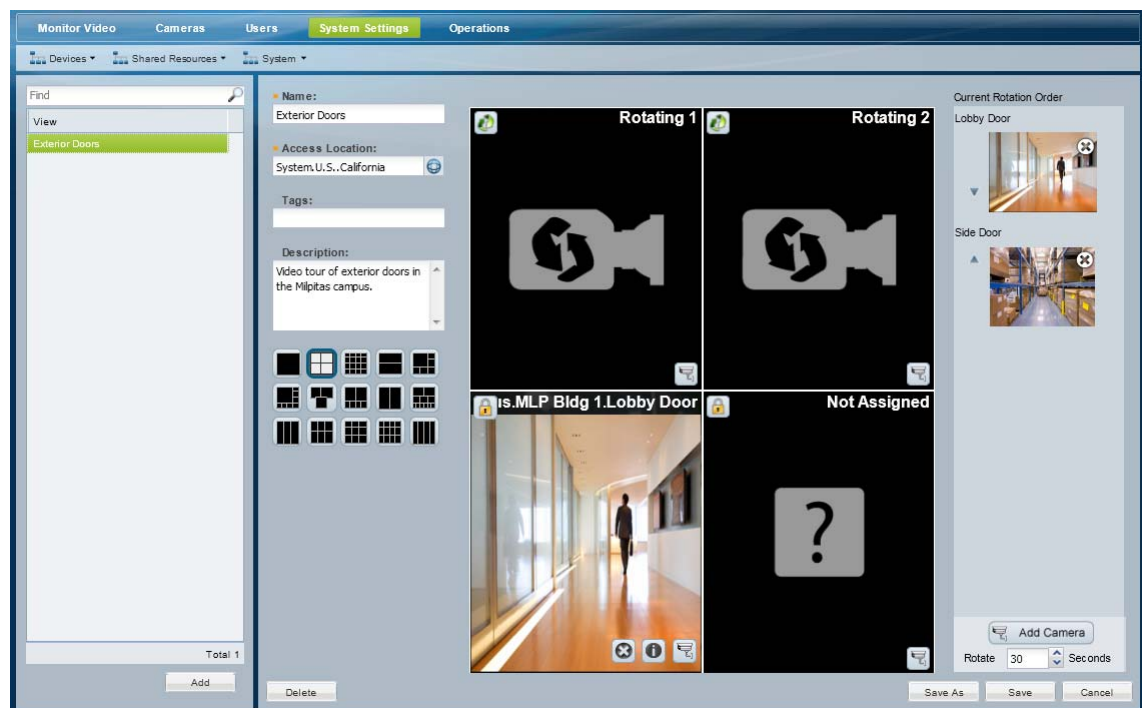
The *Current Rotation Order* defines which camera is displayed first, second, etc.







Note

Views with more than four video panes can be displayed using the Cisco Safety and Security desktop application (Operations Manager can only display Views with four or less panes).

Figure 3-2 View Configuration



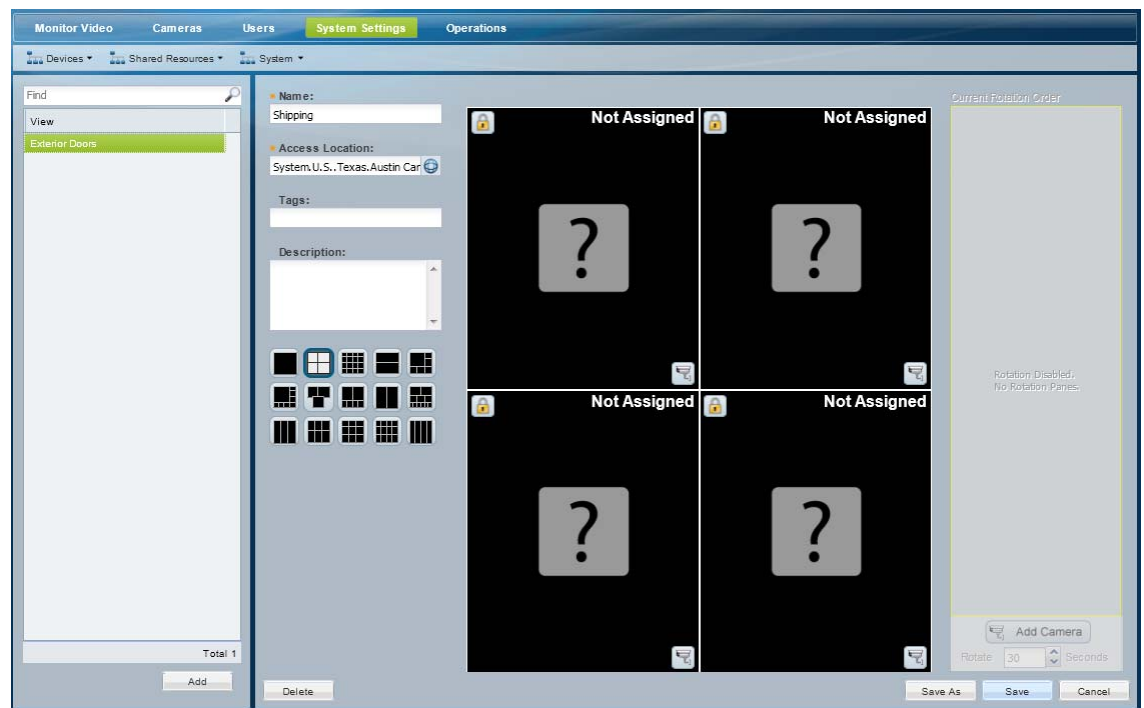
-  —Static camera panes always display video from the same camera, even if the other panes rotate video from multiple cameras.
 - Click the camera  icon to select the camera source.
 - Not Assigned* panes do not have a camera assigned to the pane. The video pane will appear blank in the View.
-  —Rotating camera panes rotate the video between cameras included in the *Current Rotation Order*.
 - Click **Add Camera** () to add the cameras that will rotate between the available panes.
 - Use the arrows in the *Current Rotation Order* to change the order of the rotation.

Procedure


To create Views that include static and/or rotating panes, do the following.

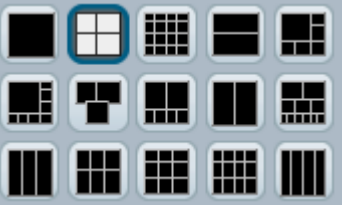
- Step 1** Log on to the Operations Manager.
 - You must belong to a User Group with permissions for *Views*.
- Step 2** Click **System Settings** and then **Views**.
- Step 3** Edit or add a *View* (Figure 3-3):
 - To edit a View, select an existing entry.
 - To add a View, click the **Add** button.

Figure 3-3 Defining the Camera View



- Step 4** Enter the basic View properties (Figure 3-3):

Setting	Description
Name	(Required) enter a descriptive name for the View. For example: <i>Exterior Doors</i> .
Access Location	(Required) click the  icon and select a location. Only users assigned to a user group with this location can access the View. Note The cameras included in a View must be at the same View <i>access location</i> , or a sub-location. For example, a View assigned to a Texas location cannot include cameras from a California location. See the “Understanding Permission-Based and Partition-Based Resources” section on page 5-3 for more information.
Tags	(Optional) Words that assist in a <i>Find</i> .

Setting	Description
Description	(Optional) enter a meaningful description for the View. For example: <i>Lobby Tour</i> .
Layout	(Required) select a layout grid that includes the required number of video panes. 

Step 5 Define the *static* panes.



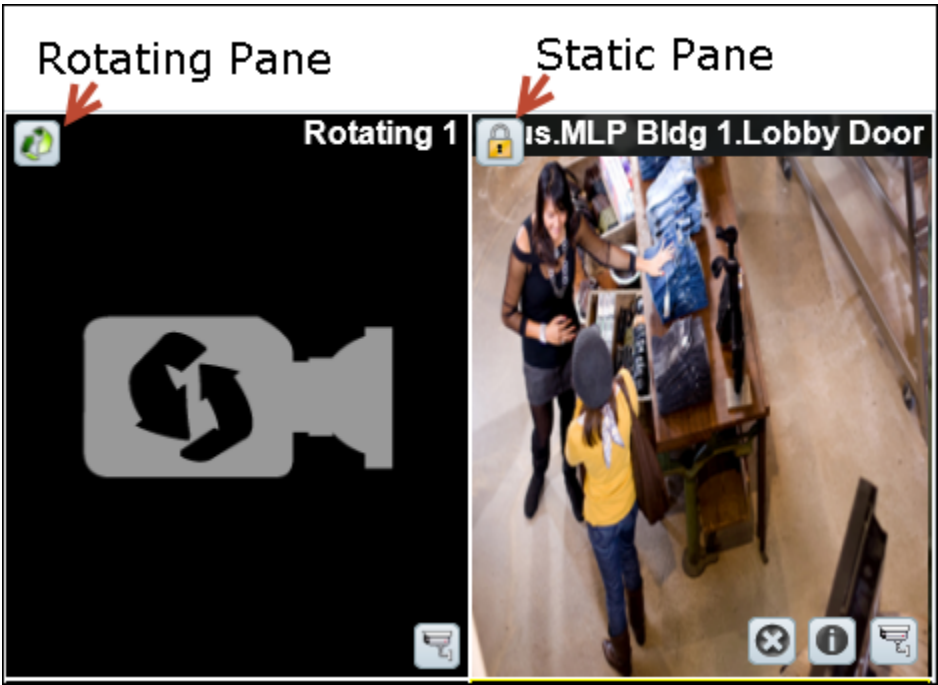






Static camera panes  always display video from the same camera, even if the other panes rotate video from multiple cameras. Static panes display the lock  icon (Figure 3-4).

Figure 3-4 Select the Static Cameras



- Click the  icon to toggle the pane to static , if necessary (Figure 3-4).
- Click the camera  icon.
- Select a camera from the location tree and click **Set**.
- Repeat these steps for each additional static video pane.

**Tip**

Roll over the pane to display additional icons (Figure 3-4). Click  to clear the camera selection (the pane changes to *Not Assigned* and the video pane will appear blank). Click  for camera information. Click  to select a different camera.

Step 6 (Optional) Define the rotating panes and *Rotation Order* (Figure 3-5).


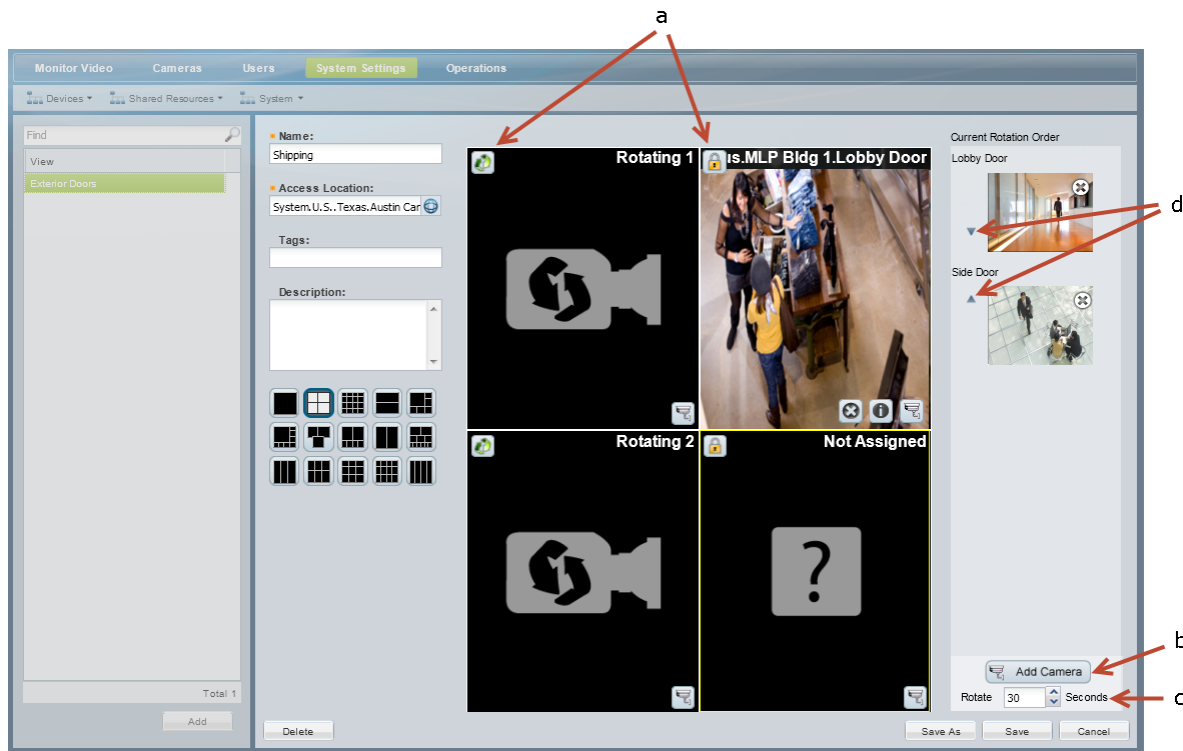






Rotating panes  rotate the video between cameras included in the *Current Rotation Order*. Cameras rotate clockwise: left to right and then top to bottom. For example, when the View is first displayed, the first camera in the *Current Rotation Order* is displayed in the *Rotating 1* pane, the second camera is displayed in the *Rotating 2* pane, etc. The camera set is displayed until the number of Rotate seconds is exceeded. The next set of cameras are then displayed in Rotating 1 and Rotating 2 in the Current Rotation Order, etc.

Figure 3-5 Defining the Camera Rotation



- a. Define the panes that will rotate the cameras included in the *Current Rotation Order*.
 - Panes with the  icon are included in the rotation.
 - Click the lock icon  to toggle the pane to rotation , if necessary.
- b. Add cameras to the *Current Rotation Order*.
 - Click **Add Camera** ().
 - Select a camera from the location tree.
 - Click **Set**.
 - Add additional cameras to the *Current Rotation Order*. For example, you could add six cameras that rotate between two rotating  panes.

**Tip**

Click  to remove a camera from the *Current Rotation Order*.

- c. Select the *Rotate* seconds (the number of seconds the View is displayed between rotations).
The View will pause on a set of cameras before rotating to the next camera in the list.
- d. Reorder the cameras in the *Current Rotation Order* using the up ▲ and down ▼ arrows.
When the View is first displayed, the first camera in the *Current Rotation Order* is displayed in the *Rotating 1* pane, the second camera is displayed in the *Rotating 2* pane, etc.

Step 7 Click **Save**.

Setting the Default View

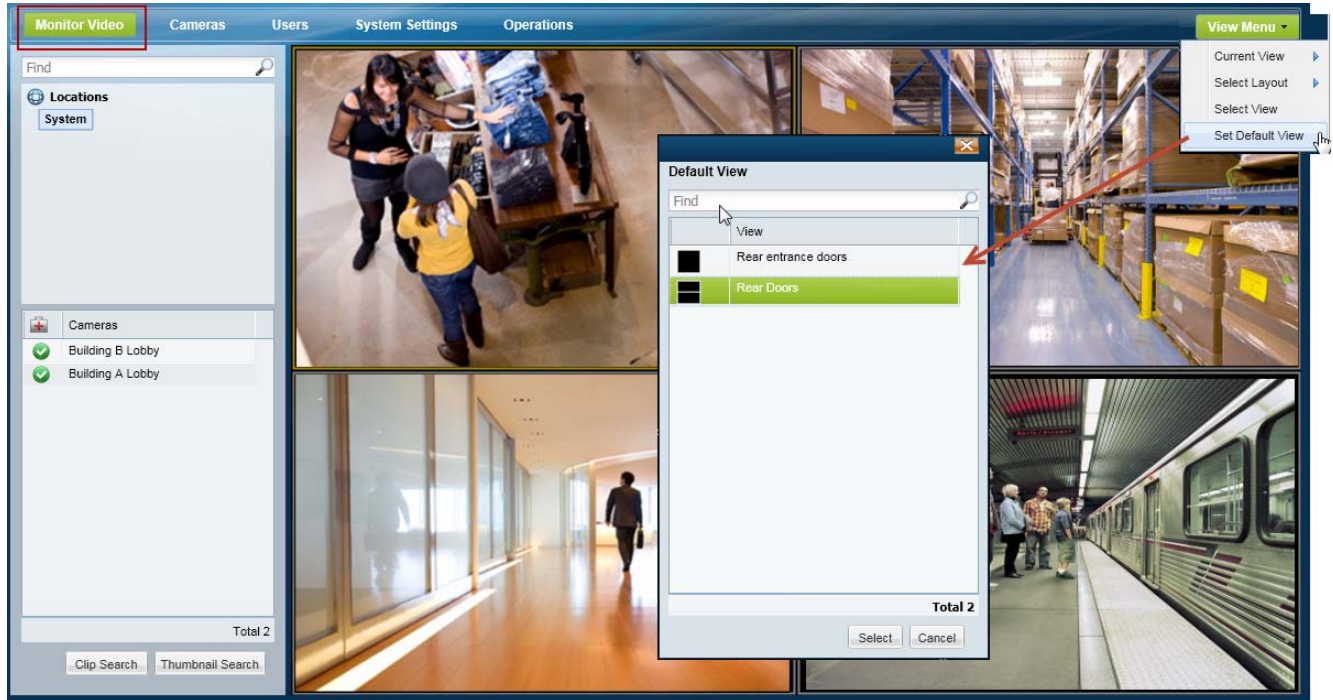
The Default View is defined by each user and is automatically loaded when they click **Monitor Video**.

Usage Notes

- If a default View is not defined, a blank 1x1 layout is displayed.
- Click **Clear** to delete the Default View setting. A blank 1x1 layout will be displayed by default.
- Only Views the user has access permissions to see can be selected as the default View.
- The Default View is saved as a cookie in the browser and is unique to each user/PC. The Default View is not displayed if using a different workstation.
- The Default View is different for each Windows user on the same workstation (the Default View set by one user will not be seen by other Windows users on that workstation).
- If the browser cookies are deleted, the Default View is deleted for all users of that browser.
- If a shared Windows login and browser are used, users may overwrite the default View (and cookie) set by another user using the same Windows account.

Procedure

- Step 1** Create one or more Views as described in the [“Creating Pre-Defined Views”](#) section on page 3-2.
- Step 2** Select **View Menu > Set Default View** ([Figure 3-6](#)).
- Step 3** To select a View from the pop-up window and click **Select**.

Figure 3-6 **Setting the Default View**

Configuring Video Walls

Video Walls are unattended screens that display a pre-defined set of video panes. Video Walls are typically monitored by a security guard or other attendant.

Use the following procedure to create Video Walls and define the default View.

**Tip**

- Refer to the [Cisco Video Surveillance Safety and Security Desktop User Guide](#) for instructions to display the Video Walls.
- To automatically display video from a different camera when an event occurs, see the [“Using Advanced Events to Trigger Actions” section on page 10-11](#). This feature allows to you switch all instances of a Video Wall to the live or recorded video from a camera that triggers an event. For example, if motion occurs or a door is opened, the Video Wall can automatically switch to the video from the camera that triggered the event.
- This feature is similar to the Virtual Matrix client available in Cisco VSM release 6.x.

Procedure

Complete the following procedure to create or edit Video Walls.

**Note**

Any changes to existing Video Walls will be automatically published to all instances of that Video Wall. For example, if you change the default View, all workstations viewing that Video Wall will automatically change to the new View.

- Step 1** Log on to the Operations Manager.
- You must belong to a User Group with permissions for *Video Walls*.
- Step 2** Create one or more Views.
- See the [“Selecting a Multi-Pane “View”” section on page 2-4](#).
- Step 3** Choose **System Settings > Video Wall**.
- Step 4** Click **Add** or select an existing entry.
- Step 5** Complete the following settings:

Setting	Description
Name	The name selected by users.
Access Location	<p>SASD users can view Video Wall that are assigned to the same location or lower.</p> <p>For example, if a user is assigned to a user group with the location “California”, they can access Video Walls assigned to that location, or a sub-location. The user cannot access Video Walls assigned to higher-level locations.</p> <p>See the “Creating the Location Hierarchy” section on page 5-1 for more information.</p>

Setting	Description
Default View	<p>(Optional) The <i>View</i> displayed when a Video Wall is selected in the SASD application.</p> <ul style="list-style-type: none"> If a SASD user chooses a different View and clicks Publish to Wall, then all other instances of that Video Wall will display the new View until the <i>rollback time</i> expires (see below). All displays will then revert back to the default View. The Publish to Wall feature is enabled for user groups with the <i>Push Video to Wall</i> permission. <p>Tip Select the No Default View option to disable the rollback time and display any selected View. A blank screen is displayed when the Video Wall is first selected, and any Views published to that wall (including video from Advanced Events) are displayed until a new View is selected.</p> <p>Refer to the Cisco Video Surveillance Safety and Security Desktop User Guide for more information.</p>
Rollback Time	The amount of time that an alternative <i>View</i> can be displayed on a Video Wall before the default View is restored.

Step 6 Click **Add** or **Save**.

Step 7 (Optional) Configure **Advanced Events** to use **Push to Video Wall** when an event occurs.

- This feature automatically switches all instances of a Video Wall to the live or recorded video from a camera that triggers an event. See the [“Using Advanced Events to Trigger Actions”](#) section on page 10-11.

Step 8 Access the Video Walls using the Cisco SASD application:

- Launch the SASD application and log in.
- Select a Video Wall from the **Wall** menu.
- (Optional) Select a **View** and click **Publish to Wall**.
 - The new View will appear on all other windows that display the same Video Wall. When the rollback time expires, the default Video Wall view is restored (if configured).
 - The **Publish to Wall** feature is enabled for user groups with the *Push Video to Wall* permission.

Enabling Record Now

Record Now allows users to trigger an immediate recording that is performed in addition to any other scheduled, continuous or event recordings. These recordings are retained on the system for the number of days specified in the camera's *Retain event recordings* setting.

HA Availability for Record Now

The Record Now feature is available on the Primary server, or on the Failover server if the Primary is down. The Record Now feature is not available on Redundant servers.

See the [“High Availability” section on page 12-1](#) for more information.

Using Record Now



See the [“Using Record Now” section on page 2-24](#) for end-user instructions to trigger recordings.

Summary Steps to Enable Record Now

To enable the Record Now option, you must define the following:

- Add the users to a User Group with Operate permissions to **View Live Video** and **View Recordings**.
- In the camera template, enable the **Record Now** option and define the number of retention days. Assign the camera(s) that should allow Record Now to that template.
- Define the **Record Now Duration** in system settings.

Procedure to Enable Record Now

-
- Step 1** Add user access permissions to view live and recorded video.
- a. Select **Users**.
 - b. Select the **Roles** tab .
 - c. Edit or add a *Role*:
 - To edit a Role, click an existing entry to highlight it.
 - To add a Role, click the **Add** button.
 - d. Select the Operate permissions to **View Live Video** and **View Recordings**.
 - e. Click **Save**.
 - f. Select the **User Groups** tab .
 - g. Select the Role that includes the view permissions.
 - h. Add the users to the role.
 - i. Click **Save**.
 - See the [“Adding Users, User Groups, and Permissions” section on page 4-1](#) for more information.
- Step 2** Enable the *Record Now* option in the camera template.
- a. Click **Cameras**.
 - b. Click **Templates**.
 - c. Select a location and template name.
 - d. Click the **Streaming, Recording and Events** tab.

- e. In the *Retain event recordings* setting, enter the number of days the recordings (and other event video) should be retained on the system.
- f. Scroll down to Record Now and select **Enable**.
- g. Click **Save**.
- h. Assign cameras to the template, if necessary (click **Cameras**, select a sample, click the **Streaming, Recording and Events** tab, and assign the template to the camera).

For more information, see the [“Adding and Editing Camera Templates”](#) section on page 10-1 and the [“Streaming, Recording and Event Settings”](#) section on page 8-49.

Step 3 Define the duration of all Record Now recordings.

- a. Choose **Settings > System Settings**.
- b. Select the **General** tab.
- c. In the *Record Now Duration* field, enter the number of seconds that video will be recorded for all Record Now requests.

The minimum value (and default) is 300 seconds (5 minutes).

- d. Click **Save**.
-



CHAPTER 4

Adding Users, User Groups, and Permissions

Refer to the following topics to create user accounts and define the features and functions that can be accessed by those users. Access permissions include operator permissions and manage (configuration) permissions.

You can also provide access to users that are managed on an external (LDAP) server

Contents

- [Overview, page 4-1](#)
- [Defining User Roles, page 4-8](#)
- [Adding User Groups, page 4-10](#)
- [Adding Users, page 4-13](#)
- [Adding Users from an LDAP Server, page 4-15](#)

Overview

Cisco Video Surveillance Manager (Cisco VSM) users can monitor video or configure the system based on the following:

- The user group(s) to which the user is assigned: user groups are associated with a user Role, which defines the access permissions for the group.
- The location assigned to the user group(s).
- Users can be assigned to multiple user groups, and gain the combined access permissions for all groups.

Before you begin, create the location hierarchy as described in the [“Creating the Location Hierarchy” section on page 5-1](#). Carefully review the [“Examples: Locations in Simple vs. Large Deployments” section on page 5-7](#).



Tip

User accounts provide access to both the browser-based Operations Manager and the Cisco Safety and Security desktop application.

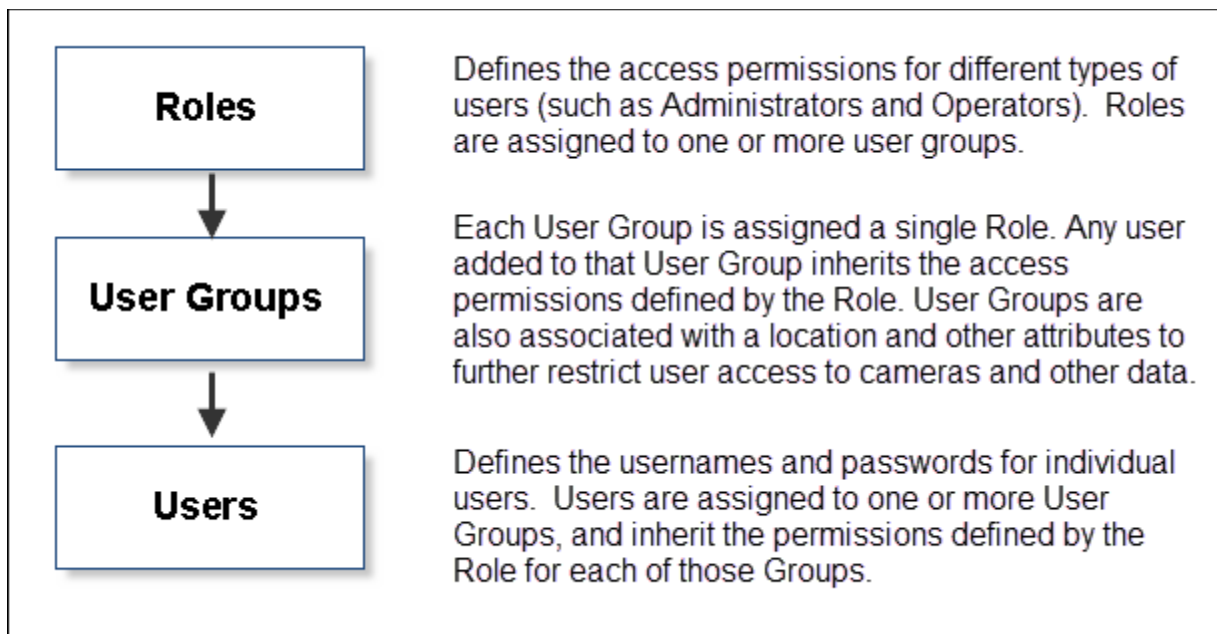
Review the following topics to understand how to configure users and user access permissions in Cisco VSM.

- [Understanding Roles, Groups and Users, page 4-2](#)
- [Understanding the System-Defined User Roles, Groups and Accounts, page 4-3](#)
- [Understanding Permissions, page 4-4](#)
- [Example Roles For Different Types of Users, page 4-7](#)

Understanding Roles, Groups and Users

Figure 4-1 summarizes the user Roles, groups and user accounts.

Figure 4-1 Users, User Groups, and Roles



Roles define the access permissions for different types of users. For example, create an *operator* Role that allows users to view live and recorded video, and an *administrator* Role that allows users to configure cameras and add new users.

When the Roles are assigned to a user group, any user added to that group will inherit the Role permissions. Users also gain access to different types of resources based on the user group location.

For example, create an *Operator* Role that allows users to view video, but does not allow configuration of cameras or other system resources. When you add that Role to a user group, any user added to the group will inherit the Role permissions. In addition, users can access the devices at the group location (including sub-locations), and the templates, schedules and other resources for any location in the same location tree.







Tip

See the [“Examples: Locations in Simple vs. Large Deployments”](#) section on page 5-7 for more information on user access based on a group’s location.


Understanding the System-Defined User Roles, Groups and Accounts

By default, Cisco VSM includes system-defined Roles, groups and users to aid in the initial configuration (see [Table 4-1](#)). System-defined Roles, groups and users cannot be updated or deleted.

Table 4-1 System-Defined User Roles, Groups and Accounts

Default		Description
Roles		<ul style="list-style-type: none"> <i>super_admin_role</i>—includes all management and operation access permissions. <i>local_admin_role</i>—provides all operator functions, but limited and commonly used management tasks such as managing cameras, Media Servers, encoders, Video Walls, locations & maps, views and alerts. <i>operator_role</i>—provides all operator permissions.
User Groups		<ul style="list-style-type: none"> <i>super_admins</i>—assigned the <i>super_admin_role</i>. <i>operators</i>—assigned the <i>operator_role</i>.
Users		<ul style="list-style-type: none"> <i>admin</i>—assigned to the <i>super_admins</i> user group, which gives the user <i>super_admin_role</i> permissions. The admin is a root system user and cannot be modified or deleted. The default admin username and password is admin/admin. <p>Note A <i>super-user</i> is anybody that has all permissions at the root location.</p> <ul style="list-style-type: none"> <i>operator</i>—assigned to the <i>operators</i> user group, which gives the user <i>operator_role</i> permissions. The default username and password is operator/operator. <p>Note A <i>local-admin</i> user account is not included by default. You must add a user and add them to a user group associated with the <i>local_admin_role</i>, if necessary.</p>
LDAP Users		Members of an external Lightweight Directory Access Protocol (LDAP) Active Directory user database can be granted access to Cisco VSM. See the “Adding Users from an LDAP Server” section on page 4-15 for more information.

Understanding Permissions

User *Roles* define the permissions for different types of users. Click the **Roles** tab  to view or modify the permissions assigned to a Role ([Figure 4-2](#)). Permissions are divided into two categories: *Manage* and *Operate*. Select or de-select the check boxes to add or remove permissions.

Default Roles

The default Roles are read-only and cannot be revised or deleted. For example:

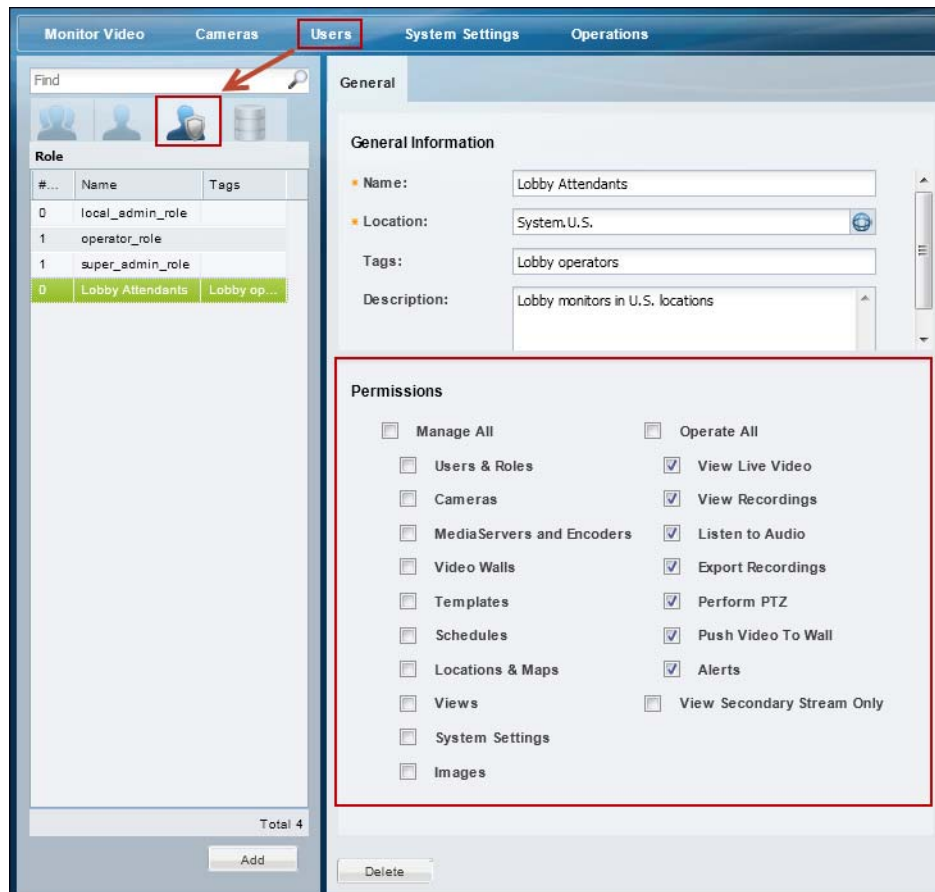
- *operator_role*—Includes most Operator permissions.
- *super_admin_role*—Includes all operate and manage permissions (a *super-admin* is any user that has access to all permissions).
- *local_admin_role*—Includes a combination of operate and manage permissions.



Tip

Select a Role to view the permissions assigned to that Role. See [Table 4-2](#) and [Table 4-3](#) for descriptions of the Operate and Manage roles. See the “[Defining User Roles](#)” section on [page 4-8](#) to create or revise Roles.

Figure 4-2 Permissions



**Note**

- Selecting a permission may automatically result in the selection of other dependent permissions if the permissions overlap. For example, if you select the *Manage Cameras* permission, the *View Live Video* and *Perform PTZ* permissions are automatically selected. The automatically selected dependent permission(s) cannot be deselected unless the parent permission is deselected first.
- See the “[Defining User Roles](#)” section on page 4-8 for detailed instructions.

Table 4-2 summarizes the *Manage* permissions:

**Tip**

Click **Manage All** to select all of the permissions.

Table 4-2 **Manage Permissions**

Manage Permission	Description	More Information
Users & Roles	Create, update, or delete user accounts, groups and Roles.	Adding Users, User Groups, and Permissions, page 4-1
Cameras	Create, delete, or update Cisco VSM cameras. Includes access to camera discovery, auto-configuration and the <i>Pending Approval</i> functions.	Adding and Managing Cameras, page 8-1
Servers & Encoders	Create, update, or delete Cisco VSM servers and analog camera encoders.	Configuring Media Server Services, page 7-1 Adding Encoders and Analog Cameras, page 11-1
Video Walls	Create, update, or delete Video Walls.	Configuring Video Walls, page 3-10
Templates	Create, update, or delete camera templates.	Adding and Editing Camera Templates, page 10-1
Schedules	Create, update, or delete schedules.	Defining Schedules, page 9-1
Locations & Maps	Create, update, or delete Cisco VSM locations and associated map images.	Creating the Location Hierarchy, page 5-1
Views	Create, update, or delete pre-set video views used to monitor multiple video cameras.	Creating Pre-Defined Views, page 3-2 Selecting a Multi-Pane “View”, page 2-4
System Settings	Update Cisco VSM system settings.	Revising the System Settings, page 14-1
Images	Allows the user to upload firmware images, define the recommended firmware version, and upgrade devices.	Upgrading Cisco Camera and Encoder Firmware, page 15-3

Table 4-3 summarizes the *Operate* permissions:

**Note**

Some permissions are mutually exclusive. For example, you can select either *View Live Video* or *View Secondary Stream Only* but not both at the same time. If you select *View Secondary Stream*, the mutually exclusive permission will be automatically deselected.

**Tip**

Click **Operate All** to select all of the permissions, except *View Secondary Stream Only*.

Table 4-3 **Operate Permissions**

Operation Permissions	Description	More Information
View Live Video	View live video streams from Cisco VSM cameras. Note If selected, View Secondary Stream Only will be automatically deselected.	Viewing Live Video, page 2-9
View Recordings	View recorded video from Cisco VSM cameras.	Viewing Recorded Video, page 2-12
Listen To Audio	Play live or recorded audio from cameras that support audio.	Editing the Camera Settings, page 8-42
Export Recordings	Export a video clip to a file.	Creating, Viewing and Managing Video Clips, page 2-17
Perform PTZ	Use the pan, tilt and zoom controls on cameras that support PTZ.	Using Pan, Tilt, and Zoom (PTZ) Controls, page 2-32
Push Video to Wall	Enables the Publish to Wall feature in the Cisco Safety and Security Desktop (SASD) application. This feature allows users to change the view shown by all other instances of a selected video wall. The new view is displayed until the dwell time is exceeded. Note If selected, View Secondary Stream Only will be automatically deselected.	Configuring Video Walls, page 3-10 Cisco Video Surveillance Safety and Security Desktop User Guide
Alerts	Allows all operators to view the alerts for cameras they can access. Users can acknowledge, clear, or comment on an alert (<i>ack/clear/add_user_comment</i>).	Cisco Video Surveillance Safety and Security Desktop User Guide
View Secondary Stream Only	Members of user groups with this permission can only view the secondary stream of cameras. If the secondary stream is not available, no video feed is shown. Note If selected, View Live Video and Push Video to Wall will be automatically deselected.	Editing the Camera Settings, page 8-42

Example Roles For Different Types of Users

Table 4-4 describes sample Roles and associated permissions.

Table 4-4 ***Sample Roles in a Cisco Video Surveillance Deployment***

Role	Permission
Guard	View Live Video View Recordings Listen to Audio Export Recordings Perform PTZ
Area Admin	View Live Video View Recordings Export Recordings Perform PTZ Manage Cameras Manage Servers and Encoders
Admin	View Live Video View Recordings Export Recordings Perform PTZ Manage Users & Roles Manage Cameras Manage Servers and Encoders Manage Templates Manage Schedules Manage Location and Maps Manage System Settings

Defining User Roles

User Roles define the functions and features available to members of a user group. For example, you can create a Role for *Operators* who only monitor video, and another Role for *Administrators* who also configure the cameras, schedules, users, or other features of the Cisco VSM deployment.

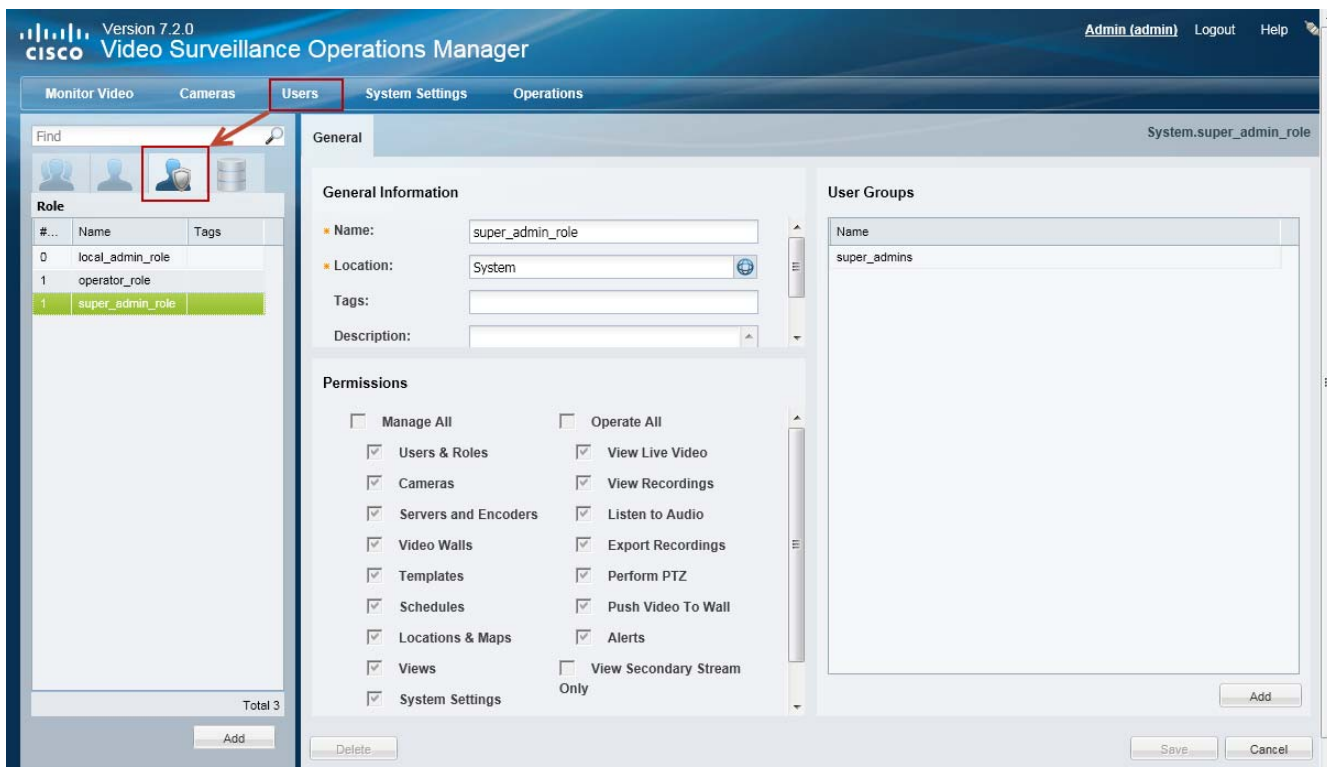


Tip

See [Understanding Permissions, page 4-4](#) for more information.


Once created, Roles are assigned to one or more user groups. Users gain the access permissions of the user groups Role.

Figure 4-3 Creating or Revising User Roles



Procedure

To create user Roles, do the following:

- Step 1** Log on to the Operations Manager.
 - See the [“Logging In” section on page 1-18](#).
 - You must belong to a User Group with permissions to manage *Users & Roles*.
- Step 2** Select **Users**.
- Step 3** Select the **Roles** tab .
- Step 4** Edit or add a *Role*:
 - To edit a Role, click an existing entry to highlight it.

- To add a Role, click the **Add** button.

Step 5 Enter the basic settings:

Table 4-5 **Role Settings**

Setting	Description
Name	(Required) Enter a meaningful name.
Location	(Required) Select the location where the Role can be used.
Tags	(Optional) Enter keywords used by the <i>Find</i> function.
Description	(Optional) Enter a description of the permissions granted by the Role.

Step 6 (Required) Select or deselect the Role permissions.

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

Step 7 (Optional) Add one or more user groups to the Role.

- a. Click **Add** under the user groups box.
- b. Select an existing user group.
- c. Click **OK**.

See the [“Adding User Groups” section on page 4-10](#) for more information.

Step 8 Select **Create** or **Save**.

Step 9 (Optional) Add the *Role* to one or more user groups.

See the [“Adding User Groups” section on page 4-10](#) for instructions.

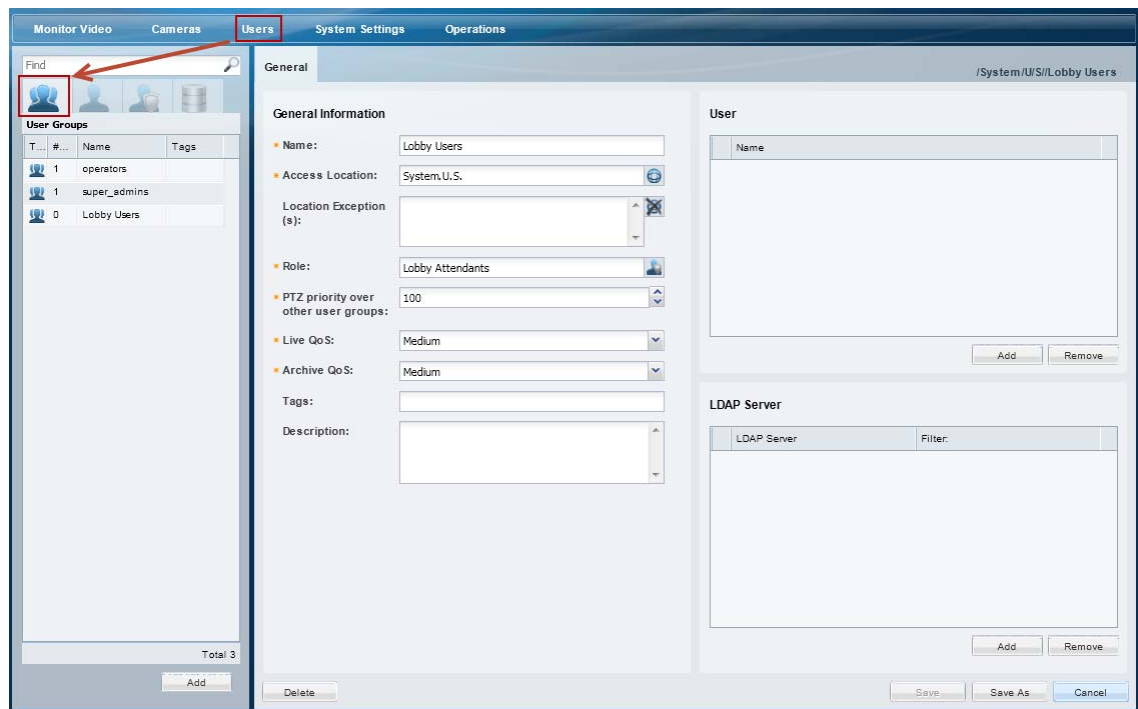
Adding User Groups

User groups allow multiple users to be assigned the same set of access permissions. For example, all lobby attendants can be assigned to a user group *Lobby* and security personnel to an *Administrator* group. Although members of the Lobby group can view live and recorded video, they cannot make configuration changes. Security administrators, however, can manage templates, schedules cameras, users, or other resources. These permissions are defined by the user Role assigned to the user group.

User groups are also associated with a specific location, allowing you to limit access to the Cisco VSM resources in a specific location (such as a campus, building, or floor). See the [“Creating the Location Hierarchy” section on page 5-1](#) for more information.


If a user belongs to more than one user group, the user inherits the combined rights and permissions of all the groups.

Figure 4-4 Creating User Groups



Procedure

To create a user group, do the following:

- Step 1** Select **Users**, and then select the **User Groups** tab .
 - The currently configured user groups are listed in the left column.
- Step 2** Edit or add a user group:
 - To edit a group, click an existing entry to highlight it, and continue to [Step 3](#).
 - To add a group, click the **Add** button.

Step 3 Enter the group settings (see [Table 4-6](#)):

Table 4-6 User Group Settings

Setting	Description
Name	(Required) Enter a meaningful name.
Access Location	(Required) Select the location that the users in this group will have access to. For example, select California to restrict access to equipment and associated video (such as cameras, Media Servers and video streams) that are also assigned to California or a sub-location.
Location Exception(s)	(Optional) Select the locations within the Access Location that users should not be able to access. For example, if you select the Access Location California, and the Location Exception San Francisco, users in the group can access all California locations <i>except</i> San Francisco.
Role	(Required) Select the Role that defines the access permissions for the group. To create or modify the available Roles, see the “Defining User Roles” section on page 4-8.
PTZ priority over other User Groups	<p>(Required) Select a number from 1 to 100 that defines use user group priority (relative to members of other user groups) to use a camera’s pan, tilt and zoom (PTZ) controls. User groups with a higher number have priority over groups with a lower number.</p> <p>For example, assign Operators a priority of 50, and Administrators a priority number 60. Assign security personnel priority 70, and building managers priority 80. See the “Defining the User Group PTZ Priority” section on page 8-69 for more information.</p> <p>The default is 100 (highest priority).</p> <p>Note If two users belong to user groups with the same priority, then the first user to access the PTZ controls gains priority and can continue to use the controls.</p> <p>Note You can also define the idle time that a lower priority user must wait to use the PTZ controls after a higher priority user stops using the controls. See the “PTZ Advanced Settings” section on page 8-76.</p>
Live QoS	<p>(Required) Defines the priority of the user group to receive <i>live</i> video if network traffic is heavy. The video quality is not affected, but user groups with a low QoS setting may have dropped packets so user groups with a higher QoS setting can continue to receive uninterrupted video.</p> <ul style="list-style-type: none"> Low—If network traffic is heavy, video packets may be dropped for users assigned to this group. Medium—the user group has secondary priority to receive video packets over the network. If network traffic is heavy, video packets may be dropped for users assigned to this group. High—the user group has the highest priority to receive video packets over the network.

Table 4-6 **User Group Settings (continued)**

Archive QoS	<p>(Required) Defines the priority of the user group to receive <i>recorded</i> (<i>archive</i>) video if network traffic is heavy. The video quality is not affected, but user groups with a low QoS setting may have dropped packets so user groups with a higher QoS setting can continue to receive uninterrupted video.</p> <ul style="list-style-type: none"> • Low—If network traffic is heavy, video packets may be dropped for users assigned to this group. • Medium—the user group has secondary priority to receive video packets over the network. If network traffic is heavy, video packets may be dropped for users assigned to this group. • High—the user group has the highest priority to receive video packets over the network.
Tags	(Optional) Enter keywords used by the <i>Find</i> function.
Description	(Optional) Enter a description of the rights granted by the Role.

Step 4 Add users who will be granted the group permissions.

- a. Click **Add** under the User box (Figure 4-4).
- b. Select one or more users from the pop-up window.
- c. Select **OK**.



Tip Press *Shift-click* or *Ctrl-click* to select multiple users. To create or modify the list of available users, see the “[Adding Users](#)” section on page 4-13.

Step 5 (Optional) Add an LDAP server filter, if necessary.

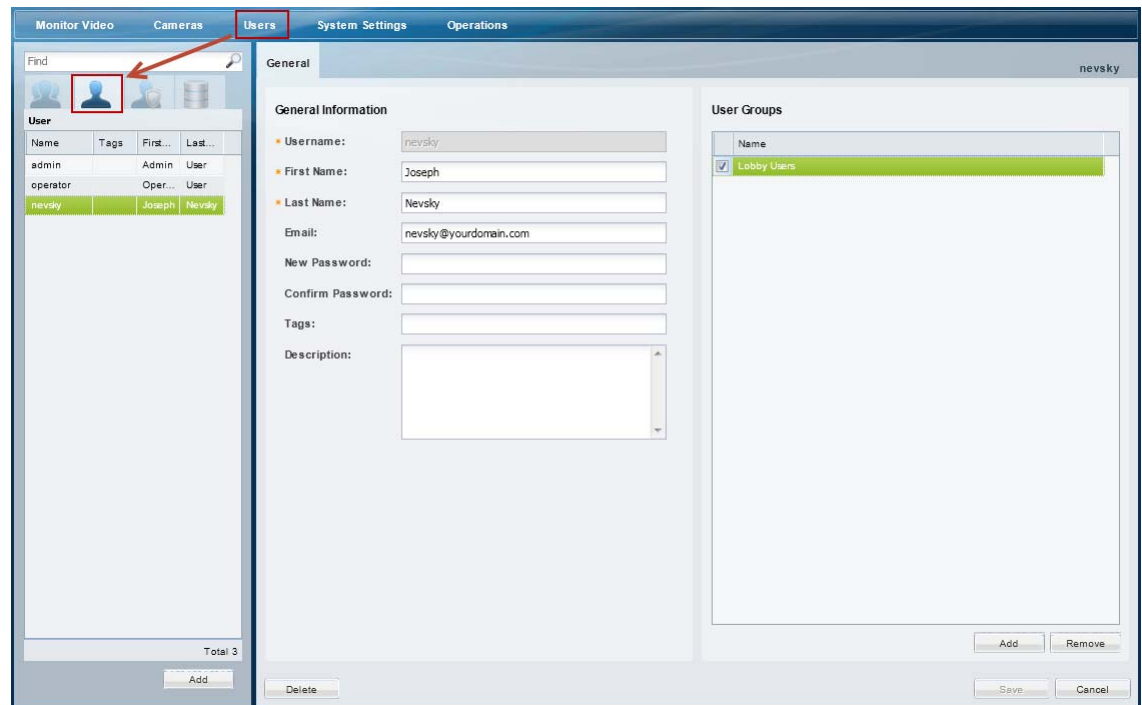
- See the “[Adding Users from an LDAP Server](#)” section on page 4-15.

Step 6 Click **Create** or **Save** to add or edit the user group.

Adding Users

Users provide login access to individuals. Once user accounts are created, you can assign the users to one or more user groups. User groups provide the users with access permissions and limit access to specific locations. See the “[Overview](#)” section on page 4-1 for more information.

Figure 4-5 **Creating Users**



Procedure

To create users, do the following:


- Step 1** Select **Users**, and then select the **User** tab .
 - The currently configured users groups are in the left column.
- Step 2** Edit or add a user:
 - To edit a user, click an existing entry to highlight it, and continue to [Step 3](#).
 - To add a user, click the **Add** button.
- Step 3** Enter the basic user settings ([Table 4-7](#)):

Table 4-7 **User Settings**

Setting	Description
Username	(Required) The username is used to log in to the Operations Manager and Cisco Video Surveillance Safety and Security Desktop.
First Name	(Required) Enter the user's first name.
Last Name	(Required) Enter the user's last name

Table 4-7 **User Settings (continued)**

Email	(Optional) Enter an email address for the user. The email address is for informational purposes only.
Password	(Required) Enter the initial password for the user. <ul style="list-style-type: none"> • The password must include 8 characters including one uppercase character and one digit. • The user is prompted to change the password the first time they log in. • If the user forgets their password, an administrator can change the password, which will again require the user to enter a new password on first login.
Confirm Password	Re-enter the password.
Tags	(Optional) Enter the keywords used by the <i>Find</i> feature.
Description	(Optional) Enter a description for the user.

Step 4 (Optional) Add the user to one or more user groups.

- a. Click **Add** under the User Groups box.
- b. Select one or more user groups from the pop-up window.
- c. Select **OK**.



Tip See the [“Adding User Groups” section on page 4-10](#) for instructions to add or edit groups.

Step 5 Select **Create** or **Save** to save the changes.

Adding Users from an LDAP Server

Add an LDAP (Lightweight Directory Access Protocol) server to the Cisco VSM user configuration to provide access to members of an external user database. After the LDAP server is added, users from that system can log in to Cisco VSM using the credentials configured on the LDAP server (the users do not need to be added individually to the Operations Manager configuration).

Refer to the following topics for more information:

- [LDAP Usage Notes, page 4-15](#)
- [Upgrade Requirements, page 4-15](#)
- [LDAP Server Settings, page 4-16](#)
- [LDAP Search Filter Settings, page 4-20](#)
- [LDAP Configuration Examples, page 4-20](#)
- [LDAP Configuration Procedure, page 4-23](#)

LDAP Usage Notes

- LDAP users can be added or removed from the source database without affecting Cisco VSM. When the LDAP user logs in to Cisco Video Surveillance, their credentials are authenticated with the LDAP server, and access is granted or denied based on the LDAP response.
- Use LDAP filters to limit the users who can access Cisco VSM.
- To delete an LDAP server, you must un-associate the LDAP server from all Cisco VSM user groups.
- The maximum number of filters is 500.

Upgrade Requirements

New fields were added in Cisco VSM release 7.0.1 to simplify the LDAP server configuration. After upgrading from release 7.0.0, the administrator must reconfigure the LDAP server settings including the following:

- Review all LDAP server configurations in the Operations Manager and update missing information after the upgrade.
- Verify and reconfigure the binding requirements.
- Reconfigure the LDAP filters and User Group associations for each server.



Note

- These settings are not imported automatically upon upgrade. Operations Manager will not prompt the administrator or display messages that indicate the new fields that need to be updated. Carefully review the LDAP configuration descriptions and instructions to implement the required changes.
- You must be logged in to the localhost domain to apply these changes (see [Figure 4-6](#)).

Figure 4-6 Localhost login for LDAP Configuration Changes

Username: admin

Password:

Domain:
 Select
 ✓ localhost
 Anon:nrb-lnx-srvr

LDAP Server Settings

The LDAP server settings define the network address of the LDAP server, the method used to bind (connect) Cisco VSM with the server, the location of the LDAP user information, and the filters that define the specific LDAP users that can access the Cisco VSM system.

Figure 4-7 LDAP Server Settings

Version 7.0
 Cisco Video Surveillance Operations Manager

Admin (admin) Logout Help

Monitor Video Cameras Users System Settings Operations

Find

LDAP Server

Name	Tags
Anon:nrb-lnx-srvr	

Total 1

Add

Add LDAP Server

General Information

- Anonymous Binding: ☐
- Name:
- Hostname:
- Port:
- Principal:

Test

LDAP Search Filters

Add

User Groups

Name	Filter
------	--------

Create Cancel

© 2008-2013 Cisco Systems, Inc. All rights reserved.

The following table describes the purpose and requirements for each setting. Refer to the [“LDAP Configuration Examples” section on page 4-20](#) for additional information. See the [“LDAP Configuration Procedure” section on page 4-23](#) to complete the configuration.

**Note**

The LDAP server settings were changed for Release 7.0.1. If you are upgrading from Release 7.0.0, you must revise the configuration to conform to the new fields and requirements.

Table 4-8 **LDAP Server: General Information Settings**

Setting	Description
Anonymous Binding	(Optional) Select this option, if the LDAP server being configured supports anonymous access.
Name	(Required) Enter a descriptive name for the server.
Hostname	(Required) Enter the server hostname or IP address.
Port	(Required) Enter the server port. Port 389 is typically used for LDAP communication.

Table 4-8 LDAP Server: General Information Settings (continued)

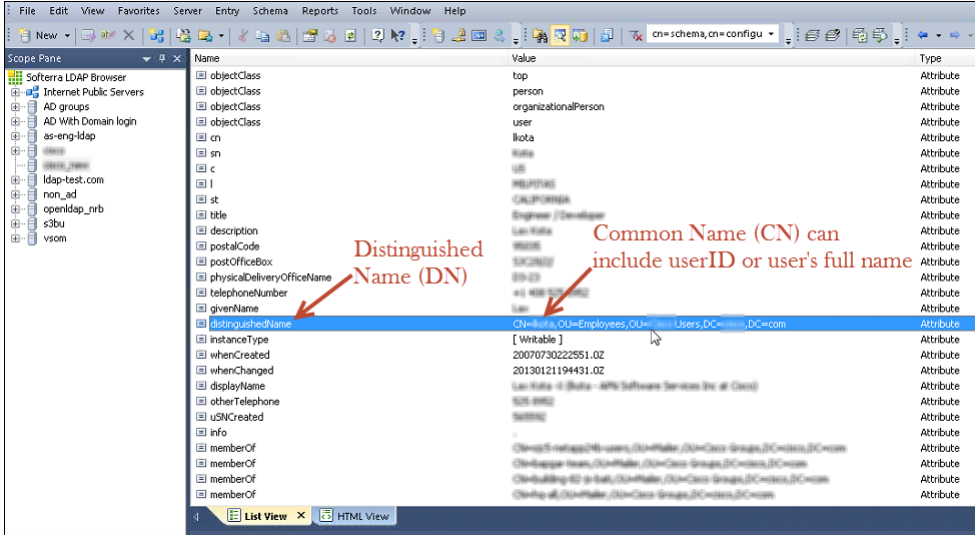
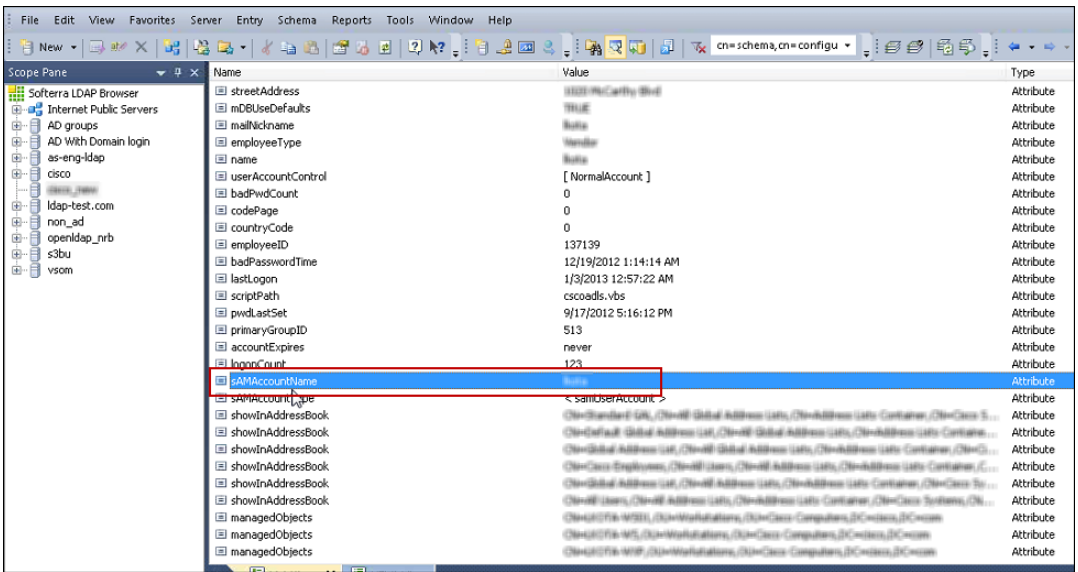
Principal	<p>(Required) The Principal setting is used to <i>bind</i> Cisco VSM to the LDAP server. In other words, the Principal setting defines the user information used to authenticate individual users with the LDAP server.</p> <p>The Principal entry includes the <code>%USERID%</code> variable, which represents the userID configured on the LDAP sever. The <code>%USERID%</code> and password are entered when the user logs into Cisco VSM, and is sent to the LDAP server for authentication.</p> <ul style="list-style-type: none"> If the Principal path (Bind DN) contains userid, enter the Principal in the following pattern: CN=%USERID%,OU=Company Users,DC=mycompany,DC=com If Principal path(Bind DN) contains user's full name instead of userid(eg. CN represents full name instead of userid) especially for AD servers, then enter the Principal in the following pattern: %USERID%@domain.com. <p>The following illustration shows an LDAP configuration that uses the userID as the CN.</p>  <p>Anonymous Binding</p> <p>Select this option if the LDAP server allows anonymous access and you prefer to connect and search the LDAP server anonymously in order to authenticate the users logging in to Cisco VSM.</p> <p>Anonymous Binding requires only the base DN, and does not require the <code>%USERID%</code> variable. For example:</p> <p>ou=employees,ou=people,o=mycompany.com</p> <p>Note The following error is returned if the LDAP server does not support Anonymous Binding:</p> <p>Operation failed: User <user id> is not found in LDAP or given distinguished name does not support anonymous access.</p>
-----------	---

Table 4-8 LDAP Server: General Information Settings (continued)

User Search Base	<p>(Required, except for Anonymous Binding) The Search Base indicates the lowest level of LDAP hierarchy where users will be found. User information includes attributes such as first name, last name, email address, etc.</p> <p>For example: OU=Company Users,DC=Mycompany,DC=com</p> <p>Anonymous Binding</p> <p>This field is optional field for Anonymous Binding.</p>
Userid Attribute	<p>(Required) Enter the name of the LDAP mapping field where the User ID is stored. For example:</p> <ul style="list-style-type: none"> • cn • uid • userid • sAMAccountName (Active Directory only—this value is used only with Active Directory servers). The following illustration shows an LDAP configuration that uses the sAMAccountName field for the userID. 
Firstname Attribute	<p>(Optional, if defined on the LDAP server).</p> <p>The name of the LDAP server attribute that holds the users' first name. For example: givenName or displayName.</p>
Lastname Attribute	<p>(Optional) The name of the LDAP server attribute that holds the users' surname.</p> <p>For example: sn (if defined on the LDAP server).</p>
Email Attribute	<p>(Optional) The name of the LDAP server attribute that holds the users' email address.</p> <p>For example: mail (if defined on the LDAP server).</p>
Tags	(Optional) Words that assist in a <i>Find</i> .
Description	(Optional) Description of the LDAP server. For example: the server purpose, location, or user base.

LDAP Search Filter Settings

Filters restrict authentication to a subset of users (the filter represents a user group that is defined on the LDAP server). Each filter can be associated with a different user group, which grants LDAP users in that filter the access permissions of the Cisco VSM user group. This allows you to grant different permissions to different sets of users.

For example, a filter for the `dept_eng` users can be associated with an admin user group while rest everyone in `company_eng` will be made an operator.

The maximum number of filters is 500.



Note

The LDAP filter settings were changed for Release 7.0.1. If you are upgrading from Release 7.0.0, you must revise the configuration to conform to the new fields and requirements.

Table 4-9 **LDAP Filter Settings**

Field	Description
Name	Enter a descriptive name for the filter. For example: <code>Security users</code>
Search Path	The directory path where user groups are stored on the LDAP server. In some LDAP configurations, the user information (User Search Base) and user group information are in different locations. This field specifies where the user group information is located. For example: <code>ou=groups,o=mycompany.com</code> .
Filter	Enter the syntax that limits access to members of a specific group on the LDAP server. For example: <code>(&(cn=%USERID%)(memberOf=CN=vsom-admins,OU=Grouper,DC=mycompany,DC=com))</code>



Tip

See the [“LDAP Configuration Examples” section on page 4-20](#) for additional configuration examples.

LDAP Configuration Examples

To enable LDAP connectivity, the Operations Manager configuration must correspond with the LDAP server configuration. A few possible variations are:

- Non Active Directory Server
 - Anonymous Binding
 - Regular Binding:
 - `uid=` user id (the user has uid attribute in the LDAP server equal to the User ID used to login)
 - `cn =` user id (the user has a cn attribute in the LDAP server equal to the User ID used to login)
 - `cn=`full name (CN contains full name)
- Active Directory Server
 - `sAMAccountName =` userid (the user has the `sAMAccountName` attribute value in AD equal to the ID used to login)

- userPrincipalName = user ID (the user has userPrincipal attribute value in AD equal to the login ID)
- cn = user id (i.e., the user has a cn attribute in the LDAP server equal to the User ID used to login)

Review the following table for additional information and configuration summaries.

Table 4-10 LDAP Configuration Options

LDAP Configuration	Description	Configuration Example
Active Directory Server CN = <i>userid</i>	<p>When the LDAP Common Name (CN) field includes the userID, the Cisco VSM “Principal” setting includes the <i>%USERID%</i> variable and the complete User Search Base path.</p> <p>Note The <i>%USERID%</i> variable is replaced with the username entered when logging into Cisco VSM.</p>	<ul style="list-style-type: none"> • Anonymous Binding: Off • Principal example: <i>cn=%USERID%,ou=active,ou=employees,ou=people,dc=mycompany,dc=com</i> • User Search Base example (corresponding to the above Principal): <i>ou=employees,ou=people,dc=mycompany,dc=com</i> • Filter example: <ul style="list-style-type: none"> – Name: <i>vsom-admins</i> – Search path: <i>dc=mycompany, dc=com</i> (corresponding to the above examples) – Filter: <i>(&(cn=%USERID%)(memberOf=CN=vsom-admins,OU=Grouper,DC=mycompany,DC=com))</i>
Active Directory Server CN = the users full name	<p>When the LDAP Common Name (CN) field includes the user’s full name:</p> <ul style="list-style-type: none"> • The Principal setting includes the <i>%USERID%</i> variable as a pattern, such as an email address. • The User Search Base defines where the user information is located. • The Userid Attribute defines the LDAP field where the userID is stored. 	<ul style="list-style-type: none"> • Anonymous Binding: Off • Principal example: <i>%USERID%@mycompany.com</i> • User Search Base example: <i>dc=mycompany, dc=com</i> (corresponding to the example shown in the following filter) • Filter example: <ul style="list-style-type: none"> – Name: <i>vsom-admins</i> – Search path: <i>ou=active,ou=employees,ou=people,o=mycompany.com</i> – Filter: <i>(&(cn=%USERID%)(memberOf=CN=vsom-admins,OU=Grouper,DC=mycompany,DC=com))</i>

Table 4-10 LDAP Configuration Options (continued)

LDAP Configuration	Description	Configuration Example
Regular LDAP binding (non-Active Directory)	<p>A non-Active Directory server uses the User Search Base path where the user information is stored in both the Principal and User Search Base fields.</p> <p>The Userid Attribute defines the LDAP field where the userID is stored.</p>	<ul style="list-style-type: none"> Anonymous Binding: Off Principal example: <i>CN=%USERID%,OU=people,OU=US,DC=mycompany,DC=com</i> User Search Base example: <i>ou=people,ou=us,dc=mycompany,dc=com</i> (corresponding to the above Principal) Filter example: <ul style="list-style-type: none"> Name: <i>vsom-admins</i> Search path: <i>ou=people,ou=us,dc=mycompany,dc=com</i> (corresponding to the above Principal) Filter: <i>(&(objectClass=posixGroup)(memberuid=%USERID%)(cn=vsomadmins))</i>
Anonymous Binding (non-Active Directory)	<p>If the LDAP server is configured to be accessed as anonymous, the <i>%USERID%</i> variable is not required.</p> <p>Only the correct server hostname, port and principal is required to bind Cisco VSM to the LDAP server.</p> <p>Note Although the communication (binding) can occur anonymously between Cisco VSM and the LDAP server, Cisco VSM also verifies that the username and password entered by the user are valid on the LDAP server.</p> <p>Note The Test button does not require you to enter a username or password since the test is only checking for server connectivity (not valid user credentials). The Test will complete successfully if the LDAP server is configured for Anonymous Binding and if the server address and port are correct.</p>	<ul style="list-style-type: none"> Anonymous Binding: On Principal example: <i>ou=people,ou=us,dc=mycompany,dc=com</i> User Search Base: Leave blank Filter example: <ul style="list-style-type: none"> Name: <i>vsom-admins</i> Search path: <i>dc=mycompany,dc=com</i> Filter: <i>(&(objectClass=posixGroup)(memberuid=%USERID%)(cn=vsomadmins))</i>

LDAP Configuration Procedure

Complete the following procedure to bind a LDAP server to Cisco VSM, and associate the LDAP user with a Cisco VSM user group.

**Note**

To configure LDAP servers, you must log in with *super-admin* privileges, using the **localhost** Domain.

Procedure

- Step 1** Log on to the Cisco VSM using the following (Figure 4-6):
- An account that belongs to a User Group with *super-admin* access permissions (for example, **admin**)
 - See the “[Logging In](#)” section on page 1-18.
 - Select the **localhost** Domain.

Figure 4-8 Localhost Login for LDAP Configuration Changes

Username: admin

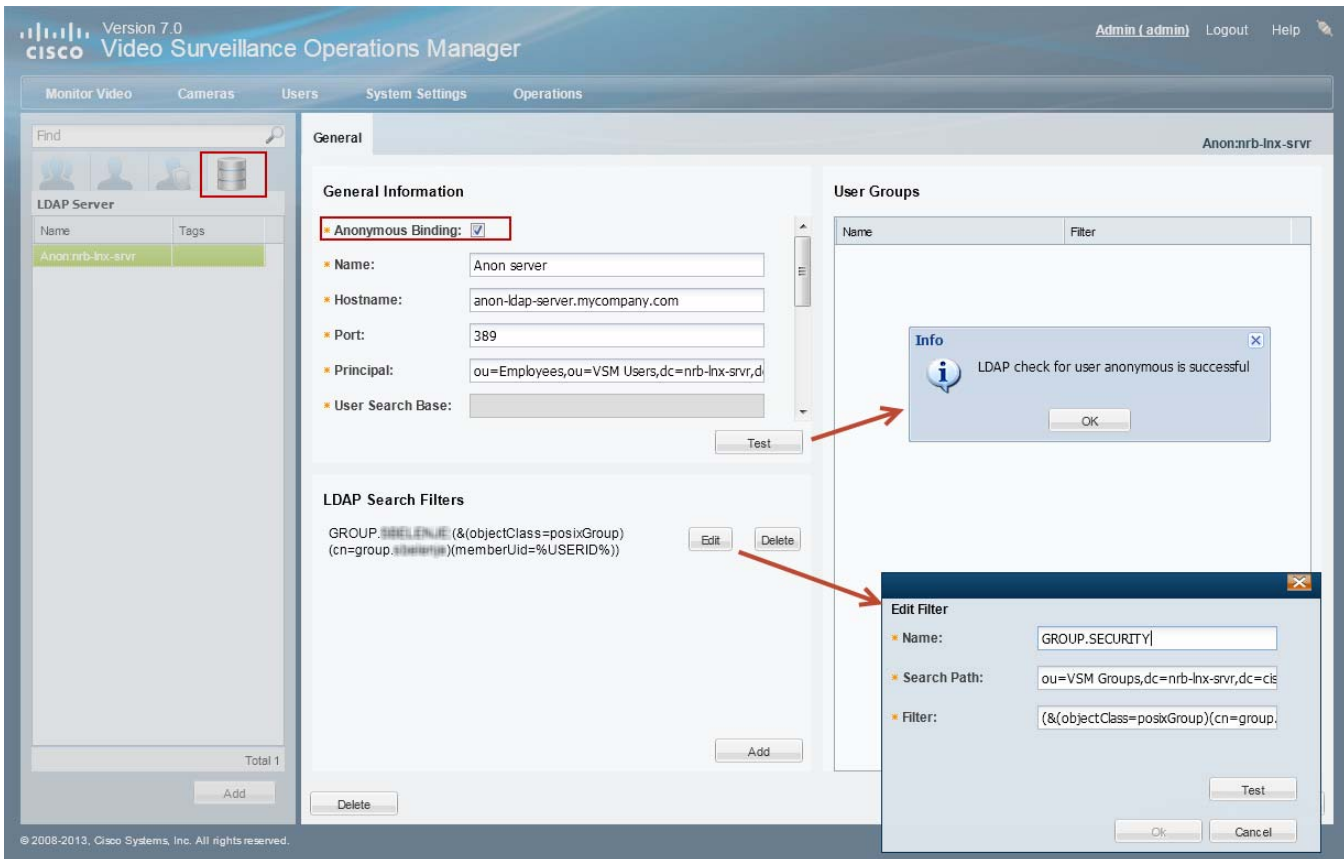
Password:

Domain:
Select
✓ localhost
Anon:nrb-lnx-srvr

- Step 2** Select the **LDAP Server** tab .

Step 3 Click **Add** (or select an existing entry to edit a server).

Figure 4-9 Sample LDAP Server Settings



Step 4 (Required) Enter the *General* LDAP server settings (Figure 4-9).

- Enter the settings as described in the “LDAP Server Settings” section on page 4-16 (see Table 4-8).
- Click **Test** and enter the test username and password (credentials are not required if **Anonymous Binding** is selected).
- If the test fails, correct the settings and try again.



Note

The LDAP server settings were changed for Release 7.0.1. If you are upgrading from Release 7.0.0, you must revise the configuration to conform to the new fields and requirements.



Tip

See the “LDAP Configuration Examples” section on page 4-20 for configuration examples.

Step 5 (Required) Define one or more *LDAP Search Filters*.

The maximum number of filters is 500.

- a. Click **Add** (Figure 4-9).
- a. Enter the settings as described in the “[LDAP Search Filter Settings](#)” section on page 4-20 (see [Table 4-9](#)).
- b. Click **Test** to verify the filter. You must enter a valid username and password for the LDAP server and filter. If the test fails, correct your entries and try again.



Note

The LDAP filter settings were changed for Release 7.0.1. If you are upgrading from Release 7.0.0, you must revise the configuration to conform to the new fields and requirements.



Tip

See the “[LDAP Configuration Examples](#)” section on page 4-20 for configuration examples.

- c. (Optional) Repeat [Step 5](#) to add additional filters. Each filter allows those LDAP users to access Cisco VSM (based on the user group assignments (see [Step 7](#)).

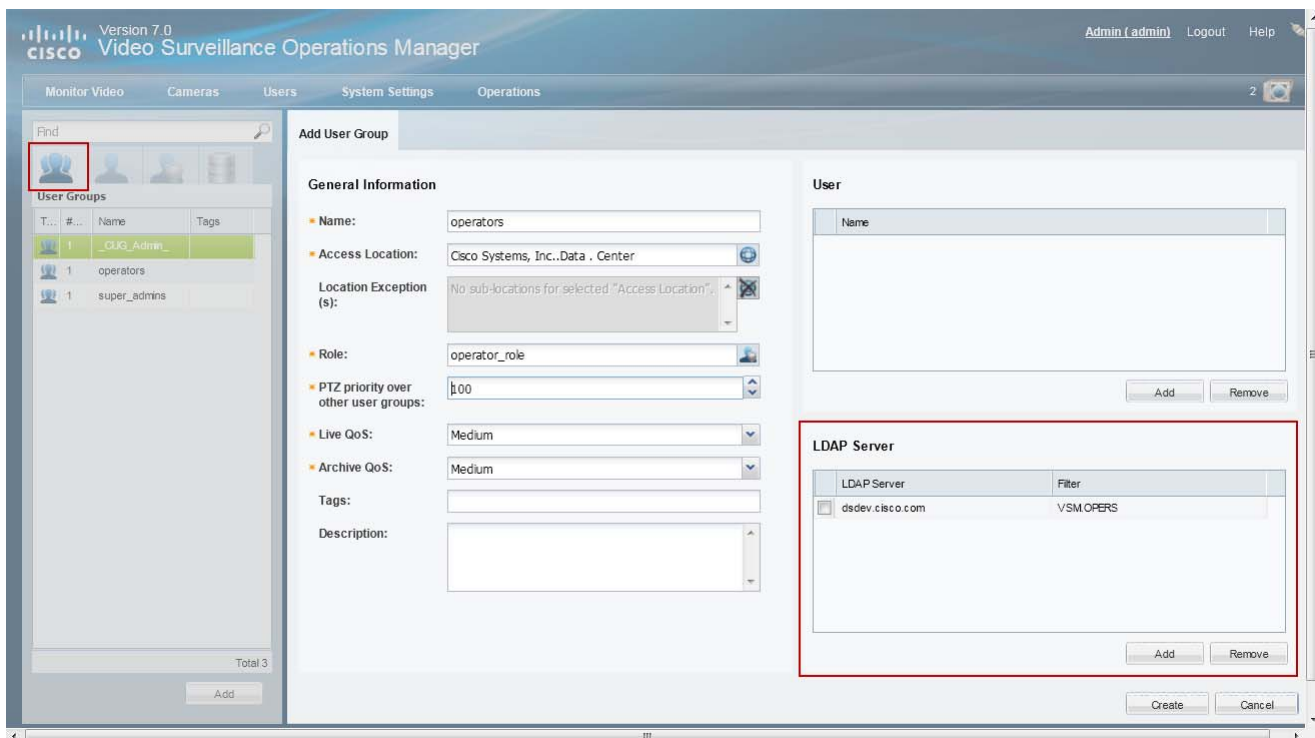
Step 6 (Required) Click **Create** or **Save** to save the LDAP server settings.


Step 7 (Required) Add the LDAP server/filters to a Cisco VSM user group.

The user group(s) define the Cisco VSM access permissions for the LDAP users (defined by the filter).

The LDAP server/filters can be added to multiple user groups. The users gain the combined access permissions of all associated user groups.

Figure 4-10 Adding an LDAP Server to a User Group




- a. Select the **User Groups** tab  (Figure 4-10).
- b. Select a user group (or create a new group as described in the “Adding User Groups” section on page 4-10).
- c. In the LDAP Server section, click **Add**.
- d. Select the *LDAP Server* name that includes the appropriate filter and click **OK**.



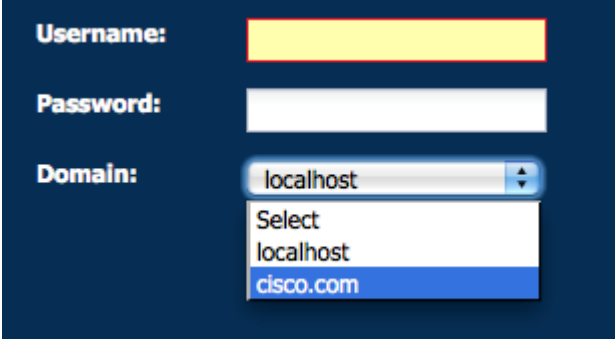
Tip The filter defines a sub-set of LDAP users that will gain the user group access permissions.

- e. Click **Save**.

Step 8 (Optional) Click the **LDAP Server** tab  to verify that the user group appears in the LDAP server configuration.

Step 9 (Optional) Log out and log back in using the credentials for an LDAP user (Figure 4-11).

Figure 4-11 Select an LDAP Login Domain



The screenshot shows the Cisco VSM Login page with a dark blue background. It has three input fields: 'Username:' (highlighted in yellow), 'Password:', and 'Domain:'. The 'Domain:' dropdown menu is open, showing a list of options: 'localhost' (selected), 'Select', 'localhost', and 'cisco.com' (highlighted in blue).

- a. Click **Log Out**.
- b. In the Cisco VSM Login page, enter the Active Directory username and password.
- c. From the *Domain* menu, select the LDAP server name and filter combination.
- d. Click **Log In**.



CHAPTER 5

Creating the Location Hierarchy

Locations allow you to organize your deployment according to the real-world location of equipment and users. Locations also allow administrators to restrict user access to the specific cameras, policies, and data (such as alerts) required by the user's role within the organization. For example, while a *super-admin* has full access to all locations and devices, a local campus administrator might have access only to the devices and policies required to manage a specific site.

This chapter describes how to create the location hierarchy, assign locations to devices, policies, and user groups, and how those assignments impact a user's ability to access Cisco VSM resources.



Tip

Since all servers, user groups and cameras must be assigned to a location, create the location hierarchy before performing other configuration tasks. Review the information in this section carefully, and then create a location plan to ensure the users in your deployment can access only the equipment, video and policies required for their role.

Contents

- [Overview, page 5-2](#)
- [Understanding Permission-Based and Partition-Based Resources, page 5-3](#)
 - [Simple Deployments \(User Access to All Devices and Resources\), page 5-4](#)
 - [Permission-Based Resources: Limiting User Access to Devices, page 5-4](#)
 - [Partition-Based Resources: User Access to Templates, Schedules and Other Resources, page 5-5](#)
- [Examples: Locations in Simple vs. Large Deployments, page 5-7](#)
- [Understanding a Camera's Installed Location Vs. the Pointed Location, page 5-9](#)
- [Creating and Editing the Location Hierarchy, page 5-10](#)
- [Impact of Device Location Changes on Alerts, page 5-11](#)
- [Deleting a Location, page 5-11](#)

Overview

Locations define the physical location of devices, such as cameras, and the logical location of attributes, such as camera templates. This allows system administrators to restrict user access to only the devices and resources required by the different users in a deployment. For example, in a simple deployment, users are assigned to the root level and gain access to all devices and resources. In larger deployments, however, users can belong to user groups that are assigned to locations at lower levels. This restricts the users' access to the devices at that location (and sub-locations). The users also have access to system resources (such as templates and schedules) that are assigned to other locations.

Summary Steps

To create a location hierarchy, do the following:

Table 5-1 *Summary Steps: Location Hierarchy and Assignments*

	Task	More Information
Step 1	Review the overview topics to understand how locations impact users' ability to access devices and resources.	<ul style="list-style-type: none"> • Contents, page 5-1 • Understanding Permission-Based and Partition-Based Resources, page 5-3 • Examples: Locations in Simple vs. Large Deployments, page 5-7
Step 2	Create the location hierarchy for your deployment.	Creating and Editing the Location Hierarchy, page 5-10
Step 3	Assign devices, user groups and resources to the locations.	<ul style="list-style-type: none"> • Creating or Modifying a Template, page 10-3 • Editing the Camera Settings, page 8-42 • Understanding a Camera's Installed Location Vs. the Pointed Location, page 5-9 • Adding External Encoders and Analog Cameras, page 11-5 • Media Server Settings, page 7-4 • Adding User Groups, page 4-10
Step 4	Assign users to one or more user groups. Users gain access to the locations assigned to the user groups.	Adding Users, page 4-13

Understanding *Permission-Based* and *Partition-Based* Resources

Locations assigned to Cisco VSM resources define the following:

- The physical location of servers and encoders.
- The installed (physical) and *pointed at* location of cameras.
- The logical location of Cisco VSM attributes, such as camera templates, schedules, Video Walls and preset *Views*.
- The location of user groups and user roles.

In addition, the following rules apply:

- Resources such as devices, user groups and view are *permission-based*, meaning that they can only be accessed by users at that same location or lower (sub-location).
- *Partition-based* resources (such as templates and schedules) can be accessed by users within the same location hierarchy (locations higher or lower in the same location tree).
- *Global* resources can be accessed by all users who have the required access permissions.
- *Super-admin* resources (such as system settings and audit logs) can only be accessed by super-admin users.

Table 5-2 summarizes the resource types.

Table 5-2 Resource Access Summary

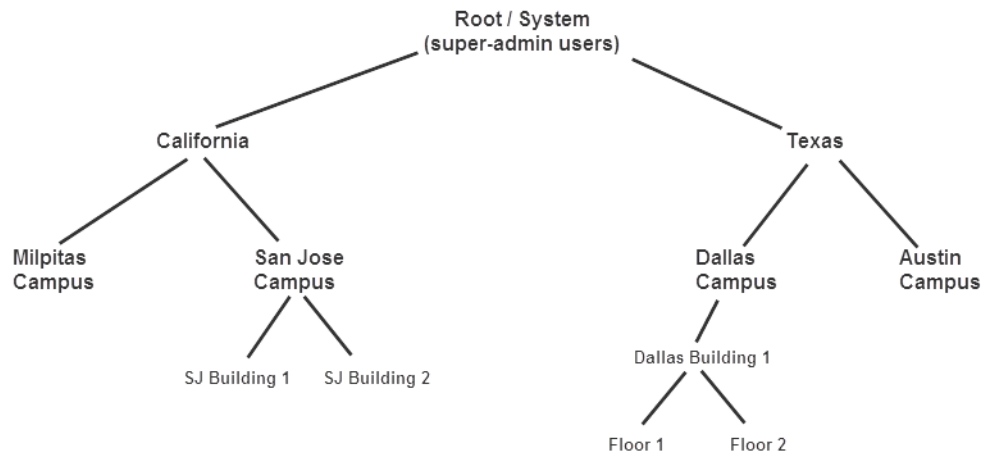
Type	Resources	Description
Permission-Based	<ul style="list-style-type: none"> • Devices (cameras, encoders, servers) • User groups • Views 	<p>Users can access <i>permission-based</i> resources that are assigned to their user group location or lower (sub-location).</p> <p>For example, in Figure 5-2 a user assigned to a <i>Dallas Campus</i> user group can access the cameras at the <i>Building 1</i> sub-location, but not at the <i>Texas</i> location. <i>Dallas</i> users also cannot access any <i>California</i> locations.</p>
Partition-Based	<ul style="list-style-type: none"> • User roles • Schedules • Camera templates 	<p>User groups can access <i>partition-based</i> resources that are in the same location hierarchy (either higher or lower, but not in a different branch).</p> <p>For example, in Figure 5-3 a user assigned to a <i>Dallas Campus</i> user group can access the templates or schedules at any higher or lower level up to the U.S. (root) location. The user cannot, however, access templates or schedules for the <i>Austin Campus</i> or any of the <i>California</i> locations.</p>
Global Resources	<i>Global</i> resources can be accessed by all users who have the required access permissions.	For example, a user with <i>manage users</i> permissions access all the users in the system. The user object is not restricted to a location.
Super-admin	<ul style="list-style-type: none"> • System Settings • Audit Logs 	Only users assigned to a <i>super-admin</i> user group can access these system-wide resources.

Simple Deployments (User Access to All Devices and Resources)

In a simple deployment (Figure 5-1), all users are assigned to a user group at the root (*System*) location. Users can access all cameras and resources at all sub-locations.

For example, in Figure 5-1, root (*System*) level users have access to the devices and resources in all sub-locations, such as California, Texas, and the associated campus and building sub-locations. A user's ability to view or configure devices and resources is based on the *role* assigned to their *user group*.

Figure 5-1 Locations and User Permissions in a Simple Deployment



Tip

User access can still be restricted based on the assigned user group. For example, an *operator* user group can provide access to only view video, but not configure system resources. See the “[Adding Users, User Groups, and Permissions](#)” section on page 4-1 for more information.

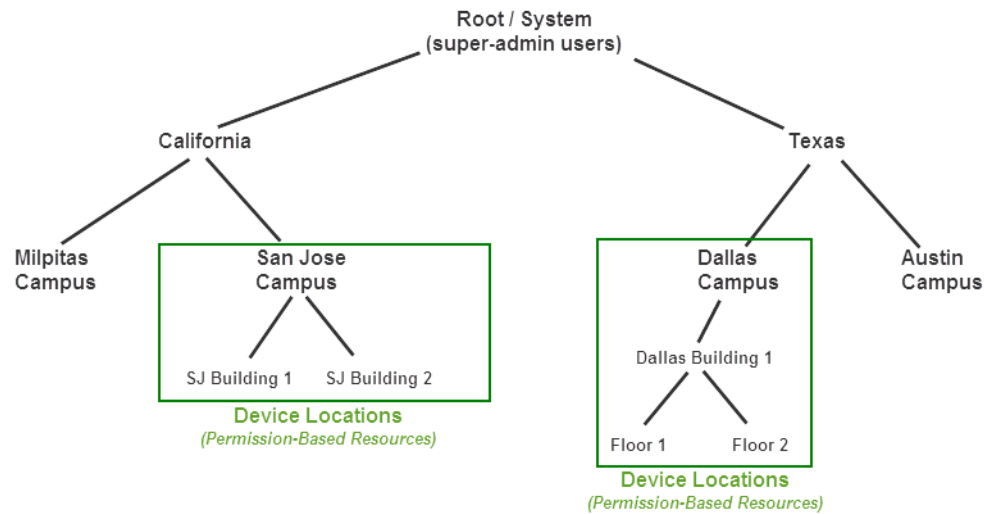
Permission-Based Resources: Limiting User Access to Devices

Users can access devices assigned to the same location, or lower. For example, if a user is assigned to a user group at the *San Jose Campus* location (Figure 5-2), the user gains access to any cameras assigned to the *San Jose Campus* location, and all sub-locations (such as *SJ Building 1*).



Note

- Users *cannot* access cameras assigned to higher locations (such as *California* in Figure 5-2), or sub-locations in a different hierarchical tree (such as the *Milpitas Campus* or *Texas*).
- A user's location includes all of the user groups to which the user is assigned. For example, if a user is assigned to a user group for the *San Jose Campus*, and is also assigned to another user group for the *Dallas Campus* (Figure 5-2), the user gains access to the devices at both locations.
- Devices, user groups and *Views* are *permission-based* resources. All *permission-based* resources adhere to these same rules.

Figure 5-2 Limiting User Access to Specific Locations**Tip**

- Servers should be assigned to a high-level location to provide support to services, devices and user groups at lower-level locations. In the [Figure 5-2](#) example, assign the servers to either the Root (System) location, or the California and Texas locations.
- Camera *Views* are also assigned to a location. Users can only access the *Views* assigned to their location and lower. See the [“Creating Pre-Defined Views”](#) section on page 3-2.

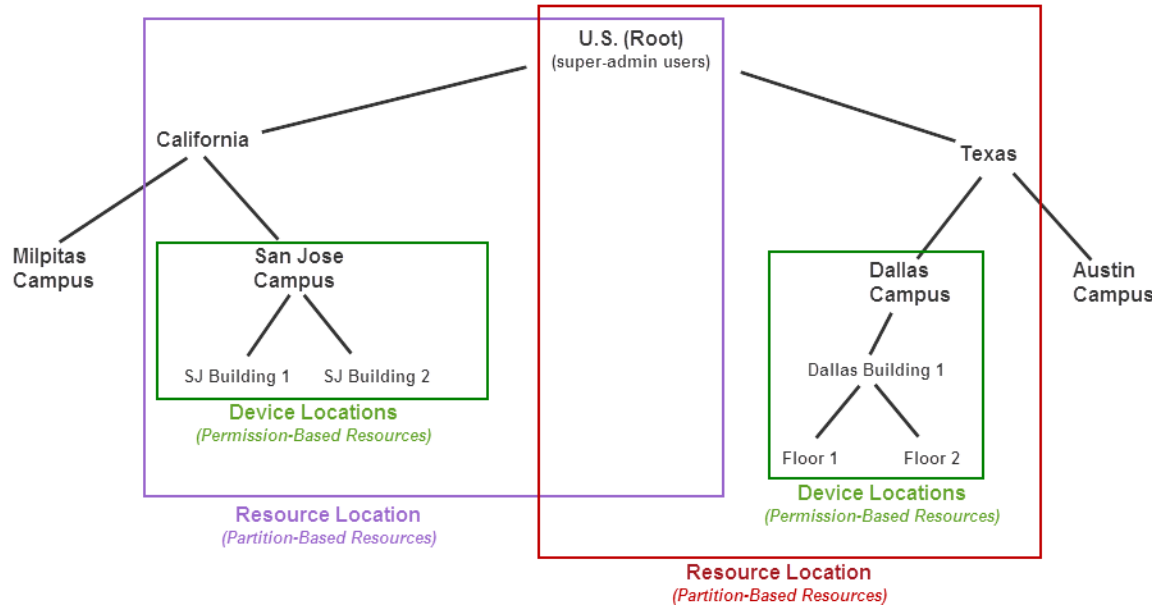
Partition-Based Resources: User Access to Templates, Schedules and Other Resources

Partition-based resources include camera templates, schedules, and user roles. If the user belongs to a user group with access to these resources, then the user can access any partition-based resource in the same location hierarchy (locations that are higher or lower, but not in a different branch).

For example, in [Figure 5-3](#) a user assigned to a *San Jose Campus* user group can access the templates or schedules at any higher level location (up to the U.S. root location). The user cannot, however, access templates or schedules for the *Milpitas Campus* or any of the *Texas* locations.

**Tip**

The user must be assigned to a user groups that provides access to the resource. See the [“Adding Users, User Groups, and Permissions”](#) section on page 4-1 for more information.

Figure 5-3 Limiting User Access to Specific Locations

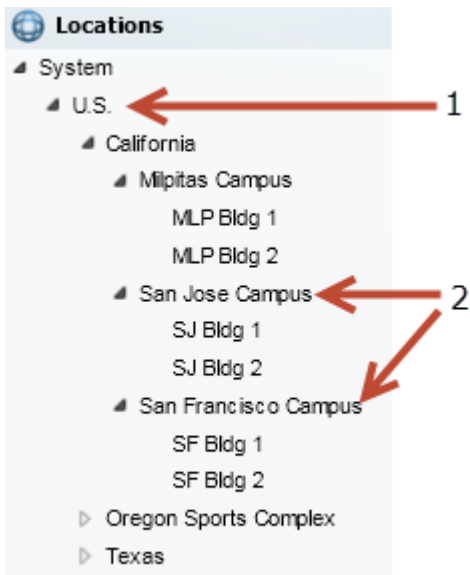
Examples: Locations in Simple vs. Large Deployments

Simple Deployment Example

A simple Cisco VSM deployment typically places *partition-based resources* (templates, roles and schedules) at the root level so they can be accessed by users at all of the sub-locations (Figure 5-4). Users must still belong to a user group that provides access to view or manage those resources.

Permission-based resources (such as cameras) can also be placed at the root level, but only users in a user group at the root level will be able to access them. You can assign both devices and users at a sub-location to restrict user access to the *permission-based resources* at that location.

Figure 5-4 Example Locations for a Simple Deployment



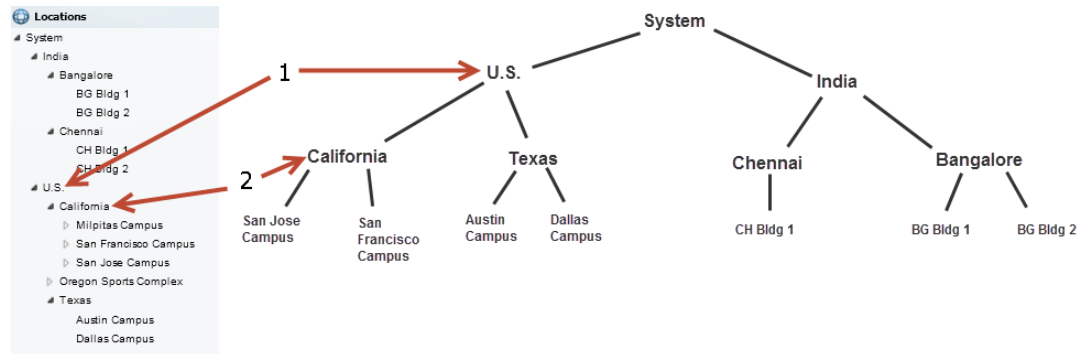
<p>1 Assign <i>partition-based resources</i> (templates, roles and schedules) to a high-level or root location.</p> <ul style="list-style-type: none"> • <i>Partition-based resources</i> (templates, roles and schedules) can be viewed and used by all users at all sub-locations. • Users can only modify the templates, roles, and schedules that are assigned to their location (or lower). • For example, in Figure 5-4 a user assigned to “Milpitas Buildings” can view <i>partition-based resources</i> assigned to the “U.S.” location, but only super-admin users can modify the resources. <p>Tip We recommend also assigning servers to a high-level location to provide support to devices and user groups at lower-level locations.</p>	<p>2 Assign <i>permission-based resources</i> (such as cameras) to sub-locations to restrict user access.</p> <ul style="list-style-type: none"> • Users can only access <i>permission-based resources</i> (such as cameras) that are assigned to the user’s location and lower. • For example, in Figure 5-4 a user assigned to “Milpitas Buildings” can access cameras at that level and lower (such as building 1 and building 2), but cannot access cameras at an equal level (such as “San Jose Buildings”) or at higher locations (such as “California” or “US”). <p>Tip Deployments with a small number of users can also assign user groups and <i>permission-based resources</i> to the “U.S.” (root) location.</p>
--	--

Large Deployment Example

Larger deployments support multiple campuses or geographically distant sites. Users at different regions or campuses require a distinct set of schedules, roles and templates. For example, the deployment in [Figure 5-5](#) includes sites in both the U.S. and India. *Partition-based resources* (templates, roles and schedules) assigned to the India location can only be viewed by users in the India sub-locations, (not by U.S. users). Resources assigned to the “U.S.” location can only be viewed by U.S. users.

This configuration also allows “India” or “U.S.” user to modify the *partition-based resources* for their region without impacting other regions.

Figure 5-5 Example Locations for a Large Deployment



<p>1 Assign <i>partition-based resources</i> (templates, roles and schedules) to a high-level branch location, such as “U.S.”</p> <ul style="list-style-type: none"> • <i>Partition-based resources</i> (templates, roles and schedules) can be viewed and used by all users within that location hierarchy (for example, from the San Jose Campus up to the System users). • Users can only modify the templates, roles, and schedules that are assigned to their location (or lower). <p>For example, in Figure 5-5 a user assigned to “California” can view <i>partition-based resources</i> assigned to the “U.S.” location, but not resources in the “India” locations.</p>	<p>2 Assign <i>permission-based resources</i> (such as cameras) to sub-locations to restrict user access.</p> <ul style="list-style-type: none"> • Users can only access <i>permission-based resources</i> (such as cameras) at their location and lower. • For example, in Figure 5-5 a user assigned to “Chennai” can access cameras at that level and lower (such as “CH Bldg 1”), but cannot access cameras at an equal level (such as “Bangalore”) or at higher level (such as “India”).
---	--



Tip

System users (such as super-admins) can view all resources at all sub-locations. Super-admins can also access system settings and other resources. See [Table 5-2 on page 5-3](#) for more information.

Understanding a Camera's Installed Location Vs. the Pointed Location

A location can represent where the device is physically installed, or a logical location. For example, camera configurations include settings for both the *Installed Location* and the *Pointed Location* (Figure 5-6). In the following example, a camera is installed on *Building 1* but is pointed at the *Building 2* lobby doors.

Figure 5-6 Sample Camera Location Entry

The screenshot displays the 'Cameras' configuration page in the Cisco Video Surveillance Operations Manager. On the left, a tree view titled 'Cameras by Location' shows a hierarchy: 'System' (expanded) -> 'Building 1' -> 'Building 2' -> 'Lobby Door 2' (selected and highlighted in green). A red arrow points from 'Lobby Door 2' to the 'Install Location' field in the 'General Information' tab. The 'General Information' tab is active, showing fields for 'Template' (NTSC Generic Medium Device Template), 'Name' (Lobby Door 2), 'Media Server' (Primary Server), 'Install Location' (System.Building 1), 'Pointed Location' (System.Building 2), 'Tags', and 'Description'. The 'Install Location' and 'Pointed Location' fields are highlighted with a red box.



Tip

This distinction is used when viewing video alarms. If an alarm occurs at *Building 1*, the Cisco Safety and Security desktop application will display the alarm (for *Building 1*) even if the camera's installed location is *Building 2* (since the camera is pointed at *Building 1*).

Creating and Editing the Location Hierarchy

To create or modify the locations in your deployment, do the following:

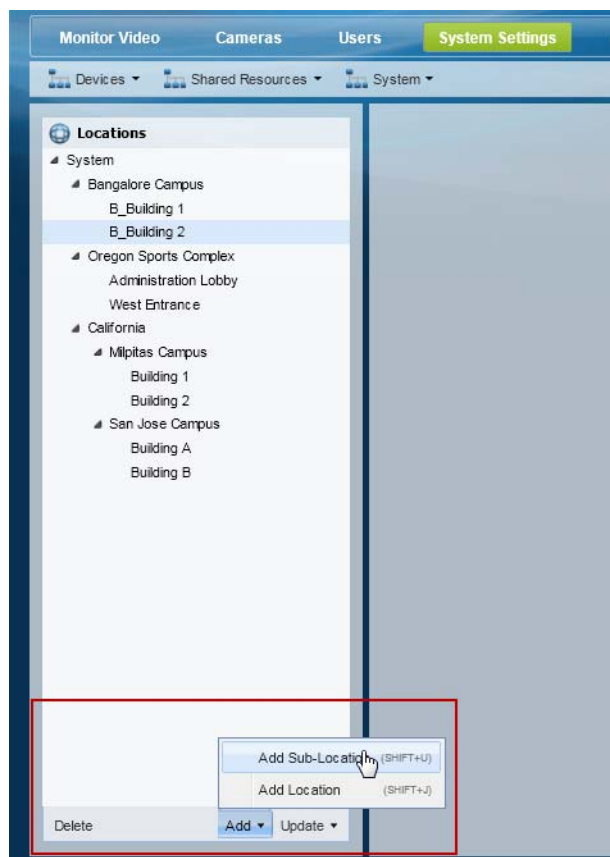
Procedure

- Step 1** Log on to the Operations Manager.
- See the “[Logging In](#)” section on page 1-18.
 - You must belong to a User Group with permissions for *Locations & Maps*.
- Step 2** Select **System Settings > Locations**.
- Step 3** Select an existing location and click **Add** to add a new location or sub-location ([Figure 5-7](#)).



Note In a new system, only the *System* location appears.

Figure 5-7 *Locations Menu*



Add menu ([Figure 5-7](#)):

- Choose **Add Location** (*Shift-J*) to add a location at the same level.
- Choose **Add Sub-Location** (*Shift-U*) to add a sub-location to the existing location.
- Enter the name and description.

- Press *Enter* or click **Save**.

Update menu:

- Choose **Detent Location** (*Shift-<*) to move the location one level higher in the hierarchy.
- Choose **Indent Location** (*Shift->*) to move the location one level lower as a sub-location.
- Choose **Rename** (*Enter*) to edit the location name. Press *Enter* or click **Save**.



Tip

Use the keyboard shortcuts (shown in parentheses) to quickly add or edit location entries.



Tip

You can also drag and drop location names within the location hierarchy.



Tip

Click **Delete** to remove an entry. You can only delete a location that does not have any resources assigned to the location, or any of its sub-locations. If the delete operation fails, remove or reassign any associated resources and try again.

Step 4 Press *Enter* or click **Save** to save the changes.

Impact of Device Location Changes on Alerts

Because device locations rarely change, the alert location will normally be the same as the device location. However, if the device location is changed, the following will occur:

- New events show the new location, but are added to the existing (and open) alert at the old location.
- When the alert is closed by an operator, any new events create a new alert at the new location (the location reference in the alert is now consistent with the device location in the event).

See the [Cisco Video Surveillance Safety and Security Desktop User Guide](#) for more information.

Deleting a Location

Locations can be deleted only if no resources (such as cameras) are associated with the location or any of its sub-locations. See [Table 5-2 on page 5-3](#) for a list of the resources that use locations.

Procedure

To delete a location or sub-location:

- Step 1** Remove all devices and resources from the location and sub-locations.
You can reassign the devices and resources to a different location, or delete the items.
- Step 2** Select **System Settings > Locations**.
- Step 3** Select the location or sub-location.
- Step 4** Click **Delete**.

- Step 5** If the delete operation fails and an error message appears, remove or reassign any resources that are associated with the location or sub-location and try again.
-



CHAPTER 6

Configuring Servers

A server is a physical server or virtual machine (VM) that runs the Cisco Video Surveillance software. Once installed, you can enable Cisco VSM services (such as Operations Manager and Media Server

Refer to the following topics for instructions to configure and monitor a server using the Operations Manager, and to enable server services.

Contents

- [Requirements, page 6-2](#)
- [Summary Steps to Add or Revise a Server, page 6-3](#)
- [Server Settings, page 6-4](#)
 - [General Information Settings, page 6-4](#)
 - [Medianet, page 6-4](#)
 - [Services, page 6-5](#)
 - [Access Information Settings, page 6-5](#)
 - [Network Information, page 6-7](#)
 - [NTP Information, page 6-8](#)
- [Adding or Editing Servers, page 6-10](#)
 - [Prerequisites, page 6-11](#)
 - [Adding or Editing a Single Server, page 6-11](#)
 - [Importing or Updating Servers Using a CSV File, page 6-13](#)
- [Deleting a Server, page 6-18](#)
- [Bulk Actions: Revising Multiple Servers, page 6-19](#)
- [Viewing Server Status, page 6-22](#)
- [Resetting the Server Device State, page 6-23](#)
- [Repairing the Configuration or Restarting the Server, page 6-23](#)
- [Operations Manager Advanced Settings, page 6-24](#)
 - [SMTP Management Settings, page 6-24](#)

Requirements

Before you begin, verify that the following requirements are met.

Table 6-1 **Server Requirements**

Requirements	Requirement Complete? (✓)
The IP address and password for the server.	<input type="checkbox"/>
You must belong to a user group with <i>Servers & Encoders</i> permissions. See the “Adding Users, User Groups, and Permissions” section on page 4-1 for more information.	<input type="checkbox"/>
A physical or virtual Cisco Video Surveillance 7.x server installed in the network where the other Cisco Video Surveillance components are deployed. <ul style="list-style-type: none"> Physical Servers: <ul style="list-style-type: none"> (Systems pre-installed with Release 7.2) See the Cisco Physical Security UCS Platform Series User Guide for more information. (Systems pre-installed with Release 7.0.0 or 7.0.1) See the Cisco Physical Security Multiservices Platform Series User Guide for more information. Virtual Machines—See the Cisco Video Surveillance Virtual Machine Deployment and Recovery Guide for UCS Platforms for instructions to install the server software .ova image as a virtual machine (VM). 	<input type="checkbox"/>
Complete the server initial configuration using the browser-based Cisco VSM Management Console. See the Cisco Video Surveillance Management Console Administration Guide for more information.	<input type="checkbox"/>
Each server must run the same versions of the <i>system software</i> and device <i>driver packs</i> . See the following for more information: <ul style="list-style-type: none"> Understanding Cisco Video Surveillance Software, page 1-21 Installing and Upgrading Driver Packs, page 15-8 	<input type="checkbox"/>

Summary Steps to Add or Revise a Server

The following steps summarize how to add or update a server.



Note

The Operations Manager server (“VsomServer”) is added by default and cannot be deleted. All servers are assigned the Primary HA role by default (see the [“High Availability” section on page 12-1](#)).

	Step	More Information
Step 1	Install the server.	Physical Servers <ul style="list-style-type: none"> (Systems pre-installed with Release 7.2) See the Cisco Physical Security UCS Platform Series User Guide for more information. (Systems pre-installed with Release 7.0.0 or 7.0.1) See the Cisco Physical Security Multiservices Platform Series User Guide for more information. Virtual Machines <ul style="list-style-type: none"> See the Cisco Video Surveillance Virtual Machine Deployment and Recovery Guide for UCS Platforms for instructions to install the server software .ova image as a virtual machine (VM).
Step 2	Complete the server <i>Initial Setup Wizard</i> .	Cisco Video Surveillance Management Console Administration Guide .
Step 3	Log on to the Operations Manager.	Logging In and Managing Passwords, page 1-18 .
Step 4	Add one or more servers. Note The server that hosts the Operations Manager is added by default as VsomServer. a. Select System Settings > Servers . b. Click Add or select an existing server entry. c. Complete the instructions to add or edit a single server, or to import servers from a CSV file.	<ul style="list-style-type: none"> Adding or Editing Servers, page 6-10 Server Settings, page 6-4 Note Servers can be added to the configuration in <i>Pre-provisioned</i> state before they are available on the network. See the “Pre-Provisioning Servers” section on page 6-11 .
Step 5	(Optional) Configure the service options.	Configuring Media Server Services, page 7-1

Server Settings

The following topics describe the server settings available in the **General** tab.

- [General Information Settings, page 6-4](#)
- [Access Information Settings, page 6-5](#)
- [Hardware Information Settings, page 6-6](#)
- [Network Information, page 6-7](#)
- [NTP Information, page 6-8](#)

General Information Settings

General settings define the server name and installed location. You can also enter a description and tags that are used for the *Find* function.

Table 6-2 **General Server Settings**

Setting	Description
Name	(Required) Enter a descriptive name that can help you identify the server. For example, enter the location of the server or its primary use. The name can include any combination of characters and spaces.
Install Location	(Required) Click the entry field to select the location where the server is installed. The location determines the cameras and users that can access the server. See the “Creating the Location Hierarchy” section on page 5-1 for more information.
Tags	Enter the tags that help identify the server using the <i>Find</i> function.
Description	Describe the purpose or use of the server. For example: “Support for Building B cameras and associated video”.

Medianet


Use the Medianet features to monitor and troubleshoot traffic from servers and endpoints:

Table 6-3 **Medianet Settings**

Field	Settings
Enabled	Select Enabled to enable or disable metadata. This feature is enabled by default.
Name	(Read-only) The Media Services Interface (MSI) username. This field is read-only and cannot be changed.
Password	Enter the password for the Media Services Interface (MSI) performance monitor to enable Mediatrace functionality.

Services

Use the **Services** field to activate or deactivate the services running on the server.


Click the **Advanced**  icon to enter additional configurations for the service.



Note

Use the browser-based Management Console to enable or disable the services running on the server. See the [Cisco Video Surveillance Management Console Administration Guide](#) for more information.

Table 6-4 Services Settings

Field	Settings
Name	(Read-only) The service name. For example, VSOM or Media Server.
SW Version	The version of the Cisco VSM package installed on the server
Active	Select to activate or deactivate the service. Activating or deactivating a service may restart the server. If VSOM (Operations Manager) is active on this server, then VSOM will be unavailable until the server is restarted.
Advanced	Click the  icon to enter additional configurations available for the service.

Access Information Settings

The *Access* settings define the hostname and login credentials used to access the server over the network.



Note

The Access Information settings do not appear for the `VsomServer`.

Table 6-5 Access Information Settings

Setting	Description
Hostname/IP	The hostname (recommended) or IP address used by the Operations Manager to access the server. <ul style="list-style-type: none"> We recommend using the server hostname. If an IP address that was assigned by a DHCP server was used, the address can change if the server reboots, and communication will be lost.


Table 6-5 Access Information Settings (continued)

Username	(Read-only) The default username for all servers is <code>localadmin</code> . The username cannot be changed.
Password	<p>To change the password used by the Operations Manager:</p> <p>This setting changes the Operations Manager’s understanding of the server password.</p> <ol style="list-style-type: none"> 1. Enter the password that is configured on the server. 2. Click Save. <p>Note The password is used by Operations Manager to access the server and execute requests (for example, to view recorded video saved on that server). This does not change the actual server password.</p> <p>To change the password that is configured on the server:</p> <p>To change the password configured on both the server and on Operations Manager:</p> <ol style="list-style-type: none"> 1. Click Change. 2. Enter the old and new password. 3. Click OK. 4. Click Save. <p>Note See the Cisco Video Surveillance Management Console Administration Guide for more information about server passwords.</p>

Hardware Information Settings

Provides information about the physical platform, if available.

Table 6-6 Hardware Information Settings

Setting	Description
Model	The server model.
Number of CPUs	The number of CPUs running on the server.
Total Memory	The amount of RAM memory on the server.
Raid Controller	The Raid controller model, if installed.
Operating System	The sever OS type and version.
Storage	<p>The bar shows the approximate percentage use of the total storage.</p> <ul style="list-style-type: none"> • Blue: used storage space • Green: unused storage space <p>The “Total” includes the total available storage space on the partitions even if the Recording, Clipping and Backup partitions are selected in the Media Server Advanced  settings (see the “Partition Settings” section on page 7-5).</p>

Network Information

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

**Caution**

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

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

Table 6-7 **Network Settings**

Setting	Description
Name	The NIC name.
Hostname	Enter the host name used to access the server over the network.
Domain	Enter the network domain name. For example: <code>cisco.com</code>
Configuration type	Select one of the following options based on the enabled server applications. <ul style="list-style-type: none">• Disabled—disables the interface.• DHCP—the IP address and other fields will be disabled and defined by a DHCP server.• Static —enter the IP address, Subnet Mask and other network settings. <p>Note The Ethernet ports must be configured with static IP address or DHCP depending on the enabled applications. See the Overview section of the Cisco Video Surveillance Management Console Administration Guide for more information.</p>
Gateway	(Static IP configuration only) Enter the IP address of the default gateway and click Add .
DNS Servers	(Optional) Enter up to three domain name service (DNS) servers. Separate multiple entries with a comma (,).
Searchable Domains	Enter the domain name. Separate multiple entries with a comma (,).

NTP Information

The network time protocol (NTP) server automatically sets the server time and date.

- **Media Server-only server**—Use the default (and recommended) **Automatic** mode to use the Operations Manager server as the NTP server. This ensures proper operation since all components will use the same time, date, and timezone.
 - **Automatic** mode can only be used after NTP is configured on the Operations Manager server.
 - **User Configured** mode should not be used unless necessary. See [Table 6-7](#) for more information.
- **Co-located server** (Operations Manager and Media Server hosted on a single server)— Only the **User Configured** option is enabled. Enter NTP server hostname(s) or IP address(es), if necessary.
- **Operations Manager-only servers**—Use the Management Console interface to change the NTP settings for a Operations Manager-only server, if necessary. We strongly recommend using an NTP server (do not set the date and time manually). Go to **Operations > Management Console** to launch the browser-based console tool. See the [Cisco Video Surveillance Management Console Administration Guide](#) for more information.

Usage Notes

- The server time synchronizes server operations, defines recording timestamps and backup schedules. To ensure correct playback and system operation, we strongly recommend using **Automatic** mode for all Media Servers, or using the same NTP server for all Media Servers and the Operations Manager.
- **Automatic** mode can only be used after NTP is configured on the Operations Manager server.
- The server will reboot if any changes are made to the NTP settings using the Operations Manager UI.
- Changes to the server time can affect video recording schedules and timestamps.
- A warning alert is generated if the time difference between the server and Operations Manager is more than 2 minutes.
- A warning message is also displayed to operators when logging in if the time difference between their workstation and the server is more than 2 minutes.
- Never modify the time and NTP settings using the Linux CLI. Settings made using the Linux CLI can result in inconsistent system performance and other issues.

Table 6-8 NTP Server Settings

Mode	Settings
Automatic	<p>(Media Server-only servers) The Operations Manager server is used as the NTP server. The Operations Manager also defines the server timezone.</p> <ul style="list-style-type: none"> • Default and recommended for all Media Server-only servers. • Disabled for co-located servers (Operations Manager and Media Server hosted on a single server). No other changes or settings are required when using Automatic mode. <p>Note We highly recommend using Automatic mode for all Media Servers. This ensures proper operation since all components use the same time, date, and timezone.</p>

Table 6-8 NTP Server Settings (continued)

Mode	Settings
User Configured	<p>Allows you to enter a custom NTP server for the current server.</p> <ul style="list-style-type: none">• Co-located servers—(Default and required) Enter the NTP server hostname(s) or IP address(es). Separate entries with a space or comma and select the Co-located server's time zone.• Media Server-only servers—(Optional) This option may be necessary based on proximity of the Media Servers. For example: if your deployment spans numerous countries or timezones, the Media Servers may need to use local NTP servers. Enter one or more NTP server hostnames or IP addresses separated by a space or comma and select the Media Server time zone. <p>Note If multiple NTP servers are used, a hierarchy of servers should ensure that the times on the various components are close.</p> <p>Note We recommend using the same network time protocol (NTP) server on all Media Servers to ensure the time settings are accurate and identical.</p>

Adding or Editing Servers

To add or edit servers, select **System Settings > Servers**. Click **Add** to create a new entry or to import servers from a CSV file.



Note

The Operations Manager server (“VsomServer”) is added by default and cannot be deleted. All servers are assigned the *Primary* HA role by default (see the [“High Availability” section on page 12-1](#)).



Tip

Select an existing entry to revise an existing server configuration (see the [“Server Settings” section on page 6-4](#) for more information).

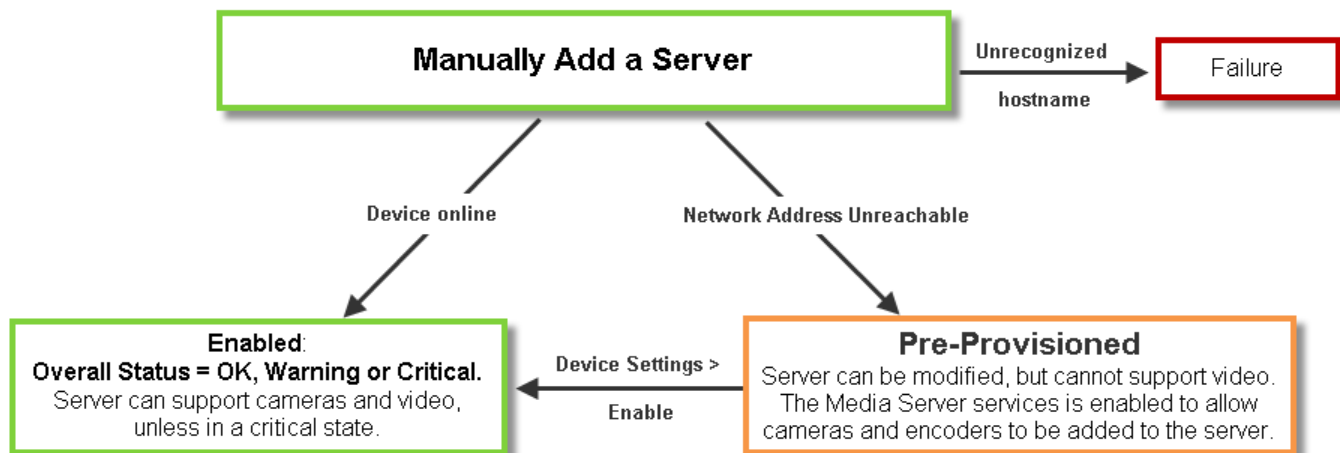
Refer to the following topics for more information:

- [Overview, page 6-10](#)
- [Pre-Provisioning Servers, page 6-11](#)
- [Prerequisites, page 6-11](#)
- [Adding or Editing a Single Server, page 6-11](#)
- [Importing or Updating Servers Using a CSV File, page 6-13](#)

Overview

To manually add a single server, open the server configuration page and click **Add**. Enter the server settings as described in the [“Adding or Editing a Single Server” section on page 11](#). If the server is not available on the network, it can be added in *pre-provisioned* state ([Figure 6-1](#)).

Figure 6-1 Adding a Server



Pre-Provisioning Servers

Pre-provisioning allows you to add a server before it is installed or available on the network. The server is waiting to be added to Cisco VSM and is not available for use. A pre-provisioned server can be modified, but cannot stream or record video.

- If a server is pre-provisioned, the Media server service is activated by default. This allows pre-provisioned cameras and encoders to be added to the pre-provisioned server.
- After the server is installed and available on the network, you can enable it by choosing **Device Settings > Enable** from the server configuration page. The server configuration must be complete, and Cisco VSM must be able to verify network communication or the *enable* action will fail.



Tip

Use **Bulk Actions** to enable multiple servers. See the [“Bulk Actions: Revising Multiple Servers”](#) section on page 6-19.

See the [“Viewing Server Status”](#) section on page 6-22 for more information.

Prerequisites

- The server(s) must be installed on a physical machine, or as a virtual machine (VM).
- Complete the server initial configuration (including network settings) using the Setup Wizard available in the browser-based Cisco VSM Management Console. See the [Cisco Video Surveillance Management Console Administration Guide](#) for more information.

Adding or Editing a Single Server

Procedure

To add a new server, complete the following procedure.



Note

The Operations Manager server (“VsomServer”) is added by default and cannot be deleted. All servers are assigned the Primary HA role by default. See the [“High Availability”](#) section on page 12-1.

- Step 1** Install the server and complete the **Initial Setup Wizard** using the browser-based Management Console.
 - [Cisco Physical Security UCS Platform Series User Guide](#)
 - [Cisco Physical Security Multiservices Platform Series User Guide](#)
 - [Cisco Video Surveillance Virtual Machine Deployment and Recovery Guide for UCS Platforms](#)
 - [Cisco Video Surveillance Management Console Administration Guide](#).
- Step 2** Log on to the Operations Manager.
 - See the [“Logging In and Managing Passwords”](#) section on page 1-18.
 - You must belong to a User Group with permissions for *Servers & Encoders*. See the [“Adding Users, User Groups, and Permissions”](#) section on page 4-1 for more information.
- Step 3** Select **System Settings > Servers**.
- Step 4** Click **Add**.

**Tip**

To edit a server, click an existing entry to highlight it, then refer to the [“Server Settings” section on page 6-4](#).

**Tip**

If you are adding a server that was previously configured in Cisco VSM, you will be prompted to import or discard any camera configurations or recordings that exist on the server.

Step 5 (Add only) Complete the initial server setup:

Figure 6-2 Add a Server

Add Server

★ Hostname/IP: vsm-server-ca1

Username: localadmin

★ Password: ••••••••

★ Name: CA campus primary server

★ Install Location: System

Add Cancel

Table 6-9 Server Settings

Setting	Description
Hostname/IP	The hostname or IP address used by the Operations Manager to access the server.
Username	The default username for all servers is <code>localadmin</code> . The username cannot be changed.
Password	The server password. Tip The server password is initially defined using the Cisco Video Surveillance Management Console interface. See the “General Information Settings” section on page 6-4 and the Cisco Video Surveillance Management Console Administration Guide for more information.
Name	A meaningful name for the server. For example, <i>Primary Server</i> or <i>Campus A Server</i> .
Install Location	The location where the server is installed. The location determines the cameras and users that can access the server. See the “Creating the Location Hierarchy” section on page 5-1 for more information.

d. Click **Add**.

- If the validation is successful, continue to [Step 6](#).
- If the server cannot be found on the network, an error message appears.
 - Verify the server hostname and login credentials and return to [Step 4](#) to try again.

- You can also *Pre-Provision* the server, meaning it is added to the configuration but remains non-functional. Select **Device Setting > Enable** when the configuration is complete, or use **Bulk Actions** to enable multiple server (see the [“Bulk Actions: Revising Multiple Servers” section on page 6-19](#)).
- Step 6** (Optional) Enter or revise the additional settings, if necessary, as described in the [“Server Settings” section on page 6-4](#).
- Step 7** Assign cameras and encoders to the Media Server service on the server, if necessary. Cameras and encoders can be assigned to the Media Server even if the server is pre-provisioned.
- Step 8** Click **Save**.
-

Importing or Updating Servers Using a CSV File

Multiple servers can be imported using a *comma separated value* (CSV) file that includes configuration details for each device. This same method can be used to update existing server configurations.

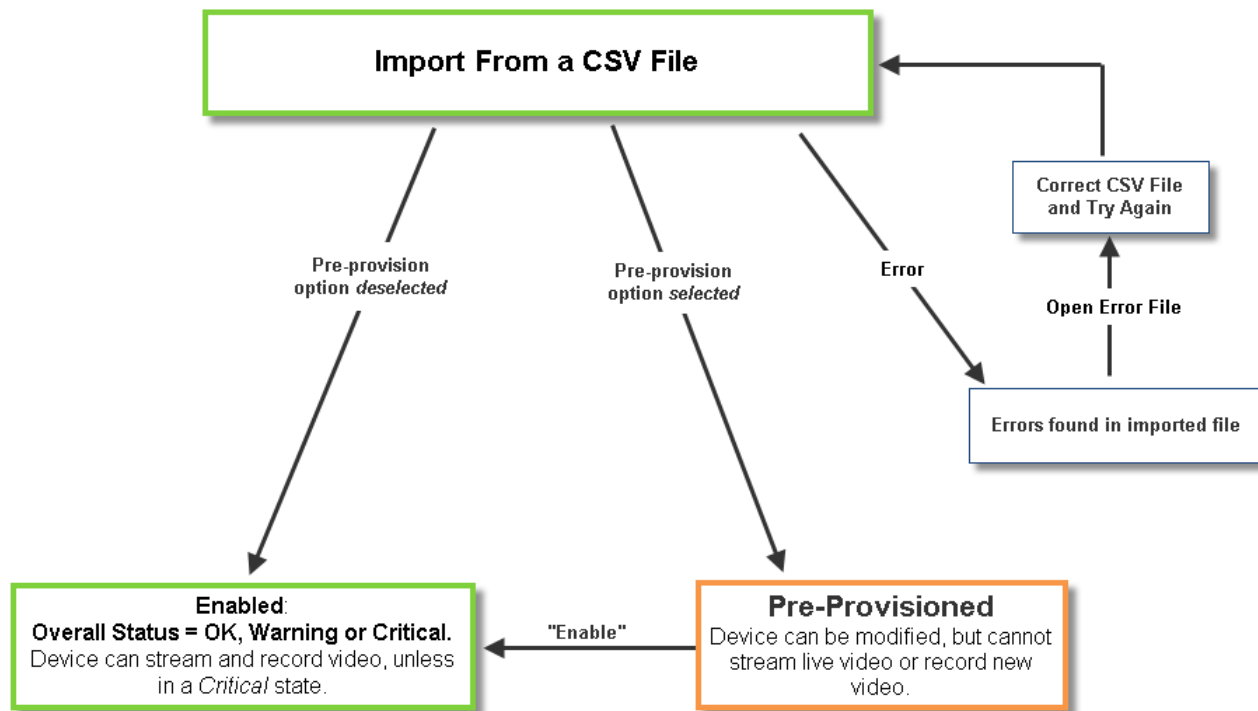
Refer to the following topics for more information:

- [Overview, page 6-13](#)
- [Usage Notes, page 6-14](#)
- [Creating the CSV File, page 6-15](#)
- [Importing the CSV File, page 6-16](#)

Overview

[Figure 6-3](#) summarizes the process to import devices from a CSV file. Devices can be added in Enabled state if all required configurations are included, or in Pre-Provisioned state if configurations are missing or if the devices are not yet available on the network. If an error occurs, correct the CSV file and try again.

Figure 6-3 Importing Servers from a CSV File



Usage Notes

- Servers can be pre-provisioned in Release 7.2 and higher.
- You can choose to retain the devices (cameras and encoders) that were previously associated with the server, or discard them. Any discarded devices must be re-added, if required.
 - Enabled cameras and encoders associated with the server are added to the Operations Manager.
 - You can also choose to Pre-Provision the devices, meaning they are added to the configuration but are not functional until available on the network. See the [“Adding Cameras from an Existing Media Server”](#) section on page 8-38 for more information.
 - Soft deleted cameras are added to the Operations Manager in the soft-deleted state, which allows recordings to be accessed.
 - Disabled cameras are not added to the Operations Manager configuration.
 - See the [“Adding and Managing Cameras”](#) section on page 8-1 and the [“Adding Encoders and Analog Cameras”](#) section on page 11-1 for information about completing the configuration and enabling the devices.
- Entries with non-ASCII characters must be tab delimited. Entries that include only ASCII characters can be comma delimited.

Creating the CSV File

Create a file in plain text CSV format that can be opened and saved using Excel or OpenOffice Calc (Figure 6-4). Blank rows or rows beginning with “//” are ignored.



Tip

To download a sample import file, launch the import wizard as described in the “[Importing the CSV File](#)” section on page 6-16. Click the **Download Sample** button in the second step of the wizard to obtain a sample file (see [Step 4](#)).

Figure 6-4 Example of a Server Import File

	A	B	C	D	E	F
1	Name	Host name or IP address	Install location path	localadmin password	Server Role	Tags
2	//<required>	//<required>	//<required>	//<required>	//<One of primary_server/redundant_server/t/><Optional>	
3	// UMS-1	10.10.10.10	USA.CA.SJ.28.Lobby	secur4u	primary_server	Sample tags
4						
5	// Supported Delimiters - Contents that have non-ASCII characters, need to be delimited by tab. If the content contains only ASCII, comma delimiter should be used					
6	//Any lines starting with "//" are treated as comments					

The CSV file can be created in plain text using a program such as Excel or OpenOffice Calc. For example, in Excel, create the file and then choose **Save As > Other formats**. Select **CSV (Comma delimited)** for the *Save as type*.

The fields (columns) must follow a specific format, which is shown in the downloadable sample. [Table 6-10](#) describes the information required in each field.

Table 6-10 Server Import File Field Descriptions

Content	Required/Optional	Description
Comment //	Optional	Blank rows or lines/cells starting with “//” are treated as comments and ignored.
Name	Required	Enter the server name For example: Primary Server
Host name or IP address	Required	The network address for the physical or virtual machine.
Install Location Path	Required	Enter the location where the server is physically installed, or the physical location of the cameras and encoders supported by the camera. For example: USA.CA.SJ.28.Lobby Tip To view the location path, go to System Settings > Locations and highlight the location name.


Table 6-10 Server Import File Field Descriptions (continued)

Content	Required/ Optional	Description
localadmin password	Required	<p>The password configured on the server to provide network access from the Operations Manager.</p> <ul style="list-style-type: none"> This setting changes the Operations Manager's understanding of the server password. This does not change the actual server password. See the Cisco Video Surveillance Management Console Administration Guide for instructions to change the server password. See the “Access Information Settings” section on page 6-5 to revise the credentials after the server is added to the system. <p>Note The default username for all servers is <code>localadmin</code>. The username is read-only and cannot be changed.</p>
Server Role	Required	<p>The high-availability role of the server. The options are:</p> <ul style="list-style-type: none"> <code>primary_server</code> <code>redundant_server</code> <code>failover_server</code> <code>long_term_storage_server</code> <p>See the “Understanding Redundant, Failover, and Long Term Storage Servers” section on page 12-4 for more information.</p>
Tags	Optional	Keywords used by the <i>Find</i> field.

Importing the CSV File

Complete the following procedure to import servers using a CSV file.

Procedure

-
- Step 1** Create the CSV file containing details for each server.
- See the “[Creating the CSV File](#)” section on page 6-15.
- Step 2** Select **System Settings > Servers**.
- Step 3** Choose **Add**  and **Import servers from file**.
- Step 4** Complete each *Import Step* as described below:
- Import Step 1 - Retain Device(s)*

(Cameras only) Select the **Retain** box if existing device(s) found on the server during import should be retained. If selected:

 - Enabled cameras and encoders associated with the server are added to the Operations Manager.
 - Soft deleted cameras are added to the Operations Manager in the soft-deleted state, which allows recordings to be accessed.
 - Disabled cameras are not added to the Operations Manager configuration.

Select **Pre-Provision** to pre-provision the devices:

 - Cameras and encoders associated with the server are added in the pre-provisioned state.


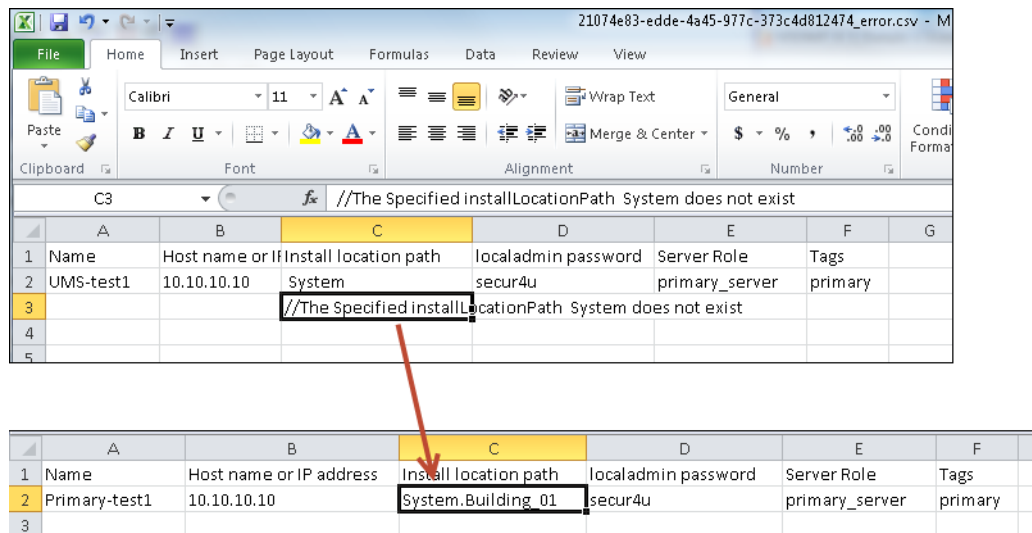
- *Pre-provisioned* devices must be enabled once the configuration is complete. See the “[Adding and Managing Cameras](#)” section on page 8-1 and the “[Adding Encoders and Analog Cameras](#)” section on page 11-1 for information about completing the configuration and enabling the devices.
- b. *Import Step 2 - Download Sample*
(Optional) Click **Download Sample** to download a sample CSV import file. Use this sample to create the import file as described in the “[Creating the CSV File](#)” section on page 6-15. Click **Next**.
- c. *Import Step 3 - File Upload:*
Click  to select the CSV file from a local or network disk. Click **Upload**.
- d. *Import Step 4 - Processing:*
Wait for the import process to complete.
- e. *Import Step 5 - Results Success:*
 - If a *success* message appears, continue to [Step 5](#).
 - If an *error* message appears, continue to [Step 4 f](#).
- f. If an *error* message appears ([Figure 6-5](#)), complete the following troubleshooting steps:
 - Click **Download Annotated CSV**, save the error file and open it in Excel or OpenOffice Calc.
 - Correct the annotated errors and save the revised file in the .csv format.
 - Correct the CSV file in the //Error rows ([Figure 6-5](#)).
 - Click **Start Over** to re-import the fixed file.
 - Return to [Step 3](#) and re-import the corrected CSV file.

Figure 6-5 Import Error File


	A	B	C	D	E	F	G
1	Name	Host name or IP	Install location path	localadmin password	Server Role	Tags	
2	UMS-test1	10.10.10.10	System	secur4u	primary_server	primary	
3			//The Specified InstallLocationPath System does not exist				
4							
5							

	A	B	C	D	E	F
1	Name	Host name or IP address	Install location path	localadmin password	Server Role	Tags
2	Primary-test1	10.10.10.10	System.Building_01	secur4u	primary_server	primary
3						

Step 5 Click **Close** once the import process is complete.

Step 6 View the device status to determine if additional configuration is required. See the “[Device Status: Identifying Issues for a Specific Device](#)” section on page 13-8.

- Step 7** Complete the camera and encoder configurations to enable the devices, if necessary. See the [“Adding and Managing Cameras” section on page 8-1](#) and the [“Adding Encoders and Analog Cameras” section on page 11-1](#) for more information.
-

Deleting a Server

To remove a server you must remove all devices and other associations with the server, or the job will fail.

Usage Notes

- You can only delete a server that is not associated with cameras or encoders.
- The Operations Manager server (“VsomServer”) cannot be deleted.
- When a camera is moved to a Media Server on a different server, recordings are begun again. Any existing recordings remain on the old Media Server. If the old Media Server is deleted, any associated recordings are removed.
- If the server is unreachable, and no HA servers are configured, the user is given an option to force-delete the server, which also deletes all camera configurations and recordings. All associated cameras must be re-added to Cisco VSM, and all recordings are lost.
- See the [“Accessing the Camera Settings” section on page 8-42](#) for instructions to change a camera’s Media Server setting.

Procedure

- Step 1** Log on to the Operations Manager.
- You must belong to a User Group with permissions for *Servers & Encoders*.
- Step 2** Verify that all cameras and encoders associated with the Media Server are switched to a different Media Server.
- The camera’s existing recordings will remain on the old server.
 - See the [“Accessing the Camera Settings” section on page 8-42](#) for instructions to change a camera’s Media Server setting.
- Step 3** Click **System Settings > Servers**.
- Step 4** Select the server name.
- Step 5** Click **Delete**.
- Step 6** Click **OK** to confirm.
- Step 7** Wait for the *Job* to complete.
-

Bulk Actions: Revising Multiple Servers

Bulk Actions allows you to change the configuration or take actions for multiple servers. For example, you can set the NTP server, repair the configurations, change the password used to access the servers, change the location, or delete the servers.

To begin, filter the devices by attributes such as name, tags, location, status, or issue. You can then apply changes to the resulting devices.

Requirements

- Users must belong to a User Group with permissions to manage *Servers and Encoders*.
- Only super-admin users can apply the **Change Password** option using Bulk Actions. Non-super-users must use the device configuration page to change one device at a time.
- See the [“Adding Users, User Groups, and Permissions” section on page 4-1](#) for more information.

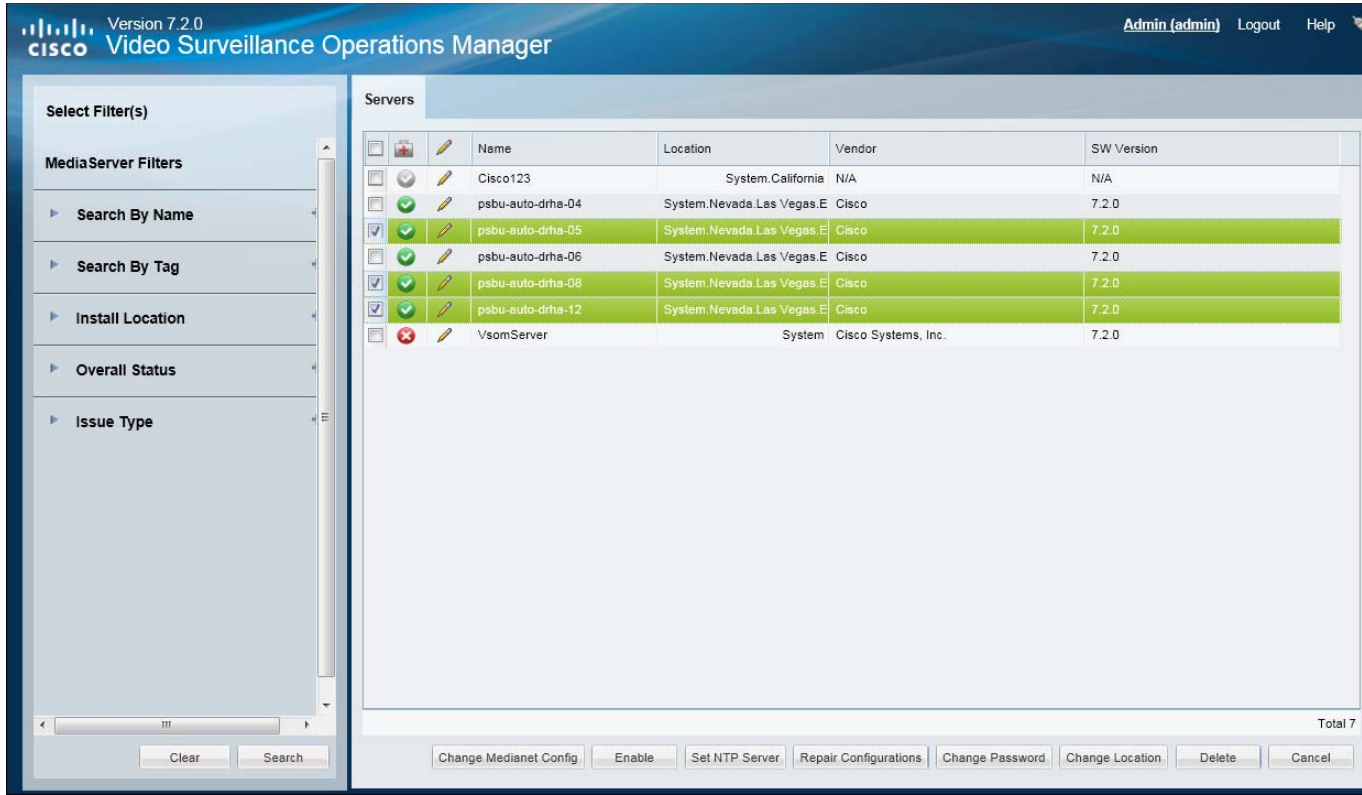
Related Topics

- [Bulk Actions: Revising Multiple Encoders, page 11-11](#)
- [Bulk Actions: Revising Multiple Cameras, page 8-85](#).

Procedure

-
- Step 1** Select **System Settings > Servers**.
- Step 2** Click **Bulk Actions** (under the device list) to open the Bulk Actions window ([Figure 6-6](#)).

Figure 6-6 Bulk Actions Window





Step 3 Click the  icon next to each field to select the filter criteria.

Table 6-11 Bulk Action Filters

Filter	Description
Search by Name	Enter the full or partial name and press Enter . For example, enter “Door” or “Do” to include all device names that include “Door”.
Search by Tag	Enter the full or partial tag string and press Enter .
Install Location	Select the location where the devices are installed.
Overall Status	Select the administrative states for the devices: Enabled (OK, Warning or Critical) —The device is enabled, although it may include a <i>Warning</i> or <i>Critical</i> event. Tip See the “Device Status: Identifying Issues for a Specific Device” section on page 13-8 for more information.
Issue Type	Select the issues that apply to the device.

Step 4 Click **Search**.

Step 5 (Optional) Click the  icon to view and edit the device status and configuration settings.

Step 6 Select the devices that will be affected by the action.

- Choose the *Select All* check box to select ALL servers matched by the filters, including the servers not shown in the grid.
- Use CTRL-CLICK and SHIFT-CLICK or to select multiple items.

Step 7 Click an *Action* button.

- For example, Set NTP Server, Set SMTP Server, Repair Configurations, Change Password, Change Location, etc.



Note Only super-admin users can apply the **Change Password** option using Bulk Actions.

Step 8 Follow the onscreen instructions to enter or select additional input, if necessary.

- For example, *Set SMTP Server Template* requires that you enter the server settings.

Step 9 Refer to the Jobs page to view the action status.

See the [“Understanding Jobs and Job Status” section on page 13-25](#).

Viewing Server Status

To view the status of a server, click the **Status** tab in the server configuration page (Figure 6-7).

Figure 6-7 Server Device Status

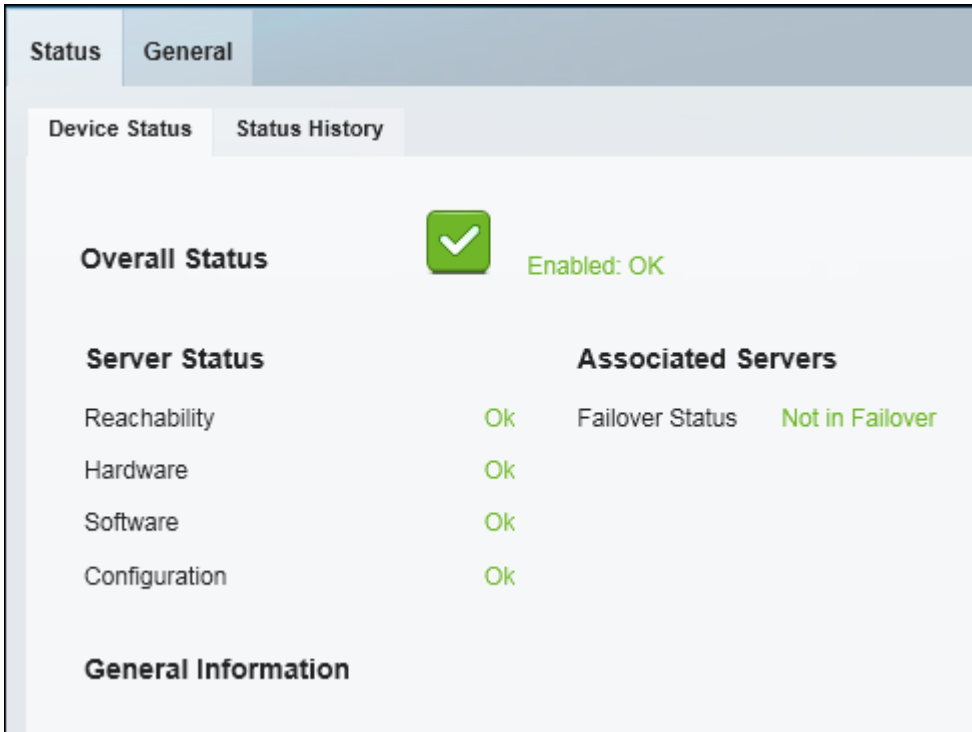


Table 6-12 Device States

State	Description
Enabled: OK	The device is operating normally. has no error.s
Enabled: Warning	A minor event occurred that did not significantly impact device operations.
Enabled: Critical	An event occurred that impacts the device operation or configuration.
Pre-provisioned	The device is added to the configuration but not available on the network. The device is waiting to be added to Cisco VSM and is not available for use. A pre-provisioned device can be modified, but the cannot stream or record video until the configuration is complete and you choose Device Settings > Enable .

Usage Notes

- Click the **Status History** tab to view detailed information regarding the events or alerts that impact the Device Status. For example, if a *Synchronization* mismatch occurs, and the *Configuration* status changes from OK to a synchronization alert, click the Status History tab to view details for the errors that caused the mismatch. See the [“Viewing Device Error Details” section on page 13-13](#).

- Click **Reset Status** to clear status issues that do not automatically clear when the issue is resolved (see the [“Resetting the Server Device State” section on page 6-23](#)).
- See the following options to repair configuration issues or reset the device state:
 - [Repairing the Configuration or Restarting the Server, page 6-23](#)
 - [Resetting the Server Device State, page 6-23](#)
- See the [“Viewing the Server HA Status” section on page 12-22](#) for more information on the Associated Servers status.

Resetting the Server Device State

Click the **Reset Status** button on the server *Status* page to clear device status and configuration issues.

- Clears status issues that do not automatically clear when the issue is resolved. For example, an issue that causes a `coredump` might still display a critical error in the Operations Manager even if the issue is resolved.
- Performs a **Repair Configuration** that synchronizes the server configuration with the Operations Manager (mismatched configurations on the Media Server are replaced with the Operations Manager settings). See the [“Repairing the Configuration or Restarting the Server” section on page 6-23](#).



Note

- Any unresolved configuration issues will reappear after the reset.
- Only the server *state* is reset, not the device alerts or events. You must still acknowledge or clear any alert using the Cisco Video Surveillance Safety and Security Desktop.
- To access the **Reset Status** button, you must be a *Super User* or belong to a user group assigned to the *super_admin_role* (a super-user is anybody that has all permissions at the root location). See the [“Adding Users, User Groups, and Permissions” section on page 4-1](#) for more information.

Repairing the Configuration or Restarting the Server

From the **General** tab, select the **Device Setting** menu and select one of the actions described in [Table 6-13](#).

Table 6-13 **Server Operations**

Operation	Description
Replace Configurations	<p>Overwrite all configuration settings on the server with the settings in the Operations Manager.</p> <p>See the “Synchronizing Device Configurations” section on page 13-17 for more information.</p>


Table 6-13 **Server Operations (continued)**

Operation	Description
Repair Configurations	Push only the configuration changes required to correct a mismatched field. Changes are pushed from the Operations Manager to the Media Server See the “Synchronizing Device Configurations” section on page 13-17 for more information.
Restart	Reboot the server and trigger a synchronization (<i>Repair Configuration</i>). Note The restart period can last 1 minute or longer. During this time, the Cisco VSM system will be offline and inaccessible.

Operations Manager Advanced Settings

SMTP settings are the only available Operations Manager-specific settings in this release.

SMTP Management Settings

Enter the **SMTP Management** settings (under the **Advanced**  icon) to send server-generated emails. For example, the SMTP Server is used to send Health Notifications, as described in the [“Health Notifications”](#) section on page 13-14.

Usage Notes

- The SMTP settings are enabled and required if the Operations Manager application is enabled on the server.
- SMTP settings can only be set for the Operations Manager server (“VsomServer”).
- SMTP changes using the browser-based Cisco VSM Management Console Management page are reflected in the Operations Manager configuration.

Table 6-14 **SMTP Settings**

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



CHAPTER 7

Configuring Media Server Services

A Media Server is a service that runs on a physical or virtual Cisco Video Surveillance server. The Media Server service provides video streaming, recording and storage for the cameras and encoders associated with that server. Media Servers can also be configured for high availability, and provide Redundant, Failover, and Long Term Storage options for other Media Servers.

Refer to the following topics for more information.


Contents

- [Overview, page 7-2](#)
- [Requirements, page 7-2](#)
- [Summary Steps to Add, Activate, and Configure a Media Server, page 7-3](#)
- [Media Server Settings, page 7-4](#)
 - [High Availability Options, page 7-5](#)
 - [Partition Settings, page 7-5](#)
 - [Storage Management Settings, page 7-6](#)
 - [Media Server Properties, page 7-6](#)
- [Viewing Media Server Status, page 7-8](#)

Overview

A Media Server is a service that runs on a physical or virtual Cisco Video Surveillance server. Media Servers perform the following functions:

- Process and store digital video streams from network cameras.
- Deliver video streams to user workstations.
- Manage the serial ports and encoders used to connect analog cameras and digitize the analog video from those cameras.

To add Media Servers, enable the Media Server service when setting up the physical or virtual server. Then use the Operations Manager to add the server, activate the Media Server service, and configure Advanced  settings, such as the high-availability role, if necessary. You can then associate cameras and other attributes to the Media Server and use the Media Server for video streaming, storage and playback.

Each deployment can have a single instance of the Operations Manager service, and multiple Media Servers. One Media Server instance can run on the same server as the Operations Manager server. Additional Media Servers (enabled on separate servers) are assigned to the Operations Manager.

Requirements


Before you begin, verify that the following requirements are met.

Table 7-1 Media Server Requirements


Requirements	Requirement Complete? (✓)
You must belong to a user group with <i>Servers & Encoders</i> permissions. See the “Adding Users, User Groups, and Permissions” section on page 4-1 for more information.	<input type="checkbox"/>
<p>A physical or virtual server that has the Media Server service enabled.</p> <ul style="list-style-type: none"> • Log in to the browser-based Cisco Video Surveillance Management Console to complete the Initial Setup Wizard and enable the Media Server service. • A single physical or virtual server can host both the Media Server and Operations Manager applications (called a co-located server). • Deployments can include multiple Media Servers. <p>See the following for more information:</p> <ul style="list-style-type: none"> • Physical Servers: <ul style="list-style-type: none"> – (Systems pre-installed with Release 7.2) See the Cisco Physical Security UCS Platform Series User Guide for more information. – (Systems pre-installed with Release 7.0.0 or 7.0.1) See the Cisco Physical Security Multiservices Platform Series User Guide for more information. • Virtual Machines—See the Cisco Video Surveillance Virtual Machine Deployment and Recovery Guide for UCS Platforms for instructions to install the server software .ova image as a virtual machine (VM). • Initial Setup—Cisco Video Surveillance Management Console Administration Guide. 	<input type="checkbox"/>

Summary Steps to Add, Activate, and Configure a Media Server

The following steps summarize how to add or update a single Media Server.

	Step	More Information
Step 1	Install and configure a Cisco VSM server.	<ul style="list-style-type: none"> • Cisco Physical Security UCS Platform Series User Guide • Cisco Physical Security Multiservices Platform Series User Guide • Cisco Video Surveillance Virtual Machine Deployment and Recovery Guide for UCS Platforms • Cisco Video Surveillance Management Console Administration Guide.
Step 2	Enable the Media Server service using the <i>Initial Setup Wizard</i> .	Cisco Video Surveillance Management Console Administration Guide .
Step 3	Log on to the Operations Manager.	Logging In and Managing Passwords, page 1-18 .
Step 4	Add the server.	Configuring Servers, page 6-1
Step 5	Under Services, select Media Server , if necessary. Note The Media Server services is enabled by default, even if the server is pre-provisioned. This allows cameras and encoders to be associated with the Media Server.	Services, page 6-5
Step 6	(Optional) Click the Advanced  icon to configure additional options.	<ul style="list-style-type: none"> • Media Server Settings, page 7-4 <ul style="list-style-type: none"> – High Availability Options, page 7-5 – Partition Settings, page 7-5 – Storage Management Settings, page 7-6 – Media Server Properties, page 7-6
Step 7	Add cameras and encoders and associate the devices with the Media Server.	<ul style="list-style-type: none"> • Adding and Managing Cameras, page 8-1 • Adding Encoders and Analog Cameras, page 11-1

Media Server Settings

Refer to the following topics for descriptions of the Media Server **Advanced**  settings:

- [High Availability Options, page 7-5](#)
- [Partition Settings, page 7-5](#)
- [Storage Management Settings, page 7-6](#)
- [Media Server Properties, page 7-6](#)

Accessing the Media Server Advanced Settings


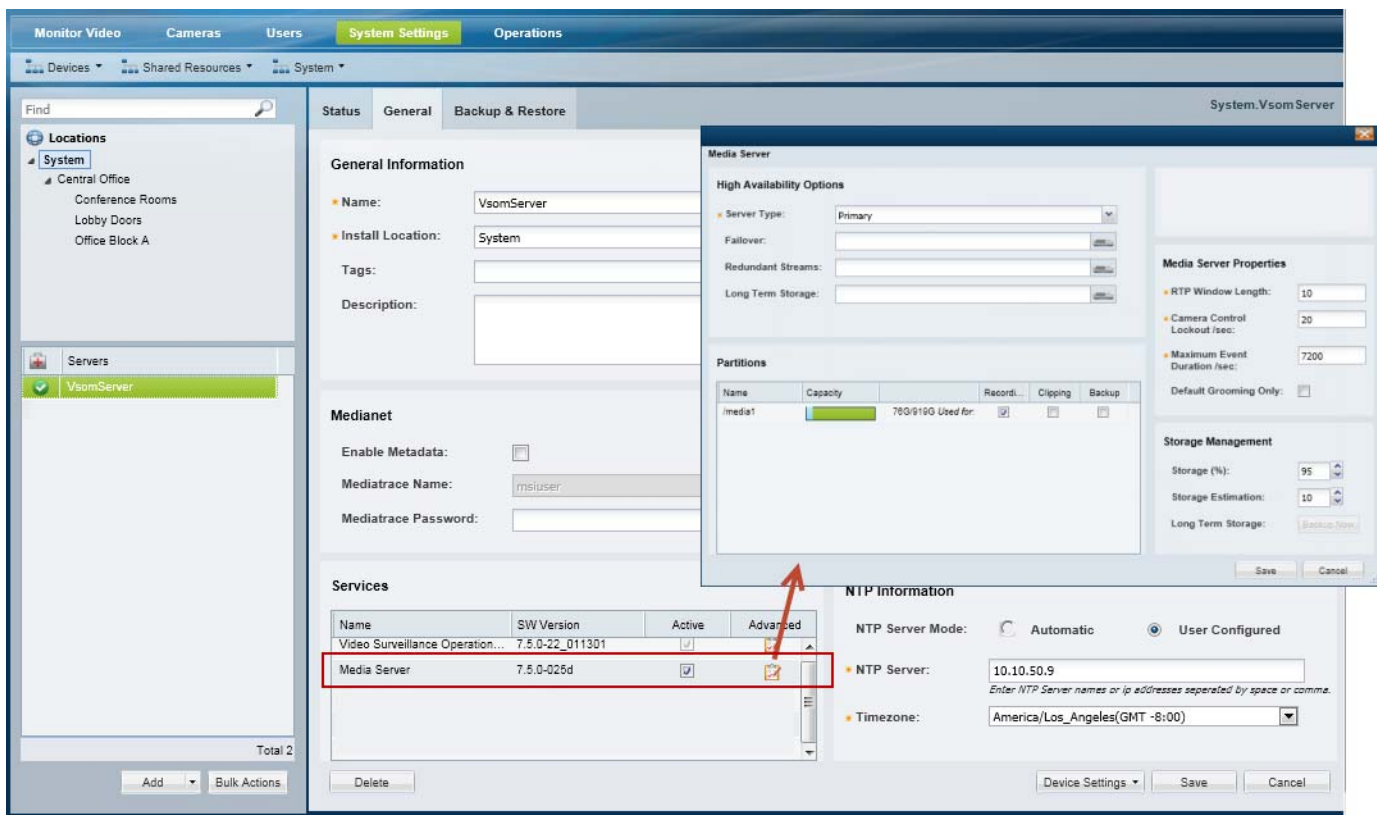
1. Select the server that hosts the Media Server service.
2. Under Services, click the **Advanced**  icon ([Figure 7-1](#)).
3. In the pop-up window, enter the available settings as described in this document ([Figure 7-1](#)).

Figure 7-1 Media Server Advanced Settings



High Availability Options


Use the **High Availability** options (under the **Advanced**  icon) to define the HA servers that support the Primary and Redundant servers ([Figure 7-1](#)):

Table 7-2 **High Availability Options**

Field	Settings
Failover	The Media Server that will assume the functionality of the Primary server if the Primary server goes offline.
Redundant Streams	The server used to record, store, and play back redundant video streams. For example, the Redundant Streams server can be used to manage Steam B from a camera.
Long Term Storage	The server used to store recorded video (continuous or motion events) for a long period of time.



Note

- For complete instructions, see the [“High Availability” section on page 12-1](#).
- Media Servers are assigned the *Primary* HA role by default.
- Each server supports only a single server type: Primary, Failover, Redundant Streams and Long Term Storage
- Primary servers can be configured with Failover, Redundant, and Long Term Storage servers. Redundant servers can be configured with a Long Term Storage server.

Partition Settings


Click the **Advanced**  icon and select the **Partitions** options to define the type of files that are saved to each available hard disk partition ([Figure 7-1](#)).

Table 7-3 **Hard Disk Partition Usage**

Field	Settings
Recording	The partition(s) used for video recordings generated by cameras associated with the Media Server.
Clipping	The partition(s) used for video clips created by a user. Note If multiple partitions are selected, the partition with the most available space is used to create video clips. CVA/CVX clips are downloaded immediately to the client workstation and not saved on the server. MP4 clips are saved on the server for 24 hours, and then deleted if they have not been downloaded. See the “Creating, Viewing and Managing Video Clips” section on page 2-17 for more information.
Backups	The partition(s) used for system backup files.

Storage Management Settings

Click the **Advanced**  icon and select the **Storage Management** settings to define how the storage space on a volume is used (Figure 7-1).

Table 7-4 *Storage Management*

Field	Settings
Storage (%)	<p>The maximum amount a disk can be full before it is declared unusable for any further recording. When the disk reached this percentage, the 200 oldest media files are groomed (deleted), until the free disk space is less than the Storage (%).</p> <ul style="list-style-type: none"> The maximum (and default) value is 98% (also the default). We recommend keeping this setting at or below the default value. 0% means that the repositories are not available to store video archives. <p>For example, if the <i>Storage %</i> is set to 90%, and a camera template <i>Retain event recordings</i> setting is Max Possible, event recordings will be deleted once the disk repositories are 90% full.</p>
Storage Estimation(%)	<p>This field defines the amount of storage space that must be available on the Media Server to start a recording if the Verify Recording Space option is enabled in a camera or template configuration. The Media Server must have this amount of storage space available or the recording will not start.</p> <p>For example, if a camera is configured to record a continuous H264 stream at 15mbps for 30 days, the Media Server would first verify that there is enough free disk space for the full recording length (30 days). If not, then recording will not start. In this example, 15 mbps of video uses approximately 2 megabytes of storage space per second, so 30 days of recording would require roughly 5 terabytes of disk storage.</p> <p>See the “Streaming, Recording and Event Settings” section on page 8-49 for more information on the Verify Recording Space option.</p>
Long Term Storage	<p>Click Backup Now to save recorded events to the LTS server used to store recorded video. Backups are removed from the original server when they are transferred to the LTS server.</p> <p>Note This button is enabled only if an LTS server is configured. See the “High Availability” section on page 12-1 for more information.</p>


Media Server Properties

The Media Server Properties define the following.

Table 7-5 *Media Server Properties*

Field	Settings
RTP Window Length	<p>The maximum number of packets the Media Server buffers per stream to determine packet loss (before declaring a lost packet). This is also known as the jitter window length. This setting may need to be changed on a system with excessive packet delay on the network.</p> <p>Note This value is normally set to 1 but may need to be increased on networks where packets can get delayed.</p>

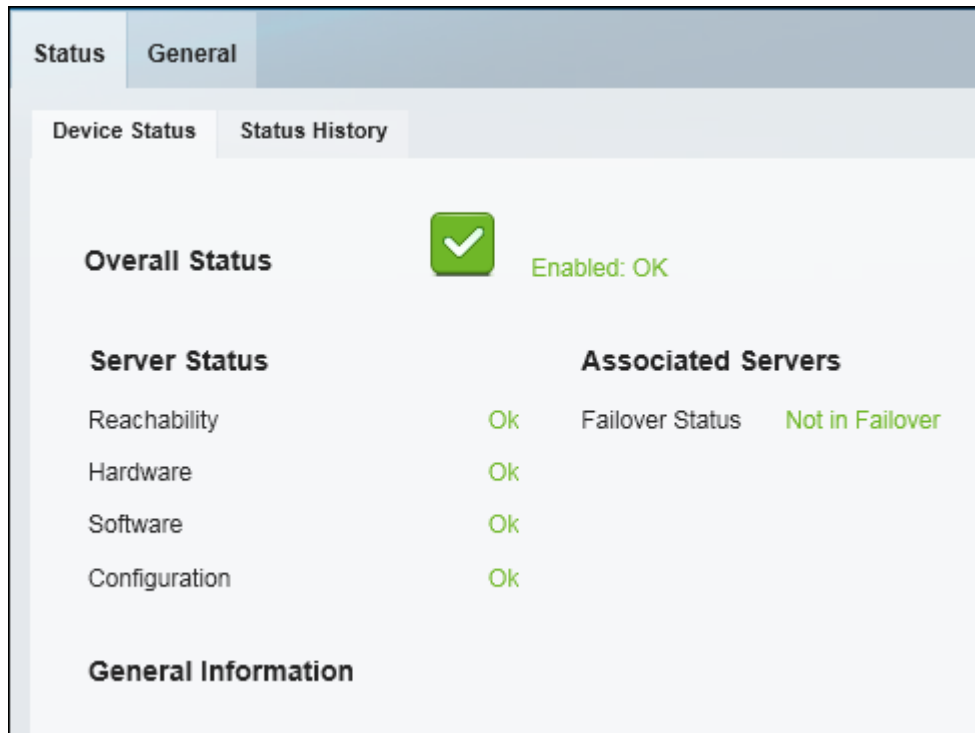
Table 7-5 Media Server Properties (continued)

Camera Control Lockout / sec	<p>Designates the number of seconds that a lower priority user has to wait before being able to move the camera after a higher priority user stops using the PTZ controls. This value is the default for all cameras assigned to a Media Server unless the camera <i>When Manual PTZ idle for</i> setting is defined in the camera <i>PTZ Advanced Settings</i>.</p> <p>For more information, see the following:</p> <ul style="list-style-type: none"> • Defining the User Group PTZ Priority, page 8-69 • PTZ Advanced Settings, page 8-76
Maximum Event Duration / sec	<p>The maximum duration for a motion or other event recording. This option should be set to the maximum number of seconds of continuous activity that any camera in a deployment might capture. Valid values are integers 1 through 86400. The default value is 7200 seconds (2 hours).</p>
Default Grooming Only	<p>If selected, recordings will only be groomed (deleted) when a media partition reaches its maximum usage level (grooming will not be performed based on the expiry time).</p> <p>Note Use this option only if the server has adequate disk space and the recordings should be retained longer than the retention settings defined in the camera template configuration. For example, the <i>Retain continuous recordings</i> and <i>Retain event recordings</i> settings will not apply for the cameras assigned to the Media Server. See the “Streaming, Recording and Event Settings” section on page 8-49.</p> <div>  <p>Caution This option can prevent new recordings from starting if all disk space is used. See the Storage Estimation setting in the “Streaming, Recording and Event Settings” section on page 8-49.</p> </div>

Viewing Media Server Status

To view the status of a Media Server, click the **Status** tab in the server configuration page (Figure 7-2). See the “[Viewing Server Status](#)” section on page 6-22 for more information.

Figure 7-2 Media Server Device Status





CHAPTER 8

Adding and Managing Cameras

Refer to the following topics for information to add, configure, and manage cameras in a Cisco VSM deployment.



Note

- Always use the Operations Manager to configure cameras. Changes made directly to the camera are unknown to Cisco VSM and can result in incorrect device behavior.
 - The camera configuration pages may not display properly if the Internet Explorer (IE) compatibility view box is checked. Deselect this option, if necessary.
-

Contents

- [Overview, page 8-3](#)
 - [Understanding Network and Analog Cameras, page 8-3](#)
 - [Viewing Cameras, page 8-5](#)
 - [Requirements, page 8-3](#)
 - [Summary Steps, page 8-4](#)
- [Manually Adding Cameras, page 8-8](#)
 - [Overview, page 8-9](#)
 - [Manually Adding a Single Camera, page 8-12](#)
 - [Importing or Updating Cameras or Encoders Using a CSV File, page 8-17](#)
- [Discovering Cameras on the Network, page 8-22](#)
 - [Understanding Discovery and Auto-Configuration, page 8-22](#)
 - [Understanding Camera Conflicts, page 8-24](#)
 - [Enabling the Auto Configuration Defaults for a Camera Model, page 8-25](#)
 - [Discovering Non-Medianet Cameras on the Network, page 8-28](#)
 - [Cameras Pending Approval List, page 8-30](#)
 - [Discovering Medianet-Enabled Cameras, page 8-32](#)
- [Adding Cameras from an Existing Media Server, page 8-38](#)
- [Blacklisting Cameras, page 8-40](#)
 - [Blacklisting a Camera, page 8-40](#)

- Viewing Cameras in the Blacklist, page 8-41
- Removing a Camera From the Blacklist, page 8-41
- Editing the Camera Settings, page 8-42
 - Accessing the Camera Settings, page 8-42
 - General Settings, page 8-45
 - Streaming, Recording and Event Settings, page 8-49
 - Image Settings, page 8-57
 - Configuring the High Availability Options for a Camera or Template, page 8-58
- Deleting Cameras, page 8-59
- Changing the Camera or Encoder Access Settings (Address and Credentials), page 8-61
- Viewing Camera and Encoder Status, page 8-63
- Configuring Camera PTZ Controls, Presets, and Tours, page 8-65
 - PTZ Requirements, page 8-66
 - PTZ Camera Configuration Summary, page 8-67
 - Defining the User Group PTZ Priority, page 8-69
 - Using Camera PTZ Controls, page 8-70
 - Configuring PTZ Presets, page 8-71
 - Configuring PTZ Tours, page 8-73
 - PTZ Advanced Settings, page 8-76
- Configuring Motion Detection, page 8-77
- Replacing a Camera, page 8-83
- Bulk Actions: Revising Multiple Cameras, page 8-85

**Note**

See also the “Upgrading Cisco Camera and Encoder Firmware” section on page 15-3.

Overview

Review the following topics for a basic understanding of camera configuration:

- [Understanding Network and Analog Cameras, page 8-3](#)
- [Requirements, page 8-3](#)
- [Summary Steps, page 8-4](#)
- [Viewing Cameras, page 8-5](#)
- [Viewing a List of Supported Cameras, page 8-7](#)

Understanding Network and Analog Cameras

Two types of cameras can be added to Cisco VSM:

- IP cameras (also called *network cameras*) are connect directly to the network and are added to Cisco VSM by entering the camera's IP address and other settings.
- Analog cameras are connected to an *encoder*. The encoder provides network connectivity and digitizes the analog video. See the [“Adding Encoders and Analog Cameras” section on page 11-1](#) for more information.

Requirements

Before you begin, verify that the following requirements are met.

Table 8-1 Requirements

Requirements	Requirement Complete? (✓)
You must belong to a user group with <i>Cameras</i> permission. See the “Adding Users, User Groups, and Permissions” section on page 4-1 for more information.	<input type="checkbox"/>
At least one Media Server must be enabled. See the “Configuring Media Server Services” section on page 7-1 for more information.	<input type="checkbox"/>
At least one supported network or analog camera must be installed on the network. See the “Viewing a List of Supported Cameras” section on page 8-7 for more information.	<input type="checkbox"/>
Analog cameras also require an encoder for network connectivity and to digitize the analog video. See the “Adding Encoders and Analog Cameras” section on page 11-1 for more information.	<input type="checkbox"/>

Table 8-1 Requirements

Requirements	Requirement Complete? (✓)
The IP address used to access the device on the network.	<input type="checkbox"/>
Note All edge devices (such as cameras and encoders) must be added to a server using a local (non-NAT) address.	
The camera username and password used to access the device on the network.	<input type="checkbox"/>

Summary Steps

The following steps summarize how to add or update a video camera.

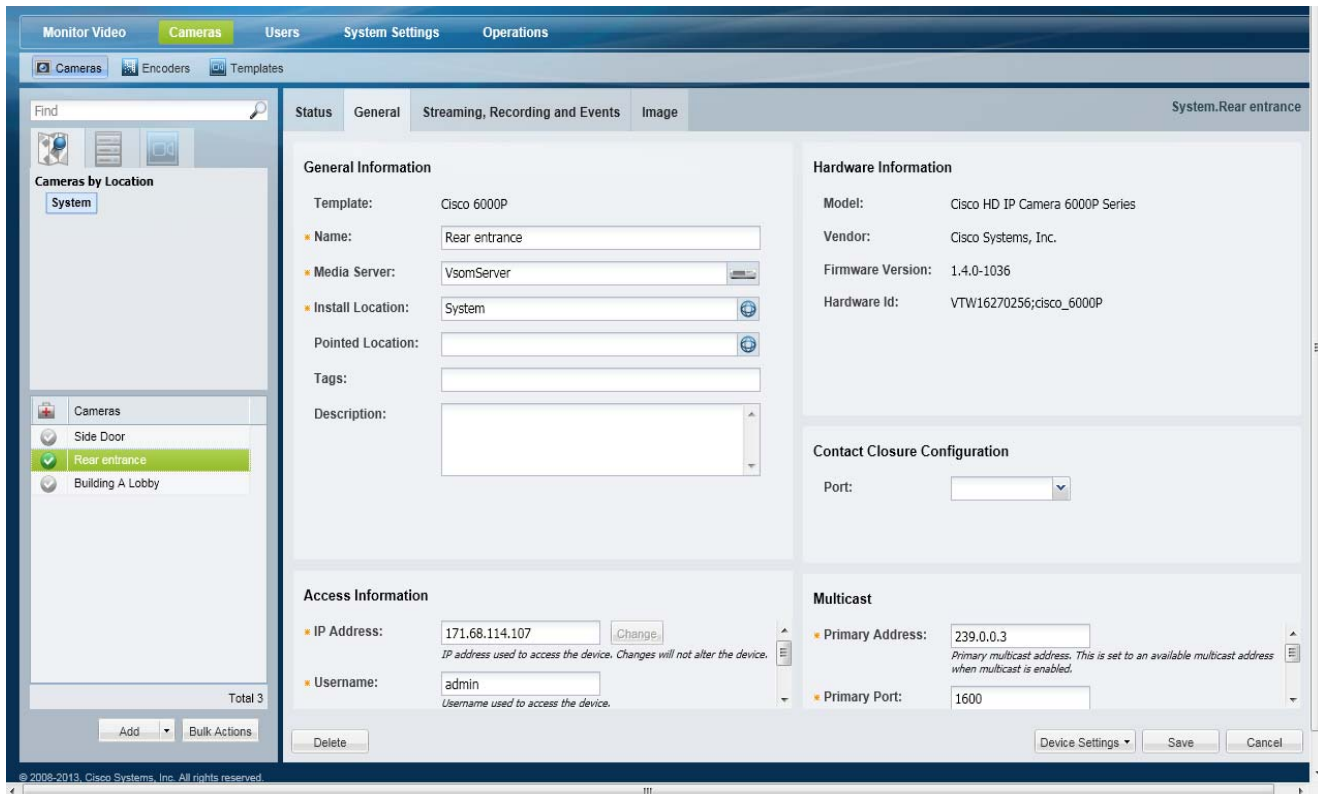
	Step	More Information
Step 1	Log on to the Operations Manager.	Logging In and Managing Passwords, page 1-18
Step 2	Configure recording schedules	<ul style="list-style-type: none"> • Defining Schedules, page 9-1
Step 3	(Optional) Add camera templates.	<ul style="list-style-type: none"> • Adding and Editing Camera Templates, page 10-1 • Configuring Continuous, Scheduled, and Motion Recordings, page 10-7
Step 4	(Optional) Add camera encoders to support analog cameras.	Adding Encoders and Analog Cameras, page 11-1
Step 5	Add one or more cameras.	Understanding the Methods to Add Cameras, page 8-9 <ul style="list-style-type: none"> • Manually Adding a Single Camera, page 8-12 • Importing or Updating Cameras or Encoders Using a CSV File, page 8-17 • Discovering Cameras on the Network, page 8-22 • Adding Cameras from an Existing Media Server, page 8-38
Step 6	Edit additional camera settings.	Editing the Camera Settings, page 8-42
Step 7	(Optional) Create a custom configuration for a single camera.	Creating a Custom Template for a Single Camera, page 10-5
Step 8	Configure the Image Settings, such as PTZ, motion detection, and brightness and contrast.	Image Settings, page 8-57 <ul style="list-style-type: none"> • Configuring Camera PTZ Controls, Presets, and Tours, page 8-65 • Configuring Motion Detection, page 8-77 • Photographic Controls, page 8-57
Step 9	Configure the high availability options.	Configuring the High Availability Options for a Camera or Template, page 8-58
Step 10	Create actions that are triggered by camera events.	“Using Advanced Events to Trigger Actions” section on page 10-11





Viewing Cameras

To display cameras already configured on the system, click **Cameras** and then choose the **Cameras** tab (Figure 8-1). You can view the cameras for a location, Media Server, or template by clicking one of the icons described below Figure 8-1.

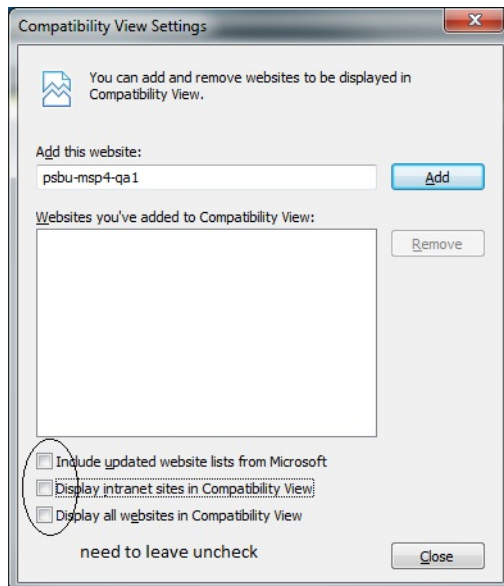
Click a camera name to view and edit the settings for that camera. Click a template name to edit the settings applied to all cameras associated with the template.

Figure 8-1 **Cameras Tab**



Tab	Description
 Cameras By Location	<p>Displays the cameras assigned to each location.</p> <p>For example, click the Cameras By Location tab  and then select a location name (Figure 8-1). The cameras assigned to that location are listed by name. Click a camera name to display and edit the camera settings.</p> <p>Tip See the “Creating the Location Hierarchy” section on page 5-1.</p>
 Cameras by Media Server	<p>Displays the cameras assigned to each Media Server.</p> <p>If only one Media Server is used, all cameras will be listed. See the “Configuring Media Server Services” section on page 7-1</p>
 Cameras By Template	<p>Displays the cameras assigned to each template.</p> <p>Tip The number next to the template name indicates the number of cameras assigned to the template. See the “Adding and Editing Camera Templates” section on page 10-1 for more information.</p>

Note The camera configuration pages may not display properly if the Internet Explorer (IE) compatibility view box is checked. Deselect this option, if necessary.



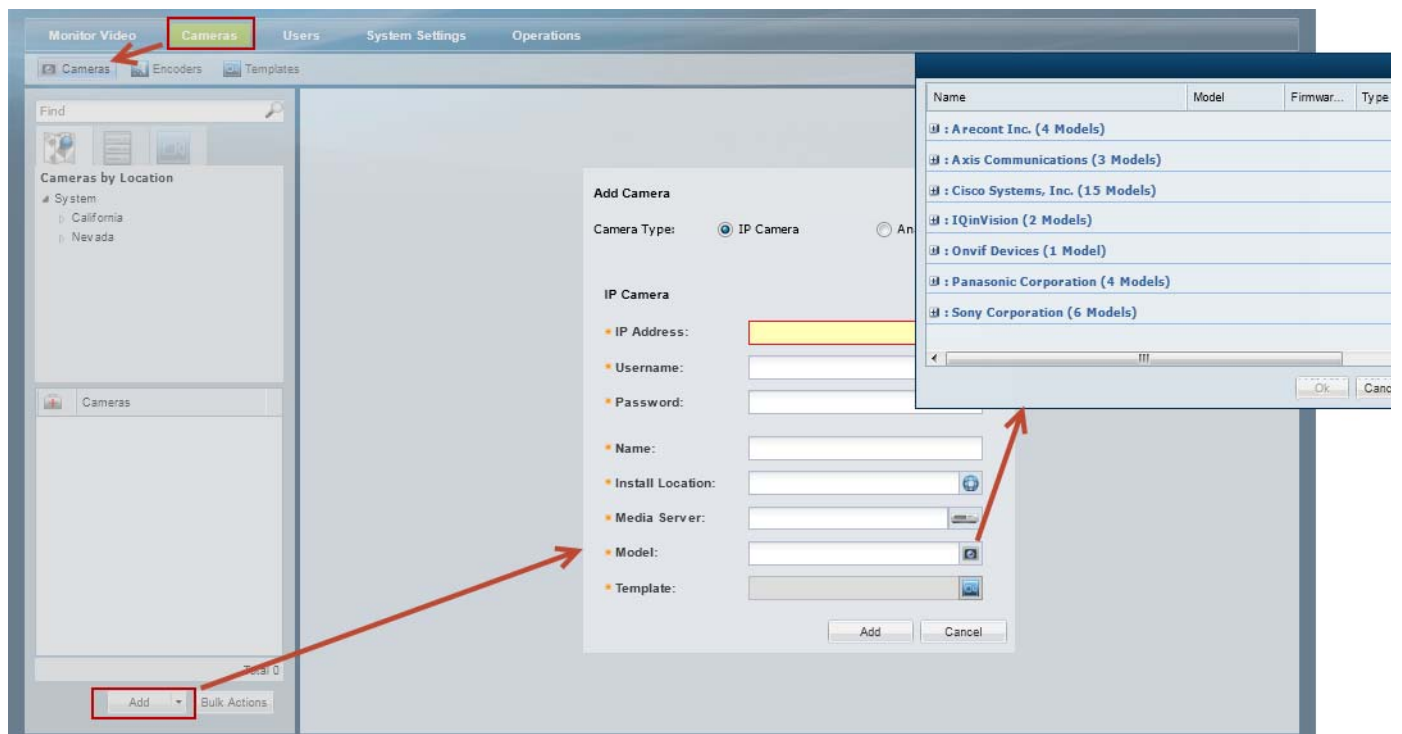
Viewing a List of Supported Cameras

To view the camera models supported in the Cisco Video Surveillance release you are using, open the model list when adding a camera.

Procedure

- Step 1** Click **Cameras** and then choose the **Cameras** tab (Figure 8-2).
- Step 2** Select the Camera Type: IP Camera or Analog Camera.
- Step 3** Click the **Model** field.
 - A list of supported cameras for that camera type and the Cisco Video Surveillance release is displayed (Figure 8-2).
- Step 4** Expand the Manufacturer names to view the list of supported models.

Figure 8-2 Supported Cameras



Manually Adding Cameras

Cameras can be added to Cisco VSM individually, or in groups. You can add cameras that are already installed, or *pre-provision* cameras that are not yet available on the network. Network cameras can also be discovered on the network and automatically configured or held offline until approved by an administrator. In addition, if you add a Media Server that was previously installed in another VSM 6.x or 7.x deployment, you will be prompted to add or discard any cameras configured on that server.

For more information, see the following topics:

- [Overview, page 8-9](#)
 - [Understanding the Methods to Add Cameras, page 8-9](#)
 - [Pre-Provisioning Cameras, page 8-10](#)
 - [Understanding Discovery and Auto-Configuration, page 8-22](#)
- [Manually Adding a Single Camera, page 8-12](#)
- [Importing or Updating Cameras or Encoders Using a CSV File, page 8-17](#)
 - [Creating the CSV File, page 8-18](#)
 - [Importing the CSV File, page 8-20](#)
- [Discovering Cameras on the Network, page 8-22](#)
 - [Enabling the Auto Configuration Defaults for a Camera Model, page 8-25](#)
 - [Discovering Non-Medianet Cameras on the Network, page 8-28](#)
- [Adding Cameras from an Existing Media Server, page 8-38](#)
 - [Adding Cameras From a 6.x or 7.x Media Server, page 8-38](#)
 - [Adding Unknown Cameras During a Media Server Synchronization, page 8-39](#)

Overview

Review the following topics to understand how cameras are added to Cisco VSM.

- [Understanding the Methods to Add Cameras, page 8-9](#)
- [Pre-Provisioning Cameras, page 8-10](#)
- [Cameras with Duplicate IP Addresses, page 8-10](#)
- [Understanding Discovery and Auto-Configuration, page 8-22](#)
- [Discovering Medianet-Enabled Cameras, page 8-32](#)

Understanding the Methods to Add Cameras

You can add cameras to Cisco VSM using one or more of the following methods:

Table 8-2 **Summary of Add Camera Methods**

Add Method	Description
Manually Adding a Single Camera, page 8-12	Add a single camera from the Camera configuration page. All required settings must be entered, although you can <i>pre-provision</i> the camera if it is not yet available on the network.
Importing or Updating Cameras or Encoders Using a CSV File, page 8-17	<p>Multiple cameras can be imported from a <i>comma separated value</i> (CSV) file that defines the camera configurations. You can choose to <i>pre-provision</i> the cameras, and add cameras with partial configurations, if necessary. This same method can be used to update existing camera configurations.</p> <p>Tip You can import network (IP) cameras, encoders and analog cameras.</p>
Discovering Cameras on the Network, page 8-22	<p>IP cameras that are added to the network can be discovered and added to Cisco VSM. You can manually trigger the discovery process, or use Medianet to automatically discover cameras as they are added.</p> <p>If the <i>auto configuration</i> feature is enabled for the camera model, the camera is automatically configured and enabled in Cisco VSM. If not, the camera is added to a <i>Cameras Pending Approval</i> list. The camera can then further configured and approved (enabled), or it can be moved to the camera blacklist, which excludes the device from future discovery.</p>

Table 8-2 Summary of Add Camera Methods (continued)

Add Method	Description
Adding Cameras From a 6.x or 7.x Media Server, page 8-38	<p>When an existing Media Server is added to Cisco VSM 7.x, you are prompted to keep or delete any cameras, recordings, or encoders that already exist on that server.</p> <p>For example, if a Media Server is migrated from a Cisco VSM 6.x deployment or re-purposed from a different Cisco 7.x system, you can choose to keep the cameras and recordings, or delete them.</p> <p>Note Cameras are kept in <i>pre-provisioned</i> state (see the “Viewing Camera and Encoder Status” section on page 8-63). Deleted cameras (and their associated recordings) are permanently removed and cannot be restored.</p> <p>See the following for related information:</p> <ul style="list-style-type: none"> Cisco Video Surveillance Migration Guide, Release 6.3.2 to 7.0
Adding Unknown Cameras During a Media Server Synchronization, page 8-39	In the unlikely event that unknown devices are discovered on the Media Server when the Media Server and Operations Manager configurations are synchronized, the devices are added to the <i>Cameras Pending Approval</i> list.

Pre-Provisioning Cameras

Pre-provisioning cameras allows you to add the cameras before they are installed or available on the network. The camera is waiting to be added to Cisco VSM and is not available for use. A pre-provisioned camera can be modified, but the camera cannot stream or record video.

After the camera is installed and available on the network, you can enable the camera by choosing **Enable** from the **Device Settings** menu. The camera configuration must be complete, and Cisco VSM must be able to verify network communication or the *enable* action will fail.

See the [“Viewing Camera and Encoder Status”](#) section on page 8-63 for more information.

Cameras with Duplicate IP Addresses

If a camera is added with a duplicate IP address (the address is the same as an existing camera), the new camera will display an *ID collision* issue. For example, cameras manually added will be placed in the *Enabled: Critical* state. Discovered cameras will be placed in the *Pending Approval* list.

To resolve the issue, do one of the following:

- Use the Operations Manager to configure the camera with an unused IP address.
- Directly connect to the camera interface and enter a unique IP address that is reachable by the Media Server, or ensure that the camera can receive a reachable address from a DHCP server.



Note

A direct camera connection may be necessary if the duplicate camera is on a different subnet than the Media Server, which causes the camera to be unreachable by the Media Server. To avoid this issue, place all devices including cameras on the same subnet. Refer to the camera documentation for instructions to revise the camera IP address or DHCP settings. The resulting IP address must be reachable by the Media Server to which it is assigned.

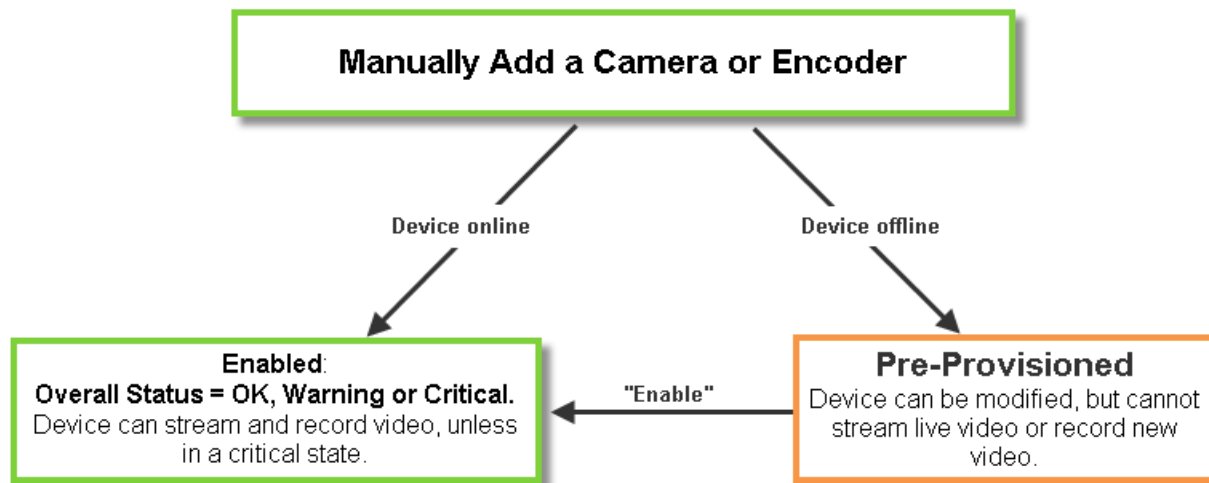
- Use the **Replace Camera** option to move the old camera's settings to the new camera. See the [“Replacing a Camera” section on page 8-83](#).
- Delete the camera and re-add it with a unique IP address. See the [“Deleting Cameras” section on page 8-59](#)).

Manually Adding a Single Camera

To manually add a single camera, open the camera configuration page and click **Add**. Enter the camera settings as described in the “[Procedure](#)” section on page 15.

If the device is not available on the network, it can be added in *pre-provisioned* state ([Figure 8-3](#)).

Figure 8-3 Manually Adding a Camera or Encoder



Note

All required fields must be complete to add a camera manually. You cannot submit a partial configuration.

Usage Notes

- To add the camera, you must choose a pre-defined configuration template and camera location. Only users with access permissions to that same location can view video from the camera.
- To make configuration changes, users must have *Camera* management permissions.
- The camera must be assigned to a Media Server, Location, and camera template. See the following for more information.
 - [Viewing Media Server Status, page 7-8](#)
 - [Creating the Location Hierarchy, page 5-1](#)
 - [Adding and Editing Camera Templates, page 10-1](#)



Tip

Although you must choose a camera template when adding the camera, you can edit the camera configuration after the initial configuration to create a custom configuration. See the “[Accessing the Camera Settings](#)” section on page 8-42.

Network (IP) Camera Rules and Settings

The camera must be accessible on the network if the device is added in *Enabled* state ([Figure 8-3](#)).

- If the camera is not available on the network, you can add the camera in *pre-provisioned* state. The camera will be disabled until you choose **Enable** from the **Device Settings** menu (all required fields must be complete).
- If the camera is still not reachable on the network it will be in *Enabled: Critical* state until the network issue is resolved.

See the “[Pre-Provisioning Cameras](#)” section on page 8-10 and the “[Viewing Camera and Encoder Status](#)” section on page 8-63

Table 8-3 **Network Camera General Settings**

Setting	Description
IP Address	Enter the hostname or IP address entered in the camera configuration. See the camera documentation for instructions. Note All edge devices (such as cameras and encoders) must added to a server using a local (non-NAT) addresses.
Username	Enter the username for accessing the camera on the network. See the camera documentation for instructions to configure the camera username.
Password	Enter the password for accessing the camera on the network. See the camera documentation for instructions to configure the camera password.
Name	Enter a descriptive name that can help you identify the camera. The name can include any combination of characters and spaces.
Install Location	Click to select the location where the camera is physically installed. Note The <i>Installed</i> and <i>Pointed</i> locations define where the camera is physically installed vs. the scene that the camera is recording. For example, a camera installed on building 2 might be pointed at the lobby door of building 1. If an alert event occurs at the Building 1 lobby, it can be flagged and viewed using the Cisco Safety and Security Desktop application even though the camera is physically installed on building 2. See the “ Understanding a Camera’s Installed Location Vs. the Pointed Location ” section on page 5-9.
Media Server	Select the Media Server responsible for storing and playing video from the camera.
Model	Select the camera model.
Template	Select a camera template from the pop-up window. <ul style="list-style-type: none"> • You must choose an existing template when the camera is added to Cisco VSM. After the camera is created, you can create a custom configuration or select a different template. See the “Accessing the Camera Settings” section on page 8-42. • Templates define attributes such as video quality and schedules. Only templates that support the camera are displayed. See the “Adding and Editing Camera Templates” section on page 10-1 for more information.

Multicast

Note The multicast fields are enabled only if a template is chosen that uses **Custom** settings to enable **UDP_Multicast** on Stream A and/or Stream B. See the “[Configuring Multicast Video Streaming](#)” section on page 10-18 for more information.

Table 8-3 Network Camera General Settings

Setting	Description
Primary Address	<p>(Optional) Enter the multicast IP address where the camera's primary video stream (Stream A) should be sent.</p> <p>This field is enabled only if the camera's template Stream A is configured for multicast.</p> <p>Addresses must be in the proper address range.</p> <ul style="list-style-type: none"> Private network addresses: 239.0.0.0 - 239.255.255.255 Public network addresses: 224.0.0.0 - 244.0.0.255 and 244.0.1.0 - 238.255.255.255 <p>Note Public addresses must be individually assigned by IANA (Internet Assigned Numbers Authority)</p>
Primary Port	Enter the port value used by Cisco Video Surveillance to listen to the camera's primary video stream.
Secondary Address	<p>(Optional) Enter the multicast IP address where the camera's secondary video stream (Stream B) should be sent.</p> <p>This field is enabled only if the camera's template Stream B is configured for multicast.</p> <p>Addresses must be in the proper address range.</p> <ul style="list-style-type: none"> Private network addresses: 239.0.0.0 - 239.255.255.255 Public network addresses: 224.0.0.0 - 244.0.0.255 and 244.0.1.0 - 238.255.255.255 <p>Note Public addresses must be individually assigned by IANA (Internet Assigned Numbers Authority)</p>
Secondary Port	Enter the port value used by Cisco Video Surveillance to listen to the camera's secondary video stream

Analog Camera Rules and Settings

Analog cameras are attached to an encoder that provides network connectivity. See the following documentation for more information

- See the encoder documentation for instructions to properly attach the serial cables to the cameras and determine the serial port and serial address for each camera.
- Verify that the encoder and analog cameras meet the requirements specified in the [“Requirements” section on page 11-4](#).
- Single analog camera are attached to the encoder directly. Multiple cameras can be attached in a daisy chain configuration. A serial port and serial address is assigned to each camera. See the encoder documentation for more information.
- See the [“Adding Encoders and Analog Cameras” section on page 11-1](#) for additional instructions to add the encoder and analog cameras. You can add analog cameras using the encoder configuration page, or the camera configuration page.

Table 8-4 Analog Camera General Settings



Setting	Description
Encoder	Select the encoder that supports the analog camera.
Video Port	<p>The physical encoder video port where the camera video cable is attached.</p> <p>Tip Only the unused ports are displayed.</p>

Table 8-4 **Analog Camera General Settings**

Setting	Description
Audio Port	(Optional) The physical encoder audio port where the camera audio cable is attached. Tip Only the unused ports are displayed.
Name	Enter a descriptive name that can help you identify the camera. The name can include any combination of characters and spaces.
Installed Location	Select the location where the camera is physically installed. Note The <i>Installed</i> and <i>Pointed</i> locations define where the camera is physically installed vs. the scene that the camera is recording. For example, a camera installed on building 2 might be pointed at the lobby door of building 1. If an alert event occurs at the Building 1 lobby, it can be flagged and viewed using the Cisco Safety and Security Desktop application even though the camera is physically installed on building 2. See the “Understanding a Camera’s Installed Location Vs. the Pointed Location” section on page 5-9.
Model	Select the camera model.
Template	Select a camera template from the pop-up window. <ul style="list-style-type: none"> • The template is based on the encoder model, not the camera model. • You must choose an existing template when the camera is added to Cisco VSM. After the camera is created, you can create a custom configuration or select a different template. See the “Accessing the Camera Settings” section on page 8-42. • Templates define attributes such as video quality and schedules. Only templates that support the camera are displayed. See the “Adding and Editing Camera Templates” section on page 10-1 for more information.

Procedure

To manually add a camera to the Cisco VSM configuration, complete the following procedure.

-
- Step 1** Log on to the Operations Manager.
- See the [“Logging In”](#) section on page 1-18.
 - You must belong to a User Group with permissions for *Cameras*.
- Step 2** (Optional) Create a camera template that defines the camera configuration, if necessary.
- You can also use an existing template, such as the default system templates for low, medium and high quality video.
 - You must assign a template to the camera when adding it to Cisco VSM.
 - After adding the camera, you can modify the template or create a custom configuration for the camera.
 - See the [“Adding and Editing Camera Templates”](#) section on page 10-1.
- Step 3** Click **Cameras**.
- Step 4** Click **Add**.
- 
- Tip** You can also click the **Add** icon  and choose **Add a camera manually**.
-
- Step 5** Select the camera type:

- **IP Camera**—networked IP camera
- **Analog Camera**—analog camera are attached to an encoder to provide network connectivity and digitize the analog video. See the [“Adding Encoders and Analog Cameras”](#) section on page 11-1 for more information.

**Tip**

To use the auto-discovery option, see the [“Viewing Camera and Encoder Status”](#) section on page 8-63.

Step 6 Enter the basic camera settings.

- [Network \(IP\) Camera Rules and Settings](#), page 8-12
- [Analog Camera Rules and Settings](#), page 8-14

Step 7 Click **Add**.

Step 8 If a camera is not found on the network (the camera is offline or the username/password are incorrect), you can choose to *pre-provision* the camera. Pre-provisioning allows the camera to be added to Cisco VSM as a disabled device. Select **Enable** from the **Device Settings** menu once camera network installation is complete.

Step 9 Wait for the *Job* to complete.

See the [“Understanding Jobs and Job Status”](#) section on page 13-25.

Step 10 (Optional) When the camera configuration page appears, update the additional *General Information* settings, if necessary

Setting	Description
Pointed Location	Click to select the location where the camera is pointed. This is the video that will be displayed and recorded by the camera. Tip See the “Understanding a Camera’s Installed Location Vs. the Pointed Location” section on page 5-9.
Description	Enter a description of the camera, if necessary.

Step 11 (Optional) Enter additional configurations, if necessary.

See the [“Editing the Camera Settings”](#) section on page 8-42.

Step 12 (Optional) If the camera was pre-provisioned, complete the configuration and select **Enable** from the **Device Settings** menu.

**Note**

The **Enable** option is only enabled if the camera configuration is complete and the device is available on the network.

Step 13 Repeat [Step 4](#) through [Step 11](#) to add additional cameras, if necessary.

Importing or Updating Cameras or Encoders Using a CSV File

Multiple cameras or encoders can be imported using a *comma separated value* (CSV) file that includes configuration details for each device (Figure 8-4). This same method can be used to update existing camera configurations.

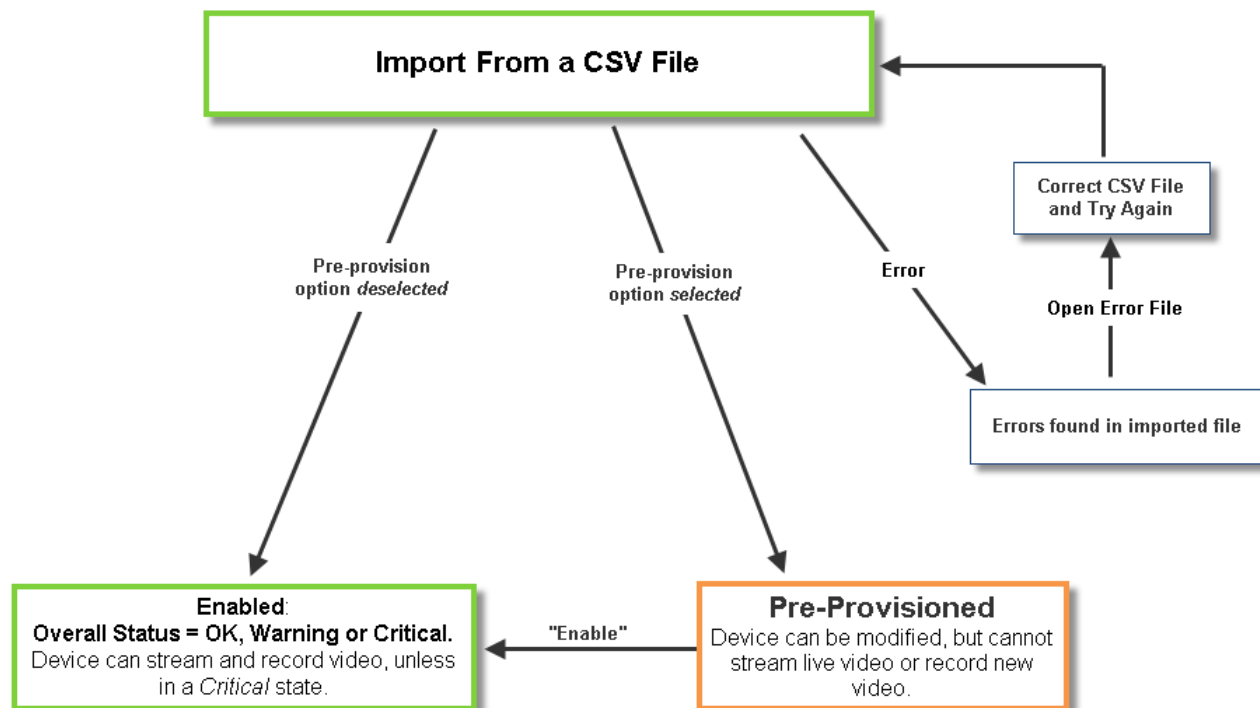
Refer to the following topics for more information:

- [Overview, page 8-17](#)
- [Usage Notes, page 8-18](#)
- [Creating the CSV File, page 8-18](#)
- [Importing the CSV File, page 8-20](#)

Overview

Figure 8-4 summarizes the process to import devices from a CSV file. Devices can be added in Enabled state if all required configurations are included, or in Pre-Provisioned state if configurations are missing or if the devices are not yet available on the network. If an error occurs, correct the CSV file and try again.

Figure 8-4 Importing Cameras or Encoders from a CSV File



Usage Notes

- Cameras, encoders and servers can be pre-provisioned in Release 7.2 and higher.
- Pre-provisioned devices are waiting to be added to Cisco VSM. You can make additional configuration changes, but the device cannot stream or record video until the configuration and network issues are resolved. Choose **Enable** from the **Device Settings** menu to enable the device video functions. See the “[Pre-Provisioning Cameras](#)” section on page 8-10 for more information.
- If the CSV file details are accurate and complete, the devices are added to Cisco VSM and video from the cameras is available for viewing and recording.
- If any *required* fields are left blank, or if any devices in the file are not available on the network, then the devices are added to Cisco VSM in *pre-provisioned* state, even if the *pre-provisioned* option is deselected. Complete the configuration to change the status to *Enabled*. See [Table 8-5](#) for the required fields.
- If any fields are inconsistent with the Cisco VSM configuration, the import action fails and an error file is created that specifies the problem(s). For example, if the CSV file specifies a Media Server or location that does not exist in your Cisco VSM configuration, an error occurs. Correct the CSV file and try again.
- You cannot mix device types in the import file. For example, the file can include servers, encoders, IP cameras, or analog cameras only.

Creating the CSV File

Create a file in plain text CSV format that can be opened and saved using Excel or OpenOffice Calc ([Figure 8-5](#)). Blank rows or rows beginning with “//” are ignored.



Tip

To download a sample import file, launch the import wizard as described in the “[Importing the CSV File](#)” section on page 8-20. Click the **Download Sample** button in the second step of the wizard to obtain a sample file (see [Step 5](#)). The import file is different for each device type: IP cameras, analog cameras, and encoders.

Figure 8-5 Example of a Camera Import File

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Name	Model	IP address	MAC address	Serial no	Mediaserver name	Install loc	Point-to-l	Template	Username	Password	Tags	
2	//<required>	//<required but r	//<One of IP/MAC/	//<One of IP/MAC/Serial no are	//<One of IP/M	//<if preprovisionec	//<if prep	//<if prep	//<if prep	//<if prep	//<if prep	//<Optional>	
3	//Lobby camera	panasonic_np_2	10.10.10.10	AA:BB:CC:DD:44	12345-12	// UMS-1	USA.CA.SJ	USA.CA.SJ	Lobby Can admin	secur4u		Sample tags	
4													
5	// Supported Delimiters - Contents that have non-ASCII characters, need to be delimited by tab. If the content contains only ASCII, comma delimiter should be used												
6	//Any lines starting with "//" are treated as comments												
7													

[Table 8-5](#) describes the CSV file fields for both IP and analog cameras (the fields vary for each cameras type).

The CSV file can be created in a program such as Excel or OpenOffice Calc and saved as a CSV file. For example, in Excel, create the file and then choose **Save As > Other formats**. Select **CSV (Comma delimited)** for the *Save as type*.

Table 8-5 Import File Field Descriptions

Content	Required/ Optional	Description
Comment //	IP / Analog Cameras Optional	Blank rows or lines/cells starting with "/" are treated as comments and ignored.
Name	IP / Analog Cameras Required	Enter the camera name For example: LOBBY INT ENTRY
Model	IP / Analog Cameras Required	The camera model. For example: cisco_2500
IP address	IP cameras Required (see description)	At least one value is required (IP address, MAC or serial number).
MAC address		<ul style="list-style-type: none"> New Cameras—The IP address, serial number, and MAC address must be unique for new cameras. See the “Cameras with Duplicate IP Addresses” section on page 8-10 for more information. Existing cameras—If all three entries are provided for an existing camera, the settings must match the devices existing settings.
Serial no		
Media Server	IP cameras Optional	Enter the Media Server name. Note The Media Server must be valid and already present in the system. See the “Viewing Media Server Status” section on page 7-8.
Encoder Name	Analog cameras Required	Enter the name of the encoder that provides connectivity for the analog camera.
Encoder video port	Analog cameras Required but non-editable	Enter the encoder port number used for video by the analog cameras
Encoder audio in port	Analog cameras Optional but non-editable	Enter the encoder port number used for audio input by the analog cameras
Install Location Path	IP / Analog Cameras Optional	Enter the location where the camera is physically installed. For example camera's installed location path. For example: CA/North Campus/bldg 2 See the “Understanding a Camera's Installed Location Vs. the Pointed Location” section on page 5-9.


Table 8-5 Import File Field Descriptions (continued)

Content	Required/ Optional	Description
Point-To Location Path	IP / Analog Cameras Optional	Enter the location where the camera is capturing video. For example, a camera installed on building 2 can be pointed at building 1, so the camera's video is from the <i>pointed at</i> location building 1. For example: CA/North Campus/bldg 1 See the “Understanding a Camera’s Installed Location Vs. the Pointed Location” section on page 5-9.
Template Name	IP / Analog Cameras Optional	The configuration template that defines the camera video quality, recording and motion parameters, and other settings. Note The template must be valid and already present in the system. See the “Adding and Editing Camera Templates” section on page 10-1.
Username	IP Cameras Optional	The username configured on the camera to provide network access. See the camera documentation for instructions to define the camera credentials.
Password	IP Cameras Optional	The password configured on the camera to provide network access. <ul style="list-style-type: none"> See the camera documentation for instructions to define the camera credentials. See the “Changing the Camera or Encoder Access Settings (Address and Credentials)” section on page 8-61 to revise the credentials after the camera is added to the system.

Importing the CSV File

Complete the following procedure to import a CSV file.

Procedure

-
- Step 1** (Optional) Enable Auto-configuration for the camera model(s).
- Auto Provisioning applies camera settings based on the camera model.
 - See the [“Enabling the Auto Configuration Defaults for a Camera Model” section on page 8-25.](#)
- Step 2** Create the camera CSV file containing details for each device.
- See the [“Creating the CSV File” section on page 8-18.](#)
- Step 3** Click **Cameras**.
- Or click **Cameras** and then **Encoders** to import a list of encoders.
- Step 4** Choose **Add**  and choose **Import cameras from file** or **Import encoders from file**.
- Step 5** Complete each *Import Step* as described below:
- Import Step 1 - Device Type*
 - (Cameras only) Select **IP Camera** or **Analog Camera**.
 - Click the **Pre-Provision** box if the devices should be pre-provisioned when added to Cisco VSM. This allows you to add the devices before they are available on the network, or before they should be available to end users.

**Note**

If any *required* fields are left blank, or if any cameras in the file are not available on the network, then the devices are added to Cisco VSM in *pre-provisioned* state, even if the *pre-provisioned* option is deselected. Complete the configuration to change the status to *Enabled*. See [Table 8-5](#) for the required fields.

- b. *Import Step 2 - Download Sample*
(Optional) Click **Download Sample** to download a sample CSV import file. Use this sample to create the import file as described in the “[Creating the CSV File](#)” section on page 8-18. Click **Next**.
- c. *Import Step 3 - File Upload:*
Click **Choose** to select the CSV file from a local or network disk. Click **Upload**.
- d. *Import Step 4 - Processing:*
Wait for the import process to complete.
- e. *Import Step 5 - Results:*
 - If a *success* message appears, continue to [Step 6](#).
 - If an *error* message appears, continue to [Step 5 f](#).
- f. If an *error* message appears ([Figure 8-6](#)), complete the following troubleshooting steps:
 - Click **Download Annotated CSV**, save the error file and open it in Excel or OpenOffice Calc.
 - Correct the annotated errors and save the revised file in the .csv format.
 - Re-import the fixed file.
 - Correct the CSV file in the //Error rows ([Figure 8-6](#)).
 - Return to [Step 4](#) and re-import the corrected CSV file.

Figure 8-6 Camera Import Error File

	A	B	C	D	E	F
1	Name	Model	IP address	MAC addr	Serial no	Mediaserver name
2	<required>	<required>	<One of IF>	<One of IF>	<One of IF>	<optional>
3		//The mo	//IP Address is ill formatted			//The Specified media server {0} does not exist
4	Lobby cam	panasonic	10.10.10.1	AA:BB:CC:12345-12	UMS-1	USA
5				//MAC Address is ill		//The Specified media server {0} does not exist

Step 6 Click **Close**.

Step 7 View the camera status to determine if additional configuration is required.

- See the “[Device Status: Identifying Issues for a Specific Device](#)” section on page 13-8.

Discovering Cameras on the Network

IP cameras that have been installed on the network can be discovered and added to Cisco VSM. Cameras that support Medianet can be discovered automatically, or you can manually trigger discovery.

See the following topics for more information:

- [Understanding Discovery and Auto-Configuration, page 8-22](#)
- [Understanding Camera Conflicts, page 8-24](#)
- [Enabling the Auto Configuration Defaults for a Camera Model, page 8-25](#)
- [Discovering Non-Medianet Cameras on the Network, page 8-28](#)
- [Cameras Pending Approval List, page 8-30](#)
- [Discovering Medianet-Enabled Cameras, page 8-32](#)
 - [Medianet Requirements, page 8-32](#)
 - [Medianet Overview, page 8-33](#)
 - [Medianet Camera Discovery Procedure, page 8-36](#)

Understanding Discovery and Auto-Configuration

Cisco VSM can discover network cameras that are added to the network using one of the following methods:

Table 8-6 *Camera Discovery Options*

Discovery Method	Description	More Information
Automatic Discovery	Medianet-enabled cameras can be discovered automatically and added to Cisco VSM when added to the network. Note Medianet cameras must be configured with an <i>admin</i> user.	“Discovering Medianet-Enabled Cameras” section on page 8-32
Manually Trigger Discovery	Cameras that do not support Medianet can still be discovered on the network, but the discovery must be manually triggered and the cameras must support the Bonjour discovery feature.	<ul style="list-style-type: none"> • Discovering Cameras on the Network, page 8-22 • Documentation for the camera(s) to be discovered

Cameras Pending Approval List

Cameras discovered on the network are added to the *Cameras Pending Approval* list ([Figure 8-7](#)), allowing you to review the discovered cameras, add additional configuration settings if necessary, and manually approve the camera addition to Cisco VSM. See the [“Cameras Pending Approval List” section on page 8-30](#) for more information.

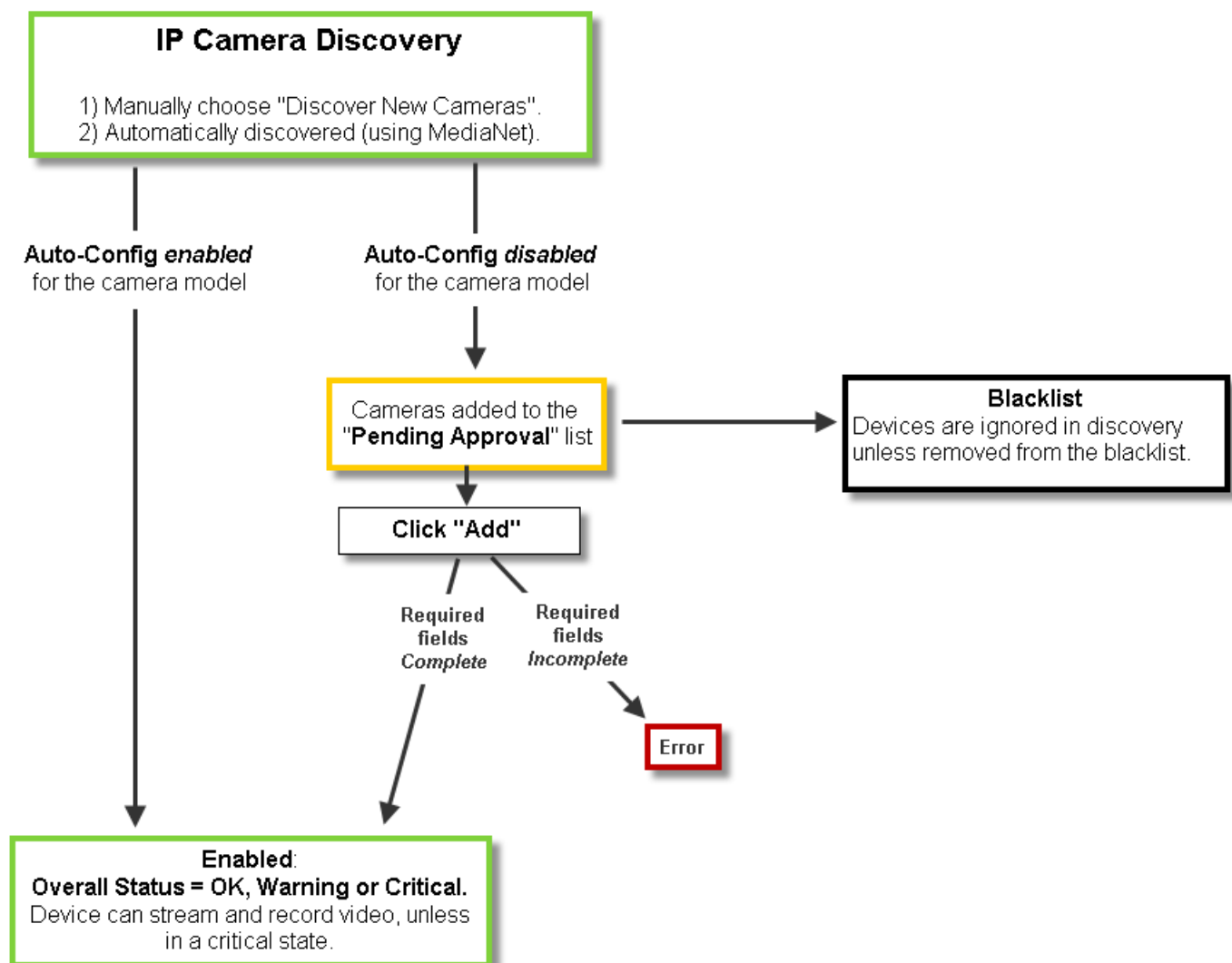
Auto-Configuration Default Configuration

If the **Auto-configuration default** option is enabled for a camera model, then the basic configuration and template is automatically applied to the camera, and the camera is added directly to the enabled state (Figure 8-7). **Auto-configuration default** settings are accessed in the System Settings page. See the [“Enabling the Auto Configuration Defaults for a Camera Model”](#) section on page 8-25 for more information.

Supported Cameras

To view the camera models that support discovery, open the Auto Configuration Settings page and click on a camera manufacturer. See the [Enabling the Auto Configuration Defaults for a Camera Model](#), page 8-25.

Figure 8-7 Camera Discovery and AutoConfig Flow Chart



**Tip**

You can also move a discovered camera to the Blacklist to prevent it from being added to Cisco VSM or from being discovered in future discovery actions ([Figure 8-7](#)).

Understanding Camera Conflicts

Cameras are identified in Cisco VSM discovery by the device IP Address, and serial number, mac address/hardware ID. If a camera is discovered with values in these fields that already exist in the Cisco VSM configuration, the camera records will either be merged, or placed in a collision state.

- If some identity fields in a discovered camera and existing camera are a perfect match, but some fields are empty, then the records are merged. For example, if a camera in Cisco VSM includes only a name and MAC address, and a discovered camera has the same MAC address plus additional fields for serial number and IP address, then the two records are merged into a single camera entry.
- If both the Cisco VSM camera and a discovered camera include identity fields that do not match, both cameras are placed in a collision state. You must replace or delete one of the cameras to remove the conflict.

Open the camera **Status** tab on the configuration page to view more information (see the [“Viewing Camera and Encoder Status”](#) section on page 8-63).

- The device overall status is *Enabled: Critical*.
- Click the link next to the *Hardware* category to open a pop-up that details the collision.
- An *Alert* is generated for “identity collision”.
- If the discovered camera uses DHCP settings, and only the IP address is in conflict, then the IP address of the discovered camera is used. If the discovered camera uses a static IP address, however, then the camera entries are in conflict.

Open the camera **Status** tab on the configuration page to view more information (see the [“Viewing Camera and Encoder Status”](#) section on page 8-63).

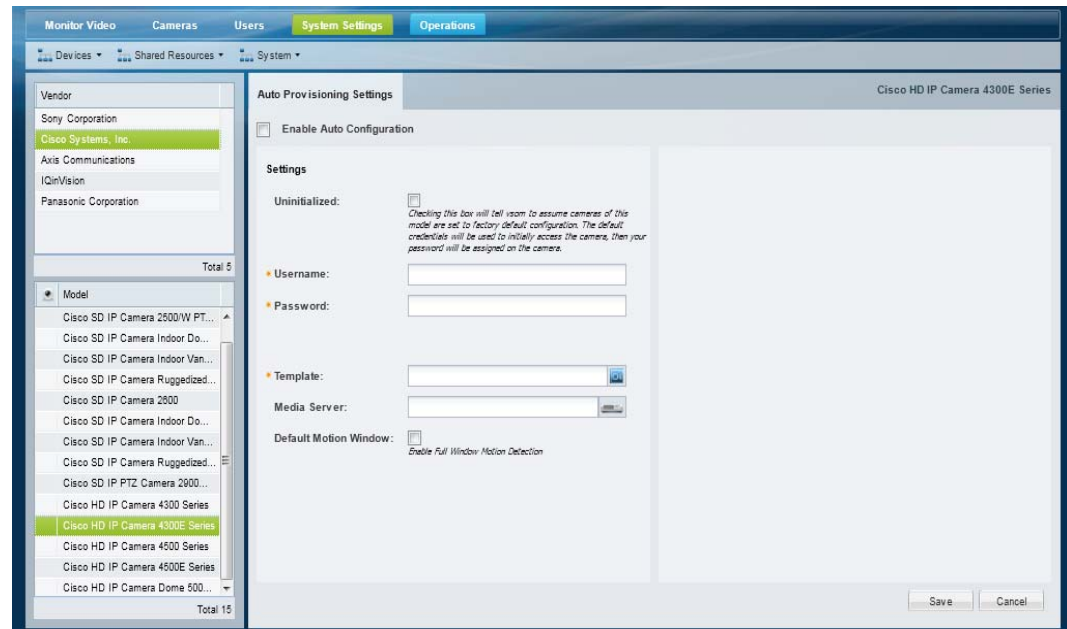
**Note**

Settings such as name, template, location, media-server associations are configurations in the Operations Manager and are not merged or overwritten by discovered settings.

Enabling the Auto Configuration Defaults for a Camera Model

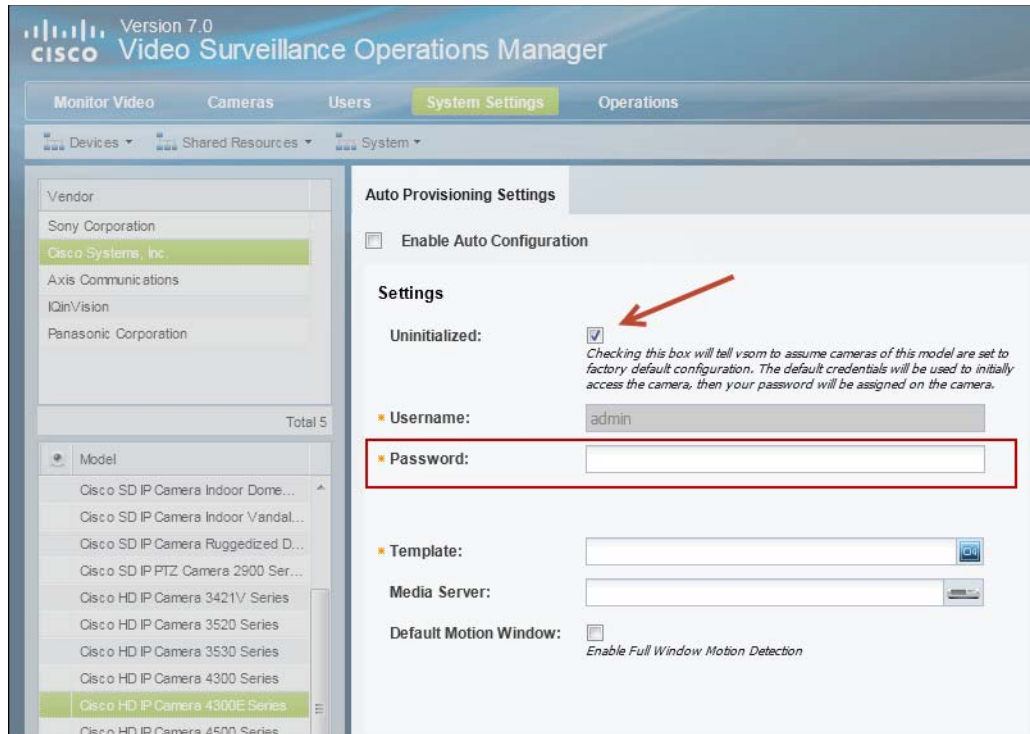
The auto-configuration default settings are automatically applied to cameras that are discovered on the network. Auto-configuration is disabled for all camera models by default. You must enable the defaults for each camera model.

Figure 8-8 Device Auto Configuration



Usage Notes

- If auto-configuration is not enabled for a camera model (or if the auto-configuration fails) then the camera is placed in the *Cameras Pending Approval* list. See the [“Cameras Pending Approval List” section on page 8-30](#) for more information.
- If the auto-configuration fails, cameras can also be placed Enabled –Critical state. For example, if the entered password does not match the password configured on the device.
- Medianet-enabled devices also include an **Uninitialized** option. Select this to log in to the camera using the default device credentials. Enter a password to automatically replace the device password with the new setting (the username is read-only).

Figure 8-9 *Uninitialized Option***Procedure**

To enable auto-configuration for cameras that are discovered on the network or imported from a CSV file, complete the following procedure.

-
- Step 1** Log on to the Operations Manager.
- See the “[Logging In](#)” section on page 1-18.
 - You must be a *Super User* or belong to a user group assigned to the *super_admin_role* (a super-user is anybody that has all permissions at the root location). See the “[Adding Users, User Groups, and Permissions](#)” section on page 4-1 for more information.
- Step 2** Select **System Settings > Auto Provisioning Settings**.
- The Device Auto Configuration screen appears ([Figure 8-8](#)).
- Step 3** Click a camera *Vendor*.
- Step 4** Click a camera *Model*.
- Step 5** Select the **Enable Auto Configuration** check-box.

- Step 6** Enter the auto-configuration settings that will be applied to all discovered or imported cameras (of that model).

Setting	Description
Uninitialized	<p>(Medianet enabled devices only) Select this option to use the default credentials to initially access the camera. Enter a new password to change the default setting.</p> <p>Note The change will not be implemented if the current username and password has been changed from the factory default.</p>
Username	Enter the username used to access the camera over the network.
Password	<p>Enter the password used to access the camera over the network.</p> <ul style="list-style-type: none"> See the camera documentation for instructions to set the credentials, or ask your system administrator for the information. See the “Changing the Camera or Encoder Access Settings (Address and Credentials)” section on page 8-61 to revise the credentials after the camera is added to the system.
Template	<p>Select the camera template that will provide the camera configuration.</p> <p>See the “Adding and Editing Camera Templates” section on page 10-1 for more information.</p>
Media Server	<p>(Optional) Select the Media Server that will manage the camera (the camera will be assigned to this Media Server).</p> <p>See the “Configuring Media Server Services” section on page 7-1 for more information.</p>
Default Motion Window	<p>(Optional) Enable motion configuration features for the entire camera view. This option is enabled only if the camera supports motion detection.</p> <p>See the “Configuring Motion Detection” section on page 8-77 for more information.</p>

- Step 7** Click **Save**.

- Step 8** (Optional) Repeat this procedure to enable auto-configuration defaults for additional camera models.

Discovering Non-Medianet Cameras on the Network

Cameras that do not support Medianet can still be discovered on the network, but the discovery must be manually triggered. The cameras must also support the Bonjour discovery feature, and Bonjour must be enabled on the device.

You can also (optionally) enable the auto-configuration defaults for the camera model to automatically complete the basic camera properties and enable the camera in Cisco VSM

Procedure

Table 8-7 **Manual Camera Discovery Steps**

	Task	Description and more information
Step 1	Review the overview sections to understand the discovery process.	Review the following topics to understand the discovery and auto-configuration process. <ul style="list-style-type: none"> • Understanding Discovery and Auto-Configuration, page 8-22 • Understanding Camera Conflicts, page 8-24 • Enabling the Auto Configuration Defaults for a Camera Model, page 8-25 • Cameras Pending Approval List, page 8-30
Step 2	Enable the Bonjour discovery feature on each camera, if not enabled by default.	See the product documentation for the device to determine Bonjour support and configuration.
Step 3	(Optional) Enable auto-configuration presets.	If auto-configuration is enabled for the camera model, the camera will automatically be added to Cisco VSM. <ol style="list-style-type: none"> Media Servers—Select the Media Server used to discover the cameras. Camera Make(s)—Select the camera make(s) that will be discovered. For example, select Cisco Systems, Inc. to discover all Cisco-branded cameras. Click Save. See the Enabling the Auto Configuration Defaults for a Camera Model , page 8-25.
Step 4	Trigger the discovery process	<ol style="list-style-type: none"> Click Cameras. Choose Add > Discover New Cameras.
Step 5	Wait for the camera to be discovered and be added to the Operations Manager.	<ul style="list-style-type: none"> • Discovery can take a few minutes based on the factors such as the camera configuration, availability of the Media Servers, and other variables. • If a discovered camera has the same device ID fields as an existing camera entry (IP Address, and serial number, mac address/hardware ID), then the records are either merged, or placed in conflict. See Understanding Camera Conflicts for more information.

Table 8-7 **Manual Camera Discovery Steps (continued)**

	Task	Description and more information
Step 6	Approve cameras that were added to the <i>Cameras Pending Approval</i> list.	<p>If auto-configuration is not enabled for the camera model, the camera is added to the <i>Cameras Pending Approval</i> list, which allows you to apply additional configurations and approve (add) the camera.</p> <ol style="list-style-type: none"> Open the <i>Cameras Pending Approval</i> list to modify the camera configuration. Approve the camera or move it to the blacklist. <p>See the “Cameras Pending Approval List” section on page 8-30 for more information</p>
Step 7	Complete the camera configuration.	<p>If auto-configuration was enabled for the camera:</p> <ol style="list-style-type: none"> Open the camera or camera template configuration page and modify the configuration, if necessary. Verify that the camera was added is in the <i>Enabled: OK</i> state. If the camera is in <i>Enabled: Warning, Critical</i> state, go to device Status page to get information, fix the problem and choose Repair Configuration from the Device Settings menu. <p>See the “Editing the Camera Settings” section on page 8-42 for more information.</p>
Step 8	Perform additional configuration, if necessary	<ul style="list-style-type: none"> Editing the Camera Settings, page 8-42 Configuring Camera PTZ Controls, Presets, and Tours, page 8-65 Configuring Motion Detection, page 8-77

Cameras Pending Approval List

Discovered cameras that are not auto-configured are held in the *Cameras Pending Approval* list so they can be reviewed and updated before being added to Cisco VSM (Figure 8-10). The cameras in this list are not available for streaming or recording video.

These cameras can also be added to the blacklist which deletes them from the Cisco VSM configuration and prevents them from being found in future discovery operations.

Figure 8-10 *Cameras Pending Approval*

MAC Address	Serial Id	Make	Model	Firmware Versic	IP Address	Name	Media Server	Install Location
FF014040208	FF014050055	Cisco Systems, Inc.	cisco_4300		10.10.53.93	Autoname...	Primary server	System
FF014050055	FF014050033	Cisco Systems, Inc.	cisco_4300		10.10.53.94	Autoname...	Primary server	System
FF014050033	FF013520043	Cisco Systems, Inc.	cisco_4300		10.10.53.95	Autoname...	Primary server	System
FF013520043	FF014050023	Cisco Systems, Inc.	cisco_4300		10.10.53.96	Autoname...	Primary server	System
FF014050023	FF014050052	Cisco Systems, Inc.	cisco_4300		10.10.53.97	Autoname...	Primary server	System
FF014050052	FF014040212	Cisco Systems, Inc.	cisco_4300		10.10.53.92	Autoname...	Primary server	System
FF014040212	FF014040190	Cisco Systems, Inc.	cisco_4300		10.10.53.90	Autoname...	Primary server	System
FF014040190	FF014040076	Cisco Systems, Inc.	cisco_4300		10.10.53.98	Autoname...	Primary server	System
FF014040076	FF013510433	Cisco Systems, Inc.	cisco_4300		192.168.0.100	Autoname...	Primary server	System
FF013510433		Cisco Systems, Inc.	cisco_4300		10.10.53.91	Autoname...	Primary server	System



Tip

Camera models that have the auto-configuration defaults enabled are added to Cisco VSM. If auto-configuration fails or is not enabled, the camera is added to *Cameras Pending Approval*. If the camera is in *Enabled: Warning* or *Critical* state, go to device **Status** page to get information, fix the problem and choose **Repair Configuration** from the **Device Settings** menu.

Procedure

To move cameras from the *Cameras Pending Approval* list to either Cisco VSM or to the blacklist, complete the following procedure.

You must have *Manage Cameras* permissions to approve or blacklist cameras. See the “[Adding Users, User Groups, and Permissions](#)” section on page 4-1 for more information.

- Step 1** Click **Cameras**.
- Step 2** Perform a camera discovery, as described in the “[Discovering Cameras on the Network](#)” section on page 8-22.
- Step 3** Choose **Add > Cameras Pending Approval**.
- Step 4** (Optional) Filter the list of discovered cameras (Figure 8-10).
For example, select a camera make or model to narrow the results.
- Step 5** Select one or more cameras from the list.



Tip Click the camera to highlight it, or use *Ctrl-Click* or *Shift-Click* to select multiple cameras.

Step 6 (Optional) Enter additional camera configurations:

- Click the buttons at the bottom of the list to edit the required fields. You can also double-click a field to edit the setting.
- Scroll the list to the right, if necessary, to display the editable fields.
- Editable fields are displayed in bold.

Setting	Description
IP Address	The IP address assigned to the camera.
Name	(Optional) Double-click the entry to change the camera name. The default entry is auto-generated.
Media Server	(Required) select the Media Server to manage the camera.
Install Location	(Required) select the location where the camera is physically installed.
Pointed Location	(Required) select the location where the camera is pointed. This is the scene shown in the camera's video.
Template	(Required) select the configuration template for the camera. See the “Adding and Editing Camera Templates” section on page 10-1 for more information.
Credential	(Required) enter the username and password used to access the camera over the network. See the camera documentation for instructions to set the credentials, or ask your system administrator for the information.

Step 7 Click **Add** to save the configuration and add the camera(s) to Cisco VSM.

Step 8 Verify that the camera(s) were successfully added.

Step 9 (Optional) Modify the camera settings, if necessary.

See the [“Accessing the Camera Settings” section on page 8-42](#) to change a camera configuration.



Note Click **Blacklist** to blacklist the camera. See the [“Blacklisting Cameras” section on page 8-40](#).

Discovering Medianet-Enabled Cameras

Network (IP) cameras that support Cisco Medianet can be automatically discovered when they are added to the network. Cameras can also be discovered by a Media Server configured in a different subnet.

Refer to the following topics for more information:

- [Medianet Requirements, page 8-32](#)
- [Medianet Overview, page 8-33](#)
- [Configuring a DHCP Server with Option 125, page 8-34](#)
- [Medianet Camera Discovery Procedure, page 8-36](#)
- [High Availability Impact on Medianet Cameras, page 8-37](#)

Medianet Requirements

For cameras to be automatically discovered on the network using Medianet, the following requirements must be met:

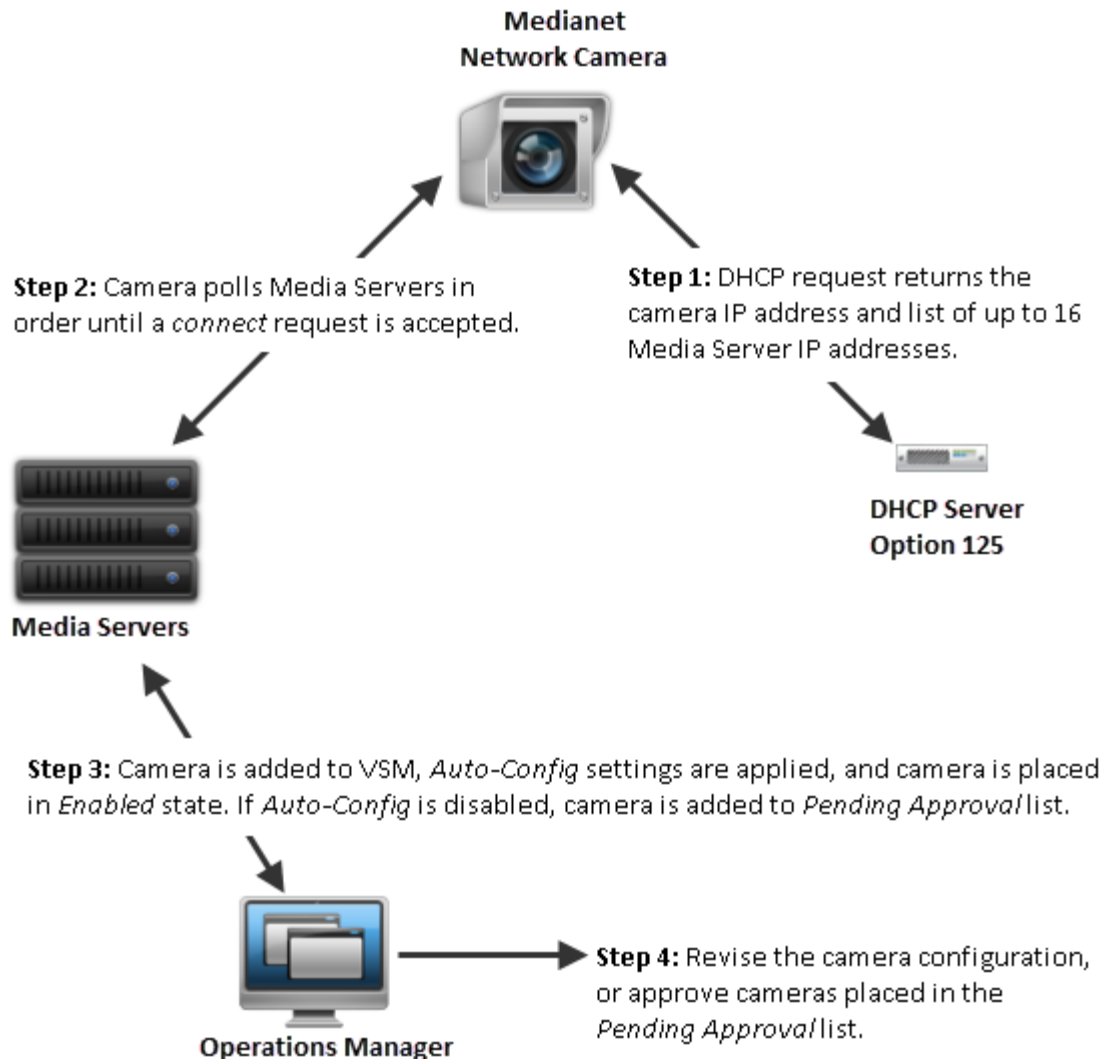
Table 8-8 **Medianet Discovery Requirements**

Requirements	Requirement Complete? (✓)
<p>The network (IP) camera must support Cisco Medianet.</p> <ul style="list-style-type: none"> • See the camera documentation for information. • Examples of Medianet cameras include the Cisco models 4300, 4300E, 4500, 4500E and 26xx. • See the Release Notes for Cisco Video Surveillance Manager, Release 7.2 for a summary of supported Cisco cameras and required firmware. <p>See also the camera product information at http://www.cisco.com/go/physicalsecurity (click View All Products, and select the camera model under <i>Video Surveillance IP Cameras</i>).</p>	<input type="checkbox"/>
<p>A DHCP server must be installed and configured with Option 125 to return a list of Media Server IP addresses. See the “Configuring a DHCP Server with Option 125” section on page 8-34 for instructions.</p> <p>Related Information</p> <ul style="list-style-type: none"> • Cisco Medianet website (http://www.cisco.com/go/medianet) • Cisco Medianet FAQ • Medianet Reference Guide 	<input type="checkbox"/>
<p>A functioning Cisco VSM 7.x system must be installed and configured on the network. See the following for more information:</p> <ul style="list-style-type: none"> • Cisco Video Surveillance Management Console Administration Guide • “Summary Steps: Basic Configuration” section on page 1-8 	<input type="checkbox"/>

Medianet Overview

To enable Medianet discovery, you must install a Medianet-enabled IP camera on the network, as shown in [Figure 8-11](#). A DHCP server must also be installed with Option 125 configured to provide a list of up to 16 Media Server IP addresses.

Figure 8-11 Medianet Camera Discovery Summary



- Step 1** When the camera is added to the network, it contacts the DHCP server, which returns the camera network settings (including IP address) and a list of Media Server IP addresses.



Note Medianet cameras are factory-configured for DHCP by default. If the camera IP address is set to static, then the DHCP address is ignored (released).

- Step 2** The IP camera attempts to connect to the Media Servers (in order of the IP addresses). If a Media Server does not reply, then the camera attempt to connect to the next server in the list.

**Note**

The camera first tries to connect to any Media Server addresses that were manually entered on the camera. If there are no manual entries, or if none of the manually-entered Media Servers accepts the connection request, then the camera attempts to connect to the Media Server addresses sent by the DHCP server.

Step 3 When the camera connects to a Media Server, the camera is also added to the Operations Manager configuration.

- If Auto-Configuration is enabled for the camera model, the configuration settings (including a static IP address) are applied and the camera is placed in Enabled state. The configuration includes a camera template, Location, and Media Server assignment. See the “[Enabling the Auto Configuration Defaults for a Camera Model](#)” section on page 8-25.
- If the Auto-Configuration is disabled (default), then the camera is placed in the *Cameras Pending Approval* list. See the “[Cameras Pending Approval List](#)” section on page 8-30.

**Note**

When the camera configuration is applied, the IP address provided by the DHCP server is retained. You can change the IP address using the camera configuration page, if necessary.

Step 4 Once the camera is added to the Operations Manager, you can apply additional configurations, or approve the camera (if it was added to the *Cameras Pending Approval* list).

See the following for more information:

- [Discovering Cameras on the Network](#), page 8-22
- [Cameras Pending Approval List](#), page 8-30
- [Editing the Camera Settings](#), page 8-42

**Tip**

You can also *Blacklist* a camera to remove it from Cisco VSM and prevent the device from being rediscovered. See the “[Blacklisting Cameras](#)” section on page 8-40.

Configuring a DHCP Server with Option 125

Complete the following procedure to configure the DHCP Option 125 for Cisco IOS devices. This is required to support Cisco VSM Medianet-enabled camera auto-discovery.

Procedure

Step 1 Convert the Media Server IP address to a HEX value.

- The Media Server IP address is the server that the Medianet camera will register with.
 - The HEX value is used in the DHCP server Option 125 configuration.
- a. Search for an online tool that can be used to convert the Media Server IP address to HEX.
 - For example, use the following URL to search for “IP to HEX Converter” tools:
<http://bit.ly/UGG6nq>.
 - b. Convert the camera’s IP address to HEX:

For example, covert the Media Server IP address **10.194.31.1** to the HEX value **0AC21F01**.

Step 2 Add additional HEX values to the Media Server HEX value, as required by your DHCP server.



Note Each DHCP server may require additional HEX strings to be added before and after the Media Server HEX value. This entire HEX string is entered in the DHCP Option 125 configuration. Be sure to use the correct HEX format, as defined in your DHCP server documentation.

For example, a Cisco IOS DHCP server requires that the following HEX values be added before and after the Media Server HEX value:

a. Prefix the following value to the Media Server HEX:

0000.0009.0b14.0901.

b. Append the following value to the Media Server HEX:

.0050.0001

The complete HEX string used in the DHCP server Option 125 configuration (for Cisco IOS devices) is:

0000.0009.0b14.0901. **0AC21F01**.0050.0001

Step 3 Configure the DHCP server to advertise Option 125 to the endpoints.

For example, for a Cisco IOS DHCP server:

```
ip dhcp pool MYADDRESSPOOL
network 10.194.31.0 255.255.255.0
option 125 hex 0000.0009.0b14.0901. 0AC21F01.0050.0001
default-router 10.194.31.254
```



Note **0AC21F01** is the HEX value of the converted Media Server IP address. The entire required HEX value is **0000.0009.0b14.0901. 0AC21F01.0050.0001**.



Note Other DHCP servers may require a different format for the HEX value such as prefixing x to the values or prefixing a \. See your DHCP server documentation for more information.

Medianet Camera Discovery Procedure

Complete the following procedures to discover new Medianet cameras.

Table 8-9 **Summary Steps: Camera Discovery**

	Task	Description and more information
Step 1	Verify that the Medianet Requirements are met.	Medianet Requirements, page 8-32 You must have: <ul style="list-style-type: none"> • A Medianet-enabled IP camera configured with DHCP. • At least one Media Server and Operations Manager. • A DHCP server configured with Option 125 to provide Media Server IP addresses to the camera during discovery. See the “Configuring a DHCP Server with Option 125” section on page 8-34 for instructions.
Step 2	Review the overview sections to understand the discovery process.	Review the following topics to understand the discovery and auto-configuration process. <ul style="list-style-type: none"> • Understanding Discovery and Auto-Configuration, page 8-22 • Discovering Medianet-Enabled Cameras, page 8-32
Step 3	Install a Medianet network camera and use the camera configuration UI to enable DHCP and add an <i>admin</i> user (if necessary).	<ul style="list-style-type: none"> • Cisco network cameras (such as the Cisco 26xx series) have Medianet and DHCP enabled by default. • If a static IP addresses is configured on the camera, or if a list of Media Server IP addresses is configured on the camera, then those values configured on the camera are used and the DHCP settings are ignored. See the camera documentation for more information.
Step 4	(Optional) Enable auto-configuration presets.	If auto-configuration is enabled for the camera model, the camera will automatically be added to Cisco VSM. Enabling the Auto Configuration Defaults for a Camera Model, page 8-25
Step 5	Wait for the camera to be discovered and be added to the Operations Manager.	<ul style="list-style-type: none"> • Discovery can take a few minutes based on the factors such as the camera configuration, availability of the Media Servers, and other variables. • If a discovered camera has the same device ID fields as an existing camera entry (IP Address, and serial number, mac address/hardware ID), then the records are either merged, or placed in conflict. See Understanding Camera Conflicts for more information.
Step 6	Approve cameras that were added to the <i>Cameras Pending Approval</i> list.	If auto-configuration is not enabled for the camera model, the camera is added to the <i>Cameras Pending Approval</i> list, which allows you to apply additional configurations and approve (add) the camera. Open the <i>Cameras Pending Approval</i> list to modify the camera configuration and either approve the camera or move it to the blacklist. See the “ Cameras Pending Approval List ” section on page 8-30 for more information

Table 8-9 **Summary Steps: Camera Discovery (continued)**

	Task	Description and more information
Step 7	Complete the camera configuration.	<ul style="list-style-type: none"> • Open the camera or camera template configuration page and modify the configuration, if necessary. • Verify that the camera was added is in the <i>Enabled: OK</i> state. • If the camera is in <i>Enabled: Warning</i>, <i>Critical</i>, or <i>pre-provisioned</i> state, complete or correct the configuration, verify that the camera is available on the network and choose Enable from the Device Settings menu. <p>See the “Editing the Camera Settings” section on page 8-42 for more information.</p>
Step 8	Perform additional configuration, if necessary	<ul style="list-style-type: none"> • Editing the Camera Settings, page 8-42 • Configuring Camera PTZ Controls, Presets, and Tours, page 8-65 • Configuring Motion Detection, page 8-77

High Availability Impact on Medianet Cameras

When the Primary Media Server is down and the Failover has taken over the role of the Primary server, and a DHCP based Medianet discovered camera has a change of IP address, the Cisco VSM Operations Manager will not reconfigure the camera to the new IP address until the Primary Media Server comes back up. This is because Cisco VSM Operations Manager does not allow any configuration changes on the cameras when the Primary server is down.

Adding Cameras from an Existing Media Server

When a Media Server from another Cisco VSM 7.x deployment is added to the configuration, any existing camera configurations (and their associated recordings) can also be added (or deleted). This can occur when a release 6.x Media Server is upgraded to 7.x, or when a Media Server was previously configured on a different Operations Manager.

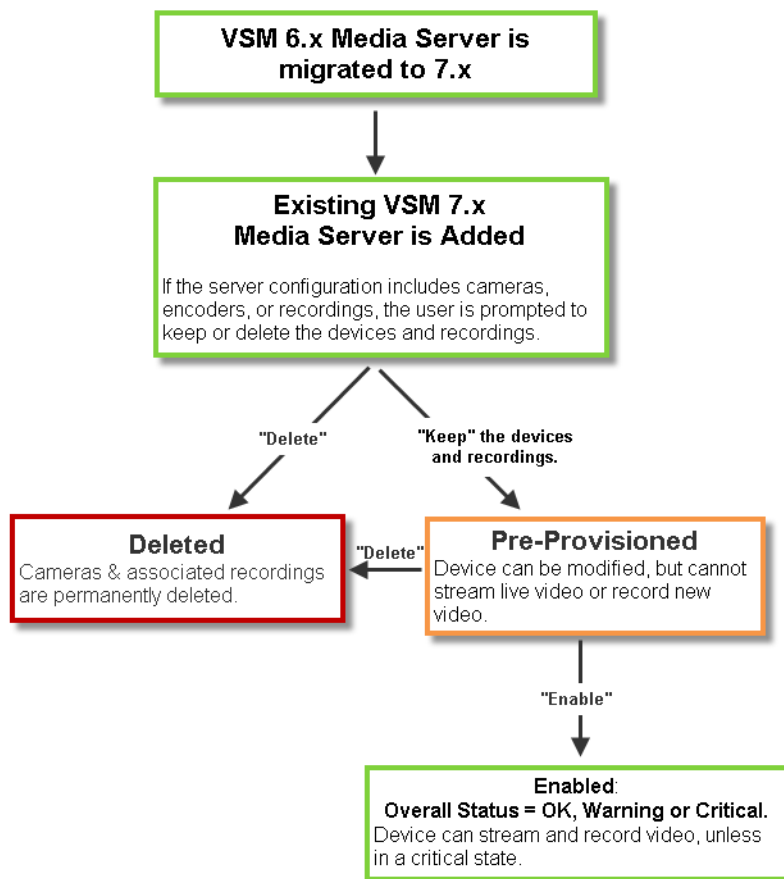
See the following for more information.

- [Adding Cameras From a 6.x or 7.x Media Server, page 8-38](#)
- [Adding Unknown Cameras During a Media Server Synchronization, page 8-39](#)

Adding Cameras From a 6.x or 7.x Media Server

When an existing Media Server is added to the Cisco VSM 7.x configuration, you are prompted to keep or delete the existing camera configurations and their associated recordings ([Figure 8-12](#)). If the cameras are not available on the network, they can still be retained so the recordings can be accessed in the **Monitor Video** window.

Figure 8-12 Adding Cameras from a Cisco VSM 6.x Media Server



**Tip**

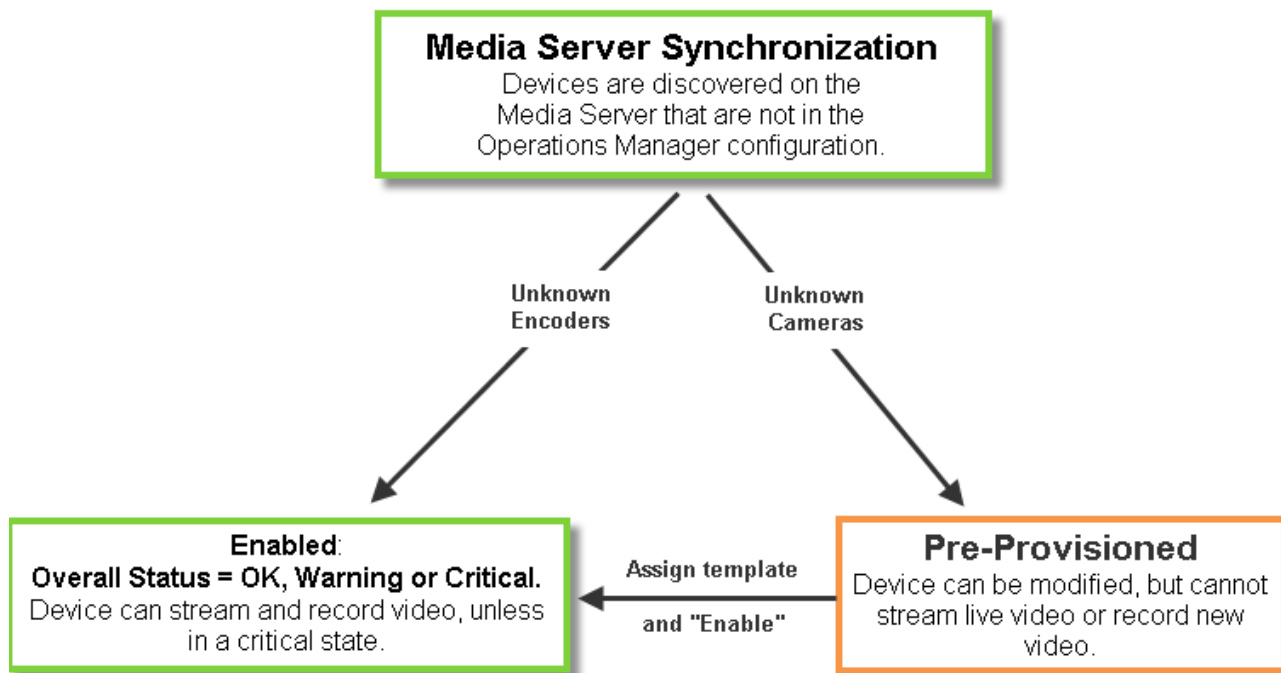
To add a Cisco VSM 6.x Media Server, you must first migrate the server to Cisco VSM 7.x. See the *Cisco Video Surveillance Migration Guide, Release 6.3.2 to 7.0* for more information. This document is available on the Cisco Developer Network (CDN). See your Cisco support representative for more information.

Adding Unknown Cameras During a Media Server Synchronization

In rare cases, a Media Server synchronization may discover cameras on the Media Server that are not configured in the Operations Manager. If this occurs, the cameras are added as Pre-Provisioned, and encoders are added as Enabled (Figure 8-13).

- To enable Pre-Provisioned cameras, assign a template to the camera and choose **Enable** from the **Device Settings** menu. See the “[Pre-Provisioning Cameras](#)” section on page 8-10 for more information.
- If a device is in *Enabled: Warning* or *Enabled: Critical* state, view the device Status page to resolve any additional issues (see the “[Viewing Camera and Encoder Status](#)” section on page 8-63).

Figure 8-13 Adding Unknown Cameras During a Media Server Synchronization

**Note**

See the *Cisco Video Surveillance Migration Guide, Release 6.3.2 to 7.0* for more information. This document is available on the Cisco Developer Network (CDN). See your Cisco support representative for more information.

Blacklisting Cameras

Blacklisted cameras are deleted from the Cisco VSM configuration and are ignored in discovery operations. Cameras can be kept in the *Blacklist* indefinitely.

Refer to the following topics:

- [Blacklisting a Camera, page 8-40](#)
 - [Blacklist a Discovered Camera in the Cameras Pending Approval List](#)
 - [Delete and Blacklist a Camera](#)
- [Viewing Cameras in the Blacklist, page 8-41](#)
- [Removing a Camera From the Blacklist, page 8-41](#)

Blacklisting a Camera

Cameras can be added to the blacklist using the following methods:

- [Blacklist a Discovered Camera in the Cameras Pending Approval List](#)
- [Delete and Blacklist a Camera](#)

Blacklist a Discovered Camera in the *Cameras Pending Approval List*

-
- Step 1** Click **Cameras**.
- Step 2** Choose **Add > Cameras Pending Approval**.
- Step 3** Select one or more cameras from the list.



Tip Click the camera to highlight it, or use *Ctrl-Click* or *Shift-Click* to select multiple cameras.

- Step 4** Click **Blacklist**.



Tip See the [“Discovering Cameras on the Network” section on page 8-22](#) for more information.

Delete and Blacklist a Camera

-
- Step 1** Click **Cameras**.
- Step 2** Select the location and camera name.
- Step 3** Click **Delete**.
- Step 4** Select **Blacklist & Full Delete**.



Caution *Full Delete* permanently deletes all recordings associated with the camera.

Viewing Cameras in the Blacklist

Procedure

- Step 1** Click **Cameras**.
- Step 2** Choose **Add > Camera Blacklist**.
- Step 3** (Optional) Use the filter settings to narrow the displayed devices.
-

Removing a Camera From the Blacklist

To remove a camera from the blacklist so it can be re-added to Cisco VSM, do one of the following:

- Remove the device from the blacklist, as described in the following procedure.
- Manually add the camera. This removes the camera from the blacklist and adds it to Cisco VSM. See the [“Manually Adding a Single Camera”](#) section on page 8-12.

Procedure

- Step 1** Click **Cameras**.
- Step 2** Choose **Add > Camera Blacklist**.
- Step 3** (Optional) Use the filter settings to narrow the displayed devices.
- Step 4** Highlight one or more entries and click **Remove From Blacklist**.
- Step 5** (Optional) Perform a camera discovery to re-add the camera. See the [“Discovering Cameras on the Network”](#) section on page 8-22.
-

Editing the Camera Settings

Camera settings are applied to cameras, camera templates, or custom configurations.

The following settings are accessed in the *Camera* configuration page. You can also update camera configurations by importing a CSV file that defines the settings (see the [“Importing or Updating Cameras or Encoders Using a CSV File”](#) section on page 8-17).

See each topic for detailed information.

- [Accessing the Camera Settings](#), page 8-42
- [General Settings](#), page 8-45
- [Streaming, Recording and Event Settings](#), page 8-49
- [Image Settings](#), page 8-57
- [Configuring the High Availability Options for a Camera or Template](#), page 8-58

Accessing the Camera Settings

To revise the setting for a camera or camera template, click the **Cameras** tab and highlight the device (or template).

Usage Notes

- Not all settings are available for all cameras. For example, *Image* settings are available only if the camera supports features such as motion detection, PTZ controls, and image adjustments.
- Device configuration changes can fail if a camera firmware upgrade is in process. Make sure that a camera firmware is not being upgraded (or wait until it is complete) and try again.
- Most camera settings are applied by the template assigned to the camera. To create a configuration for a single camera, create a custom configuration for the camera. See the [“Creating a Custom Template for a Single Camera”](#) section on page 10-5.
- The camera configuration pages may not display properly if the Internet Explorer (IE) compatibility view box is checked. Deselect this option, if necessary.

Procedure

-
- Step 1** Log on to the Operations Manager.
- See the [“Logging In”](#) section on page 1-18.
 - You must belong to a User Group with permissions for *Cameras*.
- Step 2** Click **Cameras**.

Step 3 Click the tabs in the top left column to view cameras and templates (see [Figure 8-14](#)):




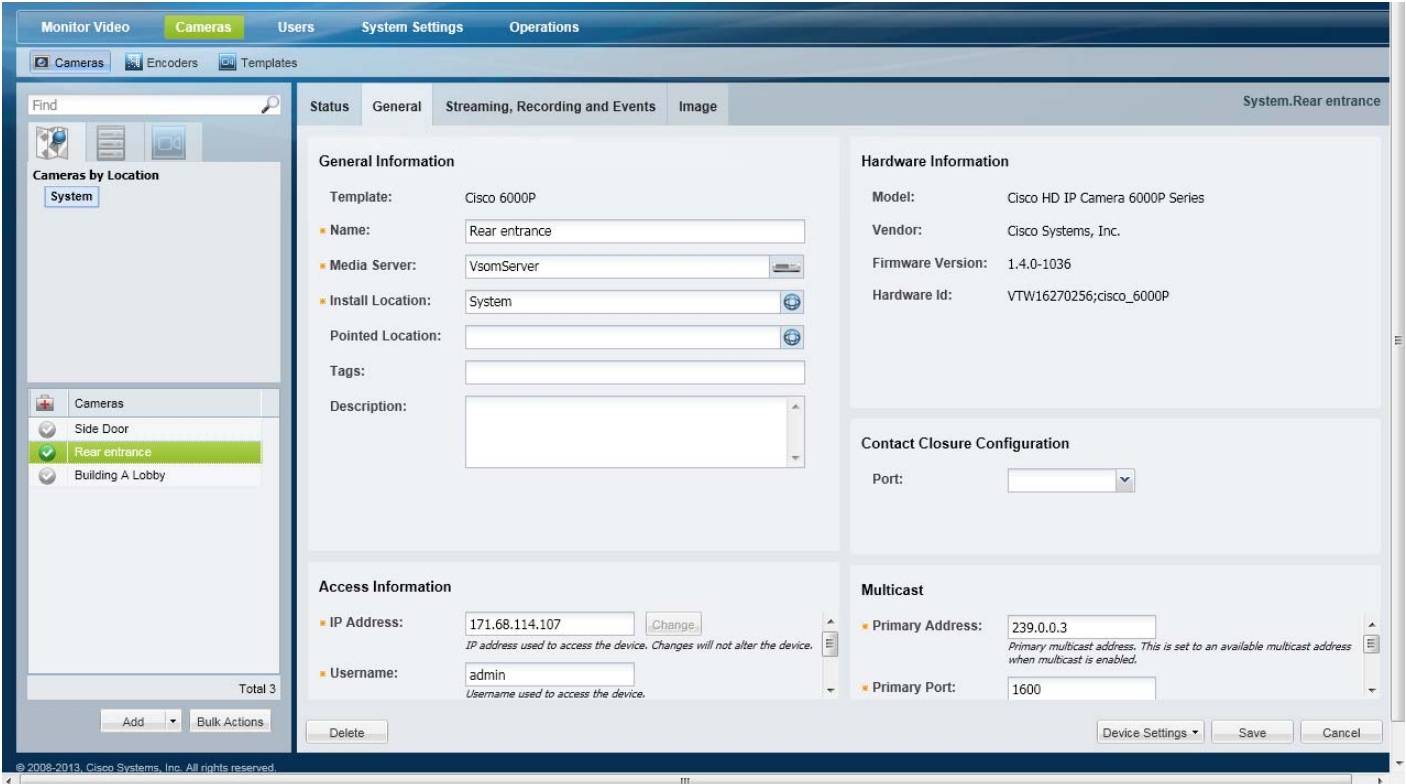
Tab	Description
 Cameras By Location	Displays the cameras assigned to each location. For example, click the Cameras By Location tab and then select a location name (Figure 8-14). The cameras assigned to that location are listed by name. Click a camera name to edit the camera settings.
 Cameras by Media Server	Displays the cameras assigned to each Media Server. If only one Media Server is used, all cameras will be listed.
 Cameras By Template	Displays the cameras assigned to each template. Tip The number next to the template name indicates the number of cameras assigned to the template.

Figure 8-14 Camera General Settings



The screenshot shows the Cisco Video Surveillance Operations Manager interface. The top navigation bar includes 'Monitor Video', 'Cameras' (selected), 'Users', 'System Settings', and 'Operations'. Below this, there are tabs for 'Cameras', 'Encoders', and 'Templates'. The left sidebar shows a tree view under 'Cameras by Location' with 'System' selected. Below this, a list of locations is shown: 'Side Door', 'Rear entrance' (selected), and 'Building A Lobby'. The main content area displays the 'General' settings for the selected camera, 'Rear entrance'. The settings are organized into several sections: 'General Information' (Template: Cisco 6000P, Name: Rear entrance, Media Server: VsomServer, Install Location: System, Pointed Location, Tags, Description), 'Hardware Information' (Model: Cisco HD IP Camera 6000P Series, Vendor: Cisco Systems, Inc., Firmware Version: 1.4.0-1036, Hardware Id: VTW16270256;cisco_6000P), 'Contact Closure Configuration' (Port), 'Access Information' (IP Address: 171.68.114.107, Username: admin), and 'Multicast' (Primary Address: 239.0.0.3, Primary Port: 1600). At the bottom, there are buttons for 'Delete', 'Device Settings', 'Save', and 'Cancel'.

Step 4 Revise the available settings as described in the following topics.

- [General Settings, page 8-45](#)
- [Streaming, Recording and Event Settings, page 8-49](#)
- [Image Settings, page 8-57](#)
- [Configuring the High Availability Options for a Camera or Template, page 8-58](#)

Step 5 Click **Save**.

Step 6 (Optional) Revise the camera template, or create a custom template.

- [Creating or Modifying a Template, page 10-3](#)
 - [Creating a Custom Template for a Single Camera, page 10-5](#)
-

General Settings

The General Settings define camera-specific attributes. These settings are specific to the camera and are not impacted by template settings.

Table 8-10 **Camera General Settings**

Setting	Description
General Information (IP and Analog Cameras)	
Name	(Required) The descriptive name for the camera.
Media Server	(Required) The Media Server that hosts the camera.
Installed Location	(Required) The physical location of the camera.
Pointed Location	(Optional) The location shown in the camera view. For example, a camera may be physically installed on building 1, but pointed at building 2. The video displays the scene at building 2. See the “Understanding a Camera’s Installed Location Vs. the Pointed Location” section on page 5-9 for more information.
Tags	(Optional) Enter keywords used by the <i>Find</i> field.
Description	(Optional) The camera purpose, location or other description.
Access Information (IP Cameras and Encoders Only)	
IP Address	<p>(Required for all cameras and encoders) Enter the IP address used by Operations Manager to access the device on the network. Entering an IP address in this field does not affect the settings stored on the device.</p> <p>(Supported devices only) Click Change to revise the network settings saved on the device <i>and</i> the IP address stored in the Operations Manager. The Change option is disabled if this action is not supported by the device. All changes are saved together when the device is saved. Camera and encoder network settings can include the device IP address, Gateway, Subnet Mask, DNS Server, and Domain. See the device documentation for more information on the required settings.</p> <p>Notes</p> <ul style="list-style-type: none"> • If the Change button is disabled, you can only change the network settings stored on the device using a direct connection or other method. Refer to the device documentation or ask your system administrator for assistance. • The IP address stored in Operations Manager must be the same as the device configuration. A mismatch between the device and Operations Manager can cause a loss of connectivity and loss of video streaming and recording. • See the “Changing the Camera or Encoder Access Settings (Address and Credentials)” section on page 8-61 for more information.

Table 8-10 **Camera General Settings (continued)**

Setting	Description
Username and Password	<p>(Required for all cameras and encoders) Enter the username and password used by Operations Manager to access the device on the network. Entering a username and password in these fields does not affect the settings stored on the device.</p> <p>(Supported cameras only) Click the password Change button and enter the new settings in the dialog provided. The Change option is disabled if this action is not supported by the device. All changes are saved together when the device is saved.</p> <p>Notes</p> <ul style="list-style-type: none"> You cannot change the username stored on the device using Operations Manager. If the password Change button is disabled, you can only change the password stored on the device using a direct connection or other method. Refer to the device documentation or ask your system administrator for assistance. See the “Changing the Camera or Encoder Access Settings (Address and Credentials)” section on page 8-61 for more information.

Serial Controller

Note The following settings are used when a serial cable is attached from an analog cameras to an encoder. The serial port connection enables the pan-zoom-tilt (PTZ) controls and/or photographic controls (brightness, contrast, etc.) on an analog camera.

Tip The following settings can also be defined using the Encoder configuration pages. See the [“Adding Encoders and Analog Cameras”](#) section on page 11-1 for more information.

Enable	<p>(Analog cameras only) Enables the PTZ controls on an analog camera.</p> <p>Note The camera and encoder must support PTZ movements and controls. See the device documentation for more information.</p>
Encoder	(Analog cameras only) The encoder for the analog camera.
Serial Port	<p>(Analog cameras only) The encoder serial port where the first analog camera is attached to the encoder. See the encoder documentation for information to determine the port number.</p>
Serial Port Address	<p>(Analog cameras only) The unique ID of the serial device (analog camera).</p> <p>Note Every device on a serial bus must have a unique ID (also called a “Serial Port Address”). This uniqueID/address is configured on most analog cameras using physical switches. See the camera documentation for more information.</p>

Hardware Information

Model	(Read-only) The camera manufacturer and model number.
Encoder	(Analog cameras only) The encoder name.
Encoder Port	(Analog cameras only) The encoder port used by the analog camera.

Table 8-10 **Camera General Settings (continued)**

Setting	Description
Firmware Version	<p>(Read-only, IP cameras only) The firmware version installed on the device.</p> <p>Device <i>firmware</i> is provided by the device manufacturer.</p> <ul style="list-style-type: none"> To upgrade the firmware for Cisco cameras, and supported encoders, see the “Upgrading Cisco Camera and Encoder Firmware” section on page 15-3. Firmware for non-Cisco cameras is upgraded using a direct connection and the device user interface. See the device documentation to upgrade or downgrade the device firmware directly on the device.
Hardware ID	(Read-only, IP cameras only) The device MAC Address (hardware address).
Contact Closure Configuration	
Contact Closure	<p>Select the contact closure port used to trigger an action.</p> <ul style="list-style-type: none"> This field is enabled for IP and analog cameras that support contact closure. Only one contact closure port can be selected for each camera (even if the camera supports more than one contact closure). When the Operations Manager GUI is used to configure a camera’s contact closure, do not modify the Event trigger settings on the camera web UI. If the default IO port setting values for event triggers on the camera’s browser UI are changed, the results might be inconsistent when also changing the contact closure settings using the Operations Manager GUI. See the “Using Advanced Events to Trigger Actions” section on page 10-11 for instructions to define the action that occurs when the contact closure is triggered. <p>Analog Camera Support Notes</p> <ul style="list-style-type: none"> Analog cameras must be attached to an encoder that supports contact closure. The encoder can provide contact closures for multiple cameras. Only the available encoder ports are displayed (the list includes only the ports supported by the encoder that are not used by another camera attached to that encoder). To view the cameras attached the encoder, select the Connections tab in the encoder configuration page. The Contact Closure Configuration field lists the contact closure ports used the analog cameras. See the “Adding External Encoders and Analog Cameras” section on page 11-5
Multicast	
Note	The multicast fields are enabled only if the corresponding template Stream A and Stream B Custom settings are configured for multicast. See the “Configuring Multicast Video Streaming” section on page 10-18 for more information.
Primary Address	<p>(Optional) Enter the multicast IP address where the camera’s primary video stream (Stream A) should be sent.</p> <p>This field is enabled only if the camera’s template Stream A is configured for multicast.</p> <p>Addresses must be in the proper address range.</p> <ul style="list-style-type: none"> Private network addresses: 239.0.0.0 - 239.255.255.255 Public network addresses: 224.0.0.0 - 244.0.0.255 and 244.0.1.0 - 238.255.255.255 <p>Note Public addresses must be individually assigned by IANA (Internet Assigned Numbers Authority)</p>
Primary Port	Enter the port value used by Cisco Video Surveillance to listen to the camera’s primary video stream.

Table 8-10 **Camera General Settings (continued)**

Setting	Description
Secondary Address	<p>(Optional) Enter the multicast IP address where the camera's secondary video stream (Stream B) should be sent.</p> <p>This field is enabled only if the camera's template Stream B is configured for multicast.</p> <p>Addresses must be in the proper address range.</p> <ul style="list-style-type: none"> • Private network addresses: 239.0.0.0 - 239.255.255.255 • Public network addresses: 224.0.0.0 - 244.0.0.255 and 244.0.1.0 - 238.255.255.255 <p>Note Public addresses must be individually assigned by IANA (Internet Assigned Numbers Authority)</p>
Secondary Port	Enter the port value used by Cisco Video Surveillance to listen to the camera's secondary video stream

**Tip**

See the [“Synchronizing Device Configurations”](#) section on page 13-17 for instructions to manually sync the camera configuration with the Media Server.

Streaming, Recording and Event Settings

The *Streaming, Recording and Event* settings are applied to camera templates and define video attributes for cameras associated with the template. For example, the quality of video streams, how video is recorded, and the advanced storage options for backing up video to a Redundant or Long Term Storage (LTS) server. The *Advanced Events* option defines the events that trigger actions.



Tip

The *Streaming, Recording and Event* settings (Table 8-11) are read-only when viewing a camera configuration. To edit the settings, edit the template associated with the camera, or create a *custom configuration* for the camera (click **Set Template** and choose **Custom**).

Table 8-11 **Streaming, Recording and Event Settings**

Setting	Description
Set Template	<p>(Cameras only) Click Set Template to select the template used for the camera:</p> <ol style="list-style-type: none"> 1. Click Set Template to select a template from the list. Only templates for the user's location that are supported by the camera are displayed. See the “Adding and Editing Camera Templates” section on page 10-1 for more information. 2. Click Custom to enter custom settings for the camera. <p>Note Although you can enter custom settings for both video streams, the IP or analog camera must also support the settings for both streams (analog camera support is dependent on the camera's encoder). If the camera or encoder model does not support the settings, or does not support two streams, the configuration will fail. See the camera or encoder documentation for more information regarding the stream settings supported by the device.</p> <ol style="list-style-type: none"> 3. Click OK to continue. <p>Tip The remaining <i>Streaming, Recording and Event</i> settings can be changed for a specific camera only if the Custom option is selected.</p>
Video Format	<p>(Templates only) Select one of the following:</p> <ul style="list-style-type: none"> • NTSC —the analog television standard primarily used in North and some countries in South America and Asia. • PAL—the analog television standard primarily used in Europe, Africa and some countries in South America and Asia. <p>Note The available quality settings depend on the camera model. For example, if a camera only supports NTSC format, only NTSC can be selected. If a camera supports both PAL and NTSC, both formats will be available.</p>

Table 8-11 **Streaming, Recording and Event Settings (continued)**


Setting	Description
Recording Schedule	<p>(Templates only) Select one of the following:</p> <ul style="list-style-type: none"> • Basic Recording: 24x7—Records 24 hours a day, every day, based on the <i>continuous</i> and <i>event</i> recording properties. or • Select a previously-defined schedule. <p>Recording schedules appear only if schedules are configured. See the “Configuring Continuous, Scheduled, and Motion Recordings” section on page 10-7 for instructions.</p> <p>Recording schedules allow you to define recording properties for different times of the day, days of the week, or for special events. For example, a school might require different video surveillance actions during <i>School</i> hours, <i>After school</i> hours, <i>School off</i> hours, and <i>Closed</i> hours. Additional exceptions to the regular schedule might be required for special events, such as a Homecoming event or the Christmas holiday. A recording entry appears for each time slot included in the schedule.</p>
Video Quality	<p>(Templates only) Slide the selector to Lo, Me or Hi to select pre-defined video quality settings for stream A (primary) and stream B (if supported). Higher quality video requires more network bandwidth, processing resources, and storage space than lower video quality.</p> <ul style="list-style-type: none"> • Select Off to disable video recording and playback. • Choosing Hi on <i>Stream A</i> may disable <i>Stream B</i> if Stream A requires a high level of processing and network resources. To enable <i>Stream B</i>, lower the quality level of <i>Stream A</i>. • Click the Lo, Me or Hi header to view the pre-set values (read-only). • Click Custom to choose specific settings (such as the video codec, transport, bitrate mode, resolution, framerate, bitrate, and quality). See the “Using Custom Video Quality Settings” section on page 8-55 for more information. <div>  <p>Caution Switching a camera's codec may take 30 seconds or more to complete, resulting in a temporary loss of the live video stream. Recorded video is not affected, but you cannot create recorded clips that include more than one codec.</p> </div> <div> <p>Tip See the “Configuring Multicast Video Streaming” section on page 10-18 for more information.</p> </div>

Table 8-11 **Streaming, Recording and Event Settings (continued)**





Setting	Description
Recording Options	<p>(Templates only) Click the recording option for each recurring schedule.</p> <p>Note If Basic Recording: 24x7 was selected, only one row appears. If a schedule was selected, a row appears for each schedule. See the “Configuring Continuous, Scheduled, and Motion Recordings” section on page 10-7 for more information.</p> <ul style="list-style-type: none"> —Select No Recording to disable recording for the stream. —Select Record on Motion to record motion events. <ul style="list-style-type: none"> In <i>Retain event recordings</i>, enter the amount of time a motion event should be retained (saved) on the system. In <i>Padding</i>, enter the number of seconds of recording that should be included before and after the event occurs. Motion recording is available only if the camera supports motion detection. See the “Configuring Motion Detection” section on page 8-77 for instructions to define the areas of the image that trigger motion events. —Select Continuous Recording to record video in a loop. <ul style="list-style-type: none"> For example, video will be recorded continuously for one day before being overridden. This allows you to view video from the past 24 hours. In <i>Retain continuous recordings</i> enter the amount of days that recorded video should be recorded in a loop, or if a recording schedule is selected, the amount of time recorded video should be retained on the system. —Select Record on Motion and Continuous Recording to record continuously and mark any motion events. This option is available only if motion detection is supported by the camera.
Retain continuous recordings	<p>(Templates only)</p> <ul style="list-style-type: none"> 24x7 Recording—Defines the amount of days that recorded video should be recorded in a loop. For example, a retention of 1 day means the system will retain continuously recorded video for the past 24 hours. As new video is recorded, the equivalent amount of the oldest video is deleted. If a recording schedule is selected—Defines the amount of time recorded video should be retained on the system. For example, if a schedule is selected that records video from 2 pm to 4 pm, and you wish to retain that recording on the system for 10 days, enter 10 in the <i>Retain continuous recordings</i> field. <ul style="list-style-type: none"> This value must be a number greater than 0 (days). The default is 1 day. The maximum value is 3650 days (10 years). <p>Note This setting will be ignored if the <i>Default Grooming Only</i> setting is enabled on the Media Server that supports the camera. This can prevent new recordings from beginning if all server disk space is used. See the “Media Server Properties” section on page 7-6 for more information.</p>

Table 8-11 **Streaming, Recording and Event Settings (continued)**


Setting	Description
Retain event recordings	<p>(Templates only) The amount of time a motion event should be retained (saved) on the system. For example, enter 10 to keep motion event recordings for 10 days after the event video is captured.</p> <p>Note This setting also applied to Record Now recordings.</p> <ul style="list-style-type: none"> Enter the number of days the video should be retained. <ul style="list-style-type: none"> Enter a number between 1 and 3650 days (10 years). The default is 30 days. <p>or</p> <ul style="list-style-type: none"> Select Max Possible to retain the recordings as long as disk space is available. If disk space is not available, then recordings are deleted based on the <i>Storage (%)</i> for the Media Server. <p>For example, if the <i>Storage (%)</i> is set to 90%, and a camera template <i>Retain event recordings</i> setting is Max Possible, event recordings may be deleted once the disk repositories are 90% full (deleted video includes the oldest regular, continuous loop or event archives).</p> <p>Note Groups of the oldest 200 video archive files are deleted until the free disk space is less that the <i>Storage (%)</i>. See the Media Server “Media Server Properties” section on page 7-6 for more information.</p> <p>Note This setting will be ignored if the Default Grooming Only setting is enabled on the Media Server that supports the camera. This can prevent new recordings from beginning if all server disk space is used. See the “Media Server Properties” section on page 7-6 for more information.</p>
Alert Notifications	<p>(Templates only)</p> <p> —Click Alert Notifications to enable or disable the alerts that are generated when a motion event occurs.</p>
Advanced Events	<p>(Templates only) Use <i>Advanced Events</i> to trigger actions when an event occurs.</p> <ul style="list-style-type: none"> <i>Instantaneous Trigger Events</i>—Events that trigger an immediate action (for example, when motion is detected). <i>States of Being</i>—Events that trigger an ongoing action as long as that event occurs (for example, while a contact remains open). <p>See the “Using Advanced Events to Trigger Actions” section on page 10-11.</p>
Advanced Storage	<p>(Templates only) Defines storage options for recorded video, such as the use of Redundant, Failover, or Long Term Storage servers. Also defined advanced streaming and recording options.</p> <p>See the “Configuring the Camera Template HA Options” section on page 12-12, which includes the following instructions:</p> <ul style="list-style-type: none"> High Availability and Failover—Configuring the Redundant and Failover Options, page 12-12. Long Term Storage—Archiving Recordings to a Long Term Storage Server, page 12-16. Recording Options—Defining the Recording Options, page 12-20

Table 8-11 **Streaming, Recording and Event Settings (continued)**

Setting	Description
Record Audio	<p>(Templates only)</p> <p>Defines if audio should be recorded when video is being recorded.</p> <p>Note The audio settings is disabled if audio is not supported by the camera.</p> <ul style="list-style-type: none">• Off—(Default) Audio is disabled for both live and recorded video playback.• Live Only—Audio is enabled for live video streaming only.• Live and Recorded—Audio is enabled for live streaming and recorded video playback.
Padding	<p>(Templates only)</p> <p>Defines the number of seconds should be included in a motion event.</p> <ul style="list-style-type: none">• Pre—Enter the number of seconds before a motion event occurs that video should be retained.• Post—Enter the number of seconds after a motion event occurs that video should be retained.

Table 8-11 **Streaming, Recording and Event Settings (continued)**

Setting	Description
Verify Recording Space	<p>(Templates only)</p> <p>Enable</p> <p>Select Enable to verify that enough storage space is available on the Media Server to complete the entire recording. The amount of required storage space is determined by the “Storage Estimation(%)” setting for the Media Server (see the “Storage Management Settings” section on page 7-6). If the required amount of storage space is not available for the entire recording, then the recording will not start.</p> <p>For example, if a camera is configured to record a continuous H264 stream at 15mbps for 30 days, the Media Server would first verify that there is enough free disk space for the full recording length (30 days). If not, then recording will not start. In this example, 15 mbps of video uses approximately 2 megabytes of storage space per second, so 30 days of recording would require roughly 5 terabytes of disk storage.</p> <p>Note The verification takes into account the storage demands required by other cameras assigned to the Media Server.</p> <p>Note Enabling the <i>Default Grooming Only</i> setting for the Media Server assigned to the camera can cause all disk space to be used and prevent new recordings from beginning. See the “Media Server Properties” section on page 7-6 for more information.</p> <p>Disable</p> <p>Disabling this setting will allow recording to be started even when storage is full. But it can cause the system to become oversubscribed, and critical alerts to occur as system performance is impacted.</p> <p>If this setting is disabled, and insufficient disk space for new recordings, the disk will become oversubscribed and default grooming will occur when storage is full.</p> <p>Frequent default disk grooming can cause the server to be slow, as the load average of the server will be high, an critical alerts can occur for the Media Server:</p> <ul style="list-style-type: none"> • Disk space usage for recordings has been over-subscribed. • Load Average is critical. • A “recording failure event” may also occur due to queue overflow, which can cause frame drops.
Record Now	<p>(Templates Only)</p> <p>Enables or disables the Record Now feature on the cameras assigned to the template.</p> <p>Note Recordings are retained according to the <i>Retain event recordings</i> setting.</p> <p>See the following for more information:</p> <ul style="list-style-type: none"> • Enabling Record Now, page 3-12 • Using Record Now, page 2-24

Using Custom Video Quality Settings

Custom video quality settings allow you to define the codec, transport method, bit rate, frame rate, and other settings that are supported by the camera model, as described in [Table 8-12](#).

Usage Notes

- Custom video quality settings can only be applied to model-specific camera templates.
- The available quality settings depend on the camera model. For example, if a camera only supports the H.264 codec, only H.264 can be selected.
- Although you can enter custom settings for both video streams, the IP or analog camera must also support the settings for both streams (analog camera support is dependent on the camera's encoder). If the camera or encoder model does not support the settings, or does not support two streams, the configuration will fail. See the camera or encoder documentation for more information regarding the stream settings supported by the device.
- To configure multicast transmission, see the [“Configuring Multicast Video Streaming” section on page 10-18](#).

Custom Video Quality Settings

Table 8-12 *Custom Video Quality Settings*


Setting	Description
Codec	<p>Select the video encoding format, such as JPEG, MPEG4 or H.264.</p> <div>  <p>Caution Switching a camera's codec may take 30 seconds or more to complete, resulting in a temporary loss of the live video stream. Recorded video is not affected, but you cannot create recorded clips that include more than one codec.</p> </div>
Transport	<p>Select an option to stream video using either TCP or UDP.</p> <p>Note We recommend UDP for most networks where packet loss and high latency are not an issue.</p> <p>Tip Also see the “Configuring Multicast Video Streaming” section on page 10-18.</p>
Bit rate mode	<p>Select CBR (Constant Bit Rate) or VBR (Variable Bit Rate).</p> <ul style="list-style-type: none"> • CBR delivers video at the selected bit rate (or at that average over time), depending on the video device. • VBR adjusts the video quality and/or frame rate as the scene changes. Depending on the video device, the selected bit rate may or not may be the stream's maximum. <ul style="list-style-type: none"> – The bit rate is reduced when there is little movement or change. – The bit rate is increased when there is more change.
Frame rate	Select a frame rate (only frame rates supported by the device are displayed).

Table 8-12 **Custom Video Quality Settings**

Setting	Description
Bit rate	Select the bit rate at which the video device will stream the selected frame rate. Note The frame rate must be specified first. Only frame rate and bit rate combinations supported by the device are displayed.
Quality	(VBR Bit rate mode only) Select the priority of the video quality against the desired frame rate. <ul style="list-style-type: none">• A high <i>Quality</i> setting may cause the video device to reduce the frame rate during periods of high motion or change (in order to maintain a higher quality image).• A low <i>Quality</i> setting may cause the video device to greatly reduce the image quality to maintain a higher frame rate during the periods of high motion or change in the video.

Procedure

-
- Step 1** Create or edit a model-specific camera template, as described in the [“Creating or Modifying a Template” section on page 10-3](#)).
 - Step 2** Select the **Streaming, Recording and Event** tab.
 - Step 3** Click **Custom** in the *Video Quality* field.
 - Step 4** Enter the settings described in [Table 8-12](#) and click **Set**.
 - Step 5** Complete the template configuration as described in the [“Streaming, Recording and Event Settings” section on page 8-49](#) and the [“Creating or Modifying a Template” section on page 10-3](#).
-

Image Settings

Image settings allow you to define the where motion is detected in a camera image, the pan, tilt, and zoom settings for a camera, and the image properties such as contrast and brightness.

Motion Settings

See the [“Configuring Motion Detection”](#) section on page 8-77.

Pan Tilt and Zoom (PTZ) Settings

See the [“Configuring Camera PTZ Controls, Presets, and Tours”](#) section on page 8-65.

Photographic Controls

Click the **Image** tab to access the **Photographic Controls** (Table 8-13) that define properties such as contrast and brightness.



Note

- Only the settings supported by the camera model are shown.
- Analog cameras support video controls only if the camera is configured for serial pass through (a serial cable must be connected from the camera to the encoder, and a serial port must be configured on the analog camera). See the [“General Settings”](#) section on page 8-45 for instructions to configure the analog camera serial port. See the [“Adding External Encoders and Analog Cameras”](#) section on page 11-5 for more information.

Table 8-13 **Photographic Controls**

Setting	Description
White Balance	Adjusts the camera to compensate for the type of light (daylight, fluorescent, incandescent, etc.) or lighting conditions in the scene so it will look normal to the human eye.
Sharpness	Adjusts <i>edge contrast</i> (the contrast along edges in a photographic image). Increase sharpness to increase the contrast only along or near the image edges without affecting the smooth areas of the image.
Contrast	Adjusts the separation between the darkest and brightest areas of the image. Increase contrast to make shadows darker and highlights brighter. Decrease contrast to lighten shadows and darken highlights.
Saturation	Adjusts the intensity and vibrancy of each color channel.
Hue	Adjusting hue will shift the entire color palate along a spectrum. This results in all colors being changed toward a different dominant color. Useful for adjusting the image to make it look more natural in unusual lighting conditions.

Configuring the High Availability Options for a Camera or Template

The Advanced Storage options allow you to define where video streams should be saved. By default, video from both streams is saved only to the Media Server associated with the camera. The Advanced Storage options allow you to also save the video streams to a *Redundant* server or to a *Long Term Storage* (LTS) server (or both). In addition, you can specify a *Failover* server that can assume the Primary functions if the Primary server goes offline (also called *hot standby*).



Note The following procedures are included in the [“High Availability” section on page 12-1](#).

	Task	Related Documentation
Step 1	Install and configure the HA servers.	<ul style="list-style-type: none">• Understanding Redundant, Failover, and Long Term Storage Servers, page 12-4• Define the Media Server HA Role and Associated Servers, page 12-9
Step 2	Configure the Primary server to use the HA servers.	<ul style="list-style-type: none">• Define the Media Server HA Role and Associated Servers, page 12-9
Step 3	Configure the HA Advanced Storage options on the camera template.	<ul style="list-style-type: none">• Configuring the Camera Template HA Options, page 12-12

Deleting Cameras

When deleting a camera, you can delete the camera and all recordings, or keep the recordings on the system. See the [Delete Options](#) for more information.

To delete one or more cameras, use the following methods:

- [Delete a Single Camera](#)
- [Delete Multiple Cameras](#)
- [Delete Options](#)

Delete a Single Camera

- Step 1** Click **Cameras**.
- Step 2** Select the location and camera name.
- Step 3** Click **Delete**.
- Step 4** Select one of the [Delete Options](#).
-


Delete Multiple Cameras

- Step 1** Click **Cameras**.
- Step 2** Click **Bulk Actions**.
- Step 3** Search for and select the cameras to be deleted
- See the [“Bulk Actions: Revising Multiple Cameras”](#) section on page 8-85 for more information.
- Step 4** Click **Delete**.
- Step 5** Select one of the [Delete Options](#).
-

Delete Options

Select one of the following options from the camera or template configuration page:

Table 8-14 **Delete Options**

Delete Option	Description
Blacklist & Full Delete	<p>The camera is removed from Cisco VSM and all recordings are deleted. The camera is placed in the Blacklist, which prevents it from being discovered.</p> <p>See the following for more information:</p> <ul style="list-style-type: none"> • Blacklisting Cameras, page 8-40 • Discovering Cameras on the Network, page 8-22
Retain Recordings	<p>The camera configuration is removed from Cisco VSM, but the camera recordings can still be accessed in the Monitor Video page.</p> <ul style="list-style-type: none"> • The camera status is  Soft Deleted. You can access the recorded video but cannot display live video. See the “Viewing Video” section on page 2-1. • Recordings are retained on the system until removed according to the recording retention settings. See the “Configuring Continuous, Scheduled, and Motion Recordings” section on page 10-7. • The camera is still included in the camera license count. See the “Installing Licenses” section on page 1-23.
Full Delete	<p>The camera is removed from Cisco VSM and all recordings are deleted (removed from the database). The camera can be manually re-added, or added using network discovery, but all recordings will be lost.</p> <p>See the following for more information:</p> <ul style="list-style-type: none"> • Manually Adding a Single Camera, page 8-12 • Discovering Cameras on the Network, page 8-22.
Cancel	Cancel the operation.

Changing the Camera or Encoder Access Settings (Address and Credentials)

The camera or encoder IP address, username, and password settings stored in Cisco VSM Operations Manager are used to access the device over the network. These settings are entered into the Operations Manager when the device is first added to the system (see the [“Manually Adding Cameras”](#) section on page 8-8 and the [“Adding External Encoders and Analog Cameras”](#) section on page 11-5).

Change Options

You can use Operations Manager to change these settings in the following ways (see [Figure 8-15](#)):

- Enter a new value in the IP Address, username or password field and click **Save**. This only changes the settings used by Operations Manager to access the device on the network. It does not change the settings stored on the device.
- Click the **Change** button and enter a new setting to change the setting stored on the device, and the setting used by the Operations Manager.

Figure 8-15 Camera Access Settings

The screenshot displays the 'Camera Access Settings' for a camera named 'Lobby Door'. The interface is divided into several sections:

- Left Sidebar:** A tree view showing the hierarchy of cameras by location, including System, India, U.S., California, Milpitas Campus, MLP Bldg 1, MLP Bldg 2, San Francisco Campus, San Jose Campus, and Oregon Sports Complex. The 'Lobby Door' camera is selected.
- Top Navigation Bar:** Tabs for Monitor Video, Cameras, Users, System Settings, and Operations. The 'Cameras' tab is active.
- Main Content Area:** Tabs for Status, General, Streaming, Recording and Events, and Image. The 'General' tab is active.
- General Information Section:**
 - Template: Cisco 4300E cameras
 - Name: Lobby Door
 - Media Server: Primary Server
 - Installed Location: System.U.S..California.Milpitas Campus.MLP Bldg 1
 - Pointed Location: (empty)
 - Tags: (empty)
 - Description: (empty)
- Access Information Section (highlighted with a red border):**
 - IP Address: 171.68.115.166 (with a 'Change' button)
 - Username: admin (with a 'Change' button)
 - Password: (masked with dots) (with a 'Change' button)

Usage Notes

- The **Change** button is disabled if this action is not supported by the device, which means you must use the device UI to change the Access settings on the device. Refer to the device documentation or ask your system administrator for assistance.
- The IP address, username and password in Operations Manager must match the settings configured on the device. If a mismatch occurs, communication with the device will be lost, including new video streams and recordings.

Changing the Operations Manager Configuration Only

To change the settings used by Operations Manager to access the device over the network, do the following. The credentials configured on the device will not be affected.


-
- Step 1** Open the camera or encoder settings page as described in the [“Accessing the Camera Settings” section on page 8-42](#).
- Step 2** Select the **General** tab, if necessary.
- Step 3** Under *Access Information*, enter the new IP address, username and password.
- Step 4** Click **Save** to apply the changes.
-

Changing the Device Setting and Operations Manager Configuration

If the Change button is enabled, you can change the access settings stored on the device *and* the Operations Manager configuration.

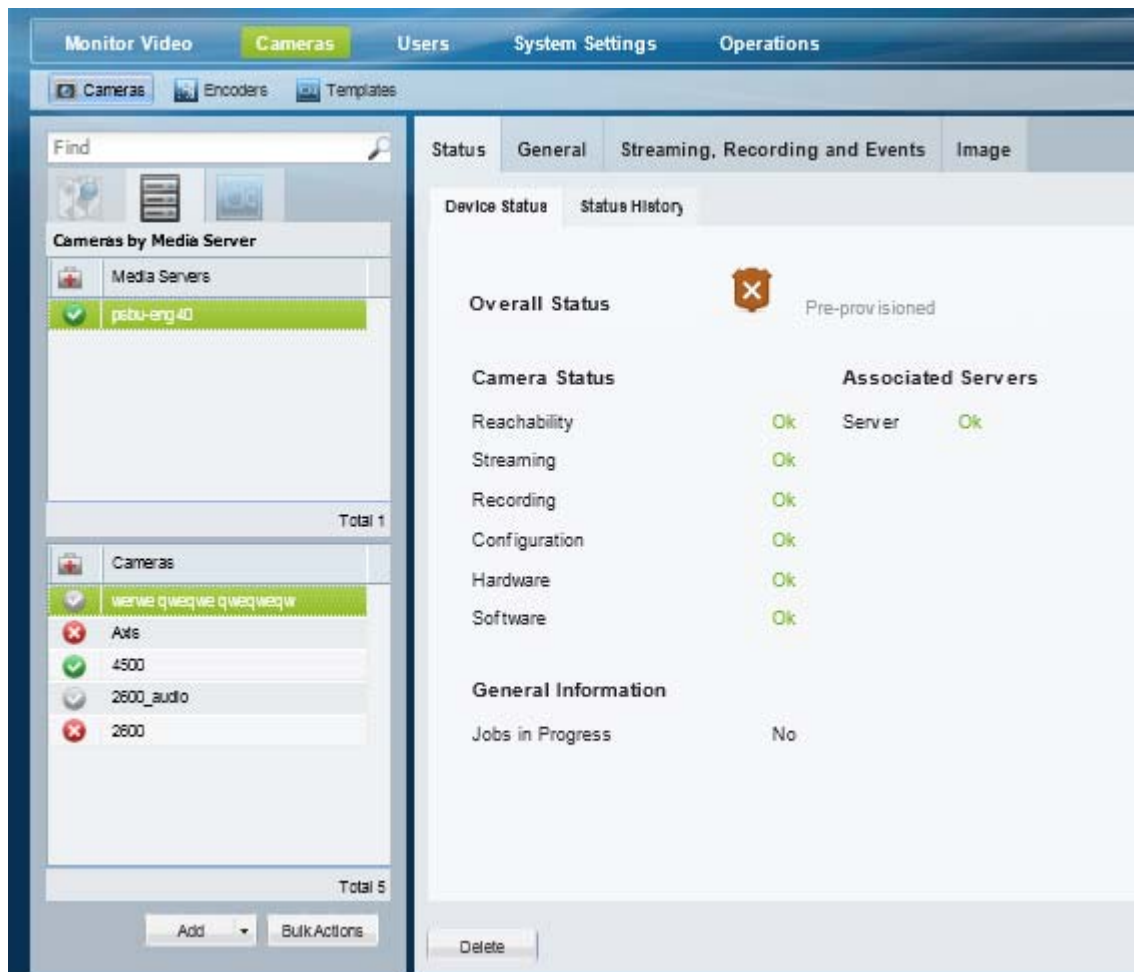
-
- Step 1** Click **Change** next to the entry field.
- Step 2** Enter the new network settings or credentials.
- Step 3** Click **OK** to save the changes.
- Step 4** (Optional) Verify the new settings:
- Click **View Status** to verify the Job was successfully completed.
 - Click the **Monitor Video** tab and select the camera name to view live video from the camera. For encoders, select an analog camera associated with the encoder.
-

Viewing Camera and Encoder Status

Click the camera or encoder **Status** tab (Figure 8-16) to display a snapshot of the camera health, including the camera's ability to communicate with a Media Server, stream video over the network, or record video. If a configuration error occurs, click the  icon to view additional information. You can also click the **Status History** tab to view the specific system events that impact the device status.

For more information see the “[Device Status: Identifying Issues for a Specific Device](#)” section on page 13-8.

Figure 8-16 Camera Device Status



The screenshot displays the Cisco VSM interface for viewing camera status. The top navigation bar includes tabs for Monitor Video, Cameras, Users, System Settings, and Operations. The sub-navigation bar shows Cameras, Encoders, and Templates. The left sidebar contains a search bar and two lists: 'Cameras by Media Server' (showing 'psbu-eng 40') and 'Cameras' (showing various models like 'various q weq we q weq weq we', 'Axis 4500', '2600_audio', and '2600'). The right panel shows the 'Status' tab for a selected camera, displaying 'Overall Status' as 'Pre-provisioned' with a warning icon. Below this, the 'Camera Status' section lists various metrics (Reachability, Streaming, Recording, Configuration, Hardware, Software) all marked as 'Ok'. The 'Associated Servers' section shows 'Server' as 'Ok'. The 'General Information' section shows 'Jobs in Progress' as 'No'.

When a camera is added to Cisco VSM, it is placed in either *Enabled* or *Pre-provisioned* state:



Note

Enabled means that the user intends the camera is to be functional. There are three possible sub-levels

[illegible]

Configuring Camera PTZ Controls, Presets, and Tours

Cameras that support pan (left-right), tilt (up-down) and zoom (in-out) movements can be controlled using either the on-screen PTZ controls, or a third-party joystick. PTZ control is available when viewing live video only.

In addition, you can configure PTZ cameras for the following:

- Create PTZ *presets* that allow operators to quickly jump to a preset position.
- Create PTZ *tours* that automatically cycle a camera between the PTZ preset positions.
- Create Advanced Events that automatically move the camera to a PTZ preset position when an event occurs.
- Define a Return To Home preset that automatically returns the camera to a selected Home position when idle for a specified number of seconds (see **Advanced Settings**).
- Define user groups that have priority for accessing PTZ controls.

Refer to the following topics for more information:

- [PTZ Requirements, page 8-66](#)
- [PTZ Camera Configuration Summary, page 8-67](#)
- [Defining the User Group PTZ Priority, page 8-69](#)
- [Using Camera PTZ Controls, page 8-70](#)
- [Configuring PTZ Presets, page 8-71](#)
- [Configuring PTZ Tours, page 8-73](#)
- [PTZ Advanced Settings, page 8-76](#)

Related information:

- [Using Pan, Tilt, and Zoom \(PTZ\) Controls, page 2-32](#)
- [Calibrating a Joystick for Windows 7, page 2-34](#)
- [Using Advanced Events to Trigger Actions, page 10-11](#)



See the [Example](#) in the “Defining the User Group PTZ Priority” section on page 8-69 to understand how users, events, tours and other features gain or are denied PTZ control based on their PTZ priority.

PTZ Requirements

Cameras that support PTZ controls automatically display an *Image* tab in the camera configuration that includes PTZ controls (choose the camera and click the **Image > Pan/Tilt/Zoom**).

PTZ cameras and PTZ users require the following:

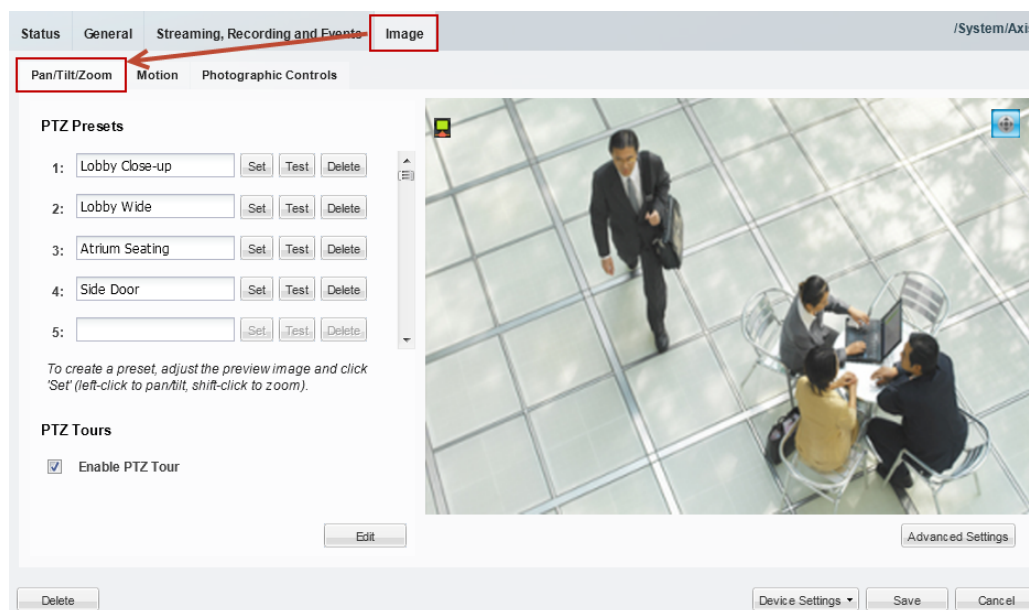
Table 8-16 **Camera PTZ Requirements**

Requirements	Requirement Complete? (✓)
Cameras must support PTZ functionality.	<input type="checkbox"/>
PTZ functionality must be enabled on the camera. See the camera documentation for more information.	<input type="checkbox"/>
To use PTZ controls, you must belong to a user group with <i>Perform PTZ</i> permissions.	<input type="checkbox"/>
To configure PTZ presets, PTZ tours, and Advanced Events, you must belong to a user group with <i>Cameras</i> permissions.	<input type="checkbox"/>
To configure the PTZ Priority and Lockout Period, you must belong to a user group with <i>Users & Roles</i> permissions.	<input type="checkbox"/>

PTZ Camera Configuration Summary

Cameras with PTZ functionality display a **Pan/Tilt/Zoom** tab under the **Image** tab of the Camera configuration page (Figure 8-17). Use the **Pan/Tilt/Zoom** tab to create PTZ presets, and PTZ tours. You can also use the Advanced Events to automatically trigger PTZ presets when an event occurs.

Figure 8-17 Camera PTZ Configuration



The following procedure summarizes the PTZ configuration options.

Procedure

	Task	Related Documentation
Step 1	Install the PTZ camera and enable PTZ functionality, if necessary.	See the camera documentation for more details. Some cameras require you to enable PTZ functionality. For example, analog cameras with PTZ capability may require the installation of a PTZ driver.
Step 2	Add the camera to the Cisco VSM configuration.	Adding and Managing Cameras, page 8-1.
Step 3	(Optional) Connect a PTZ joystick to a USB port on your PC and calibrate the device for Windows 7.	<ul style="list-style-type: none"> See the joystick documentation for more information. See the “Calibrating a Joystick for Windows 7” section on page 2-34.
Step 4	Open the camera PTZ configuration page to verify the camera PTZ controls are available: <ol style="list-style-type: none"> Select Cameras and select a camera name. Click the Image tab and verify that the Pan/Tilt/Zoom tab is selected (Figure 8-17). 	Accessing the Camera Settings, page 8-42

	Task	Related Documentation
Step 5	(Optional) Configure the camera PTZ presets. Presets are used to quickly adjust a camera view to a pre-defined PTZ setting.	Configuring PTZ Presets, page 8-71
Step 6	(Optional) Configure the camera PTZ tours. PTZ tours are used to cycle the camera view between PTZ presets.	Configuring PTZ Tours, page 8-73
Step 7	(Optional) Define if the camera should return to a selected Home position when idle for a specified number of seconds. Note If a PTZ tour is enabled, then the <i>Return to Home</i> setting is ignored	PTZ Advanced Settings, page 8-76
Step 8	(Optional) Enter the camera PTZ <i>idle</i> time that defines the following: <ul style="list-style-type: none"> PTZ Tour—the number of seconds after a manual PTZ movement or event action before the PTZ tour can resume. Return to Home—the number of seconds after a manual PTZ movement or event action before the camera returns to the <i>Return to Home</i> preset position. User PTZ control (priority lockout or camera controls lockout)—the number of seconds that a lower priority user has to wait before being able to move the camera after a higher priority user stops using the PTZ controls. Note PTZ tours and Return to Home have the lowest priority, allowing users and Advanced Events to assume PTZ control when necessary.	PTZ Advanced Settings, page 8-76
Step 9	(Optional) Define the user groups that have priority over other users for controlling PTZ cameras. Note By default, all user groups have the highest priority (100).	Defining the User Group PTZ Priority, page 8-69
Step 10	(Optional) Configure the <i>Advanced Events</i> that trigger a PTZ preset position.	Using Advanced Events to Trigger Actions, page 10-11

Defining the User Group PTZ Priority

A conflict can occur if multiple users attempt to use the PTZ controls for the same camera. For example, if a security incident occurs, a security officer may need to assume control over lower-priority users. To resolve this, each user group is assigned a PTZ priority number from 1 to 100. Users in a group with a higher number are given PTZ priority over users that belong to a group with a lower number. If the PTZ controls are in use by a lower-priority user, the higher-priority user can assume control immediately.

When a higher priority user assumes control of a PTZ camera, lower priority users are denied access to the PTZ controls. The lockout continues until the higher-priority user stops accessing the PTZ controls, *plus* the number of *idle* seconds defined in the *PTZ idle* setting (see the [“PTZ Advanced Settings” section on page 8-76](#)).

Usage Notes

- By default, all user groups have the highest priority (100).
 - See the [“Defining the User Group PTZ Priority Level” section on page 8-70](#) to define a lower value.
 - Users that belong to multiple user groups gain the highest priority from any assigned group.
- If a higher-priority user is using the PTZ controls, the PTZ controls remain locked and you cannot control the PTZ movements until released by the higher priority user (and the *idle* time has expired).
- If users belong to user groups with the same priority, they will be able to access the PTZ controls at the same time. This can result in conflicting movements.
- *Advanced Events* that trigger a PTZ preset position are assigned a priority of 50. This setting cannot be changed.
 - Event-triggered PTZ presets will take control from any user group members that have a priority lower than 50 (user groups with a higher priority can take control or will maintain control).
 - The camera remains at the PTZ preset unless a PTZ tour is enabled or a user accesses the PTZ controls.
 - See the [“Using Advanced Events to Trigger Actions” section on page 10-11](#) for more information
- *PTZ tours* and *Return to Home* are assigned the lowest priority by default. This allows users to assume control of any camera that is configured with a rotating PTZ tour. Event-triggered PTZ movements also override PTZ tours.
- When all users stop accessing the PTZ controls and *idle* time expires, the camera PTZ Tour or Return to Home position will resume, if configured (the PTZ tour continues). The lockout *idle* time is reset each time the higher-priority user accesses the PTZ controls. See the [“PTZ Advanced Settings” section on page 8-76](#).
- If the *When manual PTZ idle for* field is not defined, then cameras use the number of seconds in their associated Media Server’s *Camera Control Lockout* field (see the [“Media Server Properties” section on page 7-6](#)).

Example

The following example is based on this scenario:

- A PTZ tour is configured
- *user1* is in a user group with PTZ priority 60
- *user2* is in a user group with PTZ priority 100

- The PTZ *idle* time (lockout) is 30 seconds
- An Advanced Event is configured to move to the PTZ preset when a motion event occurs

A PTZ tour is enabled and rotating the camera between PTZ presets. *User1* can access the PTZ controls and interrupt the tour. However, if higher-priority *user2* also accesses the camera PTZ controls, then *user2* will take control and *user1*'s PTZ commands will be ignored. This is because *user2* is in a user group with priority 100 while *user1* is in a user group with priority 60 (PTZ tours have the lowest priority).


When the higher-priority *user2* stops moving the camera, *user1* must still wait the number of seconds defined in the camera *When Manual PTZ idle for* setting before they can move the camera again. If *user2* uses the PTZ controls within that idle time, then the timer is reset and *user1* must continue to wait.

Advanced Event PTZ movement is the same as a user with priority 50 moving the camera. If lower priority users (0-49) are moving the camera, those lower priority users will lose control of the camera and the event will PTZ move the camera. If higher priority users (51-100) are using the camera then the event PTZ movement will not happen.

If the event PTZ successfully moved the camera, then the camera's idle time lockout is set preventing lower priority users from moving the camera until it expires.

When all users stop accessing the PTZ controls, the PTZ tour continues (after the *idle* time expires).

Defining the User Group PTZ Priority Level

-
- Step 1** Define the PTZ priority for each user group.
- Select **Users**, and then select the **User Groups** tab .
 - Select a user group or create a new group (see the [“Adding User Groups”](#) section on page 4-10 for more information).
 - In the *PTZ priority over other user groups* field, select a number from 1 to 100 (the default is 100—highest priority).
 - Click **Save**.
- Step 2** (Optional) Enter the camera *idle* time to define the number of seconds a lower-priority user must wait after a higher-priority user stops using the PTZ controls. See the [“PTZ Advanced Settings”](#) section on page 8-76 for more information.
-

Using Camera PTZ Controls

Camera PTZ movements can be controlled using a mouse or joystick. See the [“Using Pan, Tilt, and Zoom \(PTZ\) Controls”](#) section on page 2-32 for more information.

Configuring PTZ Presets

PTZ *presets* allow operators to quickly jump to a preset position.

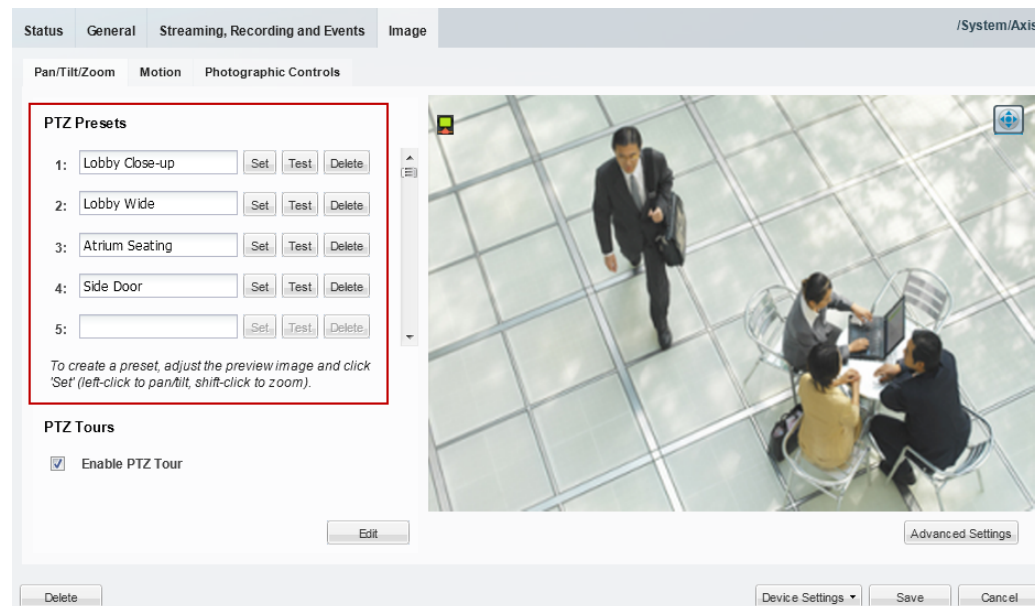
- To access the PTZ preset, go to the **Monitor** page, display the camera video, right-click the image and choose **Presets** from the **Pan, Tilt, and Zoom** menu. Choose a preset to move the camera to the defined position.
- To trigger presets with a USB joystick, press the joystick button that corresponds to the PTZ preset number. For example, joystick button 1 triggers PTZ preset 1, joystick button 2 triggers PTZ preset 2, etc.
- You can also create PTZ *tours* that automatically cycle a camera between the PTZ preset positions, or Advanced Events that automatically move the camera to a PTZ preset position when an event occurs.
- PTZ presets cannot be deleted if they are being used in a PTZ tour.
- If a camera is replaced, you must re-define the PTZ presets since the coordinates will not match the new device.

Related Topics

- [Using Pan, Tilt, and Zoom \(PTZ\) Controls, page 2-32](#)
- [Configuring PTZ Tours, page 8-73](#)
- [PTZ Advanced Settings, page 8-76](#)
- [Using Advanced Events to Trigger Actions, page 10-11](#)



To configure PTZ presets, use the PTZ controls to adjust the live video stream, enter a preset name, and click **Set**.

Figure 8-18 PTZ Preset Configuration



Procedure

To define PTZ presets, do the following:

-
- Step 1** Open the camera PTZ configuration page:
- Click **Cameras**.
 - Click a location or Media Server and select a camera.
 - Click the **Image** tab and then click **Pan/Tilt/Zoom** (Figure 8-18).
 - Verify that the PTZ controls are enabled  (if disabled, click the  icon to enable PTZ controls).
- Step 2** Position the camera using the following controls:
- Using a Mouse**
- Pan and Tilt—*Left-click* the image and drag the mouse right, left, up and down.
 - Zoom—*Shift-click* the image and drag the mouse up and down to zoom in and out.
- Using a USB Joystick**
- Pan—move the joystick bar horizontally.
 - Tilt— move the joystick bar vertically.
 - Zoom —twist the joystick.
- Step 3** Enter a PTZ Preset name.
- For example: *Lobby Door Close-up*.
- Step 4** Click **Set**.
- Step 5** (Optional) Click **Test** to move the camera position between different preset positions.
- Step 6** Repeat Step 2 through Step 5 to define additional PTZ presets.
- Step 7** Click **Save** to save the camera settings.
-

Configuring PTZ Tours

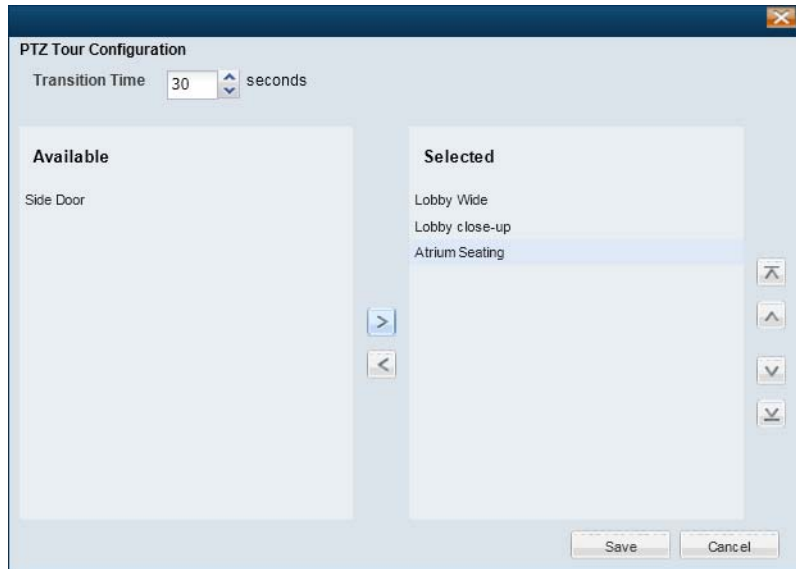
PTZ tours automatically rotate a camera's view between PTZ *presets* in a specified order, pausing at each position according to the specified *dwell time* . The camera will continue to rotate between the presets until interrupted or disabled by an operator or Advanced Event. When the last preset in the list is reached, the tour starts over at the beginning.

Usage Notes

- Any camera that supports PTZ presets also supports PTZ tours. At least two PTZ *presets* must be available to create a PTZ Tour.
- You can enable a single PTZ tour for each camera.
- PTZ tours have the lowest priority for PTZ camera movements. For example, operators can manually take PTZ control of the camera, or an Advanced Event can move the camera to a PTZ preset. Both users and events have priority PTZ access to the camera. See the [“Defining the User Group PTZ Priority” section on page 8-69](#) for more information.
- Operators can interrupt the tour by manually changing the PTZ position. The camera will stay at the user-selected position for the number of seconds configured in the Advanced Setting *“When manual PTZ idle for”*, and then resume the tour with the next preset. For more information, see:
 - [PTZ Advanced Settings, page 8-76](#)
 - [Using Pan, Tilt, and Zoom \(PTZ\) Controls, page 2-32](#)
- To stop the PTZ tour, deselect **Enable PTZ Tour**. The camera will return to the first PTZ preset in the tour list.
- If a PTZ tour is enabled, then the *Return to Home* setting is ignored (see the [“PTZ Advanced Settings” section on page 8-76](#)).
- If the PTZ tour is disabled, the camera will stay at the current position, or go to the *Return to Home* setting, if configured.

Procedure

-
- Step 1** Define at least two PTZ presets for the camera, as described in the [“Configuring PTZ Presets” section on page 8-71](#).
- Step 2** Define the PTZ presets included in the tour:
- a. Click **Add** or **Edit** ([Figure 8-20](#)) to open the PTZ Tour Configuration window ([Figure 8-19](#)).

Figure 8-19 PTZ Tour Configuration

- b. Select the *Transition Time* (the time that a camera stays at each preset position before changing to the next preset).
- c. Use the right-left arrows to move the presets from *Available* to *Selected*.



Note At least two presets must be included in the Selected column.

- d. Use the up-down arrows to move the presets up or down in the list to define the order of the preset rotation.
- e. Click **Save**.

Step 3 (Optional) Select **Enable PTZ Tour** to turn on the PTZ tour for the camera ([Figure 8-20](#)).

- The camera will display the PTZ tour whenever live video is displayed. To stop the PTZ tour, you must deselect **Enable PTZ Tour**.

Figure 8-20 **Enable the PTZ Tour**

The screenshot shows a web-based configuration interface for a camera. At the top, there are tabs: 'Status', 'General', 'Streaming, Recording and Events', and 'Image'. The 'Image' tab is selected. Below the tabs, there are sub-tabs: 'Pan/Tilt/Zoom', 'Motion', and 'Photographic Controls'. The 'Photographic Controls' sub-tab is active. The main content area is divided into two sections: 'PTZ Presets' and 'PTZ Tours'. The 'PTZ Presets' section contains five rows, each with a text input field and three buttons ('Set', 'Test', 'Delete'). The first four rows are labeled '1:', '2:', '3:', and '4:', with values 'Lobby Close-up', 'Lobby Wide', 'Atrium Seating', and 'Side Door' respectively. The fifth row is labeled '5:' and is empty. Below the presets, there is a note: 'To create a preset, adjust the preview image and click 'Set' (left-click to pan/tilt, shift-click to zoom).' The 'PTZ Tours' section is highlighted with a red rectangular box. It contains a single checkbox labeled 'Enable PTZ Tour', which is checked. Below the checkbox is an 'Edit' button. To the right of the configuration area is a vertical preview window showing a dark, narrow view of a hallway.

- Step 4** (Optional) Define the camera PTZ idle time to define the amount of time the number of seconds after a manual PTZ movement or event action before the PTZ tour can resume. See the [“PTZ Advanced Settings”](#) section on page 8-76 for more information.

PTZ Advanced Settings

Use the camera PTZ **Advanced Settings** to define if the camera should return to a selected Home position when idle for a specified number of seconds.

The idle setting also defines the number of seconds before a PTZ tour resumes (after a manual or event override), and the number of seconds a lower priority PTZ user must wait after a higher-priority user stops using the camera PTZ controls.

Table 8-17 Camera PTZ Advanced Settings

Setting	Description
When manual PTZ idle for	<p>The number of seconds the camera can be idle (no PTZ commands) before the camera returns to the home PTZ preset or continues a PTZ tour (see the <i>Return to Home</i> setting).</p> <p>Note By default, the idle time is defined by the Media Server's <i>Camera Control Lockout</i> setting (see the “Media Server Properties” section on page 7-6). Use the <i>When manual PTZ idle for</i> field to override the server setting for the current camera.</p> <ul style="list-style-type: none"> PTZ Tour—the number of seconds after a manual PTZ movement or event action before the PTZ tour can resume. The timer is reset whenever the camera PTZ controls are used by an operator or event action. See the “Configuring PTZ Tours” section on page 8-73. Return to Home—the number of seconds after a manual PTZ movement or event action before the camera returns to the <i>Return to Home</i> preset position. The timer is reset whenever the camera PTZ controls are used by an operator or event action. User PTZ control (priority lockout or camera controls lockout)—the number of seconds that a lower priority user has to wait before being able to move the camera after a higher priority user stops using the PTZ controls. See the “Defining the User Group PTZ Priority” section on page 8-69.
Enable Home Preset	<p>If enabled, the camera will move to the <i>Return to Home</i> preset location if idle for the number of seconds in the <i>When manual PTZ idle for</i> setting. Deselect this option to disable the <i>Return to Home</i> feature.</p> <p>Note If a PTZ tour is enabled, then the <i>Return to Home</i> setting is ignored.</p>
Return to Home	Select the PTZ preset used as the <i>Home</i> position.

Configuring Motion Detection

Cameras that support motion detection can trigger actions or record video when motion occurs in the camera's field of view. For example, a camera pointed at the rear door of a building can record a *motion event* if a person walks into the video frame. A *motion event* can also trigger alert notifications, a camera's PTZ controls, or a URL action on a third party system.

- Motion detection is supported for analog cameras only if the encoder supports motion detection.
- Motion detection is supported only for the primary (Stream A) video.
- Motion can be detected for a camera's entire field of view, or for specified areas. If the camera or encoder supports exclusion areas, you can also exclude areas where motion should be ignored.
- Motion detection must be configured for each camera (motion detection is not defined by camera templates). Use Bulk Actions to locate cameras without motion detection and add motion detection for the cameras' entire field of view (see [Enabling Motion Detection on All Existing Cameras \(Bulk Actions\)](#), page 8-82).
- Alerts can be configured for motion events, contact closures, analytic events, or soft triggers. Always configure these features carefully to avoid overwhelming operator(s) with an excessive number of alerts. If an excessive amount of alerts are generated, the system may ignore new alerts while deleting old entries.

Refer to the following topics for more information.

- [Motion Detection Overview](#), page 8-78
- [Motion Detection Settings](#), page 8-79
- [Configuring Motion Detection](#), page 8-80
- [Enabling Motion Detection on All Existing Cameras \(Bulk Actions\)](#), page 8-82

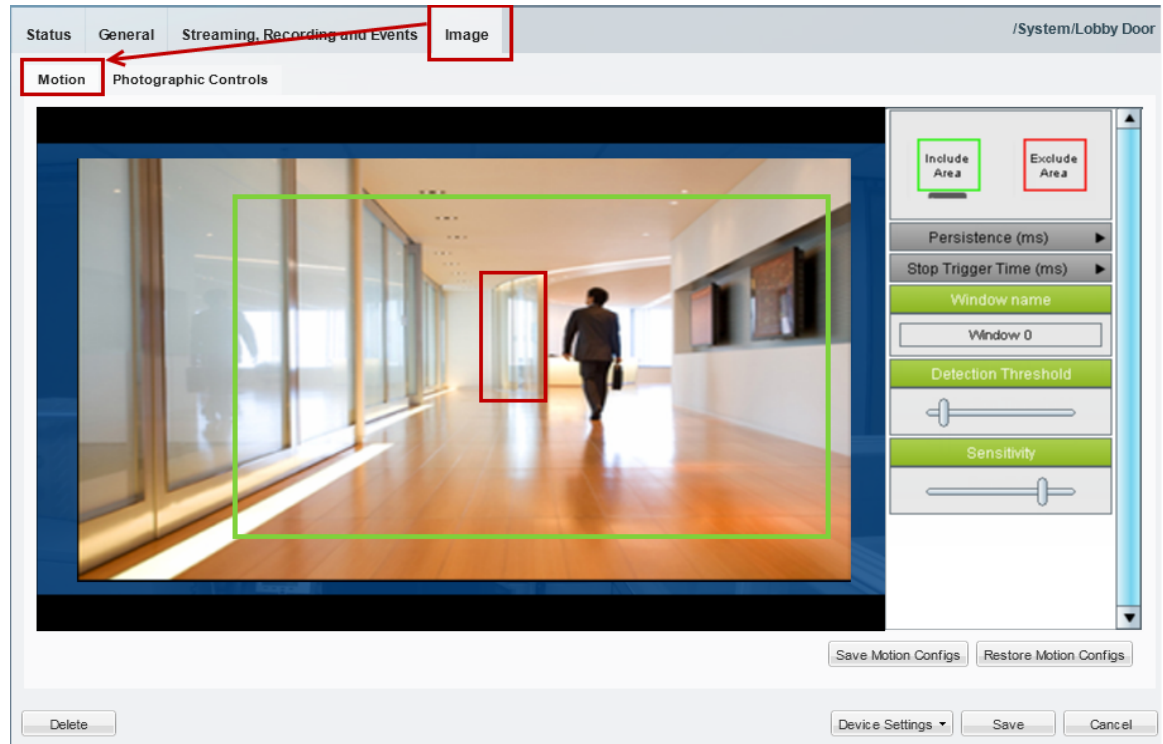
Related Documentation

[Using Advanced Events to Trigger Actions](#), page 10-11—Define additional actions that are triggered when motion events start or stop.

Motion Detection Overview

Cameras that support motion detection display a Motion tab under the camera Image settings (Figure 8-21).

Figure 8-21 Configuring Motion Detection



To enable *motion events*, you must define the areas in the camera image that should detect motion. You can define the entire field of view, or use the *Include Area* to draw a box where motion will be detected (Figure 8-21). Motion outside of the *include* box(es) is ignored. Add *exclude areas* within *include* boxes to also ignore motion in a portion of the included areas.



Tip

See the “[Enabling Motion Detection on All Existing Cameras \(Bulk Actions\)](#)” section on page 8-82 to include the entire field of view for multiple cameras.

See the “[Configuring Motion Detection](#)” section on page 8-80 for more information. Use the settings to the right of the preview window to define additional motion detection settings, as described in the [Motion Detection Settings](#), page 8-79.

Motion Detection Settings

Use the settings described in [Table 8-18](#) to define the portions of the camera image to include or exclude, and how sensitive the included areas should be (see the example in [Figure 8-21](#)). Refer to the “[Configuring Motion Detection](#)” section on page 8-80 for information to access and save these settings.

Table 8-18 **Motion Detection Settings**


Setting/Field	Description
Include Area	Drag and drop the Include Area box onto the image to define a window where motion should be detected.
Exclude Area	<p>Drag and drop the Exclude Area box onto the image to exclude portions of the included area.</p> <p>For example, if the include area covers an entire room, you can exclude an area where regular motion occurs, such as a clock or fan. Exclude areas are used to reduce unwanted motion events.</p>
Persistence	<p>The amount of time that motion must occur (within the selected window) for a motion event <i>start</i> to occur.</p> <p>The recommended value is 0 (default): motion of any duration results in a motion <i>start</i> event. Select a higher number if the motion duration should continue longer before a motion event is triggered.</p>
Stop Trigger Time	<p>Determines how many seconds to delay when a motion event is considered to have stopped (after the actual motion has ended).</p> <p>Recommended value is 0 (default): the event stops immediately when the motion ends. Select a higher number to define a motion event delay.</p> <p>This setting prevents multiple motion events from being triggered when motion reoccurs in a short period of time. Select a time that will result in only one event for the “burst of motion activity”.</p>
Window Name	<p>The name of the selected motion window.</p> <p>Click an <i>include</i> or <i>exclude</i> area, and enter a meaningful name.</p>
Detection Threshold and Sensitivity	<p>(<i>Include Areas</i> only)</p> <ul style="list-style-type: none"> Detection Threshold—The size of object needed to trigger a motion start. Sensitivity—Determines the degree of susceptibility to motion. The more sensitive, the less motion is needed to trigger a motion start. <p>These values are set by default based on the recommended settings for the camera model. For example:</p> <ul style="list-style-type: none"> Cisco 26xx: Threshold = 10, Sensitivity = 80 Cisco 29xx: Threshold = 10 Sensitivity = 80 Cisco 45xx: Threshold = 10 Sensitivity = 80 Cisco 60xx: Threshold = 1, Sensitivity = 85 <p>(The maximum value is 100. The minimum value is 0.)</p>

Table 8-18 **Motion Detection Settings (continued)**

Setting/Field	Description
Save Motion Configs	Saves the changes to the cameras motion detection settings.
Restore Motion Configs	Restores the settings to the previous saved values.

Configuring Motion Detection

Procedure

-
- Step 1** Verify that the camera or encoder supports motion detection.
See the camera or encoder documentation for more information.
- Step 2** Log on to the Operations Manager.
You must belong to a User Group with permissions for *Cameras*. See the [“Adding Users, User Groups, and Permissions” section on page 4-1](#) for more information.
- Step 3** (Optional) Complete the [“Enabling Motion Detection on All Existing Cameras \(Bulk Actions\)” section on page 8-82](#).
- Step 4** Open the camera configuration page:
- Click **Cameras**.
 - Select the camera’s location, Media Server or template.
 - Select the camera from the list in the lower left column.
- Step 5** Click the **Image** tab.
- Step 6** Click the **Motion** tab.
The current camera image appears ([Figure 8-21](#)).
- Step 7** Add green *Include Areas* (windows) where motion should be detected in the image.
- Drag the green **Include Area** box onto the video image ([Figure 8-21](#)).
 - (Optional) Enter a name in the Window Name field.
 - Move and resize the motion window.
 - To move the window, click and hold within the window, then use the move cursor  to drag the window to a new location.
 - To resize the window, click and hold the corner or edge to change the size and shape.
 - Repeat these steps to create additional *Include Areas* in the video frame.
- Step 8** Define the motion detection settings for each *Include Area*.
- Click the motion window to select it.
 - Change the motion detection settings, as necessary, as described in [Figure 8-21 on page 8-78](#).
- Step 9** (Optional) Add a red **Exclude Area** box within an include box to define where motion should be ignored ([Figure 8-21](#)).

**Note**

All areas outside of the *include* boxes are ignored by default. Add *exclude* areas within *include* boxes to also ignore motion within the included areas.

- a. Drag the red **Exclude Area** box onto the video image ([Figure 8-21](#)).
- b. (Optional) Enter a name in the Window Name field.
- c. Move and resize the motion window.

Step 10 Click **Save Motion Configs**.

**Tip**

Click **Restore Motion Configs** to return the settings to the previously saved value.

Step 11 (Optional) Configure motion event recordings for a camera or template.

See the following for more information:

- [Editing the Camera Settings, page 8-42](#)
- [Configuring Continuous, Scheduled, and Motion Recordings, page 10-7](#)

Step 12 (Optional) Configure actions that are triggered when a motion event occurs.

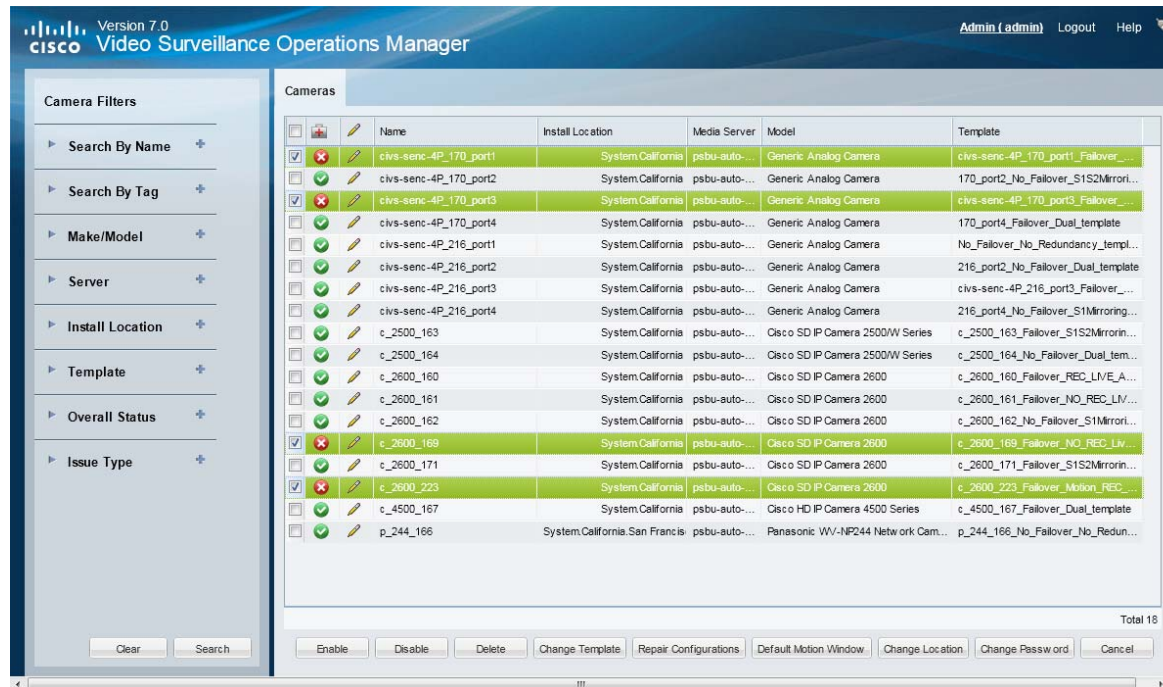
See the [“Using Advanced Events to Trigger Actions”](#) section on page 10-11.

Enabling Motion Detection on All Existing Cameras (Bulk Actions)

Use the *Bulk Actions* feature to discover all cameras where motion detection is unconfigured, and add a default motion window that includes the entire field of view (Figure 8-22).

This process selects the entire camera view to be included in the motion window. Use the camera configuration page to make further refinements or define *excluded* areas (see the “Configuring Motion Detection” section on page 8-80).

Figure 8-22 Bulk Actions



Procedure

- Step 1** Click **Cameras** to open the camera configuration page.
- Step 2** Click **Bulk Actions**.
- Step 3** Expand **Issue Type** and select **Motion Unconfigured**.
- Step 4** Click **Search**.
- Step 5** Select the cameras from the listed results.
- Step 6** Click **Default Motion Window** and confirm the change.
- Step 7** (Optional) Use the camera configuration page to refine the motion detection areas and sensitivity for each camera.
 - [Motion Detection Settings, page 8-79](#)
 - [Configuring Motion Detection, page 8-80](#)

Replacing a Camera

Replacing a camera allows you to exchange the physical camera hardware while retaining the configurations, associations and historical data of the original device. The replacement camera also uses the original camera name and device unique ID (used in API calls).

After the camera is replaced, only the hardware-specific details are changed, including the device MAC address, IP address, and camera make and model.

Camera Attributes That Are Retained

For example replacing a network or analog camera allows you to use new hardware while retaining the following:

- Existing recordings are retained.
- The new camera continues to stream video using the original camera name.
- Alert and audit records are retained.
- The camera association in maps, Views and locations is retained, allowing users to continue to access the camera based on the user's access permissions and available features.

Configurations That Must Be Reapplied On the New Camera

When a network or analog camera is replaced, you must re-configure the contact closure, PTZ preset and motion detection settings (see [Step 7](#)). Analog cameras must also reconfigure the serial connection.

Usage Notes

- Both network and analog cameras can be replaced (network cameras require the username and password configured on the device).
- Any network (IP) camera can be replaced by any other network (IP) camera, even if the devices are a different make and model (be sure to select the appropriate template for the new camera model). Network (IP) cameras cannot be replaced by an analog camera or encoder (or vice-versa).

Camera Replacement Procedure

-
- Step 1** Add the replacement camera to Cisco VSM.
- The replacement camera can be in *pre-provisioned* or *Enabled* states.
- Step 2** Open the camera configuration page for the existing camera (the camera to be replaced).
See the [“Accessing the Camera Settings”](#) section on page 8-42.
- Step 3** Select **Device Settings > Replace Camera**.
- Step 4** Enter the settings for the replacement camera

Table 8-19 **Replace Camera Settings**

Setting	Description
Camera	(Read-only) The name of the existing camera.

Table 8-19 Replace Camera Settings (continued)

Replace With	<p>(Required) Select the new (replacement) camera.</p> <ul style="list-style-type: none"> The replacement camera must be in either <i>pre-provisioned</i> or <i>Enabled</i> state (cameras that are soft-deleted or blacklisted are unavailable). The name, historical data, unique ID and configurations of the existing camera will be transferred to the replacement camera. Only hardware information such as MAC ID, IP address and make and model will be changed in the camera configuration.
Template	<p>(Required) Select the camera template.</p> <ul style="list-style-type: none"> The template is populated if defined when the replacement camera was added. You can choose a different template, if necessary. Select a template that is appropriate for the new make and model.
Username/ Password	<p>(Required for IP Cameras Only) Enter the credentials used to access the replacement camera on the network.</p> <ul style="list-style-type: none"> These fields are populated if defined when the replacement camera was added. You can modify the username and password, if necessary, but the entries must match the credentials that were configured on the camera. This field is required for IP cameras only. Analog cameras do not require a password since they are connected to an encoder.

Step 5 Click **Replace**.

Step 6 Wait for the page to reload.



Tip

When the page returns, the new camera will appear with the same name as the old camera, and will include all configurations, recordings, and event histories. Associations with locations, maps, and Views are also the same.

Step 7 Re-configure the contact closure, PTZ preset and motion detection settings. See the following topics for more information. Analog cameras must also reconfigure the serial connection.

- [Editing the Camera Settings, page 8-42](#)
- [Configuring PTZ Presets, page 8-71](#)
- [Configuring Motion Detection, page 8-77](#)
- [Adding External Encoders and Analog Cameras, page 11-5](#)

Bulk Actions: Revising Multiple Cameras

Bulk Actions allows you to change the configuration or take actions for multiple cameras. For example, you can enable, disable, or delete the devices. You can also change the template, repair the configurations, change the location or change the password used to access the device.

To begin, filter the devices by attributes such as name, tags, model, Media Server, location, status, or issue. You can then apply changes to the resulting devices.

Requirements

- Users must belong to a User Group with permissions to manage *Cameras*.
- Only super-admin users can apply the **Change Password** option using Bulk Actions. Non-super-users must use the device configuration page to change one device at a time.
- See the “Adding Users, User Groups, and Permissions” section on page 4-1 for more information.

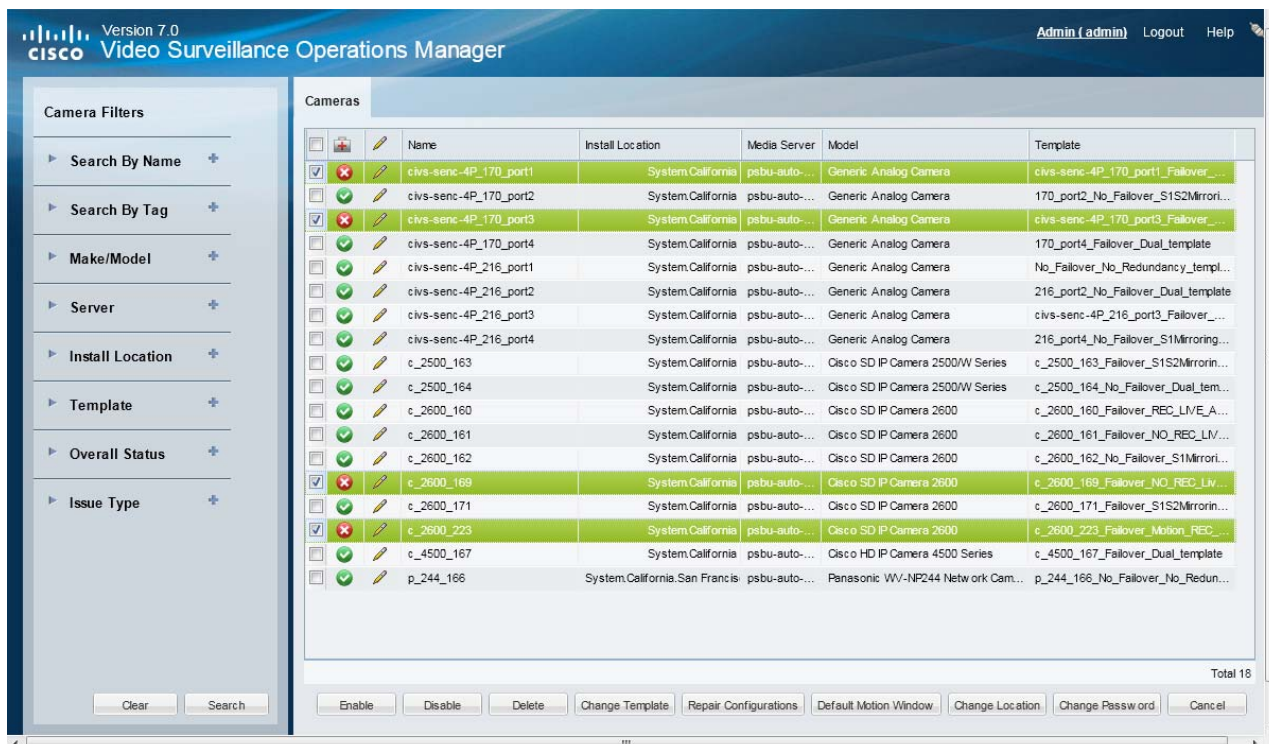
Related Topics

- [Bulk Actions: Revising Multiple Encoders, page 11-11](#)
- [Bulk Actions: Revising Multiple Servers, page 6-19](#).

Procedure

- Step 1** Select **Cameras > Cameras**.
- Step 2** Click **Bulk Actions** (under the device list) to open the Bulk Actions window ([Figure 8-23](#)).

Figure 8-23 Bulk Actions Window





Step 3 Click the  icon next to each field to select the filter criteria (Table 8-20).

Table 8-20 Bulk Action Filters

Filter	Description
Search by Name	Enter the full or partial device name. For example, enter “Door” or “Do” to include all device names that include “Door”.
Search by Tag	Enter the full or partial tag string and press <code>Enter</code> .
Make/Model	Select the device model(s). For example, “Cisco HD IP Camera 4300E Series”.
Server	Select the Media Server associated with the devices.
Install Location	Select the location where the devices are installed.
Template	Select the templates assigned to the device.
Overall Status	<p>Select the administrative states for the devices. For example:</p> <ul style="list-style-type: none"> • Enabled (OK, Warning or Critical)—The device is enabled, although it may include a <i>Warning</i> or <i>Critical</i> event. • Disabled—The device is disabled and unavailable for use. The configuration can be modified, and any existing recordings can be viewed, but cameras cannot stream or record new video. • Pre-provisioned—The device is waiting to be added to the network and is not available for use. A pre-provisioned camera can be modified, but the camera cannot stream or record video until you choose Enable from the Device Settings menu. • Soft Deleted—The device is removed from Cisco VSM but the recordings associated with that device are still available for viewing (until removed due to grooming policies). <p>Tip See the “Device Status: Identifying Issues for a Specific Device” section on page 13-8 for more information.</p>
Issue Type	<p>Select the issues that apply to the device. For example:</p> <ul style="list-style-type: none"> • Configuration Mismatch—the camera configuration on the Media Server is different than the camera configuration in the Operations Manager. <p>Tip Always use the Operations Manager to configure cameras. Changes made directly to the camera are unknown to Cisco VSM and can result in incorrect behavior.</p> <ul style="list-style-type: none"> • Capability Mismatch—the capabilities on the camera do not match the Cisco VSM configuration. • Identity Collision—the camera has an IP address or hostname that is the same as another device. • Motion Unconfigured—motion is not configured on the camera.

Step 4 Click **Search**.

Step 5 (Optional) Click the  icon to view and edit the device status and configuration settings.

Step 6 Select the devices that will be affected by the action.

- Choose the *Select All* check box to select ALL cameras matched by the filters, including the devices not shown in the grid.
- Use CTRL-CLICK and SHIFT-CLICK or to select multiple items.

- Step 7** Click an *Action* button.
- For example, Enable, Disable, Delete, Change Template, Change Location, etc.
- Step 8** Follow the onscreen instructions to enter or select additional input, if necessary.
- For example, *Reapply Template* requires that you select the template.
- Step 9** Refer to the Jobs page to view the action status.
- See the [“Understanding Jobs and Job Status” section on page 13-25](#).
-



CHAPTER 9

Defining Schedules

Schedules are used to define what type of video recording should be used at different times of the day. For example, a school administrator might want continuous recording for all lobby doors during school hours on weekdays, but only motion recording at night and on weekends. In addition, special events (such as an evening concert) or holidays (such as Christmas) might require different recording rules.

Procedure

Complete the following procedure to add or edit schedules.



Tip

To apply a schedule to a camera or template configuration, see the [“Adding and Managing Cameras” section on page 8-1](#).

Step 1 Select **System Settings > Schedules**.

Step 2 Add or edit a schedule:

- Click **Add**, or
- Select an existing schedule to edit the settings.

Step 3 (Required) Enter a schedule *Name* and *Location*.

The location defines the following:

- The users who can update or delete the schedule. Only users assigned to the same location can access the schedule.
- The users who can use the schedule in cameras and templates configurations. Users assigned to the same location, or a child location, can assign the schedule to a camera or template configuration.

For example, if a schedule is assigned the *California* location, a user must also have access to the same location (*California*) to manage the schedule. However, users who have access to child locations (such as *San Jose*, *San Francisco* or *Milpitas*) can use the schedule for camera and template configurations.

Step 4 (Optional) Enter a *Description* for the schedule.

For example: *School campus when in session*.

Step 5 Click **Create**.

Step 6 Click the **Recurring Weekly Patterns** tab.

Step 7 Define the *Time Slots* for the schedule ([Figure 9-1](#)).

In the camera or template configuration, each time slot can be assigned a different set of recording and alert rules.

Figure 9-1 Time Slots

a. Click a Time Slot entry field.

b. Enter a descriptive name.

For example: *School Hours*

c. Edit additional Time Slot fields, if necessary.

For example, a school might require different video surveillance actions during the following:

<i>School Hours</i>	Hours when school is in session.
<i>After School</i>	Hours outside of the regular school schedule.
<i>School Off</i>	Hours when school or other activities are not in session.
<i>Closed</i>	Hours when the school is closed.

- Changes are saved when entered.
- Define time slots for *Special Events* and *Holidays* if your site requires different recording rules during those occasions.
- *Time Slots* cannot be added or deleted if the schedule is used by a camera template or other Cisco VSM feature. Existing time slots can be renamed, however, and the schedule can be changed. For example, *Work Hours* could change from 9-5 Monday-Friday to 8-6 Monday-Saturday.
- You can change the schedule used by a camera template at any time.

Step 8 Define the *Active Pattern* for each day of the week (Figure 9-2).

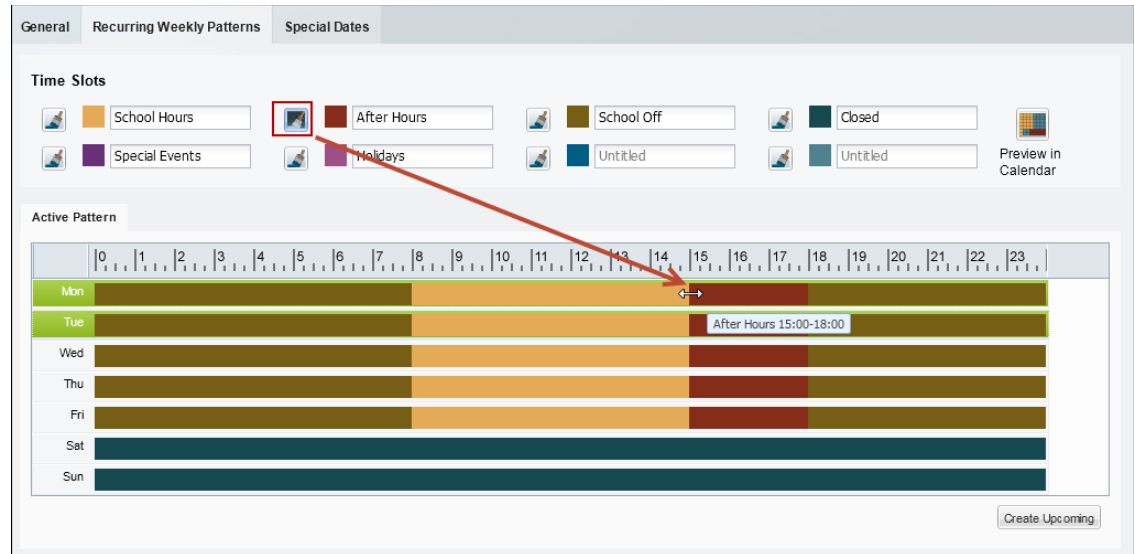
Active Patterns are the recurring schedule for each day. Paint the appropriate time slot over the hours that the time slot should be active.

- Select a time slot paint brush (the selected icon turns solid).
- Click the day of the week (on the *Active Pattern* calendar) where the time slot should be used.
A 1-hour block of time is painted with the selected Time Slot color.
- Drag the right and left edges of the time slot color to the appropriate start and end times.
This process paints over any existing time slot color.
- Repeat these steps to complete the recurring weekly patterns for each day of the week.
- Click **Save**.



Tip

The shortest time-block that can be created is 15 minutes.

Figure 9-2 Adding a Time Slot to the Active Pattern

Note A time slot must be defined for all hours and days.

For example, different recording rules can be applied when a school is in session, during after school activities, or when the school is closed. Each of these different time slots can be assigned different recording and alert properties (in the template configuration screen).

The example in [Figure 9-2](#) defines the following schedule:

- *School Hours* are from 8 a.m. to 3 p.m. Monday through Friday.
- *After School* hours are 3 p.m. to 6 p.m. Monday through Friday.
- *School Off* hours are 6 p.m. to 8 a.m. Monday through Friday.
- The school is *Closed* Saturday and Sunday.

Step 9 (Optional) Click **Preview in Calendar** to view a monthly calendar of the recurring schedule.

Step 10 (Optional) Click **Create Upcoming** to define a second schedule that will become active on a specified date ([Figure 9-3](#)).



Tip When an *Upcoming Pattern* becomes active, the old schedule is deactivated and renamed *Expired Pattern*. Expired patterns cannot be reactivated.

- Each Schedule can define two weekly recurring patterns: the *Active Pattern* and the *Upcoming Pattern*.
- *Active Patterns* are active indefinitely unless an *Upcoming Pattern* is defined.
- To create a new pattern, you must first delete one of the existing patterns. To remove a pattern, select the pattern tab and click **Delete**.
- When the *Upcoming Pattern* takes effect, the following occurs:
 - The *Upcoming Pattern* becomes the *Active Pattern*.

- The previous *Active Pattern* becomes an Expired Pattern. Click the **Expired Pattern** tab to delete it.

Figure 9-3 Defining an Upcoming Recurring Weekly Pattern

- Click **Create Upcoming** (Figure 9-2) to create an *Upcoming Pattern* (Figure 9-3). An *Upcoming Pattern* tab is added and pre-populated with the calendar from the *Active Pattern*.
- Click the **Effective Date** to select the date when the *Upcoming Pattern* will take effect.
- Define the time slots for each day of the week (as described in Step 8).



Tip The default *Upcoming Pattern* is a copy of the *Active Pattern*. Modify the recurring pattern as necessary.

- (Optional) Click **Preview in Calendar** to verify that the weekly recurring schedule changes on the time and date desired.
- Click **Save**.

For example, in Figure 9-3, the school hours are extended to 4 p.m. (16:00) on Monday and Friday (beginning on the *Effective Date*).

Step 11 (Optional) Define *Special Dates* to override the normal recurring schedule (Figure 9-4).

Special dates can be created for holidays, vacations, or other one-time events that require different recording or Advanced Event settings. For example, a special schedule may be required for a few hours (during an evening event), a single day (such as a Homecoming), or an entire week (such as the Christmas holiday).

For example, in Figure 9-4, the entire week of Christmas is defined as a Holiday. Homecoming and an evening concert, however, require a different time slot for only a few hours of the day. Any time left blank will use the *Recurring Schedule* definitions.

Figure 9-4 Defining Special Dates

- a. Click the **Special Dates** tab (Figure 9-4).
- b. Click **Add**.
- c. Enter the event **Name**.
- d. Enter the **Start Date** and **End Date**.
- e. Add time slots to define the time when the recurring schedule should be overridden (as described in Step 8).

For example, add the *Special Event* time slot from 1 to 3 p.m. to override the recurring schedule at that time. Any times left blanks will use the recurring schedule definitions.

- Click a time slot paint brush icon to highlight it (the selected icon turns solid).
- Click the time of day when the time slot should be used (Figure 9-4).
- Click and drag the right and left edges of the time slot color to define the start and end times.
- This process paints over any existing time slot color.



Tip Click **Clear Cells** and then click a time of day to delete the time slots defined for that time. Any time left blank will use the recurring schedule definitions.

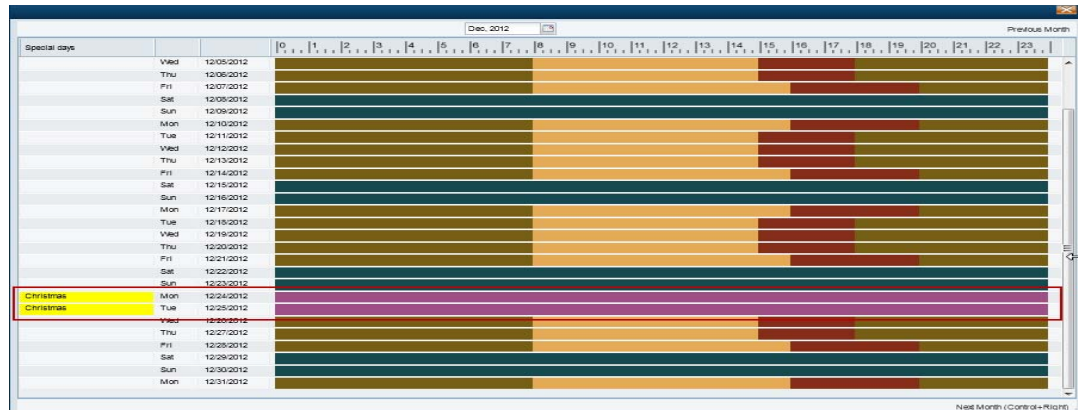
- f. Repeat these steps to define the time slot used for each hour of the day.



Tip Click the trash icon to delete a Special Date entry. Click **Yes** to confirm the change.

- g. (Optional) Click **Preview in Calendar** to see the special date in a monthly calendar (Figure 9-5).

Figure 9-5 *Previewing Special Dates in the Monthly Calendar*



Step 12 Click **Save**.

Step 13 Use the schedules to define recording schedules, alerts, or advanced events as described in the following topics:

- [“Streaming, Recording and Event Settings” section on page 8-49](#)
- [“Configuring Video Recording” section on page 10-7](#)
- [“Using Advanced Events to Trigger Actions” section on page 10-11](#)



CHAPTER 10

Adding and Editing Camera Templates

Templates simplify camera configuration by defining the image quality, recording schedule and other attributes used by a set of cameras.

Contents

- [Overview, page 10-2](#)
- [Creating or Modifying a Template, page 10-3](#)
- [Creating a Custom Template for a Single Camera, page 10-5](#)
- [Configuring Video Recording, page 10-7](#)
- [Using Advanced Events to Trigger Actions, page 10-11](#)
 - [Configuration Overview, page 10-12](#)
 - [Trigger and Action Descriptions, page 10-13](#)
 - [Configuration Summary, page 10-12](#)
 - [Configuring Soft Triggers, page 10-15](#)
- [Configuring Multicast Video Streaming, page 10-18](#)



Note

See also the [“Enabling Record Now”](#) section on page 3-12.

Overview

Templates simplify camera configuration by defining the image quality, recording schedule and other attributes used by a set of cameras. Any template changes are applied to all cameras associated with that template, allowing you to easily configure and modify groups of cameras that serve a similar purpose. You can also create *Custom Templates* that apply to a single camera.

- *Model Specific* templates are used for a specific make and model of camera.
- *Generic* templates can be applied to a mixture of camera models.
- *Custom Templates* apply to a single camera.

Figure 10-1 shows a sample template configuration page. The number of cameras associated with a template is shown next to the template name.


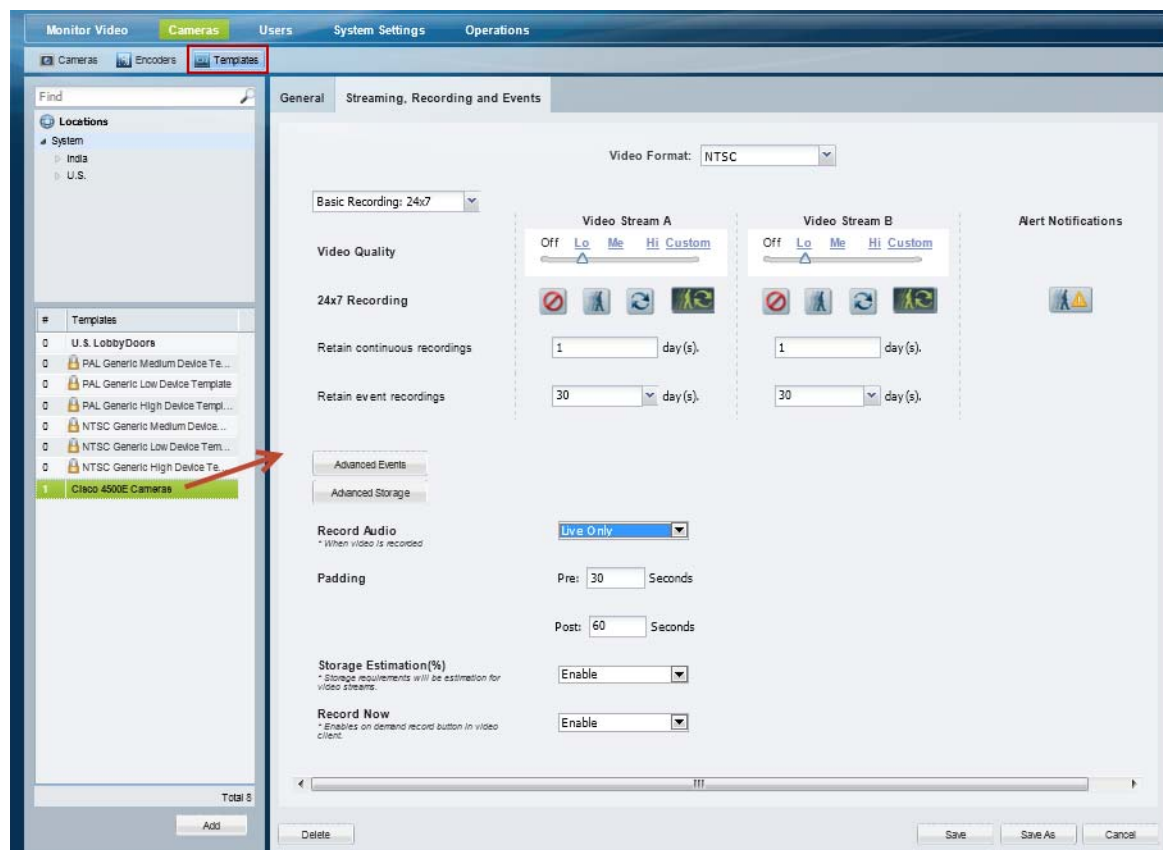
- System defined templates are locked  and cannot be modified. Click **Save As** to create a new template under a different name.
- User-defined templates are displayed in bold and can be revised. See the “[Creating or Modifying a Template](#)” section on page 10-3.

Figure 10-1 Camera Templates



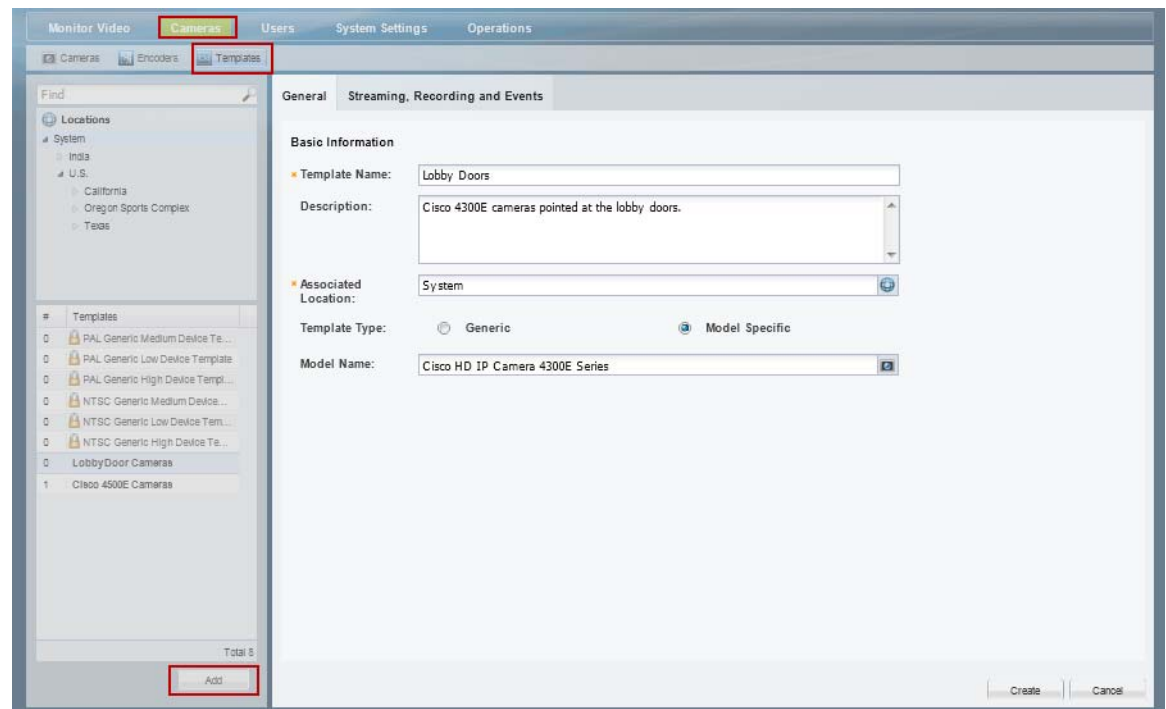
Creating or Modifying a Template

Procedure

To create or modify a template, complete the following procedure.


- Step 1** Log on to the Operations Manager.
- See the “Logging In” section on page 1-18.
 - You must belong to a User Group with permissions for *Templates*. See the [Adding Users, User Groups, and Permissions](#), page 4-1 for more information.
- Step 2** Select **Cameras > Templates** (Figure 10-2).

Figure 10-2 *Templates*



- Step 3** Edit or add a template:
- Click **Add** to create a new template.
 - To edit a template, select a location and template name.



Note System defined templates are locked  and cannot be modified.

- Step 4** Enter or revise the **General** settings:
- Template Name—(Required) Enter a descriptive name for the template.
 - Description—(Optional) Enter the purpose of the template, or other description.
 - Associated Location—(Required) Select the location for the template. This can be used to restrict access to a template to a specific location. For example, to administrators located on Campus 1.

- Template Type—(Required for new templates) Select **Generic** or **Model Specific**. Model specific templates are available for use only by the specific camera model. Generic templates can be assigned to any camera model.
- Model name—(Model specific templates only) select a camera model from the pop-up window.

Step 5 Click the **Streaming, Recording and Events** tab to define the streaming, recording and other properties.

- For example, define the quality of video from stream A and B, the recording schedule, and advanced events and storage options.
- See the following topics for more information.
 - [Configuring Video Recording, page 10-7](#)
 - [Streaming, Recording and Event Settings, page 8-49](#)

Step 6 Click **Create, Save** or **Save As**.

Step 7 Wait for the *Job* to complete.

- If you are modifying an existing template, the changes are applied to each camera associated with the template. A *Job Step* is created for each camera impacted by the template change.
 - If a large number of cameras are affected, the Job can take a significant amount of time to complete.
 - See the [“Understanding Jobs and Job Status” section on page 13-25](#) for more information.
 - Device configuration changes can fail if a camera firmware upgrade is in process. Make sure that a camera firmware is not being upgraded (or wait until it is complete) and try again.
-

Creating a Custom Template for a Single Camera

Although templates are usually applied to multiple cameras, you can also create a custom configuration for a specific camera using the *Custom* template option (Figure 10-3).

Procedure


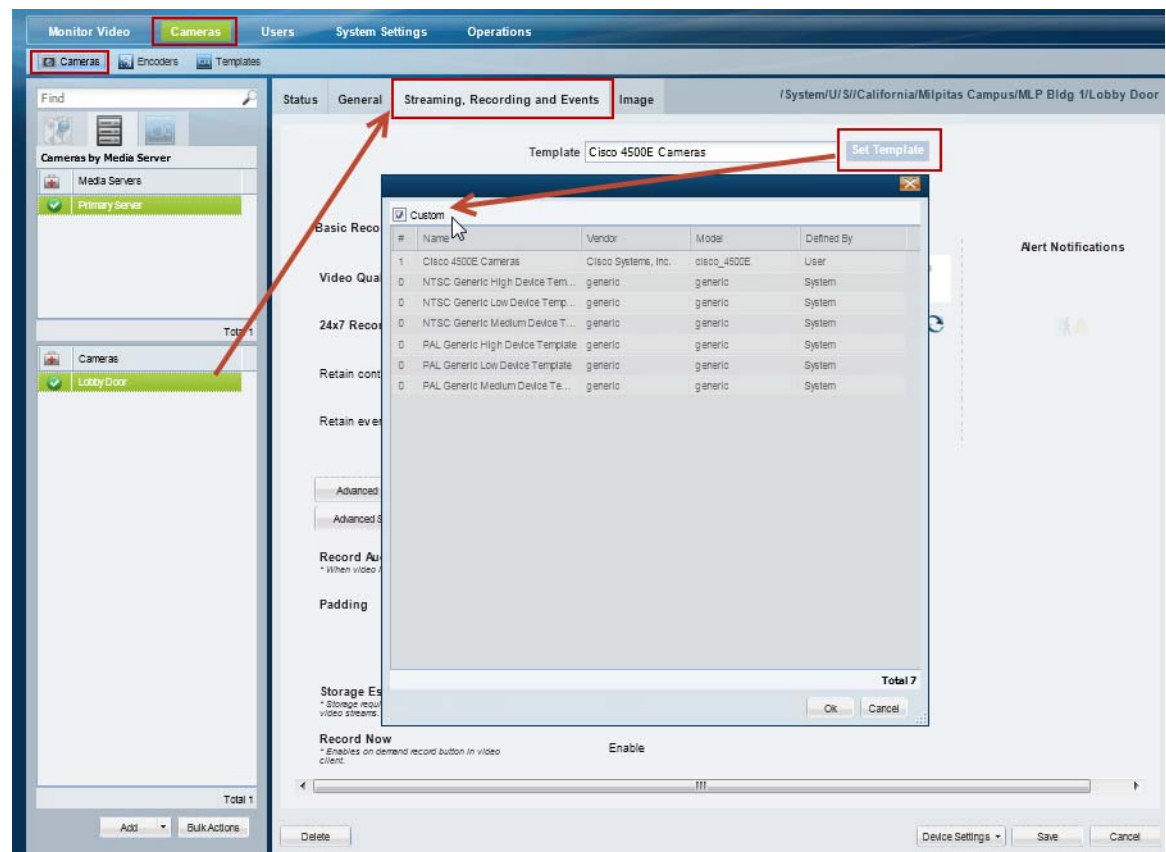
- Step 1** Select a camera name.
 - See the “[Editing the Camera Settings](#)” section on page 8-42. For example, click the  **Cameras By Location** tab, select a location and camera name.
 - You must belong to a User Group with permissions for *Cameras*. See the [Adding Users, User Groups, and Permissions](#), page 4-1 for more information.
- Step 2** Click the **Streaming, Recording and Event** tab.
- Step 3** Click **Set Template**.
- Step 4** Select the **Custom** box and click **OK** (Figure 10-3).

Figure 10-3 Custom Camera Template



- Step 5** Revise the camera settings as described in the “[Editing the Camera Settings](#)” section on page 8-42 and the “[Configuring Video Recording](#)” section on page 10-7.

Step 6 Click **Save**.

Configuring Video Recording

Video recording schedules and features are usually configured to occur automatically in a continuous loop or according to a schedule. Recordings can also be triggered when certain events (such as motion events) occur.

See the following topics for more information:

Table 10-1 **Configuring Video Topics**

Topic	Description
Configuring Continuous, Scheduled, and Motion Recordings, page 10-7	Describes how to configure video recordings to occur automatically. The recordings can occur continuously in a loop (for example, the past 30 minutes), or according to a schedule (such as Monday-Friday, 8 a.m. to 11 a.m.). In either case, recording can occur for the entire time, or only when triggered by a motion event.
Using Advanced Events to Trigger Actions, page 10-11	Describes how to trigger a recording when a variety of events occur. For example, when a contact is opened or closed, when a camera analytic trigger occurs, or when a soft trigger is received. You can define how long to record when the event occurs, and whether to record the primary or secondary stream.
Enabling Record Now, page 3-12	Describes how to enable the Record Now option when a user right-clicks a camera's live image.

Configuring Continuous, Scheduled, and Motion Recordings

Scheduled recordings allow you to define recording properties for different times of the day, days of the week, or for special events.

For example, a school might require that cameras associated with a template record video differently during *School* hours, *After school* hours, *School off* hours, and *Closed* hours. Additional exceptions to the regular recording schedule might be required for special events, such as a Homecoming event or the Christmas holiday.

The following procedure describes how to apply schedules to a camera template or custom configuration.

Procedure

-
- Step 1** Create the recording schedule.
- See the [“Defining Schedules” section on page 9-1](#) for instructions.
- Step 2** Edit or add a camera template:
- Click **Cameras**.
 - Select **Templates**.
 - Add or edit a template:
 - Click **Add** to create a new template.
 - To edit a template, select a location and then click a template name.

**Tip**

You can also create a custom template for an individual camera. See the [“Creating a Custom Template for a Single Camera”](#) section on page 10-5

Step 3 Click the **Streaming, Recording and Events** tab (Figure 10-4).

Figure 10-4 Recording Schedule

Step 4 Select a recording schedule (Figure 10-4).

- **Basic Recording: 24x7**—Records 24 hours a day, every day, based on the *continuous* and *event* recording properties.
 - or
 - Select a previously-defined schedule.
- A row of icons appears for each *Time Slot* in the schedule.





**Note**

Recording schedules appear only if schedules are configured. See the [“Defining Schedules” section on page 9-1](#) for instructions.

Recording schedules allow you to define recording properties for different times of the day, days of the week, or for special events. For example, a school might require different video surveillance actions during *School* hours, *After school* hours, *School off* hours, and *Closed* hours. Additional exceptions to the regular schedule might be required for special events, such as a Homecoming event or the Christmas holiday. A recording entry appears for each time slot included in the schedule.

Step 5 Click the recording icons for each *Time Slot*.

The options are:


-  **No Recording**—Disable recording for the stream.
-  **Record on Motion**—Record motion events. Motion recording is available only if the camera supports motion detection. See the [“Configuring Motion Detection” section on page 8-77](#) for instructions to define the areas of the image that trigger motion events.
-  **Continuous Recording**—Record video in a loop.
-  **Record on Motion and Continuous Recording**—Record continuously and mark any motion events. This option is available only if motion detection is supported by the camera.

**Tip**

The icons turn dark when selected.

Step 6 Define how long the recordings are retained:

Setting	Description
Retain continuous recordings	Enter the amount of time recorded video should be retained (saved) on the system.
Retain event recordings	Enter the amount of time a motion event should be retained (saved) on the system.
Padding	Enter the number of seconds of recording that should be included before and after the event occurs.

Step 7 Click the **Alert Notifications** icon  to enable or disable the alerts that are generated when a motion event occurs (stop or start).

**Tip**

Use the Cisco Video Surveillance Safety and Security Desktop (Cisco SASD) application to view alerts, comment and close alerts. See the [Cisco Video Surveillance Safety and Security Desktop User Guide](#) for more information.

**Tip**

Use the Advanced Events feature to trigger alerts only when motion stops, or when motion starts. You can also trigger other actions, such as recordings or moving the camera to a PTZ preset position. See the [“Using Advanced Events to Trigger Actions” section on page 10-11](#).

Step 8 Configure the optional recording options:

Table 10-2 Optional Recording Options

Recording Option	Description	More Information
Advanced Events	Define events that can trigger video recording for a specified amount of time. For example, recording can be triggered when an analytic event occurs, when a contact is closed or opened, or when a soft trigger occurs.	Using Advanced Events to Trigger Actions, page 10-11
Advanced Storage	Define the high-availability and Failover server options for streams, the Long Term Storage (LTS) server options, and other recording options. For example, recordings can be simultaneously recorded on a Redundant server, or saved to a Long Term Storage (LTS) server.	Configuring the Camera Template HA Options, page 12-12.
Record Audio	Define if audio should be recorded.	Streaming, Recording and Event Settings, page 8-49
Verify Recording Space	Select Enable to verify that enough storage space is available on the Media Server to complete the entire recording.	Streaming, Recording and Event Settings, page 8-49
Record Now	The Record Now feature allows operators to trigger recordings that are retained according to the <i>Retain event recordings</i> setting.	<ul style="list-style-type: none"> • Enabling Record Now, page 3-12 • Using Record Now, page 2-24

Step 9 Click **Create**, **Save** or **Save As**.

Step 10 Wait for the *Job* to complete.

- If you are modifying an existing template, the changes are applied to each camera associated with the template. A *Job Step* is created for each camera impacted by the template change.
- If a large number of cameras are affected, the Job can take a significant amount of time to complete.
- Click **View Status** in the Jobs window to view additional details for the Job Steps.
- See the [“Understanding Jobs and Job Status”](#) section on page 13-25 for more information.

Using *Advanced Events* to Trigger Actions

Use *Advanced Events* to trigger an immediate one-time action when a specified event occurs. For example, when motion starts or a contact is closed, the system can trigger an alert, aim the camera to a PTZ preset position, or trigger an action on an external system.

**Tip**

Multiple actions can be triggered for the same event.

Configure advanced events for camera templates to apply the rules to multiple cameras, or for a custom template to apply the trigger to a single camera.

This section includes the following topics:

- [Configuration Overview, page 10-12](#)
- [Configuration Summary, page 10-12](#)
- [Trigger and Action Descriptions, page 10-13](#)
- [Configuring Soft Triggers, page 10-15](#)

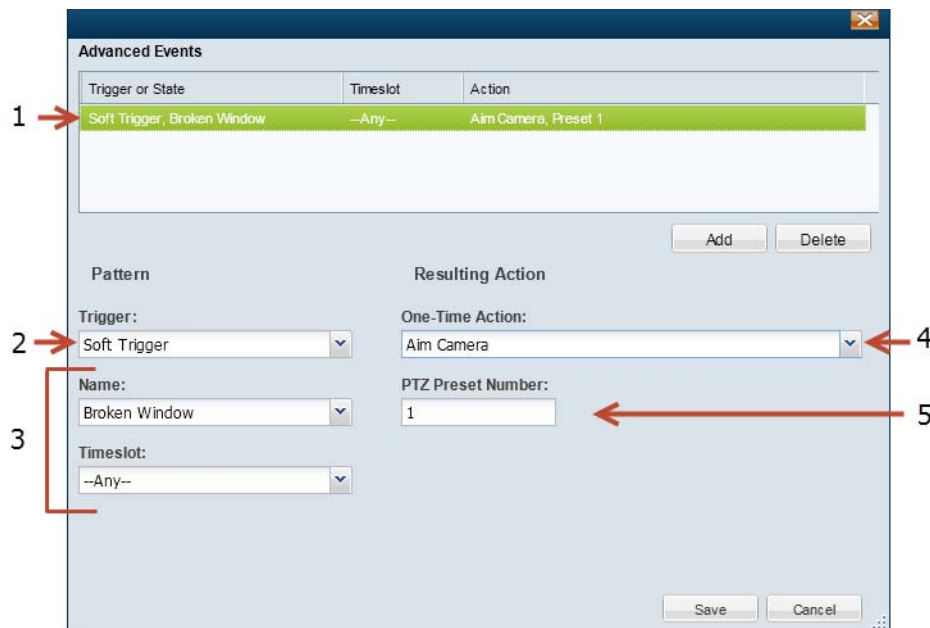
**Note**

-
- Advanced events are different from device health events. See the [“Device Status: Identifying Issues for a Specific Device”](#) section on page 13-8 for more information.
 - Some cameras do not support sending motion or contact-closure events to a Redundant server. See the [“Configuring the Redundant and Failover Options”](#) section on page 12-12 for more information.
-

Configuration Overview

Figure 10-5 describes the main elements of the Advanced Events configuration screen.

Figure 10-5 Configuring Advanced Events



1	The trigger and resulting action configured on the camera or template. Tip To define multiple actions for a single trigger, add the trigger multiple times but define a different action. See the Configuration Summary, page 10-12 for more information.
2	The event that triggers an action. See Trigger and Action Descriptions, page 10-13 for more information.
3	The options for the selected trigger.
4	The one-time action that occurs when an event is triggered. See Trigger and Action Descriptions, page 10-13 for more information.
5	The options for the selected action.

Configuration Summary

Procedure

To configure Advanced Events for a template or camera, do the following:

- Step 1** Log on to the Operations Manager.
- See the [“Logging In” section on page 1-18](#).

- You must belong to a User Group with permissions for *Templates* or *Cameras*. See the [Adding Users, User Groups, and Permissions, page 4-1](#) for more information.
- Step 2** Select a template or camera.
- Step 3** Click the **Streaming, Recording and Events** tab.
- Step 4** Click **Advanced Events**.
- Step 5** Click **Add**.
- Step 6** Select a **Trigger** and then select the additional options as described in the “[Trigger and Action Descriptions](#)” section on page 10-13.
- Step 7** Select a *Timeslot* when the event should trigger an action.
See the “[Defining Schedules](#)” section on page 9-1 to create timeslots.
- Step 8** Select a *Resulting Action* for the event, as described in the “[Trigger and Action Descriptions](#)” section on page 10-13.
- Step 9** Click **Add** to add additional entries.
To trigger multiple actions for an event, add an entry for the same trigger or state, and then select a different action.
- Step 10** Click **OK** to save the changes.

Trigger and Action Descriptions

Triggers—[Table 10-3](#) describes the events that immediately trigger a one-time action.

Actions—[Table 10-4](#) describes the resulting actions.

Table 10-3 **Advanced Event Triggers**

Event (Trigger)	Event Options
Analytic	<p>Analytic policies (such as trip wire or counting) must be configured on the camera using the camera UI. Analytics are supported for Cisco cameras only. See the camera documentation for more information.</p> <p>When the analytic event occurs, the associated action is triggered.</p> <ul style="list-style-type: none"> • <i>Timeslot</i>—the time span when the event should trigger an action. See the “Defining Schedules” section on page 9-1.
Contact Closed or Opened	<p>An electrical contact (such as a door sensor) that is monitored by a camera can trigger an action when the contact is opened or closed.</p> <ul style="list-style-type: none"> • <i>Timeslot</i>—the time span when the event should trigger an action. See the “Defining Schedules” section on page 9-1. <p>Note See the camera and contact device documentation for instructions to connect and configure the contact.</p> <p>Tip See the Contact Closure settings described in the “General Settings” section on page 8-45 for instructions to select a camera contact closure port.</p>

Table 10-3 **Advanced Event Triggers (continued)**

Event (Trigger)	Event Options
Motion Started or Stopped	<p>Motion events are triggered when motion occurs within a camera's include areas (according to the motion sensitivity settings). See the “Configuring Motion Detection” section on page 8-77 for more information.</p> <ul style="list-style-type: none"> <i>Timeslot</i>—the time span when the event should trigger an action. See the “Defining Schedules” section on page 9-1.
Soft Trigger	<p>Soft Triggers are used by external systems to trigger an action on a Cisco VSM camera.</p> <p>For example, when a door is opened, an external access control system can post a URL that causes a Cisco VSM camera to aim the camera (using a PTZ preset).</p> <p>See the “Configuring Soft Triggers” section on page 10-15 for more information.</p> <ul style="list-style-type: none"> <i>Name</i>—the name of the Soft Trigger. A URL with this name will be created for each camera associated with the template. <i>Timeslot</i>—the time span when the event should trigger an action. See the “Defining Schedules” section on page 9-1. <p>Note System integrators can add custom fields to alerts generated by a soft trigger event. See the <i>Cisco Video Surveillance API Programming Guide</i> available on the Cisco Developers Network (CDN) for more information.</p>

[Table 10-4](#) describes the action that can be associated with a trigger.

Table 10-4 **Resulting Actions**


Action	Description
Alert	<p>Generates an alert. Select the alert <i>Severity</i> and enter a <i>Message</i>. For example, if a contact is opened, an alert is triggered.</p> <p>Tip This option is not available for motion events. To trigger an alert for motion events, click the Alert Notifications  icon in the <i>Recording Options</i> section of the camera or template configuration. See the “Streaming, Recording and Event Settings” section on page 8-49.</p> <p>Note System integrators can add custom fields to alerts generated by a soft trigger event. See the <i>Cisco Video Surveillance API Programming Guide</i> available on the Cisco Developers Network (CDN) for more information.</p>
Aim Camera	<p>Select the pan, tilt and zoom (PTZ) preset that is triggered when the event occurs.</p> <ul style="list-style-type: none"> <i>PTZ Preset Number</i>—Enter the PTZ preset number. All cameras associated with the template will use this number, so the PTZ preset numbers for all cameras should be coordinated. For example, use PTZ preset #5 to zoom all Lobby Doors cameras to the door. See the “Configuring PTZ Presets” section on page 8-71. You can also view PTZ preset numbers by right clicking the camera video image. See the “Using Pan, Tilt, and Zoom (PTZ) Controls” section on page 2-32. <i>Aim Camera</i> actions are assigned a access priority of 50. This setting cannot be changed. See the “Defining the User Group PTZ Priority” section on page 8-69 for more information. The camera remains at the PTZ preset unless a PTZ tour is enabled or a user accesses the PTZ controls
Invoke URL	<p>Enter a valid <i>Get</i> or <i>Post</i> URL to trigger action on an external system. For example, if motion occurs at a certain time, a URL can be invoked to lock a door on an external access control system.</p>

Table 10-4 **Resulting Actions (continued)**

Action	Description
Record for Some Time	<p>The number of minutes that video should be recorded when the event occurs.</p> <ul style="list-style-type: none"> • Stop After (Min.)—The number of minutes to record. • Stream Number <ul style="list-style-type: none"> – Select 1 for the <i>primary</i> stream. – Select 2 for the <i>secondary</i> stream.
Push to Video Wall	<p>Displays live or recorded video (from the camera that triggered the event) on all instances of a Video Wall. For example, if the lobby receptionists are all viewing the same Video Wall <i>Lobby</i>, then the video would be replaced by video according to the following settings:</p> <ul style="list-style-type: none"> • Video Wall—The Video Wall where the video will be displayed. See the “Configuring Video Walls” section on page 3-10 for more information. • Live—Displays live video from the camera that triggered the event. • Recorded—Displays recorded video of the event. <ul style="list-style-type: none"> – Pre-Event—(recorded video only) the amount of seconds to include before the event began – Loop/Post-Event—(recorded video only) plays recorded video of the event in a loop. Enter the number of seconds of recorded video that should play after the event occurred. <p>Note The Video Wall will rollback to the default view when the rollback time elapses. If a default view and rollback time are not configured, then the event video pushed to the Video Wall will be displayed indefinitely.</p> <p>Note Select both Live and Recorded to display a 2-pane (1x2) Video Wall with both live and recorded video.</p> <p>Tip See the Cisco Video Surveillance Safety and Security Desktop User Guide for more information on viewing Video Walls, and changing the Video Wall view.</p>

Configuring Soft Triggers

Soft Triggers are used by external systems to trigger an action on a Cisco VSM camera.

For example, when a door is opened, an external access control system can post a URL that causes a Cisco VSM camera to aim the camera (using a PTZ preset).

Summary Steps

1. Create a Soft Trigger entry for a template (in Advanced Events).
For example, create a Soft Trigger entry “Door Open” with the resulting action “Aim Camera”. A unique URL with the same name is created for each camera associated with that template.
2. Copy the URL for the Soft Trigger entry from the camera’s configuration page.
3. (Optional) Configure an external system to add additional informational fields to soft trigger alerts. See the *Cisco Video Surveillance API Programming Guide* available on the Cisco Developers Network (CDN) for more information.
4. Add the URL to the external system’s configuration.
5. Whenever the URL is posted by the external system, the Cisco VSM camera will perform the action.

Detailed Procedure

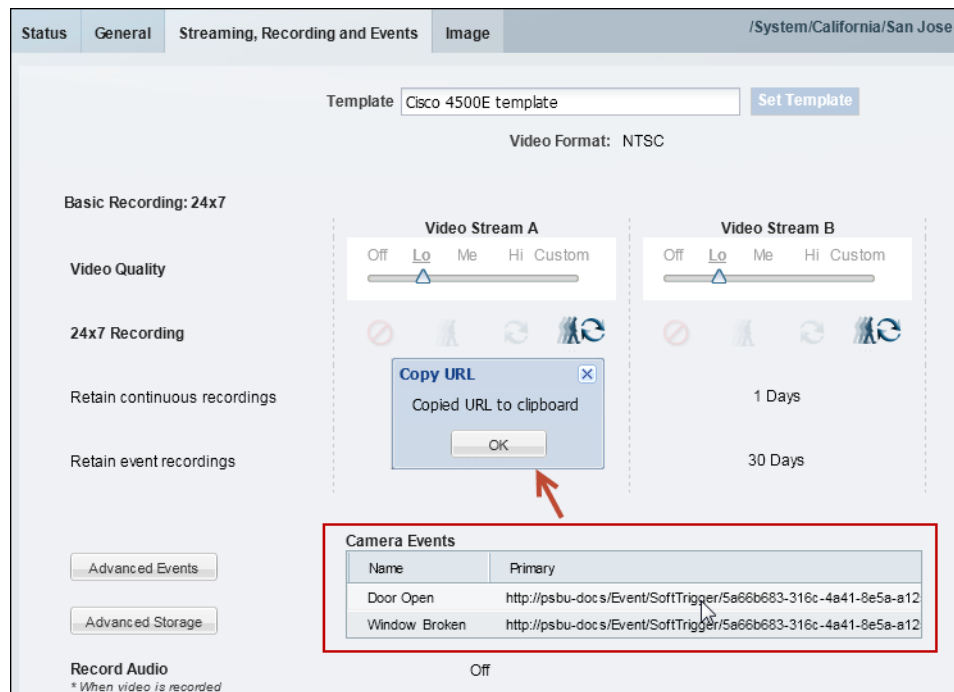
- Step 1** Create the Soft Trigger for a template:
- Log on to the Operations Manager.
 - Select a template.
 - Click the **Streaming, Recording and Events** tab.
 - Click **Advanced Events**.
 - Click **Add**.
 - Select **Soft Trigger** and enter a name for the trigger.
 - Select the *Timeslot* when the soft trigger will be enabled.
 - Select a *Resulting Action* for the event, as described in the “[Trigger and Action Descriptions](#)” section on page 10-13.
 - Click **Add**.



Tip To trigger multiple actions, add an additional soft trigger entry.

- Click **Save** to save the settings and close the Advanced Events window.
 - Click **Save** again to save the template changes.
- Step 2** Copy the camera URL for use on the external system:

Figure 10-6 Copying Soft Trigger URLs from the Camera Configuration Page



- Select **Cameras** and select the camera that to be triggered by the external system.
- Click the **Streaming, Recording and Events** tab.

- The Soft Trigger URLs are displayed in the Camera Events table ([Figure 10-6](#)).
- An entry appears for each Soft Trigger configured in [Step 1](#).

c. Click a URL to copy the Soft Trigger entry to the clipboard.

Step 3 (Optional) Configure an external system to add additional alert fields, see the *Cisco Video Surveillance API Programming Guide* for more information.

Step 4 Configure the external system use the URL to trigger the camera action.



Tip

- Soft Trigger alerts can be viewed and managed using a monitoring application such as the Cisco Video Surveillance Safety and Security Desktop (Cisco SASD) application. See the [Cisco Video Surveillance Safety and Security Desktop User Guide](#) for more information.
- System integrators can add custom fields to alerts generated by a soft trigger event. See the *Cisco Video Surveillance API Programming Guide* available on the Cisco Developers Network (CDN) for more information.

Configuring Multicast Video Streaming

Multicast allows cameras to send the same video stream to multiple destinations using a single transmission. A multicast transmission uses less network bandwidth than a unicast transmission to multiple destinations.

To configure multicast streams, you must do the following:

- Configure your network for multicast streaming.
- Create custom stream settings for the camera template.
- Configure the multicast IP address and port number on each camera that supports multicast.

Usage Notes

- Audio is unicast even if multicast video is enabled.
- Multicast is performed between the supported encoding device and the Media Servers that are listening. The Media Server does not multicast video to clients.

Procedure

Step 1 Configure your network to support multicast or ask your systems administrator for the multicast IP address(es) used by the cameras.

Step 2 Configure the template to support multicast streams.

- Select **Cameras > Templates**.
- Select a location and template name.
- Select the **Streaming, Recording and Events** tab.
- Click the **Custom** option for either Video Stream A or Video Stream B.
- Select **JPEG** from the Codec field.
- Select **UDP_Multicast** from the Transport field.
- Complete the remaining custom stream settings.
- Click **Save**.



Tip To configure a single camera for multicast, you can also create a custom template for that camera and enter the same settings. See the [“Creating a Custom Template for a Single Camera” section on page 10-5](#).

Step 3 Enter the Multicast IP address in the camera configuration page.

See the “Multicast” descriptions in the [“General Settings” section on page 8-45](#) for more information.

- Select **Cameras**.
- Select a location and camera name.
- From the General tab, enter the Multicast IP Address and port for the Primary and/or Secondary video streams.
 - See your systems administrator for the correct multicast address.
 - Primary and Secondary Multicast IP Address fields are enabled only if the corresponding template Stream A and Stream B Custom settings are configured for multicast.

- d. Click **Save**.

**Note**

The multicast settings can also be entered when adding a camera. See the [“Manually Adding a Single Camera” section on page 8-12](#).



CHAPTER 11

Adding Encoders and Analog Cameras

Encoders provide network connectivity for analog cameras, and digitize the analog video so it can be saved and transmitted by the Cisco VSM system. Refer to the following topics to add and configure encoders and analog cameras:

Contents

- [Overview, page 11-2](#)
- [Pre-Provisioning Encoders and Analog Cameras, page 11-3](#)
- [Requirements, page 11-4](#)
- [Adding External Encoders and Analog Cameras, page 11-5](#)
- [Bulk Actions: Revising Multiple Encoders, page 11-11](#)



Tip

See also the [“Upgrading Cisco Camera and Encoder Firmware”](#) section on page 15-3.



Note

Encoders are not required for IP (networked) cameras.

Overview

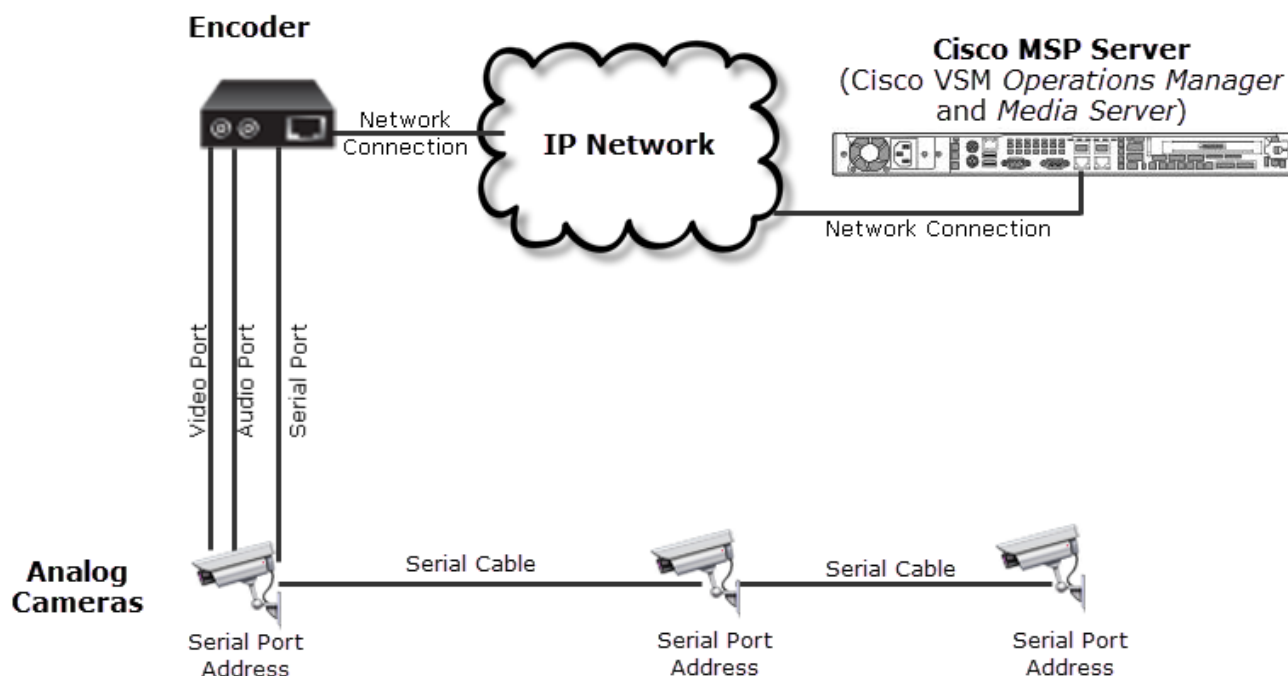
Cisco VSM 7 supports external encoders that are added to the same network as the server, and configured with an IP address, username and password. Analog cameras are then attached to the encoder with a video cable, and multiple cameras can be connected to a single encoder (Figure 11-1). In addition, serial port connections can be used between the camera and encoder to provide PTZ and other control features.

**Tip**

See the encoder documentation for more information on the number of supported video ports, physical connections, supported features and configuration.

Figure 11-1 shows an external encoder configuration.

Figure 11-1 External Encoder Configuration

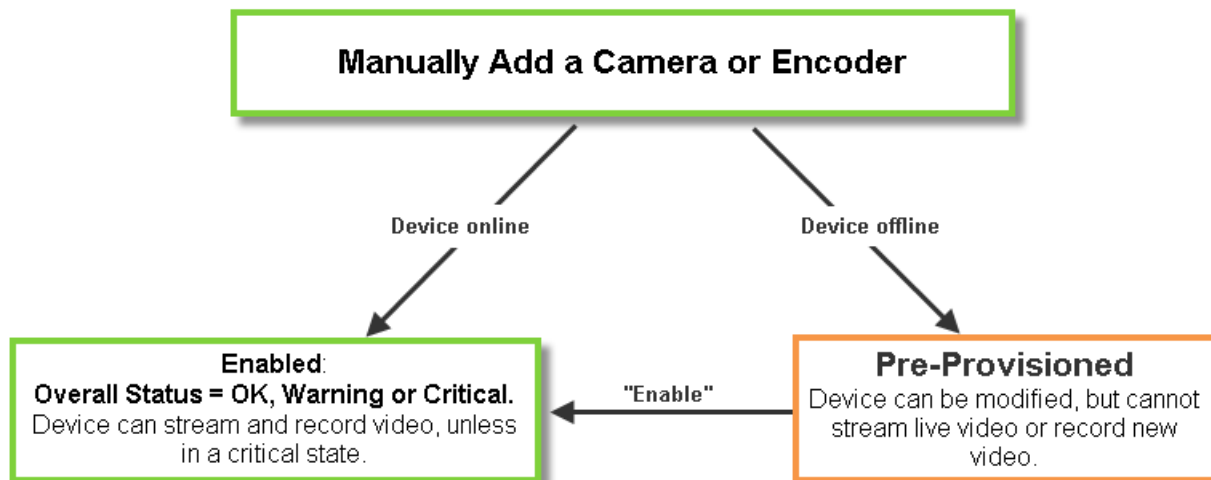


To manually add a single encoder or analog camera, open the encoder configuration page and click **Add**. Enter the settings as described in the “[Adding External Encoders and Analog Cameras](#)” section on page 5.

If the device is not available on the network, it can be added in *pre-provisioned* state (Figure 11-2). See the “[Pre-Provisioning Encoders and Analog Cameras](#)” section on page 11-3 for more information.

You can also import cameras and encoders using a *comma separated value* (CSV) file. See the “[Importing or Updating Cameras or Encoders Using a CSV File](#)” section on page 8-17.

Figure 11-2 Manually Adding a Camera or Encoder



Pre-Provisioning Encoders and Analog Cameras

Pre-Provisioning Encoders

Encoders can be added to the system before they are available on the network. If you add a encoder that cannot be reached, a message will appear asking if you want to pre-provision the device. If yes, then the device is added in *Pre-provisioned* state. You can modify the settings, but the encoder will not be available for video processing.

Once the device is available on the network, you must enable the device by selecting **Device Settings > Enable** (in the device configuration page). The device status will change to *Enabled:OK* unless other issues are present.

- A *Pre-provisioned* encoder may, or may not have been connected to the network.
- Settings can be changed, but the only device action allowed is **Device Settings > Enable**. The device can be deleted.
- You can enable an IP camera or encoder that is in Pre-provisioned state only after the device is connected to the network and the associated Media Server is enabled. The Operations Manager does not automatically enable them. An attempt to enable an IP camera or an encoder before connecting them to the network only changes its state from *Pre-provisioned* to *Enabled: Critical*.

Pre-Provisioning Analog Cameras

Analog cameras can also be added in Pre-provisioned state. Settings can be changed, but the only device action allowed is **Device Settings > Enable**. The device can be deleted.

- Analog cameras that are added to a *Pre-provisioned* encoder are also *Pre-provisioned*.
- You can enable an analog camera that is in Pre-provisioned state only after its associated encoder is enabled. The Operations Manager does not automatically enable it.

Requirements

Analog cameras attached to an encoder require the following:

Table 11-1 Analog Camera Requirements

Requirements	Requirement Complete? (✓)
<p>The wiring between the cameras and the encoder must adhere to the protocol requirements, including:</p> <ul style="list-style-type: none"> • The correct number of wires. • The correct polarity. • The cable length does not exceed the maximum allowable length. • The maximum number of devices in a daisy chain is not exceeded. <p>See the device documentation for more information.</p>	<input type="checkbox"/>
<p>The encoder serial ports must be correctly configured:</p> <ul style="list-style-type: none"> • All devices on the serial line must be configured with the same settings, baud rate, data/stop bits, parity, etc. • All devices must support the same protocol. • All cameras must support the same protocol as the encoder serial port. <p>See the device documentation for more information.</p>	<input type="checkbox"/>
<p>The camera serial port must be correctly configured:</p> <ul style="list-style-type: none"> • All cameras must be properly terminated. • All cameras must have unique serial addresses. <p>See the device documentation for more information.</p>	<input type="checkbox"/>
<p>To add and configure encoders and analog cameras in Cisco VSM, You must belong to a User Group with permissions for <i>Servers & Encoders</i>. See the Adding Users, User Groups, and Permissions, page 4-1 for more information.</p>	<input type="checkbox"/>

Adding External Encoders and Analog Cameras

To add external encoders to the Cisco VSM configuration, complete the following procedure.



Note

You can also import multiple cameras or encoders using a *comma separated value* (CSV) file. See the [“Importing or Updating Cameras or Encoders Using a CSV File”](#) section on page 8-17.

Procedure


- Step 1** Install and configure the encoder so it can be accessed on the network:
- Physically install the encoder so it can access the same network as Cisco VSM.
 - Configure the network settings on the device.
 - Ping the device to verify it can be accessed on the network.
-  **Tip** Refer to the encoder documentation for instructions.
- Step 2** Log on to the Operations Manager.
- See the [“Logging In”](#) section on page 1-18.
 - You must belong to a User Group with permissions for *Servers & Encoders*. See the [Adding Users, User Groups, and Permissions](#), page 4-1 for more information.
- Step 3** Click the **Cameras** tab.
- Step 4** Click the **Encoders** icon.
- Step 5** Click **Add**.
- Step 6** Enter the basic encoder connectivity settings ([Table 11-2](#)).

Table 11-2 General Encoder Settings

Setting	Description
Name	<p>Enter a descriptive name for the encoder.</p> <p>Enter a name that helps identify the device location or primary use. Use any combination of characters and spaces.</p>
IP Address	<p>Enter the IP address configured on the device.</p> <ul style="list-style-type: none"> See the encoder documentation for instructions to configure the device settings. See the “Changing the Camera or Encoder Access Settings (Address and Credentials)” section on page 8-61 for more information. All edge devices (such as cameras and encoders) must added to a server using a local (non-NAT) addresses. Internal encoders are automatically configured and do not need to be added to the system.

Table 11-2 **General Encoder Settings**

Setting	Description
Install Location	(Required) Select a location where the device is physically installed. See the “Understanding a Camera’s Installed Location Vs. the Pointed Location” section on page 5-9 for more information.
Model	The encoder make and model.
Server	The server where the encoder is physically installed. Note The server processes and stores video streams from the analog cameras connected to the encoder.
Username/Password	The credentials used to access the device over the network. <ul style="list-style-type: none"> • See the encoder documentation for instructions to configure the device network settings. • See the “Changing the Camera or Encoder Access Settings (Address and Credentials)” section on page 8-61 for more information.

Step 7 Click **Add**.

- If the validation is successful, continue to [Step 8](#).
- If the encoder cannot be found on the network, an error message appears asking if you want to pre-provision the server.
 - Click **Yes** to pre-provision the encoder. The encoder is added to Cisco VSM but is not available for video processing. The encoder is automatically enabled when it comes online. See the [“Pre-Provisioning Encoders and Analog Cameras”](#) section on page 11-3.
 - Click **No** to cancel the operation. Verify the encoder hostname and login credentials and return to [Step 5](#) to try again.
 - Once the device is available on the network, you must enable the device by selecting **Repair Config** from the **Device Settings** menu (in the device configuration page). The device status will change to *Enabled:OK* unless other issues are present.

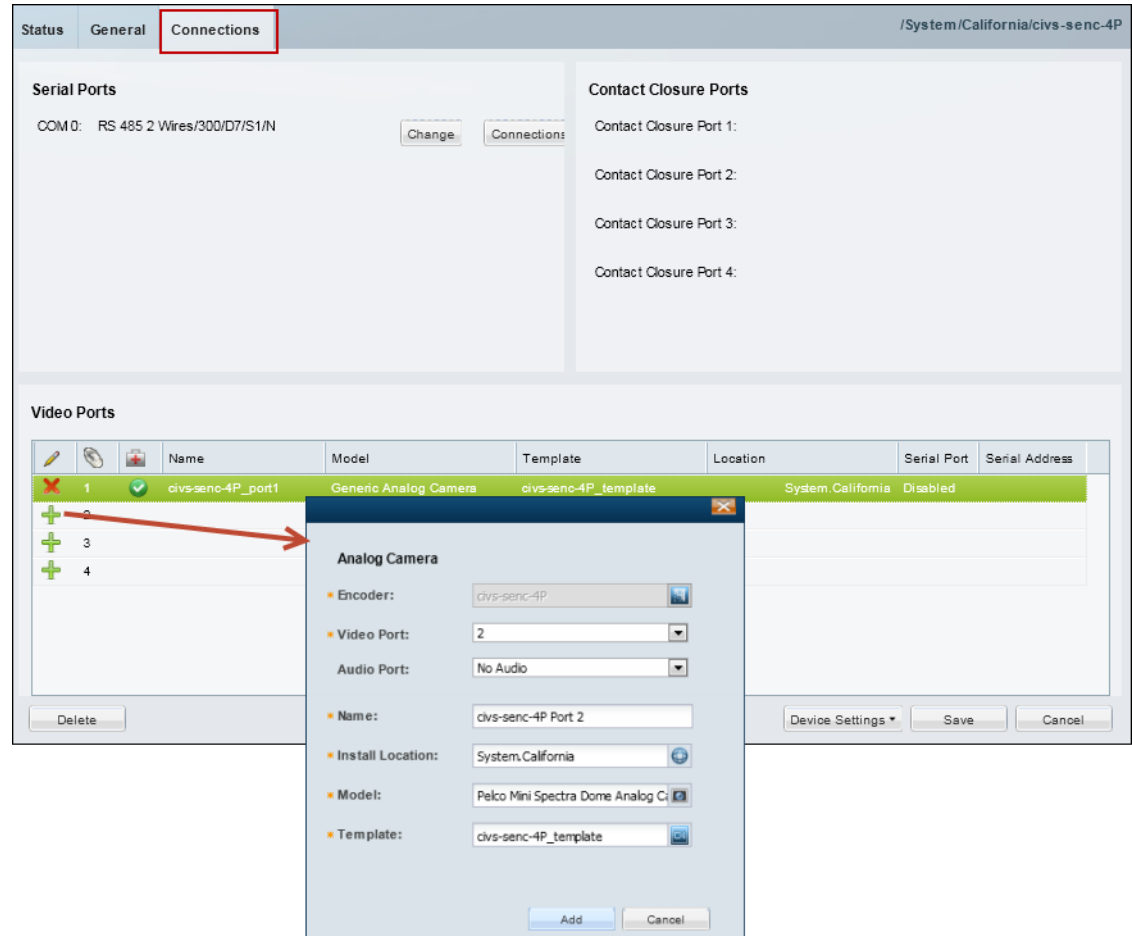
Step 8 (Optional) Add the analog camera(s) attached to the encoder ([Figure 11-3](#)).



Tip

You can also add analog cameras from the camera configuration page. See the “[Manually Adding Cameras](#)” section on [page 8-8](#) for more information.

Figure 11-3 Adding Analog Cameras to an Encoder




- Click the **Connections** tab.
- Click the **Add**  icon.
- Enter the analog camera settings ([Table 11-3](#)).

Table 11-3 Analog Camera Settings

Setting	Description
Encoder	(Read-Only) The encoder that is physically attached to the camera.
Video Port	The physical encoder video port where the camera video cable is attached.
Tip Only the unused ports are displayed.	

Table 11-3 **Analog Camera Settings (continued)**

Setting	Description
Audio Port	(Optional) The physical encoder audio port where the camera audio cable is attached. Tip Only the unused ports are displayed.
Name	The camera name that will appear in Cisco VSM.
Install Location	The physical location of the camera.
Model	The camera model.
Template	The template that defines the camera settings. <ul style="list-style-type: none"> You must choose an existing template when the camera is added to Cisco VSM. After the camera is created, you can create a custom configuration or select a different template. See the “Accessing the Camera Settings” section on page 8-42. Templates define attributes such as video quality and schedules. Only templates that support the camera are displayed. See the “Adding and Editing Camera Templates” section on page 10-1 for more information.

Step 9 Click **Add**.

If the camera is pre-provisioned, complete the configuration. Once the device is available on the network you can select **Enable** from the **Device Settings** menu in the camera configuration page.

Step 10 (Optional) Click **Change** (in the Serial Ports section) to revise the encoder serial port settings, if necessary.

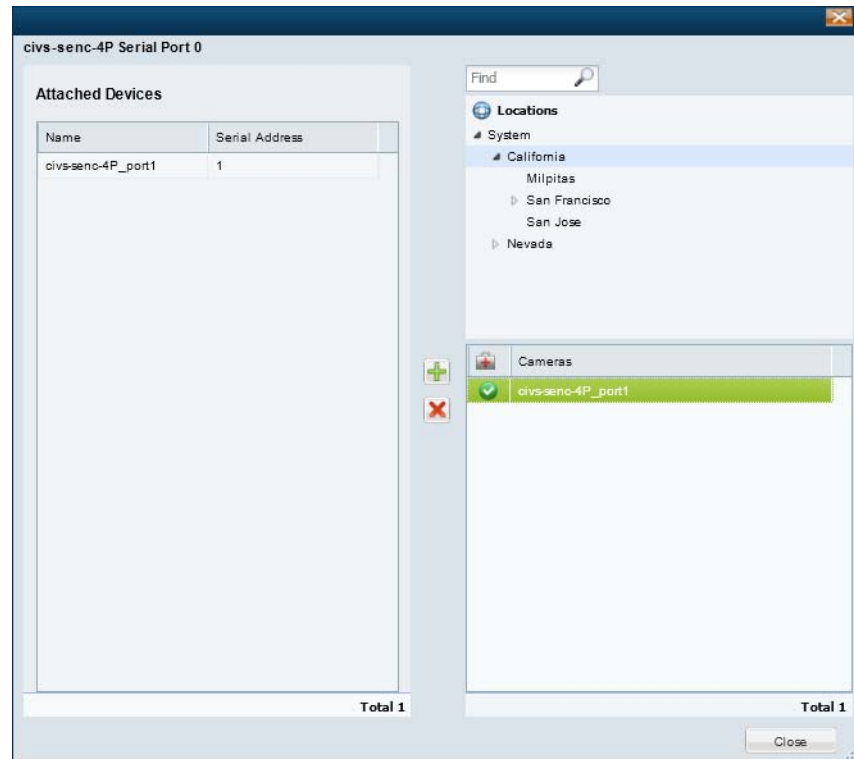
For example, protocol, baud rate, data bits, stop bit and parity.

- The serial port connection is used for control features such as PTZ movements and contact closure events. Both the camera and encoder must support serial ports.
- See the encoder documentation for instructions to connect multiple analog camera serial connections and define the serial port addresses for those cameras.
- See the [“Requirements” section on page 11-4](#) for information on the serial port setting requirements between encoders and attached cameras.

Step 11 (Optional) Click the **Connections** button (in the Serial Ports section) to define the analog camera serial port connections (Figure 11-4).

The following settings are used when a serial cable is attached from an analog cameras to an encoder. The serial port connection enables the pan-zoom-tilt (PTZ) controls and/or photographic controls (brightness, contrast, etc.) on an analog camera. See the “General Settings” section on page 8-45 for more information.

Figure 11-4 Serial Port Connections




- a. Expand the location tree and select the camera's *Install Location* (see Table 11-3).
- b. Select a camera name from the list.
- c. Click the add  icon.
- d. Enter the serial port connection settings (Table 11-4) and click **Add**.

Table 11-4 Analog Camera Serial Port Settings

Setting	Description
Encoder	The encoder for the analog camera.

Table 11-4 **Analog Camera Serial Port Settings (continued)**

Setting	Description
Serial Port	The encoder serial port where the first analog camera is attached to the encoder. See the encoder documentation for information to determine the port number.
Serial Port Address	The unique ID of the serial device (analog camera). Note Every device on a serial bus must have a unique ID (also called a “Serial Port Address”). This uniqueID/address is configured on most analog cameras using physical switches. See the camera documentation for more information.

Step 12 Click **Save**.

Step 13 Verify that the camera appears under Attached Devices.

Step 14 Click **Close**.

Step 15 Click **Save** to save the encoder settings.

Step 16 (Optional) Enter additional camera configurations, if necessary.

See the [“Editing the Camera Settings” section on page 8-42](#).

Step 17 (Optional) If the camera was *Pre-Provisioned*, complete the configuration and select **Device Settings > Enable**.

- The **Enable** option is only enabled if the camera configuration is complete and the device is available on the network.
- To enable multiple devices, see the [“Bulk Actions: Revising Multiple Encoders” section on page 11-11](#).

Bulk Actions: Revising Multiple Encoders

Bulk Actions allows you to change the configuration or take actions for multiple encoders. For example, you can delete the devices, repair the configurations, change the location or change the password used to access the device.

To begin, filter the devices by attributes such as name, tags, model, server, location, status, or issue. You can then apply changes to the resulting devices.

Requirements

- Users must belong to a User Group with permissions to manage *Servers and Encoders*.
- Only super-admin users can apply the **Change Password** option using Bulk Actions. Non-super-users must use the device configuration page to change one device at a time.
- See the “[Adding Users, User Groups, and Permissions](#)” section on page 4-1 for more information.

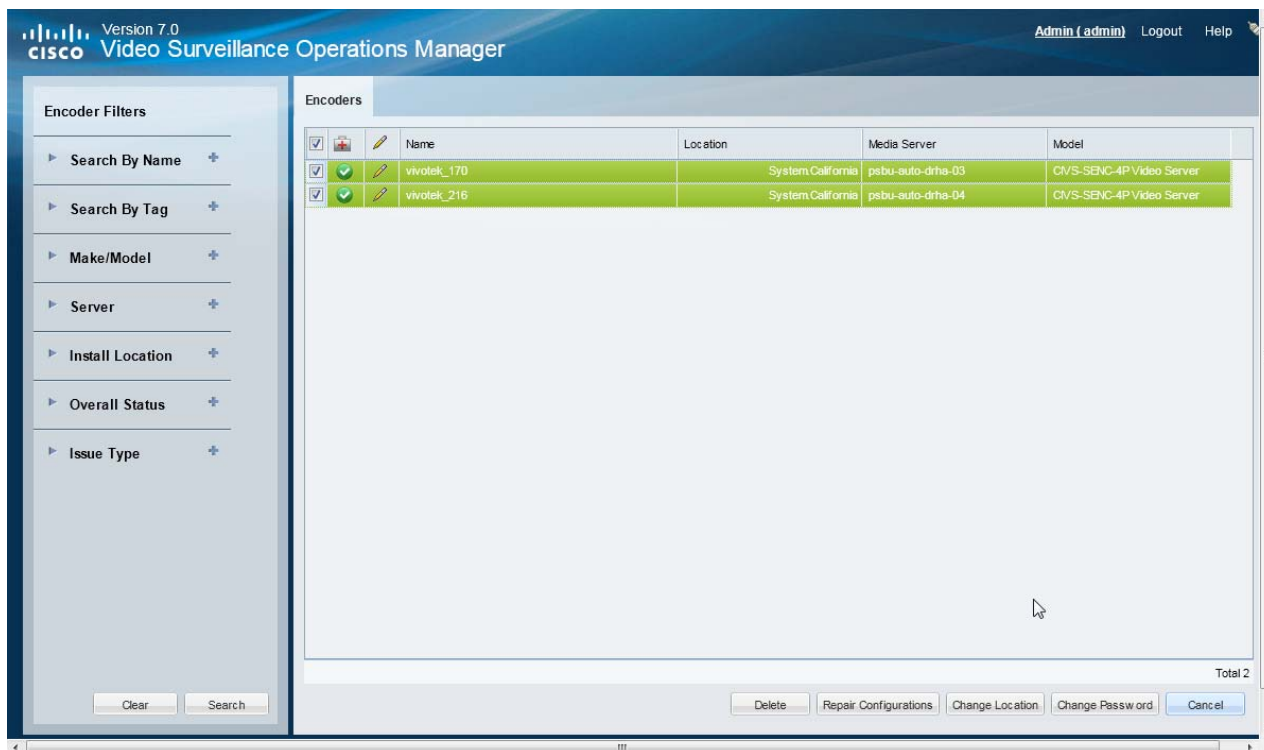
Related Topics

- [Bulk Actions: Revising Multiple Cameras](#), page 8-85
- [Bulk Actions: Revising Multiple Servers](#), page 6-19

Procedure

- Step 1** Select **Cameras > Encoders**.
- Step 2** Click **Bulk Actions** (under the device list) to open the Bulk Actions window ([Figure 11-5](#)).

Figure 11-5 Bulk Actions Window






Step 3 Click the  icon next to each field to select the filter criteria (Table 11-5).

Table 11-5 Bulk Action Filters

Filter	Description
Search by Name	Enter the full or partial device name. For example, enter “Door” or “Do” to include all device names that include “Door”.
Search by Tag	Enter the full or partial tag string and press <code>Enter</code> .
Make/Model	Select the device model(s). For example, “Cisco HD IP Camera 4300E Series”.
Media Server	Select the server that has the Media Server service activated. This is the server that will manage live and recorded video for cameras attached to the encoder.
Install Location	Select the location where the devices are installed.
Overall Status	Select the administrative states for the devices. For example: <ul style="list-style-type: none"> • Enabled (OK, Warning or Critical)—The device is enabled, although it may include a <i>Warning</i> or <i>Critical</i> event. • Disabled—The device is disabled and unavailable for use. The configuration can be modified, and any existing recordings can be viewed, but cameras cannot stream or record new video. • Pre-provisioned—The device is waiting to be added to the network and is not available for use. A pre-provisioned camera can be modified, but the camera cannot stream or record video until you choose Enable from the Device Settings menu. • Soft Deleted—The device is removed from Cisco VSM but the recordings associated with that device are still available for viewing (until removed due to grooming policies). <p>Tip See the “Device Status: Identifying Issues for a Specific Device” section on page 13-8 for more information.</p>
Issue Type	Select the issues that apply to the device. For example: <ul style="list-style-type: none"> • Configuration Mismatch—the configuration on the Media Server is different than the configuration in the Operations Manager. • Capability Mismatch—the capabilities on the device do not match the Cisco VSM configuration. • Identity Collision—the camera has an IP address or hostname that is the same as another device.
Encoders Filters	Click the  icon to select one or more encoders and limit the search to that encoder and associated cameras.

Step 4 Click **Search**.

Step 5 (Optional) Click the  icon to view and edit the device status and configuration settings.

Step 6 Select the devices that will be affected by the action.

- Choose the *Select All* check box to select ALL cameras matched by the filters, including the devices not shown in the grid.
- Use CTRL-CLICK and SHIFT-CLICK or to select multiple items.

Step 7 Click an *Action* button.

For example, Delete, Change Location, etc.

- Step 8** Follow the onscreen instructions to enter or select additional input, if necessary.
For example, *Change Location* requires that you select the new location.
- Step 9** Refer to the Jobs page to view the action status.
See the [“Understanding Jobs and Job Status” section on page 13-25](#).
-

Using “Split Model” Multi-Port Multi-IP Encoders

In “split model encoders”, each video input is a separate network encoder, and the functionality on input 1 is different from the other inputs. Cisco VSM 7.0 handles these different port functions by using a model name on input 1 that is different than the name on inputs 2+. In addition, when certain model encoders are installed in a supported chassis, the available ports on the chassis determines what each blade supports.

Summary

1. Axis 243Q and Q7406 are Multi-Port Multi-IP encoder blades. These blades are installed into the supported chassis: Axis 291 1U and Axis Q7900 4U.
2. Each port on these encoder blades is configured with its own IP. And each port has its own set of supported features (such as serial PTZ and/or contact closure).
3. When the encoder blade is installed into a chassis, the available ports on the chassis determines what each blade supports.
4. To support this model, Cisco introduced the concept of two kinds of models for each Multi-Port Multi-IP encoder:
 - axis243q_1 and axis243q_2_n
 - axisq7406_1 and axisq7406_2_n
 - axisq7404_1 and axisq7404_2_n
5. The _1 model represents different set of features as compared to _2_n model. For example:
 - axis243q_1 and axis243q_2_n, axisq7406_1 and axisq7406_2_n: only the _1 model supports Serial PTZ.
 - axisq7404_1 and axisq7404_2_n: only _1 model supports audio.

Constraints

The constraints are as follows:

- If the chassis being used is Axis 291 1U Chassis and serial PTZ is working, then irrespective of Axis 243Q or Axis Q7406 being the blade, it has to be the serial port on Channel 1 (The physical port 1 on the blade encoder). For example, when importing this device it has to be _1 device model.
- If the chassis is Axis Q7900 4U and the encoder blade is Axis 243Q has PTZ working already: it still has to be Channel (Port on the encoder blade) 1 (Physical Port 1 on the blade encoder).
- If the blade is Q7406 and PTZ is already working, then it may be any of the ports on the blade (because the chassis exposes all the serial ports on this blade through the connectors on the back side). But Cisco VSM release 7.0 supports PTZ through the first port on the blade only. So the device representing the first port on this encoder has to imported using 1 device model and the rest of the ports as the 2_n device model.



CHAPTER 12

High Availability

High Availability (HA) in Cisco VSM entails the use of one or more *Failover*, *Redundant*, or *Long Term Storage* Media Servers. These HA servers provide HA support, including hot standby, redundant stream storage and playback, and long term storage of video recordings.



Note

Each Media Server is assigned the default *Primary* HA role. can be assigned a single role. You can change the role as described in the [“Define the Media Server HA Role and Associated Servers”](#) section on page 12-9.

Review the following information to understand the roles and functions of the different Media Servers, and for instructions to install and configure the HA Media Servers.

Contents

- [Overview, page 12-2](#)
 - [Requirements, page 12-2](#)
 - [Summary Steps, page 12-3](#)
 - [Understanding Redundant, Failover, and Long Term Storage Servers, page 12-4](#)
 - [Understanding Failover, page 12-7](#)
- [Define the Media Server HA Role and Associated Servers, page 12-9](#)
- [Configuring the Camera Template HA Options, page 12-12](#)
 - [Configuring the Redundant and Failover Options, page 12-12](#)
 - [Archiving Recordings to a Long Term Storage Server, page 12-16](#)
 - [Defining the Recording Options, page 12-20](#)
- [Viewing the Server HA Status, page 12-22](#)

Overview

Review the following information to understand the HA server types, and how they support the HA features for the Primary server.

- [Requirements, page 12-2](#)
- [Summary Steps, page 12-3](#)
- [Understanding Redundant, Failover, and Long Term Storage Servers, page 12-4](#)
- [Understanding Failover, page 12-7](#)

Requirements

Before you begin, verify that the following requirements are met.

Table 12-1 **Requirements**

Requirements	Requirement Complete? (✓)
<p>You must belong to a User Group with permissions for <i>Servers & Encoders</i>.</p> <p>See the “Adding Users, User Groups, and Permissions” section on page 4-1 for more information.</p>	<input type="checkbox"/>
<p>At least two Media Servers must be enabled:</p> <ul style="list-style-type: none"> • 1 Primary Media Server • 1 HA Media Server <p>Install additional Media Servers to enable additional HA features.</p> <p>Note All Media Servers are assigned the Primary HA role by default.</p> <p>Note The co-located Media Server is automatically added to the Operations Manager and activated. The default co-located server name is “VsomServer”.</p> <p>See the “Understanding Redundant, Failover, and Long Term Storage Servers” section on page 12-4.</p>	<input type="checkbox"/>
<p>Co-located Servers—The Operations Manager and a single Media Server are enabled on the same server. The following rules apply:</p> <ul style="list-style-type: none"> • 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). 	<input type="checkbox"/>
<p>The time on all servers must be in sync, which requires NTP configuration.</p> <p>We recommend using the same network time protocol (NTP) server on all Media Servers to ensure the time settings are accurate and identical.</p> <p>See the “NTP Information” section on page 6-8 for more information.</p>	<input type="checkbox"/>

Summary Steps

To configure HA Media Servers, add the servers to Cisco VSM, enable the Media Server services, and define the Media Server High Availability options for each Media Server. Next, configure the camera templates with the HA *Advanced Storage* options.

	Task	Related Documentation
Step 1	Install the physical or virtual servers and enable the Media Server service.	<ul style="list-style-type: none"> • Cisco Physical Security UCS Platform Series User Guide • Cisco Multiservices Platform for Physical Security User Guide • Cisco Video Surveillance Management Console Administration Guide
Step 1	Use the Operations Manager to add the server and activate the Media Server. Tip A co-located Media Server is automatically added to the Operations Manager and activated. The default co-located server name is “VsomServer”.	<ul style="list-style-type: none"> • “Configuring Servers” section on page 6-1 • “Configuring Media Server Services” section on page 7-1
Step 1	Define a HA <i>Role</i> for each Media Server. Tip All Media Servers are assigned the Primary HA role by default.	<ul style="list-style-type: none"> • Understanding Redundant, Failover, and Long Term Storage Servers, page 12-4 • Define the Media Server HA Role and Associated Servers, page 12-9
Step 2	Associate the Primary and Redundant servers with other HA servers.	<ul style="list-style-type: none"> • Define the Media Server HA Role and Associated Servers, page 12-9
Step 3	Configure the HA Advanced Storage options on the camera template.	<ul style="list-style-type: none"> • Configuring the Camera Template HA Options, page 12-12

Understanding Redundant, Failover, and Long Term Storage Servers

Table 12-2 describes the different HA Media Server types.



Tip

The *Server Type* is selected using the Media Server **Advanced**  icon (**System Settings > Server**) as shown in [Figure 12-2 on page 12-10](#).

^w
Table 12-2 **HA Server Types**

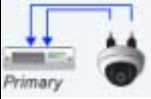


Media Server Type	Example	Description
Primary server	<p>Both streams are sent to the Primary server only</p> 	<p>The <i>Primary</i> Media Server processes the camera video feeds, stores and plays back recorded video, among other tasks.</p> <p>Usage Notes</p> <ul style="list-style-type: none"> All Media Servers are assigned the Primary HA role by default. A 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). A co-located Media Server is automatically added to the Operations Manager and activated. The default co-located server name is “VsomServer”.
Redundant server	<p>Stream A to Primary, Stream B to Redundant:</p>  <p>All Streams to Both Servers:</p> 	<p>A Redundant Media Server provides additional computing power for the cameras associated with a Primary server.</p> <ul style="list-style-type: none"> Unicast—The camera’s video streams are sent to different servers. For example, stream A is sent to the Primary server, and stream B to the Redundant server. If the Primary server goes down, the video from Stream B is still saved to the Redundant server. Multicast—Both camera video streams are simultaneously sent to both servers. <p>Note See the “Configuring Multicast Video Streaming” section on page 10-18 for more information.</p> <p>Usage Notes</p> <ul style="list-style-type: none"> A <i>Redundant</i> Media Server can support multiple Primary servers. You must ensure that the Redundant server contains the disk and processing capacity to support all cameras that send video streams to the server. The Record Now feature is not available on redundant servers. The Record Now feature is available on the Primary server, or on the failover server if the Primary is down.

Table 12-2 HA Server Types (continued)


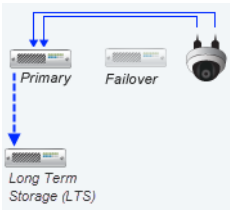
Media Server Type	Example	Description
Failover server	 <p>The diagram illustrates the failover process. In the top section, a 'Primary' server and a 'Failover' server are both connected to a camera. In the bottom section, titled 'Failover Operation', the 'Primary' server is shown with a red 'X' and smoke, indicating a failure. The 'Failover' server is then shown with a blue arrow pointing to the camera, indicating it has taken over the connection.</p>	<p>A Failover Media Server is a hot standby server that assumes system control if the Primary server fails or goes offline.</p> <p>Usage Notes</p> <ul style="list-style-type: none"> • The Failover server does not provide hot-standby functionality for the Redundant server. • See the “Understanding Failover” section on page 12-7 for more information.

Table 12-2 HA Server Types (continued)

Media Server Type	Example	Description
Long Term Storage (LTS) server		<p>A Long Term Storage (LTS) server is used to back up continuous and motion event recordings to a separate server.</p> <ul style="list-style-type: none"> Both stream A and stream B can be backed up. Backups are performed on an automatic schedule (for example, once a week at midnight). <p>Usage Notes</p> <p>Note See the “Archiving Recordings to a Long Term Storage Server” section on page 12-16 for more information.</p> <ul style="list-style-type: none"> An LTS server can be associated with both the Primary and Redundant servers. If video stream B is sent only to the Redundant server, that stream can also be archived to the LTS server. A LTS server can support multiple Primary and Redundant servers. You must ensure that the server contains the disk and processing capacity to support all associated servers and cameras. If the Primary server fails over, the Failover server continues to archive recordings to the LTS server. Click Backup Now from the Primary or Redundant server Advanced tab to immediately back up the recordings to the LTS server. Recordings remain in the Primary and Redundant servers even if they are archived to an LTS server. The recordings are removed from the Primary and Redundant servers based on the <i>Retain</i> settings available in the camera or template configuration page (<i>Retain continuous recordings</i> and <i>Retain event recordings</i>). See the “Streaming, Recording and Event Settings” section on page 8-49. Recordings are retained on the LTS server according to the settings described in the “Archiving Recordings to a Long Term Storage Server” section on page 12-16 (if the disk capacity of the LTS server is exceeded, the oldest recording is deleted to provide room for the newest recording). To access the LTS recordings, right-click the camera’s video and choose Select Streams from the menu. See the “Using the Pop-Up Menu” section on page 2-25. Only a LTS server can be associated with the co-located Primary Media Server (failover or redundant Media Servers cannot be associated with the co-located Primary Media Server).

Understanding Failover

When a Failover Media Server is associated with a Primary server, the Failover polls the Primary every two minutes to verify connectivity. If the failover does not receive a response after three successive tries, the Primary is assumed to be down or offline and the Failover assumes the Primary role.



Note

- A few minutes of recording may be lost between the loss of the Primary Media Server and the Failover assuming control.
- A Failover Media Server can only stand in for one Primary server at a time (if a Failover server is already acting as the Primary for a Media Server that is down, the Failover cannot assume control for a second Primary Media Server).
- When the Primary Media Server is down and the Failover has taken over the role of the Primary server, and a DHCP based Medianet discovered camera has a change of IP address, the Cisco VSM Operations Manager will not reconfigure the camera to the new IP address until the Primary Media Server comes back up. This is because Cisco VSM Operations Manager does not allow any configuration changes on the cameras when the Primary server is down.

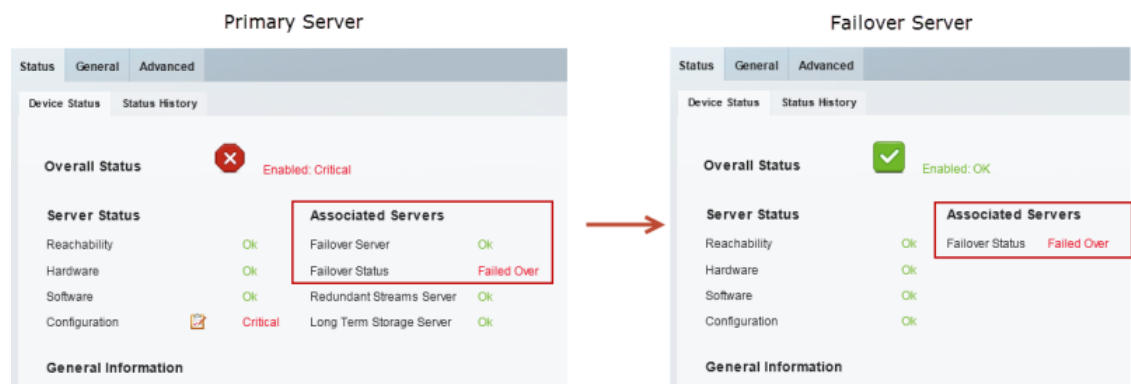
Failover status is indicated in the server Status page ([Figure 12-1](#)). The possible *Failover Status* values are:

- *In Failover*
- *Not In Failover*
- *Could Not Failover* (this occurs if a different Primary server already failed over to the same Failover server.)

For example, [Figure 12-1](#) displays a Primary Media Server with a critical configuration error that causes a failover.

- The Failover Server status is *OK* (green), indicating that the server is up and ready to assume control.
- The Failover Status is *Failed Over*, indicating that a failover occurred.
- The Failover server Status page also displays *Failed Over*.

Figure 12-1 Primary and Failover Server Status (in Failover)



Tip

See the [Viewing the Server HA Status, page 12-22](#) for more information.

When a user attempts to access live or recorded video from a camera that is associated with the Primary server, the request will time out and be forwarded to the Failover server, which completes the request and sends the requested video.

Because the Failover server maintains the same configuration as the Primary server (in real time), users will not encounter a change in network behavior other than a slight delay while communication is established with the Failover server.

Once the Primary server comes back online, it will automatically resume control from the Failover server. The Failover server will revert to hot standby status.

**Note**

Polling between the servers is coordinated based on the system time in each server. Use a NTP time source to ensure server synchronization.

Define the Media Server HA Role and Associated Servers

Complete the following procedures to define the HA role of each Media Server in your deployment. Then associate the Primary and Redundant servers with other HA servers.

Usage Notes


- All Media Servers are assigned the Primary HA role by default.
- A *Primary* Media Server can be associated with additional Failover, Redundant, or Long Term Storage Media Servers.
- A *Redundant* Media Server can only be associated with a Long Term Storage server.
- Long Term Storage and Failover servers cannot be associated with other servers.
- Co-located Servers—If the Media Server is enabled on the same server as the Operations Manager, 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).

Procedure

-
- Step 1** Enable the Media Server service when installing and configuring a Cisco Video Surveillance server. See the [Cisco Video Surveillance Management Console Administration Guide](#) for more information.
- Step 2** Add the server to Cisco VSM.
See the “[Configuring Servers](#)” section on page 6-1.
- Step 3** Activate the Media Server service on the server.
See the “[Configuring Media Server Services](#)” section on page 7-1.
- Step 4** Define the *Server Type*.



Note All Media Servers are assigned the Primary HA role by default.

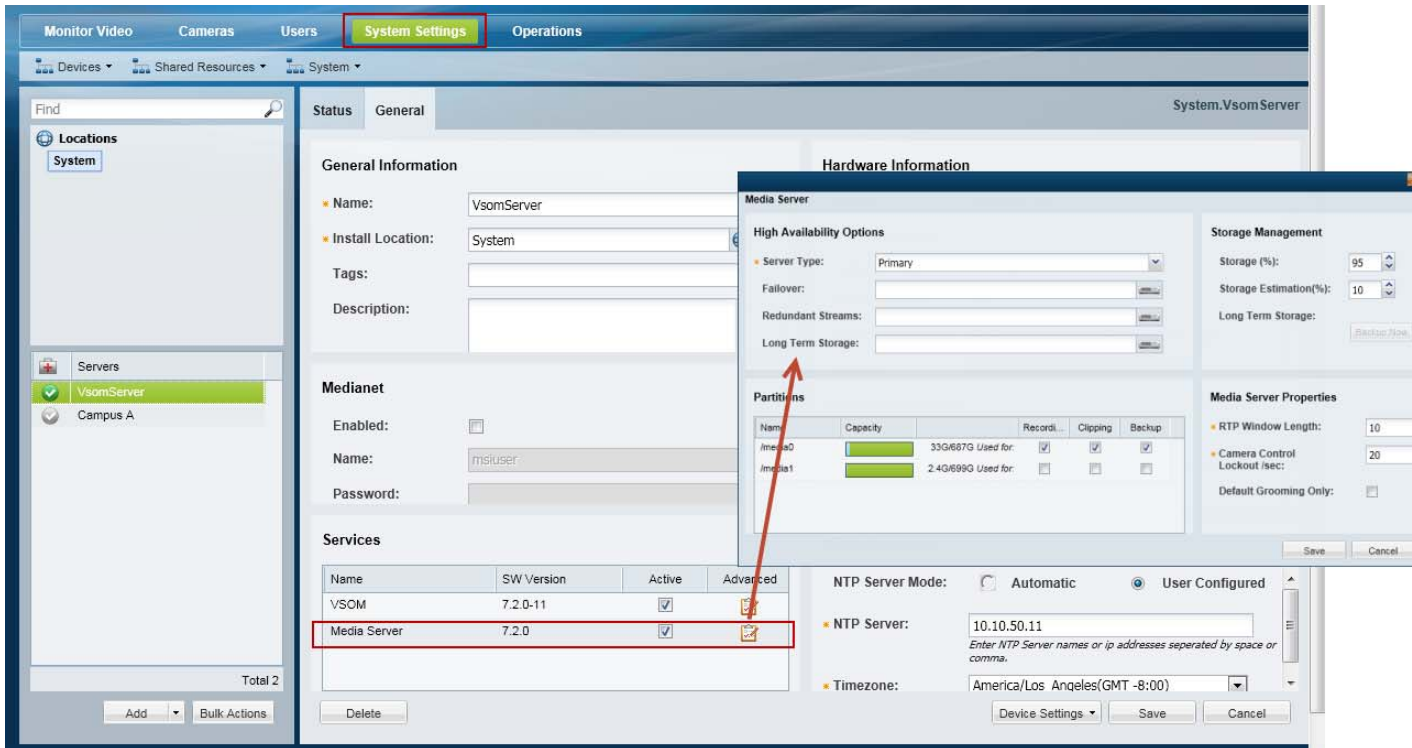
- a. Select the server (**System Settings > Server**).
- b. Click the **Advanced**  icon for the Media Server service ([Figure 12-2](#)).
- c. Select the *Server Type*.



Tip

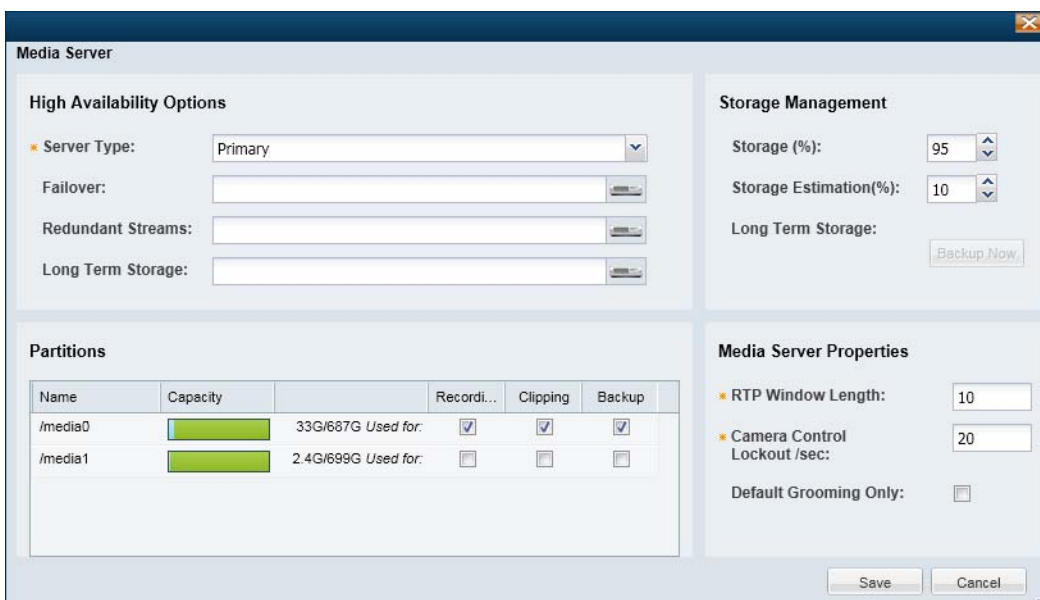
See the “[Understanding Redundant, Failover, and Long Term Storage Servers](#)” section on page 12-4 for more information.

Figure 12-2 High Availability Options



Step 5 Associate the Primary server with the Failover, Redundant, or Long Term Storage Media Servers (Figure 12-3).

Figure 12-3 Defining the High Availability Server Type and Options



Step 6 (Optional) Associate the *Redundant* Media Server with a Long Term Storage server.

Configuring the Camera Template HA Options

Each camera is assigned to a *Primary* Media Server which processes, stores, and plays back the camera's live and recorded video. Use the *Advanced Storage* options to also send the camera video to Redundant, Failover, and/or Long Term Storage servers.



Tip

Use a camera template to apply the *Advanced Storage* options to multiple cameras, or a custom template to apply the HA settings only to a single camera.



Note

You can configure the camera *Advanced Storage* settings if the HA servers are not available, but a configuration error and alert will be generated. Once the server configuration is complete, the errors will be removed.”

Summary Steps

	Task
Step 1	Verify that the HA Requirements are met, and review the “ Summary Steps ” section on page 12-3.
Step 2	Complete the “ Configuring the Redundant and Failover Options ” section on page 12-12.
Step 3	(Optional) Complete the “ Archiving Recordings to a Long Term Storage Server ” section on page 12-16.
Step 4	(Optional) Complete the “ Defining the Recording Options ” section on page 12-20.

Configuring the *Redundant* and *Failover* Options

The **High Availability and Failover** options allow you to select the type of *stream redundancy* for the camera or template.

By default, live and recorded video from a camera is sent to a single *Primary* server. If the Primary server goes down, then the live and recorded video cannot be processed, saved or displayed([Figure 12-4](#)).

- If a *Redundant* server is installed and configured, however, a camera's video streams can also be sent to the *Redundant* server.



Note

Some cameras do not support sending motion or contact-closure events to a redundant server.

- A *Failover* server can also be added as a hot standby server, ready to assume *Primary* server functionality if the Primary server goes down or is offline (the *Failover* server only serves the *Primary* server, not the *Redundant* server).

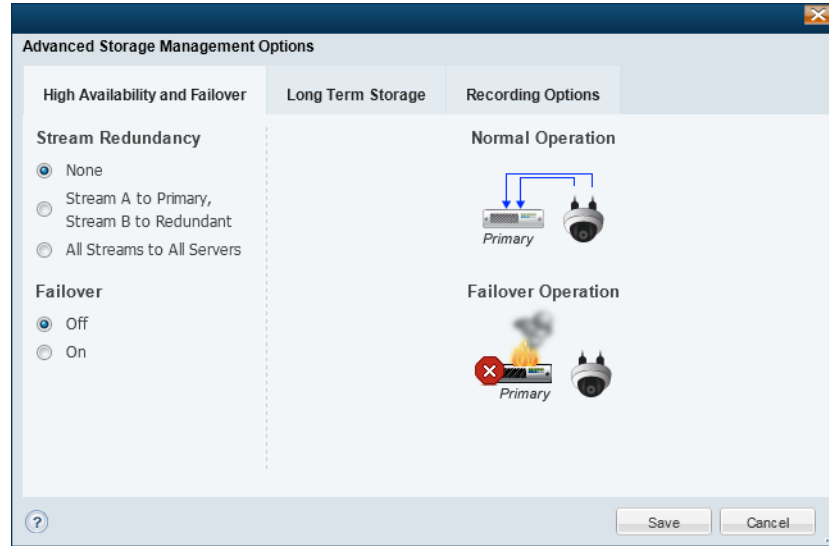
Figure 12-4 High Availability and Failover Options

Table 12-3 describes the Stream Redundancy and Failover options for a camera or camera template. Select a *Stream Redundancy* option (as shown in Figure 12-4), and then turn the *Failover* option **On** or **Off**.

Table 12-3 Stream Redundancy Options With and Without a Failover Server






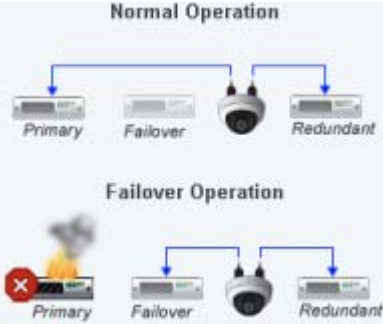

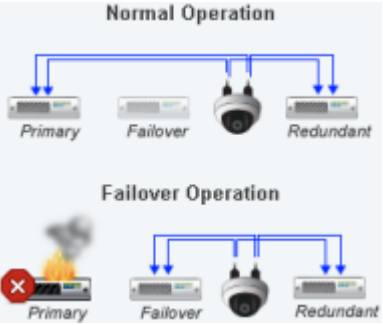
Option	Stream Redundancy	Failover Option
None	<p>All live and recorded streams are sent to a single <i>Primary</i> server.</p> <p>If the <i>Primary</i> server fails, camera control, recording, and playback is disabled.</p> <p>Normal Operation</p>  <p>Failover Operation</p> 	<p>If the <i>Primary</i> server fails or goes offline, the <i>Failover</i> server immediately assumes control (hot standby).</p> <p>Normal Operation</p>  <p>Failover Operation</p> 

Table 12-3 Stream Redundancy Options With and Without a Failover Server (continued)

Option	Stream Redundancy	Failover Option
Stream A to Primary, Stream B to Redundant	<p>A camera's stream A video is sent to the <i>Primary</i> server. Stream B is sent to the <i>Redundant</i> server.</p> <p>If the <i>Primary</i> server fails, the <i>Redundant</i> server still supports the camera stream B video, although it may be lower resolution.</p> 	<p>If the <i>Primary</i> server fails or goes offline, the <i>Failover</i> server continues to support the camera's stream A video.</p> 
All Streams to All Servers	<p>Both stream A and stream B (if configured) are sent to both the <i>Primary</i> and <i>Redundant</i> server.</p> <p>If the <i>Primary</i> server fails, both video streams are still supported by the <i>Redundant</i> server.</p> 	<p>If the <i>Primary</i> server fails or goes offline, both stream A and stream B continue to be supported by two servers (the <i>Failover</i> and <i>Redundant</i>).</p> 

Procedure

The following procedure summarizes how to configure a redundant and/or failover server for a camera or camera template.

Note: The *Primary* server associated with the camer(a) must be configured with a *Redundant* and/or *Failover* server. See the [Define the Media Server HA Role and Associated Servers](#), page 12-9.

- Step 1** Install and configure the *Primary* Media Server associated with the camera(s).
See the [Define the Media Server HA Role and Associated Servers](#), page 12-9
- Step 2** Choose **Cameras** and select a camera or camera template.
- Step 3** Select the **Streaming, Recording and Events** tab.
- Step 4** Click **Advanced Storage** ([Figure 12-4 on page 12-13](#)).

- Step 5** Select a *Stream Redundancy* option, as described in [Table 12-3](#).
- Step 6** Turn the *Failover* option **On** or **Off**, as described in [Table 12-3](#).
- Step 7** Click **Save**.
-

Archiving Recordings to a Long Term Storage Server

A **Long Term Storage** (LTS) server allows you to automatically transfer recorded video from the Primary server to a LTS server. This frees the limited space on the Primary server, and provides a dedicated resource to store and play back old recordings.

- Recordings remain in the Primary and Redundant servers even if they are archived to an LTS server. The recordings are removed from the Primary and Redundant servers based on the *Retain* settings available in the camera or template configuration page (*Retain continuous recordings* and *Retain event recordings*).
- Recordings are removed from the LTS server according to the settings described in [Figure 12-6](#).



Tip You can also click **Backup Now** from the Primary or Redundant server to immediately back up the recordings to the LTS server. Select the **Advanced** tab and click **Backup Now**.

Refer to the following topics for more information:

- [Prerequisite: Enable the Media Server Backup Partition, page 12-16](#)
- [Configuring the LTS Server, page 12-17](#)

Prerequisite: Enable the Media Server Backup Partition

To archive recordings to an LTS server, you must enable a partition on the Media Server to store the backups.



Note The Backup partition is used only to backup recordings on a Long Term Storage server.

Procedure

- Step 1** Click the **Media Servers** icon.
- Step 2** Select the location and then select the LTS Media Server.
- Step 3** Click the **Advanced** tab.
- Step 4** Under *Partitions* ([Figure 12-5](#)), select the *Backups* check box for the */media1* or */media0* repository.
- Step 5** This setting specifies which hard disk partition will be used to store the archived recordings files.
- Step 6** Click **Save**.

Figure 12-5 Media Server Partitions

The screenshot shows the 'Advanced' tab of a configuration window. It includes sections for 'High Availability Options' (Failover, Redundant Streams, Long Term Storage), 'SMTP Management' (Server, From Address), and a 'Partitions' table. A red arrow points from the 'Advanced' tab to the 'Partitions' table.

Name	Capa...	Recordi...	Clipping	Backup
/media0	10G/987G Used for	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
/media1	2.4G/999G Used for	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Configuring the LTS Server




Click the **Advanced Storage** option in a camera or template and select **Long Term Storage** (Figure 12-6). The LTS options are available only if the Primary server is configured with an LTS server and the camera or camera template is configured to record video. For example, in Figure 12-6, Video Stream B is disabled since the template is not configured to record video.

Figure 12-6 Long Term Storage Options

The screenshot shows the 'Advanced Storage Management Options' dialog box. It has three tabs: 'High Availability and Failover', 'Long Term Storage' (selected), and 'Recording Options'. The 'Long Term Storage' tab is divided into 'Video Stream A' and 'Video Stream B' sections. 'Video Stream A' is active, showing 'What to Archive' (with icons for motion, audio, and video), 'Retain archive for' (1 day(s)), and 'When to Archive' (Weekly, Sunday, 09:26:08). 'Video Stream B' is disabled, indicated by a greyed-out icon. 'Save' and 'Cancel' buttons are at the bottom right.

The following table describes the Long Term Storage Settings:

Table 12-4 Long Term Storage Options

Field	Description
What to Archive	<p>Select the following for video stream A and B:</p> <ul style="list-style-type: none">  —Do not transfer any recorded video to the LTS server.  —Transfer only video that is recorded on a motion event (if configured on the camera/template).  —Transfer both continuous and motion event recordings (if configured on the camera/template).
Retain archive for	<p>The number of days that the recorded video will be retained on the LTS. The video will be deleted from the LTS when the specified number of days are exceeded. Once deleted, the video is no longer be available for playback.</p> <p>Note If the disk capacity of the LTS server is exceeded, the oldest recording is deleted to provide room for the newest recording.</p>
When to Archive	<p>The frequency and time of day when all recorded video on the Primary server (based on “What to Archive”) will be transferred to the LTS server.</p> <ul style="list-style-type: none"> Daily—Transfers all recorded video every day at the specified time, every day of the week. For example, every day at midnight. Weekly—Transfers all recorded video on the specified day of the week and time. For example, every Sunday at 11 p.m. Monthly—Transfers the past month of recorded video every month at the specified day and time. For example, on the first day of every month at 1 a.m.

Procedure

The following procedure summarizes how to archive recordings to a LTS server.

Note: The Primary server associated with the camer(a) must be configured with an LTS server. See the [“Define the Media Server HA Role and Associated Servers”](#) section on page 12-9.

-
- Step 1** Install and configure an LTS server for the *Primary* Media Server associated with the camera(s).
- See the [Define the Media Server HA Role and Associated Servers, page 12-9](#)
- Step 2** Configure the Store Partition on the LTS Server.
- [Prerequisite: Enable the Media Server Backup Partition, page 12-16](#)
- Step 3** Choose **Cameras** and add or edit a camera or camera template.
- [Adding and Managing Cameras, page 8-1](#)
- Step 4** Select the **Streaming, Recording and Events** tab and configure recording.
- [Configuring Continuous, Scheduled, and Motion Recordings, page 10-7](#)
- Step 5** Click **Advanced Storage**.

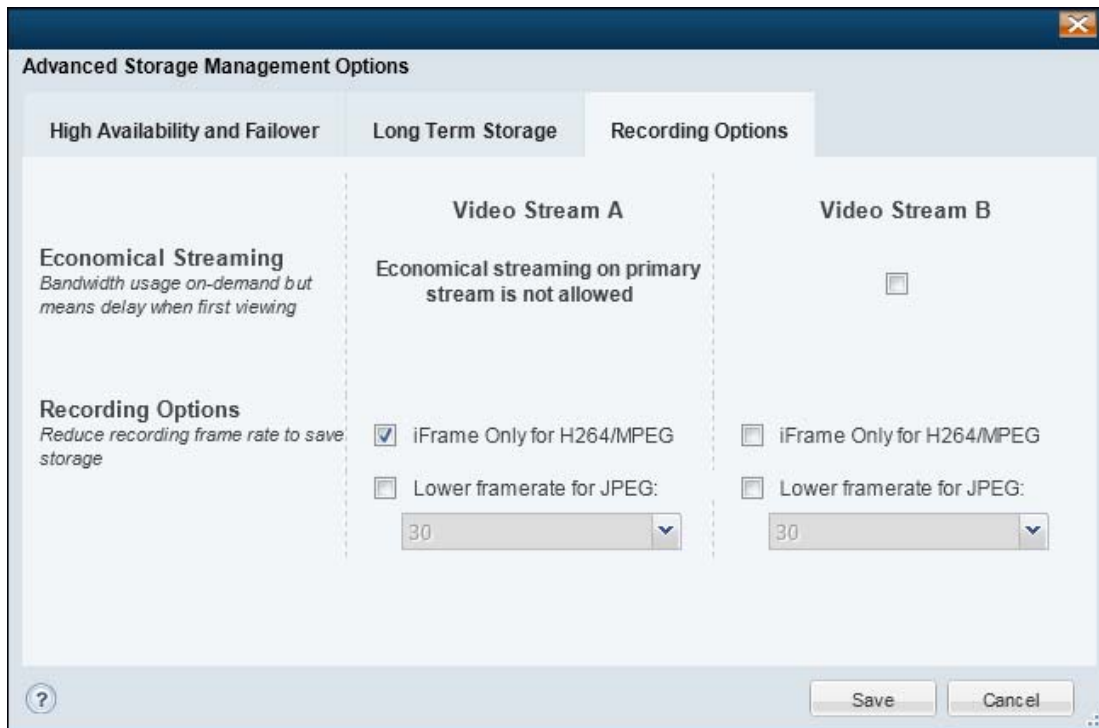
- Step 6** Click the **Long Term Storage** tab ([Figure 12-6 on page 12-17](#)).
- Step 7** Select the options for Stream A and Stream B ([Figure 12-6 on page 12-17](#)).
- Step 8** Click **Save**.
-

Defining the *Recording Options*

The *Recording Options* can be used to reduce the bandwidth and processing requirements for streaming and recording video (Figure 12-7). Select a template and click **Advanced Storage > Recording Options** to define the following options.

- [Economical Streaming, page 12-20](#)
- [Recording Options, page 12-21](#)

Figure 12-7 Camera/Template HA Recording Options



Economical Streaming

Select the Economical Streaming option to place the secondary stream in suspended mode. The stream will be active only when requested by a user (on-demand).

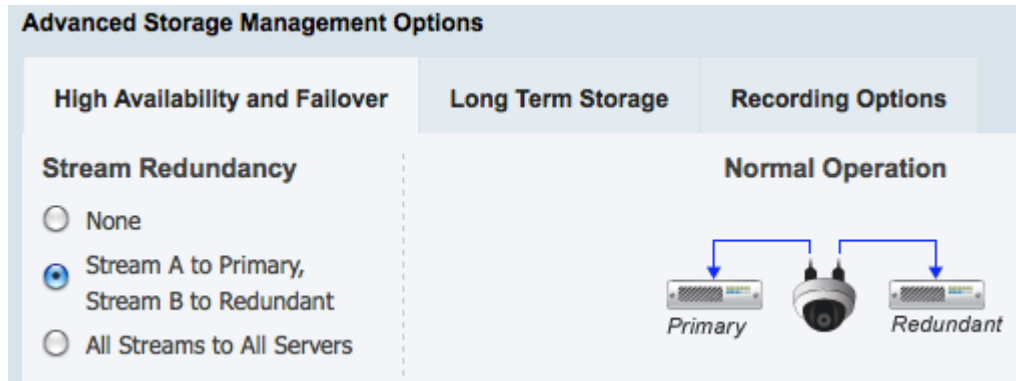
By default this feature is deselected and video is streamed at all times and is instantly available for viewing.

Usage Notes

- When selected, video playback will be delayed while the request is being processed.
- When Economical Streaming is enabled, motion event alerts and other Advanced Event processing is disabled since video is only sent when requested by a user. Do not configure these features on Stream B when Economical Streaming is enabled.
- Scheduled recordings can be configured with Economical Streaming enabled since streaming is automatically begun when the recording is scheduled.

Supported Configurations

- Economical Streaming is available only on Stream B.
- This option is only available when Stream A is sent to the Primary Media Server and Stream B is sent to the redundant Media Server (Figure 12-8).

Figure 12-8 Economical Streaming

See the “[Configuring the Redundant and Failover Options](#)” section on page 12-12 for more information.

Unsupported Configurations

Economical Streaming is not supported in the following configurations:

- Both Stream A and Stream B are sent to the Primary server.
- Both Stream A and Stream B are sent to both the Primary and Redundant servers.

Recording Options

- **iFrame Only for H264/MPEG**—Use the iFrame format only when recording H264/MPEG video.
- **Lower framerate for JPEG**—Specify a lower frame rate to reduce the bandwidth, processing, and storage requirements of video recorded from Stream B. A lower framerate number requires less network and server resources, but results in lower quality video.

Viewing the Server HA Status

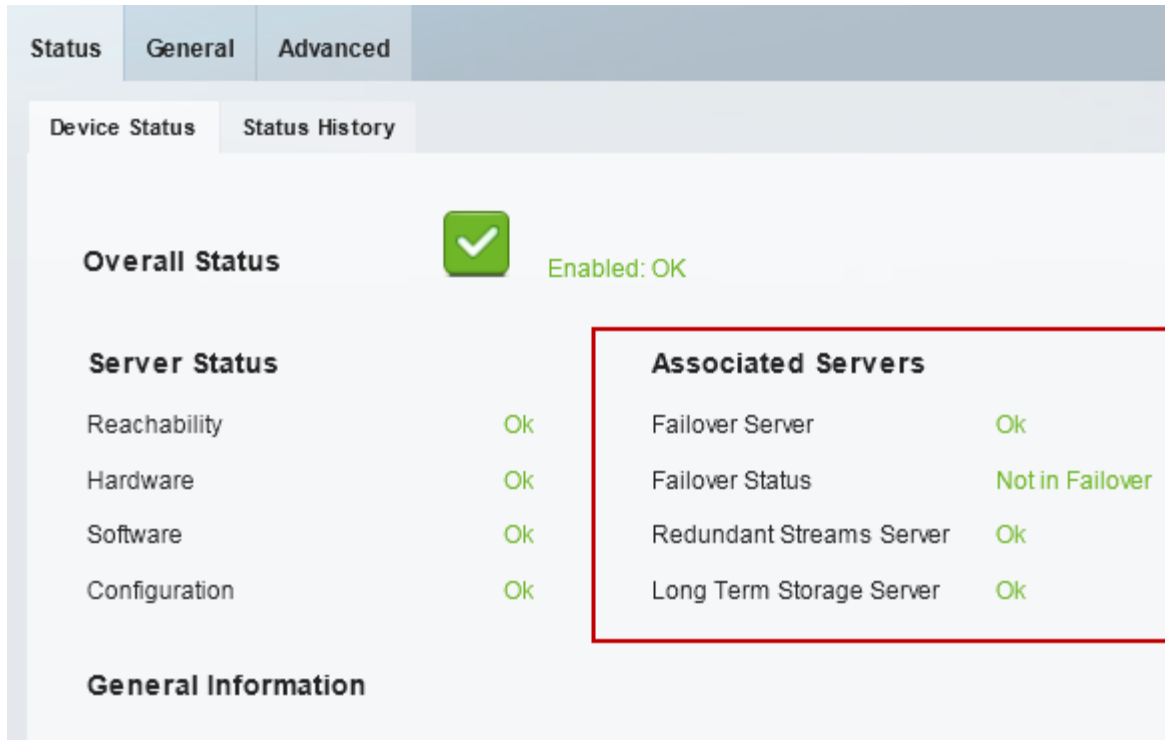
Open the camera status page to view the servers associated with that camera. For example, if the Primary server that services a camera is configured with a Failover, Redundant, or Long Term Storage server, the status of those servers is displayed.

Procedure

To view the HA server status, do the following:

-
- | | |
|---------------|--|
| Step 1 | Log on to the Operations Manager. <ul style="list-style-type: none">• See the “Logging In” section on page 1-18. |
| Step 2 | Select the Media Server or camera to edit (click Cameras or System Settings > Media Servers and select the device). |
| Step 3 | Click the Status tab. |
| Step 4 | Review the status of the current server and associated servers. For example: <ul style="list-style-type: none">• Figure 12-9: An example of a Primary Server and associated HA servers• Figure 12-10: Examples of the Status Pages for each HA Server Type.• See also Figure 12-1 on page 12-7 for an example of the Primary and Failover Status pages when a failover occurs. |

Figure 12-9 Primary Server Status Including Associated Servers

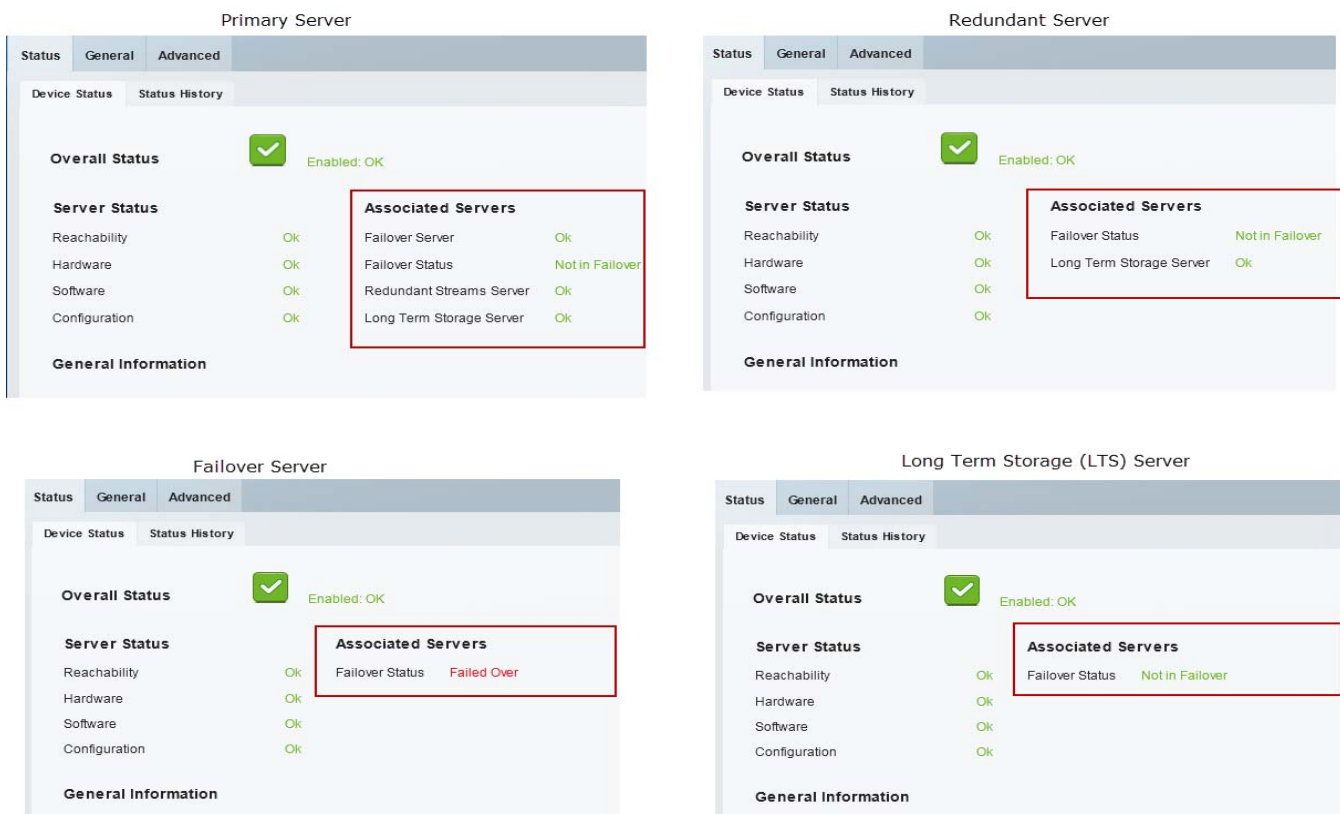


Field	Description
Overall Status	The status of the current server. See the “Understanding the Overall Status” section on page 13-8 for more information.
Associated Servers (the HA servers associated with the current server)	
Failover Status	The Overall Status of the failover server. See the “Understanding the Overall Status” section on page 13-8 for more information. Open the Status page of the associated failover server to view additional details about the server status.
Failover Status	The HA status of the Failover server. The possible values are: <ul style="list-style-type: none"> <i>In Failover</i> <i>Not In Failover</i> <i>Could Not Failover</i> (this occurs if a different Primary server already failed over to the same Failover server.) See the “Understanding Failover” section on page 12-7 for more information.
Redundant Streams Server	The Overall Status of the Redundant server that is associated with the Primary server. A <i>Redundant</i> server can support multiple Primary servers. You must ensure that the Redundant server contains the disk and processing capacity to support all cameras that send video streams to the server.

Field	Description
Long Term Storage Server	<p>The Overall Status of the Long Term Storage server associated with the Primary or Redundant server.</p> <p>A <i>Long Term Storage</i> server can support multiple Primary and Redundant servers. You must ensure that the server contains the disk and processing capacity to support all associated servers and cameras.</p>

Open the **Status** page for each HA server to view additional information about the overall status and HA status of that server (Figure 12-10).

Figure 12-10 Examples of HA Server Status



Server Status	Description
Primary server	The status of the HA servers associated with the Primary server.
Failover server	<p>The status of the Failover server as a hot standby.</p> <p>A Failover server can provide hot standby support for multiple Primary servers. If one Primary server fails over, however, the Failover server will be unavailable to support the other Primary, and the Failover Status will be “Could Not Failover”.</p> <p>See the “Understanding Failover” section on page 12-7 (and Figure 12-1) for more information.</p>

Server Status	Description
Redundant server	<p>The Failover server status, and the LTS server status.</p> <p>A <i>Redundant</i> server can support multiple servers. You must ensure that the Redundant server contains the disk and processing capacity to support all associated Primary servers.</p>
Long Term Storage server	<p>The Failover server status.</p> <p>A <i>Long Term Storage</i> server can support multiple Primary and Redundant servers. You must ensure that the server contains the disk and processing capacity to support all associated servers.</p>



CHAPTER 13

Monitoring System and Device Health

Refer to the following topics for information to monitor the health of the system or of a specific device, to view the status of user-initiated *jobs*, a record of user actions (Audit Logs), and other features.

Contents

- [Understanding Events and Alerts, page 13-2](#)
 - [Overview, page 13-2](#)
 - [Event Types, page 13-4](#)
 - [Triggering Actions Based on Alerts and Events, page 13-4](#)
 - [Monitoring Device Health Using the Operations Manager, page 13-5](#)
- [Health Dashboard: Viewing Device Health Summaries, page 13-6](#)
- [Device Status: Identifying Issues for a Specific Device, page 13-8](#)
- [Health Notifications, page 13-14](#)
- [Reports, page 13-16](#)
- [Synchronizing Device Configurations, page 13-17](#)
 - [Overview, page 13-17](#)
 - [Viewing Device Synchronization Errors, page 13-19](#)
 - [Understanding Device Configuration Mismatch Caused by Media Server Issues, page 13-20](#)
 - [Repairing a Mismatched Configuration, page 13-21](#)
 - [Manually Triggering a Media Server Synchronization, page 13-22](#)
 - [Device Data That Is Synchronized, page 13-22](#)
 - [Synchronization During a Media Server Migration, page 13-23](#)
- [Viewing the Server Management Console Status and Logs, page 13-24](#)
- [Understanding Jobs and Job Status, page 13-25](#)
- [Viewing Audit Logs, page 13-31](#)

Understanding Events and Alerts

Events and alerts reflect changes to system and device health, or security events that occur in the system. These events and alerts can be viewed in a monitoring application, such as the Operations Manager or Cisco SASD, or be used to generate notifications, or trigger additional actions.

Refer to the following topics for more information:

Overview

Events represent incidents that occur in the system and devices. Alerts aggregate (group) those events together for notification purposes. For example, if a camera goes offline, and comes back online repeatedly, all events for that issue are grouped under a single alert resulting in a single notification. This prevents operators from being flooded with notifications for multiple occurrences for the same issue.

Figure 13-1 shows the Alert-centric workspace in the Cisco SASD application. The selected alert also displays a list of the events associated with that alert.

Figure 13-1 Alerts and Associated Events in Cisco SASD



1 Selected Alert. The severity is the severity of the most recent event for that alert.

2 Events associated with the selected alert.

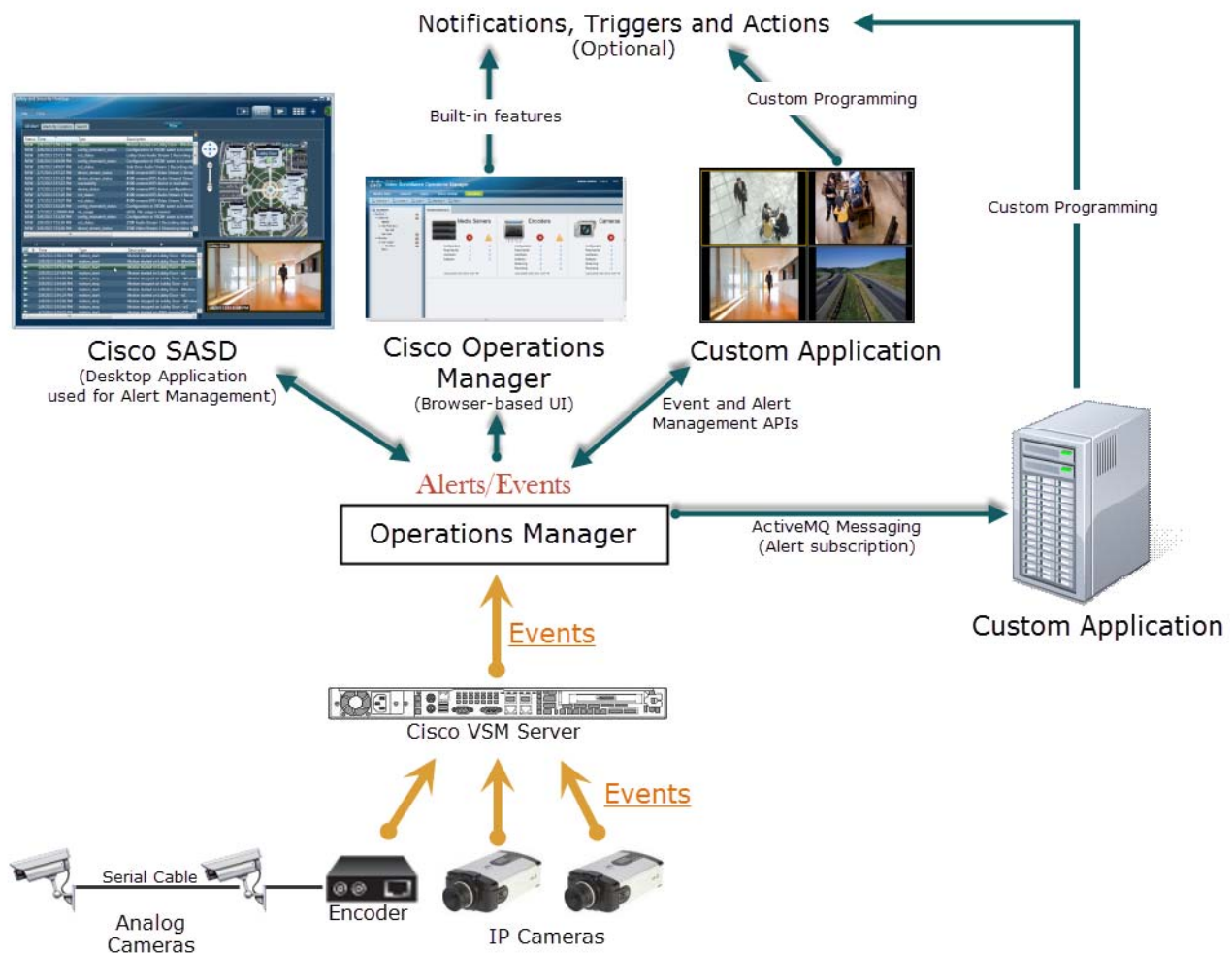


Note

The alert severity reflects the severity of the most recently generated event. For example, if a camera becomes unreachable and the streaming status is Critical, the alert is Critical. When the camera becomes reachable again, and the streaming status normal event occurs, and the alert severity is changed to INFO.

Figure 13-2 summarizes how Cisco VSM events and alerts are generated, viewed and managed.

Figure 13-2 Health Events, Alerts, and Notifications



1. Events are generated by cameras, encoders and Media Servers.
2. The Cisco VSM Operations Manager aggregates the events into alerts:
3. The browser-based Operations Manager can be used to view events, send notifications, or (optionally) perform actions that are triggered by security events (such as motion detection).
4. Additional monitoring applications can also be used to view events and alerts:

- The Cisco Video Surveillance Safety and Security Desktop (Cisco SASD) application can be used to view alerts, related events, and related video. You can also change the alert state, add comments, close the alert, and perform other management options.
- Custom applications can be written gather information, change the alert status, add comments, or trigger actions when an event or alert occurs. See the *Cisco Video Surveillance API Programming Guide* for more information.

**Note**

Custom applications can also subscribe to ActiveMQ topics to receive notifications about device and system changes. For example, the Alerts topic notifies subscribers when any alert occurs in the system. The custom application can use the ActiveMQ message contents to optionally trigger additional notification or actions. See the *Cisco Video Surveillance API Programming Guide* for more information.

Event Types


Cisco VSM generates two types of events: device health events and security events:

- **Health Events** are generated when a device health change occurs, such as reachability, fan speed, file system usage, or other device-related issues. Critical health events generate alerts by default.
- **Security Events**—Events such as motion stop or start, analytics, contact closures, or soft triggers from an external system can be configured to generate alerts, or perform other actions. Security events do not generate alerts by default.

Triggering Actions Based on Alerts and Events

The Operations Manager includes the following built-in features to trigger notifications and other actions:

Table 13-1 **Triggering Actions**

Action	Description	More Information
Critical health notifications	Use the Health Notifications feature to send notifications when a critical device error occurs. Critical errors are health events that impact the device operation or render a component unusable. For example, a Media Server that cannot be contacted on the network, or a camera that does not stream or record video.	Health Notifications, page 13-14
Motion event notifications	Click Alert Notifications  in the camera template to enable or disable the alerts that are generated when a motion event stops or starts.	Creating or Modifying a Template, page 10-3
Trigger actions when a security event occurs	Use the Advanced Events feature (in the camera template) to trigger a variety of actions when a security event occurs. For example, you can send alerts only on motion start, on motion stop, stop or start video recording, record video for a specified length of time, invoke a URL, move a camera position to a specified PTZ preset, or display video on a Video Wall.	Using Advanced Events to Trigger Actions, page 10-11

Monitoring Device Health Using the Operations Manager



The **Health Dashboard** displays a summary of all device errors in your deployment, allowing you to quickly view the health of all cameras, encoders and Media Servers. You can also click a link for any affected device to open the device status and configuration pages.


Table 13-2 summarizes the Operations Manager monitoring features.

Table 13-2 **Monitoring Features**

Monitoring Feature	Location	Description
Health Dashboard: Viewing Device Health Summaries, page 13-6	Operations > Health Dashboard	Open the Health Dashboard to view a summary of Warning or Critical errors for all configured devices. Click on an entry to open the device status and configuration page and further identify the issue.
Device Status: Identifying Issues for a Specific Device, page 13-8	Cameras > Status System Settings > Server > Status System Settings > Encoder > Status	Click the Status tab in the device configuration page to view the specific type of error for a device. The status categories show where the error occurred. <ul style="list-style-type: none"> Click the Status History to view the alert messages for the device. Click the Affecting Current Status radio button to view only the alerts that are causing the
Health Notifications, page 13-14	Operations > Health Notifications	Send emails to specified recipients when a critical device error occurs.
Reports, page 13-16	Operations > Reports	Generate and download information about the Cisco Video Surveillance user activity, device configuration, and other information.
Synchronizing Device Configurations, page 13-17	Device configuration page. Click the Repair or Replace Config button.	If a configuration mismatch error occurs, you can click the device Repair button to replace the configuration settings on the device with the settings in Operations Manager.
Viewing the Server Management Console Status and Logs, page 13-24	Operations > Management Console	Displays logs, hardware status, and system trend information for the Cisco Video Surveillance server. The Management Console is a separate browser-based interface that requires a separate <i>localadmin</i> password. See the Cisco Video Surveillance Management Console Administration Guide for more information.
Understanding Jobs and Job Status, page 13-25	System Settings > Jobs	Displays a summary of current and completed jobs triggered by user actions.
Viewing Audit Logs, page 13-31	Operations > Audit Logs	Displays successful configuration changes. You can sort or filter the results by user, device, and other categories.

Health Dashboard: Viewing Device Health Summaries

Open the **Health Dashboard** (from the **Operations** page) to view a summary of servers, encoders and cameras that are experiencing critical  or warning  faults (Figure 13-3).

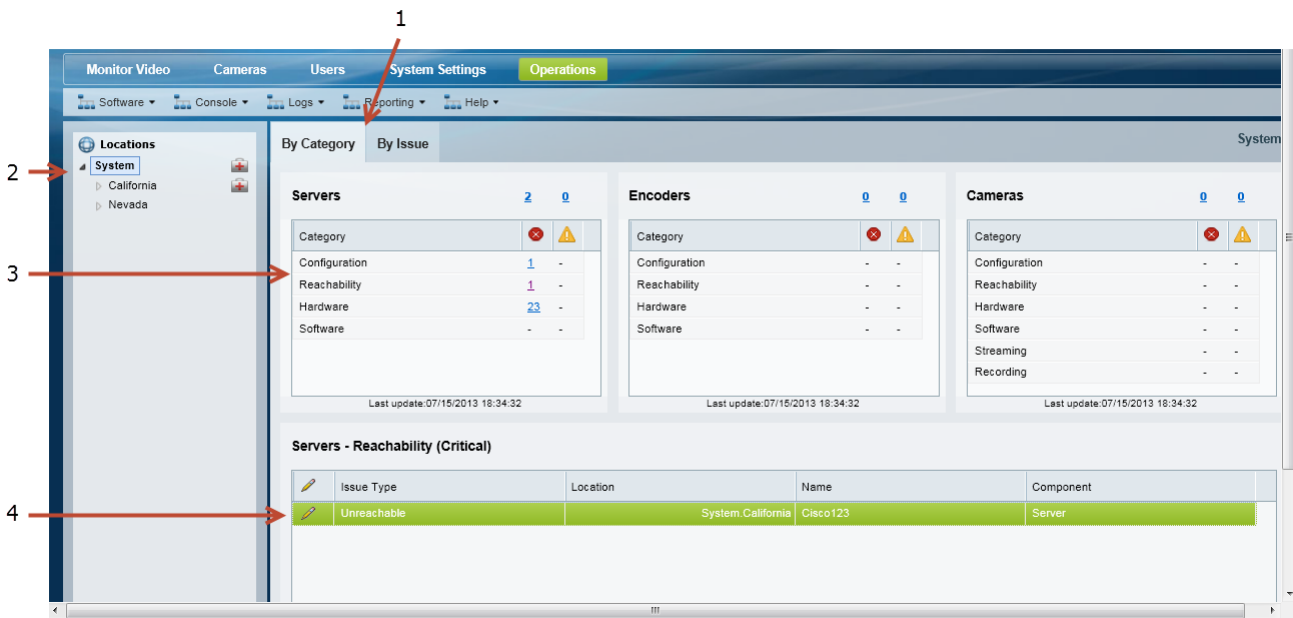
Devices are displayed for the selected location. Click the number next to a category (such as *Configuration*) to view the affected devices, and then click the  icon to open the device status and configuration pages.





Tip


Refresh the Health Dashboard page to view updated results. The dashboard does not automatically refresh.

Figure 13-3 System Health Dashboard



- 1 Click a tab to view a list of issues based on the following:
 - **By Category**—displays health issues grouped into categories,
 - **By Issue**—displays issues list for each type of device (server, encoder, camera).
- 2 Location.
Click a location to view a summary of devices assigned to that location.
- 3 Device health summary for the selected location.
Each device type shows the number of critical  or warning  faults. See Table 13-3 for more information.

Tip Click a number to display the devices that are experiencing the fault. For example, click the number 23 next to *Hardware* to view the devices experiencing hardware issues.
- 4 The devices for a selected fault category.

Tip Click the  icon to open the device’s configuration page. See the “[Device Status: Identifying Issues for a Specific Device](#)” section on page 13-8 for more information.

**Tip**

- Device errors are cleared automatically by the system or manually cleared by an operator using the Cisco SASD or another monitoring application. Refresh the page to view the latest information. Some alerts cannot be automatically reset. For example, a server I/O write error event.
- If the system or server is performing poorly, use the diagnostic tools available in the server Management Console to view performance, hardware and system information. See the [“Accessing the Management Console” section on page 15-2](#) for more information.

Procedure

Complete the following procedure to access the Health Dashboard:





- Step 1** Click the **Operations** tab.
- Step 2** Click **Health Dashboard** ([Figure 13-3](#)).
- Step 3** Choose a location to view a summary of the faulty devices at that location.
Locations with one or more faulty devices display a Health icon .
- Step 4** Click the **By Category** or **By Issue** tab.
- Step 5** Review the number of devices experiencing an error for each device type.
The number represents the number of devices experiencing that error. For example, 3 servers s might be experiencing a network error.

Table 13-3 **Device Health Fault Types**

Icon	Error Type	Description
	Warning	Warnings are based on activity that occurs without incapacitating a component, for example, interruptions in operation due to packet losses in the network. These activities do not change the overall state of the component, and are not associated with “up” and “down” health events.
	Critical	<p>Critical errors are health events that impact the device operation or render a component unusable. For example, a Media Server that cannot be contacted on the network, or a configuration error. Components in the critical state remain out of operation (“down”) until another event restores them to normal operation (“up”). Critical errors also affect other components that depend upon the component that is in the error state. For example, a camera in the critical error state cannot provide live video feeds or record video archives.</p> <p>See the “Health Notifications” section on page 13-14 for instructions to send emails when a critical event occurs.</p>

- Step 6** Click a number to display the specific devices experiencing the fault.
- Step 7** Click the  icon to open the device Status page.
- Step 8** Continue to the [“Device Status: Identifying Issues for a Specific Device” section on page 13-8](#) for more information.
- Step 9** Take corrective action to restore the device to normal operation, if necessary.
- Step 10** For example, if a configuration mismatch occurs, see the [“Synchronizing Device Configurations” section on page 13-17](#).

Device Status: Identifying Issues for a Specific Device

Cameras, encoders, and Media Server include a Status tab that displays health information for the device and associated servers (Figure 13-4). While the Overall Status summarizes the device health, the status categories specify if an error has occurred with the network connection, configuration, hardware, or other category. Click the **Status History** tab to view device events, including any specific events that are affecting the device status.

See the following topics for more information:

- [Understanding the Overall Status, page 13-8](#)
- [Understanding Device Status, page 13-10](#)
- [Viewing Device Error Details, page 13-13](#)

Understanding the Overall Status

Click the device Status tab to view the overall operational state (Figure 13-4).

Figure 13-4 Overall Status Camera Device Status

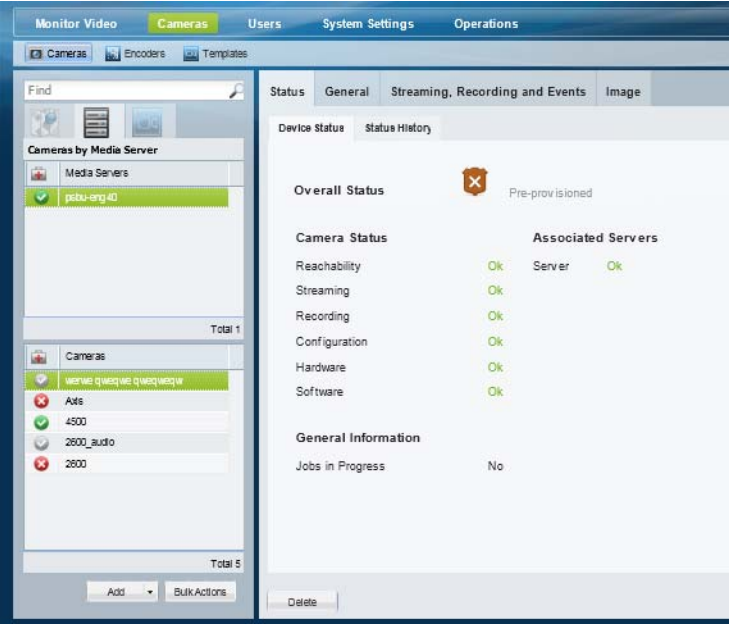


Table 13-4 describes the overall device states:

Table 13-4 Overall Status







Status	Color	Color	Description
Enabled: OK		Green	The device is operating normally.
Enabled: Warning		Yellow	A minor event occurred that did not significantly impact device operations.

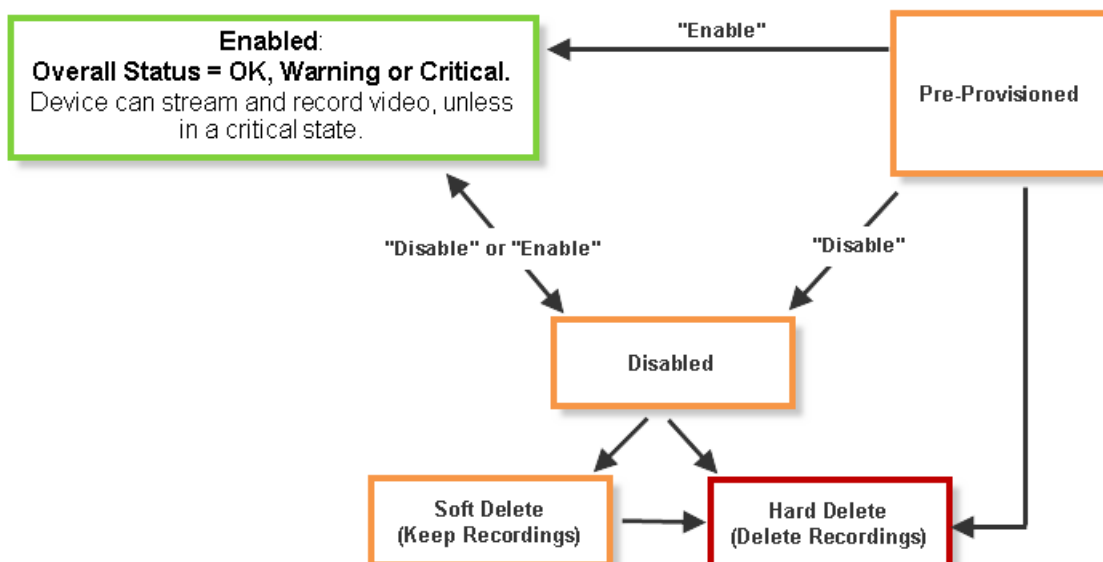
Table 13-4 Overall Status (continued)

Status	Color	Color	Description
Enabled: Critical		Red	An event occurred that impacts the device operation or renders a component unusable. See the “Health Notifications” section on page 13-14 for instructions to send automatic email notifications when a critical device issue occurs.
Pre-Provisioned		Brown	The camera is waiting to be added to the network and is not available for use. A pre-provisioned camera can be modified, but the camera cannot stream or record video until you choose Enable from the Device Settings menu.
Disabled		Brown	The device is disabled and unavailable for use. The configuration can be modified, and any existing recordings can be viewed, but the camera cannot stream or record new video.
Soft Deleted (Keep Recordings)		Brown	The device configuration is removed from the Operations Manager but the recordings associated with that device are still available for viewing (until removed due to grooming policies). To view the recordings, select the camera name in the Monitor Video page. Soft-deleted cameras are still included in the camera license count. See the “Installing Licenses” section on page 1-23 .
Hard Deleted (Delete Recordings)	None	None	The device and all associated recordings are permanently deleted from Cisco VSM. Note You can also choose to place the camera in the Blacklist. See the “Blacklisting Cameras” section on page 8-40 .

**Note**


Devices states can change due to changes in the device configuration, or by manually changing the status in the device configuration page ([Figure 13-5](#)).

Figure 13-5 Device Status



Understanding Device Status

From the device configuration page, click the **Status** tab to locate the category where the error occurred (such as configuration or hardware), and the alert messages that provide additional details regarding the cause of the error.

For example, if a critical configuration error occurs (Figure 13-6), the *Configuration* entry displays a *Critical* message in red. If a configuration mismatch occurs (where the device configuration is different than the Operations Manager configuration), click the  icon to view additional details in a pop-up window.

To resolve the issue, revise the device configuration, or click **Repair** or **Replace Config** to replace the device configuration with the Operations Manager version.

Figure 13-6 Device Status Summary

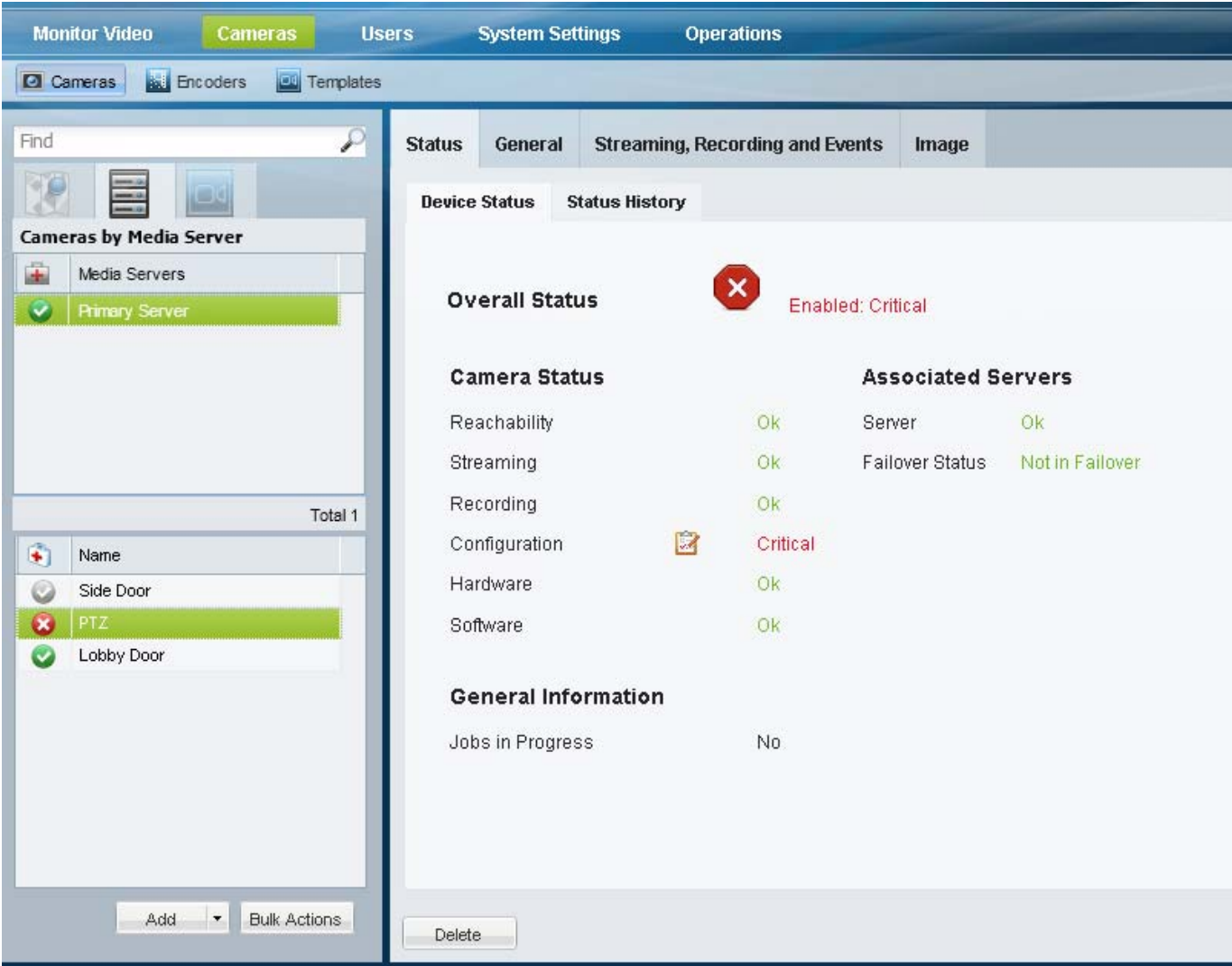


Table 13-5 describes the status categories. The categories are different for each type of device. For example, Media Servers include a *Software* category to indicate the health of server processes. An encoder does not include streaming or recording categories.

Table 13-5 **Device Status Categories**



Category	Devices	Description
Overall Status	All Devices	<p>The aggregated status of all categories included for the device.</p> <p>See the “Understanding the Overall Status” section on page 13-8.</p> <p>Note The <i>Associated Servers</i> status does not impact the <i>Overall Status</i>. For example, if the associated Media Server or Redundant Server is down, but the camera <i>Network</i> status is <i>Enabled: OK</i>, then the camera <i>Overall Status</i> is also <i>Enabled: OK</i>.</p>
Device Status		
Reachability	All Devices	<p>Indicates the health of the network connection.</p> <p>For example, a warning or critical event indicates that a device is unreachable on the network.</p>
Streaming	Cameras only	Indicates if the Media Server can stream live video from the camera
Recording	Cameras only	Indicates if the Media Server can successfully record video from the camera.
Configuration	Media Servers Cameras Encoders	<p>Indicates if the configuration was successfully applied to the device, and that the device configuration is the same on the Media Server and in Operations Manager.</p> <p>Configuration errors also display an  icon. Click the icon to view additional details about the error (see the “Viewing Device Error Details” section on page 13-13)</p> <p>For example, if a template is modified in the Operations Manager, but the configuration is not applied to the camera configuration, a synchronization mismatch occurs. See the “Synchronizing Device Configurations” section on page 13-17 for more information.</p>
Hardware	All Devices	Status of the physical device components, such as temperature.
Software	Media Servers only	Indicates the status of services hosted by a Media Server.
Jobs in Progress	All Devices	<p>Indicates if the device has one or more Jobs running.</p> <p>See the “Understanding Jobs and Job Status” section on page 13-25.</p>
Associated Servers		
Note The status of Failover, Redundant and LTS servers does not affect the overall status of a device.		
Server	Cameras and Encoders only	Indicates that the device can communicate with a Media Server.
Failover Server	HA server configurations only	Indicates the state of the Failover Media Server, when HA is enabled.
Failover Status	HA server configurations only	Indicates if the HA servers are in failover mode.

Table 13-5 *Device Status Categories (continued)*

Category	Devices	Description
Redundant Streams Server	HA server configurations only	Indicates if a Redundant server is available for streaming live video.
Long Term Storage Server	HA server configurations only	Indicates if a server is available to store recorded video beyond a specified date for archiving purposes.

Viewing Device Error Details

If a device error is displayed in the Status page (Figure 13-6), do one of the following:

- A Configuration error indicates that a configuration mismatch occurred (the configuration on the device is different than the Operations Manager settings). Click the  icon to view additional details and refer to the “[Synchronizing Device Configurations](#)” section on page 13-17 for instructions to correct configuration errors.
- Click the **Status History** tab (Figure 13-7) to view the specific events that determine device status.

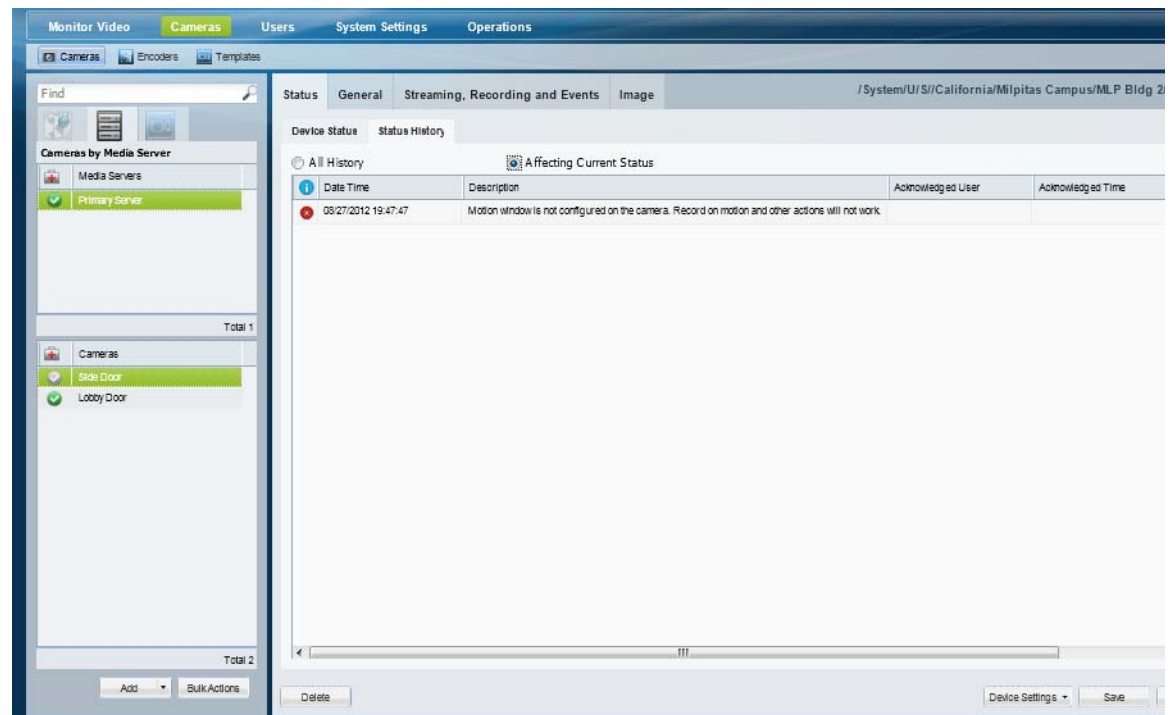


Tip


Click **Affecting Current Status** to view only the items that are currently affecting the summaries in the Device Status tab.

Use the information in these entries to take corrective action.

Figure 13-7 Camera Status History



Health Notifications

Health notifications are emails sent to one or more users when a critical device error occurs. Critical errors  are health events that impact the device operation or render a component unusable. For example, a Media Server that cannot be contacted on the network, or a camera that does not stream or record video.

**Note**

Configuration errors do not trigger health notification emails.

**Tip**

See the [“Health Dashboard: Viewing Device Health Summaries”](#) section on page 13-6 and the [“Device Status: Identifying Issues for a Specific Device”](#) section on page 13-8 for more information.

Usage Notes

- Emails are sent using the SMTP server address configured for the Operations Manager server using the Cisco VSM Management Console. The SMTP server settings must be accurate or the emails will not be sent (no error or warning is given). See the [“SMTP Management Settings”](#) section on page 6-24 for more information. To apply the settings to multiple servers, see the [“Bulk Actions: Revising Multiple Servers”](#) section on page 6-19.
- Health Notifications are created for a location. If a critical device health error occurs for any device at that location (or sub-location), an email is sent to the specified recipients).
- Email recipients can be specified for different locations (and sub-locations) by creating a new Health Notification rule. Health Notifications operate independently so the recipient will receive emails for each rule, even if the notifications are for the same issue.
- Use the settings described in [Table 13-6](#) to avoid unnecessary and excessive email traffic.

Table 13-6 **Health Notifications**

Setting	Description
Initial time	The time between the first alert and the email being sent. This avoids emails for temporary issues that cause a device to briefly go offline and come back online. For example, when a camera configuration is revised, the camera may go down briefly while being reset. <ul style="list-style-type: none">• Default—1 minute• Range—1 to 10 minutes
Wait time	The time between the first email and any subsequent email. This prevents multiple emails being sent for the same issue within a short period of time. <ul style="list-style-type: none">• Default—12 hours• Range—1 to 48 hours

Procedure**Step 1**


Verify that the SMTP server settings are configured correctly for each Media Server.

- See the [“SMTP Management Settings”](#) section on page 6-24 for more information.

- To update SMTP server settings for multiple Media Servers, see the [“Bulk Actions: Revising Multiple Servers” section on page 6-19](#).

Step 2 Select **Operations > Health Notifications**.

Step 3 Click **Add**.


Step 4 Click the **Location** icon  to select the location.

All devices from this location and sub-locations will generate a health notification.



Tip

Select the root location (for example, “System”) to include all devices from all locations. If additional rules are added for sub-locations, both rules will apply and multiple emails will be generated.

Step 5 Enter a valid email address and click the **Add Email** icon  (or press **Enter**).

Step 6 Add additional email addresses, if necessary.

Step 7 Select the **Initial Time** and **Wait Time** as described in [Table 13-6](#).

Step 8 Click **Add**.

Step 9 Create additional entries for additional locations and recipients, if necessary.

Reports

Use *Reports* to generate and download summary information about the Cisco Video Surveillance user activity, device configuration. For example, you can create Audit reports that summarize user actions, or Camera and Media Server reports that summarize device configuration and status.

- [Create a Report, page 13-16](#)
- [Delete a Report, page 13-16](#)


Create a Report

Procedure

-
- Step 1** Select **Operations > Reports**.
- Step 2** Create one or more reports.
- Click **Add**.
 - Select the **General** settings and click **Next**.
 - Report Type—The device or user information to be included in the report. For example, Audit, **Camera**, or Media Server.
 - Report Format—The file format for the downloadable report. For example, a **CSV Format** (*comma-separated value*) file.
 - Select the report **Filters** and click **Next**.
For example, you can include cameras based on the camera name, make/model, the Media Server associated with the camera, template assigned to the camera(s), etc.
 - Use the **Preview** window to select or deselect the devices or users to be included in the report.
 - Click **Finish**.
 - Wait for the report to be generated, and then click **Close**.
- Step 3** Select one or more reports from the list and click **Download**.
-

Delete a Report

Procedure

-
- Step 1** Select **Operations > Reports**.
- Step 2** Select the check-box for one or more existing reports.
-  **Tip** Click the select all box to remove all reports.
-
- Step 3** Click **Download** and confirm the deletion.
-

Synchronizing Device Configurations

Device synchronization ensures that the device configuration on the Media Server, camera or encoder is identical to the Operations Manager settings. Synchronization also ensures that no device has the same unique ID (such as a MAC address) as another device. Synchronization is automatically performed when certain events occur, such as when a Media Server goes offline and comes back online, when the Operations Manager is restarted, when drivers are upgraded, and other events.

Synchronization errors can be resolved either automatically, or manually. Refer to the following topics for more information:

- [Overview, page 13-17](#)
- [Viewing Device Synchronization Errors, page 13-19](#)
- [Understanding Device Configuration Mismatch Caused by Media Server Issues, page 13-20](#)
- [Repairing a Mismatched Configuration, page 13-21](#)
- [Manually Triggering a Media Server Synchronization, page 13-22](#)
- [Device Data That Is Synchronized, page 13-22](#)
- [Synchronization During a Media Server Migration, page 13-23](#)

Overview

The Operations Manager configuration is the master configuration([Figure 13-8](#)). A mismatch occurs if the configuration on the Media Server is different.

For example, if a synchronization event determines that the setting for a camera's video resolution is different between the Operations Manager and the Media Server, a configuration mismatch occurs.


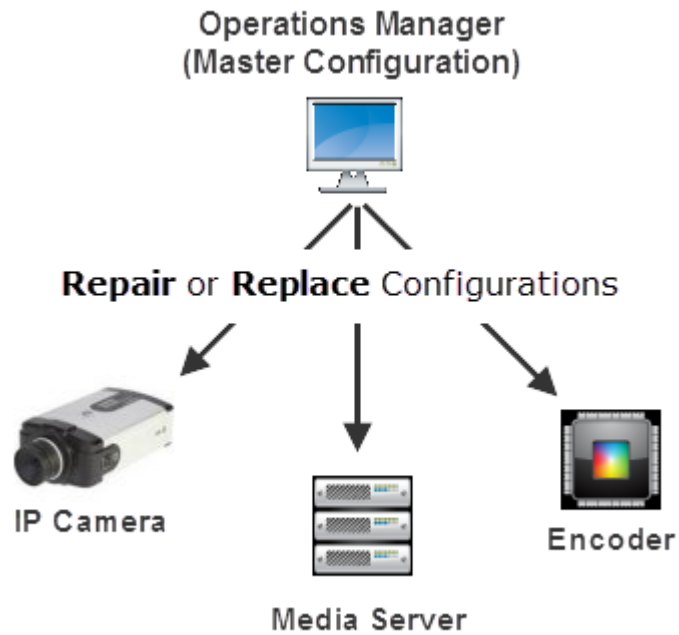
- If the *Autocorrect Synchronization Errors* system setting is enabled, the configuration is automatically replaced with the Operations Manager setting.
- If the *Autocorrect Synchronization Errors* system setting is disabled, a configuration error is displayed on the camera Status page. Click the  icon to view additional details about the mismatch and then select **Repair Configurations** or **Replace Configurations** from the **Device Settings** menu to replace the camera setting with the Operations Manager setting. See the following for more information:
 - [Device Status: Identifying Issues for a Specific Device, page 13-8](#)
 - [Synchronizing Device Configurations, page 13-17](#)


Figure 13-8 *Device Synchronization*



Viewing Device Synchronization Errors

A configuration error appears on the device Status page if a synchronization error is not automatically corrected. To view details about the error, open the device *Status* page.

Procedure

- Step 1** Open the device configuration page:
- Click **Cameras** and select a camera or encoder
 - or
 - Click **System Settings > Media Server** and select a Media Server.
- Step 2** Click the device **Status** tab.
- Step 3** Click the  icon next to *Configuration* (Figure 13-9).




Note The  icon appears only if a configuration error occurred.

Figure 13-9 Camera Configuration Mismatch

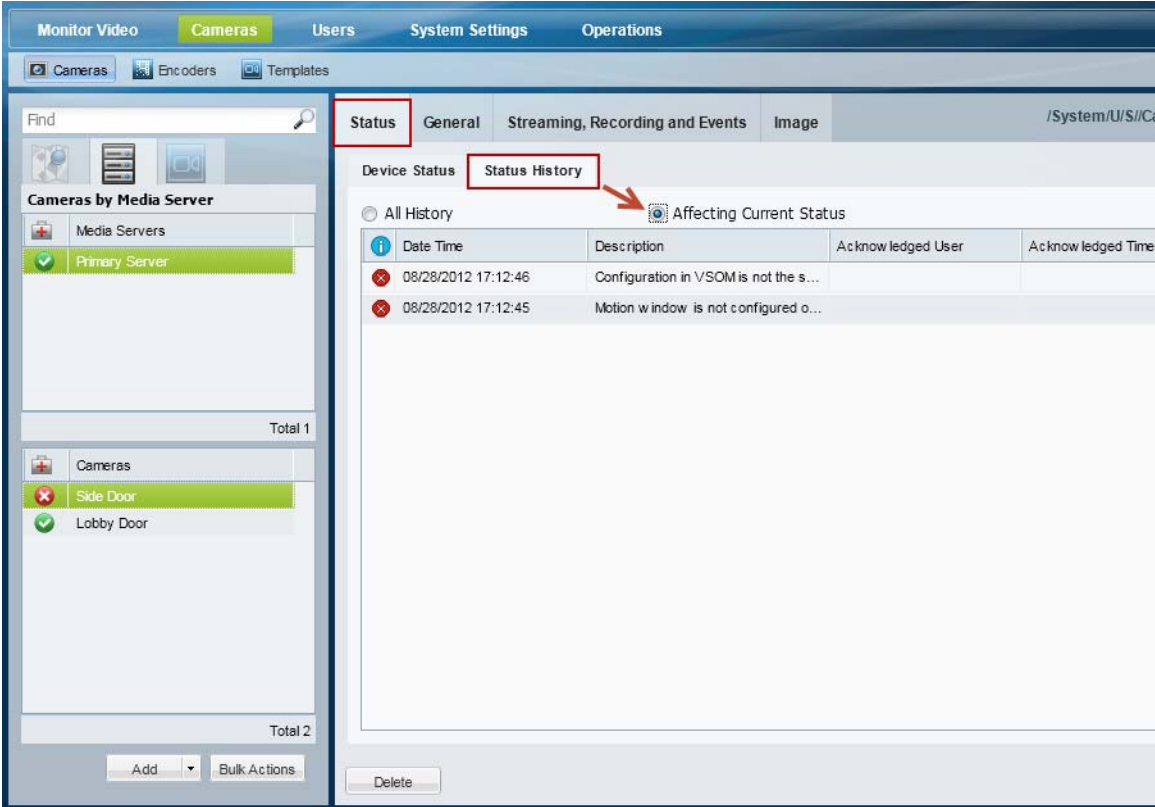
The screenshot displays the Cisco Video Surveillance Operations Manager interface. The left sidebar shows a tree view with 'Cameras by Media Server' and 'Cameras'. The 'Cameras' section is expanded, showing 'Side Door' and 'Lobby Door'. The 'Side Door' camera is selected, and its 'Status' tab is active. The 'Status' page shows the 'Overall Status' as 'Enabled: Critical' with a red 'X' icon. The 'Camera Status' section lists 'Reachability', 'Streaming', 'Recording', and 'Configuration'. The 'Configuration' item is highlighted with a red box and a red arrow pointing to a 'Configuration Mismatch' dialog box. The 'Configuration Mismatch' dialog box shows a table with the following data:

Property	Configured Value	Primary MS Value	Follower MS Value	Redundant MS Value
DeviceConfiguration	Device present	Device not present		

The 'Configuration Mismatch' dialog box also has a 'Close' button. The 'General Information' section shows 'Jobs in Progress' as 'No'.

- Step 4** (Optional) Close the window and click **Status History** to view more information regarding the synchronization events (Figure 13-10).

Figure 13-10 Camera Status History



Tip Click **Affecting Current Status** to narrow the results.

- Step 5** To resolve the configuration mismatch, do one of the following:
- (Recommended) Continue to the [“Repairing a Mismatched Configuration” section on page 13-21](#).
 - Manually resolve the configuration issue on the device, or in the Operations Manager configuration.

Understanding Device Configuration Mismatch Caused by Media Server Issues

When a Media Server issue is discovered that can impact a camera or encoder, a configuration mismatch occurs for the camera or encoder device. This allows the device configuration to be synchronized with the Media Server after the issue is resolved on the Media Server.

To resolve this mismatch, address the issue on the Media Server, and continue to the [“Repairing a Mismatched Configuration” section on page 13-21](#).

A device configuration mismatch can be caused by the following Media Server issues:

- driverpack-mismatch

- reachability
- software-mismatch
- server-pool-config-mismatch
- ntp-config-mismatch
- identity-mismatch
- schedule-config-mismatch

Repairing a Mismatched Configuration

Select **Repair Configurations** or **Replace Configurations** from the **Device Settings** menu (in a device configuration page) to manually replace the device configuration with the Operations Manager settings.

**Note**

Devices include the Media Servers, encoders and cameras.

Procedure

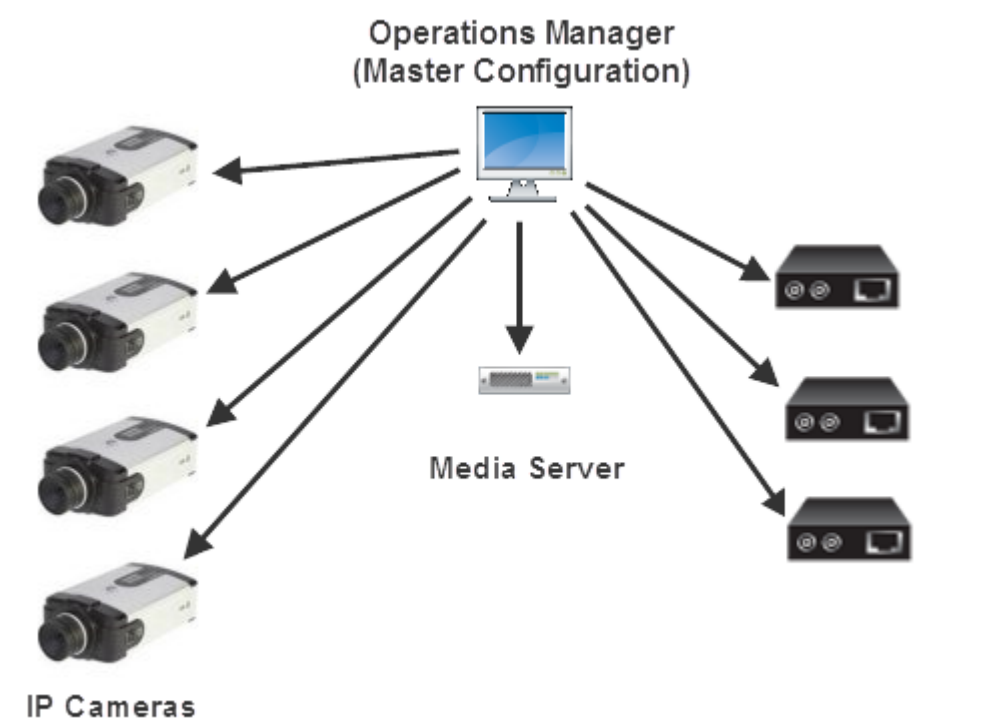
-
- Step 1** (Optional) Review the configuration mismatch errors, as described in the [“Viewing Device Synchronization Errors”](#) section on page 13-19.
- Step 2** Select the device configuration **General** tab.
- Step 3** Click one of the following options.
- **Replace Configurations**—Pushes the entire device configuration from the Operations Manager to the Media Server. The Media Server data is replaced.
 - **Repair Configurations**—Pushes only the configuration changes required correct a mismatched field. Changes are pushed from the Operations Manager to the Media Server.
- Step 4** (Optional) Complete the following optional troubleshooting steps:
- Wait for the synchronization *Job* to complete. In the Job window, click **View Status** to view any failed steps and click the error message to view additional information. See the [“Understanding Jobs and Job Status”](#) section on page 13-25 for more information.
 - Open the **Status** page for the affected device to view additional details and take corrective action, if necessary. See the [“Viewing Device Synchronization Errors”](#) section on page 13-19.
-

Manually Triggering a Media Server Synchronization

The Media Server configuration is automatically synchronized when certain events occur (such as when the Media Server offline and comes back online).

If synchronization errors are found, select the **Repair Configurations** or **Replace Configurations** options from the **Device Settings** menu to replace the Media Server settings with the Operations Manager settings (Figure 13-11).

Figure 13-11 Repairing Configuration Mismatches using Advanced Troubleshooting



Device Data That Is Synchronized

Table 13-7 describes the data synchronized between the Operations Manager and devices (Media Server, cameras, and encoders).

Table 13-7 Synchronized Device Data

Device Data Type	Master Configuration Source	Description
Configuration	Operations Manager	The device template, name, IP address, and other settings.
User-provided administrative information	Operations Manager	The device status (enabled, disabled, or pre-provisioned).

Table 13-7 *Synchronized Device Data (continued)*

Device Data Type	Master Configuration Source	Description
System-derived operational states	Media Server	<p>For example:</p> <ul style="list-style-type: none"> the device is reachable or unreachable there is a mismatch between devices the last operation status the device health other status information
Device exists in the Operations Manager but not in the Media Server	Operations Manager	<p>The device configuration is pushed to the Media Server.</p> <p>See the “Cameras Pending Approval List” section on page 8-30 for more information.</p>
Device exists in the Media Server but not in the Operations Manager	Media Server	<p>IP/Analog cameras are added in pre-provisioned state with a basic configuration.</p> <p>Encoders are added as enabled.</p> <p>You must add additional settings such as camera template, location and others settings then enable the device.</p> <p>See the “Adding Cameras from an Existing Media Server” section on page 8-38 and the “Cameras Pending Approval List” section on page 8-30 for instructions to approve the device.</p> <p>Note The device can also be placed in the blacklist or deleted.</p>

Synchronization During a Media Server Migration

When an existing Media Server is migrated from an existing Cisco VSM 6.x or 7.x deployment, you have the option of keeping or deleting any configured cameras or encoders and their associated recordings.

For more information, see the [“Adding Cameras from an Existing Media Server”](#) section on page 8-38.

Viewing the Server Management Console Status and Logs

The Cisco Video Surveillance Management Console is a browser-based interface that provides additional monitoring and troubleshooting features for the physical server that runs both the Operations Manager and Media Server.

To access the Management Console, click **System Settings > Management Console**.

See the [Cisco Video Surveillance Management Console Administration Guide](#) for more information.

Understanding Jobs and Job Status

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

A pop-up window appears when a Job is triggered, allowing you to view additional details about the Job, if necessary. You can also use the Jobs page to view a summary and additional details of all Jobs in the system.

**Note**

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

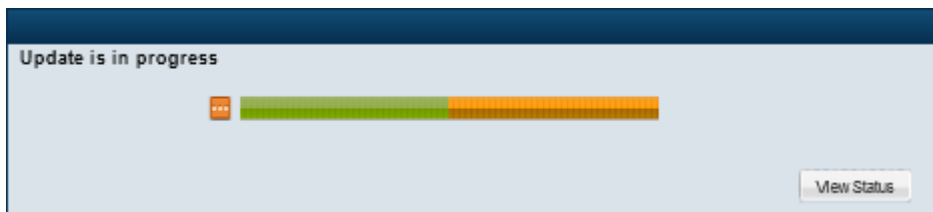
Refer to the following topics for more information:

- [Viewing Job Status and Details, page 13-25](#)
- [Understanding Job Status, page 13-27](#)
- [Viewing All Jobs in the System, page 13-28](#)
- [Viewing Audit Logs, page 13-31](#)

Viewing Job Status and Details

A job status dialog appears when a user action triggers a job ([Figure 13-12](#)).

Figure 13-12 Job Status Bar

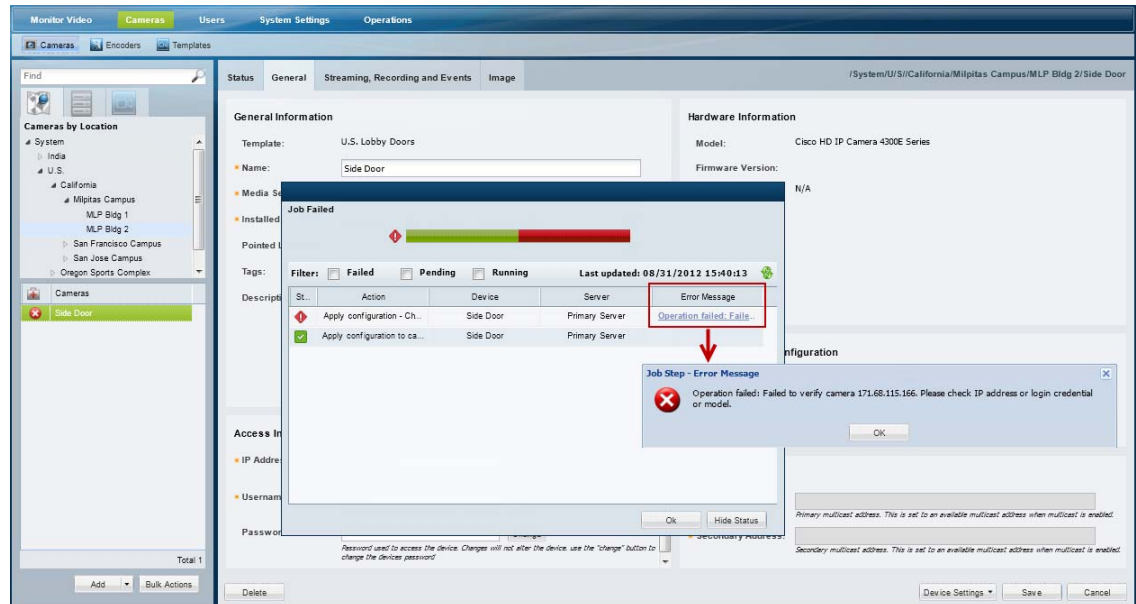


The window automatically closes when the job completes successfully.


See the [“Understanding Job Status” section on page 13-27](#) for a description of the status bar colors and states.

- Click **View Status** to view additional details ([Figure 13-13](#)).
- Navigate to a different menu. If the Job is in-progress, you can navigate to other Operations Manager menus and features while the Job continues to process in the background. If you return to the screen where the Job was performed, the Job status bar will reappear if the Job has not been completed.
- To view all Jobs in the system, open the Jobs window (see the [“Viewing All Jobs in the System” section on page 13-28](#)). The Jobs window displays Jobs initiated by the current user. Super-Admins can also view Jobs initiated by other users.

Figure 13-13 “View Status” Details






You can take one of the following actions from the Job Details dialog:

- Click refresh  to renew the display.
- Click an *Error Message* (failed job steps only) to view additional information regarding the error.
- Click **Stop** (pending job steps only) to cancel steps that have not begun (see the “[Understanding Job Status](#)” section on page 13-27 for more information).

If a Job is stopped, any completed or failed Job Steps remain completed or failed (the action is not undone). Only the pending Job Steps are cancelled. In addition, any Job Step are already running will continue until it completes or fails.



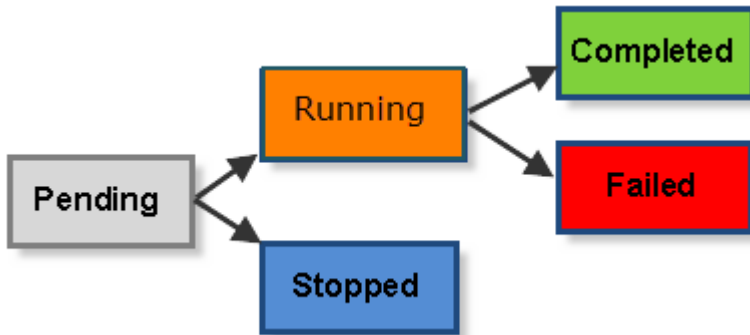
Tip

- If a user has at least one management permission, the Jobs status icons    appear at the top of the page if there is at least one Job pending or running. Click the icons to open the Jobs page.
- A second user cannot edit a resource (such as a camera or Media Server) if that resource has a pending Job. If the second user logs in and accesses the resource, the *Job loading* message is displayed and prevents the user from editing or viewing the resource.

Understanding Job Status

Each Job and Job Step has a status as shown in [Figure 13-14](#).

Figure 13-14 Job Status



Status	Color	Description
Pending	Gray	A Job or Job Step that has not begun to process. Only Pending Jobs or Job Steps can be stopped.
Running	Orange	The Job or Job Step has begun to process. The action cannot be stopped and will continue until it either succeeds or fails.
Stopped	Blue	A pending Job or Job Step that was stopped by the user.
Completed	Green	A Job or Job Step that was successfully completed.
Failed	Red	A Job or Job Step that failed to complete. Click the <i>Error Message</i> for more information regarding.

Viewing All Jobs in the System

Click **System Settings > Jobs** (Figure 13-15) to view a summary of recent Jobs, filter and sort the Job entries, and view detailed Job Steps and error messages.

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










Tip

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

Figure 13-15 Jobs

	Feature	Description
1	Filter	Select a filter to limit the Job types displayed. For example, click Failed to display only failed Jobs. Note Click My Jobs to view only the Jobs you initiated. This option is only available to super-admin. Most users can only view their own Jobs by default.

2	Job events	<p>Lists the Jobs in the system. Use the filter to narrow the Jobs displayed, or click the column headings to sort the information.</p> <p>Note The Job list automatically refreshes to display up-to date status information.</p> <p>Each Job includes the following information:</p> <ul style="list-style-type: none"> • Start Time—The date and time when the Job was initiated by the user. • End Time—The date and time when the Job ended. A Job can end when it is completed or fails. Jobs with at least one pending Job Step can be stopped (click the Stop button). See the “Understanding Job Status” section on page 13-27 for more information. • Status—Indicates the Job status. Refer to the <i>legend</i> for a description of each color. See the “Understanding Job Status” section on page 13-27. • Steps—The number of <i>Job Steps</i> required to complete the Job. Click the number to display the step details in the bottom pane. • Failed—The number of Failed <i>Job Steps</i>. Click the number to display only the failed Job Steps in the bottom pane. • Action—The action or system change performed by the Job. • Resources Affected—The resources affected by the Job. For example, name of the Media Server or the template that is modified by the Job. • User—The user who triggered the Job.
4	Job Steps	Lists the sub-steps performed for a Job (click the <i>Steps</i> number to display Job details).
5	Job Steps filter	Select a filter to limit the steps displayed. For example, click Running to display only Job Steps that are still in progress.
6	Job Steps detail	<p>Lists each sub-step that is performed for the selected Job. Click the number under the Step or Failed column to display the steps for a Job.</p> <p>Note The Job Step list does not automatically refresh. Click the refresh icon  to renew the display and view up-to-date information.</p> <p>Use the filter to narrow the Jobs steps displayed, or click the column headings to sort the information. Each Job Step includes the following information:</p> <ul style="list-style-type: none"> • Start Time—The date and time when the step began to process. • End Time—The date and time when the step ended. A step can end when it is completed or fails. • Status—Indicates the Job Step status. Refer to the <i>legend</i> for a description of each color. See the “Understanding Job Status” section on page 13-27. • Action—The action or system change performed by the Job Step. • Device—The resources affected by the Job Step. For example, a camera. • Server—The server affected by the Job Step.
7	Error Message	Click the error message (if available) to open a pop-up window with additional details.
8	Refresh icon	Click the refresh icon  to renew the display and view up-to-date Job Step status. The Last Update field shows when the information was last updated.

9	Legend	<p>Describes the meaning of each <i>status</i> color. For example, a green Job <i>status</i> bar means the Job was successfully completed.</p> <p>Legend:  Completed  Failed  Pending  Running  Stopped</p> <p>See the “Understanding Job Status” section on page 13-27 for more information.</p>
---	--------	--

Viewing Audit Logs

Audit Logs display a history of user configuration actions in the Cisco Video Surveillance deployment. The most common operations are the creation or revision of resources (such as cameras and users), but the Audit Logs also record numerous other activities.

Beginning with release 7.2, the Operations Manager will store up to 1 million audit log entries.



Note

Users must belong to a User Group with *super-admin* permissions to access the Audit Logs (the user must be added to a user group that is associated with the *super-admin* role). See the [Adding Users, User Groups, and Permissions](#), page 4-1.

To access the Audit Logs, click **Operations** and then **Audit Logs** (Figure 13-16).

Figure 13-16 Audit Logs Detail Window

The screenshot displays the 'Audit Logs (200 records)' window. The table lists various activities such as 'ADD_DEVICE_TO_UMS', 'CREATE_DEVICE', 'DELETE_DEVICE', 'ADD_DEVICE_TO_DEVICE...', 'ENABLE_DEVICE', and 'UPDATE_DEVICE'. A red arrow points to the 'Change Details' link for the entry dated 09/13/2012 21:28:51. The 'Change Details' modal window shows the following properties and values:

Property Name	New Value
Device.vendor	Cisco Systems, Inc.
Device.adminState	pre_provisioned
Device.videoController.portid	4
Device.mtpEnabled	false
Device.objectType	device_vs_camera_analog
Device.model	generic_analog

Take one or more of the following actions

- Use the *Search By* fields to filter the items displayed in the list.

You can narrow the results by Time Range, Activity Type, Object Type, Object Name (enabled only when an Object type is selected), Object Location, User Name and/or User IP address.

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

- Click the **Change Details** link (if available) to view additional information about the event (see the example in Figure 13-16).
- Click the **Job Reference** link (if available) to view the related Jobs summary.
See the “[Understanding Jobs and Job Status](#)” section on page 13-25 for more information.
- Click the column headings to sort the list.



CHAPTER 14

Revising the System Settings

Choose **System Settings** > **Settings** to define basic parameters.



Tip

The default settings are sufficient for a basic setup, but you should review and revise the settings to meet the needs of your deployment. System setting can only be modified by *super-admin* users.

- [General System Settings, page 14-1](#)
- [Password Settings, page 14-2](#)



Note

Beginning with release 7.2, retention of alerts, events and audit log entries is now managed automatically by the Operations Manager, which can store up to 1 million alerts, 1 million events, and 1 million audit log entries.

General System Settings

The General settings define user sessions, backup storage rules, and other settings.

Table 14-1 **General Settings**

Setting	Description
User Timeout	(Required) The number of minutes before a user is automatically logged out due to inactivity. After this period, users must reenter their username and password to log back in. Note The maximum value is 10080 minutes (168 hours / 7 days).
Record Now Duration	(Required) Enter the number of seconds that video will be recorded for all Record Now requests. The minimum value (and default) is 300 seconds (5 minutes). See the following for more information: <ul style="list-style-type: none">• Enabling Record Now, page 3-12• Using Record Now, page 2-24

Table 14-1 **General Settings (continued)**

Setting	Description
Autocorrect Synchronization Errors	<p>Device synchronization ensures that the device configuration on the Media Server, camera or encoder is identical to the Operations Manager settings. Synchronization is automatically performed when certain events occur, such as when a Media Server goes offline and comes back online.</p> <p>Select <i>Autocorrect Synchronization Errors</i> to automatically correct any configuration mismatches that are discovered during a synchronization. If this option is disabled, the configuration mismatch is not corrected and the device Configuration status displays a <i>Critical</i> state. You can then manually correct the error by clicking either the Repair or Replace Config button in the device configuration page.</p> <p>See the “Synchronizing Device Configurations” section on page 13-17.</p>
Medianet discovery enabled	Allows Medianet-enabled cameras to be automatically discovered by Cisco VSM Operations Manager when the cameras are added to the network. See the “ Discovering Medianet-Enabled Cameras ” section on page 8-32
Low QOS	The QoS value used for video between Media Server and client.
Medium QOS	
High QOS	

Password Settings

The password settings define the rules for user passwords.

Table 14-2 **Password Settings**

Setting	Description
Password Expiry Months	The number of months before a user password automatically expires. At the end of this period, users are required to enter a new password.
Minimum Password Length	<p>Enter a value between 1 and 40 to define the minimum number of characters for a valid password. Passwords with less characters than the entered value are rejected.</p> <p>The default is 8 characters.</p>
Maximum Password Length	<p>Enter a value between 40 and 80 to define the maximum number of characters for a valid password. Passwords with more characters than the entered value are rejected.</p> <p>The default is 40 characters.</p>
Identical Password/Username Allowed	<p>If selected, user passwords can be the same as their username.</p> <p>If de-selected, user passwords must be different than their username.</p>

Table 14-2 Password Settings (continued)

Setting	Description
3 Password Groups Required	<p>If selected, user passwords must include characters from at least three different types of characters, including:</p> <ul style="list-style-type: none">• lower case letters• upper case letters• symbols• numbers <p>If de-selected, user passwords can include only one type of character (for example, all lower case letters).</p>
Repeat Characters	<p>If selected, user passwords can repeat the same 3 characters.</p> <p>If de-selected, user passwords can <i>not</i> repeat the same 3 characters.</p>



CHAPTER 15

Software Downloads and Updates

Refer to the following topics to download additional software tools and updates.

- [Downloading Cisco SASD and the Cisco Review Player, page 15-1](#)
- [Downloading the Workstation Profiler Tool, page 15-2](#)
- [Downloading Software, Firmware and Driver Packs from cisco.com, page 15-2](#)
- [Accessing the Management Console, page 15-2](#)
- [Downloading Documentation, page 15-2](#)
- [Upgrading Cisco Camera and Encoder Firmware, page 15-3](#)
- [Installing and Upgrading Driver Packs, page 15-8](#)

Downloading Cisco SASD and the Cisco Review Player

The following tools can also be used to monitor video.

Table 15-1 Cisco Video Viewing Applications for Download from the Operations Manager

Application	Description	Documentation
Cisco Video Surveillance Safety and Security Desktop (Cisco SASD)	Desktop monitoring application that provides greater flexibility to monitor multiple cameras, view and respond to alerts, and create unattended monitoring stations.	Cisco Video Surveillance Safety and Security Desktop User Guide
Cisco Video Surveillance Review Player (Cisco Review Player)	Simple player used to view video clip files.	Cisco Video Surveillance Review Player

Go to **Operations > Software** to download these applications. When the download is complete, double-click the installation file and follow the on-screen instructions.



Tip

See the [“Understanding the Video Viewing Options” section on page 2-2](#) for more information.

Downloading the Workstation Profiler Tool

The Profiler Tool is used to analyze the ability of a monitoring PC client to render video. See [Using the Cisco Video Surveillance Monitoring Workstation Profiler Tool](#) for instructions to download, install, and use this tool.

Downloading Software, Firmware and Driver Packs from cisco.com

To download additional system, firmware and driver software can be downloaded from cisco.com, go to the following location.

Procedure

-
- Step 1** Go to the following URL.
<http://www.cisco.com/go/physicalsecurity>
- Step 2** Click **View All Products**.
- Step 3** Click the appropriate category (such as the Cisco IP Camera model).
- Step 4** Click **Download Software** and follow the on-screen instructions.



Tip

You can also navigate to the [Cisco Video Surveillance Manager download page](#) (at <http://software.cisco.com/download/type.html?mdfid=282976740&flowid=35342>) and select an option for **Video Surveillance Device Driver Software** or **Video Surveillance Media Server Software**.

Accessing the Management Console

The browser-based Cisco Video Surveillance Management Console is used to configure and monitor the server that runs the Cisco VSM services, such as the Operations Manager and Media Server.

Select to **Operations > Management Console** to open a new browser tab with the Management Console, or enter **http://<server-ip-address or hostname>/vsmc/**.

See the [Cisco Video Surveillance Management Console Administration Guide](#) for more information.



Note

The Management Console requires a separate password.

Downloading Documentation

Go to **Operations > Help** to download to download Cisco Video Surveillance documentation. See the [“Related Documentation” section on page A-1](#) regarding additional documentation available on cisco.com.

Upgrading Cisco Camera and Encoder Firmware

Firmware for Cisco cameras and encoders can be upgraded using the Operations Manager as described in the following procedure. You can upgrade a single device, or multiple devices at a time.

Refer to the following topics for more information:

- [Firmware Management Overview, page 15-3](#)
- [Usage Notes, page 15-4](#)
- [Before You Begin, page 15-4](#)
- [Firmware Management Procedure, page 15-4](#)



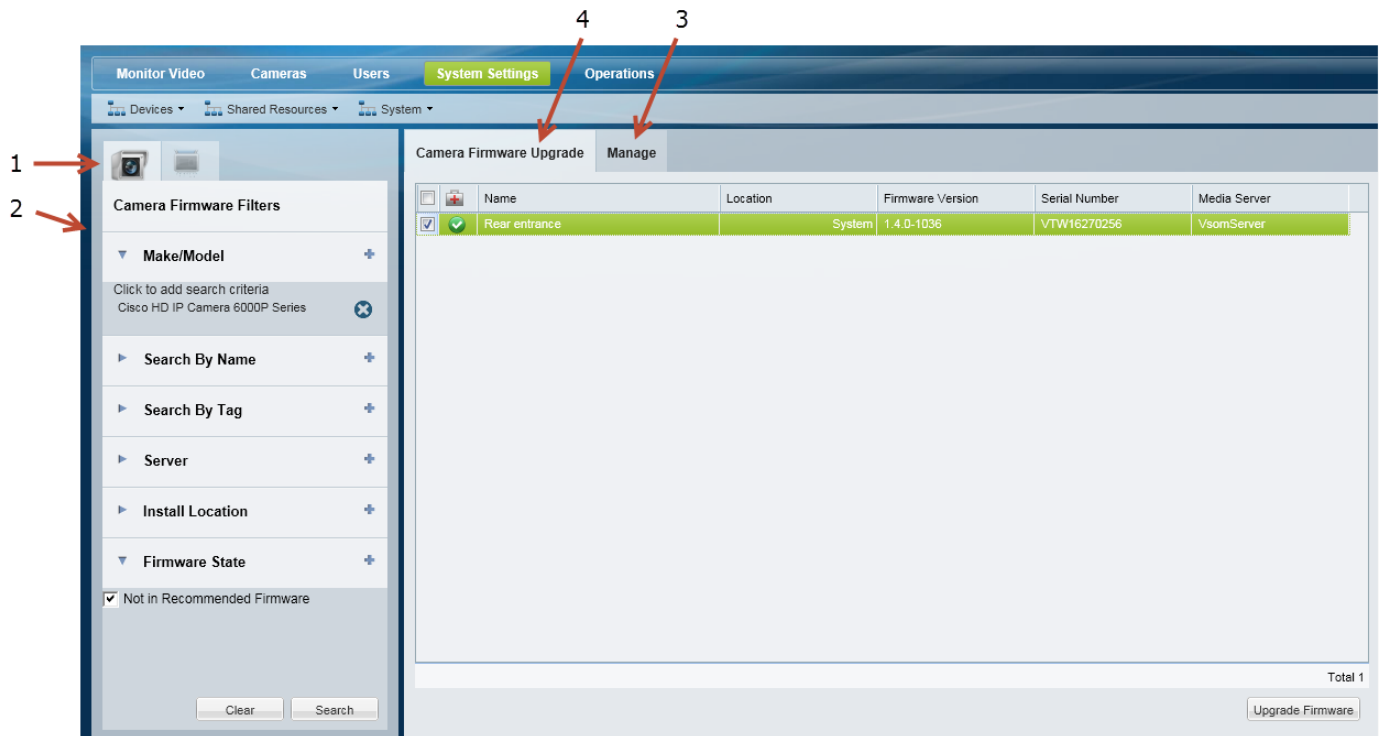
Note

Firmware for non-Cisco cameras is upgraded using a direct connection and the device user interface. See the device documentation to upgrade or downgrade the device firmware directly on the device.

Firmware Management Overview

Figure 15-2 describes the main elements used to manage firmware. See the “[Firmware Management Procedure](#)” section on page 15-4 for more information.

Figure 15-1 Firmware Management



1 Camera and Encoder tabs—Click to select the device type you want to manage.

2	Device filters—Select a Make/Model to enable the other filter fields and manage the device firmware.
3	Manage—Used to upload firmware images to the server, which can then be installed on the camera or encoder.
4	Firmware Upgrade—Used to upgrade specific devices that were discovered using the filter search.

**Tip**

See the “[Understanding Cisco Video Surveillance Software](#)” section on page 1-21 for information about firmware, driver packs and system software.

Usage Notes

- Upgrade firmware for non-Cisco devices using a direct connection. See device documentation for more information.
- The Cisco devices must be available on the network and enabled in Cisco VSM. If the device is not available to Cisco VSM, connect directly to the device to upgrade the drivers using a direct connection (see the device documentation for instructions).
- The firmware image file must be a valid file format. Because the file format is different for each camera vendor, the Operations Manager will initially accept any file format, even if invalid. However, invalid files will cause the upgrade or downgrade to fail after 2-3 minutes.
- The upgrade can fail if device configuration changes are in process when the upgrade begins. If a device configuration is started during the upgrade, then the configuration change can fail. To avoid this, verify that no device configuration changes are running or started during the firmware upgrade (open the device **Status** page; the *Jobs in Progress* field should be *No*).
- The firmware version column in the *Manage* tab is only shown after the firmware has been applied to a set of devices.
- Each Media Server can update five devices at a time.
- Only one upgrade can be executed at a time. Wait until all devices are upgraded before initiating a new request.
- The vendor and device list includes the models that support firmware upgrades using the Operations Manager.
- To downgrade device firmware, select a previous version (the device must support downgrades).

Before You Begin

Before you begin, obtain the driver firmware for your device(s).

- To obtain firmware for Cisco devices, see the [Downloading Software, Firmware and Driver Packs from cisco.com, page 15-2](#).
- To obtain firmware for non-Cisco products, go to the product website or contact your sales representative.
- Verify that the firmware version is supported in Cisco Video Surveillance Manager, Release 7.2. See the [Release Notes for Cisco Video Surveillance Manager, Release 7.2](#).

Firmware Management Procedure

Step 1 Download the firmware image from the Cisco website or device manufacturer.



See the following for more information:

- [Downloading Software, Firmware and Driver Packs from cisco.com, page 15-2](#).

- [Release Notes for Cisco Video Surveillance Manager](#)

Step 2 Choose **System Settings > Firmware Management**.

- You must belong to a User Group with manage permissions for *Cameras* and *Images*.
 - See the [“Adding Users, User Groups, and Permissions”](#) section on page 4-1.
 - Specifically, see the [“Understanding Permissions”](#) section on page 4-4.

Step 3 Select the camera  or encoder  tab ([Figure 15-1 on page 15-3](#)).

Step 4 Select a Make/Model from the Filters to enable the other fields and the **Search** button ([Figure 15-1](#)).

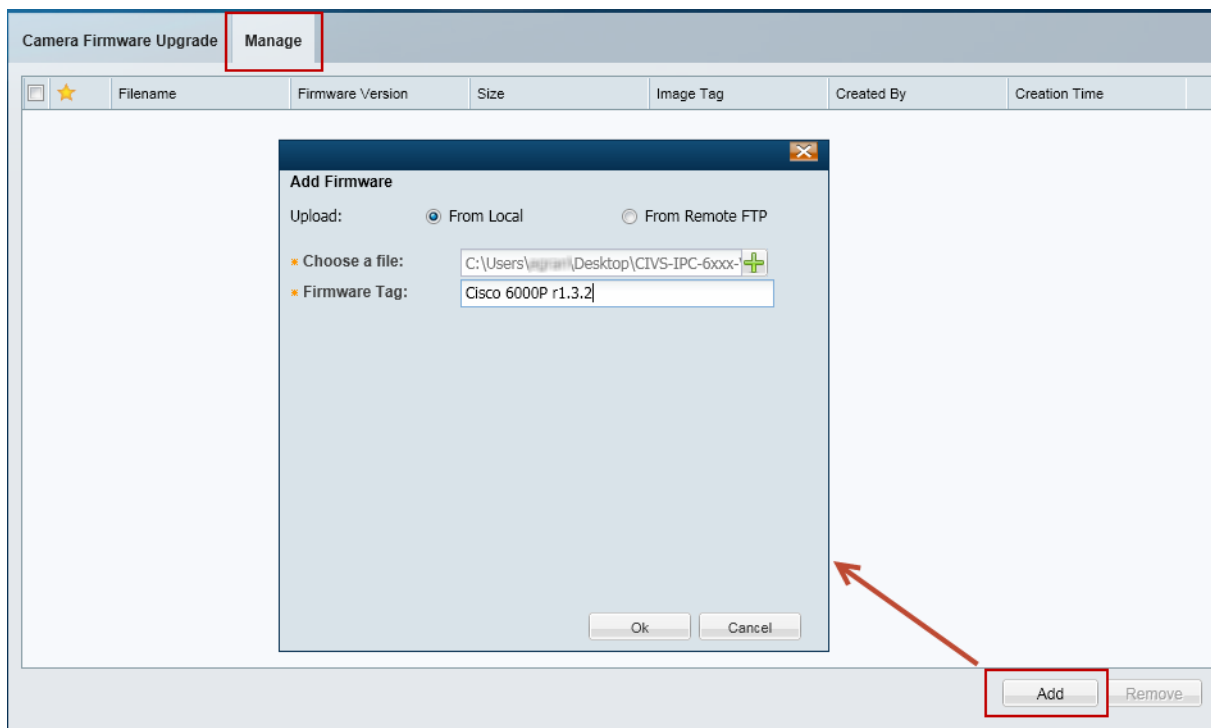
- Expand the **Make/Model**.
- Click the entry field.
- Select the camera model from the pop-up list.
- Select additional filter criteria, if necessary.
- Click **Search**.

Step 5 (Optional) Add additional filter criteria to refine the search.

You can also click the **Make/Model** field again to add additional device models.

Step 6 Add the firmware images ([Figure 15-2](#)):

Figure 15-2 Adding Firmware Images



- Select the **Manage** tab.
- Click **Add** to upload a new firmware image to the Operations Manager server.
- Select **From Local** or **From Remote FTP**.
- Select the location of the firmware file, or enter the FTP connection details.

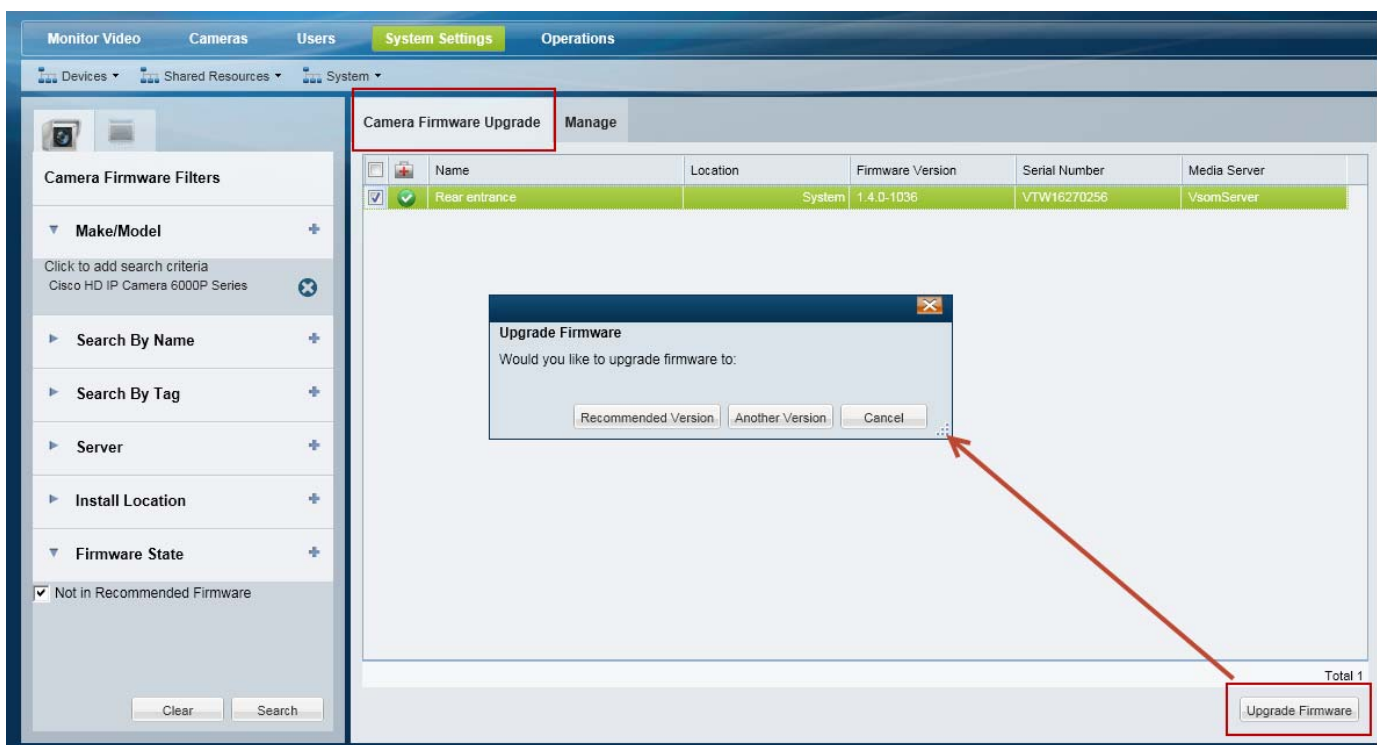
- c. Enter a firmware tag that includes the firmware device model.
- d. Click **OK**.
- e. Wait for the file to upload and click **OK** again.
- f. Select the star ★ next to a firmware image to indicate the recommended version for the device model. This image will be used in the upgrade/downgrade.

**Note**

The Firmware version column is only displayed after the firmware has been applied to a set of devices.

Step 7 Upgrade the device firmware (Figure 15-3):

Figure 15-3 Upgrading Firmware

**Note**

The firmware image file must be a valid file format for the camera model (for example: CIVS-IPC-6xxx-V1.3.2-8.bin). Although the Operations Manager will initially accept an invalid file format, the upgrade or downgrade will fail after 2-3 minutes.

**Tip**

Select the filter **Firmware State > Not in Recommended Firmware** to view only the devices that do not have the recommended firmware version (as defined by the star ★ in Step 6).

**Tip**

You can also downgrade devices by selecting a previous version, if the device supports downgrades.

- a. Select the **Camera Firmware Upgrade** or **Encoder Firmware Upgrade** tab (depending on the device type search).
- b. Select the devices to be upgraded.
- c. Click **Upgrade Firmware**.
- d. Click **Recommended Version** or **Another Version**.
 - **Recommended Version**—upgrade using the firmware version defined by the star ★ in [Step 6](#). If no version was selected, then you must select a firmware version for the upgrade.
 - **Another Version**—select the firmware version for the upgrade.

Step 8 Wait for the upgrade to complete. See the [“Usage Notes” section on page 15-4](#) if the upgrade is not successful.

Installing and Upgrading Driver Packs

Device *driver packs* are the software packages used by Media Servers and the Operations Manager to interoperate with video devices. Driver packs are included with the Cisco VSM software, or may be added to a server to support new devices.

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

Refer to the following topics for more information:

- [Usage Notes, page 15-8](#)
- [Overview, page 15-9](#)
- [Upgrade Procedure, page 15-9](#)

**Tip**

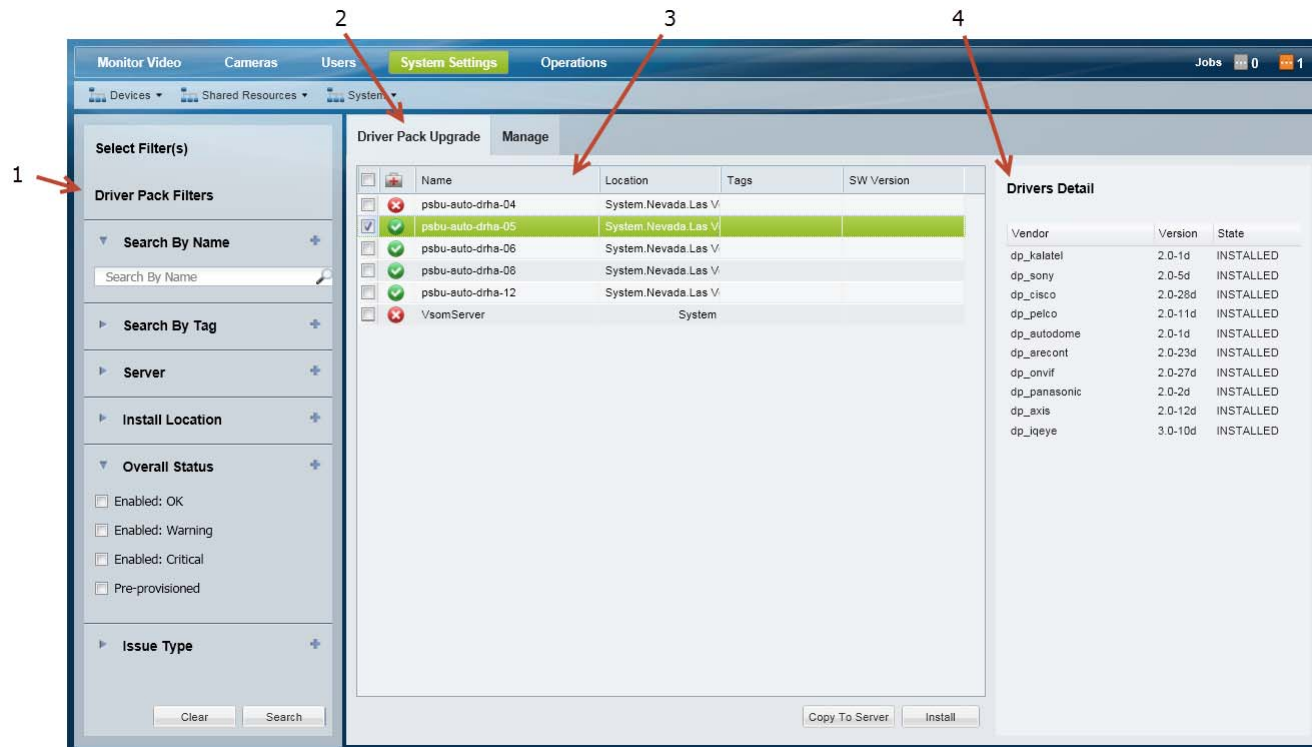
See the “[Understanding Cisco Video Surveillance Software](#)” section on page 1-21 for descriptions of the different software types.

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.
- The driver pack file format is *.zip*. For example: `dp_cisco-2.0-28d_7.2.0-12d_sles10-sp1.zip`
- See the [Release Notes for Cisco Video Surveillance Manager, Release 7.2](#) for information on the supported driver packs.
- Driver packs can only be upgraded. They cannot be downgraded.

Overview

Figure 15-4 Manage Drivers



1	Filters used to narrow the displayed servers. Select the filters and click Search . Leave all fields blank to find all servers.
2	<ul style="list-style-type: none"> • Manage—Used to copy new driver packs to the Operations Manager server. • Driver Pack Upgrade—Displays the servers discovered when you click Search (use filters to narrow the results). <ul style="list-style-type: none"> – Click Copy To Server to copy new driver files from the Operations Manager server to the selected servers. – Click Install to install all copied driver pack files on the selected servers. <p>Tip See the “Upgrade Procedure” section on page 15-9 for more information.</p>
3	The servers included in the search.
3	The driver packs installed for the selected server.

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. For example, the SUSE Linux Enterprise Server (SLES). To determine the server OS, log in to the Management Console and select **Monitor > System Summary > OS Type**. F

Step 2 Select **System Settings > Driver Pack Management**. (Figure 15-4).

Step 3 Display the servers to be upgraded.

- (Optional) Select the filter(s) to display specific servers.



Tip All servers are displayed if no filters are selected.

- Click **Search** to display the list of servers according to the filters.
- Select a server to display the driver packs installed on that server.

Step 4 Upload a new driver pack software file to the Operations Manager server.

- Select the **Manage** tab (Figure 15-4).
- Click **Add**.
- In the pop-up window, click **+** 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`
- Click **OK**.
- Wait for the drivers to upload to the Operations Manager server.
The driver pack status is “Not Installed”.

Step 5 Copy the new driver packs from the Operations Manager server to the other servers.



Note Copying the driver packs to the other servers allows the Media Servers to be upgraded.

- Select the **Driver Pack Upgrade** tab (Figure 15-4).
- Select one or more servers.
- Click **Copy To Server**.
- Select the **Manage** tab.



Note You can copy the driver packs to the servers without installing them. This allows you to stage the software on a server without performing the upgrade, if necessary.

Step 6 Install the new driver packs on the servers.



Note Copying the driver packs to the other servers allows the Media Servers to be upgraded.

- Select one or more servers from the **Driver Pack Upgrade** tab.
- Click **Install** to install all driver packs that were copied to the server.
Driver packs can only be upgraded. They cannot be downgraded.

**Caution**

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



CHAPTER 16

Backup and Restore

Refer to the following topics to backup the Operations Manager configuration and video recording files.

Contents

- [Backing Up and Restoring the Operations Manager Configuration, page 16-2](#)
 - [Performing Backups, page 16-3](#)
 - [Backup Settings, page 16-3](#)
 - [Backup File Format, page 16-4](#)
 - [Disk Usage for Backups, page 16-5](#)
 - [Restoring an Operations Manager Backup, page 16-5](#)
 - [Deleting a Backup File, page 16-6](#)
- [Backing Up the Media Server Configuration, page 16-6](#)
- [Backing Up Recordings, page 16-7](#)

Backing Up and Restoring the Operations Manager Configuration

Use Backup & Restore to backup the configurations and historical data stored on the Operations Manager. There are two backup options:

- **Configuration Only**—Backs up the user-defined configuration, including device settings (for cameras, encoders, and Media Servers), user accounts, and other attributes. Also includes installed licenses.
- **Configuration Plus Historical Data**—(Default) Backs up the configuration plus events, health notifications, logs, and other data containing information regarding the status, use and health of the system.

Usage Notes

- We recommend backing up the Operations Manager data on a regular basis to ensure configuration and event data is not lost if a hardware failure occurs. Backups are also used to restore configurations and historical data when upgrading or moving to a new system.
- 500 Mb disk space is the default amount of storage space allocated for Operations Manager backups, and cannot be changed.
- When the maximum number is reached, the oldest backup file will be deleted when a new backup is created.

Backing Up Media Servers and Recorded Video

- Media Server data is backed up using the Cisco Video Surveillance Management Console. The Media Server backup is separate from the Operations Manager backup and includes critical settings and data necessary to restore the system in the event of a hardware failure. We highly recommend that you also back up all Media Servers. See the [“Backing Up the Media Server Configuration” section on page 16-6](#) for instructions.
- Recordings are backed up using a Long Term Storage server. See the [“Archiving Recordings to a Long Term Storage Server” section on page 12-16](#).

Contents

Refer to the following topics for more information:

- [Performing Backups, page 16-3](#)
- [Backup Settings, page 16-3](#)
- [Backup File Format, page 16-4](#)
- [Disk Usage for Backups, page 16-5](#)
- [Restoring an Operations Manager Backup, page 16-5](#)
- [Deleting a Backup File, page 16-6](#)

Performing Backups

Use the Manage Backup tab to schedule automatic backups, trigger a one-time backup, view a summary of the disk space used by backups, or view a summary of failed backups.

Immediate Backup Procedure

To trigger an immediate one-time backup:

-
- Step 1** Click **System Settings > Backup & Restore > Manage Backups**.
 - Step 2** Click **Backup Now** and select **To Remote** or **To Local**.
 - Step 3** From the pop-up, select the destination and backup type (see [Table 16-1](#) for more information).
 - Step 4** Click **OK**.
 - Step 5** Backup files are saved to the selected destination as a file described in the “[Backup File Format](#)” section on page 16-4.
-

Automatic Backup Procedure

To schedule recurring backups:

-
- Step 1** Click **System Settings > Backup & Restore**.
 - Step 2** Select **Manage Backups**.
 - Step 3** Enter the backup settings as described in [Table 16-1](#).
 - Step 4** Click **Save**.



Tip

Backup files are saved to the selected destination as a file described in the “[Backup File Format](#)” section on page 16-4.

-
- Step 5** Failed backups are displayed in the Failed Backup field. Double-click an entry to display details.
-

Backup Settings

[Table 16-1](#) describes the Operations Manager backup and restore settings.

Table 16-1 Operations Manager Backup Settings

Field	Description
Automatic Backups	
Enable	Select the check box to enable or disable the automatic backup schedule.

Table 16-1 **Operations Manager Backup Settings (continued)**

Field	Description
Destination	Select where the backup file will be stored: <ul style="list-style-type: none"> • On VSOM—(Default) Saves the backup file to the Operations Manager server hard drive. • On Remote—Saves the backup file to a network server (click the Configure tab and scroll down to Remote Storage)
Type	Select the type of data to back up: <ul style="list-style-type: none"> • Configuration Only—Backs up the user-defined configuration, including device settings (for cameras, encoders, and Media Servers), user accounts, and other attributes. • Configuration Plus Historical Data—(Default) Backs up the configuration plus events, health notifications, logs, and other data containing information regarding the status, use and health of the system.
Frequency	Define how often backups will occur (Daily , Weekly , or Monthly).
On	Select the day of the week or day of the month when automatic backups will occur. Note This field is disabled for daily backups. Select the time from the <i>At</i> field.
At	Enter the time of day the backups will occur.
Remote Storage	
Note These settings define the remote server used to store backup files if the Remote option is enabled. Click Test to verify the settings are correct and the remote server can be accessed.	
Protocol	Select the type of remote server. For example, FTP .
Address	Enter the server network address.
Username	Enter the username used to access the server.
Password	Enter the server password.
Path	Enter the directory path where the backup file will be stored

Backup File Format

Backup files are saved using the following formats:

Table 16-2 **Backup File Formats**

Backup Data	Format
Config and Historical	VSOM_HostName_backup_yyyymmdd_HHmmss.tar.gz
Config Only	VSOM_HostName_backup_config_yyyymmdd_HHmmss.tar.gz

- *HostName*—the host name of the server running the Cisco VSM Operations Manager application.
- *yyyymmdd_HHmmss*—the date and time when the backup file was created.

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

Disk Usage for Backups

This section displays the total amount of disk space available to store backups:

- *Automatic*—The amount of available storage used for automatic backups. The number of backups available on the system is shown in parenthesis ().
- *Manual and Transferred*—The amount of storage used for manual backups. The number of backups available on the system is shown in parenthesis ().
- *Free*— available disk space.


Restoring an Operations Manager Backup

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

**Caution**

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

Procedure

- Step 1** Click **System Settings > Backup & Restore**.
- Step 2** Click **Restore From Backup** (default).
- Step 3** Select the backup file and click **Restore**.
- Step 4** (Optional) If the backup file does not appear in the list, you can copy a backup file stored on a PC or remote server.
 - a. Select **Transfer > From Remote** or **From PC**.
 - b. Select a backup file stored on a PC or remote server.
- 
Note To transfer a file from a remote server, enter the Remote Storage settings in the Manage Backup tab. See the [“Backup Settings” section on page 16-3](#) for more information.
- c. Click **Restore**.
- Step 5** Click **Yes** to confirm.
- Step 6** Click **OK** when the restore process is complete.
- Step 7** Re-login to the Operations Manager.

Deleting a Backup File

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

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

Procedure

-
- Step 1** Click **System Settings** and then **Backup & Restore**.
- Step 2** Select the backup file from the list (**Restore** tab).
- Step 3** (Optional) To save the file to a PC disk or remote server, click **Transfer** and then **To Remote** or **To PC**.
- **To PC**—select the location for the backup file.
 - **To Remote**—the file will be transferred to the location specified in the Remote Storage section of the Configure tab. See the [“Backup Settings” section on page 16-3](#) for more information.
- Step 4** Click **Delete** (bottom left).
- Step 5** Click **OK** to when the confirmation messages appear.
-

Backing Up the Media Server Configuration

The Media Server application backup is separate from the Operations Manager backup and includes critical server settings and data necessary to restore the system in the event of a hardware failure.

Usage Notes

- Use the browser-based Cisco VSM Management Console to back up the Media Server configuration data on each server. See the [Cisco Video Surveillance Management Console Administration Guide](#) for instructions and more information.
- Media Server backups do not include recordings. See the [“Backing Up Recordings” section on page 16-7](#) for instructions to back up recordings to a Long Term Storage (LTS) server.

Accessing the Media Server Backup and Restore Screen

-
- Step 1** Select **System Settings > Management Console**.
- Step 2** Enter your Management Console password to log in.



Tip

The console password is different from your Operations Manager password. The default console username *localadmin* cannot be changed.

- Step 3** Click the **Administration** tab.
- Step 4** Select **Back up** or **Restore** (under the Maintenance heading).
- Step 5** Select the **Media Server** application.

- Step 6** Complete the backup or restore process as described in the [Cisco Video Surveillance Management Console Administration Guide](#).
-

Backing Up Recordings

Recordings can be backed up to a Redundant Media Server or a Long Term Storage (LTS) server (or both). To do so, you must configure cameras and camera templates for Stream Redundancy and Long Term Storage.

See the following topics for more information:

- [Configuring the Redundant and Failover Options, page 12-12](#)
- [Archiving Recordings to a Long Term Storage Server, page 12-16](#)

For overview information, see the following:

- [“High Availability” section on page 12-1](#)



APPENDIX **A**

Related Documentation

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

- Click **Help** at the top of the screen to open the online help system.
- Download PDF versions at **Operations > Help**.
- 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

Table B-1 *Revision History*

Release	Date	Change Summary
Release 7.0.0	October, 2012	Initial draft. See the Release Notes for Cisco Video Surveillance Manager for more information.
Release 7.0.1	February, 2013	Maintenance Update, including various bug fixes and edits. New and revised features including the following: <ul style="list-style-type: none">• Support for additional LDAP server configurations. See “Adding Users from an LDAP Server”.• Added Importing or Updating Servers Using a CSV File• Support for custom fields in soft triggers alert URLs. See “Configuring Soft Triggers”.• Added support for 64-bit version of Internet Explorer. See the “Requirements” for more information.• Added “Using “Split Model” Multi-Port Multi-IP Encoders”.• Numerous minor revisions, updates and edits. See the Release Notes for Cisco Video Surveillance Manager , Release 7.2 for more information.

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

Release	Date	Change Summary
Release 7.2	August, 2013	<ul style="list-style-type: none"> • Servers are now configured separately from the services that run on them <ul style="list-style-type: none"> – Configuring Servers, page 6-1 – Configuring Media Server Services, page 7-1 – Operations Manager Advanced Settings, page 6-24 • Revised the “High Availability” section on page 12-1 to reflect changes in defining the Media Server HA options. • Servers can now be pre-provisioned. See the “Adding or Editing Servers” section on page 6-10. • Revised “Backup and Restore” section on page 16-1. • Added the “Understanding Events and Alerts” section on page 13-2. • Added “Issues” tab and other revisions to Health Dashboard: Viewing Device Health Summaries, page 13-6. • Added the “Installing and Upgrading Driver Packs” section on page 15-8. • Multicast server address and port number can now be defined when the camera is added, or using the camera configuration page. See the following: <ul style="list-style-type: none"> – Configuring Multicast Video Streaming, page 10-18 – Manually Adding a Single Camera, page 8-12 – General Settings, page 8-45 • Added the ability to define a default <i>View</i> for the Monitor Video feature. See the “Selecting a Multi-Pane “View”” section on page 2-4 and the “Setting the Default View” section on page 3-8 • Additional filters and revised process added to the “Upgrading Cisco Camera and Encoder Firmware” section on page 15-3. • Removed the “Records Settings” from the System Settings page. Operations Manager will now store up to 1 million alerts, events, and audit log entries. • Added chapter for Software Downloads and Updates, page 15-1.