Cisco Video Surveillance Operations Manager User Guide

Release 7.6

Cisco Systems, Inc.
www.cisco.com

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

Cisco Video Surveillance Operations Manager User Guide, Release 7.6

Preface

Revised: August 3, 2015

This document, the *Cisco Video Surveillance Operations Manager User Guide* provides an overview of Cisco Video Surveillance Operations Manager Release 7.6, 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.

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

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.	• Configuring Servers, page 6-1 • Adding and Managing Cameras, page 10-1 • Adding and Managing Cameras, page 10-1
Manage server services	Configure, enable or disable server services, such as the Media Servers that manage video playback and recording.	• Configuring Media Server Services, page 9-1 • Operations Manager Advanced Settings, page 6-32
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.	• 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.	• Configuring Continuous, Scheduled, and Motion Recordings, page 12-7 • Configuring Camera PTZ Controls, Presets, and Tours, page 10-67 • Configuring Motion Detection, page 10-82 • Using Advanced Events to Trigger Actions, page 13-7

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 19-1
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.	• Backup and Restore, page 21-1 • Archiving Recordings to a Long Term Storage Server, page 17-16

Requirements

Cisco VSM Operations Manager requires the following.

Table 1-2 Requirements

Requirements	Requirement Complete? (✓)
At least one Cisco Video Surveillance server must be installed on the network. • 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 services.	❑
The IP address or hostname of the Operations Manager.	❑
A valid Cisco VSM Operations Manager username and password.	❑
The server IP address and password if stand-alone Cisco Media Servers are deployed.	❑
At least one camera physically installed and connected to the network. • 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. **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 10-10.	❑
All the servers and camera endpoints must be reachable on the network. Review Understanding Server and Camera Network Configuration, page 7-1 for more information.	❑
A Domain Name Server (DNS) configuration must be installed and working properly. If Cisco VSM servers are added to the Operations Manager using hostnames (instead of IP addresses), then the network Domain Name Server (DNS) that resolves those hostnames must be properly configured and working. If the DNS goes down or is incorrect, "404 File Not Found" errors may be displayed by the Operations Manager when performing tasks such as downloading MP4 video clips, executing soft triggers, or streaming video. If this occurs, correct the DNS configuration to properly resolve all server hostnames to the proper IP address.	❑

Table 1-2 Requirements (continued)

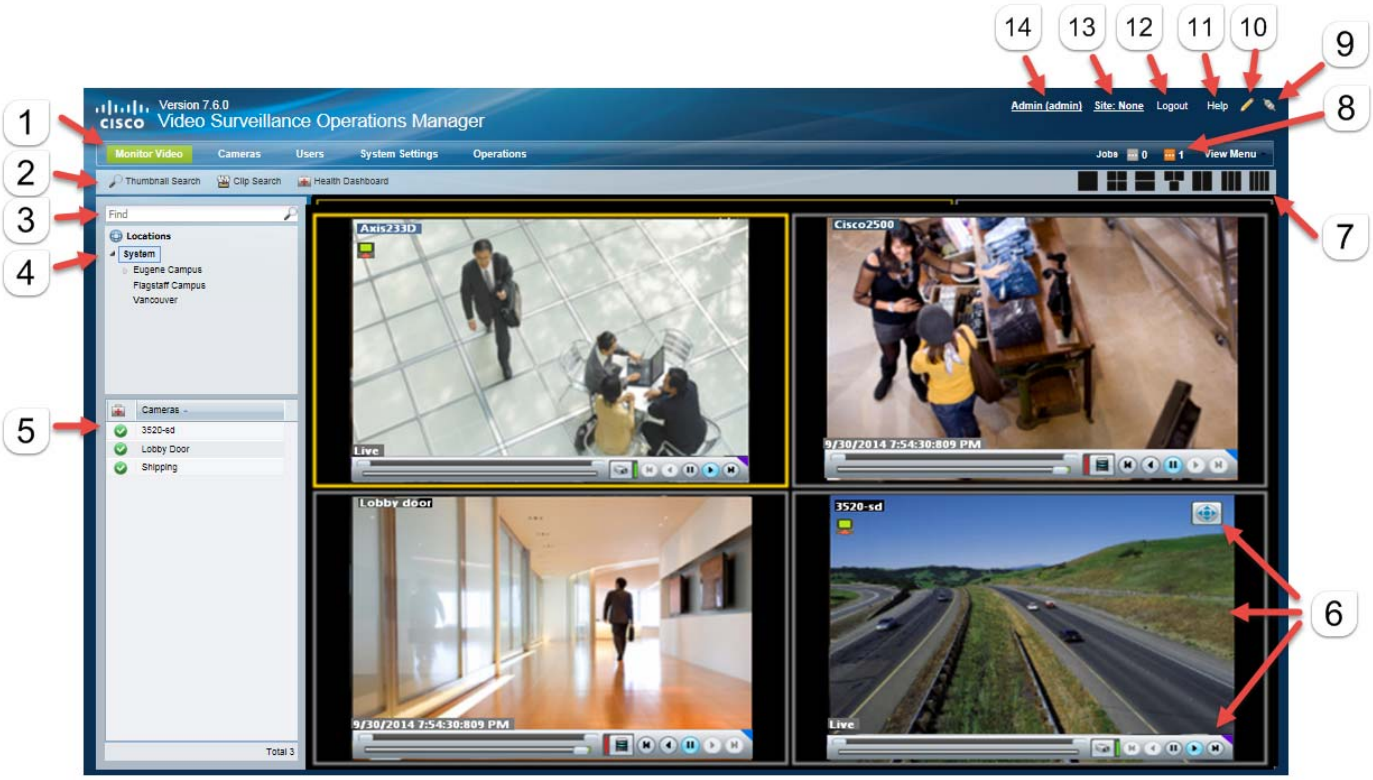
Requirements	Requirement Complete? (✓)
A PC or laptop with the following: • Windows 7 (32-bit or 64-bit) or Windows 8 (64-bit) • Minimum resolution of 1280x1024 • You must log in with a standard Windows user account. Logging in with a Guest account can prevent video streaming and result in an error to be displayed in the video pane: "Cannot create RTSP connection to server. Check network connection and server health status." See the Cisco Video Surveillance Monitoring Workstation Performance Baseline Specification for the complete baseline performance specifications for a video surveillance monitoring workstation.	❑
The Internet Explorer (IE) web browser. **Windows** • Windows 7 supports IE 9, 10 or 11. • Windows 8 supports IE 10, desktop version (the Metro version of IE 10 is not supported). **32-bit or 64-bit** • 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). The 64-bit version of Internet Explorer requires that the workstation run in "Protected Mode". See the Cisco Video Surveillance Monitoring Workstation Performance Baseline Specification for the complete workstation requirements, and instructions to enable "Protected Mode".	❑
The Cisco Multi-Pane client software installed on the PC. • 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. **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.	❑

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	Feature tabs: • **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 10-1. • **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. See the "Revising the System Settings" section on page 20-1. • **Operations**—Links to documentation, desktop monitoring software, logs, Reporting and Health features, and the Cisco VSM Management Console. **Note** Only the features and functions that the user has access permissions for are displayed.

2	Additional feature buttons. For example, **Thumbnail Search**, **Clip Search** or **Health Dashboard**. The buttons and options vary depending on the screen.
3	Find—Search for devices and attributes (see the "Using Find" section on page 1-30).
4	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.
5	Devices, users, or other attributes available for the selected location.
6	Video Monitoring panes or configuration window. The fields and contents of the main window vary depending on the feature you are accessing.
7	• Layouts—(Monitor Video window) Select a blank layout (set of video panes) and double-click cameras to view in those panes. See the "Controlling Live and Recorded Video" section on page 2-7. • Views—(Monitor Video window) Create or select a pre-defined *View* (set of video panes). See the "Selecting a Multi-Pane "View"" section on page 2-4.
8	Jobs—A user-triggered Cisco VSM system task that is completed in the background. • Click the icon to view information about the job. • The job icons are displayed only when a job is in progress. See the "Understanding Jobs and Job Status" section on page 19-29.
9	Connection—Defines if the Operations Manager is receiving real time status updates (from the ActiveMQ service).
10	Maintenance Mode—A read-only mode that allows user to access live and recorded video but locks most configuration changes. See Understanding Maintenance Mode, page 1-31.
11	**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.
12	Logout—Click to log out of the Cisco VSM Operations Manager.
13	Site—Displays the site where you are logged in. Click the site name to change the site. See the "Understanding and Changing Your "Site"" section on page 1-24.
14	Username—Displays the username for the currently logged in user. Click the username to change your password. See the "Changing Your Password" section on page 1-23.

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

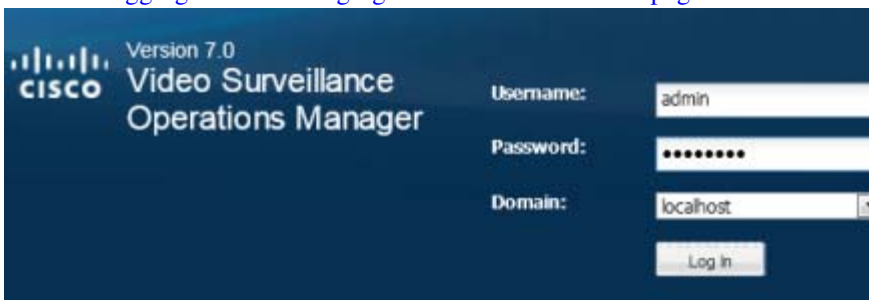
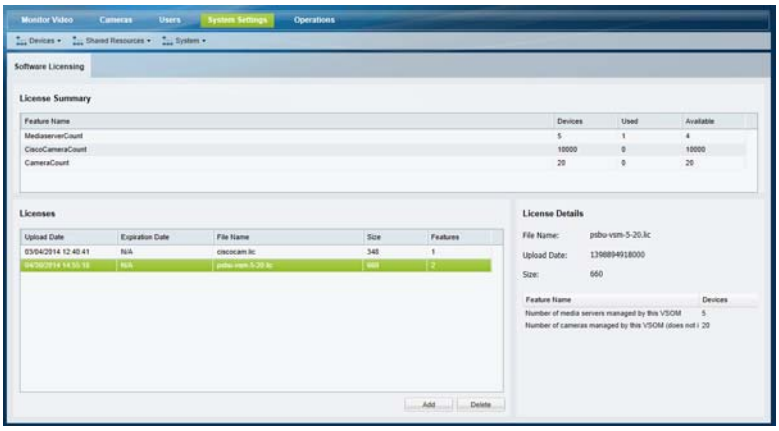
	Task	Description
Step 1	Log on to the Cisco VSM Operations Manager.	See the "Logging In and Managing Passwords" section on page 1-18. 
Step 2	Install the system licenses.	Purchase and install a license for each Media Server and non-Cisco camera added to your deployment. See the "Installing Licenses" section on page 1-26. 

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

	Task	Description
Step 3	Revise the system settings.	Revise the default user password properties, record storage rules, backup file rules, and other settings. **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.  For example: **a.** Choose **Settings** > **System Settings**. **b.** Revise the following properties, as necessary: – General System Settings, page 20-1 – Password Settings, page 20-3 See the "Revising the System Settings" section on page 20-1 for more information.

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

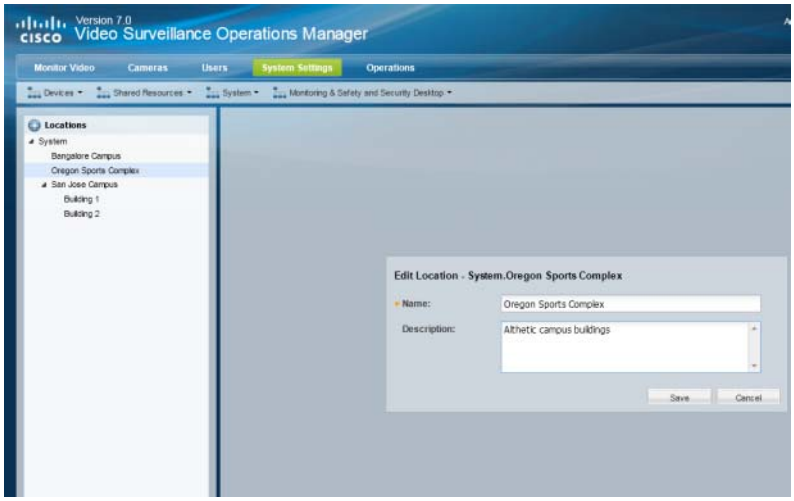
	Task	Description
Step 4	Create at least one location.	Define the locations that are assigned to devices (such as cameras) user groups, and policies. Locations allow administrators to restrict user access to the cameras, policies, and data (such as alerts) required by the user's role. For example, a security guard can have access to view video at a specific location, but not to configure the camera properties.  **a.** Select **Locations** from the **System Settings** menu. **b.** Click **Add**. **c.** Enter the location name and press *Enter*. See the "Creating the Location Hierarchy" section on page 5-1 for more information.

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

	Task	Description
Step 5	Create at least one user account.	Create the user accounts and access permissions that restrict the locations and tasks available to a user. For example: **Create a User Role** The Role defines the access permissions for different types of users. Roles are assigned to User Groups. **a.** Select **Users**. **b.** Select the **Roles** tab . **c.** Click **Add**. **d.** Enter the basic settings (see Table 4-5). **e.** Select the Role permissions (see Table 4-2 and Table 4-3). **f.** Click **Create**. See the "Defining User Roles" section on page 4-9. **Create a User Group** 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. **a.** Select the **User Groups** tab . **b.** Click **Add**. **c.** Enter the group settings, including the Role that defines the access permissions for the group (see Table 4-6). **d.** Click **Create**. See the "Adding User Groups" section on page 4-11. **Create a User Account** 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. **a.** Select the **User** tab . **b.** Click **Add**. **c.** Enter the basic user settings (see Table 4-7). **d.** Add the user to one or more user groups. – Click **Add** under the User Groups box. – Select one or more user groups from the pop-up window. – Select **OK**. **e.** Click **Create**. See the "Adding Users" section on page 4-15. See also the "Adding Users, User Groups, and Permissions" section on page 4-1 for more information.

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

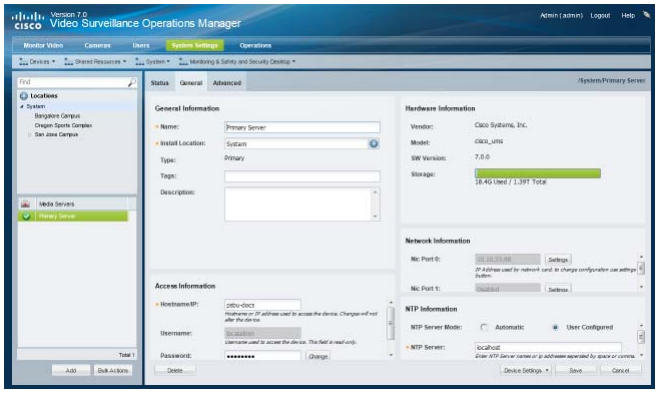
	Task	Description
Step 6	Add at least one Media Server.	Add a Media Server and camera. A Media Server is an application that runs on physical Cisco Video Surveillance server, and provides video streaming, recording and storage for the cameras associated with that server. You must add the Media Server to the Operations Manager configuration to communication between the applications.  **a.** Click **System Settings**. **b.** Click **Media Servers**. **c.** Click **Add**. **d.** Enter the basic server settings and click **Add**. **e.** Click **Save**. See the "Viewing Media Server Status" section on page 9-9 for more information.

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

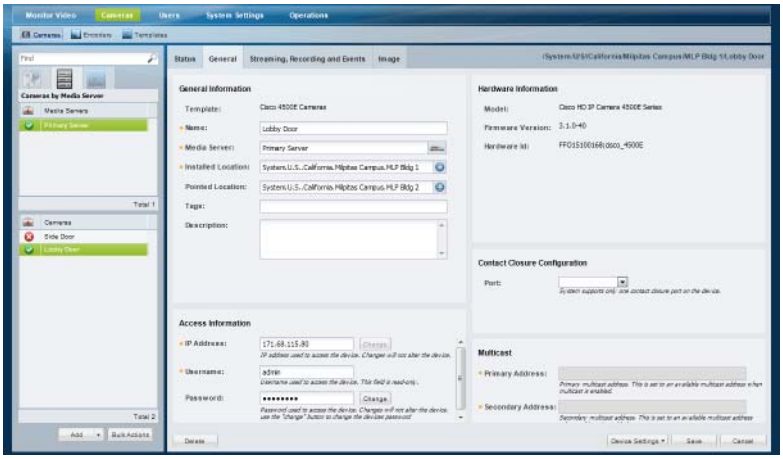
	Task	Description
Step 7	Add at least one camera.	The surveillance video camera must be installed on the network. **Note** Although cameras can be pre-provisioned (added before they are installed on the network), you should add at least one installed camera to the basic configuration to verify network connectivity, video monitoring, and other features.  **a.** Click **Cameras**. **b.** Click **Add**. **c.** 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, page 16-1 for more information. **d.** Enter the basic camera settings and click **Add**. See the "Manually Adding a Single Camera" section on page 10-11 for more information.

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

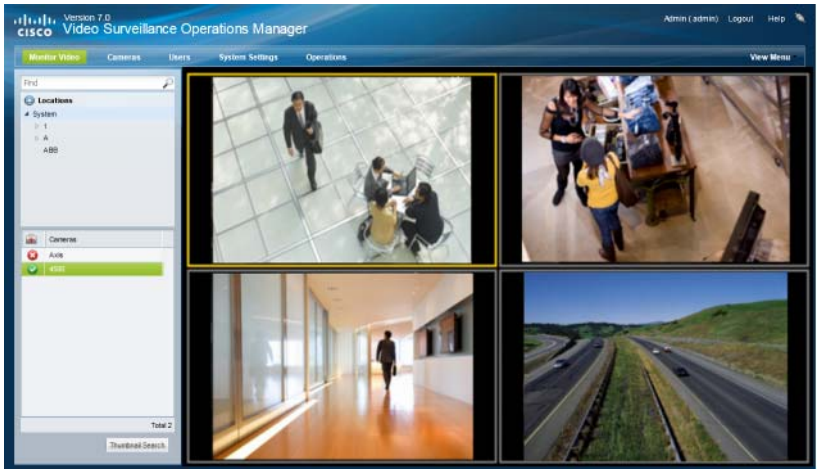
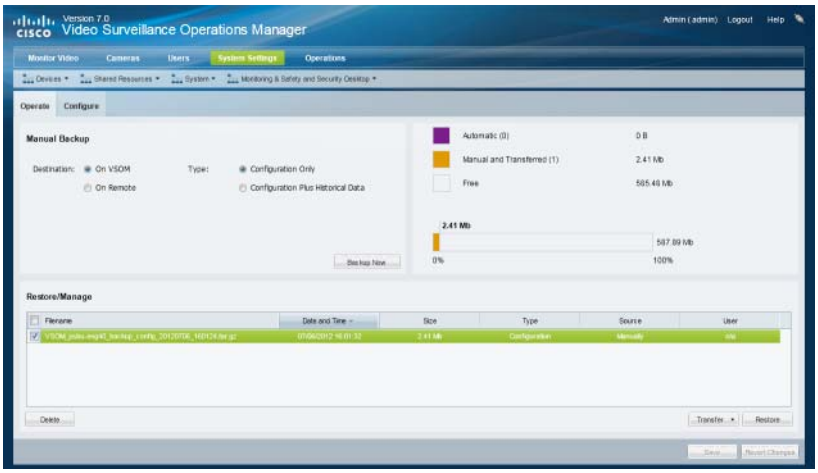
	Task	Description
Step 8	View video from the camera to verify that the system is working properly.	View the live or recorded video from the camera to verify that the settings are correct and that the devices are available on the network. See the "Controlling Live and Recorded Video" section on page 2-7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

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.	See the "Backup and Restore" section on page 21-1 for more information.  **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 Multiple Servers (Bulk Actions)" section on page 21-13 for more information.
Step 10	Troubleshoot problems or verify the system and device status.	See the "Monitoring System and Device Health" section on page 19-1 for more information. 

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).	• Adding Users, User Groups, and Permissions, page 4-1 • Adding Users from an LDAP Server, page 4-18
Step 3	Add additional Media Servers and configure the high availability options.	High availability servers provide redundant or failover support for the Primary Media Server. Long Term Storage servers can back up recordings and remove them from the Primary Media Server. • Configuring Media Server Services, page 9-1 • High Availability: Cisco Media Servers, page 17-1
Step 4	Create camera templates.	Templates define configurations that can be applied to multiple cameras. See the Adding and Editing Camera Templates, page 12-1.
Step 5	Add additional cameras.	You can import cameras from a file or discover them on the network. • Importing or Updating Cameras or Encoders Using a CSV File, page 10-17 • Discovering Cameras on the Network, page 10-23 • Adding Cameras from an Existing Media Server, page 10-38
Step 6	Configure camera recordings.	Configure cameras to record in a continuous loop, on a recurring schedule, or both. See the "Configuring Continuous, Scheduled, and Motion Recordings" section on page 12-7

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

Step 7	Configure additional camera and monitoring features.	• Configuring Camera PTZ Controls, Presets, and Tours, page 10-67 • Configuring Motion Detection, page 10-82 • Setting the Default View, page 3-1 • Configuring Video Walls, page 3-9 • Enabling Record Now, page 3-11
Step 8	Define the system events that 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. See the "Using Advanced Events to Trigger Actions" section on page 13-7 for more information.

Logging In and Managing Passwords

Logging In

To log in to the Cisco Video Surveillance Operations Manager:

Procedure

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.

- Enter the virtual IP address or hostname provided by your system administrator if redundant (HA) Operations Manager servers are deployed.

Step 3 Enter your username and password.

- The default credentials for a new or factory restored server are **admin/admin**.
- The username and initial password for all other users is defined when the user account is created (see the "Adding Users" section on page 4-15).
- All users are prompted to reset the password at first login.

Step 4 Select a domain:

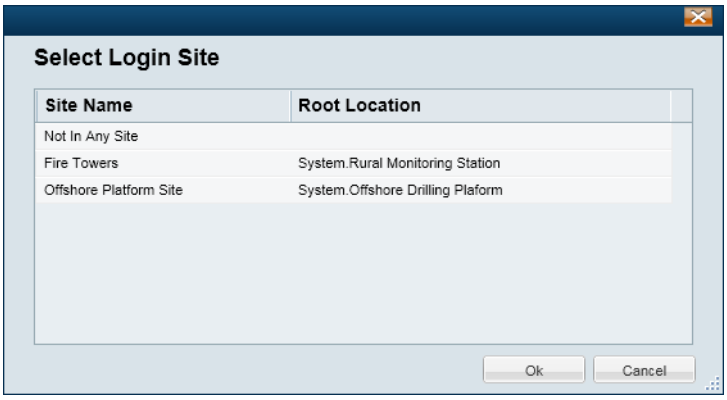
- Choose the default "localhost" if your account was created using the Operations Manager.
- Select an alternative domain if instructed by your system administrator.

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 Select a Site, if prompted (Figure 1-2).

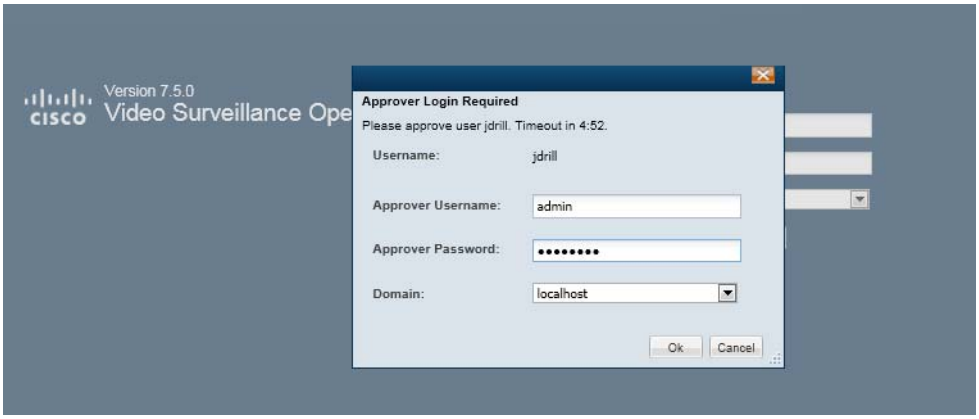
Figure 1-2 Selecting a Site on First Login



- Users with Site access are prompted for a Site on first login only, but not on subsequent logins
- Users with no Site access are not prompted for a Site.
- Users can also change their Site after log in, if configured.
- See the "Understanding and Changing Your "Site"" section on page 1-24 for more information.

Step 7 If prompted, ask your manager or other administrator to enter their "Approver Login" (Figure 1-3).

Figure 1-3 Approver Login



- This second login is required only if configured.
- See the "Understanding Dual Login" section on page 1-20 for more information.
- If the approval is not successfully submitted within the time-out period, the login is denied.

Step 8 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."

Understanding Dual Login

Dual Login requires that a second user (such as a manager) enter their credentials to approve a user's access. When the user logs in, a second prompt appears for the manager's credentials. This optional feature can be used when explicit approval is required whenever a user logs in.

To enable Dual Login, select the **Approval Required** checkbox in a User Group, and then select an "Approval Usergroup". All users assigned to the User Group can only gain access if a member of the "Approval Usergroup" also enters their password.

Procedure

Tip See the "Adding User Groups" section on page 4-11 for more information.

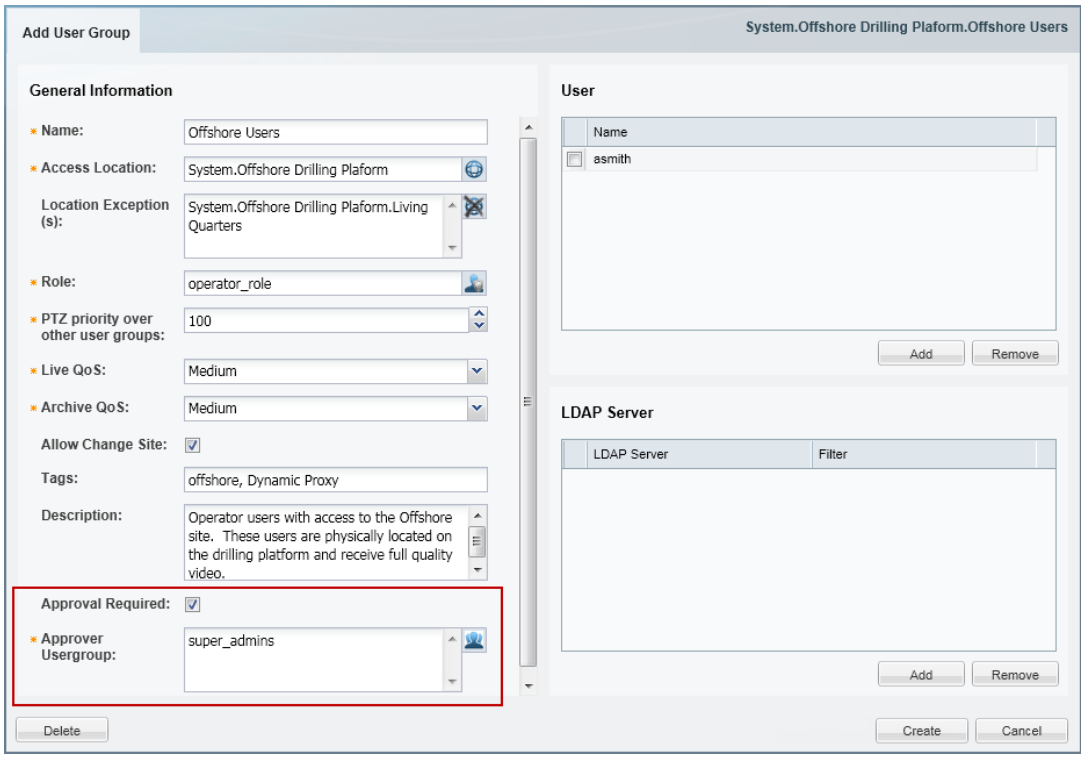
Step 1 Select the **User Groups** tab .

Step 2 Click **Add**.

Step 3 Enter the settings for the group as described in the "Adding User Groups" section on page 4-11 (specifically Table 4-6 on page 4-12).

Step 4 (Optional) Select **Approval Required** and select an "Approval Usergroup" to require a second user to approve the user login (Figure 1-4).

Figure 1-4 Creating a User Group That Requires Dual Login "Approval Required"



For example, create a User Group that includes only users who can approve user logins, or select an existing group, such as **super_admins**.

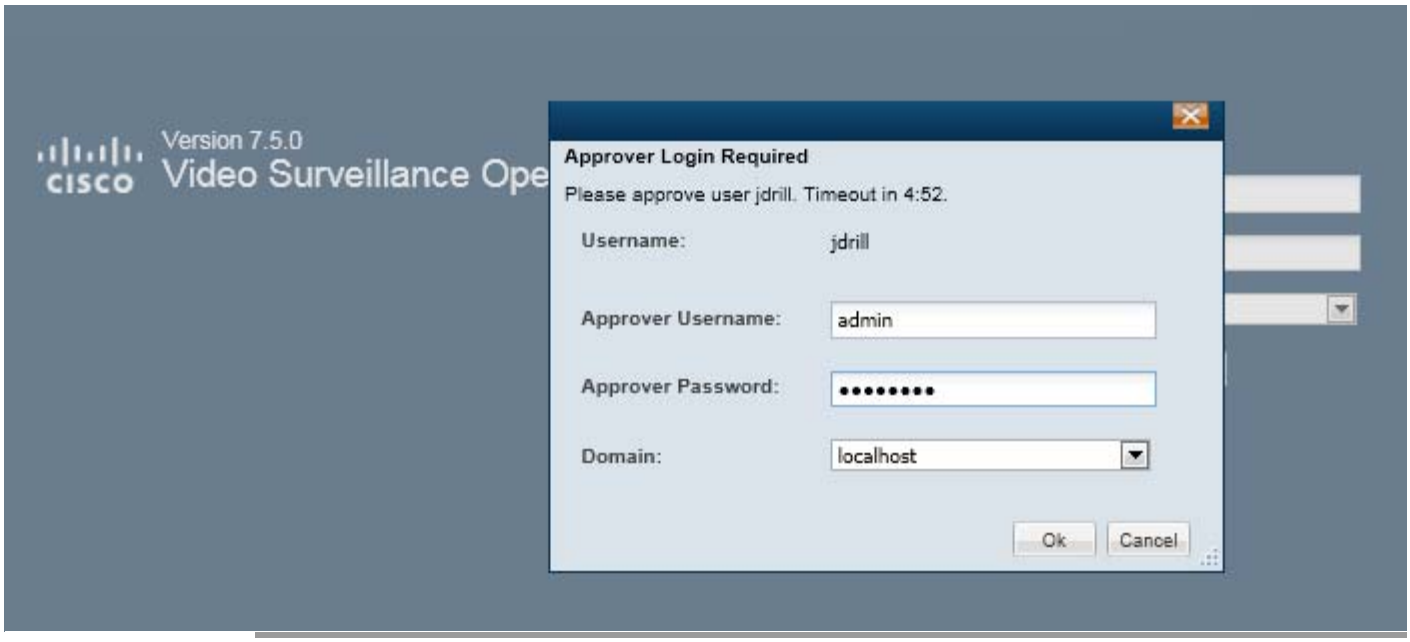
Step 5 Click **Create**.

Step 6 Assign users to the User Group, and to the Approver Usergroup.

Step 7 When the user logs in, a window appears requiring a second user to enter their username and password (Figure 1-5).

Note If the approval is not successfully submitted within the time-out period displayed, the login is denied.

Figure 1-5 Approver Login



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**	*Super-admin* 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 1-6).

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, page 1-18).

Step 2 Click your username in the top right (Figure 1-6).

Step 3 Enter your current password.

Step 4 Enter and re-enter a new password.

Figure 1-6 Changing Your Password

Changing Another User's Password

Only super-admins can change another user's password.

Procedure

Step 1 Log in to the Operations Manager with a super-admin account.

Step 2 Select **Users**, and then select the **User** tab .

Step 3 Highlight a username.

Step 4 Enter and re-enter a new password in the password fields.

Notes

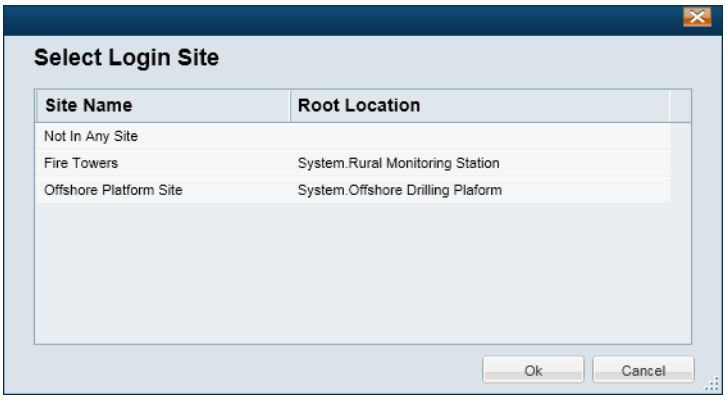
- This method can also be used by the super-admin to change their own password. All other users can change their own password by clicking on their username in the top right corner of the browser (Figure 1-6). See Changing Your Password, page 1-23.

Understanding and Changing Your "Site"

"Sites" are designated location hierarchies (a location and its sub-locations) where network connectivity between the cameras and servers is good. These *Sites*, however, may have low-bandwidth connectivity to cameras, servers and users outside the Site.

If the system is configured with Sites, and you are a member of a User Group that is assigned to a Site location, you will be prompted to select a Site the first time you log in (Figure 1-7).

Figure 1-7 Selecting a Site on First Login

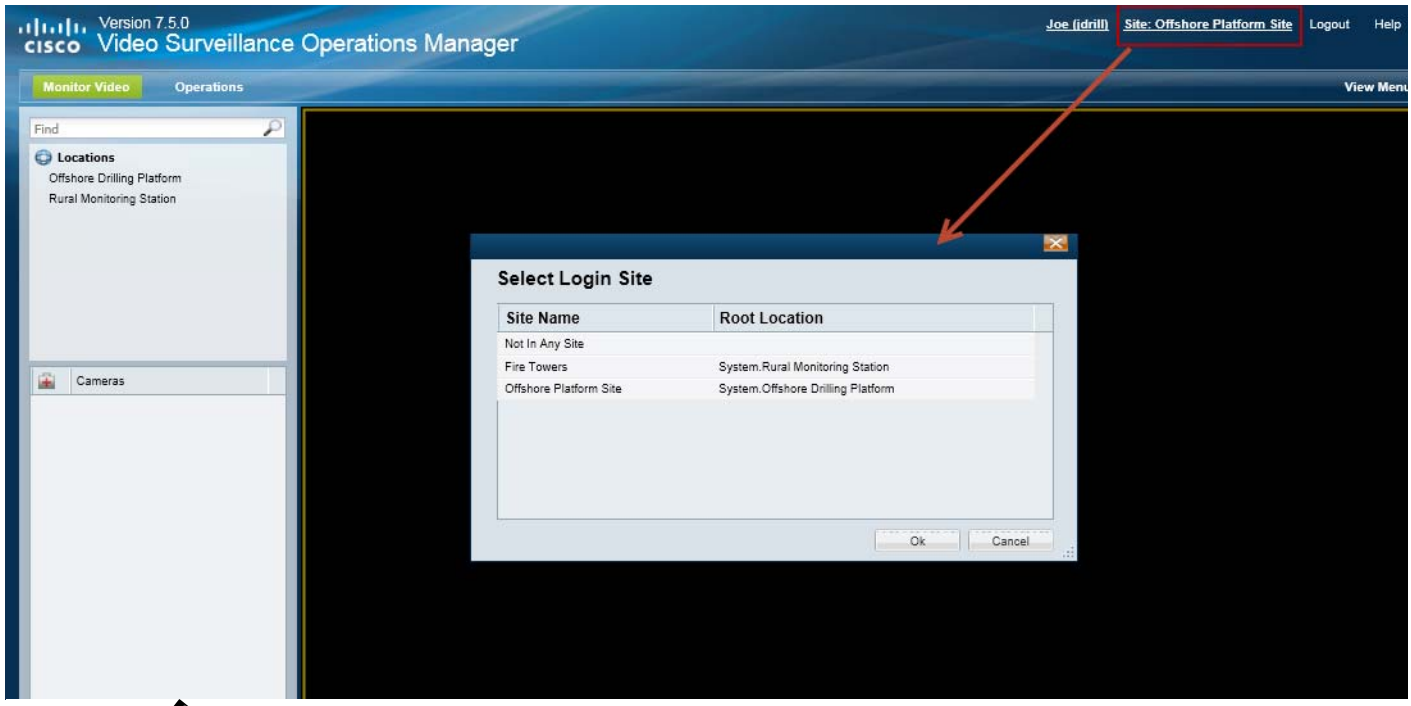


- Users with Site access are prompted for a Site on first login only, but not on subsequent logins.
- Users with no Site access are not prompted for a Site.
- Users who have access to multiple sites, but do not have the option to change sites, will default to "Not in any site" when logging in.
- If the Site is configured for Dynamic Proxy, users inside the Site are served by the Media Server in that Site (when accessing cameras inside the Site). Users outside the Site will receive video from a Dynamic Proxy server when accessing any camera inside the Site. See the "Using Dynamic Proxy to Monitor Video From Remote Sites" section on page 23-1 for more information.
- Users who do not select a Site, are not assigned a Site, or select Not in Any Site will receive video from a Dynamic Proxy server for cameras in any Site where Dynamic Proxy is enabled.

Changing Your Site While Logged In

Users can also change their Site while logged in to the system. Click the current Site name in the top right corner and select a new Site (Figure 1-8).

Figure 1-8 Changing Your Site After Login



Note Users are allowed to change their Site after logging in only if the **Allow Site Change** option is selected in their user configuration. See the "Table 4-6User Group Settings" section on page 4-12.

Installing Licenses

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

Note If your deployment includes a Cisco VSM Federator server, you must also purchase and install a Federator license to enable the number of Operations Managers managed by the Federator server. See the "Using Federator to Monitor Multiple Operations Managers" section on page 22-1.

Review the following information for more information.

Usage Notes

- You can add 1 Media Server and 10 non-Cisco cameras without a license for initial setup purposes only. This feature is removed when you add any permanent license.
- A permanent license is required for each Media Server and non-Cisco camera installed in your deployment.
- A license for 10,000 Cisco cameras is included by default (you do not need to purchase and install any additional licenses for Cisco cameras).
- Licenses are installed in the Operations Manager only (not on the individual 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.
- License files can include licenses for a single device type, or for multiple device types, such as non-Cisco cameras and Media Servers.
- 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, 10,000 cameras (including Cisco and non-Cisco devices), and 100 dynamic proxy servers.
- Soft deleted cameras are included in the camera license count. See the "Device Status: Identifying Issues for a Specific Device" section on page 19-9 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 21-1 for more information, including how to configure scheduled backups.

Tip For additional information on installing licenses, see the "Using Dynamic Proxy to Monitor Video From Remote Sites" section on page 23-1 and the "Using Federator to Monitor Multiple Operations Managers" section on page 22-1.

License Part Numbers

For a summary of the Cisco VSM licenses, see the Release Notes for Cisco Video Surveillance Manager.

Note 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 1-28.

Obtaining and Installing Licenses

To install a license, purchase the license, download the license file, and then install file in Operations Manager.

Tip License files can include licenses for a single device type, or for multiple device types, such as non-Cisco cameras and Media Servers.

Procedure

Step 1 Purchase additional licenses:

a. Determine the part number for the license you want to purchase. See the "License Part Numbers" section on page 1-27.

b. Purchase the license by contacting your Cisco sales representative or any Cisco reseller. For more information, visit http://www.cisco.com/en/US/ordering/index.shtml.

c. 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:

a. Locate the Product Authorization Key (PAK) created with the purchase.

b. In a Web browser, open the Cisco Product License Registration Web page.

http://www.cisco.com/go/license/

c. 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.

d. Transfer the file to the drive of the PC used for the configuration.

Step 3 Install the license file in Cisco VSM:

a. Log in to the Operations Manager.

b. Select **System Settings** > **Software Licensing** (Figure 1-9).

c. Click **Add** and select the license file located on your local drive.

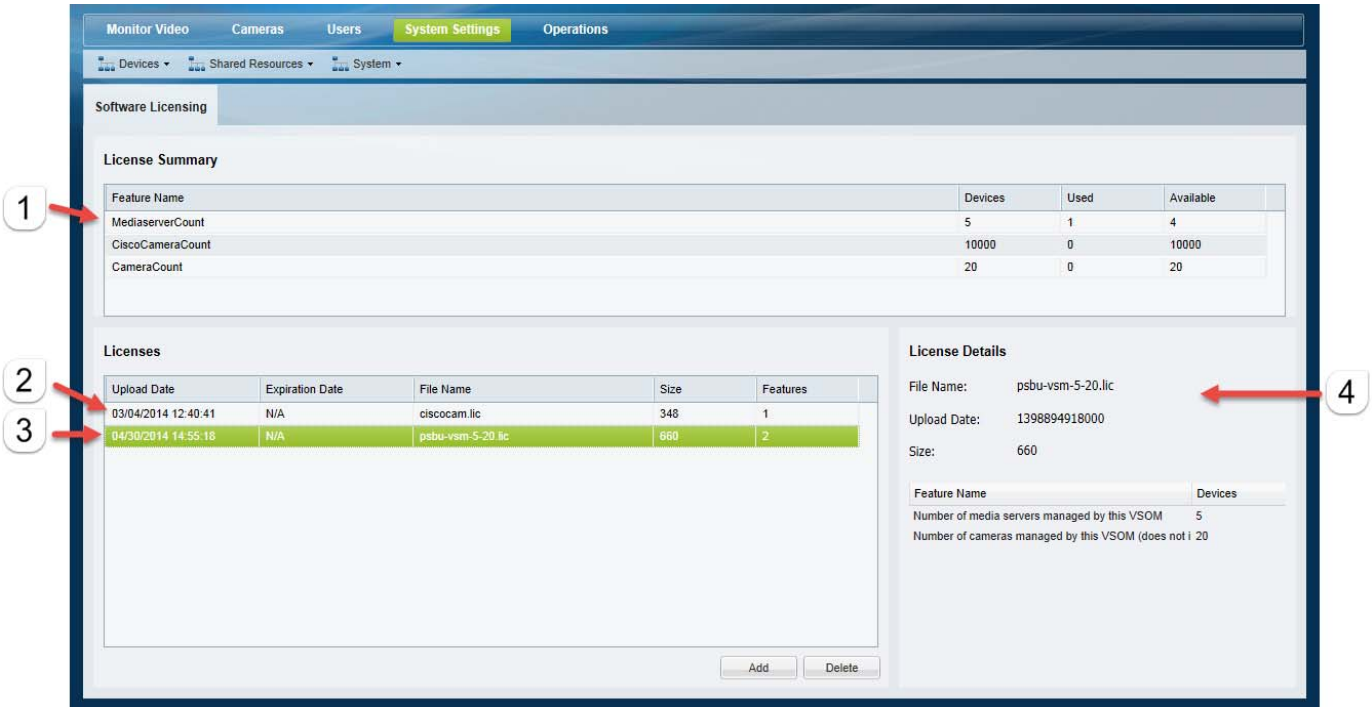
d. Click **Save** to install the file and activate the additional capacity.

Tip The additional capacity is available immediately. You do not need to restart the server or take additional steps. Entries shown in red are invalid or expired.

Displaying License Information

Select **System Settings** > **Software Licensing** to view information about each installed license, and a summary of all installed licenses (Figure 1-9).

Figure 1-9 Software Licensing



1	The *License Summary* displays the total number of Cisco cameras, non-Cisco cameras, and 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 servers and 10,000 cameras can be managed by the system. Although you can install more than the supported number of licenses, they will not be recognized.	**3**	Licenses for additional servers and non-Cisco cameras. **Note** Entries shown in red are invalid or expired.
2	The license for Cisco cameras (included).	**4**	Information about the selected license file, such as the upload date and the number of devices enabled by the license.

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 1-28).

Procedure

To remove a license:

Step 1 Select **System Settings** > **Software Licensing**.

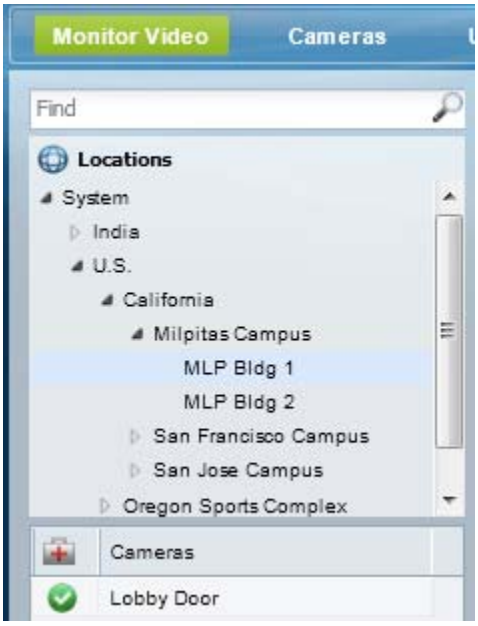
Step 2 Highlight a license entry and click **Delete** (Figure 1-9).

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 1-10) and dynamically locates any item in the open window (not just for the location selected).

Figure 1-10 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 1-11 shows the results of a partial search: entering "Lo" returns the camera "Lobby Door".

Figure 1-11 Find Results

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

Understanding Maintenance Mode

Maintenance mode is a read-only mode that allows user to access live and recorded video but locks most configuration changes while features such as Operations Manager HA are implemented. Maintenance mode allows administrators to make changes while ensuring data consistency and avoiding data corruption.

To enter maintenance mode, click the pencil icon in the title bar. The icon changes to grey and a banner appears to the top to let users know that maintenance mode is on (Figure 1-12). This means that most user configuration will be rejected This keeps the server configuration in a stable state while certain HA tasks are performed.

Figure 1-12 Maintenance Mode is ON

Examples of Tasks Allowed When Maintenance Mode is ON

The following are examples of tasks that are allowed when maintenance mode is turned on (pencil icon is grey):

- System Software upgrades
- Operations Manager HA operations
  - Add a Peer server
  - Replace the HA config
  - Repair the HA config
  - Replace the HA peer
  - Update HA config
  - Delete the HA config
  - Force failover
- Auditing
- Backup restore tasks
- System settings management
- Create clips in the Monitoring page (using the ActiveX client)

Examples of Tasks that Require Maintenance Mode to be Off

Any add, delete, or update action for location, site and other attributes are permitted only when Maintenance Mode be Off (pencil icon is yellow).

For example:

- Location
- Site
- User, role, and user groups
- Camera and encoder configuration
- Server
- Camera apps
- Health
- Driver pack installation and upgrade
- Firmware upgrades
- Licenses
- Maps
- Adding user comments
- Create clips using the Thumbnail Search or Clips Search pages.

If maintenance mode is ON (pencil icon is grey), these tasks are NOT permitted.

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

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)	• Allows simultaneous viewing of up to 25 cameras per Workspace, and up to 48 cameras per workstation. • 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
Web-based configuration and monitoring tool	Cisco Video Surveillance Operations Manager (Operations Manager)	• Allows simultaneous viewing of multiple video panes: – View up to 4 cameras with the 32-bit version of Internet Explorer. – View up to 25 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 Cisco Video Surveillance Monitoring Workstation Performance Baseline Specification for the workstation requirements when monitoring video.

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.

- 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.

- 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. To create Views, go to **System Settings** > **Views**. See Creating Video Views, page 3-4.

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

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

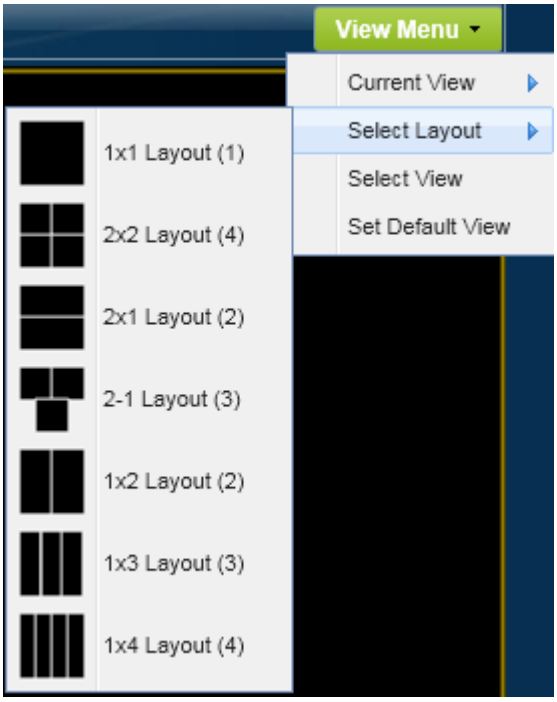


Table 2-2 View Menu

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	Reset the currently displayed layout.	Choose **Current View > Reset** to reload the last view or layout and discard any changes. **Related information** • Creating Video Views, page 3-4

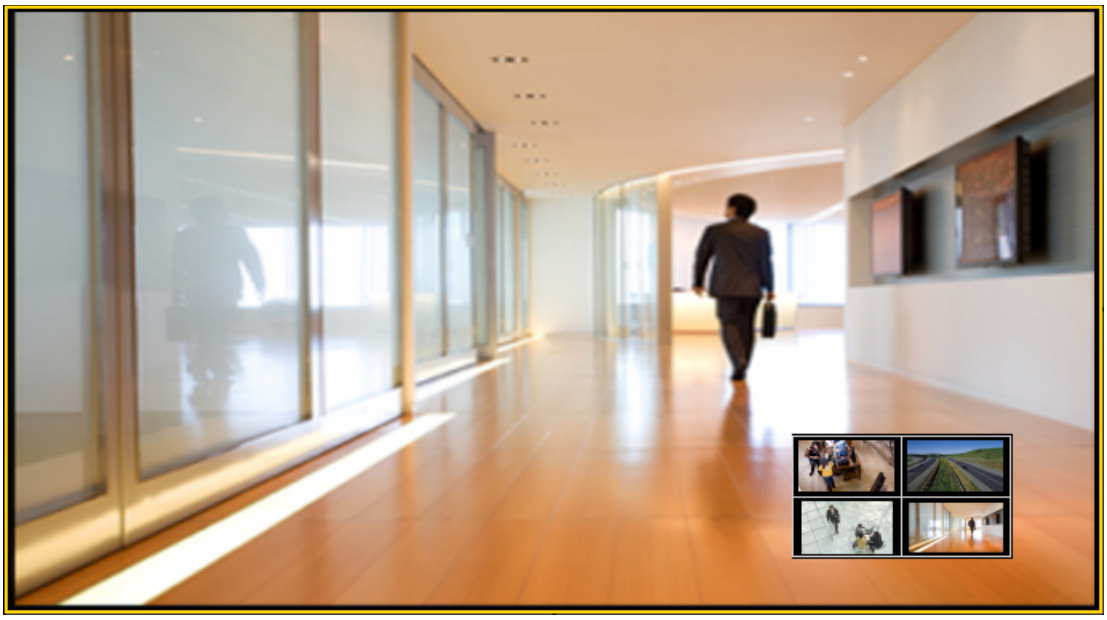
Table 2-2 View Menu (continued)

Menu	Purpose	Description
Select View	Display pre-defined views	Choose **Select View** to select a pre-defined multi-pane view. *Views* 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. **Related information** • Creating Video Views, page 3-4 • Setting the Default View, page 3-1
Set Default View	Define the view that is automatically loaded	The Default View is defined by each user and is automatically loaded when they click **Monitor Video**. 1. Create one or more Views as described in the "Setting the Default View" section on page 3-1. 2. Select **View Menu** > **Set Default View**. 3. Select a View from the pop-up window and click **Select**. **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. **Related information** • Setting the Default View, page 3-1

Tip

- To change the video in a *View* pane, drag and drop a camera name onto the pane.
- To create Views, go to **System Settings** > **Views**. See Creating Video Views, page 3-4.
- *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

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 3 shows a multi-pane view using the Cisco Video Surveillance Safety and Security Desktop (Cisco SASD) application.

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

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).

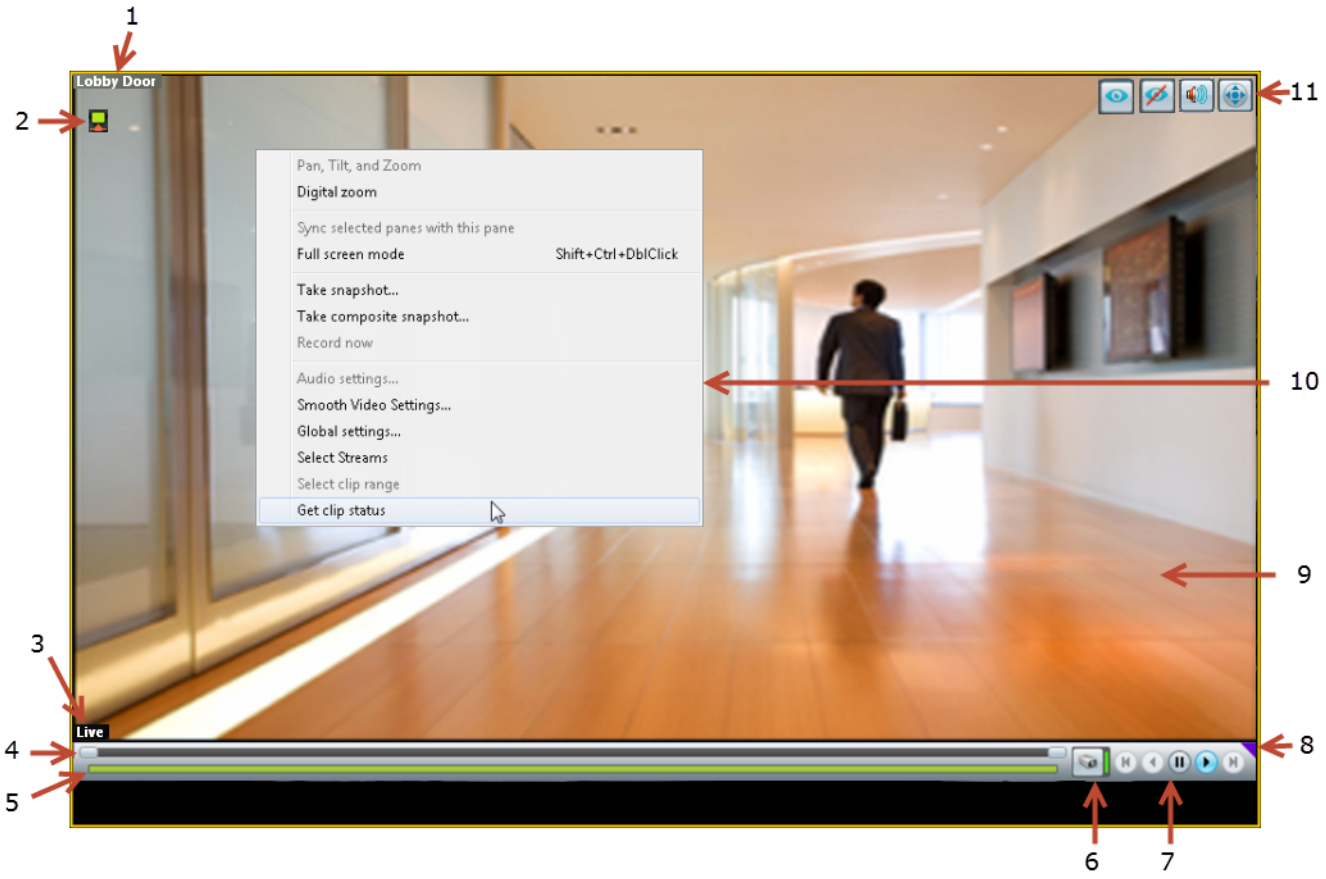
- Additional options are available by right-clicking the image. Options include synchronizing multiple viewing panes, recording live video, expanding the image to fill the screen, creating a snapshot image, and configuring smooth video options to improve playback performance when network performance 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 4 summarizes the controls available in each viewing pane.

Figure 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 2-33 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. • —Pause the video playback. • — Play the video forward at normal speed. **Note** The other playback controls are used with archived video only. See Figure 5 on page 2-12 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 *color* setting to 32-bit.
9	Video image.
10	Camera menu. 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 2-27 for more information.
11	Control icons. • —**Audio**. The audio icon appears if the camera supports audio. Click to enable or mute live audio volume. This control does not affect recorded video. • —**Privacy Mask**. Click to enable or disable the Privacy Mask. See the "Using the Privacy Mask" section on page 2-30. • —**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 2-38. • — See the "Synchronizing Video Playback in Multiple Panes" section on page 2-34. **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.

Usage Notes

- Some firewall policies on enterprise PCs can block live video streams from cameras. If this occurs, add the camera IP address to the firewall trusted list.
- To maximize the video screens, move the new workspace to a separate monitor and double-click a pane to fill the entire browser window. To fill the entire monitor screen, right-click the image and select **Full screen mode**.
- 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
- 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 2-33 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.

Additional Information

Refer to the following topics for additional options:

- Using Record Now, page 2-26
- Using the Pop-Up Menu, page 2-27
- Using the Smooth Video Options When Viewing Live Video, page 2-33
- Synchronizing Video Playback in Multiple Panes, page 2-34
- Using Pan, Tilt, and Zoom (PTZ) Controls, page 2-38

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.

Figure 5 describes the main recording features and controls.

Figure 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 . **Note** This icon is for informational purposes only when displayed with recorded video (the Smooth Video options do not apply).
3	Pop-up menu options. See the "Using the Pop-Up Menu" section on page 2-27.
4	Timestamp for the currently displayed video image. For example: 7/12/2012 4:08:39:886 AM . **Note** Changes to Live when live video is displayed.

5 Range Bar—The span of video to work with.

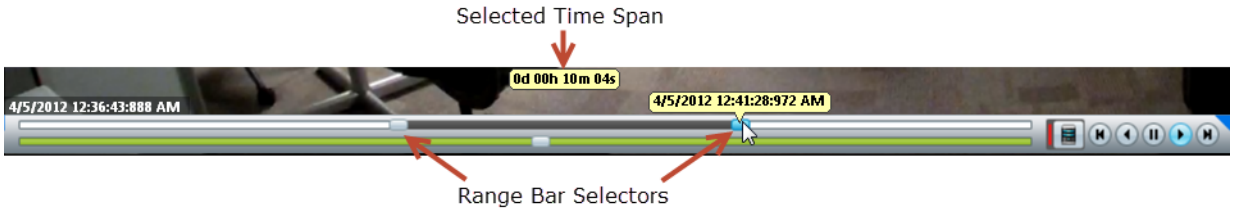
- The entire *range bar* represents the entire span of available recorded video. Slide the *range bar* selectors to shorten the range (see below).
- The lower (green) *seek bar* represents the selected range (see below).

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.

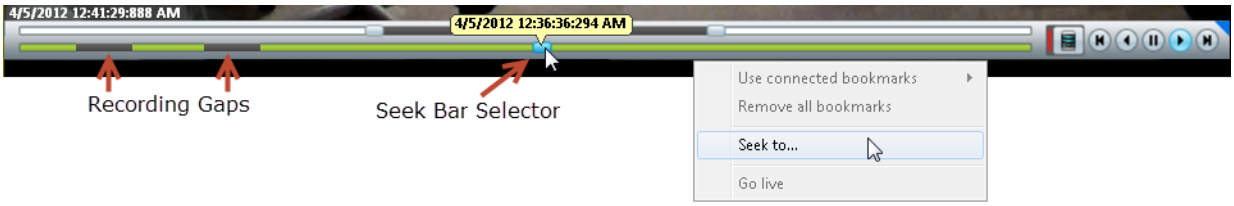


Tip The green *seek bar* represents the selected span. If the span in the top *range bar* is 10 minutes, then the green *seek* bar represents 10 minutes of video. Slide the *seek bar* selector to choose the playback time (see below).

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.

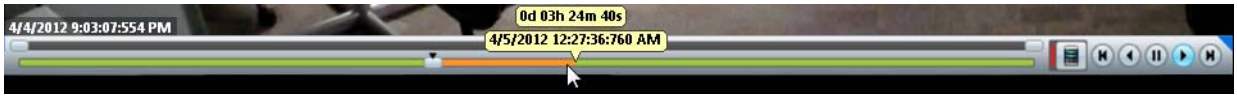
Note Gaps in the recorded video are shown in gray. Recording gaps occur if there is a manually-triggered Record Now session, if recording was manually stopped, if recording was stopped by a schedule, or if video was unavailable due to network connectivity issues, device malfunctions, or other events.

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

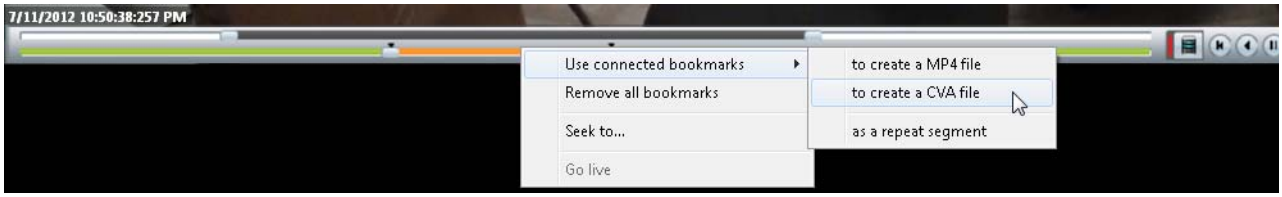
Note When you move the scroll bar for a video pane that is synchronized, that pane becomes the new synchronization master pane. The other synchronized panes play video according to the master pane. See the "Synchronizing Video Playback in Multiple Panes" section on page 2-34.

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 and Viewing Video Clips, page 2-16
- Creating a Repeat Segment, page 2-25

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

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

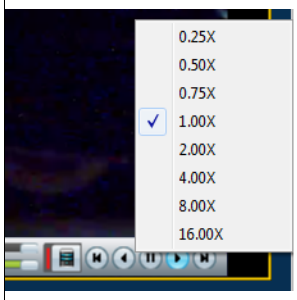
Tip The first time you select a camera's recorded video, the playback begins slightly behind the live (current) time. When you toggle between live and recorded, recorded video returns to the previously selected timestamp.

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 2-34. **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.

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.
- To maximize the video screens, move the new workspace to a separate monitor and double-click a pane to fill the entire browser window. To fill the entire monitor screen, right-click the image and select **Full screen mode**.
- 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.

Creating and Viewing Video Clips

Video clips can be created as a file for download and playback from a PC workstation, or as a *Virtual Clip* that can be streamed directly from a monitoring application (such as the Cisco VSM Operations Manager or Cisco SASD). See "Clipping Support By Application" for the clip formats supported by each application in this release.

Refer to the following topics for more information:

- Clipping Support By Application, page 2-16
- Supported File Formats And Playback Options, page 2-17
- Creating Video Clips, page 2-19
- Downloading and Viewing Clips, page 2-23

Tip

- You can also search for and download clips using the **Clip Search** feature in Operations Manager/Cisco VSM Federator and the **Clip Management** feature in Cisco SASD/Cisco SASD Federator.
- Timestamps are not displayed in 3rd-party video viewers. use the Cisco Review Player to play video clips that display timestamps (see the Cisco Video Surveillance Review Player User Guide for more information).
- Maintenance Mode must be *off* to create clips using Thumbnail Search or Clips Search (the pencil icon in the top right must be yellow).

Clipping Support By Application

You can create and view video clips using the following Cisco VSM applications:

Table 3 Video Clip Support

Application	Create MP4 Clips	Create CVA Clips	Create Virtual Clips	View MP4 Clips[1]	View CVA Clips	View Virtual Clips	Clip Search Feature
Cisco VSM Operations Manager	Yes	Yes	Yes	Yes	No	Yes	Yes
Cisco VSM Federator	Yes[2]	Yes	No	Yes[3]	No	Yes[4]	Yes
Cisco SASD	Yes	Yes	Yes[5]	Yes	No	No	Yes[6]
Cisco SASD Federator	Yes[7]	Yes	No	Yes[8]	No	No	Yes[9]
Cisco VSM Review Player	No	No	No	Yes	Yes[10]	No	No

1. MP4 clips are saved to the server and play immediately after being downloaded to the monitoring PC. Third-party video players (such as VLC) can also be used to view MP4 clips.
2. Create MP4 clips using the Federator Thumbnail Search.
3. Federator clips must be downloaded and played using either Cisco Review Player or VLC.
4. Double click the virtual clip in Federator Clip Search to play the virtual clip.
5. Thumbnail Search supports MP4 clip creation only.
6. Cisco SASD does not support Virtual Clip search in this release.

7. Create MP4 clips using the Federator Thumbnail Search.
8. Federator clips must be downloaded and played using either Cisco Review Player or VLC.
9. Cisco SASD Federator supports MP4 clips only in this release (virtual clip search is not supported).
10. CVA files can only be opened in applications that support the CVA format (such as the Cisco Review Player).

Supported File Formats And Playback Options

Video clips can be created in multiple formats:

- MP4 and CVA video files can be saved to a local disk for playback using the Cisco VSM Review Player or a third party player.
- Virtual clips can be stored on the Cisco VSM server for playback using supported applications, such as the browser-based Operations Manager.

Note Users can select id audio should be included when saving MP4 clips. MP4 clips can also be saved without audio. Audio is not supported in virtual clips, and audio cannot be included when saving MP4 files from a virtual clip.

Table 4 describes the video clip options:

Table 4 Video Clip File Formats

File Format	Description
Virtual clip	Defines a segment of video on the Cisco VSM server for playback using a supported application, such as the browser-based Operations Manager. **Notes** • In this release, Virtual Clips can be created using the Operations Manager and Cisco SASD, but not Cisco VSM Federator or Cisco SASD Federator. See the "Clipping Support By Application" section on page 2-16. • Virtual clips can be any length. There is no maximum duration for a virtual clip. • Virtual clips do not support audio recording. • Virtual clips can be saved as an MP4 file (the 10 hour MP4 limitation applies). Audio cannot be included when saving MP4 files from a virtual clip.

Table 4 Video Clip File Formats (continued)

File Format	Description
MP4	MP4 clips are saved on the server and can be downloaded to a PC workstation or local disk. MP4 clips support a single video pane and can include audio (CVA/CVX files do not support audio). MP4 is a standard video file format that is playable on most computers and useful for sending to 3rd parties. **Audio Support** • MP4 clips can be saved with or without audio. The audio options are selected when the clip is saved. • MP4 audio playback is supported only with the Cisco VSM Review Player or VLC media player. **Notes** • In this release, MP4 clips can be created using the Operations Manager and Cisco SASD. To create MP4 clips using the Cisco VSM Federator or Cisco SASD Federator, use the Clip Search and Clip Management features. See the "Clipping Support By Application" section on page 2-16. • 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. • You can also use the **Clip Search** feature to view, download and delete MP4 clips saved to the server. • The maximum duration for an MP4 clip is 10 hours per clip. • MP4 clips require that the clipping repository be selected on the Media Server associated with the camera. See the "Partition Settings" section on page 9-6. • MP4 clips are saved on the server for 7 days and are automatically deleted from the server 7 days after creation. To download the clips to a local drive, use the **Get Clips Status** menu (see also the "Downloading and Viewing Clips" section on page 2-23). • Up to five MP4 clips can be created at a time per Media Server. If the limit is reached, wait for a clip to complete before creating a new one. • 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. • 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	A Cisco video archive (CVA) can include multiple video panes that synchronize to the same time. CVA/CVX clips are downloaded immediately and not stored on the server. CVA files can only be opened in applications that support the CVA format (such as the Cisco Review Player). **Notes** • The maximum duration for a CVA clip is 24 hours per clip. • CVA files do not support audio playback.

Table 4 Video Clip File Formats (continued)

File Format	Description
CVX	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. **Notes** • CVX video playback will shut down if the file is tampered with. • CVX files do not support audio.

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 2-27 for more information.

Creating Video Clips

To create a video clip, create a bookmark span and select the clip 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.

File Formats Supported by the Monitoring Applications

Review the "Clipping Support By Application" section on page 2-16 for information on the clip formats supported by each application in this release.

Procedure

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

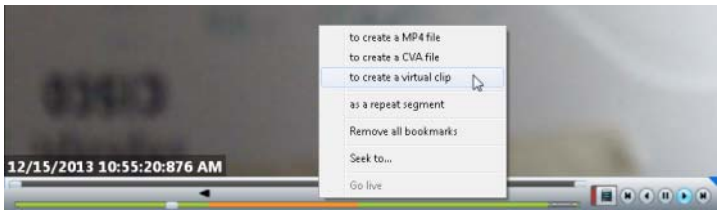
Tip To create a multi-pane clip in the CVA format, press *Shift-Click* to select multiple concurrent panes, or *Ctrl-Click* to select individual panes.

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 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 2-27). 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 MP4, CVA or virtual clip (Figure 6).

Figure 6 Creating a Video Clip



Tip See "Clipping Support By Application" for the file formats supported by each Cisco monitoring application in this release.

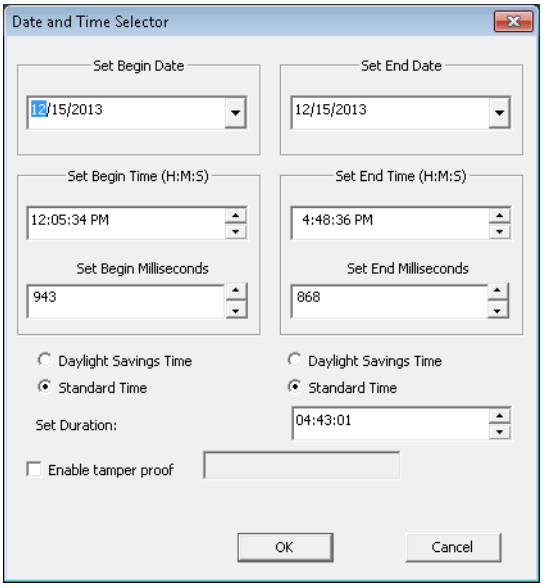
Step 4 Save the file:

CVA/CVX files

a. (Optional) Revise the start and end date and time (Figure 7). Enter a time between 30 seconds and 24 hours (the range cannot include more than one codec and the start time must be before the end time).

Tip Use the Set Duration field to enter a specific length of time for the clip. The duration begins at the beginning bookmark time.

Figure 7 CVA Clip Settings



b. (Optional) Select **Enable tamper proof** and enter a password to create a password-protected CVX file (Figure 7).

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.

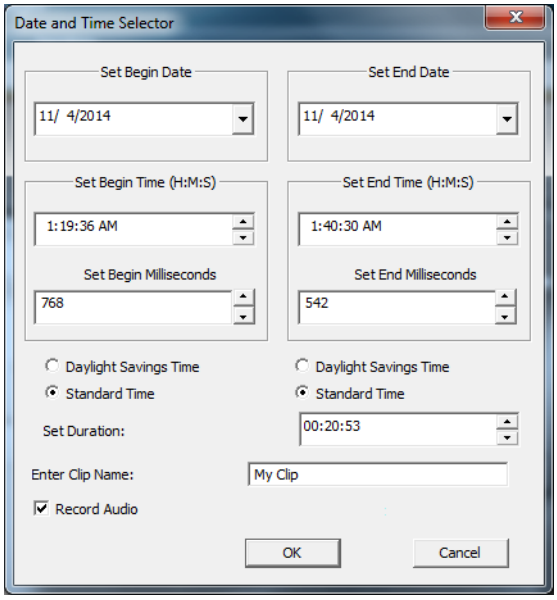
f. Play the clip using a video player such as the Cisco Review Player.

MP4 clips

a. (Optional) Revise the start and end date and time (Figure 8). Enter a time between 30 seconds and 10 hours (the range cannot include more than one codec and the start time must be before the end time).

Tip Use the Set Duration field to enter a specific length of time for the clip. The duration begins at the beginning bookmark time.

Figure 8 MP4 Clip Settings



b. (Optional) Enter a clip name that identifies the recording on the server (Figure 8). For example, if you enter “My 4500 Camera” then the clip selection will be “My 4500 Camera”. The default name is “My Clip”.

c. (Optional) Select or deselect **Record Audio** to include or exclude audio.

- This option is available if the camera supports audio and audio is enabled on the template.
- 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.

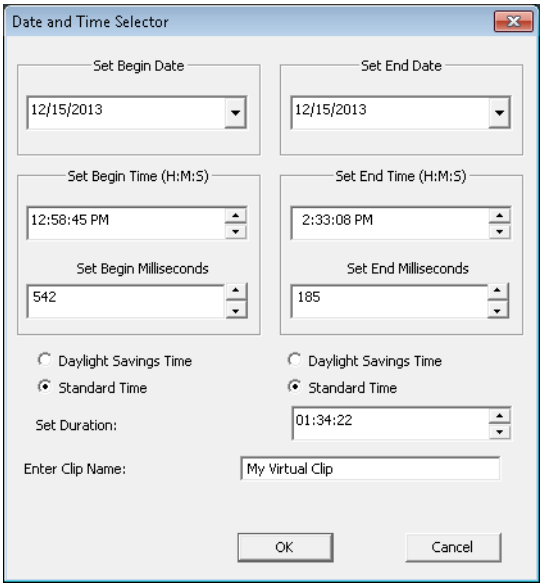
e. Download and play the clip as described in the “Downloading and Viewing Clips” section on page 2-23.

Virtual clips

a. (Optional) Revise the start and end date and time (Figure 9). (the range cannot include more than one codec and the start time must be before the end time).

Tip Use the Set Duration field to enter a specific length of time for the clip. The duration begins at the beginning bookmark time.

Figure 9 Virtual Clip Settings



b. (Optional) Enter a clip name that identifies the recording on the server (Figure 9). For example, if you enter “My 4500 Camera” then the clip selection will be “My 4500 Camera”. If blank, the default name is “My Clip”.

c. 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 “Downloading and Viewing Clips” section on page 2-23.

Downloading and Viewing Clips

Video clip formats are accessed and played in the following ways:

Tip See "Clipping Support By Application" for the file formats supported by each Cisco monitoring application in this release.

Table 5 Video Clip Download Options

Clip Format	Download Options
CVA clips	Downloaded when they are created. Play CVA clips using a supported video player, such as the Cisco Review Player.
MP4 Clips	Right-click the video pane and select **Get Clip Status** (not supported in Federator in this release). Select the clip name from the list and save the file to a local disk (the clip remains on the server for 7 days after it was created). • The clip automatically plays in the video pane when the download is complete. • You can also play the clip using a supported video player such as the Cisco Review Player or VLC. • You can also search for and download MP4 clips using the **Clip Search** feature in Operations Manager or the **Clip Management** feature in Cisco SASD.
Virtual Clips	Right-click the video pane and select **Get Clip Status** (not supported in Federator in this release). Select the clip name from the list to play the clip in the video pane. To download the clip, use the **Clip Search** feature and select the **Virtual Clip Search** tab (if supported by your monitoring application).

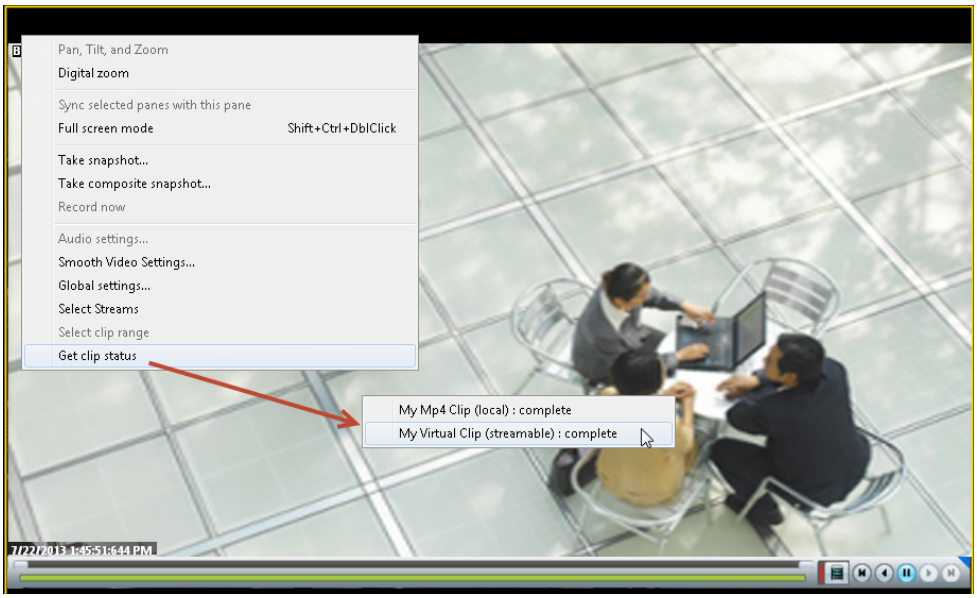
Procedure

Step 1 Right-click the video pane and choose **Get Clip Status** (Figure 10).

Step 2 Select the *Clip* name.

- "Local" clips are MP4 clips that must be downloaded to a local disk.
- "Streamable" clips are virtual clips that can be streamed in the video pane without being downloaded.

Figure 10 Accessing a MP4 Clip



Note Clips are automatically deleted from the server after 7 days.

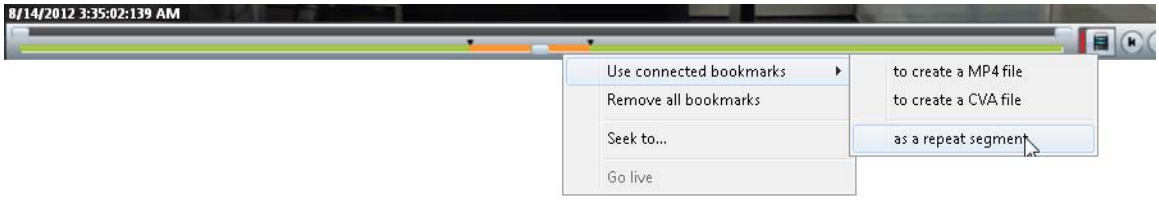
Step 3 (Virtual Clips) The clip plays in the video pane when selected.

Step 4 (MP4 clips only) Enter a file name and location, click **Save**, and wait for the clip to download. The clip will automatically play in the pane the fist time it is downloaded.

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 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 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 and Viewing Video Clips" section on page 2-16 to save the video to a separate file).

Procedure

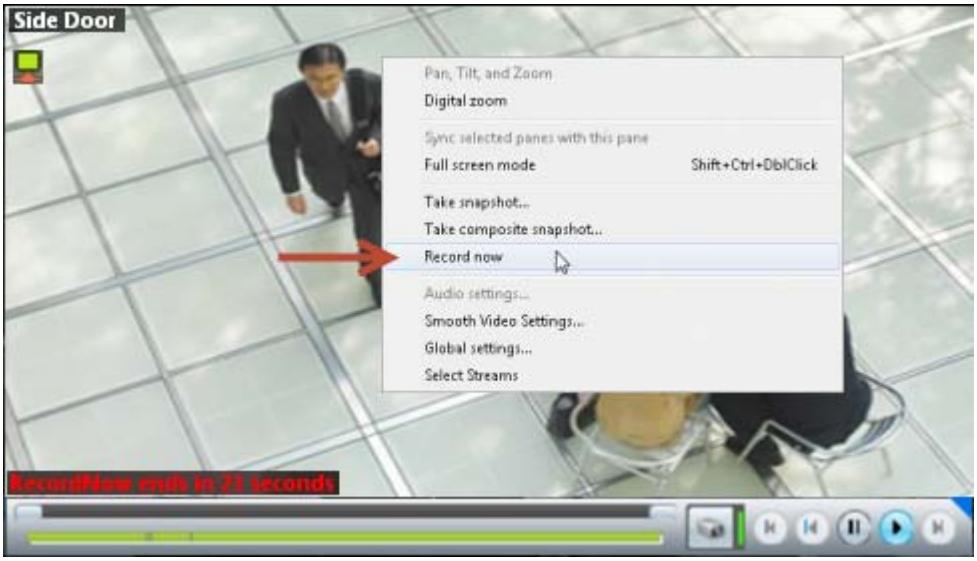
Step 1 Log in to the video viewing application and select a camera.

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 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 12) when the recording time nearly complete.

Figure 12 Record Now

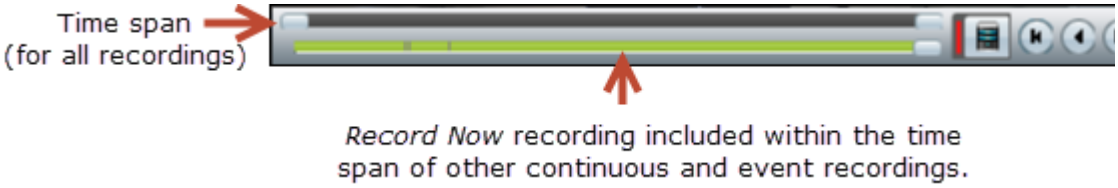


Step 4 To view the recorded video, review the following notes.

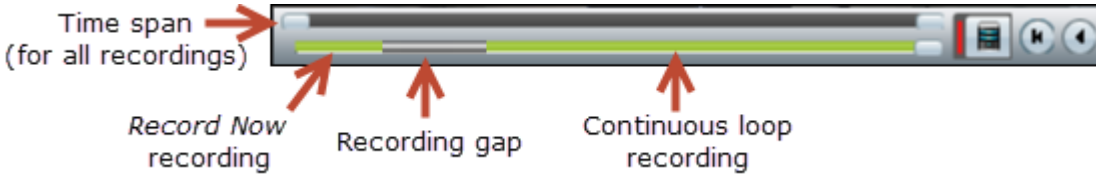
- Record Now clips are available from the primary stream only. Right click the image and choose **Select Streams and Clips** to view the recorded primary stream (disabled if the pane is synchronized).

  Note: Selecting a long term server (LTS) backup recording can result in an error if the recording is not available of the backup is not complete.

- 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 and Viewing Video Clips" section on page 2-16.

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 4 on page 2-9).

Table 6 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 2-38
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 6 Camera Pop-Up Menu (Right-Click the Video Image) (continued)

Camera Menu Item	Description
Sync selected panes with this pane	Synchronizes the playback from multiple video panes to the same time. • 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**. See the "Synchronizing Video Playback in Multiple Panes" section on page 2-34.
Full screen mode	Enlarges the video image to fill the entire monitor screen. **Tip** To exit, press `Esc`, or right-click and choose **Full screen mode** again.
Take snapshot	Saves a snapshot of a single video pane (*excluding* 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 (*including* control icons, timestamps and other information) in BMP, JPEG, PNG, or TIFF format.
Record now	(Live video only) Immediately begins recording video. See the "Using Record Now" section on page 2-26 for more information. **Note** The Record Now option must be enabled in the camera configuration.
Audio settings	(Cameras with audio support only). Opens a window used to adjust video playback volume and balance.
Smooth video settings	(Live video only) Creates a smooth video playback if the playback is choppy or delayed due to network or other performance issues. See the "Using the Smooth Video Options When Viewing Live Video" section on page 2-33.
Global settings	Provides settings that apply to all video panes. For example: *UI transparency* and *zoom video to fit the pane*.
Select Streams	Allows you to select the live and recorded video streams (primary or secondary) supported by the camera. **Note** *Select Streams* is disabled when the pane is synchronized. See the "Synchronizing Video Playback in Multiple Panes" section on page 2-34 for more information. **Note** Selecting a long term server (LTS) backup recording can result in an error if the recording is not available of the backup is not complete.
Select clip range	(Archive video only) Selects a 10 minute clip range starting from current thumb position. The range bar is automatically scaled to 1 hour. See the "Creating and Viewing Video Clips" section on page 2-16 for more information.
Get clip status	Shows the current status of MP4 and virtual clips: In-Progress, Completed or Failed. Select a clip name to view the clip. MP4 clips are downloaded to a local disk (you are prompted to enter a filename and location. See the "Creating Video Clips" section on page 2-19 for more information.

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 7 describes the meaning of each color.

Table 7 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 Privacy Mask

Overview

When the Privacy Mask is enabled on a compatible camera (Figure 13), all live video from that camera is blocked and cannot be viewed by any operator or monitor, or recorded by the Cisco Video Surveillance system. This feature is typically used with the "Virtual Sitter" feature for health care providers, allowing operators to temporarily block video from a Cisco Video Surveillance camera when the patient requires privacy. Figure 13 shows the icons used to enable or disable the Privacy Mask.

Note You must belong to a User Group with *Control Privacy Mask* access permissions to use this feature.

Figure 13 Privacy Mask Controls

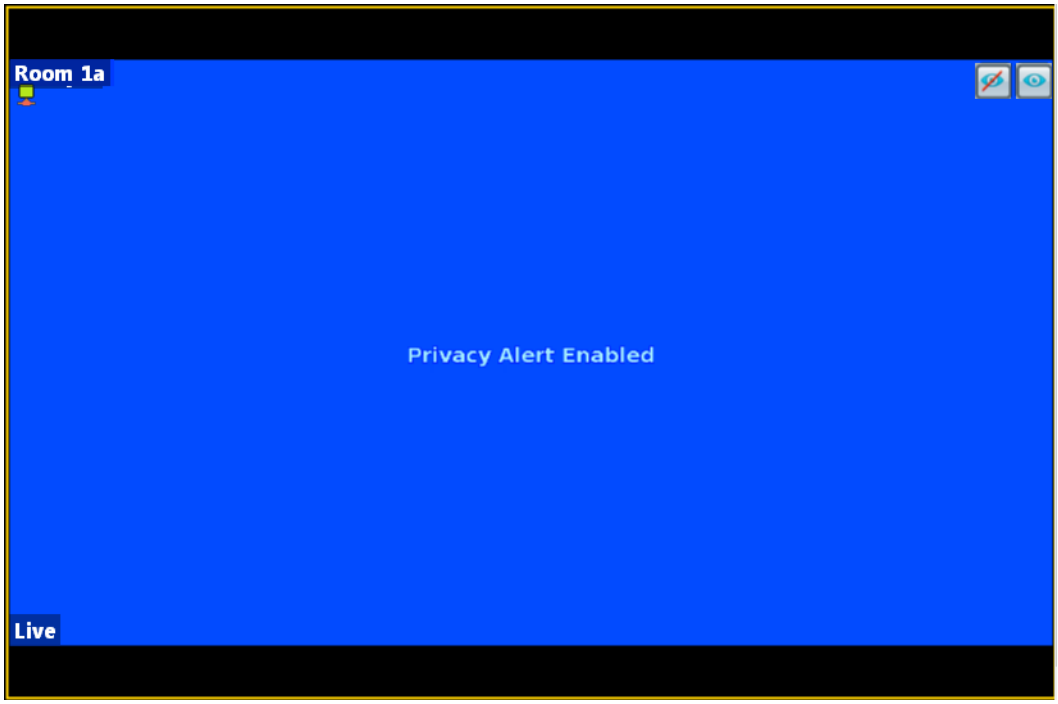
Note The function of the privacy mask icons was reversed in Cisco VSM release 7.5.

Click the privacy icons to turn the video on or off:

Icon	Purpose	Description
	Turn the Privacy Mask off (Default)	Click to enable normal video streaming, monitoring, and recording.
	Turn the Privacy Mask on	Click to block the camera's entire field of view and display a blank (blue) screen (Figure 14). • Live video is not transmitted and cannot be viewed by any workstation or monitor. • Recorded video displays the blank (blue) or flashing screen. • A "Privacy Mask Timer" causes the screen to flash after a period of time, which reminds the operator to disable the Privacy Mask. The default timer is 15 minutes and can be modified using the Operations Manager (**System Settings > Settings > Privacy Mask Timer**). **Note** The Privacy Mask is not disabled automatically; an operator must disable the Privacy Mask by clicking the icon to allow live video to be transmitted, viewed and (optionally) recorded.

For example, when you click the icon, the video frame for that camera is blank (Figure 14). The same blank (blue) screen is recorded (if recording is configured).

Figure 14 Privacy Mask Enabled



When the Privacy Mask Timer expires, the video frame flashes to remind the operator that the mask is still on. To display video, click to turn the Privacy Mask off and display and record video normally.

Note If the camera reboots due to a power cycle or other reason, the camera will power up with the Privacy Mask in the state it was before the reboot. For example, if the mask was enabled and there was 5 minutes remaining on the timer, the camera will remember the state after the reboot.

Enabling the Privacy Mask Controls

The Privacy Mask controls (icons) are displayed only for users who belong to a User Group with *Control Privacy Mask* access permissions. This operator permission is de-selected by default, so you must create a user role, user group, and use that includes *Privacy Mask*:

Step 1 Log is as a admin or other user who has *Users & Groups* access permissions.

Step 2 Create a Role that includes *Control Privacy Mask* access permissions.

Step 3 Create a user group and assign the new role to the group.

Step 4 Create users and assign them to the user group.

Tip See Adding Users, User Groups, and Permissions, page 4-1 for more information.

Related Information

Supported cameras can also be configured with "Privacy Zones" that block portions of the video image at all times, even if the Privacy Mask is disabled. See the camera documentation for instructions to define Privacy Zones.

For more information about Cisco Virtual Patient Observation, see the following:

- White Paper—Virtual Patient Observation: Centralize Monitoring of High-Risk Patients with Video.
- At-A -Glance Overview—Benefits of Virtual Patient Observation.
- Ten Use Cases—Real-life scenarios for using video surveillance in hospitals.
- Solution Blog Post—New Solution: Cisco Virtual Patient Observation.

Cameras that Support the Privacy Mask

See the Release Notes for Cisco Video Surveillance Manager for the cameras that support the privacy mask feature in your release.

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 15 describes the main synchronization attributes.

Figure 15 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 . Click the icon to enable PTZ (the icon is blue when enabled, and do one of the following:

- To pan and tilt, hold down the left mouse button while dragging the mouse right, left, up and down (the icon appears).
- To zoom:
  - Hold down the left mouse button and use the scroll wheel to zoom in and out.

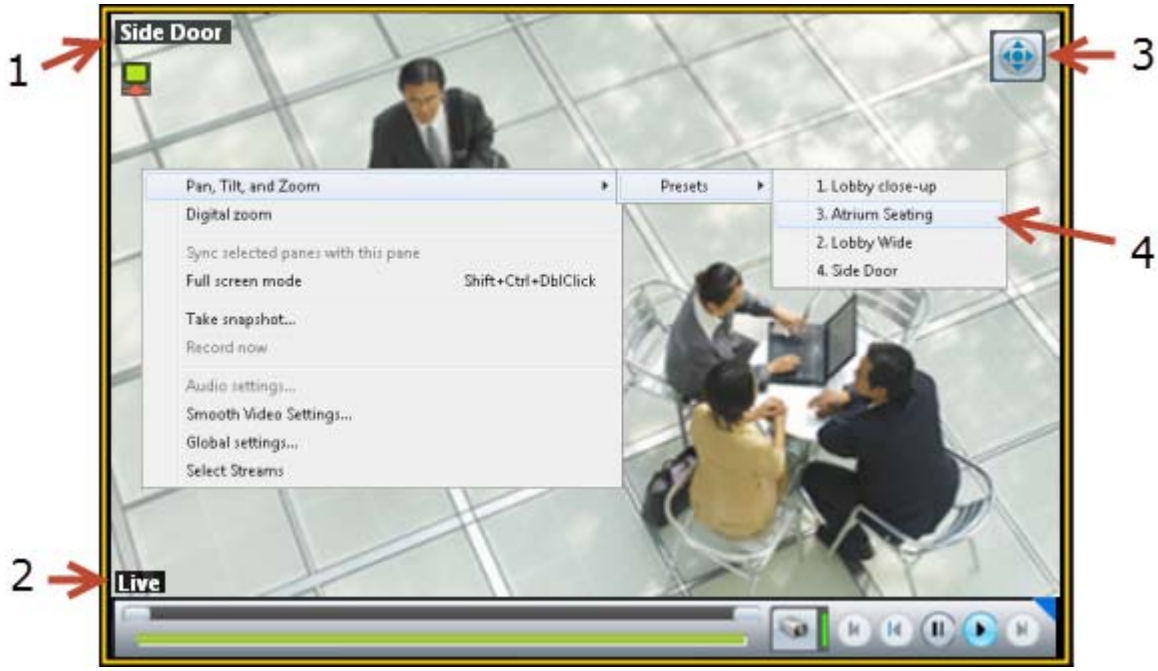
    or
  - Hold down the Shift key and then press the left mouse button. Drag the mouse up or down to zoom.

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.

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 16 summarizes the controls and information available on each PTZ camera viewing pane.

Figure 16 Camera PTZ Controls



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

PTZ Usage Notes

- To use a USB joystick, see the "Calibrating a Joystick for Windows 7" section on page 2-41.
- 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 2-43.
- 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). See the "High Availability: Cisco Media Servers" section on page 17-1 for more information.

PTZ Control 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 Click the PTZ control icon to enable PTZ:

- —(Blue) PTZ controls are supported by the camera and enabled in the viewing pane.
- —(Grey) 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—Hold down the left mouse button while dragging the mouse ( ) right, left, up and down.
- Zoom—
  - Hold down the left mouse button and use the scroll wheel to zoom in and out.

  or
  - Hold down the Shift key and then press the left mouse button. Drag the mouse up or down to zoom.

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 2-41 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** > **Presets** (Figure 16).
- 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.

Tip If Return to Home is configured, the camera will return to a default "home" PTZ location after a specific number of seconds. See "Understanding Return To Home".

Understanding Return To Home

Cameras can be configured with a Return To Home feature that automatically returns the camera to a "home" PTZ position after a specific number of seconds.

Workstations can also be configured to display a warning before the camera returns to home, which allows you to cancel the operation and reset the timer, if necessary (Figure 2-17):

Figure 2-17 Return To Home Warning

See your Cisco VSM administrator for more information about these features.

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 18). 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 18 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		

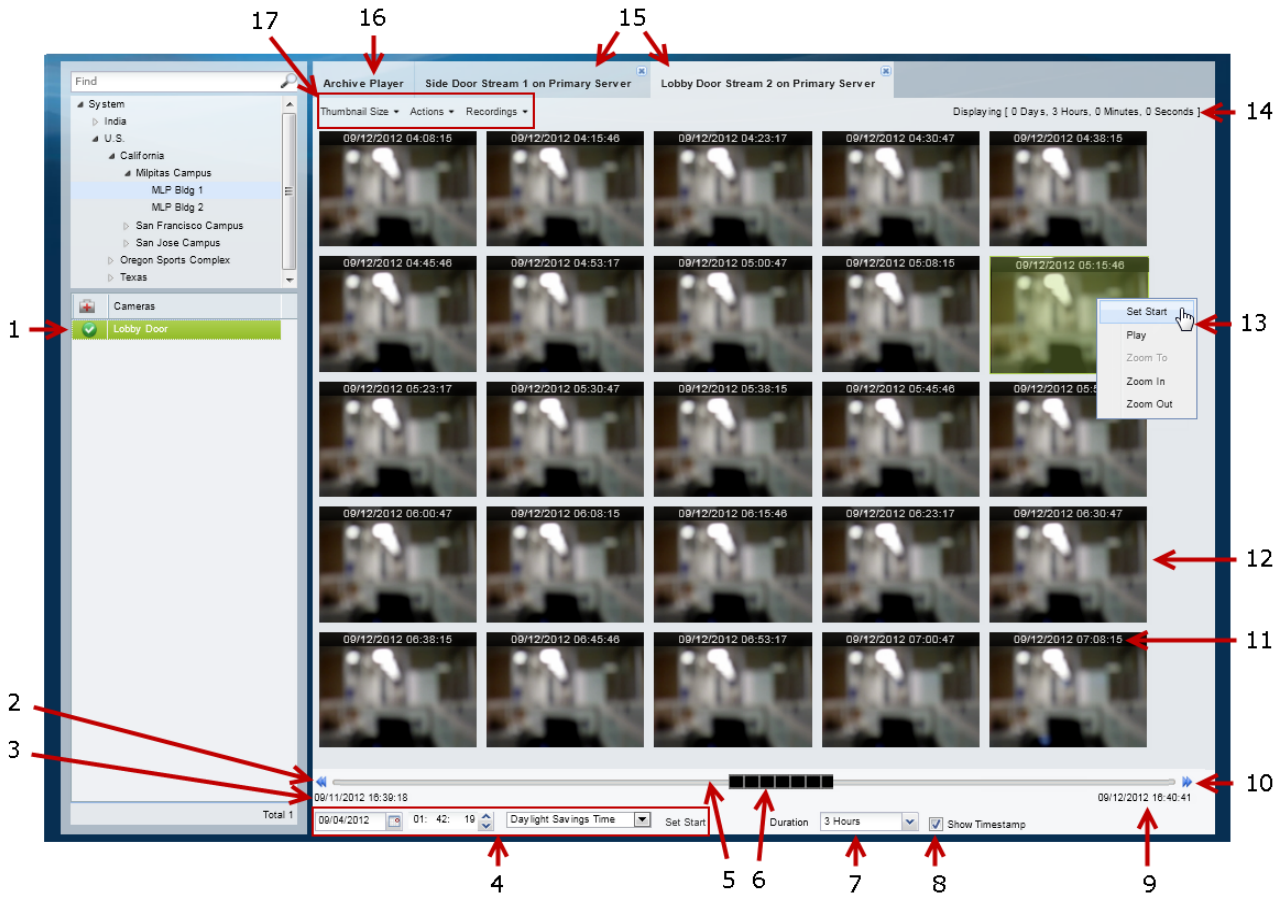
Note PTZ movements are available only when viewing live video.

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

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 2-19 provides an overview of the search and display controls. See the "Using Thumbnail Search" section on page 2-46 for step-by-step instructions.

Figure 2-19 Thumbnail Window



1	Selected Camera	Select a location and double-click a camera name to display a thumbnail summary of recorded video for the camera. **Note** Cisco VSM Federator locations are "Regions" that are linked to an Operations Manager location. See the "Using Federator to Monitor Multiple Operations Managers" section on page 22-1 for more information. • 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 *Archive Player* 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	The start date and time for the entire video archive. See #4 to select a new start time, or right-click a thumbnail and choose **Set Start**.
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	**Thumbnail Size**—select a smaller size to display more thumbnails for the displayed video duration. Select a larger size to display fewer thumbnails. **Recordings**—select a video stream or recording. **Actions**—choose one of the following options: **Note** You can also right-click a thumbnail to access the **Actions** (see #13). • **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 *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 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 2-19).
2. Select a location and double-click a camera name.
3. Use the tools described in Figure 2-19 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** (Thumbnail Search) to open the forensic search window (Figure 2-19).

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 2-19 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 (12/04/2012 10: 03: 55 Standard Time Set Start) and click **Set Start**. The thumbnail for the selected date and time is displayed in the top left corner (you can also right0click a thumbnail and choose **Set Start**).
- Choose the **Duration** (Duration 3 Hours) 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 (09/03/2012 23:36:12) 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 be set to the end of the archive minus the duration.

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

Clip Search

Select **Clip Search** from the **Monitor Video** window (Figure 2-20) to view, download and delete MP4 and virtual clips.

Tip You can also create and download clips by right-clicking a video pane. See the "Downloading and Viewing Clips" section on page 2-23.

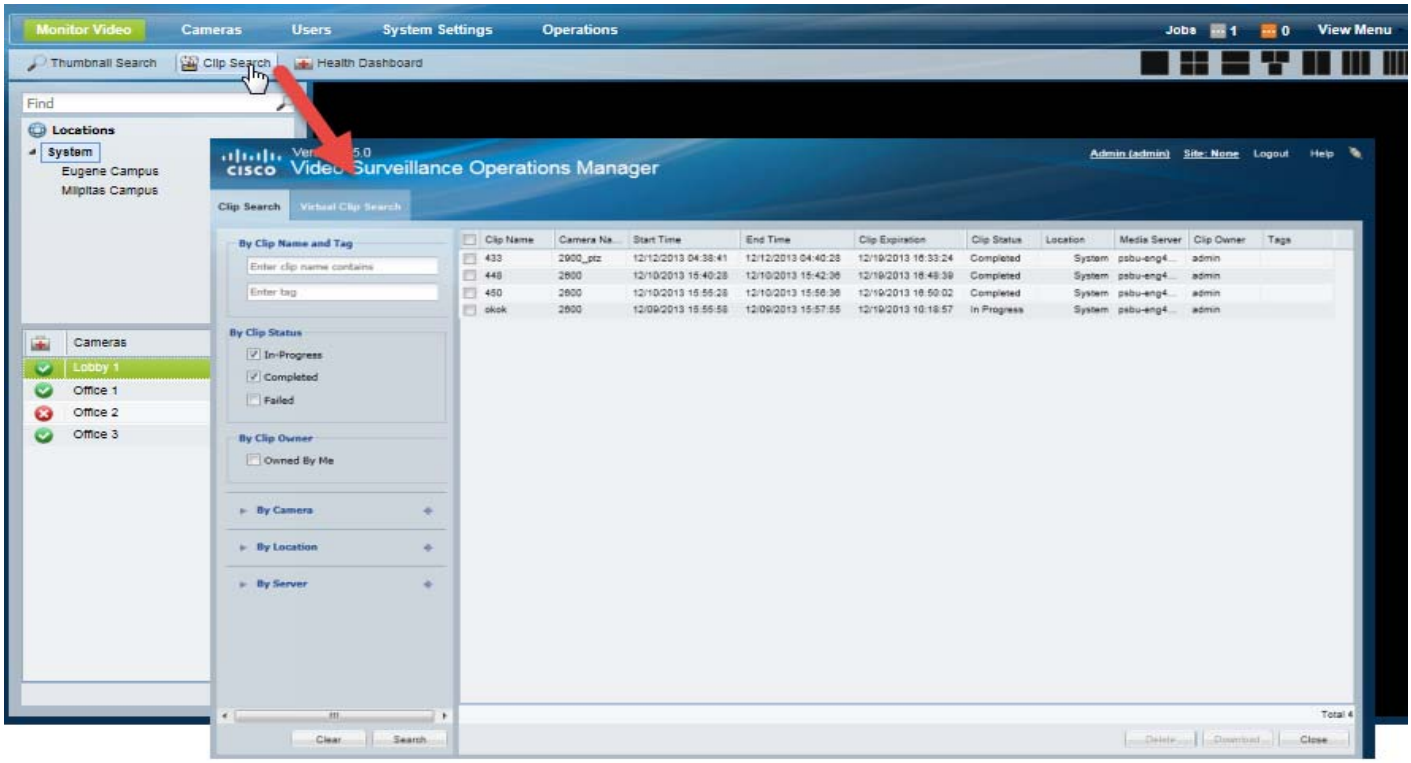
Procedure

Step 1 From the **Monitor Video** page, click **Clip Search** to open the Clip Search window (Figure 2-20).

Step 2 Select the clip type:

- **Clip Search** tab—MP4 clips
- **Virtual Clip Search** tab—Virtual clips

Figure 2-20 Clip Search Window



Step 3 (Cisco VSM Federator only) Select a region where the clip(s) were created. Only clips from the Operations Manager location mapped to that region will be displayed.

Step 4 (Optional) Use the filters to search for specific clips (Table 2-8):

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

By Clip Name	The full or partial name for the clip(s), which is entered when the clip is created
By Tag	Tags associated with the clip.
By Clip Status	Select the status for the displayed clips. Any status not selected will not be displayed.
By Clip Owner	Select **Owned by me** to display only clips you created De-select to display clips created by other users.
By Camera	The camera name where the clip originated.
By Location	Clips created by all cameras at the selected location(s).
By Server	Clips created by all cameras associated with the selected servers(s).

Step 5 Click **Search**.

Step 6 Review information about the clips.

Table 2-9 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.

Step 7 (Optional) To download an MP4 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 8 (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.

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

Additional Documentation

- Configuring Camera PTZ Controls, Presets, and Tours, page 10-67
- Configuring Motion Detection, page 10-82
- Editing the Camera Settings, page 10-42
- Adding and Editing Camera Templates, page 12-1

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 Video Views" section on page 3-4.

Step 2 Select **Monitor**.

Step 3 Select a location and select a View (Figure 3-1).

Figure 3-1 Select a View

Step 4 Select **View Menu** > **Set Default View** (Figure 3-2).

Step 5 Select a location and View from the pop-up window.

Step 6 Click **Select**.

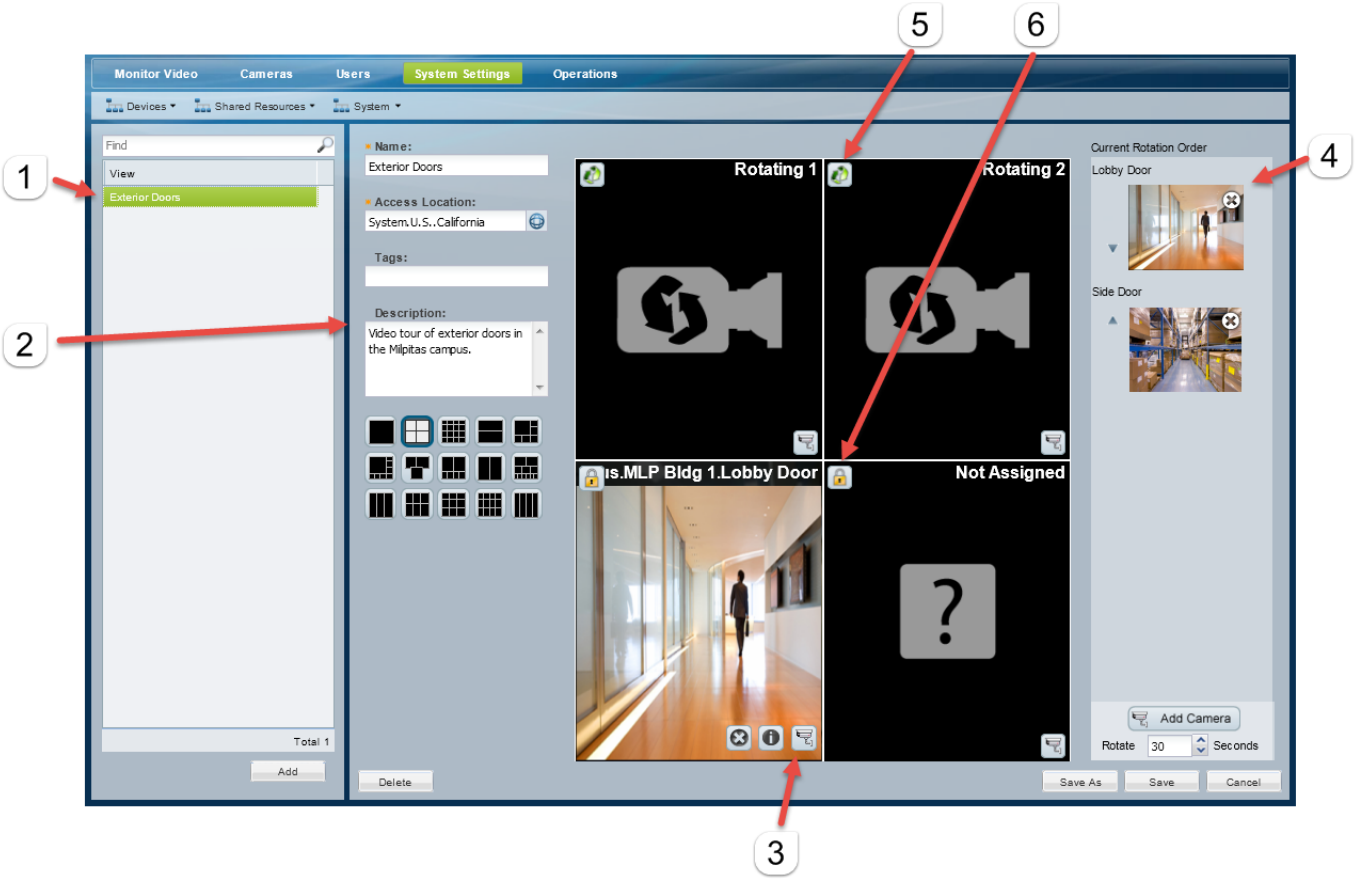
Figure 3-2 Setting the Default View

Creating Video Views

Views are pre-defined sets of video panes that can be displayed in either the Operations Manager *Monitor Video* page, or the Cisco Video Surveillance Safety and Security Desktop (Cisco SASD) application. Each view can include up to 16 video panes, and each pane can display video from a single camera (static) or rotate the video from multiple cameras.

For example, you can create a virtual tour of all *Lobby Doors* that includes 4 panes. Three of those panes can rotate the video from 8 cameras to provide a virtual tour of a building. The forth *static* pane can always display video from a single camera.

Figure 3-3 View Configuration



1	Name of the view that is selected by the user.
2	General settings such as the view name, location, description, and layout.
3	Settings for the pane. • Click the camera icon to select the camera source.
4	*Not Assigned* panes do not have a camera assigned to the pane. The video pane will appear blank in the View.

5	Current Rotation Order—Add cameras, and reorder them to define the display order. • Click **Add Camera** (Add Camera) to add the cameras that will rotate between the available panes. • Use the arrows next to each pane to change the order of the rotation.
6	—Rotating camera panes rotate the video between cameras included in the *Current Rotation Order*.
7	—Static camera panes always display video from the same camera, even if the other panes rotate video from multiple cameras.

Usage Notes

- Use the Cisco Video Surveillance Safety and Security Desktop application to create and save basic views that can be accessed using the Monitor Video page. The panes in a basic *View* are static and do not rotate.
- 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).

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** > **Views**.

Step 3 Edit or add a *View*:

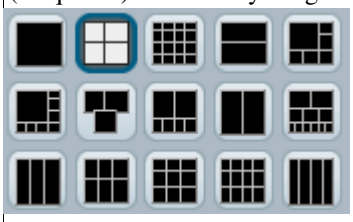
- To edit a View, select an existing entry.
- To add a View, click the **Add** button.

Step 4 Enter the basic View properties:

Table 3-1 Basic View Properties

Setting	Description
Name	(Required) enter a descriptive name for the View. For example: *Exterior Doors*.
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 *access location*, 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 *Find*.
Description	(Optional) enter a meaningful description for the View. For example: *Lobby Tour*.

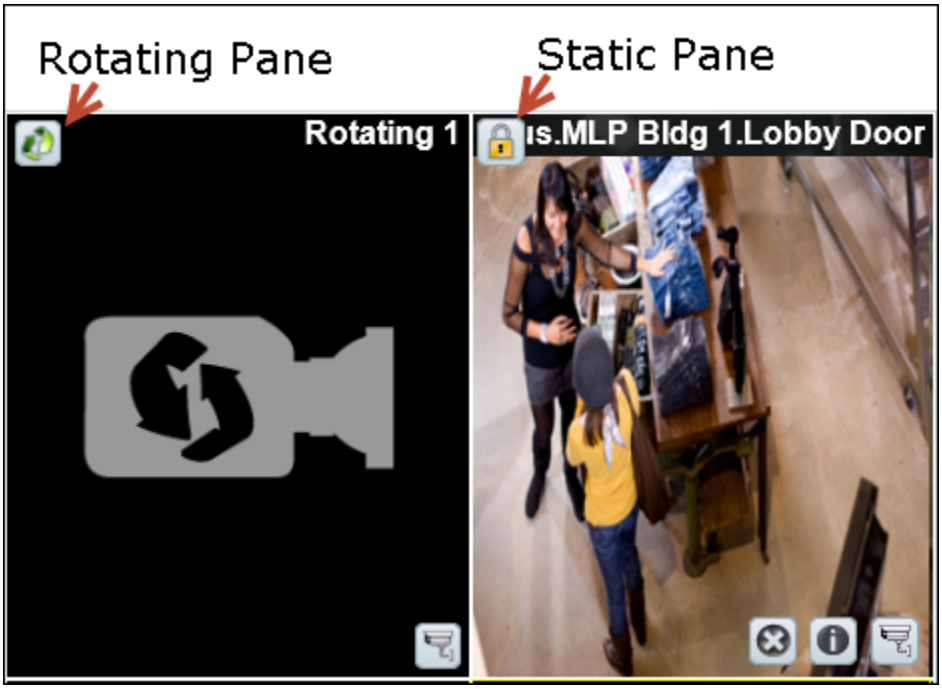
Table 3-1 Basic View Properties (continued)

Setting	Description
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



a. Click the icon to toggle the pane to static , if necessary (Figure 3-4).

b. Click the camera icon.

c. Select a camera from the Camera Selector location tree and click **Set**.

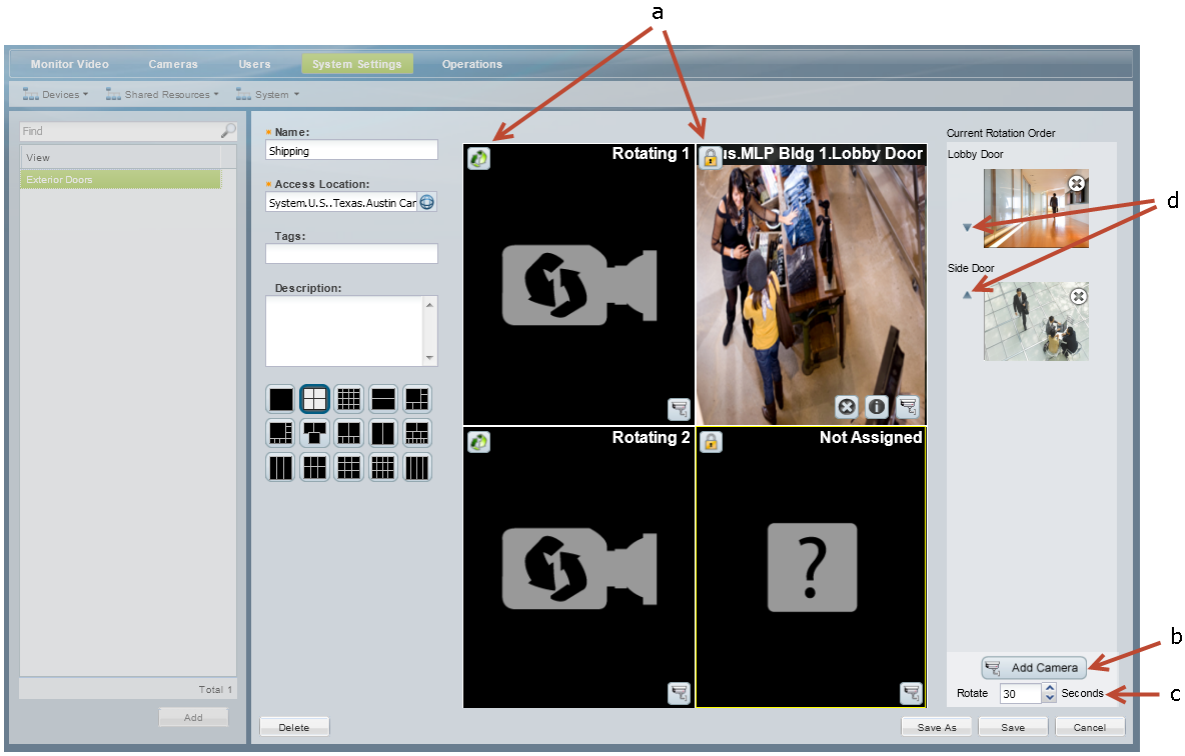
d. Repeat these steps for each additional static video pane.

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** (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**.

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.
  - Users who configure unattended video walls (using the Cisco SASD Wall Configurator) must belong to a user group that allows multiple logins. This is because each unattended video wall requires a unique Cisco VSM login session for the video wall to be displayed. See the Cisco Video Surveillance Safety and Security Desktop User Guide for more information.
- To automatically display video from a different camera when an event occurs, see the "Using Advanced Events to Trigger Actions" section on page 13-7. 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	SASD users can view Video Wall that are assigned to the same location or lower. 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. See the "Creating the Location Hierarchy" section on page 5-1for more information.
Default View	(Optional) The *View* displayed when a Video Wall is selected in the SASD application. • 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 *rollback time* 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 *Push Video to Wall* permission. **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. Refer to the *Cisco Video Surveillance Safety and Security Desktop User Guide* for more information.
Rollback Time	The amount of time that an alternative *View* 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 13-7.

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

a. Launch the SASD application and log in.

b. Select a Video Wall from the **Wall** menu.

c. (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: Cisco Media Servers" section on page 17-1 for more information.

Using Record Now

See the "Using Record Now" section on page 2-26 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 12-1 and the "Streaming, Recording and Event Settings" section on page 10-48.

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**.

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

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.

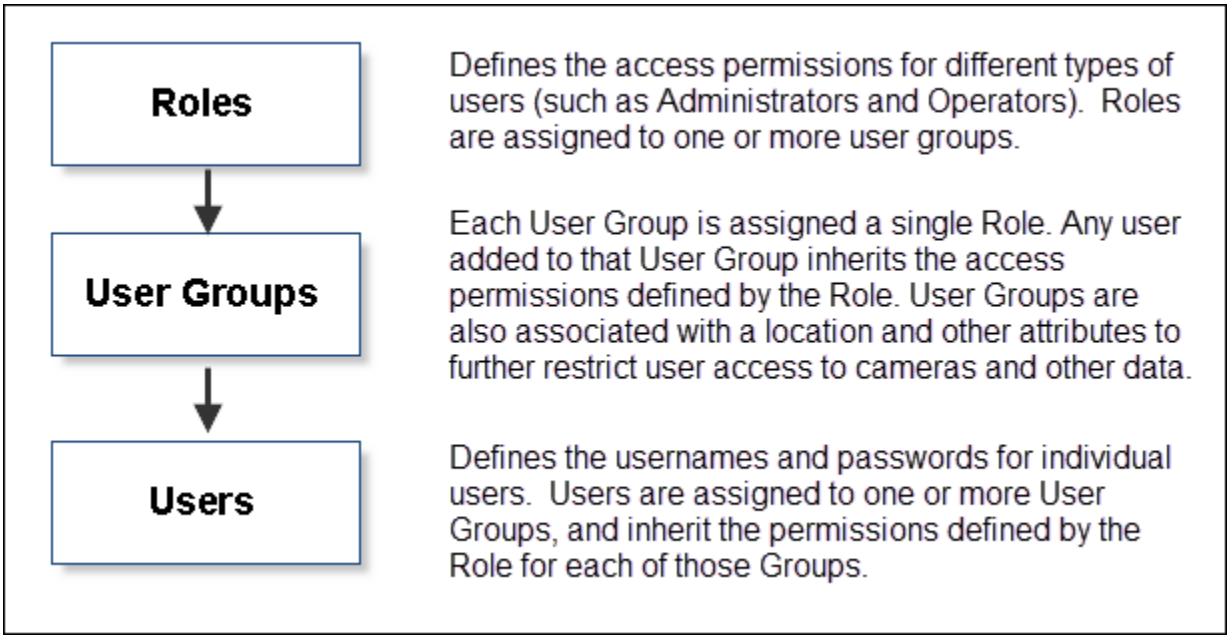
Tip A second user (such as a manager) can also be required to approve when a user logs in. See the "Understanding Dual Login" section on page 1-20.

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

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	• *super_admin_role*—includes all management and operation access permissions. • *local_admin_role*—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. • *operator_role*—provides all operator permissions.
User Groups	• *super_admins*—assigned the *super_admin_role*. • *operators*—assigned the *operator_role*.
Users	• *admin*—assigned to the *super_admins* user group, which gives the user *super_admin_role* permissions. The admin is a root system user and cannot be modified or deleted. The default admin username and password is **admin/admin**. **Note** A *super-user* is anybody that has all permissions at the root location. • *operator*—assigned to the *operators* user group, which gives the user *operator_role* permissions. The default username and password is **operator/operator**. **Note** A *local-admin* user account is not included by default. You must add a user and add them to a user group associated with the *local_admin_role*, if necessary.
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 4-18 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.

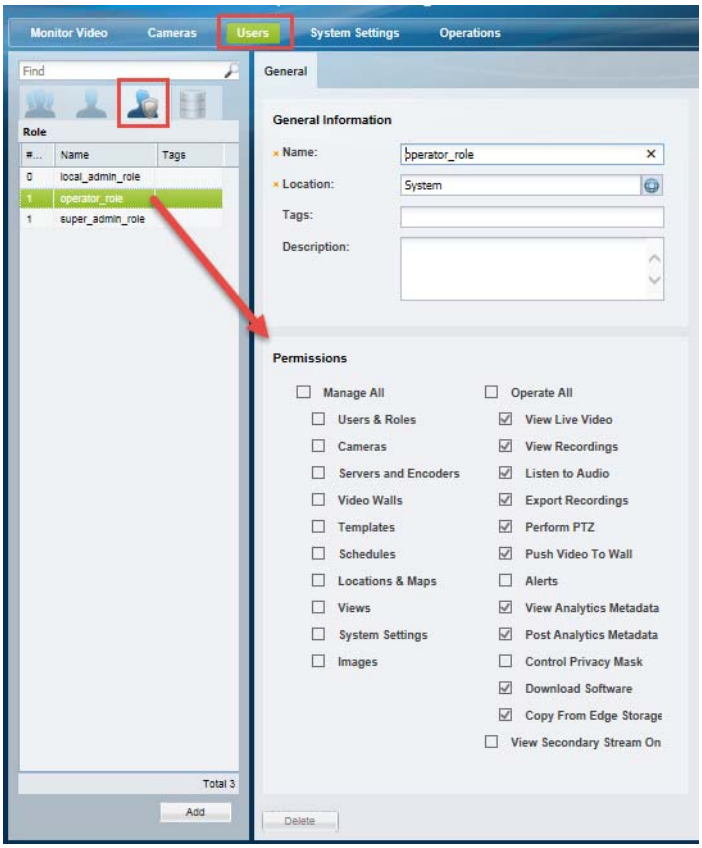
Default Roles

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 4-9 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 4-9 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 *Pending Approval* functions.	Adding and Managing Cameras, page 10-1
Servers & Encoders	Create, update, or delete Cisco VSM severs and analog camera encoders.	Configuring Media Server Services, page 9-1 Adding Encoders and Analog Cameras, page 16-1
Video Walls	Create, update, or delete Video Walls.	Configuring Video Walls, page 3-9
Templates	Create, update, or delete camera templates.	Adding and Editing Camera Templates, page 12-1
Schedules	Create, update, or delete schedules.	Defining Schedules, page 11-1
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.	Setting the Default View, page 3-1 Selecting a Multi-Pane "View", page 2-4
System Settings	Update Cisco VSM system settings.	Revising the System Settings, page 20-1
Images	Allows the user to upload firmware images, define the recommended firmware version, and upgrade devices.	Upgrading Cisco Camera and Encoder Firmware, page 26-19

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 deseleted.

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 10-42
Export Recordings	Export a video clip to a file.	Creating and Viewing Video Clips, page 2-16
Perform PTZ	Use the pan, tilt and zoom controls on cameras that support PTZ.	Using Pan, Tilt, and Zoom (PTZ) Controls, page 2-38
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 3-9 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 (*ack/clear/add_user_comment*).	Cisco Video Surveillance Safety and Security Desktop User Guide
View Analytics Metadata	View the already generated meta data and perform video motion searches (using the Cisco SASD desktop application). Users with only View permissions cannot generate the metadata using Cisco SASD.	Enabling Video Analytics, page 13-2
Post Analytics Metadata	Generate the Metadata using Cisco SASD. Users with only Post permission cannot perform searches.	Enabling Video Analytics, page 13-2

Table 4-3 Operate Permissions (continued)

Operation Permissions	Description	More Information
Control Privacy Mask	Allows operators to enable or disable the Privacy Mask on compatible cameras. All live video from the camera is blocked and cannot be viewed by any operator or monitor, or recorded by the Cisco Video Surveillance system.	Using the Privacy Mask, page 2-30
Download Software	Allows users to download the available software installation packages, such as the Review Player EX, Advanced Video Player, and MSI Installation Package.	• Downloading Cisco SASD and the Cisco Review Player, page B-1 • Configuring Medianet, page 25-1
Copy From Edge Storage	Allows users to copy recording from a camera to the Media Server.	• Copy Camera Recordings (Manually Triggered), page 15-14 • Connected Edge Storage (Camera Recording), page 15-1 • 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 10-42

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

Table 4-4 Sample Roles in a Cisco Video Surveillance Deployment (continued)

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

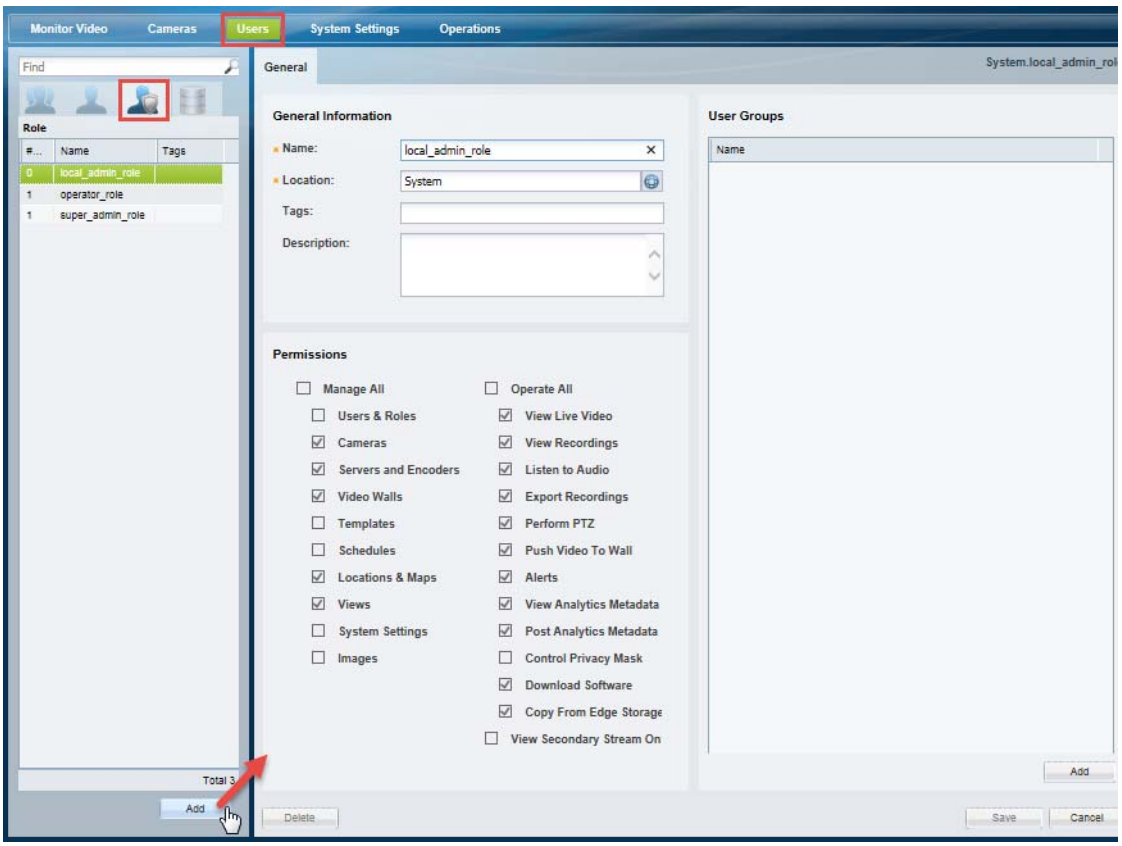
Defining User Roles

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 *Find* 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 4-11 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 4-11 for instructions.

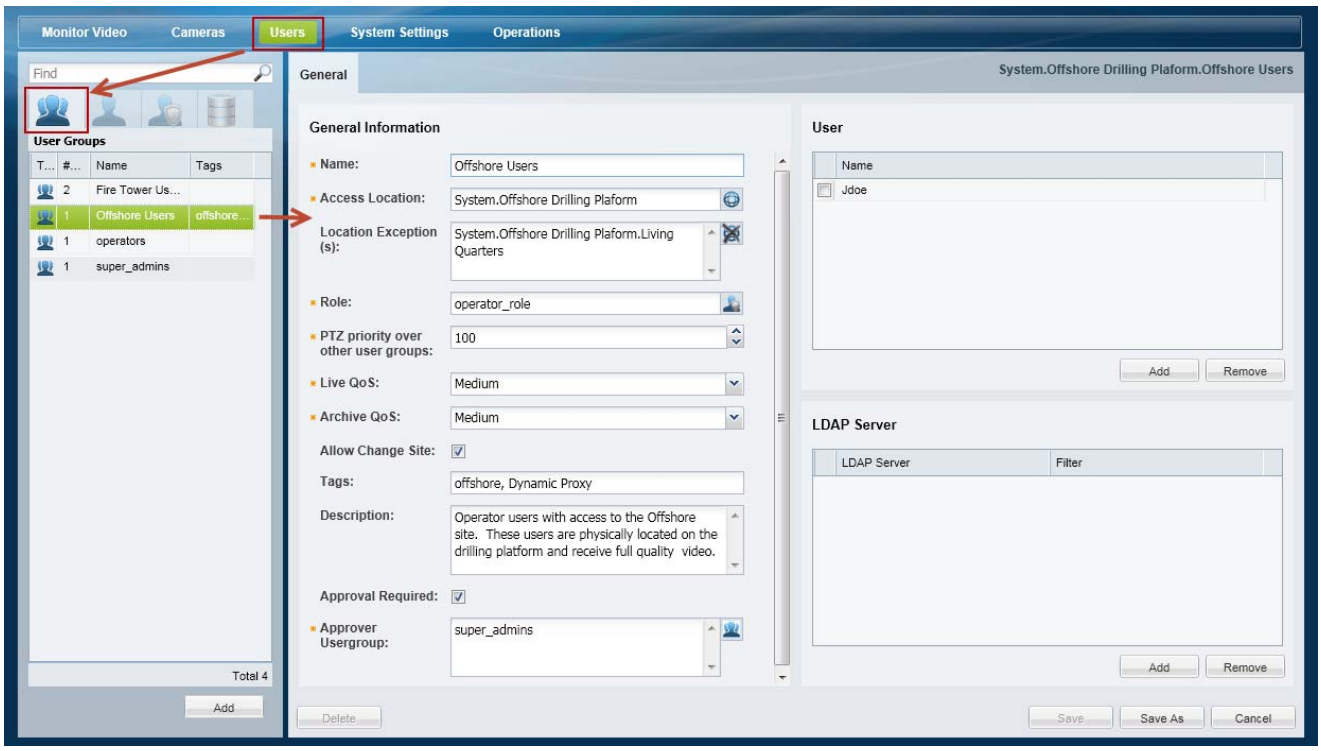
Adding User Groups

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 *except* 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 4-9.
PTZ priority over other User Groups	(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. 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 10-71 for more information. The default is 100 (highest priority). **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. **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 "Configuring Advanced Settings" section on page 10-77.
Live QoS	(Required) Defines the priority of the user group to receive *live* 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. • 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.
Archive QoS	(Required) Defines the priority of the user group to receive *recorded (archive)* 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. • 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)

Allow Site Change	(Optional) Select **Allow Change Site** to allow users to change their Site after logging into the Operations Manager. This option is disabled (deselected) by default when adding a new user group. • Deselect to disable Site changes. Users must log out and log back in to change Sites. • Users can only change Sites if they are assigned to User Groups with access to multiple Sites. • If a user selects the "Not in Any Site" option, then video from cameras in Sites that have the **Dynamic Proxy** option enabled will be streamed from the Dynamic Proxy server. **Note** Users who have access to multiple sites, but do not have the option to change sites, will default to "Not in any site" when logging in. **Note** If a Site's **Dynamic Proxy** option is disabled (deselected), video from cameras at the Site will be delivered to all users by the Site's Media Servers (and not by a Dynamic Proxy server). **Tip** Sites are used to define if you are inside or outside a location served by a Dynamic Proxy server. See the "Understanding Sites" section on page 23-3 for more information. **Defaults** • "Allow Site Change" is *disabled* by default when adding a User Group. • "Allow Site Change" is *enabled* by default for all User Groups when upgrading to r7.5 from a previous release.7.5 (or higher) from a previous release.
Tags	(Optional) Enter keywords used by the *Find* function.
Description	(Optional) Enter a description of the rights granted by the Role.
Approval Required	(Optional) If selected, a second user is required to approve the user login. When the user logs in, a window appears requiring a second user to enter their username and password. See the "Understanding Dual Login" section on page 1-20 for more information.
Approval Usergroup	(Required if **Approval Required** is selected). Select a User Group that can approve logins for members of the Approval Required usergroup.
Allow Multiple Logins	(Optional) Allows users with the same credentials to login from multiple workstations. This setting is enabled by default. **Note** Users who configure unattended video walls (using the Cisco SASD Wall Configurator) must belong to a user group that allows multiple logins. This is because each unattended video wall requires a unique Cisco VSM login session for the video wall to be displayed. See the Cisco Video Surveillance Safety and Security Desktop User Guide for more information.

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 4-15.

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

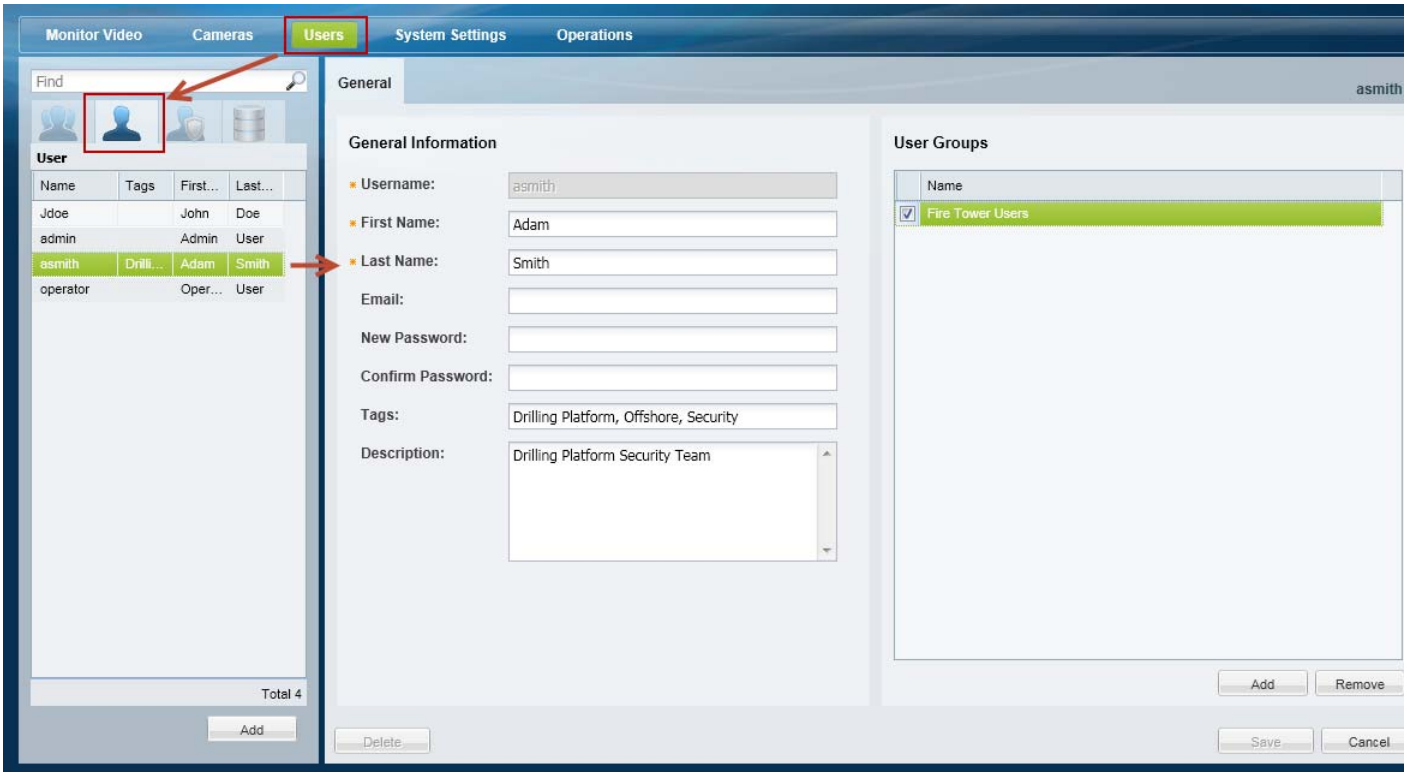
- See the "Adding Users from an LDAP Server" section on page 4-18.

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



Tip A second user (such as a manager) can also be required to approve when a user logs in. See the "Understanding Dual Login" section on page 1-20.

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
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. • The password minimum length is 8 characters and must include 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. **Tips** • See Password Settings, page 20-3 to change password rules such as expiry time and minimum and maximum length. • Only super-admins can use this field to change another user's password. All other users can change their own password by clicking on their username in the top right corner of the browser. • Super-admins can use this field to change their own password. **More Information** • Changing Your Password, page 1-23 • Changing Another User's Password, page 1-23 • Password Settings, page 20-3
Confirm Password	Re-enter the password.
Tags	(Optional) Enter the keywords used by the *Find* 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 4-11 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 4-18
- Upgrade Requirements, page 4-18
- LDAP Server Settings, page 4-19
- LDAP Search Filter Settings, page 4-23
- LDAP Configuration Examples, page 4-23
- LDAP Configuration Procedure, page 4-26

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

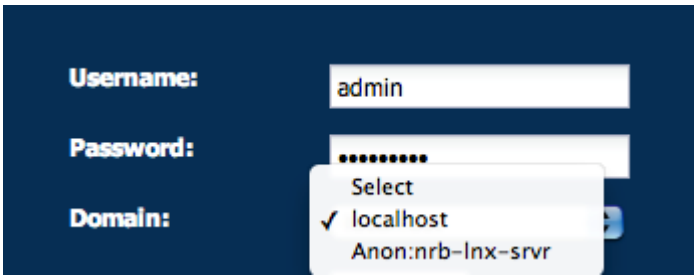
New fields were added in Cisco VSM release 7.0.1 to simplify the LDAP server configuration. After upgrading from release 7.0.0, the administrator must reconfigure the LDAP server settings including the following:

- 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).

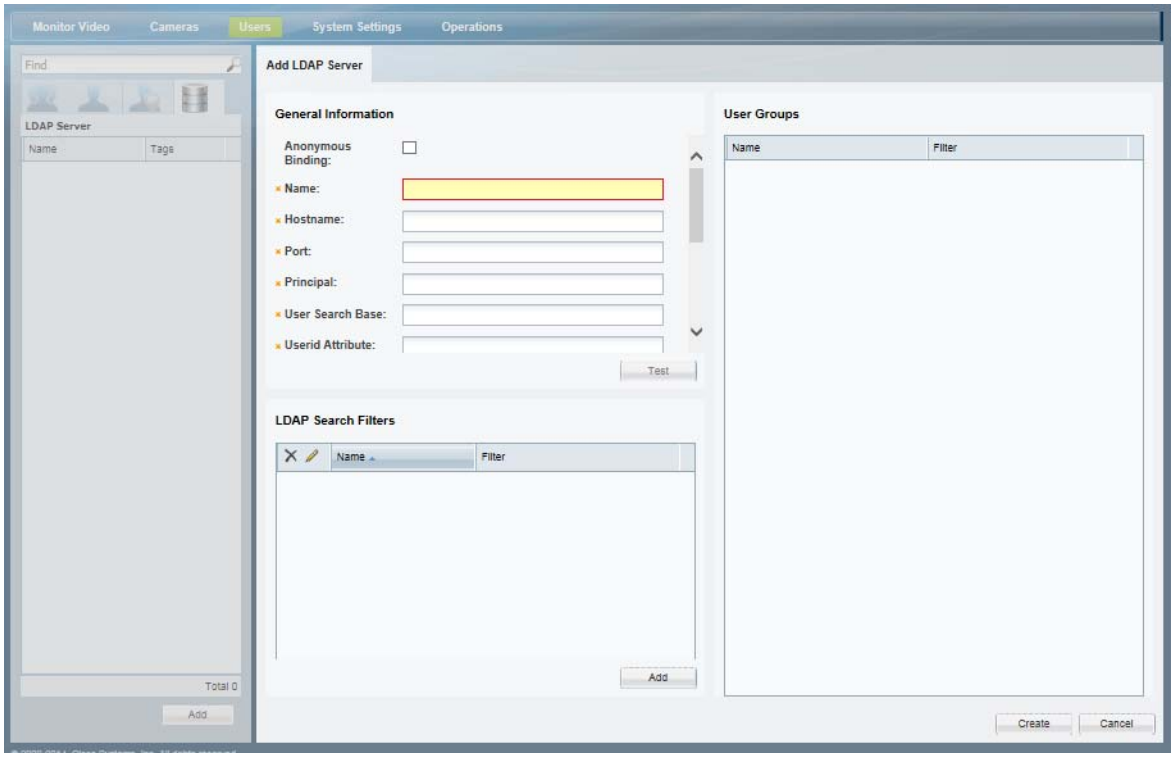
Figure 4-6 Localhost login for LDAP Configuration Changes



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



The following table describes the purpose and requirements for each setting. Refer to the "LDAP Configuration Examples" section on page 4-23 for additional information. See the "LDAP Configuration Procedure" section on page 4-26 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)

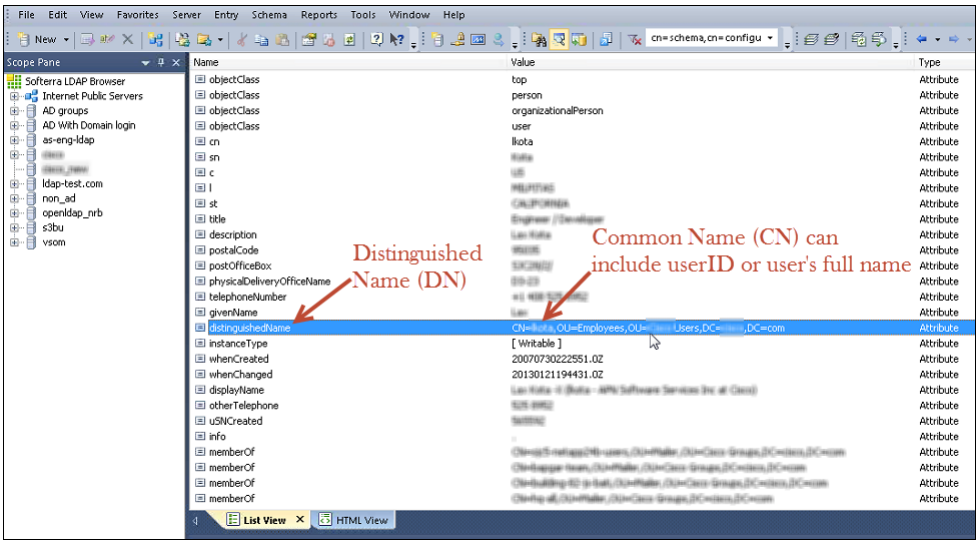
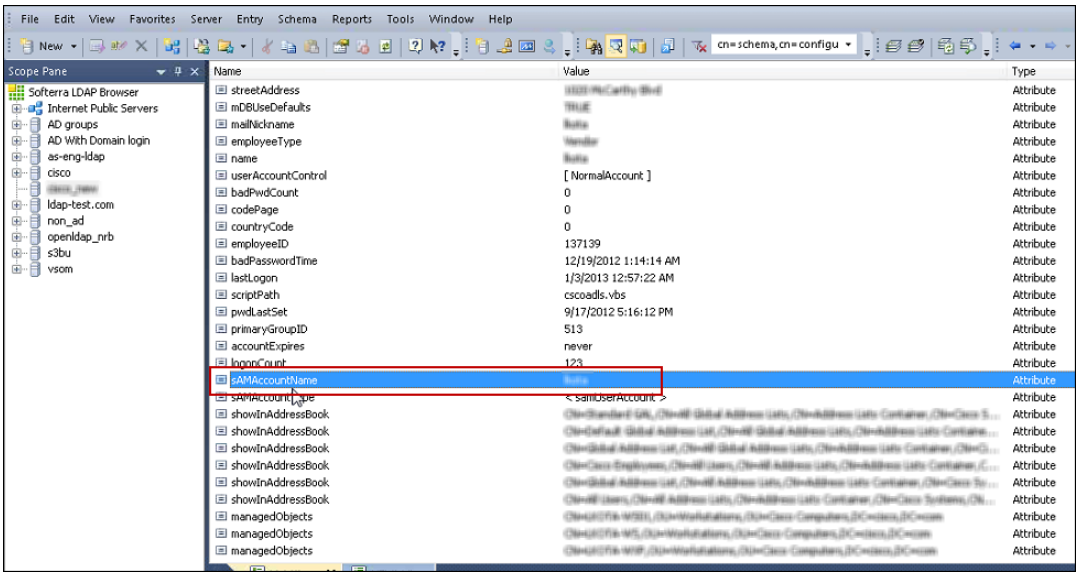
Principal	(Required) The Principal setting is used to *bind* Cisco VSM to the LDAP server. In other words, the Principal setting defines the user information used to authenticate individual users with the LDAP server. The Principal entry includes the *%USERID%* variable, which represents the userID configured on the LDAP sever. The *%USERID%* and password are entered when the user logs into Cisco VSM, and is sent to the LDAP server for authentication. • 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**. The following illustration shows an LDAP configuration that uses the userID as the CN.  **Anonymous Binding** 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. Anonymous Binding requires only the base DN, and does not require the *%USERID%* variable. For example: **ou=employees,ou=people,o=mycompany.com** **Note** The following error is returned if the LDAP server does not support Anonymous Binding: `Operation failed: User <user id> is not found in LDAP or given distinguished name does not support anonymous access.`

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

User Search Base	(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. For example: **OU=Company Users,DC=Mycompany,DC=com** **Anonymous Binding** This field is optional field for Anonymous Binding.
Userid Attribute	(Required) Enter the name of the LDAP mapping field where the User ID is stored. For example: • **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	(Optional, if defined on the LDAP server). The name of the LDAP server attribute that holds the users' first name. For example: `givenName` or `displayName`.
Lastname Attribute	(Optional) The name of the LDAP server attribute that holds the users' surname. For example: `sn` (if defined on the LDAP server).
Email Attribute	(Optional) The name of the LDAP server attribute that holds the users' email address. For example: `mail` (if defined on the LDAP server).
Tags	(Optional) Words that assist in a *Find*.
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: `Security users`
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: `ou=groups,o=mycompany.com`.
Filter	Enter the syntax that limits access to members of a specific group on the LDAP server. For example: `(&(cn=%USERID%)(memberOf=CN=vsom-admins,OU=Grouper,DC=mycompany,DC=com))`

Tip See the "LDAP Configuration Examples" section on page 4-23 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 = *userid*	When the LDAP Common Name (CN) field includes the userID, the Cisco VSM "Principal" setting includes the *%USERID%* variable and the complete User Search Base path. **Note** The *%USERID%* variable is replaced with the username entered when logging into Cisco VSM.	• Anonymous Binding: Off • Principal example: *cn=%USERID%,ou=active,ou=employees,ou=people,dc=mycompany,dc=com* • User Search Base example (corresponding to the above Principal): *ou=employees,ou=people,dc=mycompany,dc=com* • Filter example: – Name: *vsom-admins* – Search path: *dc=mycompany, dc=com* (corresponding to the above examples) – Filter: *(&(cn=%USERID%)(memberOf=CN=vsom-admins,OU=Grouper,DC=mycompany,DC=com))*
Active Directory Server CN = the users full name	When the LDAP Common Name (CN) field includes the user's full name: • The Principal setting includes the *%USERID%* 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.	• Anonymous Binding: Off • Principal example: *%USERID%@mycompany.com* • User Search Base example: *dc=mycompany, dc=com* (corresponding to the example shown in the following filter) • Filter example: – Name: *vsom-admins* – Search path: *ou=active,ou=employees,ou=people,o=mycompany.com* – Filter: *(&(cn=%USERID%)(memberOf=CN=vsom-admins,OU=Grouper,DC=mycompany,DC=com))*

Table 4-10 LDAP Configuration Options (continued)

LDAP Configuration	Description	Configuration Example
Regular LDAP binding (non-Active Directory)	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. The Userid Attribute defines the LDAP field where the userID is stored.	• Anonymous Binding: Off • Principal example: *CN=%USERID%,OU=people,OU=US,DC=mycompany,DC=com* • User Search Base example: *ou=people,ou=us,dc=mycompany,dc=com* (corresponding to the above Principal) • Filter example: – Name: *vsom-admins* – Search path: *ou=people,ou=us,dc=mycompany,dc=com* (corresponding to the above Principal) – Filter: *(&(objectClass=posixGroup)(memberuid=%USERID%)(cn=vsomadmins))*
Anonymous Binding (non-Active Directory)	If the LDAP server is configured to be accessed as anonymous, the *%USERID%* variable is not required. Only the correct server hostname, port and principal is required to bind Cisco VSM to the LDAP server. **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. **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.	• Anonymous Binding: On • Principal example: *ou=people,ou=us,dc=mycompany,dc=com* • User Search Base: Leave blank • Filter example: – Name: *vsom-admins* – Search path: *dc=mycompany,dc=com* – Filter: *(&(objectClass=posixGroup)(memberuid=%USERID%)(cn=vsomadmins))*

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.

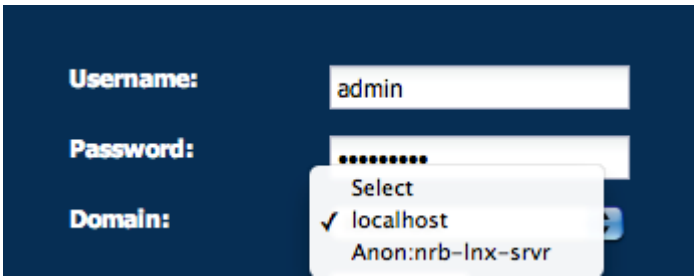
Note To configure LDAP servers, you must log in with *super-admin* privileges, using the **localhost** Domain.

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.

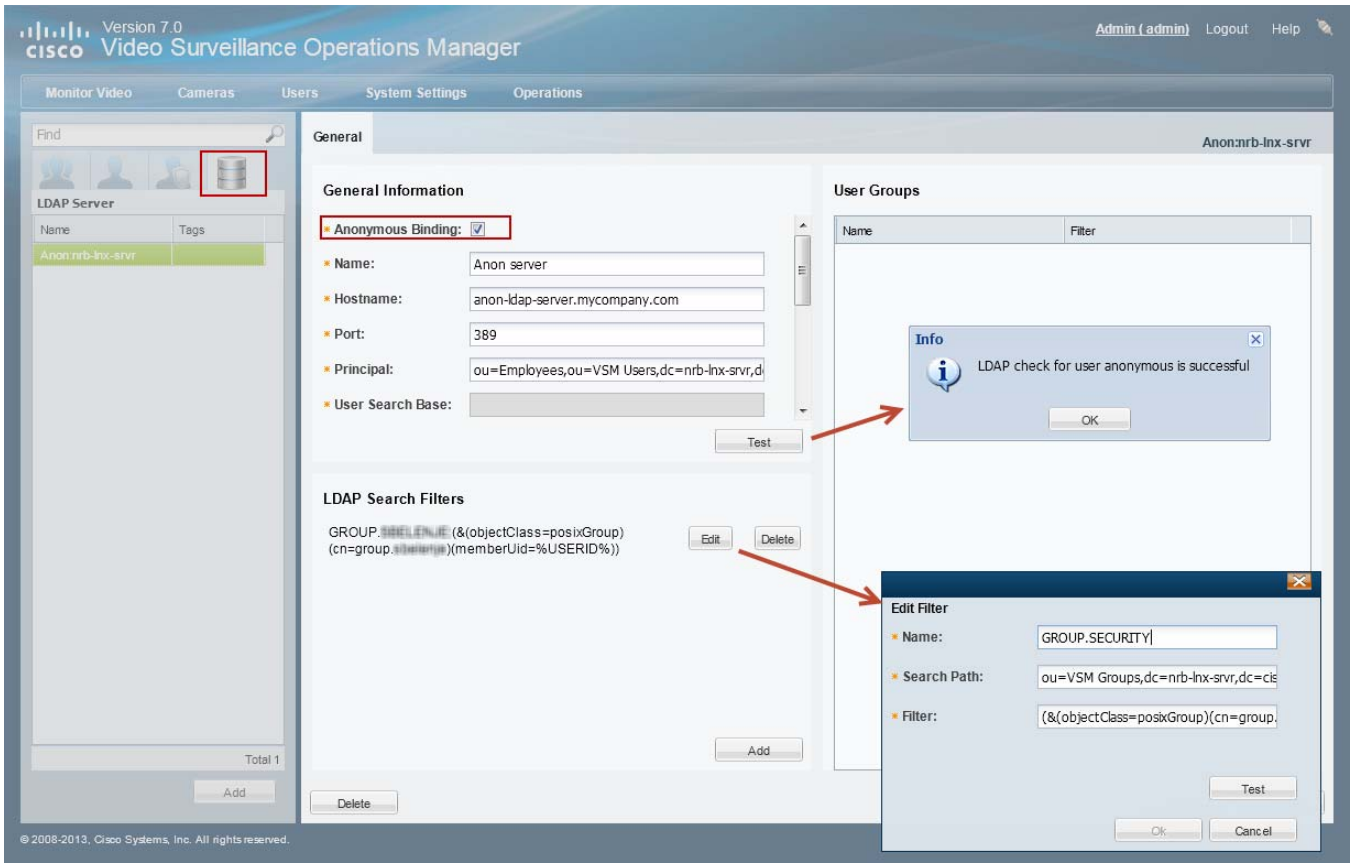
Figure 4-8 Localhost Login for LDAP Configuration Changes



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).

a. Enter the settings as described in the "LDAP Server Settings" section on page 4-19 (see Table 4-8).

b. Click **Test** and enter the test username and password (credentials are not required if **Anonymous Binding** is selected).

c. 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 4-23 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 4-23 (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 4-23 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).

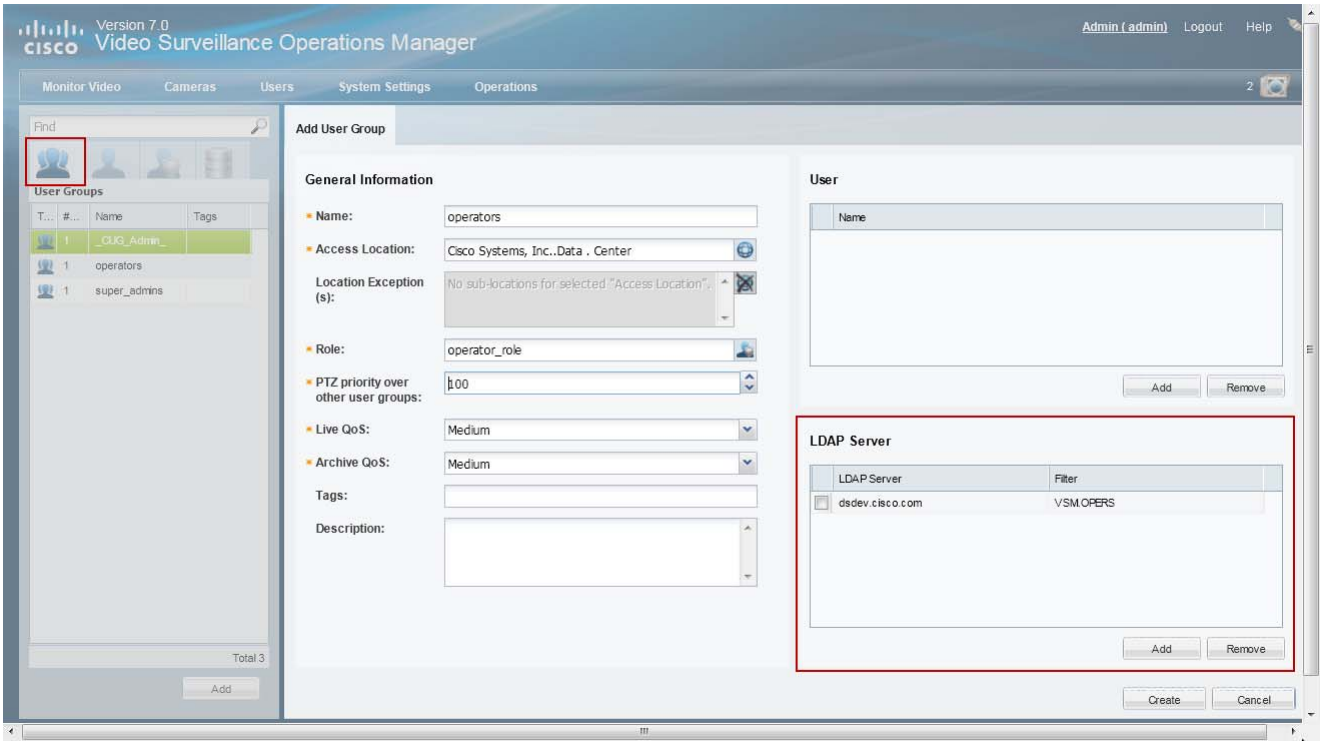
Step 6 (Required) Click **Create** or **Save** to save the LDAP server settings.

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 4-11).

c. In the LDAP Server section, click **Add**.

d. Select the *LDAP Server* name that includes the appropriate filter and click **OK**.

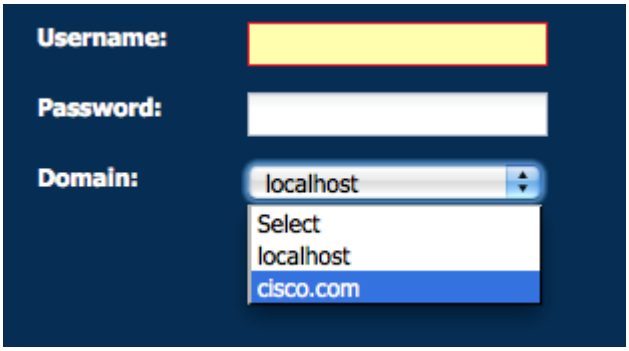
Tip The filter defines a sub-set of LDAP users that will gain the user group access permissions.

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



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**.

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

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.	• 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.	• Creating or Modifying a Template, page 12-3 • Editing the Camera Settings, page 10-42 • Understanding a Camera's Installed Location Vs. the Pointed Location, page 5-9 • Adding External Encoders and Analog Cameras, page 16-5 • Media Server Settings, page 9-5 • Adding User Groups, page 4-11
Step 4	Assign users to one or more user groups. Users gain access to the locations assigned to the user groups.	Adding Users, page 4-15

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

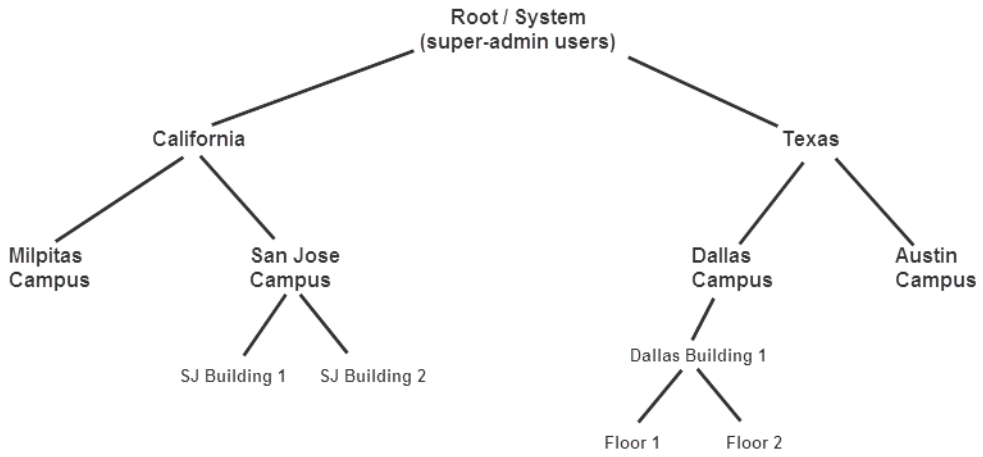
Type	Resources	Description
Permission-Based	• Devices (cameras, encoders, servers) • User groups • Views	Users can access *permission-based* resources that are assigned to their user group location or lower (sub-location). For example, in Figure 5-2 a user assigned to a *Dallas Campus* user group can access the cameras at the *Building 1* sub-location, but not at the *Texas* location. *Dallas* users also cannot access any *California* locations.
Partition-Based	• User roles • Schedules • Camera templates	User groups can access *partition-based* resources that are in the same location hierarchy (either higher or lower, but not in a different branch). For example, in Figure 5-3 a user assigned to a *Dallas Campus* 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 *Austin Campus* or any of the *California* locations.
Global Resources	*Global* resources can be accessed by all users who have the required access permissions.	For example, a user with *manage users* permissions access all the users in the system. The user object is not restricted to a location.
Super-admin	• System Settings • Audit Logs	Only users assigned to a *super-admin* 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.

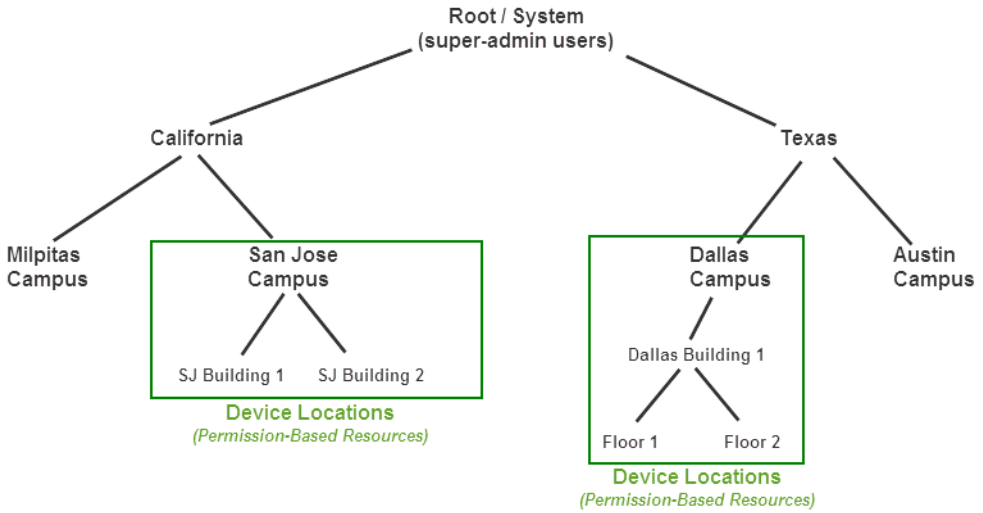
Permission-Based Resources: Limiting User Access to Devices

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 "Setting the Default View" section on page 3-1.

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

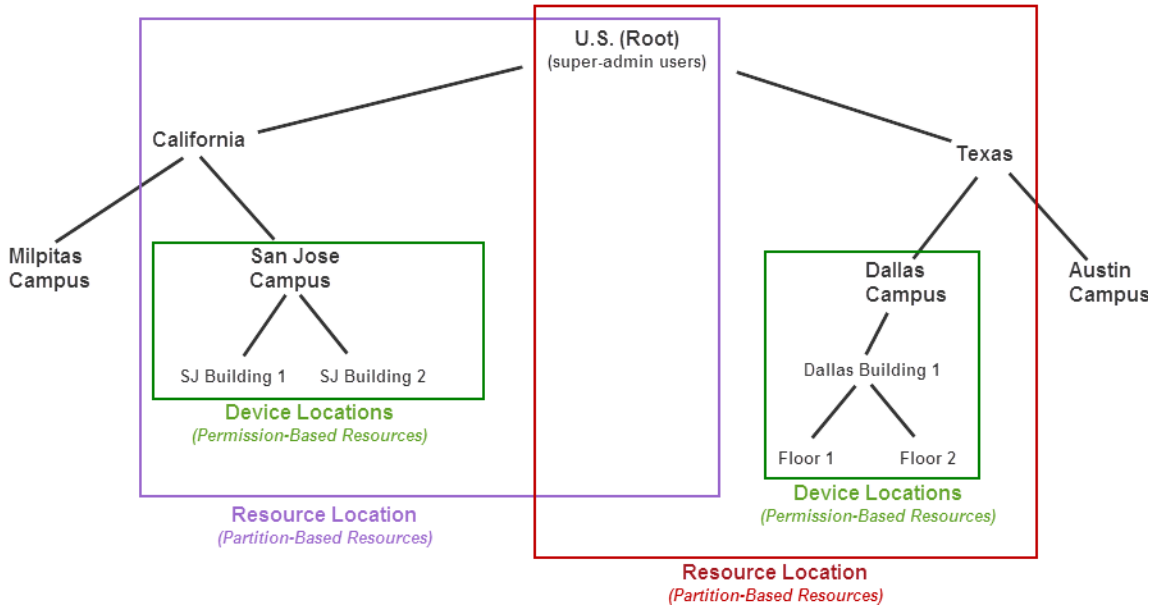
Partition-based resources include camera templates, schedules, and user roles. If the user belongs to a user group with access to these resources, then the user can access any partition-based resource in the same location hierarchy (locations that are higher or lower, but not in a different branch).

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



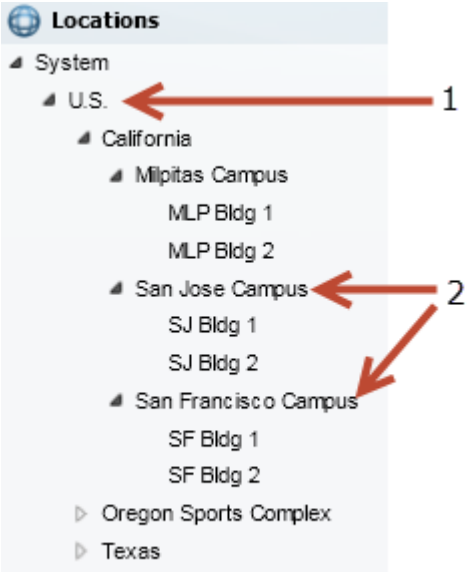
Examples: Locations in Simple vs. Large Deployments

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



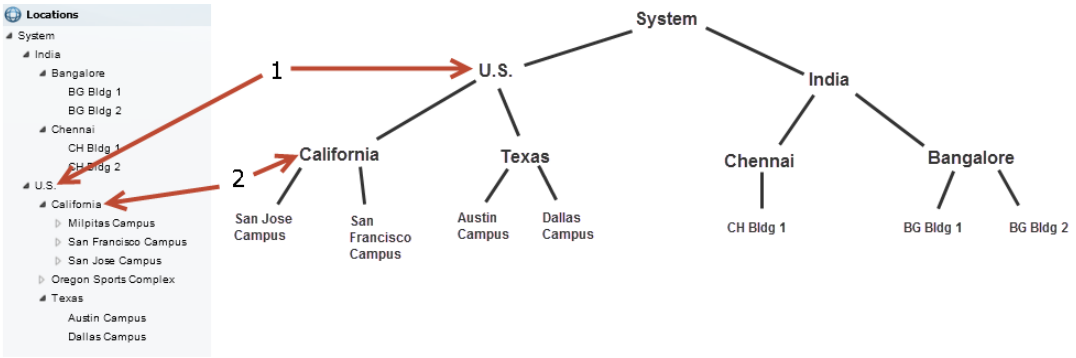
1	Assign *partition-based resources* (templates, roles and schedules) to a high-level or root location. • *Partition-based resources* (templates, roles and schedules) can be viewed and used by all users at all sub-locations. • Users can only modify the templates, roles, and schedules that are assigned to their location (or lower). • For example, in Figure 5-4 a user assigned to "Milpitas Buildings" can view *partition-based resources* assigned to the "U.S." location, but only super-*admin* users can modify the resources. **Tip** We recommend also assigning servers to a high-level location to provide support to devices and user groups at lower-level locations.	**2**	Assign *permission-based resources* (such as cameras) to sub-locations to restrict user access. • Users can only access *permission-based resources* (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"). **Tip** Deployments with a small number of users can also assign user groups and *permission-based resources* to the "U.S." (root) location.

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



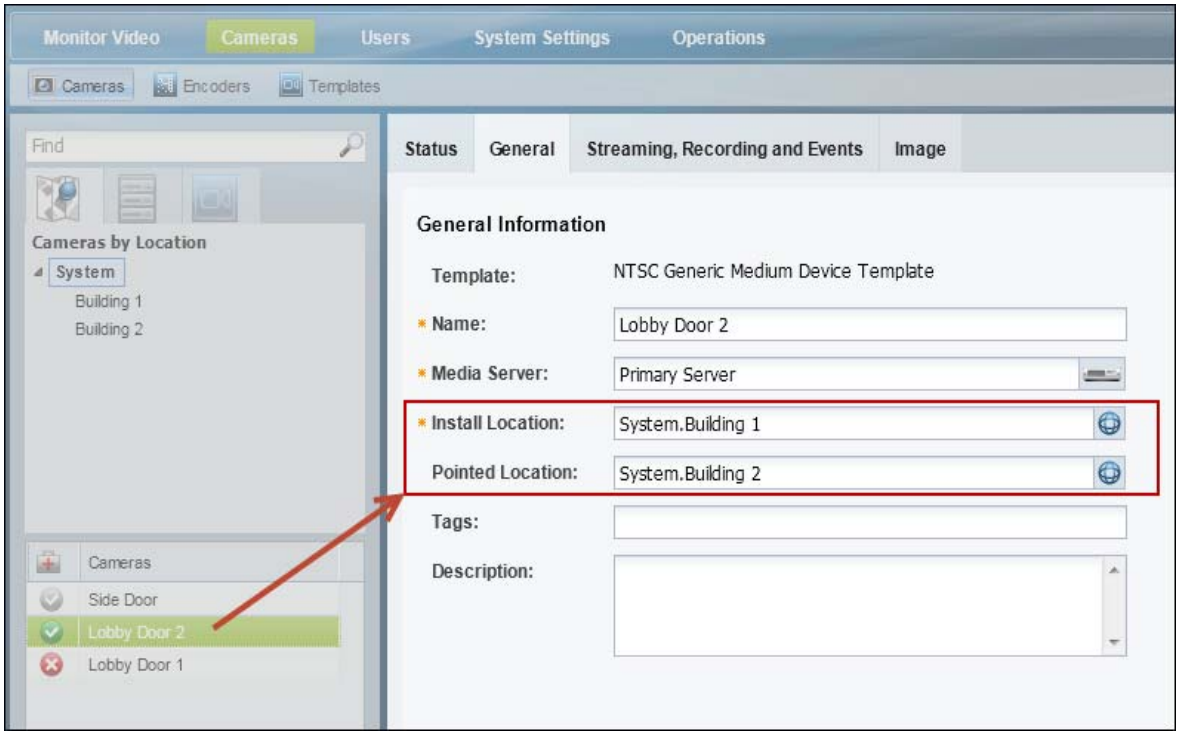
1	Assign *partition-based resources (*templates, roles and schedules) to a high-level branch location, such as "U.S." • *Partition-based resources (*templates, roles and schedules) can be viewed and used by all users within that location hierarchy (for example, from the San Jose Campus up to the System users). • Users can only modify the templates, roles, and schedules that are assigned to their location (or lower). For example, in Figure 5-5 a user assigned to "California" can view *partition-based resources* assigned to the "U.S." location, but not resources in the "India" locations.	**2**	Assign *permission-based resources* (such as cameras) to sub-locations to restrict user access. • Users can only access *permission-based resources* (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



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.

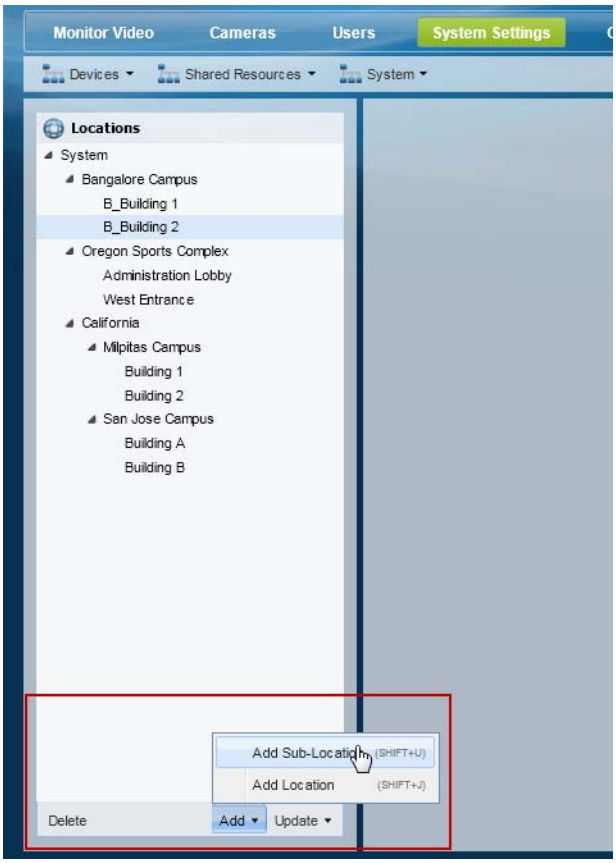
- See the "Logging In" section on page 1-18.
- You must belong to a User Group with permissions for *Locations & Maps*.

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 (Optional) Select a map for the location.

Select a map to define the aerial map view that is displayed when a location is selected using the Cisco Video Surveillance Safety and Security Desktop (Cisco SASD) application. See the "Define the Location Maps" section on page 24-8.

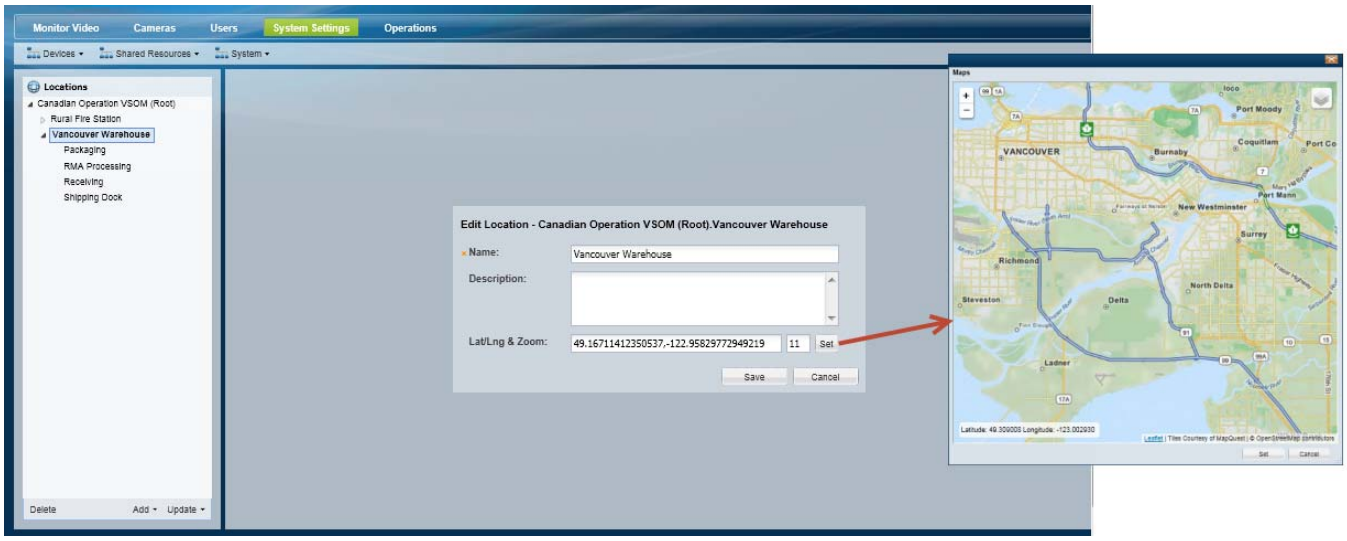
a. Click **Set** (Figure 5-8).

b. Use the Zoom In + and Zoom Out − buttons and drag the map image to locate the city, region or other aerial view that should be displayed.

c. Click **Set** to select the map as displayed on the screen.

Note The Longitude and Latitude of the visible map are automatically entered in the location settings (Figure 5-8). The second field displays the Zoom factor. For more information, see the "Configuring Location Maps" section on page 24-1.

Figure 5-8 Setting the Base Map



Step 5 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.

Configuring Servers

A server is a physical or virtual machine (VM) that runs the Cisco Video Surveillance system software. Each server can run one or more server services. For example, the Operations Manager is a server service that provides the user interface used to configure and manage a Cisco Video Surveillance deployment.

Additional services can be enabled when the server is added to the Operations Manager configuration. For example, a server can be added as a Media Server, Maps Server or Metadata Server that supports those features and functions for the entire deployment.

Tip The Cisco Video Surveillance Federator service can also be enabled on a stand-alone server. See the "Understanding Server Services" section on page 6-3 and the "Using Federator to Monitor Multiple Operations Managers" section on page 22-1 for more information.

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

Contents

Understanding Server Services

Each server can run one or more services that provide features and functions for the Cisco Video Surveillance system. For example, the Operations Manager provides the configuration interface and management features for the entire deployment, the Media Server service manages cameras and encoders and plays and records video, and the Maps service supports image layers used in location maps. In addition, a Federator service allows users to view the resources from multiple Operations Manager deployments.

Table 6-1 describes the supported server services and how each is enabled or disabled in this release.

Table 6-1 Supported Server Services

Service	Description	Activation Rules
Operations Manager	The browser-based Cisco VSM Operations Manager administration and configuration tool.	Can be added as a stand-alone server, or co-located with other services (such as a Media Server and/or Maps Server). **To Enable:** 1. Install the server and complete the Management Console Setup Wizard and select the **Operations Manager** service. 2. (Optional) Select the Media Server service to create a co-located server. This automatically enable the Media Server service on the default "VSOMServer". 3. (Optional) Add additional servers to the Operations Manager configuration, and select the Service Type to enable a service on the server. **Note** At least one Media Server must be added to the Operations Manager for the system to be functional. 4. Use the Operations Manager to further configure the services and system features. **Related Documentation:** • Summary Steps to Add or Revise a Server, page 6-8 • Configuring Media Server Services, page 9-1 • Cisco Video Surveillance Management Console Administration Guide **To Disable:** 1. Log in to the Management Console for each server associated with the Operations Manager server and click the **Remove** button. **Note** The **Remove** button disassociates the server and all server services from the Operations Manager. This allows the server (and running services) to be added and managed by a different Operations Manager. 2. Log in to the Management Console for the Operations Manager server and deselect the **Operations Manager** service.

Table 6-1 Supported Server Services (continued)

Service	Description	Activation Rules
Media 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	Can be added as a stand-alone server, or co-located on a single server with the Operations Manager or Operations Manager and Maps service. **To Enable:** 1. Install the server and complete the Management Console Setup Wizard. 2. (Co-located server) Log in to the Operations Manager, select **System Settings** > **Server**, and select the default **VSOMServer**. In the Services section, select the **Media Server** service. See the "Server Settings" section on page 6-10. 3. (Stand-alone server) Log in to the Operations Manager and add the server as a **Media Server**. See the "Adding or Editing Servers" section on page 6-16. 4. Select the Media Server **Advanced** settings to further configure the service, if necessary. See the "Media Server Settings" section on page 9-5. **Related Documentation** • Cisco Video Surveillance Management Console Administration Guide • Adding or Editing Servers, page 6-16 • Server Settings, page 6-10 • Configuring Media Server Services, page 9-1 **To Disable:** • Log in to the Operations Manager, select **System Settings** > **Server**, select the server, and deselect the **Media Server** service. or • Log in to the Management Console for the server, and click *Remove* to remove the server from the Operations Manager. Then de-select the service.

Table 6-1 Supported Server Services (continued)

Service	Description	Activation Rules
Map Server	Allows Image Layers to be added to location maps using the Operations Manager. Image layers are viewed by operators using the Cisco Video Surveillance Safety and Security Desktop application. Cameras, locations and alerts are displayed on dynamic maps, and map images that represent the real-world location of devices and events.	Use the Operations Manager to activate the service. **Note** This service is supported as a stand-alone server on a server running the RHEL 6.4 64 bit OS, or co-located on a Operations Manager server. **To Enable a Stand-Alone Server:** 1. Install the server and complete the Management Console Setup Wizard. 2. Log in to the Operations Manager and add the server as a **Maps Server**. See the "Adding or Editing Servers" section on page 6-16. 3. Continue to the "Configuring Location Maps" section on page 24-1. **To Enable a Co-Located Maps Server:** Maps Servers can be co-located on a server running Operations Manager, or Operations Manager and Media Server (a co-located Maps Server must also run Operations Manager). 1. Log in to the Operations Manager. 2. Navigate to the Operations Manager server configuration page. 3. Select the **Maps Server** to enable the service on the Operations Manager server. 4. Continue to the "Configuring Location Maps" section on page 24-1. **Related Documentation** • Cisco Video Surveillance Management Console Administration Guide • Adding or Editing Servers, page 6-16 • Server Settings, page 6-10 • Configuring Location Maps, page 24-1 **To Disable:** • If the Operations Manager is not co-located with the Maps Server, log in to the Management Console for the server, click **Remove** to remove the server from the Operations Manager, and then de-select the service. • If the Operations Manager is co-located with the Maps Server, log in to the Operations Manager and de-select the Media Server service.

Table 6-1 Supported Server Services (continued)

Service	Description	Activation Rules
Metadata Server	Allows metadata to be added to recorded video, which enables features such as Video Motion Search in the Cisco SASD desktop application. Metadata can also be accessed by 3rd party integrators for advanced analytics analysis.	Use the Operations Manager to activate the service. **Note** This service is supported as a stand-alone server only, on a server running the RHEL 6.4 64 bit OS. **To Enable:** 1. Install the server and complete the Management Console Setup Wizard. 2. Log in to the Operations Manager and add the server as a **Metadata Server**. See the "Adding or Editing Servers" section on page 6-16. 3. Continue to the "Enabling Video Analytics" section on page 13-2. **Related Documentation** • Cisco Video Surveillance Management Console Administration Guide • Adding or Editing Servers, page 6-16 • Server Settings, page 6-10 • Enabling Video Analytics, page 13-2 **To Disable:** • Use the Operations Manager to deactivate the service on the server. or • Use the Management Console to *Remove* the server from the Operations Manager, and then de-select the service.
VSF	Enables the Federator service used to monitor video and system health for the cameras and resources of multiple Operations Managers. The Federator service can only be enabled on a stand-alone server in this release. Other server services cannot be enabled on the same server as the Federator service. The Federator interface is accessed using a web browser or the Cisco SASD. Federator.	Activated using the Management Console only. Cannot be activated using the Operations Manager. **Note** This service is supported as a stand-alone server only, on a server running the RHEL 6.4 64 bit OS. **To Enable:** 1. Log in to the Management Console. 2. Install the server and complete the Setup Wizard: select the **VSF** service. 3. Log in to the Cisco VSM Federator browser-based interface. 4. Continue to the "Using Federator to Monitor Multiple Operations Managers" section on page 22-1. **Related Documentation** • Cisco Video Surveillance Management Console Administration Guide • Using Federator to Monitor Multiple Operations Managers, page 22-1 **To Disable:** • Log in to the Management Console and deselect the **VSF** service.

Requirements

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

Table 6-2 Server Requirements

Requirements	Requirement Complete? (✓)
The IP address and password for the server.	❑
You must belong to a user group with *Servers & Encoders* permissions. See the "Adding Users, User Groups, and Permissions" section on page 4-1 for more information.	❑
A physical or virtual Cisco Video Surveillance 7.x server installed in the network where the other Cisco Video Surveillance components are deployed. • Physical Servers: – (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).	❑
Each Media Server requires a license in order to be added to the Operations Manager configuration. See the "Installing Licenses" section on page 1-26.	❑
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.	❑
Each server must run the same versions of the *system software* and device *driver packs*. See the following for more information: • Upgrading System Software, page 26-5 • Installing and Upgrading Driver Packs, page 26-16	❑

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: Cisco Media Servers" section on page 17-1).

	Step	More Information
Step 1	Review the options for server network configuration.	• Understanding Server and Camera Network Configuration, page 7-1
Step 2	Install the server.	**Physical Servers** • (Systems pre-installed with Release 7.2 or higher) See the Cisco Physical Security UCS Platform Series User Guide for more information. • (Systems pre-installed with Release 7.0.0 or 7.0.1) See the Cisco Physical Security Multiservices Platform Series User Guide for more information. **Virtual Machines** • See the Cisco Video Surveillance Virtual Machine Deployment and Recovery Guide for UCS Platforms for instructions to install the server software .ova image as a virtual machine (VM).
Step 3	Complete the server *Initial Setup Wizard*.	Cisco Video Surveillance Management Console Administration Guide.
Step 4	Log on to the Operations Manager.	Logging In, page 1-18.
Step 5	Add a license, if necessary. Each Media Server requires a license in order to be added to the Operations Manager configuration.	Installing Licenses, page 1-26

	Step	More Information
Step 6	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.	• Adding or Editing Servers, page 6-16 • Server Settings, page 6-10 **Note** Servers can be added to the configuration in *Pre-provisioned* state before they are available on the network. See the "Pre-Provisioning Servers" section on page 6-17. **Note** Cameras/encoders and their associated Media Servers must belong to the same Site (you cannot associate a camera in Site A to a Media Server in Site B).
Step 7	(Optional) Configure the service options.	• Operations Manager Advanced Settings, page 6-32 • Configuring Media Server Services, page 9-1 • Configuring Location Maps, page 24-1 • Enabling Video Analytics, page 13-2

Server Settings

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

Server System Settings

General Information Settings

Select the **General** > **System** tabs to revise the server name and installed location. You can also enter a description and tags that are used for the *Find* function.

Table 6-3 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 *Find* function.
Description	Describe the purpose or use of the server. For example: "Support for Building B cameras and associated video".

Services

Select the **General** > **System** tabs to activate or deactivate the services running on the server.

- See the "Understanding Server Services" section on page 6-3 for information about the services and limitations on how many services can be enabled on a server.
- Click the **Advanced** icon (if available for the service) to enter additional configurations for the service.

Note Use the Operations Manager browser interface to enable or disable the services running on a server. The Management Console is only used to enable or disable the Operations Manager service.

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 s 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.

Hardware Information Settings

Select the **General** > **System** tabs for hardware information about the physical platform, if available.

Table 6-5 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	The bar shows the approximate percentage use of the total storage. • Blue: used storage space • Green: unused storage space 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 9-6).

Server Network Settings

Access Information Settings

Select the **General** > **Network** tabs to 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 6-6 Access Information Settings

Setting	Description
Hostname/IP	The hostname (recommended) or IP address used by the Operations Manager to access the server. • 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. • If a static IP address is changed on the server, but not in the Operations Manager configuration, communication can be lost. This is because the IP address in Operations Manager is used to access the server, and must be the same as the address configured on the server's port. Revise the server and Operations Manager configuration to use the same static IP address.
Username	(Read-only) The default username for all servers s is `localadmin`. The username cannot be changed.
Password	**To change the password used by the Operations Manager:** This setting changes the Operations Manager's understanding of the server password. 1. Enter the password that is configured on the server. 2. Click **Save**. **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. **To change the password that is configured on the server:** To change the password configured on both the server and on Operations Manager: 1. Click **Change**. 2. Enter the old and new password. 3. Click **OK**. 4. Click **Save**. **Note** See the Cisco Video Surveillance Management Console Administration Guide for more information about server passwords.

Network Information

Select the **General** > **Network** tabs to define the **Network Information** 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 Understanding Server Network Configuration, page 7-2 for more information.

Click **Settings** next to each NIC port to change the following network settings. See Understanding Server Network Configuration, page 7-2 for more information.

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: `cisco.com`
Configuration type	Select one of the following options based on the enabled server applications. • **Disabled**—disables the interface. • **DHCP**—the IP address and other fields will be disabled and defined by a DHCP server. • **Static** —enter the **IP address**, **Subnet Mask** and other network settings. **Note** The Ethernet ports must be configured with static IP address or DHCP depending on the enabled applications. See the Overview section of the Cisco Video Surveillance Management Console Administration Guide for more information.
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

Select the **General** > **Network** tabs to define the network time protocol (NTP) server automatically sets the server time and date.

Note See Understanding NTP Configuration, page 8-1 for complete information on the recommended NTP settings for cameras and servers, and the alternative configuration options.

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	(Media Server-only servers) The Operations Manager server is used as the NTP server. The Operations Manager also defines the server timezone. • 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. **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.
User Configured	Allows you to enter a custom NTP server for the current server. • Co-located servers—(Default and required) Enter the NTP server hostname(s) or IP address(es). Separate entries with a space or comma and select the Co-located server's time zone. • 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. **Note** If multiple NTP servers are used, a hierarchy of servers should ensure that the times on the various components are close. **Note** We recommend using the same network time protocol (NTP) server on all Media Servers to ensure the time settings are accurate and identical.

Medianet

Select the **General** > **Network** tabs to define the Medianet features used to monitor and troubleshoot traffic from servers and endpoints. See the "Medianet Metadata and Mediatrace" section on page 25-3 for more information.

Table 6-9 Medianet Settings

Field	Settings
Enable Metadata	Select **Enabled** to enable or disable applying metadata tags. • This also (indirectly) creates the MSI flows. The MSI flow creation is required to perform Mediatrace and performance monitoring. • This feature is enabled by default.
Mediatrace Name	(Read-only) The Media Services Interface (MSI) username. This field is read-only and cannot be changed.
Mediatrace Password	Enter the password for the Media Services Interface (MSI). This password is used to authenticate the Network Management System (such as LiveAction) with the Media Server to perform Mediatrace or performance monitoring.

Adding or Editing Servers

To add or edit servers, select **System Settings** > **Servers**, and click **Add**. You can add a single server manually, or import multiple servers using 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: Cisco Media Servers" section on page 17-1).

Tip Select an existing entry to revise an existing server configuration (see the "Server Settings" section on page 6-10 for more information).

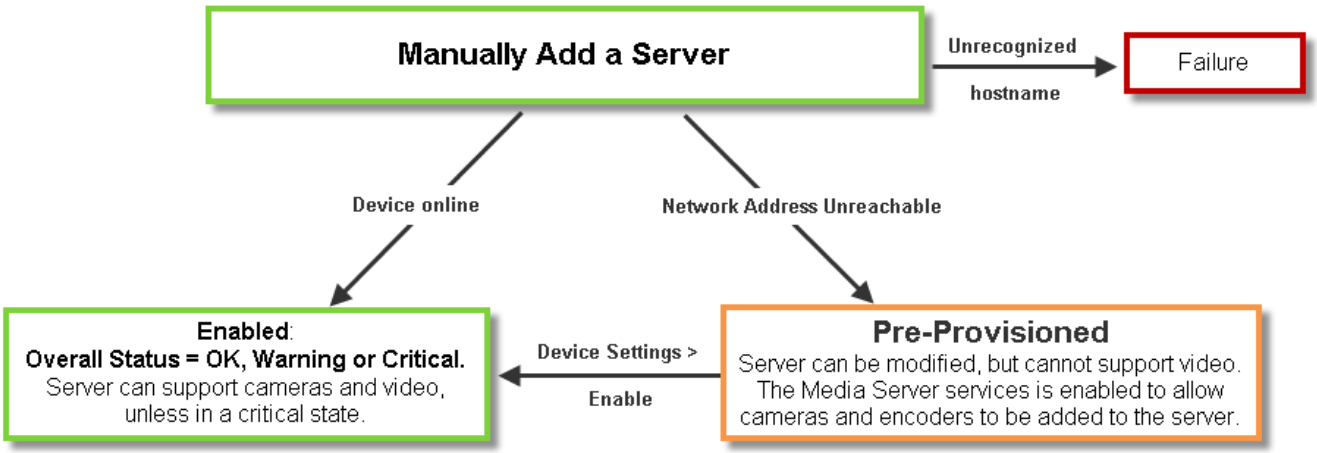
Refer to the following topics for more information:

- Overview, page 6-16
- Pre-Provisioning Servers, page 6-17
- Prerequisites, page 6-17
- Adding or Editing a Single Server, page 6-17
- Importing or Updating Servers Using a CSV File, page 6-20

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 17. 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 6-26.

See the "Viewing Server Status" section on page 6-29 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: Cisco Media Servers" section on page 17-1.

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 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 Add a server license, if necessary.

Each Media Server requires a license in order to be added to the Operations Manager configuration. See the "Installing Licenses" section on page 1-26.

Step 4 Select **System Settings > Servers**.

Step 5 Click **Add**.

Tip To edit a server, click an existing entry to highlight it, then refer to the "Server Settings" section on page 6-10.

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 6 (*Add* only) Complete the initial server setup:

Figure 6-2 Add a Server

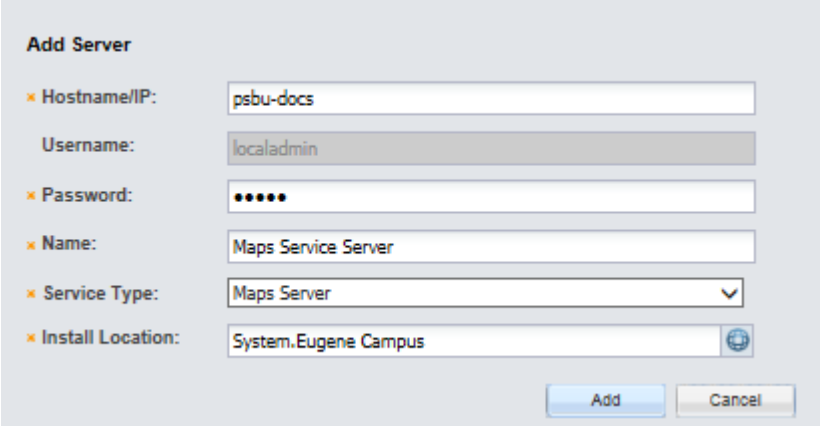


Table 6-10 Server Settings

Setting	Description
Hostname/IP	The hostname or IP address used by the Operations Manager to access the server.
Username	(Read-only) The default username for all servers is `localadmin`. 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 6-10 and the Cisco Video Surveillance Management Console Administration Guide for more information.
Name	A meaningful name for the server. For example, *Primary Server* or *Campus A Server*.

Table 6-10 Server Settings (continued)

Setting	Description
Service Type	The service that runs on the server. Select a service to enable the service functionality. See the "Understanding Server Services" section on page 6-3.
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. • Cameras/encoders and their associated Media Servers must belong to the same Site (you cannot associate a camera in Site A to a Media Server in Site B). See the "Understanding Sites" section on page 23-3.

d. Click **Add**.

- If the validation is successful, continue to Step 7.
- If the server cannot be found on the network, an error message appears.
  - Verify the server hostname and login credentials and return to Step 5 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 6-26).

Step 7 (Optional) Enter or revise the additional settings, if necessary, as described in the "Server Settings" section on page 6-10.

Step 8 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 if pre-provisioned.

Step 9 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.

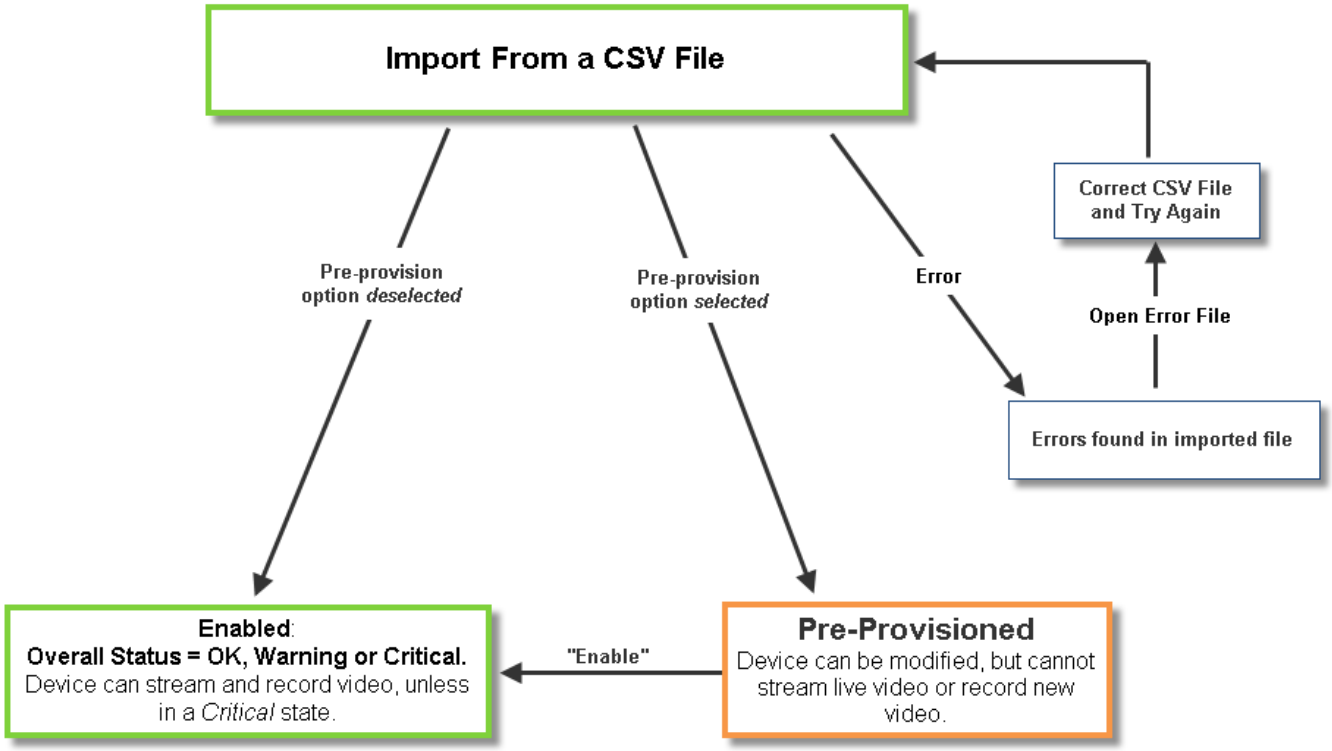
Refer to the following topics for more information:

- Overview, page 6-20
- Usage Notes, page 6-21
- Creating the CSV File, page 6-21
- Importing the CSV File, page 6-23

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

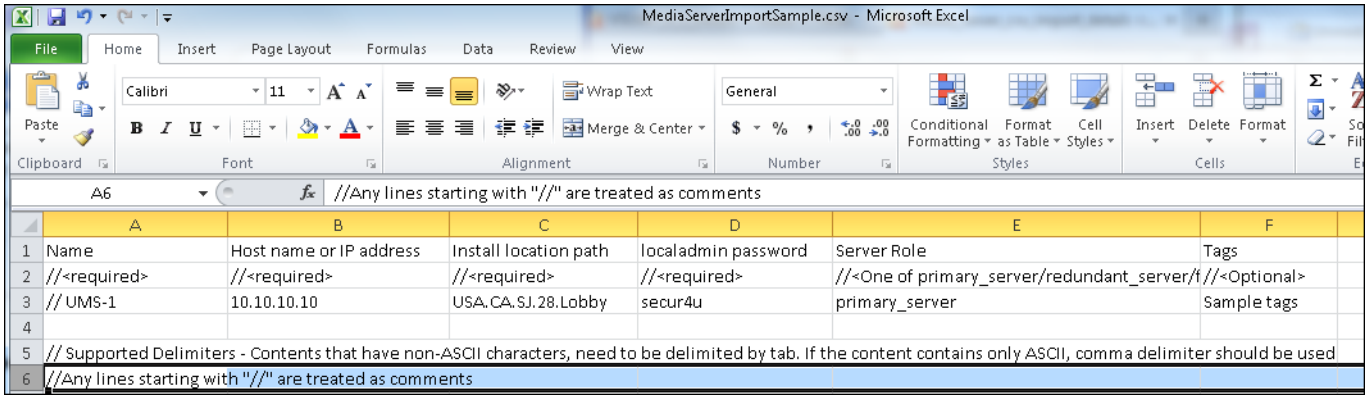
- Servers can be pre-provisioned in Release 7.2 and higher.
- You can choose to retain the devices (cameras and encoders) that were previously associated with the server, or discard them. Any discarded devices must be re-added, if required.
  - Enabled cameras and encoders associated with the server 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 10-38 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 10-1 and the "Adding Encoders and Analog Cameras" section on page 16-1 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 6-23. 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



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 6-11 describes the information required in each field.

Table 6-11 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.
localadmin password	Required	The password configured on the server to provide network access from the Operations Manager. • 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 6-12 to revise the credentials after the server is added to the system. **Note** The default username for all servers is `localadmin`. The username is read-only and cannot be changed.
Server Role	Required	The high-availability role of the server. The options are: • primary_server • redundant_server • failover_server • long_term_storage_server See the "Understanding Redundant, Failover, and Long Term Storage Servers" section on page 17-4 for more information.
Tags	Optional	Keywords used by the *Find* 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 6-21.

Step 2 Select **System Settings** > **Servers**.

Step 3 Choose **Add** and **Import servers from file**.

Step 4 Complete each *Import Step* as described below:

a. *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 10-1 and the "Adding Encoders and Analog Cameras" section on page 16-1 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 6-21. 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.

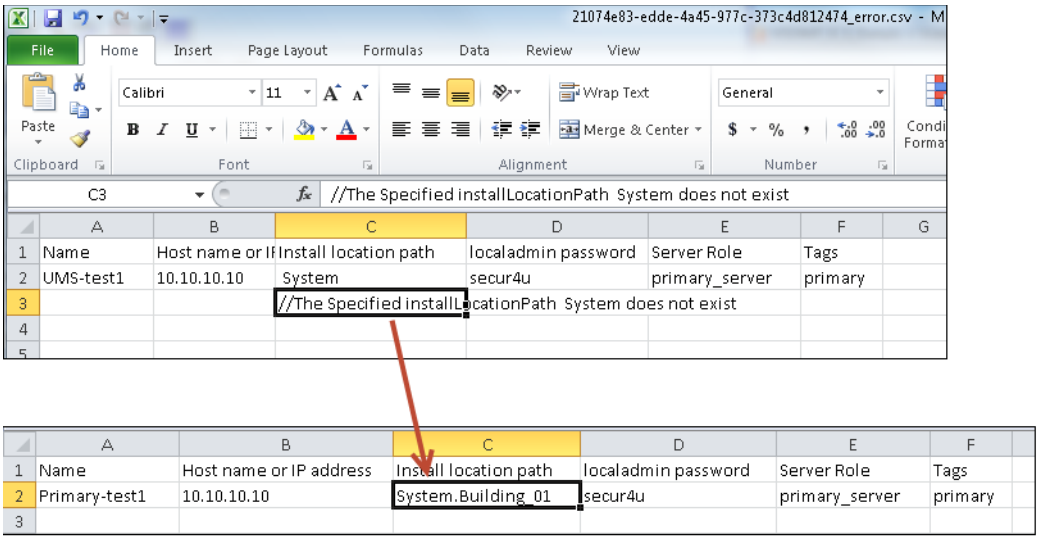
e. *Import Step 5 - Results* **Success**:

- 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



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 19-9.

Step 7 Complete the camera and encoder configurations to enable the devices, if necessary. See the "Adding and Managing Cameras" section on page 10-1 and the "Adding Encoders and Analog Cameras" section on page 16-1 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 10-42 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 10-42 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

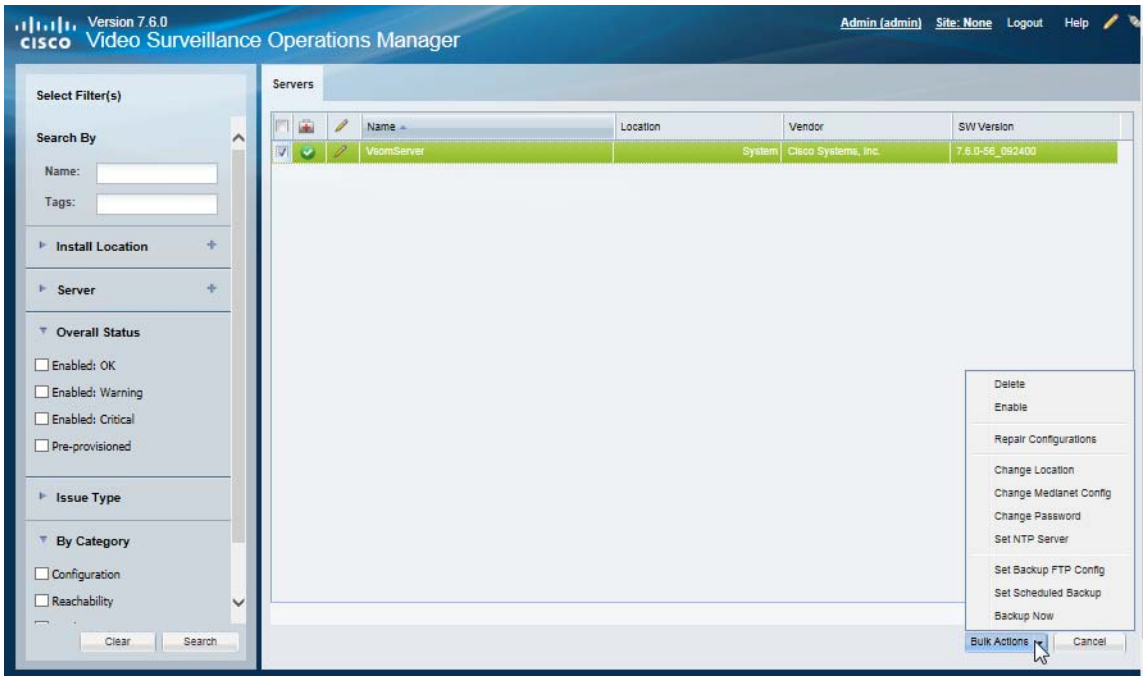
- Bulk Actions: Revising Multiple Encoders, page 16-11
- Bulk Actions: Revising Multiple Cameras, page 10-92.

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 6-12 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 *Warning* or *Critical* event. **Tip** See the "Device Status: Identifying Issues for a Specific Device" section on page 19-9 for more information.
Issue Type	Select the issues that apply to the device.
Category	Select the issue categories that apply to the device. For example, hardware issues or configuration issues.

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.

Table 6-13 Server Bulk Actions

Action	Description
Set Backup FTP Config	Defines the connection settings for the remote server used for server backups. See the "Backup Settings" section on page 21-3 for setting descriptions.
Set Scheduled Backup	Defines when the automatic backups will occur for the selected servers. See the "Backup Settings" section on page 21-3 for setting descriptions.
Backup Now	Performs an immediate one-time backup of the selected servers. A separate backup file is created for each active service running on the server. • **To Local**—Saves the backup file(s) to the disk on the server. • **To Remote**—Saved the backup file(s) to a remote FTP server. The FTP server connection must be configured (see "Set Backup FTP Config").
Change Medianet Config	Change the Medianet connection settings for the selected servers. See the "Medianet" section on page 6-15 for setting descriptions.
Enable	Enable the selected servers. See the "Viewing Server Status" section on page 6-29 for more information.

Table 6-13 Server Bulk Actions (continued)

Action	Description
Set NTP Server	Defines the NTP server for the selected servers. See the "NTP Information" section on page 6-14 for more information.
Repair Configurations	Synchronizes the configuration for the selected servers. See the "Repairing the Configuration or Restarting the Server" section on page 6-31 for more information.
Change Password	**Note** Only super-admin users can apply the **Change Password** option using Bulk Actions.
Change Location	Change the location for the selected servers. See the "General Information Settings" section on page 6-10 and the "Creating the Location Hierarchy" section on page 5-1.
Delete	Deletes the selected servers from the Operations Manager configuration. See the "Deleting a Server" section on page 6-24 for more information.

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 19-29.

Viewing Server Status

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

Device Status

Figure 6-7 Server Device Status

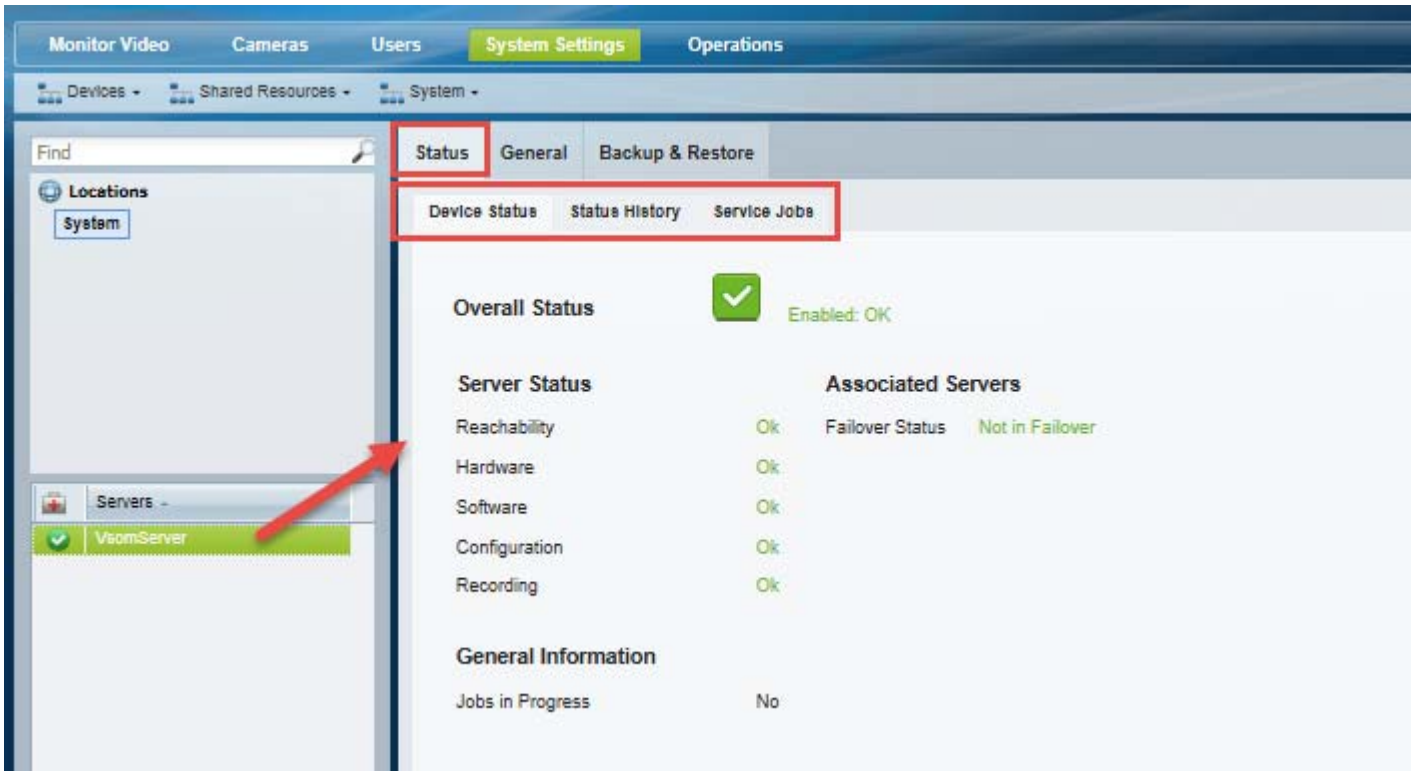


Table 6-14 Device States

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 the Status Error Details and History" section on page 19-14.
- 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 6-30).
- See the following options to repair configuration issues or reset the device state:
  - Repairing the Configuration or Restarting the Server, page 6-31
  - Resetting the Server Device State, page 6-30
- See the "Viewing the Server HA Status" section on page 17-22 for more information on the Associated Servers status.

Server Status History and Service Jobs

For more information about Status History and Service Jobs, see the "Viewing Media Server Status" section on page 9-9.

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 6-31.

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 6-15.

Table 6-15 Server Operations

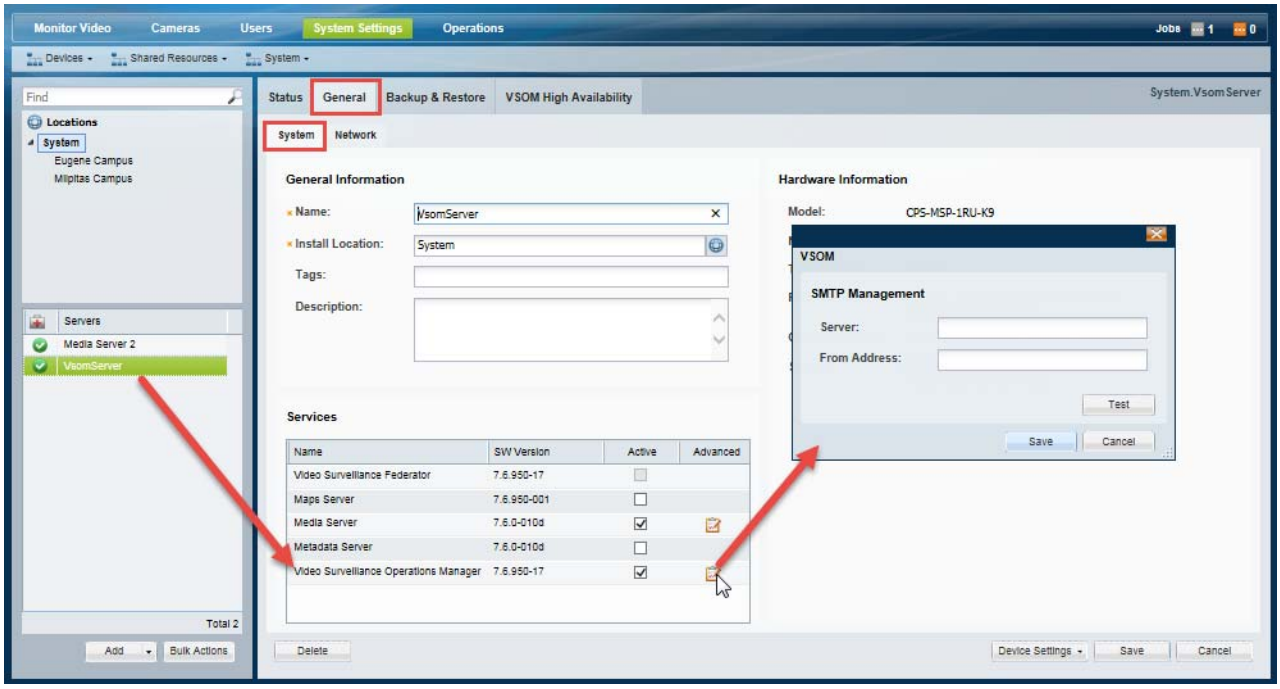
Operation	Description
Replace Configurations	Overwrite all configuration settings on the server with the settings in the Operations Manager. See the "Synchronizing Device Configurations" section on page 19-21 for more information.
Repair Configurations	Push only the configuration changes required to correct a mismatched field. Changes are pushed from the Operations Manager to the Media Server See the "Synchronizing Device Configurations" section on page 19-21 for more information.
Restart	Reboot the server and trigger a synchronization (*Repair Configuration*). **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

The Operations Manager Advanced setting are used to configure additional features.

SMTP settings are the only available Operations Manager advanced settings in this release (Figure 6-8).

Figure 6-8 Operations Manager Advanced Settings



SMTP Management Settings

Enter the **SMTP Management** settings (under the **Advanced** icon) to send server-generated emails (see Figure 6-8).

For example, the SMTP Server is used to send Health Notifications, as described in the "Health Notifications" section on page 19-17.

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 6-16 SMTP Settings

Field	Settings
SMTP Server	The IP address or hostname if the SMTP server used to send emails.

Table 6-16 SMTP Settings (continued)

From Address	The email address that appears in the *from* field. User replies will be sent to this address. This field is required to send e-mails when an SNMP event occurs.

Understanding Server and Camera Network Configuration

This document describes the network requirements, rules, and best practices for the servers, cameras, and other network devices in a Cisco Video Surveillance deployment.

Refer to the following topics for more information.

Understanding Server Network Configuration

Default Ethernet Interface Settings

The default Ethernet port configuration for each Cisco VSM server is:

- Nic Port 0— configured with a private static IP address (`http://192.168.0.200/`)
- Nic Port 1— configured for DHCP (the IP address and other settings are received from a DHCP server, if available).

These settings are applied in new servers, or servers that have been restored using the USB recovery drive. Use either of these addresses to access the Cisco VSM Management Console and complete the *Setup Wizard* (see the "Using the Initial Setup Wizard" section on page 2-1). At least one of these interfaces must reachable from the network where the workstation is installed.

Rules for Server Reachability

Dual-homed/NAT Configurations

- Dual-homed/NAT server configurations are not supported on any server running the Operations Manager service (including co-located servers). The Operations Manager server hostname can resolve to only one (correct) address. All users must be able to access that IP address.
- Dual-homed/NAT server configuration is supported only for stand-alone Maps, Metadata, and Media Servers.

Server Reachability

Stand-alone Maps, Metadata, or Media Servers must be added to Operations Manager using an IP address or hostname that can be accessed by all users.

For example, add the server using a hostname to ensure user requests resolve to the correct IP address if there is a NAT between users and the server.

Note The hostname is usually resolved via DNS, but can also be resolved by configuring the user's computer to resolve each server hostname).

- If a stand-alone Maps, Metadata, or Media Server is added to Operations Manager using an *IP address*, then every user must be able to access that specific IP address (for example, they must be in the same NAT).
- If a stand-alone Maps, Metadata, or Media Server is added to Operations Manager using a *hostname*, then every user must be able to resolve the hostname to an IP address that can be reached by the user

Supported Ethernet Port Configuration Combinations

Cisco VSM servers support two Ethernet ports that can use a static IP address, receive network settings from a DHCP server, or be disabled. The supported port configuration depends on the services enabled on the server (Table 7-1).

Table 7-1 Supported Ethernet Port Configurations

Server Services	Ethernet Port Configuration
Co-located system (Operations Manager and additional services hosted on the same server)	Only one interface can be enabled (static or DHCP). The other interface must be disabled. Verify that the Operations Manager server hostname resolves to only one (correct) address. Dual-homed/NAT server configurations are not supported on any server running the Operations Manager service.
Operations Manager-only system	Only one interface can be enabled (static or DHCP). The other interface must be disabled. Verify that the Operations Manager server hostname resolves to only one (correct) address. Dual-homed/NAT server configurations are not supported on any server running the Operations Manager service.
Stand-alone Maps, Metadata, or Media Servers	At least one Ethernet port must be enabled. The following combinations are supported: • Both interfaces configured static. • One interface static and the other disabled. • One interface configured static and the other DHCP. **Notes:** • Dual-homed/NAT server configuration is supported only for stand-alone Media Servers. • A hostname must be configured on all servers. The hostname does not have to be accessible through DNS, but all servers must have a hostname configured (a hostname is required for some services such as ActiveMQ).

Usage Notes

- At least one static interface must be configured.
- A servers network settings can be modified using either the Cisco VSM Management Console or browser-based Operations Manager tool.
- Changing network settings can cause the server to restart system services. Restarting services can take up to 90 minutes or more depending on number of devices managed by the Operations Manager and Media Server. Installed products will be offline during this time.

Using DHCP

Servers

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

To manually assign the IP address, default gateway, or DNS server, de-select **DHCP** by selecting the **Static IP** option.

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

Note Configuring an interface as DHCP may cause connectivity issues if no DHCP server is present in the network. For example, if an interface is configured for DHCP, and a DHCP server is not available in the network, then the network settings (such as the IP address and default gateway) will fail to populate and network communication cannot occur.

Cameras

Medianet cameras must be configured for DHCP.

Cameras that do not support Medianet can only be added using a static IP address.

See Discovering Medianet-Enabled Cameras, page 10-32 for more information.

DNS Server Support

Up to three DNS servers can be configured (the Linux OS supports up to three DNS servers).

Network Settings in a Virtual Machine (OVA File) Installation

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

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

See the “Configuring the Network Settings” section of the Cisco Video Surveillance Virtual Machine Deployment and Recovery Guide for UCS Platforms for more information.

Understanding Device Conflicts

If a server, camera or encoder is added to Cisco VSM with duplicate settings, such as a duplicate IP address, an error can occur. Review the following information to understand how to avoid, resolve, or allow such conflicts:

- Devices with Duplicate IP Addresses, page 7-5
- Conflicts During Camera Discovery, page 7-5
- Allowing Duplicate Camera IP Addresses, page 7-6

Devices with Duplicate IP Addresses

By default, servers, encoders, or cameras with duplicate IP addresses are not allowed.

If an server or device is added with a duplicate IP address (the address is the same as an existing device), the new entry will display an *ID collision* issue. For example:

- Devices manually added will a duplicate IP address 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 server or device with an unused IP address.
- Directly connect to the device or server interface and enter a unique IP address, or ensure that the device can receive a reachable address from a DHCP server. The camera IP address must be reachable by the Media Server to which it is assigned.
- Use the **Replace Camera** or **Replace Server** option to transfer the old settings to the new device. For example, see Replacing a Camera, page 10-88.
- Delete the camera, encoder, or server and re-add it with a unique IP address.
- Enable the **Allow Duplicate IP Address** system setting to allow servers and devices to be added with duplicate IP addresses. For example, Media Servers that are installed in NATs that use the same Access IP (NAT) address. See Allowing Duplicate Camera IP Addresses, page 7-6 for more information.

Conflicts During Camera Discovery

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 "Camera Status" section on page 10-62).

  - 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 "Camera Status" section on page 10-62).

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.

See also the "Adding Cameras From Different Networks (NATs)" section on page 7-10.

Allowing Duplicate Camera IP Addresses

By default, servers, encoders, or cameras with duplicate IP addresses are not allowed and will result in an error. See Devices with Duplicate IP Addresses, page 7-5 for more information

If your network configuration requires that devices be added with duplicate IP addresses, you can enable the **Allow Duplicate IP Address** system setting. This setting allows multiple cameras with the same access IP address to be added to the Operations Manager configuration. For example, cameras with the same IP address can be added to different Media Servers in different locations.

See the following for more information:

- Adding Cameras From Different Networks (NATs), page 7-10
- Scenario 3: Cameras in Different NATs Have Duplicate Access IP Addresses, page 7-17

Resolving ID Mismatch Errors When Changing Camera IP Addresses

If cameras are configured with IP addresses (and not hostnames), and those IP addresses change, a hardware id mismatch issue can occur and the camera will be placed in the *Enabled: Critical* state (red).

This occurs because the camera's hardware ID no longer matches the device IP address. To clear this issue, correct the network configuration for each affected camera. For example:

- Scenario 1: Cameras Configured with DHCP IP Addresses, page 7-7
- Scenario 2: Cameras Configured with a Static IP Addresses, page 7-8

Note

- Medianet cameras must be configured for DHCP. Cameras that do not support Medianet can only be added using a static IP address. See Using DHCP, page 7-4 and Discovering Medianet-Enabled Cameras, page 10-32 and for more information.
- The following scenarios can also occur for cameras configured with hostnames, if the DNS entry does not update with the correct hostname to IP address mapping.

Scenario 1: Cameras Configured with DHCP IP Addresses

Cameras that revive a new DHCP-provided IP address after reboot will be placed in *Enabled: Critical* state with a hardware ID mismatch issue. This is because the IP address no longer matches the hardware address configured in the Operations Manager. This occurs for each camera where the IP address was changed.

To resolve this issue:

Cisco Cameras

The new IP address is automatically updated in Operations Manager for Cisco cameras configured with DHCP. To clear the error message, choose **Repair Configuration** from the **Device Settings** menu.

Step 1 Open the camera configuration page.

Step 2 Select the **Status** tab and verify the following:

- The device overall status is *Enabled: Critical*.
- Click the link next to the *Hardware* category to open a pop-up window.
- Verify that a *Hardware ID Mismatch* issue occurred.

See Camera Status, page 10-62 for more information.

Step 3 Select **Device Settings** > **Repair Configuration** to clear the issue.

See Repairing Camera Configuration Errors, page 10-66 for more information.

Step 4 Verify that the camera status changes to *Enabled: OK* (green).

Non-Cisco Cameras

You must manually enter the correct IP address in the camera configuration for non-Cisco cameras configured with DHCP.

Step 1 Open the camera configuration page in Operations Manager.

Step 2 Select the **Status** tab and verify the following:

- The device overall status is *Enabled: Critical*.
- Click the link next to the *Hardware* category to open a pop-up window.
- Verify that a *Hardware ID Mismatch* issue occurred.

See Camera Status, page 10-62 for more information.

Step 3 Select the **General** tab.

See General Settings, page 10-44 for more information.

Step 4 Under Access Information, enter the correct IP address for the device.

- This is the setting used by Operations Manager to communicate with the device,
- The IP address stored in Operations Manager must be the same as the device configuration.

Step 5 Verify that the camera status changes to *Enabled: OK* (green).

Scenario 2: Cameras Configured with a Static IP Addresses

If cameras are configured with a static IP address, and that address is changed in the camera's device user interface, the device is placed in *Enabled: Critical* state with a hardware ID mismatch issue. This is because the IP address no longer matches the hardware address configured in the Operations Manager. This occurs for each camera where the IP address was changed.

- If another camera has the same IP address, an *ID collision* issue occurs. See Understanding Device Conflicts, page 7-5 for more information and to resolve the issue.
- If the camera's IP address is unique, but no longer matches the entry in the Operations Manager, you must correct the entry on the camera configuration page.

Procedure

Step 1 Open the camera configuration page in Operations Manager.

Step 2 Select the **Status** tab and verify the following:

- The device overall status is *Enabled: Critical*.
- Click the link next to the *Hardware* category to open a pop-up window.
- Verify that a *Hardware ID Mismatch* issue occurred.

See Camera Status, page 10-62 for more information.

Step 3 Select the **General** tab.

See General Settings, page 10-44 for more information.

Step 4 Under Access Information, enter the correct IP address for the device.

- This is the setting used by Operations Manager to communicate with the device,

- The IP address stored in Operations Manager must be the same as the device configuration.

Step 5 Verify that the camera status changes to *Enabled: OK* (green).

Adding Cameras From Different Networks (NATs)

This document describes how to add cameras that are installed in different network (NAT) than the Cisco VSM Operations Manager.

Contents

Overview

Review the following topics to understand the two different IP addresses assigned to cameras, and how the Cisco VSM Operations Manager determines if a duplicate entry exists when adding the new device.

- Understanding Camera IP Addresses, page 7-10
- Understanding Camera IP Address Conflicts, page 7-12
- Camera Discovery and IP Addresses Conflicts, page 7-13
- Manually Adding Cameras, page 7-14

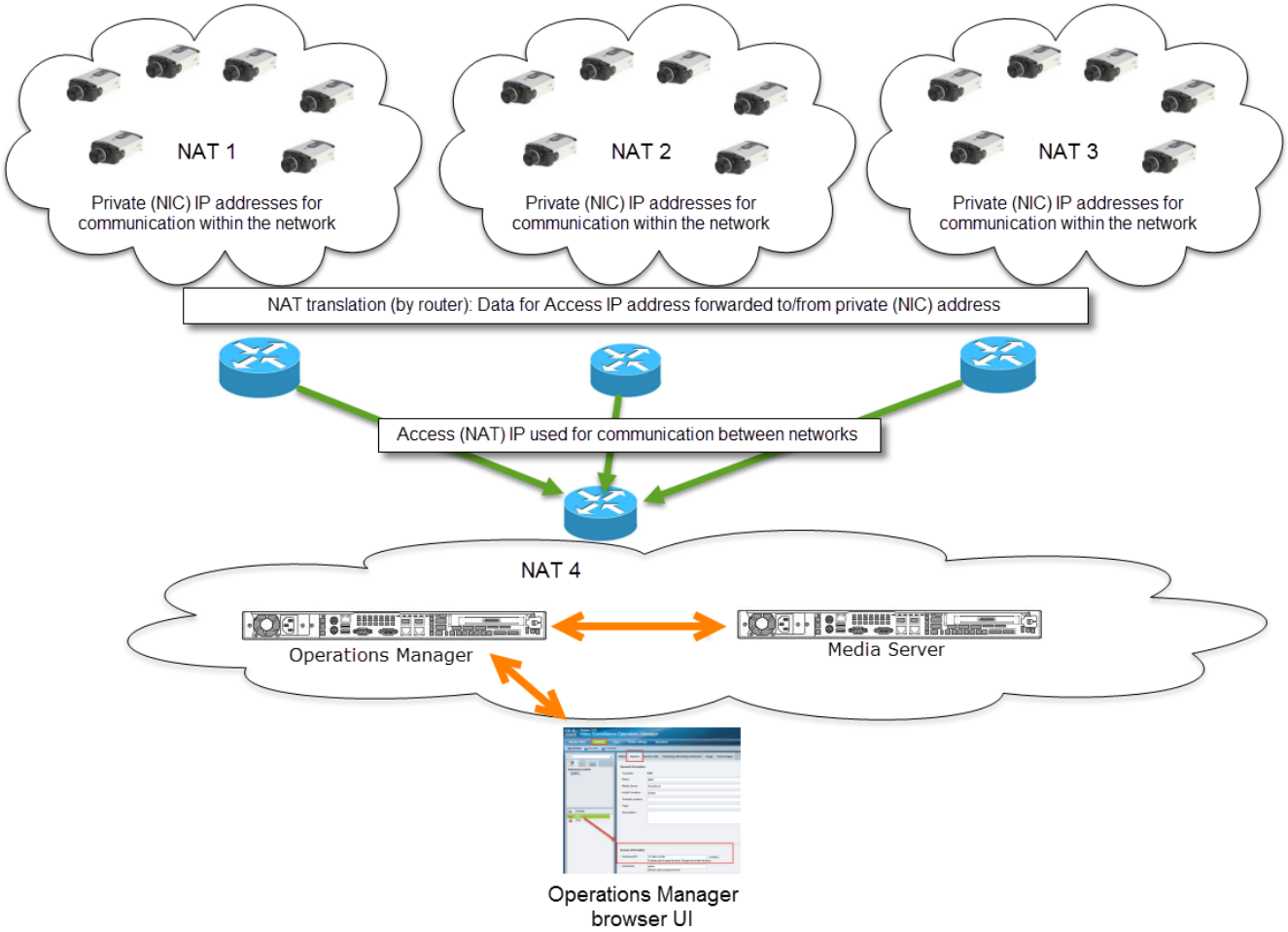
Understanding Camera IP Addresses

Each surveillance camera has two IP addresses:

- A Private (NIC) IP address—used for communication within the private network (NAT boundaries).
- An Access (NAT) IP address—used for communication between the camera and external networks.

Note If all cameras and servers are in the same network, then the Private (NIC) IP address and Access (NAT) IP address are the same. See Scenario 1: All Devices Are In the Same Network (NAT), page 7-14.

Figure 7-1 Private (NIC) and Access (NAT) IP Addresses



The network router uses network address translation (NAT) to route data from the private NIC address of a device (camera) to and from external networks. For example, in Figure 7-1, a request from the Cisco VSM Operations Manager is sent to the camera's access (NAT) IP address. The network router forwards that data to the camera's private (NIC) IP address.

To ensure data is sent to the correct device, the Operations Manager normally requires that each camera's access (NAT) IP address be unique (by default). If a camera is added or discovered, and a device entry with the same access (NAT) IP address already exists, the camera may be merged with an existing record, or an error can occur. See the "Understanding Camera IP Address Conflicts" section on page 7-12.

This document describes the following scenarios to avoid camera IP address conflicts:

Table 7-2 Camera IP Addresses: Network (NAT) Deployment Scenarios

Scenario	More Information
All devices are in the same network. Cameras are assigned static IP addresses or managed by a DHCP server that avoids IP address conflicts.	Scenario 1: All Devices Are In the Same Network (NAT), page 7-14

Table 7-2 Camera IP Addresses: Network (NAT) Deployment Scenarios (continued)

Scenario	More Information
Cameras in different networks are assigned unique static access (NAT) IP addresses.	Scenario 2: Cameras in Different NATs Use Static Access IP Addresses, page 7-16
Cameras in different networks are assigned duplicate access (NAT) IP addresses. The system setting **Allow duplicate IP addresses** is enabled to allow cameras with duplicate IPs to be added. The Operations Manager ignores IP address conflicts and allows the cameras to be added to the configuration.	Scenario 3: Cameras in Different NATs Have Duplicate Access IP Addresses, page 7-17

Understanding Camera IP Address Conflicts

A camera IP address conflict occurs if the device is assigned an IP address that is already configured on another camera that was (previously) added to Cisco VSM.

If a camera is added or discovered with a duplicate access (NAT) IP address, the following rules apply:

Cameras added with a DHCP-provided IP address

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. The device status will be *Critical* with a "Hardware ID mismatch" issue. To resolve this issue, select **Repair Configuration** from the **Device Settings** menu.

For example, if a Cisco camera is rebooted and receives a new DHCP IP address that is already used by another camera in Cisco VSM, the camera will use that IP address, but the device status will be *Critical* with a "Hardware ID mismatch" issue. Select **Repair Configuration** from the **Device Settings** menu to change the device status to *Enabled:OK* (green).

Cameras added with a static IP address

If the discovered camera uses a static IP address, however, then the camera entries are in conflict.

- If the **Allow Duplicate IP Address** system setting is enabled, the conflict is ignored and the camera is added to Cisco VSM.
- If the **Allow Duplicate IP Address** system setting not enabled (default), then both cameras are placed in a collision state. You must replace or delete one of the cameras to remove the conflict, or use the Operations Manager to reconfigure one of the cameras with a unique IP address.

For example, if you configure a static IP address on a camera using the device UI, and then add that camera to Cisco VSM, the camera is be in the *Critical* state with a "Hardware ID mismatch" issue if the IP address is already used by another Cisco VSM camera.

To resolve this issue, use the Operations Manager to reconfigure the camera with a unique IP address. The device status should change to *Enabled:OK* (green).

Viewing Camera Status

To view more information about the IP address conflict, use the camera Status page to view the "identity collision" alert.

Step 1 Select **Cameras**.

Step 2 Select a location and select the camera in conflict.

Step 3 Select the **Status** tab (see the "Camera Status" section on page 10-62).

- 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".

See the "Understanding Camera Conflicts" section on page 10-25 for more information.

Camera Discovery and IP Addresses Conflicts

Note Camera discovery occurs when an IP camera is discovered on the network and added to the Cisco VSM configuration. Camera discovery can occur automatically when the camera is added to the network, or manually triggered by an administrator. During camera discovery, Cisco VSM checks to see if a duplicate camera configuration exists. Cameras are identified 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. See the "Discovering Cameras on the Network" section on page 10-23 for more information.

Camera discovery manages camera IP addresses using the following process:

1. The Media Server detects that a camera is behind a private network and uses an access (NAT) IP address.
2. The Operations Manager determines if another camera already in the system uses the same access (NAT) IP address.
   a. If a duplicate access (NAT) IP address is found on a DHCP-enabled camera, then the discovered camera is merged with the existing camera entry. The camera's private (NIC) IP address is included in the merged entry. Select **Device Settings** > **Repair Configuration** to change the device status to *Enabled:OK* (green).
   b. If the camera uses a static IP address that is not used by another Cisco VSM camera, the camera is added normally (a collision does not occur).
   c. If the camera uses a static IP address that is already used by another Cisco VSM camera, a collision will occur.
   – If the **Allow Duplicate IP Address** system setting is *not* enabled (default), both cameras are placed in a collision state and you must replace or delete one of the cameras to remove the conflict. See the "Understanding Camera IP Address Conflicts" section on page 7-12.
   – If the **Allow Duplicate IP Address** system setting is enabled, the new camera with the duplicate access (NAT) IP address is added to Cisco VSM.

When a camera is successfully added to Cisco VSM, both the access (NAT) IP and private (NIC) IP are added to the camera entry in the Operations Manager.

Tip If auto-provisioning is enabled for the discovered camera model, the camera is also updated with settings for template, user credential, etc. See the "Enabling the Auto Configuration Defaults for a Camera Model" section on page 10-25.

Manually Adding Cameras

Cameras are manually added to Cisco VSM using the access (NAT) IP address.

If duplicate access (NAT) IP address is used, a collision will occur.

- If the **Allow Duplicate IP Address** system setting is *not* enabled (default), both cameras are placed in a collision state and you must replace or delete one of the cameras to remove the conflict. See the "Understanding Camera IP Address Conflicts" section on page 7-12.
- If the **Allow Duplicate IP Address** system setting is enabled, the new camera with the duplicate access (NAT) IP address is added to Cisco VSM.

Both the access (NAT) IP and private (NIC) IP are added to the camera entry in the Operations Manager.

Camera Network Deployment Scenarios

Scenario 1: All Devices Are In the Same Network (NAT)

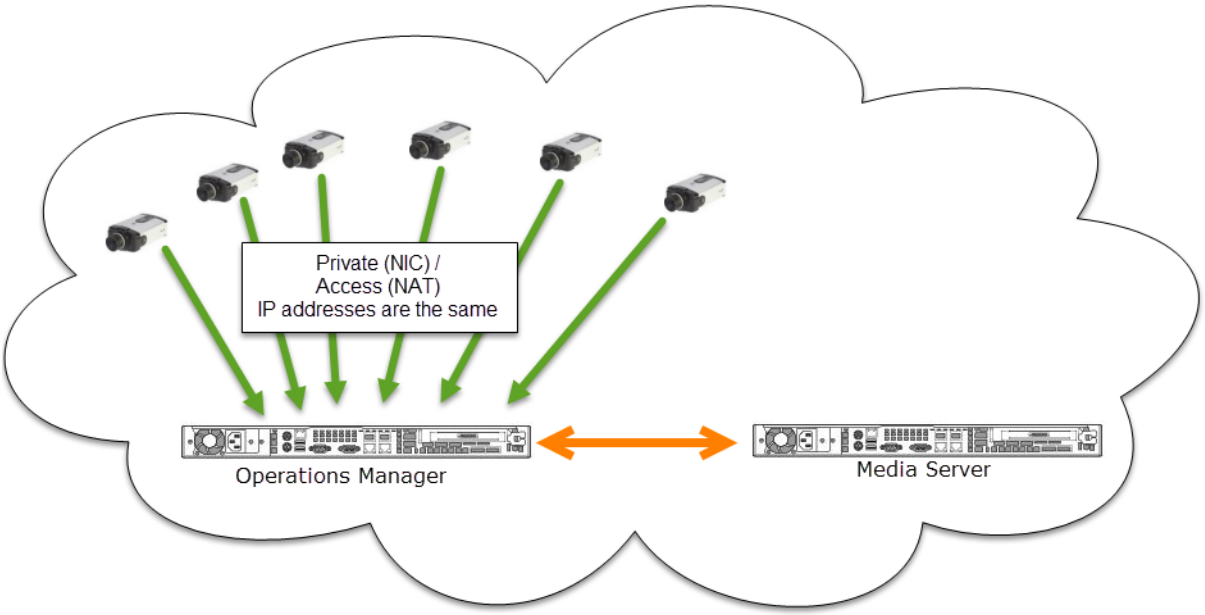
In the most basic scenario, all cameras and servers are in the same network (NAT). This includes the video surveillance cameras, Operations Manager, and Media Servers (Figure 7-2).

In this single-network scenario, the private (NIC) and access (NAT) IP addresses are the same for each camera.

Note Only the access (NAT) IP address is entered and displayed in the camera's configuration page.

Each camera should have a unique IP address, or a collision ID can occur. See the "Understanding Camera IP Address Conflicts" section on page 7-12 for more information.

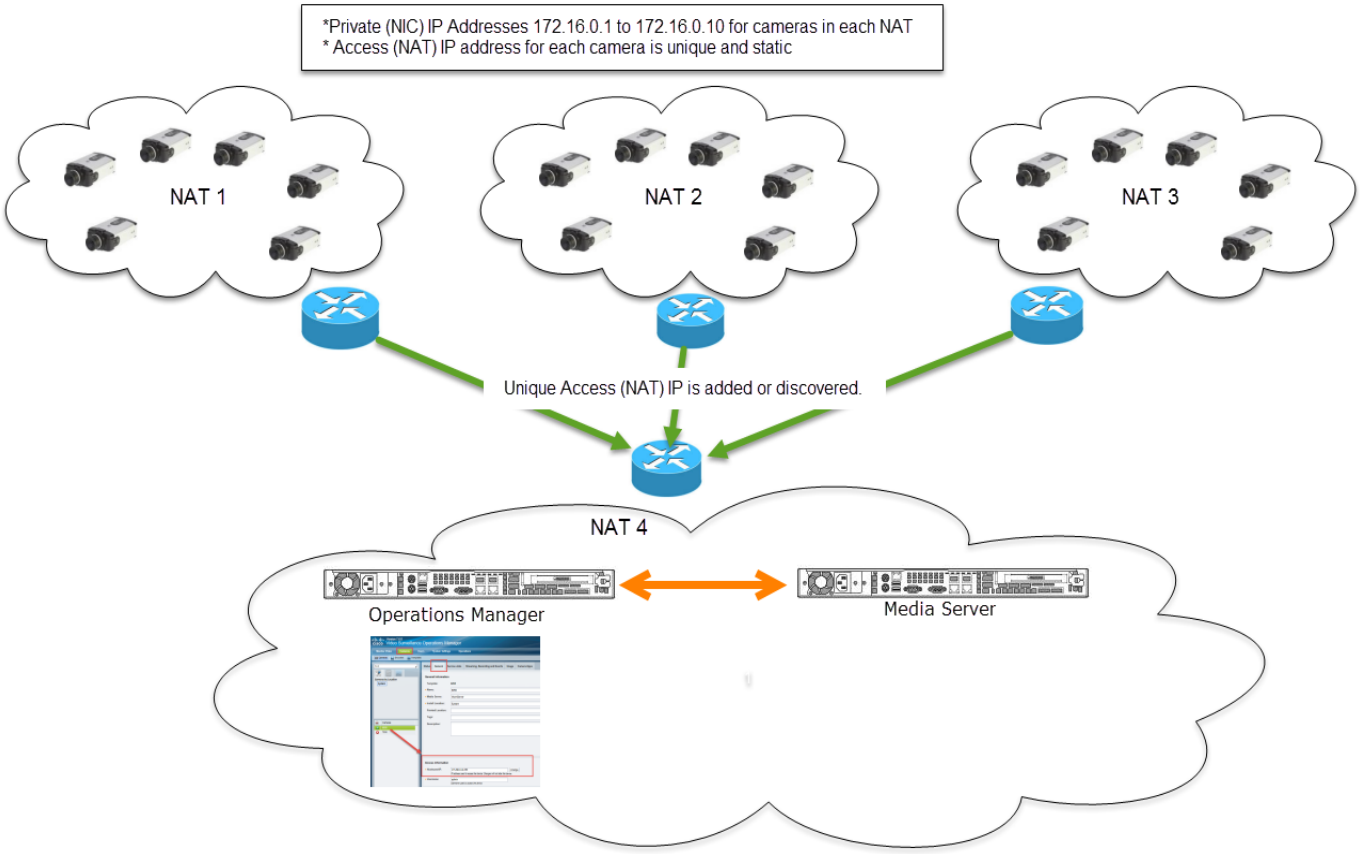
Figure 7-2 Scenario 1: All Devices in the same Network (NAT)



Scenario 2: Cameras in Different NATs Use Static Access IP Addresses

In this scenario, multiple groups of cameras are installed in different networks. The cameras in each network are assigned the same set of private (NIC) IP address. Each camera, however, is also assigned a unique static access (NAT) IP address (Figure 7-3).

Figure 7-3 Scenario 2: Cameras in Different Networks with Static "Access" (NAT) IP addresses



In this scenario:

- The camera is added using the Access (NAT) IP addresses. The Access (NAT) appears in the camera page of the Operations Manager UI.
- Only Access (NAT) IP is checked for duplicate. The Private (NIC) address is ignored during the duplicate check.
- The Access (NAT) IP addresses is static and unique, so a collision ID will not occur.
- The Private (NIC) address is taken from the IP header and added to the config.

Note

- This scenario is supported when manually adding a camera, or for automatic discovery of Medianet-enabled cameras.
- User-initiated discovery of cameras (non-Medianet devices) is not supported since the Operations Manager cannot determine that the cameras are behind a NAT (since DHCP is not used).

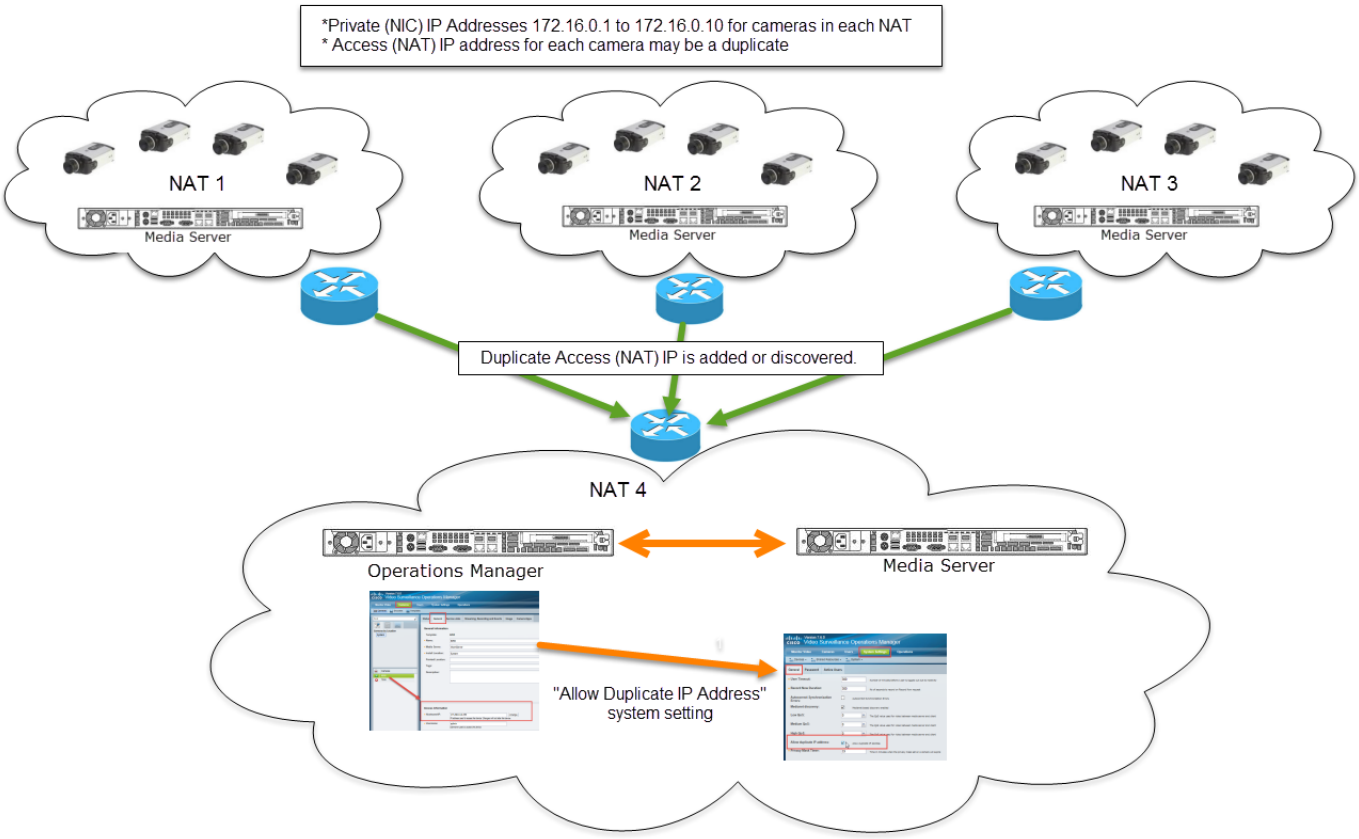
- See the "Discovering Cameras on the Network" section on page 10-23 for more information.

Scenario 3: Cameras in Different NATs Have Duplicate Access IP Addresses

In this scenario, multiple groups of cameras are installed in different networks. The cameras in each network are assigned the same set of private (NIC) IP address.

The access (NAT) IP address for each camera, however, may be a duplicate of another camera. By default, can cause a collision ID error. To avoid this, (Figure 7-4).

Figure 7-4 Scenario 3: Cameras in Different Networks with Duplicate "Access" (NAT) IP addresses



In this scenario:

- The Access (NAT) IP addresses is added or discovered.
- Only Access (NAT) IP is checked for duplicates. If a duplicate exists, a collision ID can occur. See the "Understanding Camera IP Address Conflicts" section on page 7-12.
- Select the **Allow Duplicate IP Addresses** system setting to allow duplicates. Duplicate camera entries will be ignored and the camera will be added.
- The Private (NIC) address is taken from the IP header and added to the camera config.

Understanding NTP Configuration

The server time synchronizes server operations, defines recording timestamps and backup schedules.

To ensure correct playback and system operation, we strongly recommend using a network time protocol (NTP) for all servers and devices.

Refer to the following topics for more information:

Recommended (and Default) NTP Configuration

In the default and recommended NTP configuration, the Operations Manager is configured with an NTP server, and all other servers, cameras and encoders use the Operations Manager as their NTP server. This ensures that all devices, recordings, timestamps, alerts, and other resources are synchronized.

In Figure 8-1, the cameras use their Media Servers as the NTP server, and the Media Servers use the Operations Manager as the NTP server. Since these are the default settings, no user configuration is required except to (optionally) enter a custom NTP server address for the Operations Manager server.

Figure 8-1 Recommended (and Default) NTP Configuration

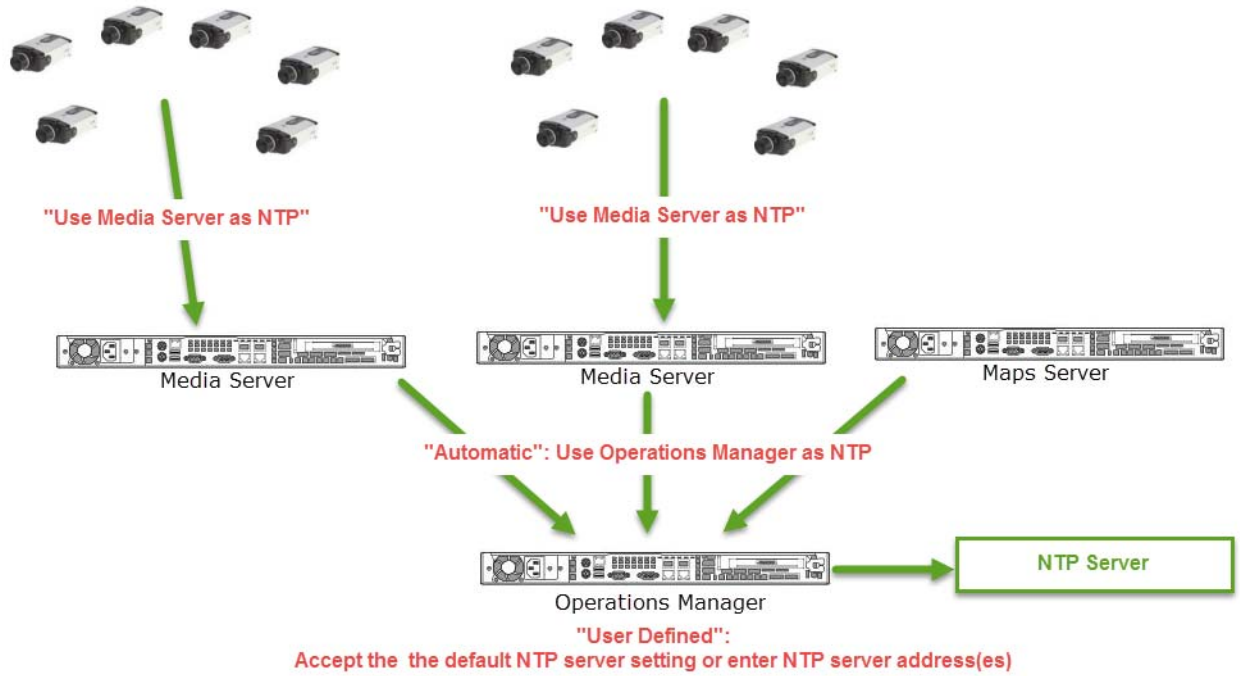


Table 8-1 Recommended NTP Configuration

Server/Device	Recommended Configuration
Operations Manager server	Enter a “User-Configured” NTP server for the Operations Manager server, including servers that are co-located with other services, such as a Media Server and/or Maps server.
Stand-alone servers	Use “Automatic” mode for all other servers. The Operations Manager is used as the NTP server, ensuring that the date and time on all servers are in sync.
Cameras and encoders	By default, cameras and encoders use the Media Server to which they are assigned as the NTP server. This ensures that the recording timestamps and schedules are in sync. **Note** The encoder NTP setting cannot be changed.

NTP Usage Notes

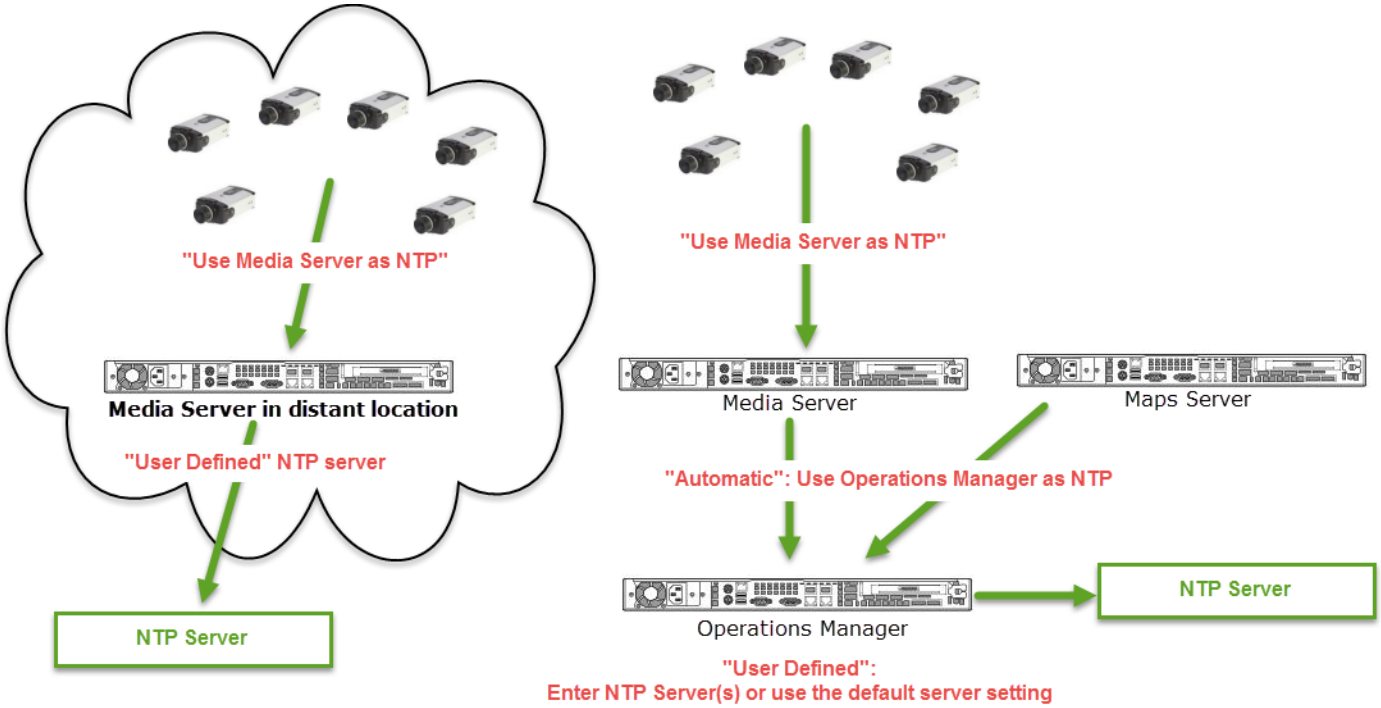
- Enter NTP Server names or IP addresses separated by space or comma.
- **Automatic** mode can only be used after NTP is configured on the Operations Manager server.
- The server will reboot if any changes are made to the NTP settings using the Operations Manager UI.
- Changes to the server time can 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.
- You can modify the NTP information for up to 10,000 cameras at a time.
- The NTP servers configured on a device are displayed in the device configuration page (under NTP Information).
- NTP settings can be configured on camera only if the camera model supports NTP configuration.
- The number of NTP servers configured on a camera are limited to the number supported by the camera model. For example, if a camera model only supports a single NTP server setting, and you attempt to add three NTP servers, the configuration will be rejected.
- 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.

Configuring Media Servers with a User-Defined NTP Server

In some situations, you may need to use different NTP server settings than the default and recommended version. This 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.

In Figure 8-2, a Media Server in a distant location is assigned a “user defined” NTP server.

Figure 8-2 NTP Settings for Media Server in a Distant Location



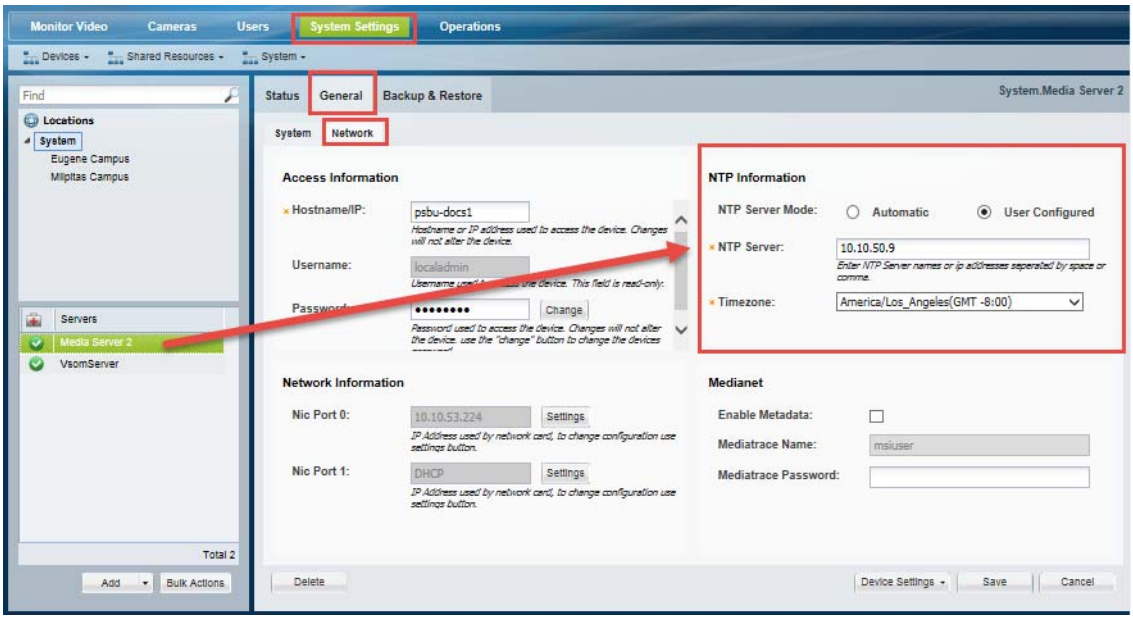
Refer to the following topics for more information:

- Changing the NTP Server for a Single Media Server, page 8-5
- Changing the NTP Server for Multiple Media Servers, page 8-6

Changing the NTP Server for a Single Media Server

To configure stand-alone Media Servers with a custom NTP server, open the Media Server network page (Figure 8-3).

Figure 8-3 Server NTP Information



Procedure

Step 1 Log in to the Operations Manager.

You must belong to a user group with *Servers and Encoders* permission. See the "Adding Users, User Groups, and Permissions" section on page 4-1 for more information.

Step 2 Go to **System Settings** > **Servers**.

Step 3 Select a location and select the Media Server.

Step 4 Select the **General** > **Network** tabs (Figure 8-3).

Step 5 Under NTP Information, select **User Configured** and enter a valid NTP server and timezone.

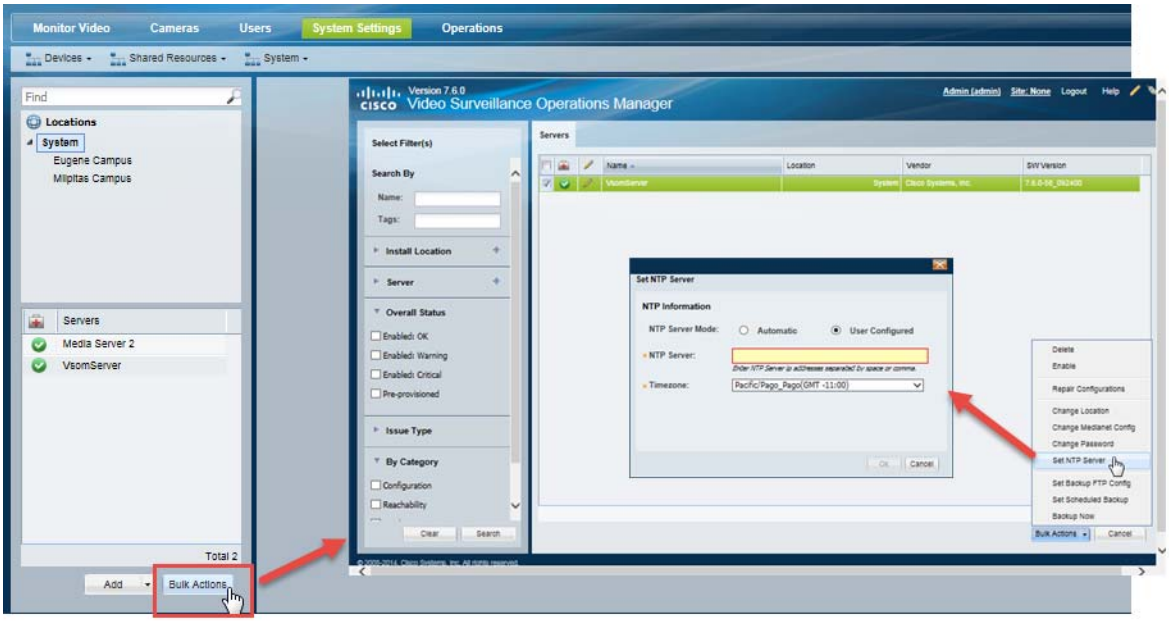
Step 6 Click **Save**.

Tip To change the NTP servers for multiple servers, see Changing the NTP Server for Multiple Media Servers, page 8-6.

Changing the NTP Server for Multiple Media Servers

Use the server Bulk Actions to change the NTP server(s) for multiple Media Servers (Figure 8-4).

Figure 8-4 Server Bulk Actions: NTP Information



Procedure

Step 1 Log in to the Operations Manager.

You must belong to a user group with *Servers and Encoders* permission. See the "Adding Users, User Groups, and Permissions" section on page 4-1 for more information.

Step 2 Go to **System Settings** > **Servers**.

Step 3 Click **Bulk Actions** (Figure 8-4).

Step 4 (Optional) Select the filter criteria (See Table 6-12 in Bulk Actions: Revising Multiple Servers, page 6-26). Leave the filters blank to display all servers.

Step 5 Click **Search**.

Step 6 Select the servers from the results list (Figure 8-7).

Step 7 Click **Set NTP Server** and enter the NTP settings:

- NTP Server Mode—Select **Automatic** to use the Operations Manager for NTP. Select **User Configured** to enter an alternate NTP server.

- NTP Server—A valid NTP server hostname or IP address. Enter multiple entries separated by a space or comma.
- Timezone—The timezone where the server is located.

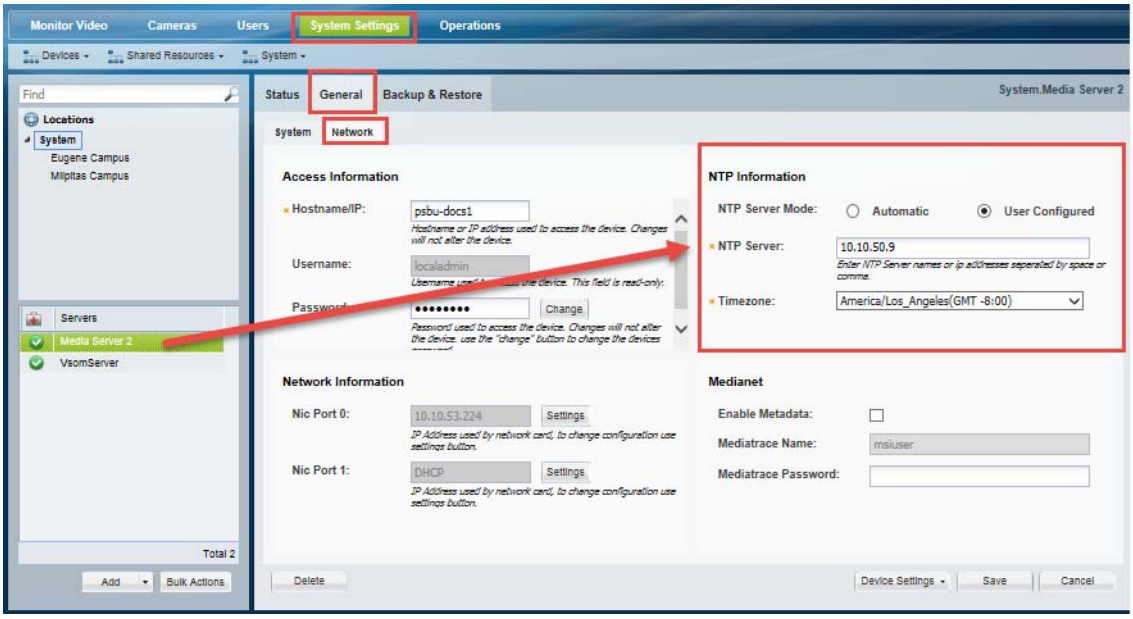
Step 8 Click **OK**.

Step 9 Click **Yes** to confirm and wait for the job to complete.

A job is created for each server being updated.

Step 10 (Optional) To confirm the new NTP setting, open the server configuration page, select the **General** > **Network** tab (Figure 8-5), and verify that the NTP server address is displayed under NTP Information.

Figure 8-5 Server NTP Information

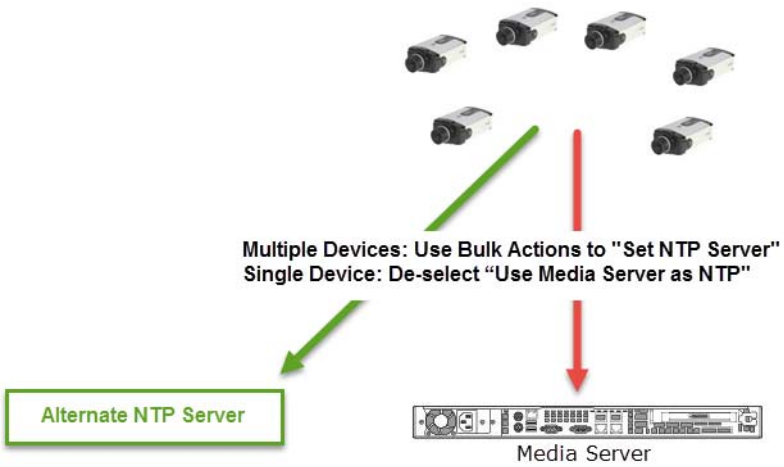


Configuring Cameras with a User-Defined NTP Server

If your configuration requires that cameras use an NTP server that is not the Media Server, you can enter a custom NTP server address for a single camera, or for multiple cameras.

Figure 8-6 shows cameras that are configured with a custom NTP server.

Figure 8-6 Cameras With an NTP Server Different than the Media Server



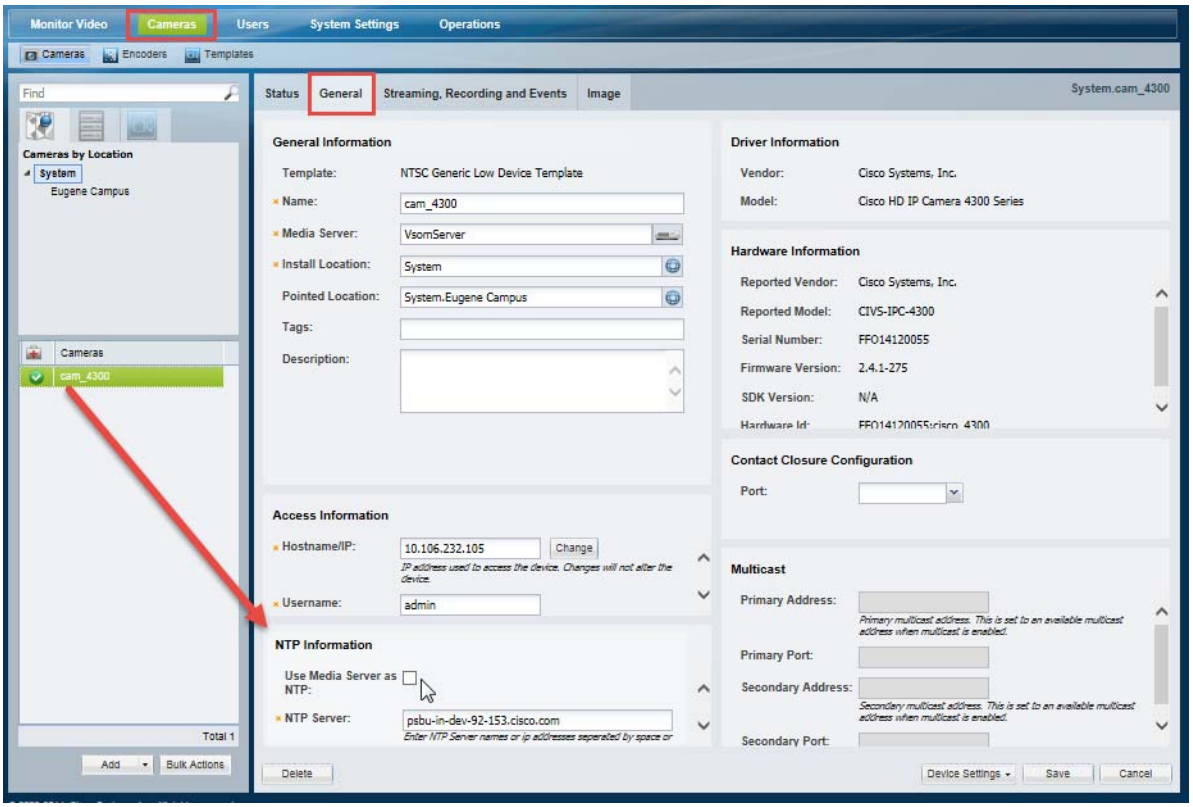
Refer to the following for more information:

- Changing the NTP Settings for a Single Camera, page 8-9
- Changing the NTP Server for Multiple Cameras, page 8-10

Changing the NTP Settings for a Single Camera

To change the NTP setting for a single camera, deselect **Use Media Server as NTP** in the camera settings page and enter a new NTP server address (Figure 8-7). The custom NTP server(s) will be used even if the camera is moved to a different Media Server,

Figure 8-7 Camera NTP Information



Procedure

Step 1 Log in to the Operations Manager.

You must belong to a user group with *Cameras* permission. See the "Adding Users, User Groups, and Permissions" section on page 4-1 for more information.

Step 2 Select **Cameras**.

Step 3 Select a location and select the camera name.

Step 4 Select the **General** tab (Figure 8-7).

Step 5 Under NTP Information, de-select **Use Media Server as NTP** and enter a valid NTP server IP address.

Step 6 Click **Save**.

Note

- The NTP server will be used even if the camera is moved to a different Media Server.

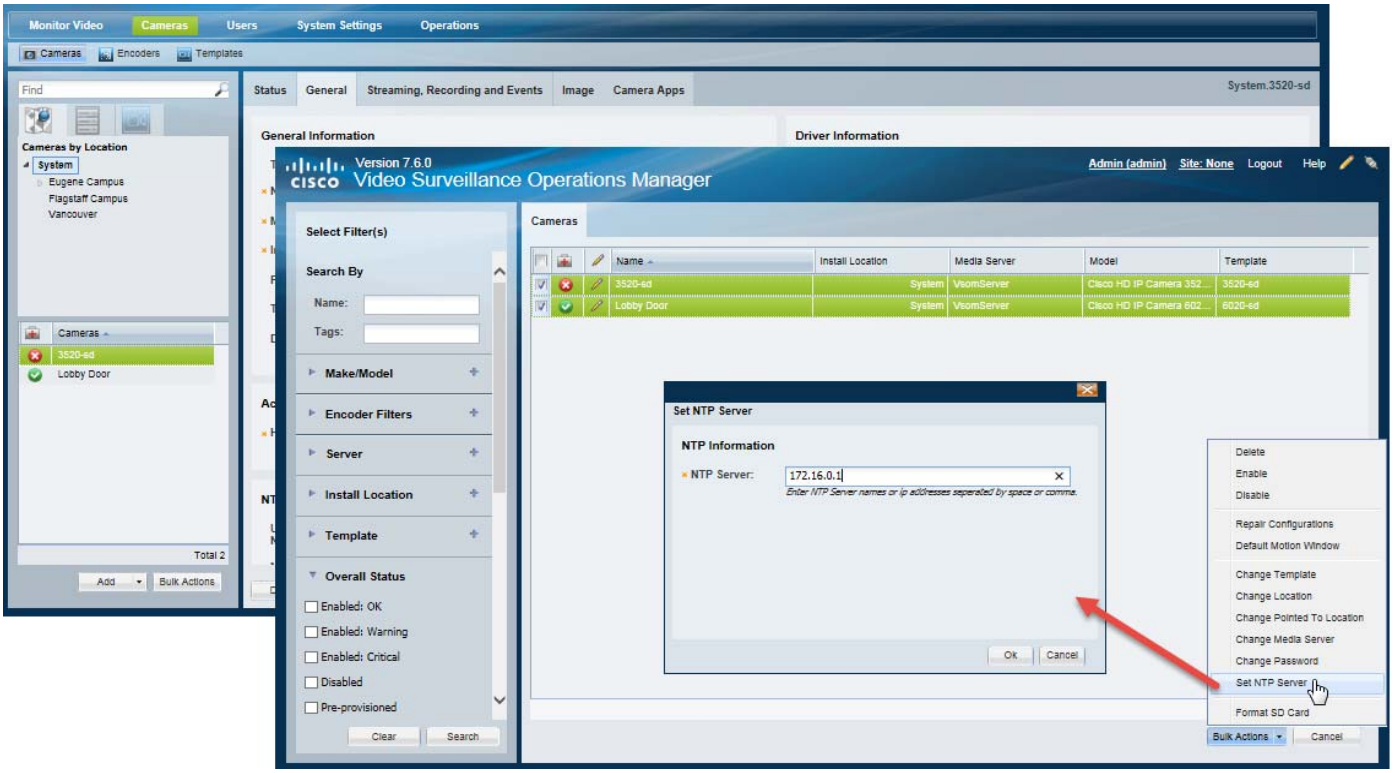
- You can also use Bulk Actions to change the NTP setting for multiple cameras, which also automatically de-selects the **Use Media Server as NTP** setting. If the camera is ever re-assigned to a different Media Server, the device will retain the user-defined NTP address entered in Bulk Actions, not the Media Server address.

Changing the NTP Server for Multiple Cameras

Use Bulk Actions to change the NTP setting for multiple cameras (Figure 8-8). The selected cameras will receive time and date settings from the custom NTP server(s), and not the Media Server.

Using Bulk Actions automatically de-selects the camera's **Use Media Server as NTP** setting. If the camera is ever re-assigned to a different Media Server, the device will retain the user-defined NTP address entered in Bulk Actions, not the Media Server address.

Figure 8-8 Camera Bulk Actions: Setting NTP Information for Multiple Cameras



Procedure

Step 1 Log in to the Operations Manager.

You must belong to a user group with *Cameras* permission. See the "Adding Users, User Groups, and Permissions" section on page 4-1 for more information.

Step 2 Select **Cameras**.

Step 3 Click **Bulk Actions** (Figure 8-8).

Step 4 (Optional) Select the filter criteria (See Table 10-20 in Bulk Actions: Revising Multiple Cameras, page 10-92). Leave the filters blank to display all devices.

Step 5 Click **Search**.

Step 6 Select the cameras from the results list (Figure 8-7).

Step 7 Click **Set NTP Server** and enter a valid NTP server IP address. Enter multiple entries separated by a space or comma.

Step 8 Click **OK**.

Step 9 Click **Yes** to confirm and wait for the job to complete.

A job is created for each camera being updated.

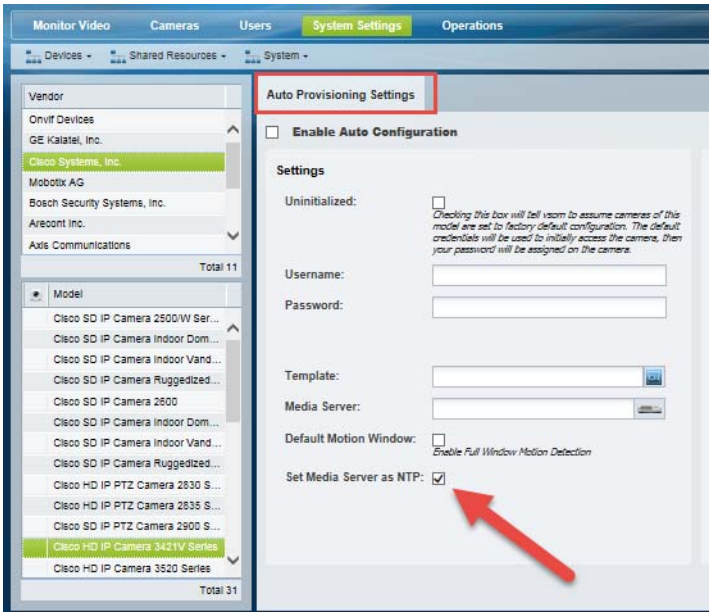
Step 10 (Optional) To confirm the new camera NTP setting, open the camera configuration page, select the **General** tab (Figure 8-7), and verify that the NTP server address is displayed under NTP Information.

Defining the NTP Setting During Camera Auto-Discovery

By default, the Media Server is used as a camera's NTP server when the device is added to Cisco VSM (see Figure 8-1).

When a camera is discovered on the network, the Media Server is also used as the camera's NTP server by default. To override this option, and retain any NTP address(es) previously configured on the device, deselect the **Use Media Server as NTP** option in the auto configuration settings (Figure 8-9).

Figure 8-9 Device Auto Configuration



If an NTP server is not configured on the device, you must update the camera settings to either enter an NTP server address or select **Use Media Server as NTP**.

- This setting is displayed only for camera models that support NTP.
- You must belong to a user group with *Cameras* permission. See the "Adding Users, User Groups, and Permissions" section on page 4-1 for more information.
- See the "Configuring Cameras with a User-Defined NTP Server" section on page 8-8 for information to define a new NTP server for one or more cameras.

Note Auto-configuration applies a set of basic configurations to cameras that are discovered on the network. Auto-configuration is disabled for all camera models by default. See Understanding Discovery and Auto-Configuration, page 10-23 for more information.

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

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, add the server to the Operations Manager configuration and select the Media Server *Service Type*. You can then configure Advanced settings, such as the high-availability role and associate cameras and other attributes to the Media Server to support video streaming, storage and playback.

Each deployment can include multiple Media Servers. A single Media Server instance can run on the same server as the Operations Manager server (to create a co-located server), and additional Media Servers can be added as stand-alone servers.

Requirements

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

Table 9-1 Media Server Requirements

Requirements	Requirement Complete? (✓)
You must belong to a user group with *Servers & Encoders* permissions. See the "Adding Users, User Groups, and Permissions" section on page 4-1 for more information.	❑
A physical or virtual server that has the Media Server service enabled. • A single physical or virtual server can host both the Media Server and Operations Manager applications (called a co-located server). • Additional Media Servers can be added as stand-alone servers. • Media Servers can also be co-located with a Maps Server. **Related Documentation** • Understanding Server Services, page 6-3 • Physical server installation: – (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 Machine installation—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 server setup—Cisco Video Surveillance Management Console Administration Guide. • Adding the server and enabling the Media Server service—Configuring Servers, page 6-1	❑

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.	• Configuring Servers, page 6-1 • Summary Steps to Add or Revise a Server, page 6-8
Step 2	Log on to the Operations Manager.	Logging In and Managing Passwords, page 1-18.
Step 3	(Co-located server) **a.** Select the default **VSOMServer**. **b.** In the Services section, select the **Media Server** service.	Media Server Settings, page 9-5 Services, page 6-11
Step 4	(Stand-alone server) Add the server as a **Media Server**.	Viewing Media Server Status, page 9-9
Step 5	(Optional) Click the **Advanced** icon to configure additional options.	• Media Server Settings, page 9-5 – High Availability Options, page 9-6 – Partition Settings, page 9-6 – Storage Management Settings, page 9-8 – Viewing Media Server Status, page 9-9
Step 6	Add cameras and encoders and associate the devices with the Media Server. **Note** Cameras/encoders and their associated Media Servers must belong to the same Site (you cannot associate a camera in Site A to a Media Server in Site B).	• Adding and Managing Cameras, page 10-1 • Adding Encoders and Analog Cameras, page 16-1 • Understanding Sites, page 23-3

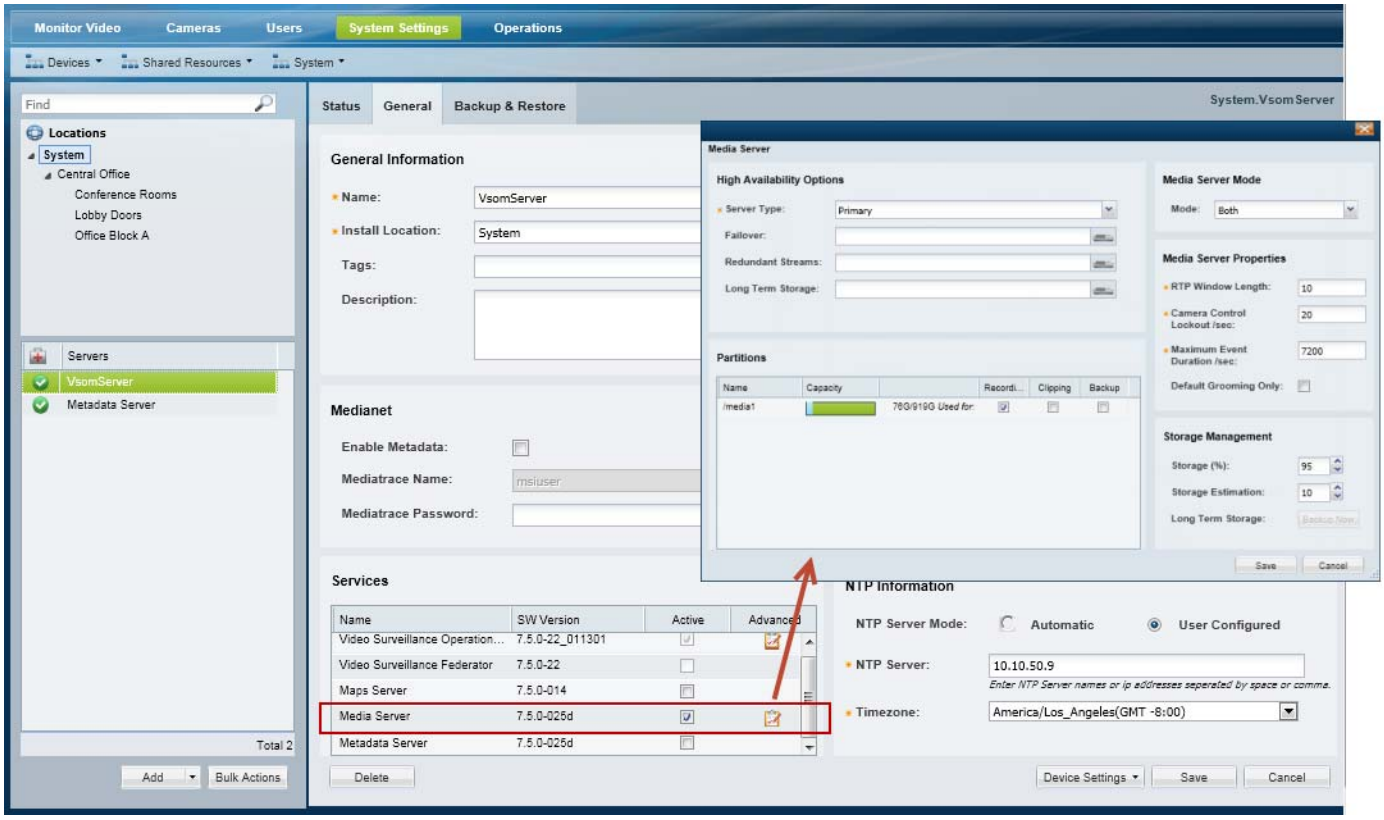
Media Server Settings

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

Accessing the Media Server Advanced Settings

1. Select the server that hosts the Media Server service.
2. Under Services, click the **Advanced** icon (Figure 9-1).
3. In the pop-up window, enter the available settings as described in this document (Figure 9-1).

Figure 9-1 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:

Table 9-2 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: Cisco Media Servers" section on page 17-1.
- 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.

Table 9-3 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 and Viewing Video Clips" section on page 2-16 for more information.
Backups	The partition(s) used for long term storage backup files. See Archiving Recordings to a Long Term Storage Server, page 17-16.

Media Server Mode (Dynamic Proxy)

Click the **Advanced** icon and select the **Media Server Mode** to enable or disable the Dynamic Proxy feature on the server. See the "Using Dynamic Proxy to Monitor Video From Remote Sites" section on page 23-1 for more information.

Table 9-4 Dynamic Proxy (Media Server Mode)

Field	Settings
Media Server Only	Disables Dynamic Proxy functionality on the server. The Media Server is used to support cameras and encoders and to deliver video directly to the user.
Both	The server can be used as a normal Media Server, and as a Dynamic Proxy.
Dynamic Proxy Only	The server is used exclusively as a Dynamic Proxy and cannot manage cameras or be used for other Media Server tasks.

Media Server Properties

Select the **Media Server Properties** to define the following.

Table 9-5 Media Server Properties

Field	Settings
RTP Window Length	The maximum number of packets the Media Server buffers per stream to determine packet loss (before declaring a lost packet). This is also known as the jitter window length. This setting may need to be changed on a system with excessive packet delay on the network. **Note** This value is normally set to 1 but may need to be increased on networks where packets can get delayed.
Camera Control Lockout / sec	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 *When Manual PTZ idle for* setting is defined in the camera PTZ *Advanced Settings*. For more information, see the following: • Defining the User Group PTZ Priority, page 10-71 • Configuring Advanced Settings, page 10-77
Default Grooming Only	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). **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 *Retain continuous recordings* and *Retain event recordings* settings will not apply for the cameras assigned to the Media Server. See the "Streaming, Recording and Event Settings" section on page 10-48. **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 10-48.

Storage Management Settings

Under Services, click the **Advanced** icon and enter the **Storage Management** settings to define how the storage space on a volume is used (Figure 9-1).

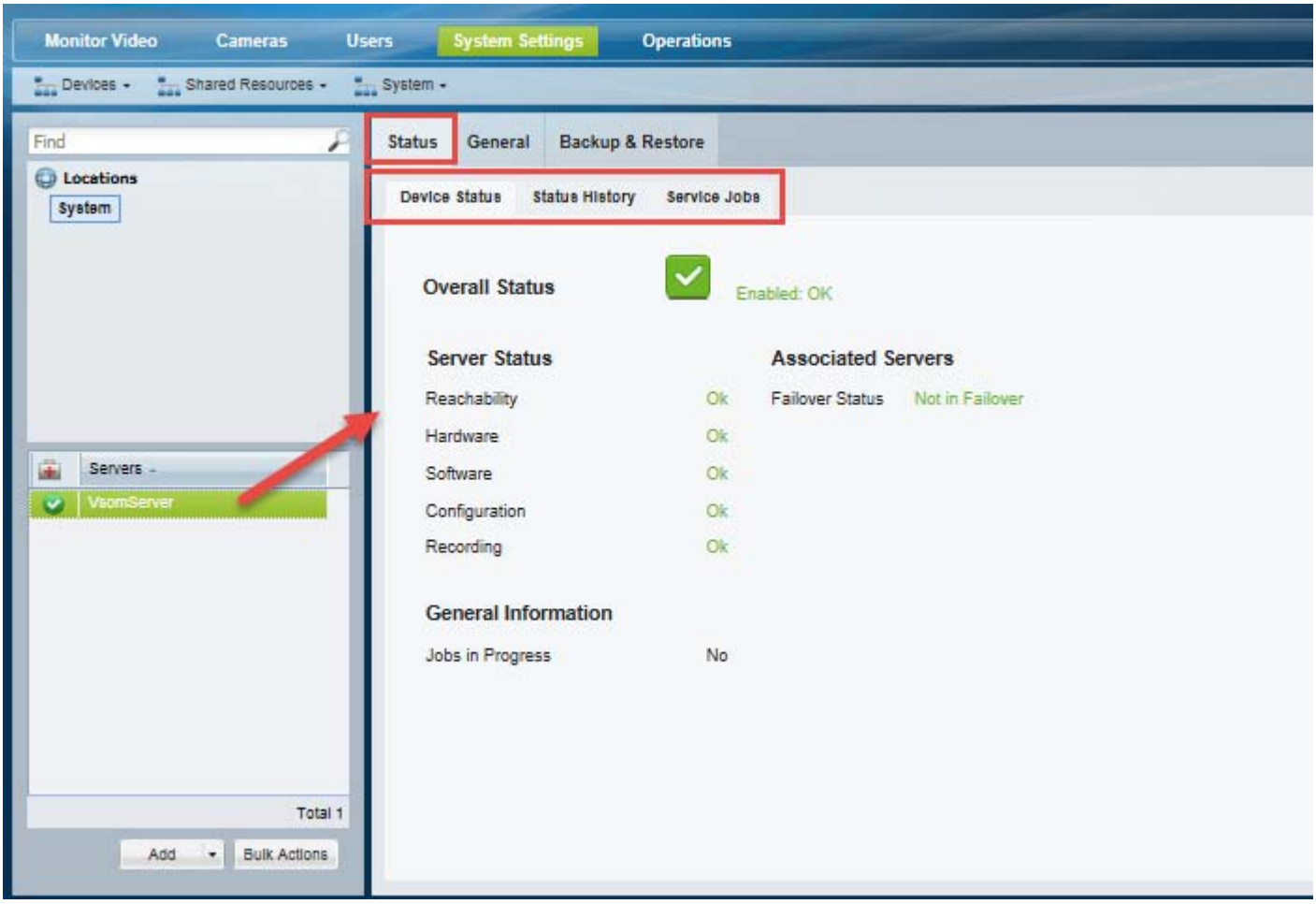
Table 9-6 Storage Management

Field	Settings
Storage (%)	The maximum amount a disk can be full before it is declared unusable for any further recording. When the disk reached this percentage, the 200 oldest media files are groomed (deleted), until the free disk space is less that the Storage (%). • 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. For example, if the *Storage %* is set to 90%, and a camera template *Retain event recordings* setting is **Max Possible**, event recordings will be deleted once the disk repositories are 90% full.
Storage Estimation(%)	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. 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. See the "Streaming, Recording and Event Settings" section on page 10-48 for more information on the **Verify Recording Space** option.
Long Term Storage	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. **Note** This button is enabled only if an LTS server is configured. See the "High Availability: Cisco Media Servers" section on page 17-1 for more information.

Viewing Media Server Status

Select the Media Server **Status** tab (Figure 9-2) to display information about the device health and service jobs (for the devices managed by the server).

Figure 9-2 Media Server Device Status



Procedure

Step 1 Select **System Settings > Servers**.

Step 2 Select a location and select a Media Server from the list.

Step 3 Select the **Status** tab.

Step 4 Select one of the following tabs:

- Device Status, page 9-10
- Status History, page 9-10

- Service Jobs (Media Server), page 9-11

Device Status

Displays a snapshot of the server health status, and the device attribute that is experiencing the error. The server's device health impacts the server's ability to communicate with cameras, stream video over the network, or record video.

Table 9-7 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**.

Related Information

Viewing Server Status, page 6-29

Device Status: Identifying Issues for a Specific Device, page 19-9

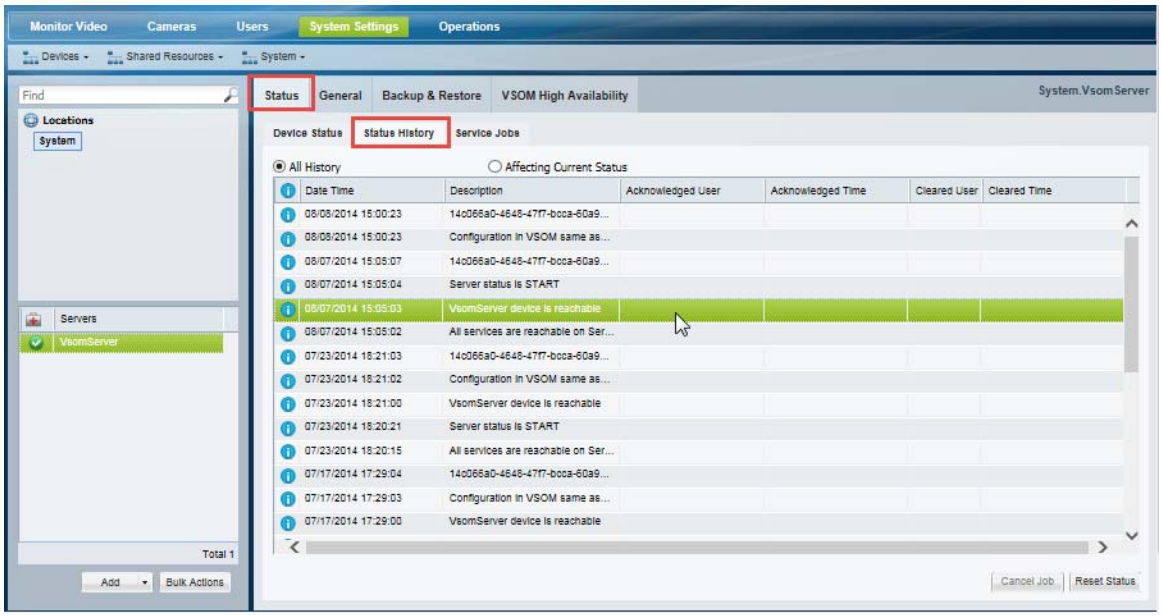
Tip Click **Refresh Status** to reload the current device status.

Status History

Click the **Status History** tab for additional details (Figure 9-3). The history page displays the specific health events that impact the device status.

- (Optional) Click **Affecting Current Status** to display only the alerts causing the current problem.
- (Optional) Double-click an entry to display the alert details (Figure 9-3). Alerts can include multiple events for the same issue. See Understanding Events and Alerts, page 19-2.
- (Optional) Double-click an event to display the event details. Alerts can include multiple events for the same issue.

Figure 9-3 Status History



Service Jobs (Media Server)

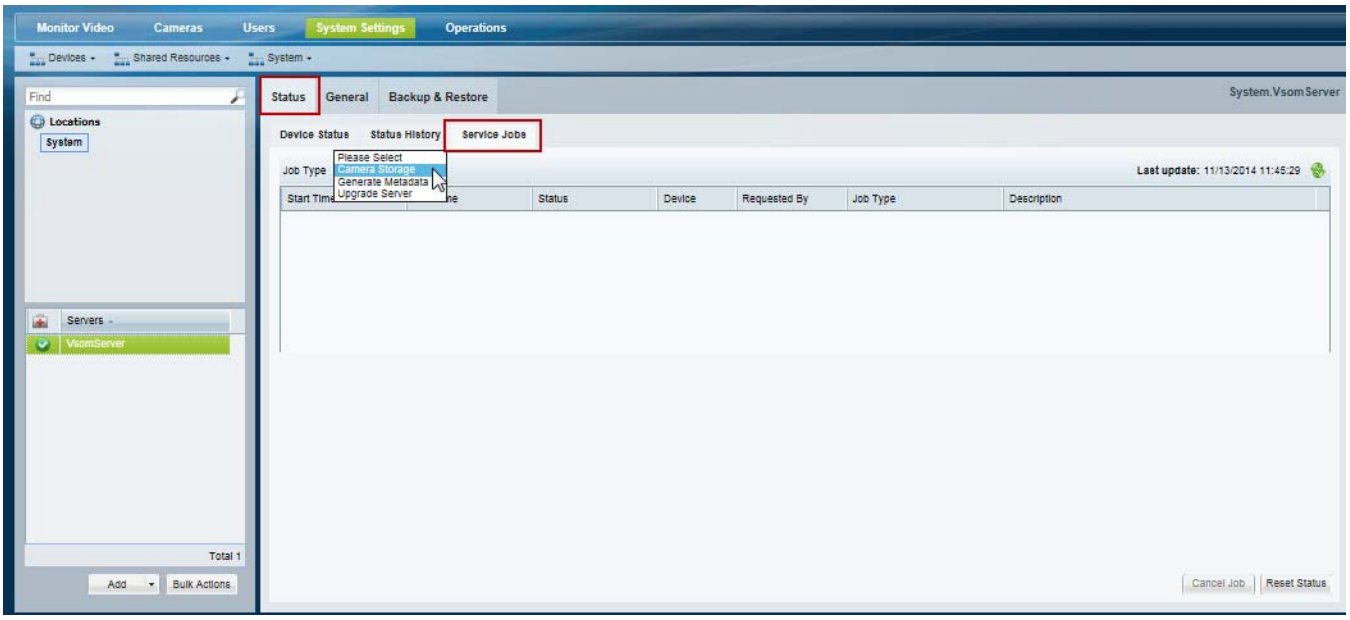
Use the Service Jobs tab (Figure 9-4) to view information about the jobs processed on the Media Server for all devices (cameras and encoders) assigned to that Media Server.

For example, job types can include:

- Camera Storage
- Generate Metadata
- Upgrade Server

Click an entry to view additional details about the job. The details also include the status and results of the job.

Figure 9-4 Service Jobs



Tip To view the service jobs for a specific cameras or encoders managed by the Media Server, select the Service Jobs tab in the camera configuration page. The camera and encoder job types may be different from the server options. See the camera "Service Jobs (Cameras)" section on page 10-65.

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. De-select this option, if necessary.

Contents

Note See also Upgrading Cisco Camera and Encoder Firmware, page 26-19.

Overview

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

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 16-1 for more information.

Requirements

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

Table 10-1 Requirements

Requirements	Requirement Complete? (✓)
You must belong to a user group with *Cameras* permission. See the "Adding Users, User Groups, and Permissions" section on page 4-1 for more information.	❑
At least one Media Server must be enabled. See the "Configuring Media Server Services" section on page 9-1 for more information.	❑
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 10-7 for more information.	❑
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 16-1 for more information.	❑
The IP address used to access the device on the network. **Note** All edge devices (such as cameras and encoders) must added to a server using a local (non-NAT) addresses.	❑
Medianet cameras must be configured for DHCP. Cameras that do not support Medianet can only be added using a static IP address.	❑
The camera username and password used to access the device on the network.	❑

Summary Steps

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

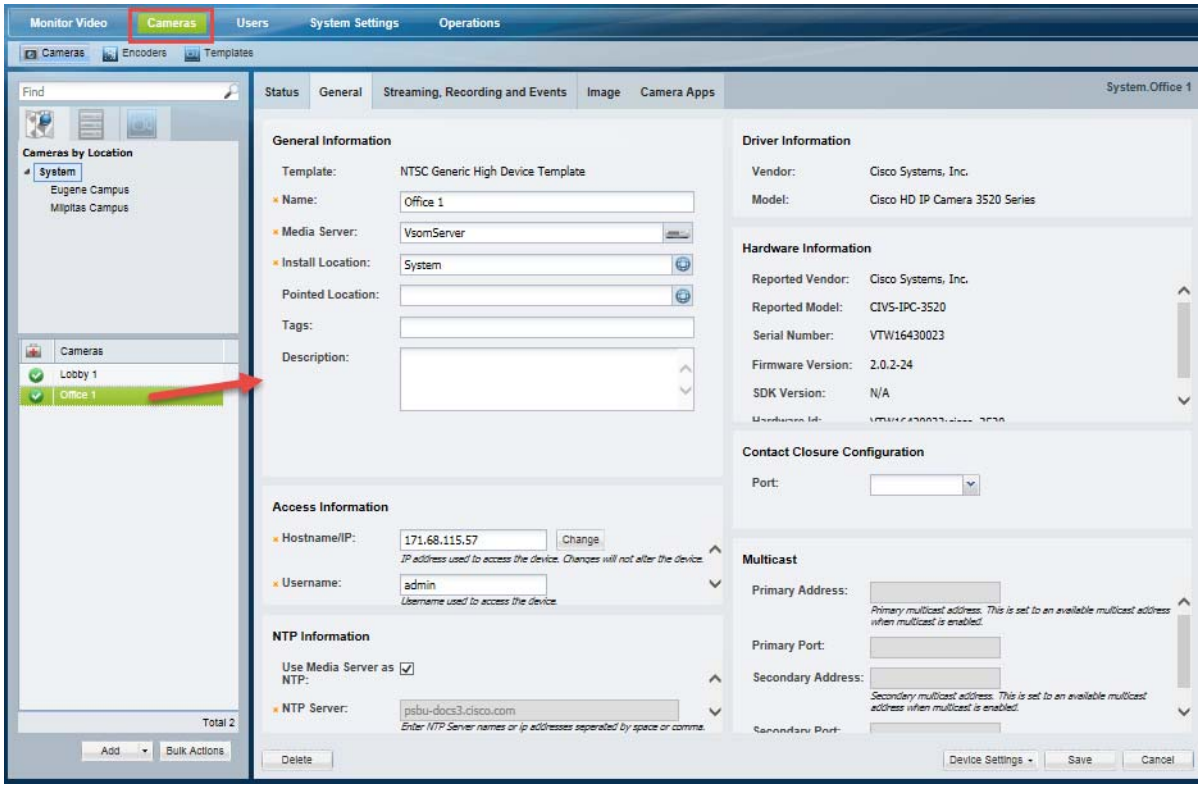
	Step	More Information
Step 1	Log on to the Operations Manager.	Logging In and Managing Passwords, page 1-18
Step 2	Configure recording schedules	• Defining Schedules, page 11-1
Step 3	(Optional) Add camera templates.	• Adding and Editing Camera Templates, page 12-1 • Configuring Continuous, Scheduled, and Motion Recordings, page 12-7
Step 4	(Optional) Add camera encoders to support analog cameras.	Adding Encoders and Analog Cameras, page 16-1
Step 5	Add one or more cameras.	Understanding the Methods to Add Cameras, page 10-9 • Manually Adding a Single Camera, page 10-11 • Importing or Updating Cameras or Encoders Using a CSV File, page 10-17 • Discovering Cameras on the Network, page 10-23 • Adding Cameras from an Existing Media Server, page 10-38
Step 6	Edit additional camera settings.	Editing the Camera Settings, page 10-42
Step 7	(Optional) Create a custom configuration for a single camera.	Creating a Custom Template for a Single Camera, page 12-5
Step 8	Configure the Image Settings, such as PTZ, motion detection, and brightness and contrast.	Image Settings, page 10-56 • Configuring Camera PTZ Controls, Presets, and Tours, page 10-67 • Configuring Motion Detection, page 10-82 • Photographic Controls, page 10-56
Step 9	Configure the high availability options.	Configuring the High Availability Options for a Camera or Template, page 10-57
Step 10	Create actions that are triggered by camera events.	"Using Advanced Events to Trigger Actions" section on page 13-7

Viewing Cameras

To display cameras already configured on the system, click **Cameras** and then choose the **Cameras** tab (Figure 10-1). You can view the cameras for a location, Media Server, or template by clicking one of the icons described below Figure 10-1.

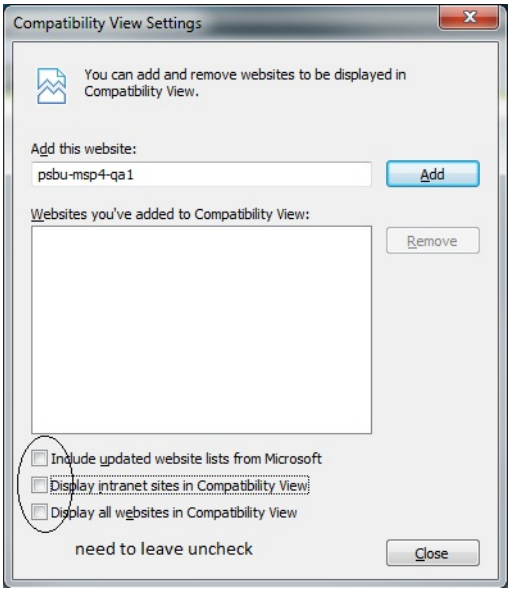
Click a camera name to view and edit the settings for that camera. Click a template name to edit the settings applied to all cameras associated with the template.

Figure 10-1 Cameras Tab



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 10-1). The cameras assigned to that location are listed by name. Click a camera name to display and edit the camera settings. **Tip** See the "Creating the Location Hierarchy" section on page 5-1.
Cameras by Media Server	Displays the cameras assigned to each Media Server. If only one Media Server is used, all cameras will be listed. See the "Configuring Media Server Services" section on page 9-1
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. See the "Adding and Editing Camera Templates" section on page 12-1 for more information.

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 10-2).

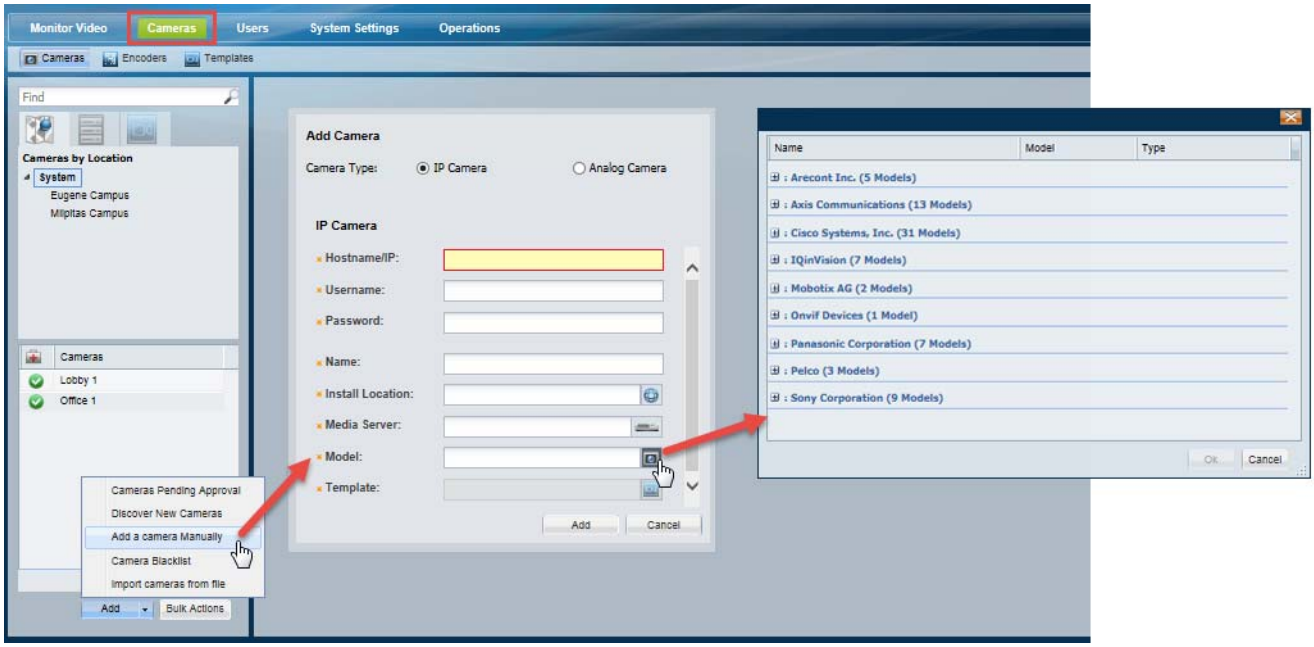
Step 2 Select the Camera Type: IP Camera or Analog Camera.

Step 3 Click the **Model** field.

- A list of supported cameras for that camera type and the Cisco Video Surveillance release is displayed (Figure 10-2).

Step 4 Expand the Manufacturer names to view the list of supported models.

Figure 10-2 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

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

- Understanding the Methods to Add Cameras, page 10-9
- Pre-Provisioning Cameras, page 10-10
- Managing Cameras with Duplicate IP Addresses, page 10-22
- Understanding Discovery and Auto-Configuration, page 10-23
- Discovering Medianet-Enabled Cameras, page 10-32

Understanding the Methods to Add Cameras

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

Table 10-2 Summary of Add Camera Methods

Add Method	Description
Manually Adding a Single Camera, page 10-11	Add a single camera from the Camera configuration page. All required settings must be entered, although you can *pre-provision* the camera if it is not yet available on the network.
Importing or Updating Cameras or Encoders Using a CSV File, page 10-17	Multiple cameras can be imported from a *comma separated value* (CSV) file that defines the camera configurations. You can choose to *pre-provision* the cameras, and add cameras with partial configurations, if necessary. This same method can be used to update existing camera configurations. **Tip** You can import network (IP) cameras, encoders and analog cameras.
Discovering Cameras on the Network, page 10-23	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. If the *auto configuration* 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 *Cameras Pending Approval* 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.

Table 10-2 Summary of Add Camera Methods (continued)

Add Method	Description
Adding Cameras From a 6.x or 7.x Media Server, page 10-38	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. 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. **Note** Cameras are kept in *pre-provisioned* state (see the "Camera Status" section on page 10-62). Deleted cameras (and their associated recordings) are permanently removed and cannot be restored. See the following for related information: • Cisco Video Surveillance Migration Guide
Adding Unknown Cameras During a Media Server Synchronization, page 10-39	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 *Cameras Pending Approval* 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.

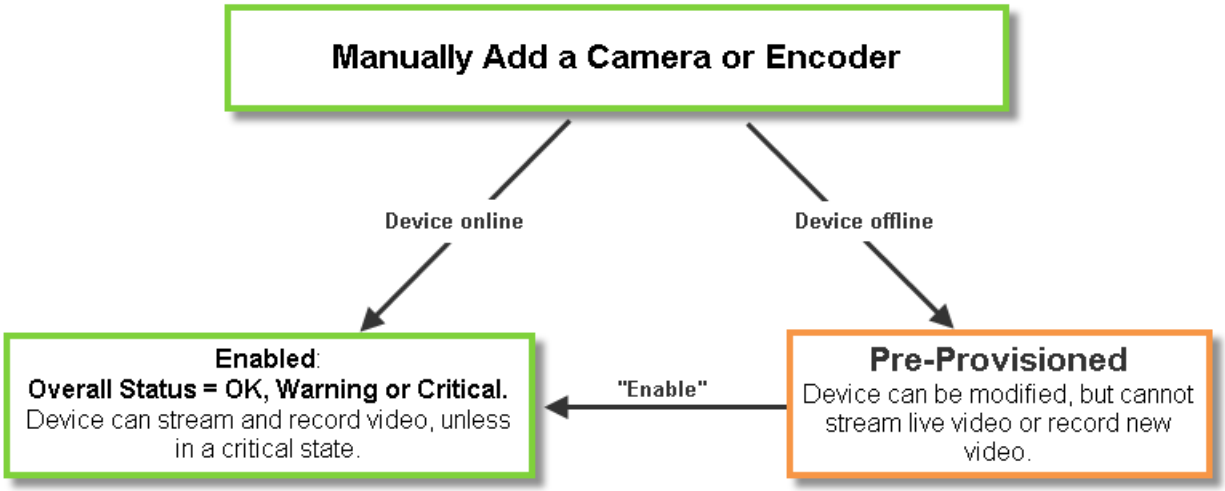
See the "Camera Status" section on page 10-62 for more information.

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 14.

If the device is not available on the network, it can be added in *pre-provisioned* state (Figure 10-3).

Figure 10-3 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 9-9
  - Creating the Location Hierarchy, page 5-1
  - Adding and Editing Camera Templates, page 12-1

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 10-42.

Network (IP) Camera Rules and Settings

The camera must be accessible on the network if the device is added in *Enabled* state (Figure 10-3).

- 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 10-10 and the "Camera Status" section on page 10-62

Table 10-3 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. • The *Installed* and *Pointed* 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. • The camera and the associated Media Server must be in the same Site. See the "Understanding Sites" section on page 23-3 for more information.
Media Server	Select the Media Server responsible for storing and playing video from the camera. The camera and the associated Media Server must be in the same Site. See the "Understanding Sites" section on page 23-3 for more information.
Model	Select the camera model.
Template	Select a camera template from the pop-up window. • 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 10-42. • 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 12-1 for more information.

Table 10-3 Network Camera General Settings

Setting	Description
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 12-11 for more information.	
Primary Address	(Optional) Enter the multicast IP address where the camera's primary video stream (Stream A) should be sent. This field is enabled only if the camera's template Stream A is configured for multicast. Addresses must be in the proper address range. • 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 **Note** Public addresses must be individually assigned by IANA (Internet Assigned Numbers Authority)
Primary Port	Enter the port value used by Cisco Video Surveillance to listen to the camera's primary video stream.
Secondary Address	(Optional) Enter the multicast IP address where the camera's secondary video stream (Stream B) should be sent. This field is enabled only if the camera's template Stream B is configured for multicast. Addresses must be in the proper address range. • 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 **Note** Public addresses must be individually assigned by IANA (Internet Assigned Numbers Authority)
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 16-4.
- 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 16-1 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.

The following table describes the settings available for analog cameras, which includes settings for the encoder that provides network connectivity.

Table 10-4 Analog Camera General Settings

Setting	Description
Encoder	Select the encoder that supports the analog camera.
Video Port	The physical encoder video port where the camera video cable is attached. **Tip** Only the unused ports are displayed.
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 *Installed* and *Pointed* 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. • 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 10-42. • 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 12-1 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 (Required) Add additional camera licenses for non-Cisco cameras, if necessary. See the "Installing Licenses" section on page 1-26.

Step 3 (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 12-1.

Step 4 Click **Cameras**.

Step 5 Click **Add**.

Tip You can also click the **Add** icon and choose **Add a camera manually**.

Step 6 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 16-1 for more information.

Tip To use the auto-discovery option, see the "Camera Status" section on page 10-62.

Step 7 Enter the basic camera settings.

- Network (IP) Camera Rules and Settings, page 10-12
- Analog Camera Rules and Settings, page 10-13

Step 8 Click **Add**.

Step 9 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 10 Wait for the *Job* to complete.

See the "Understanding Jobs and Job Status" section on page 19-29.

Step 11 (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 12 (Optional) Enter additional configurations, if necessary.

See the "Editing the Camera Settings" section on page 10-42.

Step 13 (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 14 Repeat Step 5 through Step 12 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 10-4). This same method can be used to update existing camera configurations.

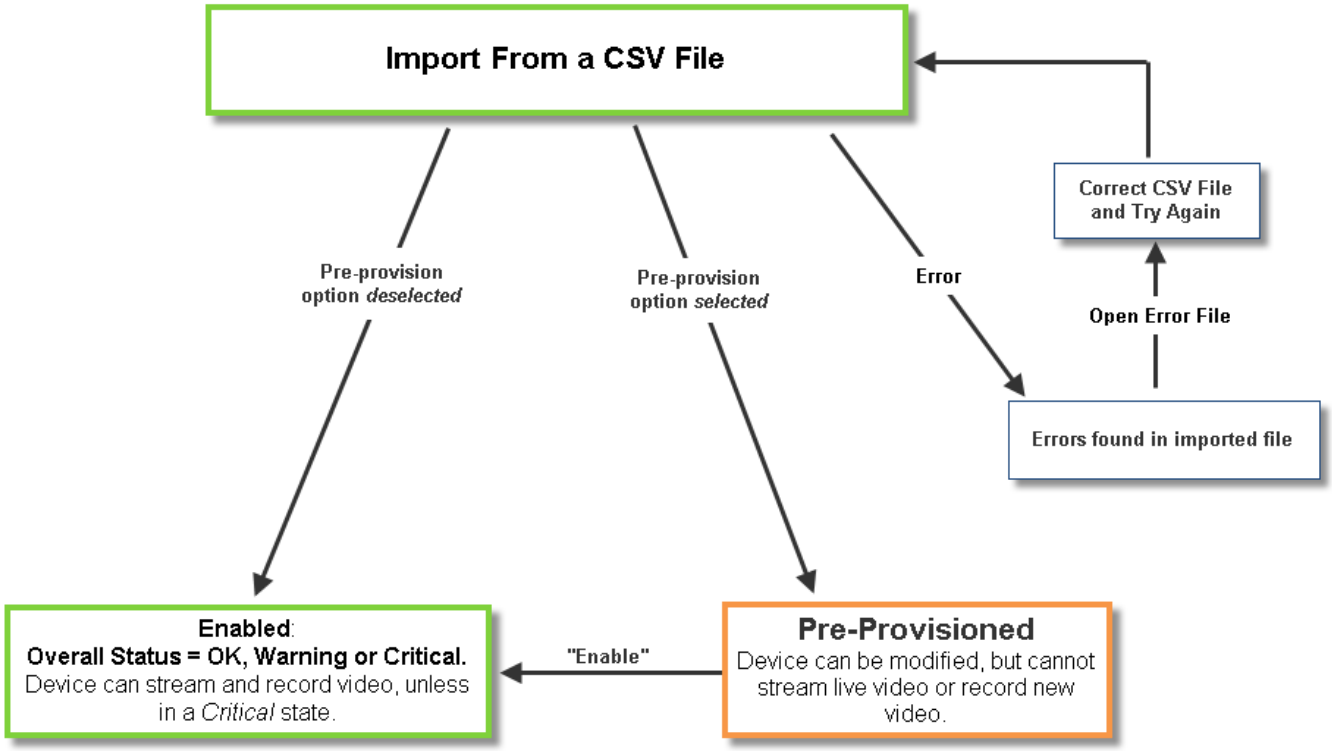
Refer to the following topics for more information:

- Overview, page 10-17
- Usage Notes, page 10-18
- Creating the CSV File, page 10-18
- Importing the CSV File, page 10-20

Overview

Figure 10-4 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 10-4 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 10-10 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 10-5 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 10-5). 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 10-20. 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 10-5 Example of a Camera Import File

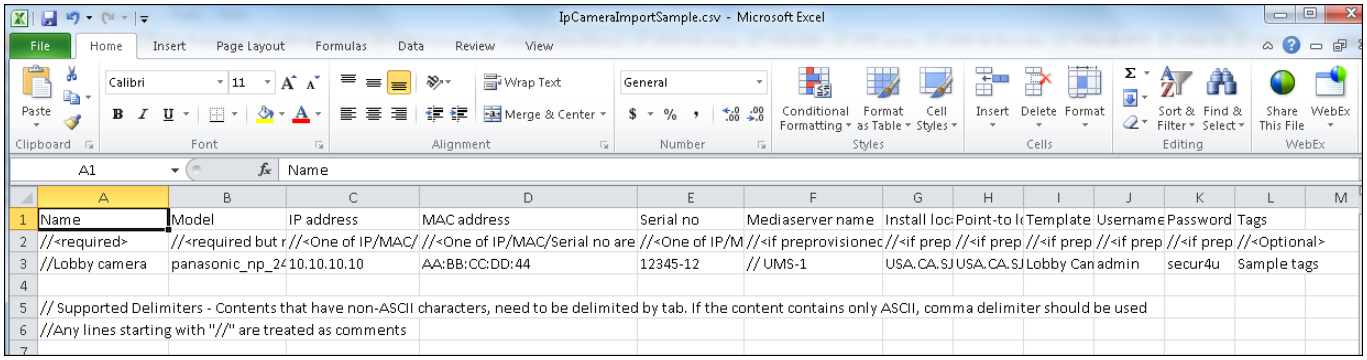


Table 10-5 describes the CSV file fields for both IP and analog cameras (the fields vary for each cameras type).

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 10-5 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 MAC address Serial no	IP cameras Required (see description)	At least one value is required (IP address, MAC or serial number). • New Cameras—The IP address, serial number, and MAC address must be unique for new cameras. See the "Managing Cameras with Duplicate IP Addresses" section on page 10-22 for more information. • Existing cameras—If all three entries are provided for an existing camera, the settings must match the devices existing settings.
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 9-9.
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 10-5 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 *pointed at* 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 12-1.
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. • 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 10-60 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 10-25.

Step 2 Create the camera CSV file containing details for each device.

- See the "Creating the CSV File" section on page 10-18.

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:

a. *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 10-5 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 10-18. 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.

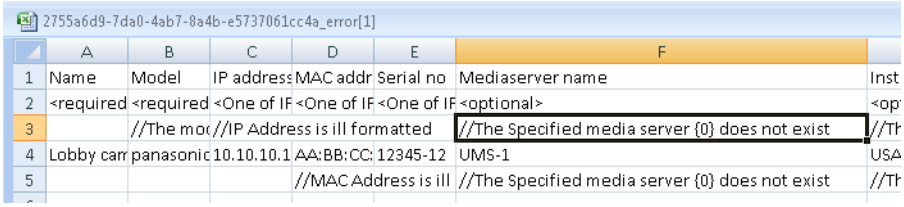
e. *Import Step 5 - Results*:

- 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 10-6), 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 10-6).
- Return to Step 4 and re-import the corrected CSV file.

Figure 10-6 Camera Import Error File



2755a6d9-7da0-4ab7-8a4b-e5737061cc4a_error[1]

	A	B	C	D	E	F	
1	Name	Model	IP address	MAC addr	Serial no	Mediaserver name	Inst
2	<required	<required	<One of IF	<One of IF	<One of IF	<optional>	<op
3		//The mo	//IP Address is ill formatted			//The Specified media server {0} does not exist	//Th
4	Lobby car	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	//Th

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 19-9.

Managing Cameras with Duplicate IP Addresses

By default, cameras must have a unique IP address, or an *ID collision* issue will occur. This prevents two devices with the same address from causing device and configuration errors.

If your network configuration requires devices with duplicate IP addresses, however, you can enable the **Allow Duplicate IP** system setting to allow multiple cameras with the same network address to be added to the Operations Manager configuration. This may be necessary when the same set of private IP addresses are used at multiple sites.

Refer to Understanding Device Conflicts, page 7-5 for more information.

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 10-23
- Understanding Camera Conflicts, page 10-25
- Enabling the Auto Configuration Defaults for a Camera Model, page 10-25
- Discovering Non-Medianet Cameras on the Network, page 10-28
- Cameras Pending Approval List, page 10-30
- Discovering Medianet-Enabled Cameras, page 10-32
  - Medianet Requirements, page 10-32
  - Medianet Overview, page 10-33
  - Medianet Camera Discovery Procedure, page 10-36

Related Documentation

- Understanding Camera IP Address Conflicts, page 7-12

Understanding Discovery and Auto-Configuration

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

Table 10-6 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 *admin* user.	"Discovering Medianet-Enabled Cameras" section on page 10-32
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. **Tip** Enable "Bonjour" on the cameras using the camera UI. For example, Cisco 3xxx,6xxx, and 7xxx cameras. See the camera documentation for more information.	• Discovering Cameras on the Network, page 10-23 • 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 10-7), 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 10-30 for more information.

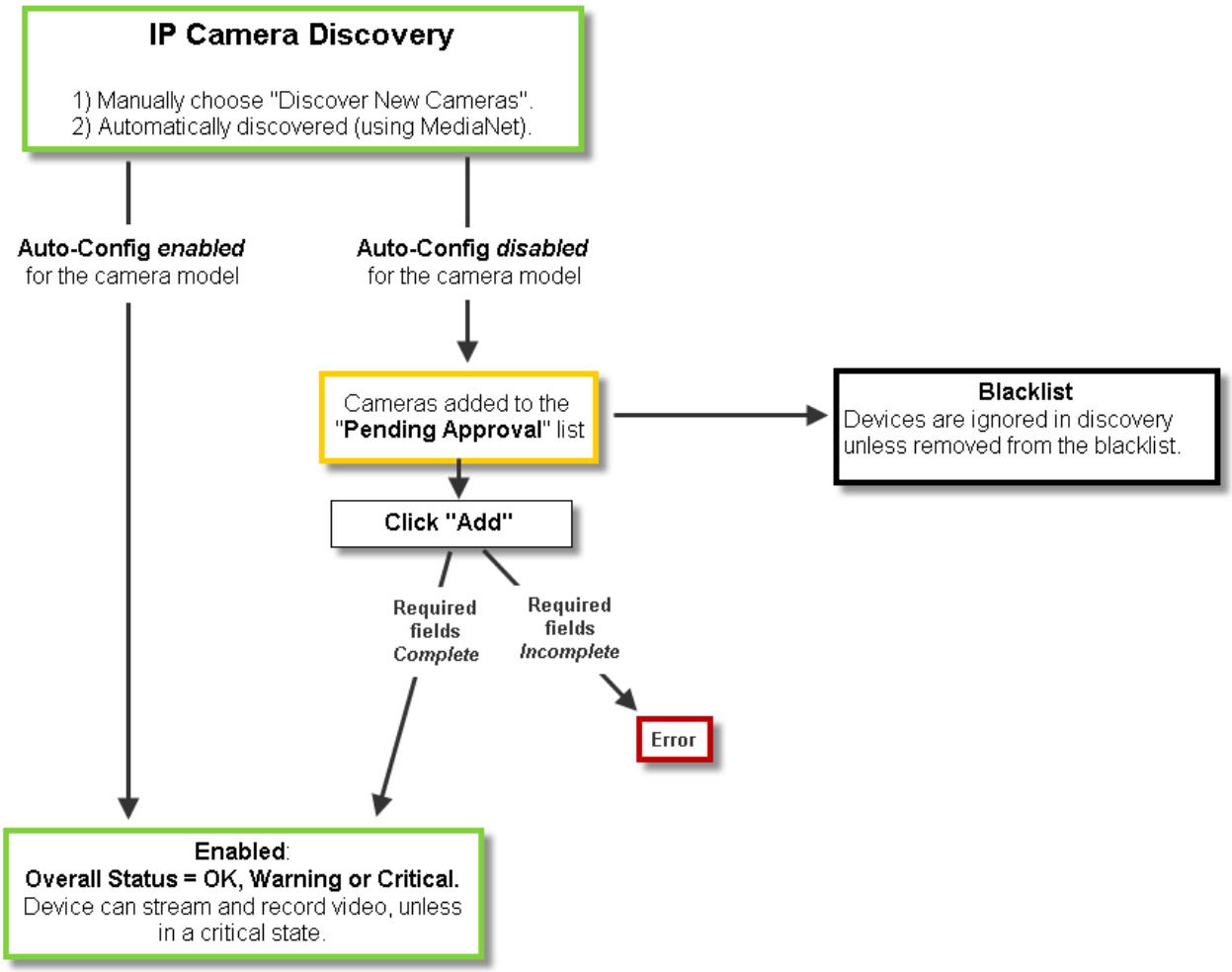
Auto-Configuration Default Configuration

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 10-7). **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 10-25 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 10-25.

Figure 10-7 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 10-7).

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.

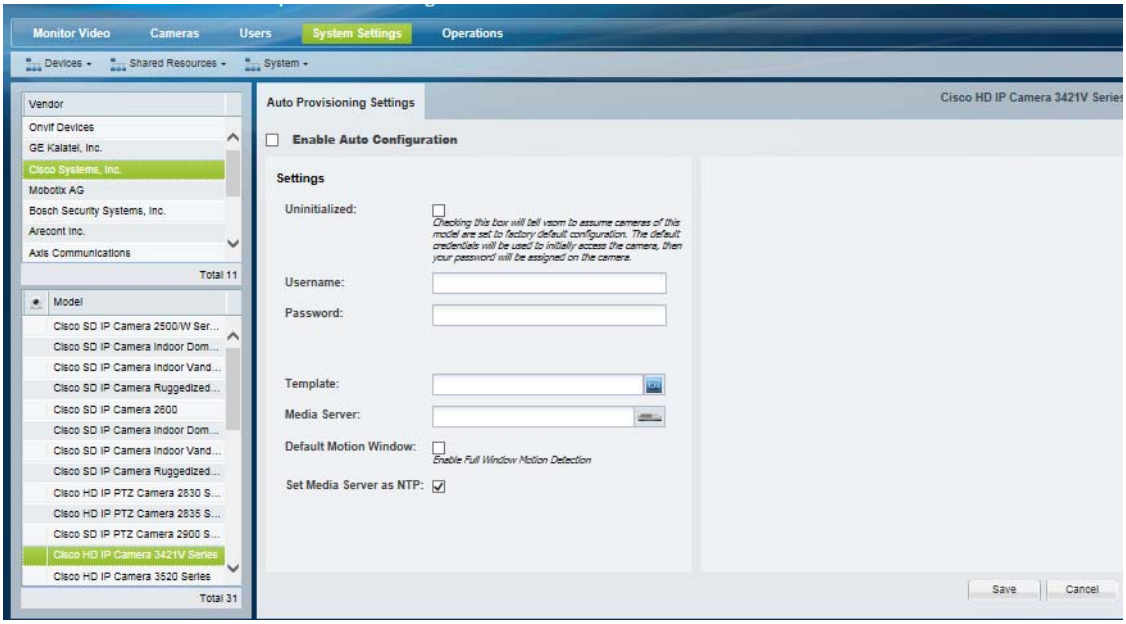
See "Understanding Device Conflicts" section on page 7-5 for more information.

Enabling the Auto Configuration Defaults for a Camera Model

Enable the auto-configuration default settings to automatically apply a set of basic configurations 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.

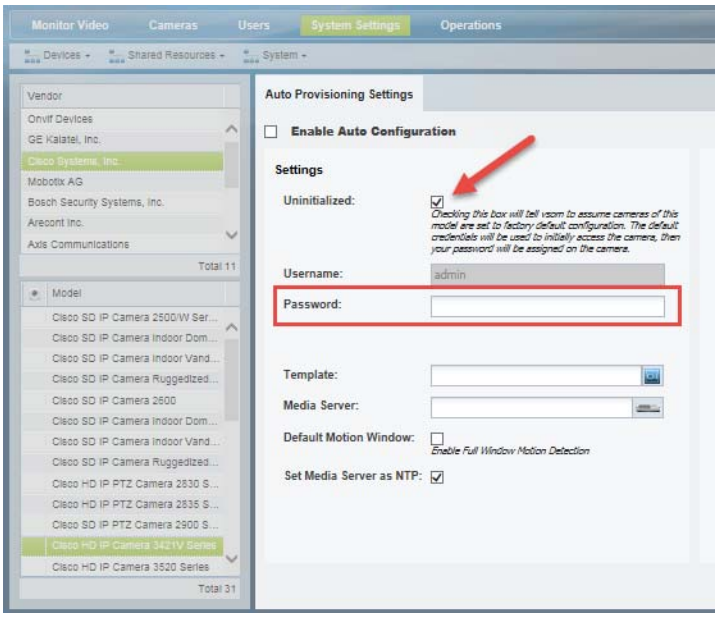
Figure 10-8 Device Auto Configuration



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 10-30 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 10-9 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 10-8).

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	(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. **Note** The change will not be implemented if the current username and password has been changed from the factory default.
Username	Enter the username used to access the camera over the network.

Setting	Description
Password	Enter the 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. • See the "Changing the Camera or Encoder Access Settings (Address and Credentials)" section on page 10-60 to revise the credentials after the camera is added to the system.
Template	Select the camera template that will provide the camera configuration. See the "Adding and Editing Camera Templates" section on page 12-1 for more information.
Media Server	(Optional) Select the Media Server that will manage the camera (the camera will be assigned to this Media Server). See the "Configuring Media Server Services" section on page 9-1 for more information.
Default Motion Window	(Optional) Enable motion configuration features for the entire camera view. This option is enabled only if the camera supports motion detection. See the "Configuring Motion Detection" section on page 10-82 for more information.
Set Media Server as NTP	(Optional) This option is enabled (selected) by default. The Media Server assigned to the camera is used as the network time protocol (NTP) server. If you de-select this option, the camera is not configured with an NTP server address. The camera retains any NTP address(es) previously configured on the device. If an NTP server is not configured on the device, you must update the camera settings to either enter an NTP server address or select **Use Media Server as NTP**. • This setting is displayed only for camera models that support NTP. • You must belong to a user group with *Cameras* permission. See the "Adding Users, User Groups, and Permissions" section on page 4-1 for more information. • See the "Configuring Cameras with a User-Defined NTP Server" section on page 8-8 for information to define a new NTP server for one or more cameras.

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. Enable Bonjour on the cameras using the camera UI (for example, Cisco 3xxx,6xxx, and 7xxx cameras). See the camera documentation for more information.

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 10-7 Manual Camera Discovery Steps

	Task	Description and more information
Step 1	Add additional camera licenses for non-Cisco cameras, if necessary.	A license is required for each non-Cisco camera added to your deployment. See the "Installing Licenses" section on page 1-26 for 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. • Understanding Discovery and Auto-Configuration, page 10-23 • Understanding Camera Conflicts, page 10-25 • Enabling the Auto Configuration Defaults for a Camera Model, page 10-25 • Cameras Pending Approval List, page 10-30
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. **a.** **Media Servers**—Select the Media Server used to discover the cameras. **b.** **Camera Make(s)**—Select the camera make(s) that will be discovered. For example, select **Cisco Systems, Inc.** to discover all Cisco-branded cameras. **c.** Click **Save**. See the Enabling the Auto Configuration Defaults for a Camera Model, page 10-25.
Step 4	Trigger the discovery process	**a.** Click **Cameras**. **b.** Choose **Add** > **Discover New Cameras**.
Step 5	Wait for the camera to be discovered and be added to the Operations Manager.	• 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 10-7 Manual Camera Discovery Steps (continued)

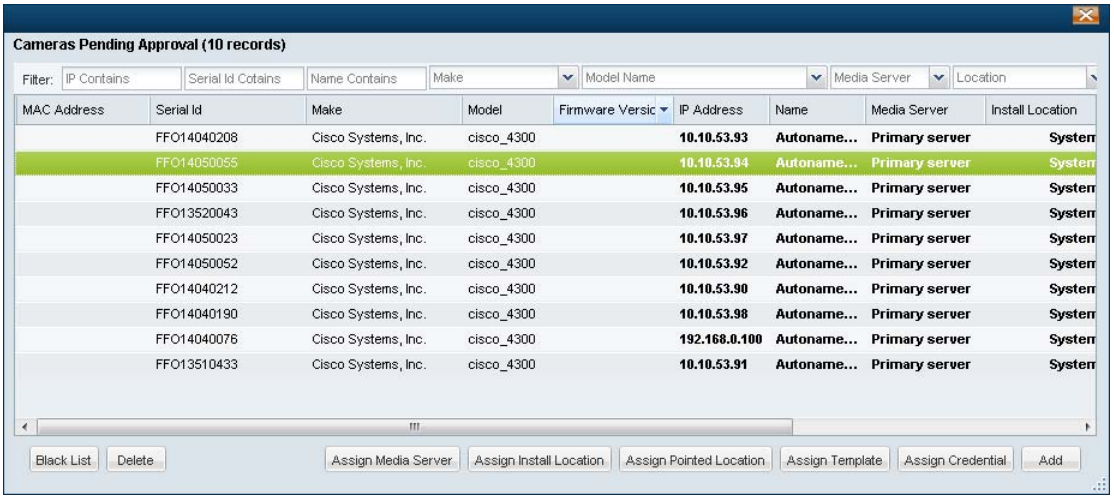
	Task	Description and more information
Step 6	Approve cameras that were added to the *Cameras Pending Approval* list.	If auto-configuration is not enabled for the camera model, the camera is added to the *Cameras Pending Approval* list, which allows you to apply additional configurations and approve (add) the camera. **a.** Open the *Cameras Pending Approval* list to modify the camera configuration. **b.** Approve the camera or move it to the blacklist. See the "Cameras Pending Approval List" section on page 10-30 for more information
Step 7	Complete the camera configuration.	If auto-configuration was enabled for the camera: **a.** Open the camera or camera template configuration page and modify the configuration, if necessary. **b.** Verify that the camera was added is in the *Enabled: OK* state. **c.** If the camera is in *Enabled: Warning*, *Critical* state, go to device Status page to get information, fix the problem and choose **Repair Configuration** from the **Device Settings** menu. See the "Editing the Camera Settings" section on page 10-42 for more information.
Step 8	Perform additional configuration, if necessary	• Editing the Camera Settings, page 10-42 • Configuring Camera PTZ Controls, Presets, and Tours, page 10-67 • Configuring Motion Detection, page 10-82

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 10-10). The cameras in this list 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 10-10 Cameras Pending Approval



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 10-23.

Step 3 Choose **Add > Cameras Pending Approval**.

Step 4 (Optional) Filter the list of discovered cameras (Figure 10-10).

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 12-1 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 10-42 to change a camera configuration.

Note Click **Blacklist** to blacklist the camera. See the "Blacklisting Cameras" section on page 10-40.

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 10-32
- Medianet Overview, page 10-33
- Configuring a DHCP Server with Option 125, page 10-34
- Medianet Camera Discovery Procedure, page 10-36
- High Availability Impact on Medianet Cameras, page 10-37

Medianet Requirements

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

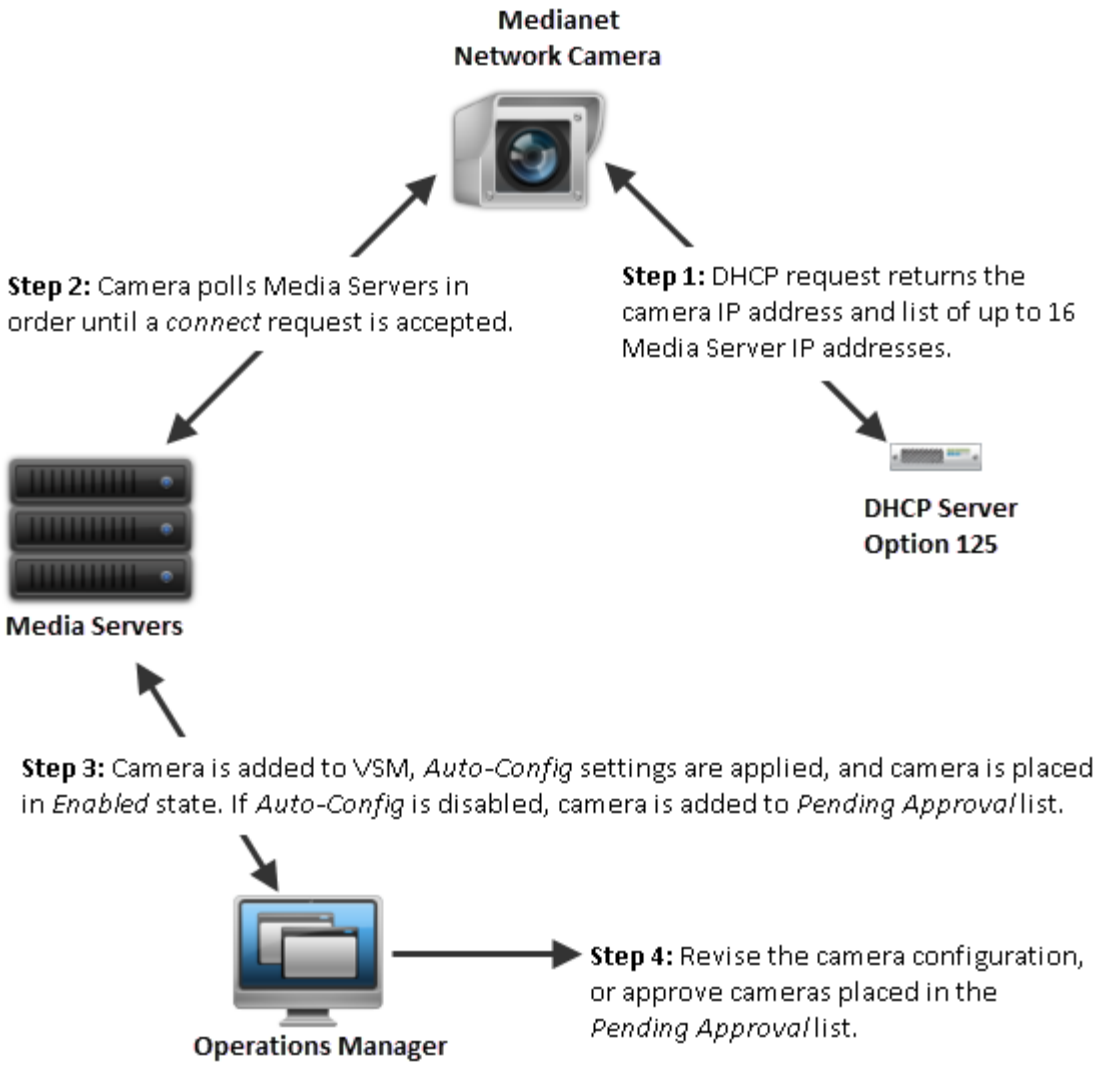
Table 10-8 Medianet Discovery Requirements

Requirements	Requirement Complete? (✓)
The network (IP) camera must support Cisco Medianet. • Medianet cameras must be configured for DHCP (cameras that do not support Medianet can only be added using a static IP address). • 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 7.6 for a summary of supported Cisco cameras and required firmware. See also the camera product information at http://www.cisco.com/go/physicalsecurity (click **View All Products**, and select the camera model under *Video Surveillance IP Cameras*).	❑
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 10-34 for instructions. **Related Information** • Cisco Medianet website (http://www.cisco.com/go/medianet) • Cisco Medianet FAQ • Medianet Reference Guide	❑
A functioning Cisco VSM 7.x system must be installed and configured on the network. See the following for more information: • Cisco Video Surveillance Management Console Administration Guide • "Summary Steps: Basic Configuration" section on page 1-8	❑

Medianet Overview

To enable Medianet discovery, you must install a Medianet-enabled IP camera on the network, as shown in Figure 10-11. A DHCP server must also be installed with Option 125 configured to provide a list of up to 16 Media Server IP addresses.

Figure 10-11 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 10-25.
- 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 10-30.

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 10-23
- Cameras Pending Approval List, page 10-30
- Editing the Camera Settings, page 10-42

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 10-40.

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 10-9 Summary Steps: Camera Discovery

	Task	Description and more information
Step 1	Verify that the Medianet Requirements are met.	Medianet Requirements, page 10-32 You must have: • 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 10-34 for instructions. **Note** Cameras that do not support Medianet can only be added using a static IP address.
Step 2	Review the overview sections to understand the discovery process.	Review the following topics to understand the discovery and auto-configuration process. • Understanding Discovery and Auto-Configuration, page 10-23 • Discovering Medianet-Enabled Cameras, page 10-32
Step 3	Install a Medianet network camera and use the camera configuration UI to enable DHCP and add an *admin* user (if necessary).	• 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 10-25
Step 5	Wait for the camera to be discovered and be added to the Operations Manager.	• 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 *Cameras Pending Approval* list.	If auto-configuration is not enabled for the camera model, the camera is added to the *Cameras Pending Approval* list, which allows you to apply additional configurations and approve (add) the camera. Open the *Cameras Pending Approval* 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 10-30 for more information

Table 10-9 Summary Steps: Camera Discovery (continued)

	Task	Description and more information
Step 7	Complete the camera configuration.	• Open the camera or camera template configuration page and modify the configuration, if necessary. • Verify that the camera was added is in the *Enabled: OK* state. • If the camera is in *Enabled: Warning*, *Critical*, or *pre-provisioned* state, complete or correct the configuration, verify that the camera is available on the network and choose **Enable** from the **Device Settings** menu. See the "Editing the Camera Settings" section on page 10-42 for more information.
Step 8	Perform additional configuration, if necessary	• Editing the Camera Settings, page 10-42 • Configuring Camera PTZ Controls, Presets, and Tours, page 10-67 • Configuring Motion Detection, page 10-82

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.

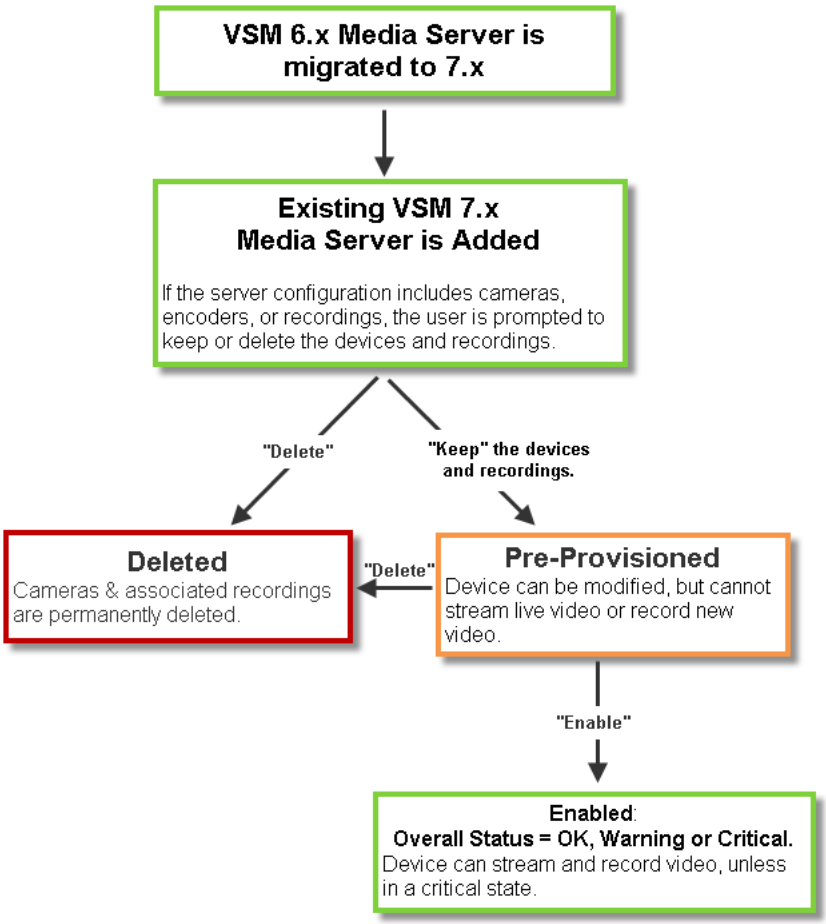
See the following for more information.

- Adding Cameras From a 6.x or 7.x Media Server, page 10-38
- Adding Unknown Cameras During a Media Server Synchronization, page 10-39

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 10-12). 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 10-12 Adding Cameras from a Cisco VSM 6.x Media Server



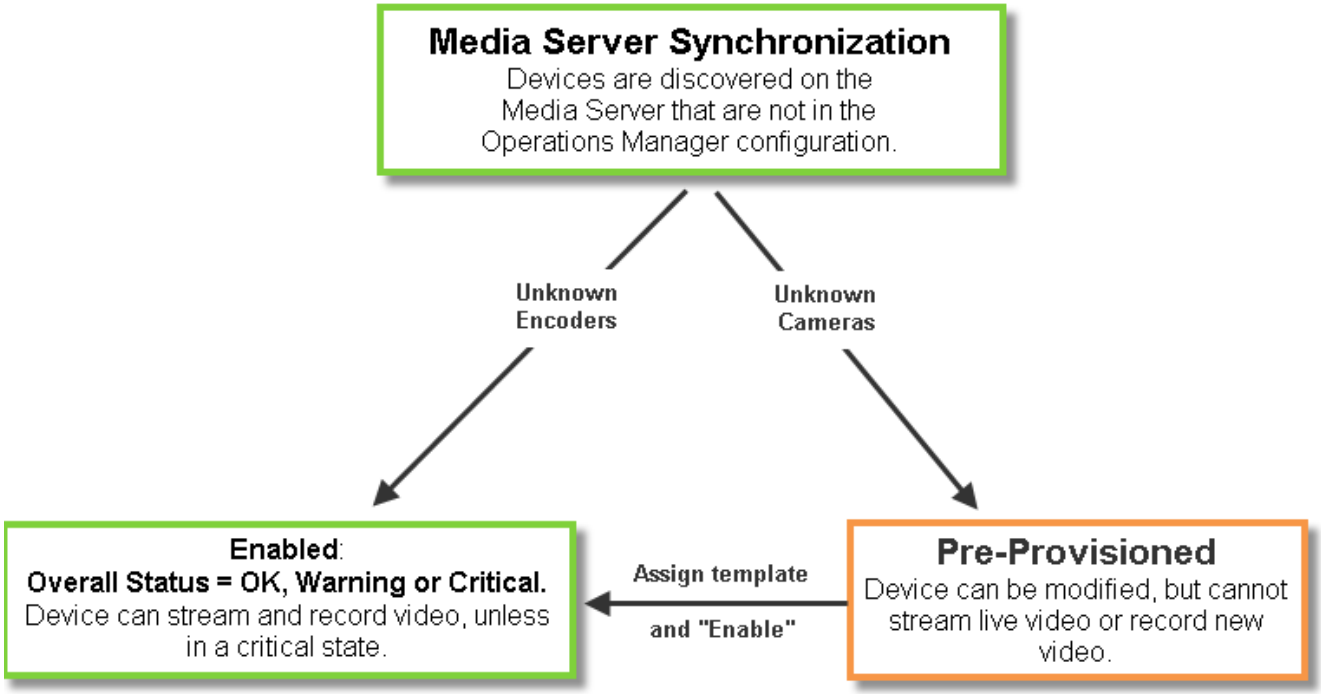
Tip To add a Cisco VSM 6.x Media Server, you must first migrate the server to Cisco VSM 7.x. See the *Cisco Video Surveillance Migration Guide, Release 6.3.2 to 7.0* for more information. This document is available on the Cisco Developer Network (CDN). See you Cisco support representative for more information.

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 10-13).

- 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 10-10 for more information.
- If a device is in *Enabled: Warning* or *Enabled: Critica*l state, view the device Status page to resolve any additional issues (see the "Camera Status" section on page 10-62).

Figure 10-13 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 you 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

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 10-23 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 10-11.

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 10-23.

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 10-17).

See each topic for detailed information.

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 is 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 12-5.
- 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.

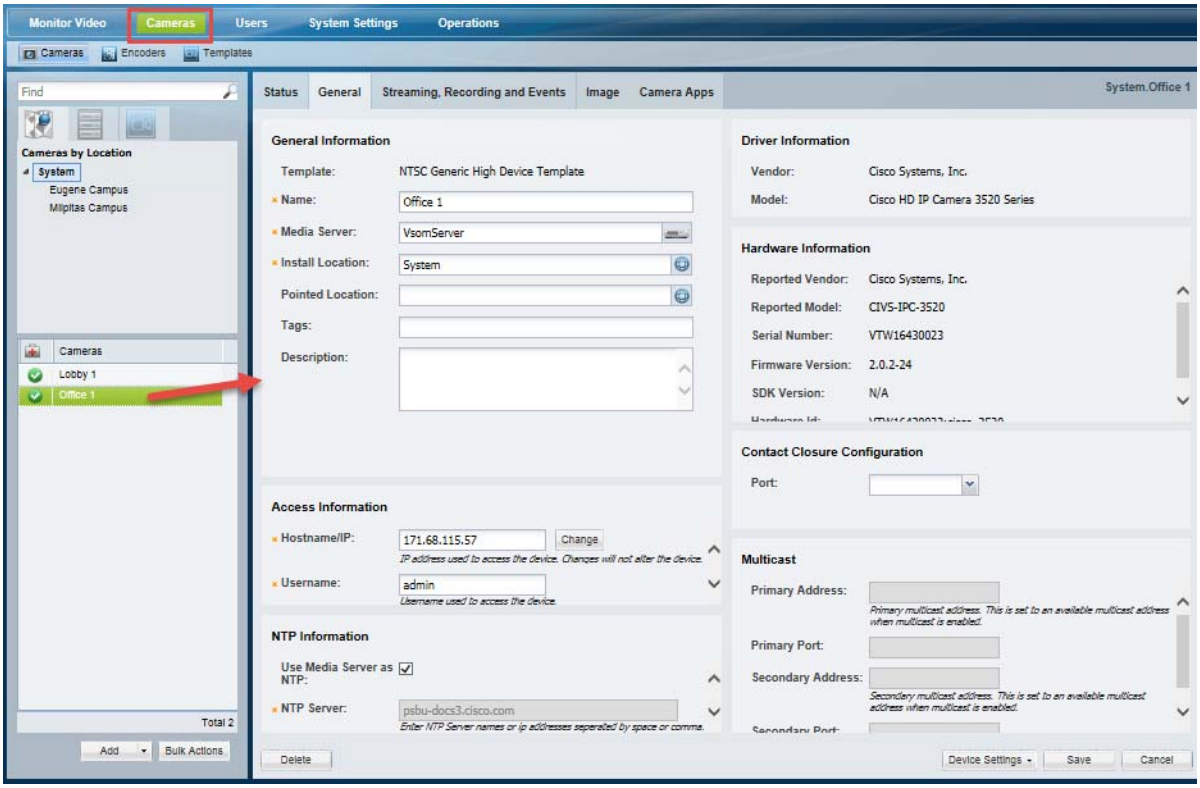
- See the "Logging In" section on page 1-18.
- You must belong to a User Group with permissions for *Cameras*.

Step 2 Click **Cameras**.

Step 3 Click the tabs in the top left column to view cameras and templates (see Figure 10-14):

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 10-14). 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 10-14 Camera General Settings



Step 4 Revise the available settings as described in the following topics.

- General Settings, page 10-44
- Streaming, Recording and Event Settings, page 10-48
- Image Settings, page 10-56
- Camera Apps, page 10-56
- Configuring the High Availability Options for a Camera or Template, page 10-57

Step 5 Click **Save**.

Step 6 (Optional) Revise the camera template, or create a custom template.

- Creating or Modifying a Template, page 12-3
- Creating a Custom Template for a Single Camera, page 12-5

General Settings

The General Settings define camera-specific attributes. These settings are specific to the camera and are not impacted by template settings.

Table 10-10 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 *Find* field.
Description	(Optional) The camera purpose, location or other description.
Access Information (IP Cameras and Encoders Only)	
Hostname/IP Address	(Required for all cameras and encoders) Enter the device hostname or IP address used by Operations Manager to access the device on the network. Entering an address in this field does not affect the settings stored on the device. (Supported devices only) Click **Change** to revise the network settings saved on the device *and* the IP address or hostname 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 address, Gateway, Subnet Mask, DNS Server, and Domain. See the device documentation for more information on the required settings. **Notes** • 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 Resolving ID Mismatch Errors When Changing Camera IP Addresses, page 7-7 for more information. • See the "Changing the Camera or Encoder Access Settings (Address and Credentials)" section on page 10-60 for more information.

Table 10-10 Camera General Settings (continued)

Setting	Description
Username and Password	(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. (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. **Notes** • 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 10-60 for more information.
NTP Information	
Note This option is only available for device models that support NTP. **Tip** See the Understanding NTP Configuration, page 8-1 for more information.	
Use Media Server as NTP	(Optional) Specifies in the Media Server assigned to the device is used as the network time (NTP) to provide the devise date and time settings.
NTP Server	(Required) The NTP server hostname or IP address for the camera. This field is read-only if **Use Media Server as NTP** is enabled.
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 16-1 for more information.	
Enable	(Analog cameras only) Enables the PTZ controls on an analog camera. **Note** The camera and encoder must support PTZ movements and controls. See the device documentation for more information.
Encoder	(Analog cameras only) The encoder for the analog camera.
Serial Port	(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.
Serial Port Address	(Analog cameras only) 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.
Driver Information	
Vendor	(Read-only) The firmware provider.
Model	(Read-only) The device model.

Table 10-10 Camera General Settings (continued)

Setting	Description
Hardware Information	
Reported Vendor	(Read-only) The camera manufacturer.
Reported Model	(Read-only) The camera model number.
Serial Number	(Read-only) The camera serial number.
Encoder	(Analog cameras only) The encoder name.
Encoder Port	(Analog cameras only) The encoder port used by the analog camera.
Firmware Version	(Read-only, IP cameras only) The firmware version installed on the device. Device *firmware* is provided by the device manufacturer. • To upgrade the firmware for Cisco cameras, and supported encoders, see the "Upgrading Cisco Camera and Encoder Firmware" section on page 26-19. • 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	Select the contact closure port used to trigger an action. • 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 13-7 for instructions to define the action that occurs when the contact closure is triggered. **Analog Camera Support Notes** • 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 16-5
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 12-11 for more information.

Table 10-10 Camera General Settings (continued)

Setting	Description
Primary Address	(Optional) Enter the multicast IP address where the camera's primary video stream (Stream A) should be sent. This field is enabled only if the camera's template Stream A is configured for multicast. Addresses must be in the proper address range. • 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 **Note** Public addresses must be individually assigned by IANA (Internet Assigned Numbers Authority)
Primary Port	Enter the port value used by Cisco Video Surveillance to listen to the camera's primary video stream.
Secondary Address	(Optional) Enter the multicast IP address where the camera's secondary video stream (Stream B) should be sent. This field is enabled only if the camera's template Stream B is configured for multicast. Addresses must be in the proper address range. • 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 **Note** Public addresses must be individually assigned by IANA (Internet Assigned Numbers Authority)
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 19-21 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 10-11) 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 Templat**e and choose **Custom**).

Table 10-11 Streaming, Recording and Event Settings

Setting	Description
Template	(Cameras only) Click **Set Template** to select the template used for the camera: 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 12-1 for more information. 2. Click **Custom** to enter custom settings for the camera. **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. 3. Click **OK** to continue. **Tip** The remaining *Streaming, Recording and Event* settings can be changed for a specific camera only if the **Custom** option is selected.
Video Format	(Templates only) Select one of the following: • **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. **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.

Table 10-11 Streaming, Recording and Event Settings (continued)

Setting	Description
Recording Schedule	(Templates only) Select one of the following: • **Basic Recording: 24x7**—Records 24 hours a day, every day, based on the *continuous* and *event* recording properties. or • Select a previously-defined schedule. Recording schedules appear only if schedules are configured. See the "Configuring Continuous, Scheduled, and Motion Recordings" section on page 12-7 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.
Video Quality	(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. • Select **Off** to disable video recording and playback. • Choosing **Hi** on *Stream A* may disable *Stream B* if Stream A requires a high level of processing and network resources. To enable *Stream B*, lower the quality level of *Stream A*. • 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 10-54 for more information. **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. **Tip** See the "Configuring Multicast Video Streaming" section on page 12-11 for more information.

Table 10-11 Streaming, Recording and Event Settings (continued)

Setting	Description
Recording Options	(Templates only) Click the recording option for each recurring schedule. **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 12-7 for more information. • —Select **No Recording** to disable recording for the stream. • —Select **Record on Motion** to record motion events. – In *Retain event recordings*, enter the amount of time a motion event should be retained (saved) on the system. Changes to this setting apply to new recordings only (the retention time cannot be changed for existing recordings). Recordings are deleted when the expired time is reached, or if the Storage% is reached (the oldest files are deleted first, regardless of their expiry time). – In *Padding*, 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 10-82 for instructions to define the areas of the image that trigger motion events. • —Select **Continuous Recording** to record video in a loop. – 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 *Retain continuous recordings* 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. Changes to this setting apply to new recordings only (the retention time cannot be changed for existing recordings). • —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	(Templates only) • *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 *Retain continuous recordings* field. – This value must be a number greater than 0 (days). – The default is 1 day. – The maximum value is 3650 days (10 years). **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 "Viewing Media Server Status" section on page 9-9 for more information.

Table 10-11 Streaming, Recording and Event Settings (continued)

Setting	Description
Retain event recordings	(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. **Note** This setting also applied to Record Now recordings. • Enter the number of days the video should be retained. – Enter a number between 1 and 3650 days (10 years). – The default is 30 days. or • 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 *Storage (%)* for the Media Server. For example, if the *Storage (%)* is set to 90%, and a camera template *Retain event recordings* 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). **File Deletion** Recordings are deleted when the expired time is reached, or if the Storage% is reached (the oldest files are deleted first, regardless of their expiry time). Video archive files are deleted until the free disk space is less than the *Storage (%)*. See the Media Server "Viewing Media Server Status" section on page 9-9 for more information. **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 "Viewing Media Server Status" section on page 9-9 for more information.
Alert Notifications	(Templates only) —Click **Alert Notifications** to enable or disable the alerts that are generated when a motion stop or start event occurs. **Tip** Use Advanced Events to generate alerts only when a motion stop or motion start event occurs. See the "Using Advanced Events to Trigger Actions" section on page 13-7 for more information.
Advanced Events	(Templates only) Use *Advanced Events* to trigger actions when an event occurs. • *Instantaneous Trigger Events*—Events that trigger an immediate action (for example, when motion is detected). • *States of Being*—Events that trigger an ongoing action as long as that event occurs (for example, while a contact remains open). See the "Using Advanced Events to Trigger Actions" section on page 13-7.

Table 10-11 Streaming, Recording and Event Settings (continued)

Setting	Description
Advanced Storage	(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. See the "Configuring the Camera Template HA Options" section on page 17-12, which includes the following instructions: • **High Availability and Failover**—Configuring the Redundant and Failover Options, page 17-12. • **Long Term Storage**—Archiving Recordings to a Long Term Storage Server, page 17-16. • **Recording Options**— Defining the Recording Options, page 17-20
Record Audio	(Templates only) Defines if audio should be recorded when video is being recorded. **Note** The audio settings is disabled if audio is not supported by the camera. • **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	(Templates only) Defines the number of seconds should be included in a motion event. • **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 10-11 Streaming, Recording and Event Settings (continued)

Setting	Description
Verify Recording Space	(Templates only) **Enable** 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 9-8). If the required amount of storage space is not available for the entire recording, then the recording will not start. 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. **Note** The verification takes into account the storage demands required by other cameras assigned to the Media Server. **Note** Enabling the *Default Grooming Only* 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 "Viewing Media Server Status" section on page 9-9 for more information. **Disable** 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. 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. 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: • 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	(Templates Only) Enables or disables the Record Now feature on the cameras assigned to the template. **Note** Recordings are retained according to the *Retain event recordings* setting. See the following for more information: • Enabling Record Now, page 3-11 • Using Record Now, page 2-26

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 10-12.

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 12-11.

Custom Video Quality Settings

Table 10-12 Custom Video Quality Settings

Setting	Description
Codec	Select the video encoding format, such as JPEG, MPEG4 or H.264. **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.
Transport	Select an option to stream video using either TCP or UDP. **Note** We recommend UDP for most networks where packet loss and high latency are not an issue. **Tip** Also see the "Configuring Multicast Video Streaming" section on page 12-11.
Bit rate mode	Select **CBR** (Constant Bit Rate) or **VBR** (Variable Bit Rate). • 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. – 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 10-12 Custom Video Quality Settings (continued)

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. • A high *Quality* 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 *Quality* 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 12-3).

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 10-12 and click **Set**.

Step 5 Complete the template configuration as described in the "Streaming, Recording and Event Settings" section on page 10-48 and the "Creating or Modifying a Template" section on page 12-3.

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 10-82.

Pan Tilt and Zoom (PTZ) Settings

See the "Configuring Camera PTZ Controls, Presets, and Tours" section on page 10-67.

Photographic Controls

Click the **Image** tab to access the **Photographic Controls** (Table 10-13) 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 10-44 for instructions to configure the analog camera serial port. See the "Adding External Encoders and Analog Cameras" section on page 16-5 for more information.

Table 10-13 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 *edge contrast* (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.

Camera Apps

See Managing Camera Apps, page 14-1.

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: Cisco Media Servers" section on page 17-1.

	Task	Related Documentation
Step 1	Install and configure the HA servers.	• Understanding Redundant, Failover, and Long Term Storage Servers, page 17-4 • Define the Media Server HA Role and Associated Servers, page 17-9
Step 2	Configure the Primary server to use the HA servers.	• Define the Media Server HA Role and Associated Servers, page 17-9
Step 3	Configure the HA Advanced Storage options on the camera template.	• Configuring the Camera Template HA Options, page 17-12

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 10-92for 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 10-14 Delete Options

Delete Option	Description
Blacklist & Full Delete	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. See the following for more information: • Blacklisting Cameras, page 10-40 • Discovering Cameras on the Network, page 10-23
Retain Recordings	The camera configuration is removed from Cisco VSM, but the camera recordings can still be accessed in the Monitor Video page. • 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 12-7. • The camera is still included in the camera license count. See the "Installing Licenses" section on page 1-26.
Full Delete	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. See the following for more information: • Manually Adding a Single Camera, page 10-11 • Discovering Cameras on the Network, page 10-23.
Cancel	Cancel the operation.

Changing the Camera or Encoder Access Settings (Address and Credentials)

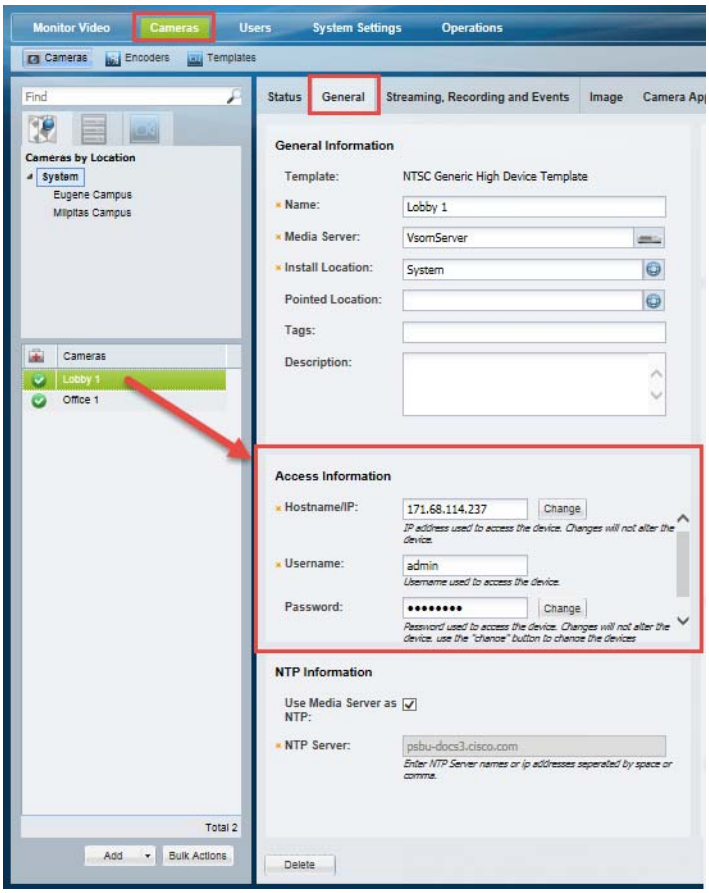
The camera or encoder IP address, username, and password settings stored in Cisco VSM Operations Manager are used to access the device over the network. These settings are entered into the Operations Manager when the device is first added to the system (see the "Manually Adding Cameras" section on page 10-8 and the "Adding External Encoders and Analog Cameras" section on page 16-5).

Change Options

You can use Operations Manager to change these settings in the following ways (see Figure 10-15):

- 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 10-15 Camera Access Settings



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 10-42.

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.

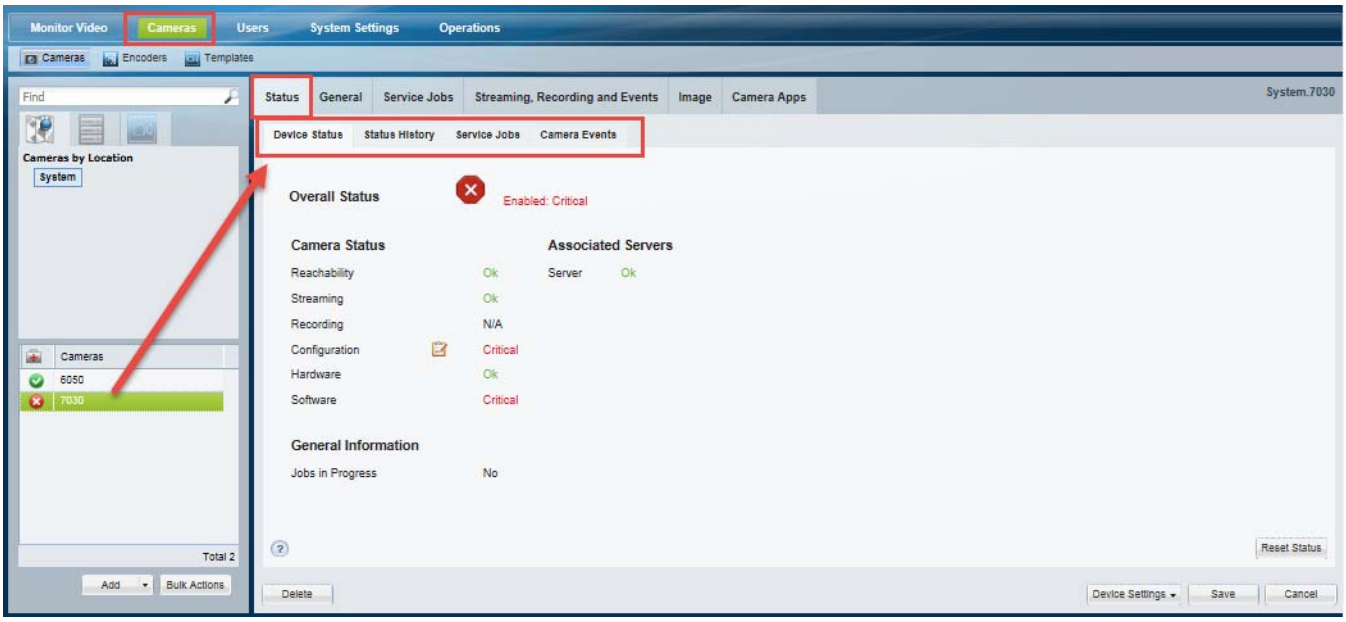
Step 4 (Optional) Verify the new settings:

- 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.

Camera Status

Select the camera or encoder **Status** tab (Figure 10-16) to display information about camera device health, service jobs, and security events.

Figure 10-16 Camera Device Status



Procedure

Step 1 Select **Cameras**.

Step 2 Select a location and select a camera from the list.

Step 3 Select the **Status** tab.

Step 4 Select one of the following tabs:

- Device Status, page 10-63
- Status History, page 10-64
- Service Jobs (Cameras), page 10-65
- Camera Events, page 10-66

Device Status

Displays a snapshot of the current device health status, and the device attribute that is experiencing the error. The camera's device health impacts the camera's ability to communicate with a Media Server, stream video over the network, or record video.

For example, in Figure 10-16, the camera is in the *Enabled: Critical* state, meaning that it cannot display or record video. This state is due to a *Critical* configuration error.

See Camera States, page 10-63 for more information.

Tip Click **Refresh Status** to reload the current device status.

Camera States

When a camera is added to Cisco VSM, it is placed in either *Enabled* or *Pre-provisioned* state.

- *Enabled* means that the user intends the camera is to be functional. There are three possible sub-levels: OK, Warning, and Critical.
- *Pre-provisioned* means that the device is added to the configuration but not available on the network.

See Table 10-15 for additional descriptions.

Table 10-15 Camera Status

State	Description
Enabled: OK	The device is operating normally and has no errors.
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. **IP Camera**—The IP camera is enabled but is in a state unable to perform its full capacity. **Analog Camera**—The analog camera is enabled but is in a state unable to perform its full capacity. **Tip** An IP camera and an analog camera that are in *Enabled: Critical* state after they are enabled from a *Pre-provisioned* state usually indicate a mis-match configuration. This is often caused by a missing motion detection configuration on the camera when the camera template requires one. See the "Synchronizing Device Configurations" section on page 19-21 for information on viewing and resolving configuration mismatches.

Table 10-15 Camera Status (continued)

State	Description
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 camera can be modified, but the camera cannot stream or record video until the configuration is complete and you choose **Enable** from the **Device Settings** menu • **IP Camera**—A *Pre-provisioned* IP camera 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. • **Encoder**—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. **Note** 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. • **Analog Camera**—An analog camera in this state is associated to an encoder that is either in a state of Pre-provisioned or Enabled. 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.

For more information see the "Device Status: Identifying Issues for a Specific Device" section on page 19-9.

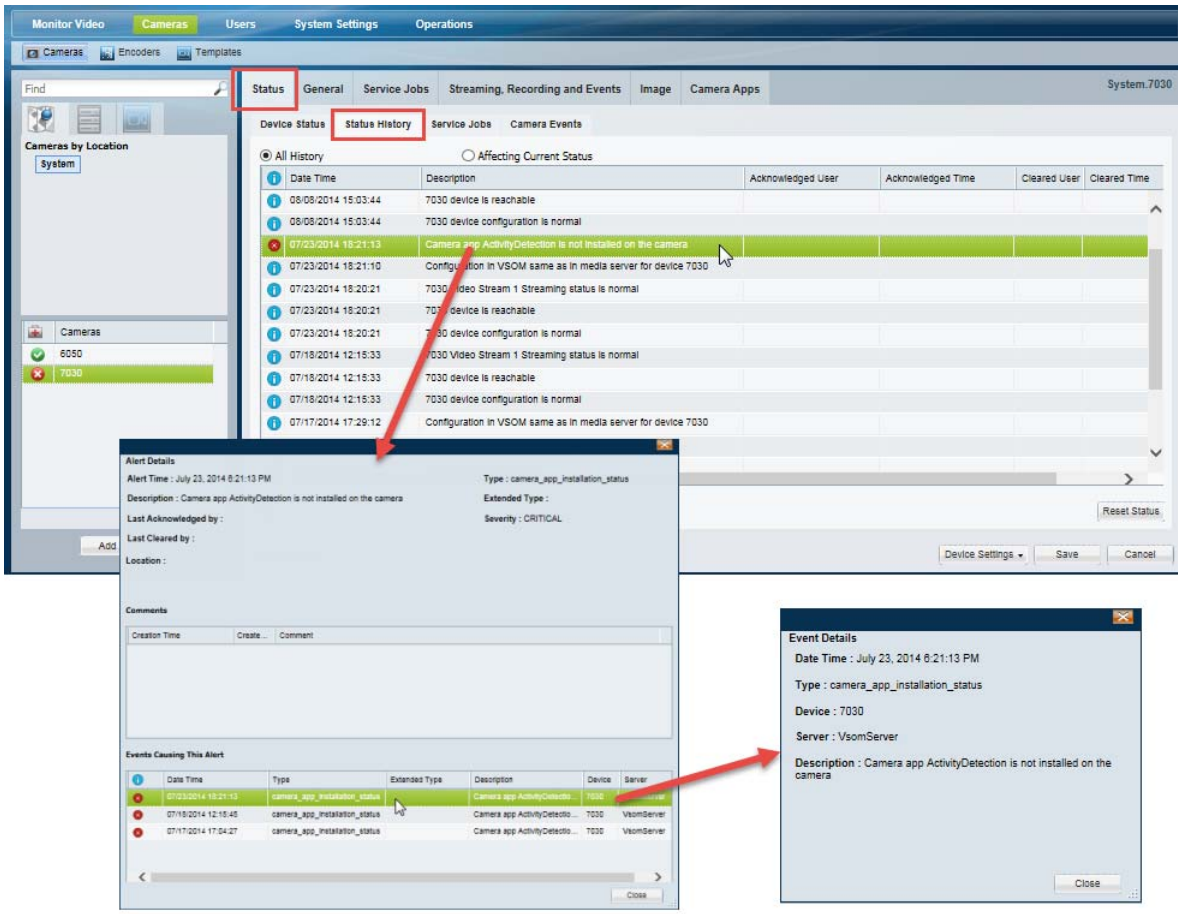
Status History

Click the **Status History** tab for additional details (Figure 10-17). The history page displays the specific health events that impact the device status.

- (Optional) Click **Affecting Current Status** to display only the alerts causing the current problem.
- (Optional) Double-click an entry to display the alert details (Figure 10-17). Alerts can include multiple events for the same issue. See Understanding Events and Alerts, page 19-2.
- (Optional) Double-click an event to display the event details. Alerts can include multiple events for the same issue.

For example, in Figure 10-17, the camera is assigned to a template where a camera app is enabled, but the app is not installed on the camera, an error will occur. To resolve the issue, install the appropriate camera app on the camera. (see the "Managing Camera Apps" section on page 14-1). Once saved, the device status should be *OK* (click **Refresh Status** if necessary).

Figure 10-17 Camera Status History



Service Jobs (Cameras)

Use the Service Jobs tab (Figure 10-18) to view information about the jobs processed on the camera. Service Jobs reflect the tasks being processed by the Media Server that manages the camera.

For example, job types can include:

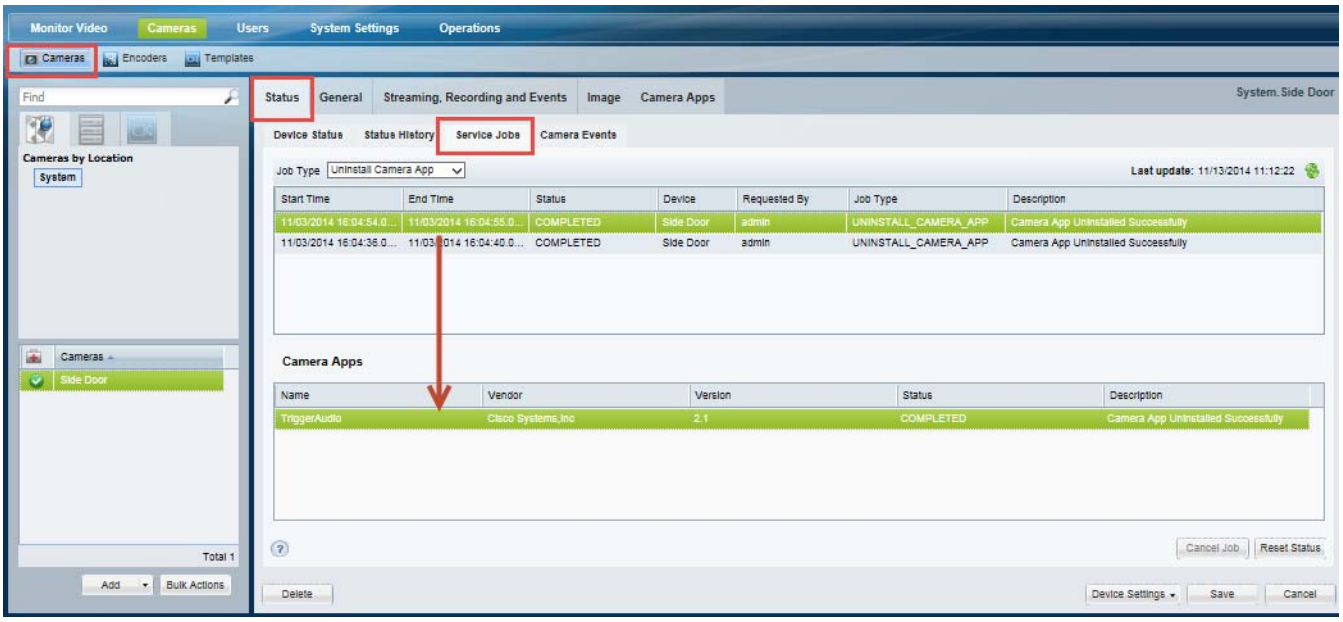
- Camera Storage
- Generate Metadata
- Camera Apps—The camera apps that were installed, uninstalled, activated or deactivated.
- Format Camera SD Cards

Click an entry to view additional details about the job. The details also include the status and results of the job.

To cancel a service job that is in progress ("Created", or "Running" state), select the job and click **Cancel Job**. Not all job types can be canceled. For example, you can cancel metadata and Camera Storage service jobs that are still in progress.

See the "Viewing the Camera App Jobs for a Specific Camera" section on page 14-20 for more information.

Figure 10-18 Camera Service Jobs



Tip To view the service jobs for all cameras and encoders managed by a Media Server, select the Service Jobs tab in the Media Server configuration page. Not all Service Jobs are supported from the Media Server page (such as camera apps). See the "Viewing Media Server Status" section on page 9-9.

Camera Events

Displays the security events that occurred on the camera for a period of time. For example, all motion start events or camera app events over the past 12 hours.

See the "Trigger and Action Descriptions" section on page 13-9 for more information on the events that can occur on a camera.

Repairing Camera Configuration Errors

If a camera configuration error occurs, use the Status History to locate and correct the problem. Other issues are the result of mismatched configuration between the device, the Media Server and/or the Operations Manager. If this occurs, use the configuration repair options described in the "Repairing a Mismatched Configuration" section on page 19-25.

For example, be sure to successfully save or revert your changes while still in the motion configuration window. Clicking out of the window before changes are successfully saved or discarded can cause a configuration mismatch to occur on the camera Status page (the error will not include any additional details). If this occurs, perform a **Repair Configuration** on the camera (see the "Repairing a Mismatched Configuration" section on page 19-25).

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.
- Define user groups that have priority for accessing PTZ controls.

Refer to the following topics for more information:

- PTZ Requirements, page 10-68
- PTZ Camera Configuration Summary, page 10-69
- Defining the User Group PTZ Priority, page 10-71
- Using Camera PTZ Controls, page 10-72
- Configuring PTZ Presets, page 10-73
- Configuring PTZ Tours, page 10-75
- Configuring Advanced Settings, page 10-77

Related information:

- Using Pan, Tilt, and Zoom (PTZ) Controls, page 2-38
- Calibrating a Joystick for Windows 7, page 2-41
- Using Advanced Events to Trigger Actions, page 13-7

Tip See the Example in the "Defining the User Group PTZ Priority" section on page 10-71 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 10-16 Camera PTZ Requirements

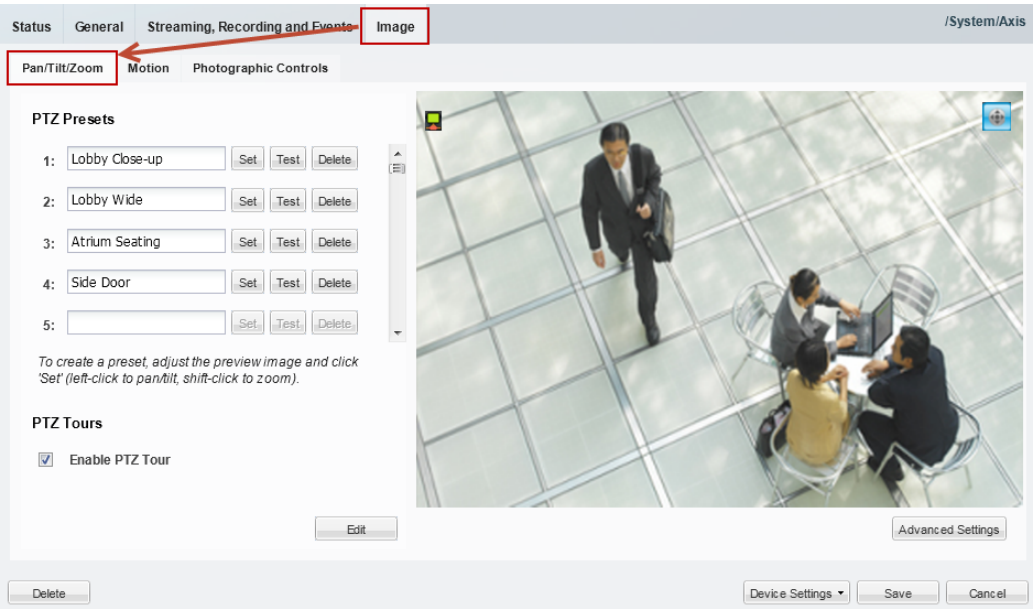
Requirements	Requirement Complete? (✓)
Cameras must support PTZ functionality.	❑
PTZ functionality must be enabled on the camera. See the camera documentation for more information.	❑
The PTZ settings require that the ActiveX player be installed on a supported browser, such as Internet Explorer. See the "Requirements" section on page 1-4 and the Cisco Video Surveillance Monitoring Workstation Performance Baseline Specification for more information.	❑
To use PTZ controls, you must belong to a user group with *Perform PTZ* permissions.	❑
To configure PTZ presets, PTZ tours, and Advanced Events, you must belong to a user group with *Cameras* permissions.	❑
To configure the PTZ Priority and Lockout Period, you must belong to a user group with *Users & Roles* permissions.	❑

PTZ Camera Configuration Summary

Cameras with PTZ functionality display a **Pan/Tilt/Zoom** tab under the **Image** tab of the Camera configuration page (Figure 10-19). 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 10-19 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 10-1.
Step 3	(Optional) Connect a PTZ joystick to a USB port on your PC and calibrate the device for Windows 7.	• See the joystick documentation for more information. • See the "Calibrating a Joystick for Windows 7" section on page 2-41.
Step 4	Verify that you are using a compatible browser (such as Internet Explorer) with the ActiveX player installed.	• Requirements, page 1-4 • Cisco Video Surveillance Monitoring Workstation Performance Baseline Specification

	Task	Related Documentation
Step 5	Open the camera PTZ configuration page to verify the camera PTZ controls are available: **a.** Select **Cameras** and select a camera name. **b.** Click the **Image** tab and verify that the **Pan/Tilt/Zoom** tab is selected (Figure 10-19).	Accessing the Camera Settings, page 10-42
Step 6	(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 10-73
Step 7	(Optional) Configure the camera PTZ tours. PTZ tours are used to cycle the camera view between PTZ presets.	Configuring PTZ Tours, page 10-75
Step 8	(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 *Return to Home* setting is ignored	Configuring Advanced Settings, page 10-77
Step 9	(Optional) Enter the camera PTZ *idle* time that defines the following: • 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 *Return to Home* 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.	Configuring Advanced Settings, page 10-77
Step 10	(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 10-71
Step 11	(Optional) Configure the Return to Home preset position and timer.	Using Advanced Events to Trigger Actions, page 13-7

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 "Configuring Advanced Settings" section on page 10-77).

Usage Notes

- By default, all user groups have the highest priority (100).
  - See the "Defining the User Group PTZ Priority Level" section on page 10-72 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, page 13-7 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 "Configuring Advanced Settings" section on page 10-77.
- 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 "Viewing Media Server Status" section on page 9-9).

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 loose 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.

a. Select **Users**, and then select the **User Groups** tab .

b. Select a user group or create a new group (see the "Adding User Groups" section on page 4-11 for more information).

c. In the *PTZ priority over other user groups* field, select a number from 1 to 100 (the default is 100—highest priority).

d. 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 "Configuring Advanced Settings" section on page 10-77 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 2-38 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 2-38
- Configuring PTZ Tours, page 10-75
- Configuring Advanced Settings, page 10-77
- Using Advanced Events to Trigger Actions, page 13-7

To configure PTZ presets, use the PTZ controls to adjust the live video stream, enter a preset name, and click **Set**.

Figure 10-20 PTZ Preset Configuration

Procedure

To define PTZ presets, do the following:

Step 1 Open the camera PTZ configuration page:

a. Click **Cameras**.

b. Click a location or Media Server and select a camera.

c. Click the **Image** tab and then click **Pan/Tilt/Zoom** (Figure 10-20).

d. 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 10-71 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:
  - Configuring Advanced Settings, page 10-77
  - Using Pan, Tilt, and Zoom (PTZ) Controls, page 2-38
- 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 "Configuring Advanced Settings" section on page 10-77).
- If the PTZ tour is disabled, the camera will stay at the current position, or go to the *Return to Home* setting, if configured.

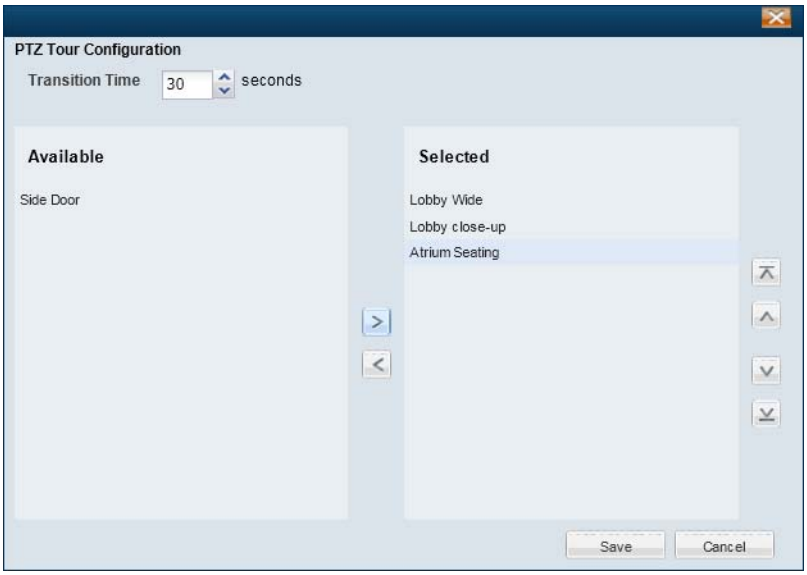
Procedure

Step 1 Define at least two PTZ presets for the camera, as described in the "Configuring PTZ Presets" section on page 10-73.

Step 2 Define the PTZ presets included in the tour:

a. Click **Add** or **Edit** (Figure 10-22) to open the PTZ Tour Configuration window (Figure 10-21).

Figure 10-21 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.

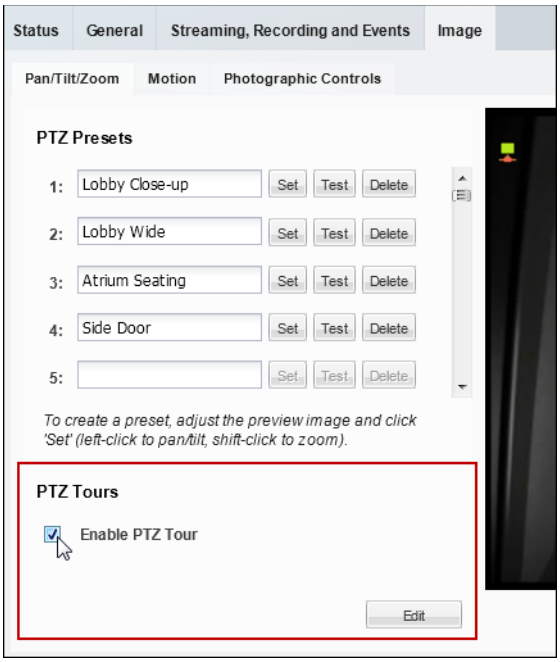
d. Use the up-down arrows to move the presets up or down in the list to define the order of the preset rotation.

e. Click **Save**.

Step 3 (Optional) Select **Enable PTZ Tour** to turn on the PTZ tour for the camera (Figure 10-22).

- The camera will display the PTZ tour whenever live video is displayed. To stop the PTZ tour, you must deselect **Enable PTZ Tour**.

Figure 10-22 Enable the PTZ Tour



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 "Configuring Advanced Settings" section on page 10-77 for more information.

Configuring Advanced Settings

The PTZ advanced settings are define the following:

- The number of *idle* seconds before the following occur:
  - The number of seconds before a PTZ tour resumes (after a manual or event override).
  - The number of seconds a lower priority PTZ user must wait after a higher-priority user stops using the camera PTZ controls.
  - The number of seconds before the camera returns to a PTZ preset "home" position.
- The Return to Home PTZ preset position. This returns a camera to a default PTZ location when the manual PTZ controls are not used for the *idle* length of time.

Procedure

Step 1 Go to the camera's PTZ configuration page.

a. Click **Cameras**.

b. Click a location or Media Server and select a camera.

c. Click the **Image** tab and then click **Pan/Tilt/Zoom** (Figure 10-20).

Step 2 Click PTZ **Advanced Settings**.

Step 3 Use the following settings to define if the camera should return to a selected Home position when idle for a specified number of seconds.

Table 10-17 Camera PTZ Advanced Settings

Setting	Description
When manual PTZ idle for	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 *Return to Home* setting). **Note** By default, the idle time is defined by the Media Server's *Camera Control Lockout* setting (see the "Viewing Media Server Status" section on page 9-9). Use the *When manual PTZ idle for* field to override the server setting for the current camera. • 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 10-75. • Return to Home—the number of seconds after a manual PTZ movement or event action before the camera returns to the *Return to Home* preset position. The timer is reset whenever the camera PTZ controls are used by an operator or event action. You can also display a countdown and cancel option on the users screen (see Configuring a PTZ "Return to Home" Countdown, page 10-79). • 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 10-71.
Enable Home Preset	If enabled, the camera will move to the *Return to Home* preset location if idle for the number of seconds in the *When manual PTZ idle for* setting. De-select this option to disable the *Return to Home* feature. **Usage Notes** • If a PTZ tour is enabled, then the *Return to Home* setting is ignored. • Configure at least one PTZ preset (see Configuring PTZ Presets, page 10-73).
Return to Home	Select the PTZ preset used as the *Home* position.

Step 4 Click **OK** to accept the advanced settings.

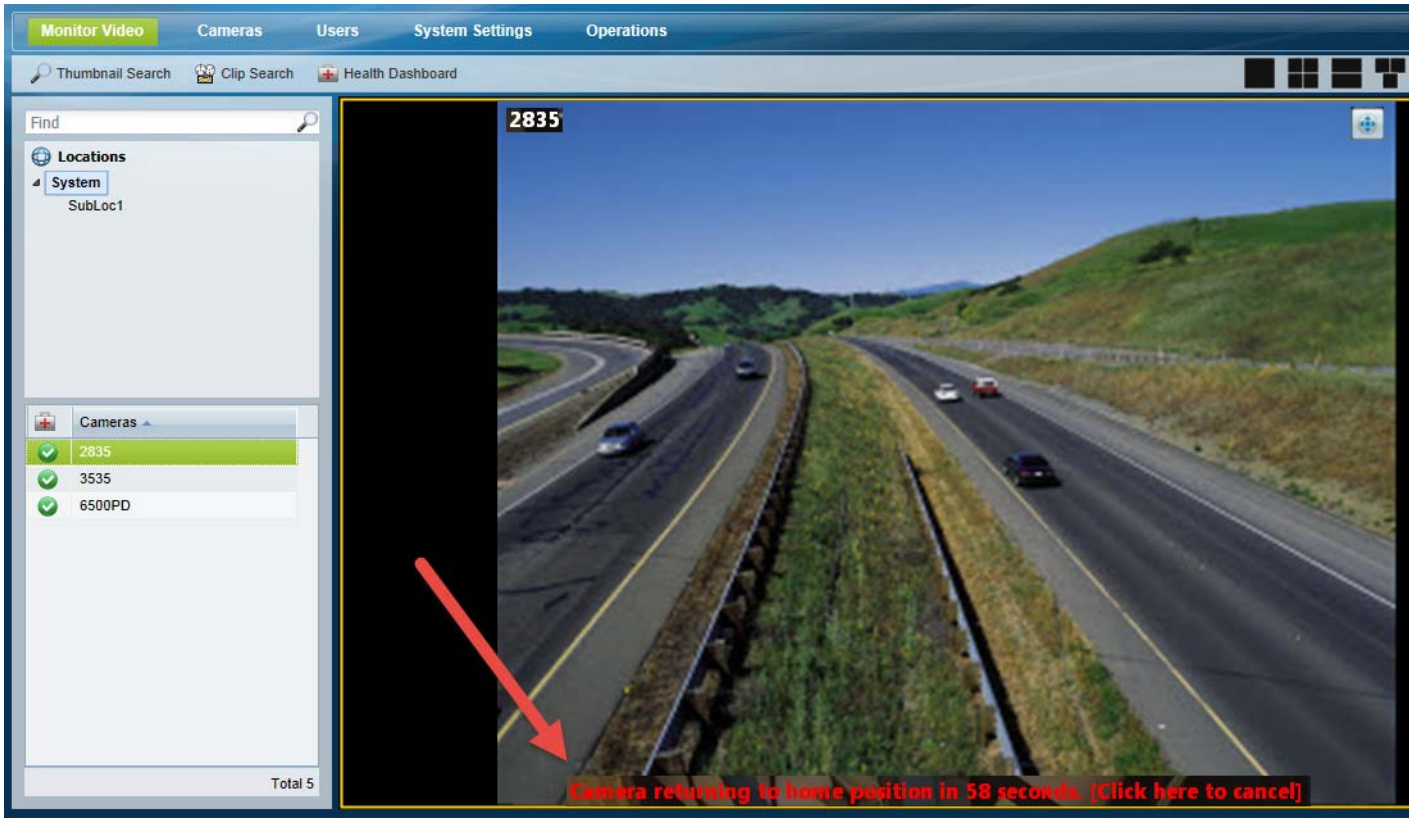
Step 5 Click **Save** to save the PTZ changes on the camera.

Configuring a PTZ "Return to Home" Countdown

Use the Advanced Settings to return a camera to a default PTZ location when the manual PTZ controls are not used for a specified length of time (see Configuring Advanced Settings, page 10-77)

If the "Return To Home" feature is enabled for one or more cameras, you can optionally display a warning on the monitoring workstation before the camera returns to the home PTZ position (Figure 10-24). This warning also allows users to cancel the operation and keep the camera at the current position, if necessary.

Figure 10-23 Return To Home Warning



This option is configured on each client workstation by editing the following setting using the computer's Registry Editor. The message appears 60 seconds before the camera returns to the home position. This value can also be (optionally) modified).

Tip The following process edits the Cisco Multi-Pane Video Surveillance Client that is installed on the workstation when you first access the Cisco VSM Operations Manager or the Cisco Video Surveillance Safety and Security Desktop application (Cisco SASD). This "Multi-Pane" client is the ActiveX utility installed on each client machine to enable video viewing and controls. See the "Requirements" section on page 1-4 and the Cisco Video Surveillance Monitoring Workstation Performance Baseline Specification for more information.

Note You must edit the setting for both the 32-bit client and the 64-bit client (if installed). The 64-bit client is used for 64-bit IE browsers and the Cisco SASD application.

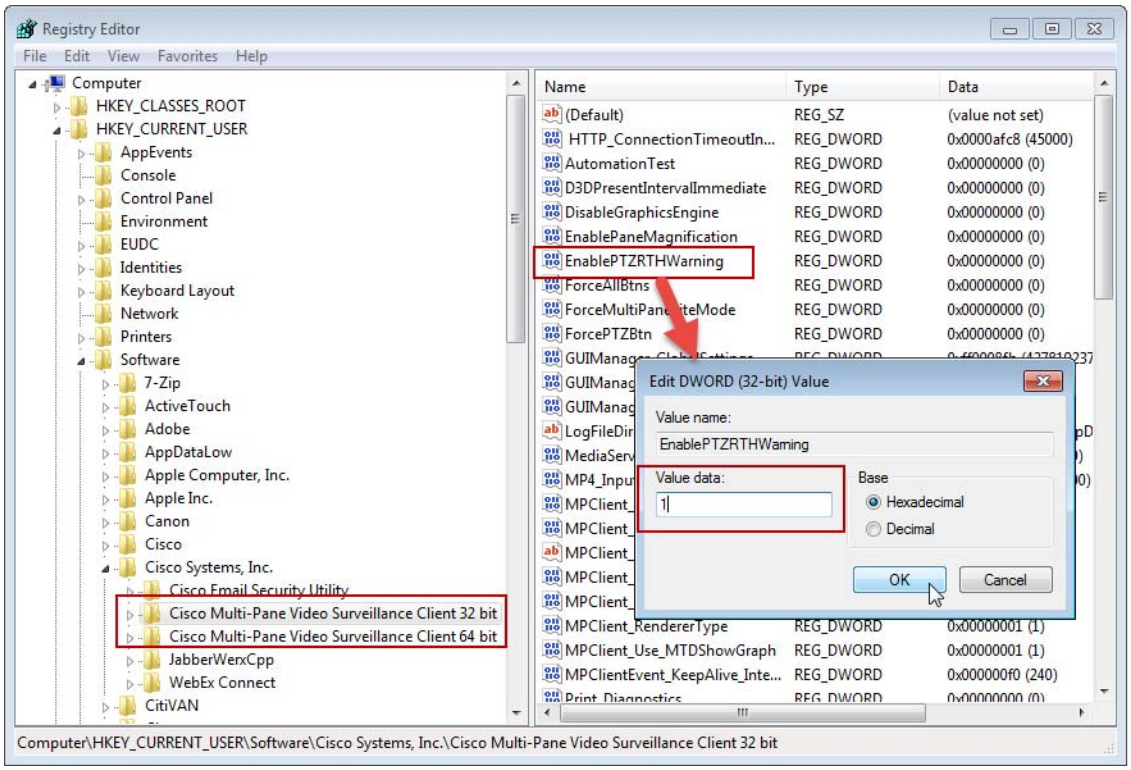
Procedure

To configure a Return to Home countdown on the monitoring workstation (as shown in Figure 10-24):

Step 1 Go to **Start** > **Search**, and enter **regedit**.

Step 2 Select **regedit** from the results to open the Registry Editor utility (Figure 10-24).

Figure 10-24 Edit the Registry Editor Entry On Each Workstation



Step 3 Enable the 32-bit multi=pane client (which is used for the browser).

a. Select to **HKEY_CURRENT_USER** > **Software** > **Cisco Systems, Inc.** > **Cisco Multi-Pane Video Surveillance Client 32 bit**.

b. Double-click the **EnablePTZRTHWarning** entry.

c. Enter **1** in the Value Data field.

1=the warning is on

0=the warning is off

d. Click **OK**.

Step 4 Repeat these steps for the 64-bit client:

a. Select **HKEY_CURRENT_USER** > **Software** > **Cisco Systems, Inc.** > **Cisco Multi-Pane Video Surveillance Client 64 bit**).

b. Double-click the **EnablePTZRTHWarning** entry.

c. Enter **1** in the Value Data field.

d. Click **OK**.

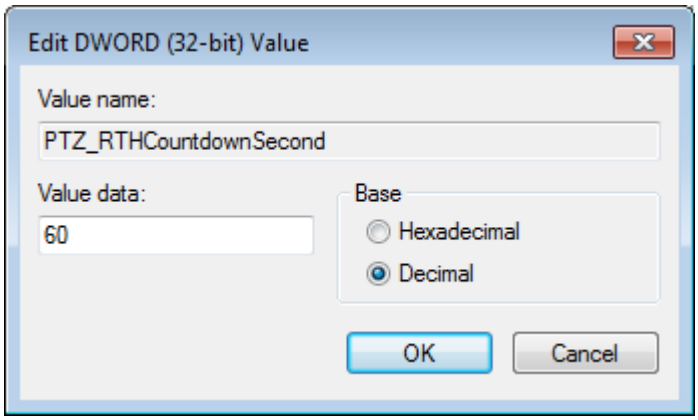
Step 5 (Optional) Change the number of seconds the message will appear before the camera returns to the home position. The default value is 60 (seconds).

a. Double-click the **PTZ_RTHCountdownSecond** entry (Figure 10-25).

b. Enter a decimal value in the Value Data field. This number is the number of seconds.

c. Click **OK**.

Figure 10-25 (Optional) Edit the Number of Countdown Seconds



Step 6 Close the Registry Editor window.

Step 7 Restart the monitoring windows by closing and re-launching any Operations Manager windows or the Cisco SASD application.

Step 8 Test the monitoring workstation to verify that the warning message appears (Figure 10-24 on page 10-80).

a. When 60 seconds remain in the countdown, a message appears: *Camera returning to home position in <X> seconds [Click here to cancel].*

b. If the user clicks **Cancel**, the cameras stays in the current position and the return to home timer is reset.

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 10-87).
- 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.
- Be sure to successfully save or revert your changes while still in the motion configuration window. Clicking out of the window before changes are successfully saved or discarded can cause a configuration mismatch to occur on the camera Status page (the error will not include any additional details). See the "Camera Status" section on page 10-62. If this occurs, perform a Repair Configuration on the camera (see the "Repairing a Mismatched Configuration" section on page 19-25).

Refer to the following topics for more information.

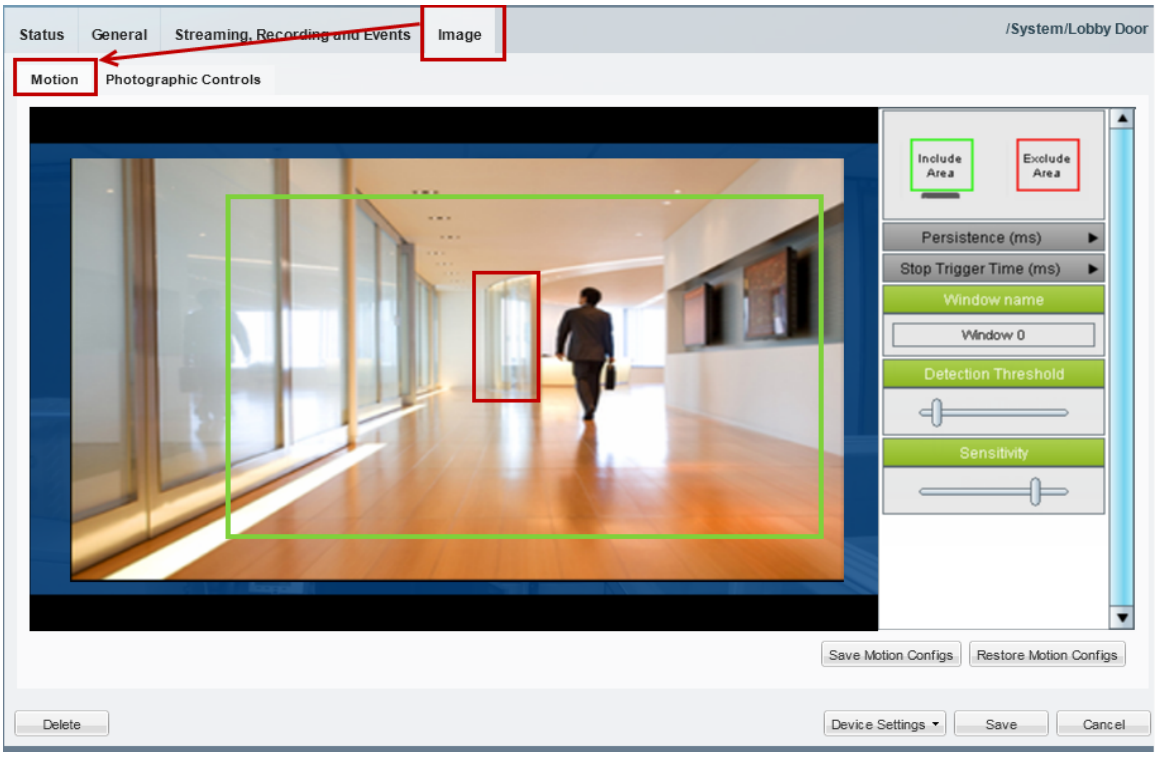
Related Documentation

Using Advanced Events to Trigger Actions, page 13-7—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 10-26).

Figure 10-26 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 10-26). 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 10-87 to include the entire field of view for multiple cameras.
- See the "Configuring Motion Detection" section on page 10-85 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 10-84.
- The motion video settings require that the ActiveX player be installed on a supported browser, such as Internet Explorer. See the "Requirements" section on page 1-4and the Cisco Video Surveillance Monitoring Workstation Performance Baseline Specification for more information.

Motion Detection Settings

Use the settings described in Table 10-18 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 10-26). Refer to the "Configuring Motion Detection" section on page 10-85 for information to access and save these settings.

Table 10-18 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	Drag and drop the **Exclude Area** box onto the image to exclude portions of the included area. 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.
Persistence	The amount of time that motion must occur (within the selected window) for a motion event *start* to occur. The recommended value is **0** (default): motion of any duration results in a motion *start* event. Select a higher number if the motion duration should continue longer before a motion event is triggered.
Stop Trigger Time	Determines how many seconds to delay when a motion event is considered to have stopped (after the actual motion has ended). Recommended value is **0** (default): the event stops immediately when the motion ends. Select a higher number to define a motion event delay. 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".
Window Name	The name of the selected motion window. Click an *include* or *exclude* area, and enter a meaningful name.
Detection Threshold and Sensitivity	(*Include Areas* only) • 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. These values are set by default based on the recommended settings for the camera model. For example: • Cisco 26xx: Threshold = 10, Sensitivity = 80 • Cisco 29xx: Threshold = 10 Sensitivity = 80 • Cisco 45xx: Threshold = 10 Sensitivity = 80 • Cisco 60xx: Threshold = 1, Sensitivity = 85 (The maximum value is 100. The minimum value is 0.)

Table 10-18 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 Verify that you are using a compatible browser (such as Internet Explorer) with the ActiveX player installed.

See the "Requirements" section on page 1-4and the Cisco Video Surveillance Monitoring Workstation Performance Baseline Specification for more information.

Step 4 (Optional) Complete the "Enabling Motion Detection on All Existing Cameras (Bulk Actions)" section on page 10-87.

Step 5 Open the camera configuration page:

a. Click **Cameras**.

b. Select the camera's location, Media Server or template.

c. Select the camera from the list in the lower left column.

Step 6 Click the **Image** tab.

Step 7 Click the **Motion** tab.

The current camera image appears (Figure 10-26).

Step 8 Add green *Include Areas* (windows) where motion should be detected in the image.

a. Drag the green **Include Area** box onto the video image (Figure 10-26).

b. (Optional) Enter a name in the Window Name field.

c. 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.

d. Repeat these steps to create additional *Include Areas* in the video frame.

Step 9 Define the motion detection settings for each *Include Area*.

a. Click the motion window to select it.

b. Change the motion detection settings, as necessary, as described in Figure 10-26 on page 10-83.

Step 10 (Optional) Add a red **Exclude Area** box within an include box to define where motion should be ignored (Figure 10-26).

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 10-26).

b. (Optional) Enter a name in the Window Name field.

c. Move and resize the motion window.

Step 11 Click **Save Motion Configs**.

Tip Click **Restore Motion Configs** to return the settings to the previously saved value.

Note Be sure to successfully save or revert your changes while still in the motion configuration window. Clicking out of the window before changes are successfully saved or discarded can cause a configuration mismatch to occur on the camera Status page (the error will not include any additional details). See the "Camera Status" section on page 10-62 for more information. If this occurs, perform a Repair Configuration on the camera (see the "Repairing a Mismatched Configuration" section on page 19-25).

Step 12 (Optional) Configure motion event recordings for a camera or template.

See the following for more information:

- Editing the Camera Settings, page 10-42
- Configuring Continuous, Scheduled, and Motion Recordings, page 12-7

Step 13 (Optional) Configure actions that are triggered when a motion event occurs.

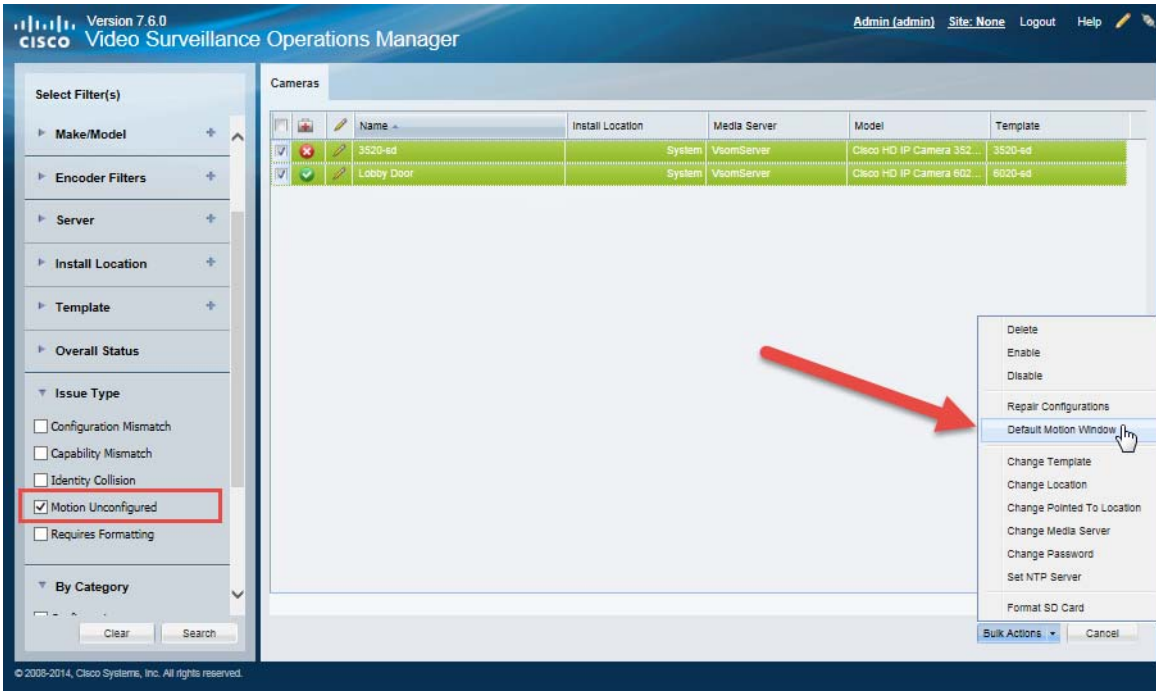
See the "Using Advanced Events to Trigger Actions" section on page 13-7.

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 10-27).

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 10-85).

Figure 10-27 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 10-84
- Configuring Motion Detection, page 10-85

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. Analog cameras must also reconfigure the serial connection.

See the following topics for more information. Analog cameras must also reconfigure the serial connection.

- Editing the Camera Settings, page 10-42
- Configuring PTZ Presets, page 10-73
- Configuring Motion Detection, page 10-82
- Adding External Encoders and Analog Cameras, page 16-5

Replacement Options

In Release 7.5 and later, you can replace a camera with an existing camera (a camera that was previously added to Cisco VSM), or with a new camera. If replacing the camera with an existing camera, the camera must have been previously added to the Operations Manager.

See the "Camera Replacement Procedure" for more information.

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).

Addressing Camera "Collisions"

When you attempt to replace a camera when a device id-collision exists, the replacement will fail and you must first clear the collision.

For example:

- If you attempt to replace CameraB with CameraA, but the devices are in id-collision.

- You attempt to replace Camera A with a newly added CameraB, but a cameraC is already in the system that is colliding with cameraB.

In these situations, the Operations Manager will not proceed with the replacement, stating that the camera is already in collision, and you must first clear the collision using one of the following methods:

- Soft-delete or delete one or more of the cameras (such as the camera already in the system). The camera may be in the Pending camera list or elsewhere.
- Replace one camera with the other (merge the devices to eliminate the collision).

Note An IP collision occurs when two devices are configured with the same IP address.

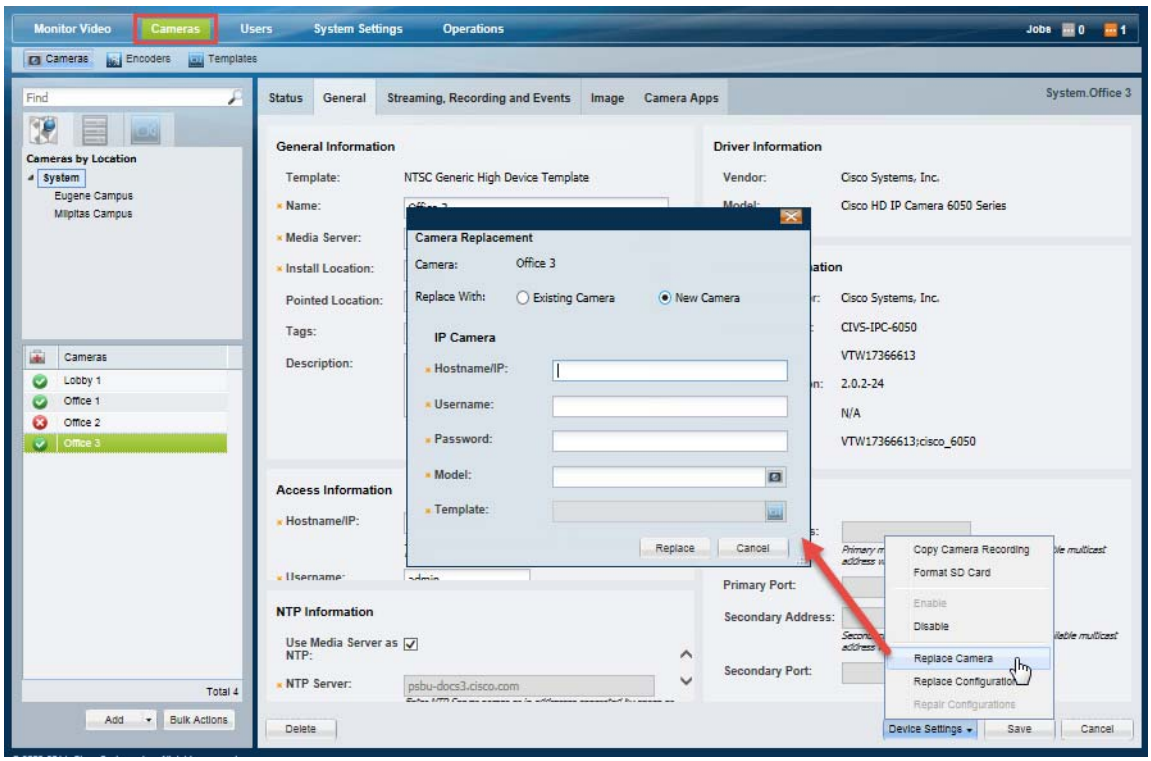
Camera Replacement Procedure

Step 1 Open the camera configuration page for the existing camera (the camera to be replaced).

See the "Accessing the Camera Settings" section on page 10-42.

Step 2 Select **Device Settings** > **Replace Camera** (Figure 10-28).

Figure 10-28 Replace Camera



Step 3 Select **Existing Camera** if the device was previously added to the Operations Manager.

a. Click the Camera Name field.

b. Select a camera from the pop-up window (the remaining fields are automatically completed).

c. Click **Replace**.

d. Modify the camera settings, if necessary:

Camera	(Read-only) The name of the existing camera.
Replace With	
Camera Name	(Required) Select the new (replacement) camera.
Template	(Required) Select the camera template.
Username/ Password	(Required for IP Cameras Only) Enter the credentials used to access the replacement camera on the network.

e. Wait for the job to complete.

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.
- If an error occurs, see the "Addressing Camera "Collisions"" section on page 10-88.

f. Re-configure the contact closure, PTZ preset and motion detection settings, if necessary. See the following topics for more information. Analog cameras must also reconfigure the serial connection.
   - Editing the Camera Settings, page 10-42
   - Configuring PTZ Presets, page 10-73
   - Configuring Motion Detection, page 10-82
   - Adding External Encoders and Analog Cameras, page 16-5

Step 4 Select **New Camera** if the device is not in the Operations Manager configuration.

a. Enter the basic device configuration:
   - IP address

- Username
- Password
- Model
- Template

b. Click **Replace**.

c. Wait for the job to complete.

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.
- If an error occurs, see the "Addressing Camera "Collisions"" section on page 10-88.

d. 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 10-42
- Configuring PTZ Presets, page 10-73
- Configuring Motion Detection, page 10-82
- Adding External Encoders and Analog Cameras, page 16-5

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

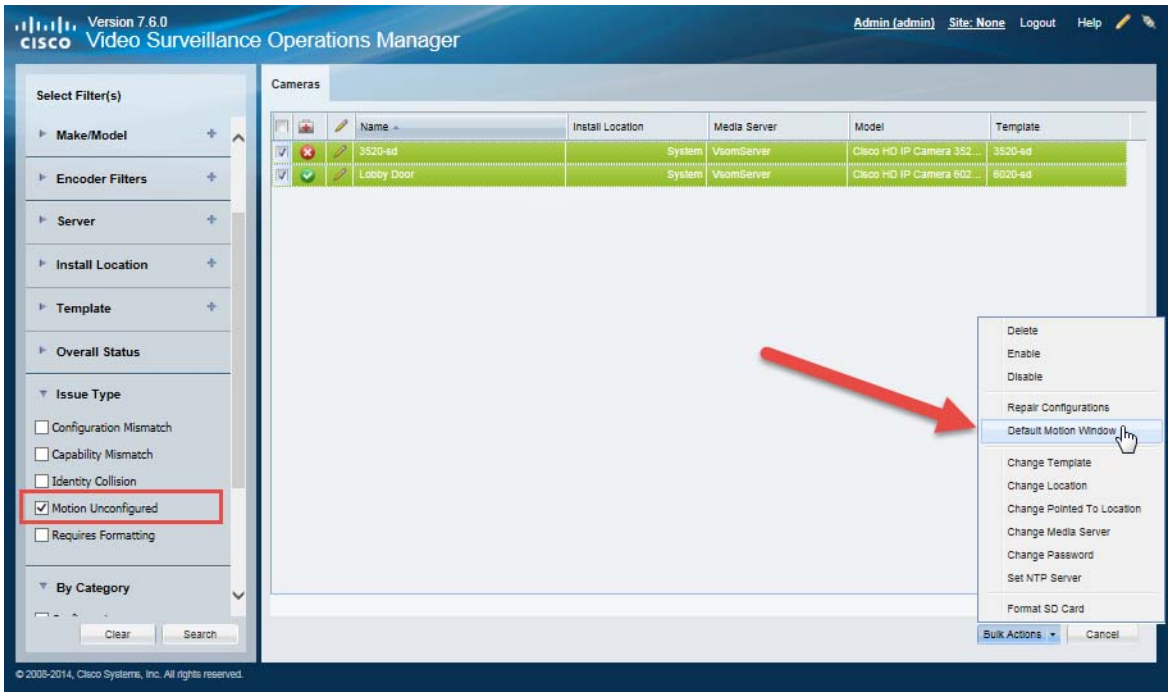
- Bulk Actions: Revising Multiple Encoders, page 16-11
- Bulk Actions: Revising Multiple Servers, page 6-26.

Procedure

Step 1 Select **Cameras** > **Cameras**.

Step 2 Click **Bulk Actions** (under the device list) to open the Bulk Actions window (Figure 10-29).

Figure 10-29 Bulk Actions Window



Step 3 Select the filter criteria (Table 10-20).

Table 10-20 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 `Enter`.
Make/Model	Select the device model(s). For example, "Cisco HD IP Camera 4300E Series".
Encoder Filters	Click to select the encoder(s).
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	Select the administrative states for the devices. For example: • **Enabled (OK, Warning** or **Critical)**—The device is enabled, although it may include a *Warning* or *Critical* 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). **Tip** See the "Device Status: Identifying Issues for a Specific Device" section on page 19-9 for more information.
Issue Type	Select the issues that apply to the device. For example: • **Configuration Mismatch**—the camera configuration on the Media Server is different than the camera configuration in the Operations Manager. **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. • **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.
Category	Select the issue categories that apply to the device. For example, hardware issues or configuration issues.

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.

Table 10-21 Camera Bulk Actions

Action	Description
Delete	Deletes the selected devices from the Operations Manager configuration. See Deleting Cameras, page 10-58 for more information.
Enable	Enable the selected devices. See Camera Status, page 10-62.
Disable	Disable the selected devices. See Camera Status, page 10-62.
Repair Configurations	Synchronizes the configuration for the selected devices. See Repairing Camera Configuration Errors, page 10-66 for more information.
Default Motion Window	Sets the motion detection window for the devices. See Enabling Motion Detection on All Existing Cameras (Bulk Actions), page 10-87.
Change Template	Changes the template assigned to the devices. See the following for more information: • Adding and Editing Camera Templates, page 12-1 • Streaming, Recording and Event Settings, page 10-48.
Change Location	Change the location for the selected devices. See the following for more information: • General Settings, page 10-44 • Creating the Location Hierarchy, page 5-1.
Change Pointed To Location	Change the location for the selected servers. See the following for more information: • General Settings, page 10-44 • Understanding a Camera's Installed Location Vs. the Pointed Location, page 5-9.
Change Media Server	Change the Media Server that manages the camera. See the following for more information: • General Settings, page 10-44 • Configuring Media Server Services, page 9-1
Change Password	Change the password for the devices. **Note** Only super-admin users can apply the **Change Password** option using Bulk Actions.

Table 10-21 Camera Bulk Actions (continued)

Action	Description
Set NTP Server	Defines the NTP server for the selected devices. This option is only available for device models that support NTP. See the following for more information: • "General Settings" section on page 10-44 • Understanding NTP Configuration, page 8-1
Format SD Card	Format the SD cards that are installed in the cameras. See the following for more information: • Formatting Camera SD Cards, page 15-5 • Connected Edge Storage (Camera Recording), page 15-1

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 19-29.

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 10-1.

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.*

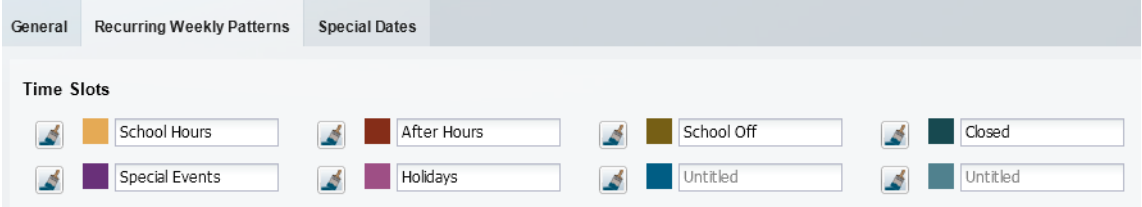
Step 5 Click **Create**.

Step 6 Click the **Recurring Weekly Patterns** tab.

Step 7 Define the *Time Slots* for the schedule (Figure 11-1).

In the camera or template configuration, each time slot can be assigned a different set of recording and alert rules.

Figure 11-1 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:

School Hours	Hours when school is in session.
After School	Hours outside of the regular school schedule.
School Off	Hours when school or other activities are not in session.
Closed	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 11-2).

Active Patterns are the recurring schedule for each day. Paint the appropriate time slot over the hours that the time slot should be active.

a. Select a time slot paint brush (the selected icon turns solid).

b. 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.

c. 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.

d. Repeat these steps to complete the recurring weekly patterns for each day of the week.

e. Click **Save**.

Tip The shortest time-block that can be created is 15 minutes.

Figure 11-2 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 11-2 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.

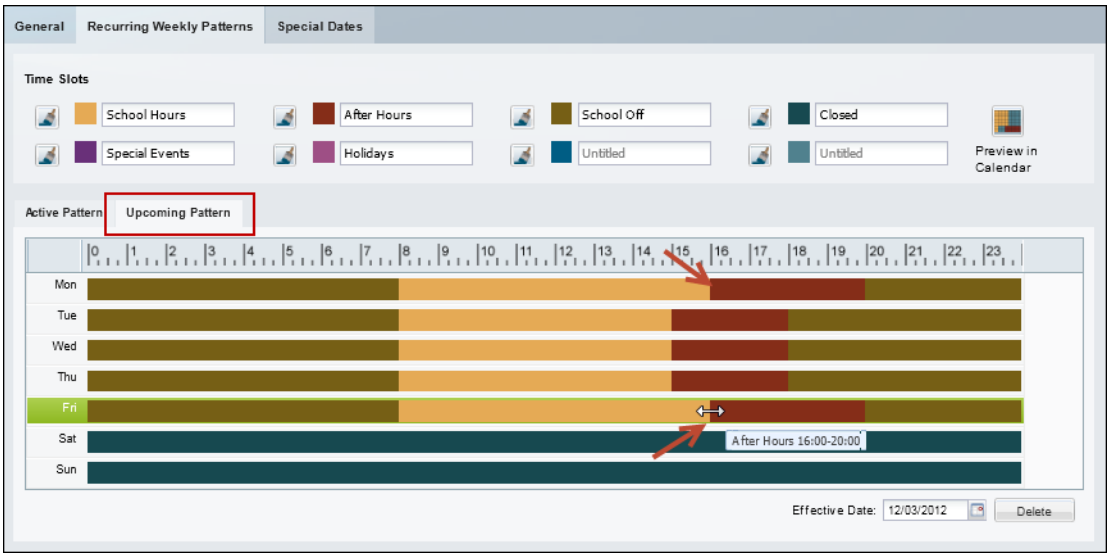
Step 10 (Optional) Click **Create Upcoming** to define a second schedule that will become active on a specified date (Figure 11-3).

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 11-3 Defining an Upcoming Recurring Weekly Pattern



a. Click **Create Upcoming** (Figure 11-2) to create an *Upcoming Pattern* (Figure 11-3). An *Upcoming Pattern* tab is added and pre-populated with the calendar from the *Active Pattern*.

b. Click the **Effective Date** 12/03/2012 to select the date when the *Upcoming Pattern* will take effect.

c. 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.

d. (Optional) Click **Preview in Calendar** to verify that the weekly recurring schedule changes on the time and date desired.

e. Click **Save**.

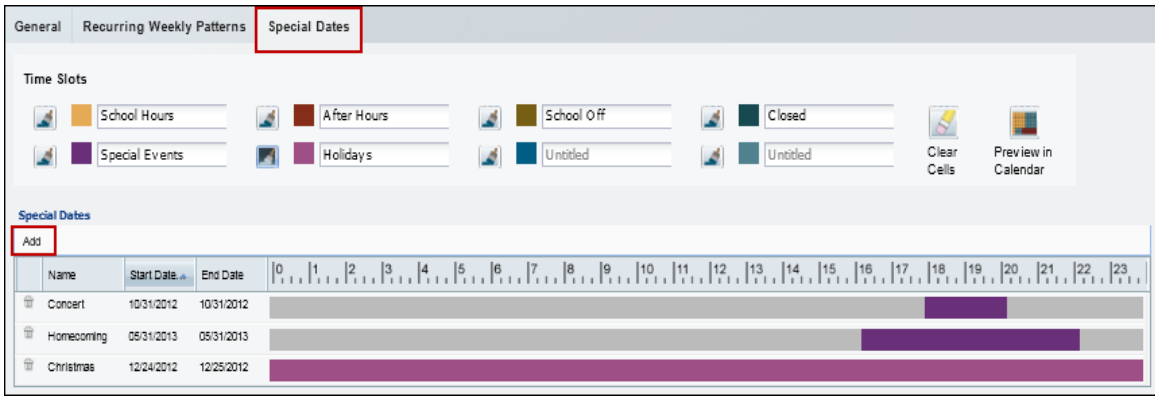
For example, in Figure 11-3, the school hours are extended to 4 p.m. (16:00) on Monday and Friday (beginning on the *Effective Date*).

Step 11 (Optional) Define *Special Dates* to override the normal recurring schedule (Figure 11-4).

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 11-4, 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 11-4 Defining Special Dates



a. Click the **Special Dates** tab (Figure 11-4).

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 11-4).
- 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 11-5).

Figure 11-5 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 10-48
- "Configuring Video Recording" section on page 12-7
- "Using Advanced Events to Trigger Actions" section on page 13-7

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

Related Documentation

- Enabling Video Analytics, page 13-2
- Using Advanced Events to Trigger Actions, page 13-7
- Enabling Record Now, page 3-11.

Overview

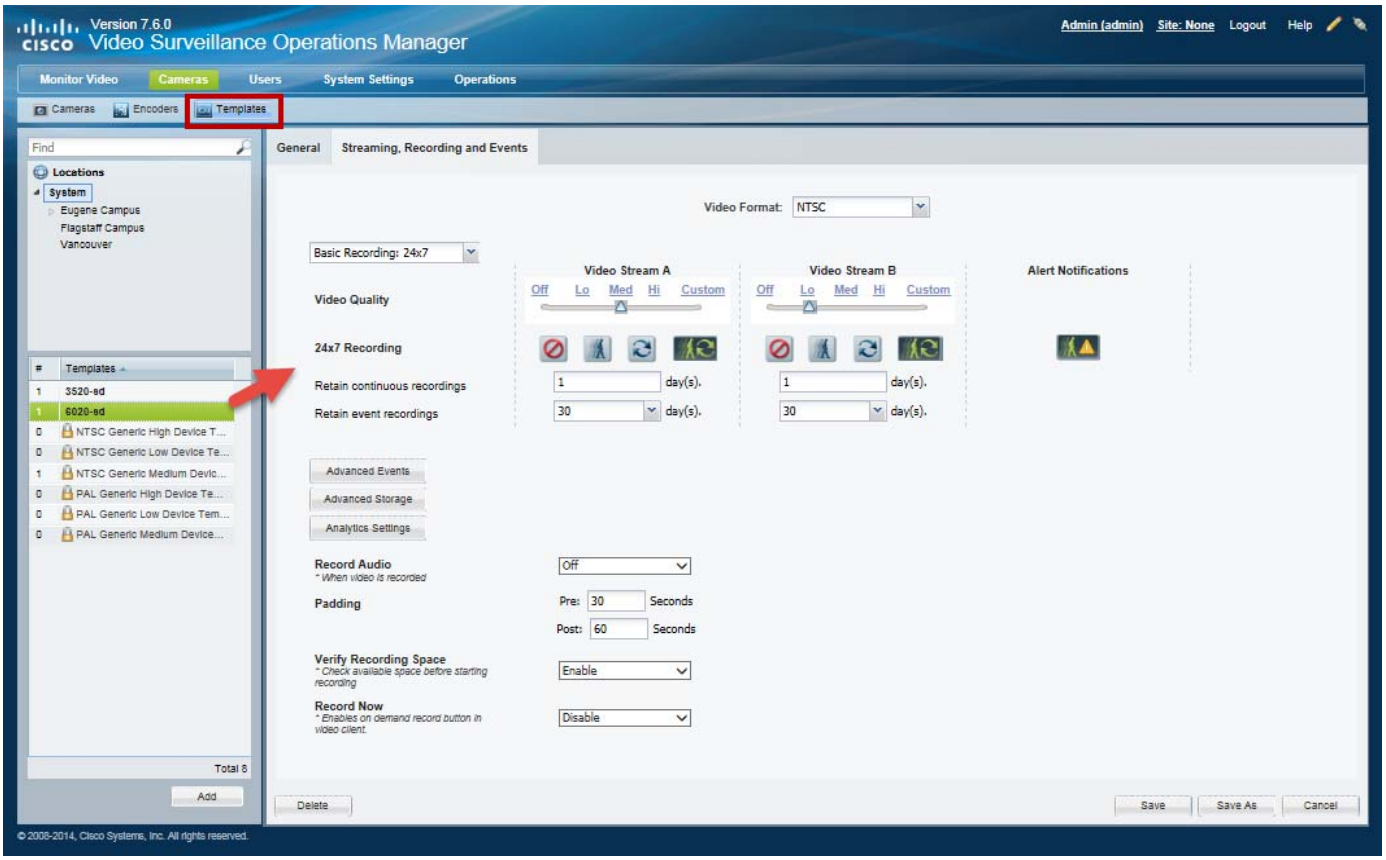
Templates simplify camera configuration by defining the image quality, recording schedule and other attributes used by a set of cameras. Any template changes are applied to all cameras associated with that template, allowing you to easily configure and modify groups of cameras that serve a similar purpose. 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 12-1 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 12-3.

Figure 12-1 Camera Templates



Creating or Modifying a Template

Procedure

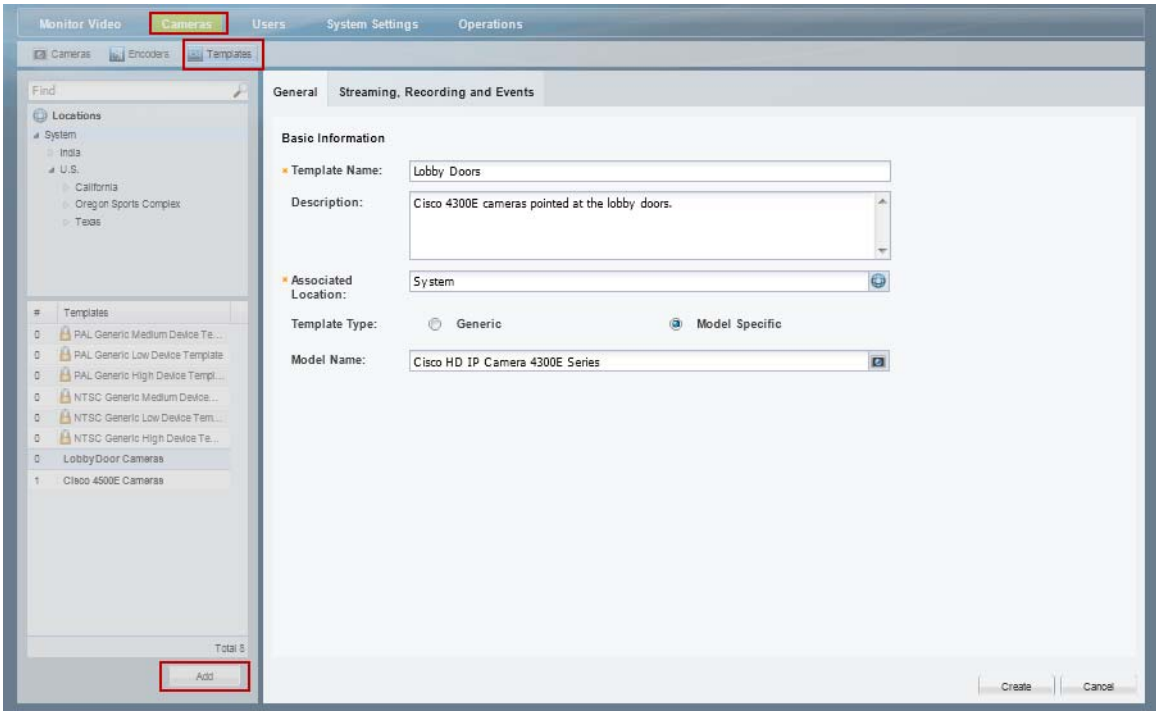
To create or modify a template, complete the following procedure.

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 12-2).

Figure 12-2 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 12-7
  - Streaming, Recording and Event Settings, page 10-48

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 19-29 for more information.
- Device configuration changes can fail is 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 12-3).

Procedure

Step 1 Select a camera name.

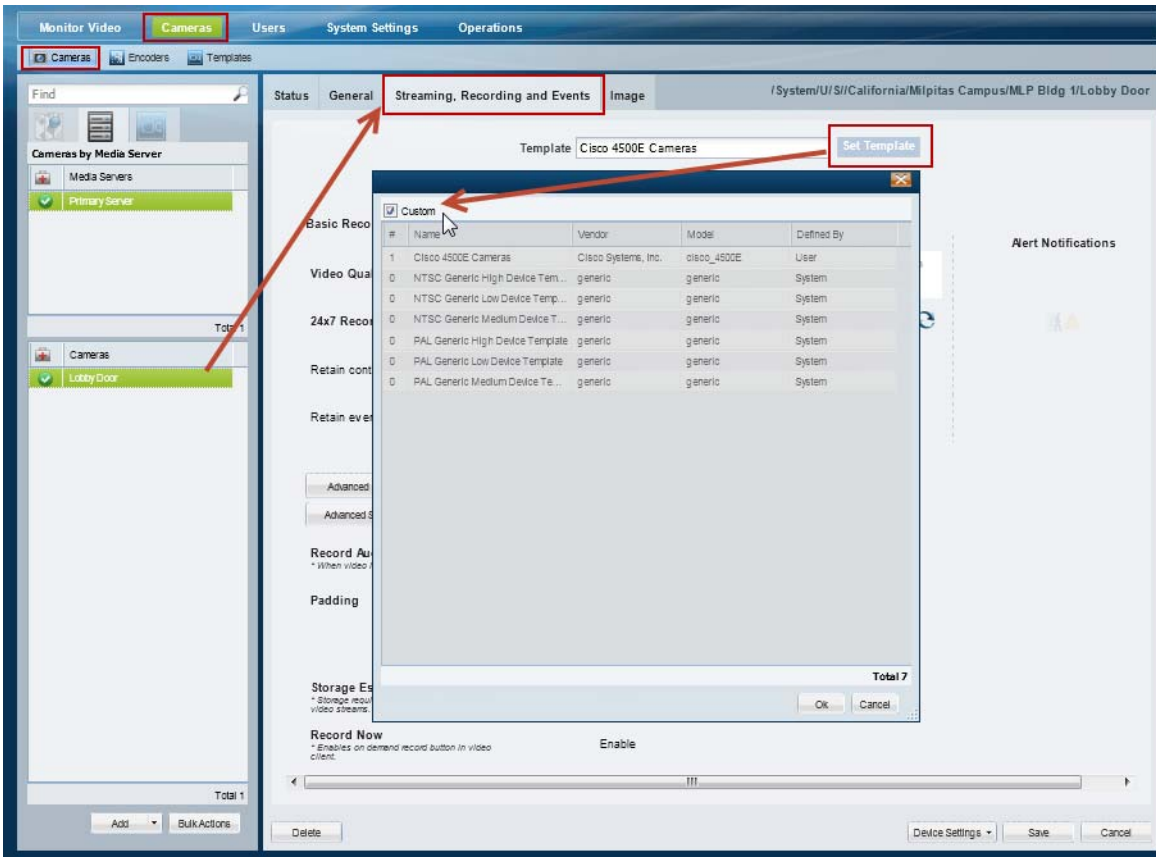
- See the "Editing the Camera Settings" section on page 10-42. For example, click the **Cameras By Location** tab, select a location and camera name.
- You must belong to a User Group with permissions for *Cameras*. See the Adding Users, User Groups, and Permissions, page 4-1 for more information.

Step 2 Click the **Streaming, Recording and Event** tab.

Step 3 Click **Set Template**.

Step 4 Select the **Custom** box and click **OK** (Figure 12-3).

Figure 12-3 Custom Camera Template



Step 5 Revise the camera settings as described in the "Editing the Camera Settings" section on page 10-42 and the "Configuring Video Recording" section on page 12-7.

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 12-1 Configuring Video Topics

Topic	Description
Configuring Continuous, Scheduled, and Motion Recordings, page 12-7	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 13-7	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 3-11	Describes how to enable the **Record Now** option when a user right-clicks a camera's live image.
Connected Edge Storage (Camera Recording), page 15-1	Cameras that support on-device storage of video recordings can be used to record video even if the camera does not have communication with the Cisco Video Surveillance system. Once network communication is re-established, the on-camera recordings can be copied to a Media Server.

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 11-1 for instructions.

Step 2 Edit or add a camera template:

a. Click **Cameras**.

b. Select **Templates**.

c. Add or edit a template:

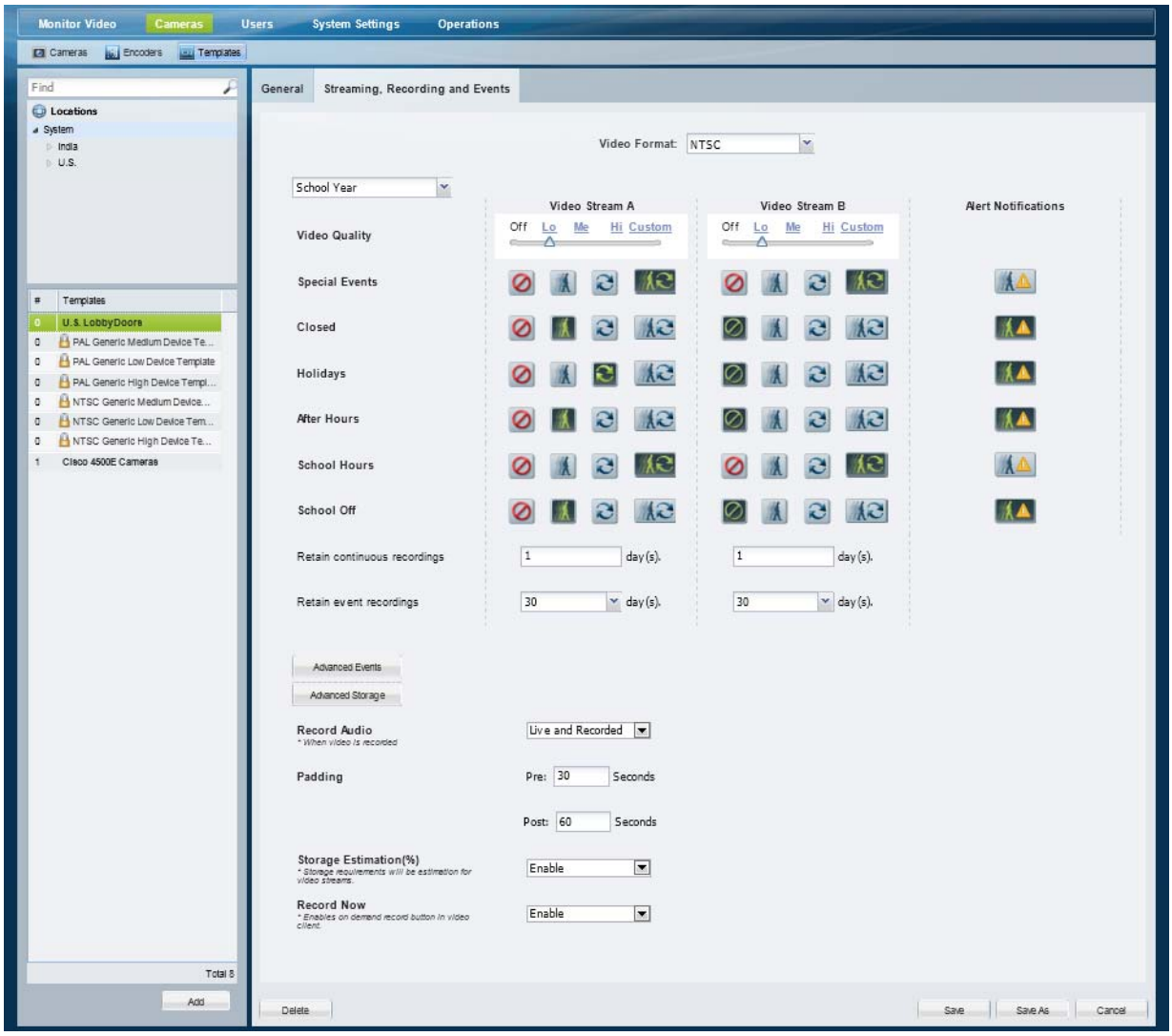
– Click **Add** to create a new template.

– 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 12-5

Step 3 Click the **Streaming, Recording and Events** tab (Figure 12-4).

Figure 12-4 Recording Schedule



Step 4 Select a recording schedule (Figure 12-4).

- **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 11-1 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 10-82 for instructions to define the areas of the image that trigger motion events.
- **Continuous Recording**—Record video in a continuous 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 13-7.

Step 8 Configure the optional recording options:

Table 12-2 Optional Recording Options

Recording Option	Description	More Information
Advanced Events	Define events that can trigger video recording far 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 13-7
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 17-12.
Analytics Settings	Enable metadata tracks used to analyze images for attributes and events that occur within the image. For example, *Luminance* metadata that is generated for a video feed can be used perform Video Motion Search using the Cisco Video Surveillance Safety and Security Desktop (Cisco SASD) application.	Enabling Video Analytics, page 13-2
Record Audio	Define if audio should be recorded.	Streaming, Recording and Event Settings, page 10-48
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 10-48
Record Now	The Record Now feature allows operators to trigger recordings that are retained according to the *Retain event recordings* setting.	• Enabling Record Now, page 3-11 • Using Record Now, page 2-26

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 19-29 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.

Requirements

To configure multicast streams, you must do the following:

Table 12-3 Multicast Requirements

Requirements	Complete? (✓)
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. The allowed multicast port range any even number from 16000 – 19999.	❑

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.

a. Select **Cameras** > **Templates**.

b. Select a location and template name.

c. Select the **Streaming, Recording and Events** tab.

d. Click the **Custom** option for either Video Stream A or Video Stream B.

e. Select **JPEG** from the Codec field.

f. Select **UDP_Multicast** from the Transport field.

g. Complete the remaining custom stream settings.

h. 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 12-5.

Step 3 Enter the Multicast IP address in the camera configuration page.

See the "Multicast" descriptions in the "General Settings" section on page 10-44 for more information.

a. Select **Cameras**.

b. Select a location and camera name.

c. 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 10-11.

Video Analytics and Advanced Events

Video analytics are used to analyze images for attributes and events that occur within the image. For example, *Luminance* metadata that is generated for a video feed can be used perform Video Motion Search using the Cisco Video Surveillance Safety and Security Desktop (Cisco SASD) application.

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.

Refer to the following topics for more information.

Contents

Enabling Video Analytics

Video analytics are used to analyze images for attributes and events that occur within the image.

For example, *Luminance* metadata that is generated for a video feed can be used to perform Video Motion Search using the Cisco Video Surveillance Safety and Security Desktop (Cisco SASD) application (or a third party monitoring application).

To enable a metadata track, a Metadata Server must be added to the Operations Manager, and the metadata track must be enabled on a camera template. Cameras added to that template will generate a lower-resolution version of the recorded video that includes the metadata information. That metadata track is then access by Cisco SASD or a third party application to analyze the video.

Refer to the following topics to enable metadata tracks using Operations Manager:

- Supported Analytics Metadata Tracks, page 13-2
- Metadata Requirements, page 13-3
- Metadata Summary Steps, page 13-4
- Metadata Detailed Steps, page 13-4
- Viewing the Registered Metadata Types, page 13-6

Tip See the Cisco Video Surveillance Safety and Security Desktop User Guide for more information to view and analyze the video metadata tracks.

Supported Analytics Metadata Tracks

This version of Cisco Video Surveillance supports the following metadata tracks:

Table 13-1 Supported Metadata Tracks

Metadata Track	Description
Luminance	Creates a lower-resolution video track that includes metadata used to perform a Video Motion Search of recorded video.

Note Metadata is retained on the system according to the Retention Time setting in the Analytics Setting page. See Figure 13-2 for more information.

Metadata Requirements

The following requirements must be met to enable and view video analytics metadata.

Table 13-2 Metadata Requirements

Requirements	Complete? (✓)
A stand-alone server configured with the Metadata Server service. • The server can be a physical or virtual machine. • Only stand-alone Metadata servers are supported in this release. The server cannot run additional server services. • Cisco VSM Release 7.5 or higher (operating system RHEL6.4) is required. **Related Information** • Configuring Servers, page 6-1 • Understanding Server Services, page 6-3 • Cisco Video Surveillance Management Console Administration Guide	❑
The server also requires an available server license. See the "Installing Licenses" section on page 1-26.	❑
You must belong to a Cisco Video Surveillance User Group with permissions for the following: **Enable Analytics on the Server (using the Operations Manager)** To enable video analytics on the Operations Manager server, you must belong to a User Group with permissions for the following: • *Servers & Encoders*—To add a Metadata Server to the Operations Manager. • *Templates* and *Cameras*—To enable analytics metadata tracks in the Operations Manager. **Generate Metadata and View Motion Results (using Cisco SASD)** All of the following permissions are required to use Cisco SASD to generate metadata, view the generated metadata, and perform video motion searches (see the Cisco Video Surveillance Safety and Security Desktop User Guide for more information). • *Post Analytics Metadata* • *View Analytics Metadata* • *View Live Video* • *Perform PTZ* (automatically enabled with *View Live Video*) • *View Recordings* • *Camera* (Manage permission) See the "Adding Users, User Groups, and Permissions" section on page 4-1 for more information.	❑

Table 13-2 Metadata Requirements (continued)

Requirements	Complete? (✓)
A camera template configured for analytics metadata. For example, add the *Luminance* metadata track to record luminance metadata used to analyze motion events. **Note** At least one camera must also be assigned to the template. **Related Information** • Adding and Editing Camera Templates, page 12-1 • Metadata Detailed Steps, page 13-4	❑
To analyze metadata tracks (such Video Motion Search), the Cisco SASD desktop application must be installed on a monitoring PC. **Related Information** • Understanding the Video Viewing Options, page 2-2 • Cisco Video Surveillance Safety and Security Desktop User Guide	❑

Metadata Summary Steps

To enable Metadata, do the following:

1. Install and configure a stand-alone Cisco Video Surveillance server.
2. Add a server license, if necessary.
3. Add the server to the Operations Manager configuration as a **Metadata Server** (Service Type).
4. Create a camera template, and click **Analytics Settings**.
5. Add the analytics types. For example, add *Luminance* to enable motion video analytics.
6. Add one or more cameras to the template.
7. Use the Cisco SASD desktop application to access the video analytics features.

Metadata Detailed Steps

Procedure

Step 1 Complete the "Metadata Requirements" section on page 13-3.

Step 2 Install a physical or virtual stand-alone Cisco Video Surveillance server and enable the Metadata service.

See the following for more information:

- Cisco Connected Safety and Security UCS Platform Series User Guide
- Cisco Video Surveillance Management Console Administration Guide

Step 3 Add a server license, if necessary.

Each server requires a server license in order to be added to the Operations Manager configuration. See the "Installing Licenses" section on page 1-26.

Step 4 Add the server to the Operations Manager configuration as a **Metadata Server** (Service Type).

- You must belong to a User Group with permissions for *Servers & Encoders*.
- See the Adding or Editing Servers, page 6-16 for instructions.

Step 5 Create a template with the *analytic type* enabled.

- You must belong to a User Group with permissions for *Templates*.

a. Select **Cameras** > **Templates**.

b. Edit or add a template (see the "Creating or Modifying a Template" section on page 12-3).

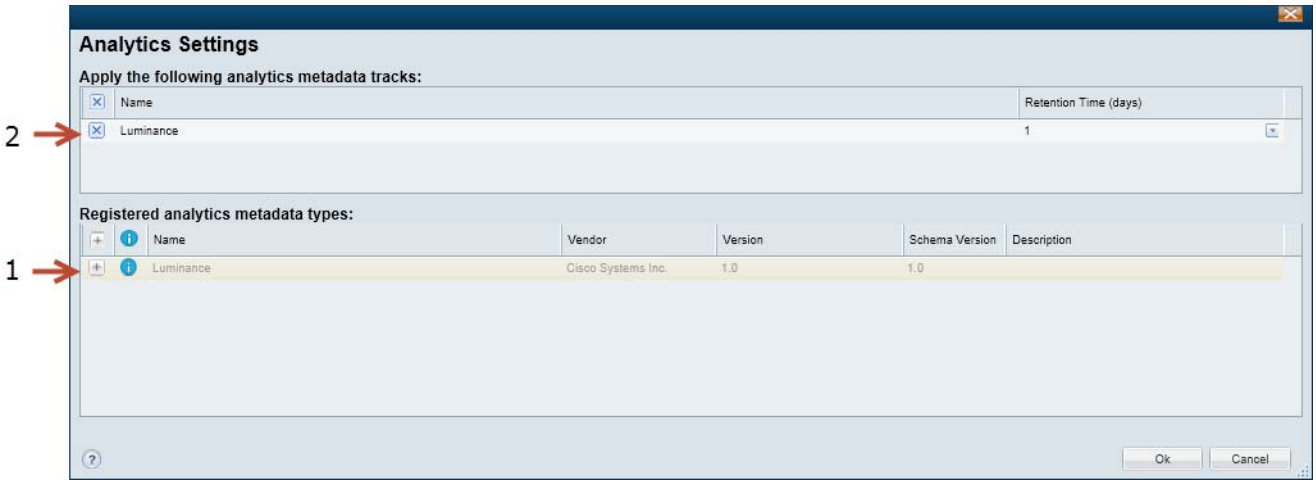
c. Click **Analytics Settings** (Figure 13-1).

d. Click the name or icon of a registered analytics metadata type to add it to enabled the top field "Apply the following analytics metadata tracks".

e. Click **OK**.

f. **Save** the template changes.

Figure 13-1 Enabling Analytics Settings



1	The registered analytics metadata types. Click the name or icon to add the item. Each entry includes the following information: • Name—The name represents the type of metadata that will be generated. • Vendor—The company that provided the metadata service. • Version—The metadata version, which defines the features and capabilities available in the service. • Schema Version—The schema used by system integrators to send and receive analytics data. • Description—More information about the metadata type, if available. **Tip** Go to **System Settings** > **Custom Data Management** > **Analytics Metadata** to view the metadata types that are registered in Cisco VSM. This information is read-only. You cannot update or delete the analytics metadata types.

2	The enabled analytics metadata types. Analytics types in this field will generate metadata tracks used to analyze the video streams. Click the name or icon ⊠ to remove and disable the metadata type. Each entry includes the following information: • Name—The name represents the type of metadata that will be generated. • Retention Time (days)—The number of days the metadata will be retained on the system (and available for analytics). Enter a number between 1 and 3650 (10 years). When the retention time expires, the metadata is deleted.

Step 6 Add one or more cameras to the template.

a. Click **Cameras**.

b. Click **Add** or select an existing camera.

c. Complete the camera settings as described in the "Adding and Managing Cameras" section on page 10-1.

d. Click **Template** and select the template from the pop-up window.

e. Click **Save** or **Create** to save the settings.

Step 7 Use the Cisco SASD desktop application to generate *luminance* metadata for a span of recorded video and perform a Video Motion Search. See the Cisco Video Surveillance Safety and Security Desktop User Guide for more information.

Viewing the Registered Metadata Types

Go to **System Settings** > **Custom Data Management** > **Analytics Metadata** to view the metadata types that are registered in Cisco VSM.

Note This information is read-only. You cannot update or delete the analytics metadata types.

- The Luminance metadata type is registered when a Metadata server is added to the Operations Manager. Luminance metadata is used for post facto metadata generation and analysis.
- Camera apps can also have metadata types that are added to Cisco VSM when a camera app is uploaded to the Cisco VSM Operations Manager. See Managing Camera Apps, page 14-1.

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:

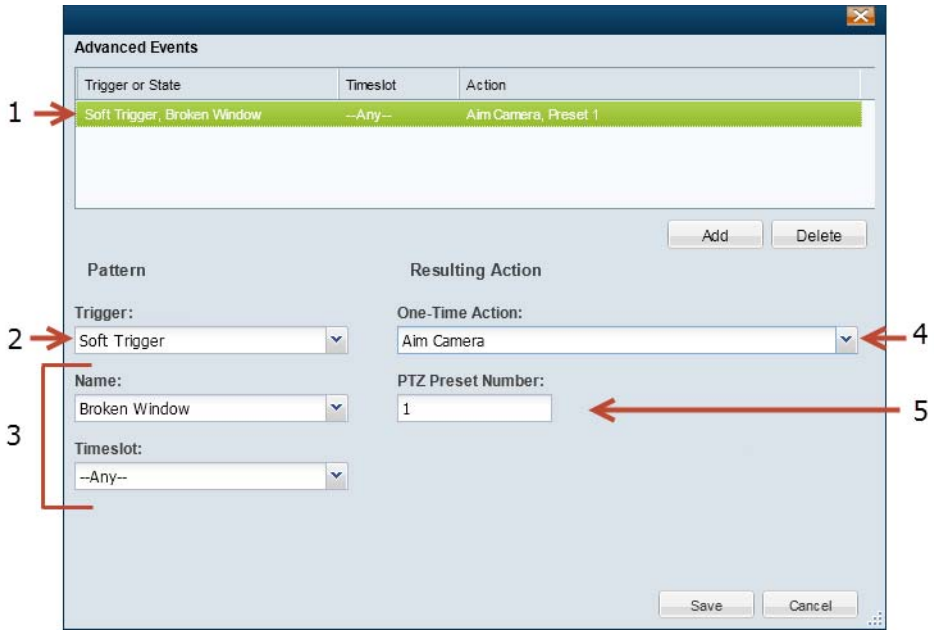
Note

- Advanced events are different from device health events. See the "Device Status: Identifying Issues for a Specific Device" section on page 19-9 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 17-12 for more information.

Configuration Overview

Figure 13-2 describes the main elements of the Advanced Events configuration screen.

Figure 13-2 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 13-9 for more information.
2	The event that triggers an action. See Trigger and Action Descriptions, page 13-9 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 13-9 for more information.
5	The options for the selected action.

Tip To view the events that occur on a camera, go to the camera configuration page and select the **Status** > **Camera Events** tabs. See the "Camera Status" section on page 10-62 for more information.

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 4-1for 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 13-9.

Step 7 Select a *Timeslot* when the event should trigger an action.

See the "Defining Schedules" section on page 11-1 to create timeslots.

Step 8 Select a *Resulting Action* for the event, as described in the "Trigger and Action Descriptions" section on page 13-9.

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.

Tip To view the events that occur on a camera, go to the camera configuration page and select the **Status** > **Camera Events** tabs. See the "Camera Status" section on page 10-62 for more information.

Trigger and Action Descriptions

The following tables describe the event triggers and resulting actions available in Advanced Events.

Note

- For templates that are model-specific, only the triggers and actions supported by the camera model are displayed. For example, triggers for Analytic, Camera App, Contact Closure, and Motion are available only on cameras that support those features.
- If a generic template is used, all options are displayed. If a camera is configured with a trigger or action that is not supported on that device, a "device capability mismatch" occurs. Remove the configuration to clear the error. See the "Camera Status" section on page 10-62 for more information.

Triggers—Table 13-3 describes the events that immediately trigger a one-time action.

Actions—Table 13-4 describes the resulting actions.

Table 13-3 Advanced Event Triggers

Event (Trigger)	Event Options
Analytic	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. When the analytic event occurs, the associated action is triggered. • *Timeslot*—the time span when the event should trigger an action. See the "Defining Schedules" section on page 11-1.
Camera App	A custom application that runs on a camera and triggers a Cisco VSM event. For example, a custom camera application could be added to trigger an event when a certain color appears in the video frame. That event could be forwarded to Cisco VSM, and trigger one of the actions described in Table 13-4. Custom Camera App event types are added when the camera app is added to Cisco VSM. See the following for more information: **Create a camera app** • The camera software development kit (SDK) • *Cisco Video Surveillance API Programming Guide*—Available on the Cisco Developer Network (CDN), or see your Cisco support representative for more information. **Add the camera app** Adding the camera app adds the camera app event type. • Managing Camera Apps, page 14-1 • Creating Custom Event Types and Sub Types, page 13-15
Contact Closed or Opened	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. • *Timeslot*—the time span when the event should trigger an action. See the "Defining Schedules" section on page 11-1. **Note** See the camera and contact device documentation for instructions to connect and configure the contact. **Tip** See the Contact Closure settings described in the "General Settings" section on page 10-44 for instructions to select a camera contact closure port.
Motion Started or Stopped	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 10-82 for more information. • *Timeslot*—the time span when the event should trigger an action. See the "Defining Schedules" section on page 11-1.
Soft Trigger	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). See the "Configuring Soft Triggers" section on page 13-12 for more information.

Table 13-4 describes the action that can be associated with a trigger.

Table 13-4 Resulting Actions

Action	Description
Alert	Generates an alert. For example, if a contact is opened, an alert is triggered. **Tip** Motion alerts triggered using the **Alert Notifications** icon generate an alert for both motion stop and start (see *Recording Options* in the "Streaming, Recording and Event Settings" section on page 10-48). Use the Advanced Events alerts to trigger motion alerts only for motion stop or motion start. **Note** 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.
Aim Camera	Select the pan, tilt and zoom (PTZ) preset that is triggered when the event occurs. • PTZ Preset Number—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 10-73. • 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 2-38). • *Aim Camera* actions are assigned a access priority of 50. This setting cannot be changed. See the "Defining the User Group PTZ Priority" section on page 10-71 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	Enter a valid *Get* or *Post* 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.
Record for Some Time	The number of minutes that video should be recorded when the event occurs. • Stop After (Min.)—The number of minutes to record. • Stream Number – Select **1** for the *primary* stream. – Select **2** for the *secondary* stream.

Table 13-4 Resulting Actions (continued)

Action	Description
Push to Video Wall	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 *Lobby*, then the video would be replaced by video according to the following settings: • **Video Wall**—The Video Wall where the video will be displayed. See the "Configuring Video Walls" section on page 3-9 for more information. • **Live**—Displays live video from the camera that triggered the event. • **Recorded**—Displays recorded video of the event. – **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. **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. **Note** Select both **Live** and **Recorded** to display a 2-pane (1x2) Video Wall with both live and recorded video. **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.
Raise Alert to Federator	Send an alert to the Cisco Video Surveillance Federator (if installed). Only security alerts that are sent to the Federator can be viewed by Federator users. See the following for more information: • Cisco Video Surveillance Safety and Security Desktop User Guide • Using Federator to Monitor Multiple Operations Managers, page 22-1 • Monitoring Device Health Using the Browser-Based Federator, page 22-34

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 (Figure 13-3):

a. Log on to the Operations Manager.

b. Select a template.

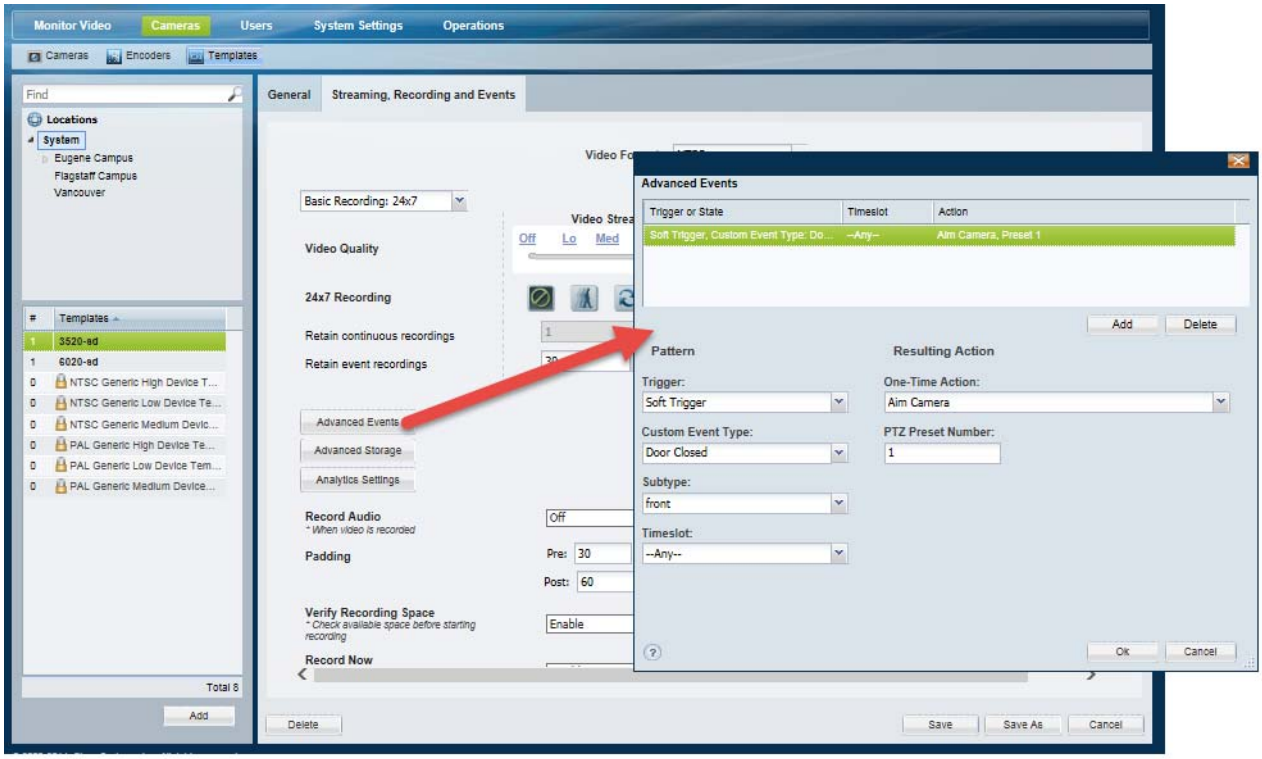
c. Click the **Streaming, Recording and Events** tab.

d. Click **Advanced Events**.

e. Click **Add** to create a new entry.

Step 2 Select the Soft Trigger and resulting action (Figure 13-3).

Figure 13-3 Copying Soft Trigger URLs from the Camera Configuration Page



a. Trigger—Select **Soft Trigger** and enter a name for the trigger.

b. Custom Event Type—Select a Soft Trigger event.

- Click **Add** to create a new Soft Trigger entry.
- Go to **System Settings** > **Custom Data Management** to manage the Soft Trigger entries. See Creating Custom Event Types and Sub Types, page 13-15 for more information.

c. Subtype—Select a subtype, if (optionally) configured for the soft trigger.

d. Timeslot—Select the *Timeslot* when the soft trigger will be enabled. For example, Aim Camera to a PTZ preset position.

e. Select a *Resulting Action* for the event, as described in the "Trigger and Action Descriptions" section on page 13-9.

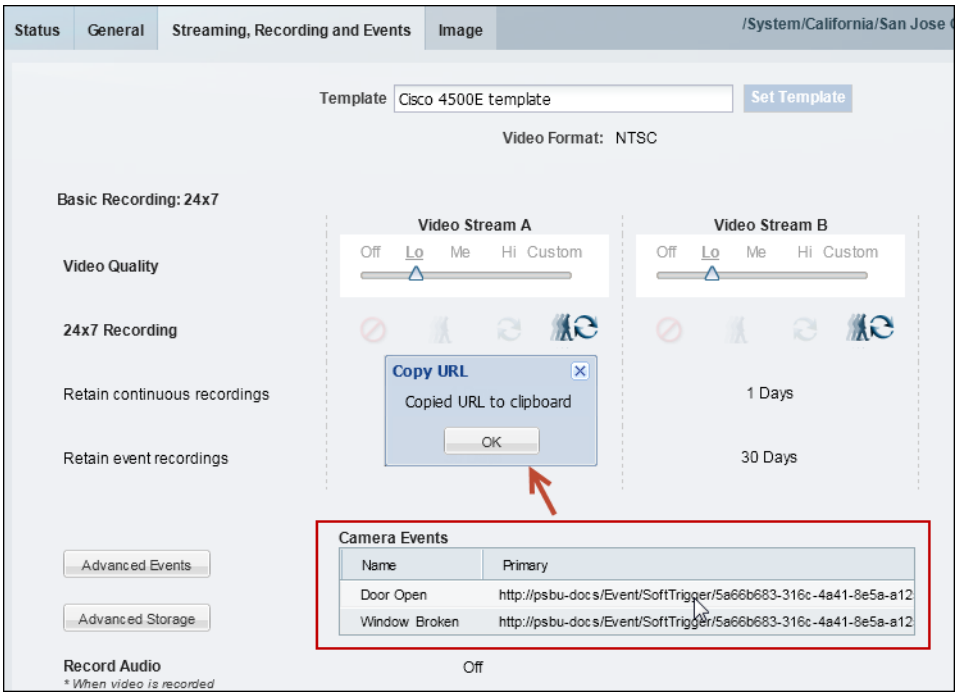
Tip To trigger multiple actions, click **Add** again to add an additional soft trigger entry.

f. Click **OK** to save the settings and close the Advanced Events window.

g. Click **Save** again to save the template changes.

Step 3 Copy the camera URL for use on the external system (Figure 13-4):

Figure 13-4 Copying Soft Trigger URLs from the Camera Configuration Page



a. Select **Cameras** and select the camera that to be triggered by the external system.

b. Click the **Streaming, Recording and Events** tab.

- The Soft Trigger URLs are displayed in the Camera Events table (Figure 13-4).
- 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 4 (Optional) Configure an external system to add additional alert fields, see the *Cisco Video Surveillance API Programming Guide* for more information.

Step 5 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.

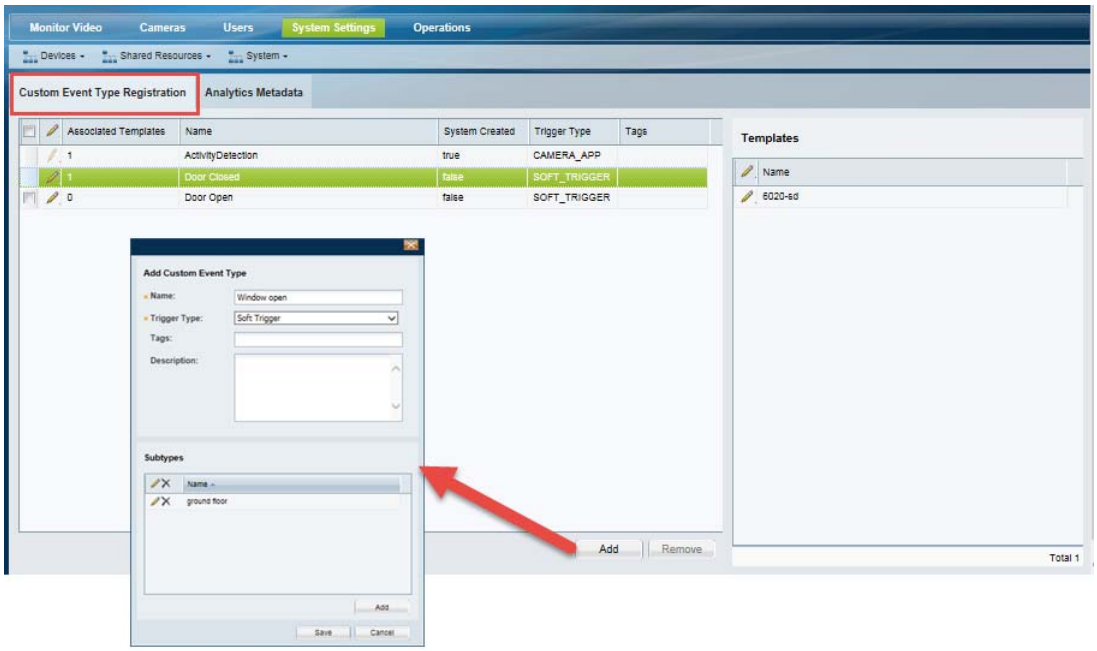
Creating Custom Event Types and Sub Types

Select **System Settings** > **Custom Data Management** to view and edit event types that can be selected using Advanced Events.

Click the **Custom Event Type Registration** tab (Figure 13-5) to view or modify the following event types:

- Soft Trigger— Create, update, or delete Soft Trigger event types and sub types.
  - Click **Add** to create new Soft Trigger entries.
  - Under Subtypes, click **Add** to create a subtype for the soft trigger. Click the icon to edit existing entries.
  - See Configuring Soft Triggers, page 13-12 for more information.
- Camera Apps—View the event types that are added to Cisco VSM when a camera app is uploaded to the Cisco VSM Operations Manager (if the camera app has a custom event type).
  - Camera App entries cannot be revised or deleted.
  - See Managing Camera Apps, page 14-1 for more information.

Figure 13-5 Custom Event Type Management



Tip Select an entry in the left pane to view a list of the templates where the event type is used.

Managing Camera Apps

Camera apps allow you to extend the functionality of cameras so they can also perform analytics and other functions (in addition to sending raw video and audio). Although camera apps can be installed directly on the camera, you can also use the Cisco Video Surveillance Operations Manager (release 7.6 and higher) to install and manage the apps on multiple cameras, and to configure actions triggered by camera app events.

Note Use the camera interface to configure application-specific features and settings. See the camera or camera app documentation for more information.

Refer to the following topics to manage camera apps using the Operations Manager:

Prerequisites

Before you begin, review the following topics to ensure the requires licenses, app files, firmware, and other requirements are met. You must complete these prerequisites before you can install and activate camera apps using Cisco VSM.

Requirements

Table 14-1 Camera App Requirements for Use With Cisco Video Surveillance

Requirements	Requirement Complete? (✓)
At least one camera that supports camera apps must be installed on the network and added to Cisco VSM. • See the "IP Cameras That Support Apps" section on page 14-5.	❑
The camera firmware must support camera apps. • See the "IP Cameras That Support Apps" section on page 14-5.	❑
Obtain and install the app license file. The appropriate license must be installed in Cisco VSM Operations Manager before the app is enabled on the camera template. • See the "Obtaining and Installing App Licenses" section on page 14-6. • If the app is free or does not require a license, this requirement does not apply.	❑

Table 14-1 Camera App Requirements for Use With Cisco Video Surveillance (continued)

Requirements	Requirement Complete? (✓)
Obtain the app file. The app file is uploaded to the Cisco VSM Operations Manager (and then installed on the camera(s) and enabled in the camera template). See the following for more information: • "Obtaining Cisco Apps" section on page 14-6. You must have a valid service contract and Cisco.com account to obtain an app file. • "Obtaining Third-Party Apps" section on page 14-7. Refer to the app provider documentation or website for instructions to download the app.	❑
Requirements to enable a camera app on a camera template: **Note** Enabling a camera app on a template also enables the app on the cameras associated with that template. The camera, however, must meet the following requirements, or the app will not be enabled on the device. • The camera model must support the app. For example, cameras that do not have microphones do not support audio-only camera apps. • The camera must have the minimum supported firmware version (or higher). See IP Cameras That Support Apps, page 14-5. • The app must be installed on the camera. • Only one video app and one audio app can be enabled on the template. • Audio must be supported by the camera model, if an audio app is enabled on the template. • The secondary video stream must be Off in the camera template. • Before the camera app is installed on a camera, the application SDK version compatibility check must pass. This means that the application SDK major version must be equal to the camera SDK version (the SDK version number is X.Y.Z, where X – is the major version number). This check is performed automatically.	❑

Supported Apps

Cisco offers the following apps for supported IP cameras. To obtain an app, contact your Cisco representative.

Table 14-2 Supported Camera Apps

Camera App	Description
Audio Analytics app	Enables an IP camera to trigger events when it detects certain sound patterns. For example, the Audio Analytics apps include the following: • Aggression— Detects aggressive speech or shouting • Car Alarm— Detects standard car alarms • Glass Break—Detects standard window glass braking • Gunshot—Detects a variety of firearms being discharged. • Demo—Lets you test the response of the Audio Analytics apps to an aggression, car alarm, glass breaking, or gunshot sound.
intuVision Video Analytics apps	Enables an IP camera to trigger events when it detects activities or behaviors that match predefined rules. For example, The intuVision Video Analytics apps include the following: • Activity—Detects moving objects within a area that is configured in the camera view • LineCrossing—Detects moving objects that cross a line that is configured in the camera view • ObjectTaken—Detects a marked object in the camera view being removed from its location • WrongWay—Detects objects that are moving in the direction of an arrow that is configured in the camera view • ZoneIntrusion—Detects objects that enter an area that is configured in the camera view
Lua app	Enables an IP camera to run scripts that are created in the Lua programming language.
SIP Client app	Lets an IP camera send and receive audio to and from an external SIP client device or the Cisco Interoperability and Collaboration System (Cisco IPICS).

IP Cameras That Support Apps

The following Cisco IP camera models support camera apps.

Table 14-3 Cameras That Support Camera Apps

Camera	Minimum Firmware Version
• CIVS-IPC-2830 • CIVS-IPC-2835 • CIVS-IPC-3421V • CIVS-IPC-3520 • CIVS-IPC-3530 • CIVS-IPC-3535 • CIVS-IPC-6000P • CIVS-IPC-6020 • CIVS-IPC-6030 • CIVS-IPC-6050 • CIVS-IPC-6400 • CIVS-IPC-6400E • CIVS-IPC-6930 • CIVS-IPC-7030 • CIVS-IPC-7030E	2.5.0

Obtaining and Installing App Licenses

If the app requires a license, you must purchase and install the license(s) that support those apps. If you app does not require a license, skip this process.

The license is required to activate the app on a camera. You must have a license for each camera where the app is activated. The app can be uploaded and installed on the camera without a license, but you cannot activate it without the proper license (if the app requires a license).

Refer to the app provider for more information. For example:

Table 14-4 Camera App Licenses

Source	Task
Cisco Licenses	1. Obtain Cisco license part number(s). See Release Notes for Cisco Video Surveillance Manager 2. Obtain the camera app license file. 3. Install the license in Cisco VSM Operations Manager. See Installing Licenses, page 1-26
Third party app providers	1. Refer to the app instructions and requirements to determine if a license is required. 2. Obtain the camera app license file. 3. Install it in Cisco VSM Operations Manager. See Installing Licenses, page 1-26

Obtaining Camera Apps

To install an app, you must first download it to a PC.

- Obtaining Cisco Apps, page 14-6
- Obtaining Third-Party Apps, page 14-7
- Creating Custom Camera Apps, page 14-7

Obtaining Cisco Apps

Camera app files must first be downloaded from the Cisco website to your local system (or on a system that can be accessed from the Operations Manager user interface). The app must then be installed on the camera, and enabled in the camera template.

For Cisco apps, complete the following steps to obtain the app(s). You must have a valid service contract and Cisco.com account to obtain an app file. For more information, contact your Cisco representative.

Procedure

Step 1 Open a web browser and go to the Cisco Video Surveillance IP Cameras software download page.

Step 2 Click the link for an IP camera series that supports apps (see IP Cameras That Support Apps, page 14-5).

For example: **Cisco Video Surveillance 7000 Series IP Cameras**

Step 3 Click your IP camera model in the list that appears on the right.

For example: **Cisco Video Surveillance 7030 IP Camera**.

Step 4 Click the **IP Camera Applications and Utilities** link near the top of the page.

Step 5 Click **Download** next to the app file that you want to obtain.

For example: **Cisco Camera LUA Application** *version*.

Step 6 In the Log In and Service Contract Required dialog box, click the **Login** button.

Step 7 In the Log In page, enter your Cisco.com user name and password, then click the **Log In** button.

Step 8 In the End User License Agreement dialog box, click the **Cisco End User License Agreement** link to review the agreement, then click the **Accept License Agreement** button to continue.

Step 9 Follow the on-screen prompts to save the license file to your local system or to a system that can be accessed from the IP camera user interface.

Obtaining Third-Party Apps

For third-party apps, refer to the app provider documentation or website for instructions to download the app.

The app must be installed on the camera, and enabled in the camera template.

Creating Custom Camera Apps

To create custom application that runs on a camera and triggers a Cisco VSM event, refer to the following:

- The camera software development kit (SDK) for your camera model.
- The *Cisco Video Surveillance API Programming Guide*—Available on the Cisco Developer Network (CDN), or see your Cisco support representative for more information.

The camera app should include a Camera App custom event type that is added to Cisco VSM Advanced Events when the app is added to Cisco VSM.

See the following for more information:

- Using Advanced Events to Trigger Actions, page 13-7
- Creating Custom Event Types and Sub Types, page 13-15

Managing Camera Apps Using the Operations Manager

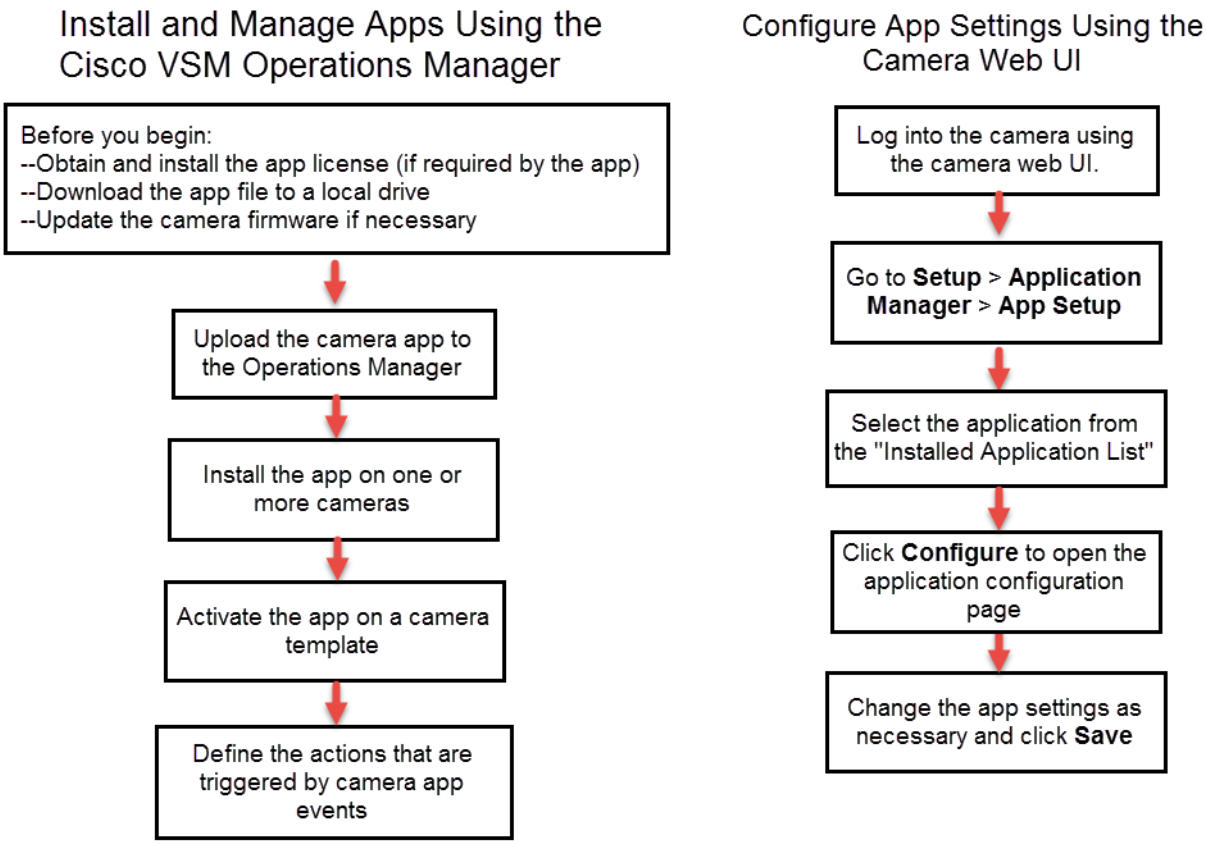
To configure camera apps, use the Cisco VSM Operations Manager to install and manage the apps on multiple cameras. Use the camera's user interface to configure the application-specific settings.

Review the following topics for more information:

Overview

To configure camera apps, use the Cisco VSM Operations Manager to install and manage the apps on multiple cameras. Use the camera web-based user interface to configure the application-specific settings (Figure 14-1).

Figure 14-1 Installing and Configuring Camera Apps



Using the Camera Web Interface to Define Application Settings

The camera's browser-based user interface can be used to install and manage apps on the camera, and to configure the application-specific settings. After the camera is added to Cisco VSM, however, the camera UI is used only to configure the app. Apps are installed and managed using the Operations Manager.

Related Information

- Cisco IP Camera Apps Reference Guide—describes how to configure the application-specific settings for supported apps, and how to install and manage camera apps using the camera web user interface, if the camera has not been added to Cisco VSM.
- Camera documentation—see the documentation for the camera model for device installation and management information.

Procedure

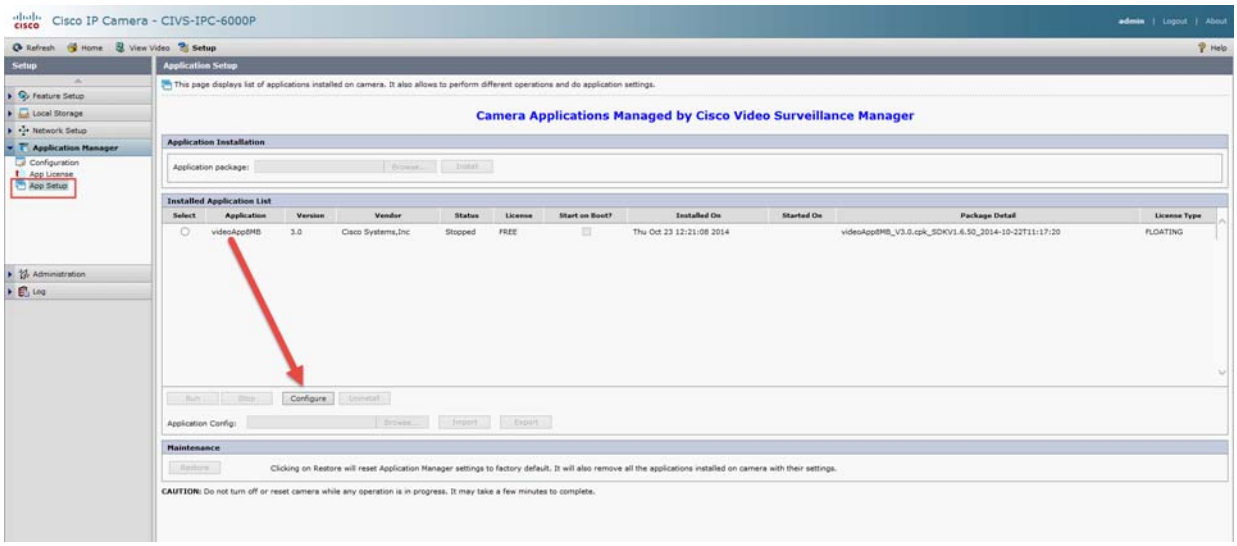
Use the following summary to access the application-specific settings on a camera that supports apps. See the Cisco IP Camera Apps Reference Guide for more information.

Step 1 Log into the camera using camera web UI.

Step 2 Go to **Setup** > **Application Manager** > **App Setup** (Figure 14-2).

Tip The **Application Manager** pages allow you to install or uninstall an app license, camera application, and start or stop an application. These features are disabled if the camera is added to Cisco VSM (use the Operations Manager to manage the camera's apps).

Figure 14-2 Camera Web UI for App Configuration



Step 3 Select the application from the Installed Application List.

Step 4 Click **Configure** to change the application settings. These settings are different for each application, and can only be configured using the camera web user interface.

Step 5 Change the app settings as necessary and click **Save**.

Camera App Status When Cameras are Added to Cisco VSM

When a camera is added to Cisco VSM, the Operations Manager takes over app management for the device. The application management pages on the camera's user interface become read-only (Figure 14-2). You cannot use the camera's interface to install, uninstall, start, or stop camera apps. Use the Operations Manager instead.

The status of the camera depends on the following:

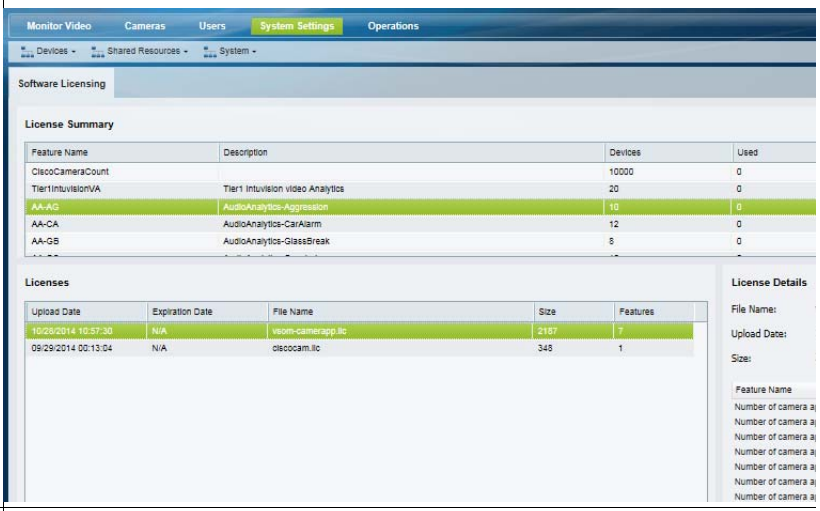
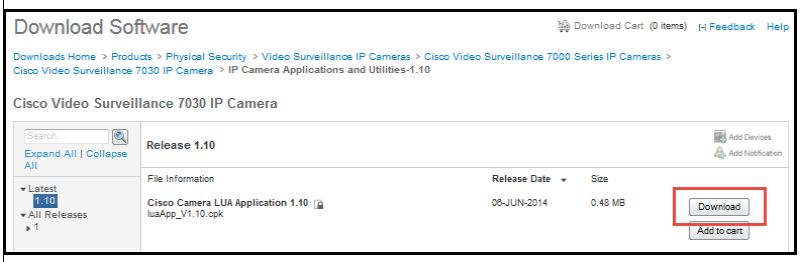
- If camera apps are already running on the camera when the device is added to the Operations Manager:
  - If the app is enabled on the Operations Manager camera template, then the app will remain enabled and running in Cisco VSM.
  - If the app is *not* enabled on the Operations Manager camera template, the app is stopped and must be enabled using the Operations Manager. See Managing Camera Apps Using the Operations Manager, page 14-8 and Enabling an App When the App is Not Installed, page 14-24.
- If the camera application was previously uploaded to the Operations Manager, then the camera status will be *Enabled:OK*.
- If the camera app is not uploaded to the Operations Manager, then the camera status will be *Critical*.

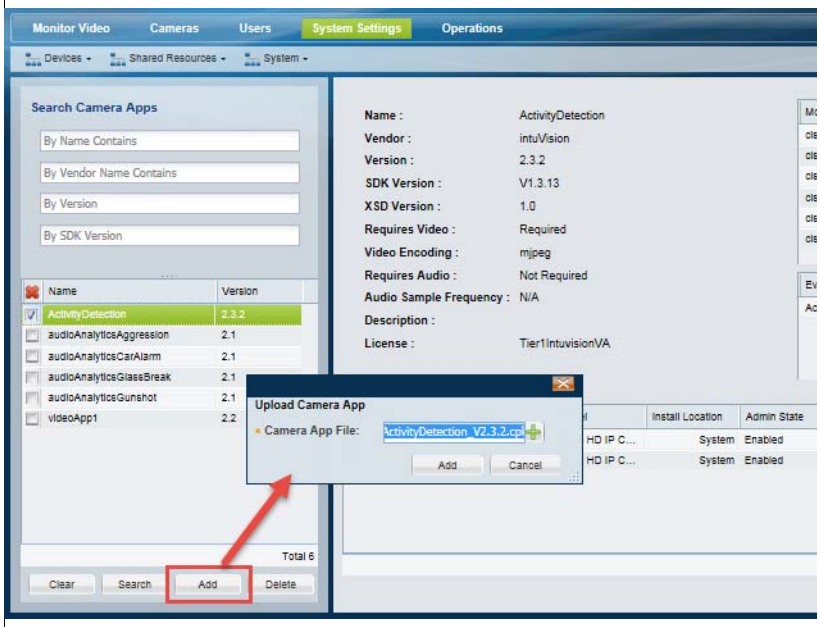
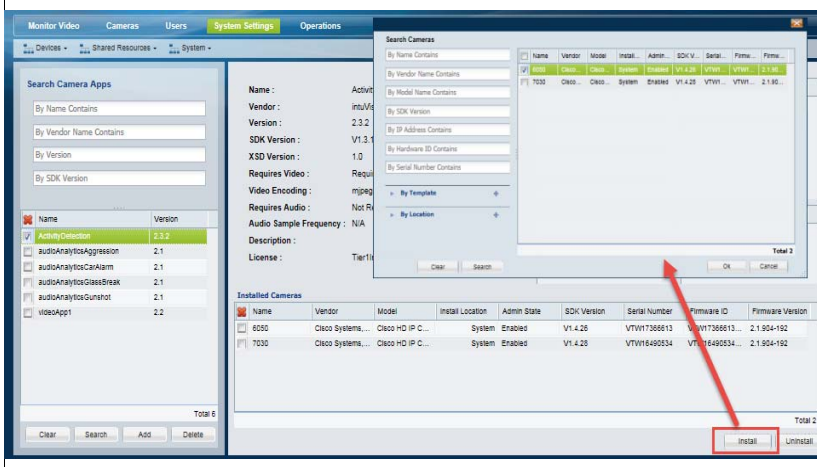
See Viewing App Logs and Status, page 14-17 for more information.

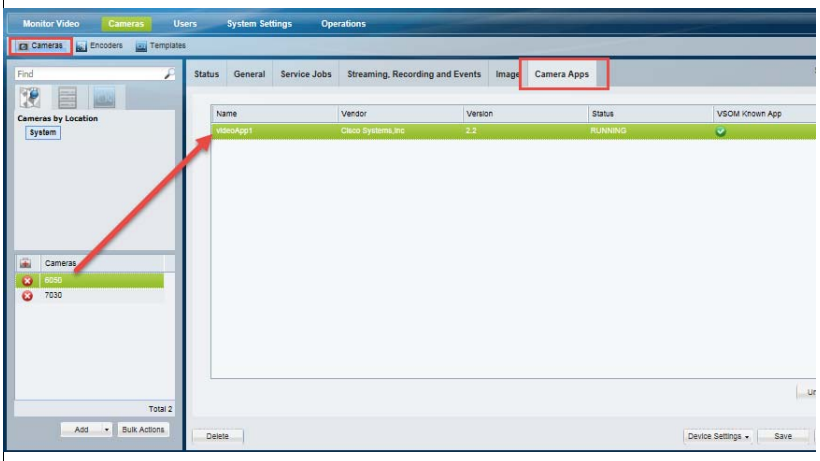
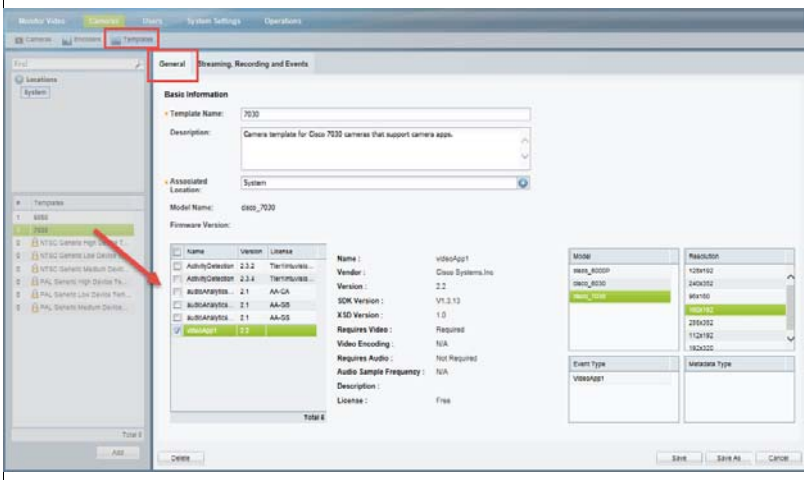
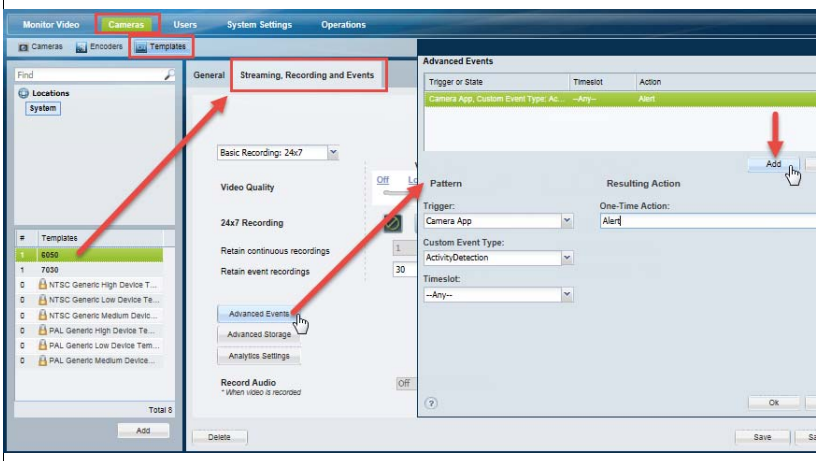
Summary Steps

Summary Steps

Review the following high-level steps to install and configure camera apps using Cisco VSM.

	Task	Example
Step 1	Obtain the camera app license file and install it in Cisco VSM Operations Manager, if required by the app. See Obtaining and Installing App Licenses, page 14-6.	
Step 2	Obtain the camera app file. See Obtaining Camera Apps, page 14-6.	

	Task	Example
Step 3	Upload the camera app to the Operations Manager.	
Step 4	Install the app on one or more cameras. **Note** Camera apps are inactive until activated on the camera template.	

	Task	Example
Step 5	Verify that the app is installed on the camera.	
Step 6	Enable the app on the camera template. This enables the app on all cameras assigned to that template.	
Step 7	Configure Advanced Events in the camera template to trigger an action when a Camera App event occurs.	

Detailed Steps

The following procedure provides additional details to install and configure camera apps using Cisco VSM.

Procedure

Step 1 Verify that all of the requirements are met.

See Requirements, page 14-2. For example, the camera firmware must support camera apps.

Step 2 Obtain the camera app license file and install it in Cisco VSM Operations Manager, if required by the app.

- You must have enough licenses to activate the camera app (you can upload and install the license, but you cannot activate it without the proper license, if required).
- See Obtaining and Installing App Licenses, page 14-6.

Step 3 Obtain the camera app file.

See Obtaining Camera Apps, page 14-6.

Step 4 Upload the camera app to the Operations Manager (Figure 14-3).

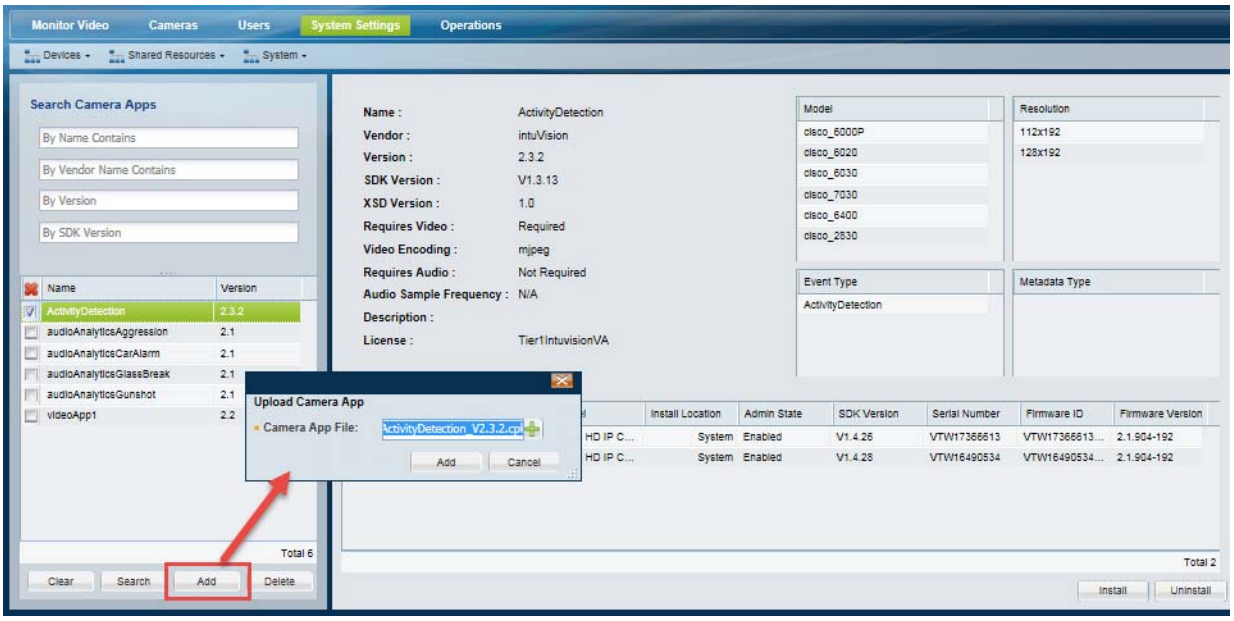
a. Select **System Settings > Camera Apps**.

b. Click **Add**.

c. Click the icon and select the camera app file from a local or network drive.

d. Click **Add**.

Figure 14-3 Uploading Camera Apps



Step 5 Install the app on one or more cameras (Figure 14-4).

Camera apps are inactive until activated on the camera template.

a. Click **Install**.

b. (Optional) Use the search filters to narrow the list of cameras.

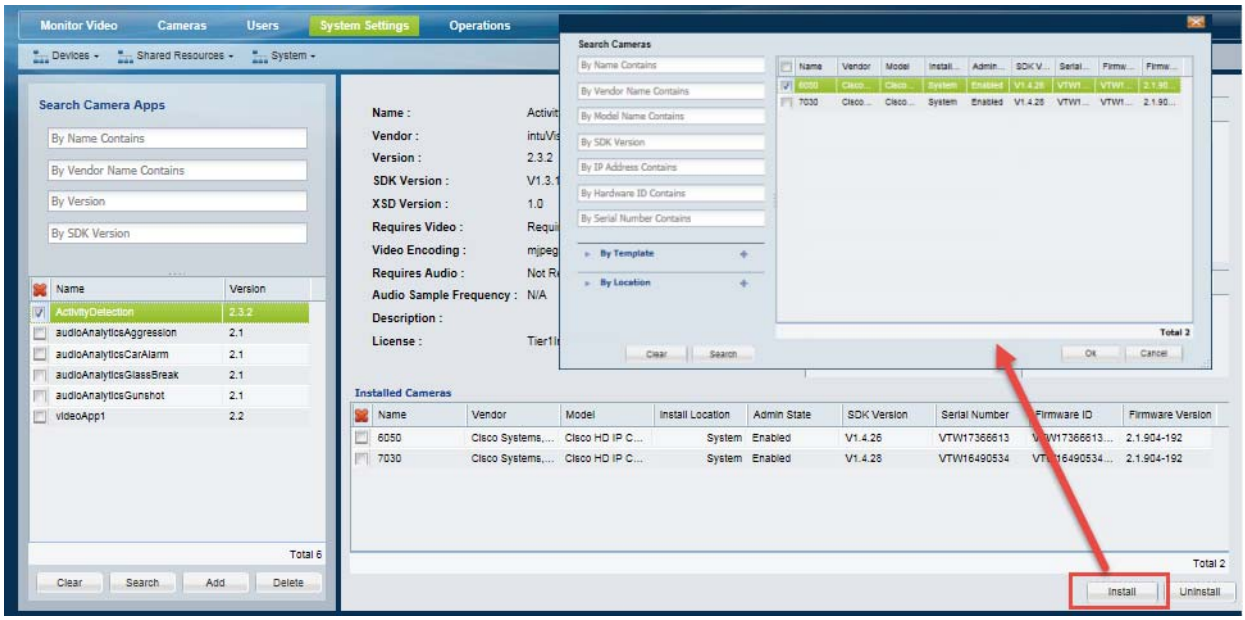
For example, display only for cameras by name, location or template.

c. Select the box next to one or more cameras.

d. Click **OK**.

e. Wait for the app to be installed on the camera.

Figure 14-4 Installing Apps on a Camera



Step 6 (Optional) Verify that the app is installed on the camera. See the Viewing the Apps Installed on a Camera, page 14-18

Step 7 Enable the app on the camera template (Figure 14-5).

Note Enabling a camera app on a template also enables the app on the cameras associated with that template. The camera, however, must meet certain requirements, or the app will not be enabled on the device. See Requirements, page 14-2: "Requirements to enable a camera app on a camera template".

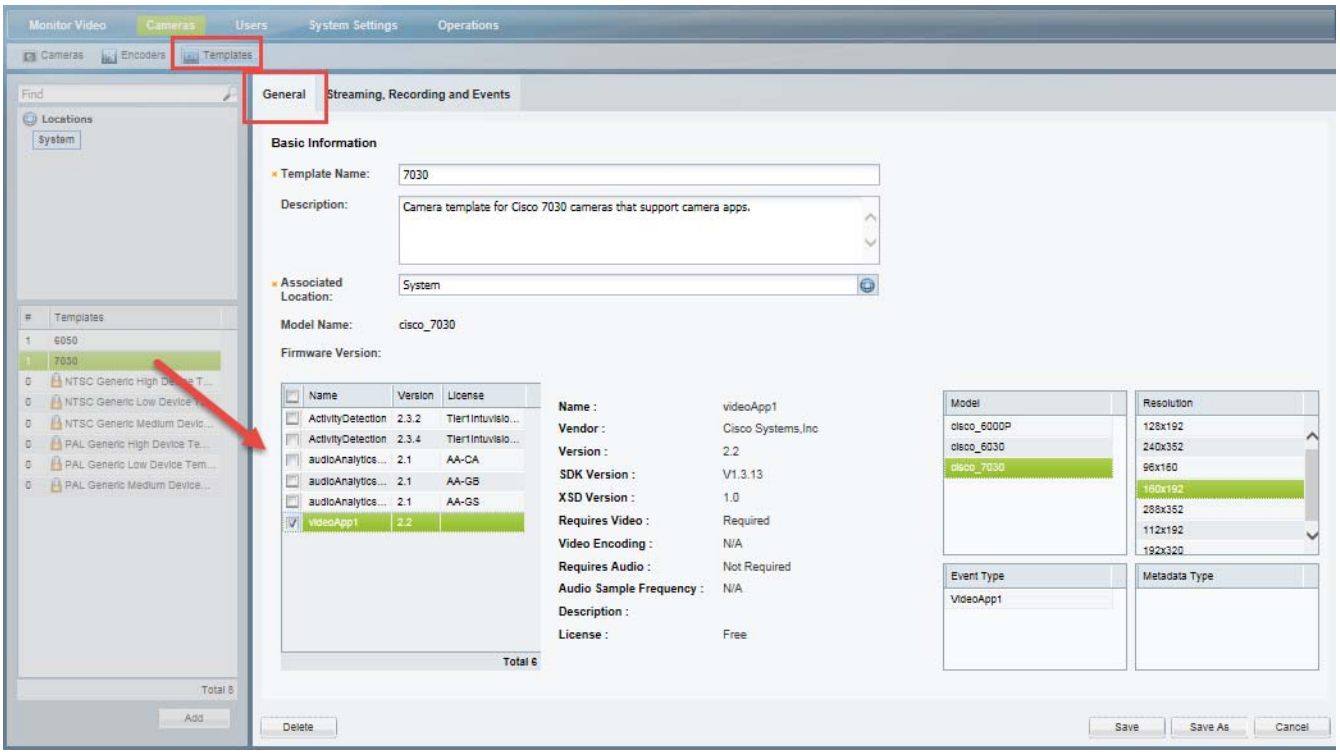
a. From the **Cameras** page, click **Templates**.

b. Select a template from the list.

c. From the **General** tab, select one or more of the camera apps that were added to the system (see Step 5).

d. Click **Save**.

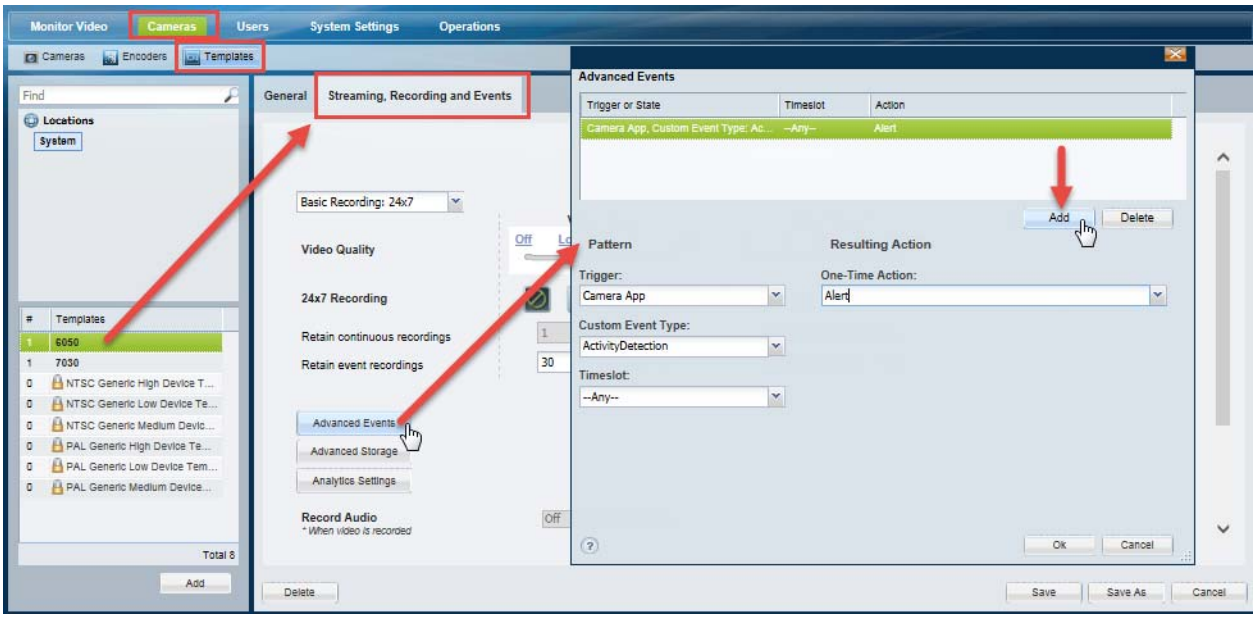
Figure 14-5 Enabling Camera Apps on a Camera Template



Step 8 Configure the Advanced Events for the camera app (Figure 14-6).

When a camera app event occurs, a resulting action can be triggered. For example, a custom camera application could be added to trigger an event when a certain color appears in the video frame. See Using Advanced Events to Trigger Actions, page 13-7.

Figure 14-6 Defining Actions for Camera App Events



a. From the **Cameras** page, click **Templates** and click the **Streaming, Recording and Events** tab.

b. Select **Advanced Events**.

c. Click **Add** to create an entry. You can create multiple entries for different camera apps, or for different types of events available on a single camera app.

d. Define the *Pattern*:

Trigger	Select **Camera App**.
Custom Event Type	(Optional) A camera app event that will trigger the action. For example: ActivityDetection. • If a Custom Event Type is *not* selected, the events generated by any camera app on the camera will trigger the selected action. • If a Custom Event Type is selected, the selected action will be performed only for the events triggered that camera app. **Tip** Select **System Settings** > **Custom Data Management** > **Custom Event Type Registration** to view the Camera App events available on the system. Camera App events are added when the camera app is uploaded to Cisco VSM.
Subtype	(Optional) If available on the app, select the optional event sub-type. Some apps can have multiple event types for different kinds of events. Select the event type that should trigger the action.
Timeslot	Select a *Timeslot* when the event should trigger an action. See the "Defining Schedules" section on page 11-1 to create timeslots.

e. Select a *Resulting Action* for the event.

See Table 13-4 of the "Trigger and Action Descriptions" section on page 13-9 for descriptions of the available actions. For example, when the event occurs, the camera can record for some time, move to a PTZ preset position, or other actions.

f. Click **OK** to save the changes and enable the advanced event settings.

g. (Optional) Repeat these steps to create additional events and actions for the camera event, if necessary.

h. (Optional) View the events triggered by the camera app. See Viewing the Camera Events Caused by a Camera App, page 14-23.

Viewing App Logs and Status

Refer to the following topics to view information about the camera apps installed and activated on the cameras in your deployment, and to identify and resolve camera app errors.

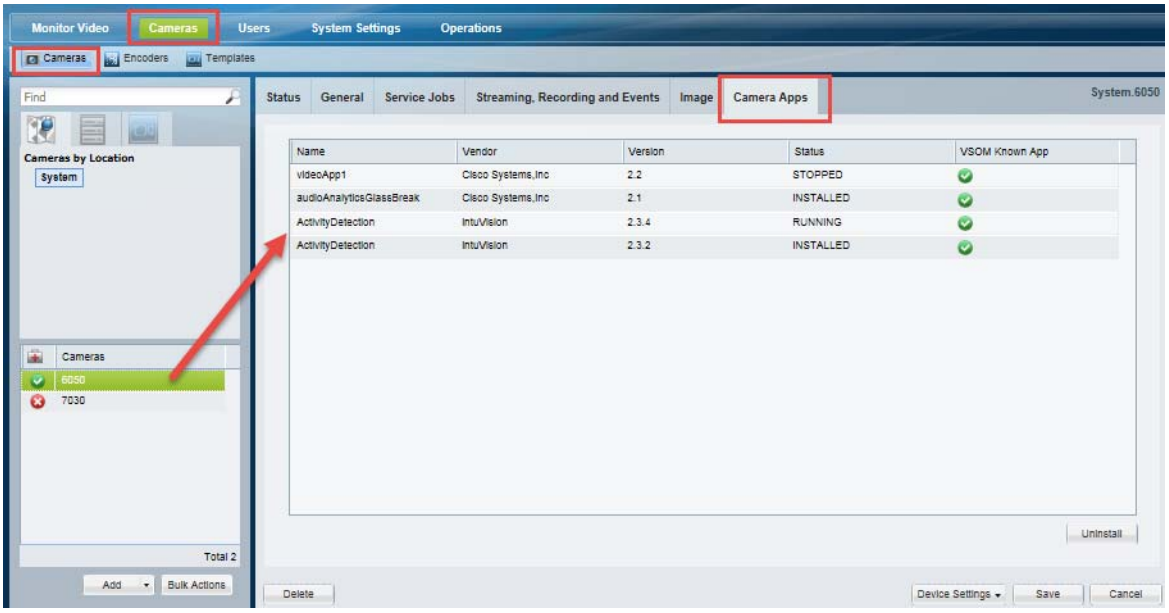
- Camera App Status When Cameras are Added to Cisco VSM, page 14-10
- Viewing the Apps Installed on a Camera, page 14-18
- Viewing the Apps that are Enabled on a Template, page 14-19
- Viewing the Camera App Jobs for a Specific Camera, page 14-20

- Viewing the Camera App Error Log for a Specific Camera, page 14-21
- Viewing the Camera Events Caused by a Camera App, page 14-23

Viewing the Apps Installed on a Camera

Use the camera configuration page to view all of the apps that are installed on a camera (Figure 14-7). This page also shows if the app is enabled. You can uninstall an app if it is already disabled. But you cannot disable an app from this page.

Figure 14-7 Viewing the Apps Installed on a Camera



Procedure

Step 1 Select **Cameras**.

Step 2 Select a location and select a camera from the list.

Step 3 Select the **Camera Apps** tab.

Step 4 The apps that are currently installed on the camera are displayed.

Field	Description
Name	The app name.
Vendor	The company that produces or supplies the app.
Version	The app version number. Up to 2 versions of the same app can be installed, but only one can be active (running).

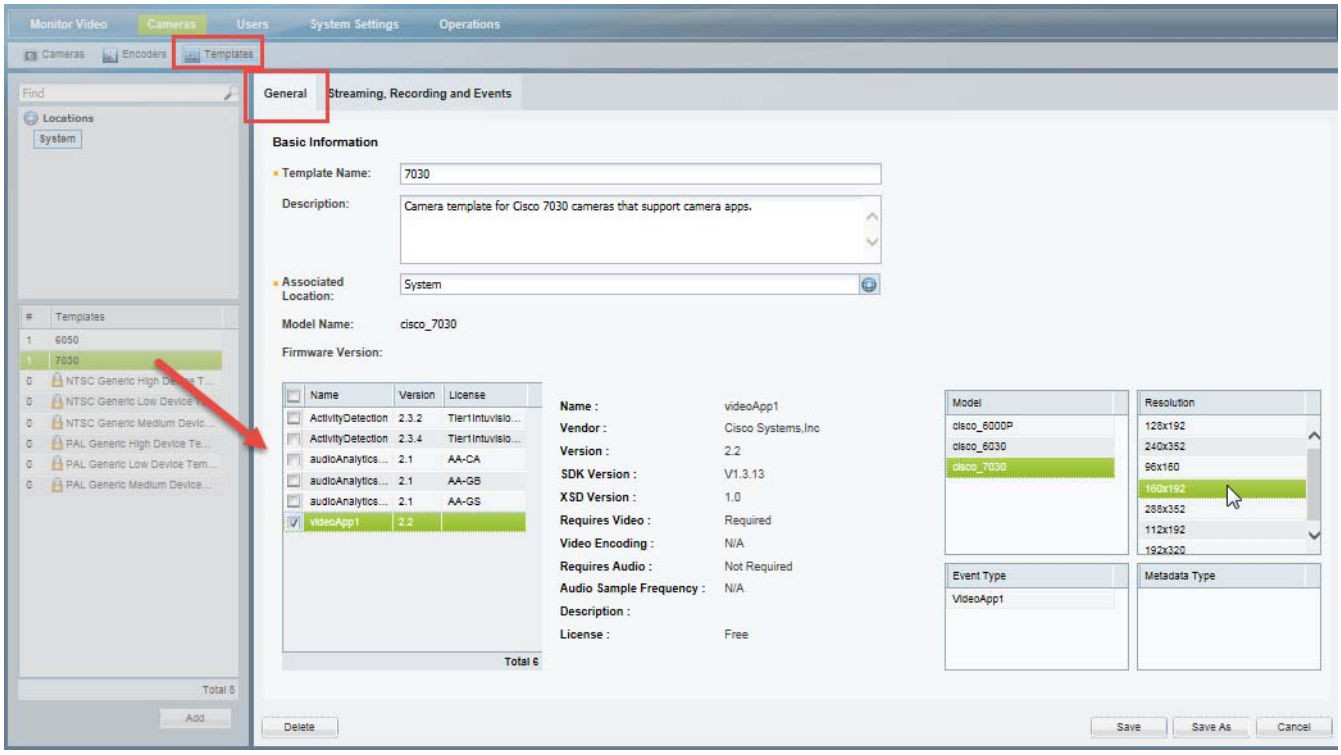
Field	Description
Status	The status of the app on the camera: • Installed—the app is installed on the camera, but is inactive. • Running—the app is active. Apps are activated on the template to which the camera is assigned. • Stopped—The app was previously active on the camera, but was deactivated.
VSOM Known App	Indicates if the app is recognized by the Operations Manager as a valid and supported app.

Step 5 (Optional) To uninstall an app, select the app and click **Uninstall**. The app must be in the Installed or Stopped status. Active apps must first be deactivated.

Viewing the Apps that are Enabled on a Template

Open the template configuration page and select a template name to view the camera apps enabled on that template (Figure 14-8).

Figure 14-8 Camera Apps Enabled on a Template

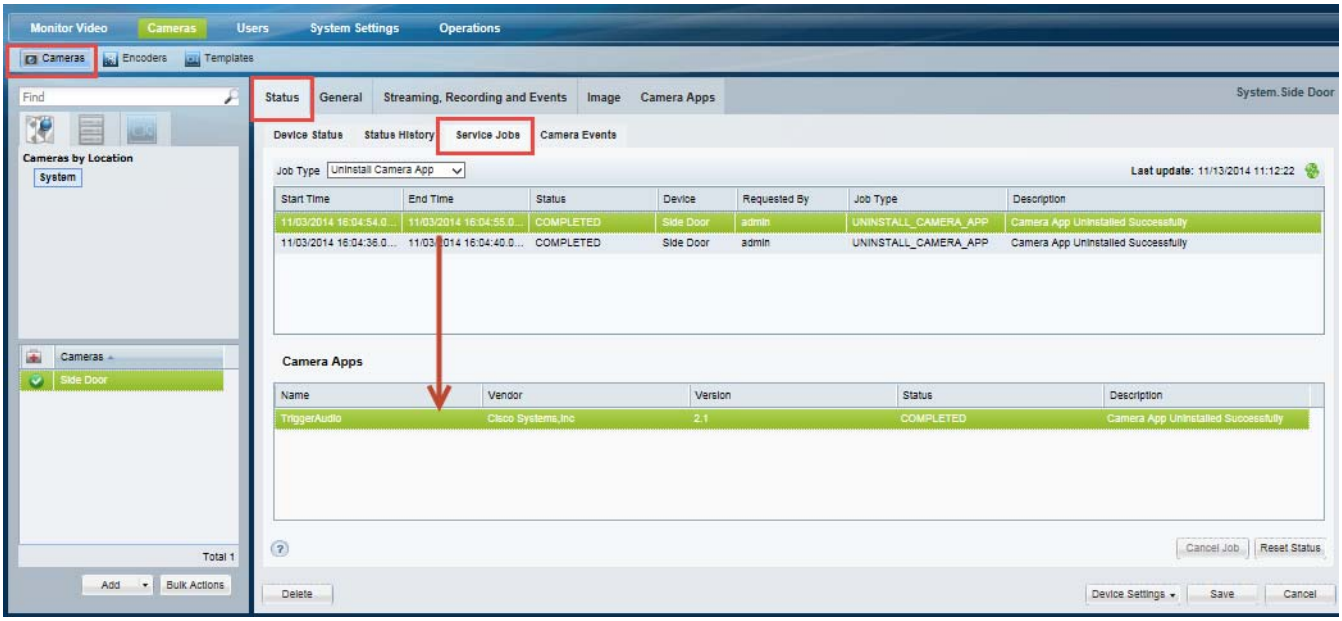


Note Enabling a camera app on a template also enables the app on the cameras associated with that template. The camera, however, must meet certain requirements, or the app will not be enabled on the device. See Requirements, page 14-2: "Requirements to enable a camera app on a camera template".

Viewing the Camera App Jobs for a Specific Camera

Use the Service Jobs tab in the camera status page to view the camera app tasks performed on a camera. For example, you can view a history of the apps that were installed, uninstalled, activated or deactivated (Figure 14-9).

Figure 14-9 Service Jobs: View Camera Apps Task History



Procedure

Step 1 Select **Cameras**.

Step 2 Select a location and select a camera from the list.

Step 3 Select **Status** and then the **Service Jobs** tab.

Step 4 Select a **Job Type**. For example:

- **Install Camera App**
- **Uninstall Camera App**
- **Enable Camera App**
- **Disable Camera App**

Step 5 Click an entry to view additional details about the job.

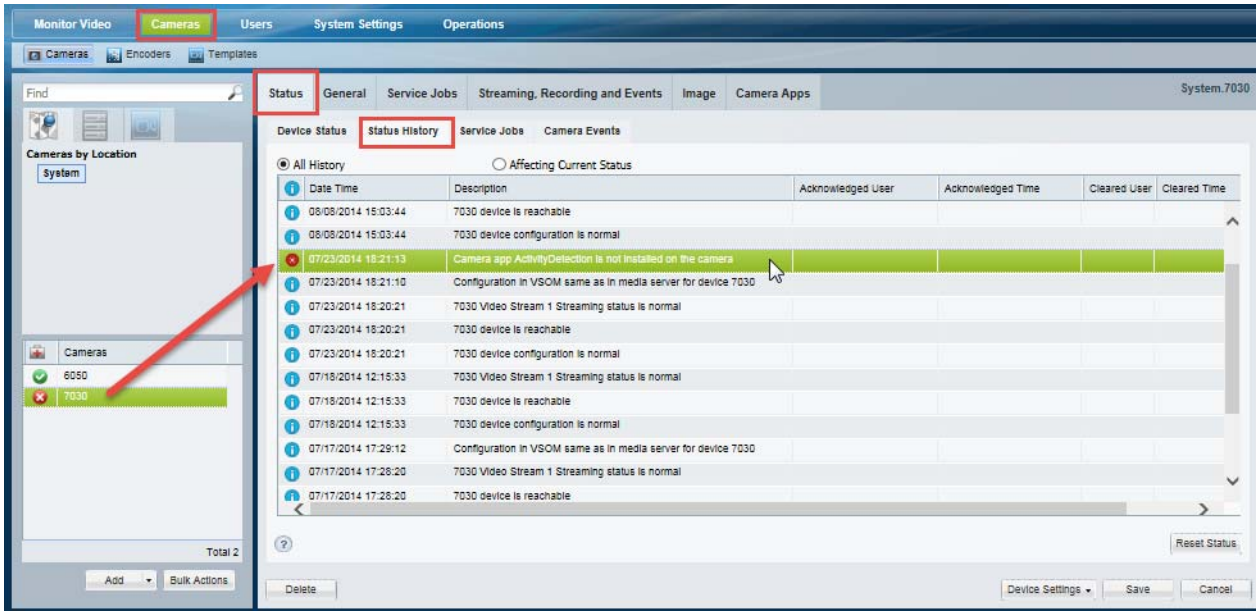
Name	The app name.
Vendor	The company that produces or supplies the app.
Version	The app version number.
Status	The job status. See Understanding Job Status, page 19-31 for more information.
Description	A summary of the job results. For example, the job success or failure.

Viewing the Camera App Error Log for a Specific Camera

Use the Status History tab in the camera configuration page to view the camera app errors on a camera. This page displays the problems that may have occurred in the camera app configuration, allowing you to resolve the problem. For example, in Figure 14-10 a camera displays a critical error . Open the Status History page to display information about the cause of that error. Click **Affecting Current Status** to display only the errors causing the current problem. Double click an entry for additional information.

Tip The camera status can be impacted when the camera is added to Cisco Video SurveillanceCisco VSM. See Camera App Status When Cameras are Added to Cisco VSM, page 14-10.

Figure 14-10 Camera Status: View Camera Apps Errors



Procedure

Step 1 Select **Cameras**.

Step 2 Select a location and select a camera from the list.

Step 3 Select the **Status** tab.

Step 4 Select the **Status History** tab.

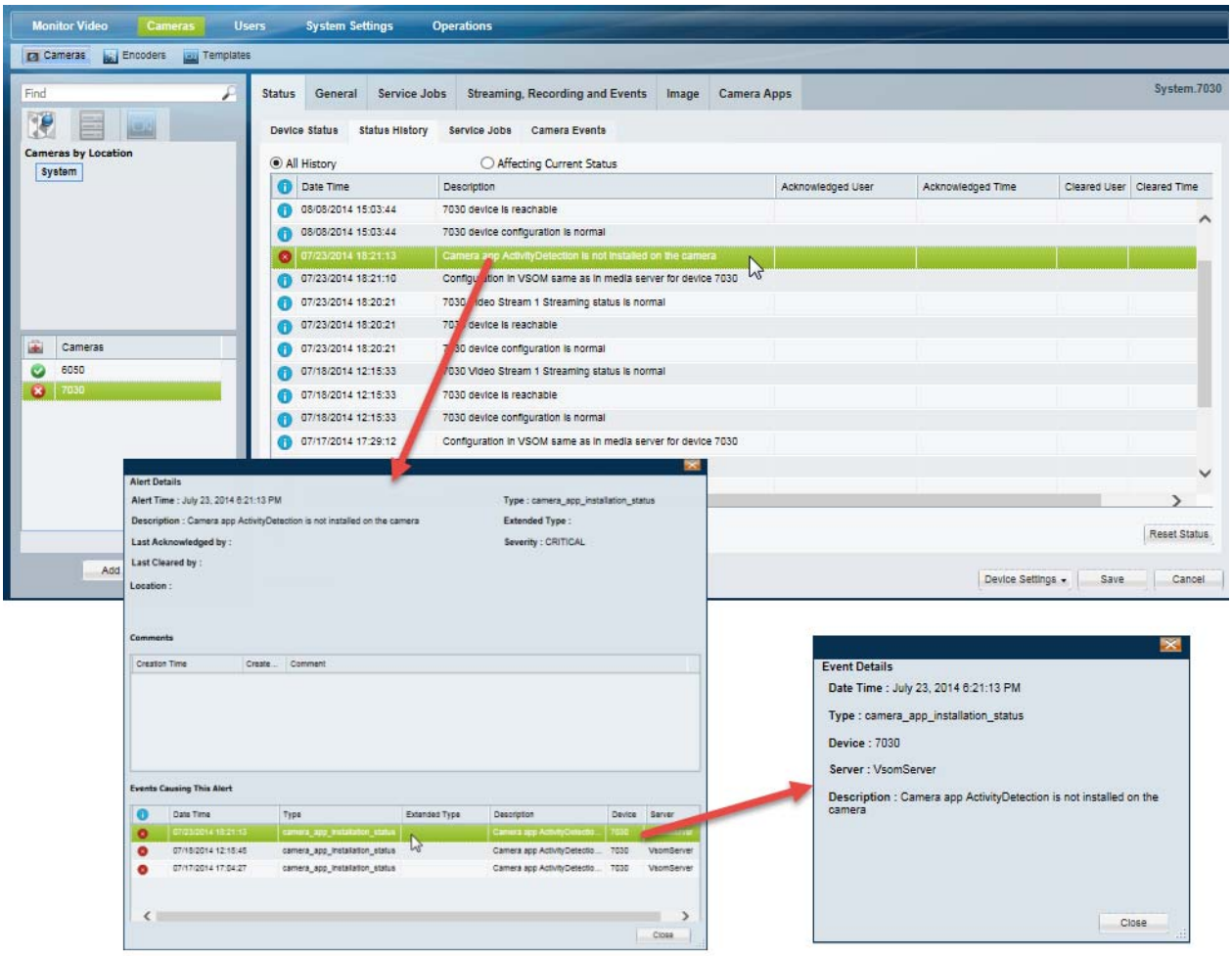
Step 5 Review the issues to locate camera app alerts that display a critical error icon. See Understanding Device Status, page 19-11.

Step 6 (Optional) Click **Affecting Current Status** to display only the errors causing the current problem.

Step 7 (Optional) Double-click an entry to display the alert details (Figure 14-11). Alerts can include multiple events for the same issue. See Understanding Events and Alerts, page 19-2.

Step 8 (Optional) Double-click an event to display the event details. Alerts can include multiple events for the same issue.

Figure 14-11 Camera Status: Viewing Alert and Event Details



Step 9 Use the information to resolve is issue. For example, if a camera is assigned to a template where a camera app is enabled, but the app is not installed on the camera, an error will occur. To resolve the issue, install the appropriate camera app on the camera.

Related Information

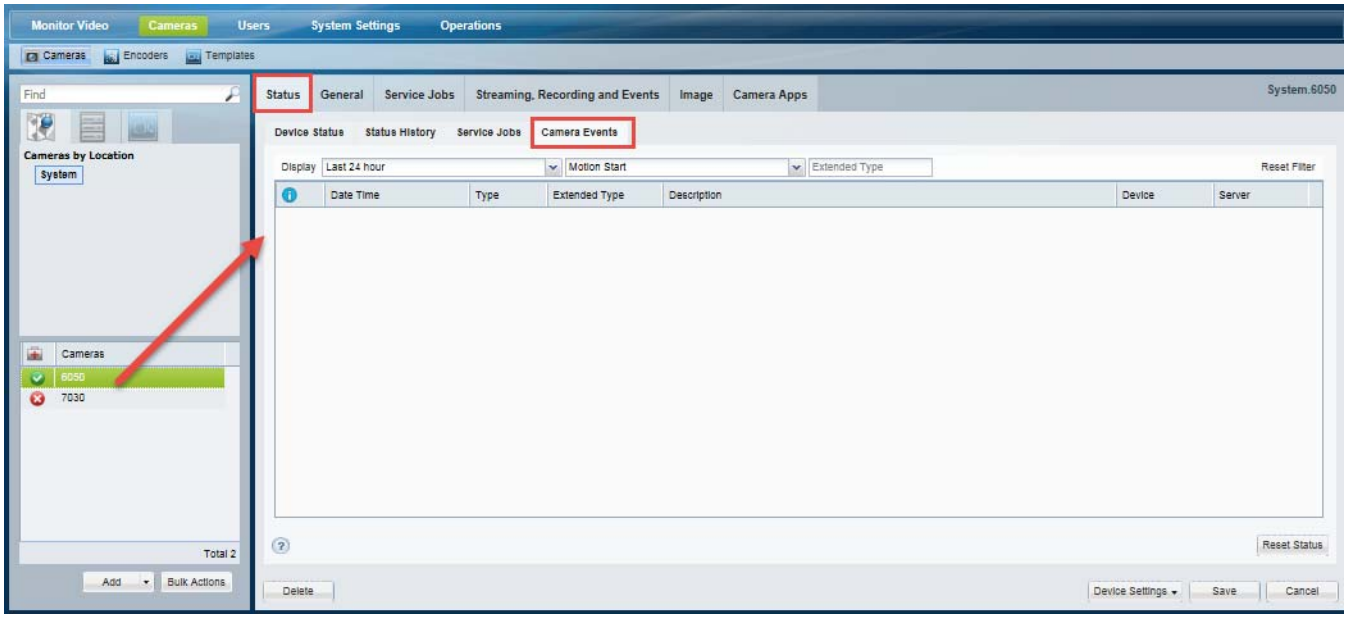
See the following for more information:

- Camera App Status When Cameras are Added to Cisco VSM, page 14-10
- Camera Status, page 10-62
- Device Status: Identifying Issues for a Specific Device, page 19-9
- Understanding Events and Alerts, page 19-2

Viewing the Camera Events Caused by a Camera App

Use the Camera Events tab in the camera configuration page to view the security events that occur on a camera (Figure 14-12). For example, you can view the motion started events caused by a camera app in the past 24 hours, such as camera app events.

Figure 14-12 Camera Events



Procedure

Step 1 Select **Cameras**.

Step 2 Select a location and select a camera from the list.

Step 3 Select the **Status** tab.

Step 4 Select the **Camera Events** tab.

Step 5 Select the time filter, such as **Last 25 hours**. Select **Special Range** to enter a custom time span.

Step 6 Select the event type, such as **Motion Start**. See Trigger and Action Descriptions, page 13-9.

Enabling an App When the App is Not Installed

If you attempt to enable a camera app on a template, the app is not installed on a camera, an error will occur. Install the app on the camera and try again.

Disabling, De-installing and Deleting Apps

You can deactivate apps so they are non-functional, de-install them from the camera hardware, or delete them from the Operations Manager. Refer to the following topics for more information.

- Disabling an App, page 14-24
- Uninstalling an App From a Camera, page 14-25
- Deleting an App from Operations Manager, page 14-27

Disabling an App

To disable a camera app, remove the app from the camera template. The app functionality will be disabled on any cameras assigned to that template (Figure 14-13).

Note The camera app will still be installed on the device, but non-operational unless the camera is assigned to another template where the app is active.

The cameras apps enabled on a template will also be enabled on all cameras assigned to that template. The camera hardware and firmware must support the app features.

Procedure

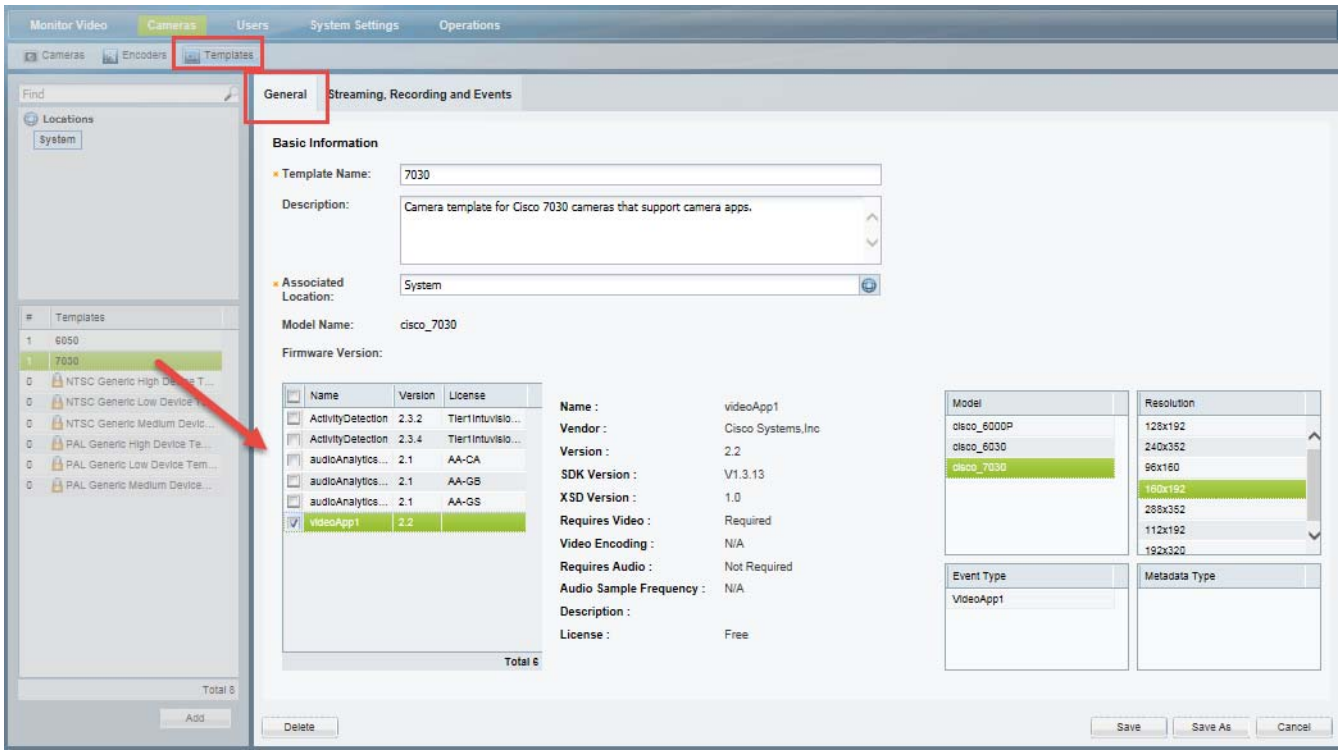
Step 1 From the **Cameras** page, click **Templates**.

Step 2 Select a template from the list.

Step 3 From the **General** tab, deselect the camera apps that you want to deactivate.

Step 4 Click **Save**.

Figure 14-13 Disabling Camera Apps on a Camera Template



Uninstalling an App From a Camera

Uninstalling an app removes the app from the camera hardware. The camera app is still available on Operations Manager and can be re-installed or installed on other cameras.

Note The camera app must be deactivated on the selected cameras before it can be uninstalled.

You can uninstall a camera app from one camera at a time. To uninstall additional apps, repeat the following procedure.

Procedure

Step 1 Deactivate the camera app on the camera template, as described in Disabling an App, page 14-24.

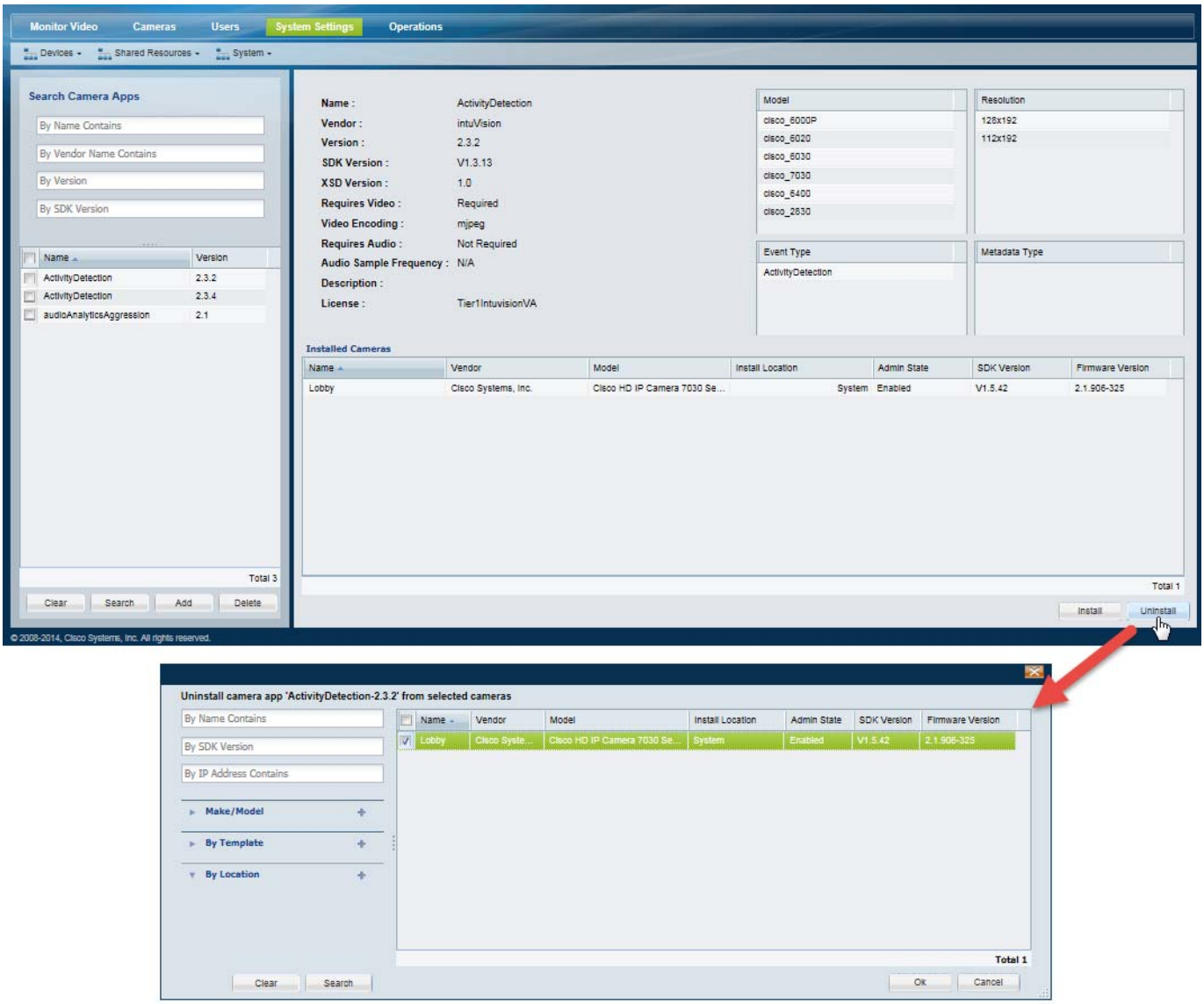
Step 2 Select **System Settings > Camera Apps**.

Step 3 Select a camera app to highlight the app name (Figure 14-14).

The Installed Cameras list displays the cameras where the app is currently installed.

Step 4 Click **Uninstall**.

Figure 14-14 Uninstalling a Camera App



Step 5 In the pop-up window:

- **a.** (Optional) Use the filters to narrow the list cameras. Leave the fields blank to display all cameras.
- **b.** Click **Search**.
- **c.** Select one or more cameras from the list.
- **d.** Click **OK** and **Yes** to verify.

Step 6 Wait for the job to complete.

Step 7 (Optional) Open the camera configuration page and click the **Camera Apps** tab to verify that the app was removed from the camera.

Deleting an App from Operations Manager

Deleting an app removes the app from the Operations Manager. The app will no longer be available for installation or activation on the cameras.

To delete an app, the app must be uninstalled from all cameras. This requires you to first deactivate the camera app on the camera templates.

Procedure

Step 1 Deactivate the camera app from all templates, as described in Disabling an App, page 14-24.

Step 2 Uninstall the camera app from all cameras, as described in Uninstalling an App From a Camera, page 14-25.

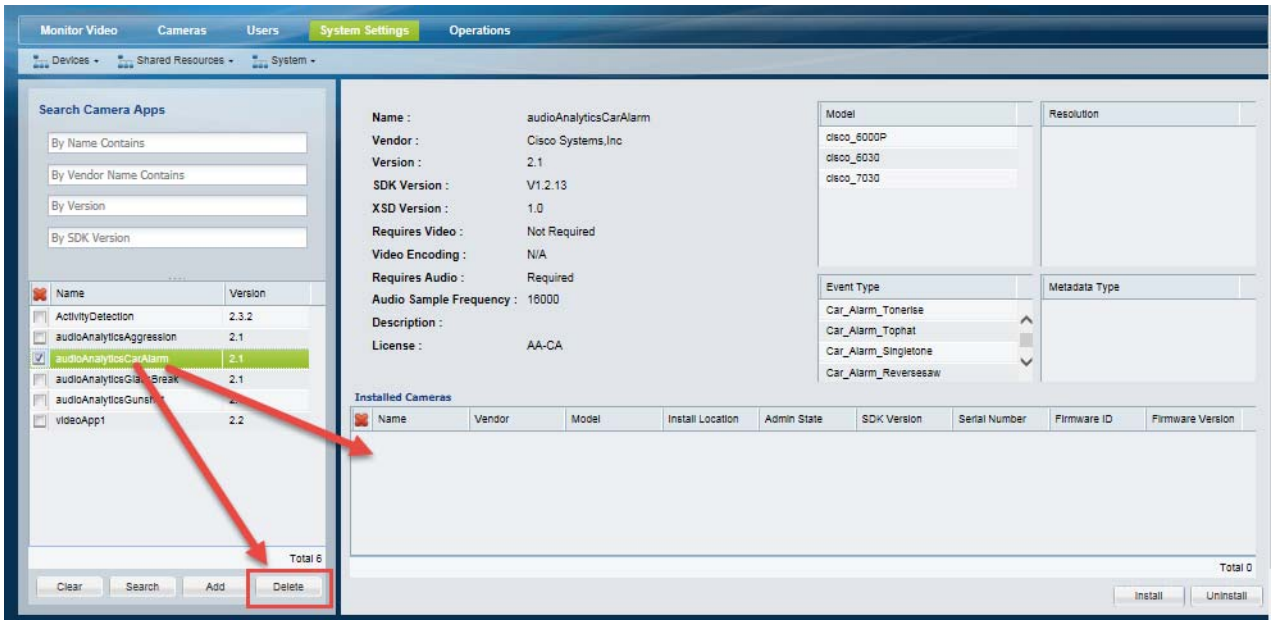
Step 3 Select **System Settings > Camera Apps**.

Step 4 Select one or more apps (Figure 14-15).

Step 5 Verify that there are no cameras listed in the Installed Cameras list.

Step 6 Click **Delete**.

Figure 14-15 Deleting a Camera App



Upgrading Camera Apps

To upgrade a camera app, upload the new version of the app to the Operations Manager. When you activate the new app version on a template, the old version will be deactivated.

Usage Notes

- You can upload multiple versions of the app to the Operations Manager, and install up to 2 versions on the camera, but only one app version can be active on a template or camera.
- When you activate the new version, the old version is automatically uninstalled from the camera.
- Advanced Event configurations must be deleted and re-added. See Configure the Advanced Events for the camera app (Figure 14-6)., page 16.
- The template and event/trigger processing is stopped and restarted during the upgrade process (while the old app is deactivated and uninstalled, and the new app is activated). Event and trigger processing may be delayed or interrupted.
- Up to 2 camera apps can be upgraded at a time (by activating the new versions in the template). Wait for the upgrade to complete before upgrading additional apps.

Procedure

See Detailed Steps, page 14-14 for instructions to perform the following tasks.

Step 1 Upload the new version of the camera app to the Operations Manager.

Multiple app versions can be uploaded to the Operations Manager.

Step 2 Install the new camera app version on a camera.

A maximum of 2 versions of the same app can be installed on a camera.

Step 3 Activate the new app version on a template, as described in Detailed Steps, page 14-14.

When the new camera app version is activated, the old app version is automatically uninstalled on the camera.

Related Documentation

To install and manage camera apps directly on the camera, see the Cisco IP Camera Apps Reference Guide.

Connected Edge Storage (Camera Recording)

Cameras that support on-device storage of video recordings can be used to record video even if the camera does not have communication with the Cisco Video Surveillance system. Once network communication is re-established, the on-camera recordings can be copied to a Media Server.

For example, cameras on buses can save video while away from the bus depot. When the bus returns to the depot and network communication is re-established with Cisco VSM, the recordings can be copied from the camera to the Cisco Media Server. This can occur automatically ("Auto-Merge Recordings"), or an operator can trigger a one-time copy (based on a time range).

Refer to the following topics for more information.

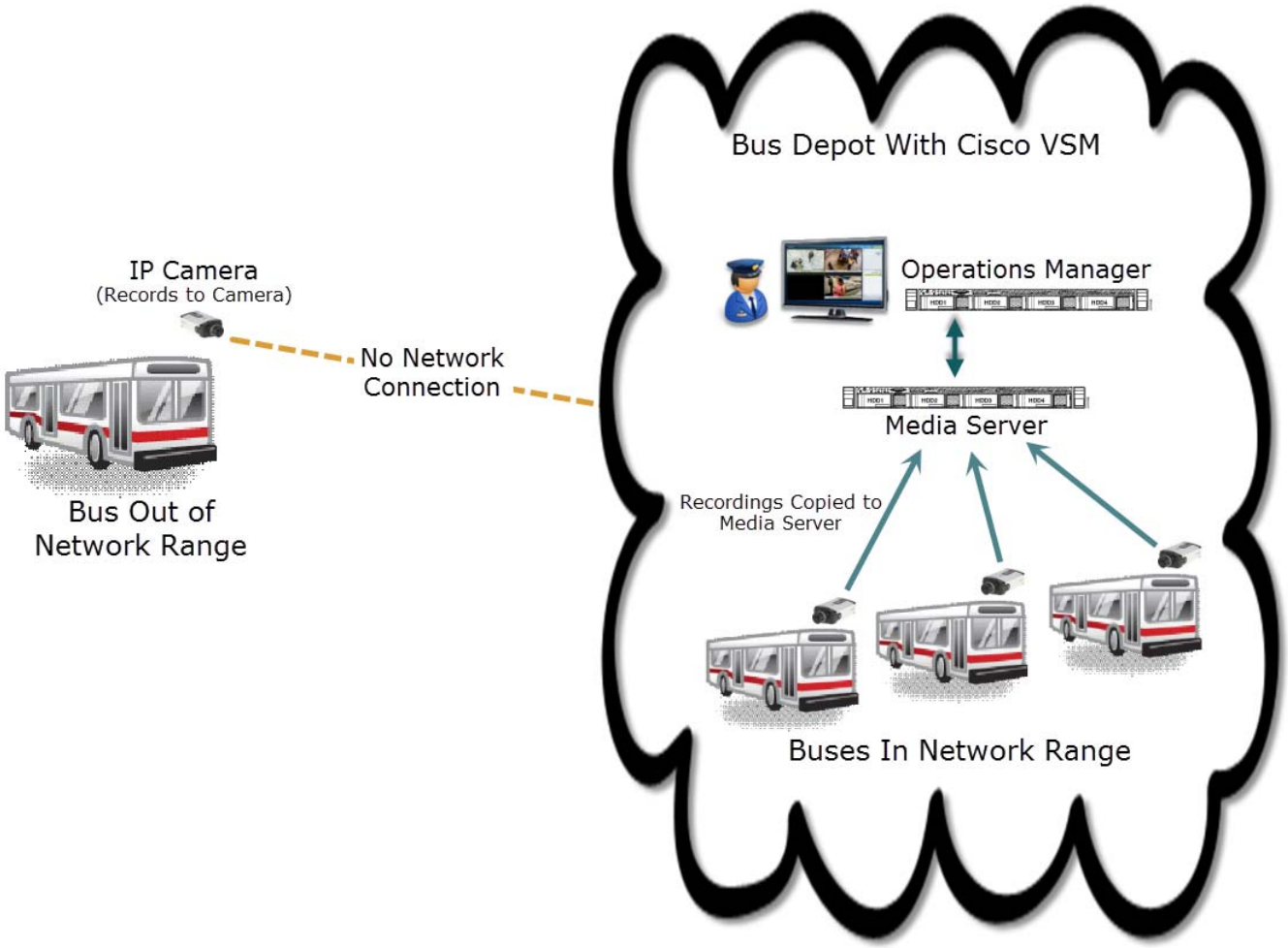
Contents

Overview

Cameras that support on-device video storage can save recordings on the camera, and copy them to the Cisco VSM system at a later time. This feature is typically used when the camera is out of network range while recording.

For example, in Figure 15-1 a bus equipped with an IP (network) camera can save video recordings to the camera even when the bus is transporting passengers. When the bus returns to the depot, and is again in network range, the recordings can be copied to the Media Server that supports the camera. The copy action can be performed automatically when the bus camera rejoins the network, or an operator can manually trigger the copy action using the Operations Manager interface.

Figure 15-1 "Connected Edge Storage": Camera Recording on Device and Copy to a Media Server



Copy Options

Table 15-1 summarizes the options to copy camera recordings:

Table 15-1 Camera Copy Methods

Copy Method	Description	More Information
Automatic "Auto-Merge Recordings"	Automatically copies a continuous recording to the Media Server based on the camera template's recording schedule. After configuration, no user interaction is required. The recordings are copied to the Media Server when camera network communication is re-established.	Auto-Merge Recordings (Automatic Copying), page 15-12
Manual "Copy Now"	Allows a Cisco VSM operator to manually trigger the copy action. The operator selects a specific time-range, and any available video within that range is copied from the camera to the Media Server. You must belong to a user group with *Copy From Edge Storage* permission. See the "Adding Users, User Groups, and Permissions" section on page 4-1 for more information.	Copy Camera Recordings (Manually Triggered), page 15-14

Usage Notes

- When on-camera recording is enabled, video is saved to the camera storage without motion or advanced events. These events are added (post-processed) after the video is copied to the Media Server. Video is recorded on the camera based on the camera template recording schedule. For example, if the camera template schedule specifies recordings from 8 am to 11 am, then only the continuous recording for those times will be recorded on the camera and available to be copied to the Media Server.
- Recorded video is groomed according to the "Retain continuous recordings" camera template setting (see the "Streaming, Recording and Event Settings" section on page 10-48). However, "Gap" video (video that is initially stored only on the camera and later manually or automatically copied to the Media Server) is considered event video, and is retained according to the "Retain event recordings" setting.
  - For example, if the "Retain continuous recordings" setting is 1 day, then video older than one day is automatically groomed (deleted).
  - If the "Retain event recordings" setting is 10 days, then the "gap" video copied from the camera to the Media Server is retained for 10 days. Those portions of the video are only removed if older than 10 days.
- Only recording gaps on the Media Server greater than 5 seconds are filled by the camera recordings. Recording gaps smaller than 5 seconds are not copied.
- One storage copy job is performed per device at a time (a job must finish before a new job can begin). Up to 10 copy jobs can be performed simultaneously.

- When the storage media (such as an SD card) is full on a Cisco camera, the oldest 5 minutes of video is deleted to create space for new video. This "grooming" policy varies for non-Cisco cameras. Refer to the camera documentation for more information. For example, some cameras may stop recording if the recording media is full.
- Select **Device Settings** > **Format SD Card** to reformat an SD card that is installed in the device. You can also reformat or replace the SD cards directly on the camera. See Formatting Camera SD Cards, page 15-5.

Requirements

Table 15-2 Camera Storage Requirements

Requirements	Complete? (✓)
A IP network camera that supports on-device video storage. • See the "Supported IP Cameras (On-Device Storage)" section on page 15-5. • See the camera documentation for more information and instructions to enable device storage and format the SD storage cards installed in the device, if necessary.	❑
The network camera(s) must be installed and configured on the Cisco VSM system, and be in *Enabled: OK* state when in network range. See the following related information: • "Adding and Managing Cameras" section on page 10-1 • "Camera Status" section on page 10-62 • "Adding and Editing Camera Templates" section on page 12-1	❑
The camera NTP setting must be properly configured and the same as the Cisco VSM system clock. See the following related information: • "Understanding NTP Configuration" • NTP Information, page 6-14 • The camera documentation.	❑
HA Requirements: • The Media Server where the recordings are copied must be in the Primary or Redundant state. • Video cannot be copied to a server in the Failover state. See the "Understanding Redundant, Failover, and Long Term Storage Servers" section on page 17-4 for more information.	❑
A Cisco VSM user account that belongs to a User Group with manage permissions for the following: • To enable camera storage and Auto-Merge Recordings (automatic copying): *Manage* permissions for *Templates* is required. • To manually trigger a one-time copy action: *Manage* permissions for *Cameras* is required. See the "Adding Users, User Groups, and Permissions" section on page 4-1 for more information.	❑
Camera recording must be enabled in the Operations Manager camera template. See the "Connected Edge Storage (Enabling Recording On Cameras)" section on page 15-8.	❑

Supported IP Cameras (On-Device Storage)

See the Release Notes for Cisco Video Surveillance Manager for the cameras that support Connected Edge Storage (camera recording) in your release.

Formatting Camera SD Cards

Camera storage (such as an SD card) must by physically installed and formatted so it is available to Cisco VSM.

To reformat the card using Cisco VSM, select the **Device Settings** > **Format SD Card** from the camera configuration page. You can also use camera Bulk Actions to format the SD cards in multiple cameras.

- SD Card Usage Notes, page 15-5
- Formatting the SD Card for a Single Camera, page 15-5
- Formatting the SD Cards in Multiple Cameras (Bulk Actions), page 15-6

SD Card Usage Notes

This formatting process will fail if:

- The SD card is not installed in the camera or is not detected.
- A format is already in progress. Wait for the format to complete.
- Recordings or clips are being downloaded from the camera to Cisco VSM.
- The SD card is not mounted. The card must be unmounted before being removed from a camera and installed in a different camera. If this occurs, use the camera UI to “mount” the card in the new camera. See the camera documentation for more information.
- To view the formatting status, see Service Jobs (Cameras), page 10-65.

Formatting the SD Card for a Single Camera

Procedure

Step 1 Physically install the storage device in the camera.

Refer to the camera documentation for more information. You can also format the storage device using the camera’s interface.

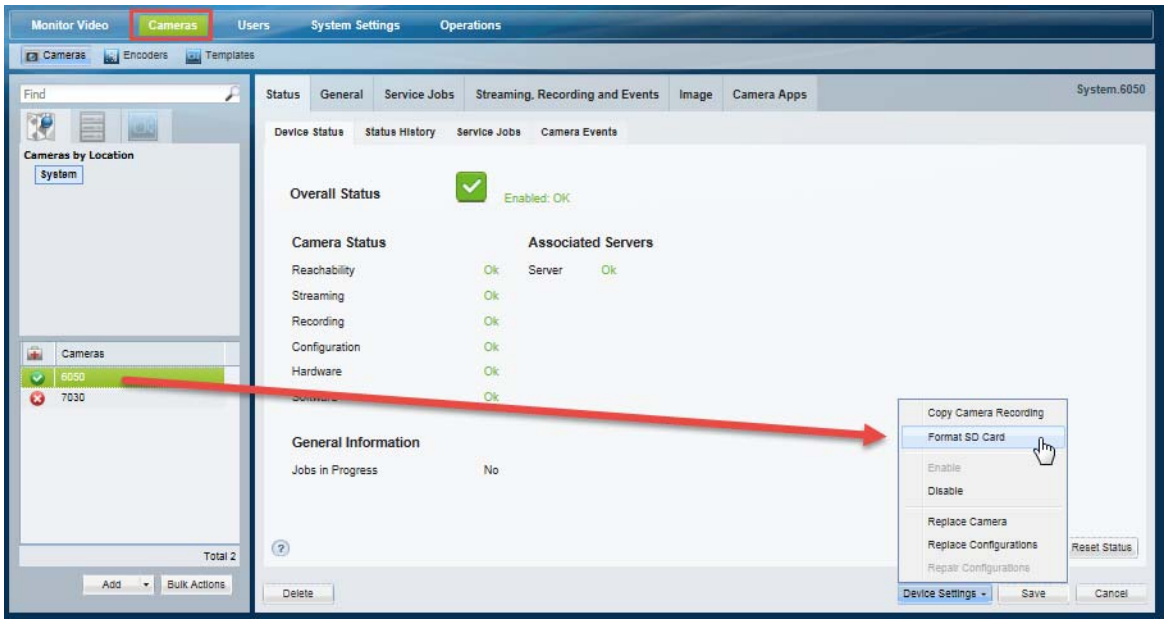
Step 2 Add the camera to Cisco VSM.

See the “Adding and Managing Cameras” section on page 10-1.

Step 3 In the Cisco VSM Operations Manager, click **Cameras**, select a location and select the camera name.

Step 4 Select **Device Settings** > **Format SD Card** (Figure 15-2):

Figure 15-2 Formatting an SD Card



Step 5 Click **Yes** to verify.

Step 6 Wait for the job to complete. To view the formatting status, see Service Jobs (Cameras), page 10-65.

Step 7 If the format fails, see the "SD Card Usage Notes" section on page 15-5 for possible reasons.

Formatting the SD Cards in Multiple Cameras (Bulk Actions)

Procedure

Step 1 Physically install the storage device in the cameras.

Refer to the camera documentation for more information. You can also format the storage device using the camera's interface.

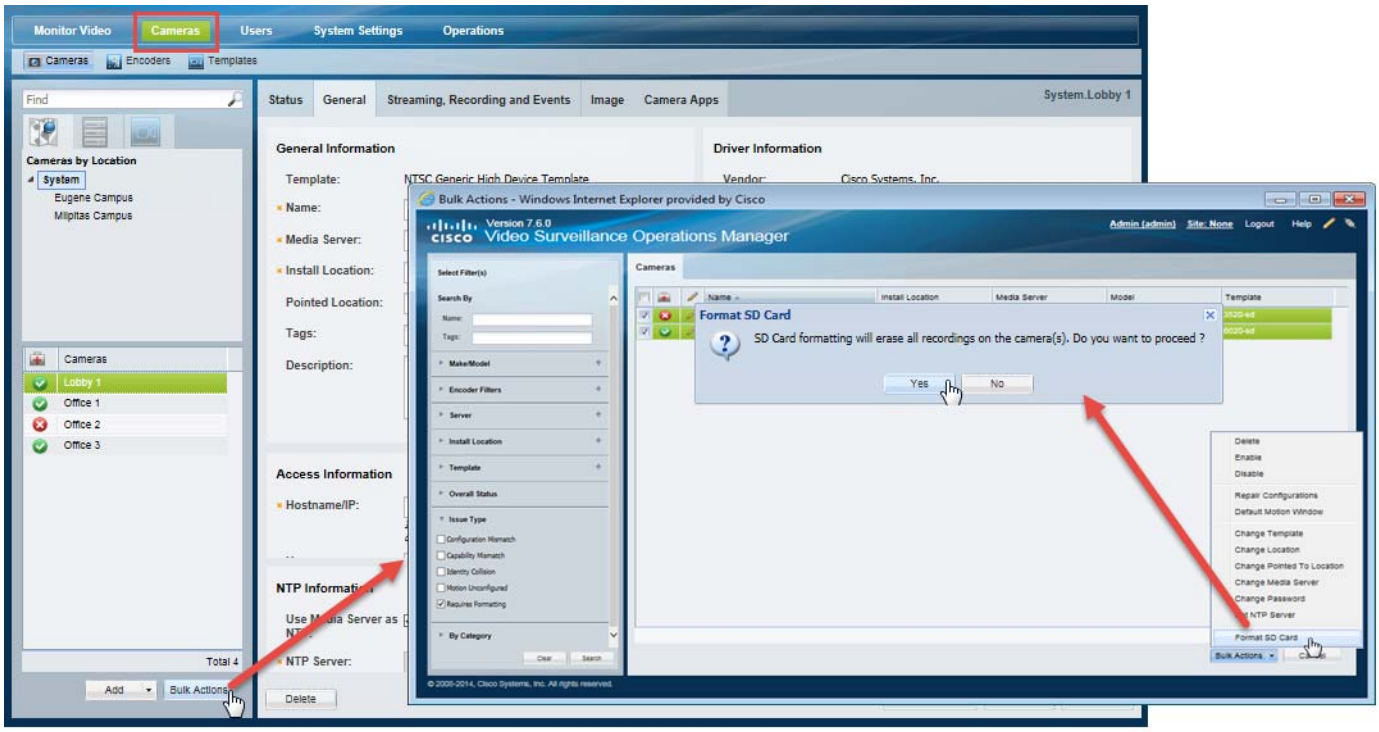
Step 2 Add the cameras to Cisco VSM.

See the "Adding and Managing Cameras" section on page 10-1.

Step 3 In the Cisco VSM Operations Manager, click **Cameras**.

Step 4 Click **Bulk Actions** (Figure 15-3):

Figure 15-3 Formatting the SD Cards in Multiple Cameras



Step 5 (Optional) Select the filter **Requires Formatting** to only display cameras with an SD card that require formatting (the cameras are in *critical* state).

Step 6 Click **Search**.

Step 7 Select the cameras from the results.

Step 8 Choose **Bulk Actions** > **Format SD Card**.

Step 9 Click **Yes** to verify.

Step 10 Wait for the jobs to complete. To view the formatting status, see Service Jobs (Cameras), page 10-65.

Step 11 If the format fails, see the "SD Card Usage Notes" section on page 15-5 for possible reasons.

Connected Edge Storage (Enabling Recording On Cameras)

To store recordings on the camera, select the "**Enable Continuous Recording**" option in the camera template.

Procedure to Enable Recording Storage on Cameras

Step 1 Complete the requirements to install and configure the network cameras.

- See the "Requirements" section on page 15-4.

Step 2 Log in to the Operations Manager.

- You must belong to a User Group with permissions for *Templates*.
- See the "Adding Users, User Groups, and Permissions" section on page 4-1 for more information.

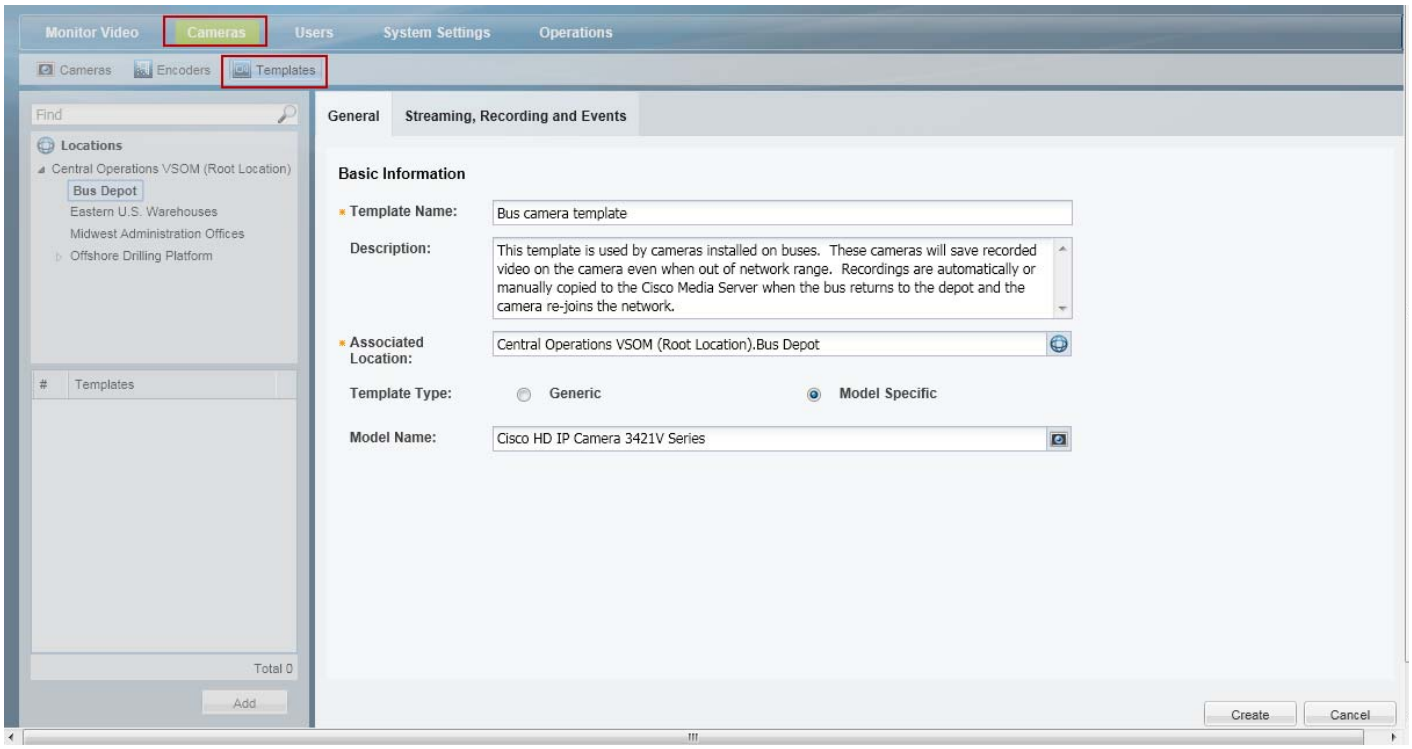
Step 3 Select **Cameras** > **Templates**.

Step 4 Add or edit a template (Figure 15-4):

See the following for more information:

- Adding and Editing Camera Templates, page 12-1
- Creating or Modifying a Template, page 12-3
- Configuring Video Recording, page 12-7

Figure 15-4 Creating a Template



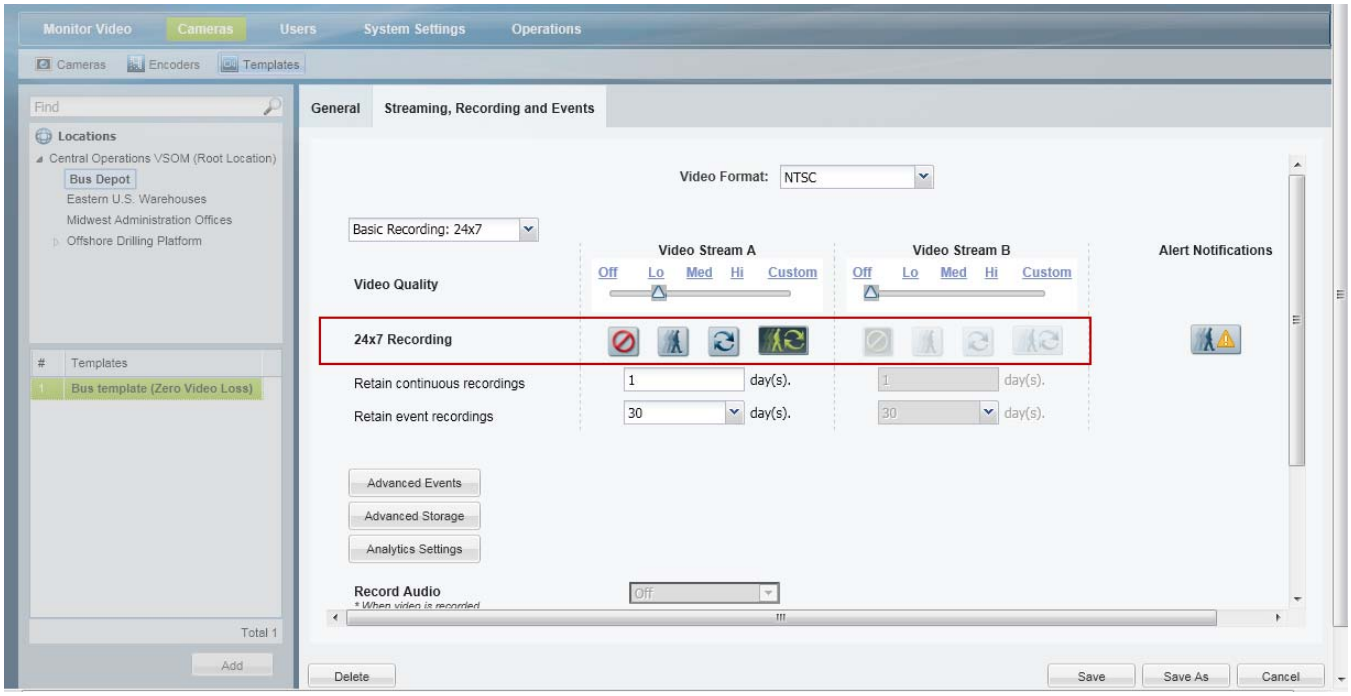
Note System defined templates are locked and cannot be modified.

Step 5 In the **Streaming, Recording and Events** tab, configure the *24x7 Recording* options(Figure 15-5).

- Auto-Merge Recordings —Automatic copying from the camera to the Media Server requires continuous recording. To enable Auto-Merge Recordings, select one of the following:
  - **Continuous Recording**—Record video in a continuous 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.
- Manually-triggered copying is allowed only when the **No Recording** option is selected.

Note When on-camera recording is enabled, video is saved to the camera storage without motion or advanced events. These events are added (post-processed) after the video is copied to the Media Server. Video is copied to the Media Server based on the camera template recording schedule. For example, if the camera template schedule specifies recordings from 8 am to 11 am, only continuous recordings for those times will be copied from the camera to the Media Server.

Figure 15-5 Selecting the Recording Options



Step 6 Enable camera recordings for Video Stream A or B.

This allows recorded video to be stored on the camera (Figure 15-6). Camera video storage can be enabled for a single stream. The video from that stream is copied to the Media Server.

a. Click **Advanced Storage**.

b. Select the **Recording Options** tab.

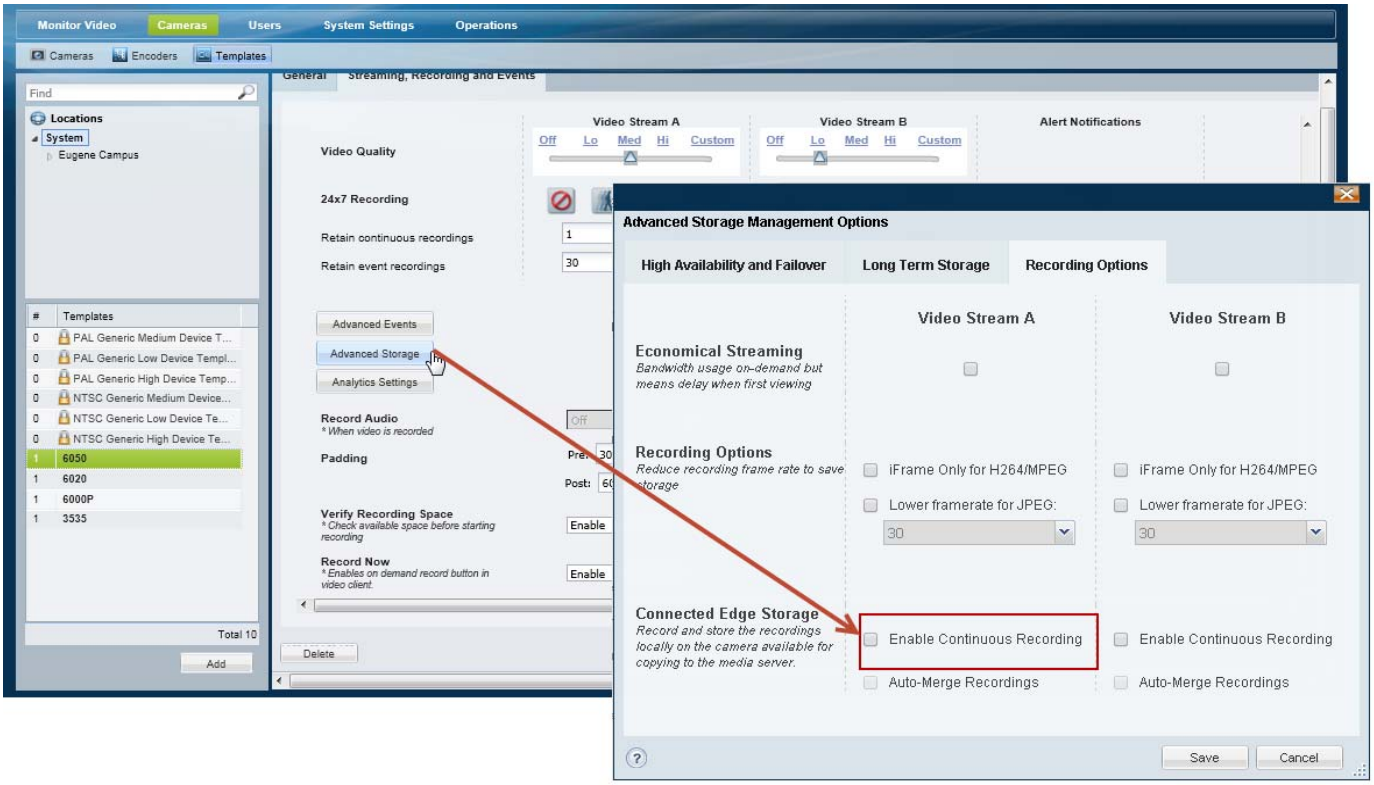
Note The **Connected Edge Storage** option appears only when the device supports on-device storage (see the "Supported IP Cameras (On-Device Storage)" section on page 15-5).

c. Select **Enable Continuous Recording** for a stream (this also enables Economical Streaming on the same stream).

d. (Optional) Select **Auto-Merge Recordings** to automatically copy a continuous recording from the camera to the Media Server (available only if a continuous recording option is configured in Step 5).

e. Click **Save** to save and close the Recording Options.

Figure 15-6 Enabling Recordings on Camera



Note

- Camera storage can be enabled for a single stream only.
- Economical Streaming is automatically selected for the stream. See the "Defining the Recording Options" section on page 17-20 for more information.

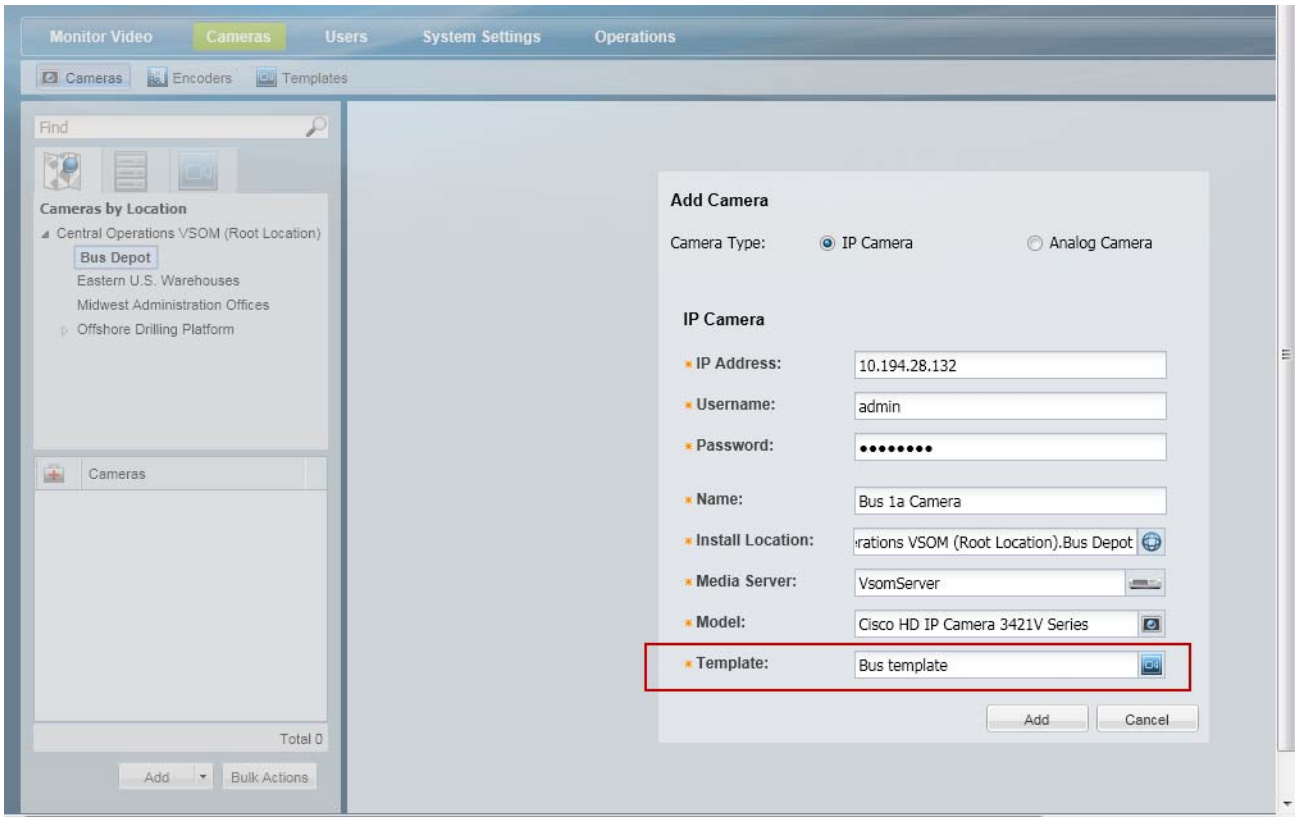
Step 7 Click **Save** again to save the template changes.

Step 8 Apply the template to the cameras that support video storage (Figure 15-7).

See the "Adding and Managing Cameras" section on page 10-1, specifically:

- Manually Adding Cameras, page 10-8
- Discovering Cameras on the Network, page 10-23.

Figure 15-7 Add Cameras to the Template



Auto-Merge Recordings (Automatic Copying)

Auto-Merge Recordings enables automatic copying of videos recorded on the camera to the Cisco Media Server (Figure 15-8). Any gaps on the media server, according to the camera template's recording schedule are filled in.

Usage Notes

- When on-camera recording is enabled, video is saved to the camera storage without motion or advanced events. These events are added (post-processed) after the video is copied to the Media Server. Video is copied to the Media Server based on the camera template recording schedule. For example, if the camera template schedule specifies recordings from 8 am to 11 am, only continuous recordings for those times will be copied from the camera to the Media Server.

Important Performance Considerations When Using "Auto-Merge Recordings"

Due to bandwidth considerations, the number of cameras that can be supported by a Media Server will drop in half when all of the cameras on that server are configured for Auto-Merge Recordings. We recommended a maximum of 10 cameras on a single Media Server be configured with Auto-Merge Recordings. See the Release Notes for Cisco Video Surveillance Manager for more information when using Auto-Merge Recordings with Release 7.5.

For example, when a camera configured with "Auto-Merge Recordings" reconnects to the Media Server after a network outage, live video recording will resume and the camera will begin copying locally-stored video to the Media Server (to fill the recording gaps on the Media Server). Video is also copied from the camera at a rate that is at least 25% faster than real-time so that all of the video from an outage is copied from the camera before it is overwritten. This means that after an outage, the total bandwidth from the camera to the Media Sever is more than 2X the video data rate until all of the video from the outage has been copied from the camera. Since the Media Server has a limit on total recording bandwidth, the use of "Auto-Merge Recordings" will reduce the total number of cameras that can be supported on a Media Server. If all of the cameras on the Media Server are configured with "Auto-Merge Recordings", the number of supported cameras will drop by more than half.

"Auto-Merge Recordings" Configuration Procedure

Step 1 Complete the requirements to install and configure the network cameras.

- See the "Requirements" section on page 15-4.

Step 2 Enable camera storage on the camera template.

- See the "Connected Edge Storage (Enabling Recording On Cameras)" section on page 15-8.

Step 3 Enable "Auto-Merge Recordings" (Figure 15-8).

a. Click **Advanced Storage**.

b. Select the **Recording Options** tab.

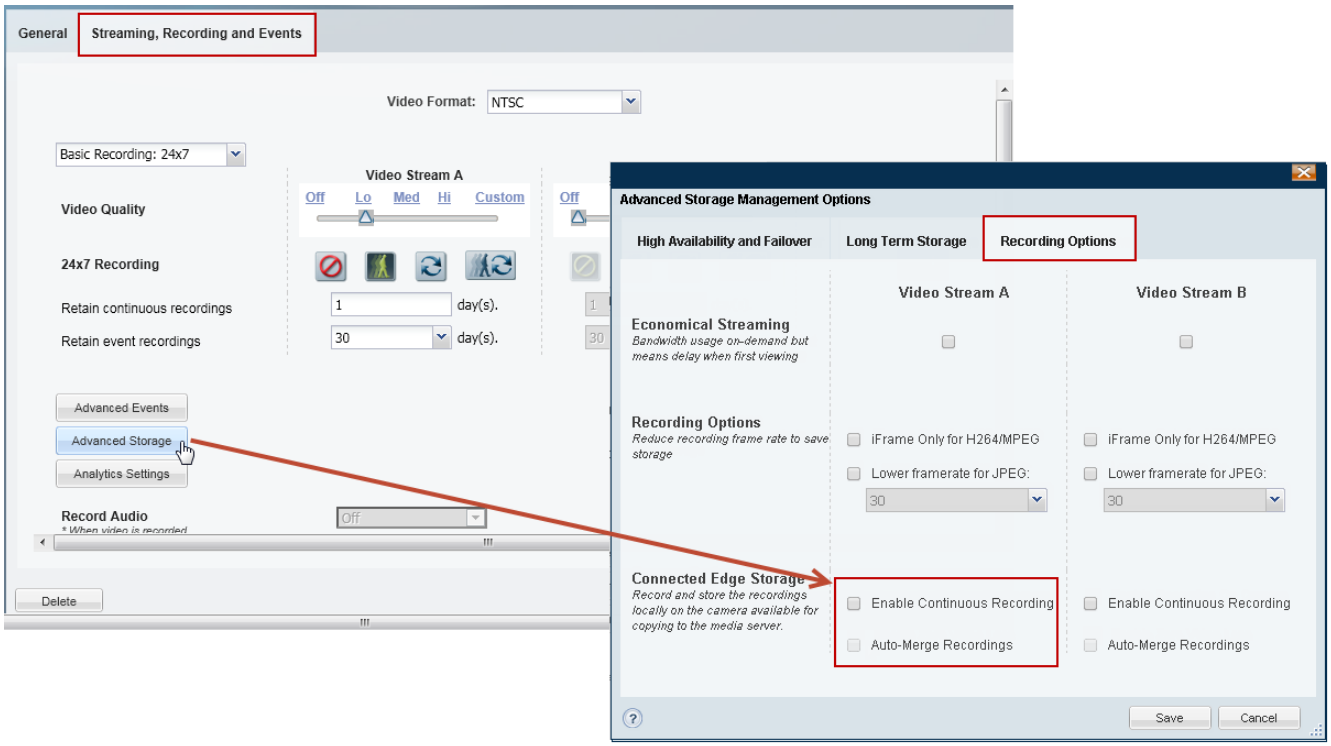
c. Select **Enable Continuous Recording** for Stream A or B.

d. Select **Auto-Merge Recordings** to automatically copy video recordings from the camera storage to the Media Server.

   This option is available only when a continuous recording option is configured for the template. See the "Connected Edge Storage (Enabling Recording On Cameras)" section on page 15-8 for more information.

e. Click **Save** to save and close the Recording Options.

Figure 15-8 Enabling Recordings on Camera



Note

- Camera storage can be enabled for a single stream only (either stream A or B).
- **Economical Streaming** is automatically elected on the same stream that has the **Enable Continuous Recording** enabled. See the "Defining the Recording Options" section on page 17-20 for more information.

Step 4 Click **Save** again to save the template changes.

Step 5 Add or edit cameras and assign them to the template.

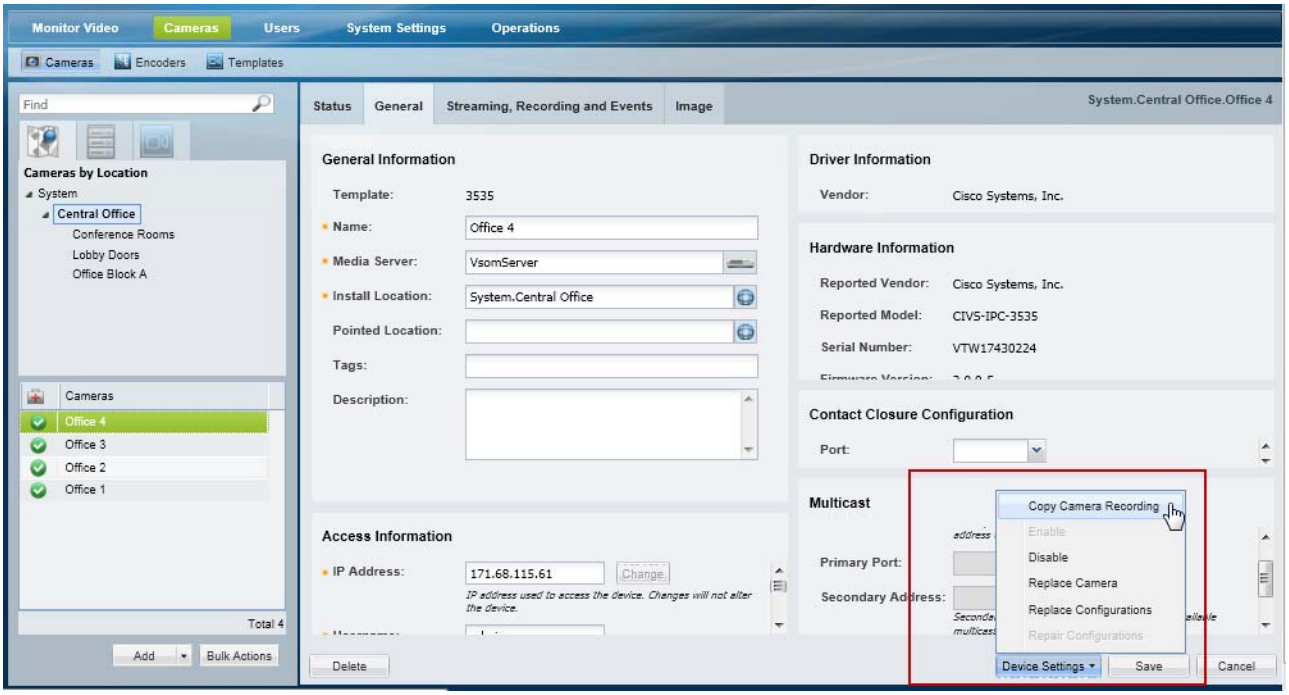
See the "Adding and Managing Cameras" section on page 10-1, specifically:

Step 6 Add Cameras to the template (Figure 15-7).

Copy Camera Recordings (Manually Triggered)

To manually copy recordings stored on a camera to the Media Server, use the **Copy Camera Recordings** command in the camera configuration page (Figure 15-9). Manually copying recordings allows you to copy one or more recordings stored on the camera to the Media Server.

Figure 15-9 Copy Camera Recordings



Tip You can also use the Cisco Video Surveillance Safety and Security Desktop application (Cisco SASD) to copy the recordings from a camera to the Media Server. See the Cisco Video Surveillance Safety and Security Desktop User Guide for more information.

Usage Notes

- You must belong to a user group with *Copy From Edge Storage* permission. See the "Adding Users, User Groups, and Permissions" section on page 4-1 for more information.
- One storage copy job is performed per device at a time (a job must finish before a new job can begin). Up to 10 copy jobs can be performed simultaneously.
- When on-camera recording is enabled, video is saved to the camera storage without motion or advanced events. These events are added (post-processed) after the video is copied to the Media Server. Video is copied to the Media Server based on the camera template recording schedule. For example, if the camera template recording schedule specifies recordings from 8 am to 11 am, only recordings for those times will be copied from the camera to the Media Server.

Procedure

Step 1 Complete the requirements to install and configure the network cameras.

- See the "Requirements" section on page 15-4.

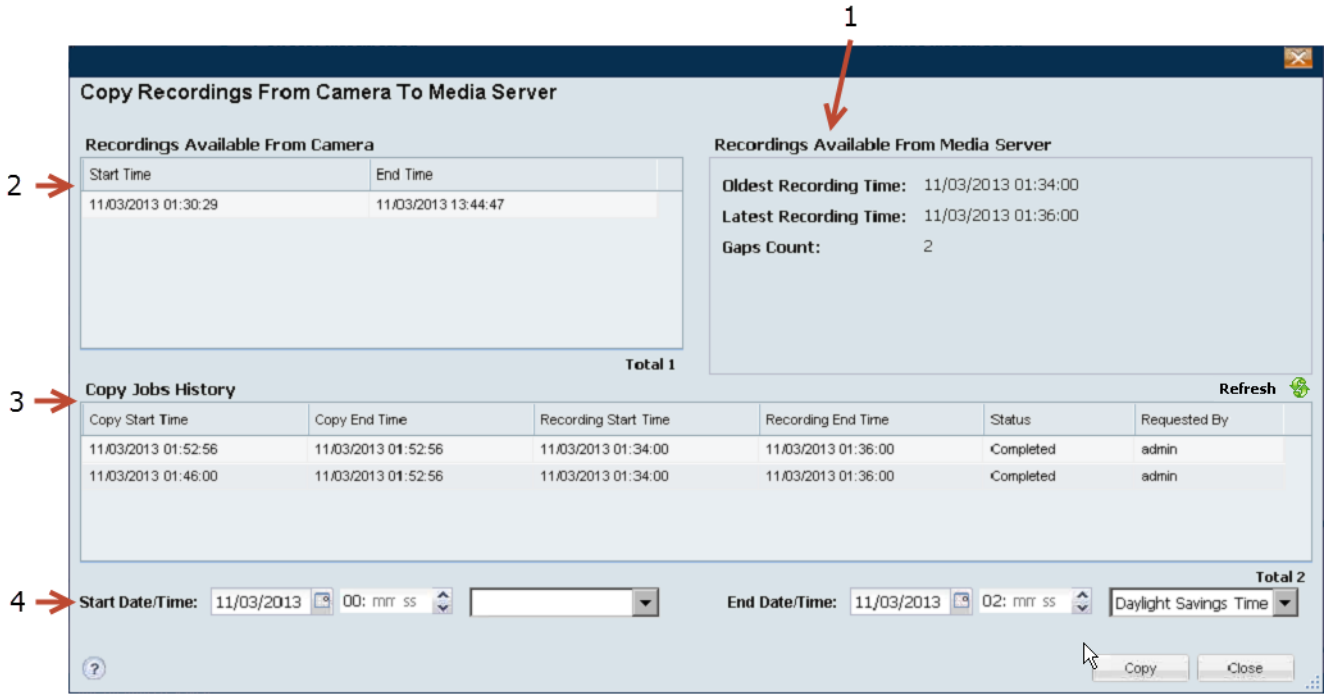
Step 2 Enable camera storage on the camera template, and assign the camera to the template.

- See the "Connected Edge Storage (Enabling Recording On Cameras)" section on page 15-8.

Step 3 Select **Device Settings** > **Copy Camera Recordings** (Figure 15-9).

Step 4 Select the recording(s) to copy from the camera to the Media Server and click **Copy** (Figure 15-9).

Figure 15-10 Copy Camera Recordings



1	The recordings that currently exist on the Media Server for the camera. • Oldest Recording Time—The oldest time stamp for all recordings (from the selected camera) on the Media Server. • Latest Recording Time—The latest time stamp for all recordings (from the selected camera) on the Media Server. • Gaps Count—The number of recording gaps in the range. For example, a gap can occur when the camera is out of range and recordings are not copied to the Media Server. Gaps can also occur if only motion events are recorded. These gaps can be filled in when video is transferred from the camera.
2	Displays the recordings that are available from the camera. • Continuous recordings typically display a long period between the start and end times. • Motion events typically display multiple short entries.
3	A history of previous copy jobs. Double-click an entry to view job details. • Rows in the job history table are read-only, except rows with a Failed status. • Select rows with a Failed status to open a popup window that displays the failure reason of that copy job. See the "Understanding Jobs and Job Status" section on page 19-29 for more information

4	Select the start and end times of the recordings to be copied to the Media Server. • Any available recordings on the camera that fall within this range will be copied. • Existing recordings are skipped. Only gaps in the existing Media Server archive are copied (filled in). • See the "Timezone Best Practices" section on page 15-16 for more information on using timezones.

Timezone Best Practices

Switching the timezone from the Standard Time to the Daylight Savings Time moves the clock forward by one hour. For example: 03/11/2013 "1:00 AM ST" becomes "2:00 AM DST". The reverse occurs when switching the timezone from Daylight Savings Time to Standard-Time (the clock moves backward by one hour, i.e. 11/04/2013 "2:00 AM DST" becomes "1:00 AM ST").

Cameras, however, are not impacted by this timezone switch-over. In rare cases when a recording on the camera having either its start time or its end time falls within the overlapping one hour during the timezone switch-over from the Daylight-Savings-Time to Standard-Time (for example 2:00 AM to 1:00 AM), the display of the recording time may appear overlapped because the clock is moved backward by one hour. However, the actual recordings on the camera are not overlapped.

Best Practice

The best practice when specifying the time range to copy camera recordings is to avoid the one hour during the timezone switch-over. Specify a start time before the timezone switch-over and specify the end time after the timezone switch-over.

Example 1

On 03/10/2013 02:00 ST-to-DST switch-over, when moving the clock forward by one hour, copy 2-minute of camera recordings starting one minute before the switch-over and ending one minute after the switch-over.

1. Specify the start time at 03/10/2013 01:59:00
2. Specify the end time at 03/10/2013 03:01:00

Example 2

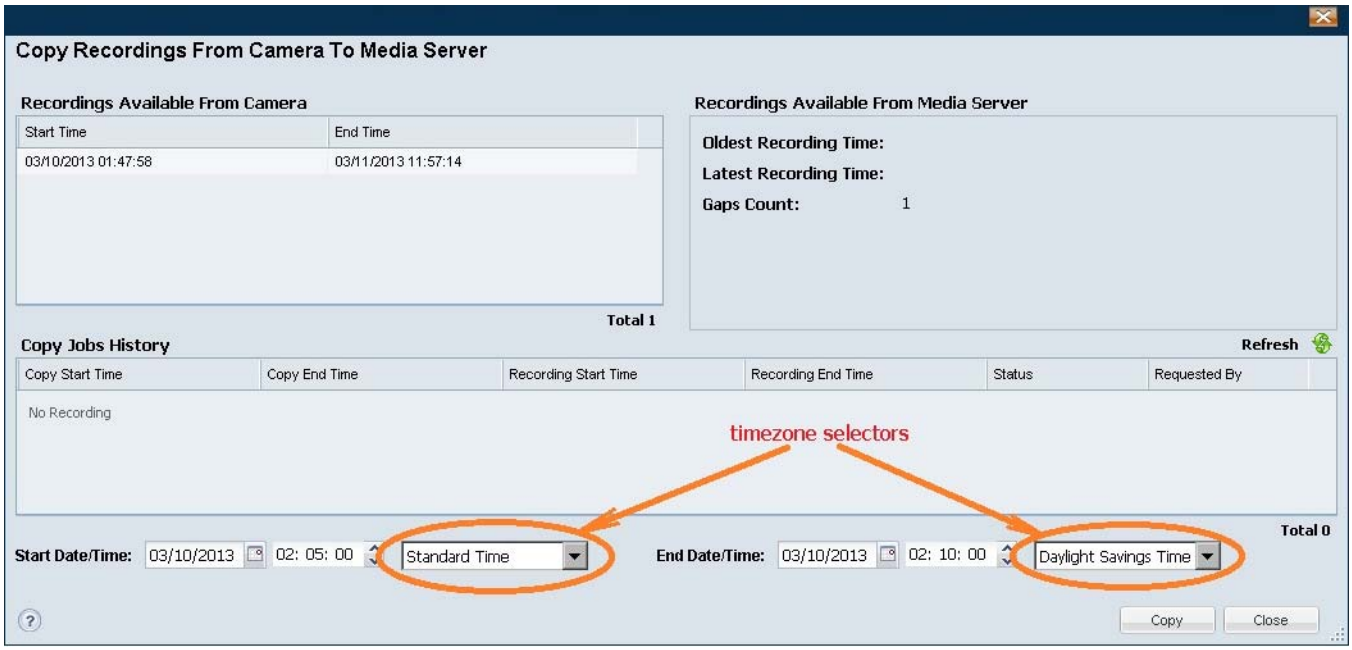
On 11/04/2013 02:00 DST-to-ST switch-over, when moving the clock backward by one hour, copy one-hour and 2-minute of camera recordings starting one minute before the switch-over and ending one minute after the switch-over.

1. Specify the start time at 11/04/2013 01:59:00
2. Specify the end time at 11/04/2013 02:01:00

Specify a Range Within a Timezone Switch-Over

To specify a precise time range when either the start-time or the end-time falls within the one hour timezone switch-over, use the timezone selectors. This option is useful when the clock is moved backward by one hour (Figure 15-11).

Figure 15-11 Timezone Selectors



The timezone selector modifies the time according to the following.

- If the specified time falls on the Standard-Time timezone and the user also selects the "Daylight-Savings-Time" timezone, then the time specified by the user is increased by one hour.
- If the specified time falls on the Daylight Savings Time timezone and the user also selects the "Standard-Time" timezone, then the time specified by the user is decreased by one hour.

On all other cases, the time specified by the user is modified.

Example 1

03/10/2013 02:05:00

The one hour between 02:00:00 and 02:59:59 is not represented because 02:00 is moved forward to 03:00 during the ST-to-DST timezone switch-over. In this case, 02:05:00 is represented as 03:05:00, and it falls into the DST timezone.

Note Technically, "03/10/2013 03:05:00" is equivalent to 1362909900000 milliseconds UTC.

If you add a "Standard Time" modifier to the "03/10/2013 02:05:00", the system will subtract one hour from "03/10/2013 03:05:00". The result of this subtraction is "03/10/2013 01:05:00" in standard time.

Example 2

03/10/2013 02:15:00

The time "03/10/2013 02:15:00" is 15-minute after the 02:00 ST-to-DST switch-over, and it falls into the DST timezone. It would be represented as "03/10/2013 03:15:00".

If you add a "Daylight Saving Time" modifier to the "03/10/2013 02:15:00", because it is already in the DST timezone, no modification is applied, and the time is sent to the Media Server for copying camera recordings.

Example 3

03/10/2013 01:58:00 to 03/10/2013 03:02:00

To copy a 4-minute camera recording starting from 2 minutes before the ST-to-DST switch-over and ending at 2 minutes after the ST-to-DST switch-over, specify the time range start-time "03/10/2013 01:58:00" and end-time "03/10/2013 03:02:00" without selecting the timezone selector on both.

Related Recording Documentation

See the following topics for more information about configuring video recordings:

Table 15-3 Configuring Video Topics

Topic	Description
Configuring Continuous, Scheduled, and Motion Recordings, page 12-7	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 13-7	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 3-11	Describes how to enable the **Record Now** option when a user right-clicks a camera's live image.
Cisco Video Surveillance Safety and Security Desktop User Guide	You can also use Cisco SASD to copy the recordings from a camera to the Media Server.

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

Tip See also the "Upgrading Cisco Camera and Encoder Firmware" section on page 26-19.

Note Encoders are not required for IP (networked) cameras.

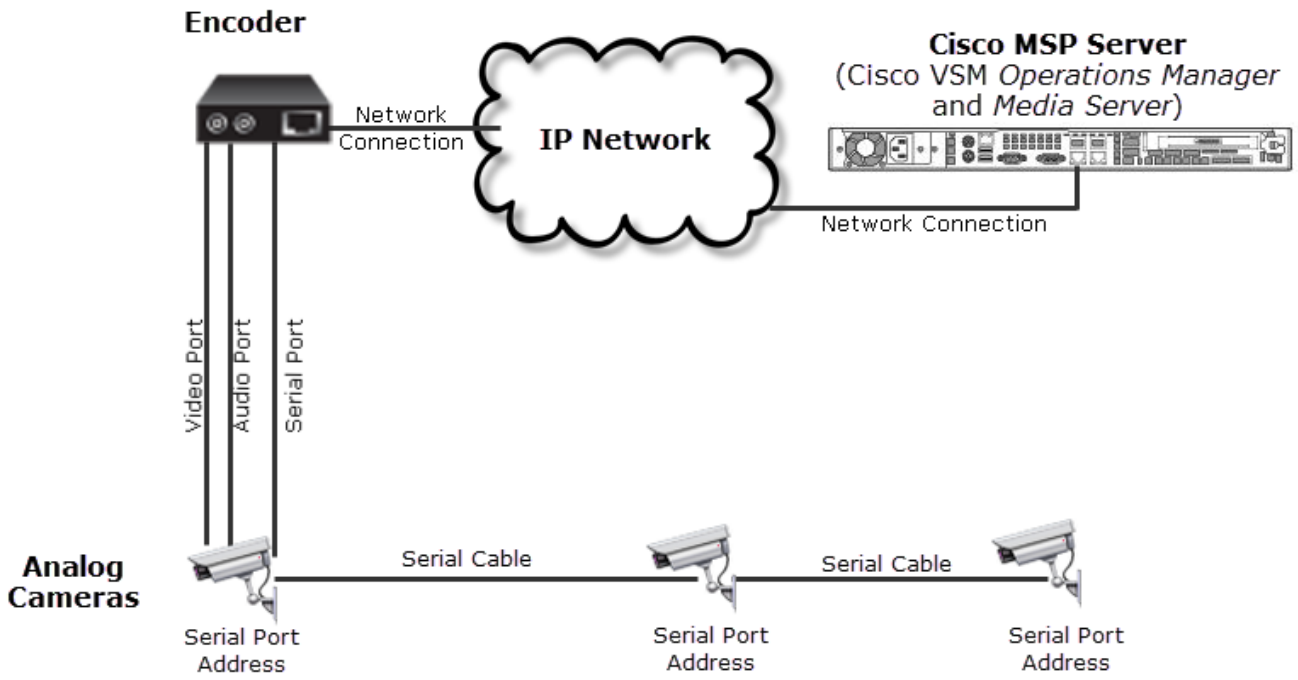
Overview

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 16-1). 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 16-1 shows an external encoder configuration.

Figure 16-1 External Encoder Configuration

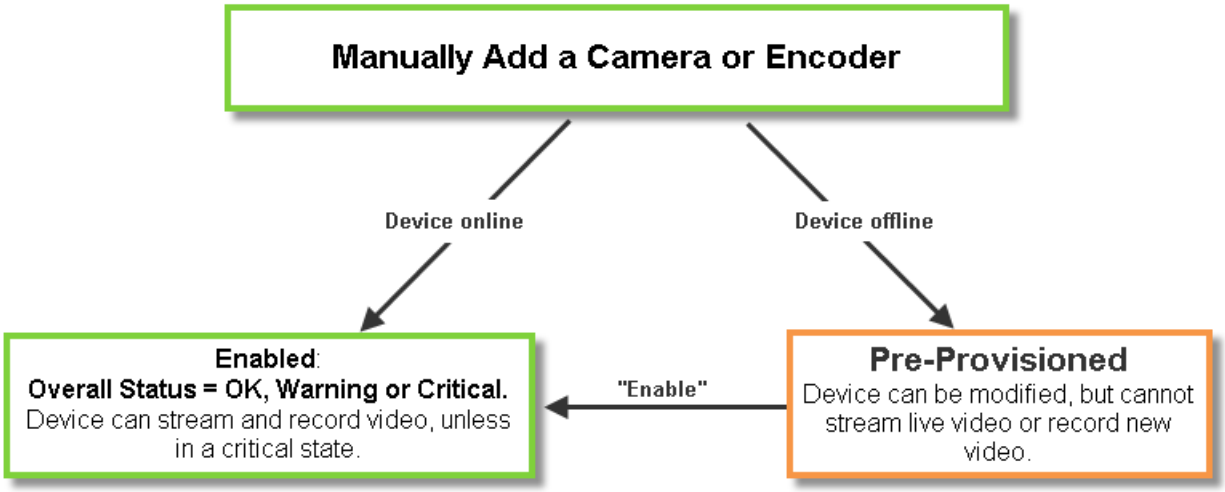


To manually add a single encoder or analog camera, open the encoder configuration page and click **Add**. Enter the settings as described in the "Adding External Encoders and Analog Cameras" section on page 5.

If the device is not available on the network, it can be added in *pre-provisioned* state (Figure 16-2). See the "Pre-Provisioning Encoders and Analog Cameras" section on page 16-3 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 10-17.

Figure 16-2 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 16-1 Analog Camera Requirements

Requirements	Requirement Complete? (✓)
The wiring between the cameras and the encoder must adhere to the protocol requirements, including: • 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. See the device documentation for more information.	❑
The encoder serial ports must be correctly configured: • 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. See the device documentation for more information.	❑
The camera serial port must be correctly configured: • All cameras must be properly terminated. • All cameras must have unique serial addresses. See the device documentation for more information.	❑
To add and configure encoders and analog cameras in Cisco VSM, 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.	❑

Adding External Encoders and Analog Cameras

Complete the following procedure to manually add external encoders to the Cisco VSM configuration.

Note To import multiple cameras or encoders using a text file, see the "Importing or Updating Cameras or Encoders Using a CSV File" section on page 10-17.

Procedure

Step 1 Install and configure the encoder so it can be accessed on the network:

a. Physically install the encoder so it can access the same network as Cisco VSM.

b. Configure the network settings on the device.

c. 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 16-2).

Table 16-2 General Encoder Settings

Setting	Description
Name	Enter a descriptive name for the encoder. Enter a name that helps identify the device location or primary use. Use any combination of characters and spaces.
IP Address	Enter the IP address configured on the device. • 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 10-60 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 16-2 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. • 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 10-60 for more information.

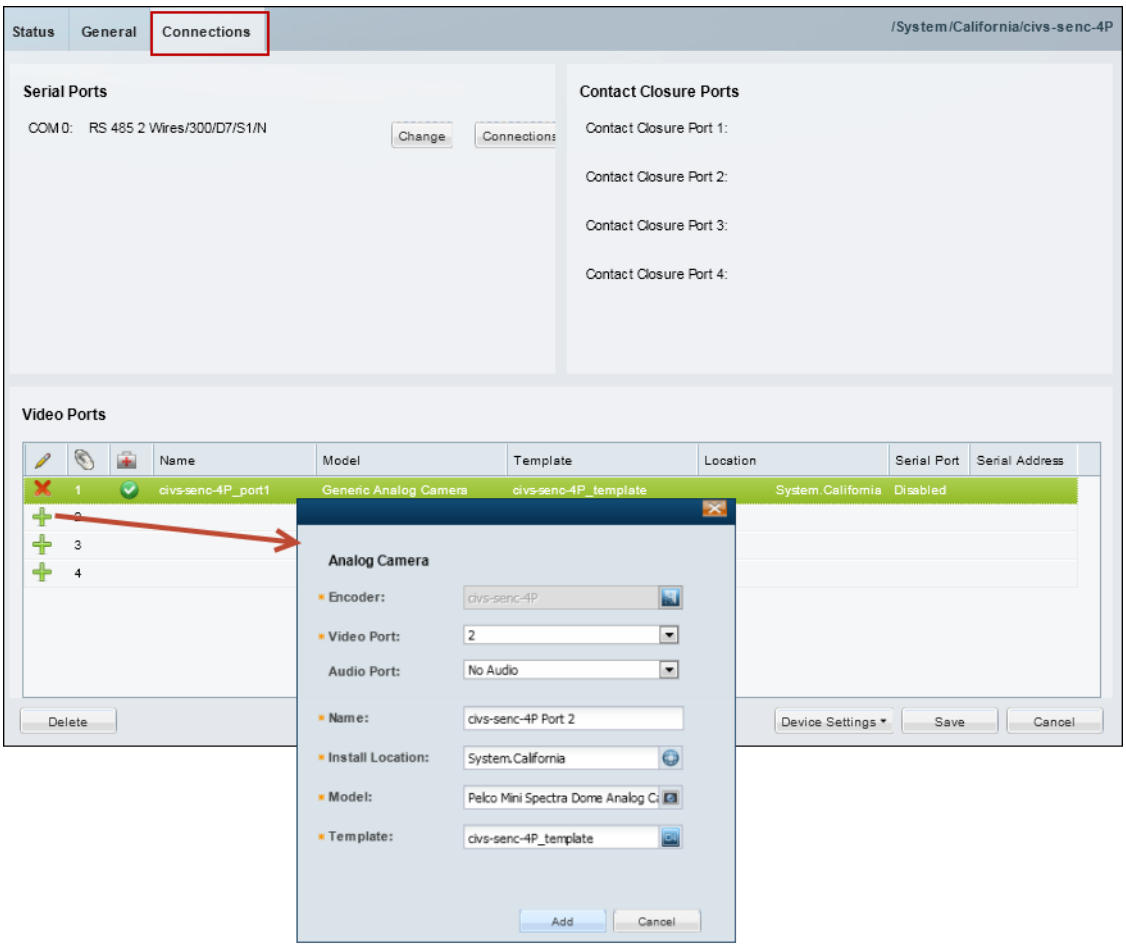
Step 7 Click **Add**.

- 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 16-3.
  - 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 16-3).

Tip You can also add analog cameras from the camera configuration page. See the "Manually Adding Cameras" section on page 10-8 for more information.

Figure 16-3 Adding Analog Cameras to an Encoder



a. Click the **Connections** tab.

b. Click the *Add* icon.

c. Enter the analog camera settings (Table 16-3).

Table 16-3 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 16-3 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. • 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 10-42. • 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 12-1 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.

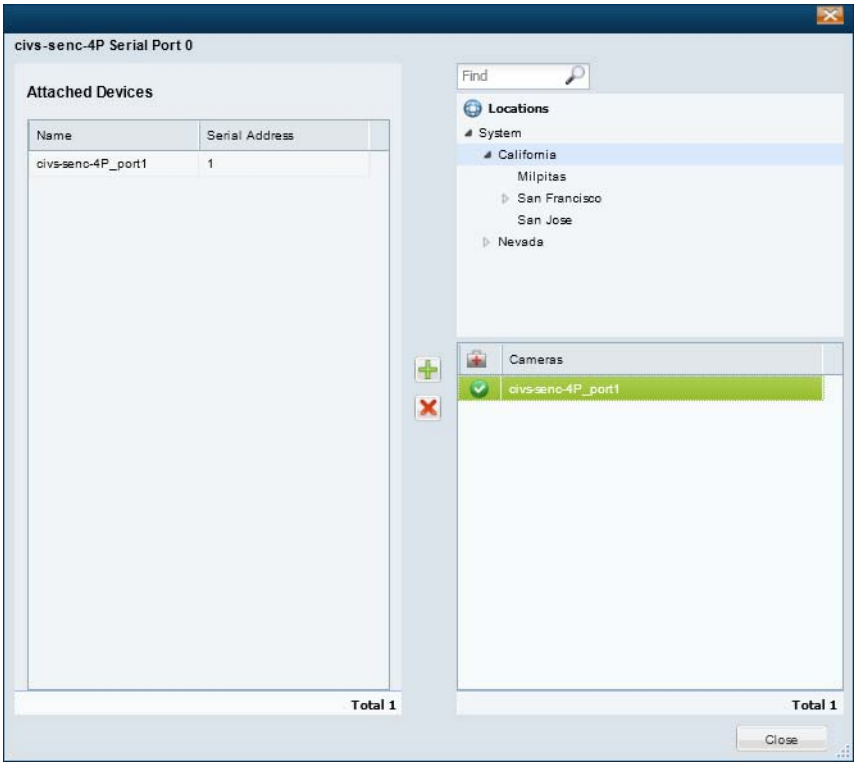
For example, protocol, baud rate, data bits, stop bit and parity.

- 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 16-4 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 16-4).

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 10-44 for more information.

Figure 16-4 Serial Port Connections



a. Expand the location tree and select the camera's *Install Location* (see Table 16-3).

b. Select a camera name from the list.

c. Click the add icon.

d. Enter the serial port connection settings (Table 16-4) and click **Add**.

Table 16-4 Analog Camera Serial Port Settings

Setting	Description
Encoder	The encoder for the analog camera.

Table 16-4 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 10-42.

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 16-11.

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 10-92
- Bulk Actions: Revising Multiple Servers, page 6-26

Procedure

Step 1 Select **Cameras** > **Encoders**.

Step 2 Click **Bulk Actions** (under the device list) to open the Bulk Actions window.

Step 3 Click the ✚ icon next to each field to select the filter criteria (Table 16-5).

Table 16-5 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 `Enter`.
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.

Table 16-5 Bulk Action Filters (continued)

Filter	Description
Overall Status	Select the administrative states for the devices. For example: • **Enabled (OK, Warning** or **Critical)**—The device is enabled, although it may include a *Warning* or *Critical* 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). **Tip** See the "Device Status: Identifying Issues for a Specific Device" section on page 19-9 for more information.
Issue Type	Select the issues that apply to the device. For example: • **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 19-29.

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
   - axisq74061 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, axisq74061 and axisq7406_2_n: only the _1 model supports Serial PTZ.
   - axisq7404_1 and axisq7404_2_n: only _1 model supports audio.

Constraints

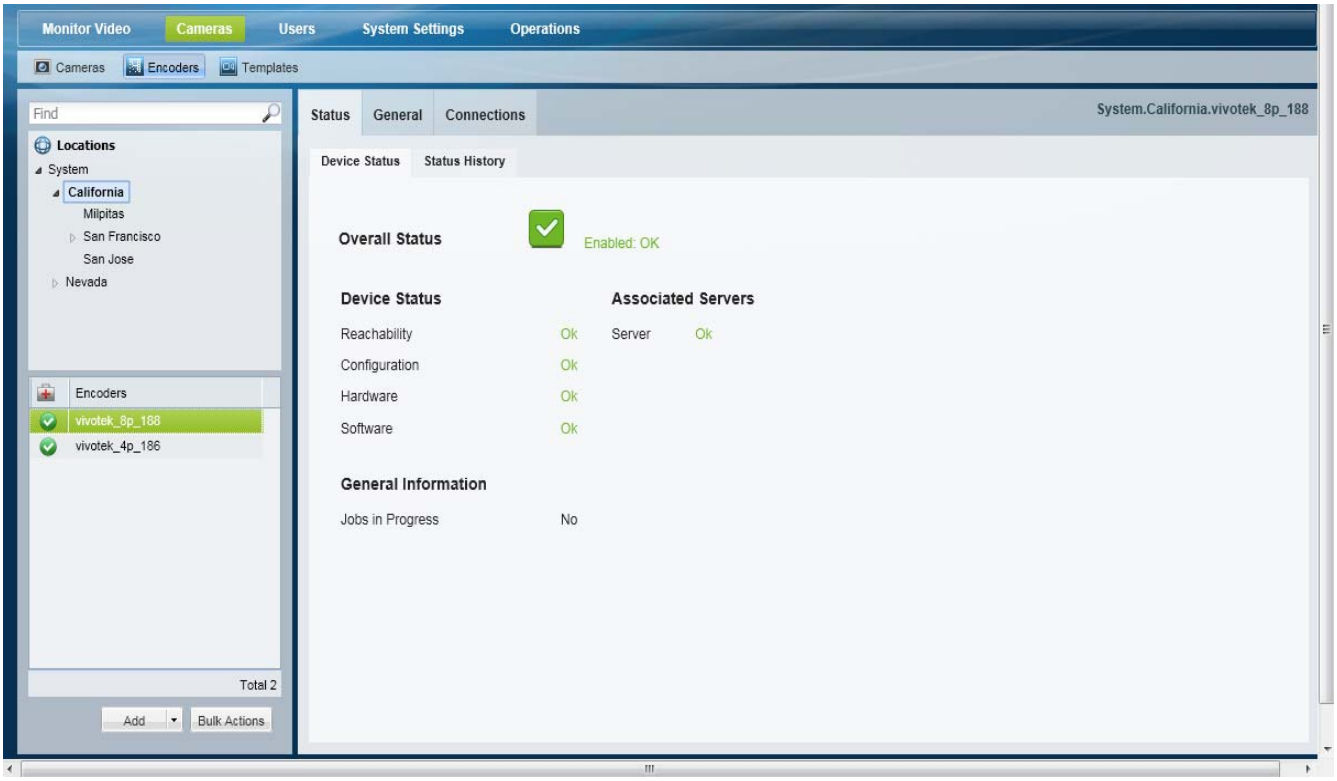
The constraints are as follows:

- 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.

Encoder Status

Click the encoder **Status** tab (Figure 16-5) to display a snapshot of the device health, including the device's ability to communicate with a Media Server. See Table 16-6 for descriptions of the Overall Status.

Figure 16-5 Camera Device Status



Device Status	Displays a snapshot of the current status, and the device attribute that is experiencing the error. **Tip** Click the **Status History** tab for additional details. Click **Refresh Status** to reload the current device status.
Status History	Displays the specific system events that impact the device status. Select **Affecting Current Status** to display only the events that are causing the current error.
Camera Events	(Analog Cameras only) See the "Camera Status" section on page 10-62 for more information.

Camera Status

When an encoder or analog camera is added to Cisco VSM, it is placed in either *Enabled* or *Pre-provisioned* state.

- *Enabled* means that the user intends the device is to be functional. There are three possible sub-levels: OK, Warning, and Critical (see Table 16-6).
- *Pre-provisioned* means that the device is added to the configuration but not available on the network. See the "Pre-Provisioning Encoders and Analog Cameras" section on page 16-3 for more information.

See Table 16-6 for additional descriptions.

Table 16-6 Device Status

State	Description
Enabled: OK	The device is operating normally and has no errors.
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. The device is enabled but is in a state unable to perform its full capacity. **Tip** An IP camera and an analog camera that are in *Enabled: Critical* state after they are enabled from a *Pre-provisioned* state usually indicate a mis-match configuration. This is often caused by a missing motion detection configuration on the camera when the camera template requires one. See the "Camera Status" section on page 10-62 for more information. See the "Synchronizing Device Configurations" section on page 19-21 for information on viewing and resolving configuration mismatches.
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 camera can be modified, but the camera cannot stream or record video until the configuration is complete and you choose **Enable** from the **Device Settings** menu • **IP Camera**—A *Pre-provisioned* IP camera 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. • **Encoder**—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. **Note** 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. • **Analog Camera**—An analog camera in this state is associated to an encoder that is either in a state of Pre-provisioned or Enabled. 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.

For more information see the "Device Status: Identifying Issues for a Specific Device" section on page 19-9.

High Availability: Cisco Media Servers

Cisco Video Surveillance Media Servers can be configured in a high availability (HA) arrangement that allows a primary server to be paired with additional *Failover*, *Redundant*, or *Long Term Storage* Media Server. These HA servers provide the primary server with hot standby, redundant stream storage and playback, and long term recording storage to help ensure that functionality and recordings are not lost if the primary server goes offline.

Review the following information to understand the roles and functions of the Media Servers in and HA configuration, and for instructions to install and configure the HA servers.

Contents

Note See the "Operations Manager High Availability" section on page 18-1 for instructions to configure Operations Manager server HA.

Overview

Review the following information to understand the HA server types, and how they support the HA features for the Primary server.

Requirements

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

Table 17-1 Requirements

Requirements	Requirement Complete? (✓)
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.	❑
At least two Media Servers must be enabled: • 1 Primary Media Server • 1 HA Media Server Install additional Media Servers to enable additional HA features. **Note** All Media Servers are assigned the Primary HA role by default. **Note** The co-located Media Server is automatically added to the Operations Manager and activated. The default co-located server name is "VsomServer". See the "Understanding Redundant, Failover, and Long Term Storage Servers" section on page 17-4.	❑
Co-located Servers—The Operations Manager and a single Media Server are enabled on the same server. The following rules apply: • The co-located Media Server can only be a Primary Media Server (co-located Media Servers do not support other HA roles such as Standby or Redundant). • Co-located Media Server cannot be configured with Failover or Redundant Media Servers. Only a long term storage (LTS) server can be associated with a co-located Primary Media Server.	❑
The time on all servers must be in sync, which requires NTP configuration. We recommend using the same network time protocol (NTP) server on all Media Servers to ensure the time settings are accurate and identical. See the "NTP Information" section on page 6-14 for more information.	❑
All edge devices (such as cameras and encoders) must be added to a server using a local (non-NAT) addresses. End points with NAT addresses are not supported.	❑

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.	• Cisco Physical Security UCS Platform Series User Guide • Cisco Multiservices Platform for Physical Security User Guide • Cisco Video Surveillance Management Console Administration Guide
Step 2	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".	• "Configuring Servers" section on page 6-1 • "Configuring Media Server Services" section on page 9-1
Step 3	Define a HA *Role* for each Media Server. **Tip** All Media Servers are assigned the Primary HA role by default.	• Understanding Redundant, Failover, and Long Term Storage Servers, page 17-4 • Define the Media Server HA Role and Associated Servers, page 17-9
Step 4	Associate the Primary and Redundant servers with other HA servers.	• Define the Media Server HA Role and Associated Servers, page 17-9
Step 5	Configure the HA Advanced Storage options on the camera template.	• Configuring the Camera Template HA Options, page 17-12

Understanding Redundant, Failover, and Long Term Storage Servers

Table 17-2 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 17-2 on page 17-10.

w
Table 17-2 HA Server Types

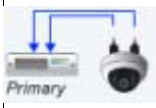
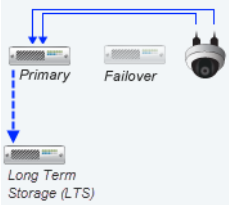
Media Server Type	Example	Description
Primary server	Both streams are sent to the Primary server only  	The *Primary* Media Server processes the camera video feeds, stores and plays back recorded video, among other tasks. **Usage Notes** • All Media Servers are assigned the Primary HA role by default. • 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	Stream A to Primary, Stream B to Redundant:  All Streams to Both Servers:  	A Redundant Media Server provides additional computing power for the cameras associated with a Primary server. • 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. **Note** See the "Configuring Multicast Video Streaming" section on page 12-11 for more information. **Usage Notes** • A *Redundant* 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 17-2 HA Server Types (continued)

Media Server Type	Example	Description
Failover server		A Failover Media Server is a hot standby server that assumes system control if the Primary server fails or goes offline. **Usage Notes** • The Failover server does not provide hot-standby functionality for the Redundant server. • See the "Understanding Failover" section on page 17-7 for more information.

Table 17-2 HA Server Types (continued)

Media Server Type	Example	Description
Long Term Storage (LTS) server		A Long Term Storage (LTS) server is used to back up continuous and motion event recordings to a separate server. • Both stream A and stream B can be backed up. • Backups are performed on an automatic schedule (for example, once a week at midnight). **Usage Notes** **Note** See the "Archiving Recordings to a Long Term Storage Server" section on page 17-16 for more information. • 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 *Retain* settings available in the camera or template configuration page (*Retain continuous recordings* and *Retain event recordings*). See the "Streaming, Recording and Event Settings" section on page 10-48. • 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 17-16 (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 2-27. • 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.

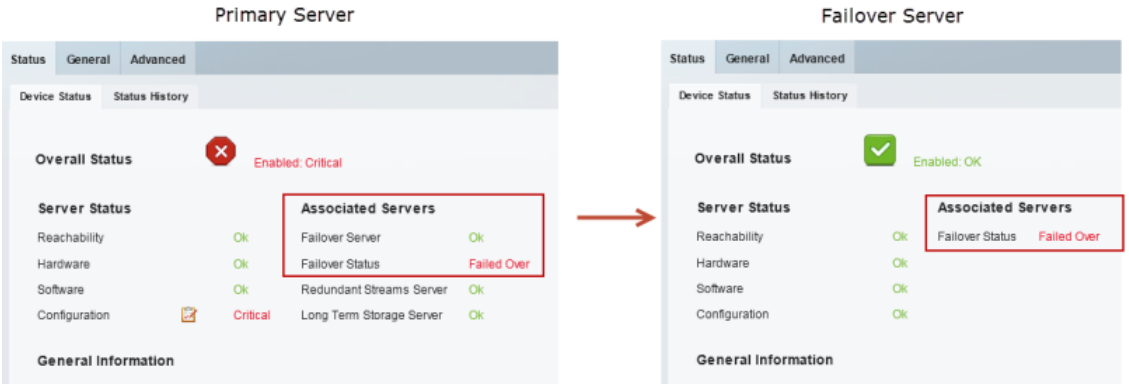
Failover status is indicated in the server Status page (Figure 17-1). The possible *Failover Status* values are:

- *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 17-1 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 17-1 Primary and Failover Server Status (in Failover)



Tip

See the Viewing the Server HA Status, page 17-22 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).
  - Co-located Media Server cannot be configured with Failover or Redundant Media Servers. Only a long term storage (LTS) server can be associated with a 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 9-1.

Step 4 Define the *Server Type*.

Note All Media Servers are assigned the Primary HA role by default.

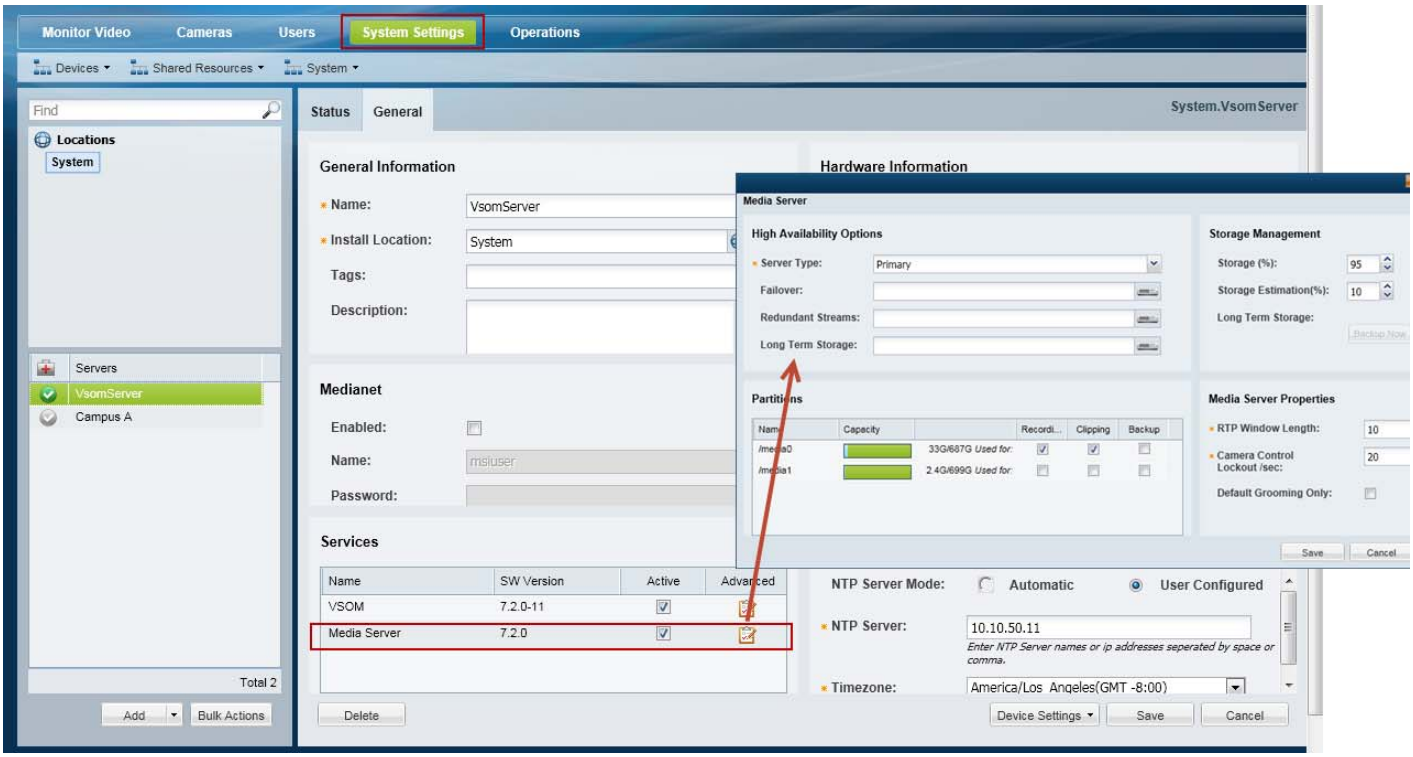
a. Select the server (**System Settings** > **Server**).

b. Click the **Advanced** icon for the Media Server service (Figure 17-2).

c. Select the *Server Type*.

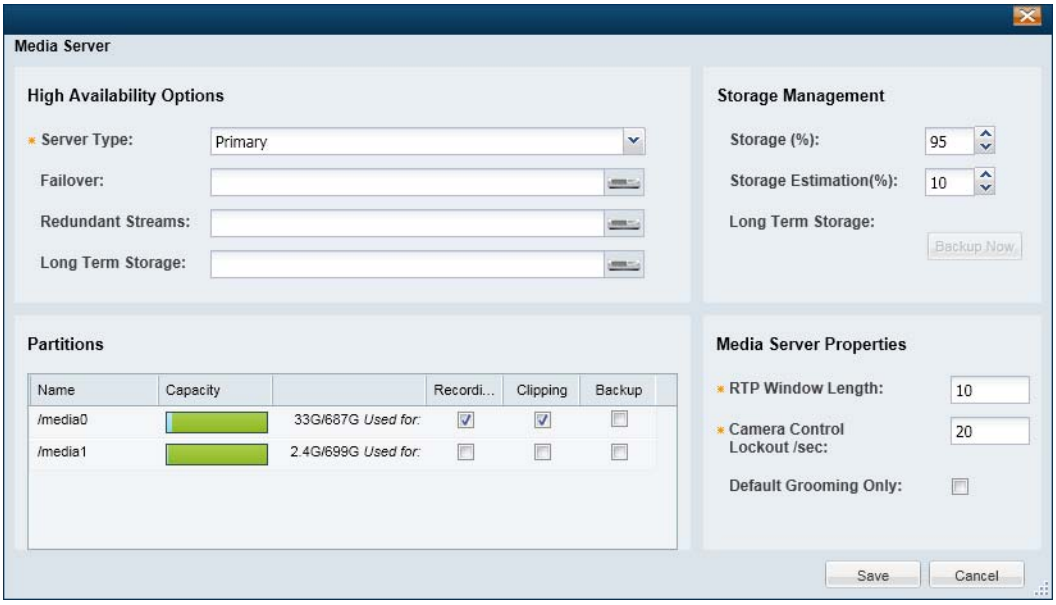
Tip See the "Understanding Redundant, Failover, and Long Term Storage Servers" section on page 17-4 for more information.

Figure 17-2 High Availability Options



Step 5 Associate the Primary server with the Failover, Redundant, or Long Term Storage Media Servers (Figure 17-3).

Figure 17-3 Defining the High Availability Server Type and Options



Primary	The server assigned to the camera or template. The *Primary* server processes the camera video feeds, stores and plays back recorded video, among other tasks.
Failover	(Primary server only) The Media Server that will assume the functionality of the Primary server if the Primary server goes offline.
Redundant Streams	(Primary server only) The server used to record, store, and server Redundant video streams. For example, the Redundant Streams server can be used to manage Steam B from a camera.
Long Term Storage	(Primary and Redundant servers only) The server used to store recorded video (continuous or motion events) for a long period of time.

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 17-3.
Step 2	Complete the "Configuring the Redundant and Failover Options" section on page 17-12.
Step 3	(Optional) Complete the "Archiving Recordings to a Long Term Storage Server" section on page 17-16.
Step 4	(Optional) Complete the "Defining the Recording Options" section on page 17-20.

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 17-4).

- 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 17-4 High Availability and Failover Options

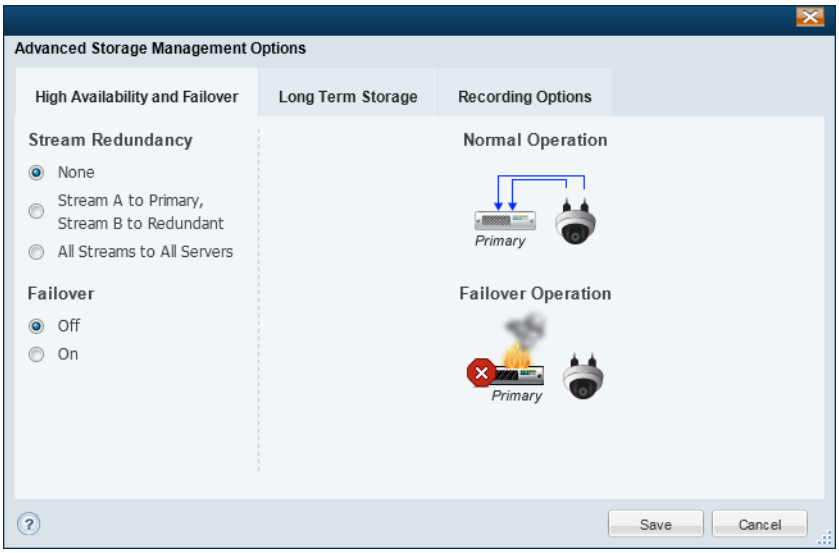


Table 17-3 describes the Stream Redundancy and Failover options for a camera or camera template. Select a *Stream Redundancy* option (as shown in Figure 17-4), and then turn the *Failover* option **On** or **Off**.

Table 17-3 Stream Redundancy Options With and Without a Failover Server

Option	Stream Redundancy	Failover Option
None	All live and recorded streams are sent to a single *Primary* server. If the Primary server fails, camera control, recording, and playback is disabled. 	If the *Primary* server fails or goes offline, the *Failover* server immediately assumes control (hot standby). 

Table 17-3 Stream Redundancy Options With and Without a Failover Server (continued)

Option	Stream Redundancy	Failover Option
Stream A to Primary, **Stream B to Redundant**	A camera's stream A video is sent to the *Primary* server. Stream B is sent to the *Redundant* server If the Primary server fails, the Redundant server still supports the camera stream B video, although it may be lower resolution.	If the *Primary* server fails or goes offline, the *Failover* server continues to support the camera's stream A video.
All Streams to All Servers	Both stream A and stream B (if configured) are sent to both the *Primary* and *Redundant* server. If the Primary server fails, both video streams are still supported by the *Redundant* server.	If the *Primary* server fails or goes offline, both stream A and stream B continue to be supported by two servers (the *Failover* and *Redundant*).

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 17-9.

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 17-9

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 17-4 on page 17-13).

Step 5 Select a *Stream Redundancy* option, as described in Table 17-3.

Step 6 Turn the *Failover* option **On** or **Off**, as described in Table 17-3.

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 17-6.

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 Backup in the Media Server Partition, page 17-16
- Configuring the LTS Server, page 17-17

Prerequisite: Enable *Backup* in the Media Server Partition

To archive recordings to an LTS server, you must enable backups on a Media Server partition (Figure 17-5). This setting specifies which hard disk partition will be used to store the archived recordings files.

Note The LTS server partition can only be used to backup recordings. Always deselect the **Recording** and **Clipping** options, or an error will occur. The LTS server cannot be used as a primary store of recording data.

Procedure

Step 1 Select **System Settings > Servers**.

Step 2 Select the location and then select the LTS Media Server.

Step 3 Select the **General > System** tab.

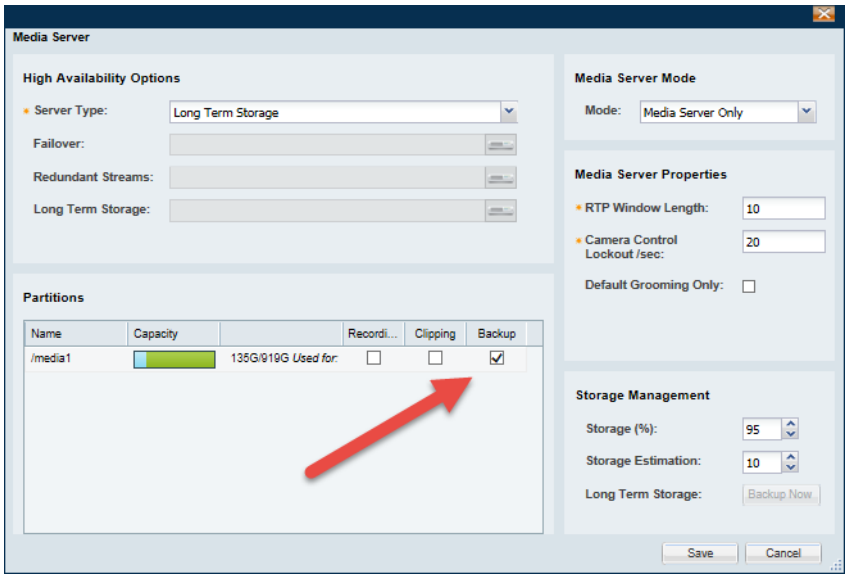
Step 4 Under Services, click the **Advanced** icon next to **Media Server**.

Step 5 Under *Partitions* (Figure 17-5), select **Backup** for the */media1* or */media0* repository.

Step 6 Deselect the **Recording** and **Clipping** options for all partitions (or an error will occur).

Step 7 Click **Save**.

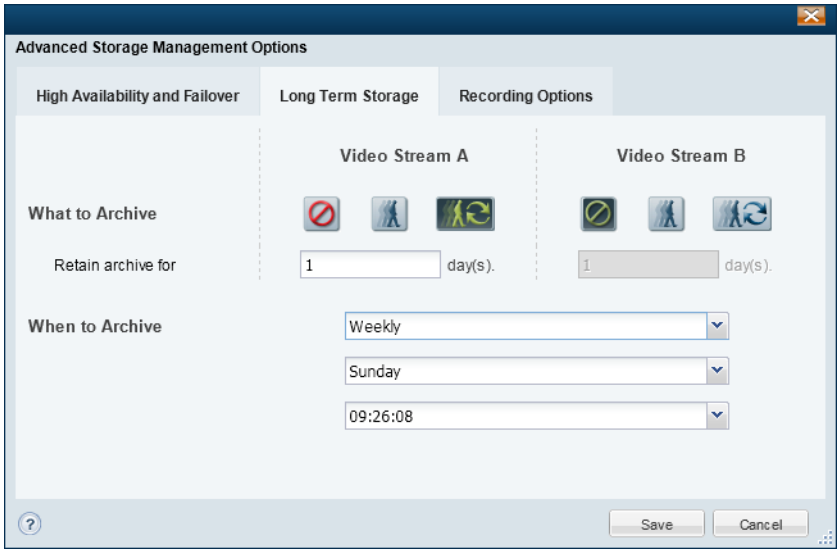
Figure 17-5 Media Server Partitions



Configuring the LTS Server

Click the **Advanced Storage** option in a camera or template and select **Long Term Storage** (Figure 17-6). 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 17-6, Video Stream B is disabled since the template is not configured to record video.

Figure 17-6 Long Term Storage Options



The following table describes the Long Term Storage Settings:

Table 17-4 Long Term Storage Options

Field	Description
What to Archive	Select the following for video stream A and B: • —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	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. **Note** If the disk capacity of the LTS server is exceeded, the oldest recording is deleted to provide room for the newest recording.
When to Archive	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. • **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 17-9.

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 17-9

Step 2 Configure the Store Partition on the LTS Server.

- Prerequisite: Enable Backup in the Media Server Partition, page 17-16

Step 3 Choose **Cameras** and add or edit a camera or camera template.

- Adding and Managing Cameras, page 10-1

Step 4 Select the **Streaming, Recording and Events** tab and configure recording.

- Configuring Continuous, Scheduled, and Motion Recordings, page 12-7

Step 5 Click **Advanced Storage**.

Step 6 Click the **Long Term Storage** tab (Figure 17-6 on page 17-17).

Step 7 Select the options for Stream A and Stream B (Figure 17-6 on page 17-17).

Step 8 Click **Save**.

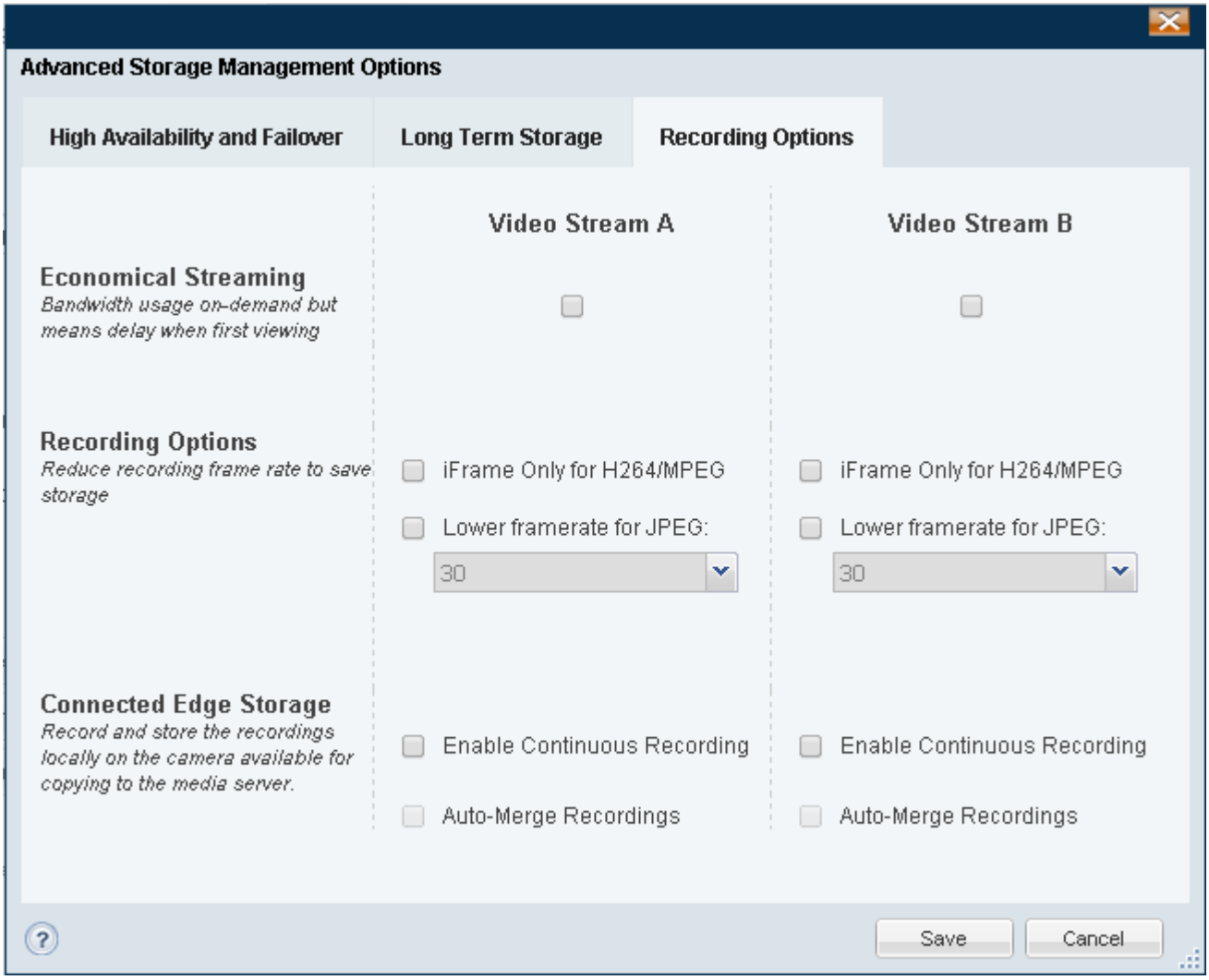
Defining the *Recording Options*

The *Recording Options* can be used to reduce the bandwidth and processing requirements for streaming and recording video, or to enable on-camera recordings that can be (optionally) transferred to the Media Server.

Select a template and click **Advanced Storage > Recording Options** (Figure 17-7) to define the following options.

- Economical Streaming, page 17-21
- Recording Options, page 17-21
- Connected Edge Storage (Enabling Recording On Cameras), page 15-8

Figure 17-7 Recording Options



Economical Streaming

Select the **Economical Streaming** option to place the secondary stream in suspended mode (Figure 17-7). 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 17-7).

See the "Configuring the Redundant and Failover Options" section on page 17-12 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.

Connected Edge Storage

See the "Connected Edge Storage (Camera Recording)" section on page 15-1 for information on using this feature.

Specifically, see the Connected Edge Storage (Enabling Recording On Cameras), page 15-8.

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.

- See the "Logging In" section on page 1-18.

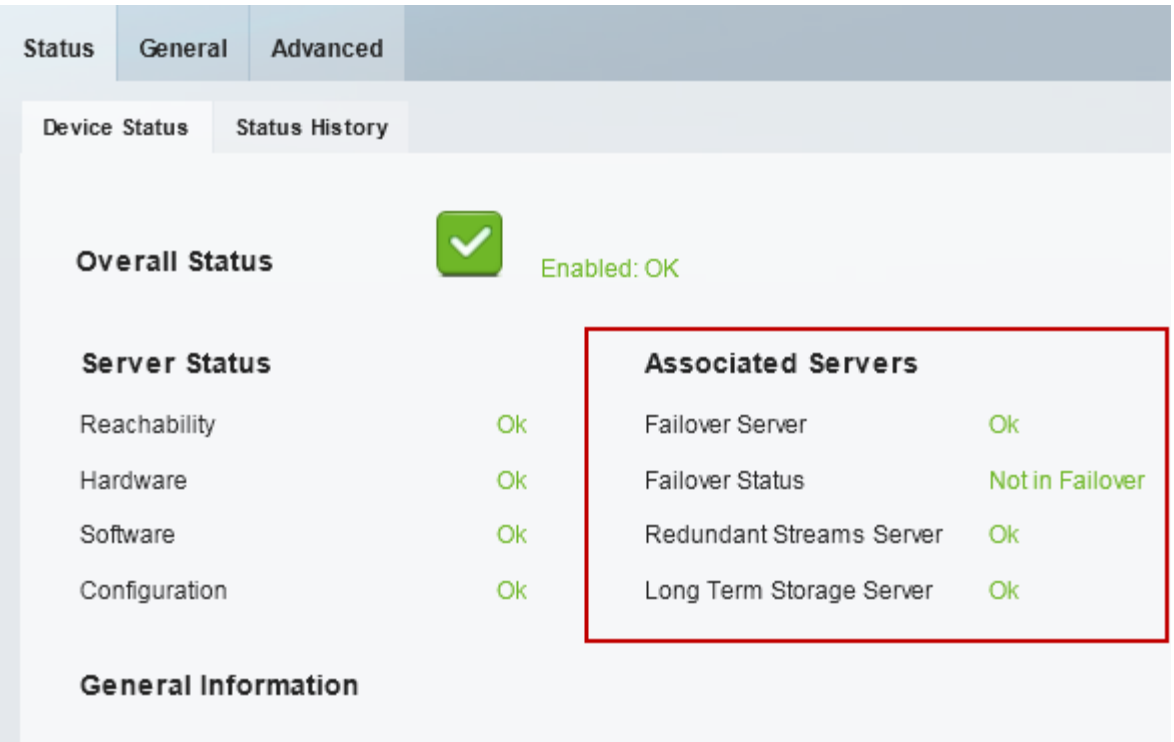
Step 2 Select the Media Server or camera to edit (click **Cameras** or **System Settings** > **Media Servers** and select the device).

Step 3 Click the **Status** tab.

Step 4 Review the status of the current server and associated servers. For example:

- Figure 17-8: An example of a Primary Server and associated HA servers
- Figure 17-9: Examples of the Status Pages for each HA Server Type.
- See also Figure 17-1 on page 17-7 for an example of the Primary and Failover Status pages when a failover occurs.

Figure 17-8 Primary Server Status Including Associated Servers

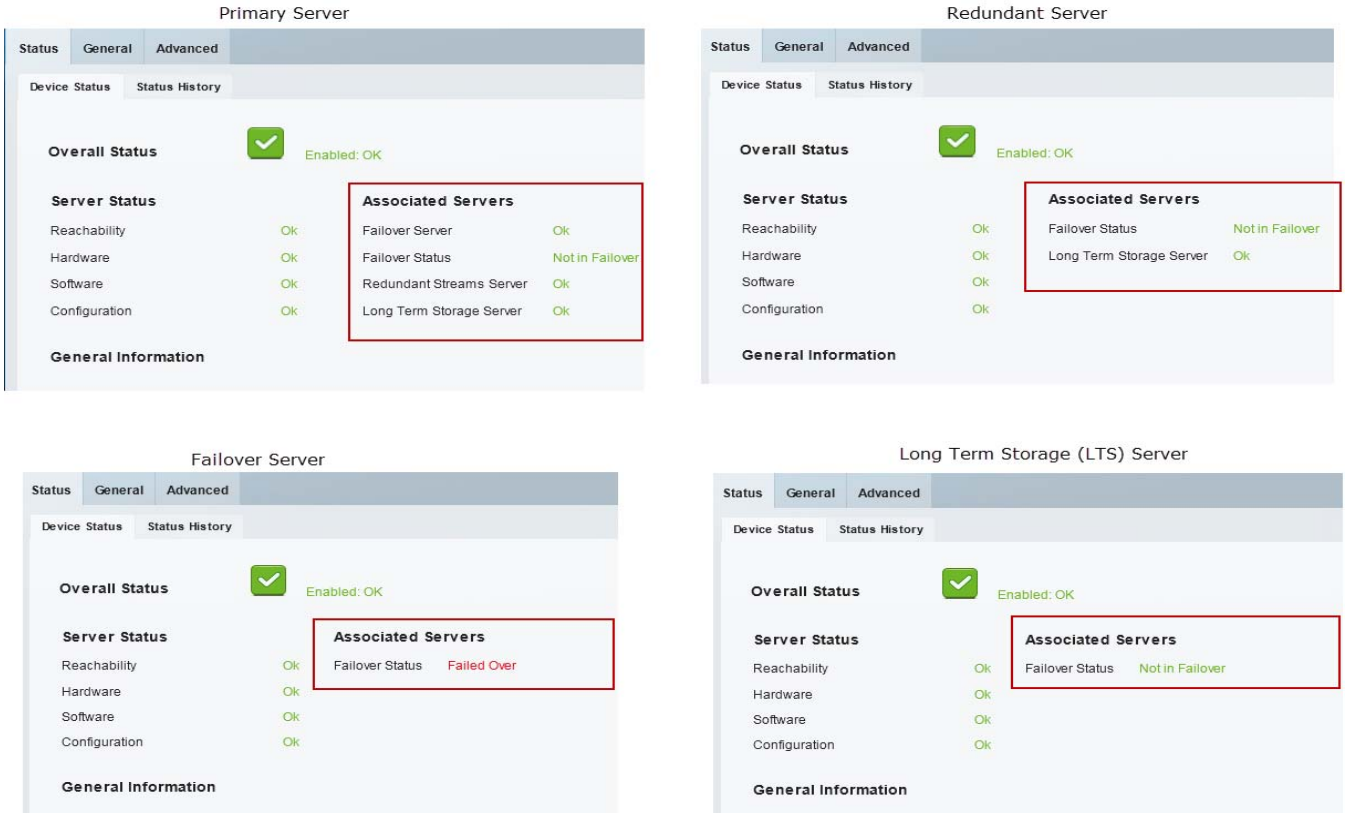


Field	Description
Overall Status	The status of the current server. See the "Understanding the Overall Status" section on page 19-9 for more information.
Associated Servers (the HA servers associated with the current server)	
Failover Status	The Overall Status of the failover server. See the "Understanding the Overall Status" section on page 19-9 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: • *In Failover* • *Not In Failover* • *Could Not Failover* (this occurs if a different Primary server already failed over to the same Failover server.) See the "Understanding Failover" section on page 17-7 for more information.
Redundant Streams Server	The Overall Status of the Redundant server that is associated with the Primary server. A *Redundant* 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	The Overall Status of the Long Term Storage server associated with the Primary or Redundant server. A *Long Term Storage* 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.

Open the **Status** page for each HA server to view additional information about the overall status and HA status of that server (Figure 17-9).

Figure 17-9 Examples of HA Server Status



Server Status	Description
Primary server	The status of the HA servers associated with the Primary server.
Failover server	The status of the Failover server as a hot standby. 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". See the "Understanding Failover" section on page 17-7 (and Figure 17-1) for more information.

Server Status	Description
Redundant server	The Failover server status, and the LTS server status. A *Redundant* server can support multiple servers. You must ensure that the Redundant server contains the disk and processing capacity to support all associated Primary servers.
Long Term Storage server	The Failover server status. A *Long Term Storage* 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.

Operations Manager High Availability

Two Operations Manager servers can be configured as a redundant pair for high availability (HA). Since the Operations Manager is responsible for configuring and coordinating the entire Cisco Video Surveillance deployment, this helps ensure uninterrupted system access for users and administrators.

To configure Operations Manager HA, install two servers: a Master server and a second Peer server. All configurations, data, and logs on the Master server are automatically replicated on the Peer server. If the Master server goes down or is unavailable, the Peer server is ready to take control with minimal impact.

Note If an HA failover occurs, the Peer server becomes the Master, and retains that role even if the other server comes back online (and assumes the Peer role).

Review the following topics for more information:

Contents

Overview

Review the following topics before configuring Operations Manager HA.

Understanding Operations Manager HA

Operations Manager HA is achieved by installing two stand-alone Cisco VSM Operations Manager servers, and configuring one as the Master server, and the other as the Peer server (Figure 18-1). A virtual IP address is shared by both servers, and used by users (video monitors, administrators and other users) to access the Cisco Video Surveillance system.

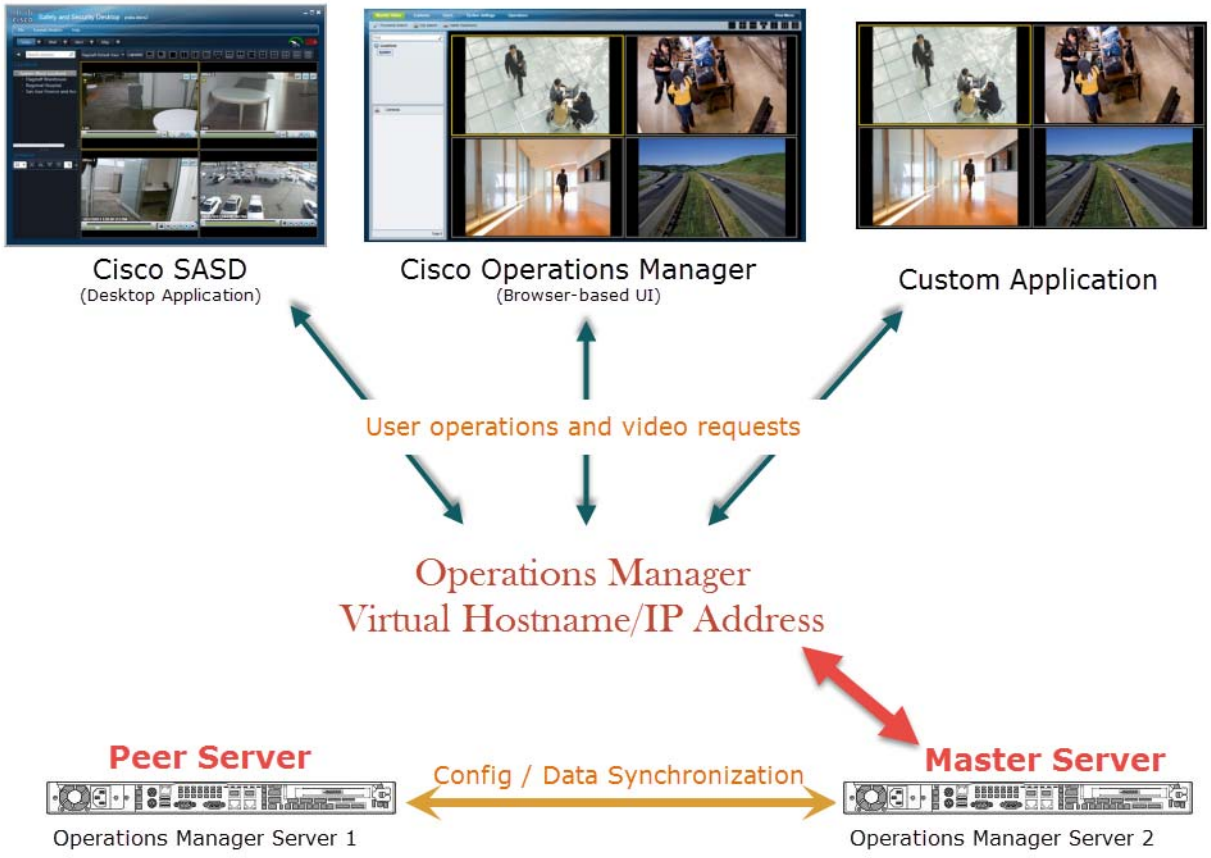
Figure 18-1 Operations Manager HA: Server 1 is the Master Server

In Figure 18-1, users enter the virtual hostname/IP address to connect to the Cisco VSM Operations Manager. Server 1 acts as the Master server, receiving and managing all user and system requests. All data and configuration changes are automatically synchronized with the Peer server (server 2) to ensure it is ready to take over if a failover occurs.

The Peer polls the Master server regularly to verify connectivity. If the Peer does not receive a response, the Master is assumed to be down or offline and the Peer assumes the Master role (Figure 18-2). The Peer server immediately takes control of the system, and the virtual hostname/IP address is redirected to the new Master server.

Note In the Figure 18-2 example, Server 1 assumes the Peer role when it comes back online, and retains that role until another failover occurs (admins can also force a failover if necessary).

Figure 18-2 After Operations Manager Failover: Server 2 is the Master Server



User Interfaces

The following user interfaces (UIs) access Cisco VSM video using the shared virtual IP address:

- Operations Manager (browser-based UI)—enter the virtual hostname/IP address in a Internet Explorer browser window.
- Cisco SASD (desktop application)—enter the virtual hostname/IP address at the login prompt.

- Custom applications—monitoring applications that use the Cisco VSM APIs access the Operations Manager using the virtual hostname/IP address.

Requirements

a. Before you configure Operations Manager HA, verify that the following requirements are met.

Note The **VSOM High Availability** configuration page appears only if the server is a stand-alone Operations Manager and is running a supported OS (such as RHEL 6.4).

Table 18-1 Requirements

Requirements	Requirement Complete? (✓)
To configure Operations Manager HA, admins 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.	❑
Two standalone physical or virtual servers must be installed on the network. – Supported physical servers: CPS-UCS-1RU-K9 or CPS-UCS-2RU-K9 – Supported virtual machines: VMs deployed using the Cisco VSM release 7.5 or 7.6 OVA templates. **Note** Any data on the server used as the Peer server will be deleted and replaced with the data from the Master server.	❑
We recommend two CPS-UCS-2RU-K9 servers for best performance. • Performance issues can occur using the CPS-UCS-1RU-K9 servers for Operations Manager HA since performance issues (such as slowness) may occur. • Do not mix a CPS-UCS-2RU-K9 server with a CPS-UCS-1RU-K9 server.	❑
Additional server requirements and recommendations: • Stand-alone servers—Only stand-alone physical or virtual servers are supported in an HA configuration. The Operations Manager servers can not be co-located with other server services, such as a Media Server. • Operating system—Red Hat 6.4 64 bit OS only (SUSE and Red Hat 5.8 are NOT supported). • We recommend that both servers have the same hardware specifications such as processor, hard disk storage, and other attributes. For example, two CPS-UCS-2RU-K9 servers. • We do not recommend using Cisco UCS E-series platform servers for Operations Manager HA. • Both servers used for HA must be fully up and running prior to configuring HA or replacing the Peer server. Verify that there are no pending jobs (of any kind) in the Peer server.	❑
Split Brain recovery support: • At least one Media Server must be added to the Split Brain Configuration to support recovery if communication between the Master and Peer server is lost. • See Resolving a Split Brain Scenario, page 18-20.	❑

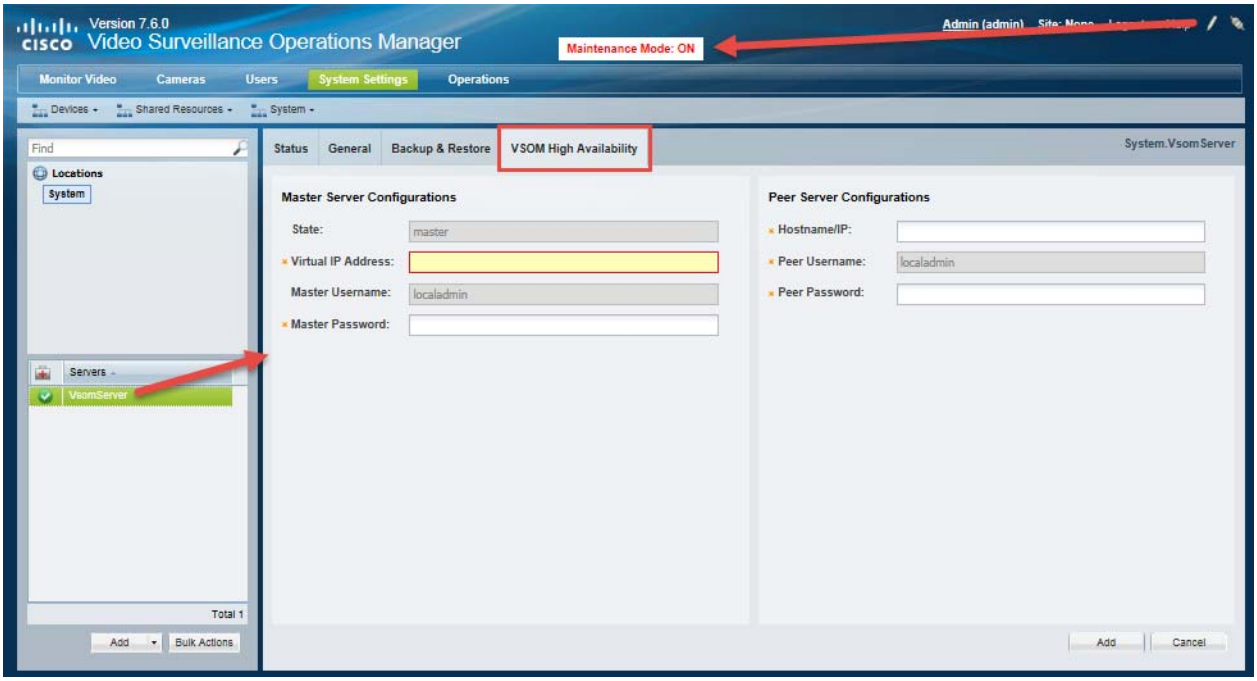
Table 18-1 Requirements

Requirements	Requirement Complete? (✓)
Network requirements: • Subnet—Both servers must be in the same network subnet. This ensures connectivity and data synchronization between the servers. • NIC port—Both servers must be connected to the network using the same NIC port: for example, Eth0. Only a single Ethernet port can be active (either Eth0 or Eth1). • Three IP addresses/hostnames are required: – An IP address/hostname for the Master server Ethernet (NIC) port. – An IP address/hostname for the Peer server Ethernet (NIC) port. – A virtual IP address that is shared by both servers. **Note** End-users should always use the virtual IP address to access the Operations Manager since it will still work even in a failover occurs. Users should never use the server Ethernet port (NIC) address since connectivity can be lost if the server is unreachable.	❑
Security certificate requirements: By default, all Cisco VSM server include a self-signed certificate. Using the self-signed certificate on the Operations Manager server causes a security warning to appear when users log in the Operation Manager. To avoid this, you can create and install a web server certificate for the Operations Manager servers. The certificate must point to the HA virtual IP address and be installed on both Operations Manager servers (Master and Peer) used in the HA configuration. For more information: • Configuring Operations Manager HA, page 18-6 • Cisco Video Surveillance Management Console Administration Guide for instructions to install the certificate. • Resolving a "Server Unreachable" Error During Force Failover, page 18-33	❑
Network Time Protocol (NTP) server: All servers must be configured with the same NTP configuration to ensure the time settings are accurate and identical. See the "NTP Information" section on page 6-14 for more information.	❑
Passwords: • The Management Console password for Operations Manager each server. This is the *localadmin* password used to access the Cisco VSM Management Console, and is set during the initial server setup. • The admin password used to access the browser-based Operations Manager interface.	❑

Configuring Operations Manager HA

To configure Operations Manager HA, select the stand-alone Operations Manager server VSOM High Availability tab (Figure 18-2) for the server that initially have the Master role. Enter the virtual IP address, Peer server address, and server passwords, and click **Add**.

Figure 18-3 Operations Manager HA Configuration

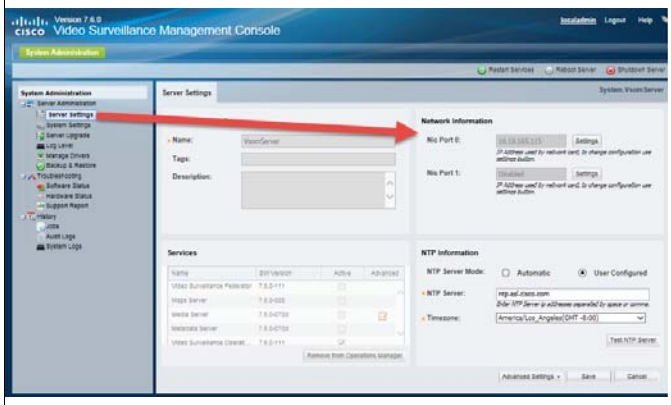


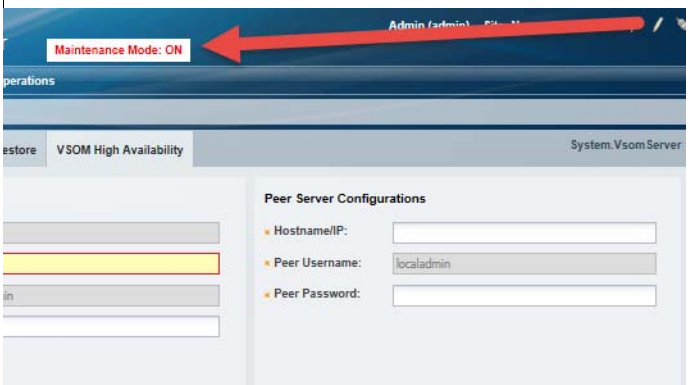
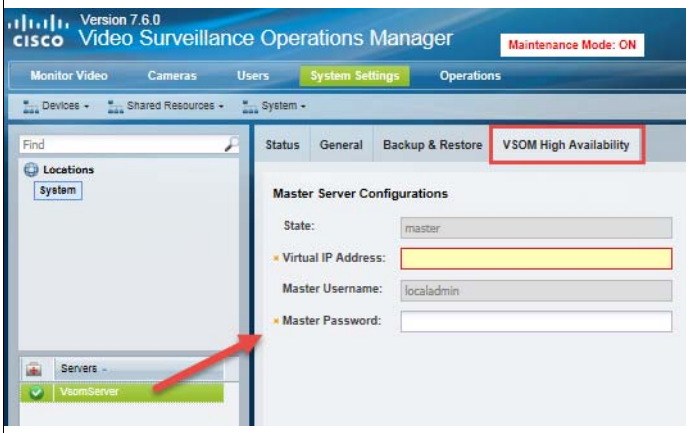
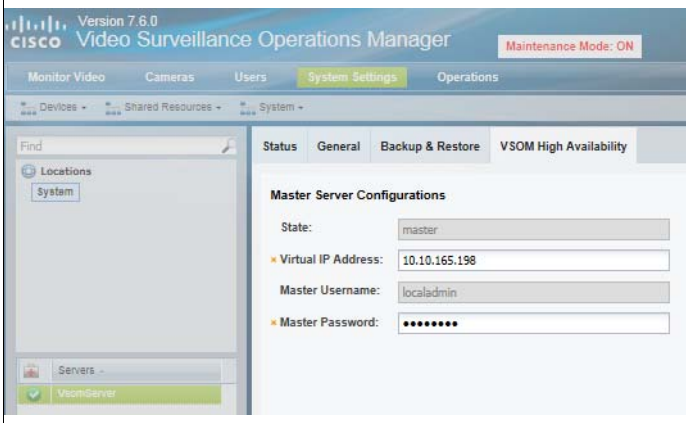
Note Before configuring Operations Manager HA, see Troubleshooting Operations Manager HA, page 18-26 for common problems that can occur. For the most recent up-to-date information, see the Cisco VSM Operations Manager High Availability Troubleshooting Guide.

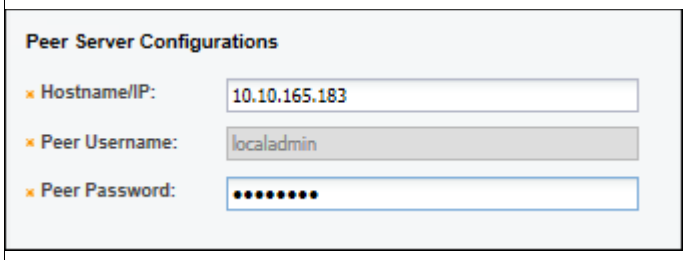
Procedure

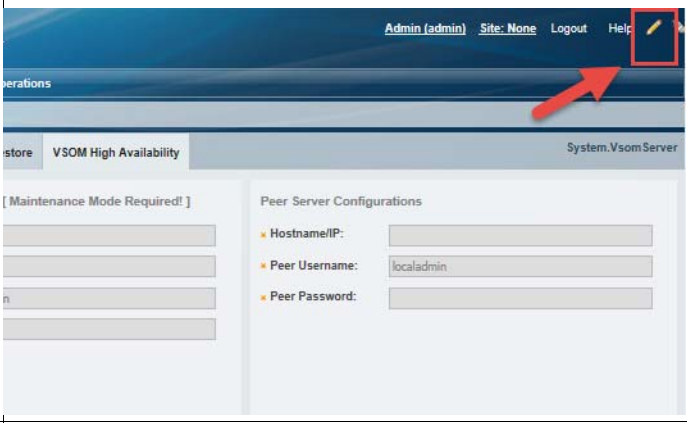
To configure Operations Manager HA, complete the following tasks:

	Task	Related Information
Step 1	Verify that all requirements are complete.	Requirements, page 18-4
Step 2	Notify users that most user configurations will not be allowed while the system is in maintenance mode.	Users will be able to view video and data but not change configurations (such as adding cameras, updating servers, modifying templates, or adding users.

	Task	Related Information
Step 3	Install two stand-alone Operations Manager servers, either physical or virtual: **a.** Both Operations Manager servers must be on the same network subnet. **b.** Both servers must be stand-alone Operations Manager servers (no other server services can be enabled).	See the following related documentation: • Cisco Physical Security UCS Platform Series User Guide • Cisco Multiservices Platform for Physical Security User Guide • Cisco Video Surveillance Management Console Administration Guide
Step 4	Create and install a custom security certificate, if required. The certificate must point to the virtual IP address and be installed on both HA servers. **a.** Obtain a signed certificate by a Certification Authority. This certificate should contain the host name mapped to the virtual IP. For example: *vsom-server3*. **b.** Install the certificate on both the Master and Peer servers using the Cisco Video Surveillance Management Console. For example *vsom-server1 and vsom-server2*. **c.** Wait for the services to be restarted. **d.** Log in again to the Operation Manager using the virtual IP address. The certificate error should not appear.	See the Cisco Video Surveillance Management Console Administration Guide for instructions to install the web server certificate on the servers.
Step 5	Gather the following information for each server: • Server password (used to access the Cisco VSM Management Console). • NIC port and IP address for network access. **Note** The username/password are the credentials used to access the Console UI, NOT the Operations Manager UI. Only a single Ethernet interface can be active for both servers, and it must be the same port. For example, both servers must use either Eth0 or Eth1.	For example: • Server 1 uses the Eth0 port and is configured with IP address 10.10.53.225. The Management Console username and password are **localadmin**/*password*. • Server 2 also uses the Eth0 port and is configured with IP address 10.10.53.224. The Management Console username and password are **localadmin**/*password*. See the following related documentation: • Cisco Video Surveillance Management Console Administration Guide 

	Task	Related Information
Step 6	Log in to the stand-alone Operations Manager server that will have the Master role.	"Logging In and Managing Passwords" section on page 1-18
Step 7	Click the pencil icon in the title bar to place the server in maintenance mode . **Note** The icon is grey when maintenance mode is on, meaning most user configuration will be rejected (only system tasks and logging are allowed). Maintenance mode locks the server configuration so changes cannot be made by other users. This keeps the server config in a stable state while the device is added to the HA config. See Understanding Maintenance Mode, page 1-31.	
Step 8	Open the server's **VSOM High Availability** tab. **a.** Go to **System Settings** > **Servers**. **b.** Select a location and the stand-alone Operations Manager that will be the Master server (for example: **VsomServer**). **c.** Click the **VSOM High Availability** tab. **Note** The VSOM High Availability tab appears only if the server is a stand-alone Operations Manager and is running a supported OS (such as RHEL 6.4).	
Step 9	Enter the **Master Server Configurations**: • **State**—(read-only) The server's HA role (Master or Peer). • **Virtual IP Address**—The IP address used by operators to log in. This address remains the same even if the servers fail over and switch the Master role. • **Master Username**—(read-only) The Management Console username is *localadmin* and cannot be changed. • **Master Password**—The password used to access the Management Console for the physical or virtual server.	

	Task	Related Information
Step 10	Enter the **Peer Server Configurations** for the second stand-alone Operations Manager server. • **Hostname /IP Address**—The IP address or hostname for the NIC used for network access. This address is configured using the Management Console. • **Peer Username**—(read-only) The *localadmin* Management Console username cannot be changed. • **Peer Password**—The password used to access the Management Console for the physical or virtual server. **Usage Notes** • If the fields are grey (read-only), verify that the Master server is in maintenance mode (see Step 7). • The Peer server must be installed and available on the network or the HA configuration will fail. • Any data on the Peer server will be deleted and replaced with the data from the Master server.	• Cisco Video Surveillance Management Console Administration Guide • Configuring Servers, page 6-1 
Step 11	Click **Add** and then **OK** to confirm the changes.	The server must be in maintenance mode for the changes to be accepted (see Step 7).
Step 12	(Optional) Modify the servers in the **Split Brain Configuration**. **Usage Notes** • At least one server must be selected to support Split Brain recovery. • Up to 3 Media Servers are automatically added to the Split Brain Configuration. • If no Media Servers are available, all fields will be blank, and Split Brain recovery will not be supported. Add the Media Server(s) to the deployment and then add them to the Operations Manager HA Split Brain Configuration. You can also add or modify the Media Servers after the Operations Manager HA setup is complete. See Adding the "Split Brain" Media Servers, page 18-21.	• Resolving a Split Brain Scenario, page 18-20 • Adding the "Split Brain" Media Servers, page 18-21 

	Task	Related Information
Step 13	On the Master server, click the grey pencil icon in the title bar to turn maintenance mode OFF. The HA fields are read-only when maintenance mode is off. The icon is yellow , meaning user configuration changes can be saved. See Understanding Maintenance Mode, page 1-31.	
Step 14	Re-log in to the Operations Manager using the virtual IP address.	Users logged in to the virtual IP address will interact with whichever server has the Master role. This ensures that any additional configuration changes are replicated on both servers (Master and Peer).
Step 15	Verify that the default Peer server name appears in the server list. **a.** Go to **System Settings** > **Servers**. **b.** Select a location. **c.** Verify that both the Master and Peer server names appear in the server list.	The default Peer server name is automatically generated. Select the name and click the **General** tab to change the server name.
Step 16	(Optional) Change the Peer server name: • Select the **General** tab. • Select the Peer server name. • Enter a new name and click **Save**. For example, "VSOM server 2". **Tip** Do not use server names with "master", "peer", "primary", "standby" etc, since the HA role can change when a failover occurs.	• Viewing Server Status, page 6-29 • General Information Settings, page 6-10
Step 17	Add at least one additional Cisco Media Server for the system to support video surveillance.	Since both Operations Manager servers must be stand-alone servers, additional servers must be added. See the "Configuring Servers" section on page 6-1
Step 18	Add at least one Media Server to the **Split Brain Configuration**, if necessary. **Usage Notes** The Split Brain Configuration fields will be blank if no Media Servers were available when Operations Manager HA was set up. If this happens, add the Media Servers to the Operations Manager HA after the servers are available.	• Resolving a Split Brain Scenario, page 18-20 • Adding the "Split Brain" Media Servers, page 18-21 

Managing the HA Configuration

Understanding the Server Management Options

To manage the Operations Manager HA servers, log in to the Operations Manager virtual IP address or hostname. All configuration changes and actions affect the Master server, and are automatically replicated on the Peer server.

Note Do not use the Cisco VSM Management Console to change the configuration for either server unless necessary. Changes made using the Management Console interface may not be replicated in the HA configuration.

Some configuration tasks require that the server be in Maintenance Mode. See Understanding Maintenance Mode, page 1-31 for more information.

To view the Status or alerts for either server, select **System Setting > Server**, select the Master or Peer server from the list, and select the **Status** page.

Information and Options Available on the Peer Server

If you select the Peer server from the server list, you can view server Status, change the server name, and view information about the HA configuration. No other configuration tasks or fields are enabled. All other changes must be made on the Master server.

Revising the Operations Manager HA Configuration

To change the HA configuration, such as changing the virtual IP address, or changing the server login credentials, access the Master server HA configuration page, enter the new configurations and save the changes.

Procedure

Step 1 Access the Master server:

a. Log in to the Operations Manager using the virtual IP address / hostname.

b. Click the pencil icon in the top right to turn maintenance mode ON.

– The icon is grey when maintenance mode is ON. Maintenance mode places the servers in a stable state and prevents other users from making most changes while high-availability tasks are performed. See Understanding Maintenance Mode, page 1-31 for more information.

c. Select **System Settings** > **Servers**.

d. Select the **Master** server from the list.

e. Select the **VSOM High Availability** tab.

Step 2 Enter the revised configuration as necessary.

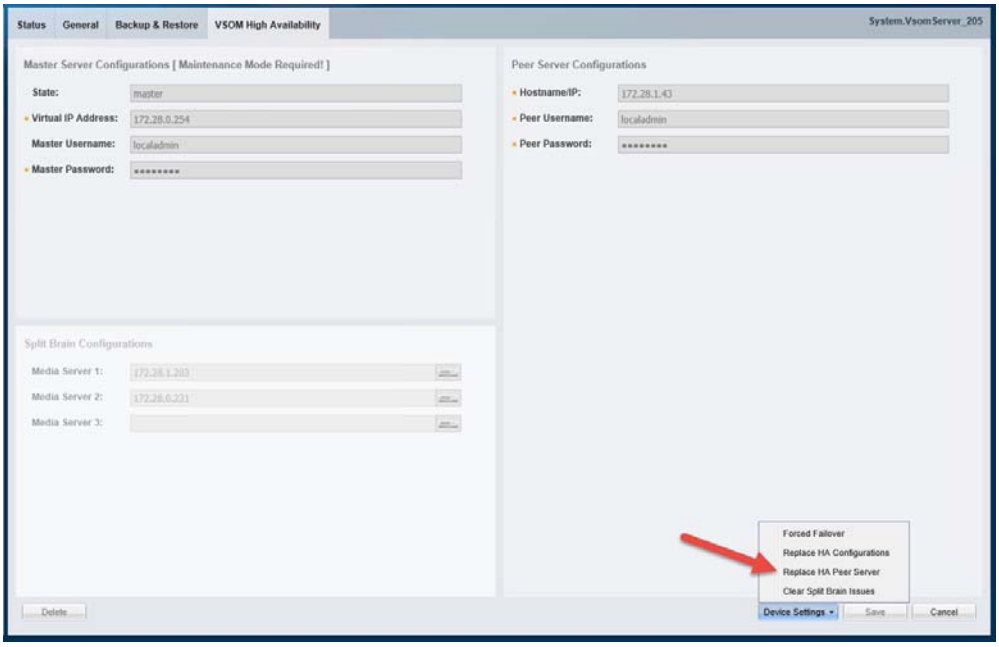
Step 3 Click **Save** and follow the on-screen prompts.

Step 4 Wait for the job to complete.

Replacing the HA Configuration

An HA configuration mismatch occurs when the configuration on the Master is out of sync with the Peer server. Use the following procedure to replace the entire configuration (which replaces the configuration on the Peer server with the version on the Master server).

Figure 18-4 Replacing the HA Configuration



Procedure

To replace the HA configuration, do the following:

Step 1 Access the Master server:

a. Log in to the Operations Manager using the virtual IP address / hostname.

b. Click the pencil icon in the top right to turn maintenance mode ON.

– The icon is grey when maintenance mode is ON. See Understanding Maintenance Mode, page 1-31 for more information.

c. Select **System Settings** > **Servers**.

d. Select the **Master** server from the list.

e. Select the **VSOM High Availability** tab (Figure 18-4).

Step 2 Select **Device Settings** > **Replace HA Configuration**.

Step 3 Click **OK** and wait for the job to complete.

Step 4 Select the server Status tab to verify that the problem is resolved.

Step 5 (Optional) If a configuration mismatch remains, you can replace the configuration on the Peer server with the version on the Master server. See the "Replacing the HA Configuration" section on page 18-12.

Step 6 On the Master server, click the grey pencil icon in the title bar to turn maintenance mode OFF.

- The icon is yellow when maintenance mode is off, meaning user configuration changes can be saved.

Deleting the HA Configuration

Deleting the HA configuration removes the Peer Operations Manager server from the HA config. the Cisco VSM will operate with a single Operations Manager server (no HA).

To delete the Operations Manager HA config, delete the Peer server.

Procedure

Step 1 Log in to the system using the virtual IP address.

Step 2 Verify that the server you want to keep as the Operations Manager for the system is in the Master state:

Step 3 Delete the HA configuration:

a. Select **System Settings** > **Servers**.

b. Click the pencil icon in the top right to turn maintenance mode ON. The icon is grey when maintenance mode is ON.

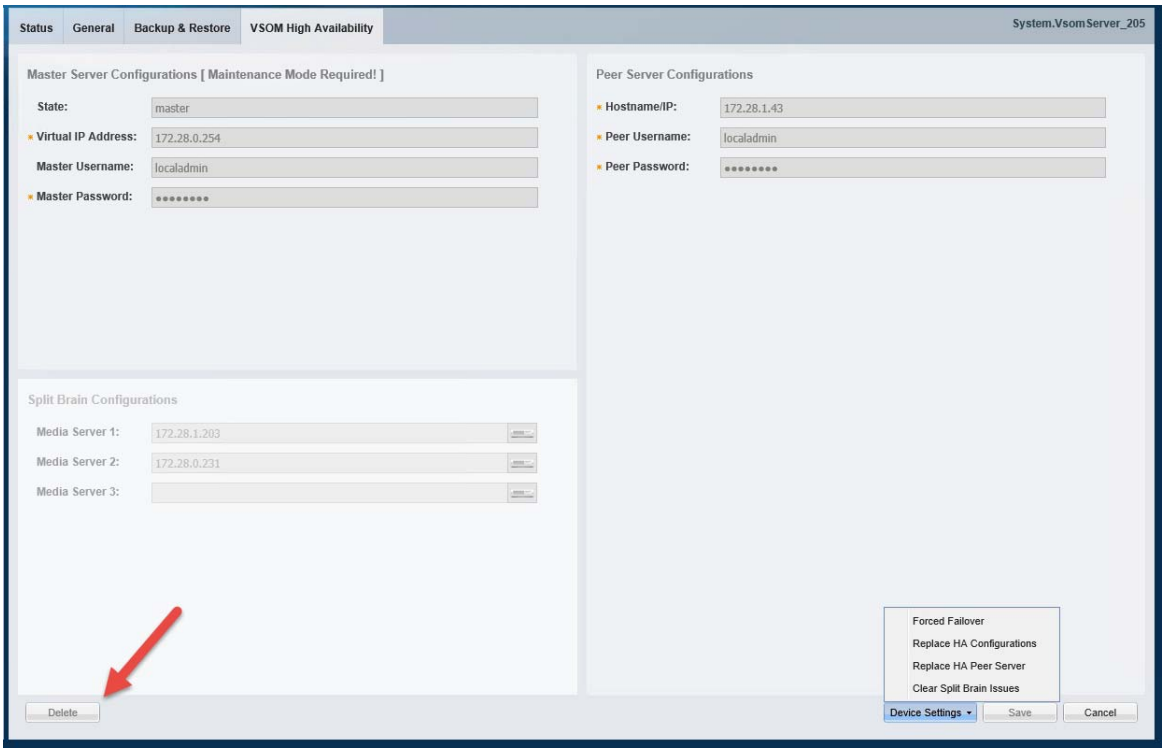
c. Select the **Master** server from the list.

d. Select the **VSOM High Availability** tab.

e. Click **Delete** (Figure 18-5).

f. Click **OK**.

Figure 18-5 Deleting the HA Configuration



Step 4 The Peer server is removed from the Operations Manager configuration.

Step 5 Click the grey pencil icon in the title bar to turn maintenance mode OFF.

- The icon is yellow when maintenance mode is off, meaning user configuration changes can be saved.

Step 6 (Optional) To re-use the Peer server in another role:

a. Log in to the Management Console for the Peer server that was removed.

b. Assign different server services to the server that are not Operations Manager (for example, Media Server, Maps or Metadata). Only a single Operations Manager can be used in a Cisco VSM system, unless configured for HA.

c. Add the modified server to the Operations Manager configuration, as described in the "Configuring Servers" section on page 6-1.

Replacing the HA Peer Server

To replace a Peer server with a different physical or virtual server, use the **Device Settings > Replace HA Peer Server** option. The replacement server must be installed and available on the network. The old Peer server can be reconfigured for a different server status, or removed.

Procedure

Step 1 Install a replacement stand-alone Cisco VSM Operations Manager server on the network.

Step 2 Access the Master server:

a. Log in to the Operations Manager using the virtual IP address / hostname.

b. Click the pencil icon in the top right to turn maintenance mode ON.

– The icon is grey when maintenance mode is ON. See Understanding Maintenance Mode, page 1-31 for more information.

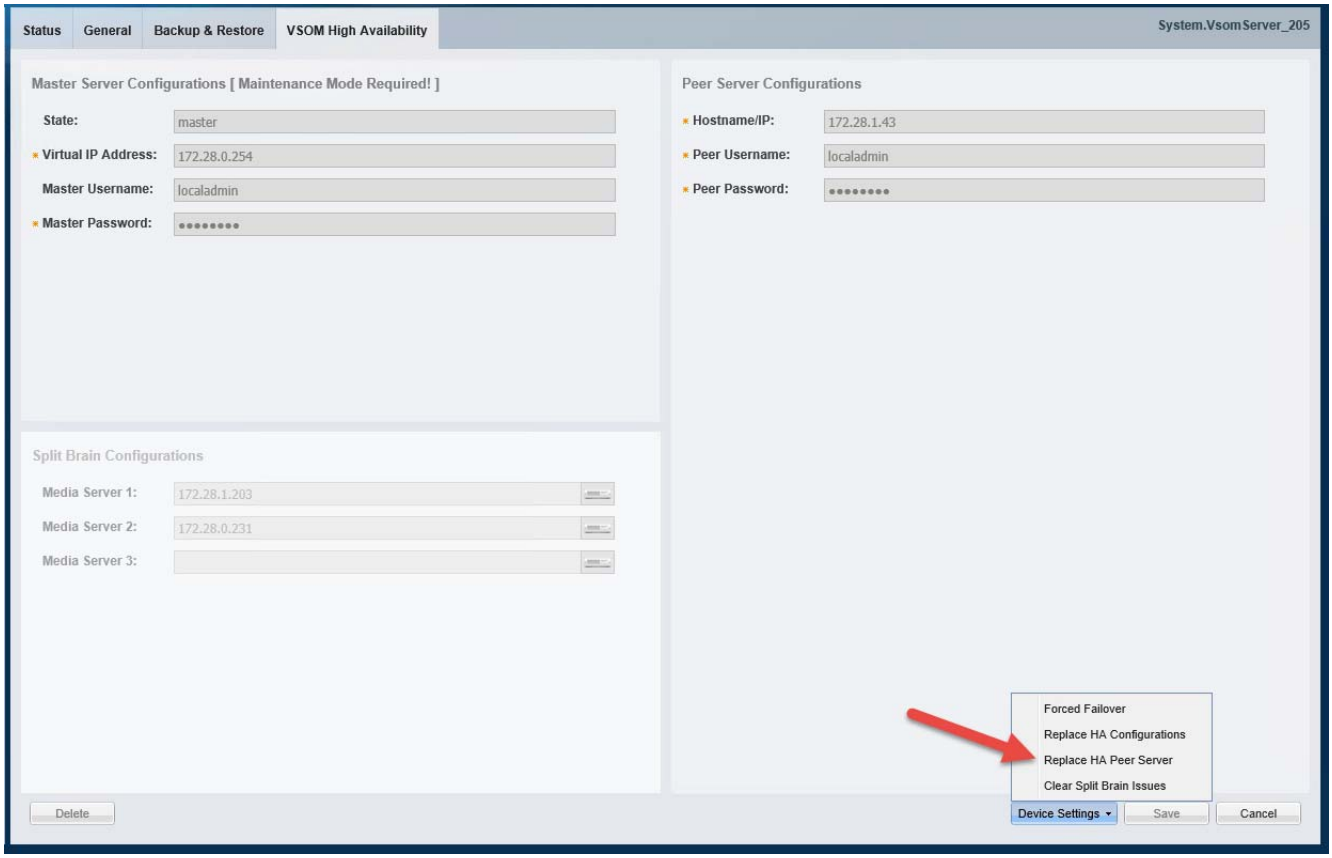
c. Select **System Settings** > **Servers**.

d. Select the **Master** server from the list.

e. Select the **VSOM High Availability** tab.

Step 3 Click **Device Settings** > **Replace HA Peer Server** (Figure 18-6).

Figure 18-6 Replacing the Peer HA Server



Step 4 Click **OK**.

Step 5 Wait for the process to complete and for the Master server data to be replicated on the new Peer server.

Step 6 Re-login to the virtual IP address / hostname, if necessary.

Step 7 On the Master server, click the grey pencil icon in the title bar to turn maintenance mode OFF.

- The icon is yellow when maintenance mode is off, meaning user configuration changes can be saved.

Backing Up and Restoring the Operations Manager Configuration

Backup operations are only supported on the server that has the Master role. All backup data is automatically synchronized with the Peer server.

Restore operations can only be performed on a non-HA (stand-alone) server. To restore data from a previous backup, you must delete the HA config, restore the backup, and re-create the HA config.

Refer to the following topics for more information:

- Backing Up the Master Operations Manager, page 18-16
- Restoring a Stand-Alone Operations Manager Server, page 18-16

Backing Up the Master Operations Manager

To back up the Master server:

Step 1 Log in to the Operations Manager virtual IP address / hostname.

Step 2 Select **System Settings > Server** and select the Master server.

Step 3 Configure the backup settings as described in the "Backing Up and Restoring a Single Server" section on page 21-8.

Note Backup operations are supported on the server that has the Master role only. All backup data is automatically synchronized with the Peer server.

Restoring a Stand-Alone Operations Manager Server

In an HA configuration, all Operations Manager data and configurations are automatically synchronized with the Peer server, so it is typically unnecessary to restore a backup.

- If the Master server goes down, the system will simply fail over to the Peer server.
- If the Peer server goes down, it can be replaced with a new server and the current data will be automatically replicated from the Master.

If you want to roll back the configuration to an earlier state, however, you must delete the HA config, restore the backup file to the Master server, then select **Replace HA configuration** to sync the restored data to the Peer server.

Procedure

Step 1 Delete the HA config.

- See the "Deleting the HA Configuration" section on page 18-13.

Step 2 Restore the server configuration on the server that will be used as the Master.

- See the "Restoring a Backup for a Single Server" section on page 21-10.

Step 3 Replace the HA configuration on the Peer server.

- See the "Replacing the HA Configuration" section on page 18-12.

Upgrading the Operations Manager HA Servers

To upgrade the system software on a Operations Manager server in HA mode, upgrade the Peer server first, force a failover so the Peer server becomes the Master, and then upgrade again to update the second server (which now has the Peer role). Only the Peer server can be upgrading when the servers are in HA mode. An error occurs if you try to upgrade the Master server.

Note You must use the Operations Manager virtual IP address/hostname to upgrade Operations Manager servers in HA mode. HA Operations Manager servers cannot be upgraded using the Cisco VSM Management Console user interface.

Procedure

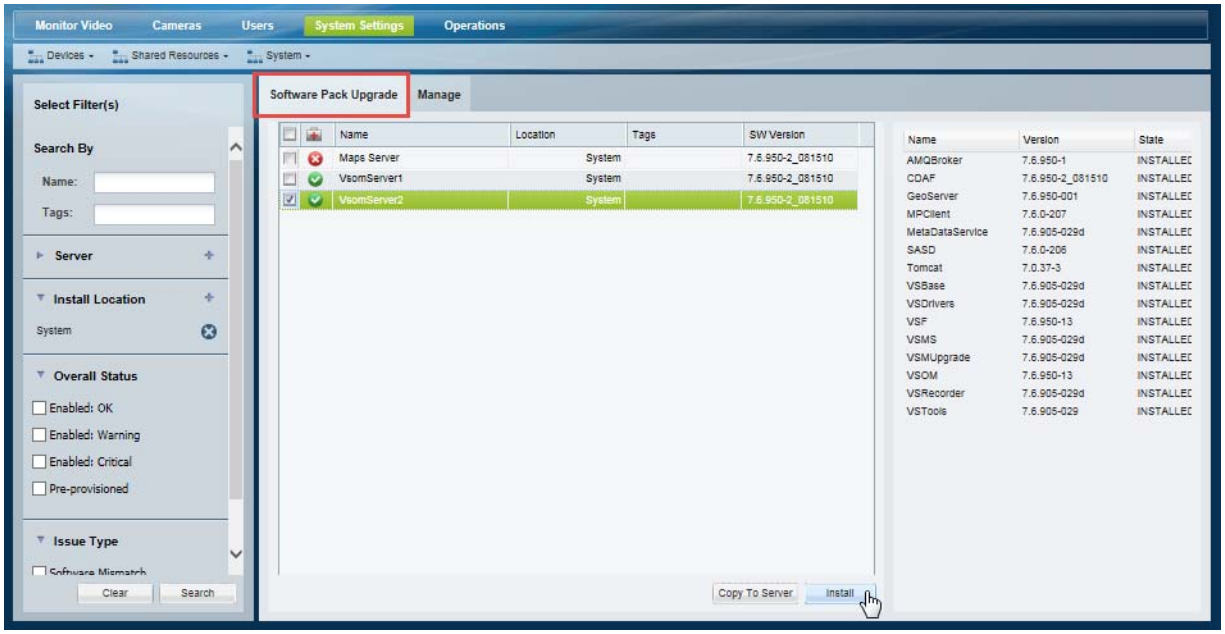
To upgrade the system software on a Operations Manager server in HA mode, do the following

Step 1 Log in to the Operations Manager using the virtual IP address / hostname.

Step 2 Click the pencil icon in the top right to turn maintenance mode ON.

- The icon is grey when maintenance mode is ON. Maintenance mode places the servers in a stable state and prevents other users from making most changes while high-availability tasks are performed.

Figure 18-7 Upgrading the Peer HA Server



Step 3 Select the Peer server and upgrade to the new system software version.

- See the "Upgrading System Software" section on page 26-5.

Step 4 Wait for the server software upgrade to complete.

Step 5 Perform a force failover to the (upgraded) Peer server.

- See the "Forcing a Failover" section on page 18-19.

Step 6 Repeat Step 1 to Step 4 to upgrade the system software again on the (new) Peer server.

- The second server (which is now the Peer server) will be upgraded, so both servers will run the upgraded software version.

Step 7 On the Master server, click the grey pencil icon in the title bar to turn maintenance mode OFF.

- The icon is yellow when maintenance mode is off, meaning user configuration changes can be saved.

Forcing a Failover

Although most failover events occur automatically if the Master server goes offline or is unavailable, you can also manually trigger a failover to switch the Master role to the Peer server. The server will retain the Master role even after the other reserver comes back online.

Troubleshooting a Force Failover

If a force failover does not complete, see Troubleshooting Errors During a Force Failover, page 18-32.

Procedure

Step 1 Access the Master server:

a. Log in to the Operations Manager using the virtual IP address / hostname.

b. Click the pencil icon in the top right to turn maintenance mode ON.

– The icon is grey when maintenance mode is ON. Maintenance mode places the servers in a stable state and prevents other users from making most changes while high-availability tasks are performed.

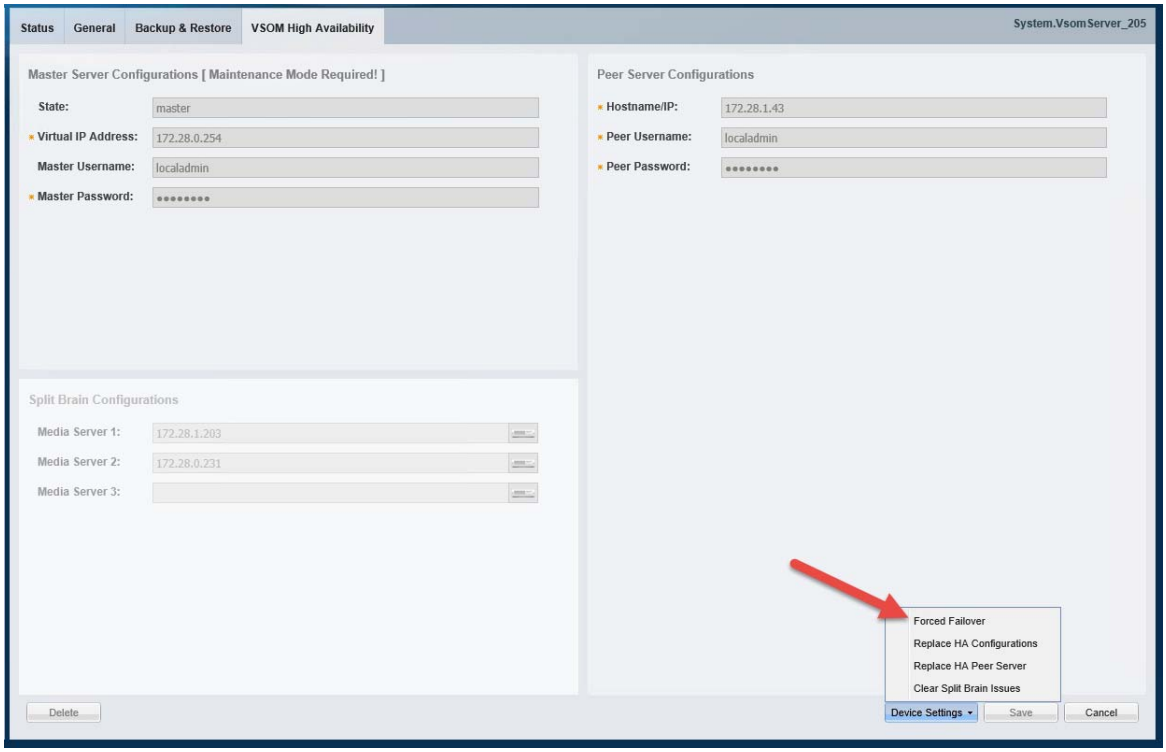
c. Select **System Settings** > **Servers**.

d. Select the **Master** server from the list.

e. Select the **VSOM High Availability** tab.

Step 2 Click **Device Settings** > **Force Failover** (Figure 18-8).

Figure 18-8 Forcing a HA Failover



Step 3 Click **OK**.

Step 4 Wait for the process to complete.

If the failover does not complete, review the information in Troubleshooting Errors During a Force Failover, page 18-32.

Step 5 When the failover is complete, you may need to refresh your browser if the servers use self-signed security certificates. See Resolving a "Server Unreachable" Error During Force Failover, page 18-33 for more information.

Step 6 Re-login to the virtual IP address / hostname, if necessary.

Step 7 On the Master server, click the grey pencil icon in the title bar to turn maintenance mode OFF.

- The icon is yellow when maintenance mode is off, meaning user configuration changes can be saved.

Resolving a Split Brain Scenario

A split brain scenario occurs when the communication between the Master and Peer servers is lost, and both servers try to independently assume the Master role. See the following for more information:

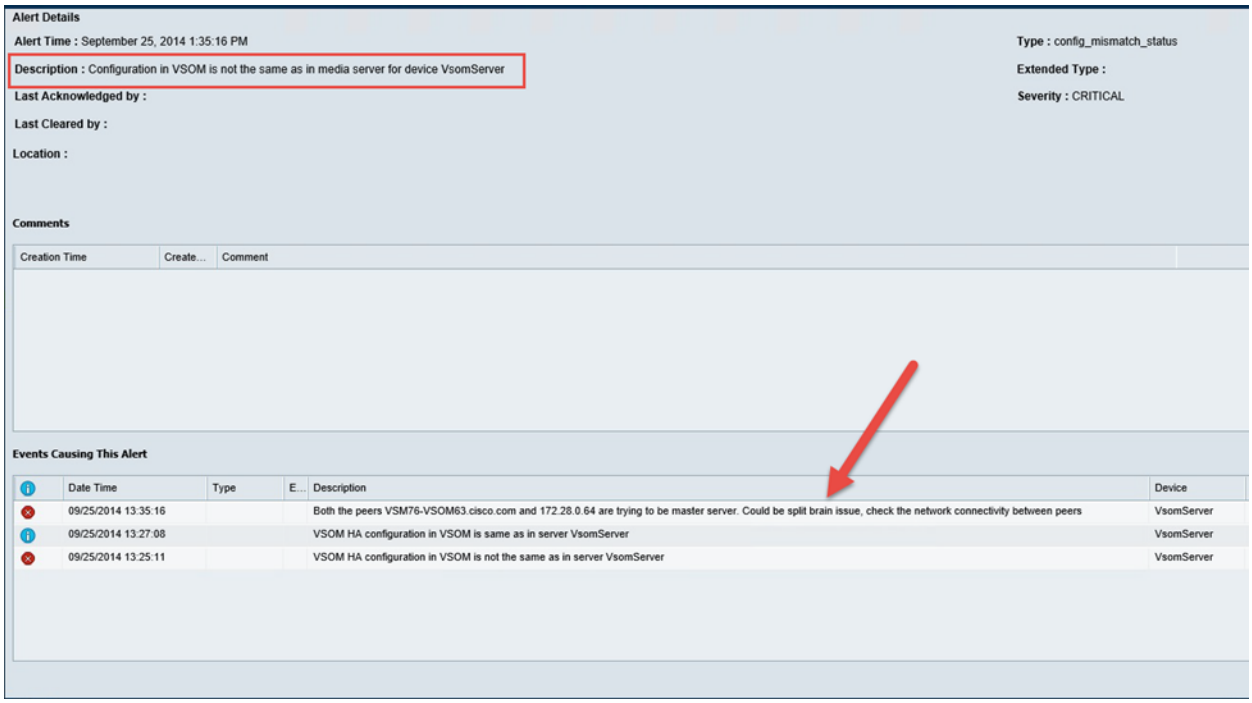
- Split Brain Overview, page 18-20
- Adding the "Split Brain" Media Servers, page 18-21
- Procedure to Resolve a Split Brain Scenario, page 18-24

Split Brain Overview

If communication between the Master and Peer servers is lost, both servers will try to independently assume the Master role. This is called a "Split Brain" scenario.

Cisco VSM will automatically detect a Split Brain scenario and direct all traffic to the server that was Master at the time of communication loss. The Peer server is put in standby and a Health alert is sent (Figure 18-9).

Figure 18-9 Split Brain Alert



Note This recovery process requires that at least one Media Server be added to the HA "Split Brain Configuration. See Adding the "Split Brain" Media Servers, page 18-21.

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

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

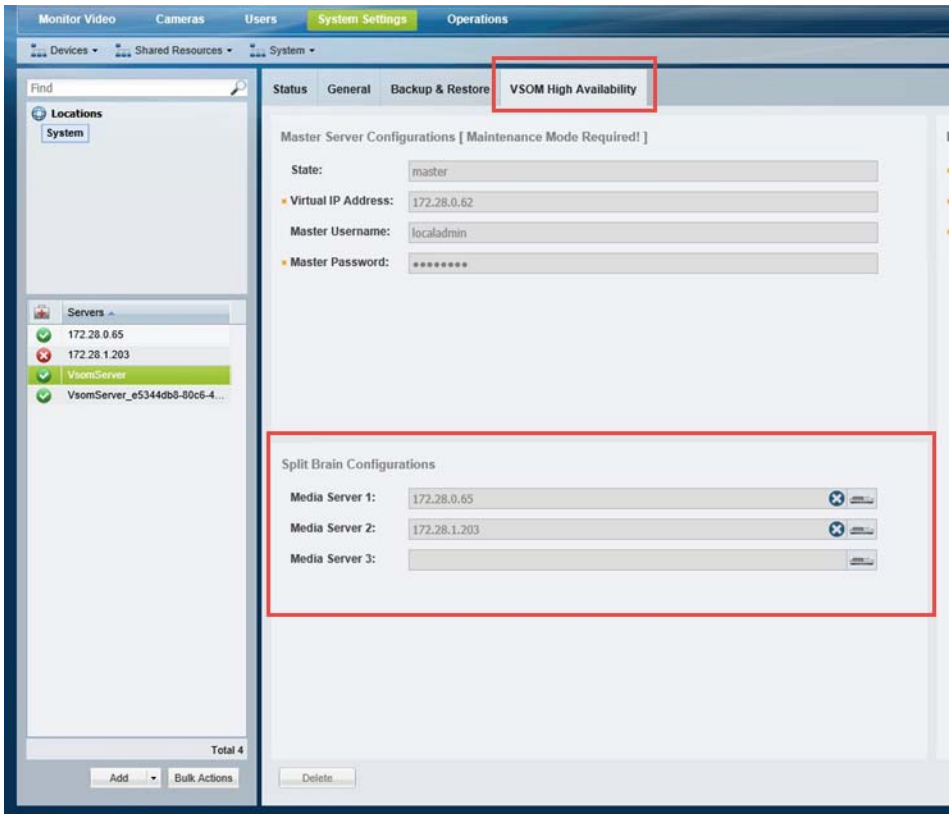
- Clear the split brain issues
- Replace the HA configuration on the Peer server

Adding the "Split Brain" Media Servers

Split Brain recovery requires that at least one Media Server be added to the Operations Manager HA configuration. These Media Servers are used to store the Master server info including the time when the server held the Master role.

Up to 3 Media Servers are automatically added to the Split Brain Configuration field when Operations Manager HA is first set up. If Media Servers are displayed, as shown in Figure 18-10, then no additional configuration is necessary.

Figure 18-10 Split Brain Configuration is Complete



Tip At least one Media Server must be added to support Split Brain recovery.

However, if no Media Servers are available when Operations Manager HA is set up, then the Split Brain Configuration will be blank (Figure 18-11), and Split Brain recovery will not be supported.

Figure 18-11 Split Brain Recovery is Not Supported if No Media Servers Are Selected

Procedure to Add Split Brain Media Servers

To add Split Brain support, do the following:

Step 1 Add one or more Media Servers to the system.

See Summary Steps to Add, Activate, and Configure a Media Server, page 9-4.

Step 2 Open the **VSOM High Availability** configuration page:

a. Log in to the Operations Manager using the virtual IP address / hostname.

b. Click the pencil icon in the top right to turn maintenance mode ON.

– The icon is grey when maintenance mode is ON. Maintenance mode places the servers in a stable state and prevents other users from making most changes while high-availability tasks are performed.

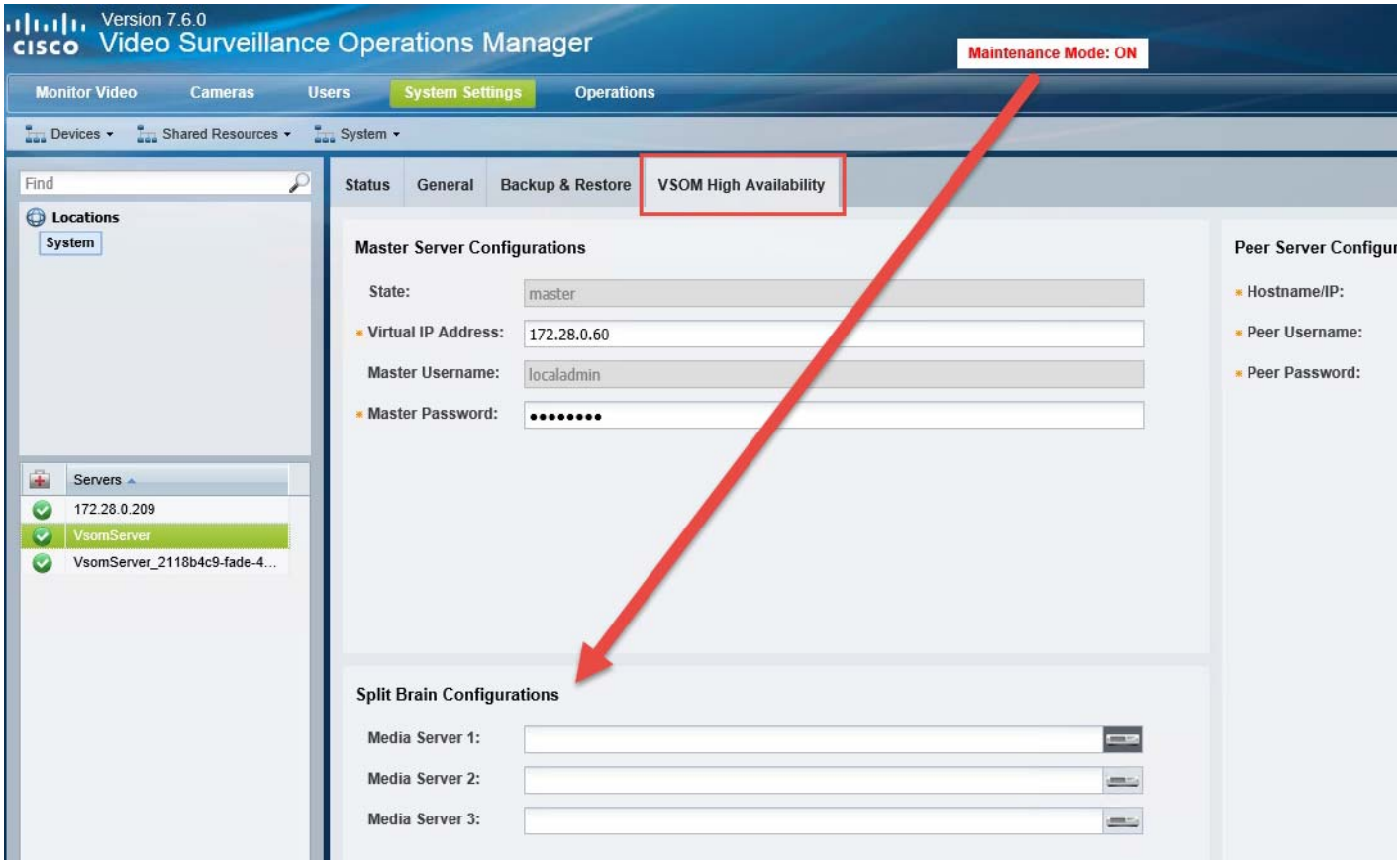
c. Select **System Settings** > **Servers**.

d. Select the **Master** server from the list.

e. Select the **VSOM High Availability** tab.

Step 3 In the Split Brain Configuration field, select one or more Media Servers (Figure 18-12).

Figure 18-12 Select the Split Brain Media Server(s)



Step 4 Click **Save**.

Step 5 Click the grey pencil icon in the title bar to turn maintenance mode OFF.

- The icon is yellow when maintenance mode is off, meaning user configuration changes can be saved.

Procedure to Resolve a Split Brain Scenario

Complete the following procedure to resolve database replication errors following a Split Brain scenario:

Procedure

Step 1 Verify that a Split Brain issue occurred:

a. Log in to the Operations Manager using the virtual IP address / hostname.

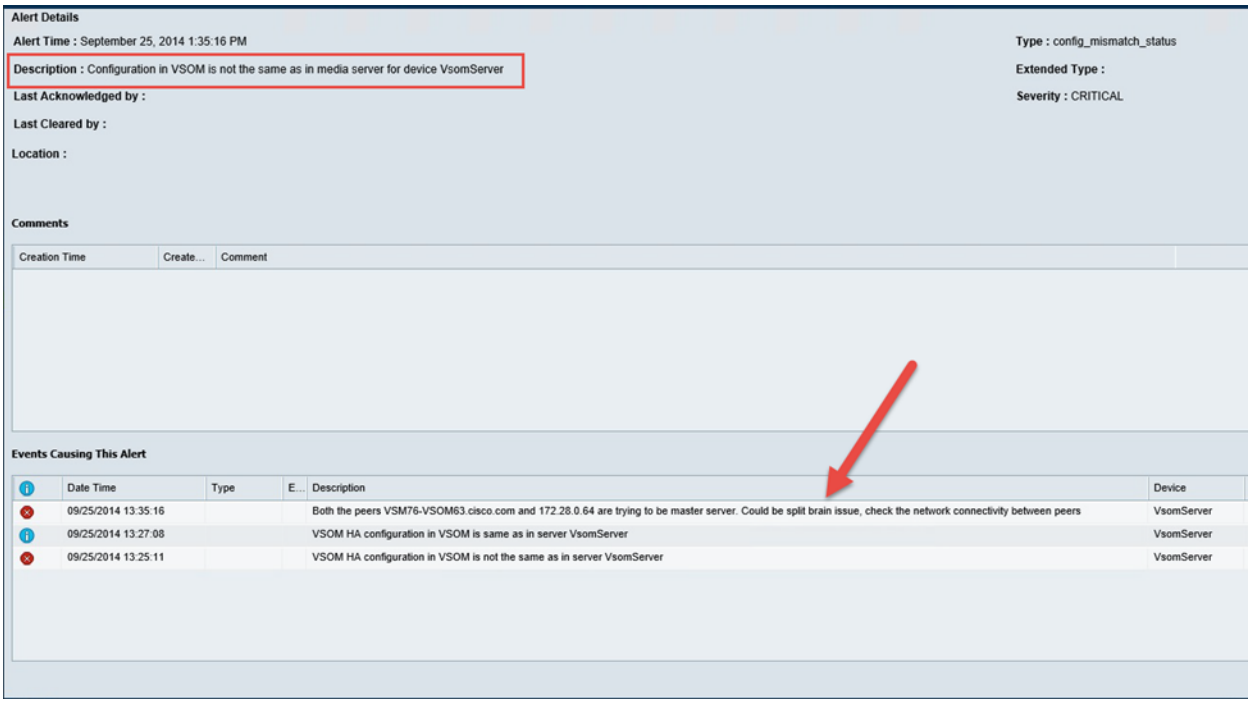
b. Select **System Settings** > **Servers**.

c. Select the **Master** server from the list.

d. Click the **Status** tab.

e. The Peer server is put in standby and a Health alert is sent (Figure 18-13).

Figure 18-13 Split Brain Alert



Step 2 Correct the issue causing the loss of communication between the Master and Peer servers.

Step 3 Clear the Split Brain issues:

a. Log in to the Operations Manager using the virtual IP address / hostname.

b. Click the pencil icon in the top right to turn maintenance mode ON.

– The icon is grey when maintenance mode is ON. Maintenance mode places the servers in a stable state and prevents other users from making most changes while high-availability tasks are performed. See Understanding Maintenance Mode, page 1-31 for more information.

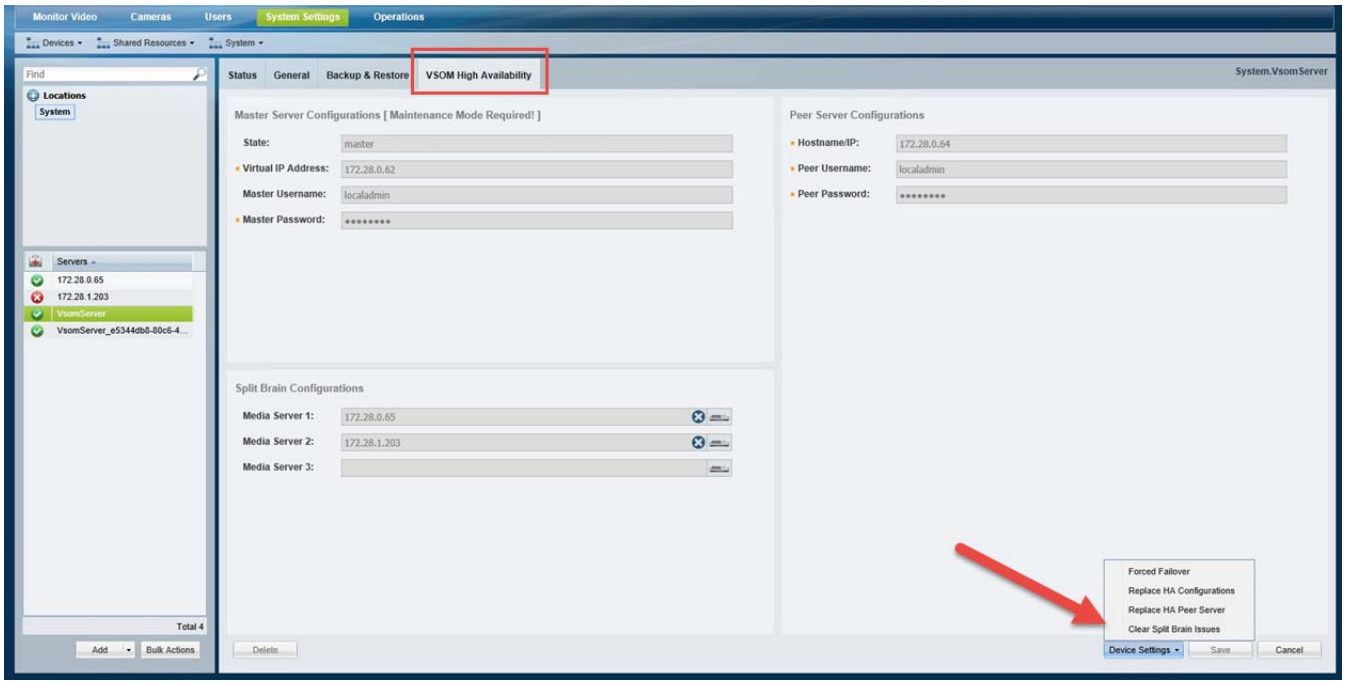
c. Select **System Settings** > **Servers**.

d. Select the **VSOM High Availability** tab.

e. Select **Device Settings** > **Clear Split Brain Issues** to clear the split brain issue (Figure 18-14).

f. Click **OK** and verify the alert and issue are cleared.

Figure 18-14 Clear Split Brain Issues



Step 4 Click **Device Settings > Replace HA Configurations** (Figure 18-14) to replace the configuration on the Peer server with the version on the Master server.

Step 5 Click **OK**.

Step 6 Wait for the process to complete and for the Master server data to be replicated on the Peer server.

Step 7 Re-login to the virtual IP address / hostname.

Step 8 On the Master server, click the grey pencil icon in the title bar to turn maintenance mode OFF.

- The icon is yellow when maintenance mode is off, meaning user configuration changes can be saved.

Troubleshooting Operations Manager HA

Review the following information for workarounds and solutions to Cisco Video Surveillance Operations Manager high availability (HA) issues:

Note For the latest, up-to-date, version of this information see the Cisco VSM Operations Manager High Availability Troubleshooting Guide.

The HA Configuration Job Does Not Complete

Issue

While configuring Operations Manager HA or replacing the HA Peer server, the sub job that updates the Peer server may not complete, and cause the job to remain in Pending/Running state.

Root Cause

This can happen if the Peer server is in any of the following states:

- The Peer server is being rebooted.
- The Peer server was recently rebooted but is not fully up.
- The Peer server has a Pending or In-progress job. This can be any job but examples include synchronization, device configuration, or template configuration.

Recovery

To clear the job and complete the HA configuration, do one or more of the following:

Step 1 Verify that there are no configuration or other tasks being performed on the Peer server, and that the Peer server does not have any Pending jobs.

a. Login to the Peer server Operations Manager interface.

b. Click **System Settings > Jobs**.

c. Verify that there are no Pending jobs in the Peer server.

See Viewing All Jobs in the System, page 19-32 for more information.

Step 2 Restart the services on the Master server:

a. Log in the Master server Management Console interface.

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

c. Follow the on-screen prompts and wait for the operation to complete (the login screen will reappear when services are fully restarted).

See the Cisco Video Surveillance Management Console Administration Guide for more information.

Step 3 Verify that the HA job is cleared on the Master server.

a. Login to the Master server Operations Manager interface.

b. Click **System Settings** > **Jobs**.

c. Verify that the previously stuck Operations Manager HA job is marked *Failed*.

See Viewing All Jobs in the System, page 19-32 for more information.

Step 4 Replace the HA configuration:

a. Select **System Settings** > **Servers**.

b. Select the **Master** server from the list.

c. Select the **VSOM High Availability** tab (Figure 18-4).

d. Click the pencil icon in the top right to turn maintenance mode ON.

– The icon is grey when maintenance mode is ON. See Understanding Maintenance Mode, page 1-31 for more information.

e. Select **Device Settings** > **Replace HA Configuration**.

f. Click **OK** and wait for the job to complete.

See Replacing the HA Configuration, page 18-12 for more information.

Step 5 Log in to the Operations Manager using the virtual IP address or hostname to verify that the HA setup was successful.

Database Replication Failures

Some events on either server in an HA configuration can cause database replication failures, where the data on the Master server is different than the data on the Peer server.

Events that can cause this include server reboots, power failures, database crashes, or a database going down on either of the participating servers.

Refer to the following topics for information to determine the cause of the failure and recover the database.

- Determining the if a Database Replication Error Occurred, page 18-28
- Detecting if the Database Crashed, page 18-29
- Recovering the Database, page 18-30

Determining the if a Database Replication Error Occurred

To detect if a database replication issue occurred, run the following command. If the fields LAST_SQL_ERRNO or LAST_SQL_ERROR fields have a value in the response, the database replication is stuck (the query is in the response).

Example Output

For example, the replication errors in the following output are shown in red:

```
mysql> show slave status\G
*************************** 1. row ***************************
               Slave_IO_State: Waiting for master to send event
                  Master_Host: 172.28.0.64
                  Master_User: vsomrepl
                  Master_Port: 6611
                Connect_Retry: 60
              Master_Log_File: vsom-mysql-bin.000001
          Read_Master_Log_Pos: 29020815
               Relay_Log_File: mysql-relay-bin.000004
                Relay_Log_Pos: 2462282
        Relay_Master_Log_File: vsom-mysql-bin.000001
             Slave_IO_Running: Yes
            Slave_SQL_Running: No
              Replicate_Do_DB:
          Replicate_Ignore_DB:
           Replicate_Do_Table:
       Replicate_Ignore_Table:
vsom.qrtz_trigger_listeners,vsom.qrtz_calendars,vsom.qrtz_fired_triggers,vsom.qrtz_job
_details,vsom.qrtz_scheduler_state,vsom.qrtz_job_listeners,vsom.qrtz_triggers,vsom.qrt
z_locks,vsom.qrtz_paused_trigger_grps
      Replicate_Wild_Do_Table:
  Replicate_Wild_Ignore_Table:
                   Last_Errno: 1032
                   Last_Error: Could not execute Delete_rows event on table
vsom.issue; Can't find record in 'issue', Error_code: 1032; handler error
HA_ERR_KEY_NOT_FOUND; the event's master log vsom-mysql-bin.000001, end_log_pos
23237993
                 Skip_Counter: 0
          Exec_Master_Log_Pos: 23237346
              Relay_Log_Space: 8246408
              Until_Condition: None
               Until_Log_File:
                Until_Log_Pos: 0
           Master_SSL_Allowed: No
           Master_SSL_CA_File:
           Master_SSL_CA_Path:
              Master_SSL_Cert:
            Master_SSL_Cipher:
               Master_SSL_Key:
        Seconds_Behind_Master: NULL
Master_SSL_Verify_Server_Cert: No
                Last_IO_Errno: 0
                Last_IO_Error:
               Last_SQL_Errno: 1032
               Last_SQL_Error: Could not execute Delete_rows event on table
vsom.issue; Can't find record in 'issue', Error_code: 1032; handler error
HA_ERR_KEY_NOT_FOUND; the event's master log vsom-mysql-bin.000001, end_log_pos
23237993
  Replicate_Ignore_Server_Ids:
             Master_Server_Id: 2
                  Master_UUID: f55e65d2-5261-11e4-a165-005056ae786a
             Master_Info_File: /mysql/data/vsom/mysql/data/master.info
```

```
                    SQL_Delay: 0
            SQL_Remaining_Delay: NULL
      Slave_SQL_Running_State:
           Master_Retry_Count: 86400
                  Master_Bind:
      Last_IO_Error_Timestamp:
     Last_SQL_Error_Timestamp: 141012 17:47:50
               Master_SSL_Crl:
           Master_SSL_Crlpath:
           Retrieved_Gtid_Set:
            Executed_Gtid_Set:
                Auto_Position: 0
1 row in set (0.00 sec)
```

Procedure

For example, complete this procedure to detect which database replication query is stuck in the following error:

> Could not execute Delete_rows event on table vsom.issue; Can't find record in 'issue', Error_code: 1032; handler error HA_ERR_KEY_NOT_FOUND; the event's master log **vsom-mysql-bin.000001**, end_log_pos **23237993**'

Step 1 Decrypt the binary error log file.

Step 2 Look in the master log file for the *end_log_pos* entry in the Example Output, page 18-28.

Step 3 Enter the following command on the master log file on the Peer server.

For example, if an HA deployment includes server 50 and server 51, and the issue was seen on server 51, go to the Peer server 50 and enter the following command on the master log file. In the example error message above it is *vsom-mysql-bin.000001*:

```
/usr/BWhttpd/vsom_be/db/mysql/bin/mysqlbinlog -r /tmp/error_log.sql
--base64-output=DECODE-ROWS --verbose
/mysql/data/vsom/mysql/data/vsom-mysql-bin.000001
```

- Notice that the command was storing the parsed output in the `/tmp/error_log.sql` file.
- Open the parsed log file `error_log.sql` and search for log position seen in above error 23237993.
- Check the query seen at the log position which gives the ASCII format of the original query that is being executed and is stuck.

Detecting if the Database Crashed

To determine if the database crashed, verify the `/usr/BWhttpd/vsom_be/mysql.log` and look for errors such as the following (in **red**):

```
2014-11-06 13:46:40 2859 [Note] Error reading relay log event: slave SQL thread was
killed
2014-11-06 13:46:40 2859 [ERROR] Error reading packet from server: Lost connection to
MySQL server during query ( server_errno=2013)
2014-11-06 13:46:40 2859 [Note] Slave I/O thread killed while reading event
2014-11-06 13:46:40 2859 [Note] Slave I/O thread exiting, read up to log
'vsom-mysql-bin.000023', position 580246
```

```
2014-10-24 15:34:39 13859 [Note] InnoDB: Not using CPU crc32 instructions
2014-10-24 15:34:39 13859 [Note] InnoDB: Initializing buffer pool, size = 64.0M
2014-10-24 15:34:39 13859 [Note] InnoDB: Completed initialization of buffer pool
2014-10-24 15:34:39 13859 [Note] InnoDB: Highest supported file format is Barracuda.
2014-10-24 15:34:39 13859 [Note] InnoDB: The log sequence numbers 46653980 and
46653980 in ibdata files do not match the log sequence number 197868345 in the
ib_logfiles!
2014-10-24 15:34:39 13859 [Note] InnoDB: Database was not shutdown normally!
```

Recovering the Database

If a Database Replication Error Occurred

If the SQL that was stuck is of no significance, log in to the Operations Manager using the virtual IP address, and then select **Replace HA Configuration**. This process clears the replication error by replacing the Peer data with the Master data.

If the Database Crashed

Step 1 Restart Cisco services using the following commands:

service cisco stop

service cisco start

Step 2 Ensure the database is fully up, by checking Cisco service status:

service cisco status

Step 3 If the VSOM database service is still not coming up, check the `/usr/BWhttpd/vsom_be/mysql.log`:

- If the log states that the slave thread was killed, fix the issue by logging into the Operations Manager using the virtual IP address, and then select **Replace HA Configuration**.
- if the *ibdata files* do not match the log sequence number, force recover the database as recommended by Oracle Support team in this link and restart Cisco services: http://dev.mysql.com/doc/refman/5.6/en/forcing-innodb-recovery.html

Step 4 If all services are up and running, a database replication issue occurred. Recover the database by logging into the Operations Manager using the virtual IP address, and then select **Replace HA Configuration**.

File Replication Failures

If a database or file replication issue is displayed in the server Status page, double-click the alert to view the events that describe why file replication is failing. The following can cause these errors:

Password Change

The *localadmin* password for the Peer server is not valid. For example, the password was changed on the Peer server but was not updated on the **VSOM HA Configuration** page.

To resolve this problem:

Step 1 Log in to the Operations Manager using the virtual IP address / hostname.

Step 2 Click the pencil icon in the top right to turn maintenance mode ON.

- The icon is grey when maintenance mode is ON. See Understanding Maintenance Mode, page 1-31 for more information.

Step 3 Select **System Settings** > **Servers**.

Step 4 Select the **Master** server from the list.

Step 5 Select the **VSOM High Availability** tab.

Step 6 Enter the new Peer server password.

Step 7 Click **Save**.

The Remote Host Identification (Hostkeys) for the Peer Server Changed

The Hostkeys for the Peer server can change if the server IP address is changed when the server is reinstalled or replaced. If this occurs:

Step 1 Log in to the Master server using an SSH client.

Step 2 SSH to the Peer server to verify that the following error is displayed. For example:

```
[root@psbu-server-qaha]# ssh localadmin@psbu-server-qa2
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that the RSA host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
d3:b5:e3:0d:fc:0b:ab:6a:c6:c4:b2:3e:17:21:7b:c9.
Please contact your system administrator.
Add correct host key in /root/.ssh/known_hosts to get rid of this message.
Offending key in /root/.ssh/known_hosts:8
RSA host key for psbu-server-qa2 has changed and you have requested strict checking.
Host key verification failed.
```

Step 3 If this message appears, edit the known hosts using the following command:

- **vi /root/.ssh/known_hosts**

Step 4 Delete the host key entry of the Peer server and save the changes.

Step 5 Verify that the database or file replication error is resolved. Wait at least one minute since health monitoring jobs are updated each minute.

a. Log in to the Operations Manager using the virtual IP address / hostname.

b. Select **System Settings** > **Servers**.

c. Select the **Master** server from the list.

d. Select the Status tab.

e. Verify that the issue is clear.

Network Connectivity Loss Results in a Split Brain Scenario

If communication between the Master and Peer servers is lost, both servers will try to independently assume the Master role. This is called a "Split Brain" scenario.

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

Note This recovery process requires that at least one Media Server be added to the HA "Split Brain Configuration. See the "Operations Manager High Availability" section of the Cisco Video Surveillance Operations Manager User Guide.

Since there can be a delay up to 90 seconds for the issue to be detected, users may still be able to log in to the wrong server. During this time, it is possible that user traffic will go to both servers.

If this occurs, refer to the "Operations Manager High Availability" section of the Cisco Video Surveillance Operations Manager User Guide for more information.

Troubleshooting Errors During a Force Failover

If a force failover does not complete or encounters errors, review the following information and workarounds.

- Summary of Force Failover Errors and Workarounds, page 18-32
- Resolving a "Server Unreachable" Error During Force Failover, page 18-33
- Force Failover During a Software Upgrade on the Peer Server, page 18-34

Summary of Force Failover Errors and Workarounds

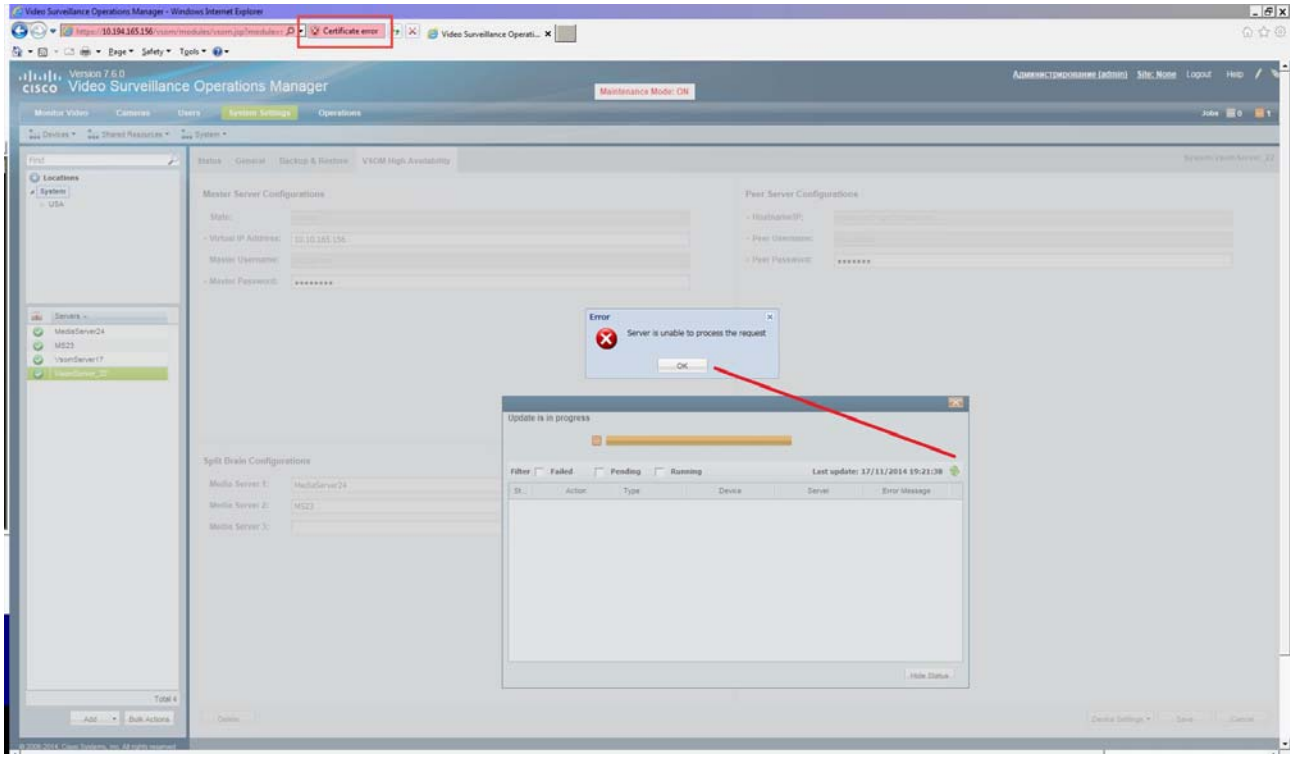
Table 18-2 Troubleshooting Force Failover

Issue	Workaround
A "Server Unreachable" error appears	Resolving a "Server Unreachable" Error During Force Failover, page 18-33
Errors during a software upgrade	Force Failover During a Software Upgrade on the Peer Server, page 18-34
The Peer server is not reachable	Check the Peer server's Status tab to see if the server is reachable.
The *pacemaker* service is not running	Go to the Peer server **Status > Status History** tab to see if there is a issue "HA Functionality is not available at this time.Pacemaker service is not running". To resolve the issue select **Device Settings > Replace HA Configuration** to bring up the pacemaker service on the Peer server.
The system is in a Split Brain state	To resolve this, go to **Server > VSOM High Availability** and select **Device Settings > Clear Split Brain Issues**. For more information See Resolving a Split Brain Scenario, page 18-20.

Resolving a "Server Unreachable" Error During Force Failover

If the default self-signed certificates are used on the master and peer servers, a "Server unreachable" error may occur when performing a force failover (Figure 18-15).

Figure 18-15 Certificate Error



To temporarily address this issue, refresh the browser page to remove the error and continue.

To resolve the issue, obtain and install a signed certificate issued by a Certification Authority.

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

For more information, see the following:

- Requirements, page 18-4
- Configuring Operations Manager HA, page 18-6
- Cisco Video Surveillance Management Console Administration Guide—for instructions to install the certificate.

Force Failover During a Software Upgrade on the Peer Server

If you perform a force failover while a software upgrade is in process on the Peer server (for example, the Peer server has not fully initialized after the upgrade), the virtual IP address/hostname can be lost.

If this happens, error messages may appear when a user attempts to log in using the Operations Manager virtual IP address. Messages include: “Invalid access, server is in standby mode” or “”Must login with Virtual IP [*IP address*] to access system”. This is because both the Master and Peer servers are in standby state.

Recovery

To resolve this issue, you must manually release *standby* mode on the original Master server.

Step 1 To determine the Master server, query the following database with the following SQL from either server:

select peerserverip from haconfig where state = 2

Step 2 Log in to the Master server from the command prompt.

crm_node -n

Step 3 This provides the node name of the server.

Step 4 Release standby mode using the following command:

crm_standby -D -N *server-name* [node name collected from above command]

For example: **crm_standby -D -N vsm-server**

Step 5 After releasing the Standby mode, the server should automatically acquire the virtual IP address.

Step 6 Log back in to the Operations Manager using the virtual IP address or hostname.

Step 7 Go to the Master server and select **Force Fail Over** to proceed with rest of the software upgrade process.

Virtual IP Login Failure

If users are not able to login using the virtual IP address or hostname, do the following:

Determine the following

- The pacemaker service may be down or crashed.
  - Check the status by entering **service pacemaker status** on both the servers.
  - Run the command **crm_mon -1** to list node status information on both the servers.
- The virtual IP address is not assigned to either of the participating Operations Manager servers:
  - Enter the command **ifconfig** on both servers. If either server returns **NO eth0:0** or **eth1:0**, then neither server acquired the virtual IP address.

If a software upgrade was not being performed, log in to the Master server using the server’s actual IP/Hostname and select **Replace HA Configuration**. Otherwise, try one of the following:

Software Upgrade Issue

If a force fail over was issued before a software upgrade was complete, see Force Failover During a Software Upgrade on the Peer Server, page 18-34.

Recovery for Pacemanker Down

Step 1 If the pacemaker is down, restart the pacemaker service using the command:

service pacemaker start

Step 2 If the pacemaker does not come up clean, run the script:

/usr/BWhttpd/vsom_be/ha/recoverPacemaker.sh

Step 3 Restart the pacemaker service:

service pacemaker start

Unmanaged Split Brain Scenario

If network connectivity is lost between the Master and Peer server, both servers can assume the Master role and acquire the virtual IP address.

If connectivity is restored between the servers, user traffic can be sent to both servers.

Root Causes

This scenario can be caused by the following:

- The Master server is disconnected from the rest of the world, but the Peer server can see all other servers (including the Media Servers used for HA storage).
- The Master server has communication with all servers except the Peer server, and the Peer server loses network communication with the rest of the world.
- No Media Servers are configured for HA storage, so the system cannot resolve the split brain.
- Media Servers are configured for HA storage but the connectivity issue was shorter than a minute.

Validate

If an unmanaged split brain scenario occurs, the virtual IP address is configured on both servers. Enter the **ifconfig** command on both servers to view the IP address on each server and verify that both servers are using the virtual IP address.

For example, if the Eth0 interface was used, the virtual IP address is displayed under the eth0:0 entry. If the eth1 interface was used for HA configuration, the virtual IP address is displayed under eth1:0.

Recovery: Method 1

After network connectivity between the Operation Manager HA servers is restored, log in to the Operation Manager browser-based interface to replace the HA configuration.

Step 1 Log in to the Operation Manager for either server using the physical IP address.

Step 2 Select **Device Settings** > **Replace HA Configuration**. See Replacing the HA Configuration, page 18-12.

Step 3 If the issue is still not resolved, delete the HA Configuration and reconfigure Operation Manager HA:

a. Complete Deleting the HA Configuration, page 18-13.

b. Continue to Configuring Operations Manager HA, page 18-6.

Recovery: Method 2

The following alternative method can also be performed to manually resolve the issues.

Step 1 Enter the command **ifconfig** on both servers to determine if both servers are configured with the virtual IP address.

- For example, if the Eth0 interface was used, the virtual IP address will appear under the eth0:0 entry.

Step 2 Verify that the Cisco service is up on both servers.

Step 3 Bring the Cisco service back up on both servers, if necessary.

Step 4 Stop the pacemaker service on both servers.

Step 5 Start the pacemaker service on the original master server.

Step 6 When the pacemaker service starts, enter the command **ifconfig** to verify it has the virtual IP address.

Step 7 Log in to the Operation Manager using the virtual IP address or hostname.

Step 8 View the server status.

Step 9 If the database replication issue is not automatically released, go to the **VSOM High Availability** tab and select **Device Settings > Replace HA Configuration**.

Useful Command Line Tools for HA Troubleshooting

Table 18-3 CLI Monitoring Tools

CLI	Description
service pacemaker status	Displays if pacemaker service is running or not. For example: *pacemakerd (pid 2583) is running...*

crm_mon -1	Lists the participating servers along with where the resources are running.
	For example:
	`Last updated: Mon Nov 17 10:47:23 2014`
	`Last change: Thu Nov 13 16:11:23 2014 via crm_attribute on vsm7-55`
	`Stack: cman`
	`Current DC: vsm7-54 - partition with quorum`
	`Version: 1.1.10-14.el6-368c726`
	`2 Nodes configured`
	`2 Resources configured`
	
	`Online: [ vsm7-54 vsm7-55 ]`
	
	`Resource Group: group1`
	`ClusterIP (ocf::heartbeat:IPaddr2): Started auto-vsm7-54`
	`vsom (lsb:vsomha): Started vsm7-54`

Table 18-3 CLI Monitoring Tools

CLI	Description
crm_node -n	Get node name as seen by the pacemaker on local server
crm_mon --failcounts	Resource current failure status and limits
crm_standby –v true [*nodename*]	To force the server to pacemaker standby state (useful for upgrades and backup restores). For example: `crm_standby -v true vsm7-server`
crm_standby –D –N [*nodename*]	Release the server from standby mode. For example: `crm_standby -D -N vsm7-server`

Monitoring System and Device Health

Refer to the following topics for information to monitor the health of the system or a device, to view the status of user-initiated *jobs*, a record of user actions (Audit Logs), and other features.

Contents

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:

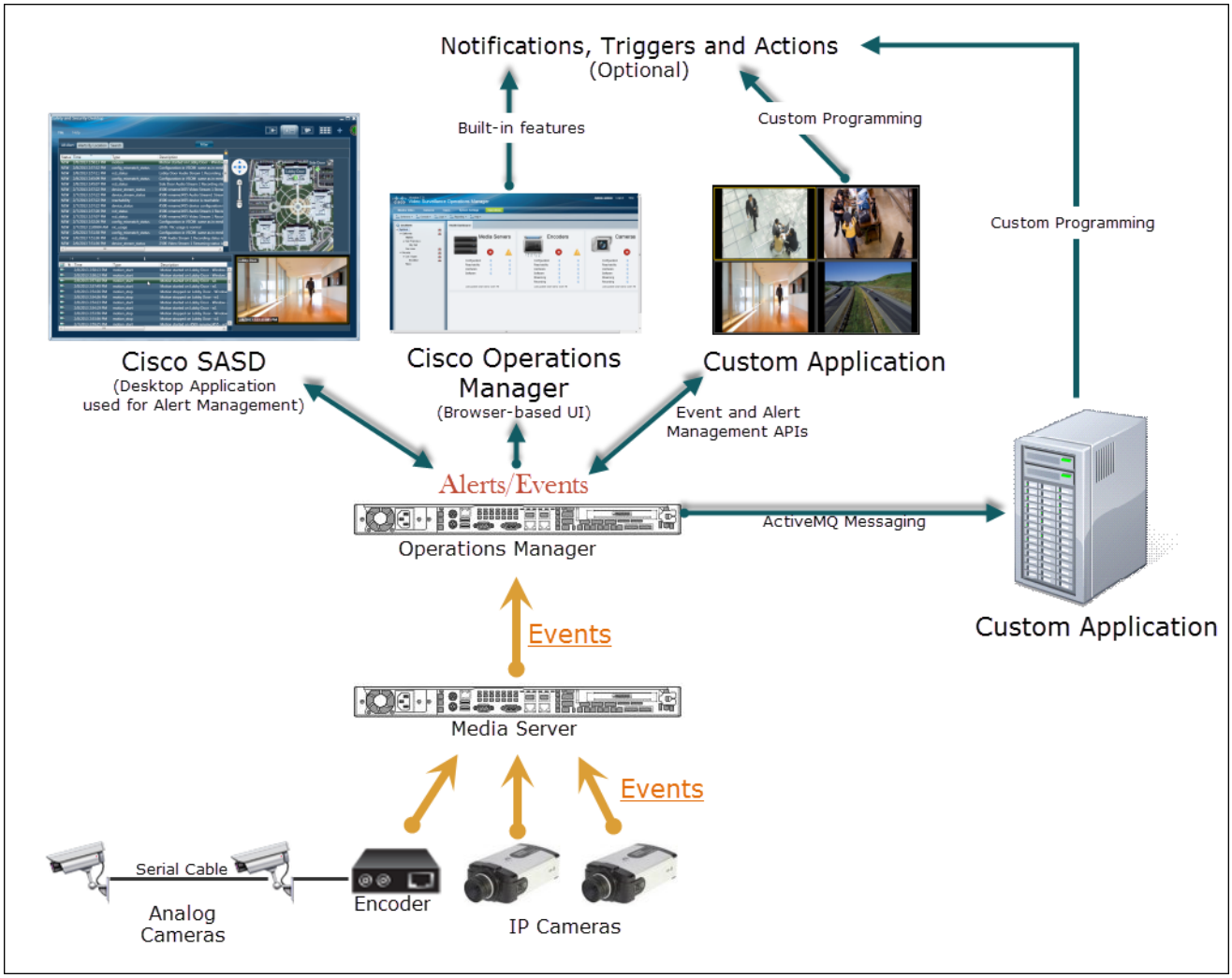
Overview

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, the individual events for that issue are grouped under a single alert, which results in a single notification. This prevents operators from being flooded with notifications for every event that occurs for the same issue.

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 19-1 summarizes how Cisco VSM events and alerts are generated, viewed and managed.

Figure 19-1 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 19-1 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 19-17
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 12-3
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 13-7

Monitoring Device Heath 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 19-2 summarizes the Operations Manager monitoring features.

Table 19-2 Monitoring Features

Monitoring Feature	Location	Description
Health Dashboard: Device Health Faults on an Operations Manager, page 19-6	**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 19-9	**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. • 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 19-17	**Operations > Health Notifications**	Send emails to specified recipients when a critical device error occurs.
Reports, page 19-20	**Operations > Reports**	Generate and download information about the Cisco Video Surveillance user activity, device configuration, and other information.
Synchronizing Device Configurations, page 19-21	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 19-28	**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 *localadmin* password. See the Cisco Video Surveillance Management Console Administration Guide for more information.
Understanding Jobs and Job Status, page 19-29	**System Settings > Jobs**	Displays a summary of current and completed jobs triggered by user actions.
Viewing Audit Logs, page 19-35	**Operations > Audit Logs**	Displays successful configuration changes. You can sort or filter the results by user, device, and other categories.

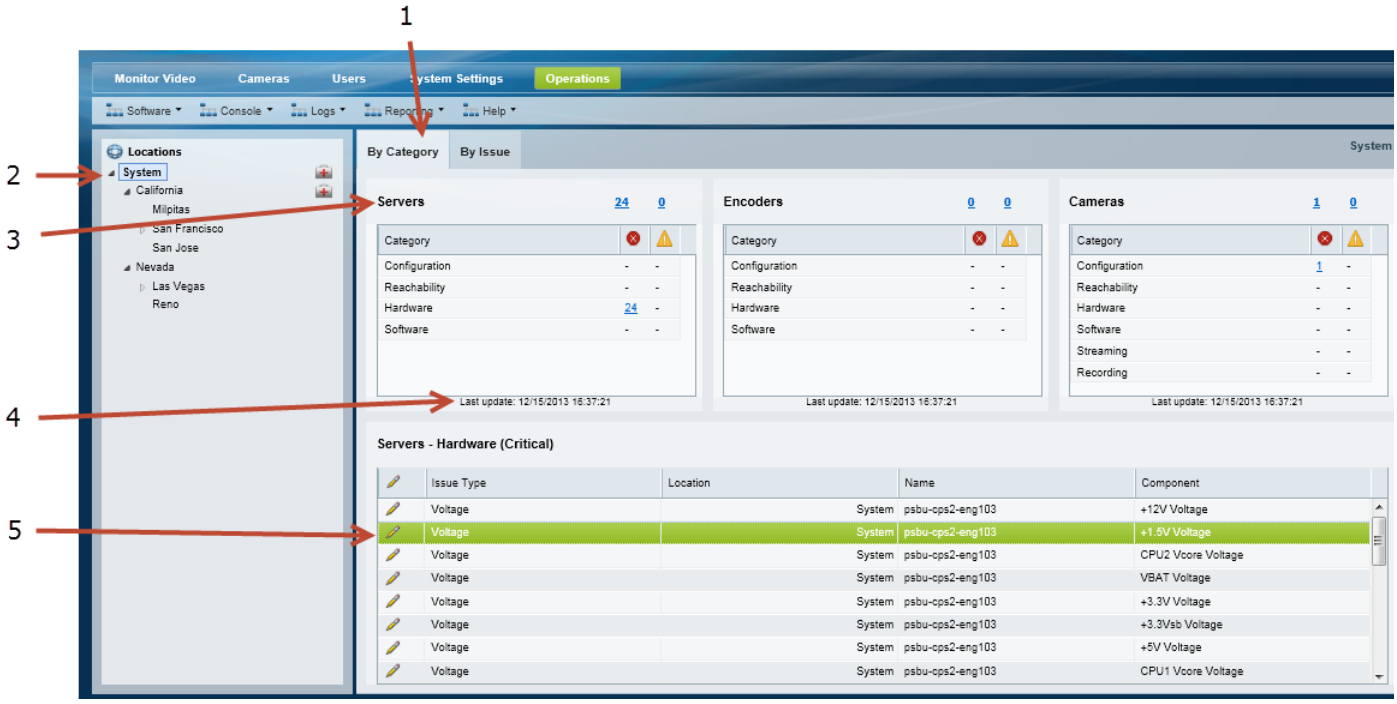
Health Dashboard: Device Health Faults on an Operations Manager

Use the Health Dashboard to view a summary of the critical or warning faults that are occurring on servers, encoders and cameras ((Figure 19-2).

For example, select **Operations > Health Dashboard** and choose a location that displays a Health icon . Click the number next to a category (such as *Configuration*) or Issue type (such as *Motion Unconfigured*) to display additional details about the issue(s) and device. Click the icon to open the device status and configuration page.

Tip To view the health issues for multiple Operations Managers, see the "Monitoring Device Health Using the Browser-Based Federator" section on page 22-34.

Figure 19-2 Operations Manager Health Dashboard



1	Click a tab to view the device issues by the following: • **By Category**—Displays the number of health issues for the location grouped into categories such as Configuration, Reachability, Hardware and Software. Click the number next to the device type (such as Servers) to display the issues for all categories. • **By Issue**—Displays the number of health issues for each type of issue. For example, server issues can include hardware problems such as temperature or fan speed. Cameras issues can include items such as "Motion Unconfigured". **Note** The number represents the total number of issues for all devices at that location, based on the selected category or issue.

2	The Health icon is displayed if a location or any of its sub-locations includes an issue. Click a location to view the device issues for the location and its sub-locations. If a sub-location has a device with a health issue, the Health icon is also displayed for the parent location(s).
3	The device type (such as Servers, Encoders, or Cameras) where the issues occurred. • Click a number to display a list of critical or warning faults for the category, issue type, or device type. For example, click the number *23* next to *Hardware* to display a list of the hardware issues for all servers (multiple issues can occur for a single device). See Table 19-3 for more information about critical and warning faults. • If issues did not occur, a number is not displayed. • The number represents the total number of issues for all devices at that location, based on the selected category or issue.
4	Last Update—Refresh the Health Dashboard page to view updated results. The dashboard does not automatically refresh.
5	The specific health issues that occurred for the selected category or issue type. • All issues are listed. Multiple issues can be displayed for the same device • Click the icon to open the device's status and configuration page. See the "Device Status: Identifying Issues for a Specific Device" section on page 19-9 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 B-2 for more information.

Understanding Warning and Critical Faults

Table 19-3 Warning and Critical Faults

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	Critical errors are health events that impact the device operation or render a component unusable. For example, a server or camera 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. See the "Health Notifications" section on page 19-17 for instructions to send emails when a critical event occurs.

Procedure

Complete the following procedure to access the Health Dashboard and view device health issues:

Step 1 Click **Operations** > **Health Dashboard** (Figure 19-2).

Step 2 Choose a location to view a summary of the health issues at that location, including its sub-locations.

- Locations (or sub-locations) with health issues display a Health icon .
- If a sub-location has a device with a health issue, the Health icon is also displayed for the parent location(s).

Step 3 Click the **By Category** or **By Issue** tab.

Step 4 Click a number to display the specific issues for the device type, category or issue type.

The number represents the total number of issues for all devices at the selected location and it's sub-locations (the number is the consolidated sum of issues in that location and it's sub-locations).

Step 5 (Optional) Click the icon to open the device status and configuration pages.

Step 6 Continue to the "Device Status: Identifying Issues for a Specific Device" section on page 19-9 for more information.

Step 7 Take corrective action to restore the device to normal operation, if necessary.

Step 8 For example, if a configuration mismatch occurs, see the "Synchronizing Device Configurations" section on page 19-21.

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 19-3). 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 19-9
- Understanding Device Status, page 19-11
- Viewing the Status Error Details and History, page 19-14
- Viewing Service Jobs, page 19-15
- Viewing Camera Events, page 19-16

Understanding the Overall Status

Click the device Status tab to view the overall operational state (Figure 19-3).

Figure 19-3 Overall Status Camera Device Status

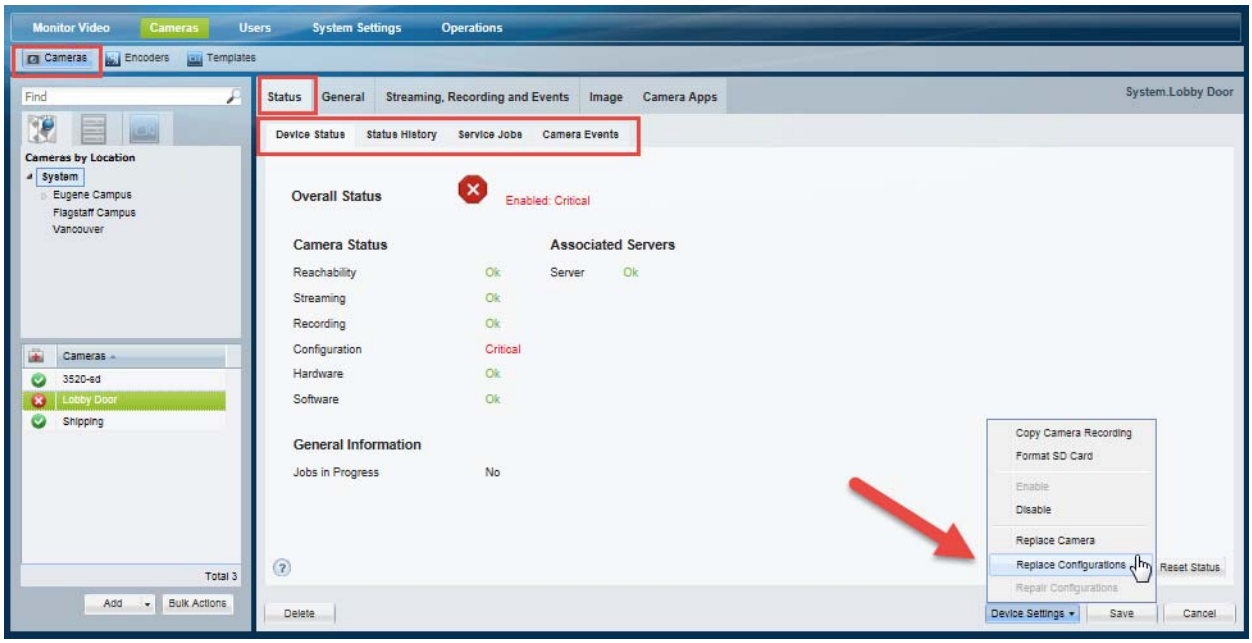


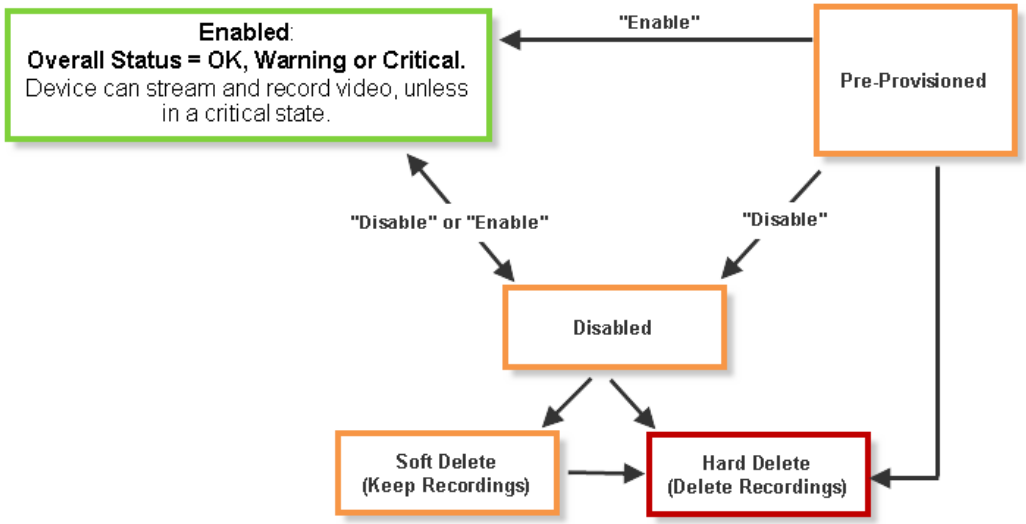
Table 19-4 describes the overall device states:

Table 19-4 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.
Enabled: Critical		Red	An event occurred that impacts the device operation or renders a component unusable. See the "Health Notifications" section on page 19-17 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 1-26.
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 10-40.

Note Devices states can change due to changes in the device configuration, or by manually changing the status in the device configuration page (Figure 19-4).

Figure 19-4 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 19-5), 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 select Device Settings > **Repair Configurations** or **Replace Configurations** to replace the device configuration with the Operations Manager version.

Figure 19-5 Device Status Summary

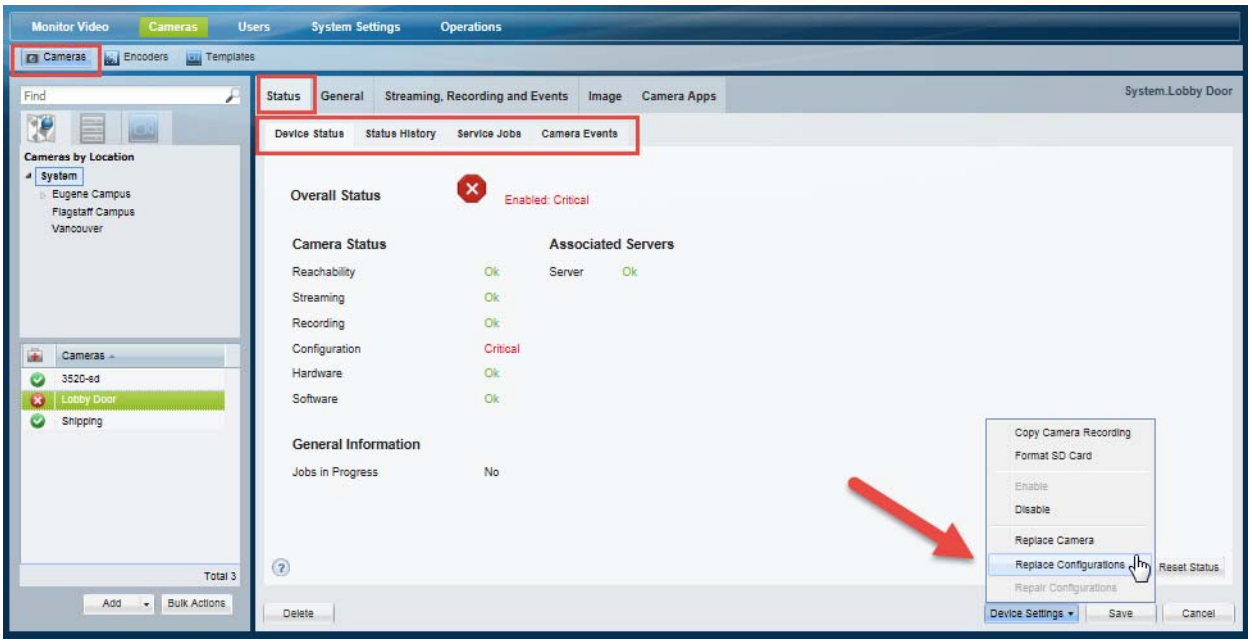


Table 19-5 describes the status categories. The categories are different for each type of device. For example, Media Servers include a *Software* category to indicate the health of server processes. An encoder does not include streaming or recording categories.

Table 19-5 Device Status Categories

Category	Devices	Description
Overall Status	All Devices	The aggregated status of all categories included for the device. See the "Understanding the Overall Status" section on page 19-9. **Note** The *Associated Servers* status does not impact the *Overall Status*. For example, if the associated Media Server or Redundant Server is down, but the camera *Network* status is *Enabled: OK*, then the camera *Overall Status* is also *Enabled: OK*.
Device Status		
Reachability	All Devices	Indicates the health of the network connection. For example, a warning or critical event indicates that a device is unreachable on the network.
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.

Table 19-5 Device Status Categories (continued)

Category	Devices	Description
Configuration	Media Servers Cameras Encoders	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. Configuration errors also display an icon. Click the icon to view additional details about the error (see the "Viewing the Status Error Details and History" section on page 19-14) 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 19-21 for more information.
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	Indicates if the device has one or more Jobs running. See the "Understanding Jobs and Job Status" section on page 19-29.
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.
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 the Status Error Details and History

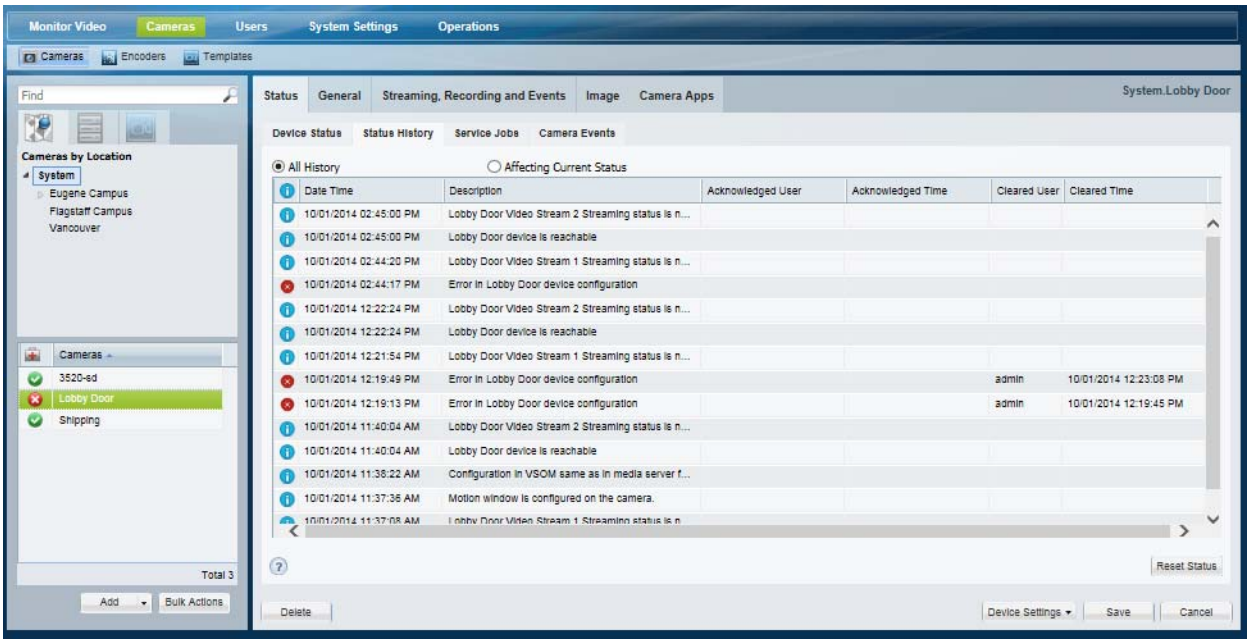
If a device error is displayed in the Status page (Figure 19-5), do one of the following:

- 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 19-21 for instructions to correct configuration errors.
- Click the **Status History** tab (Figure 19-6) 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 19-6 Camera Status History

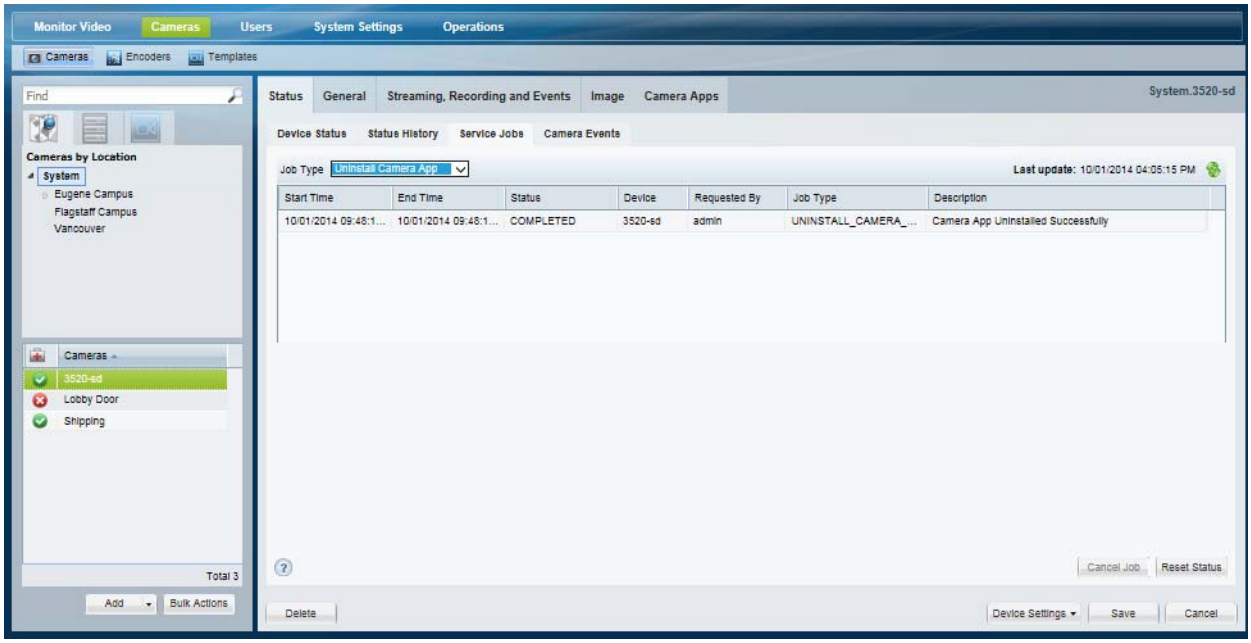


Viewing Service Jobs

Use the Service Jobs tab (Figure 19-7) to view information about the tasks being processed by the Media Server. For more information, see the following:

- Cameras—See Service Jobs (Cameras), page 10-65.
- Cameras—See Service Jobs (Media Server), page 9-11.

Figure 19-7 Camera Service Jobs

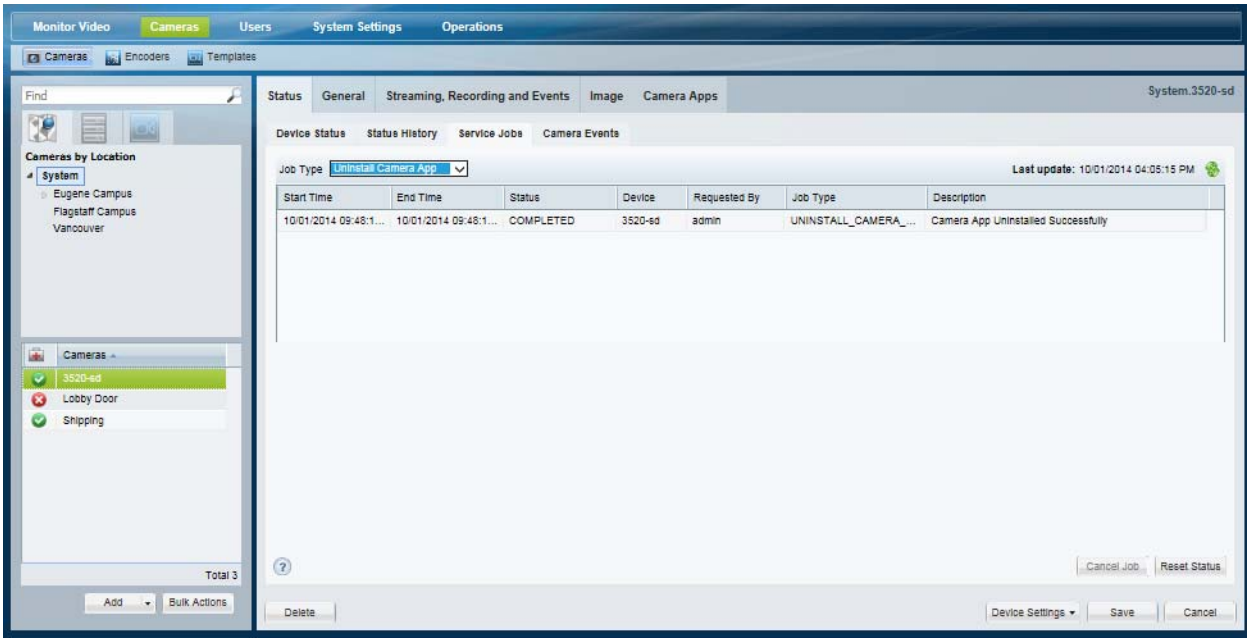


Viewing Camera Events

Use the Camera Events tab (Figure 19-8) to view the security events that occurred on the camera for a period of time. For example, all motion start events or camera app events over the past 12 hours.

See the "Trigger and Action Descriptions" section on page 13-9 for more information on the events that can occur on a camera.

Figure 19-8 Camera Events



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: Device Health Faults on an Operations Manager" section on page 19-6 and the "Device Status: Identifying Issues for a Specific Device" section on page 19-9 for more information.

Usage Notes

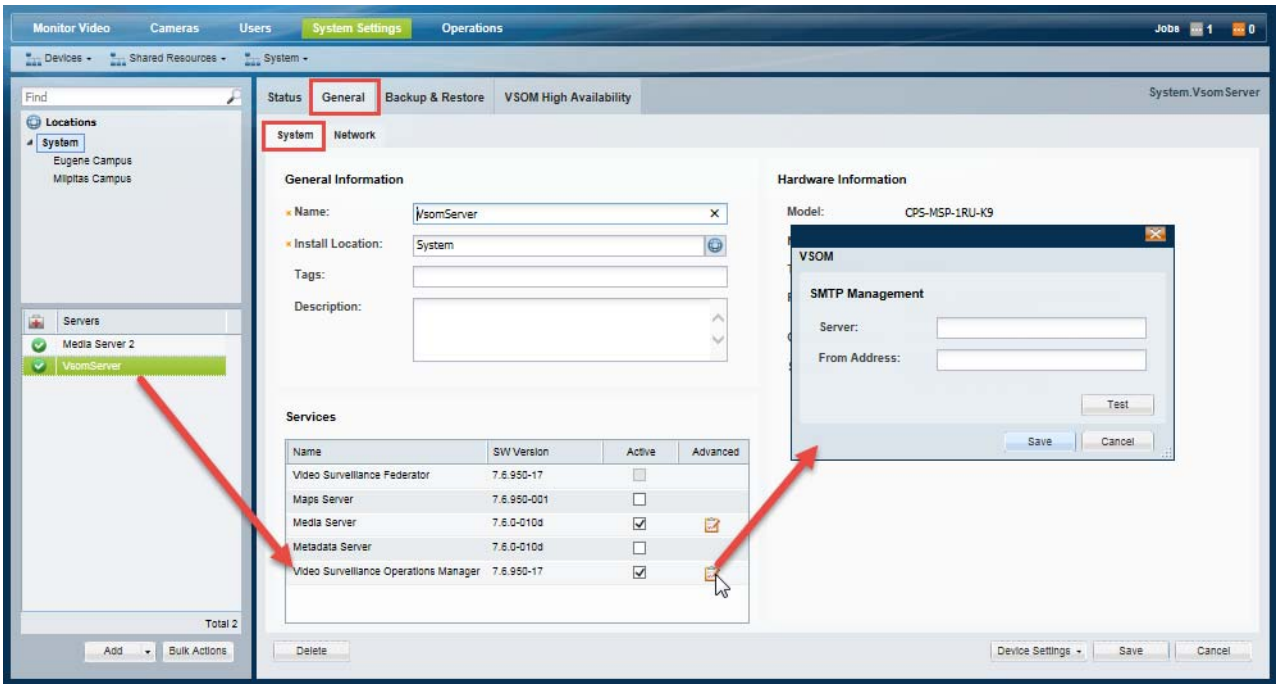
- Emails are sent using the SMTP server address configured for the Operations Manager server using the Cisco VSM Management Console. The SMTP server settings must be accurate or the emails will not be sent (no error or warning is given. See the "SMTP Management Settings" section on page 6-32 for more information. To apply the settings to multiple servers, see the "Bulk Actions: Revising Multiple Servers" section on page 6-26.
- 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 **Initial Time** and **Wait Time** as described in Table 19-6 on page 19-19 to avoid unnecessary notifications.

Procedure

Step 1 Verify that the SMTP server settings are configured correctly in the Operations Manager server (under the **Advanced** icon), as shown in Figure 19-10.

- See the "SMTP Management Settings" section on page 6-32 for more information.

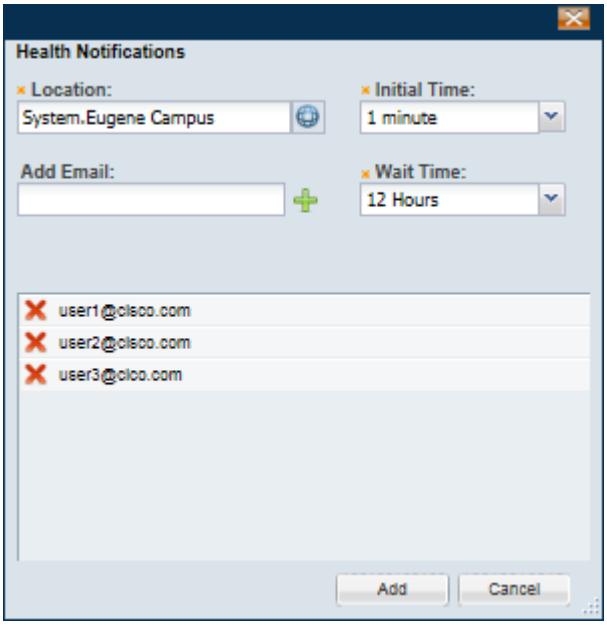
Figure 19-9 Health Notification SMTP Settings



Step 2 Select **Operations** > **Health Notifications**.

Step 3 Click **Add** and enter the notification settings (Figure 19-10).

Figure 19-10 Health Notification Settings



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 Add one or more email addresses:

a. Enter a valid email address in the **Add Email** field.

b. Click the icon (or press `Enter`).

c. Add additional email addresses if necessary.

d. Click the icon to remove an email address.

Step 6 Select the **Initial Time** and **Wait Time** as described in Table 19-6.

Table 19-6 Health Notification Settings

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. • 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. • Default—12 hours • Range—1 to 48 hours

Step 7 Click **Add**.

Step 8 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 19-20
- Delete a Report, page 19-20

Create a Report

Procedure

Step 1 Select **Operations** > **Reports**.

Step 2 Create one or more reports.

a. Click **Add**.

b. 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.

c. 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.

d. Use the **Preview** window to select or deselect the devices or users to be included in the report.

e. Click **Finish**.

f. 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:

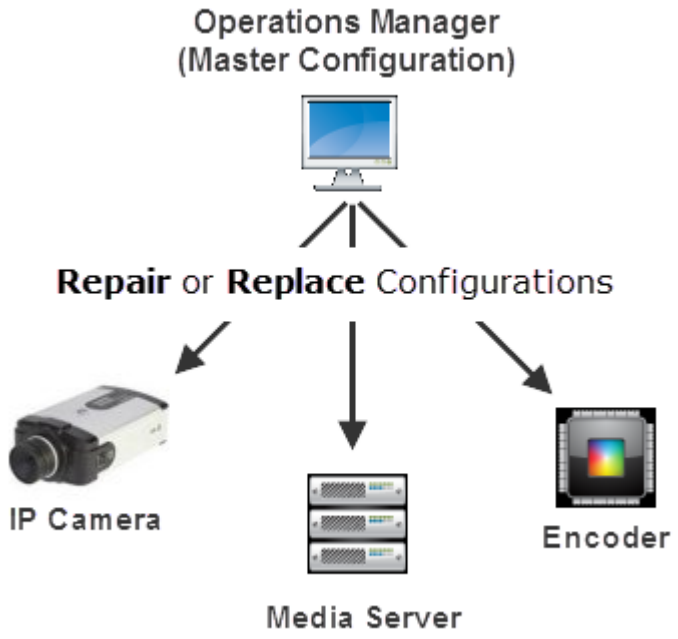
Overview

The Operations Manager configuration is the master configuration(Figure 19-11). 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 19-9
  - Synchronizing Device Configurations, page 19-21

Figure 19-11 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

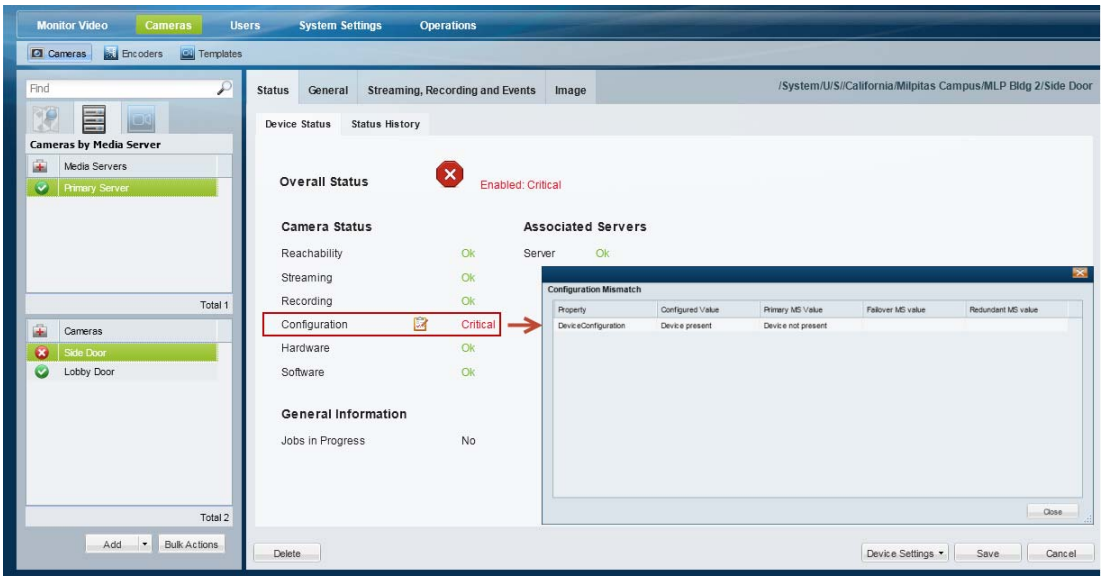
- Click **System Settings** > **Media Server** and select a Media Server.

Step 2 Click the device **Status** tab.

Step 3 Click the icon next to *Configuration* (Figure 19-12).

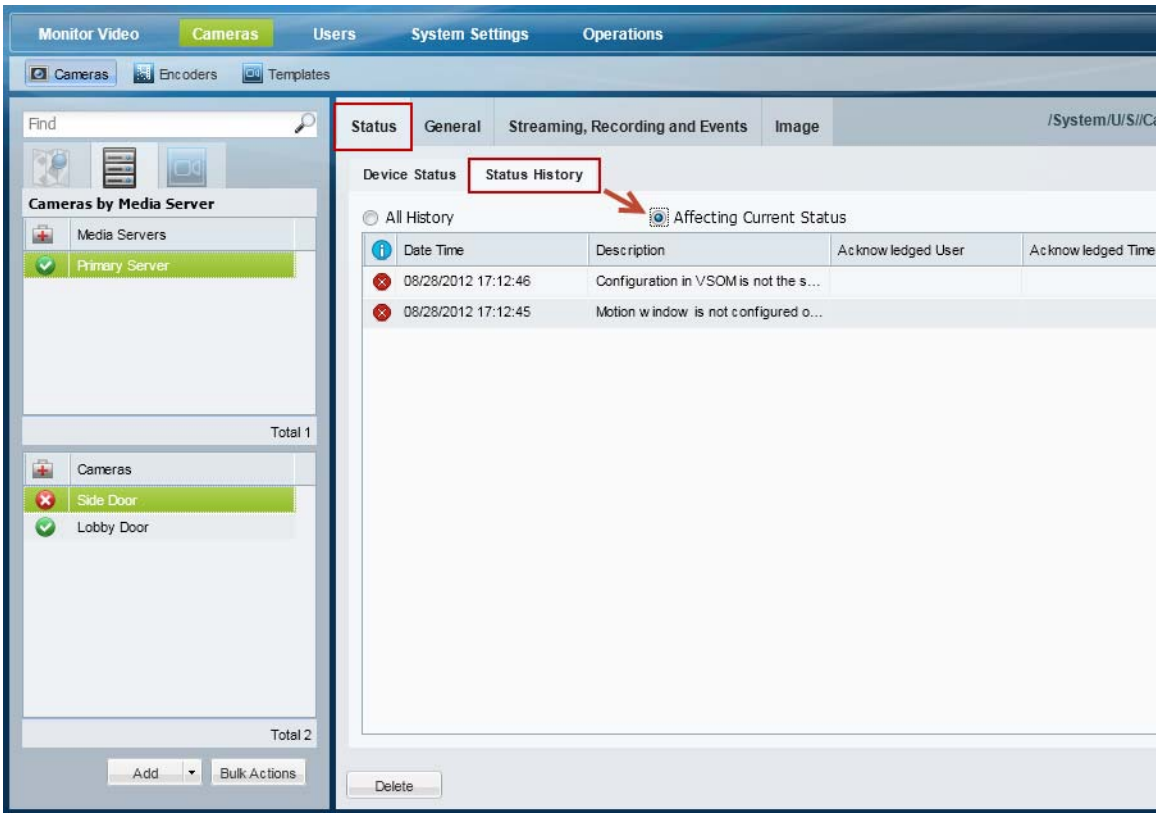
Note The icon appears only if a configuration error occurred.

Figure 19-12 Camera Configuration Mismatch



Step 4 (Optional) Close the window and click **Status History** to view more information regarding the synchronization events (Figure 19-13).

Figure 19-13 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 19-25.
- 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 19-25.

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-mistmatch
- 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 19-23.

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:

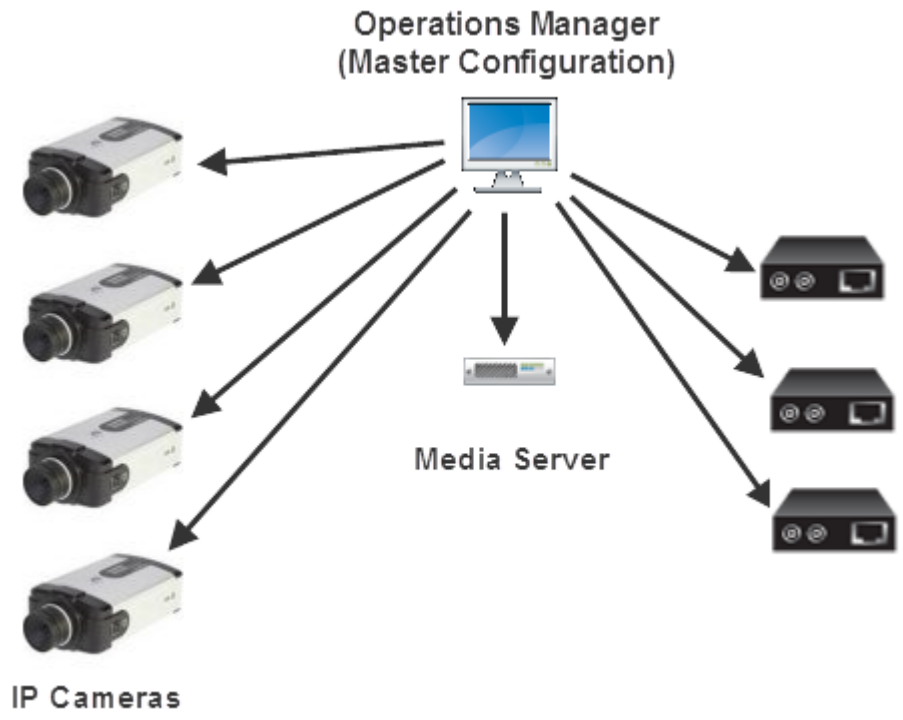
- Wait for the synchronization *Job* to complete. In the Job window, click **View Status** to view any failed steps and click the error message to view additional information.
  See the "Understanding Jobs and Job Status" section on page 19-29 for more information.
- Open the **Status** page for the affected device to view additional details and take corrective action, if necessary. See the "Viewing Device Synchronization Errors" section on page 19-23.

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 19-14).

Figure 19-14 Repairing Configuration Mismatches using Advanced Troubleshooting



Device Data That Is Synchronized

Table 19-7 describes the data synchronized between the Operations Manager and devices (Media Server, cameras, and encoders).

Table 19-7 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 19-7 Synchronized Device Data (continued)

Device Data Type	Master Configuration Source	Description
System-derived operational states	Media Server	For example: • 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	The device configuration is pushed to the Media Server. See the "Cameras Pending Approval List" section on page 10-30 for more information.
Device exists in the Media Server but not in the Operations Manager	Media Server	IP/Analog cameras are added in pre-provisioned state with a basic configuration. Encoders are added as enabled. You must add additional settings such as camera template, location and others settings then enable the device. See the "Adding Cameras from an Existing Media Server" section on page 10-38 and the "Cameras Pending Approval List" section on page 10-30 for instructions to approve the device. **Note** The device can also be placed in the blacklist or deleted.

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 10-38.

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.

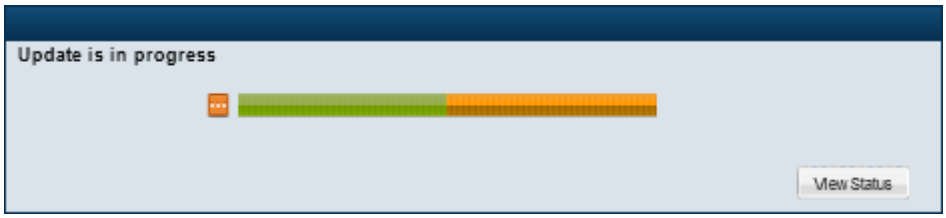
Refer to the following topics for more information:

- Viewing Job Status and Details, page 19-29
- Understanding Job Status, page 19-31
- Viewing All Jobs in the System, page 19-32
- Viewing Audit Logs, page 19-35

Viewing Job Status and Details

A job status dialog appears when a user action triggers a job (Figure 19-15).

Figure 19-15 Job Status Bar

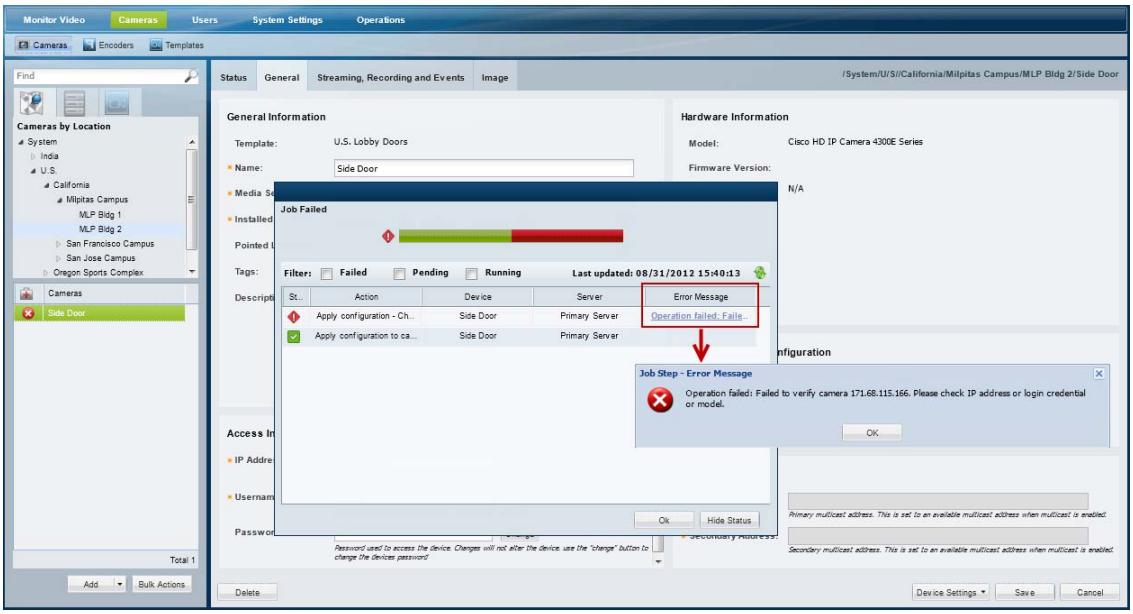


The window automatically closes when the job completes successfully.

See the "Understanding Job Status" section on page 19-31 for a description of the status bar colors and states.

- Click **View Status** to view additional details (Figure 19-16).
- 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 19-32). The Jobs window displays Jobs initiated by the current user. Super-Admins can also view Jobs initiated by other users.

Figure 19-16 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 19-31 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.

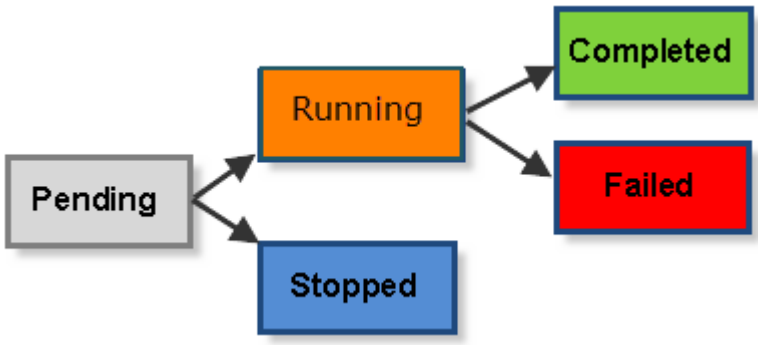
Tip

- If a user has at least one management permission, the Jobs status icons Jobs pending running 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 19-17.

Figure 19-17 Job Status



Status	Color	Description
Pending	Gray	A Job or Job Step that has not begun to process. Only Pending Jobs or Job Steps can be stopped.
Running	Orange	The Job or Job Step has begun to process. The action cannot be stopped and will continue until it either succeeds or fails.
Stopped	Blue	A pending Job or Job Step that was stopped by the user.
Completed	Green	A Job or Job Step that was successfully completed.
Failed	Red	A Job or Job Step that failed to complete. Click the *Error Message* for more information regarding.

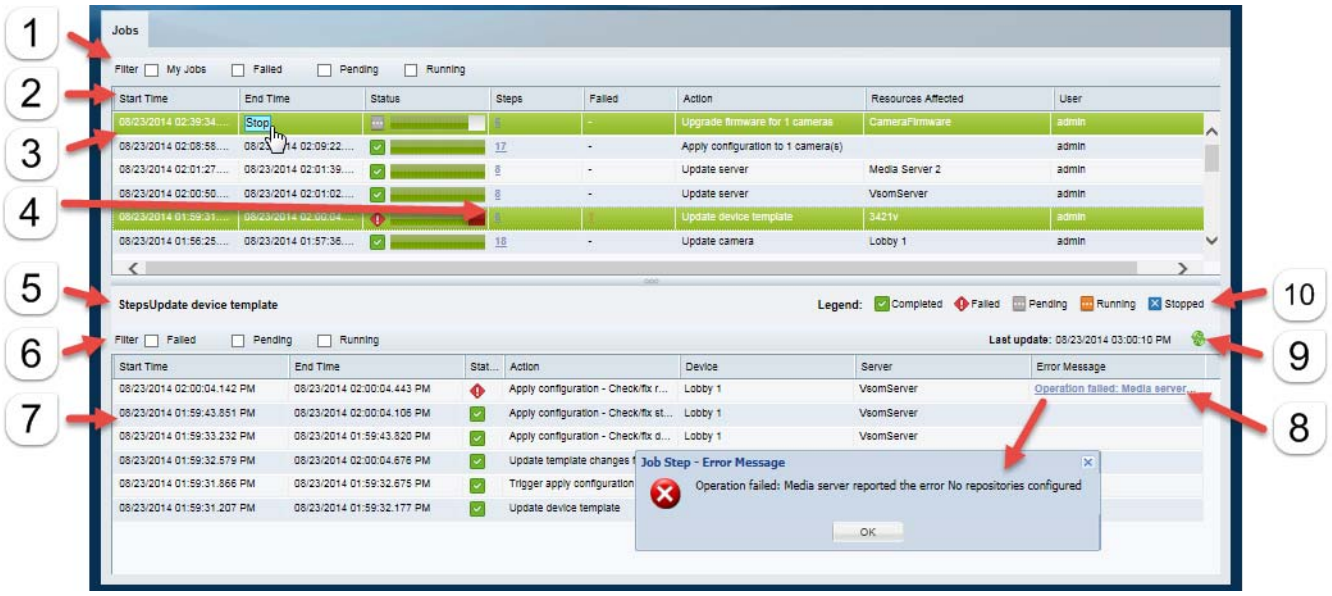
Viewing All Jobs in the System

Click **System Settings > Jobs** (Figure 19-18) 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 19-18 Jobs



	Feature	Description
1	Filter	Select a filter to limit the Job types displayed. For example, click **Failed** to display only failed Jobs. **Note** Click **My Jobs** to view only the Jobs you initiated. This option is only available to super-admin. Most users can only view their own Jobs by default.

2	Job events	Lists the Jobs in the system. Use the filter to narrow the Jobs displayed, or click the column headings to sort the information. **Note** The Job list automatically refreshes to display up-to date status information. Each Job includes the following information: • Start Time—The date and time when the Job was initiated by the user. • End Time—The date and time when the Job ended. A Job can end when it is completed or fails. Jobs with at least one pending Job Step can be stopped (click the **Stop** button). See the "Understanding Job Status" section on page 19-31 for more information. • Status—Indicates the Job status. Refer to the *legend* for a description of each color. See the "Understanding Job Status" section on page 19-31. • Steps—The number of *Job Steps* required to complete the Job. Click the number to display the step details in the bottom pane. • Failed—The number of Failed *Job Steps*. Click the number to display only the failed Job Steps in the bottom pane. • Action—The action or system change performed by the Job. • Resources Affected—The resources affected by the Job. For example, name of the Media Server or the template that is modified by the Job. • User—The user who triggered the Job.
3	Job	Double-click a job to display the sub-steps for that job. If the job is still in progress, click **Stop** to cancel the job, if available.
4	Steps	The number of steps for the job. Click the number to display the sub-steps (you can also double-click the job entry).
5	Job Steps	The sub-steps for a Job (click the *Steps* number or double-click a job entry).
6	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.
7	Job Steps detail	Lists each sub-step that is performed for the selected Job. Click the number under the Step or Failed column to display the steps for a Job. **Note** The Job Step list does not automatically refresh. Click the refresh icon to renew the display and view up-to-date information. Use the filter to narrow the Jobs steps displayed, or click the column headings to sort the information. Each Job Step includes the following information: • Start Time—The date and time when the step began to process. • End Time—The date and time when the step ended. A step can end when it is completed or fails. • Status—Indicates the Job Step status. Refer to the *legend* for a description of each color. See the "Understanding Job Status" section on page 19-31. • 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.
8	Error Message	The reason for a job step error. This is displayed only if an error occurred. Click the error message to display additional details.

9	Refresh icon	Click the refresh icon to renew the display and view up-to-date Job Step status.
9	Legend	Describes the meaning of each *status* color. For example, a green Job *status* bar means the Job was successfully completed. Legend: Completed Failed Pending Running Stopped See the "Understanding Job Status" section on page 19-31 for more information.

Viewing Audit Logs

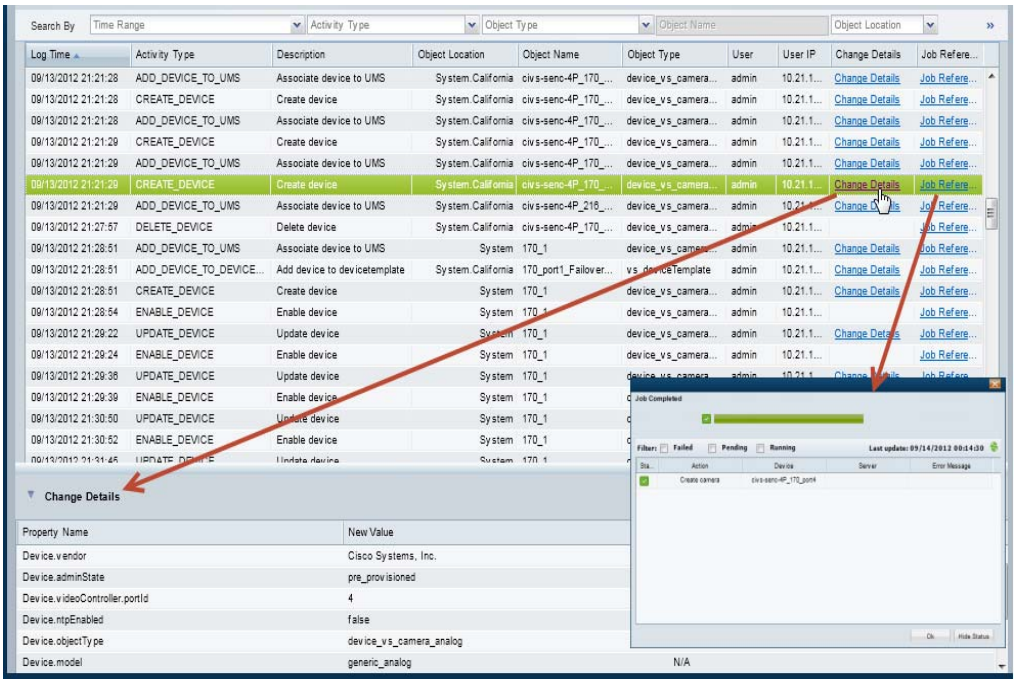
Audit Logs display a history of user configuration actions in the Cisco Video Surveillance deployment. The most common operations are the creation or revision of resources (such as cameras and users), but the Audit Logs also record numerous other activities.

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 19-19).

Figure 19-19 Audit Logs Detail Window



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 19-19).

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

  See the "Understanding Jobs and Job Status" section on page 19-29 for more information.

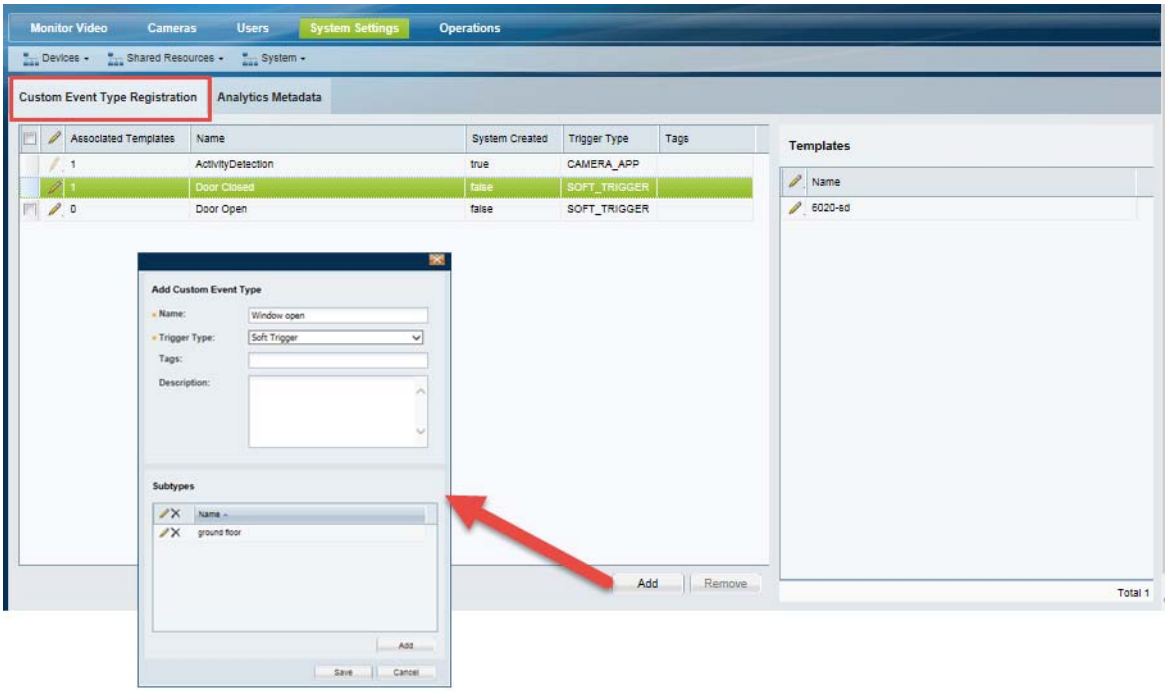
- Click the column headings to sort the list.

Custom Data Management

Use Custom Data Management to do the following:

- View the video analytics metadata types that are registered in Cisco VSM. See Viewing the Registered Metadata Types, page 13-6.
- View and edit event types that can be selected using Advanced events, such as soft triggers and camera apps. See Creating Custom Event Types and Sub Types, page 13-15.

Figure 19-20 Custom Event Type Management



Revising the System Settings

Choose **System Settings > Settings** to define basic parameters for the Operations Manager and Federator.

Note

- 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 settings can only be modified by *super-admin* users.
- The Federator settings are a sub-set of the Operations Manager settings.
- 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.

Contents

Refer to the following topics for more information:

General System Settings

The General settings define user sessions, backup storage rules, and other settings.

Choose **System Settings > Settings**, and the click the **General** tab.

Table 20-1 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 re-enter their username and password to log back in. **Note** The maximum value is 10080 minutes (168 hours / 7 days). The default is 30 minutes.

Table 20-1 General Settings (continued)

Setting	Description
Record Now Duration	(Required, Operations Manager only) 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: • Enabling Record Now, page 3-11 • Using Record Now, page 2-26
Autocorrect Synchronization Errors	(Operations Manager only) 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. Select *Autocorrect Synchronization Errors* 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 *Critical* state. You can then manually correct the error by clicking either the **Repair** or **Replace Config** button in the device configuration page. See the "Synchronizing Device Configurations" section on page 19-21.
Medianet discovery enabled	(Operations Manager only) 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 10-32
Low QOS	(Operations Manager only) The QoS value used for video between Media Server and client.
Medium QOS	
High QOS	
Allow duplicate IP address	Allow duplicate IP addresses for IP cameras. This setting allows cameras to be installed in a private network, using network address translation, (NAT), and still be added to the Operations Manager without causing a device IP address conflict. This setting is disabled by default (duplicate IP addresses are not allowed and will cause a device id conflict). See the "Managing Cameras with Duplicate IP Addresses" section on page 10-22 for more information.
Privacy Mask Timer	(Operations Manager only) The number of minutes before the camera Privacy Mask camera expires (this setting applies to all cameras that support the Privacy Mask feature). When enabled, the Privacy Mask causes a camera to block all live video from that camera. When the timer expires, the operator is reminded to disable the Privacy Mask (which restores the live video stream). The default is 15 minutes. Enter a value between 1 and 120 minutes. See the "Using the Privacy Mask" section on page 2-30 for more information.

Password Settings

The password settings define the rules for user passwords.

Choose **System Settings > Settings**, and the click the **Password** tab.

Table 20-2 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	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. The default is 8 characters.
Maximum Password Length	Enter a value between 40 and 80 to define the maximum number of characters for a valid password. Passwords with more characters that the entered value are rejected. The default is 40 characters.
Identical Password/Username Allowed	If selected, user passwords can be the same as their username. If de-selected, user passwords must be different than their username.
3 Password Groups Required	If selected, user passwords must include characters from at least three different types of characters, including: • lower case letters • upper case letters • symbols • numbers If de-selected, user passwords can include only one type of character (for example, all lower case letters).
Repeat Characters	If selected, user passwords can repeat the same 3 characters. If de-selected, user passwords can *not* repeat the same 3 characters.

Active Users

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

Choose **System Settings > Settings**, and the click the **Active Users** tab.

To log out an active session, select the user session and click **Logout Session**.

Table 20-3 Active User Fields

Setting	Description
Username	The username of the account used to access the system.
First Name	The first name in the user account
Last Name	The last name in the user account

Table 20-3 Active User Fields (continued)

Setting	Description
Super-user	Indicates if the user account is assigned the super-admin role. See Understanding the System-Defined User Roles, Groups and Accounts, page 4-3.
Logged-In Time	The date and time when the user logged in.
Last Access Time	The date and time the user last performed any action on the system.
From IP	The IP address of the device or computer used to access the system.

Language Settings

Language Settings

Language settings define the user interface language, the date and time formats, and the first day of the week. Modify the following settings as needed and click **Save**.

Table 20-4 Language Settings

Setting	Description
System Language	Select a supported language for the user interface text. To upload new or revised language packs, see Language Pack, page 20-5.
Date Format	Select the date format displayed in system messages, alerts, and other generated information. For example, **MM/DD/YYYY** means that dates will appear as month, day, and year. • d = day • M = Month • y = year
Time Format	Select the time format displayed in system messages, alerts, and other generated information. For example, **hh:mm:ss tt** means that the time will be displayed as hours, minutes, and seconds, and include the AM/PM notation. • hh = hour • mm = minute • ss = second • tt = A.M. or P.M.
First day of week	Select the day that should be considered the first day of the week. For example, **Monday**.

Language Pack

Add language packages to display the Cisco Video Surveillance interface in additional languages. You must upgrade the language packs on all servers in your deployment.

Procedure

Step 1 Download the language pack from the cisco.com (see Downloading Software, Firmware and Driver Packs from cisco.com, page 26-4).

Step 2 Upload the language pack:

a. Log in to the Cisco VSM Operations Manager.

b. Go to **System Settings** > **Language Settings** > **System Language**.

c. Click and select the language pack from a local or network drive.

d. Click **Upload**.

Step 3 Select the language for the user interface:

a. After the system is restarted, login to the Operations Manager.

b. Go to **System Settings** > **Language Settings** > **System Language**.

c. Select the system language.

d. Click **Save**.

Backup and Restore

Refer to the following topics to backup the server configuration and video recording files.

Contents

Overview

Server backups can be performed for a single server, or for multiple servers.

- Use the **Backup & Restore** tab in the server configuration page to backup a single server.
- Use the server **Bulk Operations** feature to backup multiple servers.

You can schedule automatic backups, or perform an immediate one-time backup. Each backup creates:

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

To restore a backup, you must restore the files for each server service, and restore the CDAF backup file.

Note We recommend backing up all servers on a regular basis to ensure configuration and event data is not lost if a hardware failure occurs. Backups are also used to restore configurations and historical data when upgrading or moving to a new system. Backup files can be saved to the server ("local") or to a valid FTP server.

You can backup two types of data sets:

- **Configuration Only**—Includes the user-defined configuration, device settings (for cameras, encoders, and Media Servers, user accounts, and other attributes. Also includes installed licenses.
- **Configuration Plus Historical Data**—(Default) Includes the configuration for the server service, data plus events, health notifications, logs, and other information regarding the status, use and health of the system.

Note Recordings are backed up using a Long Term Storage server. See the "Archiving Recordings to a Long Term Storage Server" section on page 17-16.

Refer to the following topics for more information:

Usage Notes

- Each backup includes a separate backup file for each *active* service on the server, *plus* a file for the CDAF service.
- CDAF runs on all servers and provides the Cisco VSM Management Console user interface and features. CDAF backups include the server database, system information, console jobs and other data. The CDAF service must be restored along with the other server services or information may be missing and system errors can occur.

- The maximum number of allowed backups are:
  - Map server service—1 manual and 1 automatic backup.
  - All other server services—5 manual and 3 automatic backups.
- When the maximum number of backups is reached, an existing backup file must be deleted to make room for the new backup file. Automatic backups will automatically delete the oldest backup file. To perform a manual backup, you must manually delete an existing backup file.
- Use Bulk Operations to set the schedule for multiple servers. See Backing Up Multiple Servers (Bulk Actions), page 21-13.
- The Media Server configuration data is backed up automatically to the local server every day by default (and cannot be disabled). Automatic backups must configured for the other server services.
- One FTP server can be configured for each server. The FTP server can be configured for a single server, or for multiple servers (using Bulk Operations).
- Manual backups can be triggered for a single server, or for multiple servers (using Bulk Operations). Bulk action is supported for Media Servers only. The Bulk Action feature does not support Map or Metadata servers.
- Server restore can be performed for a single server only. Bulk server restores are not supported.
- Failed backup(s) are only visible for a single server (on the Server Management page). There is no bulk filtering or display of failed backups in the Bulk Operations page.
- Prior to Cisco VSM release 7.5, automatic backups to local storage could include configuration and historical data. In release 7.5 and later, however, automatic backups to the local disk support configuration data only. When upgrading from release 7.2 or earlier to release 7.5 or later, any automatic backups will be changed to the configuration only option.

Backup Settings

Table 21-1 describes the server backup and restore settings.

Table 21-1 Server Backup Settings

Field	Description
Automatic Backups	
Enable	Select the check box to enable or disable the automatic backup schedule.
Destination	Select where the backup file will be stored: • **On Local**—(Default) Saves the backup file to the server hard drive. • **On Remote**—Saves the backup file to a remote storage network server.
Type	Select the type of data to back up: • **Configuration Only**—Backs up the user-defined configuration, including device settings (for cameras, encoders, and Media Servers), user accounts, and other attributes. • **Configuration Plus Historical Data**—(Default) Backs up the configuration plus events, health notifications, logs, and other data containing information regarding the status, use and health of the system.
Frequency	Define how often backups will occur (**Daily**, **Weekly**, or **Monthly**).

Table 21-1 Server Backup Settings (continued)

Field	Description
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 *At* 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.	
Enable	Select the check box to enable or disable the remote network storage option. If enabled, backups will be saved to the remote destination.
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 21-2 Backup File Formats

Backup Data	File Name Format
Config and Historical	*Service_HostName*_**backup**_*yyyyMMdd_HHmmss*.**tar.gz**
Config Only	*Service_HostName*_**backup_config**_*yyyyMMdd_HHmmss*.**tar.gz**

- *Service*—The service acronym that defines the data stored in the file. For example: VSOM=Operations Manager, VSMC=Management Console, VSF=Federator, etc.
- *HostName*—the host name of the server running the Cisco VSM Operations Manager service.
- *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_20130817_174250.tar.gz`

Backup File Information

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

Figure 21-1 Backup Files Stored on the Server

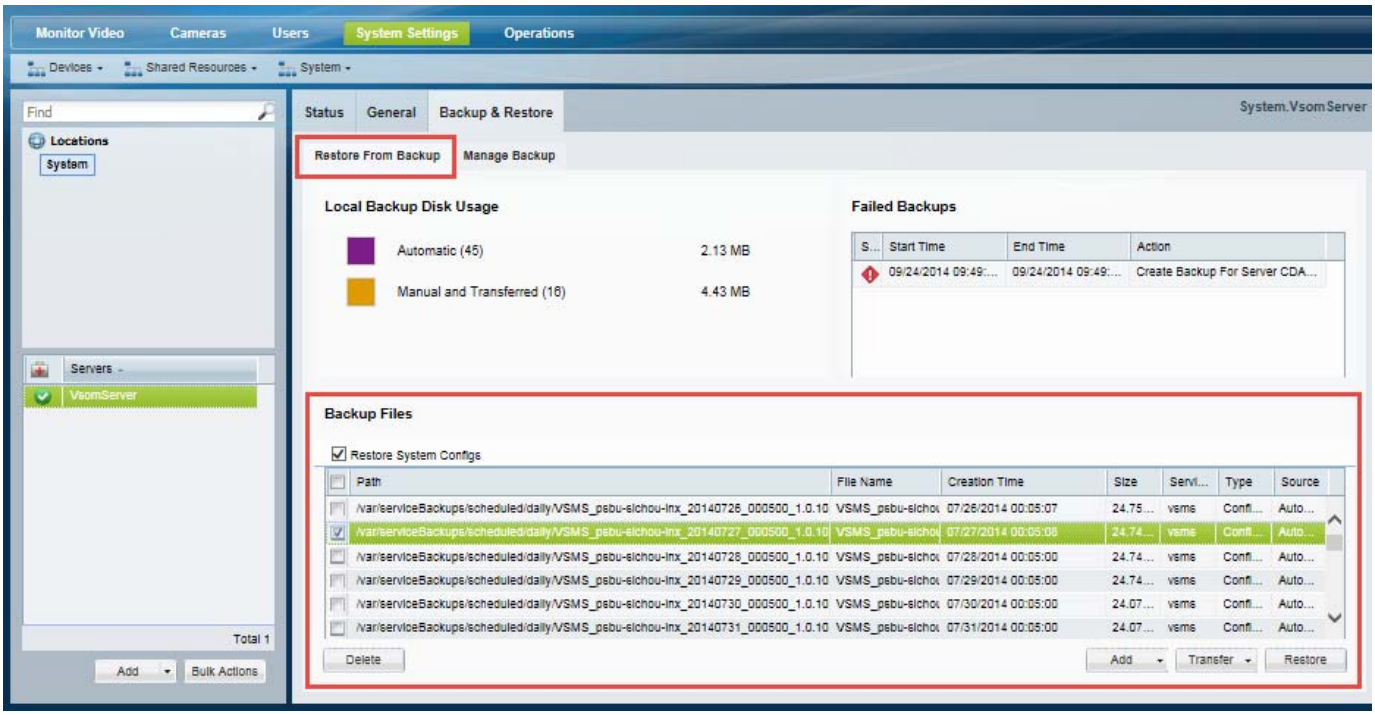


Table 21-3 Backup Files

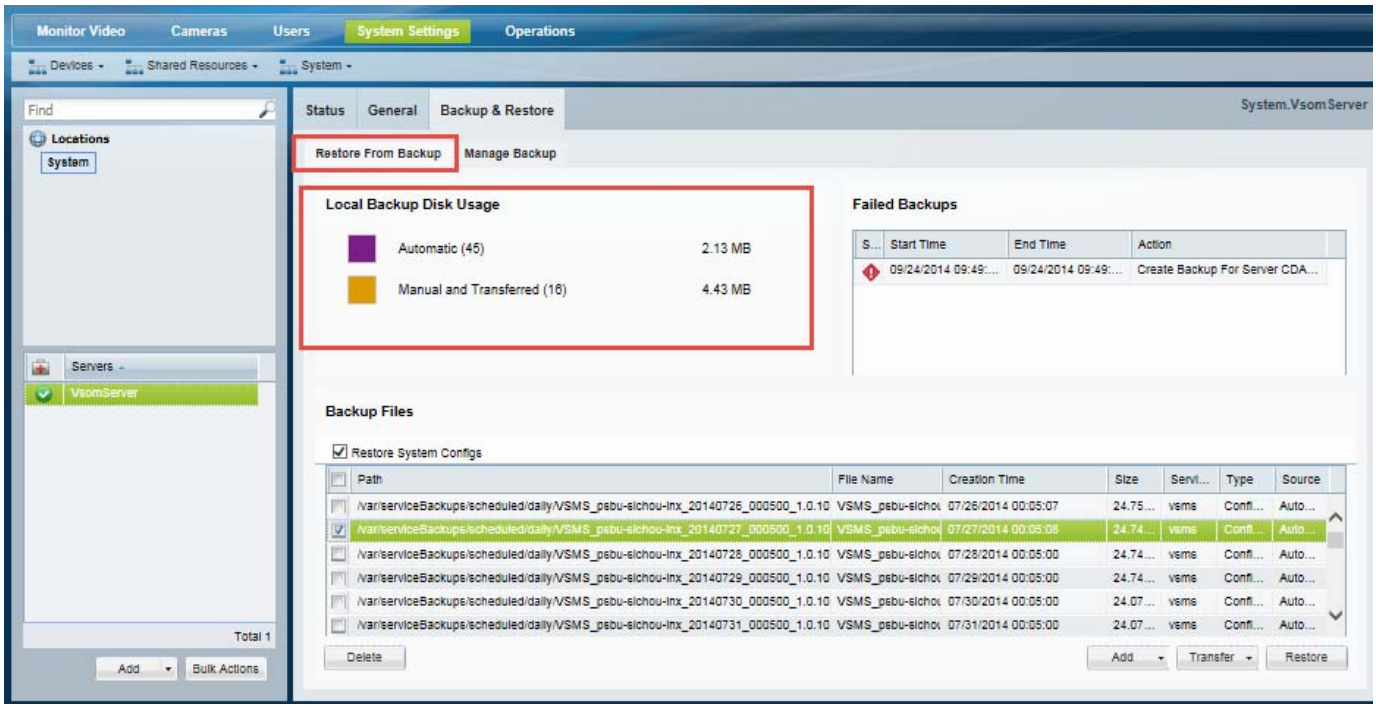
Column	Description
Path	The server directory path where the backup files are stored.
File Name	The file name. See the "Backup File Format" section on page 21-4.
Creation Time	The date and time when the backup file was created.
Size	The size of the backup file.
Service Type	The server service types included in the backup. For example: • VSOM (Operations Manager) • VSMS (Media Server) • CDAF (Console) • Geoserver • Metadata See the "Understanding Server Services" section on page 6-3.
Type	Configuration or configuration plus historical data. See the "Overview" section on page 21-2.
Source	Automatic or manually triggered backup.

Disk Usage for Backups

The Disk Usage graph (Figure 21-2) in the **Restore From Backups** tab displays the total amount of disk space used to store backups, and the number of backup files on the system:

- *Automatic*—The amount of 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 ().

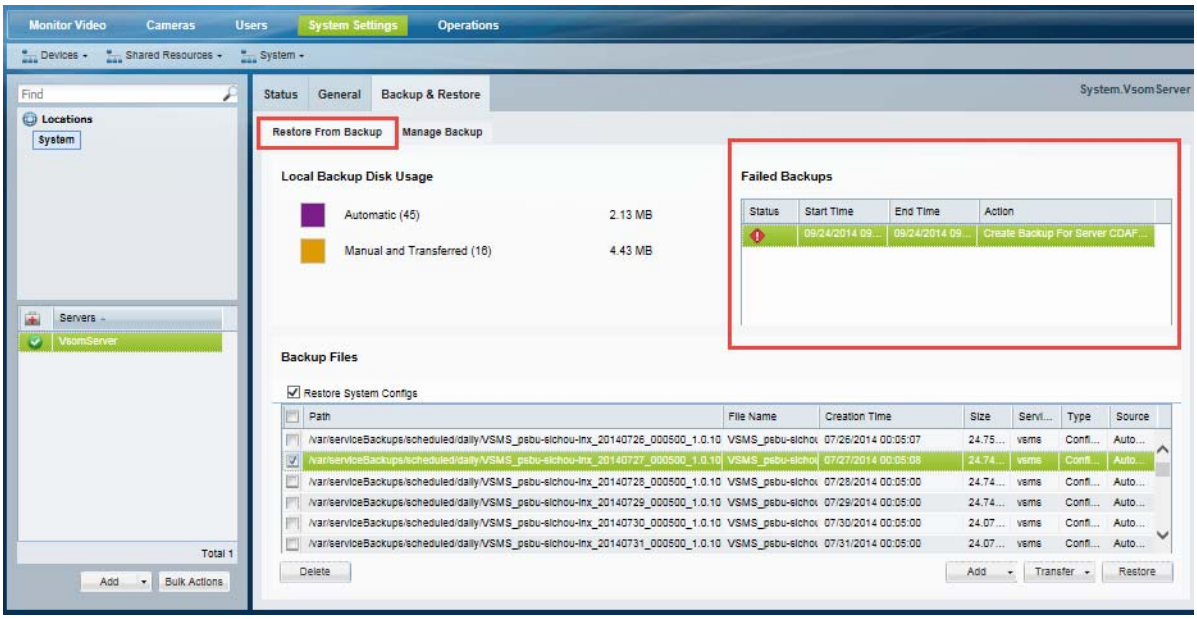
Figure 21-2 Disk Usage for Backup Files Stored on the Server



Failed Backups

The failed backup fields in the **Restore From Backups** tab (Figure 21-3) displays information about the failed manual or automatic backups.

Figure 21-3 Failed Backups



Tip Click an entry to view additional details about the failure reason.

Backing Up and Restoring a Single Server

Use the server Backup & Restore tab to backup the configurations and historical data for all services running on the server (such as the Operations Manager and Media Server).

Note These same techniques apply when backing up a Federator server. See the "Using Federator to Monitor Multiple Operations Managers" section on page 22-1 for more information.

Contents

Refer to the following topics for more information:

Manually Backup a Single Server

To trigger an immediate one-time backup, use the **Backup & Restore** tab in the server configuration page (Figure 21-4):

Procedure

Step 1 Select **System Settings** > **Servers**.

Step 2 Select the **Backup & Restore** tab.

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

Step 3 Select the **Manage Backup** tab.

Step 4 Click **Backup Now** and select **To Remote** or **To Local**.

Step 5 From the pop-up, select the destination and backup type (see Table 21-1 for more information).

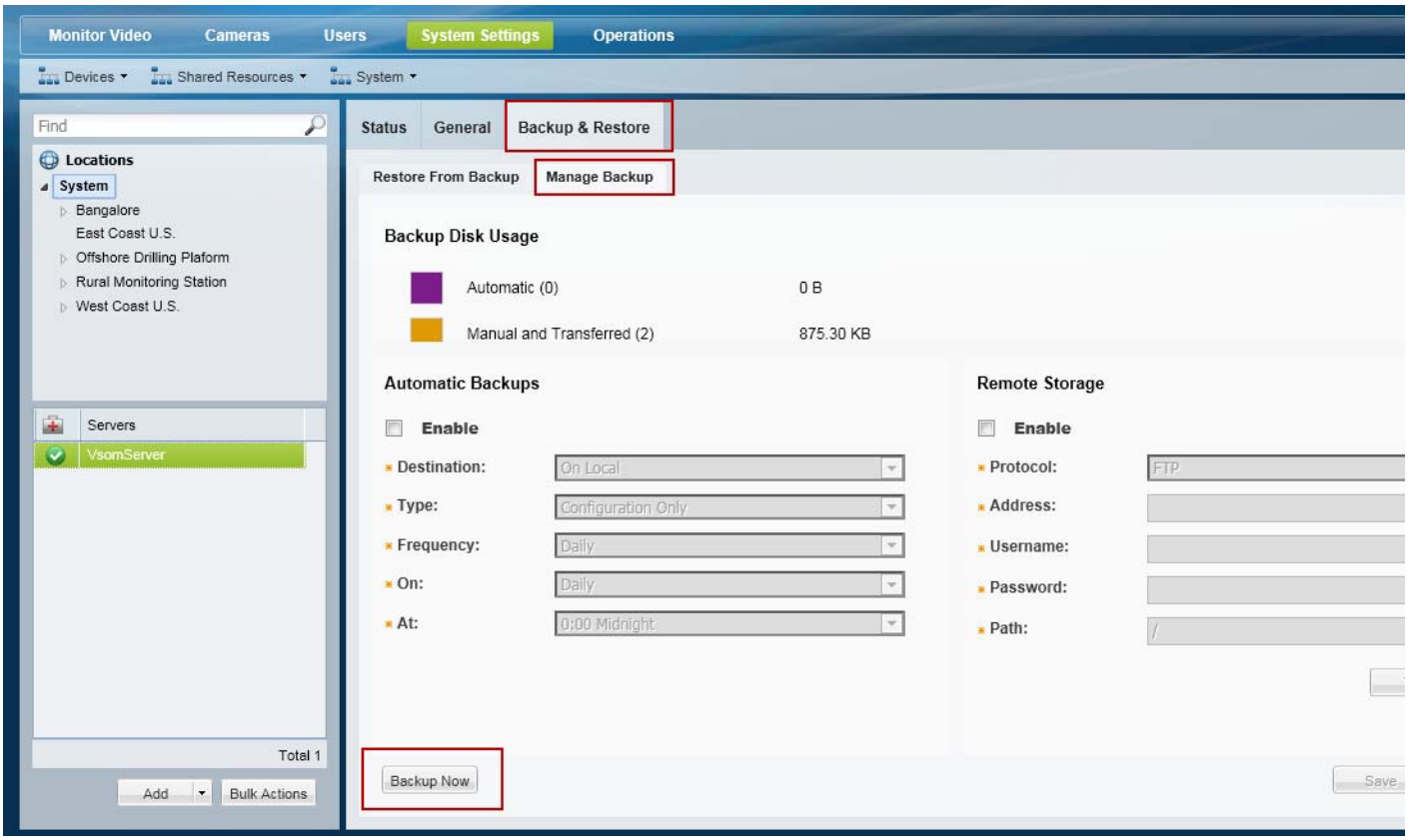
Step 6 Click **OK**.

Step 7 Backup files are saved to the selected destination.

- A separate file is created for each server service, plus an additional file for the DDAF server. See Overview, page 21-2 for more information.
- If saved "To Local", the backup files are saved on the server (in the Restore From Backup tab). See the "Backup File Format" section on page 21-4 and the "Backup File Information" section on page 21-5 for more information.

- Failed backups are displayed in the Failed Manual Backups field. See the "Failed Backups" section on page 21-7.

Figure 21-4 Backup Now



Automatic Backups (Single Server)

To schedule recurring backups for a single server, do the following:

Note

- The Media Server configuration data is backed up automatically to the local server every day by default (and cannot be disabled). Automatic backups must configured for the other server services.
- When the maximum number of backups is reached, an existing backup file must be deleted to make room for the new backup file. Automatic backups will automatically delete the oldest backup file.
- Only the **Configuration** option is supported when the automatic backups are stored on the *Local* server.

Procedure

Step 1 Select **System Settings** > **Servers** (Figure 21-5).

Step 2 Select the **Backup & Restore** tab.

Step 3 Select the **Manage Backup** tab.

Step 4 Select **Enable** in the Automatic Backups section (Figure 21-5).

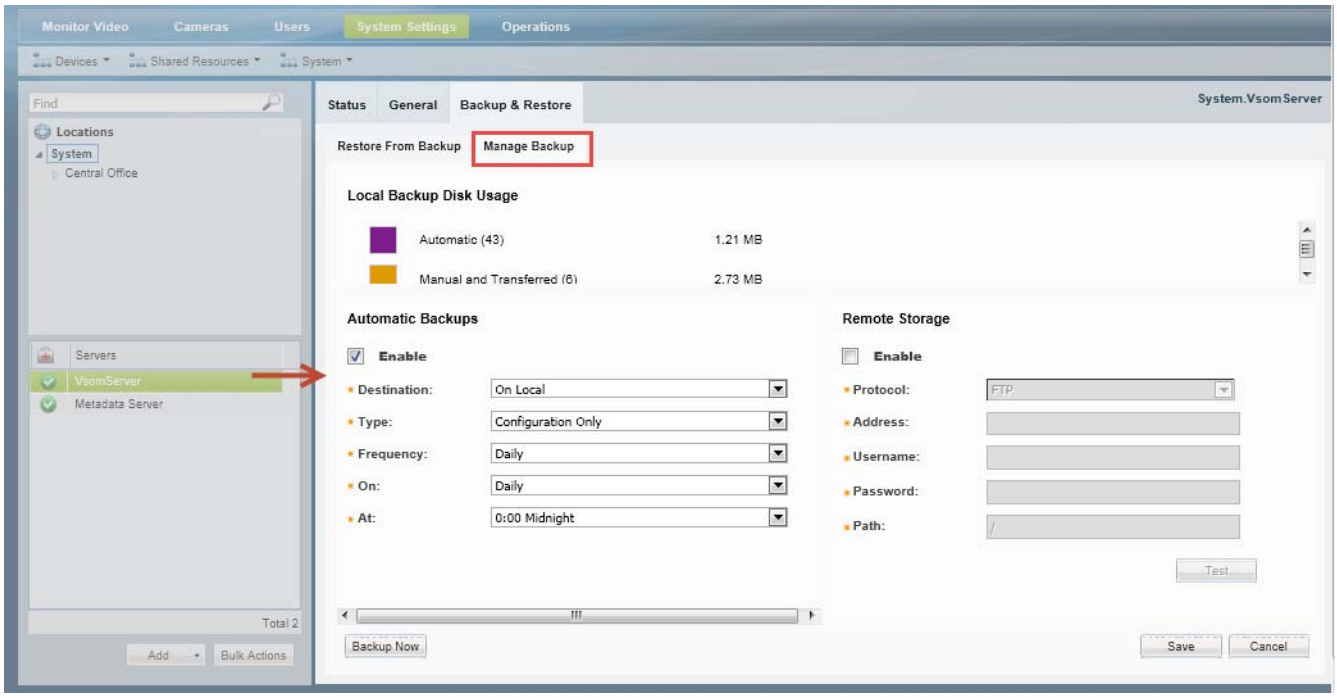
Step 5 Enter the backup settings as described in Table 21-1.

Step 6 Click **Save**.

Step 7 Backup files are saved to the selected destination.

- A separate file is created for each server service, plus an additional file for the DDAF server. See Overview, page 21-2 for more information.
- If saved "To Local", the backup files are saved on the server (in the **Restore From Backup** tab). See the "Backup File Format" section on page 21-4 and the "Backup File Information" section on page 21-5 for more information.

Figure 21-5 Automatic Backups



Restoring a Backup for a Single Server

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

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

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

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

Procedure

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

Step 1 Select **System Settings** > **Servers** (Figure 21-6).

Step 2 Select the **Backup & Restore** tab.

Step 3 Select the **Restore From Backup** tab (default).

Step 4 (Optional) Select **Restore System Config** to exclude the server configuration from the restore operation.

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

Step 5 (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 **Add** > **From Remote** or **From PC**.

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

Note You must first enter the Remote Storage settings in the Manage Backup tab before you can transfer a file from a remote server. See the "Backup Settings" section on page 21-3 for more information.

c. Click **Save**.

d. Repeat these steps to upload the backup file for each service, plus the CDAF (Console) service.

Step 6 Select the backup file for the service you want to restore.

- The Service Type displays the server service: For example: VSOM (Operations Manager), VSMS (Media Server), CDAF (Console), Geoserver, or Metadata.
- See also Backup File Format, page 21-4 and Backup File Information, page 21-5.

Step 7 Click **Restore**.

Step 8 Click **Yes** to confirm the backup and server restart.

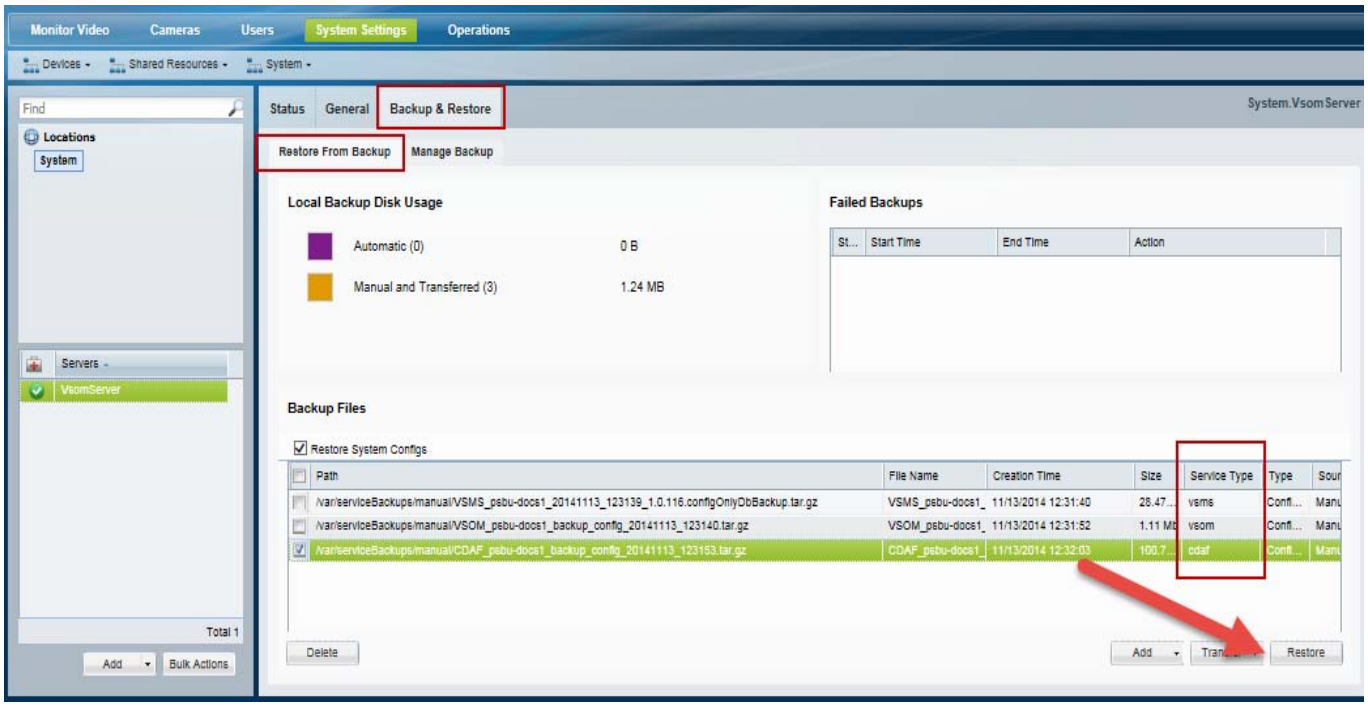
Step 9 Click **OK** when the restore process is complete.

Step 10 Re-login to the server.

Step 11 Repeat these steps to restore the configurations and data for additional service on the server.

Step 12 Repeat these steps to restore the backup for the CDAF (Console) service.

Figure 21-6 Restore Backups



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 Select **System Settings > Servers**.

Step 2 Select the **Backup & Restore** tab.

Step 3 Select the **Restore From Backup** tab (default).

Step 4 (Optional) To first save the file to a PC disk or remote server, click **Transfer** and then **To Remote** or **To PC**.

- **To PC**—select the location for the backup file.
- **To Remote**—the file will be transferred to the location specified in the Remote Storage section of the Configure tab. See the "Backup Settings" section on page 21-3 for more information.

Step 5 Click **Delete** (bottom left).

Step 6 Confirm the operation, when prompted.

Backing Up Multiple Servers (Bulk Actions)

Use the server Bulk Actions feature to back up multiple servers manually, or to schedule automatic backups for multiple servers.

Tip See the "Bulk Actions: Revising Multiple Servers" section on page 6-26 for more information on other options and actions available for multiple servers.

Usage Notes

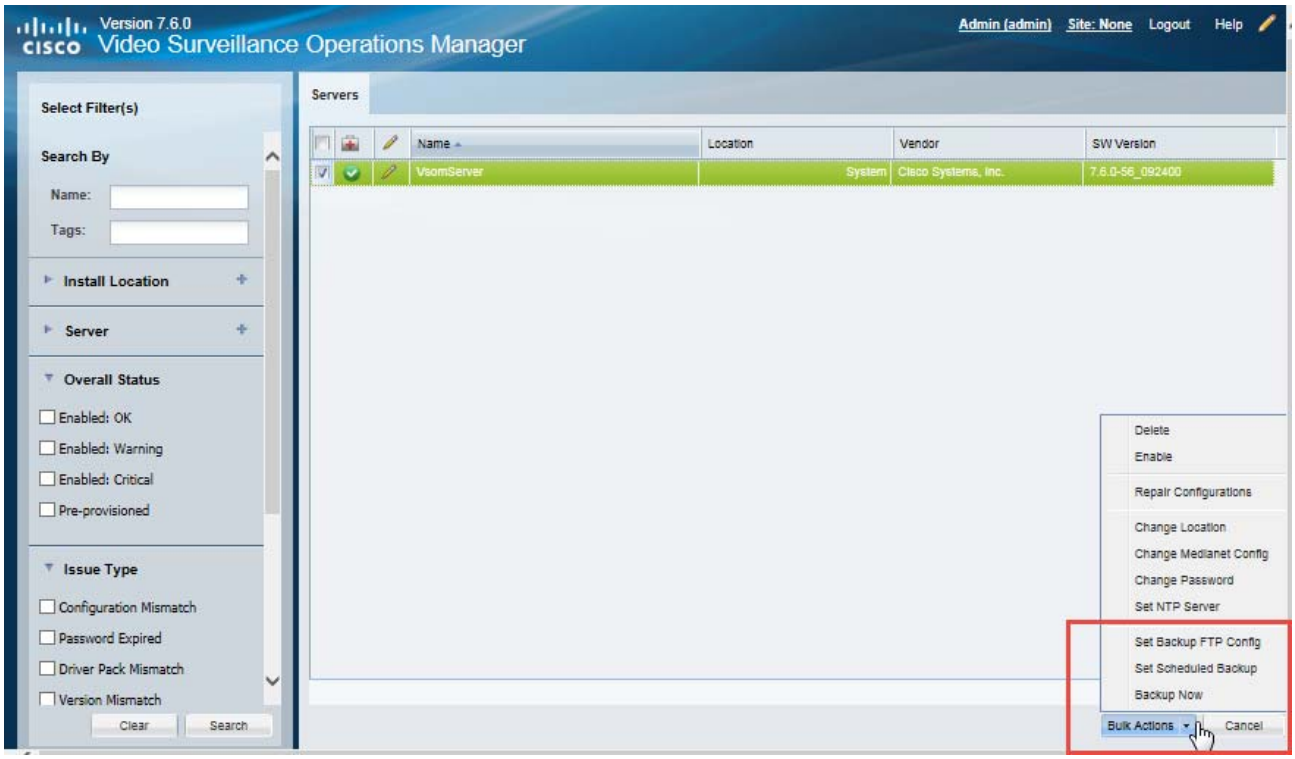
- Bulk action is supported for Media Servers only. The Bulk Action feature does not support Map or Metadata servers.
- All *Active* services in the selected server will be backed up.
- There is one scheduled backup per server. The schedule will be applied to all selected servers.
- One FTP server can be configured for each server. The FTP server configuration will be applied to all selected servers.
- You can only restore backups for a single server, as described in the "Restoring a Backup for a Single Server" section on page 21-10. Bulk Actions cannot be used to restore backups on multiple servers.
- Media Server backups do not include recordings. See the "Backing Up Recordings" section on page 21-16 for instructions to back up recordings to a Long Term Storage (LTS) server.

Procedure

Step 1 Select **System Settings** > **Servers**.

Step 2 Click **Bulk Actions** (under the device list) to open the Bulk Actions window (Figure 21-7).

Figure 21-7 Bulk Actions Window



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

Step 4 Click **Search**.

Step 5 Select the servers to back up.

- 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 6 Click the following backup *Action* buttons that apply.

Table 21-4 Server Bulk Actions

Action	Description
Set Backup FTP Config	Defines the connection settings for the remote server used for server backups. See the "Backup Settings" section on page 21-3 for setting descriptions.

Table 21-4 Server Bulk Actions (continued)

Action	Description
Set Scheduled Backup	Defines when the automatic backups will occur for the selected servers. See the "Backup Settings" section on page 21-3 for setting descriptions. **Note** The Media Server configuration data is backed up automatically to the local server every day by default (and cannot be disabled). Automatic backups must configured for the other server services.
Backup Now	Performs an immediate one-time backup of the selected servers. A separate backup file is created for each active service running on the server. • **To Local**—Saves the backup file(s) to the disk on the server. • **To Remote**—Saved the backup file(s) to a remote FTP server. The FTP server connection must be configured (see "Set Backup FTP Config"). See the "Overview" section on page 21-2 for more information.

Step 7 Refer to the Jobs page to view the action status.

See the "Understanding Jobs and Job Status" section on page 19-29.

Step 8 Review the server Manage Backups page to verify that the backups were successfully created.

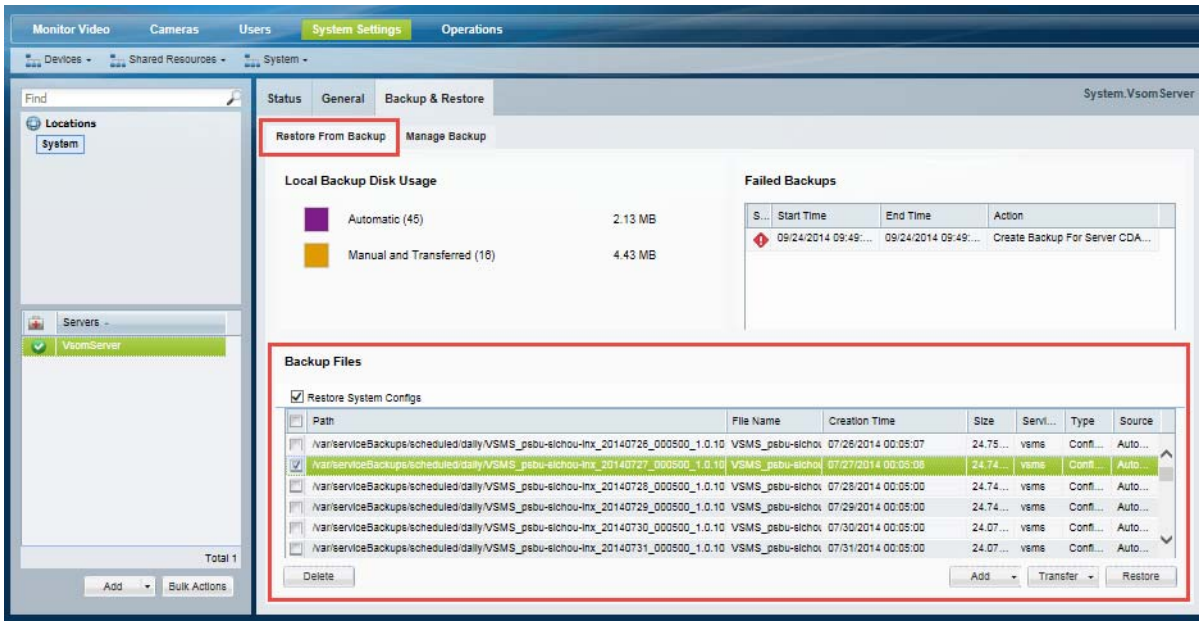
a. Select **System Settings** > **Servers** (Figure 21-6).

b. Select the **Backup & Restore** tab.

c. Select the **Restore From Backup** tab (default).

d. Verify that the backup files appear in the Backup Files list. Failed backups are displayed in the Failed Backups list (Figure 21-8).

Figure 21-8 Server Backup List



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 17-12
- Archiving Recordings to a Long Term Storage Server, page 17-16

For overview information, see the following:

- "High Availability: Cisco Media Servers" section on page 17-1

Using Federator to Monitor Multiple Operations Managers

Federator is a server service that allows users to monitor video and system health from multiple Operations Managers.

Refer to the following topics to install and manage a Federator server, and to view video from the associated Operations Managers using the browser-based utility.

Note

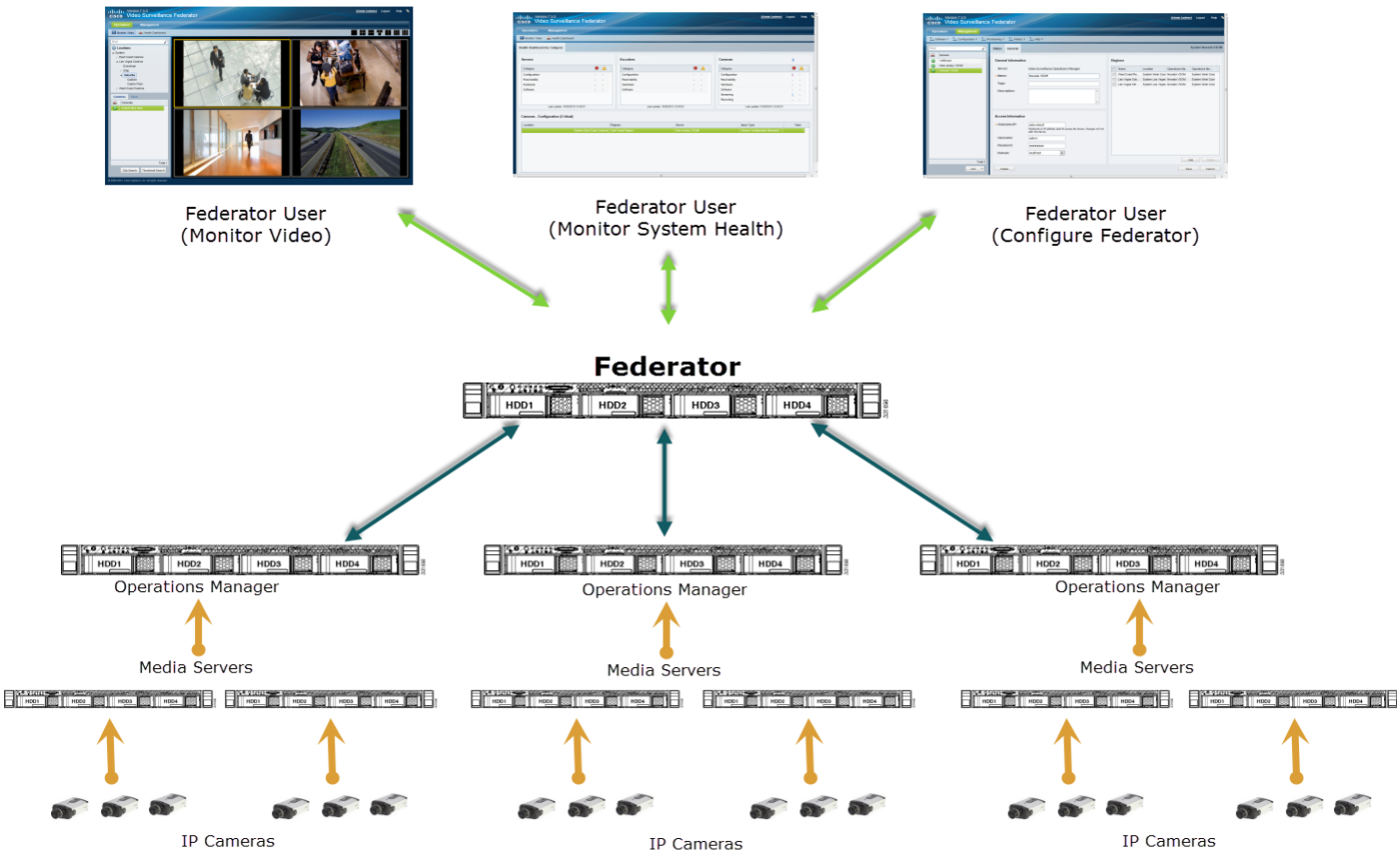
- You can also use the Cisco Video Surveillance Safety and Security Desktop (Cisco SASD) application to view Federator resources. See the Cisco Video Surveillance Safety and Security Desktop User Guide for more information.
- To configure server settings such as the network time protocol (NTP) and network settings, or to view hardware information and logs, use the Cisco VSM Management Console. See the Cisco Video Surveillance Management Console Administration Guide for more information.

Contents

Overview

The Cisco Video Surveillance Federator allows users to view video and monitor system health from multiple Operations Managers (Figure 22-1). The Federator service is enabled on a Cisco VSM server, and Operations Manager servers are then added to the Federator configuration. Federator users (which are different from the Operations Manager users) are provided access to Operations Manager locations based on their access permissions in Federator. Each Federator supports up to 500 Operations Managers (a license is required for the number of Operations Managers associated with the Federator).

Figure 22-1 Cisco Video Surveillance Federator



Note: All servers can be physical or virtual machines. Federator, Operations Manager, and Media Server are "services" that run on the server.

For example:

- A company has warehouse facilities in different regions of the country. Each facility includes an Operations Manager that manages multiple Media Servers and related cameras. Currently, users must log in to each Operations Manager separately to view video and monitor device status for each site. Federator, however, allows central office users to log in to Federator and simultaneously access video and device health from the Operations Managers in multiple warehouses.
- Another company manages retail stores in different regions of the country. Federator can be used to monitor video and system health in all regions. For example:
  - Security personnel can monitor video from the stores in different locations, even through each location has a separate Operations Manager.

  - Financial managers can monitor video only from the cashier booths.
  - System administrators can monitor system and device health for the cameras, encoders and servers in all regions.

Capacity

Each Federator server supports the following:

- 500 Operations Manager servers
- 2000 regions
- 200 client workstations

Requirements

Table 22-1 Federator Requirements

Requirements	Complete? (✓)
At least one Federator server must be installed on the network. • A physical or virtual machine must be installed. • The Federator service must be enabled (see the "Initial Server Setup" section on page 22-9). **Notes** To configure server settings such as the network time protocol (NTP) and network settings, or to view hardware information and logs, use the Cisco VSM Management Console. See the Cisco Video Surveillance Management Console Administration Guide for more information. **Related Documentation** • 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 Federator service.	❑
The IP address or hostname of the Federator server.	❑
A valid Federator server username and password. **Notes** • The default credentials for a new or factory restored server is **admin/admin**. • The username and initial password for all other users is defined when the user account is created (see the "Adding Users" section on page 4-15). • All users are prompted to reset the password at first login.	❑

Table 22-1 Federator Requirements (continued)

Requirements	Complete? (✓)
A Federator license must be purchased and installed to enable a specific number of Operations Managers that can be managed by the system. • Federator supports one Operations Manager by default. • An additional license must be installed to support multiple Operations Managers. • Each Federator supports a maximum of 500 Operations Managers. See the "Initial Server Setup" section on page 22-9 for instructions to install Federator licenses.	❑
The IP address and login credentials for each Operations Managers that will be added to the Federator configuration: • Operations Manager server address (IP address or hostname). • Login credentials (username and password) for the Operations Manager. **Notes** • See the "Adding Operations Manager Servers to Federator" section on page 22-19 for more information. • The server account must include access permissions for the required Operations Manager resources (such as cameras). • The username and password for the Operations Managers is different that the Federator credentials. Each system required a separate user account. • Operations Manager servers cannot be pre-provisioned when added to a Federator. If the Operations Manager is not accessible, the status is "unreachable".	❑
To use the browser-based administration tool described in this document, the following is required: **A PC or laptop with the following:** • 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." **The Internet Explorer (IE) web browser.** • Windows Version – Windows 7 supports IE 9 or 10. – Windows 8 supports IE 10, desktop version (the Metro version of IE 10 is not supported). • 32-bit or 64-bit – 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). See the Cisco Video Surveillance Monitoring Workstation Performance Baseline Specification for the complete baseline performance specifications for a video surveillance monitoring workstation.	❑

Table 22-1 Federator Requirements (continued)

Requirements	Complete? (✓)
The Cisco Multi-Pane client software installed on the PC is required to view video. • 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 Cisco VSM Federator, 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. **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.	❑
Federator resources (video) can be monitored using the following applications: • The browser-based monitoring tool (described in this document). • The Cisco Video Surveillance Safety and Security Desktop (Cisco SASD) desktop application. See the Cisco Video Surveillance Safety and Security Desktop User Guide for more information.	❑

Summary Steps

Configuring the Cisco VSM Federator is similar to configuring an Operations Manager. You must enable the Federator *service* on the server using the Management Console, and then use the Federator browser-based interface to configure system settings, schedule backups, and add users, servers, locations and regions. Federator users can then log in and monitor video and system health from multiple Operations Managers.

Table 22-2 summarizes the configuration process. See the "Configuring Access to Operations Manager Resources" section on page 22-17 for detailed instructions.

Table 22-2 Summary Steps: Federator Configuration

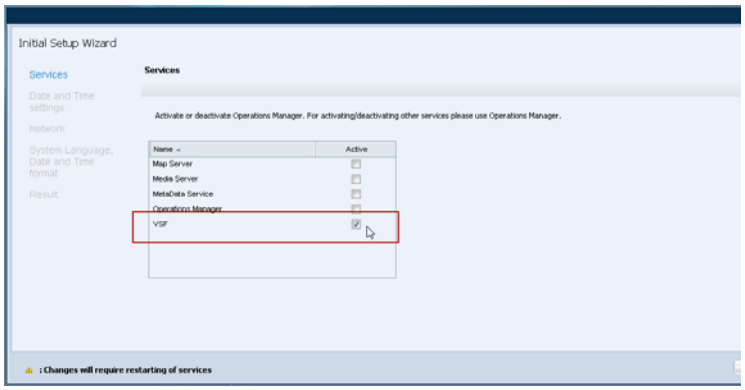
	Task	Description	Complete? (✓)
Step 1	Install a physical or virtual Cisco VSM server (Release 7.5 or higher)	• Physical Servers— See the Cisco Physical Security UCS Platform Series User Guide for more information. • Virtual Machines—See the Cisco Video Surveillance Virtual Machine Deployment and Recovery Guide for UCS Platforms for instructions to install the server software .ova image as a virtual machine (VM).	❑
Step 2	Use the Cisco VSM Management Console Initial Setup Wizard to enable the Federator service.	The Federator service enabled the Federator features and browser-based configuration interface. It also allows the Cisco SASD Federator desktop application to access the server and associated Operations Managers.  Complete the other required settings (such as the network settings) as instructed. See the Cisco Video Surveillance Management Console Administration Guide for more information.	❑

Table 22-2 Summary Steps: Federator Configuration (continued)

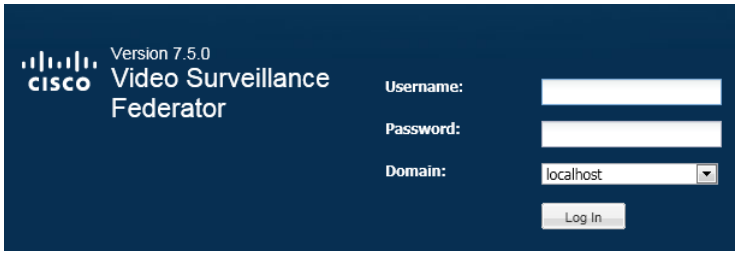
	Task	Description	Complete? (✓)
Step 3	Log in to the Cisco VSM Federator server.	See the "Logging In and Managing Passwords" section on page 1-18. Enter a new password if prompted. 	❑
Step 4	Install the Federator license.	The license defines how many Operations Manager servers can be managed by the Federator. **Tip** The license must be installed on the Federator server interface (not the Operations Manager). See the "Initial Server Setup" section on page 22-9.	❑
Step 5	Define the system settings.	The system settings define attributes such as the user timeout period and user password rules. See the "Initial Server Setup" section on page 22-9.	❑
Step 6	Define the backup schedule.	Backups preserve the Federator configuration and data if a system failure occurs or the system software is reinstalled. • You can also configure automatic backup schedule. • Backups can be stored on the server or on a remote FTP site. See the "Initial Server Setup" section on page 22-9.	❑
Step 7	Add the Operations Manager servers.	Add the Servers that will be managed by the Federator. • Resources are only available for the servers added to Federator. • The available Operations Manager resources are defined by the login credentials entered in the server configuration. For example, if the server credentials allow access to only a sub-location, then only the resources for that sub-location are available to Federator users. See the "Adding Operations Manager Servers to Federator" section on page 22-19.	❑

Table 22-2 Summary Steps: Federator Configuration (continued)

	Task	Description	Complete? (✓)
Step 8	Create the locations.	Federator locations allow you to organize the Operations Manager resources (such as video streams) according to the real-world location of the server, or by the type of video available on the server (such as cameras in warehouses). • User Groups are also associated with locations define user access permissions. • "Regions" are used to map an Operations Manager location to a Federator location. See the "Adding Federator Locations" section on page 22-23.	❑
Step 9	Create the Regions, and associate each Region with an Operations Manager location and a Federator location.	Regions allow you to map an Operations Manager location to a Federator location. The resources available in the Operations Manager location are displayed in the Federator location. For example, if an Operations Manager includes locations for California and New York, you can create a "West Coast" Region that includes only the California locations (and associated attributes), and map that to the West Coast Federator location. See the "Adding Federator Regions" section on page 22-25.	❑
Step 10	Add the users that can access the Federator server.	Add Roles, User Groups and Users. Creating users is the same as Operations Manager, but you can only grant full Manage permissions (users can manage all Federator features, or none at all). See the "Adding Federator Users" section on page 22-27.	❑
Step 11	Monitor video from the Operations Managers associated with the Federator.	See the "Monitoring Video Using Federator" section on page 22-30.	❑
Step 12	Monitor system health for all Operations Managers (and associated devices, such as Media Servers, cameras and encoders).	See the "Monitoring Device Health Using the Browser-Based Federator" section on page 22-34.	❑

Initial Server Setup

After the physical or virtual Federator server is installed and setup using the Cisco VSM Management Console, you can log in to the Federator browser-based interface and complete the initial system settings. This includes installing the license that defines how many Operations Managers can be managed by the Federator, the basic system settings, and the server backup schedule.

Initial Setup Procedure

Step 1 Install a physical or virtual Cisco VSM server.

- Physical Servers— See the Cisco Physical Security UCS 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).

Step 2 Enable the **Federator** service using the server's Initial Setup Wizard (Figure 22-2).

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

b. Enter the URL for the server's Cisco VSM Management Console. The syntax is: **http://**<*server-ip-address or hostname*>**/vsmc/**

Platform	Server Address
Physical server: Cisco Multiservices Platform (Cisco MSP)	The default (factory) static IP address is: **http://192.168.0.200/vsmc/**
Virtual Machine: Cisco Unified Computing System (Cisco UCS) platform	The Cisco VSM server includes two network ports with the following default configuration: • Eth0 port—static IP address 192.168.0.200 • Eth1 port— DHCP The network settings can also be changed using the guest OS console when installing the server software OVA image. See the "Configuring the Network Settings" section of the Cisco Video Surveillance Virtual Machine Deployment and Recovery Guide for UCS Platforms for more information.

Step 3 Enter the Management Console password.

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

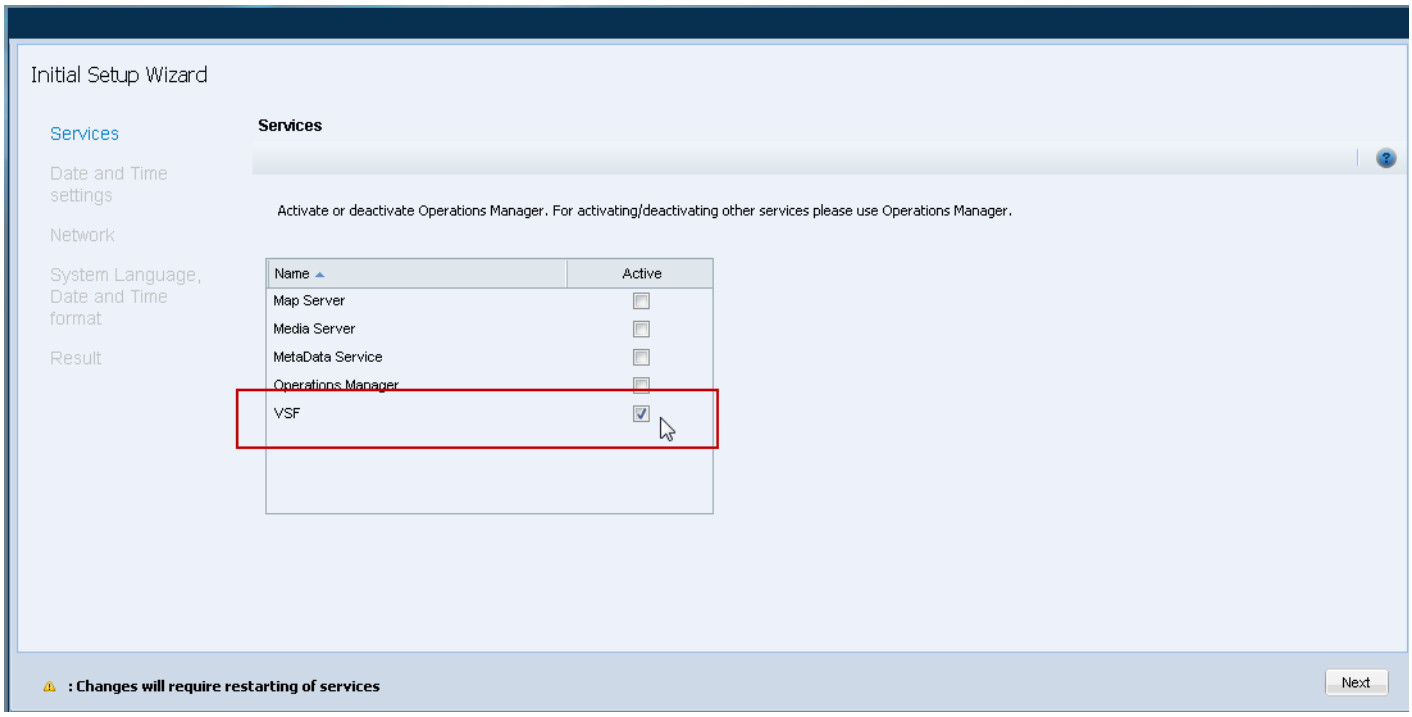
Tip See the Cisco Video Surveillance Management Console Administration Guide for more information.

Step 4 Click **Log In**.

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

Step 6 Select the **VSF** service (Federator) during the Initial Setup Wizard (Figure 22-2).

Figure 22-2 Enabling the Federator Service Using the Management Console Initial Setup Wizard



- The Wizard appears during the first login.
- Only the Federator service can be enabled on a server (to ensure system performance).
- See the Cisco Video Surveillance Management Console Administration Guide for more information.

c. Click **Next** and complete the remaining Wizard settings (such as the network settings).

d. Restart the server services when prompted (Figure 22-3).

Figure 22-3 Restarting Server Services Using the Management Console Initial Setup Wizard

Step 7 Log in to the browser-based Federator interface.

a. 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.

b. Enter the Federator URL or IP address.

The syntax is: **https://***server-address***/vsf/**

For example: `https://vsm-server.cisco.com/vsf`

c. Enter your username and password.

- The default credentials for a new or factory restored server are **admin/admin**.
- The initial system includes an admin login for the super_user. You can create additional users with various access permissions, as described in the "Adding Federator Users" section on page 22-27.
- See the "Logging In to a Federator Server" section on page 22-15 for more information.

d. Enter a new password, if prompted.

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

See the "Logging In and Managing Passwords" section on page 1-18 for more information.

Step 8 Install a Federator license to enable the number of Operations Manager (VSOM) servers that can be added to the Federator.

Tip See the "Installing Licenses" section on page 1-26 for more information.

a. Purchase and obtain the license.

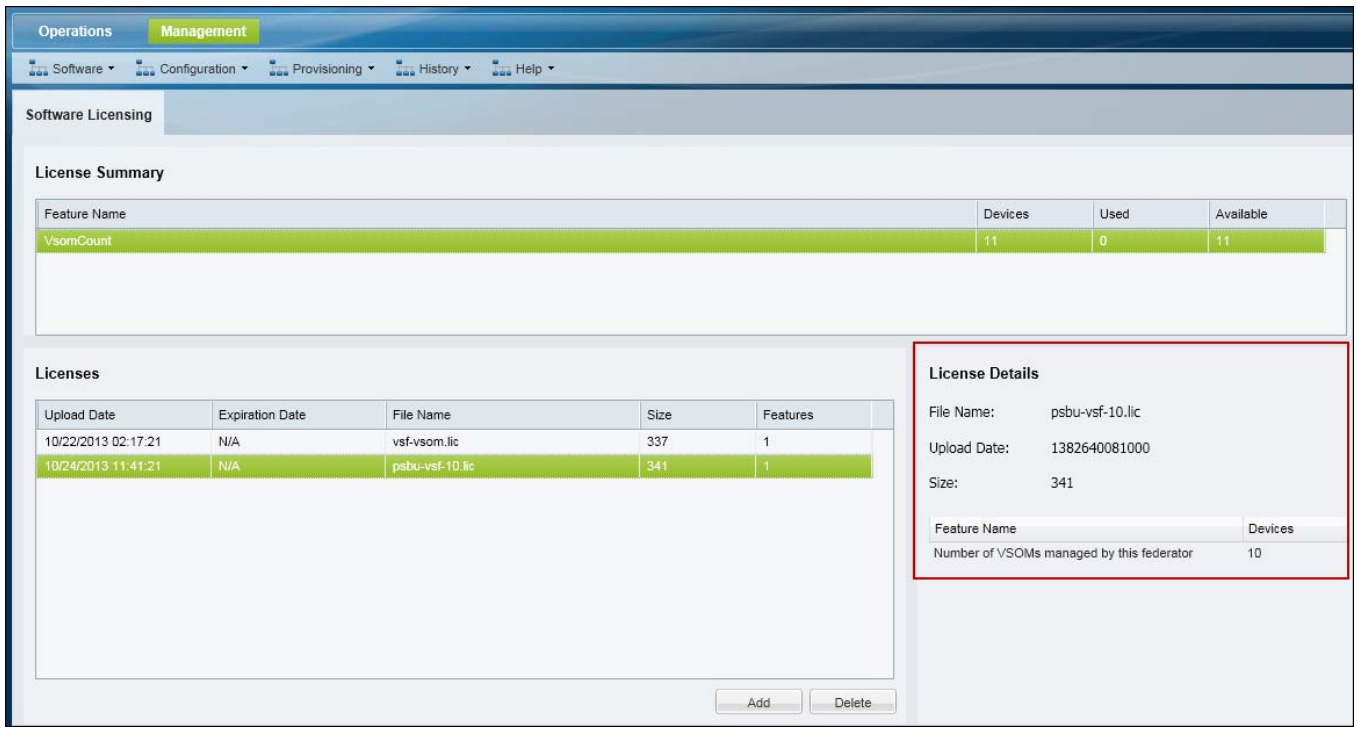
b. Select **Management > Software Licensing** (Figure 22-4).

c. Click **Add** and select the license file located on your local drive.

d. 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. The license enables the number of Operations Manager (Operations Manager) servers that can be managed by the Federator. In the Figure 22-4 example, the license supports 10 additional Operations Manager (VSOM) servers (for a total of 11).

Figure 22-4 Installing the Federator License



Step 9 (Optional) Revise the default system settings.

a. Choose **Management > Settings**.

b. In the **General** tab, enter the User Timeout, in seconds.

This is the number of minutes before a user is automatically logged out due to inactivity. After this period, users must re-enter their username and password to log back in.

See the "General System Settings" section on page 20-1 for more information.

c. In the Password tab, enter the password rules for users, such as the required length and syntax requirements.

See the "Password Settings" section on page 20-3 for more information.

Step 10 Define an automatic backup schedule.

Tip The Federator backup procedure is similar to the Operations Manager procedure. See the "Backing Up and Restoring a Single Server" section on page 21-8 for more information.

Note We recommend backing up all servers on a regular basis to ensure configuration and event data is not lost if a hardware failure occurs. Backups are also used to restore configurations and historical data when upgrading or moving to a new system.

a. Select **Management** > **Backup & Restore**.

b. Select the **Manage Backup** tab (Figure 22-5).

c. Select **Enable** in the Automatic Backups section

d. Select the backup frequency settings.

   See the "Backup Settings" section on page 21-3 for setting descriptions.

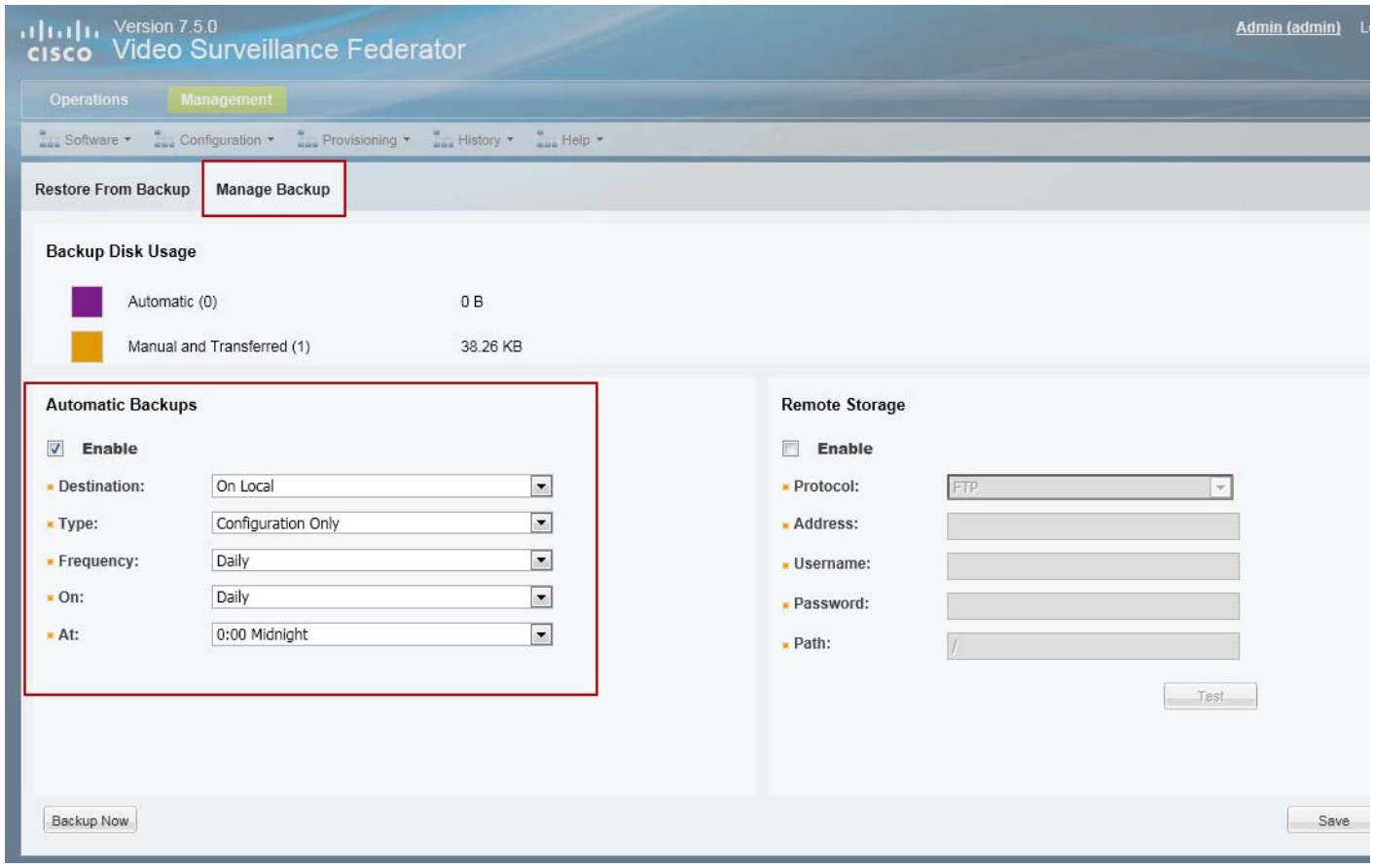
e. Click **Save**.

f. Backup files are saved to the selected destination. See the "Backup File Format" section on page 21-4 for a description of the file name.

   – If saved locally, the backup files are saved to the Backup File list in the Restore From Backup tab.

   – Failed backups are displayed in the Failed Backup field. Double-click a failed scheduled backup entry to display additional details (failed manual backups do not display additional information).

Figure 22-5 Automatic Backup



Step 11 Configure additional Federator users and add Operations Managers.

Continue to the Configuring Access to Operations Manager Resources, page 22-17

Logging In to a Federator Server

Logging in to a Federator server is similar to logging in to an Operations Manager. Enter the Federator server URL in a web browser and then enter a Federator username and password. See the "Logging In" section on page 1-18 for more information.

- The default credentials for a new or factory restored server is **admin/admin**.
- The username and initial password for all other users is defined when the user account is created (see the "Adding Users" section on page 4-15).
- All users are prompted to reset the password at first login.
- Users are required to select a domain if their credentials are authenticated using an external database, such as an LDAP server. See the "Adding Users from an LDAP Server" section on page 4-18.
- If Dual Login is enabled, a second user must also enter their credentials to approve the login (see the "Understanding Dual Login" section on page 1-20).

- Federator servers do not use Sites or Dynamic Proxies, and Federator users are not prompted to select a Site.

Note Federator user accounts are different than Operations Manager user account. You cannot use Operations Manager credentials to access the Federator. See the "Adding Federator Users" section on page 22-27 for instructions to create Federator users.

Login Procedure

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 Federator URL or IP address.

The syntax is: **https://***server-address***/vsf/**

Step 3 Enter your username and password.

- The default credentials for a new or factory restored server are **admin/admin**.
- The initial system includes an admin login for the super_user. You can create additional users with various access permissions, as described in the "Adding Federator Users" section on page 22-27.

g. Select a Domain, if necessary.

h. Enter a new password, if prompted.

i. If prompted, ask your manager or other administrator to enter their "Approver Login"

See the "Understanding Dual Login" section on page 1-20 for more information.

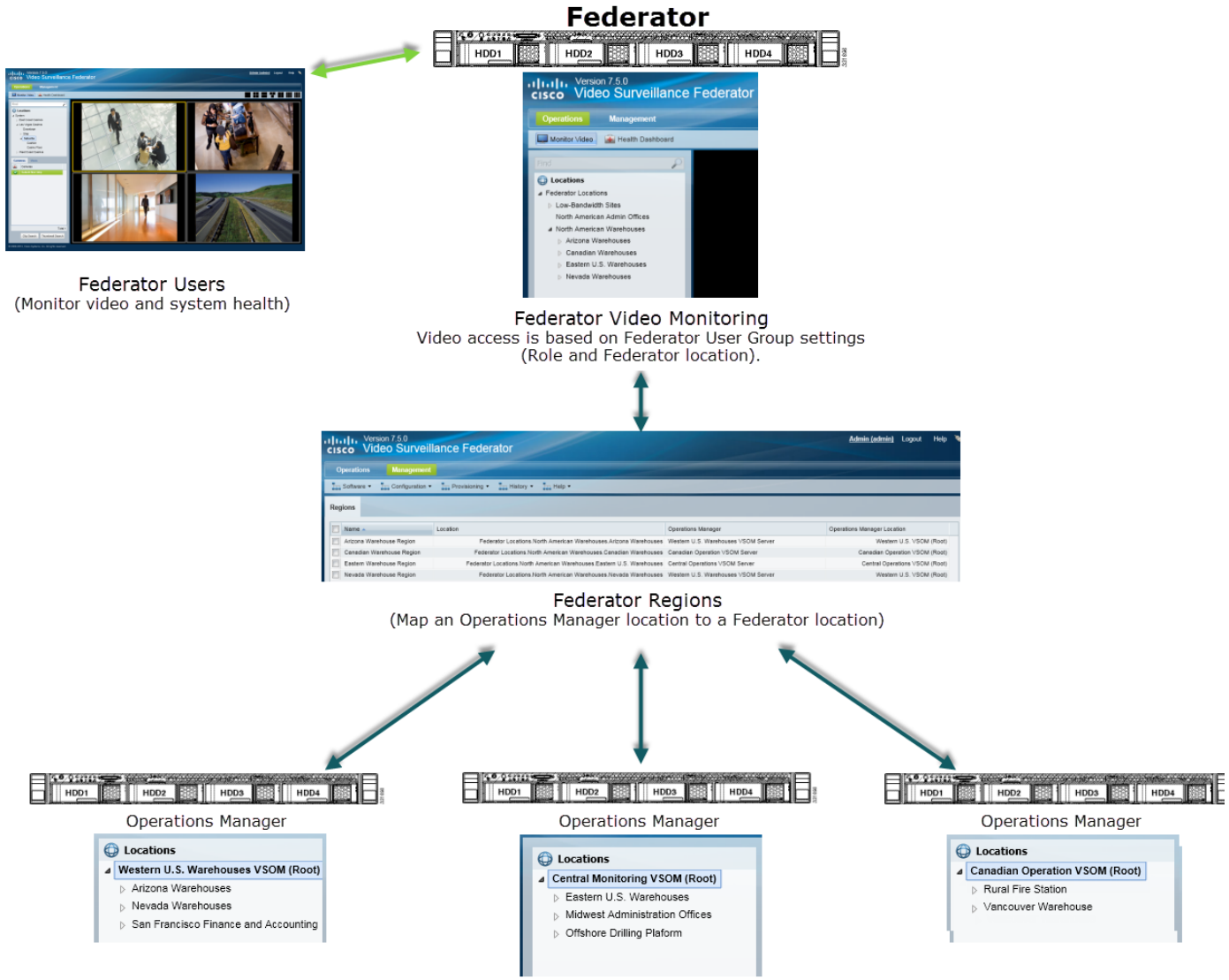
j. If prompted, complete the on-screen instructions to install or upgrade the Cisco Multi-Pane client software on your computer.

See the "Logging In and Managing Passwords" section on page 1-18 for more information.

Configuring Access to Operations Manager Resources

To provide access to the video and system health resources on multiple Operations Manager servers, add the Operations Manager servers to the Federator configuration, and then map the Operations Manager locations to the Federator locations (Figure 22-6). Federator users gain access to the resources based on the User Groups to which they are assigned (User Groups define the user Role and location for associated users).

Figure 22-6 Using Regions to Map Operations Manager Locations to Federator Locations



Note: All servers can be physical or virtual machines. Federator, Operations Manager, and Media Server are "services" that run on the server.

In Figure 22-6, three Operations Manager servers are added to the Federator, and the administrator adds Regions that map only the Operations Manager warehouse sub-locations to Federator sub-locations (under “North American Warehouse”). A Federator User Group is then created with Operator permissions to the “North American Warehouse” location, allowing users assigned to that User Group to monitor video from all North America warehouse cameras (but not financial or administrative offices).

Refer to the following topics for more information:

- Configuration Summary Steps, page 22-18
- Adding Operations Manager Servers to Federator, page 22-19
- Adding Federator Locations, page 22-23
- Adding Federator Regions, page 22-25
- Adding Federator Users, page 22-27

Configuration Summary Steps

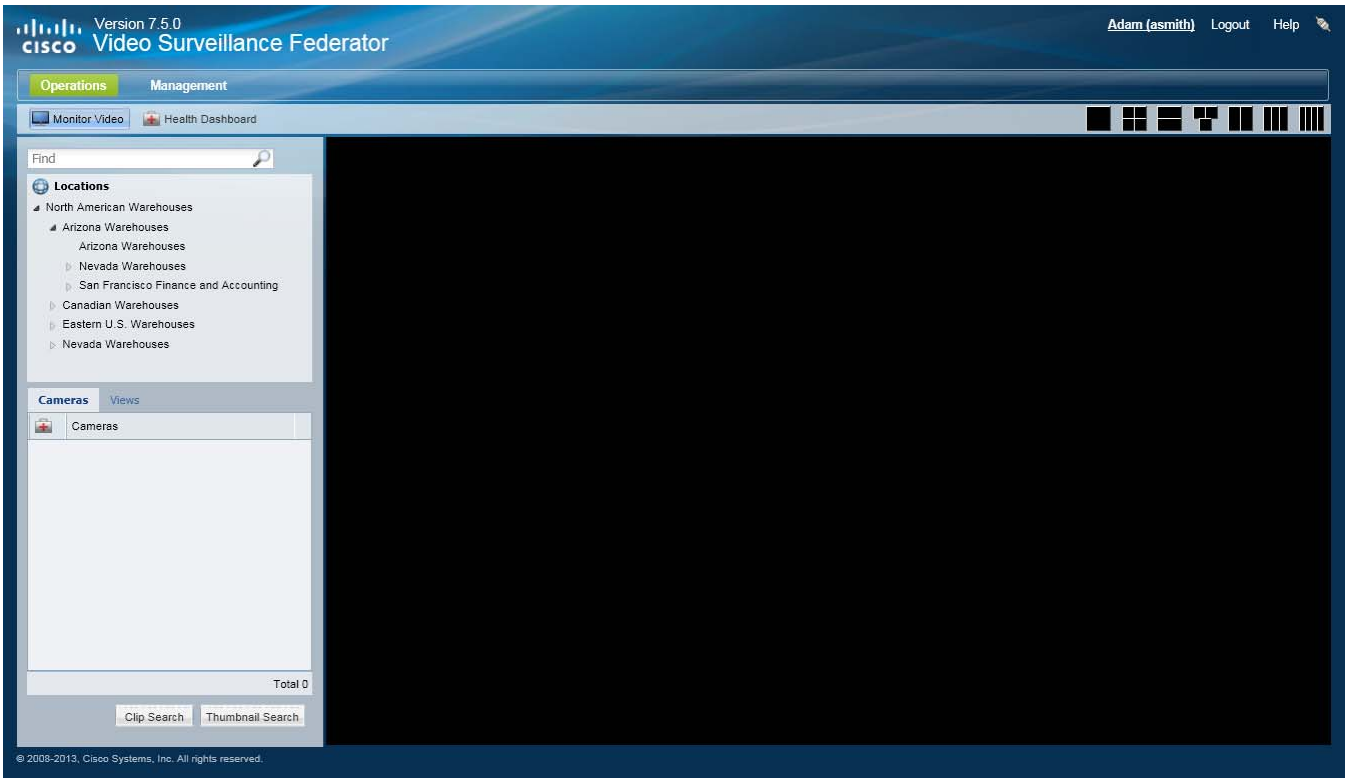
1. Add the Operations Manager servers to the Federator configuration.
2. Add locations in Federator that will include the shared resources, such as all warehouse facilities.

   For example, Figure 22-6 includes a location "North American Warehouses", and sub-locations for each Region (each Region is a mapping between a Federator location and an Operations Manager location).
3. Add Federator Regions that are associated with a Federator location and Operations Manager location.
   - For example, create a Region "Phoenix Warehouses". Associate that Region with the "Arizona Warehouse" locations in Operations Manager and Federator.
   - Select a sub-location on the Operations Manager to include only a portion of the server's resources. Select the root Operations Manager location to include all resources on the server, (such as the "Canadian Operations" server in Figure 22-6).
4. Add a Federator User Group that provides access to the location.

   For example, add a "Warehouse Operators" User Group with access to the "North American Warehouses" location.
5. Add Federator users and associate them with User Group.
6. The user can monitor the resources (such as video and system health) based on their User Group membership (Figure 22-7).

Note The Operations Manager locations are displayed under the Federator location.

Figure 22-7 Monitoring Video from Multiple Operations Manager s



Adding Operations Manager Servers to Federator

To add Operations Managers that can be accessed by Federator users, enter the network address and a username and password. The resources that are displayed in Federator depend on the access permissions granted by the server username and password. The Federator supports up to 500 Operations Managers.

Tip Servers are displayed in a flat list, and are not assigned to a location. This allows you to associate a sub-location on the server to a Region. That Region is also associated with a Federator location.

Operations Manager servers cannot be pre-provisioned when added to a Federator. If the Operations Manager is not accessible, the status is “unreachable”. Verify that the Operations Manager server(s) are reachable and online (see the “Requirements” section on page 22-4).

Refer to the following to add a single server or multiple servers from a CSV file:

- “Adding a Single Server” section on page 22-20
- “Importing Multiple Servers from a CSV File” section on page 22-21

Adding a Single Server

Procedure to Add a Single Server

Step 1 Complete the "Initial Server Setup" section on page 22-9 and log in to the Federator.

- You must belong to a User Group with permissions for *Manage All*. See the "Adding Federator Users" section on page 22-27 for more information.

Step 2 Select **Management > Servers**.

Step 3 Click **Add**.

Tip To edit a server, click an existing entry to highlight it

Step 4 (*Add* only) Complete the initial server setup (Figure 22-8):

Figure 22-8 Add a Server

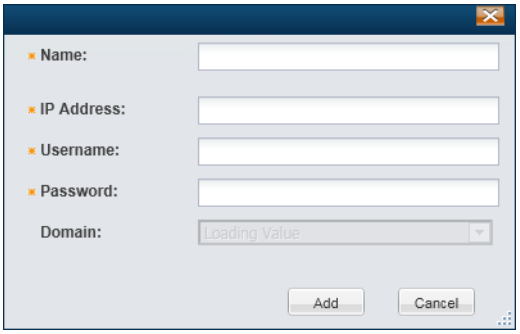


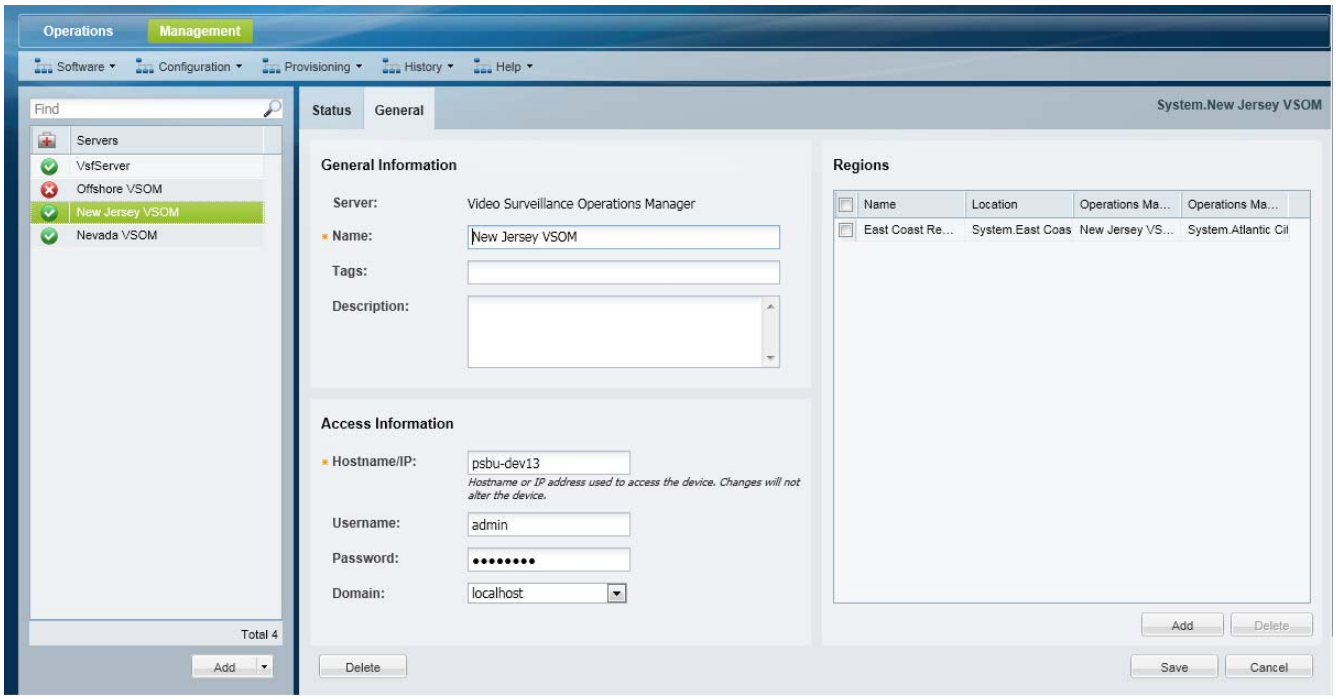
Table 22-3 Server Settings

Setting	Description
Name	A meaningful name for the Operations Manager. • This is used to identify the server when associating all or part of its resources with a Region. • For example, *Nevada Server* or *Warehouse B Server*.
Hostname/IP	The hostname or IP address of the Operations Manager server.
Username	The username used to establish communication with the Operations Manager. The access permissions for the user account define the resources available in Federator. **Note** A username and password from an external database (such as LDAP) can also be used. See the "Adding Users from an LDAP Server" section on page 4-18 to configure LDAP on the Operations Manager.
Password	The server password. **Tip** The server password is defined using the Operations Manager interface. See the "Adding Users, User Groups, and Permissions" section on page 4-1 for more information.

k. Click **Add**.

- If the validation is successful, the server appears in the server configuration page in the OK state (Figure 22-9).
- If the server cannot be found on the network, or the username/address is incorrect, the server is added in the critical state. Correct the server hostname and login credentials and click **Save**. The Federator will update the settings and attempt to establish communication.

Figure 22-9 Server Configuration Page



Note Operations Manager servers cannot be pre-provisioned when added to a Federator. If the Operations Manager is not accessible, the status is "unreachable".

Step 5 (Optional) In the Server configuration page (Figure 22-9), add a Region and associate an Operations Manager location to that region.

See the "Adding Federator Regions" section on page 22-25 for more information.

Importing Multiple Servers from a CSV File

Multiple servers can be imported using the same method used to import servers in the Operations Manager. The main differences are:

- Only the Name, Hostname or IP address, Username, and Password are required. A domain and tags are optional.
- The servers cannot be pre-provisioned. Servers with incorrect address or username/password will be added in a critical state. Correct the Access Information and wait for communication to be established.

Note Operations Manager servers cannot be pre-provisioned when added to a Federator. If the Operations Manager is not accessible, the status is "unreachable".

Procedure to Import Servers

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

Step 1 Create a file in plain text CSV format that can be opened and saved using Excel or OpenOffice Calc. Blank rows or rows beginning with "//" are ignored.

- Only the Name, Hostname or IP address, Username, and Password are required.
- See the "Creating the CSV File" section on page 6-21.

Tip To download a sample import file, launch the import wizard as described in the *Import Step 1 - Download Sample*. Click the **Download Sample** button in the second step of the wizard to obtain a sample file (see Step 4). See the "Creating the CSV File" section on page 6-21 for more information.

Step 2 Select **System Settings** > **Servers**.

Step 3 Choose **Add** and **Import servers from file**.

Step 4 Complete each *Import Step* as described below:

Tip See the "Creating the CSV File" section on page 6-21 for more information.

a. *Import Step 1 - Download Sample*
(Optional) Click **Download Sample** to download a sample CSV import file. Use this sample to create the import file (see the "Creating the CSV File" section on page 6-21). Click Next.

b. *Import Step 2 - File Upload*:
Click to select the CSV file from a local or network disk. Click **Upload**.

c. *Import Step 3 - Processing*:
Wait for the import process to complete.

d. *Import Step 4 - Results* **Success**:
   - If a *success* message appears, continue to Step 5.
   - If an *error* message appears, continue to Step 4 e.

e. If an *error* message appears, complete the following troubleshooting steps:
   - Revise the file to correct any errors.
   - Click **Start Over**.
   - Return to Step 3 and re-import the corrected CSV file.

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

Step 6 View the device status to determine if additional configuration is required.

Step 7 Continue to the "Adding Federator Locations" section on page 22-23.

Adding Federator Locations

Federator locations allow you to organize the Operations Manager resources (such as video streams) according to the real-world location of the server, or by the type of video available on the server (such as cameras in warehouses). User Groups are also associated with locations define user access permissions.

For example, a "Warehouse Operator" User Group can be associated to a location that includes sub-locations for warehouse video streams. Another "Finance Operator" User Group can be associated to the accounting locations.

Federator locations are mapped to Operations Manager locations using "Regions". See the "Configuring Access to Operations Manager Resources" section on page 22-17 for more information.

Tip Federator locations are similar to locations in an Operations Manager. See the "Creating the Location Hierarchy" section on page 5-1.

Procedure to Add Federator Locations

To create the Federator locations, do the following:

Step 1 Log in to the Federator browser-based interface.

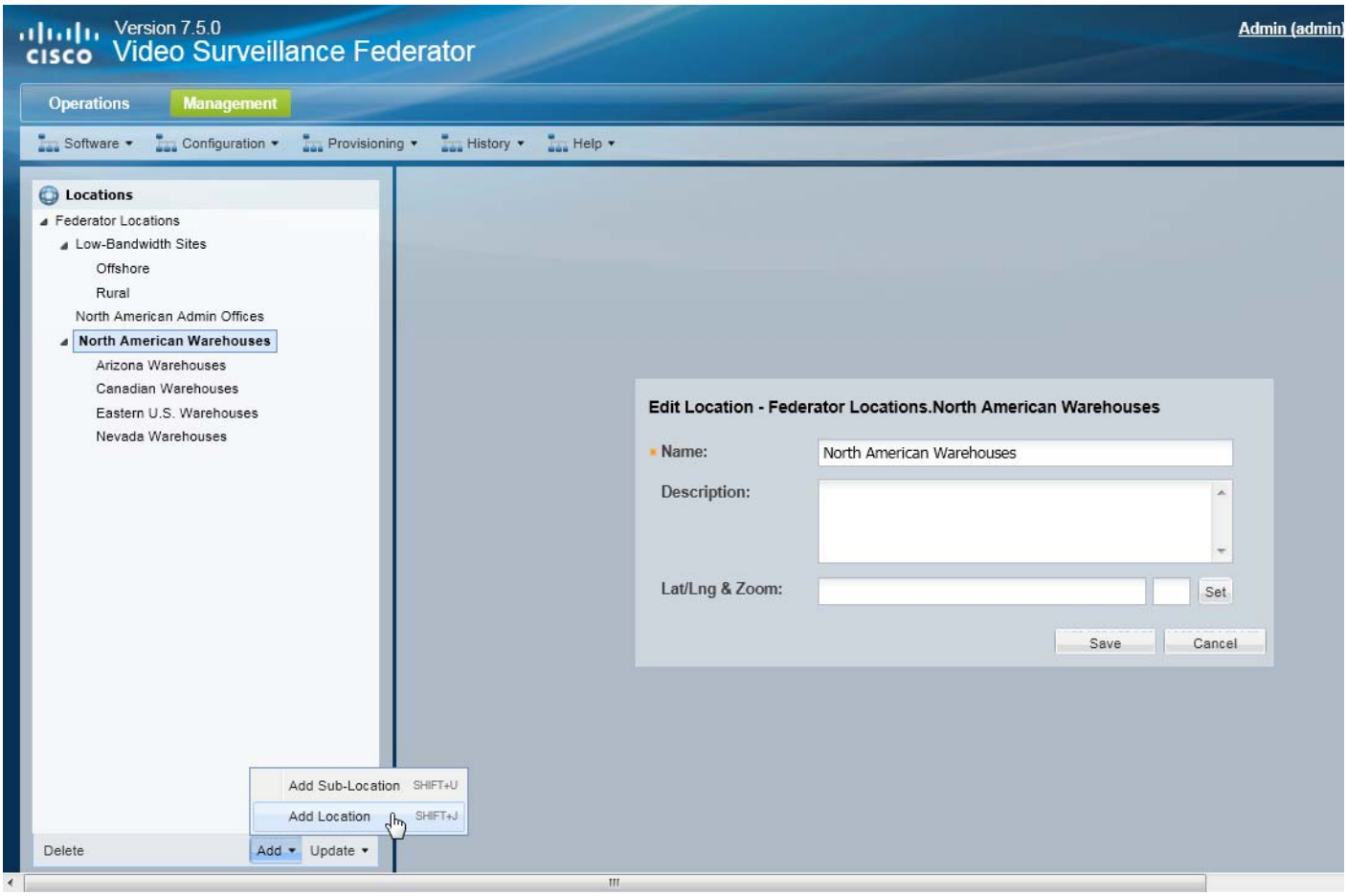
- You must belong to a User Group with permissions for *Manage All*.
- See the Logging In and Managing Passwords, page 1-18 and the "Adding Federator Users" section on page 22-27 for more information.

Step 2 Select **Management > Locations**.

Step 3 Select an existing location and click **Add** to add a new location or sub-location (Figure 22-10).

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

Figure 22-10 Locations Menu



Add menu (Figure 22-10):

- 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**.

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

Tip

- Use the keyboard shortcuts (shown in parentheses) to quickly add or edit location entries.
- You can also drag and drop location names within the location hierarchy.

- 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 5 Continue to the "Adding Federator Regions" section on page 22-25.

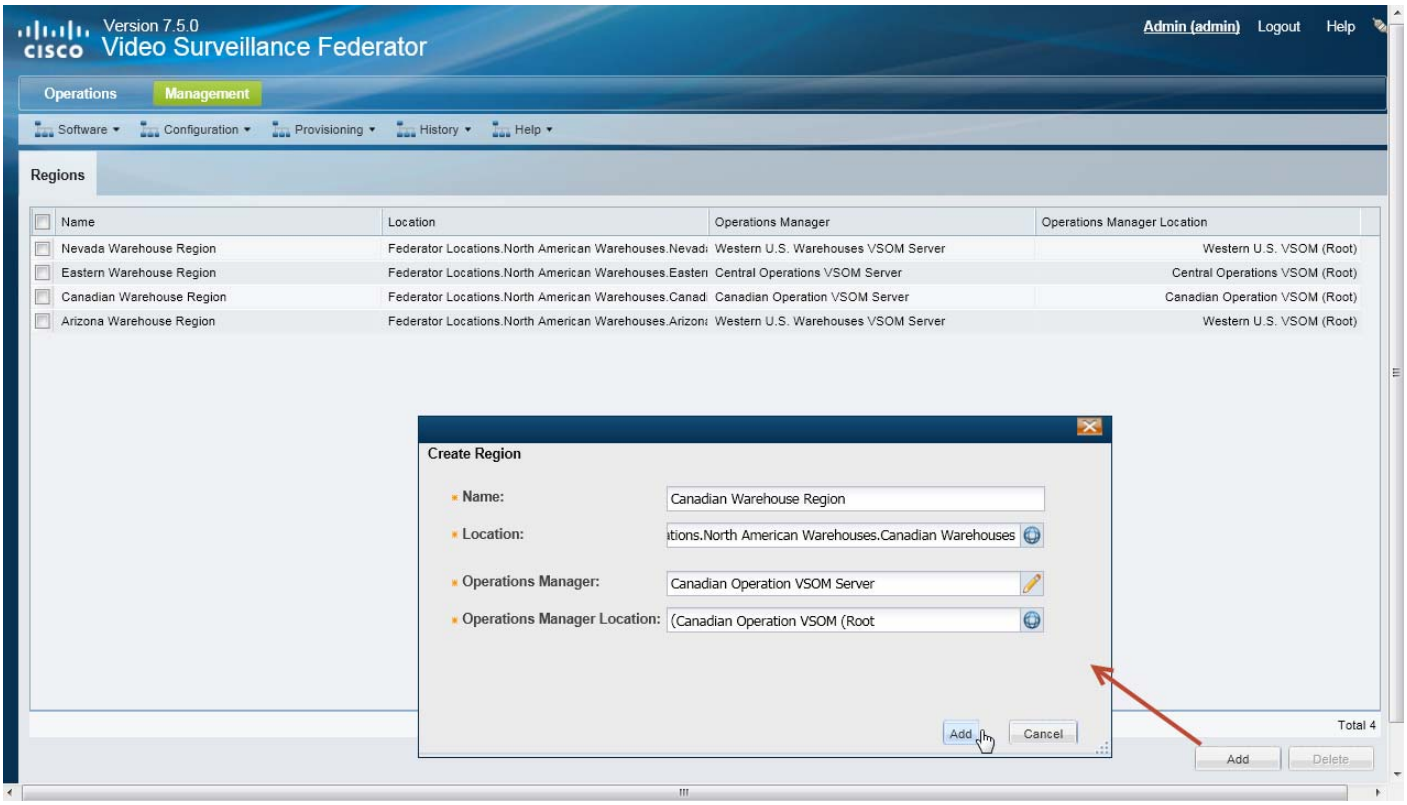
Adding Federator Regions

Regions map a Federator location to an Operations Manager location (Figure 22-11). This allows you to include all or part of the resources available on the Operations Manager, and organize those resources in Federator to provide the access permissions required by different Federator users.

Regions that map only the Operations Manager warehouse sub-locations to Federator sub-locations (under "North American Warehouse". A Federator User Group is then created with Operator permissions to "North American Warehouse", allowing users assigned to that User Group to monitor video from all North America warehouse cameras (but not financial or administrative offices).

Note Different non-overlapping locations from the same Operations Manager can be mapped as different Federator Regions. Federator supports up to 2000 regions.

Figure 22-11 Locations Menu



Procedure to Add Regions

Step 1 Log in to the Federator browser-based interface.

- You must belong to a User Group with permissions for *Manage All*.
- See the Logging In and Managing Passwords, page 1-18 and the "Adding Federator Users" section on page 22-27 for more information.

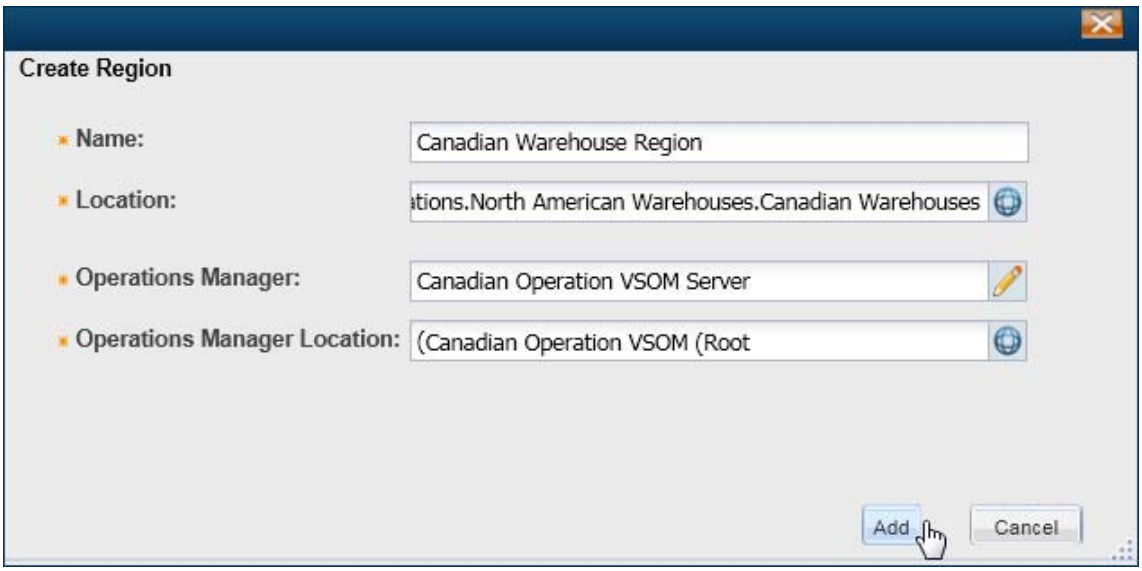
Step 2 Select **Management > Regions** (Figure 22-11).

Step 3 Click **Add**.

Step 4 Enter the following settings (Figure 22-12):

- Name—Enter a meaningful name (used to identify the Region).
- Location—Select the Federator location where the Operations Manager resources will appear.
- Operations Manager—Select the server that hosts the Operations Manager service. The server must be added to the Federator configuration, as described in the "Adding Operations Manager Servers to Federator" section on page 22-19.
- Operations Manager Location—Select the location for the Operations Manager resources that will be mapped to the Federator location. Select the server root location to include all resources available on the server. Select a sub-location to include a sub-set of resources.

Figure 22-12 Region Settings



Note

- Each Region is mapped to a single Operations Manager location.
- Only a single Region can be mapped to each Federator location.

Step 5 Click **Add**.

Step 6 Continue to the "Adding Federator Users" section on page 22-27.

Adding Federator Users

A Federator user account is required to log in to Federator and access the resources from multiple Operations Managers.

Note

- Federator user accounts are different than Operations Manager user account. You cannot use Operations Manager credentials to access the Federator.
- Creating users is similar to the method to configure Operations Manager users. See the "Adding Users, User Groups, and Permissions" section on page 4-1 for more information.
- The permissions available in Federator Roles are different than those available in Operations Manager. See the "Understanding Federator Access Permissions" section on page 22-28.

Federator users can monitor video and system health 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), and the Region(s) associated with that location (and its sub-locations).
- Users can be assigned to multiple user groups, and gain the combined access permissions for all groups.

Before You Begin

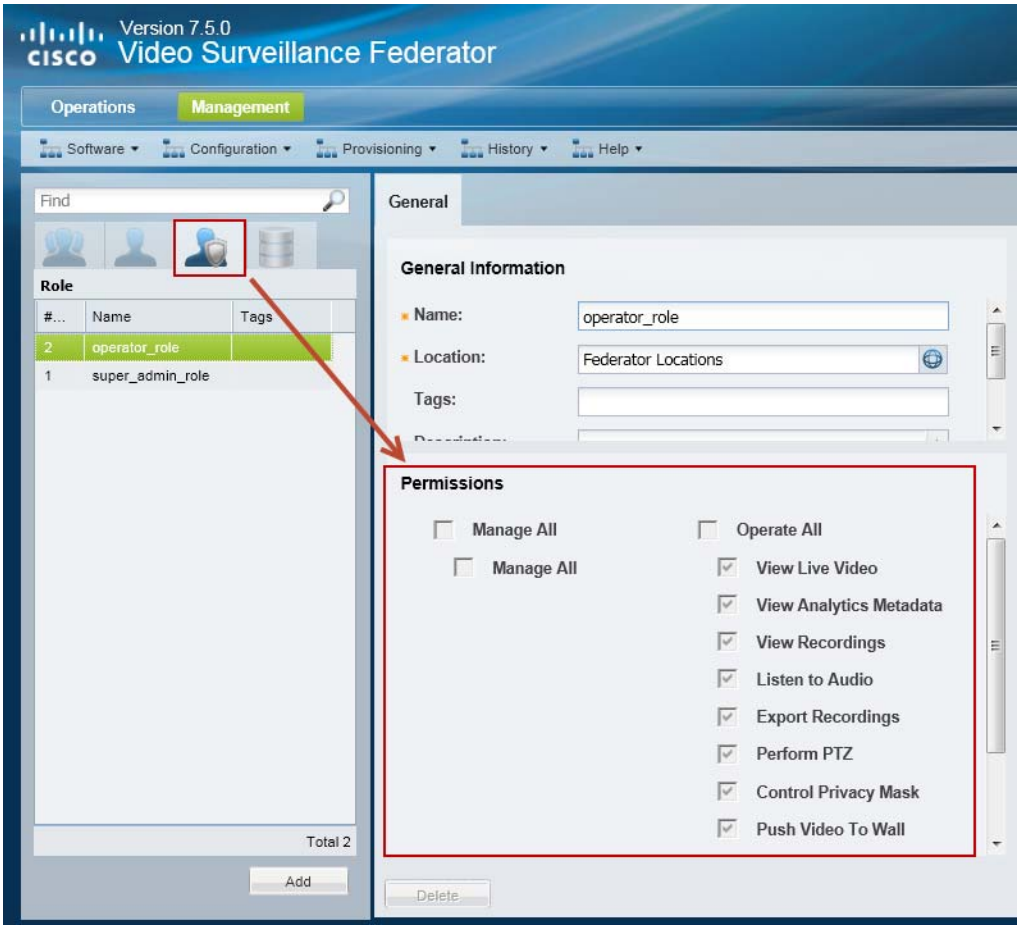
Before you begin:

1. Create the Federator location hierarchy and Regions as described in the following:
   - Adding Federator Locations, page 22-23
   - Adding Federator Regions, page 22-25.
2. See also the overview information in the following:
   - Overview, page 22-3
   - Configuring Access to Operations Manager Resources, page 22-17
3. Review the overview information and instructions to create Operations Manager users. Although the Roles are different, the general rules and configuration is the same.
   - Adding Users, User Groups, and Permissions, page 4-1

Understanding Federator Access Permissions

The Access Permissions available in Federator are a sub-set of those available in the Operations Manager (Figure 22-12). See the "Understanding Permissions" section on page 4-4 for descriptions of the available Manage and Operate permissions.

Figure 22-13 Federator Access Permissions



Procedure to Add Users

The following procedure summarizes the process to add Federator user accounts and access permissions. Configure these accounts to grant or restrict the locations and tasks available to a user. For additional information, see the "Adding Users, User Groups, and Permissions" section on page 4-1.

Tip You can also provide access to users that are managed on an external (LDAP) server. See the "Adding Users from an LDAP Server" section on page 4-18 for more information.

Step 1 Create a user *Role*.

The Role defines the access permissions for different types of users. Roles are assigned to User Groups.

a. Select **Users**.

b. Select the **Roles** tab .

c. Click **Add**.

d. Enter the basic settings (see Table 4-5 on page 4-10).

e. Select the Role permissions (see Table 4-2 on page 4-5 and Table 4-3 on page 4-6).

Note The Federator permissions are different than the Operations Manager permissions.

f. Click **Create**.

Tip See the "Defining User Roles" section on page 4-9 for more information.

Step 2 Create a *User Group*.

User Groups allow you to create groups of users. The Role assigned to the User Group grants those access permissions to all users in the group.

a. Select the **User Groups** tab .

b. Click **Add**.

c. Enter the group settings, including the Role that defines the access permissions for the group (see Table 4-6 on page 4-12).

Tip Select the **Approval Required** checkbox (and "Approval Usergroup") to enable Dual Login. All users assigned to the User Group can only gain access if a member of the "Approval Usergroup" also enters their password.

d. Click **Create**.

Tip See the "Adding User Groups" section on page 4-11.

Step 3 Create a User Account

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.

a. Select the **User** tab .

b. Click **Add**.

c. Enter the basic user settings (see Table 4-7 on page 4-16).

d. Add the user to one or more user groups.

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

e. Click **Create**.

Tip See the "Adding Users" section on page 4-15. See also the "Adding Users, User Groups, and Permissions" section on page 4-1 for more information.

Step 4 Continue to the "Monitoring Video Using Federator" section on page 22-30 and the "Monitoring Device Health Using the Browser-Based Federator" section on page 22-34.

Monitoring Video Using Federator

Federator users can access video streams from the Operations Manager locations included in their access permissions. Access permissions are a combination of the following:

- The access permissions included in the Federator User Groups to which they belong. For example, **View Live Video** or **View Recordings**.
- The Federator location associated with the Federator User Groups to which they belong. For example, User Groups with access to the root location can access all Operations Managers configured on the Federator. User Groups with access to a sub-location, can view the video streams for Operations Managers at that location and lower.
- The Operations Manager locations that are mapped to the Federator locations (using "Regions".) Regions can map to all Operations Manager locations (root) or a sub-location.

Usage Notes

- Federator users can view video from different Operations Managers in a single layout by dragging and dropping cameras in the video display grid.
- Federator users can load the Views defined in the Operations Managers.
- The Operations Manager default layouts are available in Federator.
- You can view, but not create, video clips in this release. Use the Cisco Video Surveillance Safety and Security Desktop application to create clips using Federator.
- To use the camera search, you must first select a location. Camera search is not supported across multiple Operations Managers.

Supported Monitoring Applications

Federator resources can be monitored using the following applications:

- The browser-based monitoring tool (described in this document).
- The Cisco Video Surveillance Safety and Security Desktop (Cisco SASD) desktop application.

  See the Cisco Video Surveillance Safety and Security Desktop User Guide for more information.
- The Cisco Review Player desktop application.

  See the Cisco Video Surveillance Review Player User Guide for more information.

Procedure

Step 1 Log in to the Federator browser-based interface.

Step 2 Select **Operations > Monitor Default** (Figure 22-14).

This is the default page after log in.

Step 3 Select a location from the location tree.

Locations display the cameras for the associated Operations Manager locations (based on the Federator Regions).

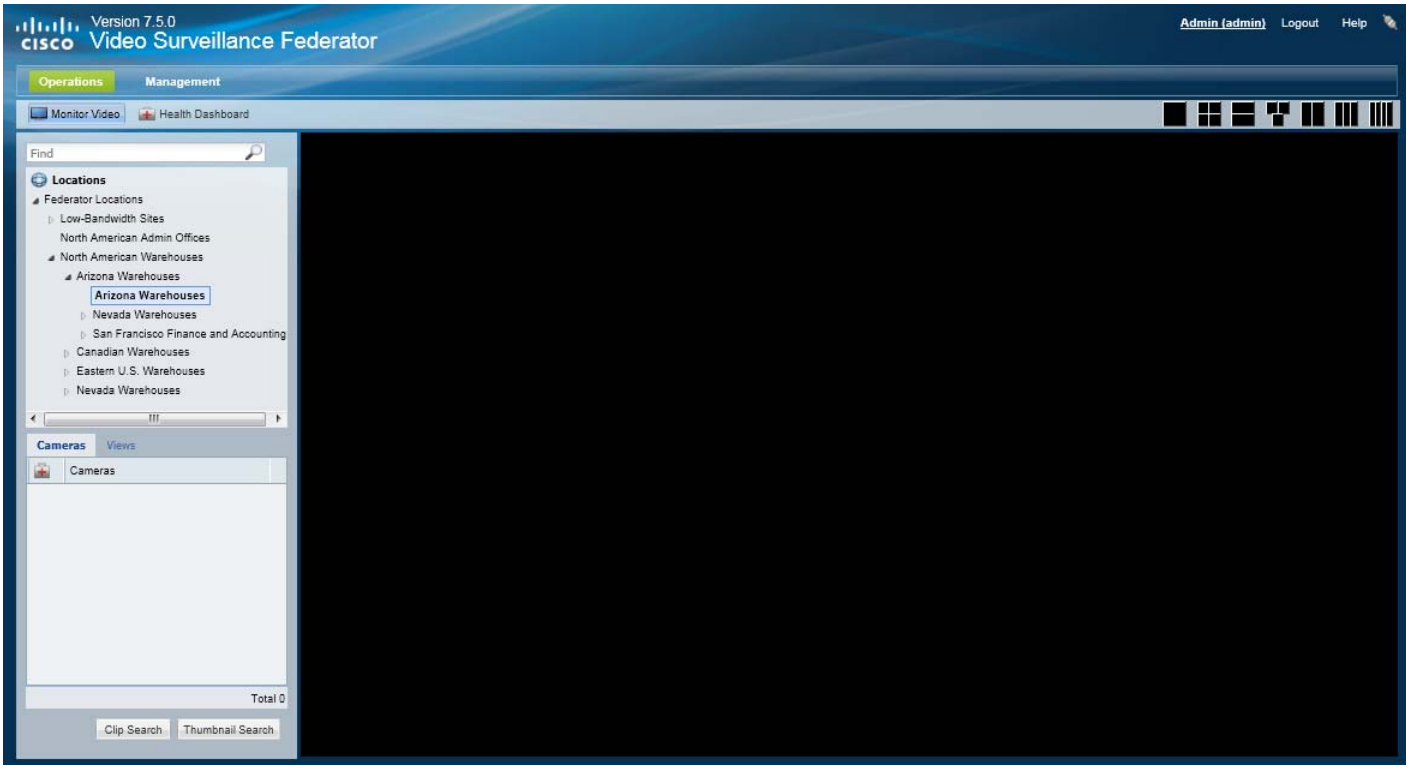
Step 4 (Optional) Use the Find field to search for a camera name (such as **Lobby Camera**).

To search for cameras, you must first select a location.

Step 5 (Optional) Select a layout (such as **2x2**).

Step 6 Drag-and-drop cameras onto the available video panes to display video from the camera.

Figure 22-14 Monitoring Video in Federator



Step 7 (Optional) Select a View that was configured on the Operations Manager.

See the "Selecting a Multi-Pane "View"" section on page 2-4.

Step 8 (Optional) Click **Clip Search** to view, download, delete and manage MP4 clips saved on the server.

See the "Federator Clip Search" section on page 22-32.

Note Clips can not be deleted using Federator. Clips cannot be created using the browser-based Federator interface in this release. Use the Cisco Video Surveillance Safety and Security Desktop application to create clips.

Step 9 (Optional) Click **Thumbnail Search** to quickly locate specific scenes or events in recorded video.

See the "Viewing a Thumbnail Summary of Video Archives" section on page 2-44.

Federator Clip Search

Select **Clip Search** from the **Monitor Video** window (Figure 22-15) to view, download and delete MP4 and virtual clips.

Tip You can also create and download clips by right-clicking a video pane. See the "Downloading and Viewing Clips" section on page 2-23.

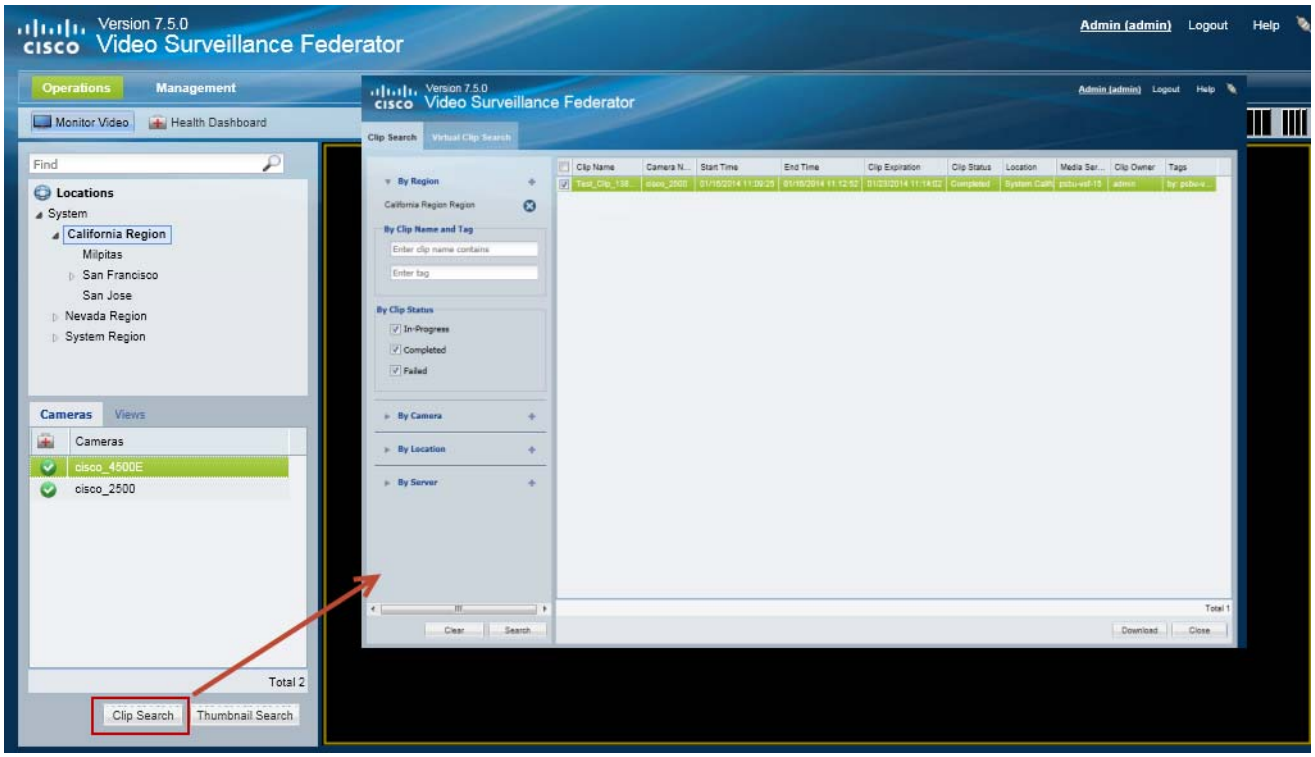
Procedure

Step 1 From the **Monitor Video** page, click **Clip Search** to open the Clip Search window (Figure 22-15).

Step 2 Select the clip type:

- **Clip Search** tab—MP4 clips
- **Virtual Clip Search** tab—Virtual clips

Figure 22-15 Federator Clip Search Window



Step 3 Select a region where the clip(s) were created. Only clips from the Operations Manager location mapped to that region will be displayed.

Step 4 (Optional) Use the filters to search for specific clips (Table 22-4):

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

Table 22-4 Filters For Searching Federator Clips

Field	Description
By Clip Name	The full or partial name for the clip(s), which is entered when the clip is created
By Tag	Not available in Release 7.2.
By Clip Status	Select the status for the displayed clips. Any status not selected will not be displayed.
By Camera	The camera name where the clip originated.
By Location	Clips created by all cameras at the selected location(s).
By Server	Clips created by all cameras associated with the selected servers(s).

Step 5 Click **Search**.

Step 6 Review information about the clips.

Table 22-5 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 7 (Optional) To download an MP4 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 8 (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.

Monitoring Device Health Using the Browser-Based Federator

Federator Health Dashboard

Overview

Use the browser-based Federator Health Dashboard (**Operations > Health Dashboard**) to view a summary of device health issues that are occurring on the servers, encoders and cameras of all Operations Managers managed by the Federator.

The browser-based Federator displays two types of alerts:

- Federator device health alerts—health alerts generated by the Federator server.
- Operations Manager health alerts—alerts gathered from the Operations Managers monitored by the Federator.

Note The browser-based Federator Health Dashboard displays device health events only. To view security events (such as motion or contact events), use the Cisco SASD Federator. See the Cisco Video Surveillance Safety and Security Desktop User Guide for more information. For example, you can use Advanced events to automatically send motion events to the Cisco SASD Federator, or manually send specific alerts from an Operations Manager to the Federator.

The Federator Health Dashboard is similar to the Health Dashboard for an Operations Manager: it displays the critical and warning faults on devices, such as servers, cameras and encoders (Figure 22-16).

The Federator Health Dashboard differs from the Operations Manager dashboard in the following ways:

- Federator health information is not updated in real-time. Device health is periodically gathered (every 30 minutes) from the Operations Managers by the Federator and cannot be updated by refreshing the page.
- Locations cannot be selected in the Federator Health Dashboard. Health issues counts (not the actual issues) are displayed for the locations that the user can view. For example, if a user is assigned to a Federator user group with the California location, then the user would see only the issue counts from California and its sub-locations. If a higher-level location (such as "System") had 10 issues, that issue count would not be displayed for California users. The Federator locations include only the Operations Manager resources mapped to the Federator regions.
- Issues do not include the icon to open the device's configuration page. You must log in to the Operations Manager for the device to access the device status and configuration pages.
- Issues are displayed by category only (and not by issue type).

Viewing Device Health Using the Federator

To view health issues, select **Operations** > **Health Dashboard** and click a number next to a category for a servers, cameras or encoders (Figure 22-16). The issues list displays more information about the source if the health issue, allowing you to log in to the correct Operations Manager and access the device's status and configuration page for more information or to correct the problem.

Tip For more information about the Operations Manager Health Dashboard, see the "Health Dashboard: Device Health Faults on an Operations Manager" section on page 19-6.

Figure 22-16 Federator Health Dashboard

1	Click **Health Dashboard** to view the critical and warning faults for all devices in all Operations Managers managed by the Federator: • Issues are displayed by category only. • The number represents the total number of issues for all devices at allOperations Managers, based on the selected category (such as Configuration, Reachability, Hardware and Software). **Tip** See Table 22-6 for more information about critical and warning faults.
2	Select a number next to the device type (Servers, Encoders or Cameras) to view all issues for that device type.
3	Select a number next to a category to display the issues for all devices that are experiencing that category of issue. For example, click the number next to the server Configuration category to view the device configuration issues. • If issues did not occur, a number is not displayed. • The number represents the total number of issues for all devices at all locations in all Operations Manager, based on the category.
4	Last Update—The date and time when the health information was automatically updated from all Operations Managers. • Federator health information is automatically updated every 30 minutes and cannot be refreshed manually. This prevents excessive polling on the Operations Managers that could degrade system performance. • For real-time health information, log in to the Operations Manager's Health Dashboard. See the "Health Dashboard: Device Health Faults on an Operations Manager" section on page 19-6 for more information.
5	The specific health issues that occurred for the selected category or device type. • All issues are listed. Multiple issues can be displayed for the same device

Tip

- Device errors are cleared automatically by the system or manually cleared by an operator using the Cisco SASD or another monitoring application. Cleared errors are removed when the Federator health information is automatically updated.
- Some alerts cannot be automatically reset. For example, a server I/O write error event.

Understanding Warning and Critical Faults

Table 22-6 Warning and Critical Faults

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	Critical errors are health events that impact the device operation or render a component unusable. For example, a server or camera 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.

Procedure

Complete the following procedure to access the Health Dashboard and view device health issues:

Step 1 Click **Operations > Health Dashboard** (Figure 22-16).

Step 2 Click a number to display the specific issues for the device type or category.

- The number represents the total number of issues for all devices in all Operations Managers managed by the Federator.
- There is no "Issue Type" option in the Federator Health Dashboard.

Step 3 Continue to the "Device Status: Identifying Issues for a Specific Device" section on page 19-9 for more information.

Step 4 Take corrective action to restore the device to normal operation, if necessary.

Step 5 For example, if a configuration mismatch occurs, see the "Synchronizing Device Configurations" section on page 19-21.

Federator Audit Logs

This Federator audit logs displays the configuration changes performed by Federator users.

Tip The Federator audit logs are similar to the Operations Manager logs. See the "Viewing Audit Logs" section on page 19-35.

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.

Procedure

Step 1 Select **Management** > **Audit Logs**.

Step 2 (Optional) Search for Audit entries using the "Search By" fields.

Step 3 (Optional) Click the Column headings to sort the results by that category.

Step 4 (Optional) Click Job Reference to display additional job details about the action performed by the user.

Step 5 Refer to the "Viewing Audit Logs" section on page 19-35 for additional features and instructions.

Administration Tasks

Refer to the following topics to perform common administrative tasks on the Federator server.

- "Backing up and Restoring the Federator Configuration" section on page 22-39
- "Updating the Federator Server System Software" section on page 22-42

Backing up and Restoring the Federator Configuration

Back up the Federator configuration so the system can be restored if it becomes unstable or to revert to an older configuration.

- Manually Backing Up a Federator Server, page 22-39
- Automatic Backups (Single Federator Server), page 22-40

Note We recommend backing up all servers on a regular basis to ensure configuration and event data is not lost if a hardware failure occurs. Backups are also used to restore configurations and historical data when upgrading or moving to a new system.

You can backup a single Federator server at a time. The following instructions are to perform a manual one-time backup. To configure an automatic backup schedule, see the "Initial Server Setup" section on page 22-9.

Tip The Federator backup procedure is similar to the Operations Manager procedure. See the "Backing Up and Restoring a Single Server" section on page 21-8 for more information.

Manually Backing Up a Federator Server

To perform a one-time manual backup, do the following.

Procedure

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

Step 2 Select the **Manage Backup** tab (Figure 22-17).

Step 3 Click **Backup Now** and select **To Remote** or **To Local**.

Step 4 From the pop-up, select the destination and backup type.

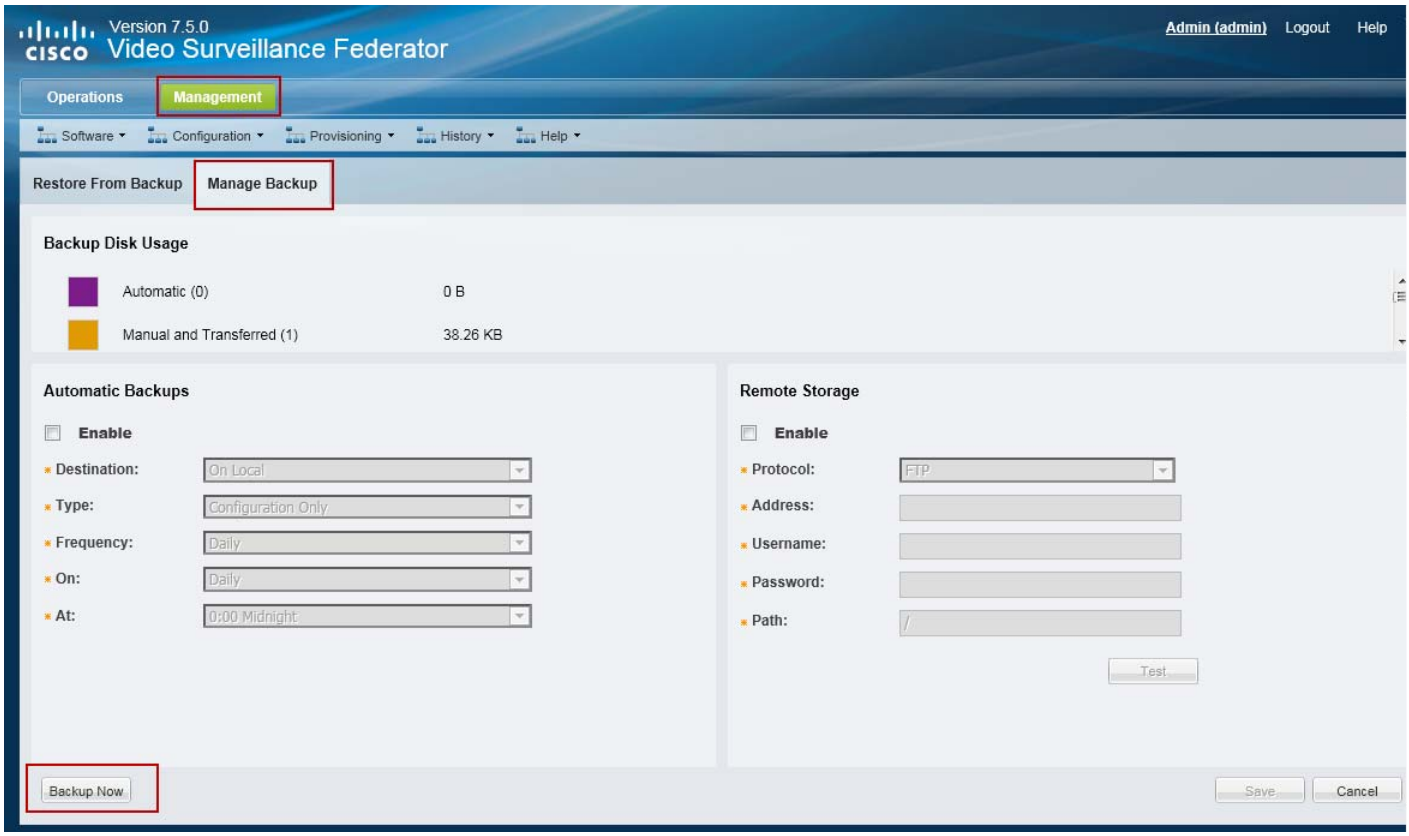
See the "Backup Settings" section on page 21-3 for more information).

Step 5 Click **OK**.

Step 6 Backup files are saved to the selected destination. See the "Backup File Format" section on page 21-4 for a description of the file name.

- If saved locally, the backup files are saved to the Backup File list in the Restore From Backup tab.
- Failed backups are displayed in the Failed Backup field. Double-click a failed scheduled backup entry to display additional details (failed manual backups do not display additional information).

Figure 22-17 Backup Now



Automatic Backups (Single Federator Server)

To schedule recurring backups for a single Federator server, see Step 10 of the "Initial Server Setup".

Restoring a Backup for a Federator Server

Federator is a service that runs on a physical or virtual Cisco VSM server. Table 22-7 describes the format for the Federator service backup files:

Table 22-7 Backup File Formats

Backup Data	File Name Format
Config and Historical	**VSF**_*HostName*_**backup**_*yyyyMMdd_HHmmss*.**tar.gz**
Config Only	**VSF**_*HostName*_**backup_config**_*yyyyMMdd_HHmmss*.**tar.gz**

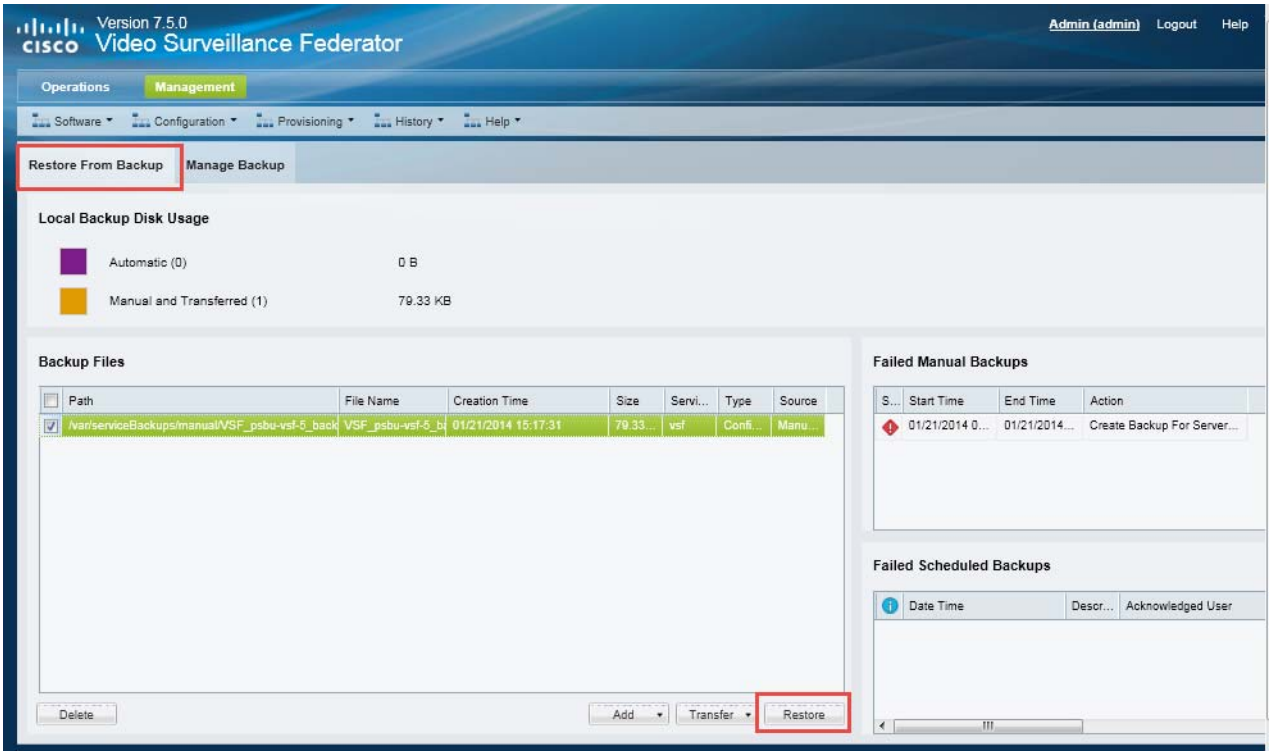
- **VSF**—The acronym that denotes the Federator service.
- *HostName*—the host name of the Cisco VSM server running the Federator service.
- *yyyyMMdd_HHmmss*—the date and time when the backup file was created.

For example, if the *psbu-docs1* server was backed up on October 29, the resulting filename would be: `VSF_psbu-docs1_backup_20131029_105018.tar.gz`

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

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

Figure 22-18 Restore Backups



Procedure

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

Step 1 Select **Management > Backup & Restore** (Figure 22-18).

Step 2 Select the **Restore From Backup** tab (default).

Step 3 (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 **Add > From Remote** or **From PC**.

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

Note You must first enter the Remote Storage settings in the Manage Backup tab before you can transfer a file from a remote server. See the "Backup Settings" section on page 21-3 for more information.

c. Click **Save**.

Step 4 Select the backup file for the service you want to restore.

Step 5 Click **Restore**.

Step 6 Click **Yes** to confirm the backup and server restart.

Step 7 Click **OK** when the restore process is complete.

Step 8 Re-login to the server.

Updating the Federator Server System Software

System Software is the Cisco VSM server software that includes the Federator service, Federator browser-based interface, and Management Console.

To update a Federator server, log in to the Federator server Management Console and use the **Server Upgrade** feature.

- Go to **Operations** > **Management Console** to launch the Management Console.
- See the Cisco Video Surveillance Management Console Administration Guide for more information. See your system administrator for login information.

Using Dynamic Proxy to Monitor Video From Remote Sites

Dynamic Proxy allows users to access video streams from remote Sites that have limited outbound bandwidth. The video can be delivered to multiple users without placing additional load on the remote Site.

Refer to the following topics for more information:

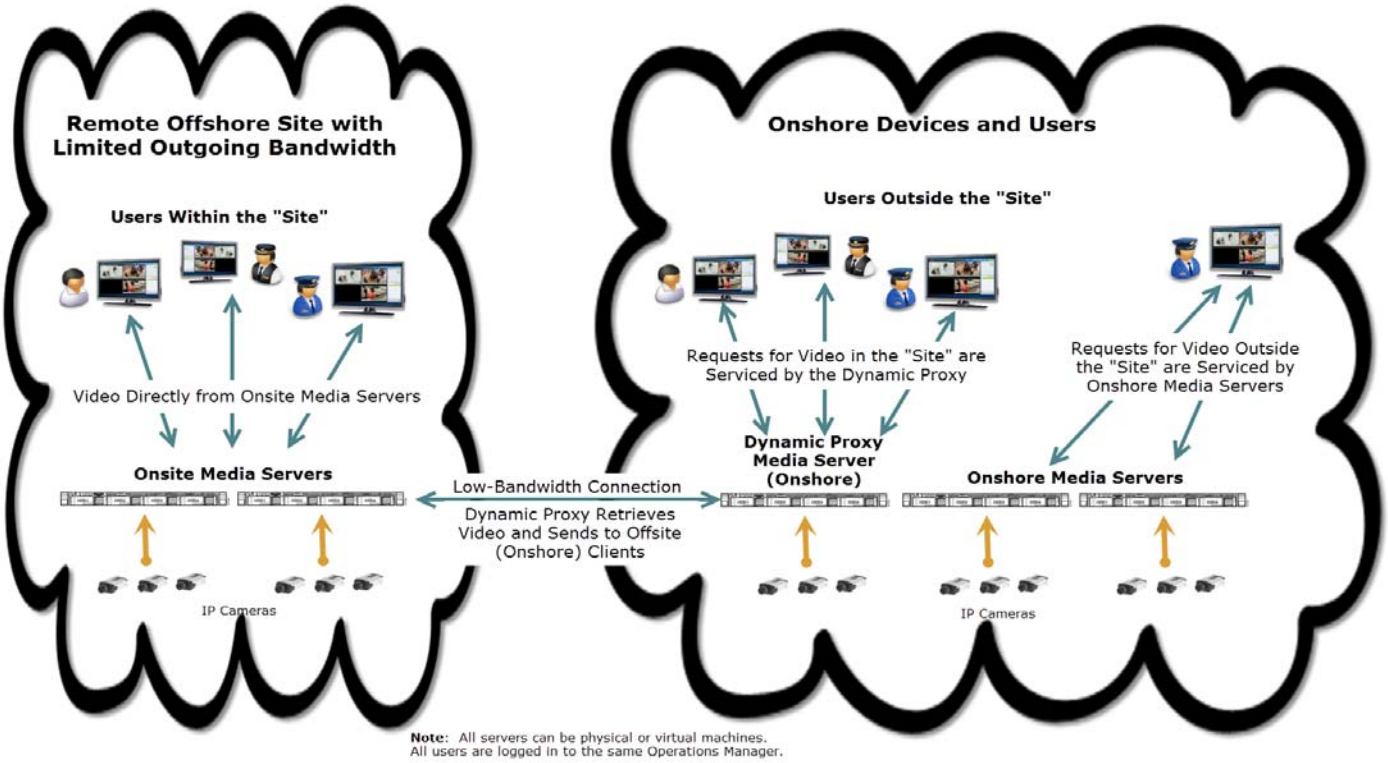
Contents

Dynamic Proxy Overview

When cameras and their associated Media Servers are located in Site with limited outgoing connectivity (such as an offshore oil platform), the Dynamic Proxy (DP) feature can be used to reduce the amount video data going out from that remote Site (Figure 23-1).

The Dynamic Proxy (DP) feature provides this service by retrieving video from the remote Media Servers and delivering it to the end users. The DP minimizes the amount of bandwidth used to deliver video data from the remote Site while allowing multiple users to access that video data.

Figure 23-1 Dynamic Proxy Example



For example, in Figure 23-1, an offshore oil platform has a set of IP cameras and Media Servers. Any requests coming from users within that Site can be serviced by those on-Site Media Servers. Since the internal network is robust, the video is delivered at high resolution.

However, since this offshore oil platform has limited bandwidth to send data to on-shore monitoring Sites, requests from off-Site users would quickly consume the available outgoing bandwidth.

When the Dynamic Proxy feature is enabled, however, requests for video from off-Site (onshore) clients can be intercepted and services by the Dynamic Proxy. This Dynamic Proxy can collect a single video stream from the off-shore Site and deliver it to multiple users onshore.

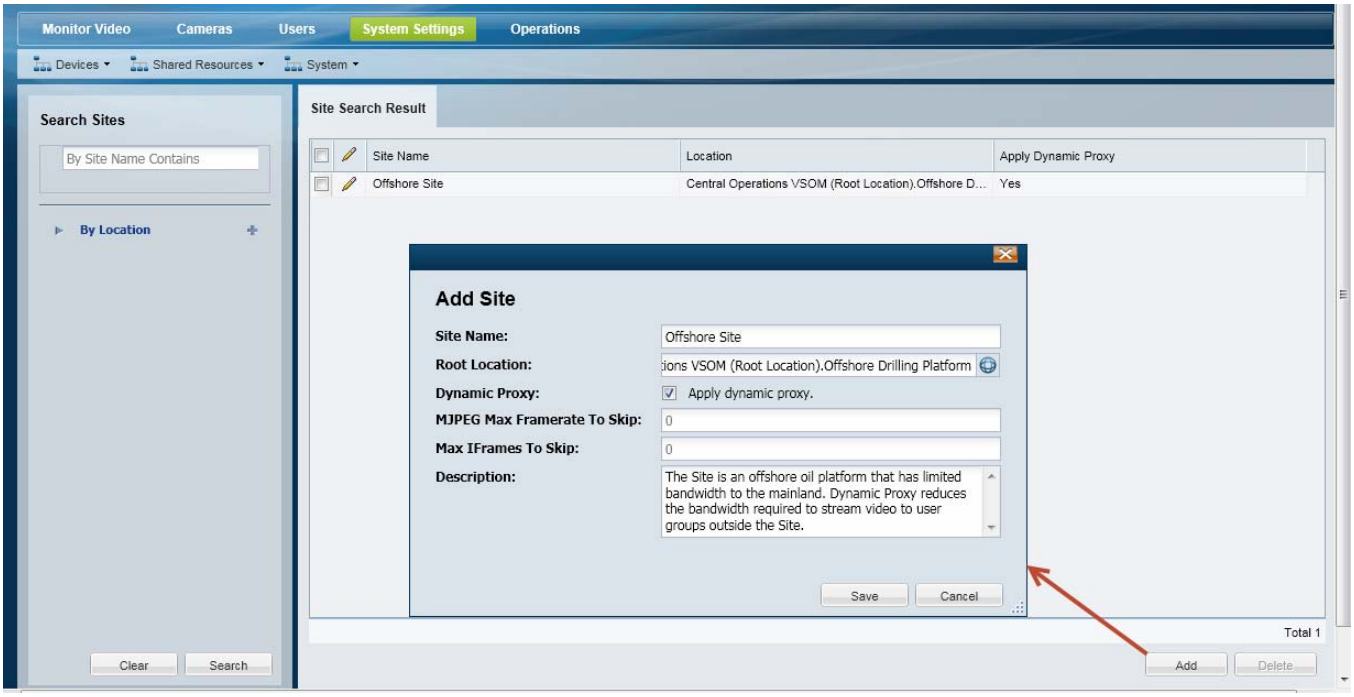
For example:

- The Dynamic Proxy establishes secure communication with the source Media Server, retrieves the video, and displays it to the off-Site user(s) who requested it.
- The Dynamic Proxy service scales down the audio/video quality to accommodate small network pipe between the Media Server and the Dynamic Proxy server.
- The Dynamic Proxy service is only available for live video streams.
- The Dynamic Proxy servers do not support Failover. If a Dynamic Proxy server goes down or is unavailable, the user must re-request the video stream. The video will be served by a different Dynamic Proxy server, if configured.
- PTZ commands can be used by users inside and outside a Site since PTZ commands use a small amount of bandwidth and are sent directly to the Media Server.

Understanding Sites

"Sites" are designated location hierarchies (a location and its sub-locations) where network connectivity between the cameras and servers is good. These *Sites*, however, may have low-bandwidth connectivity to cameras, servers and users outside the Site.

Figure 23-2 Dynamic Proxy Example



For example, in Figure 23-2, a location representing an off-shore oil drilling platform is designated as a Site:

- User Groups assigned to a location within the Site receive video directly from the Media Servers and cameras that are also in that Site location. For example, operators physically located on the oil platform are also assigned to a User Group in the Site. When they request video from cameras that are also located in the Site, they receive full-quality video from the servers in the Site.
- User Groups assigned to a location outside the Site, however, (such as an on-shore location) receive video from a Dynamic Proxy server. The Dynamic Proxy server manages the video requests and communicates directly with the on-Site servers to retrieve the requested video and deliver it to the off-Site user.
  - If users log in outside a Site and access cameras that are also outside the Site, then the DP *is not* used.
  - If users log in outside a Site and access cameras inside the Site, then DP *is* used.

See the "Dynamic Proxy Overview" section on page 23-1 for more information.

Note

- Sites can also be configured without DP support. If the Site has unlimited bandwidth, video streams can be delivered to users outside the Site directly from the Site's Media Server (without using a DP server). See the "Detailed Steps to Configure Dynamic Proxy" section on page 23-6.

- Sites cannot be nested (each Site must be in a separate location tree).
- Cameras/encoders and their associated Media Servers must belong to the same Site (you cannot associate a camera in Site A to a Media Server in Site B).

Dynamic Proxy Requirements

Table 23-1 Dynamic Proxy Configuration Requirements

Requirements	Complete? (✓)
To configure Dynamic Proxy features, 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.	❑
At least one Media Server must be configured for Dynamic Proxy (DP). This DP must be installed and configured for a location outside the Site (a non-Site location). Each Operations Manager supports up to 100 Dynamic Proxies.	❑
Each Media Server requires a server license.	❑
A Site must be created. Users outside the Site are served by the Dynamic Proxy.	❑
Users must belong to a User Group inside the Site to receive video streams directly from the local Media Server (no loss of video quality). Users outside the Site are served by the Dynamic Proxy. **Tip** Users with access to multiple Sites can switch between the Sites at login. For example, if a user has access to both on-shore and off-shore Sites, the user can login from any of the Sites. This is helpful when the user is traveling to remote Sites.	❑

Summary Steps to Configure Dynamic Proxy

To enable Dynamic Proxy, you must enable the DP service on a Media Server, add one or more Sites, and create the User Groups that are either within or outside the Site locations.

Review the following summary steps, and refer to the "Detailed Steps to Configure Dynamic Proxy" section on page 23-6 for more information.

Table 23-2 Summary Steps: Dynamic Proxy Configuration

	Task	Description	Complete? (✓)
Step 1	Log in to the Operations Manager.	Dynamic Proxy is configured using the Operations Manager browser-based interface.	❑
Step 2	Install a Media Server and license.	A license is required for each server added to the system. See Summary Steps to Add or Revise a Server, page 6-8.	❑
Step 3	Enable the Dynamic Proxy service on a Media Server	A deployment must include at least one Dynamic Proxy Media Server.	❑
Step 4	Create one or more Sites.	"Sites" are designated location hierarchies where network connectivity amongst cameras/servers within the Site is very good. • User groups within a Site location receive video directly from the Media Server that is at that location (such as the Media Server on an off-shore oil drilling platform). • Users outside the Site receive video from the Dynamic Proxy server. See the "Understanding Sites" section on page 23-3 for more information.	❑
Step 5	Create User Groups and assign the groups inside or outside the Site location.	User groups that are inside a Site can access cameras that are also in that Site at full bandwidth (no quality loss). User groups outside the Site will receive the video from the Dynamic Proxy, which can result in lower video quality to preserve bandwidth.	❑
Step 6	Monitor video.	Log in to the Operations Manager or Cisco SASD user interface, select a Site and access the video streams available based on your User Group membership. If a camera is inside a Site, and the user is not logged in to that Site, then the video will be provided by the Dynamic Proxy. **Note** If a camera is disabled and then quickly enabled in a deployment with multiple Dynamic Proxy servers, it is possible that the video stream can be viewed by two different operators using two different Dynamic Proxy servers. This occurs if an operator was viewing video before the enable-disable and the other operator starts viewing after the enable-disable. We recommend waiting at least 5 minutes after disabling a camera before re-enabling it.	❑

Detailed Steps to Configure Dynamic Proxy

Procedure

Step 1 Log in 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" section on page 4-1 for more information.

Step 2 Install a Media Server and server license.

See the Summary Steps to Add or Revise a Server, page 6-8.

Step 3 Enable the Dynamic Proxy service on the Media Server (Figure 23-3):

Note At least one Dynamic Proxy server must be available for each Operations Manager.

a. Select **System Settings** > **Servers**.

b. Select the server name.

c. Select the **General** tab.

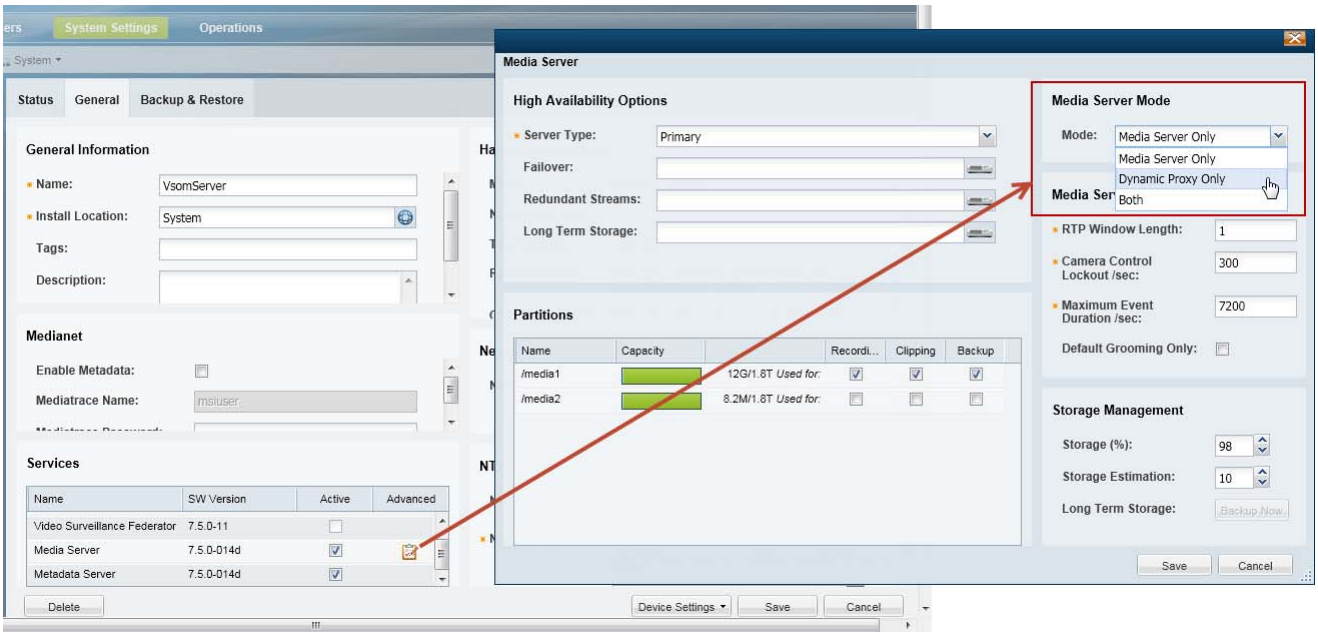
d. Under **Services**, click the **Advanced** icon next to "Media Server".

e. Select the *Media Server Mode* (see Table 23-3 and Figure 23-3):

Table 23-3 Dynamic Proxy (Media Server Mode)

Field	Settings
Media Server Only	Disables Dynamic Proxy functionality on the server. The Media Server is used to support cameras and encoders and to deliver video directly to the user.
Both	The server can be used as a normal Media Server, and as a Dynamic Proxy.
Dynamic Proxy Only	The server is used exclusively as a Dynamic Proxy and cannot manage cameras or be used for other Media Server tasks.

Figure 23-3 Enabling Dynamic Proxy on a Media Server



f. (Optional) Repeat Step 3 to create additional Dynamic Proxies, if necessary.

Step 4 Create one or more Sites.

Tip See the "Understanding Sites" section on page 23-3 for more information.

a. Go to **System Settings > Site Management**.

b. Click **Add** and enter the following settings:

Table 23-4 Site Settings

Setting	Description
Site Name	The name selected by users during login or when changing Sites.
Root Location	The Site location. The location defines the resources available to the users who log in to the Site. All devices (including Media Servers, cameras and encoders) must be in the same Site.
Dynamic Proxy (Apply Dynamic Proxy)	Select to enable the Dynamic Proxy service on the server. • Users who log in to the Site will receive video directly from the Media Servers within the Site. • Users who are outside the Site will receive video from the Dynamic Proxy. • If the Dynamic Proxy option is disabled (deselected), video from cameras at the Site will be delivered to all users by the Site's Media Servers (and not by a Dynamic Proxy server).

Table 23-4 Site Settings (continued)

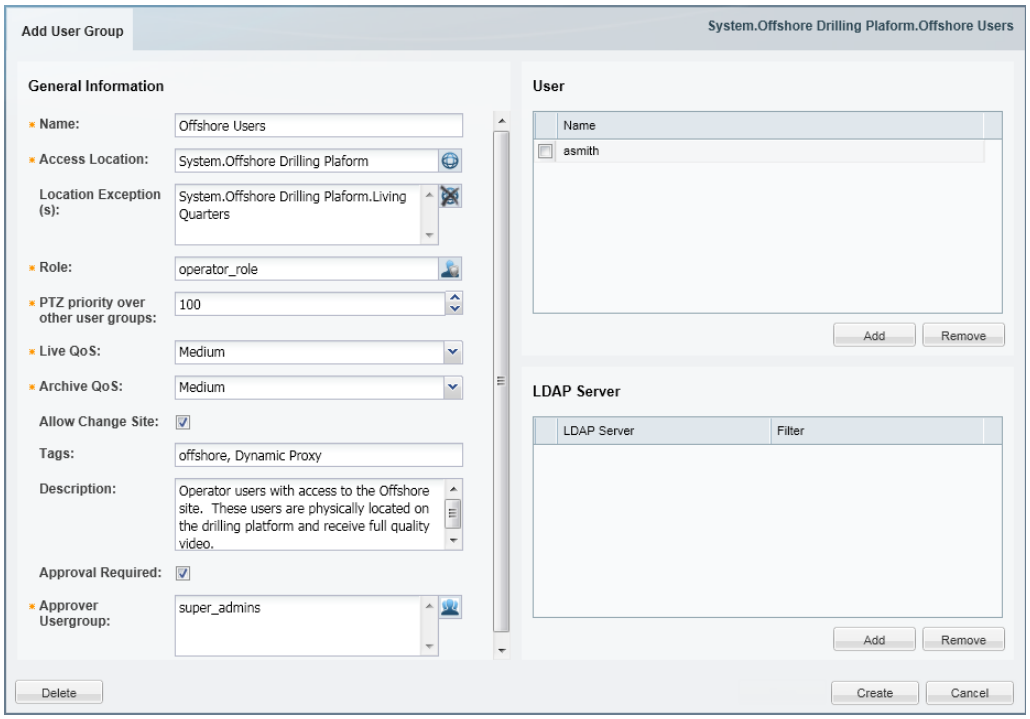
Setting	Description
MJPEG Max Framerate To Skip	(Optional) Stream thinning to be carried out for MJPEG streams. Must be set based on bandwidth availability. All MJPEG frames are IFrames. Depending on the frame rate of the original stream, skip values are supported when the cumulative frame rate is greater than or equal to 0.1 fps. Therefore, the maximum value is 10 times the MJPEG stream's framerate. The supported values are from 1 - 300. For example, if the original frame rate of the MJPEG stream is ***o_fr***, then the "MJPEG Max Framerate To Skip" can be any value, ***x***, where ***o_fr/x >= 0.1 fps***. For example, for 10fps, it is 100, for 30 fps, it is 300, for 0.1fps, it is 10, etc. **Note** This setting is enabled only if the Dynamic Proxy service is enabled.
Max IFrames To Skip	(Optional) The number of IFrames to skip for a video feed. The minimum and maximum skip rates vary depending on the video stream format: **MPEG4/H.264 Streams** The minimum and maximum values are 1– 9 (true only for cameras sending 1IFrame per second). MPEG4 and H264, setting skip results in a stream with only IFrames. Most cameras send 1 IFrame per second. If the stream (regardless of frame rate) is sending 1 IFrame per second, the maximum skip is 9. **Note** This setting is enabled only if the Dynamic Proxy service is enabled.
Description	A meaningful description available in the configuration settings.

c. Click **Save**.

Step 5 Create User Groups and assign them to a location inside or outside the Site (Figure 23-4).

See the "Dynamic Proxy Overview" section on page 23-1 and the "Understanding Sites" section on page 23-3 for more information.

Figure 23-4 Creating a User Group With Access to a "Site"



Tip See the "Adding User Groups" section on page 4-11 for more information.

a. Select the **User Groups** tab .

b. Click **Add**.

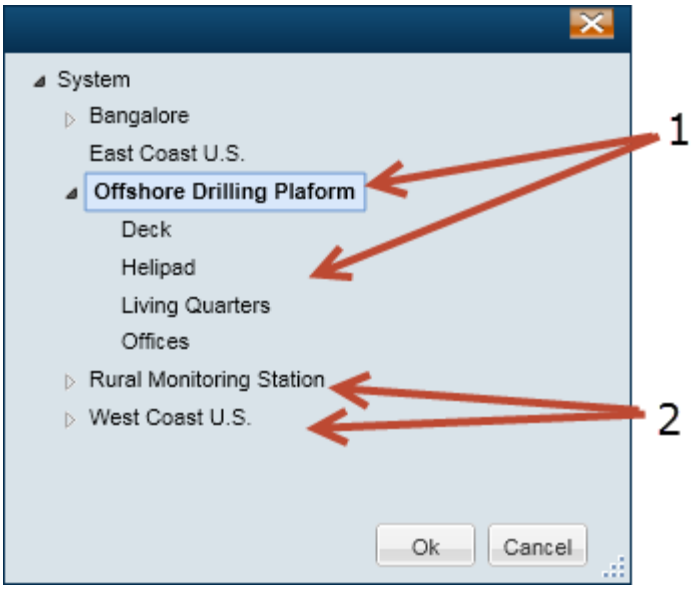
c. Enter the group name, such as "Offshore Users".

d. Select an Access Location (Figure 23-5).

   – Select a location within the Site location if group members should have direct access to video streams from the Media Server (no bandwidth limitations).

   – Select a location outside the Site if group members should receive video streams from a Dynamic Proxy. This can result in lower quality video but minimizes bandwidth uses from video that originates at the Site.

Figure 23-5 Selecting an Access Location for a User Group



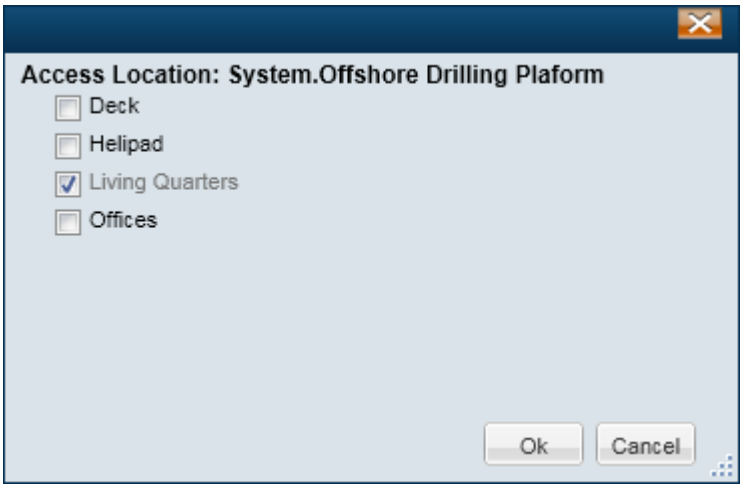
1	Examples of locations *within* the Site.
2	Examples of locations *outside* the Site.

Note The Dynamic Proxy feature is only used if a Dynamic Proxy server is enabled, as described in Step 3.

e. (Optional) Select the Location Exceptions to exclude access to sub-locations.

– For example, in Figure 23-6, the Living Quarters are selected. Although the User Group is assigned to the top-level "Offshore Drilling Platform", the cameras and video from the Living Quarters are excluded and cannot be accessed.

Figure 23-6 Selecting a Location Exception for a User Group



f. Select a Role that defines the access permissions for the group.

- For example, Operators.
- See the "Defining User Roles" section on page 4-9 for instructions to create new roles.

g. Enter the PTZ and QoS settings, as described in Table 4-6 on page 4-12.

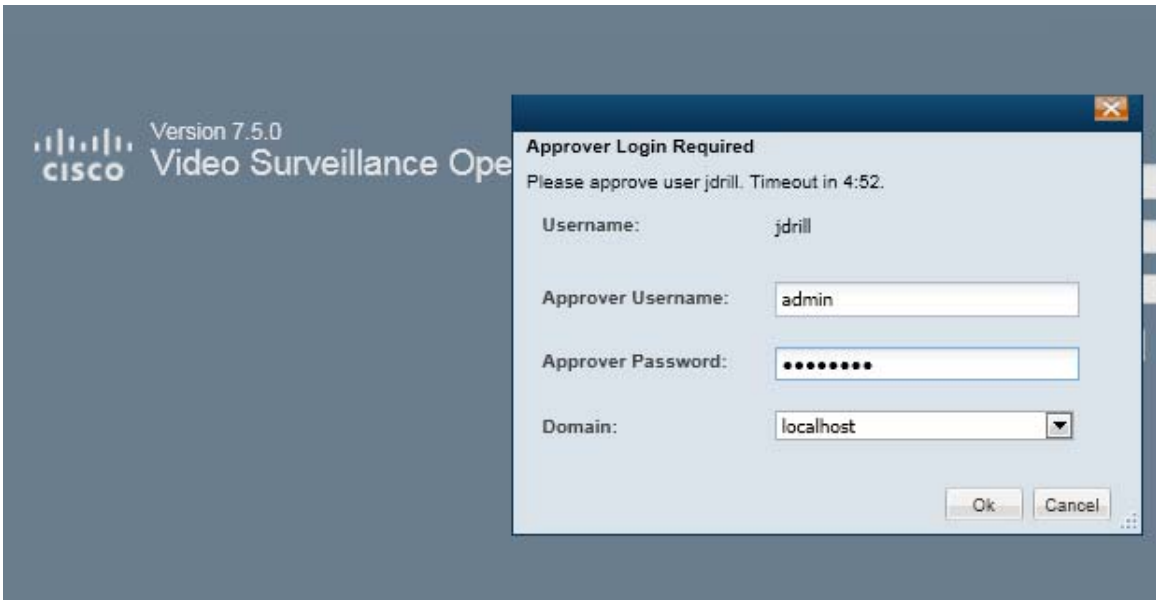
h. (Optional) Select **Allow Change Site** to allow the users to change their Site after logging in.
   - This allows the user to click on the Site name in Operations Manager and change their Site.
   - Deselect (default) to disable this option. Users must log out and log back in to change Sites.

Note Users can only change Sites if they are assigned to User Groups with access to multiple Sites. If "Not In Any Site" is selected, then all video from Sites will be delivered by the Dynamic Proxy.

i. (Optional) Enter the tags and description for the User Group.

j. (Optional) Select **Approval Required** and select an "Approval Usergroup" to require a second user to approve the user login.
   - When the user logs in, a window appears requiring a second user to enter their username and password (Figure 23-7).
   - If the approval is not successfully submitted within the approval time-out, the login is denied.

Figure 23-7 Approver Login



k. Click **Create**.

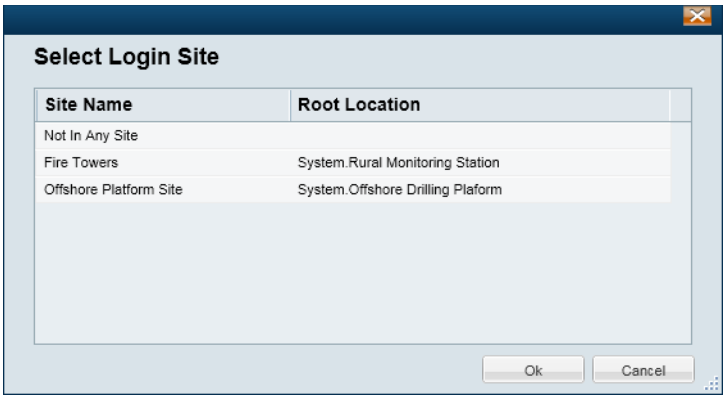
Step 6 Log in to the Operations Manager or Cisco SASD user interface.

a. Enter your username and password.

b. (Optional) Select a Domain if a member of a LDAP directory.

c. Select a Site (if you have access to more than one Site (Figure 23-6).

Figure 23-8 Selecting a Site



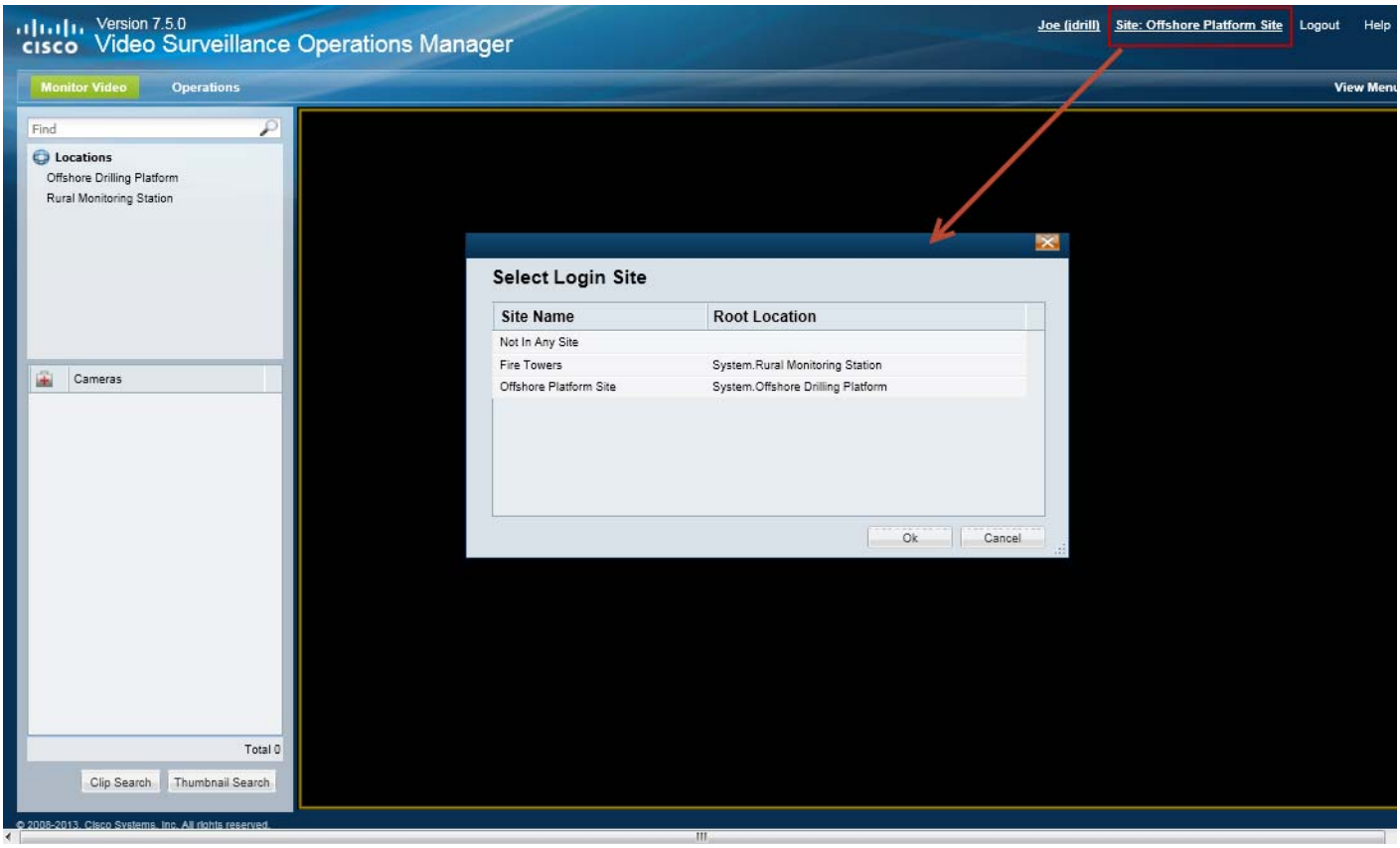
- Users with Site access are prompted for a Site on first login only, but not on subsequent logins.
- Users with no Site access are not prompted for a Site.

Note Users are prompted for a Site again if logging in with a different browser or from a different workstation.

Step 7 (Optional) Change the Login Site.

- After logging in, users can click the Site name to select a different Site (Figure 23-9).

Figure 23-9 Changing the Login Site



Step 8 Log in to the Operations Manager or Cisco SASD user interface, select a Site and access the video streams available based on your User Group membership.

If a camera is inside a Site, and the user is not logged in to that Site, then the video will be provided by the Dynamic Proxy.

Note If a camera is disabled and then quickly enabled in a deployment with multiple Dynamic Proxy servers, it is possible that the video stream can be viewed by two different operators using two different Dynamic Proxy servers. This occurs if an operator was viewing video before the enable-disable and the other operator starts viewing after the enable-disable. We recommend waiting at least 5 minutes after disabling a camera before re-enabling it.

Configuring Location Maps

Use the Maps feature to display a map image for the locations configured in the Cisco VSM deployment. For example, if a deployment includes a location for the city of San Francisco, an aerial street or satellite map can be displayed when users click on that location. The map can display just the relevant details, such as the city block or office complex. Cameras can also be added to the map to indicate where the devices are physically installed. Users of the Cisco Video Surveillance Safety and Security Desktop (Cisco SASD) application can then click on those camera icons to view video and alerts from the cameras.

In addition, image layers can be added to represent additional details on a location map. For example, if a location map shows an aerial view of a office campus, additional image layers can be placed in the same location to show the floor plan for each building. Cameras can be placed on the floor plans, allowing end users to select a building and view video and alerts from the real-world locations of the cameras. Another example is a multi-floor building: image layers can be created for each floor, allowing Cisco SASD users to select a floor from a drop-down list and view video from the cameras installed on that floor.

Refer to the following topics for more information:

Contents

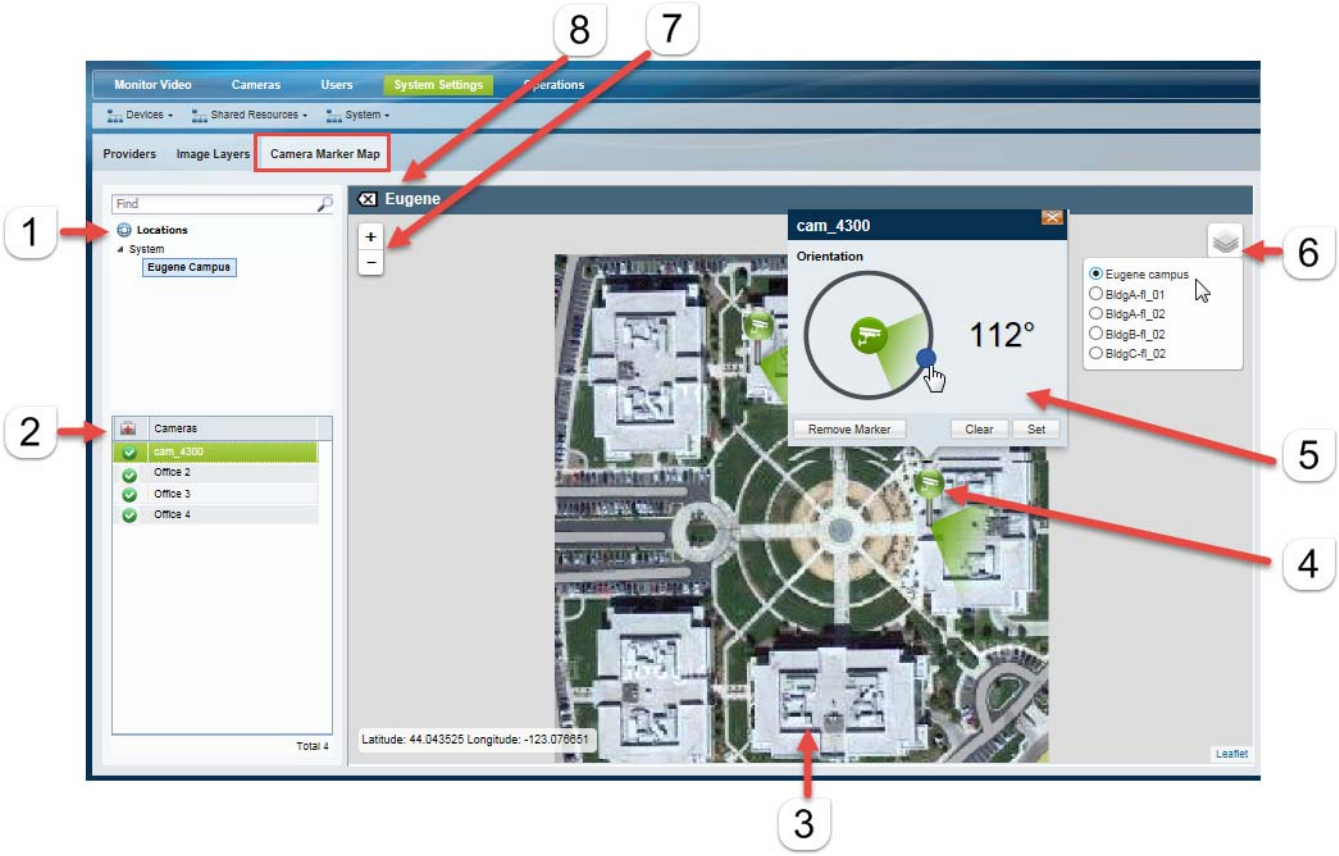
Maps Overview

Location maps display the physical locations defined by a Cisco VSM system. Cisco SASD users can select a location to view the installed cameras placed on the map and to view the image layers (such as a campus, a building or a floor) that represent the real-world location where the cameras are deployed

The Operations Manager is used to define the location map displayed for each location, add *image layers* to the map to represent additional details (such as buildings or floor plans), and add cameras to the maps and images.

For example, Figure 24-1 shows a location map with additional images of a company campus and building on that campus. A camera installed in the building is represented by a green icon. Multi-floor buildings can have a image for each floor, allowing Cisco SASD users to select a specific floor and camera to view video and alerts.

Figure 24-1 Camera Marker Map



1	The selected location.
2	The cameras available at the selected location. Drag cameras onto the map to represent the real-world location of the device.

3	An image layer. • The location map appears when you select a location. • Click the map to display the image layers associated with that location. The image layer group name appears at the top left of the image. • Click the icon to select a different image layer and drag cameras to the image as necessary. See Adding Image Layers and Image Groups, page 24-13 for more information.
4	Camera icon—Drag and drop cameras onto the image to add icons that represent that camera location and status. See Adding Cameras to Map Images, page 24-17 for more information. Cisco SASD users can also click the icons to view video from that device.
5	Camera icon settings—Click a camera icon to open the settings: • Click and drag the blue dot to represent the camera's field of view (for informational purposes only). Click **Set** to save the setting. • Click **Remove Marker** to remove the icon. Camera icons can only be in a single location or map.
6	The image layers available in the group. • Admins can click and select a layer (for example, an image layers for a specific floor-plan in a building), and drag and drop cameras onto the image. • Cisco SASD users can click to select the image for the location they want to view. • See Adding Image Layers and Image Groups, page 24-13 for more information.
7	Zoom controls—You can also click and drag the image to move it within the viewing pane.
8	Image group name—The group name assigned to a set of images. Click the group name to return to the location map.

Usage Notes

- The Operations Manager is used for configuration purposes only. It is not used to access the maps functionality. Use the Cisco SASD desktop application to view camera video and alerts using maps.
- The camera icons are informational only in the Operations Manager. Use the Cisco SASD desktop application to view video and alerts using location maps.
- You may need to adjust the image size or browser screen to properly display the image layer window.
- When upgrading to Release 7.5 or higher (from Release 7.2 or lower) you must migrate the map images from the previous system and reconfigure the map image layers. The Cisco VSM mapping system has been replaced with GIS map support which is not compatible with the earlier map support. Accessing cameras on maps now requires the use of a Cisco VSM Map Server. See the "Migrating Map Images From a Previous Cisco VSM Release" section on page 24-20.
- If a Maps server is replaced and no backup file is available to restore the previous maps configuration and data, then all image files must be re-added.
- You can also deploy the Maps service without using a Mapping provider (such as Mapquest). This is used when there is no access to the external Internet. See the "Displaying Location Maps Without Public Internet Access" section on page 24-23 for more information.

Summary Steps

The following table summarizes the main steps required to configure location maps.

Table 24-1 Summary Steps: Location Maps Configuration

	Task	Description	Complete? (✓)
Step 1	Log in to the Operations Manager.	The Operations Manager browser-based interface is used to configure the mapping features and place cameras on the map images. The Cisco SASD application is used to access camera video and alerts using maps. **Note** To configure maps, 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 2	Define the location map for each location.	Go to **System Settings** > **Locations** to select the map that appears when a location is selected. • The latitude and longitude are automatically entered based on your selection. • See the "Define the Location Maps" section on page 24-8 for more information.	❑
Step 3	(Optional) Add a Maps Server to the Operations Manager to support image layers.	A Maps Server is a Cisco VSM server service that is required to support image layers. A Maps Server can run as a stand-alone server, or be co-located on a server running Operations Manager, or Operations Manager and Media Server (a co-located Maps Server must also run Operations Manager). See the "Adding a Maps Server" section on page 24-10 for more information.	❑
Step 4	(Optional) Add image layers to the map.	Go to **System Settings** > **Maps** > **Image Layers** to add image layers to the location map. Image layers represent structures or real-world locations where the cameras are installed. For example, a campus map, building layout, floor plan, or other real-world image. Images can be stacked on each other in *groups*. For example, a group can include images for a building and each floor in the building. Admins can place cameras on the different floors, and users can select a specific floor to view the cameras installed on that floor. See Adding Image Layers and Image Groups, page 24-13 for more information. **Note** Image layers require a stand-alone or co-located Maps Server enabled on the Operations Manager.	❑

Table 24-1 Summary Steps: Location Maps Configuration (continued)

	Task	Description	Complete? (✓)
Step 5	(Optional) Add cameras to the map images.	Go to **System Settings** > **Maps** > **Camera Marker Map** to drag and drop cameras onto the map images. Camera icons that appear on the maps represent the real-world location where the cameras are installed. Cisco SASD users can click on these camera icons to view video and alerts. See the "Adding Cameras to Map Images" section on page 24-17	❑
Step 6	(Optional) Add a mapping service provider.	Go to **System Settings** > **Maps** > **Providers** to add or change the mapping service that supplies the location maps, such as an aerial street map or satellite view. **Note** Although Cisco VSM includes mapping providers, you can add additional providers, such as Google Maps. You must obtain the proper URL and other information from the mapping provider to add the service. See the "Managing Location Map Service Providers" section on page 24-21.	❑
Step 7	Verify the configuration using Cisco SASD.	Log in to Cisco SASD to verify that map settings are correct and that you can view the images and cameras configured using the Operations Manager. See the Cisco Video Surveillance Safety and Security Desktop User Guide for more information.	❑

Maps Requirements

Table 24-2 Location Maps Configuration Requirements

Requirements	Complete? (✓)
(Required for image layers only) A Maps Server enabled on the Operations Manager. • See the "Adding a Maps Server" section on page 24-10. • A Maps Server can run as a stand-alone server, or be co-located on a server running Operations Manager, or Operations Manager and Media Server (a co-located Maps Server must also run Operations Manager). **Related Documentation** • Understanding Server Services, page 6-3 • Physical server installation: – (Systems pre-installed with Release 7.2 and higher) See the Cisco Physical Security UCS Platform Series User Guide for more information. – (Systems pre-installed with Release 7.0.0 or 7.0.1) See the Cisco Physical Security Multiservices Platform Series User Guide for more information. • Virtual Machine installation—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 server setup—Cisco Video Surveillance Management Console Administration Guide. • Installing Licenses, page 1-26 • Adding a stand-alone Maps Server—Configuring Servers, page 6-1	❑
An Operations Manager user account that belongs to a User Group with manage permissions for *Servers & Encoders*. See the "Adding Users, User Groups, and Permissions" section on page 4-1 for more information.	❑

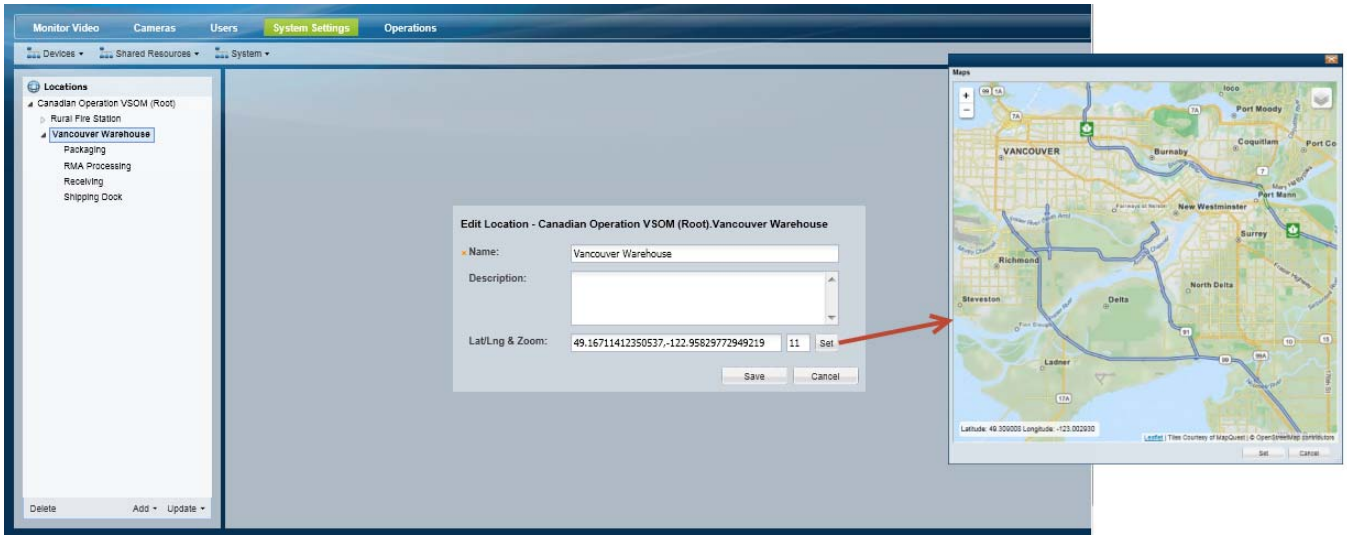
Table 24-2 Location Maps Configuration Requirements (continued)

Requirements	Complete? (✓)
Image files for the map layers, such as building, floors or other images that represent the real-world location in your deployment. **Supported File Formats** The supported image file formats include the following: • Raster format images—jpeg/jpg and png file formats are supported. • Vector (shape files)—For more information, see the Wikipedia description at http://en.wikipedia.org/wiki/Shapefile. **Maximum Recommended File Sizes** Images should be optimized to the smallest file size that preserves image quality. Large image files can consume excessive processing power and degrade system performance. We recommend images no larger than the following maximum sizes. • Vector (shape files)—maximum size 80 MB • JPEG images— maximum size 19 MB and resolution 60 MP • PNG images— maximum size 68 MB and resolution 32 MP	❑
If public Internet access is unavailable, the location maps cannot be displayed using a mapping providers (such as MapQuest). As an alternative, you can upload an image layer for the locations in your deployment. See the additional requirements in the "Displaying Location Maps Without Public Internet Access" section on page 24-23 for more information.	❑

Define the Location Maps

The location map is displayed when a user selects a location using Cisco SASD. The map is defined using the location settings from the Operations Manager and can optionally include cameras and image layers (Figure 24-2).

Figure 24-2 Defining Location Maps



Tip The maps images are provided by a mapping providers, such as MapQuest. A default set of providers is included, but you can add additional mapping providers as described in the "Managing Location Map Service Providers" section on page 24-21.

Note If public Internet access is unavailable, the location maps cannot be displayed using a mapping providers (such as MapQuest). As an alternative, you can upload an image layer for the locations in your deployment. See the "Displaying Location Maps Without Public Internet Access" section on page 24-23 for more information.

Procedure to Define a Location Map Using a Mapping Provider

Step 1 Log in 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" section on page 4-1 for more information.

Step 2 Select **System Settings** > **Locations**.

Step 3 Select a location.

Step 4 Click **Set** to display the map window (Figure 24-2).

Step 5 Use the Zoom In + and Zoom Out − buttons and drag the map image to locate the city, region or other aerial view that represents the location.

Step 6 Click **Set** to select the map as displayed on the screen.

- The Longitude and Latitude of the visible map are automatically entered in the location settings (Figure 24-2).
- The second field reflects the zoom level defined in the map window (see Step 5).

Step 7 Click **Save** to save the map settings for the location.

Step 8 (Optional) Add image layers to the location map to represent the structures or real-world locations where the cameras are installed.

See the "Adding Image Layers and Image Groups" section on page 24-13.

Step 9 (Optional) Add cameras to the map images to represent the real-world location where the cameras are installed. Cisco SASD users can click on these camera icons to view video and alerts.

See the "Adding Cameras to Map Images" section on page 24-17

Adding a Maps Server

Image layers require that a Maps Server be enabled using one of the following methods. The Maps Server allows the image files to be accessed by users of the location map features in Cisco SASD.

- Adding a Co-Located Maps Server, page 24-10
- Adding a Stand-Alone Maps Server, page 24-11

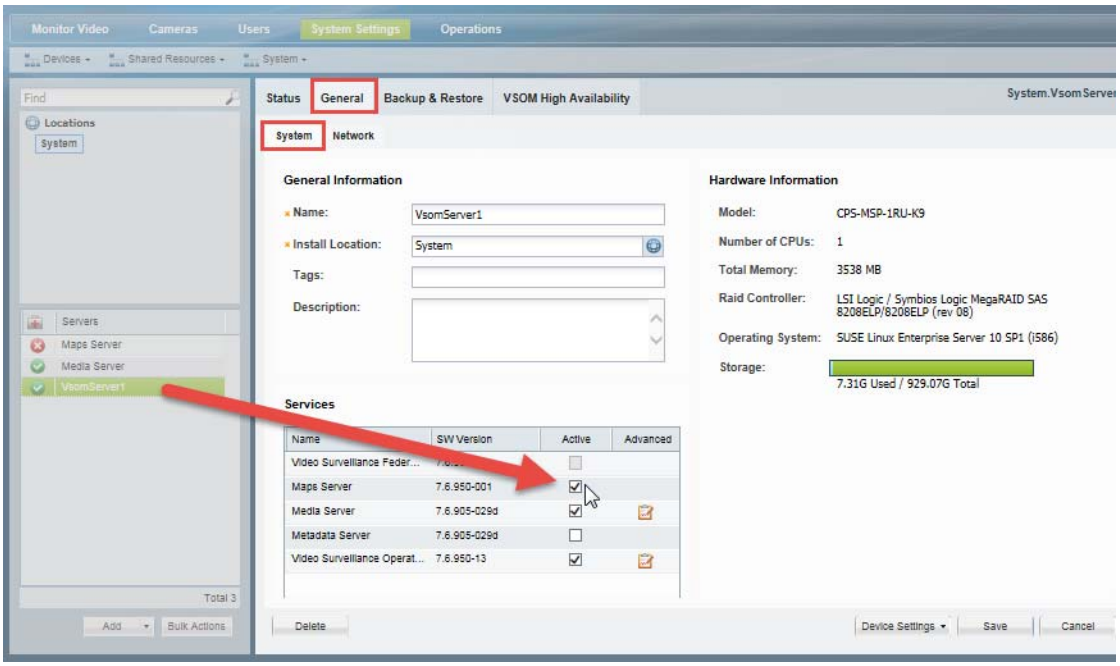
Related Information

- Understanding Server Services, page 6-3
- Server Settings, page 6-10
- Adding or Editing Servers, page 6-16

Adding a Co-Located Maps Server

To enable a co-located Maps Server, enable the service in the Operations Manager server (Figure 24-4).

Figure 24-3 Enabling a Co-Located Maps Server



Procedure

Step 1 Complete the "Maps Requirements" section on page 24-6.

Step 2 Log in to the Operations Manager.

Step 3 Navigate to the Operations Manager server configuration page.

Step 4 Select the **Maps Server** to enable the service on the Operations Manager server.

Step 5 Continue to the "Configuring Location Maps" section on page 24-1.

Adding a Stand-Alone Maps Server

To add a stand-alone Maps Server, install the physical or virtual server and add the server to the Operations Manager.

Procedure

Step 1 Complete the "Maps Requirements" section on page 24-6.

Step 2 Select **System Settings > Servers**.

Step 3 Add the Maps Server:

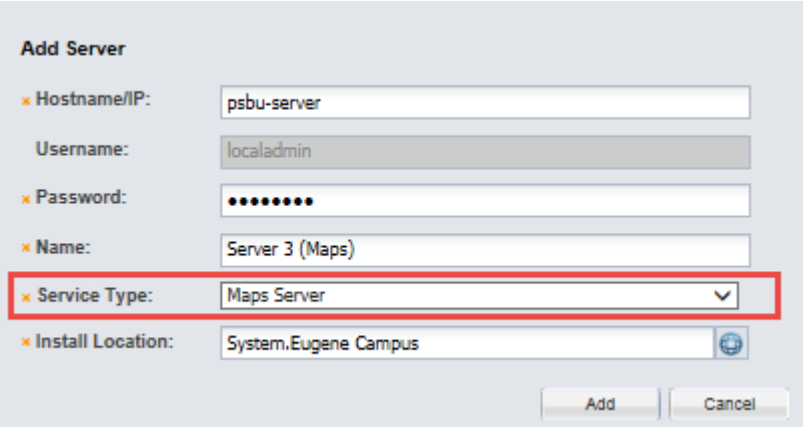
a. Select **System Settings > Servers**.

b. Click **Add**.

c. Enter the required information and select the **Maps Server** *Service Type* (Figure 24-4).

Tip See the "Adding or Editing a Single Server" section on page 6-17 for more information.

Figure 24-4 Adding a Maps Server



Step 4 Click **Add**.

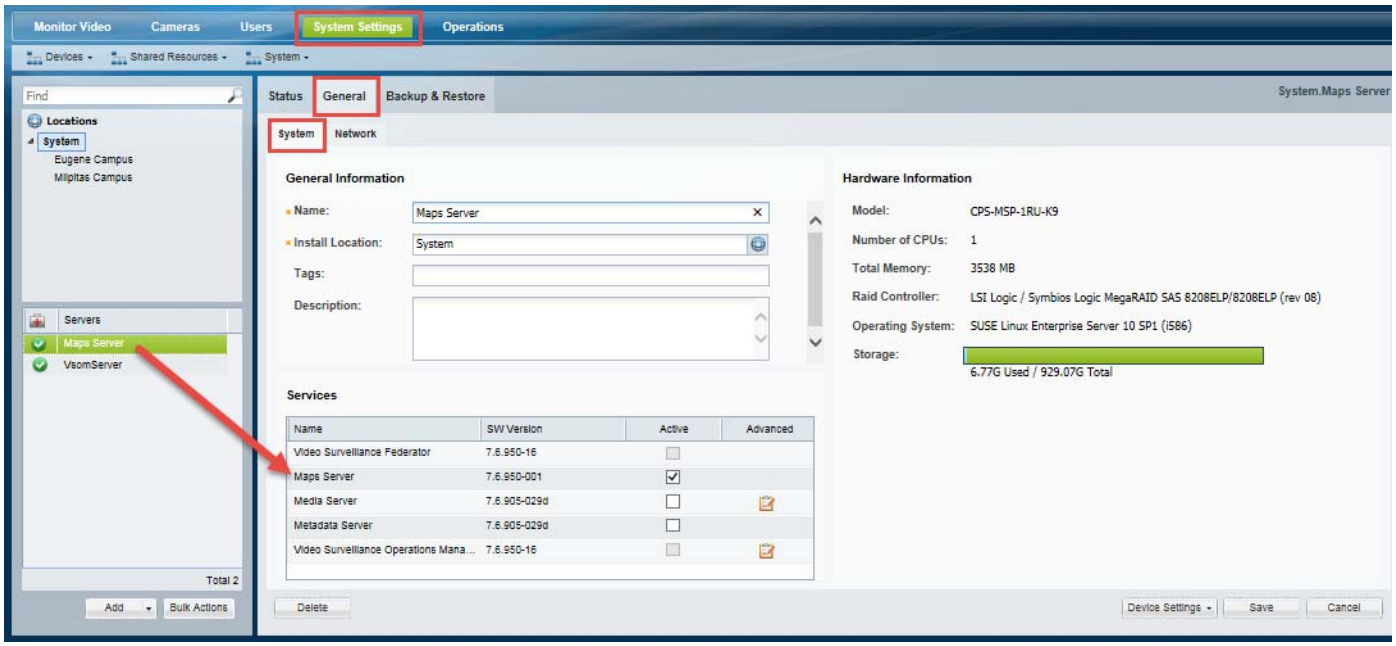
Step 5 Verify that the Maps Server was successfully added:

a. Select the **General** tab.

b. Verify that the **Maps Server** is selected in the Services section (Figure 24-5).

Tip If a server error occurs, see the "Understanding Image Layer Status Errors" section on page 24-24 for more information. See also the "Viewing and Clearing Layer Status Errors" section on page 24-25.

Figure 24-5 Verifying the Maps Server Service



Adding Image Layers and Image Groups

Overview

Image layers allow you to place additional images on top of a location map. For example, if the location map displays a campus, the image layer can display a building floor plan. If the building has multiple floors, the images for each floor can be stacked on top of each other. End users select the relevant image layer from a drop-down menu.

Each *Group* is a collection of images that represent a single entity. For example, the group could include a building image, and additional images for each floor.

Figure 24-6 Image Layers and Groupings

Table 24-3 Image Layer Information

Column	Description
Status	• Published—the image that is uploaded to the system and is bound to a latitude/longitude. • Unpublished—the image that is uploaded to the system but is not bound to a latitude/longitude. **Notes** • Unpublished image layers are stored on the Operations Manager server for 30 days, and then deleted. • We recommend publishing all images before performing an Operations Manager "Config only" backup. Operations Manager "Config only" backups do not backup Unpublished images (which are temporarily stored on Operations Manager server). The Unpublished images are not restored with the backup file, and an "map_layer_ mismatch" issue will occur on the Maps server. See the "Viewing and Clearing Layer Status Errors" section on page 24-25 for more information. • See the "Understanding Image Layer Status Errors" section on page 24-24 for more information on additional status values that can occur after restoring a server from a backup.
Name	The image layer name that is selected by end users.
Location	The location assigned to the image. When a user views a location, they see the image layers assigned to that location, along with the cameras placed on the map images.
Grouping	Images in the same group appear under a "Groupings" entry. Click "+" or "-" to expand or hide the images included in the group. For example, a 4-story building can have images for each floor.

Table 24-3 Image Layer Information (continued)

Column	Description
Elevation	The order that the image layers appear in the drop menu available to end-users. Select a layer and click **Move Up** or **Move Down** to change the display order.
Image	The image name.

Procedure to Add Image Layers

Step 1 Log on to the Operations Manager.

- You must belong to a User Group with permissions for *Locations & Maps*. See the "Adding Users, User Groups, and Permissions" section on page 4-1 for more information.

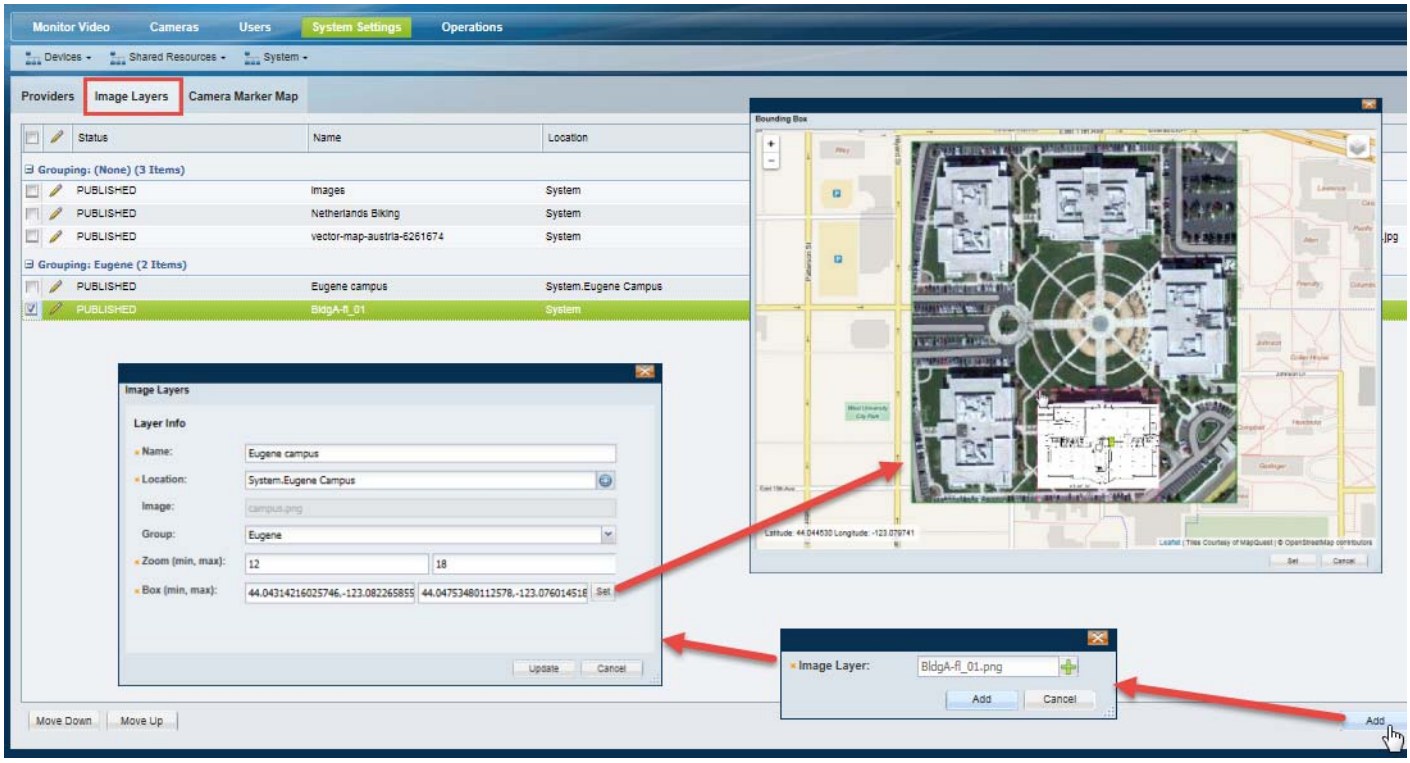
Step 2 Add a **Maps Server** to the Operations Manager to enable the Image Maps feature.

See the "Adding a Maps Server" section on page 24-10.

Step 3 Select **System Settings** > **Maps**.

Step 4 Select the **Image Layers** tab (Figure 24-7).

Figure 24-7 Adding a Map Layer



Step 5 Add an image layer.

One or more image layers can be added to represent multiple objects in the same location. For example, you can have images for a campus, the buildings on the campus, and the floors in the building.

To do this, upload an image, select a location and group (set of related images), and then use the Bounding Box to resize and relocate the image on the map.

For example, in Figure 24-7, the campus image is added and placed on the map. An additional building image is added to the same group, and resized so it appears in the correct location on the campus image. Groups allow the images to be stacked and allow the end-users to click the icon and select the relevant image layer.

a. Click **Add**.

b. Click the add icon and select the image(s) you want to upload from a local or network drive.

Tip You can select a single image file, or a compressed .zip file with multiple images. All images must be a supported file format (see the "Maps Requirements" section on page 24-6).

c. Click **Add** and wait for the job to complete.

- The upload job is complete when the image is uploaded to the Maps Server and the Image Layers pop-up settings window appears (Figure 24-7).

d. Enter the image layer settings in the pop-up window (Table 24-4).

Table 24-4 Image Layer Settings

Field	Settings
Name	The image layer name. For example: "Floor 1".
Location	The location where the image layer will appear.
Image	(Read-only) The image filename.
Group	The group of images that the image belongs to. Users click the icon to select an image from the group. For example, all floor images can belong to a group called "Building 2". • To create a group, enter the group name. The entry will be saved and can be selected when you add additional image layers. • Select a group from the drop-down menu if the group name was previously entered.
Zoom	The minimum zoom level and the maximum zoom level. The image layer is shown on the location map only when the zoom level from the location map falls between the min/max zoom levels.
Box	Click **Set** to bring up the image on the location map. You can re-size the image to display it in the correct location (Figure 24-7). a. Click **Set**. b. In the pop-up map window, use your mouse to: – Zoom in and out or re-position the map. – Click and drag the corner of the image to resize and relocate it on the map. – Click an image to enlarge it. – Click the icon to select a image in the group. c. Click **Set**. The *Box (min, max)* coordinates are automatically entered.

d. Click **Update** to save the image layer settings.

Step 6 (Optional) Add image sub-layers.

You can add additional image layers to represent sub-locations (Figure 24-8). For example:

- A campus location can have additional building layers.
- A building location can have additional floor layers.

Users click the icon to select a layer and view the cameras or alerts for the specific building, floor, or other image.

To add additional sub-layers:

a. Click **Add**.

b. Click the add icon and select the image to upload from a local or network drive.

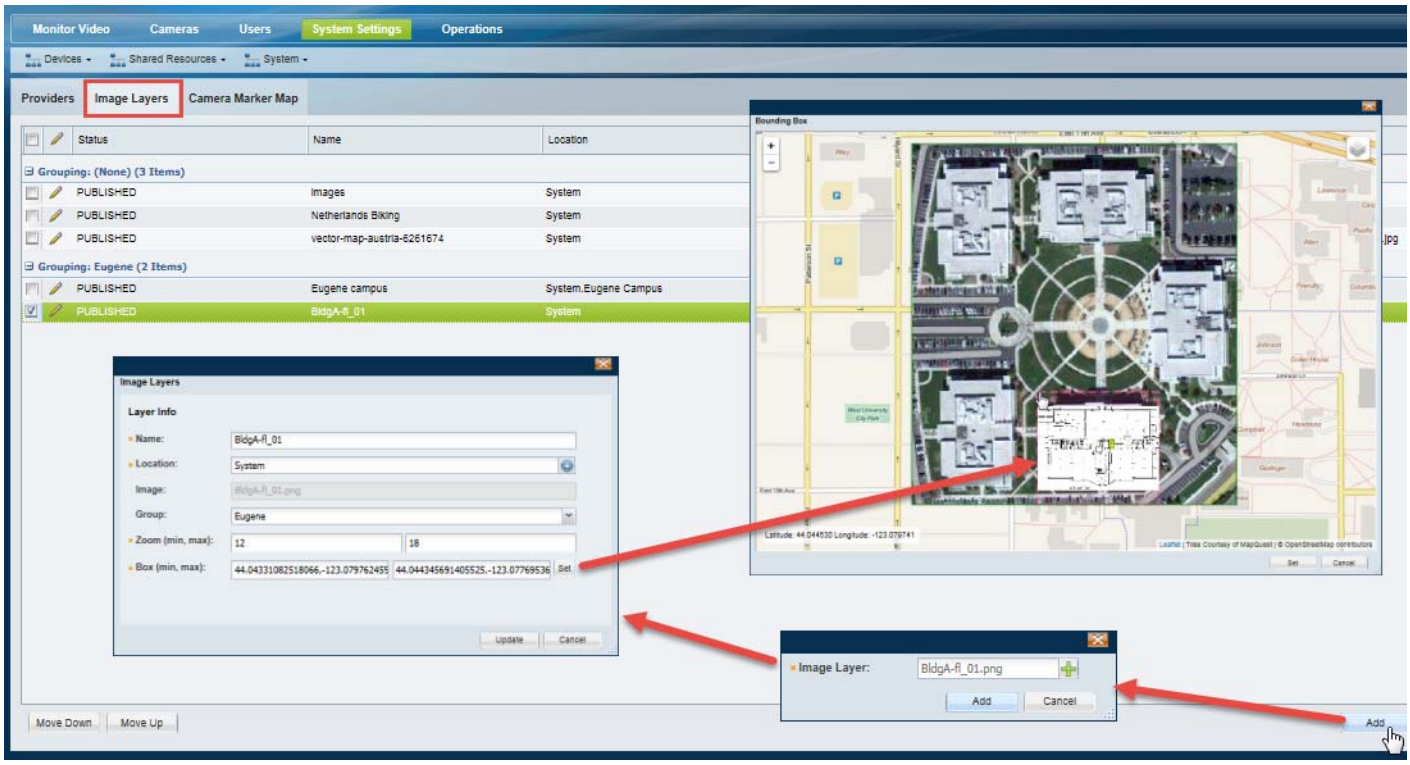
c. Click **Add** again and wait for the job to complete.

d. Enter the settings described in Table 24-4 using the following guidelines:

- Select an existing **Group**. For example, select the group created for the *campus* image. The layers included in a group can be selected by end-users from a drop-down menu.
- Click **Set** to resize the sub-layer in relation to any other images in that same group (Figure 24-8). Click **Set again** to save the box settings.

For example, in Figure 24-8, the image layer for a building floor plan is added and assigned to the same group as the campus image. The building image is re-sized on the campus to show it's location.

Figure 24-8 Adding a Sub-Layer



e. Click **Update** to save the image layer settings.

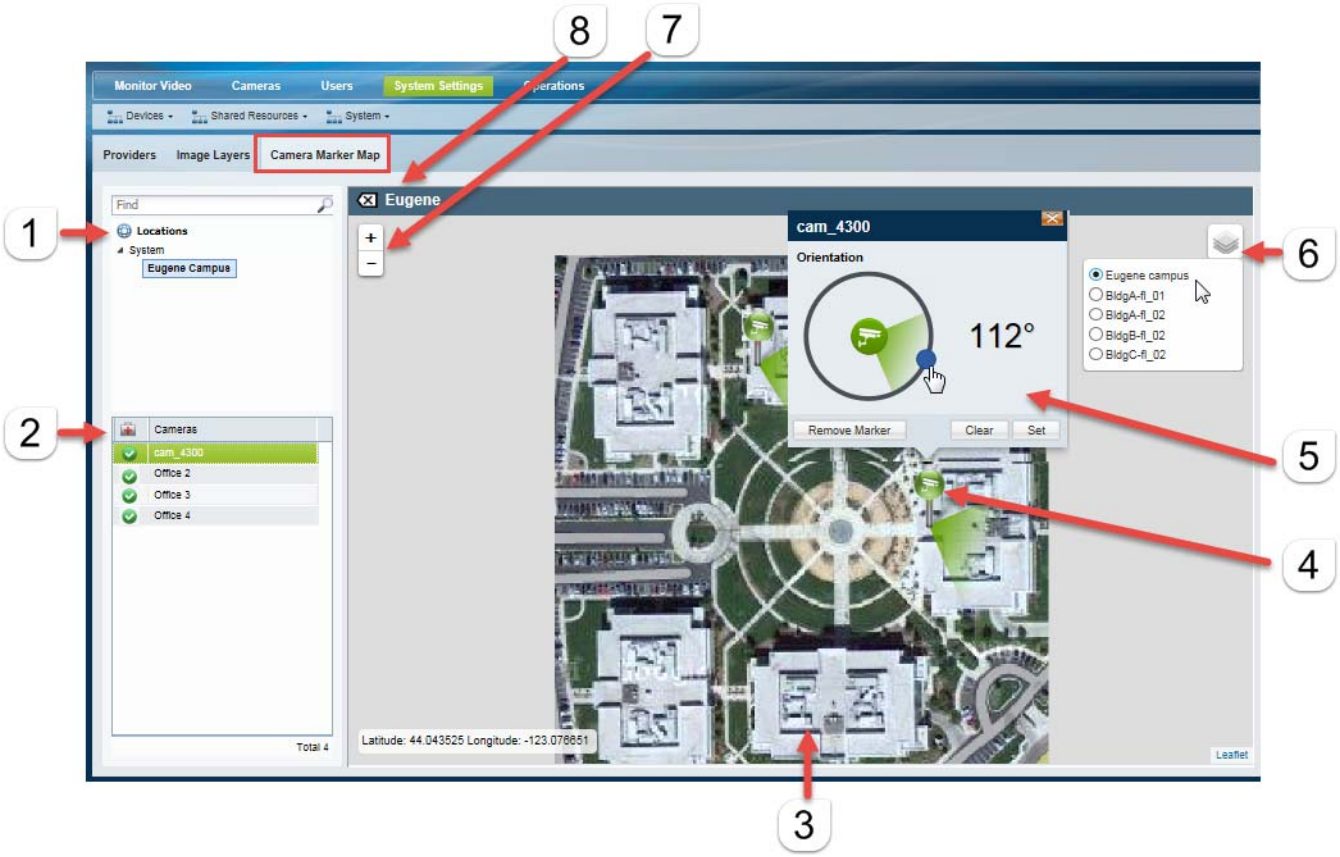
f. Repeat Step 6 to add additional layers. For example, add additional building images or floor plans for multi-story buildings (Figure 24-8).

Adding Cameras to Map Images

Use the Camera Marker Map to add cameras to the maps. The camera icons represent where cameras are physically installed (Figure 24-9), and Cisco SASD desktop application users can click the icons to view video or monitor alerts. Cameras can be added to the location map, and to the image layers placed on the location map.

Figure 24-9 shows the Camera Marker Map. Select a location, and then select a image layer (if configured). Drag and drop the cameras configured for that location onto the map. The camera is represented by a icon (the color represents the device status), and you can indicate the camera's approximate field-of-view by clicking the icon and adjusting the settings (the field of view is non-functional and for informational purposes only).

Figure 24-9 Camera Marker Map



1	The selected location.

2	The cameras available at the selected location. Drag cameras onto the map to represent the real-world location of the device.
3	An image layer. • The location map appears when you select a location. • Click the map to display the image layers associated with that location. The image layer group name appears at the top left of the image. • Click the icon to select a different image layer and drag cameras to the image as necessary.
4	Camera icon—Drag and drop cameras onto the image to add icons that represent that camera location and status. Cisco SASD users can also click the icons to view video from that device.
5	Camera icon settings—Click a camera icon to open the settings: • Click and drag the blue dot to represent the camera's field of view (for informational purposes only). Click **Set** to save the setting. • Click **Remove Marker** to remove the icon. Camera icons can only be in a single location or map.
6	The image layers available in the group. • Admins can click and select a layer (for example, an image layers for a specific floor-plan in a building), and drag and drop cameras onto the image. • Cisco SASD users can click to select the image for the location they want to view.
7	Zoom controls—You can also click and drag the image to move it within the viewing pane.
8	Image group name—The group name assigned to a set of images. Chick the group name to return to the location map.

Procedure to Add Cameras to The Location Maps and Image Layers

Complete the following steps to add cameras to the location map and to the image layer.

Note The camera icons are informational only in the Operations Manager. Use the Cisco SASD desktop application to view video and alerts using the camera icons.

Step 1 Define the location map for a location.

See the "Define the Location Maps" section on page 24-8.

Step 2 Add image layers to the same location.

See the "Adding Image Layers and Image Groups" section on page 24-13.

Step 3 Select **System Settings > Maps**, and click the **Camera Marker Map** tab.

Step 4 Select a location (Figure 24-9).

Step 5 (Optional) Click the map image to view the image layers for that location.

Step 6 (Optional) Click the selector icon to select an image layer.

Step 7 Add cameras to the image.

a. Drag and drop cameras onto the map.

b. To re-orient the camera's field of view, click the camera icon and drag the blue dot, and click **Set**. The field-of-view is not functional, and for informational purposes only. For example, the PTZ controls are not affected.

c. To move the camera marker, drag and drop the camera name to a new location.

Step 8 The changes are automatically saved (you can close the window or navigate to a different screen).

Migrating Map Images From a Previous Cisco VSM Release

When a Cisco VSM deployment is upgraded from a release prior to Release 7.5, a .zip file is created on the Operations Manager that contains all of the map images previously added (using Cisco SASD).

- Directory— `/usr/BWhttpd/vsom_be/images/`
- Filename—`mapsFromOldVersion.zip`

Note The image filename format is <*locationName*>**.**<*file extension*>. Cisco VSM does not store the original image filenames.

Note This procedure is necessary only for upgrades from a release prior to 7.5. For upgrades from Release 7.5 or higher, the map image migration is automatic.

Procedure

Step 1 Complete the upgrade to Cisco VSM Release 7.5 or higher.

Step 2 Use a file utility (such as WinSCP) to manually copy the `/usr/BWhttpd/vsom_be/images/mapsFromOldVersion.zip` file from the Operations Manager server to a monitoring workstation.

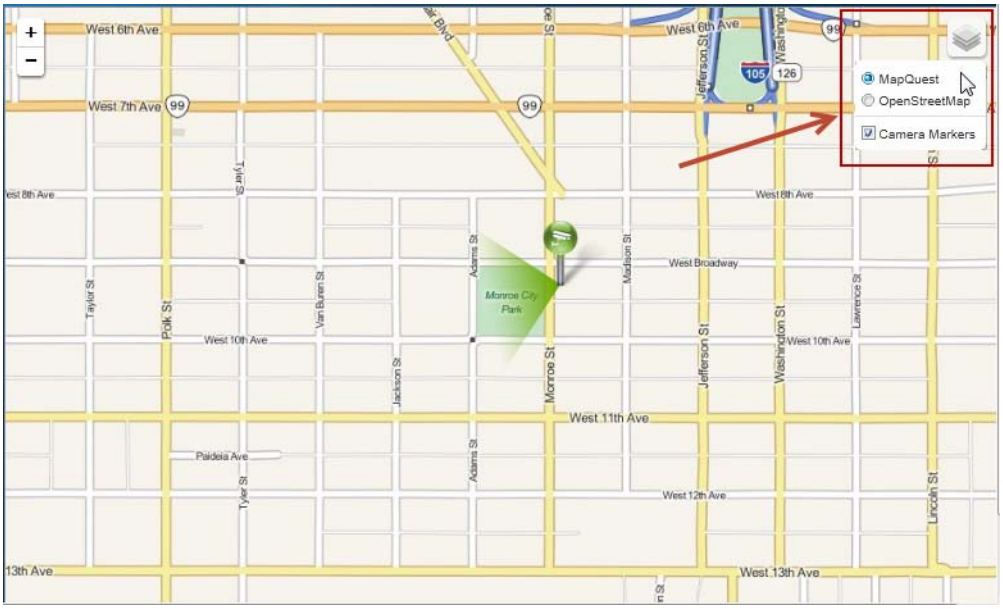
Step 3 Install and configure a Maps Server as described in the "Adding a Maps Server" section on page 24-10.

Step 4 Add the `mapsFromOldVersion.zip` file to the Operations Manager Maps Layers page. See the "Adding Image Layers and Image Groups" section on page 24-13 for more information.

Managing Location Map Service Providers

Cisco VSM includes a set of default map service providers to display the location map (the street or satellite view) for each location. The map provider can be selected using the selector icon in the top right corner of the video window (Figure 24-10).

Figure 24-10 Map Provider Selection



To add a mapping service provider, you must obtain a URL from the provider, such as Google maps. Additional providers can be selected by users, and you can change the order they appear, the default provider, and hide or show the providers.

Prerequisites

To add a provider, you must obtain a URL from the map service provider (such as Google maps). Follow the instructions provided by the map service provider.

Procedure to Add a Location Map Provider

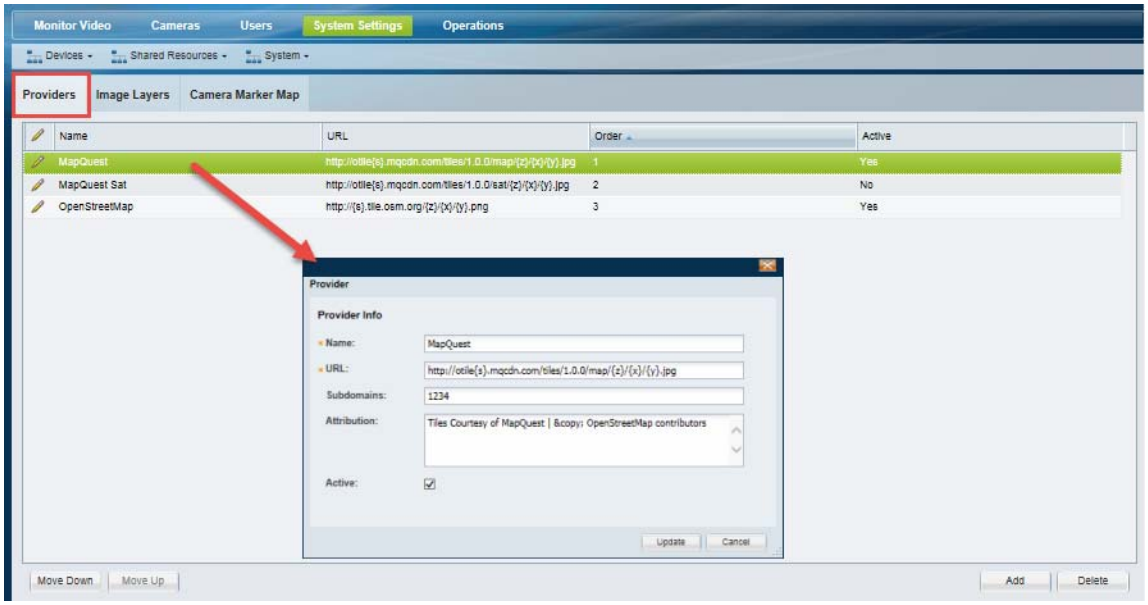
Step 1 Log on to the Operations Manager.

- You must belong to a User Group with permissions for *Locations & Maps*. See the "Adding Users, User Groups, and Permissions" section on page 4-1 for more information.

Step 2 Select **System Settings** > **Maps**.

Step 3 Select the **Providers** tab (Figure 24-11)

Figure 24-11 Map Providers



Step 4 Click **Add** to add a new provider, and enter the provider settings (Table 24-5).

Table 24-5 Map Provider Settings

Field	Settings
Name	The provider name that appears in the selection list.
URL	The URL provided by the map service provider that enables the location maps to be displayed.
Subdomains	(Optional) The subdomain, if it is provided by the map service provider.
Attribution	(Optional) The text that appears at the bottom of the page indicating the source of the map. For example: "Courtesy of MapQuest".
Active	Select **Active** (default) to display the provider name (and allow users to select the provider). Deselect **Active** to disable the provider. **Note** Deactivated providers are not displayed in the user interface. Deactivate all providers if the deployment does not have public Internet access. See the "Displaying Location Maps Without Public Internet Access" section on page 24-23.

Step 5 (Optional) Select a provider name and click **Move Up** or **Move Down** to change the order that the providers appear in the selection list (Figure 24-11).

Step 6 (Optional) To show or hide the providers that appear in the selection list, double-click a provider name and select or de-select **Active** (Table 24-5).

Step 7 Click **Update**.

Displaying Location Maps Without Public Internet Access

If a deployment does not have access to the public Internet, the mapping service (such as Mapquest) cannot be accessed to provide the base location map (such as an aerial or satellite view). This will prevent the location map from appearing.

Note A deployment may not allow public Internet access for security or other reasons.

In such situations, the Maps feature can still be used, but you must disable all mapping service providers and upload image layers for each location where you want a default location map to appear.

See the following topics for more information:

- Requirements, page 24-23
- Procedure to Display Location Maps Without Public Internet Access, page 24-23

Requirements

Verify that the following requirements are completed to display location maps when public Internet access is unavailable.

Table 24-6 Requirements to Use Maps Without Internet Access

Requirements	Complete? (✓)
A Maps Server must be installed to enable image layers. See the "Adding a Maps Server" section on page 24-10.	❑
All mapping services must be disabled in the Operations Manager. **Related Information** • Procedure to Display Location Maps Without Public Internet Access, page 24-23 • Managing Location Map Service Providers, page 24-21	❑
An image layer must be configured for each location. **Note** The mapping provider is typically used to provide a default location map for each location. If public Internet access is not available, maps cannot be loaded from the mapping provider and you must provide the image for each location using the image layers. **Related Information** • Procedure to Display Location Maps Without Public Internet Access, page 24-23 • Adding Image Layers and Image Groups, page 24-13	❑

Procedure to Display Location Maps Without Public Internet Access

Step 1 Install and enable a Cisco VSM Map server in your Cisco Video Surveillance deployment.

See the "Adding a Maps Server" section on page 24-10 for instructions.

Step 2 Disable all Map service providers.

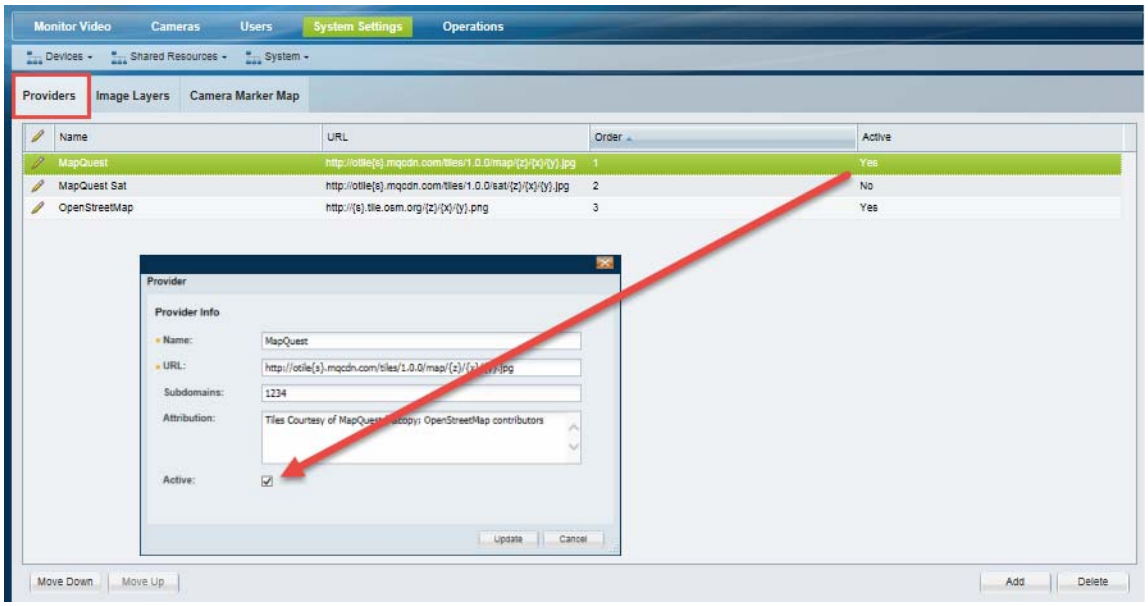
a. Log on to the Operations Manager.

– You must belong to a User Group with permissions for *Locations & Maps*. See the "Adding Users, User Groups, and Permissions" section on page 4-1 for more information.

b. Select **System Settings** > **Maps**.

c. Select the **Providers** tab (Figure 24-12)

Figure 24-12 Disabling All Map Providers



d. Double-click the provider name to edit the settings.

e. De-select **Active** to disable the provider (Figure 24-12). Deactivated providers are not displayed in the end-user interface.

f. Repeat these steps to disable all providers.

Step 3 Add an image layer for each location where a default image should appear.

See the "Adding Image Layers and Image Groups" section on page 24-13.

Step 4 (Optional) Add additional image layers for sub-locations, buildings, floors, or other real-world locations, if necessary.

Understanding Image Layer Status Errors

When a Map or Operations Manager server is restored from a backup, the normal image Layer Status is one of the following (see Table 24-7):

- Published—the image that is uploaded to the system and is bound to a latitude/longitude.
- Unpublished—the image that is uploaded to the system but is yet to be bound to a latitude/longitude.

However, depending on the state of the backup file used to restore the images, one of the following states can also occur.

For example, We recommend publishing all images before performing an Operations Manager "Config only" backup. Operations Manager "Config only" backups do not backup Unpublished images (which are temporarily stored on Operations Manager server). The Unpublished images are not restored with the backup file, and an "map_layer_ mismatch" issue will occur on the Maps Server.

Tip These states can cause Critical server status errors. See the "Viewing and Clearing Layer Status Errors" section on page 24-25 for more information.

Table 24-7 Layer Status Error States (After a Restore)

Layer Status	Description
VSOM_ONLY	Only the layer details are available on the Operations Manager but the Maps Server does not have actual layer files. Image layers in the VSOM_ONLY state are not be visible on monitoring clients (Cisco SASD). You must manually delete the layer from the Camera Marker Map and re-upload the same layer again. This can occur when the list of layers in the Maps Server backup does not match the list in the Operations Manager configuration (usually because the Maps Server backup is older than the Operations Manager configuration).
MAPSERVER_ONLY	The layer files are available only on the Maps Server (and not on the Operations Manager server). The Operations Manager has no information about these layers. Image layers in the MAPSERVER_ONLY state are not be visible on monitoring clients (Cisco SASD). You must manually delete the layer from the Camera Marker Map and re-upload the same layer again. This can occur when the Operations Manager configuration is restored from an earlier date backup than the Maps Server. The list of deployed image layers in the Operations Manager and Maps Server will not match.
CONFIG_MISMATCH	The Bounding Box values for the image layer in the Operations Manager and Maps Server do not match. Select the layer and click **Update** to push the Bounding Box value of the layer from the Operations Manager to the Maps Server.

Viewing and Clearing Layer Status Errors

Any of the Layer Status states described in Table 24-7 appear as an issue in the Map Server Status tab.

- Open the Maps Server configuration page and select **Status > Status History** (see the "Viewing Server Status" section on page 6-29).
- The "map_layer_ mismatch" issue is also displayed in the health dashboard. See the "Health Dashboard: Device Health Faults on an Operations Manager" section on page 19-6.
- Go to **System Settings > Maps> Image Layers** (Figure 24-7) to clear the image layer issues as described in Table 24-7.

Note The “map_layer_ mismatch” issues are automatically cleared from the status and health pages when the image files are deleted or updated.

Configuring Medianet

Overview

Medianet is a suite of features that enables the following:

- Automatic discovery of cameras when they are added to the network.
- Automatic configuration of switch ports based on the device type and other rules.
- The collection of metadata that can be used by a monitoring tool.
- Cisco Performance Monitoring—a Medianet feature that measures the performance of RTP, TCP and IP traffic on supported Medianet network devices. Cisco Performance Monitoring allows administrators to collect performance metrics on supported endpoints or intermediate nodes for monitoring video quality conditions.

Medianet Support in Cisco Video Surveillance Versions

Cisco VSM versions support the following Medianet features:

Table 25-1 Medianet Feature Support in Cisco VSM Releases

Release	Implementation Phase	Support
Release 7.0.0 and higher	Phase 1	Supports Camera Discovery and Auto-Smart Ports. See the "Discovering Cameras on the Network" section on page 10-23.
Release 7.2.0 and higher	Phase 2	Supports Medianet metadata and Mediatrace. See the "Medianet Metadata and Mediatrace" section on page 25-3.
Release 7.5.0 and higher	Phase 3	• Supports Media Services Interface (MSI) version 4.0 on Media Servers and the video client (the 64-bit video client uses the 64-bit MSI). This allows performance monitoring and Mediatrace on TCP flows between the Media Server and browser-based or Cisco SASD client wokstations. – Media Server and Clients—the MSI must be upgraded to v4.0. – Cameras—camera firmware version 2.0.0-175 or higher is required. – The Network Management System (such as LiveAction) must be upgraded to the latest version to communicate with the MSI endpoints (Media Server, monitoring clients, and cameras). **Note** Only inbound DSCP is supported in MSI. Outbound DSCP is not supported in MSI 4.0 (the value will always be 0). • Mediatrace is supported on all Cisco VSM ActiveX monitoring clients (including the Cisco SASD). **Note** Mediatrace and Performance monitoring are not supported on Media Servers with two Ethernet ports enabled.

Medianet Metadata and Mediatrace

Release 7.2 and higher support Medianet metadata and Mediatrace.

Refer to the following topics for more information:

Medianet Metadata

The metadata infrastructure allows end points to identify a data flow through the network. Network administrators use this data to classify network traffic (such as video) and implement quality of service (QoS) features.

In Cisco VSM Release 7.2 and later, metadata can be generated for data flowing from Cisco IP cameras to the Cisco Media Servers, and from the Cisco Media Servers to the Cisco VSM workstation clients. Metadata must be enabled on all supported devices as summarized in the "Metadata Requirements" section on page 25-8.

Once enabled, no user interaction is required. The metadata is reported in the background and you must use a monitoring tool to view results. Cisco VSM Release 7.2 and later support the LiveAction desktop application described in the "Performance Monitoring and Mediatrace" section on page 25-6.

Tip For more information, see the Cisco website "Media Awareness" at: http://www.cisco.com/web/solutions/trends/medianet/media_awareness.html

Metadata Requirements

In Cisco VSM Release 7.2 and higher, Medianet metadata is supported on the following devices.

Note Medianet metadata must be enabled on all intermediate nodes in the data path, including routers, switches, IP cameras, Cisco Media Servers and monitoring workstations.

Table 2 Medianet Metadata Supported Devices

Device	Description	Complete? (✓)
Cisco routers and switches	The Cisco VSM application and attributes (Media Server, endpoints, and clients) are supported on the following: • Cisco Integrated Services Routers (ISR) G2—Cisco IOS version 15.4(1)T • Cisco ASR 1000 Series Aggregation Services Routers (ASR)—Cisco IOS version 15.4(1)S • Cisco Catalyst Series Switches—3000 and 4000 series switches require Cisco IOS version 15.2(2)E • Cisco Catalyst Series Switches—6000 series switches require Cisco IOS version 15.2(1)SY **Note** Prior IOS versions, currently supported metadata values can be viewed and used for classification.	❑
Cisco IP cameras	See the Release Notes for Cisco Video Surveillance Manager for the cameras that support Medianet 2 features. **Note** Cisco devices must be running the minimum supported firmware version to support Medianet 2 features.	❑
Cisco Media Servers	Metadata is supported on servers running release 7.2 or higher. To enable metadata on a server running the Cisco Media Server service: 1. Log in to the browser-based Cisco VSM Operations Manager. 2. Select **System Settings** > **Servers**. 3. Select a server. 4. Select the **Enable Metadata** checkbox (under the Medianet heading). **Note** Metadata is disabled by default. No user interaction is required for metadata tagging, once enabled.	❑

Table 2 Medianet Metadata Supported Devices (continued)

Device	Description	Complete? (✓)
Workstation clients used to monitor video	Browser-based clients running the Cisco Multi-Pane client software (an ActiveX client) must have the MSI utility installed. MSI is enabled on the workstation by installing the MSI client software: 1. Log in to the browser-based Cisco VSM Operations Manager. 2. Select the **Operations** tab. 3. Select "**MSI Installation Package**" (under the "Software" heading). 4. Double-click the installer package on your workstation and complete the on-screen instructions. **Notes** • Metadata is supported on Windows 7-based workstations running the 32-bit Cisco Multi-Pane client. • Metadata is not supported on Cisco SASD in Release 7.2. • No user interaction is required for metadata tagging, but the MSI utility must be installed to enable the feature. **Related documentation:** • See Client Workstation Restrictions, page 25-6. • Cisco Video Surveillance Operations Manager Mobile App User Guide • See the Cisco Video Surveillance Monitoring Workstation Performance Baseline Specification for more information about the Cisco Multi-Pane client software.	❑

Metadata Restrictions

Cisco Media Server

Medianet metadata must be enabled on each Cisco Media Server using the browser-based Cisco VSM Operations Manager.

- Medianet metadata is disabled by default.
- Metadata is not generated or propagated by the Media Server for flows created prior to enabling this feature. Flows created prior to enablement must be re-established with Medianet feature enabled.

Cisco Routers and Switches

Cisco IOS routers and switches running IOS version earlier than 15.4(1)T are limited to 100 flows per source IP addresses (see CSCuf35612 for more information).

Since the Cisco Media Server is the only Cisco VSM device that creates a large number of flows, this 100 limit restriction can be mitigated on large scale deployments by using separate Medianet enabled routers or switches between the device-to-Media Server segments and the Media Server -to-clients segments. This can enable up to 250 camera streams per Media Server and 60 clients per Media Server.

Network Restrictions

- Medianet metadata is not supported across Network Address Translation (NAT) boundaries.

Client Workstation Restrictions

- Medianet metadata for the Cisco VSM client is only supported in 32bit mode on Windows 7.
- In Release 7.2, Medianet metadata is not supported on the Cisco Video Surveillance Safety and Security Desktop (Cisco SASD) application. Release 7.5 supports Medianet metadata on Cisco SASD clients.

Performance Monitoring and Mediatrace

Cisco Performance Monitoring

Cisco Performance Monitoring is a Medianet feature that measures the performance of RTP, TCP and IP traffic on supported Medianet network devices. Cisco Performance Monitoring allows administrators to collect performance metrics on supported endpoints or intermediate nodes for monitoring video quality conditions.

- In Cisco VSM Release 7.2 and higher, Performance Monitoring information can be collected on Cisco Media Servers, Cisco IP cameras, and all Medianet enabled intermediate nodes in the path (such as routers and switches).

Cisco Mediatrace

Cisco Mediatrace allows administrators to trace the video hop by hop across the network to detect problems along the data path.

- In Cisco VSM Release 7.2 and higher, Mediatrace can be collected between cameras, Cisco Media Servers and all Medianet-enabled intermediary nodes (such as routers and switches) on a hop by hop basis.
- In Cisco VSM Release 7.5 and higher, Mediatrace is also supported on all Cisco VSM ActiveX monitoring clients (including Cisco SASD).

Requirements

Table 25-3 Mediatrace and Performance Monitoring Requirements

Requirements	Complete? (✓)
Enable Medianet metadata on supported devices, including each Cisco Media Server. **Note** Medianet metadata is disabled by default. See the "Medianet Metadata" section on page 25-3.	❑
Enter the Media Services Interface (MSI) password on the Cisco VSM servers. See the "Enabling Performance Monitoring and Mediatrace" section on page 25-7.	❑
Install the LiveAction monitoring application. See the "LiveAction Monitoring Application" section on page 25-7.	❑
A single Ethernet port enabled on the Media Server. Mediatrace and Performance monitoring are not supported on Media Servers with two Ethernet ports enabled.	❑

Enabling Performance Monitoring and Mediatrace

To enable Mediatrace and Performance Monitoring, you must enter the Media Services Interface (MSI) password on each Cisco VSM server (using the browser-based Cisco VSM Operations Manager) and camera (using the camera UI). This same password is used to enable monitoring of the Media Server(s) and camera(s) in the LiveAction monitoring software.

Network Router Usage Notes

- You can also (optionally) enable Mediatrace on the routers that carry the video data, which allows the routers to behave as a Mediatrace responders. Router that do not support Mediatrace are not included in LiveAction data collection and reports.

Procedure

To enable Mediatrace and Performance Monitoring, do the following:

Step 1 Enable metadata on all Media Servers and cameras.

See the "Medianet Metadata" section on page 25-3.

Step 2 Define an MSI password.

The password can be any string defined by the user, and is entered on all servers and camera endpoints that will be monitored, and in the LiveAction monitoring software.

Step 3 Enter the MSI password in the Cisco VSM server configuration page to which the RTP (video stream) flows to:

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

b. Select **System Settings** > **Servers**.

c. Select a server.

d. Enter the MSI **Password** (under the Medianet heading).

Note The MSI username is read-only and cannot be changed.

Step 4 Configure the MSI password on all cameras that support Performance Monitoring and Mediatrace.

- The camera is the device where the RTP (video stream) originates.
- Cameras with a valid password can be added to LiveAction as an MSI endpoint.
- See the camera documentation for instructions to use the device configuration interface.

Step 5 In LiveAction, add the Media Server(s) and camera(s) as MSI endpoints.

The data flows can be tracked and viewed for devices that are added to LiveAction. See https://marketplace.cisco.com/catalog/products/2620 for more information.

LiveAction Monitoring Application

In Cisco VSM Release 7.2 and higher, Mediatrace data can be collected and analyzed using the LiveAction Management Server v3.0.

- For additional LiveAction information, go to: https://marketplace.cisco.com/catalog/products/2620

- For a video summary of LiveAction features, go to: http://www.actionpacked.com/solutions/medianet
- To download LiveAction Management Server v3.0 go to: http://actionpacked.com/download/liveaction/dl-links-v3-0m

Restrictions

- Performance Monitoring is not supported on Cisco VSM clients or Cisco SASD. Mediatrace is not supported between Cisco Media Servers and Cisco VSM clients or Cisco SASD.
- Only UDP based flows are supported in the Cisco Media Servers. UDP is the default setting for Cisco video cameras. There is no metadata support for TCP based flows in this release.
- Mediatrace information may not available using LiveAction when a camera is provisioned in a branch with a Natted IP address. See Understanding Server and Camera Network Configuration, page 7-1 for more information.

Metadata Requirements

Medianet metadata must be supported on all intermediate nodes in the data path, including routers, switches, IP cameras, Cisco Media Servers and monitoring workstations.

In Cisco VSM Release 7.2, Medianet metadata is supported on the following devices:

Table 4 Medianet Metadata Supported Devices

Device	Description	Complete? (✓)
Cisco routers and switches	The Cisco VSM application and attributes (Media Server, endpoints, and clients) are supported on the following: • Cisco Integrated Services Routers (ISR) G2—Cisco IOS version 15.4(1)T • Cisco ASR 1000 Series Aggregation Services Routers (ASR)—Cisco IOS version 15.4(1)S • Cisco Catalyst Series Switches—3000 and 4000 series switches require Cisco IOS version 15.2(2)E • Cisco Catalyst Series Switches—6000 series switches require Cisco IOS version 15.2(1)SY **Note** Prior IOS versions, currently supported metadata values can be viewed and used for classification.	❑
Cisco IP cameras	Camera firmware version 2.0.0-175 or higher is required. See the Release Notes for Cisco Video Surveillance Manager for the cameras that support Medianet features. **Note** Cisco devices must be running the minimum supported firmware version to support Medianet features.	❑

Table 4 Medianet Metadata Supported Devices (continued)

Device	Description	Complete? (✓)
Cisco Media Servers	Metadata is supported on servers running release 7.2 or higher. To enable metadata on a server running the Cisco Media Server service: 1. Log in to the browser-based Cisco VSM Operations Manager. 2. Select **System Settings** > **Servers**. 3. Select a server. 4. Select the **Enable Metadata** checkbox (under the Medianet heading). **Note** Metadata is disabled by default. No user interaction is required for metadata tagging, once enabled.	❑
Workstation clients used to monitor video	Browser-based clients running the Cisco Multi-Pane client software an ActiveX client) with the MSI utility installed. MSI is enabled on the workstation by installing the MSI client software: 1. Log in to the browser-based Cisco VSM Operations Manager. 2. Select the **Operations** tab. 3. Select "**MSI Installation Package**" (under the "Software" heading). 4. Double-click the installer package on your workstation and complete the on-screen instructions. **Notes** • Metadata is supported on Windows 7-based workstations running the 32-bit Cisco Multi-Pane client. • Metadata is not supported on Cisco SASD in Release 7.2. • No user interaction is required for metadata tagging, but the MSI utility must be installed to enable the feature. **Related documentation:** • See Client Workstation Restrictions, page 25-6. • Cisco Video Surveillance Operations Manager Mobile App User Guide • See the Cisco Video Surveillance Monitoring Workstation Performance Baseline Specification for more information about the Cisco Multi-Pane client software.	❑

Discovering Medianet Cameras on the Network

Network cameras that support Medianet can be automatically discovered when they are added to the network, and (optionally) configured for use with Cisco VSM.

See the following for more information:

Discovering Cameras on the Network, page 10-23	Includes descriptions and instructions about camera discovery and auto-configuration.
Discovering Medianet-Enabled Cameras, page 10-32	Includes requirements and configuration instructions.

Upgrading System and Device Software

Refer to the following topics to upgrade the Cisco Video Surveillance system software, the driver packs that enable camera and encoder models, and the device firmware for those devices.

Tip See Language Settings, page 20-4 to manage the language packs on servers in your deployment.

Understanding Cisco Video Surveillance Software

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

Table 26-1 Cisco Video Surveillance Software Types

Software Type	Description
System software	*System Software* is the Cisco VSM server software that includes services for the Media Server, Operations Manager, Management Console and monitoring clients (such as the Cisco Video Surveillance Safety and Security Desktop client). Use the Operations Manager to update the *System Software* on all servers (such as Media Servers) associated with the Operations Manager. **Notes:** • The Operations Manager and all associated servers must run the same system software version. • To update a Federator server, log in to the Federator server Management Console and use the **Server Upgrade** feature. See the "Updating the Federator Server System Software" section on page 22-42. • To repair or restore the Cisco VSM system software, see the Cisco Video Surveillance Manager Recovery Guide for your hardware platform. For VM installations, see the Cisco Video Surveillance Virtual Machine Deployment and Recovery Guide for UCS Platforms).
OVA image (for VM installations)	OVF template files are used to install the server software as a virtual machine (VM) on a supported Cisco Unified Computing System (UCS) platform. • OVA template files are downloaded from the Cisco website. • The file format is .ova. For example: `Cisco_VSM-7.2.0-331d_ucs-bc.ova` • 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	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: • 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. see the Cisco Video Surveillance Manager Recovery Guide for your hardware platform for more information.
Device *firmware*	Device *firmware* 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 26-19). Firmware for other manufacturers is upgraded using a direct connection (refer to the device documentation).

Table 26-1 Cisco Video Surveillance Software Types (continued)

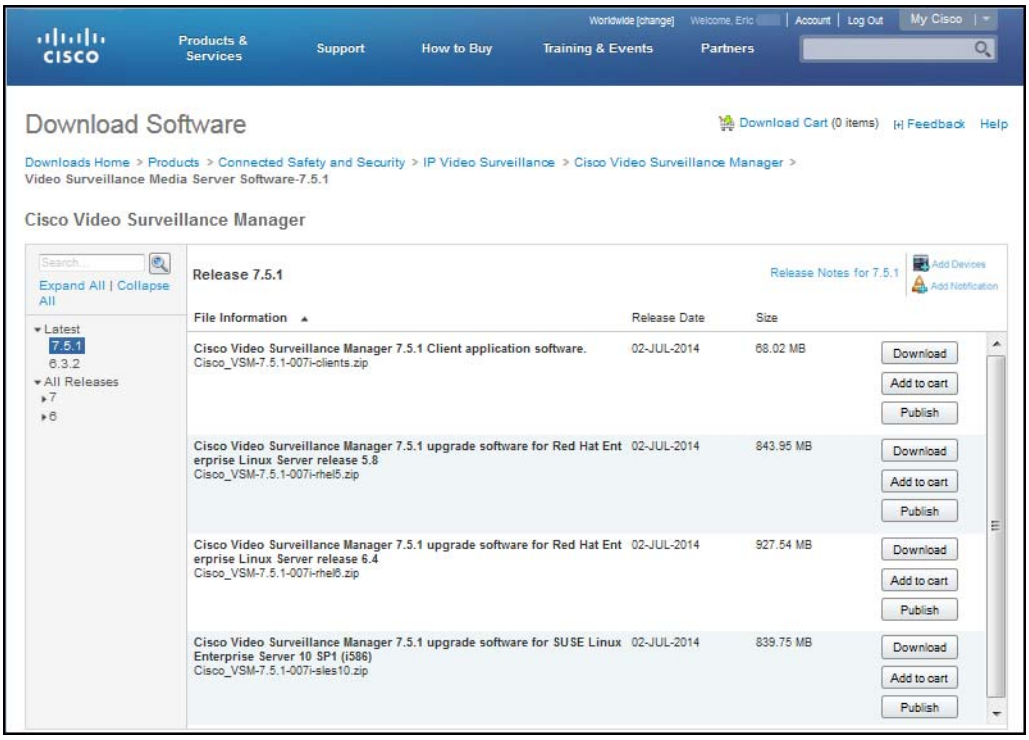
Software Type	Description
Device *driver packs*	Device *driver packs* are the software packages used by Media Server and Operations Manager to interoperate with video devices, such as cameras. Driver packs are included with the Cisco VSM software, or may be added to a server at a later time to add support for new devices or features. • 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 26-16 for instructions. **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. • *Driver pack* versions must be the same on the servers that host the Media Server and Operations Manager or a *driver pack mismatch* error. Templates cannot be revised when a *driver pack mismatch* error is present.
Language Packs	Language packs can be added to display the VSM user interfaces in non-English languages. Language packs are added using the Operations Manager. See Language Settings, page 20-4.

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 7.6.

Downloading Software, Firmware and Driver Packs from cisco.com

Additional system, firmware and driver software can be downloaded from cisco.com (Figure 26-1).

Figure 26-1 Downloading Cisco Video Surveillance Software



Procedure

Step 1 Go to the Cisco Video Surveillance Manager product page.

Step 2 Click Download Software.

Step 3 Select a product category. For example:

- **Video Surveillance Device Driver**
- **Video Surveillance Manager Stand-alone Tools**
- **Video Surveillance Media Server Software** (including system software)

Step 4 Select the release (Figure 26-1).

Step 5 Click **Download** or **Add to Cart** and follow the onscreen instructions.

Upgrading System Software

Use the Software Management feature to update the system software on all servers, including the Operations Manager server and any additional servers (such as Media Servers or Metadata servers). See Understanding Cisco Video Surveillance Software, page 26-2 for more information.

Note Software Management is supported in Cisco VSM release 7.5 and higher.

Contents

Refer to the following topics for more information:

Related Information

- Understanding Cisco Video Surveillance Software, page 26-2
- Configuring Servers, page 6-1

Overview

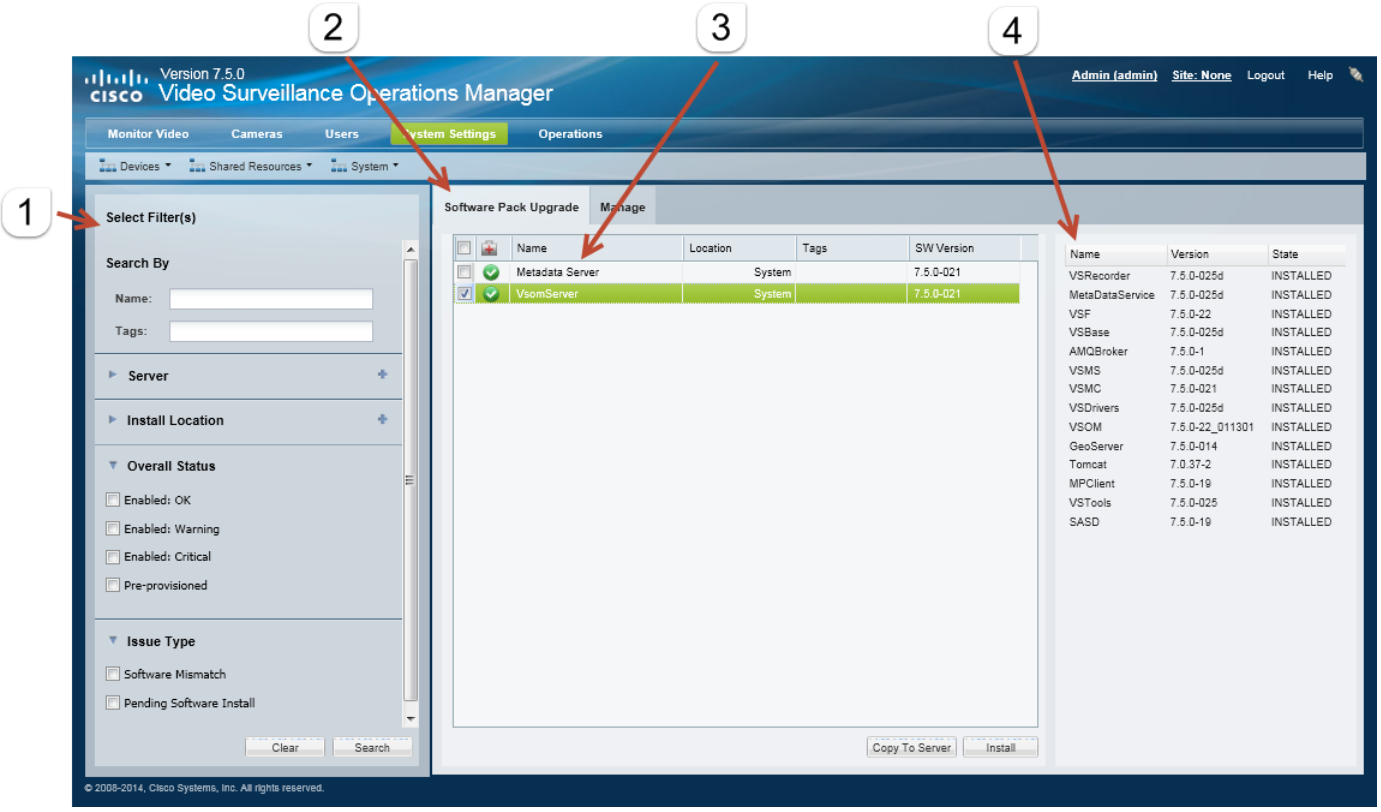
To upgrade the servers in your deployment, upload the software upgrade image to the Operations Manager, and then copy that software to the other servers that are managed by the Operations Manager. You can upload a single image for each operating system (OS), such as Red Hat or SUSE, but all servers must be upgraded to the same Cisco VSM release.

After the software upgrade image is uploaded, install in first on the Operations Manager server, and then on the additional servers as described in Server Upgrade Sequence, page 26-7.

Note The Software Management feature is supported in Cisco VSM release 7.5 and higher.

Figure 26-2 describes the main elements used to manage system software. See the "System Software Upgrade Procedure" section on page 26-8 for more detailed instructions.

Figure 26-2 Software Management



1	Filters used to narrow the displayed servers. Select the filers and click **Search**. Leave all fields blank to find all servers.
2	• **Manage**—Used to upload the new software upgrade `.zip` package to the Operations Manager server. • **Software Pack Upgrade**—Displays the servers discovered when you click **Search** (use filters to narrow the results). – Click **Copy To Server** to copy new software files from the Operations Manager server to the selected servers. You can copy the upgrade package to the servers before upgrading. – Click **Install** to install the software on the selected servers. **Tip** See the "System Software Upgrade Procedure" section on page 26-8 for more information.
3	The servers included in the search.
3	The software packages installed on the selected server. **Note** All required packages are included in the system software `.zip` installation file. The packages cannot be installed individually.

Server Upgrade Sequence

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

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

Tip See the "Understanding Server Services" section on page 6-3 for more information on the server services supported in this release.

Usage Notes

- The Operations Manager and all associated servers must run the same system software version.
- The Operations Manager server must be in maintenance mode to perform the update (click the pencil icon in the title bar to turn maintenance mode on or off). The icon is grey when maintenance mode is on, meaning most user configuration will be rejected (only system tasks and logging are allowed). See Understanding Maintenance Mode, page 1-31 for more information.
- The SLES10, RHEL5, and RHEL6 operating systems (OS) are supported in this release. You must obtain and upload the correct software image for the OS running on each of the servers in your deployment. For example, if the Operations Manager server is running SLES10, but the Maps Server is running RHEL5, you must obtain and upload both files. When the files are copied from the Operations Manager to the server, the server OS is detected and the appropriate software image is transferred (as long as it is available on the Operations Manager).
- Only one software file per OS can be present on the server. If a new software file is uploaded, then the old file for that OS is deleted.
- To update a Federator server, log in to the Federator server Management Console and use the **Server Upgrade** feature. See the "Updating the Federator Server System Software" section on page 22-42.
- To repair or restore the Cisco VSM system software, see the Cisco Video Surveillance Manager Recovery Guide for your hardware platform. For VM installations, see the Cisco Video Surveillance Virtual Machine Deployment and Recovery Guide for UCS Platforms).Upgrading the server software may also require camera or encoder firmware upgrades. Failure to upgrade device firmware can cause camera failure after the server upgrade is complete.
  - See the Release Notes for Cisco Video Surveillance Manager for information on the supported firmware versions.

  - See the "Upgrading Cisco Camera and Encoder Firmware" section on page 26-19 instructions to upgrade Cisco device firmware.
- In rare scenarios, a PC workstation firewall can cause the upgrade process to fail. If this occurs, temporarily disable the workstation firewall software until the upgrade is complete.
- The server upgrade process automatically restarts server services.
- Installation is supported only if the RAID is in a non-bad, non-failed state.
- See Language Settings, page 20-4 to manage the language packs on servers in your deployment.

System Software Upgrade Procedure

Use the following procedure to upgrade all of the servers in a deployment to the same Cisco Video Surveillance Manager release. See Server Upgrade Sequence, page 26-7 for the order in which the upgrade should be performed (by server type).

You can upload the server software to all servers before performing the upgrade.

Procedure

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

- For example, navigate to the Video Surveillance Media Server Software section from the Cisco Video Surveillance Manager download page.
- You must obtain and upload the correct software image for the OS running on each of the servers in your deployment. See the "Usage Notes" section on page 26-7 for more information.
- See the "Downloading Software, Firmware and Driver Packs from cisco.com" section on page 26-4 for information on downloading software.

Step 2 Log in to the Cisco VSM Operations Manager.

- You must belong to a User Group with manage permissions for *Servers and Encoders*. See the "Understanding Permissions" section on page 4-4.

Step 3 Click the pencil icon in the title bar to place the server in maintenance mode .

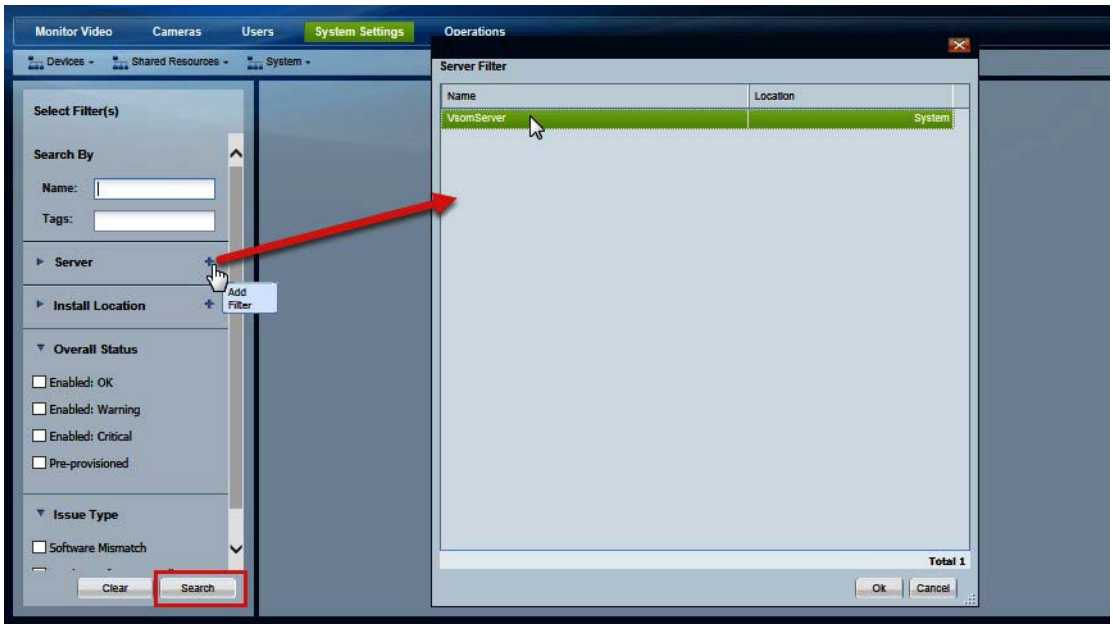
- The icon is grey when maintenance mode is on, meaning most user configuration will be rejected (only system tasks and logging are allowed).
- Maintenance mode locks the server configuration so configuration changes cannot be made by other users. This keeps the server config in a stable state while the device is added to the HA config. See Understanding Maintenance Mode, page 1-31 for more information.

Step 4 Upload the new software file(s) to the Operations Manager server.

Only one software file for each server operating system (OS) can be present on the server. If a new software file is uploaded, then the old file for that OS is deleted. See the "Usage Notes" section on page 26-7 for more information.

a. Select **System Settings > Software Management**. (Figure 26-3).

Figure 26-3 Display the Server to Upgrade

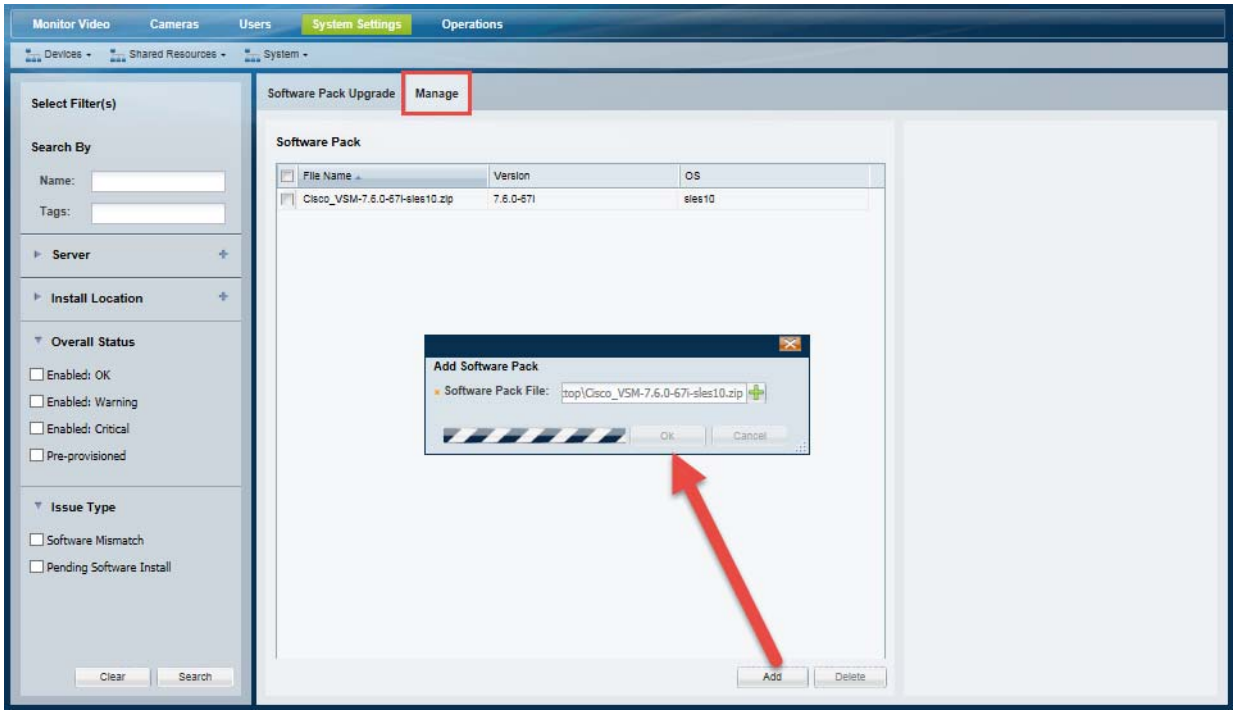


b. (Optional) Select the search filter(s), such as location or status.

c. Click **Search** to display the list of servers according to the filters. All servers are displayed if no filters are selected.

d. Select the **Manage** tab (Figure 26-4). The **Manage** tab appears only after a server is selected.

Figure 26-4 Display the Server to Upgrade



e. Click **Add**.

f. In the pop-up window, click and select a valid `.zip` software pack file from a local or network disk. For example: `Cisco_VSM-7.6.0-1-sles10.zip`

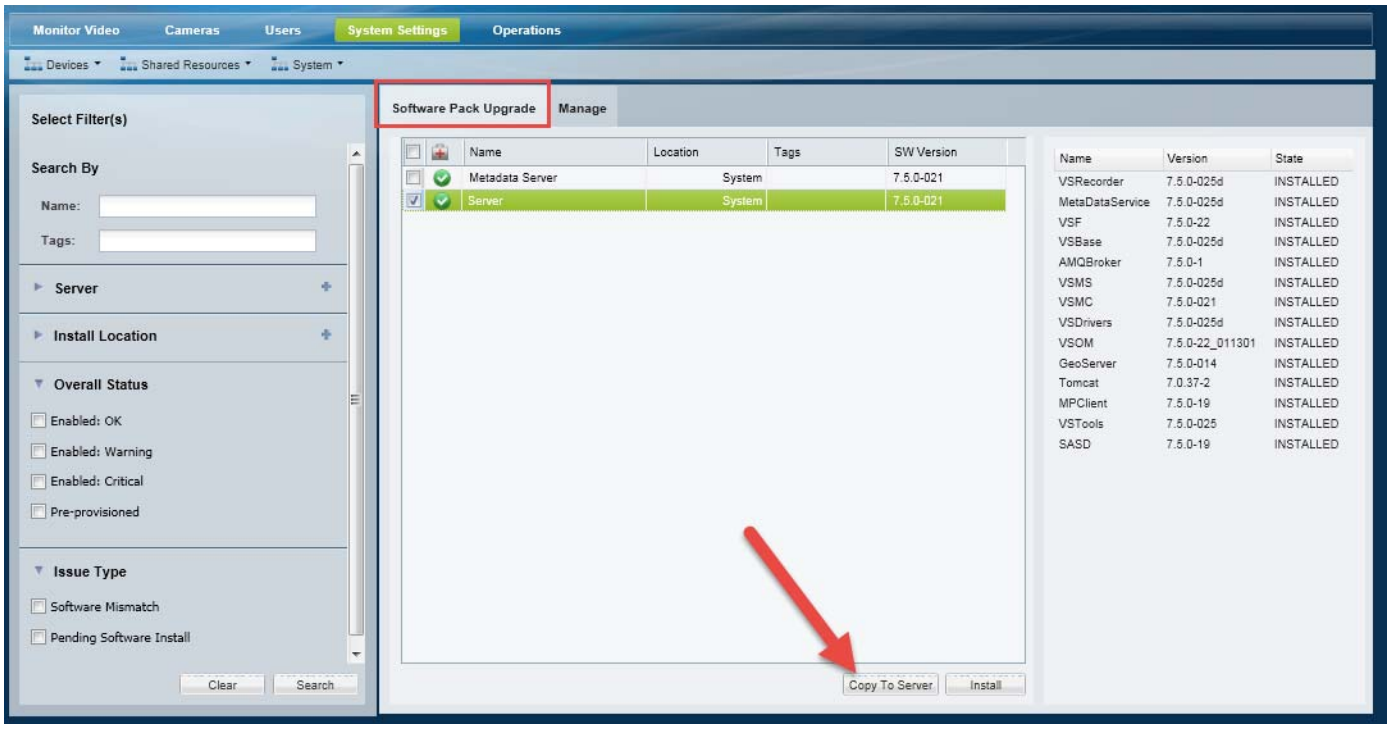
g. Click **OK**.

h. Wait for the software file to upload to the Operations Manager server. The filename will be displayed in the Software Pack list (Figure 26-4).

Step 5 Copy the upgrade software to the other servers that are managed by the Operations Manager (Figure 26-5).

Copying the software files to the other servers allows those servers to be upgraded. You can copy the software to the servers without installing it. This allows you to stage the software on all of the servers before performing the upgrade.

Figure 26-5 Copy the Software to the Additional Servers



a. Select the **Software Pack Upgrade** tab.

b. Make sure that maintenance mode is on (the icon is grey when maintenance mode is on).

c. (Optional) Use the filters to narrow the list of servers.

d. Click **Search** to display the list of servers according to the filters. All servers are displayed if no filters are selected.

e. Click **Copy To Server** (Figure 26-5) to copy the new server software from the Operations Manager server to the selected server(s).

f. Wait for the file copy job to complete.

Step 6 Install the new software on the Operations Manager server.

Upgrade the Operations Manager before updating the other servers. See Server Upgrade Sequence, page 26-7.

a. Verify that the correct software file for the Operations Manager OS is uploaded (see "Usage Notes") and that maintenance mode is on (the icon is grey).

b. Select the Operations Manager server from the **Software Pack Upgrade** tab.

For example: `VsomServer`.

c. Click **Install** to install the system software package that was copied to the server.

d. Wait for a series of status messages to appear while the status server is prepared and the upgrade package is extracted and verified.

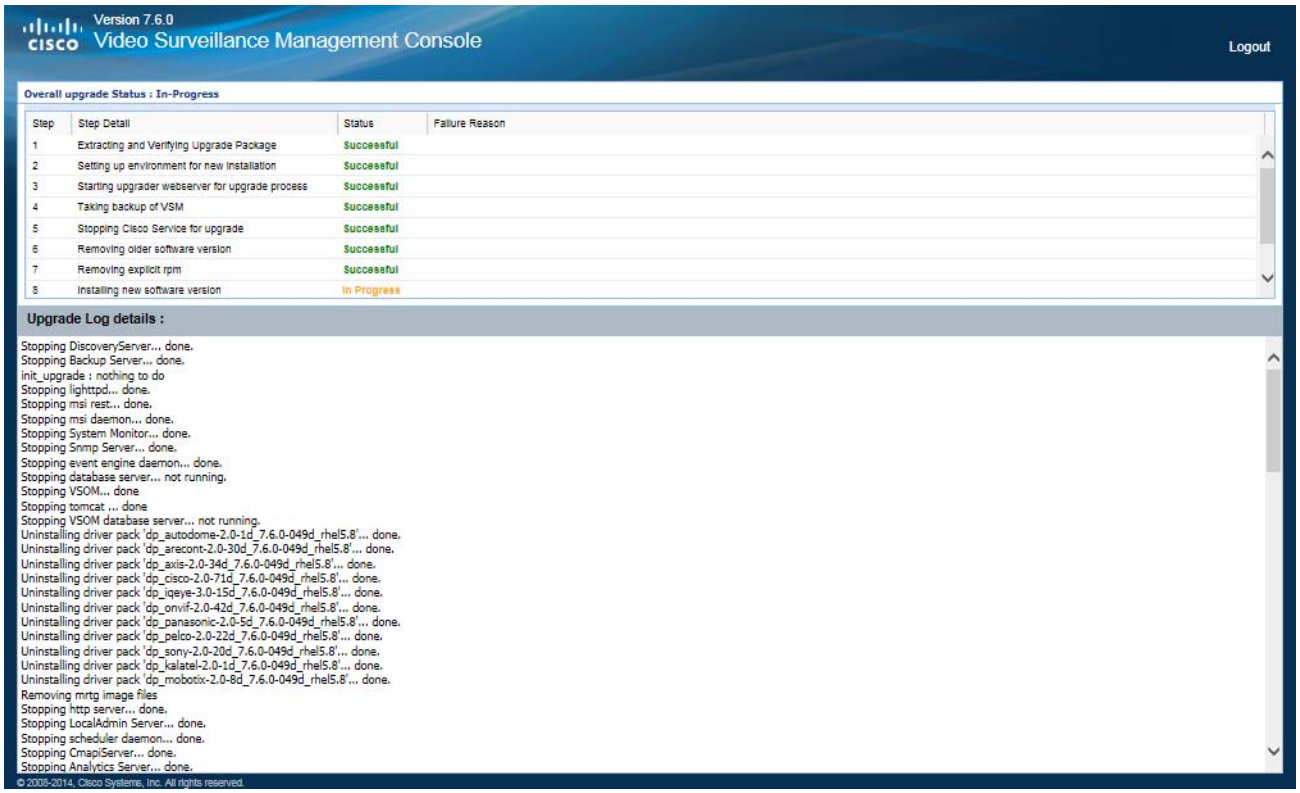
This can take a few minutes.

e. (Optional) Re-login, when instructed, using the localadmin username and password (the credentials used for the Cisco VSM Management Console) to view the Operations Manager upgrade status.

- Click **OK** when prompted to log in.
- Enter the password for the localadmin username.
- View the Operations Manager upgrade status (Figure 26-6).

Note The status window in Figure 26-6 appears only for the Operations Manager server. To view the upgrade status of additional servers, log in to the Operations Manager and open the server configuration page. Select **Status** > **Service Jobs** and select **Upgrade Server** from the menu (Figure 26-8).

Figure 26-6 Server Upgrade Status



f. Wait for the operation to complete and the server to restart. This can take up to 90 minutes (or less) depending on the server load.

g. Re-login to the Operations Manager, when instructed (you may need to refresh the browser to display the Operations Manager login page).

h. Continue to Step 7 to upgrade each additional server to the same version that is running on the Operations Manager.

Note If the upgrade fails, see the "Recovering From a Failed Upgrade" section on page 26-14.

Step 7 Install the new software on the additional servers that are managed by the Operations Manager (Figure 26-7).

a. Re-login to the Operations Manager (you may need to refresh the browser to display the Operations Manager login page).

b. Make sure that maintenance mode is on (the icon is grey when maintenance mode is on).

c. Verify that the software upgrade file was copied from the Operations Manager to the servers that will be upgraded, as described in Step 5.

d. Select **System Settings** > **Software Management**.

e. Select the **Software Pack Upgrade** tab.

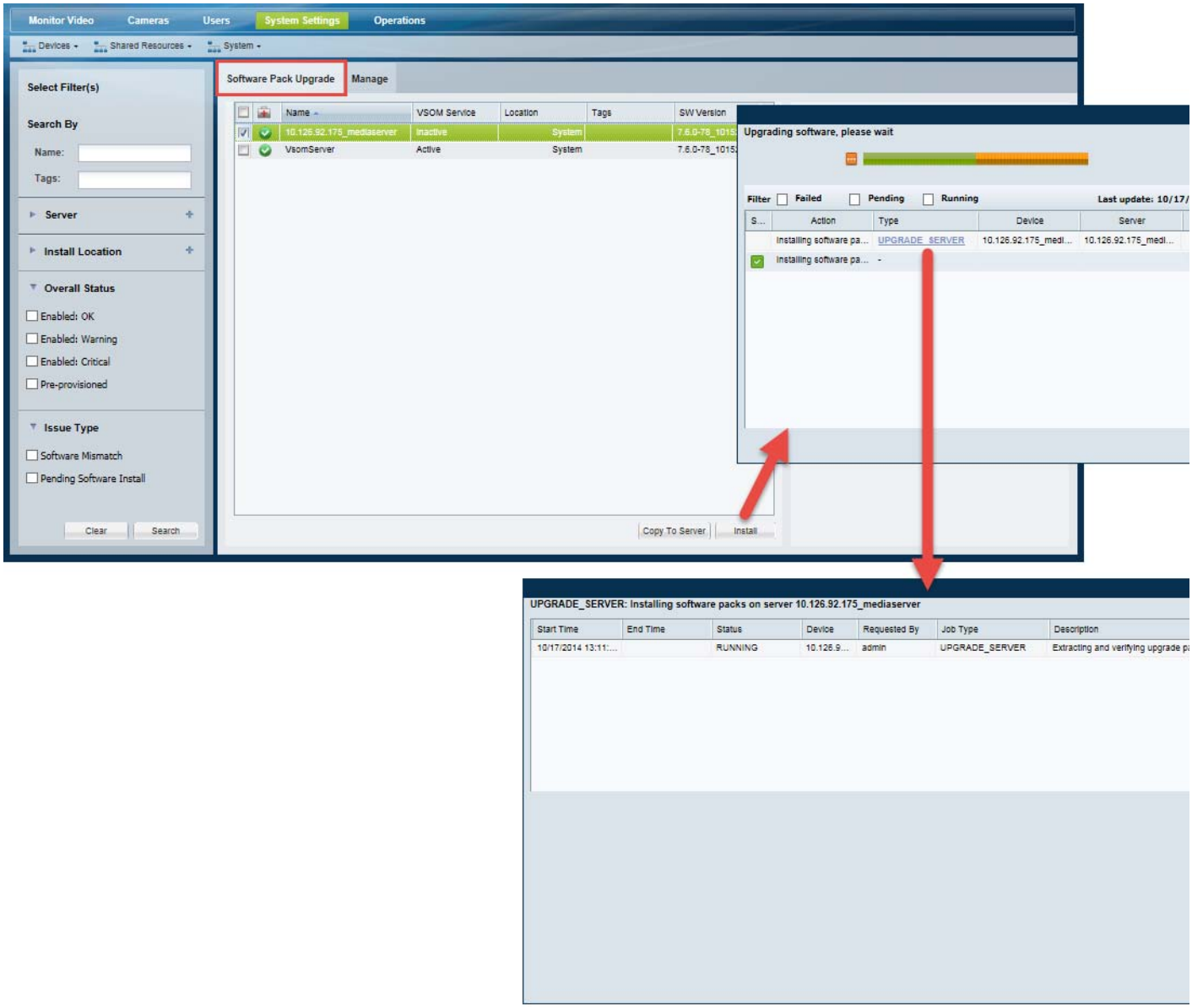
f. (Optional) Use the filters to narrow the list of servers.

g. Click **Search** to display the list of servers according to the filters. All servers are displayed if no filters are selected.

h. Select one or more servers from the list.

i. Click **Install** to install the system software package (Figure 26-7).

Figure 26-7 Upgrading Additional Servers



j. (Optional) In the Job window pop up window, click the “UPGRADE SERVER” link to view the job details.

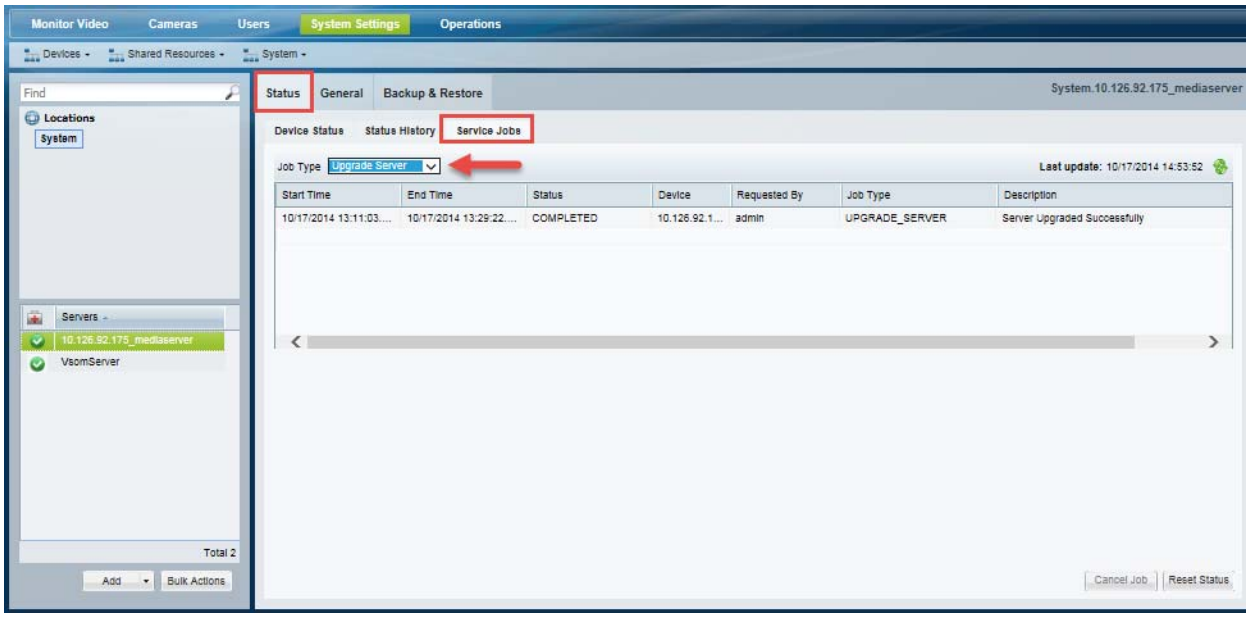
k. Wait for up to 90 minutes for the upgrade job to complete and the server(s) to restart.

l. (Optional) View the upgrade job details (Figure 26-8):

- Go to **Devices** > **Servers** and select the server.
- Select the **Status** tab.
- Select the **Service Jobs** tab.

– Select the **Upgrade server** job type.

Figure 26-8 Server Upgrade Status



Note If the upgrade fails, see the "Recovering From a Failed Upgrade" section on page 26-14.

Recovering From a Failed Upgrade

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

To address this issue, do the following:

Procedure

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

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

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

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

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

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

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

Step 3 Repeat the System Software Upgrade Procedure, page 26-8.

Deleting a Software Pack File

To delete a software pack that was copied to the Operations Manager server, do the following:

Step 1 Select **System Settings** > **Software Management**. (Figure 26-2).

Step 2 Select the **Manage** tab.

Step 3 Select a software pack file name.

Step 4 Click **Delete**.

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 26-16
- Overview, page 26-17
- Driver Pack Upgrade Procedure, page 26-17

Tip See the "Understanding Cisco Video Surveillance Software" section on page 26-2 for descriptions of the different software types.

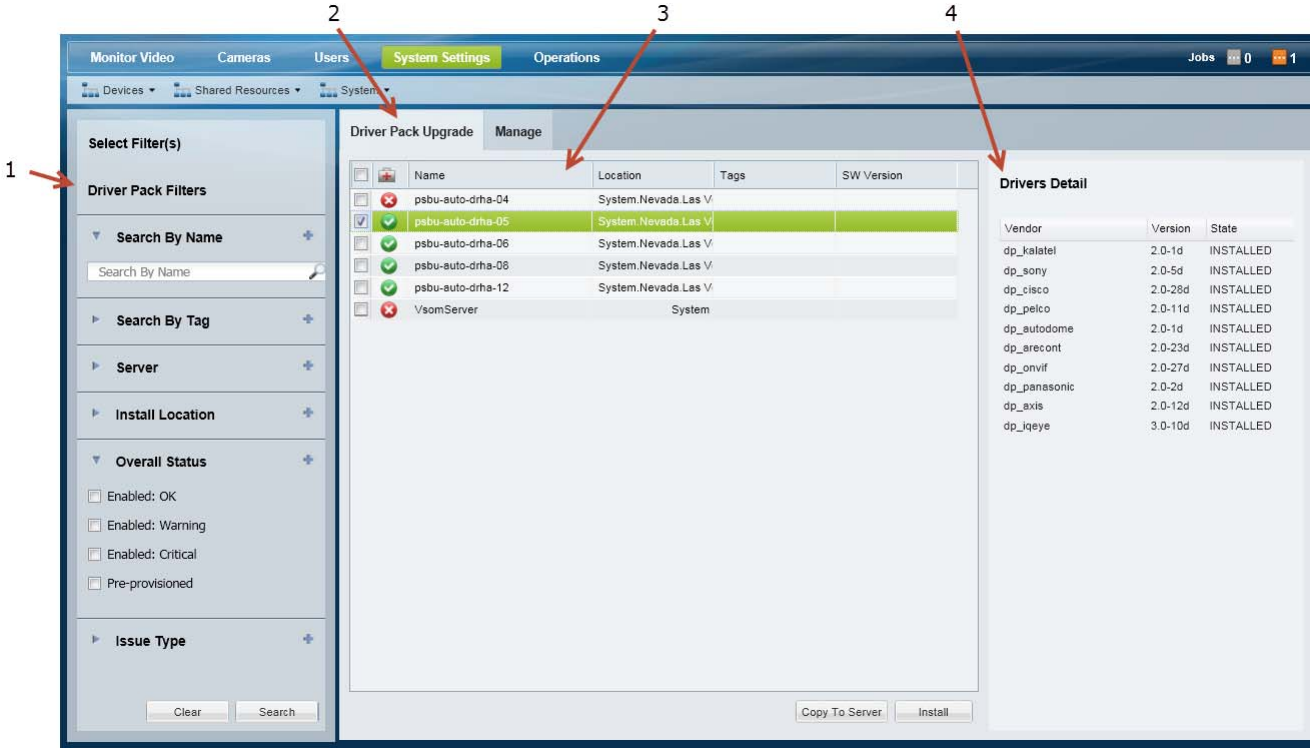
Usage Notes

- 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 7.6 for information on the supported driver packs.
- Driver packs can only be upgraded. They cannot be downgraded.

Overview

Figure 26-9 describes the main elements used to manage driver pack software. See the "Driver Pack Upgrade Procedure" section on page 26-17 for more information.

Figure 26-9 Manage Drivers



1	Filters used to narrow the displayed servers. Select the filers and click **Search**. Leave all fields blank to find all servers.
2	• **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). – 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. **Tip** See the "Driver Pack Upgrade Procedure" section on page 26-17 for more information.
3	The servers included in the search.
3	The driver packs installed for the selected server.

Driver Pack 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 7.6 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**.

Step 2 Select **System Settings > Driver Pack Management**. (Figure 26-9).

Step 3 Display the servers to be upgraded.

a. (Optional) Select the filter(s) to display specific servers.

Tip All servers are displayed if no filters are selected.

b. Click **Search** to display the list of servers according to the filters.

c. 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.

a. Select the **Manage** tab (Figure 26-9).

b. Click **Add**.

c. 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`

d. Click **OK**.

e. 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.

a. Select the **Driver Pack Upgrade** tab (Figure 26-9).

b. Select one or more servers.

c. Click **Copy To Server**.

a. 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.

a. Select one or more servers from the **Driver Pack Upgrade** tab.

b. 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.

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:

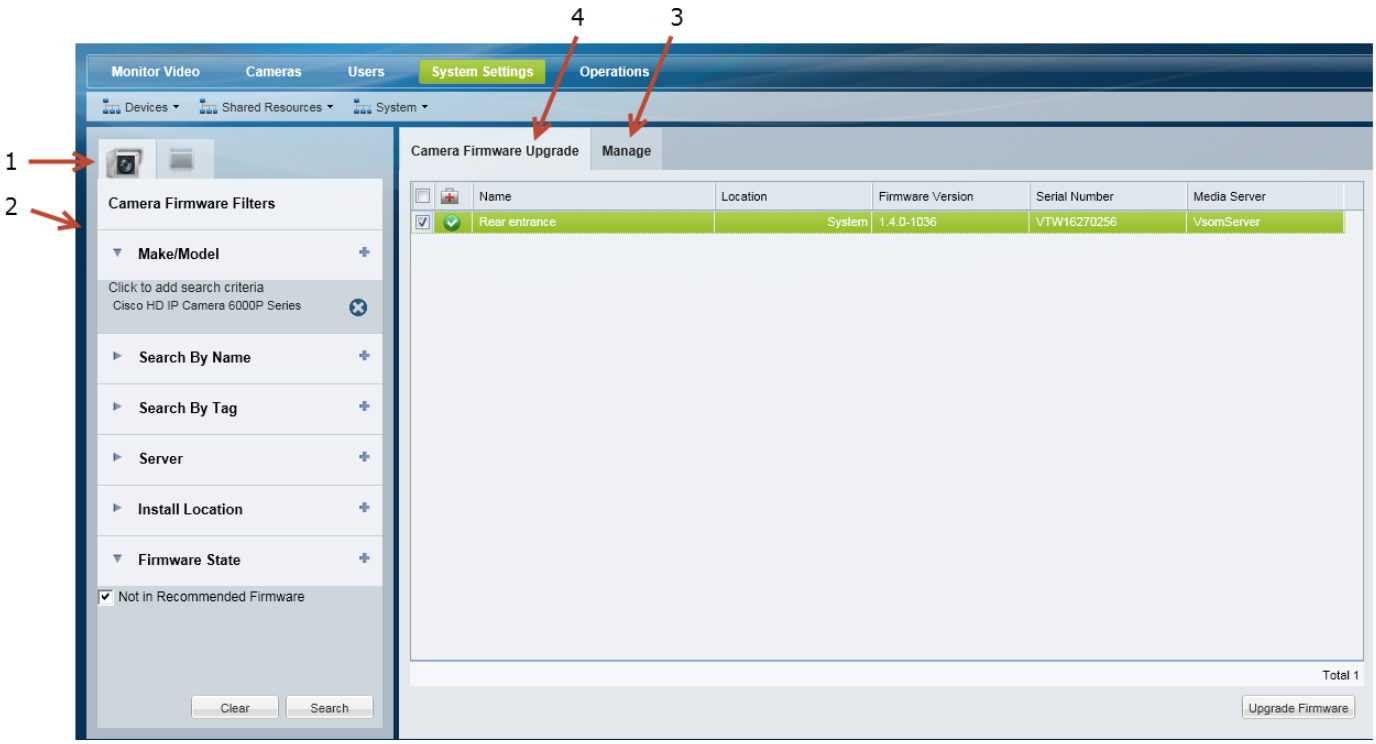
- Firmware Management Overview, page 26-20
- Usage Notes, page 26-20
- Before You Begin, page 26-21
- Firmware Management Procedure, page 26-21

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 26-11 describes the main elements used to manage firmware. See the "Firmware Management Procedure" section on page 26-21 for more information.

Figure 26-10 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 them 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 26-2 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 and upgrade the drivers (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 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 26-4.
- To obtain firmware for non-Cisco products, go to the product website or contact your sales representative.
- Verify that the firmware version is supported for your Cisco Video Surveillance Manager version. See the Release Notes for Cisco Video Surveillance Manager.

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 26-4.
- 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 26-10 on page 26-20).

Step 4 Use the filters to select camera (Figure 26-10).

a. Select a Make/Model from the Filters to enable the other fields and the **Search** button

b. Expand the **Make/Model**.

c. Click the entry field.

d. Select the camera model from the pop-up list.

e. Select additional filter criteria, if necessary.

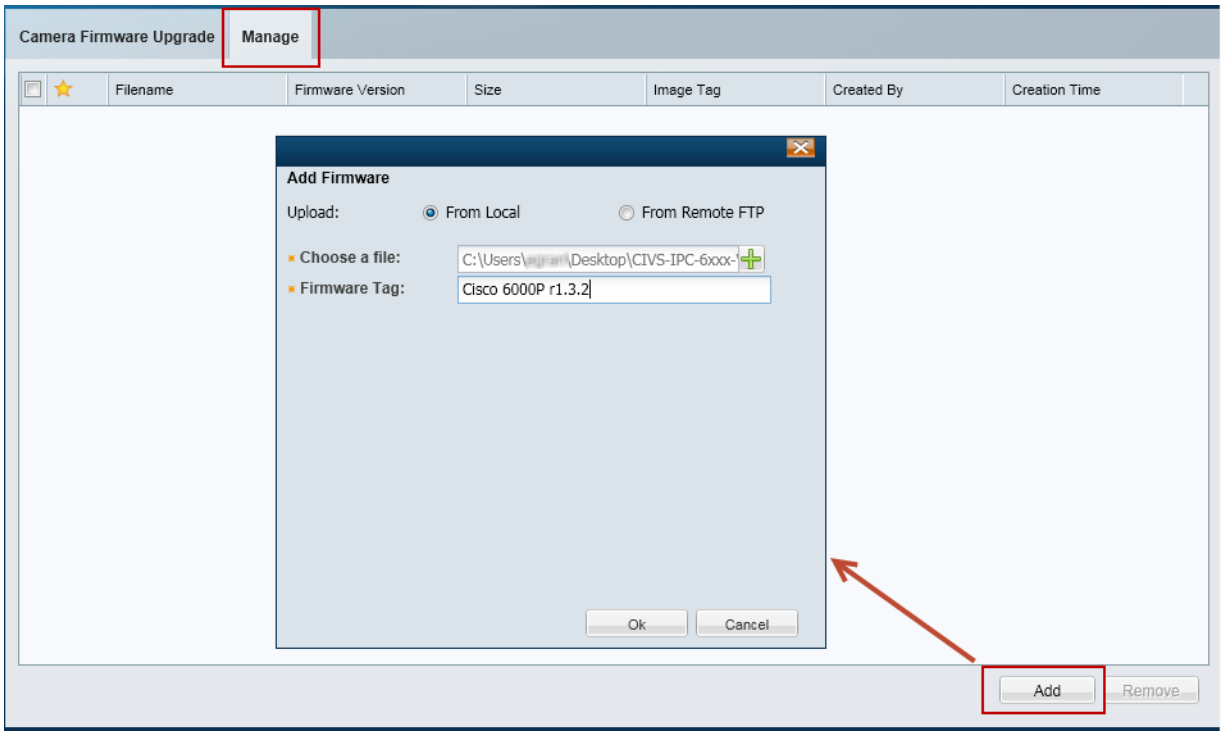
f. Click **Search**.

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 26-11):

Figure 26-11 Adding Firmware Images



a. Select the **Manage** tab.

b. Click **Add**.

c. Select **From Local** or **From Remote FTP**.

d. Click ✚ to select the location of the firmware file, or enter the FTP connection details.

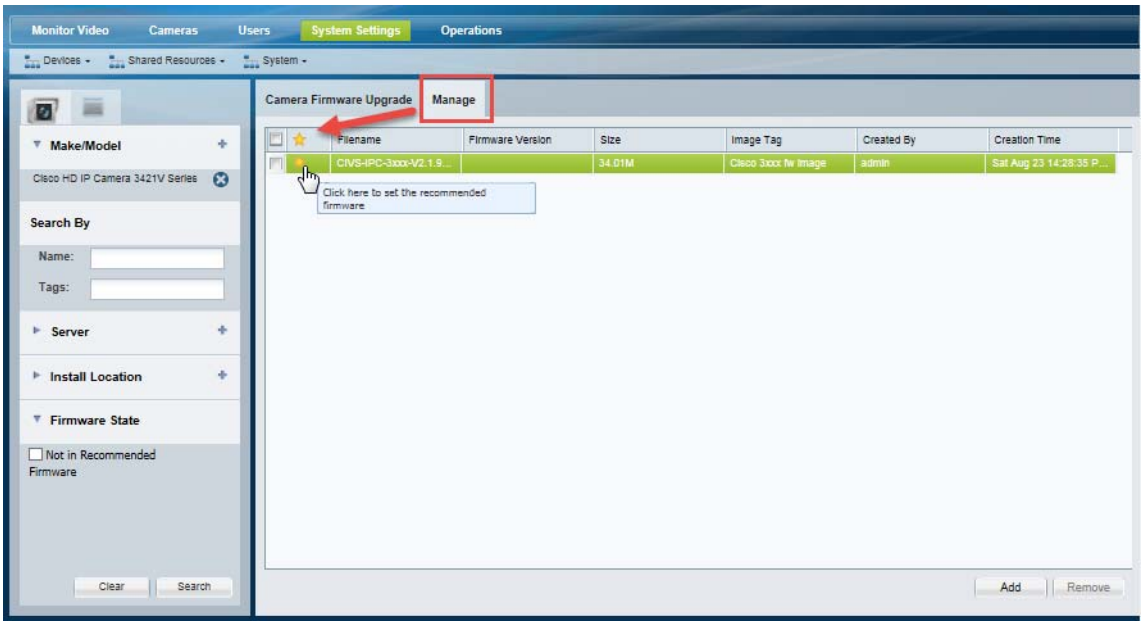
e. Enter a firmware tag that includes the firmware device model.

f. Click **OK**.

g. Wait for the file to upload and click **OK** when the success message appears.

Step 7 In the firmware list, select the star next to a firmware image that is the recommended version for the device model. This firmware image will be used in the upgrade/downgrade (Figure 26-12).

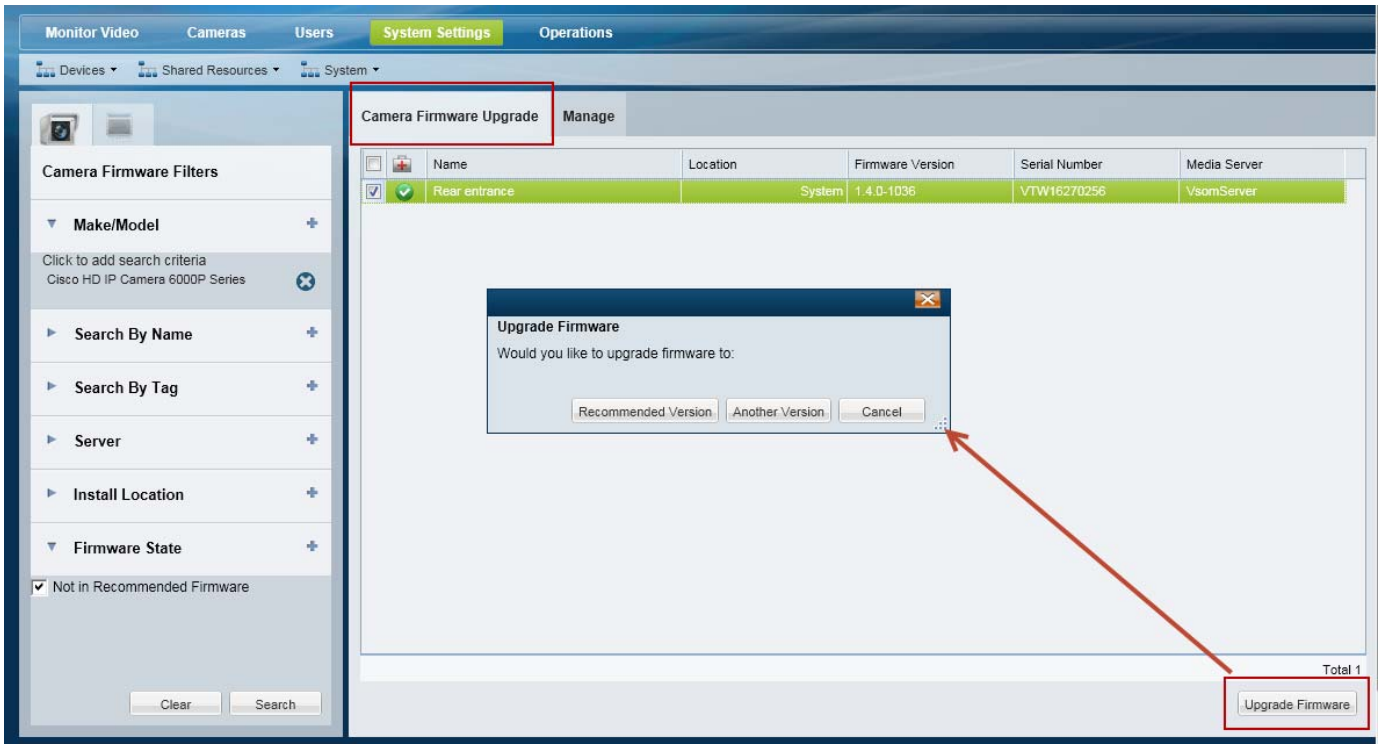
Figure 26-12 Adding Firmware Images



Note The Firmware version column is only displayed after the firmware has been applied to a set of devices.

Step 8 Upgrade the device firmware (Figure 26-13):

Figure 26-13 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** tab (or **Encoder Firmware Upgrade** tab).

b. Select the devices to be upgraded.

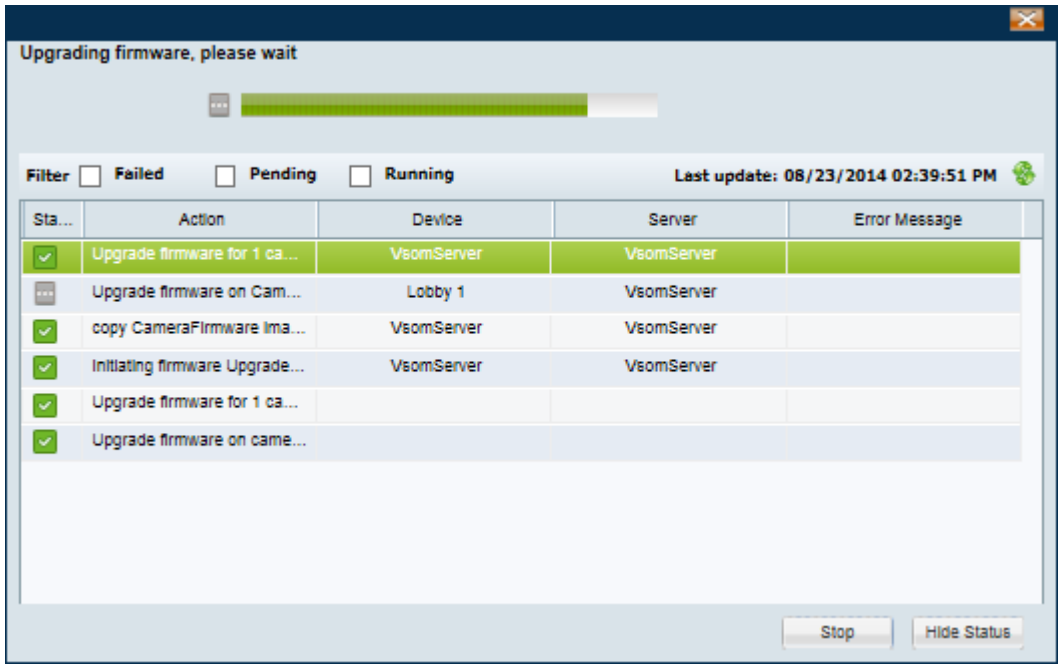
c. Click **Upgrade Firmware**.

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 9 Wait for the upgrade job to complete (Figure 26-14). See the "Usage Notes" section on page 26-20 if the upgrade is not successful.

Figure 26-14 Upgrading Job Status



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.

Downloading Utilities and Documentation

Refer to the following topics to download additional software tools and updates.

Downloading Cisco SASD and the Cisco Review Player

The following tools can also be used to monitor video.

To download these installation files, you must belong to a user group with *Download Software* permission. See the "Adding Users, User Groups, and Permissions" section on page 4-1 for more information.

Table B-1 Cisco Video Viewing Applications for Download from the Operations Manager

Application	Description	Documentation
Cisco SASD Advanced Video Player (Cisco SASD)	Desktop monitoring application that provides greater flexibility to monitor multiple cameras, and view alerts.	Cisco Video Surveillance Safety and Security Desktop User Guide Cisco SASD Advanced Video Player 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 Pofiler Tool for instructions to download, install, and use this tool.

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.

Revision History

Table C-1 Revision History

Release	Date	Change Summary
Release 7.6	December, 2014	**New Features and Content** • Configuring a PTZ "Return to Home" Countdown, page 10-79. See also Using Pan, Tilt, and Zoom (PTZ) Controls, page 2-38 • Understanding Server and Camera Network Configuration, page 7-1 • Adding Cameras From Different Networks (NATs), page 7-10 • Understanding NTP Configuration, page 8-1 • Managing Camera Apps, page 14-1 • Operations Manager High Availability, page 18-1 • Custom Data Management, page 19-36 • Active Users, page 20-3 **Revised Features and Content** • Using the Privacy Mask, page 2-30—revisions to the icon purpose. • Viewing Media Server Status, page 9-9 • Camera Status, page 10-62 • Backup and Restore, page 21-1 • Configuring Location Maps, page 24-1 • Upgrading System Software, page 26-5

Table C-1 Revision History (continued)

Release	Date	Change Summary
Release 7.5	February, 2014	The following major changes were made to the document in this release: Added the following sections: • Backing Up Multiple Servers (Bulk Actions), page 21-13 • Connected Edge Storage (Camera Recording), page 15-1 • Understanding and Changing Your "Site", page 1-24 • Understanding Dual Login, page 1-20 • Using Dynamic Proxy to Monitor Video From Remote Sites, page 23-1 • Using Federator to Monitor Multiple Operations Managers, page 22-1 • Configuring Location Maps, page 24-1 • Understanding Server Services, page 6-3 • Configuring Medianet, page 25-1 • Using the Privacy Mask, page 2-30 • Enabling Video Analytics, page 13-2 Revised the following information: • Using Advanced Events to Trigger Actions, page 13-7 ("Camera App" support) • Backing Up and Restoring a Single Server, page 21-8 • Camera Status, page 10-62 • Replacing a Camera, page 10-88 • Encoder Status, page 16-14 • Logging In and Managing Passwords, page 1-18 • Health Dashboard: Device Health Faults on an Operations Manager, page 19-6 • Installing Licenses, page 1-26 • Configuring Servers, page 6-1 • Upgrading System Software, page 26-5 • Understanding Permissions, page 4-4 (new permissions for Metadata and Privacy Mask) • Creating and Viewing Video Clips, page 2-16 • Clip Search, page 2-49 Other minor revisions, updates and edits.

Table C-1 Revision History (continued)

Release	Date	Change Summary
Release 7.2	August, 2013	• Servers are now configured separately from the services that run on them – Configuring Servers, page 6-1 – Configuring Media Server Services, page 9-1 – Operations Manager Advanced Settings, page 6-32 • Revised the "High Availability: Cisco Media Servers" section on page 17-1 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 6-16. • Revised "Backup and Restore" section on page 21-1. • Added the "Understanding Events and Alerts" section on page 19-2. • Added "Issues" tab and other revisions to Health Dashboard: Device Health Faults on an Operations Manager, page 19-6. • Added the "Installing and Upgrading Driver Packs" section on page 26-16. • Multicast server address and port number can now be defined when the camera is added, or using the camera configuration page. See the following: – Configuring Multicast Video Streaming, page 12-11 – Manually Adding a Single Camera, page 10-11 – General Settings, page 10-44 • Added the ability to define a default *View* 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 3-1 • Additional filters and revised process added to the "Upgrading Cisco Camera and Encoder Firmware" section on page 26-19. • 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 Downloading Utilities and Documentation, page B-1. • Other minor revisions, updates and edits.

Table C-1 Revision History (continued)

Release	Date	Change Summary
Release 7.0.1	February, 2013	Maintenance Update, including various bug fixes and edits. New and revised features including the following: • 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 7.6 for more information.
Release 7.0.0	October, 2012	Initial draft. See the Release Notes for Cisco Video Surveillance Manager for more information.