Cisco Video Surveillance Manager User Guide, Release 6.3.2

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

Text Part Number: OL-23994-01

Cisco Video Surveillance Manager User Guide, Release 6.3.2

CONTENTS

Preface

Overview

This document, *Cisco Video Surveillance Manager User Guide, Release 6.3.2.*, provides an overview of Cisco Video Surveillance Manager (VSM) Release 6.3.2, describes basic procedure that should be performed when you first start to use the system, and provides detailed information about using the Cisco Video Surveillance Operations Manager (VSOM) and the Cisco Video Surveillance Management Console. It also describes various strategies for configuring VSM software and provides steps for performing a basic VSM setup.

Organization

This manual is organized as follows:

Chapter 1, “Overview”	Describes how to use this manual, provides an overview of VSM, describes basic procedures to perform, and explains various configuration strategies
Part 1, Basic Setup	
Chapter 2, “Performing a Basic Setup of VSM”	Provides instructions for performing the setup of a basic VSM system
Part 2, Administrator Reference	
Chapter 3, “Managing Devices”	Describes how to use the VSOM Device area to set up your video surveillance network and equipment
Chapter 5, “Managing Video Feeds”	Describes how to use the VSOM Video Feeds area set up and manage camera groups and feeds, import camera configurations into VSOM using batch administration, and set up archives and predefined views
Chapter 7, “Managing Accounts”	Describes how to set and manage user roles and accounts
Chapter 6, “System Management”	Describes how to manage events and schedules, generate reports, manage system settings, and view a snapshot of overall system operation

Chapter 4, “Utilities”	Explains utilities that you can use to aid with system management
Part 3, Operator Reference	
Chapter 8, “Using the VSOM Operator Pages”	Provides detailed information about the VSOM Operator pages
Chapter 9, “Using Smart Search”	Describes the Cisco Smart Search feature, which helps operators to search through live or archived video to locate where motion is detected
Part 4, Management Console Reference	
Chapter 10, “Using the VSM Management Console”	Provides detailed information about the VSM Management Console

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.

CHAPTER 1

Overview

This chapter describes how to use this manual, provides an overview of the Cisco Video Surveillance Manager (VSM) system, and describes initial configuration procedures that Cisco recommends be performed. It also explains various configuration strategies, which you can use to help set up your system accurately and efficiently.

This chapter includes these topics:

How to Use this Manual

This manual is designed to help you understand the VSM system and, in particular, the Video Surveillance Operations Manager (VSOM) and the Video Surveillance Management Console. It provides overview information and instructions for configuration, management, and operational procedures that you perform with the VSOM Administrator pages and the Operator Pages, and with the Management Console.

Table 1-1 provides suggestions for using this manual.

Table 1-1 How to Use this Manual

Task	Reference
Learn about Cisco VSM.	See the "About Cisco VSM" section on page 1-2.
Perform initial setup procedures.	See the following sections: • "Setting the VSOM Log In Page as the Default Web Page for a VSOM Server" section on page 1-3 • "Accessing VSOM" section on page 1-4 • "Adding an Administrative User" section on page 1-6 • "Choosing a Configuration Strategy" section on page 1-9
Determine the best way to configure your VSM software components.	See the "Choosing a Configuration Strategy" section on page 1-9.
Perform a basic VSM setup.	See Chapter 2, "Performing a Basic Setup of VSM"
Find detailed reference information about the VSOM Administrator pages and the procedures you can perform from those pages	See the chapters in Part 2, "Administrator Reference"
Find detailed reference information about the VSOM Operator pages and the procedures you can perform from those pages	See Chapter 8, "Using the VSOM Operator Pages"
Find detailed reference information about the VSM Management Console	See Chapter 10, "Using the VSM Management Console"

About Cisco VSM

Cisco VSM comprises a suite of software modules that function with other devices in an IP network to support video transmission, monitoring, recording, archiving, and display. In addition, VSM provides a comprehensive set of features and functions for configuring, administering, managing, and performing day-to-day operations of a video surveillance solution.

The VSM software components include the following:

- Cisco Video Surveillance Media Server (VSMS)—Manages cameras, records and archives video, and provides access to live and recorded video.
- Cisco Video Surveillance Operations Manager (VSOM)—Provides a web-based user interface for configuring, managing, displaying, and controlling video throughout an IP network. Also provide features for managing video devices and users.
- Cisco Video Surveillance Virtual Matrix (VSVM)—Enables the display and control of live and recorded video on remote monitors.

Setting the VSOM Log In Page as the Default Web Page for a VSOM Server

In a typical VSM deployment, VSOM will be installed on one server. Cisco recommends that you configure VSM so that the VSOM log in page appears by default when you access that server through a web browser. To do so, perform the following steps on the VSOM server.

Note

- If you want to bookmark the VSOM server after making this configuration, Cisco recommends that you bookmark the host name. The server will then properly redirect you to the VSOM log in page.
- You can update this configuration at any time as described in the Select Homepage area of the Operations Manager Configuration page. See the "Operations Manager Configuration Page" section on page 10-19 for instructions.

Procedure

Step 1 Take one of these actions to access the VSM Management Console:

- From the keyboard and monitor that are attached to the VSOM server, click the Cisco Video Surveillance Management Console icon on the server desktop:  .
- From a client PC that can access the network in which the VSOM server is connected, start a web browser and enter this address, where <*server*> is the IP address or host name of the VSOM host: **http://<*server*>/vsmc.html**. (For information about a client PC, see the "Accessing VSOM" section on page 1-4.)

The Video Surveillance Management Console appears.

Step 2 Click the **Operations Manager** link in the Configuration area.

Step 3 In the dialog box that prompts for a user name and password take these actions:

a. In the Username field, enter **root**.

The user name is not case sensitive.

b. In the Password field, enter **secur4u**.

The password is case sensitive.

Step 4 Under Select Homepage, click the **Change default homepage to VSOM** radio button.

Step 5 Click **Update**.

Accessing VSOM

You can access various VSM features and perform various VSM operations from a *client PC*, which is a computer that can connect to the network on which VSM runs. A client PC must meet the following minimum requirements. The configuration of your client PC depends on the video and network settings and performance in your network.

- Operating system—Microsoft Windows XP SP3 32-bit with DirectX 9.0 or later; Microsoft Windows 7 64-bit
- Network connection—Gigabit Ethernet (GigE)
- Browser:
  - For Microsoft Windows XP SP3 32-bit with DirectX 9.0 or later: Microsoft Internet Explorer 7.0 or 8.0
  - For Microsoft Windows 7 64-bit: Internet Explorer 8.0 32-bit

For other validated client PC information, see Video Surveillance Monitoring Workstation Performance Baseline Specification, which is available at this URL:

http://www.cisco.com/en/US/docs/security/physical_security/video_surveillance/network/vsm/client/VsmWorkstationBaselineSpec.pdf

You can use the Cisco Video Surveillance Workstation Profile Tool to validate and test the ability of a client PC to render video. For more information, see *Cisco Profile Tool User Guide*.

For related information, see the "Client PC" section in *Installing and Upgrading Cisco Video Surveillance Manager Release 6.3.1*.

To access the VSOM Operations Manager, perform the following steps.

Note

- These steps show how to log in by using the default user name "root" and the default password "secur4u." If the default user name and password have been changed, use those new credentials when you log in.
- These steps assume that you have performed the steps in the "Setting the VSOM Log In Page as the Default Web Page for a VSOM Server" section on page 1-3.

Procedure

Step 1 On a client PC, take these actions:

a. Start Internet Explorer.

b. Enter the IP address or the host name of the server that is running VSOM.

Step 2 In the dialog box that prompts for a user name and password take these actions:

a. In the Username field, enter **root** or if you have changed the user name, enter the current user name.

The user name is not case sensitive.

b. In the Password field, enter **secur4u**, or if you have changed the password, enter the current password.

The password is case sensitive.

c. Click **OK**.

Note If you are prompted to install the ActiveX controller (AXclient), follow the on-screen prompts to do so. ActiveX is required to display video through VSM. You are prompted to install the ActiveX controller the first time that you log into VSOM.

The VSOM Operator page appears.

Using Cisco Video Analytics

The Cisco video analytics feature provides functions for performing video analyses and for triggering events based on these analyses. To use this feature, be aware of these guidelines:

- Video analytics must be enabled in VSOM for a video analytics-enabled IP camera when you configure it in VSOM. For instructions, see the "Adding a New IP/Network Camera" section on page 3-21.
- Video analytics and rules must be configured on each video analytics-enabled IP camera that you will use for this feature. For more information, see the *Cisco Video Analytics User Guide*.
- If you want to set up analytics event:
  - See the "Analytics Trigger" section on page 6-3 for an explanation of event triggers.
  - If you want to enable the default analytics event notification feature, see the "Using the Events Panel" section on page 6-3. This feature allows processing of analytics rules that are not matched with user-created VSOM analytics events.
  - Enable the analytics trigger as described in the "Adding an Event" section on page 6-4.
  - Configure analytics rules as described in Table 6-2 on page 6-6.
- If you enable the Cisco video analytics feature in VSOM for an existing video analytics-enabled IP camera, you must upgrade the camera to a firmware version that provides support for the Cisco video analytics feature and configure the analytics feature in the camera. For more information, see the *Cisco Video Analytics User Guide*.
- If you disable the Cisco video analytics feature in VSOM for an existing video analytics-enabled IP camera by unchecking the **Enable Analytics** check box, video that is associated with analytics events from that camera remains available for viewing in VSM.
- If you change a high definition resolution to a standard definition resolution for a video analytics-enabled IP camera for which video analytics rules are configured, the rules may become corrupted or deleted. In this situation, use the camera web interface to reconfigure the rules. For more information, see the *Cisco Video Analytics User Guide*.
- If you will use the Cisco video analytics feature on a camera that is running firmware version lower than 1.2.1, you must first upgrade the camera to firmware version 1.2.1, then upgrade the camera to a firmware version that provides support for the video analytics feature.

Adding an Administrative User

VSOM includes a default user account, **root**, which has full access to the system. For security and audit purposes, Cisco recommends that you configure a new administrative user account and use it instead of root as the primary administrative account instead.

To configure an administrative user account, perform the following steps. These steps describe the basic configuration items for a new user. To configure more advanced items, see the "Managing User Accounts" section on page 7-5.

Procedure

Step 1 Access VSOM, as described in Accessing VSOM, page 1-4.

Step 2 Click the **Admin** link to open the Administrator pages.

Step 3 Choose **Users** under Accounts in the side menu.

Step 4 Click **Add User**.

Step 5 In the Authentication area, take these actions:

- **a.** In the User Name field, enter a name for the for the user.

  The user name can contain up to 30 characters, including spaces. Use a name, such as **admin**, that will clearly identify the account as the administrator account.
- **b.** In the Password field, enter a password for the user. The password is case sensitive and must contain at least three characters.
- **c.** In the Confirm Password field, reenter the password.
- **d.** Enter the first name of the user in the First Name field.
- **e.** Enter the last name of the user in the Last Name field.
- **f.** (Optional) In the description field, enter a description of the user.

  For example, "Administrative User."
- **g.** (Optional) In the e-mail field, enter an e-mail address for the user.

  This field is for reference only.
- **h.** From the Status drop-down list, choose **Enabled** to allow the user to access the system.

Step 6 (Optional) From the Default View drop-down list, choose the layout that the user sees by default when opening the Operator page.

Step 7 Click the **Roles** tab and check the checkbox in the row that includes "Administrator" in the Role Name column.

In addition, check the check box for other roles that you want to manage.

Step 8 Click the **Submit** button to set up the new account.

After you create a new user, you can click **Log out**, then log in with the new user name and password.

Organizing Information in VSM

For successful installation and ongoing operation of the VSM, it is important to consider carefully how you want to organize the devices in your deployment and how you want to set up archiving, views, monitors, and events. Organizing information effectively can help streamline the deployment process and improve efficiency in day-to-day operations.

Camera Groups

Camera groups allow you to organize cameras by type, function, location, time of day, or another category that is meaningful for your installation. You can also create multiple camera groups for the same set of cameras, each of which is structured for a specific purpose.

For example, suppose that your deployment involves multiple stations along a train route. You can set up individual camera groups for the cameras in each station. If a station is large, with several floors or wings, you can create individual location-based camera groups for each floor or wing.

In addition to the location-based camera groups, it may also be useful for event tracking to create camera groups that correspond to times of day (such as morning commute, lunchtime, and evening commute). You may also want to create a camera group for the cameras in high-risk locations (such as cashier locations).

The resulting organization would involve one set of cameras (for the train route) with the following groupings:

- By location (station or station floors and wings)
- By time of day (commute intervals)
- By risk (high-risk cameras)

In VSOM, each camera group is represented as a folder. When you create camera groups, it may be best in some situations to have one level of organization (multiple folders on the same level), and in other situations to create groups and subgroups (subfolders within folders). For the train route example, the location and time of day groups would be represented by folders on the same level, but the high risk cameras could be set up as subgroups (sub folders) within the location-based station groups.

The decision about whether to create groups and subgroups depends on the size and complexity of your deployment. For example, in a small deployment of 20 cameras, it may be more useful to have a single top-level group with easily-recognizable camera names than to have multiple camera groups. However, for large deployments with hundreds or thousands of cameras, camera groups with some subgroups provide the most effective means of organizing devices.

Naming Conventions

Effective naming conventions are an essential element of a successful VSM deployment. By assigning meaningful and well-structured names to cameras, encoders, archives, views, monitors, and events, you can readily do the following:

- Immediately identify the location and function of each device in your network
- Efficiently add cameras and encoders to VSOM using batch administration
- Readily identify cameras and organize them into meaningful camera groups
- Quickly search for equipment, archives, monitors, and events

- Easily identify events that have common characteristics or triggers
- Organize archives into meaningful sets and quickly select desired archives for viewing

Use the following general guidelines when deciding on naming conventions:

- Names can include alphanumeric characters, spaces, underscores, and hyphens, but no other special characters.
- When naming cameras, make sure that a name allows you to distinguish between fixed and PTZ cameras. For example, include “PTZ” or “FIX” as part of the camera name (SJC-FIX-005 or SJC-PTZ-002).
- Do not include unnecessary information as part of the name. For example, do not include “camera” or “cam” as part of your camera names or “event” as part of your event names. The type of object is clear from the context.
- Choose meaningful prefixes, such as a geographical location, function, or time of day. For examples:
  - Use geographical designations to classify cameras and camera groups, such as airports: LAX, SFO, SJC
  - Use camera functions to classify cameras, camera groups, or archives: FIX, PTZ, HIGHRISK, DOOR
  - Use time of day to classify events: MORN, NOON, EVNG
- Incorporate nested prefixes to help locate specific areas, making sure that the order of the prefixes reflects how you plan to search for information and organize groups. For example:
  - Cameras—Use grouping such as CA-SJ–BL05-FL01. With this order, you can easily set up camera groups for different states (CA), with subgroups for cities (SJ), buildings (BL), and floors (FL).
  - Archives—Use a grouping such as Axis-looping-hour01. This grouping identifies the type of camera (Axis), then the type of archive (looping), then the archive length (one hour).
- Add numeric identifiers to the prefix for individual items, making sure that the numbering scheme allows for expansion.

  For example, use C001, C002, and so on instead of C1, C2, an so on. Adding the extra digits ensures that the system sorts appropriately as the number of cameras grows. If you have cameras in sequence 1, 2, 10, the following naming results in correct sorting:

  C01
  C02
  C10

  However, the following naming results in incorrect sorting, as shown:

  C1
  C10
  C2

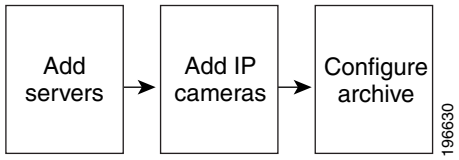
Choosing a Configuration Strategy

The best strategy for entering an configuring information in VSOM depends on the size, complexity, and overall design of your video surveillance network. One of the following strategies should be appropriate for most deployments:

- Basic setup—Used for a relatively simple deployment that implements IP cameras and basic VSM features. Figure 1-1 illustrates the workflow for this configuration strategy.

  For information about performing the steps in a basic setup, see Chapter 2, "Performing a Basic Setup of VSM."

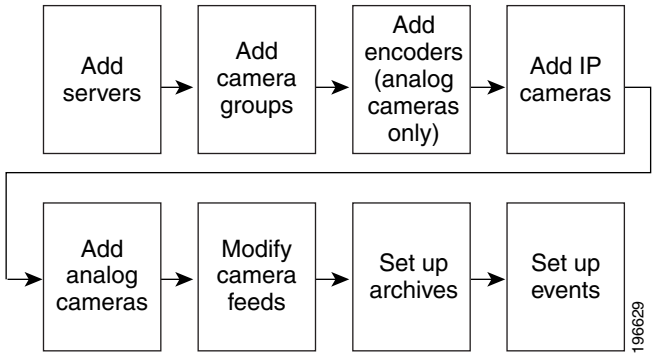
Figure 1-1 Workflow for Basic Configuration Strategy



- Advanced setup—Used for deployments that implements a variety of devices, and more features, such as event notification, than a basic VSM set up. Figure 1-2 illustrates the workflow for this configuration strategy.

  For information about performing the steps in an advanced setup, see the chapters that Part 2, "Administrator Reference" includes.

Figure 1-2 Workflow for Advanced Configuration Strategy

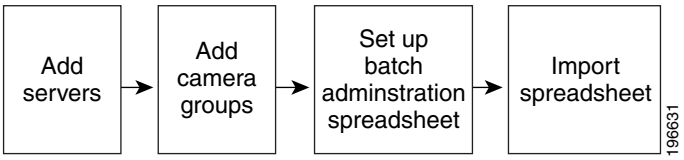


- Batch administration setup—Used for deployments that implements a variety of devices. Uses the batch administration feature to collect information for cameras, encoders, and archives into one spreadsheet that allows batch configuration of devices and configurations. Cisco recommends this strategy for most deployments.

  Figure 1-3 illustrates the workflow for the batch administration setup strategy.

  For detailed information about the batch administration feature, see the "Performing Batch Administration Functions" section on page 5-11.

Figure 1-3 Workflow for Batch Administration Setup Strategy



PART 1

Basic Set Up

CHAPTER 2

Performing a Basic Setup of VSM

This chapter describes the procedures you can perform to set up a basic VSM deployment. It includes these topics:

Overview

This chapter describes the procedures that you perform to complete a basic deployment of VSM. These procedures assume that you have already installed your VSM servers and cameras, and that these devices are connected to the network. It also assumes that you have loaded the VSM software.

A basic installation includes setting up IP cameras and archives. When you complete these setup, you will be able to view, archive, and retrieve video from the IP cameras. You can add features and devices to a basic deployment at any time as your requirements grow or change.

Use the procedures in this chapter as guidelines for a basic deployment or as a general reference for basic procedures in a more advanced deployment. See the reference chapters throughout this manual for detailed information about additional features, functions, and configuration options.

Adding a Server

Adding servers is the process of configuring information about each Multi Services Platform that runs Video Surveillance Media Server (VSMS) and each Multi Services Platform that runs Video Surveillance Virtual Matrix (VSVM) in your VSM deployment. This information includes the name and IP address or host name of each server. If a Multi Services Platform runs VSMS and VSVM, add that server twice, once for each component.

To add servers, follow these steps:

Procedure

Step 1 Access the VSOM as described in the "Accessing VSOM" section on page 1-4.

Step 2 In the VSOM Operator page, click the **Admin** link, which appears near the top left of the page

The Administration area appears.

Step 3 Take the following actions to configure each server that will run VSMS:

a. Click **Servers** under Devices in the left panel of the VSOM Administrator page.

The Servers area appears.

b. In the Servers area, click **Add a New Server**.

c. In the Server Information area in the Details tab, choose **Video Surveillance Media Server (VSMS)** from the Server Type drop-down list.

d. In the Server Name field, enter a name for the server.

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.

e. (Optional) In the Description field, enter a description for the server.

For example, the description could include the location or type of the server.

f. In the Host IP/Name field, enter the host name or IP address of the server that you are adding.

g. Click the **Submit** button to add the server.

h. Repeat this Step 3 for each server on which you will run VSMS.

Step 4 If you will use VSVM, take the following actions to configure the server that will run VSVM:

a. Click **Servers** under Devices in the left panel of the VSOM Administrator page.

The Servers area appears.

b. In the Servers area, click **Add a New Server**.

c. In the Server Information area in the Details tab, choose **Video Surveillance Virtual Matrix (VSVM)** from the Server Type drop-down list.

d. In the Server Name field, enter a name for server.

Enter a descriptive name that can help you identify the server. The name can include any combination of characters and spaces.

e. (Optional) In the Description field, enter a description for the server.

For example, the description could include the location or type of the server.

f. In the Host IP/Name field, enter the host name or IP address of the server that you are adding, followed by **:8086**.

"8086" is the default port number and appears in this field by default.

g. Click the **Submit** button to add the server.

Adding an IP Camera

Adding IP cameras is the process of configuring information about the IP cameras that will operate in your VSM deployment. This information includes the name of the camera, information about its video stream, and its log in credentials.

IP cameras (also called *network camera*s) connect directly to an IP network and do not require separate encoders.

To add an IP camera, perform the following steps. If you want to configure pan/tilt/zoom for an IP camera, follow the steps in the "Configuring PTZ and Joystick Settings" section on page 3-28 after you complete the following procedure.

Note Cisco recommends that you use the Batch Administration to add cameras. For detailed information, see the "Performing Batch Administration Functions" section on page 5-11.

Procedure

Step 1 Access the VSOM as described in the "Accessing VSOM" section on page 1-4.

Step 2 In the VSOM Operator page, click the **Admin** link, which appears near the top left of the page.

The Administration area appears.

Step 3 Click **IP/Network Cameras** under Devices in the left panel of the VSOM Administrator page.

The IP/Network Cameras area appears.

Step 4 In the IP/Network Cameras area, click **Add a New IP/Network Camera**.

Step 5 In the Camera Information area in the Camera Type tab, take these actions:

a. In the Camera Name field, enter a name for the camera.

Enter a descriptive name that can help you identify the camera. The name can include any combination of characters and spaces.

b. (Optional) In the Description field, enter a description for the camera.

For example, the description could include the location or type of the camera.

c. From the Camera Type drop-down list, choose the model of the camera that you are adding.

d. In the Host IP/Name field, enter the IP address or host name of the camera.

Step 6 In the Camera Feed area in the Camera Type tab, take these actions:

a. From the Server drop-down list, choose the VSMS that will manage the video stream.

This list displays the servers that you configured as described in the "Adding a Server" section on page 2-1.

b. From the Media Type drop-down list, choose the digital video encoding type for the video stream from the camera.

c. From the Format drop-down list, choose the format for the video stream from the camera.

The options in this list depend on the camera model that you chose.

d. From the Resolution drop-down list, choose the resolution for the video stream from the camera.

The options in this list depend on the camera model that you chose.

e. For the Transport option, take one of these actions to designate the protocol that VSMS uses to obtain video from the encoder (the available choices depend on the model of the IP camera):

- To choose Transport Control Protocol (TCP), click the **TCP** radio button
- To choose Universal Datagram Protocol (UDP) unicast, click the **UDP** radio button
- To choose UDP multicast, click the **UDP** radio button, then in the Multicast Address field enter the multicast address that camera should use to multicast the video to VSMS

f. From the Bitrate drop-down list, choose the bit rate for the video stream from the camera.

The Bitrate drop-down list appears only if you chose MPEG-2, MPEG-4, or H.264 for the media type.

g. From the Frame Rate drop-down list, choose the frame rate per second for the video stream from the camera.

The Frame Rate drop-down list appears only if you chose JPEG for the media type.

h. Use the Quality slider to specify the quality of the video stream. (This slider is not available for Cisco IP cameras with a Media Type setting other than JPEG unless the Variable Bitrate check box is checked.)

Moving the Quality slider to the right designates a higher value. A higher value uses less compression and provides higher quality.

Step 7 In the Camera requires authentication area in the Camera Type tab, take these actions:

a. Check the **Camera requires authentication** check box if the camera allows access from VSMS only if VSMS provides valid authentication credentials.

b. In the Username field, enter the user name that VSMS should provide when accessing the camera.

The user name is configured on the camera and the value that you enter in this field must match the configured name exactly. The user name can contain alphabetic and numeric characters only and is case sensitive.

c. In the Password field, enter the password that VSMS should provide when accessing the camera.

The password is configured on the camera and the value that you enter in this field must match the configured password exactly. The password can contain alphabetic and numeric characters only and is case sensitive.

d. In the Confirm Password field, reenter the password.

Step 8 Click the **Submit** button to add the camera.

Step 9 Repeat Step 4 through Step 8 as needed to add other cameras.

Configuring Archives

An archive is a recording of the feed from a camera in your VSM deployment. Configuring archives is the process of designating a camera feed that you want to record, setting parameters for the recording, and specifying a schedule for the recording. The feed includes video and, depending on the camera and VSM configuration, may include audio.

A recorded feed is called an *archive*. You can display archives when you need to review a video surveillance feed.

You can configure a scheduled archive, in which the system records based on a defined schedule, or motion-based archive, in which the system records based on motion that a camera detects.

Configuring a Scheduled Archive

You can configure any of the following schedule types for a recording:

- Simple Schedule—Recording occurs once during one or more designated time periods. You specify the start date and time and end date and time for each period.

- Recurring Schedule—Recording occurs on a weekly schedule. For each day, you can specify the time range or ranges in which recording occurs, and you can specify start and stop dates for the entire schedule.
- Continuous Loop—Records continuously and the system retains video for the duration that you designate.

Procedure

Step 1 Access the VSOM as described in the "Accessing VSOM" section on page 1-4

Step 2 In the VSOM Operator page, click the **Admin** link, which appears near the top left of the page.

The Administration area appears.

Step 3 Click **Archives** under Video Feeds in the left panel of the VSOM Administrator page.

Step 4 In the Archives area, click **Start/Schedule a New Archive**.

Step 5 In the Archive Source area in the Feeds tab, take these actions:

a. Click the radio button that corresponds to the camera feed that you want to record.

b. Click **Next**.

Step 6 In the Archive Information area in the Details tab, take these actions:

a. In the Archive Name field, enter a name for the archive.

Enter a descriptive name that can help you identify the archive. The name can include any combination of to 30 characters and spaces.

b. (Optional) In the Description field, enter a description for the archive.

c. From the Status drop-down list, make sure that **Enabled** is selected.

d. From the Force Start drop-down list, choose either of these options:

– **Default**—VSMS verifies whether there is enough capacity to store the archive that you are configuring. If there is not enough capacity when you submit the archive, the archive operation does not start and VSMS generates an error message.

– **Force**—VSMS starts recording even if there is not enough capacity for the archive that is configured. If you choose this option, make sure to provide enough disk space for the archive that you want. If the system runs out of disk space, it begins to delete the oldest retained video to make room for new video.

e. From the Keep on Server drop-down list, choose the number of days that VSMS retains the archive after the recording stops. The system deletes the archive after this period. If you choose **Forever**, the archive is never deleted.

f. If the video feed is a JPEG type, choose a frame rate for the archive from the Frame Rate drop-down list. A higher frame rate provides better quality but consumes more disk space.

Step 7 Click the **Archive Type** tab and take the appropriate actions in the Archive Type area to designate and configure the archive type:

- To record during one or more designated periods, take these actions:

1. Click the **Simple Schedule** radio button.
2. In the **Start on** and **End On** fields, specify the start date and the end date for the recording. In the corresponding **At** fields, enter the start time and end time for the recording.

   You can type information in these fields, or you can use the calendar in the date fields or the drop-down arrows in the time to select information.

3. (Optional) To designate an additional start/stop schedule, click **Add Date(s)** and enter the desired dates and times. You can repeat this process to designate as many start and stop dates and times as needed.

   To remove a start/stop schedule, click **Remove** next to the corresponding schedule.

- To designate a regular weekly schedule for recording, take these actions:
  1. Click the **Recurring Schedule** radio button.
  2. In the **Start On** field, type or use the calendar to enter the date on which the schedule becomes active.
  3. Specify the days on which the recording executes during identical time periods:

     a. Check the check box that corresponds to each day on which you want the recording to execute identically.

     b. In the **Start At** and **Stop At** fields, enter the times that the recording starts and stops on the selected day or days.

     c. (Optional) To add another time interval for the selected days, click **Add Time Range** and enter the start time and stop time in the **Start At** and **Stop At** fields that appear. Repeat as needed to add more time intervals for these days.

     d. (Optional) To specify other days with different schedules, check the check boxes that correspond to the days, enter start and stop times for as many ranges as desired, and click **Next Weekdays**. Repeat as needed.
  4. Specify whether the recurring schedule ends:

     - To stop the schedule after a designated number of weekly runs, click the **End After** radio button and enter the number of times that the schedule should run.

     - To stop the schedule at the beginning of the day on a certain date, click the **End by** radio button and enter the stop date.

     - To run the schedule indefinitely, click the **No End Date** radio button.
- To designate a continuos loop schedule, take these actions:
  1. Click the **Continuous Loop** radio button.
  2. In the **Loop Duration** field, enter the duration of the loop by entering a number and choosing the time unit from the drop-down list.

     The system archives video for the duration that you specify.

Step 8 Click Submit.

If you configured a continuous loop archive, recording starts immediately. Other recording types start as they are scheduled.

Configuring a Motion-Based Archive

You can configure VSOM to record video from a camera that supports motion detection when the camera detects motion. To do so, perform the following steps. For more detailed information about motion-based recording, see the "About Motion Detection Events" section on page 6-10 and the "Setting Up Windows for Motion Detection" section on page 6-14.

Procedure

Step 1 In the Administrator pages, take these actions to enable motion detection:

a. Click **Camera Feeds**.

b. Click the **Edit** icon in the Actions column for the desired feed.

c. Check the **Enable Motion Detection** check box.

d. Click **Submit**.

The system creates a default motion event, named motion-*camera_name_ID*.

Note For related information, see the "Enabling Motion Detection" section on page 5-11.

Step 2 In the Administrator pages, click **Events**.

Step 3 Click the **Edit** icon in the Actions column for the desired event in the Actions column.

Step 4 To set up windows for motion detection, click the **Motion Config** tab and use the following items to configure settings.

The selected motion detection window appears with a green border.

- Motion Window drop-down list—Choose the motion configuration window to configure.
- Active/inactive indication—Displays ACITVE when the selected windows senses motion, otherwise displays INACTIVE.
- **New**—Click to create new motion detection window, then enter window name (using alphanumeric characters only). Click **This is a mask window** if you want the system to ignore motion in this window. Drag the window to the desired location, and drag a border to resize the window.
- **Delete**—Click in a motion detection window, then click **Delete** to remove it.
- Mask Window—Indicates whether the window is a mask window.
- Sensitivity—Use the slider to configure sensitivity for the selected motion detection window. Higher sensitivity means that less motion is required for the system to detect motion.
- Object Size min—Choose a value from 0 to 100 to configure the relative size of an object that triggers motion detection when it moves.
- Object Size max—Not used.
- Persistence—Not used.
- **Show grid**—Click to display a grid on the video display, which can help you arrange motion detection windows.

Step 5 Configure settings on the Motion Start and Motion Stop subtabs described in Table 6-3 on page 6-12.

Step 6 Click **Submit**.

PART 2

Administrator Reference

CHAPTER 3

Managing Devices

This chapter describes how to use the VSOM Device area in the VSOM Administration pages to set up your video surveillance network and equipment.

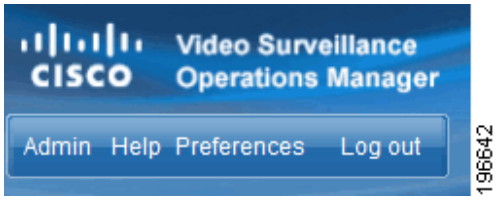
About Device Management

This section describes the tasks that you perform under Devices in the VSOM Administration area.

Using the Device Management Pages

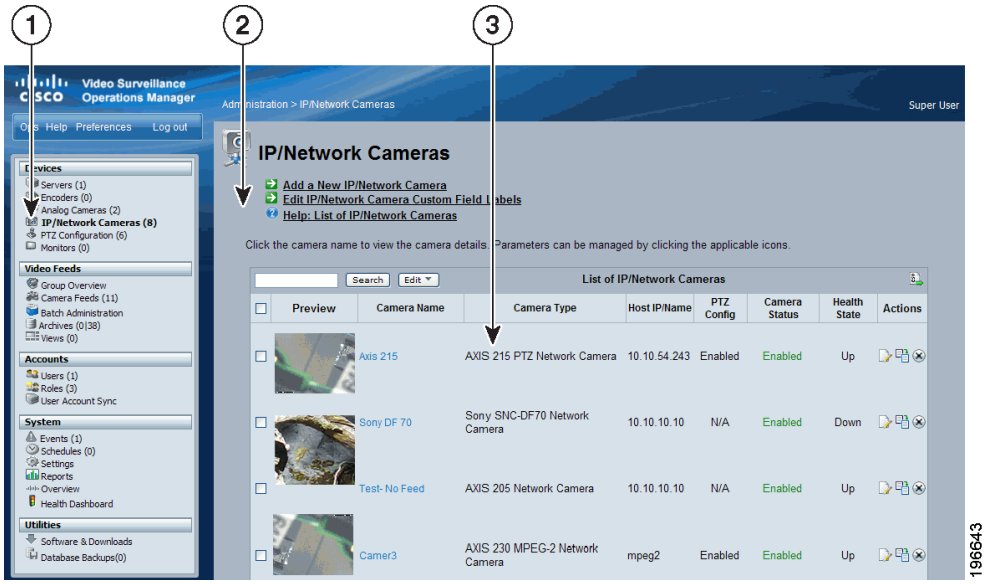
When you open VSOM, the Operator page opens. To open the Administration pages, click the **Admin** link, which appears near the top left of the page (see Figure 3-1).

Figure 3-1 Admin Link



When you choose an item under Devices in the side menu, the page opens to list the devices of that type that are configured in the system, and to provide links to perform functions and obtain help. For example, Figure 3-2 shows the table and links on the IP/Network Cameras panel.

Figure 3-2 IP/Network Cameras Page



1	Side menu	**3**	Main panel for information, interaction
2	Links to perform functions		

Table 3-1 lists the general tasks that you can perform on the Device Management pages. For additional information and detailed instructions regarding these tasks, see the specified sections.

Table 3-1 Device Management Tasks

Task	Action
Search for devices in the table	Enter a text and click **Search** to search all of the fields in the table for the entered text. Results are returned if any one of the fields matches the text. The text is not case-sensitive, and there are no special search characters. The search matches any text within the field name. For example, “df7” matches “Sony SNC-DF70 Network Camera.”
Obtain help for a specific topic	Click the **Help** icon for the topic.
Export data to a CSV file	Export data from VSOM to a CSV[1] file. See the “Exporting Data from the Administration Pages” section on page 4-1.

Table 3-1 Device Management Tasks (continued)

Task	Action
Add a new device	Click the **Add a New...** link. See the following topics: • Adding a New Server, page 3-5 • Adding a New Encoder, page 3-13 • Adding a New Analog Camera, page 3-17 • Adding a New IP/Network Camera, page 3-21 • Adding a New Monitor, page 3-32
Modify settings for an existing device	Click the **Edit** icon in the Actions column for the item. See the following topics: • Editing or Deleting a Server, page 3-7 • Editing or Deleting an Encoder, page 3-14 • Editing or Deleting an Analog Camera, page 3-18 • Editing or Deleting an IP/Network Camera, page 3-24 • Editing or Deleting a Monitor, page 3-32
Modify settings for multiple analog or IP/network cameras	Check the check boxes for the items that you want to modify, or check the check box at the top of the table to modify all the devices of that type. Click the **Edit** button to the right of the **Search** button and choose **Update Selected**. This action opens a page that contains the settings that can be modified for multiple devices at once.
Copy settings for an existing device to a new device (encoders and IP/network cameras only)	Click the **Copy** icon for the item. See the following topics: • Copying an Encoder, page 3-14 • Copying an IP/Network Camera, page 3-24.
Remove an existing device from the VSOM database	Click the **Delete** icon for the item. See the following topics: • Editing or Deleting a Server, page 3-7 • Editing or Deleting an Encoder, page 3-14 • Editing or Deleting an Analog Camera, page 3-18 • Editing or Deleting an IP/Network Camera, page 3-24 • Editing or Deleting a Monitor, page 3-32
Remove multiple cameras from the database	Check the check boxes for the items that you want to delete, or check the check box at the top of the table to delete all the devices of that type. Click the **Edit** button to the right of the **Search** button and choose **Delete Selected**. When prompted to confirm, click **Yes** to delete the item or **No** to return to the page without deleting. Some confirmation pages also allow you to decide whether to retain archive and event history data after the device is removed.

Table 3-1 Device Management Tasks (continued)

Task	Action
Display the current settings for a device	Click the underlined device name. See the following topics: • Displaying Server Information, page 3-8 • Displaying Encoder Information, page 3-15 • Displaying Analog Camera Information, page 3-19 • Displaying IP/Network Camera Information, page 3-26 • Displaying Monitor Information, page 3-33
Define custom field labels for cameras	Custom field labels allow you to specify custom fields to record additional information about the device. See the "Creating Custom Field Labels for Cameras" section on page 3-18.

1. CSV = comma separated value.

Performing Device Configuration Tasks

Table 3-2 lists the activities that are required to set up and configure the video surveillance equipment in your VSM deployment.

Table 3-2 Device Setup Activities

	Activity	Reference
	Add Servers	
Step 1	Configure information about each host that runs VSMS and each host that runs VSVM.	Managing Servers, page 3-5
Note	If you are adding several cameras or encoders at one time, Cisco recommends that you use the batch administration option instead of entering data directly in the Analog Camera and IP/Network Camera panels as described in this chapter. See the "Performing Batch Administration Functions" section on page 5-11. Steps 2-4 in this table are not needed if you use batch administration.	
	Add Encoders and Analog Cameras	
Step 2	If your deployment includes analog cameras, configure information about encoders, which convert analog video into digital video that can be used by VSM.	Managing Encoders, page 3-12
Step 3	Configure information about the individual analog cameras in your VSM deployment.	Managing Analog Cameras, page 3-16
	Add IP/Network Cameras	
Step 4	Configure information about the individual IP/network cameras in your VSM deployment.	Managing IP/Network Cameras, page 3-20

Table 3-2 Device Setup Activities (continued)

	Activity	Reference
	Set up archives, motion detection, PTZ settings, and events	
Step 5	Complete the setup by configuring the capabilities that you want to support for the installed servers, cameras, and encoder.	Managing Monitors, page 3-31 Managing Archives, page 5-17 Configuring PTZ and Joystick Settings, page 3-28 About Events, page 6-1

Managing Servers

The **Servers** page allows you to set up the following server types:

- Video Surveillance Media Server (VSMS)—Manages cameras, records and archives video, and provides access to live and recorded video.
- Video Surveillance Virtual Matrix Server (VSVM)—Enables the display and control of live and recorded video on remote monitors.
- Video Surveillance Backup Server (VSMS-Backup)—Allows you to configure a secondary server to use if a VSMS becomes unavailable. You can specify any VSMS as a backup server.

The term *VSM host* is used generically to refer to any of these server types. VSM hosts can be installed on the same Cisco Physical Security Multiservices Platform or on different platforms. For more information, see *Installing and Upgrading Cisco Video Surveillance Manager (VSM)*.

Table 3-3 lists the tasks you can perform from the Managing Servers page.

Table 3-3 Server-Related Tasks

Task	Description	Reference
Add a New Server	Define a new VSMS, VSVM, or VSMS-Backup	Adding a New Server, page 3-5
Edit or delete a server	Change the settings for a server or delete a server	Editing or Deleting a Server, page 3-7
Display server information	Display the settings for a specified server	Displaying Server Information, page 3-8

Adding a New Server

Adding servers is the process of configuring information about each VSM host that is used in your deployment. This information includes the name and IP address or host name of each server. If a single host runs both VSMS and VSVM, you must add the server twice, once for each component.

All VSOM clients that access VSMS must use same IP address. You must configure a host name rather than an IP address for access to VSMS if clients access VSMS through a system that translates the VSMS IP address, such as through another network or through a firewall that performs network address translation (NAT). In this case, make sure that each client can resolve the host name. For example, you can configure DNS or edit the Windows Hosts file on each VSOM client (see your DNS or Microsoft Windows documentation for details).

Before You Begin

- Determine the type of server that you want to configure: VSMS, VSVM, or VSMS-Backup.
- Obtain the IP address or host name of each server that you are adding. The IP address must be accessible by VSOM.

To add a new server, follow these steps:

Procedure

Step 1 In the Administrator pages, click **Servers**.

Step 2 Click **Add a New Server**.

Step 3 Choose the type of server (VSMS, VSVM, or VSMV-backup).

See the "Managing Servers" section on page 3-5 for a description of the server types.

Note To back up video archives, the system must have at least one VSMS-Backup server. After backups have started, you can click the **Backup** tab for an archive and display the information under Backup Details (see the "Editing or Deleting an Archive" section on page 5-23). The information is for the last executed backup for that archive. The VSMS-Backup server must have a repository for archive backups from other servers.

Step 4 Enter a name to identify the server (up to 30 characters, including spaces).

Step 5 (Optional) Enter a description (up to 1,024 characters, including spaces).

For example, enter the location of the server or its primary use. The name can include any combination of characters and spaces.

Step 6 Enter the host name or IP address of the server.

This address is used by VSOM and all VSOM clients to access video from the system. If the server is accessed using more than one IP address, you must enter a host name instead of an IP address, and you must configure the VSOM server and all VSOM clients to resolve the provided host name with the correct IP address. The host name or IP address must be accessible by the VSOM server and all VSOM clients.

If you are adding a VSVM server, you must include the server port in the Host IP/Name. To do so, follow the IP address or host name by a colon (:) and the port number. ":8086" is the default port number and appears in this field by default.

Example: 192.168.3.1:8086

Step 7 Click the **Rights** tab and verify the access designations.

For information about assigning rights, see the "Adding a Role" section on page 7-8.

Step 8 Click **Submit** to add the server and redisplay the list of servers.

Step 9 (VSVM servers only) Modify the display settings for the Virtual Matrix client by clicking the **Edit** icon in the Actions column for the server and specifying the following settings:

- Border Size—Width of the video window border (0 to 10 pixels)
- Colors—Enter colors in standard hexadecimal format for fixed and highlighted background (BG), text, and rotating video panes. If you enter a hexadecimal number and press **Enter**, the background and text field are updated to show the background and text in the new color.

- Title Height—Height of the title in the title bar of the server window (1 to 20 pixels).
- Server Defaults: Restores all the hexadecimal settings to the server defaults.

Table 3-4 shows example settings.

Table 3-4 Display Setting Defaults

Item	Description	Default
Border Size	0	Width of the display border. Value of 0 means that there is no border
Fixed BG Color	e0e0e0	Color of background in a fixed video pane.
Fixed Text Color	000000	Color of text in a fixed video pane.
Highlight BG Color	A0EFA0	Color of background in a highlighted video pane.
Highlight Text Color	000000	Color of text in a highlighted video pane.
Rotate BG Color	e0e0e0e	Color of background in a rotating video pane.
Rotate Text Color	000000	Color of background in a rotating video pane.
Title Height	20	Height of the camera or archive name text, in pixels.

Step 10 When you have finished modifying the display settings, click **OK**.

Editing or Deleting a Server

You can edit or delete server settings on the Servers panel.

To edit settings, click the **Edit** icon in the Actions column and then make changes on any of the tabs. You can change the server name, description, and assignment of rights. For VSVM servers, you can also change display characteristics after the server is defined. See the "Adding a New Server" section on page 3-5 for information on the available settings.

To delete a server from the VSOM database, click the **Delete** icon for the server. When you delete a server, all of the associated encoders, cameras, child feeds, and event profiles are deleted by default. The system provides you with the option of keeping the following items on the server. Check the check boxes for the items that you want to retain, and then click **Yes** to delete the server.

- Leave running feeds on the server—Does not delete currently running camera feeds from the server.
- Leave running and stored archives on the server—Does not delete currently running or stored archives from the server.
- Leave event histories on the server—Does not delete event histories from the server.

Caution Deleting a VSMS deletes all of the live connections, recordings, and view information for that server.

Importing Archives to a Server

At times, the information that is stored in the VSOM database may not match the information that is stored in VSMS. This situation occurs if a change is made to the VSOM database that is not reflected in VSMS, such as removing a camera from the VSOM database.

To understand what does not match, open the System Overview panel, as described in the "Displaying System Overview Information" section on page 6-22. This page lists the numbers of camera feeds and archives that are missing and out of sync as a fraction of the total number of camera feeds and archives:

- Missing means that an expected camera feed or archive is on VSOM but not on VSMS. To address this issue, identify whether there is a problem with the deployed equipment. If the equipment is not needed, you can remove it from the VSOM database, as described in the "Editing or Deleting an Analog Camera" section on page 3-18 or the "Editing or Deleting an IP/Network Camera" section on page 3-24.
- Out of Sync means that the camera feed or archive is on VSMS but not on VSOM. The out of sync condition typically occurs if a user installs and reinstalls VSOM, but has not yet imported archives from VSMS. To address this issue, click the **Server Import** icon  for the server on the Servers panel.

During the import operation, camera feeds and archives are obtained from the VSMS and new camera, encoder, and archive information is automatically added to VSOM.

Note Server import is supported only when archives are from a single VSMS.

Displaying Server Information

You can obtain information about a VSM server at any time. To do so, click an underlined server name link on the Servers panel. Table 3-5 describes the server information that you can display.

Table 3-5 Server Information

Item	Description
Details Tab	
Server Type	Type of server: • Video Surveillance Media Server (VSMS) • Video Surveillance Virtual Matrix Server (VSVM) • Video Surveillance Backup Server (VSMS-Backup)
Server Name	Name assigned to the server.
Host IP/Name	IP address or host name of the server.
Status	Not used.
Health State (VSMS servers only)	Indicates the status of the connection between the server and VSOM. **Up** indicates that the connection is active. **Down** indicates that either the server is down or there is a connection problem between VSOM and the server.
Console	Link to open the Management Console in a new browser window. See Chapter 10, "Using the VSM Management Console."

Table 3-5 Server Information (continued)

Item	Description
Disk Usage	• Repository—A mounted location on the VSMS host that is dedicated to storing media data • Size—Amount of disk space available to that particular repository • Used (DF)—Amount of actual used disk space at the current time • Free (DF)—Amount of actual free disk space at the current time • Used Space—Amount of disk space (bytes) that VSMS has reserved for all of its requested archive recordings and clips • Free Space—Amount of free disk space (bytes) that the VSMS server has available to reserve for future archive recordings or clips
Server Info Tab	
Installed Version	Version information for VSMS.
Configuration	Configuration information: • Storage Configuration—Percentage of storage used for archiving, including all available repositories. • PTZ Configuration—Length of time (seconds) that a lower priority PTZ command is rejected in favor of a higher priority command. PTZ priority determines what happens when simultaneous attempts are made to control the same PTZ camera. The command with the highest PTZ priority prevails and the others are blocked. • Local Repositories—Partition mount locations on the server that are available for video storage. • Clipping—Repository mount location where BWM and BWX clips are saved. • Archiving—Information about the partition mount locations on the server that are available for selection of a back-up repository. For additional information see Chapter 10, "Using the VSM Management Console."
Camera Feeds Tab	
Feed Name	Name of the camera feed with a link to open the Camera Feed panel for the specified camera. See the "Managing Camera Feeds" section on page 5-6.
Status	Indication of whether the camera feed is currently running or suspended.
Type	Type of feed, as determined by the camera model.
Source	Host name or IP address of the video source, such as an external video device, internal encoder, or another VSMS host.

Table 3-5 Server Information (continued)

Item	Description
Media Type	Format of the camera feed. Types include H264, JPEG, MPEG-2, MPEG-2 Elementary, MPEG-4, and H.263.
Resolution	Video resolution of the camera feed.
F/B Rate	Frame rate and bit rate, which determine the amount of video data transmitted in a given amount of time. Frame rate applies to MJPEG streams, and bit rate applies to MPEG-2 and MPEG-4 streams. Higher values result in smoother video and a more accurate representation of what is happening, but also result in increased system resource use.
Quality	Setting that determines the quality of an MJPEG feed. Higher values result in smoother video and a more accurate representation of what is happening, but also result in increased system resource use.
Exists in VSOM	Indication of whether VSOM recognizes the camera feed. If the feed is not recognized, it is not available for viewing, archiving, or associating with events.
Exists in VSMS	Indication of whether VSMS recognizes the camera feed. If the feed is not recognized, it is not available for viewing, archiving, or associating with events.
Archives Tab (VSMS only)	
Name	Camera and archive name. Click the link to open the Archive panel. See the "Managing Archives" section on page 5-17. Archive names are of the form a_<feed>_-_a_<archive> where <feed> is the name of the camera feed and <archive> is the name of the archive. Example: a_p_53_60-axis_-_a_arch_1.2
Status	Indication of whether the archive is shelved (available but not currently used) or running.
Type	Archive type. Types include loop, recur(ring) or regular.
First Frame Time	Time stamp for the first frame in the archive (yyyy-mm-dd hh:mm format).
Last Frame Time	Time stamp for the last frame in the archive (yyyy-mm-dd hh:mm format).
Start	Date and time that the archive was created.
End	Date and time when the archive was stopped. This entry has no value if the archive is running.
Expires	Number of days after which a shelved archive expires and is removed.
Exists in VSOM	Indication of whether VSOM is able to recognize and manage this archive.
Exists in VSMS	Indication of whether VSMS is able to recognize and manage this archive.

Table 3-5 Server Information (continued)

Item	Description
Events Tab (VSMS only)	
Name	Name assigned to the event.
Device	Host name or IP address of the device that is associated with the event.
Source	Camera or component name of the device that is associated with the event.
Channel	Encoder channel (hardware connection) of the device that is associated with the event.
Type	Type of event: • (Blank)—Motion configuration event. • Alarm—Soft event (with archive clipping). A soft event is a URL notification from a third party application or device. • Motion—Device trigger event with (archive clipping).
State	State for device trigger events: • Rising—Increasing state on device trigger. Useful only for device trigger events. • Falling—Declining state on device triggers. Useful only for device trigger events.
Action	Action that the system takes in response to the event: • None—Do not take any action • Archive Clip—Create an archive clip **Note** This parameter is set in the event/actions module and is not available for soft triggers. See the "Adding an Event" section on page 6-4 for information about soft triggers.
Camera Feeds	Name assigned to the camera feed.
Framerate	Frame rate at which the event clips are recorded when an event occurs.
Days to Live	Number of days between the time that the event video is saved and the time that it is removed from the system.
Rights Tab	
Rights	Access rights for the device: • Name—Role name with a link that opens the Roles panel for the specified role. • Rights—Indication of the rights that are assigned to the role.

Changing Server IP Addresses

You cannot change the address of a VSMS or VSVM server in VSOM after a server has been added to VSOM. If you need to change the IP address of a server, follow these steps:

Procedure

Step 1 In VSOM, delete the server and check the check boxes to leave feeds, archives, and event histories on the server. See the "Editing or Deleting a Server" section on page 3-7.

Step 2 Make the necessary hostname or IP address changes on the VSMS server.

Step 3 In VSOM, add the server using the updated IP address or hostname. See the "Adding a New Server" section on page 3-5.

Step 4 On the Servers page in VSOM, click the **Import** icon for the newly added server The camera feeds and archives are obtained from the server and new camera, encoder, and archive information is automatically added to VSOM.

Note The import process does not retain camera PTZ settings, motion events, motion detection configuration, camera feeds from Views, camera group settings for each camera, or camera user names and passwords (VSMS retains the user credentials to connect camera feeds).

Managing Encoders

Note Encoders are required only if your deployment includes analog cameras.

Encoders convert video from analog cameras into digital video that VSOM can interpret and display. VSOM identifies an encoder by its IP address and encoder type. It is common for encoders to be secured by a user name and password, and these credentials should be added if required. VSOM supports encoders for MJPEG and MPEG-4 video.

Some encoders permit multiple streams with different attributes from the same video input. For example, the same video input may be available both as a JPEG feed and a MPEG-4 feed. To support multiple streams on the same channel of an encoder, you can configure two feeds in VSOM using the 1_1 and 1_2. Encoder channel 1_1 represents encoder channel 1, stream 1 and 1_2 represents encoder channel 1, stream 2.

All configured cameras are included in camera listings in VSOM and populate all layouts in the default camera group order as set by administrators.

To open the Encoders panel, click **Encoders** on the side menu in the Administrator pages. Table 3-6 lists the tasks that you can perform on the panel. For a general description of encoder actions, see Table 3-1.

Table 3-6 Encoder-Related Tasks

Task	Description	Reference
Add a New Encoder	Define a new encoder to support analog cameras in your deployment	Adding a New Encoder, page 3-13
Edit or delete an encoder	Change the settings for an encoder or delete an encoder	Editing or Deleting an Encoder, page 3-14

Table 3-6 Encoder-Related Tasks (continued)

Task	Description	Reference
Copy an encoder	Create new encoders with settings based on a specified encoder	Copying an Encoder, page 3-14
Display encoder information	Display the settings for a specified encoder	Displaying Encoder Information, page 3-15

Adding a New Encoder

Adding encoders is the process of configuring information about each encoder that operates in your VSM deployment. You can add encoders individually, as described in this section, or copy the settings from an existing encoder to a new encoder or encoders. For instructions, see the "Copying an Encoder" section on page 3-14.

Before You Begin

- Determine the brand and model of the encoder that you want to add. Choose a naming convention for your encoders, if you do not want to use IP addresses as the encoder names.
- Obtain the IP address or host name of each encoder that you want to add.

To add a new encoder, follow these steps:

Procedure

Step 1 In the Administrator pages, click **Encoders**.

Step 2 Click **Add a New Encoder**.

Step 3 Choose the model of the encoder that you are adding from the **Encoder Type** drop-down list.

Step 4 In the Encoder name field, enter a descriptive name that can help you identify the device (up to 30 characters, including spaces).

Step 5 (Optional) In the Description field, enter a description of the device (up to 1,024 characters, including spaces).

Step 6 In the Host IP/Name field, enter the host name or IP address of the encoder that you are adding.

Step 7 If the encoder allows access from VSMS only if VSMS provides valid authentication credentials, take the following actions in the Authentication area:

a. In the Username field, enter the user name that VSMS provides when accessing the encoder. The user name is configured on the encoder and the value that you enter in this field must match the configured name exactly. The user name can contain alphabetic and numeric characters only and is case sensitive.

b. In the New Password field, enter the password that VSMS provides when accessing the encoder. The password is configured on the encoder and the value that you enter in this field must match the configured password exactly. The password can contain alphabetic and numeric characters only and is case sensitive.

c. In the Confirm Password field, reenter the password.

Step 8 Click the **Rights** tab and verify the access designations. See the "Adding a Role" section on page 7-8.

Step 9 Click **Submit**.

Editing or Deleting an Encoder

You can edit or delete encoder settings on the Encoders panel.

To edit settings, click the **Edit** icon in the Actions column and then make changes on any of the tabs. See the "Adding a New Encoder" section on page 3-13 for information on the available settings. If the encoder requires authentication credentials, click the **Update Authentication** link and specify the user name and password.

To delete an encoder from the VSOM database, click the **Delete** icon for the encoder. When you delete an encoder, all of its associated cameras, child feeds, and event profiles are deleted by default. The system provides you with the option of keeping the following items on the server. Check the check boxes for the items to retain on the server, and click **Yes**.

- Leave archive data files on the server(s)—Does not delete archive files for the deleted item from the server.
- Keep event history records from this device—Does not delete event history records for the deleted item from the server.

Copying an Encoder

You can copy encoder settings to create a new encoder with the same configuration settings as an already configured encoder.

To copy encoder settings, follow these steps:

Procedure

Step 1 In the Administrator pages, click **Encoders**.

Step 2 Click the **Copy** icon for the encoder from which you want to copy settings.

Step 3 In the Number of Copies field, enter the number of new encoders that you want to create based on the configuration settings of the existing encoder.

Step 4 In the IP Start field, enter an IP address for the first copy.

If you are creating multiple copies, the IP addresses are assigned consecutively, beginning with this specified address.

Note The system does not check for duplicate IP addresses. Make sure that consecutive addresses are available in the range that begins with the address that you specify.

Step 5 Check the **Use IP Address as Name** check box to use the IP address of the copy as the encoder name.

Step 6 If you do not want to use the IP address as the name, take these actions:

a. In the Common Name field, enter a name to identify this set of copies. The name is used with a prefix or suffix that you specify.

b. From the **Append As** drop-down list, specify whether the sequence numbers or letters are added before the common name (Prefix) or after the common name (Suffix).

c. From the **Type** drop-down list, choose **Numbers** or **Letters** to designate the type of characters in a prefix or suffix.

For example, if you make two copies, enter -**myencoder** as the common name and choose **Prefix** and **Letters**, the copies are named **a-myencoder** and **b-myencoder**. If you choose **Suffix** and **Numbers**, the copies are named -**myencoder**1 and -**myencoder**2.

Step 7 Click **Copy Encoders** to create the new encoders and add them to the encoder list.

Displaying Encoder Information

You can obtain information about an encoder at any time. Click an underlined encoder name link on the Encoders panel to display detailed information about the encoder, as described in Table 3-7.

Table 3-7 Encoder Information

Item	Description
Details Tab	
Encoder Name	Name assigned to the encoder.
Encoder Type	Encoder brand and model.
Host IP/Name	IP address or name of the encoder. Click the link to open the default configuration page for the encoder (if available).
Health State	Indicates the status of the encoder. **Up** indicates that the encoder is reachable, active, and working. **Down** indicates that there is a problem with the encoder, that it is not active or not reachable.
Status	Not used.
Requires Authentication	Indication of whether a user name and password are required to access the encoder.
Cameras Tab	
Camera Name	Name assigned to the camera. Click the link to open the Camera panel for the specified camera. See the "Managing Analog Cameras" section on page 3-16 or the "Managing IP/Network Cameras" section on page 3-20.
Camera Type	Camera brand and model.
PTZ Enabled	Indication of whether PTZ functionality is enabled on the camera.
Status	Indication of whether the camera is administratively enabled or disabled. This setting determines whether VSOM treats the camera as active (enabled), but has no affect on the operation of the camera.
Camera Feeds Tab	
Feed Name	Name assigned to the camera feed. Click the link to open the Camera Feed panel. See the "Managing Camera Feeds" section on page 5-6.

Table 3-7 Encoder Information (continued)

Item	Description
Media Type	Media format for the camera feed. Media types include H264, JPEG, MPEG-2, MPEG-2 Elementary, MPEG-4, and H.263.
F/B Rate	Frame rate and bit rate, which determine the amount of video data transmitted in a given amount of time. Frame rate applies to MJPEG streams, and bit rate applies to MPEG-2 and MPEG-4 streams. Higher values result in smoother video and a more accurate representation of what is happening, but also result in increased system resource use.
Quality	Setting that determines the quality of an MJPEG feed. Higher values represent higher quality frames, which also are associated with larger frame file sizes. **Note** A child feed inherits the quality setting from the parent feed.
Rights Tab	
Rights	Access rights for the device: • Name—Role name with a link that opens the Roles panel for the specified role. • Rights—Indication of the rights that are assigned to the role.

Managing Analog Cameras

Analog cameras provide analog video to encoders, which convert the analog signals into digital video that VSOM can interpret and display. Matching an analog camera to an encoder creates a camera feed (video stream). Some analog cameras also support PTZ functions.

Some encoders permit multiple streams with different attributes from the same video input. For example, the same video input may be available as a JPEG feed and an MPEG-4 feed.

Click **Analog Cameras** on the side menu in the Administrator pages to open the Analog Cameras panel.

Table 3-8 lists the tasks that you can perform on the panel. For a general description of device actions, see Table 3-1 on page 3-2.

Table 3-8 Analog Camera-Related Tasks

Task	Description	Reference
Add a new analog camera	Define the settings for a new analog camera	Adding a New Analog Camera, page 3-17
Edit or delete an analog camera	Change the settings for an analog camera or delete an analog camera	Editing or Deleting an Analog Camera, page 3-18
Create custom field labels for the camera	Define custom fields to store additional information about the analog cameras in your system	Creating Custom Field Labels for Cameras, page 3-18
Display analog camera information	Display the settings for a specified analog camera	Displaying Analog Camera Information, page 3-19

Adding a New Analog Camera

When you add an analog camera, you include the name of the camera and information about its video stream and encoder.

Before You Begin

- Choose a naming convention for your cameras. See the "Organizing Information in VSM" section on page 1-7.
- Determine which of the encoders in the system is used to encode the camera analog signals and the encoder channel to be used. For a list of encoders or to add a new encoder, see the "Managing Encoders" section on page 3-12.
- Determine the VSMS that is used to manage the camera. For a list of VSMS hosts or to add a new VSMS, see the "Managing Servers" section on page 3-5.
- Determine the desired characteristics of the camera feed, including media type, format, resolution, method to be used to send video information to VSOM, frame rate, and quality. The type of camera determines the available values for these parameters.

To add a new analog camera, follow these steps:

Procedure

Step 1 In the Administrator pages, click **Analog Cameras**.

Step 2 Click **Add a New Analog Camera**.

Step 3 In the Camera Name field, enter a descriptive name for the camera that is consistent with your naming conventions (up to 30 characters, including spaces).

Step 4 (Optional) In the Description field, enter a description (up to 1,024 characters, including spaces).

For example, the description could include the location or type of the camera.

Step 5 From the **Encoder** drop-down list, choose the encoder that is used to convert the cameras signals from analog to digital.

Step 6 From the **Encoder Channel** drop-down list, choose the encoder input port that the camera connects to.

Step 7 In the Camera Feed area in the Camera Type tab, specify the following settings:

- Server—Choose the VSMS that manages this camera. This list displays the servers that you configured as described in the "Adding a New Server" section on page 3-5.
- Media Type—Choose the digital video encoding type for the video stream from the camera. The options in this list depend on the encoder that you chose for this camera.
- Format—Choose the format for the video stream from the camera. The options in this list depend on the encoder that you chose for this camera.
- Resolution—Choose the resolution for the video stream from the camera. The options in this list depend on the encoder that you chose for this camera.
- Transport—Choose the protocol that VSMS uses to obtain video from the encoder (the available choices depend on the encoder that you chose for this camera). To choose UDP multicast, click the **UDP** radio button, then in the Multicast Address, field enter the multicast address that the encoder should use to multicast the video to VSMS. For unicast transmission, leave the Multicast Address field blank.
- Framerate—Choose the framerate or bit rate for transporting the video data.

Frame rate and bit rate determine the amount of video data transmitted in a given amount of time. Frame rate applies to MJPEG streams, and bit rate applies to MPEG-2 and MPEG-4 streams.

Higher values result in smoother video and a more accurate representation of what is happening, but also result in increased system resource use.

The standard bit rate selection is for constant bit rate (CBR), which specifies a fixed amount of data sent per second. For Cisco cameras with variable bit rate (VBR) support, you can conserve bandwidth by checking the **Variable bitrate** check box. The VBR option uses the amount of data in the video itself when determining the amount of data to send per second. For example, sending video of a white screen does not require much bandwidth, and that is taken into account with VBR. With VBR, the selected bit rate is treated as the maximum bit rate and is adjusted to be lower if a lower bit rate is sufficient. To use the VBR option, the camera must support VBR.

- Quality—Use the scroll bar to set video quality for camera feeds.

  For MJPEG camera feeds (MPEG-2 or MPEG-4), this parameter sets the MJPEG quality (compression) setting of the video source. 1 is the lowest quality (highest compression) and 100 is the highest quality (least compression). A setting of 50 is the default and produces a good balance between visual quality and size of the video data.

  For MPEG camera feeds, a setting of 1 through 49 sets the video source to favor a higher frame rate over compression and visual quality. A setting of 50 through 100 sets the video source to favor less compression and better visual quality over frame rate.

  See Table 3-11 for a description of VBR quality settings for different camera and encoder vendors.

Note If you are using batch administration to add Cisco cameras, you must use the following range of quality values: CBR (0–100) and VBR (101–200). For information on using batch administration, see the "Performing Batch Administration Functions" section on page 5-11.

Step 8 Click the **Rights** tab and verify the access designations. See the "Adding a Role" section on page 7-8.

Step 9 Click **Submit**.

The camera is added to the system and included in the table on the Analog Cameras panel.

Editing or Deleting an Analog Camera

You can edit or delete analog camera settings on the Analog Cameras panel.

To edit settings, click the **Edit** icon in the Actions column and then make changes on any of the tabs. See the "Adding a New Analog Camera" section on page 3-17 for information on the available settings.

To delete a camera from the VSOM database, click the **Delete** icon for the camera. When you delete a camera, all of the associated camera feeds and event configurations are deleted by default. The system provides you with the option of keeping the archive data files on the server. Check the check box if you want to retain the archive files, and click **Yes**.

Creating Custom Field Labels for Cameras

Custom field labels allow you to specify custom fields to record additional information about a camera. These fields appear on the Custom Fields tab when you edit a camera record.

To create custom fields labels, follow these steps:

Procedure

Step 1 Click the **Edit Camera Custom Field Labels** link above the list of cameras to open the Custom Fields configuration page.

Step 2 Enter up to 20 field labels in the order in which you want them to appear.

Labels that are left blank are ignored.

Step 3 Click **Submit**.

Displaying Analog Camera Information

Click an underlined camera link on the Analog Cameras panel to display detailed information about the camera, as described in Table 3-9.

Table 3-9 Analog Camera Information

Item	Description
Details Tab	
Preview Image	Preview of the video. Click + to enlarge the image and – to reduce the preview image size.
Camera Name	Name that identifies the camera.
Encoder Name	Name assigned to the encoder that is associated with the camera. Click the link to open the Encoder panel. See the "Displaying Encoder Information" section on page 3-15.
Encoder Channel	Channel on which the encoder that is associated with the camera receives video from the camera.
PTZ Information	PTZ settings, if PTZ is supported and enabled on the camera. Click a PTZ preset to set the area of the video that is shown initially in the Operator page. When you click a PTZ preset, that area is shown in the preview image. Use the – and + icons for the image to enlarge or shrink the preview.
Camera Feeds	
Feed Name	Name assigned to the camera feed. Camera feed names are assigned automatically, but can be changed.
Media Type	Media type of the camera feed. Media types include H264, JPEG, MPEG-2, MPEG-2 Elementary, MPEG-4, and H.263.
F/B Rate	Frame rate and bit rate, which determine the amount of video data transmitted in a given amount of time. Frame rate applies to MJPEG streams, and bit rate applies to MPEG-2 and MPEG-4 streams. Higher values result in smoother video and a more accurate representation of what is happening, but also result in increased system resource use.

Table 3-9 Analog Camera Information (continued)

Item	Description
Quality	Video quality value for the camera feed. 0 is the lowest quality (highest compression) and 100 is the highest quality. Higher values represent more video data every second, which means smoother video and a more accurate representation of what is happening. However, higher values also result in larger file sizes.
VBR	Indicates whether support for variable bit rate (VBR) is enabled or disabled (only for cameras that support VBR).
Custom Fields	
Custom Fields	Values for user-defined custom fields.
Rights Tab	
Rights	Access rights for the device: • Name—Role name with a link that opens the Roles panel for the specified role. • Rights—Indication of the rights that are assigned to the role.

Managing IP/Network Cameras

An IP/network camera connects directly to a network and appears to VSOM as an analog camera and encoder in a single package. Adding an IP camera to VSOM creates a camera feed (video stream) that you can display in VSOM.

Many IP/network cameras are PTZ capable. In addition, some support dual streaming, which allows you to specify a secondary feed that has different attributes than the primary feed.

Click **IP/Network Cameras** on the side menu in the Administrator pages to open the IP/Network Cameras panel.

Table 3-10 lists the tasks that you can perform on this panel. For a general description of device actions, see Table 3-1 on page 3-2.

Table 3-10 IP/Network Camera-Related Tasks

Task	Description	Reference
Add a new IP/network camera	Define the settings for a new IP/network camera	Adding a New IP/Network Camera, page 3-21
Edit or delete an IP/network camera	Change the settings for an IP/network camera or delete an IP/network camera	Editing or Deleting an IP/Network Camera, page 3-24
Copy an IP/ network camera	Create new IP/network cameras with settings based on a specified camera	Copying an IP/Network Camera, page 3-24
Upgrade an IP/ network camera	Upgrade a Cisco IP camera model 2421 or 25xx to a Cisco IP Camera 26xx model	Upgrading Selected Cisco IP/Network Camera Models to Cisco IP Camera 2600 Models, page 3-25

Table 3-10 IP/Network Camera-Related Tasks (continued)

Task	Description	Reference
Create custom field labels for the camera	Define custom fields to store additional information about the IP/network cameras in your system	Creating Custom Field Labels for Cameras, page 3-18
Display IP/network camera information	Display the settings for a specified camera	Displaying IP/Network Camera Information, page 3-26

Adding a New IP/Network Camera

When you add an IP/Network camera, you include the name of the camera and information about its video stream.

Before You Begin

- Choose a naming convention for your cameras.
- Determine the VSMS that is used to manage the camera. For a list of VSMS hosts or to add a new VSMS, see the "Managing Servers" section on page 3-5.
- Obtain authentication information for the cameras, if required by the cameras.
- Determine the characteristics of the camera feed, including media type, format, resolution, method to be used to send video information to VSOM, frame rate, and quality. The type of camera determines the available values for these parameters.
- If the camera supports dual streaming and you want to specify a secondary feed, determine the secondary stream characteristics.
- Determine the transport method that VSMS uses to obtain feeds from the cameras.

Procedure

Step 1 In the Administrator pages, click **IP/Network Cameras**.

Step 2 Click **Add a New IP/Network Camera**.

Step 3 In the Camera Name field, enter a descriptive name for the camera that is consistent with your naming conventions (up to 30 characters, including spaces).

If you will use the Cisco video analytics feature, this camera name must match exactly the name that is entered in the Server URI field in the Device Configuration window in the IP camera web interface. For more information, see the *Cisco Video Analytics User Guide*.

Step 4 (Optional) Enter a description (up to 1,024 characters, including spaces).

Step 5 From the **Camera Type** drop-down list, choose the camera brand and model.

Step 6 (Optional) If you choose a video analytics-enabled IP camera (such as **Cisco HD IP Camera 4500 Series**) from the Camera Type drop-down list and you want to enable the Cisco video analytics feature, check the **Enable Analytics** check box.

For information about other items that must be configured to use the video analytics feature, see the "Using Cisco Video Analytics" section on page 1-5.

Note If you check the **Enable Analytics** check box, the system automatically creates a 1-hour looping archive named Analytics_*camera-name* when you submit the configuration information at the end of this procedure.

Step 7 In the Host IP/Name field, enter the host name or IP address of the camera.

Step 8 In the Camera Feed section, specify the following settings:

- Server—Choose the VSMS that manages this camera.
- Media Type—Choose the media type from the drop-down list (H264, JPEG, MPEG-2, MPEG-2 Elementary, MPEG-4, or H.263). If you configured UDP to be on for the camera, leave the multicast address blank to enable unicast.
- Format—Choose the media format (NTSC or PAL) from the drop-down list.
- Resolution—Choose the resolution from the drop-down list. Resolutions under 1,024 pixels wide (for example, 800 x 600) display scrollbars and an undersized Operator page pane.
- Transport—Choose the protocol that VSMS uses to obtain video from the encoder (the available choices depend on the encoder that you chose for this camera). To choose UDP multicast, click the **UDP** radio button, then in the Multicast Address, field enter the multicast address that the encoder should use to multicast the video to VSMS. For unicast transmission, leave the Multicast Address field blank.
- Framerate or Bitrate—From the drop-down list, choose the framerate or bit rate for transporting the video data.

  Frame rate and bit rate determine the amount of video data transmitted in a given amount of time. Frame rate applies to MJPEG streams, and bit rate applies to MPEG-2 and MPEG-4 streams.

  Higher values result in smoother video and a more accurate representation of what is happening, but also result in increased system resource use.

  The standard bit rate selection is for constant bit rate (CBR), which specifies a fixed amount of data sent per second. For Cisco cameras and encoders with variable bit rate (VBR) support, you can conserve bandwidth by checking the **Variable bitrate** check box. The VBR option uses the amount of data in the video itself when determining the amount of data to send per second. For example, sending video of a white screen does not require much bandwidth, and that is taken into account with VBR. With VBR, the selected bit rate is treated as the maximum bit rate and is adjusted to be lower if a lower bit rate is sufficient. To use the VBR option, the camera must support VBR.
- Quality—Use the scroll bar to set video quality for camera feeds.

  For MJPEG camera feeds (MPEG-2 or MPEG-4), this parameter sets the MJPEG quality (compression) setting of the video source. 0 is the lowest quality (highest compression) and 100 is the highest quality (least compression). A setting of 50 is the default and produces a good balance between visual quality and size of the video data.

  For MPEG camera feeds, a setting of 1 through 49 sets the video source to favor a higher frame rate over compression and visual quality. A setting of 50 through 100 sets the video source to favor less compression and better visual quality over frame rate.

  See Table 3-11 for a description of VBR quality settings for different camera and encoder vendors.

Note If you are using batch administration to add Cisco cameras, you must use the following range of quality values: CBR (0-100) and VBR (101-200). For information on using batch administration, see the "Performing Batch Administration Functions" section on page 5-11.

Step 9 Check the **Camera requires authentication** check box if authentication is required to access the camera. Enter a user name and password, and reenter the password to confirm.

Step 10 If the camera is capable of dual streaming and you want to specify a secondary feed, click the **Secondary Feed** tab, check the **Secondary Feed** check box, and specify the feed characteristics according to the descriptions in Step 8.

Step 11 Click the **Camera Groups** tab to assign the camera to a group.

Choose the group or groups, or choose **Top Level (No Group)** if you do not want to place the camera in a group. Click **Expand All** to show the full group hierarchy or **Collapse All** to hide the hierarchy.

Step 12 Click the **Advanced Configuration** tab if you need to set PTZ options for the camera, and configure the following settings:

- Camera is PTZ-enabled—Choose if the camera supports PTZ.
- Status—Choose **Enabled** to permit PTZ camera control. Choosing **Disabled** turns the PTZ control off without removing the PTZ configurations from the list.
- Manufacturer—Choose the camera make and model from the drop-down list.
- PTZ Preset Labels—Enter PTZ labels to map to USB joystick buttons. Labels should identify the camera view or location, such as Front Lobby or Parking Garage A. You cannot map PTZ labels to mouse buttons.

Step 13 (Optional) Click the **Map Info** tab to designate the physical location of the camera. The settings on this tab are for reference only and are not used by VSOM.

Step 14 (Optional) Click the **Custom Fields** tab to add additional information about the camera.

See the "Creating Custom Field Labels for Cameras" section on page 3-18.

Step 15 Click the **Rights** tab and verify the access designations.

See the "Adding a Role" section on page 7-8.

Step 16 Click **Submit**.

Table 3-11 describes the supported VBR quality settings for different camera and encoder vendors.

Table 3-11 VBR Quality Settings

Camera or Encoder Vendor	Value in Media Type Field	Quality Slider Values
IP Cameras		
Any (Cisco or non-Cisco)	JPEG	1 through 100
Non-Cisco	Any value other than JPEG	1 through 100
Cisco	Any value other than JPEG	• If the Variable Bitrate check box is unchecked, cannot change the quality slider • If the Variable Bitrate check box is checked, quality slider values are: Very Low, Low, Normal, High, Very High

Table 3-11 VBR Quality Settings (continued)

Camera or Encoder Vendor	Value in Media Type Field	Quality Slider Values
Analog Cameras		
Any (Cisco CIVS-ES-16EX or other)	—	1 through 100
Models other than Cisco CIVS-ES-16EX	Any value other than JPEG	1 through 100
Cisco CIVS-ES-16EX	Any value other than JPEG	• If the Variable Bitrate check box is unchecked, cannot change the quality slider • If the Variable Bitrate check box is checked, quality slider values are: • 1 through 100

Editing or Deleting an IP/Network Camera

You can edit or delete IP/Network camera settings on the IP/Network Cameras panel.

To edit settings for an IP/network camera, click the **Edit** icon in the Actions column and then make changes on any of the tabs. See the "Adding a New IP/Network Camera" section on page 3-21 for information on the available settings.

Note If you are editing settings that affect the Cisco Video Analytics feature, see the guidelines in the "Using Cisco Video Analytics" section on page 1-5.

To delete an IP/network camera from the VSOM database, click the **Delete** icon for the camera. When you delete a camera, all of the associated camera feeds and event configurations are deleted by default. The system provides you with the option of keeping the following items on the server. Check the check boxes for the items to retain on the server, and click **Yes**.

- Leave archive data files on the server(s)—Retains archive files for the deleted item on the server.
- Keep event history records from this device—Retains event history records for the deleted item on the server.

Copying an IP/Network Camera

You can copy IP/network camera settings to create a new camera or cameras with the same configuration settings as an already configured camera. When you do so, the permissions are inherited from the originating camera.

To copy IP/network camera settings, follow these steps:

Procedure

Step 1 In the Administrator pages, click **IP/Network Cameras**.

Step 2 Click the **Copy** icon for the camera from which you want to copy settings.

Step 3 In the Create Fields on Server field, choose the VSMS that manages the new cameras.

Step 4 In the Number of Copies field, enter the number of new cameras that you want to create based on the configuration settings of the existing camera.

Step 5 In the IP Start field, enter an IP address for the first copy.

If you are creating multiple copies, the IP addresses are assigned automatically, beginning with this specified address.

Note The system does not check for duplicate IP addresses. Make sure that consecutive addresses are available in the range that begins with the address that you specify.

Step 6 Check the **Use IP Address as Name** check box to use the IP address of the copy as the camera name.

Step 7 If you do not want to use the IP address as the name, specify the following:

a. In the Common Name, enter a name to identify this set of copies. The name is used with a prefix or suffix that you specify.

b. From the **Append As** drop-down list, specify whether the sequence numbers or letters is added before the common name (Prefix) or after the common name (Suffix).

c. From the Type drop-down list, choose **Numbers** or **Letters** to designate the type of characters in a prefix or suffix.

For example, if you make two copies, enter -**mycamera** as the common name and choose **Prefix** and **Letters**, the copies are named **a-mycamera** and **b-mycamera**. If you choose **Suffix** and **Numbers**, the copies are named -**mycamera**1 and -**mycamera**2.

Step 8 Click **Copy IP/Network Camera** to create the new cameras.

Upgrading Selected Cisco IP/Network Camera Models to Cisco IP Camera 2600 Models

The camera upgrade feature lets you easily replace a Cisco IP camera 2421 or 25xx model with a Cisco IP camera 26xx model. When you use this feature, you do not need to manually create the new 26xx camera, camera feed, or archives in VSM. Table 3-12 lists the upgrades that this feature supports.

Table 3-12 Upgrades Supported by the Camera Upgrade Feature

Existing Camera Model	Upgraded Camera Model
Cisco IP camera 2421	Cisco IP camera 2611
Cisco IP camera 2500	Cisco IP camera 2600
Cisco IP camera 252x	Cisco IP camera 2621
Cisco IP camera 253x	Cisco IP camera 2630

To upgrade an IP/network camera, perform the following steps.

Before You Begin

- Determine IP address, user name, and password (if configured) that are configured for the old camera. You can determine the IP address and user name as described in the "Editing or Deleting an IP/Network Camera" section on page 3-24.
- Physically replace the old camera with the new camera by disconnecting the old camera from your network and connecting the new camera.
- Use the web-based interface for the new camera to configure it with the same IP address, user name, and password that were configured for the old camera.
- Make sure that the new camera is running a supported firmware version.

Procedure

Step 1 In the Administrator pages, click **IP/Network Cameras**.

Step 2 Click the **Edit** icon in the Actions column for a supported camera to upgrade (see Table 3-12)

Step 3 Click the appropriate link for the upgrade that you are performing:

- **Upgrade Camera Model to Cisco SD IP Camera 2600**—To upgrade a Cisco IP camera 2500 to a Cisco IP camera 2600
- **Upgrade Camera Model to Cisco SD IP Camera Indoor Dome 2611**—Cisco IP camera 2421 to a Cisco IP camera 2611
- **Upgrade Camera Model to Cisco SD IP Camera Indoor Vandal Dome 2621V**—Cisco IP camera 252x to a Cisco IP camera 2621
- **Upgrade Camera Model to Cisco SD IP Camera Ruggedized Dome 2630V**—Cisco IP camera 253x to a Cisco IP camera 2630

Step 4 In the confirmation dialog box, click **OK**.

The system goes through the camera model upgrade process. This process may take some time to complete.

Step 5 After the upgrade completes, check motion detection window settings for the camera and make updates if needed.

Displaying IP/Network Camera Information

To display detailed information about a camera, click an underlined camera link on the IP/Network Cameras panel. Table 3-13 describes the camera information.

Table 3-13 IP/Network Camera Information

Item	Description
Details tab	
Preview Image	Shows a preview of the video image from the camera. Click **+** to enlarge the image and **–** to reduce the preview image size.
Camera Name	Displays the name assigned to the camera.

Table 3-13 IP/Network Camera Information (continued)

Item	Description
Camera Type	Displays the camera brand and model.
Server	Displays the name of the VSMS host to which the camera is connected
Host/IP Name	Displays the host name or IP address of the camera. Click the link to open the default configuration page for the camera (if available).
Health State	Indicates the status of the connection between the camera and VSOM. **Up** indicates that the connection is active. **Down** \ indicates that either the camera is down or there is a connection problem between VSMS and the camera.
Authentication	Indicates whether authentication is required to access the camera ("Yes" or "No"). If yes, the username for the camera also is displayed.
Analytics Configuration	If analytics is configured for the camera, click this link to access the web-based user interface for the camera. For information about this interface, including how to log in, see the *Cisco Video Analytics User Guide, Cisco 4000 Series Video Surveillance High-Definition IP Cameras*.
PTZ Information	Displays the PTZ configuration if PTZ is supported and enabled for the camera. Click a PTZ preset to move the camera to that preset location. Use the + and - icons below the video pane to enlarge or shrink the preview.
Camera Feeds tab	
Feed Name	Displays the name of the camera feed. Click the link to open the Camera Feed panel. See the "Managing Camera Feeds" section on page 5-6.
Media Type	Displays the media type of the camera feed. Media types include H264, JPEG, MPEG-2, MPEG-2 Elementary, MPEG-4, and H.263. Audio is embedded if the camera is MPEG ready. MPEG media types do not display a preview.
F/B Rate	Frame rate and bit rate, which determine the amount of video data transmitted in a given amount of time. Frame rate applies to MJPEG streams, and bit rate applies to MPEG-2 and MPEG-4 streams. Higher values result in smoother video and a more accurate representation of what is happening, but also result in increased system resource use.
Quality	Displays the video quality value for the camera feed. 1 is the lowest quality (highest compression) and 100 is the highest quality.
Camera Feeds tab	
Custom Fields	Displays the values for any custom fields that have been defined (see the "Creating Custom Field Labels for Cameras" section on page 3-18).

Table 3-13 IP/Network Camera Information (continued)

Item	Description
Rights tab	
Rights	Access rights for the device: • Name—Role name with a link that opens the Roles panel for the specified role. • Rights—Indication of the rights that are assigned to the role.

Configuring PTZ and Joystick Settings

Note PTZ functions require that Cisco IP/Network cameras be installed with a motorized zoom/focus lens and in a pan/tilt mount that supports the Pelco D protocol.

VSOM supports the movement, configuration, and control of analog PTZ cameras that are connected to video encoders or PTZ IP cameras. For cameras that support PTZ functionality, you can configure and use PTZ presets in addition to pan (left-right), tilt (up-down) and zoom (in-out) movements. Other camera options such as iris and focus settings also can be controlled, depending on the camera model.

Note PTZ presets are stored in the PTZ camera, not in VSOM or in encoders.

A PTZ camera is listed on the PTZ Configuration panel only if all of the following apply:

- The camera supports PTZ functionality
- PTZ functionality is enabled for the camera
- PTZ settings are configured

For information about enabling PTZ functionality, see the "Managing Analog Cameras" section on page 3-16 and the "Managing IP/Network Cameras" section on page 3-20. For information about configuring PTZ settings, see the "Configuring PTZ Settings" section on page 3-29.

When PTZ is enabled and configured, operators can use embedded PTZ controls or a USB joystick to quickly move a specified camera. See the "Using the Camera PTZ Controls" section on page 8-34.

Operators must choose the PTZ camera to control by clicking a video pane or selecting a radio button within the PTZ tool to transfer control from the previously controlled PTZ camera. The operator can also *lock* a camera using the Lock PTZ Source option on the Operator page. See the "Using the Camera PTZ Controls" section on page 8-34. If a camera is locked, the operator continues to control that camera, even if the feed from another camera is shown in the Display panel.

PTZ preset commands are mapped to USB joystick buttons, but not to mouse buttons. If the joystick has zoom controls, twist buttons 1 and 2 are mapped to zoom-in and zoom-out, and the rest of the buttons are mapped to presets in order. The Windows Game Controller in the Control Panel shows the numbers of the buttons if they are not labeled on the USB joystick.

You can enter preset labels on the PTZ Configuration panel for the IP/network or analog camera. VSOM supports the additional of up to 99 preset labels per camera.

Configuring PTZ Settings

Click PTZ Configuration on the side menu in the Administrator pages to open the PTZ Configuration panel. For a general description of tasks you can perform on this panel, see Table 3-1.

Before You Begin

- Determine the PTZ settings that are needed for each camera (only for cameras that support PTZ functions such as setting preset labels for a camera, setting up preset schedules, and associating PTZ actions for events.

To configure PTZ settings for a camera, follow these steps:

Procedure

Step 1 In the Administrator pages, click **PTZ Configuration**.

Step 2 Click the **Edit** icon in the Actions column for the camera.

Step 3 Choose from the **PTZ Status** drop-down list to enable or disable PTZ settings.

For the PTZ settings to be active, both the camera and the PTZ settings must be enabled.

Step 4 Configure pan and tilt settings by using the Pan and Tilt controls in the crosshair box and the vertical scale zoom controls to the right of the crosshairs.

To zoom in, move the cursor up on the vertical scale. To zoom out, move down.

Availability of the following PTZ settings depends upon the camera model:

- Focus—Toggle between a close-up view and distant view, or choose the Auto adjustment option, as determined by the camera capabilities.
- Iris—Toggle between the light and dark iris, or choose the Auto adjustment option.
- Night—Toggle between On (night) and Off (day), or choose the Auto focus option, as determined by the camera capabilities.
- Backlight—Turn backlighting on or off, as determined by the camera capabilities.
- Digital Zoom—Enable or disable digital zoom, as determined by the camera capabilities.
- White Balance—Activates an automatic mechanism to adjust for indoor and outdoor environments.
- Admin—Click the **INIT** button to send an initialization command to VSMS or click **Reset** to return the PTZ view to the default configuration. Depending upon the camera model, the INIT command can set the camera point to a default position or restart the PTZ driver.
- OSP—On-screen Programming (OSP) uses built-in camera menus overlaid on the video to configure settings for the camera. This setting is for use with analog cameras. These controls are visible only if the camera driver indicates that the camera may support OSP. For example, the Pelco D driver currently enables this option, but a specific Pelco camera model may not. Click **OSP** to enter OSP mode and display the controls in the preview window. Use the **Up** and **Down** buttons, up and down cross-hair virtual joystick controls, or up and down functions on an attached USB joystick (easiest) to navigate the on-screen menu in the video, and use **Select** and **Cancel** to enter or exit the current menu.

Note OSP is available only in the Administrator pages. In the Operator page, you can access different patterns that the camera supports, but cannot access OSP options.

- OSD—On-screen Display (OSD) provides the following controls for Kalatel Cyberdome 1 and 2 camera models. The controls that appear depend on the Kalatel camera model. For related information about the Kalatel camera OSD, see your camera documentation.
  - **Menu**—Click to enter the OSD for the Kalatel camera
  - **Prev**—Click to go to the previous OSD screen
  - **Next**—Click to go to the next screen in the Programming menu
  - **Exit**—Click to enter the OSD
  - **Help**—Click to display help text for the OSD
  - **Up**, **Left**, **Right**, **Down**—Click to navigate through the OSD and to perform other activities as applicable in the OSD
  - **0** through **9**—Click to designate the corresponding digit in the OSD
  - **Clear**—Click to clear information and to perform other activities as applicable in the OSD
  - **Set**—Click to confirm information as applicable in the OSD

  For related information about using the OSD for your camera model, see the Readme file that is provided with the driver pack for your camera.
- Patterns (cameras that support the Pelco D protocol)—A pattern is a range of motion over a field of view that you can save as a recorded pattern on the camera, if the camera supports this capability (for example, Pelco Spectra IV cameras support patterns). In VSOM, you can record a pattern by moving the joystick over a field of view and performing PTZ actions while recording. You can then save the resulting pattern. You may be able to save up to eight patterns, depending on the camera model. After a pattern is saved, you can associate the patterns to schedules.

  To add or edit a PTZ pattern:
  - Choose a PTZ pattern from the drop-down menu (up to eight patterns may be available).
  - Click **Record** to record the pattern and **Stop** to stop the recording.

  The pattern is saved on the camera and played back when you click **Go**.

Note Pattern recording is available only on the Administrator pages. Operators can play back but not record patterns. Some cameras may not support this feature. See your camera documentation for information regarding the pattern feature.

Step 5 Choose the following PTZ settings for the mouse and joystick:

- Pan (x)—Choose a relative speed for moving across the image in response to mouse or joystick input (range 0 to 100, 100 fastest).
- Tilt (y)—Choose a relative speed for tilting the image in response to mouse or joystick input (range 0 to 100, 100 fastest).
- Zoom (z)—Choose a relative speed for zooming the image in response to mouse or joystick input (range 0 to 100, 100 fastest).

Step 6 Set the PTZ preset configuration:

- Use the PTZ crosshairs function or use the mouse to pan to the required view. When the position is attained, enter a description for the first preset label (for example, West Lobby, or East Staircase).

- Click the **Set Preset** button to save the parameters. Zoom levels are maintained for the created preset. Preset labels should indicate the camera view or location. Click **Test** to show and then reset a current preset view.

  Repeat the actions that this step describes to set additional presets.

Step 7 Click the **Schedules** tab and specify the following options to assign a PTZ preset according to a schedule.

Note Schedules are available only if they are preconfigured by using the Schedules settings and the camera is PTZ-ready. See the "Managing Schedules" section on page 6-16.

- Enable—Activate the specified schedule.
- Simple Schedule—Choose a predefined simple schedule from the drop-down list.
- Recurring Schedule—Choose a predefined recurring schedule from the drop-down list.
- Default State Preset—Choose the default preset to use when the video appears.
- Default State Pattern—Choose the default pattern to use if a schedule is not in effect. After the scheduled time, the pattern reverts to the default.
- Active State Preset—Choose the preset to use when the video is active.
- PTZ Priority—Determine the PTZ priority this camera has relative to other cameras with set PTZ priorities. This functionality is used for simultaneous attempts to control the same PTZ camera. The command with the highest PTZ priority prevails and the others are blocked.

Step 8 To add preset schedules, click **Add Another Preset** and configure the settings described in Step 7.

Step 9 Click the **Rights** tab and verify the access designations.

For information about assigning rights, see the "Adding a Role" section on page 7-8.

Step 10 Click **Finished** to save the settings.

Managing Monitors

Digital monitors are used as displays for predefined views. Views can be sent to a digital monitor either manually or automatically via Event Actions.

The Virtual Matrix client allows security managers and operators to select and control video displayed on digital monitors. When you install the Virtual Matrix client on a PC, you can define a single monitor or multiple monitors for the PC. For example, each operator might have a PC with a single Virtual Matrix client, while the manager has a PC with two Virtual Matrix clients, one for normal operations and one to display the video that results when an event is triggered.

For information on installing and configuring the Virtual Matrix client see *Cisco Video Surveillance Virtual Matrix Client Configuration Guide*.

Adding a New Monitor

Use the Monitor panel to configure the screens that display camera feeds and archives.

Before You Begin

- Add a VSVM to your VSM deployment. See the "Adding a New Server" section on page 3-5.
- If your installation has multiple monitors, determine a naming and numbering convention. See the "Organizing Information in VSM" section on page 1-7.
- Determine the layout to use for each monitor.

To add a monitor, follow these steps:

Procedure

Step 1 In the Administrator pages, click **Monitors**.

Step 2 Click **Add a New Monitor**.

If there are no VSMS hosts defined, an error message appears, indicating that you must first define a server. Follow the instructions in the "Adding a New Server" section on page 3-5 and then return to the Monitors page.

Step 3 In the Monitor Number field, enter an optional number to identify this monitor.

Step 4 In the Monitor Name field, enter a descriptive name for the monitor that is consistent with your naming conventions (up to 30 characters, including spaces).

Step 5 (Optional) In the Description field, enter applicable information about the monitor, such as location or type (up to 1,024 characters, including spaces).

Step 6 Choose a server name from the **Virtual Matrix** drop down list.

The servers are configured on the Servers panel, as described in the "Managing Servers" section on page 3-5.

Step 7 In the Seed View area, choose the predefined view to be displayed on the monitor.

For information about configuring views, see the "Managing Predefined Views" section on page 5-24.

Step 8 Click the **Rights** tab and verify the access designations. See the "Adding a Role" section on page 7-8.

Step 9 Click **Submit**.

Editing or Deleting a Monitor

You can edit or delete monitor settings on the Monitors panel.

To edit settings, click the **Edit** icon in the Actions column and then make changes on any of the tabs. See the "Adding a New Monitor" section on page 3-32 for information on the available settings.

To delete a monitor from the VSOM database, click the **Delete** icon for the monitor. Check the check box if you want to keep the monitor setup information on the server, and then click **Yes**.

Displaying Monitor Information

Click an underlined monitor name link on the Monitors panel to display detailed information about the monitor, as described in Table 3-14.

Table 3-14 Monitor Information

Item	Description
Monitor Information	Displays the following information; • Monitor Number—Optional number that identifies this monitor within a group of monitors. • Monitor Name—Assigned monitor name. • VSVM Client Viewer Name—Assigned name for an associated Virtual Matrix client. • Virtual Matrix Server—VSVM that controls this monitor. Click the link to open the server information panel for the monitor. See the "Displaying Server Information" section on page 3-8.
Current View	Displays the following information: • Dwell time—Amount of time in seconds between switching rotating camera feeds, or Do Not Tour if the view does not rotate between camera feeds. A rotating view is one in which camera feeds are displayed on a rotating basis in one or more video panes. • Layout—Operator page layout used for the monitor • Fixed Windows—Number of fixed windows in the Operator page layout • Rotating Source List—List of camera feeds that are displayed on a rotating basis. Camera rotation refers to the process of changing the camera feeds that are displayed by cycling through the list of camera feeds.
Rights tab	
Rights	Access rights for the device: • Name—Role name with a link that opens the Roles panel for the specified role. • Rights—Indication of the rights that are assigned to the role.

CHAPTER 4

Utilities

This chapter describes the utilities that are included in VSOM and that can aid in system management.

This chapter includes these topics:

Exporting Data from the Administration Pages

You can export the data on any of the VSOM Administration pages that include a table with an Export icon . When you export data, the system saves it in a comma separated value (CSV) format that you can open with a spreadsheet program, such as Excel, or a text editor.

To export data, click the **Export** icon . When the system prompts you to save the information, click **Save** and specify a file name and location.

Managing Software and Downloads

The Software and Downloads page contains links for downloading VSM software and documentation. To display this page, click the **Software and Downloads** link under Utilities in the Admin pages.

Table 4-1 describes the available downloads.

Table 4-1 Software and Download Tasks

Task	Description
Download a PDF version of *Cisco Video Surveillance Operations Manager User Guide*	Download this guide in PDF format.
Download the Virtual Matrix client	The Virtual Matrix client allows you to control the video that is displayed on your computer. See *Cisco Video Surveillance Virtual Matrix Client Configuration Guide* for more information.

Table 4-1 Software and Download Tasks (continued)

Task	Description
Download the VSOM video client	The VSOM video client is an ActiveX control that allows you to play back videos without being logged in to VSOM. The client is installed automatically when you open the Operator page for the first time.
Download the VSOM Install-less video client	The VSOM video client is an ActiveX control that allows you to play back videos without being logged in to VSOM. With the install-less version, you can play video on a PC even if the VSOM video client is not installed on the PC. See *Cisco Review Player User Guide* for more information.
Download Smart Search	The Cisco Smart Search application allows you to quickly search through large video archives. It is used primarily for forensic purposes and allows scanning of video archives based on specified parameters. See Chapter 9, "Using Smart Search." Smart Search is installed automatically if you click the **SmartSearch** icon on the Operator page.
Logos	The logos are used if the VSOM skins are changed. See the "Configuring System Settings" section on page 6-18.

Managing the VSOM Database

The VSOM database contains all of the configuration information that is accessible from the VSOM Administration pages, including device, video feed, account, and system information. Cisco recommends that you back up the database on a regular basis to ensure that configuration information is not lost in the event of system failure or disruption. The appropriate frequency of backups depends on how often you change the VSOM configurations. You can perform backups at any time.

VSOM supports the following backup options:

- Back up the database on demand using the Database Backups page. See the "Backing Up the Database" section on page 4-2.
- Set up scheduled backups using Settings page. See the "Configuring System Settings" section on page 6-18.

Because backups are created on the VSOM host on which you specify a backup, make sure that you create a process to copy the backups to another system on a regular basis.

Backing Up the Database

Open the Database Backups panel to manage backups of the VSOM database. When you request a backup, the VSOM database is backed up to a tar.gz file with a and given a name in the following format:

VSOM_<*server*>_backup_<*yyyy*><*mm*><*ddxxxxxx*>.tar.gz

where:

- <*server*> is the host name of the VSOM server
- <*yyyy*> is the year, <*mm*> is the month, and <*dd*> is the date that the backup is created

- <*xxxxx*> is a unique system-generated identifier

Table 4-2 describes the functions that you can perform on the Database Backups panel.

Table 4-2 Database Backup and Restore Tasks

Task	Description
Create a backup for download	Create a database backup file (tar.gz file) to save on your local computer or another computer on your network. Click **Create a backup for download** and then click **Save** to save the backup file.
Create a configuration-only backup for download	Create a backup file of the VSOM configuration (tar.gz file) to save on your local computer or another computer on your network. This backup does not include the database. Click **Create a configuration-only backup for download** and then click **Save** to save the backup file.
Create a backup on the VSOM server	Create a backup tar.gz file to save on the VSOM server. Click **Create a backup on the server**. The server backup is created and added to the list of backups on the Database Backups panel.
Download a previously created backup	Click the **Download** icon for the backup file and then click **Save**.
Delete a previously created backup	Click the **Delete** icon for the backup file.
Delete multiple previously created backup	Check the check boxes for the backup files and choose **Edit > Delete Selected**.

Restoring the Database

You can restore the database from the backup file stored on the VSOM server or copy a backup file from another machine to the VSOM server. For instructions see *Cisco Video Surveillance Manager Installation Guide*.

CHAPTER 5

Managing Video Feeds

This chapter describes how to use the VSOM Video Feeds area to set up and manage camera groups and feeds, import camera configurations into VSOM using batch administration, and set up archives and predefined views.

This chapter includes these topics:

About Video Feeds

Video feeds are the flows of video from your surveillance cameras or from archives that are stored in VSOM. Camera feeds are video feeds directly from a camera.

This section describes the tasks that you can perform on the Video Feeds panels in the VSOM Administration pages.

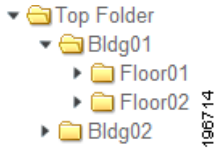
- Set up camera groups to display and work with camera feeds that have common characteristics such as location or model. See the "Managing Camera Groups" section on page 5-2.
- Display or customize camera feeds. See the "Managing Camera Feeds" section on page 5-6.
- Import new cameras and encoders into a VSM system using batch administration. See the "Performing Batch Administration Functions" section on page 5-11.
- Set up video archives to store camera feeds for a specified time. See the "Managing Archives" section on page 5-17.
- Set up views to display camera feeds in the Operator page. See the "Managing Predefined Views" section on page 5-24.

To access the Video Feeds panels, open the Administrator pages and choose items under Video Feeds in the side menu.

Managing Camera Groups

Camera groups allow you to display and work with cameras feeds that have common characteristics, such as location or type. Camera groups are organized hierarchically under the Top Folder. By default, all cameras are in the Top Folder group unless they are placed into another camera group or groups. The resulting hierarchy may include multiple levels of parent and child camera groups. For example in Figure 5-1, Bldg01 is a child folder relative to the Top Folder and the parent of the Floor01 and Floor02 folders.

Figure 5-1 Camera Groups Hierarchy



Cisco recommends that you create camera groups as appropriate for your deployment and place cameras into the groups when you add the cameras to VSOM.

You can manage camera groups using either the drag-and-drop interface or the search-based interface, both of which are accessible from the Group Overview menu item in the side menu in the Administrator pages. The interfaces are compatible, and you can use then interchangeably.

Best Practices

- Use the drag-and-drop interface for initial setup of camera groups. The drag-and drop interface allows you to easily add and organize camera groups and displays the camera group folder hierarchy clearly.
- Use the drag-and-drop interface on an ongoing basis if you have a small number of cameras to manage.
- Use the search-based interface to add cameras to camera groups if you have many cameras and a consistent naming convention that makes searching convenient. For example, if your cameras are named by location with prefixes BLDG01-, BLDG02-, and so on, you can easily search for cameras with those prefixes and add them to appropriate camera groups.

Table 5-1 describes the camera group management tasks that you can perform.

Table 5-1 Camera Group Management Tasks

Task	Description	Reference
Use drag-and-drop to manage camera groups.	Add, modify, or delete groups of camera feeds. Add camera feeds as members of camera groups or delete feeds from camera groups.	Managing Camera Groups by Using the Drag-and-Drop Interface, page 5-3.

Table 5-1 Camera Group Management Tasks (continued)

Task	Description	Reference
Use the search-based interface to manage camera groups.	Add, modify, or delete groups of camera feeds. Add camera feeds as members of camera groups or delete feeds from camera groups.	Manage Camera Groups by Using the Search-Based Interface, page 5-5.
Edit settings for multiple camera feeds.	Make changes to multiple camera feeds at one time.	Editing or Deleting a Camera Feed, page 5-8.

Managing Camera Groups by Using the Drag-and-Drop Interface

The drag-and-drop interface for camera groups allows you to set up initial camera groups, move cameras in and out of groups, and edit basic information for all of the cameras in a group at one time. Choose **Group Overview > Drag-and-Drop Camera Groups** to open the Drag-and-Drop Camera Groups panel.

For operations that affect many cameras, you might find it more convenient to use the search-based interface, as described in the "Manage Camera Groups by Using the Search-Based Interface" section on page 5-5.

This section describes how to set up camera groups using the drag-and-drop interface and add cameras to the groups.

Before You Begin

- Determine the camera groups that you want to create and which camera feeds to add to the groups.
- Choose a naming convention for the camera groups. See the "Organizing Information in VSM" section on page 1-7.

To create a camera group and add cameras to it by using the drag-and-drop interface, follow these steps:

Procedure

Step 1 In the Administrator pages, click **Group Overview**.

Step 2 Click **Drag-and-Drop Camera Groups**.

Step 3 Click the camera group that is the parent group (shown with a folder icon), or click the arrow for Top Folder if there is no parent group.

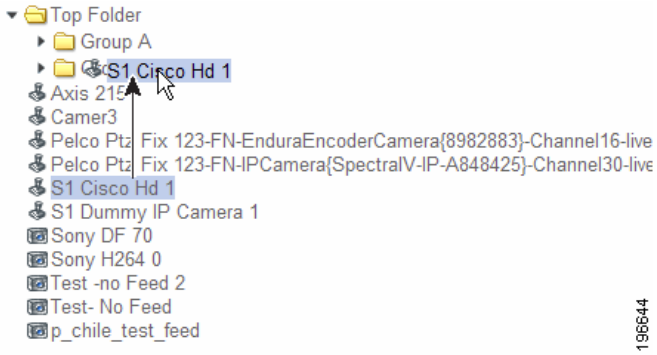
Step 4 Choose **Group > Add Group**, enter the group name, and click **OK** to add the camera group.

Step 5 Repeat Step 2 and Step 3 to add additional camera groups as needed.

Step 6 To add a camera to a camera group, locate the camera in the list on the left side of the Drag-and-Drop Camera Groups panel and drag it to the group folder.

Figure 5-2 shows how to drag and drop a camera into a group.

Figure 5-2 Using the Drag-and-Drop Interface to Add Cameras to a Group



Step 7 Repeat Step 6 to add more cameras to the camera group.

Modifying and Deleting Camera Groups and Feeds

To rename a camera group on the Drag-and-Drop Camera Groups panel, highlight the group and choose **Group > Rename Group**. Enter the new name, and click **OK**.

To remove a camera group, highlight the group and choose **Group > Delete Group**. A prompt indicates that any subgroups or camera feeds will be moved back to the Top Folder. Click **OK** to acknowledge the message and complete the removal.

To modify settings for multiple camera feeds at one time by using the drag-and-drop interface, follow these steps:

Procedure

Step 1 In the Administrator pages, click **Group Overview**.

Step 2 Click **Drag-and-Drop Camera Groups**.

Step 3 Drag the cameras and camera groups from the column on the left to the area on the right of the panel.

Step 4 Click **Batch Edit** to open an editing window to modify any of the following settings:

- In the Name field, you can modify the camera name. For example, you could add a prefix to all of the cameras in a specific camera group.
- In the Camera No. field, enter a unique camera number. When multiple operator workstations are in use, Cisco recommends that each workstation use a unique camera number and feed name.
- In the Description field, you can enter or modify descriptions for the camera.

Step 5 Click **Submit** to save the changes and return to the Drag-and-Drop Camera Groups panel.

Step 6 To remove the list of cameras specified for batch editing, click **Clear List**.

Clearing the list does not remove the cameras from the list on the left, only from the list of cameras intended for batch edit on the right side of the panel.

Manage Camera Groups by Using the Search-Based Interface

The Search-Based Camera Groups panel allows you to perform operations on multiple camera groups or camera feeds at one time. Choose **Group Overview > Search-based Camera Groups** to open the panel.

Note For initial setup of camera groups, Cisco recommends that you use the drag-and-drop interface, as described in the "Managing Camera Groups by Using the Drag-and-Drop Interface" section on page 5-3.

In the camera list on the panel, numbers in parentheses following the camera group name indicate the number of groups and cameras within that group. For example, (5/20) indicates that there are 5 groups in the specified group and that a total of 20 cameras in the group.

Table 5-2 lists the tasks you can perform on the Search-Based Camera Groups panel.

Table 5-2 Tasks for Search-Based Camera Groups

Task	Steps	Description
Show or hide the side menu	Click **Toggle**.	Shows or hides the side menu.
Adjust the height of the panel window	Click the **Larger** or **Smaller** link repeatedly to resize the preview window while keeping the same aspect ratio.	Make the camera groups and preview window areas bigger or smaller.
Check feed matches	Enter a search string and click **Check Feed Matches** to display the matching feed entries.	Display the camera feed entries that match the search string. Matching is case-sensitive, and wild card characters are not permitted.
Uncheck camera feeds	Click **Uncheck All**.	Unchecks all previously checked cameras in all camera groups. The camera groups remain checked.
Add a camera group	Enter a new camera group name and click **Add Group**.	Adds a new camera group within the specified camera group.
Change a camera group name	Choose a camera group from the list, enter the new name, and click **Update Group Name**.	Changes the name of the camera group.
Copy feeds to a specified camera group	1. Click the radio button for the camera group to receive the copies. 2. Click the camera feeds that you want to copy. 3. Click the **Copy Feeds** button  to copy the specified feeds to the specified camera group.	Copies the feeds to the specified camera group.

Table 5-2 Tasks for Search-Based Camera Groups (continued)

Task	Steps	Description
Move camera feeds to a specified camera group	1. Click the radio button for the camera group to receive the copies. 2. Choose the camera feeds that you want to move. 3. Click the **Move Feeds** button to move the feeds from the current location to the specified camera group.	Moves the feeds from the current location to the specified camera group.
Delete a camera group	1. Click the radio button for the camera group. 2. Click the **Delete Group** button . 3. Click **OK** to confirm.	Removes a camera group. Cameras that are in only that group are moved to the Top Folder.
Delete camera feeds	1. Check the check boxes for the camera feeds. 2. Click the **Delete Feeds** icon . 3. Click **OK** to confirm.	Removes the camera feeds from the specified camera group, but keeps the feeds in the system and in any other camera groups to which they are assigned.

Managing Camera Feeds

A camera feed is the stream of video from a camera. When a camera is added to VSOM, the associated camera feed is added automatically and assigned the same name as the camera. Unless you require additional changes to the camera feeds, you do not need to configure them individually. All of the needed configuration is supplied automatically when the camera is added.

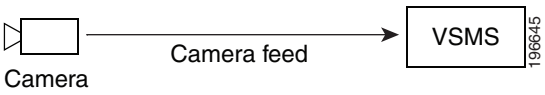
VSOM supports the following camera feed configurations:

- Simple Configuration, page 5-6
- Dual Streaming Configuration, page 5-7
- Child Feed Configuration, page 5-7

Simple Configuration

In the simple camera feeds configuration, a VSMS manages a camera that has a single camera feed. Figure 5-3 illustrates this arrangement.

Figure 5-3 Simple Camera Feed Configuration

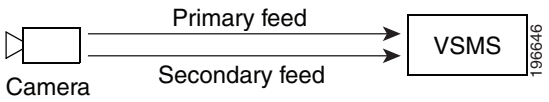


Dual Streaming Configuration

In the dual streaming camera feeds arrangement, a VSMS manages a camera that supports and has dual streaming enabled. The camera generates both a primary and a secondary feed (which may be at lower resolution than the primary feed). Batch administration is supported to add the camera with the primary feed; however, you must set up the secondary feed individually.

You can improve operational efficiency with dual streaming cameras by setting up multiple views in VSOM. For example, you can set up a normal operational view with the lower resolution secondary feed, and then switch to a view of the higher resolution primary stream to examine video more closely following an event trigger.

Figure 5-4 Dual Streaming Camera Feed Configuration



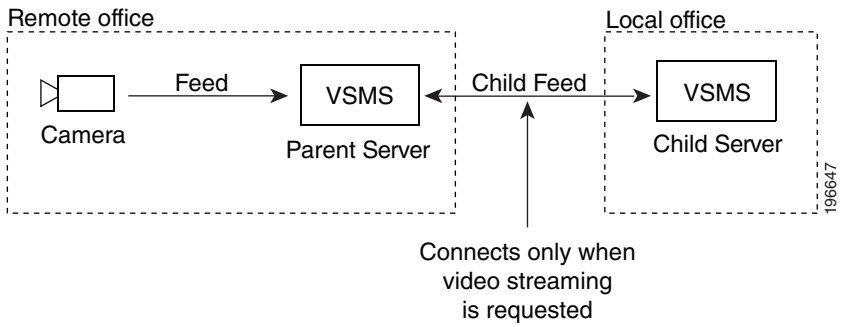
Child Feed Configuration

In a child feed configuration, a VSMS is connected to a camera and to another VSMS. The VSMS that directly manages the camera serves as the source or parent for that camera feed, and the other VSMS serves as the child. The child feed is the video stream that is sent from the first VSMS to the second. A parent camera feed can be on the same host as the child feed or on another host.

Child feeds can contribute to effective network utilization by allowing you to distribute video feeds closer to the video monitors that display the video. Efficient utilization is important in environments such as remote branch offices where limited network bandwidth is available for video delivery. By sending a single video feed to a location with several monitors, you can reduce the bandwidth requirements over the limited network. To conserve bandwidth, the child feed connects only when video streaming is requested.

Figure 5-5 shows an example in which the camera and VSMS are in a remote office, and a child feed is set up between the VSMS in the remote office and the VSMS in the local office.

Figure 5-5 Child Feed Configuration



A child feed inherits the same resolution, quality, and media type of its parent; however, in the case of MJPEG video streams, you can configure a lower frame rate for the child feed. Batch administration is not supported for adding child feeds.

Note To add cameras, see the "Adding a New Analog Camera" section on page 3-17 and the "Adding a New IP/Network Camera" section on page 3-21.

Configuring a Camera Feed

The Camera Feeds page displays the available camera feeds in the system. The default camera feed names are derived from the camera names.

If possible, avoid changing the names of your camera feeds from the default names. If you need to change the name of a camera or camera feed, make the same change to both the camera and the camera feed records.

To prevent users from having PTZ access when using child feeds, grant permission to display the child feed but not the parent.

Before You Modify Camera Feeds

- Make sure that camera groups are set up. See the "Managing Camera Groups" section on page 5-2.
- Make sure that all the cameras are added to the system. See the "Performing Batch Administration Functions" section on page 5-11.

Click **Camera Feeds** on the side menu in the Administrator pages to open the Camera Feeds panel. Table 5-3 lists the tasks you can perform on this panel.

Table 5-3 Camera Feeds Panel Links and Buttons

Item	Description	Reference
Edit names or descriptions multiple feeds.	Choose one or more items in the list and click **Edit** to modify the specified items.	—
Edit settings for a specified camera feed.	Allows you to modify feed information, camera group membership, and rights for a specified camera feed.	Editing or Deleting a Camera Feed, page 5-8.
Delete a specified camera feed.	Allows you to remove a specified camera feed from the VSOM database.	Editing or Deleting a Camera Feed, page 5-8.
Create a new child feed.	Create a new camera feed based on an existing camera feed.	Adding a Child Camera Feed, page 5-10.

Editing or Deleting a Camera Feed

To edit camera feed settings, click the **Edit** icon for the camera feed in the Actions column on the Camera Feeds panel and modify any of the settings that Table 5-4 describes.

To delete a camera feed from the VSOM database, click the **Delete** icon . The system provides you with the option of keeping the following items on the server. Check the check boxes for the items to retain on the server, and click **Yes**.

- Leave archive data files on the server(s)—Does not delete archive files for the deleted item from the server.
- Keep event history records from this device—Does not delete event history records for the deleted item from the server.

Table 5-4 Camera Feed Settings

Item	Description
Feed Info tab	
Camera Number	Enter an optional, unique camera number to identify the camera within a group of cameras. When multiple operator workstations are in use, Cisco recommends that each workstation use unique camera numbers and feed names.
Feed Name	Specify a name for the feed that is consistent with your naming convention.
Description	Enter an optional description of the camera feed.
Server	Choose the server to manage the camera feed.
Stream Type	Indicates whether the stream is a direct or child stream.
Frame Rate or Bit Rate	If the **Bitrate** drop-down list appears, choose the bit rate for the video stream from the camera. The Bitrate drop-down list appears only if you chose MPEG-2, MPEG-4, or H.264 for the media type. If the **Frame Rate** drop-down list appears, choose the frame rate per second for the video stream from the camera. The Frame Rate drop-down list appears only if you chose JPEG for the media type. Higher values represent more video data every second, which means smoother video and a more accurate representation of what is happening. However, higher values result in higher bandwidth load and larger archive file sizes.
VBR	Indicates whether support for variable bit rate (VBR) is enabled or disabled (only for cameras that support VBR).
Camera Groups tab	
Camera Groups	Add this camera to a camera group, or choose Top Folder (No Group) to indicate that you are not placing the camera in a group. Click a camera group link to display the subgroups and feeds in the group. See the "Managing Camera Groups" section on page 5-2 for more information about camera groups.
Rights Tab	
Rights	Verify the access rights for this server: • Name—Role name with a link that opens the Roles panel for the specified role. • Rights—Indication of the rights that are assigned to the role.

Adding a Child Camera Feed

A child feed is a stream of video from a camera that is sent by one VSMS to another. In a child feed configuration, a VSMS is connected to a camera and also to another VSMS. The main camera feed is the video stream that is sent to the first VSMS, and the child feed is the video stream that is sent from the first VSMS to the second. See the "Child Feed Configuration" section on page 5-7.

Note To add dual streams from the Steam Manager encoder, log in to Cisco Stream Manager Configuration. Enable the secondary stream first. You can then add the secondary stream in VSOM Administration page using the 1_1 and 1_2 channels.

Use the Camera Feeds panel to add a child feed to an existing camera feed.

To add a new child feed, follow these steps:

Procedure

Step 1 In the Administrator pages, click **Camera Feeds**.

Step 2 Click **Create a New Child Feed**.

Step 3 In the Camera Number field, enter an optional, unique camera number to identify the camera within a group of cameras.

Step 4 In the Feed Name field, enter a name that is consistent with your naming conventions (up to 30 characters, including spaces).

Step 5 (Optional) Enter a description of the feed (up to 1,024 characters, including spaces).

Step 6 From the **Server** drop-down list, choose the server to manage the child feed.

Step 7 From the **Parent Source** list, choose the camera to use as the source of the feed.

Click **Expand All** to show the cameras in all camera groups or **Collapse All** to hide all of the camera group members.

Step 8 In the Media Setup section, specify the following:

- JPEG camera—Choose the frame rate for the video stream from the camera. The Frame Rate drop-down list appears only if JPEG is the media type.
- MPEG-2, MPEG-4, or H.264 camera—Choose the bit rate for the video stream from the camera. The Bitrate drop-down list appears only if MPEG-2, MPEG-4, or H.264 is the media type.

Step 9 Click the **Camera Group**s tab and check the check boxes for the camera groups to which you want to add this feed, or choose **Top Folder/No Group** to indicate that you are not placing the camera in a camera group.

Click a camera group link to display the subgroups and feeds. See the "Managing Camera Groups" section on page 5-2 for more information about camera groups.

Step 10 Click the **Rights** tab and verify the access designations.

See the "Adding a Role" section on page 7-8.

Step 11 Click **Submit**.

Enabling Motion Detection

The ability to detect motion is a function encoding source device (IP camera or encoder), which identifies movement based on pixel changes within the image. You must enable motion detection to be able to set up events that respond to physical movement. For additional information about motion detection as it relates to events, and instructions for setting up motion detection events, see the "About Motion Detection Events" section on page 6-10.

You enable motion detection for a feed from a camera or encoder. When dual streaming, motion detection can be supported on only one feed.

Before You Begin

- Identify which of your installed encoding source devices support motion detection.

To enable motion detection for a camera feed on a camera, follow these steps:

Procedure

Step 1 In the Administrator pages, click **Camera Feeds**.

Step 2 Click the **Edit** icon in the Actions column for the feed.

Step 3 Check the **Enable Motion Detection** check box.

Step 4 Click **Submit**.

The camera feed is now set up to support motion events. See the "About Motion Detection Events" section on page 6-10.

Performing Batch Administration Functions

Batch administration is the recommended method for adding multiple cameras and encoders to the VSOM database. You can populate an Excel spreadsheet with camera and encoder settings and then import the information in the spreadsheet into VSOM. After importing cameras and encoders, you can modify settings by making entries on the Batch Administration panel.

The result is the same as if you add or modify cameras and encoders using Encoders, Analog Cameras, and IP/Network Cameras panels, as described in the "Managing Encoders" section on page 3-12, the "Managing Analog Cameras" section on page 3-16, and the "Managing IP/Network Cameras" section on page 3-20. The advantage of using batch administration is that you can add multiple cameras or encoders at one time and make changes from a single panel.

Batch administration import does not support child feeds. You must set up child feeds individually after importing the cameras. See the "Adding a Child Camera Feed" section on page 5-10.

For cameras that support motion detection, the default motion settings are included when you import the camera using batch administration. You cannot change the default motion settings on the Batch Administration page. To modify the default settings, see the "Setting Up Windows for Motion Detection" section on page 6-14.\

The Batch Administration page lists only the archives that were created using batch administration. You can create new archives or modify some settings (such as media type) for archives that were created using batch administration, but you cannot view or modify archives that were created elsewhere in VSOM.

This section describes how to use the Batch Administration panel to perform the following tasks:

- Import cameras and encoders—See the "Managing Archives" section on page 5-17.
- Perform other batch administration tasks—See the "Performing Other Batch Administration Tasks" section on page 5-16.

Importing Cameras and Encoders Using Batch Administration

VSOM allows you to copy and paste values from an Excel spreadsheet template into the Batch Administration page. You can download the template, enter the camera configuration, and then copy the results into the Batch administration page.

The template includes the following worksheets:

- CameraSetup—Use this worksheet to enter camera configuration information for multiple cameras. The worksheet includes drop-down lists from which you can choose appropriate parameters based on camera types and models. When naming cameras and encoders, follow the guidelines in "Organizing Information in VSM" section on page 1-7.
- Glossary—Open this worksheet to review camera parameters and values.

To import and encoders using batch administration, follow these steps:

Procedure

Step 1 In the Administrator pages, click **Batch Administration**.

Step 2 Click the **spreadsheet template** link at the top of the page and right-click to save the latest template on your computer.

Note Make sure that you download the latest template from the Batch Administration page. Templates from previous releases may not be compatible.

Step 3 Open the spreadsheet template and choose **Save As** to save the template as a .xls file on your local computer.

Step 4 Make sure that macros are enabled in the xls file.

Note The batch administration copy and paste feature works only if macros are enabled in the spreadsheet.

Step 5 Add configuration information for the cameras that you want to add to VSOM on the CameraSetup worksheet of the xls file.

Use separate spreadsheet templates for the cameras that are managed by different VSMS hosts.

The spreadsheet includes drop-down lists to help you specify the supported parameters. Table 5-5 describes the parameters. They also are also included on the spreadsheet Glossary tab.

Step 6 Test the copy and paste process before using it to import multiple cameras:

a. Choose a single row in the spreadsheet, and click **Copy for Import** to copy it. A pop-up message indicates that the rows have been copied for import.

- Do not copy rows, headings, or other non-camera data into the Batch Administration page. If you do, VSOM generates an error when you try to save the data on the panel.
- You must use the **Copy for Import** button, not the Copy menu item on the Edit menu.

b. On the Batch Administration page, click in the **Add A New Record** field, and press **Ctrl+V** to paste the copied information.

The new camera is automatically added to the table on the Batch Administration panel.

c. Any errors are listed on the panel. Modify the spreadsheet as needed to address the errors and repeat the testing steps if needed.

Step 7 When you have verified that you can successfully import a row of the spreadsheet into VSOM (Step 6), you are ready to import multiple entries.

You can import up to 20 devices at one time; however, Cisco recommends that you import a maximum of 10 devices at one time to limit the amount of time that it takes to troubleshoot any issues that arise.

a. Choose the rows and click **Copy for Import** to copy them. A pop-up message indicates that the rows have been copied for import.

- Do not copy rows, headings, or other non-camera data into the Batch Administration page. If you do, VSOM generates an error when you try to save the data on the panel.
- You must use the **Copy for Import** button, not the Copy menu item on the Edit menu.

b. On the Batch Administration page in VSOM, click in the **Add A New Record** field, and press **Ctrl+V** to paste the copied information.

The new cameras are automatically added to the table on the Batch Administration panel.

Step 8 Choose the entries you want to save and click **Save Selected**.

Step 9 Click the **Verify Feed** icon  for each camera to verify that the expected video is shown.

Step 10 Edit or delete any rows that have reported errors. To remove blank rows or other non-camera entries from the list on the Batch Administration page, choose the entries and click **Delete Selected**.

Table 5-5 Batch Administration Parameters

Item	Description	Type of Value
Name	Name that identifies the camera.	text
Source Type	For IP/network cameras, a list of camera models. For analog cameras, a list of encoders.	Automatically populated from the supported device types in VSOM.
Description	Text description of the camera.	text
Hostname/IP Address	For IP/network cameras, the hostname or IP address of the camera. For analog cameras, the IP address of its encoder.	text
User Name	User ID for access to the camera, if the camera supports log in.	Alphanumeric text

Table 5-5 Batch Administration Parameters (continued)

Item	Description	Type of Value
Password	Optional password for access to the camera, if the camera supports log in.	Alphanumeric text
Channel	Encoder port (analog camera) or numeric identifier for the feed (IP/network camera)	Integer value
Media Server	VSMS for the VSMS that manages the camera.	Integer value
Media Type	Video format.	MPEG-4, JPEG
Format	Media format.	NTSC, PAL
Resolution	Video resolution of the camera feed.	Fixed set of options from drop-down list
Transport	Transport protocol for the camera feed.	TCP, UDP
Multicast Address	Multicast address used if UDP is the transport mechanism for communication with the camera.	
Framerate/Bitrate	Frame rate or bit rate of the camera feed (seconds).	Frame rate: 30, 29, …, 1 Bit rate: 56, 128, 255, 256, 384, 511, 512, 640, 768, 1024, 1500, 2000, 3000, 4000, 5000, 6000, 8000, 10000, 12000, 15000
Quality	Setting that determines the quality of an MJPEG feed. Higher values represent higher quality frames, but also result in higher file sizes and greater bandwidth load on your network. For optimal performance in most networks, we recommend the value 50. If the camera supports VBR, you can use the Quality column to specify whether or not the bit rate is variable. If Quality is 0, CBR is used. **Note** When adding Cisco cameras using batch administration, you must use the following range of quality values: CBR (0-100) and VBR (101-200).	Integer: 0 through 100
PTZ	Indication of whether PTZ functionality is enabled (not supported for analog cameras).	Check box
Archive	Indication of whether an archive is created automatically.	Check box

Table 5-5 Batch Administration Parameters (continued)

Item	Description	Type of Value
Archive Duration (days)	Duration for a continuous archive (such as 1 or 1.5 days).	Numeric value
Archive Expiration	Days after which the archive expires. Forever means that the archive does not expire.	1, 2 Week(s), 1, 2, 3, 6 Month(s) 1 Year, Forever
Motion Configuration	Indication of whether VSOM sets up a motion configuration event (0 = no and 1 = yes). If you create a motion configuration event, VSOM creates a default window that covers the full video pane, using default settings. To modify the settings, you must use the Events page. See the "Setting Up a Motion Detection Event" section on page 6-11.	Check box
Reuse Archive for Motion	Indication of whether the original archive is used for the motion event	Check box
Motion Archive Expiration	Time after which the motion archive expires. Disabled when Reuse Archive for Soft is specified (see below in this table). Forever means that the archive does not expire.	1, 2 Week(s), 1, 2, 3, 6 Month(s) 1 Year, Forever
Soft Trigger	Text that you enter to create a soft event trigger. A soft event trigger is a URL notification from a third-party application or device. See the "Type of Event Triggers" section on page 6-1.	text
Reuse Archive for Soft	Indication of whether the original archive is used for the soft event trigger.	Check box
Soft Archive Expiration	Days after which the soft trigger event expires. Forever means that the event does not expire.	1, 2 Week(s), 1, 2, 3, 6 Month(s) 1 Year, Forever
Custom Fields	Custom fields (displayed only if custom fields have been defined for the camera). See the "Creating Custom Field Labels for Cameras" section on page 3-18.	text

Performing Other Batch Administration Tasks

To perform tasks on the Batch Administration panel, click **Batch Administration** on the side menu in the Administrator pages.

You must have one or more VSMS hosts configured in VSOM to be able to view information about the Batch Administration page. If no VSMS hosts are defined, the page is blank. See the "Adding a New Server" section on page 3-5 for information about adding servers.

The panel lists all of the cameras and feeds in the VSOM database. Some columns are hidden by default. To see the full list of columns and change column visibility, move your cursor over a column header to display a selection arrow. Click the arrow and then choose **Columns** from the drop-down list. The available columns are listed with check boxes, and the check boxes for the visible columns are checked. Check or uncheck any of the check boxes to customize the table. Changes made to the column visibility are not retained when the Batch Administration page is closed.

Table 5-6 lists the tasks you can perform on the Batch Administration panel.

Table 5-6 Batch Administration Tasks

Item	Description
Download the spreadsheet template.	Download the VSM Excel template to use to add the camera information for batch import. For detailed information, see the Managing Archives, page 5-17.
Apply a value to a particular column across multiple rows	Follow these steps on the Batch Administration page: 1. Check the check boxes for the rows and click **Apply Value**. 2. Choose a column and enter a value in the pop-up window. 3. Click **Update All** to apply the value to all visible rows or Click **Update Selected** to apply the value to the rows that have check boxes checked. **Note** Changes made using the Apply Value button apply only to the cameras that are listed on the current page within Batch Administration. Use the paging controls at the bottom of the table to display and apply values on other pages.
Display a short description of a column	Move your cursor over an entry in the table.
Import cameras and encoders.	Copy camera and encoder settings from the spreadsheet into VSOM. See the Managing Archives, page 5-17.
Filter the camera list.	Choose a parameter from the Filter drop-down list, enter a keyword to match, and click **Search**. Keywords are not case-sensitive, and there are no special search characters. The search matches any string within the field name. For example, "df7" matches "Sony SNC-DF70 Network Camera". Click **Clear** to remove any keywords you have entered.
Open a preview window for the camera	Click the icon to the left of the camera name to display a preview image in a new window.
Add a new camera	Add a camera by entering data on this page, as a alternative to using the Analog Cameras or IP/Network panel to add individual cameras.

Table 5-6 Batch Administration Tasks (continued)

Item	Description
Modify parameters for a camera	Scroll to the parameter field that you want to modify and click the entry and enter or choose a new value. **Note** If a parameter appears with a lock icon, it means that the field is not applicable, or that users are not allowed to change the value. If you change a high definition resolution to a standard definition resolution for a video analytics-enabled IP camera for which video analytics rules are configured, the rules may become corrupted. In this situation, use the camera web interface to delete the rules from the camera and then reconfigure the rules. For more information, see the *Cisco Video Analytics User Guide*.
Save settings for a specified camera	Check the check boxes for individual cameras, and click **Save Selected**.
Save settings for all listed cameras	Click **Save All**.
Discard unsaved changes for specified rows.	Click **Revert Selected**.
Delete cameras	Check the check boxes for the cameras, and click **Delete Selected** to delete the camera from the VSOM database.
Reload the table, discarding any unsaved changes.	Click **Cancel**.
Refresh the display on this page	Click **Refresh** to repopulate the panel with the latest information from the VSOM database.
Page through the batch administration list	Use the paging controls at the bottom of the camera list.

Managing Archives

VSOM allows you to configure video clips as archives and to shelve them for later viewing. To view the list of archives, open the Archives panel. The panel lists the archives that are viewable, currently running, scheduled, and pending.

You can identify a shelved archive by opening the Viewable Archives list. The archive state is Stopped and the feed name column is blank.

If you plan to back up your archives, Cisco recommends that you configure the settings on the Backup tab when you first create the archive. After backups have started, you can click the Backup tab for the archive and display the information in the Backup Details area. The information is for the last executed backup for that archive. For more information about backing up archives, see the "Creating Archive Backups" section on page 5-22.

You can synchronize stopped or shelved archives from another VSMS on a given VSOM by adding the server and using the Server Import option. See the "Importing Archives to a Server" section on page 3-8.

Table 5-7 provides information about configuring video archives.

Table 5-7 Archives: Configuration and Generation

Page/Method	System Action	Configuration
Video Archive Configuration Options on Batch Administration Page		
Looping	Creates a continuous looping archive.	Check the **Archive** check box for the camera on the Batch Admin page.
Soft Trigger	Creates an archive when the specified URL is received in VSOM.	Enter the URL in the Soft Trigger column for the camera on the Batch Administration page. See the "Performing Batch Administration Functions" section on page 5-11 and the "About Events" section on page 6-1.
Motion Configuration	Enables motion detection events for the camera. When a motion event is triggered, the system generates an archive, if specified in the motion event configuration.	• Check the **Motion Configuration** check box for the camera on the Batch Admin page to enable motion detection on the camera. • Set up the motion detection event to include archives. See the "Setting Up a Motion Detection Event" section on page 6-11.
Archive Page		
Scheduled - Simple	System generates one-time archives of the specified duration at the specified times.	Configure the archive, specifying the simple schedule type with the specified durations and times. See the "Adding a New Archive" section on page 5-20.
Scheduled - Recurring	System generates recurring archives of the specified duration at the specified times.	Configure the archive, specifying the recurring schedule type with the specified durations and times. See the "Adding a New Archive" section on page 5-20.
Looping	System generates a looping archive.	Configure a looping archive on the Archive page. See the "Adding a New Archive" section on page 5-20.
Events Page		
Motion Configuration	System generates an archive when a motion detection event is triggered. Video taken just before and after the event (typically 5 seconds) is included in the archive.	After creating the event, specify archive settings on the Motion Start and Motion Stop tabs. See the "Adding an Event" section on page 6-4 and the "Setting Up a Motion Detection Event" section on page 6-11.

Setting Up and Scheduling Archives

Use the Archives panel to set up and schedule video archives. Click **Archives** on the side menu in the Administrator pages to open the Archives panel. Table 5-8

Table 5-8 Archives Panel Links and Buttons

Item	Description
Start/Schedule a New Archive	Create and schedule a new archive. See the "Adding a New Archive" section on page 5-20.
Display currently defined archives	Click **There are (*N*) Viewable Archives** to open the list of archives. *N* refers to the number of defined archives in the list.
Display currently running archives	Click **There are (*N*) Running Archives** to open the list of archives. *N* refers to the number of running archives in the list.
Display scheduled archives	Click **There are (*N*) Scheduled Archives** to open the list of archives. *N* refers to the number of archives in the list for which a schedule is currently active.
Display pending archives	Archives are pending if they subject to a schedule or are in progress but are not yet complete. Click **There are (*N*) Pending Archives or Clips** to open the list of archives. *N* refers to the number of pending archives or clips. A clip is a portion of an archive that is created in the Operator page by using the Archive Clip button. See the "Understanding Video Archives" section on page 8-10.

Displaying Archive Lists

Archive lists appear when you click one of the **There are...** links on the Archives panel. Table 5-9 describes the columns that are included in each list.

Table 5-9 Archives List Columns

Item	Description
Type	Variety of archive: • Regular—Scheduled archive • Loop—Continuous looping archive. • Clip—Portion of an archive on demand (using Archive Clip function on the Operator page) • BWM—Clip in BWM format • Backup—Portion of an archive with start and end time
Archive Name	Name assigned to the archive. Click the link to display archive details, type, backup settings, and rights.
Feed Name	Name assigned to the camera feed, if there is an associated feed.

Table 5-9 Archives List Columns (continued)

Item	Description
Server Name	Name of the VSMS for this archive. Click the link to open the Server panel. For more information, see the "Managing Servers" section on page 3-5.
Health State	Indicates the status of the connection between VSMS and VSOM. **Up** indicates that the connection is active. **Down** indicates that either the VSMS is down or there is a connection problem between VSOM and VSMS. Also see the entry for Archive State in this table.
Start Time	Date and time that the archive schedule becomes active. When a schedule is active, archives are recorded at the times that the schedule specifies.
Duration	Length of time of the archive recording.
End Time	Date and time that the archive clip stops being active. When a schedule stops being active, archives are no longer recorded.
Expiration	Termination time for the archive based on the archive schedule. The archive is automatically removed from the archived video list on the expiration date. If an archive is set to never expire, it remains on the list until it is deleted.
Archive State	Indicates the status of the archive from the perspective of VSOM. Also see the entry for Health State in this table. • If Health State is **Up** and Archive State is **Running**, the archive is actively running. • If Health State is **Down** and Archive State is **Running**, then the archive is configured to record, but may not be recording. If the health state issue is resolved, VSOM automatically starts receiving the archive video again and begin recording. • If Archive State is **Stopped**, then the archive is not being recorded.
Actions	Includes icons to edit or delete the archive.

Adding a New Archive

When you add a new archive, you specify information about the camera, camera feed, and schedule for that archive.

Before You Begin

- Select a local archive repository for the VSMS host. See the "Media Server Configuration Page" section on page 10-17.
- Determine the cameras and camera feeds for which you want to create archives.
- Determine the schedule for the archive and how long you want to keep the archive on the server.
- Choose a naming convention for the archives. See the "Organizing Information in VSM" section on page 1-7.

- If you plan to back up your archives (recommended), make sure that a backup VSMS is defined. See the "Managing Servers" section on page 3-5and the "Creating Archive Backups" section on page 5-22.

To add a new archive, follow these steps:

Procedure

Step 1 In the Administrator pages, click **Archives**.

Step 2 Click **Start/Schedule a New Archive**.

Step 3 Choose the camera feed that is to be the archive source.

Click a camera group link to expand it, or click **Expand All** to display all of the camera group and subgroup members.

Step 4 Click **Next**.

The archive source that you selected is shown on the page in the Archive Source area.

Step 5 In the Archive Name field, enter a name for the archive that is consistent with your naming conventions (up to 30 characters, including spaces).

Step 6 (Optional) enter a description of the archive (up to 1024 characters, including spaces).

Step 7 Determine if the archive is to be enabled or disabled.

Enabled permits the archive to run as scheduled. **Disabled** means that the archive is retained in the archive list but does not run even if it has a schedule configured.

Step 8 In the Force Start field, choose **Default** if you want the system to check whether there is enough space to store the archive on the VSOM server.

If you use the Default option, the archiving operation does not start if there is insufficient storage space. Choose **Force** to start the operation even if there is not enough space. If you choose **Force**, you must provide additional space before the archive creations fills up the remaining disk space or the archive overwrites existing data.

Step 9 In the Keep on Server field, specify the length of time (days, weeks, months or years) after recording that the archive should be stored on the VSOM server.

The length of time that you can keep an archive depends on available storage space on the VSOM server. Use the System Overview panel to see the current storage usage, as described in the "Displaying System Overview Information" section on page 6-22.

Step 10 (MJPEG media type cameras only) In the Media Setup area, choose the frame rate at which the archive records (must be equal to or less than the frame rate that is configured for the camera feeds on the camera).

To preserve archive and backup space, you can configure a low frame rate for MJPEG feeds. For example, if you have an archive that was created from an event, you can edit the archive and reduce the frame rate to reduce the archive size.

Note The archive source that you selected in Step 3 is displayed near the bottom of the tab.

Step 11 Specify the type of archive schedule:

- Simple schedule—Choose a start and end date and time to generate the archive. To specify additional dates and times, click **Add Date(s)**. The default schedule is a simple schedule that begins at the current time and ends one day later.

- Recurring schedule—Specify information for a recurring archive. A recurring archive is repeated according to a defined schedule for a set period time or number of iterations. Choose one or more days of the week, and choose the start time and end time. To include additional start and end times for the same day, click **Add Time Range**. To specify schedules for additional days of the week, click **Next Weekdays** and enter information for a different day. Finally, choose an option for ending the schedule.
- Continuous loop—Choose a duration for a continuously running archive. Video is continuously recorded in a loop of this duration, and the video that is recorded in each period is overwritten during the next period. For example, for a continuous loop archive of one hour, only the previous hour of video is retained. Looping schedules start as soon as they are submitted.

Note If a motion detection event occurs while a continuous loop archive is recording, the video for the period containing the event is retained. If you view the archive at a later time, you see the video segment containing the motion detection event followed by the most recent continuous loop segment. See "About Motion Detection Events" section on page 6-10 for more information on motion detection events.

Step 12 To set up a backup server and schedule for the archive, see the instructions in the "Creating Archive Backups" section on page 5-22.

Cisco recommends that you set up archive backups when you first create archives.

Step 13 Click the **Rights** tab and verify the access designations.

For related information, see the "Adding a Role" section on page 7-8.

Step 14 Click **Submit**.

Creating Archive Backups

An archive backup is a copy of an archive that you save on a specified VSMS host. It is important to configure backups if you want to preserve content in the event of system failure.

Archives that are backed up to another VSMS host are available on the Operator page under **Video Archives > Shelved Archives**. They are not organized by camera group.

You can arrange to back up archives to your backup VSMS. Before configuring backups, the backup VSMS must be defined. See the "Adding a New Server" section on page 3-5.

Each backup is for a 24 hour period, and subsequent backups are added to the same backup file. Cisco recommends that you configure backups when you first define an archive to assure that there are no gaps in the backup for the first 24 hour period.

You can choose to back up full archives or back up only events:

- Backing up full archives saves all of the specified video.
- Backing up event only saves only the portions of the specified video that are involved in triggered events.

When you create an archive, you can see the Backup tab and explicitly set up the backup. However, if an archive is created automatically, for example, when Record Now is used (see the "Recording Live Video" section on page 8-18), the Backup tab is not visible and the archive is not backed up. In this case, you must open the created archive and configure the Backup tab manually.

Guidelines

- To back up all data without any interruption, configure the backup within 24 hours of creating the archive.
- After backups have started occurring, you can click the **Backup** tab for the archive and display the information in the Backup Details area. The information is for the last executed backup for that archive.

To create a backup schedule, follow these steps:

Procedure

Step 1 Click the **Backup** tab for the archive when you are first creating the archive (recommended) or by clicking **There are (N) viewable archives** on the Archives panel and then clicking the Edit icon for the archive.

Step 2 Check the **Backup this Archive** check box to activate the fields on this tab.

Step 3 Choose the backup server from the Backup Server list.

Step 4 In the Backup Start Time field, configure a start time for the backups (in HH:MM, 24-hour format).

For example, enter 23:00 to start the backups at 11 p.m.

Step 5 Check the **Backup Expires** check box and enter a number of days if you want the backup schedule to expire after the specified number of days. If you do not specify expiration, the archive runs indefinitely.

After the expiration period, the system deletes the backups.

Step 6 Check the **Backup Events Only** check box if you want to back up only events.

If you do not check this check box, the entire archive is backed up.

Step 7 Click **Submit**.

Editing or Deleting an Archive

You can change the name and description of a archive, backup settings, and settings for schedules that have not yet been activated. For schedules that have started, you can change only the end date.

If an archive is created automatically, you must open the created archive to configure the Backup tab. To back up all data without any interruption, you must configure the Backup tab within 24 hours of creating the archive.

When an archive is edited or deleted in the viewable archive list, other archives in the list with the same name are unaffected, as are any previous archive backups.

To change archive settings, follow these steps:

Procedure

Step 1 In the Administrator pages, click **Archives**.

Step 2 Choose the archive list to open (Viewable, Running, Scheduled, or Pending).

Step 3 Click **Edit** icon for the archive.

Step 4 Modify information in each tab as described in the "Adding a New Archive" section on page 5-20.

Note In edit mode, the Details tab includes a **View Video Settings** button. When you click the button, the system reads the video setting information that is being used to create the archive. For MPEG files, bit rate is shown; for JPEG files, frame rate is shown.

Step 5 Click **Submit**.

To delete an archive, choose the archive and click the **Delete** icon . Check the check box if you want to leave the portions of the archive that are already recorded on the server for future reference, and click **Yes**.

Understanding Grooming

VSM performs automatic grooming to ensure that archives do not completely fill up the storage capacity that is available in a system. The system performs two primary types of grooming:

- Retention-based grooming—This grooming process runs every 10 minutes and deletes archives that have passed their retention period. (For information about configuring the retention period, see the "Configuring System Settings" section on page 6-18.)
- Default grooming—Runs immediately when the archives exceed the storage space that is defined by the Max Storage % option in the Media Server Configuration page (see the "Media Server Configuration Page" section on page 10-17.) In this situation, the system deletes the oldest archives 200 files at a time until the maximum storage space is no longer exceeded.

Managing Predefined Views

A view consists of the video sources, layouts, and associated behavior that an operator sees in the video panel on the Operator page. A predefined view is a view that is configured in VSOM.

Click **Views** on the side menu in the Administrator pages to open the Views panel.

The following sections describe the tasks that you can perform from the Views panel:

Adding a New View

When you add a new view, you specify the camera sources, layout, and other display options for the view.

Before You Begin

- Determine the views that are needed to support your operations. For example, you may want to specify a view for each of the buildings on a campus.
- If multiple operator workstations are in use, choose a naming convention with unique view numbers and names for each workstation. See the "Organizing Information in VSM" section on page 1-7.
- Identify the camera feeds that you want to include in each view.

To add a new view, follow these steps:

Procedure

Step 1 In the Administrator pages, click **Views**.

Step 2 Click **Add a New View**.

Step 3 In the View Number field, enter an optional view number to identify the specific view within the overall set of views.

Cisco recommends that when multiple operator workstations are in use, each workstation use unique view numbers and names. The view number must be unique and greater than or equal to 1.

Step 4 In the View Name, enter a name to identify the view that is consistent with your naming conventions (up to 30 characters, including spaces).

Step 5 (Optional) In the Description field, enter a description of the view (up to 1,024 characters, including spaces).

Step 6 In the Camera Tour area, choose one of the following options. For information about using fixed and rotating views in the Operator page, see the See the "Using Predefined Views" section on page 8-5.

- **Do Not Tour**—Choose this default option if you do not want to rotate the view through video from a pool of cameras.
- **Rotate Every xx Seconds** (dwell time)—Choose this option to rotate or cycle through video from a pool of cameras and specify the number of seconds that a view displays before it rotates to the next view. Cisco recommends that you choose this option if a multiple layout view is specified. The view dwell time can be increased or decreased by using the toolbar on the Operator page. For rotation, the number of selected feeds must be greater than the number of panes.

Step 7 In the Choose Layout area, click a layout to choose it.

For each of the red highlighted panes, choose the view to designate whether the view displays live or archived video. Check **Fixed** for each pane that you want to remain fixed. Fixed means that the red-highlighted pane does not cycle video through a pool of cameras, and always shows only the video that is assigned to it. After checking the check boxes, click **Live** or **Archive** to assign either a live camera feed or archive to each red highlighted pane.

Step 8 From the Default Framerate drop-down list, choose a value to implement a frame rate cap for all configured MJPEG streams.

Reducing the frame rate reduces the bandwidth of the video signal and improves viewing performance, but may reduce the quality.

Step 9 In the Operator Lists field, check the check box to display all views available to operators in their view list.

When unchecked, views are not listed as views that the operator can switch to, but are displayed in the events and administrator lists.

Step 10 For Default Display Options, choose the title bars, video tools, timestamps, scrollbars, and fixed aspect that are presented as default view option check boxes on the Operator page. For more information, see the See the "Understanding View Option Check Boxes" section on page 8-30.

Step 11 In the Rotating Source List area, choose the camera feeds that you want to include in a source rotation.

Source rotation (or cycling) is a reservoir of randomly rotating camera views from which display panes are shown. Source rotation works by randomly displaying previously configured views in the operator layout widow. Source rotation is useful for operators who are required to monitor more camera locations than the currently configured view permits.

Expand the list to display all configured camera feeds and check the applicable boxes to associate the feed to the view layout.

Step 12 Click the **Rights** tab and verify the access designations. See the "Adding a Role" section on page 7-8.

Step 13 Click **Submit**.

If fixed panes are assigned to the view, a new panel opens to allow you to select the live or archive feed for each fixed pane. For each fixed pane, click a radio button to choose a source for the fixed pane. For archive sources, click the underlined link to display the available archives for a camera feed. Then Click **Submit** to save the settings.

Editing or Deleting a View

To edit view settings, click the **Edit** icon for the view in the Actions column on the Views panel and make changes on the View Info or Rights tab.

To delete the view from the VSOM database, click the **Delete** icon and then click **Yes** to confirm. When a view is deleted, it is no longer available on the Operator page.

Displaying View Settings

To display settings for a view, click the underlined link for the camera in the View Name column in the Views panel. Table 5-10 describes the information that appears.

Table 5-10 View Details

Item	Description
Details tab	
View Number	User-assigned number to identify a view within a set of views.
View Name	User-assigned view name.
Status	Not used.
Camera Tour	Indication of whether the view rotates and, if so, how frequently.
Layout	Visual representation of the layout for the video. Example: 
Fixed Windows	Visual representation of location of the fixed panes in the layout. The fixed panes are shown in red. Example: 
Default Framerate	Indication of the maximum configured frame rate. No cap means that the rate is determined by the video source.
Operator Lists	Indication of whether the view is shown in the list of views on the Operator page.

Table 5-10 View Details (continued)

Item	Description
Default Display Options	List of the display elements that are included on the Operator page for this view, including video tools, timestamps, scrollbars, and fixed aspect ratio.
Rotating Source List	Indication of which feed is used as the rotating video source. Click the link to open the camera feed panel for that source.
Rights tab	
Rights	Displays the access rights for this view: • Name—Displays the role name. Click the name link to open the Roles panel for the specified role. See the "Adding a Role" section on page 7-8. • Rights—Indicates the rights assigned to the role.

CHAPTER 6

System Management

This chapter describes how to manage events and schedules, generate reports, manage system settings, and view a snapshot of overall system operation. It includes these topics:

About Events

An event specifies information about an action that VSOM takes in response to a change in conditions (the event trigger). For example, an event may specify that a notification is sent when a motion sensor detects motion. When the motion occurs, the event triggers and the notification is sent.

You can configure any of the following actions to notify operators and administrators when an event triggers:

- Trigger audible and visual alarms
- Switch monitor views
- Send PTZ preset commands
- Send email notifications to designated recipients with a custom subject and message.
- Post information to a URL

The event history is updated each time an event triggers.

Type of Event Triggers

VSOM supports the following types of event triggers:

- Device Trigger
- Soft Trigger

- Motion Trigger
- Analytics Trigger, page 6-3

Device Trigger

A device trigger occurs when external physical equipment such as a building fire alarm or outdoor motion sensor detects a change in the environment.

Soft Trigger

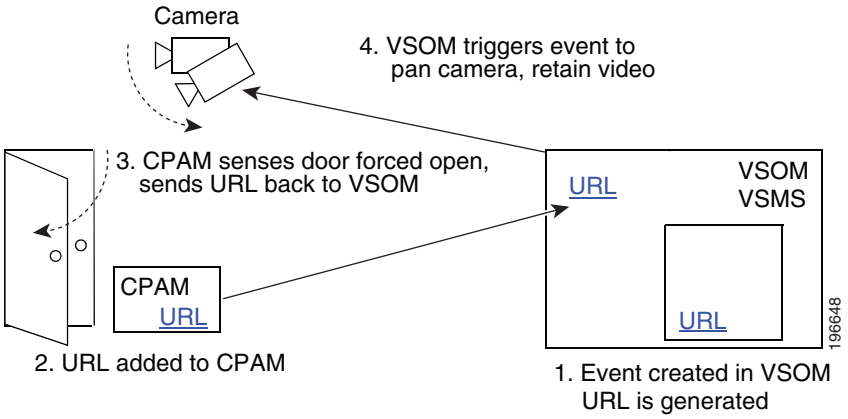
A soft trigger provides a connection between VSOM and an external program. VSOM generates a URL, which is supplied to the program. The event triggers when the external program sends the URL back to VSOM.

For example, the Cisco Physical Access Manager (CPAM) can sense when a door is forced open. You can set up a soft trigger to execute actions in response, such as panning the camera and sending and creating an archive. The process works as follows:

1. You configure the event in VSOM. When you submit the event, the soft trigger URL is automatically generated and displayed. See the "Structure of the Soft Trigger URL" section on page 6-2 for information on the soft trigger URL.
2. You add the soft trigger URL to CPAM.
3. When the door opens, CPAM detects it and sends the URL back to VSOM.
4. When VSOM receives the URL, it sends an instruction to the VSMS to pan the camera and create the archive.

Figure 6-1 illustrates this example.

Figure 6-1 Soft Trigger Event



Structure of the Soft Trigger URL

The default soft trigger URL that VSOM generates for soft event triggers is of the form

`http://<server>/vsom/service/event_notify.php?id=N`

where *N* is a unique numeric identifier that VSOM assigns to the event.

You can optionally embed additional information in the soft trigger URL. The information is added to the Description field for the event. To add additional information, append parameters to the end of the URL using the format "&param*X*=*value*" where *X* is an numeric identifier for the parameter and *value* is the content that you want to add to the Description field. Use % to represent spaces.

For example, to add information about alarm activation and evacuation to an event (with id=1) that has "Fire Event" as the current description, you can use the following URL:

```
http://<server>/vsom/service/event_notify.php?id=1&param1=Alarm%activated&param2=Please%
20Evacuate%20%Building
```

Then the event description on the Operator page Event Inbox is

```
Fire Event
param1=Alarm activated
param2=Please Evacuate Building
```

Motion Trigger

A motion trigger occurs when the camera detects motion. For additional information about events with motion triggers, see the "About Motion Detection Events" section on page 6-10.

Analytics Trigger

An analytics trigger occurs when the camera detects an event as specified by Cisco video analytics rules that are configure in a video analytics-enabled IP camera. To use the video analytics feature, you must enable this feature as described in the "Adding a New IP/Network Camera" section on page 3-21.

For analytics events, video is stored in chunks (typically five minutes each) as smd files on the VSMS host. When a analytic event triggers, the recording video is marked so that the clip is not deleted. By default, the video clip starts 30 seconds before the event (pre) and ends 60 seconds after the event (post).

Using the Events Panel

The Events panel includes options that you can use to create and configure events. Click **Events** on the side menu in the Administrator pages to open the Events panel. Table 6-1 lists the tasks that you can perform from this panel.

Table 6-1 Events Panel Tasks

Task	Description	Reference
Add a new event	Define a new event	Adding an Event, page 6-4
Enable bookmark event	Create an event to capture the time shown in a selected video pane. Later, after creating the bookmark event, you can return to the event and do a seek to return to the time that you bookmarked.	Adding an Event, page 6-4
Enable events for Record Now	Creates an event named **---Record Now Event---** that maintains the history of Record Now actions	—

Table 6-1 Events Panel Tasks (continued)

Task	Description	Reference
Enable default analytics event notification	Creates a default analytics event named **---Default Analytics Event---**. This event is used to process analytics rules that are not matched with user-created VSOM analytics events. When you enable this event, any analytics event that does not match user-created VSOM analytics events is displayed in the Event Inbox. This event does not have actions associated with it.	—
Edit or delete an event	Change the settings for an event or delete an event	Editing and Deleting Events, page 6-9
Set up motion detection	Configure events that are triggered by motion detection	About Motion Detection Events, page 6-10 Setting Up Windows for Motion Detection, page 6-14
Display event histories	Display information about events that have been triggered, with optional filtering	—
Change the labels assigned to events	Change the flags that are used to highlight events in the event list and on the Operator page	—

Adding an Event

Adding an event is the process of specifying a name for an event and configuring the conditions and triggers that result in event notification.

Before You Begin

- Because events can affect many elements of your deployment, make sure that the devices for your deployment are fully configured and that you have set up archives, monitors, PTZ configuration, and views before defining events.
- Determine the types of events that you want to create, the associated actions, and a naming convention for the events. See the "Organizing Information in VSM" section on page 1-7.
- Set up the schedules to use for the events. See "Adding a Schedule" section on page 6-16.
- Determine the camera/encoder and VSMS that are involved in the event.

To add a new event, follow these steps:

Procedure

Step 1 In the Administrator pages, click **Event**.

Step 2 Click **Add a New Event**.

Step 3 In the Event Name, enter a name to identify the event (up to 30 characters, including spaces).

For suggestions about naming conventions, see the "Naming Conventions" section on page 1-7.

Step 4 (Optional) In the Description field, enter a description of the event (up to 1,024 characters, including spaces).

Step 5 In the Server field, choose the VSMS that manages the devices that are involved in the event.

Step 6 In the **Status** drop-down list, verify that the status is **Enabled**. An event can only be triggered if it is enabled.

Step 7 In the Default Flag field, choose a flag to represent the severity of the event.

The flag is presented with the event in the Operator page.

The information bubble represents the lowest severity and the exclamation symbol represents the highest severity.

Step 8 Choose one of the following options to trigger the event:

- Device Trigger—Choose to trigger the event based on an external device (such a building fire system or outdoor motion sensor). When you click **Submit** to add the event, the following options appear on the Details tab:
  - Encoder/IP Camera—Choose the encoder or camera that triggers the event from this drop-down list.
  - Channel—Enter the number of the contact closure input on the device that triggers the event.
  - Default State—Choose whether the event triggers based on a rising state (increase in power) or falling state (decrease in power).
- Enable Soft Trigger—Choose if the trigger is a soft event. A soft event triggers when an external program requests a URL. When you click **Submit**, the link is generated and displayed.
- Enable Motion Configuration—Choose to trigger the event based on motion detection from a camera and choose the feed from the drop-down list. Feeds appear in the list only if they have motion detection enabled. See the "About Motion Detection Events" section on page 6-10.
- Enable Analytics Trigger—Choose to trigger the event based on Cisco video analytics events that are configured on a video analytics-enabled IP camera.

Step 9 Click the **Setup Rights** tab if you want to change the default roles that are permitted access to this event record. For more information, see the "Setting Up Roles" section on page 7-8.

The default settings are Manage rights for the Administrator role and View right for the Operator role.

Step 10 Click the **History Rights** tab if you want to change the default roles that are permitted access to the notifications that are triggered by this event. For more information, see the "Setting Up Roles" section on page 7-8.

The default settings are Manage rights for the Administrator role and View right for the Operator role.

Step 11 Click **Submit**.

Step 12 The new event is created, and the panel reopens to show additional tabs that allow you to specify additional details about the event (see Table 6-2).

The tabs that appear depend on the type of event that you set up.

Table 6-2 Editing the Event Configuration

Item	Description
Details tab	
Event Name	*Display only.* Displays the name of the event.
Description	Enter a description of the event (up to up to 1,024 characters, including spaces)
Server	*Display only.* Displays the VSMS host that forwards the event to VSOM.
Status	Choose **Enabled** if you want the event to appear on the VSOM Operator page when the event is triggered
Default Flag	In the Default Flag field, choose a flag to represent the severity of the event.
Analytics Rule Name	For an analytics trigger event, enter a rule name exactly as it is configured in the Manage Rules page in the web user interface for the camera that is to trigger this event, then click the **Add Rule** button. When the camera detects an event that matches this rule, this VSOM analytics event triggers. If you do not specify a rule, the event is added but it will not trigger unless you have configured a default analytics event. You can add multiple rules. **Tip** If you want to configure a common set of actions to use with analytics rules on more than one camera, use the same rule name on each camera, or add the rule from each camera here. If you want to configure one or more unique actions for rules from a specific camera, make sure to configure a rule name or names to be used only in that camera, and then add each of those rules here. For information about configuring analytics rules on a video analytics-enabled IP camera, see the *Cisco Video Analytics User Guide*. A list of analytics rules appears at the bottom of the tab. You can click the **Delete** link next to a rule to delete it from VSOM.
Operator View tab	
Change Operator View	Check the check box if you want to change the layout that appears on the Operator page when the event triggers. When you check the check box, radio buttons for the various layouts are activated. Choose the desired layout.
Layout	Choose a predefined view to include an entry in the View column of the Event Inbox on the Operator page that the operator can click to display the view. A notification also appears at the bottom of the video panel in the Operator page when the event video is viewed. Clicking the notification opens the view.

Table 6-2 Editing the Event Configuration (continued)

Item	Description
Archives tab	
Start Archives	Check a check box in the top area on the page to create an archive from the corresponding live feed. Check the check box in the bottom area on the page to configure settings if you want to create an archive clip when the event triggers. Check up to 10 archives to automatically start clipping upon an event trigger. This option is useful when only event data must be backed up for an archive. See the "Creating Archive Backups" section on page 5-22 for more details about backups.
Data Options	Choose the amount of time to be recorded and archived before and after the event.
Storage Options	Configure the following storage options: • Store each archive for—Choose the time period to store the archived event, or choose **Forever** to keep the archive indefinitely. • fps—Choose the framerate at which to record (JPEG sources only). Reducing the framerate reduces the required storage space, but records video at lower quality. The specified framerate cannot exceed the framerate of the source.
Alerts tab	
Web based Alerts	Determine if event notifications are sent through an on-screen message on the Operator page, logged in the Event History Report, or both. See the "Generating Reports" section on page 6-22 for information on generating the Event History Report. Operator notification is used only if the event is logged in the Event History Report. The on-screen notification appears momentarily in the message bar on the Operator page. If you turn this option off, the momentary notification does not appear. See the "Viewing Video Events" section on page 8-36.
Enable URL Notification	Enter a URL to which VSOM posts information when the event triggers. Multiple URL notifications are permitted. URL notifications are sent before e-mail notifications are sent.
Enable Email Notification	Enter the event notification recipients and the e-mail subject and body text that is sent when an event triggers. All of the e-mail fields are required for e-mail notification.
PTZ Presets tab	
PTZ Presets	Enable PTZ changes in response to the event trigger and choose the camera name, preset label, and PTZ priority as applicable. When the event triggers, the preset is applied to the camera with this priority. The drop-down list options are available only if the camera and presets are configured. To add additional presets, click **Add Another Preset**.

Table 6-2 Editing the Event Configuration (continued)

Item	Description
Monitors tab	
Monitors	Choose the monitor and view to display in the Operator page when the event triggers. Events can trigger multiple monitors to switch to specified views. If no monitors are defined, click **Add a New Monitor and Associated View**, and choose the desired monitor and view. To add other monitors, click **Add Another Monitor and Associated View**.
Schedules tab	
Default State	Choose the status (**Enabled** or **Disabled**) that applies to the event when it is not subject to a schedule. For example, if the event schedule covers the night period from 10 p.m. to 8 a.m. (2200 to 0800), the Default State is the state of the event in the day period from 8 a.m. to 10 p.m. (0800 to 2200). The default state is **Enabled**. Unless the default state is changed to **Disabled**, the event can be triggered outside of the specified schedule period. In the example above, if the default state is **Enabled**, the event can be triggered during the day. If you want to prevent an event from being triggered outside or specified scheduled times, do the following: • Set **Default State** to **Disabled** on the Schedules tab for the event. • Verify that the schedule status is **Enabled** on the Schedule panel > Details tab. • Verify that the status for each scheduled time period is **Enabled** on the Schedule panel > Schedule tab.
Simple Schedule	Choose the schedule to apply to the event from the drop-down list. A simple schedule runs once from a specified start time to a specified end time.
Recurring Schedule	Choose the schedule to apply to the event the drop-down list. A recurring schedule runs multiple times according to specified rules.
Setup Rights tab	
Name	User name configured in VSOM
Rights	Rights assigned to the user for modifying this event (None, View, or Manage)
History Right tab	
Name	User name configured in VSOM
Rights	Rights assigned to the user to access the history for this event (None, View, or Manage)

Editing and Deleting Events

To edit settings for an even, click the **Edit** icon for the event in the Actions column on the Events panel and make changes on any of the tabs.

To delete an event from the VSOM database, click the **Delete** icon and then click **Yes** to confirm. When an event is deleted, notifications are no longer triggered. However, the event is still listed in the event history.

Order of Event Execution

Events may involve multiple actions. When an event triggers, VSOM executes the actions in the following order:

1. Clip selected archives (as specified on the Archives tab for the event).
2. Log the event history. Operators are notified on the Operator page within two seconds.
3. Send any event trigger commands to VSMS, which clips the archive that is created for the event (as specified under Feeds in the Archives tab for the event).
4. Execute PTZ functions on a specified cameras (as specified on the PTZ Presets tab for the event).
5. Seed the monitor views (as specified on the Monitors tab for the event).
6. Send URL and e-mail notifications (as specified on the Alerts tab for the event).

About Motion Detection in VSM

The ability to detect motion is a function of the encoding source device (IP camera or encoder). The encoding source device must support motion detection for you to be able to set up and use the motion detection functionality in VSM.

Note Cisco recommends that you do not configure both PTZ and motion detection on the same camera.

For cameras that support motion detection, you can configure any of the following types of responses when is motion is detected:

- Change Operator page layout—Change the layout of the Operator page.
- Start archive—Start recording an archive when motion occurs and stop recording when motion stops. This function allows you to create archives that contain video segments of interest while avoiding the archiving of unneeded video.
- Send notification—Send a URL or an e-mail message, or notify the operator by way of a message on the Operator page.
- PTZ preset—Move the camera to a specified PTZ preset position.
- Monitors—Change the monitor that displays the video that the event triggers, along with the associated monitor view.

Detecting motion and taking actions based on motion detection is a distributed process in VSM:

- The motion detection rules and algorithms reside in an encoding source device (IP camera or encoder), and the overall functionality for motion detection is constrained by what the encoding source device can do.

- In addition to providing the communications link between a camera and VSOM, VSMS can perform some processing functions, such as smoothing to reduce the level of noise in motion detection.
- Settings in VSOM determine the specific window within a camera feed where motion detection is recognized, schedules for motion detection, and the archives and events that are created based on detected motion. The camera saves the windows that you configure in VSOM and uses these settings for motion detection.

About Motion Detection Events

The goal in setting up motion detection events is to detect and record everything of interest while excluding everything that is not of interest. There are several aspects involved:

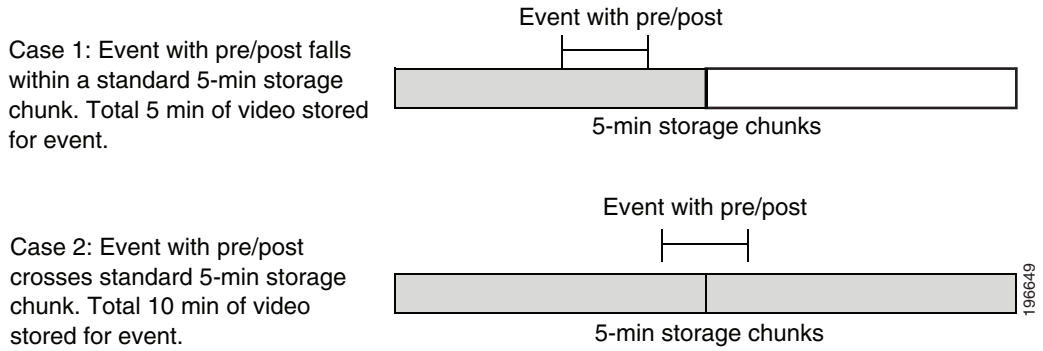
- Motion detection window—The motion detection window is the area within a video where motion detection is considered. For example, if a camera feed shows a room with a door and the goal is to detect when the door opens, the window should be specified to include the smallest area within the feed that shows movement if the door opens or closes. The window could be a small area at the top of the door that shows the movement of the hinge or the opening of a space between the door and door jamb. See the "Setting Up Windows for Motion Detection" section on page 6-14.

  Identifying a larger area risks capturing motion that may not be of interest (such as a person walking in front of the door) and can add unneeded data to the VSOM database.
- Scheduling—For a given camera feed, you may be interested in motion detection only during certain hours or days, such as evenings or weekends.
- Actions—VSOM allows you to specify the type of action to take in response to a motion detection event.

For motion detection events, video is stored in chunks (typically 5 minutes each) on the VSMS host. VSMS continuously records video from the camera to capture what occurred before motion is detected, and removes this video after 5 to 10 minutes. When a motion is detected, the recorded video is marked so that the video is not removed. By default, the video clip starts 30 seconds before the event (pre) and ends 30 seconds after the event (post).

The amount of video recorded for a motion event depends upon the timing of the event relative to the standard (5 minute) chunks used for video storage. If the event with the pre and post intervals falls within one of the chunks, a total of 5 minutes of video is associated with the event. However, if the event with the pre and post intervals crosses the time boundary between two storage chunks, a total of 10 minutes (two video chunks) is stored for the event (see Figure 6-2).

Figure 6-2 Video Storage Chunks and Motion Events



If a motion detection event occurs while a continuos loop archive is recording, the video containing the event is retained. If you view the archive at a later time, you see the video segment containing the motion detection event followed by the most recent continuous loop segment. See "Managing Archives" section on page 5-17 for more information on continuous loop archives.

Best Practice

- Experiment to determine the optimal camera placement, motion detection window, and sensitivity to avoid false positives (detected motion that is not of interest) and false negatives (motion that is not detected). Have two people available, one to adjust the camera placement and direction, and one to modify settings in VSOM.
- When motion is detected, VSMS records video until the video source indicates that motion has stopped. If the motion stop notification from the video source is not received by VSMS, VSMS marks video with motion for a maximum event marking duration period (the default period is 2 hours), and does not mark video again until a motion stop notification is received and motion resumes. If there are cameras that may capture continuous activity for long periods, the Maximum Event Marking Duration parameter must be changed on each VSMS server (see the "Media Server Configuration Page" section on page 10-17). For example, if a site has an office that is open to customers from 9:00 a.m. to 6:00 p.m. (0900 to 1800), the maximum event marking duration should be set to 9 hours to capture constant activity during that period.
- Adjust motion detection windows so that they do not cover views of busy streets or thoroughfares to avoid video being recorded due to movement of cars or pedestrians outside the intended area of coverage.

Setting Up a Motion Detection Event

To create a motion detection event, use the **Enable Motion Configuration** option when creating the event.

Before You Begin

- Add your motion detection cameras to VSOM and enable motion detection on them. See the "Adding a New Analog Camera" section on page 3-17 or the "Adding a New IP/Network Camera" section on page 3-21.
- Set up any schedules that you want to use to trigger the events. See the "Managing Schedules" section on page 6-16.

To create and enable a motion detection event, follow these steps:

Procedure

Step 1 In the Administrator pages, click **Events**.

Step 2 Choose **Add a New Event**.

Step 3 Choose the **Enable Motion Configuration** button and choose a feed from the drop-down list.

Step 4 Configure the event settings as described in the "Adding an Event" section on page 6-4, and click **Submit**.

The event is saved, and the panel reopens to display additional tabs.

Step 5 To set up active and inactive windows for motion detection, click the **Motion Config** tab and configure the settings described in the "Setting Up Windows for Motion Detection" section on page 6-14.

Step 6 Configure settings on the Motion Start and Motion Stop subtabs, as described in Table 6-3.

Step 7 Click **Submit**.

Table 6-3 Motion Start and Motion Stop Configuration

Tab	Description
Operator View Tab	
Change Operator View	Check the check box if you want to change the layout that appears on the Operator page when the event triggers. When you check the check box, radio buttons for the various layouts are activated. Choose the desired layout.
Archives Tab	
Start Archives	Check the **Start Archives** check box if you want to configure archive settings.
Archives list	Check a check box in the top area on the page to create an archive from the corresponding live feed. Check the check box in the bottom area on the page to choose up to 10 archives to automatically start clipping when an event triggers. This option is useful when only event data should be backed up for an archive. See the "Creating Archive Backups" section on page 5-22 for more details about backups.
Data Options	Enter the number of seconds before and after the event to include in the recording. The default is 5 seconds.
Storage Options	Configure the following storage options: • Store each archive for—Choose the time period to store the archived event, or choose **Forever** to keep the archive indefinitely • fps— Choose the framerate at which to record (JPEG sources only). Reducing the framerate reduces the required storage space, but records video at lower quality. The specified framerate cannot exceed the framerate of the source.

Table 6-3 Motion Start and Motion Stop Configuration (continued)

Tab	Description
Alerts tab	
Web based Alerts	• Check the **Log into the Event History Report** check box to log the event. See the "Generating Reports" section on page 6-22 for information on generating the Event History Report. **Note** If you create a motion detection event to clip a running archive when the event is triggered, you must check the **Log into the Event History Report** before you submit the event. An error message is presented if you submit the event without checking the check box. • Check the **On-screen Operator Notification** to sent notification to the operator on the Operator page when the event is triggered. You can specific Operator notification only if the **Log into the Event History Report** check box is checked. The on-screen notification appears momentarily in the message bar on the Operator page. If you turn this option off, the momentary notification does not appear. See the "Viewing Video Events" section on page 8-36.
Enable URL Notification	Enter a URL to which VSOM posts information when the event triggers. Multiple URL notifications are permitted. URL notifications are sent before e-mail notifications are sent.
Enable Email Notification	Enter the event notification recipients and the e-mail subject and body text that is sent when an event triggers. All of the e-mail fields are required for e-mail notification.
PTZ Presets tab	
PTZ Presets	Enable PTZ changes in response to the event trigger and choose the camera name, preset label, and PTZ priority as applicable. When the event triggers, the preset is applied to the camera with this priority. The drop-down list options are available only if the camera and presets are configured. To add additional presets, click **Add Another Preset**.
Monitors tab	
Monitors	Choose the monitor and Operator page view to display when the event triggers. Events can trigger multiple monitors to switch to specified views. If no monitors are defined, click **Add a New Monitor and Associated View**, and choose the desired monitor and view. To add other monitors, click **Add Another Monitor and Associated View**.

Setting Up Windows for Motion Detection

For cameras that support motion detection, you can configure motion detection windows within a video pane to determine how VSOM interprets motion that the camera identifies. Motion detection windows are specified windows (mask and non-mask) within the video pane:

- Motion in a mask window within a video pane is ignored (cannot trigger an event).
- Motion in an active or non-mask window within a video pane can trigger an event.

A video pane can have multiple mask and non-mask windows defined, and the windows can cover some or all of the same area in the pane.

Window creation order is important. Create your active windows first and then add any mask windows on top.

When motion is detected, an event is listed in the events table in the Operator page. If you specified a feed, the display shows the associated archives on the side menu.

Before You Begin

- Add motion detection cameras to VSOM and enable motion detection on them. See the "Adding a New Analog Camera" section on page 3-17 and the "Adding a New IP/Network Camera" section on page 3-21.
- Set up a motion detection event, as described in the "Adding an Event" section on page 6-4.

To set up motion detection windows, follow these steps:

Procedure

Step 1 Make sure that the camera is configured.

See the "Adding a New Analog Camera" section on page 3-17.

Step 2 In the Administrator pages, click **Events**.

Step 3 Click the **Edit** icon in the Actions column for the event and then click the **Motion Configuration** tab.

Step 4 To create a new motion detection window, click and enter the new window name. Only alphanumeric characters are permitted, and there can be no spaces.

The number of supported motion detection windows depends on the camera model. Create active windows first and then add any mask windows on top.

- For an active (non-mask) window, leave the **This is a mask window** check box unchecked.
- For a mask window, choose the **This is a mask window** check box.

A window with a green border (for non-mask) or a red border (for mask) is added to the video preview image. The window border displays the window name. To resize the window, drag the borders of the window. To move the window, drag and drop the window.

Step 5 Create additional windows as needed.

Step 6 Use the information in Table 6-4 to complete the motion configuration.

Step 7 Click **Submit**.

Table 6-4 Motion Configuration Settings

Item	Description
Window	Choose the window that you want to configure or delete from the drop-down list. You can also change the window by selecting it in the video preview. For multiple stacked windows, it is easier to use the drop-down list.
New	To create a new window, click **New**, enter the new window name, and choose whether the window is a mask window. No spaces are permitted in the name. Click **OK**.
Delete	Choose a window and click **Delete** to remove it. You must delete all motion detection windows to turn motion detection off. **Note** You cannot rename motion detection windows. You must delete a window and then add a new one to use a different name.
Mask Window	*Display only.* Check box that indicates whether the selected window is a mask window.
Sensitivity	Indicates the relative level of motion sensitivity that triggers recording when motion is detected. The sensitivity metric depends on the camera. You may need to experiment to determine the level of sensitivity that causes only the motion of interest to be recorded. The range is 0 (detects no motion) to 100 (most sensitive to motion). The default is 0. Some cameras include preset default values for sensitivity.
Inactive/Active	*Display only.* Displays the status of the motion window.
Object Size	Specify the minimum and maximum size that an object must be to have its motion detected. For example, if you want to detect whether a person has entered an area, but do not want to detect the presence of flying insects, set the minimum object size appropriately. The units for the minimum and maximum sizes are camera specific. You may need to experiment to determine the appropriate minimum and maximum object sizes.
Persistence	Specify the length of time in seconds that motion must be detected to trigger an event. Examples: .5 (for one-half second) or 3.25 (for three and one quarter seconds). Some cameras include preset default values for persistence.
Show Grid	Change the grid display options, if supported by the device. A grid includes vertical and horizontal lines for reference. Whether the feature is available depends on the camera, as does the granularity of the grid.

Managing Schedules

Schedules allow you to enable and disable specific events, user accounts, and roles on predetermined days and times. Each schedule can control multiple entities, and you can change the schedule that is assigned to an entity at any time.

The following schedule types are supported:

- Simple schedule—A simple schedule becomes active and feeds are recorded when the current date and time falls between the start and end dates and times. Simple schedules are useful for defining one-time control of an entity status or a list of exceptions (such as holidays). You can also use simple schedules for a one-time or loop archive.
- Recurring schedule—A recurring schedule becomes active and feeds are recorded when the current day is defined in the recurring schedule and the time falls within one of the start and stop intervals for that day. The schedule is considered inactive during all other dates and times.

When a scheduled entity has no active schedules, it returns to its default state.

Simple schedules takes precedence over recurring schedules. If simple and recurring schedules are active simultaneously, the simple schedule becomes active and the recurring schedule becomes inactive. When both become inactive, the entity returns to its default state.

Click **Schedules** on the side menu in the Administrator pages to open the Schedules page. Table 6-5 lists the tasks that you can perform on this panel.

Table 6-5 Schedules Panel Tasks

Item	Description	Reference
Add a schedule	Create a new schedule that can be used for users, roles, or events	Adding a Schedule, page 6-16
Edit or delete a schedule	Make changes to an existing schedule or delete a schedule	Editing or Deleting a Schedule, page 6-18

Adding a Schedule

When you create a schedule, it becomes available to apply to users, roles, and events.

Note If you check the Enable Analytics check box when you configure a video analytics-enabled IP camera, the system automatically creates a 1-hour looping archive named Analytics_*camera-name*. For more information, see the "Adding a New IP/Network Camera" section on page 3-21.

Before You Begin

- Decide whether you want to restrict user access according to time of day or days of the week and whether the restrictions are for individual users or user roles. For example, you may want to restrict access for your operators only to the times that they are scheduled to be at work, or you may want to restrict access for individual employees with the Installer role only to certain maintenance periods.
- Decide whether you want to be able to define events based on schedules. For example, you may want to set up motion detection events only for nights and weekends.

- Choose a naming convention for the schedules that you are creating. For example, you may want to include a recognizable prefix for schedules that apply to events (such as event_sched_A, event_sched_B), to periods of time (such as vacation_xmas, vacation_july4th), or to employee classifications (such as operator_A, installer_2).

To add a new schedule, follow these steps:

Procedure

Step 1 In the Administrator pages, click **Schedule**.

Step 2 Click **Add a New Schedule**.

Step 3 In the Name field, enter a name for the schedule (up to 30 characters, including spaces).

Step 4 (Optional) In the Description field, enter a description (up to 1024 characters, including spaces).

Step 5 In the Status field, determine if the schedule is to be enabled or disabled.

Enabled schedules are available for use. Disabled schedules remain on the Schedules list but are not available for use.

Step 6 Create simple schedules, recurring schedules, or both:

- To create a simple schedule, click the **Simple** tab and specify the following:
  - Click the **This is a Simple Schedule** check box.
  - Click **Enable** to active the settings on this tab.
  - Enter a start and end date in (mm/dd/yyyy format), or click the calendar icons to choose the date.
  - Choose the start and end times from the drop-down lists.

    Time ranges in schedules cannot cross midnight, so for a schedule to run past midnight, you must split it into a range from midnight to the end time, and from the start time until 23:59.
  - To add an additional start and end date and time, click **Add Date(s)**. To remove a start and end date and time, click the **Remove** link for that entry.
- To add a recurring schedule, open the Recurring tag and choose the **This is a Recurring Schedule** check box.
  - Choose whether to enable the schedule from the **Action** drop-down list.
  - Enter a start date (in mm/dd/yyyy format), or click the calendar icon to choose the date.

    Time ranges in schedules cannot cross midnight, so for a schedule to run past midnight, you must split it into a range from midnight to the end time, and from the start time until 23:59.
  - Choose one or more days of the week, and choose the start and stop times from the drop-down lists.
  - To add an additional start and stop time, click **Add Time Range**. To add additional days of the week and associated times, click **Next Weekdays**. To remove an entry, click the **Remove** link for that entry.
  - Choose one of the following options to end the schedule:
  - **End After**—End after a specified number of occurrences
  - **End By**—End after a specified date
  - **No End Date**—Do not end the schedule

Step 7 Click the **Rights** tab and verify the access designations.

Step 8 Click **Submit**.

The Schedules panel reopens to display the events, roles, and users to which you can assign the schedule.

Step 9 Check the check boxes to specify the entities.

Click **+** to expand a category, or **–** to hide the category. If there is a schedule active on an entity, the manual enable/disable is overridden by the enable/disable that the active schedule applies. If there is no currently active schedule, the manual enable/disable works as expected. However, when a schedule becomes active again, the active schedule determines the state of the entity and when the schedule becomes inactive; the entity is returns to the default state of the entity, not to the state of the manual enable/disable.

Step 10 Click **Submit**.

Editing or Deleting a Schedule

To edit schedule settings, click the **Edit** icon for the schedule in the Actions column on the Schedules panel and make changes as described in the "Adding a Schedule" section on page 6-16.

To delete a schedule from the VSOM database, click the **Delete** icon and then click **Yes** to confirm. The schedule is removed from the user, role, and event records to which it was assigned.

Configuring System Settings

Use the Settings panel to configure system-wide settings and display license information. For most deployments, it is not necessary to modify these settings.

Before making changes on the Settings panel, verify that modifications are necessary. The default settings on this panel are appropriate for most deployments.

To configure system-wide settings, click **Settings** in the Administrator pages and configure the items listed in Table 6-6, and click **Submit**.

Table 6-6 System Settings

Item	Description
Application Settings	
Skin	Use this option to set the customized appearance of the VSOM GUI.
Language	Choose the default language for the user interface for the items in the VSOM GUI.
Default Paging	Choose the number of records per page to be displayed in lists. Valid values are 5 through 100. The default value is 50.
Session Timeout	Choose the amount of time a session remains active without user action (the units are specified). When the session time is reached without user activity, the system logs the user out.
Show Previews	Check this check box to include camera image previews on pages that have a camera preview area.

Table 6-6 System Settings (continued)

Item	Description
Enable Secure Login	Check this checkbox to require users to log in to VSOM using secure socket layer (SSL). When this option is enabled, a user must enter HTTPS instead of HTTP when accessing the login page. **Note** If you are using SSL, make sure that your network administrator has obtained a valid SSL security certificate.
Database Backup	Check the check box to schedule a daily backup of the VSOM database. Choose the time at which the backup is taken (hours and minutes) from the drop-down lists. For information about database backups, see the "Managing the VSOM Database" section on page 4-2
Max no. of backup	Choose the maximum number of backups to store on the VSOM server. When the number of backups exceeds this number, the oldest backups are overwritten as new backups are taken.
Batch Administration Defaults	
Create Default Archive	Check the check box to create a default archive when a camera feed is added using batch administration. See the "Performing Batch Administration Functions" section on page 5-11.
Reuse Default Archive	Check the check box to reuse the default archive for soft trigger events. See the "About Events" section on page 6-1.
Archive Duration	Choose the duration of the default archive loop from the drop-down list. The range is 1 to 7 days. The default is 1 day.
Archive Retention	Choose the length of time that archives are retained. The archive retention setting determines how much space VSMS sets aside for archives. The setting applies to all archives. The default is 30 days. See the "Managing Archives" section on page 5-17. **Note** Regardless of the value that you configure for archive retention, archives may be deleted automatically if they exceed the storage space that is defined by the Max Storage % option in the Media Server Configuration page (see the "Media Server Configuration Page" section on page 10-17).
Operator View Settings	
Max Record Length Now	Choose the maximum default amount of time recording occurs for archives. Operators are permitted to set the record time to this length or less.
Historical Events	Set the number of events that are viewable by operators in the Operator page. If more events than this option specifies are generated, the older events are overwritten.
Use VMR	Use the video mixing renderer (VMR) on the Operator page. If the camera supports VMR and you enable this setting, VRM controls appear in the video pane on the Operator page.
Use DVR	Displays player controls in the ActiveX client.
Display Video Timestamp	Click this checkbox to display the timestamp that is generated by a video camera on the primary pane in the Operator page.

Table 6-6 System Settings (continued)

Item	Description
Use SmartSearch	Click this checkbox to enable the Smart Search function in the Operator page. See Chapter 9, "Using Smart Search."
Enable Snapshot	Allows snapshots to be taken in the Operator page. See the "Creating a Snapshot" section on page 8-19.
Event History Settings	
Event History Retention	Choose the length of time that event history is retained from the drop-down list. After this time passes, the system purges all the events that occurred previously. When events are purged, a message appears below the Event History Retention field. The system can store a maximum of 250,000 events.
Health Monitoring Settings	
Health History Retention	Choose the length of time that the system retains health history information. The default value is 1 month. See the "Using the Health Dashboard" section on page 6-23. The system begins purging events if more than 200,000 events are stored. When events are purged, a message appears below the Health Event retention field.
Health Warning Expiration	Choose the length of time that health warnings are retained for display in the Health Dashboard. The default value is 1 day. The health warning expiration allows you to see information about the most recent health warnings, while retaining full information in the health history. For example, if the network experiences intermittent lost packet events, many warnings may be generated. On the Health Summary, only the warnings that occurred within the specified period are reported; however, you can view the entire warning history by displaying the Health History for the component. After the expiration period, the warning count is reset. See the "Using the Health Dashboard" section on page 6-23. When warnings are purged, a message appears below the Event Warning Expiration field.

Table 6-6 System Settings (continued)

Item	Description
Health Email Notification	When the health monitoring email notification feature is enabled, the system sends email messages to the designated recipient if error or warning events exist in the system. Messages are sent according to a configurable time interval. Messages include a summary of each event that exists in the system and a link to the Health Dashboard. The system checks for errors and warning events when the time interval elapses and, if such events exist, the system sends an email at that time. Enter information in the following fields if you want to send an email notification about error or warning events that the health monitoring system generates. • **Enable sending a health summary email if there is an error and/or warning**—Check this check box to enable health monitoring email notification • **Send once per this interval**—Enter the number of hours for the interval at which the system sends health monitoring email notifications.Valid values are 1 through 9999. • Address field—Enter an e-mail address to which the heath monitoring notification is sent. Multiple e-mail addresses are not supported. If you want to send notifications to multiple recipients, use a mail list address. To use the health monitoring email notification feature, you also must enter information in the SMTP Server and the SMTP "From:" Address fields in the SMTP Parameters area in the Operations Manager Configuration page. For instructions, see the "Operations Manager Configuration Page" section on page 10-19.
Application Customization	
Application Name	Enter the name (maximum 127 characters) that is shown in the upper left corner of the VSOM GUI. This setting is used to customize the appearance of the VSOM user interface.
Logo	Upload an image, such as a company logo, which appears in the upper left corner of the Operator page under the application name. If you upload an image that is too large, VSOM automatically resizes it to fit. This setting is used to customize the appearance of the VSOM user interface.
Logo Link	Check the checkbox and enter a web address beginning. This site appears when a user clicks the company logo in the VSOM GUI.
Login Image	Upload an image, such as a company logo, to be displayed on the user login page. If you upload an image that is larger than 250 x 310 pixels, VSOM automatically resizes it to fit. This setting is used to customize the appearance of the VSOM user interface.

Generating Reports

VSOM includes the reports listed in Table 6-7.

Table 6-7 Report Settings

Item	Description
User Activity Report	Displays information about user login sessions. Specify a start and end date and time for the information in the report, and choose whether to include the root account.
Device Configuration Report	Displays details about the devices in the system that are involved in providing camera feeds.
Run-Time Statistics	Displays information about system activity, including the type of activity and number of current items or sessions.
Application Log File	Opens a window that shows a log of system-related activity.
Event History	Lists the events that have occurred on the system. Specify a date range, or choose **Show All Events**. You can search for or filter events in the list. For more information, see the "About Events" section on page 6-1. Click the **export data to csv** icon to export the list to a comma-separated value (CSV) file. **Note** Deleting an event deletes all of the event histories for that event.

To generate a report, follow these steps:

Procedure

Step 1 Click Reports in the Administrator pages.

Step 2 Click the link for the report type to generate (see Table 6-7.)

Step 3 If prompted, specify a time interval, and click **Submit** to display the report.

You can sort information in a report in ascending or descending alphanumeric order by any column. To do so, click a column name as needed to toggle the sort order.

Most reports include a search option. Enter search text and click **Search** to display matching entities.

Displaying System Overview Information

You can display information about disk space use on VSMS hosts that VSOM manages, and about user login sessions. To do so, choose **Overview** in the Administrator pages.

Table 6-8 describes the System Overview panel.

Table 6-8 System Overview Panel Information

Item	Description
Servers Area	
Media Server	Presents information for each VSMS host that VSOM manages. Click a link to open the Servers panel for the VSMS host that the link identifies. For more information, see the "Importing Archives to a Server" section on page 3-8.
Bar charts	A chart for each VSMS shows the percentage of used (blue) and free (green) space on the server hard drive. The path for the local data repository is also listed.
Show/Hide Details links	Shows or hides information about feeds and archives.
Feeds/ Archives	Shows the number of missing and out of sync camera feeds and archives as a fraction of the total number of feeds and archives. For example, "Missing 3/142" means that there are 3 missing feeds out of a total of 142. Missing means that an expected camera feed or archive is on VSOM but not on VSMS. Out of Sync means that the camera feed or archive is on VSMS but not on VSOM. The out of sync condition typically occurs if a user installs and then reinstalls VSOM, but has not yet performed synchronization. Click the **Feeds** or **Archives** link to display detailed feed information.
Users Area	
Currently Active Users	Lists active user sessions, including the user name and time that the user logged in. For more information about user accounts, see the "Managing User Accounts" section on page 7-5.
User Logins Today	Lists all of the user sessions for the current day (since midnight), including the user name and time that the user logged in. For more information about user accounts, see the "Managing User Accounts" section on page 7-5.

Using the Health Dashboard

The Health Dashboard provides a summary of the overall operational health of your video surveillance system and a detailed list of health event messages that are sent from VSMS hosts. VSOM processes and stores the messages and presents pertinent information on the Health Dashboard page.

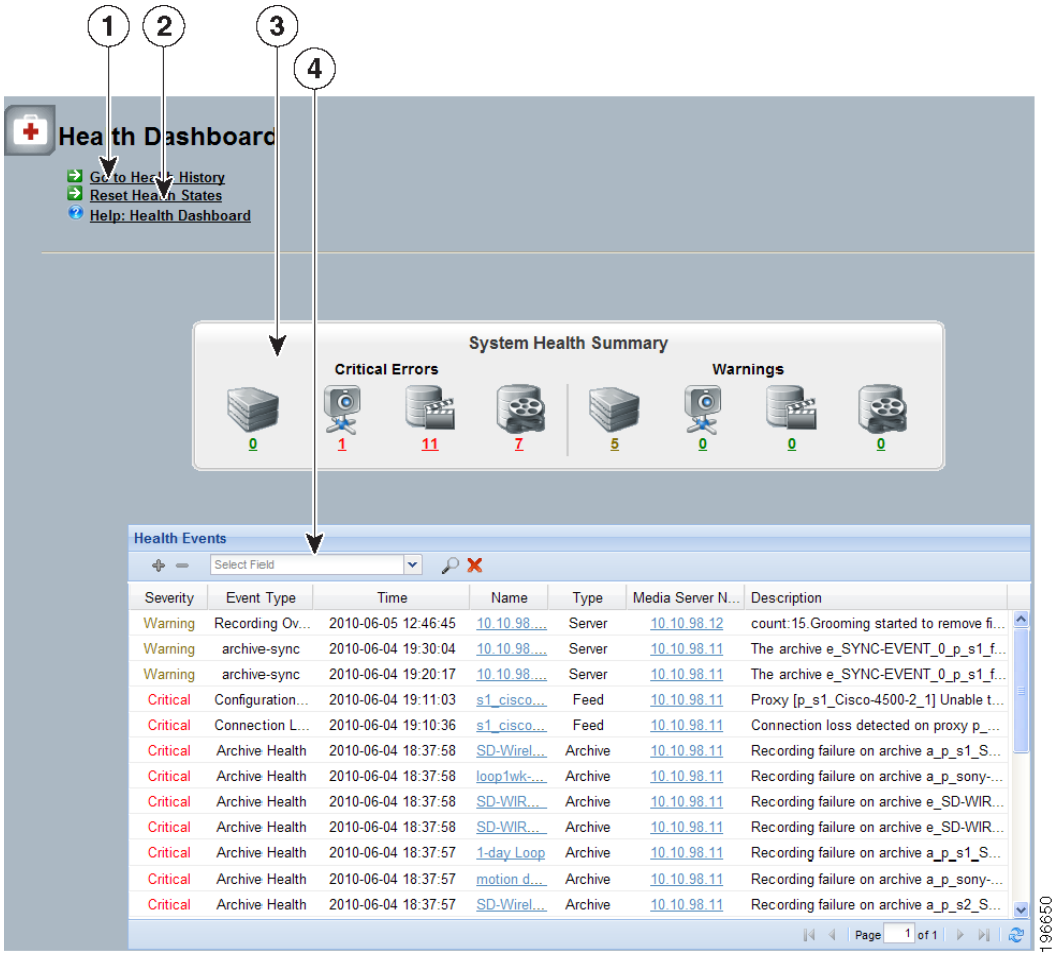
Health events are generated automatically and do not require any user configuration. You can, however, adjust the health event settings on the Settings page. See the "Configuring System Settings" section on page 6-18.

Note

- Health events are not related to the events that you can create in VSOM to capture video surveillance occurrences. See the "About Events" section on page 6-1 for a information about creating video surveillance events.
- The Health Dashboard can only report the NIC Health for the Eth0 port because bandwidth monitoring is supported only on the Eth0 port. Bandwidth monitoring is not supported for other ports.

The main Health Dashboard page is divided into the System Health Summary and Health Events table. Click the refresh icon on your browser at any time to update the display with the latest health events. See Table 6-8.

Figure 6-3 Health Dashboard



1	Link to Health History	**3**	System Health Summary
2	Reset Health States	**4**	Health Events Table

System Health Summary

The System Health Summary appears as a panel of icons and numbered links near the top of the Health Dashboard (see Figure 6-3). The panel provides a count of health related information for the following components (shown as icons from left to right in each section of the System Health Summary):


VSMS server


Endpoints, including cameras and encoders


Camera feeds


Archives (not including shelved archives)

The counts are shown as links under the critical error and warning icons.

- Critical errors are health events that render a component unusable (for example, a server that is down or archives that are unable to record). Components in the critical error 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, if a camera is in the critical error state, all feeds and archives for that camera also are in the critical error state. If there are no critical errors, the link is green; if there are critical errors, the link is red.
- 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 paired "up" and "down" health events.

The icons on the Health Summary show the types of components that have critical errors and warnings. The numeric links below the icons indicate the number of components of that type that are affected. Click a numeric link to display the associated messages in the Health Events table. If there are no warnings, the link is green; if there are warnings, the link is yellow.

If there are multiple errors associated with a condition, the count that appears under the icon does not match the number of messages. For example, if a server has three errors that are associated with its critical error state, the number below the icon is 1, and the Health Event table lists three critical errors for that server.

To reset the current health information, click **Reset Health States**. The Health Events table is cleared, and the warning and critical event counts are set back to 0. Health history is not affected; only the current health table and counts are reset.

Health Events Table

The Health Events table lists information about each health event (Table 6-8). You can sort the table and apply filters. See the "Sorting and Filtering the Health Tables" section on page 6-29.

To display the health history for a component, click the underlined link for that component in the Name or the Media Server column. See the "Health Event History" section on page 6-28 for a description of the Health Event History page.

Table 6-9 Health Events Table Information

Item	Description
Severity	Significance of the event: • Critical errors render a component unusable, such as a camera that is down. • Warnings are events that occur without incapacitating a component, such as interruptions in operation due to packet losses in the network.
Event Type	Event classification, as described. Camera event • Camera Failure—Generated if a camera experiences a hardware failure. Client event: • Client Health—Monitors CPU use and NIC traffic events of a client PC. This event is generated when CPU usage exceeds 90% or when NIC traffic is greater than 60% of available bandwidth. Media stream (camera feed) events: • Feed Health—Generated when the proxy changes state. Reflects the state of the camera feed: – Create: Operation management application creates a media stream. – Start: Media device is reachable and configured with the stream settings. The configured device streams media. – Stop: Media device stops streaming stream media. • Device Unreachable—Generated when the media device is unreachable. Traps are generated every 10 minutes if the condition persists. • Connection Loss—Generated when connection is lost to the media device (when there is no media data for more than 30 seconds). • Configuration Failure—Generated when a configuration failure is detected while applying the configuration on the media device. Traps are generated every 10 minutes if the condition persists.

Table 6-9 Health Events Table Information (continued)

Item	Description
Event Type (continued)	RAID events • Missing—Provides information when a hard drive is not detected. • Rebuild—Provides information when hard drive is rebuilding. • Optimal—Provides information when a hard drive is rebuilt and operating. Recording events: • Archive Health—Generated when the recording does not receive any video packets from the VSMS for about 30 seconds. Traps are generated every 10 minutes if the condition persists. • Archive State—Generated when the recording changes state: – start: New recording starts. – stop: Recording stops. – remove: Recording is removed from the disk. – pause: Recording pauses to record any more data. – resume: Recording resumes recording media data. – reset: Recording restarts to apply a new configuration or attempts to respond to a configuration failure. – setevent: Archive is marked between two time intervals (for clipping). – update: Recording is updated with new settings. – rename: Recording name is changed. • Archive Video Loss—Generated when the recording receives no video packets from the feed for approximately 30 seconds. • Archive Synch—Warning event indicating that an error occurred when creating an archive. The event description on the health dashboard provides the reason for the error. • Recording OverSubscribed—Generated when grooming starts to remove archive files before their retention period ends because insufficient disk space is available for the archiver to record new media data. Traps are generated every 10 minutes if the condition persists. • Recording Health—Generated when the recording changes state.

Table 6-9 Health Events Table Information (continued)

Item	Description
Event Type (continued)	VSMS events: • Server Health—Generated when the server health changes state. • NIC Health—Generated when the server link bandwidth exceeds 60% of the threshold. In half duplex mode, the interface card sends or receives bytes, but not at the same time. In this case, the threshold is 60% of total throughput (send and receive combined). In full duplex mode, bytes are sent and received concurrently. In this case, the threshold for full duplex card is 60% of traffic sent or 60% of traffic received. Traps are sent every 3 minutes. • Disk Usage—Monitors disk use of a partition to ensure that available disk space is above the a set limit. By default, all available partitions are monitored and a trap is generated when available disk space is below 10% of the total available space.
Time	Date and time that the event occurred.
Name	Link to the specific component (server, camera/encoder, feed, or archive) that generated the event.
Type	Type of component (server, camera/encoder, feed, or archive) that generated the event.
Media Server Name	User-assigned name of the VSMS associated with the event.
Description	Text description of the event, as generated by the component. If multiple warnings of the same type are generated during the current reporting interval, a single entry is presented with a count that indicates the number of occurrences. For example, the following entry indicates that 5 "NIC traffic exceeded 60%" events have been received since the last Health History Retention reset. `Count 5: NIC traffic exceeded 60%` The current reporting interval is configured on the Settings page (default is 1 day). See the "Configuring System Settings" section on page 6-18 for information on the Settings page and Table 6-6 for a description of health history retention.

Health Event History

An event specifies information about an action that VSOM takes in response to a change in conditions (the event trigger). The Health Event History panel provides detailed information about the events that are associated with a selected component.

The panel includes a details area at the top of the page and a Health History table at the bottom of the panel.

The Health History table includes the same columns that are described in Table 6-8. See the "Sorting and Filtering the Health Tables" section on page 6-29 for information about sorting and filtering the table.

You can access the Health Event History page in either of the following ways:

- Click an underlined link in the Name or Media Server column in the Health Events table.
- Click the **Go to Health History** link on the Health Summary page of the Health Dashboard. If you access the page by using this method, you must then click an underlined link in the Name or Media Server column of the Health Event History table to display the details.

The details that are presented for a selected component depend on the component type.

- Servers—Displays the same server details that are presented on the System Overview page. See the "Displaying System Overview Information" section on page 6-22.
- Cameras and encoders—Displays the component configuration and the associated camera feed configuration.
- Feeds—Displays feed information and media settings.
- Archives—Displays the archive configuration, video settings, and schedule

Note To view the details for an item, you must be assigned a role that allows you to view that item. For information on role, see the "About Role Settings, Permissions, and Rights" section on page 7-2.

Sorting and Filtering the Health Tables

You can sort information in the Health Events table or the Health History table in ascending or descending alphanumeric order by any column. To do so, click a column name as needed to toggle the sort order.

To filter Health Events or Health History events in the table, follow these steps:

Procedure

Step 1 Choose a column from the drop-down list at the top of the table.

Additional drop-down lists or fields appear for matching categories and value or range.

Step 2 Choose a matching category from the second drop-down list and specify the value or range:

- For Severity, choose a severity of Critical or Warning from the Select Field drop-down list.
- For Event Type, choose a type from the Select Field drop-down list.
- For Time, enter the start date and end date in the From and To fields.
- For Name, Media Server Name, or Description, choose one of the following matching criteria then enter the desired value in the Enter Value field:
  - **Equals**—Displays entries that exactly match the value.
  - **Not Equals**—Displays entries that do not match the value.
  - **Like**—Displays entries that contain the value. For example, the value "elco" matches all "Pelco" entries.
- For Type, choose the category type.

Step 3 Take any of these actions:

- To add filters, click the icon to the left of the filter area
- To remove a filter, click the icon.

- To clear all filters, click the icon.

Step 4 To filter the table based on the specified criteria, click the icon.

The table is updated to match the filters that you entered.

CHAPTER 7

Managing Accounts

This chapter describes how to set and manage user roles and accounts. It includes these topics:

About User Account Management

VSOM supports the creation of user accounts for the administrators and operators who use the VSOM system. By creating user accounts, you can control who has access to the system and keep track of how the system is used and by whom.

User accounts include the following information:

- User information, including user name, password, and contact details.
- Predefined view that a user sees by default in the Operator page. See "Managing Predefined Views" section on page 5-24 for more information.
- Schedules that optionally control when a user is able to access the system.
- Roles that determine which items a user can view and change within VSOM. Roles include settings, permissions, and rights, as described in the "About Role Settings, Permissions, and Rights" section on page 7-2.
- Custom fields that you can use to store additional information about a user.

About Roles

Each user account comes with assignment of roles. Roles determine which items a user is permitted to view and change within VSOM. All users must be assigned at least one role and can be assigned up to 100 roles.

An administrator role can optionally include the Pseudo Root designation, which provides unrestricted access to the VSOM host. A user with a role that has Pseudo Root assigned can do everything that the root user can do with additional personalization of login information permitted. At least one administrator should be assigned a role with the Pseudo Root designation.

The following table describes the default roles. VSOM allows you to create additional roles, as described in the "Setting Up Roles" section on page 7-8.

Table 7-1 Default Roles

Role	Description	Comment
Administrator	Provides authority to manage and display all VSOM resources. Can assign root-level access.	At least one administrator account is required to manage VSOM.
Operator	Provides limited authority, typically to display a portion of system resources, such as cameras and archives that a user is responsible for monitoring.	Create an operator account for each user.

About Role Settings, Permissions, and Rights

Each role includes specification of settings (or preferences), permissions, and rights. A role can be assigned to one or more users, and a single user can have one or more roles. If a user is assigned multiple roles, the role with the most generous permissions and rights takes precedence over the other roles.

Best Practices

- Use the default Administrator and Operator roles without modifying their settings (except to assign Pseudo Root to the Administrator role, if desired).
- If you want to assign additional permissions and rights to users, create new roles to do so.

The basic settings (*preferences*) for a role determine general privileges, which are sufficient for many installations. These settings include the following:

- Pseudo Root—This setting provides access to all resources. A user with a role that has Pseudo Root assigned can do everything the root user can do by using an individual user login rather than the general root user login. By using pseudo root, you can provide for better tracking of which user is logged in and using the system.
- Administrative Preferences—With this setting, a user can open the Administrator pages. The functions that the user can perform on the Administrator pages are determined by permissions and rights.

Note The Pseudo Root preference does not automatically include access to the Administrative pages. You must specify Administrative Preferences to allow access to the Administration pages even if you also choose Pseudo Root.

- Operator Preferences—This setting determines the type of access and interaction that are permitted on the Operator page:
  - View Only—Provides access only to predefined views on the Operator page. This option restricts the privileges that are assigned to the default Operator role.
  - View Options—Restricts the ability to override the display options for a view.

Permissions and rights add finer-grained control of roles and are useful for large deployment in which users perform specialized functions.

- Permissions are action-based and determine the general ability of a user to perform operational functions, such as managing camera feeds, archiving local clips, and modifying schedules.
- Rights restrict privileges to specific device models, events, archives, schedules, servers, and views. For a user to have rights in any area, permission to that area must be granted.

  For example, a user who is an installer may be assigned a "Pelco Installer" role, to manage Pelco cameras. The role must include *permissions* to manage cameras and feeds in general along with *rights* to manage Pelco cameras and feeds.

The following guidelines apply to roles:

- Each category for permissions and rights can be set to one of the following:
  - **None**—The category or item is not visible to the user
  - **View**—The user can see but not modify the category or item
  - **Manage**—The user can view, add, edit, and delete the category or item
- For roles with Administrator privileges, permissions are a prerequisite for rights. For example, an administrator must have permission to manage camera feeds to have the right to manage camera feeds for a specified type of camera.
- For roles with Operator but not Administrator privileges, only the rights for archives, camera feeds, monitors, and encoders apply. The camera feed rights determine which camera feeds are visible in the side menu of the Operator page.
- If a user is granted conflicting permissions and rights, then the most restrictive settings apply.

Table 7-2 shows examples of the relationship between permissions and rights.

Table 7-2 Permission and Rights Examples

Permissions	Rights	Description
None	None	The administrative icons for the resource are not displayed and individual items are not displayed in the side menu.
None	Manage	The administration icons for the resource are not displayed and the individual items with View rights are displayed in the side menu. (The use of Manage rights in this case adds no additional capabilities.)
Manage	View	The administration icon for the resource is not displayed and the individual items with View rights are listed inside the administration icon and in the side menu. This setting permits a role with Administrator privileges to display the settings for some resources.

About User Authentication

When a user tries to access VSOM, an authentication process takes place to determine whether access is allowed and, if allowed, to log the user in. The following options are supported for authenticating users who attempt to access VSOM:

- Local login/password—With this option, the VSOM server maintains user login information about locally on the VSOM server. Login information is entered in the User page, as described in the "Adding a User" section on page 7-5.
- LDAP—With this option, an existing Lightweight Directory Access Protocol (LDAP) services is used to authenticate users. If you use this option, you cannot change the user password in the VSOM interface. For more information, see the LDAP configuration information in the "Operations Manager Configuration Page" section on page 10-19.

Working with LDAP

LDAP is used to access directory servers. Directory servers access a database that holds information in a tree structure, similar to a hard disk directory structure. Administrators can navigate to the subdirectory by using path names similar to /usr/local/myapp/docs.

VSOM does not import groups or users from the LDAP server. You must create each LDAP user in VSOM and assign LDAP authentication (not local authentication) in the VSM Management Console (VSMC). The user name that is assigned for VSOM must be identical to the user name in the LDAP system. See Chapter 10, "Using the VSM Management Console," for instructions on configuring LDAP authentication.

Use the Video Surveillance Management Console to configure VSOM to work with an LDAP server, as described in the "Operations Manager Configuration Page" section on page 10-19.

Table 7-3 lists the LDAP parameters.

Table 7-3 LDAP Parameters

Item	Description
LDAP_HOST_NAME	Enter the IP address or the host name of the LDAP server to be used to authenticate user log in credentials. For example, ds.cisco.com.
LDAP_HOST_PORT	Optional parameter. Port number of the LDAP server that is used to authenticate user log in credentials. If this field is blank, the value 389 is used.
LDAP_RDN_DN	LDAP RDN[1] to be used for authentication. In the RDN, the token %username% is replaced dynamically with the user name when a user attempts to log in. For example: CN=%username%,OU=Employees,OU=cisco users.
LDAP_DCS	List of DCs[2] in order of precedence and separated with semicolons (;). The system verifies the authentication bind against each DC in order until a successful bind is achieved or there are no more domain controllers. For example: DC=amer, DC=cisco,DC=com; DC=euro,DC=cisco,DC=com

1. RDN = Relative Distinguished Names.
2. DC = Domain Controller.

Managing User Accounts

Click **Users** on the side menu in the Administrator pages to open the Users page. Table 7-4 lists the tasks that you can perform on this page.

Table 7-4 Users Panel Tasks

Task	Description	Reference
Add a user	Create a new user account	Adding a User, page 7-5
Edit or delete a user account	Make changes to an existing account or delete an account	Editing or Deleting a User, page 7-6
Edit user custom field labels	Create custom fields to store and display additional information	Creating Custom Field Labels for Users, page 7-6
Synchronize user accounts	Make user account information consistent across multiple VSOM servers	Configuring User Account Synchronization, page 7-12
Display current user account settings	Show the current configuration for a user account	Displaying User Information, page 7-7

Adding a User

Adding a new user involves specifying login and contact information and roles. You also can specify a default view and an access schedule.

Before You Begin

- Set up roles, as described in the "Setting Up Roles" section on page 7-8.
- Decide whether to use local authentication or LDAP authentication, as described in the "About User Authentication" section on page 7-4.
- Decide whether to set up parent/child relationships between servers, as described in the "Managing Encoders" section on page 3-12.
- Define schedules, as described in the "Managing Schedules" section on page 6-16.

To add a new user, follow these steps:

Procedure

Step 1 In the Administrator pages, click **Users**.

Step 2 Click **Add User**.

Step 3 In the User Name field enter a unique user login name (up to 30 characters, including spaces). The name is not case-sensitive.

Step 4 Choose the **Local Password** or the **LDAP** option to designate whether the user authentication is managed by the local VSOM server or by an LDAP server.

If you choose **Local Password**, enter a password and then re-enter the password in the Confirm Password field. Passwords must contain 5-10 characters and are case-sensitive.

If you are using LDAP, see the "Working with LDAP" section on page 7-4.

Step 5 Enter the user contact information in the First Name and Last Name (up to 64 characters each) and Email field (up to 255 characters).

The e-mail address is used for notifications.

Step 6 From the **Status** drop-down list, verify that the status is **Enabled**.

A user must be enabled to be able to access VSOM.

Step 7 (Optional) Choose a view from the **Default View** drop-down list if you want the user to see a specified view when opening the Operator page.

See the "Managing Predefined Views" section on page 5-24 for information about configuring views. If you do not specify a view, the video pane in the Operator page presents a message indicating that a default view has not been configured and provides links to complete the setup or specify a view.

Step 8 (Optional) Click the **Schedule** tab to restrict user access according to a predefined schedules, as follows.

- Default State—Choose the user status (Enabled or Disabled) to apply when a schedule is not running. For example, if you want to allow the user to access VSOM only during specific times, choose **Disabled** as the default. Choose **Enabled** if you want to allow the user to access VSOM except as restricted by the schedule.
- Simple Schedule—Choose the schedule from the drop-down list. A simple schedule runs once from a specified start time to a specified end time.
- Recurring Schedule—Choose the schedule from the drop-down list. A recurring schedule runs multiple times according to specified rules.

See the "Managing Schedules" section on page 6-16 for information about defining schedules.

Step 9 Click the **Custom Fields** tab and enter values for any custom fields that have been defined (see the "Creating Custom Field Labels for Users" section on page 7-6).

Step 10 Click the **Roles** tab and check the check boxes for the roles that you want to assign to the user.

Step 11 Click **Submit**.

Editing or Deleting a User

To edit user settings, click the **Edit** icon for the user in the Actions column on the Users panel and make changes on any of the tabs.

To change the user password, click the **Change Password** button on the Details tab. Enter the password, re-enter it to confirm, and then click **Submit**. Passwords must contain 5-10 characters and are case-sensitive.

To delete the user account from the VSOM database, click the **Delete** icon and then click **Yes** to confirm. If a user account is deleted while a user is logged in, the user is allowed to complete the login session.

Creating Custom Field Labels for Users

Custom field labels allow you to specify custom fields to record additional information about a user. The custom fields are shown on the Custom Fields tab when you edit a user record.

To create custom fields labels, follow these steps:

Procedure

Step 1 Click the **Edit User Custom Field Labels** link above the list of users to open the Custom Fields configuration page.

Step 2 Enter up to 20 field labels in the order in which you want them to appear.

Labels that are left blank are ignored.

Step 3 Click **Submit**.

Displaying User Information

Click the underlined link for a user on the Users panel to display the current settings for the user, as described in Table 7-5

Table 7-5 User Information

Item	Description
Details Tab	
User Name	Name that the user uses to log in to VSOM.
Status	Indicates whether the user has system access (enabled) or is denied access to VSOM. Users are immediately logged out if their user status changes to disabled.
First Name	First name of the user.
Last Name	Last name of the user.
Description	Optional description.
Email	Optional e-mail address of the user.
Default View	Layout that the user sees by default when opening the Operator page.
Scheduling Tab	
Default State	State of the user account when there is no running schedule. Displayed only if a schedule is assigned to the user.
Simple Schedule	Information about the simple scheduled assigned to this user. Displayed only if a simple schedule is assigned to the user.
Recurring Schedule	Information about the recurring scheduled assigned to this user. Displayed only if a recurring schedule is assigned to the user.
Custom Fields Tab	
Custom Fields	Settings of any custom fields that have been defined.
Roles Tab	
Role Name	Roles assigned to the user.
Status	Indicates whether the role is active for or inactive for the user. If a role is active, then the user is subject to the permissions and rights assigned to that role. If multiple roles are assigned to the user, then the most restrictive role takes precedence.

Setting Up Roles

Roles determine which items a user is permitted to view and change within VSOM. All users must be assigned at least one role and can be assigned up to 100 roles.

Click **Roles** on the side menu in the Administrator pages to open the Roles page. This page contains links to manage roles. It also includes a table that lists information about roles and provides various links and buttons.

Table 7-6 lists the tasks that you can perform on this panel. For more information about roles, see the "About Roles" section on page 7-2.

Table 7-6 Roles Panel Tasks

Item	Description	Reference
Add a new role	Create a new role	Adding a Role, page 7-8
Modify, copy, or delete a role	Make changes to an existing role, create a new role with the same settings as a specified role, or delete a role	Editing, Copying or Deleting a Role, page 7-10
Assign users to roles	Understand the options for assigning users to role	Associating Users with Roles, page 7-10
Display current role settings	Show the current configuration for a role	Displaying Role Information, page 7-10

Adding a Role

When you add a new role, you specify the preferences, permissions, and rights for the role. See the "About Role Settings, Permissions, and Rights" section on page 7-2 for information about these attributes.

Before You Begin

- Create a list of the roles that you need for your VSM installation. The list should include the permissions and rights for each role.
- Determine the desired administrative or operator settings for the role and whether any customer permissions or rights are required.
- Define any needed schedules, as described in the "Managing Schedules" section on page 6-16. The schedule determines when the role is active.

To add a new role, follow these steps:

Procedure

Step 1 In the Administrator pages, click **Roles**.

Step 2 Click **Add New Role**.

Step 3 In the Role Name field, enter a name to identify the role (up to 30 characters, including spaces).

Step 4 (Optional) In the Description field, enter a description (up to 1024 characters, including spaces).

Step 5 From the **Status** drop-down list, verify that the status is **Enabled**.

Step 6 In the **PTZ Priority** field, determine the PTZ priority.

The PTZ priority determines how a camera responds when it receives PTZ commands from two or more devices simultaneously. The command with the highest PTZ priority is applied to the camera and the lower priority commands are ignored.

Step 7 In the Administrative Preferences area, choose **Pseudo Root** if you want the role to include access to all resources in the system, and choose **Administrative Preferences** if you want the role to allow access to the Administration pages.

You must choose **Administrative Preferences** to allow access to the Administration pages even if you also choose **Pseudo Root**. For more information about preferences, see the "About Role Settings, Permissions, and Rights" section on page 7-2.

Step 8 In the Operator Preferences area, specify the following:

- Check the **View Only** check box if you want to allow a user to view video only with predefined views. A user who has a role with this setting sees an Operator page with the video player and a drop-down list of predefined views to select for display in the video player.
- Check the **View Option: Disabled** check box if you do not want users to have access to video play controls in the Operator page. If a user with this check box checked views the Operator page, video player control options such as title bars, video tools, and timestamps are disabled.

If you choose **View Only** you cannot also choose **View Options**. For more information about preferences, see the "About Role Settings, Permissions, and Rights" section on page 7-2.

Step 9 Click the **Schedule** tab and configure the following settings if you want to limit system access for users with this role to a specified schedule:

- Default State—Choose the user status (Enabled or Disabled) to apply when a schedule is not running. For example, if you want to allow the user to access VSOM only during specific times, choose **Disabled** as the default. Choose **Enabled** if you want to allow the user to access VSOM except as restricted by the schedule.
- Simple Schedule—Choose the schedule from the drop-down list. A simple schedule runs once from a specified start time to a specified end.
- Recurring Schedule—Choose the schedule from the drop-down list. A recurring schedule runs multiple times according to specified rules.

See the "Managing Schedules" section on page 6-16 for information about defining schedules.

Step 10 Click the **Permissions** tab and choose radio buttons to specify **None**, **View**, or **Manage** permissions for each permissions category:

- None—Users assigned to this role cannot view, add, modify, or delete items in this category.
- View—Users assigned to this role can view but not add, modify, or delete items in this category.
- Manage—Users assigned to this role can view, add, modify, and delete items in this category.

Click the **All** link at the top of the None, View, or Manage column to choose all of the permission categories in that column.

Step 11 Click the **Rights** tab, click the **+** symbol as needed to expand a functional area, and choose radio buttons to specify **None**, **View**, or **Manage** permissions for each area:

- None—Users assigned to this role do not have rights to view, add, modify, or delete items in this functional area.
- View—Users assigned to this role can view but not add, modify, or delete items in this functional area.
- Manage—Users assigned to this role can view, add, modify, and delete items in this functional area.

Click the **All** link at the top of the None, View, or Manage column for a general functional area to choose all of specific items in that functional area. For example, click **All** in the Manage column for cameras to specify management rights for all cameras in the VSOM database.

Step 12 Click **Submit**.

Associating Users with Roles

You can associate users with roles in either or both of the following ways:

- On the Roles Panel—Click the **Users** tab and check the check boxes for the users to which you want to assign the role.
- On the Users Panel—Click the **Roles** tab and check the check boxes for the roles that you want to assign to a user.

If you specify assignments by using one of these panels, your selections are shown when you open the other panel.

Editing, Copying or Deleting a Role

To edit role settings, click the **Edit** icon for the role in the Actions column on the Roles page and make changes on any of the tabs, as described in the "Adding a Role" section on page 7-8. To create a new role with the same settings as a specified role, click the **Copy** icon . Enter a new role name, change any other settings as desired.

To delete a role from the VSOM database, click the **Delete** icon and then click **Yes** to confirm. When the role is deleted, it is removed from all the users who had that role assigned. If a role is deleted while a user with the role is logged in, the user is allowed to complete the login session, but permissions and rights for the deleted role are no longer available.

Displaying Role Information

To display settings for a role, click the underlined link for a role on the Roles panel. Table 7-7 describes the role settings.

Table 7-7 Role Settings

Item	Description
Details Tab	
Role Name	Name that a user uses to log in to VSOM.
Description	Optional description.
Status	Indicates whether the role allows access to VSOM (enabled) or does not allow access.
PTZ Priority	Priority when a camera receives more than one PTZ command at the same time. The command with the highest PTZ priority is applied to the camera and the lower priority commands are ignored. PTZ priority applies to user actions and events.

Table 7-7 Role Settings (continued)

Item	Description
Pseudo Root	Indicates that the role provides unrestricted access to the VSOM host. A user with a role that has Pseudo Root assigned can do everything that the root user can do with additional personalization of login information permitted.
Administrative Preferences	Indicates whether the role permits access to the Administrator pages. You must choose **Administrative Preferences** to allow access to the Administration pages even if you also choose **Pseudo Root**.
View Only	If checked, indicates that users with this role can view video only using predefined views. A user who has a role with this setting sees an Operator page with the video player and a drop-down list of predefined views to select for display in the video player.
View Options	If checked, users with this setting do not have access to video play controls in the Operator page. If a user with a role that has this setting logs in and views the Operator page, the video player control options such as title bars, video tools, and timestamps are disabled.
Users Tab	
Role Users	List of the users who have this role assigned. Click the underlined user link to display details about the user.
Scheduling Tab	
Default State	State of the role when there is no running schedule. Displayed only if a schedule is assigned to the role.
Simple Schedule	Information about the simple scheduled assigned to this role. Displayed only if a simple schedule is assigned to the role.
Recurring Schedule	Information about the recurring scheduled assigned to this role. Displayed only if a recurring schedule is assigned to the role.
Permissions Tab	
Permission Type	Level of permission assigned to each function in the list: • None—No access to this function. Any associated GUI elements such as preferences, archive clips, and archive local clips are not displayed. • View—Read-only access to this function. Add, edit, and delete functions, icons, and links are not displayed. • Manage—Read/write access to this function.

Table 7-7 Role Settings (continued)

Item	Description
Rights Tab	
Role Rights	Rights assigned to the role for each function in the list (clicking the + symbol expands the list for a category and clicking the – symbol collapses the list for the category): • None—No access to this function. Any associated GUI elements such as preferences, archive clips, and archive local clips are not displayed. • View—Read-only access to this function. Add, edit, and delete functions, icons, and links are not displayed. • Manage—Read/write access to this function.

Configuring User Account Synchronization

The user account synchronization feature allows you to automatically copy selected users and roles from one VSOM server to another VSOM server. For the purpose of user account synchronization, the server from which users and roles are copied is called the *parent* server and the server to which the users and roles are copied is called the *child* server. For example:

- If you are logged into Server A and define Server B as a parent server, Server A is the child server and user accounts are synchronized from Server B to Server A.
- If you are logged into Server A and define Server C as a child server, Server A is the parent server and user accounts are synchronized from Server A to Server C.

Before You Begin

- Determine the IP address or host name of each server that is to be a parent or child server.
- For each role and user that you want to include in synchronization, make sure that the user is chosen in the Users tab for the role (see the "Setting Up Roles" section on page 7-8).

To configure user account synchronization, follow these steps:

Procedure

Step 1 In the Administrator pages, click **User Account Sync**.

Step 2 Configure the following information for each VSOM server that you want to designate as the parent server:

- Check the **Authorize** check box.
- In the Parent Server Name field, enter the name that is assigned to the server in VSOM.
- In the Host IP/Name field, enter the host name or IP address of the server that you want to designate as a parent server.
- In the Set Passphrase and Confirm Passphrase fields, enter and confirm a password that the child server uses to access the parent server.

Step 3 To add an additional parent server, click **Authorize Another Parent Server** and enter information for that server.

Step 4 Click the **Child Servers** tab.

Step 5 Configure the following information for each VSOM server that you want to designate as the child server.:

- Check the **Add** check box.
- In the Child Server Name field, enter the name that is assigned to the server in VSOM.
- In the Host IP/Name field, enter the host name or IP address of the server that you want to designate as a child server.
- In the Passphrase field, enter a passphrase for the child server to use to access the parent server.
- In the Availability column, click **Check** to determine whether the child server is available for connection to the parent server. Availability is checked and the result appears in the Results column.

Step 6 Click **Finished**.

Step 7 For each role and user that you want to include in synchronization, make sure that the user is chosen in the Users tab for the role. See the "Editing, Copying or Deleting a Role" section on page 7-10.

User account synchronization is now configured, and user accounts and roles that are updated on the parent server are automatically updated on the child server.

The following information applies when managing parent/child relationships for user account synchronization (examples assume Server A is the child server and Server B is the parent server; however, note that multiple parent and child servers are supported):

- Synchronization affects only user accounts. It does not affect other configuration settings.
- To enable the two servers, A and B, to communicate with each other for user account synchronization, you must log in to Server A and set Server B as the parent, and also log in to Server B and set Server A as the child.
- The passphrases that you enter into Server A and Server B must be identical.
- You must check the **Authorize** check box on the Parent Servers tab of the User Account Synch panel for all of the parent servers that are involved in user account synchronization. To remove a parent server from the list of servers involved in synchronization, uncheck the **Authorize** check box. After you submit the change, the server is no longer available for synchronization.
- You must check the **Add** check box on the Child Servers tab of the User Account Synch panel for all of the child servers that are involved in user account synchronization. To remove a child server from the list of servers involved in synchronization, uncheck the **Add** check box. After you submit the change, the server is no longer available for synchronization.
- Role modifications on the parent server, including assignments of users to the role, are applied to the role on the child server when synchronization takes place.
- Roles that have a parent user assigned cannot be deleted.
- Users on the parent server cannot delete accounts on the child server or change the rights associated with roles on the child server.

PART 3

Operator Reference

CHAPTER 8

Using the VSOM Operator Pages

The VSOM Operator Pages provide access to features that video surveillance operators can use to view, record, search, and control video. This chapter describes the Operator Pages in detail. It includes these topics:

Understanding the Operator Window

The Operator window allows operators to view live and archived video, search for video events and motion, and control pan/tilt/zoom (PTZ) cameras. To access the Operator window, take either of these actions:

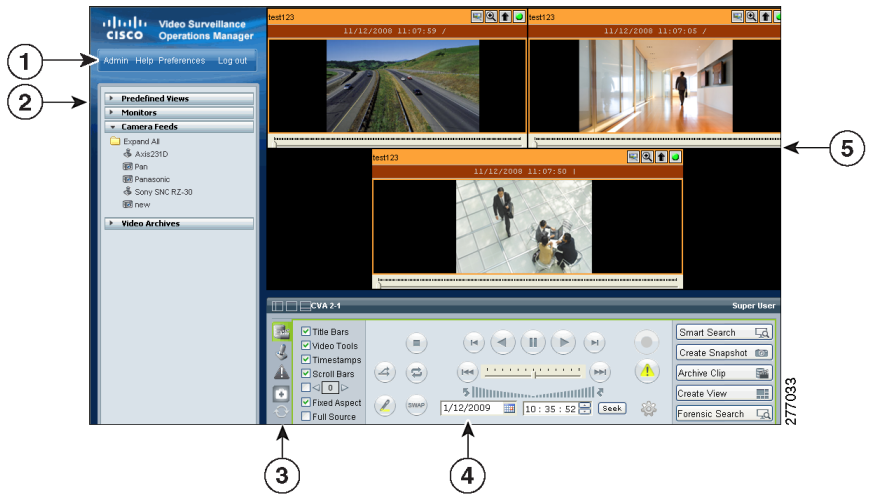
- Start VSOM and display the Operator pages, as described in the "Accessing VSOM" section on page 1-4.
- If you are viewing a VSOM Administrator page, click the **Ops** link, which appears near the top left of the page.

If you have defined a default view, this view appears when you access the Operator page. See the "Understanding and Defining the Default View" section on page 8-3 for more information.

Tip You can mouse over most icons in the Operator pages to see a short description.

Figure 8-1 shows the main elements of the Operator page.

Figure 8-1 Operator Window Overview



1	Control links. Includes these links: **Admin**—Opens the VSM Administrator pages. When you are viewing an Administrator page, this link changes to Ops. Clicking the Ops link displays the Operator pages. **Note** The Admin link appears only if you are assigned the Administrator role. See Chapter 7, "Managing Accounts" for more information. **Help**—Displays a new window with access to information about VSM and its features. **Preferences**—Displays your user name, and provides access to options for entering your name and changing your password. Also provides options for your default view and your PTZ and joystick settings. **Log out**—Logs you out of VSM.
2	Side menu. Includes these drawers: • **Predefined View**—Choose a predefined view to display a set of video panes from live or archived sources. See the "Using Predefined Views" section on page 8-5 for more information. • **Monitors**—Allows you to transfer video playing in a video pane to a physical monitor, or to view the video from a physical monitor in a selected pane. See Sending Video to a Monitor or Viewing Video from a Monitor, page 8-13 for more information. • **Camera Feeds**—Choose a feed to view live video from a camera. • **Video Archives**—Choose an archive to view recorded video. Video archives mirror the cameras listed under Camera Feeds.

3	Toolbar icons. Click an icon to display any of these toolbars: • **Feed/Archive Controls**—See the "Understanding the Toolbars" section on page 8-23. • **PTZ Camera Controls**—See the "Using the Camera PTZ Controls" section on page 8-34. • **Events**—See the "Viewing Video Events" section on page 8-36. • **System Health**—See the "Using the Health Dashboard" section on page 6-23. • **Refresh**—Refreshes the items in the left side menu, including predefined views, monitors, camera feeds and video archives. The icon appears highlighted when any of the lists have changed. For example, it appears highlighted when you modify a view or save a video clip.
4	Toolbars. Controls and options for the selected toolbar. Click an icon to display the controls (see row 3 in this table)
5	Video panes. Displays video from the selected live or archive sources. Panes display according to the selected predefined view. See the "Using Predefined Views" section on page 8-5 and "Viewing Live and Archived Video" section on page 8-7.

Understanding and Defining the Default View

The default view defines the video pane layout that appears when you log in to VSOM. This default view can display video from one or more live or archived sources, and is selected from the list of predefined views (see the "Using Predefined Views" section on page 8-5 to create views).

Tip The Administrator pages can also be assigned as the default view.

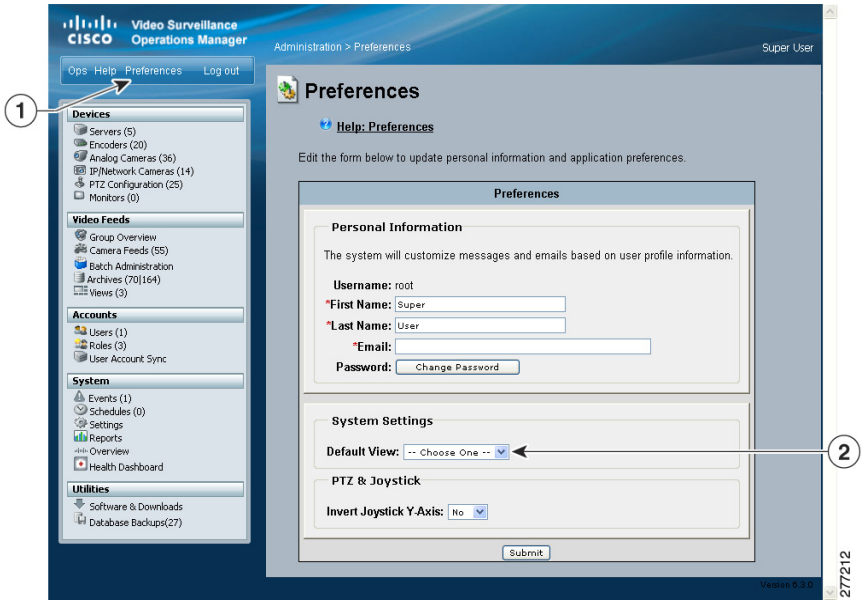
To assign a default view for your account, follow these steps:

Procedure

Step 1 Click the **Preferences** button (see Figure 8-2).

Step 2 Choose a **Default View** (under System Settings).

Figure 8-2 Preferences



1	Preferences button
2	Default View menu

Administrators can assign a default view in the Users configuration page. See the "Adding a User" section on page 7-5 for more information.

Note If a default view is not configured, the following message appears: "The application has not been configured to display a default operator view." Click the links below this message to continue to the Administration pages or to the Preferences page to define a default view.

Setting Operator Preferences

Click the **Preferences** button shown in Figure 8-2, and choose the following options:

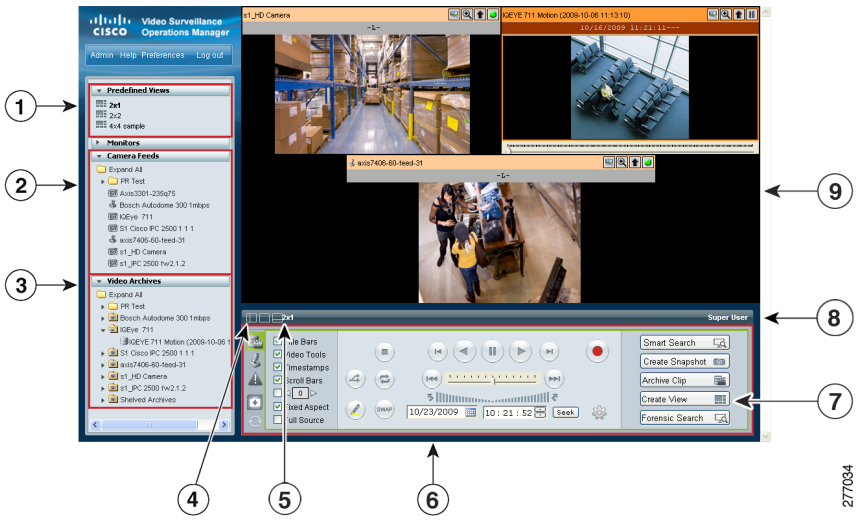
- Personal Information
  - Enter the First Name and Last Name that appears in the upper right of the window for the current account.
  - Enter the Email address that receives system messages for the current account.
  - Click the **Change Password** button to enter a new password.
- System Settings:
  - Select the Default View that will appear when you first log in. See the "Understanding and Defining the Default View" section on page 8-3.
- PTZ & JoyStick
  - **Select** No to accept the default Joystick y axis.
  - Select **Yes** to invert the joystick y-axis.

Using Predefined Views

Predefined Views provide an optional way to save and display one or more video panes from live or archived sources. For example, a predefined view might display four video panes, each with video from a different live or archived source. Another view might display video from three different sources.

In Figure 8-3, the predefined views are listed in the top left. To choose a predefined view, click the arrow next to **Predefined Views** and choose a view name. When selected, the video panes on the right display the live and archived video for that view. All available video sources are listed under **Camera Feeds** (live video) and **Video Archives** (saved video).

Figure 8-3 Predefined Views



1	Predefined Views	**6**	Video control toolbar
2	Camera Feeds (live video)	**7**	Create View button
3	Video Archives (saved video)	**8**	User name
4	Collapse/Expand the left side menu and bottom Toolbar	**9**	Video panes
5	Selected predefined view		

To change the video that a pane displays, click a pane to make it active and then choose a new video source from the **Camera Feed** or **Video Archives** list.

See the "Understanding the Toolbars" section on page 8-23 for information about controlling playback, searching for video, and viewing information about the video source.

Administrator-Defined Views

Administrators can create views that rotate video from multiple sources or are available to specific user roles. For more information,

- See the "Understanding Rotating Views" section on page 8-6
- See the "Managing Predefined Views" section on page 5-24 for information about creating views.

Operator-Defined Views

Operators can create views that are available to other users with the same role as the operator. See the "Creating Predefined Views" section on page 8-6 for instructions.

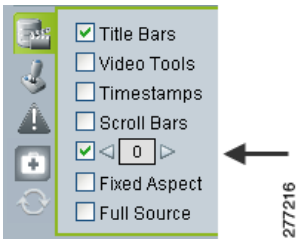
Note Only an administrator can delete views. See the "Managing Predefined Views" section on page 5-24.

Understanding Rotating Views

Administrators can create predefined views that rotate live video from a pool of cameras. Rotating video cycles through a series of views. For example, a view might include four video panes that rotate video from a pool of 10 cameras. Administrators can also *fix* specific panes so the pane only shows the video from a single live source (and is not included in the rotation).

An optional *dwell time* also can be configured to define how long the video from a source appears before video from the next source displays. You also can modify the dwell time by checking the dwell time check box and entering the number of seconds. See Figure 8-4.

Figure 8-4 Setting Dwell Time



See the "Understanding View Option Check Boxes" section on page 8-30 for more information.

Tip When a video pane is active, the video source remains fixed and does not rotate to the next video source. To begin rotating the video again, deactivate the pane by clicking on another pane or on the black background.

Note Only live camera feeds can be included in rotating views.

Creating Predefined Views

Predefined views can be created by either an administrator or by an operator.

- Operators can define views if they have permission to manage views. Operator-created views can be used by other operators with the same role as the operator who created it. For more information about roles and permissions, see Chapter 7, "Managing Accounts."
- Administrators can assign access rights, define the default view, and create rotating views (see the "Understanding Rotating Views" section on page 8-6). To create administrator-defined views, see the "Managing Predefined Views" section on page 5-24.

To create an operator defined view, follow these steps:

Procedure

Step 1 Start VSOM and display the Operator pages, as described in the "Accessing VSOM" section on page 1-4.

If you are already viewing the VSOM Administrator pages, click the **Ops** link near the top left of the VSOM window.

Step 2 Click the **Create View** button 

in the lower right corner of the Operator window (see Figure 8-3 on page 8-5).

Note Verify that the **Display Feed/Archive Controls**  toolbar is selected. Otherwise the **Create View** button does not appear.

Step 3 Choose a layout from the pop-up display that corresponds to the number and arrangement of panes required for the view.

The selected pane layout appears in the window above the pop-up.

Step 4 Choose a video source for each pane in the layout:

a. Click a video pane to select it. The pane is shown with a green border.

b. Choose a video source from either the **Camera Feeds** or **Video Archives** lists on the left.

Step 5 Enter the view name in the pop-up display.

Step 6 Click the **Save View** button.

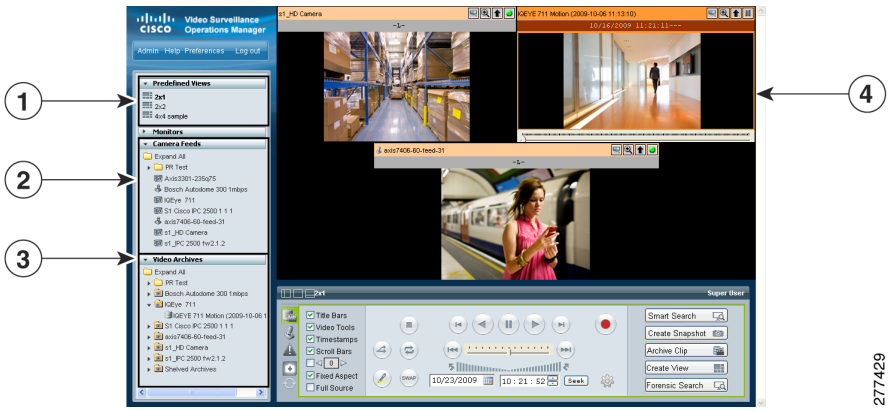
The name appears in the **Predefined Views** list.

Note Only an administrator can delete views. See the "Managing Predefined Views" section on page 5-24.

Viewing Live and Archived Video

The sources for live and archived video are listed under **Camera Feeds** and **Video Archives** in the side menu, as shown in Figure 8-5. **Camera Feeds** lists cameras individually or organized in groups (represented by folders). Video archives are organized according to the corresponding camera feed.

Figure 8-5 Choosing Video Feeds or Archives



1	Predefined Views	**3**	Video Archives
2	Camera Feeds	**4**	Video panes

To view live or archived video, click a video pane to highlight it, expand the video feed or archive folders to see the cameras or archives included in that group, and then click the feed or archive. The video plays in the selected pane.

This section includes the following information:

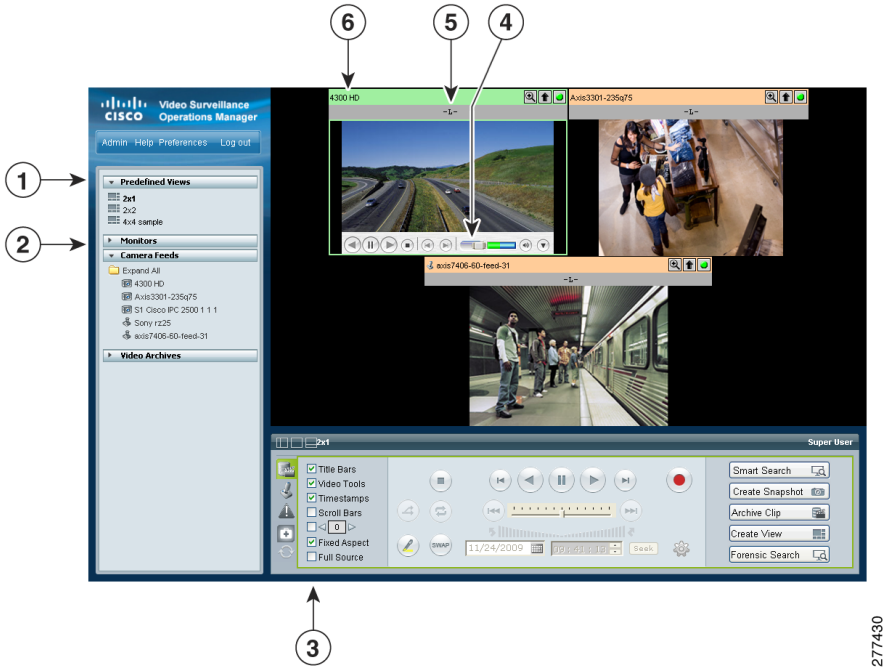
- Viewing Live Video, page 8-8
- Understanding Video Archives, page 8-10
- Viewing Archived Video, page 8-12
- Sending Video to a Monitor or Viewing Video from a Monitor, page 8-13
- Synchronizing the Playback Between Multiple Video Panes, page 8-14
- Switching Between an Archive and Live Video, page 8-15
- Creating an Archive Clip, page 8-16
- Recording Live Video, page 8-18
- Creating a Snapshot, page 8-19

Viewing Live Video

Select a video pane and then click a Camera Feed to display live video, as shown in Figure 8-6. You can also display additional information about the camera feed, or use DVR controls to stop and rewind live video.

Note To enable the DVR controls for viewing live video, enable the Use VMR and USE DVR options in the administrator Settings panel. For instructions, see the "Configuring System Settings" section on page 6-18.

Figure 8-6 Viewing Live Video Feeds



1	Predefined Views	**4**	DVR controls
2	Camera Feeds	**5**	Timestamp (“L” for live video)
3	View check boxes	**6**	Title bar showing camera source

To view live video, follow these steps:

Procedure

Step 1 Start VSOM and display the Operator pages, as described in the “Accessing VSOM” section on page 1-4.

If you are already viewing the VSOM Administrator pages, click the **Ops** link near the top left of the VSOM window.

Step 2 Choose a predefined view (see the “Creating Predefined Views” section on page 8-6).

Step 3 Click a video pane to make it active. The active pane appears with a green border.

See the “Understanding Video Pane Border Colors” section on page 8-29 for more information.

Step 4 Expand the **Camera Feeds** to display a list of live camera feeds.

The camera type is represented by the following icons:

—Camera without PTZ controls

—Camera with PTZ controls

Step 5 Choose a camera.

The video from the camera appears in the selected pane.

Tip To control video playback, adjust the quality of a live video feed, or display information about the video, see the "Understanding the Toolbars" section on page 8-23.

Tip To record a video clip from a live feed, see the "Recording Live Video" section on page 8-18.

Note For information about configuring cameras and camera groups, see Chapter 3, "Managing Devices."

Understanding Video Archives

Video archives contain recorded video. Each archive is listed under **Video Archives** in the left side menu next to an archive icon , as shown in Figure 8-7.

Figure 8-7 Video Archives

1	Video Archives	**8**	Forensic Search button
2	Cameras and camera groups	**9**	Archive Clip button
3	Archived Video	**10**	Create Snapshot button
4	Archive clip	**11**	Record Now button
5	Loop Archive button	**12**	Scroll Bar for archive video
6	Swap Live & Archive button	**13**	Timestamp
7	Player Control/Settings	**14**	Camera feed

Video Archive Types and Icons

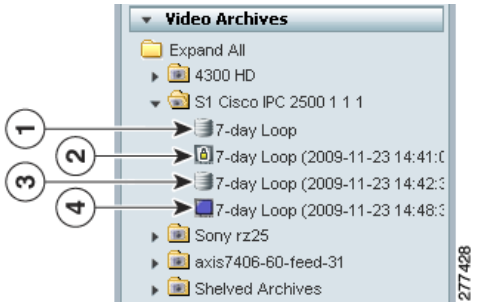
Archives are organized according to their corresponding camera feed and are configured by an administrator to record video in the following ways:

- As a one-time event. For example, from 6 p.m. to 8 p.m. (18:00 to 20:00) on a specific date.
- On a recurring schedule. For example, from 8 a.m to 10 a.m (08:00 to 10:00) every Tuesday.
- As a continuous loop. Loop archives include video from a set number of hours, days, weeks, months or years. Video that is older than the set time period is overwritten with new video. For example, a loop archive might include video from the past three hours. Video older than that three hours is automatically overwritten.

See the "Managing Archives" section on page 5-17 for information about configuring video archives.

In addition, you can create downloadable archive clips in a variety of file formats. These archive clips can contain the entire archive, or a subset of the archive video. Archive clips saved on the VSMS host server appear in the **Video Archives** list with one of the icons shown in Figure 8-8.

Figure 8-8 Video Archive Types and Icons



1.		Video Archive: an archive defined by an administrator that can be viewed using the Operator pages. For example: 7-day Loop. The recording type can include "motion" if the video is based on a motion event, or "Record Now" if the video is created using the Record Now feature.
2.		BWX Secure Video Clip. When an archive clip is saved in BWX format, it is displayed with a secure icon and the clip date and time range. For example: 7-day Loop (2009-11-23 14:41:00 2009-11-23 14:42:00)
3.		Streamable Archive Clip. When an archive clip is saved as `Streamable`, the clip name includes the date and time range for the included video. For example: 7-day Loop (2009-11-23 14:41:00 2009-11-23 14:42:00)
4.		BWM Archive Clip. When an archive clip is saved in BWM format, it is displayed with a monitor icon and the clip date and time range. For example: 7-day Loop (2009-11-23 14:41:00 2009-11-23 14:42:00)

Tip See the "Creating an Archive Clip" section on page 8-16 for more information.

Viewing Archived Video

To view archived video, follow these steps:

Procedure

Step 1 Start VSOM and display the Operator pages, as described in the "Accessing VSOM" section on page 1-4.

If you are already viewing the VSOM Administrator pages, click the **Ops** link near the top left of the VSOM window.

Step 2 Select the video pane in which you want to view the video.

Step 3 Expand the **Video Archives** in the left side menu (see Figure 8-8).

The archive includes an entry for each camera that appears in the **Camera Feeds** list.

Step 4 Expand the archive folder to display the available archives for that camera.

See Figure 8-8 for a description of the archive types and icons.

Step 5 Click the name of the archived video clip that you want to view.

- If the archive is a streamable archive with the  icon, the video plays in the selected pane. To control the video playback, see the "Switching Between an Archive and Live Video" section on page 8-15.

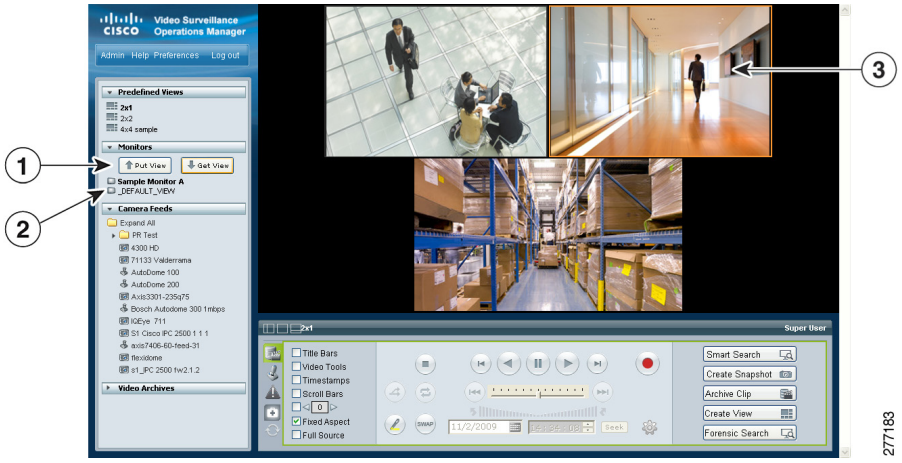
Tip To play the video as a continuous loop, click the **Loop Archive** button . The video loops to the beginning when the end is reached.

- If the archive was saved in a downloadable format (BWX or BMX), you are prompted to save the file. See the "Creating an Archive Clip" section on page 8-16 for more information.

Sending Video to a Monitor or Viewing Video from a Monitor

The Monitors feature allows you to transfer video that is playing in a video pane to a physical monitor, or to view the video from a physical monitor in a selected pane. Figure 8-9 illustrates this feature.

Figure 8-9 Monitors



1	**Get View** and **Put View** buttons
2	Available monitors. The selected monitor is shown in bold type.
3	Selected video pane.

Before You Begin

Physical monitors must be installed and configured on the system, as described in the "Managing Monitors" section on page 3-31. After they are configured, the physical monitors are listed under **Monitors**.

Note VSM supports the same number of video streams whether you are using one monitor or dual monitors.

Procedure

To send video to a monitor or view video from a monitor, follow these steps:

Step 1 Start VSOM and display the Operator pages, as described in the "Accessing VSOM" section on page 1-4.

If you are already viewing the VSOM Administrator pages, click the **Ops** link near the top left of the VSOM window.

Step 2 Choose a video pane.

Step 3 Expand the **Monitors** list (see Figure 8-9).

Step 4 Click the name of the monitor to which to send video or from which to view video.

The monitor name changes to bold type.

Step 5 Take either of these actions:

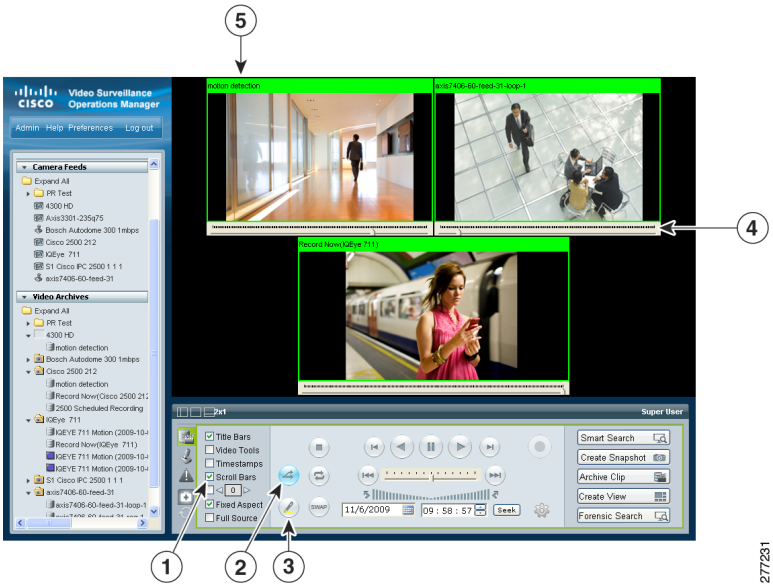
- Click the **Put View** button at the top of the monitor list to send the video from the selected pane in the Operator page to the selected monitor.

- Click the **Get View** button to display the video from a the selected monitor in the selected Operator page pane.

Synchronizing the Playback Between Multiple Video Panes

You can play multiple video panes that are synchronized to the same time by choosing the panes and clicking the **Synchronize** button , as shown in Figure 8-10.

Figure 8-10 Synchronizing Video Playback



1	Scroll bar check box	**4**	Synchronized video panes
2	Synchronize button	**5**	Master video pane
3	Highlight All button		

The following notes apply to synchronized video:

- Synchronization is supported for archived video only.
- Synchronization 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
- Synchronization is not supported when archives are stored on multiple VSMS hosts.
- 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 in the master pane, the other synchronized panes pause until the seek completes, then continue to display video that is synchronized with the new master pane time. See the "Using the Playback Controls" section on page 8-27 for information about the seek feature.

To play multiple video panes synchronized to the same time, follow these steps:

Procedure

Step 1 Control-click to select multiple video panes for synchronization.

The selected panes are displayed with a light green border.

Tip Click the **Highlight All** button to highlight all panes in the view.

Step 2 Click the **Synchronize** button .

The video playback is synchronized to the upper-leftmost pane, called the *master* pane. All synchronized panes appear with a bright green border and the synchronize button turns bright blue (see Figure 8-10).

If the time for a video pane does not overlap with the master pane, the pane is excluded from synchronization and displayed with an border color other than green.

Step 3 (Optional) To select a specific synchronization time, move the scroll bar indicator for the master pane:

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.

a. Check the scroll bar check box to turn the scroll bars on (see Figure 8-10).

b. Click and drag the scroll bar in a pane to choose a playback time.

Switching Between an Archive and Live Video

If an archive loop is configured for a camera, you can quickly switch between the archive and live video for that camera. If no archive loop is configured for that camera, then the most recent non-loop archive is displayed.

To switch between archive and live video, follow these steps:

Procedure

Step 1 Start the archive playback as described in the "Viewing Live and Archived Video" section on page 8-7.

Step 2 Use the **Swap** button to toggle the video display between the archive video and live video for that camera.

The status of the video is displayed in the timestamp. To turn on the timestamp bar above a video pane, choose the pane and check the **Timestamp** check box. See the "Understanding View Option Check Boxes" section on page 8-30 for more information.

Archive video displays the date and time in the timestamp bar. Live video displays an "L".

Creating an Archive Clip

An Archive Clip is a video file created from an existing archive that contain the entire archive, or a subset of the archive video. You can save downloadable archive clips in a variety of file formats, or save them on the VSMS host server in the **Video Archives** list. See the "Understanding Video Archives" section on page 8-10 for more information.

Tip To create a clip archive from live video, see the "Recording Live Video" section on page 8-18. To create a video clip from an event, see the "Creating Event Video Clips" section on page 8-40.

To create, save, and view an archive clip, follow these steps:

Procedure

Step 1 Choose an archive as described in the "Viewing Live and Archived Video" section on page 8-7.

Step 2 Click the **Archive Clip** button 

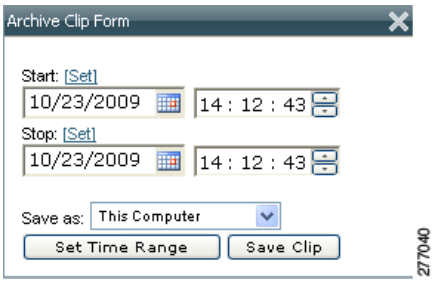
in the lower right corner of the screen.

Step 3 In the **Archive Clip Form** pop-up window, take these actions:

a. Click the **Set Time Range** button. This button enters the archive start date and time and end date and time in the time fields.

a. Enter the start date and time and the end date and time for the clip, as shown in Figure 8-11.

Figure 8-11 Start and End Date and Time for a Clip



Tip You can move the scroll bar to the desired location in the video, and then click **Set** to enter the selected date and time.

Click **Set Time Range** to automatically enter the full range of the archive.

When the archive includes video from both daylight savings (DS) and standard time (ST), the Archive Clip Form includes DS and ST buttons in front of the Start and Stop time.

Step 4 From the **Save as** drop-down list, choose a file format option for the clip:

- Server-side—Choose **BWM**, **BWX**, or **Streamable** to save the clip in a file format that can be stored on the VSMS host server.

  See the "Video Archive Types and Icons" section on page 8-11 for more information.

- This Computer—Choose the **CVA**, **AVI/MP2**, or **WMV** file formats under **This Computer** to save the file to a local or networked computer.

Step 5 Click the **Save Clip** button and take one of these actions:

- If you chose a file format for **This Computer**, choose a location for the file on a local or network computer.
- If you chose the **WMV** format, select a profile for the clip and then enter a file name.
- If you chose the **BWX** format you are prompted to enter an alphanumeric password from 6 to 64 characters. For example: `Ci0sCO3`. This password must be entered to view the clip.

Step 6 Wait for the clip to be saved.

While the clip is being saved, the video pane border turns yellow and the title bar displays a caution icon  .

Step 7 Click the **X** icon to close the **Archive Clip Form** pop-up window.

Step 8 To view the clip, do one of the following:

Server-side Clips

a. Click the **Refresh** icon  to update the **Video Archives** list.

The new archive clip appears in the **Video Archives** list under the source clip. Table 8-1 shows how to identify the clip type.

Table 8-1 Identifying Archive Clips

	BWX Secure Video Clip. When an archive clip is saved in BWX format, it is displayed with a secure icon and the clip date and time range. For example:  `7-day Loop (2009-11-23 14:41:00 2009-11-23 14:42:00)`
	BWM Archive Clip. When an archive clip is saved in BWM format, it is displayed with a monitor icon and the clip date and time range. For example:  `7-day Loop (2009-11-23 14:41:00 2009-11-23 14:42:00)`
	Streamable Archive Clip. When an archive clip is saved as `Streamable`, the clip name includes the date and time range for the included video. For example: `7-day Loop (2009-11-23 14:41:00 2009-11-23 14:42:00)`

b. Click the name of the clip and choose a location for the file on a local or network computer.

Note Streamable clips are viewed in VSOM and are not downloaded. Click the streamable archive name to begin playback in VSOM.

c. Locate the video clip on your local or network computer.

d. Double-click the file to view the clip using the Cisco ReView Player video client.

Note If the clip is in BWX secure format, enter the password for the clip when choosing to view it.

This Computer

a. Locate the video clip on your local or network computer.

b. Double-click the file to view the clip using the Cisco ReView Player video client.

Note

- To install the video client, go to the **Software & Downloads** panel in the Administrator pages click the **VSOM Video Client** link, and follow the installation instructions. See the "Managing Software and Downloads" section on page 4-1 for more information.
- CVA files with mixed media types may briefly display *No data for current time period* until each video stream is fully synchronized. Playback continues normally when synchronization is complete.
- Only play forward is supported when playing CVA clips in the Cisco ReView Player video client.; other trick play functions are not supported.

Recording Live Video

To record the live video being played in the video panes, click the **Record Now** button. Video is recorded for all currently displayed live video panes. The video panes do not need to be selected.

The button turns blue while recording is in progress. Recording stops automatically after the specified recording length.

Recorded video appears in the video archive under the camera feed folder. The name of the archive is:

`Record_Now camera feed name`

See the "Viewing Archived Video" section on page 8-12 for more information.

Note

- Only live video currently being viewed is recorded. Archive video and blank panes are not recorded.
- The **Record Now** button is active only for live video feeds. To create a clip from archived video, see the "Creating an Archive Clip" section on page 8-16.
- The **Record Now** button is enabled by default. To change the default recording time, or to disable the feature, go to the administrator Settings panel and chose the time from the **Max Record Now Length** drop-down list. (For related information about the Settings pane, see the "Configuring System Settings" section on page 6-18.)
- You can also enable events for Record Now. See the "Using the Events Panel" section on page 6-3.

Defining the Recording Length

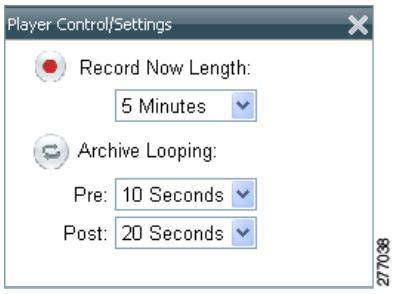
To change the default recording time, go to the administrator Settings panel and chose the time from the **Max Record Now Length** drop-down list. (For related information about the Settings pane, see the "Configuring System Settings" section on page 6-18.)

To specify the time length for the current recording session, follow these steps:

Step 1 Click the **Player Control/Settings** button before you click the **Record Now** button.

Step 2 In the Player Control/Settings pop-up window, choose the desired record length from the Record Now Length drop-down list, as shown in Figure 8-12.

Figure 8-12 Choosing a Record Length



Step 3 Click the **X** icon to close the window.

Creating a Snapshot

A snapshot is a still image that you can capture from live or archived video. You can save a snapshot if a folder that you specify and in a variety of formats.

To create a snapshot, follow these steps:

Procedure

Step 1 Choose the camera feed or video archive as described in the "Viewing Live and Archived Video" section on page 8-7.

Step 2 Click the **Create Snapshot** Create Snapshot button in the lower right corner of the screen (see Figure 8-7 on page 8-10).

Step 3 In the **Save As** window, enter a file name, choose the preferred file type, and choose a location for the file.

Step 4 Click the **Save** button.

Searching a Thumbnail Summary of Video Archives

Use the **Forensic Search** feature to create a thumbnail summary of a video archive. Use the thumbnails to locate specific scenes or events in the archive. Once located, you can play the video in the Operator window, or save the video clip to a local or network drive.

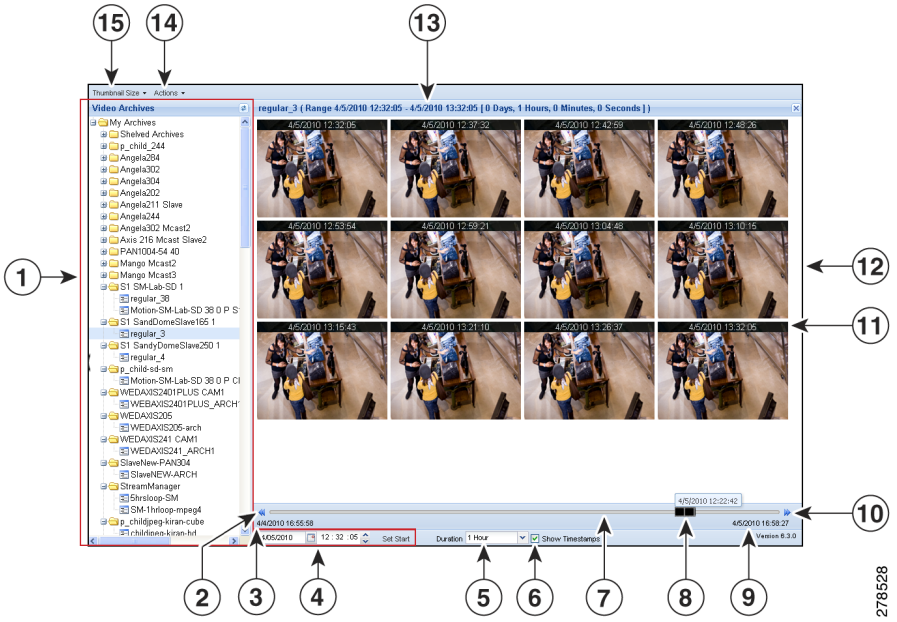
Note

- Any archive except BWX secure video clips and BWM archive clips can be searched. See the "Video Archive Types and Icons" section on page 8-11 for more information.
- The Forensic Search feature can only be used when the Operator page is open. If you close the Operator page, or click on the Admin or Preferences links, the Forensic Search window closes.

Forensic Search Window

Click the Forensic Search button Forensic Search on the Operator page to open the Forensic Search window (Figure 8-13), which includes a thumbnail summary and available controls. This button is available only if enabled by your administrator

Figure 8-13 Forensic Search Window



1	Video Archives. To create a thumbnail summary of an archive, double-click the archive name, or drag and drop the archive name to the viewing panel. Archives are displayed in alphabetical order.
2	Skip back by the **Duration** time increment. This icon is disabled if the entire archive is selected.
3	Start date and time for the entire video archive.
4	The start date and time for the first thumbnail (in the top left corner of the window pane).
5	Thumbnail **Duration** setting. Choose the time span for the video thumbnails that display. 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 other thumbnails that appear 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.
6	**Show Timestamp** check box. Check this check box to show the date and time displayed at the top of each thumbnail.

7	Timeline representing the entire video archive.
8	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.
9	End date and time for the entire video archive.
10	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	Title bar. Displays a summary of the displayed thumbnails in the following format: *archive_title* (Range *beginning-time - ending-time*) [*Duration*])
14	**Actions** menu. See Step 5 for more information.
15	**Thumbnail Size** menu. Enlarges or reduces the size of each thumbnail. Larger sizes display less thumbnails.

Using Forensic Search

To open and use the Forensic Search feature, do the following:

Procedure

Step 1 Verify that **Use Forensic Search** is enabled in the Administrator Settings pages.

The Forensic Search button 

appears on the Operator page only if the **Use Forensic Search** option is enabled in the administrator Settings panel. For instructions, see the "Configuring System Settings" section on page 6-18.

Step 2 Click the Forensic Search button 

on the Operator page to open the Forensic Search window, as shown in Figure 8-13.

Archives are displayed in alphabetical order.

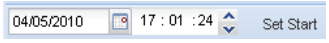
Step 3 To display a thumbnail summary for a video archive, double-click the archive name from the Video Archives list, or use your mouse to drag the archive name onto the thumbnail window pane.

Note the following when choosing a video archive:

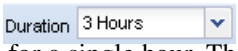
- Video archives use the same organization as archives shown in the Operator page. See the "Understanding Video Archives" section on page 8-10 for more information.
- Click the refresh icon  to update the archive list to make sure that it's current.

Step 4 Use the controls described in Figure 8-13 to refine the forensic search.

For example:

- Choose the start date and time for the first thumbnail in the display and click **Set Start** 

. The selected start thumbnail is displayed in the top left corner.

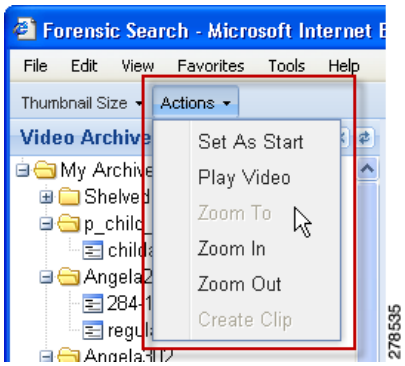
- Choose the **Duration**  for the thumbnail display. For example, choose **1 Hour** to display thumbnails for a single hour. The default is **Entire Archive**.
- Click the skip icons to skip back  or forward  in the video archive by the time that is defined in the Duration drop-down menu. For example, if the Duration is `1 hour`, click the skip buttons to skip forward or back by 1 hour.
- Click and drag the slider  to a new start time. The slider date and time appears when the slider is selected. Release the mouse button to refresh the thumbnail display with the time displayed above the slider.

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

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

Step 5 (Optional) Further refine your search by choosing one or more thumbnails and choosing one of the following options in the **Actions** menu, as shown in Figure 8-14.

Figure 8-14 Actions Menu



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

- **Set As Start**—Set a thumbnail as the first thumbnail in the range.
- **Play Video**—See Step 6.
- **Zoom To**—Set the beginning and ending thumbnail for the display. Shift-click or Ctrl-click to select multiple thumbnails. 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.

- **Create Clip**—See Step 7.

Step 6 (Optional) To play a video thumbnail, select the thumbnail and choose **Play Video** from the **Actions** menu.

- Video is played in the Operator page from the start timestamp of the thumbnail. If the start timestamp is not available, the next available frame is displayed.
- Any video being played in the Operator page is replaced by the selected forensic search video.

Step 7 (Optional) Save a video clip to a local or network drive.

- The clip is saved in CVA format and includes the video from the range represented by the thumbnails.
- The start time of the clip is the start timestamp of the first thumbnail selected. The end time is the end timestamp of the last thumbnail selected.

a. Shift-click or Ctrl-click to select a range of thumbnails.

Note You must select at least two thumbnails to save a video clip.

b. Choose **Create Clip** from the **Actions** menu.

Tip You can also right-click one of the selected thumbnails and choose **Create Clip**.

c. Choose the location to save the file.

d. Click **Save** to save the file.

e. To view the clip, double-click the file to view it using the Cisco ReView Player video client.

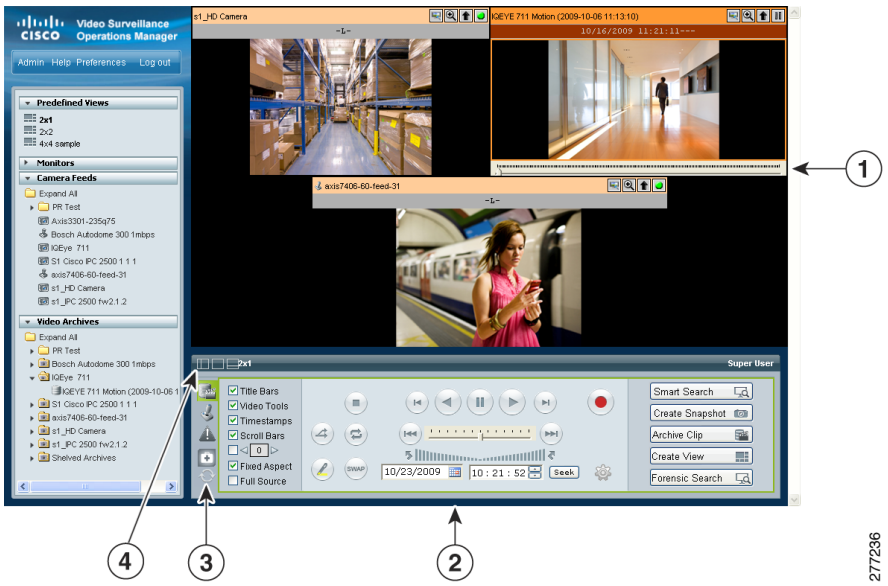
Tip

- To install the Cisco ReView Player video client, go to the Software & Downloads panel in the Administrator pages. Click the **VSOM Video Client** link and follow the installation instructions. See the "Managing Software and Downloads" section on page 4-1 for more information.
- CVA files with mixed media types may briefly display *No data for current time period* until each video stream is fully synchronized. Playback continues normally when synchronization is complete.

Understanding the Toolbars

Toolbars appear below the video panes and provide video playback controls, video information, PTZ functions, and access to video events. Figure 8-15 shows the toolbar for Feed/Archive Controls.

Figure 8-15 Toolbars



1	Video panes	**3**	Toolbar tabs
2	Toolbars	**4**	Collapse/Expand Toolbar icons

Click a tab to display the features and function for the following:

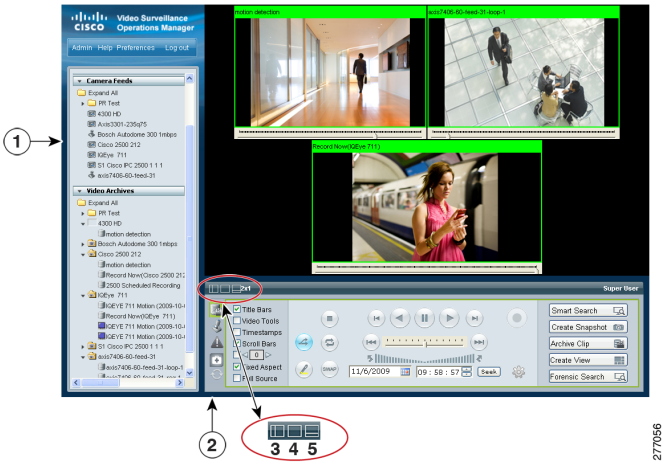
- **Feed/Archive Controls**—Default, see the "Using the Playback Controls" section on page 8-25.
- **PTZ Camera Controls**—See the "Using the Camera PTZ Controls" section on page 8-34.
- **Event** controls—See the "Viewing Video Events" section on page 8-36.
- **Health Dashboard**—See the "Using the Health Dashboard" section on page 6-23.

Note The **Refresh** icon refreshes the list of predefined views, monitors, camera feeds and video archives in the side menu. The icon appears highlighted when any of the lists have changed. For example, it appears highlighted when you modify a view or save a video clip.

Hiding or Showing the Toolbar and Side Menu

Click the Collapse/Expand icons to hide or show the toolbar and the left side menu (see Figure 8-16). Hiding the side menu or toolbar enlarges the video in the VSOM window.

Figure 8-16 Hide/Show Toolbar and Side Menu



1	Sidebar. The sidebar includes the Predefined Views, the Monitors, Video Feeds and Video Archives drawers. See the "Understanding the Operator Window" section on page 8-1 for more information.
2	Toolbar. Includes controls for video playback, PTZ, and Events. See the "Understanding the Toolbars" section on page 8-23 for more information.
3	Collapse/Expand Sidebar. Hides or shows the left side menu.
4	Collapse/Expand Both Sidebar and Toolbar. Hides or shows both the left side menu and the bottom toolbar. Use this button to expand the video to the full window.
5	Collapse/Expand Toolbar. Hides or shows the bottom toolbar.

Using the Playback Controls

The Feed/Archive Controls toolbar includes the video playback controls, options to display information and functions in each video pane, and other features. Figure 8-17 on page 8-26 describes the toolbar features in detail.

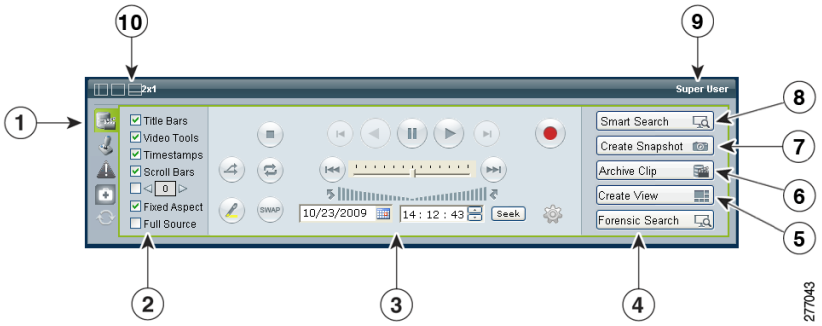
Tip

- The Feed/Archive Controls toolbar is displayed by default, or when you click the **Display Feed/Archive Controls** tab  . See the "Understanding the Toolbars" section on page 8-23 for more information.
- If no toolbar is displayed, click the Collapse/Expand Toolbar icon  as shown in Figure 8-16 on page 8-25.
- The controls that appear in the toolbar depend on your VSOM user rights.
- Controls that appear dimmed are disabled for the selected video pane.

This section includes the following information:

- Adjusting Image Quality for Live Video, page 8-31
- Using Digital Zoom, page 8-33

Figure 8-17 Feed/Archive Control Toolbar



1	Display feed/archive controls. Choose this tab to display the video controls.
2	View option checkboxes. Check or uncheck the check boxes to show or hide the information and controls that each video pane displays. See the "Understanding View Option Check Boxes" section on page 8-30.
3	Playback controls. Choose an option to control video playback. See the "Using the Playback Controls" section on page 8-27 for descriptions of each function.
4	Forensic Search. View a thumbnail summary of a video archive to locate specific events. You can then play or save the video clip. See the "Searching a Thumbnail Summary of Video Archives" section on page 8-19.
5	Create View. Creates a new camera pane layout. See the "Using Predefined Views" section on page 8-5.
6	Archive Clip. Creates a video clip from a portion of an existing archived video clip. See the "Creating an Archive Clip" section on page 8-16.
7	Create Snapshot. Create a still image from live or archived video. See the "Creating a Snapshot" section on page 8-19.
8	Smart Search. Search archived video to locate where motion is detected. See Chapter 9, "Using Smart Search."
9	User. Displays the current operator username.
10	Collapse/expand icons. See the "Hiding or Showing the Toolbar and Side Menu" section on page 8-24.

Using the Playback Controls

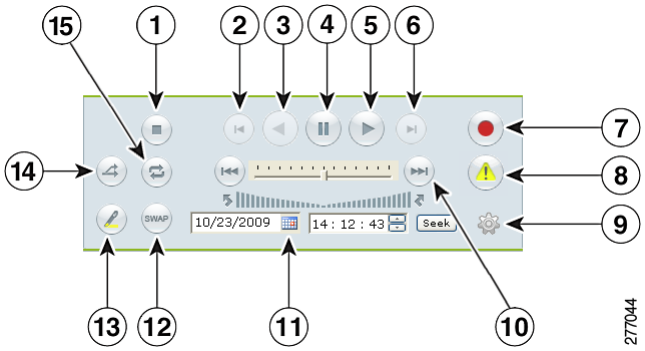
To control video playback, click anywhere in a video pane to make it active and choose the settings and actions that Figure 8-18 shows.

Many of the controls described in this section are available only for video archives. See the "Using DVR Controls for Live Video" section on page 8-28 for information about additional controls.

Note

- The active pane is shown with a green border, and the controls and actions performed in this section apply to the active pane. See the "Understanding Video Pane Border Colors" section on page 8-29 for more information.
- If the controls are not shown, click the **Display Feed/Archive** tab  . See the "Understanding the Toolbars" section on page 8-23.
- If no toolbar is displayed, click the **Collapse/Expand Toolbar** icon  as shown in Figure 8-16 on page 8-25.
- Controls that appear dimmed are disabled for the selected video pane.

Figure 8-18 Playback Controls



1	Stop button. Stop playing the video archive.
2	Step Reverse button. Play the video archive in reverse one frame at a time.
3	Play Reverse button. Play the video archive in reverse. **Note** Reverse playback is available only for archived video.
4	Pause button. Pause the archive video playback. To resume, click play. When an archive is paused, you can use the **Step Reverse** and **Step Forward** buttons to play the video archive backward or forward one frame at a time, respectively.
5	Play Forward button. Play the video archive.
6	Step Forward button. Play the video archive forward one frame at a time.
7	Record Now button. Records live video from a camera feed for the number of seconds or minutes that are specified in the Player Control/Settings pop-up window. See the "Recording Live Video" section on page 8-18 for more information

8	Bookmark Events button. A bookmark allows you to dynamically create a predefined view from the video that you are playing and create an event history record for that event and time. See the "Adding an Event" section on page 6-4.
9	Player Control/Settings button. Opens a pop-up window, which provides these options for live video recording and archive loop playback: • Record Now Length—Length of time to record live video. See the "Recording Live Video" section on page 8-18. • Pre—Length of time before an event occurred that an archive loop starts playing when you choose to play the video as a loop. • Post—Length of time after an event occurred that an archive loop continues to play before repeating when you choose to play the video as a loop. Combined, the Pre and Post values specify the total length of the loop.
10	Play speed and jump buttons Move the slider to the left to play the video archive slower or move it to the right to play it faster. You can choose from six speeds in each direction. Click  to jump to the beginning of the video archive. Click  to jump to the end of the video archive.
11	Date seek controls. To jump to a specific date and time in the video archive, enter the parameters and click the **Seek** button. You also can click the bars to jump forward or back in a currently displayed archive. Click a bar to the left to jump backward and click a bar to the right to jump forward. Click closer to the middle of the set of bars for a smaller jump. The size of a bar indicated the relative jump time. The maximum jump is 2.5 minutes per click.
12	Swap button. If an archive loop is configured for a camera, click this button to switch between archive and live video from that camera. See the "Switching Between an Archive and Live Video" section on page 8-15.
13	Highlight All button. Choose all video panes in the video panel.
14	Synchronize button. Synchronize time between panes. Choose multiple panes and click **Synchronize** to synchronize the playback time to the upper-leftmost pane. See the "Synchronizing the Playback Between Multiple Video Panes" section on page 8-14.
15	Loop Archive button. Play a video archive in a continuous loop (the video loops to the beginning when the end is reached).

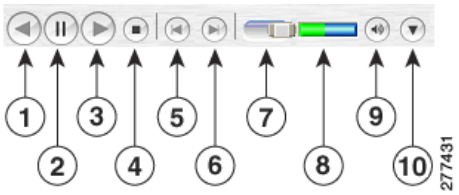
Using DVR Controls for Live Video

Figure 8-19 shows the DVR controls that are available in the top left video pane for live camera feeds. These controls are displayed only if the video pane displays a camera feed and the DVR controls are enabled.

To enable the DVR controls, enable the Use VMR and USE DVR options in the administrator Settings panel. For instructions, see the "Configuring System Settings" section on page 6-18.

For information about viewing camera feeds, see the "Viewing Live Video" section on page 8-8.

Figure 8-19 DVR Controls for Live Video



1	Play Reverse.
2	Pause. When video is paused, this button changes to an "L" (L). Click the (L) button to resume playing live video.
3	Play Forward.
4	Stop.
5	Step Back one frame
6	Step Forward one frame
7	Timeline. The horizontal bar represents the overall length of the recording. Slide the bar to jump to a location in the available video.
8	Video Cache representing the entire length of the video. The green bar shows the played video, and the blue color represents the unplayed video.
9	Audio On or Off. Click to mute the audio. Click to turn sound back on.
10	Show/Hide Image Quality Adjustments. See the "Adjusting Image Quality for Live Video" section on page 8-31.

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 green or orange. The controls and actions performed apply to the active pane.

Table 8-2 describes the meaning of each color.

Table 8-2 Video Pane Border Colors

Color	Description
Gray	The pane is not highlighted. All panes have a gray border by default.
Green	The video playback time is synchronized with one or more other panes. When synchronizing playback between multiple panes, the border color for all panes is green. See the "Synchronizing the Playback Between Multiple Video Panes" section on page 8-14.
Light green	The active pane for live or archive video. The controls and actions performed apply to the active pane. Click anywhere in a video pane to make it active.

Table 8-2 Video Pane Border Colors (continued)

Color	Description
Light orange	The pane is fixed (not included in a video rotation). See the "Understanding Rotating Views" section on page 8-6.
Orange	The pane is fixed (not included in a video rotation) and selected as the active pane. The controls and actions performed apply to the active pane.
Yellow	The pane is performing an action or has an alert. For example, when you create an archive clip, the pane border turns yellow while the clip is being saved.

Understanding View Option Check Boxes

Check or uncheck the view option check boxes (Figure 8-20) to show or hide the information and controls that appears on each video frame.

Figure 8-20 Image Quality Adjustments for Live Video

1	Check boxes. To show the following information and controls, check the appropriate check box: • Title Bars, Video Tools, Timestamps, and Scroll bars—See the following rows for descriptions. • Dwell time indicator—Overrides the dwell time for rotating video (in seconds). See the "Understanding Rotating Views" section on page 8-6. • Fixed Aspect—The view appears based on the monitor configuration. • Full Source: Display the selected video in full size (as defined by the video source).
2	Title bars. Displays the name of the camera feed or archive in the title bar of each video pane.
3	Video tools Displays shortcut tools on the right side of the title bar (you must also check the title bar check box to see these options): • Launch Smart Search — See Chapter 9, "Using Smart Search" for more information. • Toggle Full Screen on this Source —Hides the other video panes and fills the window with the selected pane. • Upload View to Monitor —Displays the video image on a configured monitor. • Video Details —Displays information about the video stream.
4	Timestamps (archived video only). Displays the time and date that the video was recorded, in 24-hour format. The time is defined by the VSOM server, which may be different from the time in the camera location. Live video streams display "L" instead of a timestamp.
5	Scroll bars (archived video only). Allow you to choose a specific time in the video archive. Click and drag the scroll bar selector. The time appears above the selector. Release the mouse button at the desired time. This control is not available for live video feeds.

Adjusting Image Quality for Live Video

Image controls adjust the appearance of live video images (see Figure 8-21). Settings that you make remain in effect until you log out of VSOM. Adjusting these control do not make changes to a camera.

Note To use this feature, the camera that provides the video must support the controls, and you must enable the **Use DVR** option on the Settings page in the Administrator pages. See the "Configuring System Settings" section on page 6-18.

To adjust image quality, follow these steps:

Procedure

Step 1 Start VSOM and display the Operator pages, as described in the "Accessing VSOM" section on page 1-4.

If you are already viewing the VSOM Administrator pages, click the **Ops** link near the top left of the VSOM window.

Step 2 Choose the live camera feed that you want to view.

See the "Viewing Live and Archived Video" section on page 8-7.

Step 3 Click the down arrow on the bottom right of the video panel, as shown in Figure 8-21.

A small window opens to show the image controls.

Note This arrow and the image quality control are available only if the **Use DVR** option is enabled in the administrator Settings page.

Figure 8-21 Image Quality Adjustments for Live Video

1	Live Camera Feed
2	Image Adjustment Icon
3	Image Adjustment Settings

Step 4 Use this slider to adjust the image settings:

- **Hue**—Slide the bar to the right to increase hue or slide it to the left to decrease hue. Hue refers to the relative strength of cools in an image.
- **Saturation**—Slide the bar to the right to increase saturation or slide it to the left to decrease saturation. High saturation provides a vivid, intense color for a video image. With less saturation, the video image appears more muted and gray.
- **Brightness**—Slide the bar to the right to increase the brightness or slide it to the left decrease the brightness. For example, if a camera is facing a bright light and the video appears too dark, you can increase the brightness.
- **Contrast**—Slide the bar to the right to increase contrast or slide it to the left to decrease contrast.
- **Transparency**—Slide the bar to allow the background to display through so that the image appears to have no visible border around it. This slider also adjusts the transparency setting for on-screen controls, such as the digital zoom controls.
- **RESET**—Click to restore all image quality adjustment settings to their default values.

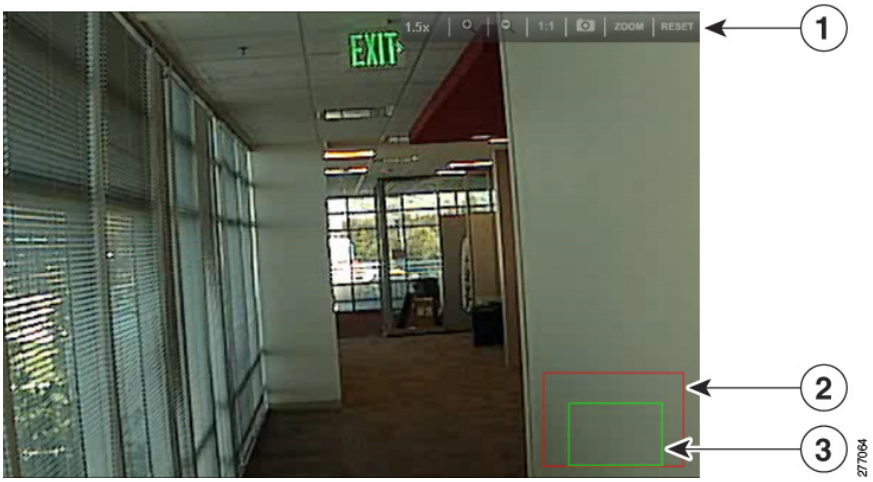
Step 5 Click the image adjustment icon again to close the settings window and save your changes.

Using Digital Zoom

Use digital zoom to digitally zoom and pan in the video window. The digital zoom controls are displayed as transparent icons in the upper right corner of the video display.

Digital zooming is a pixel-based zoom that affects the video image but does not adjust the camera lens. PTZ controls are disabled when using digital zoom.

Figure 8-22 Digital Zoom



1	Digital Zoom Controls. See Table 8-3 on page 8-34 for descriptions.
2	Field of View showing the entire camera view. This box is green when the entire field of view for the camera is shown (also referred to as 1:1 view).
3	Current display. This box indicates the portion of the video image that is currently displayed. Click and drag the box to pan within the scene. Click the zoom in and out icons to narrow or enlarge the view.

To use the video zoom feature, follow these steps:

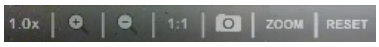
Procedure

Step 1 Verify that **Use VMR** is enabled on the Settings page in the Administrator pages.

To use digital zoom, you must enable the VMR mode as described in "Configuring System Settings" section on page 6-18.

Step 2 Choose a camera feed or archive.

The digital zoom controls appear as transparent icons in the upper right of the video display.



Note To make the control more or less transparent, use the Transparency setting as described in the "Adjusting Image Quality for Live Video" section on page 8-31.

Step 3 Click **Zoom** ZOOM to enable digital zoom mode.

A green box appears in the lower right to represent the entire image.

Step 4 Click **Zoom In** .

The box turns red to represent the original view. A smaller green box represents the zoom view. Drag the green box within the red box to pan within the image.

Step 5 Use other controls that Table 8-3 describes, as needed.

To restore the original zoom level, click **1:1**.

Table 8-3 Digital Zoom Controls

Item	Description
1.0x Magnification Level	Displays the current level of magnification.
Zoom In	Increases magnification. This control is not available when the video is paused.
1:1 Zoom Out	Reduces magnification. This control is not available when the video is paused.
1:1	Restores the full camera view.
Snapshot	Creates and saves a snapshot. The zoom toolbar is unavailable during this operation. See the "Creating a Snapshot" section on page 8-19.
ZOOM Zoom	Enables digital zoom mode.
RESET Reset	Restores the default view and exits digital zoom mode.

Using the Camera PTZ Controls

Pan-tilt-zoom (PTZ) cameras are controlled using the **PTZ Controls** toolbar. Cameras can be panned left and right, tilted up and down, or zoomed in and out. Controls are operated by using the PTZ Console or a PTZ joystick that is connected to the client workstation.

Note To use the PTZ controls, the PTZ camera must be configured. (For instructions, see Chapter 3, "Managing Devices.")

To control the PTZ functions for a PTZ camera, follow these steps:

Procedure

Step 1 Start VSOM and display the Operator pages, as described in the "Accessing VSOM" section on page 1-4.

If you are already viewing the VSOM Administrator pages, click the **Ops** link near the top left of the VSOM window.

Step 2 Click the **Display PTZ Controls** tab  to display the PTZ controls shown in Figure 8-23.

Step 3 Choose a PTZ camera from the PTZ Sources list.

Only PTZ-capable cameras are displayed.

Tip You can also choose a camera from the **Camera Feeds** in the left side menu.

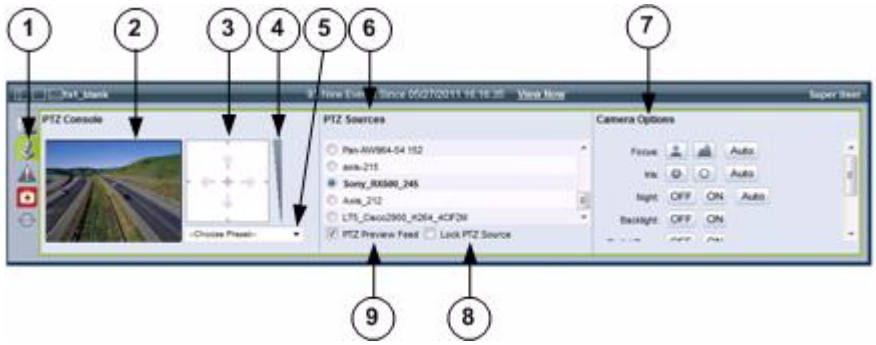
Step 4 Use the controls that Figure 8-23 describes to manipulate the camera.

For example:

- To pan or tilt the camera, drag your cursor around the center of the crosshair box.
- To zoom the camera, use the vertical scale to the right of the crosshairs.

Tip Left-click and drag to use these controls. Do not let the mouse pointer leave the control. If it does, click the control once to recover control.

Figure 8-23 PTZ Control Toolbar



1	Display PTZ controls. Click the PTZ Controls icon to display the PTZ toolbar. If the icon does not appear, see the "Hiding or Showing the Toolbar and Side Menu" section on page 8-24.
2	Display pane. Displays video from the selected PTZ source.
3	Crosshair box. Click and drag your cursor around the center of the box to pan or tilt the camera.
4	Zoom. To zoom the camera, click and drag your cursor on the vertical scale to the right of the crosshairs: drag up to zoom in and down to zoom out.
5	Presets. Choose a preset camera position from the drop-down list to move the camera PTZ camera to that position. Preset positions are configured by an administrator. See Chapter 3, "Managing Devices."

6	PTZ sources. Choose a camera to control. The video feed from the camera appears in the Display pane. **Note** If Lock PTZ Source is selected, the video in the display pane changes, but the PTZ controls still operate the previously selected camera. This way, an operator can control a camera other than the one that is feeding the Display Pane.
7	Camera adjustments. Choose additional adjustments from the available buttons. Only options that the camera supports appear. These options may include: • Focus—Focus in or out. Click Auto to auto adjust the focus. • Iris—Adjust the iris to lighten or darken the image. Click Auto to auto adjust the iris to the optimal setting. • Night—Provides improved visibility in low light. Click On or Off to enable or disable the feature. Click Auto to adjust the camera to the optimal setting. • Backlight—Enable or disable backlighting. • Digital Zoom—Enable or disable digital zoom. • White Balance—Adjust the white balance to apply a warm (indoor) or cool (outdoor) filter. Click Auto to auto adjust the indoor/outdoor white balance.
8	Lock PTZ source. Choose **Lock PTZ Source** to view a video source in the Display Pane that comes from a camera other than the one that is providing video in the PTZ Preview Feed. The PTZ controls still affect the camera in the PTZ Preview Feed.
9	PTZ preview feed. Choose **PTZ Preview Feed** to display or hide the selected video source in the Display Pane.

Using a PTZ Joystick

The Cisco VSOM supports USB joysticks for controlling PTZ cameras.

- The USB joystick must be connected to the computer before launching Internet Explorer and logging in to VSOM.
- PTZ preset commands are mapped to joystick buttons, but not to mouse buttons.
- Presets are automatically mapped to each button in order. If the joystick has zoom controls, buttons 1 and 2 are mapped to zoom in and zoom out, and the other buttons are mapped to presets in order. The Windows Game Controller in the Toolbar shows the numbers of the buttons if they are not labeled on the USB joystick.

Viewing Video Events

Events are noteworthy occurrences that may include audible and visual alarms, switching monitor views, event bookmarking, and sending preset commands. When an event is triggered, it is listed in the Events inbox, which allows you to display information about the event and take action as needed.

Note Events are defined in the Administrator pages. For more information, see the "About Events" section on page 6-1.

From the Events inbox, you can take actions to respond to triggered events. To display these controls, click the **Event** toolbar tab  (see the "Understanding the Toolbars" section on page 8-23).

Note When a new event is triggered, a message appears for the new event in the message bar (see Figure 8-24).

This section includes these topics:

Viewing Events

Use the Event inbox to view motion, analytics, device trigger, and soft trigger events that occur in VSOM. Figure 8-24 describes the Event invox. Some of the options and buttons that this figure shows are not available when **Real Time** is selected from the Time drop-down list.

For information about configuring events, see the "About Events" section on page 6-1.

Figure 8-24 Event Inbox

1	Display Events. Click this icon  to display the Events inbox.6
2	View selector. Choose an option for the layout of the Event Inbox.
3	Time selector. Choose an option to limit the events that appear in the Events Inbox, as described in the following procedures. Various other fields may appear, depending on the time option that you choose. These options allow you to designate a time and date range, priority and keyword. After you make time and filter settings, click **Go** to update the display.
4	Priority filter drop-down list. Choose to display only events that have a specific priority.
5	Keyword field. To find all events with text in the Event Time, Event Name, or Description fields that contain a designated keyword or text string, enter the text in this field.
6	Go button. Click to display events that match the designated time period, filter, or keyword string.
7	Clear button. Click to clear the Priority filter and Keyword field.
8	New event. Time and name of the event.

9	Event list. See the following instructions for field and feature descriptions.
10	Page controls. Use to page through the events list: •  —Click to display the first page •  —Click to display the previous page •  —Click to display the next page •  —Click to display the last page •  —Enter a page number and press the Enter key to display that page
11	Create clip. Click to create a 1-minute clip from an event.
12	Mark as. Click to mark an event as Read or Unread.
13	Unhide. Click to display hidden events.
14	Hide. Click to hide selected events.

To display and manage events, follow these steps:

Procedure

Step 1 Click the **Display Events** icon  to display the Events Inbox, as shown in Figure 8-24.

Step 2 (Optional) To display events that occur within a specified time period, choose one of the following options from the Time drop-down list.

When you choose an option, additional fields may appear for that option.

- **All**—Displays all events that are stored in the system. To refresh the display, choose All again (the Events Display does not refresh automatically).
- **Real Time**—Displays the most recent 100 events and adds new events to the list as they occur.
- **Date Range**—Displays events that occurred within the dates and times that you enter in the From and To fields.
- **Last 24 Hours**—Displays events that occurred within the last 24 hours.
- **Last 7 Days**—Displays events that occurred within the last 7 days.
- **Last 30 Days**—Displays events that occurred within the last 30 days.

Step 3 (Optional) To display only events that have a specific priority, choose the priority from the Filter drop-down list.

This option is not available when **Real Time** is selected from the Time drop-down list.

Step 4 (Optional) To find all events with text in the Event Time, Event Name, or Description fields that contain a designated keyword or text string, enter the text in the Keyword field.

This option is not available when **Real Time** is selected from the Time drop-down list.

Step 5 (Optional) Click **Go** to display only the events that are defined by the time, filter, and keyword settings.

The event list includes the following information:

- Priority—Severity of the event:
  -  —Priority 1 event
  -  —Priority 2 event
  -  —Priority 3 event

  - —Priority 4 event
  - —Priority 5 event
  - —Informational event
- Status—Indicates if the event is Read or Unread
- Event Time—Date and time that the event occurred
- Event Name—Name of the event
- Description—Provides information about the event:
  - For a motion event, the type of event (start or stop) and the name of the motion detection window in which the event occurred
  - For analytics event, the name of the analytics package that is used, the camera name, and the rule name
  - For a device trigger event or soft trigger event, the description that was provided when the event was created

Tip Click an underlined column header to sort on that column. Click again to reverse the sort order.

Step 6 (Optional) To view video that is associated with an event, use the following controls:

- **View icon** —Click to load the video archive that is associated with the event and play the video, starting 10 seconds before the event occurred.
- **Seek** icon —Click for an event to play the currently loaded archived videos, starting 10 seconds before the event occurred.
- **Loop** icon —Click for an event to repeatedly play a clip that is associated with the event. You must first load the archive video from the video archives list.

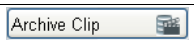
  By default, the clip starts playing from a point 10 seconds before the event occurred and plays for 30 seconds before repeating. You can adjust these settings on the Player Control/Settings pop-up window (for more information, see the "Using the Playback Controls" section on page 8-27).
- **View** link—Click for an analytics event to display the video that is associated with the event, starting 10 seconds before the event occurred

Step 7 (Optional) Choose one of the following additional settings or actions:

- **Hide**—Check the check boxes for one or more events and click **Hide** to hide the selected events for the current user.
- **Unhide**—Click the **Unhide** button to display events that were hidden by using the **Hide** button.
- **Mark As**—Check the check boxes for one or more events, and then click the **Mark As** button and choose **Read** or **Unread** to change the Status of the event.
- **Create Clip**—Check the check boxes to create clips for one or more events. See the "Creating Event Video Clips" section on page 8-40.

Creating Event Video Clips

To create video clips of events and save them to the VSMS host in BWM or BWX format, perform the following steps. After a clip is saved, it can be downloaded to a computer for viewing. Clips in BWX format are password protected, as described in the following instructions.

Tip You can also use the **Archive Clip** button 

to save video clips on the VSMS host in BWM and BWX format. This feature also allows you to save clips directly to your computer in AVI/MP2, WMV and CVA formats. See the "Creating an Archive Clip" section on page 8-16 for instructions.

Procedure

Step 1 Click the **Display Events** icon  to display the Events Inbox, as shown in Figure 8-24 on page 8-37.

Step 2 Check the check box for one or more events and choose **Create Clip**.

Step 3 Choose one of the following options from the drop-down list:

- **Create BWM Clip**—Creates the clip in BWM format
- **Create BWX Clip** —Creates the clip in BWX format

Step 4 If you are prompted to enter an alpha-numeric password from 6 to 64 characters (case-sensitive).

The password prompt appears if you are creating a BWX clip. This password is required to play the clip after it is downloaded to a computer.

Note You can create a clip on a motion stop event but not on a motion start event. You cannot clip the same event twice because the start and stop times would be the same.

Step 5 Wait for the clip to be created.

A message regarding the status of the create operation appears above the event list.

The clip is automatically saved to include a few extra seconds before and after the actual event.

Step 6 Click the **Refresh** button  to update the Video Archives list and display the new event clip.

The new clip appears next to a computer icon  in the Video Archives list.

Step 7 To save the clip to your computer, do the following:

a. Click the name of the clip and then click **Save**.

b. Choose a location for the file on a local or network computer and click **Save** again.

Step 8 Use the Cisco ReView Player video client to play the video clip.

To install the video client, go to the Software & Downloads panel in the Administrator pages. Click the **VSOM Video Client** link and follow the installation instructions. For related information, see the "Managing Software and Downloads" section on page 4-1.

Health Dashboard

The Health Dashboard that is available in the Operator page provides a summary events that are related to the operational health of the overall video surveillance system. Health events are generated automatically and do not require any user configuration.

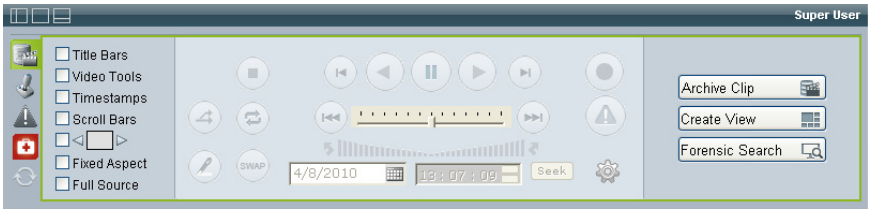
There are two types of health events: critical and warning.

- Critical health events are shown in red and render a component unusable. Examples include devices that are not reachable, archives that fail to start or stop, failed camera authentication, and motion configuration failures. Components with critical events remain out of operation until another event restores them to normal operation. Critical events also affect other components that depend upon the component that is in the error state. For example, if a camera is in the critical error state, all feeds and archives for that camera also are in the critical error state.
- Warning health events are shown in green and indicate a problem that does not incapacitate a component. For example, interruptions in operation due to packet losses in the network. Warning health events do not change the overall state of the component, and are not associated with critical health events.

Viewing the Health Dashboard

To view a summary of health events, click the **Health Dashboard** icon  shown in Figure 8-25.

Figure 8-25 Health Dashboard icon in the Control Bar



The icon changes colors depending on the health events present in the system:

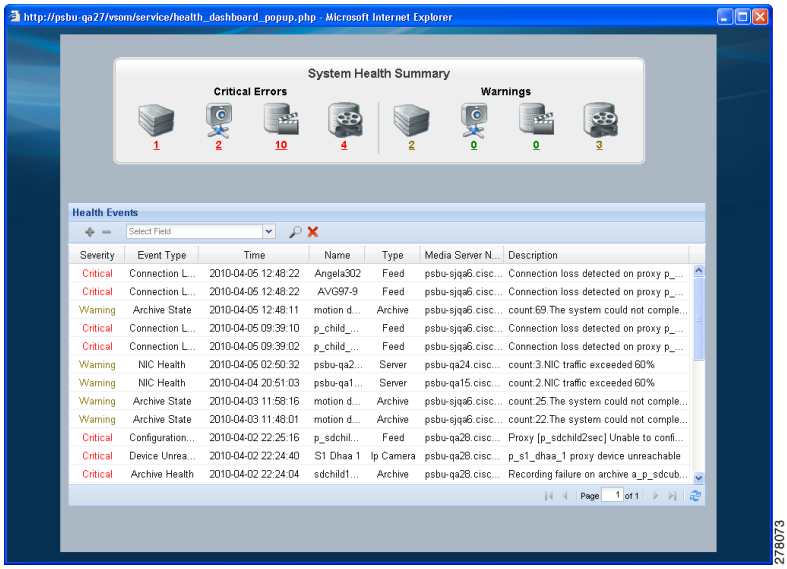
 —No health events are present in the system when the icon is gray. The icon is disabled.

 —Only warning health events are present in the system when the icon is green. There are no critical events. Click the icon to open the System Health Summary page in a separate window (Figure 8-26).

 —Critical health events are present in the system when the icon is red. Click the icon to open the System Health Summary page in a separate window (Figure 8-26).

When you click either the green or red icon, the System Health Summary page shown in Figure 8-26 opens in a separate window.

Figure 8-26 Health Dashboard



The icons at the top show the number of critical errors and warnings that exist for each of the following:

 —VSMS host servers configured in the Cisco VSM deployment.

 —Endpoints, including encoders and IP or analog cameras

 —Video feeds

 —Video archives

Tip Click the refresh icon  to update the page with all current health events.

Note

- For more information about system health events, see the "Using the Health Dashboard" section on page 6-23. Administrators can view additional health event history information, and detailed information for each health event.
- Health events are not related to the VSOM video surveillance events. See the "Viewing Video Events" section on page 8-36 for more information.

Using the Health Dashboard (Operator Page)

To view the health events and details available to Cisco VSN Operator users, do the following.

Note For detailed information about health events, you must have administrator privileges. Administrators can view additional health event history information, and detailed information for each health event. See the "Using the Health Dashboard" section on page 6-23.

Procedure

Step 1 Click the red **Health Dashboard** icon  to open the System Health Summary window shown in Figure 8-26.

Step 2 Click the number below the icons to view only entries for the corresponding source.

A summary of health events is displayed in the Health Events table. This table includes the following informationTable 8-4 describes.

Table 8-4 Health Events Table Information

Item	Description
Severity	The severity of the event: Critical or Warning.
Event Type	General event classification, such as “device unreachable” or “disk usage.”
Time	Date and time that the event occurred.
Name	Name component name assigned by an administrator or operator.
Type	Type of component: server, camera/encoder, feed, or archive.
Media Server Name	Name that is assigned to the associated VSMS.
Description	Text description of the event, as generated by the component. If multiple warnings of the same type are generated during the current reporting interval, a single entry is presented with a count that indicates the number of occurrences. See the “Health Event History” section on page 6-28 for more information. For example, the following entry indicates that 5 “NIC traffic exceeded 60%” events have been received since the last Health History Retention reset. `Count 5: NIC traffic exceeded 60%` The current reporting interval is configured on the Settings page (default is 1 day). See the “Configuring System Settings” section on page 6-18.

Step 3 To sort on a column, click the column header.

Click again to change the sort order.

Step 4 To filter events in the table, follow these steps:

a. Choose a column from the drop-down list at the top of the table.

Additional drop-down lists appear for matching categories and value or range.

b. Choose a matching category from the second drop-down list and specify the value or range.

For Name, Media Server Name, or Description, the match criteria include the following:

- **Equals**—Displays entries that exactly match the value.
- **Not Equals**—Displays entries that do not match the value.
- **Like**—Displays entries that contain the value. For example, the value “elco” matches all “Pelco” entries.

c. To add filters, click the icon to the left of the filter area. To remove a filter, click the icon. To clear all filters, click the red cross icon.

d. To filter the table based on the specified criteria, click the icon. The table is updated to match the filters that you entered.

CHAPTER 9

Using Smart Search

Cisco Smart Search analyzes archived, live, or saved video clips and detects and indexes points at which motion events occurs. Operators can then easily review these motion events by using the Smart Search video player or VSOM.

This chapter explains how to use Smart Search. It includes these topics:

Note

- The Smart Search windows, buttons and icons appear only if the VSM administrator enables Use Smart Search in the Administrator Settings page. See "Configuring System Settings" section on page 6-18 for more information.
- Before you can use the Smart Search feature, the SmartSearch service must be running on the PC that you are using. In most cases, this service starts automatically. However, if you are using a PC that is running the Microsoft Windows 7 operating system and you are logged in as a user without Administrator privileges, you must start the SmartSearch service manually. To do so, choose **Start > All Programs > Cisco Video Surveillance** and double-click **SmartSearch**.

Understanding Smart Search

Smart Search provides an efficient way to locate *motion events* in archived, live, or saved video. A motion event is a segment of a video stream in which Smart Search detects motion according to criteria that you specify.

To identify motion events in a video, Smart Search uses an indexing process. This indexing process analyzes designated video according to parameters that you specify, and creates a *motion index*, which identifies points in the video at which motion events occur. The process also optionally saves a set of still images of motion events on your local hard drive. After the motion index is created, you can view the motion events by using the Smart Search video player or the VSOM operator page.

In general, using Smart Search involves these general steps:

1. Designate the archived, live, or saved video in which you want to view motion events.

2. Configure the parameters that Smart Search uses when creating the motion index. Parameters that you can configure include the time period to analyze, specific areas in the video field to analyze, the amount of motion required to be considered a motion event, and others.
3. Initiate the indexing process.
4. View the motion events.

The following section provide detailed information about these general steps.

Understanding the Smart Search Window

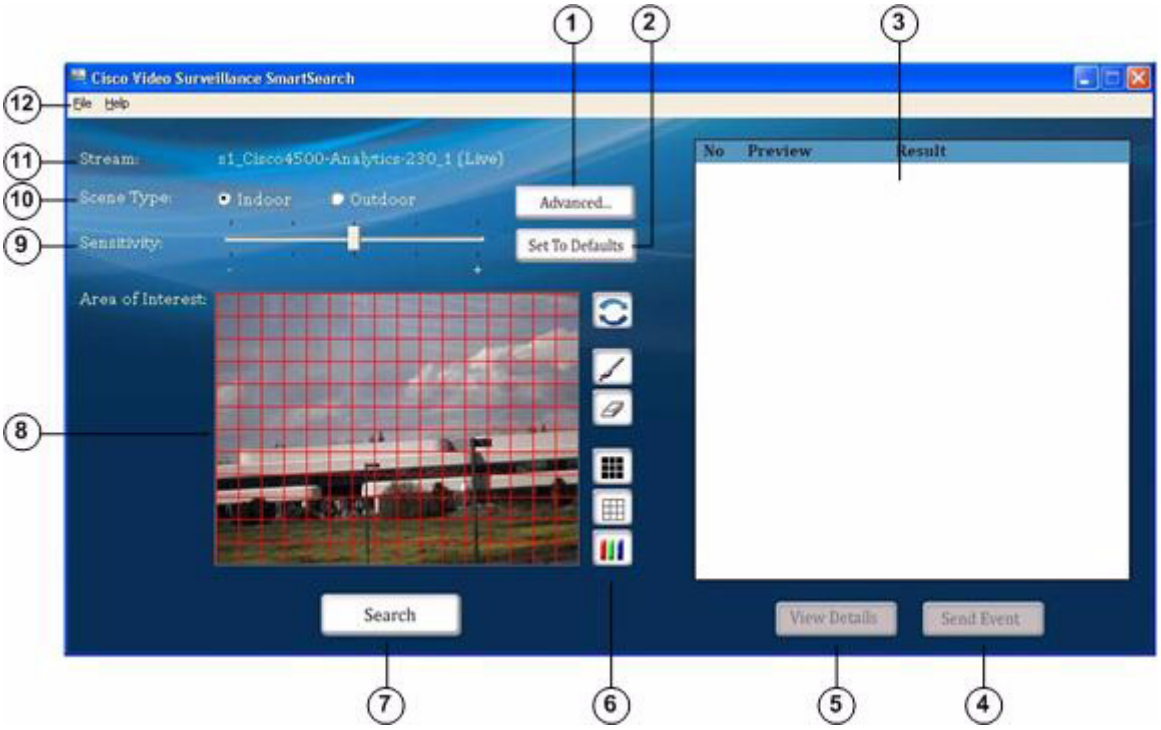
You use the Smart Search window to define parameters for the motion indexing process, to access Smart Search Advanced Settings window, to initiate the indexing process, and to view video that contains motion events.

To access the Smart Search window for an archived or live video stream, choose the video stream from the Camera Feeds or Video Archives lists in the VSOM Operator Pages, then click the **Smart Search** icon  in the top right corner of a selected video pane. Figure 9-1 shows the Smart Search window

Note If the Smart Search application is not installed, a dialog box prompts you to install it when you click the **Smart Search** icon. Click **OK**, and then follow the on-screen prompts to install the Smart Search applications.

Alternatively, you can manually download and install the Smart Search application from the Software & Downloads panel in the Administrator pages by clicking the **Smart Search** link and following the installation instructions. For more information, see the "Managing Software and Downloads" section on page 4-1.)

Figure 9-1 Smart Search Window



1	**Advanced** button—Click to display the Smart Search Advanced Settings window. For detailed information about this window, see the "Advanced Settings" section on page 9-5.
2	**Set to Defaults** button—Click to set the Scene Type, Sensitivity, and Area of Interest options to their default values.
3	Search Results area—After Smart Search completes the motion indexing process, the motion events appear in this area as a series of clips. For each motion event, this area shows the following information: • No—A reference number that the system assigns to the motion event. • Preview—Appears only if you choose to save event images on your local drive (as described in the "Viewing Motion Events by using the Smart Search Window" section on page 9-8.) The preview is a thumbnail image from the motion event that shows where the motion event started. • Result—The start date and time of the motion event ("From"), then end date and time of the motion event ("To"), and the duration of the motion event.
4	**Send Event** button—Applies only to motion events from archived video. Click to view the motion event in the VSOM Operator pages.
5	**View Details** button—Click to view a motion event that you select in the Search Results area.

6	Search area selection buttons—Use the following buttons to select specific sections in the Area of Interest that Smart Search should analyze for motion: •  —**Refresh Image** button. Click to refresh the displays of an image from a live video stream. •  —**Brush** button. Click to start the brush tool, which you can use to select parts of the area of interest in which to search for motion. When you click this button, the mouse pointer changes to a brush image. Position the brush image over a grid square in the area of interest to and click to select that square, or hold down the left mouse button and drag the brush image over several grid squares to select them. Selected grid squares appear highlighted. •  —**Erase** button. Click to start the erase tool, which you can use to deselect parts of the area of interest. When you click this button, the mouse pointer changes to an eraser image. Position the eraser image over a selected (highlighted) grid square in the area of interest and click to deselect that square, or hold down the left mouse button and drag the eraser image over several grid squares to deselect them. When you deselected a grid square, its highlight disappears. •  —**Select All** button. Click to select the entire area of interest for the search. When you click this button, the entire area of interest becomes highlighted. •  —**Clear All** button. Click to deselect all selected (highlighted) grid squares in the area of interest. •  —**Select Color** button. Click to choose the color in which selected (highlighted) grid squares appear. After you click this button, choose a color from the palette that pop up, and then click **OK**.
7	**Search** button—Click to start the motion indexing process. During the motion indexing process for archived video, a progress bar indicates progress of the process. During the motion indexing process for live video, a progress bar indicates continuous indexing.
8	Area of interest—Displays a still image from the video stream and lets you define the areas of the video frame in which Smart Search checks for motion.
9	**Sensitivity** slider—Drag the sensitivity slider to define the relative amount of motion in the designated area of interest that is required for the system to detect a motion event. Sensitivity ranges from low, indicated by -, to high, indicated by +. A lower setting designates that more motion is required to cause the system to detect a motion event. For example, use Low to avoid unnecessary detection of small animals outdoors, or movement of paper and other objects indoors. A higher setting designates that less motion is required to cause the system to detect a motion event.

10	**Scene Type**—Choose a radio button to automatically set sensitivity to a value that is appropriate for your environment: • **Indoor**— Choose for indoor environments. Sets sensitivity to the middle value. • **Outdoor**— Choose for outdoor environments. Sets sensitivity to the lowest value.
11	Stream—*Display only.* System-generated name of the live or archived video stream. Also designates "(Live)" or "(Archive)" to identify the type of stream.
12	Smart Search window menus: • File menu—Lets you choose a saved video clip that you want to open or enter the URL of a live or archived video stream. For more information, see the "Indexing Live or Archived Video" section on page 9-6 or the "Using Smart Search with Saved Video Clips" section on page 9-10. • Help menu—Provides these options: – **About...**—Choose for information about the release of Smart Search that you are using – **Help**—Click for information about using Smart Search

Advanced Settings

The advanced settings define additional settings for the Smart Search feature. To access the Advanced Settings window, click the **Advanced...** button in the Smart Search window.

Table 9-1 describes the options in the Advanced Settings window.

Table 9-1 Advanced Settings Window Options

Processing	Designates the processing method that Smart Search uses to analyze video streams when preparing a motion index: • **Normal**—Video is processed frame by frame. This method most accurate for locating motion events, but requires more time to complete. The processing time for archived video is the same as the duration of the video. For example, a 10 minute archive takes 10 minutes to process. This method is the default for processing live video. • **Fast**—Video is processed as quickly as it can be streamed over the network. This method generally is 5 times as fast as normal processing, but may not be as accurate. This method is the default for processing archived video.
Save Event Images	Check this check box to save on your local hard drive thumbnail images from motion events that the indexing process identifies. If you do not check this check box, thumbnail images of motion events do not appear in the SmartSearch window and you must send a motion event to VSOM to view it.

Table 9-1 Advanced Settings Window Options (continued)

Minimum disk space	Specify the maximum amount of disk space that can be used to store still images and related information. If the maximum disk space is exceeded, a pop-up warning message appears. The video continues to play in the area of interest in the Smart Search window, but index processing is not performed. The existing index images are saved on your hard disk, but no additional images are saved until additional disk space is available. When data is deleted and disk space is freed, Smart Search automatically resumes index processing.
Days to Keep Data	Enter the number of days that the system stores images (if you choose to save event images) and data files from the motion indexing process on your PC. These items are deleted automatically after this period. The default value is 7. If the default value is changed, the new number becomes the default for the current index and any new indexes. The maximum value is 365. A value of 0 causes Smart Search to delete index files when you close the current Smart Search session.
Display Motion	Designates whether the area in which motion is detected is highlighted when you view a motion event in the Smart Search window: • **Motion Area**—The area in which motion is detected is highlighted by a grid of red squares • **No Motion**—The area in which motion is detected is not highlighted
Time of Interest	Applies only to archived video only and when Processing is set to **Normal**. Choose the **Start** and **End** date and time of the video to search for motion. **Note** Live streams are indexed for motion until you manually stop the indexing process.
OK	Click to save the advanced settings and exit the Advanced Settings window.
Cancel	Click to exit the Advanced Settings window without saving changes.
Use Defaults	Click to set options in the Advanced Settings window to their default values.

Indexing Live or Archived Video

To locate and view motion events in live or archived video, you must first index the video. The indexing process identifies points in the video at which motion events occur, and stores images (if you choose to save event images) and data files from the motion indexing process on your PC.

For information about viewing motion events in saved video clips, "Using Smart Search with Saved Video Clips" section on page 9-10

To create an index of live or archived video, follow these steps:

Procedure

Step 1 Verify that **Use Smart Search** is enabled in the Administrator Settings pages.

For instructions, see the "Configuring System Settings" section on page 6-18.

Step 2 Take either of these actions:

- Choose the camera feed or video archive in which you want to detect motion events, then continue to Step 3.

  For information about camera feeds and video archives, see the "Viewing Live and Archived Video" section on page 8-7.

- From the VSOM Operator pages, click the Smart Search **Smart Search** button 

in the bottom right of the toolbar to launch the Smart Search application, choose **File > Open Cisco Stream...**, then enter the URL of the live or archived video stream in the Cisco Stream URL dialog box and click **OK**. The skip to Step 6.

Note If the system prompts you to install the Cisco Smart Search client application when you click the **Smart Search** button, follow the on-screen instructions to do so. After installing the application, go back to the VSOM Operator pages and click the **Smart Search** button again to continue.

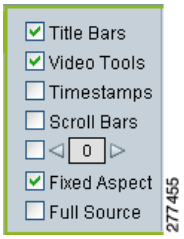
Enter the URL in the format **bwims://*server*/*proxy***, where *server* is the IP address or host name of the VSOM server that provides the video stream and *proxy* is the proxy name of the video stream. (To determine the proxy name for a live video stream, access the VSM Management Console and choose **BWT pages > Proxy Commands > All Running Proxies**. To determine the proxy name for an archive, access the VSM Management Console and choose **Archives > View All Archives**. For more information, see Chapter 10, "Using the VSM Management Console.")

For example, bwims://myserver/a_p_s1_Cisco2500_-_a_regular_170.

Step 3 Display the video pane controls by checking the **Title Bars** and **Video Tools** check boxes in the bottom left corner of the toolbar, as shown in Figure 9-2.

You can check other check boxes as desired. These other options apply only if you view the video in VSOM. See the "Understanding the Toolbars" section on page 8-23 for more information about these controls.

Figure 9-2 Video Pane Controls



Step 4 Click the **Smart Search** icon  in the top tight corner of the selected video pane.

The **Smart Search** icon appears only if Smart Search is enabled (Step 1) and the **Title Bars** and **Video Tools** check boxes are checked (Step 3).

Step 5 If the system prompts you to install the Cisco Smart Search client application, follow the on-screen instructions to do so.

Step 6 (Optional) In the Smart Search window, make the motion index settings that are described in the "Understanding the Smart Search Window" section on page 9-2 and, in the "Advanced Settings" section on page 9-5.

Smart Search uses the default value for each option that you do not set.

Step 7 Click **Search** in the Smart Search window to start the indexing process.

Information about motion events that the indexing process identifies appear in the Search Results area in the Smart Search window.

For archived video, a progress bar shows the status of total video processed.

For live video streams, the indexing continues until it is manually stopped.

After the indexing process completes, you can view video that contains motion events as described in the "Viewing Motion Events" section on page 9-8.

Viewing Motion Events

After you create a motion index as described in the "Indexing Live or Archived Video" section on page 9-6, you can view motion events by using the Smart Search window or by using the Operator window, as described in the following sections:

- Viewing Motion Events by using the Smart Search Window, page 9-8
- Viewing Motion Events in Archived Clips by using the Operator Window, page 9-10

Viewing Motion Events by using the Smart Search Window

A motion event is a segment of a video stream in which Smart Search detects motion according to criteria that you specify. To use the Smart Search window to view motion events that Smart Search detects, follow these steps:

Procedure:

Step 1 Make sure that the indexing process completes (see the "Indexing Live or Archived Video" section on page 9-6).

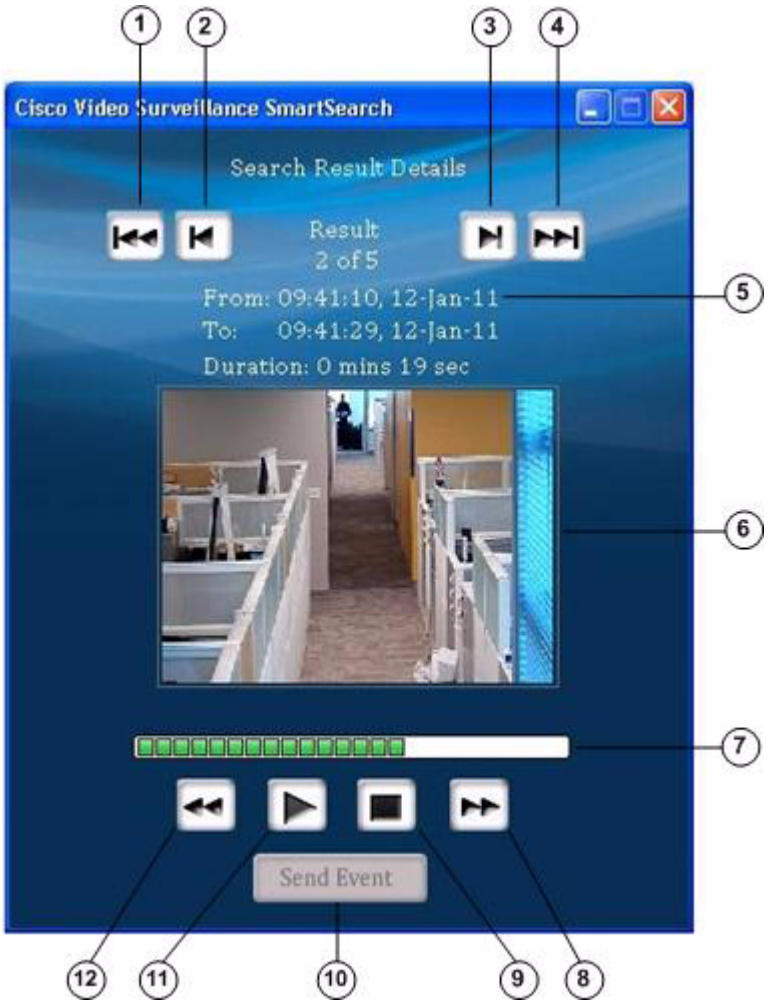
Step 2 In the Search Results area in the Smart Search window, double-click the motion event that you want to view, or click the motion event and then click the **View Details** button.

The Search Result Details window appears, as shown in Figure 9-3) and the motion event starts playing. When it reaches the end, it replays automatically.

You can use the Search Result Details window to control playback of the motion event and to view certain parts of the motion event. You also can use this window to send information about a motion event from an archived video stream to VSOM so that you can view the motion event from the Operator pages.

When you are finished viewing the motion event, close the Search Results Details window.

Figure 9-3 Search Result Details Window



1	First Record button—Displays the first motion event from the Search Results area
2	Previous Record button—Displays the previous motion event from the Search Results area
3	Next Record button—Displays the next motion event from the Search Results area.
4	Last Record button—Displays the last motion event from the Search Results area.
5	Motion event information—Motion event number (“Result”), start date and time (“From”), end date and time (“To”), and duration.
6	Video display—Looping display of the clip.
7	Progress bar—Represents the progress of the motion event playback.
8	**Next Frame** button—Appears only when playback of the clip is paused. Click to move the video display ahead by one frame.
9	**Stop** button—Appears only when the clip is playing or paused. Click to stop playback of the clip. When you click the **Play** button after stopping playback, the clip starts from the beginning.
10	**Send Event** button—Applies only to motion events from archived video. Click to view the motion event in the VSOM Operator pages.

11	**Play/Pause** toggle button—When the clip is playing, click the **Pause** button to pause playback at the current frame. When the clip is stopped or paused, click the **Play** button to play the clip.
12	**Previous Frame** button—Appears only when playback of the clip is paused. Click to move the video display back by one frame.

Viewing Motion Events in Archived Clips by using the Operator Window

You can use the Operator window to view motion events that Smart Search detects in archived clips. To do so, follow these steps:

Procedure:

Step 1 Make sure that the indexing process completes (see the "Indexing Live or Archived Video" section on page 9-6).

Step 2 In the Search Results area in the Smart Search window, click the clip that you want to view, then click the **Send Event** button.

The motion event appears in the Operator window.

Step 3 Use the archive controls to navigate the video archive.

See the "Using the Playback Controls" section on page 8-27

Using Smart Search with Saved Video Clips

You can use Smart Search to create motion indexes of video files that are saved on your computer or a network computer in AVI or WMV format, and you can view the motion events that Smart Search identifies.

To index and view motion events for a saved video file, follow these steps:

Procedure

Step 1 Take either of these actions to launch the Smart Search application:

- From the VSOM Operator pages, click the Smart Search **Smart Search** button 

in the bottom right of the toolbar.

  This button appears only if the Use SmartSearch option is enabled in the Settings panel in VSOM Administrator pages. For instructions, see the "Configuring System Settings" section on page 6-18.

- From the Windows Start Menu, choose **Start > All Programs > Cisco Video Surveillance > Smart Search**.

Step 2 Choose **File > Open Clip...**.

Step 3 In the Open dialog box, choose the desired AVI or WMV clip from your local drive or a network drive and click **Open**.

The Smart Search window appears, as shown in Figure 9-1 on page 9-3.

Note The first time that you open a clip, the system may prompt you to install the FFDShow application, which lets you view AVI and WMV clips. If you see this prompt, follow the onscreen prompts to install FFDShow.

Step 4 In the Smart Search window, make the desired configuration settings as described in the "Understanding the Smart Search Window" section on page 9-2 and in the "Advanced Settings" section on page 9-5.

Step 5 Click **Search** in the Smart Search window to start the indexing process.

Information about motion events that the indexing process identifies appear in the Search Results area in the Smart Search window.

After the indexing process completes, you can view video that contains motion events as described in the "Viewing Motion Events" section on page 9-8.

PART 4

Management Console Reference

CHAPTER 10

Using the VSM Management Console

The VSM Management Console provides a web-based interface through which you can perform various system configuration and management operations and see important information for Cisco Video Surveillance Media Server (VSMS), Cisco Video Surveillance Operations Manager (VSOM), and Cisco Video Surveillance Virtual Matrix (VSVM). The pages and options that are available from the Management Console depend on the type of system (VSMS, VSOM, or VSVM) that you are using it for and on installed VSM components.

This chapter includes these topics:

Accessing and Exiting the Management Console

To access the Management Console, use any method that Table 10-1 describes. Each method starts a Management Console for the corresponding VSM application. When you access the Management Console, it appears in a new browser window.

The default user name for logging in to the Management console is **root** and the default password is **secur4u**. For information about changing the password, see the "Management Console Password Page" section on page 10-24.

Table 10-1 Methods for Accessing the Management Console

Method	Remarks	Procedure
Accessing the Management Console for a VSOM or VSMS host by using its IP address or host name.	This procedure does not work if you have chosen the **Change default homepage to VSOM** option. (See the Operations Manager Configuration Page, page 10-19 for more information.)	From a PC that is on the same network as the host, enter the IP address or host name of the VSOM or VSMS host in a supported web browser.
Accessing the Management Console from the VSOM web interface.	This method provides access only to VSMS hosts that have been configured in VSOM.	1. Access VSOM as described in the "Accessing VSOM" section on page 1-4. 2. In the VSOM Operator page, click the **Admin** link, which appears near the top left of the page. 3. Click the **Servers** link under Devices to display a list of configured servers. 4. In the Console column, click the Cisco logo that appears in the row of the system for which you want to display the Management Console. 5. If a pop-up window prompts you to log in, enter your VSMS user name and password and click **OK**.
Accessing the Management Console from the keyboard and monitor that are attached to a VSMS system.	You can use this method to access the Management Console for VSMS systems that are not yet configured in VSOM.	1. Click the Management icon on the server desktop:  2. If a pop-up window prompts you to log in, enter your VSMS user name and password and click **OK**.
Accessing the Management Console from your PC.	You can access the Management Console for a VSMS from a PC that is on the same network as the VSMS system.	1. Start a web browser and enter the following address, where <*server*> is the IP address or host name of the VSOM host: **http://<*server*>/vsmc.html** 2. If a pop-up window prompts you to log in, enter your VSMS user name and password and click **OK**.

To exit the VSM Management Console, exit the browser window in which it appears.

Overview Pages

The Management Console provides the following overview pages:

- Installed Packages—Displays a list of installed and driver packages. For more information, see the "Installed Packages Page" section on page 10-3.
- Status Console—Provides current and historical information about system performance and resource use. For more information, see the "Status Console Page" section on page 10-3.
- Raid Status—Provides information about the Redundant Array of Independent Disks (RAID) on a system, if applicable. For more information, see the "RAID Status Page" section on page 10-5.

Installed Packages Page

The Installed Packages page appears when you access the Management Console from the VSOM Administration Area. You also can display the Installed Packages page by clicking the **Installed Packages** link under Overview at the left side of the Management Console.

The Installed Packages page displays this information:

- Installed Packages—Lists the VSM packages that you have installed.
- Additional Driver Packages—Lists the VSM drivers that you have installed for cameras and encoders. For related information, see the "Manage Drivers Page" section on page 10-15.

Status Console Page

The Status Console Overview page displays a set of graphical reports that show various information about performance and resource use of a VSMS system. This page also provide access to reports that provide historical performance and resource use data. You can use the information that the Status Console page provides to monitor and review system performance.

To display the Status Console page, click the **Status Console** link under Overview at the left side of the Management Console.

Viewing Current Reports

When the Status Console Overview page appears, it displays the following reports for the VSMS system. These reports show information that is current at the time that you display the page. To update reports, refresh your browser, or exit and then access the Status Console page.

- CPU (user and system) Load %—Displays the CPU resources that are consumed by users and by system operations, as a percentage of total CPU capacity.
- CPU Load Avg—Displays the average CPU resources that are consumed by users and the average CPU resources that are consumed by system operations, as a percentage of total CPU capacity. The system calculates averages at 5-minute intervals.
- Disk Usage—Displays the amount of disk space used on the root and /usr disks for system files, archives, and related files, as a percentage of total capacity of these disks.
- Free Memory—Displays the amount of RAM used and the amount of free RAM.
- New TCP Connections—Displays the number of existing TCP connections to and from the server.

- Traffic Analysis—Displays the amount of incoming and outgoing network traffic, in bytes per second.

Viewing Historical Reports

To display historical versions of any Status Console report, click the report name or graph in the Status Console Overview page. Historical reports include the following:

- Daily graph—Provides information for the past 32 hours, calculated by averaging values every 5 minutes. The information in this graph is the same as the information that appears in a graph on the Status Console Overview page.
- Weekly graph—Provides information for the past 8 days, calculated by averaging values every 30 minutes.
- Monthly graph—Provides information for the past 4 weeks, calculated by averaging values every 2 hours.
- Weekly graph—Provides information for the past 12 months, calculated by averaging values every 1 day.

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

To return to the Status Console Overview page from any page that displays historical reports, click the **Return to Status Console** index link at the top or bottom of the page.

Understanding Reports

Status Console reports provide information as follows:

- The time scale at the bottom of a graph progresses from left to right, as indicated by a small red arrow at the right of the scale. The time that the report generates appears at the far right of the time scale.
- The vertical red line indicates a start of a new period as follows:
  - Daily report—12:00 a.m. (00:00)
  - Weekly report—12:00 a.m. (00:00) on Monday
  - Monthly report—First day of the month
  - Yearly report—First day of the year (January 1)

The green shaded area provides information as follows:

  - CPU (user and system) Load % report—Displays the CPU resources that are consumed by users and by system operations, as a percentage of total CPU capacity.
  - CPU Load Avg report—Displays traffic load on the server, as a percentage of total CPU capacity.
  - Disk Usage report—Displays the amount of disk space use on the /usr disk of the server, as a percentage of total disk capacity.
  - Free Memory graph—Displays the amount of free memory on the server, in bytes
  - New TCP Connections graph—Displays the number of new incoming TCP connections.
  - Traffic Analysis graph—Displays the amount of incoming network traffic, in bytes per second.

- The blue line provides information as follows:
  - CPU (user and system) Load % report—Displays the server CPU use, as a percentage of total CPU capacity.
  - CPU Load Avg report—Displays traffic load on the server, as a percentage of total CPU capacity.
  - Disk Usage report—Displays the amount of space that is used for incoming traffic on the /usr disk of the server, as a percentage of total disk capacity.
  - Free Memory report—Displays the total amount of total memory, in bytes
  - New TCP Connections report—Displays the number of new outgoing TCP connections.
  - Traffic Analysis report—Displays the amount of outgoing network traffic, in bytes per second.
- The dark green line displays the maximum value for incoming traffic, calculated every 5 minutes. This line does not apply to the Traffic Analysis reports.
- The magenta line displays the minimum value for incoming traffic, calculated every 5 minutes. This line does not apply to the Traffic Analysis reports.

RAID Status Page

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

To display the RAID Status page, click the **Raid Status** link under Overview at the left side of the Management Console.

The Raid Status page includes these areas:

- VSM RAID Viewer area—The left side of this area provides general information about the RAID that is installed on the system and shows the version of the BIOS that the system is running.

  The center of this area includes these button:
  - **Refresh Status**—Click to update the information on the page with the most current data.
  - **Silence Alarms**—Click to silence the alarm that sounds when a RAID failure occurs or when the RAID array is rebuilding.
  - **Create Debug Package**—Click to create zip file that contains RAID controller log files, then follow the prompts that appear to download the zip file to your PC. The Cisco Technical Assistance Center (TAC) may request the debug package if you need assistance with troubleshooting a RAID issue.

  The right side of this area provides links that you can click to quickly display other areas of the RAID Status page.
- Disk Usage area—Provides information about the RAID file systems.
- Virtual Disks Summary—Provides summary information about the virtual disks in the RAID.
- Physical Disks Summary—Provides summary information about the physical disks in the RAID.
- Virtual Disks Details—Provides detailed information about the virtual disks in the RAID.
- Physical Disks—Provides detailed information about the physical disks in the RAID.
- Disk Error Definitions—Defines various RAID error types that can occur.

Monitoring Pages

The Management Console provides the following monitoring pages:

- Archives—Displays and provides access to information about archives. For more information, see the "Archives Page" section on page 10-6.
- Archive Backup—Displays and provides access to information about archives that are backed up on the system. For more information, see the "Archive Backup Page" section on page 10-9.
- System Log—Lets you display information from the system log files. For more information, see the "System Log Page" section on page 10-10.
- Mediaout—Displays and provides access to information about current Mediaout, HTTP, and RTSP connections to the server. For more information, see the "Mediaout Page" section on page 10-11.
- Server Status—Displays information about processes and components on this system. For more information, see the "Server Status Page" section on page 10-12.

Archives Page

The Archives page displays and provides access to information about archives that are configured for your VMS system.

To display the Archives Overview page, click the **Archives** link under Monitoring at the left side of the Management Console. The Archives Overview displays this information:

- Total number of Archives—Number of archives that are configured
- Current Recording Rate—Rate, in Mbps, at which data is being written to the server. You can use this information to calculate when the server will reach its storage capacity and to determine appropriate retention periods.

Viewing Information About Archives

You can view information about archives from the Archives Overview page as follows:

- To Display a list of all archives, click the **View All Archives** link. A list of all archives appears. Table 10-2 describes the information that the list provides.

Table 10-2 Archive Information

Item	Description
Archive Name	Name that you configured when you set up the archive. To see detailed information about the archive, click its name. The "Understanding Archive Details" section on page 10-8 describes the information that appears.
Archive Type	Type that you configured when you set up the archive: • Regular—The archive is configured as a regular archive, which runs for a set duration • Loop—The archive is configured as a loop archive, which repeats contains data for a set duration • Clip—A portion of an archive • BWM—Proprietary clip that can be played by using the Cisco ReView Player • BWX—Password-protected proprietary clip that can be played by using the Cisco ReView Player • Backup—Archive that is backed up to another VSMS
Archive Status	Whether the archive is recording: • SHELVED—Archive has stopped recording. (A regular or loop archive can be started again.) • RUNNING—Archive is actively recording
Archive Media	Type of data in the archive (for example, MPEG-4 or JPEG).
Archive Expiry	When the archive is configured to expire. Data in an archive is removed after this time. A value of 0 indicates that the archive does not expire.
Archive Size	Amount of disk space that the archive is currently using.
Storage Est.	Amount of disk space that has been reserved for the archive. If there is not sufficient space, an archive does not start.
Archive Duration	For a regular archive, indicates how long the archive runs. For a loop archive, indicates the length of time in the loop.
Retention	Percentage of the archive that is currently stored on the server. This value is calculated as follows (Table 10-3 explains each of the variables in this calculation): (Archive Stop Time – Archive Start Time) / Archive Duration A value of 1 or greater appears as 100%.

- To see detailed information about all archives, click the **View complete details of all Archives** link. The "Understanding Archive Details" section on page 10-8 describes the information that appears.
- To see detailed information about a specific archive, choose the archive from the drop-down list at the bottom of the page, then click the **View** button. The "Understanding Archive Details" section on page 10-8 describes the information that appears.

Understanding Archive Details

When you display detailed information about an archive by clicking its name, as described in the "Viewing Information About Archives" section on page 10-6, you see the information that Table 10-3 describes.

Table 10-3 Archive Details

Item	Description
Archive Name	Name that you configured when you set up the archive.
Archive Status	Whether the archive is recording: • SHELVED—Archive has stopped recording. (A regular or loop archive can be started again.) • RUNNING—Archive is actively recording
Storage Path	Location of archive on the server.
Archive Type	Type that you configured when you set up the archive: • Regular—The archive is configured as a regular archive, which runs for a set duration • Loop—The archive is configured as a loop archive, which repeats contains data for a set duration • Clip—A portion of an archive • BWM—Proprietary clip that can be played by using the Cisco ReView Player • BWX—Password-protected proprietary clip that can be played by using the Cisco ReView Player • Backup—Archive that is backed up to another VSMS
Archive Duration	For a regular archive, indicates how long the archive runs. For a loop archive, indicates the length of time in the loop.
Archive Media	Type of data in the archive (for example, MPEG-4 or JPEG)
Video Width	Width in pixels of the video image in the archive.
Video Height	Height in pixels of the video image in the archive.
Video Quality	Recording quality of stream, on a scale from 1 to 100. A higher number represents higher quality but consumes more disk space.
Video Framerate	Framerate of the video. Applies to JPEG streams only.
Video Bitrate	Bitrate of the video. Applies to non-JPEG streams only.
Archive Expiry	When the archive is configured to expire. Data in an archive is removed after this time. A value of 0 indicates that the archive does not expire.
Archive Size	Amount of disk space that the archive is currently using.
Archive Storage Est	Amount of disk space that has been reserved for the archive. If there is not sufficient space, an archive does not start.

Table 10-3 Archive Details (continued)

Item	Description
Archive Start Time	• For regular archives, date and time of first frame found on the disk. • For loop archives, date and time of first frame found on the disk. • For clips, start date and time of the clip. 0 indicates that no data was found for this clip. • For BWM or BWX clips, start date and time of the clip. • For backup archives, date and time of first frame found on the disk • For a backup clips (a backup of a non BWM or BWX clip, start time of the clip. 0 indicates that no data was found for this clip.
Archive End Time	• For regular archives, date and time of last frame found on the disk. • For loop archives, date and time of last frame found on the disk. • For clips, end date and time of the clip. 0 indicates that no data was found for this clip. • For BWM or BWX clips, end date and time of the clip. • For backup archives, date and time of last frame found on the disk • For a backup clips (a backup of a non BWM or BWX clip, end time of the clip. 0 indicates that no data was found for this clip.
Archive Create Time	For BWM and BWX clips, date and time that the clip was created.
Event Archive	Indicates whether the archive was created due to an event occurring (yes or no).
Recording Rate	Recording rate of the archive, in Mbps.
Max Fps	Maximum number of frames per second in the archive.
Max Frame Size	Maximum frame size in the archive.
Current Duration	Current length of the archive, calculated as: Archive End Time – Archive Start Time
Current Retention	Percentage of the archive that is currently stored on the server. This value is calculated as follows: (Archive Stop Time – Archive Start Time) / Archive Duration A value of 1 or greater appears as 100%.

Archive Backup Page

The Archive Backup page displays information about archives that are backed up on this server.

To display the Archive Backup page, click the **Archive Backup** link under Monitoring at the left side of the Management Console. The Archive Backup page displays the summary information that Table 10-4 describes.

Table 10-4 Archive Backup Summary Information

Item	Description
Archive Name	Name that you configured for the archive
Backup Status	Displays Succeeded for a backup that completed or Failed for an archive that did not complete
Start Time	Date and time that the backup started
End Time	Date and time that the backup completed
Number of files sent	Number of archive files sent to this backup server

To see detailed information about an archive backup, click its name in the list. The system displays a report that includes the information that Table 10-5 describes.

Table 10-5 Archive Backup Detailed Information

Item	Description
Archive name	Name that you configured for the archive
Archive status	Displays Succeeded for a backup that completed or Failed for an archive that did not complete
Start Time	Date and time that the backup started
End Time	Date and time that the backup completed
No. of files sent	Number of archive files sent to this backup server
No. of bytes sent	Number bytes in all files sent to this backup server
Last file send time	Date and time that the last file in the backup was sent to this backup server
Log file size	Size in bytes of the archive backup log file
Log file	Displays the contents of the log file, which includes additional information about the archive backup

System Log Page

The System Log page lets you display up to 400 lines from the VSMS log files.

To display the System Log page, click the **System Log** link under Monitoring at the left side of the Management Console.

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

Procedure

Step 1 Click the **System Log** link under Monitoring at the left side of the Management Console.

The System Log page appears.

Step 2 From the **Select log file to view** drop-down list, choose the log file for which you want information:

Choices are:

- **ims.log**—Primary VSMS log file. Includes system error messages and system activity messages.
- **httpd.access**—Includes HTTP requests that the VSOM or VSMS host sends to the Apache server.
- **httpd.errors**—Apache server error log.
- **snmpd.log**—Includes information about the snmp daemon, such as when the snmp daemon starts, stops, the snmpd.conf configuration file is read by the daemon.

Step 3 From the **Select number of recent lines to view** drop-down list, choose the number of log file entries that you want to view.

The system can display the most recent 100, 200, 300, or 400 entries.

Step 4 Click the **View** button.

Mediaout Page

The Mediaout page displays and provides access to information about video that the VSMS system is serving. VSMS uses a Mediaout connection to serve video.

To display the Mediaout Overview page, click the **Mediaout** link under Monitoring at the left side of the Management Console. The Mediaout Overview page displays this information:

- Total number of Mediaout Connections—Number of HTTP and RTSP connections that live or archived video is being served to. Indicates the number of users who are viewing video through an HTTP or RTSP connection.
- Bandwidth of all Mediaout Connections—Total bandwidth that is consumed by all Mediaout connections.
- Total number of HTTP Connections—Total number of HTTP connections that live or archived video is being served to. Indicates the number of users who are viewing video through an HTTP connection.
- Bandwidth of HTTP Mediaout Connections—Total bandwidth that is consumed by all HTTP Mediaout connections.
- Total number of RTSP Connections—Total number of RTSP connections that live or archived video is being served to. Indicates the number of users who are viewing video through an RTSP connection.
- Bandwidth of RTSP Mediaout Connections—Total bandwidth that is consumed by all HTTP Mediaout connections.

Viewing Information About Mediaout Connections

You can view detailed information about Mediaout connections from the Mediaout Overview page by clicking the following links:

- **View details of all Mediaout connections**—Provides detailed information about all HTTP and RTSP connections that are serving live or archived media feeds
- **View details of all HTTP connections**—Provides detailed information about HTTP connections that are serving live or archived media feeds

- **View details of all RTSP connections**—Provides detailed information about RTSP connections that are serving live or archived media feeds
- **View details of all live media connections**—Provides detailed information about HTTP or RTSP connections that are serving live media feeds
- **View details of all recorded media connections**—Provides detailed information about HTTP or RTSP connections that are serving archived media feeds

To view detailed information about a specific proxy or archive connection, choose the name of the connection from the drop-down list at the bottom of the page, then click the **View** button. A proxy connection is used for live video and an archive connection is used for recorded video.

For a description of the detailed information that you can view, see the "Understanding Media Out Connection Details" section on page 10-12.

Understanding Media Out Connection Details

When you display detailed information about a Mediaout connection as described in the "Viewing Information About Mediaout Connections" section on page 10-11, you see the information that Table 10-6 describes.

Table 10-6 Mediaout Connection Details

Item	Description
Protocol	Protocol that the Mediaout connection uses (HTTP or RTSP)
Type	Type of stream that is being viewed (live or recorded)
Name	Name of the live or recorded stream that is being viewed
Media	Type of media in the stream (for example, MPEG or JPEG)
IP Address	IP address of the client PC that is viewing the stream
Port	Port on the server from which the stream is being sent
Uptime	How long the stream has been being running
Transport Type	Transport protocol used for the stream (TCP or UDP)
Avg Bandwidth	Average bandwidth used by the stream, in bytes per second
Avg FPS	Average frames per second send in the stream
Lost Frames	Number of frames dropped by the stream
RTP loss	Number of RTP packets dropped by the stream

Server Status Page

The Server Status page displays status information about VSMS processes and components.

To display the Server Status page, click the **Server Status** link under Monitoring at the left side of the Management Console.

Configuration Pages

The Management Console provides the following configuration pages:

- SNMP Trap Destinations—Displays information about the SNMP service status and lets you configure SNMP trap destinations. For more information, see the "SNMP Trap Destinations Page" section on page 10-13.
- Manage Drivers—Lists driver packages that are installed on the Media Server and lets you upload, install, and uninstall driver packages. For more information, see the "Manage Drivers Page" section on page 10-15.
- Media Server—Provides information about Media Server settings and provides options for configuring several basic parameters. For more information, see the "Media Server Configuration Page" section on page 10-17.
- Media Server Backup—Lets you create and store a backup file that contains Media Server configuration information. For more information, see the "Media Server Backup Page" section on page 10-19
- Operations Manager—Provides information about VSOM settings and provides options for configuring several basic parameters. For more information, see the "Operations Manager Configuration Page" section on page 10-19.
- Operations Manager Backup—Lets you create and store a backup file that contains VSOM configuration information. For more information, see the "Operations Manager Backup Page" section on page 10-23.
- Virtual Matrix—Lets you designate the port number on which Video Surveillance Virtual Matrix clients communicate with the VSMS host. For more information, see the "Virtual Matrix Configuration Page" section on page 10-24.
- Console Password—Lets you designate the password that must be entered to access the Management Console. For more information, see the "Management Console Password Page" section on page 10-24.
- Camera Firmware Upgrade—Lets you upgrade the firmware on one or more cameras in your video surveillance deployment. For more information, see the "Camera Firmware Upgrade Page" section on page 10-25
- Server Upgrade—Lets you upgrade the VSMS software that is running on the VSMS host. For more information, see the "Server Upgrade Page" section on page 10-27.
- Restart Server—Lets you restart VSM applications on the server that you are accessing. For more information, see the "Restart Server Page" section on page 10-28.
- Reboot Server—Lets you reboot (power cycle) the server that you are accessing. For more information, see the "Reboot Server Page" section on page 10-29.
- Shutdown Server—Performs a graceful shutdown of the server. For more information, see the "Shutdown Server Page" section on page 10-29.

SNMP Trap Destinations Page

The SNMP Trap Destinations page displays information about the SNMP service status. It also lets you configure SNMP trap destinations.

To display the SNMP Trap Destinations page, click the **SNMP Trap Destinations** link under Configuration at the left side of the Management Console.

Viewing SNMP Trap Status

The top part of the SNMP Trap Destinations page displays the SNMP service status, which can be either of the following:

- On—SNMP service is operating. This state is the system default.
- Off—SNMP service has not started, has been stopped, or has failed. To troubleshoot this issue, start by issuing the following Linux command on the VSMS host to check the status of the SNMP service: **/etc/init.d/cisco status**.

Downloading the VS Event MIB

SNMP trap receivers on client SNMP servers use a management information block (MIB) to interpret traps that they receive from a VSMS host.

To view the MIB file, click the **VS Event MIB** link.

Configuring SNMP Trap Destinations

The system automatically configures the VSOM host as a trap destination. You can configure up to five SNMP additional trap destinations. To do so, perform the following steps.

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

Procedure

Step 1 Click the **SNMP Trap Destinations** link under Monitoring at the left side of the Management Console.

The SNMP Trap Destinations page appears.

Step 2 In the IP Address/Host Name field for the trap that you are configuring, enter the IP address or host name of the server to receive SNMP traps.

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

Repeat this step for each trap that you want to configure.

Note The first option in this field indicates the VSOM host that the system has automatically configured as an SNMP trap destination. This first option is not configurable.

Step 3 Click the **Update** button.

To remove a trap destination, delete the information in the IP Address/Host Name field, then click **Update**.

Manage Drivers Page

The Manage Drivers page lists driver packages that are installed on the Media Server. It also lets you upload, install, and uninstall driver packages. Driver packages enable the use of various Cisco and third-party cameras and encoders with VSM.

To display the Manage Drivers page, click the **Manage Drivers** link under Configuration at the left side of the Management Console.

Viewing a List of Driver Packages

The Driver packages area of the Manager Drivers page lists the driver packages that are on the Media Server. The list includes the version number of each driver package. The designation [“installed]” indicates that VSMS can be used with the device that the driver supports.

Uninstalling a Driver Package

Uninstalling a driver package makes is unavailable for use. This process does not remove the driver package from the system. You can reinstall it at any time.

To uninstall a driver package, follow these steps:

Procedure

Step 1 Click the **Manage Drivers** link under Monitoring at the left side of the Management Console.

The Manage Drivers page appears.

Step 2 From drop-down list in the Uninstall Driver Package area, choose the driver package that you want to uninstall.

This list includes all driver packages that are installed on this server.

Step 3 Click the **Uninstall** button.

The Management Console indicates the operations that it performs and give you the option to restart VSMS.

Step 4 Take either of these actions:

- To restart VSMS, click where indicated, then click the **Restart Now** button.
- To return to the Manage Drivers page without restarting VSMS, click where indicated.

If you do not restart VSMS now, make sure to do so to ensure that the uninstall process completes.

Installing a Driver Package

When you install a driver package, the system automatically uninstalls other version of the driver package that are installed on the Media Server. An uninstalled driver package is not removed from the VSMS host.

Use this process to install a driver package that you have uninstalled and that is stored on the VSMS host. To install a driver package that is not stored on the VSMS host, see the “Uploading a Driver Package” section on page 10-16.

To install a driver package, follow these steps:

Procedure

Step 1 Click the **Manage Drivers** link under Monitoring at the left side of the Management Console.

The Manage Drivers page appears.

Step 2 From drop-down list in the Install Driver Package area, choose the driver package that you want to install.

This list includes all drivers that are stored on the VSMS host.

Step 3 Click the **Install** button.

The Management Console indicates the operations that it performs and give you the option to restart VSMS.

Step 4 Take either of these actions:

- To restart VSMS, click where indicated, then click the **Restart Now** button.
- To return to the Manage Drivers page without restarting VSMS, click where indicated.

If you do not restart VSMS now, make sure to do so before using the devices that are associated with the driver package to ensure that the devices function properly with VSM.

Uploading a Driver Package

Uploading a driver package copies a driver package that you downloaded from Cisco.com to the VSMS host and then installs the driver package. You can use this procedure when you need to update the Media Server with a new driver package or you need to install a driver package for a new device.

Before you begin, download the driver package to a PC that you can access from the system on which you are running the Management Console.

To download a driver package go to http://www.cisco.com/go/physicalsecurity, click the **Products** link, then click the **Cisco Network-Centric Video Surveillance products** link. See the Download Software section on the page for information about obtaining driver packages. You must have a valid support contract or registration to access this web site.

To upload and install a driver package, follow these steps:

Procedure

Step 1 Click the **Manage Drivers** link under Monitoring at the left side of the Management Console.

The Manage Drivers page appears.

Step 2 In the field for the driver name in the Install Driver Package area, enter the full path and file name of the driver package to upload.

You can use the **Browse** button to locate the driver package.

Step 3 Click the **Upload** button.

The Management Console indicates the operations that it performs and give you the option to restart VSMS.

The system validates the driver package and displays an error message if it is not valid.

Step 4 Take either of these actions:

- To restart VSMS, click where indicated, then click the **Restart Now** button.
- To return to the Manage Drivers page without restarting VSMS, click where indicated.

If you do not restart VSMS now, make sure to do so before using the devices that are associated with the driver package to ensure that the devices function properly with VSM.

Media Server Configuration Page

The Media Server Configuration page provides information about Media Server settings and provides options for configuring several basic parameters. This page also provide options for configuring archive storage repositories.

To display the Media Server Configuration page, click the **Media Server** link under Configuration at the left side of the Management Console.

If you change any options in the Media Server Configuration page, you must click the **Update** button at the bottom of the page to save the changes. To discard the changes, exit the page by choosing another page or exiting the browser.

If addition, after changing any options in the Media Server Configuration page you must restart the VSMS host as described in the "Restart Server Page" section on page 10-28.

To update options to their last-saved values, click the **Reset** button, then click the **Update** button to save the changes.

Cisco recommends that you back up the VSMS configuration whenever you make changes to it. For instructions, see the "Media Server Backup Page" section on page 10-19.

Table 10-7 describes the options in the Media Server Configuration page.

Table 10-7 Media Server Configuration Page Options

Option	Description
Storage Configuration	
Max Storage %	Specifies the maximum amount of space that recorded data can consume on a storage volume as a percentage of the total disk space on the volume. This configuration applies to all volumes. Valid values are numbers 1 through 98. The default value is 98.
PTZ Configuration	
Camera Control Lockout	Designates how a camera behaves if PTZ contention occurs. (Contention occurs when two resources simultaneously attempt to access a camera PTZ operations.) In this case, the camera responds to PTZ commands from the first resource. It accepts PTZ commands from the next resource when the first resource is idle for the amount of time that this option defines. The default value is 5 minutes.
Media Out Ports	
HTTP Port	*Display only.* The port on the VSMS host to be used for HTTP out connections.

Table 10-7 Media Server Configuration Page Options (continued)

Option	Description
RTSP Port	The port on the VSMS host to be used for RTSP out connections. Valid values are integers 1 through 65535. The default value is 554. Unless there is a network requirement it is recommended that the default port be used because it is the standard RTSP port.
Proxy Port	The port on the VSMS host to be used for video proxy out (live media) connections. Valid values are integers 1 through 65535. The default value is 9090. Unless it is being used by another system process, it is recommended that the default port be used.
RTP Port Range	The port on the VSMS host to be used for RTP out connections. Valid values are integers 1024 through 49151. Separate a range of values with a dash (-). For example, 2024-2052.
Local Repositories	
Local Archive Repositories	Displays a list of available partition mounts on the server where recordings can be stored. VSMS can recognize up to 500 partitions mounts. Repositories in red are unmounted locations. This 500 partition mount limit includes the partitions specified in the Local Repository, Clipping (BWM and BWX), and Back-up settings. If an unmounted partition has no mount directory, it is not be listed. If the Media Server is recording archives, check the check box for at least one Local Archive Repository must be selected. (The archive directory permissions must be set to 777 if owned by root or 755 if owned by nobody. Make these configuration in the Linux operating system. To designate that partition as available for Media Server storage repositories, check the checkbox next to each partition mount.
Clipping	
Local BWM/X Clip Repository	Defines where BWM and BWX clips are stored on the VSMS host. From the Local BWM/X Clip Repository drop-down list, choose the local Media Server repository mount location where BWM are BWX clips stored. Only one mount can be recognized. If **-- No Repository --** is specified, BWM and BWX clip generation fails.

Table 10-7 Media Server Configuration Page Options (continued)

Option	Description
Back-up	
Back-up Repository	List of partitions where backup video archives can be stored. If this VSMS host is to be used as a backup server for video archives, designate each partition that should be available as a storage repository by checking the **Back-up Repository** check box next to the partition mount. A backup server is a VSMS host that is used as a resource to store backup video archives. VSMS can recognize up to 500 partition mounts. Repositories that appear in red type are unmounted locations. This 500 partition mount limit includes the partitions specified in the Local BWM/X Repository configuration settings. If an unmounted partition has no mount directory, it is not listed.
Events	
Maximum Event Marking Duration	The maximum duration for a motion or other event recording. This option should be set to the maximum number of seconds of continuous activity that any camera in a deployment might capture. Valid values are integers 1 through 86400. The default value is 7200 (2 hours).

Media Server Backup Page

The Media Server Backup page lets you create and store a backup file that contains Media Server configuration information. The backup file is a zip file that you can store on your local PC. Then, if necessary, you can use this file to restore the Media Server to a previous state. (If you need to restore the Media Server, contact the TAC for assistance.)

To display the Media Server Backup page, click the **Media Server Backup** link under Configuration at the left side of the Management Console.

To back up the current Media Server configuration, click the **Download Now** button, then use the Save As pop-up window to save the configuration file.

Operations Manager Configuration Page

The Operations Manager Configuration page provide information about VSOM settings and provides options for configuring several basic parameters.

To display the Operations Manager Configuration page, click the **Operations Manager** link under Configuration at the left side of the Management Console.

If you change any options in the Operations Manager Configuration page, you must click the **Update** button at the bottom of the page to save the changes. To discard the changes, exit the page by choosing another page or exiting the browser.

To update options to their last-saved values, click the **Reset** button, then click the **Update** button to save the changes.

Table 10-8 describes the options in the Operations Manager Configuration page.

Table 10-8 Operations Manager Configuration Page Options

Option	Description
Log Level	
Log Level	Use the log level to determine the type of information that the system writes to the VSOM log file. This log file is named vsom.log and is stored on the local host in the usr/BWhttpd/logs/ folder. Log levels are: • **Emergency Only**—Messages related to critical errors that prevent the system from running. • **Error Conditions**—Messages related to any errors that the application experiences. Also includes Emergency Only messages. • **Notice (Default)**—Messages regarding normal actions taken by the application. Also includes Error Conditions and Emergency Only messages. • **Debug**—Debugging information. Also includes messages from all other log levels. The **Emergency Only** log level provides the best performance. The **Debug** log level captures the most data but may cause the system to run slower. Any change that you make to the log level takes effect immediately after you click the **Update** button.
Database Connection	
Database Type	Choose the type of database that VSOM uses to operate. Database types are: • **MySQL 5.0**—Default database type. Specifies that storage uses a local or remote MySQL 5.0 database • **Oracle 10g**—For legacy use. Not supported.
Database Server	Enter the connection location of the database. For MySQL 5.0, enter the IP address of the MySQL server. Use either **localhost** (default) or a fully-qualified IP address.
Database Username	Enter the log in user name that is required for connecting to the database. This name must start with a letter and contain letters and numbers only. It is case sensitive. This value should be changed only if configuring an advanced deployment on a shared MySQL server. The default user name for MySQL is **cisco**.

Table 10-8 Operations Manager Configuration Page Options (continued)

Option	Description
Database Password	Enter the log in password that is required for connecting to the database. This name can contain any combination of up to 41 letters and numbers. This value should be changed only if configuring an advanced deployment on a shared MySQL server. The default password is **mysql**. **Note** Changing this Database Password does not change your database user password. You must change your user password in the database before you change this Database Password.
Database Name	Typically database servers allow multiple schemas or database instances. The Database Name points to the correct schema or instance on the database server. MySQL—The pre-determined database name used by the application. The default username is cisco. This value should be changed only if you are using a database other than MySQL or configuring an advanced deployment on a shared MySQL server. The default value is BAS.
Database Configuration Validation	
Database Status	Click the **Validate DB** button to check the database connection status and verify that database tables were created correctly. These checks are based on the database settings that were configured when you last clicked the **Update** button on this page. The validate function checks table names only. It does not validate the database schema. Information appears in a pop-up window. Click **OK** to close the window.
SMTP Parameters	
SMTP Server	Enter the IP address of host name of an SMTP server to which the system routes e-mail that the application generates when an event occurs.
SMTP “From:” Address	Enter an e-mail address to a appear in the From: field of e-mails that the system sends. This field is required if VSOM is to sending e-mail message when an SNMP event occurs.

Table 10-8 Operations Manager Configuration Page Options (continued)

Option	Description
User Login Authentication	
Authentication Type	Choose how the system validates a user name and password that a user enters when logging in to VSOM. Authentication types are: • **Application Database**—Default selection. Designates that VSOM authenticates a user name and password against its internal database. • **LDAP Server**—Designates that VSOM authenticates a user name and password against the LDAP server that is configured in the LDAP Configuration section. When using an LDAP Server, the users must be manually created in VSOM, and the user name must match exactly the user name that is configured in the authenticating LDAP server.
LDAP Configuration	
Note These fields are required only if you choose **LDAP Server** from the Authentication Type drop-down list. If you choose **Application Database** from that list, these fields are ignored and can be left empty.	
Host Name	Enter the IP address or the host name of the LDAP server to be used to authenticate user log in credentials. For example, ds.cisco.com.
Host Port	Enter the port number of the LDAP server that is used to authenticate user log in credentials. If this field is blank, the value 389 is used.
Relative Distinguished Names (RDN)	Enter the LDAP Relative Distinguished Names to be used for authentication. In the RDN, the token %username% is replaced dynamically with the user name when a user attempts to log in. For example, enter: CN=%username%,OU=Employees,OU=cisco users
Domain Controllers (DC)	Enter the list of domain controllers, in order of precedence. Separate each controller with a semicolon (;). For example, enter: DC=amer,DC=cisco,DC=com;DC=euro,DC=cisco,DC=com
Delimiter	Enter a character to use as a delimiter between the RDN and the DC. The default delimiter is a semicolon (;).

Table 10-8 Operations Manager Configuration Page Options (continued)

Option	Description
Select Homepage	
Change default homepage to VSOM Change default homepage to VSMC	Click a radio button to designate the action that the system takes when you access a VSOM or VSMS server with the following address and then log in. (<*server*> is the IP address or hostname of the server.) http://<*server*> • **Change default homepage to VSOM**—The system displays the VSOM login page. If you do not select this option, you enter **http://<*server*>/vsom** to access the VSOM Log In page, where <*server*> is the IP address or hostname of the VSOM server. • **Change default homepage to VSMC**—Displays the Management Console. If you do not select this option, a user must enter http://**<*server*>/vsmc.html** to open the Management Console, where <*server*> is the IP address or hostname of the VSMC host.

Operations Manager Backup Page

The Operations Manager Backup page lets you create and store a backup file that contains VSOM configuration information and a copy of the local VSOM database. The backup file is a zip file that you can store on your local PC. Then, if necessary, you can use this file to restore VSOM to a previous state. For information about restoring, see the "Restore the database" instructions in Table 4-2 on page 4-3.

To display the Operations Manager Backup page, click the **Operations Manager Backup** link under Configuration at the left side of the Management Console.

To back up the current VSOM configuration, follow these steps:

Procedure

Step 1 Click the **Operations Manager Backup** link under Configuration at the left side of the Management Console.

The Operations Manager Backup page appears.

Step 2 In the MySQL root password field, enter the MySQL root user password.

The system requires this password so that the SQL database can be backed up. If you provide an invalid password, the backup completes, but the SQL dump inside the resulting .tar does not contain the VSOM data.

Step 3 Click the **Download Now** button, then use the Save As pop-up window to save the configuration file.

Virtual Matrix Configuration Page

The Virtual Matrix Configuration page lets you designate the port number on a Video Surveillance Virtual Matrix (VSVM) host that VSOM uses to communicate with that host. (Cisco suggests that you consult with the TAC before changing this port number.)

To display the Virtual Matrix Configuration page, click the **Virtual Matrix** link under Configuration at the left side of the Management Console.

To change the VSVM host port number that VSOM uses to communicate with this host, follow these steps:

Procedure

Step 1 Click the **Virtual Matrix** link under Configuration at the left side of the Management Console.

The Virtual Matrix Configuration page appears.

Step 2 In the Server Port field, enter the port to use.

Valid values are integers from 1024 to 65535. The default port number is 8086.

Step 3 Click **Update** at the bottom to save the changes.

If you want to discard the change, exit the page by choose another page or exiting the browser.

Note If you want to set the Server Port value to its previously-saved value, click **Reset** and then click **Update**.

Step 4 Restart the VSVM server as described in the "Restart Server Page" section on page 10-28.

Management Console Password Page

The Management Console Password page lets you designate the password that must be entered to access the Management Console.

For security, Cisco recommends that you change the default system password immediately after installing the system, and that you continue to change the password regularly.

To display the Management Console Password page, click the **Console Password** link under Configuration at the left side of the Management Console.

To designate the management console password, perform the following steps.

Note After you change the password, the Management Console prompts for the new password before it displays another page.

Procedure

Step 1 Click the **Console Password** link under Configuration at the left side of the Management Console.

The Management Console Password page appears. The User Name field indicates that the user name for logging in to the Management Console is **root**.

Step 2 In the New Password field, enter a password that adheres to these guidelines:

- Minimum length—3 characters
- Maximum length—10 characters
- Valid characters—Upper case letters, lower case letters, and numbers

The password is case-sensitive.

Step 3 In the Confirm New Password field, enter the password again.

The entry in this field must match exactly the entry in the New Password field.

Step 4 Click **Update** to implement the new password.

Camera Firmware Upgrade Page

The Camera Firmware Upgrade page lets you upgrade the firmware in the video cameras in your deployment. When you use the upgrade camera firmware feature, be aware of these guidelines:

- This feature is available only if VSMS is installed of your system.
- Do not perform the camera upgrade procedure when a server upgrade is in process because doing so may cause the camera upgrade to fail. (If you open the Camera Firmware Upgrade page while a server upgrade is in process, an alert message informs you that the server upgrade is in process.)
- You can execute an upgrade for one camera or for multiple cameras. You can rerun the upgrade procedure as needed to upgrade cameras of the other type.
- When upgrading Cisco IP camera models 2911, 2916, 2930, 2935, 5010, or 5111, be aware that each camera includes a firmware file that is specific to the model. The camera firmware upgrade process displays the camera model family (for example, 29xx or 5xxx), not the specific model. You must determine the specific camera model before upgrading a camera. If an incorrect firmware file is used, the upgrade process fails.
- If you will use the Cisco video analytics feature on Cisco HD IP Camera 4500 model that is running a firmware version lower than 1.2.1, you must first upgrade the camera to firmware version 1.2.1, then upgrade the camera to a firmware version that provides support for the video analytics feature.
- The upgrade process can take approximately 10 minutes for each camera. If you choose to upgrade multiple cameras, they are upgraded one at a time, in the order that you selected them. A camera is not operational while it is upgrading. Cisco recommends that you perform this process during off-peak hours.
- While the upgrade process is running, you can perform other operations from the Management Console or with VSOM.
- If you are upgrading multiple cameras and a fatal error occurs while upgrading one of them, the upgrade process stops and no additional cameras are upgraded. If a non-fatal error occurs, the camera that experiences the error is not upgraded, but the upgrade process continues for the remaining cameras. Fatal errors includes a camera not coming back on-line after an upgrade or a camera failure during the upgrade. Non-fatal errors include invalid camera log-in credentials.

Note Upgrading your version of Cisco VSM may require you to update the firmware in the cameras in your VSM deployment. See the camera firmware release notes to determine if a camera firmware upgrade is required.

Upgrading a camera is a two-part process: First, obtain the firmware from Cisco.com. Then, use the Camera Firmware Upgrade page to perform the upgrade. To upgrade camera firmware, follow these steps:

Procedure

Step 1 Obtain the desired camera firmware package by going to the following URL and downloading the package to your local PC, a network PC, or an FTP server:

http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=280249565

The firmware package is in a zip file.

Step 2 Start the Management Console and click the **Camera Firmware Upgrade** link under Configuration at the left side of the Management Console.

The Camera Firmware Upgrade page appears.

Step 3 From the Camera Firmware Type drop-down list, choose the Cisco IP camera series to which the camera or cameras that you want to upgrade belongs.

In the options that appear in this list, "SD" indicates standard definition and "HD" indicates high definition. For example, the option **Cisco SD 25xx** indicates the Cisco Video Surveillance 25xx series IP camera models.

A list of cameras that you have deployed and that are in the camera series that you choose appears.

Step 4 In the list of cameras, check the check box next to each camera that you want to upgrade, or check the check box at the top of the list to choose all cameras.

If you choose multiple cameras, these cameras upgraded one at a time in the order that you choose them. If you choose all cameras, they are upgraded one at a time in the order that they appear in this list.

Each item in this list includes the following information:

- Camera Name—Name that VSMS assigned to the camera. This name is based on the camera name that is configured in VSOM, with underscores (_) and some extra text removed.
- Model—Cisco model number of the IP camera
- IP/Hostname—IP address of host name of the IP camera
- Version—Firmware version that is installed on the IP camera. The "Unknown" designation indicates a camera that has not responded to a request from VSMS for its firmware version, or for which VSMS cannot determine the firmware version for some other reason. A camera with this designation may not be able to upgrade.

You sort this list by any column in ascending or descending alphanumeric order. To do so, click a column name to toggle between ascending or descending order, or choose the desired order from the drop-down list that appears when you mouse over a column name.

To make sure that this list shows current camera version information, click the **Refresh Cameras** button.

Step 5 Take one of these actions to identify the firmware package to use for the upgrade:

- If the firmware package is on your local disk or a network disk, click the **File Upload** radio button, then enter the path and file name of the firmware package in the **Upgrade file from cisco.com** field. You can use the **Browse** button to locate the firmware package.
- If the firmware package is on an FTP server, click the **FTP Download** button and take these actions:
  - In the FTP Server field, enter the name of the FTP server

- In the Path on FTP Server field, enter the full FTP server path name relative to the home directory of the FTP account, and file name for the firmware upgrade package. Use the format */file_name*, where *file_name* is the name of the firmware package.
- FTP User Name—User name that you use to log in to the FTP server
- FTP Password—Password that you use to log in to the FTP server.

Step 6 Click **Start Upgrade**.

The system performs that upgrade. If you chose multiple cameras, they upgrade in the order that you chose them. If you chose all cameras, they are upgraded one at a time in the order that they are listed on the Camera Firmware Upgrade page.

A status panel displays the progress of the upgrade. Detailed status messages appear in the scrollable text area and general status appears in the status bar.

In addition, the system stores information about the upgrade in the following log files. Refer to the log files if an error occurs during an upgrade. You can use a text editor to view these files. If you want to save them, change their names or move them to another folder, because the system overwrites them each time you perform an upgrade.

- /usr/BWhttpd/upgrade/endpoint/endpoint_upgrade.log—Detailed upgrade log
- /usr/BWhttpd/upgrade/endpoint/endpoint_upgradesummary.log—Upgrade summary

You can abort the upgrade process by clicking the **Cancel Upgrade** button and then click OK in the confirmation pop-up window. If you are upgrading multiple cameras, you can stop the upgrade procedure clicking the **Cancel Upgrade** button. When you click this button, the upgrade that is in process for a camera completes, which can up to approximately 10 minutes, but no additional cameras are upgraded.

Server Upgrade Page

The Server Upgrade page lets you upgrade the VSMS software that is running on the VSMS host. When you use the upgrade server feature, be aware of these guidelines:

- This process upgrades VSMS only. To upgrade VSOM, see the *Installing and Upgrading Cisco Video Surveillance Manager Release 6.3.1* document.
- The server upgrade page is available only if VSMS is installed of your system.
- This feature allows upgrading from VSMS 6.3.0 or later. It does not support earlier releases.
- Do not perform the server upgrade procedure when a camera upgrade is in process because doing so may cause the camera upgrade to fail. (If you open the Server Firmware Upgrade page while a camera upgrade is in process, an pop-up message informs you that the camera upgrade is in process.)
- The upgrade process can take approximately 20 minutes. During this time, your VSM system is not operational. Cisco recommends that you perform this process during off-peak hours.
- The upgrade process automatically restarts the VSMS host.
- After the upgrade process completes, you can manually delete the files in the /usr/BWhttpd/upgrade/server/download folder.
- If you upgrade VSMS on a host on which VSOM is also installed, Cisco recommends that you also upgrade VSOM on that host. For instructions, see *Installing and Upgrading Cisco Video Surveillance Manager (VSM)*.

Upgrading VSMS software is a two-part process: First, obtain the software from Cisco.com. Then, use the Upgrade Server page to perform the upgrade.

To upgrade the VSMS software, follow these steps:

Procedure

Step 1 To obtain the new software upgrade package, from any PC, go to this URL and download the package to an FTP server:

http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=281550158

The software upgrade package is in a zip file.

Step 2 Start the Management Console and click the **Server Upgrade** link under Configuration at the left side of the Management Console.

The Management Upgrade Server page appears.

Step 3 Take one of these actions to identify the software upgrade package to use for the upgrade:

- If the software upgrade package is on your local disk or a network disk, click the **File Upload** radio button, then enter the path and file name of the software package in the **Upgrade file from cisco.com** field. You can use the **Browse** button to locate the software package.
- If the software upgrade package is on an FTP server, click the **FTP Download** button and take these actions:
  - In the FTP Server field, enter the name of the FTP server
  - In the Path on FTP Server field, enter the full FTP server path name relative to the home directory of the FTP account and file name for the software upgrade package. Use the format */file_name*, where *file_name* is the name of the software package.
  - FTP User Name—User name that you use to log in to the FTP server
  - FTP Password—Password that you use to log in to the FTP server.

Step 4 Click **Start Upgrade**.

The system performs the upgrade. When the upgrade completes, the system restarts automatically.

A status panel displays the progress of the upgrade. Detailed status messages appear in the scrollable text area and general status appears in the status bar.

In addition, the system stores information about the upgrade in this log file: /usr/BWhttpd/upgrade/server/upgrade_progress.log. Refer to this file if an error occurs during an upgrade. You can use a text editor to view this file. If you want to save this file, change its name or move it to another folder, because the system overwrites it each time you perform an upgrade.

Restart Server Page

The Restart Server page lets you restart the VSM software on the host that you are accessing. The option on this page does not reboot the host on which the software is running.

The VSM software should be restarted after a Media Server configuration change or a VSMS restore.

To restart the server that you are accessing, click the **Restart Media Server** button on the Restart Media Server page. The restart process starts and messages about the process appear in the bottom area of the page. A success message appears when the server has restarted.

Reboot Server Page

The Reboot Server page lets you reboot the VSM server that you are accessing.

To reboot the server, click the **Reboot Media Server** button on the Reboot Media Server page. The reboot process starts and messages about the process appear in the bottom area of the page. A success message appears when the server has rebooted.

Shutdown Server Page

The Shutdown Server page lets you shut down the VSM server that you are accessing.

To shut down the server, click the **Shutdown Media Server** button on the Shutdown Media Server page.

Other Utilities

The Management Console provides the following pages for accessing related do documentation and preparing a report for troubleshooting:

- Media Server User Guide—Displays an on line version of *Cisco Video Surveillance Media Server User Guide*. The document displays in a window that includes links and tools for navigating through the document and locating desired information.
- Server Report—Creates and saves a report that contains VSM logs and configuration information, and server logs and configuration information. The report is stored as a zip file and can be provided to the Cisco Technical Assistance Center (upon request).

  To create a support report, click the **Generate** button, then use the Save File pop-up window to save the report. It can take several minutes to process the report. Do not navigate away from or refresh this page until you see the Save File pop-up window.

INDEX

A

B

C

D

E

F

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

Z