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

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 6-3 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**
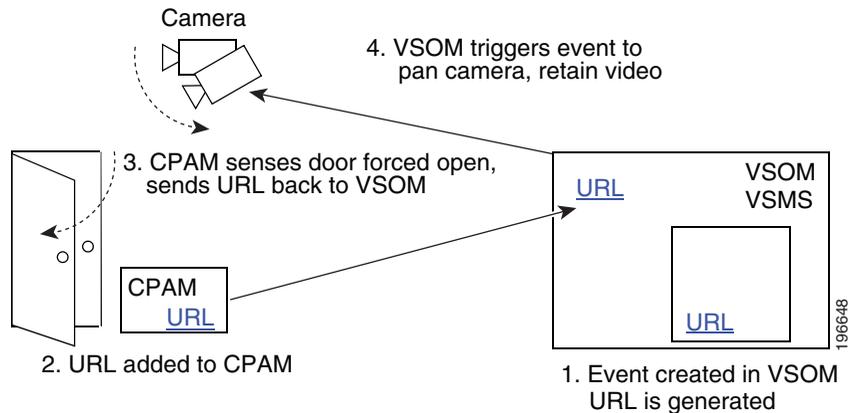
Structure of the Soft Trigger URL

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%activ
ated&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 6-12.

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 6-5
Edit or delete an event	Change the settings for an event or delete an event	Editing and Deleting Events, page 6-11
Set up motion detection	Configure events that are triggered by motion detection	About Motion Detection Events, page 6-12 Setting Up Windows for Motion Detection, page 6-18

Table 6-1   Events Panel Tasks (continued)

Task	Description	Reference
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 6-5
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 1-8.

- Set up the schedules to use for the events. See "Adding a Schedule" section on page 6-22.

- 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 1-9.

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—Check this check box 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—Check the check box 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 6-12.

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 7-12.

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 7-12.

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).

Table 6-2   Editing the Event Configuration

Item	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.
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 the check box and 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 5-34 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 number of days to store the archived event, or choose **Never Expire** to keep the archive indefinitely. • Do not permit these events to overlap—Choose if you do not want to permit archiving of overlapping events. If this is option is checked, then VSOM ignores an incoming event if it occurs during the ongoing recording of the previous event. Events might overlap, for example, if an existing archive includes video that also is captured as part of a motion detection event. Prohibiting overlapping events reduces the volume of stored archive data, but may result in gaps in a particular archive video record. • 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 6-2   Editing the Event Configuration (continued)

Item	Description
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 6-29 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 8-56.
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.

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 camera function. A camera identifies motion based on pixel changes within an image. A camera 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 a camera, and the overall functionality for motion detection is constrained by what a camera 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 6-18.
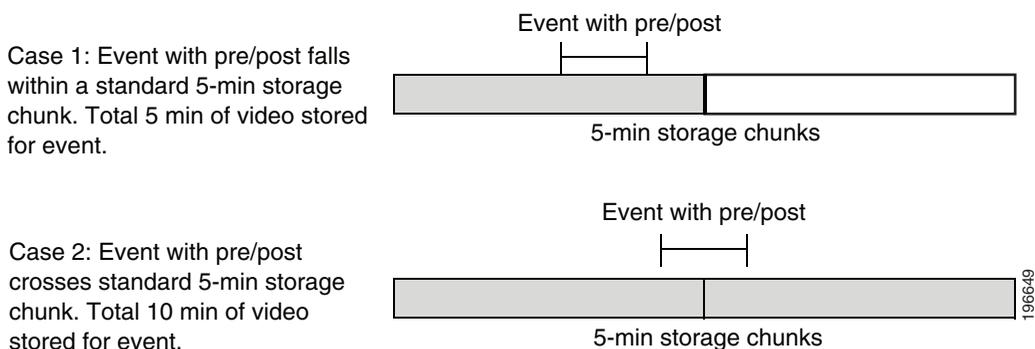
Identifying a larger area risks capturing motion that may not be of interest (such as a person walking in front of the door) and can add unneeded data to the VSOM database.

- 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 five minutes each) as smd files on the VSMS host. When a motion 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 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

Case 1: Event with pre/post falls within a standard 5-min storage chunk. Total 5 min of video stored for event.

Event with pre/post

5-min storage chunks

Case 2: Event with pre/post crosses standard 5-min storage chunk. Total 10 min of video stored for event.

Event with pre/post

5-min storage chunks

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 5-26 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.

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 3-27 or the "Adding a New IP/Network Camera" section on page 3-33.

- Set up any schedules that you want to use to trigger the events. See the "Managing Schedules" section on page 6-21.

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 6-5, 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 6-18.

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	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 5-34 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.

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

Tab	Description
Storage Options	Configure the following storage options: • Store each archive for—Choose the number of days to store the archived event, or choose **Never Expire** to keep the archive indefinitely. • Do not permit these events to overlap—Choose if you do not want to permit archiving of overlapping events. If this is option is checked, then VSOM ignores an incoming event if it occurs during the ongoing recording of the previous event. Events might overlap, for example, if an existing archive includes video that also is captured as part of a motion detection event. Prohibiting overlapping events reduces the volume of stored archive data, but may result in gaps in a particular archive video record. • 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 6-29 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 8-56.
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.

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

Tab	Description
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 3-27 and the "Adding a New IP/Network Camera" section on page 3-33.

- Set up a motion detection event, as described in the "Adding an Event" section on page 6-5.

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 3-27.

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.

Table 6-4   Motion Configuration Settings (continued)

Item	Description
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 care 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 6-22
Edit or delete a schedule	Make changes to an existing schedule or delete a schedule	Editing or Deleting a Schedule, page 6-25

Adding a Schedule

When you create a schedule, it becomes available to apply to users, roles, and events.

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 6-22.

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.

Table 6-6   System Settings (continued)

Item	Description
Show Previews	Check this check box to include camera image previews on pages that have a camera preview area.
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 4-3
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 5-16.
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.

Table 6-6   System Settings (continued)

Item	Description
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 5-26.
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.
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 8-30.
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.

Table 6-6   System Settings (continued)

Item	Description
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 6-32.
	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 6-32.
	When warnings are purged, a message appears below the Event Warning Expiration field.
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.

Table 6-6   System Settings (continued)

Item	Description
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.

Table 6-7   Report Settings (continued)

Item	Description
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 3-12.
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 7-7.
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 7-7.

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 6-25.

> **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 6-40.

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 6-39 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.

Table 6-9   Health Events Table Information (continued)

Item	Description
Event Type	Event classification, as described.
	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)	Recording events: • Archive Health—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 State—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. • 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.

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. •
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 6-25 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 6-40 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 6-30.

- 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 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 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.

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.