Preface

Revised: March 13, 2014

This document describes how to use the Cisco Video Surveillance Safety and Security Desktop (Cisco SASD) desktop software to monitor live and recorded video from the Cisco Video Surveillance Manager (Cisco VSM).

Related Documentation

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

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

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What’s New in Cisco Product Documentation at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Subscribe to What’s New in Cisco Product Documentation, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

Conventions

This document uses the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Indication</th>
</tr>
</thead>
<tbody>
<tr>
<td>bold font</td>
<td>Commands and keywords and user-entered text appear in <strong>bold</strong> font.</td>
</tr>
<tr>
<td>italic font</td>
<td>Document titles, new or emphasized terms, and arguments for which you supply values are in <em>italic</em> font.</td>
</tr>
</tbody>
</table>
Elements in square brackets are optional.

Required alternative keywords are grouped in braces and separated by vertical bars.

Optional alternative keywords are grouped in brackets and separated by vertical bars.

A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

Terminal sessions and information the system displays appear in courier font.

Nonprinting characters such as passwords are in angle brackets.

Default responses to system prompts are in square brackets.

An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note

Means reader take note. Notes contain helpful suggestions or references to material not covered in the manual.

Tip

Means the following information will help you solve a problem. The tips information might not be troubleshooting or even an action, but could be useful information, similar to a Timesaver.

Caution

Means reader be careful. In this situation, you might perform an action that could result in equipment damage or loss of data.

Timesaver

Means the described action saves time. You can save time by performing the action described in the paragraph.

Warning

IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

Statements using this symbol are provided for additional information and to comply with regulatory and customer requirements.
Getting Started

Contents

- Understanding the Cisco SASD Application Suite, page 2
- Main Features of the Cisco SASD Application, page 3
- Understanding the Video Viewing Options, page 6
- Video Viewing Applications, page 6
- Requirements, page 8
- Installing the Application Suite, page 9
- Logging In, page 11
  - Understanding Sites, page 14
  - Understanding Login Approval, page 16
  - Default User Accounts and Passwords, page 16
  - Changing Your Password, page 17
Understanding the Cisco SASD Application Suite

The Cisco Video Surveillance Safety and Security Desktop (Cisco SASD) is a suite of applications that allow Cisco Video Surveillance users to monitor live and recorded video. The application suite includes the following components:

Tip

All applications in the suite are installed using the Operations Manager browser-based interface. See the “Installing the Application Suite” section on page 9 for more information.

Table 1  Cisco SASD Applications

<table>
<thead>
<tr>
<th>Application</th>
<th>Description</th>
<th>More Information</th>
</tr>
</thead>
</table>
| Cisco SASD                     | A full-featured monitoring application that provides access to the cameras and video from a single Operations Manager.                                                                                       | *Overview*  
Getting Started                                                                  |
|                                | Cisco SASD includes the following workspaces and features:                                                                                                                                                  | *Workspaces*                                                                     |  
- Video workspace                                                             |  
- Wall workspace                                                               |  
- Alert workspace                                                              |  
- Maps workspace                                                               |  
- Forensic Analysis Tools                                                      |
| Cisco SASD Advanced Video Player | An advanced monitoring application that includes the following monitoring workspaces:                                                                                                                       | *Video Monitoring*                                                                |  
- Video workspace                                                             |  
- Wall workspace                                                               |
| Cisco SASD Wall Launcher        | Launches a monitoring application for unattended workstations. “Unattended” mode allows video monitoring windows to display Video Walls without access to the Cisco SASD configuration interface. The unattended screens can remain open even is the keyboard and mouse are disconnected, and can (optionally) re-appear when the workstation is rebooted. | *Overview*  
Using the Cisco SASD Wall Configurator                                         |  
*Video Monitoring*                                                                |  
- Controlling Video Playback                                                    |

Overview

Getting Started

Workspaces

- Video Workspace
- Wall Workspace
- Alert Workspace
- Map Workspace

Video Monitoring

- Controlling Video Playback

Forensic Analysis Tools

- Thumbnail Search
- Clip Management
- Motion Analysis

Video Monitoring

- Controlling Video Playback
Main Features of the Cisco SASD Application

The Cisco Video Surveillance Safety and Security Desktop application (Cisco SASD) is the main application in the Cisco SASD suite, allowing you to monitor live and recorded video surveillance using a variety of tools. For example:

- View a list of available cameras based on the camera location or camera name.
- View the cameras and related video on a map.
- View system alerts and the camera that generated the alert.
- View multiple cameras in a grid.
- Create multiple viewing windows and drag them onto additional monitors connected to the PC workstation.
- Create Video Walls to display the same pre-defined set of viewing panes on multiple workstations.
- Use Unattended Mode to automatically open the Video Walls on workstations that do not have a mouse or keyboard.
- Use the Forensic Analysis tools to locate recorded video, search for motion events, and locate video clips.

Table 1  Cisco SASD Applications (continued)

<table>
<thead>
<tr>
<th>Application</th>
<th>Description</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco SASD Wall Configurator</td>
<td>A utility for adding and modifying the video Walls that can be selected and displayed in the monitoring workstations.</td>
<td>Overview Using the Cisco SASD Wall Configurator</td>
</tr>
<tr>
<td>Cisco SASD Federator</td>
<td>A monitoring application that allows Federator users to monitor video from multiple Operations Managers.</td>
<td>Overview Using the Cisco VSM Federator</td>
</tr>
</tbody>
</table>

Workspaces
- Video Workspace
- Alert Workspace

Video Monitoring
- Controlling Video Playback

Forensic Analysis Tools
- Thumbnail Search
- Clip Management
Main Features of the Cisco SASD Application

Figure 1 describes the main Cisco SASD features.

**Figure 1  Overview of the Cisco SASD Features**

1. The Cisco Video Surveillance system (and optional Site) to which you are logged in.
2. Select a menu to logout, launch forensic analysis tools, or open help documents.
   - **File**
     - **Logout**—Log out of the application and disconnect from the Operations Manager. Unattended screens will still be displayed on the workstation, if configured.
   - **Forensic Analysis**
     - **Thumbnail Search**—Use Thumbnail Search to quickly locate specific scenes or events in recorded video without fast-forwarding or rewinding. Thumbnail Search displays a range of video as thumbnail images, allowing you to identify a portion of the recording to review.
     - **Clip Management**—Use Clip Management to view, download and delete MP4 clips that are stored on the server.
     - **Motion Analysis**—Use Motion Analysis to view a summary of motion events for recorded video.
   - **Help**—View additional information and documentation.
3 The video monitoring “workspaces”:

- **Video**—Use the location tree to select a camera or search a camera by name. Select a View to view multiple cameras in a grid. See “Video Workspace” for more information.
- **Wall**—Display video from multiple cameras in a simple grid that maximizes the viewing area. Drag the window to a separate monitor, if necessary. See “Wall Workspace” for more information.
- **Alert**—View and modify system alerts, including the alert video (if the alert is associated with the video). See “Alert Workspace” for more information.
- **Map**—Display maps of the Cisco VSM locations, including the camera and alerts at those locations. Single-click a camera icon to display a draggable icon, or double-click the icon to view video in a pop-up window. See “Map Workspace” for more information.
- **Duplicate**—Click to create a duplicate workspace window that can be dragged to a separate monitor. See “Displaying a Duplicate Workspace on a Separate Monitor”.

4 Click the triangle to display or hide the side panel.

5 Search—Enter the full or partial name of a camera to display matching camera names.

6 Side Panel—Side panels include the controls and search options for the workspace (side panels vary for each workspace). For example, select a location to display the cameras for that location (cameras from sub-locations are not displayed). Then drag a camera onto a viewing pane.

7 Playback Controls—See “Controlling Video Playback”.

8 Viewing Pane and control icons—See “Controlling Video Playback”.

9 - **Layouts**—Create a blank matrix from the available layouts and drag cameras onto each viewing pane.
- **Select View**—Select a pre-defined matrix of cameras. The cameras can be configured to automatically rotate. See “Viewing Camera Video in a Multi-Pane Grid”.

10 Notifications—Notify errors, such as task or software exceptions.

11 Performance Meter—Displays the workstation’s CPU performance based on available memory and bandwidth.

- Green indicates that the workstation is meeting the demands of the Cisco SASD activities.
- Yellow is a performance warning.
- Red indicates that the workstation performance is poor and processing delays may occur.

**Tip** Hover your mouse over the meter network and memory usage details.
Understanding the Video Viewing Options

The Cisco SASD application suite offers the following video viewing methods.

**Table 2 Video Viewing Options**

<table>
<thead>
<tr>
<th>Viewing Mode</th>
<th>Description</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single Camera</td>
<td>View video from a single camera based on a location, alert or map.</td>
<td>• Video Workspace</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Alert Workspace</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Map Workspace</td>
</tr>
<tr>
<td>Multiple Cameras</td>
<td>View a multi-pane matrix of live or recorded video.</td>
<td>• Video Workspace</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Wall Workspace</td>
</tr>
<tr>
<td>Video Walls</td>
<td>View the same video pane matrix on multiple workstations.</td>
<td>• Wall Workspace</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Using the Cisco SASD Wall Configurator</td>
</tr>
<tr>
<td>Unattended Mode</td>
<td>Display a Video Wall on a workstation that does not include a keyboard or mouse. The Video Walls can appear automatically even if the workstation is rebooted.</td>
<td>Using the Cisco SASD Wall Configurator</td>
</tr>
<tr>
<td>Forensic Analysis</td>
<td>Use the analysis tools for the following:</td>
<td>• Thumbnail Search</td>
</tr>
<tr>
<td></td>
<td>• Use <em>Thumbnail Search</em> to quickly locate specific scenes or events in recorded video without fast-forwarding or rewinding. <em>Thumbnail Search</em> displays a range of video as thumbnail images, allowing you to identify a portion of the recording to review.</td>
<td>• Clip Management</td>
</tr>
<tr>
<td></td>
<td>• Use <em>Clip Management</em> to view, download and delete MP4 clips. that are stored on the server.</td>
<td>• Motion Analysis</td>
</tr>
<tr>
<td></td>
<td>• Use <em>Clip Management</em> to view a summary of motion events for recorded video.</td>
<td></td>
</tr>
</tbody>
</table>

**Tip** See “Controlling Video Playback” for instructions to control playback of live or recorded video.

**Video Viewing Applications**

Live and recorded Cisco Video Surveillance video can be viewed, recorded and managed using the following Cisco-provided applications (Table 3).

**Tip** Third-party integrators can also create custom monitoring applications. See your Cisco support representative for more information.
### Table 3  Summary of Cisco Video Viewing Options

<table>
<thead>
<tr>
<th>Viewing Tool</th>
<th>Application</th>
<th>Description</th>
<th>Documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desktop monitoring application</td>
<td>Cisco Video Surveillance Safety and Security Desktop (Cisco SASD)</td>
<td>• Allows simultaneous viewing of up to 16 cameras.</td>
<td>• Cisco Video Surveillance Safety and Security Desktop User Guide</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Create Video Matrix windows for display in separate monitors.</td>
<td>• “Understanding the Cisco SASD Application Suite”</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• View Video Walls.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Create unattended workstations.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• View and manage alerts.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• View cameras, video, and alerts based on a graphical map.</td>
<td></td>
</tr>
<tr>
<td>Web-based configuration and monitoring</td>
<td>Cisco Video Surveillance Operations Manager (Operations Manager)</td>
<td>• Allows simultaneous viewing of multiple video panes:</td>
<td>Cisco Video Surveillance Operations Manager User Guide</td>
</tr>
<tr>
<td>tool</td>
<td></td>
<td>– View up to 4 cameras with the 32-bit version of Internet Explorer.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>– View up to 16 cameras with the 64-bit version of Internet Explorer.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Add the users, Views and Video Walls available in the desktop Cisco SASD</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>application.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Configure the camera, streams and recording schedules.</td>
<td></td>
</tr>
<tr>
<td>Desktop video clip player</td>
<td>Cisco Video Surveillance Review Player (Cisco Review Player)</td>
<td>Simple player used to view video clip files.</td>
<td>Cisco Video Surveillance Review Player</td>
</tr>
<tr>
<td>Web-based server console</td>
<td>Cisco Video Surveillance Management Console (Cisco VSM Management Console)</td>
<td>Provides basic viewing features for a single stream (Stream A) from a single</td>
<td>Cisco Video Surveillance Management Console Administration Guide</td>
</tr>
<tr>
<td></td>
<td></td>
<td>camera.</td>
<td></td>
</tr>
</tbody>
</table>
# Requirements

Cisco Video Surveillance Safety and Security Desktop (Cisco SASD) requires the following.

## Table 4  Cisco SASD Requirements

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Requirement Complete?</th>
</tr>
</thead>
<tbody>
<tr>
<td>At least one Cisco VSM server must be installed on the network with the following services enabled:</td>
<td>(✓)</td>
</tr>
<tr>
<td>- Cisco Media Server</td>
<td></td>
</tr>
<tr>
<td>- Cisco VSM Operations Manager</td>
<td></td>
</tr>
<tr>
<td>Additional services are required to enable features such as the location maps and Video Motion Search.</td>
<td></td>
</tr>
<tr>
<td>See the following documentation for more information:</td>
<td></td>
</tr>
<tr>
<td>- Cisco Video Surveillance Management Console Administration Guide—enable the Operations Manager service.</td>
<td></td>
</tr>
<tr>
<td>At least one camera physically installed and configured on Cisco VSM Operations Manager.</td>
<td>(✓)</td>
</tr>
<tr>
<td>The IP address or hostname of the Cisco Video Surveillance system (same as the Operations Manager).</td>
<td>(✓)</td>
</tr>
<tr>
<td>A valid Cisco Video Surveillance username and password.</td>
<td>(✓)</td>
</tr>
<tr>
<td>See the Cisco Video Surveillance Operations Manager User Guide for instructions to configure users and access permissions.</td>
<td>(✓)</td>
</tr>
</tbody>
</table>

### Workstation Requirements:

See the Cisco Video Surveillance Monitoring Workstation Performance Baseline Specification for detailed requirements. The basic requirements are:

- A PC or laptop running Windows 7 64-bit operating system.
- A standard Windows 7 user account.

**Note**  Logging in with a Guest account can prevent video streaming and result in an error to be displayed in the video pane: “Cannot create RTSP connection to server. Check network connection and server health status.”

Cisco Multi-Pane Video Surveillance client software, an Active X client that enables video playback and other features.  

**Note**  You will be prompted to install this utility when installing or updating the Cisco SASD application. Complete the on-screen instructions, if prompted. You must have administrative privileges on the PC workstation to install the software.
Installing the Application Suite

Complete the following procedure to install all Cisco SASD applications described in the “Understanding the Cisco SASD Application Suite” section on page 2.

Procedure

**Step 1** Verify that the system and workstation requirements are met, as described in the “Requirements” section on page 8.

**Step 2** Install the Microsoft .NET Framework 4.0, if necessary.


**Step 3** Log in to the Cisco VSM browser-based Operations Manager.

a. Launch the 32-bit or 64-bit version of Internet Explorer 8 on your Windows 7 computer.

b. Enter the URL for the Cisco VSM Operations Manager.

c. Enter your username and password.

d. From the Domain menu, choose the default “localhost” if your account was created using the Operations Manager. Select a different Domain only if you are a user from an external database (Active Directory LDAP domain) and are instructed to do so by your system administrator.

e. Enter a new password if prompted.

*Note* You must enter a new username the first time you log in, or when your password periodically expires.

**Step 4** Select the Operations tab (Figure 2).

**Figure 2** Installing the Cisco SASD using the Operations Manager

**Step 5** Click **Safety and Security Desktop** (under the **Software** heading).

**Step 6** Follow the onscreen instructions to complete the installation.
**Step 7** Complete the on-screen instructions to install or upgrade the Cisco Multi-Pane Video Surveillance client software on your computer. This application is an Active X client that enables video playback and other features. Video will not play unless the Cisco Multi-Pane client software is correctly installed. You must have administrative privileges on the PC workstation to install the software.

**Tip**

- To access the application on your workstation, double-click the Safety And Security Desktop icons on your desktop, or go to Start > All Programs > Cisco Safety And Security Desktop.
- You can save the installer file and use it to install the application on multiple workstations, if necessary. Users must have a valid Cisco VSM username and password to access the system.
- An error appears if the Microsoft .NET Framework 4.0 is not installed. Go to http://www.microsoft.com/en-us/download/confirmation.aspx?id=17851 to download the installer, then repeat this procedure.
Logging In

Log in to the Cisco SASD application using the username and password supplied by your administrator.

Note

- The first time you log in, you must use the browser-based Cisco VSM Operations Manager to change your password (you will be prompted to change a new password on first login).
- Users are configured using the Operations Manager.
- You must log in with a standard Windows 7 user account. Logging in with a Guest account can prevent video streaming and result in an error to be displayed in the video pane: “Cannot create RTSP connection to server. Check network connection and server health status.”

Procedure

Step 1 (First log in only) Log in to the browser-based Operations Manager and change your initial password.

a. Launch the Internet Explorer web browser on your PC and enter the IP address or hostname of the Operations Manager server.

b. Enter your username and password (provided by your system administrator).

c. Complete the form to enter a new password.

d. Log out of the Operations Manager.

Step 2 Launch the Cisco SASD application:

- Double-click the Safety And Security Desktop shortcut on your desktop, or select Start Menu > Programs > Cisco Safety And Security Desktop.

Note Select one of the applications described in “Understanding the Cisco SASD Application Suite”.

Step 3 Enter the login information (Figure 4):

- **Server**—The IP address or hostname of the Cisco VSM Operations Manager.
- **Domain**—Select “localhost” if your account was created using Cisco VSM, or select another option if logging in from an external database (Active Directory LDAP domain).
- **Username**—Enter the username provided by your system administrator.
- **Password**—Enter the password you selected using the browser-based Operations Manager (see Step 1).
Logging In

Getting Started

Figure 3  Login to Cisco SASD

Note

- The first time you log in, you must use the browser-based Cisco VSM Operations Manager to change your password (you will be prompted to change a new password on first login).
- You must log in with a standard Windows 7 user account. Logging in with a Guest account can prevent video streaming and result in an error to be displayed in the video pane: “Cannot create RTSP connection to server. Check network connection and server health status.”
Step 4  Select a Site, if prompted (Figure 4).

Figure 4  Selecting a Site on First Login

- Users with Site access are prompted to select a Site. Users with no Site access are not prompted for a Site.
- To change your Site, you must log out and log back in.
- See “Understanding Sites” for more information.
Step 5 If prompted, ask your manager or other administrator to enter their “Approver Login” (Figure 5).

Figure 5 Approver Login

- This second login is required only if configured.
- See the “Understanding Login Approval” section on page 16 for more information.
- If the approval is not successfully submitted within the time-out period, the login is denied.

Understanding Sites

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

If the Site is configured for Dynamic Proxy, users inside the Site are served by the Media Server in that Site (when accessing cameras inside the Site). Users outside the Site will receive video from a Dynamic Proxy server when accessing any camera inside the Site. See the Cisco Video Surveillance Operations Manager User Guide for more information.

If the system is configured with Sites, and you are a member of a User Group that is assigned to a Site location, you will be prompted to select a Site when you log in (Figure 6).
Users with Site access are prompted for a Site. Users with no Site access are not prompted for a Site.

Users who do not select a Site, are not assigned a Site, or select Not in Any Site will receive video from a Dynamic Proxy server for cameras in any Site where Dynamic Proxy is enabled.

To change your Site, or log in to “Lot In Any Site”, log out of Cisco SASD and log back in.
Understanding Login Approval

“Dual Login” requires that a second user (such as a manager) approve a user’s access by entering their credentials. When the user logs in, a second prompt appears for the manager’s credentials (Figure 7). This optional feature appears every time the user logs in.

![Login Approval](figure7.png)

To enable Dual Login for a user, the Cisco Video Surveillance Operations Manager User Guide.

Default User Accounts and Passwords

Cisco SASD includes two default users: the super-admin account and an operator account.

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

Log in to the browser-based Cisco VSM Operations Manager and click on your username to change your password (Figure 8).

Procedure

**Step 1**
Launch the Internet Explorer (IE) web browser.

**Step 2**
Enter the same IP address/hostname used to access Cisco SASD.

**Step 3**
Enter the same username and password used to access Cisco SASD.

**Step 4**
Click your username in the upper right corner of the Cisco VSM Operations Manager.

**Step 5**
Enter and reenter your new password.

*Figure 8 Changing Your Password Using Operations Manager*
Video Workspace

Use the Video workspace to monitor video from one or more cameras based on the camera location or camera name. You can also monitor multiple cameras in a grid layout.

Refer to the following topics for more information.

Contents
- Overview, page 20
- Viewing Camera Video in a Multi-Pane Grid, page 22
- Displaying a Duplicate Workspace on a Separate Monitor, page 24

Note
If more than 48 panes are displayed, SASD performance can be poor and, in unusual cases, can crash. We recommend displaying less than 48 video panes on a single workstation. If additional panes are required, use an additional monitoring workstation.
Overview

To view video from one or more selected cameras, select the Video workspace (Figure 1).

Figure 1  Overview of the Video Workspace

1  Forensic Analysis
   - **Thumbnail Search**—Use Thumbnail Search to quickly locate specific scenes or events in recorded video without fast-forwarding or rewinding. Thumbnail Search displays a range of video as thumbnail images, allowing you to identify a portion of the recording to review.
   - **Clip Management**—Use Clip Management to view, download and delete MP4 clips that are stored on the server.
   - **Motion Analysis**—Use Motion Analysis to view a summary of motion events for recorded video.

2  The video monitoring “workspace” Use the location tree to select a camera. Select a View to view multiple cameras in a grid.
   Tip  Click ▼ to create a duplicate workspace window that can be dragged to a separate monitor. See “Displaying a Duplicate Workspace on a Separate Monitor”.

3  Click the triangle ▼ to display or hide the side panel.

4  Search—Enter the full or partial name of a camera to display matching camera names.

5  Locations—Select a location to display only the cameras for that location (cameras from sub-locations are not displayed).

6  The cameras for the selected location or search.

7  Playback Controls—See “Controlling Video Playback”.
**Overview**

<table>
<thead>
<tr>
<th>Step</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>Viewing Pane and control icons—See “Controlling Video Playback”.</td>
</tr>
</tbody>
</table>
| 9    | **Layouts**—Create a blank matrix from the available layouts and drag cameras onto each viewing pane.  
  **Select View**—Select a pre-defined matrix of cameras. The cameras can be configured to automatically rotate.  
  See “Viewing Camera Video in a Multi-Pane Grid”. |
| 10   | Notifications—Notify errors, such as exceptions from VSOM BE calls, or software exceptions. |
| 11   | Performance Meter—Displays the workstation’s CPU performance based on available memory and bandwidth.  
  - Green indicates that the workstation is meeting the demands of the Cisco SASD activities.  
  - Yellow is a performance warning.  
  - Red indicates that the workstation performance is poor and processing delays may occur.  
  Tip Hover your mouse over the meter network and memory usage details. |

**Procedure**

| Step 1 | Select the **Video** workspace. |
| Step 2 | Select a blank **Layout** or click **Select View** to select a pre-defined layout and set of cameras. |
| Step 3 | (Optional) Select a video source (camera) for each pane:  
  a. Search for a camera name or select a location.  
  b. Drag-and-drop camera names onto the available viewing panes (you can also highlight a pane and double-click the camera name). |
| Step 4 | Use the video playback controls as described in “Controlling Video Playback”. |
| Step 5 | (Optional) Double-click a video pane to fill the Cisco SASD viewing area with that video. A preview of the other video panes is shown in a smaller grid at the bottom of the screen. Double-click the video pane again to return the grid to normal size.  
  **Tip** To fill the screen, right-click the image and select **Full screen mode**. |
| Step 6 | Click 🗞️ to create a duplicate workspace window that can be dragged to a separate monitor. See “Displaying a Duplicate Workspace on a Separate Monitor”. |


Viewing Camera Video in a Multi-Pane Grid

Use the Video or Wall workspace to view video in a grid.

Procedure

Step 1  Select the Video or Wall workspace.

Step 2  Select a blank Layout or pre-defined View (Figure 2).

Step 3  Drag cameras onto the available panes to change the video source.

Figure 2  Views Menu in the Camera Centric Workspace

- See “Displaying a Duplicate Workspace on a Separate Monitor” to create a separate window of video panes.
- See “Wall Workspace” to use pre-defined video grids that are displayed on multiple workstations.
- See “Using the Cisco SASD Wall Configurator” for instructions to create an “unattended workstation” used to monitor video without a mouse, keyboard, or other user input.
Note
Unattended video walls are backed by the SASD Monitor windows service. If a wall is closed or stop streaming, it will be bring up automatically. However, this feature is only possible if the PC is rebooted. SASD walls will not be backed up if user log off then log in.

Note
If more than 48 panes are displayed, SASD performance can be poor and, in unusual cases, can crash. We recommend displaying less than 48 video panes on a single workstation. If additional panes are required, use an additional monitoring workstation.
Displaying a Duplicate Workspace on a Separate Monitor

A duplicate workspace is an additional window that does not include menus or links to other workspaces. Duplicate workspaces maximize the video viewing area and can be dragged to another screen to monitor multiple workspaces or video grids at a single time.

You can create a duplicate of any workspace (Video, Wall, Alerts or Maps) available in your monitoring application.

To create a duplicate workspace, click the duplicate icon (Figure 3). You can then select a layout, view, map or alert to view video, and drag the window to another monitor, if necessary.

Figure 3 Creating a Duplicate Workspace

- Closing the Cisco SASD or Cisco SASD Advanced Video Player window also closes the duplicate workspace windows. Logging out of the application also closes all windows.
- To maximize the video screens, move the new workspace to a separate monitor and double-click a pane to fill the entire browser window. To fill the entire monitor screen, right-click the image and select Full screen mode.
- See “Controlling Video Playback” for more information.
Wall Workspace

Video Walls are pre-defined Views that can be displayed on multiple workstations or viewed by unattended workstations.

Refer to the following topics for more information.

Contents
- Overview, page 25
- Usage Notes, page 27
- Viewing and Publishing Video Walls, page 27

Overview

Video Walls are pre-defined Views that can be displayed on multiple workstations (Figure 1). All workstations that display the Video Wall will display the same set of pre-defined panes. Walls can be modified and “published” to the other workstations viewing the wall, and used as unattended workstations that can be monitored without user input or control.

For example, a “Lobby Door” Video Wall includes cameras in buildings 1 through 4. Each workstation that selects the “Lobby Door” Wall will display the same set of cameras. If an attendant at one workstation changes the camera for a pane, they can click Publish To Wall to display the modified scene on all other workstations that display that Wall.

Tip
Walls can also be displayed on unattended workstations using the Cisco SASD Wall Launcher. See “Using the Cisco SASD Wall Configurator” for more information.

Note
The operator must have access permissions to use the Wall feature.
Figure 1 describes the main features of the Wall workspace.

**Figure 1  Video Walls**

1. The Wall Workspace.  
   **Tip** Click to create a duplicate workspace window that can be dragged to a separate monitor. This allows you to view multiple Walls at the same time. See “Displaying a Duplicate Workspace on a Separate Monitor” for more information.

2. The selected Wall.

3. The video panes displayed by the selected Wall.  
   **Tip** Drag and drop cameras onto the video panes to change the displayed video. Click **Publish To Wall** to display the modified Wall on all workstations that are viewing the Wall (the Wall reverts to the default view after the rollback time defined in the Operations Manager).

4. **Publish To Wall**—Click to display a View or modified Wall on all other workstations and monitors that are viewing the Wall. See “Using the Cisco SASD Wall Configurator” for more information.
Usage Notes

- Video Walls are configured by system administrators using the Cisco Video Surveillance Operations Manager browser-based administration tool. See the Cisco Video Surveillance Operations Manager User Guide for more information.

- Video Walls can display a populated View or a blank matrix.

- See “Using the Cisco SASD Wall Configurator” for instructions to set up a workstation for viewing only. Unattended workstations can be operated without a mouse, keyboard, or other user input.

- If more than 48 panes are displayed, SASD performance can be poor and, in unusual cases, can crash. We recommend displaying less than 48 video panes on a single workstation. If additional panes are required, use an additional monitoring workstation.

Viewing and Publishing Video Walls

Procedure
To view, modify or publish a Video Wall, do the following:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Select the <strong>Wall</strong> workspace tab.</td>
</tr>
<tr>
<td>Step 2</td>
<td>(Optional) Click ![image] to create a duplicate workspace window that can be dragged to a separate monitor. See “Displaying a Duplicate Workspace on a Separate Monitor”.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click <strong>Select Wall</strong> and choose a Wall from the list (Figure 1).</td>
</tr>
</tbody>
</table>
| Step 4 | (Optional) Change the displayed video:  
  - Drag cameras onto the available panes.  
  - Select a different View. |

**Note** When a pane is updated, all panes in the Video Wall will refresh, which can cause a loss of video for a few seconds.

| Step 5 | (Optional) Display a different View on all instances of the selected Video Wall (such as other workstations that display the same Video Wall).  
  a. Change the displayed video.  
  b. Click **Publish to Wall**. |

**Tip**  
- The Wall reverts to the default view after the rollback time defined in the Operations Manager.  
- The **Publish to Wall** option is enabled only when you change the video displayed in the video panes.  
- You must have access permissions for **Publish to Wall**. See your system administrator for more information.
Cisco SASD Wall Configurator Overview

The Cisco SASD Wall Configurator defines the Video Walls that will appear on unattended workstations. An unattended workstation is a PC that is used to monitor Video Walls without user input or interaction. Unattended workstations can be operated without a mouse or keyboard, and do not have access to the Cisco SASD or Cisco SASD Advanced Video Player interface.

For example:

- Once the unattended workstation is configured, you can exit all other Cisco SASD applications (such as the Cisco SASD Wall Configurator or Cisco SASD Advanced Video Player). The unattended screens remain open and will (optionally) re-appear when the workstation is rebooted.
- If the keyboard and mouse are removed, the operator can view video, but cannot interact with the video playback. The workstation can also be placed out of reach (such as below a desk or in a cabinet).
- If the keyboard and mouse remain connected, the operator can interact with the video, and close and reopen the unattended screens (using the Cisco SASD Wall Launcher).
- You can create multiple unattended windows for display on different monitors. For example, one monitor can display a Video Wall of all Lobby Doors, and a second monitor can display a Video Wall that rotates the panes among all side entrances.
- Unattended mode can be set to launch automatically when the workstation is rebooted (it does not re-launch when a user logs off and logs back on). You can also use the Cisco SASD Wall Launcher (installed on the desktop) to relaunch the unattended screens (the Launcher closes any open unattended windows, and re-launches the unattended Video Wall windows configured on the PC).
If an unattended Video Wall is shutdown (for example, the application crashes or is closed), or if all panes in the wall are not streaming video, the unattended Video Wall will re-start automatically.

If the workstation is rebooted, the same unattended windows will automatically reappear on the monitor(s) in the same position (if configured).

Unattended video walls are backed by SASD Monitor windows service. If a wall is closed or stop streaming, it will be bring up automatically. However, this feature is only possible if the PC is rebooted, not log off then log in.

Figure 1 describes the main features of the Cisco SASD Wall Configurator.

**Figure 1**  Using Cisco SASD Wall Configurator to Define “Unattended” Video Walls

1. **Add**—Click to add a Video Wall that will appear on the workstation in “unattended mode”, and then select the “Wall Name”.
   - Video Walls are configured using the Operations Manager.
   - The Video Walls will appear when you save and exit the Cisco SASD Wall Configurator, when you launch the Cisco SASD Wall Launcher, or (optionally) when you restart the workstation.

2. **Launch on Startup**—
   - Select to automatically launch the Walls in unattended mode when the workstation is restarted.
   - Deselect to manually launch the unattended walls using the Cisco SASD Wall Launcher.

3. **Wall Name**—Select the Video Wall(s) that will appear when the workstation is restarted or when Cisco SASD Wall Launcher is launched.
   - Note  The Video Walls are configured using the Operations Manager.

4. **Window State**—Defines the size and location of the Video Wall when the workstation is restarted or when Cisco SASD Wall Launcher is launched.
   - **Normal**—The Video Wall window appears in the size and location defined using the Cisco SASD Wall Configurator.
   - **Minimized**—The Video Wall window is minimized on the monitor.
   - **Maximized**—The Video Wall window fills the entire screen.
Chapter Using the Cisco SASD Wall Configurator

Requirements

The following are required to use the Cisco SASD Wall Configurator to configure unattended workstations:

Table 1 Requirements

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Requirement Complete?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrative user privileges on the Windows workstation.</td>
<td>☐</td>
</tr>
<tr>
<td>An admin account in Cisco Video Surveillance.</td>
<td>☐</td>
</tr>
<tr>
<td>You must belong to a Cisco VSM User Group with access permissions for Video Walls.</td>
<td>☐</td>
</tr>
<tr>
<td>At least one Video Wall must be configured on the system (using the Operations Manager interface).</td>
<td>☐</td>
</tr>
<tr>
<td>Video Walls cannot be configured by users who are in a user group with access to multiple Sites. Only users with access to a single Site (and who are not prompted to select a Site) can configure Video Walls.</td>
<td>☐</td>
</tr>
<tr>
<td>• See the “Understanding Sites” for more information.</td>
<td></td>
</tr>
<tr>
<td>• See the Cisco Video Surveillance Operations Manager User Guide for information about creating and assigning Site access.</td>
<td></td>
</tr>
<tr>
<td>All Video Walls used in unattended mode should be configured with a Default View in the Operations Manager. If a Video Wall without a Default View is selected, all video panes will be blank.</td>
<td>☐</td>
</tr>
<tr>
<td>If all video panes are blank (no camera was selected as a video source in the Operations Manager), then the unattended window will be repeatedly re-start since video streaming is not available</td>
<td>☐</td>
</tr>
</tbody>
</table>

Note

Video Walls are configured using the browser-based Operations Manager. See your system administrator or the Cisco Video Surveillance Operations Manager User Guide for more information.
Usage Notes

- If more than 48 panes are displayed, SASD performance can be poor and, in unusual cases, can crash. We recommend displaying less than 48 video panes on a single workstation. If additional panes are required, use an additional monitoring workstation.

- If the admin account password is changed on the monitoring workstation, then the unattended windows must be re-configured.

- To change the video displayed in the Video Wall panes (such as changing the camera source), revise the Video Wall configuration using the browser-based Operations Manager (see your system administrator or the Cisco Video Surveillance Operations Manager User Guide for more information). The unattended windows revert to the Video Wall's Default View when the system is rebooted.

- Unattended configuration applies only to a single Cisco Video Surveillance system. If you log into a different Cisco Video Surveillance system on the same workstation, you cannot revise the existing unattended windows.

- Unattended SASD Wall can be changed by remote or local user who is running SASD main app, or SASD ADP, and publish a different view to the wall, or a different camera to a pane.

- The unattended mode will repeatedly restart if video to all panes is lost. This can be caused by network or system issues, or if a Video Wall without a default view is selected. This allows unattended mode to recover when the problem is resolved. For example, if the video streams for all panes are provided by a single Media Server, and that Media Server goes down, then the unattended mode will restart until communication with the server is reestablished. If the Media Server fails over to another server, then the new server will provide video streaming and the video will be displayed.

- If the video stream is lost for one (but not all) of the video panes, unattended mode will not restart and the pane will display an error message and icon. The video will automatically re-appear only if the video is in unattended mode and the camera is enabled for failover.

Configuring Unattended Workstations

Use Cisco SASD Wall Configurator to select the Video Walls that will be displayed in unattended mode on a workstation.

Once the unattended windows are defined, you can close the Cisco SASD Wall Configurator application. The unattended windows will be automatically re-launched.

Procedure

**Step 1**
Before you begin, create one or more Video Walls.

a. Log on to the Operations Manager.
   - You must belong to a User Group with permissions for Video Walls.

b. Create one or more Views.

c. Add one or more Video Walls (System Settings > Video Wall).

**Tip**
See your system administrator or the Cisco Video Surveillance Operations Manager User Guide for more information.
Step 2 Connect a keyboard and mouse to the workstation.

Step 3 Launch Cisco SASD Wall Configurator and log in to the application.

Step 4 Click **Add** (Figure 1).

Step 5 Select a Wall name.
- The Video Wall should include a **Default View**. See the “Usage Notes” section on page 32.

Step 6 Select the Window State:
- **Normal**—The Video Wall window appears in the size and location defined using the Cisco SASD Wall Configurator.
- **Minimized**—The Video Wall window is minimized on the monitor.
- **Maximized**—The Video Wall window fills the entire screen.

Step 7 Click to launch (display) the Video Wall.

Step 8 Position the Video Wall window(s) on the workstation monitors.
- The window will re-display in the same position if you selected the Normal window state.

Step 9 Repeat Step 4 through Step 8 to select a Video Wall for each unattended window and position the window on the workstation display(s).

Step 10 Select or deselect **Launch on Startup** to launch unattended mode when the workstation is restarted.

**Tip** If deselected, the unattended windows will not appear when the workstation is restarted. Use the Cisco SASD Wall Launcher to open the unattended windows. See “Launching the Unattended Windows” for more information.

Step 11 Click **Save** to save the configuration.

Step 12 Close the Cisco SASD Wall Configurator window to quit the application and launch the Video Walls in unattended mode.

**Note** If all video panes are blank (no camera was selected as a video source in the Operations Manager), then unattended window will be repeatedly re-start since video streaming is not available (see “Requirements” and “Usage Notes” for more information).

Step 13 (Optional) Move the Video Wall windows to display any unattended mode windows placed directly behind each other, if necessary.

Step 14 (Optional) Remove the keyboard and mouse.
- If the keyboard and mouse are removed, the user can only view video.
- Leave a mouse (and/or keyboard) attached to allow the user to control video playback (see “Controlling Video Playback” for more information).
Launching the Unattended Windows

To display the Video Walls on the workstation in unattended mode, do one of the following:

Table 2  Launch Options

<table>
<thead>
<tr>
<th>Launch Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save and exit the Cisco SASD Wall Configurator</td>
<td>The Video Walls are launched automatically when the Cisco SASD Wall Configurator closes.</td>
</tr>
<tr>
<td>Launch the Cisco SASD Wall Launcher</td>
<td>The Cisco SASD Wall Launcher opens all Video Walls in unattended mode that were added in the Cisco SASD Wall Configurator. The Launcher also closes any open unattended windows, and re-launches the unattended Video Wall windows configured on the PC.</td>
</tr>
<tr>
<td>Restart the workstation</td>
<td>(Optional) If the Launch on Startup option is selected in the Cisco SASD Wall Configurator, the Video Walls will launch in unattended mode when the workstation restarts. See “Usage Notes” section on page 32 for more information.</td>
</tr>
</tbody>
</table>

Related Information
To change the Video Walls that appear in unattended mode, see the following topics:
- “Configuring Unattended Workstations” section on page 32
- “Removing a Video Wall From Unattended Mode” section on page 34

Removing a Video Wall From Unattended Mode

To remove one or all Video Walls from unattended mode, do the following.

Note
The Video Walls will no longer appear when the unattended windows are launched (as described in the “Launching the Unattended Windows” section on page 34).

Step 1  Launch Cisco SASD Wall Configurator and log in to the application.
Step 2  Click Delete to remove a Video Wall from unattended mode.
Step 3  Click Save.
Step 4  Close the Cisco SASD Wall Configurator application.
Understanding Offline Mode

Offline mode allows unattended screens to continue to display video if the network connection to Operations Manager is lost, but the connection to the cameras’ Media Servers is still available. This can occur due to a network failure, or when the Operations Manager used to configure the system is located at a remote location.

Note

If the window is in Offline mode, changes by another user to the Video Wall or View not updated until the window returns to Online mode.

“Offline” appears in the window title bar when the unattended window is operating in offline mode.

- If the network connection to the Operations Manager is lost, the unattended windows will relaunch in offline mode.
- If the Operations Manager is unavailable when the unattended windows launch, the unattended windows will restart in offline mode.

Transition Times

The Unattended windows periodically check for Operations Manager connectivity, and automatically switch between online and offline mode, if necessary. The system performs this check periodically to avoid switching back and forth if a intermittent network issue occurs (such as a jitter).

Table 4-3  Online/Offline Transition Times

<table>
<thead>
<tr>
<th>Transition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online to Offline</td>
<td>If the Operations Manager connection is lost for 4 minutes, the unattended windows will switch to Offline mode.</td>
</tr>
<tr>
<td>Offline to Online</td>
<td>If the Operations Manager connection is restored for 12 minutes, the unattended windows will switch to Online mode.</td>
</tr>
</tbody>
</table>
Alert Workspace

Select the Alert Workspace (Figure 2) to view health and security alerts, and take one or more of the following actions:

- Acknowledge, close, or re-open alerts
- Add a comment, or flag the alert as a false alarm.
- View recorded video related to an event (if available).
- View live or recorded video from a camera shown on a location map.
- Send alerts to the Cisco SASD Federator.

Note
The Alert Workspace is available in the Cisco SASD and Cisco SASD Federator applications only. Alerts are not included in the Cisco SASD Advanced Video Player.

Contents
Refer to the following topics for more information:

- Understanding Events and Alerts, page 38
- Alert Workspace Overview, page 39
- Dynamic Updates of Alert Results, page 42
- Viewing Event URLs, page 43
- Common Tasks, page 44
- Impact of Device Location Changes on Alerts, page 44
- Summary of Events and Corresponding Alerts, page 46
Understanding Events and Alerts

Events represent incidents that occur in the system and in devices (such as cameras or camera encoders). Events are aggregated (grouped) into alerts for notification purposes. For example, if a camera goes offline and comes back online repeatedly, all events for that issue are grouped under a single alert, which triggers a single notification. This prevents operators from being flooded with notifications for multiple occurrences of the same issue.

Cisco VSM generates two types of events:

- **Health Events** are generated when a device health change occurs, such as reachability, fan speed, file system usage, or other device-related issues. Critical health events generate alerts by default.

- **Security Events**—Events such as motion stop or start, analytics, contact closures, or soft triggers from an external system can be configured to generate alerts, or perform other actions (security events do not generate alerts by default). Security alerts can also be forwarded to the Federator (if installed).

Figure 1 summarizes how Cisco VSM events and alerts are generated, aggregated, and viewed.
When a camera is configured for stream redundancy (for example, stream 1 to the primary Cisco Media Server and stream 2 to a redundant server), events from both streams are added to the same alert.

Alert Workspace Overview

Select the Alert Workspace (Figure 2) to view alerts and events related to that alert. You can also take numerous action depending on the alert or event type. For example:

- Right-click an alert to acknowledge, close, re-open, or comment on the alert.
- Double-click an event or camera icon to view live or recorded video (if available).
The Alert Workspace is available in the Cisco SASD and Cisco SASD Federator applications only. Alerts are not included in the Cisco SASD Advanced Video Player.

Click to create a duplicate workspace window that can be dragged to a separate monitor. See “Displaying a Duplicate Workspace on a Separate Monitor”.

---

**Figure 2**  Alert Workspace

1. Alert Workspace tab.
2. Dynamic filter
3. Location
4. Time
5. Alert type
6. Acknowledged by
7. Closed by
8. Events
9. Alerts
10. Search
11. Actions
2 **Search**—Display alerts in a static list based on the filter criteria (including a time span). The alerts already displayed on the search result table are auto updated if their status changes. However, the search result table itself is not auto refreshed (new alerts are not inserted, the table is auto re-sorted etc.). Re-search the alerts to view current results.

**Dynamic Filter**—Display alerts in a auto-updating list based on the filter criteria (such as location, alert type and severity). Click the lock icon to stop or start auto-updates

- When unlocked, new alerts will be added to the list as they occur.
- When locked, dynamic updating is paused and only the currently displayed alerts are shown. Unlock the display to refresh the results.

3 Click the triangle to display or hide the side panel.

4 Filter criteria. Select the criteria described below and click **Apply**.

<table>
<thead>
<tr>
<th>Tip</th>
<th>If a filter criteria is not selected, the all alerts for that filter are displayed.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Location</strong>—Click to select a specific location where the alert(s) were created. Only alerts from that location will be displayed.</td>
</tr>
<tr>
<td></td>
<td><strong>Device</strong>—Click to select a location and a specific device (camera). Only alerts from that device will be displayed.</td>
</tr>
<tr>
<td></td>
<td><strong>Time</strong>—(Search only). Select a span of time. Only alerts that were generated during that time are displayed. For example, Today or Month.</td>
</tr>
<tr>
<td></td>
<td><strong>Alert Type</strong>—Health or Security. See the “Understanding Events and Alerts” section on page 38 for more information.</td>
</tr>
<tr>
<td></td>
<td><strong>Severity</strong>—Select CRITICAL, MAJOR, MINOR, WARNING, or INFO.</td>
</tr>
</tbody>
</table>

**Note** The alert severity reflects the severity of the most recently generated event. For example, if a camera becomes unreachable and the streaming status is Critical, the alert is Critical. When the camera becomes reachable again, and the streaming status normal event occurs, and the alert severity is changed to INFO. See the “Summary of Events and Corresponding Alerts” section on page 46 for the severity of each event.

**Note** INFO requests also display CRITICAL alerts.

- **Status**—Acknowledged, Closed or New.
- **Acknowledged By**—Enter the full or partial name of the user who acknowledged the alert.
- **Closed By**—Enter the full or partial name of the user who acknowledged the alert.

5 Select an alert to view the events related to that alert.

Right-click an alert to take the following actions:

- Change the alert status (acknowledge, close or re-open the alert).
- Add a comment to the alert or mark it as a false alarm.
- Send the alert to the Cisco VSM Federator (see “Monitoring Alerts Using the Cisco SASD Federator” for more information).

6 Events associated with the alert (multiple events for the same issue are grouped under a single alarm).

7 If the URL icon appears, right-click the event to open a new web browser window with additional information or images.

See the “Viewing Event URLs” section on page 43.
Click the column headers to sort the displayed alerts.

- Only headings with an arrow are sortable.
  - The Time column sorts alerts with the newest alert at the top.
  - The Severity column sorts alerts with the most severe alert at the top (in the order of CRITICAL, MAJOR, MINOR, WARNING, INFO).

Select the number of items that are displayed on a page, or navigate through the available pages.

The camera icon appears if video is available for the event. Double-click the event to open a 2-pane pop-up playback window. The left pane displays live video, the right pane displays the recorded video (starting from the event trigger point). This popup window can be enlarged and dragged to another monitor for better viewing.

If video is not available (for example, if the video was automatically deleted after the duration defined by the camera retention rules), an error message appears when attempting to view the video.

Video is available for the following event types:

- Motion start/stop
- Contact closure open/close
- Soft trigger
- Analytics

Select the orientation of the results:

- Display the alerts and events results side-by-side.
- Display the alerts above the events.

Dynamic Updates of Alert Results

By default, new alerts are dynamically added to the Dynamic Filter results as they occur. New alerts will appear at the top of the list if the results are sorted by time, or in the middle of the list if the results are sorted by severity.

Click the lock icon to stop or start auto-updates

The Search tab results do not dynamically refresh. The alerts displayed remain static unless you perform another search.
Viewing Event URLs

Alerts can also include a custom URL. Right-click the event and select the URL to open a window with additional information, such as a web page, image snapshot, or video clip (Figure 3).

Figure 3 Selecting a Soft Trigger Event URL in the Cisco SASD Monitoring Application

1. Select a soft-trigger alert that was customized to include an additional URL.
2. Right-click the URL icon for the event.
3. Select the URL.
4. View the information, image or video in the pop-up window.
Common Tasks

Table 1 describes common tasks that are performed with alerts.

Table 1  Common Alert Tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Narrow the list of displayed alerts</td>
<td>Click the tabs at the top of the alert list to filter the displayed alerts:</td>
</tr>
<tr>
<td></td>
<td>• Search— keywords</td>
</tr>
<tr>
<td></td>
<td>• Dynamic Filter (narrow the results based on alert type, status, or severity,</td>
</tr>
<tr>
<td></td>
<td>• time, location, and/or device).</td>
</tr>
<tr>
<td></td>
<td><strong>Tip</strong> Any filter criteria that is not selected will return all alerts for</td>
</tr>
<tr>
<td></td>
<td>that filter.</td>
</tr>
<tr>
<td>Display the events associated with the</td>
<td>Select an alert to view the associated events.</td>
</tr>
<tr>
<td>alert</td>
<td></td>
</tr>
<tr>
<td>Acknowledge the alert</td>
<td>Right-click an alert and select <strong>Acknowledge</strong>.</td>
</tr>
<tr>
<td>Close, re-open, or flag the alert as a</td>
<td>Right-click an alert and select an option.</td>
</tr>
<tr>
<td>false alarm</td>
<td>• When an alert is closed, no new events can be added (unless the alert is</td>
</tr>
<tr>
<td></td>
<td>• reopened by a user). Any new events for the same device and issue are</td>
</tr>
<tr>
<td></td>
<td>• added to a new alert entry.</td>
</tr>
<tr>
<td></td>
<td>• Users can still modify closed alerts, including the following:</td>
</tr>
<tr>
<td></td>
<td>• Add a comment (the alert state is not changed).</td>
</tr>
<tr>
<td></td>
<td>• Re-open the alert. New events for that device and issue will be added</td>
</tr>
<tr>
<td></td>
<td>to the alert.</td>
</tr>
<tr>
<td>Add a comment</td>
<td>Right-click an alert and select <strong>Comment</strong>. Add the comment and click <strong>Apply</strong>.</td>
</tr>
<tr>
<td>View event video (motion and analytics</td>
<td>The camera icon 📹 appears if video is available for the event. Double-click</td>
</tr>
<tr>
<td>alerts only)</td>
<td>the event to open a playback window.</td>
</tr>
<tr>
<td>View alerts on a larger location map</td>
<td>Open the Map Workspace. See the &quot;Map Workspace&quot; for more information.</td>
</tr>
</tbody>
</table>

Impact of Device Location Changes on Alerts

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

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

For example:

1. Events are added to Alert 1 at the original *Location 1*:
   
   Alert 1  Location 1  Device 1
   Event 99  Location1  device1
   Event 98  Location1  device1
   Etc.
2. The device location is changed to *Location 2*.

3. New events generated for an existing (and open) Alert 1 are added to the alert using the new *Location 2*, but the alert is still associated with the original *Location 1*.

<table>
<thead>
<tr>
<th>Alert</th>
<th>Location</th>
<th>Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event 101</td>
<td>Location2</td>
<td>device1</td>
</tr>
<tr>
<td>Event 100</td>
<td>Location2</td>
<td>device1</td>
</tr>
<tr>
<td>Event 99</td>
<td>Location1</td>
<td>device1</td>
</tr>
<tr>
<td>Event 98</td>
<td>Location1</td>
<td>device1</td>
</tr>
<tr>
<td>Etc.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

4. An operator closes the alert (by right-clicking on it).

5. New events are associated with a new alert in the new *Location 2* (the location reference in the alert is now consistent with the device location in the event).

<table>
<thead>
<tr>
<th>Alert</th>
<th>Location</th>
<th>Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event 103</td>
<td>Location2</td>
<td>device1</td>
</tr>
<tr>
<td>Event 102</td>
<td>Location2</td>
<td>device1</td>
</tr>
<tr>
<td>Etc.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Summary of Events and Corresponding Alerts

The following table summarizes the events that are included in each Cisco VSM 7.0 alert.

**Note** Some alerts include events of multiple types. For example, the motion alert can include the “motion_start” and “motion_stop” events.

### Table 2 Events Included Under the Cisco VSM Alerts

<table>
<thead>
<tr>
<th>Alerts</th>
<th>Events included in the alert</th>
<th>Severity</th>
<th>Description of the alert per event type</th>
</tr>
</thead>
<tbody>
<tr>
<td>analytics</td>
<td>analyticsOccurred</td>
<td>INFO</td>
<td>Analytics event of type {0} occurred for rule {1}</td>
</tr>
<tr>
<td>auto_discovery</td>
<td>autoDiscovery</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>capability_mismatch_status</td>
<td>capability_mismatch_status</td>
<td>CRITICAL</td>
<td>Configuration defined in the template and the configuration supported by the camera do not match</td>
</tr>
<tr>
<td></td>
<td></td>
<td>INFO</td>
<td>Issue with respect to configuration defined in the template and the configuration supported by the camera has been cleared</td>
</tr>
<tr>
<td>chassis_intrusion</td>
<td>chassisIntrusion</td>
<td>CRITICAL</td>
<td>Chassis Intrusion is critical</td>
</tr>
<tr>
<td></td>
<td></td>
<td>INFO</td>
<td>Chassis Intrusion is normal</td>
</tr>
<tr>
<td>clipping</td>
<td>clip_start</td>
<td>INFO</td>
<td>Clipping initiated - {0}</td>
</tr>
<tr>
<td></td>
<td>clip_completed</td>
<td>INFO</td>
<td>Clipping completed - {0}</td>
</tr>
<tr>
<td></td>
<td>clip_deleted</td>
<td>INFO</td>
<td>Clipping deleted - {0}</td>
</tr>
<tr>
<td></td>
<td>clip_failed</td>
<td>INFO</td>
<td>Clipping failed - {0}</td>
</tr>
<tr>
<td>config_mismatch_status</td>
<td>config_mismatch_status</td>
<td>CRITICAL</td>
<td>Configuration in VSOM is not the same as in Media Server for device {0}</td>
</tr>
<tr>
<td></td>
<td></td>
<td>INFO</td>
<td>Configuration in VSOM same as in Media Server for device {0}</td>
</tr>
<tr>
<td>contact_closure</td>
<td>contact_closure_opened</td>
<td>INFO</td>
<td>Contact closure opened on port {0}</td>
</tr>
<tr>
<td></td>
<td>contact_closure_closed</td>
<td>INFO</td>
<td>Contact closure closed on port {0}</td>
</tr>
<tr>
<td>Event Type</td>
<td>Detailed Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>contact_closure_unconfigured_status</td>
<td>CRITICAL: Camera contact closure is not configured but template defines advanced events with contact-closure. INFO: Clearing contact closure configuration issue with camera and template.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>coredump</td>
<td>CRITICAL: {0} core dump critical.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>device_status</td>
<td>CRITICAL: {0} Streaming status is critical.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>device_connection_status</td>
<td>CRITICAL: {0} Streaming connection loss occurred.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>device_stream_status</td>
<td>CRITICAL: {0} Streaming videoloss.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>driverpack_mismatch_status</td>
<td>CRITICAL: Driver-packs in Media Server does not match with Driver-packs in VSOM.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>encoder_max_streams_used_status</td>
<td>CRITICAL: maximum number of streams reached for encoder.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>event_overload_status</td>
<td>CRITICAL: VSOM dropped {0} events due to a large number of events received.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>fan_speed</td>
<td>CRITICAL: {0} is critical.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>firmware_mismatch_status</td>
<td>CRITICAL: Camera's template firmware does not match the camera's firmware.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>fs_usage</td>
<td>CRITICAL: File system usage on {0} is critical.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>INFO: Clearing contact closure configuration issue with camera and template.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>INFO: {0} Streaming status is normal.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>INFO: {0} Streaming status is normal.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>INFO: {0} Streaming status is normal.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>INFO: {0} Streaming status is normal.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>INFO: Media Server's driver-pack matches Operations Manager's.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>INFO: max_streams_reached issue is resolved.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>INFO: Normal VSOM events processing has resumed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>INFO: Camera's template firmware matches the camera's firmware.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>INFO: File system usage on {0} is normal.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>INFO: File system usage on {0} is normal.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Event Type</td>
<td>Event Description</td>
<td>Status</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
<td>--------------</td>
<td>--------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ha_config_mismatch_status</td>
<td>Configuration in VSOM and primary MS is not the same as in redundant/failover Media Servers {0}</td>
<td>CRITICAL</td>
<td>Configuration in VSOM and primary MS is not the same as in redundant/failover Media Servers {0}</td>
</tr>
<tr>
<td></td>
<td></td>
<td>INFO</td>
<td>Configuration in VSOM and primary MS is same as in redundant/failover Media Servers {0}</td>
</tr>
<tr>
<td>identity_collision_status</td>
<td>Another device with one or more identity criteria exists in the system.</td>
<td>CRITICAL</td>
<td>Identity collision is resolved.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>INFO</td>
<td>Identity collision is resolved.</td>
</tr>
<tr>
<td>insufficient_backup_space_status</td>
<td>Insufficient space is stopping automatic VSOM database backup</td>
<td>CRITICAL</td>
<td>Automatic VSOM database backup is normal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>INFO</td>
<td>Automatic VSOM database backup is normal</td>
</tr>
<tr>
<td>load_average</td>
<td>Load average is critical</td>
<td>CRITICAL</td>
<td>Load average is critical</td>
</tr>
<tr>
<td></td>
<td></td>
<td>INFO</td>
<td>Load average is normal</td>
</tr>
<tr>
<td>mem_free</td>
<td>Memory usage is critical</td>
<td>CRITICAL</td>
<td>Memory usage is critical</td>
</tr>
<tr>
<td></td>
<td></td>
<td>INFO</td>
<td>Memory usage is normal</td>
</tr>
<tr>
<td>motion</td>
<td>Motion started on {0}</td>
<td>INFO</td>
<td>Motion started on {0}</td>
</tr>
<tr>
<td>motion_stop</td>
<td>Motion stopped on {0}</td>
<td>INFO</td>
<td>Motion stopped on {0}</td>
</tr>
<tr>
<td>motion_unconfigured_status</td>
<td>Motion window is not configured on the camera. Record on motion and other actions will not work.</td>
<td>CRITICAL</td>
<td>Motion window is not configured on the camera. Record on motion and other actions will not work.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>INFO</td>
<td>Motion window is configured on the camera.</td>
</tr>
<tr>
<td>nic_usage</td>
<td>{0}'s Nic usage is critical</td>
<td>CRITICAL</td>
<td>{0}'s Nic usage is critical</td>
</tr>
<tr>
<td></td>
<td></td>
<td>INFO</td>
<td>{0}'s Nic usage is normal</td>
</tr>
<tr>
<td>password_expired_status</td>
<td>Password expired - needs a password change</td>
<td>CRITICAL</td>
<td>Password expired - needs a password change</td>
</tr>
<tr>
<td></td>
<td></td>
<td>INFO</td>
<td>Password changed</td>
</tr>
<tr>
<td>power_supply</td>
<td>Power supply is critical</td>
<td>CRITICAL</td>
<td>Power supply is critical</td>
</tr>
<tr>
<td></td>
<td></td>
<td>INFO</td>
<td>Power supply is normal</td>
</tr>
<tr>
<td>raid_status</td>
<td>Virtual drive{0} Raid failure is critical</td>
<td>CRITICAL</td>
<td>Virtual drive{0} Raid failure is critical</td>
</tr>
<tr>
<td></td>
<td></td>
<td>INFO</td>
<td>Virtual drive{0} Raid failure is fixed</td>
</tr>
<tr>
<td>rcd_status</td>
<td>Recording status is critical</td>
<td>CRITICAL</td>
<td>Recording status is critical</td>
</tr>
<tr>
<td></td>
<td></td>
<td>INFO</td>
<td>Recording status is normal</td>
</tr>
<tr>
<td>recording_groomed</td>
<td>Parts of the recording {0} was groomed to free up disk space</td>
<td>INFO</td>
<td>Parts of the recording {0} was groomed to free up disk space</td>
</tr>
<tr>
<td>Event Type</td>
<td>Description</td>
<td>Severity</td>
<td></td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------</td>
<td></td>
</tr>
<tr>
<td>reachability</td>
<td>reachability</td>
<td>CRITICAL</td>
<td></td>
</tr>
<tr>
<td>recorder_oversubscribed</td>
<td>recorder_Oversubscription</td>
<td>CRITICAL</td>
<td></td>
</tr>
<tr>
<td>redundancy_unconfigured_status</td>
<td>redundancy_unconfigured_status</td>
<td>CRITICAL</td>
<td></td>
</tr>
<tr>
<td>server_status</td>
<td>server_status</td>
<td>CRITICAL</td>
<td></td>
</tr>
<tr>
<td>soft-trigger</td>
<td>soft_trigger</td>
<td>INFO</td>
<td></td>
</tr>
<tr>
<td>temperature</td>
<td>temperature</td>
<td>CRITICAL</td>
<td></td>
</tr>
<tr>
<td>time_out_of_sync_status</td>
<td>time_out_of_sync_status</td>
<td>WARN</td>
<td></td>
</tr>
<tr>
<td>ums_config_change</td>
<td>ums_config_change</td>
<td>CRITICAL</td>
<td></td>
</tr>
<tr>
<td>ums_failover_status</td>
<td>ums_failover</td>
<td>WARN</td>
<td></td>
</tr>
<tr>
<td>ums_identity_mismatch_status</td>
<td>ums_identity_mismatch_status</td>
<td>CRITICAL</td>
<td></td>
</tr>
<tr>
<td>ums_version_mismatch_status</td>
<td>ums_version_mismatch_status</td>
<td>CRITICAL</td>
<td></td>
</tr>
<tr>
<td>unknown_hw_sensor</td>
<td>unknown</td>
<td>CRITICAL</td>
<td></td>
</tr>
</tbody>
</table>

**Table 2: Events Included Under the Cisco VSM Alerts (continued)**

<table>
<thead>
<tr>
<th>Event Type</th>
<th>Description</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>reachability</td>
<td>reachability</td>
<td>INFO</td>
</tr>
<tr>
<td>recorder_oversubscribed</td>
<td>recorder_Oversubscription</td>
<td>INFO</td>
</tr>
<tr>
<td>redundancy_unconfigured_status</td>
<td>redundancy_unconfigured_status</td>
<td>INFO</td>
</tr>
<tr>
<td>server_status</td>
<td>server_status</td>
<td>INFO</td>
</tr>
<tr>
<td>soft-trigger</td>
<td>soft_trigger</td>
<td>INFO</td>
</tr>
<tr>
<td>temperature</td>
<td>temperature</td>
<td>INFO</td>
</tr>
<tr>
<td>time_out_of_sync_status</td>
<td>time_out_of_sync_status</td>
<td>INFO</td>
</tr>
<tr>
<td>ums_config_change</td>
<td>ums_config_change</td>
<td>INFO</td>
</tr>
<tr>
<td>ums_failover_status</td>
<td>ums_failover</td>
<td>INFO</td>
</tr>
<tr>
<td>ums_identity_mismatch_status</td>
<td>ums_identity_mismatch_status</td>
<td>INFO</td>
</tr>
<tr>
<td>ums_version_mismatch_status</td>
<td>ums_version_mismatch_status</td>
<td>INFO</td>
</tr>
<tr>
<td>unknown_hw_sensor</td>
<td>unknown</td>
<td>INFO</td>
</tr>
</tbody>
</table>
### Table 2  
*Events Included Under the Cisco VSM Alerts (continued)*

<table>
<thead>
<tr>
<th>Voltage</th>
<th>Voltage</th>
<th>CRITICAL</th>
<th>{0} is critical</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>INFO</td>
<td>{0} is normal</td>
</tr>
</tbody>
</table>
Map Workspace

Contents

- Overview, page 51
- Working With Image Layers, page 54

Overview

The Map Workspace displays maps of the region, city, building or other areas where the Cisco VSM is deployed (Figure 1). Use maps to view a physical representation of the camera locations in your deployment, or as an alternative way to locate cameras and drag and drop them onto a Video Wall.

For example, click a location to view the associated map(s). Cameras at that location are represented by a camera icon . Single-click the icon to display a draggable icon, or double-click the icon to view video in a pop-up window.

Tip
Maps can include an aerial view of the camera location (such as a street map or satellite view), or an image of the physical location, such as a building layout, floor plan or other image.

Note
The Map Workspace is available in the Cisco SASD application only. Maps are not included in the Cisco SASD Advanced Video Player or Cisco SASD Federator applications.

Note
When upgrading to Release 7.5 from Release 7.2 or lower, you must migrate the map images from the previous system and reconfigure the map image layers. The Cisco VSM mapping system has been replaced with GIS map support which is not compatible with the earlier map support. Accessing cameras on maps now requires the use of a Cisco VSM Map Server. See the “Migrating Map Images From a Previous Cisco VSM Release” section in the Cisco Video Surveillance Operations Manager User Guide for more information.
Figure 1 describes the main elements of the Map workspace.

**Figure 1  Map Workspace**

1. **Map Workspace** tab.
   - Cisco SASD application only. Maps are not included in the Cisco SASD Advanced Video Player or Cisco SASD Federator applications.
   - Click to create a duplicate workspace window that can be dragged to a separate monitor. See “Displaying a Duplicate Workspace on a Separate Monitor”.

2. Locations. Select a location to display the maps for that location and its sub-locations.

3. Map for the selected location.
   - Double-click anywhere on the map to zoom the map image.

4. Camera icons.
   - A number is displayed when multiple cameras are present and the map is too small to display individual icons. Zoom in to view the individual icons.
   - Single-click a camera to view video and alerts from that device. Click anywhere on the map to dismiss the video feed.
   - Double-click a camera icon to view video from the camera in a pop-up window. Click anywhere on the map to dismiss the video feed.
   - Right-click the icon and select **Filter Alert by Camera** to view the alerts for that device.
   - The camera icon color represents the device status:
     - Green—Enabled: OK
     - Yellow—Enabled: Warning
     - Red—Enabled: Critical
### Requirements

The following requirements must be met to use the Cisco SASD Maps workspace:

#### Table 1  Requirements

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Complete?</th>
</tr>
</thead>
<tbody>
<tr>
<td>A Cisco Maps Server must be installed and added to the Operations Manager configuration.</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong> The location maps and image layers configured in Operations Manager are available for use in the Cisco SASD Maps workspace.</td>
<td></td>
</tr>
<tr>
<td>Internet Explorer (IE) 9 or 10 must be installed on the monitoring workstation:</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong> Do not install IE 11 on the monitoring workstation. Cisco SASD Maps workspace uses IE to communicate with the Operations Manager Maps Server service and configuration. IE 11 can cause incompatibility issues.</td>
<td></td>
</tr>
<tr>
<td>See the Cisco Video Surveillance Monitoring Workstation Performance Baseline Specification for more information.</td>
<td></td>
</tr>
<tr>
<td>The Cisco SASD desktop application installed in the monitoring PC.</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong> The Maps workspace is not supported on the Cisco SASD Federator or Cisco SASD Advanced Video Player applications.</td>
<td></td>
</tr>
</tbody>
</table>
Working With Image Layers

Image layers (Figure 2) represent additional details on a location map. For example, if a location map shows an aerial view of a building, image layers can show images of each floor in that building.

Click the selector icon to display and select the image layers available for a location. Camera icons represent the real-world location of cameras in each image, allowing you to view video and alerts from specific cameras.

Figure 2 Image Layers

1 Image layer (represented by a green box).
   - The number indicates the number of cameras available in the image.
   - Click the box to display an enlarged image.

2 The enlarged image layer.
   - Select a camera to view video and alerts from that device.
   - Click the selector icon to display the available image layers (such as each floor in a building).
To view video from cameras using map images, do the following:

**Step 1** Select the Map Workspace (Figure 1).

**Step 2** Expand the location hierarchy and select a location from the list.

**Step 3** (Optional) Click the selector icon to choose a map provider (such as a MapQuest or OpenStreetMap).

**Step 4** (Optional) Click a image layer to display an enlarged version of the image.

**Step 5** (Optional) Click the selector icon to choose an image layers (such as a building floor plan).

**Step 6** (Optional) Double-click a camera icon to view video for that camera in a pop-up window.

**Step 7** (Optional) Single-click a camera icon to display a dragable icon, then drag and drop the icon to a Video Wall (see “Wall Workspace” for more information).

**Step 8** (Optional) Right-click an alert to change the status or enter a comment.

**Step 9** (Optional) Right-click the icon and select Filter Alert by Camera to view the alerts for that device.

---

**Tip** Review Figure 1 and Figure 2 for additional options.
Controlling Video Playback

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

The features available on your workstation depend on the following:

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

**Note**
If more than 48 panes are displayed, SASD performance can be poor and, in unusual cases, can crash. We recommend displaying less than 48 video panes on a single workstation. If additional panes are required, use an additional monitoring workstation.

**Contents**
Refer to the following topics for more information.

- Overview, page 58
- Viewing Live Video, page 59
- Viewing Recorded Video, page 62
- Managing Video Clips, page 66
- Using Record Now, page 77
- Using the Pop-Up Menu, page 78
- Understanding Video Pane Border Colors, page 80
- Using the Privacy Mask, page 81
- Using the Smooth Video Options When Viewing Live Video, page 84
- Synchronizing Video Playback in Multiple Panes, page 85
- Using Pan, Tilt, and Zoom (PTZ) Controls, page 89
Overview

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

For example, Figure 1 shows a multi-pane view using the Cisco Video Surveillance Safety and Security Desktop (Cisco SASD) application.

Figure 1  Multi-Pane View using the Cisco Video Surveillance Safety and Security Desktop Application

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

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

Viewing Live Video

Live video is displayed by default when you log in to the viewing application. Figure 2 summarizes the controls available in each viewing pane.

**Figure 2 Video Pane Controls**

1 Camera name—The source of the displayed video.
Chapter       Controlling Video Playback

Usage Notes
- Some firewall policies on enterprise PCs can block live video streams from cameras. If this occurs, add the camera IP address to the firewall trusted list.
- To maximize the video screens, move the new workspace to a separate monitor and double-click a pane to fill the entire browser window. To fill the entire monitor screen, right-click the image and select Full screen mode.
- To control the playback in multiple video panes, Shift-Click or Ctrl-Click to select the panes. The borders of all selected panes turn to orange. Controls and actions performed in one pane also affect the other selected panes. To deselect panes, select a single pane, or use Shift-Click or Ctrl-Click to deselect the panes.
- Live video may be delayed 1-2 seconds. Live video can be further delayed if the smooth video option is enabled. See the “Using the Smooth Video Options When Viewing Live Video” section on page 84 for more information.

2 Indicates the quality of the primary live video stream. If the live video quality is poor, an alternative secondary or iFrame video stream can be automatically applied. See the “Using the Smooth Video Options When Viewing Live Video” section on page 84 for more information.

3 Indicates live or recorded video (recorded video displays a timestamp such as 4/7/2012 2:03:56 PM).

4 Range Bar—Used with recorded video (see the “Viewing Recorded Video” section on page 62 for more information).

5 Seek—Used with recorded video to choose a playback time (see the “Viewing Recorded Video” section on page 62 for more information).

6 The green icon indicates live video. Click the icon to switch to the recorded view.

7 Live video playback controls.
   - —Pause the video playback.
   - —Play the video forward at normal speed.
   Note The other playback controls are used with archived video only. See Figure 3 on page 62 for more information.

8 —Click the triangle to pin the control bar to the screen, or auto-hide the bar when the cursor is moved.
   Note The control bar and audio icon will not display if your workstation monitor is set to 16-bit color setting. Change your monitor color setting to 32-bit.

9 Video image.

10 Camera menu.
   Right-click the image to open the menu and select an option. Options not supported by the camera are disabled (shown in gray). See the “Using the Pop-Up Menu” section on page 78 for more information.

11 Control icons.
   - Audio. The audio icon appears if the camera supports audio. Click to enable or mute live audio volume. This control does not affect recorded video.
   - Privacy Mask. Click to enable or disable the Privacy Mask. See the “Using the Privacy Mask” section on page 81.
   - PTZ. Click to enable or disable the Pan, Tilt and Zoom (PTZ) controls. See the “Using Pan, Tilt, and Zoom (PTZ) Controls” section on page 89.
   - — See the “Synchronizing Video Playback in Multiple Panes” section on page 85.
   Note The control bar and audio icon will not display if your workstation monitor is set to 16-bit color setting. Change your monitor color setting to 32-bit.
• Soft-deleted cameras (shown with a icon) are cameras that were removed from the system but still allow access to the camera’s recorded video. You cannot display live video from soft-deleted cameras.
• The control bar and audio icon will not display if your workstation monitor is set to 16-bit color setting. Change your monitor color setting to 32-bit.

Additional Information
Refer to the following topics for additional options:
• Using Record Now, page 77
• Using the Pop-Up Menu, page 78
• Using the Smooth Video Options When Viewing Live Video, page 84
• Synchronizing Video Playback in Multiple Panes, page 85
• Using Pan, Tilt, and Zoom (PTZ) Controls, page 89
Viewing Recorded Video

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

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

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

Figure 3 describes the main recording features and controls.

---

### Figure 3  Viewing Recorded Video

1. **Camera Name**—Source of the recorded video.
2. Indicators the video quality, which can be affected by network and system performance. The icon turns red if the video quality is poor.
   - **Note**: This icon is for informational purposes only when displayed with recorded video (the Smooth Video options do not apply).
3. Pop-up menu options. See the “Using the Pop-Up Menu” section on page 78.
4. Timestamp for the currently displayed video image. For example: **7/12/2012 4:08:39:886 AM**.
   - **Note**: Changes to **Live** when live video is displayed.
Chapter 5: Controlling Video Playback

5 Range Bar—The span of video to work with.
   - The entire range bar represents the entire span of available recorded video. Slide the range bar selectors to shorten the range (see below).
   - The lower (green) seek bar represents the selected range (see below).

6 Range Bar selectors—Drag the range bar selectors to narrow the timespan of video you want to review.
For example, drag the selectors to create a 10 minute range. You can then drag that range left or right to the appropriate place in the recorded span.

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

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

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

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

7 Seek Bar—Represents the video range, and is used to select a playback time.
For example, if the range is 10 minutes, then the seek bar represents 10 minutes of video.

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

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

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

Note: When you move the scroll bar for a video pane that is synchronized, that pane becomes the new synchronization master pane. The other synchronized panes play video according to the master pane. See the “Synchronizing Video Playback in Multiple Panes” section on page 85.
9 Bookmarks—Create bookmarks to save a video clip or a repeating segment (see below).

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

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

See the following for more information:

- Managing Video Clips, page 66
- Creating a Repeat Segment, page 76

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

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

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

12 Recorded video playback controls.

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

Variable Speed Playback

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

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

Usage Notes

- Multi-pane video clips can also be saved to your desktop and played using the Cisco Video Surveillance Review Player.

- If the Record Now feature is enabled, right-click the image and choose Record Now to record live video.

- If a camera is soft-deleted, you can still access the camera’s recorded video but cannot display live video. Recordings are retained on the system until removed according to the recording retention settings.

- Click the icon to toggle between live and recorded video. The icon appears when recorded video is displayed.

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

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

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

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

Refer to the following topics for more information:

- Clipping Support By Application, page 66
- Supported File Formats And Playback Options, page 67
- Creating Video Clips, page 69
- Downloading and Viewing Clips, page 74

Tip

- You can also search for and download clips using the Clip Search feature in Operations Manager/Cisco VSM Federator and the Clip Management feature in Cisco SASD/Cisco SASD Federator.
- Timestamps are not displayed in 3rd-party video viewers. Use the Cisco Review Player to play video clips that display timestamps (see the Cisco Video Surveillance Review Player User Guide for more information).

Clipping Support By Application

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

<table>
<thead>
<tr>
<th>Application</th>
<th>Create MP4 Clips</th>
<th>Create CVA Clips</th>
<th>Create Virtual Clips</th>
<th>View MP4 Clips¹</th>
<th>View CVA Clips</th>
<th>View Virtual Clips</th>
<th>Clip Search Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco VSM Operations Manager</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco VSM Federator</td>
<td>Yes²</td>
<td>Yes</td>
<td>No</td>
<td>Yes³</td>
<td>No</td>
<td>Yes⁴</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco SASD</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes⁵</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes⁶</td>
</tr>
<tr>
<td>Cisco SASD Federator</td>
<td>Yes⁷</td>
<td>Yes</td>
<td>No</td>
<td>Yes⁸</td>
<td>No</td>
<td>No</td>
<td>Yes⁹</td>
</tr>
<tr>
<td>Cisco VSM Review Player</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes¹⁰</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

¹. MP4 clips are saved to the server and play immediately after being downloaded to the monitoring PC. Third-party video players (such as VLC) can also be used to view MP4 clips.

². Create MP4 clips using the Federator Thumbnail Search.

³. Federator clips must be downloaded and played using either Cisco Review Player or VLC.

⁴. Double click the virtual clip in Federator Clip Search to play the virtual clip.

⁵. Thumbnail Search supports MP4 clip creation only.

⁶. Cisco SASD does not support Virtual Clip search in this release.

⁷. Create MP4 clips using the Federator Thumbnail Search.

⁸. Federator clips must be downloaded and played using either Cisco Review Player or VLC.

⁹. Cisco SASD Federator supports MP4 clips only in this release (virtual clip search is not supported).

¹⁰. Cisco VSM Review Player supports MP4 clips only in this release (virtual clip search is not supported).
10. CVA files can only be opened in applications that support the CVA format (such as the Cisco Review Player).

**Supported File Formats And Playback Options**

Video clips can be created in multiple formats:

- MP4 and CVA video files can be saved to a local disk for playback using the Cisco VSM Review Player or a third party player.
- Virtual clips can be stored on the Cisco VSM server for playback using supported applications, such as the browser-based Operations Manager.
Table 2 describes the video clip options:

<table>
<thead>
<tr>
<th>File Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual clip</td>
<td>Defines a segment of video on the Cisco VSM server for playback using a supported application, such as the browser-based Operations Manager.</td>
</tr>
<tr>
<td>MP4</td>
<td>MP4 clips are saved on the server and can be downloaded to a PC workstation or local disk. MP4 clips support a single video pane and can include audio (CVA/CVX files do not support audio). MP4 is a standard video file format that is playable on most computers and useful for sending to 3rd parties.</td>
</tr>
</tbody>
</table>

**Notes**

- In this release, Virtual Clips can be created using the Operations Manager and Cisco SASD, but not Cisco VSM Federator or Cisco SASD Federator. See the “Clipping Support By Application” section on page 66.
- Virtual clips can be any length. There is no maximum duration for a virtual clip.
- Virtual clips can be saved as an MP4 file (the 10 hour MP4 limitation applies).
- Virtual clips do not support audio recording.
- In this release, MP4 clips can be created using the Operations Manager and Cisco SASD. To create MP4 clips using the Cisco VSM Federator or Cisco SASD Federator, use the Clip Search and Clip Management features. See the “Clipping Support By Application” section on page 66.
- MP4 clips play automatically in the pane when downloaded. The clips can also be viewed using the Cisco VSM Review Player or VLC media player.
- You can also use the **Clip Search** feature to view, download and delete MP4 clips saved to the server.
- The maximum duration for an MP4 clip is 10 hours per clip.
- MP4 clips require that the clipping repository be selected on the Media Server associated with the camera. See the “Partition Settings” section on page 5.
- MP4 clips are saved on the server for 7 days and are automatically deleted from the server 7 days after creation. To download the clips to a local drive, use the **Get Clips Status** menu (see also the “Downloading and Viewing Clips” section on page 74).
- MP4 audio playback is supported only with the Cisco VSM Review Player or VLC media player.
- Up to five MP4 clips can be created at a time per Media Server. If the limit is reached, wait for a clip to complete before creating a new one.
- Users can only delete their own clips. Users that belong to a User Group with **Camera** permissions can also delete other users’ clips.
- If the clipping fails, see your system administrator for assistance.
- Use the Cisco VSM Review Player to save MP4 files in the tamper proof MPX format. See the Cisco Video Surveillance Review Player User Guide for more information.
Creating Video Clips

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

Requirements

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

File Formats Supported by the Monitoring Applications

Review the “Clipping Support By Application” section on page 66 for information on the clip formats supported by each application in this release.

Procedure

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

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

**Step 2** In the green *seek* bar, Ctrl-Click and drag the mouse cursor to create a bookmark span. The bookmark span is shown in orange (Figure 4).

**Notes**

- The maximum duration for a CVA clip is 24 hours per clip.
- CVA files do not support audio playback.

CVX

A tamper proof CVA file. CVX files require a password that is entered when the file is created. You must enter the password to open and view the video file.

**Notes**

- CVX video playback will shut down if the file is tampered with.
- CVX files do not support audio.

You can also right-click a video pane and select Take Snapshot to save a still image in BMP, JPEG, PNG, and TIFF formats. See the “Using the Pop-Up Menu” section on page 78 for more information.

**Table 2 Video Clip File Formats (continued)**

<table>
<thead>
<tr>
<th>File Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVA</td>
<td>A Cisco video archive (CVA) can include multiple video panes that synchronize to the same time. CVA/CVX clips are downloaded immediately and not stored on the server. CVA files can only be opened in applications that support the CVA format (such as the Cisco Review Player).</td>
</tr>
</tbody>
</table>

**Notes**

- The maximum duration for a CVA clip is 24 hours per clip.
- CVA files do not support audio playback.

<table>
<thead>
<tr>
<th>File Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVX</td>
<td>A tamper proof CVA file. CVX files require a password that is entered when the file is created. You must enter the password to open and view the video file.</td>
</tr>
</tbody>
</table>

**Notes**

- CVX video playback will shut down if the file is tampered with.
- CVX files do not support audio.
In recording mode, you can also right-click the image and choose **Select Clip Range** from the pop-up menu (see the “Using the Pop-Up Menu” section on page 78). A 10 minute clip range is automatically selected starting from current thumb position, and the range bar is automatically scaled to 1 hour.

**Step 3**

Right-click the bookmark and select an option to create a MP4, CVA or virtual clip (Figure 4).

**Figure 4 Creating a Video Clip**

Tip

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

**Step 4**

Save the file:

**CVA/CVX files**

a. (Optional) Revise the start and end date and time (Figure 5). Enter a time between 30 seconds and 24 hours (the range cannot include more than one codec and the start time must be before the end time).

Tip

Use the Set Duration field to enter a specific length of time for the clip. The duration begins at the beginning bookmark time.
b. (Optional) Select **Enable tamper proof** and enter a password to create a password-protected CVX file (*Figure 5*).

c. Click **OK**.

d. Select a location on a local disk and click **Save**.

e. Wait for the clip to be generated and downloaded. Video streaming is paused during CVA/CVX clip generation.

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

**MP4 clips**

a. (Optional) Revise the start and end date and time (*Figure 6*). Enter a time between 30 seconds and 10 hours (the range cannot include more than one codec and the start time must be before the end time).

**Tip** Use the Set Duration field to enter a specific length of time for the clip. The duration begins at the beginning bookmark time.
b. (Optional) Enter a clip name that identifies the recording on the server (Figure 6). For example, if you enter “My 4500 Camera” then the clip selection will be “My 4500 Camera”. The default name is “My Clip”.

c. (Optional) Select or deselect **Record Audio** (if the camera supports audio recordings) to include or exclude audio. Audio playback is supported only with the Cisco VSM Review Player or VLC media player.

d. Click **OK** to save the clip to the server.

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

e. Download and play the clip as described in the “Downloading and Viewing Clips” section on page 74.

**Virtual clips**

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

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

Figure 7  Virtual Clip Settings

b. (Optional) Enter a clip name that identifies the recording on the server (Figure 7). For example, if you enter “My 4500 Camera” then the clip selection will be “My 4500 Camera”. If blank, the default name is “My Clip”.

c. Click OK to save the clip to the server.

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

Step 5  Download and play the clip as described in the “Downloading and Viewing Clips” section on page 74.
## Downloading and Viewing Clips

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

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

<table>
<thead>
<tr>
<th>Table 3</th>
<th>Video Clip Download Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clip Format</td>
<td>Download Options</td>
</tr>
<tr>
<td>CVA clips</td>
<td>Downloaded when they are created. Play CVA clips using a supported video player, such as the Cisco Review Player.</td>
</tr>
</tbody>
</table>
| MP4 Clips | Right-click the video pane and select **Get Clip Status** (not supported in Federator in this release). Select the clip name from the list and save the file to a local disk (the clip remains on the server for 7 days after it was created).  
- The clip automatically plays in the video pane when the download is complete.  
- You can also play the clip using a supported video player such as the Cisco Review Player or VLC.  
- You can also search for and download MP4 clips using the **Clip Search** feature in Operations Manager or the **Clip Management** feature in Cisco SASD. |
| Virtual Clips | Right-click the video pane and select **Get Clip Status** (not supported in Federator in this release). Select the clip name from the list to play the clip in the video pane.  
To download the clip, use the **Clip Search** feature and select the **Virtual Clip Search** tab (if supported by your monitoring application). |

### Procedure

**Step 1**
Right-click the video pane and choose **Get Clip Status** (Figure 8).

**Step 2**
Select the *Clip* name.
- “Local” clips are MP4 clips that must be downloaded to a local disk.
- “Streamable” clips are virtual clips that can be streamed in the video pane without being downloaded.
Figure 8 Accessing a MP4 Clip

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

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

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

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

Figure 9 Create a Repeating Segment

Procedure

Step 1  Ctrl-Click-drag the seek bar in a recording to create a bookmark (Figure 9). The bookmark span is shown in orange.

Step 2  Right-click the seek bar and select as a repeat segment.

Step 3  (Optional) Enter a specific start and end date and time.

Step 4  To cancel the segment, right click the segment and choose Remove all Bookmarks. You can also click on the seek bar outside the selected range.
Using Record Now

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

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

**Usage Notes**
- Audio is not recorded.
- Video is recorded for a system-defined length of time (the default is 5 minutes).
- The recording is retained on the system according to the event retention settings for the camera. For example, if the camera’s event recordings are retained for 30 days, then the Record Now recordings will also be available for 30 days. When the retention time is exceeded, the recording is automatically deleted (see the “Managing Video Clips” section on page 66 to save the video to a separate file).

**Procedure**

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

**Step 2**  
Choose live video (see the “Viewing Live Video” section on page 59).

**Step 3**  
Right click the image and choose **Record Now** (Figure 10).

- The recording is performed in the background. You can continue to use the other playback controls.
- The recording status is displayed in red text (Figure 10) when the recording time nearly complete.

![Figure 10 Record Now](image)
Step 4  To view the recorded video, review the following notes.

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

- If the video is within the time span of other recorded video, there is no separate indication of the Record Now video. You can access the video as described in the “Viewing Recorded Video” section on page 62.

![Time span (for all recordings)](image1)

**Record Now recording included within the time span of other continuous and event recordings.**

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

![Time span (for all recordings)](image2)

**Record Now recording**  
**Recording gap**  
**Continuous loop recording**

![Note](image3)

**Note**  When the event retention time is exceeded, the Record Now recording is automatically deleted. To save the recording, see the “Managing Video Clips” section on page 66.

---

### Using the Pop-Up Menu

Select a video pane and right-click on the image to open a menu with the following options (see Figure 2 on page 59).

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

<table>
<thead>
<tr>
<th>Camera Menu Item</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Pan, Tilt, and Zoom**   | (Live video only) Open the PTZ preset list that allows you to quickly adjust the camera view.  
                             | See the “Using Pan, Tilt, and Zoom (PTZ) Controls” section on page 89          |
| **Digital zoom**          | Digitally enlarges the image to zoom in on a specific area.  
                             | Double click the enlarged image to use a window-in window view. Adjust the viewing area in the small window to define the portion of enlarged video to display. |
Chapter  Controlling Video Playback

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

<table>
<thead>
<tr>
<th>Camera Menu Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sync selected panes with this pane</strong></td>
<td>Synchronizes the playback from multiple video panes to the same time.</td>
</tr>
<tr>
<td></td>
<td>• After a pane is synchronized, the menu item changes to <strong>Remove this pane from sync</strong>.</td>
</tr>
<tr>
<td></td>
<td>• To synchronize additional panes, right-click an un-synchronized pane and select <strong>Add selected panes to sync</strong>.</td>
</tr>
<tr>
<td></td>
<td>See the “Synchronizing Video Playback in Multiple Panes” section on page 85.</td>
</tr>
<tr>
<td><strong>Full screen mode</strong></td>
<td>Enlarges the video image to fill the entire monitor screen.</td>
</tr>
<tr>
<td></td>
<td><strong>Tip</strong> To exit, press Esc, or right-click and choose <strong>Full screen mode</strong> again.</td>
</tr>
<tr>
<td><strong>Take snapshot</strong></td>
<td>Saves a snapshot of a single video pane (excluding control icons, timestamps and other information) in BMP, JPEG, PNG, or TIFF format.</td>
</tr>
<tr>
<td><strong>Take composite snapshot</strong></td>
<td>Saves a snapshot of all panes in a multi-pane layout (including control icons, timestamps and other information) in BMP, JPEG, PNG, or TIFF format.</td>
</tr>
<tr>
<td><strong>Record now</strong></td>
<td>(Live video only) Immediately begins recording video.</td>
</tr>
<tr>
<td></td>
<td>See the “Using Record Now” section on page 77 for more information.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The Record Now option must be enabled in the camera configuration.</td>
</tr>
<tr>
<td><strong>Audio settings</strong></td>
<td>(Cameras with audio support only). Opens a window used to adjust video playback volume and balance.</td>
</tr>
<tr>
<td><strong>Smooth video settings</strong></td>
<td>(Live video only) Creates a smooth video playback if the playback is choppy or delayed due to network or other performance issues.</td>
</tr>
<tr>
<td></td>
<td>See the “Using the Smooth Video Options When Viewing Live Video” section on page 84.</td>
</tr>
<tr>
<td><strong>Global settings</strong></td>
<td>Provides settings that apply to all video panes. For example: UI transparency and zoom video to fit the pane.</td>
</tr>
<tr>
<td><strong>Select Streams</strong></td>
<td>Allows you to select the live and recorded video streams (primary or secondary) supported by the camera.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> <strong>Select Streams</strong> is disabled when the pane is synchronized. See the “Synchronizing Video Playback in Multiple Panes” section on page 85 for more information.</td>
</tr>
<tr>
<td><strong>Select clip range</strong></td>
<td>(Archive video only) Selects a 10 minute clip range starting from current thumb position. The range bar is automatically scaled to 1 hour.</td>
</tr>
<tr>
<td></td>
<td>See the “Managing Video Clips” section on page 66 for more information.</td>
</tr>
<tr>
<td><strong>Get clip status</strong></td>
<td>Shows the current status of MP4 and virtual clips: In-Progress, Completed or Failed.</td>
</tr>
<tr>
<td></td>
<td>Select a clip name to view the clip. MP4 clips are downloaded to a local disk (you are prompted to enter a filename and location).</td>
</tr>
<tr>
<td></td>
<td>See the “Creating Video Clips” section on page 69 for more information.</td>
</tr>
</tbody>
</table>
Understanding Video Pane Border Colors

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

Table 5 describes the meaning of each color.

<table>
<thead>
<tr>
<th>Color</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gray</td>
<td>The pane is not highlighted. All panes have a gray border by default.</td>
</tr>
<tr>
<td>Orange</td>
<td>The pane is selected as the active pane, and the controls and actions apply to that pane. If multiple panes are selected as active panes, the controls and actions performed on one pane apply to all active panes.</td>
</tr>
</tbody>
</table>
Using the Privacy Mask

When the Privacy Mask is enabled on a compatible camera (Figure 11), all live video from that camera is blocked and cannot be viewed by any operator or monitor, or recorded by the Cisco Video Surveillance system. This feature is typically used with the “Virtual Sitter” feature for health care providers, allowing operators to temporarily block video from a Cisco Video Surveillance camera when the patient requires privacy. Figure 11 shows the icons used to enable or disable the Privacy Mask.

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

Figure 11  Privacy Mask Controls

<table>
<thead>
<tr>
<th>Icon</th>
<th>Purpose</th>
<th>Description</th>
</tr>
</thead>
</table>
| ![Enable the Privacy Mask](image) | Enable the Privacy Mask | Click to block the camera’s entire field of view and display a blank (blue) screen.  
- Live video is not transmitted and cannot be viewed by any workstation or monitor.  
- Recorded video displays the blank (blue) or flashing screen.  
- A “Privacy Mask Timer” causes the screen to flash after a period of time, which reminds the operator to disable the Privacy Mask. The default timer is 15 minutes and can be modified using the Operations Manager (System Settings > Settings > Privacy Mask Timer). |
| ![Disable the Privacy Mask (Default)](image) | Disable the Privacy Mask | Click to enable normal video streaming, monitoring, and recording. |
For example, when the Privacy Mask is enabled, the video frame for that camera is blank (Figure 12). The same blank (blue) screen is recorded (if recording is configured).

![Figure 12 Privacy Mask Enabled](image)

When the Privacy Mask Timer expires, the video frame flashes to remind the operator that the mask is still on. To display video, click to disable the Privacy Mask.

**Note**

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

**Related Information**

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

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

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

The Cisco cameras that support the Privacy Mask include the following:

- CIVS-IPC-2830
- CIVS-IPC-2835
- CIVS-IPC-3421V
- CIVS-IPC-3520
- CIVS-IPC-3530
- CIVS-IPC-3535
- CIVS-IPC-6000P
- CIVS-IPC-6020
- CIVS-IPC-6030
- CIVS-IPC-6050
- CIVS-IPC-6930
- CIVS-IPC-7030
Using the Smooth Video Options When Viewing Live Video

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

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

- Automatically switch to a different stream if the live video quality is poor.

**Icon Colors**
The video quality icons in each pane indicate the following:

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

**Usage Notes**

- The Smooth Video Options are available only for live video on non-PTZ cameras (the Smooth Video Options are automatically disabled on PTZ cameras).

- The settings are applied to all non-PTZ cameras and are persistent for the current PC workstation. For example, the settings will remain if you log out and back in, or view a different camera and then return to the current camera.

- The settings also apply to the non-PTZ cameras when using the Cisco Safety and Security Desktop (SASD) application and the Cisco Video Surveillance Management Console.

- The Smooth Video options are disabled if you manually select a stream (right-click a video pane and choose Select Streams and Clips). The pane will display the selected stream even if the video quality is poor (the video will not automatically switch to the Smooth Video alternative stream). To cancel the manually selected stream and re-enable the Smooth Video settings, reload the view or drag and drop the camera again.

- If a video stream is selected from a redundant media server, the Smooth Video option is disabled (the camera will not use a secondary stream even if the video quality icon is red).

**Procedure**

**Step 1**
Right-click a live video image to open the pop-up menu.

**Step 2**
Select or deselect Enable Smooth Video for Live non-PTZ Camera to enable the smooth video options.

**Step 3**
(Optional) Enter the Preroll Buffer Size in Seconds to define the number of seconds that live video will be delayed.

Video data is saved in a cache on your PC to avoid pauses caused by network bandwidth and other issues. We recommend a value between 1.5 and 3 seconds.
We strongly recommend that the Preroll Buffer be disabled (enter 0 or leave the field blank) since streaming delays can cause a potential security risk. We recommend that you address the network bandwidth or performance issues causing the delays. Use the Preroll Buffer only when significant stuttering occurs and a network resolution is not available.

Step 4 Use the Smooth Video Options to define an alternative video stream that will be used if video quality is poor despite the smooth video buffer (video quality is indicated by the icon on the live viewing pane).

- **Secondary Stream**—(Only if configured on the camera) If the live video quality is poor, the secondary video stream is used. Secondary streams typically present a lower-quality image that requires less bandwidth and processing.
- **I frame only**—If the live video quality is poor, then only the iFrame video is displayed. iFrame video reduces the bandwidth requirement to correct the situation.
- **None**—If the live video quality is poor, no change is made and the selected stream is displayed even if it results in choppy or paused playback.

Note

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

**Synchronizing Video Playback in Multiple Panes**

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

Usage Notes

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

<table>
<thead>
<tr>
<th>Format</th>
<th>Resolution</th>
<th>Framerate</th>
</tr>
</thead>
<tbody>
<tr>
<td>JPEG</td>
<td>640x480</td>
<td>30 fps</td>
</tr>
<tr>
<td>H-264</td>
<td>1920x1080</td>
<td>30 fps</td>
</tr>
</tbody>
</table>
Figure 13 describes the main synchronization attributes.

**Procedure**

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

1. Select a layout or pre-defined view from the **View** menu.
2. *Shift-click* or *Control-click* to select multiple video panes for synchronization.

   The selected panes are displayed with a light yellow border.
Step 3  Right-click a video pane and select **Sync Selected Panes With This Pane** from the menu.
The selected pane becomes the master pane.

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

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

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

Cameras that support pan, tilt and zoom (PTZ) movements display a PTZ icon. Click the icon to enable PTZ (the icon is blue when enabled, and do one of the following:

- To pan and tilt, hold down the left mouse button while dragging the mouse ( ) right, left, up and down.
- To zoom:
  - Hold down the left mouse button and use the scroll wheel to zoom in and out.
  or
  - Hold down the Shift key and then press the left mouse button. Drag the mouse up or down to zoom.

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

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

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

![Camera PTZ Controls](image)

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Selected Camera</td>
<td>3</td>
<td>PTZ Enabled/Disabled Icon (click to toggle).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>PTZ is available in Live mode only</td>
<td>4</td>
<td>PTZ Preset Menu (right-click to access)</td>
</tr>
</tbody>
</table>

- Blue — Enabled
- Grey — Disabled
Usage Notes

- To use a USB joystick, see the “Calibrating a Joystick for Windows 7” section on page 91.
- PTZ movements are available only when viewing live video.
- PTZ can only be enabled for a single video pane if multiple panes are displayed. See the “Using PTZ Controls When Multiple Video Windows are Displayed” section on page 92.
- You must also belong to a user group with Perform PTZ permissions.
- PTZ commands are available only if the primary Media Server is functional. If the Primary server goes down, or is not available on the network, PTZ commands will not function even if video is still being delivered by a redundant server (if configured). See the “High Availability” section on page 1 for more information.

PTZ Control Procedure

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

---

**Step 1**
Display the live video from a PTZ-enabled camera:

- Click **Monitor Video**.
- Expand the location tree and select the camera.
- Highlight a video pane and double-click a camera name.

**Step 2**
Click the PTZ control icon to enable PTZ:

- -(Blue) PTZ controls are supported by the camera and enabled in the viewing pane.
- -(Grey) PTZ controls are disabled. Click the icon to enable PTZ controls.

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

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

**Using a Mouse**

- Pan and Tilt—Hold down the left mouse button while dragging the mouse ( ) right, left, up and down.
- Zoom—
  - Hold down the left mouse button and use the scroll wheel to zoom in and out.
  or
  - Hold down the Shift key and then press the left mouse button. Drag the mouse up or down to zoom.

**Using a USB Joystick**

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

**Tip**
See the “Calibrating a Joystick for Windows 7” section on page 91 for information to set up a USB joystick for the first time.
Step 4  (Optional) Select a PTZ preset position.

Using a Mouse

– Right-click the image and choose Pan, Tilt, and Zoom > Presets (Figure 14).
– Choose a preset to move the camera to the defined position.

Using a USB Joystick

– Press the joystick button that corresponds to the PTZ preset number.
– For example, joystick button 1 triggers PTZ preset 1, joystick button 2 triggers PTZ preset 2, etc.

Calibrating a Joystick for Windows 7

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

Procedure

Step 1  Install and configure the USB joystick according to the manufacturer instructions.
• See the device documentation for more information.
• The manufacturer may also include a calibration utility that can be used instead of the built-in Windows utility.

Step 2  In Windows 7, calibrate the device using the Game Controllers control panel.
 a. Select Control Panel from the Start menu.
 b. Select Hardware and Sound.
 c. Select Devices and Printers.
 d. Double-click Game Controllers.
 e. Highlight the joystick device and click Properties.
 f. Click Calibrate in the pop-up window.
 g. Follow the on-screen instructions to complete the process.

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

Step 3  Click Finish or OK to close the windows.
Using PTZ Controls When Multiple Video Windows are Displayed

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

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

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

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>PTZ enabled viewing pane</td>
</tr>
<tr>
<td>2</td>
<td>PTZ disabled viewing pane</td>
</tr>
<tr>
<td>3</td>
<td>PTZ not supported by camera (no icon)</td>
</tr>
</tbody>
</table>

**Note**
PTZ movements are available only when viewing live video.

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

Contents
- Overview, page 94
- Procedure, page 95
Overview

Use Thumbnail Search to quickly locate specific scenes or events in recorded video without fast-forwarding or rewinding. Thumbnail Search displays a range of video as thumbnail images, allowing you to identify a portion of the recording to review.

Figure 1 provides an overview of the search and display controls.

Figure 1  Thumbnail Window

1. Camera and Video Stream.
   - Camera—Drag and drop a camera onto the Forensic Thumbnail Search window.
   - Stream—Select the primary or secondary stream.

2. Thumbnail image size.

3. The start date and time for the displayed thumbnails.

4. Play button.
   - Hover over an image to display the button.
   - Click to play the recorded video for that thumbnail and display the playback controls.

Tip  See “Controlling Video Playback” for more information.

5. Thumbnail clip start time.

6. Video playback.

Tip  See “Controlling Video Playback” for more information.
To view a thumbnail summary of a camera’s recordings:

**Step 1** Log into the Cisco SASD or Cisco SASD Federator application.

**Note** Thumbnail Search is not supported in the Cisco SASD Advanced Video Player application.

**Step 2** Select **Forensic Analysis > Thumbnail Search** (Figure 2).

**Step 3** Drag and drop a camera from the Video workspace onto the Forensic Thumbnail Search window (Figure 2).
Step 4  (Optional) Select the a video stream.
The primary stream is selected by default.

Step 5  Select the start and end time (duration) for the video included in the thumbnails.

Step 6  (Optional) Slide the range bar right or left within the recording timeline.

Step 7  (Optional) Click a thumbnail to play video from the start time (in white text).

Tip
- Use the video playback controls to search within the thumbnail span. See the “Controlling Video Playback” section for more information.
- Double click a pane to enlarge the video in the browser window. Right click and select Full Screen Mode to fill the entire monitor.

Step 8  (Optional) Create an MP4 clip:
   a. Click and drag to select multiple thumbnails.
   b. Select Create MP4 clip.

Step 9  (Optional) Narrow the thumbnail search.
Step 10  (Optional) Select a new time range.
   a. Click and drag to select multiple thumbnails.
   a. Select Zoom In.
Clip Management

Use Clip Management (Figure 1) to view, download and delete MP4 video clips. MP4 video clips are saved to the Cisco Video Surveillance server by default. Clips can be downloaded using any of the following methods:

- Right-click a video pane and select Get Clip Status. Select the clip name from the list and save the file to a local disk (the clip remains on the server for 7 days after it was created).
- Cisco SASD or Cisco SASD Federator—Use the Clip Management feature to find and download video clips.
- Operations Manager—Use the Clip Search feature to find and download video clips.

Tip
- Clip Management is supported by the Cisco SASD or Cisco SASD Federator applications only. The Cisco SASD Advanced Video Player does not include the Clip Management feature.

Procedure
To locate, download, and view MP4 video clips, do the following:

Step 1 Log into the Cisco SASD or Cisco SASD Federator application.

Note Clip Management is not supported in the Cisco SASD Advanced Video Player application.

Step 2 Create one or more MP4 video clips.
See the “Managing Video Clips” in the Cisco Video Surveillance Safety and Security Desktop User Guide for more information.

Step 3 Select Forensic Analysis > Clip Management (Figure 1).

Step 4 (Cisco SASD Federator only) Select a region where the clip(s) were created. Only clips from the Operations Manager location mapped to that region will be displayed.
Step 5  (Optional) Select a location or device (Figure 2):

- Location—Click + to select a specific location where the clip(s) were created. Only clips from the cameras at that location will be displayed.
- Device—Click + to select a location and a specific device (camera). Only clips from that device will be displayed.

Tip  If a location or device is not selected, clips from all locations or all devices are displayed.
**Figure 2**  Select a Location or Device

![Select a Location or Device](image)

**Step 6**  Use the additional clip filters to search for specific clips (Table 1):

- **Tip**  Click **Apply** without filters to display all available clips.

**Table 1**  Filters For Searching Clips

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Servers</td>
<td>Click <img src="link" alt="link" /> to select a specific Cisco Video Surveillance Media Server. Only clips created by the cameras managed by that Media Server will be displayed.</td>
</tr>
<tr>
<td>Name/Tag Contains</td>
<td>Enter a full or partial name for the clip(s).</td>
</tr>
<tr>
<td>Clip Status</td>
<td>Select the status for the displayed clips. Any status not selected will not be displayed.</td>
</tr>
<tr>
<td>Owner</td>
<td>Select <strong>Me</strong> to display only clips you created. De-select to display clips created by other users.</td>
</tr>
</tbody>
</table>

**Step 7**  Click **Apply**.
Step 8  Review information about the clips.

**Table 2  Video Clip Information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clip Name</td>
<td>The clip name entered when the clip was created. The default is “My Clip” if no name is entered.</td>
</tr>
<tr>
<td>State</td>
<td>In-Progress, Completed or Failed</td>
</tr>
<tr>
<td>Camera</td>
<td>The camera name where the clip originated.</td>
</tr>
<tr>
<td>Start Time</td>
<td>The start timestamp for the clip.</td>
</tr>
<tr>
<td>End Time</td>
<td>The end timestamp for the clip.</td>
</tr>
<tr>
<td>Expiration Time</td>
<td>The date/time when the clip will be automatically deleted from the server. See “Managing Video Clips” in the Cisco Video Surveillance Safety and Security Desktop User Guide for more information.</td>
</tr>
<tr>
<td>Location</td>
<td>Location of the cameras where the clip originated.</td>
</tr>
<tr>
<td>Media Server</td>
<td>The Media Server that manages the camera video where the clip originated.</td>
</tr>
<tr>
<td>Owner</td>
<td>The user that created the clip.</td>
</tr>
<tr>
<td>Tags</td>
<td>Tags associated with the clip.</td>
</tr>
<tr>
<td>Download %</td>
<td>The status of the clip download (see Step 9).</td>
</tr>
</tbody>
</table>

Step 9  (Optional) To download and view an MP4 clip, select a clip and click **Download**.

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

a. Click **Continue** and accept the security certificate when the Internet Explorer web browser prompts you to proceed to the secure page. This prompt appears only once for each Media Server.

b. Select one of the following options:
   - **Open**—Plays the file using your default video player.
   - **Save As**—Enter a filename and select a location on the local disk.
   - **Cancel**—Cancel the download.

Step 10 (Optional) To permanently delete a clip from the server, select one or more clips and click **Delete**.

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

Contents

- Motion Video Analysis Overview, page 103
- Understanding Luminance Metadata and Motion Analysis, page 104
- Requirements, page 104
- Summary Steps, page 105
- Motion Video Search Detailed Procedure, page 106
- Metadata Job Management, page 117

Motion Video Analysis Overview

Motion Video Analysis allows you to examine recorded video for motion, even if motion was (or was not) discovered when the video was originally recorded. You can examine specific time span and apply sensitivity filters to discover or ignore motion in different sections of the video frame. These filters can be modified and the video re-examined to discover different time spans, or to fine tune the amount of motion required to detect an event. You can then view motion events individually, watch a summary of the motion events, or play the entire video (including portions that did not include motion events).

Motion Video Analysis is enabled by generating luminance metadata for the recorded video. This metadata defines a luminance value for each pixel in the frame. The metadata can then be analyzed for changes to the luminance values from one frame to the next. Motion is detected based on these luminance value changes, and the sensitivity filters you apply.

Video motion analysis is supported for the primary stream only in this release. JPEG recordings are not supported. Luminance metadata must be enabled on the Operations Manager. See the “Requirements” section on page 104 for more information.

Motion Video Analysis can be used for security purposes, or to perform other analysis such as the number of cars entering or leaving a parking garage. The number of motion events can be determined for a large amount of time, or to quickly view a video summary of only the times when a vehicle enters or exits the parking structure.

The video viewing window supports the recorded video controls, allowing you to save video clips (or capture still images) of all or part of the motion event video (see “Viewing Recorded Video” and “Managing Video Clips”).
Understanding **Luminance Metadata and Motion Analysis**

Luminance metadata defines the luminance value for each pixel in a video frame. For example, black pixels have a specific luminance value, while white, green, orange or other pixels have different luminance values. This luminance metadata is appended to a span of recorded video using the Cisco SASD Motion Video Analysis feature described in this document (see Stage 1 in the “Motion Video Search Detailed Procedure”).

---

**Note**

Cisco VSM adds metadata to a sample of the video frames available in a recording. For example, metadata is appended to the video at 10 frames per second, which provides enough information to detect motion, but does not degrade system performance or require excessive storage requirements.

To determine if motion occurred in a video recording, the Motion Video Analysis feature analyzes the luminance metadata for changes to the luminance value from one frame to the next. For example, if the pixels have the same luminance values from one frame to the next, then no motion (or change) occurred. However, if a person or object moves within the frame, the luminance values for the affected pixels will change, and a motion event can be detected.

The amount luminance value changes required to trigger a motion event are defined by the sensitivity settings you define. For example, you can paint a grid to define the areas that should detect motion, and specify normal or high sensitivity for each grid (sensitivity defines if more or less of the pixels in that grid must experience a luminance change). You can also define the percentage of grids that must be affected for a motion event to occur. See the “Motion Video Search Detailed Procedure” for more information.

---

**Note**

The Motion Video Analysis feature described in this document is enabled only if a Metadata server is installed, the Metadata server service is added to the Operations Manager, and the Luminance metadata track is enabled. See the Cisco Video Surveillance Operations Manager User Guide for instructions and more information.

---

### Requirements

The following requirements must be met to use the Motion Video Analysis feature.

**Table 10-1 Metadata Requirements**

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Complete?</th>
</tr>
</thead>
<tbody>
<tr>
<td>A Metadata Server service must be enabled on a stand-alone virtual or physical server running Cisco VSM Release 7.5 or higher (operating system RHEL6.4). The Metadata Server service must then be added to the Operations Manager for your deployment.</td>
<td>✓</td>
</tr>
</tbody>
</table>

**Related Information**

- Cisco Video Surveillance Operations Manager User Guide
- See your system administrator for more information.
Table 10-1  Metadata Requirements (continued)

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Complete?</th>
</tr>
</thead>
<tbody>
<tr>
<td>The camera’s configuration template must be configured to record video, and be enabled for the Luminance metadata track.</td>
<td></td>
</tr>
<tr>
<td>Note Video motion analysis is supported for the primary stream only in this release. JPEG recordings are not supported.</td>
<td></td>
</tr>
<tr>
<td>Note An error message appears if a camera the Luminance metadata track is not configured on the camera template.</td>
<td></td>
</tr>
<tr>
<td>Related Information</td>
<td></td>
</tr>
<tr>
<td>• Cisco Video Surveillance Operations Manager User Guide</td>
<td></td>
</tr>
<tr>
<td>You must belong to a Cisco Video Surveillance User Group with permissions for the following:</td>
<td></td>
</tr>
<tr>
<td>Note All of the following permissions are required to generate metadata, view the generated metadata, and perform video motion searches (using the Cisco SASD desktop application).</td>
<td></td>
</tr>
<tr>
<td>• Post Analytics Metadata</td>
<td></td>
</tr>
<tr>
<td>• View Analytics Metadata</td>
<td></td>
</tr>
<tr>
<td>• View Live Video</td>
<td></td>
</tr>
<tr>
<td>• Perform PTZ (automatically enabled with View Live Video)</td>
<td></td>
</tr>
<tr>
<td>• View Recordings</td>
<td></td>
</tr>
<tr>
<td>• Camera (Manage permission)</td>
<td></td>
</tr>
<tr>
<td>Related Information</td>
<td></td>
</tr>
<tr>
<td>• See your system administrator for more information.</td>
<td></td>
</tr>
<tr>
<td>• See the Cisco Video Surveillance Operations Manager User Guide for instructions to define user access permissions.</td>
<td></td>
</tr>
<tr>
<td>The Cisco SASD desktop application must be installed on a monitoring PC.</td>
<td></td>
</tr>
<tr>
<td>Note Motion Video Analysis is not supported using the Cisco SASD Advanced Video Player or Cisco SASD Federator applications.</td>
<td></td>
</tr>
<tr>
<td>Related Information</td>
<td></td>
</tr>
<tr>
<td>• Cisco Video Surveillance Safety and Security Desktop User Guide</td>
<td></td>
</tr>
</tbody>
</table>

Summary Steps

The following summarizes the main steps to generate the luminance metadata and view motion events. See “Motion Video Search Detailed Procedure” for more information.

1. Complete the “Requirements”.
2. Select Forensic Analysis > Motion Analysis > Motion Video Search to open the Stage 1 window.
3. Drag and drop a camera onto the pop-up window.
4. Select a span of recorded video.
5. Click Next to generate the luminance metadata for the video, if necessary.

Tip
Only one metadata request is allowed per camera at a time in this release. Wait until the metadata generation is complete before submitting a new request for that camera. See the “Metadata Job Management” section on page 117 for more information.

6. In the Stage 2 window, select a span of time for the motion search (at least part of the recording must have metadata).

7. Select the parts of the video to analyze, and the motion sensitivity and threshold.

8. Click Next to continue to Stage 3 and process the motion search results.

9. Click the motion thumbnails (which display the number of motion events detected) to view video from the motion events.

Motion Video Search Detailed Procedure

To generate luminance metadata for a recording, define the motion detection filters, and view the resulting motion events, do the following.

Procedure

Step 1
Log in to the Cisco SASD application.
- See “Logging In”.
- Motion Video Analysis is not supported using the Cisco SASD Advanced Video Player or Cisco SASD Federator applications.

Step 2
Select Forensic Analysis > Motion Analysis > Motion Video Search (Figure 1).

Step 3
Drag and drop a camera onto the Motion Video Analysis window (Figure 1).

Note
An error message appears if a camera the Luminance metadata track is not configured on the camera (using the Operations Manager). See “Requirements” for more information.
Step 4  Stage 1: Generate the \textit{luminance} metadata:

In Stage 1, select a span of recorded video and generate the \textit{luminance} metadata used to detect motion events.

- See “Understanding Luminance Metadata and Motion Analysis” for more information.
- Only one metadata request is allowed per camera at a time in this release. Wait until the metadata generation is complete before submitting a new request for that camera. See the “Metadata Job Management” section on page 117 for more information.
- Up to 5 metadata jobs can run at a time. Additional jobs are queued and begin when another job is completed, fails or is cancelled.

a. Select a recording span using the Recording Full Range, Detail Range, and Selected Range fields (Figure 2).
Figure 2 Stage 1: Generating Metadata

1. The camera and stream (source) for the video recording.

Note: Only the primary stream is supported in this release.

2. Recording Full Range—The entire recording range available on the camera. The selected span of time on Recording Full Range will define the Detail timeline's entire duration.

   Drag the orange bars right and left to select a sub-set of the available recording. Click and drag the middle of the bar right or left to adjust the selection.

   - Start—the beginning timestamp of the first available recording.
   - Duration—the entire duration of video available on the camera.
   - End—the end timestamp of the most recent recording available on the camera.

   For example, a continuous recording that is configured to retain recordings for one day will display a duration of 01:00:00:00 (Day:hours:minutes:seconds). The start and end times indicate the beginning and end of the available recording.

3. Detail Range—The time range selected in the Recording Full Range. Use the Detail Range to fine-tune the video time span that will be analyzed for motion.

   Drag the orange bars right and left. Click and drag the middle of the bar right or left to adjust the selection.

   For example, if an hour of video was selected, click and drag the orange bars in the Detail Range to reduce the time range to 55 minutes.
4 Selected Range—The start and end timestamps for the video that will be analyzed for motion. Enter different values to micro-tune your selection.

Tip For example, you can edit the beginning and ending seconds.

5 Recording video feed from the selected camera stream. Use this preview to verify you have selected the correct camera.

6 Click Next to generate analytics metadata and continue to Stage 2.

- If metadata is not available for all or part of the selected recording range, you will be prompted to confirm that metadata should be created.
- If your selection includes partial metadata, you will be prompted to complete the metadata, or continue to motion analysis.
- If metadata is available for the entire range, the Stage 2 window appears.

Note Metadata is used to locate motion in the video. See the “Understanding Luminance Metadata and Motion Analysis” section on page 104.

7 Legend—Describes the recording status in the timeline.

- Green—Video recording is available. Gaps in the green bar indicate times when video was not recorded.
- Blue—Metadata was generated and is available for motion analysis.
- Grey—The video span(s) where metadata is being created by the Cisco Metadata server. When metadata is generated, the grey bar turns blue.

Tip See the “Metadata Job Management” section on page 117 for instructions to view the status of metadata creation.

- Red—Resolution change. Indicates if the resolution of the recording changed, which can occur if the camera template and/or template recording settings were modified. You cannot select a time span that includes a resolution change (an error occurs when you attempt to proceed to Stage 2). Select a time span where the recording resolution is the same for the entire span.

8 Green—Recorded video.

9 Grey—Metadata is currently being generated.

See the “Metadata Job Management” section on page 117 for information on job status.

10 Blue—Metadata was successfully generated.

b. Click Next and do one of the following:

- If all of the selected time span includes metadata (generated in a previous session), skip to Step 5.
- If a time span with no metadata was selected:
  - Click OK to confirm that metadata should be created.
  - (Optional) Select Forensic Analysis > Motion Analysis > Metadata Job Management to verify that the metadata job was successfully started (see Figure 7).
  - Click Next again to proceed to Stage 2 (see Step 5). You can proceed even if the metadata generation is not complete.

Note You can proceed to Stage 2 (Step 5) if a portion of the selected recording has metadata (blue bar), but you cannot proceed if there is no metadata in the selected time span.

- If part of the selected time span includes previously created metadata (blue bar), you are prompted to either generate metadata for the remainder of the selected video, or proceed directly to the analysis window (Figure 3).
Step 5  Stage 2: Define the motion areas, sensitivity, and threshold.

These settings determine how motion should be defined within the video frame.

a. Select a recording time range (that includes metadata) where you want to apply the motion settings.
   - You cannot continue unless a portion of the selected recording has metadata. To generate metadata, return to Stage 1 (Step 4).
   - See Figure 2 for more information about using the settings to select and fine-tune the time range selection.

b. Select a **Sensitivity** level (**High** or **Low**) and click the area of interest to paint a grid that should detect motion.
   - **Low**—grids with low sensitivity are painted green. To trigger motion detection for a low sensitivity grid, large luminance value changes are required on the entire area of the grid.
   - **High**—grids with high sensitivity are painted red. To trigger motion detection for a high sensitivity grid, small luminance value changes are required on only part of the grid.

See Figure 4 for more information.
c. Select the Threshold—Slide the selector to a number from 1 to 100. Threshold applies to all of the selected grids, and represents the percentage of grids that must be triggered for a motion event to be recorded.

For example, a threshold of 20 means that 20% of the grids must be detected motion in order to trigger a motion event. A threshold of 100 means that all of the grids must detect motion in order to trigger a motion event. A threshold of 1 means only 1% percent of the grids detected motion in order to trigger a motion event, which means motion event is triggered if any grid detected motion.

Figure 4 Stage 2: Defining the Motion Detection Settings

1 Time range selectors—Select and fine-tune the recording time span that will be analyzed for motion.

Tip See Figure 2 for more information about using the Recording Full Range, Detail Range and Selected Range.

2 Sensitivity—Select High or Low and click the area of interest to paint a grid that should detect motion.

- **Low**—grids with low sensitivity are painted green. To trigger motion detection for a low sensitivity grid, large luminance value changes are required on the entire area of the grid.
- **High**—grids with high sensitivity are painted red. To trigger motion detection for a high sensitivity grid, small luminance value changes are required on only part of the grid.

3 Threshold—The percentage of selected grids that must detect motion for a motion event to occur.

4 Motion grid—Click a grid or click and drag multiple grids to select the areas of the video frame that will detect motion. High sensitivity areas appear in red. Low sensitivity areas are green.

5 Click Next to view the motion detection results.
Tools to assist in grid selection

<table>
<thead>
<tr>
<th>Paint All</th>
<th>Paints all of the grids with low or high detection (depending on the sensitivity selected).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Erase All</td>
<td>Deselects all grids. No grids will detect motion.</td>
</tr>
<tr>
<td>Invert All</td>
<td>Invert all the painted area to be not painted. Unpainted areas are changed to painted.</td>
</tr>
</tbody>
</table>

6. Click **Next** to view the motion results.

**Note**
You cannot continue unless a portion of the selected recording has metadata. To generate metadata, return to Stage 1 (Step 4). Also, motion analysis is not supported if you selected a time range during which recording stream has resolution change.

**Step 6** View the motion events for the select recording (Figure 5).

- **a.** Wait for the motion event generation to complete (thumbnail groups display “Processing” if the video is still being analyzed).

**Tip**
- Results are displayed in 24 thumbnail groups. The time included in each group is evenly divided based on the select time duration.
- The number of motion events in each group is indicated by a large number on the video image.
- Unprocessed times display a “Processing” thumbnail and green status bar.
- See Figure 5 for additional details and descriptions of the available options.

- **b.** Click the **icon** in a thumbnail group to view and play the individual events for that group (see Figure 6).
- **c.** Click **Play Motion Summary** to play all motion event video together.
- **d.** Click **Root** to return to the top level thumbnail group.
- **e.** (Optional) Click **New Search** to return to Stage 2 (Step 5) and change the filters or time span used in the analysis.
Figure 5 Stage 3: Motion Analysis Results (Root Level)

1. The camera and stream (source) for the video recording.
   
   **Note** Only the primary stream is supported in this release.

2. Analysis Full Range—The entire range of recorded video that was selected in Stage 2 (see Step 5).
   The motion results are displayed for this range by default. Drag the orange bars right and left to display results for a sub-set of the available recording. Click and drag the middle of the bar to adjust the selection.

3. Blue markers—The motion events discovered in the video based on the filters applied in Stage 2 (see Step 5).

4. Detail Range—The time range selected in the Analysis Full Range.
   (Optional) Drag the orange bars right and left to fine-tune the results that are displayed. Click and drag the middle of the bar right or left to adjust the selection.

5. Selected Range—(Optional) Enter different values to micro-tune your selection.
   
   **Tip** For example, you can edit the beginning and ending seconds.

6. The root level of results. When viewing a sub-set of results, click **Root** to return to the top level.
Chapter 6
Motion Analysis

Motion Video Search Detailed Procedure

Step 7
Use the options described in Figure 6 to view recorded video from specific motion events.

Tip
If a thumbnail group includes more than 24 motion events, an additional layer of thumbnails is displayed. Click to display the next layer of detailed thumbnails. Click Root to navigate to a higher level.
Figure 6  Stage 3: Motion Analysis Results (Detail Level)

1. The time span for the motion events being viewed.
2. Blue bar—Motion events
3. Red triangle—The location of the video currently being played.
4. Root—Click Root to return to the higher level thumbnails.
5. Motion thumbnail—An individual motion event. Click the thumbnail to play the event video. Double click to play the video in a larger window.
6. Video playback controls. See “Controlling Video Playback” for more information.
7. Start and end times of the motion event video.
8. Play icon. Click to play the motion event from the motion start to motion stop time.
9. Video pop-up. Double-click a thumbnail image to play the event video in a larger window. See “Controlling Video Playback” for more information about recorded video controls and options.
### Motion Video Search Detailed Procedure

| Step 8 | Use the embedded video controls to navigate through the recorded video, save video clips, or capture still images. See “Viewing Recorded Video” and “Managing Video Clips” for more information. |

- **Play Motion Summary**—Plays the motion event video for the events included in the group.
- **Play Continuous Video**—Plays all video for the selected duration, including video that does not include motion events.
Metadata Job Management

Select **Forensic Analysis > Motion Analysis > Metadata Job Management** (Figure 7) to view the status of metadata jobs triggered in the Motion Video Analysis window.

- (Optional) Click , select a camera, and click **Apply** to display only metadata jobs for recordings from that device.
- (Optional) Select one or more users to narrow the results to the user(s) that triggered the jobs.
- (Optional) Select a job and click **Cancel** to cancel the metadata job.

**Figure 7**  Metadata Job Management

**Usage Notes**
- Up to 5 metadata jobs can run at a time. Additional jobs are queued and begin when another job is completed, fails, or is cancelled.
- Only one metadata request is allowed per camera at a time. Wait until the metadata generation is complete for that camera before submitting a new request for the same device.

**Job Information**
Metadata jobs include the following information:
- Name—The camera that created the recording.
- Start Time—The start time of the metadata generation job.
- End Time—The end time of the metadata generation job.
- Progress—The percentage of the job that has been completed.
- Status—The current job status (for example, started, completed, or failed).
- Owner—The Cisco VSM user who initiated the job.
Metadata Job Management
Using the Cisco VSM Federator

Cisco SASD Federator allows users to monitor video from multiple Operations Managers.

Note
Federator resources, such as the Regions that map an Operations Manager location to a Federator location, are configured using the browser-based Cisco VSM Federator interface. Use this browser-based interface to also view the system health of the Operation Manager servers. See your system administrator for more information.

Contents
Refer to the following topics for more information:

- Federator Overview, page 120
- Federator Requirements, page 121
- Logging In to Cisco SASD Federator, page 122
- Monitoring Video Using Federator, page 123
- Monitoring Alerts Using the Cisco SASD Federator, page 125
Federator Overview

The Cisco SASD Federator allows users to view video from multiple Operations Managers (Figure 1).

**Note**
- The Federator resources and regions are configured using the Cisco VSM Federator browser-based interface.
- Federator users are provided access to Operations Manager locations based on their access permissions in Federator.
- Each Federator supports up to 500 Operations Managers.

**Figure 1** Cisco SASD Federator

To monitor system health for all Operations Managers (and associated devices, such as Media Servers, cameras and encoders), use the browser-based Federator interface. See the Cisco Video Surveillance Operations Manager User Guide for more information.
Example
For example:

- A company has warehouse facilities in different regions of the country. Each facility includes an Operations Manager that manages multiple Media Servers and related cameras. Currently, users must log in to each Operations Manager separately to view video for each site. Federator, however, allows central office users to log in to Cisco SASD Federator and simultaneously access video from the Operations Managers in multiple warehouses.

- Another company manages casinos in different regions of the country. Cisco SASD Federator can be used to monitor video in all regions. For example:
  - Security personnel can monitor video from the casino floors in different locations, even through each location has a separate Operations Manager.
  - Financial managers can monitor video only from the cashier booths at all casinos.

Capacity
Each Federator server supports the following:

- 500 Operations Manager servers
- 2000 regions
- 200 client workstations

Federator Requirements

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Complete?</th>
</tr>
</thead>
<tbody>
<tr>
<td>At least one Federator server must be installed and configured on the network.</td>
<td>☐</td>
</tr>
</tbody>
</table>

Note The Federator server must be configured with “Regions” which map the Operations Manager locations to the Federator locations. See your system administrator for more information.

The IP address or hostname of the Federator server. | ☐ |
Logging In to Cisco SASD Federator

Logging in to Cisco SASD Federator is similar to logging in to Cisco SASD. Launch the Cisco SASD Federator application, enter the Federator server IP address or hostname, and your Federator username and password.


**Notes**
- The default credentials are `admin/admin`.
- The username and initial password for all other users is defined when the user account is created (see the Cisco Video Surveillance Operations Manager User Guide for more information).
- The first time you log in, you must use the browser-based Federator interface to change your password (you will be prompted to change a new password on first login).
- Users are required to select a domain if their credentials are authenticated using an external database, such as an LDAP server.
- If Dual Login is enabled, a second user must also enter their credentials to approve the login (see “Understanding Login Approval” in the Cisco Video Surveillance Safety and Security Desktop User Guide).
- Federator servers do not use Sites or Dynamic Proxies, and Federator users are not prompted to select a Site.

---

**Table 11-1 Federator Requirements (continued)**

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Complete?</th>
</tr>
</thead>
<tbody>
<tr>
<td>A valid Federator server username and password.</td>
<td>☑</td>
</tr>
</tbody>
</table>

**Notes**
- The default credentials for a new or factory restored server is `admin/admin`.
- The username and initial password for all other users is defined when the user account is created (see the Cisco Video Surveillance Operations Manager User Guide for more information).
- The first time you log in, you must use the browser-based Federator interface to change your password (you will be prompted to change a new password on first login).

The Cisco SASD Federator application installed on the monitoring workstation.


**Notes**
- The Federator resources (video) can be monitored using the following applications:
  - The Cisco SASD Federator desktop application (described in this document).
  - The browser-based monitoring tool (see the Cisco Video Surveillance Operations Manager User Guide for more information).
Note

Cisco SASD Federator user accounts are different than Cisco SASD user account. You cannot use Cisco SASD credentials to access the Federator.

Login Procedure

Step 1
Launch the Cisco SASD Federator application on your Windows computer.
- The first time you log in, you must use the browser-based Federator interface to change your password (you will be prompted to change a new password on first login).

Step 2
Enter the Federator hostname or IP address.

Step 3
Enter your Federator username and password.
  a. Select a Domain, if necessary.
  b. Enter a new password, if prompted.
  c. If prompted, ask your manager or other administrator to enter their “Approver Login”

Monitoring Video Using Federator

Federator users can access video streams from the Operations Manager locations included in their access permissions. Access permissions are a combination of the following:

- The access permissions included in the Federator User Groups to which they belong. For example, View Live Video or View Recordings.
- The Federator location associated with the Federator User Groups to which they belong. For example, User Groups with access to the root location can access all Operations Managers configured on the Federator. User Groups with access to a sub-location, can view the video streams for Operations Managers at that location and lower.
- The Operations Manager locations that are mapped to the Federator locations (using “Regions”). Regions can map to all Operations Manager locations (root) or a sub-location.

Usage Notes

- Federator users can view video from different Operations Managers in a single layout by dragging and dropping cameras in the video display grid.
- Federator users can load the Views defined in the Operations Managers.
- The Operations Manager default layouts are available in Federator.
- You can create video clips using Cisco SASD Federator.
- To use the camera search, you must first select a region. Camera search is not supported across multiple Operations Managers.
Chapter 4 Using the Cisco VSM Federator

Monitoring Video Using Federator

Procedure

**Step 1** Log in to the Cisco SASD Federator application.
- See the “Logging In to Cisco SASD Federator” section on page 122 for more information.

**Step 2** Select a Federator location (Figure 2).
Locations display the cameras for the associated Operations Manager locations (based on the Federator Regions).

**Step 3** (Optional) Use the search field to search for a camera name (such as **Lobby Camera**).
To search for cameras, you must first select a location.

**Step 4** (Optional) Select a layout (such as 2x2).

**Step 5** Drag-and-drop cameras onto the available video panes to display video from the camera.

*Figure 2 Monitoring Video in Cisco SASD Federator*

**Step 6** (Optional) Select a View that was configured on the Operations Manager.
Monitoring Alerts Using the Cisco SASD Federator

Overview

The Cisco SASD Federator displays two types of alerts:

- Federator device health alerts—health alerts generated by the Federator server.
- Operations Manager health and security alerts—alerts forwarded by the Operations Managers to the Cisco SASD Federator. See “Sending Operations Manager Alerts to Cisco SASD Federator” for more information.

Note

Cisco SASD Federator can display security events (such as motion or contact events), Federator device health events and Operation Managers reachability alerts. The browser-based Federator Health Dashboard displays only device health events (see the Cisco Video Surveillance Safety and Security Desktop User Guide for more information).

Step 7  (Optional) Select Forensic Analysis > Clip Management to view, download, and manage MP4 clips saved on the server.

See “Clip Management” for more information.

Step 8  (Optional) Select Forensic Analysis > Thumbnail Search to quickly locate specific scenes or events in recorded video.

See “Thumbnail Search” for more information.
## Sending Operations Manager Alerts to Cisco SASD Federator

Alerts generated by an Operations Manager can be viewed by Cisco SASD Federator users if they are sent to the Federator server using one of the following methods:

### Table 2   Methods to Send Alerts to the Federator

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device health alerts (automatic)</td>
<td>Cisco SASD Federator device health alerts.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Only Operations Manager reachability alerts are displayed in the Cisco SASD Federator.</td>
</tr>
<tr>
<td>Security alerts (automatic)</td>
<td>Security alerts can be automatically sent to the Cisco SASD Federator when an event occurs.</td>
</tr>
<tr>
<td><strong>Tip</strong></td>
<td>Create an Advanced Event in the Operations Manager (Figure 3) that automatically sends alerts to Cisco SASD Federator when an event occurs (for example, when motion stops or starts). See the Cisco Video Surveillance Operations Manager User Guide for more information.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>When the Operations Manager is configured to always create alerts and to also send alerts to Cisco SASD Federator according to a schedule, the alerts will continue to be updated with new events even if the scheduled time is past. Updates continue until there are 100 events in the alert or when a gap of 30 minutes between the events occurs.</td>
</tr>
<tr>
<td>Manually send alerts to the Cisco SASD Federator</td>
<td>Right-click the alert in Cisco SASD and select <strong>Send to Federator</strong> (Figure 4).</td>
</tr>
</tbody>
</table>

### Note

When a camera is configured for stream redundancy (for example, stream 1 to the primary Cisco Media Server and stream 2 to a redundant server), events from both streams are added to the same alert.

### Tip

See “Understanding Events and Alerts” in the Cisco Video Surveillance Safety and Security Desktop User Guide to understand the difference between health and security alerts.
For example, in Figure 3 an Advanced Event is created that automatically sends an alert to the Federator when a motion event occurs.

**Figure 3  Cisco SASD Federator**

In Figure 4, Cisco SASD is used to manually send an event to the Federator.

**Figure 4  Manually Send Alerts to Federator Using Cisco SASD**
Viewing Alerts

Procedure

**Step 1** Launch the Cisco SASD Federator application and log in using your Cisco SASD Federator credentials.

* Note  The Federator username and password are different than the Cisco SASD or Cisco SASD Advanced Video Player credentials. See your system administrator for more information.

**Step 2** Select the Alert workspace (Figure 5).


**Step 3** Select an alert to view the events related to that alert.

**Figure 5  Cisco SASD Federator Alert Workspace**

**Step 4** Select a dynamic or static view:

- **Search**—Display alerts in a static list based on the filter criteria (including a time span). The search results do not auto-refresh. Re-search the alerts to view current results.
- **Dynamic Filter**—Display alerts in an auto-updating list based on the filter criteria (such as location, alert type and severity). Click the lock icon to stop or start auto-updates
  - When unlocked, new alerts will be added to the list as they occur.
- When locked, dynamic updating is paused and only the currently displayed alerts are shown. Unlock the display to refresh the results.

**Step 5** (Optional) Select the filter criteria and click **Apply** (Figure 6).

- **Location**—Click to select a Federator location (Figure 6) where the alert(s) were created. Only alerts from that location will be displayed.

  **Note** Federator Locations represent a location tree on an Operations Manager.

- **Device**—Click to select a location and a specific device (camera). Only alerts from that device will be displayed.

- **Time**—(Search only). Select a span of time. Only alerts that were generated during that time are displayed. For example, Today or Month.

- **Alert Type**—Health or Security. See “Understanding Events and Alerts” in the Cisco Video Surveillance Safety and Security Desktop User Guide for more information.

- **Alert Severity**—Select CRITICAL, MAJOR, MINOR, WARNING, or INFO.

- **Status**—Acknowledged, Closed or New.

- **Acknowledged By**—Enter the full or partial name of the user who acknowledged the alert.

- **Closed By**—Enter the full or partial name of the user who acknowledged the alert.

**Figure 6** *Cisco SASD Federator Locations*

**Step 6** (Optional) Right-click an alert to:

- Change the alert status (acknowledge, close or re-open the alert).
• Add a comment to the alert or mark it as a false alarm.

**Step 7**  (Optional) Double-click the event to open a dual-pane pop-up window with live and event video (if available).

**Step 8**  (Optional) If the URL icon 🌐 appears, right-click the event to open a new web browser with additional information or images. See “Viewing Event URLs” in the Cisco Video Surveillance Safety and Security Desktop User Guide for more information.

**Step 9**  Use the additional tools to view and manage alerts as described in “Alert Workspace”.
Related Documentation

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

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

<table>
<thead>
<tr>
<th>Release</th>
<th>Document Revision Date</th>
<th>Change Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 7.0.0</td>
<td>January, 2013</td>
<td>Initial draft.</td>
</tr>
</tbody>
</table>
| Release 7.0.1 | March, 2013 | - Added overview information and user-interface (UI) enhancements to “Viewing Alerts”, including the following new and revised topics:  
  - “Understanding Events and Alerts”  
  - “Alert Workspace”  
  - “Viewing Event URLs”  
  - “Summary of Events and Corresponding Alerts”  
- Added user-interface (UI) enhancements to “Viewing Cameras and Alerts on Map”.  
- Added a “Configuring Unattended Windows” section, including:  
  - “Launching the Unattended Windows”  
  - “Understanding Offline Mode”  
- Various minor edits and revisions.  
- Revised the “Related Documentation” section. |
| Release 7.2 | August, 2013 | - Added the “Viewing a Thumbnail Summary of Video Archives” section on page 1.  
- Various minor edits and revisions. |
Add the following sections and topics:
- Getting Started, page 1
- Wall Workspace, page 25
- Using the Cisco SASD Wall Configurator, page 29
- Clip Management, page 99
- Motion Analysis, page 103
- Using the Cisco VSM Federator, page 119

Revised the following sections and topics:
- Video Workspace, page 19
- Alert Workspace, page 37
- Map Workspace, page 51
- Controlling Video Playback, page 57
- Thumbnail Search, page 93
- Related Documentation, page 131

Added note regarding the limit of 48 video panes per workstation.