Cisco Video Surveillance Manager Safety and Security Desktop User Guide

Release 7.6
December, 2014

Cisco Systems, Inc.
www.cisco.com

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2014 Cisco Systems, Inc. All rights reserved.

Preface

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:

Convention	Indication
bold font	Commands and keywords and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.

{x | y | z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`courier` font	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

Warning **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 7
- Video Viewing Applications, page 8
- Requirements, page 9
- Installing the Application Suite, page 10
  - Installing the Cisco SASD Application Suite, page 10
  - Installing the Cisco SASD Advanced Video Player, page 11
- Logging In, page 13
  - Understanding Sites, page 16
  - Understanding Login Approval, page 18
  - Default User Accounts and Passwords, page 18
  - Changing Your Password, page 19
- Understanding Maintenance Mode, page 20

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 10 for more information.

Table 1 Cisco SASD Applications

Application	Description	More Information
Cisco SASD	A full-featured monitoring application that provides access to the cameras and video from a single Operations Manager. Cisco SASD includes the following workspaces and features: • Video workspace • Wall workspace • Alert workspace • Maps workspace • Forensic Analysis Tools	**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
Cisco SASD Advanced Video Player	An advanced monitoring application that includes the following monitoring workspaces: • Video workspace • Wall workspace	**Video Monitoring** • Controlling Video Playback **Workspaces** • 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

Table 1 Cisco SASD Applications (continued)

Application	Description	More Information
Cisco SASD Wall Configurator	A utility for adding and modifying the video Walls that can be selected and displayed in the monitoring workstations.	**Overview** Using the Cisco SASD Wall Configurator
Cisco SASD Federator	A monitoring application that allows Federator users to monitor video from multiple Operations Managers.	**Overview** Using the Cisco VSM Federator **Workspaces** • Video Workspace • Alert Workspace **Video Monitoring** • Controlling Video Playback **Forensic Analysis Tools** • Thumbnail Search • Clip Management

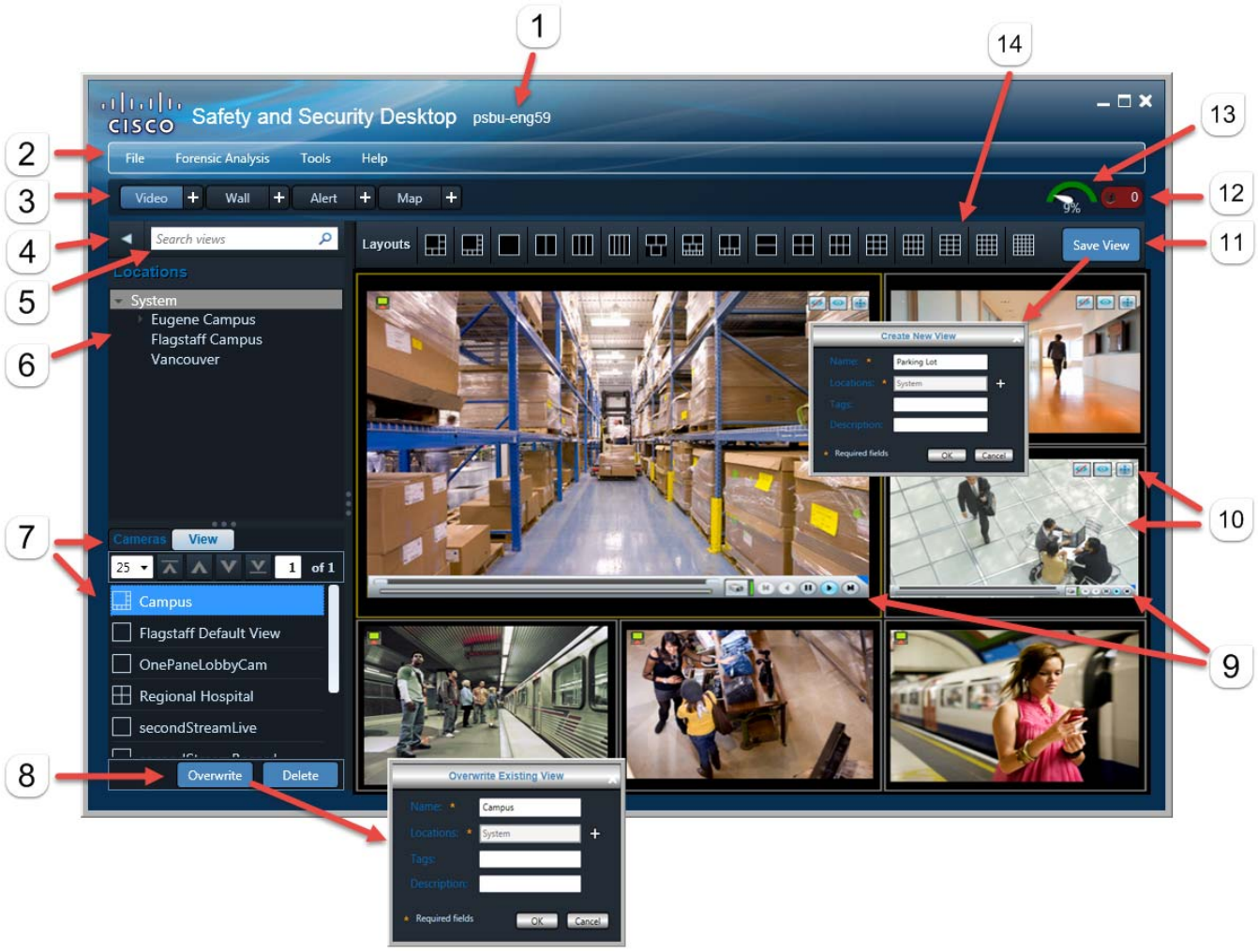
Main Features of the Cisco SASD Application

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.

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. – **Camera Recording Management**—Use *Recording Management* to view the recordings available on a camera's local storage device (such as an SD card), and copy them to the Cisco Media Server. • **Tools**—Select **Tools > Options** to select if video should appear in a pop-up window or enlarge within the viewing window when you double-click a video pane. • **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 a grid. Views can be saved or edited using the Video workspace only. See "Video Workspace" for more information. • **Wall**—Display Video Walls. Walls are pre-defined *Views* that can be displayed on multiple workstations. 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. 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 dragable 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	**Camera** and **View** tabs. • **Camera**—Select the **Camera** tab to view the available cameras based on the location or search. Double-click or drag & drop the camera to the video area. See Video Workspace, page 21 for more information. • **View**—Select the **View** tab to view the pre-defined camera matrix. Double-click or drag & drop the View to the video area. Views can be modified using the Video workspace, or configured to automatically rotate using the Operations Manager interface. See Saving a Video "View" (Multi-Pane Grid), page 26.

8	**Overwrite** and **Delete**—(Video workspace only) Allows you to overwrite the settings for a view (such as the camera or stream displayed in a pane). See Saving a Video "View" (Multi-Pane Grid), page 26.
9	Playback Controls—See "Controlling Video Playback".
10	Viewing Pane and control icons—See "Controlling Video Playback".
11	**Save View**—(Video workspace only) Saves a layout so it can be selected using the **View** tab. • For new views only. To modify an existing view, use the **Overwrite** button. • Views can be assigned to the same location as the cameras, or to a higher level location. • Only users assigned to a user group with this location can access the View.
12	Notifications—Notify errors, such as task or software exceptions.
13	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 to view network and memory usage details.
14	**Layouts**—Create a blank matrix from the available layouts and drag cameras onto each viewing pane. See "Saving a Video "View" (Multi-Pane Grid)".

Understanding the Video Viewing Options

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

Table 2 Video Viewing Options

Viewing Mode	Description	More Information
Single Camera	View video from a single camera based on a location, alert or map.	• Video Workspace • Alert Workspace • Map Workspace
Multiple Cameras	View a multi-pane matrix of live or recorded video.	• Video Workspace • Wall Workspace
Video Walls	View the same video pane matrix on multiple workstations.	• Wall Workspace • Using the Cisco SASD Wall Configurator
Unattended Mode	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.	Using the Cisco SASD Wall Configurator
Alerts and Events	Display recorded video for an event. You can also view live video from the same camera.	• Playing Event Video
Forensic Analysis	Use the analysis tools for the following: • 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. • Use *Clip Management* to view, download and delete MP4 clips. that are stored on the server. • Use *Motion Analysis* to view a summary of motion events for recorded video.	• Thumbnail Search • Clip Management • Motion Analysis

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

Viewing Tool	Application	Description	Documentation
Desktop monitoring application	Cisco Video Surveillance Safety and Security Desktop (Cisco SASD)	• Allows simultaneous viewing of up to 25 cameras per Workspace, and up to 48 cameras per workstation. • Create Video Matrix windows for display in separate monitors. • View Video Walls. • Create unattended workstations. • View and manage alerts. • View cameras, video, and alerts based on a graphical map.	• Cisco Video Surveillance Safety and Security Desktop User Guide • "Understanding the Cisco SASD Application Suite"
Web-based configuration and monitoring tool	Cisco Video Surveillance Operations Manager (Operations Manager)	• Allows simultaneous viewing of multiple video panes: – View up to 4 cameras with the 32-bit version of Internet Explorer. – View up to 25 cameras with the 64-bit version of Internet Explorer. • Add the users, Views and Video Walls available in the desktop Cisco SASD application. • Configure the camera, streams and recording schedules.	Cisco Video Surveillance Operations Manager User Guide

Table 3 Summary of Cisco Video Viewing Options (continued)

Viewing Tool	Application	Description	Documentation
Desktop video clip player	Cisco Video Surveillance Review Player (Cisco Review Player)	Simple player used to view video clip files.	Cisco Video Surveillance Review Player
Web-based server console	Cisco Video Surveillance Management Console (Cisco VSM Management Console)	Provides basic viewing features for a single stream (Stream A) from a single camera.	Cisco Video Surveillance Management Console Administration Guide

Requirements

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

Table 4 Cisco SASD Requirements

Requirements	Requirement Complete? (✓)
At least one Cisco VSM server must be installed on the network with the following services enabled: • Cisco Media Server • Cisco Video Surveillance Operations Manager Additional services are required to enable features such as the location maps and Video Motion Search. See the following documentation for more information: • Cisco Physical Security Multiservices Platform Series User Guide—physically install the server. • Cisco Video Surveillance Management Console Administration Guide—enable the Operations Manager service. • Cisco Video Surveillance Operations Manager User Guide— Add servers and enable server services. Configure network and analog cameras to stream live and recorded video.	❑
At least one camera physically installed and configured on Operations Manager.	❑
The IP address or hostname of the Cisco Video Surveillance system (same as the Operations Manager).	❑
A valid Cisco Video Surveillance username and password. See the Cisco Video Surveillance Operations Manager User Guide for instructions to configure users and access permissions.	❑

Table 4 Cisco SASD Requirements (continued)

Requirements	Requirement Complete? (✓)
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 (32-bit or 64-bit) or Windows 8 (64-bit). • The Microsoft .NET Framework 4.0 (full setup) must be installed on the client PC. Go to http://www.microsoft.com/en-us/download/confirmation.aspx?id=17851 to download the installer. • 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

The Cisco SASD Advanced Video Player installer is downloaded from the browser-based Operations Manager (**Operations** tab).

All other Cisco SASD applications can be downloaded from the cisco.com download page, as described below.

- Installing the Cisco SASD Application Suite, page 10
- Installing the Cisco SASD Advanced Video Player, page 11

Installing the Cisco SASD Application Suite

All Cisco SASD applications can be downloaded from the cisco.com website. This includes all components described in the Understanding the Cisco SASD Application Suite, page 2.

Procedure

Step 1 Go to the Cisco Video Surveillance Manager product page.

Step 2 Click Download Software.

Step 3 Select **Video Surveillance Manager Stand-alone Tools**.

Step 4 Select the release.

Step 5 Select the Cisco Video Surveillance Safety and Security Desktop application.

Step 6 Click **Download Software** next to the software package and follow the on-screen instructions.

Step 7 Locate and launch the installation file, and follow the onscreen instructions.

Step 8 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.

Installing the Cisco SASD Advanced Video Player

The Cisco SASD Advanced Video Player application can also be downloaded from the browser-based Operations Manager.

Procedure

Step 1 Log in to the Cisco VSM browser-based Operations Manager.

a. Launch Internet Explorer on your Windows 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 2 Select the **Operations** tab (Figure 2).

Figure 2 Downloading the Cisco SASD Advanced Video Player Installer from the Operations Manager

Step 3 Click **Advanced Video Player** (under the *Software* heading).

Step 4 Follow the onscreen instructions to complete the installation.

Step 5 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, go to **Start > SASD Video Player**.
- You can also 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 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).

Figure 3 Login to Cisco SASD

Note

- The first time you log in, you must use the browser-based 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 18 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).

Figure 6 Selecting a Site on First Login

- 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.

Figure 7 Login Approval

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 5 Default User Accounts

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

Changing Your Password

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

Procedure

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

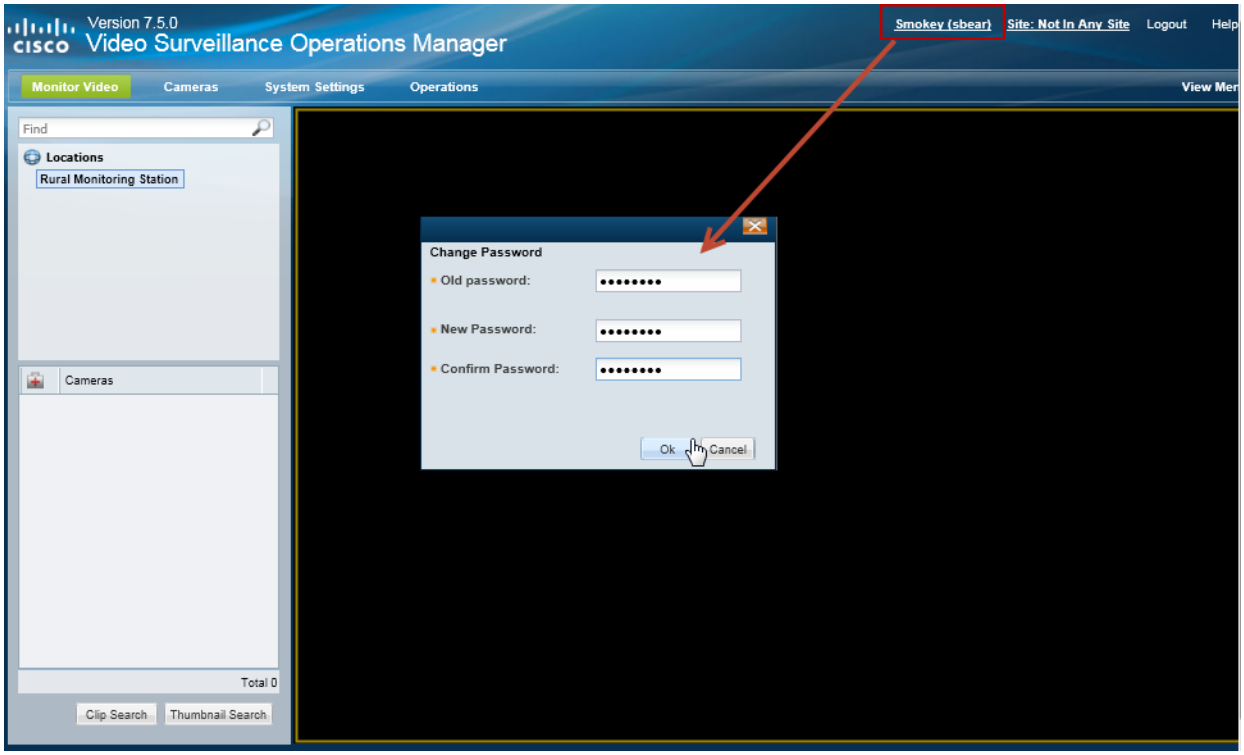
Step 2 Enter the same IP address/hostname used to access Cisco SASD.

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 Video Surveillance Operations Manager.

Step 5 Enter and reenter your new password.

Figure 8 Changing Your Password Using Operations Manager



Understanding Maintenance Mode

Maintenance mode is a read-only mode that allows user to access live and recorded video but locks most configuration changes while other system features are implemented. For example, you cannot save or modify views, or acknowledge alerts.

When maintenance mode is on, a white and red banner appears at the top of the page.

Figure 1-9 Maintenance Mode is ON

Video Workspace

Use the Video workspace to monitor video from a single camera, or from multiple cameras in a grid layout. Refer to the following topics for more information.

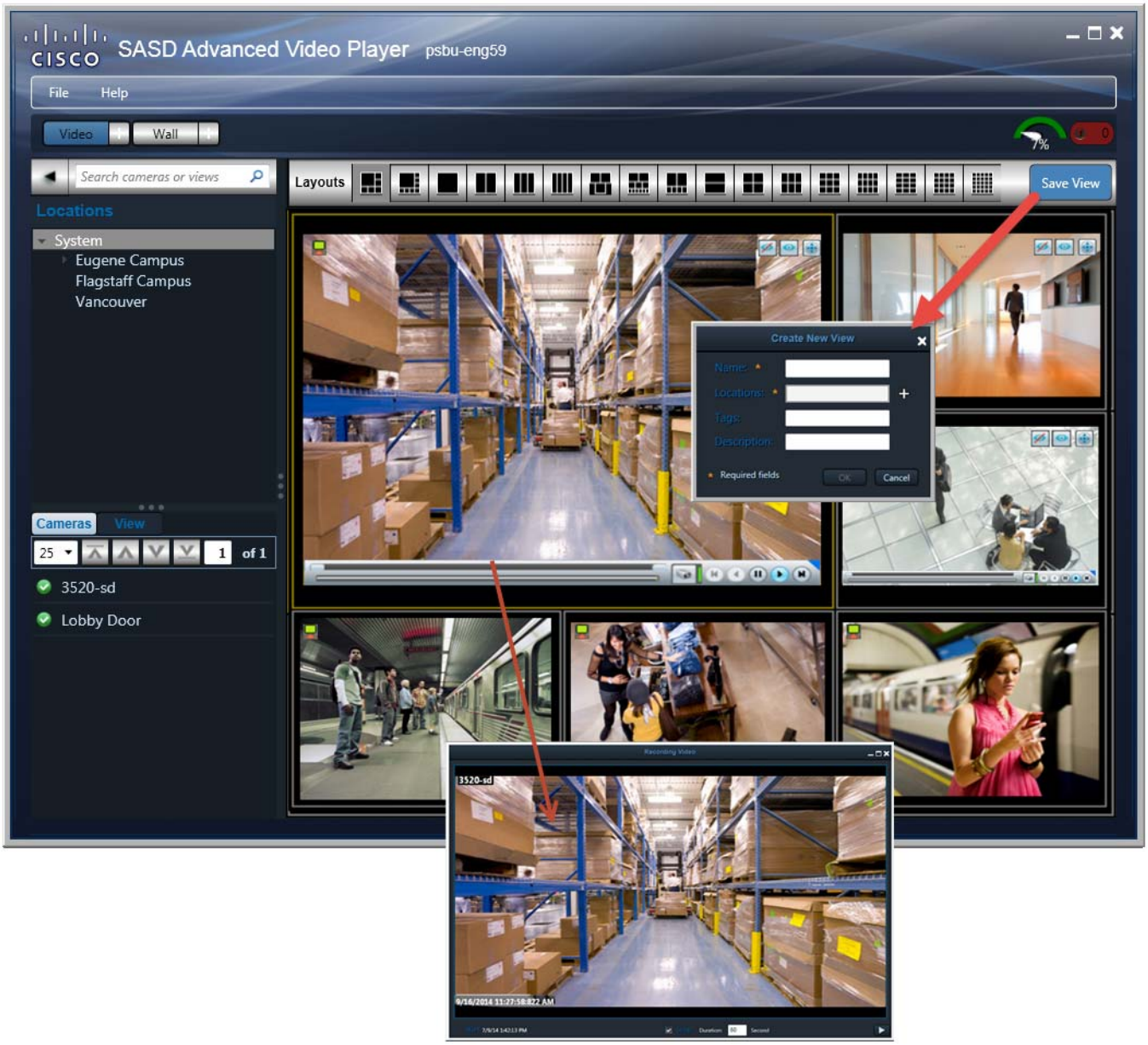
Contents

- Overview, page 22
- Saving a Video “View” (Multi-Pane Grid), page 26
- Displaying a Duplicate Workspace on a Separate Monitor, page 28

Overview

Select the **Video** workspace (Figure 1) to view video from the cameras in your Cisco Video Surveillance deployment.

Figure 1 Overview of the Video Workspace



For example:

- Drag and drop a camera name onto a viewing pane to view video from that camera. See Controlling Video Playback, page 65 to view recorded video, create clips, control camera PTZ movements, and use the other video viewing features available in each video pane.

- Select a layout and drag and drop cameras to each pane in the layout to view video from multiple cameras in a grid.
- Click **Save View** to save the layout for future viewing. You can save views with live video, and each pane can display the video from the live primary or secondary stream for that camera. To modify a view, click the **Overwrite** button.
- Click the **Views** tab to select a previously-saved views, including rotating views that were configured using the Cisco Video Surveillance Operations Manager. Double-click any pane to enlarge the video or open it in a pop-up window.

Procedure

Step 1 Select the **Video** workspace.

Step 2 Select a blank **Layout** or select the **View** tab 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 (Optional) Right click a pane and select **Select Streams** to display a secondary video stream.

Step 5 (Optional) Save the view so it can be accessed using the **View** tab.

a. Click **Save View**.

b. Enter a name and *Access Location*.

- Views can be assigned to the same location as the cameras, or to a higher level location.
- Only users assigned to a user group with this location can access the View.

c. (Optional) Enter tags that can be used in keyword searches, and a description of the view.

d. Click **OK**.

Tip For new views only. To modify an existing view, use the **Overwrite** button.

Step 6 (Optional) Use the video playback controls as described in "Controlling Video Playback".

Step 7 (Optional) Double-click a video pane to enlarge the video, or open it in a pop-up window.

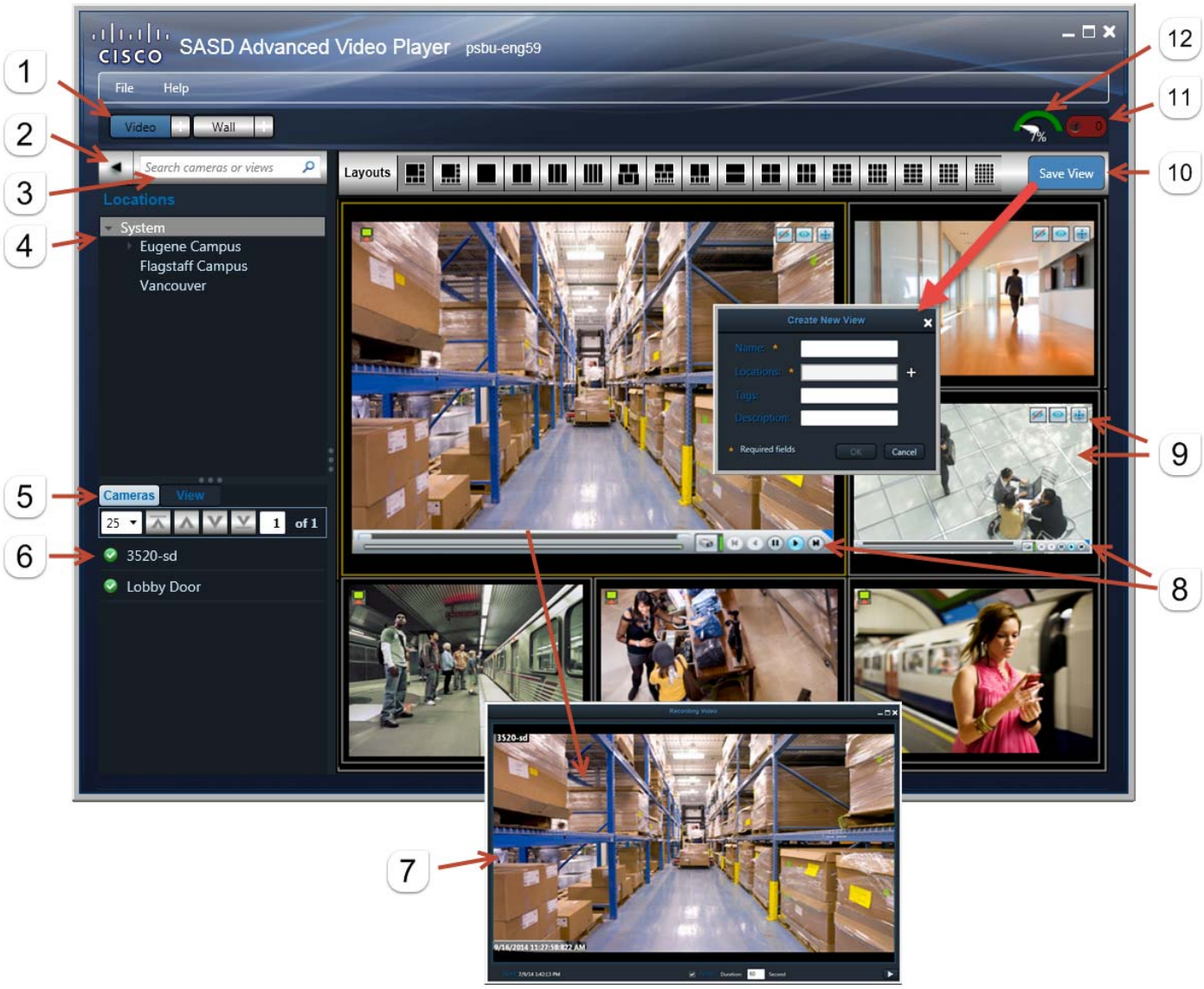
- Go to **Tools > Options** to select if the video should fill the window, or open in a pop-up window when double-clicked.
- Double-click the video pane again to return it to normal size.
- To fill the monitor, right-click the image and select **Full screen mode**.

Step 8 (Optional) Click to create a duplicate workspace window that can be dragged to a separate monitor. See "Displaying a Duplicate Workspace on a Separate Monitor".

Overview

Figure 2 shows the main features of the Video Workspace.

Figure 2 Video Workspace Overview



1	The video monitoring "workspace" Use the location tree to select a camera. Select a **View** to view multiple cameras in a a grid. Views can display primary or secondary streams from multiple cameras. **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".
2	Side panel—Click the triangle ◀ to display or hide the side panel.
3	Search—Enter the full or partial name of a camera to display matching camera names.
4	Locations—Select a location to display only the cameras for that location (cameras from sub-locations are not displayed).

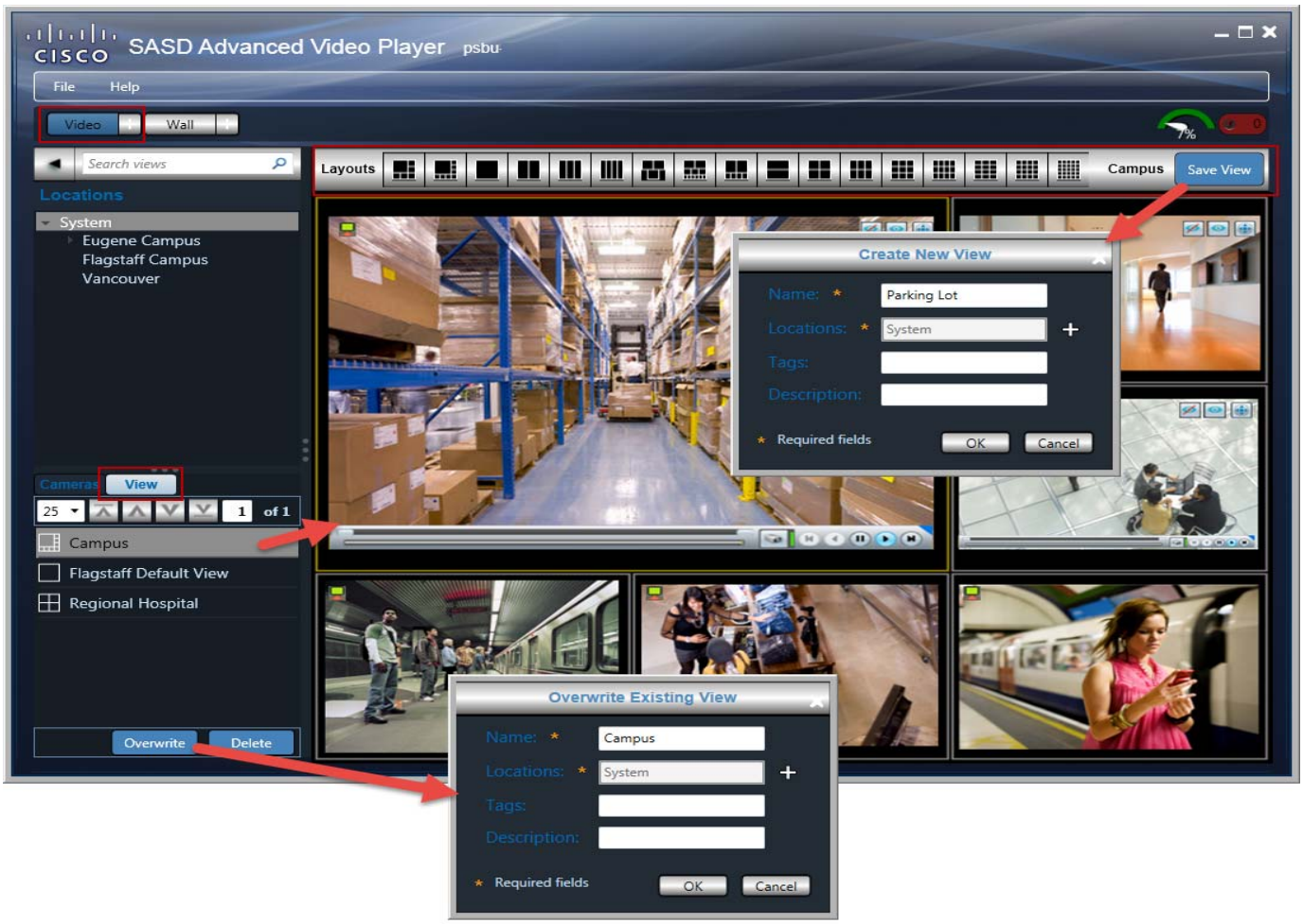
5	**Camera** and **View** tabs. • **Camera**—Select the **Camera** tab to view the available cameras based on the location or search. Double-click or drag & drop the camera to the video area. • **View**—Select the **View** tab to view the pre-defined camera matrix. – Double-click or drag and drop the View to the video area. – Views can display primary or secondary streams from multiple cameras. – The cameras in the View can be configured to automatically rotate. See Saving a Video "View" (Multi-Pane Grid), page 26.
6	The cameras or Views available for the selected location or search.
7	Double-click a video pane to enlarge the video, or open it in a pop-up window. **Tip** Go to **Tools > Options** to select if the video should fill the window, or open in a pop-up window when double-clicked.
8	Playback Controls—See "Controlling Video Playback".
9	Viewing Pane and control icons—See "Controlling Video Playback".
10	**Layouts**—Create a blank matrix from the available layouts and drag cameras onto each viewing pane. See "Saving a Video "View" (Multi-Pane Grid)".
11	Notifications—Notify errors, such as exceptions from Operations Manager back-end calls, or software exceptions.
12	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.

Saving a Video "View" (Multi-Pane Grid)

Views are pre-defined sets of video panes that can be displayed in either the **Video** or **Wall** workspace. Views created using Cisco SASD can include the live primary or secondary video stream from a camera (views cannot include recorded video).

Tip Views that rotate the video from multiple cameras are created using the Cisco Video Surveillance Operations Manager.

Figure 3 Video Layouts and Views



Procedure

Step 1 Select the **Video** workspace.

You must belong to a User Group with permissions for *Views*.

Step 2 Select a blank **Layout** or pre-defined **View** (Figure 3).

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

Step 4 (Optional) Right-click a video pane and select **Select Streams** to display the secondary stream, if necessary. The selected stream will be shown when the View is displayed.

Step 5 (Video workspace only) Save the view so it can be accessed using the **View** tab.

a. Click **Save View**.

b. Enter a name and *Access Location*.

c. (Optional) Enter tags that can be used in keyword searches, and a description of the view.

d. Click **OK**.

- Views can be assigned to the same location as the cameras, or to a higher level location.
- Only users assigned to a user group with this location can access the View.
- If a "Maintenance Mode" message appears, the system has been placed in Maintenance Mode by an Operations Manager administrator, and configuration changes are not allowed. See your Cisco VSM for assistance.

Tip For new views only. To modify an existing view, use the **Overwrite** button.

Step 6 (Video workspace only) To overwrite an existing View:

a. Display a View and modify the cameras or video streams (see Step 1 to Step 4).

b. Click **Overwrite** (Figure 3).

Note

- Unattended video walls are backed by the SASD Monitor windows service. If a wall is closed or stop streaming, it will be brought 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.
- If a "Maintenance Mode" message appears, the system has been placed in Maintenance Mode by an Operations Manager administrator, and configuration changes are not allowed. See your Cisco VSM for assistance.

Related Information

- 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.

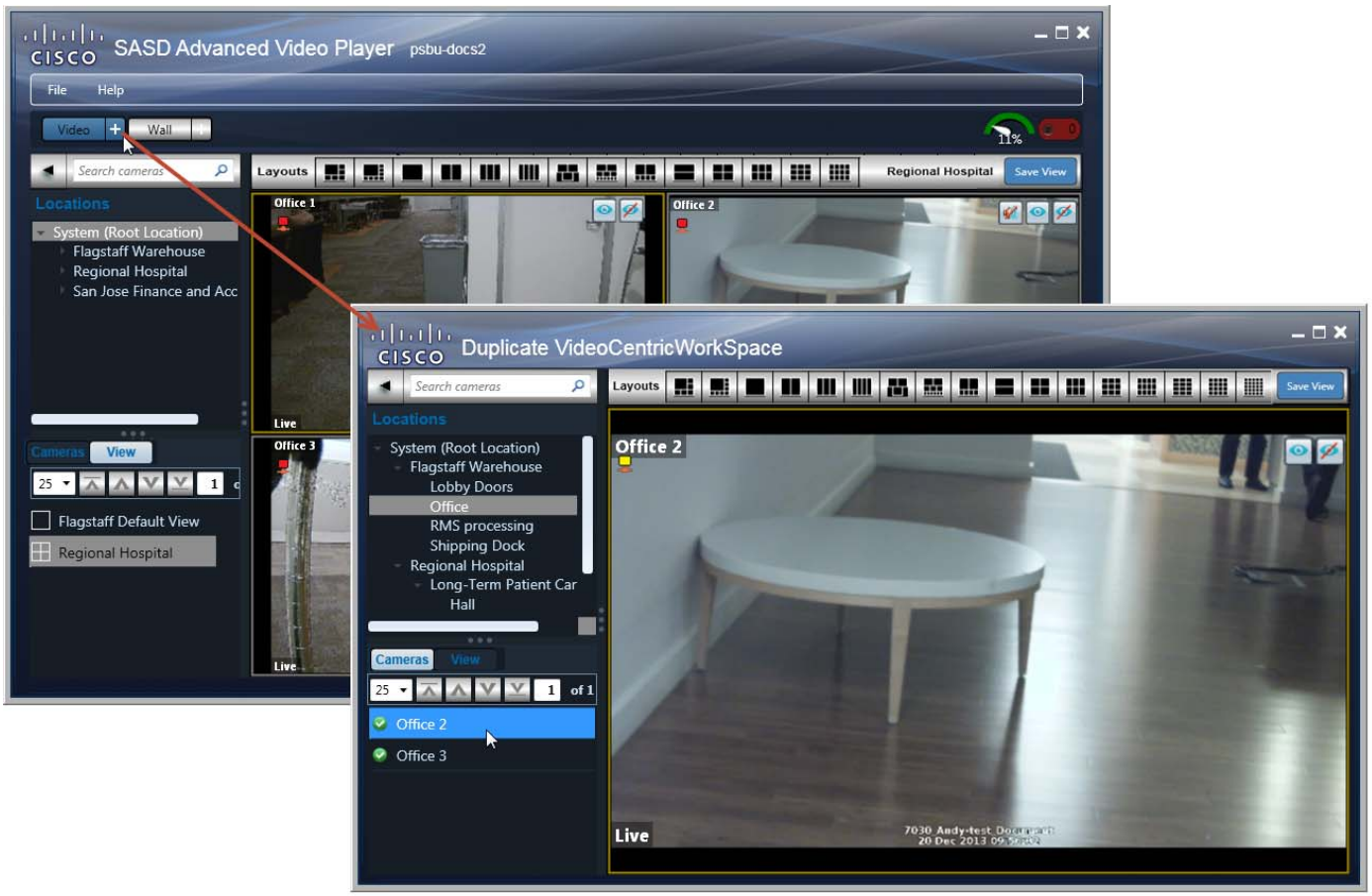
Displaying a Duplicate Workspace on a Separate Monitor

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 4). You can then select a layout, view, map or alert to view video, and drag the window to another monitor, if necessary.

Figure 4 Creating a Duplicate Workspace



Tip

- 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 29
- Usage Notes, page 31
- Viewing and Publishing Video Walls, page 31

Overview

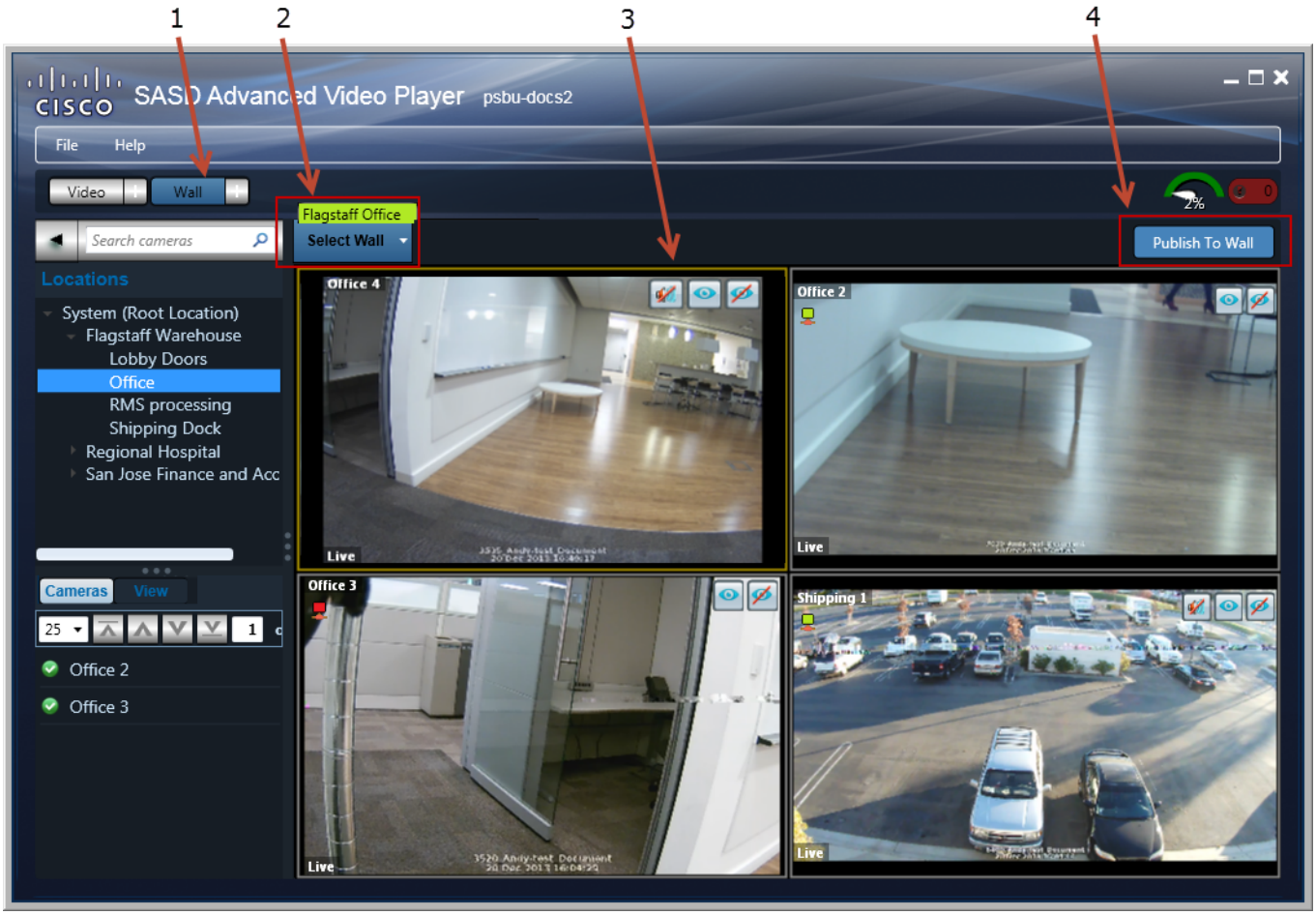
Video Walls are pre-defined *Views* that can be displayed on multiple workstations (Figure 1). All workstations that display the Video Wall will display the same set of pre-defined panes. Walls can be modified and "published" to the other workstations viewing the wall, and used as unattended workstations 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.

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. This feature requires **Push Video to Wall** access permissions. See "Using the Cisco SASD Wall Configurator" for more information.

Requirements

Video Walls require the following:

Table 1 Cisco SASD Requirements

Requirements	Requirement Complete? (✓)
Access Permissions—The following access permissions must be granted using the Cisco Video Surveillance Operations Manager. • **Video Walls**—Create, update, or delete Video Walls using Operations Manager and Cisco SASD Wall Configurator. • **Push Video to Wall**—Enables the **Publish to Wall** feature in Cisco SASD. This feature allows users to change the view shown by all other instances of a selected video wall. The new view is displayed until the dwell time is exceeded. Note: If selected, View Secondary Stream Only will be automatically deselected.	❑
At least one Video Wall must be configured on the system (using the Operations Manager interface).	❑

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.

Viewing and Publishing Video Walls

Procedure

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

Step 1 Select the **Wall** workspace tab.

Step 2 (Optional) Click ✚ to create a duplicate workspace window that can be dragged to a separate monitor. See "Displaying a Duplicate Workspace on a Separate Monitor".

Step 3 Click **Select Wall** and choose a Wall from the list (Figure 1).

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.

Using the Cisco SASD Wall Configurator

Contents

Refer to the following topics for more information:

- Cisco SASD Wall Configurator Overview, page 33
- Requirements, page 35
- Usage Notes, page 36
- Configuring Unattended Workstations, page 36
- Launching the Unattended Windows, page 38
- Understanding Offline Mode, page 40

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.

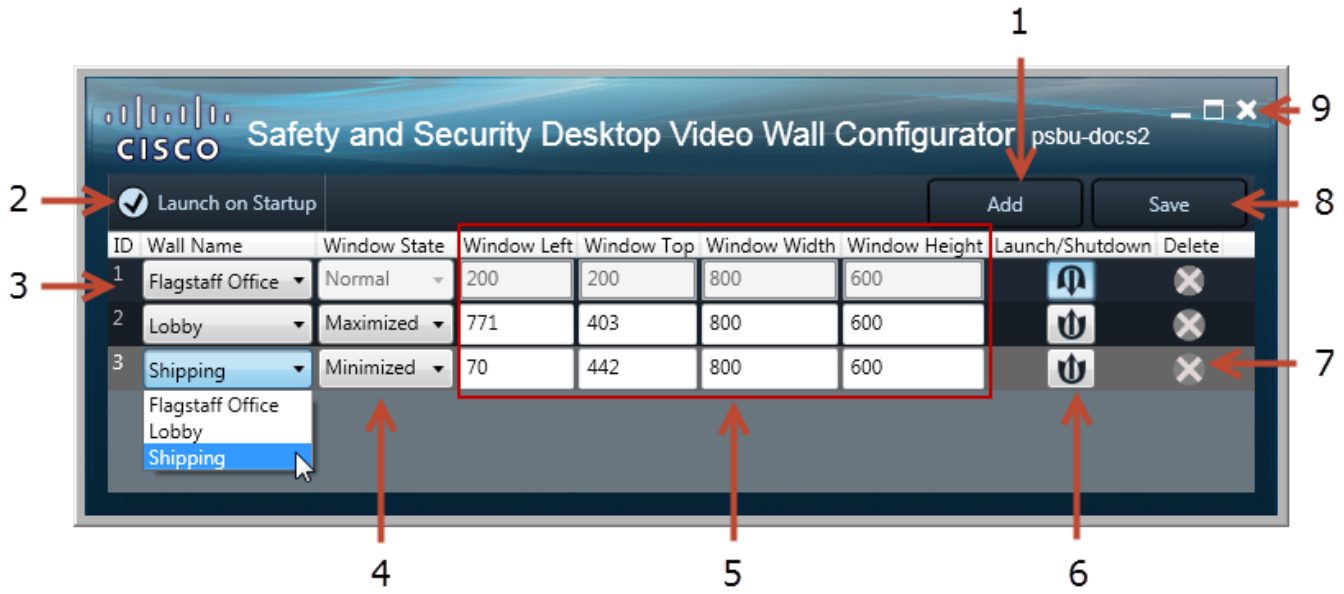
For example:

- 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. • De-select 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.

5	Position—The size and location of the Video Wall in Normal window state. Move the Video Wall on the screen to automatically change the settings, or enter the coordinates manually.
6	Launch/Shutdown—Open or close the Video Walls for testing and positioning in the Cisco SASD Wall Configurator. • —Launch. Opens the Video Wall so you can resize and re-position the window. • —Shutdown. Closes the Video Wall window. **Tip** All 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.
7	—Delete. Removes the Video Wall from unattended mode. The Video Wall window will not launch.
8	**Save**—Save the configuration.
9	Close—Quits the Cisco SASD Wall Configurator and launches the Video Walls in unattended mode.

Requirements

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

Table 1 Requirements

Requirements	Requirement Complete? (✓)
Administrative user privileges on the Windows workstation.	❑
An admin account in Cisco Video Surveillance.	❑
Access Permissions—The following access permissions must be granted using the Cisco Video Surveillance Operations Manager. • **Video Walls**—Create, update, or delete Video Walls using Operations Manager and Cisco SASD Wall Configurator. • **Push Video to Wall**—Enables the **Publish to Wall** feature in Cisco SASD. This feature allows users to change the view shown by all other instances of a selected video wall. The new view is displayed until the dwell time is exceeded. Note: If selected, View Secondary Stream Only will be automatically deselected. • The **Allow Multiple Logins** option must be enabled. This is because each unattended video wall requires a unique Cisco VSM login session for the video wall to be displayed.	❑
At least one Video Wall must be configured on the system (using the Operations Manager interface).	❑
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. • See the "Understanding Sites" for more information. • See the Cisco Video Surveillance Operations Manager User Guide for information about creating and assigning Site access.	❑
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. 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	❑

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 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.
- If a "Maintenance Mode" message appears, the system has been placed in Maintenance Mode by an Cisco Video Surveillance Operations Manager administrator, and configuration changes are not allowed. See your Cisco VSM for assistance.

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* and *Push Video to Wall*.

- The user group must have the **Allow Multiple Logins** option enabled. This is because each unattended video wall requires a unique Cisco VSM login session for the video wall to be displayed.

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 36.

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

Launch Option	Description
Save and exit the Cisco SASD Wall Configurator	The Video Walls are launched automatically when the Cisco SASD Wall Configurator closes.
Launch the Cisco SASD Wall Launcher	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.
Restart the workstation	(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 36 for more information.

Note To launch unattended windows, you must belong to a user group with the **Allow Multiple Logins** option enabled. This is because each unattended video wall requires a unique Cisco VSM login session for the video wall to be displayed.

Related Information

To change the Video Walls that appear in unattended mode, see the following topics:

- "Configuring Unattended Workstations" section on page 36
- "Removing a Video Wall From Unattended Mode" section on page 38

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 38).

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 off-line mode.
- If the Operations Manager is unavailable when the unattended windows launch, the unattended windows will restart in off-line 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

Transition	Description
Online to Offline	If the Operations Manager connection is lost for 4 minutes, the unattended windows will switch to Offline mode.
Offline to Online	If the Operations Manager connection is restored for 12 minutes, the unattended windows will switch to Online mode.

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.
- 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.
- If a "Maintenance Mode" message appears, the system has been placed in Maintenance Mode by an Cisco Video Surveillance Operations Manager administrator, and some actions such as acknowledging an alert are not allowed. See your Cisco VSM for assistance.

Contents

Refer to the following topics for more information:

- Understanding Events and Alerts, page 42
- Alert Workspace Overview, page 43
- Dynamic Updates of Alert Results, page 45
- Viewing Event URLs, page 50
- Common Tasks, page 51
- Impact of Device Location Changes on Alerts, page 51
- Summary of Events and Corresponding Alerts, page 53

Understanding Events and Alerts

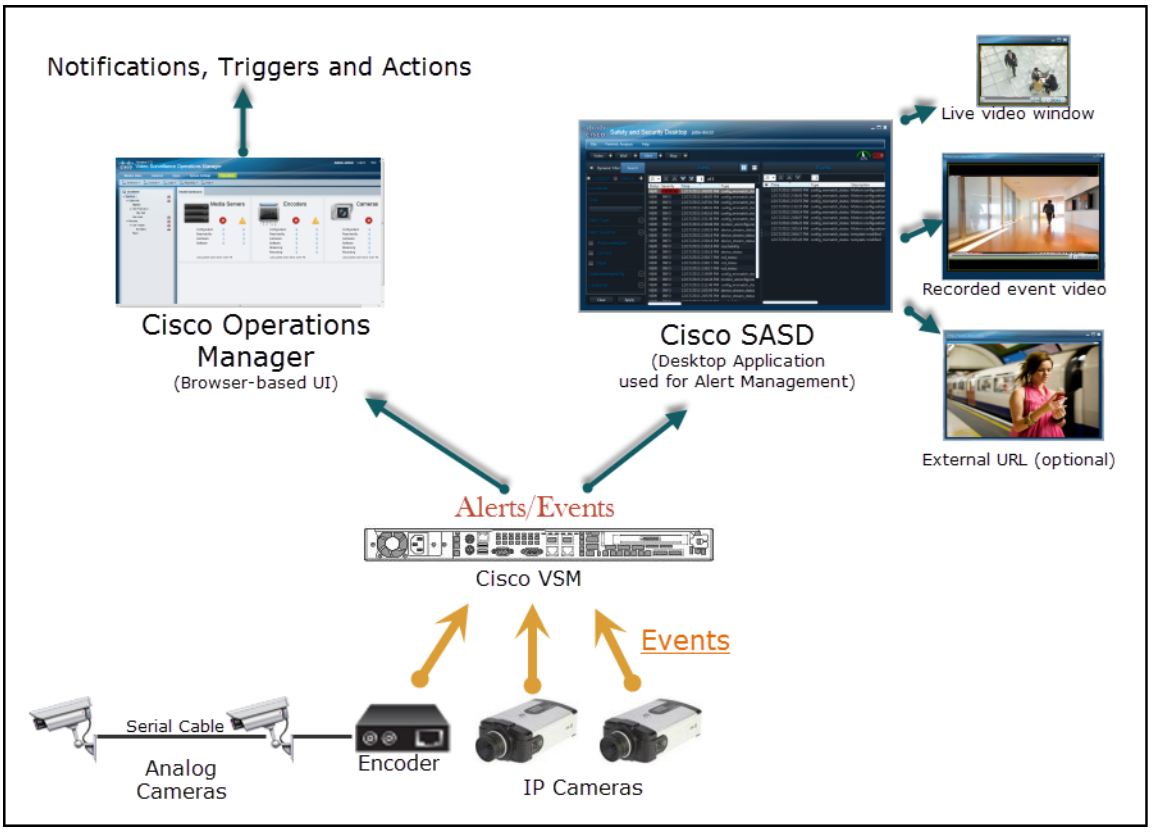
Events represent incidents that occur in the system and in devices (such as cameras or camera encoders). Events are aggregated (grouped) into alerts for notification purposes. For example, if a camera goes offline and comes back online repeatedly, all events for that issue are grouped under a single 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.

Figure 1 Health Events, Alerts, and Notifications

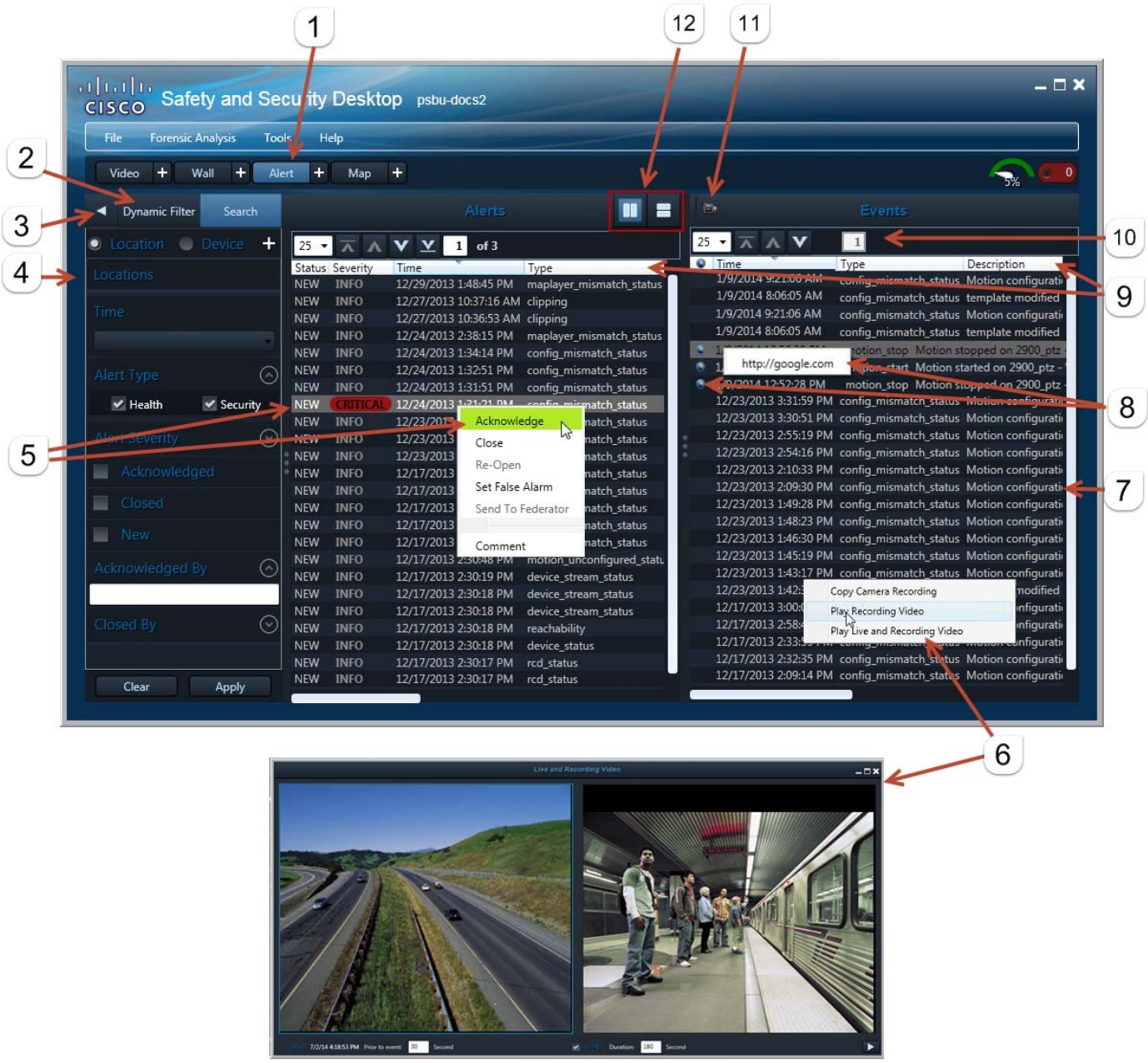


Note When a camera is configured for stream redundancy (for example, stream 1 to the primary Cisco Media Server and stream 2 to a redundant server), events from both streams are added to the same alert.

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.

Figure 2 Alert Workspace



For example:

- Right-click an alert to acknowledge, close, re-open, or comment on the alert.
- View live or recorded event video (if available).

Review the following descriptions for more information:

1	Alert Workspace tab. • 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".
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**. **Tip** If a filter criteria is not selected, the all alerts for that filter are displayed. • Location—Click to select a specific location where the alert(s) were created. Only alerts from that location will be displayed. • 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 Category—Health or Security. See the "Understanding Events and Alerts" section on page 42 for more information. • Alert Types—The type of alert that will appear in the results. For example: Compatibility Mismatch Status, Contact Closure, Camera Storage Unconfigured, etc. • Alert Severity—Select CRITICAL, MAJOR, MINOR, WARNING, or INFO. **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 53 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 50.
8	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).
9	Select the number of items that are displayed on a page, or navigate through the available pages.
10	—The camera icon appears if video is available for the event. Right-click the event to select one of available following options. See the following for more information: • Copy Camera Recordings From Alerts, page 139 • Play Recorded Video, page 46 • Play Live and Recorded Video, page 48 Video is available for the following event types: • Motion start/stop • Contact closure open/close • Soft trigger • Analytics
11	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.

Playing Event Video

To play video for security alerts that include video clips, right-click the event and select a playback option. Video is available for the following event types:

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

Refer to the following topics for more information:

- Copy Camera Recordings From Alerts, page 139
- Play Recorded Video, page 46
- Play Live and Recorded Video, page 48

Copy Camera Recording

Recordings that are stored on a camera's local storage (such as an SD card) must be transfered to the Cisco Media Server before they can be viewed. For more information, refer to the following:

- Camera Recording Management, page 129
- Copy Camera Recordings From Alerts, page 139

Play Recorded Video

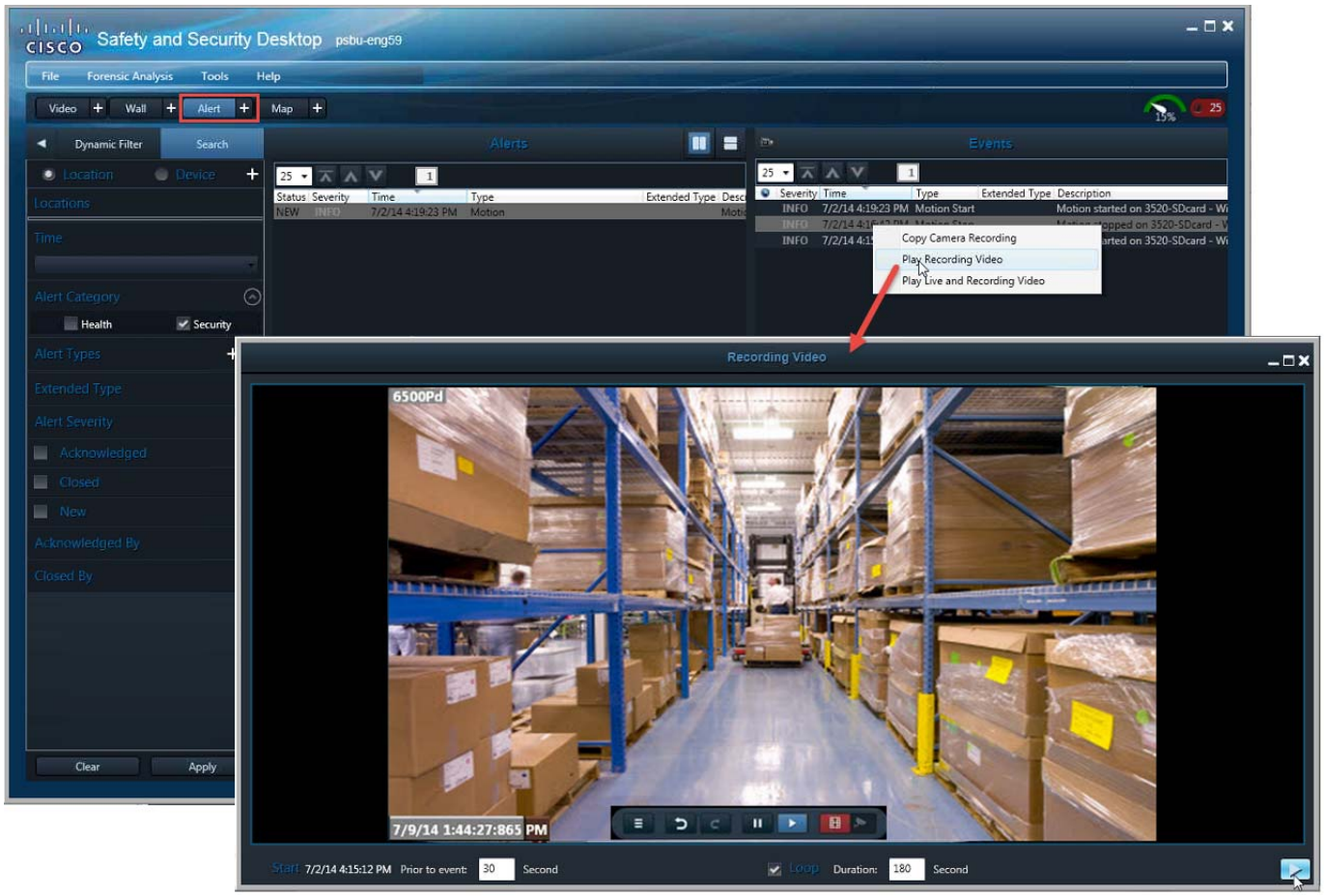
To view the video recordings for a security event (such as a motion event), right click the event and choose **Play Recorded Video** (Figure 3). The popup window can be enlarged and dragged to another monitor for better viewing.

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

Figure 3 Play Recorded Video From an Alert



Procedure

Step 1 Select the **Alert** workspace.

Step 2 Use the filters to narrow the results, and click **Apply**.

- For example, select the **Security** category to display only security alerts, such as motion stop and start events.
- See Alert Workspace Overview, page 43 and Understanding Events and Alerts, page 42 for more information.

Step 3 Select a security alert to display the individual events for that alert.

Step 4 Right-click a event and select **Play Recording Video** (Figure 3).

Step 5 (Optional) Use the playback controls to view the event video that was copied form the camera.

- **Prior to Event**—Enter the number of seconds that should be played before the event was triggered. Click the Play icon to activate the change.
- Select **Loop** to play the video segment in a continuous loop. Click the Play icon to activate the change.

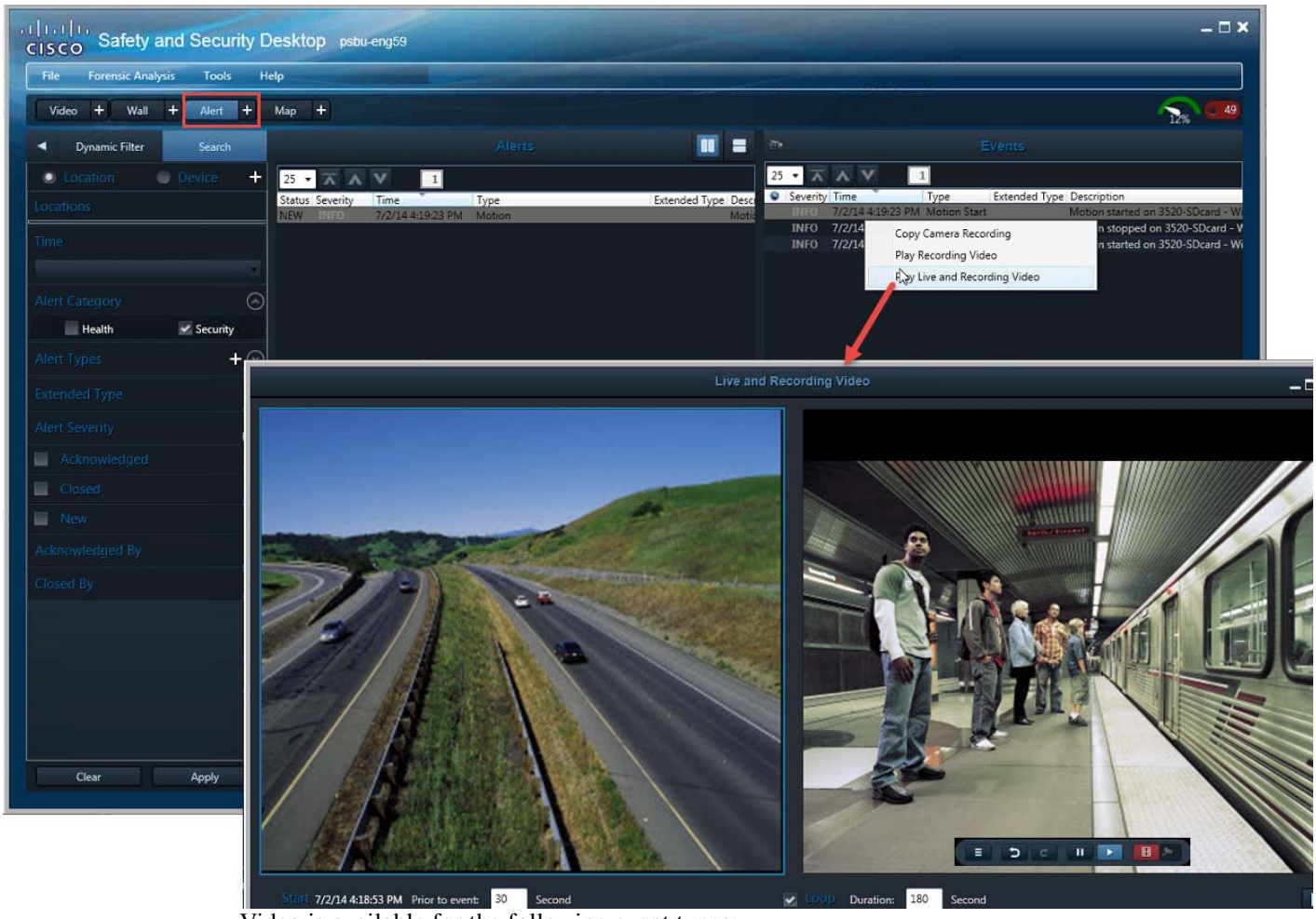
- Enter a **duration** to play a longer or shorter portion of the video. Click the Play icon to activate the change.

Play Live and Recorded Video

To view the video recordings for a security event alongside a live video stream from the same camera, right click the event and choose **Play Live and Recording Video** to opens a 2-pane pop-up playback window (Figure 4).

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.

Figure 4 Play Recorded and Live Video Side-By-Side



Video is available for the following event types:

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

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.

Procedure

Step 1 Select the **Alert** workspace.

Step 2 Use the filters to narrow the results, and click **Apply**.

- For example, select the **Security** category to display only security alerts, such as motion stop and start events.
- See Alert Workspace Overview, page 43 and Understanding Events and Alerts, page 42 for more information.

Step 3 Select a security alert to display the individual events for that alert.

Step 4 Right-click a event and select **Play Live and Recording Video** (Figure 4).

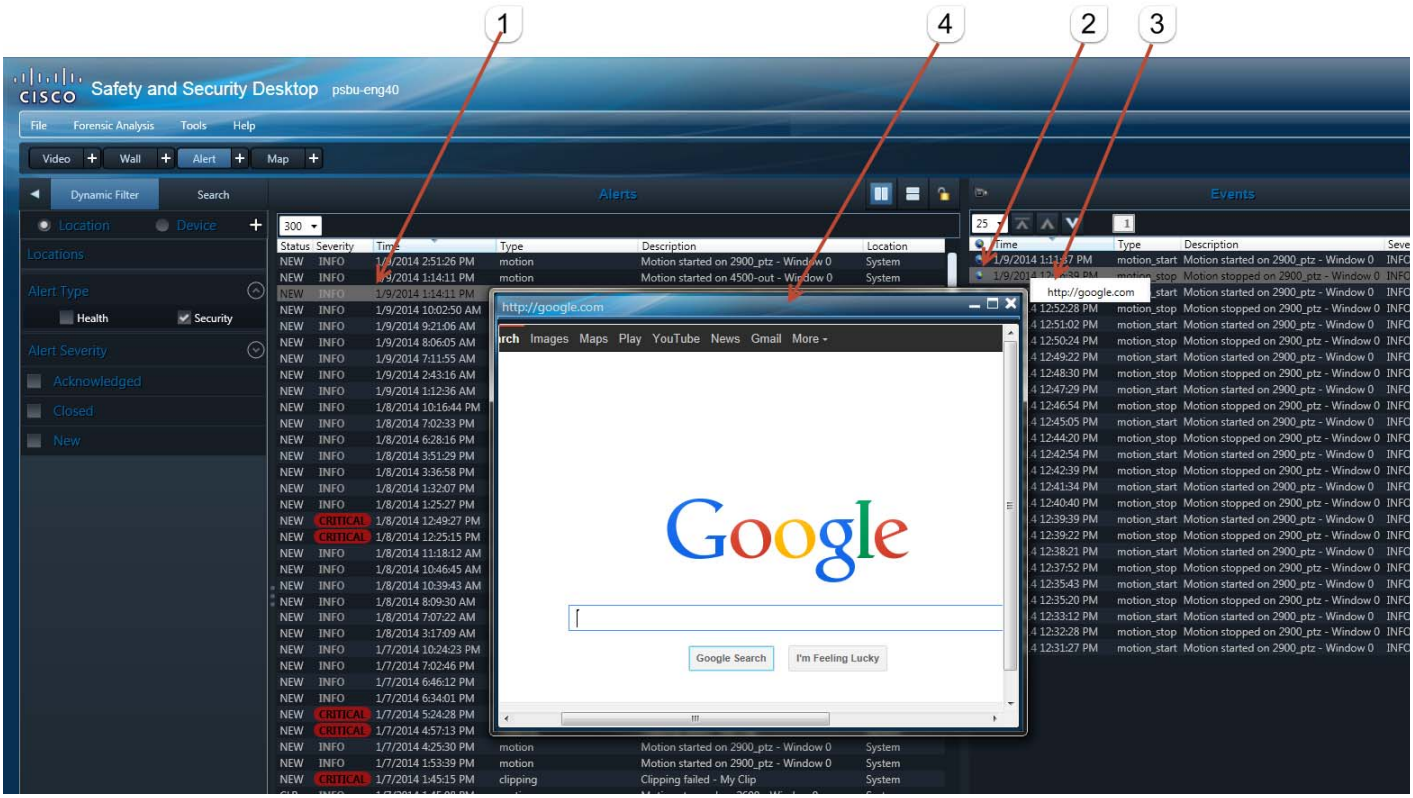
Step 5 (Optional, for the recorded video pane only) Use the playback controls to view the event video that was copied form the camera.

- **Prior to Event**—Enter the number of seconds that should be played before the event was triggered. Click the Play icon to activate the change.
- Select **Loop** to play the video segment in a continuous loop. Click the Play icon to activate the change.
- Enter a **duration** to play a longer or shorter portion of the video. Click the Play icon to activate the change.

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 5).

Figure 5 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

Task	Description
Narrow the list of displayed alerts	Click the tabs at the top of the alert list to filter the displayed alerts: • **Search**— keywords • **Dynamic Filter** (narrow the results based on alert type, status, or severity, time, location, and/or device). **Tip** Any filter criteria that is not selected will return all alerts for that filter.
Display the events associated with the alert	Select an alert to view the associated events.
Acknowledge the alert	Right-click an alert and select **Acknowledge**.
Close, re-open, or flag the alert as a false alarm	Right-click an alert and select an option. • When an alert is closed, no new events can be added (unless the alert is reopened by a user). Any new events for the same device and issue are added to a new alert entry. • Users can still modify closed alerts, including the following: – Add a comment (the alert state is not changed). – Re-open the alert. New events for that device and issue will be added to the alert.
Add a comment	Right-click an alert and select **Comment**. Add the comment and click **Apply**.
View event video (motion and analytics alerts only)	The camera icon appears if video is available for the event. Right-click the event to select an option and open a playback window. See Playing Event Video, page 46.
View alerts on a larger location map	Open the Map Workspace. See the "Map Workspace" for more information.

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*.

   Alert 1 Location 1 Device 1

   Event 101 Location2 device1

   Event 100 Location2 device1

   Event 99 Location1 device1

   Event 98 Location1 device1

   Etc.

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).

   Alert 2 Location 2 Device 1

   Event 103 Location2 device1

   Event 102 Location2 device1

   Etc.

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

Alerts	Events included in the alert	Severity	Description of the alert per event type
analytics	analytics_occurred	INFO	Analytics event of type {0} occurred for rule {1}
auto_discovery	auto_discovery	N/A	N/A
capability_mismatch_status	capability_mismatch_status	CRITICAL	Configuration defined in the template and the configuration supported by the camera do not match
		INFO	Issue with respect to configuration defined in the template and the configuration supported by the camera has been cleared
chassis_intrusion	chassis_intrusion	CRITICAL	Chassis Intrusion is critical
		INFO	Chassis Intrusion is normal
clipping	clip_start	INFO	Clipping initiated - {0}
	clip_completed	INFO	Clipping completed - {0}
	clip_deleted	INFO	Clipping deleted - {0}
	clip_failed	INFO	Clipping failed - {0}
config_mismatch_status	config_mismatch_status	CRITICAL	Configuration in VSOM is not the same as in Media Server for device {0}
		INFO	Configuration in VSOM same as in Media Server for device {0}
contact_closure	contact_closure_opened	INFO	Contact closure opened on port {0}
	contact_closure_closed	INFO	Contact closure closed on port {0}

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

contact_closure_unconfigured_status	contact_closure_unconfigured_status	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
coredump	coredump	CRITICAL	{0} core dump critical
device_status	device_status	CRITICAL	{0} Streaming status is critical
		INFO	{0} Streaming status is normal
	device_config_status	CRITICAL	Error in {0} device configuration
		INFO	{0} device configuration is normal
device_stream_status	device_stream_status	CRITICAL	{0} Streaming videoloss
		INFO	{0} Streaming status is normal
	device_connection_status	CRITICAL	{0} Streaming connection loss occurred
		INFO	{0} Streaming status is normal
driverpack_mismatch_status	driverpack_mismatch_status	CRITICAL	Driver-packs in Media Server does not match with Driver-packs in VSOM
		INFO	Media Server's driver-pack matches Operations Manager's
encoder_max_streams_used_status	encoder_max_streams_used_status	CRITICAL	maximum number of streams reached for encoder
		INFO	max_streams_reached issue is resolved
event_overload_status	event_overload_status	CRITICAL	VSOM dropped {0} events due to a large number of events received
		INFO	Normal VSOM events processing has resumed
fan_speed	fan_speed	CRITICAL	{0} is critical
		INFO	{0} is normal
firmware_mismatch_status	firmware_mismatch_status	CRITICAL	Camera's template firmware does not match the camera's firmware
		INFO	Camera's template firmware matches the camera's firmware
fs_usage	fs_usage	CRITICAL	File system usage on {0} is critical
		INFO	File system usage on {0} is normal

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

ha_config_mismatch_status	ha_config_mismatch_status	CRITICAL	Configuration in VSOM and primary MS is not the same as in redundant/failover Media Servers {0}
		INFO	Configuration in VSOM and primary MS is same as in redundant/failover Media Servers {0}
identity_collision_status	identity_collision_status	CRITICAL	Another device with one or more identity criteria exists in the system.
		INFO	Identity collision is resolved.
insufficient_backup_space_status	insufficient_backup_space_status	CRITICAL	Insufficient space is stopping automatic VSOM database backup
		INFO	Automatic VSOM database backup is normal
load_average	load_average	CRITICAL	Load average is critical
		INFO	Load average is normal
mem_free	mem_free	CRITICAL	Memory usage is critical
		INFO	Memory usage is normal
motion	motion_start	INFO	Motion started on {0}
	motion_stop	INFO	Motion stopped on {0}
motion_unconfigured_status	motion_unconfigured_status	CRITICAL	Motion window is not configured on the camera. Record on motion and other actions will not work.
		INFO	Motion window is configured on the camera.
nic_usage	nic_usage	CRITICAL	{0}'s Nic usage is critical
		INFO	{0}'s Nic usage is normal
password_expired_status	password_expired_status	CRITICAL	Password expired - needs a password change
		INFO	password changed
power_supply	power_supply	CRITICAL	{0} Power supply is critical
		INFO	{0} Power supply is normal
raid_status	raid_status	CRITICAL	Virtual drive{0} Raid failure is critical
		INFO	Virtual drive{0} Raid failure is fixed
rcd_status	rcd_status	CRITICAL	{0} Recording status is critical
		INFO	{0} Recording status is normal
	recording_groomed	INFO	Parts of the recording {0} was groomed to free up disk space

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

reachability	reachability	CRITICAL	{0} device is unreachable
		INFO	{0} device is reachable
recorder_oversubscribed	recorder_Oversubscription	CRITICAL	{0} Disk space usage for recordings has been over-subscribed
		INFO	{0} Disk space usage for recordings is normal
redundancy_unconfigured_status	redundancy_unconfigured_status	CRITICAL	Failover/Redundancy servers are not configured for the camera's primary media-server.
		INFO	Failover/Redundancy servers are configured for the camera's primary media-server.
server_status	server_status	CRITICAL	Server status is {0}
		INFO	Server status is START
soft-trigger	soft_trigger	INFO	Soft trigger {0} occurred on camera
temperature	temperature	CRITICAL	{0} is critical
		INFO	{0} is normal
time_out_of_sync_status	time_out_of_sync_status	WARN	Media Server time does not match with the VSOM time.
		INFO	Media Server time matches with the VSOM time.
ums_config_change	ums_config_change	CRITICAL	{0} Change in Media Server configuration
		INFO	{0} No Change in Media Server configuration
ums_failover_status	ums_failover	WARN	UMS failed over {0}
	ums_failback	INFO	UMS failed back {0}
ums_identity_mismatch_status	ums_identity_mismatch_status	CRITICAL	UMS alternate id in Media Server does not match with alternate id in VSOM
		INFO	UMS alternate id in Media Server matches the alternate id in VSOM
ums_version_mismatch_status	ums_version_mismatch_status	CRITICAL	Media Server's version does not match Operations Manager
		INFO	Media Server's version matches Operations Manager
unknown_hw_sensor	unknown	CRITICAL	{0} Unknown hardware sensor is critical
		INFO	{0} Unknown hardware sensor is normal

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

voltage	voltage	CRITICAL	{0} is critical
		INFO	{0} is normal

Map Workspace

Contents

- Overview, page 59
- Working With Image Layers, page 63

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 dragable icon, or double-click the icon to view video in a pop-up window.

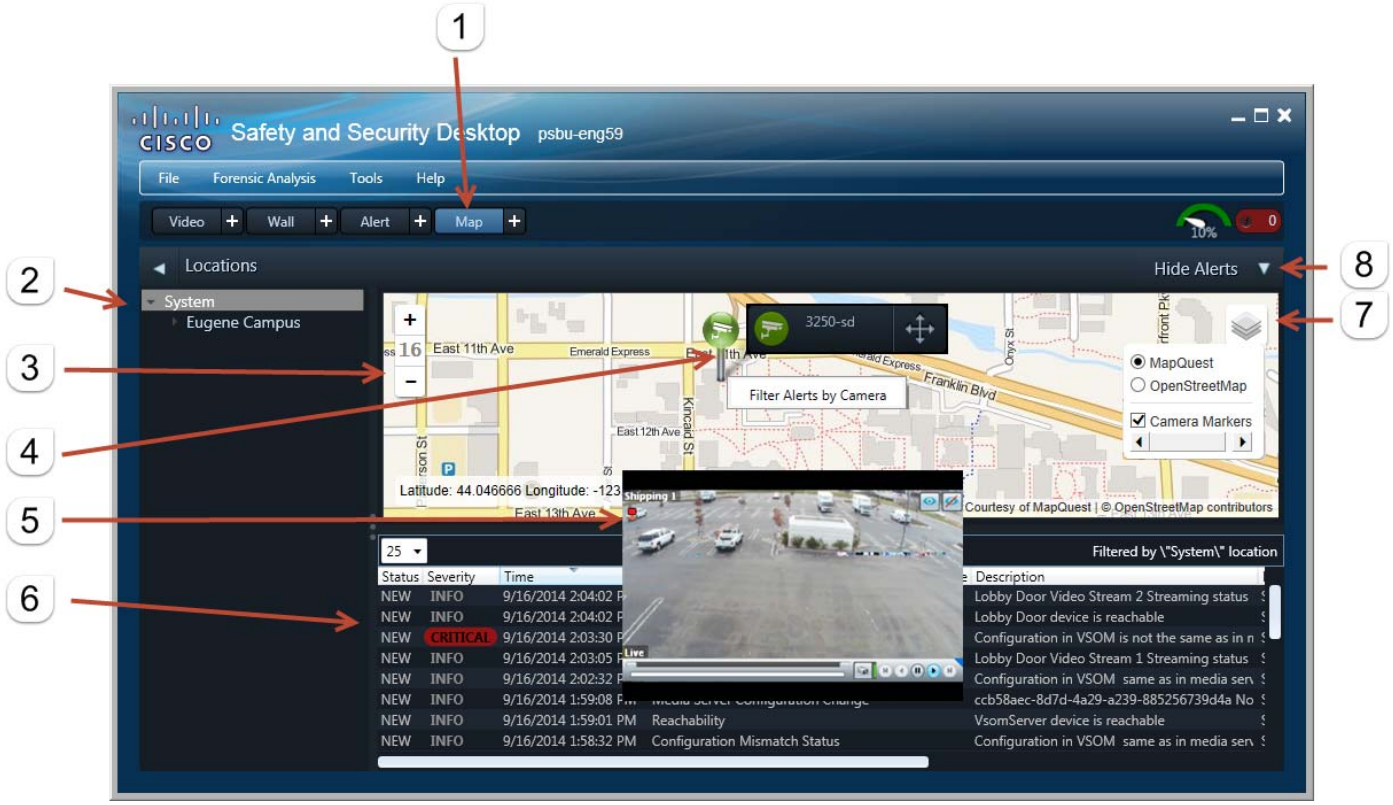
Tip Maps can include an aerial view of the camera location (such as a street map or satellite view), or an image of the physical location, such as a building layout, floor plan or other image).

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 icon to display a dragable icon. Drag and drop the icon onto a duplicate workspace (icons cannot be dragged onto an unattended Video Wall). • 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*
5	Video playback window for the selected camera. See "Controlling Video Playback" for more information.
6	Alerts for the selected location. • Right-click an alert to take an action (such as close, comment, acknowledge or send to Federator). • Click the **Time** or **Severity** 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). See "Alert Workspace" for more information about viewing and managing alerts.
7	Map provider selector. • Click the selector icon to choose a map provider (such as a MapQuest or OpenStreetMap). • The provider displays the map (such as the street or satellite view) for the selected location. **Tip** A selector icon is also used to choose image layers (such as floor plans in a building). See "Working With Image Layers" for more information.
8	Click **Hide Alerts** to hide or show the alerts related to the location or camera.

Requirements

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

Table 1 Requirements

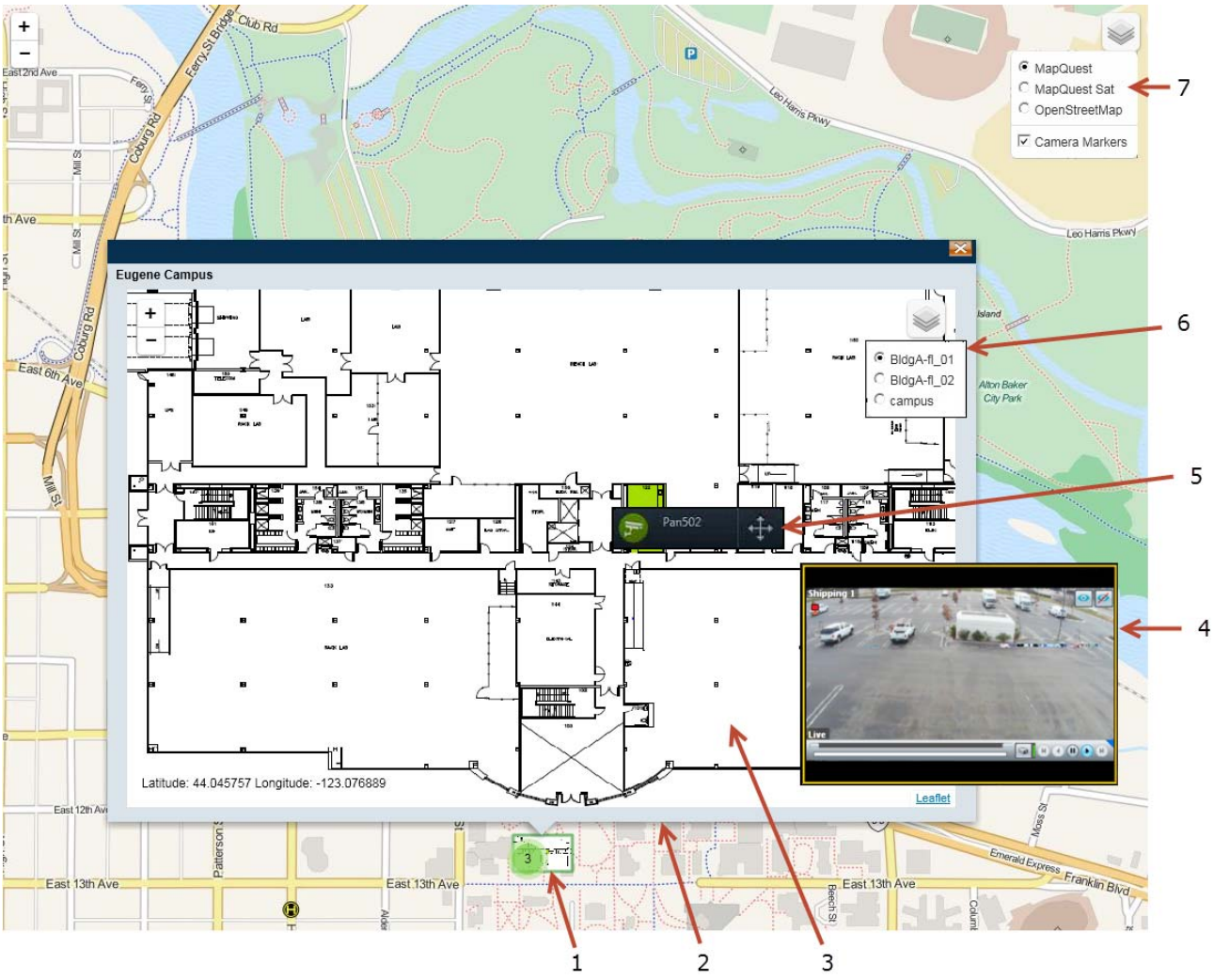
Requirements	Requirement Complete? (✓)
A Cisco Maps Server must be added to the Operations Manager configuration. **Note** The location maps and image layers configured in Operations Manager are available for use in the Cisco SASD Maps workspace.	❑
Internet Explorer (IE) 9 or 10 must be installed on the monitoring workstation: **Note** 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. See the Cisco Video Surveillance Monitoring Workstation Performance Baseline Specification for more information.	❑
The Cisco SASD desktop application must be installed on the monitoring PC. **Note** The Maps workspace is not supported on the Cisco SASD Federator or Cisco SASD Advanced Video Player applications.	❑

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-word 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).

3	Camera icon. • Select a camera to view video and alerts from that device. • Right-click the icon and select **Filter Alert by Camera** to view the alerts for that device. • The color represents the device status: – Green—*Enabled: OK* – Red—*Enabled: Critical*
4	Video playback window for the selected camera. • See "Controlling Video Playback" for more information.
5	Dragable icon. • Single-click a camera icon to display a dragable icon. • Drag and drop the icon onto a duplicate workspace (icons cannot be dragged onto an unattended Video Wall).
6	Image Layer selection. • Click the selector icon to choose an image layers (such as a building floor plan).
7	Location map selection. • Click the selector icon to choose a map provider (such as a MapQuest or OpenStreetMap). • The provider displays the map (such as the street or satellite view) for the selected location.

Summary of Map Workspace Options

Procedure

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.

Contents

Refer to the following topics for more information.

- Overview, page 66
- Viewing Live Video, page 67
- Viewing Recorded Video, page 70
- Creating and Viewing Video Clips, page 74
- Using Record Now, page 84
- Using the Pop-Up Menu, page 85
- Understanding Video Pane Border Colors, page 87
- Using the Privacy Mask, page 88
- Using the Smooth Video Options When Viewing Live Video, page 91
- Synchronizing Video Playback in Multiple Panes, page 92
- Using Pan, Tilt, and Zoom (PTZ) Controls, page 96

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).

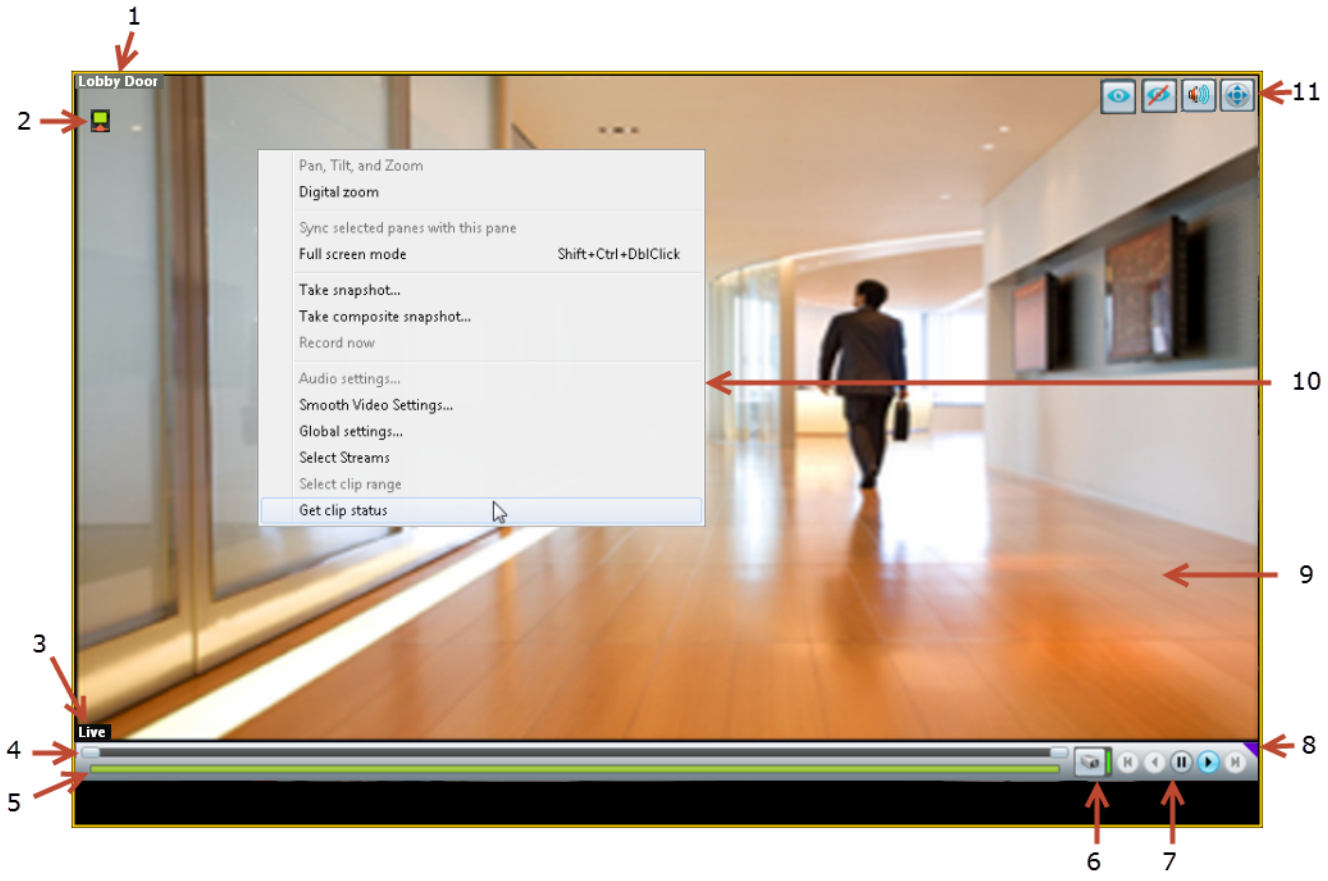
- Additional options are available by right-clicking the image. Options include synchronizing multiple viewing panes, recording live video, expanding the image to fill the screen, creating a snapshot image, and configuring smooth video options to improve playback performance when network performance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

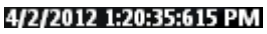
Viewing Live Video

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.

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 91 for more information.
3	Indicates live or recorded video (recorded video displays a time stamp such as ).
4	Range Bar—Used with recorded video (see the "Viewing Recorded Video" section on page 70 for more information).
5	Seek—Used with recorded video to choose a playback time (see the "Viewing Recorded Video" section on page 70 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 70 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 85 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 88. • —**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 96. • — See the "Synchronizing Video Playback in Multiple Panes" section on page 92. **Note** The control bar and audio icon will not display if your workstation monitor is set to 16-bit color setting. Change your monitor *color* setting to 32-bit.

Usage Notes

- Some firewall policies on enterprise PCs can block live video streams from cameras. If this occurs, add the camera IP address to the firewall trusted list.
- To maximize the video screens, move the new workspace to a separate monitor and double-click a pane to fill the entire browser window. To fill the entire monitor screen, right-click the image and select **Full screen mode**.
- To control the playback in multiple video panes, `Shift-Click` or `Ctrl-Click` to select the panes. The borders of all selected panes turn to orange. Controls and actions performed in one pane also affect the other selected panes. To deselect panes, select a single pane, or use `Shift-Click` or `Ctrl-Click` to deselect the panes
- Live video may be delayed 1-2 seconds. Live video can be further delayed if the smooth video option is enabled. See the "Using the Smooth Video Options When Viewing Live Video" section on page 91 for more information.

- *Soft-deleted* cameras (shown with a icon) are cameras that were removed from the system but still allow access to the camera's recorded video. You cannot display live video from *soft-deleted* cameras.
- The control bar and audio icon will not display if your workstation monitor is set to 16-bit color setting. Change your monitor *color* setting to 32-bit.

Additional Information

Refer to the following topics for additional options:

- Using Record Now, page 84
- Using the Pop-Up Menu, page 85
- Using the Smooth Video Options When Viewing Live Video, page 91
- Synchronizing Video Playback in Multiple Panes, page 92
- Using Pan, Tilt, and Zoom (PTZ) Controls, page 96

Viewing Recorded Video

You can view recorded video from a continuos 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	Indicates the video quality, which can be affected by network and system performance. The icon turns red if the video quality is poor . **Note** This icon is for informational purposes only when displayed with recorded video (the Smooth Video options do not apply).
3	Pop-up menu options. See the "Using the Pop-Up Menu" section on page 85.
4	Timestamp for the currently displayed video image. For example: 7/12/2012 4:08:39:886 AM . **Note** Changes to Live when live video is displayed.

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

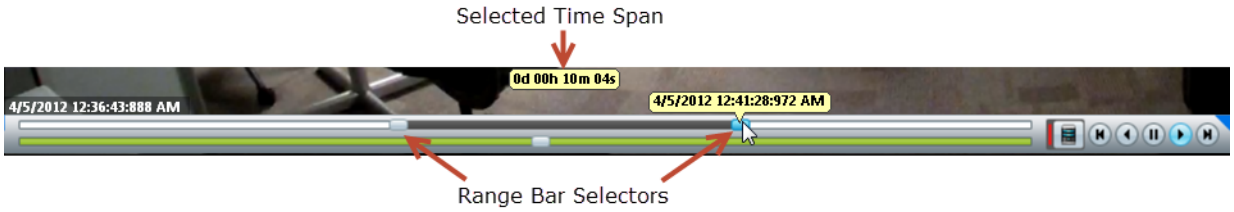
- The entire *range bar* represents the entire span of available recorded video. Slide the *range bar* selectors to shorten the range (see below).
- The lower (green) *seek bar* represents the selected range (see below).

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

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

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

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

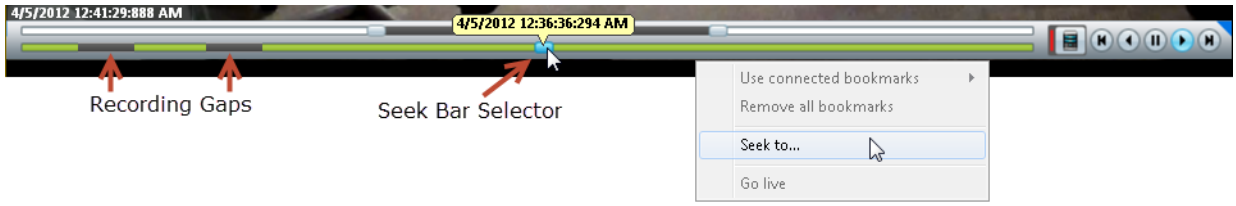


Tip The green *seek bar* represents the selected span. If the span in the top *range bar* is 10 minutes, then the green *seek* bar represents 10 minutes of video. Slide the *seek bar* selector to choose the playback time (see below).

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

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

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



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

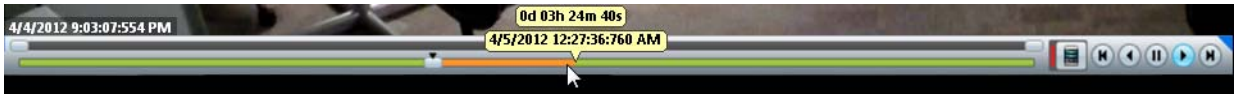
Note Gaps in the recorded video are shown in gray. Recording gaps occur if there is a manually-triggered Record Now session, if recording was manually stopped, if recording was stopped by a schedule, or if video was unavailable due to network connectivity issues, device malfunctions, or other events.

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

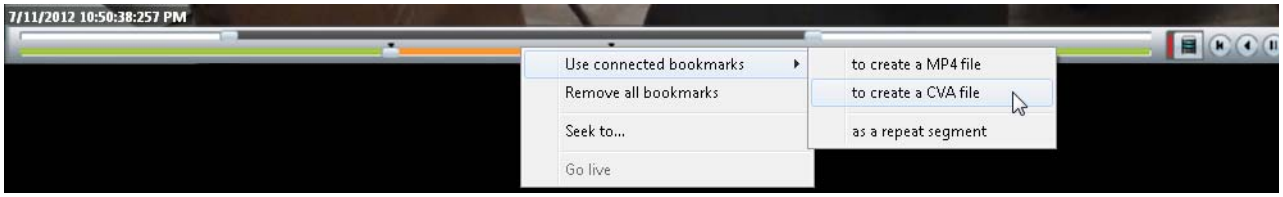
Note When you move the scroll bar for a video pane that is synchronized, that pane becomes the new synchronization master pane. The other synchronized panes play video according to the master pane. See the "Synchronizing Video Playback in Multiple Panes" section on page 92.

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

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



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



See the following for more information:

- Creating and Viewing Video Clips, page 74
- Creating a Repeat Segment, page 83

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

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

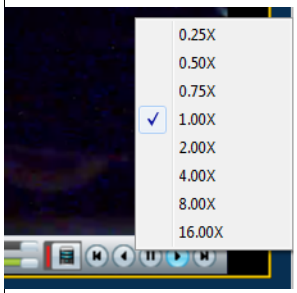
Tip The first time you select a camera's recorded video, the playback begins slightly behind the live (current) time. When you toggle between live and recorded, recorded video returns to the previously selected timestamp.

12 Recorded video playback controls.

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

Variable Speed Playback

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



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

13	—Click the triangle to pin the control bar to the screen, or auto-hide it when the cursor is moved. **Note** The control bar and audio icon will not display if your workstation monitor is set to 16-bit color setting. Change your monitor *color* setting to 32-bit.
14	Camera feature icons. For example: • or —Audio is supported by the camera and enabled or disabled in the viewing pane. • —The synchronization icon appears in video panes that play synchronized video. See the "Synchronizing Video Playback in Multiple Panes" section on page 92. **Note** The PTZ icons are enabled only for live video. **Note** The control bar and audio icon will not display if your workstation monitor is set to 16-bit color setting. Change your monitor *color* setting to 32-bit.

Usage Notes

- Multi-pane video clips can also be saved to your desktop and played using the Cisco Video Surveillance Review Player.
- If the Record Now feature is enabled, right-click the image and choose **Record Now** to record live video.
- If a camera is *soft-deleted*, you can still access the camera's recorded video but cannot display live video. Recordings are retained on the system until removed according to the recording retention settings.
- Click the icon to toggle between live and recorded video. The icon appears when recorded video is displayed.
- The first time you select a camera's recorded video, the playback begins slightly behind the live (current) time. When you toggle between live and recorded, recorded video returns to the previously selected timestamp.
- To maximize the video screens, move the new workspace to a separate monitor and double-click a pane to fill the entire browser window. To fill the entire monitor screen, right-click the image and select **Full screen mode**.
- To control the playback in multiple video panes, press `Shift-Click` to select multiple concurrent panes, or `Ctrl-Click` to select individual panes. The borders of all selected panes turn to orange. Controls and actions performed in one pane also affect the other selected panes. To deselect panes, select a single pane, or use `Shift-Click` or `Ctrl-Click` to deselect the panes.

Creating and Viewing Video Clips

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

Refer to the following topics for more information:

- Clipping Support By Application, page 74
- Supported File Formats And Playback Options, page 75
- Creating Video Clips, page 77
- Downloading and Viewing Clips, page 81

Tip

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

Clipping Support By Application

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

Table 1 Video Clip Support

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

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

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

Supported File Formats And Playback Options

Video clips can be created in multiple formats:

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

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

Table 2 describes the video clip options:

Table 2 Video Clip File Formats

File Format	Description
Virtual clip	Defines a segment of video on the Cisco VSM server for playback using a supported application, such as the browser-based Operations Manager. **Notes** • In this release, Virtual Clips can be created using the Operations Manager and Cisco SASD, but not Cisco VSM Federator or Cisco SASD Federator. See the "Clipping Support By Application" section on page 74. • Virtual clips can be any length. There is no maximum duration for a virtual clip. • Virtual clips do not support audio recording. • Virtual clips can be saved as an MP4 file (the 10 hour MP4 limitation applies). Audio cannot be included when saving MP4 files from a virtual clip.

Table 2 Video Clip File Formats (continued)

File Format	Description
MP4	MP4 clips are saved on the server and can be downloaded to a PC workstation or local disk. MP4 clips support a single video pane and can include audio (CVA/CVX files do not support audio). MP4 is a standard video file format that is playable on most computers and useful for sending to 3rd parties. **Audio Support** • MP4 clips can be saved with or without audio. The audio options are selected when the clip is saved. • MP4 audio playback is supported only with the Cisco VSM Review Player or VLC media player. **Notes** • In this release, MP4 clips can be created using the Operations Manager and Cisco SASD. To create MP4 clips using the Cisco VSM Federator or Cisco SASD Federator, use the Clip Search and Clip Management features. See the "Clipping Support By Application" section on page 74. • 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 6. • MP4 clips are saved on the server for 7 days and are automatically deleted from the server 7 days after creation. To download the clips to a local drive, use the **Get Clips Status** menu (see also the "Downloading and Viewing Clips" section on page 81). • Up to five MP4 clips can be created at a time per Media Server. If the limit is reached, wait for a clip to complete before creating a new one. • Users can only delete their own clips. Users that belong to a User Group with *Camera* permissions can also delete other users' clips. • If the clipping fails, see your system administrator for assistance. • Use the Cisco VSM Review Player to save MP4 files in the tamper proof MPX format. See the Cisco Video Surveillance Review Player User Guide for more information.
CVA	A Cisco video archive (CVA) can include multiple video panes that synchronize to the same time. CVA/CVX clips are downloaded immediately and not stored on the server. CVA files can only be opened in applications that support the CVA format (such as the Cisco Review Player). **Notes** • The maximum duration for a CVA clip is 24 hours per clip. • CVA files do not support audio playback.

Table 2 Video Clip File Formats (continued)

File Format	Description
CVX	A tamper proof CVA file. CVX files require a password that is entered when the file is created. You must enter the password to open and view the video file. **Notes** • CVX video playback will shut down if the file is tampered with. • CVX files do not support audio.

Tip You can also right-click a video pane and select **Take Snapshot** to save a still image in BMP, JPEG, PNG, and TIFF formats. See the "Using the Pop-Up Menu" section on page 85 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 74 for information on the clip formats supported by each appliaction in this release.

Procedure

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

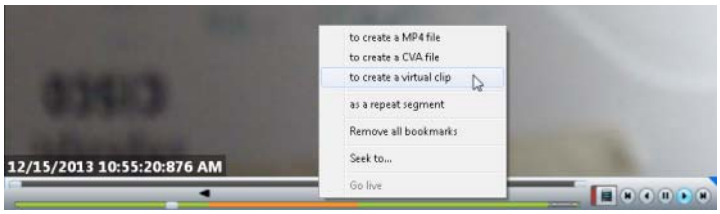
Tip To create a multi-pane clip in the CVA format, press *Shift-Click* to select multiple concurrent panes, or *Ctrl-Click* to select individual panes.

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).

Tip In recording mode , you can also right-click the image and choose **Select Clip Range** from the pop-up menu (see the "Using the Pop-Up Menu" section on page 85). 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.

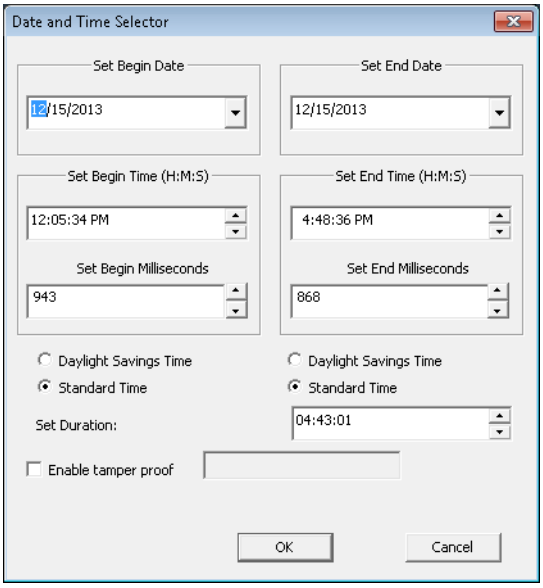
Step 4 Save the file:

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.

Figure 5 CVA Clip Settings



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.

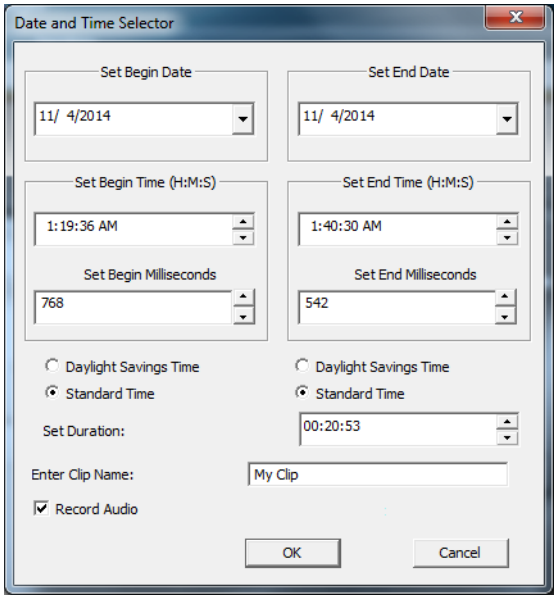
f. Play the clip using a video player such as the Cisco Review Player.

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.

Figure 6 MP4 Clip Settings



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** to include or exclude audio.

- This option is available if the camera supports audio and audio is enabled on the template.
- Audio playback is supported only with the Cisco VSM Review Player or VLC media player.

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

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

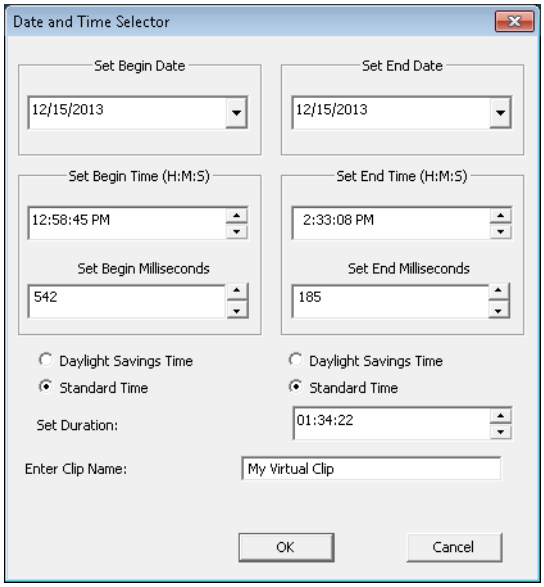
e. Download and play the clip as described in the “Downloading and Viewing Clips” section on page 81.

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.

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 81.

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 3 Video Clip Download Options

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

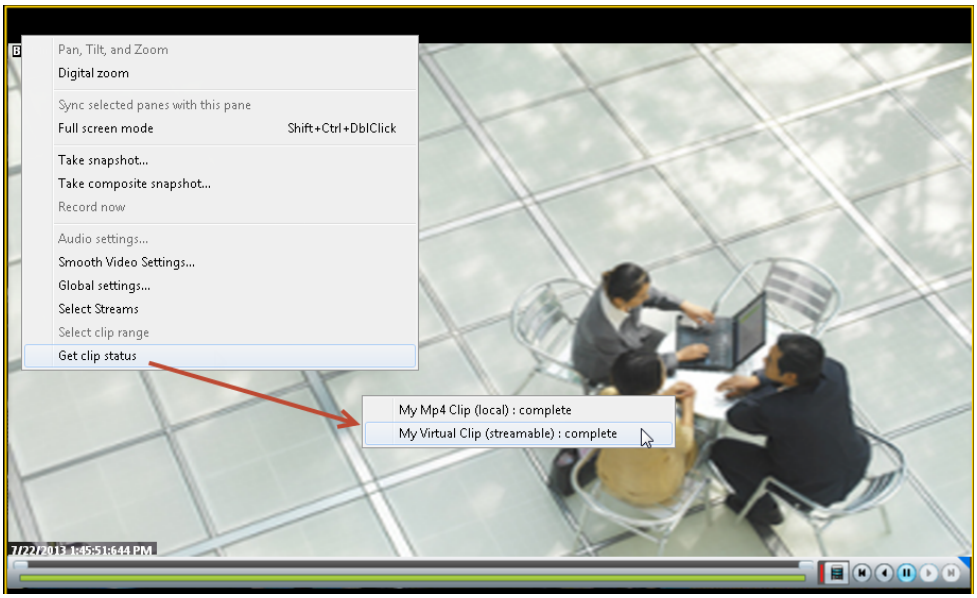
Procedure

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

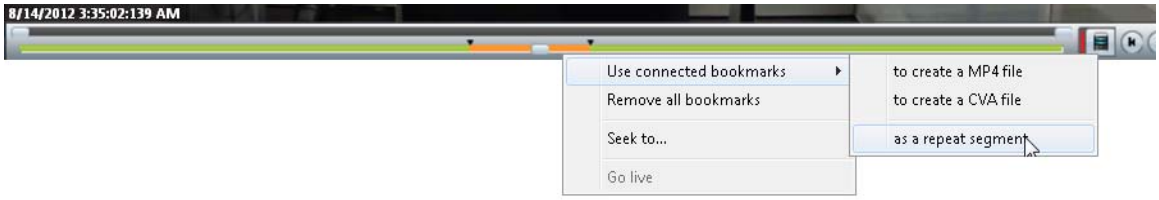
Step 3 (Virtual Clips) The clip plays in the video pane when selected.

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 fist time it is downloaded.

Creating a Repeat Segment

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

Figure 9 Create a Repeating Segment



Note Repeating segments are used with recordings only.

Procedure

Step 1 *Ctrl-Click-drag* the *seek bar* in a recording to create a bookmark (Figure 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 "Creating and Viewing Video Clips" section on page 74 to save the video to a separate file).

Procedure

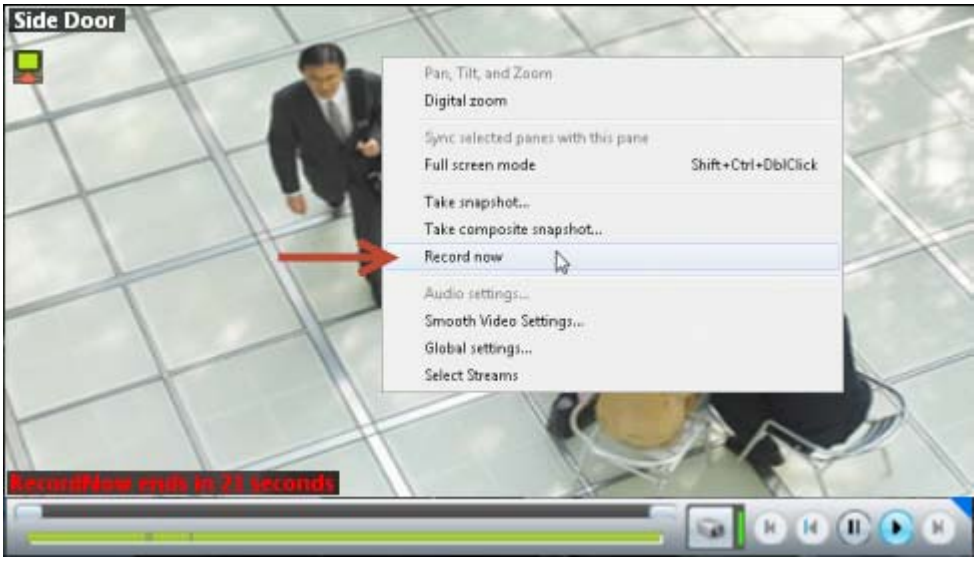
Step 1 Log in to the video viewing application and select a camera.

Step 2 Choose live video (see the "Viewing Live Video" section on page 67).

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

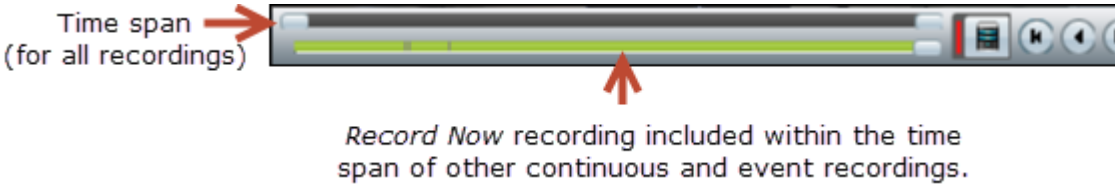


Step 4 To view the recorded video, review the following notes.

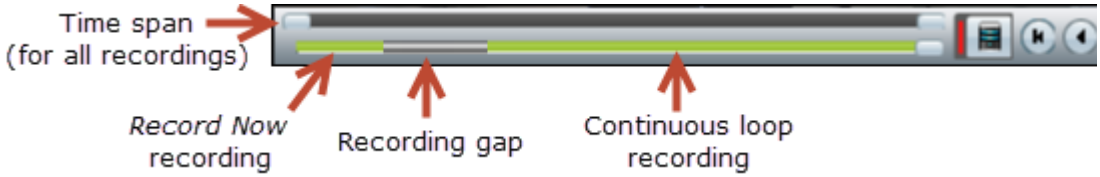
- Record Now clips are available from the primary stream only. Right click the image and choose **Select Streams and Clips** to view the recorded primary stream (disabled if the pane is synchronized).

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

- If the video is within the time span of other recorded video, there is no separate indication of the Record Now video. You can access the video as described in the "Viewing Recorded Video" section on page 70).



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



Note When the event retention time is exceeded, the Record Now recording is automatically deleted. To save the recording, see the "Creating and Viewing Video Clips" section on page 74.

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 67).

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

Camera Menu Item	Description
Pan, Tilt, and Zoom	(Live video only) Open the PTZ preset list that allows you to quickly adjust the camera view. See the "Using Pan, Tilt, and Zoom (PTZ) Controls" section on page 96
Digital zoom	Digitally enlarges the image to zoom in on a specific area. Double click the enlarged image to use a window-in window view. Adjust the viewing area in the small window to define the portion of enlarged video to display.

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

Camera Menu Item	Description
Sync selected panes with this pane	Synchronizes the playback from multiple video panes to the same time. • After a pane is synchronized, the menu item changes to **Remove this pane from sync**. • To synchronize additional panes, right-click an un-synchronized pane and select **Add selected panes to sync**. See the "Synchronizing Video Playback in Multiple Panes" section on page 92.
Full screen mode	Enlarges the video image to fill the entire monitor screen. **Tip** To exit, press `Esc`, or right-click and choose **Full screen mode** again.
Take snapshot	Saves a snapshot of a single video pane (*excluding* control icons, timestamps and other information) in BMP, JPEG, PNG, or TIFF format.
Take composite snapshot	Saves a snapshot of all panes in a multi-pane layout (*including* control icons, timestamps and other information) in BMP, JPEG, PNG, or TIFF format.
Record now	(Live video only) Immediately begins recording video. See the "Using Record Now" section on page 84 for more information. **Note** The Record Now option must be enabled in the camera configuration.
Audio settings	(Cameras with audio support only). Opens a window used to adjust video playback volume and balance.
Smooth video settings	(Live video only) Creates a smooth video playback if the playback is choppy or delayed due to network or other performance issues. See the "Using the Smooth Video Options When Viewing Live Video" section on page 91.
Global settings	Provides settings that apply to all video panes. For example: *UI transparency* and *zoom video to fit the pane*.
Select Streams	Allows you to select the live and recorded video streams (primary or secondary) supported by the camera. **Note** *Select Streams* is disabled when the pane is synchronized. See the "Synchronizing Video Playback in Multiple Panes" section on page 92 for more information. **Note** Selecting a long term server (LTS) backup recording can result in an error if the recording is not available of the backup is not complete.
Select clip range	(Archive video only) Selects a 10 minute clip range starting from current thumb position. The range bar is automatically scaled to 1 hour. See the "Creating and Viewing Video Clips" section on page 74 for more information.
Get clip status	Shows the current status of MP4 and virtual clips: In-Progress, Completed or Failed. Select a clip name to view the clip. MP4 clips are downloaded to a local disk (you are prompted to enter a filename and location. See the "Creating Video Clips" section on page 77 for more information.

Understanding Video Pane Border Colors

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

Table 5 describes the meaning of each color.

Table 5 Video Pane Border Colors

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

Using the Privacy Mask

- Overview, page 88
- Enabling the Privacy Mask Controls, page 90
- Related Information, page 90
- Cameras that Support the Privacy Mask, page 90

Overview

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

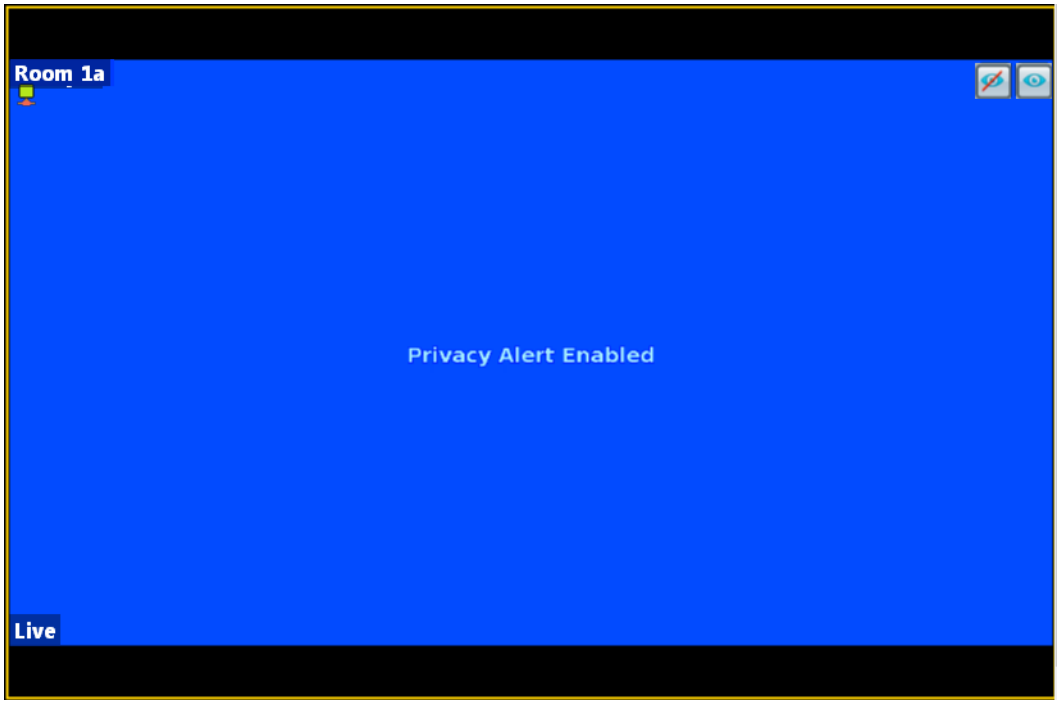
Note The function of the privacy mask icons was reversed in Cisco VSM release 7.5.

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

Icon	Purpose	Description
	Turn the Privacy Mask off (Default)	Click to enable normal video streaming, monitoring, and recording.
	Turn the Privacy Mask on	Click to block the camera's entire field of view and display a blank (blue) screen (Figure 12). • Live video is not transmitted and cannot be viewed by any workstation or monitor. • Recorded video displays the blank (blue) or flashing screen. • A "Privacy Mask Timer" causes the screen to flash after a period of time, which reminds the operator to disable the Privacy Mask. The default timer is 15 minutes and can be modified using the Operations Manager (**System Settings > Settings > Privacy Mask Timer**). **Note** The Privacy Mask is not disabled automatically; an operator must disable the Privacy Mask by clicking the icon to allow live video to be transmitted, viewed and (optionally) recorded.

For example, when you click the icon, the video frame for that camera is blank (Figure 12). The same blank (blue) screen is recorded (if recording is configured).

Figure 12 Privacy Mask Enabled



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

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

Enabling the Privacy Mask Controls

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

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

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

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

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

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

Related Information

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

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

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

Cameras that Support the Privacy Mask

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

Using the Smooth Video Options When Viewing Live Video

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

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

Icon Colors

The video quality icons in each pane indicate the following:

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

Usage Notes

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

Procedure

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

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

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

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

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

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

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

Note

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

Synchronizing Video Playback in Multiple Panes

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

Usage Notes

- All panes will play forward when synchronization begins, even if one or more of the panes was playing in reverse.
- Synchronization for recorded video is performed only if the time in the selected panes overlap. If the time for a video pane does not overlap with the master pane, the pane is excluded from synchronization.
- When you move the scroll bar for a video pane that is synchronized, that pane becomes the new synchronization master pane. The other synchronized panes play video according to the new master pane.
- If the seek controls are used to search video, the other synchronized panes pause until the seek completes, then continue to display video that is synchronized with the new master pane time.
- You can switch the synchronized panes between live and recorded video.

- To remove a pane from the synchronized playback, right-click the pane and choose **Remove This Pane From Sync** to remove it.
- To add un-synchronized panes, right-click the pane and choose **Add selected panes to sync**.
- The **Select Streams and Clips** menu item is disabled when a pane is synchronized.
- When 16 video panes are synchronized, some live video panes may appear to be not synchronized if the video stream is configured for the following:

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

Figure 13 describes the main synchronization attributes.

Figure 13 Synchronized Playback of Recorded Video

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

Procedure

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

Step 1 Select a layout or pre-defined view from the **View** menu.

Step 2 *Shift-click* or *Control-click* to select multiple video panes for synchronization.

The selected panes are displayed with a light yellow border.

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

The selected pane becomes the master pane.

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

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

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

Using Pan, Tilt, and Zoom (PTZ) Controls

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

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

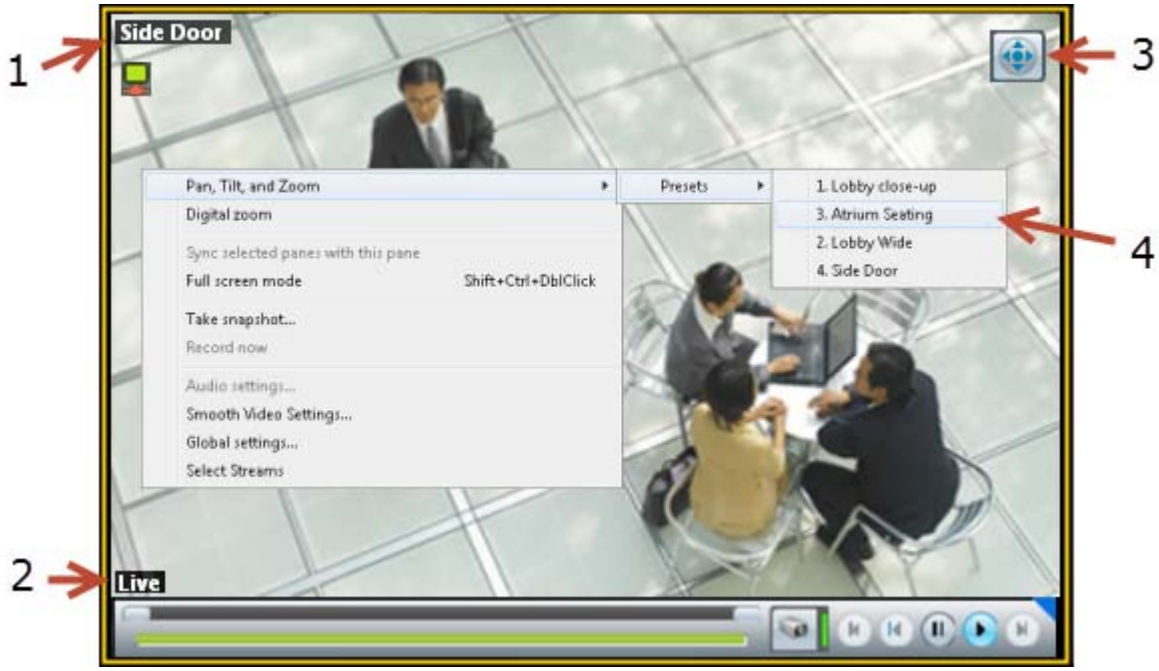
    or
  - Hold down the Shift key and then press the left mouse button. Drag the mouse up or down to zoom.

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

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

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

Figure 14 Camera PTZ Controls



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

PTZ Usage Notes

- To use a USB joystick, see the "Calibrating a Joystick for Windows 7" section on page 99.
- 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 101.
- You must also belong to a user group with *Perform PTZ* permissions.
- PTZ commands are available only if the primary Media Server is functional. If the Primary server goes down, or is not available on the network, PTZ commands will not function even if video is still being delivered by a redundant server (if configured). See the "High Availability: Cisco Media Servers" section on page 1 for more information.

PTZ Control Procedure

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

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

a. Click **Monitor Video**.

b. Expand the location tree and select the camera.

c. Highlight a video pane and double-click a camera name.

Step 2 Click the PTZ control icon to enable PTZ:

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

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

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

Using a Mouse

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

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

Using a USB Joystick

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

Tip See the "Calibrating a Joystick for Windows 7" section on page 99 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.

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

Understanding Return To Home

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

Workstations can also be configured to display a warning before the camera returns to home, which allows you to cancel the operation and reset the timer, if necessary (Figure 15):

Figure 15 Return To Home Warning

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

Calibrating a Joystick for Windows 7

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

Procedure

Step 1 Install and configure the USB joystick according to the manufacturer instructions.

- See the device documentation for more information.
- The manufacturer may also include a calibration utility that can be used instead of the built-in Windows utility.

Step 2 In Windows 7, calibrate the device using the **Game Controllers** control panel.

a. Select **Control Panel** from the **Start** menu.

b. Select **Hardware and Sound**.

c. Select **Devices and Printers**.

d. Double-click **Game Controllers**.

e. Highlight the joystick device and click **Properties**.

f. Click **Calibrate** in the pop-up window.

g. Follow the on-screen instructions to complete the process.

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

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

Using PTZ Controls When Multiple Video Windows are Displayed

When multiple viewing panes are displayed, only a single pane can have PTZ controls enabled at a time (Figure 16). This prevents a USB joystick from affecting more than one pane.

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

Figure 16 PTZ Controls in a Multi-Pane View

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

Note PTZ movements are available only when viewing live video.

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

Thumbnail Search

Contents

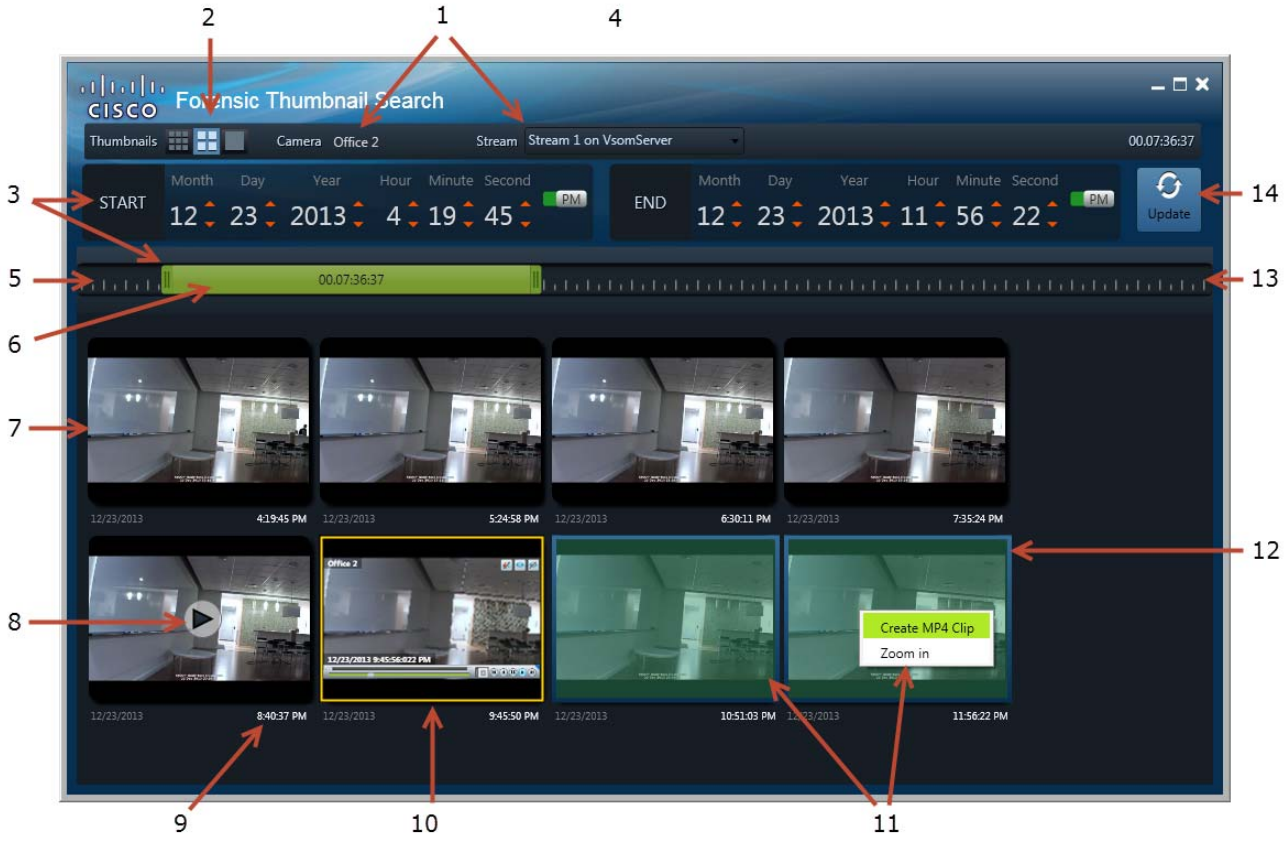
- Overview, page 104
- Procedure, page 105

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.	**8**	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.
2	Thumbnail image size.	**9**	Thumbnail clip start time.
3	The start date and time for the displayed thumbnails.	**10**	Video playback. **Tip** See "Controlling Video Playback" for more information.

4	The end date and time for the displayed thumbnails.	**11**	Shift-drag the mouse to select multiple thumbnails and display the following options: • **Create MP4 Clip**— create a video clip. Enter the clip name and select a supported audio codec. • **Zoom In**— refresh the thumbnails to include only the selected span.
5	Recording start time—The start of the entire video archive.	**12**	Thumbnail image from the end of the time span.
6	Range Bar— • Drag the bar left or right to change the span of video that displays thumbnails. • Click and drag the start and end time to adjust the duration.	**13**	Recording end time—The end of the entire video archive.
7	Thumbnail clips—The top left thumbnail displays an image from the beginning of the time span.	**14**	Refresh the displayed thumbnails.

Procedure

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

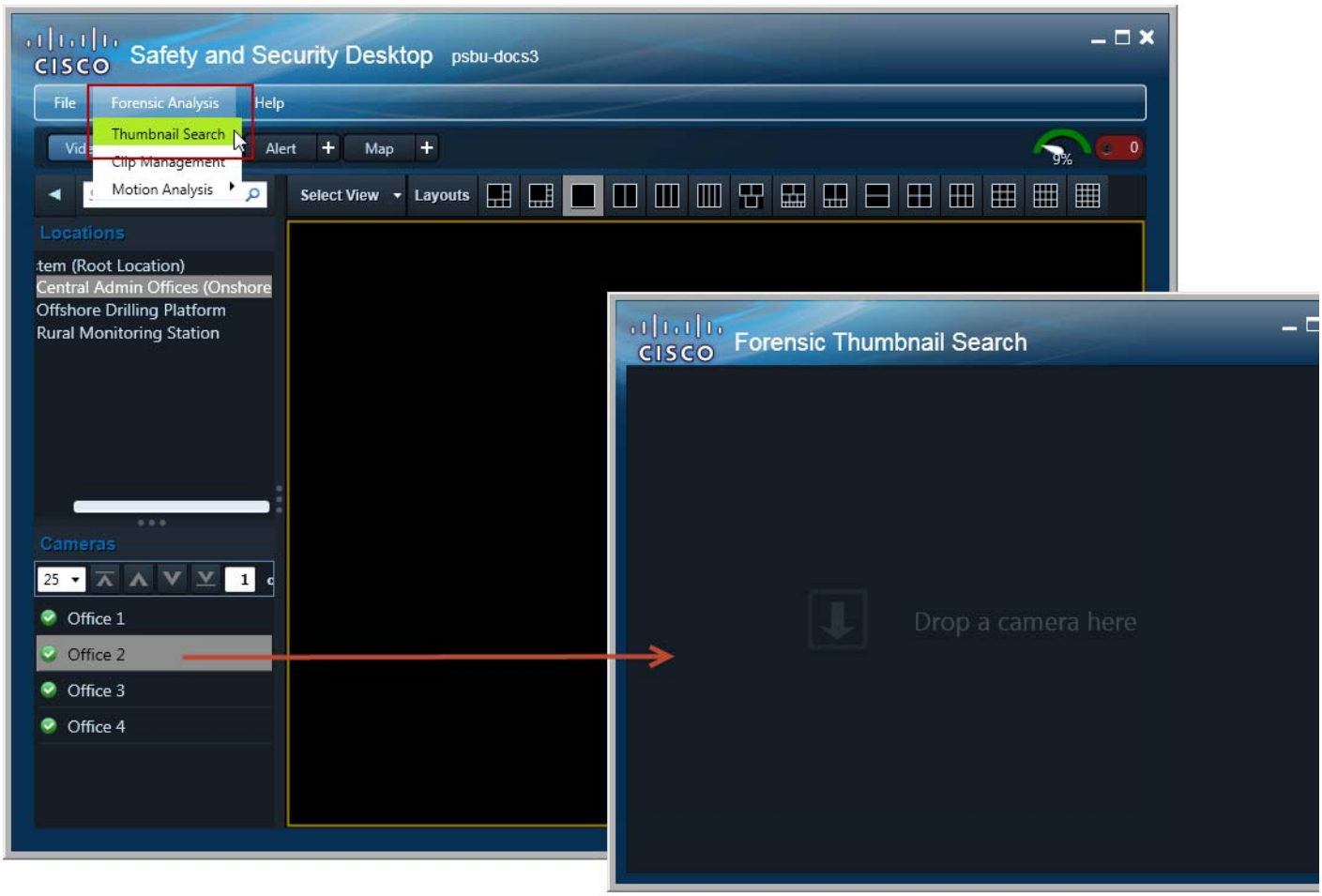
Step 1 Log into the Cisco SASD or Cisco SASD Federator application.

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).

Figure 2 Drag a Camera to the Forensic Thumbnail Search Window



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**.

c. Enter a clip name.

d. Select a supported audio codec, if audio is available for the selected time.

e. Click **OK**.

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 download 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

- See "Managing Video Clips" in the Cisco Video Surveillance Safety and Security Desktop User Guide for more information.
- 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.

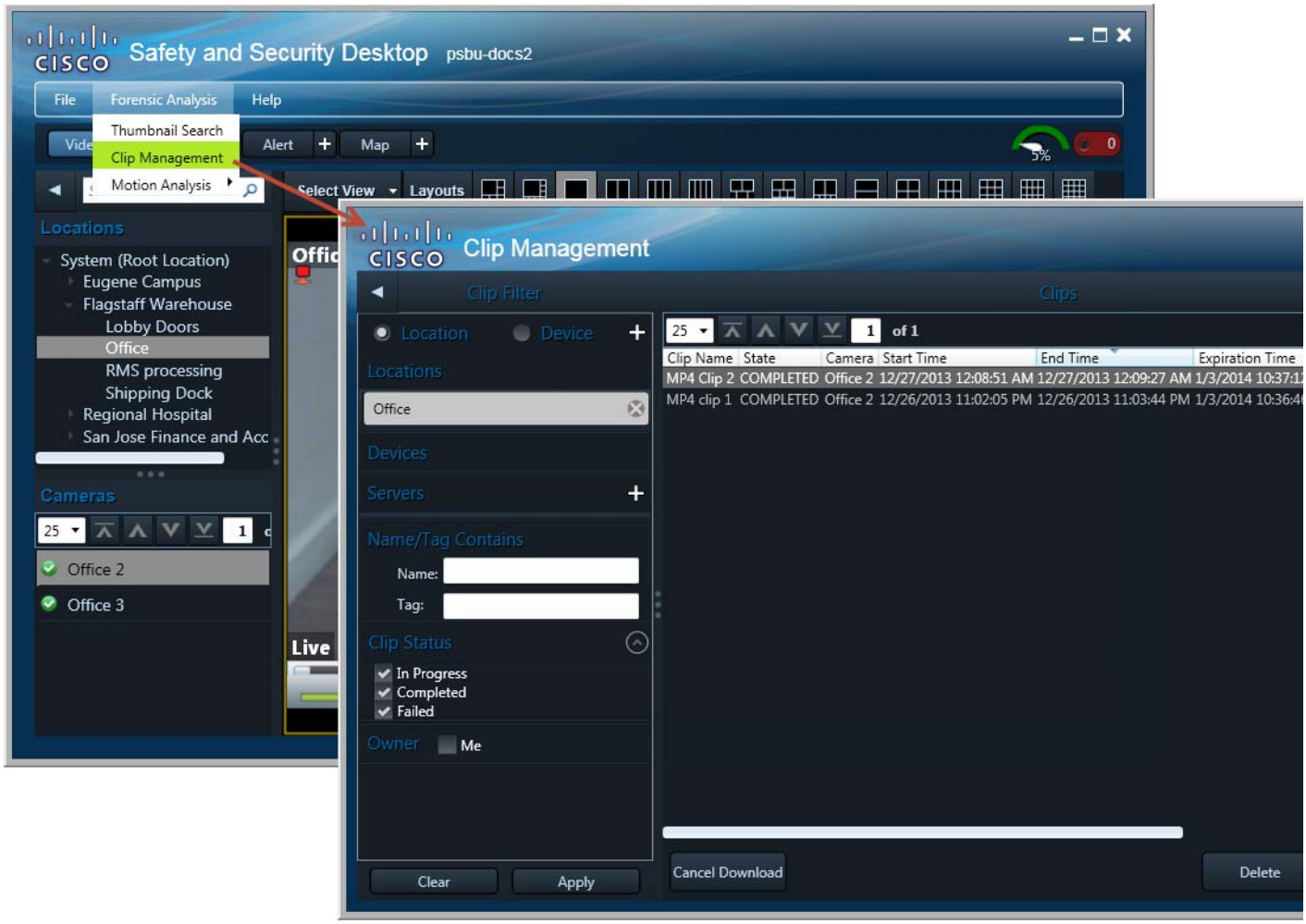
Step 2 Create one or more MP4 video clips.

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.

Figure 1 Clip Management Window

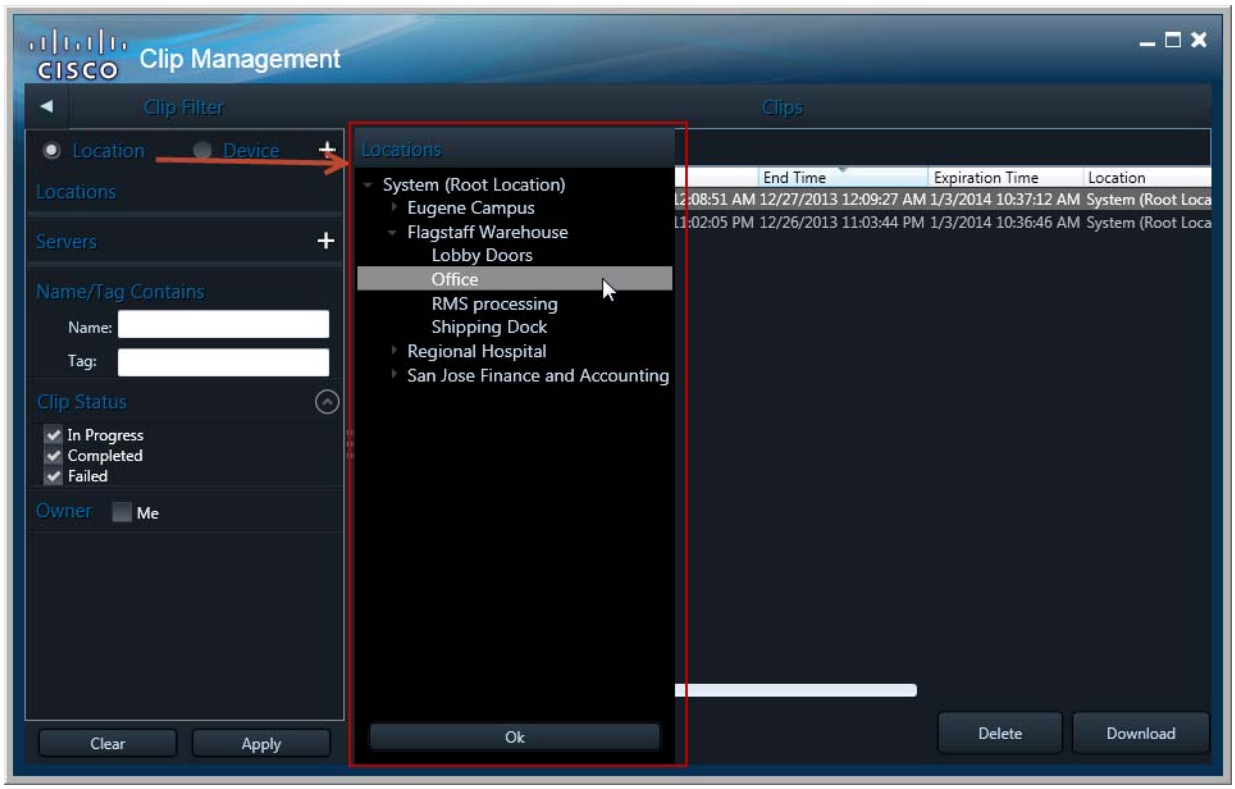


Step 5 (Optional) Select a location or device (Figure 2):

- 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



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

Field	Description
Servers	Click + to select a specific Cisco Video Surveillance Media Server. Only clips created by the cameras managed by that Media Server will be displayed.
Name/Tag Contains	Enter a full or partial name for the clip(s). **Tip** The clip name is entered when the clip is created
Clip Status	Select the status for the displayed clips. Any status not selected will not be displayed.
Owner	Select **Me** to display only clips you created. De-select to display clips created by other users.

Step 7 Click **Apply**.

Step 8 Review information about the clips.

Table 2 Video Clip Information

Field	Description
Clip Name	The clip name entered when the clip was created. The default is “My Clip” if no name is entered.
State	In-Progress, Completed or Failed
Camera	The camera name where the clip originated.
Start Time	The start timestamp for the clip.
End Time	The end timestamp for the clip.
Expiration Time	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.
Location	Location of the cameras where the clip originated.
Media Server	The Media Server that manages the camera video where the clip originated.
Owner	The user that created the clip.
Tags	Tags associated with the clip.
Download %	The status of the clip download (see Step 9).

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 113
- Understanding Luminance Metadata and Motion Analysis, page 114
- Requirements, page 114
- Summary Steps, page 115
- Motion Video Search Detailed Procedure, page 116
- Metadata Job Management, page 127

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.

Note 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 114 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 "Creating and Viewing 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

Requirements	Complete? (✓)
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. **Related Information** • Cisco Video Surveillance Operations Manager User Guide • See your system administrator for more information.	❑

Table 10-1 Metadata Requirements (continued)

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

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 127 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.

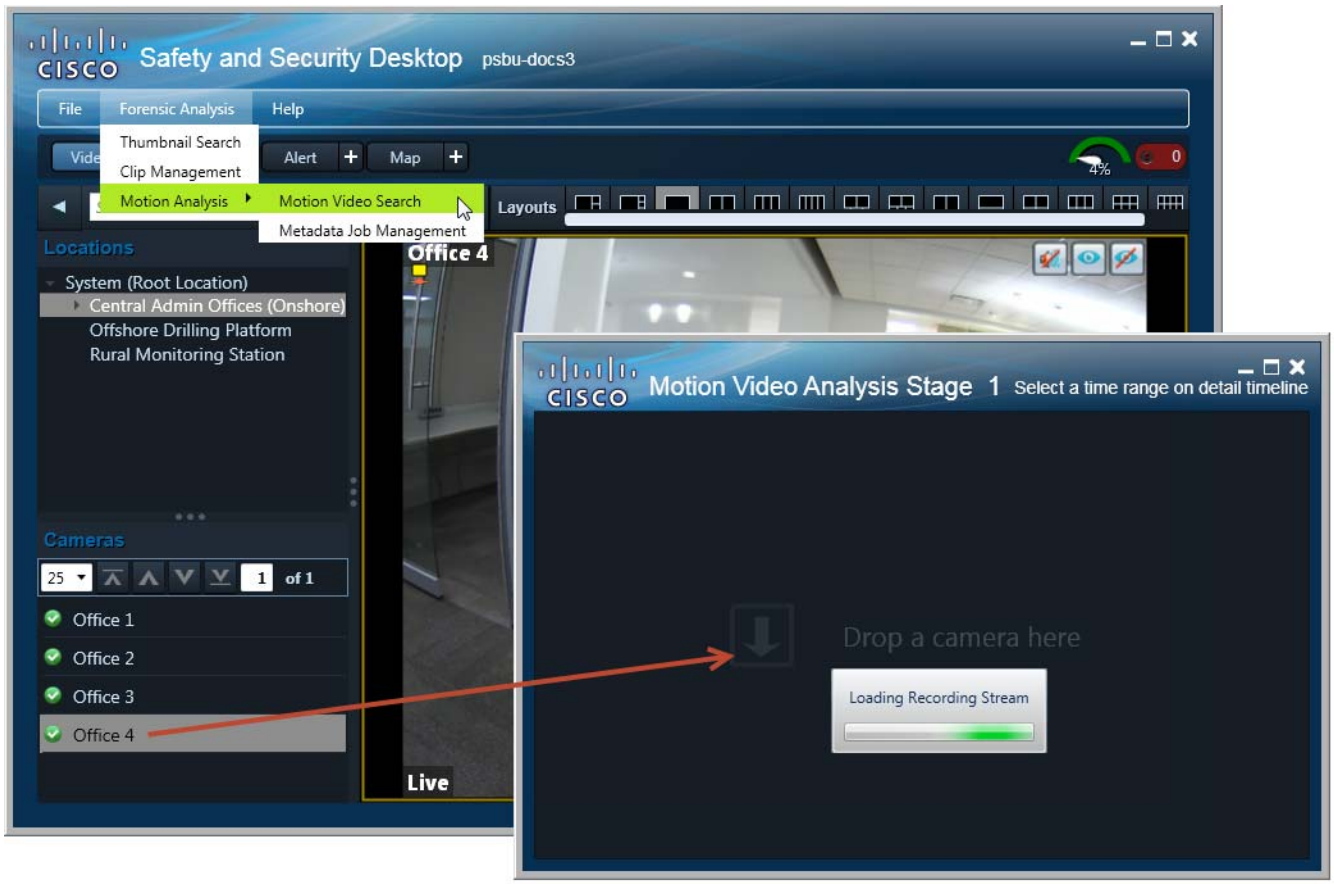
- See "Logging In".
- Motion Video Analysis is not supported using the Cisco SASD Advanced Video Player or Cisco SASD Federator applications.

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 the *Luminance* metadata track is not configured on the camera (using the Operations Manager). See "Requirements" for more information.

Figure 1 Motion Video Search Window



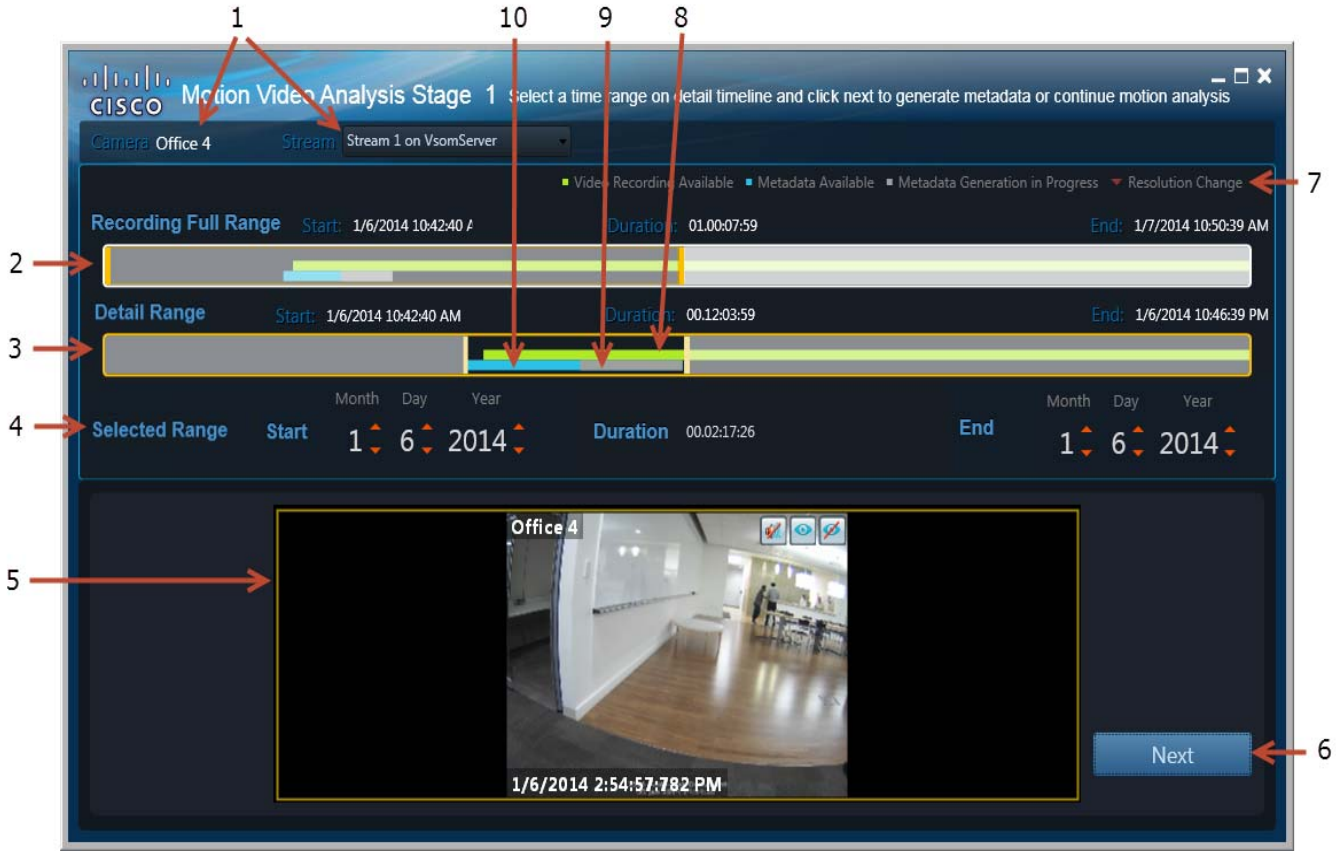
Step 4 Stage 1: Generate the *luminance* metadata:

In Stage 1, select a span of recorded video and generate the *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 127 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 114.
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 127 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 127 for information on job status.
10	Blue—Metadata was successfully generated.

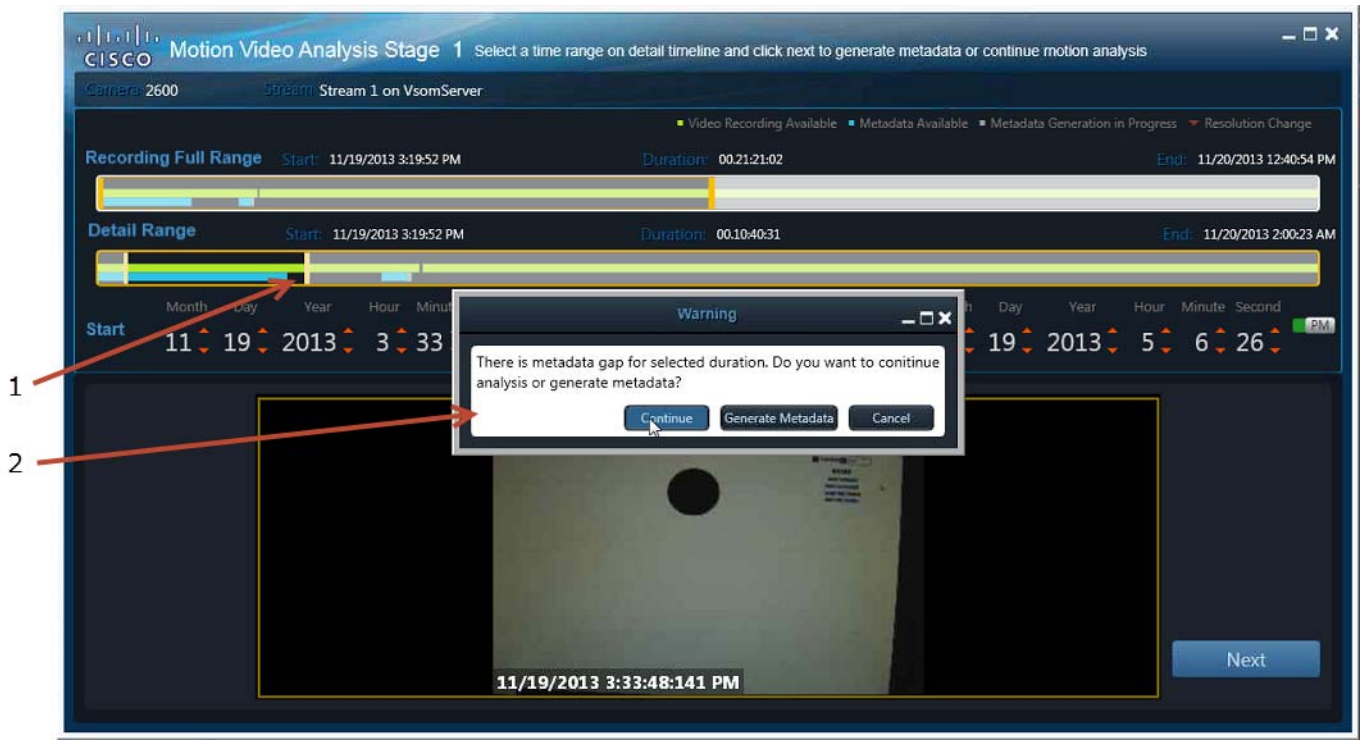
b. Click **Next** and do one of the following:

- 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).

Figure 3 Metadata Gap



1	Metadata gap in the selected recording.
2	Prompt that appears if a metadata gap is selected: • **Continue**—Continue to the motion analysis window without generating metadata for the metadata gap(s). • **Generate Metadata**—Generate metadata for the gaps. Click Next again to continue to Stage 2 (Step 5). • **Cancel**—Cancel the operation and return to the Stage 1 window.

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.

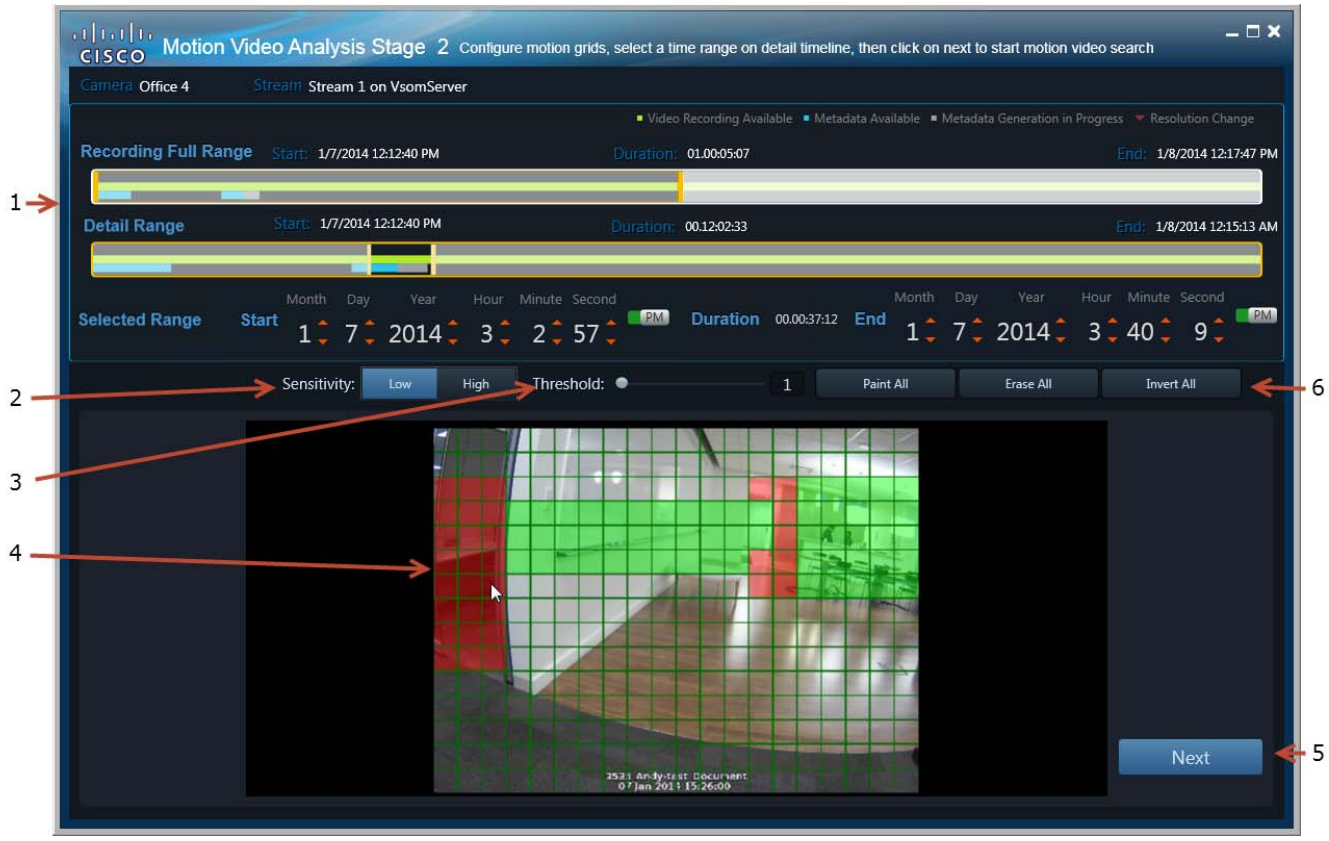
- **Low**—grids with low sensitivity are painted green. To trigger motion detection for a low sensitivity grid, large luminance value changes are required on the entire area of the grid.
- **High**—grids with high sensitivity are painted red. To trigger motion detection for a high sensitivity grid, small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

6	Tools to assist in grid selection **Paint All**—Paints all of the grids with low or high detection (depending on the sensitivity selected). **Erase All**—Deselects all grids. No grids will detect motion. **Invert All**—Invert all the painted area to be not painted. Unpainted areas are changed to painted.

d. 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)

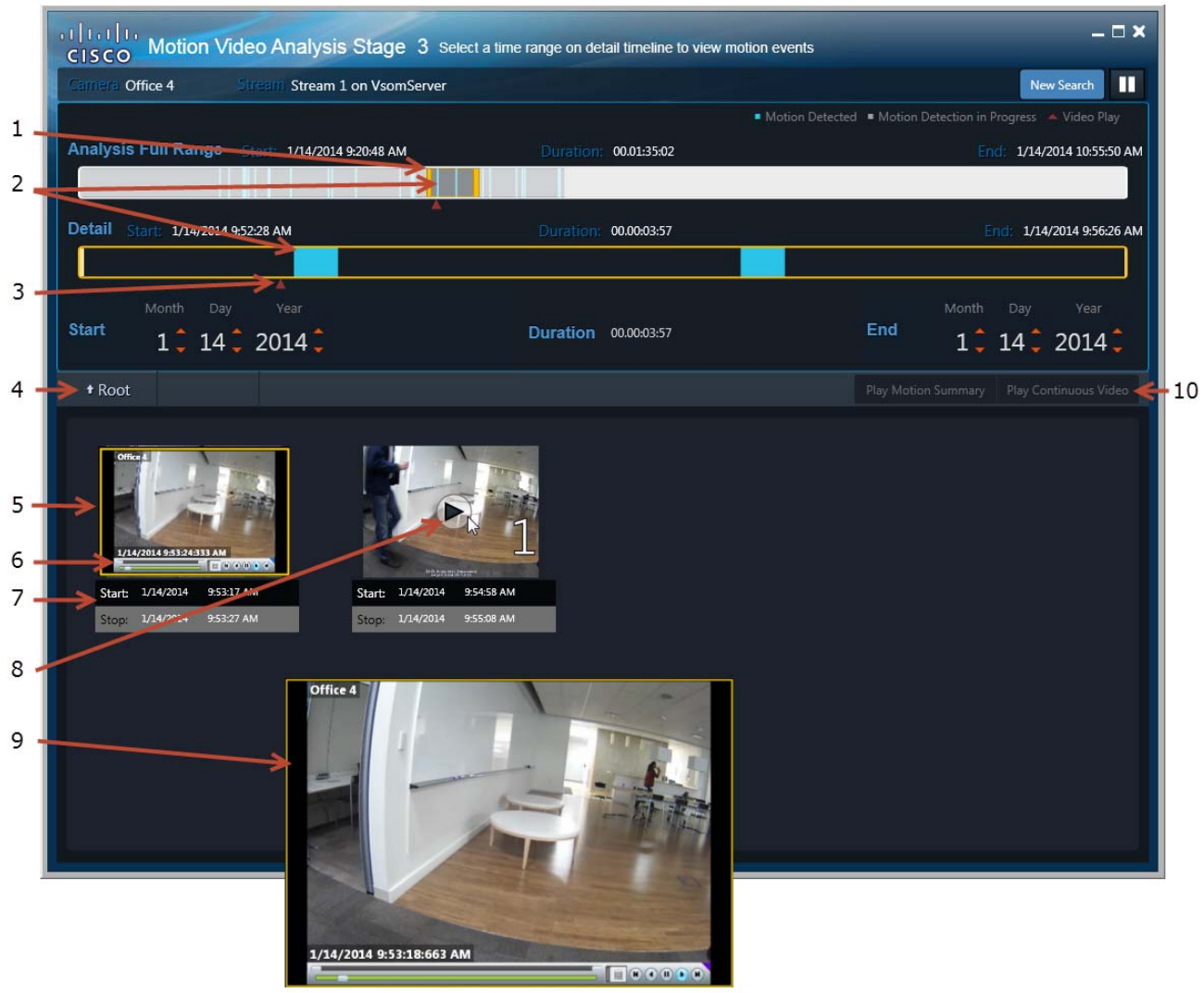
1	The camera and stream (source) for the video recording. **Note** Only the primary stream is supported in this release.
2	Analysis Full Range—The entire range of recorded video that was selected in Stage 2 (see Step 5). The motion results are displayed for this range by default. Drag the orange bars 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.

7	Thumbnail Groups—The thumbnail representation of motion events for the Selected Range. • If there are more than 24 motion events for Selected Range, the motion events are displayed in “Summary Mode”. • The Selected Range is divided into 24 equal duration of time. Each is called “Thumbnail Group”. Click in a thumbnail group to view and play the individual events for that group (see Figure 6). • Each Thumbnail Group has a From/To timestamp, and the image is the first motion event in that group's duration. • If there are less than 24 motion events for Selected Range, all motion events are displayed in “Detail Mode”. Each motion is represented by a thumbnail, and has a Start/Stop time.
8	The number of motion events in the thumbnail group.
9	The beginning and end time of the recorded data included in the thumbnail group.
10	No Motion—No motion started in the thumbnail group’s duration. **Note** Any motion event that began in the previous thumbnail group and continued into this group is not included in the motion count.
11	Command menu—Left-click and drag to select multiple thumbnails and select one of the following options: • **Create MP4 Clip**: Create clips, one for each motion event in the selected thumbnail groups (up to 5). • **Zoom In**: Change the Selected Range to the selected thumbnail groups duration.
12	Click in a thumbnail group to view and play the individual events for that group.
13	Processing—Indicates that the video is still being analyzed for motion events based on the filters applied in Stage 2 (see Step 5).
14	Motion event continuation—Indicates that a motion event begins in one thumbnail group and continues to the next thumbnail group. • “Motion Continued” is displayed if the motion started in the previous group's duration and stopped in (or beyond) the group's duration. • Click the beginning group to view the motion event.
15	• **Play Motion Summary**—Plays all motion event video. • **Play Continuous Video**—Plays all video for the selected duration, including video that does not include motion events.
16	Legend—Describes the recording status in the timeline. • Blue—A motion event was detected based on the filters applied in Stage 2 (see Step 5). • Grey—The video is being analyzed for motion. • Red—Video Play. The location of the video currently being played (see Figure 6).
17	Pause—Pauses the motion analysis processing. Select again to resume processing.
18	**New Search**—Return to Stage 2 to select a different time span and/or apply different filters.

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.

10	• **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.

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 "Creating and Viewing Video Clips" for more information.

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.

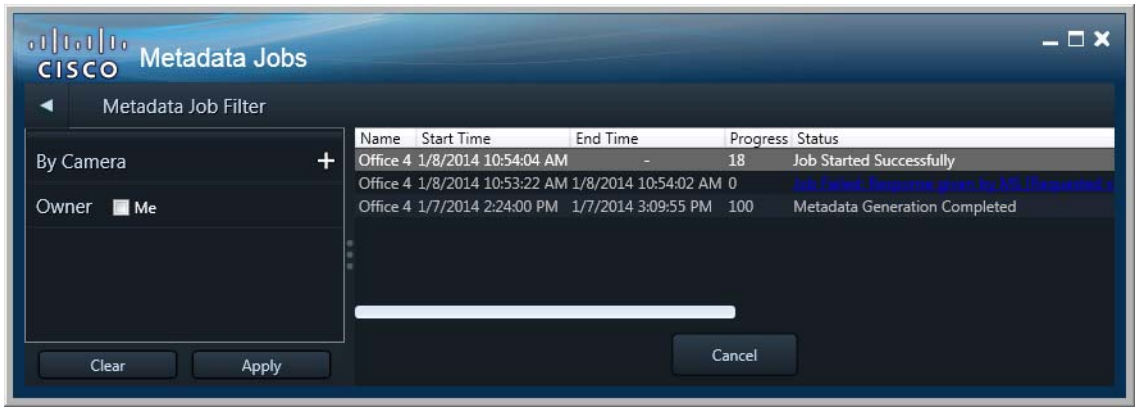
Procedure

Step 1 Click ✚, select a camera, and click **Apply** to display the metadata jobs for recordings from that device.

Step 2 Select one or more users to narrow the results to the user(s) that triggered the jobs.

Step 3 (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.

Camera Recording Management

Contents

- Overview, page 130
- Requirements, page 132
- Camera Local Recording Management Window, page 133
- Procedure to Copy Video From a Camera to a Server, page 136
- Viewing Camera Storage Job Status, page 137

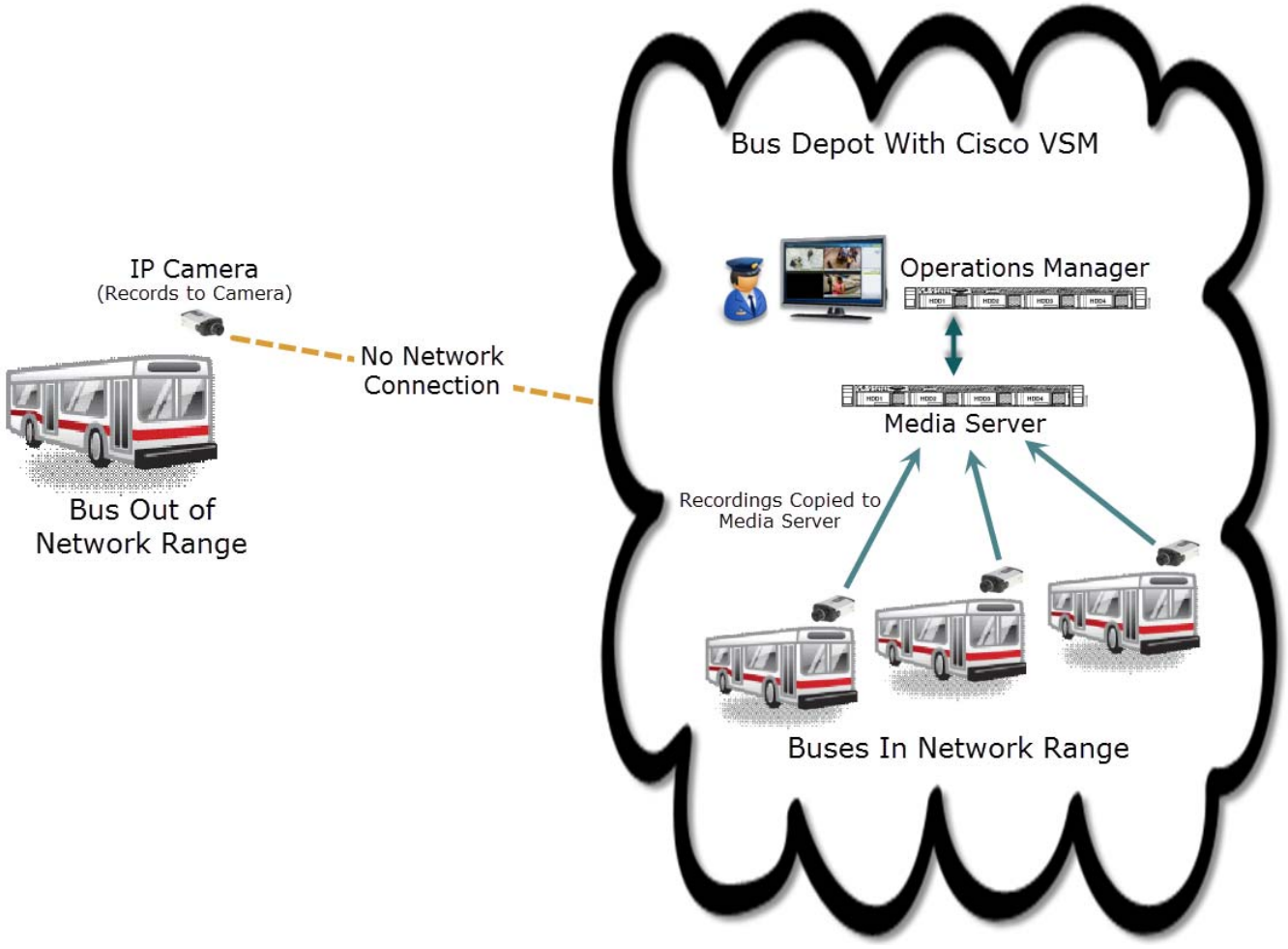
Overview

Cameras that support on-device video storage (such as an SD card) can save recordings on the camera, and copy the video to the Cisco VSM system at a later time. This feature is typically used when the camera is out of network range while recording.

For example, in Figure 11-1 a bus equipped with an IP (network) camera can save video recordings to the camera even when the bus is transporting passengers. When the bus returns to the depot, and is again in network range, the recordings can be copied to the Media Server that supports the camera.

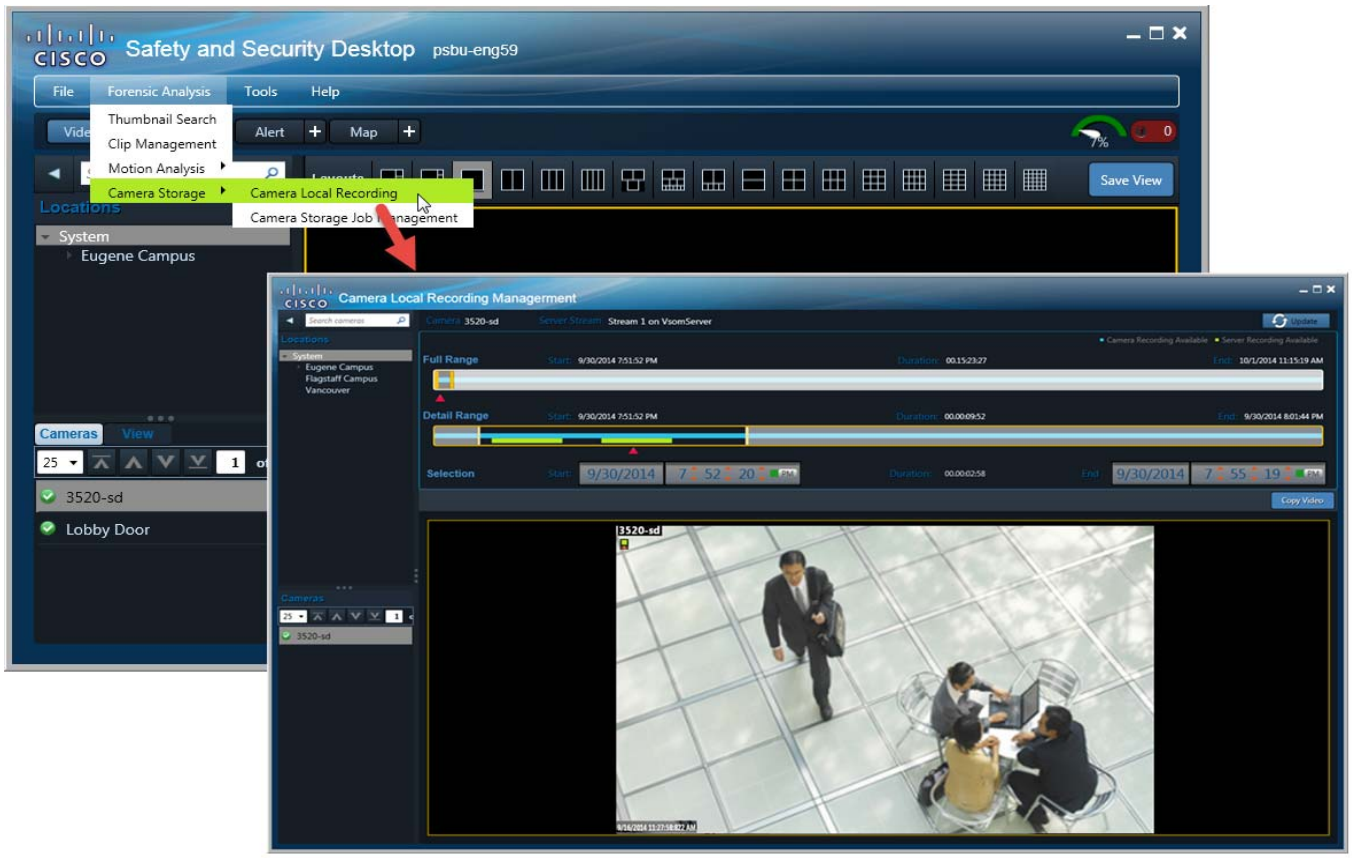
A Cisco VSM administrator uses the Operations Manager browser-based interface to define the camera's recording schedule, and whether the recordings should be automatically copied to the server when the device rejoins the Cisco VSM network.

Figure 11-1 "Connected Edge Storage": Camera Recording on Device and Copy to a Media Server



The Cisco SASD Camera Local Recording Management feature can also be used to manually copy additional recordings from the camera to the server for viewing and analysis (Figure 2). This feature lets you view the video that was already copied to the server, identify the video that exists on the camera but was not yet copied, and copy additional video to the Cisco Media Server.

Figure 2 Camera Local Storage Management Window



See Camera Local Recording Management Window, page 133 and Procedure to Copy Video From a Camera to a Server, page 136 for more information.

Note You can play the video that is copied to the server, but you cannot play video that exists only on the camera.

Tip A Operations Manager user can also manually trigger the copy action using the Operations Manager interface.

Requirements

Complete the following requirements to enable local camera recording. At least one camera must support local storage.

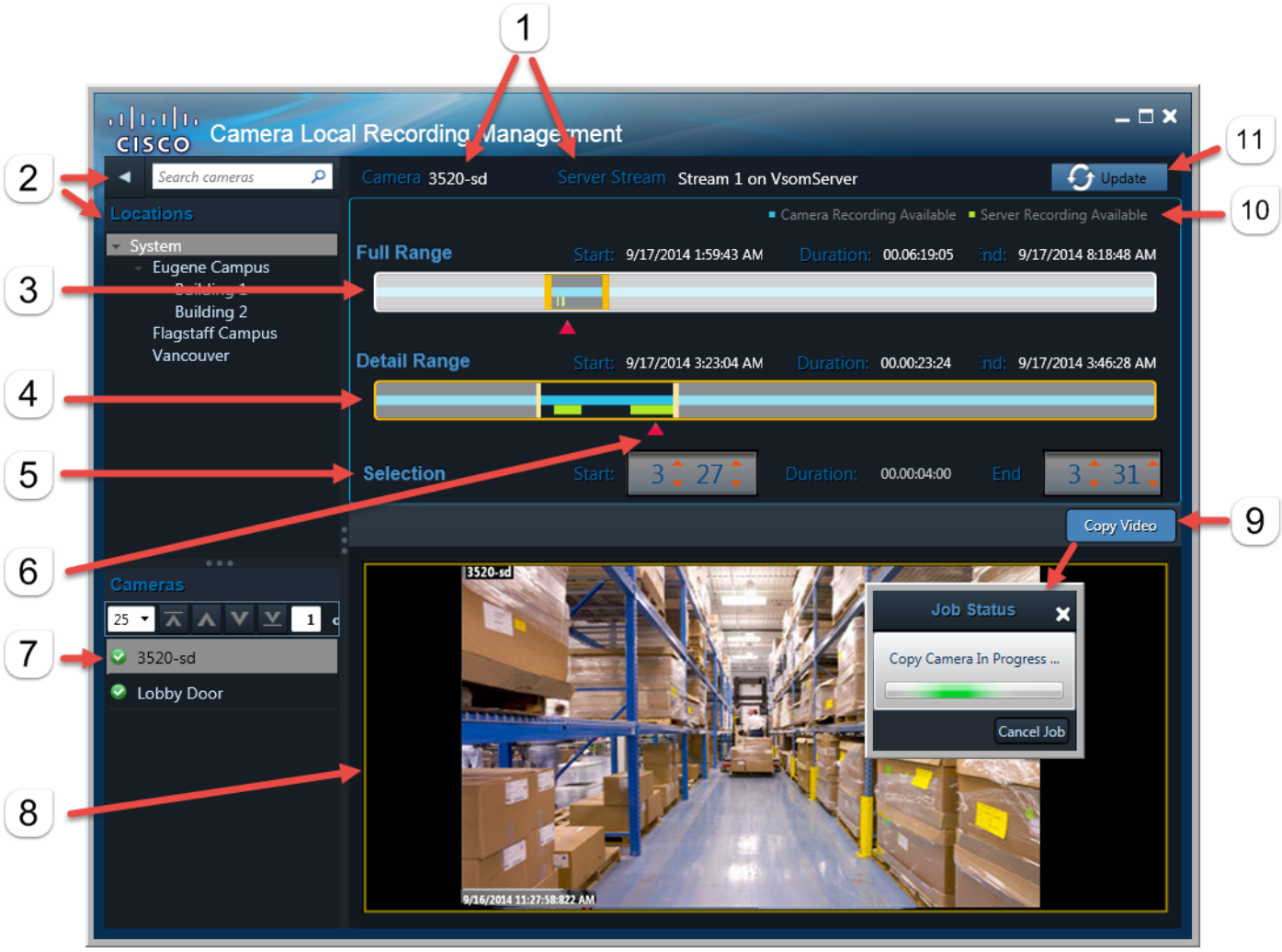
Table 11-1 Requirements

Requirements	Complete? (✓)
At least one IP network camera that supports on-device video storage. The Cisco Video Surveillance Operations Manager is used to add cameras to Cisco VSM, configure camera recording schedules, and define the rules to automatically copy camera recordings to the Cisco Media Server. **Related Information** • Cisco Video Surveillance Operations Manager User Guide • See your system administrator for more information.	❑
A Cisco VSM user account that belongs to a User Group with *Manage* permissions for *Cameras* is required. **Related Information** • Cisco Video Surveillance Operations Manager User Guide • See your system administrator for more information.	❑
The Cisco SASD desktop application must be installed on a monitoring PC. **Note** Camera Local Recording Management is not supported using the Cisco SASD Advanced Video Player or Cisco SASD Federator applications. **Related Information** • Cisco Video Surveillance Safety and Security Desktop User Guide	❑

Camera Local Recording Management Window

Figure 3 summarizes the controls available in the Camera Local Recording Management window. See the Procedure to Copy Video From a Camera to a Server, page 136 for additional instructions to use these controls.

Figure 3 Camera Local Recording Management Window



1	The camera and stream for the video recording.
2	Search for cameras by name or keyword, or select a location.

3	Full Range—The entire recording range available on the camera storage device, such as an SD card. The selected span (between the orange bars) is displayed in the Detail timeline. • 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. The timestamps show the entire range of the available recording: • Start—the beginning time stamp of the first available recording on the camera storage device. • Duration—the entire duration of video available on the camera storage device. • End—The end time stamp of the most recent recording available on the camera storage device
4	Detail Range—The time range selected in the Full Range. Use the Detail Range to fine-tune the video span that will be copied from the camera to the server. 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.
5	Selection—The start and end timestamps for the video that will be copied. Enter different values to micro-tune your selection. For example, you can edit the beginning and ending seconds.
6	Play head—The recorded video that is being played in the viewing pane. Drag the red play head to a different location to play that video. Only video copied to the Media Server can be played. IF you try to play video that exists only on the camera, the play head skips to the next available server recording.
7	Cameras for the selected location, or from the camera search. Drag and drop a camera onto the viewing pane to view the available recordings on that device.
8	Recording video feed from the selected camera stream. • Use the video area to watch the video after it's copied to the server (shown as a green bar in the timeline). • Any recording segments not yet copied to the server are displayed as gaps in the green bar on the timeline bar. • Video playback skips over any recording gaps (recording segments not available on server). • The play head (red triangle) corresponds with the video that is currently playing. When gaps occur, the play head skips to the next available recording segment (in green). • Drag the red play head along the timeline bar to locate the time of interest. The video will play from that time when you release the play head. If video is not available on the server for the selected time, however, the play head skips to the next available video on server.
9	Click **Copy Video** to copy the selected video span from the camera to the Cisco Media Server. • Only video that is not already on the server will be copied (video that is already copied to the server will be skipped). • The video will play after the copy is complete. • See Viewing Camera Storage Job Status, page 137 to view the copy jobs.
10	Legend—Describes the recording status in the timeline. • Green—Recording that was copied to the Cisco Media Server. Gaps in the green bar indicate times when video was not copied. • Blue—Recording that is available on the camera's local storage device, such as an SD card.

11	**Update**—Refresh the screen to display changes to the recorded video. • The display is automatically updated on a regular basis, but you can click **Update** to immediately refresh the results. • For example, changes may occur if additional video was added to the camera storage device, or if video was copied to the server by the system or another user.

Procedure to Copy Video From a Camera to a Server

Use the Camera Local Recording Management window (Figure 3) to copy recorded video from a camera's storage device (such as an SD card) to the Cisco Media Server.

Procedure

Step 1 Complete the Requirements, page 132.

Step 2 Log in to the Cisco SASD application.

- See "Logging In".
- Camera Local Recording Management is not supported using the Cisco SASD Advanced Video Player or Cisco SASD Federator applications.

Step 3 Select **Forensic Analysis > Camera Storage > Camera Local Recording** (Figure 2).

Step 4 Select a location, and drag and drop a camera onto the management window (Figure 3).

Note An error message appears if the camera does not support local recording storage. See "Requirements" for more information.

Tip You can also search for a camera by name or keyword.

Step 5 Select a span of recorded video from the Full Range bar to narrow the results displayed in the Detail Range (Figure 3).

Step 6 Use the Detail Range to select a span of video that should be copied from the camera to the server.

Step 7 (Optional) Use the Start and End settings to fine-tune your selection.

Step 8 (Optional) Use the red play head to play video that was previously copied to the Media Server.

Step 9 Click **Copy Video** to copy the video from the camera to the Media Server.

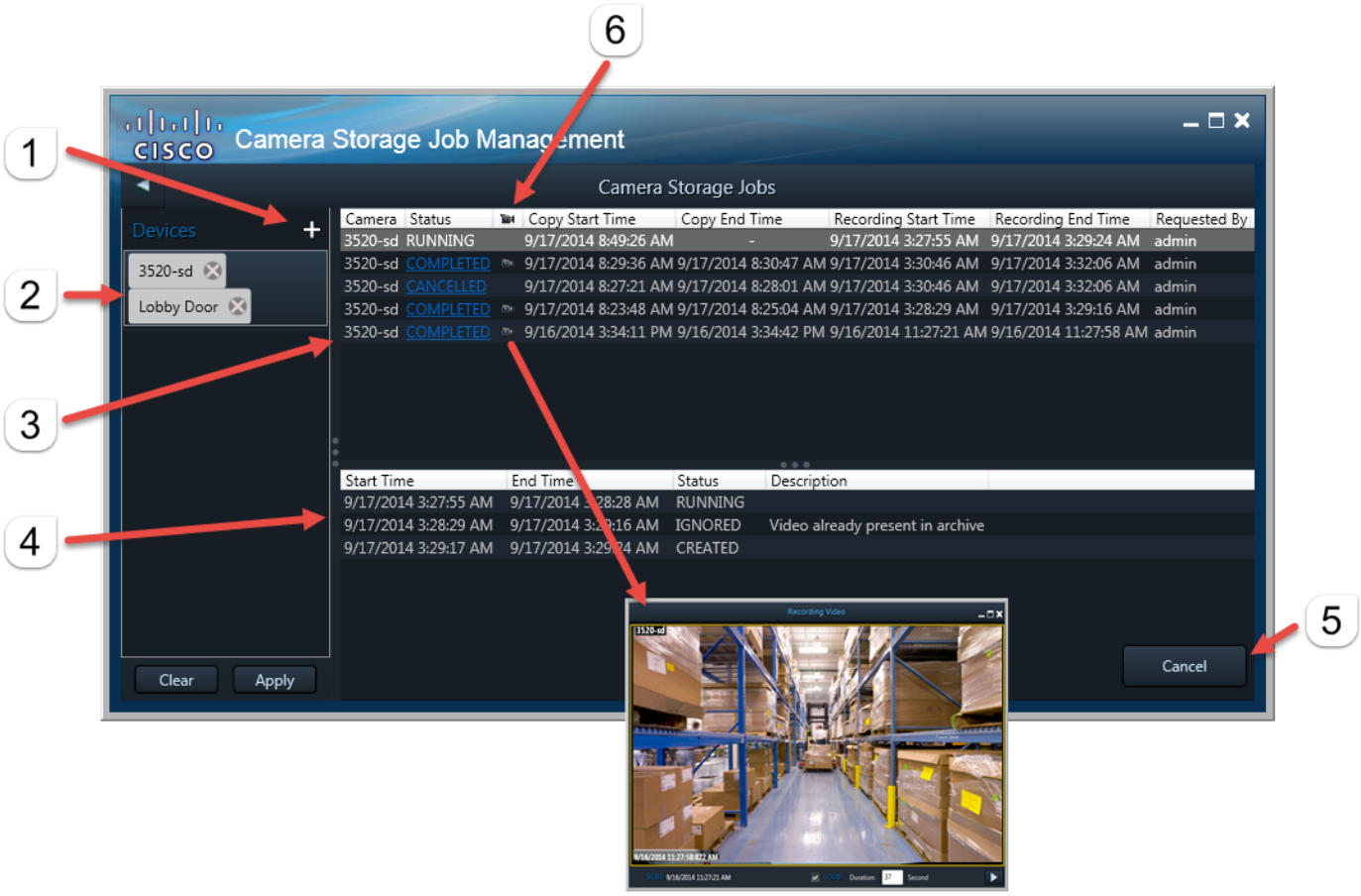
- Any video already on the Media Server will be skipped.
- The selected video will play after the copy operation is complete.

Step 10 (Optional) Use the Camera Storage Job Management page to view the status of the copy jobs. See Viewing Camera Storage Job Status, page 137.

Viewing Camera Storage Job Status

Select **Forensic Analysis > Camera Storage > Camera Storage Job Management** (Figure 4) to view the status of camera storage copy jobs triggered in Cisco SASD.

Figure 4 Camera Storage Job Management



1	Click ✚ to select one or more cameras, and click **Apply** to display the jobs for those devices.
2	The selected cameras. Click **Apply** to display the jobs for the cameras in the list.

3	The cameras storage jobs. Select a job to view the sub-jobs. Jobs include the following information: • Camera—The camera where the recording is stored. • Status—The job status, such as Completed, Running, or Canceled. • camera icon —Double-click the icon to play the copied video in a pop-up window. • Copy Start Time—The start time of the copy generation job. • Copy End Time—The end time of the copy generation job. • Recording Start Time—The start time stamp of the recorded video to be copied. • Recording End Time—The end time stamp of the recorded video to be copied. • Requested By—The Cisco VSM user who initiated the job. Job status can include the following: • Created—The job was created, but has not yet begun. • Running—The selected video is being copied to the server. • Completed—The video was successfully copied video from the camera to the server. • Canceled—The copy job was canceled by the user. • Failed—A portion of the video failed to copy. • Partial—at least one frame for the time range was copied, but not all of the expected video.
4	Sub-jobs for a selected job. A sub-job is displayed for each portion of the selected video. For example, if a copy job includes portions that were previously copied, or that need to be copied, a separate sub-job is displayed for each action. **Note** Copy jobs can still be successfully completed even if some sub-jobs display other status. For example, if a sub-job is ignored, it can mean that a portion of the video was skipped since it was already copied to the server, or that it is not available. The overall job can still complete even though some (or all) of the video was ignored. • Created—The sub-job was created, but has not yet begun. • Running—The selected video is being copied to the server. • Completed—The video was successfully copied video from the camera to the server. • Canceled—The copy job was canceled by the user. • Failed—A portion of the video failed to copy. • Ignored—A sub-job for the portion of the video that was skipped The job will still successfully complete even if portions of the video are “ignored”. • Partial—at least one frame for the time range was copied, but not all of the expected video.
5	(Optional) Select a Running job and click **Cancel** to cancel the job.

Usage Notes

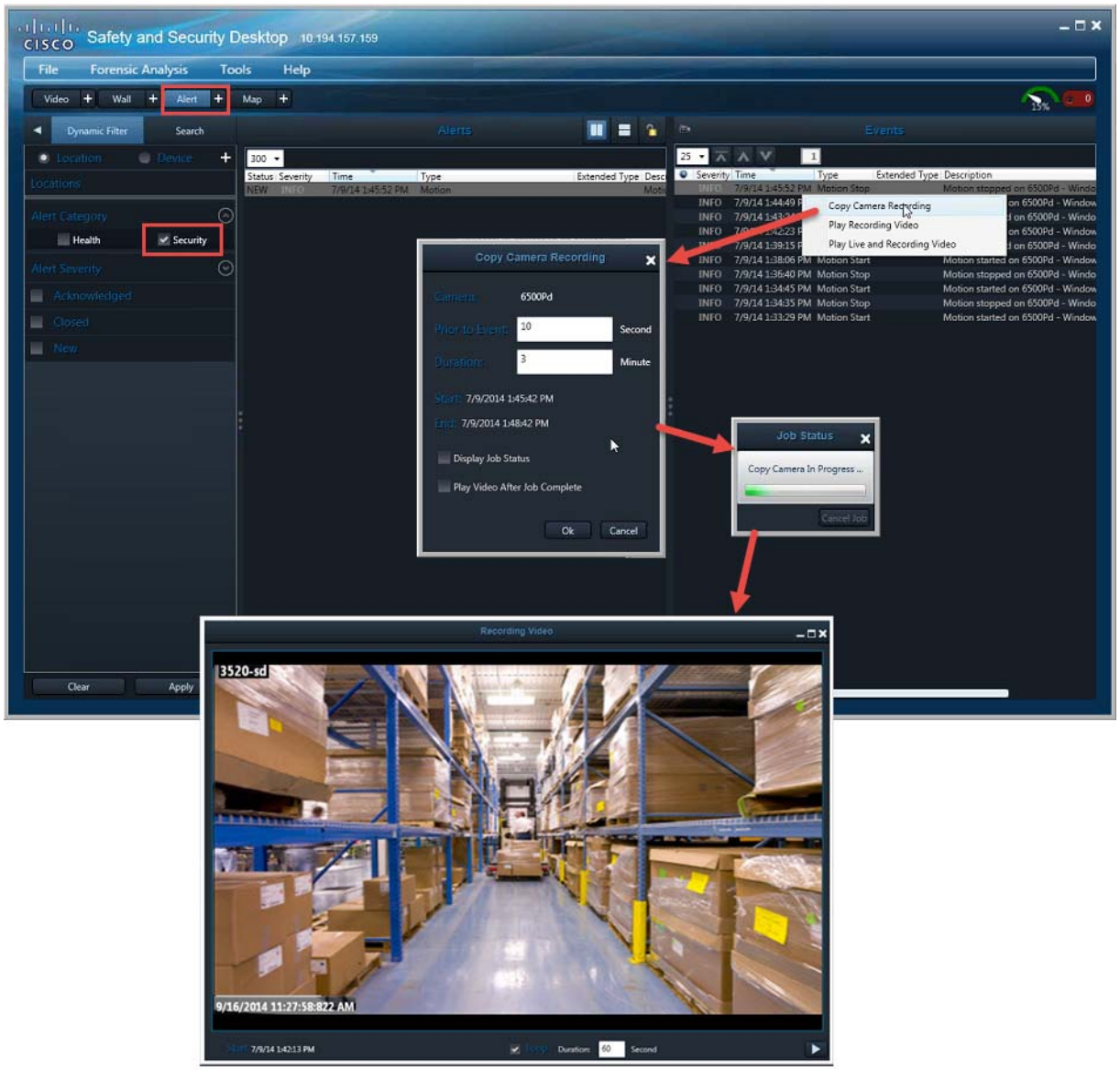
- Up to 10 jobs can run at a time. Additional jobs are queued and begin when another job is completed, fails, or is canceled.
- Only one copy request per camera can be processed at a time.

Copy Camera Recordings From Alerts

You can also copy camera recordings directly from an alert (Figure 5). This can be useful to copy and view only the video related to a specific security event, such as a motion stop or start event.

Note Video can be copied for any security alert or event where the camera is configured with local storage.

Figure 5 Copying Camera Recordings from an Alert



Procedure

Step 1 Select the **Alert** workspace.

Tip See Alert Workspace, page 41 for more information.

Step 2 Use the filters to narrow the results, and click **Apply**.

- For example, select the **Security** category to display only security alerts, such as motion stop and start events.
- See Alert Workspace Overview, page 43 and Understanding Events and Alerts, page 42 for more information.

Step 3 Select a security alert.

Recordings can only be copied from security alerts.

Step 4 Right-click a event for that alert, and select **Copy Camera Recording** (Figure 5).

Step 5 Enter the copy settings:

- Camera—(Read-only) The camera name.
- Prior to Event—(Optional) Enter the amount of video that should be copied before the event was triggered, in seconds. The default value is automatically entered.
- Duration—(Optional) Enter the total amount of video that should be copied, in minutes. The event duration is automatically entered. Revise this value to copy more or less video than occurred for the event.
- Start—(Read-only) The start time stamp of the video to be copied.
- End—(Read-only) The end time stamp of the video to be copied.
- Display Job Status—(Optional) Select to display the job status (Figure 5).
- Play Video After Job Complete—(Optional) Plays the video segment in a separate window after the copy job is complete (Figure 5).

Step 6 (Optional) Use the playback controls to view the event video that was copied form the camera (Figure 5).

- Select **Loop** to play the video segment in a continuous loop.
- Enter a duration to play a smaller portion of the video.
- Use the playback controls to pause or play the video.

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 to view the system health of the Operation Manager servers. See you system administrator for more information.

Contents

Refer to the following topics for more information:

- Federator Overview, page 142
- Federator Requirements, page 143
- Logging In to Cisco SASD Federator, page 144
- Monitoring Video Using Federator, page 145
- Monitoring Alerts Using the Cisco SASD Federator, page 147

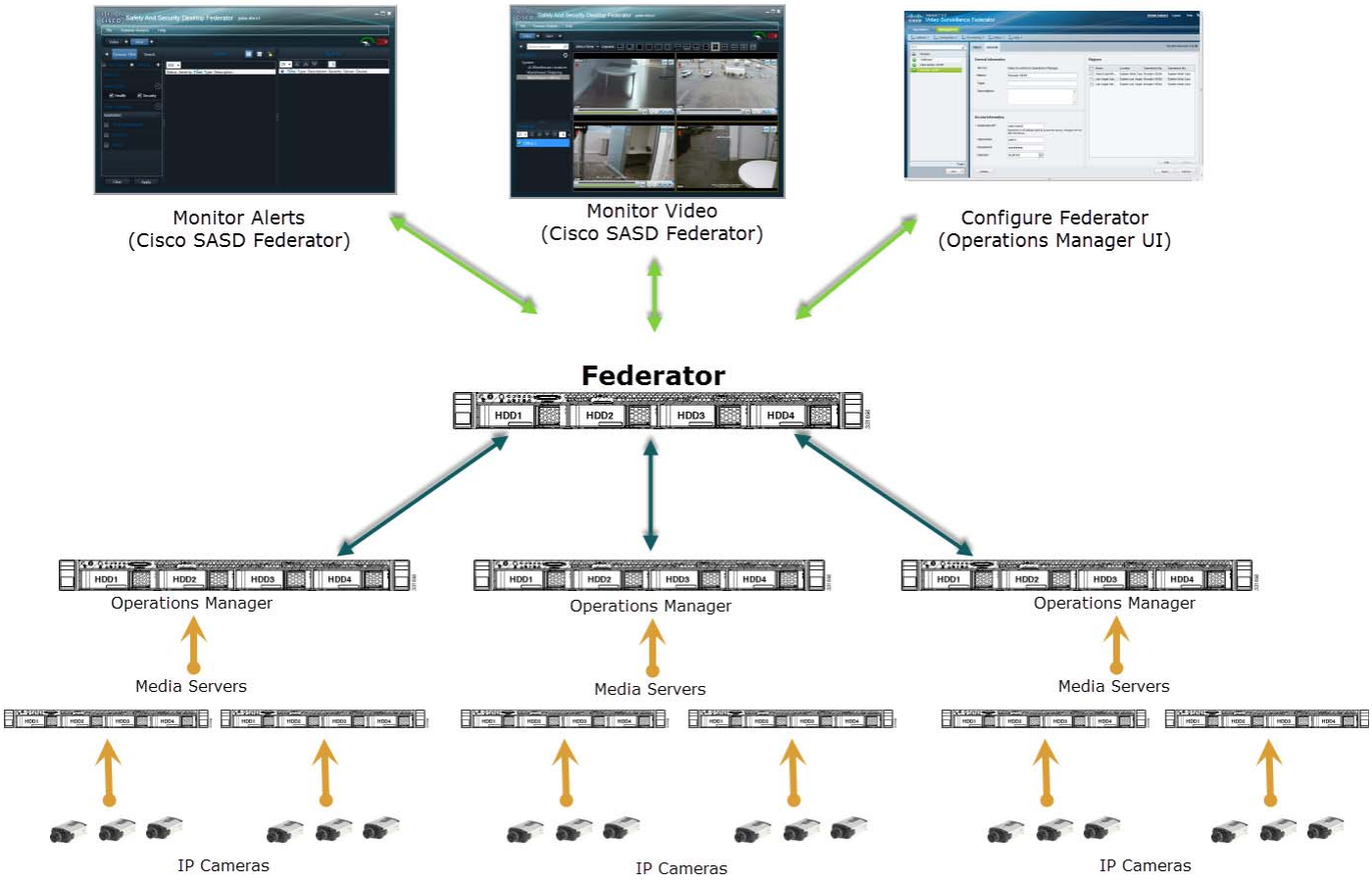
Federator Overview

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



Note: Cisco SASD Federator requires a different username/password than Cisco SASD. See your system administrator for more information.

Tip

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 12-1 Federator Requirements

Requirements	Complete? (✓)
At least one Federator server must be installed and configured on the network. **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.	❑

Table 12-1 Federator Requirements (continued)

Requirements	Complete? (✓)
A valid Federator server username and password. **Notes** • The default credentials for a new or factory restored server is **admin/admin**. • The username and initial password for all other users is defined when the user account is created (see the 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. See "Installing the Application Suite" in the Cisco Video Surveillance Safety and Security Desktop User Guide for more information. **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).	❑

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.

See "Logging In" (Cisco Video Surveillance Safety and Security Desktop User Guide) for more information.

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.

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.

- See "Requirements" in the Cisco Video Surveillance Safety and Security Desktop 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).

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"

See "Understanding Login Approval" in the Cisco Video Surveillance Safety and Security Desktop User Guide for more information.

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.

Procedure

Step 1 Log in to the Cisco SASD Federator application.

- See the "Logging In to Cisco SASD Federator" section on page 144 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).

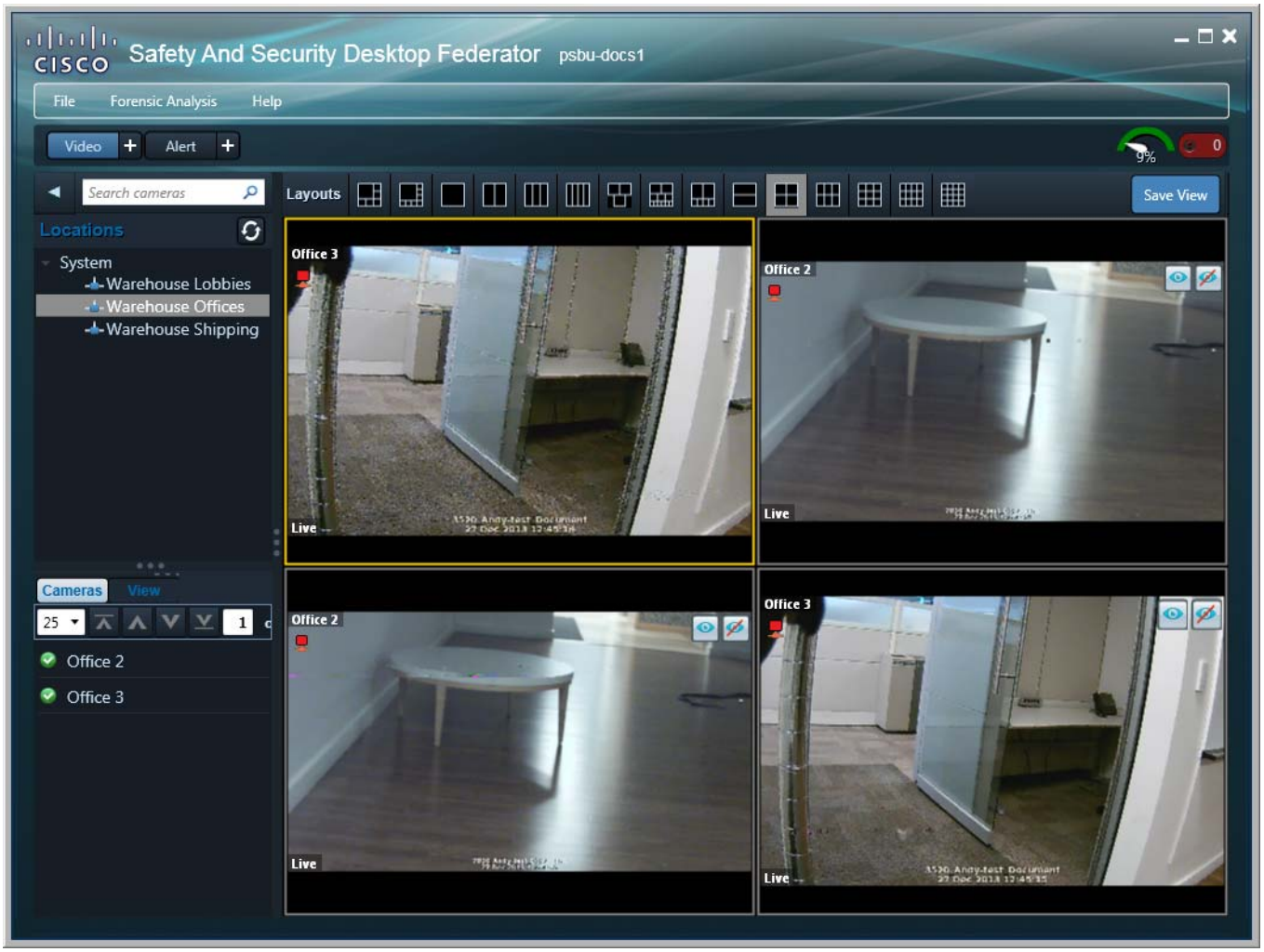
Step 3 (Optional) Use the search field to search for a camera name (such as **Lobby Camera**).

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.

See "Viewing Camera Video in a Multi-Pane Grid" in 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.

Monitoring Alerts Using the Cisco SASD Federator

- Overview, page 147
- Sending Operations Manager Alerts to Cisco SASD Federator, page 148
- Viewing Alerts, page 150

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).

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

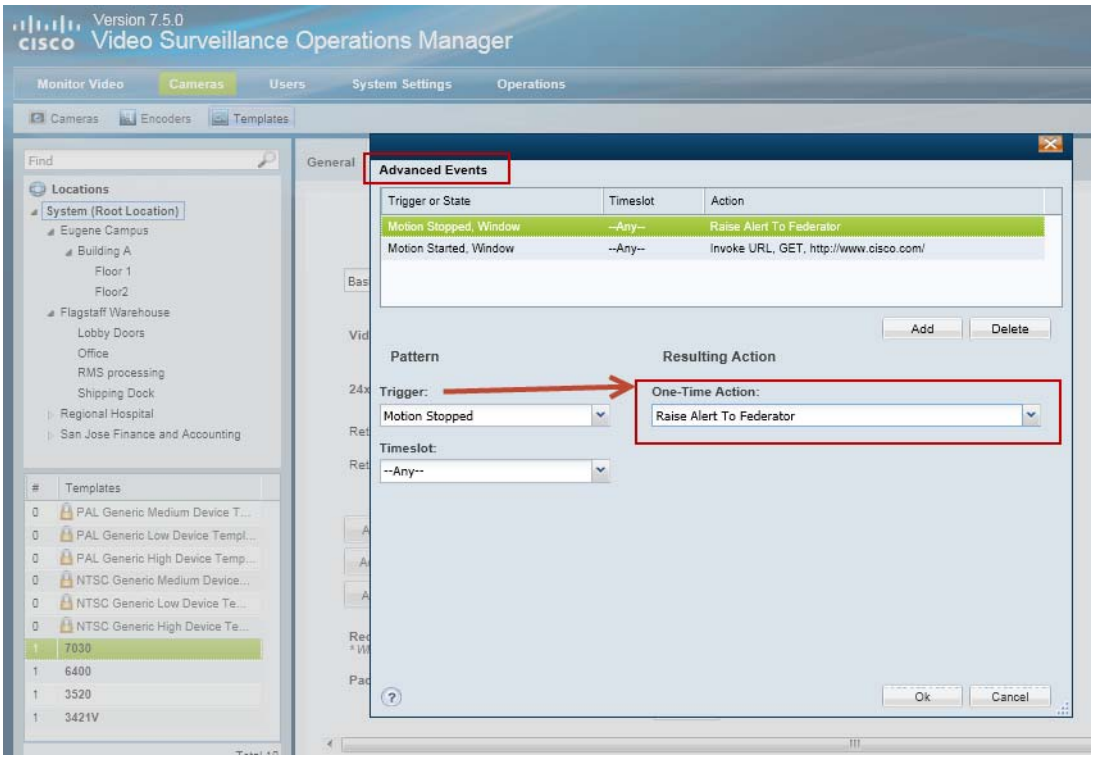
Method	Description
Device health alerts (automatic)	Cisco SASD Federator device health alerts. **Note** Only Operations Manager reachability alerts are displayed in the Cisco SASD Federator.
Security alerts (automatic)	Security alerts can be automatically sent to the Cisco SASD Federator when an event occurs. **Tip** 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. **Note** 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.
Manually send alerts to the Cisco SASD Federator	Right-click the alert in Cisco SASD and select **Send to Federator** (Figure 4).

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.

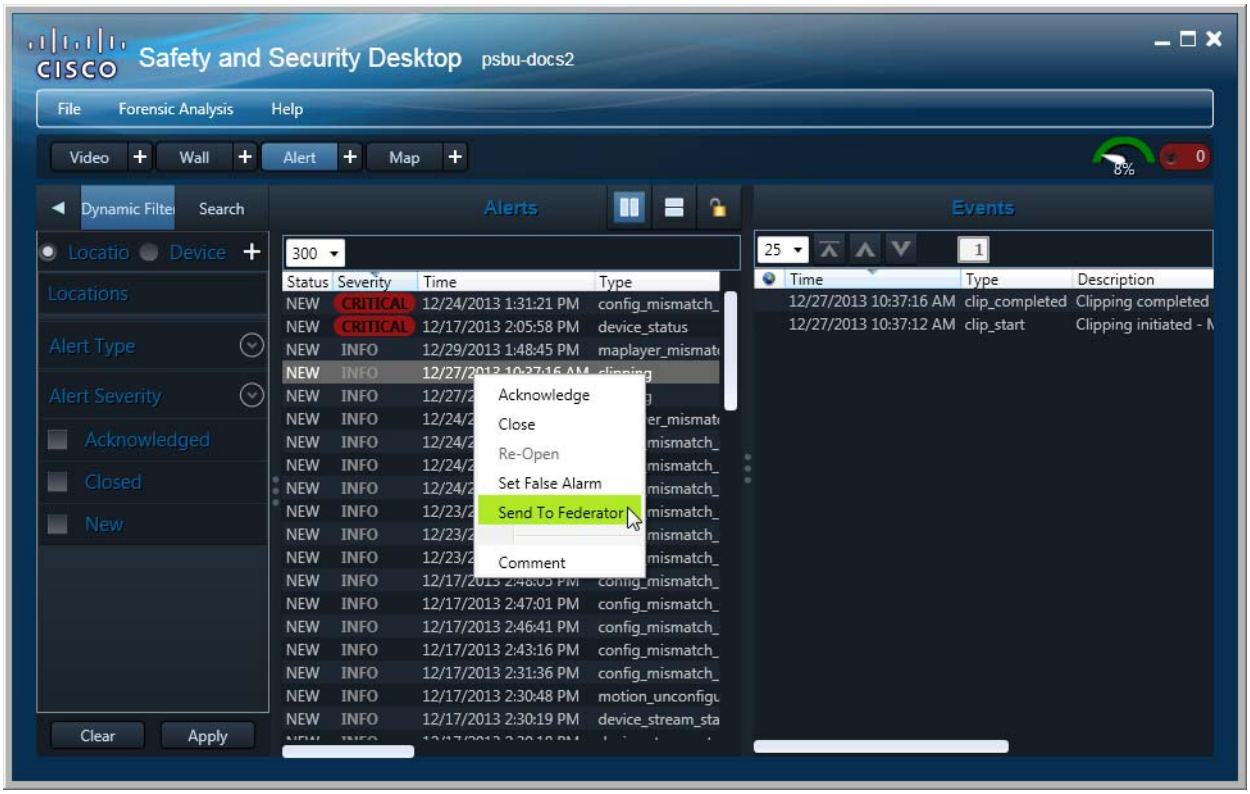
For example, in Figure 3 an Advanced Event is created that automatically sends an alert to the Federator when a motion event occurs.

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.

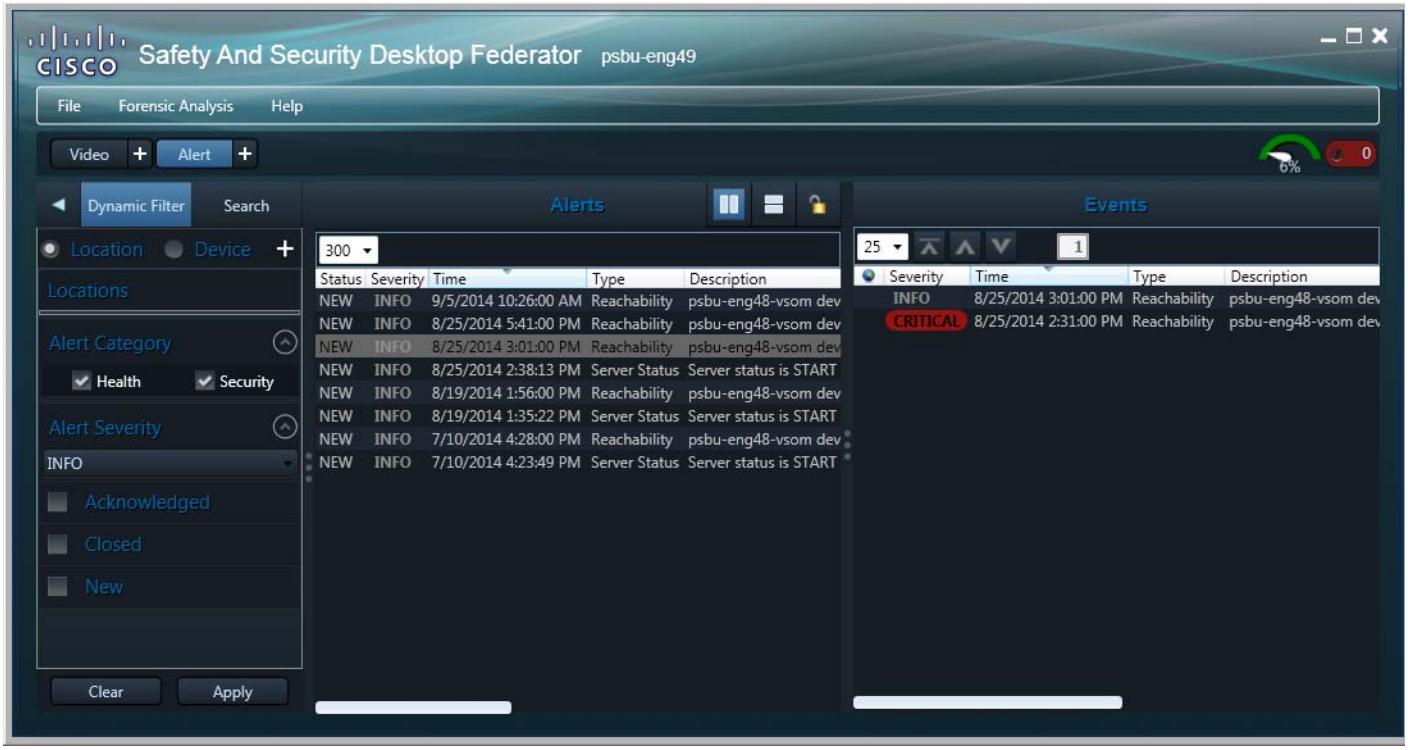
Note The Federator username and password are different than the Cisco SASD or Cisco SASD Advanced Video Player credentials. See you system administrator for more information.

Step 2 Select the Alert workspace (Figure 5).

Tip See "Alert Workspace" in the Cisco Video Surveillance Safety and Security Desktop User Guide for more information on managing and viewing alerts.

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 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.

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

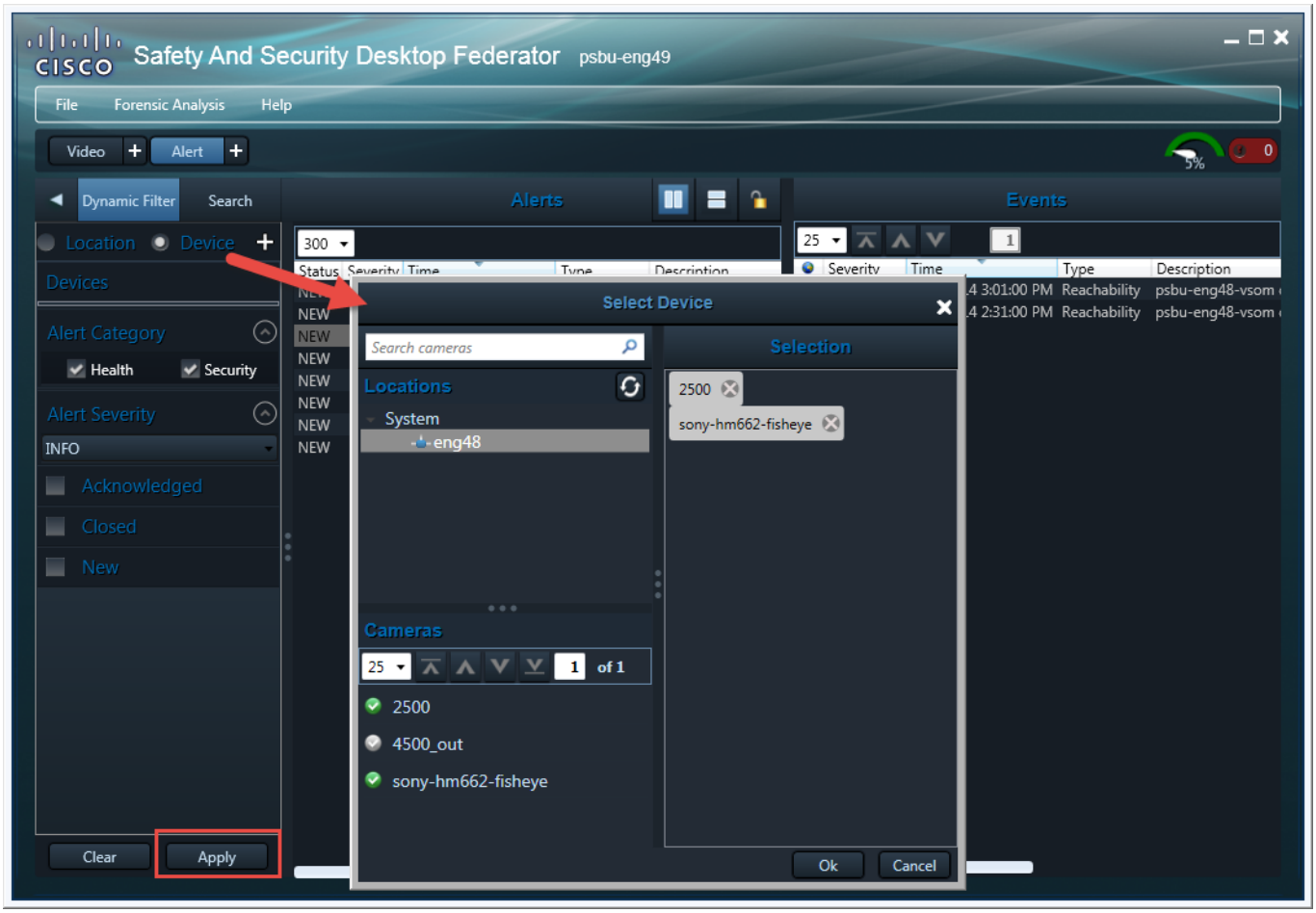
- **Location**—Click + to select a Federator location (Figure 6) where the alert(s) were created. Only alerts from that location will be displayed.

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 1 Revision History

Release	Document Revision Date	Change Summary
Release 7.6	December, 2014	Added the following sections and topics: • Camera Recording Management, page 129 Revised the following sections and topics: • Video Workspace, page 21 • Alert Workspace, page 41 • Map Workspace, page 59 • Controlling Video Playback, page 65 • Related Documentation, page 153
Release 7.5	February, 2014	Added the following sections and topics: • Getting Started, page 1 • Wall Workspace, page 29 • Using the Cisco SASD Wall Configurator, page 33 • Clip Management, page 109 • Motion Analysis, page 113 • Using the Cisco VSM Federator, page 141 Revised the following sections and topics: • Video Workspace, page 21 • Alert Workspace, page 41 • Map Workspace, page 59 • Controlling Video Playback, page 65 • Thumbnail Search, page 103 • Related Documentation, page 153
Release 7.2	August, 2013	• Added the "Viewing a Thumbnail Summary of Video Archives" section on page 1. • Various minor edits and revisions.

Table 1 Revision History (continued)

Release	Document Revision Date	Change Summary
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 7.0.0	January, 2013	Initial draft.