Cisco Video Surveillance Manager Safety and Security Desktop User Guide

Release 7.9
January 4, 2017

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.

© 2017 Cisco Systems, Inc. All rights reserved.

Getting Started

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

- Cisco SASD
- Cisco SASD Advanced Video Player
- Cisco SASD Wall Launcher
- Cisco SASD Wall Configurator
- Cisco SASD Federator

This section covers the following topics.

- Main Features of the Cisco SASD Application, page 3
- Video Settings, page 6
- Understanding the Video Viewing Options, page 8
- Video Viewing Applications, page 8
- Requirements, page 10
- Installing the Application Suite, page 11
- Logging In, page 15
- Understanding Maintenance Mode, page 21

Table 1 lists the Cisco Video Surveillance Safety and Security Desktop application suite components.

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 • Investigation Tools	**Overview** Getting Started **Workspaces** • Video Workspace • Wall Workspace • Alert Workspace • Map Workspace **Video Monitoring** • Viewing Video **Investigation Tools** • Event Recording Analysis • Thumbnail Search • Clip Management • Motion Video Analysis
Cisco SASD Advanced Video Player	An advanced monitoring application that includes the following monitoring workspaces: • Video workspace • Wall workspace	**Video Monitoring** • Viewing Video **Workspaces** • Video Workspace • Wall Workspace
Cisco SASD Wall Launcher	Launches a monitoring application for unattended workstations. "Unattended" mode allows video monitoring workstations to display Video Walls without access to the Cisco SASD configuration interface. The unattended workstations can remain open even if the keyboard and mouse are disconnected, and can (optionally) re-appear when the workstation reboots.	**Overview** • Using the Cisco SASD Wall Configurator **Video Monitoring** • Viewing Video
Cisco SASD Wall Configurator	A utility for adding and modifying Video Walls to display on monitoring workstations.	**Overview** Using the Cisco SASD Wall Configurator

Table 1 Cisco SASD Applications (continued)

Application	Description	More Information
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** • Viewing Video **Investigation Tools** • Thumbnail Search • Clip Management

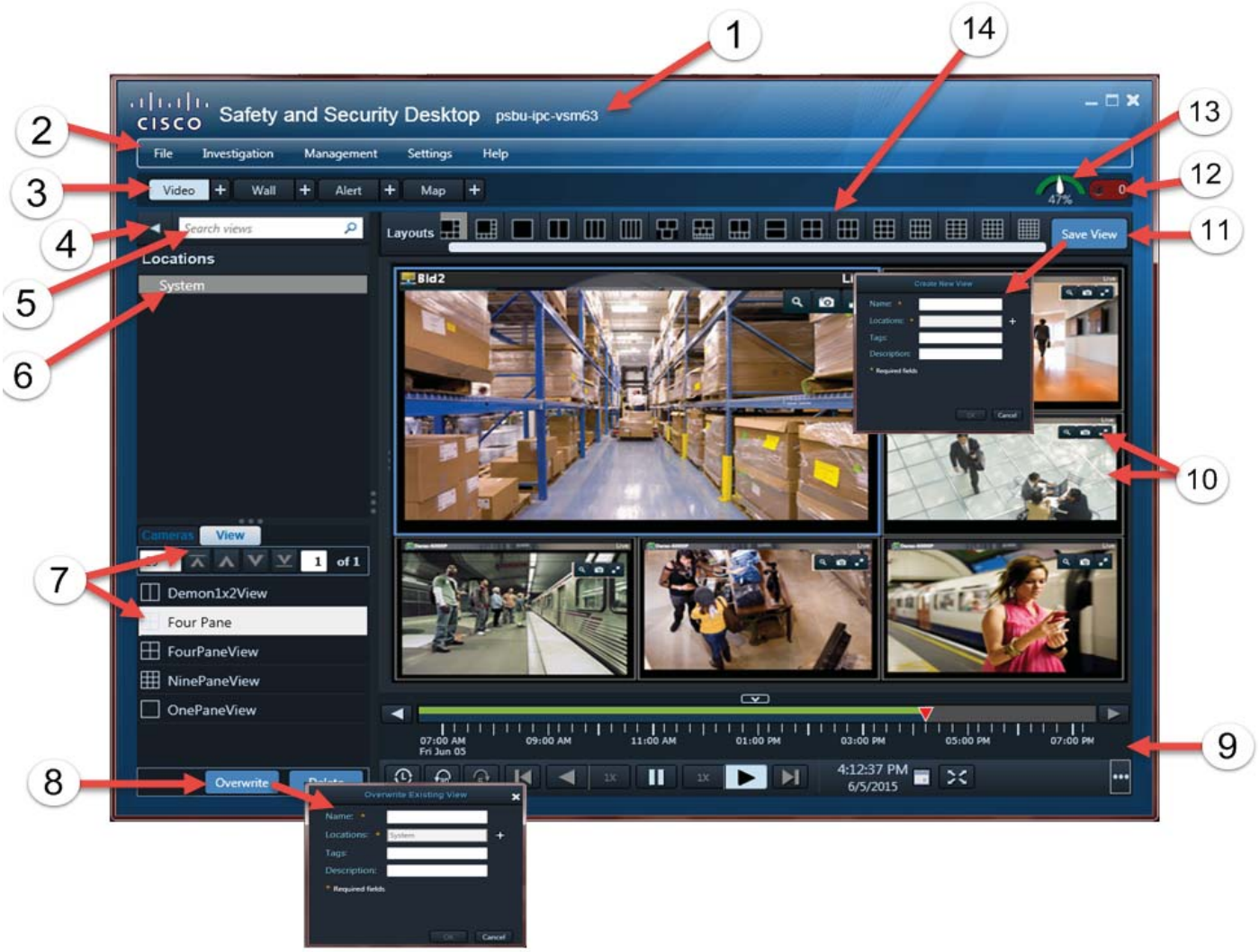
Main Features of the Cisco SASD Application

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

- 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 predefined set of viewing panes on multiple workstations.
- Use Unattended Mode to automatically open the Video Walls on monitoring workstations that do not have a mouse or keyboard.
- Use the Investigation tools to locate recorded video, search for motion events, and locate video clips.

Figure 1 highlights the features of the Cisco SASD user interface (UI).

Figure 1 Cisco SASD Features



1	The current Cisco Video Surveillance system (and optional Site).

2	Menu bar: • **File>Log Out** Logs you out of the application and disconnects from the Cisco Video Surveillance Operations Manager (VSOM). Monitoring workstations continue to display as configured. • **Investigation>** – **Event Recording Analysis**–View recorded video, mark video timeline by event type, seek to events, and search for all the events of a given type in a video recording. – **Thumbnail Search**–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. – **Motion Video Analysis**–View a summary of motion events for recorded video. • **Management>** – **Clip Management**–View, download, and delete MP4 video clips and virtual clips. – **Camera Storage>Camera Local Recording**–Copy recorded video from a storage device on the camera (such as an SD card) to the Cisco Media Server. – **Camera Storage>Camera Storage Job Management**–View camera storage copy job status. – **Event Suppression**–Suspend event notifications during maintenance periods. Events are still logged, but notifications are suspended. • **Settings>Video**–Customize video pane views to enable smooth video for jittery live cameras, set mouse double-click properties to expand or pop out video panes, and select general workspace properties. • **Help**—View online documentation.
3	Workspace tabs: • Video Workspace—In the Video workspace, you can: – Search for cameras by name. – Select sites in the **Locations** pane to display those cameras in the **Cameras** tab. – Drag and drop cameras from the **Camera** tab into the viewing pane. – Select a saved **View** for view multiple cameras in a grid. • **Duplicate** tab—Duplicate any workspace window and drag it to a separate monitor (see Displaying a Duplicate Workspace on a Separate Monitor, page 29). • Wall Workspace—Video Walls are predefined *Views* to display on multiple workstations. – All workstations displaying that Video Wall display the same view. – You can publish modified walls to other workstations viewing the wall such as unattended workstations, which are monitored without operator input or control. • Alert Workspace—View and modify alerts. • Map Workspace—Display maps of the Cisco VSM locations, including cameras and their alerts at those locations. – Single-click a camera icon to display a dragable icon. – Double-click the icon to view video in a pop-up window. – Right-click the icon to see only Alerts related to this camera.
4	Click the triangle to display or hide the Locations pane.
5	Search—Enter the full or partial name of a camera to display matching camera names.

6	Side Pane—Side panes include the controls and search options for that workspace. For example, in the **Video** workspace, the **Locations** pane displays connected Cisco Video Surveillance installations.
7	**Camera** and **View** tabs. • **Camera**—View available cameras based on selected location or search. – Drag and drop cameras into the viewing pane or double-click a camera to display it in the active viewing pane. • **View**—Access predefined camera grids. – Double-click or drag and drop views into the viewing pane. – Save views displaying in the Video workspace **Note:** You can automatically rotate cameras using the Operations Manager interface.
8	**Overwrite** and **Delete** Buttons—(Video workspace only) Allows you to overwrite views (for example, the camera or stream displaying in a pane). See Saving a Video "View" (Multi-Pane Grid), page 27.
9	Playback Controls—See Viewing Video, page 77.
10	Viewing Pane and Controls—See Viewing Video, page 77.
11	**Save View** (Video workspace only)— Save layouts to the **View** tab. • Use the **Overwrite** button to modify existing views. • Assign views to the same location as the cameras or to higher-level locations. **Note:** Only users assigned to the user group at the location can access views.
12	Notifications—Notify errors, such as exceptions from Operations Manager back-end calls or software exceptions.
13	Performance Meter—Displays CPU performance of the workstation based on available memory and bandwidth. • Green = Meeting the demands of Cisco SASD activities. • Yellow = Performance warning. • Red = Workstation performance is poor and processing delays may occur. **Tip:** Hover your mouse over the meter to view real-time network and memory usage.
14	**Layouts** (Video workspace only)—Click a predefined grid layout and drag cameras into the viewing panes.

Video Settings

From the SASD menu bar, select **Settings>Video** to Customize video pane views and application settings.

Note: For more information about the Smooth Video Settings, see Using the Smooth Video Settings When Viewing Live Video, page 100.

Table 2 Video Settings

Setting	Description
Smooth Video Settings	
Smooth Video Option	Selects whether to automatically switch to a different stream or use I-frames only if the live video quality is poor.
Enable Buffering for Live/Non-PTZ Camera	Creates a video data buffer (in seconds) that delays live playback while video data caches.

Table 2 Video Settings

Setting	Description
Pre-Roll Buffer Size in Seconds	Defines the number of seconds for live video to delay until recording begins.
Mouse Settings	
Double-click video pane to:	Select what the double-click mouse action does in a video pane: • Expand pane—Expands the pane to the size of the video display area. • Popup window—Opens the video pane in a new window.
Global Settings	
Zoom to Fit Pane	Removes the black bars from around the video image so that it occupies the entire area of the pane. Some clipping of the image will occur. Use the mouse wheel to scroll the clipped image if an area of interest is obscured.
Select Pane to PTZ	For PTZ cameras, this option enables PTZ functions when you select the video pane (this is a shortcut to clicking the PTZ icon in the top right of the pane). **Note**: This feature is ignored if the camera also supports the **PTZ to region** functionality.

Understanding the Video Viewing Options

Table 3 describes the Cisco SASD application suite video viewing methods.

Table 3 Video Viewing Options

Viewing Mode	Description	More Information
Single Camera	View video from a single camera based on location, alert, or map.	• Video Workspace • Alert Workspace • Map Workspace
Multiple Cameras	View a multi-pane grid layout of live or recorded video.	• Video Workspace • Wall Workspace
Video Walls	View the same video grid layout on multiple workstations.	• Wall Workspace • Using the Cisco SASD Wall Configurator
Unattended Mode	Display a video wall on monitoring workstations. Video walls can automatically display on workstation reboots.	• Using the Cisco SASD Wall Configurator
Alerts and Events	Display recorded video for an event. You can simultaneously view live video from the same camera.	• Playing Event Video
Investigation Tools	The following Investigation tools are available: • **Event Recording Analysis**–View recorded video, mark video timeline by event type, seek to events, and search for all the events of a given type in a video recording • **Thumbnail Search**–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. • **Motion Video Analysis**–View a summary of motion events for recorded video.	• Thumbnail Search • Motion Video Analysis
Management Tools	• Use *Clip Management* to view, download and delete MP4 and virtual clips that are stored on the server.	• Clip Management

Tip: See Viewing Video, page 77 for instructions to control playback of live or recorded video.

Video Viewing Applications

Table 4 lists the Cisco-provided applications you can use to view and manage live and recorded Cisco Video Surveillance video.

Tip: Third-party integrators create custom monitoring applications. Contact your Cisco support representative for information.

Table 4 Summary of Cisco Video Viewing Options

Viewing Tool	Application	Description	Documentation
Desktop monitoring application	Cisco Video Surveillance Safety and Security Desktop (Cisco SASD)	• Simultaneous viewing of up to 25 cameras per workspace, and up to 48 cameras per workstation. • Create Video walls to display on monitoring workstations. • View Video walls. • Create monitoring workstations. • View and manage alerts. • View cameras, video, and alerts based on a graphical map.	• Cisco Video Surveillance Safety and Security Desktop User Guide • Table 1
Web-based configuration and monitoring tool	Cisco Video Surveillance Operations Manager (VSOM or Operations Manager)	• Simultaneous viewing of multiple video panes: – View up to 4 cameras with 32-bit Internet Explorer. – View up to 25 cameras with 64-bit Internet Explorer. • Add users, Views, and Video walls for the Cisco SASD application. • Configure cameras, streams, and recording schedules.	Cisco Video Surveillance Operations Manager User Guide
Desktop video clip player	Cisco Video Surveillance Review Player (Cisco Review Player)	Simple player for viewing video clip files.	Cisco Video Surveillance Review Player
Web-based server console	Cisco Video Surveillance Management Console (Cisco VSM Management Console)	Basic viewing features for a single stream (Stream 1) from a single camera.	Cisco Video Surveillance Management Console Administration Guide

Requirements

Use the Table 5 checklist to ensure you meet Cisco SASD requirements.

Table 5 Cisco SASD Requirements

Requirements	Requirement Complete? (✓)
(Minimum) One Cisco VSM server installed on your 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.	❑
(Minimum) One camera physically installed and configured using Operations Manager.	❑
The IP address or hostname for the Cisco Video Surveillance installation (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 5 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 one of the following *64-bit* operating systems: – Windows 7 SP1 – Windows 8.1 – Windows 10 • The Microsoft .NET Framework 4.5 (full setup) installed on the client PC. If your workstation does not have Internet access, download the .Net 4.5 installer. • (Windows N and KN versions only) Install the Windows Media Feature Pack to enable video and audio playback. • Standard Windows user account (you need Admin privileges to install SASD). **Note:** The following message is displayed and video streaming is disabled if you log in as Guest: "Cannot create RTSP connection to server. Check network connection and server health status." To avoid this, sign in with a user name.	❑
Cisco Multi-Pane Video Surveillance client software. This Active X client enables video playback and other UI features. **Note:** Install this utility as prompted during Cisco SASD installation or update. Administrative privileges are required on the PC workstation to install the software.	❑

Installing the Application Suite

You can download all Cisco SASD applications from the cisco.com website.

The following installations procedures are covered in this section:

- Installing the Cisco SASD Application Suite, page 11
- Installing the Cisco SASD Advanced Video Player, page 12
- Upgrading Cisco SASD Applications, page 13

Note: You can also download the Cisco SASD Advanced Video Player installer from the browser-based Operations Manager (**Operations** tab).

Installing the Cisco SASD Application Suite

You download all Cisco SASD applications from the cisco.com website. This includes all components described in Table 1.

Note: Close all SASD applications, including Cisco SASD Wall Configurator, before upgrading the SASD Application Suite. The upgrade will fail if Cisco SASD Wall Configurator is running.

To install the Cisco SASD application suite:

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 Active X client enables video playback and other UI features.

Note: Video does not play if the Cisco Multi-Pane client software is incorrectly installed. You must have administrative privileges on the PC workstation to install the software.

Installing the Cisco SASD Advanced Video Player

You can also download the Cisco SASD Advanced Video Player installer from the browser-based Operations Manager (**Operations** tab).

Note: Microsoft .NET Framework 4.5 must be installed on the PC running Cisco SASD.

To install the Cisco SASD Advanced Video Player:

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

a. Launch Internet Explorer on your Windows computer.

b. Enter the Server Name for the Cisco VSM Operations Manager.

c. From the Domain menu, choose the default “localhost” (for accounts created using the Operations Manager).

Note: 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.

d. Enter your username and password.

Note: Enter a new password if prompted. 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** (in the *Software* pane).

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.

Tips:

- 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.
- Users must have a valid Cisco VSM username and password to access the system.
- Go to http://www.microsoft.com/en-us/download/confirmation.aspx?id=17851 to download the installer.

Upgrading Cisco SASD Applications

If the Cisco VSM system is upgraded, you will be prompted to upgrade Cisco SASD when logging in.

Select **Install**, when prompted (Figure 3) and follow the onscreen instructions.

Figure 3 Upgrading the Cisco SASD Application

Logging In

Log in to the Cisco SASD application using the username and password supplied by your administrator. You will be prompted to change your password the first time you log in (or when your password expires).

Note You must log in to the workstation using a standard Windows user account. If you log in as Guest, video streaming is disabled and the following error is displayed: "Cannot create RTSP connection to server. Check network connection and server health status."

Procedure

Step 1 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 Table 1.

Step 2 Enter the login information (Figure 4):

- **Server**—The IP address or hostname of the Operations Manager (provided by your administrator).
- **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 your password.

Figure 4 Cisco SASD Login Screen

Note You will be prompted to enter and reenter a new password on first login or when your password expires. Follow the onscreen prompts. See Changing Your Password to change your password using the Operations Manager

Step 3 For users with Site access, select a site from the Select login site dialog box (Figure 5).

Figure 5 Select Login Site Screen

Note: To change sites, you must log out and log back in. See Understanding Sites, page 17 for more information.

Step 4 If prompted, ask your manager or other administrator to enter their Approver Login information (Figure 6).

Figure 6 Approver Login Screen

Notes

- This second login is required only if configured.
- See the Understanding Login Approval, page 18 for more information.
- If approval is not successfully submitted within the time-out period, the login is denied.

Understanding Sites

Sites are designated location hierarchies (locations and sub-locations), where there is good network connectivity between the cameras and servers. 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). When accessing any camera inside the Site, users outside the Site receive video from a Dynamic Proxy server. 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 assigned to a Site location, you are prompted to select a Site when you log in (Figure 7).

Figure 7 Select Login Site Screen

Notes

- 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, who are not assigned a Site, or who select the Not in Any Site check box, receive video from a Dynamic Proxy server for cameras in any Site where Dynamic Proxy is enabled.
- To change sites, you must log out and log back in.

Understanding Login Approval

Dual Login requires that a second user (such as a manager) approve user access by entering their credentials. When the user logs in, a second screen appears requesting approver login (Figure 8). If this optional feature is enabled, the Approver Login Required screen appears every time the user logs in.

Figure 8 Approval Login Required Screen

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

Default User Accounts and Passwords

Table 5 lists the Cisco SASD default user accounts for the super-admin and operator.

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**	View live and recorded video, control PTZ camera movements, push views to a Video wall, and export recordings.

Changing Your Password

You will be prompted to enter and re-enter a new password on first login or when your password expires. Follow the onscreen prompts.

To change your password at other times, you must log in to the browser-based Cisco Video Surveillance Operations Manager.

Procedure To Change Your Password Using Operations Manager

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

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

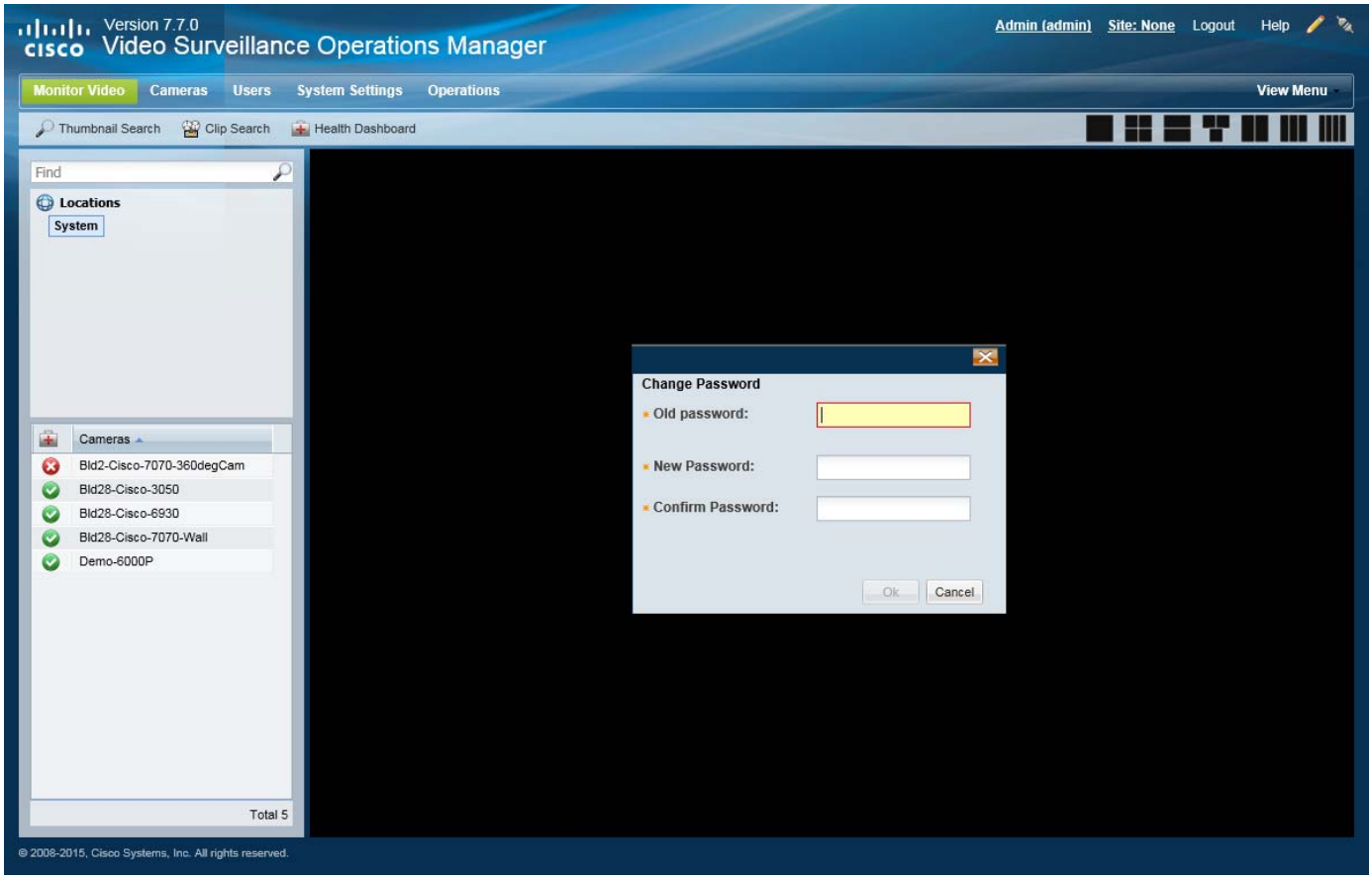
Step 3 Enter the same username and password used to access Cisco SASD.

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.

Step 6 Logout of the Operations Manager and log in to Cisco SASD using your new password.

Figure 9 Changing Your Password Using Operations Manager



Understanding Device States and Warning Icons

Table 6 describes the overall device state icons.

Table 6 Device Status

Status	Color	Color	Description
Enabled: OK		Green	The device is operating normally.
Enabled: Warning		Yellow	A minor event occurred that did not significantly impact device operations.
Disabled		Yellow	The device is disabled and unavailable for use. The configuration can be modified and existing recordings viewed, but the camera cannot stream or record new video.
Enabled: Critical		Red	An event occurred that impacts the device operation or renders a component unusable.
Pre-Provisioned		Brown	The camera is waiting to be added to the network and is not available for use. A pre-provisioned camera can be modified, but the camera cannot stream or record video until you choose **Enable** from the **Device Settings** menu.
Soft Deleted (Keep Recordings)		Grey	The device configuration is removed from the Operations Manager but the recordings associated with that device are still available for viewing (until removed due to grooming policies). To view the recordings, select the camera name in the **Monitor Video** page. Soft-deleted cameras are still included in the camera license count.
Hard Deleted (Delete Recordings)	None	None	The device and all associated recordings are permanently deleted from Cisco VSM. **Note:** In the Operations Manager, you can place the camera in the Blacklist.

Table 7 describes warnings and fault.

Table 7 Warning and Critical Faults

Icon	Error Type	Description
	Warning	Warnings are based on activity that occurs without incapacitating a component, for example, interruptions in operation due to packet losses in the network. These activities do not change the overall state of the component, and are not associated with “up” and “down” health events.
	Critical	Critical errors are health events that impact the device operation or render a component unusable. For example, a server or camera that cannot be contacted on the network, or a configuration error. Components in the critical state remain out of operation (“down”) until another event restores them to normal operation (“up”). Critical errors also affect other components that depend upon the component that is in the error state. For example, a camera in the critical error state cannot provide live video feeds or record video archives.

Understanding Maintenance Mode

Read-only maintenance mode allows operators to access live and recorded video, but locks configuration settings from modification. For example, operators cannot save or modify views, or acknowledge alerts.

You enter maintenance mode in the Operations Manager.

Figure 10 shows the white and red maintenance mode banner displaying at the top of the page in Operations Manager and Cisco SASD. In the Operations Manager, the pencil icon is gray (red circle) during maintenance mode. See the Cisco Video Surveillance Operations Manager User Guide.

Figure 10 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.

- Saving a Video "View" (Multi-Pane Grid), page 27
- Displaying a Duplicate Workspace on a Separate Monitor, page 29

Select the **Video** workspace (Figure 11) to view video from the cameras in your Cisco Video Surveillance deployment.

For example:

- Drag a camera name onto a viewing pane to view video from that camera. See Viewing Video, page 77 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 cameras onto 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 view, 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 popup window.

To create and save a view:

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 camera names onto the available viewing panes (you can also highlight a pane and double-click the camera name).

Step 4 (Optional) Click a pane and select **Stream 2** 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 Viewing Video, page 77.

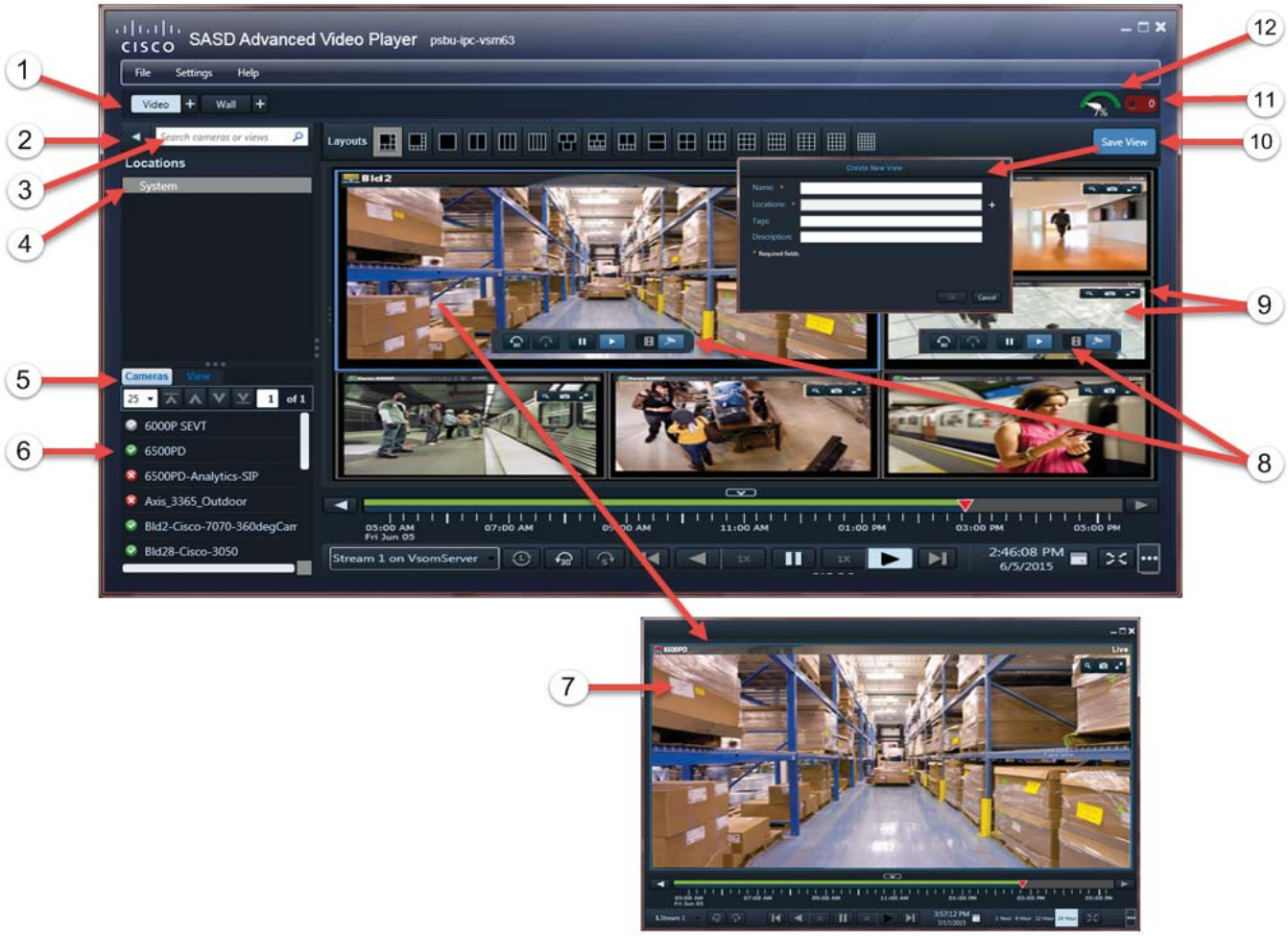
Step 7 (Optional) Double-click a video pane to enlarge the video, or open it in a popup window.

- Go to **Tools > Options** to select if the video should fill the window, or open in a popup window when double-clicked.
- Double-click the video pane again to return it to normal size.
- To fill the monitor screen, 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, page 29.

Figure 11 shows the main features of the Video Workspace.

Figure 11 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 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, page 29.
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).

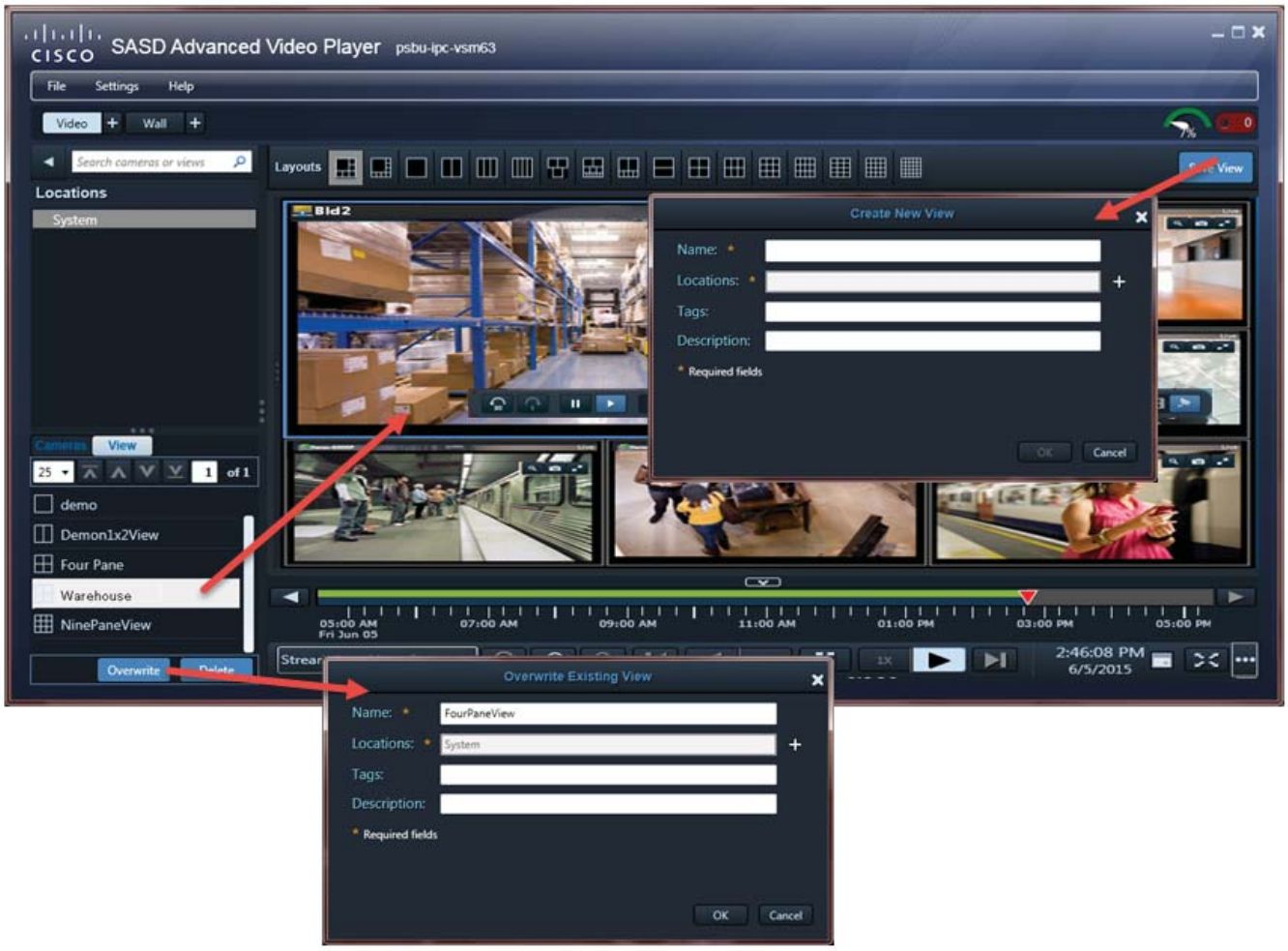
5	**Camera** and **View** tabs. • **Camera**—Select the **Camera** tab to view the available cameras based on the location or search. Double-click or drag the camera onto the video area. • **View**—Select the **View** tab to view the pre-defined camera matrix. – Double-click or drag the View to the video 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 27.
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 popup window. **Tip:** Go to **Settings>Video** to select if the double-clicking the video pane will fill the window or open in a popup window when double-clicked.
8	Playback Controls—See Viewing Video, page 77.
9	Viewing Pane and control icons—See Viewing Video, page 77.
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), page 27.
11	Notifications—Notify errors, such as exceptions from Operations Manager back-end calls or software exceptions.
12	Performance Meter—Displays the CPU performance for the workstation 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 for 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 12 Video Layouts and Views



To save a video view:

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 12).

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

Step 4 (Optional) Click a video pane and select Stream 2 to display the secondary stream, if necessary.

The selected stream appears when the View displays.

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 12).

Notes

- If an unattended video wall is closed or stops streaming, it can only be brought back up if the PC is rebooted. Unattended video walls will not start up again if you only log off and log back on (you must restart the PC).
- If a "Maintenance Mode" banner appears at the top of the window, the system was placed in Maintenance Mode by an Operations Manager administrator, and configuration changes are not allowed. See your Cisco VSM administrator for assistance.

Related Information

- See Displaying a Duplicate Workspace on a Separate Monitor, page 29 to create a separate window of video panes.
- See Wall Workspace, page 31 to use pre-defined video grids on multiple workstations.
- See Using the Cisco SASD Wall Configurator, page 35 for instructions to create an "unattended workstation" to monitor video without a mouse, keyboard, or other user input.

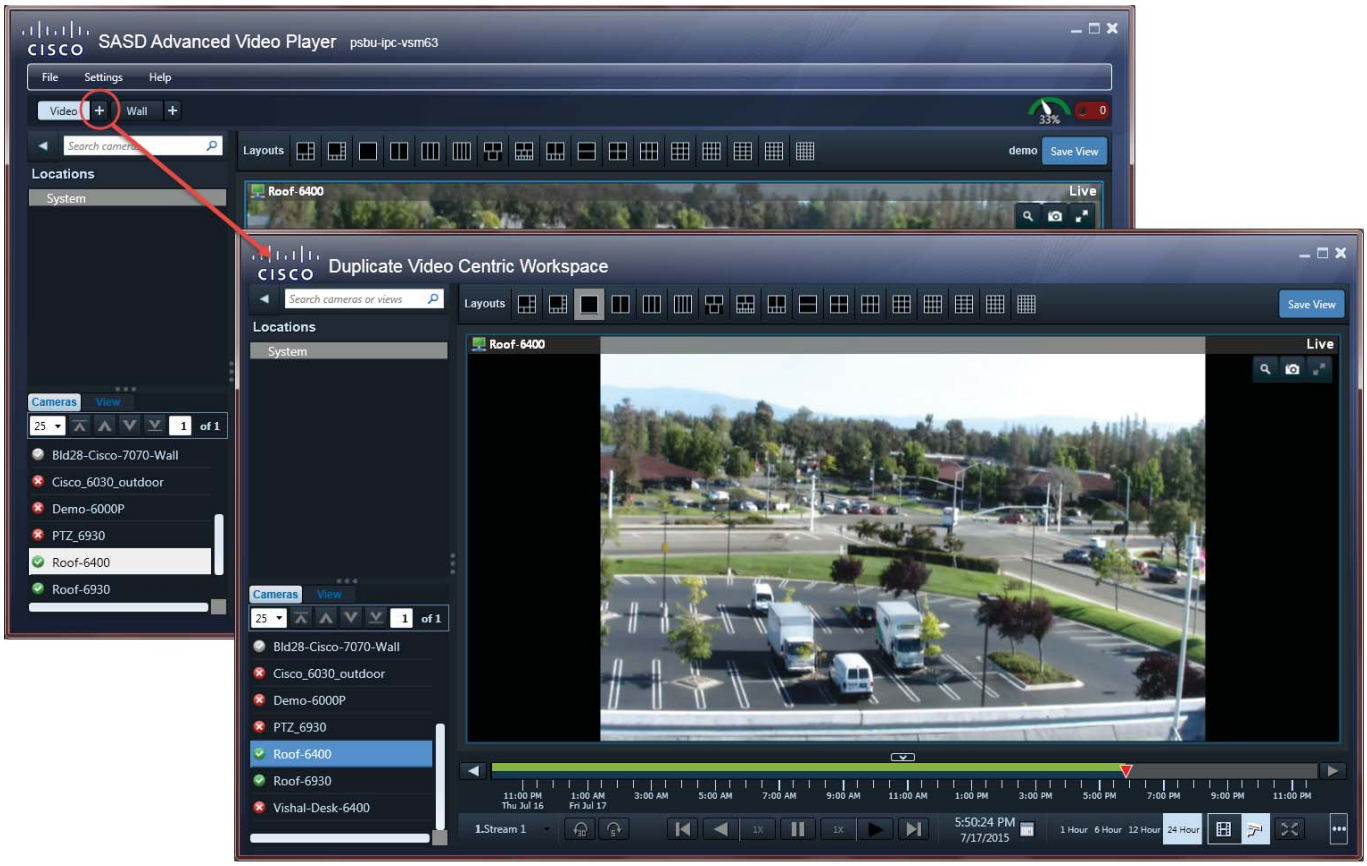
Displaying a Duplicate Workspace on a Separate Monitor

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

Figure 13 Creating a Duplicate Workspace



Tips

- 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 window. To fill the entire monitor screen, select **Full screen mode** .
- See Viewing Video, page 77 for more information.

Wall Workspace

Video Walls are predefined *Views* to display on multiple workstations, including *unattended* workstations (Figure 14). All workstations then display the same set of predefined panes.

This section contains the following topics:

- Usage Notes, page 33
- Viewing and Publishing Video Walls, page 33

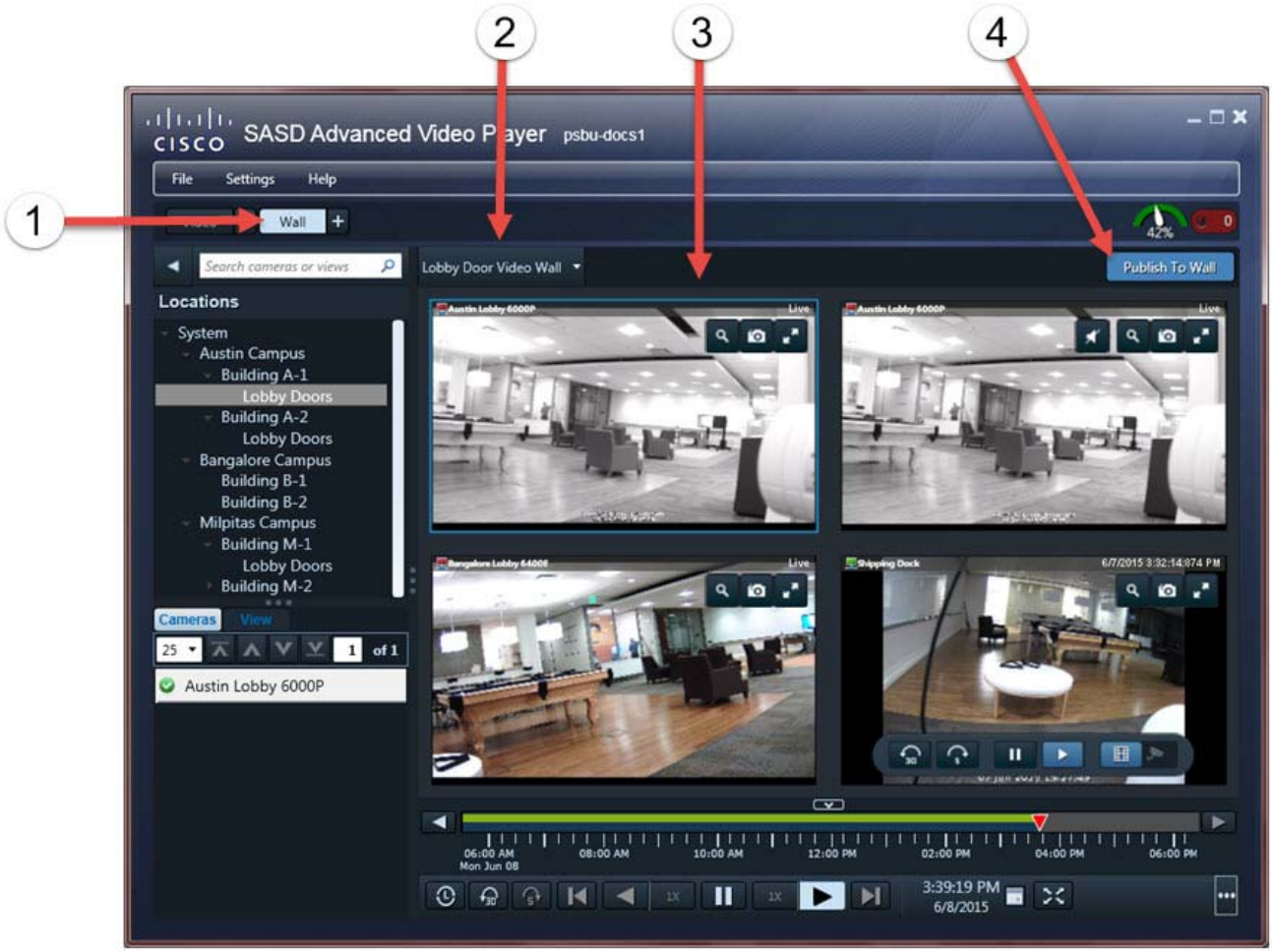
You can modify Walls and publish those views to all workstations viewing the Wall, including unattended workstations that have no user input or controls.

For example, you can configure a *Lobby Door* Wall view to include cameras in buildings 1 through 4. Each workstation that selects the Lobby Door Wall view displays 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 view on all other workstations displaying that Wall.

Tip: Use the Cisco SASD Wall Launcher to display Walls on unattended monitoring workstations. See Using the Cisco SASD Wall Configurator, page 35.

Figure 14 highlights the main features of the Wall workspace.

Figure 14 Video Wall



1	Wall workspace. Click + to create a duplicate workspace window that you can drag onto a separate monitor to simultaneously view multiple walls. See Displaying a Duplicate Workspace on a Separate Monitor, page 29.
2	Wall drop-down menu.
3	Video pane grid layout for the selected Wall. **Tip:** Drag cameras onto the video panes to change the video display. Click **Publish To Wall** to display a modified wall on all workstations viewing that Wall. The Wall reverts to the predefined view after the rollback time defined in the Operations Manager (see Configuring Video Walls in the Cisco Video Surveillance Operations Manager User Guide).
4	**Publish To Wall**—Display a View or modified Wall on all other workstations and monitors viewing that Wall. This feature requires access permissions. See Using the Cisco SASD Wall Configurator, page 35.

Requirements

Table 8 lists Video Wall requirements.

Table 8 Cisco SASD Requirements

Requirements	Requirement Complete? (✓)
Set access permissions—These access permissions must be granted in the Operations Manager: • **Video Walls**—Create, update, or delete Walls using the Operations Manager and Cisco SASD Wall Configurator. • **Push Video to Wall**—Enables the **Publish to Wall** feature in Cisco SASD to allow users to change the view shown on all other instances of the selected Wall. The new view displays until the Rollback Time set in the Operations Manager is exceeded. **Note:** Camera views set to **Stream 2 on VSOM Server** automatically revert to **Stream 1 on VSOM Server**.	❑
(Minimum) Configure one Video wall on the system (using the Operations Manager)	❑

Usage Notes

- Video Walls are configured by system administrators using the browser-based Operations Manager administration tool. See the Cisco Video Surveillance Operations Manager User Guide.
- Video Walls can display a populated *View* or blank grid layouts.
- See Using the Cisco SASD Wall Configurator, page 35 for instructions on setting up an unattended workstation. Unattended workstations usually have no mouse, keyboard, or other operator input.

Viewing and Publishing Video Walls

To view, modify, or publish a Video wall:

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

Step 2 (Optional) Click ⊞ to create a duplicate workspace window to drag onto a separate monitor. See Displaying a Duplicate Workspace on a Separate Monitor, page 29.

Step 3 Click **Select Wall** and choose a wall from the drop-down menu (Figure 14).

Step 4 (Optional) Change the video display:

- Drag cameras from the Camera tab onto available panes in a grid layout.
- Select a different View.

  Note: When the pane updates, all panes in that Video wall refresh, which causes a momentary loss of video.

Step 5 (Optional) Click **Publish to Wall** to display the modified View on all instances of that Video wall (such as other workstations displaying that Video wall).

Tips:

- The Wall reverts to the default view after the Rollback Time defined in the Operations Manager.
- The **Publish to Wall** option is enabled when the video panes in a View are modified.
- Access permissions are required for **Publish to Wall**. See your system administrator for more information.

Using the Cisco SASD Wall Configurator

The Cisco SASD Wall Configurator defines the Video Walls to display on unattended workstations.

This section covers the following topics:

- Requirements, page 37
- Usage Notes, page 38
- Configuring Unattended Workstations, page 39
- Launching Unattended Windows, page 40
- Removing a Video Wall From Unattended Mode, page 41
- Understanding Offline Mode, page 41

An unattended workstation is a PC that monitors Video Walls without user input or interaction. Unattended workstations usually have no mouse, keyboard or other user input, and cannot access the Cisco SASD or Cisco SASD Advanced Video Player interface.

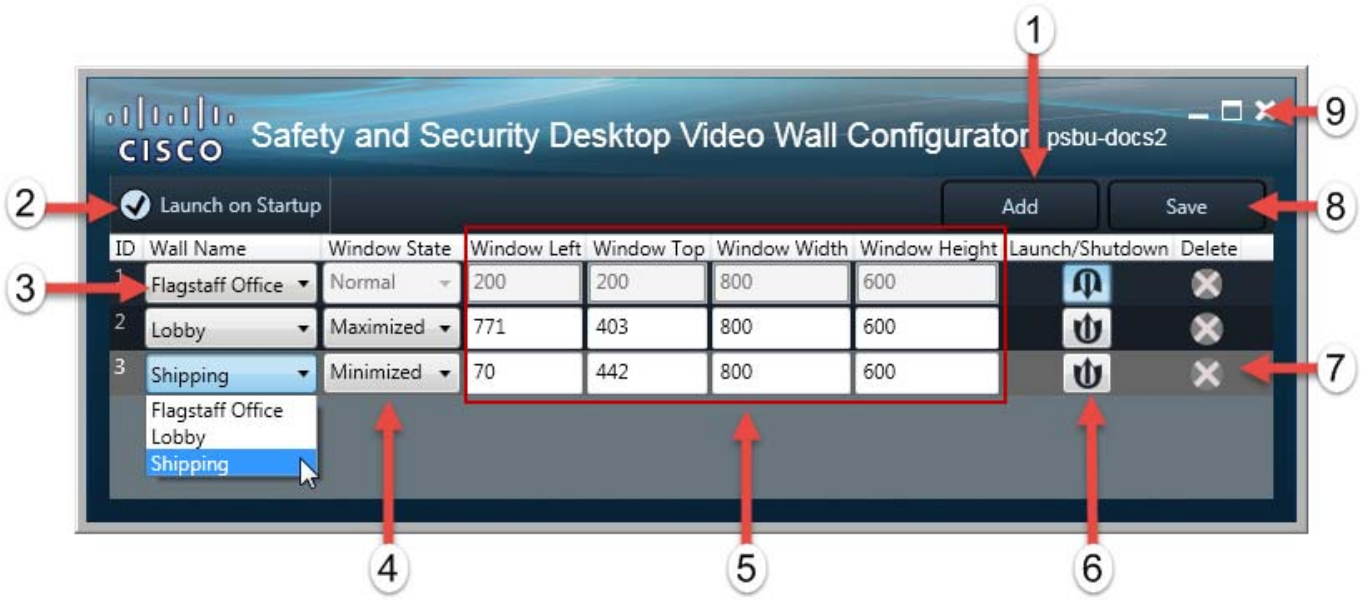
For example:

- 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 (optionally) the Video Wall displays on a workstation reboot.
- Without keyboard and mouse, the operator can view video, but cannot interact with the video playback. The PC can be placed out of reach (such as locked in a desk or cabinet).
- If a keyboard and mouse are connected, the operator can interact with the video, and close and reopen unattended screens using the Cisco SASD Wall Launcher.
- You can create multiple unattended windows to display on different monitors. For example, one monitor can display the All Lobby Doors Video wall, while a second monitor displays a Video wall that rotates panes of side entrances.
- Use Unattended mode to automatically launch a Video Wall on a workstation reboot. This feature can only be enabled for PC reboots. The Video Wall does not relaunch the operator logs off and logs back in.
- You can also use the Cisco SASD Wall Launcher (installed on the desktop) to launch Video Walls on unattended workstations. The Launcher closes any open unattended windows, and relaunches unattended Video Walls, which display as configured in the Operations Manager.
- If an unattended Video Wall is shut down (for example, the Cisco SASD Advanced Video Player application crashes or was closed) or if all panes in the Wall are not streaming video, the unattended Video Wall automatically relaunches.

- On a workstation reboot, unattended windows automatically relaunch on the monitors, maintaining their position (if configured).
- If an unattended Video Wall is closed or stops streaming, it can only be brought back up if the PC is rebooted. Unattended video walls will not start up again if you only log off and log back on (you must restart the PC).

Figure 15 describes the main features of the Cisco SASD Wall Configurator.

Figure 15 Using Cisco SASD Wall Configurator to Define "Unattended" Video Walls



1	**Add**—Click to add a predefined Video Wall to display on a workstation in Unattended mode, and then select the Wall Name from the drop-down menu. • 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 Video Walls in Unattended mode on a workstation restart. • Deselect to manually launch unattended walls using the Cisco SASD Wall Launcher.
3	Wall Name drop-down menu—Select the Video Wall(s) to display on a workstation restart or when the Cisco SASD Wall Launcher starts. **Note:** Video Walls are configured using the Operations Manager.
4	Window State—Defines the size and location of the Video Wall on a workstation restart or when the Cisco SASD Wall Launcher is launched. • **Normal**—The Video Wall window displays in the size and location defined in 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	Video Wall Position—The size and location of the Video Wall in the Normal window state. Resize the Video Wall on screen to automatically change the settings or manually enter the coordinates.
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 appear when you save and exit the Cisco SASD Wall Configurator, when you launch the Cisco SASD Wall Launcher, or (optionally) on a workstation restart.
7	—Delete. Removes the Video Wall from Unattended mode. The deleted Video Wall window will not launch.
8	**Save**—Save the configuration.
9	Close—Quit the Cisco SASD Wall Configurator and launch the Video Walls in unattended mode.

Requirements

Table 9 is a checklist of the Cisco SASD Wall Configurator requirements for configuring unattended workstations:

Table 9 Requirements

Requirements	Requirement Complete? (✓)
Administrative user privileges on the Windows workstation.	❑
An admin account in Cisco Video Surveillance.	❑
Access Permissions—The following access permissions are granted using the Cisco Video Surveillance Operations Manager. • **Video Walls**—Create, update, or delete Video Walls using the 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 displays until the Rollback Time set in the Operations Manager is exceeded. **Note:** Camera views set to **Stream 2 on VSOM Server** automatically revert to **Stream 1 on VSOM Server**. • **Allow Multiple Logins**—This option must be enabled because each unattended video wall requires a unique Cisco VSM login session for the video wall to be displayed. **Note** DO NOT add the user to any user group where “Enable Fixed Duration Timeout” setting is selected. If enabled, the user will be logged out and the unattended wall will restart.	❑
(Minimum) Configure one Video wall on the system (using the Cisco Video Surveillance Operations Manager)	❑

Table 9 Requirements (continued)

Requirements	Requirement Complete? (✓)
Video Walls cannot be configured by users in a user group with access to multiple Sites. Only users with access to a single Site (those not prompted to select a Site) can configure Video Walls. See Understanding Sites, page 17. See the Cisco Video Surveillance Operations Manager User Guide for information about creating and assigning Site access. **Note** An error will occur if a user configured for multiple Sites attempts to log into the SASD Wall Configurator.	❑
Configure all Video Walls in Unattended mode with a Default View in the Operations Manager. **Note:** If you select a Video Wall that does not have a Default View, all video panes will be blank. If all video panes are blank (that is, no camera was selected as a video source in the Operations Manager), then the unattended window repeatedly restarts because video streaming is not detected.	❑

Note: Configure Video Walls 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 unattended workstation, then the unattended windows must be reconfigured.
- DO NOT add the user to any user group where “Enable Fixed Duration Timeout” setting is selected. If enabled, the user will be logged out and the unattended wall will restart.
- To change the video displaying 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 workstations revert to the Default View for the Video Wall on a system reboot.
- Unattended mode configuration applies only to a single Cisco Video Surveillance system. If you log in to a different Cisco Video Surveillance system on the same workstation, you cannot revise existing unattended windows.
- Remote or local users running Cisco SASD or Cisco SASD Advanced Video Player can change unattended SASD Walls views, and publish modified views to the Wall or a different camera to a pane.
- Unattended mode repeatedly restarts if streaming video to all panes is lost. This can be caused by network or system issues or if a Video Wall without a Default View was 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 Unattended mode restarts until communication with the server is reestablished. If the Media Server fails over to another server, then the new server provides video streaming and the video displays.
- If the video stream is lost for one (but not all) video pane, Unattended mode does not restart and the pane displays an error message.

- If a Maintenance mode banner appears at the top of the window, the system was placed in Maintenance Mode in Cisco Video Surveillance Operations Manager by an administrator, and configuration changes are not allowed. See your Cisco VSM Administrator for assistance.

Configuring Unattended Workstations

Use the Cisco SASD Wall Configurator to select Video Walls to display in Unattended mode on a workstation.

Once unattended windows are defined, you can close the Cisco SASD Wall Configurator application. Unattended windows will still automatically relaunch.

Before you begin you must create one or more Video Walls:

1. Log on to the Operations Manager.
   - You must belong to a User Group with permissions to create Video Walls and for the **Push Video to Wall** option.
   - 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.
   - DO NOT add the user to any user group where “Enable Fixed Duration Timeout” setting is selected. If enabled, the user will be logged out and the unattended wall will restart.
2. Create one or more Views.
3. Add one or more Video Walls (**System Settings > Video Wall**).
4. Connect a keyboard and mouse to the workstation.

Note: See your system administrator or the Cisco Video Surveillance Operations Manager User Guide for more information.

To configure unattended workstations:

Step 1 Launch the Cisco SASD Wall Configurator and log in to the application with your Cisco SASD credentials.

Step 2 Click **Add** (Figure 15).

Step 3 Select a Wall Name.

Note: The Video Wall must include a Default View (see Usage Notes, page 38).

Step 4 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 5 Click to launch (display) the Video Wall in Unattended mode.

Step 6 Position the Video Wall window(s) on the workstation monitors.

If the Normal window state is selected the window displays in the same position as defined in the Cisco SASD Wall Configurator.

Step 7 Repeat the above steps to select a Video Wall for each unattended window and position the window on the workstation monitor(s).

Step 8 Select or deselect **Launch on Startup** to launch Unattended mode on a workstation restart.

Tip: If deselected, the unattended windows do *not* appear on a workstation restart. Use the Cisco SASD Wall Launcher to open the unattended windows (see Launching Unattended Windows, page 40).

Step 9 Click **Save** to save the configuration.

Step 10 Close the Cisco SASD Wall Configurator window to quit the application and launch the Video Walls in unattended mode.

Note: If a Video Wall is selected without a Default View, all video panes will be blank. If all video panes are blank (that is, no camera was selected as a video source in the Operations Manager), then the unattended window repeatedly restart since video streaming is not detected (see Requirements and Usage Notes).

Step 11 (Optional) Move the Video Wall windows to display Unattended mode windows one directly behind the other.

Step 12 (Optional) Remove the keyboard and mouse so that the operator can only view video.

Note: You can leave a mouse attached to allow the operator to control video playback (see Viewing Video, page 77).

Launching Unattended Windows

Table 10 lists the options for displaying the Video Walls on a workstation in Unattended mode.

Table 10 Launch Options

Option	Description
Save and exit the Cisco SASD Wall Configurator	Launches the Video Walls when the Cisco SASD Wall Configurator closes.
Launch the Cisco SASD Wall Launcher	Opens all Video Walls added to the Cisco SASD Wall Configurator in Unattended mode. The Launcher also closes any open unattended windows, and then relaunches the unattended Video Wall windows as configured in the Operations Manager.
Restart the workstation	(Optional) If the **Launch on Startup** option is selected in the Cisco SASD Wall Configurator, the Video Walls launch in Unattended mode on a workstation restart (see Usage Notes, page 38).

Note: Only users in user groups with the **Allow Multiple Logins** option enabled can launch unattended windows. Each unattended Video Wall requires a unique Cisco VSM login session to display the Video Wall.

Related Information

To modify Video Walls appearing in Unattended mode, see the following topics:

- Configuring Unattended Workstations, page 39
- Removing a Video Wall From Unattended Mode, page 41

Removing a Video Wall From Unattended Mode

Remove Video Walls from Unattended mode so they no longer automatically appear when unattended windows launch (see Launching Unattended Windows, page 40).

To remove one or all Video Walls from Unattended mode:

Step 1 Launch Cisco SASD Wall Configurator and log in to the application using your Cisco SASD credentials.

Step 2 Click **Delete** in line with the Video Wall to remove 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 display video if the network connection to the Operations Manager is lost, but the connection to the Media Servers for the cameras 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 Views are not updated until the window returns to Online mode.

"Offline" appears in the window title bar when:

- the network connection to the Operations Manager is lost. The unattended windows relaunch in Offline mode.
- the Operations Manager is unavailable during the unattended windows launch. The unattended windows restart in Offline mode.

Transition Times

The Unattended windows periodically check for Operations Manager connectivity, and automatically switch between Online and Offline mode. This avoids switching back and forth during intermittent network issues (such as jitter). Table 11 lists wait times for Online-Offline mode transitions.

Table 11 Online-Offline Transition Times

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

Alert Workspace

Select the Alert workspace (Figure 17) 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

Notes

- 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 the "Maintenance Mode" banner appears, an Operations Manager administrator placed the system in Maintenance Mode and some actions such as acknowledging an alert are not allowed. See your Cisco VSM administrator for assistance.

This section covers the following topics:

- Understanding Events and Alerts, page 44
- Alert Workspace, page 45
- Dynamic Updates of Alert Results, page 50
- Viewing Event URLs, page 56
- Common Tasks, page 57
- Impact of Device Location Changes on Alerts, page 58
- Summary of Events and Corresponding Alerts, page 59

Understanding Events and Alerts

Events represent incidents that occur in the system and devices (such as cameras or camera encoders). Events are aggregated (grouped) into alerts for notification purposes. For example, if a camera goes off-line 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**–Generated on a device health change such as reachability, fan speed, file system usage, or other device-related issues.

  Note: Critical health events always generate alerts.

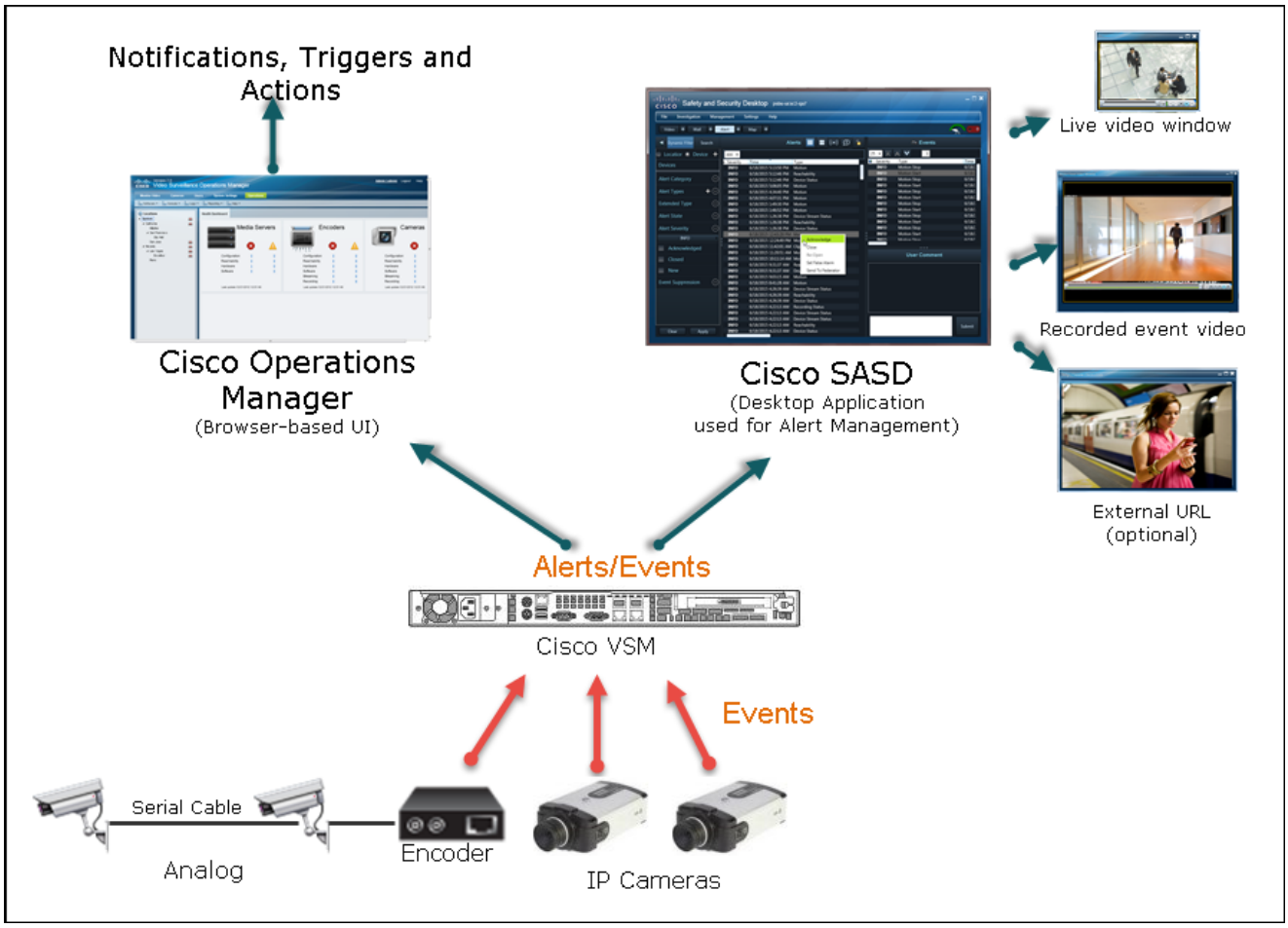
- **Security Events**–You can configure events (such as motion stop or start, analytics, contact closures, or soft triggers from an external system) to generate alerts or perform other actions. You can also forward security alerts to the Federator (if installed).

  Note: By default, Security events do not generate alerts.

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 appear in the same alert.

Figure 16 summarizes how Cisco VSM events and alerts are generated, aggregated, and viewed.

Figure 16 Health Events, Alerts, and Notifications



Alert Workspace

Select the Alert workspace (Figure 17) to view alerts and events related to the selected alert. Numerous actions are available, depending on the alert or event type, for example:

- Right-click an alert to acknowledge, close, re-open, or mark the alert as a false alert.
- View live or recorded event video (if available).

Figure 17 Alert Workspace

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, page 29.
2.	**Search**—Display alerts in a static list based on the filter criteria (including a time span). The alerts in the search results table auto-update on a status change. However, the search result table itself does not auto refresh (new alerts are not inserted, the table does not auto sort, and so on). Refresh the search to view current alerts. **Dynamic Filter**—Display alerts in a auto-updating list based on selected filters (such as location, alert type, and severity).
3.	Click the triangle to display or hide the side panel.

4. Select from the following criteria and click **Apply**.

Tip: If a filter criteria is not selected, all alerts for that filter are displayed.

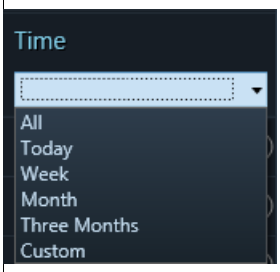
- **Location**—Click + to select a specific location where the alert(s) were created.

  Only alerts from that location are displayed.

- **Device**—Click + to select a location and a specific device (camera).

  Only alerts from that device are displayed.

- **Time** (Search only)—To narrow your search by date and time, select a time from the options in the drop-down menu.



  - To display alerts that occurred in a specific time period, select Custom, click +, select the From and/or To check boxes, and set the dates and times.

    Note: If you do not select a From or To check box, that field cannot be modified and the date in the field is used as the search criteria.

- **Alert Category**—Health or Security (see Understanding Events and Alerts, page 44).
- **Alert Types**—To narrow the results by alert type (for example, Compatibility Mismatch Status or Contact Closure) click +, move all desired alert types into the Selection pane, and click **OK**.
- **Alert Severity**—Click the INFO bar to select the alert severity CRITICAL, MAJOR, MINOR, WARNING, or INFO.

  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 marked CRITICAL. When the camera becomes reachable and a streaming status normal event occurs, the alert severity changes to INFO (see Summary of Events and Corresponding Alerts, page 59).

  Note: INFO requests also display CRITICAL alerts.

- **Extended Type**—Manually enter a search parameter in this field.
- **Alert State**—Filters alerts by All or Only Recovered.
- **Status**—Acknowledged, Closed, or New.
- **Acknowledged By**—Enter the full or partial name of the user who acknowledged the alert. This information appears in the **Ack'd By** column in the Alerts pane.
- **Closed By**—Enter the full or partial name of the user who closed the alert. This information appears in the Closed column in the Alerts pane.
- **Event Suppression** (see Event Suppression, page 67)—Select from the options to:
  - Exclude suppressed alerts
  - Only include suppressed alerts
  - Include all

5.	Select an alert to view related events. Right-click to perform the following: • Change the alert status (acknowledge, close, or re-open the alert). • Mark an alert as a false alarm or change the false alarm state. **Note:** When you change the false alarm state, the System generates a comment visible in the User Comment pane. • Send the alert to the Cisco VSM Federator (see Monitoring Alerts Using the Cisco SASD Federator, page 174 for more information). Alerts in italics are either stale or indicate that the camera was in ES (Event Suppression) mode when the event occurred. Stale alerts are triggered when the camera loses connection with the Media Server and later reconnects. Alerts triggered during the disconnect load into the list when the Media Server connection is restored. Use the User Comment field to add notes about the event.
6.	Right-click the event and select an action to perform in a new Cisco SASD window. • Play Recording Video–Play video of the time of the event. • Play Live and Recording Video–A dual-pane window with live video in the left pane, and recorded video of the event in the right pane. You can set a time prior to the event to start the playback, and set a duration to loop the playback for closer analysis. See Playing Event Video, page 50. **Note:** Multiple events for the same issue are grouped under a single alarm in the Events pane.
7.	—If the URL icon appears in the Events pane, right-click the event to open a new web browser window with additional information or images. See Viewing Event URLs, page 56.
8.	Click the column headers to sort the alerts. **Note:** Only headings with an arrow are sortable. • By default, the Time column sorts alerts with the newest alert at the top. • By default, the Severity column sorts alerts top-to-bottom in the following order: CRITICAL, MAJOR, MINOR, WARNING, INFO
9.	—The camera icon appears if video is available for the event. Right-click the event to select one of the available options, as discussed in these topics: • Copy Camera Recordings From Alerts, page 164 • Play Recording Video, page 51 • Play Live and Recording Video, page 54 Video is available for the all security event types: • Motion start/stop • Contact closure open/close • Soft trigger • Analytics

10.	Click the lock icon to stop or start auto-update of the list: • When unlocked, new alerts are added to the list as they occur. • When locked, dynamic updating pauses and no new alerts are added to the list. Unlock the display to refresh the results. • If the alert list is sorted by time, existing alerts with new events are pushed to the top of the list. **Note:** For existing alerts, the status and timestamp update, but their order in the Alert list changes (that is, newly updated alerts are not pushed to the top of the table).
11.	Select an audible option: • —Beep on incoming alerts. • —Narrate incoming alerts (English language only). All columns in the incoming alert row are read aloud. **Note**: SASD alert narration works only for English content. If any alert content (such as alert type, description, device name, and so on) is in a foreign language, narration will not work correctly. It will skip the non-English text.
12.	Select the workspace view: • —Display the Alerts pane and the Events and Comments pane results side-by-side. • —Display the Alerts pane on the top, and the Events and Comments pane on the bottom.

Dynamic Updates of Alert Results

By default, new alerts are dynamically added to the **Dynamic Filter** results as they occur. New alerts 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. High-severity alerts appear at the top of the list if the results are sorted by Severity.

Note: Click the lock icon to stop or start auto-updates.

The **Search** tab results do not dynamically refresh. The alert table remains static until 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 all security 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 164
- Play Recording Video, page 51
- Play Live and Recording Video, page 54

Copy Camera Recording

You must transfer recordings stored locally on the camera (such as an SD card) to the Cisco Media Server to allow you to view the video. For more information, refer to the following:

- Camera Local Recording Management, page 155
- Copy Camera Recordings From Alerts, page 164

Play Recording Video

To view the video recordings for a security event (such as a motion event), right-click the event and choose **Play Recording Video** (Figure 18). You can enlarge and drag the popup window to another monitor for better viewing.

Figure 18 Play Recording Video From an Alert

If video is unavailable (for example, if the video was automatically deleted after the duration defined in the camera retention rules), an error message appears when you attempt to view the video.

To view available alert video:

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, page 45 and Understanding Events and Alerts, page 44 for more information.

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

Step 4 In the Events pane, right-click an event and select **Play Recording Video** (Figure 18).

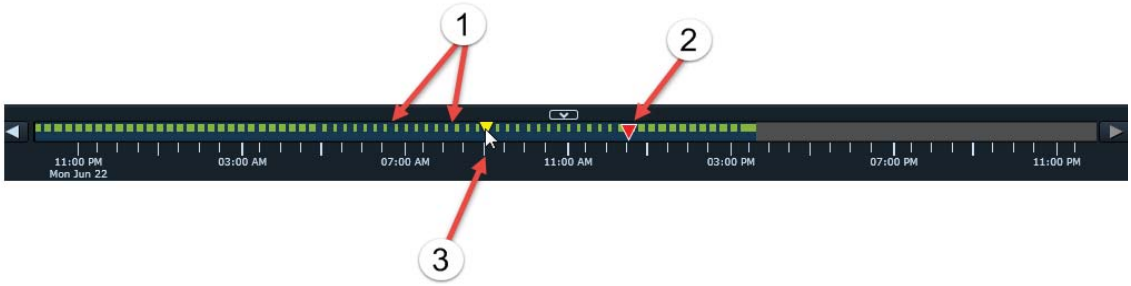
Step 5 (Optional) Use the playback controls to view the event video that was copied from the camera.

- **Prior to Event**—Enter the number of seconds to play before the event was triggered. Click **Apply** to activate the change.
- Select **Loop** to play the video segment in a continuous loop. Click **Apply** to activate the change.
- Enter a **Duration** to define the loop duration. Click **Apply** to activate the change.

The green bar in the timeline indicates recorded video. If the green bar in the timeline is not contiguous, there may be gaps in the recording. When video plays to a gap, it automatically jumps to the recording after the gap.

To play the recording of another event, select that event and select **Play Recording Video** or **Play Live and Recoding Video** from the drop-down menu. The video begins to play *N* seconds before the selected event time, as defined in the **Prior to Event** field.

Figure 19 Recording Video Time Line



1.	Recorded events.
2.	Current event.
3.	Click on a gap in the time line to view the event.

Play Live and Recording 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 open a 2-pane pop-up video window (Figure 20). The left pane displays live video. The right pane displays the recorded video (starting from the selected event trigger point). You can enlarge this popup window and drag it to another monitor for better viewing.

Figure 20 Play Recorded and Live Video Side-by-Side

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

To view the recorded event and live video playback window:

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, page 45 and Understanding Events and Alerts, page 44 for more information.

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

Step 4 In the Events pane, right-click an event and select **Play Live and Recording Video** (Figure 20).

Step 5 (Optional, for recording video panes only) Use the playback controls to view the event video that was copied from the camera.

- **Prior to Event**—Enter the number of seconds to play before the event was triggered. Click **Apply** to activate the change.
- Select **Loop** to play the video segment in a continuous loop. Click **Apply** to activate the change.
- Enter a **Duration** to define the loop duration. Click **Apply** to activate the change.

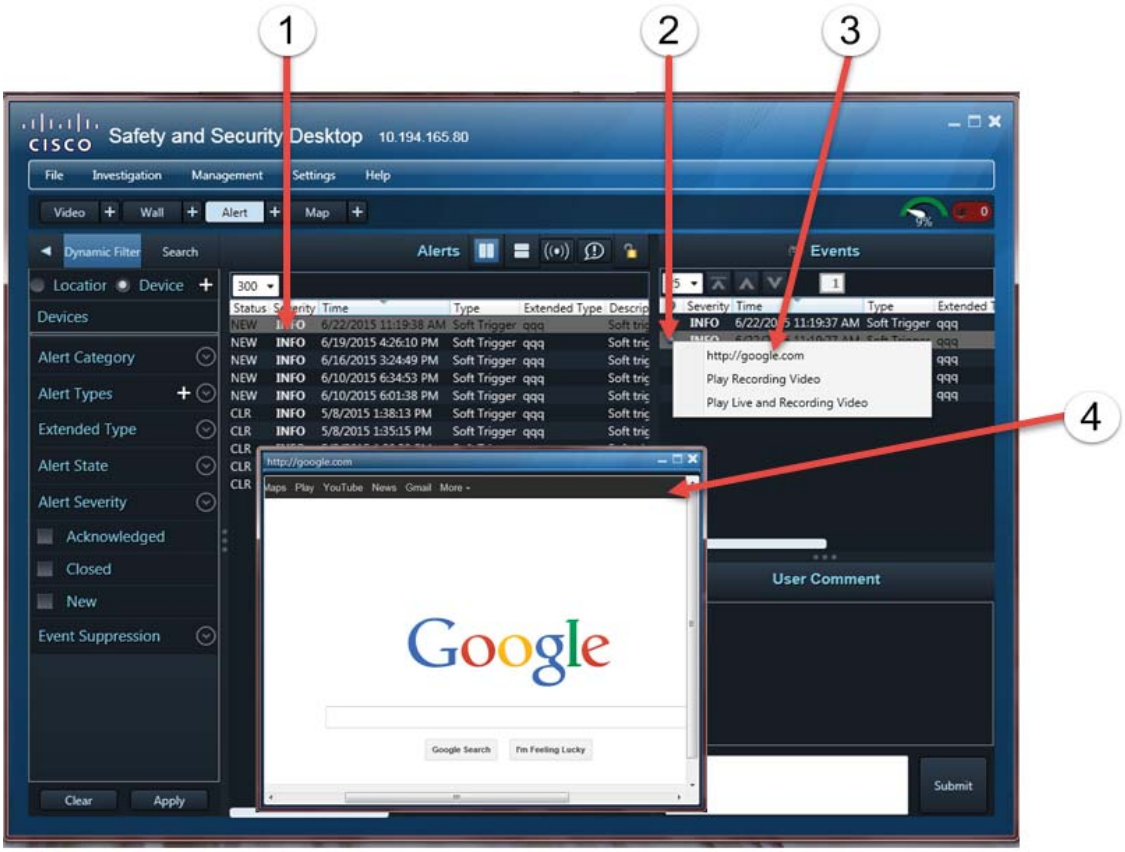
The green bar in the timeline indicates recorded video. If the green bar in the timeline is not contiguous, there may be gaps in the recording. When video plays to a gap, viewing automatically jumps to the recording after the gap.

To play the recording of another event, select that event and select **Play Recording Video** or **Play Live and Recoding Video** from the drop-down menu. The video begins to play *N* seconds before the selected event time, as defined in the **Prior to Event** field.

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 21).

Figure 21 Selecting a Soft Trigger Event URL in Cisco SASD



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 12 describes common tasks you can perform with alerts.

Table 12 Common Alert Tasks

Task	Description
Narrow the list of alerts	• Click the tabs at the top of the Alert list to sort the list by that label. • Click the **Search** tab to refine the list using keywords. • **Dynamic Filter** (narrow the results based on alert type, status, or severity, time, location, and/or device). **Note:** If you do not select filter criteria, all alerts for that filter are displayed.
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**. A system alert appears in the User Comment box with the user name, date, and time.
Close, re-open, or flag an 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. • You can modify closed alerts by: – Adding a comment (the alert state is not changed). – Re-opening the alert. New events for that device and issue are added to the alert.
Add a comment	Select an alert and enter your comment in the User Comment field. Click **Submit** when finished.
View event video (motion and security alerts only)	The camera icon appears if video is available for the event. Right-click the event to select an option and open a video playback window. See Playing Event Video, page 50.
View alerts on a larger location map	Open the Map workspace (see Map Workspace, page 71).

Impact of Device Location Changes on Alerts

Because device locations rarely change, the alert location is normally the same as the device location. However, if the device location changes, the following occurs:

- New events show the new location, but are added to the existing (and open) alert at the old location.
- When an operator closes an alert, new events create a new alert at the new location. That is, the location reference in the alert is 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. An administrator changes the device location 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 *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 at *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

Table 13 summarizes the events included in each Cisco VSM alert.

Note: Some alerts include events of multiple types. For example, a motion alert can include the "motion_start" and "motion_stop" events.

Table 13 Events Included in Operations Manager Alerts

Alert	Events included in the alert	Severity	Alert Description
activemq_connectivity_status	activemq_connectivity_status	INFO	Active MQ connectivity established.
		CRITICAL	Active MQ connectivity not established.
analytics	analytics_occurred	INFO	Analytics event of type occurred for rule.
auto_discovery	auto_discovery	N/A	N/A
backup_configuration_mismatch	backup_configuration_mismatch	INFO	Backup configuration mismatch status.
		CRITICAL	Media Server backup configuration settings do not match VSOM.
camera_app	camera_app	INFO	Camera app event occurred.
camera_app_config_status	camera_app_config_status	INFO	Camera app is on the camera.
		CRITICAL	Camera app is not on the camera.
camera_app_installation_status	camera_app_installation_status	INFO	Camera app is installed on the camera.
		CRITICAL	Camera app is not installed on the camera.
camera_missed_notification	camera_missed_notification	WARNING	Recovered events from camera.
camera_reported_health	camera_reported_health	INFO	Camera health is normal.
		CRITICAL	Camera health is critical.
camera_security	camera_security	INFO	Camera security event occurred.
camera_storage_unconfigured_status	camera_storage_unconfigured_status	INFO	Camera storage configuration issue with camera and template cleared.
		CRITICAL	Camera has no storage disks, but the template defines advanced storage with camera storage enabled.

Table 13 Events Included in Operations Manager Alerts (continued)

Alert	Events included in the alert	Severity	Alert Description
camera_tamper_config_status	camera_tamper_config_status	INFO	Camera tamper configuration template was removed or configured on the camera.
		CRITICAL	Camera tamper configuration template is not configured on the camera. **Note:** Upgrade the firmware or remove the configuration template.
capability_mismatch_status	capability_mismatch_status	INFO	Configuration defined in the template and the configuration supported by the camera match.
		CRITICAL	Configuration defined in the template and the configuration supported by the camera do not match.
chassis_intrusion	chassis_intrusion	INFO	No chassis intrusion detected.
		CRITICAL	Chassis intrusion occurred.
clipping	clip_start	INFO	Clipping initiated.
	clip_completed	INFO	Clipping completed.
	clip_deleted	INFO	Clipping deleted.
	clip_failed	INFO	Clipping failed.
config_mismatch_status	config_mismatch_status	INFO	Configuration matches between VSOM and the Media Server for the device.
	hwid_mismatch_status	CRITICAL	Configuration mismatch between VSOM and the Media Server for the device.
contact_closure	contact_closure_opened	INFO	Contact closure opened on port.
	contact_closure_closed	INFO	Contact closure closed on port.

Table 13 Events Included in Operations Manager Alerts (continued)

Alert	Events included in the alert	Severity	Alert Description
contact_closure_unconfigured_status	contact_closure_unconfigured_status	INFO	Camera contact closure template mismatch event cleared.
		CRITICAL	Camera contact closure is not configured, but advanced contact closure events are defined in the template.
coredump	coredump	CRITICAL	Core dump critical.
database_inconsistency	database_inconsistency	INFO	Media Server database is consistent.
		CRITICAL	Media Server database is inconsistent.
device_status	device_status	INFO	Streaming status normal.
		CRITICAL	Streaming status critical.
	device_config_status	INFO	Device configuration normal.
		CRITICAL	Error in the device configuration.
device_stream_status	device_stream_status	INFO	Streaming status normal.
		CRITICAL	Streaming video loss.
	device_connection_status	INFO	Streaming status normal.
		CRITICAL	Streaming connection loss occurred.
disk_usage_status	disk_usage_status	INFO	Storage requirements met.
		CRITICAL	Storage requirements insufficient.
driver_pack_event	driver_pack	INFO	Driver pack event.
driverpack_mismatch_status	driverpack_mismatch_status	INFO	Driver pack match between VSOM and the Media Server for the device.
		CRITICAL	Driver pack mismatch between VSOM and the Media Server for the device.
encoder_max_streams_used_status	encoder_max_streams_used_status	INFO	Number of streams is under the maximum range.
		CRITICAL	Maximum number of streams reached for encoder.

Table 13 Events Included in Operations Manager Alerts (continued)

Alert	Events included in the alert	Severity	Alert Description
event_overload_status	event_overload_status	INFO	Normal VSOM events processing resumed.
		CRITICAL	VSOM dropped events due to a large number of events received.
fan_speed	fan_speed	INFO	Fan speed is normal.
		CRITICAL	Fan speed is critical.
firmware_mismatch_status	firmware_mismatch_status	INFO	Camera template firmware matches with the camera firmware.
		CRITICAL	Camera template firmware mismatch with the camera firmware.
fs_usage	fs_usage	INFO	File system usage on normal.
		CRITICAL	File system usage on critical.
ha_config_mismatch_status	ha_config_mismatch_status	INFO	Configuration matches between VSOM and the primary Media Server and the redundant/failover Media Servers.
		CRITICAL	Configuration mismatch between VSOM and the primary Media Server and the redundant/failover Media Servers.
identity_collision_status	identity_collision_status	INFO	Identity collision issue resolved.
		CRITICAL	Another device with one or more identity criteria exists in the system.
insufficient_backup_space_status	insufficient_backup_space_status	INFO	Automatic VSOM database backup resumed.
		CRITICAL	Insufficient space is preventing automatic VSOM database backups.
load_average	load_average	INFO	Load average normal.
		CRITICAL	Load average critical.
maplayer_mismatch_status	maplayer_mismatch_status	INFO	Geo server map layers matches VSOM.
		CRITICAL	Map layers on Geo server do not match VSOM.

Table 13 Events Included in Operations Manager Alerts (continued)

Alert	Events included in the alert	Severity	Alert Description
mem_free	mem_free	INFO	Memory usage normal.
		CRITICAL	Memory usage critical.
motion	motion_start	INFO	Motion started on.
	motion_stop	INFO	Motion stopped on.
motion_unconfigured_status	motion_unconfigured_status	INFO	Camera configuration includes motion window.
		CRITICAL	Motion window is not configured on the camera. Record on motion and other actions are disabled.
ms_db_down	ms_db_down	INFO	Media Server regained connection to database.
		CRITICAL	Media Server lost connection to database.
nic_usage	nic_usage	INFO	NIC usage normal.
		CRITICAL	NIC usage critical.
pacemaker_state	pacemaker_state	INFO	HA functionality currently available. Pacemaker service running.
		CRITICAL	HA functionality is not available. Pacemaker service not running.
password_expired_status	password_expired_status	INFO	Password change accepted.
		CRITICAL	Password expired. New password required.
pending_driverpack_upload_status	pending_driverpack_upload_status	INFO	Pending driver pack upload: the Media Server and VSOM have these driver packs uploaded.
		CRITICAL	Pending driver pack upload: the Media Server and VSOM do not have these driver packs uploaded.
pending_software_upload_status	pending_software_upload_status	INFO	Pending software upload: the Media Server and VSOM have this software uploaded.
		CRITICAL	Pending software upload - the Media Server and VSOM do not have this software uploaded.

Table 13 Events Included in Operations Manager Alerts (continued)

Alert	Events included in the alert	Severity	Alert Description
power_supply	power_supply	INFO	Power supply normal.
		CRITICAL	Power supply critical.
ptz	ptz_start	INFO	PTZ start event occurred.
	ptz_stop		PTZ stop event occurred.
raid_status	raid_status	INFO	Virtual drive Raid failure cleared.
		CRITICAL	Virtual drive Raid failure critical.
rcd_backup	rcd_backup	INFO	Recording backup failure normal.
		CRITICAL	Recording backup failed for last file time.
rcd_status	rcd_status	INFO	Recording status normal.
		CRITICAL	Recording status critical.
	recording_groomed	INFO	Parts of the recording were groomed to free disk space.
reachability	reachability	CRITICAL	Device unreachable.
	hostname_resolution_failure_status	INFO	Device reachable.
recorder_oversubscribed	recorder_Oversubscription	INFO	Disk space usage for recordings normal.
		CRITICAL	Disk space usage for recordings over subscribed.
redundancy_unconfigured_status	redundancy_unconfigured_status	INFO	Redundancy/failover servers configured as the camera primary Media Server.
		CRITICAL	No redundancy/failover servers configured as the camera primary Media Server.
scheduled_backup_status	scheduled_backup_status	INFO	Scheduled backups succeeded.
		CRITICAL	Scheduled backups failed.

Table 13 Events Included in Operations Manager Alerts (continued)

Alert	Events included in the alert	Severity	Alert Description
serial_ptz_controller_unconfigured_status	serial_ptz_controller_unconfigured_status	INFO	Serial PTZ controller is configured on the camera or PTZ notification is not set in the configuration template.
		CRITICAL	Serial PTZ controller is not configured on the camera. PTZ operations are not enabled.
server_status	server_status	INFO	Server status is START.
		CRITICAL	Server status is.
server_storage_write_status	disk_write_failure	INFO	Write access to normal.
		CRITICAL	Write access to critical.
services_reachablity	services_reachablity	INFO	Is reachable on Server.
		CRITICAL	Is unreachable on Server.
soft_trigger	soft_trigger	INFO	Camera soft trigger event occurred.
software_mismatch_status	software_mismatch_status	INFO	Software mismatch: the Media Server and VSOM have this software installed.
		CRITICAL	Software mismatch: the Media Server and VSOM do not have this software installed.
temperature	temperature	INFO	Temperature normal.
		CRITICAL	Temperature critical.
time_out_of_sync_status	time_out_of_sync_status	INFO	VSOM time matches the Media Server.
		WARN	VSOM time mismatch with the Media Server.
ums_config_change	ums_config_change	INFO	No Media Server configuration change.
		CRITICAL	Media Server configuration change.
ums_failover_status	ums_failover	WARN	UMS failed over.
	ums_failback	INFO	UMS failed back.
ums_identity_mismatch_status	ums_identity_mismatch_status	INFO	VSOM UMS alternate ID matches the Media Server alternate ID.
		CRITICAL	VSOM UMS alternate ID mismatch the Media Server alternate ID.

Table 13 Events Included in Operations Manager Alerts (continued)

Alert	Events included in the alert	Severity	Alert Description
ums_version_mismatch_status	ums_version_mismatch_status	INFO	VSOM UMS version matches the Media Server.
		CRITICAL	VSOM UMS version mismatch with the Media Server.
unknown_camera_app_status	unknown_camera_app_status	INFO	Camera app was either uploaded to VSOM or uninstalled from the camera.
		CRITICAL	Unknown camera app is installed on the camera.
unknown_hw_sensor	unknown	INFO	Unknown hardware sensor normal.
		CRITICAL	Unknown hardware sensor critical.
voltage	voltage	INFO	Voltage normal.
		CRITICAL	Voltage critical.
vsom_ha_replication_status	vsom_ha_replication_status	INFO	VSOM HA database/file system replication succeeded.
		CRITICAL	VSOM HA database/file system replication failed.
vsom_version_mismatch_status	vsom_version_mismatch_status	INFO	VSOM server version matches VSF.
		CRITICAL	VSOM server version mismatch with VSF.

Event Suppression

You can enable Event Suppression (ES) for a camera to stop all configured actions for events (as set in the VSOM configuration template), except Security alerts. ES mode is useful when the system is in Maintenance mode to prevent the Alerts list from reporting alerts while you are working on an issue.

ES mode suppresses only Security events; Health events are not suppressed. When ES mode is enabled and the action Alert is configured, then events and alerts are created with the state "Created during event suppression." No other actions execute. When ES mode expires or is disabled by the user, event actions are processed normally.

Note: You must be in a user group with access permissions for "Control Event Suppression" to enable or disable ES mode. Ask your administrator for assistance, if necessary.

Note: ES is not supported in Cisco SASD Federator and Cisco Advanced video player.

This section covers the following topics:

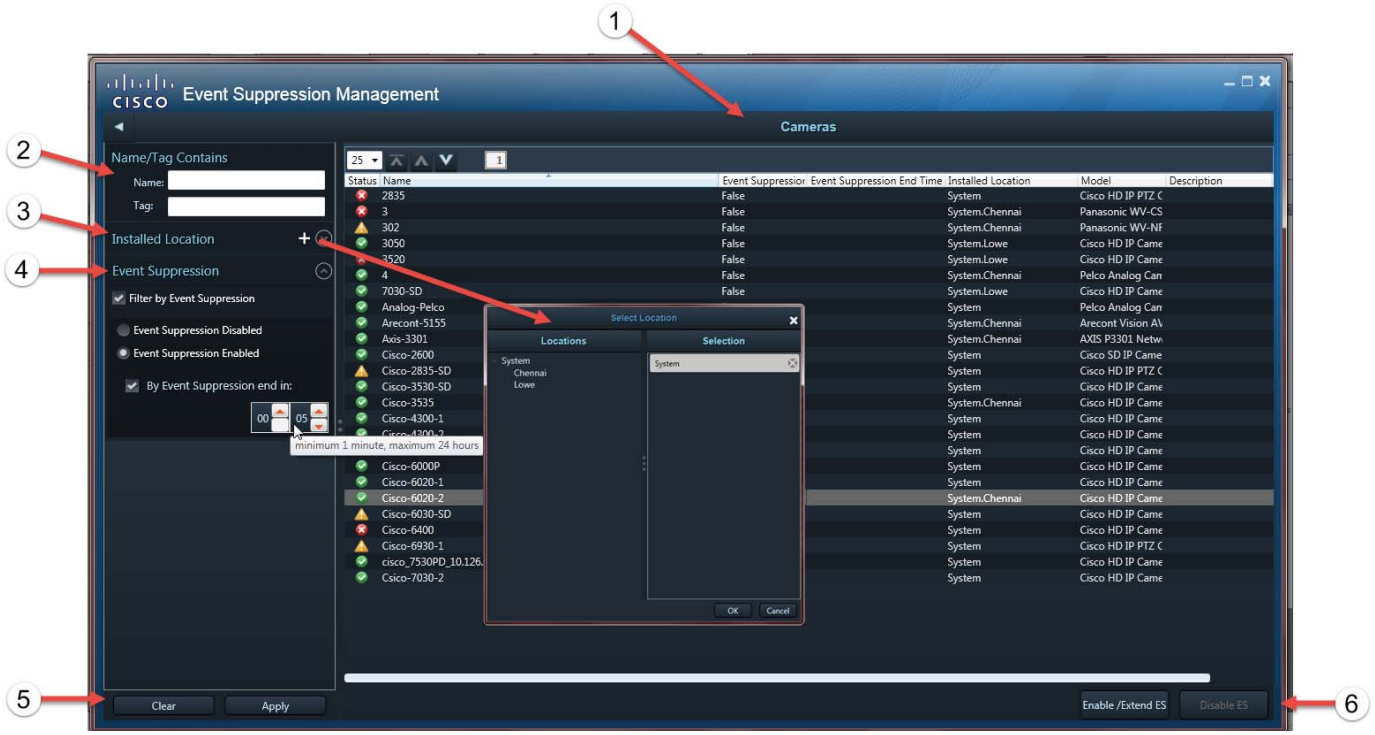
- Enabling ES Mode, page 69
- Disabling ES Mode, page 70

When a camera is in ES mode, the following occurs on event detection:

- All Security events with Alert action are tagged with "Created Under Event Suppression Mode," which allows you to filter alerts using this label.
- All other actions defined for Security events are not executed by either VSM or VSOM.
- Event handling automatically reverts to normal when ES mode expires or is disabled.
- ES mode is also available in HA and DR installations, including when a redundant or failover server is streaming video from the camera. The Media Server will not perform actions associated with events.

Note: You can filter alerts to include or exclude cameras in Event Suppression mode (see Figure 17 on page 46).

Figure 22 Event Suppression Management Windows



1.	**Cameras** list—Devices in the selected location and listed by applied filters.
2.	Device **Name** and **Tag**—Apply this filter to search by the name and tag assigned to cameras in VSOM.
3.	**Installed Location**—Click + to open the Select Location window to refine the list by camera location.
4.	**Event Suppression**—Expand the Event Suppression pane, select **Filter by Event Suppression**, and choose from the following: • **Event Suppression Disabled** to list cameras not in ES mode. • **Event Suppression Enabled** to list cameras in ES mode. – (Optional) Set the **By Event Suppression end in** time to list cameras whose ES mode is expiring within that time.
5.	**Apply**—Applies the filters to the Cameras list. **Tip:** Click **Clear** to reset the filters.
6.	**Enable/Extend ES**—Enables ES mode or extends ES mode by the time set in the VSOM configuration template for the selected cameras. **Disable ES**—Disables ES mode on the selected cameras.

Enabling ES Mode

To enable Event Suppression mode, do the following:

Note You must be in a user group with access permissions for “Control Event Suppression”.

Step 1 Select **Management > Event Suppression**.

The Event Suppression Management window appears (Figure 22).

Step 2 (Optional) Apply filters to display only devices on which you want to enable ES mode.

Step 3 Select cameras in the Cameras list.

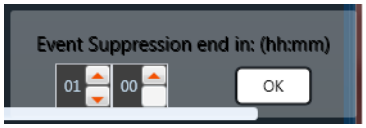
You can use standard Windows-style selection actions:

- To select one camera, click one row in the Cameras list.
- To select multiple cameras not contiguously listed, CTRL-click the desired rows in the Cameras list.
- To select multiple contiguously listed cameras, Shift-click the desired beginning and end rows in the Cameras list.

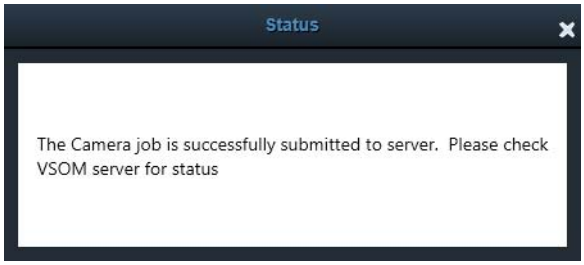
Step 4 Click **Enable/Extend ES**.

- (Optional) Set the ES mode expiration timer between 1 minute and 24 hours.

  Note: This extends ES mode in selected cameras that already have ES mode enabled.



The following status message appears:



On job completion, ES mode is enabled on the selected cameras.

Disabling ES Mode

To disable ES mode:

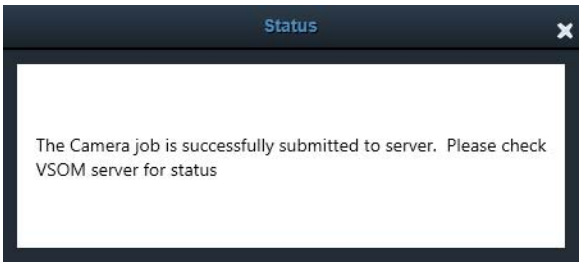
Step 1 Apply the Event Suppression filters to display only cameras in ES mode.

Step 2 Select cameras in the list

Tip: Shift-click to select all cameras in the list

Step 3 Click **Disable ES**.

The following status message appears:



On job completion, ES mode is disabled on the selected cameras.

Map Workspace

The Map Workspace displays maps of the region, city, building, or other areas where the Cisco VSM is deployed (Figure 23). Use maps to view a physical representation of the camera locations in your deployment or as an alternative way to locate cameras and drag them onto a Video Wall.

This section contains the following topics:

- Viewing Maps, page 71
- Requirements, page 74
- Working With Image Layers, page 75
- Summary of Map Workspace Options, page 76

Viewing Maps

Click a location to view the associated map(s). 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). Cameras at that location appear as a camera marker on the map.

Click the camera marker to display a dragable icon or double-click the camera marker to view video in a popup window.

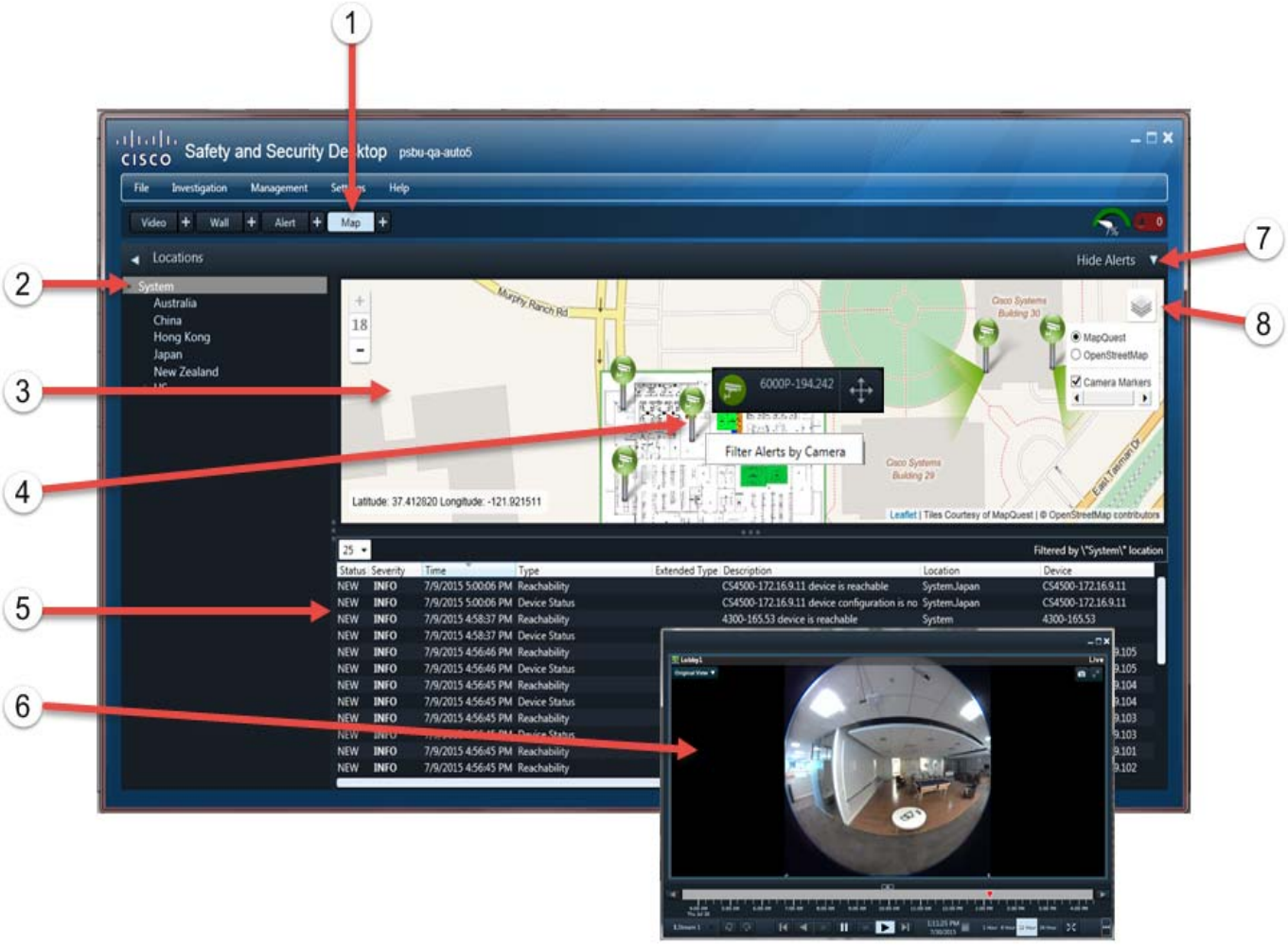
Notes

- 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.
- When upgrading Cisco SASD, 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 requires a Cisco VSM Map server. See “Migrating Map Images From a Previous Cisco VSM Release” in the Cisco Video Surveillance Operations Manager User Guide for more information.
- Location map images are typically provided by a mapping service (such as Mapquest), which requires access to the public Internet. For example, the base layer image can be a city, region, or campus that all other images appear on.

  Map images may not be displayed if your organization prefers not to use a mapping service, or does not allow public Internet access for security or other reasons. In this case, a base layer image can be manually added. See your Cisco VSM administrator for more information.

Figure 23 describes the main elements of the Map workspace.

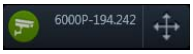
Figure 23 Map Workspace



1.	**Map Workspace** tab. **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, page 29. **Note:** The Map Workspace is only available in the Cisco SASD application. Maps are not included in the Cisco SASD Advanced Video Player or Cisco SASD Federator applications.
2.	Locations. Select a location to display maps for that location.
3.	Map for the selected location. **Tip:** Double-click anywhere on the map or click and roll the mouse wheel to zoom the map image.

4. Camera marker

- A number is displayed when multiple cameras are present and the map is too zoomed out to display individual icons. Zoom in to view individual icons.

- Single-click a camera marker to display a dragable icon 

that you can drag onto a duplicate video or wall workspace.

  Note: You cannot drag icons onto an unattended Video Wall.
- Double-click a camera marker to view video from that camera in a popup window. Click anywhere on the map to dismiss the video feed.
- Right-click a camera marker and select **Filter Alert by Camera** to view alerts for that device.
- Camera marker color represents device status:
  - Green—*Enabled: OK*
  - Yellow—*Enabled: Warning*
  - Red—*Enabled: Critical*

5. Location alerts

- 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 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 following order:

    CRITICAL, MAJOR, MINOR, WARNING, INFO

See Alert Workspace, page 43 for more information about viewing and managing alerts.

6. Video playback window for the selected camera.

See Viewing Video, page 77 for more information.

7. Click **Hide Alerts** to hide or show the alerts pane below the map.

8. Map provider selector.

- Click to select a map provider (such as MapQuest or OpenStreetMap).
- The provider displays the map (such as the street or satellite view) for the selected location.
- Image layers (such as floor plans in a building) are also available in the selector icon. See Working With Image Layers, page 75.
- Select Camera Markers to display camera markers on the map.

Requirements

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

Table 14 Requirements

Requirements	Requirement Complete? (✓)
A Cisco Maps Server must be added to the Operations Manager configuration. The location maps and image layers configured in Operations Manager are available for use in the Cisco SASD Maps workspace. **Note:** GeoServer (GIS) is required for adding and displaying layers. For simple maps, the GIS is not required, but you must have an Internet connection and at least one active Map server provider (enabled by default in VSOM) to display maps.	❑
Internet Explorer (IE) 10 or 11 must be installed on the monitoring workstation: 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.	❑

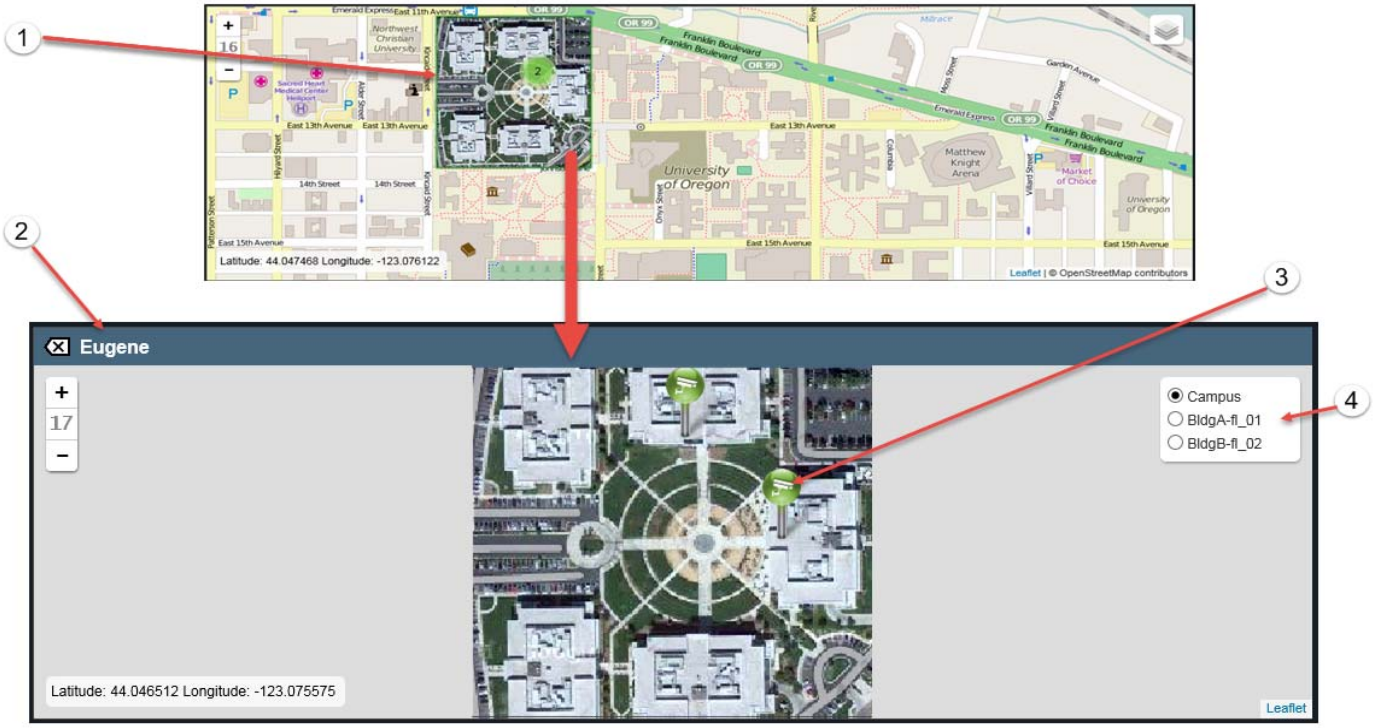
Working With Image Layers

Image layers (Figure 24) 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 green box to show the enlarged image layer, then click to display and select the image layers available for a location. Camera markers represent the real-world location of cameras in each image, allowing you to view video and alerts from specific cameras.

Click the X in the enlarged image layer to close the image group, and then the icon will allow you to select a Map provider.

Figure 24 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 markers • 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* – Yellow—*Enabled: Warning* – Red—*Enabled: Critical*
4.	Image Layer selection. • Click the selector icon to choose an image layer (such as a building floor plan).

Summary of Map Workspace Options

To use map images:

Step 1 Select the Map Workspace (Figure 23).

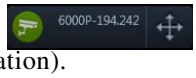
Step 2 Expand the location hierarchy and select a location from the list.

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

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

Step 5 (Optional) Click to choose an image layer (such as a building floor plan).

Step 6 (Optional) Double-click a camera marker to view video for that camera in a popup window.

Step 7 (Optional) Single-click a camera marker to display a dragable icon 

that you can drag onto a Video Wall (see Wall Workspace, page 31 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.

Viewing Video

This section describes the controls and features for video playback. 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.

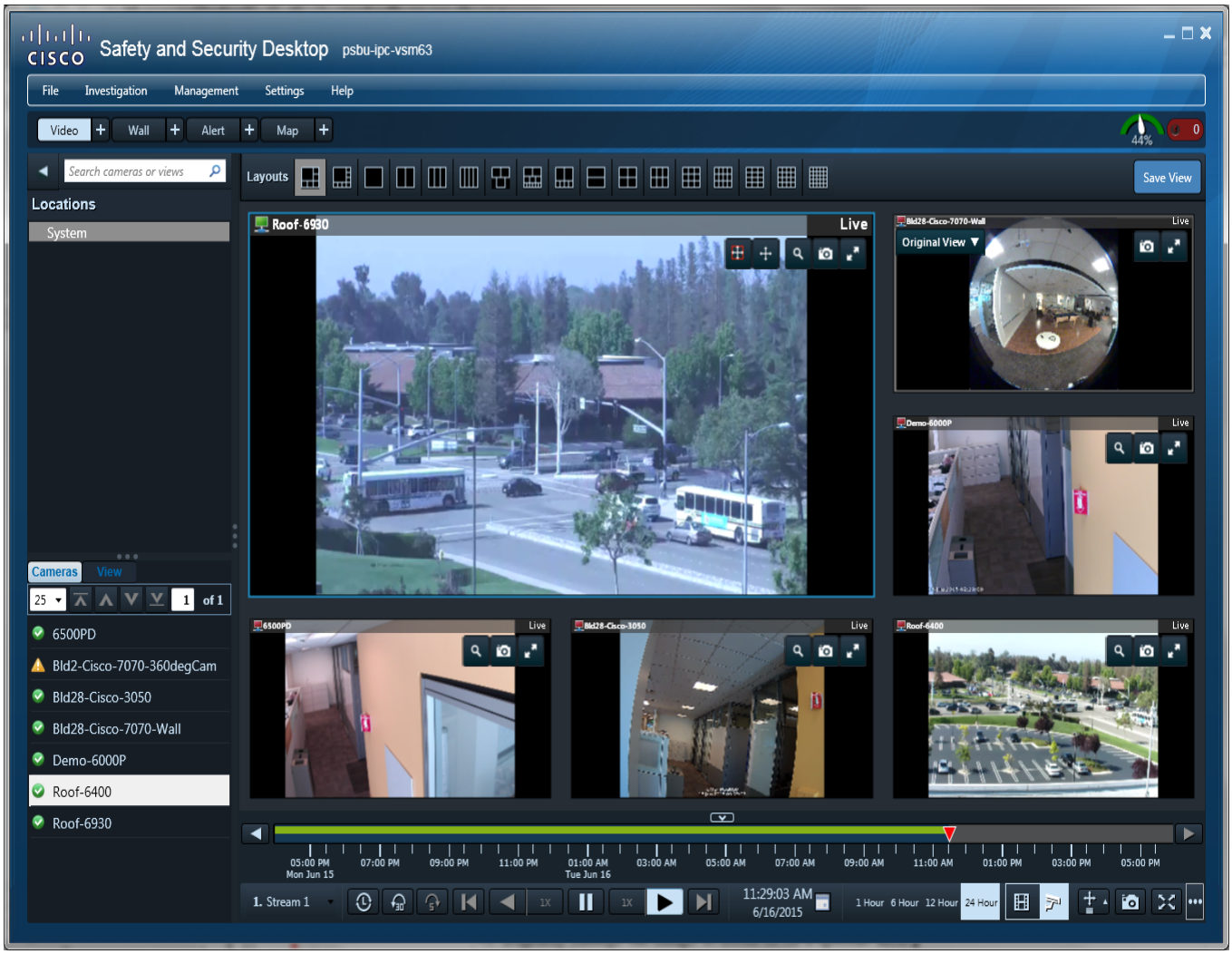
This section covers the following topics:

- Viewing Live Video, page 80
- Viewing Recorded Video, page 82
- Creating and Viewing Video Clips, page 87
- Creating a Repeat Segment, page 94
- Using On-Demand Recording, page 95
- Using the Privacy Mask, page 97
- Using the Smooth Video Settings When Viewing Live Video, page 100
- Synchronizing Video Playback in Multiple Panes, page 102
- Using the Pan-Tilt-Zoom (PTZ) Controls, page 104
- Using 360° Camera Controls, page 109

To view live and recorded video, log on to the monitoring application and drag 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 25 shows a multi-pane view using the Cisco Video Surveillance Safety and Security Desktop (Cisco SASD) application.

Figure 25 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:

- Mute or unmute the audio (if available).
- Digitally enlarge the image to zoom in on a specific area.
- Save a snapshot of a video pane.
- Expand an image to fill the window.
- Control the pan-tilt-zoom (PTZ) movements of a camera (if supported by the camera).
- Pause, play, or skip forward and back.
- Switch between live and recorded video.

The timeline and controls at the bottom of the window provide additional options, including:

- Select a video stream.
- Select a time range (which can be used to play a loop of recorded video or to create a clip).
- Synchronize multiple viewing panes.
- Accurate frame step forward or backward.

- Play forward or backward (and play at slower or faster than normal speeds).
- Seek to an exact time in the recording.
- Take a composite snapshot of all panes.
- PTZ the camera to a preset position (if configured).
- Expand an image to fill the screen.
- Adjust audio volume and balance (cameras with audio capability).
- Create and save video clips from recorded video.
- Record live video.
- Synchronize the playback of multiple recordings.

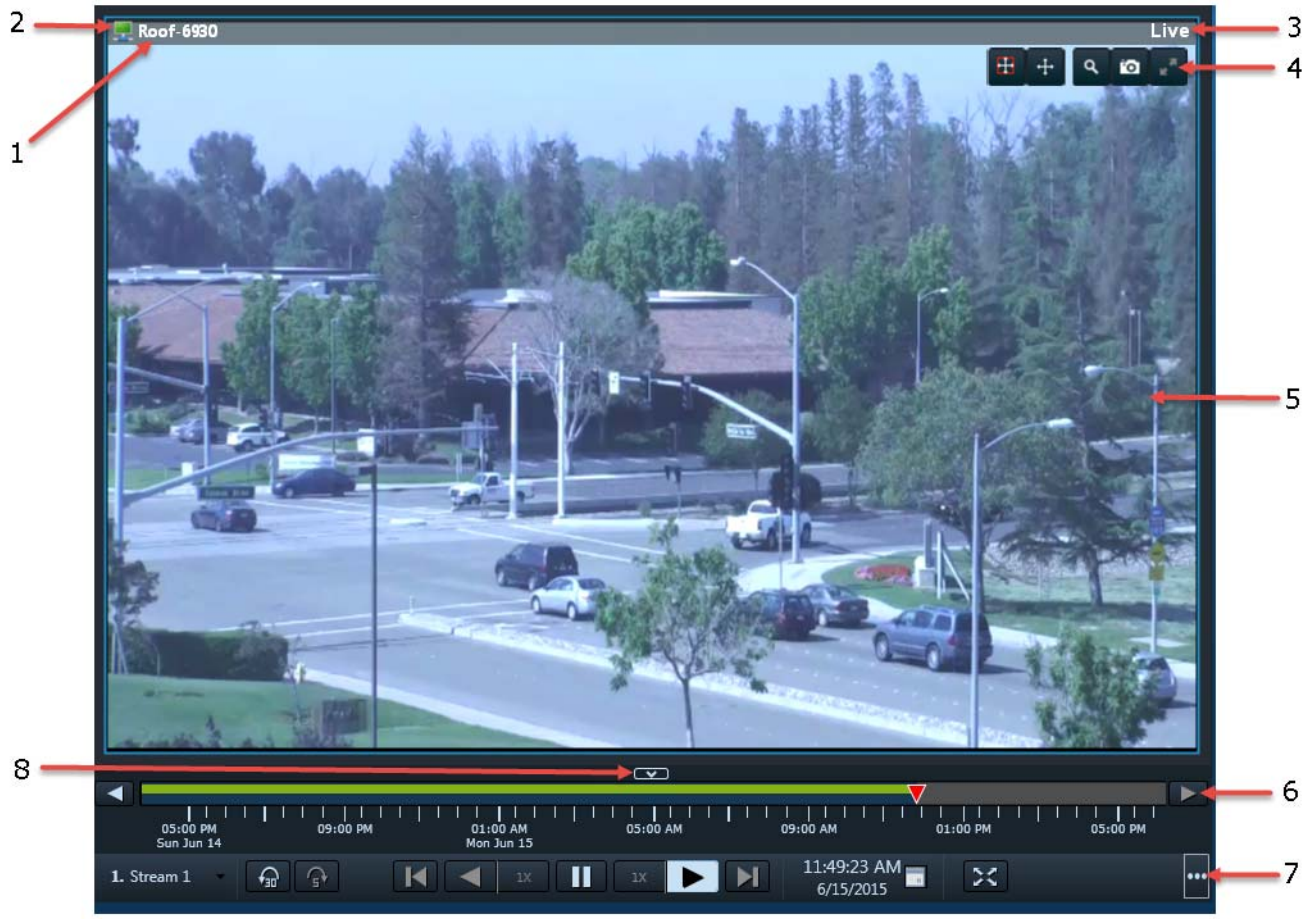
The blue border that surrounds a video pane indicates that the pane is selected, and the controls and actions apply to that pane. Click anywhere in a video pane to make it active. If multiple panes are synchronized, all panes are active and the controls and actions performed using the control bar at the bottom of the application window apply to all panes.

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. On-demand recording options are available only if On-Demand Recording is enabled on the camera. Synchronized playback is available for recorded video. See your system administrator for more information.

Viewing Live Video

Live video displays by default when you log in to the viewing application. Figure 26 summarizes the controls available in each viewing pane and below the video display area.

Figure 26 Live 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 I-frame video stream can be automatically applied. See the Using the Smooth Video Settings When Viewing Live Video, page 100 for more information.
3.	Indicates live or recorded video (recorded video displays a time stamp such as).

4. Control icons.

- **Toggle audio mute**—The audio icon appears if the camera supports audio. Click to enable or mute audio volume. To control volume and balance, use the Toggle Audio button in the control bar (see below).
- **Toggle PTZ**—Enables or disables the pan, tilt and zoom (PTZ) controls. See the Using the Pan-Tilt-Zoom (PTZ) Controls, page 104.
- **Toggle PTZ to region**—Enables or disables the PTZ controls for a region of the viewing area that you select. See the Using the Pan-Tilt-Zoom (PTZ) Controls, page 104.
- **Privacy Mask**—Enables or disables the Privacy Mask. See the Using the Privacy Mask, page 97.
- **Toggle digital zoom**—Digitally enlarges the image to zoom in on a specific area. Adjust the viewing area in the small window to define the portion of enlarged video to display.
- **Save a snapshot of the video**—Saves a snapshot of a single video pane (*excluding* control icons, timestamps and other information) in BMP, JPEG, PNG, or TIFF format.
- **Toggle Expanded pane mode**—Enlarges the video to the size of the video display area.

Note: Set your monitor color setting to 32-bit. The control bar and audio icon cannot display if your workstation monitor color setting is 16-bit.

5. Video image.

6. Timeline—Use with recorded video (see the Viewing Recorded Video, page 82 for more information).

7. Live and recorded video control bar. Click to show all the icons in the control bar.

- 1. Stream 1 —Selects the live and recorded video streams (primary or secondary) supported by the camera.
- **Sync all panes**—Controls the playback in multiple video panes. See the Synchronizing Video Playback in Multiple Panes, page 102.
- **Pause**—Pauses the video playback (if enabled).
- **Play Forward**—Plays the video forward at normal speed.
- **Skip Back**—Switches to recorded video and skips back 30 seconds.
- **Switch Between Live and Recording**—Switches between live and recorded video. indicates live video. Click to switch to the recorded view.
- **PTZ Presets** (Live video only)—Opens the PTZ preset list that allows you to quickly adjust the camera view.
- **Composite Snapshot**—Saves a snapshot of multiple video panes (*including* control icons, timestamps and other information) in BMP, JPEG, PNG, or TIFF format.
- **Enable FullScreen Mode**—Enlarges the video image to fill the entire monitor screen. To exit, press `Esc`.
- **Toggle Audio**—Enables or mutes the audio. Click the down arrow to adjust the volume and balance settings.

  Notes

  - The other playback controls are used with recorded video only. See Figure 27 on page 83 for more information.
  - When viewing video in multiple panes (not synchronized), each pane has a quick-access control bar with icons to play the video, pause, and switch between live and recorded video .
  - When viewing video in a single pane or multiple synchronized panes, all playback controls are in the control bar at the bottom of the application window.

8. —Hides the timeline and the control bar. Click to show the timeline and control bar again.

Usage Notes

- You can view up to 48 video streams simultaneously per workstation.
- 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.
- 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 Settings When Viewing Live Video, page 100 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.
- You can display a camera's secondary stream by default, if necessary. This is useful if playback performance is poor, and you want to display lower-resolution video. To do this, select the camera's secondary stream and save the View. See Saving a Video "View" (Multi-Pane Grid), page 27.

Additional Information

Refer to the following topics for additional options:

- Using On-Demand Recording, page 95
- Using the Smooth Video Settings When Viewing Live Video, page 100
- Synchronizing Video Playback in Multiple Panes, page 102
- Using the Pan-Tilt-Zoom (PTZ) Controls, page 104

Viewing Recorded Video

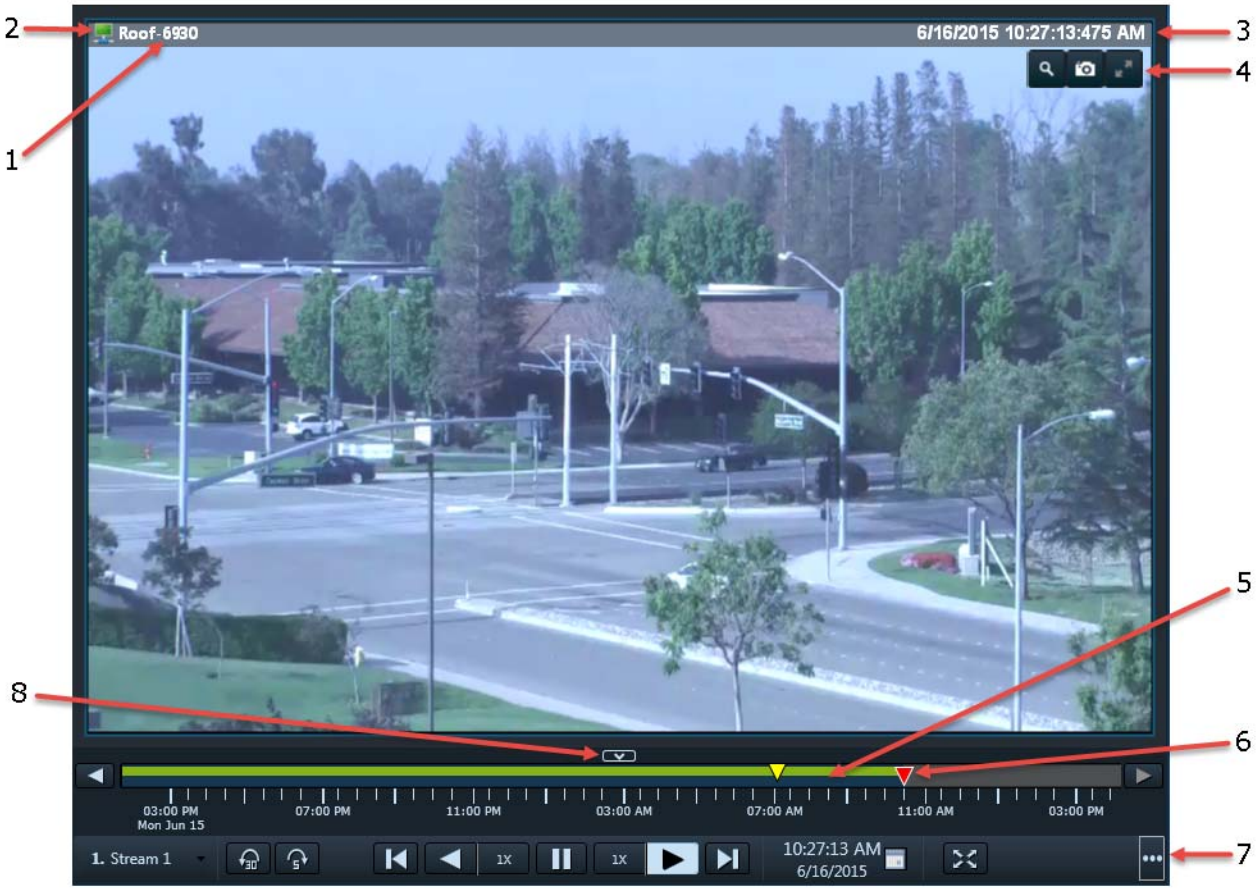
You can view recorded video from a continuous loop, for a motion event, or from a video clip. The camera must be configured to support each of these options, and you must have access to a video viewing application that supports these functions (some applications are for viewing only).

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 are automatically triggered by motion. Video records 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 27 identifies the main recording features and controls.

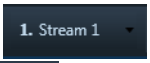
Figure 27 Viewing Recorded Video

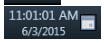


1.	Camera Name—Source of the recorded video.
2.	Indicates the video quality, which can be affected by network and system performance. The icon turns red if the video quality is poor . **Note:** This icon is for informational purposes only when displayed with recorded video. Smooth Video options do not apply.
3.	Timestamp for the currently displayed video image. For example: 6/1/2015 1:14:55:103 PM. **Note:** Changes to Live when live video displays.

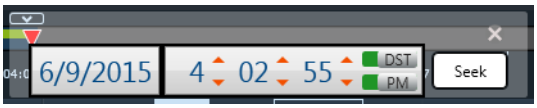
4.	Control icons. See Figure 26 on page 80 for more information. **Notes** • The PTZ icons are enabled only for live video. • The PTZ icons appear on the pane during some operations (for example, Skip), especially in Sync mode. This is expected behavior. Even when a recording exists, SASD assumes the play head is in a gap until the first frame of video. • Set your monitor *color* setting to 32-bit. The control bar and audio icon cannot display if your workstation monitor is set to 16-bit color setting.
5.	Timeline—Displays available video recordings over a time span. • The green bar represents available recorded video for the time duration. • The displayed timeline is associated with the active video pane and the selected video stream. If no recorded video exists for the selected stream, the entire timeline is gray. • Gaps in the recorded video are indicated by gaps in the green bar. Recording gaps exist any time there is no data present during a period in the recording. This can be for a variety of reasons, including On-Demand Recording in which the recording on that stream is triggered manually and may therefore be non-continuous, if recording was stopped manually or by a schedule, or if video was unavailable due to network connectivity issues, device malfunctions, or other events. • Click ◀ or ▶ next to the timeline to scroll the timeline to the left or right. • Click ▼ to move the timeline so that the play head is in center. • You can change the displayed time span and time range selection mode, and you can seek to a specific time in the range of recorded video to begin playing (see below).
6.	Play head—Indicates the point on the timeline where the video plays. • Click on a point in the timeline or drag the red play head to play video from the selected time. • If you drag the play head after the available recorded video, the displayed video changes to live video.

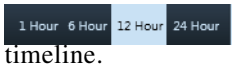
7. Live and recorded video control bar. Click to show all the icons in the control bar.

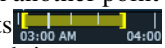
- 

—Selects the live and recorded video streams (primary or secondary) supported by the camera.
- **Sync all panes**—Controls the playback in multiple video panes. See the Synchronizing Video Playback in Multiple Panes, page 102.
- **Step Back**—Pauses the playback and steps back one frame at a time.
- **Play Reverse**—Plays the video in reverse at the currently selected speed.
Click the drop-down menu to select the playback speed. For example, you can play the video slower or faster than the normal rate (forward or reverse). Selecting the speed causes playback to begin at the displayed playback speed of the associated button. SASD maintains independent playback speeds for each direction.
- **Pause**—Pauses the video playback.
- **Play Forward**—Plays the video forward at the currently selected speed. Click the drop-down menu to select the playback speed. For example, you can play the video slower or faster than the normal rate (forward or reverse). Selecting the speed causes playback to begin at the displayed playback speed of the associated button. SASD maintains independent playback speeds for each direction.
- **Step Forward**—Pauses the playback and steps forward one frame at a time.
- **Skip Back**—Skips back 30 seconds.
- **Skip Forward**—Skips forward 5 seconds.
- 

Seek To—Click the calendar icon to display a selector for the start of the video playback.



The red play head moves to the specified time on the timeline.
- 

Change Displayed Timespan—Selects the time unit (1, 6, 12, or 24 hours) displayed on the timeline.
- **Switch Between Live and Recording**—Switches between live and recorded video.
indicates live video. Click to switch to the recorded view.
- **PTZ Presets** (Live video only)—Opens the PTZ preset list that allows you to quickly adjust the camera view.
- **Composite Snapshot**—Saves a snapshot of multiple video panes (*including* control icons, timestamps and other information) in BMP, JPEG, PNG, or TIFF format.
- **Toggle Time-Range Selection Mode**—Selects a range of time on the timeline. Click a point on the timeline for the start of the range, and then click another point to mark the end of the range. Time ranges are shown on the timeline as a yellow bar between brackets 

. You can click the down arrow to display a date and time selector to fine-tune the range start and end times.

Note: The time fields in the selector flash red if you select an invalid time, such as a start time later than the end time or a time outside of the recording.

- —**Clear Time-Range Selection**. Clears the selected time range.
- —**Create Clip**. Saves the selected video clip as a file for download and playback. See Creating and Viewing Video Clips, page 87.

- **Toggle Repeat Segment Mode**—Plays a video segment continuously in a loop. See Creating a Repeat Segment, page 94.
- **Toggle On-Demand Recording**—Begins recording immediately. See Using On-Demand Recording, page 95.
- **Enable FullScreen Mode**—Enlarges the video image to fill the entire monitor screen. To exit, press Esc.
- **Toggle Audio**—Enables or mutes the audio. Click the down arrow to adjust the volume and balance settings.

Note: When viewing video in multiple panes, each pane has a quick-access control bar with icons to play the video, pause, and switch between live and recorded video. When viewing video in a single pane, all playback controls are in the control bar at the bottom of the application window.

8. —Hides the timeline and the control bar. Click to show the timeline and control bar again.

Usage Notes

- You can view up to 48 video streams simultaneously per workstation.
- Multi-pane video clips (only CVA and only in Sync mode) can be saved to your desktop and played using the Cisco Video Surveillance Review Player.
- If a camera is *soft-deleted* , you can still access its recorded video but cannot display live video. Recordings are retained on the system until removed according to the Camera Recording Retention settings in the Operations Manager.
- 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.
- SASD automatically adjusts the default time span based on recording length. For example, when you drag a camera onto the viewing pane and the archive is less than 1 hour, SASD selects a granularity of 1 hour for the timeline. If the archive is less than 6 hours, SASD selects a granularity of 6 hours, and so on.
- Rendered gaps in video data may be imperceptible when the given granularity and window size would result in a gap of less than one pixel. The following are general guidelines for whether gaps are shown, with the window size at 800 pixels for the pane containing the timeline (the locations/camera panel collapsed):
  - One-hour granularity—Gaps less than 5 seconds may not be shown
  - 6-hour granularity—Gaps less than 30 seconds may not be shown
  - 12-hour granularity—Gaps less than 60 seconds may not be shown
  - 24-hour granularity—Gaps less than 90 seconds may not be shown
  - One-week granularity (Statistics mode in Event Recording Window)—Gaps less than 700 seconds may not be shown

  Note that there are other factors such as how the framework renders across pixels that affect whether very small gaps appear.
- If Smart Stream Selection is configured for the camera, only the recorded video from stream A is retained when an event occurs.

Calling a Video or Voice Phone

Click the phone icon in Cisco SASD to call a person or location when viewing video.

Procedure

Step 1 Launch your IP video or voice client, such as Cisco Jabber, or Skype.

Step 2 Click the phone icon.

Step 3 Follow the on screen prompts to complete the connection to the configured person or location.

Note The client and call recipient are defined by your administrator.

Creating and Viewing Video Clips

You can create video clips 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, page 88 for the clip formats supported by each application in this release.

Refer to the following topics for more information:

- Clipping Support By Application, page 88
- Supported File Formats And Playback Options, page 88
- Creating Video Clips, page 90
- Downloading and Viewing Clips, page 93

Tips:

- You can 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 third-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 of the Operations Manager must be yellow).

Clipping Support By Application

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

Table 15 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[5]	Yes[6]	Yes	No	Yes	Yes
Cisco SASD Federator	Yes	Yes	Yes[7]	Yes	No	Yes	Yes
Cisco VSM Review Player	No	No	No	Yes	Yes[8]	No	No

1. MP4 clips are saved to the Media Server and play immediately after being downloaded to the monitoring PC. Third-party video players (such as VLC media player™) 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 launch the player.
5. SASD allows CVA clipping for multi-pane in Sync Mode only.
6. Thumbnail Search supports MP4 clip creation only.
7. Thumbnail Search supports MP4 clip creation only.
8. Cisco video archive (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

You can create video clips in multiple formats:

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

Table 16 describes the video clip options:

Table 16 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, you can create virtual clips using the Operations Manager, Cisco SASD, and Cisco SASD Federator but not Cisco VSM Federator. See the Clipping Support By Application, page 88. • Virtual clips can be any length. There is no maximum duration for a virtual clip. • Virtual clips support audio in Cisco VSM 7.8 and higher. • You can save a virtual clip as an MP4 file for download (note that the 10-hour MP4 limitation applies).
MP4	Save MP4 clips on the Media Server and download them 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 playable on most computers and useful for sending in email or saving to a local server. **Notes** • In this release, you can create MP4 clips using the Operations Manager, Cisco SASD and Cisco SASD Federator. To create MP4 clips using the Cisco VSM Federator, use the Clip Search and Clip Management features. See the Clipping Support By Application, page 88. • MP4 clips play automatically in the pane when downloaded. Use the Cisco VSM Review Player or VLC media player to view clips. • Use the **Clip Search** feature to view, download, and delete MP4 clips saved on the Media Server. • The maximum duration for an MP4 clip is 10 hours. • MP4 clips require that the clipping repository be selected on the Media Server associated with the camera. See “Configuring Media Server Services” in *Cisco Video Surveillance Operations Manager User Guide*. • MP4 clips are saved on the Media Server for 7 days and are then automatically deleted. To download clips to a local drive, use the **Get Clips Status** menu (see also the Downloading and Viewing Clips, page 93). • Up to five MP4 clips can be created at a time per Media Server. If the limit is reached, wait for clip recording 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 the clips of other users. • 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.

Table 16 Video Clip File Formats (continued)

File Format	Description
CVA	A Cisco video archive (CVA) can include multiple video panes that synchronize to the same time. CVA files can only be opened in applications that support the CVA format (such as the Cisco Review Player). **Notes** • CVA clips download immediately and are not stored on the server. • The maximum duration for a CVA clip is 24 hours. • CVA files support audio playback in Cisco VSM 7.9 and higher, when configured on the camera. Users can click the audio icon in each frame during playback with the Cisco VSM Review Player. • You must display multiple video panes and use Sync mode to create a CVA clip using Cisco SASD. • The 64-bit version of the Cisco Review Player is required to play files with more than 4 video panes. See the Cisco Video Surveillance Review Player User Guide for more information.
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 clips download immediately and are not stored on the server. • CVX video playback shuts down if the file is tampered with. • CVX files do not support audio.

Tip: You can also click the camera icon in the upper right of a video pane to save a still image in BMP, JPEG, PNG, and TIFF formats. See the Viewing Live Video, page 80 for more information.

Creating Video Clips

Requirements

You must meet the following requirements to create video clips:

- 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.

Notes

- Review the Clipping Support By Application, page 88 for information on the clip formats supported by each application in this release.
- Video clips (such as virtual clips and MP4 clips) can be created from merged streams. If the codec changes during the clip segment, only virtual clips can be created. In the Operations Manager, codec changes are indicated by a small red triangle on the timeline. The triangle is not displayed in Cisco SASD. See “Smart Stream Selection” in the Cisco Video Surveillance Operations Manager User Guide for more information.

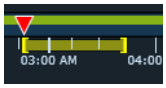
Procedure

To create a video clip, select the clip format and specify the start and end times for the clip:

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

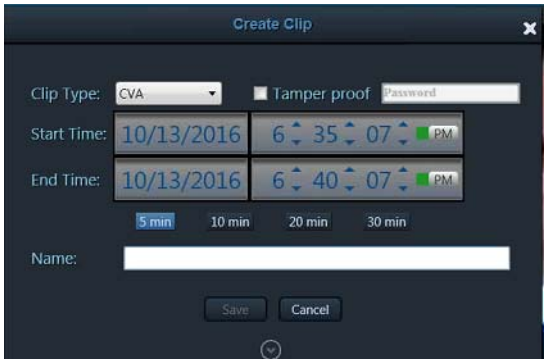
Tip: To create a multi-pane clip in the CVA format, click **Sync all panes** to select multiple concurrent panes.

Step 2 (Optional) To create a range for the clip on the timeline, click **Toggle Time-Range Selection Mode** and click the start and end points for the range. A time range is shown on the timeline as a yellow bar between brackets:



Step 3 Click **Create Clip** and select the Clip Type: MP4, CVA, or virtual clip (Figure 28).

Figure 28 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 (Optional, CVA clip type only) Select **Tamper proof** and enter a password to create a password-protected CVX file.

Step 5 (Optional) Revise the start and end date and time (Figure 28). 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).

- If you created a time range in Step 2, those start and end times are displayed.
- The clip start time defaults to the time indicated by the red play head on the timeline. If the play head is at the end of the recording, the default start time for the clip is 5 minutes before the end of the recording.

Step 6 (Optional) Select a duration from 5 to 30 minutes to enter a specific length of time for the clip.

The duration begins from the selected start time.

Step 7 (Optional) Click the expander button to display thumbnails of the clip start and end frames and to fine-tune the duration of the clip.

Step 8 Enter a clip name and click **Save**.

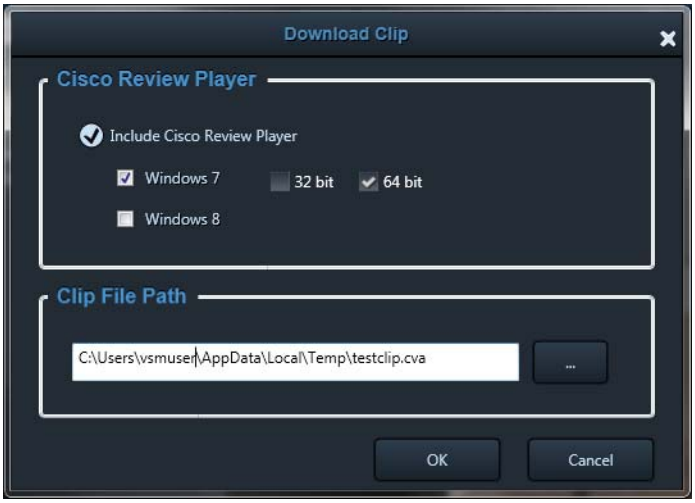
CVA/CVX Files

a. (Optional) Select whether to include Cisco Review Player with the CVA/CVX file, and then select one or more operating systems.

A Cisco Review Player will be included for each operating system that you select.

b. Select a location on a local disk and click **OK**.

Figure 29 Download Clip



c. Wait for the clip to be generated and downloaded to the local system.
   - Video streaming is paused during CVA/CVX clip generation.
   - You can still select the + Map or + Alert to create a new workspace.

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

MP4 Clips

a. Wait for the clip to be generated on the server.

   Tips:
   - Click the down arrow next to **Create Clip** to check the clip status. If the clip name is green with a check mark, the clip creation is successful (Figure 30). Yellow indicates that the clip creation is in progress, and red indicates that the clip creation failed.
   - You can also select **Management > Clip Management**, **MP4** tab 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.

b. Download and play the clip as described in the Downloading and Viewing Clips, page 93.

Virtual clips

a. Wait for the clip to be generated on the server.

   Tips:
   - Click the down arrow next to Create Clip to check the clip status. If the clip name is green with a check mark, the clip creation is successful. Yellow indicates that the clip creation is in progress, and red indicates that the clip creation failed.
   - Select **Management > Clip Management**, the **Virtual** tab to view the current status: In-Progress, Completed, or Failed. Use the **Clip Search** option to view, download, delete, and manage Virtual clips saved on the server.

b. Download and play the clip as described in the Downloading and Viewing Clips, page 93.

Downloading and Viewing Clips

Table 17 lists the ways that you can access and play video clip formats.

Tip: See Clipping Support By Application, page 88 for the file formats supported by each Cisco monitoring application in this release.

Note: You can select clips created using Cisco SASD Federator from the Cisco SASD main window (using the **Create Clip** pull down menu). However, clips that you create using Cisco SASD are not available for selection from the Cisco SASD Federator main window (using the **Create Clip** pull down menu).

Table 17 Video Clip Download Options

Clip Format	Download Options
CVA clips	Downloads when created. Play CVA clips using a supported video player such as the Cisco Review Player. You can download Cisco Review Player with the clip. • The 64-bit version of the Cisco Review Player is required to play files with more than 4 video panes. See the Cisco Video Surveillance Review Player User Guide for more information.
MP4 Clips	After you create the clip, you can download and save the file to a local disk. The clip remains on the server for 7 days. • 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 download Cisco Review Player with the clip. • 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. See Clip Management, page 133 for more information.
Virtual Clips	Click the down arrow next to Create Clip . Select the clip name from the list to play the clip in the video pane. You can also search for virtual clips using the **Clip Search** feature in Operations Manager or the **Clip Management** feature in Cisco SASD, and save the virtual clip as an MP4 file for download. See Clip Management, page 133 for more information.

To download video clips:

Step 1 Click the down arrow next to Create Clip (Figure 30).

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 30 Accessing an MP4 Clip

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

For Virtual Clips, the clip that you select plays in the video pane.

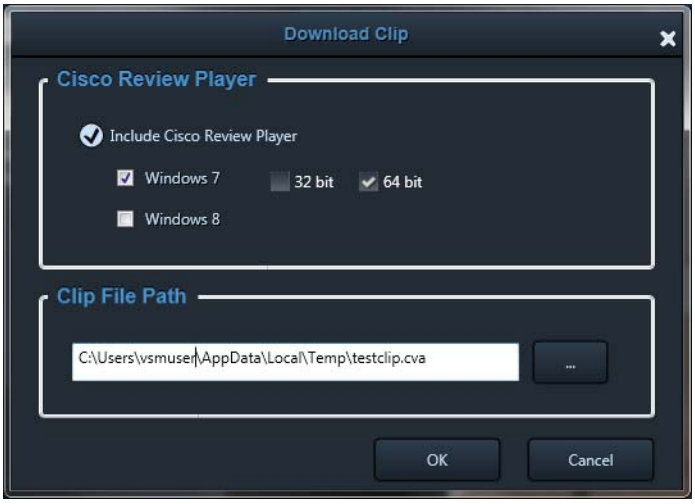
Step 3 (MP4 clips only) In the Download Clip window:

a. Select whether to include Cisco Review Player with the download.

b. Select an operating system if including Cisco Review Player.

c. Enter a file name and location, click **Save**, and wait for the clip to download.

Figure 31 Download Clip



The clip automatically plays in the pane the first time you download it.

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 it.

Note: Repeating segments are used with recordings only.

To create a repeating segment:

Step 1 Click **Toggle Time-Range Selection Mode** to create a video segment to repeat.

- Click a point on the timeline for the start of the range, and then click another point to mark the end of the range. A time range is shown on the timeline as a yellow bar between brackets

.
- Click the down arrow to display a date and time selector to fine-tune the range start and end times.

Step 2 Click **Toggle Repeat Segment Mode** .

Step 3 Click **Play Forward** .

Step 4 To cancel the repeating segment, click **Clear Time-Range Selection** or **Toggle Repeat Segment Mode** .

You can also click anywhere on the timeline outside the selected range.

Using On-Demand Recording

On-Demand Recording allows you to immediately start and stop recording a live video stream.

Usage Notes

- Audio is not recorded.
- Video is recorded for a system-defined length of time, up to a maximum of 3 days.
- The recording is retained on the server according to the camera's Retain event recordings settings in Operations Manager.

  For example, if the retention setting is 30 days, then the On-Demand recordings are also available for 30 days.

  When the retention time expires, the recording is automatically deleted (see the Creating and Viewing Video Clips, page 87 to save the video to a separate file).

You must meet the following requirements to enable On-Demand Recording:

- The On-Demand Recording option must be enabled for the camera configuration in Operations Manager.
- Your user account must include access permissions to view recorded video.
- You can record video from the live primary video stream only.

To immediately begin recording video:

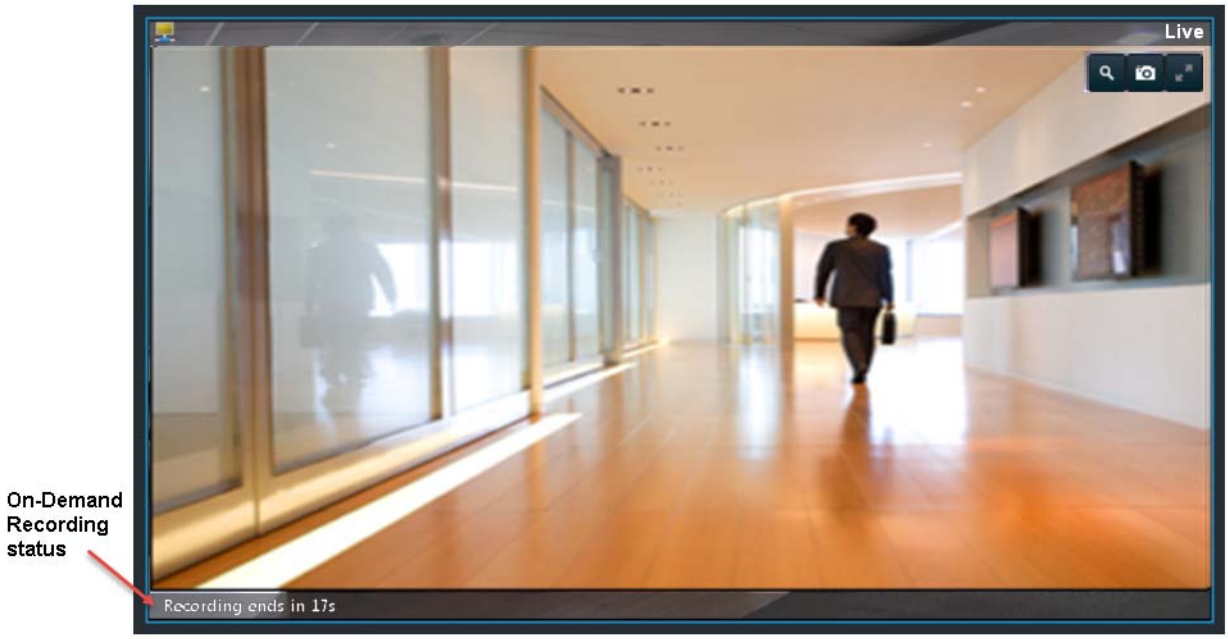
Step 1 Log in to the video viewing application and select a camera.

Step 2 Choose live video (see the Viewing Live Video, page 80).

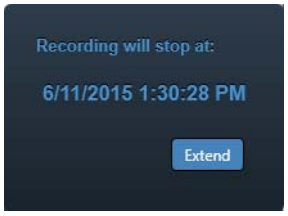
Step 3 Click **Toggle On-Demand Recording** .

- The recording is performed in the background. You can continue to use the other playback controls.
- The recording status (Figure 32) indicates when the recording time is nearly complete.

Figure 32 On-Demand Recording



Step 4 (Optional) To extend the recording time, click the down arrow next to **Toggle On-Demand Recording** , and then click **Extend**.

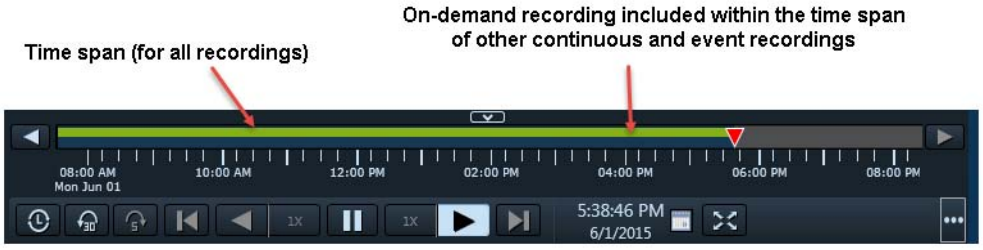


The recording time extends for the amount of time configured in the Operations Manager.

Step 5 To view the recorded video, review the following notes.

- On-Demand Recording clips are available from Stream 1 only.
- Select 1. Stream 1 to view the recorded primary stream (disabled if the pane is synchronized).

  Note: Selecting a long term server (LTS) backup recording may result in an error if the recording is not available or the backup is not complete.
- If the video is within the time span of other recorded video, there is no separate indication of the On-Demand Recording video. You can access the video as described in the Viewing Recorded Video, page 82).



- If the On-Demand Recording video is older than the continuous loop, the gap between the recording times is shown in blue:

Note: When the Camera Recording Retention time expires, the On-Demand Recording is automatically deleted. To save the recording, see the Creating and Viewing Video Clips, page 87.

Using the Privacy Mask

When enabled on a compatible camera, the Privacy Mask blocks all live video and cannot be viewed by an 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 33 shows the icons used to enable or disable the Privacy Mask.

You must meet the following requirements to enable privacy mask:

- You must belong to a User Group with *Control Privacy Mask* access permissions configured in Operations Manager to use this feature.

Figure 33 Privacy Mask Controls

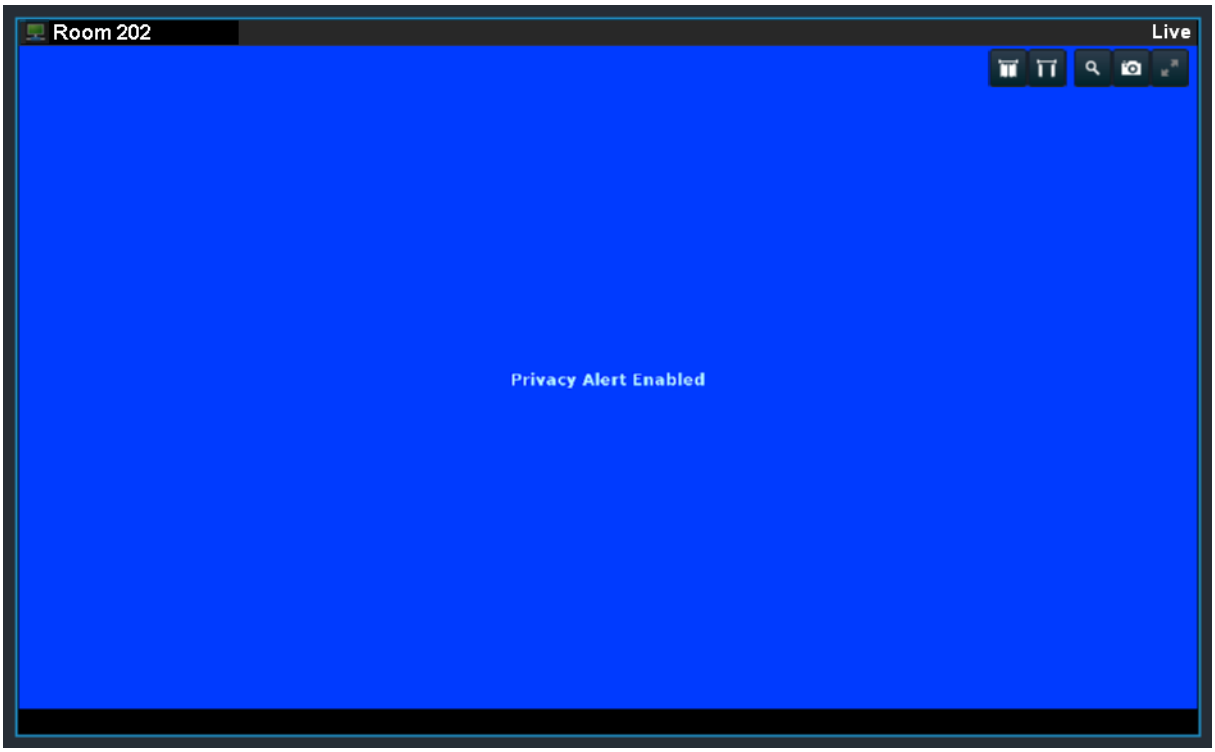
To display the privacy mask:

Step 1 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 entire field of view and display a blank (blue) screen (Figure 34). • 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 34). The same blank (blue) screen is recorded (if recording is configured).

Figure 34 Privacy Mask Enabled



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

Step 2 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 powers up with the Privacy Mask in the pre-reboot state. For example, if the mask was enabled and there was 5 minutes remaining on the timer, the camera remembers the state after the reboot, and displays the blue privacy window.

Related Information

Supported cameras can also be configured with Privacy Zones to 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.

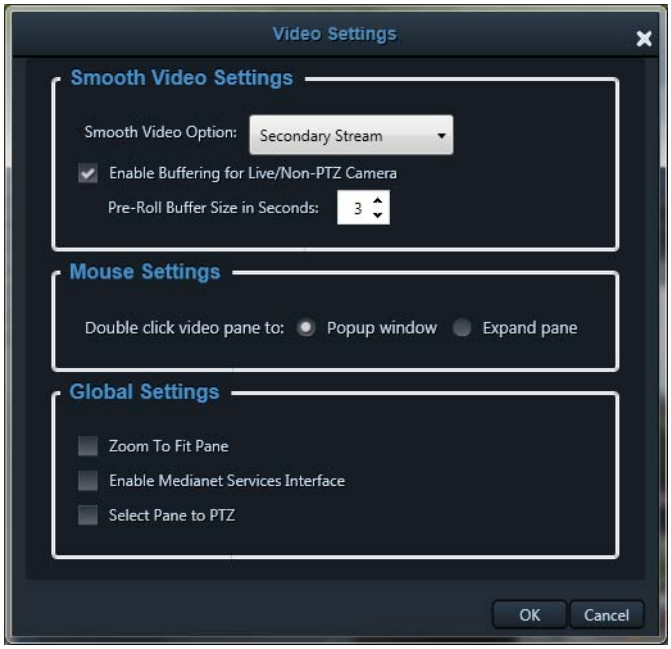
Using the Smooth Video Settings When Viewing Live Video

If live video playback is jittery due to network or other performance issues, use the **Smooth Video Settings** (Figure 35) to automatically do the following:

- Create a video data buffer (in seconds) that delays live playback while video data caches.

  Live video can then be played back smoothly despite network delays between the camera, Media Server, and workstation.
- Automatically switch to a different stream or use I-frames only if the live video quality is poor.

Figure 35 Smooth Video Settings



Icon Colors

The video quality icons in each pane indicate the following:

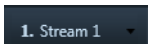
- Green indicates video is performing as expected.
- Yellow indicates that the client workstation has detected that playback is not smooth.
- Red indicates a severe adverse situation. Action will be taken to correct the situation such as switching to secondary stream or I-frame streaming.

Icon Cable Colors

- A blue cable (or) indicates that the primary stream is being used.
- A red cable indicates that the secondary or I-frame stream is being used.

Usage Notes

- The Smooth Video Option is available only for live video (all cameras).
- Buffering applies to live video only and to non-PTZ cameras only.
- When **Enable Buffering for Live/Non-PTZ Camera** is selected, "Buffering..." appears in the video pane while video is delayed for the number of seconds defined in **Pre-Roll Buffer Size in Seconds**.
- The settings are applied to all cameras (buffering is applied to all non-PTZ cameras) and are persistent for the current PC workstation.

  For example, the settings remain if you log out and back in, or view a different camera and then return to the current camera.
- The Smooth Video options are disabled if you manually select a stream (click 

in the control bar).
  - The pane displays the selected stream even if the video quality is poor (the video does *not* automatically switch to the Smooth Video alternate stream).
  - To cancel the manually selected stream and re-enable the Smooth Video Settings, reload the view or drag the camera onto the pane again.
- The Smooth Video option is disabled if you choose a video stream from a redundant media server (the camera will not use a secondary stream even if the video quality icon is red).

To enable smooth video:

Step 1 Select **Settings > Video** to display the Video Settings window.

Step 2 In the **Smooth Video Settings** pane, select the **Enable Buffering for Live/Non-PTZ Camera** check box to enable to enable pre-roll buffering.

Step 3 (Optional) Enter a value for **Pre-Roll Buffer Size in Seconds** to define the number of seconds for live video to delay until recording begins.

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 **Pre-Roll Buffer Size in Seconds** be disabled (= **0**) because streaming delays can cause a potential security risk. It is a better practice to address the network bandwidth or performance issues that are causing the delays. Use **Pre-Roll Buffer Size in Seconds** only when significant jitter occurs and a network resolution is not available.

Step 4 Use the **Smooth Video Settings** to define an alternate video stream to use 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 , automatically switch to the secondary video stream. 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 display only I-frame video. I-frame video reduces the bandwidth requirement to correct the situation.

- **None**—If the live video quality is poor , make no change and display the selected stream even if it results in jittery or paused playback.

  Notes

  – These options are not used if the video quality is *acceptable* or if the icon is yellow (*intermediate*) . The selected stream displays.

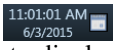
  – A red cable displays when the secondary or I-frame stream is applied.

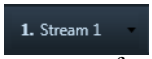
  – If an alternate stream is applied, the settings remain until you close and reopen the video source (camera).

Synchronizing Video Playback in Multiple Panes

To synchronize video playback from multiple panes, click the pane to make it active, and then click **Sync all panes** . All panes become active with a blue border and 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.
- Up to 9 panes can be synchronized (such as a 3x3 layout). The synchronization option is disabled for 4x4 and 5x5 views.
- Synchronization for recorded video is performed only if the time in the selected panes overlaps. If the time for a video pane does not overlap with the master pane, the pane is excluded from synchronization, as indicated by this icon .
- When you move the play head on the timeline or use **Seek To** 

when panes are synchronized, the synchronized panes pause, and then continue to display video from the selected date and time.
- You can switch the synchronized panes between live and recorded video.
- Stream selection 

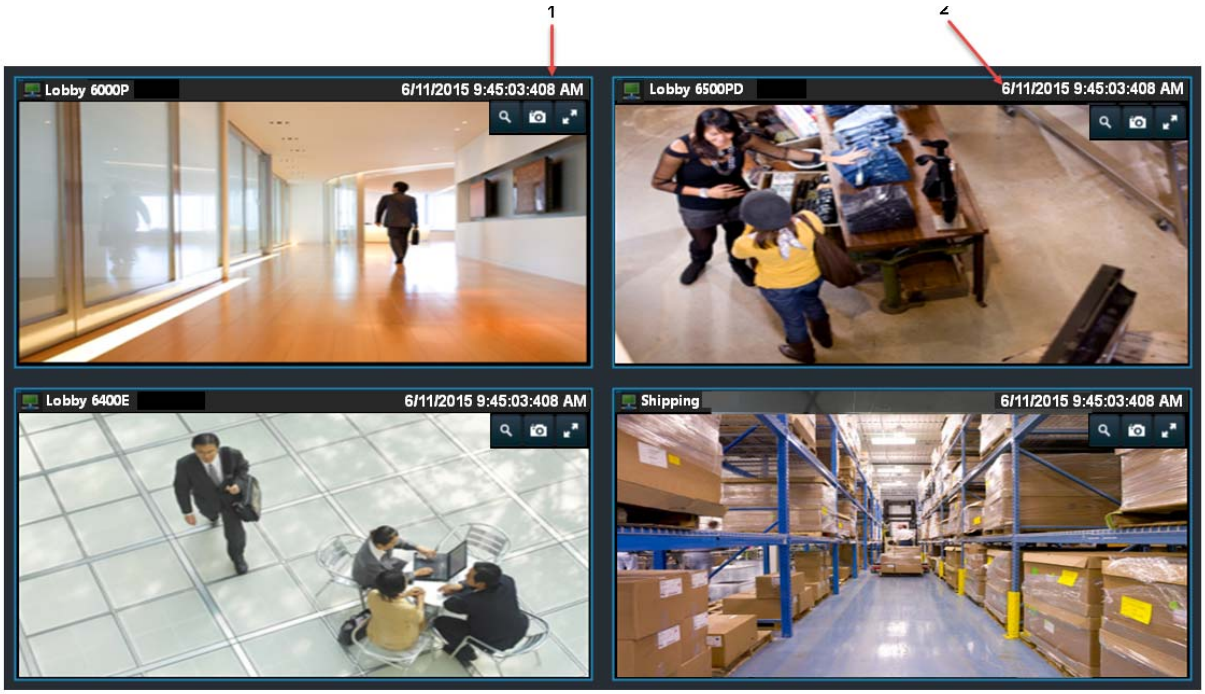
is not available when panes are synchronized.
- If the live secondary stream for a camera is in Sync mode, and only the camera's primary stream is configured to record, toggling from live to recorded streams while in Sync mode will cause the pane to switch from the live secondary stream to the recorded primary stream.
- **Sync all panes** does not show if the view or layout only has one pane.
- **Sync all panes** is disabled if:
  – no panes have video or only one pane has video (either live or recorded video).
  – a camera is rotating.
- When 16 video panes are synchronized, some live video panes may not appear as synchronized when the video stream is configured with the following:

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

- The icon appears briefly on the pane during some operations (for example, Skip Back), especially in Sync mode. This is expected behavior. Even when a recording exists, SASD assumes the play head is in a gap until the first frame of video.
- In Sync mode, if you play video faster than 4X, you may observe a time difference between panes of up to five seconds under certain circumstances. This is a result of a large group of pictures (GOP) size difference between streams, most likely involving the Arecont camera.

Figure 36 describes the main synchronization attributes.

Figure 36 Synchronized Playback of Recorded Video



1	The recorded video time in this pane does not overlap with the recorded video in the other panes.
2	The timestamp for synchronized video is the same.
3	Synchronized panes all have a blue border (all are active). Actions that you perform using the timeline and control bar affect all panes.
	Pattern on green bar—One or more cameras have no video available for the time shown (partial data).

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

Step 1 Select a layout and add cameras to the view or select a predefined view from the **View** menu.

Up to 9 panes can be synchronized (such as a 3x3 layout). The synchronization option is disabled for 4x4 and 5x5 views.

Step 2 Click **Sync all panes** .

All panes become synchronized and have a blue border.

Step 3 (Optional) To make changes to the synchronized group, perform steps 1 and 2 again.

Using the Pan-Tilt-Zoom (PTZ) Controls

Cameras that support pan-tilt-zoom (PTZ) movements display PTZ icons . Click **Toggle PTZ mode** 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:
  - Use the zoom control.
  - Hold down the Shift key and then press the left mouse button. Drag the mouse up or down to zoom.

Click **Toggle PTZ to region** to select part of the full image and perform the PTZ controls within that region.

PTZ presets allow the camera to quickly jump to preset positions. 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. The tour resumes after a set amount of time. See your system administrator for more information.

You must meet the following requirements to use the PTZ features:

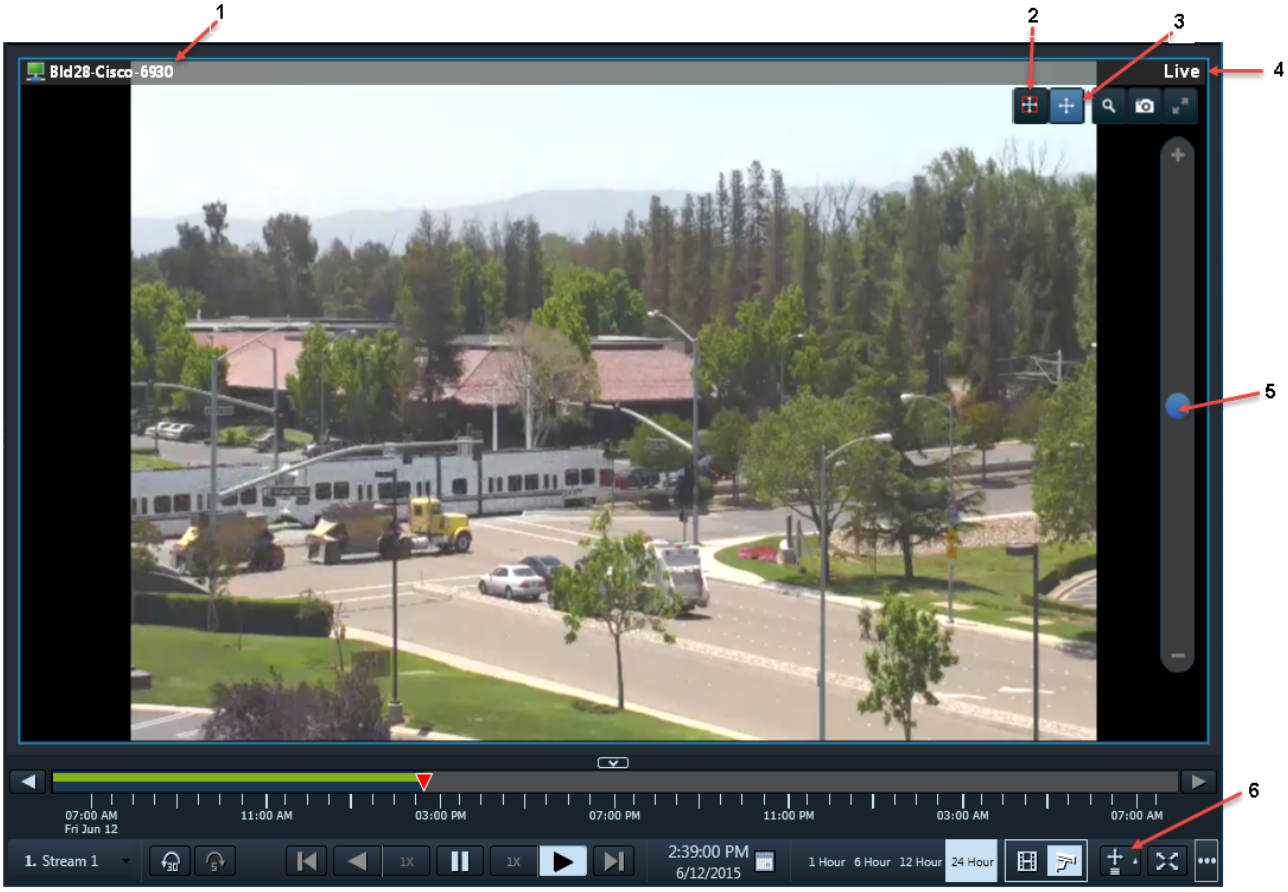
- You must belong to a user group with *Perform PTZ* permissions.

Usage Notes

- To use a USB joystick, see Calibrating a Joystick for Windows 7, page 107.
- PTZ movements are available only when viewing live video.
- When viewing multiple panes, you can only enable PTZ in a single video pane. See Using PTZ Controls with Multiple Video Windows, page 108.
- PTZ commands are only available if the primary Media Server is functional. If the primary Media Server goes down or is not available on the network, PTZ commands do not function even if video is still being delivered by a redundant server. See the *Cisco Video Surveillance Operations Manager User Guide* for more information.
- If a higher-priority user is using the PTZ controls, they remain locked, and you cannot control the PTZ movements until released by the higher-priority user.

Figure 37 summarizes the controls and information available on each PTZ camera viewing pane.

Figure 37 Camera PTZ Controls



1	Selected camera.	**4**	PTZ is available in Live mode only.
2	Toggle PTZ to region.	**5**	Zoom control
3	PTZ Enabled/Disabled (click to toggle) • Blue—Enabled • Black—Disabled	**6**	PTZ Presets menu

To control the PTZ movements of a camera or trigger a PTZ preset position:

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

Step 2 Click to enable PTZ or PTZ to region:

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

Step 3 (PTZ to region only) Hold the left mouse button while dragging the mouse to frame the image area, then release the mouse to pan, tilt and zoom to the selected rectangle. To zoom all the way out, click without moving the mouse.

Step 4 To move the camera position, use the following controls.

Using a Mouse

- Pan and Tilt—Press the left mouse button while dragging the mouse ( ) right, left, up and down.
- Zoom
  - Click and drag the blue slider on the zoom control at the right of the video pane. Drag up to zoom in and down to zoom out. The distance from the center controls the zoom speed. Releasing the slider stops the zoom at the current level. (The '+' and '-' are not active buttons, they are for information only.)
  - Shift-click in the video pane, and drag the mouse 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, page 107 when setting up the USB joystick for the first time.

Step 5 (Optional) Select a PTZ preset position.

Using a Mouse

- Click **PTZ Presets** .
- 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, and so on.

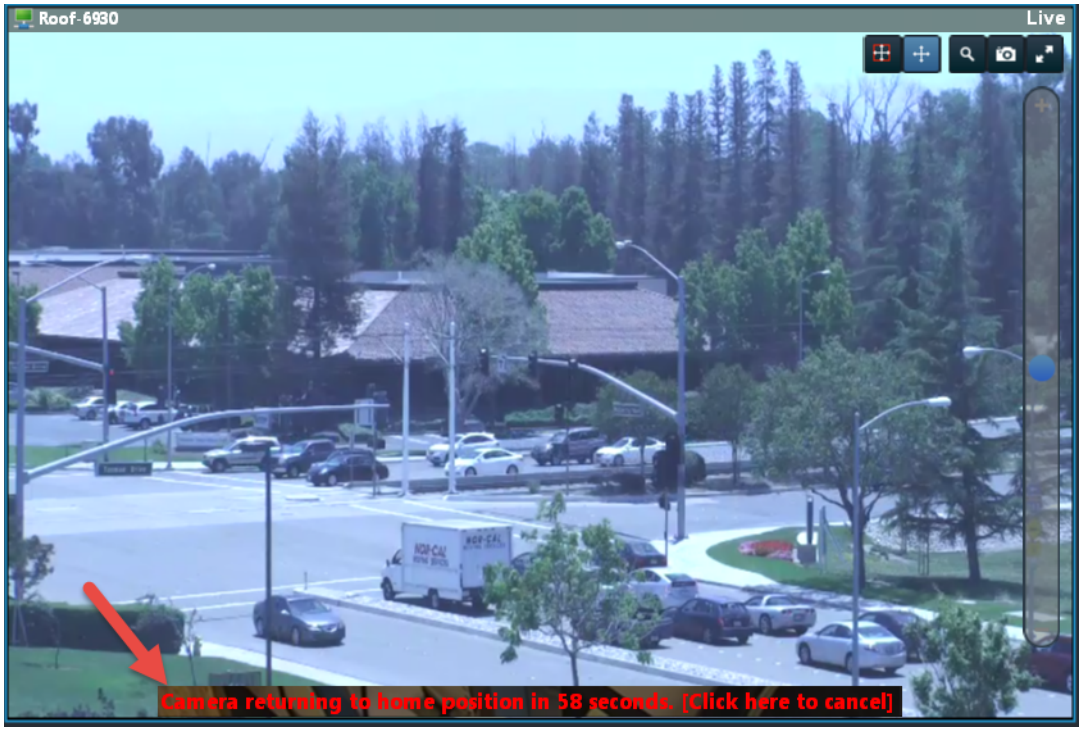
Tip: If Return to Home is configured, the camera will return to a default “home” PTZ location after a specific number of seconds. See Understanding Return To Home, page 107.

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 38):

Figure 38 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.

To calibrate a USB joystick:

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.

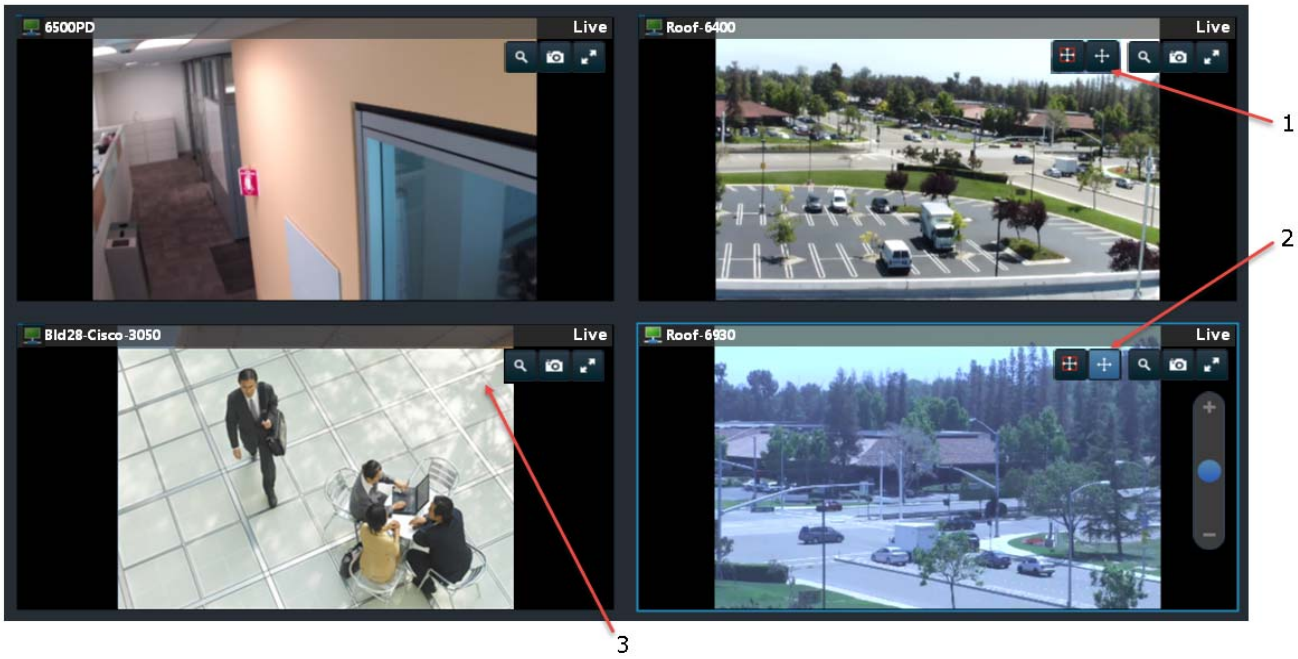
Step 3 Click **Finish** or **OK** to close the windows.

Using PTZ Controls with Multiple Video Windows

When viewing multiple video panes, only a single pane can have PTZ controls enabled at a time (Figure 39). 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).
- When a pane does not display an icon, the camera does not support PTZ movements.
- PTZ movements are only available when viewing live video.

Figure 39 PTZ Controls in a Multi-Pane View



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

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

Using 360° Camera Controls

The Cisco VSM Operations Manager and the Cisco SASD support 360° cameras. You use 360° camera views to monitor different regions in the field of view (see "Creating Video Views" in *Cisco Video Surveillance Operations Manager User Guide*). You can set the Video Wall to a multiple pane view from one 360° camera.

Some features are model-specific. See the release notes for supported cameras.

Notes

- The Cisco SASD Investigation tools cannot run on 360° camera footage.
- You must mount 360° cameras perfectly flat, on either a vertical or horizontal surface. For example, do not install the camera on a cathedral ceiling.

Orientation

Orientation options reflect camera mounting.

Note: Cameras must be mounted perfectly flat, on either a vertical or horizontal surface.

- Ceiling
- Wall
  - Dual Panoramic Dewarp mode is not available.
  - In Single Region Dewarp mode, image rotation is not available.
- Table

Note: You cannot modify orientation once video recording begins.

Dewarp Mode

A 360° camera image is not a typical, flat image. The image is round and distorted, which is the result of capturing an ultra-wide field of view. You can use Dewarp modes to flatten or *dewarp* the image to make it accessible to the operator.

Figure 40 Dewarp Mode Drop-Down Menu

Dewarp mode varies by orientation. For example, Double Panoramic View is available in Ceiling and Table orientations, but not for Wall orientations.

Note: PTZ operation is not available in either panoramic Dewarp mode. Digital PTZ is available in individual regions.

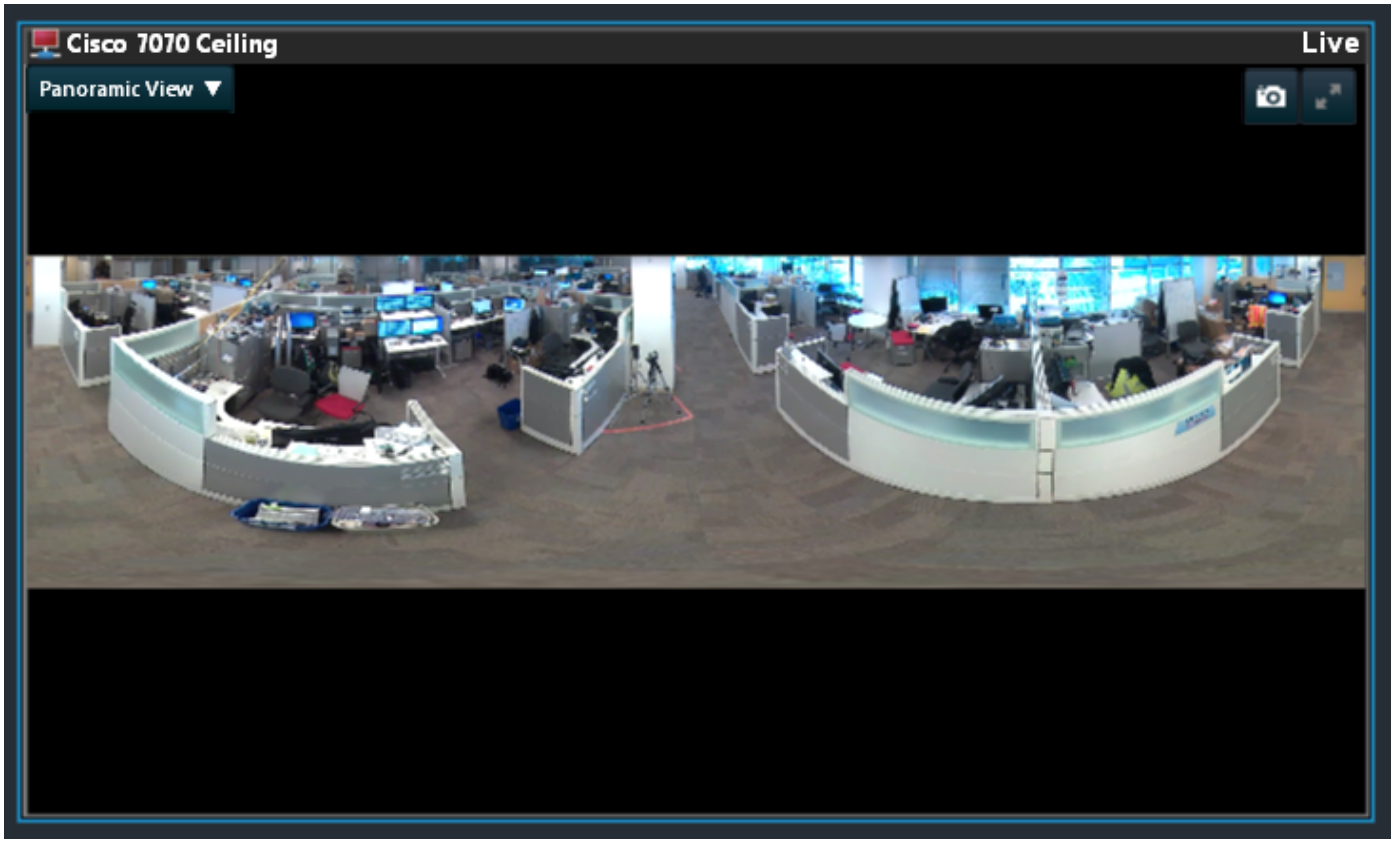
Views vary in the recorded video formats:

- **MP4:** When viewing an MP4 clip, recorded video always appears in Original mode.
- **CVA:** When viewing a CVA clip, recorded video appears as it did on the screen when the clip was created.

Use the different Dewarp modes to set the view to a grid layout of different regions of the 360° image:

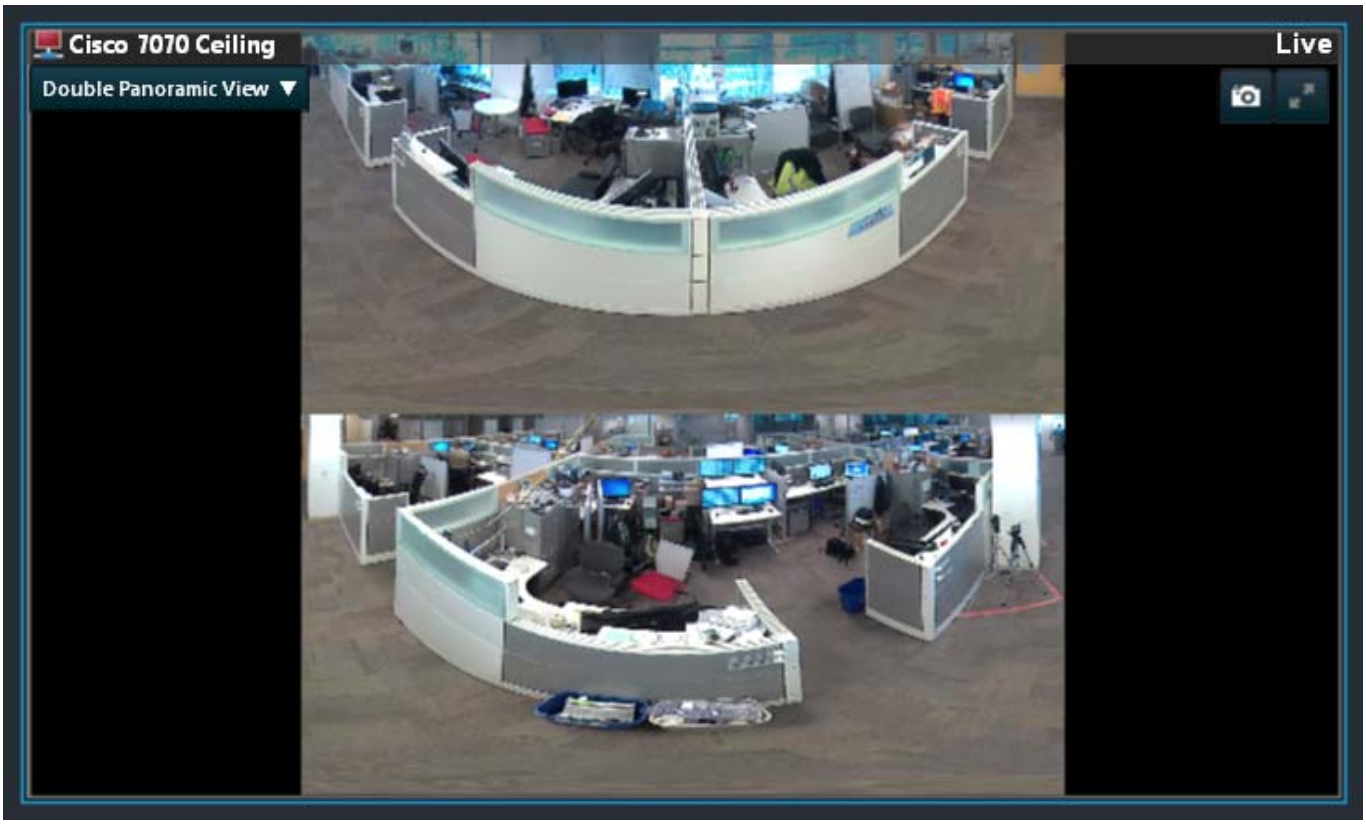
- Original View–Single-pane view without dewarping.
- Panoramic View–Single-pane view with dewarping (Figure 41). The image is divided down the center, with the left and right sides flattened and joined from the top-center location.

Figure 41 Ceiling Orientation Camera in Panoramic View



- Double Panoramic View (Ceiling and Table orientations only)–Single-pane view that splits the Panoramic view down the center, top-to-bottom, and creates a stacked view (Figure 42).

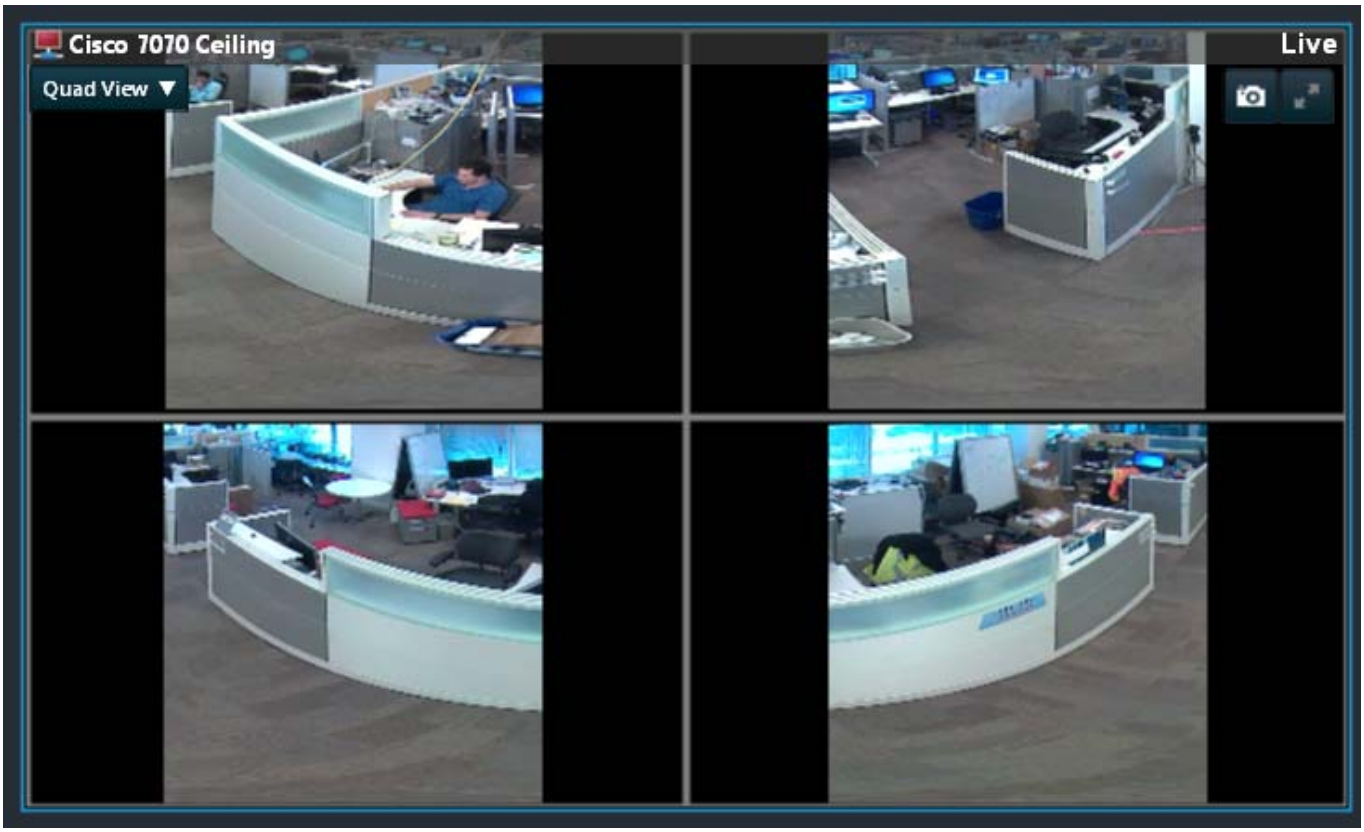
Figure 42 Ceiling Orientation Camera in Double Panoramic View



- Quad View–Single-pane view that splits the Panoramic View into four quadrants (Figure 43).

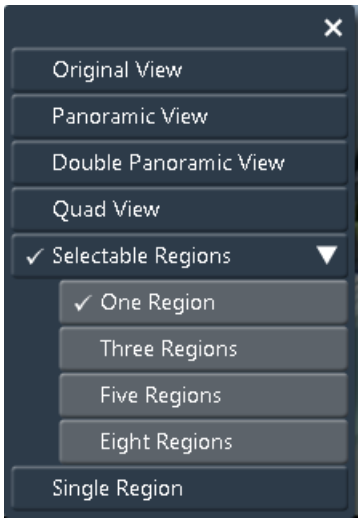
  Note: In individual panes, PTZ features are available in Quad View. You can move the image region and zoom in on a region. Use the mouse wheel to zoom and the left mouse button to drag the view to a new region.

Figure 43 Ceiling Orientation Camera Quad View



- Selectable Regions–This single-pane view allows you to select up to 8 regions in the Original View to display in a grid layout (Figure 44). These regions are not dewarped, but are rotated and zoomed for viewing.

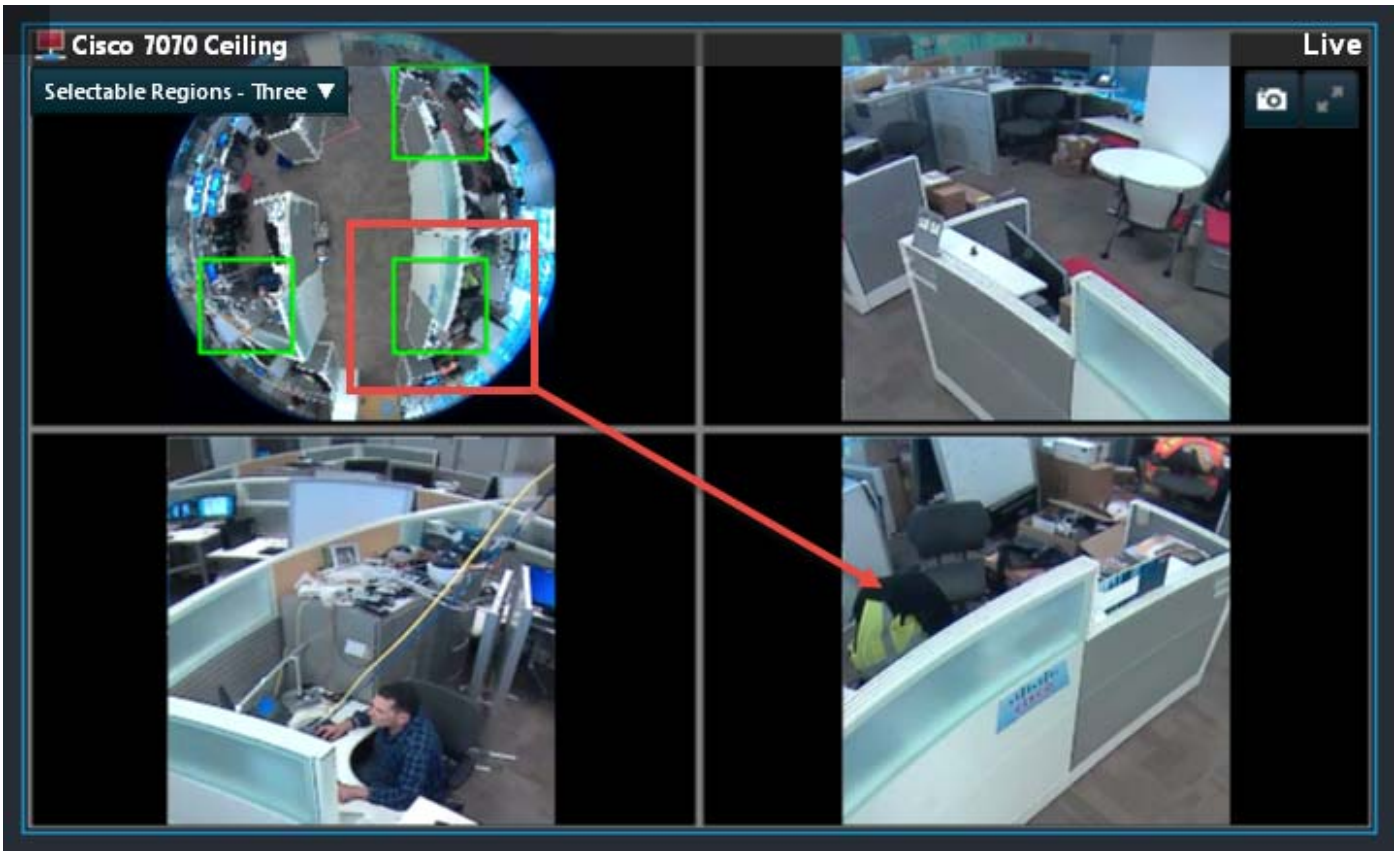
Figure 44 Selectable Regions Menu



Selectable regions appear as individual green squares that you can select and drag to the desired region to display in the grid. The selected region is outlined in red in Figure 45, and appears zoomed and rotated in the grid layout.

Note: PTZ controls are not available in these regions. What appears in the grid cannot be zoomed any further.

Figure 45 Three Selectable Regions



- Single Region–This single-pane view narrows the field of view (Figure 46). Left-click your mouse and drag the desired region into view. Use the mouse wheel to zoom. If panning is set in the Operations Manager, as the view pans operators can pause to focus on one region or left-click the mouse to drag to the desired region.

  Figure 46 shows a Single Region view, zoomed in to floor level.

Figure 46 Ceiling Orientation Camera Single Region View

Event Recording Analysis

Event recording analysis allows you to analyze recorded video based on events. You can select an event that you want to analyze from the configured event types, and then jump from one event to the next while playing video. This feature allows you to quickly find and view all the events of a given type in a video recording.

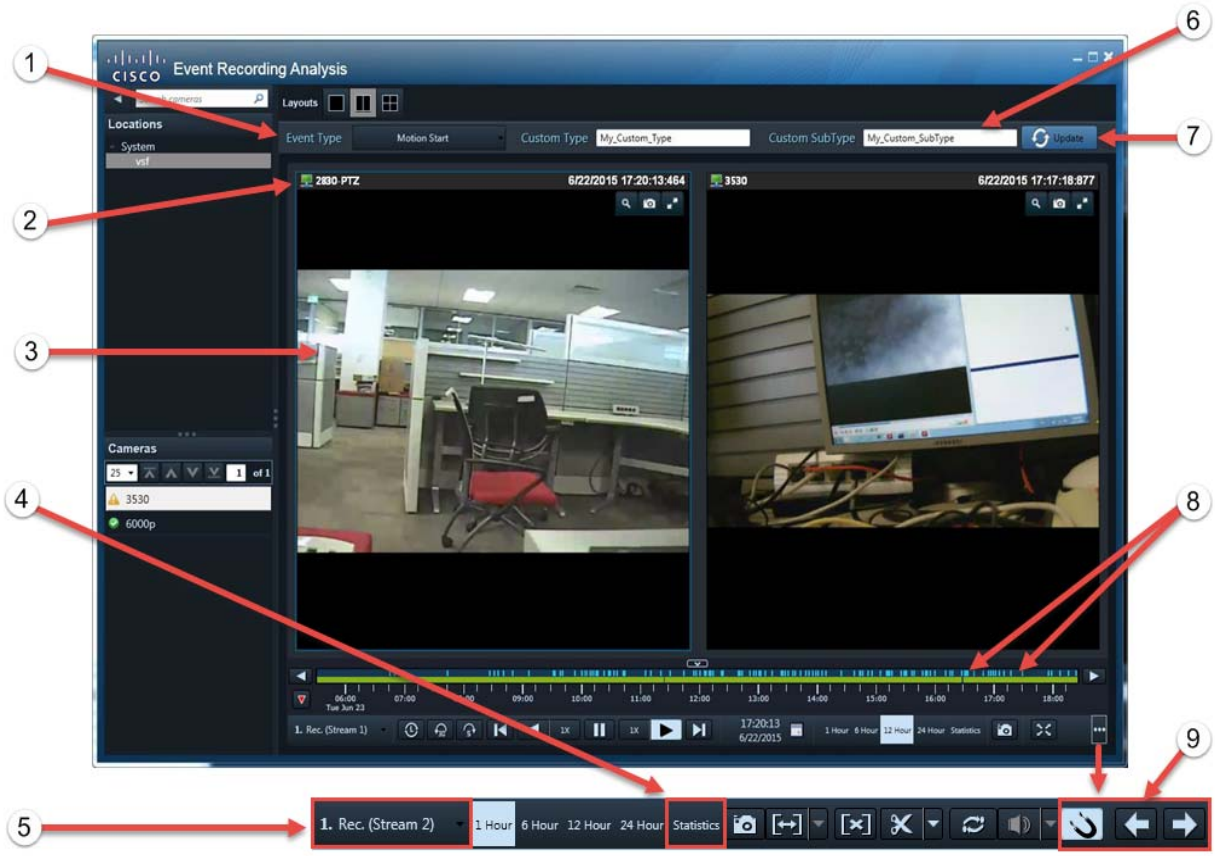
You can use this feature with other features in performing video analysis. For example, you can use Event Recording Analysis with a camera that can switch from low resolution to high resolution when triggered by an event to easily view all recorded video for certain events in high resolution.

To analyze video by event, select **Investigation > Event Recording Analysis** from the Cisco Video Surveillance Safety and Security Desktop (Cisco SASD) menu. Figure 47 provides an overview of the Event Recording Analysis window.

- Overview
- Understanding Statistics and Detail Modes
- Requirements
- Using Event Recording Analysis
- Analyzing Events in Multi-Pane and Sync Mode

Overview

Figure 47 Event Recording Analysis window



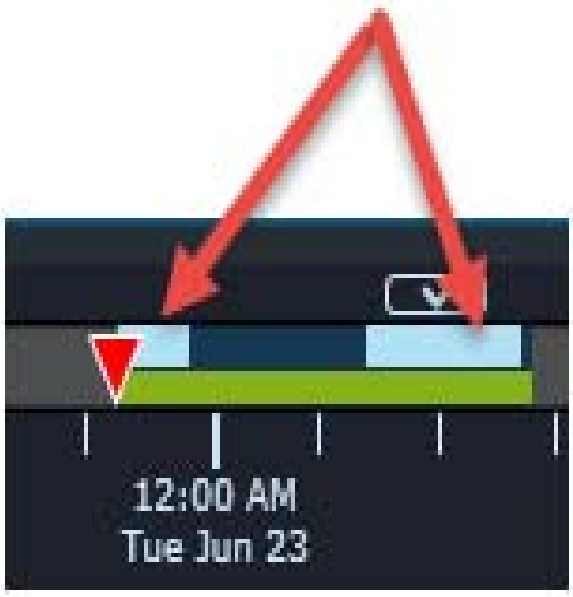
1.	Event Type—The security event type configured in Operations Manager for the selected camera. Possible events are: • Analytics • Camera App • Camera Security • Contact Closure Closed • Contact Closure Opened • Motion Start • Motion Stop • PTZ Start • PTZ Stop • Soft Trigger **Note:** The camera must be configured in VSOM for the selected event type and for recording when the event occurs. For more information on advanced events, see "Video Analytics and Advanced Events" in *Cisco Video Surveillance Operations Manager User Guide*.

2.	Camera Name—Source of the recorded video. Use the left pane of the workspace to search for and select cameras. Only cameras with recorded video appear in the Cameras list.
3.	Active pane—Shows recorded video for the selected camera. The blue border indicates that the pane is active, and the time line applies to the active pane. **Note:** You can also use Event Recording Analysis with multiple video panes. See Analyzing Events in Multi-Pane and Sync Mode, page 124.
4.	Time span—Selects a span of time for the recorded video. 1 hour is always displayed in detail mode with a blue line for each event. The other time spans display events in either detail mode or statistics mode, based on the number of events. See Understanding Statistics and Detail Modes, page 120.
5.	Recording—Selects an available recording, if there are multiple recordings for the same camera across different streaming servers. If recordings are not available for the event(s) you wish to view, select a different recording stream. Recording may be configured differently on a different stream.
6.	Custom Type, Custom SubType—Enter the name of the custom event type and subtype. These are configured in VSOM for Soft Trigger and Camera App event types. See “Creating Custom Event Types and Sub Types” in *Cisco Video Surveillance Operations Manager User Guide* for more information.
7.	Apply—Refreshes the screen to display changes.
8.	Events—Indicates times in the video recording when an event of the selected type occurred. Events on the time line correlate to events in the SASD Events table in the Alert Workspace. Events are displayed as individual events or as groups. See Understanding Statistics and Detail Modes.
9.	Recording—A green bar is displayed on the timeline where recording is available. **Tip** Select as alternate recording stream since streams may be configured to record and retain video differently.
10.	Event icons. Click to show the overflow items in the control bar. • —**Snap to Event**. Enable this button to drag the play head on the time line and snap to the next available event. Disable this button to drag the play head or seek to any point on the time line. • —**Previous Event**. Click to jump to the previous event of the selected type. • —**Next Event**. Click to jump to the next event of the selected type.

Understanding Statistics and Detail Modes

Statistics mode displays events as gray bars that represent groups of events. This mode is displayed automatically anytime you select a time span greater than 1 hour and there are multiple events over a short period of time that cannot be individually displayed on the time line (Figure 48).

Figure 48 Event Recording Analysis: Statistics Mode



1	Time span for the displayed video. • Time spans greater than 1 hour are displayed in either Detail mode or Statistics mode, depending on the number of events. • 1 hour is always displayed in Detail mode (each event is displayed as a thin blue line). See Figure 49.
2	Events in Statistics mode. Events are grouped together to form a histogram. Each bar of the histogram represent the total number of events during a particular time interval. • Mouse hover over a histogram bar to view the total number of event during a period of time. • Event statistics are displayed in 1 hour intervals, except the 1 week time span, which show 6 hour intervals. • The green lines represent recorded video.
3	Information is displayed when you mouse hover a histogram bar, such as the number of events in the time span.

Detail mode is displayed for the 1 hour time span or if there are only a small number of events for greater time spans (Figure 49).

Figure 49 Event Recording Analysis: Detail Mode

1	Time span for the displayed video. • 1 hour is always displayed in Detail mode (each event is displayed as a thin blue line. • Time spans greater than 1 hour are displayed in either Detail mode or Statistics mode, depending on the number of events.
2	Events in Detail mode. Each event is displayed as a think blue line. • Click on **Next Event** or **Previous Event** to jump to the next event time. • If you jump to an event where there is a recording gap, the application jumps to the next event with available video. • In Sync mode, all video panes with video available for the event play the video. • (Optional)

3	A green bar is displayed where video is available.
4	The recorded stream. Select a different stream if recording is not available for the event. Different streams may be configured to record and retain video.
5	Click **Snap to Event** and drag the play head to snap it to the next event.

Requirements

Table 18 lists the requirements for using the Event Recording Analysis feature.

Table 18 Event Recording Analysis Requirements

Requirements	Complete? (✓)
The camera's configuration template must be configured to record video, there must be recorded video available, and the event type that you want to analyze must be configured in Operations Manager as an Advanced Event with the action to record when the event occurs. **Related Information** • Cisco Video Surveillance Operations Manager User Guide	❑
You must belong to a Cisco Video Surveillance User Group with permissions for the following: • View Recordings **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:** Event Recording 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	❑

Using Event Recording Analysis

To analyze recorded video based on an event:

Step 1 Log in to the Cisco SASD application.

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

Step 2 Select **Investigation > Event Recording Analysis** (Figure 47).

Step 3 In the Event Recording Analysis window, drag a camera onto the video pane.

Step 4 (Optional) Select a recording stream.

The green bar appears on the time line, indicating recorded video.

Select as alternate recording stream since streams may be configured to record and retain video differently.

Note: SASD automatically adjusts the default time span based on recording length. If the archive is longer than 24 hours, SASD sets the timeline granularity to 24 hours.

Step 5 Select an event type from the **Event Type** drop-down list.

The camera must be configured in VSOM for the selected event type and for recording when the event occurs.

Step 6 Click **Apply**

to display event markers on the timeline.

Step 7 Green lines indicate where recorded video is available. If the recording is not continuous, there may be gaps in the recording, and you may have event markers where there is no recording.

Event markers (blue lines) appear on the time line. If there are no blue lines, either the event type you selected is not configured, or there are no events for that type.

- Detail mode—A blue line indicates a point in the video recording where the event occurred. The 1 hour time span is always displayed in Detail mode.
- Statistic mode—If there are multiple events for a short period of time, then events are bundled into hourly intervals (except the 1 week time span where events are displayed in 6 hour intervals).

Step 8 See also Analyzing Events in Multi-Pane and Sync Mode and Understanding Statistics and Detail Modes.

Analyzing Events in Multi-Pane and Sync Mode

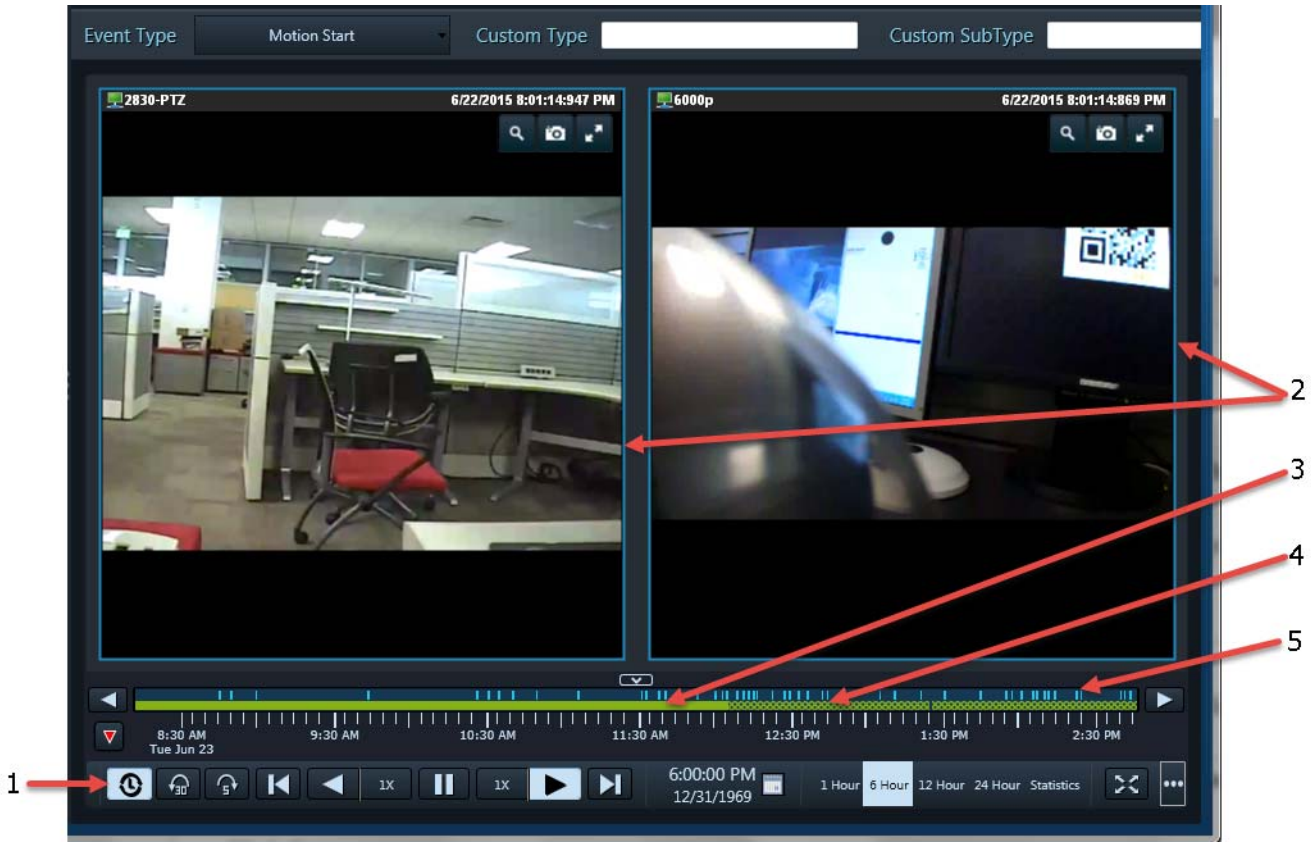
You can use the Event Recording Analysis feature with multiple video panes and in Sync mode .

- In multi-pane mode, you can use Event Recording Analysis to analyze video from multiple cameras and events that occurred at the same time or different times. Each video pane can have a different event type. In non-Sync mode, the time line shows video and events for the selected video pane.
- In Sync mode, all video panes show video for the same time, if video exists for the selected cameras and event type of the pane. The time line shows combined video and events for all panes. If video does not exist for a camera in Sync mode, the video pane displays the following image:

Note the following when using Event Recording Analysis in Sync mode:

- If *all* cameras have video for the same time duration, the green bar on the time line appears solid to indicate full data. If *any* but not all cameras have video for the same time duration, the bar appears with a cross-hatched pattern to indicate partial data. See Figure 50.
- If you select multiple cameras with different event types and then select Sync mode, the Event Type field will be blank and the combined event markers on the time line are for any event from any of the video panes.
- If you select an Event Type after selecting Sync mode, the combined event markers on the time line are for the selected event from any of the video panes.

Figure 50 Event Recording Analysis in Sync Mode



1	Sync mode button enabled.
2	Video panes in Sync mode.
3	Solid green—All cameras have video available for the time shown (full data).
4	Pattern—At least one camera but not all cameras have video available for the time shown (partial data).
5	Combined events.

To analyze events in multiple panes or in Sync mode:

Step 1 Log in to the Cisco SASD application.

- See Logging In, page 15.
- Event Recording Analysis is not supported using the Cisco SASD Advanced Video Player or Cisco SASD Federator applications.

Step 2 Select **Investigation > Event Recording Analysis** (Figure 47).

Step 3 In the Event Recording Analysis window, select a layout, and then drag cameras onto the video panes.

Step 4 (Optional) Select a recording stream.

The green bar appears on the time line for the selected video pane (the pane with the blue border), indicating recorded video.

Step 5 Select an event type from the **Event Type** drop-down list and click **Apply** to display event markers on the timeline.

Note: The camera must be configured in VSOM for the selected event type and for recording when the event occurs.

Tip: You can see the events listed for a device in the Cisco SASD Events table in the Alert workspace.

Step 6 Green lines indicate where recorded video is available. If the recording is not continuous, there may be gaps in the recording, and you may have event markers where there is no recording.

Event markers (blue lines) appear on the time line. If there are no blue lines, either the event type you selected is not configured, or there are no events for that type.

- Detail mode—A blue line indicates a point in the video recording where the event occurred. The 1 hour time span is always displayed in Detail mode.
- Statistic mode—If there are multiple events for a short period of time, then events are bundled into hourly intervals (except the 1 week time span where events are displayed in 6 hour intervals).

Step 7 (Optional) Click **Sync all panes** .

If you selected different event types for the videos panes before putting them in Sync mode, the time line shows combined events of each pane's selected event type.

Step 8 (Optional) Select an Event Type for all video panes and click **Apply** to display event markers on the timeline.

The time line shows combined events of the selected type for all video panes.

Step 9 Click on **Next Event** or **Previous Event** to jump to the next event time.

- If you jump to an event where there is a recording gap, the application jumps to the next event with available video.
- In Sync mode, all video panes with video available for the event play the video.

  Note: Cisco SASD displays a message if there are no more events in the video.

Step 10 (Optional) Click **Snap to Event** and drag the play head to snap it to the next event.

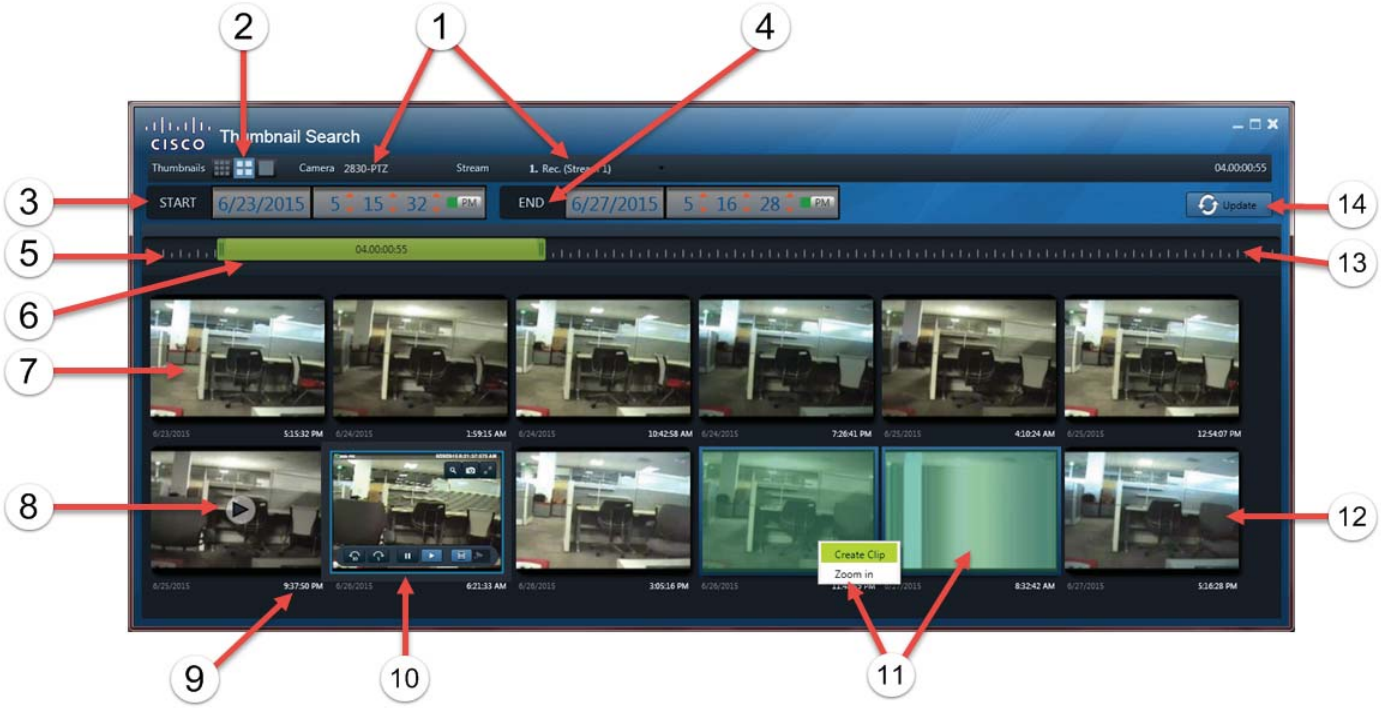
Thumbnail Search

You can 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.

- Viewing a Thumbnail Summary, page 129

Figure 51 provides an overview of the search and display controls.

Figure 51 Thumbnail Window



1	Camera and Video Stream • Camera—Drag a camera onto the Thumbnail Search window. • Stream—Select the recording 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. • Double-click to play the recorded video for that thumbnail in a full size window. See Viewing Video, page 77 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 See Viewing Video, page 77 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 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.

Viewing a Thumbnail Summary

To view a thumbnail summary of recordings on a camera:

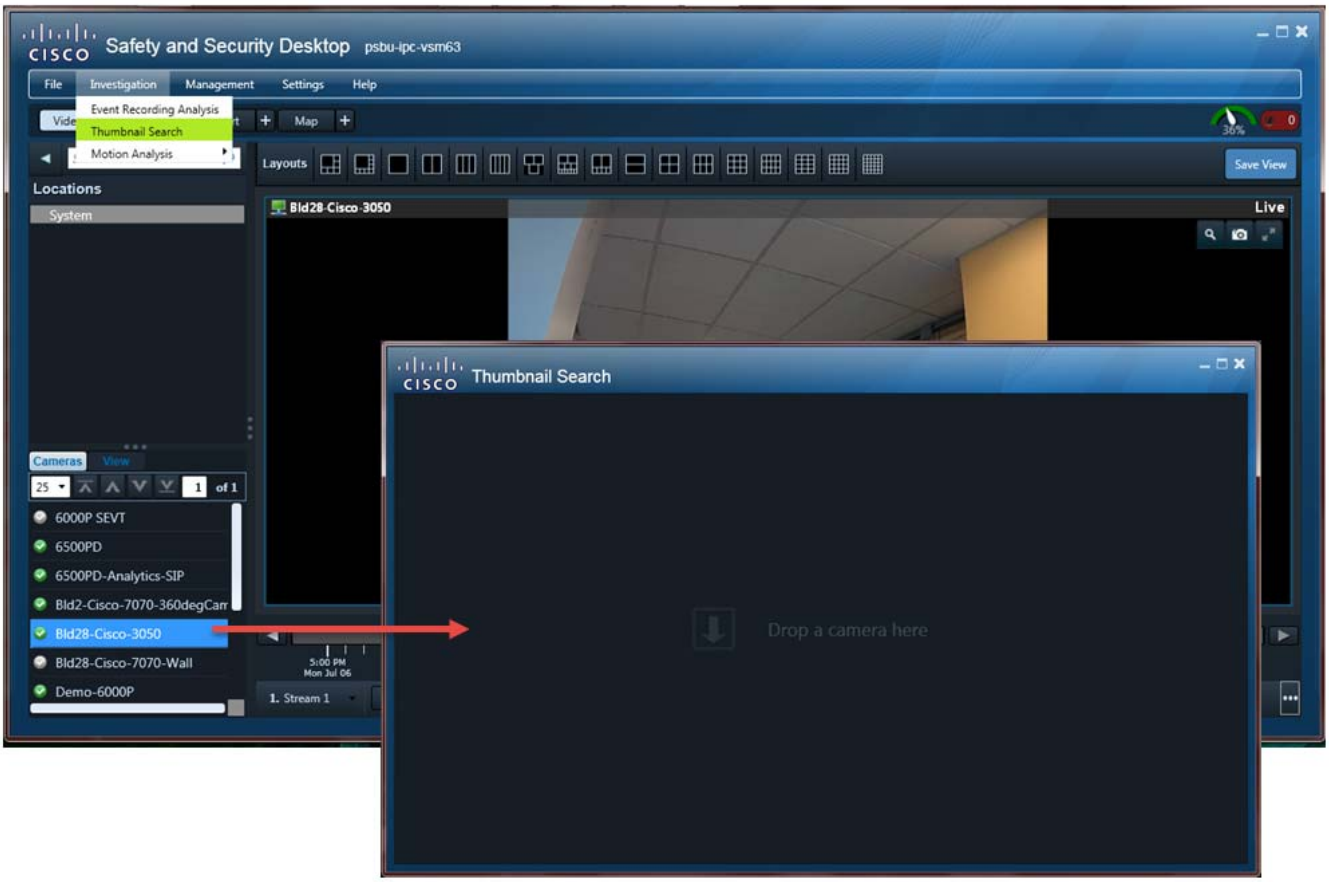
Step 1 Log into the Cisco SASD or Cisco SASD Federator application.

Note: The Cisco SASD Advanced Video Player application does not support Thumbnail Search.

Step 2 Select **Investigation > Thumbnail Search** (Figure 52).

Step 3 Drag a camera from the Video workspace onto the Thumbnail Search window (Figure 52).

Figure 52 Drag a Camera to the Thumbnail Search Window



Step 4 (Optional) Select a video stream.

Stream 1 is selected by default.

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

Step 6 Click Update to refresh the displayed thumbnails.

Step 7 (Optional) Slide the range bar right or left within the recording timeline.

Step 8 (Optional) Click a thumbnail to play video from the start time (in white text).

Tips:

- Use the video playback controls to search within the thumbnail span. See the Viewing Video, page 77 section for more information.
- Double-click a thumbnail to enlarge the video in the browser window. Select **Full Screen Mode** to fill the entire monitor screen.

Step 9 (Optional) Create a clip:

a. Click and drag to select multiple thumbnails.

b. Select **Create clip**.

c. Enter a clip name.

d. Select a clip type:

- MP4

- Virtual
- CVA

e. Click **OK**.

Step 10 (Optional) Narrow the thumbnail search.

Step 11 (Optional) Select a new time range.

a. Click and drag to select multiple thumbnails.

a. Select **Zoom In**.

Clip Management

Use **Clip Management** (Figure 53) to view, download and delete MP4 video clips and virtual clips.

MP4 video clips and virtual clips are saved to the Cisco Video Surveillance server by default. You can download clips using any of the following methods:

- Click the down arrow next to **Create Clip** in the SASD control bar. Select the clip name from the list. Save MP4 files to a local disk (the clip remains on the server for 7 days after it was created). Virtual clips play in the video pane after you download them.
- Use the **Clip Management** feature to find and download video clips.
- Operations Manager—Use the **Clip Search** feature to find and download video clips.

Note: You can select clips created using Cisco SASD Federator from the Cisco SASD main window (using the **Create Clip** pull down menu). However, clips that you create using Cisco SASD are not available for selection from the Cisco SASD Federator main window (using the **Create Clip** pull down menu).

Tips

- See Creating and Viewing Video Clips, page 87 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.

To locate, download, and view MP4 or virtual video clips:

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.

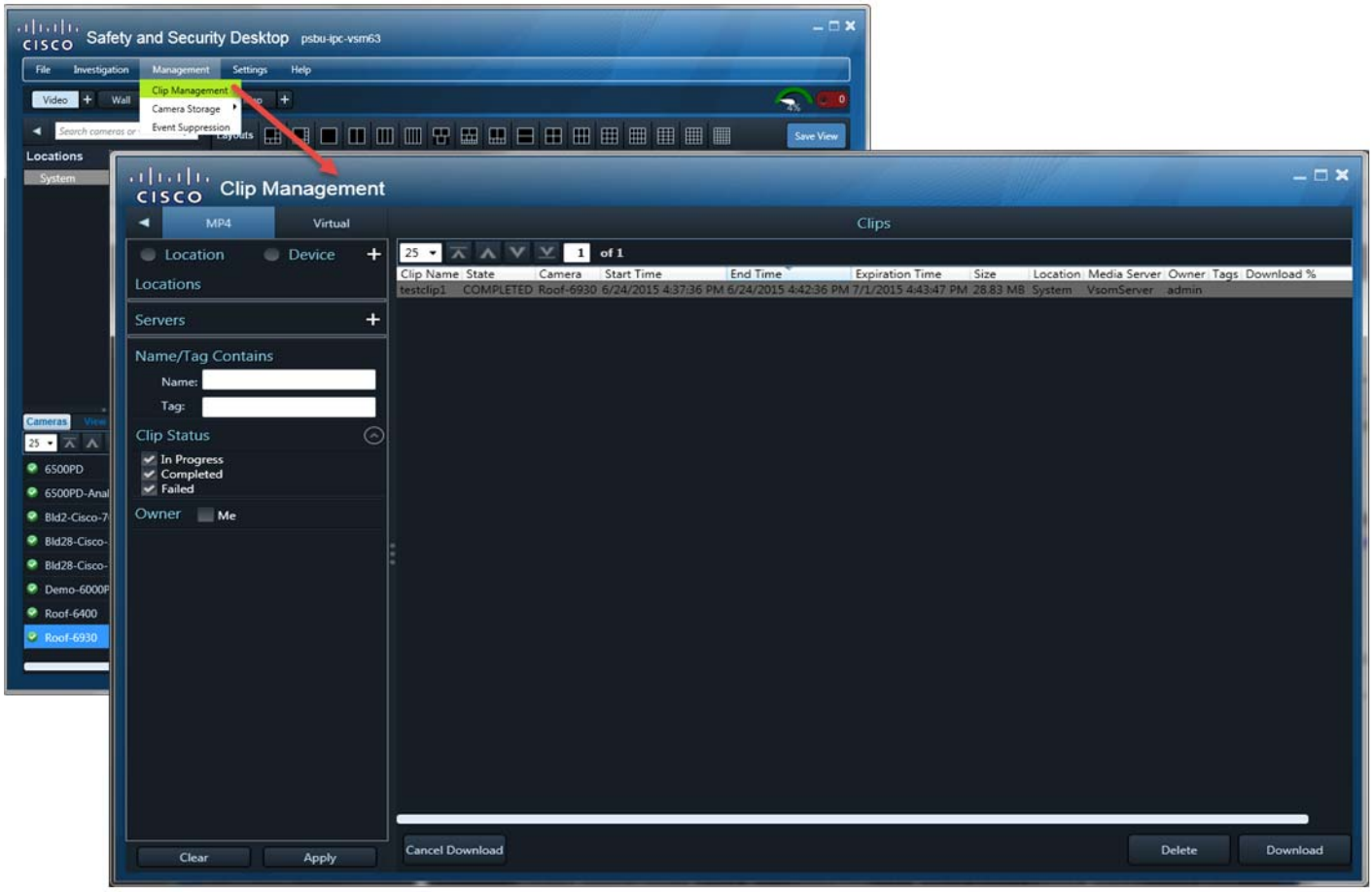
Step 2 Create one or more MP4 or virtual video clips.

See the Creating and Viewing Video Clips, page 87 in the Cisco Video Surveillance Safety and Security Desktop User Guide for more information.

Step 3 Select **Management** > **Clip Management** (Figure 53).

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 53 Clip Management Window



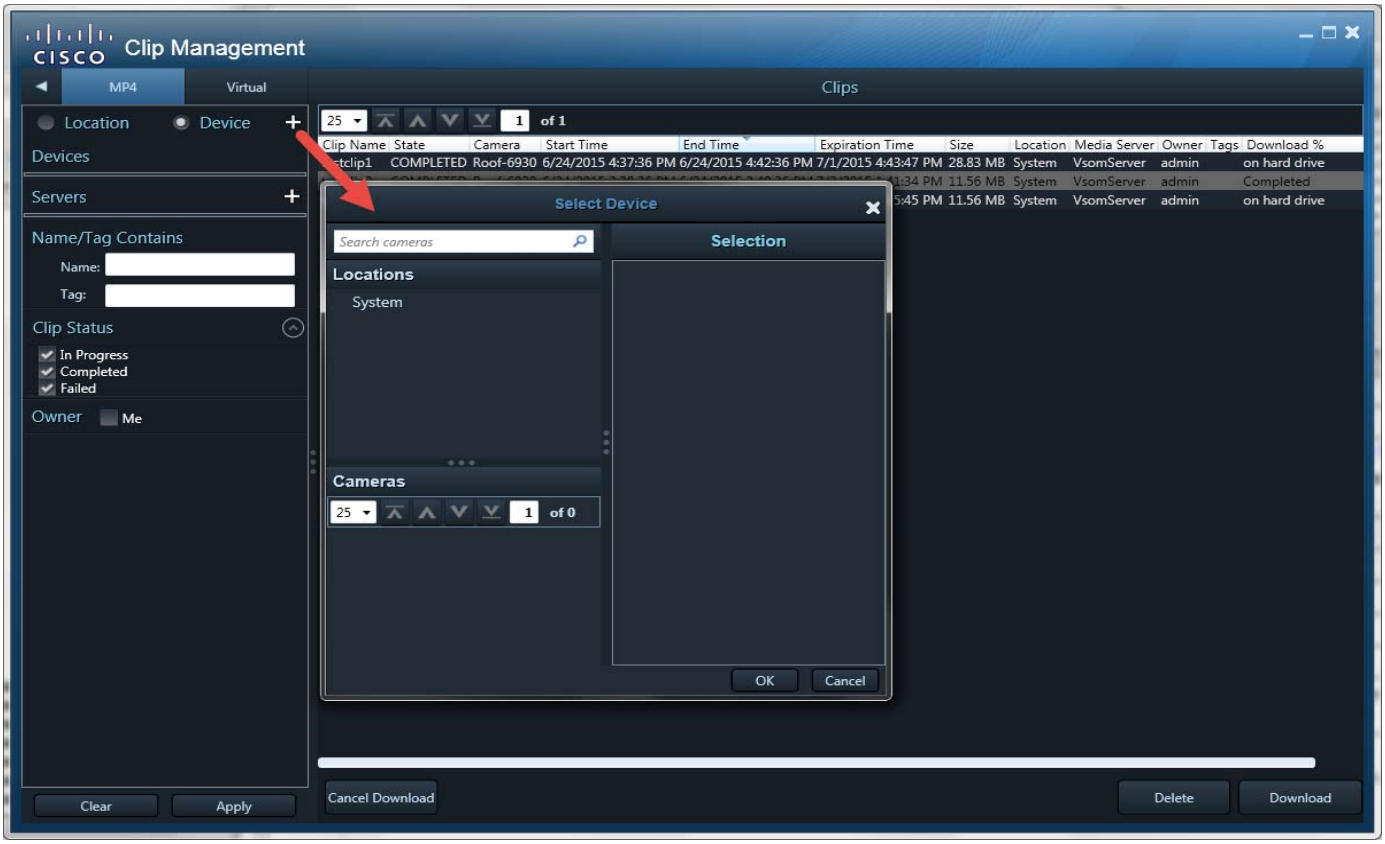
Step 5 Select the **MP4** tab for MP4 clips, or select the **Virtual** tab for virtual clips.

Step 6 (Optional) Select a location or device (Figure 54):

- 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 54 Select a Location or Device



Step 7 Use the additional clip filters to search for specific clips (Table 19):

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

Table 19 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 (MP4 only)	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 8 Click **Apply**.

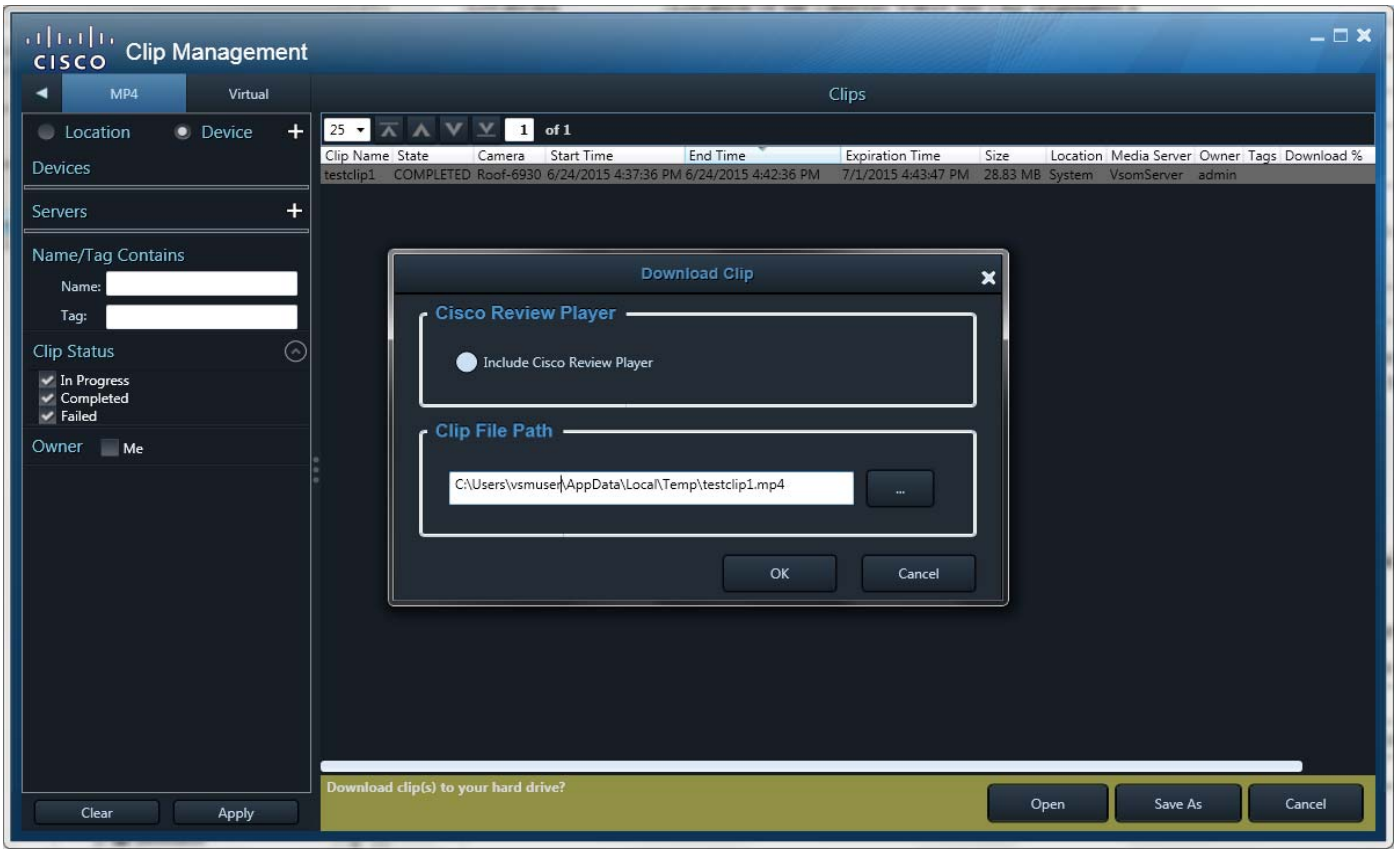
Step 9 Review information about the clips.

Table 20 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	Initiated, 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 (MP4 only)	The date/time when the clip will be automatically deleted from the server. See “Creating and Viewing Video Clips” in the Cisco Video Surveillance Safety and Security Desktop User Guide for more information.
Size (MP4 only)	The clip file size.
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 % (MP4 only)	The status of the clip download: percentage downloaded, or completed or on hard drive. See Step 10.

Step 10 (Optional) To download and view an MP4 clip, select one or more MP4 clips in the **MP4** tab and click **Download** (Figure 55).

Figure 55 MP4 File Download



a. Click **Open** to download the clip to a temp directory and immediately play it in Cisco Review Player.

   or

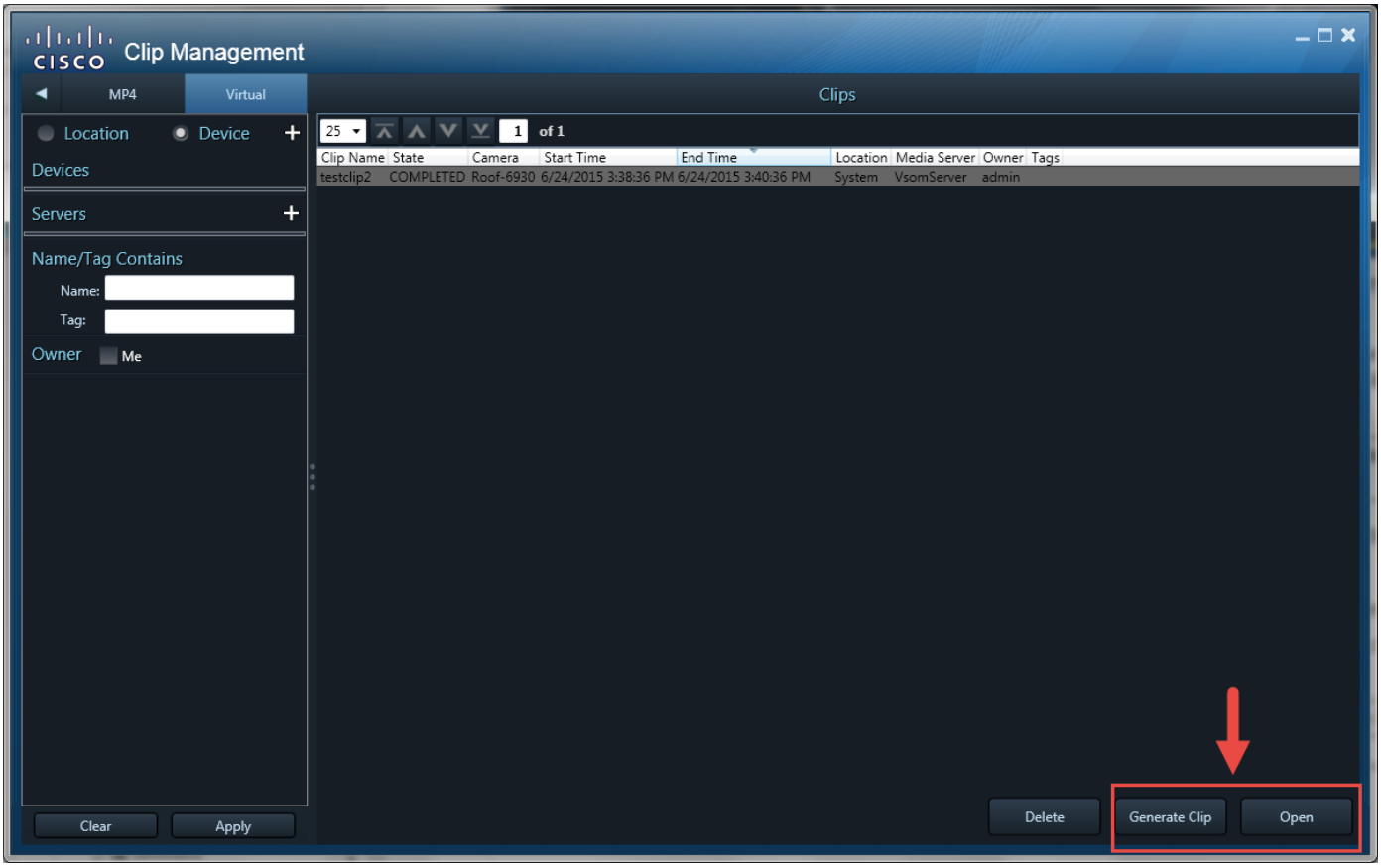
   Click **Save As** to specify a location on your hard drive for the file. In the Download Clip pop-up window, select whether to include Review Player with the clip and the clip file path, and click **OK**.

Tip: After you download an MP4 file, you can double-click the file name in Clip Management to play it.

Step 11 (Optional) To view a virtual clip, select the clip in the **Virtual** tab and double-click it or click **Open** (Figure 56).

The clip plays in a separate window.

Figure 56 Virtual Clip Options



Step 12 (Optional) To save a virtual clip as an MP4 file, select the clip in the **Virtual** tab and click **Generate Clip** (Figure 56).

a. Click the **MP4** tab to download or open the clip as an MP4 file.

Step 13 (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 Video Analysis

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 a specific time span and apply sensitivity filters to detect or ignore motion in different sections of the video frame. These filters can be modified and the video examined to discover different time spans or 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).

This section includes the following topics:

- Understanding Luminance Metadata and Motion Analysis, page 139
- Requirements, page 140
- Process Summary, page 141
- Initiating a Motion Video Search, page 142
- Metadata Job Management, page 152

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 the luminance value changes and sensitivity filters you apply.

Note: In this release, Motion Video Analysis is supported only for Stream 1. JPEG recordings are not supported. Luminance metadata must be enabled in the Operations Manager. See the Requirements, page 140 for more information.

You can use Motion Video Analysis for security purposes or to perform other analysis such as monitoring cars entering or leaving a parking garage. For example, you can determine the number of motion events in a large amount of time or quickly view a video summary with only the times 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 and 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 (see Stage 1 in Initiating a Motion Video Search, page 142).

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 change and a motion event is triggered.

Note: You must have a Metadata server installed to enable the Motion Video Analysis feature. This adds the Metadata server service to the Operations Manager and enables the luminance metadata track (see the Cisco Video Surveillance Operations Manager User Guide).

Sensitivity Settings and Motion Events

You use the Sensitivity settings to define the luminance value changes required to trigger a motion event. For example, you can paint a grid to define the areas for detecting motion, and specify low or high Sensitivity for each grid. Sensitivity defines if more or fewer of the pixels in that grid must experience a luminance change to trigger an event. You can also define the percentage of grids that must be affected to trigger a motion event. See Initiating a Motion Video Search, page 142.

Requirements

Table 21 lists the requirements to support the Motion Video Analysis feature.

Table 21 Metadata Requirements

Requirements	Complete? (✓)
A Metadata Server service enabled on a standalone virtual or physical server running Cisco VSM Release 7.7 or higher (operating system RHEL6.6). Enable the Metadata Server service in the Operations Manager for your deployment. See your system administrator for more information. **Related Information** • Cisco Video Surveillance Operations Manager User Guide	❑
Enable record video in the camera configuration template, and enable the Luminance metadata track. **Note:** In this release, only one metadata request is allowed per camera until the metadata generation completes for the last request. A new request from that camera can then be processed (see Metadata Job Management, page 152). An error message appears if the Luminance metadata track is not configured in the camera configuration template. **Related Information** • Cisco Video Surveillance Operations Manager User Guide	❑

Table 21 Metadata Requirements (continued)

Requirements	Complete? (✓)
You must belong to a Cisco Video Surveillance user group in the Operations Manager with permissions for the following: • *Post Analytics Metadata* • *View Analytics Metadata* • *View Live Video* • *Perform PTZ* (automatically enabled with *View Live Video*) • *View Recordings* • *Camera* (Manage permission) **Note:** All of these permissions are required to generate metadata, view generated metadata, and perform video motion searches using the Cisco SASD desktop application. See your system administrator for more information. **Related Information** • Cisco Video Surveillance Operations Manager User Guide	❑
The Cisco SASD desktop application 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	❑

Process Summary

These are the steps for generating luminance metadata and viewing motion events. See Initiating a Motion Video Search, page 142 for more information.

1. Complete the Requirements, page 140.
2. Select **Investigation > Motion Analysis > Motion Video Search** to open the MVA Stage 1 window.
3. Drag a camera onto the popup window.
4. Select a Start and End time for the duration of recorded video to analyze.

   Tip: You can use the yellow lines in the Detail Range timeline to set the duration or recorded video to analyze.
5. Click **Next**.

- If selected time duration (yellow lines on the Detail Range timeline) does not have metadata, you are prompted to generate metadata.
- If selected time duration has metadata, the process jumps to Stage 2.

Note: In this release, only one metadata request is allowed per camera until the metadata generation completes for the last request. A new request from that camera can then be processed (see Metadata Job Management, page 152).

6. In the MVA Stage 2 window, select a span of time for the motion search (at least part of the recording must have metadata).
7. Click inside the video pane and select the portion of the video frame to analyze.
8. Set the motion Sensitivity and Threshold levels.
9. Click **Next** to continue to Stage 3 and start processing the motion search results.
10. In the Stage 3 window, click the motion thumbnails to view video from the motion events.

Tip: The number of motion events detected appear on the thumbnail groups.

Initiating a Motion Video Search

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

Step 1 Log in to the Cisco SASD application (see Logging In, page 15).

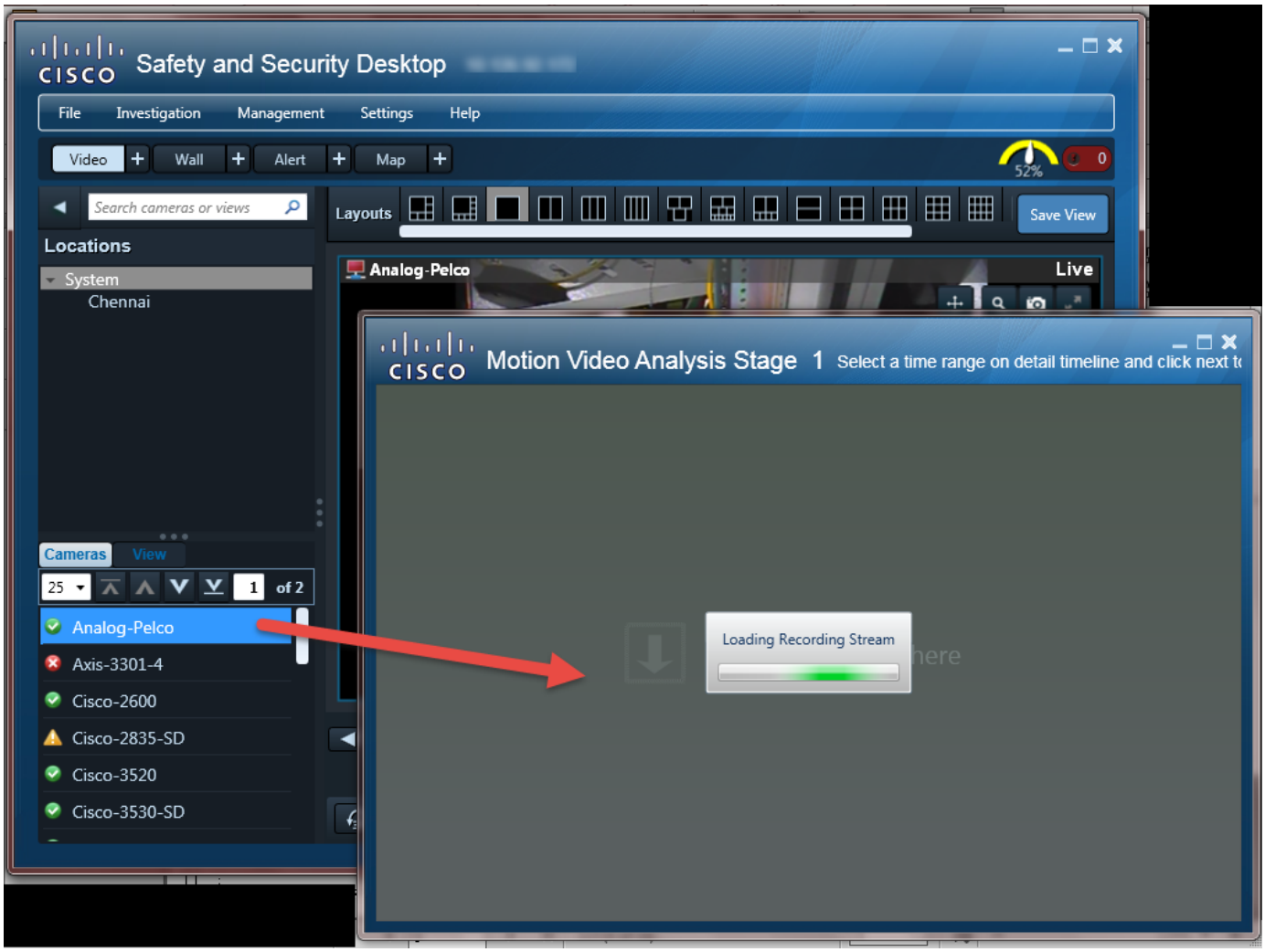
Note: Motion Video Analysis is not supported using the Cisco SASD Advanced Video Player or Cisco SASD Federator applications.

Step 2 Select **Investigation > Motion Analysis > Motion Video Search** (Figure 57).

Step 3 Drag a camera onto the Motion Video Analysis window (Figure 57).

An error message appears if the Luminance metadata track is not configured in the camera configuration template using the Operations Manager (see Requirements, page 140).

Figure 57 Motion Video Analysis Search Window–Stage 1 Loading a Camera



Step 4 Stage 1: Generate the luminance metadata:

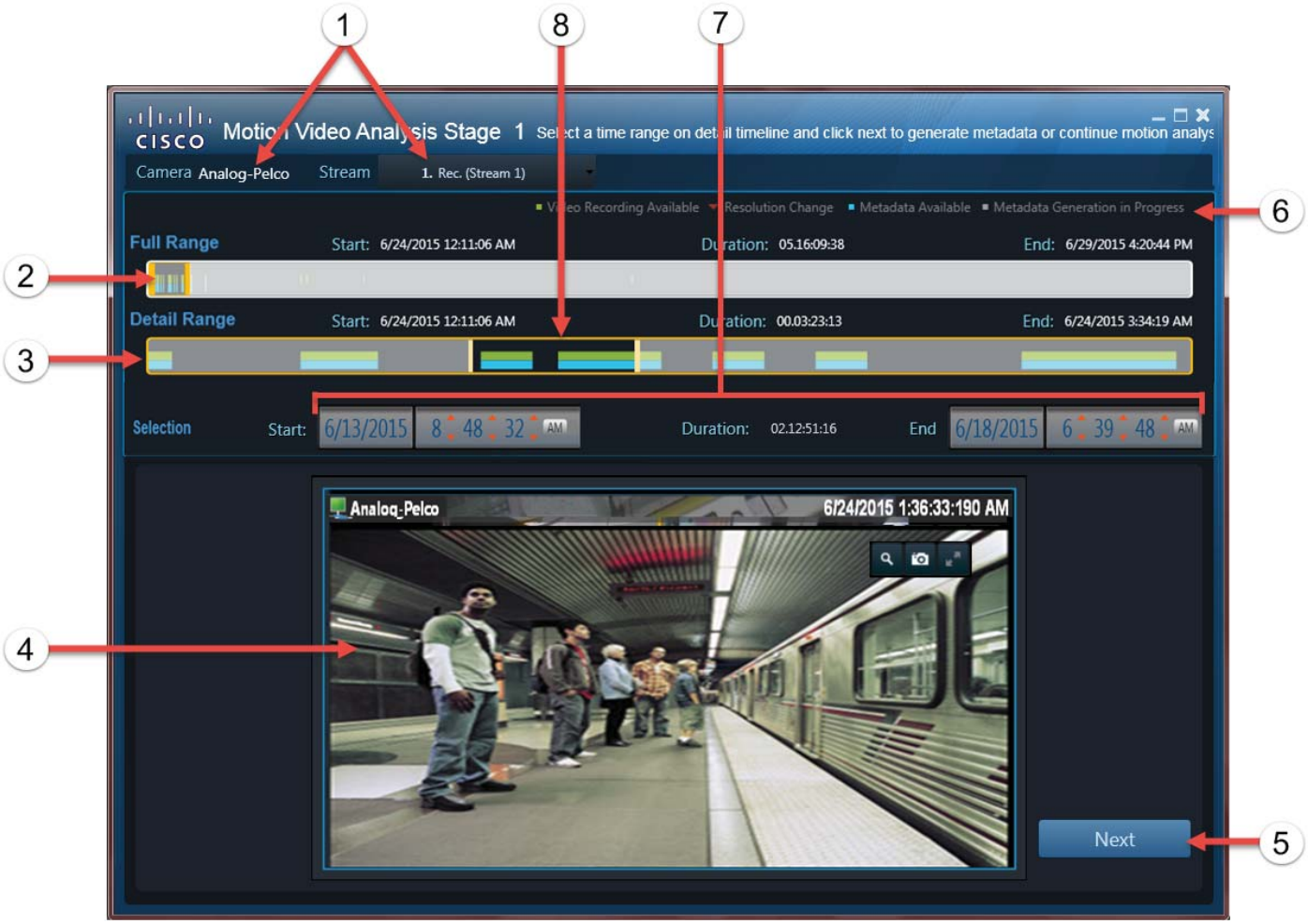
a. Use the Recording Full Range, Detail Range, and Selected Range fields (Figure 58), select a span of recorded video and generate the luminance metadata used to detect motion events.

See Understanding Luminance Metadata and Motion Analysis, page 139 for more information.

Note: In this release, only one metadata request is allowed per camera until the metadata generation completes for the last request. A new request from that camera can then be processed (see Metadata Job Management, page 152).

– Up to 5 metadata jobs can run at a time. Additional jobs are queued and begin when another job is completed, fails, or is canceled.

Figure 58 Stage 1: Generating Metadata



1	The camera and stream (source) for the video recording. **Note:** In this release, only Stream 1 recorded video is supported.
2	Recording Full Range—The entire recording range available on the camera. The selected span of time on Recording Full Range defines the duration (*Day*:*hours*:*minutes*:*seconds*) of the Detail Range timeline. **Tip:** The shorter the selected time span in the Full Range timeline, the larger the metadata readings appear in the Detail Range timeline. Drag the orange bars right and left to define a sub-set of the available recording. Click and drag the middle of the bar right or left to select a different section of the recording using the same duration. When the Stage 1 window opens, the Duration Selection pane time boxes display as follows: • Start time box—Indicates the beginning timestamp of the first available recording. • Duration—Displays the entire duration of video available on the camera. • End time box—Indicates the end timestamp of the most recent recording available on the camera. For example, a continuous recording configured to retain recordings for one day displays a duration of 01:00:00:00. The start and end times indicate the beginning and end of the available recording.

3	Detail Range—The time range selected inside the orange bars in the Full Range timeline. Use the Detail Range timeline to fine-tune the video time span to analyze for motion. **Tip:** Drag the yellow bars right and left to refine the analysis duration. Click and drag the middle of the bar right or left to select a different section of the recording using the same duration.
4	Recording video feed from the selected camera stream. Use this preview to verify the selected camera.
5	Click **Next** to generate the analytics metadata and continue to Stage 2. • If metadata is not available for all or part of the selected recording range, a prompt appears to confirm metadata generation. • If your selection includes partial metadata, a prompt appears to complete metadata generation or continue to motion video 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, page 139.
6	Legend—Key to the recording status in the timeline: • **Video Recording Available** (green)—Video is available for viewing. Gaps in the green bar indicate times when video was not recorded. • **Metadata Available** (blue)—Metadata is available for motion analysis. • **Metadata Generation in Progress** (gray)—The video span(s) where metadata is being created by the Cisco Metadata server. When the gray bar turns blue, metadata generation is complete. See Metadata Job Management, page 152 for instructions on viewing the metadata generation status. • **Resolution Change** (red)—Resolution changes can occur on camera template and/or template recording settings modification. You cannot select a time span that includes a resolution change. This generates an error when you attempt to proceed to Stage 2. **Tip:** Select a time span without recording resolution changes.
7	Selected Range—Set the start and end times to select the recorded video for motion video analysis. Enter different values to fine-tune the selection. For example, you can edit the beginning and ending seconds.
8	Defined duration—This is the time defined in the duration settings. • Green—Recorded video. • Gray—Metadata is currently being generated. See the Metadata Job Management, page 152 for information on job status. • Blue—Metadata generation successful. **Tip:** Drag the orange bars right and left to refine duration. Click and drag the middle of the bar right or left to select a different section of the recording using the same duration.

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

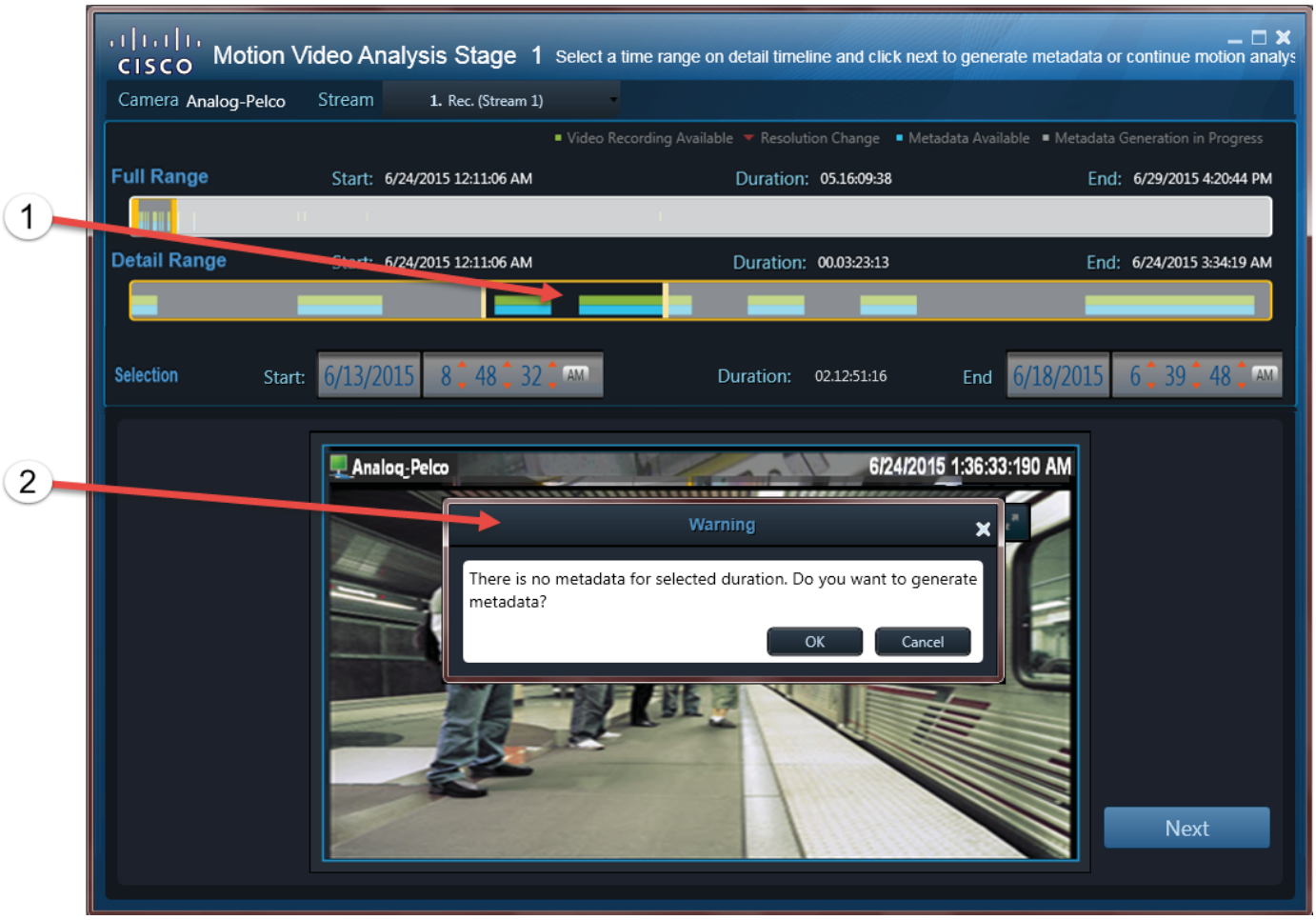
- If all of the selected duration includes metadata (generated in a previous session), skip to Step 5.
- If a duration with no metadata was selected:
  - Click **OK** to continue metadata generation.
  - (Optional) In the main SASD window, select **Investigation > Motion Analysis > Metadata Job Management** to view metadata generation progress (see Figure 63).
  - Click **Next** 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 duration 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 Stage 2 (configuration) window (Figure 59).

Figure 59 Metadata Gap



1	Metadata gap in the selected recording.
2	Prompt that appears when a metadata gap is selected: • **OK**—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 detection grids, Sensitivity, and Threshold level.

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 58 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 the grid for motion detection (Figure 60).

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

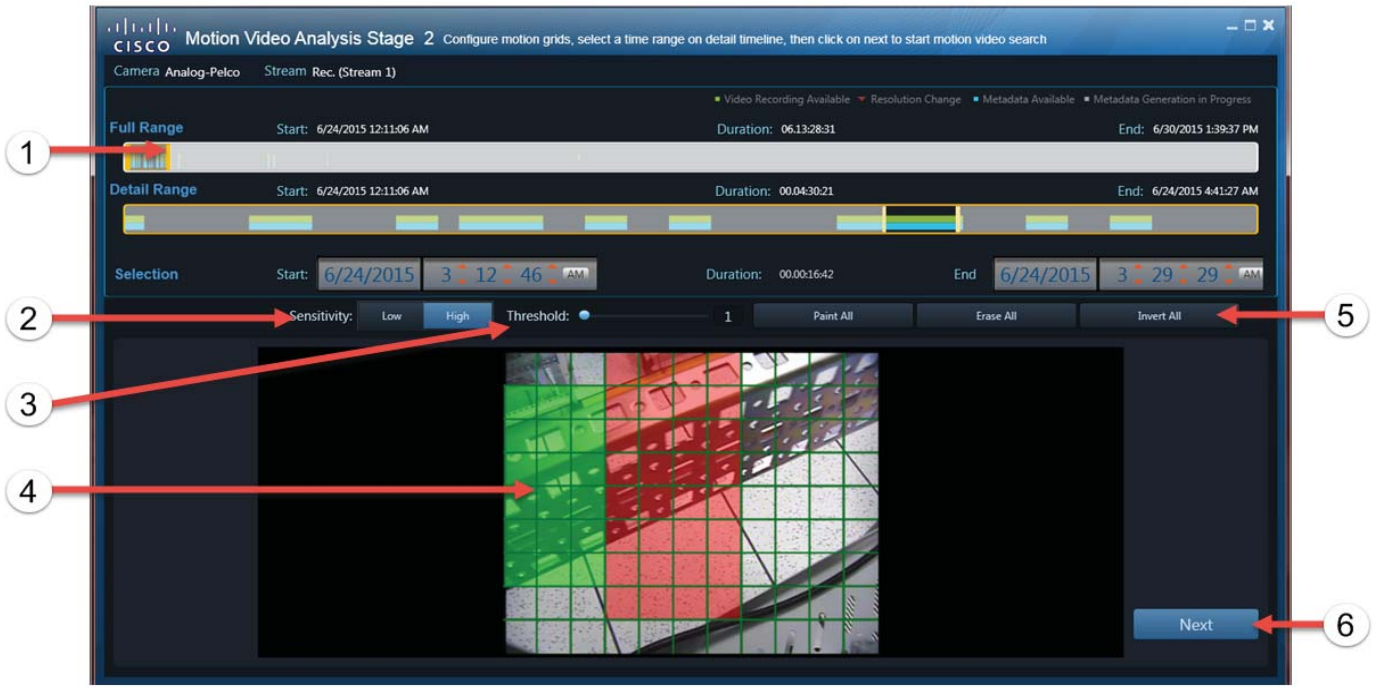
c. Select the **Threshold** by sliding the selector to a number from 1 to 100.

Threshold applies to all painted grids and represents the percentage of grids that must be triggered to record a motion event.

For example, a threshold of 20 means that 20% of the grids must detect motion to trigger a motion event. A threshold of 100 means that all grids must detect motion to trigger a motion event.

A threshold of 1 means that only 1% percent of the grids must detect motion to trigger a motion event (that is, if any grid detects motion).

Figure 60 Stage 2: Defining the Motion Detection Settings



1	Time range selectors—Select and fine-tune the recording duration to analyze for motion. **Tip:** See Figure 58 for more information about using the Recording Full Range, Detail Range, and Selected Range.
2	Sensitivity—Select **High** or **Low** and click the area to paint for motion detection (Step 5).
3	Threshold—The percentage of selected grids that must detect motion to trigger a motion event.

4	Motion grid—Click a grid or click and drag multiple grids to select the areas of the video frame for motion detection.
5	Grid selection tools: • **Paint All**—Paints all grids with low or high luminescence detection, depending on Sensitivity setting. • **Erase All**—Clears all grids. **Note:** If no grids are selected, motion detection is disabled. • **Invert All**—Clear all painted areas and paint all unpainted areas.
6	Click **Next** to view the motion detection results.

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

Notes

- You cannot continue unless a portion of the selected recording has metadata. To generate metadata, return to the Stage 1 window (Step 4).
- Motion analysis is not supported on time ranges with resolution changes.

Step 6 View the motion events for the selected recording (Figure 61).

Wait for the motion detection generation to complete. “Processing” appears on the thumbnail groups during video analysis. See Figure 61 for descriptions of available options.

a. Click the icon on a thumbnail group to view and play the individual events for that group (see Figure 62).

b. (Optional) Click **New Search** to return to Stage 2 (Step 5) to change the luminescence settings or analysis duration.

Figure 61 Stage 3: Motion Analysis Results (Root Level)

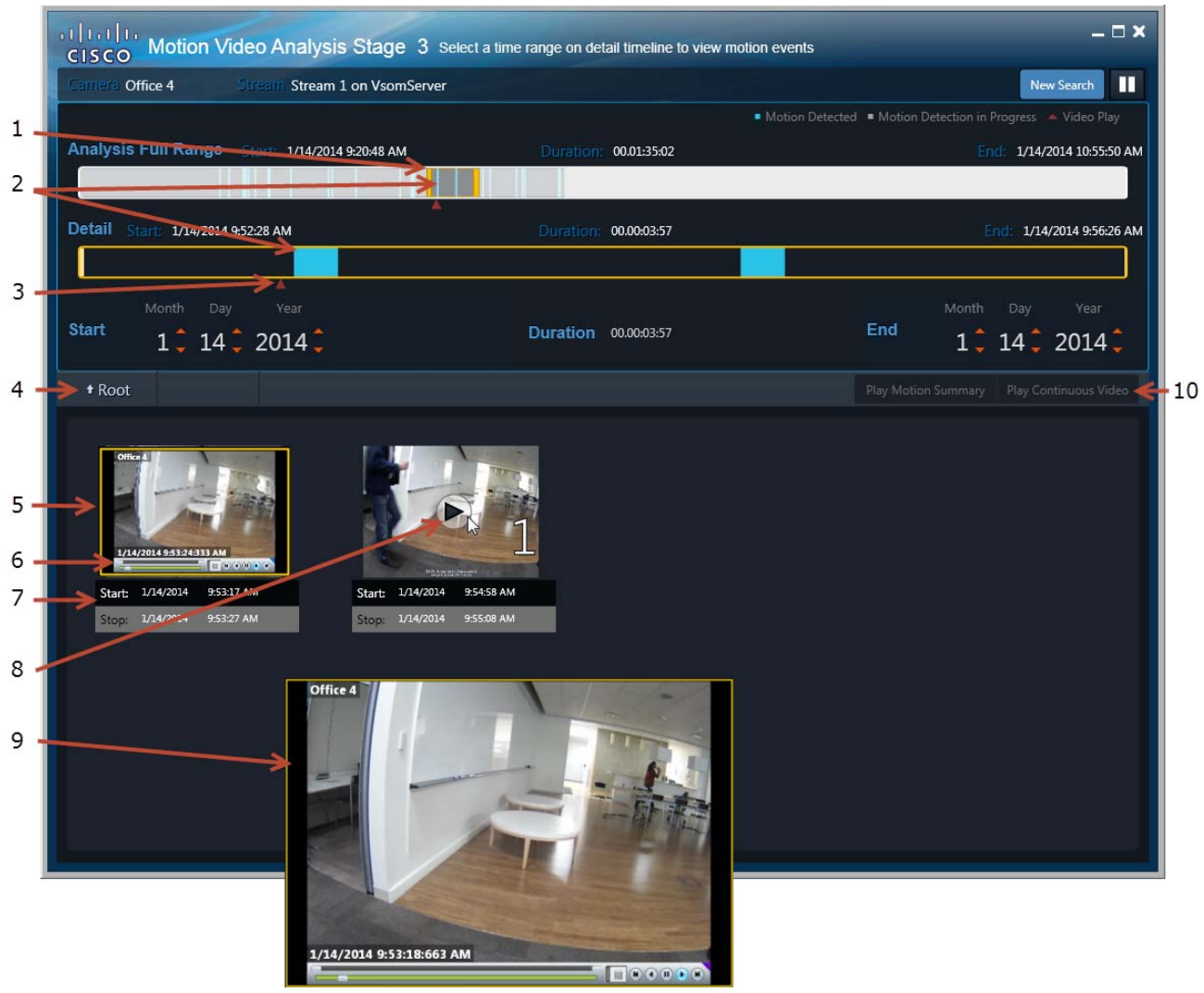
1	The camera and stream (source) for the video recording. **Note:** In this release, only Stream 1 is supported.
2	Analysis Full Range—The range of recorded video for analysis as selected in Stage 2 (see Step 5). By default, the motion results are for this range. **Tip:** Drag the orange bars right and left to display results for a subset of the recording being analyzed. Click and drag the middle of the bar to move through the timeline, but retain the duration.
3	Blue bars—The motion events in the video based on the filters applied in Stage 2 (see Step 5).
4	Detail Range—The time range subset selected in the Analysis Full Range timeline. **Tip:** 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 move through the timeline, but retain the duration.
5	Selected Range—(Optional) Enter different values to fine-tune the duration. For example, you can edit the beginning and ending seconds.
6	**Root** returns to the top-level results.

7	Thumbnail groups—Motion events for the duration. • If there are more than 24 motion events for Selected Range, motion events display in Summary Mode. • The duration is divided into 24 equal time segments, called a *thumbnail group*. • Each thumbnail group has a From /To timestamp, and the image is the first motion event in that duration. • If there are less than 24 motion events for the duration, all motion events display in Detail Mode, where each motion has a thumbnail (no thumbnail groups) and 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 detected in the thumbnail group. **Note:** Continuing motion events (from the previous thumbnail group) are 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 duration and luminescence settings for the selected thumbnail groups.
12	Click to open the View and Play pane with the individual events for that thumbnail group (see Figure 62).
13	**Processing**—Motion event detection based on the Stage 2 filters is ongoing (see Step 5).
14	**Motion Continued**—A motion event that exceeds the thumbnail group duration begins in one thumbnail group and continues to the next thumbnail group. Click the thumbnail group with this label to view the continuing event.
15	• **Play Motion Summary**—Plays all motion event video one event after the other. • **Play Continuous Video**—Plays all video for the selected duration, including video without motion events.
16	Legend—Colors indicate the recording status in the timeline. • Blue—Motion event based on the duration and luminescence settings applied in Stage 2 (see Step 5). • Grey—Motion analysis detection in progress. • Red (Video Play)—The location of the video being played (see Figure 62).
17	—Pauses motion analysis processing. Select again to resume processing.
18	**New Search**—Return to Stage 2 to refine the duration and luminescence settings.

Step 7 Use the options described in Figure 62 to view recorded video from specific motion events.

Note: If a thumbnail group includes more than 24 motion events, an additional layer of thumbnails appears. Click to display the next layer of detailed thumbnails. Click **Root** to navigate to a higher level.

Figure 62 Stage 3: Motion Analysis Results–View and Play Window



1	The time span for the Detailed Range timeline.
2	Blue bar—Motion events detected during analysis.
3	Red triangle (Video Play)—The location of the video being played.
4	**Root**—Return to 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 Viewing Video, page 77 for more information.
7	Start and end times of the motion event video.
8	Plays the motion event from the motion start to motion stop time.
9	Video popup window. Double-click a thumbnail image to play the event video in a larger window. See Viewing Video, page 77 for more information about recorded video controls and options.

10	• **Play Motion Summary**—Plays all motion event video one event after the other. • **Play Continuous Video**—Plays all video for the selected duration, including video without 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, page 82 and Creating and Viewing Video Clips, page 87.

Metadata Job Management

To view the status of metadata jobs triggered in the Motion Video Analysis window (Figure 63):

Step 1 Select **Investigation > Motion Analysis > Metadata Job Management**.

Step 2 Click ✚, select a camera, and click **Apply** to display the metadata jobs for recordings from that device.

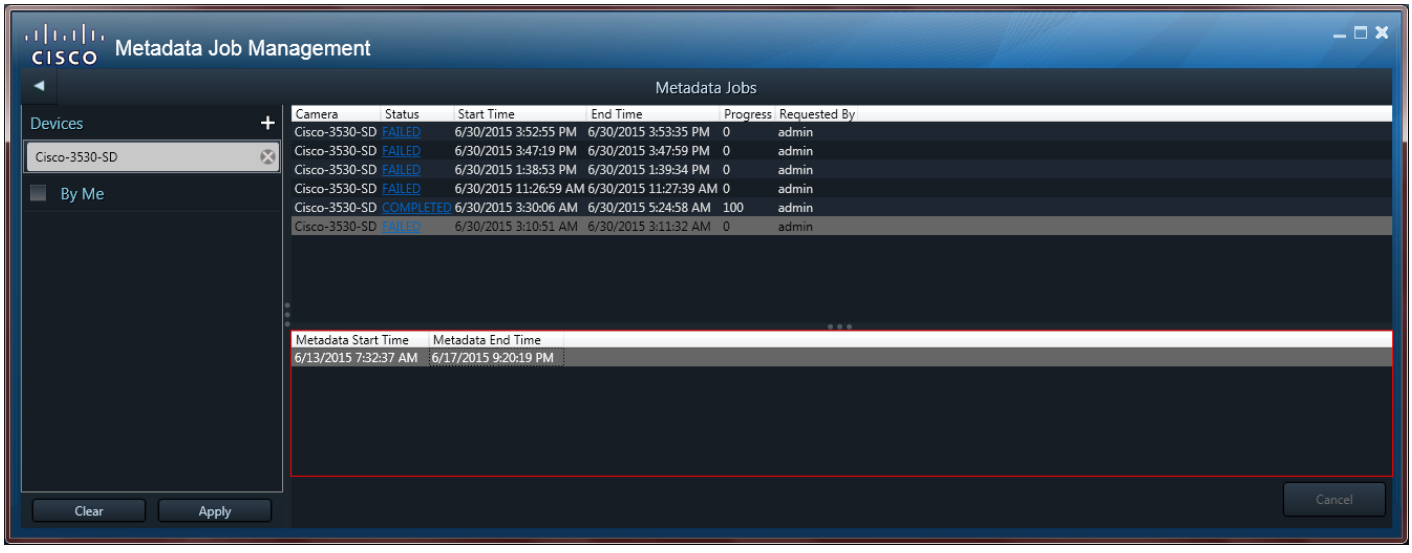
Tip: Select one or more users to narrow the results to the user(s) that triggered the jobs.

Metadata start and stop times appear in the lower pane. As seen in Figure 63, selected failed jobs have a red box around the metadata start and stop times pane.

Step 3 (Optional) Select a job and click **Cancel** to cancel the metadata job.

Note: Failed and complete processes cannot be canceled.

Figure 63 Metadata Job Management



Usage Notes

- Up to 5 metadata jobs can run at a time. Additional jobs are queued and begin when another job completes, fails, or is canceled.

- In this release, only one metadata request is allowed per camera until the metadata generation completes for the last request. A new request from that camera can then be processed (see Metadata Job Management, page 152).

Job Information

Metadata jobs include the following information:

- Name—The camera that created the recording.
- Status—The current job status (for example, started, completed, or failed).
- 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.
- Requested By—The Cisco VSM user who initiated the job.
- Metadata Start Time—The start time in the video recording of the metadata.
- Metadata End Time—The end time in the video recording of the metadata.

Camera Local Recording Management

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. For example, use this feature when the recording camera is out of network range.

Note: Camera Local Recording Management is not supported using the Cisco SASD Advanced Video Player or Cisco SASD Federator applications

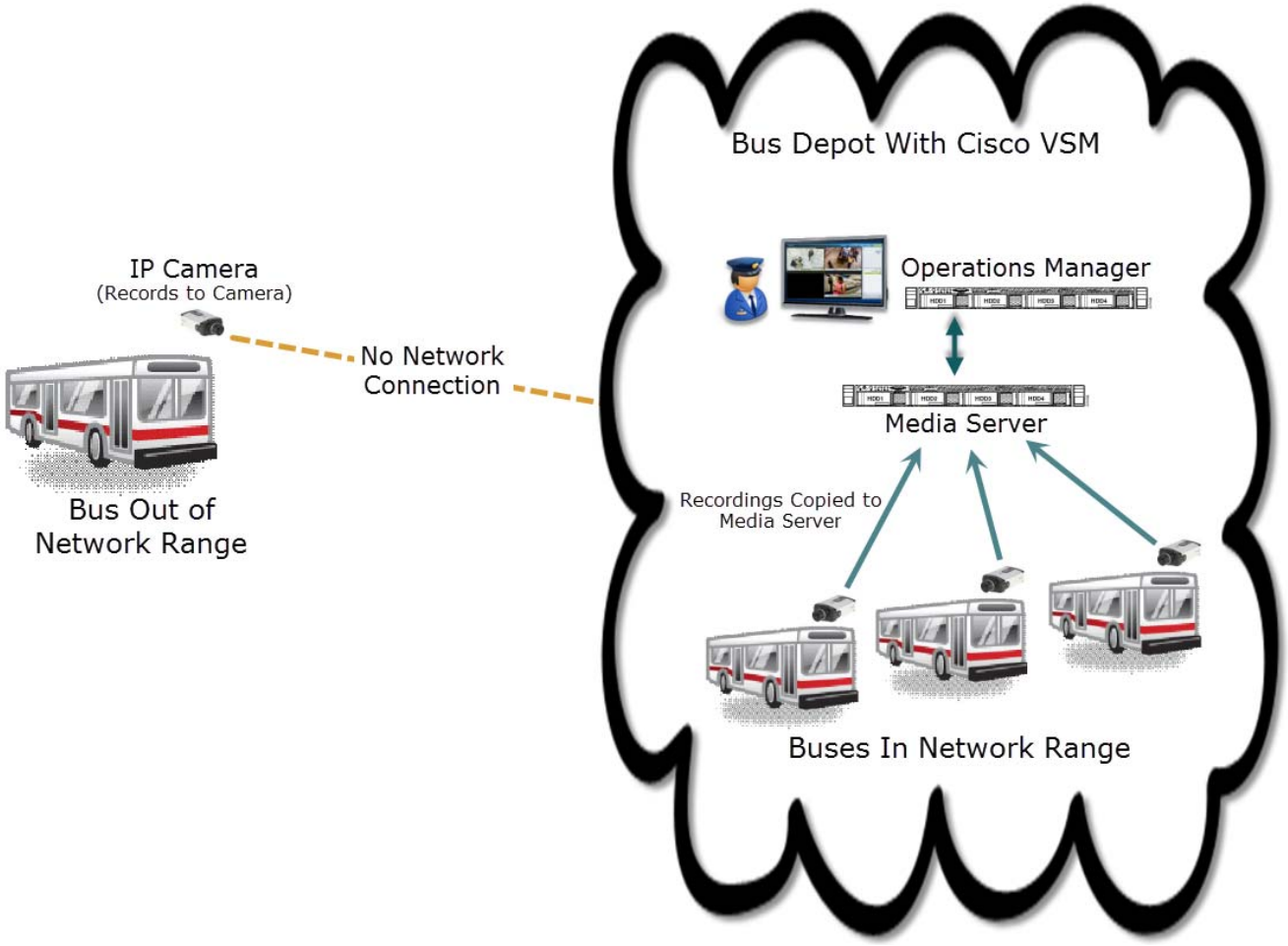
This section covers the following topics:

- Requirements, page 158
- Camera Local Recording Management Window, page 159
- Copying Video From a Camera to a Server, page 161
- Viewing Camera Storage Job Status, page 162

The example in Figure 64 shows a bus equipped with an IP (network) camera that is saving video recordings even when the bus is in transit. When the bus returns to the depot and is in network range, the recordings automatically upload (copy) to the Media Server that supports the camera.

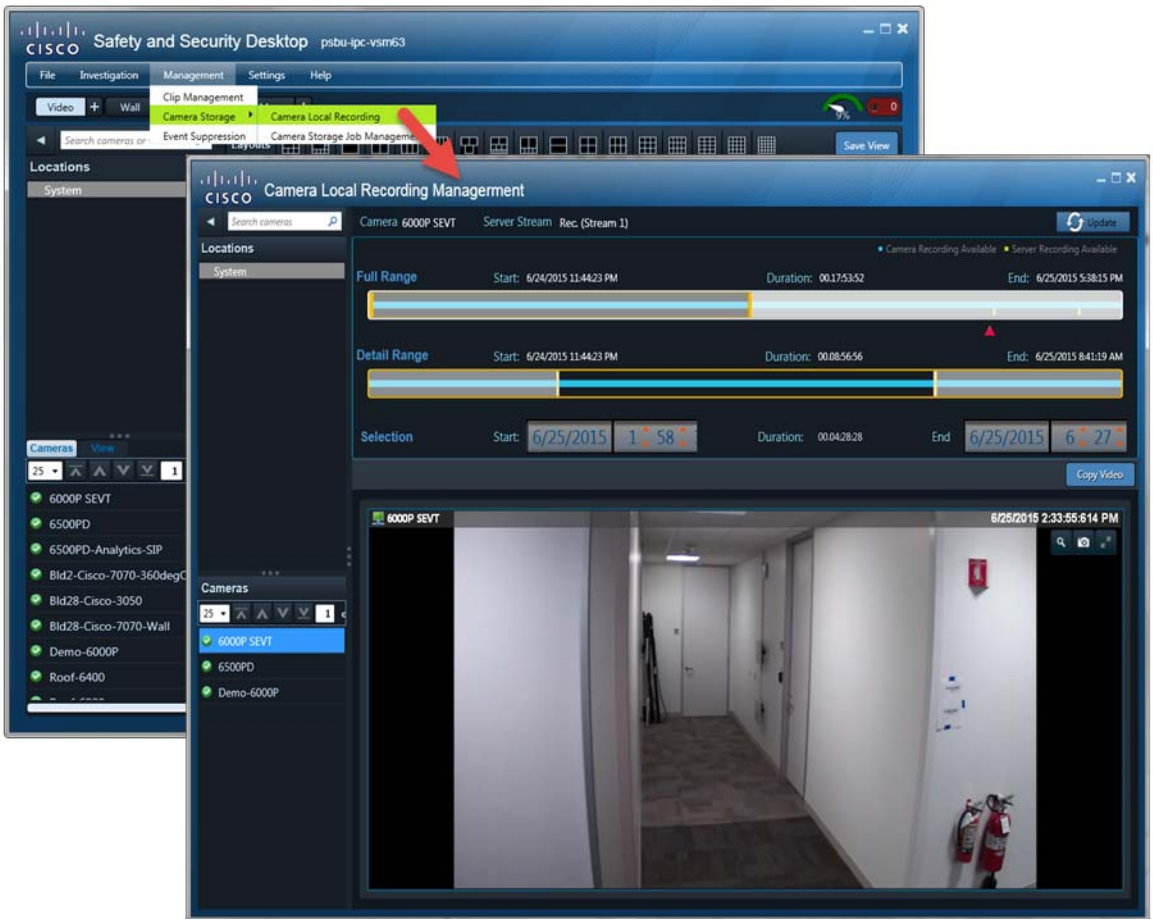
The Cisco VSM administrator uses the Operations Manager to define the recording schedule and if recordings automatically upload to the Media Server when the device joins the Cisco VSM network.

Figure 64 "Connected Edge Storage": Camera Recording on Device and Copy to a Media Server



You can use the Cisco SASD Camera Local Recording Management feature to manually copy recordings from the camera to the Media Server for viewing and analysis (Figure 65). You can view video already copied to the server, identify the video on the camera not yet copied, and copy additional video to the Cisco Media Server.

Figure 65 Camera Local Recording Management Window



See Camera Local Recording Management Window, page 159 and Copying Video From a Camera to a Server, page 161 for more information.

Note: You can play the video on the server, but not video that exists only on the camera.

Tip: Any user with Operations Manager permissions can manually copy video using the Operations Manager.

Requirements

Table 22 lists the requirements for enabling local camera recording.

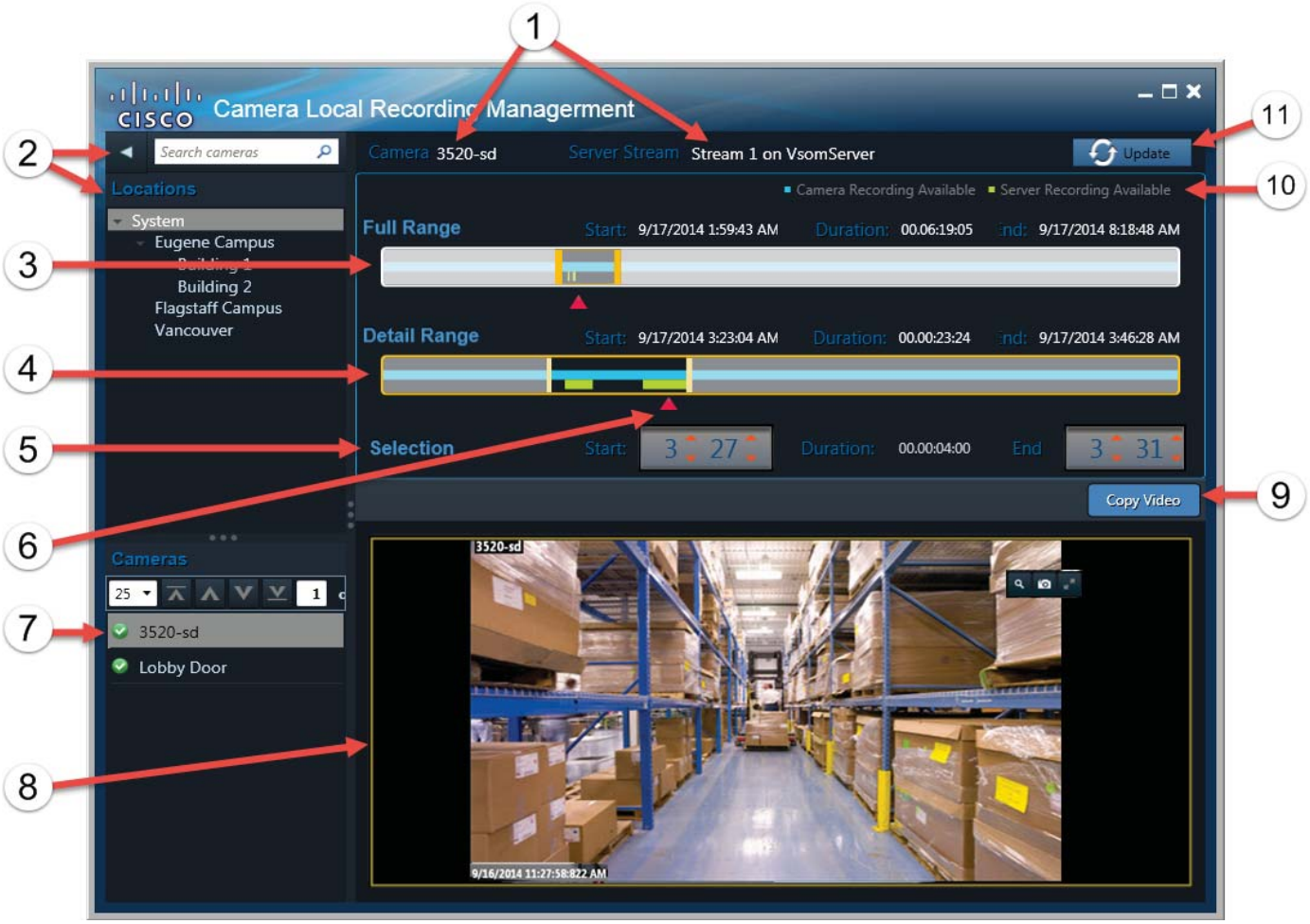
Table 22 Requirements

Requirements	Complete? (✓)
At least one IP network camera that supports on-device video storage. You use the Operations Manager to add cameras to Cisco VSM, configure camera recording schedules, and define the rules to automatically upload camera recordings to the Media Server. See your system administrator for more information. **Related Information** • Cisco Video Surveillance Operations Manager User Guide	❑
A Cisco VSM user account that belongs to a User Group with *Manage* permissions for *Cameras* is required. See your system administrator for more information. **Related Information** • Cisco Video Surveillance Operations Manager User Guide	❑
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 66 summarizes the controls available in the Camera Local Recording Management window. See the Copying Video From a Camera to a Server, page 161 for additional instructions to use these controls.

Figure 66 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. You can only play video copied to the Media Server. 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 a camera onto the viewing pane to view available recordings on that device.
8	Recording video feed from the selected camera stream. • Use the video area to watch the video after it is copied to the server (shown as a green bar in the timeline). • Any recording segments not yet copied to the server displays 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 begins to play from the time you release the play head. If video is not available on the server for the selected time, 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 Media Server. • Only video that is not already on the server is copied (that is, video already copied to the server is skipped). • The video begins to play after the copy is complete. • See Viewing Camera Storage Job Status, page 162 to view the copy jobs.
10	Legend—Describes the recording status in the timeline. • Green—Recording that was copied to the 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.

Copying Video From a Camera to a Server

To copy recorded video from a camera's storage device (such as an SD card) to the Cisco Media Server (Figure 66):

Step 1 Complete the Requirements, page 158.

Step 2 Log in to the Cisco SASD application.

See Logging In, page 15.

Note: Camera Local Recording Management is not supported using the Cisco SASD Advanced Video Player or Cisco SASD Federator applications.

Step 3 Select **Management > Camera Storage > Camera Local Recording** (Figure 65).

Step 4 Select a location, and drag a camera into the management window (Figure 66).

Note: An error message appears if the camera does not support local recording storage. See Requirements, page 158 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 in the Detail Range (Figure 66).

Step 6 Use the Detail Range to select a span of video to copy from the camera to the server.

Tips:

- Use the Start and End settings to fine-tune your selection.
- Use the red play head to play video that was previously copied to the Media Server.

Step 7 Click **Copy Video** to start copying.

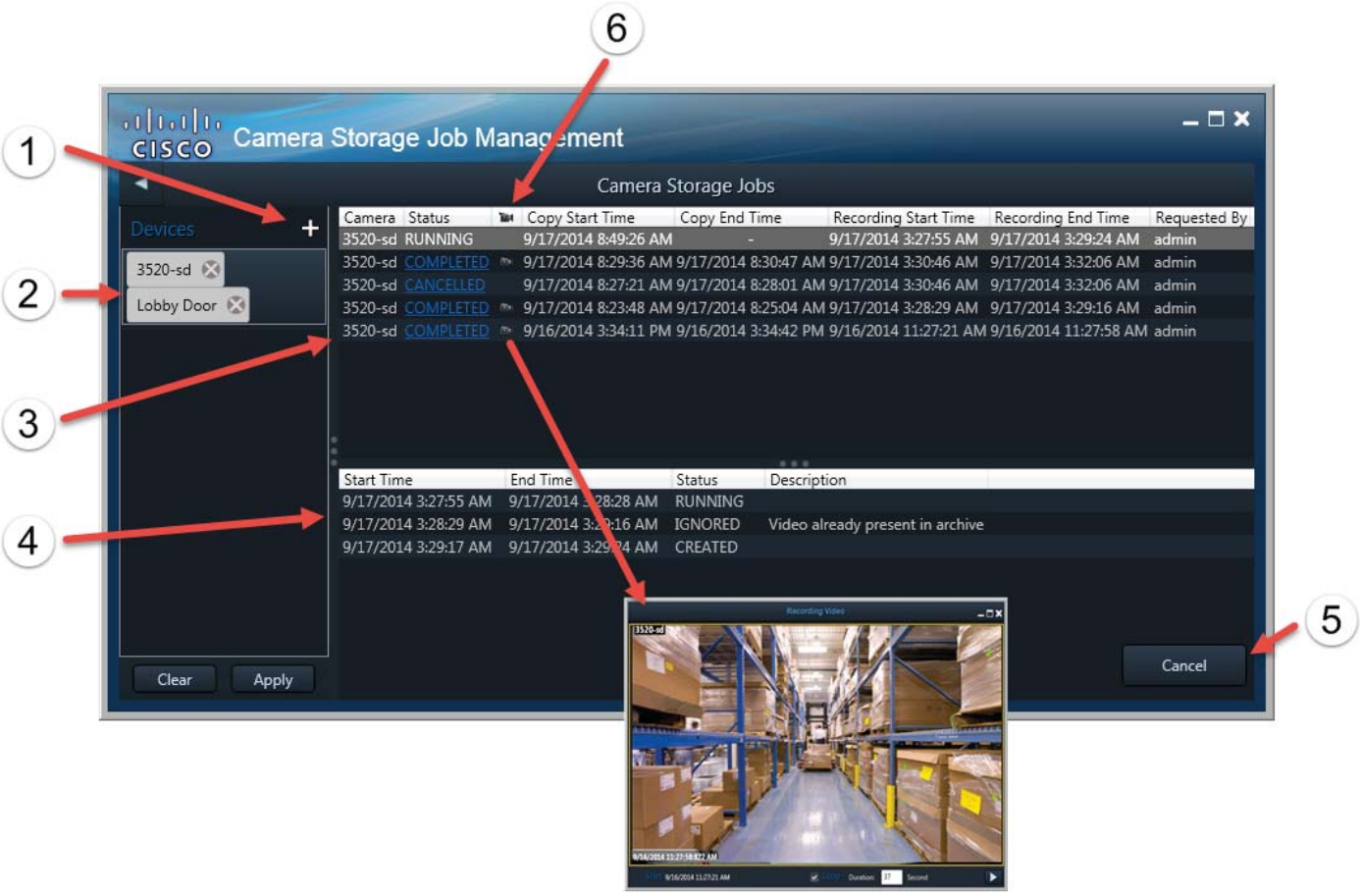
- Any video already on the Media Server is skipped.
- The selected video plays after the copy operation completes.

Step 8 (Optional) Use the Camera Storage Job Management page to view copy job status (see Viewing Camera Storage Job Status, page 162).

Viewing Camera Storage Job Status

Select **Management > Camera Storage > Camera Storage Job Management** (Figure 67) to view the status of camera storage copy jobs triggered in Cisco SASD.

Figure 67 Camera Storage Job Management



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

3	Camera storage jobs. Select a job to view the sub-jobs. The following information displays: • Camera—The camera where the recording is stored. • Status—The job status, such as Completed, Running, or Canceled. • —Double-click to play the video copy in a popup 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—Video copy job created, but has not started. • Running—Video copy job in progress. • Completed—Video successfully copied from the camera to the Media Server. • Canceled—Video copy job canceled by the user. • Failed—Video copy job failed. • 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 displays for each portion of the selected video. For example, if a video copy job includes previously copied portions or portions that still need to be copied, a separate sub-job displays for each action. **Note:** Video copy jobs can successfully complete even if sub-jobs display another status. For example, if a sub-job is ignored, it can mean that a portion of the video was skipped because it was already copied to the server or is not available. The overall job can still complete even though some (or all) of the video was ignored. • Created—Sub-job was created, but has not started. • Running—Video copy job in progress. • Completed—Video successfully copied from the camera to the server. • Canceled—Video copy job canceled by the user. • Failed—Video copy sub-job failed. • Ignored—Video copy sub-job for a portion of the video was skipped. The job successfully completes 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 completes, fails, or is canceled.
- Only one copy request per camera can be processed at a time.

Copy Camera Recordings From Alerts

You can copy camera recordings directly from an alert (Figure 68). This is useful to copy and view only the video related to a specific Security event such as a motion stop or start event.

Note: You can copy video for any Security alert or event where the camera has local storage.

Figure 68 Copying Camera Recordings from an Alert

To copy camera recordings directly from an alert:

Step 1 Select the **Alert** workspace (see Alert Workspace, page 43).

Step 2 Select the desired filters to narrow the results, and then click **Apply**.

For example, select the **Security** category to display only security alerts, such as motion stop and start events.

See Alert Workspace, page 45 and Understanding Events and Alerts, page 44 for more information.

Step 3 Select a Security alert.

Note: Recordings can only be copied from security alerts.

Step 4 Right-click an event for that alert, and select **Copy Camera Recording** (Figure 68).

Step 5 Enter the copy settings:

- Camera—(Read-only) The camera name.
- Prior to Event—(Optional) Amount of video to copy before an event is triggered. To modify the value, enter the desired number of seconds. A default value populates automatically.
- Duration—(Optional) Total amount of video to copy. To modify the value and copy more or less video than occurred for the event, enter the desired number of minutes. The event duration populates automatically.
- Start—(Read-only) The start time for the video to copy.
- End—(Read-only) The end time for the video to copy.
- Display Job Status—(Optional) Select to display the video copy job status (Figure 68).
- Play Video After Job Complete—(Optional) Select to play the video segment in a separate window after the video copy job completes (Figure 68).

Step 6 To save the copy settings, click **OK**.

Step 7 (Optional) Use the playback controls (see Viewing Live Video, page 80) to view the event video copied from the camera (Figure 68).

- 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

The Cisco SASD Federator allows users to view video from multiple instances of the Operations Manager (Figure 69).

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. You can also use this browser-based interface to view the system health of Operations Manager servers. See your system administrator for more information.

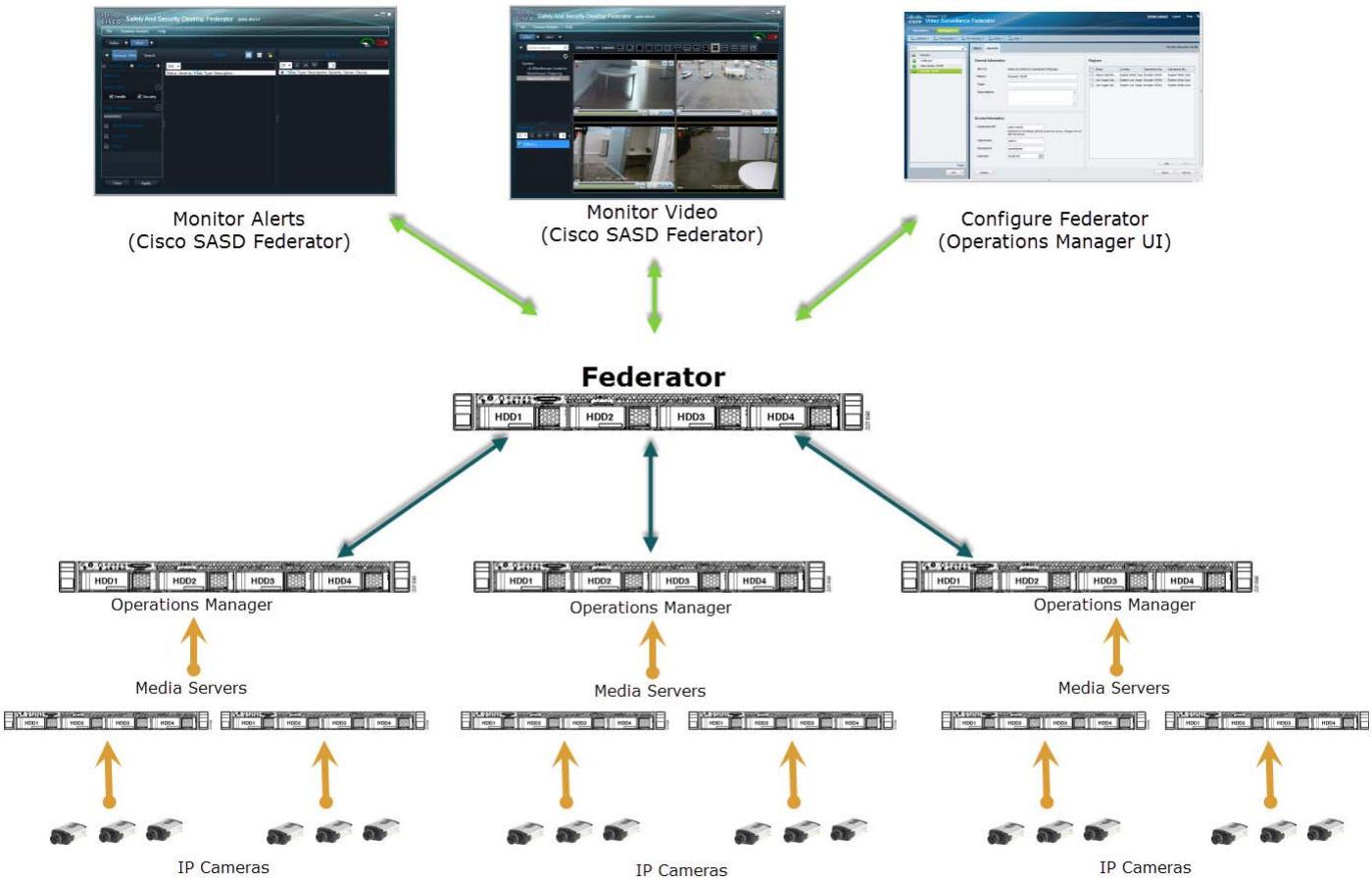
This section contains the following topics:

- Federator Requirements, page 169
- Logging In to Cisco SASD Federator, page 170
- Monitoring Video Using Federator, page 171
- Monitoring Alerts Using the Cisco SASD Federator, page 174

Notes

- Federator resources and regions are configured using the Cisco VSM Federator browser-based interface.
- Federator user access to Operations Manager locations is based on their access permissions in Federator.
- Each Federator supports up to 500 instances of the Operations Manager.
- Federator requires a different username and password than Cisco SASD. See your system administrator for more information.

Figure 69 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 open instances of the Operations Manager (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 INSTALLATIONS

- 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 allows central office users to log in and simultaneously access video from the Operations Manager in each warehouse.
- Another company manages casinos in different regions of the country. Cisco SASD Federator allows operators to monitor video in all regions. For example:
  - Security personnel can monitor video from the casino floors in different locations, even though 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

Use the checklist in Table 23 to ensure that your installation meets the minimum requirements for your Federator installation.

Table 23 Federator Requirements

Requirements	Complete? (✓)
At least one Federator server must be installed and configured on the network. **Note:** The Federator server must have Regions configured that map Operations Manager locations to Federator locations. See your system administrator for more information.	❑
The IP address or hostname of the Federator server.	❑
A valid Federator server username and password. **Notes** • The default credentials for a new or factory restored server is **admin/admin**. • The username and initial password for all other users are defined when the user account is created (see the Cisco Video Surveillance Operations Manager User Guide for more information). • You will be prompted to enter and re-enter a new password on first login or when your password expires. Follow the onscreen prompts. • To change your password at other times, you must log in to the browser-based Cisco Video Surveillance Federator.	❑
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** You can monitor Federator resources (video) 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 are defined when the user account is created (see the Cisco Video Surveillance Operations Manager User Guide for more information).
- You will be prompted to enter and reenter a new password on first login or when your password expires. Follow the onscreen prompts.
- To change your password at other times, to you must use the browser-based Federator interface.
- 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.
- Federator user accounts are different than Cisco SASD user accounts. You cannot use Cisco SASD credentials to access the Federator.

To log in to Federator:

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.
- On first-time log in, you are prompted to change the password.

Step 2 Enter the Federator hostname or IP address.

Figure 70 Cisco SASD Federator Login Screen

Step 3 Enter your Federator username and password.

c. Select a Domain, if necessary.

d. Enter a new password, if prompted.

e. 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.

Monitoring Video Using Federator

Federator users can access video streams from all 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 Manager locations in a single layout by dragging cameras onto the video display grid.
- Federator users can load the Views defined in different Operations Manager locations.
- 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.

  Note: Camera search is not supported across multiple Operations Manager locations.
- If a camera becomes disabled, you must manually trigger a refresh of the Cisco SASD Federator UI (for example, by moving to a different location and then moving back) for the camera's disabled status to be reflected correctly.

To use the Cisco SASD Federator to monitor video:

Step 1 Log in to the Cisco SASD Federator application.

See Logging In to Cisco SASD Federator, page 170.

Step 2 Select a Federator location (Figure 71).

Locations display the cameras for the associated Operations Manager locations based on Federator Regions.

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

To search for cameras, you must first select a location.

Step 4 (Optional) Select a layout (for example, **2x2**).

Step 5 Drag cameras onto the available video panes or select a pane and double-click the camera name to display video from the camera.

Figure 71 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 **Management > Clip Management** to view, download, and manage MP4 clips saved on the server.

See Clip Management, page 133 for more information.

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

See Thumbnail Search, page 127 for more information.

Monitoring Alerts Using the Cisco SASD Federator

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 Operations Managers to the Cisco SASD Federator. See Sending Operations Manager Alerts to Cisco SASD Federator, page 174 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.

This section contains the following topics:

- Sending Operations Manager Alerts to Cisco SASD Federator, page 174
- Viewing Alerts, page 176

Sending Operations Manager Alerts to Cisco SASD Federator

You can view alerts generated by an Operations Manager in Cisco SASD Federator if they are sent to the Federator server using one of the methods listed in Table 24.

Table 24 Methods to Send Alerts to the Federator

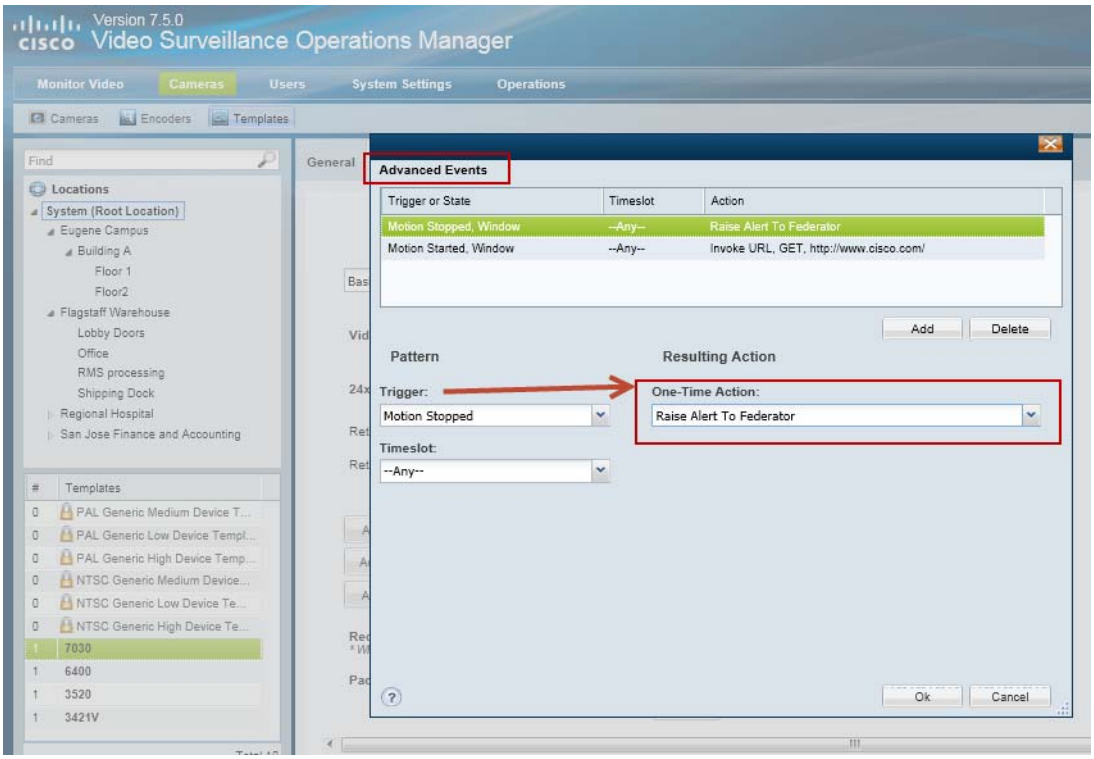
Method	Description
Device health alerts (automatic)	Cisco SASD Federator device health alerts. **Note:** Only Operations Manager reachability alerts display in the Cisco SASD Federator (Figure 73).
Security alerts (automatic)	Security alerts can be automatically sent to the Cisco SASD Federator when an event occurs. **Tip:** Create an Advanced Event in the Operations Manager (Figure 73) to automatically send alerts to 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 send alerts to Cisco SASD Federator according to a schedule, the alerts continue to update 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 Federator	Right-click the alert in Cisco SASD and select **Send to Federator**.

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 72 an Advanced Event is created that automatically sends an alert to the Federator when a motion event occurs.

Figure 72 Setting Advanced Events in Cisco Video Surveillance Operations Manager



In Figure 73, Cisco SASD is used to manually send an event to the Federator.

Figure 73 Manually Send Alerts to Federator Using Cisco SASD

Viewing Alerts

To view alerts in Cisco SASD Federator:

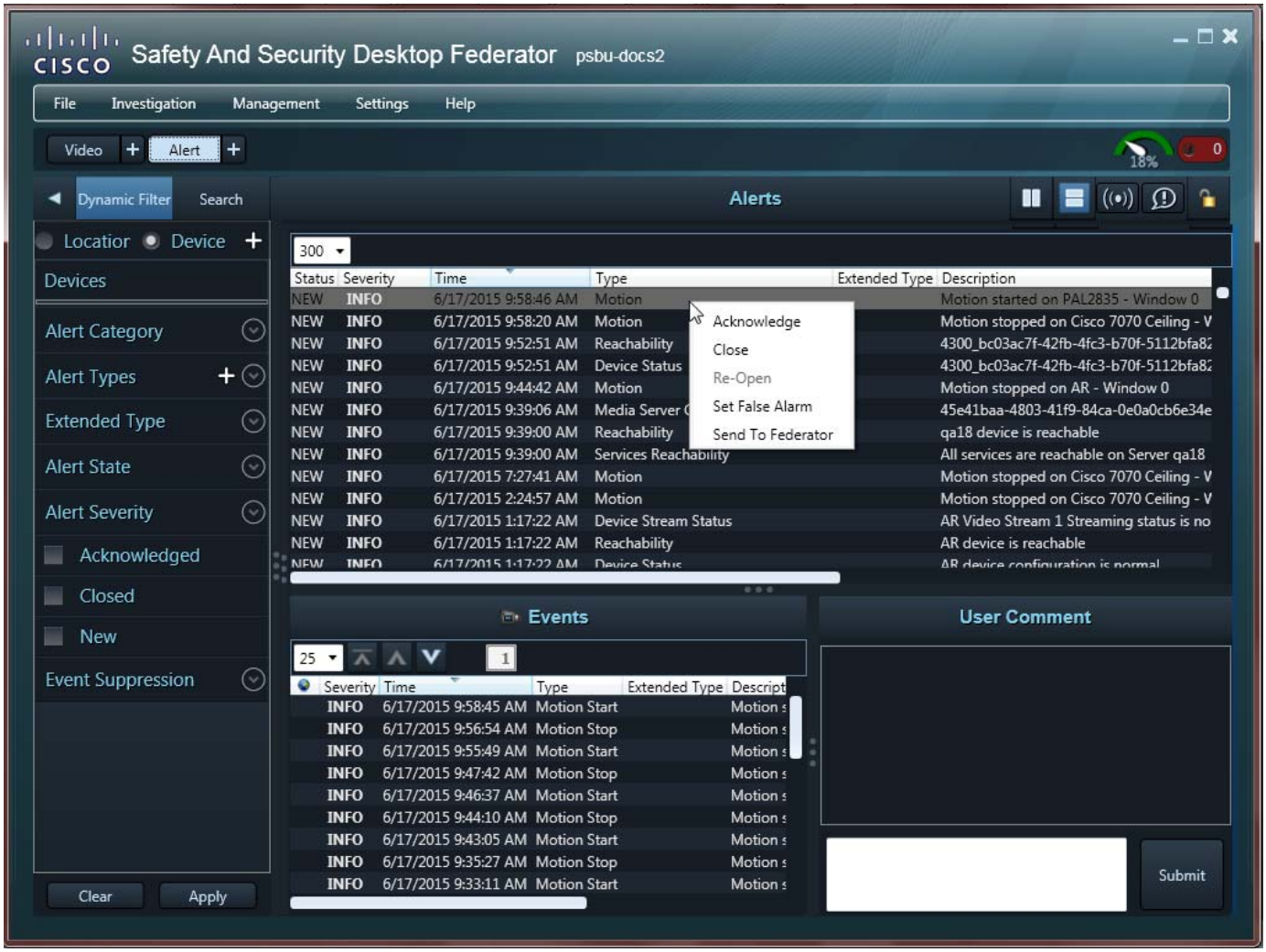
Step 1 Log in using your Cisco SASD Federator credentials.

Step 2 Select the Alert workspace (Figure 74).

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 74 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. Click **Search** again to refresh the 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 75).

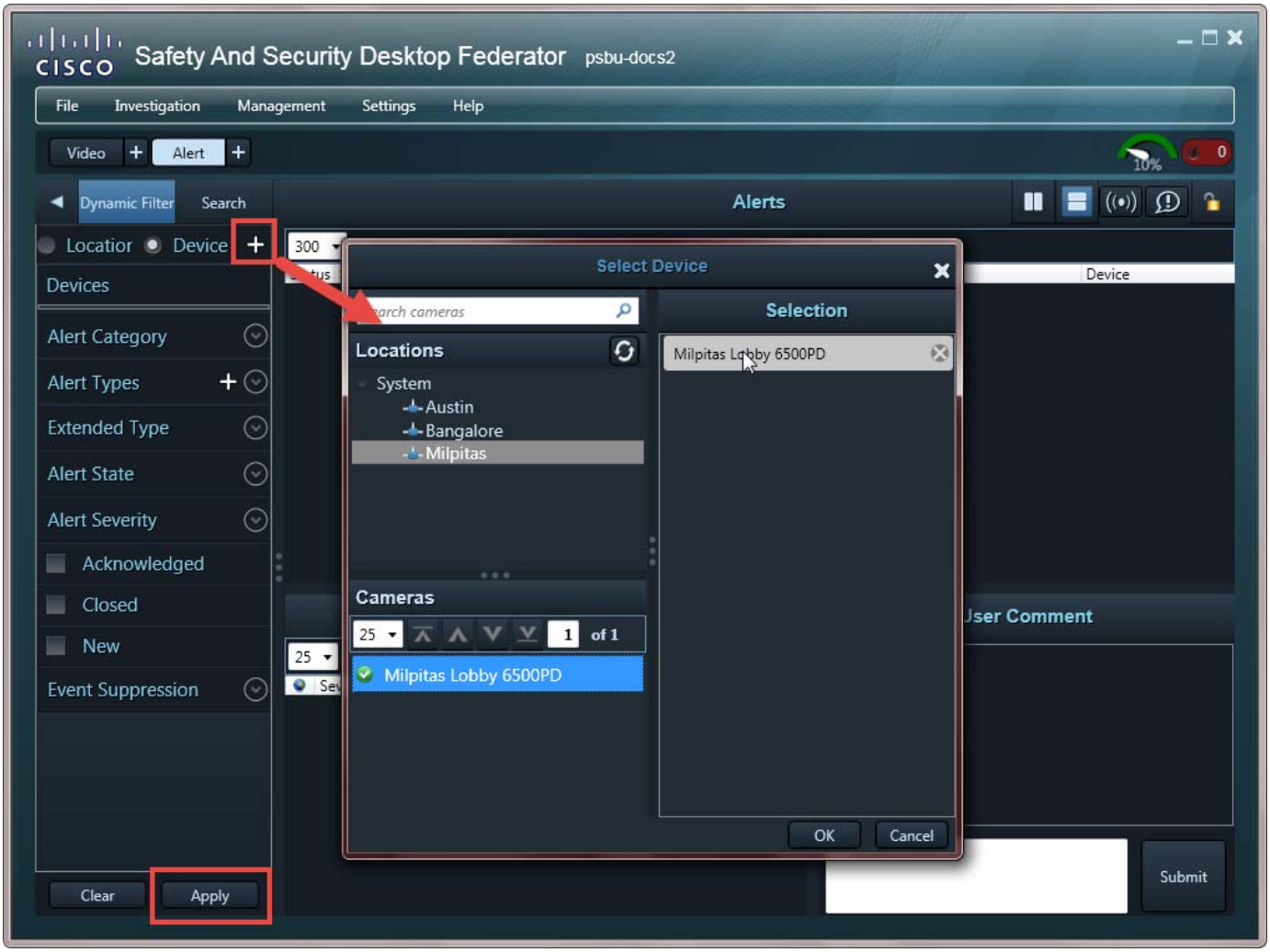
- **Location**—Click to select a Federator location (Figure 75) where the alert(s) were created.

  Only alerts from that location display.

  Note: Federator Locations represent a location tree in an Operations Manager.
- **Device**—Click to select a location and a specific device (camera).

Only alerts from that device display.

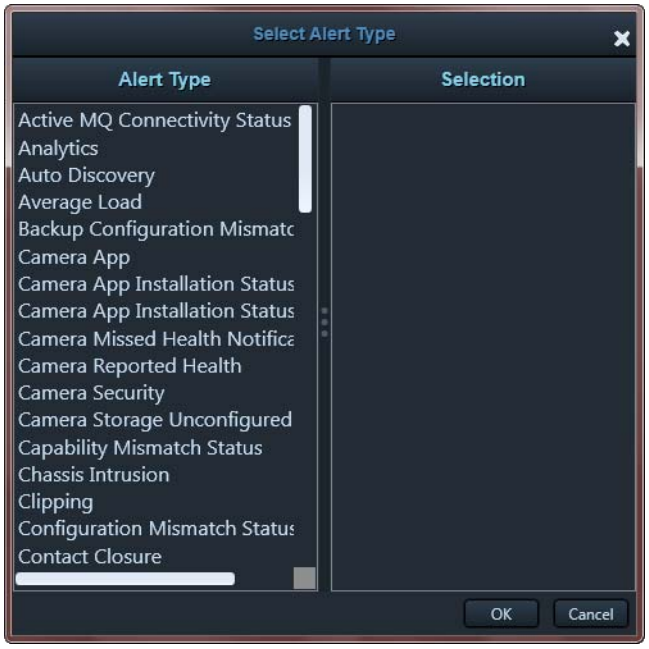
Figure 75 Cisco SASD Federator Locations



- **Time**—(Search only). Select a span of time.

  Only alerts generated during that time display (for example, Today or Month).
- **Alert Category**—Health or Security.
- **Alert Type**—Click + to select the type of alert that appears in the results (for example: Capability Mismatch Status, Contact Closure, Camera Storage Unconfigured, and so on, see Figure 76).

Figure 76 Select Alert Type Dialog Box



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

- **Alert Severity**—Select the alert severity filter: 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.
- **Event Suppression**—Select from the options to:
  - Exclude suppressed alert
  - Only include suppressed alert
  - Include all

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, page 43.

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 25 lists changes between the different versions of Cisco SASD.

Table 25 Revision History

Release	Document Revision Date	Change Summary
Release 7.7	August 2015	Added the following sections and topics: • Event Suppression, page 67 • Using On-Demand Recording, page 95 • Synchronizing Video Playback in Multiple Panes, page 102 • Using 360° Camera Controls, page 109 • Dewarp Mode, page 110 • Event Recording Analysis, page 117 Revised the following sections and topics: • All UI screen shots updated to reflect Release 7.7 menu structure. • Edit sweep of entire document.
Release 7.6	December 2014	Added the following sections and topics: • Camera Local Recording Management Revised the following sections and topics: • Video Workspace • Alert Workspace • Map Workspace • Controlling Video Playback • Related Documentation

Table 25 Revision History (continued)

Release	Document Revision Date	Change Summary
Release 7.5	February 2014	Added the following sections and topics: • Getting Started • Wall Workspace • Using the Cisco SASD Wall Configurator • Clip Management • Motion Video Analysis • Using the Cisco VSM Federator Revised the following sections and topics: • Video Workspace • Alert Workspace • Map Workspace • Controlling Video Playback • Thumbnail Search • Related Documentation
Release 7.2	August, 2013	• Added the "Viewing a Thumbnail Summary of Video Archives" section. • Various minor edits and revisions.
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 the 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.