



# Release Notes for Cisco Video Surveillance Manager, Release 7.10

---

Revised: November 29, 2017



Note

---

Always refer to the [latest online version of these Release Notes](#) for up to date information.

---

This document provides important information for Release 7.10 of the Cisco Video Surveillance Manager (Cisco VSM).

This document includes the following sections:

- [What's New in Release 7.10, page 2](#)
- [Getting Started, page 22](#)
- [Released Versions, page 24](#)
- [Supported Devices, page 25](#)
- [Clipping Support By Application, page 45](#)
- [Obtaining and Installing Licenses, page 46](#)
- [Understanding the Cisco VSM Software Types, page 48](#)
- [Obtaining Cisco VSM Software, page 49](#)
- [Caveats, page 51](#)
- [Related Documentation, page 52](#)



# What's New in Release 7.10

Cisco VSM Release 7.10 includes the following new features and enhancements:

- [Health Dashboard Improvements](#), page 2
- [Display Text and Time in a Cisco Camera's Video View](#), page 4
- [Save Alert Filters in Cisco SASD](#), page 5
- [Security Event Notification by Camera](#), page 7
- [Storage Retention and Recording Dashboard](#), page 8
- [Mark and Search Video Streams Using Cisco SASD](#), page 15
- [Support for Cisco and Vivotek Cameras, and Axis Encoder](#), page 17
- [Exclude Padding from On-Demand Recordings](#), page 18
- [Support for Additional Axis Cameras and Encoders](#), page 18
- [Support for JRE 1.8](#), page 19
- [Get Custom Resolution API](#), page 19
- [Covert Cameras](#), page 20
- [Supported SSL cipher algorithms](#), page 20
- [Other Improvements](#), page 21

## Health Dashboard Improvements

The Health Dashboard has been enhanced to provide an overall snapshot of the servers, cameras and encoders in your deployment. You can view overall information, information about a specific device, or the estimated number of cameras that can be added to a Media Server, and other information.

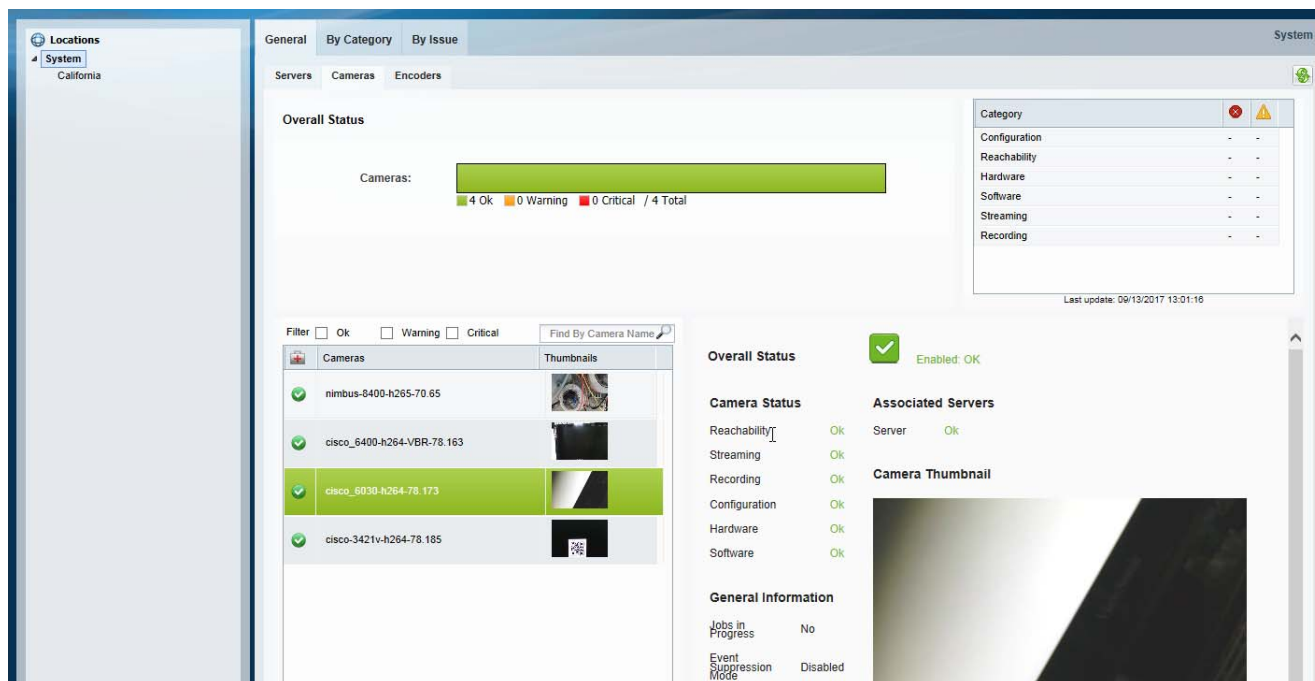
- 
- Step 1** Click **Operations** > **Health Dashboard** ([Figure 1](#)).
  - Step 2** Choose a location to view a summary of the health issues at that location, including its sub-locations.
  - Step 3** Click the **General** tab.
  - Step 4** Select the Servers, Cameras or Encoders tab for more information.
- 

**Note**

Only camera specific templates are supported when calculating the number of cameras can be added.

---

**Figure 1 Health Dashboard: General Tab**



## Servers

The Overall Status is a graphical representation of the servers at the selected location including the device health status.

Select a server to view additional details, including:

- Storage—The total storage and used storage on the server.
- Existing Camera Count—The number of cameras currently added on the server.
- Server Type—VSOM/ Primary Media Server/ Map Server/ Metadata Server.
- Location—The location where this server is installed.
- Camera Estimation—The approximate number of camera's that can be added on this Media Server. Select a pre-defined device template. The camera count is estimated based on the template's recording configurations and the free space available on the selected server.  
**Note:** Estimated camera count is calculated based on the valid file types and formats (.smd, .mp4) stored in the /media repository. If the media repository contains unsupported file types, then the space consumed by these files will not be factored in while calculating the estimated cameras that can be added. In addition, if the recordings for certain cameras are shelved, then the algorithm will consider the space occupied by the recordings of those cameras until the time the recording state was moved to shelved. If the recording state of those cameras are altered at a later date, then "Camera Count" estimation will have to be re-run or else going with the old camera estimated count will have an impact on the number of cameras that can be added, and could result in recordings getting groomed.

## Cameras

The Overall Status is a graphical representation of the cameras at the selected location including the device health status.

Select a camera to view additional details, including:

- Camera Status—The status including Reachability, Streaming, Recording, Configuration, and other information.
- General Information—The running jobs.
- Large thumbnail—A larger thumbnail of the camera's live stream.

## Encoders

The Overall Status is a graphical representation of the device at the selected location including health status.

Select a device to view additional details, including:

- Encoder Status—The status including Reachability, Configuration, and other information.
- General Information—Running jobs.

## Display Text and Time in a Cisco Camera's Video View

You can now display custom text or a timestamp in the camera's live and recorded video view. This information allows users to better identify the camera and current time and date.



### Note

This feature is supported by Cisco cameras only.

**Step 1** Log on to the Operations Manager.

**Step 2** Click **Cameras**.

**Step 3** Select a camera.

**Step 4** In the **General > Settings** tab, enter the following **Text Overlay** settings (Figure 2).

- Overlay placement—Display the text or time at the top or bottom of the video image.
- Enable Date/Time Display—Select or deselect to display or hide the timestamp.
  - Date/Time Alignment In Overlay—Select Left/Center/Right.
- Enable Text Display—Select or deselect to display or hide the text.
  - Text Alignment In Overlay—Select Left/Center/Right.
  - Display Text—Enter the text to be displayed in the camera's video view. A maximum of 26 characters are allowed. Enter only letters and numbers. Special (such as spaces and dashes) characters are not allowed.

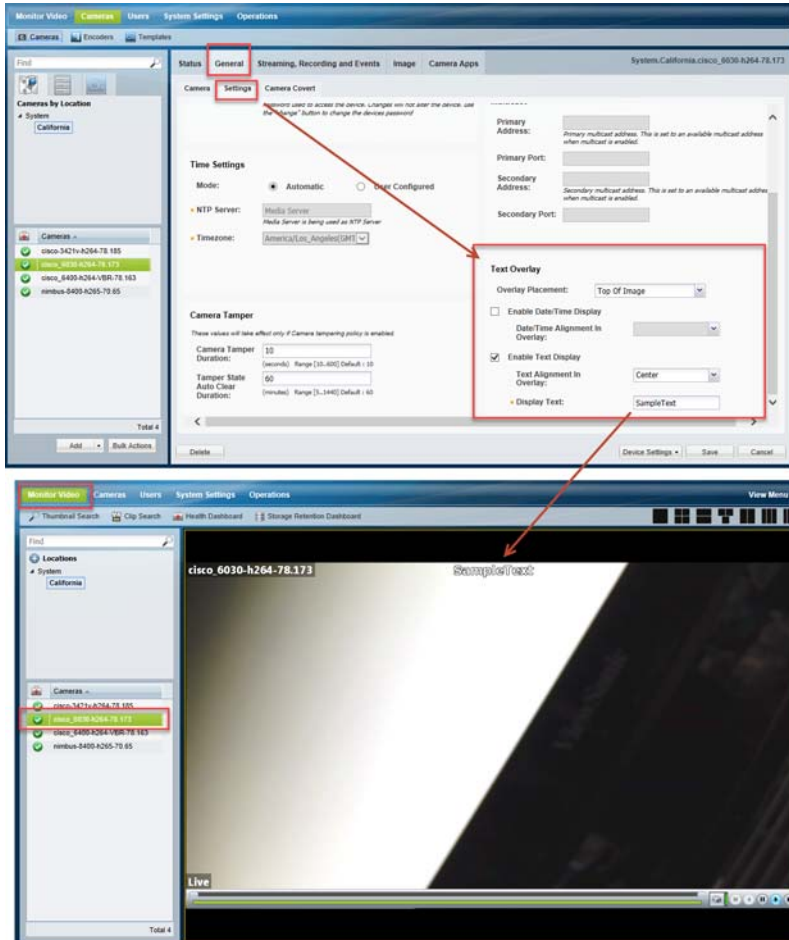
**Step 5** Click **Save**.



### Tip

Use bulk actions to apply the settings to multiple cameras. Go to **Cameras > Bulk Actions** and filter the results. Select one or more Cisco Cameras and click **Bulk Actions > Camera Settings**. Create a setting with a text overlay or select an existing setting.

Figure 2 Text Overlay



## Save Alert Filters in Cisco SASD

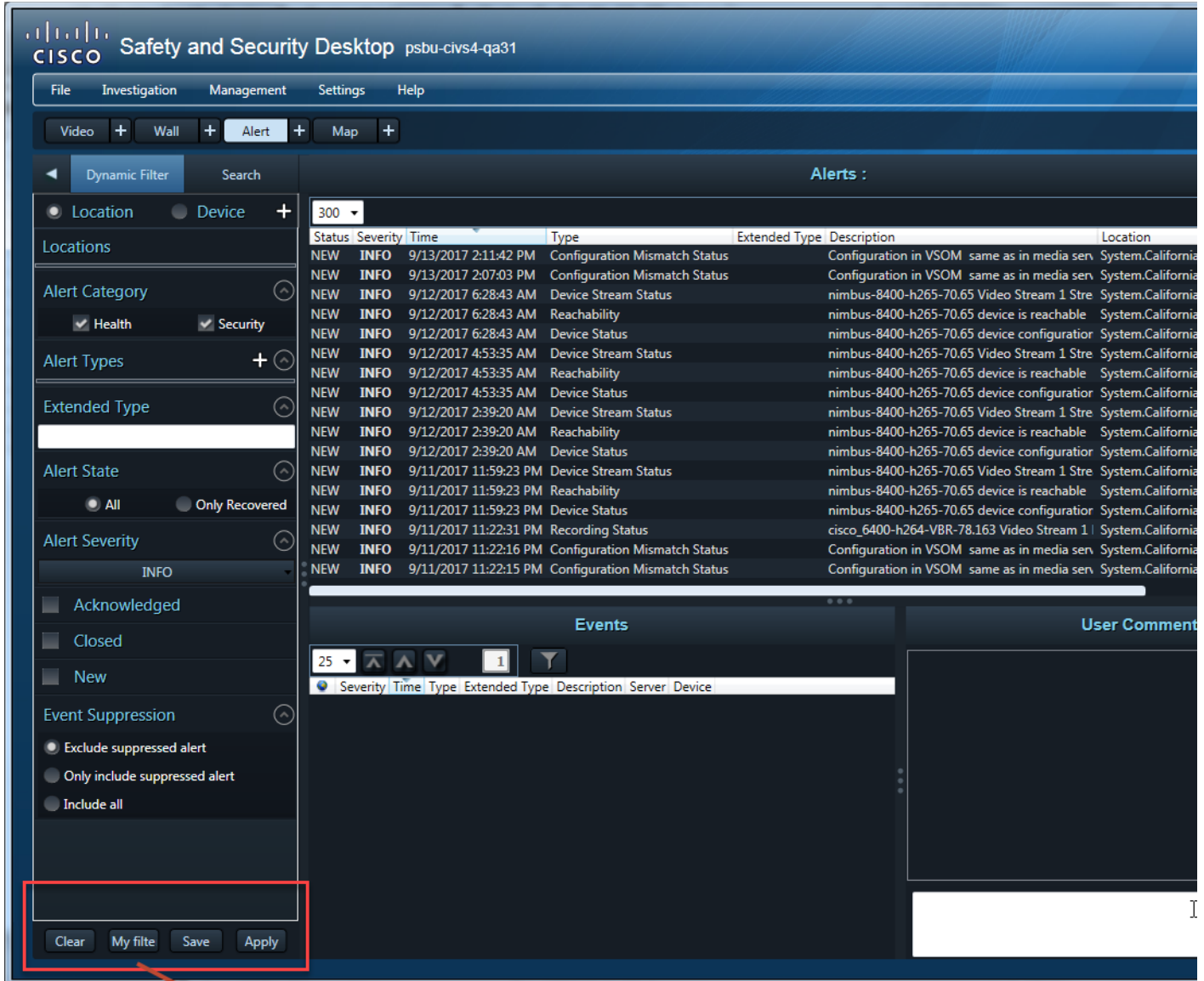
You can save alert filters for future use in Cisco SASD, allowing you to quickly perform the same search.

### Create a new filter

- Step 1** Launch the Cisco SASD application and log in.
- Step 2** Select the **Alert** workspace (Figure 3).
- Step 3** 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.
- Step 4** Click **Save** to save the filter for future use.
- Step 5** Enter a filter name and click **Save**.
- Step 6** Click **Apply**.

**Step 7** Click **My Filters** to view and select a previously saved filter.

**Figure 3** Saved Filters in Cisco SASD



**Tip**

To rename or delete a saved filter, click **My Filters** and select the edit icon. Change the name and click **Apply**, or click **Remove**.

**Modify an existing filter**

To edit an existing filter:


- 
- Step 1** Select the **Alert** workspace ([Figure 3](#)).
  - Step 2** Click **My Filters**, select a filter and click **Apply**.
  - Step 3** Modify the filter settings and click **Save**.
  - Step 4** You will be prompted to modify the existing filter or save the settings as a new filter.
- 

## Security Event Notification by Camera

Alert Emails (Notification Policies) can now be created for cameras, allowing you to create the same policy for multiple cameras at different locations.

You can also include a snapshot of the event in the email.



### Procedure

- 
- Step 1** Verify that the SMTP server settings are configured correctly in the Operations Manager server (under the **Advanced**  icon).
  - Step 2** Configure Alerts (using the Advanced Alert feature). See “Using Advanced Events to Trigger Actions” in the [Cisco Video Surveillance Operations Manager User Guide](#) for more information.
  - Step 3** Enable continuous recording on the camera(s).
  - Step 4** Select **Operations > Notification Policies**.
  - Step 5** Click **Add**.
  - Step 6** Select **Security**.
  - Step 7** For Security, select **By Camera**.
  - Step 8** Enter the notification settings.

**Table 1**      **Security Event Notification—By Camera**

Setting	Description
By Camera	Select <b>By Camera</b> to create a notification for cameras. This allows you to create the same policy for multiple cameras at different locations.
Add camera	Click <b>Select / View Camera(s)</b> to filter and select the cameras for the notification. Click <b>Search</b> to find all cameras.
Alert Type	The type of security alert. For example, Soft trigger, contact open or close, PTZ, etc.
Custom Event Type and Subtype	Select a user-created event type and subtype, if available, for Soft Trigger or Camera App alerts.

**Table 1** Security Event Notification—By Camera

Setting	Description
Capture Snapshot	Select this option to include a snapshot of the event in the email. The Media Server and camera should be time synced or a mismatch between the event and snapshot can occur.
Add Email	Add one or more email addresses. The maximum number of email recipients per notification policy is 50. We recommend using email aliases to include additional recipients. <ol style="list-style-type: none"> <li>Enter a valid email address in the <b>Add Email</b> field.</li> <li>Click the  icon (or press <code>Enter</code>).</li> <li>Add additional email addresses if necessary.</li> <li>Click the  icon to remove an email address.</li> </ol>

**Step 9** Click **Add**.

**Step 10** Create additional entries for additional locations, cameras, and recipients, if necessary.  
The maximum number of policies is 1000.

## Storage Retention and Recording Dashboard

### Overview

A new Storage Retention Dashboard displays your cameras' estimated storage requirements based on the cameras' actual bitrate. You can also configure this actual bitrate value in a camera template so Cisco VSM can more accurately estimate the associated camera's storage requirements. This ensures that Cisco VSM can utilize all available disk space for adding cameras and recording video.

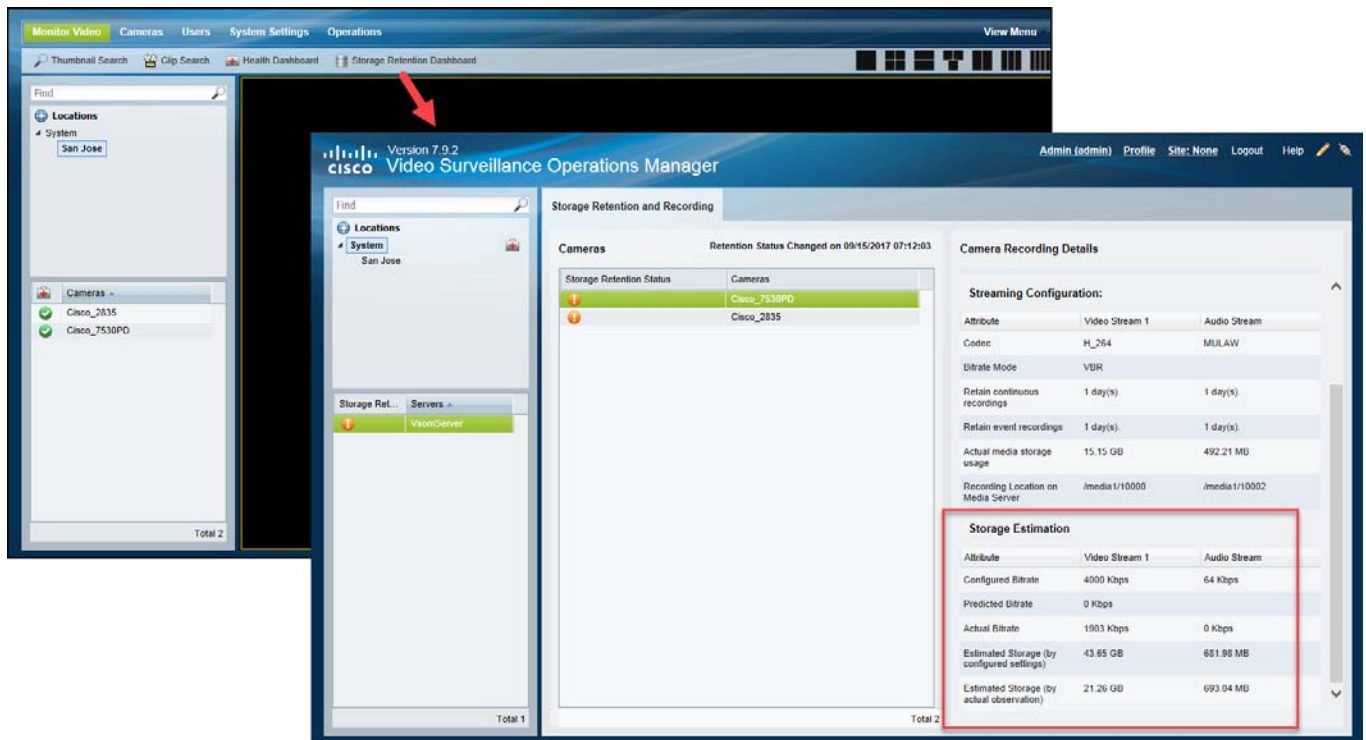
For example, the Storage Retention Dashboard in [Figure 4](#) shows that the estimated storage needed by a camera (based on the configured settings) is almost twice the estimated storage based on the actual video being recorded.

- Estimated Storage (by configured settings)—43.65 GB
- Estimated Storage (by actual observation)—21.26 GB

This is because the camera is configured for VBR, and the configured VBR bitrate used to estimate disk usage is over twice the actual bitrate being used by the camera. To correct the discrepancy so Cisco VSM can accurately estimate the camera's storage use, enter the actual bitrate in the camera template's Predicted Bitrate setting.



Figure 4 Storage Retention Dashboard



## Using the Actual Bitrate to Estimate Storage

To improve the estimated storage accuracy for your cameras, enter the actual bitrate into a camera template's Predicted Bitrate field. Cisco VSM will calculate the estimated storage capacity based on this Predicted Bitrate.

If the Predicted Bitrate field is blank, the configured CBR or VBR bitrate is used.



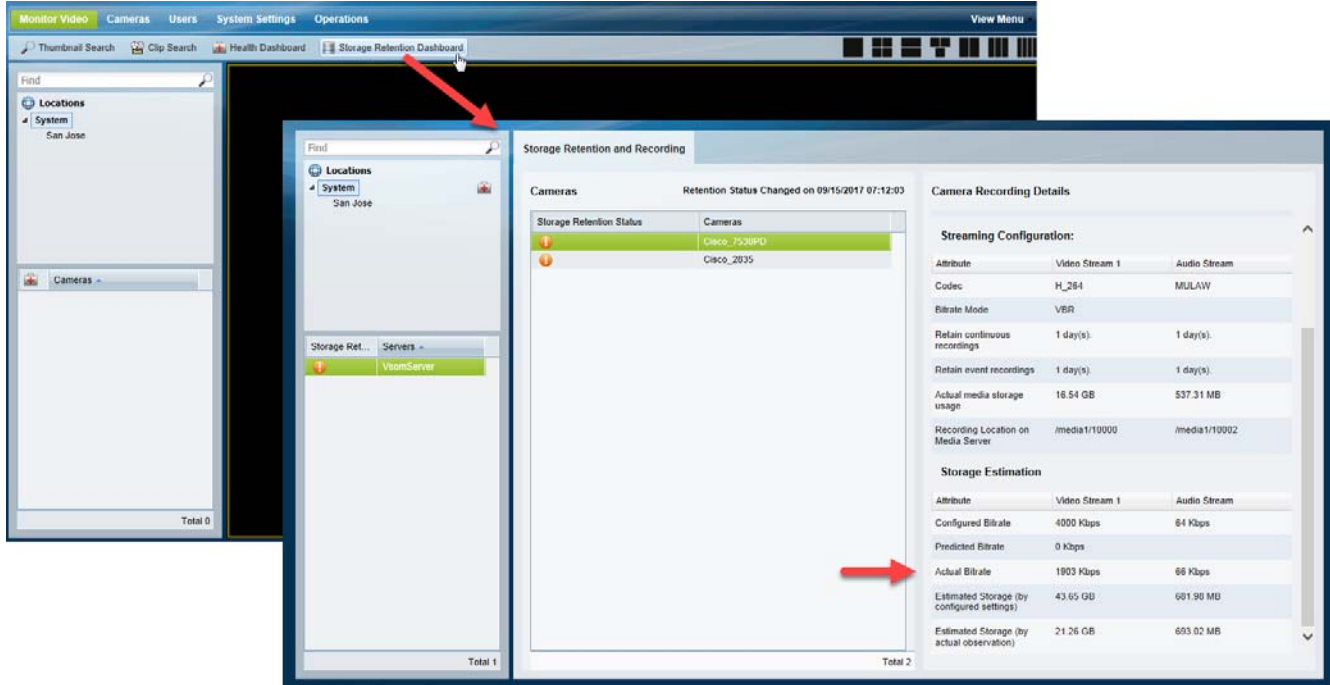
### Caution

Use the Predicted Bitrate only if you have measured the camera's average bit rate over a considerable period of time. Providing an incorrect value could either lead to records getting groomed before the retention time or restrict the number of cameras that can be added to your deployment.

### Procedure

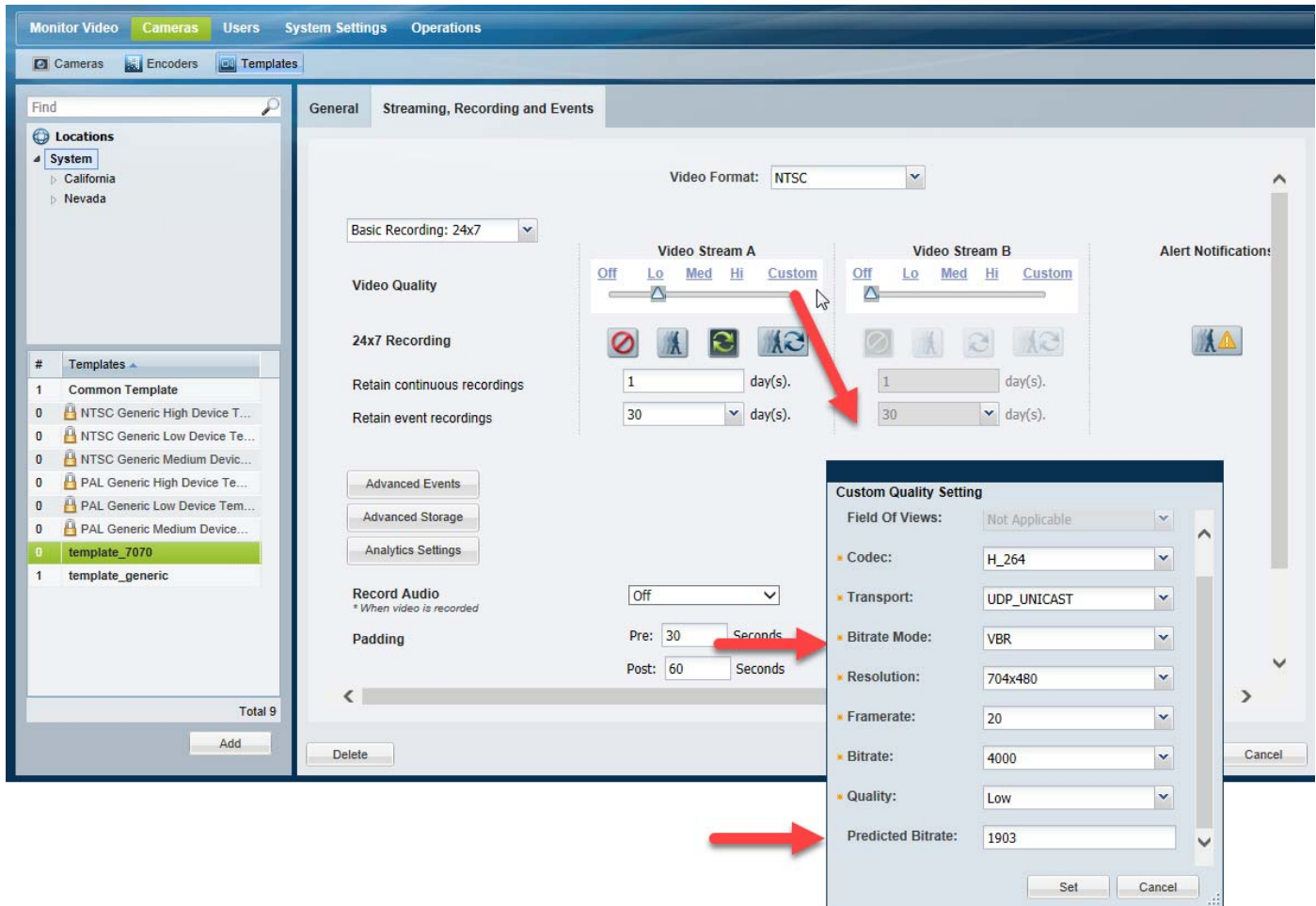
- Step 1** Copy the actual bitrate used by the camera (Figure 5).
- Click **Monitor Video**.
  - Click **Storage Retention Dashboard**.
  - Select a Media Server.
  - Select a camera.
  - Under Storage Estimation, copy the Actual Bitrate.

Figure 5 Actual Bitrate in the Storage Retention Dashboard



- Step 2** Enter the actual bitrate into the Predicted Bitrate field (Figure 6).
- a. Select **Cameras > Templates**.
  - b. Add or edit a template.
  - c. Next to Video Quality, click **Custom**.
  - d. Next to Bit rate mode, verify that VBR is selected.
  - e. In the Predicted Bitrate field, paste the actual bitrate copied from the Storage Retention Dashboard.
  - f. Click **Set**.
  - g. Click **Save**.
  - h. The estimated storage needs of the cameras associated with the template will be recalculated based on the Predicted Bitrate value.

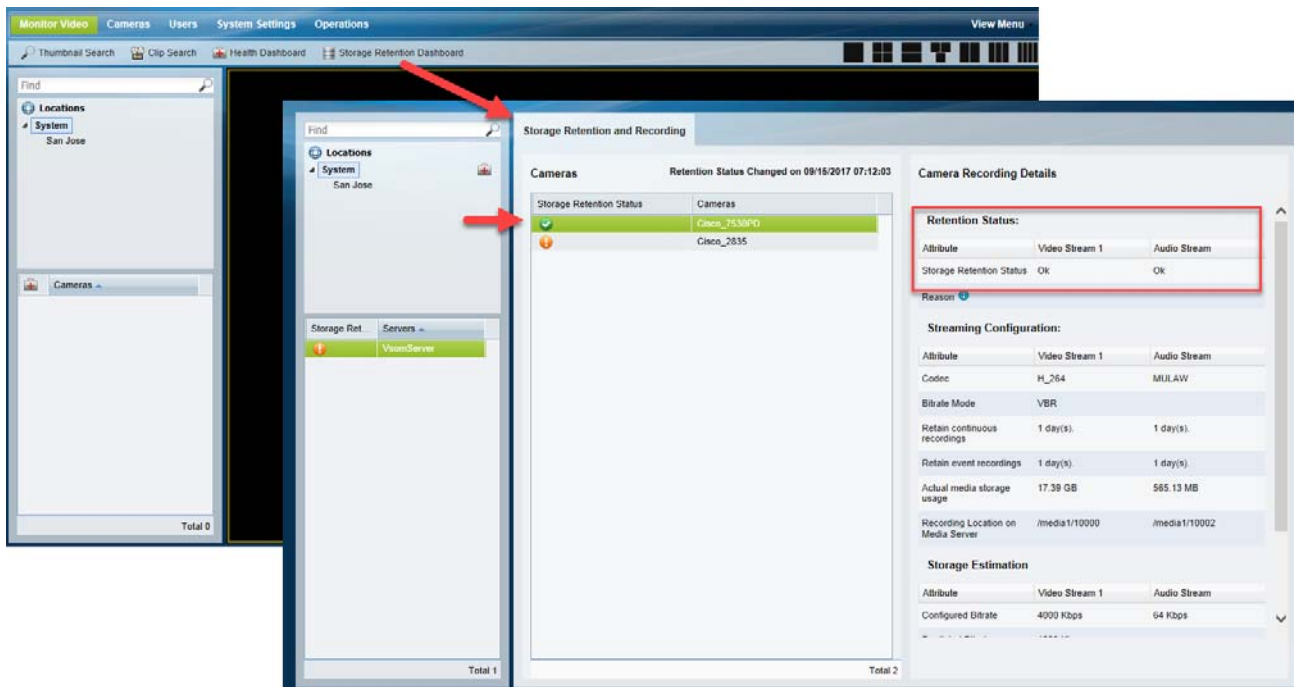
**Figure 6** Configure VBR Predicted Bitrate



**Step 3** Verify that Storage Retention Dashboard warning is cleared (Figure 7).

- a. Click **Monitor Video**.
- b. Click **Storage Retention Dashboard**.
- c. Select a Media Server and select the camera.
- d. Verify that the status icon is green.
- e. Verify that Storage Retention Status is "OK".

Figure 7 Retention Status



## View Storage and Bitrate Information in the Storage Retention Dashboard

Use the Storage Retention Dashboard to view the estimated and actual bitrates for a camera, and the estimated storage use.

- Step 1** Log in to the Cisco VSM Operations Manager.
- Step 2** Click **Monitor Video**.
- Step 3** Click **Storage Retention Dashboard**.
- Step 4** Select a Media Server and select a camera.
  - Retention Status—Warnings are displayed if the deviation goes above or below the specified percentage (defined in [Configure Storage Retention Status Warnings and Emails](#)).
  - Streaming Configuration—The camera configuration details, such as Bitrate mode (CBR or VBR) and Codec (H264 or MULAW). The actual disk space used by the camera is also displayed.
  - Storage Estimation—
    - The configured bitrate vs. the actual bitrate. The Predicted Bitrate shows a value only if entered in the camera template (see [Using the Actual Bitrate to Estimate Storage](#)).
    - The estimated storage is also displayed
  - Review details such as the “Estimated Storage (by configured settings)” vs. the “Estimated Storage (by actual observation)”. The “Estimated Storage (by configured settings)” is adjusted if a Predicted Bitrate is entered (see [Using the Actual Bitrate to Estimate Storage](#)).

## Usage Notes

- Storage retention is supported only for continuous recordings. However the user will also be able to view storage retention statistics for continuous + motion based recordings. The data will be accurate as long as the camera performs continuous recording. However when motion events occur there will be a significant deviation in the data as it is hard to predict the number of motion events.
- Retention Status Changed on *mm/dd/yyyy hh:mm:ss* indicates the last date and time stamp when the storage retention status changed for any camera associated with the selected Media Server.
- The supported Codecs are H264 (video) and MULAW (audio).
- The estimated storage is calculated every 30 minutes.
- If a camera configuration is changed, it may take some time (based on the retention period) to estimate and reflect the correct value of “Estimated Storage (by configured settings)”.
- If recording gaps or packet loss occurs during streaming, the calculated estimated storage or calculated bitrate may not be accurate.
- This feature supports cameras streaming to the Primary Media Server only. Streams to the Redundant, Failover and LTS servers are not supported.
- Cisco 8000 series cameras and Vivotek HD Outdoor IP PTZ cameras support the “Constrained bit rate” mode in VSM as CBR. This feature, together with the “Dynamic intra frame period” feature supported by the cameras, results in reduced average bit rates. In CBR mode, the “Estimated storage (by configured settings)” for these cameras might be higher than the “Estimated Storage (by actual observation)”.

## How disk space is estimated using VBR

When a camera is configured to use VBR, the disk space required by the camera is based on the VBR setting. Because camera manufacturers use the bitrate setting differently, Cisco VSM may overestimate or underestimate the amount of storage required by a camera, and prevent additional cameras from being added or other issues.

For example, most cameras use VBR to vary the bitrate depending on the actual scene the camera is viewing. The bitrate is reduced when there is little movement or change, or increased when there is more change.

However, the bitrate setting can mean different things for different camera models. For example:

- For some cameras, the VBR value is a maximum data rate that will not be exceeded. The actual data rate, however, is often far below this set value.
- For some cameras, the VBR is a target average bitrate. The actual bitrate varies above or below the target value. On average, the camera makes a best effort to use the target bitrate.

## Configure Storage Retention Status Warnings and Emails

Storage retention warnings let you know the “Estimated Storage (by configured settings)” deviates from the “Estimated Storage (by actual observation)” by a certain percentage. This usually indicates that the actual bitrate in a camera configured for VBR is different than the configured bitrate, resulting in an inaccurate storage estimation.



### Note

Storage retention status warning are informational only, and do not affect or represent the health of the camera.

To determine when a warning is displayed in the Storage Retention Dashboard, enter the amount of deviation (as a percentage) between the actual and estimated storage for each video codec (Figure 8).

Email notifications can also be sent if this percentage is exceeded.

**Figure 8** Storage Retention Settings

The screenshot shows the 'Storage Retention Settings' page in the Cisco VSM Operations Manager. The page is divided into several sections:

- Navigation:** Monitor Video, Cameras, Users, **System Settings** (highlighted with a red arrow), and Operations.
- Sub-navigation:** Devices, Shared Resources, System.
- Tabs:** General, Password, Language Settings, Alerts Severity, and **Storage Retention Settings**.
- Codec Settings:**
  - Codec:** mulaw
  - Actual to Estimated Storage Deviation (%):** 10
  - Codec:** h264
  - Actual to Estimated Storage Deviation (%):** 10
- Add Email:** A text input field with a green plus sign icon.
- Instructions:** Please add email addresses using the "Add Email" field above.

### Procedure

- 
- Step 1** Log in to the Cisco VSM Operations Manager.
  - Step 2** Choose **System Settings > Settings**.
  - Step 3** Click **Storage Retention Settings**.
  - Step 4** **Actual to Estimated Storage Deviation percentage (%)**—Enter a percentage value for each supported codec (MULAW and H264). The dashboard will display a ‘Warning’ for cameras that deviate above or below the specified percentage.
  - Step 5** **Add Email**—Enter the email addresses where warnings should be sent if the deviation between the actual and estimated storage exceeds the defined percentage.
  - Step 6** Click **Save**.
-

## Mark and Search Video Streams Using Cisco SASD

This feature, called Bookmarks in Cisco SASD, allows an operator to mark live and recorded video streams whenever an event or incident happens. You can create these bookmarks for either a location or a particular camera. Operators can mark the events for something they may have spotted or viewed as important.

The users can search the bookmarks by providing the names or browse through bookmarks by location and view the event again without the need for creating a clip. These bookmarks, can be viewed by any user with “view recording” permissions; which makes it easy to share.

For example, if a security gets a call that a purse was lost in a store, or a car was damaged in a parking lot, they can quickly create a bookmark for an approximate time and date that is tied to the general location (all cameras at that location, or to a specific camera).

Cisco SASD bookmarks allow an operator to manually mark important events in the real time video stream.



### Note

The Cisco SASD Advanced Video Player, SASD Federator, and Cisco SASD Wall Configurator do not support this feature.

## Create a Bookmark

### Procedure



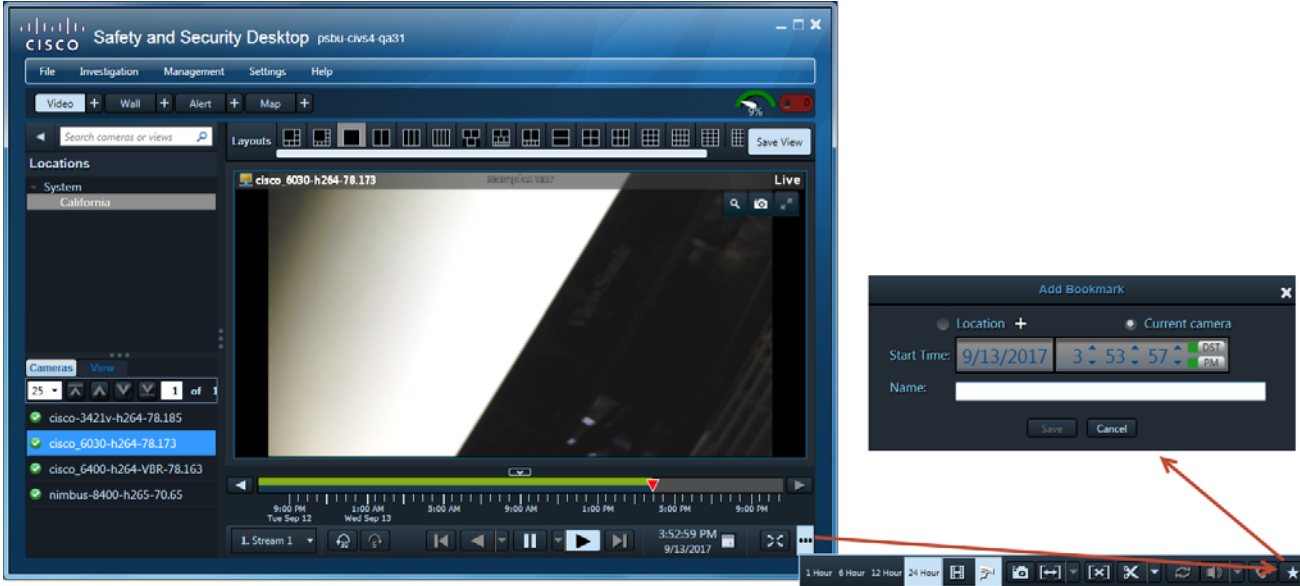
- 
- Step 1** Launch the Cisco SASD application and log in.
  - Step 2** Select the **Video** workspace (Figure 9).
  - Step 3** While viewing video, click  and then .
  - Step 4** In the Add Bookmark window, the current camera is selected by default.
    - a. (Optional) Select a location instead, if necessary, to create a bookmark for all cameras in that location.
    - b. (Optional) Adjust the start date and time, if necessary.
  - Step 5** Enter the bookmark name.
  - Step 6** Click **Save**.
-

Figure 9 Create a Bookmark



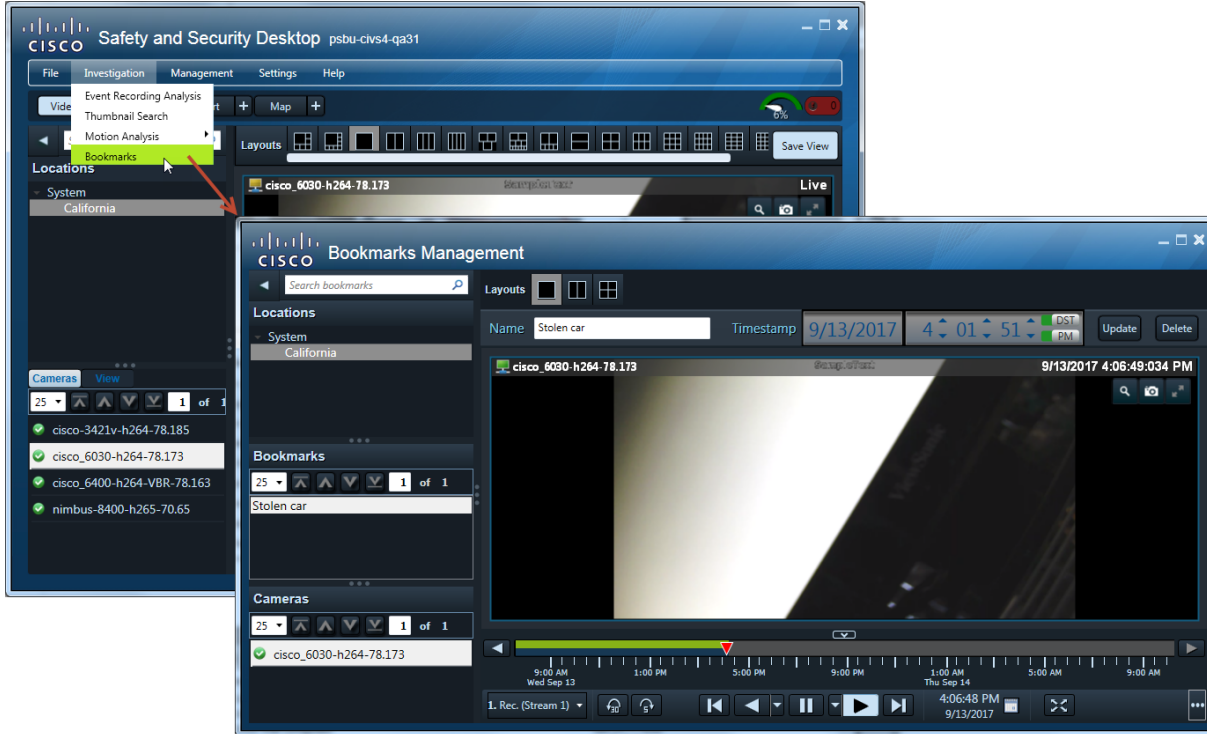
## Open a Bookmark

### Procedure

- 
- Step 1** Launch the Cisco SASD application and log in.
  - Step 2** Select **Investigation > Bookmarks** menu (Figure 10).
  - Step 3** Select a location to view all of the bookmarks in that location, or enter a name in the **Search bookmarks** field.
  - Step 4** Select a bookmark to display the cameras associated with the bookmark.
  - Step 5** Double-click a camera to see the bookmarked video for that device.
  - Step 6** (Optional) Use the following additional options:
    - a. Name—Change the bookmark name.
    - b. Timestamp—Change the bookmark start time.
    - c. Click **Update** to save the settings.
    - d. Click **Delete** to delete the bookmark.
  - Step 7** Use the additional playback controls to create clips or view the video.
-



**Figure 10**      **Open a Bookmark**



## Support for Cisco and Vivotek Cameras, and Axis Encoder

The following cameras and encoders are supported in this release. See the [Supported Devices](#), page 25 for more information.

### Cameras

- Cisco CIVS-IPC-8000P
- Cisco CIVS-IPC-8020
- Cisco CIVS-IPC-8030
- Cisco CIVS-IPC-8400
- Vivotek SD9361-EHL
- Vivotek SD9362-EH/EHL

### Encoder


- AXIS F44 (Encoder)

## Exclude Padding from On-Demand Recordings

Beginning with Release 7.9.1, administrators can specify if on-demand recordings in Cisco SASD excludes additional time (padding) before and after the selected recording time.

For example, when padding is enabled, additional recording is added before and after the user click start and stop. If padding is disabled, only the recording time selected by the user is included.

To enable or disable padding:

- 
- Step 1** Log in to the Cisco VSM Operations Manager.
- Step 2** Edit or add a template to enable or disable padding:
- a. Select **Cameras > Templates**.
  - b. Click **Add** to create a new template or select a location and template name.
-  **Note** System defined templates are locked and cannot be modified.
- 
- c. Click the **Streaming, Recording and Events** tab.
  - d. Next to On-Demand Recording, select **Enable**.
  - e. Check or uncheck **Disable Padding**.
  - f. Click **Create, Save** or **Save As**.
  - g. Wait for the *Job* to complete.
- Step 3** Add cameras to the template if necessary.
- a. Select **Cameras > Cameras**.
  - b. Select the camera.
  - c. Select **Streaming, Recording and Events**.
  - d. Click **Set Template** and select the template where padding is disabled, if necessary.  
Tip: You can also click **Custom** to create a custom template for a single camera.
  - e. Click **Save** to save the camera settings.
- Step 4** When Cisco SASD users select on-demand recording, the recording will include or exclude additional video based on the camera settings.
- 

## Support for Additional Axis Cameras and Encoders

The following cameras and encoders are supported in this release.

See the [Table 12](#) and [Table 13](#) in [Supported Devices: Axis, page 32](#) for more information.

### Cameras

- Q6000E
- Q6052E PTZ

- P3707-PE

#### Encoders

- Q7436
- P7214
- P7224 Blade
- Q7424-R Mk II
- Q7401

## Support for JRE 1.8

Release 7.10 includes Java Runtime Environment (JRE) 1.8 to address security vulnerabilities in previous JRE releases.

## Get Custom Resolution API

The `getThumbnails` Operations Manager API includes a new `customResolution` option to extract a thumbnail image with a specified resolution.

Request format:

```
{
  "request": {
    "cameraRef": {
      "refUid": "someString_2",
      "refName": "someString_2",
      "refObjectType": "vs_multiPaneLayout",
      "refVsomUid": "someString_2"
    },
    "recordingCatalogEntryUid": "someString_1",
    "numThumbnails": 1,
    "forRecordings": false,
    "startTimeInMsec": 1488353349000,
    "endTimeInMsec": 1488363534000,
    "encoding": "someString_1",
    "thumbnailResolution": "half",
    "customResolution": "1000x1200",
    "thumbnailQuality": "medium",
  }
}
```

Input parameters:

- **cameraRef**—CameraReference object for the camera for which snapshot is to be returned
- **forRecordings**
  - **True** if snapshot is to be fetched from recorded stream.
  - **False** if snapshot is to be fetched from Live stream.
- **startTimeInMsec**—Start Time of image.
- **endTimeInMsec**—End time of image.
- **encoding**—"base64" - currently only base64 encoding is supported.
- **Recording Catalogue Entry**—This field is specific to recording stream for cameras.

- **resolution**—resolution of the output JPEG image
  - **full**—Full resolution of the image will be returned in the output. e.g. If the camera Stream is configured with a resolution of 1280 x 720, the resolution of the output image will be 1280 x 720
  - **half**—Half resolution image will be returned in the output. e.g. If the camera Stream is configured with a resolution of 1280 x 720, the resolution of the output image will be 640 x 360
  - **quarter**—Quarter resolution image will be returned in the output. e.g. If the camera Stream is configured with a resolution of 1280 x 720, the resolution of the output image will be 320 x 180
- **customResolution**—Enter a custom for the image, such as 1000x1200.
- **thumbnailQuality**—low, high, or medium.

## Covert Cameras

If a user is monitoring a video stream in Cisco SASD or Operations Manager, and the stream is switched to covert mode, the message “Attempting to Reconnect” is displayed (previously, the view would switch to the next available stream).

If a user is monitoring recorded video in Cisco SASD or Operations Manager, and the stream switched to covert or un-covert mode, the video will switch to the live video stream. If a user tries to reload the recording stream, however, the message “Failed to load Camera feed. Error message 401 Unauthorized” is displayed.

## Supported SSL cipher algorithms

The following SSL cipher algorithms are supported. Contact your Cisco support representative for assistance to modify the cipher options, if necessary.

**Table 2** Supported Algorithms

Algorithm	Strength
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	Strong
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	Strong
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	Strong
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	Strong



**Tip**

By default, Cisco VSM supports all algorithms except RC4 and MD5. [Learn more](#) about the need for strong algorithms.

## Android and iOS Limitations

The following limitations apply after enabling strong ciphers on Android or Apple iOS.

- Cisco VSM Viewer is supported on Android version 5.0.2 (Lollipop) and higher.
- Cisco VSM Viewer is supported on iOS version 9.0 and higher.

## Windows 7 Limitations

The following Cisco VSM Operations Manager features do not work when strong ciphers are enabled on Windows 7.

- Clip creation.
- Pan, tilt, and zoom (PTZ) actions on the **Monitor Video** page and in a camera's **Image > PTZ** tab.
- Motion window configuration. You can set the motion window but cannot view the configured motion window.
- Photographic controls.

**Note**

---

Basic streaming capabilities such as viewing live or recorded videos and snapshots continue to work.

---

## Other Improvements

- Maps uses OpenStreetMap by default for new installations. For existing upgrades from previous releases, you must manually change the default map provider.
- Security and performance enhancements.
- In **Operations > Reports**, added new reports for All Users and Templates reports.
- The 32 bit ActiveX client is depreciated after Release 7.10. The 64-bit client will be used for future releases. See [Enabling 64-Bit Video Monitoring using Internet Explorer \(IE\)](#) for more information.
- The Operations Manager works as a Single Page Application (SPA) on supported browsers for faster UI rendering. Supported Browsers are Internet Explorer 10 and higher, Chrome, Firefox, Edge & Safari 10 and higher.
- Cameras can be added in Cisco SASD from different locations into a Wall without losing changes, and then publish the modified View to the Wall.

# Getting Started

Cisco VSM Release 7.10 is pre-installed on new servers, can be installed as a virtual machine, or used to upgrade an existing deployment.

**Table 3** *Cisco VSM Installation and Upgrade Options*

Option	Description	Notes
Pre-installed	Release 7.10 is pre-installed in new installations on the Cisco Connected Safety and Security UCS Platform Series servers: <ul style="list-style-type: none"> <li>CPS-UCSM4-1RU-K9 and Cisco CPS UCSM4 2RU</li> </ul>	See <a href="#">Cisco Connected Safety and Security UCS Platform Series Servers, page 23</a> for more information.
Upgrade from Release 7.8, or 7.9.x	Upgrades can be performed on Cisco VSM virtual machines (VMs) and on Cisco Video Surveillance servers. Supported servers include: <ul style="list-style-type: none"> <li>Cisco Connected Safety and Security UCS Platform Series (CPS-UCS-1RU-K9 / CPS-UCS-2RU-K9 or CPS-UCSM4-1RU-K9 / Cisco CPS UCSM4 2RU)</li> </ul>	<ul style="list-style-type: none"> <li>For previous releases, upgrade to 7.8 or 7.9 first, and then upgrade to the latest release.</li> <li>Upgrades are supported on physical or virtual servers running the RHEL 6 operating system (upgrades are not supported on servers running the RHEL5 and SUSE operating systems).</li> <li>The CIVS platform is not supported and cannot be upgraded to VSM 7.7 or higher.</li> </ul> See <a href="#">Upgrading from Previous Cisco VSM Releases, page 23</a> for more information.
Virtual Machine (OVA templates)	An .OVA template file is used to install a new virtual machine (VM) instance of the server.	After an .OVA virtual machine is installed, you can use the Cisco VSM Management Console to perform future upgrades of the system software. See <a href="#">Cisco Video Surveillance Virtual Machine Deployment and Recovery Guide for UCS Platforms</a> for more information.

See the following for more information:

- [Cisco Video Surveillance Manager: Install and Upgrade Guide](#)
- [Cisco Connected Safety and Security UCS Platform Series Servers, page 23](#)
- [Upgrading from Previous Cisco VSM Releases, page 23](#)
- [Recovery/Factory Image, page 24](#)

## Cisco Connected Safety and Security UCS Platform Series Servers

Cisco VSM Release 7.10 is pre-installed on new installations of the Cisco Connected Safety and Security UCS Platform Series when ordered with the Cisco VSM software installed.

### Supported Servers

- CPS-UCSM4-1RU-K9 and Cisco CPS UCSM4 2RU

### Related Documentation

- [Cisco CSS UCS Server User Guide](#)— supported features, physical installation and setup instructions
- [Release Notes for the Cisco CSS UCS Servers](#)

### Notes

- After the server appliance is installed, see the [Cisco Video Surveillance Manager: Install and Upgrade Guide](#) to perform the initial Cisco VSM setup.
- For additional server hardware documentation, see the [Cisco UCS C-Series Server Documentation \(Roadmap\)](#).

## Upgrading from Previous Cisco VSM Releases

Cisco VSM can be upgraded using a `.zip` upgrade file that includes all required software packages. Installing the `.zip` file upgrades all components and ensures that all packages are running the required versions.

For complete instructions, see the [Cisco Video Surveillance Manager: Install and Upgrade Guide](#).

### Upgrade Notes

- Release 7.7 and later—Use the Software Management page on the browser-based Operations Manager to upgrade all of the servers in your deployment.
- Release 7.5 and earlier—Upgrades to Release 7.10 are supported only from releases 7.8 or 7.9. To upgrade from an earlier release, you must first upgrade to 7.8 or 7.9, and then upgrade to Release 7.10.



**Note** Upgrades from Release 7.2 and earlier are performed using the Management Console. See [Cisco Video Surveillance Management Console Administration Guide](#) for your release.

- Clear the cache in each user's web browser after upgrading Cisco VSM. If not cleared, the browser may attempt to use outdated content and display the error message "Operation failed: Authentication failed, this request is not allowed" until the page is refreshed.
- Always upgrade using the Cisco VSM user-interfaces. Do not perform the upgrade using the Linux CLI.

### Platform Notes

- **Release 7.0** was pre-installed on the Cisco Multiservices Platform (Cisco MSP) servers, including the CPS-MSP-1RU-K9 and CPS-MSP-2RU-K9.
- **Release 7.2 to Release 7.7** was pre-installed on the CPS-UCS-1RU-K9 and CPS-UCS-2RU-K9 Cisco CSS UCS series servers.

- The CIVS platform is not supported and cannot be upgraded to VSM 7.7 or later.
- **Release 7.7 to 7.10** is also pre-installed on the Cisco CSS UCS series servers:
  - CPS-UCSM4-1RU-K9 / Cisco CPS UCSM4 2RU




---

**Note** Virtual Machine (VM) installations can also be upgraded using the Cisco VSM Management Console. Upgrades are supported from release 7.8 or higher on the RHEL6 operating system.

---

## Recovery/Factory Image

You can also create a bootable USB flash drive that can be used to recover an installation or perform a factory installation of Cisco VSM Release 7.10 on a supported physical server that shipped with Cisco VSM Release 7.10 pre-installed. This includes CPS-UCSM4-1RU-K9 and Cisco CPS UCSM4 2RU.

## Related Recovery Documentation

For more information, see the following documents:

### Release 7.6 and higher

[Cisco Video Surveillance Manager: Install and Upgrade Guide](#)

### Release 7.5 and lower

- [Cisco CSS UCS Server User Guide](#)
- [Cisco Video Surveillance Manager Recovery Guide \(Cisco MSP Platform\)](#)

## Released Versions

Cisco VSM Release 7.10 is released with 7.10 – 205i. The component package versions are:

- Cisco\_Tomcat-7.0.55-3.el6.noarch
- Cisco\_MetaDataService-7.10.0-090d.i686
- Cisco\_VSTools-7.10.0-090d.i686
- Cisco\_GeoServer-7.8.0-1.noarch
- Cisco\_VSMUpgrade-7.10.0-090d.i686
- Cisco\_AMQBroker-7.10.0-1.noarch
- Cisco\_VSRecorder-7.10.0-090d.i686
- Cisco\_VSDrivers-7.10.0-090d.i686
- Cisco\_MPClient-7.10.0-68.noarch
- Cisco\_DashCast-7.10.0-090d.i686
- Cisco\_CDAF-7.10.0-176.noarch
- Cisco\_VSF-7.10.0-176.noarch
- Cisco\_VSBase-7.10.0-090d.i686
- Cisco\_VSMS-7.10.0-090d.i686



- Cisco\_SASD-7.10.0-94.noarch
- Cisco\_VSOM-7.10.0-176.x86\_64

Updated Firmware version for supported devices: v2.9.1-2.

The following Cisco IP cameras models support this firmware version:

- CIVS-IPC-283x
- CIVS-IPC-3050
- CIVS-IPC-3535
- CIVS-IPC-36xx
- CIVS-IPC-3xxx
- CIVS-IPC-65xx
- CIVS-IPC-66xx
- CIVS-IPC-6930
- CIVS-IPC-6xxx
- CIVS-IPC-7070
- CIVS-IPC-75xx
- CIVS-IPC-7xxx

## Supported Devices

The following sections provide information about the devices that this version of Cisco VSM supports:

- [Supported Devices: Cisco, page 25](#)
- [Supported Devices: Arecont, page 31](#)
- [Supported Devices: Axis, page 32](#)
- [Supported Devices: IQinVision, page 35](#)
- [Supported Devices: Mobotix, page 36](#)
- [Supported Devices: Panasonic, page 36](#)
- [Supported Devices: Pelco, page 37](#)
- [Supported Devices: Sony, page 38](#)
- [Supported Devices: Vivotek, page 39](#)
- [Supported Devices: Generic IP Cameras, page 39](#)
- [Supported Devices: Analog Cameras, page 42](#)
- [Device Models Validated in Cisco VSM as Generic IP Cameras, page 43](#)

## Supported Devices: Cisco

Table 4 through Table 10 provide information about Cisco devices supported in this release:

- [Cisco 2400/2500, 2600, 2800, and 2900 Series](#)
- [Cisco 3000 Series](#)

- Cisco 4000 Series and 5000 Series
- Cisco 6000 Series
- Cisco 7000 Series
- Cisco 8000 Series
- Cisco CIVS-SENC-4P and CIVS-SENC-8P

**Table 4** Cisco 2400/2500, 2600, 2800, and 2900 Series

Model	FW Version for Release 7.10 Compatibility <sup>1</sup>	Video Format	Media Types	Audio	Dual Stream	Motion Detection	Firmware Upgrade	Privacy Mask	Edge Storage	Camera App Min. FW Version	Medianet Support
2400 Series	Minimum: 2.5.2.2	NTSC / PAL	MPEG-4 MJPEG	NA	Yes	Yes	Yes	No	No	N/A	No
2500 Series	Minimum: 2.5.2.2	NTSC / PAL	MPEG-4 MJPEG	Yes	Yes	Yes	Yes	No	No	N/A	No
2600 Series	Minimum: 4.4.2	NTSC / PAL	H.264 MPEG-4 MJPEG	Yes	Yes	Yes	Yes	No	No	N/A	Partial <sup>2</sup>
2830	Minimum: 2.0.3 Latest: 2.9.1-2	NTSC	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	2.5.0	Yes <sup>3</sup>
2835	Minimum: 2.0.3 Latest: 2.9.1-2	PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	2.5.0	Yes
2900 Series	Minimum: 1.6.18	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	No	No	N/A	No

1. The **minimum firmware** is required for video streaming and recording functionality. The **latest firmware** may be required to support new features, as indicated in the feature columns or descriptions. For more information, including caveats and supported features, see the release notes for the camera model and firmware version.
2. Phase 1 only
3. Phases 1 - 3 (Phase 3 requires firmware 2.0.0-175)

**Table 5** *Cisco 3000 Series*

<b>Model</b>	<b>FW Version for Release 7.10 Compatibility<sup>1</sup></b>	<b>Video Format</b>	<b>Media Types</b>	<b>Audio</b>	<b>Dual Stream</b>	<b>Motion Detection</b>	<b>Firmware Upgrade</b>	<b>Privacy Mask</b>	<b>Edge Storage</b>	<b>Camera App Min. FW Version</b>	<b>Medianet Support<sup>2</sup></b>
3050	Minimum: 2.6.0  Latest: 2.9.1-2	NTSC/ PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	2.7.0	Yes
3421V	Minimum: 2.0.3  Latest: 2.9.1-2	NTSC / PAL	H.264 MJPEG	No	Yes	Yes	Yes	Yes	Yes	2.5.0	Yes
3520	Minimum: 2.0.3  Latest: 2.8.0	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	2.5.0	Yes
3530	Minimum: 2.0.3  Latest: 2.9.1-2	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	2.5.0	Yes
3535	Minimum: 2.0.3  Latest: 2.9.1-2	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	2.5.0	Yes
3620	Minimum: 2.7.1  Latest: 2.9.1-2	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	2.7.0	Yes
3630	Minimum: 2.7.1  Latest: 2.9.1-2	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	2.7.0	Yes

1. The **minimum firmware** is required for video streaming and recording functionality. The **latest firmware** may be required to support new features, as indicated in the feature columns or descriptions. For more information, including caveats and supported features, see the release notes for the camera model and firmware version.
2. Phases 1 - 3 (Phase 3 requires firmware 2.0.0-175)

**Table 6** *Cisco 4000 Series and 5000 Series*

<b>Model</b>	<b>FW Version for Release 7.10 Compatibility<sup>1</sup></b>	<b>Video Format</b>	<b>Media Types</b>	<b>Audio</b>	<b>Dual Stream</b>	<b>Motion Detection</b>	<b>Firmware Upgrade</b>	<b>Privacy Mask</b>	<b>Edge Storage</b>	<b>Camera App Min. FW Version</b>	<b>Medianet Support<sup>2</sup></b>
4300	Minimum: 2.4.2-289	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	No	No	N/A	Partial
4300E	Minimum: 3.2.3-218	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	No	No	N/A	Partial
4500	Minimum: 2.4.2-289	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	No	No	N/A	Partial

Table 6 Cisco 4000 Series and 5000 Series (continued)

Model	FW Version for Release 7.10 Compatibility <sup>1</sup>	Video Format	Media Types	Audio	Dual Stream	Motion Detection	Firmware Upgrade	Privacy Mask	Edge Storage	Camera App Min. FW Version	Medianet Support <sup>2</sup>
4500E	Minimum: 3.2.3-218	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	No	No	N/A	Partial
5000 Series	Minimum: 1.6.17	NTSC	H.264 MJPEG	NA	Yes	Yes	Yes	No	No	N/A	No

1. The **minimum firmware** is required for video streaming and recording functionality. The **latest firmware** may be required to support new features, as indicated in the feature columns or descriptions. For more information, including caveats and supported features, see the release notes for the camera model and firmware version.

2. Phase 1 only

Table 7 Cisco 6000 Series

Model	FW Version for Release 7.10 Compatibility <sup>1</sup>	Video Format	Media Types	Audio	Dual Stream	Motion Detection	Firmware Upgrade	Privacy Mask	Edge Storage	Camera App Min. FW Version	Medianet Support <sup>2</sup>
6000P	Minimum: 2.0.3 Latest: 2.9.1-2	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	2.5.0	Yes
6020	Minimum: 2.0.3 Latest: 2.9.1-2	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	2.5.0	Yes
6030	Minimum: 2.0.3 Latest: 2.9.1-2	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	2.5.0	Yes
6050	Minimum: 2.0.3 Latest: 2.9.1-2	NTSC / PAL	H.264 MJPEG	No	Yes	Yes	Yes	Yes	Yes	2.5.0	Yes
6400	Minimum: 2.0.3 Latest: 2.9.1-2	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	2.5.0	Yes
6400E	Minimum: 2.0.3 Latest: 2.9.1-2	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	2.5.0	Yes
6500PD	Minimum: 2.5.1 Latest: 2.9.1-2	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	2.5.1	Yes
6620	Minimum: 2.7.1 Latest: 2.9.1-2	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	2.7.0	Yes

**Table 7** Cisco 6000 Series (continued)

Model	FW Version for Release 7.10 Compatibility <sup>1</sup>	Video Format	Media Types	Audio	Dual Stream	Motion Detection	Firmware Upgrade	Privacy Mask	Edge Storage	Camera App Min. FW Version	Medianet Support <sup>2</sup>
6630	Minimum: 2.7.1 Latest: 2.9.1-2	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	2.7.0	Yes
6930	Minimum: 2.0.3 Latest: 2.9.1-2	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	2.5.0	Yes

1. The **minimum firmware** is required for video streaming and recording functionality. The **latest firmware** may be required to support new features, as indicated in the feature columns or descriptions. For more information, including caveats and supported features, see the release notes for the camera model and firmware version.
2. Phases 1 - 3 (Phase 3 requires firmware 2.0.0-175)

**Table 8** Cisco 7000 Series

Model	FW Version for Release 7.10 Compatibility <sup>1</sup>	Video Format	Media Types	Audio	Dual Stream	Motion Detection	Firmware Upgrade	Privacy Mask	Edge Storage	Camera App Min. FW Version	Medianet Support <sup>2</sup>
7030	Minimum: 2.0.3 Latest: 2.9.1-2	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	2.5.0	Yes
7030E	Minimum: 2.0.3 Latest: 2.9.1-2	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	2.5.0	Yes
7070	Minimum: 2.6.0 Latest: 2.9.1-2	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	2.7.0	Yes
7530PD	Minimum: 2.5.1 Latest: 2.9.1-2	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	2.5.1	Yes

1. The **minimum firmware** is required for video streaming and recording functionality. The **latest firmware** may be required to support new features, as indicated in the feature columns or descriptions. For more information, including caveats and supported features, see the release notes for the camera model and firmware version.
2. Phases 1 - 3 (Phase 3 requires firmware 2.0.0-175)

Table 9 Cisco 8000 Series

Model	FW Version for Release 7.10 Compatibility <sup>1</sup>	Video Format	Media Types <sup>2</sup>	Dual Stream	Motion Detection <sup>3</sup>	Firmware Upgrade	Privacy Mask	Edge Storage	Audio	Camera App Support	Medianet Support
8000P	Minimum: 1.0.0-08  Latest: 1.0.0-08	NTSC/ PAL	H.264 MJPEG	Yes	Yes	Yes	No	No	Yes G.711 pcmu	No	No
8020	Minimum: 1.0.0-08  Latest: 1.0.0-08	NTSC/ PAL	H.264 MJPEG	Yes	Yes	Yes	No	No	Yes G.711 pcmu	No	No
8030	Minimum: 1.0.0-08  Latest: 1.0.0-08	NTSC/ PAL	H.264 MJPEG	Yes	Yes	Yes	No	No	Yes G.711 pcmu	No	No
8400	Minimum: 1.0.0-08  Latest: 1.0.0-08	NTSC/ PAL	H.264 MJPEG	Yes	Yes	Yes	No	No	Yes G.711 pcmu	No	No

1. The **minimum firmware** is required for video streaming and recording functionality. The **latest firmware** may be required to support new features, as indicated in the feature columns or descriptions. For more information, including caveats and supported features, see the release notes for the camera model and firmware version.
2. Camera mode SHOULD be 5MP while adding to VSOM to support all resolutions.
3. Five window video motion detection.

Table 10 Cisco CIVS-SENC-4P and CIVS-SENC-8P

Model	FW Version for Release 7.10 Compatibility <sup>1</sup>	Video Format	Media Types	Audio	Dual Stream	Motion Detection	Firmware Upgrade	Privacy Mask	Edge Storage	Camera App Support	Medianet Support
CIVS-SENC-4P (encoder)	Minimum: V1.2.0-4	NTSC/ PAL	H.264 MPEG-4 MJPEG	Yes	Yes	Yes	Yes	No	No	No	No
CIVS-SENC-8P (encoder)	Minimum: V1.2.0-4	NTSC/ PAL	H.264 MPEG-4 MJPEG	Yes	NA	Yes	Yes	No	No	No	No

1. The **minimum firmware** is required for video streaming and recording functionality. The **latest firmware** may be required to support new features, as indicated in the feature columns or descriptions. For more information, including caveats and supported features, see the release notes for the camera model and firmware version.

### Additional Notes on Cisco Devices

- Cisco 4500 and 4500E support video analytics.
- Redundancy is supported for all Cisco devices some exceptions for the 2400, 2500, 2900 and 5000 series. The 2400, 2500, 2900 and 5000 series do not support sending events to the redundant server such motion detection and contact closure events.
- Cisco 5000 series does not support motion detection at video bit-rates above 4,000 (4 Mbps). The “H” video preset in Templates has been chosen to not exceed this, so motion detection will work.
- The Cisco 5000 and 2900 camera series do not allow changes to the authentication settings (username/password) or networking settings (DHCP/Static, DNS, etc.) through Cisco VSM. These values can only be changed using the camera web interfaces.
- Focus, Auto Focus and Zoom support are not available for Cisco 6000P, 3421V, 3520, 3530, 3535, and 3050 camera models.
- When Cisco VSM manages a Cisco 6930, 2830, or 2835 camera, it automatically enables the HTTP protocol on the camera and uses this protocol to send PTZ commands to the camera. Other configuration commands continue to use the HTTPS protocol.
- The Cisco 2830, 2835, 3000 series, 6000 series and 7030 cameras now support MJPEG primary streams.
- Cisco 3421V and 6050 cameras do not support Contact Closure, Cisco 7030 camera supports 3 input ports. All other Cisco 3000, 6000, 8000 series cameras support 1 input port.
- In PTZ Tour Configuration, the configured transition time configured includes the time that it takes the camera to move from the one preset position to the next preset position in addition to the time that the camera is expected to stay in the preset position. If the transition time is configured to a value that is less than the time that it takes the camera to move from one preset position to the next, the camera moves between the first and second presets positions only, instead of touring between all preset positions that are configured in the tour.
- The minimum firmware version required to support camera applications is 2.5.0-10.
- The minimum firmware version required to support connected edge storage is 2.0.

## Supported Devices: Arecont

Table 11 provides information about Arecont devices that this Cisco VSM release supports.

**Table 11** Supported Arecont Cameras

Model	Type	Supported FW Version	Media Types	Dual Stream	Motion Detection	Firmware Upgrade
AV2115	2MP IP Camera	65218	H.264 MJPEG	Yes	Yes	No
AV5155	5MP IP Camera	65152	H.264 MJPEG	Yes	Yes	No
AV5115	5MP IP Camera	65220	H.264 MJPEG	Yes	Yes	No
AV10XX5	10MP IP Camera	65218, 65202	H.264 MJPEG	Yes	Yes	No
AV8185DN	4 Sensor 2MP Panoramic IP Camera	65183, 65192	H.264 MJPEG	Yes	Yes	No

**Table 11** Supported Arecont Cameras (continued)

Model	Type	Supported FW Version	Media Types	Dual Stream	Motion Detection	Firmware Upgrade
AV8365DN	4 Sensor 2MP Panoramic IP Camera	65170	H.264 MJPEG	Yes	Yes	No
AV12186DN	4 Sensor 3MP Panoramic IP Camera	65184	H.264 MJPEG	Yes	Yes	No
AV20365DN	4 Sensor 5MP Panoramic Camera	65170	H.264 MJPEG	Yes	Yes	No
AV20185DN	4 Sensor 5MP Panoramic Camera	65183, 65200	H.264 MJPEG	Yes	Yes	No

**Additional Notes on Arecont Devices**

- AV20185, AV20365, AV12186, AV8365 and AV8185 are 4-channel IP cameras. In order to support multiple video channels from a single device, Cisco VSM 7 models these devices as “Encoders”.
- Arecont devices have not yet been qualified to support redundancy in Cisco VSM 7.
- Secondary streams are not supported in H, M, L template settings for Arecont Devices. However secondary stream can be configured using Custom templates.
- Arecont cameras divide the Maximum FPS the camera supports by the number of streams. This could result in lower FPS when both primary and secondary streams are configured for these cameras.
- Arecont AV10XX5, AV5115, AV2115 support VBR and multicast streaming.
- There is a restriction with motion detection for Arecont multi-sensor cameras. False motion events are generated if both half and full resolution size images are requested simultaneously using Cisco VSM or Arecont Camera Web Interface or a third party Media Player.

**Supported Devices: Axis**

Table 12, Table 13, and Table 14 provide information about Axis devices supported in this release.

**Table 12** Supported Axis Cameras

Model	Type	Supported Firmware Version <sup>1</sup>	Video Format	Media Types	Video Ports	Dual Stream	Motion Detection	Max Motion Window	Audio	PTZ
Q6000-E	Encoder	6.40.1	NTSC/ PAL	H264/ MJPEG	4	Yes	Yes	10	No	No
P3707-PE	Encoder	6.50.1.3	NTSC/ PAL	H264/ MJPEG	4	Yes	Yes	10	No	No
Q6052-E	IP Camera	7.20.1	NTSC/ PAL	H264/ MJPEG	1	Yes	Yes	10	No	Yes



1. The minimum firmware is required for video streaming and recording functionality. The latest firmware may be required to support new features, as indicated in the feature columns or descriptions. For more information, including caveats and supported features, see the release notes for the camera model and firmware version.

**Table 13**      **Supported Axis Encoders**

Model	Type	Supported Firmware Version <sup>1</sup>	Video Format	Media Types	Video Ports	Dual Stream	Motion Detection	Audio	Firmware Upgrade	Zoom to Region
P7224	Encoder	5.51.2.7	NTSC/ PAL	H264/ MJPEG	4	Yes	Yes	Yes	Yes	No
Q7424-R MK II	Encoder	5.51.3.2	NTSC/ PAL	H264/ MJPEG	4	Yes	Yes	Yes	Yes	No
Q7436	Encoder	6.30.1	NTSC/ PAL	H264/ MJPEG	6	Yes	Yes	No	Yes	No

1. The minimum firmware is required for video streaming and recording functionality. The latest firmware may be required to support new features, as indicated in the feature columns or descriptions. For more information, including caveats and supported features, see the release notes for the encoder model and firmware version.

[Table 14](#) provides information about additional Axis devices that this Cisco VSM release supports.

**Table 14**      **Additional Supported Axis Devices**

Model	Type	Supported FW Version	Video Format	Media Types	Audio	Dual Stream	Stream Mirroring	Motion Detection	Firmware Upgrade	Zoom to Region
233D	IP Camera	4.48.4	NTSC / PAL	MPEG-4 MJPEG	Yes	Yes	Yes	Yes	Yes	No
243SA	Encoder	4.45	NTSC / PAL	MPEG-4 MJPEG	Yes	Yes	Yes	Yes	Yes	No
241Q	Encoder	4.47.5	NTSC PAL	MPEG-4 MJPEG	No	Yes	Yes	Yes	Yes	No
241S	Encoder	4.40	NTSC PAL	MPEG-4 MJPEG	No	Yes	Yes	Yes	Yes	No
243QBlade	Encoder	4.46.1	NTSC / PAL	MPEG-4 MJPEG	NA	Yes	Yes	Yes	Yes	No
247S	Encoder	4.42	NTSC / PAL	MPEG-4 MJPEG	Yes	Yes	Yes	Yes	Yes	No
F44	Encoder	6.50.1.2	NTSC / PAL	MPEG-4 MJPEG	Yes	Yes	Yes	Yes	Yes	No
M3006	IP Camera	5.55.1.2	NTSC	H.264 MJPEG	No	Yes	Yes	Yes	Yes	No
M3007	Panoramic Camera	5.40.13.2	NTSC	H.264 MJPEG	No	Yes	Yes	Yes	Yes	No
P1214	IP Camera	5.40.12.3	NTSC	H.264 MJPEG	No	Yes	Yes	Yes	Yes	No

Table 14 Additional Supported Axis Devices (continued)

Model	Type	Supported FW Version	Video Format	Media Types	Audio	Dual Stream	Stream Mirroring	Motion Detection	Firmware Upgrade	Zoom to Region
P1353	IP Camera	5.40.19.1	NTSC	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	No
P3301	IP Camera	5.40.92	NTSC	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	No
P3364	IP Camera	5.40.17.1	NTSC	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	No
P3367	IP Camera	6.10.1	NTSC	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	No
P3915	IP Camera	5.55.3	NTSC	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	No
P7214	Encoder	5.50.2	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	No
Q1604	IP Camera	5.50.3	NTSC	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	No
Q6045	IP Camera	5.55.11	NTSC	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes
Q7401	Encoder	5.50.2	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	No
Q7404	Encoder	5.50.2	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes
Q7406	Encoder	5.11.1	NTSC / PAL	H.264 MJPEG	N/A	Yes	Yes	Yes	Yes	Yes
Q7424	Encoder	5.50.02	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes

**Additional Notes on Axis Devices**

- Axis P3301 IP camera and Q7401, Q7404, and Q7406 encoders have been qualified to support redundancy in Cisco VSM 7.0.1.
- Axis 233D supports contact closure configuration and events.
- Support for 0.1fps MJPEG stream for all supported Axis models.

The following table documents the various Field-Of-Views supported for the Axis M3007 panoramic cameras and support for PTZ and Motion Detection for these Field-Of-Views.

**Table 15** *Axis M3007 Options*

Model	Field Of View	PTZ	Motion Detection
Axis M3007	360° view	No	Yes
	Panoramic view (180 degree view)	No	No
	Double Panoramic view(2 panoramic view of 180 degree)	No	No
	Quad view (view area 1,2,3,4)	No	No
	View Area 1	Yes	No
	View Area 2	Yes	No
	View Area 3	Yes	No
	View Area 4	Yes	No

The Axis M3007 camera allows the user to configure various mounting options directly in the camera web interface that affects the possible values for Field-Of-Views that can be configured on the camera. The table below provides this mapping:

**Table 16** *Axis M3007 Field-Of-View Options*

Field of View / Mount Point	Wall	Ceiling	Desktop
360 Degree View	Yes	Yes	Yes
Panoramic View	Yes	Yes	Yes
Double Panoramic View	No	Yes	Yes
Quad View	No	Yes	Yes
View Area 1/2/3/4	Yes	Yes	Yes

## Supported Devices: IQinVision

[Table 17](#) provides information about IQinVision devices that this Cisco VSM release supports.

**Table 17** *Supported IQinVision Devices*

Model	Type	Supported FW Version	Video Format	Media Types	Audio	Dual Stream	Stream Mirroring	Motion Detection	Firmware Upgrade
IQ032SI-V11	IP Camera	V3.4/5	NTSC	H.264	No	No	No	Yes	Yes
IQM32NE-B5	IP Camera	V3.4/5	NTSC	H.264	No	No	No	Yes	Yes
IqeyeA35N	IP Camera	V3.4/5	NTSC	H264	No	No	No	Yes	Yes

**Table 17** Supported IQinVision Devices (continued)

Model	Type	Supported FW Version	Video Format	Media Types	Audio	Dual Stream	Stream Mirroring	Motion Detection	Firmware Upgrade
Iqeye765N	IP Camera	V3.4/5	NTSC	H264	No	No	No	Yes	Yes
Iqeye755	IP Camera	V3.1/2	NTSC	MJPEG	No	No	No	Yes	Yes

**Additional Notes on IQinVision Devices**

- IQinVision devices have not yet been qualified to support redundancy in Cisco VSM 7.
- Support configuring NTP on the IQinVision cameras to synchronize with their Cisco VSM Media Server.
- Added support for Firmware upgrade for all supported models.
- Added support for Camera Discovery for H.264 models.

## Supported Devices: Mobotix

Table 18 provides information about Mobotix devices that this Cisco VSM release supports.

**Table 18** Supported Mobotix Devices

Model	Type	Supported FW Version	Video Format	Media Types	Audio	Dual Stream	Motion Detection	Firmware Upgrade
x10	IP Camera	MX-V4.x	NTSC	MPEG-4 MJPEG	No	No	No	No

**Additional Notes on Mobotix Devices**

- Mobotix M10 and D10 IP cameras running with M10 series firmware work with the x10 Model.
- Mobotix devices are not qualified to support redundancy in Cisco VSM 7.

## Supported Devices: Panasonic

Table 19 provides information about Panasonic devices that this Cisco VSM release supports.

**Table 19** Supported Panasonic Devices

Model	Type	Supported FW Version	Video Formats	Media Types	Audio	Dual Stream	Motion Detection	Firmware Upgrade
NP 244	IP Camera	1.80 E4	NTSC	MPEG-4 MJPEG	NA	No	Yes	No
NS 202A	IP Camera	2.74P0	NTSC	MPEG-4 MJPEG	No	No	Yes	No

**Table 19** Supported Panasonic Devices (continued)

Model	Type	Supported FW Version	Video Formats	Media Types	Audio	Dual Stream	Motion Detection	Firmware Upgrade
NP 304	IP Camera	1.64E0_1.06	NTSC	MPEG-4 MJPEG	No	No	Yes	No
SW 458	Panoramic Camera	1.42	NTSC	H.264, MJPEG	No	Yes	Yes	No
SF 438	Panoramic Camera	1.42	NTSC	H.264, MJPEG	No	Yes	Yes	No
NF 302	IP Camera	1.64E0_1.06	NTSC	MPEG-4 MJPEG	No	No	Yes	No

**Additional Notes on Panasonic Devices**

- Panasonic devices have not yet been qualified to support redundancy in Cisco VSM 7.
- Only same field of views can be configured on primary and secondary streams on Panasonic cameras SW458/SF438.
- The following table documents the various Field-Of-Views supported for the Panasonic SF 458 and SF 438 panoramic cameras and support for PTZ and Motion Detection for these Field-Of-Views.

**Table 20** Panasonic SF 458 and SF 438 Field-Of-Views Support

Model	Field Of View	PTZ	Motion Detection
Panasonic SW458 and SF438	Panoramic 360 degree view	No	Yes
	Double Panorama view(2 panoramic view of 180 degree)	No	Yes
	Panorama view (180 degree view)	No	Yes
	Quad view	No	No
	Single view	Only with View Area 1	No

**Supported Devices: Pelco**

Table 21 provides information about Pelco devices that this release supports.

**Table 21** Supported Pelco Devices

Model	Type	Supported FW Version	Video Formats	Media Types	Audio	Dual Stream	Motion Detection	Firmware Upgrade
Pelco ExSite	IP Camera	TXB-N-1.9.2.12-2 0131118-1.2084-O 1.10263	NTSC, PAL	H.264, MJPEG	No	Yes	Yes	Yes
Pelco Spectra IV TXB IP (MPEG4)	IP Camera	01.02.0018	NTSC	MPEG4, MJPEG	No	Yes	No	No

**Table 21** Supported Pelco Devices (continued)

Model	Type	Supported FW Version	Video Formats	Media Types	Audio	Dual Stream	Motion Detection	Firmware Upgrade
Pelco NET5404T	Encoder	1.8.2.18-20121109-1.3081-O3.8503	NTSC, PAL	H.264, MJPEG	Yes	Yes	Yes	No
Pelco NET5401T	Encoder	1.9.2.1-20130619-3.3081-O3.9819	NTSC, PAL	H.264, MJPEG	Yes	Yes	Yes	No

**Additional Notes on Pelco Devices**

- Pelco devices have not yet been qualified to support Redundancy in Cisco VSM 7.
- Audio volume controls are not supported for NET540XT
- For Pelco NET540xT PTZ to work, the analog camera should be chosen as Pelco Analog Camera (pelco\_sarix) in Operations Manager and not as Pelco D.
- The user needs to directly configure the Serial protocol on the Pelco NET540XT encoder outside of Cisco VSM.
- The Pelco Spectra IV TXB-N (H.264 capable model) run Pelco Sarix firmware and can be supported in Cisco VSM as a Pelco Sarix Generic IP camera (additional details in the Generic IP camera section).

## Supported Devices: Sony

Table 22 provides information about Sony devices that this release supports.

**Table 22** Supported Sony Devices

Model	Type	Supported FW Version	Video Formats	Media Types	Audio	Dual Stream	Motion Detection	Firmware Upgrade
HM662	Panoramic Camera	1.1.1	NTSC / PAL	H.264 MJPEG	No	Yes	No	No
RX 530	IP Camera	3.15	NTSC / PAL	H.264 MPEG-4 MJPEG	Yes	No	Yes	No
RX 570	IP Camera	3.15	NTSC / PAL	H.264 MPEG-4 MJPEG	Yes	No	Yes	No
RX 550	IP Camera	3.14	NTSC / PAL	H.264 MPEG-4 MJPEG	Yes	No	Yes	No

**Additional Notes on Sony Devices**

- Sony devices have not yet been qualified to support redundancy in Cisco VSM 7.
- These Sony devices do not support motion detection with the H.264 media type.
- The Sony SNC-RX5x0 cameras stop streaming video when the Object Detection window is opened in the camera's web interface.

- For Sony HM662 Panoramic camera, only the 360 degree view is supported. De-warped views are not supported.

## Supported Devices: Vivotek

Table 23 provides information about Vivotek devices that this release supports.

**Table 23** Vivotek

Model	FW Version for Release 7.10 Compatibility <sup>1</sup>	Video Format	Media Types	Dual Stream	Motion Detection <sup>2</sup>	Firmware Upgrade	Privacy Mask	Edge Storage	Audio	Contact Closure
SD9361-EHL	Latest: 0102f	NTSC/ PAL	H.264 MJPEG	Yes	Yes	Yes	No	No	Yes G.711 pcmu	Yes
SD9362-EH/ SD9362-EHL	Latest: 0102f	NTSC/ PAL	H.264 MJPEG	Yes	Yes	Yes	No	No	Yes G.711 pcmu	Yes

- The **minimum firmware** is required for video streaming and recording functionality. The **latest firmware** may be required to support new features, as indicated in the feature columns or descriptions. For more information, including caveats and supported features, see the release notes for the camera model and firmware version.
- Five window video motion detection.

## Supported Devices: Generic IP Cameras

Cisco VSM Release 7.10 provides the following device drivers to support IP cameras from various vendors. The functionality they support will depend on the particular device that they are used with. They are intended to provide a quick and easy way to support devices for which there isn't yet a specific driver available for Cisco VSM. Since these drivers may not be tested with a specific device, some issues may be encountered. When using these drivers with a device, failover and redundancy are not supported.



**Note**

The vendor specific generic driver should always be used before a non-vendor specific driver such as ONVIF.

**Table 24** Supported Generic Devices

Type	Supported Version	Video Formats	Media Types	Audio	Dual Stream	PTZ	Motion Detection <sup>1</sup>	Firmware Upgrade
ONVIF	2.2	NTSC / PAL	H.264 MPEG-4 MJPEG	Yes	Yes	Yes	Yes	No
Generic Axis	3.0 / Firmware 5.x	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	No

Table 24 Supported Generic Devices (continued)

Type	Supported Version	Video Formats	Media Types	Audio	Dual Stream	PTZ	Motion Detection <sup>1</sup>	Firmware Upgrade
Generic Axis	2.0 / Firmware 4.3	NTSC / PAL	MPEG4 MJPEG	Yes	Yes	Yes	Yes	No
Arecont	Arecont Non Panoramic Models	NTSC	H.264 MJPEG	No	Yes	No	Yes	No
IQEye JPEG	V3.1/2	NTSC	MJPEG	No	No	No	Yes	Yes
IQEye H264	V3.4/5	NTSC	H264 MJPEG	No	Yes	No	Yes	Yes
Mobotix	MX Series	NTSC / PAL	MJPEG	No	No	No	Yes	No
Panasonic	-	NTSC / PAL	H.264 MPEG-4 MJPEG	No	Yes	Yes	Yes	No
Pelco Sarix	Only IP cameras with Sarix Firmware	NTSC / PAL	H.264 MJPEG	No	Yes	Yes	Yes	No
Sony	6 <sup>th</sup> Generation IP cameras VMxxx and VBxxx	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	No
Sony	2 <sup>nd</sup> , 3 <sup>rd</sup> , 4 <sup>th</sup> and 5 <sup>th</sup> generation Sony IP cameras	NTSC / PAL	H.264, MPEG-4, MJPEG	Yes	Yes	Yes	Yes	No

1. Only ONVIF cameras manufactured by Hikvision and Samsung support motion detection. Motion windows must be configured directly on the camera using the camera UI before the camera is configured using Cisco VSM.

#### Known Limitations

- Supports only IP Cameras, no support for Encoders
- No contact closure support
- Multicast streaming is supported only for the primary stream
- Multicast port must be an even number within the range 16000:19999
- Audio Multicast issues are observed on most of the ONVIF cameras. Hence do not enable audio when multicast is enabled for video.
- Capture Mode on the camera cannot be changed using ONVIF APIs. So, it is assumed that the camera is in the desired capture mode before adding it to VSOM using ONVIF



### Device Specific Limitations

- This ONVIF driver has been tested with a limited number of camera models from Axis, Sony, Panasonic, Bosch, Pelco, Samsung, J2000IP, Hikvision and Cohu. We have found that these cameras have some variations in how they have implemented the ONVIF specification. Hence there may be compatibility issues when using this ONVIF driver with a particular device that is ONVIF compliant.
- Some of the known caveats are listed below:

### AXIS

- ONVIF user account—Some Axis cameras require a special ONVIF user account, which can be created on the camera's web interface before adding an AXIS ONVIF camera to the VSOM. This page is at **Setup --> System Options --> Security --> ONVIF --> Add**
- Camera and VSMS (Media Server) Time Synchronization—ONVIF camera and VSMS server to which ONVIF camera is being added should have their time synchronized ideally using NTP.

### HIKVISION

- Codec Change through VSOM—Hikvision camera requires a reboot after the codec is changed from VSOM.
- The Minimum Firmware Version of Hikvision cameras supported is V5.3.0, to be added as ONVIF camera in Cisco VSM.

### SAMSUNG

- Megapixel Mode setting on the camera SND-7080
- To support the resolutions (1600\*1200) and (2048\*1536), change the Megapixel Mode to 3-Megapixel in the following page on the camera browser: **Settings -> Audio & Video -> video profile -> Megapixel mode**

### COHU

- Enable Authentication on the camera before adding it to VSOM In the camera browser, go to **Camera Setup -> Configuration -> User Settings**. Select **User** and enable “Require Password” field.
- Media Transport Type— Only UDP is supported. Streaming fails if TCP is selected.
- Unsupported Resolutions —Streaming fails for the resolutions 176\*144, 176\*120, 160\*120
- Codec Change through VSOM— Switching from H264 to JPEG or vice-versa requires a camera reboot. And camera needs to be deleted and added in VSOM after camera is up.
- Support for Audio— Camera does not support ONVIF Audio

### BOSCH

- Frame rate— Only Framerate 30 is supported
- Dual Streaming— Secondary configuration overwrites the primary configuration. So, dual streaming is not supported on Bosch cameras using ONVIF.

### PANASONIC

- Capture Mode Setting— If the camera is added in VSOM using Multicast, changing the capture mode on the camera browser manually causes the streaming to fail. After this, only the unicast streaming works

- User Authentication— User Authentication should be enabled in the camera browser as follows - **Setup -> User mng -> User auth**. Choose **ON** for User auth.

### SONY

- Media Transport Type— Only UDP is supported. Streaming fails if TCP is selected
- Support for Audio— Camera does not support ONVIF Audio
- Set Configuration Issues — Camera returns success even if one or more of the parameters are not valid for that camera/video stream. ONVIF profile gets updated with values but Camera still uses the previous correct value. Recommend to configure only the values as allowed in the camera browser.
- Support for Password change on the camera— Camera does not support password change for the administrator users using ONVIF API.

## Supported Devices: Analog Cameras

This Cisco VSM release provides support for the following analog cameras.

**Table 25**      **Supported Devices: Analog Cameras**

Type	Video Formats	Serial Protocol Support
Generic	NTSC / PAL	No
Axis Analog Camera	NTSC / PAL	Encoder dependent: use the encoder's PTZ driver. For use with Axis VAPIX 3.0 video encoders
Bosch	NTSC / PAL	Yes
Panasonic	NTSC / PAL	Yes
Generic Pelco-D	NTSC / PAL	Pelco-D
Generic Pelco P	NTSC / PAL	Pelco P
Pelco Min-Spectra	NTSC / PAL	Pelco-D
Pelco Analog Camera	NTSC / PAL	Encoder Dependent (for use with only PelcoNET540xT encoders)

**Table 25** *Supported Devices: Analog Cameras (continued)*

Type	Video Formats	Serial Protocol Support
Cyberdome I	NTSC	Yes
Cyberdome II	NTSC	Yes

**Notes on Cyberdome devices**

- The Cyberdome I and Cyberdome II devices also have On Screen Display Menu support.

## Device Models Validated in Cisco VSM as Generic IP Cameras

The camera models listed in [Table 26](#) have been tested with VSM Release 7.10 as generic IP cameras.

**Table 26** *Supported Generic IP Cameras*

Model	Type	Firmware	Format	Media Types	Audio	Dual Stream	PTZ	Motion Detection	Firmware Upgrade
Arecont AV1355	Arecont	65151	NTSC / PAL	H.264	No	Yes	No	Yes	No
Arecont AV3115	Arecont	65218	NTSC / PAL	H.264	No	Yes	No	Yes	No
Axis 215	Axis VAPIX 2.0 /Firmware 4.3	4.48.4	NTSC / PAL	MPEG4, MJPEG	Yes	Yes	Yes	Yes	No
Axis 3301	Axis VAPIX 3.0/Firmware 5.x	5.41.2	NTSC / PAL	H.264, MJPEG	Yes	Yes	No	Yes	No
Axis 3367	Axis VAPIX 3.0/Firmware 5.x	6.10.1	NTSC / PAL	H.264, MJPEG	Yes	Yes	No	Yes	No
Axis Q6034	Axis VAPIX 3.0/Firmware 5.x	5.41.1.2	NTSC / PAL	H.264, MJPEG	Yes	Yes	Yes	Yes	No
Axis Q6034-E	ONVIF 2.0	5.41.1.2	NTSC	H.264, MJPEG	Yes	Yes	Yes	No	No
Axis Q6045	ONVIF 2.2	5.55.1.1	NTSC	H.264, MJPEG	No	Yes	Yes	No	No
IQinVision IQ755	IQEye JPEG	V3.1/2	NTSC	MJPEG	No	No	No	Yes	Yes
IQinVision IQ853	IQEye Jpeg	V3.1/2	NTSC	MJPEG	No	No	No	Yes	Yes
IQinVision IQA35N	IQEye H264	V3.4/6	NTSC	H.264, MJPEG	No	Yes	No	Yes	Yes

Table 26 Supported Generic IP Cameras (continued)

Model	Type	Firmware	Format	Media Types	Audio	Dual Stream	PTZ	Motion Detection	Firmware Upgrade
IQinVision IQM32N	IQEye H264	V3.4/6	NTSC	H.264, MJPEG	No	Yes	No	Yes	Yes
Panasonic NP-502S	Panasonic	1.81	NTSC / PAL	H.264, MPEG4, MJPEG	No	Yes	No	Yes	No
Panasonic SC384	Panasonic	1.44	NTSC / PAL	H.264, MJPEG	No	Yes	Yes	Yes	No
Panasonic SF538	ONVIF 2.1.1	1.31	NTSC	H.264, MJPEG	No	Yes	No	No	No
Panasonic SW458	ONVIF 2.0	1.42	NTSC	H.264, MJPEG	Yes	Yes	No	No	No
Panasonic SW458	Panasonic	1.42	NTSC / PAL	H.264, MJPEG	No	Yes	Yes	Yes	No
Pelco IDS0DN-AD AURX7	Pelco	1.8.2.20-2013021 1-2.9110-03.9240	NTSC	H.264, MJPEG	No	Yes	No	Yes	No
Pelco ISXOC	Pelco	1.9.2.2-20130717-1.9080-A 1.9926	NTSC	H.264, MJPEG	No	Yes	No	Yes	No
Samsung SND-7080	ONVIF 2.1.0	1.10_110819	NTSC	H.264, MJPEG	No	Yes	No	No	No
Samsung SND-7080	ONVIF 2.0	2.00_121004	NTSC	H.264, MJPEG	No	Yes	No	No	No
Sony CH 240	Sony 2nd, 3rd, 4th and 5th generation Sony IP cameras	1.79.00	NTSC / PAL	H.264, MPEG4, MJPEG	Yes	Yes	No	Yes	No
Sony CH180	ONVIF 2.2	1.34.00	NTSC	H.264, MJPEG	Yes	Yes	No	No	No
Sony VM 631	Sony 6th Generation IP cameras VMxxx and VBxxx	1.3.0	NTSC / PAL	H.264, MJPEG	Yes	Yes	No	No	No

# Clipping Support By Application

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

**Table 27**      **Video Clip Support**

Application	Create MP4 Clips	Create CVA Clips	Create Virtual Clips	View MP4 Clips <sup>1</sup>	View CVA Clips	View Virtual Clips	Clip Search Feature
Cisco VSM Operations Manager	Yes	Yes	Yes	Yes	No	Yes	Yes
Cisco VSM Federator	Yes <sup>2</sup>	Yes	No	Yes <sup>3</sup>	No	Yes <sup>4</sup>	Yes
Cisco SASD	Yes	Yes <sup>5</sup>	Yes <sup>6</sup>	Yes	No	Yes	Yes
Cisco SASD Federator	Yes	Yes	Yes <sup>7</sup>	Yes	No	Yes	Yes
Cisco VSM Review Player	No	No	No	Yes	Yes <sup>8</sup>	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).



**Note**

When converting a virtual clip to an MP4 file, only the entire duration of the virtual clip can be saved, not a segment.

# Obtaining and Installing Licenses

To install a license, purchase the license and obtain the license file, then upload the file to the Operations Manager.

Table 28 lists the part numbers for the Cisco VSM licenses. Multiple camera and VSMS licenses can be included in a single license file. For example, a single license file might include support for 25 additional cameras and two additional VSMS devices.

**Table 28 License Part Numbers**

Part	Description
<b>Physical Server Licenses (for Server Services)</b>	
FL-CPS-MS-SW7	License for 1 Media Server on a physical server (Cisco UCS or MSP)
FL-CPS-OM-SW7	License for 1 Operations Manager on a physical server (Cisco UCS or MSP)
L-CPS-MS-SW7=	eDelivery license for 1 Media Server on a physical server (Cisco UCS or MSP)
<b>Virtual Machine (VM) Licenses (for Server Services)</b>	
L-CPS-VSMS7-B-VM=	eDelivery license for one Media Server on a VM running on a Cisco UCS B Series
L-CPS-VSOM7-B-VM=	eDelivery license for one Operations Manager on a VM running on a Cisco UCS B Series
L-CPS-VSMS7-C-VM=	eDelivery license for one Media Server on a VM running on a Cisco UCS C Series
L-CPS-VSOM7-C-VM=	eDelivery license for one Operations Manager on a VM running on a Cisco UCS C Series
L-CPS-VSMS7-E-VM=	eDelivery license for one Media Server on a VM running on a Cisco UCS E-Series
L-CPS-VSOM7-E-VM=	eDelivery license for one Operations Manager on a VM running on a Cisco UCS E-Series
<b>Cisco VSM Federator Licenses</b>	
L-CPS-VSM7-FD=	eDelivery license for one base Cisco VSM 7 Federator
L-CPS-FD-VSOM=	eDelivery license for one Operations Manager in Federator
L-CPS-FD-VSOM-X=	eDelivery license for one Operations Manager Express in Federator
<b>Cisco SASD Licenses</b>	
L-CPS-SASD-7=	eDelivery license for 1 SASD with Cisco VSM 7
<b>Camera Licenses</b>	
L-CPS-VSM7-1CAM=	eDelivery license for 1 camera connection with Cisco VSM 7
<b>Camera App Licenses</b>	
<b>Note</b>	The following licenses are used when managing Camera Apps using Cisco VSM Operations Manager. These licenses are different than those used when installing and managing the Camera Apps directly on the device (using the device UI).
L-FL-AA-CA-VSM=	Car Alarm Detection Application for Cisco IP Cameras for VSM
L-FL-AA-GB-VSM=	Glass Break Detection App for Cisco IP Cameras for VSM

**Table 28 License Part Numbers (continued)**

Part	Description
L-FL-AA-GS-VSM=	Gun Shot Detection Application for Cisco IP Cameras for VSM
L-FL-C-AP1-VSM=	Tier 1 Cisco Application for Cisco IP Cameras for VSM
L-FL-C-AP2-VSM=	Tier 2 Cisco Application for Cisco IP Cameras for VSM
L-FL-IVVA-T1-VSM=	Tier 1 Cisco IP Camera Intuivision Video Analytic App for VSM

**Notes**

- A license for 10,000 Cisco cameras is included by default (you do not need to purchase and install an additional license for Cisco cameras).
- You can add 1 Media Server and 10 non-Cisco cameras without a license for initial setup purposes only. This feature is removed when you add any permanent license.

**Procedure**

- 
- Step 1** Purchase additional licenses:
- Determine the part number for the license you want to purchase (see [Table 28](#)).
  - Purchase the license by contacting your Cisco sales representative or any Cisco reseller. For more information, visit <http://www.cisco.com/en/US/ordering/index.shtml>.
  - When the purchase is complete, you are issued a Product Authorization Key (PAK) in paper form, or in an e-mail message.
- Step 2** Obtain the license file:
- Locate the Product Authorization Key (PAK) that was created with the purchase.
  - In a web browser, open the Cisco Product License Registration web page.  
<http://www.cisco.com/go/license/>
  - Follow the on-screen instructions to complete the form and enter the Product Authorization Key (PAK). When you are done, a license file with the extension `.lic` is sent to your e-mail address.
  - Transfer the file to the drive of the PC used for the configuration.
- Step 3** Install the license file in Cisco VSM:
- Log in to the Operations Manager.
  - Select **System Settings > Software Licensing**.
  - Click **Add** and select the license file located on your local drive.
  - Click **Save** to install the file and activate the additional capacity.
- The additional capacity is available immediately. You do not need to restart the server or take additional steps.
- See the [Cisco Video Surveillance Operations Manager User Guide](#) for more information.
-

# Understanding the Cisco VSM Software Types

Table 29 describes the different types of software and firmware that are installed on servers, cameras, and encoders.

**Table 29** Cisco VSM Software Types

Software Type	Description
System software	<p>System software denotes the Cisco VSM software, including Media Server, Operations Manager, Cisco VSM Management Console, Safety and Security Desktop and Multipane clients. All servers running the Operations Manager and associated Media Server services must run the same software version.</p> <p>Use the Operations Manager to update the <i>System Software</i> on all servers (such as Media Servers) associated with the Operations Manager. See the <a href="#">Cisco Video Surveillance Operations Manager User Guide</a> for instructions.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>The Operations Manager and all associated servers must run the same system software version.</li> <li>To update a Federator server, log in to the Federator server Management Console. See the <a href="#">Cisco Video Surveillance Operations Manager User Guide</a> for instructions.</li> <li>To repair or restore the Cisco VSM system software, see the <a href="#">Cisco Video Surveillance Manager: Install and Upgrade Guide</a> for your hardware platform. For VM installations, see the <a href="#">Cisco Video Surveillance Virtual Machine Deployment and Recovery Guide for UCS Platforms</a>.</li> </ul>
OVA image (for VM installations)	<p>OVF template files are used to install the system software as a virtual machine (VM) on a supported Cisco Unified Computing System (UCS) platform.</p> <ul style="list-style-type: none"> <li>OVA template files are downloaded from the Cisco website.</li> <li>The file format is <code>.ova</code>. For example: <code>Cisco_VSM-7.10-331d_ucs-bc.ova</code></li> <li>See the <a href="#">Cisco Video Surveillance Virtual Machine Deployment and Recovery Guide for UCS Platforms</a> for instructions to install the <code>.ova</code> image and perform the initial VM setup.</li> <li>After the VM setup is complete, use the Management Console to complete the configuration.</li> </ul>
USB Recovery Disk image	<p>Use the USB Recovery Disk image to create a Cisco VSM 7 Recovery Flash Drive (for example, on a USB stick). The recovery disk can be used do the following:</p> <ul style="list-style-type: none"> <li>Repair: reinstalls the Operating System files and partitions without erasing video files stored on the server. You must backup the Cisco VSM database before using the recovery image, and then restore the database after the recovery process is complete. This action also preserves the RAID configuration.</li> <li>Factory Restore: Restores the server to its factory default settings, reinstalls the operating system, and clears and reconfigures the RAID. This action deletes all data, configurations, software and video files from the appliance, and then reinstalls the operating system and Cisco VSM software. Perform this procedure only if necessary.</li> </ul> <p>See the <a href="#">Cisco CSS UCS Server User Guide</a> for more information.</p>
Device <i>firmware</i>	<p>Device <i>firmware</i> is provided by the device manufacturer. The firmware for Cisco devices can be upgraded using Operations Manager. Firmware for other manufacturers is upgraded using a direct connection.</p> <p>See the “Upgrading Camera and Encoder Driver Firmware” section of the <a href="#">Cisco Video Surveillance Operations Manager User Guide</a> for instructions to upgrade Cisco device firmware, or refer to the device documentation.</p>



Table 29 Cisco VSM Software Types (continued)

Software Type	Description
Device driver packs	<p>Device <i>driver packs</i> are the software packages used by Media Servers and the Operations Manager to interoperate with video devices, such as cameras. Driver packs are included with the Cisco VSM software, or may be added to a server at a later time to add support for new devices or features.</p> <ul style="list-style-type: none"> <li>• Install new driver packs to add support for additional devices.</li> <li>• Upgrade existing driver packs to enable support for new features.</li> <li>• When updating or installing a driver pack, you first install the file on the Operations Manager, and then on the Media Servers that support the cameras or encoders. You can install the new version on all Media Servers, or only the Media Server(s) that support the affected devices. If the driver pack version is different on the Media Servers in your deployment, a <i>driver pack mismatch</i> error can occur. <ul style="list-style-type: none"> <li>– A warning message is informational only and the cameras and encoders can be configured normally.</li> <li>– A critical message appears if the driver pack mismatch will impact the functionality or compatibility between the Operations Manager, Media Servers, and the video device. The upgrade is not allowed. Camera and encoder templates cannot be revised until the same driver pack version is installed on all Media Servers.</li> </ul> </li> </ul> <p><b>Note</b> We strongly recommend upgrading driver packs using the Operations Manager interface (see the “Driver Pack Management” section of the <a href="#">Cisco Video Surveillance Operations Manager User Guide</a>). This allows you to upgrade multiple servers at once.</p>
Language Packs	<p>Language packs can be added to display the Cisco VSM user interfaces in non-English languages.</p> <p>Language packs are added using the Operations Manager (release 7.6 and higher). See the <a href="#">Cisco Video Surveillance Operations Manager User Guide</a> for instructions.</p>

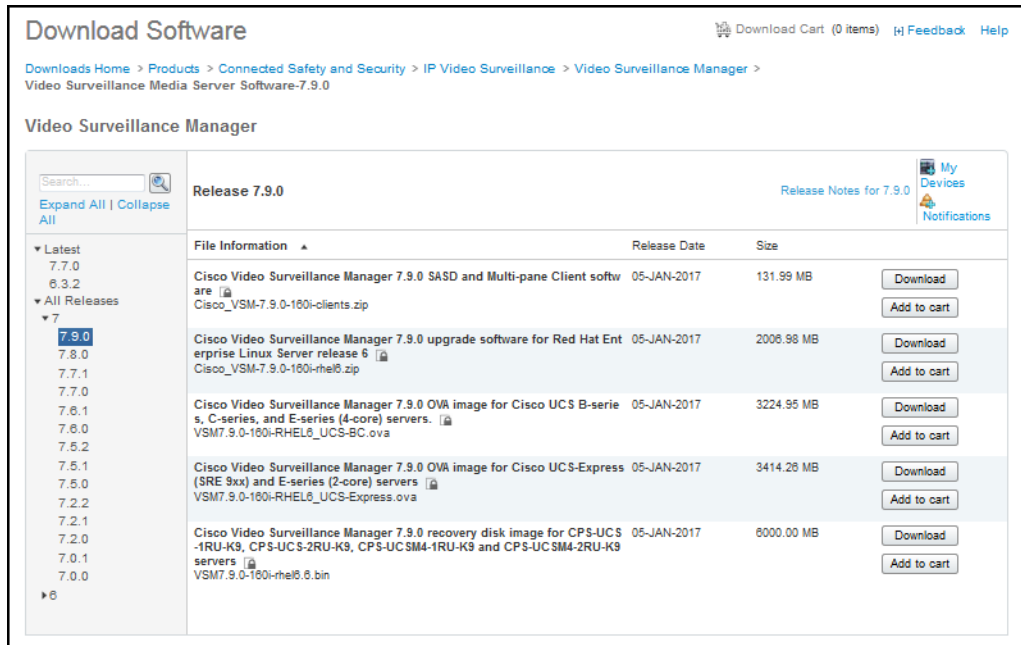
## Obtaining Cisco VSM Software

Complete the following procedure to obtain software and other information for the Cisco VSM products and components:

### Procedure

- 
- Step 1** Go to the [Cisco Video Surveillance Manager product page](#).
- Step 2** Click [Download Software](#).
- Step 3** Select a product category. For example:
- **Video Surveillance Device Driver**
  - **Video Surveillance Manager Stand-alone Tools**
  - **Video Surveillance Media Server Software** (including system software)
- Step 4** Select the release for your server, device, or deployment ([Figure 11](#)).
- Step 5** Click **Download** or **Add to Cart** and follow the onscreen instructions.

Figure 11 Download Software Page



### Alternate Procedure

You can also navigate the Cisco Physical Security product pages to download software updates and other information:

- Step 1** Go to the following URL.  
<http://www.cisco.com/go/physicalsecurity>
- Step 2** Click **View All Physical Security Products**.
- Step 3** Click **IP Video Surveillance**.
- Step 4** Click **Cisco Video Surveillance Manager**.
- Step 5** Click **Download Software for this Product**.
- Step 6** Click a Software Type and follow the onscreen instructions.  
For example: **Video Surveillance Media Server Software** (Figure 11).
- Step 7** Select the release for your server, device, or deployment.
- Step 8** Click **Download** or **Add to Cart** and follow the onscreen instructions.

# Caveats

This section includes the following topics:

- [Using the Software Bug Search Tool, page 51](#)
- [Open Caveats, page 51](#)
- [Resolved Caveats, page 52](#)

## Using the Software Bug Search Tool

You can use the Bug Search Tool to find information about most caveats for Cisco VSM releases, including a description of the problems and available workarounds. The Bug Search Tool lists both open and resolved caveats.

To access Bug Search Tool, you need the following items:

- Internet connection
- Web browser
- Cisco.com user ID and password

To use the Software Bug Search Tool, follow these steps:

### Procedure

- 
- Step 1** To access the Bug Search Tool, go to <https://tools.cisco.com/bugsearch/>
- Step 2** Log in with your Cisco.com user ID and password.
- Step 3** To look for information about a specific problem, enter the bug ID number in the **Search for** field.
- Step 4** For more information, go to the [Bug Search interactive tour](#).
- 

## Open Caveats

[Table 30](#) lists caveats that are open in this release.

**Table 30**      **Open Caveats**

Caveat	Description
CSCvf52437	HTML5: stream switching is not working for HTML5 if camera is covered
CSCvf03229	HTML5: Default latency in HTML stream causing much more time to adjust exact PTZ location
CSCvf32217	HTML5: Firefox, Chrome :- PTZ not able to zoom with mouse only
CSCve89230	HTML5: Stream not getting played with small delay/ahead in time of the client machine
CSCve97833	HTML5: User is not able to view streaming for a rotational view having 10 second as rotation period
CSCve92586	HTML5: Not able to see image tab after logging out from camera module
CSCvc46394	HTML5: Recording seek bar does not show latest recording
CSCvc45147	HTML5: User is not able to play the paused stream from the accurate paused point

**Table 30**      **Open Caveats**

Caveat	Description
CSCvf83785	Recovered event emails contain wrong image, even redundant server is configured.
CSCvf60474	Emails of all recovered events contain Snapshot at time of reconnecting
CSCvf16081	Bookmark search does not show the correct location for searched bookmark
CSCvg03037	HTML5: Joystick/Gamepad behavior is not same as active-x
CSCve85269	Recording is Not saved when the Server is Replaced when 'On Demand Recording' is in progress
CSCve85293	Disable padding does NOT work when Server is replaced and ODR is allowed to stop automatically
CSCvf74759	Storage Retention statistics for Cameras with Motion + Continuous Recording
CSCve87539	Blank recording stream pushed to PTW when live covered.

## Resolved Caveats

Table 31 lists caveats that are resolved in this release.

**Table 31**      **Resolved Caveats**

Caveat	Description
CSCve84076	VSM 7.10.0-105i: Unable to log into VSF using AD credentials after upgrading from 7.8.0 FCS
CSCve45283	VSM 7.9.1/7.9.2: Views don't load in VSF after upgrade (VSOM is at a lower version - 7.9.0)
CSCvd22665	VSM 7.10: VSF Views: Operator with permission to view only secondary stream can view Primary stream
CSCvc97737	7.9: SASD: Views are not loading on SASD Federator

## Related Documentation

See the following locations for the most current information and documentation:

**Cisco Video Surveillance 7 Documentation Roadmap**

Descriptions and links to Cisco Video Surveillance documentation, server and storage platform documentation, and other related documentation.

<http://www.cisco.com/go/physicalsecurity/vsm/roadmap>

**Cisco Physical Security Product Information:**

[www.cisco.com/go/physicalsecurity/](http://www.cisco.com/go/physicalsecurity/)

**Cisco Video Surveillance Manager Documentation Website**

[www.cisco.com/go/physicalsecurity/vsm/docs](http://www.cisco.com/go/physicalsecurity/vsm/docs)

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](http://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. (1721R)

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.

*Release Notes for Cisco Video Surveillance Manager, Release 7.10*  
© 2008 - 2017 Cisco Systems, Inc. All rights reserved.

