



Release Notes for Cisco Video Surveillance Manager, Release 7.2.2

Revised: April 25, 2014

This document provides important information for Release 7.2.2 of the Cisco Video Surveillance Manager (Cisco VSM).

This document includes the following sections:

- [What's New in this Release, page 2](#)
- [Getting Started, page 2](#)
- [Important Notes, page 4](#)
- [Medianet 2.0 Support, page 4](#)
- [Released Versions, page 9](#)
- [Supported Hardware Platforms, page 9](#)
- [Supported Devices, page 10](#)
- [Minimum Supported Firmware for IP cameras and Encoders, page 20](#)
- [Obtaining and Installing Licenses, page 22](#)
- [Understanding the VSM Software Types, page 24](#)
- [Obtaining VSM Software, page 25](#)
- [Caveats, page 26](#)
- [Related Documentation, page 28](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

What's New in this Release

Cisco VSM Release 7.2.2 is a maintenance update of Cisco VSM 7.2 that resolves various defects (see the [“Resolved Caveats”](#) section on page 28).

Getting Started

Cisco VSM Release 7.2.2 is being delivered as upgrades of Cisco VSM 7.0, 7.0.1, 7.2.0, and 7.2.1 deployed in VMs and on Cisco MSP servers.

The following sections provide information about getting started with this Cisco VSM release. There are different options depending on your deployment:

- [Cisco Physical Security UCS Platform Series Servers \(Release 7.2\)](#), page 2
- [Upgrading from Release 7.0 and 7.2](#), page 2
- [Recovery/Factory Image](#), page 3
- [Migrating from Cisco VSM Release 6.3.x](#), page 3

Cisco Physical Security UCS Platform Series Servers (Release 7.2)

Cisco VSM Release 7.2 is pre-installed on the Cisco Physical Security UCS Platform Series (CPS-UCS-1RU-K9 and CPS-UCS-2RU-K9).

- See the [Cisco Physical Security UCS Platform Series User Guide](#) for supported features, installation and setup instructions.
- After the server appliance is installed, see the [Cisco Video Surveillance Management Console Administration Guide](#) to perform the initial Cisco VSM setup.
- For additional server hardware documentation, see the [Cisco UCS C-Series Server Documentation \(Roadmap\)](#).

Upgrading from Release 7.0 and 7.2

Previous Cisco VSM releases can be upgraded using the Release 7.2.2 system `.zip` file that includes all required software packages (including the Cisco Media Server, Operations Manager, Management Console, Cisco Video Surveillance Safety and Security Desktop client and other components). Installing the `.zip` file upgrades all components and ensures that all packages are running the required versions.

The upgrade is performed using the browser-based Cisco VSM Management Console, and should not be performed using the Linux CLI.

See [Cisco Video Surveillance Management Console Administration Guide](#) for detailed information.



Note

- Release 7.0 was pre-installed on the Cisco Multiservices Platform (Cisco MSP) servers, including the CPS-MSP-1RU-K9, CPS-MSP-2RU-K9, CIVS-MSP-1RU, CIVS-MSP-2RU and CIVS-MSP-4RU.

- Virtual Machine (VM) installations can also be upgraded using the Cisco VSM Management Console.

Special Instructions for Linux Red Hat

If you are upgrading from VSM 7.0 and your Cisco VSM server is running the Linux Red Hat operating system, complete the following steps before you begin the upgrade process. These steps update the date that the password was last set for the root user.



Note

If you are upgrading from VSM 7.0.1, you have previously performed this step and it is not necessary to perform it again.

Procedure

- Step 1** Use an SSH client to access the Cisco VSM server and log in as the *localadmin* user.
- Step 2** Enter the following command to update the date that the root user password was last set, where **date** is the current date in yyyy-mm-dd format:
- ```
[localadmin@linux ~]# sudo chage -d date root
```

## 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 7 on a supported physical server that shipped with Cisco VSM 7 pre-installed. This includes:

- Release 7.2.2—Cisco Physical Security UCS series servers (CPS-UCS-1RU-K9 and CPS-UCS-2RU-K9).
- Release 7.0.0—Cisco Physical Security Multiservices platform servers (CPS-MSP-1RU-K9, CPS-MSP-2RU-K9, CIVS-MSP-1RU, CIVS-MSP-2RU and CIVS-MSP-4RU)

For more information, see the [Cisco Video Surveillance Manager Flash Drive Recovery Guide](#) for your server platform.



### Note

There is no USB recovery image for Release 7.0.1. You must recover the system to 7.0 and then upgrade the RPMs to 7.0.1. When using Cisco VSM 7.0.1, use the recovery image for release 7.0.0, and then upgrade the system software to Release 7.0.1 using the Cisco VSM Management Console.

## Migrating from Cisco VSM Release 6.3.x

You can migrate from Cisco VSM 6.3.2 MR2 and 6.3.3 to Cisco VSM 7.2.1, and then upgrade your deployment to 7.2.2. The migration procedure requires assistance from a Cisco representative. Contact your Cisco representative for more information.

## Important Notes

- Cisco VSM Release 7.2.2 provides more information to inform and warn users when configuration changes may result in grooming of recordings. Release 7.2.2 also addresses conditions where recordings may be removed unexpectedly due to unavailability of recording archives. We recommend upgrading deployments running VSM Release 7.2 or VSM Release 7.2.1 to Release 7.2.2.
- Support was added for the following Cisco cameras:
  - CIVS-IPC-3535
  - CIVS-IPC-6050
  - CIVS-IPC-6500E
  - CIVS-IPC-7030E

See the [“Supported Devices: Cisco” section on page 10](#).

- Cisco VSM Release 7.2.2 resolves issues with video recording that can leave random gaps in motion recording or cause some recording configuration operations to fail with an error after a period of operation. If you are running VSM Release 7.2, we recommend that you upgrade to Release 7.2.2.
- Issues may be encountered when using VSM with high latency network links such as data transmitted through satellite links. When the latency through the network from VSM to a camera or exceeds 500 ms, problems may be experienced that are dependent on the model of the camera and the video mode in use. In particular, there are known issues when Economical Streaming mode is used with .1FPS video sent from a camera via a high latency network link to a remote VSM server.

Please contact Cisco for recommendations on deployments requiring use of high latency network connections.

## Medianet 2.0 Support

Release 7.2 adds support for the Medianet metadata and Mediatrace.

Refer to the following topics for more information:

- [Medianet Metadata, page 4](#)
  - [Metadata Requirements, page 5](#)
  - [Metadata Restrictions, page 6](#)
- [Performance Monitoring and Mediatrace, page 7](#)
  - [Requirements, page 7](#)
  - [Enabling Performance Monitoring and Mediatrace, page 7](#)
  - [LiveAction \(Monitoring Application\), page 8](#)
  - [Restrictions, page 8](#)

## Medianet Metadata

The metadata infrastructure allows end points to identify a data flow through the network. Network administrators use this data to classify network traffic (such as video) and implement quality of service (QoS) features.

In Cisco VSM Release 7.2, metadata can be generated for data flowing from Cisco IP cameras to the Cisco Media Servers, and from the Cisco Media Servers to the Cisco VSM workstation clients. Metadata must be enabled on all supported devices as summarized in the “[Metadata Requirements](#)” section on page 5.

Once enabled, no user interaction is required. The metadata is reported in the background and you must use a monitoring tool to view results. Release 7.2 supports the LiveAction desktop application described in the “[Performance Monitoring and Mediatrace](#)” section on page 7.



Tip

For more information, see the Cisco website “[Media Awareness](#)” at: [http://www.cisco.com/web/solutions/trends/medianet/media\\_awareness.html](http://www.cisco.com/web/solutions/trends/medianet/media_awareness.html)

## Metadata Requirements

Medianet metadata must be supported on all intermediate nodes in the data path, including routers, switches, IP cameras, Cisco Media Servers and monitoring workstations.

In Cisco VSM Release 7.2, Medianet metadata is supported on the following devices:

**Table 1** Medianet Metadata Supported Devices

| Device                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cisco routers and switches | <p>The Cisco VSM application and attributes (Media Server, endpoints, and clients) are supported on the following:</p> <ul style="list-style-type: none"> <li>• <a href="#">Cisco Integrated Services Routers (ISR) G2</a>—Cisco IOS version 15.4(1)T</li> <li>• <a href="#">Cisco ASR 1000 Series Aggregation Services Routers (ASR)</a>—Cisco IOS version 15.4(1)S</li> <li>• <a href="#">Cisco Catalyst Series Switches</a>—3000 and 4000 series switches require Cisco IOS version 15.2(2)E</li> <li>• <a href="#">Cisco Catalyst Series Switches</a>—6000 series switches require Cisco IOS version 15.2(1)SY</li> </ul> <p><b>Note</b> Prior IOS versions, currently supported metadata values can be viewed and used for classification.</p> |
| Cisco IP cameras           | <p>See the “<a href="#">Supported Devices: Cisco</a>” section on page 10 for the cameras that support Medianet 2 features.</p> <p><b>Note</b> Cisco devices must be running the minimum supported firmware version to support Medianet 2 features.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Cisco Media Servers        | <p>Metadata is supported on servers running release 7.2 or higher. To enable metadata on a server running the Cisco Media Server service:</p> <ol style="list-style-type: none"> <li>1. Log in to the browser-based Cisco VSM Operations Manager.</li> <li>2. Select <b>System Settings &gt; Servers</b>.</li> <li>3. Select a server.</li> <li>4. Select the <b>Enable Metadata</b> checkbox (under the Medianet heading).</li> </ol> <p><b>Note</b> Metadata is disabled by default. No user interaction is required for metadata tagging, once enabled.</p>                                                                                                                                                                                      |

**Table 1** Medianet Metadata Supported Devices (continued)

| Device                                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Workstation clients used to monitor video | <p>Browser-based clients running the Cisco Multi-Pane client software (an ActiveX client) with the MSI utility installed.</p> <p>MSI is enabled on the workstation by installing the MSI client software:</p> <ol style="list-style-type: none"> <li>1. Log in to the browser-based Cisco VSM Operations Manager.</li> <li>2. Select the <b>Operations</b> tab.</li> <li>3. Select “<b>MSI Installation Package</b>” (under the “Software” heading).</li> <li>4. Double-click the installer package on your workstation and complete the on-screen instructions.</li> </ol> <p><b>Notes</b></p> <ul style="list-style-type: none"> <li>• Metadata is supported on Windows 7-based workstations running the 32-bit Cisco Multi-Pane client.</li> <li>• Metadata is not supported on Cisco SASD in Release 7.2.</li> <li>• No user interaction is required for metadata tagging, but the MSI utility must be installed to enable the feature.</li> </ul> <p><b>Related documentation:</b></p> <ul style="list-style-type: none"> <li>• See <a href="#">Client Workstation Restrictions</a>, page 7.</li> <li>• <a href="#">Cisco Mobile Video Surveillance Operations Manager User Guide</a></li> <li>• See the <a href="#">Cisco Video Surveillance Monitoring Workstation Performance Baseline Specification</a> for more information about the Cisco Multi-Pane client software.</li> </ul> |

## Metadata Restrictions

### Cisco Media Server

Medianet metadata must be enabled on each Cisco Media Server using the browser-based Cisco VSM Operations Manager.

- Medianet metadata is disabled by default.
- Metadata is not generated or propagated by the Media Server for flows created prior to enabling this feature. Flows created prior to enablement must be re-established with Medianet feature enabled.

### Cisco Routers and Switches

Cisco IOS routers and switches running IOS version earlier than 15.4(1)T are limited to 100 flows per source IP addresses (see [CSCuf35612](#) for more information).

Since the Cisco Media Server is the only Cisco VSM device that creates a large number of flows, this 100 limit restriction can be mitigated on large scale deployments by using separate Medianet enabled routers or switches between the device-to-Media Server segments and the Media Server -to-clients segments. This can enable up to 250 camera streams per Media Server and 60 clients per Media Server.

### Network Restrictions

- Medianet metadata is not supported across Network Address Translation (NAT) boundaries.

**Client Workstation Restrictions**

- Medianet metadata for VSM Client is only supported in 32bit mode on Windows 7.
- Medianet metadata is not supported on the Cisco Video Surveillance Safety and Security Desktop (Cisco SASD) application.

## Performance Monitoring and Mediatrace

**Cisco Performance Monitoring**

Cisco Performance Monitoring is a Medianet feature that measures the performance of RTP, TCP and IP traffic on supported Medianet network devices. Cisco Performance Monitoring allows administrators to collect performance metrics on supported endpoints or intermediate nodes for monitoring video quality conditions.

In Cisco VSM Release 7.2, Performance Monitoring information can be collected on Cisco Media Servers, Cisco IP cameras, and all Medianet enabled intermediate nodes in the path (such as routers and switches).

**Cisco Mediatrace**

Cisco Mediatrace allows administrators to trace the video hop by hop across the network to detect problems along the data path.

Mediatrace can be collected between cameras, Cisco Media Servers and all Medianet-enabled intermediary nodes (such as routers and switches) on a hop by hop basis.

## Requirements

To use Mediatrace and Performance Monitoring, you must:

- Enable Medianet metadata on supported devices, including each Cisco Media Server. Medianet metadata is disabled by default. (see the [“Medianet Metadata” section on page 4](#)).
- Enter the Media Services Interface (MSI) password on the Cisco VSM servers (see the [“Enabling Performance Monitoring and Mediatrace” section on page 7](#)).
- Install the LiveAction monitoring application (see the [“LiveAction \(Monitoring Application\)” section on page 8](#)).

## Enabling Performance Monitoring and Mediatrace

To enable Mediatrace and Performance Monitoring, you must enter the Media Services Interface (MSI) password on each Cisco VSM server (using the browser-based Cisco VSM Operations Manager) and camera (using the camera UI). This same password is used to enable monitoring of the Media Server(s) and camera(s) in the LiveAction monitoring software.

**Network Router Usage Notes**

- You can also (optionally) enable Mediatrace on the routers that carry the video data, which allows the routers to behave as a Mediatrace responders. Router that do not support Mediatrace are not included in LiveAction data collection and reports.

**Procedure**

To enable Mediatrace and Performance Monitoring, do the following:

- 
- Step 1** Enable metadata on all Media Servers and cameras.  
See the “[Medianet Metadata](#)” section on page 4.
- Step 2** Define an MSI password.  
The password can be any string defined by the user, and is entered on all servers and camera endpoints that will be monitored, and in the LiveAction monitoring software.
- Step 3** Enter the MSI password in the Cisco VSM server configuration page to which the RTP (video stream) flows to:
- a. Log in to the browser-based Cisco VSM Operations Manager.
  - b. Select **System Settings > Servers**.
  - c. Select a server.
  - d. Enter the MSI **Password** (under the Medianet heading).




---

**Note** The MSI username is read-only and cannot be changed.

---

- Step 4** Configure the MSI password on all cameras that support Performance Monitoring and Mediatrace.
- The camera is the device where the RTP (video stream) originates.
  - Cameras with a valid password can be added to LiveAction as an MSI endpoint.
  - See the camera documentation for instructions to use the device configuration interface.
- Step 5** In LiveAction, add the Media Server(s) and camera(s) as MSI endpoints.  
The data flows can be tracked and viewed for devices that are added to LiveAction. See <https://marketplace.cisco.com/catalog/products/2620> for more information.
- 

## LiveAction (Monitoring Application)

In Cisco VSM Release 7.2, Mediatrace data can be collected and analyzed using the LiveAction Management Server v3.0.

- For additional LiveAction information, go to:  
<https://marketplace.cisco.com/catalog/products/2620>
- For a video summary of LiveAction features, go to:  
<http://www.actionpacked.com/solutions/medianet>
- To download LiveAction Management Server v3.0 go to:  
<http://actionpacked.com/download/liveaction/dl-links-v3-0m>

## Restrictions

- Performance Monitoring is not supported on Cisco VSM clients or Cisco SASD. Mediatrace is not supported between Cisco Media Servers and Cisco VSM clients or Cisco SASD.



- Only UDP based flows are supported in the Cisco Media Servers. UDP is the default setting for Cisco video cameras. There is no metadata support for TCP based flows in this release.

## Released Versions

The Cisco VSM Release 7.2.2 component packages versions are:

- VSMS 7.2.2-30
- VSOM 7.2.2-005
- VSMC 7.2.2-001
- Multi-pane Client 7.2.15
- SASD 7.2.18

## Supported Hardware Platforms

Cisco VSM Release 7.2.2 runs on the following hardware platforms:

**Table 2**      **Supported Hardware Platforms**

| Platform Type   |                                                                                                                                                                                                            | Installation Method                                                                                                                                                                                                                                                                                                                                                     |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Physical Server | Cisco Physical Security UCS platform servers:<br>CPS-UCS-1RU-K9 and<br>CPS-UCS-2RU-K9                                                                                                                      | <ul style="list-style-type: none"> <li>• Pre-installed in new servers.</li> <li>• Recover using the USB recovery stick.</li> <li>• Upgrade RPMs using the Management Console.</li> </ul> See the <a href="#">Cisco Video Surveillance Management Console Administration Guide</a> and the <a href="#">Cisco Video Surveillance Manager Flash Drive Recovery Guide</a> . |
| Physical Server | Cisco Multiservices platform servers: <ul style="list-style-type: none"> <li>• CPS-MSP-1RU-K9</li> <li>• CPS-MSP-2RU-K9</li> <li>• CIVS-MSP-1RU</li> <li>• CIVS-MSP-2RU</li> <li>• CIVS-MSP-4RU</li> </ul> | Upgrade RPMs using the Management Console.<br>See the <a href="#">Cisco Video Surveillance Management Console Administration Guide</a> .                                                                                                                                                                                                                                |
| Virtual Machine | Cisco UCS platform: B, C, E and Express series                                                                                                                                                             | Install the Cisco VSM Release 7.2.2 .OVA image on the virtual machine.<br>See the <a href="#">Cisco Video Surveillance Virtual Machine Deployment and Recovery Guide for UCS Platforms</a> .                                                                                                                                                                            |

# Supported Devices

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

- [Supported Devices: Cisco, page 10](#)
- [Supported Devices: Arecont, page 13](#)
- [Supported Devices: Axis, page 14](#)
- [Supported Devices: IQinVision, page 15](#)
- [Supported Devices: Panasonic, page 15](#)
- [Supported Devices: Pelco, page 16](#)
- [Supported Devices: Sony, page 16](#)
- [Supported Devices: Generic IP Cameras, page 17](#)
- [Supported Devices: Analog Cameras, page 19](#)

## Supported Devices: Cisco

Table 3 provides information about Cisco devices supported in this release:

**Table 3** *Supported Devices: Cisco*

| Model       | Minimum FW Version for Release 7.2 Compatibility | Video Format | Media Types              | Audio | Dual Stream | Motion Detection | Firmware Upgrade | Medianet 1.0 (r7.0 features) | Medianet 2.0 (firmware 1.4.1 required) |
|-------------|--------------------------------------------------|--------------|--------------------------|-------|-------------|------------------|------------------|------------------------------|----------------------------------------|
| 2400 Series | 2.5.1                                            | NTSC / PAL   | MPEG-4 MJPEG             | NA    | Yes         | Yes              | Yes              | No                           | No                                     |
| 2500 Series | 2.5.1                                            | NTSC / PAL   | MPEG-4 MJPEG             | Yes   | Yes         | Yes              | Yes              | No                           | No                                     |
| 2600 Series | 4.4.1-1                                          | NTSC / PAL   | H.264<br>MPEG-4<br>MJPEG | Yes   | Yes         | Yes              | Yes              | Yes                          | No                                     |
| 2830        | 1.2.2-20                                         | NTSC         | H.264<br>MJPEG           | Yes   | Yes         | Yes              | Yes              | Yes                          | Yes                                    |
| 2835        | 1.2.2-20                                         | PAL          | H.264<br>MJPEG           | Yes   | Yes         | Yes              | Yes              | Yes                          | Yes                                    |
| 2900 Series | 1.6.18                                           | NTSC / PAL   | H.264<br>MJPEG           | Yes   | Yes         | Yes              | Yes              | No                           | No                                     |
| 3421V       | 1.2.1-73                                         | NTSC / PAL   | H.264<br>MJPEG           | No    | Yes         | Yes              | Yes              | Yes                          | Yes                                    |
| 3520        | 1.2.1-73                                         | NTSC / PAL   | H.264<br>MJPEG           | Yes   | Yes         | Yes              | Yes              | Yes                          | Yes                                    |

**Table 3**      **Supported Devices: Cisco (continued)**

|               |           |            |                    |     |     |     |     |     |     |
|---------------|-----------|------------|--------------------|-----|-----|-----|-----|-----|-----|
| 3530          | 1.2.1-73  | NTSC / PAL | H.264 MJPEG        | Yes | Yes | Yes | Yes | Yes | Yes |
| 3535          | 2.0.0-175 | NTSC / PAL | H.264 MJPEG        | Yes | Yes | Yes | Yes | Yes | Yes |
| 4300          | 2.4.1-275 | NTSC / PAL | H.264 MJPEG        | Yes | Yes | Yes | Yes | Yes | No  |
| 4300E         | 3.2.2-204 | NTSC / PAL | H.264 MJPEG        | Yes | Yes | Yes | Yes | Yes | No  |
| 4500          | 2.4.1-275 | NTSC / PAL | H.264 MJPEG        | Yes | Yes | Yes | Yes | Yes | No  |
| 4500E         | 3.2.2-204 | NTSC / PAL | H.264 MJPEG        | Yes | Yes | Yes | Yes | Yes | No  |
| 5000 Series   | 1.6.17    | NTSC       | H.264 MJPEG        | NA  | Yes | Yes | Yes | No  | No  |
| 6000 series   | 1.2.1-73  | NTSC / PAL | H.264 MJPEG        | Yes | Yes | Yes | Yes | Yes | Yes |
| 6050          | 2.0.0-175 | NTSC / PAL | H.264 MJPEG        | No  | Yes | Yes | Yes | Yes | Yes |
| 6400E         | 2.0.0-175 | NTSC / PAL | H.264 MJPEG        | Yes | Yes | Yes | Yes | Yes | Yes |
| 6930          | 1.2.2-20  | NTSC / PAL | H.264 MJPEG        | Yes | Yes | Yes | Yes | Yes | Yes |
| 7030          | 1.2.1-73  | NTSC / PAL | H.264 MJPEG        | Yes | Yes | Yes | Yes | Yes | Yes |
| 7030E         | 1.2.1-73  | NTSC / PAL | H.264 MJPEG        | Yes | Yes | Yes | Yes | Yes | Yes |
| CIVS-SE NC-4P | V1.2.0-4  | NTSC / PAL | H.264 MPEG-4 MJPEG | Yes | Yes | Yes | Yes | No  | No  |
| CIVS-SE NC-8P | V1.2.0-4  | NTSC / PAL | H.264 MPEG-4 MJPEG | Yes | NA  | Yes | Yes | No  | No  |

**Notes**

- Medianet support:
  - VSM 7.2 supports new Medianet features including Metadata, Performance Monitoring, and Mediatrace. These features are supported in the Cisco 2830, 2835, 3421, 3520, 3530, 6000 series, 6930, 7030 cameras. The minimum supported firmware version for this feature is 1.4.1. See the [“Medianet 2.0 Support” section on page 4](#) for more information. Cameras with the previous supported firmware version will support only the Medianet 1.0 features from Cisco

## VSM Release 7.0.1.

- The Cisco 2600 series, 4300, 4300E, 4500, and 4500E cameras support only the Medianet 1.0 features in VSM 7.0 and 7.0.1.
- 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 as 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 VSM. These values can only be changed using the camera web interfaces.
- The camera controls focus, auto focus and zoom support are not available for Cisco 6000P, 3421V, 3520, 3530 camera models.
- When 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. The minimum supported firmware version for this feature is 1.4.1.
- Resolution support:
  - Support for 352 x 208, 704 x 400, and 768 x 432 resolutions for both primary and secondary streams on Cisco 3000 Series, 6000 Series, and 7030 cameras. The minimum supported firmware version for this feature is 1.3.2-8.
  - Additional resolutions are also available for the 6930 cameras (requires 1.4.1 firmware and VSM 7.2): 1536 x 864, 1472 x 832, 768 x 432, 704 x 400, 352 x 208, 320 x 192, 192 x 112 and 160 x 96. The minimum supported firmware version for this feature is 1.4.1.
  - Support for 1536x864, 1472x832, 720x576, 704x576, 352x288 for the Cisco 6000 series and 7030 models, support for 2560x1920 resolutions for the Cisco 7030.
  - Support for 1Mbps bitrate for the 1920 x1080 resolution on Cisco 6000 Series and 7030 cameras. The minimum supported firmware version for this feature is 1.3.2-8.
- Support for 1.5 Mbps bitrate for certain resolutions on Cisco 2830, 2835, 3000 Series, 6000 Series and 7030 cameras. The minimum supported firmware version for this feature is 1.3.2-8.
- Contact closure:
  - Cisco 3000, 6000 series cameras support 1 input port.
  - Cisco 7030 camera supports 3 input ports.
  - Cisco 6930, 2830 and 2835 cameras support all 4 contact closures.
  - Cisco 3421V cameras do not support contact closure.
- 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.

## Supported Devices: Arecont

Table 4 provides information about Arecont devices that this VSM release supports.

**Table 4** *Supported Devices: Arecont*

| Model         | Type                                | Minimum Supported FW Version | Media Types    | Dual Stream | Motion Detection | Firmware Upgrade |
|---------------|-------------------------------------|------------------------------|----------------|-------------|------------------|------------------|
| AV2115        | 2MP IP Camera                       | 65218                        | H.264<br>MJPEG | Yes         | Yes              | No               |
| AV5155        | 5MP IP Camera                       | 65152                        | H.264<br>MJPEG | Yes         | Yes              | No               |
| AV5115        | 5MP IP Camera                       | 65218                        | H.264<br>MJPEG | Yes         | Yes              | No               |
| AV10XX5       | 10MP IP Camera                      | 65218,<br>65202              | H.264<br>MJPEG | Yes         | Yes              | No               |
| AV8185DN      | 4 Sensor 2MP<br>Panoramic IP Camera | 65183                        | H.264<br>MJPEG | Yes         | Yes              | No               |
| AV8365DN      | 4 Sensor 2MP<br>Panoramic IP Camera | 65170                        | H.264<br>MJPEG | Yes         | Yes              | No               |
| AV12186D<br>N | 4 Sensor 3MP<br>Panoramic IP Camera | 65184                        | H.264<br>MJPEG | Yes         | Yes              | No               |
| AV20365D<br>N | 4 Sensor 5MP<br>Panoramic Camera    | 65170                        | H.264<br>MJPEG | Yes         | Yes              | No               |
| AV20185D<br>N | 4 Sensor 5MP<br>Panoramic Camera    | 65183                        | H.264<br>MJPEG | Yes         | Yes              | No               |

### Notes

- AV20185, AV20365, AV12186, AV8365 and AV8185 are 4-channel IP cameras. In order to support multiple video channels from a single device, VSM 7 models these devices as “Encoders”.
- Arecont devices have not yet been qualified to support redundancy in 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 VSM or Arecont Camera Web Interface or a third party Media Player.

## Supported Devices: Axis

Table 5 provides information about Axis devices that this VSM release supports.

**Table 5** *Supported Devices: Axis*

| Model     | Type      | Minimum Supported FW Version | Video Format | Media Types   | Audio | Dual Stream | Stream Mirroring | Motion Detection | Firmware Upgrade |
|-----------|-----------|------------------------------|--------------|---------------|-------|-------------|------------------|------------------|------------------|
| 233D      | IP Camera | 4.48.4                       | NTSC / PAL   | MPEG-4 MJPEG  | Yes   | Yes         | Yes              | Yes              | Yes              |
| 241Q      | Encoder   | 4.47.5                       | NTSC / PAL   | MPEG-4, MJPEG | No    | Yes         | Yes              | Yes              | Yes              |
| 241S      | Encoder   | 4.40                         | NTSC / PAL   | MPEG-4, MJPEG | No    | Yes         | Yes              | Yes              | Yes              |
| 243SA     | Encoder   | 4.45                         | NTSC / PAL   | MPEG-4 MJPEG  | Yes   | Yes         | Yes              | Yes              | Yes              |
| 243QBlade | Encoder   | 4.46                         | NTSC / PAL   | MPEG-4 MJPEG  | NA    | Yes         | Yes              | Yes              | Yes              |
| Q7401     | Encoder   | 5.20.3                       | NTSC / PAL   | H.264 MJPEG   | Yes   | Yes         | Yes              | Yes              | Yes              |
| Q7404     | Encoder   | 5.20                         | NTSC / PAL   | H.264 MJPEG   | Yes   | Yes         | Yes              | Yes              | Yes              |
| Q7406     | Encoder   | 5.11.1                       | NTSC / PAL   | H.264 MJPEG   | NA    | Yes         | Yes              | Yes              | Yes              |
| 247S      | Encoder   | 4.42                         | NTSC / PAL   | MPEG-4 MJPEG  | Yes   | Yes         | Yes              | Yes              | Yes              |
| P3301     | IP Camera | 5.40.92                      | NTSC         | H.264 MJPEG   | Yes   | Yes         | Yes              | Yes              | Yes              |

### Note

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

## Supported Devices: IQinVision

Table 6 provides information about IQinVision devices that this VSM release supports.

**Table 6** Supported Devices: IQinVision

| Model       | Type      | Minimum 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              | No               |
| IQM32NE-B5  | IP Camera | V3.4/5                       | NTSC         | H.264       | No    | No          | No               | Yes              | No               |
| IQA35N      | IP Camera | V3.4/5                       | NTSC         | H264        | No    | No          | No               | Yes              | No               |
| IQ765N      | IP Camera | V3.4/5                       | NTSC         | H264        | No    | No          | No               | Yes              | No               |
| IQ755       | IP Camera | V3.1/2                       | NTSC         | MJPEG       | No    | No          | No               | Yes              | No               |

### Notes

- IQinVision devices have not yet been qualified to support redundancy in VSM 7.
- Support configuring NTP on the IQinVision cameras to synchronize with their VSM Media Server.

## Supported Devices: Panasonic

Table 7 provides information about Panasonic devices that this VSM release supports.

**Table 7** Supported Devices: Panasonic

| Model   | Type      | Minimum Supported FW Version | Video Formats | Media Types     | Audio | Dual Stream | Motion Detection | Firmware Upgrade |
|---------|-----------|------------------------------|---------------|-----------------|-------|-------------|------------------|------------------|
| NP 244  | IP Camera | 1.80 E4                      | NTSC          | MPEG-4<br>MJPEG | NA    | No          | Yes              | No               |
| NS 202A | IP Camera | 2.74P0                       | NTSC          | MPEG-4<br>MJPEG | No    | No          | Yes              | No               |
| NP 304  | IP Camera | 1.64E0_1.06                  | NTSC          | MPEG-4<br>MJPEG | No    | No          | Yes              | No               |
| NF 302  | IP Camera | 1.64E0_1.06                  | NTSC          | MPEG-4<br>MJPEG | No    | No          | Yes              | No               |

### Note

Panasonic devices have not yet been qualified to support redundancy in VSM 7.

## Supported Devices: Pelco

Table 8 provides information about Pelco devices that this release supports.

**Table 8** *Supported Devices: Pelco*

| Model          | Type    | Minimum Supported FW Version    | Video Formats | Media Types  | Audio | Dual Stream | Motion Detection | Firmware Upgrade |
|----------------|---------|---------------------------------|---------------|--------------|-------|-------------|------------------|------------------|
| 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 VSM 7.
- Audio volume controls are not supported for NET5401T.

## Supported Devices: Sony

Table 9 provides information about Sony devices that this release supports.

**Table 9** *Supported Devices: Sony*

| Model  | Type      | Minimum Supported FW Version | Video Formats | Media Types              | Audio | Dual Stream   | Motion Detection | Firmware Upgrade |
|--------|-----------|------------------------------|---------------|--------------------------|-------|---------------|------------------|------------------|
| RX 530 | IP Camera | 3.14                         | NTSC / PAL    | H.264<br>MPEG-4<br>MJPEG | Yes   | Not supported | Yes              | No               |
| RX 570 | IP Camera | 3.15                         | NTSC / PAL    | H.264<br>MPEG-4<br>MJPEG | Yes   | Not supported | Yes              | No               |
| RX 550 | IP Camera | 3.14                         | NTSC / PAL    | H.264<br>MPEG-4<br>MJPEG | Yes   | Not supported | Yes              | No               |

### Notes

- Sony devices have not yet been qualified to support redundancy in 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 in the camera's web interface.



## Supported Devices: Generic IP Cameras

VSM 7.2 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 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 10** Supported Devices: Generic IP Cameras

| Type        | Minimum Supported FW Version                                                                       | Video Formats | Media Types                | Audio | Dual Stream | PTZ | Motion Detection | Firmware Upgrade |
|-------------|----------------------------------------------------------------------------------------------------|---------------|----------------------------|-------|-------------|-----|------------------|------------------|
| ONVIF       | 2.0                                                                                                | NTSC / PAL    | H.264<br>MPEG-4<br>MJPEG   | Yes   | Yes         | Yes | No               | No               |
| Axis        | VAPIX 3.0/Firmware 5.x                                                                             | NTSC / PAL    | H.264<br>MJPEG             | Yes   | Yes         | Yes | Yes              | No               |
| Axis        | VAPIX 2.0 /Firmware 4.3                                                                            | NTSC / PAL    | MPEG4,<br>MJPEG            | Yes   | Yes         | Yes | Yes              | No               |
| Arecont     | Arecont Non Panoramic Models                                                                       | NTSC          | H.264, PAL                 | No    | Yes         | No  | Yes              | No               |
| IQEye JPEG  | V3.1/2                                                                                             | NTSC          | MJPEG                      | No    | No          | No  | Yes              | No               |
| IQEye H264  | V3.4/5                                                                                             | NTSC          | H264,<br>MJPEG             | No    | Yes         | No  | Yes              | No               |
| Panasonic   | -                                                                                                  | NTSC PAL      | H.264,<br>MPEG-4,<br>MJPEG | No    | Yes         | Yes | Yes              | No               |
| Pelco Sarix | Only IP cameras with Sarix Firmware                                                                | NTSC PAL      | H.264<br>MJPEG             | No    | 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,<br>MPEG-4,<br>MJPEG | Yes   | Yes         | Yes | Yes              | No               |

### Additional notes on Axis Generic Devices

- 5MP, 3MP and 2MP resolution support has been added to Generic Axis VAPIX version 3.0 capable devices. There are other 4:3 and 16:9 aspect ratio resolutions that are also supported for these devices.

**Additional notes on ONVIF devices**

- ONVIF Compliant 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.
- Audio Multicast issues are observed on most of the ONVIF cameras. Hence do not enable audio when multicast is enabled for video.
- Capture Mode settings required to support certain resolutions on most cameras cannot be changed using the ONVIF APIs. So, it is assumed that the camera is in the desired capture mode before adding it to the Operations Manager using ONVIF driver.
- For information to configure ONVIF with Axis devices, see the [Axis Communications website](http://www.axis.com/techsup/faq/index.php/?action=artikel&&cat=175&id=115393) at: <http://www.axis.com/techsup/faq/index.php/?action=artikel&&cat=175&id=115393>.
- Before adding an ONVIF camera to a Media Sever server the camera's time should be synchronized with the Media Server or the same NTP time source as the Media Server.
- For Sony models, only UDP is supported. Streaming fails if TCP is selected.
- With Bosch ONVIF devices VSM must configure the camera with a frame rate of 30 frames per second, and dual streaming is not supported.
- For some Hikvision models, the camera requires a reboot after the codec is changed from VSM.

**Additional notes on Arecont Generic Devices**

- Arecont Generic Device support does not include support for the Arecont Panoramic models
- Dual stream with 1080p and its quarter resolution(960x528) cannot be configured for Arecont AV2115 models when added using a generic arecont device XML.
- When generic arecont device XML is used, VBR applies for only AVxx15, AVxx25, AVx255 models as per Arecont. For other models, maximum bit rate from the camera may exceed the configured value.

**Additional notes on IQinVision Generic Devices**

- JPEG generic driver: HML will work only for 5M cameras namely 755, 705,805,855.
- H264 generic driver: Only below combinations works for IQinVision M3x, D3x, 03x series: H-H, H-M, H-L, M-M, M-L, L-L
- IQinVision 805 Model is not rendering more than 2 fps in our tests.
- VBR mode is not supported for H264, 1080p stream

**Additional notes on Panasonic Generic Devices**

- Support for Panasonic camera WV-NP1004 for firmware Ver1.25P0 or later.
- Only MJPEG stream supported as secondary stream.
- Secondary stream is not supported if primary stream is MJPEG stream.
- 4:3(800x600) capture mode not supported

**Additional notes on Pelco Generic Devices**

- Some valid streaming combinations may not get saved. In such cases try turning secondary off and try to save again.

**Additional notes on Sony Generic Devices**

- The Sony 1st generation cameras (like RZ30N) are not supported.

- For 2nd Generation cameras, motion detection is not supported.
- Our tests with the RZ25P, we could not get the camera to consistently respond to configuration APIs and this particular model is not supported with this driver.
- For all the Sony cameras supporting dual streams, primary and secondary should be configured with same transport type i.e. both should be either unicast or multicast.
- For the some Sony cameras, we have noticed failures when the attempting to change configurations multiple times in quick succession, retrying the same configuration change after 5 minutes will succeed.

## Supported Devices: Analog Cameras

This VSM release provides support for the following analog cameras.

**Table 11**      **Supported Devices: Analog Cameras**

| Type              | Video Formats | Serial Protocol Support |
|-------------------|---------------|-------------------------|
| Generic           | NTSC / PAL    | No                      |
| 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                 |
| 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.

# Minimum Supported Firmware for IP cameras and Encoders

Table 12 describes the minimum firmware versions for cameras and encoders in this release of Cisco VSM.

**Table 12** Supported Camera and Encoder Firmware

| Manufacturer | Model                | Minimum Supported Firmware Versions<br>(Compatible with Release 7.2) |
|--------------|----------------------|----------------------------------------------------------------------|
| Cisco        | 2400 Series Cameras  | 2.5.1                                                                |
| Cisco        | 2500 Series Cameras  | 2.5.1                                                                |
| Cisco        | 2600 Series Cameras  | 4.4.1-1                                                              |
| Cisco        | 2830 Camera          | 1.2.2-20                                                             |
| Cisco        | 2835 Camera          | 1.2.2-20                                                             |
| Cisco        | 3000 Series Cameras  | 1.2.1-73                                                             |
| Cisco        | 3421V Cameras        | 1.2.1-73                                                             |
| Cisco        | 4300 Camera          | 2.4.1-275                                                            |
| Cisco        | 4500 Camera          | 2.4.1-275                                                            |
| Cisco        | 4300E Camera         | 3.2.2-204                                                            |
| Cisco        | 4500E Camera         | 3.2.2-204                                                            |
| Cisco        | 2900 Series Cameras  | 1.6.18                                                               |
| Cisco        | 5000 Series Cameras  | 1.6.17                                                               |
| Cisco        | 6000 Series Cameras  | 1.2.1-73                                                             |
| Cisco        | 6930 Camera          | 1.2.2-20                                                             |
| Cisco        | 7030 Camera          | 1.2.1-73                                                             |
| Cisco        | CIVS-SENC-4P encoder | 1.2.0-4                                                              |
| Cisco        | CIVS-SENC-8P encoder | 1.2.0-4                                                              |
| Arecont      | AV10XX5              | v65218, v65202                                                       |
| Arecont      | AV20185              | v65183                                                               |
| Arecont      | AV20365              | v65170                                                               |
| Arecont      | AV2115               | v65218                                                               |
| Arecont      | AV5115               | v65218                                                               |
| Arecont      | AV5155               | v65152                                                               |
| Arecont      | AV8185DN             | v65183                                                               |
| Arecont      | AV8365DN             | v65170                                                               |
| Axis         | 233D                 | v4.48.4                                                              |
| Axis         | 243SA                | v4.45                                                                |
| Axis         | 243Q                 | v4.46                                                                |
| Axis         | Q7401                | v5.20.3                                                              |
| Axis         | Q7404                | v5.20                                                                |

**Table 12** Supported Camera and Encoder Firmware (continued)

|            |            |                                  |
|------------|------------|----------------------------------|
| Axis       | Q7406      | v5.11.1                          |
| Axis       | 247S       | v4.42                            |
| Axis       | P3301      | 5.40.92                          |
| Axis       | Q6035      | v5.25                            |
| Axis       | 241Q       | v4.47.5                          |
| IQinVision | IQ032S     | v3_4_5                           |
| IQinVision | IQM32NE-B5 | v3_4_5                           |
| IQinVision | IQ755      | v3.1.2                           |
| IQinVision | IQ765N     | v3_4_5                           |
| IQinVision | IQA35N     | v3_4_5                           |
| IQinVision | IQD32S     | v3_4_5                           |
| IQinVision | IQ705      | v3.1.2                           |
| IQinVision | IQ711      | v3.1.2                           |
| IQinVision | IQ852      | v3.1.2                           |
| IQinVision | IQ853      | v3.1.2                           |
| IQinVision | IQ855      | v3.1.2                           |
| IQinVision | IQA22S     | v3.1.2                           |
| Panasonic  | NP244      | 1.80 E4                          |
| Panasonic  | NS202A     | 2.74P0                           |
| Panasonic  | NP304      | 1.64E0_1.06                      |
| Panasonic  | NF302      | 1.64E0_1.06                      |
| Panasonic  | NP-502S    | np502_166E_cam_110               |
| Panasonic  | SC-385     | sc385_166E_cam_139               |
| Pelco      | Net5401    | 1.9.2.1-20130619-3.3081-O3.9819  |
| Pelco      | ISX0C      | 1.8.2.18-20121109-1.9080-A1.8503 |
| Pelco      | SD4E23     | 1.8.2.11-20120623-1.2084-O1.8120 |
| Pelco      | SD5118     | 1.8.2.18-20121126-1.9310-A1.8726 |
| Sony       | RX530      | V3.14                            |
| Sony       | RX570      | V3.15                            |
| Sony       | RX550      | V3.14                            |
| Sony       | DM110      | V1.11                            |
| Sony       | RZ25       | V1.40                            |
| Sony       | RZ30       | V3.14                            |
| Sony       | EP580      | V1.78                            |
| Sony       | CH240      | V1.77                            |
| Axis       | P3301      | 5.40.9.2                         |
| Axis       | 6032e      | 5.41.1.3                         |

**Table 12 Supported Camera and Encoder Firmware (continued)**

|                |               |                                       |
|----------------|---------------|---------------------------------------|
| Bosch AutoDome | 700IP         | 39500570                              |
| Pelco          | D5118-AD74029 | 1.8.2.18-20121126-1.9310-A1.8726      |
| Samsung        | SND-7080      | 2.00_121004                           |
| Sony           | CH240         | 1.77.00                               |
| Sony           | EP520         | 1.78.00                               |
| Panasonic      | SF335         | Application: 1.66<br>Image data: 2.02 |

## 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 13](#) 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 13 License Part Numbers**

| Part              | Description                                                                          |
|-------------------|--------------------------------------------------------------------------------------|
| FL-CPS-MS-SW7     | License for one Media Server on a physical server (Cisco UCS or MSP)                 |
| FL-CPS-OM-SW7     | License for one Operations Manager on a physical server (Cisco UCS or MSP)           |
| L-CPS-MS-SW7=     | eDelivery License for one Media Server on a physical server (Cisco UCS or MSP)       |
| L-CPS-OM-SW7=     | eDelivery License for one SASD on a physical server (Cisco UCS or MSP)               |
| L-CPS-SASD-7=     | eDelivery License for 1 SASD with VSM 7                                              |
| L-CPS-VSM7-1CAM=  | eDelivery License for 1 camera connection with VSM 7                                 |
| 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 |

**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).
- By default, you can add one Media Server and 10 non-Cisco cameras without purchasing or installing an additional license.

**Procedure**

---

**Step 1** Purchase additional licenses:

- a. Determine the part number for the license you want to purchase (see [Table 13](#)).
- b. 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>.
- c. 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:

- a. Locate the Product Authorization Key (PAK) that was created with the purchase.
- b. In a web browser, open the Cisco Product License Registration web page.  
<http://www.cisco.com/go/license/>
- c. 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.
- d. Transfer the file to the drive of the PC used for the configuration.

**Step 3** Install the license file in VSM:

- a. Log in to the Operations Manager.
- b. Select **System Settings > Software Licensing**.
- c. Click **Add** and select the license file located on your local drive.
- d. 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.

---

# Understanding the VSM Software Types

Table 14 describes the different types of software and firmware that are installed on servers, cameras, and encoders.

**Table 14** VSM Software Types

| Software Type                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| System software                     | <p>System software denotes the 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 Cisco VSM Management Console to update System Software, as described in the <b>Server Upgrade</b> section of <a href="#">Cisco Video Surveillance Management Console Administration Guide</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| OVA image<br>(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-7.2.0-331d_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 Video Surveillance Manager Flash Drive Recovery 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 14** 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> </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. Driver packs must be upgraded to the same version on each server where the Media Server and Operations Manager services are enabled or a driver pack mismatch error occurs. Templates cannot be revised when a driver pack mismatch error is present.</p> <ul style="list-style-type: none"> <li>• The Management Console interface can also be used to upgrade the driver packs for a single server at a time. See the “Driver Pack Management” section of the <a href="#">Cisco Video Surveillance Operations Manager User Guide</a>.</li> </ul> |
| Language Packs      | <p>Language packs can be added to display the VSM user interfaces in non-English languages. Language packs are added using the <b>Server Upgrade</b> page of the Cisco VSM Management Console. You must upgrade the language packs on all servers in your deployment.</p> <p>See the <b>Server Upgrade</b> section of <a href="#">Cisco Video Surveillance Management Console Administration Guide</a> for more information.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

## Obtaining VSM Software

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

### Procedure

- Step 1** Go to the following URL.  
<http://www.cisco.com/go/physicalsecurity>
- Step 2** Click **View All Products**.
- Step 3** Click the appropriate category (such as the Cisco IP Camera model).
- Step 4** Click **Download Software** and follow the on-screen instructions.



### Tip

You can also navigate to the [Cisco Video Surveillance Manager download page](#) and select an option for **Video Surveillance Device Driver Software** or **Video Surveillance Media Server Software**.

# Caveats

This section includes the following topics:

- [Using the Software Bug Toolkit, page 26](#)
- [Open Caveats, page 27](#)
- [Resolved Caveats, page 28](#)

## Using the Software Bug Toolkit

You can use the Bug Search Tool to find information about caveats (bugs) for this release, including a description of the problems and available workarounds. The Bug Search Tool lists both open and resolved caveats.

**Note**

---

Bug Search Tool is the successor to the Bug Toolkit.

---

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

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

To use the 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, then press **Enter**.
- Step 4** To look for information if you do not know the bug ID number, enter keywords which search for text matches in the following sections of a bug:
- headline/title
  - release note text
  - product
  - known affected releases/ known fixed releases:
- 

For more information about the Bug Search Tool, click **Help** on the main Bug Search Tool page:

<https://tools.cisco.com/bugsearch/>

## Open Caveats

Table 15 lists caveats that are open in this release.

**Table 15**      **Open Caveats**

| ID         | Description                                                               |
|------------|---------------------------------------------------------------------------|
| CSCtz36101 | Expand/Collapse mode for video not working when PTZ is enabled from MPC.  |
| CSCtz60444 | MS should not allow FmUpgrade and ServerUpgrade at the same time.         |
| CSCtz67269 | FmUpgr and driver pack upgrade should not be allowed to run concurrently. |
| CSCub06627 | SASD-Crash when total number of panes from multiple processes exceeds 48. |
| CSCub70689 | Bulk Soft deleting 101 cameras, 6 cameras failed.                         |
| CSCuc07318 | Client: Hard to re-size the Motion Window with low resolution.            |
| CSCuc23160 | Medianet camera not removed from MS cache.                                |
| CSCuc37050 | DHCP camera will not stream after MS goes down & up with IP change.       |
| CSCue26428 | Memory Leaks in SecureTcpSocket for HttpServer.                           |
| CSCue36418 | Media Server keeps sending Chassis Intrusion Event.                       |
| CSCue53069 | Audio not clear for Generic VAPIX2 drivers enabled camera.                |
| CSCue69485 | Perf: Queue overflow & frame drops seen when MS backup is initiated.      |
| CSCue81572 | Virtual MS has critical alert - Load Avg above threshold.                 |
| CSCue84002 | medianet: failover MS entry is not push to the camera NVRAM.              |
| CSCue86163 | Cameras' NTP entries not updated after MS's interface IP addr changes.    |
| CSCuf08169 | Serial PTZ connection on both Cyberdome I&II cannot be set at same time.  |
| CSCuf39097 | init_XXX scripts need to log failures to ims.log.                         |
| CSCug47472 | Critical hardware error when no hardware data reported.                   |
| CSCug72403 | Make event notifications "not fail" when bad XML encountered.             |
| CSCug82414 | SDT reports 0 values for all health data causing VSM critical event.      |
| CSCuh31987 | multicast port range validation is not happening for onvif devices        |
| CSCuh90217 | VSOM Global Settings doesn't work, when non-Admin user login to Win 8.    |
| CSCui02832 | UpdateCamera operation with 24 cameras take 2 hrs to complete.            |
| CSCui02955 | Cisco 29xx JPEG video freeze and jump.                                    |
| CSCui12720 | Missed RTP packets from 2830 camera.                                      |
| CSCui28694 | Sony RZ25P fails to configure HML stream intermittently.                  |
| CSCui38584 | RUS: Review Player Tamper Proof Tool exposes password on RUS client.      |

**Table 15**      *Open Caveats (continued)*

|            |                                                                          |
|------------|--------------------------------------------------------------------------|
| CSCui45429 | SASD Smooth video settings: issues with Cisco and onvif cameras.         |
| CSCui54480 | VSOM doesn't prompt to reset password.                                   |
| CSCui58382 | SASD Thumbnail: Need an error msg when creating clip with duped name.    |
| CSCui63138 | VSOM do not display 3M bitrate for 15FPS in 283x camera.                 |
| CSCui65920 | SASD Light: Cannot launch Wall if it's created by LDAP user.             |
| CSCui66256 | Cannot delete In-Progress Clip- Invalid clip type/state error.           |
| CSCui67961 | VSOM 7.0.x - After oversubscription error triggered, server still Red X. |
| CSCui69759 | Error when enable all 4 ports on 4P encoder.                             |

## Resolved Caveats

Table 16 lists caveats that are resolved in this release.

**Table 16**      *Resolved Caveats*

| ID         | Description                                                              |
|------------|--------------------------------------------------------------------------|
| CSCu154061 | Mediaout memory usage increase                                           |
| CSCu154864 | umsdevice core file generated from rebooting server for Motion Detection |
| CSCum30297 | All Cisco Services need to be stopped if init_mysql script fails         |
| CSCum50804 | VSMS DB server fails to start due to incorrect file permissions          |
| CSCum98663 | Detect DB issues - lost connectivity and missing files                   |
| CSCun92476 | Change to recording setting' warning not displayed in some scenarios     |

## 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. (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.

*Release Notes for Cisco Video Surveillance Manager, Release 7.2.2*  
© 2014 Cisco Systems, Inc. All rights reserved.

