Release Notes for Cisco Video Surveillance Manager, Release 7.6.1

Revised: December 2, 2015

This document provides important information for Release 7.6.1 of the Cisco Video Surveillance Manager (Cisco VSM).

Release 7.6.1 is a maintenance release that includes all features and improvements from Release 7.6.0, plus additional significant improvements in the quality of audio streaming and recording.

This document includes the following sections:

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

What's New in Release 7.6

The new features in Release 7.6.1 include the following:

New Features in Release 7.6.1

Support for Cisco 3050, 3620, 3630, 6620 and 6630 Cameras

Cisco VSM 7.6.1 adds support for Cisco 3050, 3620, 3630, 6620 and 6630 cameras. See the "Supported Devices" section on page 21 for more information.

Resolved Defects

Numerous defects were resolved in this release. See Resolved Caveats, page 44.

Support for Server Platforms

Release 7.6.1 can be installed on supported platforms only. See the "Supported Hardware Platforms" section on page 14 for more information.

Security Enhancements

Cisco Video Surveillance Manager release 7.6.1 resolves CSCur71072, the vulnerability to CVE-2014-3566- Poodle. Cisco recommends that you upgrade to this latest release.

Information about this vulnerability, and the affected versions, can be found at https://www.openssl.org/news/vulnerabilities.html.

New Features in Release 7.6.0

Operations Manager High Availability

In Release 7.6.x, two Operations Manager servers can be configured as a redundant pair for high availability (HA). Since the Operations Manager is responsible for configuring and coordinating the entire Cisco Video Surveillance deployment, this helps ensure uninterrupted system access for users and administrators.

To configure Operations Manager HA, install two servers: a Master server and a second Peer server. All configurations, data, and logs on the Master server are automatically replicated on the Peer server. If the Master server goes down or is unavailable, the Peer server is ready to take control with minimal impact.

For more information, see the following:

- Operations Manager HA Supported Configurations, page 8 for server, network, configuration, and other requirements.
- Cisco Video Surveillance Operations Manager User Guide for the following:
  - Overview information and configuration instructions.
  - See also the Troubleshooting section in the "Operations Manager High Availability" section for important information.

Camera App Licensing and Management

Cisco VSM 7.6.x introduces support for Camera Apps, which can be installed, licensed, updated, monitored, enabled, or disabled using the Operations Manager. These bulk management features allow Camera Apps to be managed in large numbers of cameras.

See the following important notes for more information:

- Camera App Licenses Must be Installed Using Operations Manager, page 10
- Camera Apps Are Disabled for When Modifying Templates, page 11

Installation and Upgrade Status

Cisco VSM 7.6.x includes major software installation and upgrade improvements using Operations Manager. You can now monitor the installation and upgrade status, including the installation/upgrade progress of Operations Manager and Media Server software, and all other services such as Map Server, Metadata generation, and Federator.

iOS Application for Apple Mobile Devices

Cisco VSM 7.6.x includes a new iOS mobile application for Apple devices such as the iPad and iPhone. App features include recorded video playback, thumbnail video preview, and user profiles that allow multiple users to share a single device. See the Apple App Store for more information.

New Cisco VSM Management Console Interface

The Cisco VSM Management Console has been redesigned for improved system maintenance features and functions. The Management Console user interface design is now also similar to the Operations Manager to improve functionality and ease-of-use.

Support for DSP Cameras

Cisco VSM 7.6.x supports the new Cisco 6500PD and 7030PD DSP cameras, which include:

- Camera App management and licensing.
- Integration of camera alerts (such as motion detection, video analytics and camera health) with Cisco VSM.

Additional Connected Edge Storage Features

- Cisco Video Surveillance Safety and Security Desktop (Cisco SASD) operators can now copy video from camera storage to Cisco VSM and play back the video using the SASD Alert workspace.
- Operations Manager can be used to format SD Cards installed in supported cameras.
- Camera health alerts are supported in IP Cameras configured with Connected Edge Storage. Health alerts include of SD Card failures.

Improvements in Network Management of Endpoints

- Cisco VSM 7.6.x supports NAT for IP cameras and encoders. This allows deployment models where the Media Server is separated from the cameras and encoders by NAT.
- The NTP server can be configured on multiple IP cameras and encoders (bulk management).
- IP cameras and encoders can be added using a hostname, or an IP address.

Recording and Grooming Improvements

- Cisco VSM 7.6.x changes the behavior for motion and event based recording when a camera generates events for a long period of time. In previous versions, the default behavior for record on motion/event was to stop recording after two hours. This was by design since events continuing for such a long period of time meant that motion detection or event recording was not properly configured. By stopping recording in this case, Cisco VSM protected the available storage and retention for other cameras. Customer feedback indicated that it was preferred that video continue to be recorded even at the expense of overall system retention time. As a result, Cisco VSM 7.6.x changes the behavior in this case to continue recording. See the Important Notes section for more information on how to properly configure motion recording.
- Cisco VSM 7.6.x includes improved performance when grooming video on heavily loaded Media Servers. The grooming will always complete as long as the overall recording load meets the supported specifications for the system.

Other Improvements

- The Internet Explorer (IE) 11 browser is supported for video monitoring on Windows 7 computers. See the Cisco Video Surveillance Monitoring Workstation Performance Baseline Specification for detailed information.
- Usability improvements for GIS Maps.

- The Cisco VSM Map Server can now be co-installed with the Operations Manager.
- 4x3 and 5x5 Views are now supported.
- Views can be configured with secondary streams.
- Cisco VSM can be configured with an external NTP server.
- Templates are now available for 8 additional Axis IP camera models and 2 additional Axis encoder models.
- A separate pop-up video window can be displayed in Cisco SASD.
- Multi-pane Views can be created, edited and saved using Cisco SASD.
- The CPS-UCS-1RU-K9 and CPS-UCS-2RU-K9 servers support 4TB drives.
- Usability improvements to SASD Alert/Event display including sortable alert types and color coded event status.

Getting Started

Cisco VSM Release 7.6.1 is pre-installed on new servers, can be installed as a virtual machine, or used to upgrade an existing deployment.

Table 1 Cisco VSM Installation and Upgrade Options

Option	Description	Notes
Pre-installed	Release 7.6.1 is pre-installed in new installations on the Cisco Connected Safety and Security UCS Platform Series servers CPS-UCS-1RU-K9 and CPS-UCS-2RU-K9.	See Cisco Connected Safety and Security UCS Platform Series Servers (Release 7.2 and Higher), page 6 for more information.
Upgrade from Release 7.2.x or higher	Cisco VSM Release 7.2.x and 7.5.x can be upgraded directly to Release 7.6.1. Upgrades can be performed on Cisco VSM virtual machines (VMs) and on Cisco Video Surveillance servers. Servers include the Cisco Multiservices Platform (Cisco MSP) and the Cisco Connected Safety and Security UCS Platform Series servers.	Upgrades from 7.2.0 and earlier are not supported. Upgrade to r7.2.1 or 7.2.2, or 7.5 first, and then upgrade to release 7.6.1. Upgrading from Previous Cisco VSM Releases, page 7 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 Cisco Video Surveillance Virtual Machine Deployment and Recovery Guide for UCS Platforms for more information.

See the following for more information:

- Cisco Connected Safety and Security UCS Platform Series Servers (Release 7.2 and Higher), page 6
- Upgrading from Previous Cisco VSM Releases, page 7
- Recovery/Factory Image, page 7
- Migrating from Cisco VSM Release 6.3.x, page 7

Cisco Connected Safety and Security UCS Platform Series Servers (Release 7.2 and Higher)

Cisco VSM Release 7.6.1 is pre-installed on new installations of the Cisco Connected Safety and Security UCS Platform Series (CPS-UCS-1RU-K9 and CPS-UCS-2RU-K9) when ordered with the Cisco VSM software installed.

- 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 Previous Cisco VSM Releases

Cisco VSM releases 7.2.x and higher can be upgraded using the Release 7.6.1 system `.zip` file that includes all required software packages. 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.

To upgrade from Release 7.2.0 or lower, you must first upgrade to Release 7.2.1, 7.2.2 or 7.5, and then upgrade to Release 7.6.1. See the Release Notes for the release running in your deployment for more 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.
- Release 7.2 was pre-installed on the Cisco Connected Safety and Security UCS Platform Series (CPS-UCS-1RU-K9 and CPS-UCS-2RU-K9).
- Virtual Machine (VM) installations can also be upgraded using the Cisco VSM Management Console.

Recovery/Factory Image

You can also create a bootable USB flash drive that can be used to recover an installation or perform a a factory installation of Cisco VSM 7 on a supported physical server that shipped with Cisco VSM 7 pre-installed. This includes:

- Release 7.2.0 and higher—Cisco Connected Safety and 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) shipped with Cisco VSM 7.0.
- Release 6.3.2—Cisco Physical Security Multiservices platform servers (CIVS-MSP-1RU, CIVS-MSP-2RU and CIVS-MSP-4RU)

For more information, see the following documents:

- Cisco Video Surveillance Manager Recovery Guide (Cisco Connected Safety and Security UCS Platform Series)
- Cisco Video Surveillance Manager Recovery Guide (Cisco MSP Platform)

Migrating from Cisco VSM Release 6.3.x

The migration procedure requires assistance from a Cisco representative. To migrate an existing system, you must first migrate the servers and data from Cisco VSM 6.3.2 MR2 and 6.3.3 to Cisco VSM 7.2.x, and then upgrade the system to Release 7.6.1:

1. Contact your Cisco representative for assistance and instructions.
2. Migrate the system from Cisco VSM 6.3.2 MR2 or 6.3.3 to Cisco VSM 7.2.x.
3. Upgrade all physical and virtual Cisco VSM servers to Release 7.6.1 using the Cisco VSM Management Console.

Contact your Cisco representative for more information.

Important Notes

Note Please also see the Cisco VSM 7.5 Release Notes for more other important notes that apply to this release.

Operations Manager HA Supported Configurations

Cisco VSM Operations Manager high availability (HA) is supported with the following hardware and software requirements. For more information, see the following:

- "Operations Manager High Availability" section of the Cisco Video Surveillance Operations Manager User Guide configuration, monitoring, and management instructions.
- Cisco VSM Operations Manager High Availability Troubleshooting Guide for up-to-date solutions to common issues.

Table 1-2 Requirements

Requirements	Requirement Complete? (✓)
To configure Operations Manager HA, admins must belong to a User Group with permissions for *Servers & Encoders*. See the Cisco Video Surveillance Operations Manager User Guide for more information.	❑
Two standalone physical or virtual servers must be installed on the network. – Supported physical servers: CPS-UCS-1RU-K9 or CPS-UCS-2RU-K9 – Supported virtual machines: VMs deployed using the Cisco VSM release 7.5 or 7.6 OVA templates. **Note** Any data on the server used as the Peer server will be deleted and replaced with the data from the Master server.	❑
We recommend two CPS-UCS-2RU-K9 servers for best performance. • Performance issues can occur using the CPS-UCS-1RU-K9 servers for Operations Manager HA since performance issues (such as slowness) may occur. • Do not mix a CPS-UCS-2RU-K9 server with a CPS-UCS-1RU-K9 server.	❑

Table 1-2 Requirements

Requirements	Requirement Complete? (✓)
Additional server requirements and recommendations: • Stand-alone servers—Only stand-alone physical or virtual servers are supported in an HA configuration. The Operations Manager servers can not be co-located with other server services, such as a Media Server. • Operating system—Red Hat 6.4 64 bit OS only (SUSE and Red Hat 5.8 are NOT supported). • We recommend that both servers have the same hardware specifications such as processor, hard disk storage, and other attributes. For example, two CPS-UCS-2RU-K9 servers. • We do not recommend using Cisco UCS E-series platform servers for Operations Manager HA. • Both servers used for HA must be fully up and running prior to configuring HA or replacing the Peer server. Verify that there are no pending jobs (of any kind) in the Peer server.	❑
Split Brain recovery support: • At least one Media Server must be added to the Split Brain Configuration to support recovery if communication between the Master and Peer server is lost. • See the Cisco Video Surveillance Operations Manager User Guide for more information.	❑
Network requirements: • Subnet—Both servers must be in the same network subnet. This ensures connectivity and data synchronization between the servers. • NIC port—Both servers must be connected to the network using the same NIC port: for example, Eth0. Only a single Ethernet port can be active (either Eth0 or Eth1). • Three IP addresses/hostnames are required: – An IP address/hostname for the Master server Ethernet (NIC) port. – An IP address/hostname for the Peer server Ethernet (NIC) port. – A virtual IP address that is shared by both servers. **Note** End-users should always use the virtual IP address to access the Operations Manager since it will still work even in a failover occurs. Users should never use the server Ethernet port (NIC) address since connectivity can be lost if the server is unreachable.	❑
Security certificate requirements: By default, all Cisco VSM server include a self-signed certificate. Using the self-signed certificate on the Operations Manager server causes a security warning to appear when users log in the Operation Manager. To avoid this, you can create and install a web server certificate for the Operations Manager servers. The certificate must point to the HA virtual IP address and be installed on both Operations Manager servers (Master and Peer) used in the HA configuration. For more information: • See the “Operations Manager High Availability” section of the Cisco Video Surveillance Operations Manager User Guide. • Cisco Video Surveillance Management Console Administration Guide for instructions to install the certificate.	❑

Table 1-2 Requirements

Requirements	Requirement Complete? (✓)
Network Time Protocol (NTP) server: All servers must be configured with the same NTP configuration to ensure the time settings are accurate and identical. See the "NTP Information" section of the Cisco Video Surveillance Operations Manager User Guide for more information.	❑
Passwords: • The Management Console password for Operations Manager each server. This is the *localadmin* password used to access the Cisco VSM Management Console, and is set during the initial server setup. • The admin password used to access the browser-based Operations Manager interface.	❑

Firewall Service on a Red Hat Cisco VSM Server

If the firewall service was stopped on a Red Hat Cisco VSM server prior to upgrading to Cisco VSM release 7.6.1, the Cisco VSM 7.6.1 upgrade will start the firewall service.

Camera App Licenses Must be Installed Using Operations Manager

There are two types of camera app licenses:

- A device-specific license installed directly on a single device. This license does not allow Operations Manager to manage the license or app.
- A single or group license that is installed and managed using Operations Manager.

Only one of these license types can be active on the camera device at a time. To use the license(s) managed by Operations Manager, you must first deactivate any device-specific licenses.

Procedure

Step 1 If any camera app licenses are installed on the device, deinstall those licenses using the camera UI.

Step 2 Obtain the Operations Manager license(s), See the "Obtaining and Installing Licenses" section on page 37.

Step 3 Use Operations Manager to install and manage the camera app licenses. See the Cisco Video Surveillance Operations Manager User Guide for more information.

Camera Apps Are Disabled for When Modifying Templates

Camera video apps may be automatically disabled on Cisco cameras if the camera template is modified in one of the following ways:

1. Camera video apps are automatically disabled on Cisco cameras if a custom template is applied that is configured with a high primary stream resolution (5M) or a frame rate higher than 15fps. This occurs even if camera apps are enabled on the template. A configuration mismatch also occurs on the device. To avoid this, you must configure the camera custom template before enabling the camera apps.

   Affected Cameras—Cisco camera models 2830, 2835, 3421, 3520, 3530, 3535, 6020, 6050, 6400, 6030, 6000P, 6400E, 6930, 7030, and 7530E.

2. If the device has camera apps enabled, and the primary stream configuration is changed from Low or Medium to High, or if you enable the secondary video stream, then the camera apps are automatically disabled on the device.

   Affected Cameras—Cisco camera models 3421, 3520, 3530, 3535, 2830, and 2835.

To avoid this, you must configure the camera custom template before enabling the camera apps, as described in the following Workaround.

Workaround

1. Disable all video apps that are running on the device.
2. Change the configuration, as necessary:
   a. Configure the custom template with high primary stream resolution or a frame rate higher than 15fps.
   b. Enable the secondary video stream.
3. Enable all required camera apps in the camera's custom template.

See CSCuq09351 for more information.

Backups to Local Disk Support Configuration Data Only

Prior to Cisco VSM release 7.5, automatic backups to local storage could include configuration and historical data. In release 7.5 and later, however, automatic backups to the local disk support configuration data only. When upgrading from release 7.2 or earlier to release 7.5 or later, any automatic backups will be changed to the configuration only option.

Record on Motion Enhancements

In Cisco VSM Release 7.5, Record on Motion recordings are started when as single Motion Start command is received from the camera. Recording continues until a Motion Stop is received. If the camera is not configured correctly, it may detect motion continuously and it will not send a Motion Stop command for a long time. Also, in the rare scenario where a Motion Stop event from the camera is missed, motion recording would continue indefinitely and a large amount of storage would be used.

To address these issues, Cisco VSM Release 7.5 limits the maximum duration for motion recording after a Start command to 2 hours if no stops are received. However, it is possible that valid motion that lasts longer than 2 hours is being seen by the camera, and the video after 2 hours will not be recorded with motion recording in Cisco VSM Release 7.5.

Cisco VSM 7.6.x resolves all of these issues by changing Record on Motion in two ways:

- Configures Cisco cameras to send Motion Start commands continuously as long as there is motion. Recording starts when a Motion Start is received and it stops after 1 minute if no more Start commands are received.
- The 2 hour limit on motion recording has also been eliminated.

Best Practices for Recording on Motion

When using motion recording in Cisco VSM, there are several important considerations that should be followed to properly control the recording of video with motion detection.

Cisco VSM supports configuration for default motion detection settings to allow quick setup of camera motion detection. The motion detection inclusion window is set to the full frame and sensitivity is set to a default value. These settings may or may not be optimal for detecting video in all situations depending on many factors such as lighting, the camera placement and if there is extraneous motion in the scene. For example, if there is an area in the frame where there is always motion, the camera may continuously detect motion and motion recording will continuously record video. Prior to Cisco VSM 7.6.x, recording would stop by default after 2 hours of continuous motion activity. In Cisco VSM 7.6.x, that behavior has been changed and motion based recording will continue as long as there is motion activity. This may negatively affect video retention for all cameras on the same Media Server, if this motion recording behavior s not expected.

Review the following best practices and recommendations when using motion recording.

- Do not rely solely on the default motion detection settings for motion recording for outdoor cameras without assessing the results. Outdoor scenes are more complex with changes in lighting (day/night), clouds, people, cars, trees, and leaves moving in the wind. For outdoor cameras, it is very common to have extraneous motion that should be ignored because that activity is not of interest. First, adjust the zoom and focus so the camera's field of view and focus so that the detection settings are optimal for all moving objects in that field of view. Second, the motion detection inclusion and/or exclusion windows should to be set, not just the sensitivity settings. This helps to accurately trigger recording for the important motion activity while ignoring undesired activity. Roads and trees in the background are common causes of unexpected motion activity where motion only in the foreground is desired for controlling recording.
- When configuring motion recording, make sure that the camera is detecting motion as expected. Use the Operation Manager's motion detection configuration page to observe the camera's motion activity, and ensure the field of view is correct. Make sure that motion is being detected as expected and adjust the inclusion and exclusion windows and settings as needed.
- When configuring motion detection for a camera using Operation Manager, always click the **Save Motion Config** button to save changes before closing the browser or leaving the motion configuration page. If you do not save the motion settings, the motion detection recording will not operate as intended.

Event History Cleared When Upgrading from 7.2 or Earlier

Upgrades from versions 7.2 or earlier will clear all event history (the event history data is not included in the upgrade).

Save View is Removed from the Operations Manager *Monitor* Page

The Save View option is removed from the Operations Manager Monitor page in Release 7.6.x.

To create views, use the Operations Manager Views admin page, or the Cisco Video Surveillance Safety and Security Desktop (Cisco SASD) application.

Released Versions

Cisco VSM Release 7.6.1 is released with Build 34i. The component package versions are:

- VSBase-7.6.1-016d.i686
- VSRecorder-7.6.1-016d.i686
- MPClient-7.6.0-35.noarch
- CDAF-7.6.1-11.noarch
- Tomcat-7.0.55-3.noarch
- VSMUpgrade-7.6.1-016d.i686
- VSMS-7.6.1-016d.i686
- VSDrivers-7.6.1-016d.i686
- SASD-7.6.0-47.noarch
- VSOM-7.6.1-11.i386
- GeoServer-7.6.1-001.noarch
- AMQBroker-7.6.1-1.noarch
- MetaDataService-7.6.1-016d.i686
- VSTools-7.6.1-016.noarch
- VSF-7.6.1-11.noarch

In addition, the monitoring client versions are:

- AXClient: 7.6.35.50124
- SASD: 7.6.47.12016

Supported Hardware Platforms

Cisco VSM Release 7.6.1 runs on the following hardware platforms:

Table 3 Supported Hardware Platforms

Platform Type	Server Models	Installation Method
Physical Server	Cisco Physical Security UCS platform servers: CPS-UCS-1RU-K9 and CPS-UCS-2RU-K9 **Note** The CPS-UCS-xRU-K9 servers are available only with Red Hat 6.4 x64 pre-installed. See Red Hat 6.4 Support (64-bit), page 14 for more information.	• Pre-installed in new servers. • Recover using the USB recovery stick. • Upgrade RPMs using the Management Console. **Related Documentation** • Cisco Video Surveillance Management Console Administration Guide • Cisco Video Surveillance Manager Recovery Guide (Cisco Connected Safety and Security UCS Platform Series)
Physical Server	Cisco Multiservices platform servers: • CPS-MSP-1RU-K9 • CPS-MSP-2RU-K9 **Note** The CIVS-MSP 1RU, 2RU and 4RU server platforms are supported in Cisco VSM Release 7.5.x and lower only.	Upgrade RPMs using the Management Console. See the Cisco Video Surveillance Management Console Administration Guide.
Virtual Machine	Cisco UCS platform: B, C, E and Express series	• New VM Installations—Install the Cisco VSM Release 7.6.1 `.OVA` image on the virtual machine. See the Cisco Video Surveillance Virtual Machine Deployment and Recovery Guide for UCS Platforms. • Upgrade existing VM installations using the Management Console.

Red Hat 6.4 Support (64-bit)

Cisco VSM Release 7.5 and higher is available with Red Hat 6.4 x64 (a 64-bit version of Red Hat Linux) on the following platforms:

- Pre-installed on physical CPS-UCS-1RU-K9 and CPS-UCS-2RU-K9 servers.
- Virtual machines deployed from a VSM 7.5 or later OVA template.

This allows a larger maximum storage partition size for video in Cisco VSM Release 7.5 and higher:

- Cisco VSM Release 7.2: 16TB (Terabytes) maximum
- Cisco VSM Release 7.5 and higher: 100TB (Terabytes) maximum

Supported Server Services

Each server can run one or more services that provide features and functions for the Cisco Video Surveillance system.

Cisco VSM Release 7.6.1 supports the following server services:

- Operations Manager—The browser-based Cisco VSM Operations Manager administration and configuration tool. Each deployment requires a single Operations Manager. Two Operations Manager servers can be installed in a redundant configuration.
- Media Server—The Cisco Media Server service provides video streaming, recording and storage for the cameras and encoders associated with that server. Media Servers can also be configured for high availability, and provide redundant, failover, and long term storage.
- Map Server—Allows Image Layers to be added to location maps and viewed by operators using the Cisco Video Surveillance Safety and Security Desktop application. Map images represent the real-world location of devices and events.
- Metadata Server for Motion Analysis—Allows metadata to be added to recorded video, which enables the Video Motion Search in the Cisco SASD desktop application (and for access by 3rd party integrators).
- Federator Server—the Federator service is used to monitor video and system health for the cameras and resources of multiple Operations Managers. The Federator interface is accessed using a web browser or the Cisco SASD. Federator desktop application.

Note The Maps, Metadata and Federator server services each require a standalone server in this release. See Table 4 for more information.

Table 4 describes the supported server services and how each is enabled or disabled in this release.

Table 4 Supported Server Services In This Release

Service	Description	Activation Rules
Operations Manager	The browser-based Cisco VSM Operations Manager administration and configuration tool.	Can be added as a stand-alone server, or co-located with other services (such as a Media Server and/or Maps Server). **To Enable:** 1. Install the server and complete the Management Console Setup Wizard and select the **Operations Manager** service. 2. (Optional) Select the Media Server service to create a co-located server. This automatically enable the Media Server service on the default "VSOMServer". 3. (Optional) Add additional servers to the Operations Manager configuration, and select the Service Type to enable a service on the server. **Note** At least one Media Server must be added to the Operations Manager for the system to be functional. 4. Use the Operations Manager to further configure the services and system features. **Related Documentation:** • Cisco Video Surveillance Operations Manager User Guide. Specifically: – "Summary Steps to Add or Revise a Server" – "Configuring Media Server Services" • Cisco Video Surveillance Management Console Administration Guide **To Disable:** 1. Log in to the Management Console for each server associated with the Operations Manager server and click the **Remove** button. **Note** The **Remove** button disassociates the server and all server services from the Operations Manager. This allows the server (and running services) to be added and managed by a different Operations Manager. 2. Log in to the Management Console for the Operations Manager server and deselect the **Operations Manager** service.

Table 4 Supported Server Services In This Release (continued)

Service	Description	Activation Rules
Media Server	The Media Server service provides video streaming, recording and storage for the cameras and encoders associated with that server. Media Servers can also be configured for high availability, and provide Redundant, Failover, and Long Term Storage	Can be added as a stand-alone server, or co-located on a single server with the Operations Manager and/or Maps service. **To Enable:** 1. Install the server and complete the Management Console Setup Wizard. 2. (Co-located server) Log in to the Operations Manager, select **System Settings > Server**, and select the default **VSOMServer**. In the Services section, select the **Media Server** service. 3. (Stand-alone server) Log in to the Operations Manager and add the server as a **Media Server**. 4. Select the Media Server **Advanced** settings to further configure the service, if necessary. **Related Documentation** • Cisco Video Surveillance Operations Manager User Guide. Specifically: – "Adding or Editing Servers" – "Server Settings" – "Configuring Media Server Services" • Cisco Video Surveillance Management Console Administration Guide **To Disable:** • Log in to the Operations Manager, select **System Settings > Server**, select the server, and deselect the **Media Server** service. or • Log in to the Management Console for the server, and click *Remove* to remove the server from the Operations Manager. Then deselect the service.

Table 4 Supported Server Services In This Release (continued)

Service	Description	Activation Rules
Map Server	Allows Image Layers to be added to location maps using the Operations Manager. Image layers are viewed by operators using the Cisco Video Surveillance Safety and Security Desktop application. Cameras, locations and alerts are displayed on dynamic maps, and map images that represent the real-world location of devices and events.	Use the Operations Manager to activate the service. **Note** This service is supported as a stand-alone server on a server running the RHEL 6.4 64 bit OS, or co-located on a Operations Manager server. **To Enable a Stand-Alone Server:** 1. Install the server and complete the Management Console Setup Wizard. 2. Log in to the Operations Manager and add the server as a **Maps Server**. 3. Configure the Location Maps. **To Enable a Co-Located Maps Server:** 1. Log in to the Operations Manager. 2. Navigate to the Operations Manager server configuration page. See 3. Select the **Maps Server** to enable the service on the Operations Manager server. 4. Configure the Location Maps. **Related Documentation** • Cisco Video Surveillance Management Console Administration Guide • Cisco Video Surveillance Operations Manager User Guide. Specifically: – "Adding or Editing Servers" – "Server Settings" – "Configuring Media Server Services" **To Disable:** • If the Operations Manager is not co-located with the Maps Server, log in to the Management Console for the server, click **Remove** to remove the server from the Operations Manager, and then deselect the service. • If the Operations Manager is co-located with the Maps Server, log in to the Operations Manager and deselect the Media Server service. **Image Layer Considerations** Images used for map layers should be optimized to the smallest file size that preserves image quality. Large image files can consume excessive processing power and degrade system performance. For details, refer to the Cisco Video Surveillance Operations Manager User Guide ("Configuring Location Maps" requirements section).

Table 4 Supported Server Services In This Release (continued)

Service	Description	Activation Rules
Metadata Server	Allows metadata to be added to recorded video, which enables features such as Video Motion Search in the Cisco SASD desktop application. Metadata can also be accessed by 3rd party integrators for advanced analytics analysis.	Use the Operations Manager to activate the service. **Note** This service is supported as a stand-alone server only, on a server running the RHEL 6.4 64 bit OS. **To Enable:** 1. Install the server and complete the Management Console Setup Wizard. 2. Log in to the Operations Manager and add the server as a **Metadata Server**. 3. Continue to "Enabling Video Analytics". **Related Documentation** • Cisco Video Surveillance Management Console Administration Guide • Cisco Video Surveillance Operations Manager User Guide. Specifically: – "Adding or Editing Servers" – "Server Settings" – "Enabling Video Analytics" **To Disable:** • Use the Operations Manager to deactivate the service on the server. or • Use the Management Console to *Remove* the server from the Operations Manager, and then deselect the service. **Metadata Server Considerations** • Video motion analysis is supported for the primary stream only in this release. JPEG recordings are not supported. • Only one request per camera to generate the luminance metadata is supported by the Metadata server. The second request to generate luminance metadata for the same camera will fail while the previous request is still being processed. • The Metadata server will execute only five parallel request for luminance metadata, remaining requests will be queued and executed in the order they were requested.

Table 4 Supported Server Services In This Release (continued)

Service	Description	Activation Rules
VSF	Enables the Federator service used to monitor video and system health for the cameras and resources of multiple Operations Managers. The Federator service can only be enabled on a stand-alone server in this release. Other server services cannot be enabled on the same server as the Federator service. The Federator interface is accessed using a web browser or the Cisco SASD. Federator.	Activated using the Management Console only. Cannot be activated using the Operations Manager. **Note** This service is supported as a stand-alone server only, on a server running the RHEL 6.4 64 bit OS. **To Enable:** 1. Log in to the Management Console. 2. Install the server and complete the Setup Wizard: select the **VSF** service. 3. Log in to the Cisco VSM Federator browser-based interface. 4. Continue to the "Using Federator to Monitor Multiple Operations Managers" section. **Related Documentation** • Cisco Video Surveillance Management Console Administration Guide • Cisco Video Surveillance Operations Manager User Guide. Specifically: – "Using Federator to Monitor Multiple Operations Managers" **To Disable:** • Log in to the Management Console and deselect the **VSF** service.

Supported Devices

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

Supported Devices: Cisco

Table 5 provides information about Cisco devices supported in this release:

Table 5 Supported Devices: Cisco

											Medianet. Support		
Model	**FW Version for Release 7.6.x Compatibility**	**Video Format**	**Media Types**	**Audio**	**Dual Stream**	**Motion Detection**	**Firmware Upgrade**	**Privacy Mask**	**Edge Storage**	**Camera App Support**	**Phase 1**	**Phase 2**	**Phase 3 (requires firmware 2.0.0-175)**
2400 Series	2.5.2.2	NTSC / PAL	MPEG-4 MJPEG	NA	Yes	Yes	Yes	No	No	No	No	No	No
2500 Series	2.5.2.2	NTSC / PAL	MPEG-4 MJPEG	Yes	Yes	Yes	Yes	No	No	No	No	No	No
2600 Series	4.4.2	NTSC / PAL	H.264 MPEG-4 MJPEG	Yes	Yes	Yes	Yes	No	No	No	Yes	No	No
2830	Minimum 2.0.3 Latest 2.7.0	NTSC	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
2835	Minimum 2.0.3 Latest 2.7.0	PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 5 Supported Devices: Cisco (continued)

2900 Series	1.6.18	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	No	No	No	No	No	No
3050	Minimum 2.0.3 Latest 2.7.0	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
3421V	Minimum 2.0.3 Latest 2.7.0	NTSC / PAL	H.264 MJPEG	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
3520	Minimum 2.0.3 Latest 2.7.0	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
3530	Minimum 2.0.3 Latest 2.7.0	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
3535	Minimum 2.0.3 Latest 2.7.0	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
3620	Minimum 2,7.1 Latest 2.7.1	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
3630	Minimum 2,7.1 Latest 2.7.1	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
4300	Minimum 2.4.2-289	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	No	No	No	Yes	No	No
4300E	Minimum 3.2.3-218	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	No	No	No	Yes	No	No
4500	Minimum 2.4.2-289	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	No	No	No	Yes	No	No
4500E	Minimum 3.2.3-218	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	No	No	No	Yes	No	No
5000 Series	Minimum 1.6.17	NTSC	H.264 MJPEG	NA	Yes	Yes	Yes	No	Yes	No	No	No	No
6000P	Minimum 2.0.3 Latest 2.7.0	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
6020	Minimum 2.0.3 Latest 2.7.0	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 5 Supported Devices: Cisco (continued)

6030	Minimum 2.0.3 Latest 2.7.0	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
6050	Minimum 2.0.3 Latest 2.7.0	NTSC / PAL	H.264 MJPEG	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
6400	Minimum 2.0.3 Latest 2.7.0	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
6400E	Minimum 2.0.3 Latest 2.7.0	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
6500PD	Minimum 2,5.1 Latest 2.7.0	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
6620	Minimum 2.7.1 Latest 2.7.1	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
6630	Minimum 2.7.1 Latest 2.7.1	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
6930	Minimum 2.0.3 Latest 2.7.0	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
7030	Minimum 2.0.3 Latest 2.7.0	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
7030E	Minimum 2.0.3 Latest 2.7.0	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
7530PD	Minimum 2.0.3 Latest 2.7.0	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 5 Supported Devices: Cisco (continued)

CIVS-SENC-4P (encoder)	Minimum V1.2.0-4	NTSC/PAL	H.264 MPEG-4 MJPEG	Yes	Yes	Yes	Yes	No	No	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	No	No

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 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 does not support Contact Closure, Cisco 7030 camera supports 3 input ports. All other Cisco 3000, 6000 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 6 provides information about Arecont devices that this Cisco VSM release supports.

Table 6 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	65187	H.264 MJPEG	Yes	Yes	No
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	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 7 provides information about Axis devices that this Cisco VSM release supports.

Table 7 Supported Axis Devices

Model	Type	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
243SA	Encoder	4.45	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
243QBlade	Encoder	4.46.1	NTSC / PAL	MPEG-4 MJPEG	NA	Yes	Yes	Yes	Yes
247S	Encoder	4.42	NTSC / PAL	MPEG-4 MJPEG	Yes	Yes	Yes	Yes	Yes
M3006	IP Camera	5.55.1.2	NTSC	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes
M3007	Panoramic Camera	5.40.13.2	NTSC	H.264 MJPEG	No	Yes	Yes	Yes	Yes
P1214	IP Camera	5.40.12.3	NTSC	H.264 MJPEG	No	Yes	Yes	Yes	Yes
P1353	IP Camera	5.40.19.1	NTSC	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes
P3301	IP Camera	5.40.92	NTSC	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes
P3364	IP Camera	5.40.17.1	NTSC	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes
P3367	IP Camera	5.50.3	NTSC	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes
P3915	IP Camera	5.55.3	NTSC	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes
P7214	Encoder	5.50.2	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes
Q1604	IP Camera	5.50.3	NTSC	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes
Q6045	IP Camera	5.55.11	NTSC	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes
Q7401	Encoder	5.50.2	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes

Table 7 Supported Axis Devices (continued)

Q7404	Encoder	5.20	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes
Q7406	Encoder	5.11.1	NTSC / PAL	H.264 MJPEG	N/A	Yes	Yes	Yes	Yes
Q7424	Encoder	5.40.10	NTSC / PAL	H.264 MJPEG	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 8 Axis M3007 Options

Model	Field Of View	PTZ	Motion Detection
Axis M3007			
	360 degree 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 9 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

Table 9 Axis M3007 Field-Of-View Options (continued)

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

Supported Devices: IQinVision

Table 10 provides information about IQinVision devices that this Cisco VSM release supports.

Table 10 Supported IQinVision Devices

Model	Type	Supported FW Version	Video Format	Media Types	Audio	Dual Stream	Stream Mirroring	Motion Detection	Firmware Upgrade
IQ032SI-V 11	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
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 11 provides information about Mobotix devices that this Cisco VSM release supports.

Table 11 Supported Mobotix Devices

Model	Type	Supported FW Version	Video Format	Media Types	Audio	Dual Stream	Motion Detection	Firmware Upgrade
x10	IP Camera	M10 v.2.0	NTSC	MPEG-4 MJPEG	No	No	No	No

Additional Notes on Mobotix Devices

- Moboitx 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 12 provides information about Panasonic devices that this Cisco VSM release supports.

Table 12 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
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 13 Panasonic SF 458 and SF 438 Field-Of-Views Support

Model	Field Of View	PTZ	Motion Detection
Panasonic SW458 and SF438	Fisheye 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 14 provides information about Pelco devices that this release supports.

Table 14 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
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 15 provides information about Sony devices that this release supports.

Table 15 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	3.154	NTSC / PAL	H.264 MPEG-4 MJPEG	Yes	Not supported	Yes	No

Table 15 Supported Sony Devices (continued)

RX 570	IP Camera	3.15	NTSC / PAL	H.264 MPEG-4 MJPEG	Yes	Not supported	Yes	No
RX 550	IP Camera	3.14	NTSC / PAL	H.264 MPEG-4 MJPEG	Yes	Not supported	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: Generic IP Cameras

Cisco VSM Release 7.6.1 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 16 Supported Generic Devices

Type	Supported Version	Video Formats	Media Types	Audio	Dual Stream	PTZ	Motion Detection	Firmware Upgrade
ONVIF	2.0	NTSC / PAL	H.264 MPEG-4 MJPEG	Yes	Yes	Yes	No	No
Generic Axis	3.0 / Firmware 5.x	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	No
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

Table 16 Supported Generic Devices (continued)

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	6th Generation IP cameras VMxxx and VBxxx	NTSC / PAL	H.264 MJPEG	Yes	Yes	No	No	No
Sony	2nd, 3rd, 4th and 5th generation Sony IP cameras	NTSC / PAL	H.264, MPEG-4, MJPEG	Yes	Yes	Yes	Yes	No

Additional notes on Axis Generic Devices

- 5MP, 3MP and 2MP resolution support has been added to Generic Axis version 3.0 capable devices. There are other 4:3 and 16:9 aspect ratio resolutions that are also supported for these devices.
- Axis VAPIX 3.0 cameras running firmware version 5.4 or higher support the connected edge storage feature.

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 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.
- 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 Operations Manager. This page is at Setup --> System Options --> Security --> ONVIF --> Add
- ONVIF camera and VSMS server to which ONVIF camera is being added should have their time synchronized ideally using NTP.
- For Sony models, only UDP is supported. Streaming fails if TCP is selected.
- For Bosch models, a frame rate of 30 alone is supported, and dual streaming is not supported.
- For some Hikvision models, the camera requires a reboot after the codec is changed from Cisco 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 Mobotix Generic Devices

- For M12 cameras, if the NTP server on the camera is not configured successfully, motion detection does not work reliably.

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.
- We have added support for ‘move command’ and ‘continuous PTZ command’ depending upon whatever supported by the Sony camera. If both supported, ‘continuous PTZ command’ is chosen for PTZ operations. When using a mouse for models that only support ‘move command’, PTZ will require the user to continuously move the mouse for the camera to pan. PTZ behavior with a joystick is closer to other models supporting ‘continuous PTZ’ commands.
- Sony 6th generation cameras have a separate have a separate driver and need to added as 6th generation in Cisco VSM. Note that current Sony 6th generation model numbers start with like VM6XX or VB6XX.

Supported Devices: Analog Cameras

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

Table 17 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
Pelco Analog Camera	NTSC / PAL	Encoder Dependent (for use with only PelcoNET540xT encoders)
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

Following camera models have been tested as generic IP cameras.

Table 18 Supported Generic IP Cameras

Camera Model	Generic IP Camera Type	Validated Firmware Version	Video Formats	Media Types	Audio	Dual Stream	PTZ	Motion Detection	Firmware Upgrade
Axis 6034-E	ONVIF 2.0	5.41.1.2	NTSC	H.264 MJPEG	Yes	Yes	Yes	No	No
Samsung SND-7080	ONVIF 2.0	2.00_121004	NTSC	H264 MJPEG	No	Yes	No	No	No
Sony CH240	ONVIF 2.0	1.79.00	NTSC	H264 MJPEG	Yes	Yes	No	No	No
Panasonic SW458	ONVIF 2.0	1.42	NTSC	H264 MJPEG	Yes	Yes	No	No	No
Axis 3301	Axis VAPIX 3.0/Firmware 5.x	5.41.2	NTSC / PAL	H264 MJPEG	Yes	Yes	Yes	Yes	No
Axis 3367	Axis VAPIX 3.0/Firmware 5.x	5.50.3	NTSC / PAL	H264 MJPEG	Yes	Yes	Yes	Yes	No
Axis Q6034	Axis VAPIX 3.0/Firmware 5.x	5.41.1.2	NTSC / PAL	H264 MJPEG	Yes	Yes	Yes	Yes	No
Axis 215	Axis VAPIX 2.0 /Firmware 4.3	4.48.4	NTSC / PAL	MPEG4 MJPEG	Yes	Yes	Yes	Yes	No
Arecont AV3115	Arecont	65218	NTSC / PAL	H.264	No	Yes	No	Yes	No
Arecont AV1355	Arecont	65151	NTSC / PAL	H.264	No	Yes	No	Yes	No
IQinVision IQ755	IQEye JPEG	V3.1/2	NTSC	MJPEG	No	No	No	Yes	Yes
IQinVision IQA35N	IQEye H264	V3.4/6	NTSC	H264 MJPEG	No	Yes	No	Yes	Yes
Panasonic NP-502S	Panasonic	1.81	NTSC/ PAL	H.264 MPEG-4 MJPEG	No	Yes	Yes	Yes	No

Table 18 Supported Generic IP Cameras (continued)

Panasonic SW458	Panasonic	1.42	NTSC/ PAL	H.264 MJPEG	No	Yes	Yes	Yes	No
Pelco IDS0DN-ADAU RX7	Pelco	1.8.2.20-201302 11-2.9110-03.92 40	NTSC	H264 MJPEG	No	Yes	No	Yes	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
Sony CH 240	Sony 2nd, 3rd, 4th and 5th generation Sony IP cameras	1.79.00	NTSC/ PAL	H.264 MPEG-4 MJPEG	Yes	Yes	Yes	Yes	No

Clipping Support By Application

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

Table 19 Video Clip Support

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

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

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 20 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 20 License Part Numbers

Part	Description
Physical Server Licenses (for Server Services)	
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)

Table 20 License Part Numbers (continued)

Part	Description
L-CPS-MS-SW7=	eDelivery license for 1 Media Server on a physical server (Cisco UCS or MSP)
Virtual Machine (VM) Licenses (for Server Services)	
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
Cisco VSM Federator Licenses	
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
Cisco SASD Licenses	
L-CPS-SASD-7=	eDelivery license for 1 SASD with Cisco VSM 7
Camera Licenses	
L-CPS-VSM7-1CAM=	eDelivery license for 1 camera connection with Cisco VSM 7
Camera App Licenses	
Note 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
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 Intuvision 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:

a. Determine the part number for the license you want to purchase (see Table 20).

b. Purchase the licence 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 Cisco 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.

See the Cisco Video Surveillance Operations Manager User Guide for more information.

Understanding the Cisco VSM Software Types

Table 21 describes the different types of software and firmware that are installed on servers, cameras, and encoders.

Table 21 Cisco VSM Software Types

Software Type	Description
System software	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. Use the Operations Manager to update the *System Software* on all servers (such as Media Servers) associated with the Operations Manager. See the Cisco Video Surveillance Operations Manager User Guide for instructions. **Notes:** • The Operations Manager and all associated servers must run the same system software version. • To update a Federator server, log in to the Federator server Management Console. See the Cisco Video Surveillance Operations Manager User Guide for instructions. • To repair or restore the Cisco VSM system software, see the Cisco Video Surveillance Manager Recovery Guide for your hardware platform. For VM installations, see the Cisco Video Surveillance Virtual Machine Deployment and Recovery Guide for UCS Platforms).
OVA image (for VM installations)	OVF template files are used to install the system software as a virtual machine (VM) on a supported Cisco Unified Computing System (UCS) platform. • OVA template files are downloaded from the Cisco website. • The file format is `.ova`. For example: `Cisco_VSM-7.2.0-331d_ucs-bc.ova` • See the Cisco Video Surveillance Virtual Machine Deployment and Recovery Guide for UCS Platforms for instructions to install the *`.ova`* image and perform the initial VM setup. • After the VM setup is complete, use the Management Console to complete the configuration.
USB Recovery Disk image	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: • 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. • 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. See the Cisco Video Surveillance Manager Recovery Guide (Cisco Connected Safety and Security UCS Platform Series) for more information.
Device *firmware*	Device *firmware* 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. See the "Upgrading Camera and Encoder Driver Firmware" section of the Cisco Video Surveillance Operations Manager User Guide for instructions to upgrade Cisco device firmware, or refer to the device documentation.

Table 21 Cisco VSM Software Types (continued)

Software Type	Description
Device *driver packs*	Device *driver packs* 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. • Install new driver packs to add support for additional devices. • Upgrade existing driver packs to enable support for new features. **Note** We strongly recommend upgrading driver packs using the Operations Manager interface (see the "Driver Pack Management" section of the Cisco Video Surveillance Operations Manager User Guide). 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.
Language Packs	Language packs can be added to display the Cisco VSM user interfaces in non-English languages. Language packs are added using the Operations Manager (release 7.6.0 and higher). See the Cisco Video Surveillance Operations Manager User Guide for instructions.

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.

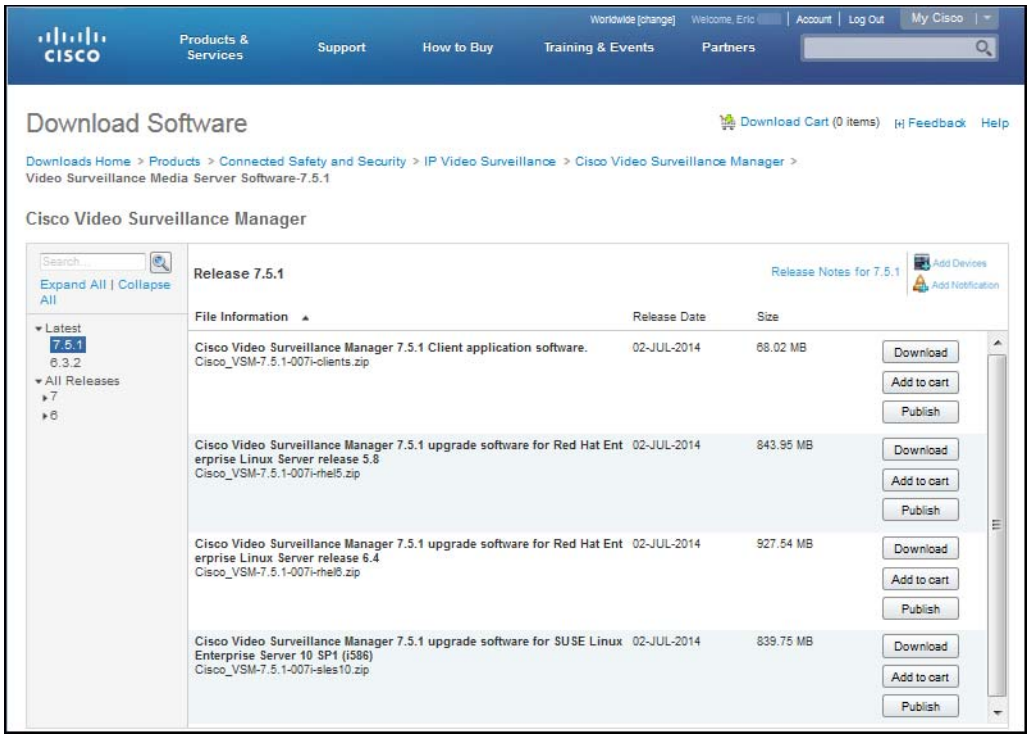
Step 3 Select a product category. For example:

- **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 1).

Step 5 Click **Download** or **Add to Cart** and follow the onscreen instructions.

Figure 1 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 1).

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 Toolkit

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

To access Bug Toolkit, you need the following items:

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

To use the Software Bug Toolkit, follow these steps:

Procedure

Step 1 To access the Bug Toolkit, 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 22 lists caveats that are open in this release.

Table 22 Open Caveats

ID	Description
CSCul34422	Dropping new event when lastSyncNotificationTime set to future date/time
CSCuq76277	Upgrade status not displayed when upgraded from 7.2.X and 7.5.X to 7.6
CSCur19117	Upgrade from 7.5.X -7.6 total number of steps incorrect in UpgradeStatus
CSCur34281	VSOM HA:Master VSOM status is partial after cisco restart
CSCur59418	CDAF: In Stream detail admin state is enabled even device got disable
CSCur63685	Recording Bootstarp failure trap is not received on failure
CSCur73118	During Upgrade, after Force Failover, both vsom_ha server are StandBy
CSCur73767	Scheduled backups failing when none are configured

Table 22 Open Caveats

ID	Description
CSCur75349	Entries of Soft deleted cams are duplicated when MS sync's with VSOM
CSCur75938	Backup of VSOM fails while upgrading from 722 to 7.6
CSCur77710	VSOMHA tab disappear from VSOM WEBUI server page
CSCur79678	Occasionally saving Adv.PTZ setting makes page look disabled; err in log
CSCur79743	Unable to remove DNS server entry from VSOM/CDAF
CSCur87353	Time out error seen when upgrading firware of multiple cameras
CSCur87914	Due to Synch err, cameras are not pulled into VSOM.
CSCur88257	No error message, when Custom Event/Soft Trigger is added in Maint. Mode
CSCur88317	config mismatch happens when setting ntp server mode to automatic
CSCur89208	After upgrade from 7.2.1 to 7.6, IQinVision camera goes critical
CSCur97480	Pacemaker alert not cleared after replaceHAconfig
CSCus06779	VSOM HA, after FO - cannot add MS or cameras due to license issue

Resolved Caveats

Resolved Caveats in Release 7.6.1

Table 23 Resolved Caveats in Release 7.6.1

Bug ID	Title
CSCuw65291	Max possible retention event recordings removed on camera replacement
CSCur71072	RHEL6 servers affected by POODLE ssl vulnerability
CSCuu04877	If one of Wall has disabled cam, no Unattended Walls can be configured
CSCuu67536	Vidoe not played on Motion video analysis state-1 window
CSCus94858	HW ID mismatch msg when IQeye,Axis cameras are discovered
CSCuu28987	ONVIF driver pack fails configuring multicast settings
CSCur89208	After upgrade from 7.2.1 to 7.6, IQinVision camera goes critical
CSCus96863	ONVIF: Core in camctrldriver in 7.6 fcs build
CSCut07779	umsdevice running high cpu usage in case of hwid mismatch
CSCuu06484	VSMS configuration lost due to VSM 7.6.0 upgrade error
CSCus63407	LTS backs up only one archive even if there are many LTS archives
CSCuu24690	Event queue limit reached, pruning events is not completing
CSCut65500	Cannot change server IP address when DNS server is unreachable
CSCut90019	VSOM allows configuring more than 32 video repositories

Table 23 Resolved Caveats in Release 7.6.1

Bug ID	Title
CSCuu29173	VSOM unable to sync with VSM server due to missing ManagementUid header
CSCur73776	Cannotadd or configure VSM server after static address error
CSCur79743	Unable to remove DNS server entry from VSOM/CDAF
CSCur95343	Displayed Version Mismatch in SWmgmt page for peer
CSCuu69220	Motion events are not received after 10 mins of connection loss for Axis
CSCuv40014	Add Cisco Camera to VSM deletes existing DNS entry in camera
CSCuu47480	Audio playback for mp4 clip ends abruptly
CSCuu58670	Multiple policies setup in VSOM - some of them are not working
CSCuu28957	Santiago time zone data out of date in 2015
CSCuu57376	VSM installation fails with error cannot open Packages database
CSCuv25350	3xxx/6xxx/6930- Audio may go out of sync relative to video
CSCuu03665	CIVS HW paltform should not be allowed to upgrade to 7.6 and later
CSCuw30239	Umsdevice crashes processing SOAP response
CSCuw49615	No video in VSM client using IQeye Camera
CSCuw49400	Critical camera after upgrade due to VSOM has new a password
CSCuu79807	VSOM enables disable camera
CSCus06601	Enable IP cams doesn't work after updateCamera API used to assign tmplte

Resolved Caveats in Release 7.6.0

Table 24 Resolved Caveats in Release 7.6.0

Bug ID	Title
CSCue84002	Medianet: failover MS entry is not push to the camera NVRAM
CSCul51057	DP: using view to load multiple device cause load on DPs to be imbalance
CSCum09030	Unable to download clip, thumbnail search in SASD without DNS entry
CSCum46855	After MS restarts, not all streams on multiplane Wall are back on time
CSCum49147	Sometimes create clip fails with Timeout waiting for server response err
CSCum50804	VSMS DB server fails to start due to incorrect file permissions
CSCum51257	DP streaming in pending while bulk in is in pgroess in VSOM
CSCum52648	SYNC:Unable to delete soft deleted cam after restore
CSCum53146	Clips not deleted after deleting the replaced camera after one day
CSCum63540	TCP checksum error

Table 24 Resolved Caveats in Release 7.6.0

CSCum71697	SWupgrade - takes a long time to upload swpack to server for end user
CSCum72098	FileUpload to MS failed - stream ended unexpectedly
CSCum83947	HTTP response error, when create MP4 clip from the VClip Details page
CSCum89109	Default Motion Detection Windows configuration in VSOM changes
CSCum89707	SOAP API works with HTTP in backward compatibility for v1.0
CSCum91630	Intermittent failure of mp4 clipping when start/end is in a gap
CSCum92017	Syntax Error adding Layer, when connected via VPN
CSCum96239	Media Servr-Unable to put device in disabled state;cannot enable fr VSOM
CSCum99355	when GIS is force deleted, unpublished image files in VSOM not deleted
CSCun06266	No MSI perfmon/mediatrace infocollected when MS has dual interfaces
CSCun08169	After backup/restore of VSOM, server is in backup config mismatch state
CSCun08886	SASD: Delete multiple clips - enumeration operator may not execute error
CSCun10001	Users are not notified when the Server is updated in VSF
CSCun11560	Clipping on RD, LTS, FO goes to primary server
CSCun12988	PFMD-Time disappears when crossing a day on Detailed range bar
CSCun14084	Mediaout core@H264ArchiveReader when used UDP streaming
CSCun14389	UCS-1U/RH6.4 - "rescue" mode does not work
CSCun16432	clipping estimated storage is not being computed for storage estimation
CSCun19173	CamStorage:Turning ON/OFF Storage recording doesnt issue applyconfig
CSCun19396	MS LoadAvg critical events are seen frequently in VSOM
CSCun19465	SASD: When VSOM is down, SASD Light does not work
CSCun19700	SASD:Can't login to SASD as LDAP user who requires approval-diff domains

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/

Cisco Video Surveillance Manager Documentation Website

www.cisco.com/go/physicalsecurity/vsm/docs

Release Notes for Cisco Video Surveillance Manager, Release 7.6.1