Release Notes for Cisco Video Surveillance Manager, Release 7.0.0

November 21, 2014

This document provides important information for Cisco Video Surveillance Manager (VSM).

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 this Release

VSM 7.0 is completely new and redesigned version of VSM that is highly scalable system that is easy to configure, manage, and use. This system enables your network and security teams to collaborate effectively in a scalable environment, combining both video and network techniques to optimize the experience. Enable your team with this secure, policy-based system to help ensure that they maximize their productivity across thousands of cameras.

Cisco VSM 7.0 includes the following components that combine to create a flexible, scalable system for the enterprise:

- Video Surveillance Operations Manager (VSOM)—Enables the efficient and effective configuration and management of video throughout an enterprise. VSOM provides a secure web portal to configure, manage, display, and control video in an IP network, and allows you to easily manage a large number of security assets and users, including media servers, cameras, encoders, and event sources. VSOM also provides an easy to use web portal for viewing live and recorded video.
- Video Surveillance Media Server (VSMS)—A core component of the VSM, VSMS provides a scalable platform for delivering live and recorded surveillance video. By using the power and advanced capabilities of IP networks, VSMS software allows applications, users, cameras, and storage to be added over time. As a result, the software provides unparalleled video surveillance system flexibility and scalability.
- Review Player—Supports off-line playback of video clips that are saved from VSM 7 in either standard .mp4 format for a single stream or Cisco .CVA format for multiple streams. Playback of secured clips also is supported.
- Safety and Security Desktop (SASD)—A powerful Windows thick-client application, SASD is designed with the needs of security professionals in mind. It provides multiple screens and tools for viewing video and alerts in the VSM system, including viewing video by location, hierarchical maps, and real-time alerts with sorting and filtering. SASD can also run in an *unattended mode* in which it is used to display video on a video wall under the command of the VSM system.

Notable new features of VSM 7 include the following:

- A highly scalable platform with up to 10,000 cameras in a single system, with even higher-scale options are available
- Simple and easy-to-use operator and administrative interfaces
- Enterprise-wide discovery through Medianet
- A comprehensive advance scheduling capability for recording policy
- Flexible user configuration with full integration into Lightweight Directory Access Protocol/Active Directory (LDAP/AD) to minimize administrative overhead
- Extensive health reporting, including inline status indications
- N + 1 redundancy on a camera-by-camera level
- Secure local, remote, and redundant video archive capabilities
- Standard video codecs ((Motion JPEG, MPEG-4, and H.264) simultaneously in a single VSMS
- Conservation of storage using events, clipping, record-on-motion, and loop-based archival options
- Flexible deployment options ranging from modules within the Cisco Integrated Services Routers, a dedicated 1- or 2-rack-unit (1RU or 2RU, respectively) server, Cisco Unified Computing System (Cisco UCS) C-Series Rack Servers, up to Cisco UCS B-Series Blade Servers

Getting Started

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

OVA Virtual Machine Images

VSM 7.0 is available in a virtual machine (VM) in two configurations for use with Cisco UCS B series, C series, and Express (SRE9xx modules) servers that are running VMware Hypervisor. These images are available for download as OVA files. See the VSM 7 deployment and recovery guides for USC B series, C series and Express servers for detailed information about installation and recovery of VSM 7 using the VM images on these platforms. (These documents are available at http://www.cisco.com/en/US/products/ps9152/prod_installation_guides_list.html.)

CPS-MSP-1RU-K9 and CPS-MSP-2RU-K9 Servers

VSM 7 is available pre-installed on the MSP-1RU and MSP-2RU servers. See *Cisco Video Surveillance Management Console Administration Guide* for more detailed information.

Recovery/Factory Image

A recovery image is available for download. This image is used to create a bootable USB flash drive that can be used for a recovery installation or a factory installation of VSM 7 on a CPS-MSP-1RU-K9 or CPS-MSP-2RU-K9 server that shipped with VSM 7 pre-installed. For more detailed information, see *Cisco Video Surveillance Manager 7.0 Recovery USB Flash Drive*.

Note Using the recovery image to upgrade from a previous version is not supported.

Released Versions

VSM 7.0 is released with Build 331. The component package versions are:

- AxClient—7.0.689
- SASD—7.0.108
- VSMC—7.0.0-122
- VSMS—7.0.0-331d
- VSOM—7.0.0-319

Migrating from VSM 6.3.2

You can migrate from VSM 6.3.2 to VSM 7.0. Because of the many new features and capabilities of VSM 7.0, an automatic upgrade from 6.3.2 is not possible. Migration from 6.3.2 to VSM 7.0 is supported through trained partners and Cisco Services. Contact your Cisco representative for additional information about the migration process and availability.

Important Notes

The following sections provides important information that applies to this VSM release:

Dual-Stream and Custom Configurations

This release provides validated High, Medium, and Low video quality settings for video supported devices. These settings have been tested and, unless otherwise noted, work in single stream mode and in all combinations in dual stream mode.

Custom settings allow customizing video settings for both single and stream and dual stream situations. The single stream custom settings are validated to allow only what a device supports. However, in dual-stream situations with custom settings, VSM 7 does not validate that the device supports a configured dual stream custom combination. The device may reject the configuration VSM may report an error to the user. In some cases, the device may accept the configuration but deliver poor quality video or video at a different frame rate or bit rate than what was requested. When using custom settings, make sure to verify that the video quality is acceptable after configuring the camera.

Deployment Considerations

The following notes apply to deployments of this VSM release:

- Cisco VSM 7 servers must be able to receive network traffic from other VSM servers, cameras and user workstations on the following network ports:

]

TCP ports	80, 443, 22, 161, 554, 2755, 9090, 61613, 61616
UDP ports	69, 123, 161, 5353, 16000-19999

- Time synchronization is enforced between all VSM system components.

  To provide accurate video recording, event notifications, and security, all system components of VSM must be synchronized to the same time. Cisco recommends that NTP be used to synchronize time between servers, cameras, and clients. Windows 7 time settings can be configured to point to

VSOM as an NTP source, and each VSMS can be configured with VSOM as an NTP source through the VSM Management Console or through VSOM. Finally, VSOM should be configured with the NTP source to synchronize the entire system with the correct time.

- Multiple DNS servers are not supported.

  VSM 7 allows configuring more than one DNS server in the Cisco VSM Management Console. However, VSM 7 does not preserve the order in which they are used, which can result in a Configuration Mismatch error in VSOM in some cases. If this situation occurs, perform the Repair Configuration procedure to clear the error. To avoid this situation, configure only one DNS server for VSM 7 deployments.

- Using DHCP is required for using Medianet camera discovery in VSM 7. DHCP also offers a convenient way to assign IP addresses to many cameras at once.

  When using DHCP, it is important to configure the DHCP server properly. DHCP servers support assigning addresses to devices in these ways:

  - Dynamic assignment—An IP address is assigned temporarily for the duration of a *lease time*. At the end of this time, the address expires and a new address is assigned.
  - Automatic assignment—A camera is assigned a permanent IP address that is based on its MAC address.
  - Static assignment—A system administrator must assign IP addresses based on MAC addresses of devices and enter the IP addresses into the DHCP server.

  With dynamic assignment, an IP address can change when the lease expires. In general, this event causes a short loss in video while the IP address changes and streaming resumes. However, in some cases, such as if the IP address changes during certain administrative operations or during a failover, VSM is not informed of the address change and loses connectivity with the camera until the camera is reset. To avoid this situation, Cisco recommends that the DHCP server be configured with automatic assignment. If dynamic assignment must be used, Cisco recommends that a long lease time be configured.

- When using dual graphics cards, Cisco recommends that both cards be the same model. See the Cisco Video Surveillance Monitoring Workstation Performance Baseline Specification for information about workstation performance and graphics cards.

  When using dual-graphics cards, disable Windows Desktop Composition on the client workstation to avoid a reduction in video performance. (Make this setting in the Windows 7 Control Panel by choosing **Advanced System Settings**, clicking the **Settings** button under Performance, and unchecking the **Enable Desktop Composition** checkbox in the Performance Options window.)

VSOM, VSMS, and Cisco VSM Management Console Considerations

The following notes apply to deployments of this VSM release VSOM, VSMS, and Cisco VSM Management Console:

- Device firmware upgrades not recommended during upgrades of software or driver packs

  VSOM provides support for firmware upgrades for some supported devices. VSM 7 does not block system administration functions in Cisco VSM Management Console while VSOM is performing firmware upgrades. However, you should not perform Cisco VSM Management Console system administration tasks that might disrupt the connection to the devices being upgraded while the upgrade is in progress. For example, using Cisco VSM Management Console to upgrade software on a VSMS that is connected to a device or upgrading the driver for the device while VSOM is upgrading the device firmware upgrade is not recommended.

If you perform a system administration task during an upgrade and the upgrade does not completed properly, VSOM detects an error and displays information in the Jobs status information for the upgrade. In this case, the firmware upgrade process must be repeated.

- Re discovery of a Medianet camera can take up to 10 minutes after a camera is deleted.

  Medianet cameras are discovered by VSM automatically and added to the system in approximately 30 seconds. After the camera is provisioned in the system, VSOM administration features should be used if it is necessary to make changes to the VSMS to which the camera is assigned or to change camera configuration settings. Avoid deleting a camera from the system to allow it to be rediscovered so that it can be reconfigured because it can take up to 10 minutes for the camera to be rediscovered (or longer if the if the camera is rebooted).

- The VSOM Health Dashboard does not report a RAID failure on a dedicated VSOM server

  If VSOM is installed on a dedicated server (without a coresident VSMS), there is no support in the VSOM health dashboard to report a RAID failure on that server. In this case, use the Cisco VSM Management Console to monitor the health of the server. If VSOM is coresident with VSMS, the VSOM health dashboard shows the health status of the RAID system and other server health information.

- Filenames for VSOM and VSMS backup files should not contain Russian characters.

  VSM 7 supports internationalization and localization for Russian. However, filenames for files that are to be saved on the VSM 7 Linux servers cannot use Russian characters. For example, do not user Russian characters for VSOM or VSMS configuration backup file names. If Russian characters cause filenames to be corrupted, which makes the files unusable.

- In some cases camera video analytics configuration errors are not reported.

  VSM 7 supports video analytics for devices. During normal analytics configuration operations on these devices, configuration errors that occur are reported correctly to the user. However, in some less common situations such, as loss of connection to a camera or rebooting a camera, it that the video analytics may become misconfigured without an error reported to the user. If analytics events stop arriving from a camera with video analytics, use the Repair Configuration function to fix the problem. See defect number CSCuc26875 for related information.

Video Client Considerations

The following notes apply to video clients in this VSM release:

- Clipping is not supported across failover and failback boundaries.

  By design, VSM 7 does not support creating a video clip, (in either .CVA or .MP4 format) that crosses a failover or failback boundary. See defect number CSCuc32294 for related information.

- An error may not be reported if a video clip fails to complete as requested

  In some cases when an .MP4 clip is requested, the clip may fail to generate but no error is reported. This situation can occur if there is not enough storage on the VSMS to temporarily store the clip after it is created and before it is downloaded to the client workstation.

- Smooth playback is not supported across changes in media type in a video recording

  VSM 7 allows reconfiguring a camera, including changing the media type, while recording is active. For example, the media type can be changed from MJPEG to H.264 if the camera supports it. This action results in recorded video with changes in the media type. In this situation, playback is not smooth across the changes. In some cases, such as normal forward play, the transition may appear

relatively smooth. In other cases, such as reverse play and stepping, or when audio is used, the transition can have noticeable issues. In some cases, audio may not be available for as long as 15 seconds.

- In some cases, Cisco Review Player may not display the first pane in a .CVA clip.

  When **File > Open** in Cisco Review Player or dragging a .CVA clip to a running Cisco Review Player application, the first pane of video may not display. This situation does not occur when double-clicking the .CVA clip or dragging it to the Cisco Review Player icon. See defect number CSCuc34862 for related information.

- Issues with synchronized playback of multiple video panes.

  In some cases in which there are gaps in the video or changes on the media type, synchronized playback of multiple video panes in the video client can get out of sync.

- Reverse playback of video from 10 Mpixel cameras requires additional memory.

  Reverse playback of video streams, particularly of 10 Mpixel video streams, requires additional resources on a client workstation. During reverse video playback of 10 Mpixel video, memory use on the client workstation is heaviest. If the resources of the client workstation are overloaded, reverse playback does not run at the proper speed and is not smooth. For best performance of reverse playback of 10 Mpixel video streams, Cisco recommends that SASD be used because it runs in 64 bit mode. In addition, Cisco recommends that the client workstation have 16GB of DRAM.

SASD Considerations

The following notes apply when using SASD in this VSM release:

- SASD requires the Windows 7 64-bit operating system.
- The .NET Framework 4.0 must be installed on a client workstation before the SASD client software is installed on that system.

  A standalone .NET Framework 4 installer is available from the Microsoft website. If .NET 4.0 is not installed, the following message appears during installation of the SASD client software:

  Microsoft .NET Framework 4.0 Full Package is Required.

- SASD does not enforce the performance limit of 48 panes of video on a single workstation.

  During normal SASD operations, SASD enforces a limit of 48 panes of video. However, during Unattended Mode operation, there is no limit enforced on the number of panes. If more than 48 panes are displayed, SASD performance can be poor and, in unusual cases, can crash. See defect number CSCub06627 for related information.

- Reenabled cameras do not reappear automatically.

  If a camera is disabled and then reenabled, it does not automatically reappear in SASD. To workaround this situation, refresh the camera list by clicking on a different location and then clicking on the location in which the camera is located.

- In some cases, updates to alerts do not appear immediately in the alerts page that is being viewed.

  When an alert scrolls beyond the first page of the Alerts in the Alert Centric View, new events that update it do not appear on the first page. To see these alerts, refresh the alert list on the first page by going to different alert tab and back to the first page.

- Subregions on maps do not appear unless their parent map location is displayed in the location tree.

  In the Map Centric View, subregions on a map are displayed only if their parent location is visible in the location hierarchy list. See defect number CSCuc34667 for related information.

- Map Editor zoom level and reset-button behavior is inconsistent.

  Clicking the **Reset** button in the map editor can have inconsistent results. If the map is not properly scaled or zoomed after clicking the **Reset** button, click it again and the map should be properly scaled.

Supported Devices

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

Supported Devices: Cisco

Table 1 provides information about Cisco devices that this VSM release supports.

Table 1 Cisco Supported Devices

Model	Supported Firmware Version	Video Format	Media Types	Audio	Dual Stream	Motion Detection	Firmware Upgrade	Medianet
2400 Series cameras	2.5.0-9	NTSC PAL	MPEG-4 MJPEG	—	Yes	Yes	Yes	No
2500 Series cameras	2.5.0-9	NTSC PAL	MPEG-4 MJPEG	Yes	Yes	Yes	Yes	No
2600 Series cameras	4.4.0-13	NTSC PAL	H.264 MPEG-4 MJPEG	Yes	Yes	Yes	Yes	Yes
4300 camera	2.4.0-271	NTSC PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes
4500 camera	2.4.0-271	NTSC PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes
4300E camera	3.2.1-200	NTSC PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes
4500E camera	3.2.1-200	NTSC PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes
2900 Series cameras	1.6.18	NTSC PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	No

Table 1 Cisco Supported Devices (continued)

Model	Supported Firmware Version	Video Format	Media Types	Audio	Dual Stream	Motion Detection	Firmware Upgrade	Medianet
5000 Series cameras	1.6.17	NTSC	H.264 MJPEG	—	Yes	Yes	Yes	No
CIVS-SENC-4P encoder	V1.1.0-1	NTSC PAL	H.264 MPEG-4 MJPEG	Yes	Yes	Yes	Yes	No
CIVS-SENC-8P encoder	V1.1.0-1	NTSC PAL	H.264 MPEG-4 MJPEG	Yes	—	Yes	Yes	No

Notes

- Cisco 4500 and 4500E cameras support video analytics.
- All Cisco devices support failover.
- All Cisco devices support redundancy, with some exceptions for the 2400, 2500, 2900, and 5000 Series cameras. The 2400, 2500, 2900, and 5000 series cameras do not support sending events such motion detection and contact closures to the redundant server.
- Cisco 5000 Series cameras do not support motion detection at video bit-rates that are greater than 4,000 Kbps (4 Mbps).
- Some custom dual-stream settings for Cisco 5000 and 2900 Series cameras may not operate properly when after changing the configuration of these settings. To workaround this issue, first configure the primary stream with the desired settings and then apply the configuration for the primary streams once time. See defect number CSCuc12346 for related information.
- The Cisco 5000 and 2900 series cameras do not allow changes to authentication settings (username and password) or networking settings (DHCP, static IP address, DNS, and so on) through VSM. These values must be configured by using web interface of a camera.

Supported Devices: Arecont

Table 2 provides information about Arecont devices that this VSM release supports.

Table 2 Arecont Supported Devices

Model	Type	Supported Firmware Version	Media Types	Dual Stream	Motion Detection	Firmware Upgrade
AV5155	5MP IP camera	65202	H.264 MJPEG	Yes	Yes	No
AV10XX5	10MP IP camera	65202	H.264 MJPEG	Yes	Yes	No
AV2115	2MP IP camera	65202	H.264 MJPEG	Yes	Yes	No

Table 2 Arecont Supported Devices (continued)

Model	Type	Supported Firmware Version	Media Types	Dual Stream	Motion Detection	Firmware Upgrade
AV5115	5MP IP camera	65202	H.264 MJPEG	Yes	Yes	No
AV20185DN	4 sensor 5MP panoramic camera	65170	H.264 MJPEG	Yes	Yes	No
AV8185	4 sensor 2MP panoramic IP camera	65043	H.264 MJPEG	Yes	Yes	No

Notes

- AV20185DN and AV8185 models are 4-channel IP cameras. To support multiple video channels from a single device, VSM 7 models these devices as Encoders. There are no validated H, M, or L template settings for these devices in the VSIN templates. Custom settings must be used instead to configure streaming settings.
- Arecont devices have not been qualified to support redundancy with this VSM release.
- VSM 7 allows H quality to be selected for both streams in dual-stream configurations for some Arecont devices. However, this configuration is not supported by the cameras and may result in poor video quality.
- The using the L quality setting for both streams in a dual stream configuration may result in poor video quality.

Supported Devices: Axis

Table 3 provides information about Axis devices that this VSM release supports.

Table 3 Axis Supported Devices

Model	Type	Supported Firmware 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
243QBlade	Encoder	4.46	NTSC PAL	MPEG-4 MJPEG	—	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

Table 3 Axis Supported Devices (continued)

Model	Type	Supported Firmware Version	Video Format	Media Types	Audio	Dual Stream	Stream Mirroring	Motion Detection	Firmware Upgrade
Q7406	Encoder	5.11.1	NTSC PAL	H.264 MJPEG	—	Yes	Yes	Yes	Yes
247S	Encoder	4.42	NTSC PAL	MPEG-4 MJEG	Yes	Yes	Yes	Yes	Yes
P3301	IP camera	5.40.92	NTSC	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes

Note

Axis devices have not been qualified to support redundancy with this VSM release.

Supported Devices: IQinVision

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

Table 4 IQinVision Supported Devices

Model	Type	Supported FW Version	Media Types	Dual Stream	Motion Detection	Firmware Upgrade
IQ032SI-V11	1080p IP camera	V3.3/8	H.264	No	Yes	No
IQM32NE-B 5	1080p IP camera	V3.3/9	H.264	No	Yes	No

Notes

- There are no validated H, M, or L template settings for IQinVision devices in the VSOM templates. Custom settings must be used instead to configure streaming settings.
- IQinVision devices have not been qualified to support redundancy with this VSM release.

Supported Devices: Panasonic

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

Table 5 Panasonic Supported Devices

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

Table 5 Panasonic Supported Devices (continued)

Model	Type	Supported Firmware Version	Video Formats	Media Types	Audio	Dual Stream	Motion Detection	Firmware Upgrade
NP 304	IP camera	1.64E0_1.06	NTSC	MPEG-4 MJPEG	No	No	Yes	No
NF 302	IP camera	1.64E0_1.06	NTSC	MPEG-4 MJPEG	No	No	Yes	No

Note

Panasonic devices have not been qualified to support redundancy with this VSM release.

Supported Devices: Sony

Table 6 provides information about Sony devices that this Panasonic release supports.

Table 6 Sony Supported Devices

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

Notes

- Sony devices have not been qualified to support redundancy with this VSM release
- Sony devices do not support motion detection with the H.264 media type

Supported Devices: Generic Drivers for Axis and ONVIF IP Cameras

VSM 7.0 provides two *generic* device drivers for supporting ONVIF 2.0 and Axis VAPIX Version 3 compatible devices. These generic drivers are for use with IP cameras only. The functionality that they support depends on the device that they are used with. These drivers are intended to provide a quick and easy way to support devices for which VSM does not currently have a dedicated driver available. Because 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.

Table 7 described the generic device driver support for Axis and ONVIF cameras.

Table 7 Generic Device Driver Supper for Axis and ONVIF Cameras

Type	Supported Version	Video Formats	Media Types	Audio	Dual Stream	PTZ	Motion Detection	Firmware Upgrade
Axis	Version 3	NTSC PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	No
ONVIF	2.0	NTSC PAL	H.264 MPEG-4 MJPEG	Yes	Yes	Yes	No	No

Supported Devices: Analog Cameras

This VSM release provides support for several of analog cameras.

Table 8 describes the support for analog cameras.

Table 8 Analog Camera Support

Type	Video Formats	Serial Protocol Support
Generic	NTSC PAL	No
Bosch	NTSC PAL	No
Panasonic	NTSC PAL	No
Generic Pelco-D	NTSC PAL	Pelco-D
Pelco Min-Spectra	NTSC PAL	Pelco-D

Obtaining and Installing Licenses

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

Table 9 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 9 License Part Numbers

Part	Description
FL-CPS-MS-SW7	License for one VSMS on an MSP
FL-CPS-OM-SW7	License for one VSOM on an MSP
L-CPS-MS-SW7=	eDelivery License for one VSMS on MSP
L-CPS-OM-SW7=	eDelivery License for one SASD on an MSP
L-CPS-SASD-7=	eDelivery License for 1 SASD with VSM 7

Table 9 License Part Numbers (continued)

Part	Description
L-CPS-VSM7-1CAM=	eDelivery License for 1 camera connection with VSM 7
L-CPS-VSMS7-B-VM=	eDelivery License for one VSMS on a UCS B Series
L-CPS-VSMS7-C-VM=	eDelivery License for one VSMS on a UCS C Series
L-CPS-VSOM7-B-VM=	eDelivery License for one VSOM on a UCS B Series
L-CPS-VSOM7-C-VM=	eDelivery License for one VSOM on a UCS C Series

Procedure

Step 1 Purchase additional licenses:

a. Determine the part number for the license you want to purchase (see Table 9).

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 VSOM.

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.

Tip The additional capacity is available immediately. You do not need to restart the server or take additional steps.

Supported Firmware for Cisco Network Cameras and Encoders

The following table describes the minimum firmware versions for Cisco cameras and encoders in this release of Cisco VSM.

Table 10 Cisco Camera and Encoder Firmware Required for Release 7.0

Model Number	Required Version for Release 7.0	Medianet
2421/25xx	2.5.0-9	Not supported
26xx	4.4.0-13	Supported
2900 series	1.6.18	Not supported
4300/4500	2.4.0-271	Supported
4300E/4500E	3.2.1-200	Supported
5000 series	1.6.17	Not supported
CIVS-SENC-4P/8P	1.0.0-10	Not supported

Understanding the VSM Software Types

Table 11 VSM Software Types

Software Type	Description
Cisco camera device firmware	Device firmware is provided by the device manufacturer. The firmware for Cisco devices can be upgraded using VSOM. Firmware for other manufacturers is upgraded using a direct connection. See Cisco Video Surveillance Operations Manager User Guide for instructions to upgrade Cisco device firmware, or refer to the device documentation.
Device driver packs	Device driver packs are the software packages used by VSMS and VSOM to inter-operate with video devices. Driver packs are included with the VSM software, or may be added to a server at a later time to add support for new devices. • Use the Cisco VSM Management Console to update *driver packs*, as described in the **Manage Drivers** section of Cisco Video Surveillance Management Console Administration Guide. • Go to **Operations** > **Management Console** to launch the browser-based interface. See your system administrator for login information. • Driver pack versions must be the same on the servers that host the VSMS and VSOM or a driver pack mismatch error occurs. Templates cannot be revised when a driver pack mismatch error is present.
System (server) software	System software denotes the VSM software, including Media Server, Operations Manager, Cisco VSM Management Console, Safety and Security Desktop and Multipane clients. The Operations Manager and all associated Media Servers must run the same software version. Use the Cisco VSM Management Console to update System Software, as described in the **Server Upgrade** section of Cisco Video Surveillance Management Console Administration Guide.

Table 11 VSM Software Types (continued)

Software Type	Description
Language Packs	Language packs can be added to display the VSM user interfaces in non-English languages. Language packs are added using the **Server Upgrade** page of the Cisco VSM Management Console. You must upgrade the language packs on all servers in your deployment. See the **Server Upgrade** section of Cisco Video Surveillance Management Console Administration Guide for more information.
USB Recovery Disk image	Use the USB Recovery Disk image to create a Cisco VSM 7.0 Recovery Flash Drive (for example, on a USB stick). The recovery disk can be used to restore (reinstall) the server Operating System files and partitions without erasing video files stored on the server, or restore the Cisco VSM server to the original factory state (which deletes all data, configurations, software and video files from the appliance).

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 access software downloads using the Cisco Video Surveillance home page or the Cisco software navigator for *IP Video Surveillance software*.

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 http://tools.cisco.com/Support/BugToolKit/.

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 bug ID** field, then click **Go**.

Step 4 To look for information if you do not know the bug ID number:

a. Choose **Security** from the Select Product Category menu.

b. Choose the desired product from the Select Product menu.

c. Choose the version number from the Software Version menu.

d. Under Advanced Options, choose **Use default settings** or **Use custom settings**. The default settings search for severity 1, 2, and 3 bugs, open and fixed bugs, and only bugs containing bug details. Use the custom settings to change the severity and status parameters, or to search for keywords within the bug headline and description.

Open Caveats

Table 12 lists caveats that are open in this release.

Table 12 Open Caveats

ID	Description
CSCtr84305	To get audio after changing its setting, user has to reload the stream
CSCtt47533	After camera goes offline, transitioning to recording needs right-click
CSCtz54223	Need to change color of Acknowledged/Closed Alerts
CSCtz60444	MS should not allow firmware upgrade and server upgrade at the same time
CSCtz67269	Firmware upgrade and driver pack upgrade should not be allowed to run concurrently
CSCub00814	Analog camera added on unreachable encoder should be preprovisioned
CSCub06627	Crash when total number of panes from multiple processes exceeds 48
CSCub61805	Map Editor—Clicking reset zooms map image

Table 12 Open Caveats

ID	Description
CSCub70689	Bulk soft deleting 101 cameras, 6 cameras failed
CSCub73269	8 codes jump in playing reverse while trickplay
CSCub81632	Reenabled cameras do not appear immediately in camera list
CSCub85939	Intermittent "'invalid symbol '\x01' detected in XML stream" error
CSCub87961	VSOM does not require Cisco restart when camera control lockout changed
CSCub88854	Contact closure event not listed immediately in SASD alert space
CSCub89072	Critical alerts do not autoshow in alerts when device goes offline
CSCub90123	HA/DR: Clicking on the failover gap when in live stream mode will fail
CSCub91153	VSOM RAID failure not reported in VSOM health dashboard
CSCuc14172	ActiveMQ session does not renew immediately with FO server after network address change
CSCuc17282	Cannot restore VSOM backup when filename has RUS characters
CSCuc17336	VSOM config backup does not contain time zone information
CSCuc23160	Medianet camera not removed from MS cache
CSCuc24662	VSOM failed to sync MD config to FO server via Sync after primary fallback
CSCuc24690	Firmware upgrade with wrong image fails and devices must be reenabled
CSCuc25504	Multiple DNS servers are not fully supported
CSCuc26875	No configuration failure notification when failed to configure analytics on 4500E
CSCuc30084	Not getting recording_backup_failed alert
CSCuc32294	HADR: MP4/CVA Clips create fails when start position is in failover gap
CSCuc34667	Map subregions not displayed until location tree opened to level
CSCuc34862	Cisco Review Player (32/64) CVA clip does not display video on first pane
CSCuc35612	Issue in restore only MS after camera replacement
CSCuc37050	DHCP camera will not stream after MS goes down and up with IP change

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