Release Notes for Cisco Video Surveillance Manager Release 6.3

This document provides important information for the following Cisco Video Surveillance Manager (VSM) products:

- Cisco Video Surveillance Media Server
- Cisco Video Surveillance Operations Manager
- Cisco Video Surveillance Virtual Matrix

Contents

This document includes the following sections:

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

Introduction

The Cisco Video Surveillance Manager consists of the following products:

- Cisco Video Surveillance Media Server—The core component of the Cisco Video Surveillance Software Suite, the Media Server enables the collection and routing of video from a wide range of cameras; event-tagging, record-on-motion, and recording of video for review and archive; secure local, remote, and redundant video archive capabilities; and bandwidth management for both live distribution and historical recording.

- Cisco Video Surveillance Operations Manager—Allows organizations to quickly and effectively configure and manage video throughout the enterprise. Provides a secure web portal to configure, manage, display, and control video throughout an IP network, and the ability to manage a large number of security assets and users, including Media Server instances, cameras, encoders, DVRs, and event sources, and digital monitors powered by Virtual Matrix.

- Cisco Video Surveillance Virtual Matrix—Enables flexible delivery of live and recorded video to command centers and provides high-availability access to network video for continuous monitoring applications. Virtual Matrix capabilities include aggregation and display of video from the Media Server platform on almost any number of digital monitors distributed across the IP network. Authorized users and integrated applications control the video that is displayed on any number of digital monitors.

VSM Security Best Practices

Securing Cisco Video Surveillance Manager 4.1/6.1: Best Practices and Recommendations provides best practices and recommendations for helping to ensure the security of VSOM, VSMS, video devices, and client PCs in a Cisco VSM environment. This document also applies to VSM 6.3. To access this document, go to the following URL, click the **Products** link, then click the **Cisco Network-Centric Video Surveillance products** link:

http://www.cisco.com/go/physicalsecurity

New and Changed Information

New features in Cisco VSM 6.3 include the following:

System Health Monitoring

The Health Dashboard provides a summary of the overall operational health of your video surveillance system from within the Cisco Video Surveillance Operations Manager. VSOM processes and stores health event messages and presents pertinent information on the Health Dashboard page for items including, but not limited to:

- Media streams (camera feeds)
- Recordings
- Viewing client health
- Camera status
- And much more

Forensic Video Thumbnail Search

The Forensic Video Thumbnail Search feature allows you to create a series of thumbnail snapshots from a video archive that helps you quickly navigate to a specific event in the archive. You can create a series of thumbnails for the entire archive or for a specific time range within the archive. You can also zoom out to create a series of thumbnails for a larger time range or zoom in to create a series of thumbnails for a smaller time range, which allows you to rapidly drill down to a specific event.

After you have located an event, you can play the video in the Operator window, or save the video clip to a local drive through simple right-click menu options.

User Interface Enhancements

User Interface enhancements for VSM 6.3 includes the following:

- Improved motion detection configuration
- Quality slider that supports variable bit rates for Cisco SD/HD cameras

Software and Cisco IP Camera Firmware Updates from the Management Console

This release introduces a command-line-free method of performing the following updates from the Management Console:

- Media Server software updates using a local path or FTP
- Cisco SD/HD camera firmware update in management console

Support for New Devices

VSM 6.3 now supports Cisco 5000 Series IP HD 5" Dome Cameras.

Notable Areas of Improvement

This section includes the following topics:

- VSOM and VSMS Consistency on Archives, page 4
- Event Processing Improvements, page 4

VSOM and VSMS Consistency on Archives

Before VSM 6.3, there were a number of situations where the archives displayed in VSOM would not be consistent with the running and shelved archives in VSMS. In these cases, archives in VSMS would not be displayed in VSOM or archives displayed in VSOM would not exist in VSMS. VSM 6.3 contains improvements to keep information on archives consistent between VSOM and VSMS. Here are some of the cases that these improvements resolve:

- If connections to cameras were lost for extended periods due to problems with the camera, network or DNS problems, running archives for these cameras would become shelved on VSMS while still being shown as running in VSOM. (Resolved caveats CSCtf36555 and CSCtg53116)
- Editing archive configuration settings in Batch Administration in some cases could result in multiple archives being displayed in VSOM that corresponded to a single archive in VSMS. (Resolved caveat CSCtf99865)
- Under certain conditions, starting an archive would fail in VSOM, yet the archive would successfully start in VSMS. The archive would not be displayed in VSOM, but would be running n VSMS. (Resolved caveat CSCtf01454)

Event Processing Improvements

VSM 6.3 contains significant improvements in the number and rate of events that the system can process and display. This improvement in system performance allows for higher reliability when processing large numbers of motion based recordings and/or large numbers of simultaneous viewing client connections.

Important Notes

The following important notes apply to VSM 6.3:

- Camera Firmware Upgrade Considerations
- Software Installation Considerations
- Synchronizing the Linux Server System Time to the Hardware Clock, page 5
- Health Dashboard Bandwidth Monitoring
- Using Multiple Monitors
- Using Video Playback Synchronization

- Using Encoders Cards
- Trick Play Buttons
- Displaying New Video Resolutions in Virtual Matrix
- Using VSM when VMR is Disabled

Camera Firmware Upgrade Considerations

VSM 6.3 supports new firmware versions for the Cisco 2400 series and 2500 series SD cameras, and the Cisco 4300 series and 4500 series HD cameras. The new camera firmware versions contain new features and improvements that are supported by VSM 6.3, including improvements to Motion Detection. Please see the release notes for these new firmware versions for details.

- For Cisco 2400 series and 2500 series SD cameras, the new firmware version is: 2.1.5
- For the Cisco 4300 series and 4500 series cameras, the new firmware version is: 1.1.0

We strongly recommended that, after upgrading to VSM 6.3, the firmware on existing camera models be upgraded to the new versions. These new camera firmware versions are required for any new cameras added to the system, and in the event that any configuration changes, are required for existing cameras.

VSM 6.3 contains a new feature for Camera Firmware Upgrade that simplifies and automates this process.

Software Installation Considerations

VSM 6.3 now includes a Java Runtime Environment (JRE) in the release package. This is new for VSM 6.3 and changes how the software is installed compared to previous VSM releases.

⚠️

Caution   It is extremely important that the VSM 6.3 software installation and upgrade instructions in the *Installing and Upgrading Cisco Video Surveillance Manager (VSM) Release 6.3* document is followed to ensure proper removal of any previous JRE components and proper installation of the new JRE. If the installation and upgrade instructions are not performed correctly, new features in VSM 6.3, such as the Health Monitoring Dashboard and Forensic Video Thumbnail Search, will not work properly.

The *Installing and Upgrading Cisco Video Surveillance Manager (VSM) Release 6.3* document can be obtained from the following URL:
http://www.cisco.com/en/US/docs/security/physical_security/video_surveillance/network/vsm/6_3/install_upgrade/vsm_install_upgrade.html

Synchronizing the Linux Server System Time to the Hardware Clock

A Linux server includes a hardware clock and the system time. For proper system operation, these items should be kept synchronized. Linux maintains clock synchronization as follows:

- On system boot up, system time is initialized from the hardware clock
- On normal system shutdown, the hardware clock is updated from the system time

Cisco recommends that you immediately set the hardware clock to the system time in either of the following situations:

- You manually change the system time
- NTP becomes functional for the server

To manually set the hardware clock to the current system time, enter this command:

shell> **hwclock --systohc**

In addition, you might find the following Linux commands to be useful:

- To display the Linux system time, enter this command:

  shell > **date**

- To display the hardware clock time, enter this command:

  shell > **hwclock**

Health Dashboard Bandwidth Monitoring

The Health Dashboard can only report the NIC Health for the Eth0 port because bandwidth monitoring is supported only on the Eth0 port. Bandwidth monitoring is not supported for other ports.

Using Multiple Monitors

When using multiple monitors with a client workstation to display video, the client workstation must be set up to display the monitors in an extended desktop mode. Other configurations for multiple monitors are not supported.

Using Video Playback Synchronization

Synchronization has been updated and optimized for playback performance. Two or more video archives may be selected and synchronized. Individual video archives can be added or removed from the synchronization. Synchronization supports fast forward playback and seeking across gaps in the video streams. Other advanced playback functions (step forward, step reverse, and fast reverse) are not supported.

Using Encoders Cards

A multiservices platform with encoder cards and the Video Surveillance Encoder Servers do not support camera feeds from other devices, such as IP cameras and standalone encoders.

Trick Play Buttons

Trick play buttons are disabled when any selected video pane or panes display archives that include a MPEG-2 or H.263 media type.

Displaying New Video Resolutions in Virtual Matrix

If you are upgrading VSM and want to display video images with the new 1600 x1050 and 1600 x1200 resolutions, you must merge the hydra_state file manually.

Using VSM when VMR is Disabled

When Video Mixing Renderer (VMR) is not supported by a PC and is disabled, be aware of the following affect on the VSM system:

- Motion configuration—Displays video window without motion configuration rectangles
- Digital zoom—Not available
- Hue, saturation, luminosity, contrast—Not available
- Alpha blending of VMR toolbar—Not available
- .CVA files—Review Player displays a message that .CVA is not supported on a machine without VMR and does not load the file
- High-definition video does not render
- Overall client performance is degraded
- Trick play with multiple panes consumes a significant amount of CPU and memory resources

Note You can disable VMR on a PC that does not support it by running the Cisco Video Surveillance Workstation Profile Tool.

Using the Workstation Profiling Tool

You can use the Cisco Video Surveillance Workstation Profile Tool 6.2.1 to validate the performance of your client workstation for use with VSM 6.3.

Note For client workstations running Windows XP Service Pack 3 (SP3), the Cisco Video Surveillance Workstation Profile Tool may erroneously identify SP3 as an issue. However, VSM 6.3 supports client workstations running Windows XP SP3, so the SP3 issue identified by the Cisco Video Surveillance Workstation Profile Tool can be ignored.

Obtaining a Driver Pack

VSM may require a driver pack update to work with certain cameras. To obtain documentation and important information about Cisco VSM and system requirements, go to the following URL, click the **Products** link, then click the **Cisco Network-Centric Video Surveillance products** link. See the Download Software section for information about obtaining driver packs.

http://www.cisco.com/go/physicalsecurity

Using Cisco VSM with the Cisco Video Surveillance Standard Definition IP Camera

You can use a Cisco Video Surveillance standard definition IP camera model with this version of VSM, but be aware that the IP camera includes features that are not currently integrated with VSM.

The following sections provide information about using VSM with these standard definition IP camera models:

Standard Definition IP Camera Features that VSM Does Not Support

Table 1 provides information about the compatibility of Cisco standard definition IP cameras running firmware release 2.1.5 and VSM 6.3.

Note The VSM driver that this release includes is compatible only with Cisco IP camera firmware 2.1.2 or later. It is highly recommended that SD camera firmware level 2.1.5 or later be used with this VSM release. You must upgrade standard definition cameras to a supported version.

Table 1   Standard Definition IP Camera Features Compatibility for Firmware Release 2.1.5 and VSM 6.3

Feature	Standard Definition IP Camera Implementation	Compatibility with Firmware Release 2.1.5
Alarm events outputs	2 out / FTP clip / e-mail.	Not supported.
Alarm inputs	2 in.	Fully supported.
Audio	Simplex / half duplex / full duplex.	Not supported.
Cisco Discovery Protocol (CDP)	Sends CDP discovery messages.	Not supported.
Event scheduling	You can schedule event notification from the IP camera web interface.	Not configurable by using VSM. If configured by using the IP camera, the schedule applies to notifications sent to VSM.
Event notification	E-mail, FTP, HTTP, or API alerts if an event occurs.	Includes the VSM event notification API only.
IP Filter	Allows controlling access to the IP camera by IP address.	Not configurable by using VSM.
Motion detection	Detects motion in up to 4 configured areas in the video field with individual region support.	Motion detection is supported for primary MPEG-4 streams with region support. As a result, a single motion JPEG stream does not support motion detection.

Table 1   Standard Definition IP Camera Features Compatibility for Firmware Release 2.1.5 and VSM 6.3 (continued)

Feature	Standard Definition IP Camera Implementation	Compatibility with Firmware Release 2.1.5
PTZ (RS-485)	Enables pan, tilt, zoom (PTZ) functions.	PTZ Preset support only.
QoS	Quality of Service (QoS) for audio streams, video streams, or both.	Not configurable by using VSM. If configured by using the IP camera, QoS marking affects only streams between the IP camera and the Media Server.
SNMP	Provides options for configuring SNMP settings.	Not configurable by using VSM.
Multicast	Streaming UDP multicast.	Supported.

Guidelines for Using a Standard Definition IP Camera with VSM

The following guidelines apply when you use a standard definition IP camera with VSM:

- The IP camera must be installed and configured as described in *Cisco Video Surveillance IP Camera User Guide* for the standard definition IP camera.

- You must create a separate user account with administrator privileges for each Media Server. Configuration connections for a Media Server are limited just as they are for user sessions. Viewing and managing video streams from VSM requires administrator-level privileges.

Troubleshooting a Standard Definition IP Camera when used with VSM

If you experience difficulty when using a standard definition IP camera with VSM, refer to these troubleshooting guidelines:

- If you are using the Cisco Video Surveillance Operations Manager, it may take a few attempts to bring up video the first time that a standard definition IP camera is selected

- Verify that VSM is installed properly

- Verify no firewalls are conflicting on VSM servers

- Verify that the default gateway is configured for the standard definition IP camera

- Verify that your web browser supports ActiveX controls

- Verify that the user name and password are configured identically for the camera and the VSOM standard definition IP camera settings

- Verify that the appropriate graphics card is installed in the system on which you are displaying video

- Verify that VSM configures the camera using the default port address of 80

- Verify the camera is configured to use HTTPS for API access

- Verify that the VSMS can reach the camera over the network

Using Cisco VSM with the Cisco Video Surveillance 4300 Series and 4500 Series High Definition IP Cameras

You can use a Cisco Video Surveillance 4300 series and 4500 series high definition IP cameras with VSM 6.3, but be aware that the high definition camera includes features that are not currently integrated with VSM.

✎
Note The VSM driver that this release includes is compatible only with Cisco IP camera firmware 1.0.3 or later. It is highly recommended that HD camera firmware level 1.1.0 be used with this VSM release.

The following sections provide information about using VSM with these 4300 series and 4500 series high definition IP cameras:

- 4300 Series and 4500 Series High Definition IP Camera Features that VSM Does Not Support
- Guidelines for Using a 4300 Series and 4500 Series High Definition IP Camera with VSM
- Troubleshooting a 4300 Series and 4500 Series high definition IP Camera when used with VSM

4300 Series and 4500 Series High Definition IP Camera Features that VSM Does Not Support

Table 2 lists the 4300 series and 4500 series high definition IP camera features that are not compatible with VSM.

Table 2   4300 Series and 4500 Series High Definition IP Camera Features not Currently Compatible with VSM

Feature	Implementation Notes
720p at 60 fps	VSM supports up to 30 fps for 720p resolution.
Audio	Simplex / half duplex / full duplex.
Cisco Discovery Protocol (CDP)	Sends CDP discovery messages.
Constant Bit Rate (CBR), Variable Bit Rate (VBR), and VBR with a Cap	The high definition IP supports CBR or VBR (constant quality), and VBR with ceiling (bandwidth management by reducing frame rate rather than quality). VSM supports CBR and VBR.
Digital event outputs	Two outputs, logic level programmable in the high definition IP camera.
Event scheduling	You can schedule event notification from the high definition IP camera web interface.
IP Filter	Allows controlling access to the IP camera by IP address. Can be modified through the IP camera web interface but not through VSM.
QoS	Quality of Service (QoS) for audio streams, video streams, or both.
SNMP	Provides options for configuring SNMP settings

*Table 2   4300 Series and 4500 Series High Definition IP Camera Features not Currently
Compatible with VSM (continued)*

Feature	Implementation Notes
Unicast/multicast (TCP/UDP)	VSM supports UDP unicast and multicast, but not TCP unicast.
USB memory card	Optional onboard memory USB 4GB (CIVS-IPC-USB-4G).

Guidelines for Using a 4300 Series and 4500 Series High Definition IP Camera with VSM

The following guidelines apply when you use a 4300 series and 4500 series high definition IP camera with VSM:

- The high definition IP camera must be installed and configured as described in *Cisco Video Surveillance IP Camera User Guide* for the high definition IP camera.

- You must to create a separate user account with administrator privileges for each Media Server. Configuration connections for a Media Server are limited just as they are for user sessions. Viewing and managing video streams from VSM requires administrator-level privileges.

Troubleshooting a 4300 Series and 4500 Series high definition IP Camera when used with VSM

If you experience difficulty when using a 4300 series and 4500 series high definition IP camera with VSM, refer to these troubleshooting guidelines:

- Verify that VSM is installed properly

- Verify no firewalls are conflicting on VSM servers

- Verify that the default gateway is configured for the high definition IP camera

- Verify that your web browser supports ActiveX controls

- Verify that the user name and password are configured identically for the camera and the VSOM high definition IP camera settings

- Verify that the appropriate graphics card is installed in the system on which you are displaying video

- Verify that VSM configures the high definition IP camera using the default port address of 80

- Verify the camera is configured to use HTTPS for API access

- Verify that the VSMS can reach the camera over the network

Using Cisco VSM with the Cisco Video Surveillance 5000 Series High Definition IP Cameras

You can use a Cisco Video Surveillance 5000 series high definition IP cameras with VSM 6.3, but be aware that the high definition cameras include features that are not currently integrated with VSM.

> **Note** The VSM driver that this release includes is compatible only with Cisco IP camera firmware 1.5.9 or later.

The following sections provide information about using VSM with these 5000 series high definition IP cameras:

- 5000 Series High Definition IP Camera Features that VSM Does Not Support
- Guidelines for Using a 5000 Series High Definition IP Camera with VSM
- Troubleshooting a 5000 Series High Definition IP Camera When Used with VSM

5000 Series High Definition IP Camera Features that VSM Does Not Support

Table 2 lists the 5000 series high definition IP camera features that are not compatible with VSM.

Table 3   5000 Series High Definition IP Camera Features not Currently Compatible with VSM

Feature	Implementation Notes
Audio	Simplex / half duplex / full duplex.
Event scheduling	You can schedule event notification from the high definition IP camera web interface.
QoS	Quality of Service (QoS) for audio streams, video streams, or both.
Unicast/multicast (TCP/UDP)	VSM does not support multicast.

Guidelines for Using a 5000 Series High Definition IP Camera with VSM

The following guidelines apply when you use a 5000 series high definition IP camera with VSM:

- The high definition IP camera must be installed and configured as described in *Cisco Video Surveillance IP Camera User Guide* for the high definition IP camera.
- You must to create a separate user account with administrator privileges for each Media Server. Configuration connections for a Media Server are limited just as they are for user sessions. Viewing and managing video streams from VSM requires administrator-level privileges.

Troubleshooting a 5000 Series High Definition IP Camera When Used with VSM

If you experience difficulty when using a 5000 series high definition IP camera with VSM, refer to these troubleshooting guidelines:

- Verify that VSM is installed properly
- Verify no firewalls are conflicting on VSM servers
- Verify that the default gateway is configured for the high definition IP camera
- Verify that your web browser supports ActiveX controls
- Verify that the user name and password are configured identically for the camera and the VSOM high definition IP camera settings

- Verify that the appropriate graphics card is installed in the system on which you are displaying video
- Verify that VSM configures the high definition IP camera using the default port address of 80
- Verify the camera is configured to use HTTPS for API access
- Verify that the VSMS can reach the camera over the network

Orderability Matrix

Table 4 shows the orderability matrix for versions of SuSE Linux Enterprise Server (SLES) and various Cisco Video Surveillance hardware platforms and Cisco VSM releases.

Table 4   SLES and Cisco Video Surveillance Hardware/Software Orderability Matrix

Hardware	Cisco VSM Release	SLES Version
Multiservices Platform for Video Surveillance	3.1.1/5.1.1	SLES 10, SP 1
	4.0/6.0	
	4.1.1/6.1.1	
	4.2/6.2	
	4.2.1/6.2.1	
	6.3	
Multiservices Platform for Physical Security	6.3 only	SLES 10, SP 1
Legacy Cisco Video Surveillance servers	3.1.1/5.1.1[1]	SLES 9, SP 3
Legacy Cisco Video Surveillance international servers (CIVS-MSA1R-250)	3.1.1/5.1.1	SLES 9, SP 3
	4.0/6.0	SLES 10, SP 1
	4.1.1/6.1.1	
	4.2/6.2	

1.   You can upgrade to Cisco VSM 6.3 on legacy Cisco Video Surveillance servers.

Known Issues when using VSM 6.3 with a Cisco Video Surveillance IP Camera

Table 5 describes known issues when using VSM 6.3 with a Cisco Video Surveillance IP Camera.

Table 5   Known Issues when Using VSM 6.3 with a Cisco IP Camera

Known Issues	Customer Affect	Notes
Known issues when using VSM 6.3 with an SD IP Camera		
Stuttering video is seen in JPEG and MPEG-4 live proxies.	Live playback is not smooth.	More prevalent with VMD configured.
The camera interface must be closed for VSM to function.	VSM cannot configure proxies on a camera while a user is viewing video.	—

Table 5   *Known Issues when Using VSM 6.3 with a Cisco IP Camera (continued)*

Known Issues	Customer Affect	Notes
Using motion detection on dual streams causes issues. Motion detection must be set up on only the primary stream.	Configuring motion detection on the dual streams of a single camera causes motion detection notifications to behave unexpectedly.	Motion events detected on the primary stream may be used for both archives.
Known issues when using VSM 6.3 with a 4300 Series and 4500 Series HD IP Camera		
Performance tests show a latency of 1,000 milliseconds.	A latency of at least 1 second under best network conditions. This issue is most noticeable when using pan-tilt mounts.	Seen with 1080p H.264 streams up to 30 fps.
High definition streams can take from 6 to 13 seconds to render.	For HD IP camera streams, many operations take 6 to 13 seconds (variable GoP affects timing), including seeking, switching play directions, start up, and resume after pausing.	You may also experience the same start up issues that occur with the SD camera. To work around this issue, select a feed a second time. To work around this issue, delete and then reconfigure the camera in VSOM.
Using motion detection on dual streams causes issues. Motion detection must be set up on only the primary stream.	Configuring motion detection on the dual streams of a single camera causes motion detection notifications to behave unexpectedly.	Motion events detected on the primary stream may be used for both archives.
Known issues when using VSM 6.3 with a 5000 Series HD IP Camera		
Enabling motion detection limits the maximum bitrate to 4.6Mb/s.	Cannot use bitrates higher than 4.6Mb/s when motion detection is enabled.	—
Known issues when using VSM 6.3 with an All Cameras		
Standalone clips in .AVI and .WMV formats play back at incorrect speeds.	Occurs because these clip container formats use only a single frame rate. When frame rates of a clip segment change or do not match what is expected, these clips play too slow or too fast.	Limitations of container format. Use .CVA format instead.

Caveats

This section includes the following topics:

Using the Software Bug Toolkit

You can use the Bug Toolkit to find information about the 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 6 lists caveats that are open in this release.

Table 6   *Open Caveats*

ID	Description
CSCtf31214	Status of the scheduled archive is incorrect when repos is full
CSCtf32328	VSMS stops sending SNMP traps to VSOM if DNS is down after power outage
CSCtf60876	VSM 6.3.0-10 and HD 4500 1.0.8.3 PTZ latency is greater than one second
CSCtg07152	Thumbnails for live/forensic tool are incorrect for interlaced streams
CSCtg14939	Health Dashboard not show critical events for device in down/up state
CSCtg19117	Refreshing IE after uploading file, stops the upgrade process
CSCtg28075	ServerUpgrade: When disk is full, no error message is displayed
CSCtg28175	vsom show no error when archive fail to be added due to not enough space
CSCtg38567	Thumbnails not generated for some Sony devices
CSCtg43479	Upgrade: Incorrect msg in VSMC when there is power outage during upgrade
CSCtg53688	Scroll bar does not move to the beginning of the archive
CSCtg58667	Unable to generate thumbnails for vsm 6.2.1 archives for some devices
CSCtg58671	Unable to generate thumbnails for 6.2.1 archives: Stream Manager encoder

Table 6   Open Caveats (continued)

ID	Description
CSCtg59077	Child proxy should not send connectionloss trap when ciscoservice stops
CSCtg95379	Multipane cva save clip is unsuccessful if one archive has no data
CSCth12257	VSOM should not report "archive added successfully" when it fails
CSCth12454	seek - reverse play - fast forward for an hour or more, pauses the video
CSCth13972	Axis devices do not implement motion detection persisience
CSCth25439	Persistence value for motion windows not obeyed (IQEye)
CSCth27300	Cisco 5000: MD window sensitivity settings is same for all the windows
CSCth32988	No archive event generated when scheduled archives fail to start
CSCth33129	Request to document VSMS support of eth0 for bandwidth monitoring to wk
CSCth34738	Cannot set any HD motion window at cif resolution
CSCth34998	Batch Admin Resets Motion Config When Proxy Params Changed
CSCth39179	IE8 crashes when playing with DVR buttons (play, pause)
CSCth39290	Seek To Beginning did not happen at all. Video Freezes
CSCth39482	Cannot get motion events at any setting under 60 with Cisco AVG
CSCth40750	Motion window is active upto stop event in Panasonic and Sony devices
CSCth43727	VSM allows creation of mixed type archives (with more than one encoding)
CSCth46655	No alarm generated when Cisco 5000 device with JPEG config disconnected.
CSCth48939	Error is displayed after swap, even though archive data is available
CSCth53268	No Proxy Failure to HDB when proxy not steaming due DNS failure
CSCth56230	VSMS server failed to send PTZ Stop command after mouse moved off video
CSCth61279	Upgrading VSOM without doing Cisco daemon stop and start will not initiate new tomcat session and many features in VSOM will not work as needed.
CSCth66695	Delay in archive creation
CSCth75456	HD-VSM 6.3 will not stream if camera firmware is 1.0.7 and quality > 80
CSCth83853	Cisco 5000 JPEG proxy requires click twice to play when suspended
CSCth83853	Cisco 5000 JPEG proxy requires click twice to play when suspended
CSCth89305	VSMC console passwd not preserved during upgrade from 4.2/6.2 to 6.3
CSCth91083	Event History gets truncated when upgrading to 6.3
CSCth91648	Cisco 5000:Varying Brightness, saturation with a JPEG stream (cloudy Video)
CSCth91963	VSVM/VSOM Crashes when more than one DVR mode enabled
CSCth91968	HD Camera sets secondary frame rate to 1fps for 1.0.7 firmware
CSCth96291	Clock sync Health warning event not cleared from dashboard when expired
CSCth98622	Describe behavior when a camera is in fixed and rotating list of a view
CSCth99050	Play Reverse doesn't work for Stream Manager H264 archives

Resolved Caveats

Table 7 lists caveats that are open in this release.

Table 7   Resolved Caveats

ID	Description
CSCsz68563	Admin Overview page take very long to load with many servers
CSCtc20837	VSOM operator's view hits a performance bottle neck
CSCtd72971	Event history rights are recorded for each event history entry
CSCtd94791	IQEye 2M feeds do not display on ATI 4850 graphics interface
CSCte07790	RTSP streams from same VSMS not working
CSCte25970	Upgrade doc is incorrect for MySql upgrade steps
CSCte32881	Need defensive code to handle simultaneous, identical clip requests
CSCte46953	Cannot view H.264 video through camera interface with VS Client installed
CSCte66906	No archives started after power loss
CSCte69511	Media_master files corrupted after archive is stopped
CSCte87966	Renamed archives have wrong dates in new name
CSCte91155	Rights not set when archive is renamed through Batch Admin
CSCtf01454	'Malformed Response' err is displayed and arch is in VSMS & not in VSOM
CSCtf12417	Archive expiration set incorrectly
CSCtf19177	Batch administration 60s timeout hampers editing large number of assets
CSCtf23454	15 seconds when loading many shelved archive video
CSCtf27967	Remove mmconf_properties query before archive playback
CSCtf36555	Archiver XML file removed when proxy unavailable
CSCtf36839	Load on server builds up when we get 4 or 5 motion events per min
CSCtf49010	New Icons for Health Monitoring
CSCtf69838	Artifacts occur during stepping and slow speed playback
CSCtf76264	DST changes cause seek to fail in archive between 02:00-03:00
CSCtf76840	VSVM template needed for 1920x1080 resolution on Clients
CSCtf79338	Creating VSOM backup for download consumes disk space
CSCtf79361	Purge event operation fails if an event is marked to be hidden
CSCtf79383	Issue with archive expiration time when using Batch Admin
CSCtf82942	Hardware clock is not synchronized with system clock on SuSE Linux
CSCtf94355	Cannot create device trigger events with Cisco 252x and 253x
CSCtf94703	Archives are groomed for oversubscription even though storage is available
CSCtf99865	More than one archives in VSOM point to one archive in VSMS
CSCtg14025	Need proper shutdown restart procedures documented
CSCtg20370	Out-of-synch PTZ source and PTZ feed preview
CSCtg25542	Administrator Role unable to manage all archives
CSCtg38505	sess_ files fill up /tmp directory
CSCtg39229	Cannot delete camera due to event activity

Table 7   ***Resolved Caveats (continued)***

ID	Description
CSCtg43926	Grooming starts while xvcrman shuts down and stops archives
CSCtg54990	Event URL should always use IP, never hostname
CSCtg67090	When motion event > 70, MSP 2RU run into high CPU.
CSCtg79624	references to the trusted_ip file should be removed from the docs
CSCtg86311	Illegal Characters in VSOM Camera Names Causes IE Errors
CSCtg90779	notifyurl is being generated from the address typed into the browser
CSCtg95116	Event History logging required with some motion recording
CSCth11619	High CPU usage on the VSOM server when multiple operators logon to VSOM
CSCth14764	Archive start time inconsistent in archive table % runn/shelve archive
CSCth36268	Archives on VMSS Cannot be Stopped or Removed
CSCth43765	Archive 2x2 rotating view lost after a full screen toggled?

Obtaining Documentation, Software, and Related Information

To obtain documentation and important information about Cisco VSM and about system requirements, go to the following URL, click the **Products** link, then click the **Cisco Network-Centric Video Surveillance products** link:

http://www.cisco.com/go/physicalsecurity

To access the self-service portal and obtain software, documents, and tools, log in to the Cisco Support Center at http://www.cisco.com/support/. You must be a registered user of Cisco.com to access this page. You must have a current Cisco support contract that is linked to your Cisco.com account to download software and obtain help from the Cisco Technical Assistance Center.