Release Notes for Cisco Video Surveillance Manager 4.2.1/6.2.1

January, 2010

These release notes provide important information for the following Cisco Video Surveillance Manager (VSM) products:

- Cisco Video Surveillance Media Server Release 6.2.1
- Cisco Video Surveillance Operations Manager Release 4.2.1
- Cisco Video Surveillance Virtual Matrix Release 6.2.1

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.

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.

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 4.2.1/6.2.1. 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

The following sections provide an overview of the new features in this release and in release 4.2/6.2.

What's New in 4.2.1/6.2.1

New features in Cisco VSM 4.2.1/6.2.1 include the following:

- Support added for Windows XP Service Pack 3 (32 bit) using Internet Explorer release 7 only
- Improved trick play functionality across motion JPEG, MPEG-4, and H.264
- Enhanced 1080p trick play
- Updated synchronization playback operation
- Added motion detection to the driver for the Panasonic NF-284
- Extended integration with LDAP
- Cisco standard definition IP camera VSM driver updates support only firmware versions 2.1.0 and later
- Updated video client error messages in VSOM and VSVM
- Review Player EX supported in Windows Vista
- Updated layout resolutions for VSVM (1600 x1050 and 1600 x1200)
- The video client uses the VMR flag that the Profiler Tool sets to identify whether VMR is supported

What's New in 4.2/6.2

New features in Cisco VSM 4.2/6.2 include the following:

- Video startup performance—Reduces the playback start-up time for multiple video streams by starting all streams in parallel.
- Pelco D driver updates—Support added for PTZ Patterns and On-screen Programming (OSP).
- Cisco high definition IP camera driver updates—HTTPS has been implemented for commands that are sent to configure Cisco Video Surveillance IP camera high definition models.
- Cisco standard definition IP camera driver updates—Supports existing firmware versions and the new firmware version that includes the Cisco Media API. The new firmware version enables motion detection, event triggers, and other features.
- Seeking—Seeking within archives has been improved.
- Driver pack consolidation—This release consolidates the driver packs for the following devices:
  - Cisco IP camera high definition models
  - Cisco IP camera standard definition models
  - Optelecom C-44 4-port encoder
  - Pelco Spectra IV IP PTZ dome camera
  - ICX serial driver
  - AXIS Q7406 6-port encoder blade
  - Sony SNC-DF85 network mini-dome camera

Important Notes

Licensing

Beginning with Cisco VSM 4.2/6.2, you no longer need to obtain license keys to install, upgrade, or operate VSM. Previous releases required license keys that are tied to hardware MAC addresses.

Setting Login Page as Default Web Page

Because license keys no longer determine the home page for a VSM host, you now set the VSOM 4.2.1 Log In page as the default web page as part of the VSOM 4.2.1 installation or upgrade process.

Upgrading

Beginning with Cisco VSM 4.0/6.0, VSM includes a new data format and a new Storage Manager that controls the data repository and available storage. The 4.0/6.0 upgrade process requires that you delete stored video data, but it maintains Cisco VSM configuration information.

Before you upgrade, make sure to back up any stored video data that you want to keep.

Detailed upgrade instructions are available with your upgrade package. You can also obtain an advanced service to assist with the upgrade and data retention. For more information, contact your Cisco sales representative or partner.

Using Multiple Monitors

When using multiple monitors with a client workstation to display video, the client workstation must be set up so that you can see the task bar across the multiple monitors. Other configurations for multiple monitors are not supported.

Using 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 Encoder Cards

To improve efficiency in the use of system resources, the Multi Services 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

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
- VMR control panel—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

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, page 5
- Guidelines for Using the Standard Definition IP Camera with VSM, page 6
- Troubleshooting the Standard Definition IP Camera when used with VSM, page 7

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 2.1.2 and VSM 4.2.1/6.2.1.

Note The VSM driver that this release includes is compatible only with Cisco IP camera firmware 2.1.2 or later. You must upgrade standard definition cameras to a supported version.

Table 1 Standard Definition IP Camera Features Compatibility for Firmware Release 2.1.2 and VSM 4.2.1/6.2.1

Feature	Standard Definition IP Camera Implementation	Compatibility with Firmware Release 2.1.0
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, 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 3 configured areas in the video field.	Motion detection is supported for primary MPEG-4 streams only. As a result, a single motion JPEG stream does not support motion detection.
PTZ (RS-485)	Enables pan, tilt, zoom (PTZ) functions.	Not supported.
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.	Not supported.

Guidelines for Using the Standard Definition IP Camera with VSM

The following guidelines apply when you use the 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.
- A user with administrator privileges cannot be logged in to the standard definition IP camera and use VSM at the same time.

Troubleshooting the Standard Definition IP Camera when used with VSM

If you experience difficulty when using the 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 High Definition IP Camera

You can use a Cisco Video Surveillance high definition IP camera model with VSM 4.2.1/6.2.1, but be aware that the high definition camera includes features that are not currently integrated with VSM. In addition:

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

- High Definition IP Camera Features that VSM Does Not Support
- Guidelines for Using the High Definition IP Camera with VSM
- Troubleshooting the high definition IP Camera when used with VSM

High Definition IP Camera Features that VSM Does Not Support

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

Table 2 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.

Table 2 High Definition IP Camera Features not Currently Compatible with VSM (continued)

Feature	Implementation Notes
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 only.
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
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 the High Definition IP Camera with VSM

The following guidelines apply when you use the 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.
- A user with administrator privileges cannot be logged in to the high definition IP camera and use VSM at the same time.

Troubleshooting the high definition IP Camera when used with VSM

If you experience difficulty when using the 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 3 shows the orderability matrix for versions of SuSE Linux Enterprise Server (SLES) and various Cisco Video Surveillance hardware platforms and Cisco VSM releases.

Table 3 SLES and Cisco Video Surveillance Hardware/Software Orderability Matrix

Hardware	Cisco VSM Release	SLES Version
Multiservices Platform	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	
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	
	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 4.2/6.2 on legacy Cisco Video Surveillance servers.

Known Issues when using VSM 4.2.1/6.2.1 with a Cisco Video Surveillance IP Camera

Table 4 describes known issues when using VSM 4.2.1/6.2.1 with a Cisco Video Surveillance IP Camera.

Table 4 Known Issues when Using VSM 4.2.1/6.2.1 with a Cisco IP Camera

Known Issues	Customer Affect	Notes
Known issues when using VSM 4.2.1/6.2.1 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.
Clips in .AVI and .WMV format do not play properly.	Occurs due to limitations of the VSM API and 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 at incorrect speeds.	Limitations of container format. Use .CVA format instead.

Table 4 Known Issues when Using VSM 4.2.1/6.2.1 with a Cisco IP Camera (continued)

Known Issues	Customer Affect	Notes
The camera interface must be closed for VSM to function.	VSM cannot configure proxies on a camera while a user is viewing video.	—
Known issues when using VSM 4.2.1/6.2.1 with an 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.
Standalone clips in .AVI and .WMV formats play back at incorrect speeds.	Playback of .AVI and .WMV clips is too slow or too fast.	Limitations of container format. Use .CVA format instead.
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 one of the dual streams.	Configuring two motion detection windows for a single camera causes motion detection notifications to behave unexpectedly.	Motion events may be used for both archives.

Caveats

This section lists significant caveats (bugs) that are resolved or open in this release.

In addition, 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.

Resolved Caveats

Table 5 lists caveats that are resolved in this release.

Table 5 Resolved Caveats

ID	Description
CSCsq42019	Page not found when motion event is submitted without entering values
CSCsu05798	Cannot create server clip with long name—no feedback in UI
CSCsy15827	HD—Ghost image is seen in live and archive and mediaout missing frames
CSCsz36557	Disk usage graph is a white box with VSMS server without repository
CSCta59991	Client - Sync is not completely in sync
CSCtb08685	Upgrade 4.1/6.1 to 4.2/6.2 /dev/disk/by-id does not mount
CSCtb43034	Cannot change video feed after PTZ is activated
CSCtb95949	Shelved archives do not play from start after playing once
CSCtc10280	Multiple archive start commands result in bad archive
CSCtc13321	User session is frequently terminated in Internet Explorer 7
CSCtc13594	3.x to 4.x upgrade miss MS version; VSOM does not use new AxClient API
CSCtc18344	VSMC, VSOM LDAP configuration to allow input of delimiter
CSCtc20586	Title bar is not shown for the “connection failed” feeds
CSCtc20825	Sony DF70 PTZ is not supported
CSCtc23485	Sony RX550-H264-V camera feed not streaming with firmware 3.10, 3.04, 3.0
CSCtc25633	Synchronize does not work properly on feeds with mix media types
CSCtc29527	VSMS runs out of memory and cannot start all archives and Apache
CSCtc31799	PTZ operation reverse on selected Sony models
CSCtc34020	VSVM management by VSOM
CSCtc47809	Hydra_state file becomes corrupt on the VSVM server
CSCtc47822	VSOM—Issue with “motion detection” archive created via Batch Admin
CSCtc47830	Batch Admin—Feed media type and VSMS proxy out-of-synch
CSCtc59378	Proper error message should be displayed while swapping
CSCtc65366	Switching away from PTZ camera with tour stops tour
CSCtc69050	Disable reverse play and step forward/back in sync mode
CSCtc71633	Batch Admin—Add proxy name prefix when creating looping archives

Open Caveats

Table 6 lists caveats that are open in this release.

Table 6 Known Caveats

ID	Description
CSCsz90559	Changing from static IP to DHCP with discovery tool fails
CSCtb17225	Excessive motion detection failure errors with Sony driver pack
CSCtc83105	VSM server firewall configuration prevents discovery
CSCtc87452	SNMP monitoring always set to off in VSMC pages
CSCtc88693	Trailing spaces are not stripped in Batch Admin
CSCtd17155	Warning message is needed when synch used with archives from different servers
CSCtd20058	Synch is not applied to all panes when one of the panes is an invalid archive
CSCtd21806	Reverse play jumps timestamp and scroll bar to 10–15 seconds for H.264
CSCtd21955	Clicking reverse play continuously 5–6 times on H.264 BWM clip stops video
CSCtd27190	After reverse play in H.264-V archive, playback pauses for 1–3 seconds
CSCtd31732	When performing a synchronized seek, some feeds appear to not synch
CSCtd32724	Client connections to system under upgrade generate core files on server
CSCtd34692	When archives are in synch, exiting a loop fails
CSCtd34758	VSVM hydra_state file pane4 overlap with pane8 at 1x3x4 layout at 1600x1
CSCtd34766	Reverse play of 4x4 (H.264 4CIF archive) causes the browser to crash
CSCtd50804	Some MPEG-4 archives affect system stability
CSCtd56982	Rotated views not display at 2x3x6, 4x4, and 1x3x4 layouts
CSCtd67365	The combination of play, reverse, and seek to the beginning does not work
CSCtd68162	DVR Play and Reverse buttons not working after pressing several times
CSCtd77542	Seek to beginning does not work after one archive reaches end
CSCtd77587	Seek does not work in some archives when using Seek button
CSCtd82748	PTZ Configuration page does not list all cameras correctly
CSCtd83377	Video sometimes pauses and plays when archives played faster
CSCtd86421	403 Forbidden error displayed on user account sync for non-root user
CSCtd89922	Usage of Extended desktop option for multiple monitor setup—Axclient
CSCtd90259	Play control button does not display the correct status
CSCtd90670	1280 x 960 resolution is missing 1x2, 2-1, 2-4, 3x3, 4x3 layouts
CSCtd91080	Browser crash due to memory fragmentation when 4x3 layout played in reverse
CSCtd91176	SLES9/RH4—Server load increases when archives played fast forward or reverse
CSCtd92596	Seeking does not work when archive goes to pause state for longer than 15 minutes
CSCtd93532	Stop button does not bring the view back to unsynch mode
CSCtd94428	When Internet Explorer memory usage approaches 2 GB, the system becomes unstable

Table 6 Known Caveats (continued)

ID	Description
CSCtd95227	Initial synch does not work if the master pane is an invalid archive
CSCtd95231	Synch does not work if one of the archive is MPEG-2
CSCtd95242	Switching into synch mode after reverse play leaves one pane in reverse