



Release Notes for Cisco Video Surveillance Manager 4.1/6.1

February, 2009

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

- Cisco Video Surveillance Media Server Release 6.1.
- Cisco Video Surveillance Operations Manager Release 4.1
- Cisco Video Surveillance Virtual Matrix Release 6.1

Contents

This document includes the following sections:

- [Introduction, page 2](#)
- [Obtaining Documentation, Software, and Related Information, page 2](#)
- [VSM Security Best Practices, page 2](#)
- [New and Changed Information, page 3](#)
 - [Cisco Video Surveillance Media Server 6.1 New and Changed Information, page 3](#)
 - [Cisco Video Surveillance Operations Manager 4.1 New and Changed Information, page 4](#)
 - [Cisco Video Surveillance Virtual Matrix 6.1 New and Changed Information, page 5](#)
- [Important Upgrade Notes, page 5](#)
- [Supported Devices Correction, page 5](#)
- [Using Cisco VSM with the Cisco Video Surveillance Standard Definition IP Camera, page 5](#)
- [Orderability Matrix, page 7](#)
- [Caveats, page 7](#)



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

© 2009 Cisco Systems, Inc. All rights reserved.

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

The following new document available with this release: *Securing Cisco Video Surveillance Manager 4.1/6.1: Best Practices and Recommendations*. This document provides best practices and recommendations for helping to ensure the security of VSOM, VSMS, video devices, and client PCs in a Cisco VSM 4.1/6.1 environment. 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 describe new and changed information in this release:

- [Cisco Video Surveillance Media Server 6.1 New and Changed Information, page 3](#)
- [Cisco Video Surveillance Operations Manager 4.1 New and Changed Information, page 4](#)
- [Cisco Video Surveillance Virtual Matrix 6.1 New and Changed Information, page 5](#)

Cisco Video Surveillance Media Server 6.1 New and Changed Information

Enhancements and changes in Cisco Video Surveillance Media Server 6.1 include the following:

- Dual streaming support for MPEG-4 and H.264—Dual MPEG-4 and H.264 streams are now supported from a single encoder port. Separate proxies are created for each feed.
- Cisco Video Surveillance Encoder features—Variable bit rate and video loss are now supported features for the Cisco Video Surveillance Encoder (source type is exacq). SNMP traps are sent when the encoder detects loss of analog video input.
- Restrict API access—It is now possible to restrict administration API access to a single administrative IP address.
- Support for Stream Manager H.264 events and serial pass-through—The Stream Manager encoder now supports all H.264 resolutions and serial-pass-through of PTZ and camera control commands. The encoder also can receive and process events. Support is included for the new x-code value `h264.ciscosm_x`.
- Improved motion configuration—The AXClient supports the detection of motion from different segments (windows) of a single feed. During motion configuration setup, a VSOM user provides specific names for each of these segments/windows, although the segment/window name is not displayed in the Motion Configuration panel.
- Multiple stream export and support in ReView Player—VSOM now supports multi-stream exports from the Operator page. When you choose this option, the system prompts for the export start and end time (default values are the earliest start time and the latest end time). VSOM then creates the export CVA file. The resulting video clip contains a multi-pane window player with all playable video clips and can be viewed in the ReView player.
- Sony PAL for Generation 3 cameras—Support is now provided for the Sony PAL Generation 3 camera models CS50, DF50, DF80, RZ50, RX530, RX550, and RX570.
- Clipping from Pelco DVRs—It is now possible to create server-side and client-side clips from the Pelco Endura DVR by using the standard VSMS interfaces.
- New H.264 device codec support—This release adds support for IQEye.
- AXClient installer enhancement—A more efficient installer is now provided for the AXClient.

Important Notes about Changes Carried forward from Cisco Video Surveillance Media Server 6.0

- New archive format and Storage Manager—The minimum looping archive duration is 1 hour, which can be increased in 1-hour increments. When you upgrade to Media Server 6.0, you must reclaim the disk space that is used by the existing archives. For additional information, see the [“Important Upgrade Notes” section on page 5](#).

- Change in suspended proxy behavior—To enable fast MPEG-4 start up times and reliable event communication, direct proxies do not suspend for devices from these vendors: Cisco, AXIS, IQEye, Panasonic, and Sony. To allow these devices to suspend and disable fast MPEG-4 start up times and reliable event communication, contact the Cisco Technical Assistance Center.

Cisco Video Surveillance Operations Manager 4.1 New and Changed Information

Enhancements and changes in Cisco Video Surveillance Operations Manager 4.1 include the following:

- Dual streaming support for MPEG-4 and H.264—Dual MPEG-4 and H.264 streams are now supported from a single encoder port. Separate proxies are created for each feed.
- Improved motion configuration—The AxClient supports the detection of motion from different segments (windows) of a single feed. During motion configuration setup, a VSOM user provides specific names for each of these segments/windows, although the segment/window name is not displayed in the Motion Configuration panel.
- Multiple stream export and support in ReView Player—VSOM now supports multi-stream exports from the Operator page. When you choose this option, the system prompts for the export start and end time (default values are the earliest start time and the latest end time). VSOM then creates the export CVA file. The resulting video clip will contain a multi-pane window player with all playable video clips and can be viewed in the ReView player.
- Support for Stream Manager H.264 events, and serial pass-through—The Stream Manager encoder now supports all H.264 resolutions and serial-pass-through of PTZ and camera control commands. The encoder can also receive and process events. Support is also included for the new x-code value `h264.ciscosm_x`.
- Clipping from Pelco DVRs—It is now possible to create server-side and client-side clips from the Pelco Endura DVR using the standard VSMS interfaces.
- Batch administration—Users can add cameras and change multiple camera parameters at one time from a single page.
- Database backups—Support is provided to back up the VSOM database.
- Custom fields—Users can create custom field labels in VSOM to add additional information on users or cameras.
- System Overview—The System Overview panel in the VSOM Administration pages displays information disk space usage for the media servers managed by VSOM and user login sessions.
- Event pagination—Pagination controls are provided for the Events Inbox in the VSOM Operator page.



Note

Cisco Video Surveillance Operations Manager 4.0 is backward compatible only with Cisco Video Surveillance Media Server 5.x. In addition, Cisco Video Surveillance Operations Manager 4.1 is backward compatible Cisco Video Surveillance Media Server 5.x with the following exceptions:

- Batch Administration uses new APIs that are available only in VSMS 6.1 to update existing settings.
- Batch Administration requires new Encoding Server updates to bulk add new cameras.

Cisco Video Surveillance Virtual Matrix 6.1 New and Changed Information

New features in Cisco Video Surveillance Virtual Matrix 6.1 include a variety of client performance enhancements and internal upgrades to make it compatible with the Cisco Media Server client:

- VSVM installer enhancement—A new and more efficient installer is now provided for VSVM.
- VSVM configuration utility enhancement—The new configuration utility allows for multiple configurations in a single installation of VSVM. This arrangement simplifies the use of multiple installations of VSVM.

Important Upgrade Notes

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.

Supported Devices Correction

The supported devices, which is linked from “Supported Devices Matrix” in *Video Surveillance Media Service User Guide*, and listed in the Camera Model drop-down menu in the VSOM IP/Network Camera page, list the IQEye Alliance 22S Network Camera and the Sony SNC-P1 Network Camera as supported devices. These cameras are not supported in this release.

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

You can use the Cisco Video Surveillance IP Camera model CIVS-IPC-2500 (wired model) and CIVS-IPC-2500W (wireless model) with VSM 3.1.1/5.1.1 and above, 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 IP camera models:

- [IP Camera Features that VSM Does Not Support](#), page 6
- [Obtaining a Required Driver Pack](#), page 6
- [Guidelines for Using the IP Camera with VSM](#), page 6
- [Troubleshooting the IP Camera when used with VSM](#), page 7

IP Camera Features that VSM Does Not Support

Table 1 lists the IP camera features that are not compatible with VSM.

Table 1 IP Camera Features not Currently Compatible with VSM

Feature	IP Camera Implementation
Alarm events outputs	2 out / FTP clip / e-mail
Alarm inputs	2 in
Audio	Simplex / half duplex / full duplex
Cisco Discovery Protocol (CDP)	Sends CDP discovery messages
Event scheduling	You can schedule event notification from the IP camera web interface
Event notification	E-mail or FTP alerts if an event occurs
IP Filter window	Provides options for controlling access to the IP camera by IP address
Motion detection	Detects motion in up to 3 configured areas in the video field
Multicasting	Sends video and audio data as multicast streams
PTZ (RS-485) window	Provides options for pan, tilt, zoom (PTZ) functions
QoS	Quality of Service (QoS) for audio streams, video streams, or both
SNMP window	Provides options for configuring SNMP settings

Obtaining a Required Driver Pack

If you update the IP camera firmware, you may need to download and install a driver pack so that the IP camera works with VSM. 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>

Guidelines for Using the IP Camera with VSM

The following guidelines apply when you use the IP camera with VSM:

- The IP camera must be installed and configured as described in *Cisco Video Surveillance IP Camera User Guide*.
- 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 IP camera and use VSM at the same time

Troubleshooting the IP Camera when used with VSM

If you experience difficulty when using the 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 camera is selected
- Verify that VSM is installed properly
- Verify that the VSM driver pack for the IP camera is installed properly
- Verify there are no firewalls enabled on VSM servers
- Verify that the default gateway is configured for the IP camera
- Verify that your web browser supports Active X controls
- Verify that the user name and password are configured identically for the camera and the VSOM 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

Orderability Matrix

Table 1 shows the orderability matrix for versions of SuSE Linux Enterprise Server (SLES) and various Cisco Video Surveillance hardware platforms and Cisco VSM releases.

Table 2 *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	SLES 10, SP 1
	4.1/6.1	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
	4.1/6.1	SLES 10, SP 1

1. You can upgrade to Cisco VSM 4.1/6.1 on legacy Cisco Video Surveillance servers. Cisco VSM 4.1/6.1 can run under SLES 9, SP3 or SLES 10, SP 1.

Caveats

Use the Bug Toolkit to find information about the caveats (bugs) for the current release of Cisco Video Surveillance Media Server, 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/action.do?hdnAction=searchBugs>.
- 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:
- Choose **Physical Security** from the Select Product Category menu.
 - Choose the desired product from the Select Product menu.
 - Choose the version number from the Software Version menu.
 - 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.
-

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0809R)