



Release Notes for Cisco Video Surveillance Manager 4.2/6.2

July, 2009

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

- Cisco Video Surveillance Media Server Release 6.2.
- Cisco Video Surveillance Operations Manager Release 4.2.
- Cisco Video Surveillance Virtual Matrix Release 6.2.

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](#)
- [Important Licensing Note, page 3](#)
- [Important Upgrade Notes, page 3](#)
- [Obtaining a Driver Pack, page 4](#)
- [Using Cisco VSM with the Cisco Video Surveillance Standard Definition IP Camera, page 4](#)
- [Using Cisco VSM with the Cisco Video Surveillance High Definition IP Camera](#)
- [Orderability Matrix, page 7](#)
- [Known Issues when using VSM 4.2/6.2 with a Cisco Video Surveillance IP Camera, page 8](#)
- [Caveats, page 10](#)



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

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 4.2/6.2. 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 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 Licensing Note

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.

Because license keys no longer determine the home page for a VSM host, you now set the VSOM 4.2 Log In page as the default web page as part of the VSOM 4.2 installation or upgrade process.

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.

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 the Cisco Video Surveillance standard definition IP camera 2400 series and 2500 series 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 standard definition IP camera models:

- [Standard Definition IP Camera Features that VSM Does Not Support, page 4](#)
- [Guidelines for Using the Standard Definition IP Camera with VSM, page 5](#)
- [Troubleshooting the Standard Definition IP Camera when used with VSM, page 5](#)

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 2.1.0 and VSM 4.2/6.2.



Note

The VSM driver that this release includes is compatible with all existing versions of the Cisco IP camera firmware. However, the features that this section describe require firmware release 2.1.0. None of these features are supported when using VSM with firmware releases earlier than 2.1.0.

Table 1 *Standard Definition IP Camera Features Compatibility for Firmware Release 2.1.0 and VSM 4.2/6.2*

| 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. |

Table 1 Standard Definition IP Camera Features Compatibility for Firmware Release 2.1.0 and VSM 4.2/6.2 (continued)

| Feature | Standard Definition IP Camera Implementation | Compatibility with Firmware Release 2.1.0 |
|--------------------|--|---|
| Event notification | E-mail or FTP alerts if an event occurs | Includes the VSM event notification API. |
| 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 | Supported for primary stream only. Use VSOM tools to detect motion in 1 configured area in the video field. Masking an area is not supported. |
| Multicasting | Sends video and audio data as multicast streams | Not supported. |
| 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. |

Guidelines for Using the Standard Definition IP Camera with VSM

When you use the standard definition IP camera with VSM, the camera must be installed and configured as described in *Cisco Video Surveillance IP Camera User Guide* for the standard definition IP camera.

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 that the VSM driver, dp_cisco, for the standard definition IP camera is installed properly
- Verify there are no firewalls enabled 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

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

You can use the Cisco Video Surveillance high definition IP camera model CIVS-IPC-4500 and CIVS-IPC-4300 with VSM 4.2/6.2, but be aware that the high definition camera includes features that are not currently integrated with VSM.

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. |
| 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 |
| QoS | Quality of Service (QoS) for audio streams, video streams, or both. |
| SNMP | Provides options for configuring SNMP settings |

Table 2 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 the High Definition IP Camera with VSM

When you use the high definition IP camera with VSM, the camera must be installed and configured as described in *Cisco Video Surveillance IP Camera User Guide* for the high definition IP camera.

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 that the VSM driver, dp_cisco, for the high definition IP camera is installed properly
- Verify there are no firewalls enabled 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

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 | SLES 10, SP 1 |
| | 4.1.1/6.1.1 | SLES 10, SP 1 |
| | 4.2/6.2 | SLES 10, SP 1 |

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

| Hardware | Cisco VSM Release | SLES Version |
|--|--------------------------|---------------|
| 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 | SLES 10, SP 1 |
| | 4.2/6.2 | SLES 10, SP 1 |

1. You can upgrade to Cisco VSM 4.2/6.2 on legacy Cisco Video Surveillance servers.

Known Issues when using VSM 4.2/6.2 with a Cisco Video Surveillance IP Camera

Table 4 describes known issues when using VSM 4.2/6.2 with a Cisco Video Surveillance IP Camera.

Table 4 Known Issues when Using VSM 4.2/6.2 with a Cisco IP Camera

| Known Issues | Customer Affect | Notes |
|--|---|--|
| Known issues when using VSM 4.2/6.2 with both SD IP Camera and HD IP Camera | | |
| The current VSM 4.2/6.2 Cisco Device Driver version is less than the version for the previous VSM 4.1.1/6.1.1 Driver Pack. | When you upgrade you will see that the Cisco Device Driver version listed under Management Console is lower than the previous one. | For the VSM 4.2/6.2 release, the current Cisco Device Driver version is dp_cisco 1.5-02d. |
| Special characters in passwords do not allow you to add Cisco IP cameras to VSM. | Passwords may not contain punctuation or special characters (for example &, #, ?, and %). | By default, SD cameras require special characters, but you can disable this by unchecking the password complexity option #1 in the camera configuration pages. |
| Known issues when using VSM 4.2/6.2 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. |
| 370 milliseconds latency in MPEG-4 camera feed. | A latency of at least 370 milliseconds under best network conditions. | — |
| 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 4.2/6.2 with a Cisco IP Camera (continued)

| Known Issues | Customer Affect | Notes |
|--|--|--|
| Cold start MPEG-4 feed may take up to 40 seconds. | When dual streaming and both streams need to be configured by Media Server, video takes 30 to 40 seconds to start up. If the proxy and camera settings match, start-up takes less than 1 second. | Longest start up times occur when both streams need to have configuration changes (MPEG-4+MPEG-4 and MPEG-4+JPEG). This situation does not occur often because proxy settings typically match the settings of the IP camera in a production environment. |
| Video motion detection fails after session times out on an SD IP camera, despite an active RTSP connection for that session ID. | Unable to use motion event for SD camera with firmware release 2.1.0. The following message appears in the ims.log after a session times out: "Unable to set the event trigger settings." | This issue exists in firmware release 2.1.0. |
| A user with administrative privileges cannot change configuration on an SD IP camera. This behavior is a change Administrative privileges in the camera. | You must use the user name "admin" to configure the SD IP camera with VSM | — |
| Restarting VSM software when any SD IP cameras are offline causes problems. Cameras that experience this issue will not be able to be displayed. | Offline SD IP cameras will not display properly even after they are brought back online. | If any SD IP cameras get into this state, bring the cameras online first, then restart VSM to resolve this issue. |
| Confusing behavior while adding an offline SD IP camera. | Even though VSOM returns an error message when adding an offline SD IP camera, once the camera is brought online the Camera Feed will appear properly after VSOM syncs with the Media Server. | It is highly recommended that you wait until any device is online and configured properly before adding it to VSOM |
| Adding an SD IP camera with firmware release 1.1.1 to VSOM with an incorrect or blank password causes problems that require you to restart VSMS. | Even after you correct the password in VSOM, you must restart the Media Server process before you will see video displayed for any affected SD IP cameras. | This only affects cameras running firmware release 1.1.1. |
| Known issues when using VSM 4.2/6.2 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 H.264 streams up to 30 fps. |
| Reverse play on H.264 archives does not work consistently. In addition to not working smoothly intermittently, a browser can hang in some cases. | While using reverse play by itself or with a combination of other trick play buttons on the VSOM Operator page, the browser can hang. In this case, you must exit the browser and log back in to VSOM. | 1 out of 4 clicks hangs; bit rate does not matter; the video may repeat for 2 to 3 seconds. All remaining H.264 HD camera reverse play related defects are still open. Other H.264 cameras do not have open issues. |
| Short or partial frames from the high definition IP camera are dropped by VSM to address the stuttering issue. | Pixilation or macro-blocking artifacts are seen when archives are initially loaded and when seeking. | Seen using any supported resolution/bit rate on H.264 streams. |

Table 4 Known Issues when Using VSM 4.2/6.2 with a Cisco IP Camera (continued)

| Known Issues | Customer Affect | Notes |
|--|---|---|
| Seek does not work consistently with H.264 archives. | Seeking on H.264 archives or seeking from the Event Inbox does not always succeed. Occurs more frequently with higher resolutions such as 1080p and 720p. | 1 out of 40 seeks fail when using the scrollbar; using Event Inbox within 3 clicks at 1080p, within 10 clicks at 720p. |
| Standalone clips in .AVI and .WMV formats play back at incorrect speeds. | Playback of .AVI and .WMV clips is too slow or too fast. | Affects all resolutions on HD IP cameras running H.264. This issue occurs due to limitations of the VSM API and because these clip container formats use only a single frame rate. |
| 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 should 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

Use the Bug Toolkit to find information about the caveats (bugs) for the current release of Cisco VSM, 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 **Physical 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.
-

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)