



Release Notes for Cisco Video Surveillance High Definition IP Cameras, Release 2.5.1

April 10, 2015

These release notes provide important information for the Cisco Video Surveillance High Definition IP camera Release 2.5.1, which applies to the following Cisco IP camera models:

- CIVS-IPC-6500PD
- CIVS-IPC-7530PD

For information about firmware compatibility and Cisco VSM releases that new cameras require, see the current Cisco VSM Release Notes at the following URL:

http://www.cisco.com/en/US/products/ps10818/prod_release_notes_list.html

Contents

This document includes the following sections:

- [What's New, page 2](#)
- [Important Notes, page 4](#)
- [Upgrading to Release 2.5.1, page 5](#)
- [Installing ActiveX Client, page 6](#)
- [Caveats, page 7](#)
- [Troubleshooting, page 8](#)
- [MIB Support, page 9](#)
- [Related Documentation, page 10](#)
- [Obtaining Documentation and Submitting a Service Request, page 10](#)



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

What's New

Cisco Video Surveillance IP camera firmware release 2.5.1 supports the following new features:

- [Support for Camera App Management from VSM, page 2](#)
- [Alerts, page 2](#)
- [Support for Video Recordings with Audio Storage, page 3](#)
- [Local Storage Drawer, page 3](#)
- [Support for Flip and Mirror, page 3](#)
- [Support for Day and Night Profiles, page 3](#)
- [Support for Import/Export Application Configuration, page 4](#)
- [IPv6 Support, page 4](#)
- [Cross Browser Support for Web UI, page 4](#)

Support for Camera App Management from VSM

IP camera apps can be managed from Cisco Video Surveillance Operations Manager (VSOM) release 7.6. This feature allows you to efficiently manage apps on multiple cameras. From VSOM you can install, unisntall, start, and stop apps. (To configure apps. use Configure Apps Settings page in the IP Camera web-based interface.)

Alerts

IP cameras send alert notification as described in [Table 1](#)

Table 1 Alerts

Alert Name	Description	Severity	Category
Health Alerts			
Continuous Recording Failure	Continuous recording of IP camera video failed. This alert is generated only when continuous recording is enabled on the IP camera.	Critical/Info	Recording
Camera App Health	The camera has rebooted four times within a configured time window.	Critical/Info	Software
SD Card-Not Read-Format Required	An SD or MicroSD card is not ready for recording and formatting is required.	Critical/Info	Recording
SD Card-In Recovery Mode	An SD or MicroSD that was removed from a camera has been placed in another camera.	Critical/Info	Recording
Audit Alerts			
SD Card State	An SD or MicroSD card has been inserted or removed from the IP camera.	Info	Hardware

Table 1 **Alerts (continued)**

Alert Name	Description	Severity	Category
SD Card Formatted	An SD or MicroSD card has been formatted successfully.	Info	Hardware
Camera Apps Status	The status of an app changed. For example, the app restarted or stopped.	Info	Software
Security Alert			
Camera Tamper	The camera view has been changed or blocked. This alert is generated only when tamper detection is enabled on the IP camera.	Critical/Info	Hardware

Support for Video Recordings with Audio Storage

Video recordings that include audio can be stored on an SD or MicroSD card. Configure settings from the IP camera web-based interface by choosing **Setup > Local Storage > Settings** and configuring the **Enable continuous recording** and **Enable audio recording** options.

Audio-only recordings are not supported.

Local Storage Drawer

The Local Storage page was moved to its own drawer under the Setup menu.

Support for Flip and Mirror

The Advanced Settings options under View Video > Camera Settings include the following new check boxes:

- **Flip**—Rotates the video image by 180 degrees, which results in a reversal of an original image across a horizontal axis
- **Mirror**—Reverses the video image across a vertical axis

Updates that you make by using these settings affect stored video from the camera, and live video from the camera that is viewed on the camera or on another client device.

Both settings apply to the primary and secondary video streams. An individual stream cannot be flipped or mirrored.

Support for Day and Night Profiles

The IP camera supports now supports separate configuration settings for day mode and for night mode. You can choose **Day** from the Mode drop-down list in the Setup > Camera window to configure settings for day mode, and you can choose **Night** to configure settings for night mode.

Support for Import/Export Application Configuration

App configuration can be exported from an IP camera and imported to other IP cameras.

IPv6 Support

IP cameras support IPv6 functionality for many features and operations. (IPv6 functionality is not supported for multicast events and alerts.)

Cross Browser Support for Web UI

Each supported web browser now supports all IP Camera features, except motion detection, custom exposure region, and privacy zone, which are available only on supported Internet Explorer versions.

Important Notes

The following important notes apply to this release:

- By default, app management for an IP camera that has been added to VSM Release 7.6 is performed from VSOM. If you want to manage apps from the IP camera web-based interface (called local apps management), delete the camera from VSM. If you physically removed a camera from a deployment without deleting it from VSM, you can enable local apps management by performing a factory reset procedure on the camera.
- The Enable Video option on the App Configuration page in the IP camera web-based interface has been removed.
- Before you use the IP camera web-based interface to install an app cpk file that is 2 Mb or larger in size, stop any audio or video app that is running on the camera. Otherwise, the installation fails.
- Camera Tamper alert is enabled automatically when Security alert is enabled on the IP camera.
- When a privacy alert region is enabled, the text “Privacy Alert Enabled” appears as an overlay on the video in the Camera Video & Control window.
- After you save updated settings on the Setup > Administration > Initialization page or the Setup > Network Setup > IP Addressing page, redirection to the Login page takes approximately 30 seconds.
- After you update to this firmware release, clear your web browser cache to ensure that new features in this release appear in the IP camera web-based interface.
- The automatic refresh feature that was available in the camera Home page is disabled in this release. To update information in this page, click the **Refresh** button in your web browser.
- If ActiveX is not installed on the client PC from which you access the IP camera web-based interface, the system prompts you to install the Cisco Camera UI Control when you access the View Video window or the Setup > Local Storage window. This message can take some time to display.
- If ActiveX does not work properly you install it, restart your client PC.
- The following 802.1x authentication options are not supported:
 - PEAP authentication with Server Certificate validation
 - EAP-FAST authentication with manually uploaded PAC files
- The SRTP feature has been removed from the IP camera web-based interface.

Upgrading to Release 2.5.1

If your IP camera has an earlier firmware release, you can upgrade it to firmware release 2.5.1 by using the Camera Firmware Upgrade feature in the VSM Management Console. For instructions, see the “Using the VSM Management Console” chapter in *Cisco Video Surveillance Manager User Guide*.

Alternatively, you can upgrade your IP camera to firmware release 2.5.1 by performing the following steps.

Procedure

-
- Step 1** Take these actions to obtain the release 2.5.1 firmware:
- a. Go to the following URL:
<http://www.cisco.com/cisco/software/navigator.html>
 - b. Choose **Product > Physical Security > Connected Physical Security > Video Surveillance IP Cameras > Cisco Video Surveillance *serial_num* Series IP Cameras > Cisco Video Surveillance *model_num* IP Camera**, where *serial_num* is the IP camera series number and *model_num* is the IP camera model number.
 - c. From the navigation pane on the left, choose the **2.5.1** release.
 - d. Download the 2.5.1 firmware with the file name that applies to your IP camera:
 - For 6500PD IP cameras: CIVS-IPC-65xx-2.5.1-5.bin
 - For 7530PD IP cameras: CIVS-IPC-75xx-2.5.1-5.bin
 - e. Log in and follow the on-screen prompts to download it to your PC.
- Step 2** Take these actions to display the Firmware window in the web interface for your IP camera:
- a. Start Internet Explorer and enter the following in the address field:
`protocol://ip_address:port_number`
 where:
 - *protocol* is the connection that you use for your IP camera (either HTTPS or HTTP).
 - *ip_address* is the IP address of your IP camera.
 - *port_number* is the port number that is used for HTTPS or HTTP connections to the IP camera. You do not need to enter a port number if you are connecting through the default HTTPS port 443 or the default HTTP port 80.
 - b. Enter your IP camera user name and password when prompted, then click **OK**.
 The IP Camera Main window appears.
 - c. Click the **Setup** link to access configuration menus for the camera.
 - d. Click **Administration**, then click **Firmware**.
 The Firmware window appears.
- Step 3** In the Firmware Maintenance area, click **Browse**, choose the upgrade file, and then click **Open**.
 The upgrade file may be stored on another PC.

Step 4 Click **Upgrade**.

Do not power down the IP camera during the upgrade procedure.

After upgrading to the 2.5.1 firmware, clear the browser cache, close and reopen the browser to ensure the changes from the new firmware are reflected correctly.

After you upgrade the firmware, the IP camera automatically restarts. It retains all configuration information.

Installing ActiveX Client

The following sections provide information about installing the ActiveX client:

- [Minimum Installation Requirements, page 6](#)
- [Installation Procedure, page 6](#)

Minimum Installation Requirements

- Windows 7 with Standard User Rights
- DirectX End-User Runtime (DirectX 9.0 or higher)
DirectX 11 installed with Windows 7
- .Net Framework 2.0 SP 1 or higher
Installed with Windows 7 by default
- Computer Display drivers installed properly
- Support for the 32-bit version of Internet Explorer 8, 9, and 10

Installation Procedure

If you go to the View Video window or the Local Storage window in the IP camera web-based interface and ActiveX is not installed, the window indicates that ActiveX is required provides instructions that explain how to download and install ActiveX.

To download and install ActiveX, follow these steps:

Procedure

- Step 1** From the window IP camera web-based interface that instructs you to install the Cisco Camera UI Control , click **Install** in the yellow banner.
 - Step 2** If a Security Warning dialog box appears, click **Install**.
-

Caveats

The following sections provide information about caveats in this IP camera release:

- [Using the Bug Search Tool, page 7](#)
- [Open Caveats, page 8](#)
- [Resolved Caveats, page 8](#)

Using the Bug Search Tool

You can use the Bug Search Tool to find information about caveats (bugs) for this release, including a description of the problems and available workarounds. The Bug Search Tool lists both open and resolved caveats.

**Note**

Bug Search Tool is the successor to the Bug Toolkit.

To use the Bug Search Tool, follow these steps:

Procedure

-
- Step 1** Go to <https://tools.cisco.com/bugsearch/>.
- 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 field, then press **Enter**.
- Step 4** To look for information if you do not know the bug ID number, enter keywords which search for text matches in the following sections of a bug:
- headline/title
 - release note text
 - product
 - known affected releases/ known fixed releases
-

For more information about the Bug Search Tool, click Help on the main Bug Search Tool page:

<https://tools.cisco.com/bugsearch/>

Open Caveats

Table 2 describes the caveats that are open in this release.

Table 2 *Caveats Resolved in this Release*

Identifier	Description
CSCus59584	Cisco license error on camera
CSCut10929	Cannot use apps on an IP camera if you log in to the camera via IPv6 address with the Mozilla or Chrome browser

Resolved Caveats

Table 3 describes the caveats that are resolved in this release.

Table 3 *Caveats Resolved in this Release*

Identifier	Description
CSCus79904	Extension for domain name limited on SMTP configuration fields.

Troubleshooting

Symptom View Video page does not show the video stream after the installation is complete.

Recommended Action Reset Internet Explorer to its default settings.

- Under the Tools menu, select Internet Options.
- Click on the Advance Tab.
- In the Reset Internet Explorer settings section, click **Reset**.

Symptom Unable to view streaming video (black viewing panel and/or message that ActiveX plug-in is missing).

Recommended Action Validate that the ActiveX plug-in is installed on the IE Web Browser.

- In the IE Tools menu, select Manage Add-ons.
- In the Add-on Types section, select Toolbars and Extensions. In the Name section under Cisco, check that DxPlay.Viewer is listed for the name of the plug-in.
- If the plug-in is not present, close IE.
- Run IE as Administrator to ensure no domain or PC policies prevent IE from running in Administrator mode.
- Repeat checking for the plug-in the browser.

Symptom Unable to install ActiveX or view streaming video because of firewall settings.

Recommended Action To ensure the firewall is not blocking the installation of ActiveX or preventing streaming video, adjust your firewall settings accordingly.

Symptom Unable to view streaming video because of the firewall on the ports.

Recommended Action Check with your network administrator to ensure the following ports are open for streaming:

- Primary Stream—1024 (video), 1026 (audio)
- Secondary Stream—1032 (video), 1034 (audio)

Symptom Unable to install ActiveX or view streaming video because of an existing version.

Recommended Action

- Go to Control Panel from the Start menu.
- Select Programs and Features.
- Search for Cisco Camera UI Control v.X.XX.X.XX.
- Right click and click on Uninstall to remove ActiveX.

MIB Support

SNMP Versions 2c and 3 are supported in Release 2.5.1.

Table 4 shows the supported and unsupported MIBs.

Table 4 MIB Support in Release 2.5.1

MIBs	RFC	Support
RFC1213-MIB	RFC1213	
system		Yes
interface		Yes
at		No
ip		Yes
icmp		Yes
tcp		No
udp		No
snmp		Yes
ENTITY-MIB		
Host-Resource-MIB	RFC1514	Yes
SNMP Trap (Ver 1)		
cold start, warm start		Yes

Table 4 **MIB Support in Release 2.5.1 (continued)**

MIBs	RFC	Support
reconfigure		No
link up/down		link up (yes), link down (no)
SNMP Trap (Ver 3)		
authentication failure		Yes
Wireless LAN MIBs - IEEE802dot11-MIB		No
CISCO-CDP-CAPABILITY.MIB.my		No
CISCO-CDP-MIB.my		No

Related Documentation

For additional information about the Cisco Video Surveillance IP camera, see the *Installation Guide* and *Configuration Guide* for your IP camera. The documentation is available at this URL:

www.cisco.com/go/ipcamera

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned 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. (1110R)

© 2015 Cisco Systems, Inc. All rights reserved.