Release Notes for Cisco Video Surveillance High Definition IP Cameras, Release 2.5.0

First Published: December 12, 2014

These release notes provide important information for the Cisco Video Surveillance High Definition IP camera, Release 2.5.0, which applies to the following Cisco IP camera models:

- 3000 Series IP Cameras
  - CIVS-IPC-3421V
  - CIVS-IPC-3520
  - CIVS-IPC-3530
  - CIVS-IPC-3535
- 6000 Series IP Cameras
  - CIVS-IPC-6000P
  - CIVS-IPC-6020
  - CIVS-IPC-6030
  - CIVS-IPC-6050
  - CIVS-IPC-6400
  - CIVS-IPC-6400E
- 7000 Series IP Camera
  - CIVS-IPC-7030
  - CIVS-IPC-7030E
- PTZ IP Cameras
  - CIVS-IPC-2830
  - CIVS-IPC-2835
  - CIVS-IPC-6930

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

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

Contents

This document includes the following sections:

What's New

Cisco Video Surveillance IP camera firmware release 2.5.0 supports the following new features:

Support for Camera App Management from VSM

IP camera apps can be managed from Cisco Video Surveillance Operations Manager (VSOM) in VSM Release 7.6. User VSOM to install and manage the apps on multiple cameras and to configure actions triggered by camera app events.

When camera apps are managed from VSOM, you can only configure the app-specific settings through the IP camera web UI. Installing, uninstalling, starting and stopping the apps must done through VSOM License management for the apps is also done through VSOM.

Alerts

IP cameras send alert notification about following alert types:

Health Alerts

Alert Name	Description	Severity	Category
Continuous Recording Failure	Continuous recording of IP camera video fails. This alert is generated only when continuous recording is enabled on the IP camera.	Critical/Info	Recording
Camera App Health	Any application that crashed frequently affects the IP camera health and is stopped.	Critical/Info	Software
SD Card-Not Read–Format Required	The SD card is not ready for recording, and formating is required.	Critical/Info	Recording
SD Card-In Recovery Mode	The SD card recording details do not match the IP camera into which it has been inserted. To start recording on the SD card, you must perform a format of the SD card. **Note** Copy all required data before performing a format of the card.	Critical/Info	Recording

Audit Alerts

Alert Name	Description	Severity	Category
SD Card State	The SD card is inserted or removed from the IP camera.	Info	Hardware
SD Card Formatted	The SD card is formatted successfully.	Info	Hardware
Camera Apps Status	Any application changes its status, for example, restarted, stopped, and so forth.	Info	Software

Security Alert

Alert Name	Description	Severity	Category
Camera Tamper	Camera view is changed or blocked. This alert is generated only when the tamper detection is enabled on the IP camera.	Critical/Info	Hardware

PTZ Movement Alert

Alert Name	Description	Severity	Category
PTZ Movement	This alert is triggered by the movement start and stop caused by pan/tilt/zoom actions. **Note** This alert is only applicable to the PTZ IP cameras.	Info	Software

Flip and Mirror

Flip is the mirror reversal of an original image across a horizontal axis.

Mirror is the mirror reversal of an original image across a vertical axis.

Flip and mirror are applicable to both the primary and secondary channels simultaneously. An individual channel cannot be flipped or mirrored.

Support for Day and Night Profiles

In Release 2.5.0, IP cameras support separate profiles and settings for day mode and night mode. In previous releases, the IP camera supported the same settings in day mode and night mode.

You can configure different settings for day and night mode through web UI. Based on the day or night mode, the respective profiles and settings are automatically selected and applied on the IP camera sensor.

New User Roles—Guard and Supervisor

The following two new user's roles have been added to the user list. The user list displays the new authorized users and access levels.

- Guard—Has access to view video and navigate between presets.
- Supervisor—Has access to view video, navigate presets, and perform PTZ movements.

Note These user roles are only applicable to PTZ IP cameras.

Support for Audio Storage

The edge storage now has support for audio recordings along with video recordings. Audio recordings can be enabled from Setup => Local Storage => Settings => Enable continuous recording & Enable audio recording.

Note Audio-only recordings are not supported.

IPv6 Support

The IP cameras now support IPv6 functionality.

Note IPv6 functionality is not supported for multicast events and alerts.

Support for Import/Export Application Configuration

The application configuration can be exported from the IP camera and be imported to other cameras.

Cross Browser Support for Web UI

More camera features are supported from cross browser now except motion detection, custom exposure region, and privacy zone.

Local Storage

A new tab for local storage has been added with separate web UI pages for local storage settings and local storage recordings.

Important Notes

- Camera App Management from VSM
  - When the IP camera is added to VSM Release 7.6, by default app management is done from VSM.
  - To enable apps management from the IP camera web UI, the camera needs to be deleted and removed from VSM.
  - If the IP camera is physically removed without being deleted from VSM, do a factory reset to enable apps management from camera web UI.
  - The enable video option on the app configuration page has been removed.
  - If you are installing app cpk files that are at least 2Mb from the camera web UI or from VSM, stop any video or audio app that is running on the camera. Otherwise, the installation fails.
- Camera Tamper alert is enabled automatically when security alert is enabled.
- Privacy Alert Region—Text overlay, “Privacy Alert Enabled,” is supported to show that the privacy alert region is enabled.
- Redirection to the login page after setting and initialization updates takes approximately 30 seconds.
- To ensure that the new features display, clear the browser cache and reload the web page.
- The auto refresh feature in the camera home page has been disabled. Click the refresh icon in the home page to update the contents.

- If ActiveX is not installed on your client PC, the View Video window and the Setup > Local Storage window prompts you to install the Cisco Camera UI Control. This message can take some time to display.
- If ActiveX is not working properly after installation, close the browser and restart the machine.
- The following 802.1x authentication options are not supported:
  - PEAP authentication with Validate Server Certificate
  - EAP-FAST authentication with uploaded PAC files
- The SRTP feature is not supported on the IP cameras.

  In previous firmware releases, this option was disabled in the Web UI. In this release, this option has been removed from Web UI.

Upgrading to Release 2.5.0

If your IP camera has an earlier firmware release, you can upgrade it to firmware release 2.5.0 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 2.5.0 by performing the following steps.

Note Upgrading from Release 2.0.0 and earlier to Release 2.5 formats the IP camera SD or MicroSD card, which permanently removes any data that the card contains.

Procedure

Step 1 Take these actions to obtain the release 2.5.0 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 **2.5.0** release.

d. Download the 2.5.0 firmware with the file name that applies to your IP camera:

- For 2830 and 2835 PTZ IP cameras: CIVS-IPC-283x-V2.5.0-10.bin
- For 3000 series IP cameras: CIVS-IPC-3xxx-V2.5.0-10.bin
- For 3535 IP camera: CIVS-IPC-3535-V2.5.0-10.bin
- For 6000 series IP cameras: CIVS-IPC-6xxx-V2.5.0-10.bin
- For 6930 PTZ IP camera: CIVS-IPC-6930-V2.5.0-10.bin
- For 7000 series IP cameras: CIVS-IPC-7xxx-V2.5.0-10.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 2.5.0 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 7
- Installation Procedure, page 8

Minimum Installation Requirements

- Windows 7 with Standard User Rights

  Windows XP with Admin Rights
- DirectX End-User Runtime (DirectX 9.0 or higher)
  - DirectX 9.0 installed with Windows XP
  - DirectX 11 installed with Windows 7
- .Net Framework 2.0 SP 1 or higher
  - Installed with Windows 7 by default

  - Needs to be installed on Windows XP
- 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**.

Backward Compatibility

If you downgrade firmware in an IP camera from Release 2.5.0 to a release earlier than 1.4.1 and if the configured number of presets is greater than 16, all preset configurations are cleared, and the IP camera does not reset after the downgrade. In other cases, the IP camera does reset automatically.

Caveats

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

- Using the Bug Search Tool, page 8
- Known Caveats, page 9
- Resolved Caveats, page 9

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/

Known Caveats

Table 1 describes the know caveats in this release.

Table 1 Caveats Open in this Release

Identifier	Description
CSCub85297	Video distortion may occur when viewing multiple cameras on the same PC.
CSCue99434	MJPEG config change may take up to 5 minutes before streaming start.
CSCui95069	283x/3xxx/6xxx/6930/7xxx: 802.1x does not work after certificate change

Resolved Caveats

Table 2 describes the know caveats that are resolved in this release.

Table 2 Caveats Resolved in this Release

Identifier	Description
CSCui23498	283x/3xxx/6xxx/6930/7xxx: Camera does not send Cold Start SNMP trap.
CSCun13628	Audio clicking from Camera GUI ActiveX.
CSCup88035	7xxx: Video is jerky and shows inconsistent jumps for 5MP resolution.
CSCur01560	Extension for domain name limited on SMTP config 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 2.5.0.

Table 3 shows the supported and unsupported MIBs.

Table 3 MIB Support in Release 2.5.0

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
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.