Release Notes for Cisco Video Surveillance High Definition IP Cameras, Release 2.7.0

December 4, 2015

These release notes provide important information for the Cisco Video Surveillance High Definition IP camera, Release 2.7.0, which applies to the following Cisco IP camera models:

- 3000 Series IP Cameras
  - CIVS-IPC-3050
  - 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
  - CIVS-IPC-6500PD
- 7000 Series IP Camera
  - CIVS-IPC-7030
  - CIVS-IPC-7030E
  - CIVS-IPC-7070
  - CIVS-IPC-7530PD
- 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

Contents

This document includes the following sections:

What's New

- Table 1 describes the new features that Cisco Video Surveillance IP camera firmware release 2.7.0 supports.

Table 1   *New Features*

Feature	Description
Event history	The IP camera can capture and store information about events, including video that is associated with event. You can configure how the camera displays event history, see information about events, and download video files that are associated with events.
Updated operating system and browser support[1]	Support for Microsoft Windows 8 (32-bit or 64-bit) and Microsoft Internet Explorer 11 (32-bit).
Image overlay[1]	New image overlay options in the Video Overlay window allow configuring an image that appears as an overly on the video image from the IP camera.
Clear tamper alert[1]	New options in the Camera Window allow configuring the IP camera to clear a tamper alert automatically after a designated amount of time

1. The feature was introduced for the CIVS-IPC-3050 and CIVS-IPC-7070 models in the firmware 2.6.0 release.

- Poodle Fix—Cisco Video Surveillance IP camera firmware release 2.7 resolves CSCut56581, the camera vulnerability to CVE-2014-3566- Poodle. Cisco recommends that you upgrade to this latest release.

Important Notes

- Redirection to the IP Camera login page after making setting and initialization updates takes approximately 30 seconds.

- To ensure that new features display after a firmware update, clear the browser cache and reload the web page.

- If you install the following sequences of firmware on and IP camera, reformat the SD or MicroSD card that is installed in the IP camera, or delete all recording data on the card:

  - For all cameras except CIVS-IPC-6500PD and CIVS-IPC-7530PD:

    - Release 2.5.0 -> Release 2.7.0 -> Release 2.5.0 -> Release 2.7.0

    - Release 2.7.0 -> Release 2.5.0 -> Release 2.7.0

  - For CIVS-IPC-6500PD and CIVS-IPC-7530PD:

    - Release 2.5.1 -> Release 2.7.0 -> Release 2.5.1 -> Release 2.7.0

    - Release 2.7.0 -> Release 2.5.1 -> Release 2.7.0

Upgrading to Release 2.7.0

If your IP camera has an earlier firmware release, you can upgrade it to firmware release 2.7.0 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 2.7.0 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 2.7.0 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 **2.7.0** release.

d. Download the 2.7.0 firmware with the file name that applies to your IP camera:

   - For 2830 and 2835 PTZ IP cameras: CIVS-IPC-283x-V2.7.0-20.bin

   - For 3000 series IP cameras: CIVS-IPC-3xxx-V2.7.0-20.bin

   - For 3050 IP cameras: CIVS-IPC-3050-V2.7.0-20.bin

   - For 3535 IP camera: CIVS-IPC-3535-V2.7.0-20.bin

- For 6000 series IP cameras: CIVS-IPC-6xxx-V2.7.0-20.bin
- For 6930 PTZ IP camera: CIVS-IPC-6930-V2.7.0-20.bin
- For 7000 series IP cameras: CIVS-IPC-7xxx-V2.7.0-20.bin
- For 7070 IP camera: CIVS-IPC-7070-V2.7.0-20.bin
- For 6500PD IP camera: CIVS-IPC-65xx-V2.7.0-20.bin
- For 7630PD IP camera: CIVS-IPC-75xx-V2.7.0-20.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 2.7.0 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

- 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 9, 10, and 11

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 2.7.0 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

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 2 describes the known caveats in this release.

Table 2   *Caveats Open in this Release*

Identifier	Description
CSCub85297	Video distortion may occur when viewing multiple cameras on the same PC
CSCue99434	MJPEG configuration change may take up to 5 minutes before streaming starts
CSCum43626	Camera fails to install license for camera application
CSCut10929	Cannot use apps if log in via IPv6 address with Mozilla or Chrome browser
CSCuv10473	Cannot configure .255 network addresses

Resolved Caveats

Table 3 describes the resolved caveats in this release.

Table 3   ***Caveats Resolved in this Release***

Identifier	Description
CSCut56261	Stream 2 disabled when camera apps enabled by VSM
CSCuu25141	3xxx/6xxx/6930—Audio may appear to pause or stutter
CSCuv47587	ActiveX installation is not working for some systems

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.