Release Notes for Cisco Video Surveillance High Definition IP Camera, Release 1.3.2

July 2013

These release notes provide important information for the Cisco Video Surveillance High Definition IP camera, Release 1.3.2, which applies to the following Cisco IP camera models:

- 3000 Series IP Cameras
  - CIVS-IPC-3421V
  - CIVS-IPC-3520
  - CIVS-IPC-3530
- 6000 Series IP Cameras
  - CIVS-IPC-6000P
  - CIVS-IPC-6020
  - CIVS-IPC-6030
  - CIVS-IPC-6400
- 7000 Series IP Camera
  - CIVS-IPC-7030

This firmware is compatible with Cisco VSM 7.0.1 and Cisco VSM 7.0.1 Driver Pack, Release 2.0-27d.

Contents

This document includes the following sections:

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

What's New in this Release

Cisco Video Surveillance IP camera firmware release 1.3.2 provides fixes for caveats (see the "Caveats" section on page 4) and supports the following news features:

- Open Network Video Interface Forum (ONVIF) 2.0—ONVIF is an open industry forum for the development of a global standard for the interface of IP-based physical security products. The following features are supported in this release.
  - Device Discovery Service
  - Device Service
  - Media Service

  This mode is available from the Basic Operations section of the Basic window area of the camera's interface (**Setup > Network Setup> Basic**).

  For more information, refer to the Cisco 7000, 6000, and 3000 Series IP Camera Configuration Guides on Cisco.com.

  Note Do not enable ONVIF when using with Cisco VSM to avoid conflicts with configurations.

- New Resolutions—The following new 16:9 resolutions are supported for both primary and secondary streams on the Cisco 3000 Series, Cisco 6000 Series, and Cisco 7030 cameras with this release:
  - 768 x 432
  - 704 x 400
  - 352 x 208

Note If you configure the camera for one of these resolutions and then downgrade the firmware, the camera might reboot. Before downgrading, change the resolution back to an older resolution.

Important Notes

The following features are not supported on the IP cameras:

- SRTP
- Event/FTP

In previous firmware releases, these options were disabled in the Web UI. In this release, these options have been removed from Web UI.

Upgrading to Release 1.3.2

If your IP camera has an earlier firmware release, you can upgrade it to firmware release 1.3.2 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 1.3.2 by performing the following steps.

Procedure

Step 1 Take these actions to obtain the release 1.3.2 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 **1.3.2** release.

d. Download the 1.3.2 firmware with the file name that applies to your IP camera:

- For 3000 series IP cameras: CIVS-IPC-3xxx-V1.3.2-8.bin
- For 6000 series IP cameras: CIVS-IPC-6xxx-V1.3.2-8.bin
- For 7000 series IP cameras: CIVS-IPC-7xxx-V1.3.2-8.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 1.3.2 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.

Caveats

Table 1 describes the caveats that are open 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.

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

To access Bug Toolkit, you need an Internet connection and a Cisco.com user ID and password.

To use the 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:

a. Choose **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.

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.