Release Notes for Cisco Video Surveillance High Definition IP Camera Release 2.3.1

August, 2011

These release notes provide important information for the Cisco Video Surveillance high definition IP camera Release 2.3.1.

Firmware release 2.3.1 applies to the following Cisco IP camera models:

- CIVS-IPC-4300
- CIVS-IPC-4500

This firmware is compatible with Cisco Video Surveillance Manager (VSM) 6.3.2 and later. VSM 6.3.2 and later contains a camera firmware upgrade feature that simplifies and automates the firmware upgrade process.

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

Cisco Video Surveillance high definition IP camera firmware provides the following new features and updates:

Release 2.3.1

IP cameras with part numbers 74-5461-04 or 74-5459-04 that could not upgrade from Release 2.0.0 to Release 2.3.0 can now upgrade to Release 2.3.1 using an upgrade hot fix utility. For more information, see the "Using the Upgrade Hot Fix Utility to Upgrade to Release 2.3.1" section on page 4.

Release 2.3.0

- Enhanced Motion Detection—Improved motion detection algorithm that results in better accuracy and ease of deployment.
- Support for Windows 7 Enterprise and Internet Explorer 8.

Features No Longer Available

The following IP camera features are not available in this release:

- The USB port on an IP camera does not support a USB device for storing video
- Video clip for e-mail event notification—Attaching a video clip of an event to an e-mail notification is no longer supported

Upgrading to Release 2.3.1

Caution Do not use the procedure in this section to upgrade your IP camera to Release 2.3.1 if the IP camera part number is 74-5461-04 or 74-5459-04 and the firmware release on the IP camera is 2.0.0. Instead, you must use the upgrade hot fix utility available on Cisco.com to upgrade to Release 2.3.1.

You can find the IP camera part number listed on the camera user interface Home window, under the General Information area.

For more information about upgrading your IP camera using the upgrade hot fix utility, see the "Using the Upgrade Hot Fix Utility to Upgrade to Release 2.3.1" section on page 4.

Note You can upgrade an IP camera to firmware release 2.3.1 only from firmware release 1.2.1 or higher.

You can upgrade your IP camera to firmware 2.3.1 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 release 2.3.1 by performing the following steps.

Procedure

Step 1 Take these actions to obtain the release 2.3.1 firmware:

a. Go to this URL:

http://www.cisco.com/cisco/software/type.html?mdfid=282582478&flowid=7145

b. Click the **Video Surveillance IP Camera Firmware** link.

c. Locate and choose the 2.3.1 firmware file, which is named **CIVS-IPC-4xxx-V2.3.1-1.bin**, and click **Download Now**.

d. 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 window, click the **Upgrade** button.

The Upgrade Firmware window appears.

Step 4 In the Upgrade Firmware window, click the **Browse** button, choose the upgrade file, and then click **Open**.

The upgrade file may be stored on another PC.

Step 5 Click **Upgrade** and follow the on-screen prompts to load the firmware upgrade on the IP camera.

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

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

Using the Upgrade Hot Fix Utility to Upgrade to Release 2.3.1

Perform the following procedure to upgrade your IP camera to Release 2.3.1 only if the IP camera part number is 74-5461-04 or 74-5459-04 and the firmware release on the IP camera is 2.0.0. Otherwise, use the procedure in the "Upgrading to Release 2.3.1" section on page 2.

Note You can find the IP camera part number listed on the camera user interface Home window, under the General Information area.

Procedure

Step 1 Take these actions to ensure that SSH is enabled on 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 **Initialization**.

The Account Initialization window appears.

e. In the Access Protocols area, verify that the **Enable SSH** check box is checked; if it is unchecked, check it and click **Save Settings**.

Step 2 Take these actions to obtain the release 2.3.1 firmware:

a. Go to this URL:

http://www.cisco.com/cisco/software/type.html?mdfid=282582478&flowid=7145

b. Click the **Video Surveillance IP Camera Firmware** link.

c. Locate and choose the 2.3.1 firmware file, which is named **CIVS-IPC-4xxx-V2.3.1-1.bin**, and click **Download Now**.

d. Log in and follow the on-screen prompts to download the 2.3.1 firmware file to your PC.

Step 3 Take these actions to obtain the upgrade hot fix utility:

a. Go to this URL:

http://www.cisco.com/cisco/software/type.html?mdfid=282582478&flowid=7145

b. Click the **Video Surveillance IP Camera Utility** link.

c. Locate and choose the upgrade hot fix utility file, which is named **HotFixUtilityInstallerV1.1.0.msi**, and click **Download Now**.

d. Log in and follow the on-screen prompts to download the upgrade hot fix utility file to your PC.

e. Close Internet Explorer.

Step 4 Double-click the **HotFixUtilityInstallerV1.1.0.msi** file that you downloaded in Step 3 and follow the on-screen prompts to install the utility on your PC.

During the installation process, the installer adds the Hot Fix Utility icon to your desktop.

Step 5 Double-click the **Hot Fix Utility** icon to open the utility.

Step 6 Enter the IP address and password for the IP camera to be upgraded.

Step 7 Click **Upgrade** and follow the on-screen prompts to load the firmware upgrade on the IP camera.

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

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

Caveats

Table 1 describes the caveats that are resolved in this release.

Table 1 Caveats Resolved in this Release

Identifier	Description
CSCtr71180	Upgrade fails from 2.0.0 to 2.3.0

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

Table 2 Caveats Open in this Release

Identifier	Description
CSCtf87756	Users sometime logged out after resetting the camera when using static IP addresses
CSCtg22847	Camera UI hotspot Pan/Tilt command does not work correctly in certain resolutions
CSCtg73910	PEAP authentication fails when using Validate Server Certificate option
CSCtg76338	When using e-mail notification for motion events, if the e-mail server is unreachable, video stops streaming
CSCtg81428	Motion detection windows configured from VSM do not show the same boundaries on camera UI
CSCtg93230	Change in video resolution changes motion detection area
CSCtj42755	Browser logs out of the Analytics web UI after prolonged inactivity
CSCtj68155	In Edit mode, existing rules may not display in Analytics web UI
CSCtk33308	Upgrade from 1.2.1 to latest firmware using camera web UI may give false error
CSCtk75349	Missing duplex and power parameters in CDP
CSCtn22813	H.264 video may stutter in Web UI if AAC audio codec is enabled

Table 2 Caveats Open in this Release (continued)

Identifier	Description
CSCto34506	DirectShow setup may sometimes fail
CSCto40637	Video distortion may occur when viewing multiple cameras on the same PC

You can use the Bug Toolkit to find information about caveats (bugs) for the 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 *User Guide* for your IP camera. User Guides are available at this URL:

www.cisco.com/go/ipcamera

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information about obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and recommended aliases and general Cisco documents, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

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