



Release Notes for Cisco Video Surveillance High Definition IP Camera Release 1.1.2

October, 2012

These release notes provide important information for the Cisco Video Surveillance High Definition IP camera Release 1.1.2.

Firmware release 1.1.2 applies to the following Cisco IP camera models:

- CIVS-IPC-6000P
- CIVS-IPC-6020
- CIVS-IPC-6030
- CIVS-IPC-6400

This firmware is compatible with Cisco Video Surveillance Manager (VSM) 6.3.2 and 7.0. VSM 6.3.2 and 7.0 contain a camera firmware upgrade feature that simplifies and automates the firmware upgrade process.

Contents

This document includes the following sections:

- [What's New in this Release, page 2](#)
- [Upgrading to Release 1.1.2, page 2](#)
- [Caveats, page 3](#)
- [Related Documentation, page 4](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 4](#)



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

© 2012 Cisco Systems, Inc. All rights reserved.

What's New in this Release

Cisco Video Surveillance IP camera and IP dome firmware release 1.1.2 provides the following new features and functionality:

- Support for the new CIVS-IPC-6030 and CIVS-IPC-6400 IP camera models.
- Fixes for several caveats (see the “Caveats” section on page 3).

Upgrading to Release 1.1.2

You can upgrade your IP camera to firmware 1.1.2 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 release 1.1.2 by performing the following steps.

Procedure

-
- Step 1** Take these actions to obtain the release 1.1.2 firmware:
- Go to the following URL:
<http://www.cisco.com/cisco/software/navigator.html>
 - Choose **Product > Physical Security > Connected Security > Video Surveillance IP Cameras > Cisco Video Surveillance 6000 Series IP Cameras > Cisco Video Surveillance 6000 IP Camera**.
 - From the navigation pane on the left, choose the **1.1.2** release.
 - Download the 1.1.2 firmware file named CIVS-IPC-6xxx-V1.1.2-30.bin.
 - 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:
- 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.
 - Enter your IP camera user name and password when prompted, then click **OK**.
The IP Camera Main window appears.
 - Click the **Setup** link to access configuration menus for the camera.
 - Click **Administration**, then click **Firmware**.
The Firmware Settings 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**.

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
CSCuc56526	6xxx: Multiple configuration changes may cause camera to reboot
CSCuc84668	6xxx: Changing resolutions may cause view video page to freeze

Table 2 describes the caveats that are open 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

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 *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>

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at 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. (1005R)