Release Notes for Cisco Video Surveillance High Definition IP Cameras, Release 2.0.2

First Published: May 2014

These release notes provide important information for the Cisco Video Surveillance High Definition IP camera, Release 2.0.2, 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 in this Release

Cisco Video Surveillance IP camera firmware release 2.0.2 supports the following new features:

Heartbleed Fix

Cisco Video Surveillance IP camera firmware release 2.0.2 resolves CSCuo37282, the camera vulnerability to CVE-2014-0160- Heartbleed. Cisco recommends that you upgrade to this latest release.

Camera Support

This release supports the following new Cisco IP cameras. These cameras require Cisco VSM 7.5.

- CIVS-IPC-3535
- CIVS-IPC-6050
- CIVS-IPC-6400E
- CIVS-IPC-7030E

Local Storage

This firmware release provides updates and enhancements to the local storage features on the IP camera. Updates and guidelines include:

- Continuous recording—This feature enables VSM to "auto-merge" video archive that has gaps due to network or other issues (assuming that camera was not affected), using camera storage as a temporary archiving medium. It also enables archiving only video that is close to generated events. Either the primary stream or secondary stream can recorded in this mode.
- Grooming—Starts when continuous recording is enabled and operates as follows:
  1. Groom files that are marked as deleted.
  2. Groom the oldest files on the local SD or MicroSD card when available space on the card is less than 1 GB.
- The IP camera supports an SD or MicroSD card with a maximum storage capacity of 32 GB. For efficiency and performance of the local storage feature, Cisco recommends that you use a SD or MicroSD card with a storage capacity of 32 GB.
- 1 GB of the storage capacity on an SD or MicroSD card is reserved for system use and is not available to store recordings.
- When you put an SD or MicroSD card in the IP camera for the first time, the card is formatted automatically if the card does not have the ext2 file system and if the directory structure that is required for recording is not present on the card. In this case, any data that is on the card is permanently deleted. A card with a storage capacity of 32 GB can take up to 15 minutes to format.
- If you move an SD or MicroSD card from one IP camera to another, the IP camera to which you moved the card does not format the card automatically. This feature allows you to manually recover any video that is stored on the card by downloading the video from the IP camera user interface. You must format the card before you enable recording for it in the new IP camera.
- If you are not using the IP camera with Cisco VSM, set the system time and time zone from the IP camera user interface before you enable recording to an SD or MicroSD card. If you are using the IP camera with Cisco VSM, enable recording through the Cisco VSM user interface, which synchronizes the camera time with the NTP server. Changing the system time after recording starts can cause issues.
- An IP camera has limited bandwidth for simultaneous reading from and writing to an SD or MicroSD card, which can affect the amount of data that you can copy from the card when recording to the card is enabled. For optimum performance of the IP camera, set the maximum bit rate for the recorded stream to 6 Mbps or lower. At higher bit rates, video may not be copied from the card before the video is groomed.
- Recording MJPEG streams to an SD or MicroSD card is not recommended because the relatively high bit rate of these streams can affect system performance. If you do record MJPEG streams, Cisco recommends that you stop recording before you use the IP camera user interface to copy MJPEG recordings from the card.
- The system allows one active download of video from an SD card or MicroSD card at a time. If VSM is copying data from a card (due to a user or system initiated copy operation), you cannot initiate another download from the IP camera user interface until the VSM download completes. Similarly, if you are using the IP camera user interface to download video from a SD or MicroSD card, video cannot be downloaded from VSM until this download completes.

To access the Local Storage window from the IP camera user interface, click the **Setup** link, click **Feature Setup** to expand the menu, then click **Local Storage**.

Table 1 describes updated Local Storage window.

Note To use the features in the Recordings area, ActiveX must be installed on your client PC. If ActiveX is not installed, the Recordings area displays a message with this information. To install ActiveX, see the "Installing ActiveX Client" section on page 13.

Caution To prevent corruption to data on an SD or MicroSD card or the inability of the IP camera to detect the card again, before removing an SD or MicroSD card from an IP camera, stop recording to the card and use the **Unmount** button (described in Table 1) to prepare the card for ejection. In addition, use care when inserting, removing, and handling the card to avoid damaging the card.

Table 1 Local Storage Window

Option	Description
SD/MicroSD Information Area	
Serial Number	*Display only.* Serial number of the SD or MicroSD card that is installed in the IP camera.
Total Size	*Display only.* Total storage capacity in megabytes of the SD or MicroSD card.
Free Space	*Display only.* Free storage space in megabytes of the SD or MicroSD card.
Model	*Display only.* Model number of the SD or MicroSD card.
Manufacturer	*Display only.* Manufacturer of the SD or MicroSD card.
Mount/Unmount (toggle button)	Mount button—When you insert an SD or MicroSD card, the IP camera typically mounts it automatically. If you see a message that indicates that the card is not mounted, click this button to mount it. Unmount button—Click on this button to prepare an SD or MicroSD card for ejection from the IP camera.
Format	Formats an SD or MicroSD card. Use this button to format a card if you switch recording modes or switch the the video stream configuration.
Settings Area	
Enable recording to Local Storage on network loss	This options causes the IP camera to save video recordings to its local SD or MicroSD card if the IP camera looses network connectivity. When the network connectivity is restored, recording to the card stops. This option and the **Enable continuous recording** option cannot be enabled at the same time.
Enable Encryption	Available only if **Enable recording to Local Storage on network loss is** enabled. Check to encrypt video that is recorded to the local SD or MicroSD card during a loss of network connectivity.
Encryption Method	When encryption is enabled, choose one of the following encryption methods: • AES 256 • AES 128 • RC2 64

Table 1 Local Storage Window (continued)

Option	Description
Enable continuous recording	This options causes the IP camera to save video all recordings to its local SD or MicroSD card. This option and the **Enable recording to Local Storage on network loss** option cannot be enabled at the same time.
Continuous recording stream	Choose which video stream is recorded with continuous recording is enabled. Options are: • Stream 1 • Stream 2
Save	Click this button to save changes that you make in the **Settings** area.
Recordings Area (requires a supported version of Microsoft Internet Explorer)	
Recordings list	Displays a list of video recording on the local SD or MicroSD card and the following information and options for each recording: • Select check box. Check the check box next to a recording to select that recording for download or deletion. • Size—Size of the recording in MB. • Name—System-assigned name of the recording. • Start Time (UTC)—Start time of the recording in UTC format. • End Time (UTC)—End time of the recording in UTC format. • Download From (UTC)—To download a recording or part of a recording to your local drive or a network drive, enter the time in UTC format that the video that you want from the recording started. • Duration——To download a recording or part of a recording to your local drive or a network drive, enter the duration of the video that you want from the recording is in hh:mm:ss format. The recording begins from the time that you entered in the Download From field and lasts for the time that you enter in the Duration field. • Progress(%)—The percentage of a video file download operation that has completed. • Status—The status of a video file download or delete operation.
Download	To download a video recording to your local drive or a network drive, check the Select check box for the recording that you went, then click the **Download** button. Follow the on-screen prompts to save the recording. When you save a recording, the system creates a directory called Recordings_*TimeStamp* in the location that you choose and saves recordings in that directory. If the recording that you download contains more than 10 minutes of video, the system divides the recording into separate files that contains 10 minutes of video each. **Note** Network-loss recordings that are created on an IP camera that is running firmware 2.0.1 cannot be downloaded with the 1.4.1 SD utility.

Table 1 Local Storage Window (continued)

Option	Description
Delete	To delete a video recording from the SD or MicroSD card in the IP camera, check the Select check box for the recording that you went, then click the **Delete** button. You can quickly select all video recordings in the list by right-clicking in the Recordings list and then choosing **Select All**.
Refresh	To refresh the list of video recording so that the list shows the latest information about the recordings on the SD or MicroSD card in the IP camera, click the **Refresh** button.
Cancel	This button appears when a video recording is downloading. To cancel the download operation, click the **Cancel** button.

SD or MicroSD Card Health

SD or MicroSD cards can fail. If a card fails, the recordings that it contains can be lost. To protect the data on an SD or MicroSD card, take these actions:

- From the IP camera or Cisco VSM, periodically check the SD or MicroSD card to make sure video is recorded properly.
- Periodically copy the data from an SD or MicroSD card to another storage device. Cisco VSM provides a feature for copying data from and SD or MicroSD card to the VSM storage device.

In the IP camera Alert Notification Screen, you can configure the camera to send an alert notification if the SD or MicroSD card fails.

Custom Apps

Cisco offers an optional software developer kit (SDK) for the IP camera that allows developers to write custom apps and run these apps on supported Cisco IP camera models.

You can upload up to 16 custom apps to an IP camera. Depending on the complexity of an app, you may be able to run multiple apps simultaneously on an IP camera, but you cannot run two audio apps or two video apps at the same time.

Installing Licenses for Custom Apps

The appropriate license should be installed on a camera before the corresponding app package is installed on the camera. To install a license on a camera, follow these steps:

Procedure

Step 1 From the IP camera user interface, click the **Setup** link, click **Application Manager** to expand the menu, then click **App License**.

Step 2 Click **Browse** next to the License file field and navigate to the license file that you downloaded.

Step 3 Select the license file and click **Install License**.

Uploading a Custom App to a Camera

To use a custom app on an IP camera, the packaged app must be uploaded to the IP camera. To upload a custom app, follow these steps:

Procedure

Step 1 From the IP camera user interface, click the **Setup** link, click **Application Manager** to expend the menu, then click **App Setup**.

If you have not yet enabled app support for the camera, a dialog box appears that says "Application support is not enabled on this camera. You will be redirected to Configuration window where you can enable application support on camera."

Step 2 If the Application support dialog box appears, take these actions:

a. Click **OK** to display the Configuration window.

b. In the Configuration window, check the **Enable Application** check box.

c. (Optional) Check the **Enable Video** check box and choose a resolution from the Resolution drop-down list if you will run applications that use the video features of the camera.

d. (Optional) Check the **Enable Audio** check box if you will run applications that use the audio features of the camera.

e. Click **Save**.

f. Choose **App Setup** from the Application Manager drawer.

Step 3 Click **Browse** in the Application Installation area and navigate to the app package that you want to upload.

The app file must have the extension .cpk.

Step 4 Select the app file and click **Open**.

Step 5 Click the **Install** button in the Application Installation area.

A dialog box informs you when the application is installed.

Step 6 (Optional) If you want to enable logging of events that the app sends, take these actions:

a. From the Setup menu in the web-based interface of the camera, choose **Event** from the Feature Setup drawer.

b. Check the **App** check box in the Event Triggering area.

c. Check the **Syslog** check box for the App option in the Event Triggering area.

d. Click **Set All** in the Event Scheduling area.

e. Click **Save** at the bottom of the window.

f. From the Setup menu in the web-based interface of the camera, choose **Setup** from the Log drawer

g. Check the **Enable Syslog** check box in the Syslog Settings area.

h. Enter the IP address of the server on which to log events.

i. Click **Save** at the bottom of the window.

Configuring a Custom App

After you upload a custom app to an IP camera, you must configure its operation.

To configure the operation of a custom app on an IP camera follow these steps:

Procedure

Step 1 From the IP camera user interface, click the **Setup** link, click **Application Manager** to expend the menu, then click **App Setup**.

Step 2 Click the radio button for the custom app that you want to configure.

Step 3 Click the **Configure** button.

Step 4 In the window that appears, make configuration settings as needed and click the **Save** button.

Running a Custom App

To run a custom app on an IP camera, follow these steps:

Procedure

Step 1 From the IP camera user interface, click the **Setup** link, click **Application Manager** to expend the menu, then click **App Setup**.

Step 2 Click the radio button for the custom app that you want to run.

Step 3 Click the **Run** button.

Stopping a Custom App

To stop a custom app that is running on an IP camera, follow these steps:

Procedure

Step 1 From the IP camera user interface, click the **Setup** link, click **Application Manager** to expend the menu, then click **App Setup**.

Step 2 Click the radio button for the custom app that you want to stop.

Step 3 Click the **Stop** button.

Uninstalling a Custom App

To uninstall a custom app from an IP camera, perform the following steps.

If the app is running, you must first stop it as described in the "Stopping a Custom App" section on page 8.

Procedure

Step 1 From the IP camera user interface, click the **Setup** link, click **Application Manager** to expend the menu, then click **App Setup**.

Step 2 Click the radio button for the custom app that you want to uninstall.

Step 3 Click the **Uninstall** button.

Step 4 Click **OK** in the confirmation window that appears.

If you do not want to uninstall the app , click **Cancel**.

Restoring the Application Manager

When you restore the application manager to the factory default condition, all custom apps that you uploaded to the IP camera are removed from the camera.

To restore the application manager on an IP camera, follow these steps:

Procedure

Step 1 From the IP camera user interface, click the **Setup** link, click **Application Manager** to expend the menu, then click **App Setup**.

Step 2 Click the **Restore** button in the Maintenance area.

Step 3 Click **OK** in the confirmation window that appears.

If you do not want to restore the application manager, click **Cancel**.

PTZ Preset Enhancement

The number of presets that the PTZ IP camera supports has been increased from 16 to 100.

Day/Night Mode Optimization

To avoid frequent or unnecessary changes between day mode and night mode, the behavior of the IP camera has been optimized when the Switch Modes is set to **Auto** in the Day Night filter area in the Feature Setup > Camera window. This optimization helps improve performance in situations such as when an IP camera is set up on a street where car headlights cause constant changes between day mode and night mode.

With this optimization, when the IP camera detects that a switch from day to night mode might be necessary, the IP camera monitors the light level for 10 seconds. If the light level remains below or above the configured Day to Night Threshold for the entire 10 seconds, the IP camera switches modes. Otherwise, the IP camera remains in the current mode.

If the IP camera goes through 3 day/night mode transitions within a 60 second period, the camera stops detecting and implementing day/night changes for a period of 5 minutes from the point of the third transition. During these 5 minutes, the IP camera remains in the current day or night mode.

Camera Tamper

The new camera tamper feature lets you configure the IP camera to generate alerts when any of the following events occur and persist for a designated period:

- The IP camera view is changed
- The IP camera view is blocked
- The IP camera view is substantially out of focus

To access the camera tamper options from the IP camera user interface, click the **Setup** link, click **Feature Setup** to expand the menu, then click **Camera**.

The following options are available in the Camera Tamper area. If you change either of these options, click **Save** in the Camera window to save your changes.

- Enable camera tamper detection —Check this check box to enable the camera tamper feature.
- Minimum duration—Enter the minimum length of time that a tamper event persists before a tamper alert is generated. To prevent false alerts, the IP camera waits for this period after detecting a tamper event before it generates an alert. If the tamper event is resolved (the IP camera view is returned to its original setting, the IP camera view blockage is removed, or the IP camera is put back in focus), an alert is not generated. Valid values are 10 to 600 seconds.

PTZ Auto Tracking

The PTZ auto tracking feature lets you configure a PTZ IP camera to automatically track an object that is larger than a configured threshold. When tracking, the IP camera uses its pan and tilt features to keep the object in its field of view.

If there are several objects that are travelling in different direction within the field of view, the IP camera identifies each object that is larger than the configured threshold and tracks the object that is closest to the top left of the field of view.

When you enable PTZ auto tracking on an IP camera, motion detection, if enabled for the camera, is disabled automatically. In this case, motion detection reenables automatically when you disable PTZ auto tracking.

If you change the video resolution for an IP camera when PTZ auto tracking is enabled, the PTZ auto tracking configuration is deleted. In this case, you must reconfigure PTZ auto tracking if you want to continue using the feature .

To access the PTZ auto tracking options from the IP camera user interface, click the **Setup** link, click **Feature Setup** to expand the menu, then click **PTZ Auto Tracking**.

The following options are available in the Auto Tracking area. If you change any of these options, click **Save** in the PTZ Auto Tracking window to save your changes.

- Enable PTZ Auto Tracking—Check this check box to enable the PTZ auto tracking feature.
- Sensitivity—Drag the slider to designate the relative amount of activity that the IP camera must detect in the field of view before it start tracking an object. Move the slider to the left to designate less activity or to the right to designate more activity.
- Threshold—Drag the slider to designate the percentage of pixels that the IP camera must identify as changed in the field of view before it starts tracking. Move the slider to the left to designate fewer pixels or to the right to designate more pixels.

Expanded Browser Support

This release adds support for the following features through Chrome and Firefox on Windows, and through Chrome, Firefox, and Safari on the Mac. These features are in "Beta" on these browsers for this release to get feedback about the platforms and browsers are most important to users.

When you use one of these browsers, you can view video from the IP camera by using either the VLC Media Player or the QuickTime plugin.

- Log in
- Network Setup > Basic window
- Network Setup >IP Addressing window
- View Video window
- Home window

To access other IP camera features, use a supported version of Microsoft Internet Explorer.

Important Notes

- To ensure that the new features display, clear the browser cache and reload the web page.
- 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 2.0.2

If your IP camera has an earlier firmware release, you can upgrade it to firmware release 2.0.2 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 2.0.2 by performing the following steps.

Note Upgrading to 2.0.1 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 2.0.2 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 **2.0.2** release.

d. Download the 2.0.2 firmware with the file name that applies to your IP camera:

- For 2830 and 2835 PTZ IP cameras: CIVS-IPC-283x-V2.0.2-24.bin
- For 3000 series IP cameras: CIVS-IPC-3xxx-V2.0.2-24.bin
- For 3535 IP camera: CIVS-IPC-3535-V2.0.2-24.bin
- For 6000 series IP cameras: CIVS-IPC-6xxx-V2.0.2-24.bin
- For 6930 PTZ IP camera: CIVS-IPC-6930-V2.0.2-24.bin
- For 7000 series IP cameras: CIVS-IPC-7xxx-V2.0.2-24.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 2.0.2 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.

Installing ActiveX Client

The following sections provide information about installing the ActiveX client:

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 2.0.2 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 Cisco IPICS 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 know 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 config change may take up to 5 minutes before streaming start
CSCui23498	283x/3xxx/6xxx/6930/7xxx: Camera does not send Cold Start SNMP trap
CSCui95069	283x/3xxx/6xxx/6930/7xxx: 802.1x does not work after certificate change

Resolved Caveats

Table 3 describes the know caveats that are resolved in this release.

Table 3 Caveats Resolved in this Release

Identifier	Description
CSCud42131	VSMS IP addresses are not cleared when Preferred MS list is disabled
CSCug04204	283x/3xxx/6xxx/6930/7xxx: Email notification not received if SMTP requires authentication
CSCug60062	6930: Exposure time option may get disabled sometimes
CSCuj67246	Device name is set to default after reboot
CSCun69551	PTZ camera reboots every 3 minutes with new SD card
CSCun69557	Webserver response is slow if the camera is configured with wrong DNS
CSCun71993	Applications may not start automatically after reboot
CSCun72219	Storage Recordings may show incorrect time
CSCuo37282	Multiple Video Surveillance cameras are vulnerable to CVE-2014-0160

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 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 Unable to install ActiveX or view streaming video because of an existing version.

- 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 2.0.2.

Table 4 shows the supported and unsupported MIBs.

Table 4 MIB Support in Release 2.0.2

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

Table 4 MIB Support in Release 2.0.2 (continued)

MIBs	RFC	Support
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.