



## **Cisco Video Surveillance 7000 Series IP Camera Configuration Guide**

Release 2.0.0

### **Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

Text Part Number: OL-32287-01

NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://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. (1110R)

*Cisco Video Surveillance 7000 Series IP Camera Configuration Guide, Release 2.0.0*  
Copyright © 2014 Cisco Systems, Inc. All rights reserved.



# Preface

---

## Overview

This document, *Cisco Video Surveillance 7000 Series IP Camera Configuration Guide*, provides information about installing and deploying the Cisco Video Surveillance 7000 Series IP Cameras.

## Organization

This manual is organized as follows:

<a href="#">Chapter 1, “Overview”</a>	Provides information about the IP camera features, instructions for accessing the user interface, and information about the user interface.
<a href="#">Chapter 2, “Performing the Initial Setup of the IP Camera”</a>	Provides information and instructions about performing the initial setup of the IP camera.
<a href="#">Chapter 3, “Viewing Live Video”</a>	Provides information and instructions about viewing live video.
<a href="#">Chapter 4, “Feature Setup”</a>	Provides information and instructions for configuring IP camera features, such as streaming, camera capabilities, video overlay, I/O ports, and events.
<a href="#">Chapter 5, “Network Setup”</a>	Provides information and instructions for configuring network settings, such as IP addressing, time, discovery, IP filtering, and quality of service (QoS).
<a href="#">Chapter 6, “Application Manager”</a>	Provides information and instructions about using apps with the IP camera
<a href="#">Chapter 7, “Administration”</a>	Provides information and instructions for performing administrative tasks, such as IP camera initialization, user management, maintenance, firmware upgrade, device processes management, and password complexity.
<a href="#">Chapter 8, “Log Configuration”</a>	Provides information and instructions for configuring and viewing logs.

## Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: <http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html>.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.



# CHAPTER 1

## Overview

---

This chapter provides information about the Cisco Video Surveillance 7000 Series IP camera features, instructions for accessing the user interface, and information about the user interface. It includes the following topics:

- [IP Camera Features, page 1-1](#)
- [Accessing the IP Camera, page 1-2](#)
- [Understanding the IP Camera User Interface, page 1-4](#)

## IP Camera Features

The Cisco Video Surveillance 7000 Series IP cameras offer a feature-rich digital camera solution for a video surveillance system. The cameras provide high-definition (HD) video and simultaneous H.264 and MJPEG compression, streaming up to 30 frames per second (fps) at 1080p (up to 2560 x 1920) resolution.

In addition, the 7000 Series IP cameras provide networking and security capabilities, including multicast support, hardware-based Advanced Encryption Standard (AES), and hardware-based Data Encryption Standard/Triple Data Encryption Standard (DES/3DES) encryption. The cameras can be powered through an external power supply or by integrated Power over Ethernet (PoE).

The 7000 Series IP cameras include the following key features:

- **H.264 and MJPEG compression**—The IP camera can generate H.264 and MJPEG streams simultaneously.
- **Privacy regions**—Up to four user-defined masking zones can be used to provide regions of privacy in the camera field of view. Video within privacy regions is not recorded in the camera, nor sent in the video stream.
- **Progressive scan video**—The IP camera captures each frame at its entire resolution using progressive scan rather than interlaced video capture, which captures each field of video.
- **Analog video output**—Supports analog video for all resolutions with 15 fps or lower with no secondary stream.
- **Medianet**—The IP camera supports the Auto Smartports feature of the Media Services Interface (MSI). MSI enables a camera to participate as an endpoint in the Cisco medianet architecture when connected to a medianet enabled switch.
- **Local Storage**—Supports up to 32 GB of video data storage on a micro SD memory card when the camera loses network connectivity.

- **Two-way audio communication**—Audio can be encoded with the video. With the internal or optional external microphone and optional external speaker, you can communicate with people at the IP camera location while you are in a remote location and viewing images from the IP camera.
- **Day/night switch support**—An IR-cut filter provides increased sensitivity in low-light conditions.
- **Multi-protocol support**—Supports these protocols: DHCP, HTTP, HTTPS, NTP, RTP, RTSP, SMTP, SSL/TLS, and TCP/IP.
- **Web-based management**—You perform ongoing administration and management of the IP camera through web-based configuration menus.
- **Remote Focus/Zoom Control**—Built-in stepping motors allow you to remotely adjust the IP camera focal length and zoom factor.
- **Motion detection**—The IP camera can detect motion in user-designated fields of view by analyzing changes in pixels and generate an alert if motion is detected.
- **Flexible scheduling**—You can configure the IP camera to respond to events that occur within a designated schedule.
- **Syslog support**—The IP camera can send log data to a Syslog server.
- **IP address filter**—You can designate IP addresses that can access the IP camera and IP addresses that cannot access the IP camera.
- **User-definable HTTP/ HTTPS port number**—Allows you to define the port that is used to connect to the camera through the Internet.
- **DHCP support**—The IP camera can automatically obtain its IP addresses in a network in which DHCP is enabled.
- **Network Time Protocol (NTP) support**—Allows the IP camera to calibrate its internal clock with a local or Internet time server.
- **Support for C and CS mount lenses**—The IP camera supports a variety of C and CS mount lenses.
- **Power options**—The IP camera can be powered with 24 volts AC, which is provided through an optional external power adapter, or through PoE (802.3af), which is provided through a supported switch.
- **Camera access control**—You can control access to IP camera configuration windows and live video by configuring various user types and log in credentials.
- **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:
  - Device Discovery Service
  - Device Service
  - Media Service
- **Apps**—You can extend the functionality of a supported Cisco IP Camera by uploading and running an app on the camera.

## Accessing the IP Camera

After you perform the initial configuration as described in [Chapter 2, “Performing the Initial Setup of the IP Camera,”](#) follow the steps in this section each time that you want to access the IP camera windows to make configuration settings, view live video, or perform other activities.

You access these windows by connecting to the IP camera from any PC that is on the same network as the IP camera and that meets these requirements:

- Operating system—Microsoft Windows 7 (32-bit or 64-bit)
- Browser—Internet Explorer 9.0 (32-bit only)

You need this information to access the IP camera windows:

- IP address of the IP camera. By default, the IP camera attempts to obtain an IP address from a DHCP server in your network. If the IP camera cannot obtain an IP address through DHCP within 90 seconds of powering up or resetting, it uses the default IP address of 192.168.0.100.
- Port number, if other than the default value. Default port numbers for the IP camera are 443 for HTTPS and 80 for HTTP. The IP camera administrator can configure an HTTPS port and an HTTP port as described in the [“Initialization Window” section on page 7-1](#).
- Your user name and password for the IP camera. The IP camera administrator configures user names and passwords as described in the [“User Window” section on page 7-3](#).

To access the IP camera windows, perform these steps.

### Before you Begin

Microsoft .NET Framework version 2.0 or later must be installed on the PC that you use to connect to the IP camera. You can download the .NET Framework from the Microsoft website.

### Procedure

**Step 1** Start Internet Explorer, and enter the following in the address field:

***protocol://ip\_address:port\_number***

where:

- *protocol* is **HTTPS** for a secure connection or **HTTP** for a non-secure connection. You can use HTTP only if you configure the camera to accept non-secure HTTP connections as described in [Chapter 2, “Performing the Initial Setup of the IP Camera.”](#)
- *ip\_address* is the IP address of the IP camera. The default IP address is 192.168.0.100.
- *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.

For example,

- Enter the following for a secure connection if the IP address is 192.168.0.100 and the HTTPS port number is 443:  
**https://192.168.0.100**
- Enter the following for a secure connection if the IP address is 203.70.212.52 and the HTTPS port number is 1024:  
**https://203.70.212.52:1024**
- Enter the following for a non-secure connection if the IP address is 203.70.212.52 and the HTTP port number is 80:  
**http://203.70.212.52**
- Enter the following for a non-secure connection if the IP address is 203.70.212.52 and the HTTP port number is 1024:

**http://203.70.212.52:1024**

**Step 2** Enter your IP camera user name and password in the Username and Password fields, then click **Login**.

To log in as the IP camera administrator, enter the user name **admin** (which is case sensitive) and the password that is configured for the administrator. To log in as a user, enter the user name and password that are configured for the user.

The Home window for the IP Camera appears.

---

## Understanding the IP Camera User Interface

After you log in to the IP camera, you can access the IP camera windows and perform a variety of administrative and user procedures.

The links and activities that you can see and access in the IP camera windows depend on your IP camera privilege level. Privilege levels are configured as described in the “[User Window](#)” section on page 7-3 and include the following:

- Administrator—Can access all IP camera windows, features, and functions.
- Viewer—Can access the Camera Video & Control window with limited controls, and can access the **Refresh**, **Logout**, **About**, and **Help** links from that window.

## IP Camera Window Links

The IP Camera user interface includes links that you use to access various windows and perform other activities. [Table 1-1](#) describes each link and lists the IP camera privilege level that you must have to access the link.

**Table 1-1** *Links in the IP Camera Windows*

Link	Description	Privilege Level
<b>Refresh</b>	Updates the information in the window that is currently displayed.	Administrator User
<b>Home</b>	Displays the System Information window. For more information, see <a href="#">Table 1-2</a> .	Administrator
<b>View Video</b>	Displays the Camera Video & Control window.  You may be prompted to install ActiveX controls when trying to access this window for the first time. ActiveX controls are required to view video from the IP camera. Follow the on-screen prompts to install ActiveX controls.	Administrator User
<b>Setup</b>	Displays the Setup window and provides access to the configuration menus for the IP camera.	Administrator
<b>Logout</b>	Logs you out from the IP camera.	Administrator User



**Table 1-1** *Links in the IP Camera Windows (continued)*

Link	Description	Privilege Level
About	Displays a pop-up window with model, version, and copyright information for the IP camera.	Administrator User
Help	Displays reference information for the window that is currently displayed.	Administrator User

## IP Camera Windows

The IP camera user interface includes these main windows:

- System Information window—Accessed by clicking the Home link. Displays the information that is described in [Table 1-2](#).
- Camera Video & Control window—Accessed by clicking the View Video link. Displays live video from the camera and lets you control a variety of camera and display functions. For detailed information, see [Chapter 3, “Viewing Live Video.”](#)
- Setup window—Accessed by clicking the Setup link. Provides access to the IP camera configuration windows. For detailed information, see the following chapters:
  - [Chapter 4, “Feature Setup.”](#)
  - [Chapter 5, “Network Setup.”](#)
  - [Chapter 7, “Administration.”](#)
  - [Chapter 8, “Log Configuration.”](#)

**Table 1-2** *System Information Window*

Field	Description
<b>General Information</b>	
ID	Identifier of the IP camera. To configure the ID, see the <a href="#">“Basic Window” section on page 5-1</a> .
Name	Name of the IP camera. To configure the name, see the <a href="#">“Basic Window” section on page 5-1</a> .
Current Time	Current date and time of the IP camera. To set the date and time, see the <a href="#">“Time Window” section on page 5-5</a> .
S/N	Serial number of the IP camera.
Firmware	Version of the firmware that is installed on the IP camera.
Part Number	Cisco manufacturing part number of the IP camera.
Top Assembly Revision	Cisco assembly revision number.
<b>Network Status</b>	
MAC Address	MAC address of the IP camera.
Configuration Type	Method by which the IP camera obtains its IP address. To configure this method, see the <a href="#">“IP Addressing Window” section on page 5-3</a> .
LAN IP	IP address of the LAN to which the IP camera is connected. To configure this IP address, see the <a href="#">“IP Addressing Window” section on page 5-3</a> .

**Table 1-2**      **System Information Window (continued)**

Field	Description
Subnet Mask	Subnet mask of the LAN to which the IP camera is connected. To configure the subnet mask, see the <a href="#">“IP Addressing Window” section on page 5-3</a> .
Gateway Address	IP address of the gateway through which the IP camera is connected. To configure this IP address, see the <a href="#">“IP Addressing Window” section on page 5-3</a> .
Primary DNS	IP address of the primary DNS server, if configured for the IP camera. To configure a primary DNS server, see the <a href="#">“IP Addressing Window” section on page 5-3</a> .
Secondary DNS	IP address of the secondary DNS server, if configured for the IP camera. To configure a secondary DNS server, see the <a href="#">“IP Addressing Window” section on page 5-3</a> .
<b>IO Port Status</b>	
Input Port	Current state of the three input ports on the IP camera. To configure an input port, see the <a href="#">“IO Ports Window” section on page 4-17</a> .
Output Port	Current state of the output port on the IP camera. To configure an output port, see the <a href="#">“IO Ports Window” section on page 4-17</a> .
<b>Stream 1 and Stream 2</b>	
User	<p>IP camera user name of each user who is accessing the primary video stream (Stream 1) or the secondary video stream (Stream 2) through a client PC or a third-party device.</p> <p>By default, users appear in order of start time. To display users in ascending order of any information in any corresponding column, click the column heading. Click a column heading again to reverse the display order.</p>
IP Address	IP address of the client device.
Start Time	Time and date that the client accessed the video stream for this session.
Elapsed Time	Length of time that the client has been accessing the video stream.
Codec	Video codec (H.264 or MJPEG) being used for the stream.



## Performing the Initial Setup of the IP Camera

After you install the IP camera, or after you perform a factory reset procedure, you must access the IP camera and make initial configuration settings. These settings include administrator and root passwords, and whether the IP camera can be accessed through an HTTP connection in addition to the default HTTPS (HTTP secure) connection.

To make these configuration settings, you connect to the IP camera from any PC that is on the same network as the IP camera. The PC must meet these requirements:

- Operating system—Microsoft Windows 7 Enterprise (32-bit or 64-bit)
- Browser—Internet Explorer 8.0 (32-bit only)

In addition, you must know the IP address and default login credentials of the IP camera. By default, when the IP camera powers on, it attempts to obtain an IP address from a DHCP server in your network. If the camera cannot obtain an IP address through DHCP within 90 seconds, it uses a default IP address of 192.168.0.100. The default login credentials (Username/Password) are admin/admin.

To connect to the IP camera for the first time and make initial configuration settings, perform the following steps. You can change these configuration settings in the future as described in the *Cisco Video Surveillance 7000 Series IP Camera Configuration Guide*.

### Before you Begin

The Microsoft .NET Framework version 2.0 or later must be installed on the PC that you use to connect to the IP camera. You can download the .NET Framework from the Microsoft website.

### Procedure

- 
- Step 1** Start Internet Explorer, enter **HTTPS://ip\_address** in the address field, and press **Enter**.  
Replace *ip\_address* with the IP address that the IP camera obtained through DHCP or, if the camera was unable to obtain this IP address, enter **192.168.0.100**.  
The Login window appears.
- Step 2** Enter the default login credentials:  
Username: **admin**  
Password: **admin**  
The Initialization window appears.

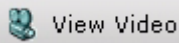
- Step 3** In the Password and Confirm Password fields of the admin row, enter a password for the IP camera administrator.
- You must enter the same password in both fields. The password is case sensitive and must contain at least eight characters, which can be letters, numbers, and special characters, but no spaces. Special characters are: ! " # \$ % & ' ( ) \* + , - . : ; < = > ? @ [ \ ] ^ \_ ` { | } ~.
- Step 4** In the Password and Confirm Password fields of the Root row, enter a password that is used when accessing the IP camera through a Secure Shell (SSH) connection.
- You must enter the same password in both fields. The password is case sensitive and must contain at least eight characters, which can be letters, numbers, and special characters, but no spaces. Special characters are: ! " # \$ % & ' ( ) \* + , - . : ; < = > ? @ [ \ ] ^ \_ ` { | } ~.
- You use the root password if you need to troubleshoot the IP camera through a SSH connection with the assistance of the Cisco Technical Assistance Center.
- Step 5** In the Access Protocols area, check the **Enable HTTP** check box if you want to allow both HTTP and HTTPS connections to the IP camera.
- By default, only the Enable HTTPS check box is checked, which allows only HTTPS (secure) connections to the IP camera.
- Step 6** Click **Apply**.
- The IP camera reboots and the Login window appears.
- Step 7** After the IP camera reboots, start Internet Explorer and, in the Address field, enter the following:  
*protocol://ip\_address*  
 where:
- *protocol* is **HTTPS** or **HTTP**. (You can use HTTP only if you enabled it in [Step 5](#).)
  - *ip\_address* is the IP address that you used in [Step 1](#).
- Step 8** If you are prompted to install ActiveX controls, which are required to view video from the IP camera, follow the on-screen prompts to do so.
- The Home window appears.
-



## Viewing Live Video

After you install and set up the Cisco Video Surveillance IP Camera, you can connect to the IP camera through Internet Explorer and access the Camera Video & Control window to view live video from the IP camera.

The Camera Video & Control window also provides for controlling the video display, configuring preset positions, and controlling certain IP camera functions. Available controls depend on the privilege level of the user.



To view live video, log in to the IP camera and click **View Video** in the IP camera Main window menu bar. The Camera Video & Control window appears. This window displays live video from the camera and lets you control a variety of camera and display functions.

The controls that you see in the Camera Video & Control window depend on your IP camera privilege level and the configurations settings for the IP camera. Users with the Administrator privilege can access all controls. Users with the Viewer privilege do not have access to the following controls:

- Video Control
- Camera Settings
- Motion Detection
- Focus/Zoom controls
- Privacy Zone

Table 3-1 describes the controls in the Camera Video & Control window.

**Table 3-1** Camera Video & Control Window Controls

Control	Description
<b>Video Control</b>	
Video Codec drop-down list Pri. H.264 ▾	Choose the codec for video transmission (H.264 or MJPEG).
Video Resolution display 2560x1920 ▾	Displays the resolution for video transmission. The resolutions in this depends on the video standard that you selected.

Table 3-1 Camera Video &amp; Control Window Controls (continued)








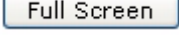









Control	Description
<b>Viewer</b>	
Video viewer drop-down list 	Choose the viewer to use for video. Options are: <ul style="list-style-type: none"> <li>• <b>ActiveX</b>—Available only if you are using accessing the IP camera through Microsoft Internet Explorer. Allows you to configure several IP camera options, such as motion detection and privacy zone.</li> <li>• <b>QuickTime</b>—Allows viewing of H.264 streams only. Does not allow you to configure several IP camera options, such as motion detection and privacy zone.</li> <li>• <b>VLC</b>—Allows viewing of H.264 and MJPEG streams. Does not allow you to configure several IP camera options, such as motion detection and privacy zone.</li> </ul> The default video viewer value is ActiveX.
<b>Image tools</b>	
<b>Hotspot Zoom</b> button 	Click this latch button to enables the digital zoom feature, which provides five-step digital zooming in for the normal (not full screen) video display. Click this button again to disable the digital zoom feature.  To perform a digital zoom, engage the <b>Hotspot Zoom</b> button and click the video display. The first five clicks zoom the display. The sixth click returns to unzoomed display.
<b>Hotspot Pan+Tilt</b> button 	Not supported.
<b>Save Snapshot</b> button 	Captures and saves a the current video image as a .gif file or a .jpg file in the location of your choice and with the file name of your choice.  When you click this button, the Snapshot window appears. Click <b>Save</b> and follow the on-screen prompts to save the image with the name and in the location that you want.
<b>Flip</b> button 	Rotates the video image by 180 degrees.
<b>Mirror</b> button 	Reverses the video image.
<b>Restore</b> button 	Displays the default video image, which is not rotated and not reversed.
<b>Full Screen</b> button 	Displays the video image in full screen mode.  To return to normal display mode, click the full screen image.

Table 3-1 Camera Video &amp; Control Window Controls (continued)

Control	Description
<b>Audio Control</b>	
<b>Enable/Disable Speaker toggle button</b>	<p>Click the <b>Disable Speaker</b> button  to mute audio that is sent from the IP camera to the PC that you are using. The button changes to the Enable Speaker button .</p> <p>Click the <b>Enable Speaker</b> button to unmute audio. The button changes to the Disable button.</p>
<b>Mute/Un-Mute Microphone toggle button</b>	<p>Click the <b>Mute Microphone</b> button  to mute the audio stream that is captured and sent to the IP camera from the internal or external microphone of the PC that you are using. When you click this button, the speaker that is attached to the IP camera does not play audio that is transmitted from your PC.</p> <p><b>Note</b> If you are simultaneously accessing other IP cameras in different browser sessions on the same PC, clicking this button in one browser session does not mute the audio that the PC sends to the other IP cameras.</p> <p>When you click the Mute Microphone button, it changes to the Un-Mute Microphone button .</p> <p>Click the <b>Un-Mute Microphone</b> button to unmute audio that is sent to the IP camera. The button changes to the Mute Microphone button.</p>
<b>Restore button</b> 	Resets audio controls to their default values.
<b>Speaker Volume slider</b> 	<p>When the speaker is unmuted, drag this slider to adjust the volume at which your PC speakers play the audio from the IP camera, or enter a value from 0 through 100 in the field and press the Enter key.</p> <p>The default value is 50.</p>
<b>Microphone Sensitivity slider</b> 	<p>Drag this slider to adjust the gain of the PC microphone (that is, how sensitive it is to the audio that it picks up and that is sent to the IP camera), or enter a value from 0 through 100 in the field and press the Enter key.</p> <p>The default value is 50.</p>

**Table 3-1 Camera Video & Control Window Controls (continued)**

Control	Description
<b>Camera Settings controls</b>	
<b>Note</b>	To display these controls click the Expand icon  next to Camera Settings under the video image. The icon changes to the Collapse icon  . Click the Collapse icon to hide these controls.  If you make changes to any of the Camera Settings options, click the <b>Save</b> button to save the changes.
<b>Picture Adjustments</b>	
Brightness slider	To control the brightness of the video image, drag the slider to select a value from 1 through 10. A higher value increases the brightness and a lower value decreases the brightness. For example, if the IP camera is facing a bright light and the video appears too dark, you can increase the brightness.  The default value is 5.
Contrast slider	To control contrast of the video image, drag the slider to select a value from 1 through 10. A higher value increases the contrast and a lower value decreases the contrast.  The default value is 5.
Sharpness slider	To control the sharpness of the video from the IP camera, drag the slider to select a value from 1 through 100. A higher value increases the sharpness and a lower value decreases the sharpness.  The default value is 50.
Saturation slider	To control the saturation of the video from the IP camera, drag the slider to select a value from 1 through 10. A higher value increases the saturation and a lower value decreases the saturation.  High saturation provides a vivid, intense color for a video image. With less saturation, the video image appears more muted and gray.  The default value is 50.
<b>Restore</b> button	Resets brightness, contrast, sharpness, and saturation to their default values.
White Balance Mode drop-down menu	Choose one the following white balance modes: <ul style="list-style-type: none"> <li>• <b>Auto</b>—White balance automatically set by camera and suitable for most conditions.</li> <li>• <b>Manual</b>—Choose this option if you want to set the white balance by setting RGain (Red Gain) and BGain (Blue Gain) manually.</li> </ul> The default setting is Auto.
<b>Exposure Control</b>	
Exposure level drop-down menu	Choose a value to increase or decrease the exposure level of the video image.  The default value is 0.0.
Exposure mode drop-down menu	Choose one of these options: <ul style="list-style-type: none"> <li>• <b>Manual</b>—Choose this option if you want to set Exposure time and Gain control manually.</li> <li>• <b>Auto</b> —Suitable for most conditions.</li> </ul> The default setting is Auto.



**Table 3-1 Camera Video & Control Window Controls (continued)**

Control	Description
Flickerless check box	<p>Appears when you choose <b>Manual</b> from the Exposure mode drop-down menu.</p> <p>Flickering can occur when a combination of indoor and outdoor light get to the IP camera, due to a difference in capture frequency and actual indoor lighting frequency. Check this check box to limit the range of exposure time, which prevents flickering.</p>
Exposure time slider	<p>Appears when you choose <b>Manual</b> from the Exposure mode drop-down menu.</p> <p>To control the minimum length of time in seconds that the IP camera keeps its iris open for each frame, drag the left slider box. To control the maximum length of time in seconds that the IP camera keeps its iris open for each frame, drag the right slider box.</p> <p>When capturing video, the IP camera automatically selects the optimum value between the minimum and maximum values that you configure.</p> <p>If the Flickerless check box is not checked, the minimum exposure value is 1/32000 and the maximum value is 1/5. If the Flickerless check box is checked, the minimum exposure value is 1/120 and the maximum value is 1/5.</p>
Gain control slider	<p>Appears when you choose <b>Manual</b> from the Exposure mode drop-down menu.</p> <p>To control the minimum gain of the IP camera, drag the left slider box. To control the maximum gain, drag the right slider box. A value of 0 does not boost the gain, so the image may appear darker in a darker environment. A higher value increases the exposure of the image, which can cause the image to look brighter, but can also cause the image to appear more noisy.</p> <p>When capturing video, the IP camera automatically selects the optimum value between the minimum and maximum values that you configure.</p>
Iris mode drop down menu	<p>Appears only when you choose <b>Auto</b> from the Exposure mode drop-down menu. Choose one of these options for the IP camera iris:</p> <ul style="list-style-type: none"> <li>• <b>Indoor</b>—Suitable for indoor conditions</li> <li>• <b>Outdoor</b>—Suitable for outdoor conditions</li> </ul>

**Table 3-1 Camera Video & Control Window Controls (continued)**

Control	Description
Measurement Window	<p>Choose one of the following options to control how the IP camera calculates exposure:</p> <ul style="list-style-type: none"> <li>• <b>Full View</b>—The entire IP camera image is considered for the exposure calculation.</li> <li>• <b>Custom</b>—Lets you draw up to 4 Inclusion regions and up to 4 Exclusion regions for the exposure calculation.</li> </ul> <p>To designate regions, right-click the video image, choose <b>Draw Region</b>, then hold down the left mouse button and draw the region, which is indicated by a green rectangle.</p> <p>A region is an Inclusion region by default.</p> <p>To move a region, left-click it and drag its window to the desired area.</p> <p>To resize a region, left-click it and drag a box in the edge or corner of the region.</p> <p>To remove a region, left-click it, then right-click it and choose <b>Delete Region</b>.</p> <ul style="list-style-type: none"> <li>• <b>BLC</b>—Back Light Compensation causes only the middle part of the IP camera image, indicated by a white dashed rectangle, to be considered for the exposure calculation.</li> </ul>
Region Properties	<p>Appears when you click a custom region that you created.</p> <p>To expand region properties information, click the + icon next to <b>Region Properties</b>. The icon changes to a – icon, which you click to collapse region properties information.</p> <ul style="list-style-type: none"> <li>• <b>Location</b>—X and Y coordinates, respectively, of the top left corner of the selected custom region. To expand location information, click the + icon next to <b>Location</b>. The icon changes to a – icon, which you click to collapse region location information.</li> <li>• <b>Region Type</b>—Type of the region (Inclusion or Exclusion). To change the region type, left-click that region, click <b>Region Type</b>, then choose one of the following values from the drop-down menu that appears on the Region Type line. Alternatively, you can double-click <b>Inclusion</b> or <b>Exclusion</b> to toggle between these values. <ul style="list-style-type: none"> <li>– <b>Inclusion</b>—The region is used to calculate the exposure value</li> <li>– <b>Exclusion</b>—The region is ignored in the exposure value calculation</li> </ul> </li> </ul>
<b>Advanced Settings</b>	
Enable Low Light Compensation check box	In a low-light environment, check this check box to reduce noise in the video image.
Enable DRX check box	In situations in which there is significant contrast between light and dark parts of an image, check this check box to cause the IP camera to continually adjust the image for optimal appearance.

**Table 3-1 Camera Video & Control Window Controls (continued)**

Control	Description
Sensitivity drop-down menu	Appears when you check the Enable DRX check box. Choose <b>Low</b> or <b>High</b> to specify how quickly the IP camera adjusts the image for optimal appearance.
Strength drop-down menu	Appears when you check the Enable DRX check box. Choose <b>Low</b> , <b>Medium</b> , or <b>High</b> to specify the relative adjustment that the IP camera makes between the light and dark parts of an image.
Gamma Curve	Select a gamma curve value to adjust the monitor gray-scale for video from the IP camera.



**Motion Detection**

**Note** To display these controls click the Expand icon  next to Motion Detection under the video image. The icon changes to the Collapse icon . Click the Collapse icon to hide these controls.

If you make changes to any of the Motion Detection options, click the **Save** button to save the changes.

<b>Enable Motion Detection</b> check box	<p>Enables the motion detection feature.</p> <p>When motion detection is enabled, the IP camera monitors activity in the video field areas that you specify. If activity at a defined level occurs in any of these areas, the IP camera generates an alert and takes the configured actions.</p> <p>To designate regions, right-click the video image, choose <b>Draw Region</b>, then hold down the left mouse button and draw the region, which is indicated by a green rectangle (for an inclusion region) or a red rectangle (for an exclusion region).</p> <p>You can draw up to 4 Inclusion regions and up to 4 Exclusion regions for a total of up to 8 regions.</p> <p>To move a region, left-click it and drag its window to the desired area.</p> <p>To resize a region, left-click it and drag a box in the edge or corner of the region.</p> <p>To remove a region, left-click it, then right-click it and choose <b>Delete Region</b>.</p>
------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------



**Table 3-1** Camera Video & Control Window Controls (continued)

Control	Description
Region Properties	<p>To expand region properties information, click the + icon next to <b>Region Properties</b>. The icon changes to a – icon, which you click to collapse region properties information.</p> <ul style="list-style-type: none"> <li>• <b>IsActive</b>—To indicate whether the IP camera monitors a region for motion detection, left-click that region, click <b>IsActive</b>, then choose <b>True</b> (consider region) or <b>False</b> (do not consider region) from the drop-down menu that appears on the IsActive line. Alternatively, you can double-click <b>True</b> or <b>False</b> to toggle between these values.</li> <li>• <b>Location</b>—X and Y coordinates, respectively, of the top left corner of the selected custom region. To expand location information, click the + icon next to <b>Location</b>. The icon changes to a – icon, which you click to collapse region location information.</li> <li>• <b>Name</b>—Name of the region. By default, the system assigns the name RegionX, where X is a number 1 through 8. To rename a region, click its name (which appears in bold type on this line) and type a unique name of up to 32 characters.</li> <li>• <b>Region Type</b>—Type of the region. To change the region type, left-click that region, click <b>Region Type</b>, then choose one of the following values from the drop-down menu that appears on the Region Type line. Alternatively, you can double-click <b>Inclusion</b> or <b>Exclusion</b> to toggle between these values. <ul style="list-style-type: none"> <li>– <b>Inclusion</b>—The IP camera examines this region for motion</li> <li>– <b>Exclusion</b>—The IP camera ignores motion in this area</li> </ul> </li> </ul>
Sensitivity slider	<p>Becomes available when you left-click a motion detection region.</p> <p>Designates the relative amount of activity that the IP camera must detect in the area before it generates an alert. A lower value means that more, or faster, activity is required to trigger an alert. A higher value means that less, or slower, activity is required. The default value is 80.</p>
Threshold slider	<p>Becomes available when you left-click a motion detection region.</p> <p>Designates the percentage of pixels that the IP camera must identify as changed in the area before it generates an alert. The camera monitors for pixel changes at the defined sensitivity level. The default threshold value is Low.</p>
<b>Focus/Zoom</b>	
<p><b>Note</b> To display these controls click the Expand icon  next to Focus/Zoom under the video image. The icon changes to the Collapse icon . Click the Collapse icon to hide these controls.</p>	
Zoom slider	<p>Drag to the right to increase the zoom level of the video image (tele) and drag to the left to decrease the zoom level (wide). You also can use these buttons to adjust the zoom level:</p> <ul style="list-style-type: none"> <li>• <b>–10</b>—Decreases the zoom level by 10 steps</li> <li>• <b>–1</b>—Decreases the zoom level by 1 step</li> <li>• <b>+1</b>—Increases the zoom level by 1 step</li> <li>• <b>+10</b>—Increases the zoom level by 10 steps</li> </ul>

**Table 3-1 Camera Video & Control Window Controls (continued)**

<b>Control</b>	<b>Description</b>
Focus slider	<p>Drag to the right sharpen the focus on objects that are farther away from the camera and drag to the left to sharpen the focus on objects that are nearer. You also can use these buttons to adjust the focus:</p> <ul style="list-style-type: none"> <li>• <b>-10</b>—Decreases the focus by 10 steps</li> <li>• <b>-1</b>—Decreases the focus by 1 step</li> <li>• <b>+1</b>—Increases the focus by 1 step</li> <li>• <b>+10</b>—Increases the focus by 10 step</li> </ul>
<b>Auto Focus</b> button	<p>Click to have the IP camera automatically adjust its focus. This adjustment uses larger steps than the full auto focus feature (see the “<a href="#">Full Auto Focus button</a>” row in this table), but takes less time to complete than a full auto focus.</p> <p>The auto focus process can take a few minutes to complete, and the Focus/Zoom controls are dimmed during this process. When the process completes, click <b>OK</b> in the dialog box that displays the message “Set Auto Focus successfully.”</p>
<b>Reset</b> button	<p>Click to set the zoom and focus controls to their default values. When the process completes, click <b>OK</b> in the dialog box that displays the message “Settings reset successfully.”</p>
<b>Specify Region</b> check box	<p>To automatically adjust the focus with priority given to a particular region in the field of view:</p> <ol style="list-style-type: none"> <li>1. Check the <b>Specify Region</b> check box.</li> <li>2. Right-click the video image and choose <b>Draw Region</b>.</li> <li>3. Hold down the left mouse button and draw the region, which is indicated by a green rectangle.</li> </ol> <p>To move a region, left-click it and drag its window to the desired area.</p> <p>To resize a region, left-click it and drag a box in the edge or corner of the region.</p> <p>To remove a region, uncheck the <b>Specify Region</b> check box.</p>
<b>Full Auto Focus</b> button	<p>Click to have the IP camera automatically adjust its focus. This adjustment uses smaller steps than the auto focus feature (see the “<a href="#">Auto Focus button</a>” row in this table), but can result in a sharper focus and takes more time to complete than an auto focus.</p> <p>The full auto focus process can take some time, and the Focus/Zoom controls are dimmed during this process. If you see a dialog with the message “Operation still in progress,” click <b>OK</b>. When the process completes, click <b>OK</b> in the dialog box that displays the message “Set Full Auto Focus successfully.”</p>

**Table 3-1** Camera Video & Control Window Controls (continued)

Control	Description
<b>Privacy Zone</b>	
<b>Note</b>	To display these controls click the Expand icon  next to Privacy Zone under the video image. The icon changes to the Collapse icon  . Click the Collapse icon to hide these controls.  If you make changes to any of the Privacy Zone options, click the <b>Save</b> button to save the changes.
<b>Enable Privacy Region</b> check box	<p>Enables the Privacy Zone feature.</p> <p>You can create up to four user-defined masking zones that can used to provide regions of privacy in the camera field of view. When the Privacy Zone feature is enabled, video within privacy each region is not recorded in the camera, nor sent in the video stream. Instead of the actual video, privacy regions display as solid rectangles that you choose from the Region Color drop-down list.</p> <p>To designate regions, right-click the video image, choose <b>Draw Region</b>, then hold down the left mouse button and draw the region, which is indicated by a green rectangle.</p> <p>To move a region, left-click it and drag its window to the desired area.</p> <p>To resize a region, left-click it and drag a box in the edge or corner of the region.</p> <p>To remove a region, left-click it, then right-click it and choose <b>Delete Region</b>.</p>
Region Color drop-down menu	Choose the color in which the system displays the zones that are defined by privacy regions. You can choose <b>Red</b> , <b>Green</b> , <b>Black</b> , or <b>Blue</b> .
Privacy Zone properties	<p>To expand region properties information, click the + icon next to <b>Privacy Zone Properties</b>. The icon changes to a – icon, which you click to collapse region properties information.</p> <ul style="list-style-type: none"> <li>• <b>Name</b>—Name of the region. By default, the system assigns the name RegionX, where X is a number 1 through 4. To rename a region, click its name (which appears in bold type on this line) and type a unique name of up to 32 characters .</li> <li>• <b>IsActive</b>—To indicate whether the IP camera displays a region as a privacy mask, left-click that region, click <b>IsActive</b>, then choose <b>True</b> (mask the region) or <b>False</b> (do not mask the region) from the drop-down menu that appears on the IsActive line. Alternatively, you can double-click <b>True</b> or <b>False</b> to toggle between these values.</li> </ul>



# CHAPTER 4

## Feature Setup

---

The Feature Setup windows let you configure a variety of IP camera features and functions. The following sections describe the Feature Setup windows in detail:

- [Streaming Window, page 4-1](#)
- [Camera Window, page 4-14](#)
- [Video Overlay Window, page 4-16](#)
- [IO Ports Window, page 4-17](#)
- [Event Notification Window, page 4-18](#)
- [Alert Notification Window, page 4-24](#)
- [Local Storage Window, page 4-27](#)

## Streaming Window

The Streaming window provides options for configuring audio and video streams from the IP camera. You can configure settings for the primary and an optional secondary video stream.

Configuring a secondary stream is useful for providing a video stream that is at a lower resolution than the primary stream to third-party devices or software.

Both streams support H.264 and MJPEG for video, and G.711 A-law and G.711 u-law for audio.

When configuring video streams, be aware of the following guidelines:

- The resolution of the primary stream must be higher than the resolution of the secondary stream.
- You cannot configure a maximum frame rate of 30 for the primary stream if the secondary stream is enabled.
- Multiple secondary frame rates are supported. [Table 4-1](#) shows the frame rate combinations of primary and secondary streams with a 16:9 aspect ratio. [Table 4-2](#) shows the frame rate combinations of primary and secondary streams with a 4:3 aspect ratio. [Table 4-3](#) shows other aspect ratio resolutions. If a secondary frame rate that is not shown in this table is selected in Cisco Video Surveillance Manager, the IP camera uses the closest available frame rate.



### Note

If you configure the camera for 768 x 432, 704 x 400, and 352 x 208 resolutions and then downgrade the firmware, the camera might reboot. Before downgrading, change the resolution back to an older resolution.

**Table 4-1** *Cisco Video Surveillance 7000 Series IP Camera Video Stream Support for 16:9 Aspect Ratio*

Primary (H.264)	FPS	Bit Rate	Secondary (H.264 or MJPEG)	FPS	Bit Rate
2560 x 1920 (4:3 aspect ratio)	8	15M, 12M, 10M, 8M, 6M	—	—	—
	5	10M, 8M, 6M	—	—	—
	3	8M, 6M	—	—	—
1920 x 1080	20, 25, 30	2M, 4M, 6M, 8M, 10M, 12M, 15M	—	—	—
	15	2M, 4M, 6M, 8M, 10M, 12M, 15M	1024 x 576	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M
				1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M, 2M
	6, 8, 10	2M, 4M, 6M, 8M, 10M	960 x 544	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M
				1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M, 2M
			768 x 432	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M
				1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M
			704 x 400	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M
				1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M
			640 x 368	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M
				1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M
			352 x 208	10, 15	64K, 128K, 256K, 384K, 768K
				1, 3, 5, 6, 8	64K, 128K, 256K, 384K
			320 x 192	10, 15	64K, 128K, 256K, 384K, 768K
				1, 3, 5, 6, 8	64K, 128K, 256K, 384K
			192 x 112	10, 15	64K, 128K, 256K
				1, 3, 5, 6, 8	64K, 128K
			160 x 96	10, 15	64K, 128K, 256K
				1, 3, 5, 6, 8	64K, 128K



**Table 4-1** Cisco Video Surveillance 7000 Series IP Camera Video Stream Support for 16:9 Aspect Ratio (continued)

Primary (H.264)	FPS	Bit Rate	Secondary (H.264 or MJPEG)	FPS	Bit Rate
1536 x 864	20, 25, 30	64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M, 6M, 8M, 10M	1024 x 576	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M
	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M, 6M		1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M, 2M
	1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M	960 x 544	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M
				1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M, 2M
			768 x 432	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M
				1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M
			704 x 400	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M
				1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M
			640 x 368	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M
				1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M
			352 x 208	10, 15	64K, 128K, 256K, 384K, 768K
				1, 3, 5, 6, 8	64K, 128K, 256K, 384K
			320 x 192	10, 15	64K, 128K, 256K, 384K, 768K
				1, 3, 5, 6, 8	64K, 128K, 256K, 384K
			192 x 112	10, 15	64K, 128K, 256K
				1, 3, 5, 6, 8	64K, 128K
			160 x 96	10, 15	64K, 128K, 256K
				1, 3, 5, 6, 8	64K, 128K
1472 x 832	20, 25, 30	64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M, 6M, 8M, 10M	1024 x 576	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M
	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M, 6M		1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M, 2M
	1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M	960 x 544	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M
				1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M, 2M

**Table 4-1** Cisco Video Surveillance 7000 Series IP Camera Video Stream Support for 16:9 Aspect Ratio (continued)

Primary (H.264)	FPS	Bit Rate	Secondary (H.264 or MJPEG)	FPS	Bit Rate
			768 x 432	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M
				1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M
			704 x 400	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M
				1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M
			640 x 368	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M
				1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M
			352 x 208	10, 15	64K, 128K, 256K, 384K, 768K
				1, 3, 5, 6, 8	64K, 128K, 256K, 384K
			320 x 192	10, 15	64K, 128K, 256K, 384K, 768K
				1, 3, 5, 6, 8	64K, 128K, 256K, 384K
			192 x 112	10, 15	64K, 128K, 256K
				1, 3, 5, 6, 8	64K, 128K
			160 x 96	10, 15	64K, 128K, 256K
				1, 3, 5, 6, 8	64K, 128K
1280 x 720	20, 25, 30	64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M, 6M, 8M, 10M	1024 x 576	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M
	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M, 6M		1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M, 2M
	1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M	960 x 544	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M
				1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M, 2M
			768 x 432	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M
				1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M
			704 x 400	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M
				1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M

**Table 4-1** Cisco Video Surveillance 7000 Series IP Camera Video Stream Support for 16:9 Aspect Ratio (continued)

Primary (H.264)	FPS	Bit Rate	Secondary (H.264 or MJPEG)	FPS	Bit Rate
			640 x 368	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M
				1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M
			352 x 208	10, 15	64K, 128K, 256K, 384K, 768K
				1, 3, 5, 6, 8	64K, 128K, 256K, 384K
			320 x 192	10, 15	64K, 128K, 256K, 384K, 768K
				1, 3, 5, 6, 8	64K, 128K, 256K, 384K
			192 x 112	10, 15	64K, 128K, 256K
				1, 3, 5, 6, 8	64K, 128K
			160 x 96	10, 15	64K, 128K, 256K
				1, 3, 5, 6, 8	64K, 128K
1024 x 576	20, 25, 30	64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M, 6M	1024 x 576	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M
	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M		1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M, 2M
	1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M, 2M	960 x 544	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M
				1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M, 2M
			768 x 432	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M
				1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M
			704 x 400	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M
				1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M
			640 x 368	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M
				1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M
			352 x 208	10, 15	64K, 128K, 256K, 384K, 768K
				1, 3, 5, 6, 8	64K, 128K, 256K, 384K
			320 x 192	10, 15	64K, 128K, 256K, 384K, 768K

**Table 4-1** Cisco Video Surveillance 7000 Series IP Camera Video Stream Support for 16:9 Aspect Ratio (continued)

Primary (H.264)	FPS	Bit Rate	Secondary (H.264 or MJPEG)	FPS	Bit Rate
			192 x 112	1, 3, 5, 6, 8 10, 15	64K, 128K, 256K, 384K 64K, 128K, 256K
			160 x 96	1, 3, 5, 6, 8 10, 15	64K, 128K 64K, 128K, 256K
				1, 3, 5, 6, 8	64K, 128K
960 x 544	20, 25, 30	64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M, 6M	960 x 544	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M
	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M		1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M, 2M
	1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M, 2M	768 x 432	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M
				1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M
			704 x 400	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M
				1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M
			640 x 368	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M
				1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M
			352 x 208	10, 15	64K, 128K, 256K, 384K, 768K
				1, 3, 5, 6, 8	64K, 128K, 256K, 384K
			320 x 192	10, 15	64K, 128K, 256K, 384K, 768K
				1, 3, 5, 6, 8	64K, 128K, 256K, 384K
			192 x 112	10, 15	64K, 128K, 256K
				1, 3, 5, 6, 8	64K, 128K
			160 x 96	10, 15	64K, 128K, 256K
				1, 3, 5, 6, 8	64K, 128K
768 x 432	20, 25, 30	64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M	768 x 432	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M
	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M		1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M
	1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M	704 x 400	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M
				1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M

**Table 4-1 Cisco Video Surveillance 7000 Series IP Camera Video Stream Support for 16:9 Aspect Ratio (continued)**

Primary (H.264)	FPS	Bit Rate	Secondary (H.264 or MJPEG)	FPS	Bit Rate
			640 x 368	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M
				1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M
			352 x 208	10, 15	64K, 128K, 256K, 384K, 768K
				1, 3, 5, 6, 8	64K, 128K, 256K, 384K
			320 x 192	10, 15	64K, 128K, 256K, 384K, 768K
				1, 3, 5, 6, 8	64K, 128K, 256K, 384K
			192 x 112	10, 15	64K, 128K, 256K
				1, 3, 5, 6, 8	64K, 128K
			160 x 96	10, 15	64K, 128K, 256K
				1, 3, 5, 6, 8	64K, 128K
704 x 400	20, 25, 30	64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M	704 x 400	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M
	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M		1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M
	1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M	640 x 368	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M
				1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M
			352 x 208	10, 15	64K, 128K, 256K, 384K, 768K
				1, 3, 5, 6, 8	64K, 128K, 256K, 384K
			320 x 192	10, 15	64K, 128K, 256K, 384K, 768K
				1, 3, 5, 6, 8	64K, 128K, 256K, 384K
			192 x 112	10, 15	64K, 128K, 256K
				1, 3, 5, 6, 8	64K, 128K
			160 x 96	10, 15	64K, 128K, 256K
				1, 3, 5, 6, 8	64K, 128K
640 x 368	20, 25, 30	64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M	640 x 368	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M
	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M		1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M

**Table 4-1** Cisco Video Surveillance 7000 Series IP Camera Video Stream Support for 16:9 Aspect Ratio (continued)

Primary (H.264)	FPS	Bit Rate	Secondary (H.264 or MJPEG)	FPS	Bit Rate	
	1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M	352 x 208	10, 15	64K, 128K, 256K, 384K, 768K	
			320 x 192	1, 3, 5, 6, 8	64K, 128K, 256K, 384K	
				10, 15	64K, 128K, 256K, 384K, 768K	
			192 x 112	1, 3, 5, 6, 8	64K, 128K, 256K, 384K	
				10, 15	64K, 128K, 256K	
			160 x 96	1, 3, 5, 6, 8	64K, 128K	
				10, 15	64K, 128K, 256K	
				1, 3, 5, 6, 8	64K, 128K	
				352 x 208	10, 15	64K, 128K, 256K, 384K, 768K
				320 x 192	1, 3, 5, 6, 8	64K, 128K, 256K, 384K
					10, 15	64K, 128K, 256K, 384K, 768K
				192 x 112	1, 3, 5, 6, 8	64K, 128K, 256K, 384K
					10, 15	64K, 128K, 256K
				160 x 96	1, 3, 5, 6, 8	64K, 128K
10, 15	64K, 128K, 256K					
				1, 3, 5, 6, 8	64K, 128K	
				320 x 192	10, 15	64K, 128K, 256K, 384K, 768K
				192 x 112	1, 3, 5, 6, 8	64K, 128K, 256K, 384K
					10, 15	64K, 128K, 256K
				160 x 96	1, 3, 5, 6, 8	64K, 128K
					10, 15	64K, 128K, 256K
192 x 112	10, 15	64K, 128K, 256K				
160 x 96	1, 3, 5, 6, 8	64K, 128K				
	10, 15	64K, 128K, 256K				
160 x 96	1, 3, 5, 6, 8	64K, 128K				
	10, 15	64K, 128K, 256K				
				1, 3, 5, 6, 8	64K, 128K	
				10, 15	64K, 128K, 256K	
				1, 3, 5, 6, 8	64K, 128K	
				10, 15	64K, 128K, 256K	
				1, 3, 5, 6, 8	64K, 128K	
				10, 15	64K, 128K, 256K	
				1, 3, 5, 6, 8	64K, 128K	
				10, 15	64K, 128K, 256K	
				1, 3, 5, 6, 8	64K, 128K	

**Table 4-2 Cisco Video Surveillance 7000 Series IP Camera Video Stream Support for 4:3 Aspect Ratio**

Primary (H.264)	FPS	Bit Rate	Secondary (H.264 or MJPEG)	FPS	Bit Rate
1280 x 960	20, 25, 30	64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M, 6M, 8M, 10M	720 x 480	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M
	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M, 6M		1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M
	1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M	704 x 480	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M
				1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M
			352 x 240	10, 15	64K, 128K, 256K, 384K, 768K, 1M
				1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K
			720 x 576	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M
				1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M
			704 x 576	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M
				1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M
			352 x 288	10, 15	64K, 128K, 256K, 384K, 768K, 1M
				1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K
720 x 576	20, 25, 30	64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M	720 x 576	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M
	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M		1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M
	1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M	704 x 576	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M
				1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M
			352 x 288	10, 15	64K, 128K, 256K, 384K, 768K, 1M
				1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K
704 x 576	20, 25, 30	64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M	704 x 576	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M

**Table 4-2** Cisco Video Surveillance 7000 Series IP Camera Video Stream Support for 4:3 Aspect Ratio (continued)

Primary (H.264)	FPS	Bit Rate	Secondary (H.264 or MJPEG)	FPS	Bit Rate
	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M	352 x 288	1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M
	1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M		10, 15	64K, 128K, 256K, 384K, 768K, 1M
				1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K
720 x 480	20, 25, 30	64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M	720 x 480	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M
	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M	704 x 480	1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M
	1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M		10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M
				1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M
			352 x 240	10, 15	64K, 128K, 256K, 384K, 768K, 1M
				1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K
704 x 480	20, 25, 30	64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M	704 x 480	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M
	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M	352 x 240	1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M
	1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M		10, 15	64K, 128K, 256K, 384K, 768K, 1M
				1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K
352 x 240	20, 25, 30	64K, 128K, 256K, 384K, 768K, 1M, 2M	352 x 240	10, 15	64K, 128K, 256K, 384K, 768K, 1M
	10, 15	64K, 128K, 256K, 384K, 768K, 1M		1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K
	1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K			
352 x 288	20, 25, 30	64K, 128K, 256K, 384K, 768K, 1M, 2M	352 x 288	10, 15	64K, 128K, 256K, 384K, 768K, 1M
	10, 15	64K, 128K, 256K, 384K, 768K, 1M		1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K
	1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K			



**Table 4-3** Cisco Video Surveillance 7000 Series IP Camera Video Stream Support for Other Aspect Ratio Resolutions

Primary (H.264)	FPS	Bit Rate	Secondary (H.264 or MJPEG)	FPS	Bit Rate
1280 x 1024 (1.25 aspect ratio)	20, 25, 30	64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M, 6M, 8M, 10M	720 x 480	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M
	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M, 6M		1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M
	1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M	704 x 480	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M
				1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M
			352 x 240	10, 15	64K, 128K, 256K, 384K, 768K, 1M
				1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K
			720 x 576	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M
				1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M
			704 x 576	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M
				1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M
			352 x 288	10, 15	64K, 128K, 256K, 384K, 768K, 1M
				1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K

To display the Streaming window, perform the following steps:

#### Procedure

**Step 1** From the IP camera user interface, click the **Setup** link.

**Step 2** Click **Feature Setup** to expand the menu.

**Step 3** From the Feature Setup menu, click **Streaming**.

The Streaming window appears. If you change any options in this window, you must click the **Save** button to save the changes. If you do not click this button, changes are not retained when you exit the window. The **Save** button appears at the bottom of the window. You might need to scroll down to it.

Table 4-4 describes the options in the Streaming window.

**Table 4-4**      **Streaming Window Options**

Option	Description
<b>Current Stream Area</b>	
Stream	Choose the video stream (Stream 1 or Stream 2) to which the configuration settings in the Streaming window apply. Stream 1 is the primary stream, and Stream 2 is the secondary stream.
Enable Stream	Check this check box to cause the IP camera to send audio/video data on the selected stream.
<b>Streaming Area</b>	
<b>Note</b> Each video stream uses its own set of streaming options. The settings shown in the <b>Streaming Area</b> apply to the currently selected stream only.	
RTSP Port	<p>Transmission Control Protocol (TCP) port on which the IP camera receives Real-Time Streaming Protocol (RTSP) commands. You must configure this port if you want to allow third-party devices or software to access video streams from the IP camera.</p> <p>RTSP is a standard for connecting a client to control streaming data over the web.</p> <p>Valid values are 554 and 1024 through 65535. The default port is 554.</p>
Video Source Port	<p>Universal Datagram Protocol (UDP) port on which the IP camera transmits Video Real-Time Transport Protocol (RTP) data.</p> <p>Valid values are even numbers 1024 through 65534. The default port is 1024.</p>
Audio Source Port	<p>UDP port on which the IP camera transmits audio RTP data.</p> <p>Valid values are even numbers 1024 through 65534. The default value is 1026.</p>
Max RTP Packet Size	<p>Maximum number of bytes per data packets that are sent in each RTP request.</p> <p>Configure a lower number if you are streaming video to a cell phone that requires smaller data packets.</p> <p>Valid values are 400 through 1400. The default value is 1400.</p>
Enable Multicast	<p>Check this check box to send video and audio data as a multicast stream.</p> <p>When multicast is enabled, the IP camera sends video and audio to the multicast addresses that you designate. Multicast enables several devices to receive the video and audio signals from the IP camera simultaneously.</p>
Multicast Address	Enter the multicast IP address on which the IP camera sends a multicast audio/video stream.
Multicast Video Port	<p>Enter the port on which the IP camera sends a multicast video stream.</p> <p>Valid values are even numbers 1024 through 65534.</p>
Multicast Audio Port	<p>Enter the port on which the IP camera sends a multicast audio stream.</p> <p>Valid values are even numbers 1024 through 65534.</p>

**Table 4-4 Streaming Window Options (continued)**

Option	Description
Time to Live	Enter the number of hops, which specifies the number of network devices that an audio/video stream can pass before arriving at its destination or being dropped.  Valid values are 1 through 255.
<b>Video Area</b>	
<b>Note</b> Each video stream uses its own set of video options. The settings shown in the <b>Video Area</b> apply to the currently selected stream only.	
Video Standard	Choose the system for video transmission: NTSC or PAL.  The setting that you make affects each channel that is enabled.
Video Codec	Choose the codec for video transmission: H.264 or MJPEG. Both options are supported on the primary and secondary streams.
Video Resolution	Choose the resolution for video transmission. The resolutions in this drop-down list depend on the video standard that you selected.
Maximum Frame Rate	Choose the maximum frame rate of the video stream.
Video Quality	Choose an option for the video quality of the video stream from the IP camera: <ul style="list-style-type: none"> <li>• <b>Constant Bit Rate</b>—Available for the primary stream only. Specifies that the video stream is output at or close to the constant bit rate that you choose.  You can select one of the Mbps values in the drop-down menu. The default value is 4 Mbps. A higher bit rate provides better video quality but consumes more bandwidth.  You can also select the Customized option to enter a rate within the valid range, depending on resolution and frame rate.</li> <li>• <b>Fixed Quality</b>—Specifies that video is output at a fixed quality, which ranges from Very High to Low. The bit rate may vary to maintain this quality. The default fixed quality is Normal. A higher fixed quality provides better video quality but consumes more bandwidth.</li> </ul> <p>You can use these options to help manage bandwidth use in your network. For example, if the IP camera is focused on an area with little movement, such as an emergency exit, you can configure it with a low fixed quality.</p>
<b>Analog Video Area</b>	
<b>Note</b> This option applies to the primary stream only.	
Enable Analog Video Port	Check this check box if you if you want the IP camera to enable analog video for installation purposes. To enable analog video, the following settings are required: <ul style="list-style-type: none"> <li>• The primary video stream frame rate must be set to 15 fps or lower</li> <li>• The secondary video stream must be disabled</li> </ul>
<b>Audio Area</b>	
Enable Audio	Check this check box if you want to enable audio.

**Table 4-4 Streaming Window Options (continued)**

Option	Description
Audio Codec	<p>Choose the audio codec to use for encoding audio:</p> <ul style="list-style-type: none"> <li>• <b>G.711 A-Law</b>—Encodes 14-bit signed linear PCM samples to logarithmic 8-bit samples.</li> <li>• <b>G.711 u-Law</b>—Encodes 13-bit signed linear PCM samples to logarithmic 8-bit samples.</li> </ul> <p><b>Note</b> The G.711 A-law algorithm provides more quantization levels at lower signal levels whereas the G.711 <math>\mu</math>-law algorithm tends to give more resolution to higher range signals.</p>
Audio Sampling Rate	<i>Display only.</i> Indicates the sampling rate of the audio stream from the IP camera
Audio Resolution	<i>Display only.</i> Indicates the resolution for audio transmission from the IP camera.

## Camera Window

The Camera window provides options for selecting a microphone and configuring the operation of the IP camera day and night filters.

A microphone captures audio at the camera location. This audio is sent to the PC that you use to view video from the IP camera. You can listen to the audio when viewing video in the Camera Video & Control window.

The IP camera day and night filters allow the IP camera to optimize its video image for various lighting conditions. When the IP camera uses its day filter, it is operating in *day mode*. In this mode, the camera displays video images in color. When the IP camera uses its night filter, it is in *night mode*. In this mode, the camera displays video images in black and white.

To display the Camera window, perform the following steps:

### Procedure

- 
- Step 1** From the IP camera user interface, click the **Setup** link.
  - Step 2** Click **Feature Setup** to expand the menu.
  - Step 3** From the Feature Setup menu, click **Camera**.

The Camera window appears. If you change any options in this window, you must click the **Save** button to save the changes. If you do not click this button, changes are not retained when you exit the window. The **Save** button appears at the bottom of the window. You might need to scroll down to it.

---

Table 4-5 describes the options in the Camera window.

**Table 4-5**      **Camera Window Options**

Option	Description
<b>Microphone</b>	
Microphone Type	The Cisco 7030 IP camera supports only an external microphone. Audio is captured by an optional external microphone, available from third-parties.
<b>Day Night Filter Area</b>	
Switch Mode	<p>Choose the day/night mode for the IP camera:</p> <ul style="list-style-type: none"> <li>• <b>Day</b>—IP camera always remains in day mode.</li> <li>• <b>Night</b>—IP camera always remains in night mode.</li> <li>• <b>Auto</b>—IP camera automatically switches between day and night mode based on the lighting condition threshold that you specify.</li> </ul> <p>When the IP camera is in Auto mode, it attempts to avoid frequent or unnecessary changes between day mode and night mode (such as can occur when an IP camera is set up on a street where car headlights could cause constant changes between these modes). When the IP camera detects that a switch from day to night mode might be necessary, it 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.</p> <p>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.</p> <ul style="list-style-type: none"> <li>• <b>Night External</b>—IP camera switches to night mode based on the external Input port. It switches to day mode when the external Input port is not in the triggered status. Check the external Input port of “Alarm I/O Ports.” Output port is optional and can be used to trigger devices connected externally.</li> <li>• <b>Night Schedule</b>—IP camera switches to and from Night mode based on the Start and End times.</li> </ul> <p><b>Note</b> If you configure a Night Schedule, make sure that the time on the IP camera is set correctly.</p>
Day to Night Threshold	<p>(The Day to Night Threshold option is available only when the Switch Mode is set to Auto.) Choose a value that specifies the relative light threshold at which the IP camera switches from day to night mode. A lower value designates that the IP camera switches from day to night mode in brighter conditions. A higher value designates that the IP camera switches modes in darker conditions.</p> <p>The default value is 45</p>

**Table 4-5**      **Camera Window Options (continued)**

Option	Description
Night to Day Threshold	<p>(The Night to Day Threshold option is available only when the Switch Mode is set to Auto.) Choose a value that specifies the relative light threshold at which the IP camera switches from night to day mode. A lower value designates that the IP camera switches from night to day mode in darker conditions. A higher value designates that the IP camera switches modes in lighter conditions.</p> <p>The default value is 85.</p>
Input	(The Input option is available only when the Switch Mode is set to Night External.) Choose the Input port that is connected to an external device that is to trigger the switch to night mode.
Output	<p>Choose the Output port that is connected to an external device that is to be triggered.</p> <p>This option is not when the Switch Mode is set to Day.</p>
Start Time	(The Start Time option is available only when the Switch Mode is set to Night Schedule.) Enter the time, in 24 hour format, when the camera enables its night filter.
End Time	(The Start Time option is available only when the Switch Mode is set to Night Schedule.) Enter the time, in 24 hour format, when the camera disables its night filter.
<b>Camera Tamper Area</b>	
Enable camera tamper detection	<p>Check this check box to enable the camera tamper feature.</p> <p>When enabled, this feature causes the IP camera to generate alerts when any of the following events occur and persist for a designated period:</p> <ul style="list-style-type: none"> <li>• The IP camera view is changed</li> <li>• The IP camera view is blocked</li> <li>• The IP camera view is substantially out of focus</li> </ul>
Minimum duration	<p>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.</p> <p>Valid values are 10 to 600 seconds.</p>

## Video Overlay Window

The Video Overlay window provides options for configuring overlay information that appears on the video image in the Camera Video & Control window.

To display the Video Overlay window, perform the following steps:

### Procedure

**Step 1** From the IP camera user interface, click the **Setup** link.

**Step 2** Click **Feature Setup** to expand the menu.

**Step 3** From the Feature Setup menu, click **Video Overlay**.

The Video Overlay window appears. If you change any options in this window, you must click the **Save** button to save the changes. If you do not click this button, changes are not retained when you exit the window. The **Save** button appears at the bottom of the window. You might need to scroll down to it.

Table 4-6 describes the options in the Video Overlay window.

**Table 4-6** Video Overlay Window Options

Option	Description
<b>Text Overlay Area</b>	
Enable Date/Time Display	Check this check box to display the time from the internal clock of the IP camera as an overlay on the video image from the IP camera.
Date/Time alignment in Overlay	Choose whether the Date/Time is to be aligned to the <b>Left</b> , <b>Center</b> , or <b>Right</b> .
Enable Text Display	Check this check box to display the text that you enter in the Display Text field as an overlay on the video image from the IP camera.  This option can be useful for identifying this IP camera in an installation with several IP cameras.
Text Alignment in Overlay	Choose whether the text overlay is to be aligned to the <b>Left</b> , <b>Center</b> , or <b>Right</b> .
Text Format	Specifies the text format to use for the text overlay. Currently, English (ASCII) is the only available text format.
Display Text	If you check the Enable Text Display check box, the text that you enter in this field appears as an overlay on the video image from the IP camera.  The text can contain up to 26 characters, which can include letters, numbers, spaces, and these characters: ! \$ % ( ) + , - . / : = @ ^ _ ` { } ~
Overlay Placement	Choose whether the text overlay is to appear at the <b>Top of Image</b> or <b>Bottom of Image</b> .

## IO Ports Window

The IO Ports window lets you configure various options for the three input and one output ports on the IP camera. A state change of an input port triggers a camera to take configured actions. An output port sends signals that can control external devices, such as alarms or door switches.

The IP camera can trigger an action only when the input that is received on an input port comes from a contact that is in a normally closed condition. The camera triggers the action when the contact changes to an open condition.

To display the IO Ports window, perform the following steps:

**Procedure**

**Step 1** From the IP camera user interface, click the **Setup** link.

**Step 2** Click **Feature Setup** to expand the menu.

**Step 3** From the Feature Setup menu, click **IO Ports**.

The IO Ports window appears. If you change any options in this window, you must click the **Save** button to save the changes. If you do not click this button, changes are not retained when you exit the window. The **Save** button appears at the bottom of the window. You may need to scroll down to it.

Table 4-7 describes the options in the IO Ports window.

**Table 4-7 IO Ports Window Options**

Option	Description
<b>Input Ports</b>	
Port #	<i>Display only.</i> Indicates input port 1, input port 2, and input port 3.
Current State	<i>Display only.</i> Indicates the current state (High or Low) of the port.
Event Trigger	Choose the state (Rising or Falling) that triggers designated camera actions. When an input port changes to the configured state, the camera determines that an event has occurred and takes the actions that you have configured.
<b>Output Ports</b>	
Port #	<i>Display only.</i> Indicates output port 1.
Current State	<i>Display only.</i> Indicates the current state (High or Low) of the corresponding port.
Default State	Choose the state (Low or High) to which the corresponding port is set when the IP camera powers on or resets.  The port changes to this state when you click <b>Save</b> .  The default setting is High.
Event Action	<i>Display only.</i> Indicates the current state (High or Low) that the output port changes to when an event occurs.
Automatic Reset	Check this check box if you want the output port to go back to its default state after an event occurs.
Duration	If you checked the Automatic Reset check box, enter the amount of time, in milliseconds, that elapses before the port goes back to its default state after an event changes it from the default state.

## Event Notification Window

The Event Notification window provides options for how the IP camera handles system triggers and generates event notification. A system trigger is any of the following:

- A change of state from low to high or from high to low on an input port of the IP camera. For related information about input ports, see the [“IO Ports Window” section on page 4-17](#).



- Motion that the IP camera detects. For related information about motion detection, see the “[Motion Detection](#)” rows in [Table 3-1](#).
- An activity that is defined by a camera app.

When an event occurs, it triggers the IP camera to take certain configured actions:

- Email notification—An event can cause the IP camera to send a notification e-mail message to designated recipients. The message can include a video clip or a snapshot of the activity that triggered the event.  
This message includes the same information that is provided with HTTP notification.
- Output port state change—Changes the state of an IP camera output port from low to high or from high to low.
- Syslog server message—Sends a notification message to the designated Syslog server.
- HTTP notification—IP camera sends notification to a remote system via HTTP. This information includes the following:
  - Device ID—ID of the IP camera
  - Device name—Name of the IP camera
  - IP address—IP address of the IP camera
  - MAC address—MAC address of the IP camera
  - Channel ID—Channel identification number (1 for primary stream or 2 for secondary stream)
  - Channel name—Name that is configured for the channel
  - Date and time—Date and time that the event occurred
  - Active post Count—Sequence number of the notification for this event
  - Event type—Type of event
  - Event state—Indicates whether the event is active or inactive at the time that the event was detected for this notification
  - Event description—Description of the event
  - Input port ID—If the event was triggered by an input port state change, port ID of the port
  - Region index—If the event was triggered by motion detection, identification number of the region in which the IP camera detected motion
  - Sensitivity level—If the event was triggered by motion detection, sensitivity that is configured for the region in which motion was detected
  - Detection threshold—If the event was triggered by motion detection, threshold that is configured for the region in which motion was detected
- FTP notification—An event can cause the IP camera to upload a video clip or a snapshot of the activity that triggered the event to an FTP server.

The Event Notification window also allows you to designate schedules. If an event takes place within a designated schedule, the IP camera takes the actions that you configure.

### Procedure

- 
- Step 1** From the IP camera user interface, click the **Setup** link.
  - Step 2** Click **Feature Setup** to expand the menu.
  - Step 3** From the Feature Setup menu, click **Event**.

The Event Notification window appears. If you change any options in this window, you must click the **Save** button to save the changes. If you do not click this button, changes are not retained when you exit the window. The **Save** button appears at the bottom of the window. You might need to scroll down to it.

Table 4-8 describes the options in the Event Notification window.

**Table 4-8 Event Notification Window Options**

Option	Description
<b>Event Triggering Area</b>	
Triggered by	<p>Check the desired check boxes to designate the events that trigger actions:</p> <ul style="list-style-type: none"> <li>• <b>Input 1</b>—Event is triggered when input port 1 on the IP camera changes state from high to low.</li> <li>• <b>Input 2</b>—Event is triggered when input port 2 on the IP camera changes state from high to low.</li> <li>• <b>Input 3</b>—Event is triggered when input port 3 on the IP camera changes state from high to low.</li> <li>• <b>Motion Detection</b>—Event is triggered when the camera detects motion, if motion detection is configured as described in the “<a href="#">Motion Detection</a>” rows in <a href="#">Table 3-1 on page 3-1</a>.</li> <li>• <b>App</b>—Event is triggered by an activity that is defined by an app that is running on the IP camera.</li> </ul>
Actions	<p>Check the desired check boxes to designate the actions that the IP camera takes when the corresponding trigger occurs.</p> <ul style="list-style-type: none"> <li>• <b>Email</b>—Sends information about the event in an e-mail message to the designated recipient. You designate the recipient and configure e-mail options in other fields in this window.</li> <li>• <b>Output 1</b>—Changes the state of the output 1 port on the IP camera as defined in the Port window.</li> <li>• <b>Syslog</b>—Sends information about the event to a designated Syslog server.</li> <li>• <b>HTTP</b>—Sends information about the event as an HTTP stream to a remote system.</li> <li>• <b>FTP</b>—Uploads a snapshot or video clip of the event to an FTP server.</li> </ul>
Interval	Choose the time interval (in minutes) from the drop-down list to wait after an event occurs before detecting the next event.
<b>Event Scheduling Area</b>	
Scheduling Grid	<p>Designate the times at which an event causes the IP camera to take the designed actions. If an event occurs during a time that is not designated, the IP camera does not take any action.</p> <p>Each cell in this grid represents one hour on the corresponding day, starting at 12:00 a.m. (0:00). To designate times, click the desired cells. Selected cells appear shaded.</p>
Set All button	Select all times in the scheduling grid.

**Table 4-8 Event Notification Window Options (continued)**

Option	Description
<b>Clear All</b> button	Deselect all times in the scheduling grid.
<b>Undo All</b> button	Change the scheduling settings to the last saved configuration.
<b>HTTP Notification Area</b>	
High Availability	Check this check box if you want to send HTTP messages to a secondary HTTP server in the event that the primary HTTP server is unreachable.
Primary HTTP Server	Identify the primary server to which HTTP messages are sent by choosing <b>IP Address</b> or <b>Hostname</b> from the drop-down list and entering the IP address or host name in the corresponding field.
URL Base	Enter a string to be used as the prefix in the HTTP URL. The HTTP URL is sent in this format:  http://<IP address>/<URL Base>?<system-provided-name-value-pairs>  where <i>IP address</i> is the IP address of the destination server, <i>URL Base</i> is the string that you enter, and <i>system-provided-name-value-pairs</i> is information about the event.
Port Number	Enter the port number that receives messages on the primary server to which HTTP messages are sent.
User Name	If authentication is required on the primary server to which HTTP messages are sent, enter the user name.
Password	If authentication is required on the primary server to which HTTP messages are sent, enter the password.  <b>Note</b> Invalid special characters are: []\&!:"';<>?./+=%*'# blank
HTTP Authentication	If authentication is required on the primary server to which HTTP messages are sent, choose the MD5 Digest Authentication method from the drop-down list.
Secondary HTTP Server	If the High Availability check box is checked, you can identify an optional secondary server to which HTTP messages are sent by choosing <b>IP Address</b> or <b>Hostname</b> from the drop-down list and entering the IP address or host name in the corresponding field.
URL Base	Enter a string to be used as the prefix in the HTTP URL for the secondary server. The HTTP URL is sent in this format:  http://<IP address>/<URL Base>?<system-provided-name-value-pairs>  where <i>IP address</i> is the IP address of the destination server, <i>URL Base</i> is the string that you enter, and <i>system-provided-name-value-pairs</i> is information about the event.
Port Number	Enter the port number that receives messages on the secondary server to which HTTP messages are sent.
User Name	If authentication is required on the secondary server to which HTTP messages are sent, enter the user name.
Password	If authentication is required on the secondary server to which HTTP messages are sent, enter the password.  <b>Note</b> Invalid special characters are: []\&!:"';<>?./+=%*'# blank

**Table 4-8** *Event Notification Window Options (continued)*

Option	Description
HTTP Authentication	If authentication is required on the secondary server to which HTTP messages are sent, choose the MD5 Digest Authentication method from the drop-down list.
<b>Email Notification Area</b>	
Primary SMTP Server	Identify the primary SMTP server that is used for sending e-mail by choosing <b>IP Address</b> or <b>Hostname</b> from the drop-down list and entering the IP address or host name in the corresponding field.
Primary SMTP Port	Enter the port number for the primary SMTP server. The default SMTP port number is 25.
POP Server	Identify the primary POP server that is used for sending e-mail by choosing <b>IP Address</b> or <b>Hostname</b> from the drop-down list and entering the IP address or host name in the corresponding field.  This field is dimmed if you do not choose <b>Requires POP Before SMTP</b> in the Authentication field that follows.
Authentication	If the primary SMTP server requires authentication to send e-mail, choose the appropriate authentication type from the drop-down list. The authentication type typically is the same as that for the POP3 server that you use to receive e-mail.
Account Name	If the primary SMTP server requires authentication, enter the account name for the server.
Password	If the primary SMTP server requires authentication, enter the account password for the server.
Secondary SMTP Server	Identify an optional secondary SMTP server that is used for sending e-mail by choosing <b>IP Address</b> or <b>Hostname</b> from the drop-down list and entering the IP address or host name in the corresponding field.
Secondary SMTP Port	Enter the port number for the secondary SMTP server. The default SMTP port number is 25.
POP Server	Identify an optional secondary POP server that is used for sending e-mail by choosing <b>IP Address</b> or <b>Hostname</b> from the drop-down list and entering the IP address or host name in the corresponding field.  This field is dimmed if you do not choose <b>Requires POP Before SMTP</b> in the Authentication field that follows.
Authentication	If the secondary SMTP server requires authentication to send e-mail, choose the appropriate authentication type from the drop-down list. The authentication type typically is the same as that for the POP3 server that you use to receive e-mail.
Account Name	If the secondary SMTP server requires authentication, enter the account name for the server.
Password	If the secondary SMTP server requires authentication, enter the account password for the server.
Send To	Enter an e-mail address to which an e-mail message is sent when an event occurs.

**Table 4-8 Event Notification Window Options (continued)**

Option	Description
Show From Address As	Enter the e-mail address to be shown in the From field for the e-mail message that is sent when an event occurs.
Subject	Enter the text to be shown in the Subject field for the e-mail messages that the IP camera sends when events occur. The subject can contain up to 118 characters, including spaces.
Attach Video Streaming URL Address	Check this check box to include in the e-mail message body the URL from which the recipient can access the live video stream from the camera on which the event was detected.
Attach Snapshot	Check this check box to include with the e-mail message a still picture from the beginning of the event. This snapshot is stored on the IP camera until the message is sent.  This functionality is available only when the secondary video stream is enabled.
Attach Video Clip	This option is available if the secondary video stream (H.264 only) is enabled.  Check this check box and enter the following values to include with the e-mail message a video clip of the event: <ul style="list-style-type: none"> <li><b>Pre-Capture Length</b>—Enter the amount of video (in seconds) before the event to include in the video clip.</li> </ul> <p><b>Note</b> The maximum pre-capture length is 5 seconds.</p> <ul style="list-style-type: none"> <li><b>Post-Capture Length</b>—Enter the amount of video (in seconds) after the event to include in the video clip.</li> </ul> <p><b>Note</b> The maximum combined pre-capture and post-capture length is 10 seconds.</p> <p>This video clip is stored on the IP camera until the message is sent.</p>
<b>FTP Notification Area</b>	
Primary FTP Server	Identify the primary FTP server to which snapshots or video clips are uploaded by choosing <b>IP Address</b> or <b>Hostname</b> from the drop-down list and entering the IP address or host name in the corresponding field.
Primary FTP Port	Enter the port number that receives messages on the primary FTP server. The default FTP port number is 21.
User Name	Enter the primary FTP server login user name.
Password	Enter the primary FTP server login password.
Enable Passive Mode	Check this check box to enable the passive mode feature of the primary FTP server.
Secondary FTP Server	Identify an optional secondary FTP server to which snapshots or video clips are uploaded by choosing <b>IP Address</b> or <b>Hostname</b> from the drop-down list and entering the IP address or host name in the corresponding field.
Secondary FTP Port	Enter the port number that receives messages on the secondary FTP server. The default FTP port number is 21.
User Name	Enter the secondary FTP server login user name.

**Table 4-8** *Event Notification Window Options (continued)*

Option	Description
Password	Enter the secondary FTP server login password.
Enable Passive Mode	Check this check box to enable the passive mode feature of the secondary FTP server.
Upload Snapshot	Check this check box to upload a snapshot of the activity that triggered the event.  This functionality is available only when the secondary video stream is enabled.
Upload Video Clip	Check this check box and enter the following values to upload a video clip of the activity that triggered the event: <ul style="list-style-type: none"> <li>• <b>Pre-Capture Length</b>—Enter the amount of video (in seconds) before the event to include in the video clip. The default pre-capture length is 0 seconds.</li> </ul> <p><b>Note</b> The maximum pre-capture length is 5 seconds.</p> <ul style="list-style-type: none"> <li>• <b>Post-Capture Length</b>—Enter the amount of video (in seconds) after the event to include in the video clip. The default post-capture length is 5 seconds.</li> </ul> <p><b>Note</b> The maximum combined pre-capture and post-capture length is 10 seconds.</p>

## Alert Notification Window

The Alert Notification window provides options for how the IP camera handles health triggers and generates event notification. A health trigger is any of the following:

- Loss of video input to the IP camera
- Tampering that the IP camera detects (if IP camera tamper detection is configured as described the “Camera Tamper Area” rows in Table 4-5)
- An alert that is triggered by any of the following:
  - An IP camera app is stopped, restarted, or uninstalled
  - The IP Camera app manager settings are restored to their factory default values
  - An SD or MicroSD card inserted, removed, or formatted
  - The IP Camera is reboots continually

When a health event occurs, it triggers the IP camera to take certain configured actions:

- Email notification—An event can cause the IP camera to send a notification e-mail message to designated recipients. The message can include a video clip or a snapshot of the activity that triggered the event.

This message includes the same information that is provided with HTTP notification.

- Output port state change—Changes the state of an IP camera output port from low to high or from high to low.
- Syslog server message—Sends a notification message to the designated Syslog server.

- HTTP notification—IP camera sends notification to a remote system via HTTP. This information includes the following:
  - Device ID—ID of the IP camera.
  - Device name—Name of the IP camera.
  - IP address—IP address of the IP camera.
  - MAC address—MAC address of the IP camera.
  - Channel ID—Channel identification number (1 for primary stream or 2 for secondary stream).
  - Channel name—Name that is configured for the channel.
  - Date and time—Date and time that the event occurred.
  - Active post Count—Sequence number of the notification for this event.
  - Event type—Type of event.
  - Event state—Indicates whether the event is active or inactive at the time that the event was detected for this notification.
  - Event description—Description of the event.
  - Input port ID—If the event was triggered by an input port state change, port ID of the port
  - Region index—If the event was triggered by motion detection, identification number of the region in which the IP camera detected motion.
  - Sensitivity level—If the event was triggered by motion detection, sensitivity that is configured for the region in which motion was detected.
  - Detection threshold—If the event was triggered by motion detection, threshold that is configured for the region in which motion was detected.
- FTP notification—An event can cause the IP camera to upload a video clip or a snapshot of the activity that triggered the event to an FTP server.

The Event Notification window also allows you to designate schedules. If an event takes place within a designated schedule, the IP camera takes the actions that you configure.

#### Procedure

---

**Step 1** From the IP camera user interface, click the **Setup** link.

**Step 2** Click **Feature Setup** to expand the menu.

**Step 3** From the Feature Setup menu, click **Alert**.

The Alert Notification window appears. If you change any options in this window, you must click the **Save** button to save the changes. If you do not click this button, changes are not retained when you exit the window. The **Save** button appears at the bottom of the window. You may need to scroll down to it.

---

Table 4-9 describes the options in the Alert Notification window.

**Table 4-9 Alert Notification Window Options**

Option	Description
<b>Alert Triggering Area</b>	
Triggered by	<p>Check the desired check boxes to designate the alerts that trigger actions:</p> <ul style="list-style-type: none"> <li>• <b>Video Loss</b>—Alert is triggered if the IP camera loses input to its codec sensor module.</li> <li>• <b>Tamper</b>—Alert is triggered when the camera detects tampering, if camera tamper detection is configured as described the “<a href="#">Camera Tamper Area</a>” rows in <a href="#">Table 4-5</a>.</li> <li>• <b>Alert</b>—Alert is triggered by any of the following: <ul style="list-style-type: none"> <li>– An IP camera app is stopped, restarted, or uninstalled</li> <li>– The IP Camera app manager settings are restored to their factory default values</li> <li>– An SD or MicroSD card inserted, removed, or formatted</li> <li>– The IP Camera is reboots continually</li> </ul> </li> </ul>
Actions	<p>Check the desired check boxes to designate that actions that the IP camera takes when the corresponding trigger occurs.</p> <ul style="list-style-type: none"> <li>• <b>Email</b>—Sends information about the alert in an e-mail message to the designated recipient. You design the recipient and configure other e-mail options in other fields in this window.</li> <li>• <b>Output 1</b>—Changes the state of the output 1 port on the IP camera as defined in the Port window.</li> <li>• <b>Syslog</b>—Sends information about the alert to a designated Syslog server.</li> <li>• <b>HTTP</b>—Sends information about the alert as an HTTP stream to a remote system.</li> </ul>
<b>HTTP Notification Area</b>	
HTTP Server	Identify the server to which HTTP messages are sent by choosing <b>IP Address</b> or <b>Hostname</b> from the drop-down list and entering the IP address or host name in the corresponding field.
URL Base	<p>Enter a string to be used as the prefix in the HTTP URL. The HTTP URL is sent in this format:</p> <p><code>http://&lt;IP address&gt;/&lt;URL Base&gt;?&lt;system-provided-name-value-pairs&gt;</code></p> <p>where <i>IP address</i> is the IP address of the destination server, <i>URL Base</i> is the string that you enter, and <i>system-provided-name-value-pairs</i> is information about the event.</p>
Port Number	Enter the port number that receives messages on the primary server to which HTTP messages are sent.
User Name	If authentication is required on the primary server to which HTTP messages are sent, enter the user name.
Password	If authentication is required on the primary server to which HTTP messages are sent, enter the password.



**Table 4-9 Alert Notification Window Options (continued)**

Option	Description
HTTP Authentication	If authentication is required on the primary server to which HTTP messages are sent, choose the authentication method from the drop-down list.
<b>Email Notification Area</b>	
SMTP Server	Identify the SMTP server that is used for sending e-mail by choosing <b>IP Address</b> or <b>Hostname</b> from the drop-down list and entering the IP address or host name in the corresponding field.
SMTP Port	Enter the port number for the SMTP server. The default SMTP port number is 25.
POP Server	Identify the POP server that is used for sending e-mail by choosing <b>IP Address</b> or <b>Hostname</b> from the drop-down list and entering the IP address or host name in the corresponding field.  This field is dimmed if you do not choose <b>Requires POP Before SMTP</b> in the Authentication field that follows.
Authentication	If the SMTP server requires authentication to send e-mail, choose the appropriate authentication type from the drop-down list. The authentication type typically is the same as that for the POP3 server that you use to receive e-mail.
Account Name	If the SMTP server requires authentication, enter the account name for the server.
Password	If the SMTP server requires authentication, enter the account password for the server.
Password	If the secondary SMTP server requires authentication, enter the account password for the server.
Send To	Enter an e-mail address to which an e-mail message is sent when an event occurs.
Show From Address As	Enter the e-mail address to be shown in the From field for the e-mail message that is sent when an event occurs.
Subject	Enter the text to be shown in the Subject field for the e-mail messages that the IP camera sends when events occur. The subject can contain up to 118 characters, including spaces.

## Local Storage Window

The Local Storage window allows you to enable storing video on a local storage device in case of a network loss. You can download these video recordings from the Local Storage window.

When you use local storage, be aware of the following:

- You can configure the IP camera to save all recordings (*continuous recording mode*) to the SD or MicroSD card, or to save only recording that are made when the IP camera loses network connectivity (*network loss mode*).
- 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. 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.
- The continuous recording 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 be 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.
- 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 display the Local Storage window, perform the following steps:

#### Procedure

- 
- Step 1** From the IP camera user interface, click the **Setup** link.
- Step 2** Click **Feature Setup** to expand the menu.
- Step 3** From the Feature Setup menu, click **Local Storage**.

The Local Storage window appears. If you change any options in this window, you must click the **Save** button to save the changes. If you do not click this button, changes are not retained when you exit the window. The **Save** button appears at the bottom of the window. You might need to scroll down to it.

Table 4-10 describes the options in the 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, From the window IP camera web-based interface that instructs you to install the Cisco Camera UI Control , click **Install** in the yellow banner. If a Security Warning dialog box appears, click **Install**.



#### 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 4-10 ) to prepare the card for ejection. In addition, use care when inserting, removing, and handling the card to avoid damaging the card.

**Table 4-10 Local Storage Window Options**

Option	Description
<b>SD/MicroSD Information Area</b>	
Serial Number	<i>Display only.</i> Serial number of the SD or MicroSD card that is installed in the IP camera.
Total Size	<i>Display only.</i> Total storage capacity in megabytes of the SD or MicroSD card.
Free Space	<i>Display only.</i> Free storage space in megabytes of the SD or MicroSD card.
Model	<i>Display only.</i> Model number of the SD or MicroSD card.
Manufacturer	<i>Display only.</i> 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 video stream configuration.
<b>Settings Area</b>	
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 loses network connectivity. When the network connectivity is restored, recording to the card stops.  This option and the <b>Enable continuous recording</b> option cannot be enabled at the same time.

**Table 4-10** Local Storage Window Options (continued)

Option	Description
Enable Encryption	Available only if <b>Enable recording to Local Storage on network loss</b> 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: <ul style="list-style-type: none"> <li>• AES 256</li> <li>• AES 128</li> <li>• RC2 64</li> </ul>
Enable continuous recording	This options causes the IP camera to save all recordings to its local SD or MicroSD card.  This option and the <b>Enable recording to Local Storage on network loss</b> option cannot be enabled at the same time.
Continuous recording stream	Choose which video stream is recorded with continuous recording is enabled. Options are: <ul style="list-style-type: none"> <li>• Stream 1</li> <li>• Stream 2</li> </ul>
Save	Click this button to save changes that you make in the <b>Settings</b> area.
<b>Recordings Area (requires a supported version of Microsoft Internet Explorer)</b>	
File Decryption Password	Enter the key that is used to decrypt encrypted video recording files.  This field is available only when the Enable recording to Local Storage on network loss mode check box is checked.
Recordings list	Displays a list of video recording on the local SD or MicroSD card and the following information and options for each recording: <ul style="list-style-type: none"> <li>• Select check box. Check the check box next to a recording to select that recording for download or deletion.</li> <li>• Size—Size of the recording in MB.</li> <li>• Name—System-assigned name of the recording.</li> <li>• Start Time (UTC)—Start time of the recording in UTC format.</li> <li>• End Time (UTC)—End time of the recording in UTC format.</li> <li>• 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.</li> <li>• 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.</li> <li>• Progress(%)—The percentage of a video file download operation that has completed.</li> <li>• Status—The status of a video file download or delete operation.</li> </ul>

**Table 4-10**      **Local Storage Window Options (continued)**

Option	Description
Download	<p>To download a video recording to your local drive or a network drive, check the Select check box for the recording that you want, then click the <b>Download</b> button. Follow the on-screen prompts to save the recording.</p> <p>When you save a recording, the system creates a directory called <i>Recordings_TimeStamp</i> 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.</p> <p><b>Note</b> Network-loss recordings that are created on an IP camera that is running firmware 2.0.0 cannot be downloaded with the 1.4.1 SD utility.</p>
Delete	<p>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 want, then click the <b>Delete</b> button.</p> <p>You can quickly select all video recordings in the list by right-clicking in the Recordings list and then choosing <b>Select All</b>.</p>
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 <b>Refresh</b> button.
Cancel	This button appears when a video recording is downloading. To cancel the download operation, click the <b>Cancel</b> button.





# CHAPTER 5

## Network Setup

---

The Network Setup windows let you configure various network-related settings for the IP camera.

The following sections describe the Network Setup windows in detail:

- [Basic Window, page 5-1](#)
- [IP Addressing Window, page 5-3](#)
- [Time Window, page 5-5](#)
- [Discovery Window, page 5-6](#)
- [Medianet Window, page 5-7](#)
- [SNMP Window, page 5-8](#)
- [802.1x Window, page 5-10](#)
- [IP Filter Window, page 5-12](#)
- [QoS Window, page 5-13](#)

## Basic Window

The Basic window provides options for identifying the IP camera and controlling basic operations.

To display the Basic window, perform the following steps:

### Procedure

---

**Step 1** From the IP camera user interface, click the **Setup** link.

**Step 2** Click **Network Setup** to expand the menu.

**Step 3** From the Network Setup menu, click **Basic**.

The Basic window appears. If you change any options in this window, you must click the **Save** button to save the changes. If you do not click this button, changes are not retained when you exit the window. The **Save** button appears at the bottom of the window. You might need to scroll down to it.

---

[Table 5-1](#) describes the options in the Basic window.

**Table 5-1 Basic Window Options**

Option	Description
<b>Basic Settings Area</b>	
ID	<p>Enter a unique identification number for the IP camera, which is used to identify the IP camera to various external applications.</p> <p>The ID can be 0 through 9999.</p>
Name	<p>Enter a name for the IP camera. This name appears in the IP camera log file for information that is associated with this IP camera.</p> <p>The name can contain up to 64 characters, which can include letters, numbers, and these characters: - _ ~. Do not use spaces. We recommend that you give each IP camera a unique name so that you can identify it easily.</p>
Description	<p>Enter a description of the IP camera. For example, enter the IP camera location, such as “North Entrance Camera 1.”</p> <p>The description can contain up to 128 characters, which can include letters, numbers, spaces, and these characters: ! # \$ % &amp; ( ) * + , - . / : ; &lt; &gt; = ? @ [ ] ^ _ ` { }   ~.</p>
Location	<p>Enter the physical location of the IP camera, such as “North Entrance.”</p> <p>The location can contain up to 64 characters, which can include letters, numbers, and these characters: ! \$ % ( ) + , - . / = @ ^ _ ` { } ~. Do not use spaces.</p>
Contact	<p>Enter system contact information for someone such as the system administrator. For example, enter the e-mail address of the system administrator.</p> <p>The contact can contain up to 64 characters, which can include letters, numbers, and these characters: ! \$ % ( ) + , - . / = @ ^ _ ` { } ~. Do not use spaces.</p>
<b>Basic Operation Area</b>	
Enable LED	<p>Check this check box if you want the Power LED on the back of the IP camera to light.</p> <p>If you do not check this check box, this LED does not light.</p>
Disable Session ID	<p>The following camera API mechanisms are available:</p> <ul style="list-style-type: none"> <li>• SessionID—Tracks each client session. Session IDs are required by Cisco Video Surveillance Media Server (VSMS). For more information about Cisco VSMS, refer to the documentation at:  <a href="http://www.cisco.com/en/US/customer/products/ps9152/tsd_products_support_series_home.html">http://www.cisco.com/en/US/customer/products/ps9152/tsd_products_support_series_home.html</a></li> <li>• Basic Authentication—Requires a user ID and password to be passed with every API command.</li> </ul> <p>SessionID is enabled by default. To disable SessionID, and enable Basic authentication, check this option.</p>



**Table 5-1 Basic Window Options (continued)**

Option	Description
Enable ONVIF	<p>Check this check box if you want the IP camera to work in Open Network Video Interface Forum (ONVIF) mode.</p> <p>The following features are supported:</p> <ul style="list-style-type: none"> <li>• Device Discovery Service</li> <li>• Device Service</li> <li>• Media Service</li> </ul> <p>Enabling ONVIF disables SessionID as indicated by the informational message that appears after you click the check box.</p> <p>Click <b>Save</b> to be redirected to the login page. After login, ONVIF service starts working. You can verify this service by using any ONVIF tool.</p> <p>By default, ONVIF is disabled.</p> <p><b>Note</b> We recommend that you do not enable ONVIF when using Cisco VSM to avoid conflicts with configuration.</p>

## IP Addressing Window

The IP Addressing window provides options for configuring the IP address of the IP camera.

To display the IP Addressing window, perform the following steps:

### Procedure

**Step 1** From the IP camera user interface, click the **Setup** link.

**Step 2** Click **Network Setup** to expand the menu.

**Step 3** From the Network Setup menu, click **IP Addressing**.

The IP Addressing window appears. If you change any options in this window, you must click the **Save** button to save the changes. If you do not click this button, changes are not retained when you exit the window. The **Save** button appears at the bottom of the window. You might need to scroll down to it.

Table 5-2 describes the options in the IP Addressing window.

**Table 5-2 IP Addressing Window Options**

Option	Description
<b>IP Addressing Area</b>	
IP Version	Choose the IP version from the drop-down list. Currently, only IPv4 is supported.

**Table 5-2** IP Addressing Window Options (continued)

Option	Description
Configuration Type	<p>Choose the method by which the IP camera obtains its IP address:</p> <ul style="list-style-type: none"> <li>• <b>Dynamic</b>—If your network includes a DHCP server for dynamic allocation of IP addresses, choose this option if you want DHCP to assign an IP address and subnet mask to the IP camera. Depending on your router, the default gateway, primary DNS server, and secondary DNS server may also be assigned. The DHCP server must be configured to allocate static IP addresses based on MAC addresses so that the IP camera always receives the same address.</li> <li>• <b>Static</b>—Choose this option if you want to manually enter an IP address, subnet mask, default gateway, and DNS server IP addresses for the camera.</li> </ul>
IP Address	If you configured the IP camera for a static IP address, enter that IP address.
Subnet Mask	If you configured the IP camera for a static IP address, enter the subnet mask for the IP camera. Use the same value that is configured for the PCs on your network.
Gateway Address	If you configured the IP camera for a static IP address, enter the gateway for the IP camera. Use the same value that is configured for the PCs on your network.
Primary DNS	<p><i>Optional.</i> Enter the IP address of the primary DNS server that is used in your network. Use the same value that is used for the PCs on your network. Typically, your ISP provides this address.</p> <p>This address is required if you use a host name instead of an IP address in any configuration field in the IP camera configuration windows.</p>
Secondary DNS	<p><i>Optional.</i> Enter the IP address of a secondary (backup) DNS server to use if the primary DNS server is unavailable.</p> <p>This address is required if you have a secondary DNS server and you use a host name instead of an IP address in any configuration field in the IP camera configuration windows.</p>
<b>Network transmission Unit</b>	
MTU	<p>Maximum transmission unit size in bytes for packets that the network transmits. Cisco recommends that you use the default value of 1500 unless there are special requirements for your network. If you experience operational issues after changing this value, set this value back to 1500.</p> <p>If you change this value, restart the IP camera after saving the change.</p> <p>Valid values are 600 through 1500. The value 1500.</p>

# Time Window

The Time window provides options for setting and maintaining the time of the IP camera.

To display the Time window, perform the following steps:

## Procedure

**Step 1** From the IP camera user interface, click the **Setup** link.

**Step 2** Click **Network Setup** to expand the menu.

**Step 3** From the Network Setup menu, click **Time**.

The Time window appears. If you change any options in this window, you must click the **Save** button to save the changes. If you do not click this button, changes are not retained when you exit the window. The **Save** button appears at the bottom of the window. You might need to scroll down to it.

Table 5-3 describes the options in the Time window.

**Table 5-3** Time Window Options

Option	Description
<b>Set Time Mode Area</b>	
Manually Configure Time	Choose this option if you want to set the time for the IP camera manually.
Use NTP Server to Update Time	Choose this option if you want the IP camera to obtain its time from a Network Time Protocol (NTP) server.  If you check this check box, the camera contacts the designated NTP server every 64 seconds and synchronizes its internal clock with the time of that server.
<b>Local Time Area</b>	
<b>Note</b> These options do not apply if you choose the Use NTP Server to Update Time option.	
Set Local Date	Enter a date for the IP camera. The camera is updated with this date when you click <b>Save</b> .
Set Local Time	Enter a time for the IP camera. The camera is updated with this time when you click <b>Save</b> .
<b>Clone PC Time</b> button	Click this button to update the IP camera date and time with the date and time of the PC that you are using.
<b>Time Zone and Daylight Saving Area</b>	
Time Zone	Choose the time zone in which the IP camera is located.  The time that appears when you view video from this IP camera reflects this time zone.
Adjust for Daylight Saving Time	Check this check box if you want the time of the IP camera to adjust automatically for daylight saving time.

**Table 5-3** Time Window Options (continued)

Option	Description
Edit Default Daylight Saving Configuration for Time Zone	Check this check box if you want the daylight saving time adjustment of the IP camera to be different than the default adjustment for the selected time zone.
Time Offset	<p>If you choose to overwrite the default time zone configuration, enter the number of minutes that the time of the camera adjusts when daylight saving time starts.</p> <p>The camera automatically adjusts its time back by this number of minutes when daylight saving time ends.</p>
Start Date Start Time	If you choose to overwrite the default time zone configuration, enter the day and time (in 24 hour format) that daylight saving time begins. At this day and time, the time of the IP camera adjusts by the value in the Time Offset field.
End Date End Time	If you choose to overwrite the default time zone configuration, enter the day and time (in 24 hour format) that daylight saving time ends. At this day and time, the time of the IP camera adjusts to the non-daylight saving time.

**NTP Server Settings Area**

**Note** These options do not apply if you choose the Manually Configure Time option.

Primary NTP Server	If you configured the IP camera to obtain its time from an NTP server, identify the primary NTP server by choosing <b>IP Address</b> or <b>Hostname</b> from the drop-down list and entering the IP address or host name in the corresponding field.
Primary NTP Server Port	<p>If you configured the IP camera to obtain its time from an NTP server, enter the primary NTP server port number.</p> <p>Valid values are 123 and 1024 through 65535. The default port is 123.</p>
Secondary NTP Server	If you configured the IP camera to obtain its time from an NTP server, identify the secondary NTP server by choosing <b>IP Address</b> or <b>Hostname</b> from the drop-down list and entering the IP address or host name in the corresponding field.
Secondary NTP Server Port	<p>If you configured the IP camera to obtain its time from an NTP server, enter the optional secondary NTP server port number.</p> <p>Valid values are 123 and 1024 through 65535. The default port is 123.</p>

## Discovery Window

The Discovery window provides options for configuring the IP camera to work with Cisco Discovery Protocol or Bonjour. These applications facilitate monitoring and management of your network.

To display the Discovery window, perform the following steps:

**Procedure**

- 
- Step 1** From the IP camera user interface, click the **Setup** link.
- Step 2** Click **Network Setup** to expand the menu.

**Step 3** From the Network Setup menu, click **Discovery**.

The Discovery window appears. If you change any options in this window, you must click the **Save** button to save the changes. If you do not click this button, changes are not retained when you exit the window. The **Save** button appears at the bottom of the window. You might need to scroll down to it.

Table 5-4 describes the options in the Discovery window.

**Table 5-4**      **Discovery Window Options**

Option	Description
<b>Cisco Discovery Protocol (CDP) Area</b>	
<b>Show Neighbors</b> button	Display a new window with information about CDP-enabled device neighbors in your network.
<b>Bonjour Area</b>	
Enable Bonjour	Check this check box if Bonjour is enabled in your network and you want the IP camera to broadcast Bonjour discovery messages.
<b>Cisco Video Surveillance Media Server (VSMS) Area</b>	
Enable Preferred Media Server List	Check this check box if you want the camera to send discovery messages to the media server list.
Media Server IP address	Enter the IP addresses for a maximum of four servers to auto discover your camera. They are to be listed in order of preference, such that when VSMS 1 does not respond to the camera's discovery request, the camera sends a registration request to VSMS 2; and continues down the list until the camera is registered.

## Medianet Window

The Media Services Interface (MSI) is a software component that is embedded in video endpoints and collaboration applications. MSI ties the network to user devices and applications that enables an end-to-end architecture called Cisco Medianet.

The Medianet window on the IP cameras contains the Enable Flow Meditate option. By default this setting is enabled to allow metadata about the camera to be sent across the network and to the network elements in the media path.

For more information about Medianet, refer to the *Cisco Video Surveillance Operations Manager User Guide* at the following URL:

[http://www.cisco.com/en/US/products/ps10818/products\\_user\\_guide\\_list.html](http://www.cisco.com/en/US/products/ps10818/products_user_guide_list.html)

To display the Medianet window, perform the following steps:

**Step 1** From the IP camera user interface, click the **Setup** link.

**Step 2** Click **Network Setup** to expand the menu.

**Step 3** From the Network Setup menu, click **Medianet**.

The Medianet window appears. If you change any options in this window, you must click the **Save** button to save the changes. If you do not click this button, changes are not retained when you exit the window. The **Save** button appears at the bottom of the window. You might need to scroll down to it.

Table 5-5 describes the options in the Medianet window.

**Table 5-5 Medianet Window Options**

Option	Description
<b>Medianet Features Area</b>	
Enable Flow Metadata	<p>Check this check box if Medianet is supported in your network. Flow metadata is the data that describes flow in network.</p> <p>Enabling this feature helps with sending metadata across the network and network elements in the media path.</p> <p><b>Note</b> This feature is enabled by default.</p>

## SNMP Window

The SNMP window provides options for configuring Simple Network Management Protocol (SNMP) settings for the IP camera. These settings can help you manage complex networks by sending messages to different devices on the network.

To display the SNMP window, perform the following steps:

- Step 1** From the IP camera user interface, click the **Setup** link.
- Step 2** Click **Network Setup** to expand the menu.
- Step 3** From the Network Setup menu, click **SNMP**.

The SNMP window appears. If you change any options in this window, you must click the **Save** button to save the changes. If you do not click this button, changes are not retained when you exit the window. The **Save** button appears at the bottom of the window. You might need to scroll down to it.

Table 5-6 describes the options in the SNMP window.

**Table 5-6 SNMP Window Options**

Option	Description
<b>SNMP v2c Area</b>	
Enable SNMP v2c	Check this check box to enable SNMP v2c.
Read Community String	Enter the SNMP read community string, which identifies the valid read community.
Trap Community String	Enter the SNMP trap community string.
Primary Trap Receiver	Identify the primary trap receiver of the SNMP v2c manager by choosing <b>IP Address</b> or <b>Hostname</b> from the drop-down list and entering the IP address or host name in the corresponding field.

**Table 5-6** *SNMP Window Options (continued)*

Option	Description
Secondary Trap Receiver	Identify an optional secondary trap receiver of the SNMP v2c manager by choosing <b>IP Address</b> or <b>Hostname</b> from the drop-down list and entering the IP address or host name in the corresponding field.
<b>SNMP v3 Area</b>	
Enable SNMP v3	Check this check box to enable SNMP v3.
Use Default Local Engine ID	Click this radio button if you want to use the default local engine ID for SNMP.  The default local engine ID is 8000000903<MAC>, where <MAC> is the MAC address of the IP camera.
Manually Configure Local Engine ID	Click this radio button if you want to enter a local engine ID manually, then enter a unique local engine ID.  Enter this information in a standard format as defined in RFC3411. Valid formats include (but are not limited to) the following: <ul style="list-style-type: none"> <li>8000000903&lt;MAC&gt; where &lt;MAC&gt; is the MAC address of the IP camera. For example, if the IP camera MAC address is 00:04:9F:11:22:33, enter 800000090300049F112233. This format is the default.</li> <li>8000000901&lt;IPv4_address_hex&gt; where &lt;IPv4_address_hex&gt; is the IPv4 address of the IP camera in hexadecimal format. For example, if the IP camera IPv4 address is 192.168.0.100, enter 8000000901C0A80064.</li> <li>8000000904&lt;text&gt; where &lt;text&gt; is a string of up to 54 characters.</li> </ul>
Primary Trap Receiver	Identify the primary trap receiver of the SNMP v3 manager by choosing <b>IP Address</b> or <b>Hostname</b> from the drop-down list and entering the IP address or host name in the corresponding field.
Secondary Trap Receiver	Identify an optional secondary trap receiver of the SNMP v3 manager by choosing <b>IP Address</b> or <b>Hostname</b> from the drop-down list and entering the IP address or host name in the corresponding field.
User #	<i>Display only.</i> Lists the user number of each IP camera user who is configured with the administrator privilege level.
User Name	<i>Display only.</i> Displays the name that is associated with the corresponding user number
Authentication Method	Choose the authentication protocol for SNMP v3 messages that are sent on behalf of the corresponding user.
Authentication Password	Enter a password for the authentication protocol for SNMP v3 messages that are sent on behalf of the corresponding user.  This password can contain from 8 to 63 characters, which can be letters, numbers, and special characters, but no spaces. Special characters are: ! \$ ( ) - . @ ^ _ ` { } ~

**Table 5-6** *SNMP Window Options (continued)*

Option	Description
Privacy Method	Choose <b>DES</b> if you want to use this privacy method for SNMP v3 messages that are sent on behalf of the corresponding user.  If you do not want to use a privacy method, choose <b>None</b> .
Privacy Password	If you choose a privacy method, enter a password for SNMP v3 messages that are sent on behalf of the corresponding user.  This password can contain from 8 to 63 characters, which can be letters, numbers, and special characters, but no spaces. Special characters are: ! \$ ( ) - . @ ^ _ ` { } ~

## 802.1x Window

The 802.1x window provides options for configuring 802.1x authentication for the IP camera. These settings require that RADIUS be configured on your network to provide the client authentication.

To display the 802.1x window, perform the following steps:

**Step 1** From the IP camera user interface, click the **Setup** link.

**Step 2** Click **Network Setup** to expand the menu.

**Step 3** From the Network Setup menu, click **802.1x**.

The 802.1x window appears. If you change any options in this window, you must click the **Save** button to save the changes. If you do not click this button, changes are not retained when you exit the window. The **Save** button appears at the bottom of the window. You might need to scroll down to it.

[Table 5-7](#) describes the options in the 802.1x window.

**Table 5-7** *802.1x Window Options*

Option	Description
<b>802.1x Settings Area</b>	
Enable 802.1x	Check this check box to enable 802.1x authentication for the IP camera.
Protocol Type	Choose the protocol for 802.1x authentication. Options are <ul style="list-style-type: none"> <li>• EAP-TLS</li> <li>• EAP-TTLS</li> <li>• EAP-PEAP</li> <li>• EAP-FAST</li> </ul> The remaining fields in this window change depending on the protocol type that you choose.
<b>EAP-TLS Configuration Options</b>	
<b>Note</b> These options appear if you select the protocol type <b>EAP-TLS</b> .	
User Name	Enter the user name that the IP camera uses to access the RADIUS server.



**Table 5-7 802.1x Window Options (continued)**

Option	Description
Device (Client) Certificate	Path and folder where the device certificate for the IP camera is stored. You can click <b>Browse</b> to find this location.  After you enter this information, click <b>Upload</b> to upload the certificate to the IP camera.
Password (for Private Key)	If the private key in the device certificate is password protected, enter the password that is required to unlock the private key.
Root CA Certificate	Path and folder where the root certificate that is required for 802.1x authentication is stored. You can click <b>Browse</b> to find this location.  After you enter this information, click <b>Upload</b> to upload the certificate to the IP camera.

**EAP-TTLS Configuration Options**

**Note** These options appear if you select the protocol type **EAP-TTLS**.

Inner Authentication	Choose an inner authentication method for EAP-TTLS. Options are <b>MS-CHAP</b> , <b>MS-CHAP v2</b> , <b>PEAP</b> , and <b>EAP-MDS</b> .
User Name	Enter the user name that the IP camera uses to access the RADIUS server.
Password	Enter the password that the IP camera uses to access the RADIUS server.
Anonymous ID	<i>Optional.</i> Unsigned public identifier to be used instead of a user name for logging in to the RADIUS server.
Validate Server Certificate	Check this check box if you want the identity of the RADIUS server to be validated.
Root CA Certificate	Path and folder where the root certificate that is required for 802.1x authentication is stored. You can click <b>Browse</b> to find this location.  After you enter this information, click <b>Upload</b> to upload the certificate to the IP camera.

**EAP-PEAP Configuration Options**

**Note** These options appear if you select the protocol type **EAP-PEAP**.

Inner EAP Protocol	Choose an inner authentication method for EAP-PEAP.
User Name	Enter the user name that the IP camera uses to access the RADIUS server.
Password	Enter the password that the IP camera uses to access the RADIUS server.
Anonymous ID	<i>Optional.</i> Anonymous identifier to be used instead of a user name for logging in to the RADIUS server.
Validate Server Certificate	Check this check box if you want the identity of the RADIUS server to be validated.
Root CA Certificate	Path and folder where the root certificate that is required for 802.1x authentication is stored. You can click <b>Browse</b> to find this location.  After you enter this information, click <b>Upload</b> to upload the certificate to the IP camera.

**EAP-FAST Configuration Options**

**Note** These options appear if you select the protocol type **EAP-FAST**.

Inner EAP Protocol	Choose an inner authentication method for EAP-FAST.
--------------------	-----------------------------------------------------

**Table 5-7** 802.1x Window Options (continued)

Option	Description
User Name	Enter the user name that the IP camera uses to access the RADIUS server.
Password	Enter the password that the IP camera uses to access the RADIUS server.
Anonymous ID	<i>Optional.</i> Anonymous identifier to be used instead of a user name for logging in to the RADIUS server.

## IP Filter Window

The IP Filter window provides options for controlling access to the IP camera by designating a maximum of 10 IP addresses or address ranges that are allowed or denied access to the IP camera.

To display the IP Filter window, perform the following steps:

### Procedure

- 
- Step 1** From the IP camera user interface, click the **Setup** link.
- Step 2** Click **Network Setup** to expand the menu.
- Step 3** From the Network Setup menu, click **IP Filtering**.

The IP Filter window appears. If you change any options in this window, you must click the **Save** button to save the changes. If you do not click this button, changes are not retained when you exit the window. The **Save** button appears at the bottom of the window. You might need to scroll down to it.

---

Table 5-8 describes the options in the IP Filter window.

**Table 5-8** IP Filter Window Options

Option	Description
<b>IP Filter Area</b>	
Enable IP Filtering	Check this check box to cause the IP camera to allow or deny access to IP addresses as configured in the IP Filtering window.
<b>Filter Entries Area</b>	
#	<i>Display only.</i> Filter number.
Action	Choose an action for the corresponding IP address or address range: <ul style="list-style-type: none"> <li><b>Deny</b>—IP address or address range cannot access the IP camera.</li> <li><b>Allow</b>—IP address or address range can access the IP camera.</li> </ul>
IP Address/Bit Mask	Enter the IP address and bit mask to which the corresponding action applies. Make these entries in Classless Inter-Domain Routing (CIDR) notation. CIDR is defined in RFC 4632.

# QoS Window

The QoS window provides options for configuring quality of service (QoS) settings for audio/video streams.

To display the QoS window, perform the following steps:

## Procedure

- Step 1** From the IP camera user interface, click the **Setup** link.
- Step 2** Click **Network Setup** to expand the menu.
- Step 3** From the Network Setup menu, click **QoS**.

The QoS window appears. If you change any options in this window, you must click the **Save** button to save the changes. If you do not click this button, changes are not retained when you exit the window. The **Save** button appears at the bottom of the window. You might need to scroll down to it.

Table 5-9 describes the options in the QoS window.

**Table 5-9 QoS Window Options**

Option	Description
<b>Class of Service (CoS) Area</b>	
Enable CoS for Video Streaming	Check this check box to enable class of service (CoS) control for video streams.  If you enable this option, the IP camera specifies a VLAN tag that appends to an Ethernet MAC frame for video streaming data.
Video Priority	Choose a value from 0 (lowest priority) through 7 (highest priority) that specifies the CoS priority value for streaming video data.
Video VLAN ID	Enter the ID of the video VLAN to which CoS packets are directed.
Enable CoS for Audio Streaming	Check this check box to enable CoS control for audio streams.
Audio Priority	Choose a value from 0 (lowest priority) through 7 (highest priority) that specifies the CoS priority value for streaming audio data.
Audio VLAN ID	Enter the ID of the audio VLAN to which CoS packets are directed.
<b>Differentiated Services (DiffServ) Area</b>	
Enable DiffServ for Video Streaming	Check this check box to enable Differentiated Services (DiffServ) for video streams.  If you enable this option, the IP camera specifies the DSCP priority value that appends to an IP header for video streaming packets.
Video DSCP Priority Value	Enter a value from 0 (lowest priority) through 63 (highest priority) that specifies the DSCP priority value for streaming video data.
Enable DiffServ for Audio Streaming	Check this check box to enable DiffServ for audio streams.

**Table 5-9**      **QoS Window Options (continued)**

Option	Description
Audio DSCP Priority Value	Enter a value from 0 (lowest priority) through 63 (highest priority) that specifies the DSCP priority value for streaming audio data.



# Application Manager

The Application Manager windows let you configure and manage apps for the IP camera. Apps let you extend the functionality of a supported Cisco IP Camera. For related information, see *Cisco IP Camera Apps Reference Guide*.

The following sections describe the Application Manager windows in detail:

- [Configuration Window, page 6-1](#)
- [App License Window, page 6-2](#)
- [App Setup Window, page 6-3](#)
- [Managing Apps, page 6-5](#)

## Configuration Window

The Initialization window provides options enabling Apps on the IP camera, and for enabling audio and video for apps that support these features.

To display the Configuration window, perform the following steps:

### Procedure

- Step 1** From the IP camera user interface, click the **Setup** link.
- Step 2** Click **Application Manager** to expand the menu.
- Step 3** From the Application Manager menu, click **Configuration**.

The Initialization window appears. If you change any options in this window, you must click the **Save** button to save the changes. If you do not click this button, changes are not retained when you exit the window. The **Save** button appears at the bottom of the window. You might need to scroll down to it.

[Table 6-1](#) describes the options in the Configuration window.

**Table 6-1 Configuration Window Options**

Option	Description
Enable Applications	Check this check box if you want to allow apps to run on the IP camera.

**Table 6-1 Configuration Window Options (continued)**

Option	Description
<b>Video Area</b>	
Enable Video	Check this check box to enable video for installed apps that support video. Before you can enable video, Stream 2 and Analog Video must be disabled. For Stream 1, Maximum Frame Rate should be set to a value of 15 fps or less and Video Resolution should be set to a value of 1920x1080 or less, as described in the <a href="#">“Streaming Window” section on page 4-1</a> .
Resolution	Select the video resolution for installed apps that support video.
<b>Audio Area</b>	
Enable Audio	Check this check box to enable audio for installed apps that support audio. Before you can enable audio, Stream 2 and audio for Stream 1 must be disabled.
Sampling Frequency	<i>Display only.</i> Sampling frequency of audio from the IP Camera for installed apps that support audio (16 kHz).

## App License Window

The App License window lets you install and uninstall licenses for apps, and provides information about licenses that are installed on the IP camera.

The appropriate license must be installed on an IP camera before an app is installed on the camera. Before you can install a license, obtain a valid license from Cisco and save the license file on your local PC or on a PC that you can access from your local PC.

To display the App License window, perform the following steps:

### Procedure

- 
- Step 1** From the IP camera user interface, click the **Setup** link.
- Step 2** Click **Application Manager** to expand the menu.
- Step 3** From the Application Manager menu, click **App License**.
- 

[Table 6-2](#) describes the options in the App License window.

**Table 6-2 App License Window Options**

Option	Description
<b>License Installation Area</b>	
License File	To install a license file, use the <b>Browse</b> button to navigate to the file, select the file to enter it in the License File field, and then click <b>Install License</b>

**Table 6-2**      *App License Window Options (continued)*

Option	Description
<b>Installed License List Area</b>	
License list	Provides this information for each license that is installed on the IP camera: <ul style="list-style-type: none"> <li>• License Type—Name of the license</li> <li>• Total—Number of corresponding license types that are currently installed</li> <li>• Used—Number of corresponding license types that are in use</li> <li>• Free—Number of corresponding license types that are available</li> </ul>
<b>Uninstall License</b> button	To remove all instances of a license, click the radio button that corresponds to the license, click <b>Uninstall License</b> , and then click <b>OK</b> in the confirmation dialog box

## App Setup Window

The App Setup window lets you install, uninstall, configure, start, and stop apps, and perform related operations.

The appropriate license must be installed on an IP camera before you install the app (see the “[App License Window](#)” section on page 6-2).

Some operations that you perform in the App Setup window can take several minutes to complete. Do not turn off or restart the IP camera while an operation is in progress.

To display the App Setup window, perform the following steps:

### Procedure

- 
- Step 1** From the IP camera user interface, click the **Setup** link.
- Step 2** Click **Application Manager** to expand the menu.
- Step 3** From the Application Manager menu, click **App Setup**.
- 

[Table 6-3](#) describes the options in the App Setup window.

**Table 6-3**      *App License Window Options*

Option	Description
<b>Application Installation Area</b>	
Application package	Name of the application to install.
Browse button	Click to display a window that you can use to navigate to and choose the application to install.
Install button	Click to install the application that is specified in the Application package field.

**Table 6-3**      **App License Window Options (continued)**

Option	Description
<b>Installed Application List Area</b>	
Application list	<p>Provides this information for each app that is installed on the IP camera:</p> <ul style="list-style-type: none"> <li>• <b>Select</b>—Click the radio button that corresponds to an app to start, stop, configure, or uninstall the app</li> <li>• <b>Application</b>—Name of the app</li> <li>• <b>Version</b>—Version of the app</li> <li>• <b>Vendor</b>—Provider of the app</li> <li>• <b>Status</b>—Operating status of the app (Running or Stopped)</li> <li>• <b>Start on Boot?</b>—To cause an app to run automatically each time the IP camera restarts, click the radio button for the app, check this check box, and then click <b>Run</b></li> <li>• <b>Installed On</b>—Date and time that the app was installed on the IP camera</li> <li>• <b>Started On</b>—Date and time that a running app was last started</li> <li>• <b>Package Detail</b>—Name of the app package that was installed</li> </ul>
<b>Run</b> button	<p>To run an app, click the radio button in the Select column that corresponds to the app, then click <b>Run</b>.</p> <p>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.</p>
<b>Stop</b> button	<p>To stop an app that is running, click the radio button in the Select column that corresponds to the app, click <b>Stop</b>, and then click <b>OK</b> in the confirmation dialog box.</p>
<b>Configure</b> button	<p>To configure an app, click the radio button in the Select column that corresponds to the app, then click <b>Configure</b>.</p> <p>The configuration window for the app appears. The options in this window depend on the app. For detailed information, see <i>Cisco IP Camera Apps Reference Guide</i>.</p> <p>If you configure an app that is running, you must stop and then restart the app before the changes take effect.</p>
<b>Uninstall</b> button	<p>To permanently remove an app from the IP camera, click the radio button in the Select column that corresponds to the app, <b>Uninstall</b>, and then click <b>OK</b> in the confirmation dialog box.</p> <p>You must stop a running app before you can uninstall it.</p>
<b>Maintenance Area</b>	
<b>Restore</b> button	<p>Click this button to reset all app manager settings to their factory default values and permanently remove all apps from the IP camera.</p> <p>This button should be used only if the IP camera becomes unstable after an app is installed or run.</p>



# Managing Apps

The following sections provide detailed instructions for managing apps on an IP camera:

- [Installing a License for an App, page 6-5](#)
- [Configuring an App, page 6-6](#)
- [Configuring Event Triggering, page 6-6](#)
- [Running an App, page 6-7](#)
- [Stopping an App, page 6-7](#)
- [Uninstalling an App, page 6-8](#)
- [Restoring the Application Manager, page 6-8](#)

## Installing a License for an App

The appropriate license must be installed on a camera before the corresponding app package is installed on the camera.

To install a license on an IP camera, follow these steps:

### Procedure

- 
- |               |                                                                                                                                                       |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Obtain a valid app license from Cisco for the app and save the license file on your local PC or on a PC that you can access from your local PC.       |
| <b>Step 2</b> | From the IP camera user interface, click the <b>Setup</b> link, click <b>Application Manager</b> to expand the menu, then choose <b>App License</b> . |
| <b>Step 3</b> | Click <b>Browse</b> next to the License file field and navigate to the license file that you saved.                                                   |
| <b>Step 4</b> | Select the license file and click <b>Install License</b> .                                                                                            |
- 

## Installing an App on an IP Camera

Before you can run an app on an IP camera, the app must be installed on the IP camera. To install an app, perform the following steps.

### Before You Begin

Install the appropriate license for the app on the IP camera as described in the [“Installing a License for an App”](#) section on page 6-5.

### Procedure

- 
- |               |                                                                                                                                                     |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | From the IP camera user interface, click the <b>Setup</b> link, click <b>Application Manager</b> to expand the menu, then choose <b>App Setup</b> . |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|

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 are redirected to Configuration window where you can enable application support on camera.”

- Step 2** If the Application support dialog box appears, take these actions:
- Click **OK** to display the Configuration window.
  - In the Configuration window, check the **Enable Application** check box.
  - (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.
  - (Optional) Check the **Enable Audio** check box if you will run applications that use the audio features of the camera.
  - Click **Save**.
  - 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 install.
- 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.
- 

## Configuring an App

After you install an app on an IP camera, you must configure its operation.

To configure the operation of an 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 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.
- For detailed information about configuration settings for a particular app, see *Cisco IP Camera Apps Reference Guide*.
- 

## Configuring Event Triggering

This section describes how to enable event triggering on an IP camera, which allows apps that support triggers to cause the camera to take certain actions when an event occurs.

To enable the triggering of actions by apps that support triggers, follow these steps:

- 
- Step 1** From the IP camera user interface, click the **Setup** link, click **Feature Setup** to expend the menu, then choose **Event**.
- Step 2** In the Event Notification window, take these actions:
- Check the **App** check box in the Event Triggering area.
  - Check one of more of the Actions check boxes for the App option in the Event Triggering area to designate the action that the IP camera takes when it receives an event trigger.
  - Click **Set All** in the Event Scheduling area.
  - Click **Save** at the bottom of the window.
- Step 3** From the Setup menu in the web-based interface of the camera, click **Log** to expend the menu, then choose **Setup**.
- Step 4** In the Log Setup window, take these actions:
- Check the **Enable Syslog** check box in the Syslog Settings area.
  - Enter the IP address of the server on which to log events.
  - Click **Save** at the bottom of the window.
- 

## Running an App

To run an 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 app that you want to run.
- Step 3** Click the **Run** button.
- 

## Stopping an App

To stop an 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 app that you want to stop.
- Step 3** Click the **Stop** button.
-

## Uninstalling an App

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

If the app is running, you must first stop it as described in the [“Stopping an App” section on page 6-7](#).

### Procedure

---

- Step 1** From the IP camera user interface, click the **Setup** link, click **Application Manager** to expand the menu, then click **App Setup**.
  - Step 2** Click the radio button for the 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 apps that you uploaded to the IP camera are removed from the camera.

This feature should be used only if the IP camera becomes unstable after an app is installed or run.

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 expand 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**.
-



## CHAPTER

# 7

## Administration

---

The Administrator windows let you perform several general administrative operations, including enabling HTTP and HTTPS access to the IP camera, configuring users, resetting or rebooting the IP camera, and updating firmware.

The following sections describe the Administration windows in detail:

- [Initialization Window, page 7-1](#)
- [User Window, page 7-3](#)
- [Maintenance Window, page 7-4](#)
- [Firmware Window, page 7-6](#)
- [Device Processes Window, page 7-7](#)
- [Password Complexity Window, page 7-8](#)

## Initialization Window

The Initialization window provides options for configuring passwords for the IP camera default administrator accounts, and for configuring which protocols can be used to access the IP camera.

The IP camera always has an HTTP/HTTPS administrator who can access the IP camera through an HTTP or HTTPS connection. The name of this administrator is **admin**. The password is configurable.

If you want to access the IP camera through SSH, you must configure a password for an SSH administrator. The name of this administrator is **root**. The password is configurable.

To display the Initialization window, perform the following steps:

### Procedure

---

- Step 1** From the IP camera user interface, click the **Setup** link.
- Step 2** Click **Administration** to expand the menu.
- Step 3** From the Administration menu, click **Initialization**.

The Initialization window appears. If you change any options in this window, you must click the **Save** button to save the changes. If you do not click this button, changes are not retained when you exit the window. The **Save** button appears at the bottom of the window. You might need to scroll down to it.

---

Table 7-1 describes the options in the Initialization window.

**Table 7-1 Initialization Window Options**

Option	Description
<b>Administrator Accounts Area</b>	
Protocol	<i>Display only.</i> Indicates the protocol that the corresponding administrator can use to access the IP camera: HTTP/HTTPS or SSH
User Name	<i>Display only.</i> Indicates the default user name for the corresponding administrator: admin or root
Password	Enter a password for the corresponding administrator. The password is case sensitive and must contain from 8 to 32 characters, which can be letters, numbers, and special characters, but no spaces. Special characters are: ! \$ ( ) - . @ ^ _ ` { } ~
Confirm Password	Re-enter the password for the corresponding administrator.
<b>Access Protocols Area</b>	
Enable HTTP	Check this check box if you want to allow HTTP connections to the IP camera.
HTTP Port	Enter the HTTP port that is used to access the IP camera. Valid port numbers are 80 and 1024 through 32767. The default port is 80.  If you configure the HTTP port to a value other than 80, you must specify the port number in the URL for the IP camera when you access it through an HTTP connection. For example, if the IP address of the IP camera is 192.168.1.100 and the HTTP port is 1024, enter this URL for the IP camera: http://192.168.1.100:1024.
Enable HTTPS	Check this check box if you want to allow HTTPS connections to the IP camera.
HTTPS Port	Enter the HTTPS port that is used to access the IP camera. Valid port numbers are 443 and 1024 through 65535. The default port is 443.  If you configure the HTTPS port to a value other than 443, you must specify the port number in the URL for the IP camera when you access it through an HTTPS connection. For example, if the IP address of the IP camera is 192.168.1.100 and the HTTPS port is 1024, enter this URL for the IP camera: https://192.168.1.100:1024.
Enable Secure Shell (SSH)	Check this check box if you want to allow access to the camera through an SSH connection.
Secure Shell (SSH) Port	Enter the SSH port that is used to access the IP camera. Valid port numbers are 22 and 1024 through 65535. The default port is 22.

# User Window

The User window lets you configure the following types of IP camera users:

- Administrator—Can access all IP camera windows, features, and functions.
- Viewer—Can access only the Camera Video & Control window and all features in that window except:
  - Video controls
  - Camera Settings
  - Motion Detection controls
  - Focus/Zoom controls
  - Privacy Zone

There is always at least one user with Administrator privileges configured. The user name of this user is “admin.” You can configure up to four additional users and assign privilege levels to each one.

When you configure users, follow these guidelines:

- After you enter a name, password, and privilege level for a user, click **Add** next to the user information to save your changes.
- To change the password for an existing user, click **Change** next to the user name.
- To remove a user, click **Delete** next to the user. If you delete a user who is logged into the IP camera, the user remains logged in and can continue access the IP camera.
- To change the name of a user, you must delete the user then create a new user.

To display the User window, perform the following steps:

## Procedure

- 
- Step 1** From the IP camera user interface, click the **Setup** link.
- Step 2** Click **Administration** to expand the menu.
- Step 3** From the Administration menu, click **Users**.
- The User window appears.
- 

Table 7-2 describes the options in the User window.

**Table 7-2 User Window Options**

Option	Description
<b>User List Area</b>	
User Name	<p>Enter a unique name for the user.</p> <p>The user name is case sensitive and can include up to 32 letters, numbers, and special characters, but no spaces. Special characters are: ! % ( ) + , - = @ _ ~</p> <p>There is always one user named admin (all lower case), which cannot be deleted.</p>

**Table 7-2**      *User Window Options (continued)*

Option	Description
Password	Enter a password for the user.  The password is case sensitive and must contain from 8 to 32 characters, which can be letters, numbers, and special characters, but no spaces. Special characters are: ! \$ ( ) - . @ ^ _ ` { } ~
Confirm Password	Re-enter the password for the user.
Privilege Level	Select the desired privilege level for the user: <ul style="list-style-type: none"> <li>• <b>Administrator</b>—Can access all IP camera windows, features, and functions.</li> <li>• <b>Viewer</b>—Can access the Camera Video &amp; Control window with limited controls, and can access the <b>Refresh</b>, <b>Logout</b>, <b>About</b>, and <b>Help</b> links from that window.</li> </ul>
<b>Change</b> button	Click this button to change the password of the corresponding user.
<b>Add</b> button	Click this button to add the corresponding user. That user can then log in to the IP camera.
<b>Delete</b> button	Click this button to remove the corresponding user. This user can no longer log in to the IP camera.

## Maintenance Window

The Maintenance window provides options for setting or restarting the IP camera, saving configuration information from the IP camera, and uploading the configuration information to the IP camera.

Saving and uploading configuration is useful for these activities:

- **Configuring multiple IP cameras**—If your network includes several IP cameras that should have similar configurations, you can configure one IP camera, save that configuration, and upload it to other IP cameras. Then, instead of manually configuring all options on each IP camera, you manually configure only the options that are unique, such as the IP address, if not obtained from DHCP.
- **Backing up configuration**—If you save the configuration from the IP camera, you can upload it to the IP camera to restore the configuration if it is lost. You can upload it to a replacement IP camera, if needed.

To display the Maintenance window, perform the following steps:

### Procedure

- 
- Step 1** From the IP camera user interface, click the **Setup** link.
- Step 2** Click **Administration** to expand the menu.
- Step 3** From the Administration menu, click **Maintenance**.
- The Maintenance window appears.
- 

Table 7-3 describes the options in the Maintenance window.



**Table 7-3**      **Maintenance Window Options**

Option	Description
<b>Factory Default Area</b>	
<b>Restore</b> button	<p>Click the <b>Restore</b> button to reset all IP camera settings to their factory default values.</p> <p>To confirm the restore procedure, click <b>OK</b> in the confirmation pop-up window. Otherwise, click <b>Cancel</b>.</p> <p>This action has the same effect as pressing and holding the <b>Reset</b> button on the IP camera for at least 15 seconds. After you perform this procedure, follow the steps in the <a href="#">Chapter 2, “Performing the Initial Setup of the IP Camera.”</a></p>
<b>Reset</b> button	<p>Click the <b>Reset</b> button to reset all IP camera settings except the static IP address, gateway IP address, and log in credentials (user name and password) to their factory default values.</p> <p>To confirm the restore procedure, click <b>OK</b> in the confirmation pop-up window. Otherwise, click <b>Cancel</b>.</p>
<b>Reboot Area</b>	
<b>Reboot</b> button	<p>Click the <b>Reboot</b> button to reboot the software on IP camera.</p> <p>To confirm the reboot procedure, click <b>OK</b> in the confirmation pop-up window. Otherwise, click <b>Cancel</b>.</p> <p>This action has the same effect as pressing and immediately releasing the Reset button on the IP camera, or powering the IP camera down and then powering it up.</p>
<b>Device Configuration Area</b>	
Export Configuration from Camera	<p>Click the <b>Export</b> button to save the current IP camera configuration information to a binary file.</p> <p>Check the Exclude Network Basic and IP Addressing Setting check box if you do not want the configuration to contain network basic configuration information and the IP address of the camera.</p> <p>When you click this button, the File Download window appears. Use this window to save the configuration file.</p> <p>You can then load this configuration information to any same-model IP camera in the network. This feature is useful for creating a backup of this configuration and for configuring other IP cameras based on this configuration.</p>

**Table 7-3 Maintenance Window Options (continued)**

Option	Description
Import Configuration to Camera	<p>Path and folder where a configuration file is stored. You can click <b>Browse</b> to find this location. After you enter this information, click <b>Import</b> to load the configuration file to the IP camera.</p> <p>After you upload a configuration file to the IP camera, the IP camera restarts automatically.</p> <p>If you upload configuration from another IP camera that is active in your network, make sure to configure this IP camera with a name, description, and unique IP address (if not obtained through DHCP). To change these options, see the “<a href="#">Basic Window</a>” section on page 5-1 and the “<a href="#">IP Addressing Window</a>” section on page 5-3.</p> <p>A configuration file that you upload includes the passwords that are configured for the administrator and for users. If you change any passwords after saving the configuration file, be aware that uploading the file overwrites the new passwords with the saved ones.</p>
<b>Camera Logs Area</b>	
Export Logs from Camera	<p>Click the <b>Export</b> button to save the current IP camera log information in .tar.gz format.</p> <p>When you click this button, the File Download window appears. Use this window to save the log file.</p> <p>Depending on the size of logs it may take some time to download the logs.</p>
Clear Logs from Camera	Click the <b>Clear</b> button from the Camera Logs section to clear the camera log information from the IP camera. Depending on the amount of log information, it may take some time to clear the information.

## Firmware Window

The Firmware window lets you view information about the firmware that is installed on the IP camera and upgrade the firmware.

Before you upgrade firmware, download the firmware file to a PC that is accessible on your network and unzip the file if it is zipped. To download firmware, go to this web page:

[http://www.cisco.com/en/US/products/ps6918/Products\\_Sub\\_Category\\_Home.html](http://www.cisco.com/en/US/products/ps6918/Products_Sub_Category_Home.html)

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

To display the Firmware window, perform the following steps:

### Procedure

- 
- Step 1** From the IP camera user interface, click the **Setup** link.
  - Step 2** Click **Administration** to expand the menu.
  - Step 3** From the Administration menu, click **Firmware**.

The Firmware window appears.

Table 7-4 describes the options in the Firmware window.

**Table 7-4 Firmware Window Options**

Option	Description
<b>Device Information Area</b>	
IP Address	<i>Display only.</i> IP address of the IP camera
MAC Address	<i>Display only.</i> MAC address of the IP camera.
Device Name	<i>Display only.</i> ID of the IP camera, as configured in the Basic window. For more information, see the “ <a href="#">Basic Window</a> ” section on page 5-1.
<b>Firmware Maintenance Area</b>	
Firmware Version	Version of the firmware that is installed on the IP camera.
Firmware Released Date	Release date of the current firmware.
<b>Details</b> button	Click this button to display a pop-up window with additional information about the firmware on the IP camera (for example, bootloader version).
Firmware Upgrade	To upgrade the firmware on the IP camera, begin by entering the path and folder where the new firmware file for the IP camera is stored. The upgrade file might be stored on another PC. Click <b>Browse</b> to find this location.
<b>Upgrade</b> button	After entering the path and folder for the firmware file, click this button to load the firmware upgrade on the IP camera.  Do not power down the IP camera during the upgrade procedure.

## Device Processes Window

The Device Processes window displays the processes that occupy TCP or UDP ports, and lets you stop any of these processes.



### Note

To stop any process, click the **Delete** button that appears to the right of the process in the window.

Take care when stopping processes because some processes are required for the camera to operate properly. Processes that you stop in this window can restart the next time that you log in to the IP camera. If you delete a required process and the camera stops functioning, exit your web browser and then log back in to the IP camera to restart the process. If the process does not restart, power the IP camera off and then back on.

To display the Device Processes window, perform the following steps:

### Procedure

- Step 1** From the IP camera user interface, click the **Setup** link.
- Step 2** Click **Administration** to expand the menu.

- Step 3** From the Administration menu, click **Device Processes**.  
The Device Processes window appears.

Table 7-5 describes the options in the Device Processes window. All options are for display only.

**Table 7-5** *Device Processes Window Options*

Option	Description
Protocol	Port (tcp or udp) that the process occupies
Local Address	IP address of the device that the process is listening to
Foreign Address	IP address and port number of the client device that is connected for the process
State	State of the process
Program Name	Name of the process

## Password Complexity Window

IP camera administrator and user passwords must always meet the requirements that are described in the “[User Window](#)” section on page 7-3. The Password Complexity window provides options for configuring additional requirements for the IP camera passwords.

To display the Password Complexity window, perform the following steps:

### Procedure

- Step 1** From the IP camera user interface, click the **Setup** link.  
**Step 2** Click **Administration** to expand the menu.  
**Step 3** From the Administration menu, click **Password Complexity**.

The Password Complexity window appears. If you change any options in this window, you must click the **Save** button to save the changes. If you do not click this button, changes are not retained when you exit the window. The **Save** button appears at the bottom of the window. You might need to scroll down to it.

Table 7-6 describes the options in the Password Complexity window.

**Table 7-6** *Password Complexity Window Options*

Option	Description
Password must contain at least three of the following: lower case letters, upper case letters, digits, and special characters	Password must contain characters from at least 3 of these categories: <ul style="list-style-type: none"> <li>• Lower case letters (a through z)</li> <li>• Upper case letters (A through Z)</li> <li>• Digits (0 through 9)</li> <li>• Special characters: ! " # \$ % &amp; ' ( ) * + , - . : ; &lt; = &gt; ? @ [ \ ] ^ _ ` {   } ~</li> </ul>

**Table 7-6** Password Complexity Window Options (continued)

Option	Description
Password cannot include any character that occurs three or more times consecutively	Administrator password cannot include any character that occurs 3 or more times in a row.
Password cannot be a repeat or reverse of the user name	Password cannot be the same as the user name either forward or reversed.





## CHAPTER 8

# Log Configuration

---

The Log windows let you set up and view the IP camera log file, which captures information about the IP camera and its activities.

The IP camera stores the log file in its internal SDRAM. If the SDRAM becomes full, the IP camera begins to overwrite existing information. To avoid losing log information, you can configure the IP camera to send log information to a Syslog server.



### Caution

Because the logs are stored in the internal camera SDRAM, all existing logs in the camera are lost after a camera reboot, power-up, or power-down.

---

The following sections describe the Log windows in detail:

- [Log Setup Window, page 8-1](#)
- [Local Log Window, page 8-4](#)

## Log Setup Window

The Log Setup window provides options for configuring the log file and an optional Syslog server on which to store log files.

To display the Log Setup window, perform the following steps:

### Procedure

---

- Step 1** From the IP camera user interface, click the **Setup** link.
- Step 2** Click **Log** to expand the menu.
- Step 3** From the Log menu, click **Setup**.

The Log Setup window appears. If you change any options in this window, you must click the **Save** button to save the changes. If you do not click this button, changes are not retained when you exit the window. The **Save** button appears at the bottom of the window. You might need to scroll down to it.

---

[Table 8-1](#) describes the options in the Log Setup window.

**Table 8-1 Log Setup Window Options**

Option	Description
<b>Local Log Settings Area</b>	
Minimum Log Severity	<p>Choose the minimum severity of messages that the appear in the log file. The system logs all messages of this severity and higher. Message severities, from highest to lowest, are:</p> <ul style="list-style-type: none"> <li>• <b>Emergency</b>—The system is unusable.</li> <li>• <b>Alert</b>—A situation occurred that requires immediate action.</li> <li>• <b>Critical</b>—A situation occurred that requires action soon.</li> <li>• <b>Error</b>—An error occurred, but it does not necessarily affect the ability of the system to function.</li> <li>• <b>Warning</b>—A undesirable condition occurred.</li> <li>• <b>Notice</b>—Notification about a system condition that is not necessarily an error condition.</li> <li>• <b>Informational</b>—Information about a system activity.</li> <li>• <b>Debug</b>—Information about a system activity with detailed technical information. Includes messages of every other severity.</li> </ul> <p>The default severity is Informational.</p>
Maximum Log Entries	<p>Maximum number of entries that the log file maintains. When the log file reaches this limit, it begins overwriting entries, starting with the oldest one.</p> <p>The default value is 100.</p>
<b>Syslog Settings Area</b>	
Enable Syslog	<p>Check this check box to send the log information to a designated Syslog server. The selected information also is maintained on the IP camera until it is overwritten.</p> <p>This option is useful for consolidating logs in deployments with several IP cameras and for retaining logs.</p>
Primary Syslog Server	Identify the primary Syslog server by choosing <b>IP Address</b> or <b>Hostname</b> from the drop-down list and entering the IP address or host name in the corresponding field.
Primary Syslog Server Port	Enter the primary Syslog server port number that receives the logs. Valid values are 514 and 1024 through 65535. The default Syslog port is 514.
Facility	Enter the system facility that receives logs on the Syslog server.



**Table 8-1 Log Setup Window Options (continued)**

Option	Description
Minimum Log Severity	<p>Choose the minimum severity of messages that are sent to the Syslog server. The system sends all messages of this severity and higher. Message severities, from highest to lowest, are:</p> <ul style="list-style-type: none"> <li>• <b>Emergency</b>—The system is unusable.</li> <li>• <b>Alert</b>—A situation occurred that requires immediate action.</li> <li>• <b>Critical</b>—A situation occurred that requires action soon.</li> <li>• <b>Error</b>—An error occurred, but it does not necessarily affect the ability of the system to function.</li> <li>• <b>Warning</b>—A undesirable condition occurred.</li> <li>• <b>Notice</b>—Notification about a system condition that is not an error condition.</li> <li>• <b>Informational</b>—Information about a system activity.</li> <li>• <b>Debug</b>—Information about a system activity with detailed technical information. Includes messages of every other severity.</li> </ul> <p>The default severity is Informational.</p>
Secondary Syslog Server	Identify an optional secondary Syslog server by choosing <b>IP Address</b> or <b>Hostname</b> from the drop-down list and entering the IP address or host name in the corresponding field.
Secondary Syslog Server Port	Enter the port number that receives the logs on the secondary Syslog server. Valid values are 514 and 1024 through 65535. The default Syslog port is 514.
Facility	Enter the system facility that receives logs on the Syslog server.
Minimum Log Severity	<p>Choose the minimum severity of messages that are sent to the secondary Syslog server. The system sends all messages of this severity and higher. Message severities, from highest to lowest, are:</p> <ul style="list-style-type: none"> <li>• <b>Emergency</b>—The system is unusable.</li> <li>• <b>Alert</b>—A situation occurred that requires immediate action.</li> <li>• <b>Critical</b>—A situation occurred that requires action soon.</li> <li>• <b>Error</b>—An error occurred, but it does not necessarily affect the ability of the system to function.</li> <li>• <b>Warning</b>—An undesirable condition occurred.</li> <li>• <b>Notice</b>—Notification about a system condition that is not an error condition.</li> <li>• <b>Informational</b>—Information about a system activity.</li> <li>• <b>Debug</b>—Information about a system activity with detailed technical information. Includes messages of every other severity.</li> </ul>

# Local Log Window

The Local Log window lets you view the log file that is stored on the IP camera.

To display the Local Log window, perform the following steps:

## Procedure

**Step 1** From the IP camera user interface, click the **Setup** link.









**Step 2** Click **Log** to expand the menu.

**Step 3** From the Log menu, click **Local Log**.





The Local Log window appears.

Table 8-2 describes the options in the Local Log window.

**Table 8-2 Local Log Window Options**

Option	Description
<b>Log List Area</b>	
Rows per page	Choose the number of log entry rows to display per page and click the <b>Go</b> button to the right of this option to update the display.
Filter	Choose the type of log message to include in the display. To include messages of every severity, choose <b>All</b> .
Since	Choose the time period for which you want to view log messages.
<b>Go</b> button	Update the log display based on the values in the Filter and Since fields.
Severity	<p>An icon in this column indicates the severity of the corresponding log message:</p> <ul style="list-style-type: none"> <li> —Emergency message</li> <li> —Alert message</li> <li> —Critical message</li> <li> —Error message</li> <li> —Warning message</li> <li> —Notice message</li> <li> —Informational message</li> <li> —Debug message</li> </ul> <p>To display log messages in order of severity with the least severity first, click the Severity column heading. Click the heading again to reverse the display order.</p>
Date/Time	<p>Date and time that the logged activity occurred.</p> <p>By default, log messages appear in the order that the activity occurred with the oldest message first. To reverse this display order, click the Date/Time column heading.</p>

**Table 8-2 Local Log Window Options (continued)**

Option	Description
Description	Message that describes the logged activity. For detailed information about log messages, see <a href="#">Table 8-3 on page 8-5</a> .
Page controls	<p>Let you move through the log file entries:</p> <p>Page field—Enter a page number and press Enter.</p> <p> —Go to first page</p> <p> —Go to previous page</p> <p> —Go to next page</p> <p> —Go to last page</p>

[Table 8-3](#) describes the messages that can appear in the IP camera log file. When you view the log file, each message includes the date and time that it was logged. In this table:

- Messages appear in alphabetical order
- Angle brackets (<>) indicate items that are replaced by appropriate information when the message appears. *Italic text* describes these items.
- Severity indicates the severity of the message:
  - 0—Emergency (the system is unusable)
  - 1—Alert (a situation occurred that requires immediate action)
  - 2—Critical (a situation occurred that requires action soon)
  - 3—Error (an error occurred, but it does not necessarily affect the ability of the system to function)
  - 4—Warning (an undesirable condition occurred)
  - 5—Notice (notification about a system condition that is not an error condition)
  - 6—Informational (information about a system activity)
  - 7—Debug (information about a system activity with detailed technical information)

**Table 8-3 Log Messages**

Message Name	Description that Appears in Log File	Explanation	Severity
AUTHENTICATION_FAILED	Access authentication to <web server, streaming server, or SSH server> by user <user> <IP address or hostname> failed.	An attempt to log in or authenticate to the IP camera failed.	3
AUTHENTICATION_FAILED	Access authentication to <server type> server <server IP address or hostname> failed.	The IP camera was unable to access an SNTP, Syslog, DNS, SMTP, HTTP, or 802.1x server.	4
AUTHORIZATION_FAILED	Unauthorized address <IP address or hostname> attempted to access camera.	An attempt was made to access the IP camera by using invalid user credentials from an IP address that has been configured for no access.	3

Table 8-3 Log Messages (continued)

Message Name	Description that Appears in Log File	Explanation	Severity
CODEC_LOST	Connection to Codec/Sensor module was lost. Internal module is either down or not responding.	The IP camera codec/sensor module is not responding.	4
CONFIG_SAVE_FAILED	Saving configuration to user <user> <IP address or hostname> failed.	A user attempt to save the IP camera configuration failed.	3
CONFIG_SAVED	Configuration saved by user <user> <IP address or hostname>.	The IP camera configuration was saved by a user.	5
CONFIG_UPLOAD_FAILED	Uploading configuration failed from user <user> <IP address or hostname>.	A user attempt to import the IP camera configuration failed.	3
CONFIG_UPLOADED	Configuration uploaded from user <user> <IP address or hostname>.	The IP camera configuration was imported by a user.	5
DEFAULTS_FAILED	Restoring factory defaults failed for user <user> <IP address or hostname>.	An attempt to reset the IP camera to its factory default configuration failed.	3
DEFAULTS_RESTORED	Factory defaults restored successfully by user <user> <IP address or hostname>.	The IP camera was reset to its factory default configuration.	5
DEVICE_REBOOT_AUTO	Device rebooted.	The IP camera rebooted automatically.	5
DEVICE_REBOOT_MANUAL	Device was rebooted manually by user <user> <IP address or hostname>.	The IP camera was rebooted by a user.	5
DHCP_LEASE	DHCP lease renewal was successful.	The IP camera renewed its DHCP lease.	6
DSP_ENCODING_HALTED	The Codec/Sensor module's DSP encoding was halted. Either the analog image signal from the sensor has been lost, or an internal encoding error has occurred.	The DSP of the IP camera codec/sensor module DSP stopped encoding. The analog image signal from the sensor may be lost or an internal encoding error may have occurred.	2
EMAIL_TRIGGERED	Event triggered: email sent to <e-mail address>.	An event occurred and e-mail notification of the event was sent.	5
ETH_BER	Bit Error Rate (BER) exceeded specified threshold of <threshold>.	The bit error rate (BER) exceeded the specified threshold.	4
ETH_SIGNAL_DEGRADE	Ethernet signal degrading.	The IP camera detected a degrading Ethernet signal.	4
FRAMES_DROPPED	Output frame rate does not match the camera's configured frame rate.	The IP camera is sending video at a frame rate that does not match the configured frame rate.	3
FW_UPGRADE_FAILED	Upgrading firmware failed from user <user> <IP address or hostname>.	An attempt to upgrade the IP camera firmware failed.	0
FW_UPGRADED	Firmware upgraded successfully from user <user> <IP address or hostname>.	The IP camera firmware was updated.	5
HTTP_TRIGGERED	Event triggered: notification sent to HTTP server <IP address or hostname>.	An event occurred and HTTP notification of the event was sent.	5

Table 8-3 Log Messages (continued)

Message Name	Description that Appears in Log File	Explanation	Severity
INPUT_ONE_CHANGED	Input port one changed to <i>&lt;high/low&gt;</i> .	Input port 1 on the IP camera changed state.	5
INPUT_ONE_RESET	Input port one reset to <i>&lt;high/low&gt;</i> .	Input port 1 on the IP camera reset to its default state.	5
INPUT_TWO_CHANGED	Input port two changed to <i>&lt;high/low&gt;</i> .	Input port 2 on the IP camera changed state.	5
INPUT_TWO_RESET	Input port two reset to <i>&lt;high/low&gt;</i> .	Input port 2 on the IP camera reset to its default state.	5
IP_CONFLICT	IP Address conflict for <i>&lt;IP address&gt;</i> .	IP camera experienced an IP address conflict.	4
IR_FILTER_DAY_AUTO	IR filter changed to day automatically.	The IP camera enabled its day filter automatically.	6
IR_FILTER_DAY_MANUAL	IR filter manually changed to day by user <i>&lt;user&gt;</i> <i>&lt;IP address or hostname&gt;</i> .	The IP camera day filter was enabled by a user.	6
IR_FILTER_NIGHT_AUTO	IR filter changed to night automatically.	The IP camera enabled its night filter automatically.	6
IR_FILTER_NIGHT_MANUAL	IR filter changed to night by user <i>&lt;user&gt;</i> <i>&lt;IP address or hostname&gt;</i> .	The IP camera night filter was enabled by a user.	6
LOG_IN	User <i>&lt;user&gt;</i> <i>&lt;IP address or hostname&gt;</i> logged in to <i>&lt;web server or SSH server&gt;</i> .	A user logged in to the IP camera.	5
LOG_OUT	User <i>&lt;user&gt;</i> <i>&lt;IP address or hostname&gt;</i> logged out of <i>&lt;web server or SSH server&gt;</i> .	A user logged out of the IP camera.	5
MOTION_DETECTED	Motion detected in region <i>&lt;region index&gt;</i> .	The IP camera detected motion in its video field.	5
MOTION_STOPPED	Motion in region <i>&lt;region index&gt;</i> stopped.	The IP camera stopped detecting motion in its video field.	5
OUTPUT_ONE_RESET	Output port one reset to <i>&lt;high/low&gt;</i> .	Output port 1 on the IP camera reset to its default state.	5
OUTPUT_ONE_TRIGGERED	Output port one triggered to <i>&lt;high/low&gt;</i> .	Output port 1 on the IP camera changed state.	5
POWER_SUPPLY_FAILURE	DC power supply failure.	The DC power for the IP camera failed.	2
SERVER_CONTACTED	Communication established with <i>&lt;server type&gt;</i> server <i>&lt;server or IP address&gt;</i> .	The IP camera established communication with an SNTP, DHCP, Syslog, DNS, SMTP, HTTP, or 802.1x server.	6
SERVER_LOST	Communication lost with <i>&lt;server type&gt;</i> server <i>&lt;server or IP address&gt;</i> .	The IP camera lost communication with an SNTP, DHCP, Syslog, DNS, SMTP, HTTP, or 802.1x server.	4
SERVER_UNREACHABLE	Failed to contact <i>&lt;server type&gt;</i> server <i>&lt;server or IP address&gt;</i> .	The IP camera was unable to contact an SNTP, DHCP, Syslog, DNS, SMTP, HTTP, or 802.1x server or a gateway.	4

Table 8-3 Log Messages (continued)

Message Name	Description that Appears in Log File	Explanation	Severity
START_STREAM	Channel <channel ID> started streaming to user <user> <IP address or hostname>.	The IP camera began streaming video to a user device.	6
STOP_STREAM	Channel <channel ID> stopped streaming to user <user> <IP address or hostname>.	The IP camera stopped streaming video to a user device.	6
TEMP_THRESHOLD_T1	Current temperature, <temperature>, <exceeds/is below> <high temperature/low temperature> threshold.	The internal temperature of the IP camera is lower than 59°F (15°C) or higher than 149°F (65°C).	2
TEMP_THRESHOLD_T2	Current temperature, <temperature>, <exceeds/is below> <high temperature/low temperature> threshold.	The internal temperature of the IP camera is lower than 32°F (0°C) or higher than 176°F (80°C).	4
TEMP_THRESHOLD_T3	Current temperature, <temperature>, <exceeds/is below> <high temperature/low temperature> threshold.	The internal temperature of the IP camera is lower than 5°F (–15°C) or higher than 194°F (90°C).	5
TIME_DST_SWITCH	Time switched to Daylight Savings time with an offset of <offset> minutes.	The IP camera internal clock switched to daylight saving time.	6
TIME_REG_SWITCH	Time switched from Daylight Savings time with an offset of <offset> minutes.	The IP camera internal clock switched to standard time.	6
UNEXPECTED_EXCEPTION	Unexpected exception occurred. Could not <read/write> <to/from> repository by user <user> <IP address or hostname>.	IP camera could not read or write information to its internal repository.	2



## INDEX

---

### Numerics

#### 802.1x window

- EAP-FAST configuration [5-11](#)
- EAP-PEAP configuration [5-11](#)
- EAP-TTLS configuration [5-11](#)
- enable 802.1x [5-10](#)
- EPA-TLS configuration [5-10](#)
- overview [5-10](#)

---

### A

About link [1-5](#)

#### Account Initialization window

- options [7-2](#)

#### action

- triggered by event [4-19](#)

action, triggered by event [4-24](#)

ActiveX controls [1-4](#)

Administration windows [7-1, 8-1](#)

alert, trigger types [4-26](#)

#### Alert Notification window

- options [4-26](#)
- overview [4-24](#)

#### app

- configuring [6-6](#)
- description [6-1](#)
- enabling [6-1](#)
- installing [6-5](#)
- license, installing [6-5](#)
- running [6-7](#)
- stopping [6-7](#)
- uninstalling [6-8](#)

#### App Configuration window

- options [6-1](#)
- overview [6-1](#)

application manager, restoring [6-8](#)

Application Manager windows [6-1](#)

#### App License window

- options [6-2](#)
- overview [6-2](#)

#### App Setup window

- options [6-3](#)
- overview [6-3](#)

#### audio

- settings [4-13](#)

---

### B

backing up, configuration of IP camera [7-4](#)

#### Basic Settings window

- options [5-2](#)
- overview [5-1](#)

bit rate, of video [4-13](#)

Bonjour, enabling on camera [5-7](#)

brightness [3-4](#)

---

### C

camera settings, controls in Camera Video/Control window [3-4](#)

#### Camera Settings window

- options [4-15](#)
- overview [4-14](#)

#### Camera Video & Control window

- accessing [3-1](#)

- description [1-5](#)
- displaying [1-4](#)
- configuration windows
  - 802.1x window [5-10](#)
  - accessing [1-2](#)
  - Administration windows [7-1](#)
  - Alert Notification window [4-24](#)
  - App Configuration window [6-1](#)
  - Basic Settings window [5-1](#)
  - Camera Settings window [4-14](#)
  - Device Processes window [7-7](#)
  - Discovery Settings window [5-6](#)
  - Event Notification window [4-18](#)
  - Feature Setup windows [4-1](#)
  - Firmware Settings window [7-6](#)
  - Initialization window [7-1](#)
  - IO Ports Settings window [4-17](#)
  - IP Addressing window [5-3](#)
  - IP Filter Settings window [5-12](#)
  - Local Log window [8-4](#)
  - Local Storage window [4-27](#)
  - Log Setup Settings window [8-1](#)
  - Log windows [8-1](#)
  - Maintenance Settings window [7-4](#)
  - Medianet window [5-7](#)
  - Network Setup windows [5-1](#)
  - Password Complexity window [7-8](#)
  - QoS Settings window [5-13](#)
  - SNMP Settings window [5-8](#)
  - Streaming Settings window [4-1](#)
  - Time Settings window [5-5](#)
  - User Settings window [7-3](#)
  - Video Overlay Settings window [4-16](#)
- configuring, app [6-6](#)
- connecting, to the IP camera
  - after the first time [1-2](#)
  - for the first time [2-1](#)
  - PC requirements for [1-3, 2-1](#)
  - secure connection [1-3](#)

- contrast [3-4](#)

---

## D

- date and time
  - configuring manually [5-5](#)
  - updating through NTP server [5-5](#)
- day
  - filter [4-14](#)
  - mode [4-14](#)
- daylight saving time, adjustment for [5-5](#)
- Device Processes window
  - options [7-8](#)
  - overview [7-7](#)
- DHCP, obtaining IP address through [2-1, 5-4](#)
- Differentiated Services (DiffServ) [5-13](#)
- Discovery Settings window
  - options [5-7](#)
  - overview [5-6](#)
- DNS server
  - primary [5-4](#)
  - secondary [5-4](#)
- dual streaming [4-1](#)

---

## E

- e-mail notification
  - configuring [4-21, 4-22](#)
  - for alert [4-26, 4-27](#)
  - From field [4-23, 4-27](#)
  - recipients [4-22, 4-27](#)
- event
  - actions
    - email notification [4-19, 4-24](#)
    - FTP notification [4-19, 4-25](#)
    - HTTP notification [4-19, 4-25](#)
    - output port state change [4-19, 4-24](#)
    - syslog server message [4-19, 4-24](#)



- notification
  - from health trigger [4-24](#)
  - from system trigger [4-18](#)
- trigger types [4-20](#)

Event Notification window

- options [4-20](#)
- overview [4-18](#)

event triggering, enabling for app [6-6](#)

## F

factory default configurations, resetting [7-5](#)

factory default configurations, restoring [7-5](#)

Feature Setup windows [4-1](#)

- Local Storage [4-27](#)

firmware

- upgrading [7-6, 7-7](#)
- version in IP camera [7-7](#)

Firmware Settings window

- options [7-7](#)
- overview [7-6](#)

focus and zoom controls [3-8](#)

FTP notification

- configuring [4-23](#)

## G

gateway, for IP camera [5-4](#)

## H

help, for IP camera windows [1-5](#)

Home window

- accessing [1-2](#)
- description [1-4, 1-5](#)
- displaying [1-4](#)

HTTP

- accessing camera through [1-3](#)

- allowing access through [2-2, 7-2](#)

- default port [7-2](#)

- port [7-2](#)

HTTPS

- accessing camera through [1-3](#)

- allowing access through [7-2](#)

- default port [7-2](#)

- port [7-2](#)

## I

Initialization window

- overview [7-1](#)

input ports, state change [4-18](#)

installing

- app [6-5](#)
- app license [6-5](#)

IO Ports Settings window

- options [4-18](#)
- overview [4-17](#)

IP address

- controlling access by [5-12](#)
- default for IP camera [1-3, 2-1](#)
- fixed [5-4](#)
- obtaining from DHCP server [2-1](#)
- obtaining through DHCP [5-4](#)
- static [5-4](#)

IP Addressing window

- options [5-3](#)
- overview [5-3](#)

IP camera

- accessing through a web browser [1-2, 2-1](#)
- connecting to after the first time [1-2](#)
- connecting to for the first time [2-1](#)
- controlling access to [5-12](#)
- day mode [4-14](#)
- logging in to [1-4](#)
- logging out of [1-4](#)
- MAC address [7-7](#)

- name [5-2](#)
- night mode [4-14](#)
- overview [1-1](#)
- rebooting [7-5](#)
- restarting [7-5](#)
- restoring factory default configurations [7-5](#)
- time zone [5-5](#)
- windows [1-2, 1-5](#)

#### IP Filter Settings window

- options [5-12](#)
- overview [5-12](#)

## L

#### live video

- viewing
  - through home window [3-1](#)
  - through third-party device or software [3-1](#)

*See also* video

Local [4-27](#)

#### Local Log window

- options [8-4](#)
- overview [8-4](#)

Local Storage window, overview [4-27](#)

#### log file

- sending to Syslog server [8-2](#)
- storage of [8-1](#)
- viewing [8-4](#)

log in, to IP camera [1-4](#)

log out, of IP camera [1-4](#)

#### Log Setup Settings window

- options [8-2](#)
- overview [8-1](#)

## M

MAC address, of IP camera [7-7](#)

#### Maintenance Settings window

- options [7-5](#)
- overview [7-4](#)

#### Medianet window

- Enable Flow Metadata [5-8](#)
- overview [5-7](#)

#### microphone

- use [4-14](#)

#### motion detection

- controls [3-7, 3-10](#)
- enabling [3-7](#)
- sensitivity [3-8](#)

#### multicast

- address [4-12](#)
- enabling [4-12](#)
- port [4-12](#)

## N

name, of IP camera [5-2, 7-7](#)

Network Setup windows [5-1](#)

#### night

- filter [4-14](#)
- mode [4-14](#)

## O

#### output ports

- power on state [4-18](#)

## P

#### password

- complexity [7-8](#)
- configuring requirements for [7-8](#)
- for primary SMTP server [4-22](#)
- for secondary SMTP server [4-22, 4-27](#)
- for SMTP server [4-27](#)

- for user [7-4](#)
- hardening [7-8](#)
- requirements for [2-2, 7-4](#)

#### Password Complexity window

- options [7-8](#)
- overview [7-8](#)

port number [1-3](#)

#### processes

- descriptions [7-8](#)
- stopping [7-7](#)

## Q

#### QoS Settings window

- options [5-13](#)
- overview [5-13](#)

quality of service [5-13](#)

## R

rebooting, IP camera [7-5](#)

Refresh link [1-4](#)

resetting, factory default configurations [7-5](#)

restarting, IP camera [7-5](#)

restoring, factory default configurations [7-5](#)

## S

saturation [3-4](#)

secure connection [1-3](#)

#### security

- controlling processes [7-7](#)
- password hardening [7-8](#)
- stopping processes [7-7](#)

#### Setup window

- description [1-5](#)
- displaying [1-4](#)

sharpness [3-4](#)

SNMP, configuring [5-8](#)

#### SNMP Settings window

- options [4-29, 5-8](#)
- overview [5-8](#)
- SNMP v2c [5-8](#)
- SNMP v3 [5-9](#)

#### SSH

- allowing access through [7-2](#)
- alternative port [7-2](#)
- default port [7-2](#)

#### Streaming Settings window

- options [4-12](#)
- overview [4-1](#)

subnet mask, of IP camera [5-4](#)

Syslog server [8-2](#)

## T

text overlay, on video [4-17](#)

#### Time Settings window

- options [5-5](#)
- overview [5-5](#)

time stamp, on video [4-17](#)

time zone, of IP camera [5-5](#)

#### trigger

- for alert [4-26](#)
- health [4-24](#)
- system [4-18](#)

trigger, for event [4-20](#)

## U

uninstalling app [6-8](#)

user, password [7-4](#)

user name, requirements for [7-3](#)

#### User Settings window

- options [7-3](#)
- overview [7-3](#)

---

**V**

## video

- bit rate [4-13](#)

- codec, controls in Camera Video/Control window [3-1](#)

- primary stream [4-1](#)

- quality [4-13](#)

- resolution, controls in Camera Video/Control window [3-1](#)

- secondary stream [4-1](#)

- text overlay [4-17](#)

- time stamp on [4-17](#)

- viewing live

  - through Home window [3-1](#)

  - through third-party device or software [3-1](#)

- See also* live video

## video codec

- display in Streaming Settings window [4-13](#)

## video image

- optimizing for lighting condition [4-14](#)

## Video Overlay Settings window

- options [4-17](#)

- overview [4-16](#)

video resolution, configuration guidelines [4-1](#)View Video link [1-4](#)