Cisco Video Surveillance 6000 Series IP Camera Configuration Guide

Release 1.3.2

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Text Part Number: OL-29852-01

Cisco Video Surveillance 6000 Series IP Camera Configuration Guide, Release 1.3.2

CONTENTS

Preface v

Overview v

Organization v

Obtaining Documentation, Obtaining Support, and Security Guidelines vi

CHAPTER 1 **Overview** 1-1

IP Camera Features 1-1

Accessing the IP Camera 1-2

Understanding the IP Camera User Interface 1-4

IP Camera Window Links 1-4

IP Camera Windows 1-5

CHAPTER 2 **Performing the Initial Setup of the IP Camera** 2-1

CHAPTER 3 **Viewing Live Video** 3-1

CHAPTER 4 **Feature Setup** 4-1

Streaming Window 4-1

Camera Window 4-14

Video Overlay Window 4-16

IO Ports Window 4-17

Event Notification Window 4-18

CHAPTER 5 **Network Setup** 5-1

Basic Window 5-1

IP Addressing Window 5-3

Time Window 5-4

Discovery Window 5-6

IP Filter Window 5-7

QoS Window 5-8

CHAPTER 6 **Administration** 6-1

Initialization Window 6-1

User Window 6-3

Maintenance Window 6-4

Firmware Window 6-6

Device Processes Window 6-7

Password Complexity Window 6-8

CHAPTER 7 **Log Configuration** 7-1

Log Setup Window 7-1

Local Log Window 7-4

INDEX

Preface

Overview

This document, *Cisco Video Surveillance 6000 Series IP Camera Configuration Guide*, provides information about installing and deploying the following Cisco Video Surveillance 6000 Series IP Cameras:

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

Organization

This manual is organized as follows:

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

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information about obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

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

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

Overview

This chapter provides information about the Cisco Video Surveillance 6000 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 6000 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 (1920 x 1080) resolution.

In addition, the 6000 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 6000 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 8 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 12 volts DC or 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

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 8.0 (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 6-1.
- 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 6-3.

To access the IP camera windows, perform these steps.

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, 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 6-3 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
Refresh	Updates the information in the window that is currently displayed.	Administrator User
Home	Displays the System Information window. For more information, see Table 1-2.	Administrator
View Video	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
Setup	Displays the Setup window and provides access to the configuration menus for the IP camera.	Administrator
Logout	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 6, "Administration."
  - Chapter 7, "Log Configuration."

Table 1-2 Home Window Information

Field	Description
General Information	
ID	Identifier of the IP camera. To configure the ID, see the "Basic Window" section on page 5-1.
Name	Name of the IP camera. To configure the name, see the "Basic Window" section on page 5-1.
Current Time	Current date and time of the IP camera. To set the date and time, see the "Time Window" section on page 5-4.
S/N	Serial number of the IP camera.
Firmware	Version of the firmware that is installed on the IP camera.
Codec	Version of the codec that is running on the IP camera.
Part Number	Cisco manufacturing part number of the IP camera.
Top Assembly Revision	Cisco assembly revision number.
Network Status	
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 "IP Addressing Window" section on page 5-3.

Table 1-2 Home Window Information (continued)

Field	Description
LAN IP	IP address of the LAN to which the IP camera is connected. To configure this IP address, see the "IP Addressing Window" section on page 5-3.
Subnet Mask	Subnet mask of the LAN to which the IP camera is connected. To configure the subnet mask, see the "IP Addressing Window" section on page 5-3.
Gateway Address	IP address of the gateway through which the IP camera is connected. To configure this IP address, see the "IP Addressing Window" section on page 5-3.
Primary DNS	IP address of the primary DNS server, if configured for the IP camera. To configure a primary DNS server, see the "IP Addressing Window" section on page 5-3.
Secondary DNS	IP address of the secondary DNS server, if configured for the IP camera. To configure a secondary DNS server, see the "IP Addressing Window" section on page 5-3.
IO Port Status	
Input Port 1	Current state of input port 1 on the IP camera.
Output Port 1	Current state of output port 1 on the IP camera.
Stream 1 and Stream 2	
User	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. Be default, users appear in order of start time. To displays 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.
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.

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 DCHP 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 6000 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
- Privacy Zone

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

Table 3-1 Camera Video & Control Window Controls

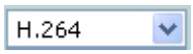
Control	Description
Video controls	
Video Codec drop-down list 	Choose the codec for video transmission (H.264 or MJPEG). You can choose H.264 only if the primary video stream (channel 1) is enabled. You can choose MJPEG only if the secondary video stream (channel 2) is enabled. For information about enabling and disabling video streams, see the "Streaming Window" section on page 4-1.

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

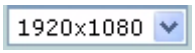
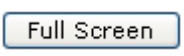
Control	Description
Video Resolution drop-down list 	Choose the resolution for video transmission. The resolutions in this drop-down list depend on the video standard that you selected. The default value for H.264 is 1920 x 1080. The default value for MJPEG is 704 x 480. You cannot configure a secondary stream if you configure this resolution for 1920 x 1080. **Note** You can also change the resolution for video transmission by changing the value in the Video Resolution Type field, as described in the "Streaming Window" section on page 4-1.
Image tools	
Hotspot zoom button 	Click this latch button to enable 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 **Hotspot zoom** button and click the video display. The first five clicks zoom the display. The sixth click returns to unzoomed display.
Hotspot pan+tilt button 	Click this latch button to enable the hotspot pan/tilt feature, which lets you pan and tilt the IP camera toward a point that you click in the video display. To perform a hotspot pan/tilt action, engage the **Hotspot pan+tilt** button, then click the video image at the location toward which you want the IP camera to pan and tilt. This feature requires that the IP camera be installed with a pan/tilt mount that supports the Pelco D protocol and that pan and tilt functions are enabled.
Save snapshot button 	Capture and save 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 **Save** and follow the on-screen prompts to save the image with the name and in the location that you want.
Flip button 	Rotate the video image by 180 degrees.
Mirror button 	Reverse the video image.
Restore button 	Display the default video image, which is not rotated and not reversed.
Full Screen button 	Display the video image in full screen mode. To return to normal display mode, click the full screen image.

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

Control	Description
Audio Control	
Disable Speaker toggle button 	Click the **Disable Speaker** 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. Click the **Enable Speaker** button to unmute audio. The button changes to the **Disable** button.
Enable Speaker toggle button 	
Mute Microphone toggle button 	Click the **Mute Microphone** 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. **Note** 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. When you click the **Mute Microphone** button, it changes to the Unmute Microphone button. Click the **Unmute Microphone** button to unmute audio that is sent to the IP camera. The button changes to the **Mute Microphone** button.
Unmute Microphone toggle button 	
Restore button 	Reset audio controls to their default values.
Speaker Volume slider and field 	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 and press the **Enter** key. The default value is 50.
Microphone Sensitivity slider and field 	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 and press the **Enter** key. The default value is 50.
Camera Settings	

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

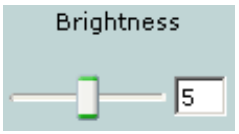
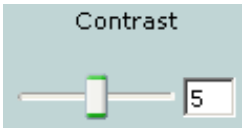
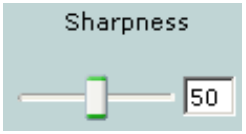
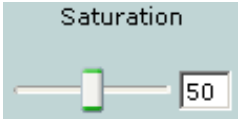
Control	Description
Up Arrow toggle button 	Click the Up Arrow to display the camera settings. The button changes to the Down Arrow button Click the Down Arrow button to hide the camera settings. The button changes to the Up Arrow button. When the Up Arrow is clicked to display the camera settings, three drawers appear to the right of the video image. The camera settings are grouped into the three drawers as follows: • Picture Adjustments • Exposure Control • Advanced Settings To view the settings within a drawer, click on it to expand it. To hide the settings, click on the drawer to collapse it.
Down Arrow toggle button 	
Save button	Save the current camera setting configurations.
Picture Adjustments **Note** These controls appear when you click **Camera Settings Up Arrow > Picture Adjustments**.	
Brightness slider 	To control the brightness of the video image, drag the slider, or enter a value from 1 through 10 and press the **Enter** key. 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, or enter a value from 1 through 10 and press the **Enter** key. 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, or enter a value from 1 through 100 and press the **Enter** key. 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, or enter a value from 1 through 100 and press the **Enter** key. 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.
Restore button	Click this button to restore the picture adjustments to their default values.

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

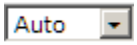
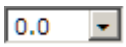
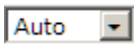
Control	Description
White Balance Mode 	Choose one the following White Balance modes from the drop-down list: • **Manual**—Choose this option if you want to set the white balance by setting RGain (Red Gain) and BGain (Blue Gain) manually. • **Auto**—White balance is automatically set by camera, which is suitable for most conditions. The default setting is Auto.
Exposure Control **Note** These controls appear when you click **Camera Settings Up Arrow > Exposure Control**.	
Exposure Level 	Increases or decreases the exposure level. For example, if you want to add light (overexpose) to properly expose the image, set the value to +1. If you need to underexposure the scene, set value to -1. Default value is 0.0
Exposure Mode 	Choose one of the following Exposure modes: • **Auto**—Automatically sets the exposure level, which is suitable for most conditions. • **Manual**—Choose this option if you want to set Exposure time and Gain control manually. Default setting is Auto.
Flickerless	(The Flickerless check box is available only when the Exposure mode is set to Manual.) Check this check box to avoid flickering when a combination of indoor and outdoor light is getting to the camera. Using this option limits the range of exposure time which avoids flicker.
Exposure Time 	(The Exposure time option is available only when the Exposure mode is set to Manual.) Specify the range of shutter speed settings to be used by the IP camera. Shutter speed is measured in fractions of a second. You can adjust both ends of the shutter speed range. Default range is 1/5 sec to 1/32000 sec in Manual mode.
Gain Control	(The Gain control option is available only when the Exposure mode is set to Manual.) Specify the range of gain (amount of amplification applied to pixel values) settings to be used by the IP camera. You can adjust both ends of the gain control range. Default range is to 0 to 100.
Iris Mode 	(The Iris mode is available only when the Exposure mode is set to Auto.) Choose one of the following Iris modes: • Indoor—Suitable for indoor conditions. • Outdoor—Suitable for outdoor conditions. Default mode is Indoor.

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

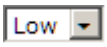
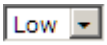
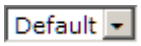
Control	Description
Measurement Window	Choose how exposure is calculated based on video data from one of the following measurement windows: • **Full View**—Exposure is calculated based on full view. • **Custom**—You can designate specific regions (areas within the field of view) to use for exposure calculation. Inclusion regions designate areas that are used to calculate the exposure value. Exclusion regions designate areas that are ignored when calculating the exposure value. You can draw up to four inclusion regions and four exclusion regions. To create a region, right-click on the video image and choose **Draw Region**. Drag the region to the desired area and drag an edge or corner of the region to resize it. To remove region, right-click on it and choose **Delete Region**. Inclusion regions are created by default. To toggle between inclusion and exclusion regions, right-click on a region and change the **Region Properties > Region Type** setting. • **BLC**—Back Light Compensation (BLC) window adds a weighted region in the middle of the image view to give necessary exposure compensation.
Advanced Settings **Note** These controls appear when you click **Camera Settings Up Arrow > Advanced Settings**.	
Enable Low Light Compensation	Use this option in low light situations.
Enable DRX	Check this check box to enable the Dynamic Range Enhanced (DRX) feature. DRX helps recover washed out details when there are extreme contrast lighting conditions. To reach better image quality, adjust Sensitivity (Low and High) and Strength (Low, Medium and High).
Sensitivity 	(The Sensitivity option is available only when DRX is enabled.) Choose how sensitive (Low or High) DRX is to extreme contrast lighting conditions.
Strength 	The Strength option is available only when DRX is enabled. Choose how much DRX processing (Low, Medium, or High) to use for recovering washed out details.
Gamma Curve 	Choose the value that provides the optimal gray-scale intensity. Larger gamma curve values make shadows darker, and larger values make dark regions lighter.
Save button	Save the current camera settings.
Motion detection	
Up Arrow toggle button 	Click the Up Arrow to display the motion detection controls. The button changes to the Down Arrow button. Click the Down Arrow button to hide the motion detection controls. The button changes to the Up Arrow button.
Down Arrow toggle button 	

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

Control	Description
Motion detection controls	
Note These controls appear when you click the Up Arrow in the Motion Detection area and are available only viewing the primary (H.264) stream.	
Enable Motion Detection check box	Enable the motion detection feature and display a grid over the video image. When motion detection is enabled, the IP camera monitors activity in regions of the video that you specify. If activity at a defined level occurs in any of these areas, the IP camera generates an alert and takes the actions that are configured as described in the "Event Notification Window" section of Feature Setup. After motion detection has been enabled, you create specific regions that the IP camera monitors for activity. To create a motion detection region, right-click on the video image, choose **Draw Region**, and then click and drag across the motion detection grid to draw a green square or rectangle comprised of one or more grid squares. Up to eight of the following regions can be drawn: • **Motion Inclusion Regions**—Designate areas to examine for motion. You can draw up to four motion inclusion regions. • **Motion Exclusion Regions**—Designate areas to ignore for motion. You can draw up to four motion exclusion regions. For each region listed under the Region Properties area, you can configure the following properties: • **IsActive**—Specifies whether the region is active (enabled) or not active (disabled). Chose **true** to enable a region; choose **False** to disable a region. • **Location**—Specifies the grid coordinate (X, Y) for the upper left corner of the region. • **Name**—You can enter a name of up to 12 characters for a region. • **Region Type**—Specifies whether the region is an inclusion or an exclusion region. Choose **Inclusion** to have the region examine for motion; choose **Exclusion** to have the region ignore motion. • **Sensitivity**—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. • **Threshold**—Designates the percentage of pixels that the IP camera must identify as changed in the area before it generates an alert. The camera detects pixel changes at the defined sensitivity level. The default threshold value is 10. To reset the sensitivity and threshold to their default values of 80 and 10 respectively, right-click on the region, and choose **Restore Values**. To remove a region, right-click it, and choose **Delete Region**.

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

Control	Description
Focus/Zoom	
Up Arrow toggle button 	Click the Up Arrow to display the focus/zoom controls. The button changes to the Down Arrow button. Click the Down Arrow button to hide the focus/zoom controls. The button changes to the Up Arrow button.
Down Arrow toggle button 	
Focus/Zoom controls **Note** These controls appear when you click the Up Arrow in the Focus/Zoom area.	
Zoom slider	To control the field of view zoom factor, drag the slider left to zoom out (wide), or drag the slider to the right to zoom in (telephoto).
Focus slider	To control the field of view focus, drag the slider left to focus on near objects, or drag the slider to the right to focus on far objects.
Auto Focus button	Click to automatically focus the IP camera for the selected zoom.
Specify Region check box	Used in conjunction with the **Auto Focus** option. Check **Specify Region** check box and click **Auto Focus** to focus the IP camera with priority to a selected region in the field of view. The region is user configurable and can be moved around the screen.
Reset button	Resets the lens position and slider control positions to their default values (full wide and near).
Full Auto Focus button	Used to auto focus the full image. Lens is adjusted automatically to provide sharp focus of the image for selected zoom.
Privacy Zone	
Up Arrow toggle button 	Click the Up Arrow to display the privacy zone controls. The button changes to the Down Arrow button. Click the Down Arrow button to hide the privacy zone controls. The button changes to the Up Arrow button.
Down Arrow toggle button 	

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

Control	Description
Privacy Zone controls	
Note These controls appear when you click the Up Arrow in the Privacy Zone area.	
Enable Privacy Region	Check this check box to enable the privacy zone feature that allows you to create a maximum of four user-defined privacy regions. Any video within a privacy region is masked in the video stream. To create a region, right-click on the video image and choose **Draw Region**. Drag the region to the desired area and drag an edge or corner of the region to resize it. To remove region, right-click on it and choose **Delete Region**. For each region listed under the Privacy Zone Properties area, you can configure the following properties: • **Current Region**—You can enter a name of up to 12 characters for a region. • **IsActive**—Specifies whether the region is active (enabled) or not active (disabled). Chose True to enable a region; choose False to disable a region.
Region Color	Choose a color from the Region Color drop-down list to specify the color that is used to mask the actual video in all privacy regions.
Save button	Save the current privacy zone configuration.

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

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.

The primary stream supports H.264 for video and G.711 A-law, G.711 u-law, and AAC for audio. The secondary stream supports MJPEG for video and does not support 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, and 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 6000 Series IP Camera Video Stream Support for 16:9 Aspect Ratio

Primary (H264)	FPS	Bit Rate	Secondary (H264 or MJPEG)	FPS	Bit Rate
1920 x 1080	20, 25, 30	2M, 4M, 6M, 8M, 10M, 12M, 15M	NA	–	–
1920 x 1080	15	2M, 4M, 6M, 8M, 10M, 12M, 15M	1024 x 576	10, 15	64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M
	6, 8, 10	2M, 4M, 6M, 8M, 10M		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
				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
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

Table 4-1 Cisco Video Surveillance 6000 Series IP Camera Video Stream Support for 16:9 Aspect Ratio (continued)

Primary (H264)	FPS	Bit Rate	Secondary (H264 or MJPEG)	FPS	Bit Rate
				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
			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

Table 4-1 Cisco Video Surveillance 6000 Series IP Camera Video Stream Support for 16:9 Aspect Ratio (continued)

Primary (H264)	FPS	Bit Rate	Secondary (H264 or MJPEG)	FPS	Bit Rate
				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
			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

Table 4-1 Cisco Video Surveillance 6000 Series IP Camera Video Stream Support for 16:9 Aspect Ratio (continued)

Primary (H264)	FPS	Bit Rate	Secondary (H264 or MJPEG)	FPS	Bit Rate
				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
				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 6000 Series IP Camera Video Stream Support for 16:9 Aspect Ratio (continued)

Primary (H264)	FPS	Bit Rate	Secondary (H264 or MJPEG)	FPS	Bit Rate
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
			640 x 368	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 6000 Series IP Camera Video Stream Support for 16:9 Aspect Ratio (continued)

Primary (H264)	FPS	Bit Rate	Secondary (H264 or MJPEG)	FPS	Bit Rate
			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
	1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M, 2M, 4M	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

Table 4-1 Cisco Video Surveillance 6000 Series IP Camera Video Stream Support for 16:9 Aspect Ratio (continued)

Primary (H264)	FPS	Bit Rate	Secondary (H264 or MJPEG)	FPS	Bit Rate
			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
352 x 208	20, 25, 30	64K, 128K, 256K, 384K, 768K, 1M	352 x 208	10, 15	64K, 128K, 256K, 384K, 768K
	10, 15	64K, 128K, 256K, 384K, 768K		1, 3, 5, 6, 8	64K, 128K, 256K, 384K
	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
320 x 192	20, 25, 30	64K, 128K, 256K, 384K, 768K, 1M	320 x 192	10, 15	64K, 128K, 256K, 384K, 768K
	10, 15	64K, 128K, 256K, 384K, 768K		1, 3, 5, 6, 8	64K, 128K, 256K, 384K
	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
192 x 112	20, 25, 30	64K, 128K, 256K, 384K	192 x 112	10, 15	64K, 128K, 256K
	10, 15	64K, 128K, 256K		1, 3, 5, 6, 8	64K, 128K
	1, 3, 5, 6, 8	64K, 128K	160 x 96	10, 15	64K, 128K, 256K
				1, 3, 5, 6, 8	64K, 128K
160 x 96	20, 25, 30	64K, 128K, 256K, 384K	160 x 96	10, 15	64K, 128K, 256K
	10, 15	64K, 128K, 256K		1, 3, 5, 6, 8	64K, 128K
	1, 3, 5, 6, 8	64K, 128K			

Table 4-2 Cisco Video Surveillance 6000 Series IP Camera Video Stream Support for 4:3 Aspect Ratios

Primary (H264)	FPS	Bit Rate	Secondary (H264 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 6000 Series IP Camera Video Stream Support for 4:3 Aspect Ratios (continued)

Primary (H264)	FPS	Bit Rate	Secondary (H264 or MJPEG)	FPS	Bit Rate
	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	352 x 288	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		1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M
	1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M	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
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		1, 3, 5, 6, 8	64K, 128K, 256K, 384K, 768K, 1M
	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
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 6000 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
Current Stream Area	
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. **Note** Stream 2 can be enabled only if Stream 1 is set to a video resolution lower than 1920 x 1080.
Streaming Area **Note** Each video stream uses its own set of streaming options. The settings shown in the **Streaming Area** apply to the currently selected stream only.	
RTSP Port	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. RTSP is a standard for connecting a client to control streaming data over the web. Valid values are 554 and 1024 through 65535. The default port is 554.
Video Source Port	Universal Datagram Protocol (UDP) port on which the IP camera transmits Video Real-Time Transport Protocol (RTP) data. Valid values are even numbers 1024 through 65534. The default port is 1024.
Audio Source Port	UDP port on which the IP camera transmits audio RTP data Valid values are even numbers 1024 through 65534. The default value is 1026.
Max RTP Packet Size	Maximum number of bytes per data packets that are sent in each RTP request. Configure a lower number if you are streaming video to a cell phone that requires smaller data packets. Valid values are 400 through 1400. The default value is 1400.
Enable Multicast	Check this check box to send video and audio data as a multicast stream. 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 signal from the IP camera simultaneously.
Multicast Address	Enter the multicast IP address on which the IP camera sends a multicast audio/video stream.
Multicast Video Port	Enter the port on which the IP camera sends a multicast video stream. Valid values are even numbers 1024 through 65532.
Multicast Audio Port	Enter the port on which the IP camera sends a multicast audio stream. Valid values are even numbers 1024 through 65532.

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.
Video Area	
Note Each video stream uses its own set of video options. The settings shown in the **Video Area** 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	*Display only*: Shows the codec for video transmission: H.264 for the primary stream and MJPEG for the secondary stream.
Video Resolution	Choose the resolution for video transmission. The resolutions in this drop-down list depend on the video standard that you selected. You can also change the resolution for video transmission by using the Video Resolution drop-down list in the Camera Video & Control window, as described in Table 3-1.
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: • **Constant Bit Rate**—Available for the primary stream only. Specifies that the video stream is output at or close to the constant bit rate that you choose. The default value is 4 Mbps. A higher bit rate provides better video quality but consumes more bandwidth. • **Fixed Quality**—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. 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.
Analog Video Area	
Note 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: • The primary video stream frame rate must be set to 15 fps or lower. • The secondary video stream must be disabled.
Audio Area	
Enable Audio	Check this check box if you want to enable audio.

Table 4-4 Streaming Window Options (continued)

Option	Description
Audio Codec	Choose the audio codec to use for encoding audio: • **G.711 A-Law**—Encodes 14-bit signed linear PCM samples to logarithmic 8-bit samples. • **G.711 u-Law**—Encodes 13-bit signed linear PCM samples to logarithmic 8-bit samples. **Note** The G.711 A-law algorithm provides more quantization levels at lower signal levels whereas the G.711 µ-law algorithm tends to give more resolution to higher range signals.
Audio Sampling Rate	*Display only.* Displays the sampling rate for audio from the IP camera.
Audio Resolution	*Display only.* Displays the resolution for audio 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
Microphone	
Microphone Type	The Cisco 6000 Series IP cameras support only an external microphone. Audio is captured by an optional external microphone, available from third-parties.
Day Night Filter Area	
Switch Mode	Choose the day/night mode for the IP camera: • **Day**—IP camera always remains in day mode. • **Night**—IP camera always remains in night mode. • **Auto**—IP camera automatically switches between day and night mode based on the lighting condition threshold that you specify. • **Night External**—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. • **Night Schedule**—IP camera switches to and from Night mode based on the Start and End times. **Note** If you configure a Night Schedule, make sure that the time on the IP camera is set correctly.
Day to Night Threshold	(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. The default value is 10.
Night to Day Threshold	(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. The default value is 15.
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	(The Output option is available only when the Switch Mode is set to Night External.) Choose the Output port that is connected to an external device that is to be triggered.

Table 4-5 Camera Window Options (continued)

Option	Description
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.

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
Text Overlay Area	
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 **Left**, **Center**, or **Right**.
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.
Date/Time alignment in Overlay	Choose whether the Date/Time is to be aligned to the **Left**, **Center**, or **Right**.

Table 4-6 Video Overlay Window Options (continued)

Option	Description
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 **Left**, **Center**, or **Right**.
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 **Top of Image** or **Bottom of Image**.

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
Input Ports Area	
Port #	*Display only.* Indicates input port 1, input port 2, and input port 3.

Table 4-7 IO Ports Window Options (continued)

Option	Description
Current State	*Display only.* 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.
Output Ports	
Port #	*Display only.* Indicates output port 1.
Current State	*Display only.* 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 **Save**. The default setting is High.
Event Action	*Display only.* 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 events. An event 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 controls" rows in Table 3-1.
- Loss of video signal.

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

- 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.
- 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.

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
Event Triggering Area	
Triggered by	Check the desired check boxes to designate the events that trigger actions: **Input 1**—Event is triggered when input port 1 on the IP camera changes state from high to low. **Input 2**—Event is triggered when input port 2 on the IP camera changes state from high to low. **Input 3**—Event is triggered when input port 3 on the IP camera changes state from high to low. **Motion Detection**—Event is triggered when the camera detects motion, if motion detection is configured as described the "Motion detection controls" rows in Table 3-1. **Video Loss**—Event is triggered if the IP camera loses input to its codec sensor module.
Actions	Check the desired check boxes to designate that actions that the IP camera takes when the corresponding trigger occurs. • **Email**—Sends information about the event 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. • **Output 1**—Changes the state of the output 1 port on the IP camera as defined in the Port window. • **Syslog**—Sends information about the event to a designated Syslog server. • **HTTP**—Sends information about the event as an HTTP stream to a remote system.
Interval	Choose the time interval (in minutes) from the drop-down list to wait after an event occurs before detecting the next event.
Event Scheduling Area	
Scheduling Grid	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. 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.
Set All button	Select all times in the scheduling grid.
Clear All button	Deselect all times in the scheduling grid.
Undo All button	Change the scheduling settings to the last saved configuration.
HTTP Notification Area	
Primary HTTP Server	Identify the primary server to which HTTP messages are sent by choosing **IP Address** or **Hostname** from the drop-down list and entering the IP address or host name in the corresponding field.

Table 4-8 Event Notification Window Options (continued)

Option	Description
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 *IP address* is the IP address of the destination server, *URL Base* is the string that you enter, and *system-provided-name-value-pairs* 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. **Note** 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	Identify an optional secondary server to which HTTP messages are sent by choosing **IP Address** or **Hostname** 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 *IP address* is the IP address of the destination server, *URL Base* is the string that you enter, and *system-provided-name-value-pairs* 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. **Note** Invalid special characters are: []\&|:";<>?,/+=*'%# blank
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.
Email Notification Area	
Primary SMTP Server	Identify the primary SMTP server that is used for sending e-mail by choosing **IP Address** or **Hostname** 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.

Table 4-8 Event Notification Window Options (continued)

Option	Description
POP Server	Identify the primary POP server that is used for sending e-mail by choosing **IP Address** or **Hostname** 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 **Requires POP Before SMTP** 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 **IP Address** or **Hostname** 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 **IP Address** or **Hostname** 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 **Requires POP Before SMTP** 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.
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.

Table 4-8 Event Notification Window Options (continued)

Option	Description
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. **Note** This functionality is available only when the secondary video stream is enabled.

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 5-4
- Discovery Window, page 5-6
- IP Filter Window, page 5-7
- QoS Window, page 5-8

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
Basic Settings Area	
ID	Enter a unique identification for the IP camera, which is used to identify the IP camera to various external applications. The ID can contain up to 64 numbers.
Name	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. The name can contain up to 64 characters, which can include letters, numbers, spaces, and these characters: ! $ % ( ) + , - . / = @ ^ _ ` { } ~. We recommend that you give each IP camera a unique name so that you can identify it easily.
Description	Enter a description of the IP camera. For example, enter the IP camera location, such as "North Entrance Camera 1." The description can contain up to 128 characters, which can include letters, numbers, spaces, and these characters: ! $ % ( ) + , - . / = @ ^ _ ` { } ~
Location	Enter the physical location of the IP camera, such as "North Entrance." The location can contain up to 64 characters, which can include letters, numbers, spaces, and these characters: ! $ % ( ) + , - . / = @ ^ _ ` { } ~
Contact	Enter system contact information for someone such as the system administrator. For example, enter the e-mail address of the system administrator. The contact can contain up to 64 characters, which can include letters, numbers, spaces, and these characters: ! $ % ( ) + , - . / = @ ^ _ ` { } ~
Basic Device Operations Area	
Enable Power LED	Check this check box if you want the Power LED on the back of the IP camera to light. If you do not check this check box, this LED does not light.
Disable Session ID	The following camera API mechanisms are available: • 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: http://www.cisco.com/en/US/products/ps10818/products_user_guide_list.html • Basic Authentication—Requires a user ID and password to be passed with every API command. SessionID is enabled by default. To disable SessionID, and enable Basic authentication, check this option.

Table 5-1 Basic Window Options (continued)

Option	Description
Enable ONVIF	Check this check box if you want the IP camera to work in Open Network Video Interface Forum (ONVIF) mode. The following features are supported: • Device Discovery Service • Device Service • Media Service Enabling ONVIF disables SessionID as indicated by the informational message that appears after you click the check box. Click **Save** to be redirected to the login page. After login, ONVIF service starts working. You can verify this service by using any ONVIF tool. By default, ONVIF is disabled. **Note** We recommend that you do not enable ONVIF when using Cisco VSM to avoid conflicts with configuration.

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
IP Addressing Area	
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	Choose the method by which the IP camera obtains its IP address: • **Dynamic**—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. • **Static**—Choose this option if you want to manually enter an IP address, subnet mask, default gateway, and DNS server IP addresses for the camera.
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	*Optional*. 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. 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.
Secondary DNS	*Optional*. Enter the IP address of a secondary (backup) DNS server to use if the primary DNS server is unavailable. 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.

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
Set Time Mode Area	
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.
Local Time Area **Note** 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 **Save**.
Set Local Time	Enter a time for the IP camera. The camera is updated with this time when you click **Save**.
Clone PC Time button	Click this button to update the IP camera date and time with the date and time of the PC that you are using.
Time Zone and Daylight Saving Area	
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.
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	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. The camera automatically adjusts its time back by this number of minutes when daylight saving time ends.
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.

Table 5-3 Time Window Options (continued)

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

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
Cisco Discovery Protocol (CDP) Area	
Show Neighbors button	Click this button to display a new window with information about CDP-enabled device neighbors in your network.

Table 5-4 Discovery Window Options (continued)

Option	Description
Bonjour Area	
Enable Bonjour	Check this check box if Bonjour is enabled in your network and you want the IP camera to broadcast Bonjour discovery messages.
Cisco Video Surveillance Media Server (VSMS) Area	
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.

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 may need to scroll down to it.

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

Table 5-5 IP Filter Window Options

Option	Description
IP Filter Area	
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.
Filter Entries Area	
#	*Display only.* Filter number.
Action	Choose an action for the corresponding IP address or address range: • **Deny**—IP address or address range cannot access the IP camera. • **Allow**—IP address or address range can access the IP camera.

Table 5-5 IP Filter Window Options (continued)

Option	Description
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 may need to scroll down to it.

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

Table 5-6 QoS Window Options

Option	Description
Class of Service (CoS) Area	
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.

Table 5-6 QoS Window Options (continued)

Option	Description
Differentiated Services (DiffServ) Area	
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.
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.

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 6-1
- User Window, page 6-3
- Maintenance Window, page 6-4
- Firmware Window, page 6-6
- Device Processes Window, page 6-7
- Password Complexity Window, page 6-8

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 6-1 describes the options in the Initialization window.

Table 6-1 Initialization Window Options

Option	Description
Administrator Accounts Area	
Protocol	*Display only.* Indicates the protocol that the corresponding administrator can use to access the IP camera: HTTP/HTTPS or SSH.
User Name	*Display only.* 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.
Access Protocols Area	
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
  - 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 6-2 describes the options in the User window.

Table 6-2 User Window Options

Option	Description
User List Area	
User Name	Enter a unique name for the user. The user name is case sensitive and can include up to 64 letters, numbers, and special characters, but no spaces. Special characters are: ! % ( ) + , - = @ _ ~ There is always one user named admin (all lower case), which cannot be deleted.

Table 6-2 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: • **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.
Change button	Click this button to change the password of the corresponding user.
Add button	Click this button to add the corresponding user. That user can then log in to the IP camera.
Delete 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 6-3 describes the options in the Maintenance window.

Table 6-3 Maintenance Window Options

Option	Description
Factory Default Area	
Restore button	Click the **Restore** button to reset all IP camera settings to their factory default values. To confirm the restore procedure, click **OK** in the confirmation pop-up window. Otherwise, click **Cancel**. This action has the same effect as pressing and holding the **Reset** button on the IP camera for at least 15 seconds. After you perform this procedure, follow the steps in the Chapter 2, "Performing the Initial Setup of the IP Camera."
Reset button	Click the **Reset** 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. To confirm the restore procedure, click **OK** in the confirmation pop-up window. Otherwise, click **Cancel**.
Reboot Area	
Reboot button	Click the **Reboot** button to reboot the software on IP camera. To confirm the reboot procedure, click **OK** in the confirmation pop-up window. Otherwise, click **Cancel**. 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.
Device Configuration Area	
Export Configuration from Camera	Click the **Export** button to save the current IP camera configuration information to a binary file. When you click this button, the File Download window appears. Use this window to save the configuration file. 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.

Table 6-3 Maintenance Window Options (continued)

Option	Description
Import configuration to camera	Path and folder where a configuration file is stored. You can click **Browse** to find this location. After you enter this information, click **Import** to load the configuration file to the IP camera. After you upload a configuration file to the IP camera, the IP camera restarts automatically. 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 "Basic Window" section on page 5-1 and the "IP Addressing Window" section on page 5-3. 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.
Camera Logs Area	
Export Logs from Camera	Click the **Export** button to save the current IP camera log information. Downloading the logs might take some time depending on their size. When you click this button, the File Download window appears. Use this window to save the log file.

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

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 6-4 describes the options in the Firmware window.

Table 6-4 Firmware Window Options

Option	Description
Device Information Area	
IP Address	*Display only.* IP address of the IP camera
MAC Address	*Display only.* MAC address of the IP camera.
Device Name	*Display only.* ID of the IP camera, as configured in the Basic window. For more information, see the "Basic Window" section on page 5-1.
Firmware Maintenance Area	
Firmware Version	Version of the firmware that is installed on the IP camera.
Firmware Released Date	Release date of the current firmware.
Details 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 **Browse** to find this location.
Upgrade 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 6-5 describes the options in the Device Processes window. All options are for display only.

Table 6-5 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 6-3. 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 6-6 describes the options in the Password Complexity window.

Table 6-6 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: • Lower case letters (a through z) • Upper case letters (A through Z) • Digits (0 through 9) • Special characters: ! " # $ % & ' ( ) * + , - . : ; < = > ? @ [\ ] ^ _ ` { | } ~

Table 6-6 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 of reversed.

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 7-1
- Local Log Window, page 7-4

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 7-1 describes the options in the Log Setup window.

Table 7-1 Log Setup Window Options

Option	Description
Local Log Settings Area	
Minimum Log Severity	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: • **Emergency**—The system is unusable. • **Alert**—A situation occurred that requires immediate action. • **Critical**—A situation occurred that requires action soon. • **Error**—An error occurred, but it does not necessarily affect the ability of the system to function. • **Warning**—A undesirable condition occurred. • **Notice**—Notification about a system condition that is not necessarily an error condition. • **Informational**—Information about a system activity. • **Debug**—Information about a system activity with detailed technical information. Includes messages of every other severity. The default severity is Informational.
Maximum Log Entries	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. The default value is 100.
Syslog Settings Area	
Enable Syslog	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. This option is useful for consolidating logs in deployments with several IP cameras and for retaining logs.
Primary Syslog Server	Identify the primary Syslog server by choosing **IP Address** or **Hostname** 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 7-1 Log Setup Window Options (continued)

Option	Description
Minimum Log Severity	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: • **Emergency**—The system is unusable. • **Alert**—A situation occurred that requires immediate action. • **Critical**—A situation occurred that requires action soon. • **Error**—An error occurred, but it does not necessarily affect the ability of the system to function. • **Warning**—A undesirable condition occurred. • **Notice**—Notification about a system condition that is not an error condition. • **Informational**—Information about a system activity. • **Debug**—Information about a system activity with detailed technical information. Includes messages of every other severity. The default severity is Informational.
Secondary Syslog Server	Identify an optional secondary Syslog server by choosing **IP Address** or **Hostname** 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	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: • **Emergency**—The system is unusable. • **Alert**—A situation occurred that requires immediate action. • **Critical**—A situation occurred that requires action soon. • **Error**—An error occurred, but it does not necessarily affect the ability of the system to function. • **Warning**—An undesirable condition occurred. • **Notice**—Notification about a system condition that is not an error condition. • **Informational**—Information about a system activity. • **Debug**—Information about a system activity with detailed technical information. Includes messages of every other severity.

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 7-2 describes the options in the Local Log window.

Table 7-2 Local Log Window Options

Option	Description
Log List Area	
Rows per page	Choose the number of log entry rows to display per page and click the **Go** 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 **All**.
Since	Choose the time period for which you want to view log messages.
Go button	Update the log display based on the values in the Filter and Since fields.
Severity	An icon in this column indicates the severity of the corresponding log message: —Emergency message —Alert message —Critical message —Error message —Warning message —Notice message —Informational message —Debug message 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.
Date/Time	Date and time that the logged activity occurred. 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.

Table 7-2 Local Log Window Options (continued)

Option	Description
Description	Message that describes the logged activity. For detailed information about log messages, see Table 7-3 on page 7-5.
Page controls	Let you move through the log file entries: Page field—Enter a page number and press Enter.  —Go to first page  —Go to previous page  —Go to next page  —Go to last page

Table 7-3 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 7-3 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 7-3 Log Messages

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 7-3 Log Messages

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

Table 7-3 Log Messages

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

A

About link 1-5
Account Initialization window
  options 6-2
action
  triggered by event 4-18
ActiveX controls 1-4
Administration windows 6-1, 7-1
audio
  controls in Camera Video & Control window 3-3
  settings 4-13

B

backing up, configuration of IP camera 6-4
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
  picture adjustments
    white balance 3-5
Camera Settings window
  options 4-15
  overview 4-14
Camera Video & Control window
  accessing 3-1
  description 1-5
  displaying 1-4
configuration windows
  accessing 1-2
  Administration windows 6-1
  Basic Settings window 5-1
  Camera Settings window 4-14
  Device Processes window 6-7
  Discovery Settings window 5-6
  Event Notification window 4-18
  Feature Setup windows 4-1
  Firmware Settings window 6-6
  Initialization window 6-1
  IO Ports Settings window 4-17
  IP Addressing window 5-3
  IP Filter Settings window 5-7
  Local Log window 7-4
  Log Setup Settings window 7-1
  Log windows 7-1
  Maintenance Settings window 6-4
  Network Setup windows 5-1
  Password Complexity window 6-8
  QoS Settings window 5-8
  Streaming Settings window 4-1
  Time Settings window 5-4
  User Settings window 6-3
  Video Overlay Settings window 4-16
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 6-8
- overview 6-7

DHCP, obtaining IP address through 2-1, 5-4
Differentiated Services (DiffServ) 5-9
Discovery Settings window
- options 5-6
- overview 5-6

DNS server
- primary 5-4
- secondary 5-4

dual streaming 4-1

E

e-mail notification
- configuring 4-20, 4-21
- From field 4-22
- recipients 4-22

event
- actions
  - email notification 4-19
  - HTTP notification 4-18
  - output port state change 4-19
  - syslog server message 4-19
- overview 4-18
- trigger types 4-20

Event Notification window
- options 4-20
- overview 4-18

F

factory default configurations, resetting 6-5
factory default configurations, restoring 6-5
Feature Setup windows 4-1
firmware
- upgrading 6-6, 6-7
- version in IP camera 6-7

Firmware Settings window
- options 6-7
- overview 6-6

flickerless 3-5
focus/zoom
- accessing controls 3-8
- controls 3-8

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, 6-2
- default port 6-2
- port 6-2

HTTPS
- accessing camera through 1-3
- allowing access through 6-2
- default port 6-2
- port 6-2

I

Initialization window
  overview 6-1
input ports
  state change 4-18
IO Ports Settings window
  options 4-17
  overview 4-17
IP address
  controlling access by 5-7
  default for IP camera 1-3, 2-1
  fixed 5-4
  obtaining from DCHP 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 5-7
  day mode 4-14
  logging in to 1-4
  logging out of 1-4
  MAC address 6-7
  name 5-2
  night mode 4-14
  overview 1-1
  panning 3-2
  rebooting 6-5
  restarting 6-5
  restoring factory default configurations 6-5
  tilting 3-2
  time zone 5-5
  windows 1-2, 1-5
IP Filter Settings window
  options 5-7
  overview 5-7

L

live video
  viewing
    through home window 3-1
    through third-party device or software 3-1
  See also video
Local Log window
  options 7-4
  overview 7-4
log file
  sending to Syslog server 7-2
  storage of 7-1
  viewing 7-4
log in, to IP camera 1-4
log out, of IP camera 1-4
Log Setup Settings window
  options 7-2
  overview 7-1

M

MAC address, of IP camera 6-7
Maintenance Settings window
  options 6-5
  overview 6-4
microphone
  muting PC 3-3
  PC 3-3
  sensitivity 3-3
  use 4-14
motion detection
  accessing controls 3-4, 3-6, 3-8
  enabling 3-7
Motion detection controls 3-7, 3-9

multicast
address 4-12
enabling 4-12
port 4-12
muting
PC microphone 3-3
PC speaker 3-3

N

name, of IP camera 5-2, 6-7
Network Setup windows 5-1
night
filter 4-14
mode 4-14

O

output ports
power on state 4-18

P

panning 3-2
password
complexity 6-8
configuring requirements for 6-8
for primary SMTP server 4-22
for secondary SMTP server 4-22
for user 6-4
hardening 6-8
requirements for 2-2, 6-4
Password Complexity window
options 6-8
overview 6-8
picture adjustments
white balance 3-5
port number 1-3
processes
descriptions 6-8
stopping 6-7

Q

QoS Settings window
options 5-8
overview 5-8
quality of service 5-8

R

rebooting, IP camera 6-5
Refresh link 1-4
resetting, factory default configurations 6-5
restarting, IP camera 6-5
restoring, factory default configurations 6-5

S

saturation 3-4
secure connection 1-3
security
controlling processes 6-7
password hardening 6-8
stopping processes 6-7
Setup window
description 1-5
displaying 1-4
sharpness 3-4
speaker
volume 3-3
SSH
allowing access through 6-2
alternative port 6-2
default port 6-2
Streaming Settings window

options 4-12
overview 4-1
subnet mask, of IP camera 5-4
Syslog server 7-2

T

text overlay, on video 4-16, 4-17
tilting 3-2
Time Settings window
options 5-5
overview 5-4
time stamp, on video 4-16
time zone, of IP camera 5-5
trigger, for event 4-20

U

user, password 6-4
user name, requirements for 6-3
User Settings window
options 6-3
overview 6-3

V

video
bit rate 4-13
primary stream 4-1
quality 4-13
secondary stream 4-1
text overlay 4-16, 4-17
time stamp on 4-16
viewing live
through Home window 3-1
through third-party device or software 3-1
See also live video
video codec
controls in Camera Video/Control window 3-1
display in Streaming Settings window 4-13
video image
optimizing for lighting condition 4-14
Video Overlay Settings window
options 4-16
overview 4-16
video resolution
configuration guidelines 4-1
controls in Camera Video/Control window 3-2
View Video link 1-4

W

white balance mode 3-5

Z

zoom
accessing controls 3-8
zoom controls 3-8