ADMINISTRATION GUIDE

Cisco Small Business

VC240 Bullet Network Camera

Document Revision Number 78-19564-01B0

Contents

1

Introduction

Thank you for purchasing the Cisco Small Business VC240 Indoor/Outdoor Wide Dynamic Range (WDR) Day/Night PoE Network Camera. The Cisco VC240 is a standalone camera that can be connected directly to an Ethernet network. It provides an all-in-one indoor/outdoor video camera solution by incorporating a weather-resistant enclosure with a removable sun shield. The camera provides flexibility to be mounted indoors or outdoors on a wall or roof.

The Cisco VC240 camera features day and night functions for 24-hour surveillance purposes, with configurable IR illuminators. The light sensor detects the amount of ambient light and switches the camera from day to night mode. If light is too low, the light sensor triggers the IR LEDs to turn on to offer infrared light for up to 50 feet (15 meters). Therefore, the Cisco VC240 delivers high image quality in either day and night conditions.

By enabling Wide Dynamic Range (WDR), the camera can compensate for challenging lighting conditions. Use WDR when there are both very bright and very dark areas simultaneously in the field of view of the camera. The WDR feature captures both the bright and dark parts of an image and combines the differences to generate a highly realistic image representative of the original scene. The video quality achieved is close to the capabilities of the human eye. WDR is widely applied in high contrast environments such as lobby entrances, parking lots, ATMs, or loading areas.

NOTE Before installing a surveillance system, check with local government agencies to determine if video surveillance and audio monitoring are permitted in your area.

Features of the Cisco VC240

- Provides an optimal combination of viewing live and stored video by using simultaneous dual codecs (MPEG-4, MJPEG).
- Provides a 1/3.3 Wide Dynamic Range (WDR) CMOS sensor to support Auto Gain Control (AGC), Auto White Balance (AWB) and Auto Exposure Control (AEC).
- Features a 3.3 mm x 12 mm varifocal lens with 3.63x manual zoom.
- Provides a built-in light sensor to detect the amount of ambient light and switch the camera from day to night. If light is too low, the light sensor triggers the IR LEDs to turn on.
- Allows for day or night video surveillance with 12 built-in IR illuminators, with a range of up to 50 feet (15 meters) in complete darkness.
- Provides input and output audio connectors so you can use an external microphone and/or speakers.
- Provides I/O ports so you can set up external devices or turn on/off lights.
- Provides an RS-485 port which allows you to control a Pan Tilt Zoom (PTZ) camera for more flexible viewing.
- Allows for flexible installations with Power over Ethernet (PoE).
- Easily installs outdoors with its IP 66 weather-resistant enclosure and removable sun shield. Indoors, the protective enclosure allows for viewing in harsh and dusty conditions.
- Supports RTSP Video/Audio Streaming to Unicast and Multicast clients.
- Allows viewing of video on a mobile device with 3GPP support.
- Provides motion detection event triggering.
- Supports privacy masks that allow you to block specified areas where you don't want to view or record activity.
- Includes basic Cisco Video Monitoring System software that can be used with up to 16 cameras.

  The Cisco VC240 camera is also fully compatible with the Cisco Advanced Video Monitoring System software that provides monitoring for up to 64 cameras. The advanced video monitoring software is not included. See www.cisco.com/go/avms for more information.
- Allows JPEG snapshots at multiple resolutions to be sent to an FTP server.

- Provides timestamp and text overlay on images.
- Allows for up to 10 unicast users and unlimited multicast users.
- Provides a built-in web server for remote access over IP, and secure control over HTTPS or HTTP via Digest Encryption.

Minimum Requirements

The following table lists the minimum requirements for your computer when using the Cisco VC240 network camera.

NOTE These storage requirements are approximate. Number of cameras, lighting, frame rate, codec, and resolution can all affect the storage size.

Minimum System Requirements	
CPU	2GHz Pentium 4, or AMD Athlon Class CPU For multiple cameras: Pentium 4 class, 3 GHz dual-core
Memory	1 to 2 GB
Operating System	Microsoft Windows XP, Windows 7, or Vista
Hard Drive	500 MB of available space
Graphics Card	AGP or PCI Express with a minimum 128 MB For multiple cameras: NVidia high performance or equivalent with a minimum of 256 MB
Browser	Internet Explorer 6.x (or later) with ActiveX support for viewing, recording, playback and setting motion detection. Limited support for Apple Safari and Mozilla Firefox (no motion detection, instant recording, or audio control due to lack of ActiveX).

Multiple cameras can be monitored if you reduce the resolution and frame rate settings for the video captures. For more information about making these settings, see **Camera Control > Video Settings, page 61**.

Where to Go Next

For hardware installation instructions, start here:

- **Getting to Know the Cisco VC240 Network Camera, page 10**

For software installation instructions, start here:

- **Installing the Cisco VC240 Network Camera Software, page 29**

2

Getting to Know the Cisco VC240 Network Camera

This chapter contains the following information:

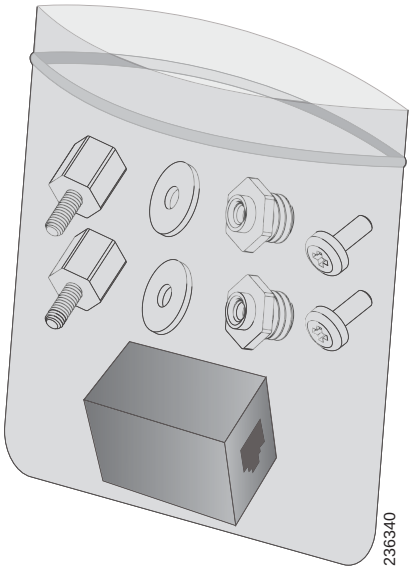
Package Contents

When you receive the camera package, it should contain the following:

- Cisco VC240 Outdoor Network Camera
- Mounting and Installation Accessories
- Open-end Wrench and Allen Wrench
- Female-to-Female Ethernet Adapter
- I/O and RS-485 Connectors
- Sun Shield
- Camera Stand
- Setup and Documentation CD
- Quick Start Guide

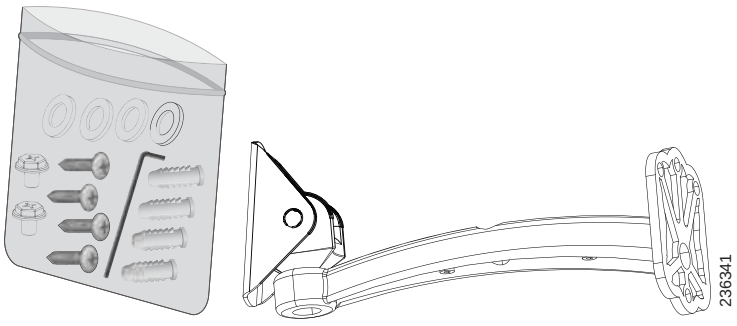
The mounting and installation accessories include the following:

- Screws and RJ45 Ethernet Female/Female Coupler:



  - 1 Ethernet female/female coupler
  - 2 screws (M3 x 8 mm)
  - 2 M3 washers
  - 2 M6-to-M3 male-to-female adapters
  - 2 M3-to-M6 male-to-female adapters

- Camera Stand Installation Accessories:

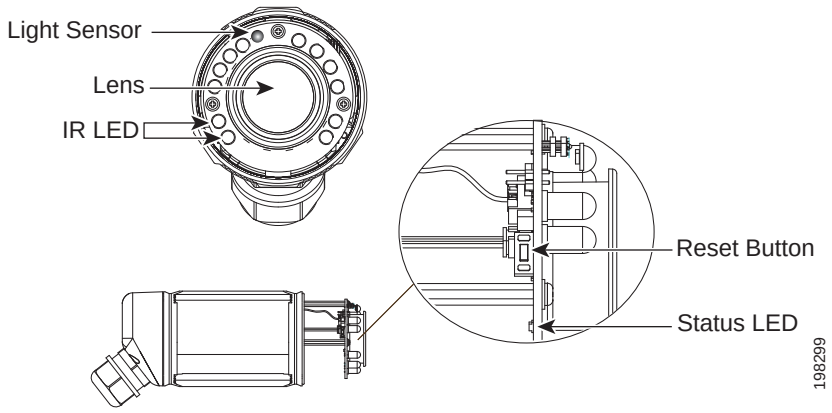


  - 4 #6M anchors

- 1 Allen wrench (5 mm)
- 4 washers (6 mm)
- 2 hex-head bolts (6 mm x 8 mm)
- 4 self-tapping screws (M4 x 32 mm)

Camera Details

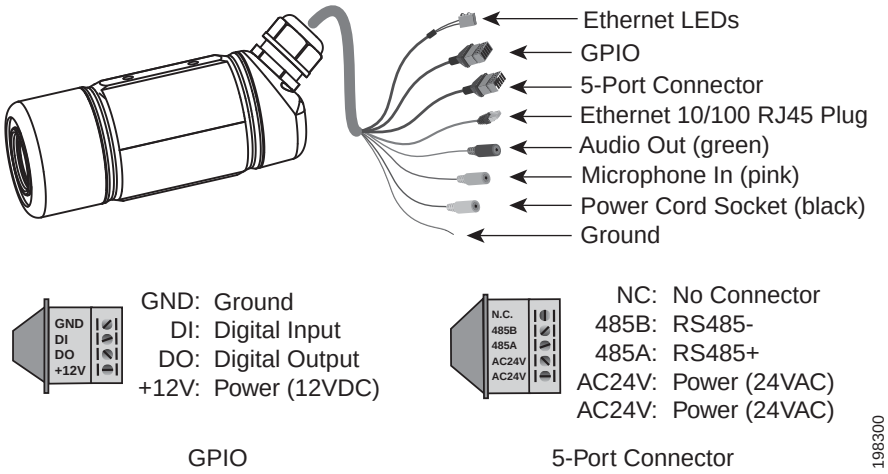
Front Panel



Light Sensor	Detects the amount of ambient light and switches the camera from day to night mode. If light is too low, the light sensor triggers the IR LEDs to turn on.
Lens	• Computar varifocal board lens 3.3–12mm F/1.4 • Viewing angle 23.9–89.8° (horizontal) • Removable IR-cut filter with focus compensation • Manual zoom (3.5x)
IR LED	Enables operation in complete darkness. The ring of 12 infrared (IR) LEDs are built-in with a working range of 50 feet (about 15 meters).

Reset Button	Allows you to perform two functions: • **Reset**—Press and hold the Reset button for less than five seconds to reset the camera. • **Restore Factory Defaults**—Press and hold the Reset button over five seconds until the Status LED is flashing red every 0.2 seconds.
Status LED	• **Light off**—Power is off or Status LED is off. • **Flashing red every second**—Camera and network are functioning (heartbeat). • **Steady red**—Network failure. • **Flashing red every 2 seconds**—Audio is disabled. • **Flashing red every 0.2 seconds**—Restoring default settings. • **Flashing red every 0.5 seconds**—Upgrading firmware.

Back Panel



Ethernet LEDs	The green and amber Status LEDs indicate status. If powered using PoE: • **Green steady, amber steady**—Power on. • **Green blinking, amber steady**—Power on with Ethernet data activity. If powered using an external power adapter: • **Green steady, amber off**—Power on. • **Green blinking, amber off**—Power on with Ethernet data activity.
General Purpose Input/ Output (GPIO)	See **General Purpose Input and Output Terminal Block, page 15** for more information.
5-Port Connector	Connects the camera to 24 VAC power (0.5 A) or serves as an RS-485 port.
Ethernet 10/100 RJ45 Plug	Connects the Cisco VC240 camera to a PoE switch or router, or to a PoE power injector (not provided) for connection to a non-PoE switch or router.
Audio Out (green)	Connects the Cisco VC240 camera through the 3.5 mm input jack to an external speaker or computer.

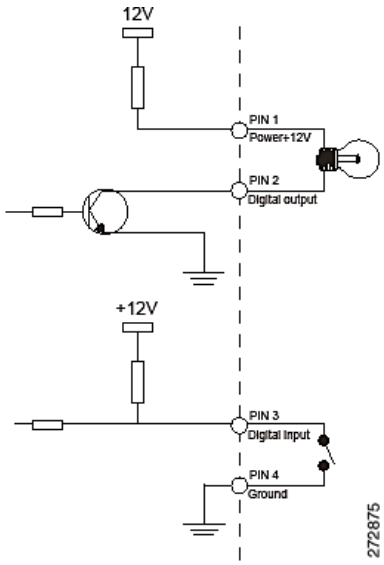
Microphone In (pink)	Connects the Cisco VC240 camera through the 3.5 mm input jack to an external microphone.
Power Cord Socket (black)	Connects the Cisco VC240 camera to 12 VDC (1 A) power when not using PoE or 24 VAC.
Ground	Connects the Cisco VC240 camera to ground.

General Purpose Input and Output Terminal Block

The GPIO allows you to connect the camera to external input/output devices that can provide additional controlling functions. The ports are numbered 1 through 4 and are described in the following table:

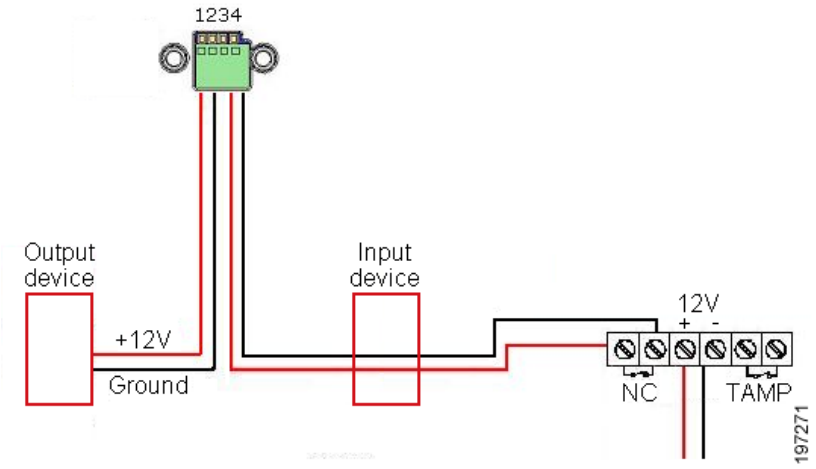
Port #	Description
1	Power 12VDC +- 5% 1.5A max, Max rating 2.0A
2	Digital output Max. 40 VDC, Max. 400mA, isolation 2kV
3	Digital input Open/short-to-ground, isolation 2kV, internal pull-up
4	Ground

Ports 1 to 4 are used to connect with digital input and digital output devices. Refer to the following illustrations for the connection methods.



Ports 1 and 2 are for output devices. The external device must be 12V, 1.5A (2A maximum) or 18 W (24 W maximum).

Ports 3 and 4 are for input devices. The digital input is triggered when the device opens or closes the circuit between pin 3 and pin 4 (dependent on whether your input device is normally an open or closed device).



The state of your input device determines how to configure the ports on the Camera Control > I/O ports page found on **page 67**. If the input device is normally closed, set the configuration of Triggered When to **Low**. Set the output port to **Open**. For input devices that are normally open, set the configuration to **High** and **Open**.

See also **Configuring the GPIO Ports, page 109** for a sample configuration.

Cautions and Warnings

- Power off the Cisco VC240 network camera if smoke or unusual odors are detected. Contact your distributor immediately.
- Do not place the Cisco VC240 network camera on unsteady surfaces.
- Do not disassemble the Cisco VC240 network camera.
- Do not drop the Cisco VC240 network camera.
- Do not insert sharp or tiny objects into the camera.

Where to Go Next

For instructions on setting up your camera connections, start here:

- **Connecting the Cisco VC240 Camera, page 19**

For software installation instructions, start here:

- **Installing the Cisco VC240 Network Camera Software, page 29**

3

Connecting the Cisco VC240 Camera

This chapter describes how to connect the camera and contains the following sections:

Camera Installation Guidelines

Consider the following guidelines before installing and mounting your cameras. While the motion detection window and the degree of sensitivity can be optimized later, it is best to optimize your camera location during initial setup.

- Choose a location that provides adequate coverage of the area to be monitored.
- If using video motion detection, consider potential sources of movement that can create false positives, such as trees and shrubs, drastic light changes, wandering animals, and traffic.
- If using an external microphone or speaker, place the microphone far enough away from the speaker to avoid feedback. The volume of the speaker and the background noise of the environment will determine the exact distance, possibly up to one meter away.

Before You Begin

Before you begin the installation, make sure that you have the following equipment and services:

- Power over Ethernet (PoE)-enabled Ethernet network switch or an 802.3af-compliant PoE power injector
- Tools for installing the camera (drill, 1/4-inch drill bits, Phillips screwdriver, stud finder if attaching the camera to a dry wall)
- All the connections must be long enough to connect to the camera's 6-foot I/O connector
- PC with Microsoft Internet Explorer 6.x or later for accessing the camera's web-based configuration utility
- One or more Ethernet network switches

Placement Tips

- Ambient Temperature—To prevent the camera from overheating, do not operate it in an area that exceeds an ambient temperature of 140°F (60°C).
- Air Flow—Be sure that there is adequate air flow around the device to prevent the camera from overheating.
- Mechanical Loading—To avoid accidents or hazardous conditions, make sure the device is level, stable, and securely mounted.

Mounting the Cisco VC240 Camera

This section describes how to mount the camera. This does not include connecting the camera and adjusting the zoom and focus, which is covered later in this guide.

WARNING The power line of either 24 VAC or PoE is prohibited being exposed outdoor and bridged over buildings for surge protection by lightning strike.

WARNING Make sure the camera's Ground cable is connected to ground.

WARNING Make sure that all the camera's cables, including I/O and power, are connected to other devices in an indoor environment.

NOTE Install the VC240 camera with a UL-listed and marked outdoor conduit for the cable exposed in an outdoor environment.

NOTE You should reliably connect the VC240 camera to the main protective earthing terminal.

NOTE The VC240 camera uses a UL-listed AC/DC power adapter with a marked output rating of 12 VDC, 600 mA.

NOTE The VC240 camera uses a UL-listed AC/DC power adapter with a marked output rating of 24 VAC, 700 mA.

Mounting the Camera to a Wall or Ceiling

You can mount the Cisco VC240 camera on the flat surface of a wall or a ceiling. The flat surface must be smooth, dry, and sturdy. A mounting kit is provided that includes anchors (#8–#10 US) and screws (#8 US) to help you secure the camera to the wall or ceiling.

CAUTION Before drilling holes into the wall or ceiling when mounting the camera, make sure there are no electrical wires, water pipes, or other objects that might get damaged by the drilling.

NOTE If you plan on using the supplied sun shield with the camera, review the steps in the **Attaching the Sun Shield, page 98** before mounting the camera.

To adjust the camera's zoom and focus settings, wait until you can view live video from the camera. After mounting the camera as described in this section, follow the steps in the **Connecting the Equipment, page 25**, the "**Verifying the Hardware Installation, page 28**, and the **Installing the Camera, page 31** After you get live feed from the camera, follow the instructions in the **Adjusting the Lens, page 97** to adjust the zoom and focus settings.

WARNING Installation of the equipment must comply with local and national electrical codes. Statement 1074

STEP 1 Unscrew the Allen-head bolt from the bracket mount using the supplied Allen wrench.

STEP 2 Attach the bracket mount to the camera using the two supplied hex-head bolts (6 mm x 8 mm).

STEP 3 Place the bracket mount, with the camera attached to it, over the pivot of the camera stand.

STEP 4 Attach the bracket mount to the pivot using the supplied M6 Allen-head bolt and its M6 lock washer. Use the Allen wrench to tighten the screw.

STEP 5 Attach the base of the camera stand to the wall or ceiling:

a. Use the base of the camera stand to mark the location of the four holes that you are going to drill in the next step.

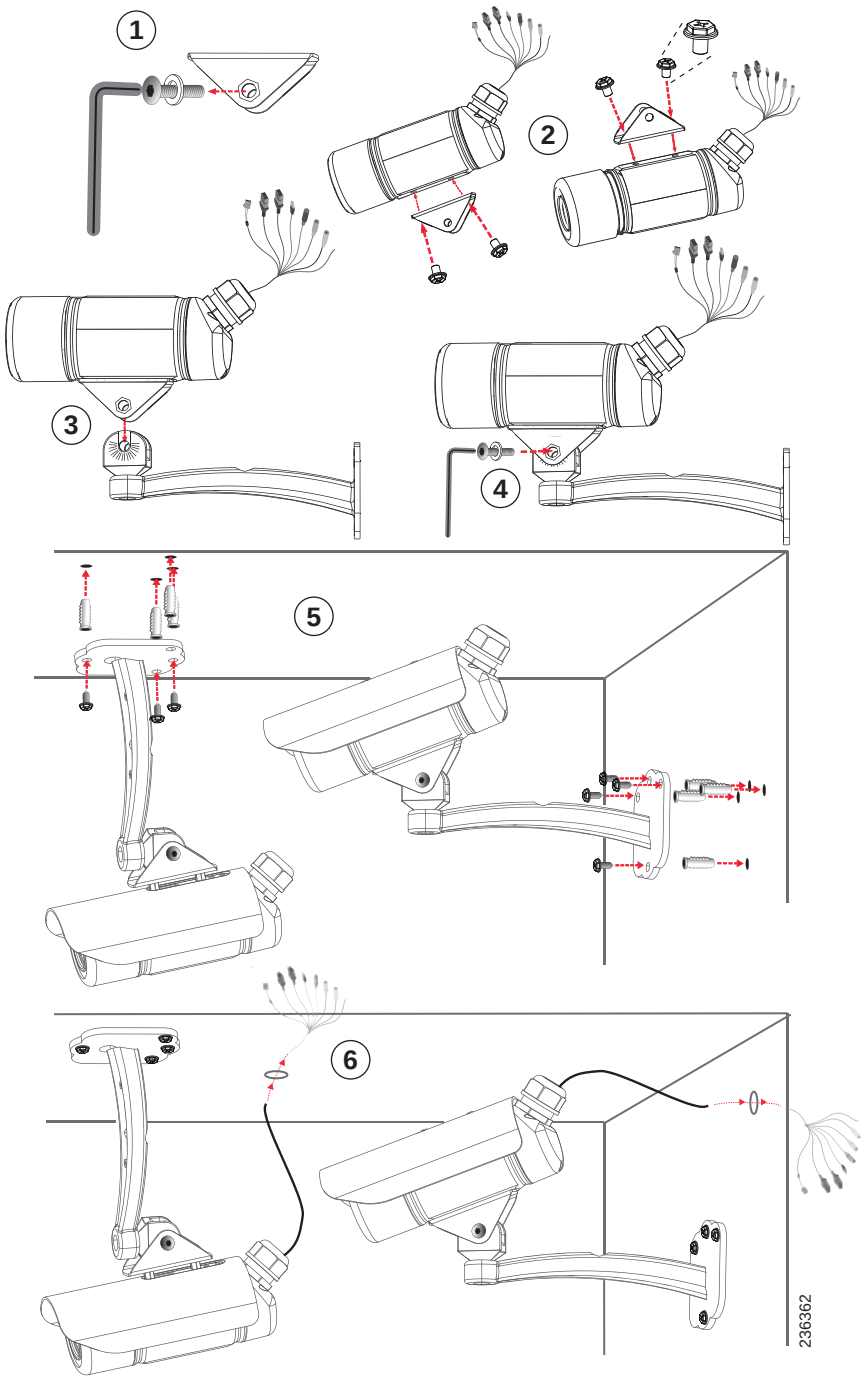
b. Using a 1/4-inch drill bit, drill four holes into the surface.

c. Insert the provided four wall-mounting screw anchors into the holes.

d. Attach the base of the camera stand to the wall or ceiling using the four self-tapping screws (#10 x 1.5 inch) and the corresponding M6 flat washers.

STEP 6 If you plan to connect the camera's cables from behind the wall or above the ceiling, drill a 1-inch diameter hole in the wall or ceiling and thread the cables through the hole.

In an outdoor installation, make sure that only the portion of the connector cables covered in black is exposed to the elements because it is weather proof. The individual cables should be behind the ceiling or wall.


1
2
3
4
5
6
236362

Connecting the Equipment

You can provide power to the camera over Ethernet using a PoE-enabled network switch or a PoE power injector. You can also use an external power adapter (not supplied).

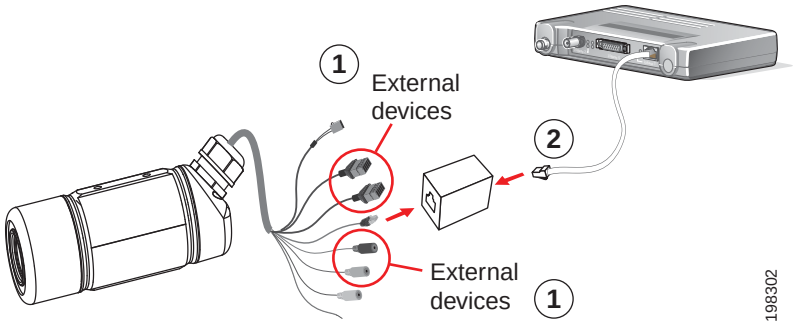
Connecting the Camera to a PoE-Enabled Switch

To connect your camera to a PoE-enabled switch, follow these steps.

STEP 1 Connect the camera's cables as needed to I/O port devices, an audio speaker, or a microphone.

STEP 2 Use the supplied RJ45 female-to-female Ethernet adapter to connect the camera to a PoE-enabled switch.

NOTE Use a Category 5 crossover cable to directly connect the camera to a computer.



Connecting the Camera to a PoE Power Injector

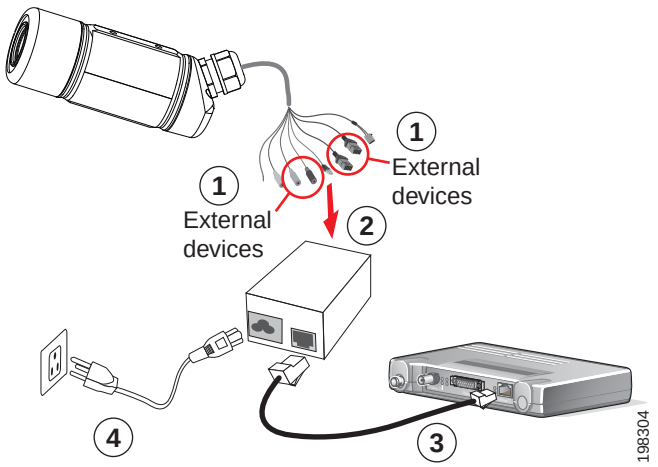
To connect the camera to a non-PoE-enabled switch using an 802.3af-compliant PoE power injector, follow these steps:

STEP 1 Connect the camera's cables as needed to I/O port devices, an audio speaker, or a microphone.

STEP 2 Use the supplied RJ45 female-to-female Ethernet adapter to connect the camera to a PoE power injector.

STEP 3 Connect the switch to the PoE power injector.

STEP 4 Connect the PoE power injector to a power outlet.



Connecting the Camera to an External Power Adapter

To connect the camera to an external power adapter (not supplied) through the camera's power cord socket, you'll need an adapter with the following specifications:

- 12-VDC (1 A) power adapter with an output barrel connector
- Diameter of the outer barrel is 5.5 mm
- Diameter of the inner barrel is 2.1 mm
- Length of the barrel connector is 9.5 mm

You can also connect the camera to power through the 5-port connector (24 VAC, 0.5 A).

To connect the camera to your network and provide power using an external power adapter (not supplied), follow these steps:

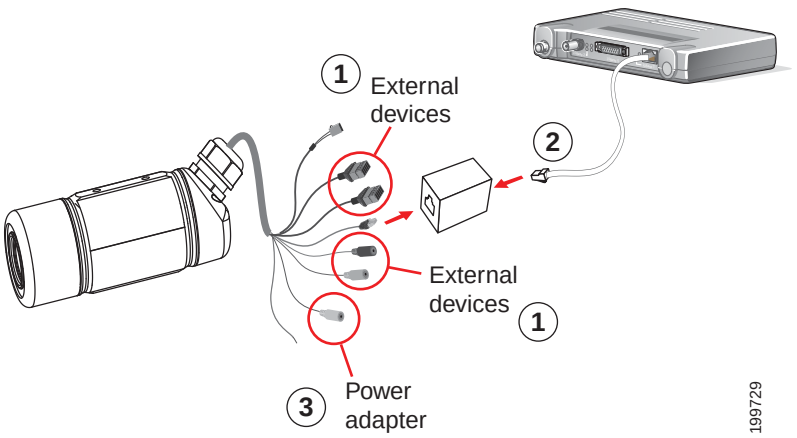
STEP 1 Connect the camera's cables as needed to I/O port devices, an audio speaker, or a microphone.

STEP 2 Use the supplied RJ45 female-to-female Ethernet adapter to connect the camera to a switch.

NOTE Use a Category 5 cross cable to directly connect the camera to a computer.

STEP 3 Connect the power supply to the camera's power cord socket (black connector).

Alternatively, you can use the 5-port connector to connect the camera to power.



Verifying the Hardware Installation

To verify the hardware installation, complete the following tasks:

- Check the cable connections.
- Verify that the Status LED is flashing red as described in the **Front Panel, page 12**.

NOTE If you need help resolving a problem, visit the Cisco Small Business Support Community at www.cisco.com/go/smallbizsupport.

Where to Go Next

To adjust the camera's zoom and focus settings, you have to wait until you can view live video from the camera. After mounting the camera and connecting the equipment as described in this section, follow the steps in the **Installing the Cisco VC240 Network Camera Software, page 29** After you are able to get live feed from the camera, follow the instructions in the **Adjusting the Lens, page 97** to adjust the zoom and focus settings.

4

Installing the Cisco VC240 Network Camera Software

Before You Begin

There are two ways of installing your Cisco VC240 camera. You can use the Cisco Video Monitoring System, or you can use the Cisco VC240 product CD. The product CD includes a Setup Wizard software program. Before using either method of installation, consider the following recommendations.

General Recommendations

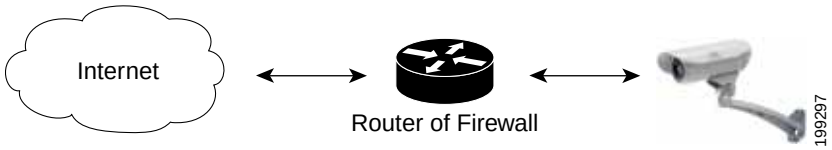
- Read through this guide and other supporting materials to familiarize yourself with the camera before continuing.
- Internet Explorer may prompt you to accept ActiveX to view video; follow the instructions to accept ActiveX.
- Make sure that you have a computer that meets the following requirements:
  - Windows XP, Windows Vista, or Windows 7.
  - Internet Explorer (6x or later)

  NOTE You get limited functionality if you use Firefox or Safari. And to view MPEG-4 video, install the QuickTime plug-in.

Security Recommendations

- The default username and password is **cisco**. For security purposes, it is highly recommended that you change the default name and password using the camera's web-based configuration utility at a later time.
- Use the IP filtering feature to control which IP addresses can access your cameras. See **Network Setting > IP Filter, page 53** for more information.

- To secure your camera from possible intrusion, it should be located behind a router or appropriate firewall in your LAN.



IP Configuration Recommendations

- Use the Setup Wizard to install your cameras. The Setup Wizard is found on the CD that shipped with your camera. Designed to make set up easy, the Setup Wizard eliminates the need to configure IP addresses yourself. You can use the Setup Wizard whether you are installing one or multiple cameras.
- A MAC address is an important unique identifier that is assigned to each camera. The Setup Wizard lists the IP addresses and MAC addresses of all the cameras discovered. If you have more than one camera, make a note of the MAC address found on the side of the camera. Knowing the MAC address makes it easier to identify multiple cameras. Your MAC address will be something like the following: 00:21:29:72:7D:2C.
- DHCP is the default IP addressing option. The camera is automatically assigned an IP address from a DHCP server or a DHCP router. If no DHCP server is present in the network, after 90 seconds the camera defaults to a static IP address of 192.168.1.99.
- If the camera is connected directly to your computer, then your computer needs to be on the same subnet as the camera's default static IP address so you can access the configuration utility. For example, your computer needs to have an IP address of 192.168.1.2 to 192.168.1.254, with the exception of the camera's IP address of 192.168.1.99. The computer's subnet mask will be 255.255.255.0.

Installing the Camera

You can install your Cisco VC240 camera in three different ways. You can use the Cisco Video Monitoring System, Cisco FindIT, or you can use the Cisco VC240 Setup Wizard.

- **Installing the Camera Using the Cisco Video Monitoring System, page 31**
- **Installing the Camera Using Cisco FindIT, page 31**
- **Installing the Camera Using the Setup Wizard, page 32**

Installing the Camera Using the Cisco Video Monitoring System

If you have multiple cameras, you can use the included Video Monitoring System software to discover, monitor, and manage the cameras. For instructions on using the video monitoring software, see the SW VMS16, VM 200, and VM 300 Video Monitoring System Administration Guide found at www.cisco.com/go/avms-cams.

After discovering your cameras, you can use the camera's web-based configuration utility to view video or configure the cameras. See **Launching the Web-Based Configuration Utility, page 33**.

Installing the Camera Using Cisco FindIT

The Cisco VC240 works with Cisco Small Business network tools and services including the Cisco FindIT Network Discovery Utility. Cisco FindIT enables you to automatically discover all supported Cisco Small Business devices in the same local network segment as your computer. You can get a snapshot view of each device or launch the product configuration utility to view and configure the settings. For more information, see www.cisco.com/go/findit.

After discovering your cameras, you can use the camera's web-based configuration utility to view video or configure the cameras. See **Launching the Web-Based Configuration Utility, page 33**.

Installing the Camera Using the Setup Wizard

You can use the Setup Wizard found on the Cisco VC240 product CD to install one or more cameras. The following instructions will help you install the Cisco VC240 software using the Setup Wizard.

STEP 1 Insert the Setup CD into your CD-ROM drive.

STEP 2 Launch the Setup Wizard in one of two ways:

1. You can launch the Setup Wizard from the CD without installing the software on the computer. This option is useful if you do not want to install anything on your computer.
2. You can install the software on your computer. This option is useful if you will install more cameras in the future, and don't want to search for the CD. The Setup Wizard is stored in **Start** > **Cisco Small Business** > **VC240** > **Setup Wizard**.

STEP 3 Run the Setup Wizard according to the online instructions.

- The Setup Wizard prompts you to accept the License Agreement and enter the default username and password of the camera, which is **cisco**/**cisco**. You will also be given the opportunity to name your camera and give it a unique description.
- The Setup Wizard searches your network for your cameras automatically. If the Setup Wizard does not find your Cisco VC240 camera, enable UPnP on your computer. See instructions for enabling Universal Plug and Play (UPnP) in **Questions and Answers, page 113**.
- When the Setup Wizard prompts you for a response to configure Network Settings, for most standard installations choose **Obtain an IP Address Automatically (DHCP)**.

STEP 4 When complete, the last page of the Setup Wizard allows for multiple options. You can install more cameras, install the video monitoring software, or launch the camera web-based configuration utility to view video or configure the camera. See **Launching the Web-Based Configuration Utility, page 33**.

Launching the Web-Based Configuration Utility

By default, the Cisco VC240 network camera is set to receive an IP address from a DHCP server. If there is no DHCP server present in the network, after 90 seconds, the camera defaults to a static IP address of 192.168.1.99. Make sure that your computer is in the same subnet (192.168.1.x) to access the default camera static IP address.

Instructions for determining your camera's DHCP address can be found in **Questions and Answers, page 113**. If you do not have a DHCP server, access your camera through the default static IP address.

To launch the Cisco VC240 camera, follow these steps to access the web-based configuration utility from your computer:

STEP 1 Launch Internet Explorer (6.x or later).

STEP 2 In the Address field, enter the IP address of the camera.

- By default, the Cisco VC240 camera obtains an IP address from a DHCP server. Instructions for determining your camera's DHCP address can be found in **Questions and Answers, page 113**.
- Enter the default static IP address (192.168.1.99) if there is no DHCP server present.
- If you used the Setup Wizard to configure the IP address, use that same IP address in this step.

The web-based configuration utility login page appears.

STEP 3 If this is your first time to access the web-based configuration utility, follow these steps at the login page:

a. Enter **cisco** in the Username field.

b. Enter **cisco** in the Password field.

c. Click **OK**.

For security purposes, it is recommended that you reset your password. See the **Administration > Users, page 84** page. See also **Administration > Password Strength, page 87** for information on minimum password security settings that are enabled on the camera by default.

NOTE If it is not your first time to access the web-based configuration utility, or if you changed the password using the Setup Wizard, remember to use the username and password that you set.

Where to Go Next

- **Using the Web-Based Configuration Utility, page 35** for information about the features found in the configuration utility and the View Video page.
- **Configuring the Cisco VC240 Network Camera Software, page 43** for complete descriptions of the camera's configuration utility.
- **Finalizing the Cisco VC240 Hardware Setup, page 97** for instructions on adjusting the lens and attaching the sun shield.

5

Using the Web-Based Configuration Utility

This section provides an overview of the Cisco VC240 network camera's web-based configuration utility software.

This chapter contains the following sections:

Microsoft Internet Explorer (IE) 6.x or later is the official supported browser for the Cisco VC240 network camera. Other browsers provide limited functionality.

Session and Camera Settings

By default, the inactivity time-out for the camera's web-based configuration utility is 600 seconds (10 minutes). It is recommended that you log out of your session when complete so that you are able to log back in as needed. If you accidently close the browser without logging out, open the same browser. The session should still be active.

View Video

The View Video page is the default display. From this page, live video can be viewed and the output can be updated. This page identifies the camera in the upper left hand corner. You can always return to the View Video page by clicking the **View Video** icon in the toolbar.

This section describes the options available to you on the View Video page.

NOTE Internet Explorer may prompt you to accept ActiveX to view video; follow the instructions to accept ActiveX.

Header

- **Connected User**—Displays the number of concurrent connections including the current view.
- **Language**—Click this button to choose a language for the displayed interface. The supported languages are: English, German, Spanish, French, Italian, Japanese, Portuguese, Simplified Chinese, and Traditional Chinese.
- **Logout**—Logout of this session.
- **About**—Displays information about the device including the device model name, description, and firmware version.
- **Help**—Provides online help information about the camera's features.

Toolbar

- **View Video**—Click from any location to view live video.
- **Client Settings**—Click to access the Client Settings page. See **Client Settings, page 39** for more information.
- **Setup**—Click to access the Cisco VC240 network camera web-based configuration utility page. See **Configuring the Cisco VC240 Network Camera Software, page 43** for full information.

Camera Control Panel

- **Output**—Toggles the I/O ports On and Off.
- **Day/Night**—Switches from day to night mode.

If RS-485 is enabled:

- **Preset Camera View**—Select a Preset Location list. To add preset positions to the preset locations list, see Preset Positions under **Camera Control > RS-485, page 68**.
- **Pan**—Start auto pan. The pattern of movement depends on the RS-485 device.
- **Patrol**—Moves the camera between the preset positions on the Patrol List. After one patrol cycle, the camera returns to the original position.
- **Stop**—Stops the auto pan and auto patrol functions.
- **Pan/Tilt control buttons**—The control buttons move the camera left, right, up, down, and home. The Home button centers the camera.
- **Zoom**—Zoom works with PTZ devices that have zoom capabilities. If your PTZ device does not have zoom capabilities, the zoom feature built into the Cisco VC240 camera can not work.

Video Options Icons

The video options icons are found above the live video of the connected camera and allow you to control the camera and the live video feed.

NOTE All functions are available only in Internet Explorer 6.x or later. Other browsers provide limited functionality.

Icon	Description
Snapshot 	Click to take a single JPEG picture snapshot of the video image and right-click to save it to a desired location on your computer.
Zoom 	Provides 4x digital zoom. Click **zoom** and then use your mouse to select the section you want to magnify. Click the icon again to disable the zoom feature.
Play 	Allows the live video feed to play.

Icon	Description
Pause 	Pauses the live video feed.
Stop 	Stops the live video feed.
Record 	Records the live video feed. The default location is `C:\Record`. Configure the recording path in the Client Settings page. See **Client Settings, page 39** for more information.
Enable/Disable Mute 	In **Listen Only** mode, your computer speakers are enabled and your camera's microphone is enabled. When you enable **Listen Only** in the Camera Control > Audio page, the icon is displayed on the View Video page and audio is picked up through the camera. You can then click the icon to turn audio on and off.
Start /Stop Talk 	In **Talk Only** mode, the camera's external speakers are enabled. When you enable **Talk Only** in the Camera Control > Audio page, an icon is displayed on the View Video page and audio from your computer is played through your camera's speakers. You can then click the icon to turn on or turn off the camera's external speakers.
Two-Way Audio  	In **Two-Way Audio** mode, both the **Listen Only** and **Talk Only** icons appear on the View Video page. You can use the talk and listen modes simultaneously. **NOTE** If none of the audio icons are displayed on the View Video page, audio is disabled.

Client Settings

Click **Client Settings** in the toolbar to set how you want to see video on the local client. Most settings apply to the MPEG-4 stream. Set up MJPEG for the stream in **Camera Control > Video Settings, page 61**.

Follow these steps to configure the Cisco VC240 network camera streaming options:

STEP 1 Select **Stream 1** (default) or **Stream 2** as the streaming source.

STEP 2 Select one of the following options to configure the MPEG-4 media options. These options only work when the video mode is set to MPEG-4.

- **Video and Audio**—Default. Streams audio and video.
- **Video Only**—Streams only video.
- **Audio Only**—Streams only audio.

STEP 3 Select one of the following options to configure the MPEG-4 protocol options (the options available to you depend on your network environment):

- **UDP Unicast**—Allows for more real-time audio and video streams. However, network packets may be lost due to network burst traffic and images may be obscured. Activate this UDP connection when occasions require time-sensitive responses and the video quality is less important. Note that ten simultaneous client accesses are allowed; however, each unicast client connecting to the server takes up additional bandwidth.
- **UDP Multicast**—Allows multicast-enabled routers to forward network packets to all clients requesting streaming media. This helps reduce the network transmission load of the Cisco VC240 network camera while serving multiple clients at the same time.

  NOTE To use this feature, you must configure the Cisco VC240 network camera to enable multicast streaming. See **Network Setting > Multicast, page 51** for more information.
- **TCP**—This is the default. Guarantees the complete delivery of streaming data and thus provides better video quality. Due to the narrower bandwidth, you may notice a delay in the real-time video when you choose TCP instead of UDP.
- **HTTP**—Provides the same quality as the TCP protocol. In some network environments, you do not need to open a specific port for streaming when

you choose HTTP. If you are inside a firewall, use this protocol to allow the streaming data to come through.

STEP 4 Configure the MPEG-4 saving options:

- **Folder**—Specify where to store the recorded video files. `c:\Record` is the default path.
- **File Name Prefix**—Specify the text that precedes the video file name. `CLIP` is the default.
- **Add date and time suffix to the file name**—Check this to add the date and time to the file name suffix. The format is YYYYMMDD_HHMMSS.

  For example, in the following filename:

  `CLIP_200801008_180853`

  The filename prefix is `CLIP_` and the date and time suffix is `200801008_180853`.

STEP 5 Click **Save** to save your settings.

Getting Started

Click **Setup** in the toolbar to access the Getting Started page. The Getting Started page provides you quick links to some of the most used features.

Initial Setup

- **Change Default Admin Password and Add Users**—It is recommended that you change the password of the camera after you first set up the camera. See **Administration > Users, page 84** for instructions on changing your password. See also **Administration > Password Strength, page 87** for information on minimum password security settings.
- **Configure Device IP Settings—**See **Network Setting > IP Setting, page 45** for instructions on changing your IP settings.
- **Change Streaming Video Settings—**See **Camera Control > Video Settings, page 61** for instructions on changing your video streaming and image settings.

Video Monitoring System

- Provides a link to the www.cisco.com/go/avms website. The Cisco Video Monitoring System offers video monitoring of up to 16 cameras. This is a free product with the Cisco VC240 camera.
- The Advanced Video Monitoring System supports up to 64 cameras and provides video analytics, business applications, and instant alerts. This is an optional product.

Quick Access

- **Upgrade Device Firmware**—The Cisco VC240 camera may not always ship with the most up-to-date firmware. It is recommended that you upgrade the firmware after you first set up the camera. See **Administration > Firmware, page 91** for complete information.
- **Backup Device Configuration—**See **Administration > Configuration File, page 92** for backup information.
- **Create Motion Detection—**See **Applications > Motion Detection, page 77** for instructions on setting motion detection.

More Ways To Use Your Camera

Provides a link to the Cisco Small Business Video Surveillance Cameras web page. This webpage provides an all-encompassing view of Cisco video surveillance equipment, features, and solutions.

Other Resources

Support and Forums—Provides a link to the Small Business Support Community webpages.

Don’t show this on setup

Clicking **Setup** accesses the Getting Started page. When you check **Don’t show this on setup**, the default landing page when you click **Setup** becomes the System Summary page.

The Cisco VC240 camera landing page remains the View Video page.

Where to Go Next

For complete descriptions of the camera's configuration utility, start here:

- **Configuring the Cisco VC240 Network Camera Software, page 43**

For instructions on adjusting the lens and attaching the sun shield:

- **Finalizing the Cisco VC240 Hardware Setup, page 97**

6

Configuring the Cisco VC240 Network Camera Software

This section describes the functions of the camera's configuration utility. For information on how to use your camera for advanced monitoring, see the **Cisco Small Business Video Monitoring System Administration Guide**.

Microsoft Internet Explorer (IE) 6.x or later is the official supported browser for the Cisco VC240 network camera. Other browsers provide limited functionality.

NOTE The inactivity time-out for the camera's configuration utility is 10 minutes.

This chapter contains the following sections:

Network Setting > IP Setting

Use the Network Setting > IP Setting page to set the IP address and other related settings. When you complete the configuration, click **Save** to save the settings; otherwise click **Cancel** to discard the changes.

- **Camera Name**—Enter the preferred name of the camera. The camera name can contain alphanumeric characters (A-Z, a-z, 0-9, or -). By default, the camera name is camera plus the last six digits of the MAC address; for example camera727e1e.
- **Description**—Enter a description of your camera, such as the location of the camera. Entering a description can help you identify the camera when you have multiple cameras. The description must not exceed 32 alphanumeric characters. The description is displayed in the installation Setup Wizard and on UPnP AV clients.
- **Disable LED Operators**—Select to disable the Status LED. You may choose to do this if you don't want to alert others that the network camera is on.

Choose **LAN** or **PPPoE**, and then enter the settings described below.

- **LAN**—If **LAN** is enabled, enter the following information:
- **Configuration Type**—Choose either **Obtain Address Automatically (DHCP)** or **Fixed IP Address**.
  - **DHCP**—This is the default. Select this option when your network uses a DHCP server. When the camera starts up, all IP settings, including address, are automatically assigned by the DHCP server. You do not have to input an IP, Subnet, Gateway, or DNS address. See **Questions and Answers, page 113** for information on how to find your camera's IP address.
  - **Fixed IP Address**—Select this option to assign a static IP address to the camera. The default static IP address is 192.168.1.99 if you are using a Cisco Small Business router. If you are not using a Cisco Small Business router, your camera may be assigned a different default IP address. The IP address would be an IP address under your router's IP addressing scheme, such as 192.168.2.x or 192.168.0.x. See **Questions and Answers, page 113** for information on how to find your camera's IP address.
  - **IP Address**—If setting a static IP address, enter the IP address of the camera.

- **Subnet Mask**—If setting a static IP address, enter the subnet mask of the camera.
- **Gateway**—If setting a static IP address, enter the default gateway of the camera.
- **Primary DNS / Secondary DNS**—Domain Name System (DNS) translates domain names into IP addresses. Enter the Primary DNS and Secondary DNS addresses that are provided by your Internet Service Provider (ISP).
- **Primary WINS / Secondary WINS**—Enter the Primary Windows Internet Name Service (WINS) and Secondary WINS addresses if known, but these are not mandatory.

• **PPPoE**—Select the **PPPoE** option when you use a direct connection through an ADSL modem. You should have a PPPoE account from your ISP.

If **PPPoE** is enabled, enter the ISP Provider, and your **UserName** and **Password** as provided by your ISP. The camera will get an IP address from the ISP at start up.

After the camera gets an IP address from the ISP, it automatically sends a notification email to you. Therefore, when you select PPPoE as your connecting type, you have to set up the email or DDNS configuration in advance. See **Network Setting > DDNS, page 55** or **Applications > Servers, page 72**.

NOTE The Cisco VC240 IP camera only supports the PAP authentication method of PPPoE.

• **Enable IPv6**—Enable Internet Protocol version 6 (IPv6) if you are required to use an IPv6 address instead of an IPv4 address. An IPv6 address is a longer IP address (up to 128-bits) and allows you to have more Internet users. Dual stack routers allow for both IPv6 and IPv4 address formats.

When you enable **IPv6**, DHCP information is automatically received from your router and there is no need to enter information into the rest of the IPv6 fields. However, if you prefer, you can manually provision your IPv6 address using the following fields:

- **Optional IP Address**—Enter the IPv6 address.
- **Prefix Length**—The default prefix length is 64.
- **Optional Default Router**—Enter the IPv6 default gateway of the camera.

- **Optional Primary DNS**—Enter the IPv6 Primary DNS address as provided by your ISP.

- Click the **IPv6 Info** button to display the current configuration for IPv6.

Network Setting > TCP/UDP Port Settings

Use the Network Setting > TCP/UDP Port Settings page to set HTTP, FTP, HTTPS, Audio, and Real-time Transport Protocol (RTP)/ Real-time Streaming Protocol (RTSP) ports and related settings. When you complete the configuration, click **Save** to save the settings; otherwise click **Cancel** to discard the changes.

- **Authentication**—Depending on your network security requirements, the Cisco VC240 network camera provides two types of security settings for a HTTP transaction: **basic** and **digest**. If **basic** authentication is selected, the password is sent in plain text format. Basic is often required for interoperability with other products; for example, the Cisco Video Monitoring System. Note that password interception is a potential risk when using basic authentication.

  If **digest** authentication is selected, user credentials are encrypted using the MD5 algorithm and this method provides better protection against unauthorized access.

- **HTTP Port/Secondary HTTP Port**—Assigns the HTTP port for communication. The default HTTP port is 80 and the default secondary HTTP port is 8080. If you'd prefer to assign a different port number, the port should be within the range of 1024 and 65535.

  To access the camera within a LAN, both the HTTP port and secondary HTTP port can be used to access the camera. For example, if the HTTP port is set to 80 and the secondary HTTP port is set to 8080, the camera's IP address in a LAN could be:

  ```
  http://192.168.4.160 or
  http://192.168.4.160:8080
  ```

- **Access Name for Stream 1/Stream 2**—Differentiates the streaming source by name. The default is video.mjpg and video2mjpg, respectively. This can also be useful for viewing on one stream and recording on another.

- **FTP Port**—Enter the port number used for the FTP server. The default port is 21.

- **HTTPS Port**—Assign an HTTPS port in the text box. The default HTTPS port is 443.

- **Two-Way Audio Port**—Enter the port number used for audio. The default port is 5060.

- **Authentication**—Used for RTP/RTSP. Select from three authentication options: Disabled, Basic, and Digest.
  - **Disabled**—Allows an RTP/RTSP session without a username or password.
  - **Basic**—Allows the username and password to be sent over the network in clear text.
  - **Digest**—An agreed-upon method that a web page can use to negotiate credentials with a web user using the HTTP protocol. The Digest authentication method is an application of MD5 cryptography.
- **Access Name for Stream 1**—Specifies the access name for Stream 1. This name is the access URL for accessing the camera from client software (for example, QuickTime Player) when the codec type is MPEG-4.
- **Access Name for Stream 2**—Specifies the access name for Stream 2. This name is the access URL for accessing the camera from client software (for example, QuickTime Player) when the codec type is MPEG-4.

  NOTE Stream 1 and Stream 2 can use the same codec, but can use different resolutions, bitrates, or frame rates.
- **RTSP port**—Configure your router to forward traffic to this port on your computer. The default RTSP port is 554.
- **RTP port for video**—RTP is used to deliver video and audio data to the clients. By default, the RTP port for video is set to 5556 and the RTP port for audio is set to 5558. Change the port number if more than one camera is doing multicast and using the same default IP address.
- **RTCP port for video**—The Real-time Transport Control Protocol (RTCP) allows the Cisco VC240 network camera to transmit data by monitoring Internet traffic volume. By default, the RTCP port for video is set to 5557 and the RTCP port for audio is set to 5559. It must be the port number of video RTP, plus 1. Change the port number if more than one camera is doing multicast and using the same default IP address.
- **RTP port for audio**—The audio channel port for RTP. It must be an even number. Change the port number if more than one camera is doing multicast and using the same default IP address.
- **RTCP port for audio**—The audio channel port for RTCP. It must be the port number of audio RTP, plus 1. You can modify the multicast setting for Stream 1 and Stream 2. Change the port number if more than one camera is doing multicast and using the same default IP address.

NOTE You can reassign the five ports to any value between 1024 and 65535. The RTP port must be an even number and the RTCP port is the RTP port number plus one, and is always an odd number. When the RTP port changes, the RTCP port will change accordingly.

Network Setting > Multicast

Use Network Setting > Multicast to send a stream to a multicast group address. Multicast allows multiple clients to acquire the stream at the same time by requesting a copy from the multicast group address, saving Internet bandwidth. Multicast can be set per video stream. When you complete the multicast configuration, click **Save** to save the settings; otherwise click **Cancel** to discard the changes.

- **Always Multicast**—Select this option to enable the multicast function of the camera so that you can deliver information from your camera to a set of receivers.
- **Multicast Group Address**—The camera's video and audio IP address has been pre-configured and can be used for multicasting. This does not normally need to be re-configured. If an address does need to be changed, contact your network administrator. To change, enter the Video Address/ Audio Address in the field provided.
- **Multicast Video and Audio Ports**—The camera's video and audio ports have been pre-configured for multicasting. They do not normally need to be re-configured. If a port number does need to be changed, contact your network administrator. To change, enter the Video Port/Audio Port numbers (between 1024 to 65534) in the fields provided. The Video Port/Audio Port numbers you enter must be even values.

  If there are multiple cameras that use the same default group multicast IP address, modify the Video Port and Audio Ports to be a unique value.
- **Multicast TTL [1-255]**—Defines the number of hops (the number of network routers that can be passed before the multimedia data packets arrive at their destination or are dropped) that can occur before the packets are dropped. A value in the range of 1 to 255 can be defined. The default value is 15.

Network Setting > HTTPS

HTTPS refers to the combination of HTTP interaction over an encrypted Secure Socket Layer (SSL) or Transport Layer Security (TLS). HTTPS technology ensures end-to-end security and provides complete defense against eavesdropping, impersonation, and hijacking. When you complete the HTTPS configuration, click **Save** to save the settings; otherwise click **Cancel** to discard the changes.

Create and Install a Certificate

The first step is to create a self-signed certificate:

STEP 1 Click **Create** next to **Self-Signed certificate** and the Create Certificate window appears.

STEP 2 Fill in the required information and click **Save** to generate a self-signed certificate.

STEP 3 The certificate will be automatically installed upon generation, then you can enable the HTTPS service (check **Enable HTTPS secure connection**).

Certificate Information

Once a certificate is present, you can press the **Property** button to view the certificate details. After a certificate is installed or generated you cannot generate a new one. The old certificate must be removed before a new certificate can be generated. To remove the certificate, press the **Remove** button. The same rule applies to certificate request. You need to remove an old certificate request before generating a new one.

Network Setting > IP Filter

The Network Setting > IP Filter page controls the access permission of clients by checking the client's IP addresses. When you complete the configuration, click **Save** to save the settings; otherwise click **Cancel** to discard the changes.

Enable Filter

Check the **Enable IP address filtering** box to enable IP filtering. Uncheck the box to disable this feature.

There are two options for permission control in the drop-down list: **Allow** and **Deny**.

Only those clients whose IP address is in the Allowed List and not in the Denied List can connect to the Cisco VC240 network camera to receive the audio or video streaming. Both the Allowed List and Denied List can include a single IP address, a list of IP address ranges, or a network mask.

If you want to add a new IP address, click the **Add** button and type the IP address you want to allow or deny. There are three methods of filtering in the drop-down list: **Single**, **Range**, and **Network**.

If you want to add a new IP Address range, click the **Add** button and enter the Begin IP Address on the left text box and End IP Address in the right text box. If you want to add a new Network, click the **Add** button and enter the Network you want to **Allow** or **Deny**.

If you want to remove an existing IP Address, IP address range, or Network, make a selection from the menu and click on the **Delete** button. Both the Allowed List and Denied List can have up to 10 entries.

Administrator IP Address

The Administrator IP Address is a restrictive IP filter that only allows administrator privileges from a **Super Admin Address** that you enable. The Super Admin then has root access and can have one session active at a time. This feature provides additional security and prevents unauthorized access. Even if an IP address is in a **Deny** list, the Super Admin still has access to the camera.

NOTE If you forget the administrative IP address, the camera must be reset to gain access.

Enable super admin—Click to enable the super admin feature.

Super Admin Address—Enter the IP address that you would like an administrator to use to access to the camera.

Network Setting > DDNS

Dynamic Domain Name Service (DDNS) is a service that allows your Cisco VC240 network camera, especially when assigned with a dynamic IP address, to have a fixed host and domain name. When you complete the configuration, click **Save** to save the settings; otherwise click **Cancel** to discard the changes.

NOTE Sign up for DDNS service with the service provider before completing this procedure.

- **Enable DDNS**—Check the box to enable the Dynamic DNS feature, which allows you to assign a fixed host and domain name to a dynamic Internet IP address.
- **Service Provider**—Select a DDNS provider of your choice from the list.
  - **Dyndns.org(Dynamic) / Dyndns.org(Custom)**—http://www.dyndns.com/
  - **TZO.com**
  - **3322.org**
- **Host Name**—Enter the name registered with the DDNS server.
- **Account**—Enter either the Username or Email to log into the DDNS server. When you input a Username, you must input a Password in the next field.
- **Password**—Input the password or key to get the DDNS service.

After you complete the fields of Host Name, Account and Password, you can press **Test** to test your configuration. The camera attempts to connect with the DDNS server to verify the account information was entered correctly. If the test was not successful, verify the information provided in the DDNS fields.

Network Setting > QoS

QoS, or Quality of Service, ensures that camera video packets are prioritized in a network. QoS in the network optimizes network performance by classifying traffic types and assigning network resources based on the traffic classes. The Cisco VC240 camera offers two QoS modes: 802.1p CoS and DSCP.

NOTE Cisco Small Business Smart and Managed Switches offer configurations that match all the necessary QoS priority values and queue mapping required for the Cisco VC240 camera.

When you complete the configuration, click **Save** to save the settings; otherwise click **Cancel** to discard the changes.

CoS

- **Enable CoS**—Class of Service (CoS) specifies data packet priority based on the 802.1p QoS value in the VLAN priority tag of the packet. This feature is disabled by default. To enable CoS mode, check the box.
- **VLAN ID**—Enter the VLAN ID (1 to 4095) in the field provided.
- **Priority**—Set priority to a value between 0 and 7. The highest priority value is 7. The default CoS Priority value is 4 (video), which matches the Cisco Small Business Smart and Managed Switch QoS settings.

DSCP

- **Enable DiffServ**— Differentiated Services (DiffServ) is based on packet marking and queuing disciplines. The marking is done by adding a field to the IP header, called the DSCP (Differentiated Services Codepoint). This is a 6-bit field that provides 64 different class IDs.
- **DSCP Priority Value**—Describes a particular service level in terms of bandwidth, queueing theory, and dropping (discarding the packet) decisions. Network packets are classified according to their DSCP value and are given a particular forwarding treatment; for example, the bandwidth required to reserve for the packet. The range is from 0 to 63. The default is 34.

Network Setting > SNMP

Use Network Setting > Simple Network Management Protocol (SNMP) for network monitoring and control. The Cisco VC240 supports SNMPv3, including traps. When you complete the configuration, click **Save** to save the settings; otherwise click **Cancel** to discard the changes.

- **Enable SNMPv3**—Select this option to enable SNMP.
- **Read/Write Security Name**—Enter the Read/Write community name according to your network management system. The default is Private.
- **Authentication type**—Select MD5 or SHA as the authentication protocol method. The default is MD5.
- **Authentication Password**—Enter a password for authentication (at least 8 characters).
- **Encryption Password**—Enter a password for privacy and encryption (at least 8 characters). Both the authentication and encryption passwords are required by SNMPv3.
- **Read only Security Name**—Enter the Read only community name according to your network management system. The default is Public.
- **Authentication type**—Select MD5 or SHA as the authentication protocol method. The default is MD5.
- **Authentication Password**—Enter a password for authentication (at least 8 characters).
- **Encryption Password**—Enter a password for privacy and encryption (at least 8 characters). Both the authentication and encryption passwords are required by SNMPv3.
- **Trap Receiver IP Address**—The IP address of the network management system.

Network Setting > 802.1X

802.1X is an IEEE standard for media-level access control, offering the capability to permit or deny network connectivity, control VLAN access, and apply traffic policy based on user or machine identity. When you complete the configuration, click **Save** to save the settings; otherwise click **Cancel** to discard the changes.

IEEE802.1X

Enable this function if your network environment uses IEEE 802.1x, which is a port-based network access control. 802.1X uses Extensible Authentication Protocol (EAP) so multiple different authentication schemes may be added including smart cards, Kerberos, public key, one-time passwords, and others.

A summary of the most used EAP authentication mechanism are listed below. A full list of registered EAP authentication types is available at IANA: http://www.iana.org/assignments/eap-numbers.

CAUTION Not all authentication mechanisms are considered secure.

EAP-MD5

MD5-Challenge requires a username and password, and is equivalent to the PPP CHAP protocol, RFC1994. This method does not provide dictionary attack resistance, mutual authentication, or key derivation, and has therefore little use in a wireless authentication environment.

EAP-TLS

Creates a TLS session within EAP, between the Supplicant and the Authentication Server. Both the server and the client(s) need a valid (x509) certificate, and therefore a PKI. This method provides dual authentication. EAP-TLS is described in RFC2716.

EAP-TTLS

Sets up an encrypted TLS tunnel to safely transport authentication data. Within the TLS tunnel, other authentication methods may be used. Developed by Funk Software and Meetinghouse, and is currently an IETF draft.

Protected EAP (EAP-PEAP)

Like EAP-TTLS uses an encrypted TLS-tunnel. Supplicant certificates for both EAP-TTLS and EAP-PEAP are optional, but Authentication Server (AS) certificates are required. Developed by Microsoft, Cisco, and RSA Security, it is currently an IETF draft.

The following table provides a summary of the authentication methods:

	EAP-MD5	EAP-TLS	EAP-TTLS	EAP-PEAP
Server Authentication	None	Public Key (Certificate)	Public Key (Certificate)	Public Key (Certificate)
Supplicant Authentication	Password Hash	Public Key (Certificate or Smart Card)	MSCHAP, MS-CHAP(v2)	MSCHAP, MS-CHAP(v2)
Authentication Attributes	One-Way Authentication	Mutual Authentication	Mutual Authentication	Mutual Authentication
Dynamic Key Delivery	No	Yes	Yes	Yes
Deployment Difficulty	Easy	Hard	Moderate	Moderate
Security Risks	Identity exposed, Dictionary attack, Man-in-the-Middle (MitM) attack	Identity exposed	MitM attack	MitM attack Identity hidden in Phase 2, but potential exposure in Phase 1

Network Setting > DHCP Auto Configuration

DHCP Auto Configuration supports mass camera deployments so that camera configuration files can be downloaded using DHCP option 66 and 67. To use DHCP Auto Configuration, you must select DHCP as your IP Setting, which allows the camera to retrieve configuration files from the DHCP server in the network. You cannot use this feature if you are using a static IP address.

When you complete the configuration, click **Save** to save the settings; otherwise click **Cancel** to discard the changes.

- **Enable Automatic Configuration Download From TFTP Server (Option 66/150 and 67)**—When enabled, the camera as a DHCP client tries to obtain the TFTP server and configuration file specified by the DHCP router in the network. If the DHCP router does not provide the TFTP server and configuration file location, the Cisco VC240 camera looks for the **Backup TFTP Server** and the **Backup Configuration File**.
- **Backup TFTP Server**—The camera attempts to retrieve the configuration file from a backup server if the TFTP server assigned by the DHCP server has failed.
- **Backup configuration file**—Specify the file name of configuration file on the backup TFTP server.

Camera Control > Video Settings

Use the Camera Control > Video Settings page to set video parameters. When you complete the video configuration, click **Save** to save the settings; otherwise click **Cancel** to discard the changes.

Video Quality Settings For Stream 1 and 2

You can set two streams for the Cisco VC240 network camera for different viewing devices. For example, set one stream of the Cisco VC240 network camera to a smaller frame size and a lower bit rate for viewing on mobile phones. Then set the other stream to a larger video size and a higher bit rate for viewing on web browsers.

NOTE The Apple QuickTime plug-in supports only HTTP and UDP media streams. If you have trouble viewing video using a Firefox browser with the QuickTime plug-in, set Stream 1 and Stream 2 to MJPEG.

- **Mode**—The Cisco VC240 network camera offers two choices of video compression standards for real-time viewing: MPEG-4 and MJPEG. If MPEG-4 is selected, it is streamed in RTP encapsulation over UDP. There are four dependent parameters provided in MPEG-4 mode for video performance adjustment.
- **Resolution**—The video resolutions are selectable at the following settings: 640x480, 320x240, and 176x144. A larger frame resolution takes up more bandwidth, so always balance your desired resolution against the capacity of your network.
- **Video quality**—A complex scene generally produces larger file size, meaning that higher bandwidth will be needed for data transmission. Therefore, if Constant Bit Rate is selected, the bandwidth usage is fixed at a selected level, resulting in varying video quality performances. The bit rates are selectable at the following rates: 40Kbps, 50Kbps, 64Kbps, 128Kbps, 256Kbps, 512Kbps, 768Kbps, 1Mbps, 1.5 Mbps, 2Mbps, 3Mbps, and 4Mbps.

  If **Fixed Quality** is selected, all frames are transmitted with the same quality and bandwidth usage is unpredictable. Select the video quality from the following choices: Medium, Standard, Good, Detailed, and Excellent.

If **MJPEG** is selected, the Cisco VC240 network camera continuously sends JPEG images to the clients, producing dynamic effects similar to movies. Every single JPEG image transmitted guarantees the same image quality, which in turn comes at the expense of variable bandwidth usage. And because the media contents are a combination of JPEG images, no audio data is transmitted to the clients.

- **Maximum frame rate**—Limits the refresh frame rate per second. Set the frame rate higher for a smoother video quality.

  If the power line frequency is set to 50 Hz, the frame rates are selectable at the following rates: 1 fps, 2 fps, 3 fps, 5 fps, 8 fps, 10 fps, 15 fps, 20 fps and 25 fps. If the power line frequency is set to 60 Hz, the frame rates are selectable at the following rates: 1 fps, 2 fps, 3 fps, 5 fps, 8 fps, 10 fps, 15 fps, 20 fps, 25 fps, and 30 fps.

- **Intra Frame Interval**—A lower Intra Frame Interval increases video quality, but increases bandwidth consumption. A higher Intra Frame Interval decreases video quality, but saves bandwidth. Always balance picture quality against your available network capacity.

Day/Night settings

- **Switch to B/W in night mode**—Enables the camera to automatically switch to black and white during night mode.
- **Disable IR LED**—Disables the IR LEDs in night mode.
- **IR cut filter**—Switches the camera to the IR cut filter when dark. Select one of the following modes from the menu:
  - **Auto mode**—The camera automatically removes the filter by judging the level of ambient light.
  - **Day mode**—In day mode, the camera switches on the IR cut filter to block infrared light from reaching the sensor so that colors are not distorted.
  - **Night mode**—In night mode, the camera switches off the IR cut filter so the sensor can accept infrared light, helping to improve low light sensitivity.
  - **Schedule mode**—The camera switches between day mode and night mode based on a specified schedule. Enter the start and end time for day mode. The time format is expressed in hh:mm in a 24-hour format (00:00 - 23:59).

- **Light sensor sensitivity**—Select Low, Normal, or High sensitivity for the light sensor.

Options

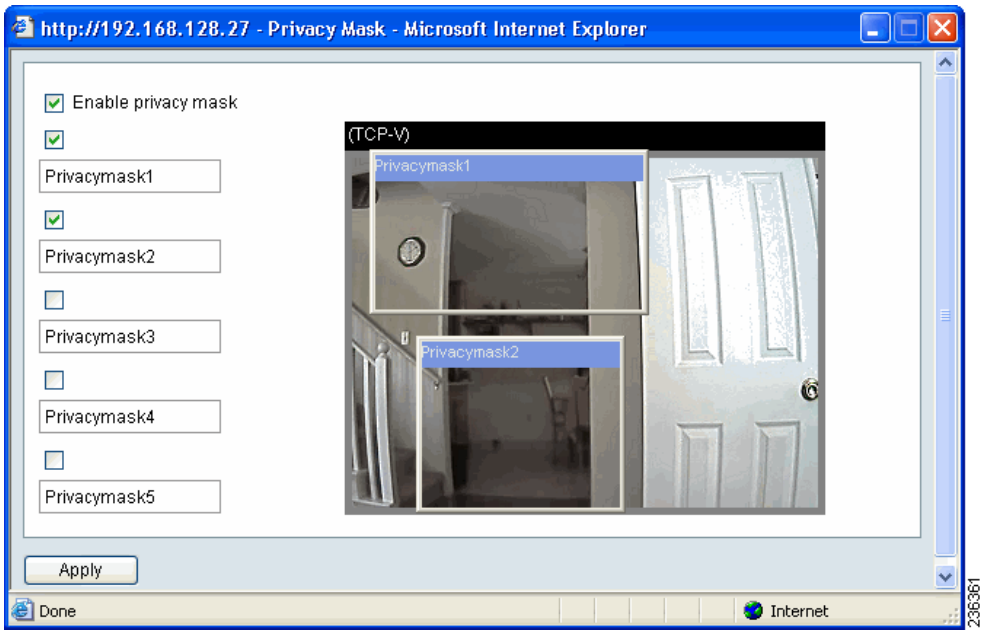
- **Video Adjustments**—Click **Adjust** to make adjustments to the Brightness, Saturation, White Balance, Sharpness, Hue, and Contrast.

  Click **Privacy Mask** to open a window that allows you to enable up to five privacy masks.

  Privacy masks allow you to block specified areas where you don't want to view or record activity. For example, you can create a privacy mask to block a public area where recording might be illegal, but still record the surrounding private area. Or you could use a privacy mask to block the view of a keyboard where individuals type private passwords.

  To create a privacy mask:

  Check **Enable privacy mask**, and check one of the Privacy Mask entries. A privacy mask appears in the preview window. Click the privacy mask and adjust the size and location of it in the preview window. Rename the privacy mask, if desired. Create up to five privacy masks, and then click **Apply**.



- **Sensor Adjustments**—Click to enable Wide Dynamic Range (WDR). WDR allows the camera to compensate for intense lighting in the background to distinguish subjects in the foreground and in the background. For example, when an indoor WDR camera points toward a window, the camera can see subjects both inside and outside the window.

  You can also adjust the Exposure Level and Maximum Gain.

- **Video Title**—Enter a name that will be displayed on the title bar of the live video.

- **Video Orientation—**Sets the orientation of the live video.

  - **Flip**—Vertically reflect the display of the video.

  - **Mirror**—Horizontally reflect the display of the video.

- **Color**— Select to display color or black/white video streams. The default is color.

- **Power Line Frequency**—To eliminate unwanted image flickering associated with fluorescent lights, set the power line frequency so it is consistent with local utility settings. Choices are 50 Hz and 60 Hz. A powerline frequency of 50 Hz allows a maximum of 25 fps, while a power line frequency of 60 Hz allows a maximum of 30 fps. The default is 60 Hz.

  NOTE: For the new power line frequency setting to take effect, disconnect and reconnect the camera.

- **Enable Time Stamp and Video Title**—Places the video title and time on video streams. Note that when the frame size is set to 176 x 144, only the time is stamped on video streams.

  If this feature is not selected, only one image is retained because all images are contained in one folder.

- **Date Format**—Sets the format for the date. Choices are MM/DD/YYYY, DD-MM-YYYY, and YYYY-MM-DD.

- **Time Format**—Sets the time format. Choices are 24 hour and 12 hour, which uses AM/PM.

Camera Control > Audio Settings

Use the Camera Control > Audio Settings page to configure audio settings. When you complete the configuration, click **Save** to save the settings; otherwise click **Cancel** to discard the changes.

Audio Settings

- **Disable Audio**—Select to mute audio transmission from the Cisco VC240 network camera to all clients. If this option is selected, no audio is transmitted to clients even if audio transmission is enabled in the Client Settings page.

  Audio is disabled by default to save bandwidth.

- **Audio Options**—Select **Listen Only**, **Talk Only**, or **Two-Way Audio**. **Two-Way Audio** is the default.

  - In **Listen Only** mode, your computer speakers are enabled and your camera's microphone is enabled. When you enable **Listen Only**, an icon is displayed on the View Video page and audio is picked up through the camera. You can then use the icon to turn audio on and off.

  - In **Talk Only** mode, the camera's external speakers are enabled. When you enable **Talk Only,** an icon is displayed on the View Video page and audio from your computer is played through your camera's speakers. You can then use the icon to turn the camera's external speakers on and off.

  - In **Two-Way Audio** mode, both the **Listen Only** and **Talk Only** icons appear on the View Video page. You can use the talk and listen modes simultaneously.

- **External Microphone Gain**—Select the gain of the external microphone input according to ambient conditions. Adjust the gain in 33 steps from +21 db (most sensitive) to -33 db (least sensitive). The default gain is 0.

- **Audio type**—Select an audio codec. Choices are AAC or GSM-AMR. The default is AAC.

- **AAC Bit Rate**—Select the bit rate for the AAC codec. This codec produces good sound quality at the cost of higher bandwidth consumption. The supported bit rates are: 16 Kbps, 32 Kbps, 48 Kbps, 64 Kbps, 96 Kbps, and 128 Kbps. The default bit rate is 128 Kbps.

- **GSM-ARM bit rate**—Select the bit rate for the GSM-ARM codec. This codec optimizes speech quality and requires less bandwidth. The supported bit rates are: 4.75 Kbps, 5.15 Kbps, 5.90 Kbps, 6.7 Kbps, 7.4 Kbps, 7.95 Kbps, 10.2 Kbps, and 12.2 Kbps. The default bit rate is 12.2 Kbps.

Camera Control > I/O Ports

Use the Camera Control > I/O ports page to set the input and output port functions. It is recommended that you connect your input and output devices before configuring them. When you complete the configuration, click **Save** to save the settings; otherwise click **Cancel** to discard the changes.

Input Ports

- **Triggered When**—Select **High** or **Low** to define the normal status of the digital input. The Cisco VC240 network camera shows whether the trigger is activated or not. The default is High.

Output ports State at Power On

- **Default State**—Select **Grounded** or **Open** to define the normal status of the digital output. The Cisco VC240 network camera shows whether the trigger is activated or not. The default is Grounded.

TIP For connection diagrams see **General Purpose Input/Output (GPIO), page 14**. For configuration steps, see **Configuring the GPIO Ports, page 109**.

Camera Control > RS-485

Use the Camera Control > RS-485 page to connect your VC240 camera to a PTZ driver or scanner using an RS-485 device. An RS-485 device allows you to use pan, tilt, and zoom when you operate the camera.

You can also connect your VC240 camera to another RS-485 device with an RS-485 port. This allows you to use the VC240 camera's web interface to control the movement of another RS-485 camera or base. This feature is dependent on the features of the other RS-485 device.

The Cisco VC240 camera works with **Samsung**, **DynaDome/SmartDOME** or **Pelco D** protocol devices or cameras. Due to the differences in protocol implementations, the Cisco VC240 camera works at different speeds and can use different features with each PTZ device. For example, while the Cisco VC240 has configurable pan, tilt, and zoom speeds, these features only work if your PTZ device has those capabilities. If your PTZ device does not have pan, tilt, or zoom capabilities, those features built into the Cisco VC240 camera cannot work.

RS-485 Settings

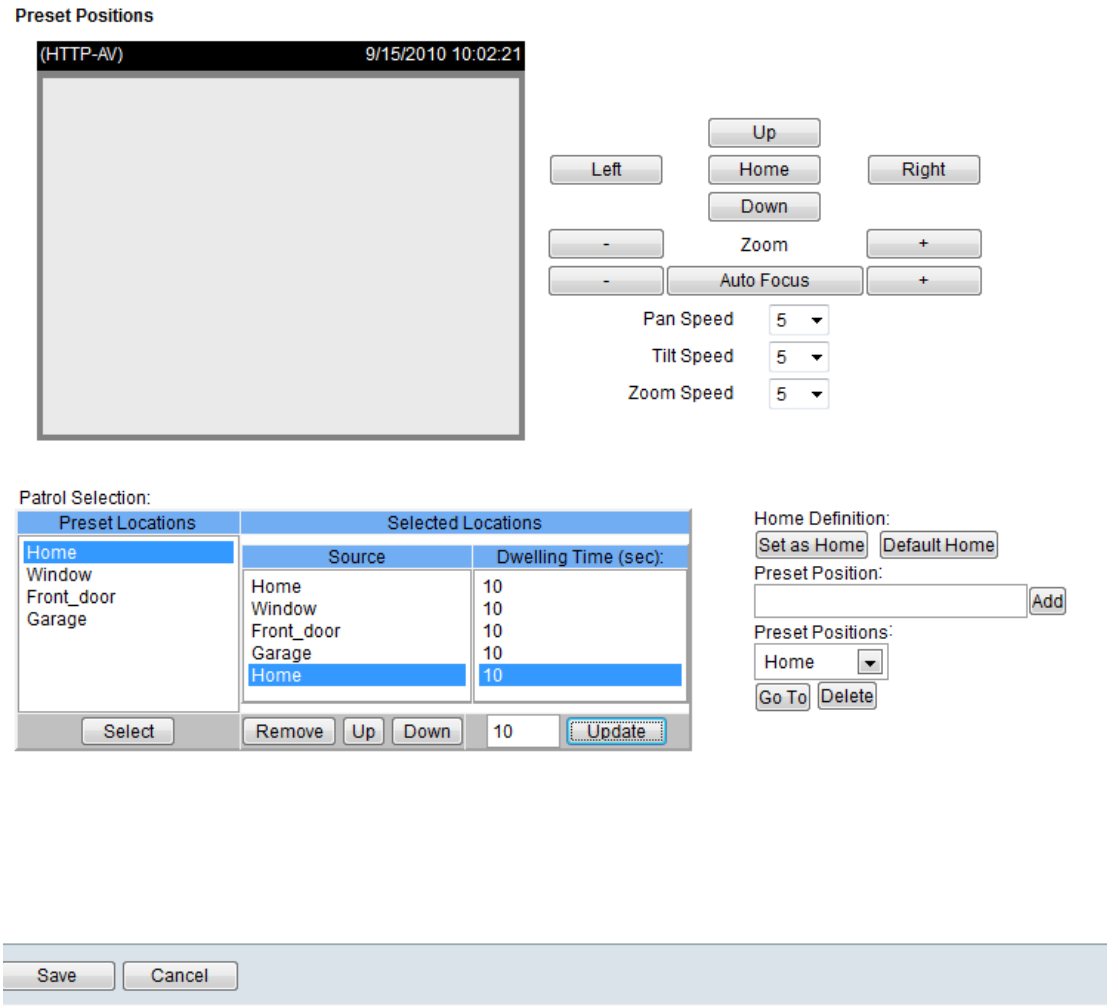
- **Disable**—Disables the RS-485 functionality. The default is Disable.
- **PTZ Camera**—Select this option to enable PTZ operation.
- **Camera ID**—Enter a Camera ID. The camera ID usually comes from the device you are connecting to. If you have multiple cameras, it is beneficial to have multiple camera IDs so each camera can be controlled individually.
- **PTZ Driver**—To use this feature, connect the camera to a **Samsung Scc643**, **DynaDome/SmartDOME,** or **Pelco D** protocol devices using the RS-485 interface. Other protocol devices may or may not work.

  NOTE Refer to the users manual of your PTZ device to determine how to set up the PTZ driver and what values should be set in the **Port Settings** field. The desired port settings vary depending on your device.

- **Port Settings**
  - **Baud Rate**—The number of symbols per second transferred. Choices are: 110, 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600, or 115200. The default is **9600**.
  - **Data Bits**—The number of bits to represent one character of data. Choices are 6, 7, or 8. The default is 8.
  - **Stop Bits**—Additional bits transmitted after the data bit. Choices are 1 or 2. The default is 1.
  - **Parity Bits**—Ensures that the number of bits in a set is even or odd. Choices are None, Odd, or Even. The default is None.
- **Preset Position—**Active after you click **Save**. Click **Preset Position** to open the settings page.

NOTE If you click **Save** and enable the PTZ camera function, the camera control panel is displayed on the Home page. See **Camera Control Panel, page 36**.

- **Preset Positions**



To preset a position:

Use **Up**, **Down**, **Left**, and **Right** to adjust the aim of the camera. **Pan speed** determines the speed that the camera moves to the left and right. **Tilt speed** determines the speed that the camera moves up and down. **Zoom speed** determines the speed that the camera adjusts the zoom. Pan, tilt, and zoom speeds are selectable in the range of 1 to 10 seconds.

To set a Home position:

Use **Up**, **Down**, **Left**, and **Right** to adjust the aim of the camera. Click **Set as Home** to set the Home position. To set the scanner boot-up position, click **Default Home.**

Preset Position Settings:

Enter a name for the preset position in the **Preset Position** box. Each preset position name can be up to forty characters in length. Click **Add**. The preset position is added and listed under the **Preset Locations** column.

Up to 20 preset positions can be added. To move the camera to a preset position, select a Preset Position from the menu. Click **Go To**, and the scanner moves to the selected preset position. To remove a preset position, select the preset position and click **Delete**.

Patrol Settings:

Some or all of the preset positions in the Preset Locations column can be selected for patrol. To construct a patrol sequence, select a preset location from the Preset Locations column and click **Select**. The selected preset location is displayed in the Source column. Up to 20 patrol positions can be added.

The time the camera stays in each position can be modified by entering the number of seconds and clicking **Update**.

To delete a patrol position, select a position and click **Remove**.

To rearrange the patrol order, select a location and click **Up** or **Down**.

Click **Save** to activate the settings.

Once the RS-485 is configured, additional buttons appear on the Home page. See **Camera Control Panel, page 36**.

Applications > Servers

Use the Applications > Servers page to set how alerts are to be reported. When you complete each configuration, click **Test** to test your settings or **Save** to save the settings; otherwise click **Cancel** to discard the changes.

Click a tab to choose the type of server:

- **Simple Mail Transfer Protocol (SMTP)**
- **File Transfer Protocol (FTP)**
- **Samba**
- **HTTP**
- **Instant Message (IM Server)**

Simple Mail Transfer Protocol (SMTP)

Complete the Simple Mail Transfer Protocol (SMTP) server section if you want an alert sent to you by email when motion detection is triggered.

- **Server name**—Enter a descriptive name for the server.
- **Sender email address**—Enter the sender's email address.
- **Recipient email address**—Enter the recipient's email address; that is, to whom the media should be sent when a trigger is activated.
- **Server address**—Enter the domain name or IP address of the email server.
- **Username**—Enter the username of the email account.
- **Password**—Enter the password of the email account.
- **Server port**—Defaults to 25 for the SMTP port setting.
- **SSL Encryption**—Check to enable. May be required for data security by your email provider. By selecting SSL encryption, the default port changes from 25 to 465.

To verify that the email settings are correctly configured, click **Test**. The result is shown in a pop-up window.

If successful, you will also receive an email indicating the result. The email will display the sender that you specified and will have a subject line similar to "Notification: Result of Server Test of Your IP Camera."

File Transfer Protocol (FTP)

The File Transfer Protocol (FTP) server allows the Cisco VC240 network camera to send snapshots and video to the FTP server based on events. This function is similar to the alert via email found in **Simple Mail Transfer Protocol (SMTP), page 72**.

- **Server name**—Enter a descriptive name for the server.
- **Server address**—Enter the domain name or IP address of the FTP server.
- **Server port**—By default, the FTP port is set to 21. It can be assigned a different port number between 1024 and 65535.
- **Username**—Enter the username of the FTP account. A username and password are only required if your FTP server requires authentication.
- **Password**—Enter the password of the FTP account. A username and password are only required if your FTP server requires authentication.
- **FTP folder name**—Enter the FTP folder name.
- **Passive mode**—Passive mode is a common FTP protocol that helps you avoid firewall issues. It is active by default. In FTP passive mode, the camera initiates the connection to the FTP server, resolving issues with the firewall filtering the connection from the FTP server to the camera.

Samba

Samba implements the file transfer protocol SMB/CIFS, allowing the camera to save video directly on a Network Storage System (NSS) or a Samba file server. Complete the Samba server section if you want an alert sent to a NSS or to a Samba file server when an event is triggered. The NSS or file server can then store the snapshots or video.

- **Server name**—Enter a descriptive name for the NSS server or Samba file server.
- **Network storage location**—Enter the location of your NSS server or Samba file server.
- **Workgroup**—Enter the name of the workgroup LAN. A Workgroup is used to share information. For example, if Emily wants to share a folder with Nick, Emily needs to create an account that Nick can access. Emily can create an account in her computer, or use an existing account in an NT domain. If the name of Emily's computer is Emily_PC and the NT domain is FOLDERS, the account for Nick is Emily_PC\Nick or FOLDERS\Nick. The Workgroup field can be referred to Workgroup or Domain.

  The name of the workgroup has to match the name in the NSS or Samba file server. If the account is created in a NSS server, there might not be a Workgroup, and this field can be skipped.
- **Username**—Enter the username of the NSS or Samba file server account. A username and password are only required if your NSS or Samba file server requires authentication.
- **Password**—Enter the password of the NSS or Samba file server account. A username and password are only required if your NSS or Samba file server requires authentication.

HTTP

Complete the HTTP server section if you want an alert sent to an HTTP location when motion detection is triggered.

- **Server name**—Enter a descriptive name for the server.
- **URL**—Enter the HTTP URL.
- **Username**—Enter the username of the HTTP account. A username and password are only required if your HTTP account requires authentication.
- **Password**—Enter the password of the HTTP account. A username and password are only required if your HTTP account requires authentication.

Instant Message (IM Server)

Complete the IM server section if you want an alert sent to an IM address when motion detection is triggered.

- **Server name**—Enter a descriptive name for your IM server.
- **Server address**—Enter the domain name or IP address of the IM server.
- **Jabber ID**—Enter the Instant Message (IM) user ID that the Cisco VC240 camera should use to log in.
- **Password**—Enter the password of the IM account. A password is only required if your IM account requires authentication.
- **Send to**—Enter the address where the alert IM should be sent.
- **Server port**—By default, the IM port is set to 5222. It can be assigned a different port number between 1024 and 65535.

Applications > Motion Detection

The Motion Detection page allows you to set motion detection parameters for the camera. When you complete the configuration, click **Apply** to save the settings.

Microsoft Internet Explorer (IE) 6.x or later is the official supported browser for the Cisco VC240 IP camera. If another browser is used, you may not be able to successfully set values on the Motion Detection page.

- **Enable Motion Detection**—Check this option to turn on motion detection.
- **Window 1/2/3** check boxes—Click to activate a new window. Up to three windows can exist simultaneously. Use the mouse to click, hold, and drag the window frame to resize or the title bar to move. Click the checkbox again to delete the window.
- **Window Name**—You can name the window. It's suggested that you name it for the event being monitored.

  There are two parameters for setting motion detection: Sensitivity and Percentage. After Sensitivity and Percentage are configured and saved, the Indicator bar shows how much motion triggers a response.
- **Sensitivity** is a value that expresses the sensitivity to moving objects. Higher sensitivity settings are expected to sense a slight movement while smaller sensitivity settings tend to ignore the movement.

- **Percentage** is a value that expresses the proportion of “alerted pixels” to all pixels in the motion detection window. For applications that require higher security management, higher sensitivity settings and lower percentage values allow for easier motion detection. Set your percentage to low and the chances are greater that motion will be detected.

Applications > Events

An event can be triggered by many sources, such as motion detection or external digital input devices. When an event is triggered, you can specify what kind of action will be performed. For example, you can configure the Cisco VC240 network camera to send buffered images to an FTP server and to send email notifications when motion is detected.

A maximum of three events can be configured.

NOTE Configure motion detection events in the following order:

1. Set up your servers to specify event delivery; see **Applications > Servers, page 72**.
2. Configure your media; see **Configuring Media Settings, page 78**.
3. Configure your event settings, such as triggers; see **Configuring Event Settings, page 80**.

Configuring Media Settings

Media

- **Media Name**—Enter a descriptive name for the media setting.

Media Type

- **Snapshot**—Sends snapshots when a trigger is activated.
  - **Source**—Choices are **Stream 1** or **Stream 2**.
  - **Send # pre-event images (0-7)—**Specify how many images to capture before a trigger is activated. Up to seven images can be captured. The default is 1 image.
  - **Send # post-event images (0-7)**—Specify how many images to capture after a trigger is activated. Up to seven images can be captured.

For example, if both the Send pre-event images and Send post-event images are set to seven, a total of 15 images are captured after a trigger is activated. The default is 1 image.

- **File Name Prefix—**Enter the text to be added in front of the file name.
- **Add date and time suffix to file name**—Select this option to add a date and time after the file name.

- **Video Clip—**Sends video clips when a trigger is activated.
  - **Source**—Select to record video clips from stream 1 or stream 2.
  - **Pre-event Recording**—Specify to record video clips for a number of seconds before a trigger is activated. Up to nine seconds can be set.
  - **Maximum duration**— Specify to record video clips for a number of seconds before a trigger is activated. Choices are from 1 to 10 seconds; the default is 5 seconds.
  - **Maximum file size**—Specify the maximum file size. Range is from 50 to 800 kb. The default is 500 kb.
  - **File Name Prefix—**Enter the text to be added in front of the video clip name.
- **System Log—**Select to send a system log when a trigger is activated.
- **Instant Message—**Sends an IM message when a trigger is activated.
  - **Message—**Enter the message to be sent when a trigger is activated.

When completed, click **OK** to take effect. The new media name appears in the media drop-down list on the Application > Events page. To remove a media setting from the list, select a media name from the drop-down list and then click **Delete**. If a media setting is currently applied to an event setting it can't be edited or deleted.

Configuring Event Settings

Click **Add** to open up a window where you name an event, and configure the details that trigger the event, when to act upon it, and what action to take.

Event

- **Event name**—The unique name for a recorded event. The maximum length is 40 characters, and the following characters are not allowed: spaces, <, >, &, `, ', or ".
- **Enable this event**—Check to enable recording of this event.
- **Priority**—Select the relative importance of this event. Choose from High, Normal, and Low.
- **Wait at least___ seconds before detecting next event**—The delay to check for the next event. This field is used with motion detection and digital input triggers. The default is 10 seconds.

Trigger

- **Video motion detection**—Select the windows that need to be monitored. Motion Detection must be set first.
- **Periodically—**Trigger the event in specified intervals. The unit of trigger interval is in minutes. The default is 1 minute.
- **Digital input**—Allows you to monitor digital input.
- **System boot**—Trigger the event when the system boots up. Useful if the trigger is caused by a loss of power or tampering.

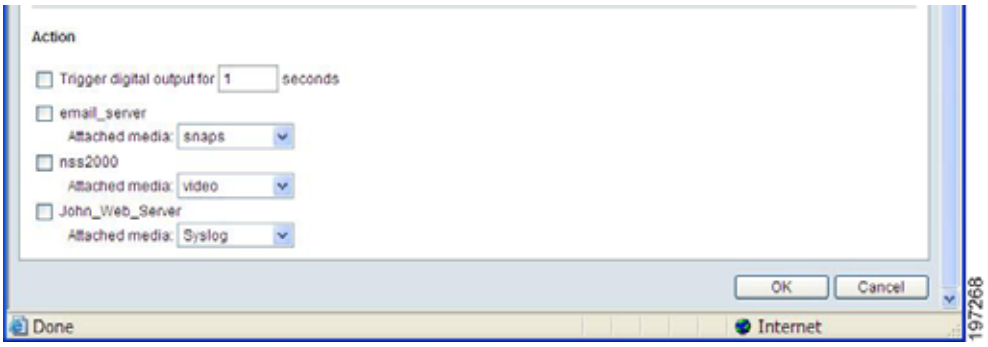
Event Schedule

- **Event Schedule**—Select the specific days that you would like recording to occur.
- **Time**—Select when to record. Choices are Always, or a specific time period in a 24-hour time format.

Action

To display servers as action output, be sure to configure the server settings in **Applications > Servers, page 72**. After you configure multiple servers, additional server entries appear under the **Action** section.

For each event, you can configure the trigger input and select a server as its action output. The digital output is turned on for a set amount of seconds when an event is triggered. The default duration is 1 second.



When completed, click **OK** to take effect. The new media name appears in the Events drop-down list on the Application > Events page. To remove an event setting from the list, select an event name from the drop-down list and then click **Delete**.

Applications > Recording

Recording shows a single item, **Recording**, which allows the configuration of the recording name, status, schedule, stream source and destination of recording. To record to a network storage server device, you must add the NSS device to the Samba file server first. See **Samba, page 74** for more information.

The camera allows a maximum of two recording entries.

Click **Add** to open up the Recording Setting page.

Recording

- **Recording entry name**—Enter a descriptive name for the recording setting.
- **Enable this recording**—Select this option to enable video recording.
- **Priority**—Select the relative importance of this recording setting. Choices are high, normal, and low.
- **Source**—Select either Stream 1 or Stream 2 as the recording source.

Recording Schedule

- **Recording Schedule**—Specify the recording schedule and duration.
  - Select the specific days that you would like recording to occur.
  - Select when to record. Choices are **Always**, or a specific time period in a 24-hour time format.

Destination

- **Destination**—Specify a storage destination for the recorded video files. A network storage server must be configured before an entry appears. See the Samba section on **page 74**.
- **Capacity**—Allows you to set up a quota. If you want the camera to keep recording until all the space is used, choose **Entire Free Space.** Entire Free Space allows recordings to takes up the entire disk free space, reserving a default 100MB disk space. If you want to predefine a specific amount of storage space for recording, choose **Reserved Space.** Reserved Space allows recordings to take up everything except the defined reserve space. In either case, you also have the option to recycle the recording, which overwrites the older video when new video is recorded.
- **File name prefix**—Enter the text that will be put in front of the file name.
- **Enable Cyclic Recording**—If enabled, it works with Capacity and takes precedence over the choices of Entire Free Space or Reserved Space.

  If enabled: When the spare disk space is less than the reserved space, the camera deletes the oldest recording until the spare space is greater than the reserved.

  If not enabled: Recording is stopped when the spare disk space is less than the reserved space (default 100MB, unless specified otherwise).

When completed, click **OK** to take effect. The new recording name appears in the recording drop-down list on the Recording page. To remove a recording setting from the list, select a recording name from the drop-down list and click **Delete**.

Administration > Users

Use the Administration > Users folder to define user settings. This page has two sections: **Admin Password** and **Add/Manage User**. See also **User and Camera Sessions, page 85** for details on user privileges and camera sessions.

Admin Password—The Admin refers to the root administrator. The administrator account is permanent and can not be deleted. If you want to add more accounts, you must first apply a password to the administrator account. See also **Administrator IP Address, page 53**.

STEP 1 Type the admin password identically in both text boxes.

STEP 2 Click **Save** to enable password protection.

STEP 3 A window appears for authentication; type the correct user's name and password to access the Cisco VC240 network camera.

To add a user

Administrators can add up to twenty separate user accounts. The steps to add a user are shown below.

STEP 1 Click **Add**.

STEP 2 Enter the new user's name and password. See **Administration > Password Strength, page 87** for password guidelines.

STEP 3 Choose an **Authentication** type. Authentication types assign access rights. Choices are **Administrator** and **Viewer**.

STEP 4 Click **OK** for the changes to take effect.

To manage a user

Allows an administrator to change access rights or delete user accounts. The steps to change a user account are shown below.

STEP 1 Choose a user from the list of users.

STEP 2 Click **Delete** or **Edit** to make appropriate changes.

STEP 3 Click **OK** for the changes to take effect.

User and Camera Sessions

The Cisco VC240 camera supports three types of user privileges: **root administrator (super admin)**, **administrator**, and **viewer**.

- **Root administrator**—Created by default. Can access, view, and configure the camera. Three root administrator sessions are allowed, but only one root administrator at a time can modify the configuration pages.
- **Administrator**—Created by the root administrator. Can access, view, and configure the camera. Ten administrator sessions are allowed, but only one administrator at a time can modify the configuration pages.
- **Viewer**—Can access and view the camera (monitor the View Video page). Ten sessions are allowed.

Sessions

When logged in, the camera returns a session ID to the browser that is accessing the camera. The browser caches the returned session ID and carries the session ID in each configuration.

The session idle time-out is 10 minutes. The counter to session idle time-out starts when there is inactivity in the configuration pages; that is, the Setup and Client Settings pages. If you are just viewing video, your session in the View Video page never time-outs.

If you accidently close the browser without logging out, open the same browser. The session should still be active.

Connections

The camera allows 10 concurrent connections to the View Video page. Concurrent access degrades the video performance, so any users over 10 will received a message saying that the connection failed.

Sessions are different than connections. Use a session for camera management and a connection to view streaming video. Consider the following examples:

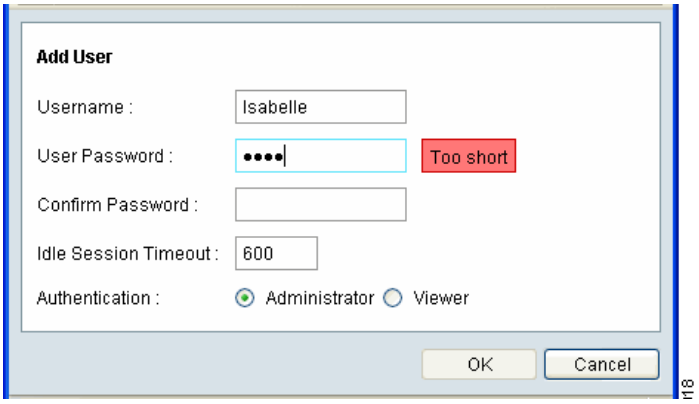
- Viewer logs into the View Video page with 10 Internet Explorer windows on the same computer. This is considered one session and 10 connections.
- Viewer logs into the View Video page with seven Internet Explorer windows and three Firefox windows. This is considered two sessions and 10 connections.
- Viewer logs into the View Video page with two Internet Explorer windows and three Firefox windows and uses the Cisco Video Monitoring System to record a VC240 video stream. This is considered three sessions and six connections.
- Viewer uses five VLC Media Player connections to view video stream 1 and three QuickTime windows to view video stream 2. This is considered zero sessions and eight connections.

Administration > Password Strength

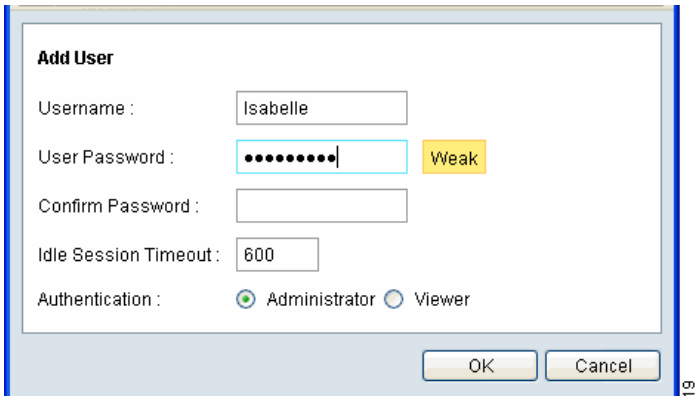
Use the Administration > Password Strength page to help an administrator secure the Cisco VC240 camera. When you complete the configuration, click **Save** to save the settings; otherwise click **Cancel** to discard the changes.

- **Enable Minimum Password Complexity**—Enabled by default. Enforces password complexity when users choose a password. This feature provides added security for your product. When enabled, the following requirements must be met:
  - A password must contain characters from at least three of the following four categories: uppercase letters, lowercase letters, numbers, and special characters available on a standard keyboard.
  - A password cannot be the same as the username, which is cisco by default.
  - A password cannot be the same as the current password.
  - **Minimum Password Length**—Set the minimum password length. The default is 8 and the maximum length is 64.

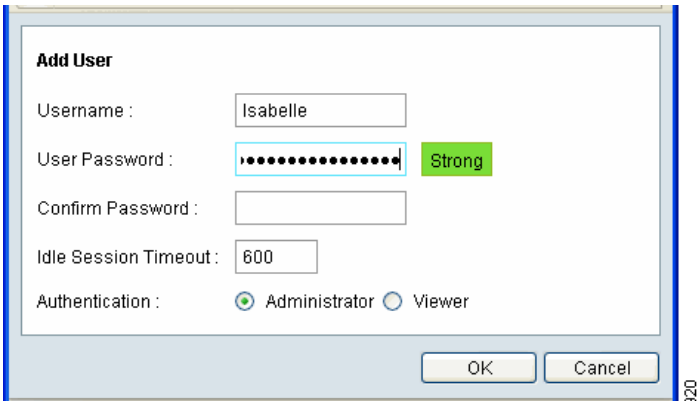
    When a user sets a password in **Administration > Users, page 84** a window appears letting the user know if the password is acceptable. Consider the following examples:
  - **Red**—The password has failed and did not meet the minimum requirements. A message appears indicating the fail reasons.



- **Yellow**—The password is weak, but will be accepted. A message appears indicating that the password is weak. You should try to improve a weak password by adding more characters or using special characters.



- **Green**—The password meets acceptable guidelines. A message appears indicating that the password is strong.



Administration > Time Settings

Use the Administration > Time Settings page to set your camera's date, time, and time zone. When you complete the configuration, click **Save** to save the settings; otherwise click **Cancel** to discard the changes.

Time Zone

- **Camera Date/Time**—Displays the current date and time. You can change the date or time by clicking on the **Change** button. A page appears that has parameters you can modify. The default time zone is Pacific Time.
- **Time Zone**—Set your time zone here.
- **Enable Daylight Saving Time**—Select this option if your location is currently using daylight saving time. You must uncheck the box manually when daylight saving time ends in your time zone.
  - Enter the Start and End dates of Daylight Savings Time.
  - Enter the Daylight Savings Time bias. The default setting is 1 hour.

Network Time Protocol (NTP) Settings

- **Check here if you want to update the time automatically through the NTP Server from the Internet**—Enable or disable the NTP time server feature as required. If enabled, the camera contacts a network time server at regular intervals and update its internal timer. This field is disabled by default.
- **NTP Server Address**—Enter the address of the NTP Server.
- **Default NTP server**—Enter the fully-qualified domain name of a recognized NTP server.
- **NTP Update Interval**—Enter the interval the camera contacts a network time server. Choices are hourly, daily, weekly, or monthly.

NOTE Set the date and time when you first install the VC240 camera or if you restore the camera's default settings. We recommend that you change the time zone and daylight saving period first, and then set the date and time. Set the date and time by either syncing to a local PC, setting the date and time manually, or connecting to an NTP server.

Administration > Discovery Settings

Use the Administration > Discovery Settings page to set the UPnP (Universal Plug and Play) and Bonjour functions of the camera. When you complete the configuration, click **Save** to save the settings; otherwise click **Cancel** to discard the changes.

UPnP

- **Enable Discovery**—Enables the UPnP (Universal Plug and Play) function of the camera, which is a set of computer network protocols that enable device-to-device interoperability. UPnP-compatible systems such as Windows XP are able to detect the presence of the Cisco VC240 network camera. For instructions on setting UPnP on your system, see **Questions and Answers, page 113**.
- **Enable UPnP A/V**—Audio/Video is enabled by default. The UPnP A/V service of the camera allows it to stream video to clients like an iPod touch or XBox.
- **Enable Traversal (Port Mapping)**—If enabled, you must specify the router's WAN IP address and the secondary HTTP port when accessing the Cisco VC240 camera. For example:

  ```
  http://<IP address>:<sec http port>
  ```

Bonjour

Devices with Bonjour automatically broadcast their services and listen for services being advertised by other Bonjour-enabled devices. If you have a Bonjour-enabled browser, such as Microsoft Internet Explorer with a Bonjour plug-in, or the Apple Mac Safari browser, you can find the camera on your local network without knowing its IP address.

You can download the complete Bonjour for Internet Explorer browser from Apple's Web site by visiting http://www.apple.com/bonjour/.

- Select **Enable Discovery** to enable the Bonjour function.

Administration > Firmware

Use Administration > Firmware to upgrade the camera firmware. Click on the **Upgrade** button and the utility checks for available updates at Cisco.com.

- Cisco recommends that you use a computer within the camera's local network to perform the upgrade. If you attempt to upgrade the camera's firmware from a remote location—using a computer outside of the camera's local network—the upgrade may fail.
- If for any reason the firmware upgrade process is interrupted and results in corrupted firmware, the Cisco VC240 upon reboot will go to a Firmware Recovery page where you can upload the latest firmware.

Administration > Configuration File

Use Administration > Configuration File to create text-editable configurations, making deployment and configuration changes easier. A text-editable configuration means that the configuration file is saved in ASCII format and can be viewed and modified by a standard text editor. These configuration files are validated during processing and rejected if there are errors.

- **Export Configuration File**—Specify one of three types of configuration files to export to a local PC:
  - **Startup**—Current file used by the Cisco VC240 network camera.
  - **Mirror**— A file is generated automatically by the Cisco VC240 network camera if the startup configuration file has not been modified for 24 hours. The intention is to allow the administrator to recover the last known good configuration if an error occurs.
  - **Backup**—A redundant file specified by the user.

NOTE When you export a file to later import into another camera, make sure that the new camera is on the same firmware version as the camera that created the config file.

- **Import Configuration File**—Copy an existing configuration file (Startup, Mirror, or Backup) from your computer to the camera.
- **Copy Configuration File**—Specify the file name of configuration file to copy and place in either Mirror or Backup.

The uploaded configuration file will be written to flash and saved over either the Startup or Backup configuration file, whichever was selected by the administrator. The camera must reboot for an overwrite of the Startup Config to take effect.

Administration > Maintenance

The Administration > Maintenance page gives options for Restart and Restore. When you complete the configuration, click **Save** to save the settings; otherwise click **Cancel** to discard the changes.

Restart

- **Restart**—Resets the camera. Reset preserves your network settings.

Restore Defaults

- **Restore Defaults**—Click to reset all settings to the factory defaults. During the restoration process, you will receive a message that the device is rebooting, and that your browser will reconnect to your camera's IP address. Restore Defaults preserves your network settings.

Restore to Factory Default

- **Restore to Factory Defaults**—Click to restore the factory default settings. The system is reset to the initial factory settings and changes previously made are lost.

NOTE Set the date and time if you restore the camera's default settings. We recommend that you change the time zone and daylight saving period first, and then set the date and time. Set the date and time by either syncing to a local PC, setting the date and time manually, or connecting to an NTP server.

Administration > System Log

Use Administration > System Log to send the system log file to a remote server as a log backup instead of receiving the log information locally. Before using this feature, it is suggested that you install a log-recording tool to receive system log messages from the camera. One example of a tool is the Kiwi Syslog Daemon.

Follow the steps below to set up the remote log:

STEP 1 Check the **Enable remote log** box.

STEP 2 In the IP address text box, enter the IP address of the remote server.

STEP 3 In the port text box, enter the port number of the remote server. The default port is 514.

STEP 4 When completed, click **Save** to take effect.

Status > System Summary

Use Status > System Summary to display up-to-date camera information.

- **General Information**—Displays the camera name, serial number, date and time, firmware version, MAC address, and firmware MD5 checksum of the camera.
- **Network Status**—Displays the information about network type and IP address.
- **Image Status**—Display the mode, resolution, video quality, and frame rate of Stream 1 and Stream 2.
- **Audio**—Displays the audio status and source.
- **I/O Ports Status**—Displays the status of I/O ports.

Where to Go Next

For instructions on adjusting the lens and attaching the sun shield, see:

- **Finalizing the Cisco VC240 Hardware Setup, page 97**

For sample configurations, see:

- **Sample Configurations for the Cisco VC240 Network Camera, page 100**

For troubleshooting questions and answers, see

- **Troubleshooting, page 113**

7

Finalizing the Cisco VC240 Hardware Setup

This chapter describes how to adjust and focus the lens, and reattach the dome cover:

Adjusting the Lens

While viewing live video from your camera, you can now adjust the zoom factor and focus range as needed.

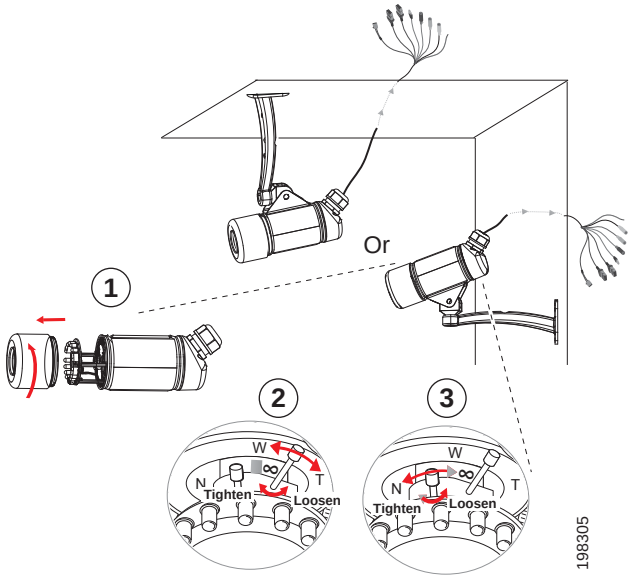
To adjust the zoom factor and focus range, follow these steps:

STEP 1 Remove the lens cover.

STEP 2 Gently loosen the zoom controller (back adjustment) and adjust the zoom factor from Wide (W) to Telephoto (T). Upon completion, gently tighten the zoom controller.

STEP 3 Gently loosen the focus controller (front adjustment) to adjust the focus range from Near to Infinity. Upon completion, gently tighten the focus controller.

STEP 4 Reattach the lens cover.



Attaching the Sun Shield

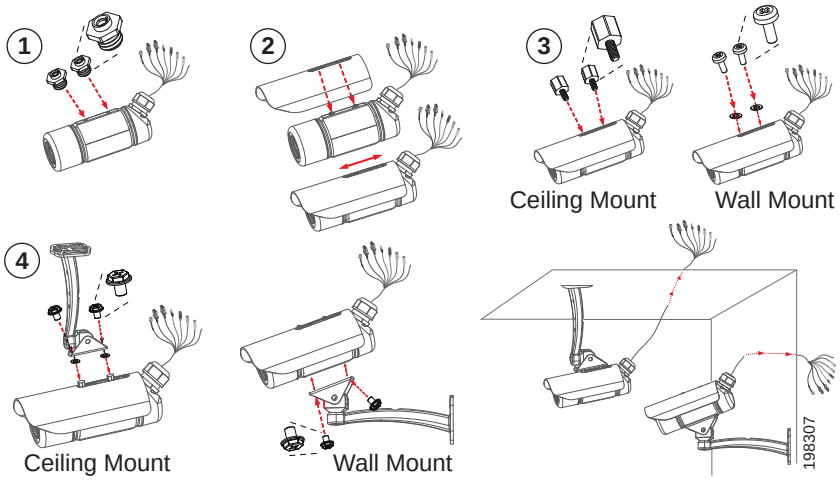
To use the supplied sun shield in outdoor environments, follow these steps.

STEP 1 Insert the supplied screws in the corresponding hole on top of the camera as shown below. Then, tighten the screws using the supplied open-end wrench.

STEP 2 Attach the supplied sun shield to the camera and slide it to the desired position.

STEP 3 Secure the sun shield with the appropriate screws. If you are mounting the camera on a ceiling, insert the screws as shown below.

STEP 4 Attach the camera to the camera stand.



Placing Silica Gel Desiccant Bags Inside the Camera

The VC240 camera comes with silica gel desiccant bags. One is placed inside the camera using two-sided adhesive tape and the other is a replacement bag provided in a sealed aluminum bag.

If you decide to remove the lens cover after more than six months of camera use, remove the used silica bag and place the replacement bag inside the camera before reattaching the lens cover.

While the camera is 100% waterproof, the silica gel desiccant bags help protect the camera by absorbing the small amount of moisture that might form during the initial startup when components go from cold to hot in a matter of few seconds. This prevents moisture from condensing on the lens or its glass cover

8

Sample Configurations for the Cisco VC240 Network Camera

Your Cisco VC240 network camera is capable of many functions. The following are sample configurations for the most popular Cisco VC240 camera settings:

Microsoft Internet Explorer (IE) or later is the official supported browser for the Cisco VC240 network camera. Other browsers provide limited functionality.

Configuring One-Click Recording

To record a video event happening immediately, follow these steps:

STEP 1 Click **View Video** in the toolbar to go to the Cisco VC240 View Video page.

STEP 2 On the View Video page, click **Start Recording** (light red icon).

Recording is enabled.

STEP 3 Click **Stop Recording** when you want to stop recording (bright red icon).

STEP 4 Go to `C:\Record` (default location) to view the video.

Configuring Server Push on Firefox

While Mozilla Firefox is not the recommended browser, it can be used to stream video. If the video mode is set to MJPEG you can receive continuous JPEG pictures, which is known as server push. Microsoft Internet Explorer does not support server push technology.

In Mozilla Firefox use one of the following URL formats:

```
http://<ip_address>/video.mjpg
```

```
http://<host_name>.local/video.mjpg
```

Use the following procedure to set the access name for Stream 1 to video.mjpg.

STEP 1 Configure a user to have viewer privileges. (An administrator login is acceptable, but not convenient in multiple viewer situations.) See **Administration > Users, page 84** for instructions on setting up a user.

STEP 2 Launch Mozilla Firefox.

STEP 3 Set the video mode to MJPEG.

STEP 4 Type the URL command in the address field. Press **Enter**.

STEP 5 Enter your username and password for the camera, as the first time the browser accesses the video, user authentication is required. After the first login, the browser caches the session credentials and for any sessions initiated after that, no further user input is required.

Using Third-Party Video Players to View Video

Over a LAN Interface

You can use third-party video players, such as Apple QuickTime Player or VideoLAN VLC Player to stream real-time video and playback recorded video on your local LAN. In most applications, simply enter the URL of your camera into the video player application in the following format:

```
rtsp://<IP Address of camera>/<live_video.sdp>
```

NOTE <live_video.sdp> is example of an access name for Video Stream 1. For information on access stream configurations, see the VC240 Administration Guide.

In some cases when using Apple QuickTime Player some additional configuration is required. In that case, use the following instructions to play video on a UDP media stream.

NOTE Apple QuickTime Player does not support HTTPs media streams.

Setup

STEP 1 Open QuickTime and in the main menu choose **Edit** > **Preferences** > **QuickTime Preferences**.

STEP 2 In the **Advanced** tab, under Streaming, choose **Custom...** from Transport Setup. The Streaming Transport pop-up appears.

- Enter **UDP** as the Transport Protocol.
- Enter **554** as the Port ID.
- Click **OK** to close the popup window.

STEP 3 Click **Apply** in the Advanced tab.

STEP 4 In the Advanced tab, under **Video**, choose the button for **DirectX**.

STEP 5 Check **Enable DirectDraw acceleration**. (Do not check the other two items.)

STEP 6 Click **OK**.

View Video

STEP 1 In QuickTime, choose **File** > **Open URL**.

STEP 2 Enter the URL for the video using this format: `rtsp://<IP Address of camera>/<live_video.sdp>`.

STEP 3 Click **OK**.

Over a WAN Interface

You can also use VLC Player to stream real-time video and playback recorded video over a WAN connection. To do so, you must set up port forwarding on your router. For complete instructions on setting up port forwarding, see **Configuring Port Forwarding, page 111**.

When setting up port forwarding:

- The destination IP address is the camera's IP address
- Set HTTP to port 80 (for web access)
- Set RTSP to port 554 (for video viewing)

Then use the following format in VLC Player:

`rtsp://<WAN router IP Address>/<live_video.sdp>`

Use the same format in your cell phone, but change the resolution on your cell phone to the smallest size.

Configuring Motion Detection with Email Notification

When configuring motion detection, once an action is detected, you may want to be advised by email. The following steps are required to set up an email notification system:

1. Define your video parameters for each stream.
2. Define your SMTP email server.
3. Configure motion detection.
4. Configure your media settings.
5. Configure your event settings.

NOTE **Motion Detection cannot be configured using the Firefox browser.** Internet Explorer must be used to configure motion detection.

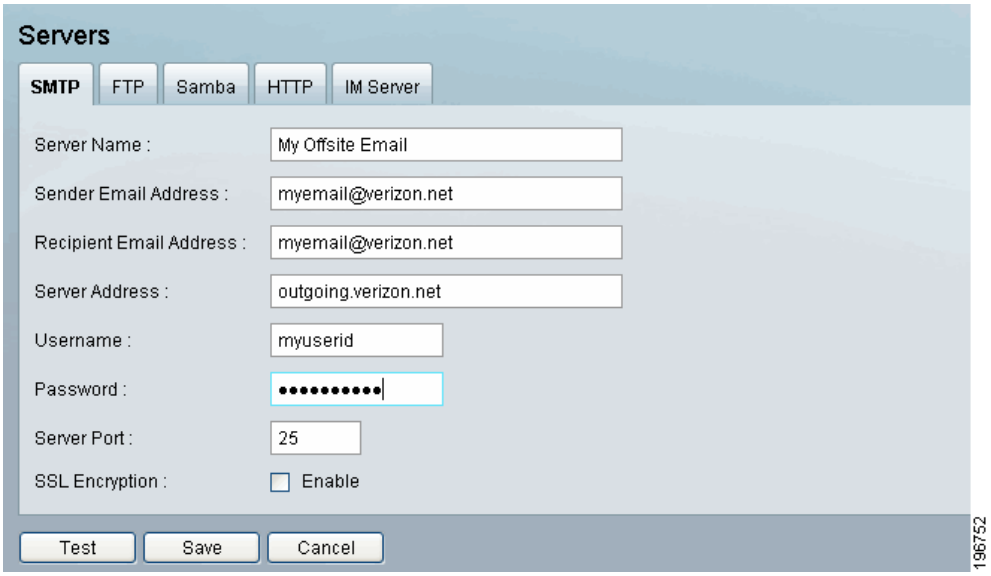
STEP 1 Define your media as either MPEG-4 or MJPEG for each stream. See **Camera Control > Video Settings, page 61** to define your media and for more information about the differences between MPEG-4 and MJPEG.

STEP 2 Configure your SMTP email server.

a. Go to the Applications > Servers page. See **Applications > Servers, page 72** for more information on this page.

b. In the SMTP Server tab, enter the SMTP server name or the IP address and port number of the SMTP server. An account name and password are only required if your mail server requires authentication.

c. Enter the appropriate email addresses.



d. Click **Test** to test your settings.

e. Click **Save**.

STEP 3 Configure motion detection.

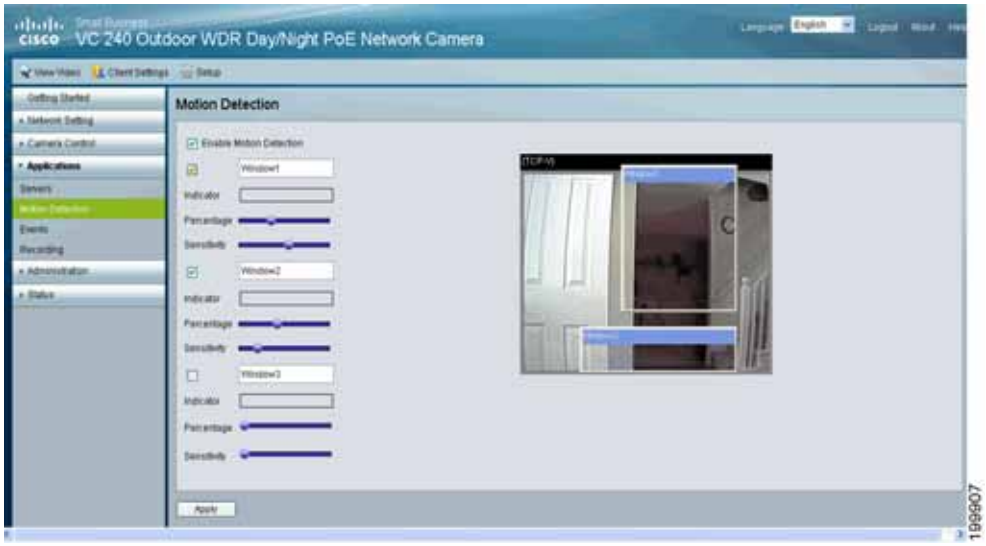
NOTE **Motion Detection cannot be configured using the Firefox browser.** Internet Explorer must be used to configure motion detection.

a. Access the setup options for your Cisco VC240 network camera by clicking **Setup**.

b. Go to the Applications > Motion Detection page.

c. Check **Enable Motion Detection**. You can now set the areas to be monitored, as well as the sensitivity.

d. Customize the desired areas of monitoring. You can select one or more windows and isolate specific sections to be monitored by clicking and dragging the monitoring box that appears in the video window.



e. Adjust the sensitivity of each section by using the sensitivity slider.

f. Adjust the percentage of each section by using the percentage slider.

g. Click **Apply** to save your settings. You are now set to receive motions detection email alerts.

STEP 4 Configure your media settings.

a. Access the setup options for your Cisco VC240 network camera by clicking **Setup** > **Applications** > **Events**.

b. Go to **Configuring Media Settings, page 78** for more information.

c. Configure the media settings that you require. For example, if you choose **Snapshot** you can specify the number of pre- and post-event motion detection images you would like sent to you.

STEP 5 Configure your event settings.

a. Access the setup options for your Cisco VC240 network camera by clicking **Setup** > **Applications** > **Events**.

b. Go to **Configuring Event Settings, page 80** for more information.

c. Configure the event features that you require. At minimum, activate the following fields:

- Check **Enable This Event** to enable recording of the event.
- Select the **Video Motion Detection** trigger.
- Set an **Event Schedule** and **Time**.

With the completion of these steps, email notification is set.

Configuring the GPIO Ports

The following instructions help you configure the General Input and Output (GPIO) on the Cisco VC240 camera. In general, you will need to:

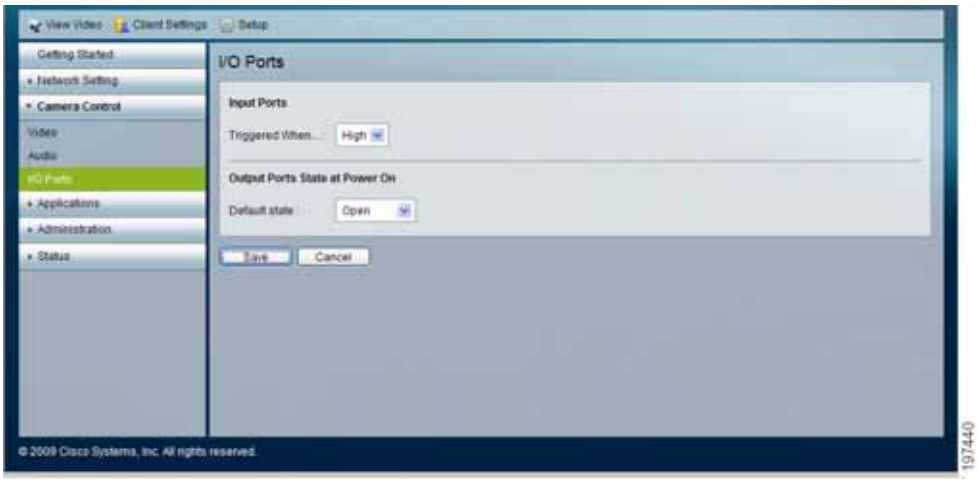
- Make the GPIO connections and test the external device connections. See **General Purpose Input/Output (GPIO), page 14** for connection diagrams and further information.
- Setup an event.

Consider the following example:

STEP 1 Make and test the output GPIO connection.

a. Connect the output device to pin 1 and pin 2.

b. Go to the Camera Control > I/O Port page to select the proper **Default State** for the output port.



c. Go to the View Video page

d. Click the **On** button on the View Video page. The device should turn on.

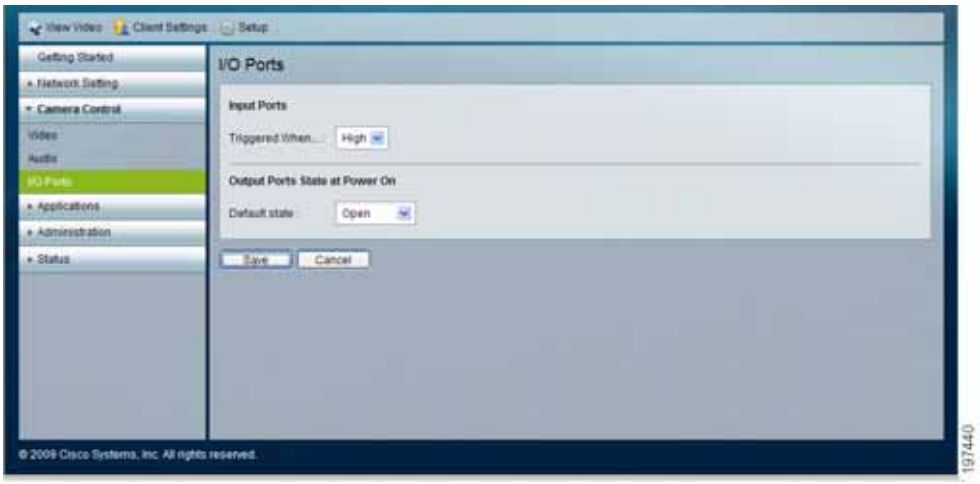
e. Click the **Off** button on the View Video page. The device should turn off.

f. Go to the Status > System Summary page. **I/O Port Status** should show the output as Triggered when the device is on and Normal when the device is off.

STEP 2 Make and test the input GPIO connection.

a. Connect the input device to pin 3 and pin 4.

b. Go to the Camera Control > I/O Port page to select the proper **Triggering When (State)** for the input port.



c. Go to the Status> System Summary page. **I/O Port Status** should show the input as Triggered when the device is sensing (keep clicking **Refresh**) and Normal when the device is off.

STEP 3 Setup an event connecting the input and output devices on the Application > Event page. This is similar to setting up motion detection and an email video clip. See **Configuring Event Settings, page 80** for more information.

a. Enter an **Event Name**.

b. Enable the **Event**.

c. Select **Digital Input** as the Trigger.

d. Configure the **Event Schedule**.

e. Under Action, enter a number of seconds in **Trigger digital output for x seconds**.

Your GPIO devices are now configured.

Configuring Port Forwarding

Port forwarding allows Internet access to multiple cameras that are located inside a local network. For example, you have two cameras behind a NAT router – one is on primary or alternate port 1024 and the second one is on port 1028. To access each camera individually, set up two port forwarding rules to access the web interface of the camera. You can then go to http://x.x.x.x:####/ where x.x.x.x is the WAN IP of the router and #### is the defined alternate port on the camera.

To set up port forwarding, follow these steps:

STEP 1 From the camera's web-based configuration utility, click **Network Setting > Port Setting**.

STEP 2 Enter a port number in the primary or secondary HTTP Port field. For example, enter 1028. Valid port settings are 1024-65535.

NOTE When you open the URL to the camera, you now must specify the WAN IP address and the port number.

STEP 3 Click **Save** and close the page.

STEP 4 Enter the IP address of your router in your web browser's Address field and press **Enter**. In this example, the default IP address of the router is used (**192.168.1.1**).

STEP 5 From the web-based configuration utility, click **Firewall > Port Range Forwarding**.

STEP 6 In the Port Range Forwarding page, configure the following:

a. Enter the Application name, such as **Camera**.

b. Enter the Start and End RTSP port. In this example, 1028 is used and this should match the HTTP port configured on the camera in **Step 2 on page 111**.

c. Ensure that Protocol is set to **Both** (TCP and UDP).

d. Enter the IP address of the camera, in the IP Address field.

e. Check the **Enable** box to enable forwarding.

STEP 7 Click **Save** to save the configuration to the router.

STEP 8 Locate the WAN IP address for your router. Click **Setup > Summary** to view the WAN IP address of the router. The WAN IP address is displayed in the Network Setting Status section.

This example shows the Summary page of the Cisco WRVS4400N router.

Now you should be able to access your camera over the Internet by typing in the WAN IP address of your router, a colon, and the defined port number in the following format: `http://router's WAN IP address:port`

For example, `http://12.19.89.212:1028`

A

Troubleshooting

Questions and Answers

This appendix provides solutions to some problems that may occur during the installation and operation of the Cisco VC240 Network Camera. Read the description below to solve your problems. If you can't find an answer here, check the Cisco Small Business Video Surveillance Cameras homepage at www.cisco.com/go/surveillance.

NOTE Microsoft Internet Explorer (IE) 6.x or later is the official supported browser for the Cisco VC 240 network camera.

Q. When I try to connect to the camera, I am prompted for a username and password.

You should be prompted for a username and password when you first connect to the camera. Enter the Administrator ID and Password that was set on the Administrator > Users page. See the **Administration > Users, page 84**. The Username/Password prompt indicates that the Administrator has restricted access to specified users. Ask the Administrator for your username and password.

If a username/password has not been set, it should be the default of cisco/cisco.

Q. I can't connect to the camera with my Web Browser.

It is possible that the IP address of your computer is not compatible with the IP address of the camera. Run the Setup Wizard to configure the camera with a valid IP address. See **Installing the Cisco VC240 Network Camera Software, page 29** for more information on IP addressing.

Q. My video quality suddenly deteriorated.

This can happen when additional viewers connect to the camera, overloading the camera or the available bandwidth. The image size and quality can be adjusted to the required number of viewers and the available bandwidth. Make these adjustments on **Camera Control > Video Settings, page 61**.

Q. I don't receive any emails when an event is detected.

It may be that the SMTP (Simple Mail Transport Protocol) server used by the camera to send the e-mail will not accept mail. (This is to prevent Spam from being sent to an SMTP server). Try using a different SMTP server, or contact your ISP to see if SMTP access is being blocked.

You can also try a ping test to the SMTP server to see if it responds. While a response doesn't necessarily prove that your SMTP will accept email, it does let you know if the server is up. Also note that if SSL Encryption is active, on port 465, then the SMTP server must support SSL. Otherwise don't check SSL and configure your local mail server (such as your Windows 2003/2008 mail server or Exchange mail server) to handle local mail.

Q. When using the motion detection feature, I receive emails that don't show any moving objects.

The motion detection feature may be too sensitive and can cause false alarms. Motion detection compares frames to see if they are different. Major differences between frames are assumed to be caused by moving objects.

If the sensitivity is set too high, motion detection can be triggered by sudden changes in the level of available light or movement of the camera itself. For example, twilight, like dusk and dawn, can cause false positive detections. Motion detection should not be used if the camera is outdoors because of the possibility of false positives. The motion detection feature works best in locations where there is good steady illumination, and the camera is mounted securely.

Q. The video image is blurry.

Try cleaning the dome, or adjusting the MPEG-4 or MJPEG image quality setting found in **Camera Control > Video Settings, page 61**. Video created with lower settings will contain less detail; this is the trade-off for using less bandwidth. You should also manually adjust the focus and zoom. See **Adjusting the Lens, page 97**.

Q. How can I find out my camera's IP address?

By default, the camera automatically receives a DHCP IP address. To identify the IP address, you can do the following procedure:

STEP 1 On a computer connected to your router go to **Start > Run**.

STEP 2 Type **cmd window**.

STEP 3 At command line, type **ipconfig**.

STEP 4 Look for Default Gateway. This is your LAN router's IP address

STEP 5 In a web browser, login to your router by typing the router's IP address.

STEP 6 Each router shows the IP address differently.

- Look for a DHCP client table that lists DHCP IP addresses. It can be found on the Summary, Status > LAN, or DHCP page.
- Look for your camera's MAC address. The camera's IP address should be next to your MAC address.

Q. How do I set up UPnP so my cameras broadcast their availability to my network?

UPnP networking technology provides automatic IP configuration and dynamic discovery of devices added to a network. Services and capabilities offered by networked devices, such as printing and file sharing, are available among each other without a lot of network configuration.

UPnP Is automatically enabled on the cameras. In a Windows environment, it may or may not be enabled. On Windows XP, you must log on to the computer as a system administrator to install the UPnP components. If using Windows Vista, UPnP Is enabled by default. However, if it is not enabled, turn off UAC (User Access Control) before following this procedure.

Follow these steps to enable UPnP user interface on your computer:

STEP 1 Go to **Start**, click **Control Panel**, and then click **Add or Remove Programs**.

STEP 2 In the **Add or Remove Programs** dialog box, click **Add/Remove Windows Components.**

NOTE If the default ports are already used by another device connecting to the same router, the camera will select another port.

STEP 3 In the **Windows Components Wizard** dialog box, make sure Networking Services is checked.

STEP 4 Highlight Networking Services, and then click **Details**.

STEP 5 In the Networking Services dialog box, select Universal Plug and Play and then click **OK**.

STEP 6 Click **Next** in the following window.

STEP 7 Click **Finish**. UPnP is enabled.

NOTE Another way to enable UPnP on Windows XP is to go to **My Network Places** and on the left tab click on **Show icons for networked UPnP devices**.

B

Where to Go From Here

Cisco provides a wide range of resources to help you and your customer obtain the full benefits of the Cisco VC240 network camera.

Product Resources

Support	
Cisco Small Business Support Community	www.cisco.com/go/smallbizsupport
Cisco Small Business Support and Resources	www.cisco.com/go/smallbizhelp
Phone Support Contacts	www.cisco.com/en/US/support/tsd_cisco_small_business_support_center_contacts.html
Cisco Small Business Firmware Downloads	www.cisco.com/go/smallbizfirmware Select a link to download firmware for Cisco Small Business Products. No login is required. Downloads for all other Cisco Small Business products, including Network Storage Systems, are available in the Download area on Cisco.com at www.cisco.com/go/software (registration/login required).
Product Documentation	
SW VMS16, VM 200, and VM 300 Video Monitoring System Administration Guide	www.cisco.com/go/surveillance

Quick Start Guide for the Cisco VC240 Camera	www.cisco.com/go/smallbizcameras
Accessories Guide for the Cisco VC240 Camera	www.cisco.com/go/smallbizcameras
Cisco Small Business	
Cisco Partner Central for Small Business (Partner Login Required)	www.cisco.com/web/partners/sell/smb
Cisco Small Business Home	www.cisco.com/smb
Cisco Small Business Surveillance	www.cisco.com/go/surveillance