CISCO

ADMINISTRATION GUIDE

Cisco Small Business

WVC210 Wireless-G PTZ Internet Video Camera With 2-Way Audio

.

Contents

Contents

Introduction

Congratulations on purchasing your Cisco Small Business WVC210 Wireless-G PTZ Internet Camera. Cisco is the leader in Wi-Fi certified Internet cameras, and the Cisco WVC210 Network Camera is part of the largest portfolio of Wi-Fi certified cameras in the marketplace.

The Cisco WVC210 Wireless-G PTZ Internet Video Camera sends live video through the Internet to a web browser anywhere in the world. The camera supports dual codecs (MPEG-4 and MJPEG), which can be used simultaneously. MPEG-4 gives efficient bandwidth consumption with good-quality compression and is optimal for real-time viewing of video. MJPEG gives optimal video quality, making it ideal for large-volume storage to a network attached storage (NAS) device.

The Cisco WVC210's audio capabilities include two-way audio, an embedded microphone, external speaker and microphone ports, and voice compression. With extensive support for features such as IP multicast, Real Time Streaming Protocol (RTSP), Real Time Protocol (RTP), and 3rd Generation Partnership Project (3GPP), it enables video to be viewed from multiple endpoints and client applications, such as 3G phones and QuickTime clients on PCs or Wi-Fi phones. Network protocols such as 802.1p priority, 802.1Q VLANs, and Dynamic DNS (DDNS) are also supported.

The pan/tilt and digital zoom functions allow you to remotely control the camera's movement and zoom, giving you maximum remote flexibility. Up to 10 simultaneous unicast users can access the camera at any time. Video monitoring software is included for monitoring multiple cameras and recording to your hard drive, with advanced search by time and date. Recording can be set up to start by motion trigger or by manual or scheduled recording. Playback is available on Windows Media Player, with no need for a proprietary player.

You can also enable security mode, which tells the camera to send a message with a short attached video to up to three e-mail addresses whenever it detects motion in its field of view. You can then log in through a web browser to view the live video stream if the situation warrants. Wireless security options include Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), WPA2, and WPA Enterprise.

The guide focuses on the hardware and software features of the Cisco Small Business WVC210 Wireless-G PTZ Internet Camera. Advanced video monitoring features and procedures are covered in the Cisco Small Business Video Monitoring System Administration Guide.

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

Minimum Requirements

The following tables list the minimum requirements for your PC when monitoring one camera or up to eight cameras.

NOTE These requirements are approximate. Lighting, frame rate, codec, and resolution can all affect the storage size.

Minimum System Requirements (for one camera)

CPU	Pentium 4 class, 2 GHz
Memory	512 MB
Operating System	Microsoft Windows 2000, XP, or Vista
Hard Drive	500 MB of available space
Graphics Card	AGP with a minimum 128 MB
Browser	Internet Explorer 6.0 (or later) with ActiveX support for viewing, recording, playback and setting motion detection; limited support for Safari and Mozilla Firefox (no motion detection).

Minimum System Requirements (for up to eight cameras)

CPU	Pentium 4 class, 3 GHz dual-core
Memory	1 GB
Operating System	Microsoft Windows 2000, XP, or Vista
Hard Drive	4 GB of available space
Graphics Card	NVidia high performance or equivalent with a minimum of 256 MB
Browser	Internet Explorer 6.0 (or later) with ActiveX support for viewing, recording, playback and setting motion detection; limited support for Safari and Mozilla Firefox (no motion detection).

NOTE More than 8 cameras can be monitored if you reduce the resolution and frame rate settings for the video captures. For more information about these settings, see **Audio/Video, page 45**.

Planning Your Wireless Network

Careful planning is required for a wireless network, to ensure that your users can access the network resources that they need and to ensure that intruders are kept out.

This chapter includes the following sections:

Ad-Hoc and Infrastructure Modes

A wireless local area network (WLAN) is exactly like a regular local area network (LAN), except that each computer in the WLAN uses a wireless device to connect to the network. Computers and other devices, such as peripherals, in a WLAN share the same frequency channel and SSID, which is an identification name for wireless devices.

Unlike wired networks, wireless networks have two different modes in which they may be set up: infrastructure and ad-hoc.

- **Infrastructure mode**—The WLAN and wired LAN communicate through an access point. Choose this mode if the wireless network needs to share data or peripherals, such as printers, with a wired network.

  The basis of infrastructure mode centers around an access point, which serves as the main point of communications in a wireless network. (A wireless router can also be used because a wireless router incorporates the capabilities of an access point.) Access points transmit data to PCs equipped with wireless network cards, which can roam within a certain radial range of the access point. Multiple access points can be arranged to work in succession to extend the roaming range, and can be set up to communicate with your Ethernet (wired) hardware as well.

- **Ad-hoc mode**—Wireless computers communicate directly with one another. Choose this mode if your wireless network does not require access to data or peripherals on a wired network.

  If the wireless network is relatively small and needs to share resources only with the other computers on the wireless network, then ad-hoc mode can be used. Ad-hoc mode allows computers equipped with wireless transmitters and receivers to communicate directly with each other, eliminating the need for an access point. The drawback of this mode is that wireless-equipped computers are not able to communicate with computers on a wired network. And, of course, communication between the wireless-equipped computers is limited by the distance and interference directly between them.

Wireless Network Layout

The Cisco WVC210 Internet camera is compatible with all 802.11g and 802.11n routers, such as model number WRVS4400N, as well as all 802.11g access points, including model number WAP4410N. The camera can also communicate with network adapters, such as the Wireless-G Notebook Adapter (model number WPC4400N) for your laptop computers, Wireless-G PCI Adapter (model numbers WMP200) for your desktop PCs, and Wireless-G USB Adapter (model number WUSB200) for your computers that connect to the wireless network through USB modems.

With these, and many other Cisco products, your networking options are limitless. Go to the Cisco website at www.cisco.com for more information about Cisco products.

NOTE Your wireless range is variable and depends on your environment.

Security Threats Facing Wireless Networks

Cisco wants to make wireless networking as safe and easy for you as possible. The current generation of Cisco products provide several network security features, but they require specific action on your part for implementation. So, keep the following suggestions in mind whenever you are setting up or using your wireless network. Also see **Setting Security Precautions on the Cisco WVC210, page 70**.

Wireless networks are easy to find. Hackers know that in order to join a wireless network, wireless networking products first listen for "beacon messages." These messages can be easily decrypted and contain much of the network's information, such as the network's SSID (Service Set Identifier). Here are the steps you can take to prevent intruders:

Change the administrator's password regularly—With every wireless networking device you use, keep in mind that network settings (SSID, WEP keys, etc.) are stored in its firmware. Your network administrator is the only person who can change network settings. If a hacker learns the administrator's password, he, too, can change those settings. So, make it harder for a hacker to get that information. Change the administrator's password regularly.

SSID—There are several things to keep in mind about the SSID:

- Do not broadcast it
- Make it unique
- Change it often

Most wireless networking devices will give you the option of broadcasting the SSID, meaning that the SSID can be seen by anyone who is scanning for an available wireless network. While this option may be more convenient for your users, it is also convenient for hackers. So, don't broadcast the SSID.

Wireless networking products come with a default SSID set from the factory. (The Cisco default SSID is "ciscosb".) Hackers know these defaults and can use them to find your network, even if you are not broadcasting the SSID. Change your SSID to something unique and that does not identify your company or the networking products you use.

Change your SSID regularly so that any hackers who have gained access to your wireless network will have difficulty finding it again.

MAC Addresses—Enable MAC Address filtering. MAC addresses are unique identification numbers that are assigned to a device at the factory. MAC Address filtering allows you to provide access only to devices that you specify. This feature makes it harder for a hacker to access your network with a random MAC Address.

WEP Encryption—Wired Equivalent Privacy (WEP) is an older encryption method that is not considered to be secure and can easily be broken. Select this option only if you need to allow access to devices that do not support WPA or WPA2.

If you must use WEP, take the following precautions to make a hacker's job more difficult:

- Use the highest level of encryption possible

- Use "Shared Key" authentication

- Change your WEP key regularly

WPA/WPA2 Personal—WPA stands for Wi-Fi Protected Access, which is a security standard stronger than WEP encryption. A network encrypted with WPA/WPA2 is more secure than a network encrypted with WEP, because WPA/WPA2 uses dynamic key encryption. To protect the information as it passes over the airwaves, you should enable the highest level.

WPA/WPA Enterprise—Enterprise refers to using RADIUS server for authentication, while RADIUS stands for Remote Authentication Dial-In User Service. This type of authentication requires some advanced expertise because it involves setting up a RADIUS server for authentication and, in some cases, creation of certificates for both the RADIUS server and the camera.

If you are using WPA/WPA2 Enterprise security, you will need to upload security certificates to the camera. Certificates must be in the following format:

- Root certificate: DER encoded binary x.509 (CER/PEM)

- User certificate: Personal Information Exchange (PKCS#12(.PFX))

Implementing encryption may have a negative impact on your network's performance, but if you are transmitting sensitive data over your network, encryption should be used.

These security recommendations should help keep your mind at ease while you are enjoying the most flexible and convenient technology Cisco has to offer.

⚠️

CAUTION Always remember that each device in your wireless network MUST use the same encryption method and encryption key or your wireless network will not function properly.

Additional Security Tips

The following tips can help prevent hackers from gaining access into your wireless network.

- Keep wireless routers, access points, or gateways away from exterior walls and windows.

- Turn wireless routers, access points, or gateways off when they are not being used (at night, during vacations).

- Use strong passphrases that are at least eight characters in length. Combine letters and numbers to avoid using standard words that can be found in the dictionary.

3

Getting to Know the Cisco WVC210 Internet Camera

In this chapter, you'll find the following sections:

Side Panel

On the side panel, you'll find the antenna connector. Attach the antenna here.

Front Panel

The camera, LEDs, built-in microphone, and LCD screen are located on the front of the camera.

.
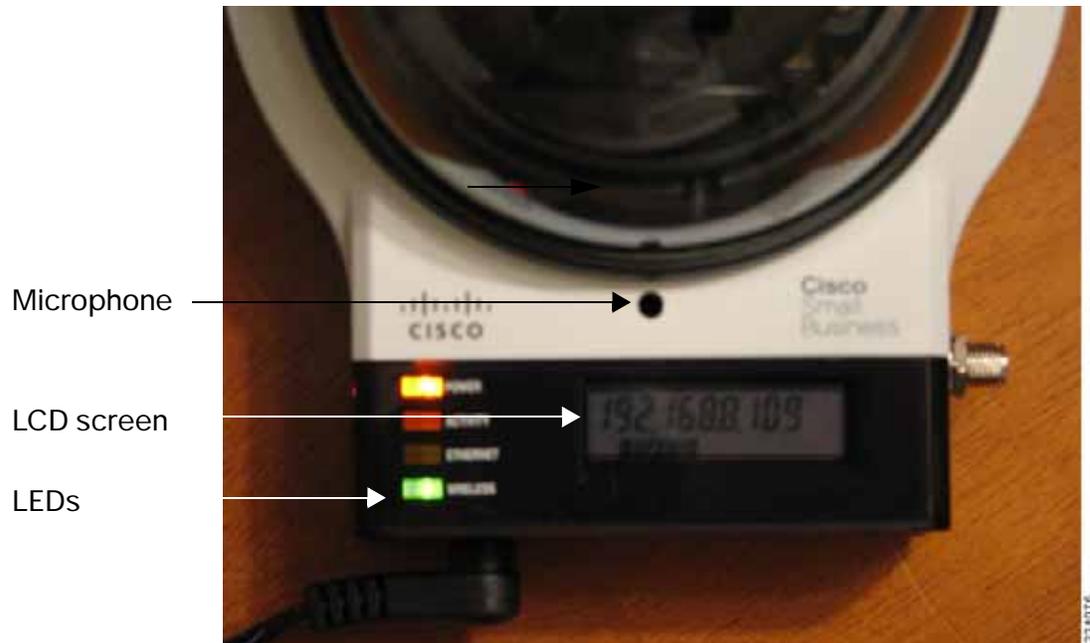
LCD Screen

The LCD screen indicates the camera's current IP address and whether it is a fixed or dynamic address. If the camera uses a fixed IP address, then the screen displays the word "FIXED." If the camera uses a dynamic IP address, then the screen displays the word "DHCP."

Built-in Microphone

The built-in microphone is located above the LCD screen, in the middle of the Cisco WVC210 camera's front panel. It has a range of approximately 6 feet (2 meters), depending on environmental conditions.

Camera LEDs

Four LEDs let you know how the camera is functioning.

LED	Color	Description
Power	Amber	The POWER LED lights up when the camera is powered on. It flashes for about 10-15 seconds while the camera is initializing.
Activity	Green	The ACTIVITY LED flashes when there is activity.
Ethernet	Green	The ETHERNET LED lights up when there is a connection to a wired network. It flashes when data is transmitted to or received from the wired network.
Wireless	Green	The WIRELESS LED lights up when there is a connection to a wireless network. It flashes when data is transmitted to or received from the wireless network.

Bottom Panel

The LAN port, input jacks, and the reset button are located on the bottom panel of the camera. The following illustration shows the bottom panel of the Cisco WVC210 camera.

The following features are found on the bottom of the camera.

Port, Jack, or Button	Description
POWER	The Power port is where you connect the 5V power adapter.
SPKR OUT	Use the SPKR OUT input to connect with the 3.5 mm input jack of your optional external speaker. The speaker needs to be a PC, or a powered speaker.
MIC IN	Use the MIC IN input to connect with the 3.5 mm input jack of your optional external microphone.
LAN	The LAN port is where you connect your Ethernet cable. Use a Cat5E (or better) network cable.
RESET	The reset button can be accessed with a straightened paper clip or similar object. The reset button has two functions: • **Restore Factory Defaults**—To restore the factory default settings, press the **Reset** button for more than 3 seconds. When you let go of the button, the LEDs on the front of the camera will flash and then return to a normal state when the camera is ready. • **Set Static IP Address**—By default the camera is set to receive an IP address from a DHCP server. If you do not have a DHCP server on your network, you can set a static IP address by pressing the **Reset** button on the camera for less than 3 seconds. A default IP address of 192.168.1.99 will be assigned to the camera. This information also can set in the Setup Wizard and in the web-based configuration utility for the camera. Tips when using the default IP address: • If the camera is connected directly to your computer, then your computer needs to be on the same subnet as the default IP address in order to access the configuration utility. • If you are using a router, you may be on a different subnet such as 192.168.2.1.

Connecting the Cisco WVC210 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 first.

- Choose a location that provides adequate coverage of the area to be monitored.

- If using the microphone in the camera, note that the cameras are designed to pick up audio from a distance (unlike a web camera that you would place near you.)

- If using motion detection, consider potential sources of 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 yard (one meter) away.

Cisco Wireless Network

The illustration provides an example of a Cisco wireless network.
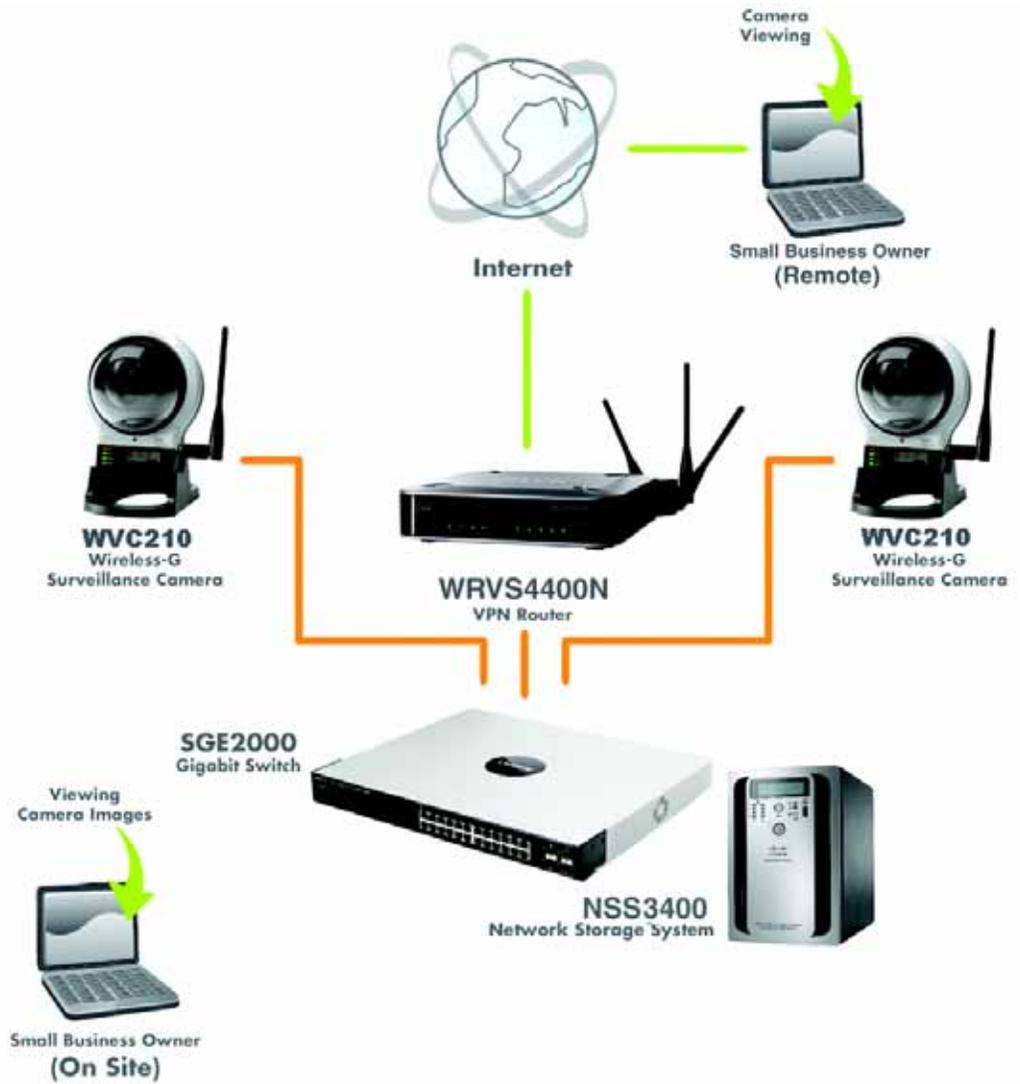
Connecting to a Wired Network for Setup

You must perform the initial configuration of the Cisco WVC210 camera from a personal computer connected to the camera using a wired connection to the LAN port. The initial configuration cannot be performed over a wireless connection.

STEP 1   Connect the antenna to the antenna connector on the camera.

STEP 2   (Optional) The Cisco WVC210 camera includes a camera desktop stand. Set the bottom of the camera into the stand.

STEP 3   Place the camera, and adjust its aim accordingly.

STEP 4   Connect the included Ethernet network cable to the network router or switch.
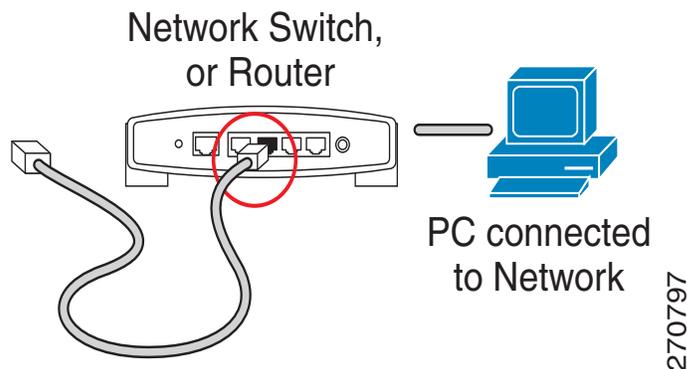
STEP 5   Connect the other end of the cable to the Cisco WVC210 camera's LAN port.

Camera

Network Switch
or Router

270798
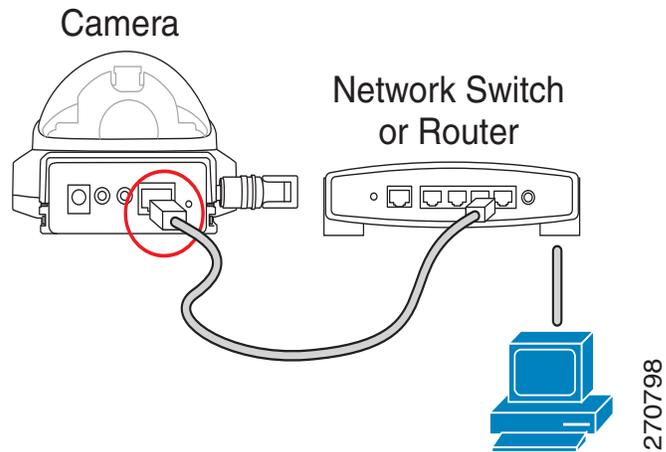
STEP 6   Connect the included power adapter to the camera's Power port. Insert the other end into a standard electrical outlet.

Outlet

Camera

Power

270799
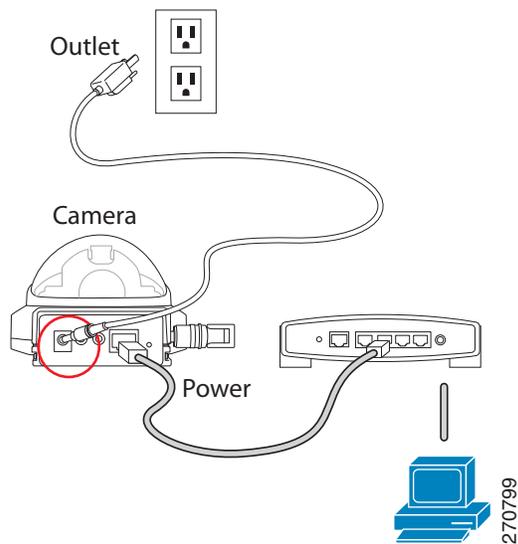
STEP 7   Verify that the camera LEDs are lit.

Changing Your Network Mode

After the initial configuration, you can use the camera in one of two modes: wired or wireless. You cannot use the camera in both modes simultaneously.

When you move the camera from a wired network to a wireless network, or vice versa, you must power off the camera before connecting to the new network. Unplugging the Ethernet cable does not automatically switch the camera to wireless mode.

Wired to Wireless

To move the camera from a wired network to a wireless network, follow these instructions:

STEP 1   Unplug the power adapter from the camera.

STEP 2   Unplug the Ethernet network cable from the camera.

STEP 3   Re-connect the power adapter to the Power port on the camera. The camera's Ready LED flashes while the camera is initializing. The camera is ready for use when the Ready and Wireless LEDs are solidly lit.

Wireless to Wired

To move the camera from a wireless network to a wired network, follow these instructions:

STEP 1   Unplug the power adapter from the camera.

STEP 2   Connect the Ethernet network cable to your PC, router, or switch.

STEP 3   Connect the other end of the cable to the Ethernet port on the camera.

STEP 4   Re-connect the power adapter to the Power port on the camera. The camera's Ready LED flashes while the camera is initializing. The camera is ready for use when the Ready and LAN LEDs are solidly lit.

NOTE   You must perform the initial configuration of the Cisco WVC210 camera from a personal computer connected to the camera using a wired connection to the LAN port. The initial configuration cannot be performed over a wireless connection.

Audio Options

If you want to use your own microphone instead of the camera's built-in microphone, then follow these instructions. The microphone you use must have its own source of power, like your computer speakers.

STEP 1   Connect the 3.5 mm input jack of your microphone to the MIC IN port on the camera's bottom panel. The built-in microphone will automatically be disabled.

STEP 2   Place the external microphone in an appropriate location.

If you want to use an optional external speaker with the camera, then follow these instructions:

STEP 1   Connect the 3.5mm jack of your speaker to the SPKR OUT port on the camera's bottom panel.

STEP 2   Place the external speaker in an appropriate location.

Installing the Cisco WVC210 Internet Camera Software

The product CD for your camera includes a Setup Wizard software program, which helps to set up your Cisco WVC210 Internet camera. There are two ways to use the Wizard:

1. You can launch the Wizard from the CD without installing the software on the PC. 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.

This chapter contains the following sections:

- **Configuring Basic Camera Settings, page 21**

- **Configuring the Network Settings, page 22**

Please note that Microsoft Internet Explorer (IE) is the official supported browser for the Cisco WVC210 Internet camera.

Configuring Basic Camera Settings

NOTE If the Setup Wizard does not find your Cisco WVC210 camera, enable UPnP on your computer. See instructions for enabling Universal Plug and Play (UPnP) in **Appendix A, "Troubleshooting."**

STEP 1 Insert the Setup CD into your CD-ROM drive. If the CD doesn't run automatically, go to **My Computer** and click on your CD-ROM drive.

STEP 2 The Welcome window appears. Click **Start**.

STEP 3 The License Agreement window appears. Click **Next** if you agree and wish to proceed.

The Wizard searches your network for your camera and displays a list of all cameras it found.

STEP 4 Highlight the camera you wish to configure and click **Next** to continue.

If the camera you want is not displayed in the Selection box, enable UPnP on your computer as described in **Appendix A, "Troubleshooting,"** and click **Search Again**.

STEP 5 The default user name and password is **admin**. Type **admin** in lowercase letters, in the Administrator Name and Administrator Password fields, and then click **OK**.

NOTE For security purposes, it is highly recommended that you change the default name and password using the camera's web-based utility at a later time.

STEP 6 On the Basic Settings window, configure the following settings as desired:

- **Camera Name**—Enter a unique name for the camera, up to 16 characters in length. Unique names are helpful when you are using multiple cameras on the same network.

- **Description**—Enter a description, up to 32 characters in length, with additional information, such as the location of the camera.

- **Time Zone**—Select the time zone that corresponds with the camera's location.

- **Date**—Enter the current date This sets the camera's calendar date and the information is used when the date stamp is referenced in the image captures.

- **Time**—Enter the current time. This sets the camera's clock and is used when the time stamp is referenced in the image captures.

You have now finished identifying the camera and configuring the basic settings. To continue configuring the camera, click **Next**.

Configuring the Network Settings

Follow these steps to configure the network settings of the camera. These steps continue from the previous section.

STEP 1 In the Network Settings window, if you want to assign the IP address, then select Static IP address, otherwise leave the default setting, Obtain An IP Address Automatically (DHCP). Click **Next** to continue.

STEP 2 The current settings of the camera are displayed. Make any changes as needed for your network, and then click **Next** to continue.

STEP 3 A confirmation window appears. Click **Next** to confirm the settings, or **Back** to go back and make any changes.

STEP 4 In the confirmation window, click **OK** to continue or click **Cancel** to close the window. If you click **Cancel**, you can then click **Back** and make changes.

Once **OK** is clicked, the new settings are saved.

STEP 5 A dialog box appears informing you that your configuration has been saved successfully. Click **OK** to continue.

STEP 6 Congratulations! Your camera is now configured. Click **Finish** to complete the process.

STEP 7   The Cisco WVC210 Wireless-G PTZ Internet Camera Home window launches.
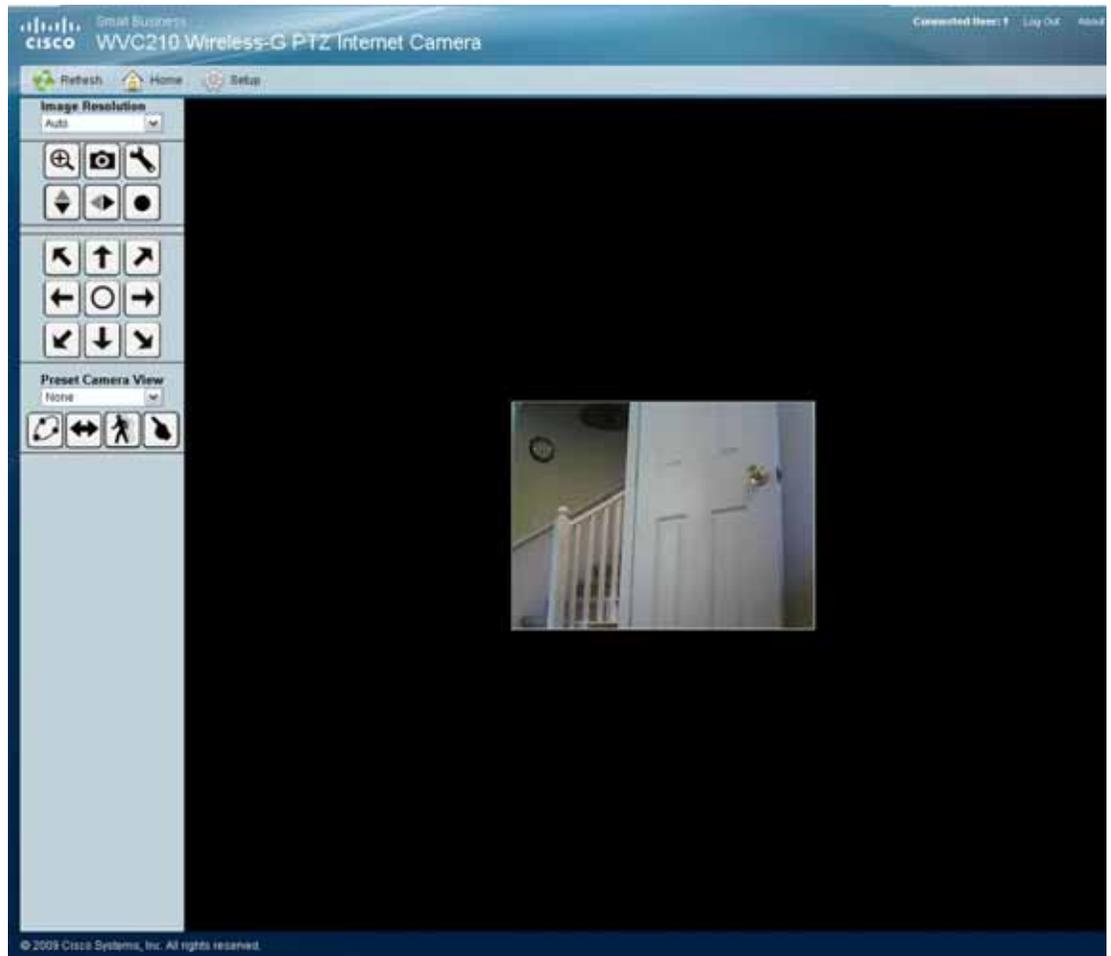
NOTE   Internet Explorer may prompt you to accept ActiveX to view video; follow the instructions to accept ActiveX.

The basic installation procedure is now complete. You may now proceed with **Chapter 8, "Configuring the Cisco WVC210 Internet Camera Software."**

Upgrading the Cisco WVC210 Internet Camera Firmware

The Cisco WVC210 Internet camera may not always ship with the most up-to-date firmware. You can update the camera's firmware through the web-based utility's **Maintenance** window.

NOTE Microsoft Internet Explorer (IE) is the official supported browser for the Cisco WVC210 Internet camera.

To access the web-based configuration utility, follow these steps:

STEP 1 Launch a web browser, such as Internet Explorer.

STEP 2 In the Address field, enter **192.168.1.99** and press **Enter**.

NOTE If you used the Setup Wizard to configure the IP address, use that same IP address in this step. Your camera's default IP Address is displayed in the LCD screen on the front of the camera.

The web-based utility login window appears.

STEP 3 If this is your first time accessing the web-based utility, follow these steps at the login window:

a. Enter **admin** in the User name field.

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

c. Click **OK**.

For security purposes, it is recommended that you later reset your password in the Administration > Users window.

To upgrade the camera firmware, follow these steps:

STEP 1 Click **Download Software** on the Cisco Small Business Video Surveillance Cameras page. Login is required.

STEP 2 Follow the online directions to download the appropriate firmware.

STEP 3 Launch the web-based configuration utility. See **Launching the Web-Based Configuration Utility, page 27**.

STEP 4 Click **Setup** in the toolbar.

STEP 5 Click **Administration > Maintenance** link in the navigation tree.

STEP 6 Click **Upgrade Firmware**.

STEP 7 Click **Browse** to find the extracted file, and then double-click the filename.

STEP 8 Click **Start Upgrade**, and follow the on-screen instructions. Click **Cancel** to cancel the firmware upgrade.

NOTE Cisco recommends that you upgrade the camera's firmware within your network; in other words, use a computer within the camera's local network. 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.

7

Using the Web-Based Configuration Utility

This section provides an overview of the Cisco WVC210 Internet camera's web-based utility software.

This chapter contains the following sections:

Please note that Microsoft Internet Explorer (IE) is the official supported browser for the Cisco WVC210 Internet camera.

Launching the Web-Based Configuration Utility

By default, the Cisco WVC210 Internet camera is set to receive an IP address from a DHCP server. If you do not have a DHCP server on your network, you can set a static IP address by pressing the **Reset** button on the camera for less than three seconds. A default IP address of 192.168.1.99 will be assigned to the camera.

To determine if you have a DHCP server on your network, consult your network administrator. If you do not have a DHCP server, access your camera through the default IP address.

To configure the Cisco WVC210 camera follow these steps to access the web-based configuration utility from your computer:

STEP 1 Launch a web browser, such as Internet Explorer.

STEP 2 In the Address field, enter **192.168.1.99** and press **Enter**. The web-based utility login window appears.

If you used the Setup Wizard to configure the IP address, use that same IP address in this step.

NOTE Your camera's default IP Address is displayed in the LCD screen on the front of the camera.

STEP 3 If this is your first time accessing the web-based utility, follow these steps at the login window:

a. Enter **admin** in the User name field.

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

c. Click **OK**.

For security purposes, it is recommended that you later reset your password in the Administration > Users window.

Home

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

This section describes the options available to you on the Home window.
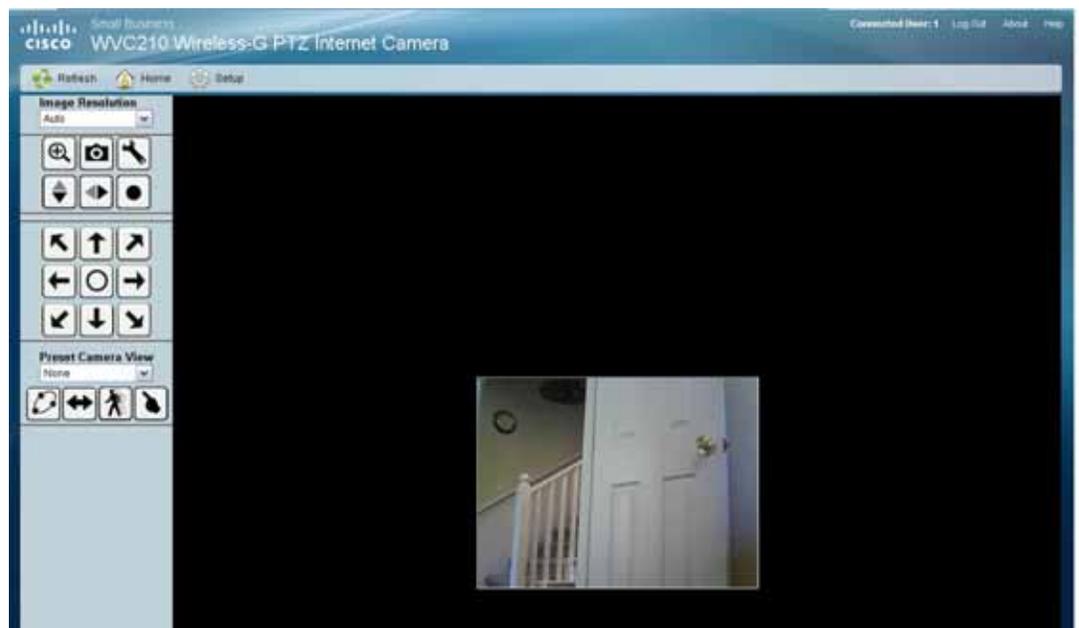
Refresh

Refreshes the display.

Setup

Provides most of the Cisco WVC210 Internet camera features. See **"Setup Options," on page 33** for more information.

Connected Users

Displays the number of users. The maximum number of users is 10.

Log Out

Allows you to log out of your camera session.

About

Describes the camera, including the current firmware version.

Help

The camera software includes detailed Help files for all configuration tasks. To view a Help page, click the Help link in the top right corner of the window. A new window appears with information about the task that you are currently viewing.

Video Options Panel

The **Video Options Panel** on the Home window is used to control the real-time view of your camera. The icons allow you to control the basic functions of the Cisco WVC210 camera.
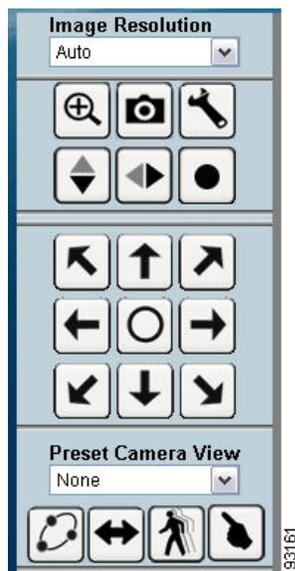
Icon	Description
Image Resolution	Use this drop-down list to select the desired video size. The options are Auto, 640 x 480, 320 x 240, 160 x 120. The default is **Auto** and lets the camera determine the resolution.
Zoom	Click zoom and then use your mouse to select the section you want to magnify. Click the icon again to disable the zoom feature.
Snapshot	Click to take a single JPEG picture snapshot of the video image and save it to a desired location on your computer.
Streaming Video Format	Set the video format to either MPEG-4 or MJPEG.
Flip Video	Flip the video image top to bottom.
Mirror Video	Mirror the video image left to right.

Icon	Description
Start/Stop Recording	Click the black icon to start recording, and click the red icon to stop recording. Consider the following:
	• The default location for saved recordings is \My Documents\Record.
	• Click **Browse** to choose another location to save your recordings.
	• Your folder selection is remembered in the registry. If that folder no longer exists the next time the camera is used, the default location is restored.
	• The file name is saved in .avi format by default, and the maximum length for the video file is 30 minutes. If the recording is longer than 30 minutes, a second file is created automatically.
	• The available disk space required is at least 750 MB.
PTZ Directional Movement	Allows you to incrementally adjust the camera in eight directions, and back to home (the icon that is displayed). Please note that there may be a short delay after a direction is clicked.
Preset Camera View	Select the preset area to patrol. See **Rotation Sequence, page 58** for more information on setting these positions.
Camera Patrol	Move the camera one time through the Preset positions.
Camera Auto Pan	Rotate the camera one time to the left, to the right, and then back to center.
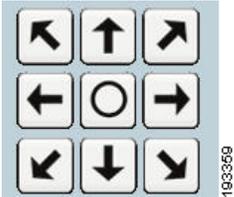
Icon	Description
Motion Detection	Click to move the camera to the previously defined Motion Detection area. Instructions on defining a motion detection area can be found in **"Applications > Motion Detection," on page 54**.
On-Image PT Control	Click in the video image and adjust/move the image.
Audio On **Audio Off**	When audio is enabled (**"Audio/Video," on page 45**), an icon is displayed on the Home window. You can then use the icons to turn audio on and off.
Speaker On **Speaker Off**	When the speaker is enabled (**"Audio/Video," on page 45**), an icon is displayed on the Home window. You can then use the icons to turn the speaker on and off.

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

Setup Options

To access the setup options for your Cisco WVC210 Internet camera, click **Setup** in the toolbar.

The login window appears:

Enter the default username (admin) and the default password (admin) and the Setup > Basic Settings window appears:
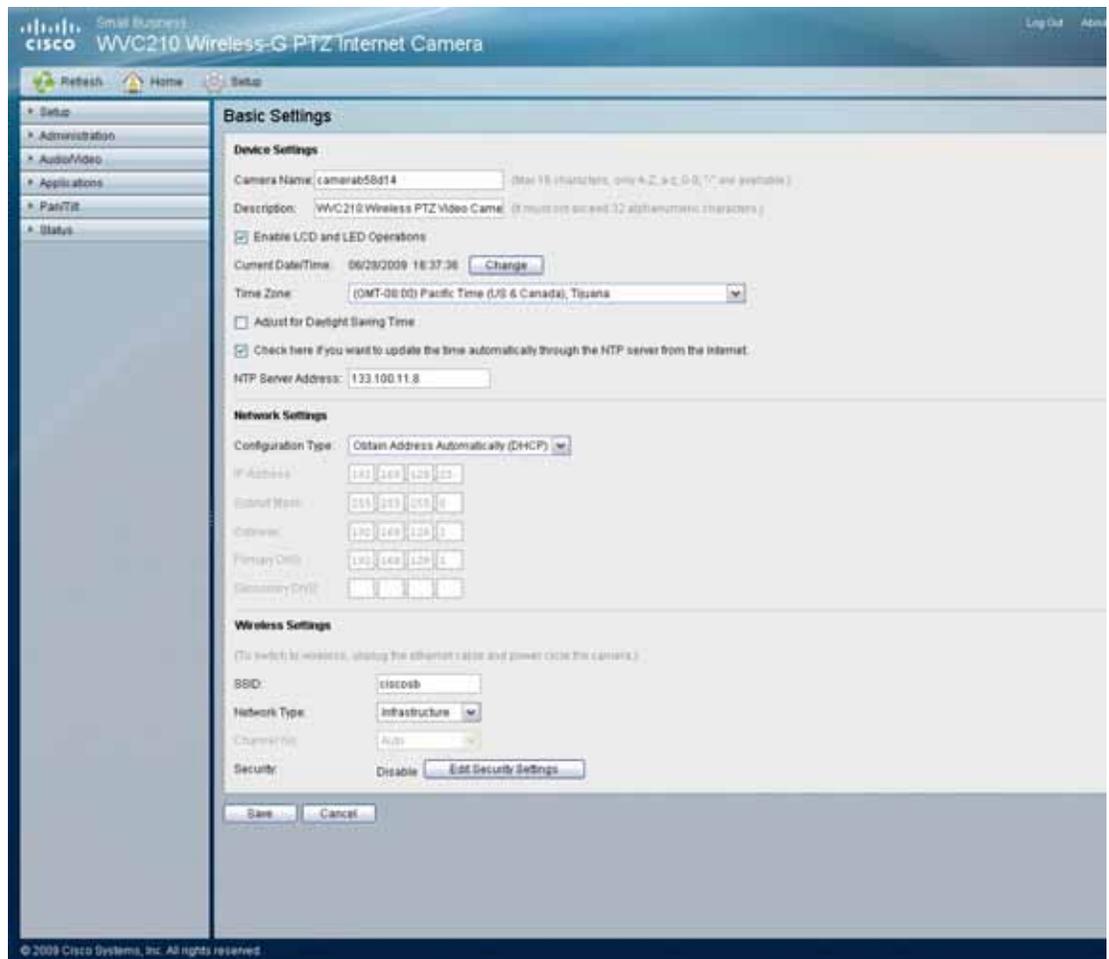
The following section, **Configuring the Cisco WVC210 Internet Camera Software, page 35** describes all of the options available in the navigation tree.

NOTE The inactivity timeout for the camera's web-based utility software is 5 minutes.

8

Configuring the Cisco WVC210 Internet Camera Software

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

This chapter contains the following sections:

Please note that Microsoft Internet Explorer (IE) is the official supported browser for the Cisco WVC210 Internet camera.

Setup > Basic Settings

The Setup > Basic Settings window has options for Device Settings, Network Settings, and Wireless Settings.

Device Settings

- **Camera Name**—Enter the preferred name for the camera. The camera name must not exceed 16 alphanumeric characters. By default, the last six digits of the camera name come from the last three bytes of the MAC address, but this can be overwritten.

- **Description**—Enter a description of your camera, such as the location of the camera. Entering a description will help you identify the camera. It must not exceed 32 alphanumeric characters. By default, your camera description is WVC210 Wireless PTZ Video Camera.

- **Enable LCD** and **LED Operations**—Enable to turn on the LCD or LED.

- **Current Date/Time**—Displays the current date and time. If it's not correct, click **Change** to modify the time settings.

NOTE To be able to change the current date and time, uncheck the box next to **Check here if you want to update the time automatically through the NTP Server on the Internet**.

Set Date/Time

- **PC's Date and Time**—Displays the current time of the PC connected to the web-based utility.

- **Camera Date and Time**—Displays the current time as configured on the camera.

- **Sync with PC**—Allows you to synchronize the camera to the clock on the PC connected to the web.based utility.

- **New Date**—Allows you to manually enter the date for the camera.

- **New Time**—Allows you to manually enter a new clock setting for the camera.

- **Set New Time**—Implement the new date and/or time setting.

- **Time Zone**—Choose the time zone for your location from the drop-down list.

- **Adjust for Daylight Saving Time**—Select this option if your location is currently using Daylight Saving Time. You must uncheck the Adjust for Daylight Saving Time check box manually when Daylight Saving Time ends in your time zone.

- **Check here if you want to update the time automatically through the NTP Server on the Internet**—Enable or disable the time server feature as required. If enabled, the camera will contact a network time server at regular intervals and update its internal timer.

- **NTP Server Address**—Enter the address of the NTP Server.

NOTE If connecting to a router, it may be necessary to enable port forwarding. See **"Configuring Port Forwarding" on page 67**.

Network Settings

Configuration Type

- **Obtain An IP Address Automatically**—The camera defaults to this option, allowing a DHCP server on your network to automatically assign the camera an IP address.

- **Fixed IP Address**—Use this option to assign a fixed (static) IP address to the camera. Assign an IP address that is unique to your local network. When using a fixed IP address, you must configure the IP Address, Subnet Mask, Gateway, and DNS.

- **IP Address**—The IP address assigned to the camera.

- **Subnet Mask**—The Subnet Mask assigned to the camera.

- **Gateway**—IP address of the gateway router between this device and management stations that exist on other network segments.

- **Primary DNS**—The IP address of your ISP's primary server, which translates the names of websites into IP addresses.

- **Secondary DNS**—The IP address of your ISP's secondary server, which translates the names of websites into IP addresses.

Wireless Settings

- **SSID**—Enter the network's SSID or network name here. The default is **ciscosb**.

- **Network Type**—Select the network's mode. Choices are: **Infrastructure** or **Ad-hoc**.

- **Channel No**—If the camera is set to **Ad-hoc** mode, select the appropriate channel from the list provided to correspond with your network settings. All devices in your wireless network must use the same channel in order to function correctly. In **Infrastructure** mode, you cannot specify a channel setting on the Wireless-G Internet Camera. It is automatically configured to match the device your camera is connected to.

- **Security**—Click **Edit Security Settings** to display the Wireless Security window.

- **Security Mode**—Select the appropriate option based on your wireless network configuration. Options are: Disable, WEP, WPA Personal, WPA2 Personal, WPA/WPA2 Enterprise.

Disable

This option implements no security on your wireless network. Data is not encrypted before transmission.

WEP

WEP is a basic encryption method, which is not as secure as later methods such as WPA. WEP stands for Wired Equivalent Privacy.

- **TX Key**—Select the number of the key used on the wireless network.

- **WEP Encryption**—Select the appropriate option for key length based on your network settings.

- **Passphrase**—Type in the passphrase used to generate WEP keys on your network and click **Generate**.

- **Key 1-4**—Key values can be entered in manually or generated from a passphrase.

- **Authentication**—Select the appropriate authentication type used on the wireless network.

WPA Personal

This method offers two encryption methods, TKIP (default) and AES with dynamic encryption keys. Select the type of encryption method you want to use, TKIP or AES. Enter the Shared Key, which can have 8 to 63 characters. Then enter the Key Renewal Timeout, which instructs the device how often it should change the encryption keys.

WPA2 Personal

This method always set to AES encryption methods, with dynamic encryption keys. Enter the Shared Key, which can have 8 to 63 characters. Then enter the Key Renewal Timeout, which instructs the device how often it should change the encryption keys.

WPA/WPA2 Enterprise

WPA2 Enterprise requires some advanced expertise because it involves setting up a RADIUS server for authentication and, in some cases, creation of certificates for both the RADIUS server and the camera.

If you are using WPA/WPA2 Enterprise security, you will need to upload security certificates to the camera. Certificates must be in the following format:

- Root certificate: DER encoded binary x.509 (CER/PEM)

- User certificate: Personal Information Exchange (PKCS#12(.PFX))

In WPA/WPA2 Enterprise, you can choose your protocol type. Select between EAP-TLS and EAP-TTLS.

EAP-TLS

With EAP-TLS you enter the User ID and Password for the RADIUS server and choose where the camera should check for the Server and User certificate.

- **User ID**—The user ID used to login to your RADIUS server.

- **Root CA**—A root certificate is an unsigned public key certificate, or a self-signed certificate, which implies that you trust your browser's publisher to include correct root certificates, and in turn the certificate authorities it trusts, and anyone to whom the CA may have issued a certificate-issuing-certificate, to faithfully authenticate the users of all their certificates.

- **User CA**—A user certificate is a signed private key certificate, which implies that you trust your browser's publisher to include correct user certificates, and in turn the certificate authorities it trusts, and only user to

whom the CA may have issued a certificate-issuing-certificate, to faithfully authenticate the users of all their certificates.

- **Password**—The login to the RADIUS server, and must match the key stored on the RADIUS server.

EAP-TTLS

With EAP-TTLS you choose the authentication protocol (MS-CHAP V2, MS-CHAP, PAP, EAP-MD5, and EAP-GTC) to transfer the CA to the RADIUS server. You will also enter the User ID, Password, and anonymous ID for the RADIUS server and choose where the camera should check for the server certificate.

- **Process Method**—Choose an authentication method (MS-CHAP, MS-CHAP v2, PAP, EAP-MD5, and EAP-GTC) as required to handle the processing and transmission of the CA to your RADIUS server.

- **User ID**—The user ID used to login to your RADIUS server.

- **Password**—The login to the RADIUS server.

- **Anonymous ID**—The unsigned public ID used for login to your RADIUS server.

- **Root CA**—A root certificate is an unsigned public key certificate, or a self-signed certificate, which implies that you trust your browser's publisher to include correct root certificates, and in turn the certificate authorities it trusts, and anyone to whom the CA may have issued a certificate-issuing-certificate, to faithfully authenticate the users of all their certificates.

Setup > Advance Settings

The Setup > Advance Settings window has options for RTSP/RTP and Other.

RTSP/RTP

Real Time Streaming Protocol (RTSP) is a standard for connected client(s) to control streaming data (MPEG-4) over the World Wide Web. Real-Time Transport Protocol (RTP) is an Internet protocol used for transmitting single real-time multimedia data such as audio and video to a select group of connected clients. RTSP uses RTP to format packets of multimedia content.

- **RTSP Port**—Enter the RTSP Port number (between 1024 to 65535) in the field provided. The default RTSP port is **554**.

- **RTP Data Port**—The camera's data port number has been pre-configured and can be used for multicasting. It does not normally need to be re-configured. If a port number does need to be changed, please contact your network administrator. If a change is necessary, enter the data port number (1024 to 65494, even numbers only) in the field provided. The default RTP port is **5000**.

- **Max RTP Data Packet**—Allows you to define the maximum size of the RTP data packets. The length can be between 400 to 1400 bytes. The default value is **1400** bytes.

- **Enable Multicast**—The camera's video and audio IP addresses have been pre-configured and can be used for multicasting. Normally these settings do not need to be reconfigured. If an address does need to be changed, please contact your network administrator and refer to the camera's online Help.

HTTP

- **HTTP Port**—The default port of 80 is the port your web browser uses to access your camera. If a different port is entered, HTTP connections (from your web browser, viewer and recorder utility) can use that port instead of the standard HTTP port 80 to access the camera. The supported port numbers are in the range of 1024 to 65534. If you change the port number, when you open the URL to the camera, you now must specify the port number, for example: http://192.168.128.23:8002. You must specify the port for either LAN or WAN connections.

Discovery Settings

*   **Enable UPnP (Discover Only)**—If enabled, the camera will broadcast its availability through Universal Plug and Play protocol. UPnP compatible systems such as Windows XP will then be able to detect the presence of the camera. For instructions on setting UPnP on your system, see **"Questions and Answers," on page 71**.

*   **Enable Bonjour**—Enabled by default. If enabled, the Cisco WVC210 IP Camera is accessible through a Bonjour-enabled browser, such as Microsoft Internet Explorer with a Bonjour plug-in, or the Apple Mac Safari browser. By using Bonjour, you can easily find and click on Bonjour-enabled items on your network.

QoS

*   **Enable QoS Mode**—Check to enable Quality of Service (QoS) for media streams.

*   **DSCP**—If QoS is enabled, please enter the Differentiated Services Code Point (DSCP) to be used on processing QoS packets. The default value is 12.

Administration > Users Settings

The Administration > Users Settings window gives options for Authentication, Administrator, and User List.

Authentication

- **Authentication**—Enables an authentication check when the box is checked. The user will need to login for all activities, even to see video on Home window. If this box is not checked, the user can view video, but will need to login to go to any of the setup pages.

Administrator

- **Admin**—The default administrator name and password should be changed for security purposes. To change the administrator name and password, enter the desired name and password (enter the password twice). Click **Change** to apply the change. Spaces, punctuation, and special characters are not supported. The administrator name is case sensitive.

User List

- **User ID**—The User ID cannot be modified.

- **User Name**—Enter the desired user name. Spaces, punctuation, and special characters are not supported. The name is case sensitive. The maximum length of a user name is 16 characters.

- **Password**—Enter the desired password in this field. The maximum length of a password is 16 characters.

- **Confirm Password**—Retype the password in this field.

- **Pan/Tilt**—Click to allow user control PAN and TILT function.

- **Setup**—Click to authorize user control as an administrator.

Enter the information in the fields and click **Add** to add or modify a User ID. After a user has been added, you can delete a user by selecting **Delete**. Select **Save** to save the user configuration.

Administration > Maintenance

The Administration > Maintenance window gives options for Restore Factory Defaults, Restart, Firmware Upgrade, and Configuration.

Restore Factory Defaults

- **Restore Defaults**—Restores the camera to the factory default settings.

Restart

- **Restart**—Restarts the camera.

Firmware Upgrade

- **Upgrade Firmware**—Updates the camera's firmware; see **Chapter 6, "Upgrading the Cisco WVC210 Internet Camera Firmware."**

Configuration

- **Save**—Use this option to save a configuration file containing all of the current camera management settings.

- **Browse**—Locate a previously saved configuration file.

- **Upload**—Upload a previously saved configuration file into the camera.

Audio/Video

Clicking on the Audio/Video window shows options for Video Settings and Audio Settings.

Audio/Video > Video Settings

NOTE Higher video quality settings and higher frame rate settings require more bandwidth.

MPEG-4 Settings

MPEG is the designation for a group of audio and video coding standards and related technology agreed upon by the ISO/IEC. The primary uses for the MPEG-4 standard are web (streaming media) and CD distribution, and broadcast television.

- **Resolution**—Select the desired video resolution setting. The default resolution is set to **320x240**.

- **Video Quality Control**—Choose one of the following:

  - **Fixed Bit Rate**—Select the desired fix bit rate. The default bit rate is set to **256 Kbps**.

  - **Fix Quality**—Select the desired image quality. The default image quality is set to **Normal**.

- **Max Frame Rate**—Select the desired maximum frame rate. The default maximum frame rate is set to **30 fps**.

MJPEG Settings

MJPEG (Motion JPEG) is a video codec where each video field (frame) is separately compressed into a JPEG image.

- **Resolution**—Select the desired video resolution format. The default resolution is set to **320x240**.

- **Fixed Quality**—Select the desired video quality. The default image quality is set to **Normal**.

- **Frame Rate Control**—Select the desired frame rate. The default frame rate is set to **30**.

Mobile Settings

- **Enable Mobile Streaming**—Enable streaming video for the mobile devices by selecting this option.

    - **Resolution**—Shows the default resolution of **160x120**.

    - **Video Quality Control**—Choose from one of the following options:

        - **Fixed Bit Rate**—Select the desired fix bit rate. The default bit rate is set to **32 Kbps**.

        - **Fix Quality**—Select the desired image quality. The default image quality is set to **Normal**.

    - **Max Frame Rate**—Select the desired maximum frame rate. The default maximum frame rate is set to **15 fps**.

    - **Access Code**—Entered at the end of a URL to access a live video camera feed through another source, for example, a cell phone connection:

        ```
        rtsp://<IP Address>/access_code
        ```

Adjustments

- **Power Line Frequency**—Select the power frequency (50Hz or 60Hz) used in your region to improve the picture quality under fluorescent lighting.

- **Color Balance**—Select the desired option to match your environment to obtain a better image. Options are: auto, indoor (incandescent), fluorescent (white and yellow light), outdoor, or black and white.

- **Exposure**—Adjust the exposure to obtain a better image. For example, if the camera is facing a bright light, the image may be too dark. In this case, you should increase the exposure. You can select an exposure value between -3 and 3.

- **Sharpness**—Adjust the sharpness to obtain a better image. You can select a sharpness value between -3 and 3.

Video Options

- **Flip Image**—Enable this feature if you want to rotate the image 180° on the vertical axis.

- **Mirror Image**—Enable this feature if you want to rotate the image 180° on the horizontal axis.

- **Enable Time Stamp**—Enable this feature by checking the check box if you want to display a time stamp on your video.

- **Enable Text Display**—Enable this feature by checking the check box, if you want to display text on the video. The text can be up to 20 characters in length. This feature is often used to identify the camera location when multiple cameras are installed.

Audio/Video > Audio Settings

Audio is disabled by default.

- **Enable Audio**—Enable audio by checking the check box. When audio is enabled, an icon is displayed on the Home window and audio is picked up through the camera. You can then use the icons to turn audio on and off.

Audio On

Audio Off

Audio Mode Settings	Function
Simplex—Talk Only	Enables the speaker jack.
Simplex—Listen Only	Enables the microphone jack.
Half Duplex—Talk or Listen (Not simultaneously)	Enables the speaker and microphone jack but only one can be used at a time.
Full Duplex—Talk and Listen (Can be simultaneously)	Enables the speaker and microphone jack and both can be used simultaneously.

- **Audio Type**—When the microphone is enabled, this drop-down list allows you to select the audio compression type.

Compression Settings	Description
G.711 A-Law	A standard compression algorithm that uses 64 kbps of bandwidth and is primarily used in Europe.
G.711 u-Law	A standard compression algorithm that uses 64 kbps of bandwidth and is primarily used in North America and Japan.

- **Enable Speaker**—Check the box to activate an optional external speaker. When the speaker is enabled, an icon is displayed on the Home window. You can then use the icons to turn the speaker on and off.

Speaker On

Speaker Off

Applications > Mail

Clicking on the Applications > Mail window shows options for Primary and Secondary SMTP Servers and E-mail Setup.

NOTE Only one SMTP server is used, even if both the primary and secondary SMTP servers are enabled. The secondary SMTP server is used if the camera can't connect to the primary server.

Primary SMTP Server

- **Enable Primary SMTP**—Check the box to enable an SMTP Server. This is disabled by default.

- **SMTP Mail Server**—Enter the address of the Simple Mail Transport Protocol (SMTP) server to be used to send e-mail.

- **Port**—Enter the port number for the mail server. The default is **25**.

- **Authentication**—Check the box if your mail server requires authentication and enter the following options:

  - **Account Name**—Enter the account name to be used on the e-mail server.

  - **Password**—Enter the password associated with the account name.

- **Test SMTP Server**—Sends a test e-mail to verify the connection with the SMTP Mail server.

Secondary SMTP

- **Enable Secondary SMTP**—Check the box to upload to the Secondary SMTP server if the camera can not connect to the primary SMTP server.

- **SMTP Mail Server**—Enter the address of the SMTP server to be used to send e-mail.

- **Port**—Enter the port number for the mail server. The default is **25**.

- **Authentication**—Check the box if your mail server requires authentication and enter the following options:

  - **Account Name**—Enter the account name to be used on the e-mail server.

      - **Password**—Enter the password associated with the account name.

E-mail Setup

- **Send To**—Enter at least one (1) e-mail address; the 2nd and 3rd addresses are optional. The e-mail alert will be sent to the e-mail address or addresses specified here.

- **Show "From" as**—Enter the e-mail address to be shown in the From field when the e-mail is received.

- **Subject**—Enter the desired text to be shown as the subject for the e-mail when it is received. The maximum field length is 48 characters.

NOTE The Cisco WVC210 camera does not support Secure Sockets Layer (SSL) protocols used by many e-mail providers, such as Gmail. Therefore you will not be able to use Simple Mail Transport Protocol (SMTP) Mail servers like Gmail that require SSL encryption. You can only use e-mail providers that do not require SSL encryption. Please contact your e-mail provider if you are not sure whether your SMTP server uses SSL encryption.

Applications > FTP

Clicking on the Applications > FTP window shows options for Primary and Secondary FTP.

NOTE Only one FTP server is used, even if both the primary and secondary FTP servers are enabled. The secondary FTP server is used if the camera can't connect to the primary server.

Primary FTP

- **Enable Primary FTP**—Check the box to enable the FTP server. This is disabled by default.

- **FTP Server**—Enter the address of the primary FTP server.

- **Port**—Enter the port number of the FTP Server. The default is 21.

- **Login Name**—Enter the login name associated with the specified primary FTP server.

- **Password**—Enter the password associated with the login name for the primary FTP server.

- **Enable Passive Mode**—Check the box to enable the passive mode feature. Passive mode is a more secure form of data transfer. The use of passive mode FTP ensures all data flow initiation comes from inside the network rather than from the outside.

- **File Path Name**—Enter the desired file path name on the primary FTP server.

Secondary FTP

- **Enable Secondary FTP**—Enable this option to allow the camera to connect to a secondary FTP server if the primary FTP server is not available.

- **FTP Server**—Enter the address of the secondary FTP server.

- **Login Name**—Enter the login name associated with the secondary FTP server.

- **Password**—Enter the password associated with the login name for the secondary FTP server.

- **Enable Passive Mode**—Check the box to enable the Passive mode feature.

- **File Path Name**—Enter the desired file path name on the secondary FTP server.

Applications > SMB/CIFS

The Applications > SMB/CIFS window shows options for SMB/CIFS. SMB/CIFS allows the camera to record directly into a Network Attached Storage (NAS) device. There is no need to record to a computer and keep a computer active all the time.

- **Enable SMB/CIFS Recording**—When enabled, provides seamless file recording and uploading to a NAS device. The TCP/IP protocol installed on the NAS device is used for file transfer.

- **SMB/CIFS Server**—Enter the server hostname or IP address of your NAS device (SMB/CIFS host server).

- **Login Name**—Enter your login name for the NAS device.

- **Password**—Enter your password for the NAS device.

- **Upload Path**—Enter the folder name to upload video to your NAS device (SMB/CIFS host server).

- **Maximum Size of Each File (MB)**—Enter the maximum upload size of each file to upload to the NAS device. The default is 10 MB.

- **Enable adding timestamp to files**—Enabled by default. A timestamp is added to each recorded file and there will be multiple recorded files. Older files will not be over-written, so the size of your recording continuously grows. If disabled, the first video image is timestamped; any images saved thereafter are not timestamped.

Applications > Motion Detection

The Applications > Motion Detection window shows options for Event and Pan/Tilt.

Event

NOTE Complete the Mail or FTP sections prior to enabling alerts.

- **Enable E-mail Alert**—If enabled, e-mail alert with attachments are sent when motion is detected.

- **Enable FTP Alert**—If enabled, FTP alert with attachments are sent when motion is detected.

- **Enable SMB/CIFS Alert**—If enabled, connects to the SMB/CIFS Server when motion is detected.

  - **SMB/CIFS Server**—Enter the server hostname or IP address of your NAS device (SMB/CIFS host server).

  - **File Path**—Enter the folder name to upload video to your NAS device (SMB/CIFS host server).

  - **Login Name**—Enter your login name for the NAS device.

  - **Password**—Enter your password for the NAS device.

Checking either alert box will display options for the attachment.

- **Interval**—Defaults to two minutes before detecting the next event For no delay, choose 0.

- **Attachment Type**—JPEG Image or Video.

- **Frame Rate**—Defaults to 1 fps.

- **Pre-Capture Length**—Defaults to 0 seconds. It is definable from 0 to 4 seconds.

- **Post Capture Length**—Defaults to 1 second.

Pan/Tilt

When Motion Detection is used in conjunction with pan and tilt, the results may not be as desired. For example, if you set motion detection for a doorway and then pan and tilt to a different location, the motion detection may now be pointed at the sky or the floor. It is recommended to disable pan and tilt when motion detection is enabled; however, three options are available:

- Enable Motion Detection in all positions.

- Disable Pan/Tilt while Motion Detection is enabled. (Recommended)

- Allow Motion Detection only in the set motion detection zone (ignore zones outside of set area). If you move the position of the camera (by panning or tilting) then motion detection is disabled.

- Check the box to set the idle time for motion detection position. One minute is the default.

- **Set Area & Sensitivity**—Click to enter the motion detection sub-window. You can set the area or areas of the video image to be examined, and adjust the sensitivity of detection for each area.

NOTE Motion detection can be triggered by rapid changes in lighting conditions, as well as by moving objects. For this reason, it should only be used indoors.

Applications > DDNS Settings

The Applications > DDNS window contains DDNS Settings.

- **Enable DDNS**—Enables Dynamic Domain Name Service (DDNS). When used with a DDNS service provider, you can access your camera over the Internet using a domain name instead of an IP address.

- **Service Provider**—Select your service provider. If you do not have an account, you can select a service provider and click **Web Site**.

- **Host Name**—Enter the host name (Domain Name) allocated to you by the DDNS Server provider.

- **Account**—Enter the login name for the DDNS account.

- **Password**—Enter the password for the DDNS account.

- **Check WAN IP Address**—Allows you to pick how often the device should check to see if the IP address has changed. If the IP address has changed, the DDNS Server will be notified.

- **Starting at**—Allows you set when to start checking if the IP address has changed.

NOTE To complete the DDNS Service setup, port forwarding needs to be configured on your router. See **"Configuring Port Forwarding" on page 67**.

Pan/Tilt Settings

The Pan/Tilt Settings window shows the Set Preset, Pan/Tilt Control, and Rotation Sequence settings for the camera.
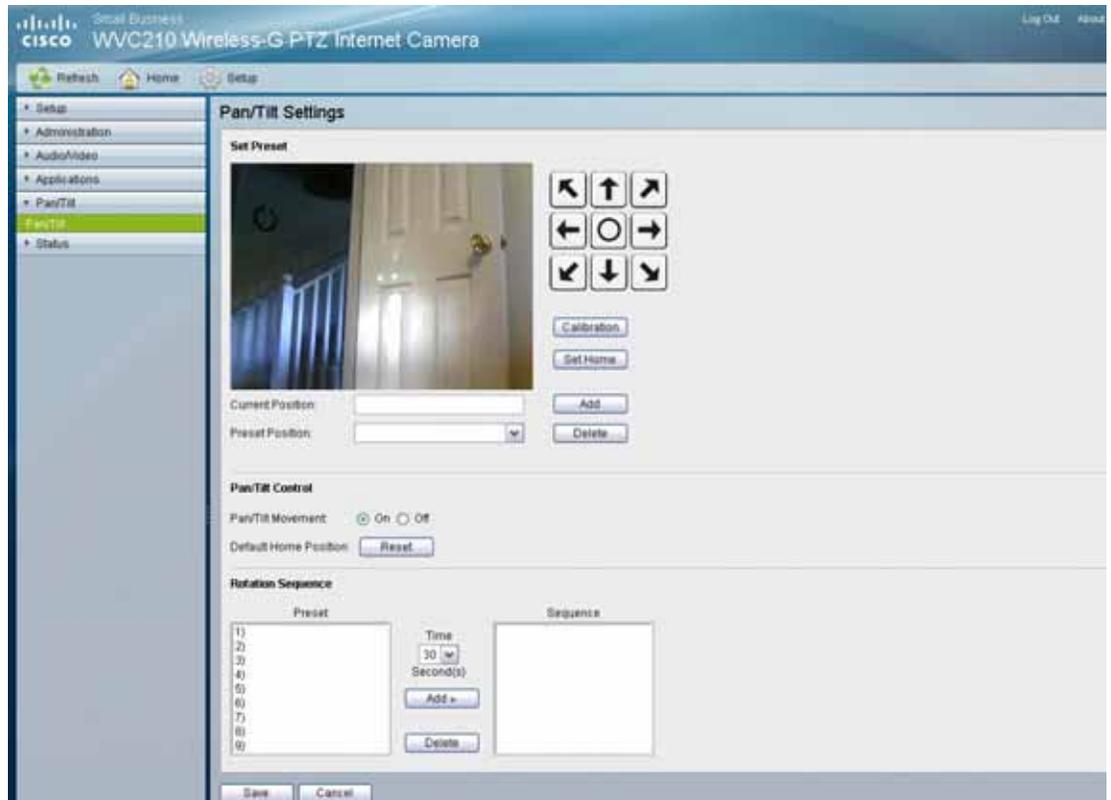
Set Preset

- **Set Positions**—Set the desired position through adjusting the control panel.

- **Calibration**—Reset the calibration of Pan/Tilt area.

- **Set Home**—Sets the desired Home position.

- **Current Position**—Name the current desired position and then click **Add** to add into the preset list. You can add up to nine preset points.

- **Preset Position**—Use to delete a preset position. Select the preset position you don't need and then click **Delete**.

Pan/Tilt Control

- **Pan/Tilt Movement**—Check **On** if you want to use the Pan/Tilt Movement feature.

- **Default Home Position**—Click to reset to the default home position.

Rotation Sequence

- **Rotation Sequence Window**—This feature determines how the camera will move when it is set to Rotate. You can set a number of Preset Positions; the camera will go to the first position, then move through the list of preset positions until it is finished. The camera will stop at the last position in the list.

  - To create the Preset Sequence, select the desired Preset Position in the left column, and click **Add >>**. Repeat until the desired sequence is complete. Note that you can add the same Preset Position more than once; this can be used to make the camera stay longer at one position.

  - To delete a position from the Sequence, select the desired position and click **Delete**.

- **Time**—Determines how long the camera will stay at each position while executing the sequence. Set this to the desired value.

Status

The Status window shows options for System, Image, Network, Wireless, and Syslog.

System Status

- **Firmware Version**—Version of the firmware currently installed.

- **MAC Address**—Displays the MAC address of the camera.

- **Camera Name**—Displays the name of the camera, as defined on the Basic > Device Settings window. By default, the last six digits of the camera name come from the last three bytes of the MAC address.

- **Description**—Displays the description of the camera, as defined on the Basic > Device Settings window.

- **Date/Time**—Displays the current date/time as configured on the camera.

Image Status

- MPEG-4/MJPEG

    - **Resolution**—Displays the image size of the video stream.

    - **Image Quality**—Displays the image quality of the video stream.

    - **Frame Rate**—Displays the frame rate of the video stream.

Network Status

- **Network Type**— Displays the type of network the camera is connected to.

- **IP Address**— Displays the IP address assigned to the camera.

- **Subnet Mask**—Displays the subnet mask assigned to the camera.

- **Gateway**—Displays the IP address of the gateway used by the camera.

- **Primary DNS**—Displays the IP address of the primary Domain Name Server used by the camera.

- **Secondary DNS**—Displays the IP address of the secondary Domain Name Server used by the camera.

Wireless Status

- **SSID**—Displays the wireless network name (SSID) used by the camera.

- **Channel**—Displays the wireless channel used by the camera.

- **Security**—Indicates if wireless security is being used by the camera.

- **Signal Strength**—Shows the wireless signal strength.

Syslog

- **Syslog Server**—Check this to enable the Syslog server, and then enter the IP address of your Syslog server.

- **Log**—Displays the systems activities. Click **Clear Log** to erase all the entries in the System Log.

Sample Configurations for the Cisco WVC210 Internet Camera

Your Cisco WVC210 Internet camera is capable of many functions. The following are sample configurations for the most popular Cisco WVC210 camera settings:

Please note that Microsoft Internet Explorer (IE) is the official supported browser for the Cisco WVC210 Internet camera.

Configuring Instant Recording

To configure instant recording, follow these steps:

STEP 1 Click **Home** in the toolbar to go to the Cisco WVC210 Home window.

STEP 2 On the Home window, click **Start Recording** in the **Video Options Panel** (see **Video Options Panel, page 29** for more information).

Recording is enabled.

STEP 3 Click **Save** in the dialog box if you agree with the default location (\My Documents\Record). Otherwise, click **Browse** and choose another location.

STEP 4 Click **Stop Recording** when you want to stop recording.

Defining Preset Locations for Auto Patrol

To define preset positions for the camera patrol sequence, follow these steps:

STEP 1 Access the setup options for your Cisco WVC210 Internet camera by clicking **Setup**.

STEP 2 Log in as required.

STEP 3 Go to the Pan/Tilt window.

STEP 4 Use the PTZ Directional Movement arrows to set a preset position.

STEP 5 Name the position in the Current Position box.

STEP 6 Click **Add**. This position is now is your first preset position.

STEP 7 Continue to add more positions, up to 9.

STEP 8 When you are done setting preset positions, click **Save**.

Using Auto Patrol

Once your preset positions are set, you can use the Rotational Sequence window to set a patrol schedule. The camera will go to the first position, then move through the list of preset positions until it is finished. The camera will stop at the last position on the list.

To create the patrol sequence, follow these steps:

STEP 1 Access the setup options for your Cisco WVC210 Internet camera by clicking **Setup**.

STEP 2 Log in as required.

STEP 3 Go to the Pan/Tilt window.

STEP 4 Click a preset in the Rotational Sequence Window (1-9).

STEP 5 Set a time for the camera to stay in that position (options range from 5 -60 seconds).

STEP 6 Click **Add**. This position is now is the first in your rotational sequence.

STEP 7 Continue to add more positions; when you are done, click **Save**.

STEP 8 Return to the Home window.

STEP 9 Click the **Camera Patrol** icon to pan once through your preset locations.

Configuring E-Mail Alerts

When using motion detection, you may want to be advised by e-mail when something is detected. Configure your e-mail settings first, and then configure Motion Detection. See **Configuring Motion Detection, page 66**.

NOTE The Cisco WVC210 camera does not support Secure Sockets Layer (SSL) protocols used by many e-mail providers, such as Gmail. Therefore you will not be able to use SMTP Mail servers like Gmail that require SSL encryption. You can only use e-mail providers that do not require SSL encryption. Please contact your e-mail provider if you are not sure whether your SMTP server uses SSL encryption.

To configure e-mail alerts, follow these steps:

STEP 1 Access the setup options for your Cisco WVC210 Internet camera by clicking **Setup**.

STEP 2 Log in as required.

STEP 3 Go to the Applications > Mail window.

STEP 4 Check the box to enable an SMTP Server.

STEP 5 Provide the SMTP server name or the IP address and port number of the SMPT server. An account name and password are only required if your mail server requires authentication.

NOTE If both the Primary and Secondary SMTP servers are configured, e-mail alerts are sent out only through the Primary Server. If there is an e-mail failure with the Primary Server, then the camera attempts to route the e-mail alert through the Secondary Server.

STEP 6 Enter a subject and fill in the Send To and Show From e-mail addresses.

STEP 7 Click **Save** to save your settings.

Configuring Motion Detection

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

To set the motion detection area of the video image to be examined and adjust the sensitivity of detection, follow these steps:

STEP 1 Access the setup options for your Cisco WVC210 Internet camera by clicking **Setup**.

STEP 2 Log in as required.

STEP 3 Go to the Applications > Motion Detection window.

STEP 4 Under **Event**, check **Enable E-mail Alert**.

STEP 5 A message window is displayed; click **OK**.

STEP 6 Click **Save** to save your settings.

STEP 7   Click **Set Area & Sensitivity** near the bottom of the window. The Set Area and Sensitivity window is displayed

STEP 8   Customize the desired areas of sensitivity. You can choose the entire window to monitor by selecting **Full Screen.** Or, you can select one or more windows (2, 3, and 4) and isolate smaller and specific sections within the window.

STEP 9   Adjust the sensitivity of each window by using the threshold slider (less threshold means more sensitivity).

STEP 10   Click **Save** to save your settings. You are now set to receive motions detection e-mail alerts.

NOTE   Motion detection is triggered only if the camera is facing the preset motion detection position. If you would like enable motion detection in all positions, select **Enable Motion Detection In All Positions** in the Applications > Motion Detection > Pan/Tilt section.

Configuring Port Forwarding

Port forwarding allows Internet access to multiple cameras that are located inside a private network. For example, you have two cameras behind a NAT router – one is on alternate port 1024 and the second one is on port 1028. To access each camera individually, setup 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 utility, click **Setup > Advance Setup**.

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

When you open the URL to the camera, you now must specify the port number. For example: `http://192.168.1.99:1028`

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

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

STEP 5 From the web-based configuration utility, click **Firewall > Port Range Forwarding**. This example shows the Port Range Forwarding window of the Cisco WRVS4400N router.
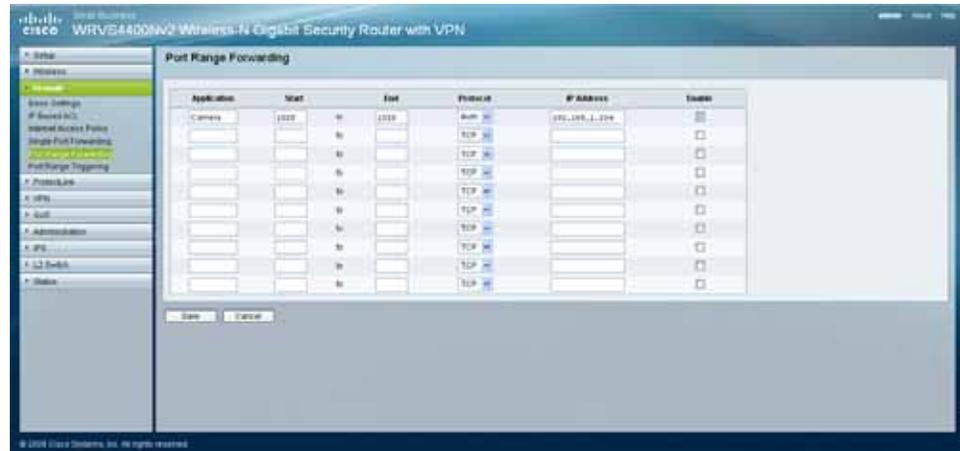
STEP 6 In the Port Range Forwarding window, configure the following:

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

    b. Enter the Start and End port. In this example, **1028** is used and this should match the HTTP port configured on the camera in **Step 2 on page 67**.

    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 Status Setting section.

This example shows the Summary window 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`

Setting Security Precautions on the Cisco WVC210

The following is a short list of recommended security precautions:

STEP 1   Change the default SSID from the Setup > Basic window, scroll to Wireless settings.

Change the SSID periodically.

STEP 2   Disable SSID Broadcast on your access point or wireless router.

STEP 3   Change the default user name and password for the administrator account from the Setup > Users window.

STEP 4   Use the highest encryption algorithm possible.

- Use WPA if it is available. From the Setup > Basic window, scroll to Wireless settings. Please note that this may reduce your network performance.

- If using WEP, change the WEP encryption keys periodically. From the Setup > Basic window, scroll to Wireless settings.

NOTE   Some of these security features are available only through the network router or access point. Refer to the router or access point documentation for more information.

Troubleshooting

Questions and Answers

This appendix provides solutions to problems that may occur during the installation and operation of the Cisco WVC210 Wireless-G Internet 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) is the official supported browser for the Cisco WVC210 Internet camera.

Q. **When I try to connect to the Wireless Network Camera, I get prompted for a user name and password.**

You should be prompted for a user name and password when you first connect to the camera. Enter the Administrator ID and Password set on the User window. The Username/Password prompt indicates that the Administrator has restricted access to specified users. Ask the Administrator for your Username and Password. If this has not been set, it should still be the default of admin/admin.

Q. **I can't connect to the Wireless Network Camera using a Wireless connection.**

You must perform the initial configuration of the Cisco WVC210 camera from a personal computer connected to the camera using a wired connection to the Ethernet port. The initial configuration cannot be performed over a wireless connection.

Once the initial configuration is complete, disconnect the LAN cable and unplug the camera. If a LAN cable is connected to the LAN port, the Wireless interface is disabled. In order to switch from wired to wireless (or wireless to wired) the camera needs to be rebooted (unplugged and then plugged in again.)

Also check that your PC and the Wireless Network Camera have compatible Wireless settings.

- The mode (Infrastructure or Ad-hoc) must be correct.

- The SSID must match.

- The wireless security settings must match.

- In Ad-hoc mode, the channel should match, although this is often not required.

Q.   **My video quality suddenly deteriorated.**

This can happen when an additional viewer connects to the Wireless Network Camera, overloading the camera or the available bandwidth. The image size and quality can be adjusted to cater for the required number of viewers and the available bandwidth.

Q.   **The motion detection feature doesn't send me any e-mails.**

The Cisco WVC210 camera does not support Secure Sockets Layer (SSL) protocols used by many e-mail providers, such as Gmail. Therefore you will not be able to use Simple Mail Transport Protocol (SMTP) Mail servers like Gmail that require SSL encryption. Contact your e-mail provider if you are not sure whether your SMTP server uses SSL encryption.

You must use a static IP address (you can copy the DHCP Address), but the DNS server must be that of the ISP and not of the router. You can find this address in the router's status log for WAN IP Address.

Q.   **When using the motion detection feature, I receive e-mails that don't show any moving objects.**

The motion detection feature doesn't actually detect motion. It compares frames to see if they are different. Major differences between frames are assumed to be caused by moving objects.

But the motion detector can also 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 **Audio/Video > Video Settings, page 45**.

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.

> **TIP** 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**.

Windows Help

Almost all wireless products require Microsoft Windows. Windows is the most used operating system in the world and comes with many features that help make networking easier. These features can be accessed through Windows Help and are described in this appendix.

TCP/IP

Before a computer can communicate with an access point or router, TCP/IP must be enabled. TCP/IP is a set of instructions, or protocol, all PCs follow to communicate over a network. Your PCs will not be able to use networking without having TCP/IP enabled. Windows Help provides complete instructions on enabling TCP/IP.

Shared Resources

If you wish to share printers, folders, or files over your network, Windows Help provides complete instructions on using shared resources.

Network Neighborhood/My Network Places

Other PCs on your network appear under Network Neighborhood or My Network Places (depending upon the version of Windows you're running). Windows Help provides complete instructions on adding PCs to your network.

B

Specifications

Cisco WVC210

Resource	Description
Standards	IEEE802.11g, IEEE802.11b, IEEE802.3, IEEE802.3u, IEEE802.1p (QoS Priority), IEEE802.1q (VLAN), 802.11e (Wireless QoS)
Ports	Ethernet, Antenna, Microphone in, Speaker Out, Power
Protocols	TCP/IP, HTTP, DHCP, SMTP, FTP, NTP, DNS, UPnP, RTP, RTSP, and DDNS
Button	One Reset Button
Cabling	UTP CAT 5
LEDs	Power, Activity, Ethernet, Wireless
Sensor	1/4 in. CMOS
Focal Length	500mm~Infinity
Frame Rate	Up to 30 fps
Resolution	640 x 480, 320 x 240, 160 x 120
Illumination	1LUX@F2.0
Field of View	60 degrees
Auto Patrol	9 Definable Preset Points by User
Pan	± 67 degrees

Resource	Description
Tilt	-34 degrees (down) to +30 degrees (up)
Web UI	Built in Web UI for Easy Browser-Based Configuration (HTTP)
Web Browser	Browser Internet Explorer 6.0 (or later) with ActiveX support for viewing, recording, playback and setting motion detection; limited support for Safari and Mozilla Firefox (no motion detection).
Logging	Event Logging (SYSLOG)
Upgrades	Firmware Upgradable Through Web-Browser
Dual Streaming Codecs	MPEG-4 Simple Profile, MJPEG
Snapshot	JPEG
Image Position	Flip and Mirror
Image Settings	Brightness and Contrast
Motion Detection	4 detection areas with individual sensitivity thresholds; triggers alerts.
Compression	G.711 A-law and U-law
Sampling Rate	8 KHz
Dual Bit Rate	16 Kbps
Image Settings	Brightness and Contrast
Monitor and Recording Software	Monitoring and recording for up to 16 cameras. Monitor live video, record, and play back simultaneously.
WEP/WPA	WEP 64bit/128bit, WPA-TKIP, WPA-PSK, WPA2-PSK
User List	Three-level user rights list to view video and to control camera.
Username/Password	Logon authentication 20 characters username and 8 characters password.

Resource	Description
NTP	Network Time Protocol synchronizes camera date and time with your network.
SMTP	Simple Mail Transfer Protocol Client allows video clips to be emailed.
FTP Client	FTP Client facilitates scheduling transfer of images to an FTP server.
DDNS	Dynamic DNS facilitates accessing the camera by name, irrespective of the camera IP address.
Samba Client	Used for recording files straight to a NAS without having to leave the PC running.
UPnP	On by default. Allows auto-discovery of the camera by other UPnP devices.
Dimensions	1.26 in. x 7.83 in. x 6.89 in. (32 mm x 199 mm x 175 mm)
Unit Weight	1.01 lb (.46 kg)
Power	5DVC 2.0A Switching Power Supply
Certifications	Wi-Fi, FCC, CE and UL
Operating Temp	-32 to 113°F (0 to 45°C)
Storage Temp	-4 to 140°F (-20 to 70°C)
Operating Humidity	10 to 80%, Non-condensing
Storage Humidity	0 to 90%, Non-condensing

C

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 WVC210 Internet Video Cameras.

Product Resources

Support	Location
Online Technical Support and Documentation	www.cisco.com/support
Product Information	www.cisco.com/go/surveillance
Phone Support Contacts	www.cisco.com/en/US/support/ tsd_cisco_small_business_support_cent er_contacts.html
Camera Software Downloads	http://www.cisco.com/en/US/products/ ps9944/ tsd_products_support_series_home.html
Product Documentation	**Location**
Cisco Small Business Model WVC210 Wireless-G PTZ Internet Video Camera with 2-Way Audio Quick Start Guide	http://www.cisco.com/en/US/products/ ps9944/ prod_installation_guides_list.html
Administration Guide for the SW-VMS16 Video Monitoring System	http://www.cisco.com/en/US/products/ ps9944/ prod_maintenance_guides_list.html

Cisco Small Business Model WVC210 Wireless-G PTZ Internet Video Camera with 2-Way Audio Administration Guide	http://www.cisco.com/en/US/products/ps9944/prod_maintenance_guides_list.html
Cisco Small Business	**Location**
Cisco Partner Central site for Small Business (Partner Login Required)	www.cisco.com/web/partners/sell/smb
Cisco Small Business Home	www.cisco.com/smb
Marketplace	www.cisco.com/go/marketplace