



Cisco Video Surveillance Standalone Encoder Series User Guide

Americas Headquarters

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

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

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

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

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

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

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Cisco Video Surveillance Standalone Encoder Series User Guide
Copyright © 2012 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface v

Audience v

Organization v

Obtaining Documentation, Obtaining Support, and Security Guidelines vi

CHAPTER 1

Overview 1-1

Read Before Use 1-1

Package Contents 1-2

Physical Description 1-2

CIVS-SENC-4P Front and Back View 1-2

CIVS-SENC-8P Front and Back View 1-3

General I/O Terminal Block 1-5

DI/DO Diagram 1-6

Status LED 1-7

Hardware Reset 1-8

Network Deployment 1-8

Setting up the Encoder on the Network 1-8

Enabling Authentication 1-10

Ready to Use 1-11

CHAPTER 2

Accessing the Encoder 2-1

Determining the Encoder IP Address 2-1

Using DHCP 2-1

Using Link-Local Address Scheme 2-1

Accessing the Encoder Using a Web Browser 2-2

Accessing the Encoder Using an RTSP Player 2-2

CHAPTER 3

Home Window 3-1

Home Window Overview 3-1

Home Window Features 3-2

Camera Control Area 3-2

Manual Trigger Area 3-2

DI/DO Control Area 3-3

Configuration Area	3-3
Live Video Window	3-3

CHAPTER 4

Client Settings 4-1

Accessing Client Settings	4-1
Managing Client Settings	4-1
H.264 / MPEG-4 Media Options	4-1
H.264 / MPEG-4 Protocol Options	4-2
MP4 Saving Options	4-2
Quadview Settings	4-3
Local Streaming Buffer Time	4-3
Joystick Settings	4-3
Assigning Functions to Joystick Buttons	4-4

CHAPTER 5

Configuration 5-1

Accessing Configuration Options	5-1
System Window	5-2
System Settings	5-2
System Time Settings	5-2
Security Window	5-3
Root Password Settings	5-3
Manage Privilege Settings	5-3
Manage User Settings	5-4
HTTPS Window	5-5
Enable HTTPS Settings	5-5
Create and Install Certificate Methods	5-5
Cancel HTTPS Settings	5-7
Remove a Signed Certificate	5-8
SNMP Window	5-8
Network Window	5-8
Network Type Settings	5-9
IEEE 802.1x Settings	5-10
QoS (Quality of Service) Settings	5-10
HTTP Settings	5-12
HTTPS Settings	5-13
Two Way Audio Settings	5-13
FTP Settings	5-13
RTSP Streaming Settings	5-13
Access List Settings	5-16

General Access List Settings	5-16
Filter Type Settings	5-18
Filter	5-18
Administrator IP Address	5-18
Digital I/O Window	5-19
Digital Input Settings	5-19
Digital Output Settings	5-19
Audio and Video Window	5-19
Audio and Video Settings Overview	5-19
Video Settings	5-20
Audio Settings	5-25
Motion Detection Window	5-26
How Motion Detection Works	5-27
Camera Tampering Detection Window	5-27
Camera Control Window	5-28
RS485 Settings	5-28
Camera ID Settings	5-29
Customization Settings	5-29
Homepage Layout Window	5-32
Preview Area	5-32
Customized Button	5-32
Theme Options	5-32
Application Window	5-34
Event Settings	5-35
Recording Window	5-42
Local Storage Window	5-42
System Log Window	5-42
Remote Log	5-42
Current Log	5-43
View Parameters Window	5-43
Maintenance Window	5-43
Rebooting the Encoder	5-43
Restoring the Encoder	5-44
Exporting and Uploading Files	5-44
Upgrading the Firmware	5-47

APPENDIX A
Technical Specifications A-1

INDEX



Preface

This document provides the information that is required to understand and use the Cisco video surveillance encoders, models CIVS-SENC-4P and CIVS-SENC-8P.

Audience

This document is intended for users who want to install and configure the Cisco video surveillance encoders, models CIVS-SENC-4P and CIVS-SENC-8P, to convert data from analog cameras to digital format.

Organization

This document is organized as follows:

Chapter 1, “Overview”	Introduces the encoder models, describing key features of the hardware, and how to set it up.
Chapter 2, “Accessing the Encoder”	Describes how to access the encoder through a web page, or using an RTSP player.
Chapter 3, “Home Window”	Describes key features on the home window of the encoder user interface.
Chapter 4, “Client Settings”	Describes how to select the stream transmission mode and saving options on the local computer.
Chapter 5, “Configuration”	Describes the configuration options that are available on the encoder user interface.
Appendix A, “Technical Specifications”	Describes key features and technical specifications of the encoder models.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information about obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

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



CHAPTER 1

Overview

The Cisco video surveillance encoders, models CIVS-SENC-4P and CIVS-SENC-8P, convert analog video into high quality digital video, and set a new standard in encoder security. The CIVS-SENC-4P and CIVS-SENC-8P models contain the following key features:

- Allow 4-CH or 8-CH high resolution video capture with a high frame rate.
- Use the H.264 compression format, resulting in greatly reduced video file sizes, and conserving valuable bandwidth and storage space.
- The 4 port model, CIVS-SENC-4P, supports simultaneous dual streams, while the 8 port model, CIVS-SENC-8P, supports single stream to be transmitted in H.264, MPEG-4, and MJPEG formats. The video stream can also be individually configured with frame rates, resolution, and image quality to meet different platforms or bandwidth constraints.
- Use motion detection.
- Upgrade the security level of the associated IP surveillance system with the HTTPS network security protocol.
- Compatible with Cisco Video Surveillance Manager Version 6.3.2 and later software, providing scalability and easy-to-use operation.
- Designed as a rack mount solution for easy installation. (Needs optional accessory kit.)

These features make the CIVS-SENC-4P and CIVS-SENC-8P models easy to install and integrate with an existing analog camera. As a highly innovative video encoder series, the CIVS-SENC-4P and CIVS-SENC-8P models allow you to easily upgrade to a full-featured, high-end, IP surveillance solution.

Read Before Use

It is important to verify that all contents received are complete according to the package contents list (see the [“Package Contents” section on page 1-2](#)). Take note of the warnings in the Quick Start Guide before installing the encoder; then carefully read and follow the instructions in the Network Deployment section of this guide (see the [“Network Deployment” section on page 1-8](#)) to avoid damage during installation.

The encoder is a network device, and it is designed for various applications, including video sharing, general security/surveillance, and so on. The Configuration chapter (see the [“Configuration” section on page 5-1](#)) suggests ways to make best use of the encoder, and to ensure proper operation.

Package Contents

The Cisco video surveillance encoder package includes these items:

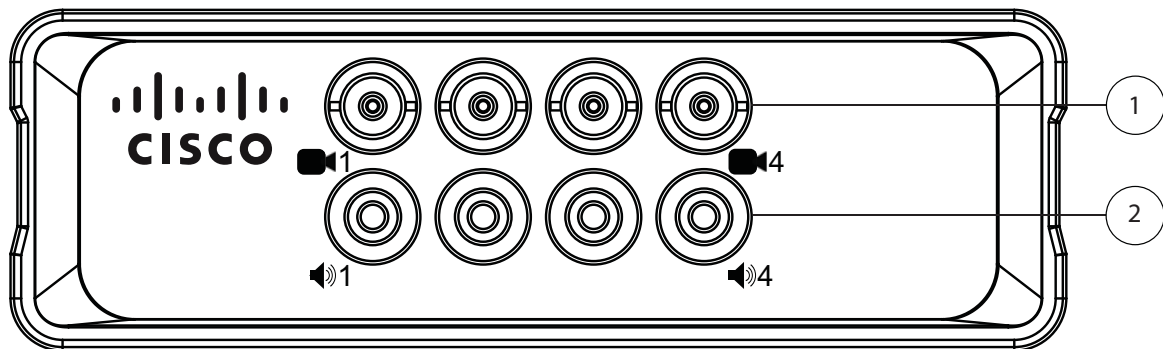
- CIVS-SENC-4P (4 channel) or CIVS-SENC-8P (8 channel) encoder (qty. 1)
- Power adapter (qty. 1)
- General I/O terminal blocks for CIVS-SENC-4P (10 pins x 3 pieces) or CIVS-SENC-8P (16 pins x 3 pieces) (qty. 3)
- Warranty card (qty. 1)

Physical Description

CIVS-SENC-4P Front and Back View

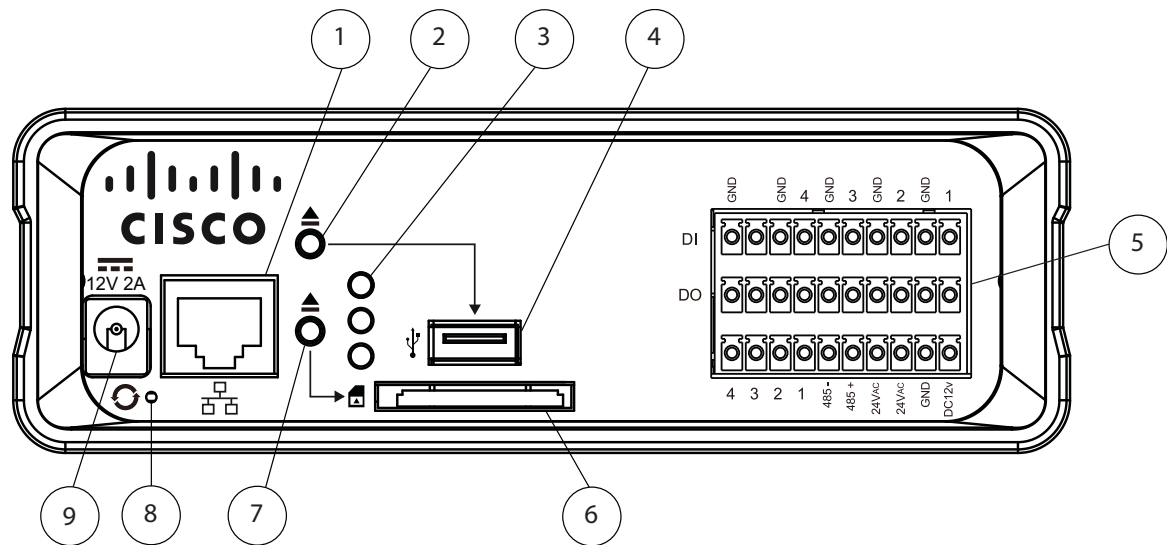
Figure 1-1 shows the front view of the CIVS-SENC-4P encoder. The top row is comprised of four video input slots, and the bottom row is comprised of four audio input slots.

Figure 1-1 *CIVS-SENC-4P Front View*



1	BNC video inputs (qty. 4)
2	RCA audio inputs (qty. 4)

Figure 1-2 shows the back view of the CIVS-SENC-4P encoder.

Figure 1-2 CIVS-SENC-4P Back View

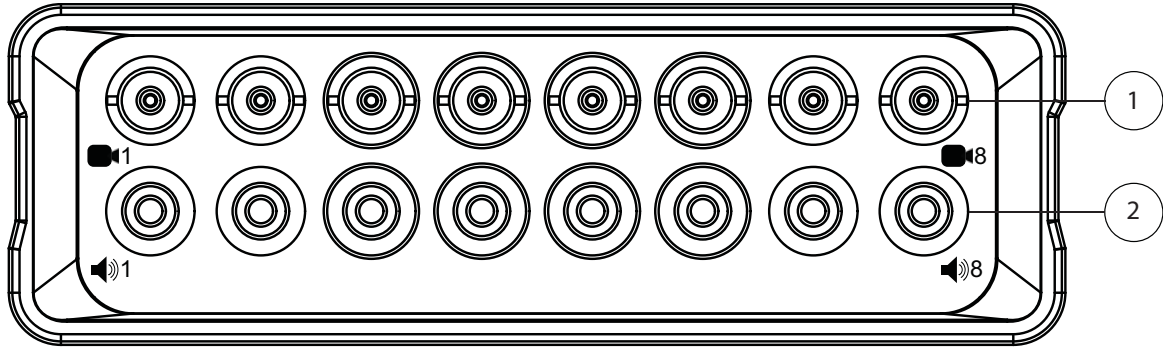
1	Ethernet 10/100/1000 RJ45 port	6	SD/SDHC card slot. While the SD/SDHC slot is on the device, it is not currently supported by Cisco.
2	In encoders that support USB, press this button before removing the USB device.	7	In encoders that support SD/SDHC, press this button before removing the SD/SDHC device.
3	Status LEDs. For more information, see the “Status LED” section on page 1-7.	8	Reset button (recessed). For more information, see the “Hardware Reset” section on page 1-8.
4	USB port. While the USB port is on the device, it is not currently supported by Cisco.	9	Power input
5	General I/O terminal block. For more information, see the “General I/O Terminal Block” section on page 1-5.		

**Note**

Where enabled, the USB port is for maintenance purposes only.

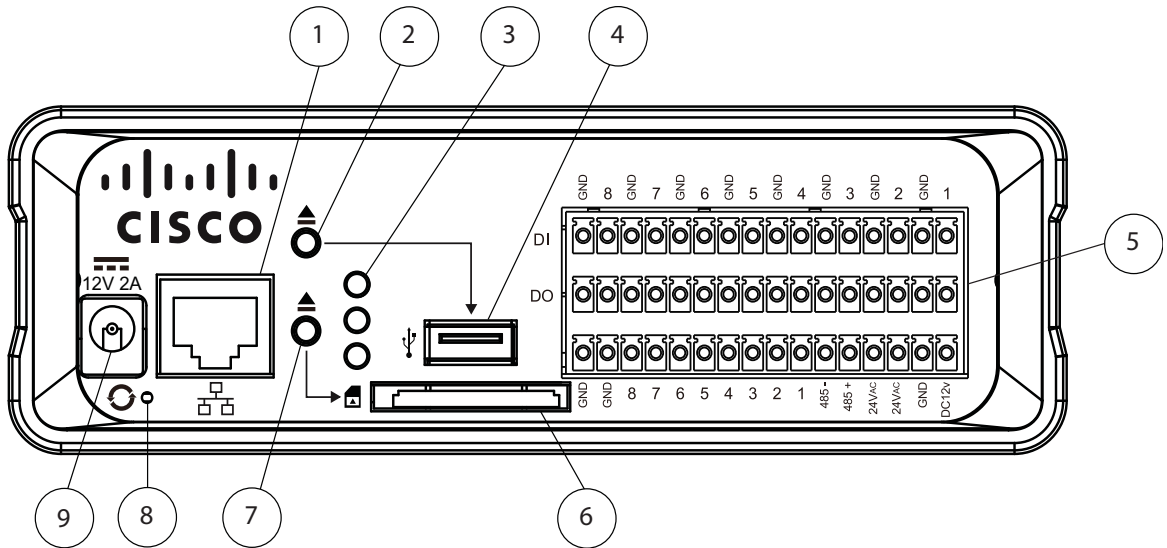
CIVS-SENC-8P Front and Back View

[Figure 1-3](#) shows the front view of the CIVS-SENC-8P encoder. The top row is comprised of eight video input slots, and the bottom row is comprised of eight audio input slots.

Figure 1-3 CIVS-SENC-8P Front View

1	BNC video inputs (qty. 8)
2	RCA audio inputs (qty. 8)

Figure 1-4 shows the back view of the CIVS-SENC-8P encoder.

Figure 1-4 CIVS-SENC-8P Back View

1	Ethernet 10/100/1000 RJ45 port	6	SD/SDHC card slot. While the SD/SDHC slot is on the device, it is not currently supported by Cisco.
2	In encoders that support USB, press this button before removing the USB device.	7	In encoders that support SD/SDHC, press this button before removing the SD/SDHC device.

3	Status LEDs. For more information, see the “Status LED” section on page 1-7 .	8	Reset button (recessed). For more information, see “Hardware Reset” section on page 1-8 .
4	USB port. While the USB port is on the device, it is not currently supported by Cisco.	9	Power input
5	General I/O terminal block. For more information, see “General I/O Terminal Block” section on page 1-5 .		

**Note**

Where enabled, the USB port is for maintenance purposes only.

General I/O Terminal Block

This encoder provides a general I/O terminal block which is used to connect external input /output devices. For information about the pin definitions, see the [“Pin Definitions of the General I/O Terminal Blocks” section on page 1-5](#).

Pin Definitions of the General I/O Terminal Blocks

[Figure 1-5](#) shows the pin locations on the back panel of the CIVS-SENC-4P encoder, and [Table 1-1](#) provides definitions for each of the pins.

Figure 1-5 *CIVS-SENC-4P Pin Locations*

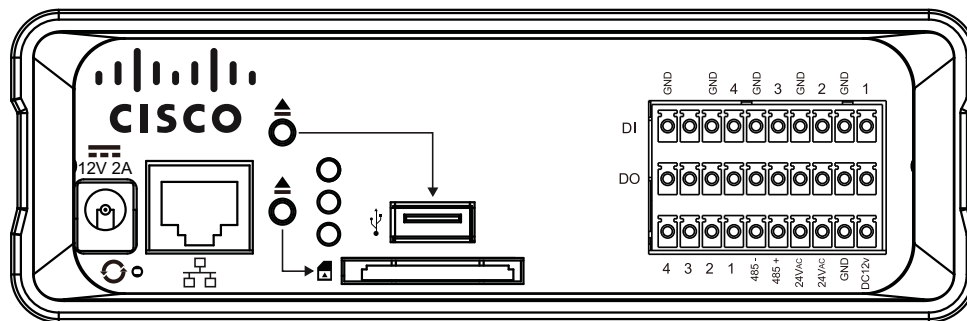


Table 1-1 *CIVS-SENC-4P Pin Definitions*

GND	N/A	CH 4 GND	CH 4 DI	CH 3 GND	CH 3 DI	CH 2 GND	CH 2 DI	CH 1 GND	CH 1 DI
GND	N/A	CH 4 GND	CH 4 DO	CH 3 GND	CH 3 DO	CH 2 GND	CH 2 DO	CH 1 GND	CH 1 DO
CH 4 Audio out	CH 3 Audio out	CH 2 Audio out	CH 1 Audio out	RS 485-	RS 485+	24V AC	24V AC	GND	DC 12V

Figure 1-6 shows the pin locations on the back panel of the CIVS-SENC-8P encoder, and Table 1-2 provides definitions for each of the pins.

Figure 1-6 CIVS-SENC-8P Pin Locations

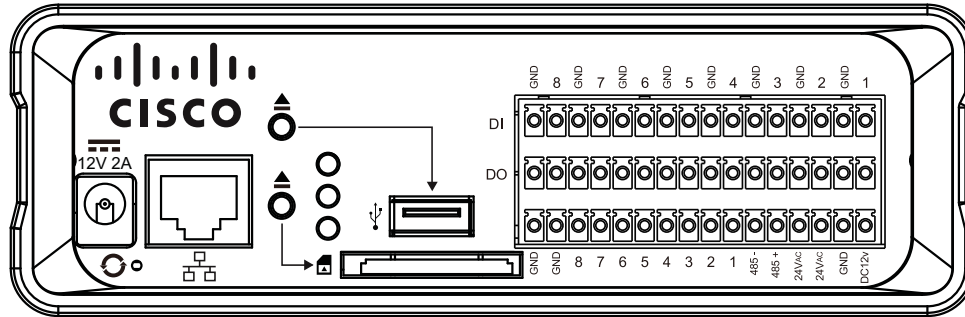


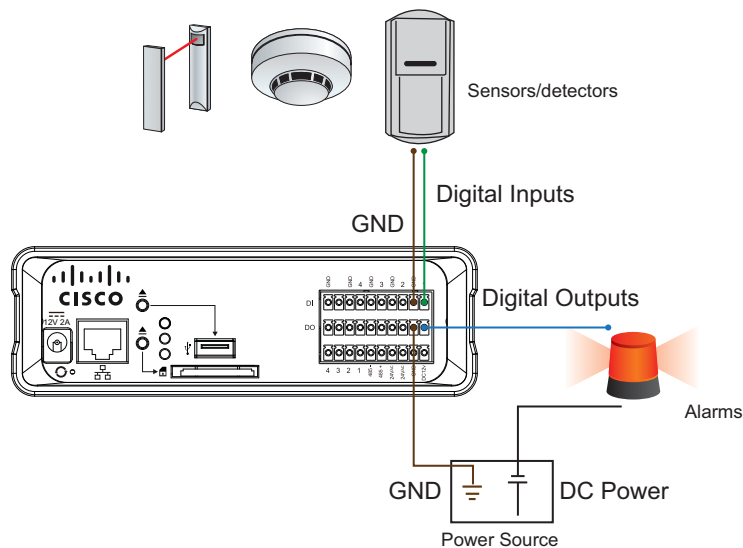
Table 1-2 CIVS-SENC-8P Pin Definitions

CH 8	CH 8	CH 7	CH 7	CH 6	CH 6	CH 5	CH 5	CH 4	CH 4	CH 3	CH 3	CH 2	CH 2	CH 1	CH 1
GND	DI	GND	DI	GND	DI	GND	DI	GND	DI	GND	DI	GND	DI	GND	DI
CH 8	CH 8	CH 7	CH 7	CH 6	CH 6	CH 5	CH 5	CH 4	CH 4	CH 3	CH 3	CH 2	CH 2	CH 1	CH 1
GND	DO	GND	DO	GND	DO	GND	DO	GND	DO	GND	DO	GND	DO	GND	DO
GND	GND	CH 8	CH 7	CH 6	CH 5	CH 4	CH 3	CH 2	CH 1	RS	RS	24V	24V	GND	DC
		Audio	Audio	Audio	Audio	Audio	Audio	Audio	Audio	485-	485+	AC	AC		12V
		out	out	out	out	out	out	out	out						

DI/DO Diagram

Figure 1-7 shows the connections necessary to set up the encoder with various external devices.

Figure 1-7 DI/DO Connections



**Note**

The following guidelines should be observed:

- External alarms or other devices that connect to the digital outputs require an external power supply, for example, DC power from a power adapter.
- 12V Ground should connect to the encoder ground terminal block. For detailed pin definitions, see the [“Pin Definitions of the General I/O Terminal Blocks” section on page 1-5](#).
- It is recommended that you keep the current running through each of the DO lines under 1A.

Status LED

The LED indicates the status of the encoder. [Table 1-3](#) describes the different status levels of the Yellow (SD), Green (Network), and Red (Power) LEDs.

Table 1-3 LED Status Indicators

LED Name	LED Status	Indication
SD	Steady yellow	SD card is present and functioning normally
	Blinking yellow	SD card is present yet problems occurred with data access
	Yellow LED off	No SD card in the slot
Network	Blinking green every 1 sec.	Network activity (heartbeat)
	Green LED off	Network failed
Power	Steady red	Power on and during system boot
	Red LED off	Power off

[Table 1-4](#) describes LED blinking states.

Table 1-4 Blinking LED Status Indicators

LED Status	Indication
Blinking green every 2 sec.	Audio mute (heartbeat)
Blinking red every 0.15 sec. and blinking green every 1 sec.	Upgrading firmware
Blinking red every 0.15 sec. and blinking green every 0.15 sec.	Restoring default

Hardware Reset

See [Figure 1-2](#) (CIVS-SENC-4P) or [Figure 1-4](#) (CIVS-SENC-8P) for the location of the hardware reset button on your encoder. The reset button is used to reset the system or to restore the factory default settings. Sometimes, if your encoder is experiencing a problem, resetting the system can return the encoder to normal operation. If, after performing a reset, the problem remains, restore the factory settings and install the system again.

Use one of the following methods to reset or restore the settings:

- **Reset**—Press and release the recessed reset button using a straightened paper clip. Wait for the encoder to reboot.
- **Restore**—Press and hold the reset button down until the status LED blinks rapidly. It takes about 30 seconds. Note that all settings are restored to factory default. When the system has been restored successfully, the status LED blinks green and red during normal operation.

Network Deployment

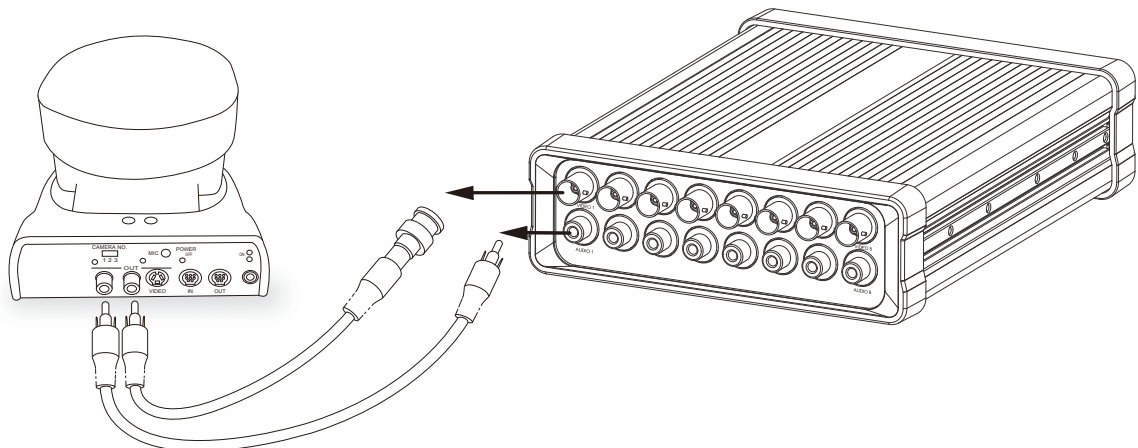
Setting up the Encoder on the Network

To connect the encoder to the camera and the network, follow these steps:

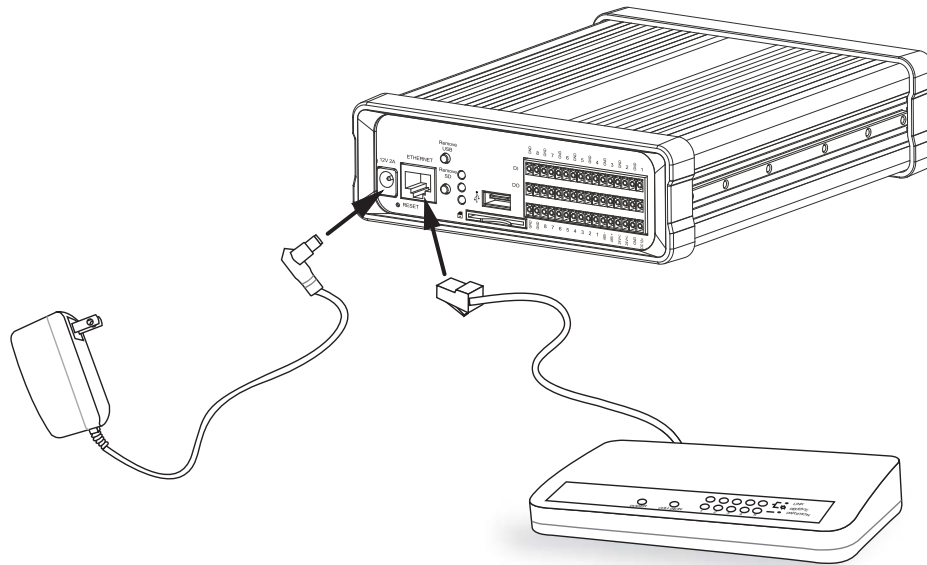
Procedure

- Step 1** Connect the video out slot on the camera to a BNC video input slot on the encoder. See [Figure 1-8](#).
- Step 2** Connect the line-out audio source on the camera to an RCA audio input slot on the encoder.

Figure 1-8 Video and Audio Connections



- Step 3** Connect the encoder to a switch using an Ethernet cable. See [Figure 1-9](#).
- Step 4** Connect the encoder to a power outlet using the power cable.
- Step 5** If you have external devices, such as sensors or alarms, connect them to the general I/O terminal block. For detailed pin definitions, see the “[Pin Definitions of the General I/O Terminal Blocks](#)” section on [page 1-5](#).

Figure 1-9 Network, Power, and External Device Connections

- Step 6** You can set up the encoder on the network in any of the following ways:
- Set up the encoder behind a router. For more information, see the [“Setting up the Encoder Behind a Router”](#) section on page 1-9.
 - Use a static IP address. For more information, see the [“Setting up the Encoder Using a Static IP Address”](#) section on page 1-10.
 - Use PPPoE. For more information, see the [“Ready to Use”](#) section on page 1-11.

Setting up the Encoder Behind a Router

To set up the encoder behind a router, perform the following procedure:

Before you begin

- Make sure you have a router.
- Find out the public IP address of your router provided by your ISP (Internet Service Provider).

Procedure

- Step 1** Connect your encoder behind a router. For information on how to obtain your IP address, see the [“Accessing the Encoder”](#) section on page 2-1.
- Step 2** In this case, if the Local Area Network (LAN) IP address of your encoder is 192.168.0.3, forward the following ports for the encoder on the router:
- HTTP port
 - RTSP port
 - RTP port for audio
 - RTCP port for audio

- RTP port for video
- RTCP port for video

If you have changed the port numbers on the Network window, open the ports accordingly on your router. For information on how to forward ports on the router, refer to the user manual for your router.

- Step 3** Use the public IP address of your router and the secondary HTTP port to access the encoder from the Internet. For more information, see the [“Network Type Settings” section on page 5-9](#).

Setting up the Encoder Using a Static IP Address

Choose this connection type if you are required to use a static IP address for the encoder. For more information, see the [“LAN Settings” section on page 5-9](#).

Enabling Authentication

Cisco recommends that you use the following procedure to enable authentication on the encoder via its Web-based user interface.

Procedure

- Step 1** On the home window of the encoder user interface, choose **Configuration > Security**.

For more information about accessing the encoder user interface, see the [“Accessing the Encoder” section on page 2-1](#).

- Step 2** Set a root password and then confirm it.



Note

These encoders allow up to 20 user accounts plus the root account. The default passwords are blank for both users and the root. For user names and all passwords, the minimum length is one character and the maximum length allowed is 64 characters. The root, user names, and their passwords can include the following characters: a-z, A-Z, 0-9, !, \$, %, -, ., ^, _, ~, @

- Step 3** In the Manage Privilege area, ensure that the Allow Anonymous Viewing checkbox is unchecked.

- Step 4** Click **Save**.

- Step 5** Click **HTTPS** in the left-hand pane, ensure that the Enable HTTPS secure connection checkbox is unchecked, and click **Save**.

HTTPS is not supported by VSM.

- Step 6** Click **Network** in the left-hand pane and do the following:

- In the HTTP area, choose **Basic** on the Authentication drop-down menu, and ensure that the HTTP port is 80.
- In the RTSP Streaming area, choose **Basic** on the Authentication drop-down menu. The digest mode is not supported.
- Click **Save**.

**Note**

The credentials you set up here should also be used when the encoder is added in Video Surveillance Manager Server (VSMS) and Video Surveillance Operations Manager (VSOM).

Ready to Use

When you have completed setup, you are ready to access the encoder. For more information, see the [“Accessing the Encoder” section on page 2-1](#).



CHAPTER 2

Accessing the Encoder

This chapter describes how to access the video encoder, and includes the following sections:

- [Determining the Encoder IP Address, page 2-1](#)
- [Accessing the Encoder Using a Web Browser, page 2-2.](#)
- [Accessing the Encoder Using an RTSP Player, page 2-2.](#)

Determining the Encoder IP Address

To access the encoder, you must determine what its IP address is. You can use one of the following two methods to determine what the encoder IP address is:

- [Using DHCP, page 2-1](#)
- [Using Link-Local Address Scheme, page 2-1](#)

Using DHCP

By default, when the encoder is turned on it attempts to obtain an IP address from a DHCP server in your network.

Using Link-Local Address Scheme

If the encoder cannot obtain an IP address through DHCP, an IP address is assigned using the Link-Local address scheme. The Link-Local address scheme enables the video encoder to be seen with a default IP address of 169.254.0.99. If another device on your network is already using this default IP address, the video encoder acquires an IP address by inserting part of its MAC address into the 169.254.x.x IP address. To do this, the encoder converts the hex digits of the MAC address to decimal values and then applies them to create an IP address in the following format:

169.254.MAC:9-10.MAC:11-12

where MAC:9-10 are the 9th and 10th digits in the MAC address, and MAC:11-12 are the 11th and 12th digits.

For example, using this method, an encoder with a MAC address of 00-11-22-33-44-55 acquires an IP address of 169.254.68.85, given that hex 44 = 68 decimal and hex 55 = 85 decimal.

**Note**

To find the encoder MAC address, see the label on the bottom of the device.

Accessing the Encoder Using a Web Browser

To access the encoder using a Web browser, perform the following procedure:

Before you begin

Make sure you have the IP address of the encoder. For more information about acquiring the encoder IP address, see the [“Determining the Encoder IP Address” section on page 2-1](#).

Procedure

-
- Step 1** Open your Web browser (for example, Microsoft® Internet Explorer).
- Step 2** Enter the IP address of the encoder in the address field using the following format: **http://ip-address**, where ip-address is the IP address of your encoder.
- Step 3** Press **Enter**.
- The live video is displayed in your web browser.
- Step 4** If this is your first time installing the CIV-SENC-4P or CIV-SENC-8P encoder, a dialog box may be displayed asking you to install required plug-ins. Follow the instructions onscreen to install the required plug-ins on your computer.

**Note**

The following guidelines should be observed:

- By default, the encoder is not password-protected. To prevent unauthorized access, it is highly recommended that you set a password for the encoder. For more information about how to enable password protection, see the [“Security Window” section on page 5-3](#).
 - If you see a dialog box indicating that your security settings prohibit running ActiveX® Controls, you must enable the ActiveX® Controls for your browser. For information about enabling ActiveX® Controls, see the user documentation for your computer.
-

Accessing the Encoder Using an RTSP Player

You can use one of the following RTSP players to view MPEG-4 streaming media:

- Quick Time Player
- Real Player

To access the encoder using an RTSP player, perform the following procedure:

Procedure

- Step 1** Open the RTSP player.
- Step 2** Choose **File > Open URL**.
A URL dialog box is displayed.
- Step 3** Enter the address in the following format: **rtsp://ip-address:rtsp-port/stream-name**
where *ip-address* is the IP address of the encoder (for more information, see the [“Determining the Encoder IP Address”](#) section on page 2-1), and *stream-name* is the RTSP streaming access name for stream1 or stream2.
As most ISPs and players only allow RTSP streaming through port number 554, set the *rtsp-port* to 554.
For more information, see the [“RTSP Streaming Settings”](#) section on page 5-13.
- Step 4** Click **OK**.
The live video displays in your player.
-



CHAPTER 3

Home Window

This chapter describes the layout of the home window of the encoder user interface, and includes the following sections:

- [Home Window Overview, page 3-1](#)
- [Home Window Features, page 3-2](#)

Home Window Overview

[Figure 3-1](#) provides an overview of the main features on the home window of the encoder user interface.

Figure 3-1 Encoder User Interface Home Window




1	Cisco logo. Click this logo to go to the Cisco website.	5	DI/O control area. For more information, see the “ DI/DO Control Area ” section on page 3-3.
2	Host name. This can be customized to fit your needs. For more information, see the “ System Window ” section on page 5-2.	6	Manual trigger area. For more information, see the “ Manual Trigger Area ” section on page 3-2.
3	Live view window. For more information, see the “ Live Video Window ” section on page 3-3.	7	Camera control area. For more information, see the “ Camera Control Area ” section on page 3-2.
4	Configuration area. For more information, see the “ Configuration Area ” section on page 3-3.		

Home Window Features

Camera Control Area

[Table 3-1](#) describes the features available in the camera control area.

Table 3-1 Camera Control Area Features

Option	Description
Video Stream	The CIVS-SENC-4P model supports four channels for live video viewing, and the CIVS-SENC-8P model supports eight channels. Each channel allows you to view only one stream. You can choose from channels 1,2,3,4,(5,6,7,8), and Quad View. For more information about video settings, see the “ Video Settings ” section on page 5-20.
PTZ Control Area	The PTZ navigation panel is available only when a PTZ camera is attached. The up/down/left/right/zoom/focus/pan buttons allow you to adjust the video in the viewing window to the view you want to watch. Click the Home  button to return to the center of the screen. Click the Patrol button to move from one point to another, and click it again to stop patrolling. Click Stop to stop the pan movement. For more information about controlling the camera, see the “ Camera Control Window ” section on page 5-28.
Pan/Tilt/Zoom Speed	In the Pan, Tilt, and Zoom Speed drop-down lists, choose speed ranges from -5 (slow) to 5 (fast).

Manual Trigger Area

Click to enable/disable an event trigger manually. Event triggers must be configured on the Application window before enabling this function. Up to four event settings can be configured. For more information about event settings, see the “[Event Settings](#)” section on page 5-35.

**Tip**

If you want to hide this feature on the home window, uncheck the **Show manual trigger button** checkbox on the Homepage layout window. For more information, see the [“Homepage Layout Window” section on page 5-32](#).

DI/DO Control Area

[Table 3-2](#) describes the features available in the DI/O control area.

Table 3-2 *DI/O Control Area Features*

Option	Description
Digital Output	The CIVS-SENC-4P model has four digital output switches, and the CIVS-SENC-8P model has eight. Click to turn the digital output device on or off for a switch. Switch 1 is for the channel 1 digital output control, switch 2 is for the channel 2 digital output control, and so on.
Digital Input	The CIVS-SENC-4P model has four digital input status indicators, and the CIVS-SENC-8P model has eight. Red indicates that the digital input status is active, while white indicates that it is inactive.

Configuration Area

[Table 3-3](#) describes the features available in the Configuration area.

Table 3-3 *Configuration Area Features*

Option	Description
Client Settings	Click this button to access the client settings window. For more information, see the “Client Settings” section on page 4-1 .
Configuration	Click this button to access the configuration window of the encoder UI. It is recommended that a password be applied to the encoder so that it can only be configured by the administrator. For more information, see the “Configuration” section on page 5-1 .
Language	Click this button to select a language for the user interface.

Live Video Window

[Table 3-4](#) describes the features available in the live video window.

Table 3-4 *Live Video Window Features*

Option	Description
Video Title	Located above the live video window, in the upper-left corner. The video title can be configured. For more information, see the “Video Settings” section on page 5-20 .
MPEG-4 Protocol and Media Options	The transmission protocol and media options for MPEG-4 video streaming are located above the live video window, in the upper-left corner. For information about configuring these settings, see the “Client Settings” section on page 4-1 .
Time	Displays the current time. For information about configuring this setting, see the “Video Settings” section on page 5-20 .
Title and Time	The video title and time can be stamped on the streaming video. For more information about configuring these settings, see the “Video Settings” section on page 5-20 .
Video and Audio Control Buttons	Located along the bottom of the live video window. Depending on the encoder model and configuration, some buttons may not be available. For more information about the video and audio control buttons, see “Video and Audio Control Buttons” section on page 3-4 .
Go To	Located to the right of the video and audio control buttons, this drop-down menu enables you to locate and move to a preset location instantly on the viewing window.

Video and Audio Control Buttons

[Table 3-5](#) describes the video and audio control buttons.

Table 3-5 *Video and Audio Control Buttons*


















Icon	Description
	Snapshot—Click this button to capture and save still images. The captured images are displayed in a pop-up window. Right-click on the image and select Save Picture As to save it in JPEG (*.jpg) or BMP (*.bmp) format.
	Digital Zoom—Click this button to display the Digital Zoom dialog box, and uncheck the Disable digital zoom checkbox to enable the zoom operation. The Digital Zoom dialog box contains a navigation area on the right-hand side. The shaded box on the navigation area indicates the part of the image that is currently being magnified. Drag the shaded box to move to a different area of the image. To control the zoom level, drag the slider bar on the Digital Zoom dialog box.
	Pause—Pause transmission of the streaming media. This button becomes the Resume  button when the Pause button is clicked.
	Stop—Stop transmission of the streaming media. To continue transmission, click the Resume  button.
	Start MP4 Recording—Click this button to record video clips in MP4 file format that can be saved to your computer. Press the Stop MP4 Recording  button to end recording. When you exit the web browser, video recording stops automatically. For information about saving and naming files, see the “Video Settings” section on page 5-20 .

Table 3-5 Video and Audio Control Buttons (continued)

Icon	Description
	Volume—When the  Mute function is not activated, move the slider bar to adjust the volume on the local computer.
	Full Screen—Click this button to switch to full screen mode. Press the Esc key to switch back to normal mode.
	Talk—Click this button to talk to people around the encoder. Sound projects from an external speaker connected to the encoder. Click  again to end talking transmission.
	Broadcast—Click this button to broadcast to all channels.
	Mic Volume—When the Mic Mute button  is not activated, click the Mic volume button and drag the slider bar to adjust the microphone volume on the local computer.
	Mic Mute—Click this button to turn off the Mic volume on the local computer.



CHAPTER 4

Client Settings

This chapter describes how to select the stream transmission mode and saving options on the local computer, and it contains the following sections:

- [Accessing Client Settings, page 4-1](#)
- [Managing Client Settings, page 4-1](#)

Accessing Client Settings

To access client settings, click **Client settings** on the encoder user interface home window. For information about configuring client settings, see the “[Managing Client Settings](#)” section on page 4-1.

When you have finished configuring client settings, click **Save** at the bottom of the Client settings window.

Managing Client Settings

You can configure the following client settings on the Client settings window:

- [H.264 / MPEG-4 Media Options, page 4-1](#)
- [H.264 / MPEG-4 Protocol Options, page 4-2](#)
- [MP4 Saving Options, page 4-2](#)
- [Quadview Settings, page 4-3](#)
- [Local Streaming Buffer Time, page 4-3](#)
- [Joystick Settings, page 4-3](#)

H.264 / MPEG-4 Media Options

These options are enabled only when the video mode is set to H.264 or MPEG-4. For more information, see the “[Video Settings](#)” section on page 5-20.

[Table 4-1](#) describes the H.264/MPEG-4 media options.

Table 4-1 H.264/MPEG-4 Media Options

Option	Description
Video and audio	Select to stream both video and audio data.
Video only	Select to stream video data only.
Audio only	Select to stream audio data only.

H.264 / MPEG-4 Protocol Options


Depending on your network environment, you can choose one of four transmission modes of H.264 or MPEG-4 streaming.

[Table 4-2](#) describes the transmission mode options.

Table 4-2 H.264/MPEG-4 Protocol Options

Option	Description
UDP unicast	A protocol that allows for more real-time audio and video streams. Network packets may be lost, however, due to network burst traffic and images may be broken. Activate UDP connection when occasions require time-sensitive responses and the video quality is less important. Note that each unicast client connecting to the encoder takes up additional bandwidth and the encoder allows up to ten simultaneous accesses.
UDP multicast	A protocol that allows multicast-enabled routers to forward network packets to all clients requesting streaming media. This helps to reduce the network transmission load of the encoder while serving multiple clients at the same time. Note that to use this feature, the encoder must be configured to enable multicast streaming. For more information, see the “RTSP Streaming Settings” section on page 5-13 .
TCP	A protocol that guarantees the complete delivery of streaming data and thus provides better video quality. The downside of this protocol is that its real-time effect is not as good as that of the UDP protocol.
HTTP	A protocol that allows the same quality as the TCP protocol without the need to open specific ports for streaming under some network environments. Users inside a firewall can use this protocol to allow streaming data through.

MP4 Saving Options

To record live video as you are watching it, click the start MP4 recording button  on the home window. You can specify the storage destination and file name prefix for recorded videos on the Client settings window.

[Table 4-3](#) describes the MP4 Saving Options.

Table 4-3 **MP-4 Saving Options**

Option	Description
Folder	Click Browse and choose a storage destination for the recorded video files.
File name prefix	Enter text that will be appended to the front of the video file name.
Add date and time suffix to file name	Choose this option to append the date and time to the end of the file name.

Quadview Settings

These settings are available on the 4 port model (CIVS-SENC-4P) only.

The CIVS-SENC-4P encoder can support four analog cameras via its four channels. Each of the four channels supports a primary stream and a secondary stream. In Quadview, the user views four streams simultaneously, and for each channel the stream chosen can be either the primary or the secondary one. You can configure which video streams are displayed in the Quadview settings area (see [Figure 4-1](#)). The default is stream 2 with a lower resolution.

Figure 4-1 **Quadview Settings**

Quadview Settings

Select which stream to be used in Quad View Mode

Channel	Stream
1	2 ▼
2	2 ▼
3	2 ▼
4	2 ▼

Local Streaming Buffer Time

Due to unsteady bandwidth flow, live streaming may sometimes lack smoothness. If you enable the local streaming buffer time option, live streaming is stored on the camera buffer area for a specified period before playing in the live viewing window. This can improve streaming smoothness. The streaming delay value must be entered in milliseconds, so, for example, to set a 3 second streaming delay, enter 3000 Milliseconds.

Joystick Settings

Make sure a joystick is already attached to your COM port or USB port on your client computer.

[Table 4-4](#) describes the Joystick Setup options.

Table 4-4 Joystick Setup Options

Option	Description
Selected joystick	Choose the joystick you want to set up in the drop-down list.
Calibrate	Click this button to start Windows Game Controller function. If properly connected, your operating system should detect the joystick automatically. Follow the onscreen instructions to calibrate your joystick.
Configure buttons	Click this button to open a configuration dialog box and assign functions to individual joystick buttons. For more information about assigning functions to joystick buttons, see the “Assigning Functions to Joystick Buttons” section on page 4-4 .

Assigning Functions to Joystick Buttons

To assign functions to joystick buttons, perform the following procedure:


Note

For information about how to access the joystick settings, see the [“Joystick Settings” section on page 4-3](#).

Procedure

-
- Step 1** Click the down arrow button beside the Button field and choose the button to which you want to assign a function.
 - Step 2** Click the down arrow beside the Actions field and choose the action you want to assign to the button.
 - Step 3** Click **Assign**.
 - Step 4** (Optional) Repeat steps 1 to 3 to assign functions to other buttons.
-



CHAPTER 5

Configuration

This chapter describes the configuration options of the Cisco video surveillance encoders, models CIVS-SENC-4P and CIVS-SENC-8P, and includes the following sections:

- [Accessing Configuration Options, page 5-1](#)
- [System Window, page 5-2](#)
- [Security Window, page 5-3](#)
- [HTTPS Window, page 5-5](#)
- [SNMP Window, page 5-8](#)
- [Network Window, page 5-8](#)
- [Access List Settings, page 5-16](#)
- [Digital I/O Window, page 5-19](#)
- [Audio and Video Window, page 5-19](#)
- [Motion Detection Window, page 5-26](#)
- [Camera Tampering Detection Window, page 5-27](#)
- [Camera Control Window, page 5-28](#)
- [Homepage Layout Window, page 5-32](#)
- [Application Window, page 5-34](#)
- [System Log Window, page 5-42](#)
- [View Parameters Window, page 5-43](#)
- [Maintenance Window, page 5-43](#)

Accessing Configuration Options

You must have administrator rights to access the encoder configuration options. You can choose to display configuration options in one of two modes—Basic Mode or Advanced Mode. Advanced Mode displays all possible configuration options for the CIVS-SENC-4P and CIVS-SENC-8P encoder models, and Basic Mode displays a subset of all options.

To access configuration options, perform the following procedure:

Procedure

-
- Step 1** On the video encoder home window, click **Configuration**.
- Step 2** To switch between Basic Mode and Advanced Mode, click **Basic mode/Advanced mode** at the bottom of the left hand frame.
- Step 3** To go to the various configuration option windows, click the window name in the left hand frame.
-

System Window

This section describes the configuration options available on the System window, and contains the following topics:

- [System Settings, page 5-2](#)
- [System Time Settings, page 5-2](#)

For information about accessing the System window, see the [“Accessing Configuration Options” section on page 5-1](#).

When you have finished with the settings on this window, click **Save** to enable the settings.

System Settings

[Table 5-1](#) describes the System settings.

Table 5-1 **System Settings**

Option	Description
Host name	Enter a name for the encoder. The name is displayed at the top of the home window.
Turn off the LED indicator	If you do not want to let others know that the encoder is in operation, you can choose this option to turn off the LED indicators.

System Time Settings

[Table 5-2](#) describes the System Time settings.

Table 5-2 **System Time Settings**

Option	Description
Time zone	This setting is available in Advanced Mode only. Choose the appropriate time zone from the drop-down list. For information about uploading Daylight Savings Time rules on the Maintenance window, see the “Uploading Daylight Saving Time Rules” section on page 5-46 .
Keep current date and time	Choose this option to preserve the current date and time of the encoder. The internal real-time clock of the encoder maintains the date and time even when the system power is turned off.

Table 5-2 **System Time Settings (continued)**

Option	Description
Synchronize with computer time	Choose this option to synchronize the date and time of the encoder with the local computer. The read-only date and time of the local computer is displayed as updated.
Manual	The administrator can enter the date and time manually. Note that the date and time formats are [yyyy/mm/dd] and [hh:mm:ss].
Automatic	<p>The Network Time Protocol synchronizes computer clocks automatically by periodically querying an NTP Server.</p> <ul style="list-style-type: none"> • NTP server—Assign the IP address or domain name of the time server. Leaving the text box blank connects the encoder to the default time servers. • Update interval—Choose this setting to update the time using the NTP server on an hourly, daily, weekly, or monthly basis.

Security Window

This section describes the settings on the Security window, such as how to enable password protection and create multiple accounts. It includes the following topics:

- [Root Password Settings, page 5-3](#)
- [Manage Privilege Settings, page 5-3](#)
- [Manage User Settings, page 5-4](#)

For information about accessing the Security window, see the [“Accessing Configuration Options” section on page 5-1](#).

When you have finished with the settings on this window, click **Save** to enable the settings.

Root Password Settings

[Table 5-3](#) describes the Root Password settings.

Table 5-3 **Root Password Settings**

Option	Description
Root password	The administrator account name is “root”. This is permanent and cannot be deleted. If you want to add more accounts in the Manage User area, you must first set the password for the “root” account. Enter a root password in the Root password field and confirm it in the Confirm password field.

Manage Privilege Settings

This setting is available in Advanced Mode only.

[Table 5-4](#) describes the Manage Privilege settings.

Table 5-4 **Manage Privilege Settings**

Option	Description
Digital output	Choose to grant users operator or viewer privileges over digital output.
PTZ control	Choose to grant users operator or viewer privileges over camera PTZ controls. For more information about PTZ controls, see the “Camera Control Area” section on page 3-2 .
Allow anonymous viewing	If you choose this item, any client can access the live stream without entering a User ID and Password.

Manage User Settings

Administrators can add up to 20 user accounts. Access rights are sorted by user privilege—Administrator, Operator, and Viewer. Only administrators can access the Configuration window. Viewers can access only the home window for live viewing.

You can perform the following tasks to manage users:

- [Adding a User, page 5-4](#)
- [Modifying or Deleting a User Account, page 5-4](#)

Adding a User

To add a user, perform the following procedure:

Procedure

-
- | | |
|---------------|--|
| Step 1 | Choose Add new user in the Existing user name field. |
| Step 2 | Enter the new user name in the User name field. |
| Step 3 | Enter the new user password in the User password field. Enter the password again in the Confirm user password field. |
| Step 4 | Choose the privilege level for the new user account in the Privilege field. |
| Step 5 | Click Add to enable the setting. |
-

Modifying or Deleting a User Account

To modify or delete a user account:

Procedure

-
- | | |
|---------------|--|
| Step 1 | Choose the account you want to modify in the Existing user name field. |
| Step 2 | Do one of the following: |

- To modify the account: Make the required changes and click **Update**.
 - To delete the account: Click **Delete**.
-

HTTPS Window

This feature is available in Advanced Mode only.

This section describes how to enable authentication and encrypted communication over SSL (Secure Socket Layer). This helps protect streaming data transmission over the Internet by using a higher security level. This section contains the following topics:

- [Enable HTTPS Settings, page 5-5](#)
- [Create and Install Certificate Methods, page 5-5](#)
- [Cancel HTTPS Settings, page 5-7](#)
- [Remove a Signed Certificate, page 5-8](#)

When you have finished with the settings on this window, click **Save** to enable the settings.

Enable HTTPS Settings

To enable HTTPS communication, perform the following procedure:

Before you begin

Create and install a certificate. For more information, see [“Create and Install Certificate Methods” section on page 5-5](#).

Procedure

- | | |
|---------------|---|
| Step 1 | Choose Configuration > HTTPS . |
| Step 2 | Check the Enable HTTPS secure connection checkbox. |
| Step 3 | Choose a connection option— HTTP & HTTPS or HTTPS only . |
| Step 4 | Check one of the certificate creation checkboxes in the Create and install certificate method section. For more information, see “Create and Install Certificate Methods” section on page 5-5 . |
| Step 5 | Click Save . |
-

Create and Install Certificate Methods

Before using HTTPS for communication with the encoder, a certificate must be created. There are three options for creating and installing a certificate:

- [Creating a Self-signed Certificate Automatically, page 5-6](#)
- [Creating a Self-signed Certificate Manually, page 5-6](#)
- [Creating a Certificate Request and Install, page 5-7](#)

For information about removing certificates, see [“Remove a Signed Certificate”](#) section on page 5-8.

Creating a Self-signed Certificate Automatically

To create a self-signed certificate automatically, perform the following procedure:

Procedure

- Step 1** Choose **Configuration > HTTPS**.
- Step 2** Click the **Create self-signed certificate automatically** radio button.
- Step 3** In the Enable HTTPS section, check the **Enable HTTPS secure connection** checkbox, and then choose a connection option—**HTTP & HTTPS** or **HTTPS only**.
- Step 4** Click **Save** to generate a certificate.
The certificate Information is displayed automatically at the bottom of the window.
- Step 5** (Optional) To view detailed information about the certificate, click **Property** (see [Figure 5-1](#)).

Figure 5-1 Certificate Information

Certificate information

Status:	Active ▼
Country:	US
State or province:	California
Locality:	San Jose
Organization:	Cisco Systems Inc
Organization Unit:	Cisco Systems Inc
Common name:	www.cisco.com

Property
Remove

- Step 6** Click **Home** to return to the encoder home window.
- Step 7** Change the URL from “http://” to “https://” in the address bar and press **Enter** on your keyboard.
Security Alert dialog boxes may pop up.
- Step 8** Click **OK** or **Yes** to enable HTTPS.

Creating a Self-signed Certificate Manually

To create a self-signed certificate manually, perform the following procedure:

Procedure

- Step 1** Choose **Configuration > HTTPS**.
- Step 2** Click the **Create self-signed certificate manually** radio button.
- Step 3** Click **Create** to open the Create Certificate window.

- Step 4** Click **Save** to generate the certificate.
- The Certificate Information is displayed automatically at the bottom of the window.
- Step 5** (Optional) To view detailed information about the certificate, click **Property** (see [Figure 5-2](#)).

Figure 5-2 Certificate Information

The screenshot shows a window titled "Certificate information". It contains the following fields and values:

Status:	Active
Country:	US
State or province:	California
Locality:	San Jose
Organization:	Cisco Systems Inc
Organization Unit:	Cisco Systems Inc
Common name:	www.cisco.com

At the bottom of the window, there are two buttons: "Property" and "Remove".

Creating a Certificate Request and Install

Select this option if you want to create a certificate from a certificate authority.

To create a certificate request and install, perform the following procedure:

Procedure

- Step 1** Choose **Configuration > HTTPS**.
- Step 2** Click the **Create certificate request and install** radio button.
- Step 3** Click **Create** to open the Create Certificate window.
- Step 4** Click **Save** to generate the certificate.
- Step 5** If the browser pop-up window is displayed, click **OK**, and then click on the information bar at the top of the window to allow pop-ups.
- Step 6** Look for a trusted certificate authority that issues digital certificates, and enroll the encoder.
- Step 7** Wait for the certificate authority to issue a SSL certificate. To search for the issued certificate, click **Browse**, and then click **Upload**.

Cancel HTTPS Settings

To cancel HTTPS Settings, perform the following procedure:

Procedure

- Step 1** Choose **Configuration > HTTPS**.

- Step 2** Uncheck the **Enable HTTPS secure connection** checkbox.
- Step 3** Click **Save**.
A warning dialog box displays.
- Step 4** Click **OK** to disable HTTPS.
The web page redirects to a non-HTTPS page automatically.
-

Remove a Signed Certificate

If you want to create and install other certificates, you must first remove the existing one.

To remove a signed certificate, perform the following procedure:

Procedure

-
- Step 1** Choose **Configuration > HTTPS**.
- Step 2** Uncheck the **Enable HTTPS secure connection** checkbox.
- Step 3** Click **Save**.
- Step 4** Click **Remove** to erase the certificate.
- Step 5** Click **OK** to confirm that you want to remove the certificate.
-

SNMP Window

While SNMP is shown on the user interface, it is not currently supported by Cisco.

Network Window

This section describes the options for configuring a wired network connection for the encoder on the Network window, and it contains the following topics:

- [Network Type Settings, page 5-9](#)
- [IEEE 802.1x Settings, page 5-10](#)
- [HTTP Settings, page 5-12](#)
- [HTTPS Settings, page 5-13](#)
- [Two Way Audio Settings, page 5-13](#)
- [FTP Settings, page 5-13](#)
- [RTSP Streaming Settings, page 5-13](#)

For information about accessing the Network window, see the [“Accessing Configuration Options” section on page 5-1](#).

When you have finished with the settings on this window, click **Save** in the relevant section to enable the settings.

Network Type Settings

Table 5-5 describes the top-level options in the Network Type area:

Table 5-5 *Network Type Settings*

Option	Description
LAN	Choose this option when the encoder is deployed on a local area network (LAN) and is intended to be accessed by local computers. The default setting for the Network Type is LAN. For more information about LAN settings, see the “ LAN Settings ” section on page 5-9.
PPPoE	While PPPoE is shown on the user interface, it is not currently supported by Cisco.
Enable IPv6	While Enable IPv6 is shown on the user interface, it is not currently supported by Cisco.

LAN Settings

Table 5-6 describes the LAN settings.

Table 5-6 *LAN Settings*

Option	Description
Get IP address automatically	Choose this option to obtain an available dynamic IP address assigned by the DHCP server each time the encoder is connected to the LAN.
Use fixed IP address	Select this option to manually assign a static IP address to the video server. For more information about the Use fixed IP address settings, see the “ Use Fixed IP Address Settings ” section on page 5-9.
Enable UPnP presentation	While Enable UPnP presentation is shown on the user interface, it is not currently supported by Cisco.
Enable UPnP port forwarding	While Enable UPnP port forwarding is shown on the user interface, it is not currently supported by Cisco.



Note

If the default ports are already in use by other devices connected to the same router, the encoder will select other ports.

Use Fixed IP Address Settings

Table 5-7 describes the Use fixed IP address settings.

Table 5-7 Use Fixed IP Address Settings

Option	Description
IP address	This information is provided by your Network Administrator.
Subnet mask	This is used to determine if the destination is in the same subnet. The default value is 255.255.255.0. This information is provided by your Network Administrator
Default router	This is the gateway used to forward frames to destinations in a different subnet. An invalid router setting will prevent transmission to destinations in different subnet. This information is provided by your Network Administrator.
Primary DNS	The primary domain name server that translates hostnames into IP addresses. This information is provided by your Network Administrator.
Secondary DNS	A secondary domain name server that backs up the Primary DNS
Primary WINS server	The primary WINS server that maintains the database of computer names and IP addresses.
Secondary WINS server	The secondary WINS server that maintains the database of computer names and IP addresses.

Manually Setup the IP Address Settings

Choose this option to manually set up IPv6 settings if your network environment does not have DHCPv6 server and router advertisements-enabled routers. [Table 5-8](#) describes the information required when you choose this setting.

Table 5-8 Manual IP Address Setup Settings

Setting	Description
Optional IP address / Prefix length	Enter an optional IP address and prefix length.
Optional default router	Enter the address of the default router.
Optional primary DNS	Enter the primary DNS address.

IEEE 802.1x Settings

While IEEE 802.1x is shown on the user interface, it is not currently supported by Cisco.

QoS (Quality of Service) Settings

This feature is available in Advanced Mode only.

Quality of Service refers to a resource reservation control mechanism, which guarantees a certain quality to different services on the network. Quality of service guarantees are important if the network capacity is insufficient, especially for real-time streaming multimedia applications. Quality can be defined as, for example, a maintained level of bit rate, low latency, no packet dropping, and so on.

The following are the main benefits of a QoS-aware network:

- The ability to prioritize traffic and guarantee a certain level of performance to the data flow.
- The ability to control the amount of bandwidth each application may use, and thus provide higher reliability and more stability on the network.

To use QoS in a network environment, all network switches and routers in the network must include support for QoS. Also, the network video devices used in the network must be QoS-enabled.

The following two QoS models are available:

- [CoS \(The VLAN 802.1p Model\)](#), page 5-11
- [QoS/DSCP \(The DiffServ Model\)](#), page 5-11

CoS (The VLAN 802.1p Model)

IEEE802.1p defines a QoS model at OSI Layer 2 (Data Link Layer), which is called CoS (Class of Service). It adds a 3-bit value to the VLAN MAC header, which indicates prioritization from 0~7 (eight different classes of service are available). The priority is set up on the network switches, which then use different queuing disciplines to forward the packets.

[Table 5-9](#) describes the settings that are required when you choose CoS.

Table 5-9 CoS Settings

Setting	Description
VLAN ID	Enter the VLAN ID of your switch (from 0 to 4095).
Live video	Choose the priority for the live video application (from 0 to 7).
Live audio	Choose the priority for the live video audio (from 0 to 7).
Event/Alarm	Choose the priority for the event/alarm application (from 0 to 7).
Management	Choose the priority for the management application (from 0 to 7).

If you assign Video the highest level, the switch will handle video packets first.



Note

Consider the following points:

- Web browsing may fail if the CoS setting is incorrect.
- Class of Service technologies do not guarantee a level of service in terms of bandwidth and delivery time; they offer a "best-effort." Users can think of CoS as "coarsely-grained" traffic control and QoS as "finely-grained" traffic control.
- Although CoS is simple to manage, it lacks scalability and does not offer end-to-end guarantees since it is based on L2 protocol.

QoS/DSCP (The DiffServ Model)

DSCP-ECN defines QoS at Layer 3 (Network Layer). The Differentiated Services (DiffServ) model is based on packet marking and router 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. It gives an indication of how a given packet is to be forwarded, known as the Per Hop Behavior (PHB). The PHB describes a particular service level in terms of bandwidth, queueing theory,

and dropping (discarding the packet) decisions. Routers at each network node classify packets according to their DSCP value and give them a particular forwarding treatment; for example, how much bandwidth to reserve for it.

[Table 5-10](#) describes the settings that are required when you choose QoS/DSCP.

Table 5-10 QoS/DSCP Settings

Setting	Description
Live video	Enter the DSCP value for the live video application.
Live audio	Enter the DSCP value for the live audio application.
Event/Alarm	Enter the DSCP value for the event/alarm application.
Management	Enter the DSCP value for the management application.

HTTP Settings

This feature is available in Advanced Mode only.

To use HTTP authentication, make sure you have set a password for the encoder. For more information, see the [“Security Window” section on page 5-3](#).

[Table 5-11](#) describes the HTTP settings.

Table 5-11 HTTP Settings

Setting	Description
Authentication	Depending on your network security requirements, the encoder provides two types of security settings for an HTTP transaction: basic and digest. If basic authentication is selected, the password is sent in plain text format and there is a potential risk that it could be intercepted. If digest authentication is selected, user credentials are encrypted using the MD5 algorithm, which provides better protection against unauthorized accesses.
HTTP port/Secondary HTTP port	By default, the HTTP port is set to 80 and the secondary HTTP port is set to 8080. These can also be assigned to another port number between 1025 and 65535. If the ports are incorrectly assigned, warning messages are displayed. Both the HTTP port and secondary HTTP port can be used to access the encoder on the LAN. For example, when the HTTP port is set to 80 and the secondary HTTP port is set to 8080, the IP address of the encoder might be as follows: http://192.168.4.160 or http://192.168.4.160:8080
Access Name	Enter access names for channel 1 to 4/8. The CIVS-SENC-4P encoder model supports four channels for live video viewing, and the CIVS-SENC-8P model supports eight channels. Each channel allows you to view only one stream. The access name is used to differentiate the streaming source. To manage the video quality of linked streams, go to Configuration > Audio and video > Video settings .

HTTPS Settings

By default, the HTTPS port is set to 443. It can also be assigned to another port number between 1025 and 65535.

Two Way Audio Settings

By default, the two way audio port is set to 5060. It can also be assigned to another port number between 1025 and 65535.

The encoder supports two way audio communication so that operators can transmit and receive audio simultaneously. By using the built-in or external microphone and an external speaker, you can communicate with people around the encoder.








Note

As JPEG only transmits a series of JPEG images to the client, to enable the two-way audio function, you must make sure the video mode is set to “MPEG-4” on the Audio and video settings window and the media option is set to “Video and Audio” on the Client settings window. For more information, see the “Client Settings” section on page 4-1 and the “Audio and Video Window” section on page 5-19.

Table 5-12 describes the Two Way Audio control buttons that are available on the encoder home window.

Table 5-12 Two Way Audio Control Buttons

Button	Description
	Talk—Click this button enable audio transmission to the encoder. Click  again to end talking transmission.
	Broadcast—Click this button to broadcast.
	Mic Volume—Click this to adjust the mic volume.
	Mute—Click this to turn off the audio.

FTP Settings

The FTP server allows the user to save recorded video clips. By default, the FTP port is set to 21. It can also be assigned to another port number between 1025 and 65535.

RTSP Streaming Settings

To use RTSP streaming authentication, make sure that you have set a password for the encoder. For more information about setting a password, see the “Security Window” section on page 5-3.

Table 5-13 describes the RTSP Streaming settings.

Table 5-13 RTSP Streaming Settings

Setting	Description
Authentication	<p>Depending on your network security requirements, the encoder provides three types of security settings for streaming via RTSP protocol: disable, basic, and digest.</p> <ul style="list-style-type: none"> • Disable—No password is required when this option is selected. • Basic—The password is sent in plain text format, but there is a potential risk of it being intercepted. • Digest—User credentials are encrypted using MD5 algorithm, thus reducing the risk of unauthorized access. <p>Note To secure access to the video stream, it is recommended that you apply the Basic authentication setting.</p> <p>Table 5-14 describes the availability of RTSP streaming for the three authentication modes.</p>
Access name for channel 1 ~ 4/8	The CIVS-SENC-4P encoder model supports four channels for live video viewing and the CIVS-SENC-8P model supports eight channels. Each channel allows you to view only one stream. The access name is used to differentiate the streaming source.
RTSP port	RTSP (Real-Time Streaming Protocol) controls the delivery of streaming media. By default, the port number is set to 554. This port can be changed to a value between 1025 and 65535.
RTP port for video	<p>RTP (Real-time Transport Protocol) is used to deliver video and audio data to clients. By default, the RTP port for video is set to 5556.</p> <p>This port can be changed to a value between 1025 and 65535, but the RTP port must be an even number.</p>
RTCP port for video	<p>RTCP (Real-time Transport Control Protocol) allows the encoder to transmit data by monitoring the Internet traffic volume. By default, the RTCP port for video is set to 5557.</p> <p>The RTCP port is the RTP port number plus one, so it is always an odd number. When the RTP port changes, the RTCP port changes accordingly.</p>
RTP port for audio	<p>RTP (Real-time Transport Protocol) is used to deliver video and audio data to clients. By default, the RTP port for audio is set to 5558.</p> <p>This port can be changed to a value between 1025 and 65535, but the RTP port must be an even number.</p>

Table 5-13 RTSP Streaming Settings (continued)

Setting	Description
RTCP port for audio	<p>RTCP (Real-time Transport Control Protocol) allows the encoder to transmit data by monitoring the Internet traffic volume. By default, the RTCP port for audio is set to 5559.</p> <p>The RTCP port is the RTP port number plus one, so it is always an odd number. When the RTP port changes, the RTCP port changes accordingly.</p>
Multicast settings for channel 1 ~ 4/8	<p>Click the top-level items to display detailed configuration information.</p> <p>Unicast video transmission delivers a stream through point-to-point transmission. Multicast, on the other hand, sends a stream to the multicast group address and allows multiple clients to acquire the stream at the same time by requesting a copy from the multicast group address. Enabling multicast, therefore, can effectively save Internet bandwidth.</p> <p>Table 5-15 describes the Multicast setting fields.</p>

Table 5-14 Availability of RTSP Streaming

Setting	Quick Time Player	Real Player
Disable	O	O
Basic	O	O
Digest	O	X

Table 5-15 Multicast Settings

Setting	Description
Always multicast	Choose this to enable multicasting for a channel.
Multicast group address	Enter a multicast group address.
Multicast video port	This port can be changed to a value between 1025 and 65535.
Multicast RTCP video port	<p>Multicast RTCP (RTCP (Real-time Transport Control Protocol) video port.</p> <p>This port can be changed to a value between 1025 and 65535. The RTCP port is the RTP port number plus one, so it is always an odd number. When the RTP port changes, the RTCP port changes accordingly.</p>
Multicast audio port	This port can be changed to a value between 1025 and 65535.
Multicast RTCP audio port	<p>Multicast RTCP (RTCP (Real-time Transport Control Protocol) audio port.</p> <p>This port can be changed to a value between 1025 and 65535. The RTCP port is the RTP port number plus one, so it is always an odd number. When the RTP port changes, the RTCP port changes accordingly.</p>
Multicast TTL [1 ~ 255]	The multicast TTL (Time To Live) is the value that tells the router the range over which a packet can be forwarded.

Using an RTSP Player to Access the Encoder

If you want to use an RTSP player to access the encoder, you must set the video mode to MPEG-4 and use the following RTSP URL command to request transmission of the streaming data:

rtsp://ip-address:rtsp-port/access-name-for-stream1~channel-1~4/8

The following example procedure shows how to request transmission of streaming data when the access name for stream 1 is set to “live.sdp”:

Procedure

-
- | | |
|---------------|---|
| Step 1 | Open an RTSP player. |
| Step 2 | Choose File > Open URL .
A URL dialog box is displayed. |
| Step 3 | Enter the URL command in the text box in the following format:
rtsp://ip-address:rtsp-port/access-name-for-stream1~channel-1~4/8
For example: rtsp://192.168.5.151:554/live.sdp |
| Step 4 | Click OK .
The live video is displayed in your player. |
-

Access List Settings

This feature is available in Advanced Mode only.

This describes configuration options available on the Access list window, including how to control access permission by verifying the client PC IP address. It contains the following topics:

- [General Access List Settings, page 5-16](#)
- [Filter Type Settings, page 5-18](#)
- [Filter, page 5-18](#)
- [Administrator IP Address, page 5-18](#)

For information about accessing the Access list window, see the “[Accessing Configuration Options](#)” section on page 5-1.

When you have finished with the settings on this window, click **Save** to enable the settings.

General Access List Settings

[Table 5-16](#) describes the General access list settings.

Table 5-16 General Settings

Setting	Description
Maximum number of concurrent streaming connection(s) limited to	Allows simultaneous live viewing for 1~10 clients (including stream 1 and stream 2). The default value is 10. If you modify the value and click Save, all current connections are disconnected and automatically attempt to re-link (IE Explore or Quick Time Player).
View Information	Click this button to display the connection status window showing a list of the current connections. For more information about current streaming connection information, see the “Current Streaming Connection Information” section on page 5-17 .
Enable access list filtering	Check this item and click Save to enable the access list filtering function.

Current Streaming Connection Information

[Table 5-17](#) describes the features of the Connection Status window.

Table 5-17 Connection Status Information

Setting	Description
IP address	Current connections to the encoder.
Elapsed time	The amount of time for which the client has been at the webpage
User ID	<p>If the administrator has set a password for the webpage, clients must enter a user name and password to access the live video. The Client user name is displayed in the User ID column. If the administrator allows clients to link to the webpage without a user name and password, the User ID column remains empty.</p> <p>Clients are allowed access to the live video without a user name and password in the following situations:</p> <ul style="list-style-type: none"> The administrator does not set up a root password. For more information about how to set up a root password and manage user accounts, see the “Security Window” section on page 5-3. The administrator has set up a root password, but set RTSP authentication to “disable”. For more information about RTSP authentication, see the “RTSP Streaming Settings” section on page 5-13. The administrator has set up a root password, but allows anonymous viewing. For more information about Allow Anonymous Viewing, see the “Security Window” section on page 5-3.
Refresh	Click this button to refresh all current connections.

Table 5-17 **Connection Status Information (continued)**

Setting	Description
Add to deny list	You can select entries from the Connection Status list and add them to the Deny List to deny access. Note that these connections are only disconnected temporarily and will try to re-link again automatically (in IE Explore or Quick Time Player). If you want to enable the denied list, check the Enable access list filtering checkbox (see Table 5-16) and then click Save in the General settings area.
Disconnect	To break off a current connection, select the connection, and then click Disconnect . Note that these connections are only disconnected temporarily and will try to re-link again automatically (in IE Explore or Quick Time Player).

Filter Type Settings

Select **Allow** or **Deny** as the filter type. If you choose the Allow filter type, only those clients whose IP addresses are on the Access List can access the Network Camera. If you choose the Deny filter type, those clients whose IP addresses are on the Access List are not allowed to access the Network Camera, while other clients can access it.

Filter

Once you have selected a filter type, you can then add a rule to the Access list. To add a filter rule to the Allowed/Denied list, perform the following procedure:

Procedure

-
- Step 1** Choose **Configuration > Access list**.
- Step 2** Click **Add** in the Filter area.
- Step 3** Choose one of the following rule types from the Rule drop-down list:
- **Single**. Then add the IP address that is to be added to the Allowed/Denied list in the IP address field.
 - **Network**. Then add the network address and network mask to the Network address/Network mask fields.
 - **Range**. Then add the two IP addresses that make up the beginning and end of the IP address range.
- Step 4** Click **OK**.
-

Administrator IP Address

Choose the **Always allow the IP address to access this device** checkbox and enter the IP address that is to be given access.

Digital I/O Window

This section describes how to change digital input and digital output settings, and it contains the following topics:

- [Digital Input Settings, page 5-19](#)
- [Digital Output Settings, page 5-19](#)

For information about accessing the Digital I/O window, see the [“Accessing Configuration Options” section on page 5-1](#).

When you have finished with the settings on this window, click **Save** to enable the settings.

Digital Input Settings

You can select High or Low to define normal status for the digital input. The encoder displays the current status.

Digital Output Settings

You can select Grounded or Open to define normal status for the digital output. The encoder displays whether or not the trigger is activated.

Audio and Video Window

This section describes how to configure the audio and video settings of the encoder on the Audio and video window, and it includes the following topics:

- [Audio and Video Settings Overview, page 5-19](#)
- [Video Settings, page 5-20](#)
- [Audio Settings, page 5-25](#)

For information about accessing the Audio and video window, see the [“Accessing Configuration Options” section on page 5-1](#).

When you have finished with the settings on this window, click **Save** to enable the settings.

Audio and Video Settings Overview

Click **Overview** at the top of the Audio and video window to see all current stream settings for each channel. See [Figure 5-3](#).

Figure 5-3 Channel Stream Settings

Overview:

Channel	Stream	Codec	Modulation	Frame size	Maximum frame rate	Intra frame period	Bitrate/Quality
1	1	H264	NTSC	QCIF- >176x120	1	1 S	Good
2	1	H264	NTSC	4CIF	20	1 S	Good
3	1	H264	NTSC	4CIF	20	1 S	Good
4	1	H264	NTSC	4CIF	20	1 S	Good
5	1	MJPEG	NTSC	D1	20	N/A	Good
6	1	H264	NTSC	4CIF	20	1 S	Good
7	1	H264	NTSC	4CIF	20	1 S	Good
8	1	H264	NTSC	4CIF	20	1 S	Good

Video Settings

You can choose from channels 1~4 or 8. Select one channel in the Channel drop-down list. You can then select video settings for that channel in the section below the drop-down list. [Table 5-18](#) describes the Video settings.

Table 5-18 Video Settings

Setting	Description
Check frame rate	Choose this to display the current available frame rate status for all frame sizes. For more information, see the “Available FPS” section on page 5-25 .
Video title	The name you enter is displayed on the title bar of the live video.
Color	Choose to display color or black/white video streams.
Video orientation	Choose Flip (vertically reflects the display of the live video) or Mirror (horizontally reflects the display of the live video). Choose both options if the linked device is installed upside-down (for example, on the ceiling) to correct the image orientation.
Overlay title and time stamp on video and snapshot	Choose this option to place the video title and time on the video streams.
Enable time shift caching stream	This feature is available in Advanced Mode only. Choose this item to enable the time shift cache stream on the encoder. This stores video in the embedded memory of the video server for a period of time depending on the cache memory size of each encoder. When an event occurs, the recording software can request time shift cache stream from the camera, which allows the user to retrieve pre-event video data.

Table 5-18 Video Settings (continued)

Setting	Description
Image Settings	This feature is available in Advanced Mode only. For more information, see the “Image Settings” section on page 5-21 .
Privacy Mask	This feature is available in Advanced Mode only. For more information, see the “Privacy Mask” section on page 5-22 .
Video Quality Settings for Stream 1	This feature is available in Advanced Mode only. For more information, see the “Video Quality Settings for Stream 1” section on page 5-22 .
Video Quality Settings for Stream 2	This feature is available in Advanced Mode only, and only on the CIVS-SENC-4P encoder model. For more information, see the “Video Quality Settings for Stream 1” section on page 5-22 .

Image Settings

Click **Image Settings** to open the Image Settings window. On this window, you can tune white balance, brightness, saturation, contrast, and sharpness settings for the video. Before tuning video settings, you must first choose a channel to which the settings will apply from the Channel drop-down list.

When you have finished with the settings on this window, click **Save** to enable the settings.

[Table 5-19](#) describes the options available on the Image Settings window.

Table 5-19 Image Settings

Setting	Description
Brightness	To adjust the image brightness level, drag the slider to the right (+) to increase the effect or to the left (-) to reduce the effect.
Saturation	To adjust the image saturation level, drag the slider to the right (+) to increase the effect or to the left(-) to reduce the effect.
Contrast	To adjust the image contrast level, drag the slider to the right (+) to increase the effect or to the left(-) to reduce the effect.
Sharpness	To adjust the image sharpness level, drag the slider to the right (+) to increase the effect, or to the left(-) to reduce the effect.
X-offset	Adjust the image to the proper position horizontally.
Y-offset	Adjust the image to the proper position vertically.
Enable deinterlace	Check to enable deinterlace, and choose Adaptive or Blend in the Mode drop-down list. Adaptive mode provides the best image quality, while Blend mode provides image quality that is better than not using the deinterlace function at all.
Enable edge enhancement	Check to enable edge enhancement, and drag the slider bar to adjust the strength.

Table 5-19 *Image Settings (continued)*

Setting	Description
Enable noise reduction	Check to enable noise reduction. You can also choose to reduce Gaussian noise, impulse noise, or Gaussian and impulse noise in the Remove noise drop-down list. Drag the slider to adjust the strength.
Restore	Click to restore the default setting.

**Note**

Applying Enable deinterlace, Enable edge enhancement, or Enable noise reduction to all channels at the same time will consume quite a lot computing power.

Privacy Mask

You can add a masking window to the video feed to block out sensitive zones to address privacy concerns.

To add a privacy mask, perform the following procedure:

Procedure

- Step 1** Click **Privacy Mask** to open the Privacy Mask settings window.
- Step 2** Choose a channel in the Channel drop-down list.
- Step 3** Click **New** to add a new window.
- Step 4** Drag and drop with the mouse to size and place the masking window. This window should be at least twice the size of the object (height and width) you want to cover.
- Step 5** Click in the **Window name** field and enter a window name.
- Step 6** Click **Save** to save the setting.
- Step 7** Check the **Enable privacy mask** checkbox to enable the function.

**Note**

Consider the following points:

- Up to five privacy mask windows can be set up on the same screen.
- To delete a privacy mask window, click the 'x' button on the upper right corner of the window.

Video Quality Settings for Stream 1

This feature is available in Advanced Mode only.

The CIVS-SENC-4P encoder model allows you to configure video quality settings for streams 1 and 2. The CIVS-SENC-8P model only permits the configuration of video quality settings for stream 1. For information about Available FPS data, see [“Available FPS” section on page 5-25](#).

[Table 5-20](#) describes the video quality settings for stream 1. The same settings also apply to stream 2 on the CIVS-SENC-4P encoder model.

Table 5-20 Video Quality Settings for Stream 1 (and 2)

Setting	Description
Enable aspect ratio correction	<p>By default, the size of the video window changes according to the layout of the live viewing window you choose. The frame size may be distorted, however. If you choose Enable aspect ratio correction, the video window is adjusted to the same frame size as the preview window. This function is disabled by default.</p> <p>Please note the following:</p> <ul style="list-style-type: none"> Aspect ratio correction doesn't support QCIF. When aspect ratio correction takes effect, the frame size for D1 is adjusted to 640x480.
MPEG-4	If MPEG-4 mode is selected, the video is streamed via RTSP protocol. Table 5-21 describes the parameters that can be set to adjust video performance.
H.264	If H.264 mode is selected, the video is streamed via RTSP protocol. Table 5-21 describes the parameters that can be set to adjust video performance.
JPEG	If JPEG mode is selected, the encoder continuously sends JPEG images to the client, producing a moving effect similar to a filmstrip. Every single JPEG image transmitted guarantees the same image quality, which in turn comes at the expense of variable bandwidth usage. Because the media contents are a combination of JPEG images, no audio data is transmitted to the client. Table 5-22 describes the parameters that can be set to adjust video performance.

Table 5-21 MPEG-4 and H.264 Settings

Setting	Description
Frame size	You can set up different video resolutions for different viewing devices. For example, set a smaller frame size and lower bit rate for remote viewing on mobile phones and a larger video size and a higher bit rate for live viewing on web browsers. Note that a larger frame size takes up more bandwidth. The following frame size resolutions are available: QCIF, CIF, 4CIF, and D1.
Maximum frame rate	This limits the maximum refresh frame rate per second. Set the frame rate higher for smoother video quality. You can also choose Customize and manually enter a value. The frame rate decreases if you select a higher resolution.

Table 5-21 MPEG-4 and H.264 Settings (continued)

Setting	Description
Intra frame period	Determine how often to plant an I frame. The shorter the duration, the more likely you are to get better video quality, but at the cost of higher network bandwidth consumption. Select the intra frame period from the following durations: 1/4 second, 1/2 second, 1 second, 2 seconds, 3 seconds, and 4 seconds.
Video quality	<p>A complex scene generally produces a larger file size, meaning that higher bandwidth is needed for data transmission.</p> <p>If Constant bit rate is selected, therefore, the bandwidth use is fixed at a selected level, resulting in mutable video quality performance. The following bit rates are available: 20Kbps, 30Kbps, 40Kbps, 50Kbps, 64Kbps, 128Kbps, 256Kbps, 512Kbps, 768Kbps, 1Mbps, 2Mbps, 3Mbps, and 4Mbps. You can also select Customize and enter a value manually.</p> <p>If Fixed quality is selected, all frames are transmitted with the same quality, and bandwidth use is therefore unpredictable. Video quality can be adjusted to the following settings: Medium, Standard, Good, Detailed, and Excellent. You can also select Customize and adjust the slider bar manually. You can adjust the slider bar to the right to achieve better video quality.</p>

Table 5-22 JPEG Settings

Setting	Description
Frame size	You can set up different video resolutions for different viewing devices. For example, set a smaller frame size and lower bit rate for remote viewing on mobile phones and a larger video size and a higher bit rate for live viewing on web browsers. Note that a larger frame size takes up more bandwidth. The following frame size resolutions are available: QCIF, CIF, 4CIF, and D1.
Maximum frame rate	This limits the maximum refresh frame rate per second. Set the frame rate higher for smoother video quality. You can also select Customize and enter a value manually. The frame rate decreases if you select a higher resolution.
Video quality	Video quality can be adjusted to the following settings: Medium, Standard, Good, Detailed, and Excellent. You can also select Customize and enter a value manually.

**Note**

Consider the following points:

- Video quality and fixed quality refer to the compression rate, so a lower value will produce higher quality.
- Converting high-quality video may significantly increase the CPU loading, and you may encounter streaming disconnection or video loss while capturing a complicated scene. If this occurs, we suggest you customize to a lower video resolution or reduce the frame rate to obtain smooth video.

Available FPS

Choose the **Check frame rate** checkbox at the top of the Audio and video window to display the current available frame rate status (Available FPS). Available FPS provides information about the unused encoding capability, with available frame rates in different frame sizes. See [Figure 5-4](#).

Figure 5-4 Available FPS

Video quality settings for stream 1:

☐ Enable aspect ratio correction

☐ MPEG-4:

☒ H.264:

Frame size:

Maximum frame rate:

Intra frame period:

Video quality:

☐ Constant bit rate:

☒ Fixed quality:

☐ JPEG:

Available FPS	
D1:	24 FPS
4CIF:	28 FPS
CIF:	112 FPS
QCIF:	449 FPS

The embedded Soc (System-on-Chip) has limited encoding capability, so you may set the video quality according to the available FPS. Due to the limited encoding capability, the maximum frame rate that can be supported for 4CIF in H.264 or MPEG-4 codec is up to 24 FPS, when all channels are in use and have this setting applied. If the total frame rate exceeds encoding capability, a warning message "Frame rate is not guaranteed" is displayed in a pop-up window. Also, the frame rate that cannot be reached for each stream is marked in red in the Maximum frame rate drop-down list.

Audio Settings

[Table 5-23](#) describes the audio settings.

Table 5-23 Audio Settings

Setting	Description
Mute	Choose this option to disable audio transmission from the encoder to all clients. Note that if mute mode is turned on, no audio data is transmitted, even if audio transmission is enabled on the Client Settings window. In that case, a message is displayed.
External microphone input	Choose the gain of the internal audio input according to ambient conditions. Adjust the gain from +9 db (most sensitive) ~ -12 db (least sensitive).
G.711 Mode	G.711 also provides good sound quality and requires approximately 64Kbps. Choose pcmu (Pulse code Modulation μ -Law) or pcma (Pulse code Modulation A-Law) mode.
Save	Choose the channel(s) to which you want the audio settings to apply in the drop-down list. You can choose Current channel, All channels, Current channel and channel 2, and so on. Click Save to enable your settings.

Motion Detection Window

This section describes how to configure the encoder to enable motion detection by configuring motion detection windows. A total of three motion detection windows can be configured for each channel. For information about how motion detection works, see the [“How Motion Detection Works” section on page 5-27](#).

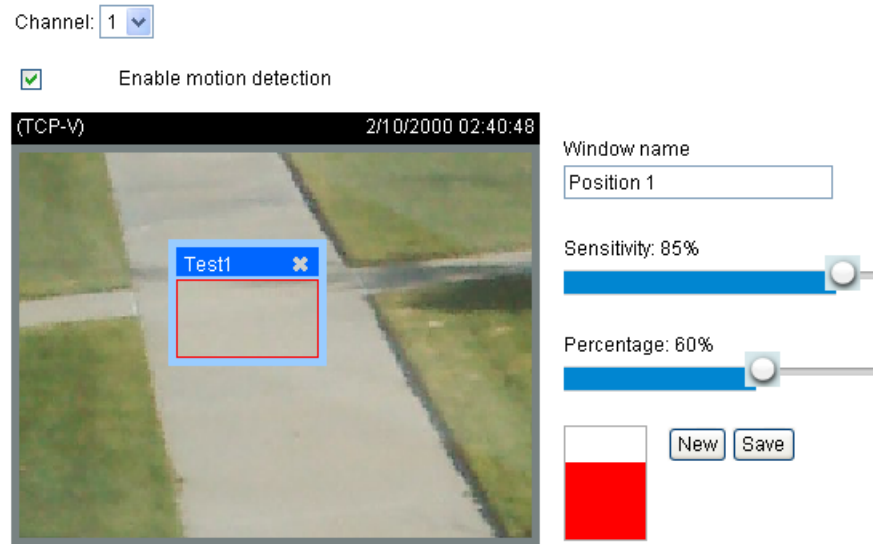
To enable motion detection, perform the following procedure:

Procedure

-
- Step 1** Choose **Configuration > Motion detection**.
 - Step 2** Choose a channel in the Channel drop-down box.
 - Step 3** Click **New** to add a new motion detection window.
 - Step 4** Click in the Window name field and enter a name for the motion detection window.
 - Step 5** To move the window, click on it and drag it to the desired location.
 - Step 6** To resize the window, click on any of the sides and drag it.
 - Step 7** To delete window, click **X** in the upper right corner of the window.
 - Step 8** To define the sensitivity to moving objects and the space ratio of all alerted pixels, move the **Sensitivity** and **Percentage** slider bars.
 - Step 9** Click **Save** to enable your settings.
 - Step 10** Check **Enable motion detection** to enable this function.
-

The percentage indicator rises or falls depending on the variation between sequential images. When motion is detected by the network camera and it is judged to exceed the defined threshold, the red bar rises. Meanwhile, the motion detection window is outlined in red. See [Figure 5-5](#).

Photos or videos can be captured instantly and configured to be sent to a remote server (via Email or FTP) by using this feature as a trigger source. For more information about setting an event, see the [“Application Window” section on page 5-34](#).

Figure 5-5 Motion Detection Window

A green bar indicates that even though motion has been detected, an event has not been triggered because the image variations still fall below the defined threshold.

The motion detection window is also displayed on the Event Settings window. To set a trigger event, choose **Application > Event Settings > Trigger**. For more information, see the [“Event Settings” section on page 5-35](#).

How Motion Detection Works

There are two motion detection parameters: Sensitivity and Percentage. Sensitivity is a value that expresses sensitivity to moving objects, and percentage is a value that expresses the proportion of “alerted pixels” to the total number of pixels in a motion detection window.

Motion is represented by pixel differences between sequential frames within the area of a motion detection window. The pixel differences between two frames are first compared against the sensitivity setting. Higher sensitivity settings are expected to detect slight movements, while lower sensitivity settings neglect small movements. When the sensitivity is set to 85%, for example, the Network Camera defines even those pixels that have experienced only slight change as “alerted pixels”. See [Figure 5-5](#).

If, for example, the percentage is set to 60% and 85% of pixels are identified as “alerted pixels”, as the motions are therefore judged to exceed the defined threshold, the motion window is outlined in red, and an event may be triggered.

For applications that require a high level of security management, it is suggested that you use higher sensitivity settings and lower percentage values.

Camera Tampering Detection Window

This section describes how to set up camera tampering detection. With tampering detection, the camera is capable of detecting incidents such as redirection, blocking or defocusing, or even spray painting.

To set up camera tampering detection, perform the following procedure:

Procedure

-
- Step 1** Click the **Enable** checkbox for any channel.
- Step 2** Enter the trigger duration (10 sec. ~ 10 min.).
- The alarm is triggered only when the tampering factor (the difference between current frame and pre-saved background) exceeds the trigger threshold.
- Step 3** Choose **Application > Event settings > Trigger**, and set the event source as Camera tampering detection On. For more information, see the [“Event Settings” section on page 5-35](#).
- Step 4** Click **Save**.
-

Camera Control Window

This section describes how to control the Pan/Tilt/Zoom operation of the Network Camera by connecting to a PTZ driver or camera via RS485 interface. It includes the following topics:

- [RS485 Settings, page 5-28](#)
- [Configuring Camera Patrol Settings, page 5-30](#)
- [Customization Settings, page 5-29](#)

For information about accessing the Camera control window, see the [“Accessing Configuration Options” section on page 5-1](#).

When you have finished with the settings on this window, click **Save** to enable the settings.

RS485 Settings

[Table 5-24](#) describes the RS485 settings:

Table 5-24 *RS485 Settings*

Setting	Description
Disable	Choose this option to disable the camera control function.
PTZ camera	Choose this option to enable PTZ operation. To use this feature, connect the Network Camera to a PTZ driver or camera via an RS485 interface first. Table 5-25 describes the settings for configuring the PTZ driver and the RS485 port.
Transparent HTTP tunnel	If you want to use your own RS-485 device, you can use UART commands to build a Transparent HTTP Tunnel. The UART commands are sent through a HTTP tunnel established between the RS-485 device and the linked camera. Table 5-26 describes the Transparent HTTP tunnel settings

Table 5-25 PTZ camera Settings

Setting	Description
PTZ driver	Choose a PTZ driver from the drop-down list.
Baud rate	Choose the baud rate to be configured.
Data bits	Choose the data bit level to be configured.
Stop bits	Choose the stop bit level to be configured.
Parity bit	Choose the parity bit level to be configured.

Table 5-26 Transparent HTTP Tunnel Settings

Setting	Description
Baud rate	Choose the baud rate to be configured.
Data bits	Choose the data bit level to be configured.
Stop bits	Choose the stop bit level to be configured.
Parity bit	Choose the parity bit level to be configured.

Camera ID Settings

The following five PTZ drivers are available:

- DynaDome/SmartDOME
- Lilin PIH-7x00
- Pelco D protocol
- Pelco P protocol
- Samsung scc643 protocol

**Note**

Only the Pelco D protocol driver is currently supported by Cisco.

If none of the above PTZ drivers is supported by your PTZ camera, choose **Custom camera** in the PTZ driver drop-down list (see the PTZ camera entry in [Table 5-25](#)). Refer to the user guide of your PTZ camera to determine the Camera ID, PTZ driver, and Port settings. The Camera ID is required to control multiple cameras. When you click Save to enable this function, the camera control panel is displayed on the home window.

Customization Settings

This section contains the following topics:

- [Configuring Camera Preset Positions, page 5-30](#)
- [Configuring Camera Patrol Settings, page 5-30](#)
- [Configuring Custom Commands, page 5-31](#)

Configuring Camera Preset Positions

If you select DynaDome/SmartDOME, Lilin PIH-7x00, Pelco D, Pelco P protocol, or Samsung scc643 protocol as the PTZ driver and click the Save button, the Preset position button at the bottom of the Camera control window is enabled. This button opens the Preset position window, from where you can configure up to 20 preset positions for the camera.

To configure a preset position, perform the following procedure:

Procedure

-
- Step 1** Choose **Configuration > Camera control**.
- Step 2** Click the **PTZ camera** radio button in the RS485 settings area, and then select one of the following in the PTZ driver drop-down list:
- **DynaDome/SmartDome**
 - **Lilin PIH-7x00**
 - **Pelco D protocol**
 - **Pelco p protocol**
 - **Samsung scc643 protocol**



Note

Only the Pelco D protocol driver is currently supported by Cisco.


- Step 3** Click the **Preset Position** button at the bottom of the window.
- Step 4** In the Preset position dialog box, choose a channel in the Channel drop-down list.
- Step 5** Use the buttons on the right hand side of the dialog box to adjust the shooting area to the desired position. The default Home position is set as the center position.
- The control functions are the same as those on the home window control panel. For more information, see the [“Camera Control Area” section on page 3-2](#).
- Step 6** Click in the **Name** field and enter a name for the preset position. This field allows up to forty characters.
- Step 7** Click **Add** to enable the settings.
- The preset positions are displayed in the User preset locations list.
- Step 8** To add additional preset positions, repeat steps 6 to 7.
- Step 9** To configure the current camera position as the home location, click **Set current position as home**. To reset the home location to the center position, click **Restore home position to default**.
- Step 10** Choose the preset positions and click **Save** to enable the settings.
- The saved preset positions are available in the Go to drop-down list on the Home window. See the [“Home Window Overview” section on page 3-1](#).
- Step 11** To remove a preset position from the list, choose it, and click **Remove**.
-

Configuring Camera Patrol Settings

You can select some preset positions for the Network Camera to patrol.

To set up a patrol schedule, perform the following procedure:

Procedure

-
- Step 1** Choose **Configuration > Camera control**.
 - Step 2** If you have not configured camera preset positions, see the [“Customization Settings” section on page 5-29](#).
 - Step 3** Click **Preset position**.
 - Step 4** Select the preset locations you want to patrol in the User preset locations list, and click .
The selected preset locations are displayed in the Patrol locations list.
 - Step 5** In the Patrol locations list, set the Dwelling time (in seconds) for each preset location during auto patrol.
 - Step 6** (Optional) To delete a preset location from the Patrol locations list, select it, and click **Remove**.
 - Step 7** To arrange the patrol order for your preset locations, select each location individually, and click the up and down buttons at the bottom of the Patrol locations list to move each one to the desired position.
 - Step 8** To enable the patrol settings, check the patrol locations you want to save in the list, and click **Save**.
 - Step 9** To implement the patrol schedule, go to the home window and click the **Patrol** button.
-

Configuring Custom Commands

If Custom camera is selected as the PTZ driver (see the PTZ camera entry in [Table 5-25](#)), the Preset position button on the Camera control window and the PTZ Control Panel on the home window are disabled. In this event, you must configure command buttons to control the PTZ camera.

To configure custom commands for the Network Camera, perform the following procedure:

Procedure

-
- Step 1** Choose **Configuration > Camera control**.
 - Step 2** Click the **PTZ camera** radio button in the RS485 settings area, and then choose **Custom camera** in the PTZ driver drop-down list.



Note

It is also possible to configure custom commands for any of the preset PTZ drivers. For all PTZ drivers, a total of five additional command buttons can be configured.

-
- Step 3** Click **Custom command** at the bottom of the window.
The Custom command dialog box appears.
 - Step 4** In the Custom command dialog box, enter a button name and PTZ command.
Refer to your PTZ camera user guide to find the commands to be entered in the Control settings and Custom command fields.



Note

Consider the following points:

- If you select DynaDome/SmartDOME, Lilin PIH-7x00, or Pelco D protocol as the PTZ driver, the Control settings section is not displayed. Only the Pelco D protocol is currently supported by Cisco.
- For all PTZ drivers, a total of five additional command buttons can be configured.

Step 5 Click **Save** to close the Custom command dialog box.

Step 6 Click **Save** to enable your settings.

The command buttons you set are displayed on the home window, below the live video.

Homepage Layout Window

This feature is available in Advanced Mode only.

This section explains how to set up your own customized home window layout, and it contains the following topics:

- [Preview Area, page 5-32](#)
- [Customized Button, page 5-32](#)
- [Theme Options, page 5-32](#)

For information about accessing the Homepage layout window, see the [“Accessing Configuration Options” section on page 5-1](#).

When you have finished with the settings on this window, click **Save** to enable the settings.

Preview Area

The Preview area gives you a preview of your home window layout settings. You can manually select the background and font colors in Theme Options (see the [“Theme Options” section on page 5-32](#)), and the updated settings are displayed automatically in the Preview area.

Customized Button

To display the manual trigger buttons on the home window, check the **Show manual trigger** checkbox. To hide this function, uncheck the **Show manual trigger** checkbox. For more information, see the [“Manual Trigger Area” section on page 3-2](#).

Theme Options

You can choose either of the following options to customize your home window:

- [Use a Preset Theme, page 5-33](#)
- [Create Your own Customizations, page 5-33](#)

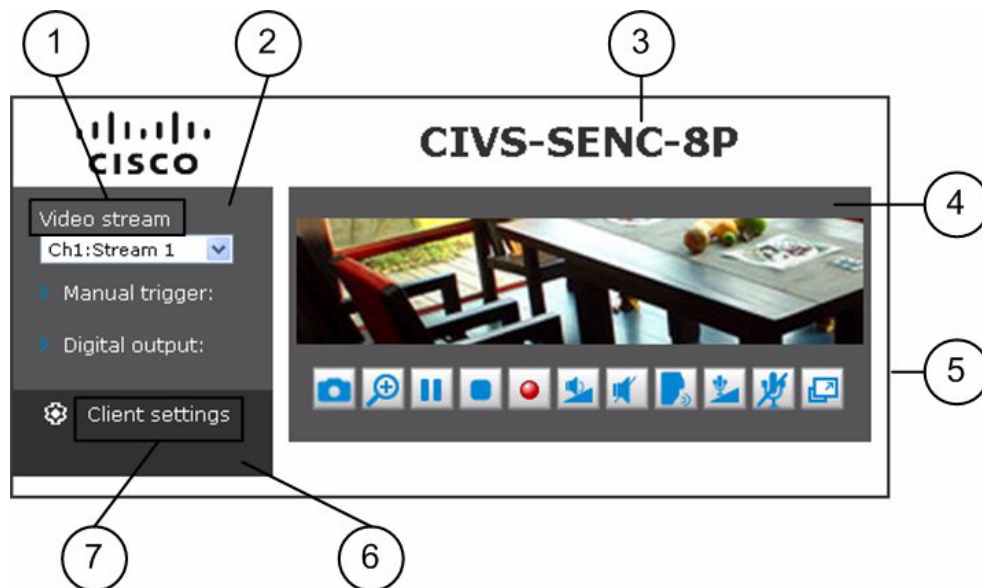
Use a Preset Theme

You can change the color scheme of your home window by choosing one of three preset themes that are listed in the Themes frame within Theme options. When you choose a new color scheme, it is displayed in the Preview area. Click **Save** to enable the settings.

Create Your own Customizations

Figure 5-6 shows the areas of the home window that can be customized from Theme options.

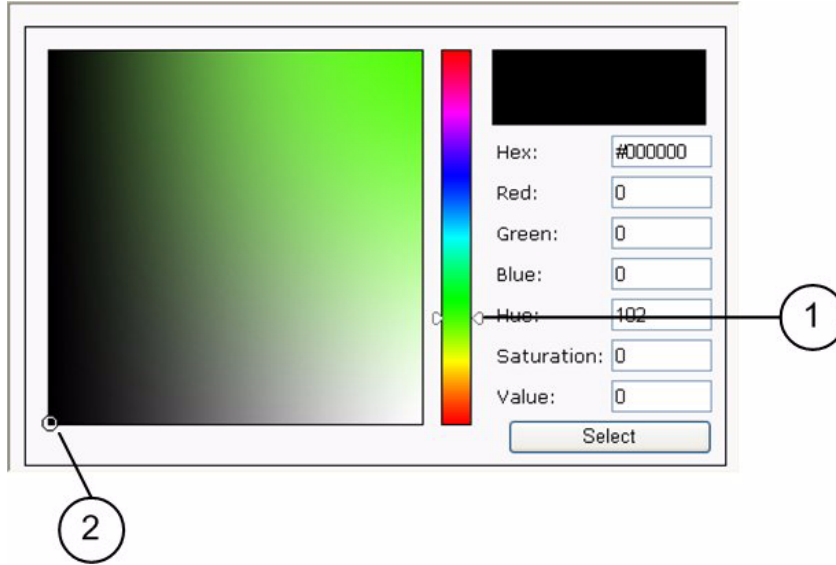
Figure 5-6 Customizable Home Window Features



1	Font color.	5	Frame color.
2	Background color of control area.	6	Background color of configuration area.
3	Font color of video title.	7	Font color of configuration area.
4	Background color of video area.		

To customize your home window, perform the following procedure:

- Step 1** Choose **Configuration > Homepage layout**.
- Step 2** Click **Custom** in the Themes frame of the Theme options area.
- Step 3** In the Color area, click the field representing the feature whose color you want to change. The palette window is displayed.
- Step 4** Click and drag the slider bar to choose the desired color. See Figure 5-7.
- Step 5** Click and drag the color pointer within the color area to refine your color selection.

Figure 5-7 *Palette Window*

1	Slider bar
2	Color pointer

The new color is displayed in the Preview area.

Step 6 Click **Select**.

Step 7 Click **Save** to enable the settings.

Application Window

This feature is available in Advanced Mode only.

This section describes how to configure the encoder to respond to particular events. An event can be triggered by many sources, such as motion detection or external digital input devices. You can specify the type of action that is performed when a specific event is triggered, and the encoder can be configured to send snapshots or videos to your email address or FTP site. This section contains the following topics:

- [Event Settings, page 5-35](#)
- [Recording Window, page 5-42](#)

For information about accessing the Application window, see the [“Accessing Configuration Options” section on page 5-1](#).

When you have finished with the settings on this window, click **Save** to enable the settings.

Event Settings

In the Event settings area, click **Add** to open the Event settings window. On this window, you can configure general event settings (see [Table 5-27](#)), as well as the following three key elements of an event:

- [Event Trigger, page 5-35](#)
- [Event Schedule, page 5-36](#)
- [Event Action, page 5-36](#)

Up to three event settings can be configured.

Table 5-27 General Event Settings

Setting	Description
Event name	Enter a name for the event setting.
Enable this event	Choose this option to enable the event setting.
Priority	Choose a setting (High, Normal, or Low) in the drop-down list to describe the relative importance of this event. Events with a higher priority setting are executed first.
Detect next event after <i>n</i> seconds	Where <i>n</i> is the number of seconds. Enter the duration in seconds for which motion detection should be paused after a motion is detected.

Event Trigger

The event trigger is the stimulus that defines when to trigger the encoder. The trigger source can also be configured to use the built-in motion detection mechanism of the encoder or external digital input devices.

[Table 5-28](#) describes the trigger sources that you can choose in the Source drop-down list.

Table 5-28 Trigger Settings

Setting	Description
Video motion detection	This option uses the built-in motion detection mechanism as a trigger source. To enable this function, you must first configure a Motion Detection Window. For more information, see the “Motion Detection Window” section on page 5-26 .
Camera tampering detection	This option allows the encoder to trigger when the camera detects that is is being tampered with. To enable this function, you must first configure the Camera tampering detection option. For more information, see the “Camera Tampering Detection Window” section on page 5-27 .
Video loss	This option triggers the encoder when the transmitted media files are missing. Check the appropriate channel fields to enable the trigger source for those channels.
Video restore	This option triggers the encoder when the camera starts to transmit video files.
Periodically	This option allows the encoder to trigger periodically every other defined minute. Enter the number of minutes in the Trigger every other <i>n</i> minute(s) field. Up to 999 minutes are allowed.

Table 5-28 **Trigger Settings (continued)**

Setting	Description
Digital input	This option allows the encoder to use an external digital input device or sensor as a trigger source. Depending on your application, you can choose from a wide selection of digital input devices that help to detect changes in temperature, vibration, sound, light, and so on.
System boot	This option triggers the encoder when the power to the encoder is disconnected.
Recording notify	This feature is available on CIVS-SENC-4P encoder model only. This option allows the encoder to trigger when the recording disk is full or when recording begins to rewrite older data.
Manual trigger	This option allows users to enable event triggers manually by clicking the on/off button on the home window. You should configure one to three events before using this function.

Event Schedule

The Event schedule settings allow you to specify the period in which an event can occur. [Table 5-29](#) describes the event schedule settings.

Table 5-29 **Event Schedule Settings**

Setting	Description
Days of the week	Choose the days of the week on which an event can occur.
Time	Set the recording schedule. You can choose Always or enter a specific time frame in 24-hour format.

Event Action

An event action is an action to be performed by the encoder when a trigger is activated. [Table 5-30](#) describes the Event action settings.

Table 5-30 Event Action Settings

Setting	Description
Trigger digital output for	Where n is the number of seconds. Check the box beside the desired DO number to turn on a connected external digital output device when a trigger is activated. Enter the following information: <ul style="list-style-type: none"> Duration (seconds)—Specify the duration (in seconds) of the trigger interval. Delay before trigger (seconds)—Specify the duration (in seconds) of the delay for the trigger after the event has been detected.
Move to preset location	Choose this option to make the Network Camera move to a preset location when a trigger is activated. You must first set up the preset locations. Click Preset locations to set up more preset locations for each channel, where each channel represents a Network Camera. For more information about preset locations settings, see the “Configuring Camera Preset Positions” section on page 5-30 .
Server	To set up an event with recorded video or snapshots, you must configure the server settings so that the encoder knows what action to take (such as which server to send the media files to) when a trigger is activated. To configure server settings, click Server . For more information about configuring server settings, see the “Server Settings” section on page 5-38 .
Media	To set up an event with recorded video or snapshots, you must configure the media settings so that the encoder knows what action to take when a trigger is activated. To configure media settings, click Media . For more information about configuring media settings, see the “Media Settings” section on page 5-40 .

When you finish configuring event settings, click **Save** to enable the settings. Click **Close** to exit the Event settings window. The new Event settings, Server settings, and /or Media settings are displayed on the Application window.

After you configure a server or media type for an event, you can continue to select other servers and media types for the event. For more information, see the [“Selecting a Server and Media Type for an Event” section on page 5-41](#).

**Tip**

If you have an SD card, click the **SD test** button to test its availability. The camera displays a message indicating success or failure. If you want to use an SD card for local storage, you must format it before use.

Managing Event Settings on the Application Window

When the Event Status is ON, once an event is triggered by motion detection, the encoder sends snapshots via e-mail automatically.

You can perform the following actions from the Application window:

- To deactivate an event trigger, select the event in the drop-down list in the Event settings area, and click **ON** to turn the setting off.

- To remove an event trigger permanently, select the event in the drop-down list in the Event settings area, and click **Delete**.
- To remove a server setting from the list, choose a server name in the drop-down list in the Server settings area, and click **Delete**. Note that a server setting cannot be deleted when it is being applied to an event setting.
- To remove a media setting from the list, choose a media name in the drop-down list in the Media settings area, and click **Delete**. Note that a media setting cannot be deleted when it is being applied to an event setting.

Server Settings

On the Server settings window, you can specify where notification messages are sent when a trigger is activated. To access the Server settings window, perform the following procedure:

Procedure

-
- Step 1** Choose **Configuration > Application**.
- Step 2** Click **Add** in the Server settings area.
- Step 3** Click **Server** at the bottom of the Event settings window.
- Step 4** Enter a name for the server setting in the Server name field.
- Step 5** You can configure any number of the following server types:
- [Email, page 5-38](#)
 - [FTP, page 5-39](#)
 - [HTTP, page 5-39](#)
 - [Network Storage, page 5-40](#)

When you finish, the new server settings are displayed automatically on the Event settings window.



Note

By default, the server folder is named after the date and hour in the following format: `%Y%M%D%H`. Where `%Y%M%D%H` refers to Year/Month/Date/Hour. If you retain the default folder name, your saved media files are classified automatically in folders named after the date and hour. You can also customize the folder names.

Email

Choose this option to send the media files via email when a trigger is activated. [Table 5-31](#) describes the Email settings.

Table 5-31 Email Settings

Setting	Description
Sender email address	The email address of the sender.
Recipient email address	The email address of the recipient.

Table 5-31 Email Settings (continued)

Setting	Description
Server address	The domain name or IP address of the email server.
User name	The user name of the email account, if required.
Password	The password of the email account, if required.
Server port	The default mail server port is set to 25. You can also manually set another port.
This server requires a secure connection (SSL)	Choose this if your SMTP server requires a secure connection (SSL).

To verify that the email settings are correctly configured, click **Test**. The result is displayed in a pop-up window. If successful, you will also receive an email indicating the result.

Click **Save** to enable your settings, then click **Close** to exit the window.

FTP

Choose this option to send the media files to an FTP server when a trigger is activated. [Table 5-32](#) describes the FTP settings.

Table 5-32 FTP Settings

Setting	Description
Server address	The domain name or IP address of the FTP server.
Server port	By default, the FTP server port is set to 21. It can also be assigned to another port number between 1025 and 65535.
User name	The login name of the FTP account.
Password	The password of the FTP account.
FTP folder name	The folder in which the media file will be placed. If the folder name does not exist, the encoder will create one on the FTP server.
Passive mode	Most firewalls do not accept new connections initiated from external requests. If the FTP server supports passive mode, choose this option to enable passive mode FTP and allow data transmission to pass through the firewall.

To verify that the FTP settings are correctly configured, click **Test**. The result is displayed in a pop-up window. If successful, you will also receive a test.txt file on the FTP server.

Click **Save** to enable the settings, then click **Close** to exit the window.

HTTP

Choose this option to send the media files to an HTTP server when a trigger is activated. [Table 5-33](#) describes the HTTP settings.

Table 5-33 HTTP Settings

Setting	Description
URL	The URL of the HTTP server.
User name	The user name, if required.
Password	The password, if required.

To verify that the HTTP settings are correctly configured, click **Test**. The result is displayed in a pop-up window. If successful, you will receive a test.txt file on the HTTP server.

Click **Save** to enable the settings, and then click **Close** to exit the window.

Network Storage

While Network Storage is shown on the user interface, it is not currently supported by Cisco.

Media Settings

On the Media settings window, you can specify the type of media that are sent when a trigger is activated. To access the Media settings window, perform the following procedure:

Procedure

-
- Step 1** Choose **Configuration > Application**.
 - Step 2** Click **Add** in the Server settings area.
 - Step 3** Click **Media** at the bottom of the Event settings window.
 - Step 4** Enter a name for the media setting in the Media name field.
 - Step 5** You can configure any number of the following media types:
 - [Snapshot, page 5-40](#)
 - [Video Clip, page 5-41](#)
 - [System Log, page 5-41](#)
-

Snapshot

Choose this option to send snapshots when a trigger is activated. [Table 5-34](#) describes the Snapshot settings.

Table 5-34 Snapshot Settings

Setting	Description
Channel	Select to the channel from which to take snapshots.
Stream	Select the stream from which to take snapshots.
Send <i>n</i> pre-event image(s) [0-7]	Where <i>n</i> is the number of pre-event images. Choose a number to determine how many images to capture before a trigger is activated. Up to seven images can be captured and stored temporarily in the encoder buffer area.

Table 5-34 Snapshot Settings (continued)

Setting	Description
Send n post-event image(s) [0-7]	Where n is the number of post-event images. Choose a number to determine how many images to capture after a trigger is activated. Up to seven images can be generated. For example, if both Send pre-event images and Send post-event images are set to seven, a total of 15 images are generated after a trigger is activated.
File name prefix	The text that is appended to the front of the file name.
Add date and time suffix to the file name	Choose this option to add a date/time suffix to the file name.

Click **Save** to enable the settings, and then click **Close** to exit the window.

Video Clip

Choose this option to send video clips when a trigger is activated. [Table 5-35](#) describes the Video Clip settings.

Table 5-35 Video Clip Settings

Setting	Description
Channel	The video source. The stream source is identical to the preset time shift caching stream. For more information about the time shift caching stream, see the “ Video Settings ” section on page 5-20.
Pre-event recording	Enter a number to determine the amount of recording time to save before a trigger is activated. Up to nine seconds of video can be stored temporarily in the encoder buffer area.
Maximum duration	Specify the maximum recording duration in seconds. The encoder can record up to 10 seconds. For example, if pre-event recording is set to five seconds and the maximum duration is set to ten seconds, the encoder continues to record for another 4 seconds after a trigger is activated.
Maximum file size	Specify the maximum file size allowed.
File name prefix	Enter the text that is appended to the front of the file name.

Click **Save** to enable the settings, and then click **Close** to exit the window.

System Log

Choose this option to send a system log when a trigger is activated. Click **Save** to enable the settings, and then click **Close** to exit the window.

Selecting a Server and Media Type for an Event

When you have configured your server and media type settings, you can proceed to select a server and media type for the event.

To select a server and media type, perform the following procedure:

Procedure

-
- Step 1** Choose **Configuration > Application**.
- Step 2** Click **Add** in the Server settings area.
- Step 3** Check a server option in the Server column at the bottom of the Event settings window. For example, you can choose Network Storage, Email, FTP, or HTTP. For more information about server options, see the “[Server Settings](#)” section on page 5-38.
- Step 4** Choose a media type from the drop-down list associated with your chosen server option on the Event settings window. For more information about media types, see the “[Media Settings](#)” section on page 5-40.
- Step 5** (Optional) If you want the system to generate folders automatically by date, time, and hour, check the **Enable customized folder** checkbox.
- Step 6** Click **Save** to enable your settings.
-

Recording Window

While Recording is shown on the user interface, it is not currently supported by Cisco.

Local Storage Window

While Local Storage is shown on the user interface, it is not currently supported by Cisco.

System Log Window

This feature is available in Advanced Mode only.

This section describes how to configure the encoder to send the system log to the remote server as backup.

The following logs are produced by the encoder:

- [Remote Log](#), page 5-42
- [Current Log](#), page 5-43

For information about accessing the System log window, see the “[Accessing Configuration Options](#)” section on page 5-1.

When you have finished with the settings on this window, click **Save** to enable the settings.

Remote Log

You can configure the encoder to send the system log file to a remote server as a log backup.

Before using this feature, it is recommended that you install a log recording tool to receive system log messages from the encoder. For an example of a log recording tool, go to the Kiwi Syslog Daemon website at <http://www.kiwisyslog.com/kiwi-syslog-daemon-overview/>.

To set up a remote log, perform the following procedure:

Procedure

-
- | | |
|---------------|---|
| Step 1 | Choose Configuration > System log . |
| 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. |
| Step 4 | When finished, click Enable remote log , and then click Save to enable the setting. |
-

Current Log

The Current log area displays the system log in chronological order. The system log is stored in the encoder buffer area and is overwritten when a specific limit is reached.

View Parameters Window

This feature is available in Advanced Mode only.

The View Parameters window lists the parameters for the entire system in alphabetical order. If you need technical assistance, you may be asked to provide information listed on this window.

Maintenance Window

This section describes how to restore the video server to factory default, upgrade firmware version, etc, and includes the following topics:

- [Rebooting the Encoder, page 5-43](#)
- [Restoring the Encoder, page 5-44](#)
- [Exporting and Uploading Files, page 5-44](#)
- [Upgrading the Firmware, page 5-47](#)

Rebooting the Encoder

To reboot the encoder, perform the following procedure:

Procedure

-
- | | |
|---------------|---|
| Step 1 | Choose Maintenance > Reboot .

A message is displayed while the reboot is in progress. When the reboot is finished, the live video window is displayed in your browser. |
|---------------|---|

- Step 2** If the connection fails after rebooting, manually enter the IP address of the encoder in the address field to resume the connection. For information about determining the IP address of your encoder, see the [“Determining the Encoder IP Address” section on page 2-1](#).

Restoring the Encoder

To restore the encoder to the factory default settings, perform the following procedure:

Procedure

- Step 1** Click **Maintenance**.
- Step 2** (Optional) In the Restore area, you can choose to retain the following settings (see [Table 5-36](#)):

Table 5-36 **Restore Settings**

Setting	Description
Network type	Choose this option to retain the Network type settings. For more information about Network type settings, see the “Network Type Settings” section on page 5-9 .
Daylight saving time	Choose this option to retain the Daylight saving time settings. For more information about Daylight saving time settings, see the “System Window” section on page 5-2 .
Custom language	Choose this option to retain the Custom Language settings.

If none of the above options is selected, all settings are restored to factory default.

- Step 3** Click **Restore**.
- The encoder reboots as part of the restore procedure, and a message is displayed while the reboot is in progress.
- Step 4** If the connection fails after rebooting, manually enter the IP address of the encoder in the address field to resume the connection. For information about determining the IP address of your encoder, see the [“Determining the Encoder IP Address” section on page 2-1](#).

Exporting and Uploading Files

This feature is available in Advanced Mode only.

This feature allows you to export and upload daylight saving time rules, custom language files, and setting backup files.

You can perform the following actions:

- [Exporting the Daylight Savings Time File Configuration, page 5-45](#)
- [Uploading the Custom Language File, page 5-46](#)
- [Uploading the Setting Backup File, page 5-46](#)

- [Uploading Daylight Saving Time Rules, page 5-46](#)
- [Uploading the Custom Language File, page 5-46](#)
- [Uploading the Setting Backup File, page 5-46](#)

Exporting the Daylight Savings Time File Configuration

To export the daylight saving time configuration file from the encoder, perform the following procedure:

Procedure

-
- | | |
|---------------|--|
| Step 1 | Click Maintenance . |
| Step 2 | In the Export files area, click Export beside Export daylight saving time configuration file.
A file download dialog box is displayed. |
| Step 3 | Click Open to review the XML file, or click Save to store the file for editing. |
| Step 4 | Open the file with Microsoft® Notepad and locate your time zone. Set the start and end time of DST.
When finished, save the file. |
-

For information about uploading the daylight saving time rule, see the [“Uploading Daylight Saving Time Rules” section on page 5-46](#).

Exporting the Language File

To export the language file from the encoder, perform the following procedure:

Procedure

-
- | | |
|---------------|--|
| Step 1 | Click Maintenance . |
| Step 2 | In the Export files area, click Export beside Export language file.
A file download dialog box is displayed. |
| Step 3 | Click Open to review the XML file, or click Save to store the file for editing. |
-

For information about uploading a custom language file, see the [“Uploading the Custom Language File” section on page 5-46](#).

Exporting the Setting Backup File

To export the setting backup file from the encoder, perform the following procedure:

Procedure

-
- | | |
|---------------|--|
| Step 1 | Click Maintenance . |
| Step 2 | In the Export files area, click Export beside Export setting backup file. |

A file download dialog box is displayed.

- Step 3** Click **Open** to review the XML file, or click **Save** to store the file for editing.
-

For information about uploading a setting backup file, see the [“Uploading the Setting Backup File” section on page 5-46](#).

Uploading Daylight Saving Time Rules

To upload daylight saving time rules to the encoder, perform the following procedure:

Procedure

- Step 1** Click **Maintenance**.
- Step 2** In the Upload files area, click **Browse** beside Upload daylight saving time rules and choose the XML file to upload.
- Step 3** Click **Upload**.
- If an incorrect date and time are assigned in the XML file, a warning message is displayed when the file is being uploaded to the encoder.
-

Uploading the Custom Language File

To upload a custom language file to the encoder, perform the following procedure:

Procedure

- Step 1** Click **Maintenance**.
- Step 2** In the Upload files area, click **Browse** beside Upload custom language file and choose the file to upload.
- Step 3** Click **Upload**.
-

Uploading the Setting Backup File

To upload a custom language file to the encoder, perform the following procedure:

Procedure

- Step 1** Click **Maintenance**.
- Step 2** In the Upload files area, click **Browse** beside Upload setting backupfile and choose the file to upload.
- Step 3** Click **Upload**.

**Note**

The model and firmware version of the encoder should be the same as the setting backup file. If you have set up a fixed IP or other special settings for your encoder, it is not suggested that you upload a settings backup file.

Upgrading the Firmware

This feature allows you to upgrade the firmware of your encoder.

**Warning**

Do not power off the encoder during the upgrade.

To upgrade the firmware, perform the following procedure:

Procedure

- Step 1** Download the latest firmware file from the Cisco website. The file is in .pkg file format. For more information, see <http://www.cisco.com/support>.
- Step 2** Click **Maintenance**.
- Step 3** Click **Browse** in the Upgrade firmware area, and choose the firmware file.
- Step 4** Click **Upgrade**.

The encoder starts to upgrade and reboots automatically when the upgrade is finished.

If the upgrade is successful, a message is displayed to inform you that the system is about to reboot immediately.

If you selected an incorrect firmware file, a message is displayed to inform you that the unpack procedure has failed.



APPENDIX A

Technical Specifications

The Cisco standalone video encoders (CIVS-SENC-4P and CIVS-SENC-8P) can be used to convert analog video sources into digital formats so they can be integrated into a networked IP based video surveillance system. The 4-Port model (CIVS-SENC-4P) supports four analog video inputs, while the 8-Port model (CIVS-SENC-8P) supports eight analog video inputs. Both devices can be used in a stacked configuration, or they can be rack mounted. A power supply is included with both. [Table A-1](#) lists key features and technical specifications for both encoder models.

Table A-1 **Technical Specifications**

Feature	CIVS-SENC-4P	CIVS-SENC-8P
Protocols Supported	Supports two simultaneous video streams. The two streams can be compressed in H.264, MPEG-4 or MJPEG formats, in various combinations of resolution, frame-rate and bit-rate combinations.	Supports a single video stream per port. The stream can be compressed in H.264, MPEG-4 or MJPEG formats and configured with different resolution, frame-rates and bit-rates.
PTZ Interface	Provides a RS-485 interface to allow for connection to PTZ control units supporting the Pelco-D protocol, in order to control Pan-Tilt-Zoom functions in an external camera or PTZ mount.	Provides a RS-485 interface to allow for connection to PTZ control units supporting the Pelco-D protocol, in order to control Pan-Tilt-Zoom functions in an external camera or PTZ mount.
Digital Inputs/ Outputs	Has 4 Digital Outputs and 4 Digital Inputs to connect to/from external sensors.	Has 8 Digital Outputs and 8 Digital Inputs to connect to/from external sensors.
Web Interface	Supports Internet Explorer® 8.0 Web browser for remote setup and administration.	Supports Internet Explorer® 8.0 Web browser for remote setup and administration.
Video Management	The encoder connects to Cisco Video Surveillance Manager Version 6.3.2 and later.	The encoder connects to Cisco Video Surveillance Manager Version 6.3.2 and later.

Table A-1 Technical Specifications

Feature	CIVS-SENC-4P	CIVS-SENC-8P
Features and Benefits	<ul style="list-style-type: none"> Up to D1 Resolution per channel Up to 30 Frames per Second (FPS) at D1 resolution H.264, MPEG-4 and MJPEG Compression options Up to 2 Simultaneous Video Streams per port Up to 5 Privacy Mask windows per port Up to 3 Motion Detection windows per port 	<ul style="list-style-type: none"> Up to D1 Resolution per port Up to 30 Frames per Second (FPS) at D1 resolution H.264, MPEG-4 and MJPEG Compression options Up to 5 Privacy Mask windows per port Up to 3 Motion Detection windows per port
Analog Video Input Ports	4	8
Digital Alarm Inputs	4	8
Digital Alarm Outputs	4	8
Security	Password protected administrative interface. HTTPS access to the administrative interface.	Password protected administrative interface. HTTPS access to the administrative interface.
Certifications/Ratings/Patents	CE, FCC Class B, C-Tick UL /cUL Listed	CE, FCC Class B, C-Tick UL /cUL Listed
Port	RJ-45 connector for 100/1000 Base-TX Auto MDI/MDI-X	RJ-45 connector for 100/1000 Base-TX Auto MDI/MDI-X
Cable Type	Cat5 or better	Cat5 or better
Power Input	12VDC/24VAC (Power supply included)	12VDC/24VAC (Power supply included)
Power Consumption	24 W (Max)	24 W (Max)
Local Storage	SD/SDHC slot	
Operational Temperature	50° to 122° F (10° to 50° C)	50° to 122°F (10° to 50°C)
Operational Humidity	20% to 80%, noncondensing	20% to 80%, noncondensing
Dimensions	189 mm (L) x 153 mm (W) x 49.3 mm (H)	189 mm (L) x 153 mm (W) x 49.3 mm (H)
Weight	800g	837g
Video Encoding	H.264, MPEG-4 and MJPEG (for both PAL and NTSC)	H.264, MPEG-4 and MJPEG (for both PAL and NTSC)
Video Streams	Up to 2 simultaneous streams; the second stream is variable based on the setup of the primary stream.	Single stream per port.

Table A-1 Technical Specifications

Feature	CIVS-SENC-4P	CIVS-SENC-8P
Audio	G.711 audio encoding (64 Kbps) μ -Law, or A-Law mode selectable. Audio input (up to 1Vrms) 3.5 mm Phone Jack Audio output Terminal block x 4. Supports two-way audio (Per channel) Supports audio mute.	G.711 audio encoding (64 Kbps) μ -Law, or A-Law mode selectable. Audio input (up to 1Vrms) 3.5 mm Phone Jack Audio output Terminal block x 8. Supports two-way audio (Per channel) Supports audio mute.
PTZ Serial Interface	RS-485 Half Duplex, supporting Pelco-D protocol	RS-485 Half Duplex, supporting Pelco-D protocol
Available Resolutions	See Table A-2 .	See Table A-3 .
Minimum PC Client Requirements	<ul style="list-style-type: none"> Processor: Intel® Core® 2 Duo microprocessor, 2.6 GHz. Operating System: Microsoft® Windows® 7 Memory: 2 GB RAM Network Interface Card: 100 megabits (or greater) Monitor: Minimum of 1024 x 768 resolution, 16- or 32-bit pixel color resolution Web browser: Internet Explorer® 8.0, Quicktime 6.5 and above 	<ul style="list-style-type: none"> Processor: Intel® Core® 2 Duo microprocessor, 2.6 GHz. Operating System: Microsoft® Windows® 7 Memory: 2 GB RAM Network Interface Card: 100 megabits (or greater) Monitor: Minimum of 1024 x 768 resolution, 16- or 32-bit pixel color resolution Web browser: Internet Explorer® 8.0, Quicktime 6.5 and above

Table A-2 Available Resolutions: CIVS-SENC-4P

Dual streams supported on channels 1-4	Primary stream Max resolution	Primary Max Frame rate (fps)/ Bitrate (Kbps) or Quality/ Intra Frame period (S)	Secondary stream max resolutions	Secondary Max Frame rate (fps)/ Bitrate (Kbps) or Quality/ Intra Frame period (S)
H.264 + H.264	D1	30 fps 2000 Kbps 1S	D1	15 fps 2000 Kbps 1S
H.264 + MPEG 4	D1	30 fps 2000 Kbps 1S	D1	3 fps 2000 Kbps 1S
H.264 + MJPEG	D1	30 fps 2000 Kbps 1S	D1	30 fps Good NA

Table A-2 Available Resolutions: CIVS-SENC-4P (continued)

Dual streams supported on channels 1-4	Primary stream Max resolution	Primary Max Frame rate (fps)/ Bitrate (Kbps) or Quality/ Intra Frame period (S)	Secondary stream max resolutions	Secondary Max Frame rate (fps)/ Bitrate (Kbps) or Quality/ Intra Frame period (S)
MPEG-4 + MJPEG	D1	20 fps Good 1S	D1	30 fps NA Good
MPEG-4 + MPEG-4	D1	15 fps 2000 Kbps 1S	D1	5 fps 2000Kbps 1S
MJPEG + MJPEG	D1	30 fps Good NA	D1	25 fps Good NA

The following are the definitions of resolutions used in the table:

- D1: 720 x 480 (NTSC), 720 x 576 (PAL)
- 4CIF: 704 x 480 (NTSC), 704 x 576 (PAL)
- CIF: 352 x 240 (NTSC), 352 x 288 (PAL)

Table A-3 Available Resolutions: CIVS-SENC-8P

Stream	Max Resolution	Max Frame rate (fps)/ Bitrate (Kbps) or Quality/ Intra Frame period (S)
H.264	D1	30 fps 2000 Kbps 1S
MPEG-4	D1	30 fps 2000 Kbps 1S
MJPEG	D1	30 fps Good NA

The following are definitions of resolutions used in the table:

- D1: 720 x 480 (NTSC), 720 x 576 (PAL)
- 4CIF: 704 x 480 (NTSC), 704 x 576 (PAL)
- CIF: 352 x 240 (NTSC), 352 x 288 (PAL)



INDEX

A

- accessing
 - client settings [4-1](#)
 - configuration options [5-1](#)
 - encoder
 - RTSP player [2-2](#)
 - web browser [2-2](#)
- access list, general settings [5-16](#)
- account
 - deleting user account [5-4](#)
 - modifying user account [5-4](#)
- adding user [5-4](#)
- administrator IP address [5-18](#)
- Application window
 - managing event settings [5-37](#)
 - overview [5-34](#)
- assigning functions, joystick buttons [4-4](#)
- audio
 - settings [5-25](#)
 - two way settings [5-13](#)
- audio and video
 - audio and video window [5-19](#)
 - settings overview [5-19](#)
- audio control buttons [3-4](#)
- authentication, enabling [1-10](#)
- available FPS [5-25](#)
- available frame rate [5-25](#)

B

- buffer time, streaming [4-3](#)

C

- camera
 - Camera tampering detection window [5-27](#)
 - configuring preset positions [5-30](#)
 - ID settings [5-29](#)
 - patrol settings [5-30](#)
- camera control
 - area [3-2](#)
 - Camera control window [5-28](#)
 - RS485 settings [5-28](#)
- camera patrol settings [5-30](#)
- certificate
 - creating a certificate request and install [5-7](#)
 - creating a self-signed certificate automatically [5-6](#)
 - creating a self-signed certificate manually [5-6](#)
 - removing signed certificate [5-8](#)
- CIVS-SENC-4P, front and back view [1-2](#)
- CIVS-SENC-8P, front and back view [1-3](#)
- client settings
 - accessing [4-1](#)
 - managing [4-1](#)
- configuration
 - area [3-3](#)
 - options [5-1](#)
- configuring
 - camera patrol settings [5-30](#)
 - camera preset positions [5-30](#)
 - custom commands [5-31](#)
- connection information, current streaming [5-17](#)
- control buttons, video and audio [3-4](#)
- COS [5-11](#)
- create certificate [5-5](#)

current log [5-43](#)
 current streaming, connection information [5-17](#)
 custom commands, configuring [5-31](#)
 customization
 camera settings [5-29](#)
 Homepage layout window theme options [5-32](#)
 using preset themes [5-33](#)
 customizing, home window [5-33](#)
 custom language file, uploading [5-46](#)

D

daylight savings time
 exporting file configuration [5-45](#)
 uploading rules [5-46](#)
 DHCP server, obtaining IP address [2-1](#)
 DI/DO
 control area [3-3](#)
 diagram [1-6](#)
 window [5-19](#)
 diffserv model [5-11](#)
 digital input settings [5-19](#)
 digital output settings [5-19](#)

E

email, server settings [5-38](#)
 enabling authentication [1-10](#)
 enabling HTTPS authentication [5-5](#)
 encoder
 accessing using web browser [2-2](#)
 determining IP address [2-1](#)
 physical description [1-2](#)
 pin definitions [1-5](#)
 rebooting [5-43](#)
 restoring [5-44](#)
 setting up behind a router [1-9](#)
 setting up on the network [1-8](#)

setting up using a static IP address [1-10](#)

event

action [5-36](#)
 schedule [5-36](#)
 selecting a media type [5-41](#)
 selecting a server [5-41](#)
 settings [5-35](#)
 trigger [5-35](#)

event settings, managing [5-37](#)

exporting

daylight savings time file configuration [5-45](#)
 files [5-44](#)
 language file [5-45](#)
 settings backup file [5-45](#)

F

files

exporting [5-44](#)
 uploading [5-44](#)

filter [5-18](#)

filter type settings [5-18](#)

firmware, upgrading [5-47](#)

fixed IP address settings, using [5-9](#)

FPS [5-25](#)

frame rate status [5-25](#)

front and back view

CIVS-SENC-4P [1-2](#)
 CIVS-SENC-8P [1-3](#)

FTP

send media files [5-39](#)
 server settings [5-13](#)

H

H.264

media options [4-1](#)
 protocol options [4-2](#)

hardware

CIVS-SENC-4P, front and back view [1-2](#)

CIVS-SENC-8P, front and back view [1-3](#)

physical description [1-2](#)

pin definitions [1-5](#)

rebooting the encoder [5-43](#)

reset [1-8](#)

restoring the encoder [5-44](#)

Homepage layout window, theme options [5-32](#)

home window

customization [5-33](#)

features [3-2](#)

overview [3-1](#)

using a preset theme [5-33](#)

HTTP

network settings [5-12](#)

server settings for media files [5-39](#)

HTTPS

cancel settings [5-7](#)

enabling HTTPS authentication settings [5-5](#)

network settings [5-13](#)

window [5-5](#)

I

I/O

pin definitions [1-5](#)

terminal blocks [1-5](#)

ID settings, camera [5-29](#)

IEEE 802.1x [5-10](#)

image settings [5-21](#)

install certificate [5-5](#)

IP address

administrator [5-18](#)

assigning using link-local address scheme [2-1](#)

determining the encoder IP address [2-1](#)

manually set up address settings [5-10](#)

obtaining with DHCP server [2-1](#)

setting up an encoder [1-10](#)

using fixed address settings [5-9](#)

J

joystick buttons, assigning functions [4-4](#)

joystick settings [4-3](#)

L

LAN, settings [5-9](#)

language file, exporting [5-45](#)

LED, status [1-7](#)

link-local address scheme, assigning an IP address [2-1](#)

list settings, access [5-16](#)

live streaming, buffer time [4-3](#)

live video, window [3-3](#)

Local storage window [5-42](#)

log

current log [5-43](#)

remote log [5-42](#)

system log [5-41](#)

M

Maintenance window [5-43](#)

managing

client settings [4-1](#)

privilege settings [5-3](#)

user settings [5-4](#)

manual trigger

area [3-2](#)

show [5-32](#)

media options

H.264 [4-1](#)

MPEG-4 [4-1](#)

media settings [5-40](#)

motion detection

how it works [5-27](#)

window [5-26](#)

MP4 saving options [4-2](#)

MPEG-4

media options [4-1](#)

protocol options [4-2](#)

N

network

deployment [1-8](#)

network type settings [5-9](#)

Network window [5-8](#)

setting up an encoder [1-8](#)

storage [5-40](#)

notifications, server settings [5-38](#)

P

package contents [1-2](#)

password, root password settings [5-3](#)

pin definitions, I/O terminal blocks [1-5](#)

preset theme [5-33](#)

preview area [5-32](#)

privacy mask, adding [5-22](#)

protocol options

H.264 [4-2](#)

MPEG-4 [4-2](#)

Q

QOS, quality of service settings [5-10](#)

QOS/DSCP, diffserv model [5-11](#)

quadview settings [4-3](#)

quality of service, QOS settings [5-10](#)

quality settings, video [5-22](#)

R

rebooting, encoder [5-43](#)

Recording window [5-42](#)

remote log [5-42](#)

removing a signed certificate [5-8](#)

reset, encoder [1-8](#)

restoring, encoder [5-44](#)

root password settings [5-3](#)

router, setting up an encoder [1-9](#)

RS485 settings [5-28](#)

RTSP player, accessing encoder [2-2](#)

RTSP streaming settings [5-13](#)

S

saving options, MP4 [4-2](#)

Security window

managing, user settings [5-4](#)

managing privilege settings [5-3](#)

overview [5-3](#)

server settings

email [5-38](#)

notifications [5-38](#)

trigger activation [5-38](#)

settings

accessing client [4-1](#)

access list [5-16](#)

settings backup file

exporting [5-45](#)

uploading [5-46](#)

show manual trigger [5-32](#)

snapshot [5-40](#)

SNMP window [5-8](#)

status, LED [1-7](#)

storage

local [5-42](#)

network storage [5-40](#)

stream 1, video quality settings [5-22](#)

streaming

buffer time [4-3](#)RTSP [5-13](#)

system

log [5-41](#)log window [5-42](#)parameters, View parameters window [5-43](#)settings [5-2](#)time settings [5-2](#)System window [5-2](#)

Ttheme options [5-32](#)time settings, system [5-2](#)

trigger

email settings [5-38](#)event [5-35](#)manual trigger area [3-2](#)server settings [5-38](#)show manual trigger [5-32](#)two way audio settings [5-13](#)

Uupgrading firmware [5-47](#)

uploading

custom language file [5-46](#)daylight saving time rules [5-46](#)files [5-44](#)settings backup file [5-46](#)user, adding [5-4](#)

user account

deleting [5-4](#)modifying [5-4](#)user privileges, managing [5-3](#)user settings, managing [5-4](#)

V

video

adding a privacy mask [5-22](#)live video window [3-3](#)quality settings for stream 1 [5-22](#)settings [5-20](#)video control buttons [3-4](#)video stream, quadview settings [4-3](#)View parameters window [5-43](#)VLAN 802.1p model [5-11](#)

Wweb browser, accessing encoder [2-2](#)

window

Application [5-34](#)Audio and video [5-19](#)Camera control [5-28](#)Camera tampering detection [5-27](#)DI/DO [5-19](#)HTTPS [5-5](#)Live video [3-3](#)Local storage [5-42](#)Maintenance [5-43](#)Recording [5-42](#)Security [5-3](#)SNMP [5-8](#)System [5-2](#)System log [5-42](#)View parameters [5-43](#)

