Cisco Video Surveillance 8930 IP Camera Reference Guide

Release 1.0.2

April 20, 2018

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 NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Copyright © 2018 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface v

Overview v

Organization v

Obtaining Documentation and Support v

CHAPTER 1 **Getting Started** 1-1

Overview 1-1

Physical Description 1-2

LED Definitions 1-4

Hardware Reset 1-5

SD/SDHC/SDXC Card Capacity 1-5

DI/DO Diagram 1-5

Power Adapters 1-8

Hardware Installation 1-8

I/O Combo Cable Specifications 1-22

Mechanical Dimensions 1-26

Network Deployment 1-26

Setting up the Network Camera over the Internet 1-26

General Connection 1-29

CHAPTER 2 **Accessing the IP Camera** 2-1

Using Web Browsers 2-1

Performing the Initial Setup of the IP Camera 2-2

Using RTSP Players 2-2

Using 3GPP-Compatible Mobile Devices 2-3

CHAPTER 3 **IP Camera Main Page** 3-1

Mouse and Screen Control 3-2

PTZ Control Panel 3-3

Live Video Window for H.264 or H.265 Video Streams 3-4

Live Video Window for MJPEG Video Streams 3-6

CHAPTER 4 **Client Settings** 4-1

H.265/H.264 Media Options 4-1
H.265/H.264 Protocol Options 4-1
Two Way Audio 4-2
MP4 Saving Options 4-2
Local Streaming Buffer Time 4-2
Joystick settings 4-2

CHAPTER 5 **Configuration** 5-1

Accessing the Settings Pages 5-2
System > General settings 5-3
System > Homepage layout 5-3
General settings 5-3
Theme Options 5-4
System > Logs 5-5
Log server settings 5-5
System log 5-5
Access log 5-5
System > Parameters 5-6
System > Maintenance 5-6
General settings > Upgrade firmware 5-6
General settings > Reboot 5-7
General settings > Restore 5-7
Import/Export files 5-7
Media > Image 5-8
General settings 5-8
IR control 5-9
Image settings 5-9
Exposure 5-10
Privacy Mask 5-13
Media > Video 5-14
Mode 5-14
Stream settings 5-14
Media > Audio 5-20
Network > General settings 5-20
Network > Streaming protocols 5-23
HTTP streaming 5-23

RTSP Streaming 5-24
SIP 5-25
Network > QoS (Quality of Service) 5-26
Requirements for QoS 5-26
QoS models 5-26
Network > SNMP (Simple Network Management Protocol) 5-27
SNMP Configuration 5-28
Security > User accounts 5-28
Root Password 5-28
Privilege Management 5-28
Account Management 5-29
Security > HTTPS (Hypertext Transfer Protocol over SSL) 5-29
Create and Install Certificate Method 5-29
Security > Access List 5-31
General Settings 5-31
Filter 5-31
Administrator IP address 5-32
Security > IEEE 802.1X 5-32
Security > SSH 5-33
PTZ > PTZ settings 5-33
Home location settings 5-33
Patrol list 5-33
Recorded Patrol 5-34
Preset Patrol 5-35
Misc. settings 5-35
PTZ > Calibrate 5-37
PTZ > Auto tracking 5-37
Event > Event settings 5-38
Event 5-38
Add server 5-40
Additional Actions 5-41
Add media 5-42
Customized Script 5-44
Applications > Motion detection 5-44
How does Motion Detection Work? 5-45
Applications > DI and DO 5-45
Applications > Tampering detection 5-46
Applications > Audio detection 5-46

Applications > Package management 5-48
Recording > Recording settings 5-49
Recording Settings 5-49
Local storage > SD card management 5-50
SD card status 5-51
SD card format 5-51
SD card control 5-51
Local storage > Content management 5-51
Searching and Viewing the Records 5-51
Search Results 5-52

Preface

Overview

This document provides information about installing deploying, and using the Cisco Video Surveillance 8930 IP Camera.

Organization

This manual is organized as follows:

Chapter 1, “Getting Started”	Provides information about getting started with and understanding the IP Camera
Chapter 2, “Accessing the IP Camera”	Explains how to access the IP camera through web browsers and RTSP players
Chapter 3, “IP Camera Main Page”	Describes the layout of the main page of the IP camera web based interface
Chapter 4, “Client Settings”	explains how to select the stream transmission mode and saving options on the local computer
Chapter 5, “Configuration”	Describes the IP camera settings options

Obtaining Documentation and Support

For information about obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What’s New in Cisco Product Documentation*. This document also lists new and revised Cisco technical documentation. It is available at:

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

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

Getting Started

This chapter provides information about getting started with and understanding the IP camera. It includes the following sections:

- Overview, page 1-1
- Physical Description, page 1-2
- LED Definitions, page 1-4
- Hardware Reset, page 1-5
- SD/SDHC/SDXC Card Capacity, page 1-5
- DI/DO Diagram, page 1-5
- Power Adapters, page 1-8
- Hardware Installation, page 1-8
- I/O Combo Cable Specifications, page 1-22
- Mechanical Dimensions, page 1-26
- Network Deployment, page 1-26

Overview

he Cisco Video Surveillance 8930 IP Cameras is a high-definition, full-functioned video endpoint, designed to enhance low light surveillance in large coverage areas and provides a superb image in challenging situations. The camera comes with integrated camera optics package that offer 360° continuous pan rotation and 256 PTZ presets. In addition, the camera supports an SD/SDHC slot for local storage that can be used if network connectivity is lost. The camera supports four simultaneous video streams, which can be compressed in MJPEG, H.264, and H.265 formats across several resolution configurations, and can be configured in a variety of frame rates and bit rates or additional bandwidth administration. It features a 1/2.8-inch CMOS for increased sensitivity, and low light technology that allows the cameras to compensate in scenes where minimal light is present. In addition, the camera features built-in motion detection and advanced wide dynamic range (WDR) that enables the system to compensate in scenes where dramatic contrasts in lighting are present.

Key features and benefits of the Cisco Video Surveillance cameras include:

- High definition video from a full range of motion—The camera streams crisp and clear 1080p (1920 x 1080) video at 30 frames per second through a continuous 360° pan rotation, 220° tilt angle range, and 30x optical zoom. The camera operator can remotely control the camera to track subjects or reposition the camera's field of view.

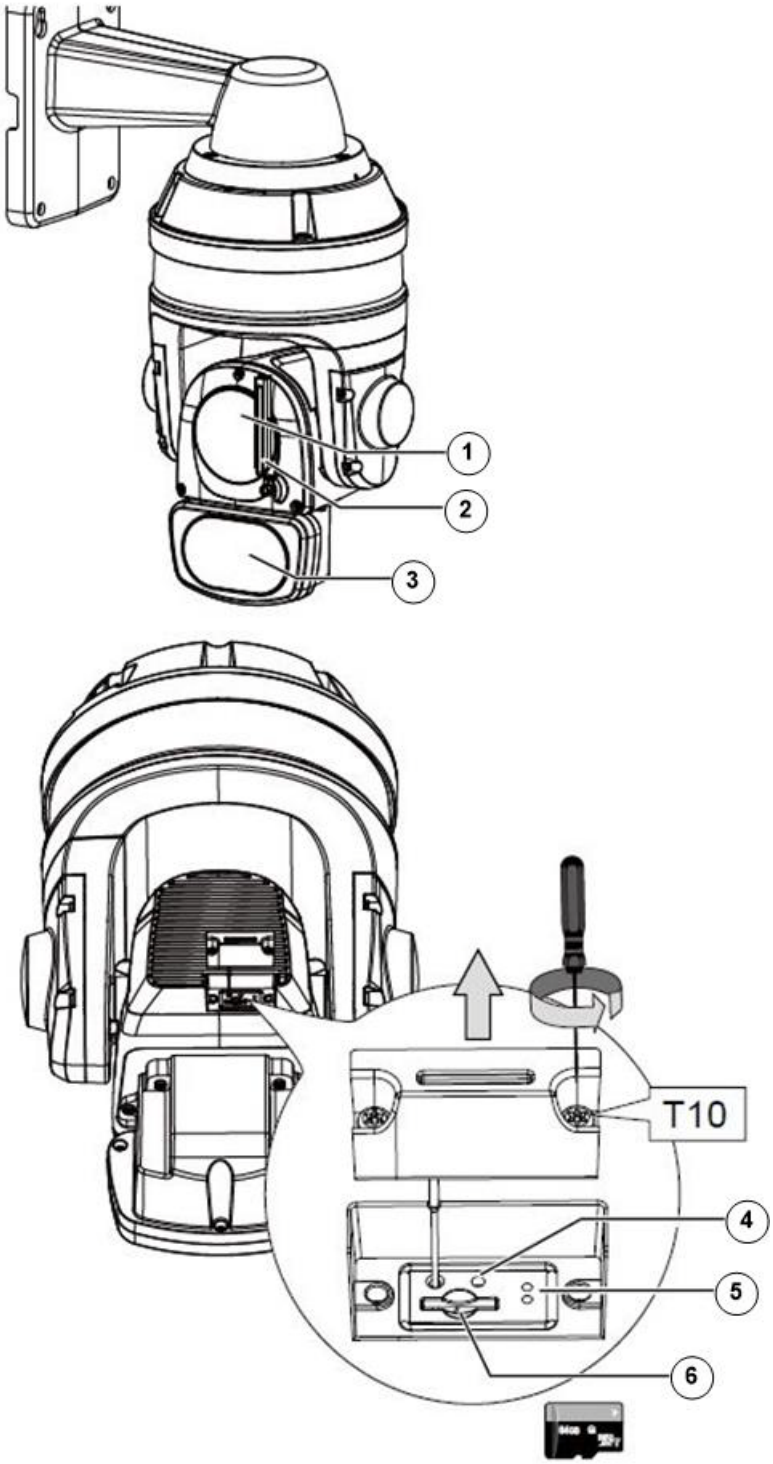
- Streaming—The cameras can stream H.264, H.265, and MJPEG video simultaneously. Each video stream can be configured with individual resolution, quality, and frame-rate settings.
- Outdoor ready—The housing for the camera is IP66, IK10 & NEMA 4X, and UL rated, allowing for outdoor mounting without an additional enclosure.
- Flexible power options—The camera supports PoH (95W) or 24 VAC power through an external power supply.
- Mounting options—The cameras can be installed to a ceiling or wall.

Physical Description

The following figures illustrate the cameras:

- Figure 1-1—Cisco Video Surveillance 8930 IP Camera outer view
- Figure 1-2—Cisco Video Surveillance 8930 IP Camera inner view

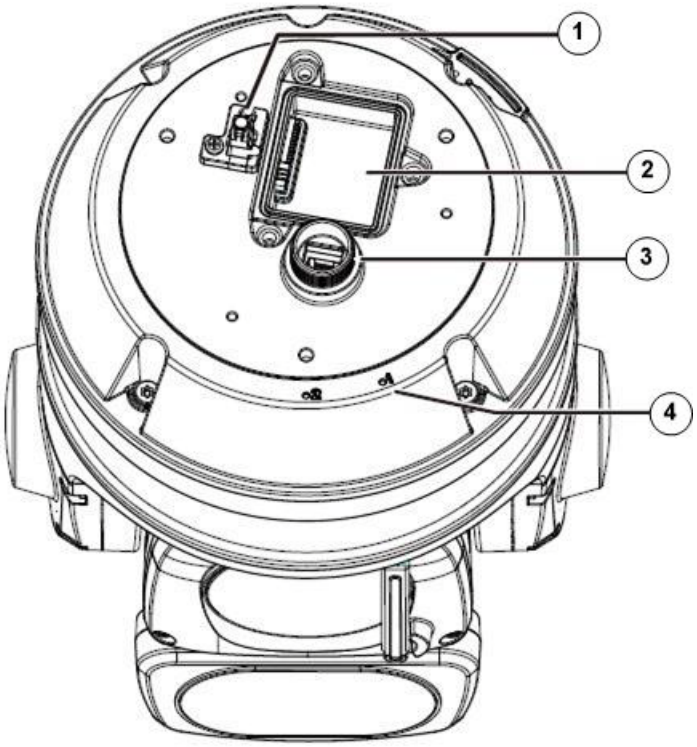
Figure 1-1 Cisco Video Surveillance 8930 IP Camera Outer View



1	Lens
2	Wiper
3	IR LEDs

4	Reset button
5	Status LEDs
6	MicroSD card slot

Figure 1-2 Cisco Video Surveillance 8930 IP Camera Inner View



1	Safety wire hook
2	I/O combo connector
3	LAN connector
4	Alignment marks

LED Definitions

Table 1-1 describes the LEDs on the Cisco Video Surveillance IP Camera.

Table 1-1 IP Camera LEDs

Item	LED Status	Description
1	Steady red	Powered and system booting
	Red LED off	Power off

Table 1-1 IP Camera LEDs (continued)

Item	LED Status	Description
2	Steady red and green blinking every 1 second	Network normal (heartbeat)
	Steady red and green LED OFF	Network failed
3	Red blinking every 0.15 second and Green blinking every 1 second	Upgrading firmware
4	Red blinking every 0.15 second and green blinking every 0.15 second	Restoring defaults

Hardware Reset

The recessed button (see Figure 1-1 on page 1-3) is used to reset the system or restore the factory default settings. Sometimes resetting the system can return the camera to normal operation. If the system problems remain after reset, restore the factory settings and install again.

- Reset—Press and release the reset button with a paper clip or thin object. Wait for the camera to reboot.
- Restore—Press and hold the reset button for at least 30 seconds to restore system defaults. All settings will be restored to factory defaults.

SD/SDHC/SDXC Card Capacity

The camera is compliant with SD/SDHC/SDXC 32GB, 64GB, and other preceding standard SD cards.

Tip If you forget the root (administrator) password for the camera, you can restore the camera defaults by pressing the reset button for longer than 5 seconds.

If DHCP is enabled in your network, and the camera cannot be accessed, run the Cisco setup software utility to search the network. If the camera has been configured with a fixed IP that does not comply with your local network, you may see its default IP 169.254.x.x. If you still cannot find the camera, you can restore the camera to its factory defaults. The factory default is DHCP client.

If you change your network parameters, for example by adding a camera via a connection to a LAN card, restart the Cisco setup software utility.

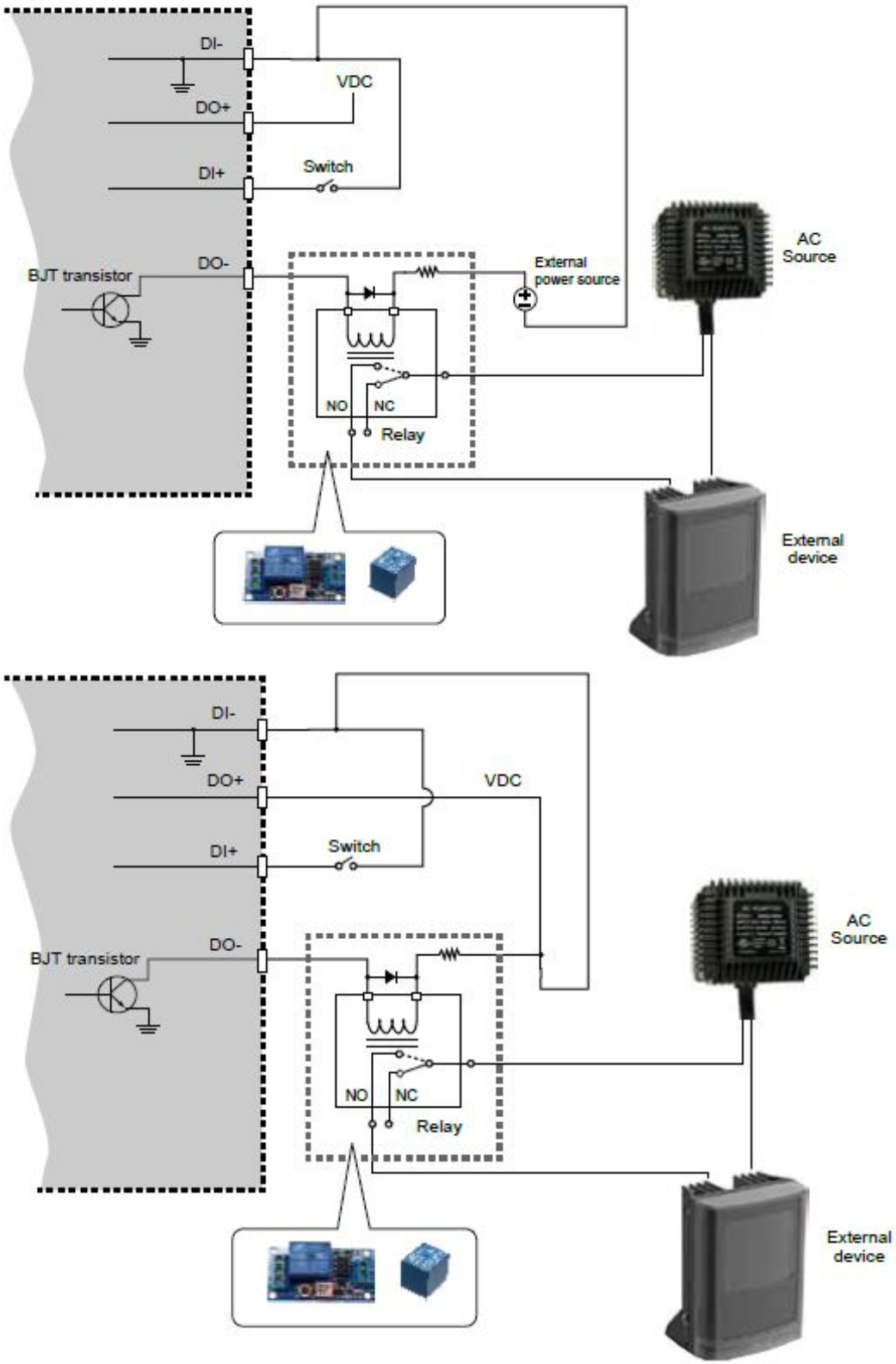
DI/DO Diagram

- The DO+ pin (5V) provides 5V±10% output voltages, and the max. load is 50mA.
- The max. voltage for DO– pins is 30VDC (external power).

  In order to control AC devices, Figure 1-3 can be taken into consideration. This figure uses a relay to control the ON/OFF condition of the AC device.
- An external relay can be triggered by using the DO+ or by an external power source, depending on the type of relay you use.

- In case of using an individual relay (instead of using a relay module), for protection against voltage or current spikes, a transient voltage suppression diode must be connected in parallel with the inductive load.

Figure 1-3 DI/DO Diagram



Power Adapters

Figure 1-4 Power Adapters

CIVS-IPC-8930	The product is intended to be supplied by a Listed Power Unit marked "L.P.S." (or "Limited Power Source") and rated output 24Vac, 50/60Hz, 1.28A minimum or 48Vdc (PoE), 0.35A minimum

Hardware Installation

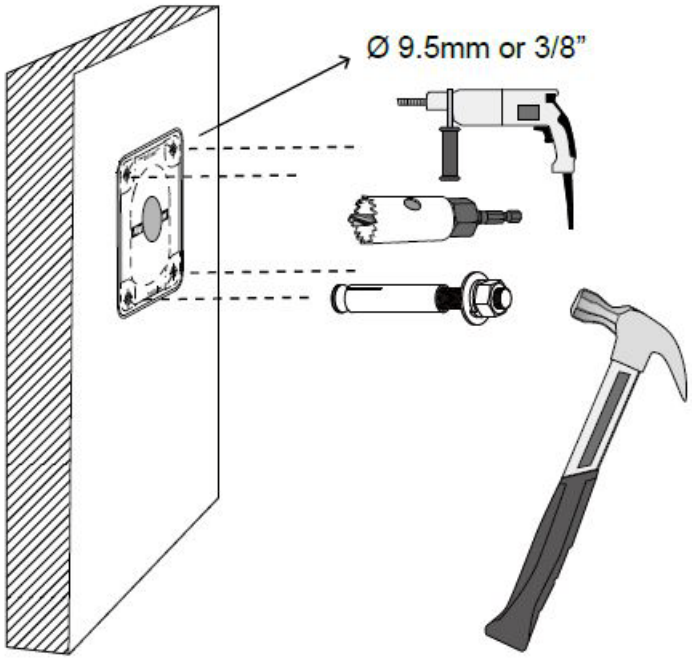
To install the Cisco Video Surveillance 8930 IP Camera, on a ceiling or wall, follow these steps:

Step 1 Make a note of the MAC address of the camera.

The MAC address is printed on the label that is attached to the camera.

Step 2 The camera weighs 6kg. Select a rigid mounting location to prevent vibration to the camera. Attach the alignment sticker to the wall.

Step 3 Drill 4 pilot holes (9.5mm in diameter and 4cm deep) into the wall, and then hammer in threaded anchors. You should hammer the anchors with hex nuts on them so that the threaded poles will not be deformed. If preferred, drill another hole for routing cables

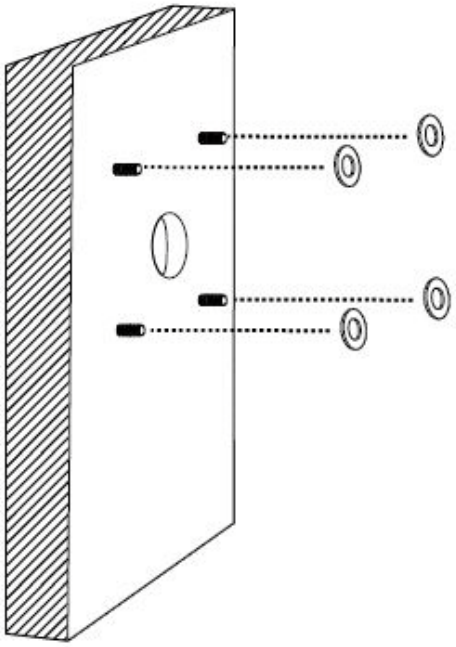


Step 4 Remove the hex nuts, washers, and leave one washer on each of the threaded poles.

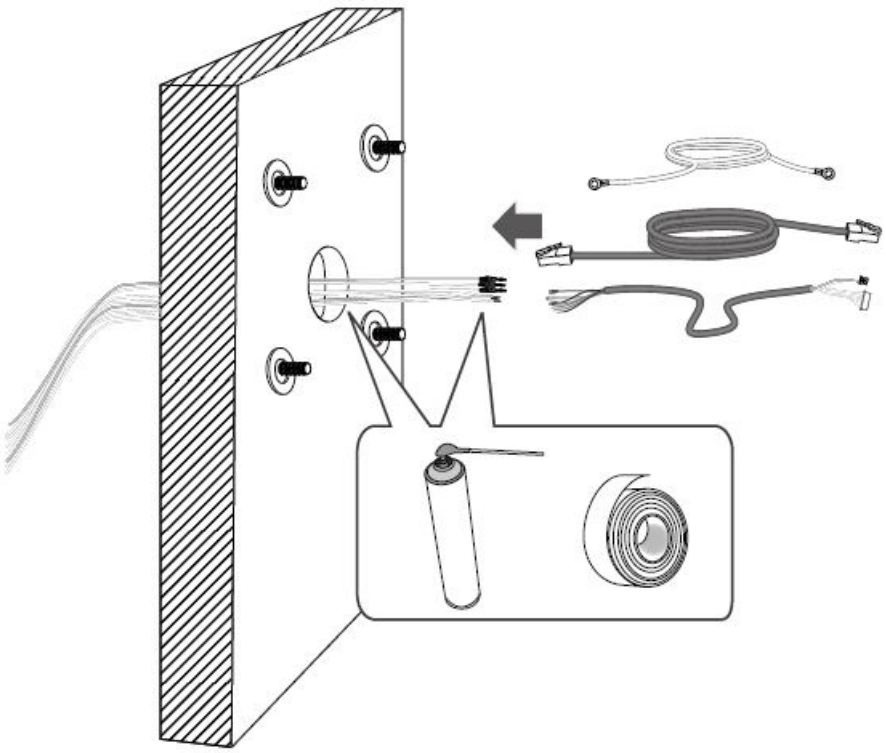
Note IO wires are user-supplied.

Avoid touching the circuit boards to prevent damage by electro static discharge.

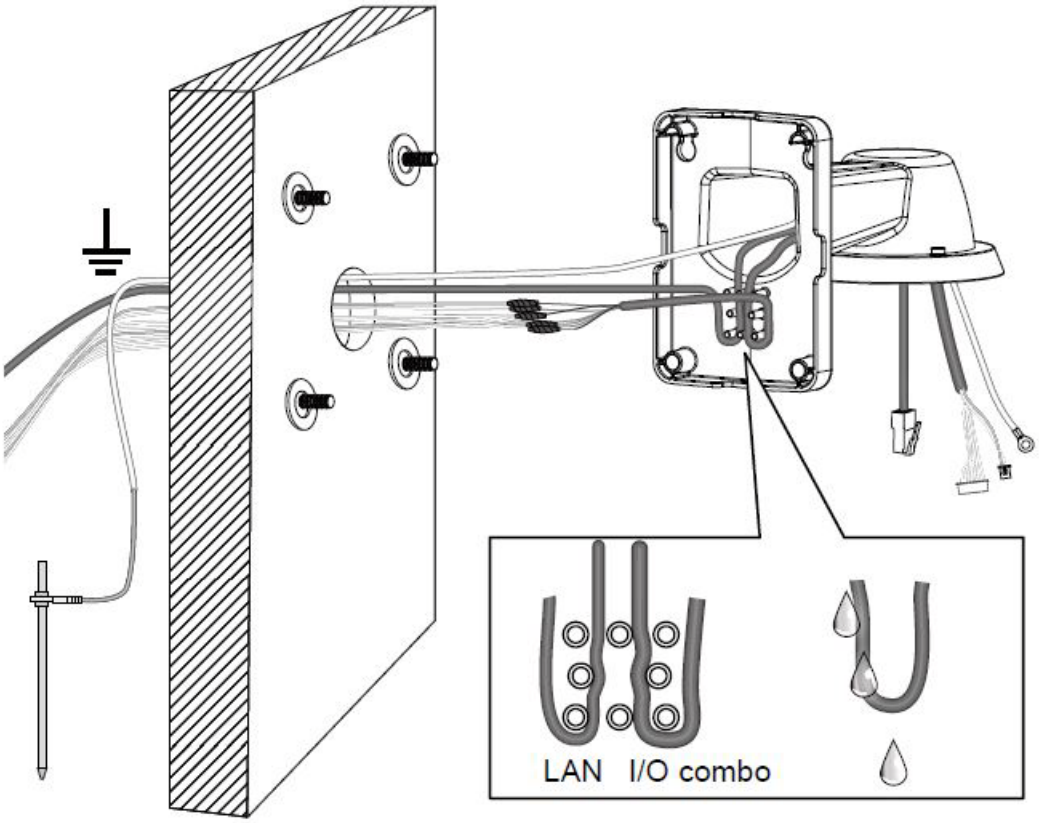
Use CAT5e, CAT6 cables only.



Step 5 Connect power or I/O wires, and use foam tapes or seal foam to ensure the back-end connection is waterproof.

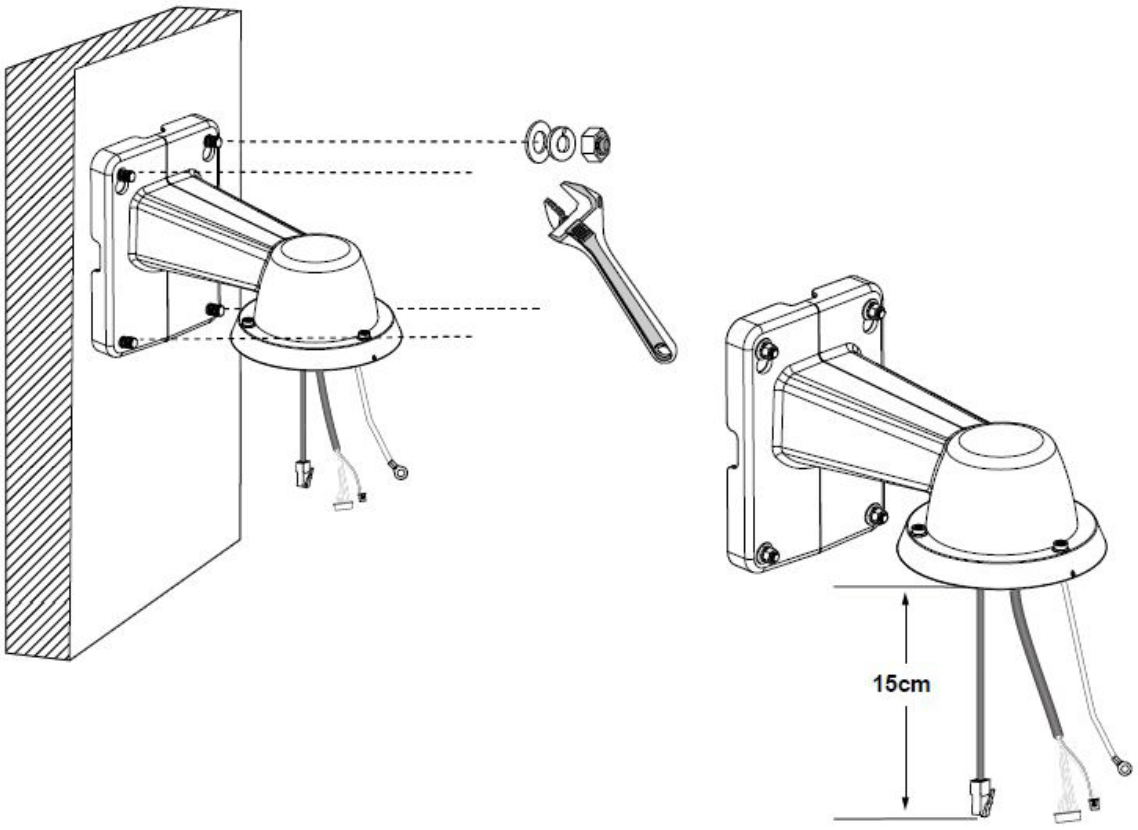


Step 6 Route your I/O combo and Ethernet cables along the routing guide poles to form drip loops.

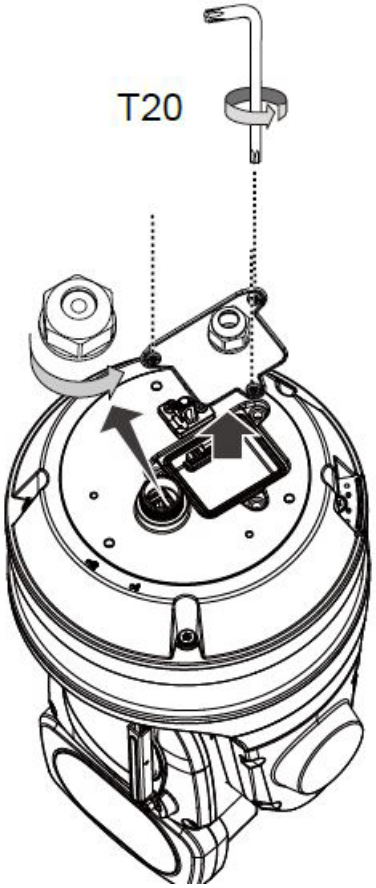


Step 7 Secure the bracket to wall.

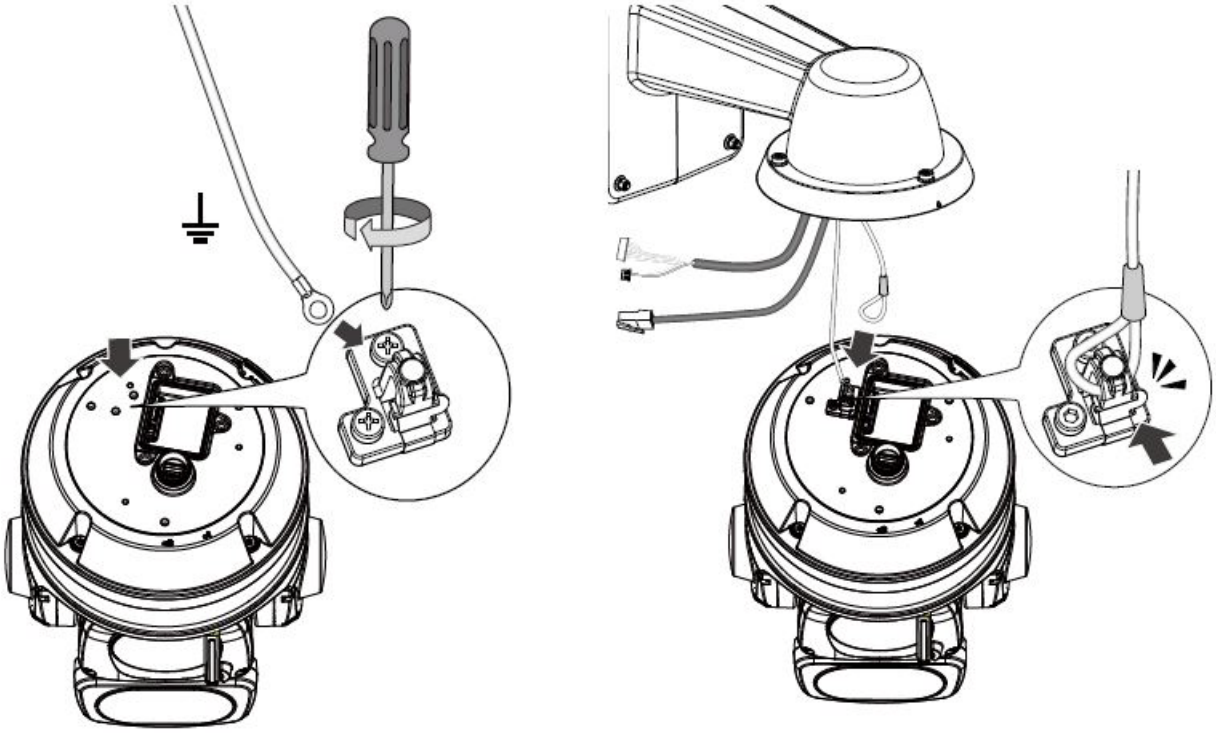
The cable length hanging on the outside of the bracket should be 15cm.



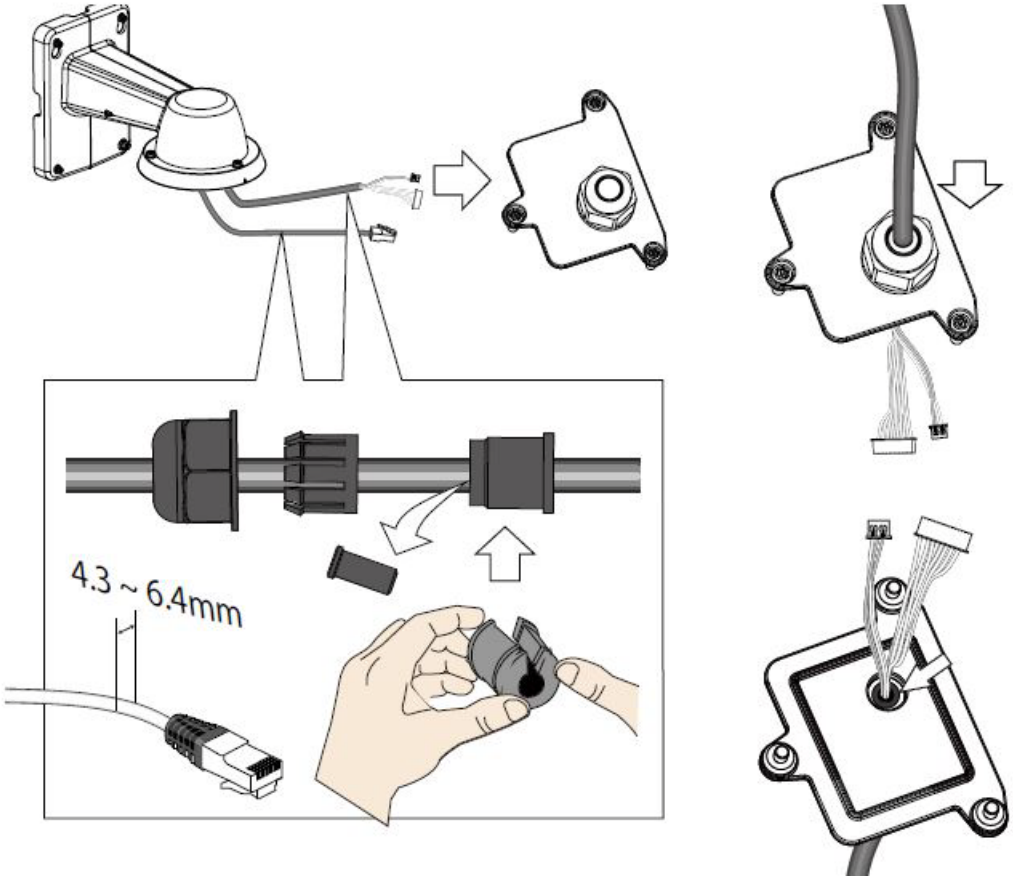
Step 8 Remove the cable gland from the LAN port. If I/O wires or 24V power are preferred, use the T20 L-wrench to remove the top cover on the I/O connectors.



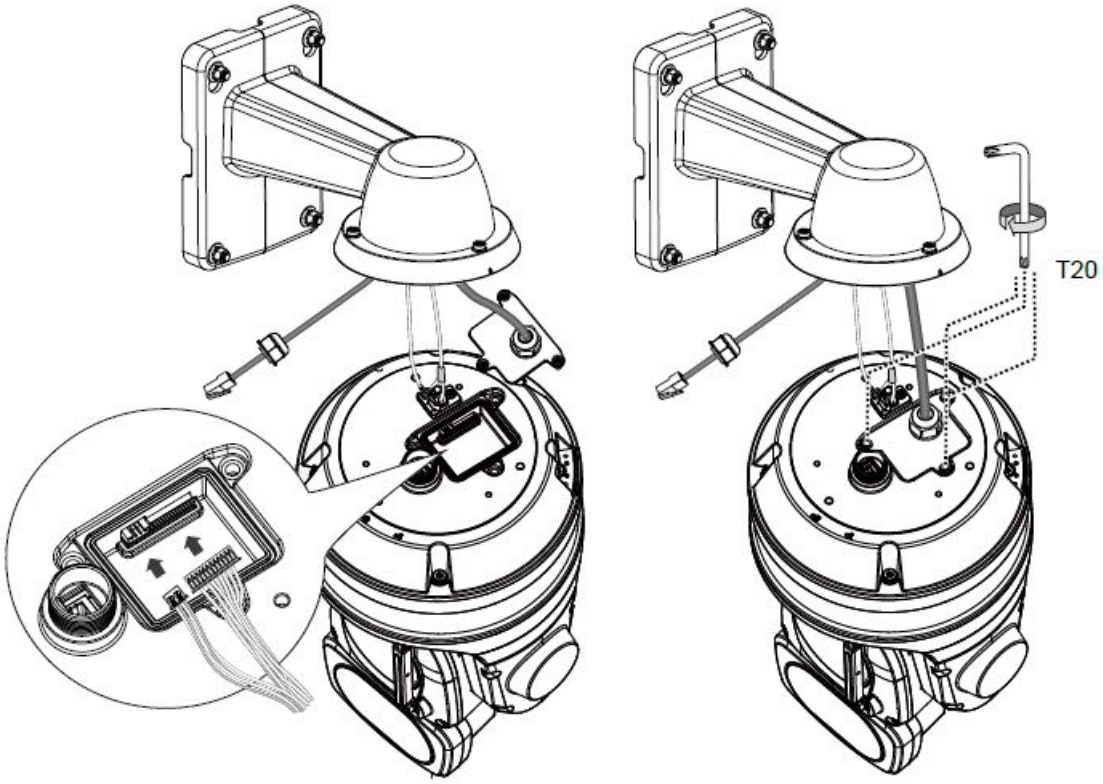
Step 9 Install the safety wire bracket, and hook up the safety wire between the bracket and the camera. Also connect the ground wire to the safety wire bracket.



Step 10 Install the components of the waterproof cable gland to the Ethernet and I/O combo cables. Make sure the outer jacket of the combo cable is flush with the cabling hole.

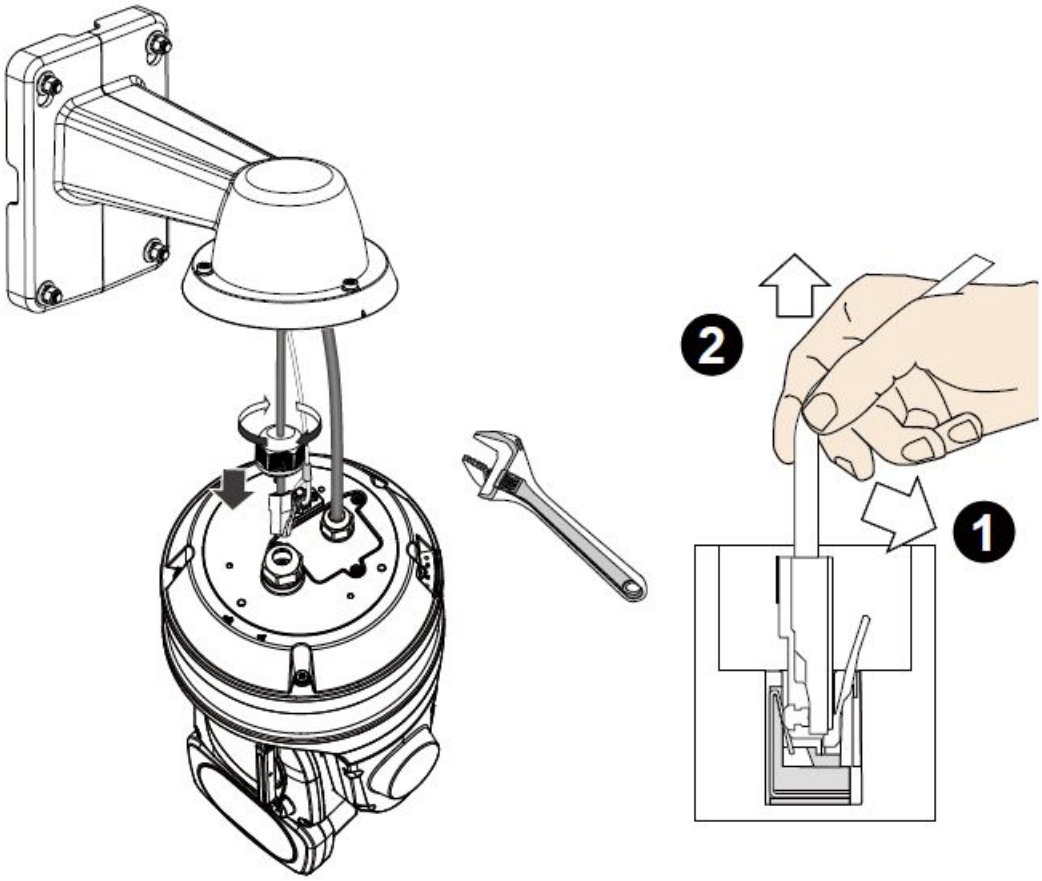


Step 11 Connect the I/O wire headers to the camera and then secure the top cover.



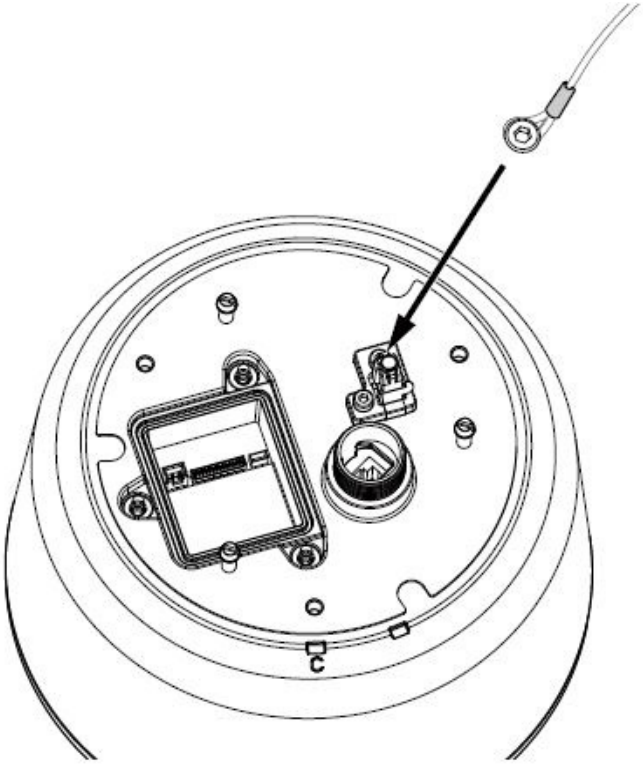
Step 12 Connect the Ethernet cable (along with its cable gland) to the camera.

Note To disconnect a LAN cable, loosen the cable gland and pull the cable against the socket wall towards the side of the locking tab

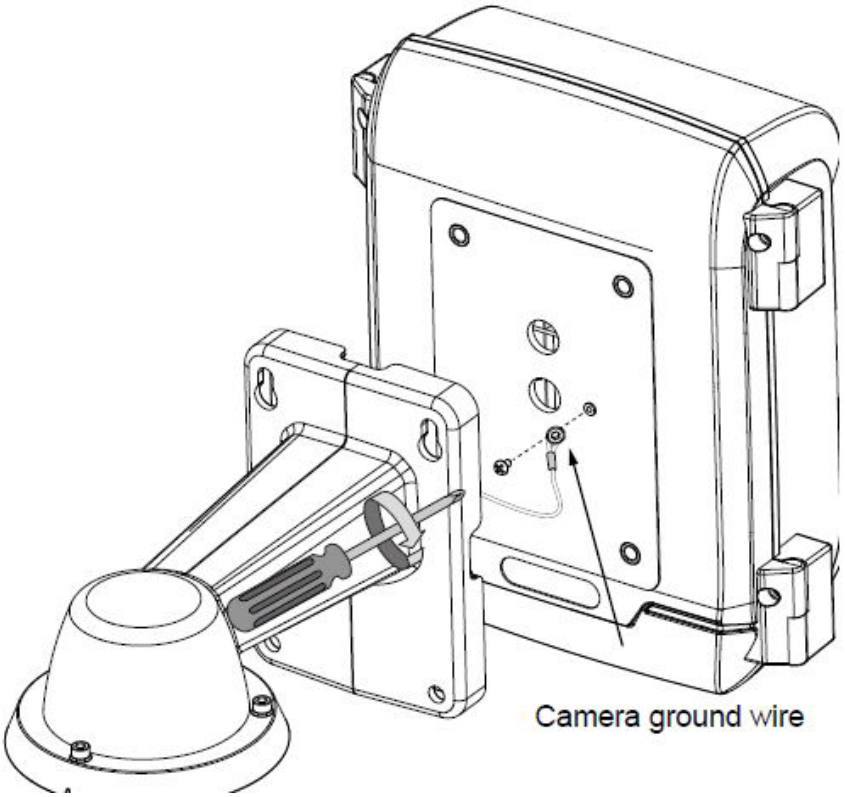


Important: Make sure all waterproof cable glands have been properly installed. Water leakage will cause irreparable damage to the camera

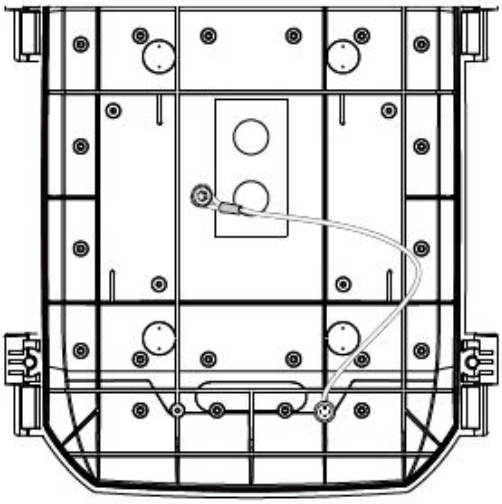
Step 13 Connect the included ground wire.

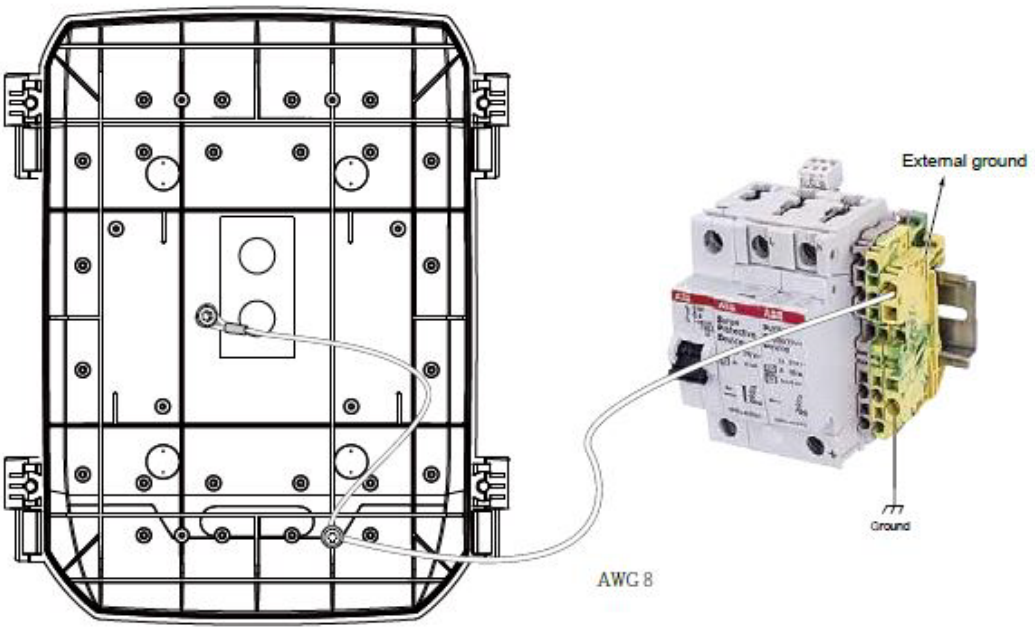


Connect the ground wire to the copper screw hole on the cabinet door.

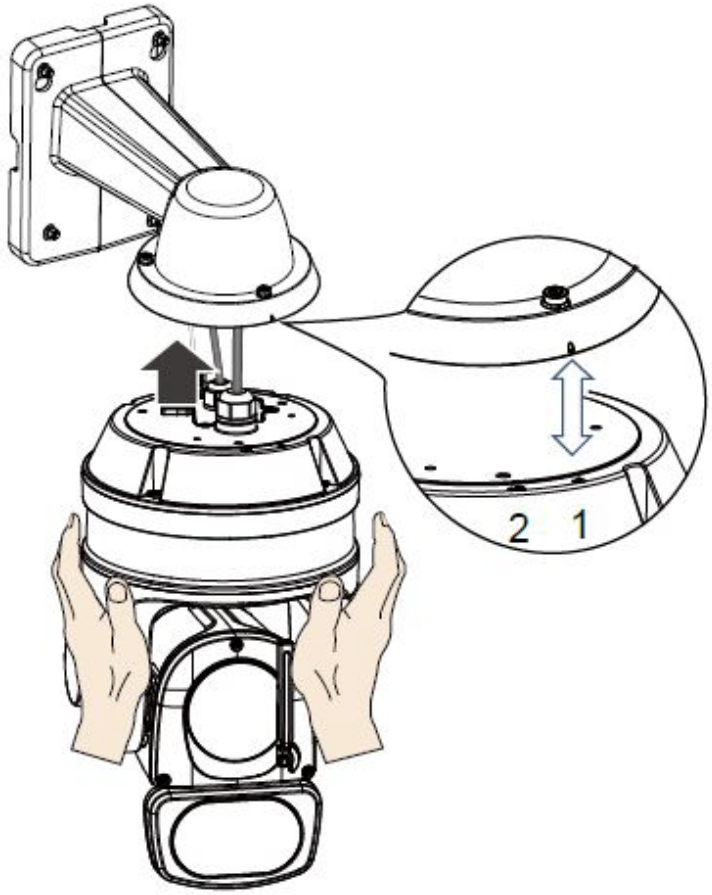


Connect all ground wires (including those from the surge protectors) to one position on the cabinet door, to the terminal block, and then to the external ground.

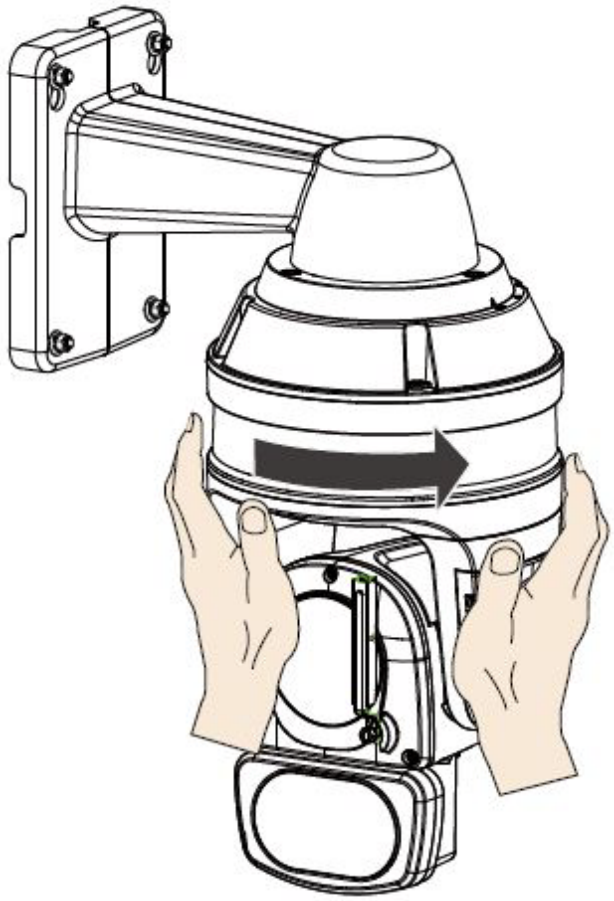




Step 14 Install the camera to bracket by aligning the mark on bracket with the #1 marking on the camera.



Step 15 Turn the camera clockwise. The camera should be locked in place.



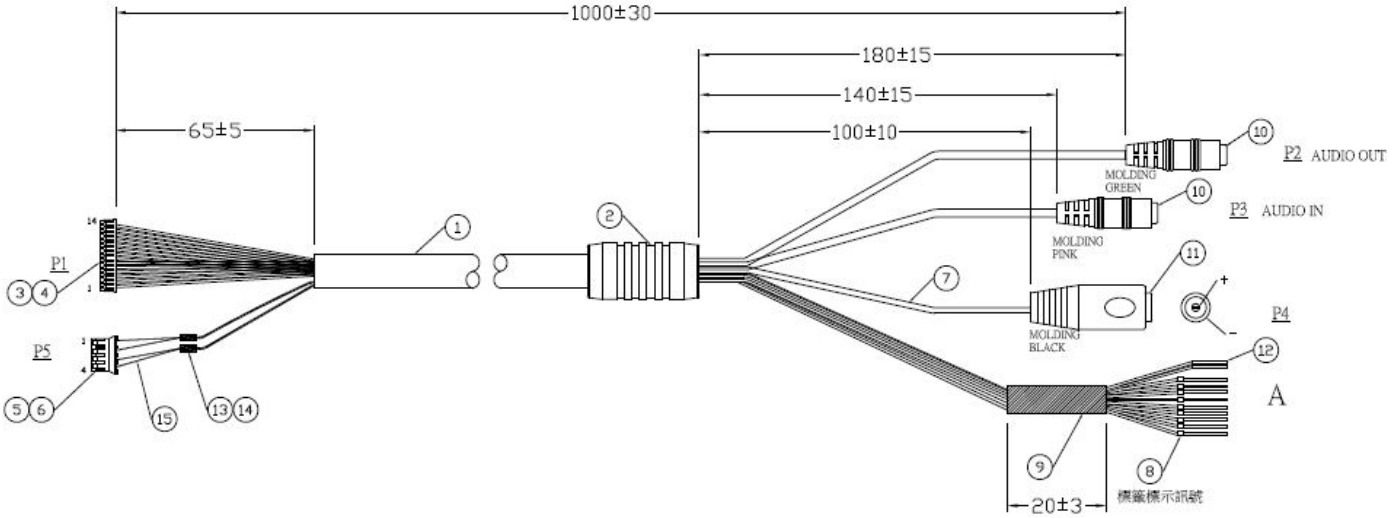
Step 16 Secure the connection using the T25 L-wrench from the top

I/O Combo Cable Specifications

Figure 1-5 shows specifications for the I/O combo cable for the camera.

All materials must be RoHS Compliant

Figure 1-5 I/O Combo Cable Specifications



1	Cable: #26x11C+#28COAXx2C+22c2c OD=7.5 mm	**9**	HT-TUBE-ϕ5mm*20mm
2	SR PVC #SC09095	**10**	Phone jack
3	Housing: Molex 51021-1400 or equivalent	**11**	DC 5.5*2.1, female #955-913
4	Thermal: Molex 50058-8000 or equivalent	**12**	Nylon-insulated butt splice conn.: KST #BNYT0.5
5	Housing: JST PHR-4 or equivalent	**13**	Terminal: CY U8005-BS0 or equivalent
6	Terminal: JST SPH-002T-P0.5S or equivalent	**14**	HT-Tube-ϕ3.5mm*10mm
7	PVC Tube ϕ2.6mm*135mm	**15**	Wire: UL1007 #24
8	Label		

Pin assignment:

Camera Input/Output Connections	**P1**	**A(COLOR)**	**P3**	**P2**
DI_4	1	Brown		
DI_3	2	Light-green		
DI_2	3	Orange		
DI_1	4	Yellow		
DO_2	5	Green		
DO_1	6	Blue		
DO+	7	Purple		
Reserved	8	Pink		
RS485–	9	White		
RS485+	10	Gray		

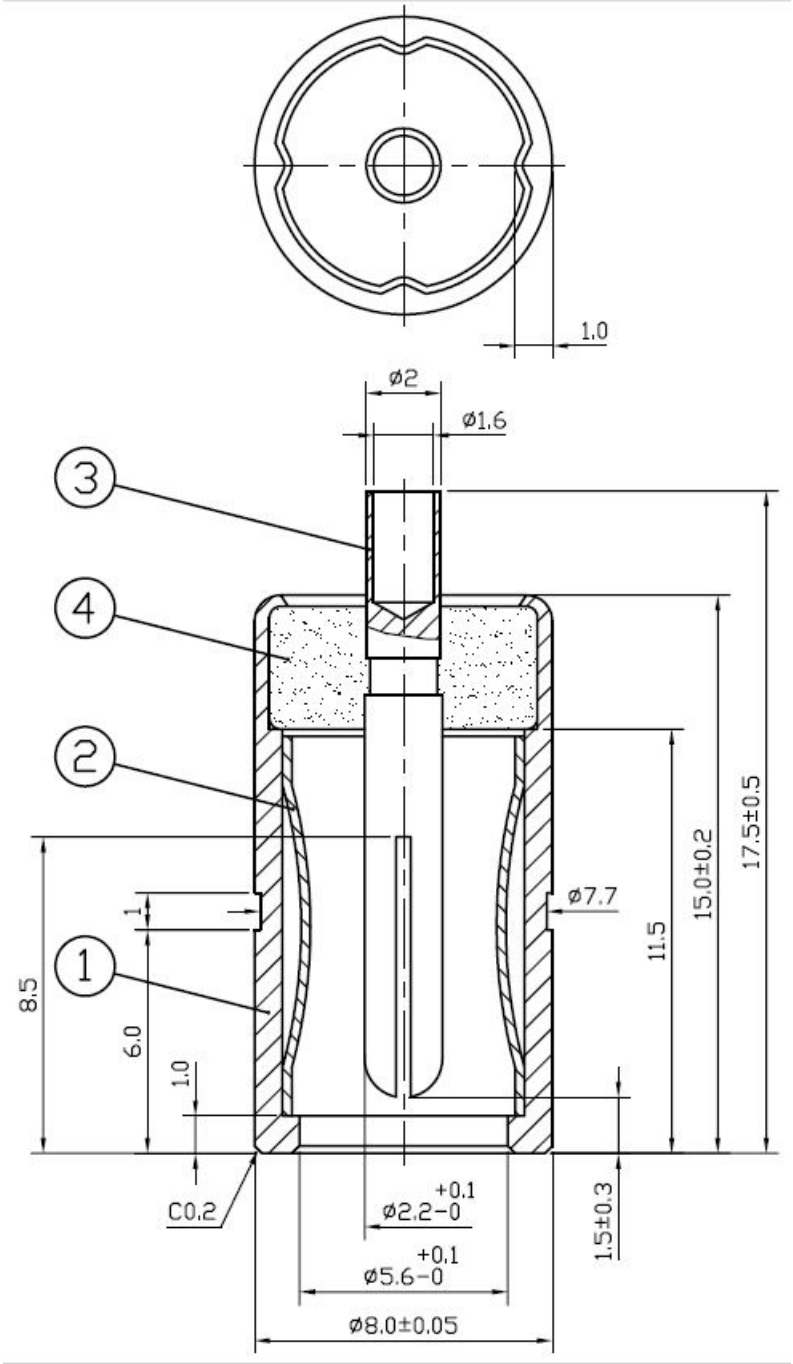
Camera Input/Output Connections	P1	A(COLOR)	P3	P2
DI–	11	Light blue		
AUDIO_IN	12	Red	1	
AUDIO_GND	13	—	GND	GND
AUDIO_OUT	14	White		1,2

P5	P4
1 (black)	—
2 (black)	—
3 (red	+
4 (red	+

The 24V DC socket dimensions are shown in Figure 1-6. The DC socket should comply with a DC jack of the following parameters:

- Connector—Straight round barrel
- Pin size /DC plug dimensions—2.1 x 5.5 x 10 mm (AxBxC)
  - A inner diameter: 2.1mm
  - B outer diameter: 5.5mm
  - C length: 10 mm

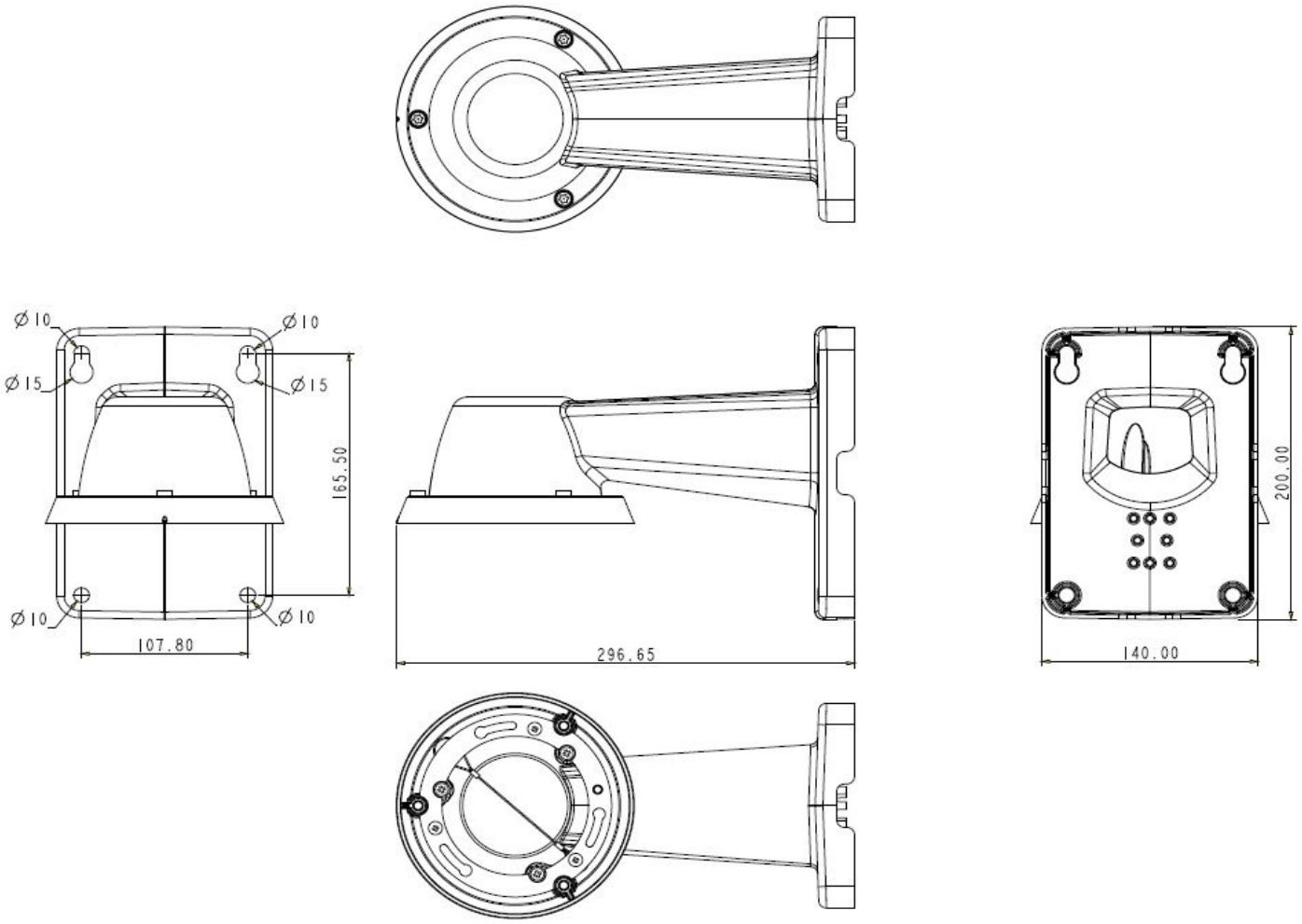
Figure 1-6 24V DC Socket Dimensions



Mechanical Dimensions

Figure 1-7 shows the dimensions of the wall mount bracket and its mounting holes.

Figure 1-7 Mechanical Dimensions



Network Deployment

The following sections provide information about deploying the camera on a network:

- Setting up the Network Camera over the Internet, page 1-26
- General Connection, page 1-29

Setting up the Network Camera over the Internet

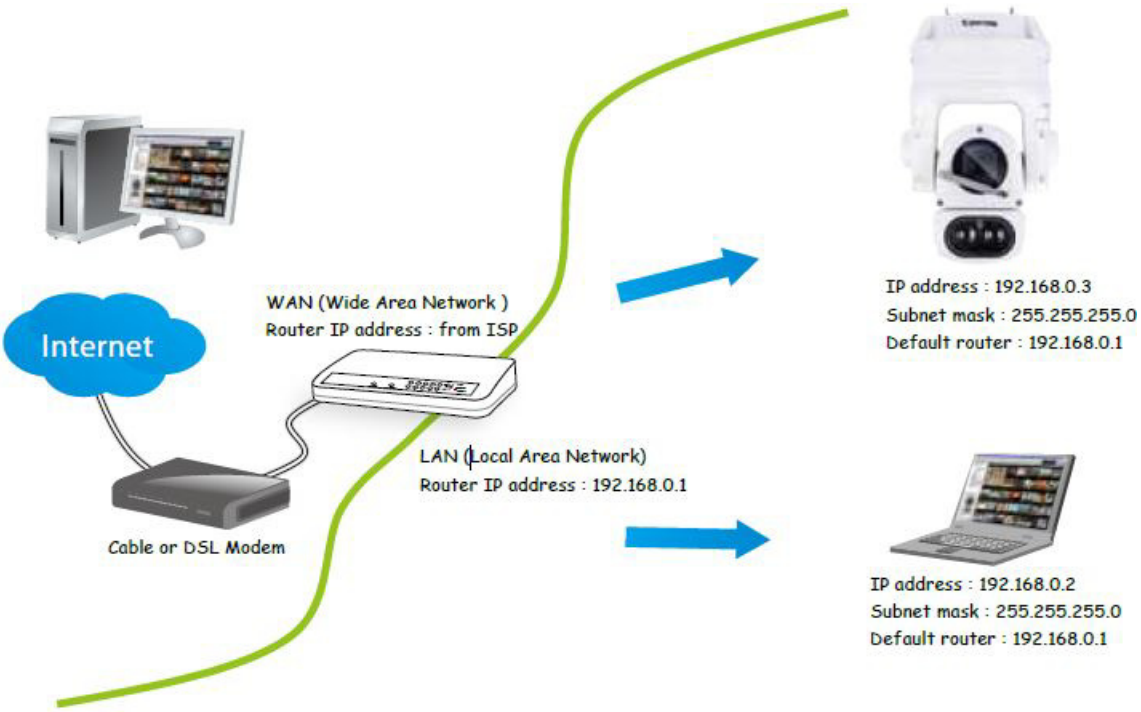
There are several ways to set up the Network Camera over the Internet. The first way is to set up the Network Camera behind a router. The second way is to utilize a static IP. The third way is to use PPPoE.

Internet Connection via a Router

Before enabling the access to the Network Camera over the Internet, make sure you have a router and follow these steps:

Step 1 Connect your camera behind a router, the Internet environment is illustrated in Figure 1-8.

Figure 1-8 Connecting the Camera Via a Router



Step 2 In this case, if the Local Area Network (LAN) IP address of your camera is 192.168.0.3, forward the following ports for the camera on the router.:

- Secondary HTTP port: 8080
- RTSP port: 554
- RTP port for audio: 5558
- RTCP port for audio: 5559
- RTP port for video: 5556
- RTCP port for video: 5557

If you have changed the port numbers on the Network page, open the ports accordingly on your router. For information about how to forward ports on the router, see your router documentation.

Step 3 Find out the public IP address of your router provided by your Internet Service Provider (ISP).

Use the public IP and the secondary HTTP port to access the camera from the Internet. See the "Network > General settings" section on page 5-20 for more information.

For example, your router and IP settings may look like this:

Device	IP Address: Internal Port	IP Address: External Port (Mapped Port on the Router)
Public IP of router	122.146.57.120	
LAN IP of router	192.168.2.1	
Camera 1	192.168.2.10:80	122.146.57.120:8000
Camera 2	192.168.2.11:80	122.146.57.120:8001
...	...	...

Configure the router, virtual server, or firewall so that the router can forward any data coming into a preconfigured port number to a camera on the private network, and allow data from the camera to be transmitted to the outside of the network over the same path.

From	Forward to
122.146.57.120:8000	192.168.2.10:80
122.146.57.120:8001	192.168.2.11:80
...	...

When properly configured, you can access a camera behind the router using the HTTP request such as: http://122.146.57.120:8000.

If you change the port numbers on the Network configuration page, open the ports accordingly on your router. For example, you can open a management session with your router to configure access through the router to the camera within your local network. See your network administrator for router configuration if you have trouble with the configuration.

For more information about network configuration options (such as that of streaming ports), choose **Configuration > Network** in the IP camera web-based interface. Cisco also provides the automatic port forwarding feature as an NAT traversal function with the precondition that your router must support the UPnP port forwarding feature.

Internet connection with static IP

Choose this connection type if you are required to use a static IP for the Network Camera. See the "Network > General settings" section on page 5-20 for more information.

Internet connection via PPPoE (Point-to-Point over Ethernet)

Choose this connection type if you are connected to the Internet via a DSL Line. See the description of PPPoE (Point-to-point over Ethernet) in the "Network > General settings" section on page 5-20.

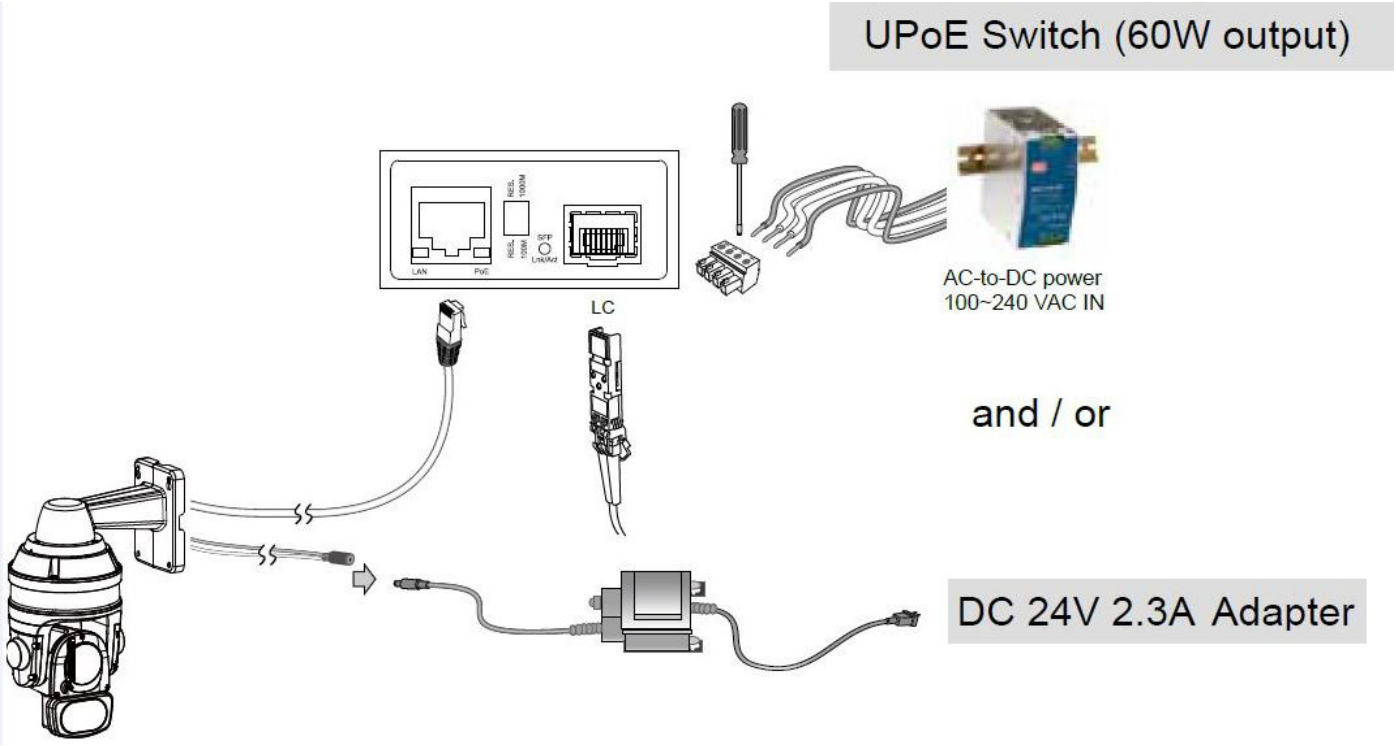
General Connection

Step 1 Connect the Network Camera's Ethernet cable (CAT5e) to a PoE Plus switch.

A 60W PoE output port alone can not drive the onboard heater, so if using the PoE switch alone, the application does not apply in low-temperature condition. When working under a temperature lower than –10ºC, a DC 24V 2.3A power adapter is required.

Step 2 Connect the power wires to a DC 24V power adapter (user-supplied). The DC 24V adapter can drive the camera and the onboard heater.

You can connect both power sources for redundancy in power supply.

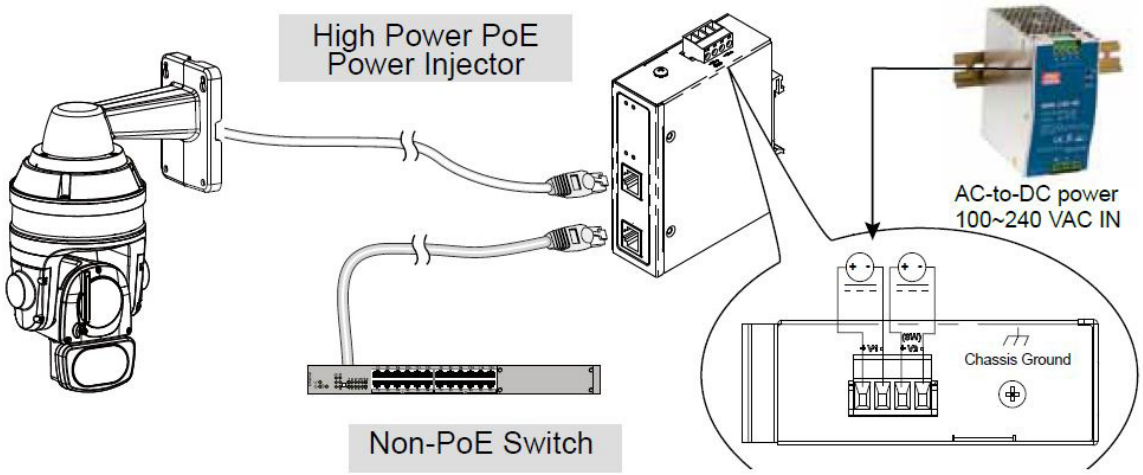


Power over Ethernet (High Power PoE)

Using a Non-PoE Switch

Use a High Power PoE power injector capable of 60W output or higher to connect between the camera and a non-PoE switch, as shown in Figure 1-9. Sufficient power is required for low temperature conditions when the onboard heater is activated

Figure 1-9 Connecting the Camera to a Non-PoE Switch



- Currently the Network Camera utilizes a 32-bit ActiveX plugin. You cannot open a management/view session with the camera using a 64-bit IE browser.
- If you encounter this problem, try execute the Iexplore.exe program from C:\Windows\ SysWOW64. A 32-bit version of IE browser will be installed.
- On Windows 7, the 32-bit explorer browser can be accessed from here: C:\Program Files (x86)\Internet Explorer\iexplore.exe
- If you experience compatibility issues between the plug-in control, you may try to uninstall the Camera Stream Controller located in: C:/Program Files (x86)/Camera Stream Controller

Accessing the IP Camera

This chapter explains how to access the IP camera through web browsers and RTSP players.

This chapter includes these topics:

- Using Web Browsers, page 2-1
- Performing the Initial Setup of the IP Camera, page 2-2
- Using RTSP Players, page 2-2
- Using 3GPP-Compatible Mobile Devices, page 2-3

Using Web Browsers

To access the camera, follow these steps:

Step 1 Launch your web browser (Microsoft Internet Explorer Mozilla Firefox).

Step 2 Enter the IP address of the camera in the address field and then press **Enter**.

Live video is displayed in your web browser.

If it is the first time installing the camera, a dialog box prompts for information. Follow the instructions to install the required plug-in on your computer.

Step 3 If you see a dialog box indicating that your security settings prohibit running ActiveX Controls, enable the ActiveX Controls for your browser:

a. Choose **Tools > Internet Options > Security > Custom Level**.

b. Look for Download signed ActiveX controls, select **Enable** or **Prompt**, and then click **OK**.

c. Refresh your web browser, then install the ActiveX control. Follow the instructions to complete installation.

Note For Mozilla Firefox or Netscape users, your browser will use Quick Time to stream live video. If you do not have QuickTime on your computer, you can download QuickTime from the web and then launch your web browser.

By default, the camera is not password-protected. To prevent unauthorized access, it is highly recommended to configure a password for your camera later. For more information about how to enable password protection, see the "Security > User accounts" procedure on page 5-28.

If you see a dialogue box indicating that your security settings prohibit running ActiveX Controls, enable ActiveX Controls for your browser:

1. Choose **Tools > Internet Options > Security > Custom Level**.
2. Look for Download signed ActiveX controls, select **Enable** or **Prompt**, and then click **OK**.
3. Refresh your web browser, then install the ActiveX control. Follow the instructions to complete installation.

Performing the Initial Setup of the IP Camera

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

By default, when the IP camera powers on, it attempts to obtain an IP address from a DHCP server in your network. If the camera cannot obtain an IP address through DCHP, an IP address is assigned using the Link-Local address scheme. The camera acquires an IP address by inserting part of its MAC address into the 169.254.x.x IP address. To do this, the camera 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, camera 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.

To connect to the IP camera for the first time and make initial configuration settings, perform the following steps:

Step 1 Start Internet Explorer, enter HTTP://*ip_address* in the address field, and press **Enter**.

Replace *ip_address* with the IP address that the IP camera obtained through DHCP or, if the camera was unable to obtain this IP address, enter 169.254.x.x as obtained by camera.

The Configure password window appears

Step 2 In the Password and Confirm Password fields, enter a password for the IP camera root user.

Step 3 Enable / disable HTTPs check box as required.

Step 4 Click **Save**.

Using RTSP Players

To view the H.265/H.264 streaming media using RTSP players, you can use one of the following players that support RTSP streaming:

- QuickTime Player

- VLC media player

Step 1 Launch the RTSP player.

Step 2 Choose **File > Open URL**. A URL dialog box will pop up.

Step 3 The address format is rtsp://*ip_address*:*rtsp_port*/*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" section on page 5-24.

Step 4 The live video will be displayed in your player.

For more information about how to configure the RTSP access name, see the "RTSP Streaming" section on page 5-24.

Using 3GPP-Compatible Mobile Devices

To view the streaming media through 3GPP-compatible mobile devices, make sure the camera can be accessed over the Internet. For more information on how to set up the camera over the Internet, see the "Network Deployment" section on page 1-26.

To utilize this feature, check the following settings on your camera:

Step 1 Because most players on 3GPP mobile phones do not support RTSP authentication, make sure the authentication mode of RTSP streaming is set to disable. For more information, see the "RTSP Streaming" section on page 5-24.

Step 2 As the bandwidth on 3G networks is limited, you will not be able to use a large video size. Set the video streaming parameters as follows. For more information, see the "RTSP Streaming" section on page 5-24.

- Video Mode—MEG-4
- Frame Size—176 X 144
- Maximum frame rate—5 fps
- Intra frame period—1S
- Video quality (Constant bit rate)—40kbps
- Audio type (GSM-AMR)—12.2 kbps

Step 3 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" section on page 5-24.

Step 4 Launch the player, such as Real Player, on the 3GPP-compatible mobile devices.

Step 5 Type the following URL command into the player. The address format is *rtsp://public_ip_address_of_your camera:rtsp_port/RTSP streaming access name for stream 3*.

For example:

rtsp://192.168.5.151:554/live.sdp

Note

- QuickTime player supports only the playback of H.265 or H.264 stream, and not the MJPEG stream. In terms of audio codec, QuickTime player supports only AAC. Since this camera supports G.711 codec, audio is not available on QuickTime player.
- VLC player supports H.265/H.264/MPEG-4/MJPEG, and all audio codecs supported by Cisco cameras.

IP Camera Main Page

This chapter explains the layout of the IP camera Main page. It is composed of the following sections: Cisco Logo, Host Name, Camera Control Area, Configuration Area, Menu, and Live Video Window.

Figure 3-1 illustrates the Main page.

Figure 3-1 Camera Main Page

1	Cisco Logo. Click this logo to visit the Cisco website

2	Resize buttons: • Click the Auto button, the video cell will resize automatically to fit the monitor • Click 100% is to display the original homepage size • Click 50% is to resize the homepage to 50% of its original size • Click 25% is to resize the homepage to 25% of its original size.
3	Host Name. The host name can be customized to fit your needs. For more information, see the "System > General settings" section on page 5-3.
4	Configuration Area: • Client Settings—Click this button to access the client setting page. For more information, see Chapter 4, "Client Settings." • Configuration—Click this button to access the configuration page of the camera. It is suggested that a password be applied to the camera so that only the administrator can configure the camera. For more information, see Chapter 5, "Configuration." • Language—Click this button to choose a language for the user interface. You can also change a language on the Configuration page
5	Video view window. Shows the video stream from the IP camera. The information in this window depends on the video stream configuration. Depending on the camera model and camera configuration, some buttons may not be available. See the "Live Video Window for MJPEG Video Streams" section on page 3-6 and the "Live Video Window for H.264 or H.265 Video Streams" section on page 3-4.
6	Go to drop-down list. If you have PTZ preset positions, these positions will be available in the Go to menu. See the "PTZ > PTZ settings" section on page 5-33 for more information.
7	Hide button. You can click the hide button to hide or display the control panel.
8	Camera Control Area: • Video stream—This camera supports multiple streams (streams 1 through 4) simultaneously. You can select any of them for live viewing. For more information about multiple streams, see the "Media > Video" section on page 5-14. • Manual trigger—Manual triggers can be turned on/off by users from the main page. The manual triggers can be associated with the Event settings, and, as the result, can be used to perform recording actions, sending notifications, and so on. see the "Event > Event settings" section on page 5-38. • Digital Output—Click to turn the digital output device on or off. • Heater control—Allows you to manually turn on or turn off the onboard heater in case you need to preheat the camera and let it become ready in a cold weather some time later. • Washer control—Wipes the exterior of the lens and IR lights twice. The function automatically turns off. • PTZ Control Panel. See the "PTZ Control Panel" section on page 3-3.

Mouse and Screen Control

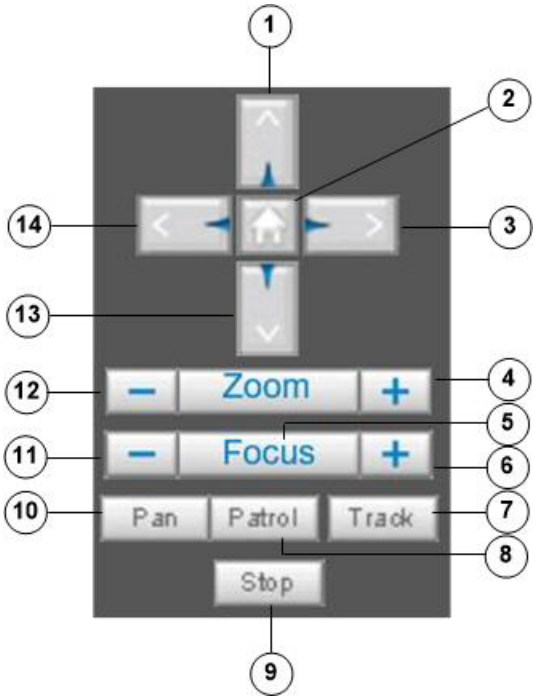
In addition to the use of a joystick, mouse control is also supported by the web session. You can click on any spot on the screen to bring that spot to the center of the view. To pan 360 degrees, you can click and hold down the left mouse button when clicking a PTZ button. The same applies to arrow keys Zoom, and Focus buttons on the PTZ panel.

Note If your screen control malfunctions, it is possible that the CPU of your current view station can not cope with the HD video feeds or that an incompatibility issue occurred with the ActiveX control plugins.

PTZ Control Panel

Figure 3-2 shows the PTZ Control Panel.

Figure 3-2 PTZ Control Panel



1	Up.
2	Return to home position.
3	Right.
4	Zoom in.
5	Auto focus.
6	Focus far.
7	Auto tracking. Allows the camera to move along following the moving objects in the current field of view. If you observe an object of your interest, click this button to track the object. Note that this function does not apply in an extremely crowded area, such as a market or sidewalk full of pedestrian activities. Constant shift of tracked objects will decrease the usability of this feature. Once started, you can use the Stop button to stop the current action. A click on the screen can also stop the tracking action. The camera only detect movements within the current field of view

8	Start auto patrol. Once the administrator has determined the list of preset positions (including the zoom-in action on a particular position), click this button to command the camera to patrol among those positions on the Patrol List. The camera will patrol continuously. For more information, please see the "PTZ > PTZ settings" section on page 5-33. Once started, you can use the Stop button to stop the current action.
9	Stop Auto Panning/patrolling/tracking. Click this button to stop the auto pan, auto patrol, and auto tracking functions
10	Start auto pan. Click to start the auto pan (360° continuous rotation). Once started, you can use the Stop button to stop the current action.
11	Focus near.
12	Zoom out.
13	Down.
14	Left

See the "PTZ > Auto tracking" section on page 5-37 for tracking configuration details

Pan /Tilt /Zoom/focus Speed

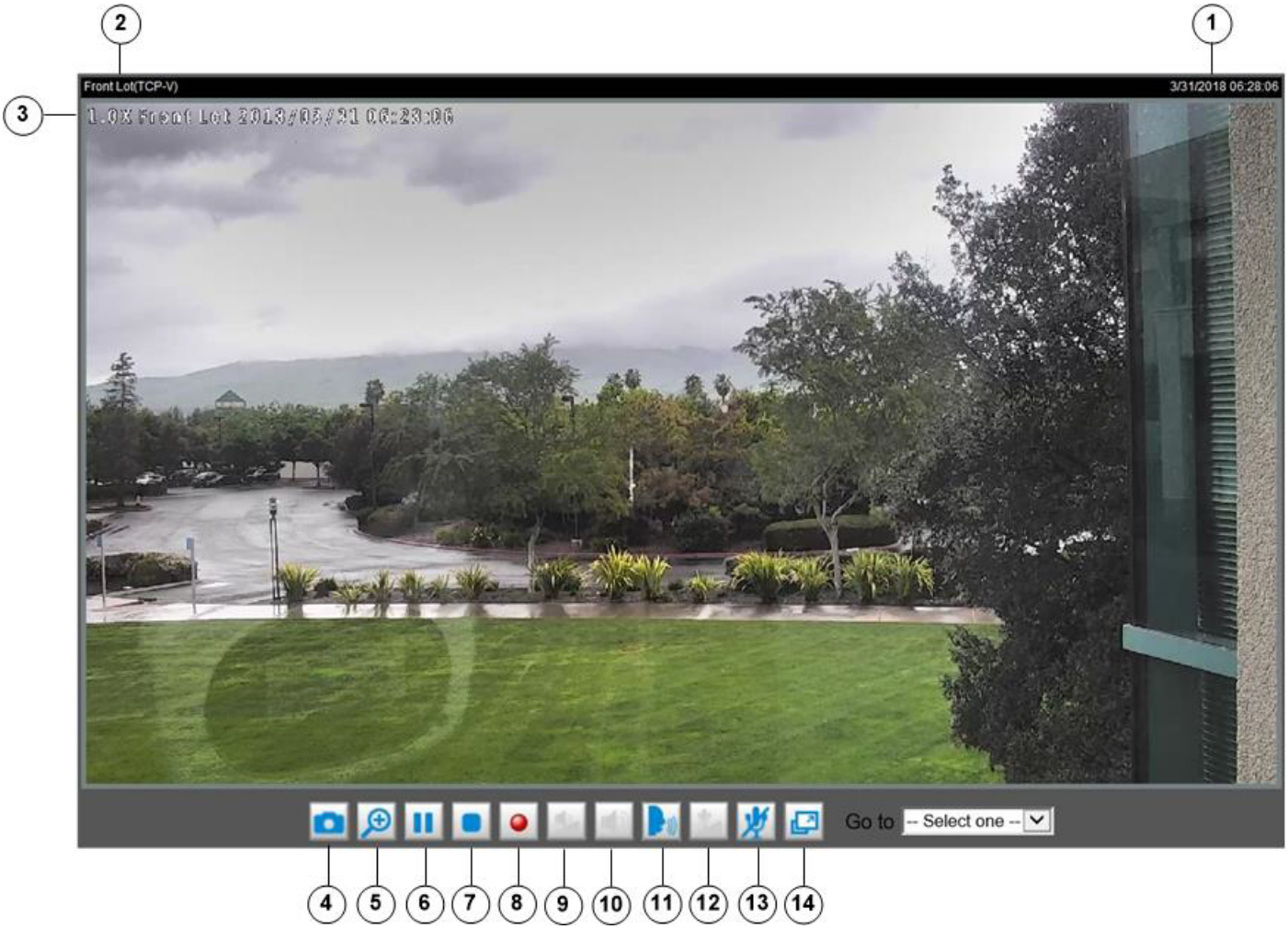
Adjust the speed of these controls when exerted:

Pan Speed	Tilt Speed	Zoom Speed	Focus Speed	
–5	–5	–5	–5	Slower
–4	–4	–4	–4	
–3	–3	–3	–3	
–2	–2	–2	–2	
–1	–1	–1	–1	
0	0	0	0	
1	1	1	1	
2	2	2	2	
3	3	3	3	
4	4	4	4	
5	5	5	5	Faster

Live Video Window for H.264 or H.265 Video Streams

When the video mode is set to H.264 or H.265, the Live Video window appears as shown in Figure 3-3. For further configuration, see Chapter 4, "Client Settings."

Figure 3-3 Live Video Window for H.264 or H.265



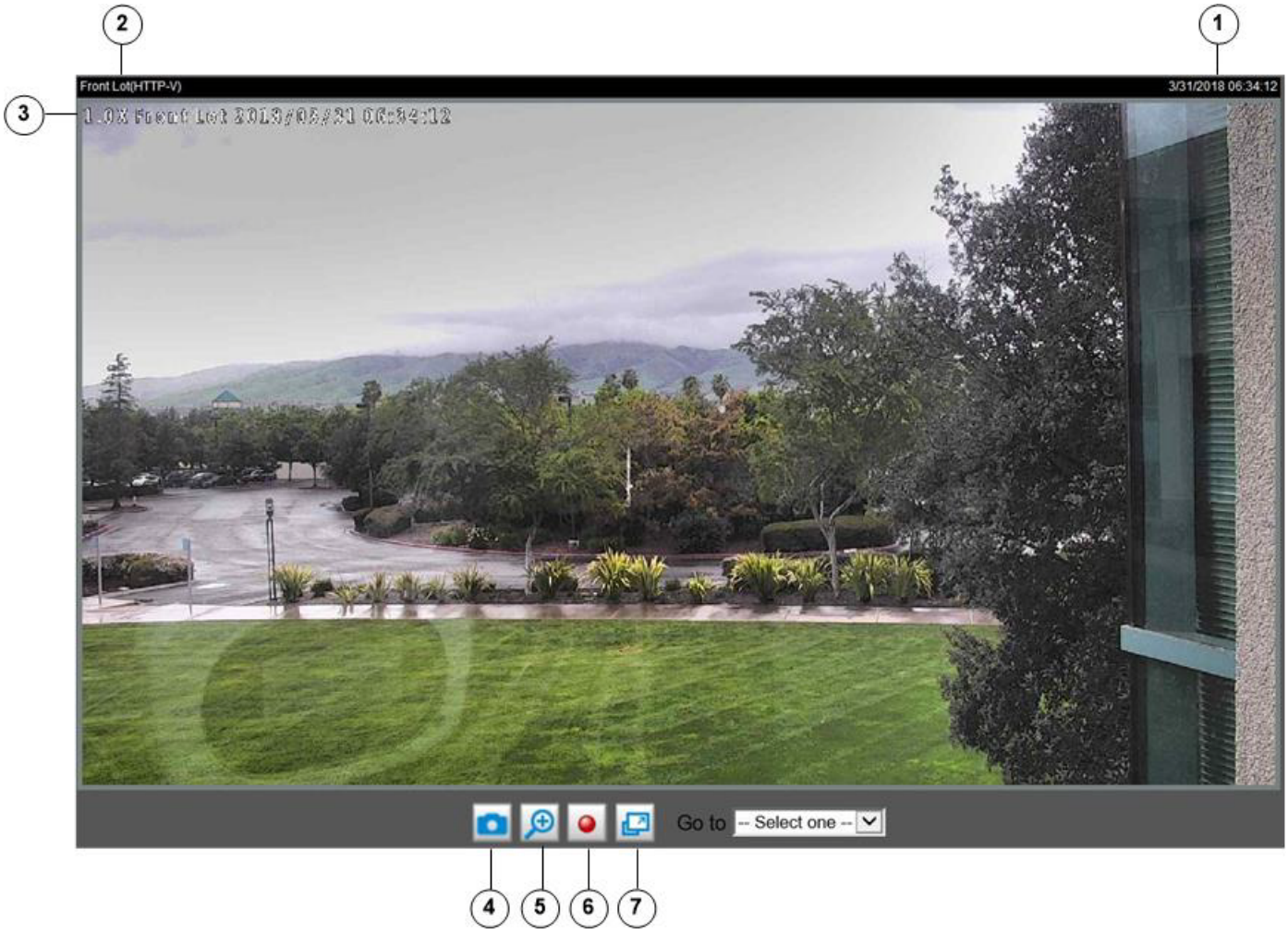
1	Time. Display the current date and time. For more information, see the "Media > Image" section on page 5-8.
2	H.265/H.264 Protocol, Media Options, and title if configured: The transmission protocol and media options for H.265 / H.264 video streaming. For further configuration, see Chapter 4, "Client Settings." The title can be configured. For more information, see the "Image settings" section on page 5-9.
3	Title and Time. The video title and time can be stamped on the streaming video. For more information, see the "Image settings" section on page 5-9.
4	Snapshot button. Click this button to capture and save still images. The captured images will be displayed in a pop-up window. Right-click the image and choose **Save Picture As** to save it in JPEG (*.jpg) or BMP (*.bmp) format.
5	Digital Zoom. Click and deselect **Disable digital zoom** to enable the zoom operation. The navigation screen indicates the part of the image being magnified. To control the zoom level, drag the slider bar. To move to a different area you want to magnify, drag the navigation screen.
6	Pause button. Pause the transmission of the streaming media. The button becomes the Resume button after clicking the Pause button.

7	Stop button. Stop the transmission of the streaming media. Click the Resume button to continue transmission.
8	Start MP4 Recording button. Click this button to record video clips in MP4 file format to your computer. Press the Stop MP4 Recording button to end recording. When you exit the web browser, video recording stops accordingly. To specify the storage destination and file name, see the "MP4 Saving Options" procedure on page 4-2.
9	Volume button. When the Mute function is not activated, move the slider bar to adjust the volume on the local computer.
10	Mute button. Turn off the volume on the local computer. The button becomes the Audio On button after clicking the Mute button.
11	Talk button. Click this button to talk to people around the camera. Audio will project from the external speaker connected to the camera. Click this button again to end talking transmission.
12	Mic Volume button. When the Mute function is not activated, move the slider bar to adjust the microphone volume on the local computer.
13	Mute. Turn off the mic volume on the local computer. The button becomes the Mic On button after clicking the Mute button.
14	Full Screen. Click this button to switch to full screen mode. Press the **Esc** key to switch back to normal mode.

Live Video Window for MJPEG Video Streams

When the video mode is set to MJPEG, the Live Video window appears as shown in Figure 3-4.

Figure 3-4 Live Video Window for MJPEG



1	Time. Display the current date and time. For more information, see the "Media > Image" section on page 5-8.
2	Video title. The video title can be configured. For more information, see the "Image settings" section on page 5-9.
3	Title and Time. The video title and time can be stamped on the streaming video. For more information, see the "Image settings" section on page 5-9.
4	Snapshot button. Click this button to capture and save still images. The captured images will be displayed in a pop-up window. Right-click the image and choose **Save Picture As** to save it in JPEG (*.jpg) or BMP (*.bmp) format.
5	Digital Zoom. Click and uncheck **Disable digital zoom** to enable the zoom operation. The navigation screen indicates the part of the image being magnified. To control the zoom level, drag the slider bar. To move to a different area you want to magnify, drag the navigation screen.
6	Start MP4 Recording button. Click this button to record video clips in MP4 file format to your computer. Press the Stop MP4 Recording button to end recording. When you exit the web browser, video recording stops accordingly. To specify the storage destination and file name, see the "MP4 Saving Options" procedure on page 4-2.

7	Full Screen button. Click this button to switch to full screen mode. Press the **Esc** key to switch back to normal mode.

Client Settings

This chapter explains how to select the stream transmission mode and saving options on a local computer. When completed with the settings on the Client Settings page, click **Save** on the page bottom to enable the settings.

This chapter includes the following sections:

- H.265/H.264 Media Options, page 4-1
- H.265/H.264 Protocol Options, page 4-1
- Two Way Audio, page 4-2
- MP4 Saving Options, page 4-2
- Local Streaming Buffer Time, page 4-2
- Joystick settings, page 4-2

H.265/H.264 Media Options

Select to stream video or audio data or both. This option is enabled only when the video mode is set to H.264 or H.265.

H.265/H.264 Protocol Options

Depending on your network environment, there are four transmission modes of H.264 or H.265 streaming:

- UDP unicast—This protocol allows for more real-time audio and video streams. However, network packets may be lost 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. Each unicast client connecting to the server takes up additional bandwidth and the camera allows up to ten simultaneous accesses.
- UDP multicast—This protocol allows multicast-enabled routers to forward network packets to all clients requesting streaming media. This helps to reduce the network transmission load of the camera while serving multiple clients at the same time. To utilize this feature, the camera must be configured to enable multicast streaming at the same time. For more information, see the "RTSP Streaming" section on page 5-24.

- TCP—This protocol 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—This protocol allows the same quality as TCP protocol without needing to open specific ports for streaming under some network environments. Users inside a firewall can utilize this protocol to allow streaming data through.

Two Way Audio

- Half duplex—Audio is transmitted from one direction at a time, for example, from a PC holding a web console with the camera.
- Full duplex—Audio is transmitted in both directions simultaneously.

MP4 Saving Options

You can record live video as you are watching it by clicking . Start MP4 Recording on the main page. Here, you can specify the storage destination and file name.

- Folder—Specify a storage destination on your PC for the recorded video files.
- File name prefix—Enter the text that will be appended to the front of the video file name.
- Add date and time suffix to the file name—Select this option to append the date and time to the end of the file name of the recorded videos. The date and time appear in the format YYYYMMDD_HHMMSS. An example files name is CLIP_20180713_180853.

Local Streaming Buffer Time

In a busy network, fluctuations in available bandwidth can occur. Video streaming may lag and may not proceed very smoothly. If you enable this option, video streams from the camera will be temporarily stored on the computer cache memory for a configurable period of time (seconds or milliseconds) before being played on a web session. This will help you see the streaming more smoothly. If you enter 3,000 Millisecond, the streaming will delay for 3 seconds.

Joystick settings

Enable Joystick

Connect the USB plug of the joystick to a USB port on your management computer. Once a USB joystick is connected, the related joystick configuration will be available on the Client settings window. The joystick should work properly without installing any other driver or software.

Then you can begin to configure the joystick settings of connected devices.

To enable joystick settings, click on the Configure buttons button. If your joystick is working properly, it will be displayed on the drop-down list.

Buttons Configuration

In the Joystick Settings window, you can use the combinations of pull-down menus, Actions and Button number, to assign joystick buttons with different functions. The number of buttons may differ from the joystick you attached.

To configure your joystick buttons, follow these steps:

Step 1 Select a button number from the Button # pull-down menu.

For example: Assign Preset 1 (move to preset 1 position) to Button 1.

Step 2 Select an action from the Actions menu. Click **Assign** to associate the button with an action.

Your configuration will be automatically saved.

Step 3 To disable an assignment, select the number of a button, and then click the **Delete** button. The associated action will then be cleared.

Step 4 Repeat the above process to assign actions to other buttons. When done, close the configuration window.

Note

- If you want to assign Preset actions to your joystick, the PTZ preset locations should be configured in advance.
- If your joystick is not working properly, it may need to be calibrated. Click the **Calibrate** button to open the Game Controllers window located in Microsoft Windows control panel and follow the instructions for trouble shooting.
- The joystick will appear in the Game Controllers list in the Windows Control panel. If you want to check out for your devices, go to the following page: Start > Control Panel > Game Controllers. Follow the onscreen instructions to calibrate your joystick.

Configuration

This chapter describes the IP camera settings options. It includes the following topics

- Accessing the Settings Pages, page 5-2
- System > General settings, page 5-3
- System > Homepage layout, page 5-3
- System > Logs, page 5-5
- System > Parameters, page 5-6
- System > Maintenance, page 5-6
- Media > Image, page 5-8
- Media > Video, page 5-14
- Media > Audio, page 5-20
- Network > General settings, page 5-20
- Network > Streaming protocols, page 5-23
- Network > QoS (Quality of Service), page 5-26
- Network > SNMP (Simple Network Management Protocol), page 5-27
- Security > User accounts, page 5-28
- Security > HTTPS (Hypertext Transfer Protocol over SSL), page 5-29
- Security > Access List, page 5-31
- Security > IEEE 802.1X, page 5-32
- Security > SSH, page 5-33
- PTZ > PTZ settings, page 5-33
- PTZ > Calibrate, page 5-37
- PTZ > Auto tracking, page 5-37
- Event > Event settings, page 5-38
- Applications > Motion detection, page 5-44
- Applications > Audio detection, page 5-46
- Applications > Package management, page 5-48
- Applications > Package management, page 5-48
- Recording > Recording settings, page 5-49

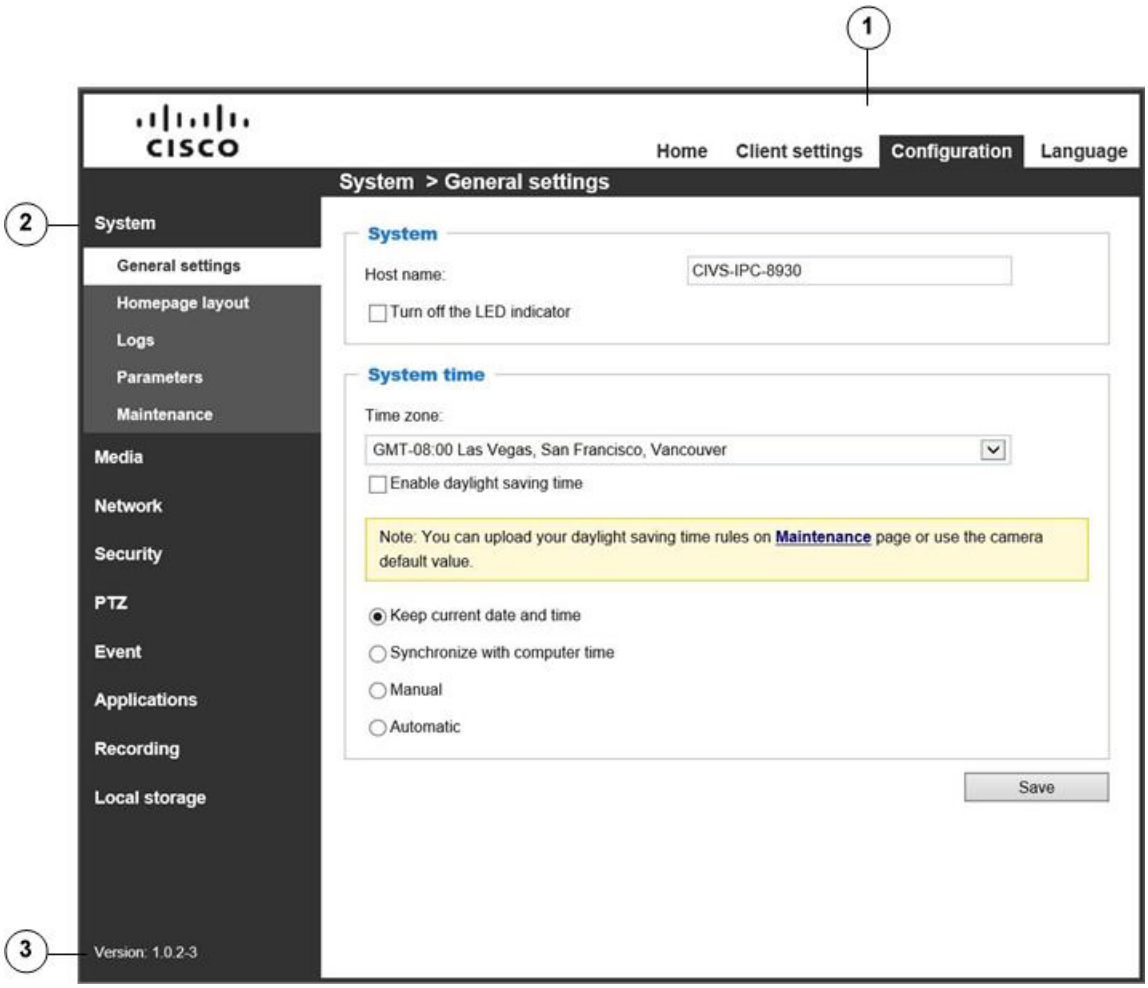
- Local storage > SD card management, page 5-50
- Local storage > Content management, page 5-51

Accessing the Settings Pages

To access the settings pages, click **Configuration** on the main page. Only Administrators can access the configuration page.See the "Security > User accounts" section on page 5-28for how to configure access rights for different users.

Figure 5-1 illustrates the configuration main page.

Figure 5-1 Configuration Main Page



1	Navigation area—Provides provides an instant switch among Home page (the monitoring page for live viewing), Configuration page, and multi-language selection
2	Configuration list—Provides access to configuration pages
3	Firmware version

System > General settings

This section explains how to configure the basic settings for the camera, such as the host name and system time. It is composed of the following two columns: System, and System Time. When finished with the settings on this page, click **Save** at the bottom of the page to enable the settings.

- Host name—Enter a desired name for the camera. The text will be displayed at the top of the main page.
- Turn off the LED indicator—Select this option to turn on the status LEDs on the camera
- Time Zone—Select the appropriate time zone from the list. If you want to upload Daylight Saving Time rules, please see the "Import/Export files" section on page 5-7.
- Keep current date and time—Select this option to preserve the current date and time of the camera. The camera internal real-time clock maintains the date and time even when the power of the system is turned off.
- Synchronize with computer time—Select this option to synchronize the date and time of the camera with the local computer. The read-only date and time of the PC is displayed as updated.
- Manual—You can enter the date and time manually. The date and time format are [yyyy/mm/dd] and [hh:mm:ss].
- Automatic—The Network Time Protocol is a protocol that synchronizes computer clocks by periodically querying an NTP server.
  - NTP server—Assign the IP address or domain name of the time-server. Leaving the text box blank connects the camera to the default time servers. Your camera must have access to the Internet.
  - Update interval—Select to update the time using the NTP server on an hourly, daily, weekly, or monthly basis.

System > Homepage layout

This section explains how to set up your own customized homepage layout.

General settings

This column shows the settings of your home page layout. You can manually select the background and font colors in Theme Options (the second tab on this page). The settings will be displayed automatically in this Preview field.

- Logo graph—Here you can change the logo that is placed at the top of your homepage. To to upload a new logo, follow these steps:
  1. Click **Custom** and the Browse field will appear.
  2. Select a logo from your files.
  3. Click **Upload** to replace the existing logo with a new one.
  4. Enter a website link if necessary.
  5. Click **Save** to enable the settings.
- Customized button—Deselect the checkbox if you do not need the Manual trigger buttons on the main page.

Theme Options

Here you can change the color of your homepage layout. There are three types of preset patterns for you to choose from. The new layout will simultaneously appear in the Preview filed. Click **Save** to enable the settings.

Figure 5-2 illustrates theme options.

Figure 5-2 Theme Options

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

To set up the custom home page, follow these steps:

Step 1 Click **Custom** on the left column.

A double-click on the color selection area (the right hand side column) will bring up a color palette window.

The palette window will pop up.

Step 2 Drag the slider bar and click on the left square to select a desired color.

The selected color will be displayed in the corresponding fields and in the Preview column.

Step 3 Click **Save** to enable the settings.

System > Logs

This section explains how to configure the camera to send the system log to a remote server as backup.

Log server settings

To set up the remote log, follow these steps:

Step 1 Select **Enable remote 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 completed, click **Save** to enable the setting.

You can configure the camera to send the system log file to a remote server as a log backup. Before utilizing this feature, we suggest that you install a log-recording tool to receive system log messages from the camera. An example is Kiwi Syslog Daemon.

System log

This column displays the system log in a chronological order. The system log is stored in the camera's buffer area and will be overwritten when the number of events reaches a preset limit.

Access log

Access log displays the access time and IP address of all viewers (including operators and administrators) in a chronological order. The access log is stored in the camera buffer area and will be overwritten when the number of events reaches a certain limit.

System > Parameters

The View Parameters page lists the entire system's parameters in an alphabetical order. If you need technical assistance, you can provide the information listed on this page to your Cisco support representative.

System > Maintenance

This chapter explains how to restore the camera to factory default, reboot, upgrade firmware version, and so on.

General settings > Upgrade firmware

This feature allows you to upgrade the firmware of your camera. It takes a few minutes to complete the process.

Note Do not power off the camera during the upgrade.

To upgrade the firmware, follow these steps:

Step 1 Download the latest firmware file from the Cisco website at this link: https://software.cisco.com/download/navigator.html.

The file is in .pkg file format.

Step 2 Click **Browse…** and locate the firmware file.

Step 3 Click **Upgrade**.

The camera starts to upgrade and will reboot automatically when the upgrade completes.

If the upgrade is successful, you will see "Reboot system now!! This connection will close". After that, access the camera again.

The following message displays when the upgrade has succeeded:

```
Reboot system now!!
This connection will close.
```

The following message is displayed when you have selected an incorrect firmware file:

```
Starting firmware upgrade...
Do not power down the server during the upgrade.
The server will restart automatically after the upgrade is
completed.
This will take about 1 - 5 minutes.
Wrong PKG file format
Unpack fail
```

General settings > Reboot

This feature allows you to reboot the camera, which takes about 1 minute to complete. When completed, the live video page will be displayed in your browser. During the reboot process, the system displays an information message and a a progress bar shows the status of the process.

If the connection fails after rebooting, manually enter the IP address of the camera in the address field to resume the connection.

General settings > Restore

This feature allows you to restore the camera to factory default settings.

- Network—Select this option to retain the Network Type settings (see the "Network > General settings" section on page 5-20).
- Daylight saving time—Select this option to retain the Daylight Saving Time settings (see the "Import/Export files" section on page 5-7).
- Custom language—Select this option to retain the Custom Language settings.
- VADP—Retain the VADP modules (third-party software stored on the SD card) and related settings.

If none of the options is selected, all settings will be restored to factory default. A status message and progress bar is displayed during the restoring process.

Import/Export files

This feature allows you to Export / Update daylight saving time rules, custom language file, configuration file, and server status report.

- Export daylight saving time configuration file—Click to set the start and end time of DST (Daylight Saving Time).

  To export, follow these steps:

  1. In the Export files column, click **Export** to export the daylight saving time configuration file from the camera.
  2. In the File Download dialog box that pops up, click **Open** to review the XML file or click **Save** to store the file for editing.
  3. Open the file with a text editor such ac Microsoft Notepad and locate your time zone; set the start and end time of DST.
  4. When completed, save the file.

- Update daylight saving time rules—Click **Browse…** and specify the XML file to update.

  If the incorrect date and time are assigned, you will see a warning message when uploading the file to the camera.

  The message "The file must have a .xml filename suffix" displays when attempting to upload an incorrect file format.

- Export language file—Click to export language strings.
- Update custom language file—Click **Browse...** and specify your own custom language file to upload.
- Export configuration file—Click to export all parameters for the device and user-defined scripts.

- Export server status report—Click to export the current server status report, such as time, logs, parameters, process status, memory status, file system status, network status, kernel message, and so on.

Tip If a firmware upgrade is accidentally disrupted, for example, by a power outage, you still have a last resort method to restore normal operation. See the following for how to bring the camera back to work:

Applicable scenario:

- Power disconnected during firmware upgrade.
- Unknown reason causing abnormal LED status, and a Restore cannot recover normal working condition.

You can use the following methods to activate the camera with its backup firmware:

1. Press and hold down the reset button for at least 1 minute.
2. Power on the camera until the red LED blinks rapidly.
3. After boot up, the firmware should return to the previous version before the camera hung. (The procedure should take 5 to 10 minutes, longer than the normal boot-up process.) When this process is completed, the LED status should return to normal.

Media > Image

This section explains how to configure the image settings of the camera. It includes the following tabs: General settings, IR Control, Image Settings, Exposure, and Privacy mask.

General settings

Video settings

- Video title.
- Show timestamp and video title in video and snapshots—Enter a name that will be displayed on the title bar of the live video.
- Position of timestamp and video title on image—Select to display time stamp and video title on the top or at the bottom of the video stream.
- Timestamp and video title font size—Select the font size for the time stamp and title.
- Video font (.ttf)—You can select a True Type font file for the display of textual messages on video.
- Color—Select to display color or black/white video streams.
- Power line frequency—Set the power line frequency consistent with local utility settings to eliminate image flickering associated with fluorescent lights.
- Power line frequency—Set the power line frequency consistent with local utility settings to eliminate image flickering associated with fluorescent lights. Note that after the power line frequency is changed, you must disconnect and reconnect the power cord of the camera in order for the new setting to take effect.
- Video orientation:

- Flip—Vertically reflect the display of the live video
- Mirror—Horizontally reflect the display of the live video. Change the settings if the camera is installed in a different orientation (which is rare for a speed dome) to correct the image orientation.

Day/Night settings

- IR cut filter—With a removable IR-cut filter, this camera can automatically remove the filter to let IR light enter the light sensor during low light conditions.
  - Auto mode—The camera automatically removes the filter by judging the level of ambient light. The Day/Night Exposure Profile will not be available if Auto mode is selected.

    Use the **Sensitivity of IR cut filter** slider that appears to tune the responsiveness of the IR cut filter to lighting conditions by the percentage. Judging by the light level, contrast, and color hue, he light sensing algorithms enable the switch between day and night modes. The actual lighting conditions can vary when the lens modules zooms in/out to a target area.
  - Day mode—The camera switches on the IR cut filter at all times to block infrared light from reaching the sensor so that the colors will not be distorted.
  - Night mode—The camera switches off the IR cut filter at all times for the sensor to accept infrared light, thus helping to improve low light sensitivity.
  - Synchronize with digital input—The camera automatically removes the IR cut filter when a digital input is triggered.
  - –Schedule mode—The camera switches between day mode and night mode based on a specified schedule. Enter the start and end time for day mode. Note that the time format is [hh:mm] and is expressed in 24-hour clock time. By default, the start and end time of a day mode are set to 07:00 and 18:00.

When completed with the settings on this page, click **Save** to enable the settings.

IR control

- Turn on built-in IR illuminator in night mode—Select this to turn on the built-in IR illuminator when the camera detects low light condition and enters the night mode.
- Turn on external IR illuminator in night mode—Select this to turn on the external IR illuminator when the camera detects low light condition and enters the night mode. A Digital Output connection to external IR is needed.

When completed with the settings on this page, click **Save** to enable the settings.

Image settings

On this page, you can make various image adjustments.

Normal light mode is for normal situations and Profile mode is for special situations.

- Enable to apply these settings at—Appears on the **Profile mode** tab only. Select the mode this profile is to apply to: Day mode or Schedule mode. Manually enter a range of time if you choose Schedule mode.
- White balance—Adjust the value for the best color temperature.
  - Auto—Automatically adjusts the image based on lighting conditions.

  - Outdoor (system default)—Using this mode enables the camera to capture images with natural white balance observable in the morning.
  - Indoor—3,200K base mode, suitable for indoor applications.
  - Sodium vapor lamp—Suitable for applications in which the field of view is lit by sodium vapor lamps.
  - Fixed current value—This option is available when the tuning the white balance. When selected, the camera will use the current color temperature setting. Note that you should use the Save button below to preserve current configuration. Otherwise, the white balance mode will return to Auto after you leave the configuration page.
  - Manual—In the manual mode, you can manually tune the R gain and Blue gain values by dragging the slide bars. Index numbers will be shown on the right hand side while changes in image is immediately displayed.
- Image Adjustment:
  - Brightness—Adjust the image brightness level, which ranges from 0% to 100%.
  - Contrast—Adjust the image contrast level, which ranges from 0% to 100%.
  - Saturation—Adjust the image saturation level, which ranges from 0% to 100%.
  - Sharpness—Adjust the image sharpness level, which ranges from 0% to 100%.
- Defog—Helps improve the visibility quality of captured image in poor weather conditions such as smog, fog, or smoke.
- 3D Noise reduction—Adjust the 3D noise reduction strength, which ranges from Low to High.

  This applies to the onboard 3D Noise Reduction feature. Use the slider to adjust the reduction strength. Applying this function to the video channel will consume system computing power.

  3D Noise Reduction is mostly applied in low-light conditions. When enabled in a low-light condition with fast moving objects, trails of after-images may occur. You may then select a lower strength level or disable the function.
- Electronic image stabilizer—Select the checkbox to enable the Electronic image stabilization (EIS) function at installation sites where vibration is expected, such as a train station.

You can click **Restore** to recall the original settings without incorporating the changes. When completed with the settings on this page, click **Save** to enable the setting. You can also click **Profile mode** to adjust the settings described above in a tabbed window for special lighting conditions.

Exposure

On this page, you can set the Exposure level, Max gain, Exposure mode, and IR cut filter related settings Detailed configurations will be automatically adjusted since the sensor library will automatically adjust the value according to the ambient light.

The Normal light mode tab provides options for configuring Sensor Setting 1, which is for normal situations. The Profile mode tab provides options for configuring Sensor Setting 2, which is for special situations.

Normal light mode

- Measurement Window—This function allows you to set measurement window(s) for low light compensation. For example, where low-light objects are posed against an extremely bright background. You may want to exclude the bright sunlight shining through a building corridor.
  - Full view—Calculate the full range of view and offer appropriate light compensation.
  - BLC (Back Light Compensation)—This option will automatically add a “weighted region” in the middle of the window and give the necessary light compensation.
  - HLC (Highlight Compensation)—Firmware detects strong light sources and compensates on affected spots to enhance the overall image quality. For example, the HLC helps reduce the glares produced by spotlights or headlights.
- Exposure control:
  - Exposure level—You can manually set the Exposure level, which ranges from –2.0 to +2.0 (dark to bright). You can also select other values from the Exposure mode menus and select a preferred scenario or manually configure the associated settings. You may prefer a shorter shutter time to better capture moving objects, while a faster shutter reduces light and needs to be compensated by electrical brightness gains.
  - Exposure mode—Select Auto, Iris Priority, Quality Priority, Shutter Priority, or Manual mode according to your needs.

    - Auto—System default, which automatically adjusts the iris, shutter speed, and gain for an optimal exposure level.

    - Iris Priority—When selected, the Iris adjustment slide bar will appear, allowing you to select an aperture size ranging from F14 to F1.6. Once a fixed value is selected, system firmware will automatically tune the gain and exposure time to match an optimal exposure level. The value is measured in the F-number as the ratio of the focal length to the lens diameter. Iris size is inversely proportional to the F-number; therefore, the smaller the F-number, the greater is the exposure ratio.

    - Shutter Priority—When selected, the Fixed exposure time slide bar will appear, allowing you to select an exposure time ranging from 1/10,000, to 1/1 second. Once a fixed value is selected, system firmware will automatically tune the gain and iris settings to match an optimal exposure level. Smaller F-number (larger exposure ratio, largest size of lens aperture opening) is shown on the right of the slide bar.

    - Manual—Select Manual to set a fixed exposure time, iris, and gain. Then, tune the slide bars to set the Iris adjustment, Exposure time, and Gain control to the best image quality. A shorter exposure time allows less amount of light to enter the sensor; while a higher gain control value generates certain amount of noises.

    When Manual mode is selected:

    1. The Exposure level bar will not be available.

    2. The IR cut filter setting will switch to Day Mode. If it was previously configured into other modes, the previous setting remains intact.

    3. WDR and Defog functions will be disabled using the Manual mode setting.

Note When Iris Priority is selected for the Exposure mode, the tunable aperture size is related to zoom ratio. When using different zoom ratios, the range of aperture sizes can be different. When zoom ratio is 0x, the range of iris sizes is F1.6~F14. When zoom ratio is 20x, the iris size is F3.4

Maximum gain control—Select a maximum value for the electronic gain from the slide bar. The gain value also has its effect on the sensitivity of the IR cut filter. When applying the gain control, IR cut filter setting will change accordingly.

- WDR:
  - Enable WDR Pro—Refers to the Wide Dynamic Range function that enables the camera to capture details in a high contrast environment. Use the check box to enable the function.
  - Enable WDR enhanced—This function allows users to identify more image details with an extreme contrast from an object of interest with one shadowed side against a bright background, for example, an entrance. You may select the Enable WDR enhanced check box, and then use the slide bar to adjust the strength from low to high to reach the best image quality.

You can click **Restore** to recall the original settings without incorporating the changes. When completed with the settings on this page, click **Save** to enable the settings.

Note
- Because the exposure settings are also available in the Profile setting, incorrect configurations such as a very high exposure level will let the camera consider it is operating in the Day mode even when the ambient light is actually low. The camera will falsely remove the IR cut filter, and thus results in distorted image colors. Therefore, when the IR cut filter is in the Auto mode, the Profile setting is not available.
- When set to the Night mode, the image display automatically changes to Black and White.
- There is no Preview button in the Exposure window. Configuration changes are directly reflected in the live view window.

Due to the imaging characteristics, some the related imaging functions will be disabled when the Exposure mode is changed. See the following table for details:

Exposure Mode					Default Gain
Auto					37
Shutter priority	BLC - hidden	Defog - disabled	WDR Pro - disabled		37
Iris priority	BLC - hidden	Defog - disabled	WDR Pro - disabled		37
Manual	BLC - hidden	Defog - disabled	WDR Pro - disabled	ICR mode - Auto	0

- Exposure Profile (available only when the IR cut filter is not set to the Auto mode)—If you want to configure another sensor and exposure setting for an individual day/night/schedule mode, click **Profile mode** to open the Profile of exposure settings page.

Profile mode

To set up a profile, perform the following steps.

Note Profile mode is not available if the IR cut filter option is set to Auto on the Media > Image > General tab.

Step 1 Select the Profile mode tab.

Step 2 Select the applicable mode: **Night mode** or **Schedule mode**. Manually enter a range of time if you choose the Schedule mode. These options appear only if you first enable **Enable to apply these settings at**.

When a span of time is configured using the Schedule mode, you can configure the Day/Night setting for controlling the behavior of the IR cut filter during that time.

Step 3 Configure other settings in the tab. See the previous discussions for detailed information.

Step 4 Click **Save** to enable the setting and click **Close** to exit the window.

Privacy Mask

Click **Privacy Mask** to open the settings page. On this page, you can block out sensitive zones to address privacy concerns.

Note

- The navigation buttons on the Privacy Mask tab also support the continuous move. You can click and hold down the button to move across the screen until you release the button.
- You can not create privacy masks at angles between +70° and –70°.

To set the privacy mask windows, follow theses:

Step 1 Click on the **Enable privacy mask** checkbox to enable this function.

Step 2 Use mouse clicks on the screen to move to a place where you want to create a mask. You can also use the PTZ panel to fine-tune the move to the target area.

Step 3 Enter a name for the masking window. Click **Add** to create a new window.

Step 4 Click on the **Modify** button and then use the mouse cursor to re-size the masking window, which is recommended to be at least twice the size of the object (height and width) you want to cover. You can select the Drawing mode as “Fixed in center” or “Drag to move.”

- When using the Fixed in center mode, you can move to the area of your interest, and then manually change the size and shape of the masking window.
- When using the Drag to move mode, you can move to an area of your interest using the PTZ buttons above, and then click and drag to draw a masking window. The click to move maneuver is not available when you select the Drag to move mode.

Step 5 You can also change the color of the mask from the Color menu.

Step 6 If preferred, move the field of view to other places to create more privacy masks.

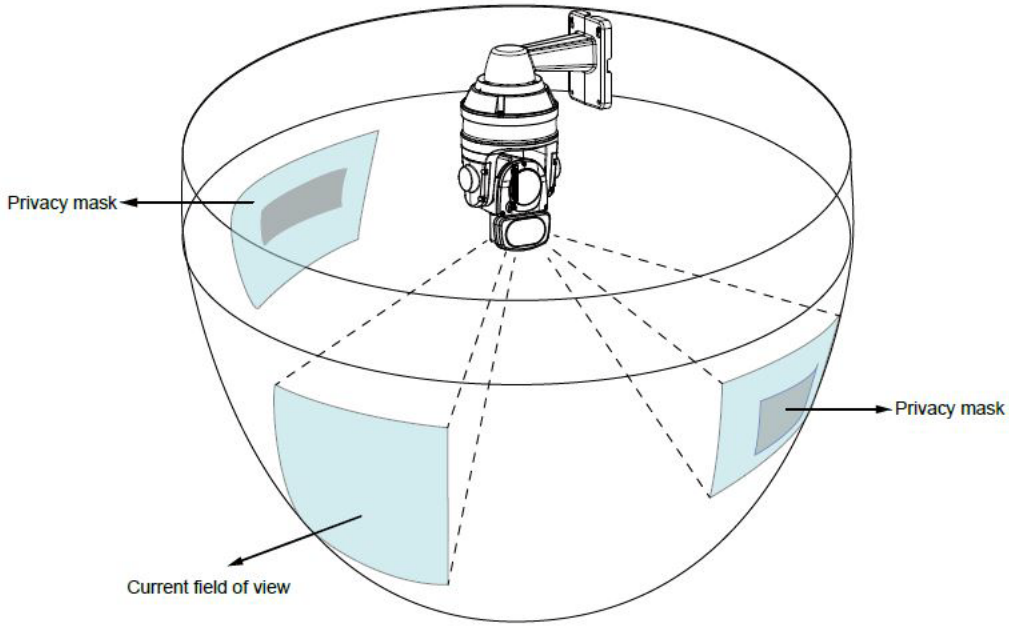
Step 7 You may be prompted by the message when trying to create a privacy mask at angles between +70° and –70°.

The camera supports “3D Privacy Mask.” Privacy masks should stay at the same positions regardless of how the camera lens may move.

When the **Enabled privacy mask** checkbox is deselected, no privacy masks will appear on screen.

Up to 24 privacy mask windows can be configured over the camera hemispheric coverage.

If you want to delete a privacy mask window, select its name from the pull-down menu at the bottom, and then click Delete to remove it.



Media > Video

Mode

The default resolution is 1080P FULL HD at 60fps, and if bandwidth or frame rate per second is of the concern, you can select a lower frame rate for the video to be streaming at 30fps.

Stream settings

The camera supports multiple streams with frame sizes ranging from 384 x 216 to 1920 x 1080 pixels.

The definition of multiple streams:

- Stream 1—Users can define the Frame sizes, compression format, image quality, etc.
- Stream 2—The default frame size for stream 2 is configured to 1280 x 720

- Stream 3—The default frame size for Stream 3 is set to the minimized 640 x 360 for viewing on mobile devices
- Stream 4—The default frame size for stream 4 is configured to 1920 x 1080 in the H.265 or H.264 mode

Click the stream item to display the detailed information.

This camera offers real-time H.265, H.264, and MJPEG compression standards (Multiple Codec) for real-time viewing. If the H.265 / H.264 mode is selected, the video is streamed via RTSP protocol. There are several parameters through which you can adjust the video performance

Note

- Video quality and fixed quality refers 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. In the event of occurrence, we suggest you customize a lower video resolution or reduce the frame rate to obtain smooth video.

- 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. A larger frame size takes up more bandwidth.
- Maximum frame rate—This limits the maximum refresh frame rate per second. Set the frame rate higher for smoother video quality and for recognizing moving objects in the field of view.

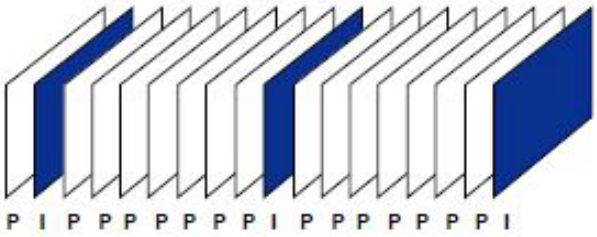
  If the power line frequency is set to 50Hz, the frame rates are selectable at 1fps, 2fps, 3fps, 5fps, 8fps, 10fps, 15fps, 20fps, 25fps, 30fps, 40fps, 45fps, and 50fps. If the power line frequency is set to 60Hz, the frame rates are selectable at 1fps, 2fps, 3fps, 5fps, 8fps, 10fps, 15fps, 20fps, 25fps, 30fps, 40fps, 45fps, 50fps, 55fps, and 60fps. You can also select Customize and manually enter a value.
- Intra frame period—Determine how often for firmware to plant an I frame. The shorter the duration, the more likely you will 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.

Smart Stream II

- Dynamic Intra frame period—High quality motion codecs, such as H.265, utilize the redundancies between video frames to deliver video streams at a balance of quality and bit rate.

  The encoding parameters for H.264/H.265 frame types are summarized and illustrated in Figure 5-3. The I-frames are completely self-referential and they are largest in size. The P-frames are predicted frames. The encoder refers to the previous I- or P-frames for redundant image information.

Figure 5-3 H.264/H.265 Frame Types



By dynamically prolonging the intervals for I-frames insertion to up to 10 seconds, the bit rates required for streaming a video can be tremendously reduced. When streaming a video of a static scene, the Dynamic Intra frame feature can save up to 53% of bandwidth. The amount of bandwidth thus saved is also determined by the activities in the field of view. If activities occur in the scene, firmware automatically shortens the I-frame insertion intervals in order to maintain image quality. In the low light or night conditions, the sizes of P-frames tend to be enlarged due to the noises, and hence the bandwidth saving effect is also reduced.

Streaming a typical 2MP scene normally requires 3~4Mb/s of bandwidth. With the Dynamic Intra frame function, the bandwidth for streaming a medium-traffic scene can be reduced to 2~3Mb/s, and during the no-traffic period of time, down to 500kb/s.

Figure 5-4 shows dynamic intra frame with static scenes. Figure 5-5 dynamic intra frame shows activities in scenes

Figure 5-4 Dynamic Intra Frame with Static Scenes

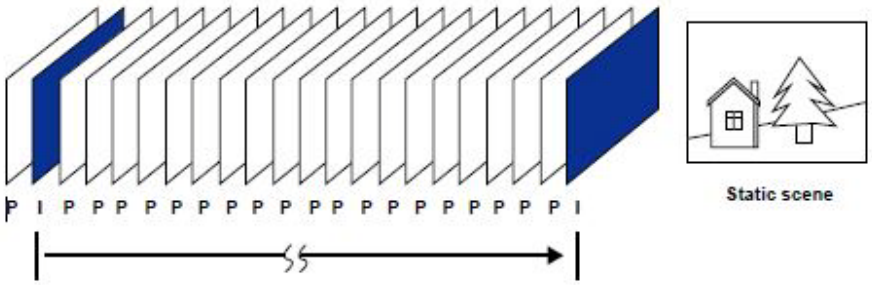
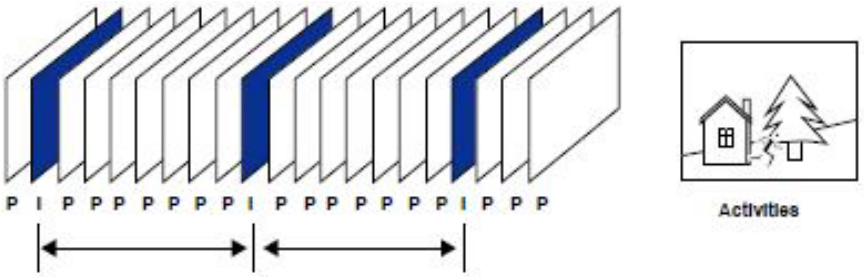


Figure 5-5 Dynamic Intra Frame with Activities in Scenes



With the H.265 codec in an optimal scenario and when Dynamic Intra frame is combined with the Smart Stream function, an 80% of bandwidth saving can be achieved compared with using H.264 without enabling these bandwidth-saving features.

- Smart codec—Smart codec effectively reduces the quality of the whole or the non-interested areas on a screen and therefore reduces the bandwidth consumed.

  You can manually specify the video quality for the foreground and the background areas.

  Select an operation mode if Smart codec is preferred:

  – Auto tracking—The Auto mode configures the whole screen into the non-interested area. The video quality of part of the screen returns to normal when one or more objects move in that area. The remainder of the screen where there are no moving objects (no pixel changes) will still be transmitted in low-quality format.

  – Manual—The Manual mode allows you to configure 3 ROI windows (Region of Interest, with Foreground quality) on the screen. Areas not included in any ROI windows will be considered as the non-interested areas. The details in the ROI areas will be transmitted in a higher-quality video format.

    As shown in Figure 5-6, the upper screen may contain little details of your interest, while the sidewalk on the lower screen is included in an ROI window.

    As the result, the lower screen is constantly displayed in high details, while the upper half is transmitted using a lower-quality format. Although the upper half is transmitted using a lower quality format, you still have an awareness of what is happening on the whole screen.

Figure 5-6 ROI Window

  – Hybrid—The major difference between the “Manual” mode and the “Hybrid” mode is that in the “Hybrid” mode, any objects entering the non-interested area will restore the video quality of the moving objects and the area around them. The video quality of the associated non-interested area is immediately restored to normal to cover the moving objects. In the “Manual” mode, the non-interested area is always transmitted using a low quality format regardless of the activities inside.

  Use the Quality priority slide bar to tune the quality contrast between the ROI and non-interested areas.

  The farther the slide bar button is to the right, the higher the image quality of the ROI areas. The farther the slide bar button to the left, the higher the image quality of the non-interested area.

In this way, you may set up an ROI window as a privacy mask by covering a protected area using an ROI window, while the remaining screen become the non-interested area. You may then configure the non-interested area to have a high image quality, or vice versa.

You should also select the Maximum bit rate from the pull-down menu as the threshold to contain the bandwidth consumption for both the high- and low-quality video sections in a smart stream.

Bit rate control

- Constrained bit rate—A complex scene generally produces a larger file size, meaning that higher bandwidth will be needed for data transmission. The bandwidth utilization is configurable to match a selected level, resulting in mutable video quality performance. The bit rates are selectable at the following rates: 20Kbps, 30Kbps, 40Kbps, 50Kbps, 64Kbps, 128Kbps, 256Kbps, 512Kbps, 768Kbps, 1Mbps, 2Mbps, 3Mbps, 4Mbps, 6Mbps, 8Mbps, 10Mbps, 12Mbps, 14Mbps, ~ to 40Mbps. You can also select Customize and manually enter a value up to 40Mbps.
  - Target quality—Select a desired quality ranging from Medium to Excellent.
  - Maximum bit rate—Select a bit rate from the pull-down menu. The bit rate ranges from 20kbps to a maximum of 40Mbps. The bit rate then becomes the Average or Upper bound bit rate number. The camera will strive to deliver video streams around or within the bit rate limitation you impose.
  - Policy—If Frame Rate Priority is selected, the camera will try to maintain the frame rate per second performance, while the image quality will be compromised. If Image quality priority is selected, the camera may drop some video frames in order to maintain image quality.
- Fixed quality:

  If Fixed quality is selected, all frames are transmitted with the same quality; bandwidth utilization is therefore unpredictable.
  - Quality—The video quality can be adjusted to the following settings: Medium, Standard, Good, Detailed, and Excellent. You can also select Customize and manually enter a value.
  - Maximum bit rate—With the guaranteed image quality, you might still want to place a bit rate limitation to control the size of video streams for bandwidth and storage concerns. The configurable bit rate starts from 1Mbps to 40Mbps.

    The Maximum bit rate setting in the Fixed quality configuration can ensure a reasonable and limited use of network bandwidth. For example, in low light conditions where a Fixed quality setting is applied, video packet sizes can tremendously increase when noises are produced with electrical gains.

    You may also manually enter a bit rate number by selecting the Customized option.

If JPEG mode is selected, the camera sends consecutive 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. There are three parameters provided in MJPEG mode to control the video performance:

- Frame size—You can set up different video resolution 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. A larger frame size takes up more bandwidth.
- Maximum frame rate—Limits the maximum refresh frame rate per second. Set the frame rate higher for smoother video quality.

If the power line frequency is set to 50Hz, the frame rates are selectable from 1fps to 25fps. If the power line frequency is set to 60Hz, the frame rates are selectable from 1fps to 30fps. You can also select Customize and manually enter a value. The frame rate will decrease if you select a higher resolution.

- Bit rate control—Fixed quality:

  If Fixed quality is selected, all frames are transmitted with the same quality; bandwidth utilization is therefore unpredictable.

  – Quality— The video quality can be adjusted to the following settings: Medium, Standard, Good, Detailed, and Excellent. You can also select Customize and manually enter a value.

  – Maximum bit rate—With the guaranteed image quality, you might still want to place a bit rate limitation to control the size of video streams for bandwidth and storage concerns. The configurable bit rate starts from 1Mbps to 40Mbps.

  The Maximum bit rate setting in the Fixed quality configuration can ensure a reasonable and limited use of network bandwidth. For example, in low light conditions where a Fixed quality setting is applied, video packet sizes can tremendously increase when noises are produced with electrical gains.

  If JPEG mode is selected, the camera sends consecutive 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. There are three parameters provided in MJPEG mode to control the video performance:

  – Frame size—You can set up different video resolution 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.

  – Maximum frame rate—Limits the maximum refresh frame rate per second. Set the frame rate higher for smoother video quality. If the power line frequency is set to 50Hz (at the 5MP resolution), the frame rates are selectable at 1fps, 2fps, 3fps, 5fps, 8fps, 10fps, and up to 25fps. If the power line frequency is set to 60Hz, the frame rates are selectable at 1fps, 2fps, 3fps, 5fps, 8fps, 10fps, and up to 30fps. You can also select Customize and manually enter a value. The frame rate will decrease if you select a higher resolution.

  – Video quality—Refer to the previous page setting for an average or upper bound threshold for controlling the bandwidth consumed for transmitting motion jpegs. The configuration method is identical to that for H.264/5.

  For Constant Bit Rate and other settings, see the explanations earlier in this section.

Note Video quality and fixed quality refers to the compression rate, so a lower compression rate 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. In the event of occurrence, we suggest you customize a lower video resolution or reduce the frame rate to obtain smooth video.

Media > Audio

Audio settings tab

The Audio settings tab includes the following items:

- Mute—Select this option to disable audio transmission from the camera to all clients. If muted, no audio data will be transmitted even if audio transmission is enabled on the Client Settings page. In that case, this message is displayed: “The media type has been changed to video only because the media from server contains no audio.”
- External microphone input gain—Select the gain of the external audio input according to ambient conditions. Adjust the gain from +21 db (most sensitive) or –33db (least sensitive).
- Audio type—Select audio codec as G.711 or G.726 and the bit rate.
  - G.711 also provides good sound quality and requires about 64Kbps. Select pcmu (u-Law) or pcma (A-Law) mode.
  - G.726 is a speech codec standard covering voice transmission at rates of 16, 24, 32, and 40kbit/s.

When completed with the settings on this page, click **Save** to enable the settings.

Note The network camera does not come with embedded microphone. An external microphone will be necessary especially if you prefer the Audio Detection feature. By default, the Audio setting is muted, and you need to manually deselect the Mute option.

Audio clips tab

The Audio clips tab includes the following items:

- Output gain—Use the slide bar to change the audio output gains value.
- Audio clip—When the camera audio input is connected to a microphone, you can record a short period of audio recordings (1 to 10 seconds). You can also use the camera embedded microphone to record an audio clip, if available. Because the memory space is limited, a recording count down will be available on screen.

  You can also upload an audio file to the camera flash memory. With amplified speakers, you can playback the audio, for example, to deter an intruder. A maximum of 2 audio clips are supported. The maximum size of the audio file to be uploaded is 2,000Kbytes.

  The voice alert is enabled in Event settings > action > Play Audio Clip. The action can be associated with triggering conditions.

Network > General settings

- LAN—Select this option when the camera 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. Remember to click on the **Save** button when you complete the Network setting.
  - Get IP address automatically—Select this option to obtain an available dynamic IP address assigned by the DHCP server each time the camera is connected to the LAN.

– Use fixed IP address—Select this option to manually assign a static IP address to the camera.

  Enter the Static IP, Subnet mask, Default router, and Primary DNS provided by your ISP or 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”.

  - Default router—This is the gateway used to forward frames to destinations in a different subnet. Invalid router setting will disable the transmission to destinations across different subnets.

  - Primary DNS—The primary domain name server that translates host names into IP addresses.

  - Secondary DNS—Secondary domain name server that backups 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.

– Enable UPnP presentation—Select this option to enable UPnP presentation for your camera so that whenever a camera is presented to the LAN, the shortcuts to connected cameras will be listed in My Network Places. You can click the shortcut to link to the web browser. To utilize this feature, make sure the UPnP component is installed on your computer.

– Enable UPnP port forwarding—To access the camera from the Internet, select this option to allow the camera to open ports automatically on the router so that video streams can be sent out from a LAN. To utilize of this feature, make sure that your router supports UPnP and it is activated.

- PPPoE (Point-to-point over Ethernet)—Select this option to configure your camera to make it accessible from anywhere as long as there is an Internet connection. To utilize this feature, it requires an account provided by your ISP.

  To acquire your camera’s public IP address, follow these steps:

  1. Set up the camera on the LAN.
  2. Go to **Configuration > Event > Event settings > Add server** (see the “Add server” section on page 5-40) to add a new email or FTP server.
  3. Go to **Configuration > Event > Event settings > Add media** (see the “Add media” section on page 5-42).

     Select System log so that you will receive the system log in TXT file format that contains the camera public IP address in your email or on the FTP server.
  4. Go to **Configuration > Network > General settings > Network type**. Select **PPPoE** and enter the user name and password provided by your ISP. Click **Save** to enable the setting.

     The camera will reboot.
  5. Disconnect the power to the camera; remove it from the LAN environment.

  If the default ports are already used by other devices connected to the same router, the camera will select other ports for the camera.

  If UPnP is not supported by your router, you will see the following message: “Error: Router does not support UPnP port forwarding.”

  To enable the UPnP user interface on your computer, follow these steps (you must log on to the computer as a system administrator to install the UPn components):

  1. From the Start menu, click **Control Panel**, then click **Add or Remove Programs**.

2. In the Add or Remove Programs dialog box, click **Add/Remove Windows Components**.
3. In the Windows Components Wizard dialog box, select Networking Services and click **Details**.
4. In the Networking Services dialog box, select **Universal Plug and Play** and click **OK**.
5. Click **Next** in the following window
6. Click **Finish**. UPnP is enabled.

UPnP networking technology provides automatic IP configuration and dynamic discovery of devices added to a network. Services and capabilities offered by networked devices, such as printing and file sharing, are available among each other without the need for cumbersome network configuration. In the case of cameras, you will see camera shortcuts under My Network Places.

Enabling UPnP port forwarding allows the camera to open a secondary HTTP port on the router—not HTTP port—meaning that you have to add the secondary HTTP port number to the camera's public address in order to access the camera from the Internet. For example, when the HTTP port is set to 80 and the secondary HTTP port is set to 8080, the following table shows the camera's IP address

From the Internet	In LAN
http://203.67.124.123:8080	http://192.168.4.160 or http://192.168.4.160:8080

If the PPPoE settings are incorrectly configured or the Internet access is not working, restore the camera to factory default; see the "General settings > Restore" section on page 5-7 for details. After the camera is reset to factory default, it will be accessible on the LAN.

- Enable IPv6—Select this option and click **Save** to enable IPv6 settings. This only works if your network environment and hardware equipment that support IPv6. The browser should be Microsoft Internet Explorer or Mozilla Firefox.

  When IPv6 is enabled, by default, the camera will listen to router advertisements and be assigned with a link-local IPv6 address accordingly.

  – IPv6 Information—Click this button to obtain the IPv6 information. If your IPv6 settings are successful, the IPv6 address list will be listed in the pop-up window.

    To link to an IPv6 address, follow these steps:

    1. Open your web browser.

    2. Enter the link-global or link-local IPv6 address in the address bar of your web browser. For example: http://[2001:0c08:2500:0002:0202:d1ff:fe04:65f4]/

    3. Press **Enter** on the keyboard or click **Refresh** button to refresh the web page.

    If you have a secondary HTTP port (the default value is 8080), you can also link to the web page using the following address format (see the "HTTP streaming" section on page 5-23for detailed information):

    http://[2001:0c08:2500:0002:0202:d1ff:fe04:65f4]/:8080

    If you choose PPPoE as the Network Type, the [PPP0 address] will be displayed in the IPv6 information column.

  – Manually setup the IP address: Select this option to manually set up IPv6 settings if your network environment does not have DHCPv6 server and router advertisements-enabled routers. If you check this item, the following fields will be displayed for you to enter the corresponding information:

- Optional IP address / Prefix length
- Optional Default Router
- Optional primary DNS

Tip You can also FTP the camera or use the "http://ip/cgi-bin/admin/lsctrl.cgi?cmd=search" command to examine the recorded files on your SD card.

Network > Streaming protocols

HTTP streaming

To utilize HTTP authentication, make sure that your have set a password for the camera first; see the "Security > User accounts" section on page 5-28 for details.

- Authentication—Depending on your network security requirements, the camera 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 can be potential risks of it being intercepted. If digest authentication is selected, user credentials are encrypted using MD5 algorithm and thus provide 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. They can also be assigned to another port number between 1025 and 65535. If the ports are incorrectly assigned, warning messages will be displayed.

  To access the camera on the LAN, both the HTTP port and secondary HTTP port can be used to access the camera. For example, when the HTTP port is set to 80 and the secondary HTTP port is set to 8080, the camera IP address on the LAN is http://192.168.4.160 or http://192.168.4.160:8080.
- Access name for stream 1 ~ 4—The camera supports multiple streams simultaneously. The access name is used to differentiate the streaming source. Users can click **Media > Video > Stream settings** to set up the video quality of linked streams. For more information about how to set up the video quality, see the "Stream settings" section on page 5-14.

  When using Mozilla Firefox to access the camera and the video mode is set to JPEG, you will receive video composed of continuous JPEG images. This technology, known as "server push," allows the camera to feed live pictures to Mozilla Firefox.

  URL command: http://*ip address*:*http port*/*access name for stream 1, 2, 3, or 4*

  For example, when the Access name for stream 2 is set to video2.mjpg:

  1. Launch Mozilla Firefox.
  2. Type the above URL command in the address bar. Press **Enter**.
  3. The JPEG images will be displayed in your web browser.

Note Microsoft Internet Explorer does not support server push technology; therefore, using http://*ip address*:*http port*/*access name for stream 1, 2, 3, or 4* will not work.

RTSP Streaming

To utilize RTSP streaming authentication, make sure that you have set a password for controlling the access to video stream first. See the "Security > User accounts" section on page 5-28 for details.

- Authentication—Depending on your network security requirements, the camera provides three types of security settings for streaming via RTSP protocol: disable, basic, and digest. If basic authentication is selected, the password is sent in plain text format, but there can be potential risks of it being intercepted. If digest authentication is selected, user credentials are encrypted using MD5 algorithm, thus providing better protection against unauthorized access.

  The availability of the RTSP streaming for the three authentication modes is listed in the following table:

	QuickTime Player	VLC Player
Disable	Yes	Yes
Basic	Yes	Yes
Digest	Yes	No

- Access name for stream 1 ~ 4—This camera supports multiple streams simultaneously. The access name is used to differentiate the streaming source. If you want to use an RTSP player to access the camera, you have to set the video mode to H.264 or H.265 and use the following RTSP URL command to request transmission of the streaming data.

  rtsp://*ip address*:*rtsp port*/*access name for stream 1 to 5*

  For example, when the access name for stream 1 is set to live.sdp:

  1. Launch an RTSP player.
  2. Choose **File > Open URL**. A URL dialog box will pop up.
  3. Type the above URL command in the text box.
  4. The live video will be displayed in your player.

- RTSP port; RTP port for video, metadata, audio; RTCP port for video, metadata, audio:
  - RTSP (Real-Time Streaming Protocol) controls the delivery of streaming media. By default, the port number is set to 554.
  - The RTP (Real-time Transport Protocol) is used to deliver video and audio data to the clients. is used to deliver video and audio data to the clients. By default, the RTP port for video is set to 5556 and the RTP port for audio is set to 5558.
  - The RTCP (Real-time Transport Control Protocol) allows the camera to transmit the data by monitoring the Internet traffic volume. the RTP port for video is set to 5557 and the RTP port for audio is set to 5559.

  The ports can be changed to values between 1025 and 65535. The RTP port must be an even number and the RTCP port is the RTP port number plus one, and thus is always an odd number. When the RTP port changes, the RTCP port will change accordingly. If the RTP ports are incorrectly assigned, the following warning message will be displayed.

  ```
  Invalid port number. RTP video port must be an even number.
  ```

- Multicast settings for stream 1, 2, 3, and 4—Click the items to display the detailed configuration information. Select the Always multicast option to enable multicast for video streams.

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. Therefore, enabling multicast can effectively save Internet bandwith.

The ports can be changed to values between 1025 and 65535. The multicast RTP port must be an even number and the multicast RTCP port number is the multicast RTP port number plus one, and thus is always odd. When the multicast RTP port changes, the multicast RTCP port will change accordingly.

If the multicast RTP video ports are incorrectly assigned, the following warning message will be displayed:

```
Invalid port number. Multicast stream 1 video port must be an even number.
```

- Multicast TTL [1~255]—The multicast TTL (Time To Live) is the value that tells the router the range a packet can be forwarded.

Initial TTL	Scope
0	Restricted to the same host
1	Restricted to the same subnetwork
32	Restricted to the same site
64	Restricted to the same region
128	Restricted to the same continent
255	Unrestricted in scope

The Multicast metadata port is utilized by Cisco VADP (Video Audio development platform) modules to transfer video analytics results, PTZ stream, textual data, and event messages between the camera and the client side running and observing the video analysis. If your client side computer is located outside the local network, you may need to open the associated TCP port on routers and firewall.

SIP

SIP is short for Session Initiation Protocol. If necessary, you can change the default port number, 5060, to one between 1025 and 65535.

- Two way audio port—By default, the two way audio port is set to 5060. Also, it can also be assigned to another port number between 1025 and 65535.

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

  As JPEG transmits only a series of JPEG images to the client, to enable the two-way audio function, make sure the video mode is set to H.264 on the Media > Video > Stream settings page and the media option is set to Media > Video > Stream settings on the Client Settings page. See Chapter 4, “Client Settings,”and see the “Stream settings” section on page 5-14.

When audio is being to the camera, “AV” appears at the end of the video title at the top of the Live Video window. In this window, click the Talk button to enable audio transmission to the camera; click to adjust Mic Volume button to adjust the volume of the microphone; click the Mute button to turn off the audio. To stop talking, click the Talk button again. (See Figure 3-3 on page 3-5 for an illustration of these buttons.)

Network > QoS (Quality of Service)

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 instance, 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 stability on the network

Requirements for QoS

To utilize QoS in a network environment, the following requirements must be met:

- All network switches and routers in the network must include support for QoS
- The network video devices used in the network must be QoS-enabled

QoS models

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 the frame priority level from 0 (lowest) to 7 (highest). The priority is set up on the network switches, which then use different queuing disciplines to forward the packets.

In the setting column for CoS, enter the VLAN ID of your switch (0~4095) and choose the priority for each application (0~7).

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

Note

- A VLAN Switch (802.1p) is required. Web browsing may fail if the CoS setting is incorrect.
- The Class of Service technologies do not guarantee a level of service in terms of bandwidth and delivery time; they offer a “best-effort.” You 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.

Use the setting options of DSCP (DiffServ Codepoint) to specify the DSCP value for each application (0~63).

Note Different vendors of network devices might have different methodologies and unique implementations. You should enter a DSCP tag value according to the information provided by the network devices.

The following table shows QoS Baseline/Technical Marketing Classification and Marking recommendations.

Application	Layer3 Classification			Layer 2 CoS/MPLS EXP	
	IPP	PHB	DSCP		
IP Routing	6	CS6	48	6	
Voice	5	EF	46	5	
Interactive video	4	AF41	34	4	QoS B
Streaming video	4	CS4	32	4	
Locally-defined mission-critical data	3	—	25	3	
Call signaling	3	AF31/CS3	26/24	3	
Transactional data	2	AF21	18	2	
Network management	2	CS2	16	2	
Bulk data	1	AF11	10	1	
Scavenger	1	CS1	8	1	
Best Effort	0	0	0	0	

Network > SNMP (Simple Network Management Protocol)

This section explains how to use the SNMP on the camera. The Simple Network Management Protocol is an application layer protocol that facilitates the exchange of management information between network devices. It helps network administrators to remotely manage network devices and find, solve network problems with ease.

The SNMP consists of the following key components:

- Manager—Network-management station (NMS), a server that executes applications that monitor and control managed devices.
- Agent—A network-management software module on a managed device that transfers the status of managed devices to the NMS.
- Managed device—A network node on a managed network. For example, routers, switches, bridges, hubs, computer hosts, printers, IP telephones, cameras, web server, and database.

Before configuring SNMP settings on the this page, enable your NMS.

SNMP Configuration

- Enable SNMPv1, SNMPv2c—Select this option and enter the names of Read/Write community and Read Only community according to your NMS settings.
- Enable SNMPv3—This option contains cryptographic security, a higher security level, that allows you to set the Authentication password and the Encryption password.
  - Read/Write security name—Enter a name for the SNMP server.
  - Authentication type—Select MD5 or SHA as the authentication method.
  - Authentication password—Enter the password for authentication (at least 8 characters).
  - Encryption password—Enter a password for encryption (at least 8 characters).
  - Read only security name—Enter a name for read only security.
  - Authentication type—Choose the type of authentication for the SNMP server.
  - Authentication password—Enter the password of the SNMP server.
  - Encryption password—Enter the encryption password of the SNMP server.

Security > User accounts

This section explains how to enable password protection and create multiple accounts.

Root Password

The administrator account name is “root”, which is permanent and can not be deleted. If you want to add more accounts in the Account management window, apply the password for the root account first.

1. Type the password identically in both text boxes, then click **Save** to enable password protection.
2. A window will prompt for authentication; type the correct user name and password in their respective fields to access the camera

Privilege Management

- Digital Output & PTZ control: You can modify the management privilege as operators or viewers. Select or deselect the check boxes, and then click **Save** to enable the settings. If you give Viewers the privilege, Operators will also have the ability to control the camera through the main page.

- Allow anonymous viewing—If you check this item, any client can access the live stream without entering a User ID and Password.

Account Management

The administrator account name is “root”, which is permanent and can not be deleted. If you want to add more accounts in the Account management window, apply the password for the root account first.

Administrators can create up to 20 user accounts.

To create a new user, follow these steps:

Step 1 Click to unfold the pull-down menu. Select **New user**.

Step 2 Enter the new user name and password. Type the password identically in both text boxes.

Some, but not all special ASCII characters are supported: !, $, %, -, ., @, ^, _, and ~. You can use them in the password combination.

The strength of your password combination is shown on the right, use the combination of alphabetic, numeric, upper case, and lower case characters until the password strength is good enough.

Step 3 Select the privilege level for the new user account. Click **Add** to enable the setting.

The privilege levels are:

- Administrator—Full control
- Operator—Control DO, white-light illuminator, snapshot, and PTZ; unable to enter the camera Configuration page
- Viewer—Control DO, white-light illuminator, view, listen, PTZ, and talk through the camera interface

Access rights are sorted by user privilege (Administrator, Operator, and Viewer). Only administrators can access the Configuration page. Viewers access only the main page for live viewing.

Here you also can change a user’s access rights or delete user accounts.

1. Select an existing account to modify.
2. Make necessary changes and click **Update** or **Delete** to enable the setting.

Security > HTTPS (Hypertext Transfer Protocol over SSL)

This section explains how to enable authentication and encrypted communication. It helps protect streaming data transmission over the Internet on higher security level.

Create and Install Certificate Method

Before using HTTPS for communication with the camera, a Certificate must be created. There are two ways to create and install a certificate:

Method 1: Create and Install Certificate

Step 1 Select the first option.

Step 2 Check **Enable HTTPS secure connection**, then select a connection option: **HTTP & HTTPS** or **HTTPS only**.

Step 3 Click **Create certificate** to generate a certificate.

The Certificate Information will automatically be displayed in the lower screen. You can click **Certificate properties** to view detailed information about the certificate.

Step 4 Click **Save** to preserve your configuration, and your current session with the camera will change to the encrypted connection.

Step 5 If your web session does not automatically change to an encrypted HTTPS session, click **Home** to return to the main page. Change the URL address from "http://" to "https://" in the address bar and press **Enter** on your keyboard. Some Security Alert dialogs will pop up. Click **OK** or **Yes** to enable HTTPS.

Method 2: Create Certificate Request and Install

Step 1 Select the option from the Method pull-down menu.

Step 2 Click **Create certificate** to proceed.

Step 3 Certificate information will show up in a pop-up window after clicking Create. Then click **Save** to generate the certificate request.

Step 4 The Certificate request displays. If you see a "pop-up blocked" message in the bar, click **OK** and click on the Information bar at the top of the page to allow pop-ups.

Step 5 Look for a trusted certificate authority, such as Symantec VeriSign Authentication Services, that issues digital certificates. Sign in and purchase the SSL certification service. Copy the certificate request from your request prompt and paste it in the signing request window of the CA. Proceed with the rest of the process as CA instructions on their web page.

Step 6 Once completed, your SSL certificate should be delivered to you via an email or other means. Copy the contents of the certificate in the email and paste it in a text/HTML/hex editor/converter, such as IDM Computer Solution UltraEdit.

Step 7 Open a new edit, paste the certificate contents, and press **ENTER** at the end of the contents to add an empty line.

Step 8 Convert file format from DOS to UNIX. Open **File** menu **> Conversions > DOS to Unix**.

Step 9 Save the edit using the ".crt" extension, using a file name like "CAcert.crt."

Step 10 Return to the original firmware session, use the **Browse** button to locate the crt certificate file, and click **Upload** to enable the certification.

Step 11 When the certificate file is successfully loaded, its status will be stated as Active. A certificate must have been created and installed before you can click the **Save** button for the configuration to take effect.

Step 12 To begin an encrypted HTTPS session, click **Home** to return to the main page. Change the URL address from "http://" to "https://" in the address bar and press Enter on your keyboard. Some Security Alert dialogs will pop up. Click **OK** or **Yes** to enable HTTPS.

Security > Access List

This section explains how to control access permission by verifying the client PC IP address.

General Settings

- Maximum number of concurrent streaming connection(s) limited to—Simultaneous live viewing for 1~10 clients (including all streams). The default value is 10. If you modify the value and click **Save**, all current connections will be disconnected and automatically attempt to re-link (IE Explorer or QuickTime Player).
- Connection management—Click this button to display the connection status window showing a list of the current connections.
  - IP address—Current connections to the camera.
  - Elapsed time—How much time the client has been at the web page (only clients currently at the live view window will be listed here).
  - User ID—If the administrator has set a password for the web page, the clients have to enter a user name and password to access the live video. The user name will be displayed in the User ID column. If the administrator allows clients to link to the web page without a user name and password, the User ID column will be empty.

    There are some situations that allow clients access to the live video without a user name and password:

    - 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 > User accounts" section on page 5-28.

    - The administrator has set up a root password, but set RTSP Authentication to "disable." For more information about RTSP Authentication, see the "RTSP Streaming" section on page 5-24.

    - The administrator has set up a root password, but allows anonymous viewing. For more information, see the "Security > User accounts" section on page 5-28.
  - Refresh—Click this button to refresh all current connections.
  - Add to deny list—You can select entries from the Connection Status list and add them to the Deny List to deny access. Those checked connections will only be disconnected temporarily and will automatically try to re-link again (IE Explore or QuickTime Player). If you want to enable the denied list, check **Enable access list filtering** and click **Save** in the first column.
  - Disconnect—If you want to break off the current connections, please select them and click this button. Those checked connections will only be disconnected temporarily and will automatically try to re-link again (IE Explorer or QuickTime Player.

Filter

- Enable access list filtering—Check this item and click **Save** if you want to enable the access list filtering function.
- Filter type—Select **Allow** or **Deny** as the filter type. If you choose Allow, only those clients whose IP addresses are on the Access List below can access the camera, and exclude the access from those that are not on the list. If you choose **Deny Type**, those clients whose IP addresses are on the Access List will not be allowed to access the camera, while those that are not on the list can.

Then you can Add a rule to the following Access List. Note that the IPv6 access list column will not be displayed unless you enable IPv6 on the Network page. For more information about IPv6 Settings, see the "Network > General settings" section on page 5-20.

There are three types of rules:

- Single—This rule allows the user to add an IP address to the Allowed/Denied List.
- Network—This rule allows the user to assign a network address and corresponding subnet mask to the Allow/Deny list. The routing prefix is written in CIDR (Classless Inter-Domain Routing) format. For example, 192.168.xx.xx/24.
- Range—This rule allows the user to assign a range of IP addresses to the Allow/Deny List. This rule is only applicable to IPv4 addresses.

Administrator IP address

- Always allow the IP address to access this device—You can check this item and add the Administrator IP address in this field to make sure the Administrator can always connect to the device.

Security > IEEE 802.1X

Enable this function if your network environment uses IEEE 802.1x, which is a port-based network access control. The network devices, intermediary switch/access point/hub, and RADIUS server must support and enable 802.1x settings.

The 802.1x standard is designed to enhance the security of local area networks, which provides authentication to network devices (clients) attached to a network port (wired or wireless). If all certificates between client and server are verified, a point-to-point connection will be enabled; if authentication fails, access on that port will be prohibited. 802.1x utilizes an existing protocol, the Extensible Authentication Protocol (EAP), to facilitate communication.

The components of a protected network with 802.1x authentication include the following:

- Supplicant—A client end user (camera), which requests authentication
- Authenticator (an access point or a switch)—A "go between" that restricts unauthorized end users from communicating with the authentication server
- Authentication server (usually a RADIUS server)—Checks the client certificate and decides whether to accept the end user access request.

Cameras support two types of EAP methods to perform authentication: EAP-PEAP and EAP-TLS.

To enable 802.1x settings, follow these steps:

Step 1 Before connecting the camera to the protected network with 802.1x, apply a digital certificate from a Certificate Authority (such as your network administrator) that can be validated by a RADIUS server.

Step 2 Connect the camera to a PC or notebook outside of the protected LAN. Open the configuration page of the camera. Select EAP-PEAP or EAP-TLS as the EAP method. In the field, enter your ID and password issued by the CA, then upload related certificate(s).

Step 3 When all settings are complete, move the camera to the protected LAN by connecting it to an 802.1x enabled switch. The devices will then start the authentication automatically.

Note The authentication process for 802.1x:

1. The Certificate Authority (CA) provides the required signed certificates to the camera (the supplicant) and the RADIUS server (the authentication server).

2. A camera requests access to the protected LAN using 802.1X via a switch (the authenticator). The client offers its identity and client certificate, which is then forwarded by the switch to the RADIUS server, which uses an algorithm to authenticate the camera and returns an acceptance or rejection to the switch.

3. The switch also forwards the RADIUS server certificate to the camera.

4. Assuming all certificates are validated, the switch then changes the camera state to authorized and is allowed access to the protected network via a preconfigured port.

Security > SSH

- Enable SSH server—Check this check box if you want to allow access to the camera through an SSH connection.
- SSH port—Enter the SSH port that is used to access the IP camera. Valid port numbers are 22 and 1024 through 65535. The default port is 22.

Click **Save** to enable the settings.

PTZ > PTZ settings

This section explains how to control the camera digital e-PTZ (Pan/Tilt/Zoom) operation. The camera comes with built-in PTZ mechanisms.

Home location settings

Move your current field of view to a preferred location using the PTZ panel or mouse clicks on the screen, and use the below buttons to configure the current view as the default home position. You can also restore the home position to the factory default, which is approximately 45 degree looking down with the lens lined up with the Cisco logo.

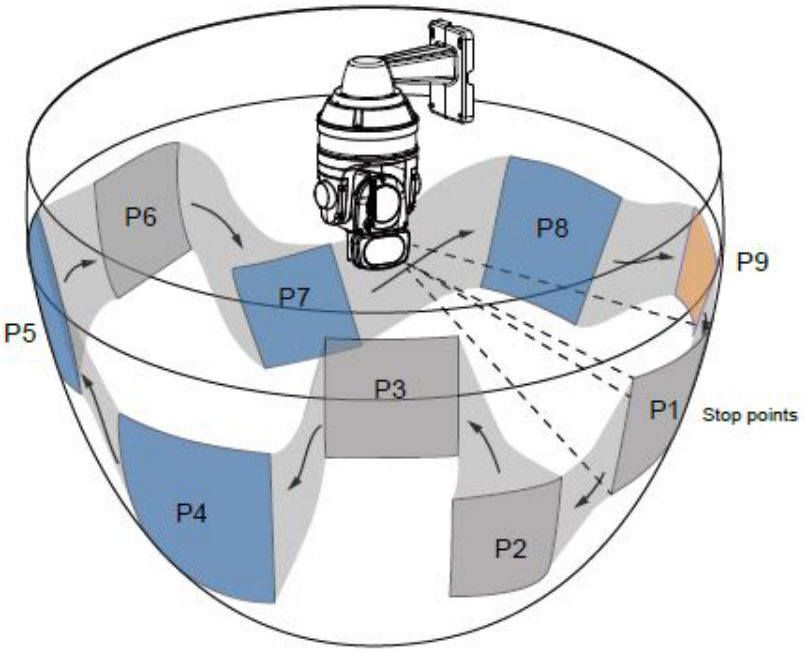
Patrol list

This column displays the configured patrols. Only one patrol can apply at a time. Use the ON/OFF buttons to enable or disable an existing patrol.

Use the **Add a recorded patrol** or **Add a reset patrol** buttons to create a recorded patrol or a preset patrol.

Recorded Patrol

The recorded patrol allows you to record the process moving along interested points (positions) in your surveillance area while the camera memorizes every Pan/Tilt/Zoom/Focus commands you gave in the process. You can then save the process as a recorded patrol. Due to the limitation on system memory, you can configure 4 recorded patrols, each with a length of 2 minutes.



To create a recorded patrol, follow these steps:

Step 1 Click the **Add a recorded patrol** button.

Step 2 In the Name field, enter a name for the patrol.

Step 3 Use the direction, zoom, and focus buttons or the PTZ panel to select a field of view as your start point.

Step 4 Select the Pan/Tilt/Zoom/Focus speed, and the PTZ control mode.

Step 5 You can then click on the Record button and start to scan through your surveillance area by moving along and staying at the points of your interest. Click the record button again to stop the recording when you visited all of your points of interest. Zoom and focus are also supported.

Step 6 You can use the playback button to review your recorded patrol before you click the Save button. When you are satisfied with the recording, click Save and Close to leave the configuration page. If you start a new recording without saving the previous one, the previous recording will be abandoned. PTZ Settings

Note The Joystick mode simulates joystick control using your mouse. Move your mouse target cursor to the direction you want and click on the screen, the lens will move to that direction. You can click and hold down the mouse button to continue scanning.

Preset Patrol

Note The navigation buttons here also support the continuous move. You can click and hold down the button to move across the screen until you release the button.

Preset positions and patrol settings

In the PTZ settings page, you can configure preset positions for the camera to travel through. A total of 256 preset positions can be configured. 40 of them can be configured into one patrol.

Follow these steps to configure preset positions and arrange them in a pan/tilt/zoom tour:

Step 1 Click the **Add a recorded patrol** button.

Step 2 Adjust the shooting area to the desired position using the keypad on the upper right side of the window. The default Home position refers to the center position defaulted in the factory. You can select another area of interest as the “Home” position. You should also select the speeds for the actions that occur during the patrol; pan, tilt, zoom, focus, and the auto pan/patrol.

Step 3 In the Name field, enter a name for a new preset position. The name can contain up to forty characters. Click **Add** to enable the settings. The preset positions will be listed on the User preset locations. (To add positions you wish, please repeat Step 2 and Step 3.)

Step 4 Select the User preset positions and click on the **Save** button at the bottom of the screen.

Step 5 Click on the move button (>>) to move positions to the Patrol locations window.

Step 6 You may select some or all of the imported positions as the stop points during the tour.

Step 7 Enter a preferred dwell time before the camera lens moves to the next position.

Step 8 Select a speed level for the auto patrol tour.

Step 9 Click on the Save button to preserve your configuration.

To remove a preset position from the list, select it and click **Remove**.

You can re-arrange the patrol order of the positions on the list using the ▲ ▼ buttons.

Misc. settings

Use the checkboxes and the pull-down menus for the camera to automatically resume the previous action or return to the home position after the camera has stayed idle for a period of time.

- PTZ control panel operation mode—Determines how your mouse and PTZ control panel works on a live view window.

  The **Continuous move** allows your screen control action to continue as long as you click and hold down the left mouse button. For example, if you click on the left button on the PTZ control panel, the camera's view should continuously rotate to the left until you release the button. The same applies to arrow keys, Zoom, and Focus buttons on the PTZ panel. If you select **Click to move**, every single mouse click takes effect for once without the ensuing move.

  If your screen control malfunctions, it is possible that the CPU of your current view station can not cope with the HD video feeds or that an incompatibility issue occurred with the ActiveX control plugins.

- Focus mode—Determines how focus takes place when camera lens is ordered to aim at different areas or preset points, or zoom in or out on a scene.
  - Auto—Firmware automatically adapts to different environments regarding the distances of objects in scene, and generates the best focus results.
  - One-time focus—Because image blurs can occur during a repeated focusing process, once moved to a scene (a preset point), the camera exerts only one automatic focus in this mode. This applies when users prefer an expected depth of field and prefer the view not to be affected by the continuous focusing acts resulting from moving objects in the scene. The One-time focus applies when using presets and a general imaging result is expected without focusing near and far.
  - Spotlight avoidance—The Spotlight avoidance mode automatically avoids the interferences of strong light sources such as spotlights in a stadium or road lamp in a dark scene.
  - Manual:

    1. When applied and moved to a position, a manual focus action is required.

    2. The second scenario applies to the use of an intelligent video analytics software, which may utilize an independent focusing algorithm. If such a 3rd-party software is implemented, none of the above focus modes apply.

- Washer options—Select Washer or Wiper. The Washer mode requires a washer kit that is externally mounted. The camera should move to a preset point where the washer kit will spill water onto it and with the help of the wiper, wash dirt from the lens. A washer action should not apply to a freezing environment.
- Washer dwelling time—The default dwelling time is 15 seconds, which allows the wiper to move twice across the lens and IR lights surface. You can change the default value for more wipes across the surface. A 4 seconds lapse exists between wipes.
- If you select the **Enable digital zoom** checkbox, you will be able to zoom in on an image by up to 360X magnification with the combination of the 30x mechanical zoom and another 12X digital zoom.
- The **Freeze image during patrol** skips the display of the process when moving from one position to another. Only the preset points are displayed.
- Zoom factor display—If you check this item, the zoom indicator will be displayed on the home page when you zoom in/out the live viewing window
- Apply previous action if the camera idles for __(1~999) seconds—You can assign an action to be taken when the camera sits idle for a configurable period time. For example, you can let camera resume a patrol tour. The resumed patrol will continue from the last preset position. You may also let the camera return to the home position. The idle state does not include the situations when the camera is performing pan or patrol action.

Return to home position: When no activities occur after a configurable period of time, let the camera lens return to the default home position.

- Positions on the Home page— The Preset positions will also be displayed on the home page. Select one from the Go to drop-down list, and the Network Camera will move to the selected position.
  - Pan button—Click this button to start the 360° horizontal auto pan.
  - Patrol button—Click this button, then the Network Camera will patrol continuously among the selected positions.

PTZ > Calibrate

This function re-calibrates the home position to the default center to recover any displacement caused by external forces. Please note that there is no confirm message after using the function, and the calibration immediately takes place. If, after a long use, a user finds it is difficult to move camera's field of view to a specific point, use this function to restore the camera original coordinates in pan and tilt motions.

PTZ > Auto tracking

In this window, you can modify the minimum object size as the triggering factor while performing the Auto Tracking function. You can move the camera view to an area of your interest, estimate, and define the possible size of objects. For example, you can designate the object size such as that of a human trespasser. The silhouette of the trespasser must be larger than the whole of the object size square box. The minimum object size is 30x30 pixels within a 320x420 view window.

Use the slide bar to tune the sensitivity of the tracking function.

This function stops when the user clicks on any buttons on the PTZ panel, or a mouse click takes place on a view window.

Users can choose to perform other functions, such as pan or patrol, simply by clicking their buttons on the PTZ panel while the camera is performing the auto tracking function.

When Auto Tracking is taking place, a "Tracking" message is displayed on the message bar.

Auto tracking is configured by designating the minimum object size. Moving objects that enter the current region of view will trigger the tracking action.

Auto tracking, if applied, is designed to track an intruder in a place where human traffic is not heavy, such as a warehouse or a load area. Heavy traffic can result in a constant shift of tracked objects, and reduce the effectiveness of the feature.

The conditions for using this function are as follows:

- The speed dome can track one object at a time.
- If multiple objects are present in the FOV, the camera tracks the object that is farthest from the camera.
- If a tracked object stays motionless for 10 seconds, camera will abandon it and start tracking another object that is farthest away from the center.
- The zoom-in ratio while tracking is determined by the zoom ratio of the camera lens when the tracking is triggered.

- Manual control always has a higher priority than Auto tracking, such as using a joystick to pan or tilt or using a click on VAST view cell.
- Objects can easily move away from an FOV when the zoom-in ratio is high. Therefore, it is recommended not to zoom in too much on where the Auto tracking is expected to take place.

Event > Event settings

This section explains how to configure the camera to respond to particular situations (events). A typical application is that when a motion is detected, the camera sends buffered images to an FTP server or e-mail address as notifications. Click **Help**, there is an illustration shown in the pop-up window explaining that an event can be triggered by many sources, such as motion detection or external digital input devices. When an event is triggered, you can specify what type of action that will be performed. You can configure the camera to send snapshots or videos to your email address or FTP site.

Event

An event is an action initiated by a user-defined trigger source. In the Event column, click **Add** to open the event settings window.

- Event name—Enter a name for the event setting.
- Enable this event—Select this checkbox to enable the event setting.
- Priority—Select the relative importance of this event (High, Normal, or Low). Events with a higher priority setting will be executed first.
- Detect next motion detection or digital input after *x* seconds—Enter the duration in seconds to pause motion detection after a motion is detected.

Follow the steps 1 through 3 to arrange the three elements—Schedule, Trigger, and Action—to configure an action to take when an event is triggered. You can configure three event-triggered conditions.

1. Schedule

Specify the time span for the event-triggering condition. Please select the days of the week and the time in a day (in 24-hr time format) for the recording schedule.

2. Trigger

This is the cause or stimulus which defines when to trigger the camera. The trigger source can be configured to use the Network Camera's built-in motion detection mechanism or external digital input devices.

There are several choices of trigger sources. Select the item to display the detailed configuration options.

- Video motion detection—This option makes use of the built-in motion detection mechanism as a trigger source. To enable this function, you need to configure a Motion Detection Window first. For more information, see the "Applications > Motion detection" section on page 5-44.
- Periodically—This option allows the camera to trigger periodically for every other defined minute. Up to 999 minutes are allowed.
- Digital input—This option allows the camera to use an external digital input device or sensor as a trigger source. Depending on your application, there are many choices with digital input devices on the market which help detect changes in temperature, vibration, sound, light, and so on.

- System boot—This option triggers the camera when the power to the camera is disconnected and reconnected.
- Recording notify—This option allows the camera to trigger when the recording disk is full or when recording starts to overwrite older data.
- Audio detection—A preset threshold can be configured with an external microphone as the trigger to system event. The triggering condition can be an input exceeding or falling below a threshold. Audio detection can take place as a complement to motion detection or as a method to detect activities not covered by the camera view.

  Once you have a preset audio alarm level, you can define the triggering condition either as an audio input rises above or falls below the alarm level.
- Camera tampering detection—This option triggers an event when tampering with the camera is detected.
- Manual Triggers—An event can be manually triggered by the manual trigger buttons on the main page.
- VADP—It is presumed that you already uploaded and enabled the Cisco APP Package modules before you can associate Cisco APP Package triggers with an Event setting.

  Click on the **Set VADP Trigger** button to open the VADP triggers menu. The triggering conditions available with third-party software modules known as Cisco APP Packages will be listed. Use the arrow buttons to select these triggers. You may implant these modules for different purposes such as triggering motion detection, or applications related to video analysis, etc. See the "Applications > Package management" section on page 5-48 for the configuration options with Cisco App Package modules.

3. Action

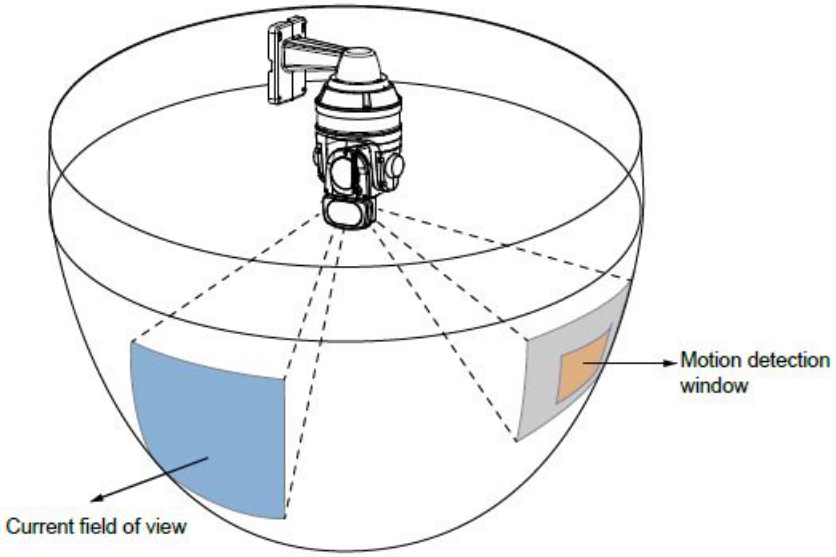
Define the actions to be performed by the camera when a trigger is activated.

Define the actions to be performed by the camera when a trigger is activated.

- Trigger digital output for *x* seconds—Select this option to turn on the external digital output device when a trigger is activated. Specify the length of the trigger interval in the text box.
- SD—Select this option to back up media files on an SD card if the network is disconnected. This function will only be displayed after you set up a network storage (NAS). The media to back up can include snapshot images, video, or system logs depending on your event settings.
- Play audio clip—Select this option to playback an audio file that has been uploaded to the camera flash memory. For more information, see the "Audio clips tab" section on page 5-20.
- Move to preset location—Select a preset location you have configured. Configure Preset locations first. For detailed information, see the "Misc. settings" section on page 5-35. Another checkbox will appear, Capture media after moving to the location. You can select to record associated snapshot, video clip or system event once the event is triggered and the camera moves to the preset location. See Add Media in the following discussion.
- Trigger auto tracking—Auto tracking starts by the occurrence of another trigger.

To set an event with recorded video or snapshots, it is necessary to configure the server and media settings so that the Network Camera will know what action to take (such as which server to send the media files to) when a trigger is activated.

If you configured a motion detection window as a trigger, the motion detection may become invalid when the camera field of view moved away from the detection window. You can let camera return to the motion detection position to detect the coming event by re-configuring your Home position in PTZ > PTZ settings (see the "PTZ > PTZ settings" section on page 5-33) or turn the camera to a preset position.



Add server

Click **Add server** in the Action display to open the server setting window. You can specify where the notification messages are sent to when a trigger is activated. A A total of five server settings can be configured.

There are four choices of server types available: Email, FTP, HTTP, and Network storage. Select the item to display the detailed configuration options. You can configure either one or all of them.

Server type: Email

Select to send the media files via email when a trigger is activated.

- Server name—Enter a name for the server setting.
- Sender email address—Enter the email address of the sender
- Recipient email address—Enter a valid email address as the recipient address.
- Server address—Enter the domain name or IP address of the email server.
- User name—Enter the user name of the email account if necessary.
- Password—Enter the password of the email account if necessary.
- Server port—The default mail server port is set to 25. You can also manually set another port.

If your SMTP server requires a secure connection (SSL), select **This server requires a secure connection (SSL)**.

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

Click **Save server** to enable the settings, then click **Close** to exit the Add server page.

After you configure the first event server, the new event server will automatically display on the Server list. If you wish to add other server options, click **Add server**.

Server type: FTP

Select to send the media files to an FTP server when a trigger is activated.

- Server name—Enter a name for the server setting.
- Server address—Enter 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—Enter the login name of the FTP account.
- Password—Enter the password of the FTP account.
- FTP folder name—Enter the folder where the media files will be placed. If the folder name does not exist, the camera will automatically 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, select this option to enable passive mode FTP and allow data transmission to pass through the firewall.

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

Click **Save server** to enable the settings.

Server type: HTTP

Select to send the media files to an HTTP server when a trigger is activated.

- Server name—Enter a name for the server setting.
- URL—Enter the URL of the HTTP server.
- User name—Enter the user name if necessary.
- Password—Enter the password if necessary.

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

Click **Save server** to enable the settings.

Network storage

Select to send the media files to a networked storage when a trigger is activated. See the "Recording > Recording settings" section on page 49 for details.

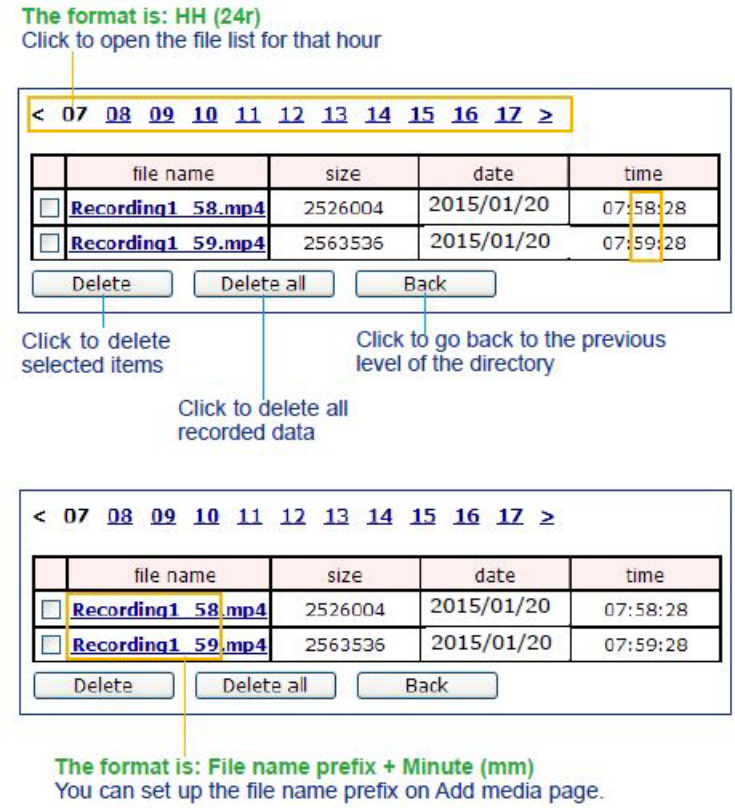
Click **Save server** to enable the settings, then click **Close** to exit the Add server page.

Additional Actions

- SD Test—Click to test your SD card. The system will display a message indicating the result as a success or a failure. If you want to use your SD card for local storage, format it before use.
- View—Click this button to open a file list window. This function is only for SD card and Network Storage. If you click the View button for an SD card, a Local storage page will prompt so that you can manage the recorded files on SD card. For more information about Local storage, see the "Local storage > SD card management" section on page 5-50. If you click the View button for a Network storage, a file directory window will prompt for you to view recorded data on Network storage.
- Create folders by date, time, and hour automatically—If you select this item, the system will automatically create folders by the date when video footages are stored onto the networked storage.

The following is an example of a file destination with video clips:

Click 20150120 to open the directory:



Add media

Click **Add media** in the Action display to open the media setting window. You can specify the type of media that will be sent when a trigger is activated. A total of five media settings can be configured. There are three choices of media types available: Snapshot, Video Clip, and System log. Select the item to display the detailed configuration options. You can configure either one or all of them.

Media type: Snapshot

Select to send snapshots when a trigger is activated.

- Media name—Enter a name for the media setting.

- Source—Select to take snapshots from stream 1 ~ 4. (The following options are available when the check circle is selected
- Send *x* pre-event images—The camera has a buffer area; it temporarily holds data up to a certain limit. Enter a number to decide how many images to capture before a trigger is activated. Up to 7 images can be generated.
- Send *x* post-event images—Enter a number to decide how many images to capture after a trigger is activated. Up to seven images can be generated. For example, if both the Send pre-event images and Send post-event images are set to 7, a total of 15 images can be generated after a trigger is activated.
- File name prefix—Enter the text that will be appended to the front of the file name.
- Add date and time suffix to the file name—Select this option to add a date/time suffix to the file name. The date and time suffix format is YYYYMMDD_HHMMSS.

Click **Save media** to enable the settings, then click **Close** to exit the Add media page.

After you set up the first media server, a new column for media server will automatically display on the Media list. If you wish to add more media options, click **Add media**.

Media type: Video clip

Select to send video clips when a trigger is activated.

- Media name—Enter a name for the media setting.
- Source—Select the source of video clip.
- Pre-event recording—The camera has a buffer area; it temporarily holds data up to a certain limit. Enter a number to decide the duration of recording before a trigger is activated. Up to 9 seconds of video can be recorded.
- Maximum duration—Specify the maximum recording duration in seconds. Up to 20 seconds can be set. For example, if pre-event recording is set to 5 seconds and the maximum duration is set to 10 seconds, the camera 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 will be appended to the front of the file name.

Click **Save media** to enable the settings.

Media type: System log

Select to send a system log when a trigger is activated.

Click **Save media** to enable the settings, then click **Close** to exit the Add Media page.

- View—Click this button to open a file list window. This function only applies of SD card and networked storage are available.

  If you click View button of SD card, a Local storage page will pop up for you to manage recorded files on SD card. For more information about Local storage, see the "Local storage > SD card management" section on page 5-50. If you click View button of Network storage, a file directory window will pop up for you to view recorded data on Network storage.
- Create folders by date, time, and hour automatically—If you select this item, the system will automatically create folders by the date.

When completed the settings with steps 1~3 to arrange Schedule, Trigger, and Action of an event, click **Save event** to enable the settings and click **Close** to exit the page.

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

If you want to stop the event trigger, you can click on the **ON** button to turn it to OFF status or click the **Delete** button to remove the event setting.

To remove a server setting from the list, select a server name and click **Delete**. You can only delete a server setting when the server setting is currently not applied to an event setting.

To remove a media setting from the list, select a media name and click Delete. You can only delete a media setting when the media setting is currently not applied to an event setting.

Customized Script

This function allows you to upload a sample script (.xml file) to the camera, which will save your time on configuring the settings. There are a limited number of customized scripts you can upload; if the current amount of customized scripts has reached the limit, an alert message will prompt.

Click **Add** to upload a file. Click in the script display to modify the script online.

Applications > Motion detection

This section explains how to configure the camera to enable motion detection. A total of five motion detection windows can be configured.

Motion detection setting 1, Normal light mode, is for normal situations. Motion detection setting 2, Profile mode, is for special situations.

To enable motion detection, follow these steps:

Step 1 Click **New** to add a new motion detection window.

Step 2 In the Window Name text box, enter a name for the motion detection window.

Use four mouse clicks to designate a detection window. You can change the window shape by dragging the corner marks to a preferred location.

Drag the item size tab to change the minimum size of item to trigger an alarm. An item size box will appear in the center of screen for your reference (in semi-transparent red). An intruding object must be larger than the Item size to trigger an alarm. Change the item size according to the live view.

To delete a window, click the X mark on the right of the window name.

Step 3 Define the sensitivity to moving objects by moving the Sensitivity slide bar.

A high sensitivity is prone to produce false alarms such as the fast changes of light (such as day/night mode switch, turning lights on/off). A movement must persist longer than 0.3 second for the motion to be detected.

Step 4 **Click** Save to enable the settings.

Step 5 Select **Enable motion detection** to enable this function.

The Percentage Indicator will rise or fall depending on the variation between sequential images. When motions are detected by the camera and are considered to exceed the preset threshold, the red bar rises. Meanwhile, the motion detection window will be outlined in red.

Photos or videos can be captured instantly and configured to be sent to a remote server (via an email or FTP server). For more information about how to configure an event setting, see the "Event > Event settings" section on page 5-38.

A green bar indicates that even though motions have been detected, the event has not been triggered because the image variations still fall under the preset threshold.

If you want to configure other motion detection settings for day/night/schedule mode (for example, for a different lighting condition during a specific period of time), click **Profile** to open the Motion Detection Profile Settings page. Another three motion detection windows can be configured on this page.

To set up a profile, follow these steps:

Step 1 Create a new motion detection window.

Step 2 Click the **Profile mode** tab.

Step 3 Select the applicable Schedule mode. Manually enter a time range.

Step 4 Click **Save** to enable the settings and click **Close** to exit the page.

This motion detection window will also be displayed on the Event Settings page. You can go to **Event > Event settings > Trigger** to select it as a trigger source. Seethe "Event > Event settings" procedure on page 5-38 for detailed information.

How does Motion Detection Work?

There are two motion detection parameters: Sensitivity and Min. Item Size. Sensitivity is a value that expresses the sensitivity to moving objects. A higher sensitivity setting allows camera to detect slight movements while a lower sensitivity setting will neglect them.

The minimum item size is a threshold value that determines how many "alerted pixels" can trigger an event. When the size of an intruding object is larger than the minimum size, and its movement persist for 0.3 second, the motion is judged to exceed the defined threshold; and the motion window will be outlined in red. With a large minimum item size, the size of moving object is considered as smaller than the minimum item size, no motion alarm is triggered. With a smaller minimum item size, the same moving object triggers the alarm.

For applications that require a high level of security management, it is suggested to use higher sensitivity settings. However, a higher sensitivity level can also produce false alarms due to fast light changes when switching between the day and night modes, AE switch, turning the light on or off, and so on.

Applications > DI and DO

- Digital input—Select **High** or **Low** as the Normal status for the digital input. Connect the digital input pin of the camera to an external device to detect the current connection status. You may then configure the Normal status (non-trigger status) as High or Low.
- Digital output—Select **Open** or **Grounded** to define normal status for the digital output. Connect an output line to an external device, the Network Camera will report the current signal status. You may then configure the Normal status (non-trigger status) as High or Low.

Set up the event source as DI on Event > Event settings Add Event > Trigger. See the "Event > Event settings" section on page 5-38 for detailed information.

Applications > Tampering detection

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

To set up the camera tamper detection function, follow these steps:

Step 1 Click to select the check box before tampering conditions: Tampering detection, Image too dark, Image too bright, and Image too blurry, then enter the tamper trigger duration (10 sec. ~ 10 min.). The duration specifies the set of time before the tampering is considered as a real alarm. This helps avoid false alarms by short-lived changes.

The tamper alarm will be triggered only when the tampering factor (the difference between current frame and pre-saved background) exceeds the trigger threshold. Conditions such as image too dark, too bright, or too blurry (defocused) can also be configured as tampering conditions. The Trigger threshold determines how sensitive your is tamper detection setting. Lower the threshold number, easier to trigger.

- Too bright—Shining a flashlight. The average lighting level of the scene is taken into consideration.
- Too dark—Covering the objective or spraying paint.
- Too blurry—Blurry scene can be the result of strong interference on the device, such as EMI interference.

Step 2 You can configure Tampering Detection as a trigger element to the proactive event configurations in Event > Event settings > Trigger.

For example, when the camera is tampered with, the camera can be configured to send the pre- and post-event video clips to a networked storage device. See the "Event > Event settings" section on page 5-38 for detailed information.

Applications > Audio detection

Audio detection, along with video motion detection, is applicable in the following scenarios:

- Detection of activities not covered by camera view, for example, a loud input by gun shots or breaking a door/window
- A usually noisy environment, such as a factory, suddenly becomes quiet due to a breakdown of machines
- A PTZ camera can be directed to turn to a preset point by the occurrence of audio events
- Dark environments where video motion detection may not function well

In the example shown in Figure 5-7, the red circles indicate where the audio alarms can be triggered when breaching or falling below the preset threshold.

Figure 5-7 Audio Detection

To configure audio detection, follow these steps:

Step 1 Once the Audio detection window is opened, the current sound input will be interactively indicated by a fluctuating yellow wave diagram.

Step 2 Use a mouse click to drag the Alarm level tab to a preferred location on the slide bar.

Step 3 Select the **Enable audio detection** check box and click **Save** to enable the feature.

Note

- The volume numbers (0~100) on the side of wave diagram do not represent decibel (dB). Sound intensity level has already been mapped to preset values. You can, however, use the real-world inputs at your installation site that are shown on the wave diagram to configure an alarm level.
- To configure this feature, you must not mute the audio in Configuration > Media > Audio. The default of the camera can be muted due to the lack of an internal microphone. An external microphone is provided by users.

You can use the Profile window to configure a different Audio detection setting. For example, a place can be noisy in the day time and become very quiet in the night. To make this configuration, follow these steps:

Step 1 Click on the **Enable this profile** check box.

Once the Audio detection window is opened, the current sound input will be interactively indicated by a fluctuating yellow wave diagram.

Step 2 Use a mouse click to drag the Alarm level tab to a preferred location on the slide bar.

Step 3 Select the Day, Night, or Schedule mode check circles.

You may also manually configure a period of time during which this profile will take effect.

Step 4 Click **Save** and then click **Close** to complete your configuration.

If the Alarm level and the received volume are set within a range of 20% on the wave diagram, frequent alarms will be triggered. It is recommended to set the Alarm level farther apart from the detected sound level.

To configure and enable this feature, you must not configure video stream #1 into Motion JPEG. If an external microphone input is connected and recording of audio stream is preferred, audio stream is transmitted between camera and viewer/recording station along with stream #1.

See the "Media > Audio" section on page 5-20 for audio settings and the "Media > Video" section on page 5-14 for video streaming settings.

Applications > Package management

You can store and execute Cisco software modules onto the camera's flash memory or SD card. These software modules can apply in video analysis for intelligent video applications such as license plate recognition, object counting, or as an agent for edge recording, and so on.

- Once the software package is successfully uploaded, the module configuration (vadp. xml) information is displayed. When uploading a module, the camera will examine whether the module fits the predefined Cisco APP package requirements. Contact Cisco or the vendor of your third-party module for the parameters contained within.
- You can also run Cisco APP package packages as a means to access updated functionality instead of replacing the entire firmware.
- For some cameras the flash is too small to hold Cisco APP package packages. These cameras will have their Save to SD card check boxes selected and grayed-out for all time.
- The file system of SD card (FAT32) does not support soft (symbolic) link. It will return failure if your module tries to create soft links on SD card.

To utilize a software module, acquire the software package and click **Browse** and **Upload** buttons.

To start a module, select the radio button in front, and click the **Start** button.

If you need to remove a module, select the radio button in front and then click the **Stop** button. By then the module status will become OFF, and the X button will appear at the end of the row. Click on the **X** button to remove an existing module.

To set a time that a module starts and stops each day, click the **Schedule** button, and then use the From and To fields that appear to set the times.

When prompted by a confirm message, click **Yes** to proceed.

That the actual memory consumed while operating the module will be indicated on the Memory status field. This helps determine whether a running module has consumed too much of system resources.

Recording > Recording settings

This section explains how to configure the recording settings for the camera.

Recording Settings

Insert your SD card and click **SD test** to test

Note to format your SD card when using it for the first time. See the "Local storage > SD card management" section on page 5-50 for detailed information.

Click **Add** to open the recording setting window. On this page, you can define the adaptive recording, recording source, recording schedule, and recording capacity. A total of two recording settings can be configured.

- Recording name—Enter a name for the recording setting.
- Enable this recording—Select this option to enable video recording.
- With adaptive recording—Selecting this option will activate the frame rate control according to alarm trigger. The frame control means that when there is a triggered alarm, the frame rate will raise to the value you configured on the Stream setting page. See the "Media > Video" section on page 5-14 for more information.

  If you enable adaptive recording on Camera A, only when an event is triggered on Camera A will the server record video streams in the full frame rate; otherwise, it will only request the I frame data during normal monitoring, thus effectively saves bandwidths and storage space.

Note To enable adaptive recording, make sure you have set up the trigger source such as Motion Detection, DI Device, or Manual Trigger.

When there is no alarm trigger:
- JPEG mode: record 1 frame per second
- H.265 or H.264 mode: record the I frame only

When the I frame period is >1s on Video settings page, firmware will force decrease the I frame period to 1s when adaptive recording is enabled.

  The alarm trigger includes motion detection and DI detection. See the "Event > Event settings" section on page 5-38.

- Pre-event recording and post-event recording—Available when you enable **With adaptive recording**. The camera has a buffer that temporarily holds data up to a certain limit. Enter a number to define the duration of recording before and after a trigger is activated.
- Priority—Select the relative importance of this recording (High, Normal, or Low). Recording with a higher priority setting will be executed first.
- Source—Select a stream as the recording source.

To enable recording notification configure Event settings first. See the "Event > Event settings" section on page 5-38.

Follow these steps to set up recording:

1. Trigger: Select a trigger source.
   - Schedule—The server will start to record files on the local storage or network storage (NAS).
   - Network fail—Since network fail, the server will start to record files on the local storage (SD card).
2. Destination: You can select the SD card or network storage (NAS) for the recorded video files.

NAS server

1. Click **Add NAS** server to open the server setting window.
2. Fill in the information for your server.
   - In the Server name field, enter the name of the NAS server.
   - In the Network storage location field, enter the network storage path in the format *server_name* or *IP_address**folder_name*
   - In the Workgroup field, enter the workgroup of the NAS server.
   - In the Username and password field, enter information for your server
3. Click **Test** to check the setting. The result will be shown in a pop-up window. If successful, you will receive a test.txt file on the network storage server.
4. Enter a server name.
5. Click **Save Server** to complete the settings and click **Close** to exit the page.

- Capacity—You can select either the entire storage space available or specify a reserved space. The recording size limit must be larger than the reserved space for cyclic recording. The reserved space is used during cyclic recording to prevent malfunctions that might occur during the transaction stage when the video feeds are about to fill up the storage space, and new data is still coming. This value must be larger than 15 MB.
- Enable cyclic recording—If you check this item, when the maximum capacity is reached, the oldest file will be overwritten by the latest ones.
- File name prefix—Enter the text that will be appended to the front of the file name.

If you want to enable recording notification, click Event to set up. See the "Event > Event settings" section on page 5-38 for more details.

When completed, select Enable this recording. Click **Save** to enable the setting and click **Close** to exit this page. When the system begins recording, it will send the recorded files to the network storage or SD card. The new recording name will appear on the recording page.

To remove an existing recording setting from the list, single-click to select it and click **Delete**.

- Video (Name)—Click to open the Recording Settings page to modify.
- ON (Status)—Click to manually adjust the Status. (ON: start recording; OFF: stop recording.)
- NAS or SD (Destination): Click to open the file list of recordings. For more information about folder naming rules, see the "Add media" section on page 5-42.

Local storage > SD card management

This section explains how to manage the local storage on the Network Camera. Here you can view SD card status, and implement SD card control.

Note

- It is recommended to turn OFF the recording activity before you remove an SD card from the camera.
- The lifespan of an SD card is limited. Regular replacement of the SD card can be necessary.
- Camera file system takes up several megabytes of memory space. The storage space cannot be used for recording.
- An SD card that already contains data recorded by another device should not be used in this camera.
- Do not modify or change the folder names in the SD card. That may result in camera malfunctions.

SD card status

This column shows the status, file system, size, and usage information for your SD card. Remember to format the SD card when using for the first time. If the SD card status field shows “Detached,” there is no SD card.

SD card format

The Linux kernel EXT4 file system format applies to SD card larger than 32GB. However, if EXT4 is applied, computers running Windows will not be able to access the contents on the SD card unless using some third-party software.

SD card control

- Enable cyclic storage—Check this item if you want to enable cyclic recording. When the maximum capacity is reached, the oldest file will be overwritten by the latest one.
- Enable automatic disk cleanup—Check this item and enter the number of days you wish to retain a file. For example, if you enter “7 days,” the recorded files will be stored on the SD card for 7 days.

Click **Save** to enable your settings.

Local storage > Content management

This section explains how to manage the content of recorded videos on the camera. Here you can search and view the records and view the searched results.

Searching and Viewing the Records

To set up search criteria for recorded data, use the following options. If you do not select any criteria and click **Search** button, all recorded data will be listed in the Search results area.

- Trigger types—Select one or more trigger types.
- Media type—Select the media type (Video clip, Snapshot, or text).

- Time—Use the options to search the last *x* minutes, hours, day, or weeks, to search designated from and to dated and times.

Click **Search** and the recorded data corresponding to the search criteria will be listed in Search results area.

Search Results

The Search results window includes four columns: Name, Trigger time, Starting Time, and Ending time.

From the drop-down list at the bottom left, choose the number of entries to be displayed on one page.

You can sort the search results by any column by clicking the column title. Click as needed choose ascending or descending order.

- Play—Click on a search result, which will highlight the selected item. A Play window will appear on top for immediate review of the selected file.
- Download—Click on a search result to highlight the selected item in purple. Then click the Download button and a file download window will pop up for you to save the file.
- Lock/Unlock—Select the check box in front of a desired search result, then click this button. The selected items will become Locked, which will not be deleted during cyclic recording. You can click again to unlock the selections.
- JPEGs to AVI—This functions only applies to JPEG format files such as snapshots. You can select several snapshots from the list, then click this button. Those snapshots will be converted into an AVI file.
- Remove—Select the desired search results, then click this button to delete the files.