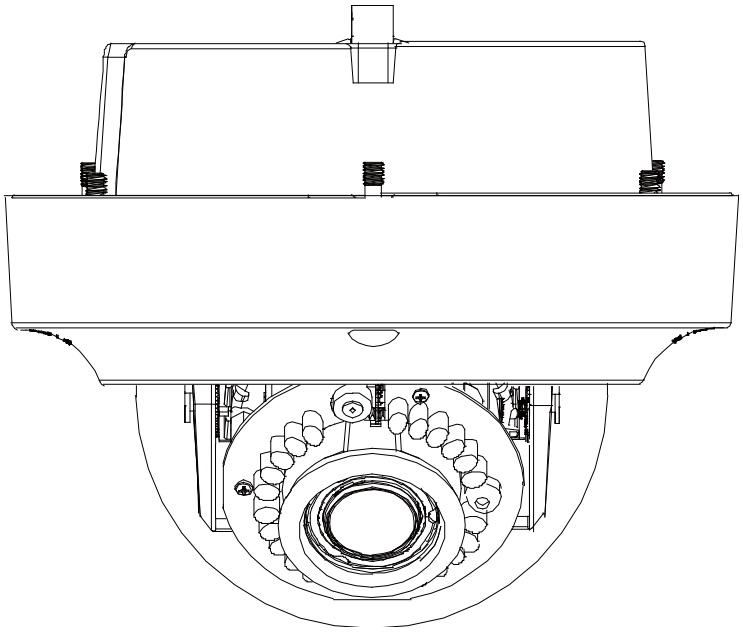
PELCO

by Schneider Electric

Sarix® IMP Series Environmental Mini Dome with IR

User Manual



C3957M-EN (10/13)

Contents

Important Notices

REGULATORY NOTICES

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

RADIO AND TELEVISION INTERFERENCE

This equipment has been tested and found to comply with the limits of a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Changes and Modifications not expressly approved by the manufacturer or registrant of this equipment can void your authority to operate this equipment under Federal Communications Commission’s rules.

In order to maintain compliance with FCC regulations shielded cables must be used with this equipment. Operation with non-approved equipment or unshielded cables is likely to result in interference to radio and television reception.

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

LEGAL NOTICE

SOME PELCO EQUIPMENT CONTAINS, AND THE SOFTWARE ENABLES, AUDIO/VISUAL AND RECORDING CAPABILITIES, THE IMPROPER USE OF WHICH MAY SUBJECT YOU TO CIVIL AND CRIMINAL PENALTIES. APPLICABLE LAWS REGARDING THE USE OF SUCH CAPABILITIES VARY BETWEEN JURISDICTIONS AND MAY REQUIRE, AMONG OTHER THINGS, EXPRESS WRITTEN CONSENT FROM RECORDED SUBJECTS. YOU ARE SOLELY RESPONSIBLE FOR INSURING STRICT COMPLIANCE WITH SUCH LAWS AND FOR STRICT ADHERENCE TO ANY/ALL RIGHTS OF PRIVACY AND PERSONALTY. USE OF THIS EQUIPMENT AND/OR SOFTWARE FOR ILLEGAL SURVEILLANCE OR MONITORING SHALL BE DEEMED UNAUTHORIZED USE IN VIOLATION OF THE END USER SOFTWARE AGREEMENT AND RESULT IN THE IMMEDIATE TERMINATION OF YOUR LICENSE RIGHTS THEREUNDER.

VIDEO QUALITY CAUTION

FRAME RATE NOTICE REGARDING USER SELECTED OPTIONS

Pelco systems are capable of providing high quality video for both live viewing and playback. However, the systems can be used in lower quality modes, which can degrade picture quality, to allow for a slower rate of data transfer and to reduce the amount of video data stored. The picture quality can be degraded by either lowering the resolution, reducing the picture rate, or both. A picture degraded by having a reduced resolution may result in an image that is less clear or even indiscernible. A picture degraded by reducing the picture rate has fewer frames per second, which can result in images that appear to jump or move more quickly than normal during playback. Lower frame rates may result in a key event not being recorded by the system.

Judgment as to the suitability of the products for users' purposes is solely the users' responsibility. Users shall determine the suitability of the products for their own intended application, picture rate and picture quality. In the event users intend to use the video for evidentiary purposes in a judicial proceeding or otherwise, users should consult with their attorney regarding any particular requirements for such use.

OPEN SOURCE SOFTWARE

This product includes certain open source or other software originated from third parties that is subject to the GNU General Public License (GPL), GNU Library/Lesser General Public License (LGPL) and different and/or additional copyright licenses, disclaimers, and notices.

The exact terms of GPL, LGPL, and some other licenses are provided to you with this product. Please refer to the exact terms of the GPL and LGPL at http://www.fsf.org (Free Software Foundation) or http://www.opensource.org (Open Source Initiative) regarding your rights under said license. You may obtain a complete corresponding machine-readable copy of the source code of such software under the GPL or LGPL by sending your request to digitalsupport@pelco.com; the subject line should read Source Code Request. You will then receive an email with a link for you to download the source code.

This offer is valid for a period of three (3) years from the date of the distribution of this product by Pelco.

CCC POWER CORD STATEMENT

Models shipped to China do not include power cords.

NOTE: A CCC approved power cord must be used to power the equipment when used in China.

KCC CERTIFICATION

Korean Class A EMC

이 기기는 업무용 (A 급) 전자파 적합기기로서 판매자 또는 사용자는
이 점을 주의하시길 바라며 , 가정 외의 지역에서 사용하는 것을 목적
으로 합니다 .

Korean Class B EMC

이 기기는 가정용 (B 급) 전자파 적합기기 로서 주로 가정에서 사용하는
것을 목적으로 하며 , 모든 지역에서 사용할 수 있습니다 .

ESD WARNING

WARNING: This product is sensitive to Electrostatic Discharge (ESD). To avoid ESD damage to this product, use ESD safe practices during installation. Before touching, adjusting or handling this product, correctly attach an ESD wrist strap to your wrist and appropriately discharge your body and tools. For more information about ESD control and safe handling practices of electronics, please refer to ANSI/ESD S20.20-1999 or contact the Electrostatic Discharge Association (www.esda.org).

Network Topology Statement

IMPORTANT NOTE. PLEASE READ. The network implementation is shown as a general representation only and is not intended to show a detailed network topology. Your actual network will differ, requiring changes or perhaps additional network equipment to accommodate the system as illustrated. Please contact your local Pelco Representative to discuss your specific requirements.

Legal Notice (Audio Notice)

NOTE: Improper use of audio/visual recording equipment may subject you to civil and criminal penalties. Applicable laws regarding the use of such capabilities vary between jurisdictions and may require, among other things, express written consent from the recorded subjects. You are solely responsible for insuring strict compliance with such laws and for strict adherence to any/all right of privacy and personality.

WARRANTY STATEMENT

For information about Pelco's product warranty and thereto related information, refer to *www.pelco.com/warranty.*

Preface

This user manual is to be used as a reference for the installation and manipulation of the camera unit including features, functions, and a detailed explanation of the menu tree.

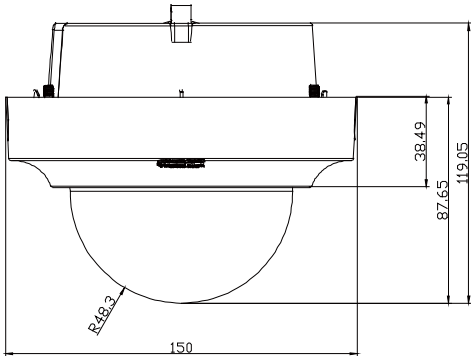
This manual provides the reader with the following information:.

- **Product Overview:** the main functions and system requirements of the unit
- **Installation and Connection:** instructions on unit installation and wire connections
- **Administration and Configuration:** the main menu navigation and controls explanations

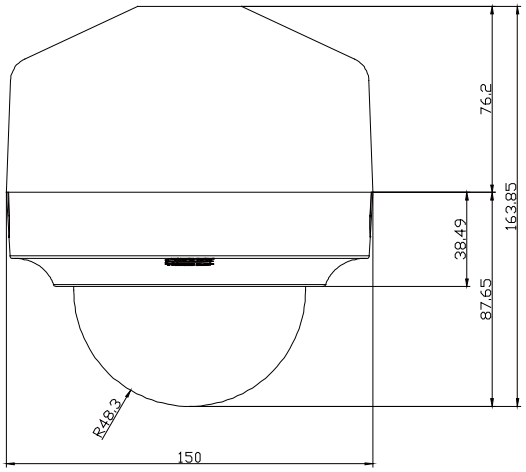
1. Product Overview

1.1 Dimensions

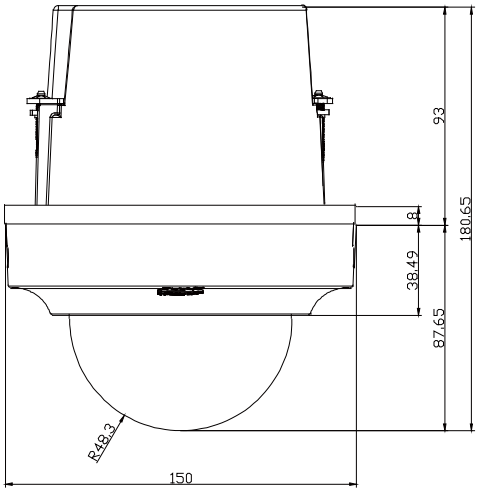
The Sarix Series network IR dome camera has three installation methods (refer to ***2.3.4 Installing the Camera*** on page 14). Figure 1-1 depicts the dimensions of the environmental mini dome with IR, as well as the dimensions of three backbox configurations (pendant mount, ceiling mount, surface mount).



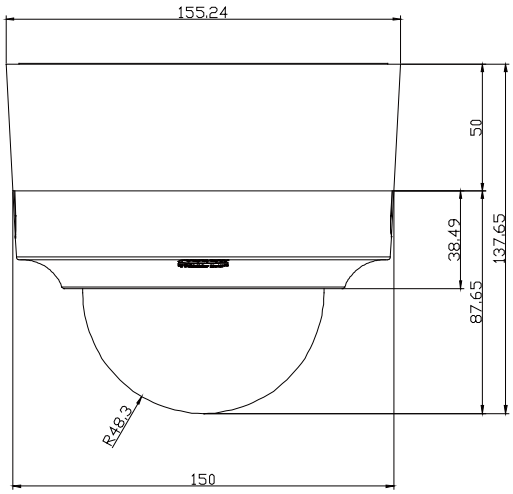
ENVIRONMENTAL IR DOME



ENVIRONMENTAL IR DOME IN ENVIRONMENTAL PENDANT MOUNT



ENVIRONMENTAL IR DOME IN ENVIRONMENTAL CEILING MOUNT



ENVIRONMENTAL IR DOME IN ENVIRONMENTAL SURFACE MOUNT

FIGURE 1-1: PHYSICAL DIMENSIONS

1.2 Physical Characteristics

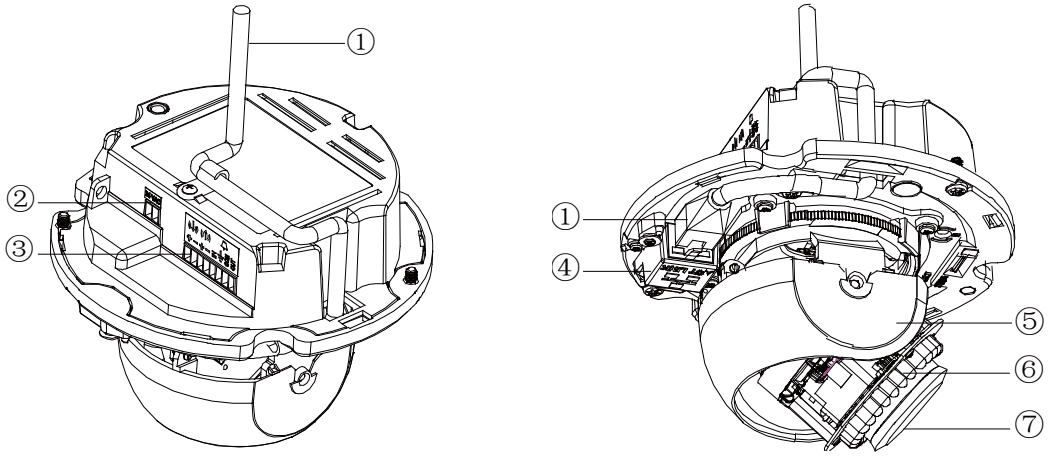


FIGURE 1-2: CAMERA CONNECTIONS AND FEATURES 1/2

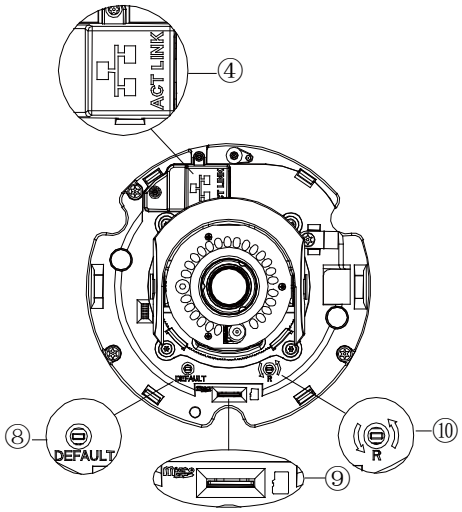


FIGURE 1-3: CAMERA CONNECTIONS AND FEATURES 2/2

1. **Network Cable:** Connect the network cable, pass the cable through the cable hole and fix it to the cable slot as the figure shows.
2. **24 VAC Power:** Supports 24 VAC as the power source.
3. **Audio In**, **Alarm In/ Out**
   - **Audio In:** Connect to device that responds to audio signals.
   - **Alarm In/ Out:** Connect to device that responds to alarm signals.
4. **RJ-45 Network Port:** Connects the camera to the IP network. Also supplies power to the camera through the network using PoE. If PoE is not available, the camera is prewired for 24 VAC.
5. **Dome Liner**
6. **IR Leds**
7. **Lens**
8. **Default:** Using a small tool, such as a paper clip, hold down the reset button longer than 5 seconds to reset the camera to factory defaults.
9. **Micro-SD Card:** To record images when events happen.
10. **Reset:** Using a small tool, such as a paper clip, press the reset button briefly and release to restart the camera.

2. Installation and Connection

2.1 Unpacking Everything

Check that all items in the packing box against the order form and the packing slip. In addition to this manual, the items below are included in the packing box:

- One Mini Environmental IR Dome Camera
- One CD containing the DU2.2, User Manual, Specifications
- One printed Quick Installation Guide
- One Terminal header 2P
- One Terminal header 8P
- One Wrench pin torx

Please contact your dealer if any items are missing.

2.2 Optional Accessories

- IMPBB-ES: a Sarix Environmental Surface Mount for Mini IR Dome White
- IMPBB-EP: a Sarix Environmental Pendant Mount for Mini IR Dome White
- IMPBB-EI: a Sarix Environmental In-Ceiling Mount for Mini IR Dome

2.3 Installation

Following tools might help you complete the installation:

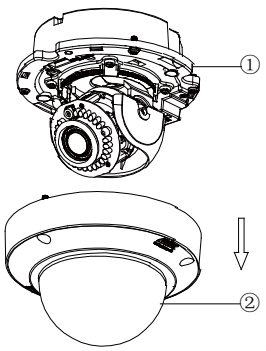
- a drill
- screwdrivers
- wire cutters

2.3.1 Checking Appearance

Although the protective materials used for the packaging should be able to protect the unit from most accidents during transportation, check the unit and its accessories for any visible damage. Remove the protective film to check items in accordance with the list in **2.1 Unpacking Everything**.

2.3.2 Disassembling the Camera

Before you mount and adjust the camera, push and remove the dome cover (#2) with caution.



① Camera Body
② Dome Cover

FIGURE 2-1: DISASSEMBLING THE CAMERA

2.3.3 Connecting the Wires

This unit supports one of the following options as power supply.

- **24 VAC:** Connect 24V (~) cables to terminals ~24 VAC
- **PoE:** Connect the RJ-45 network connector to a PoE compatible network device that has supplied power through the Ethernet cable.
- **(Optional)** Insert audio cable and alarm cable to the unit, and connect the network cable to the RJ-45 network port of a switch. Refer to **Network Cable** in ***1.2 Physical Characteristics*** on page 13 to manage the cables.
  NOTE: To avoid the length deficiency, it's proposed to reserve about 10mm length of the network cable for connecting the cable to the RJ-45 network port before fix the cable to the cable slot.

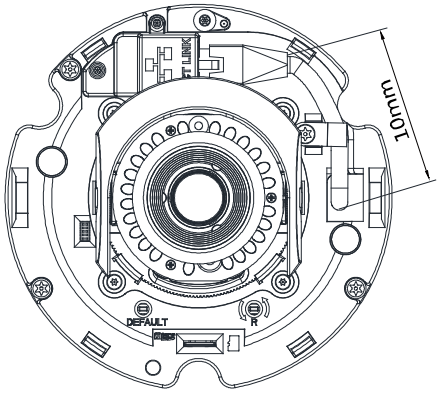


FIGURE 2-2: CONNECTING THE NETWORK CABLE

2.3.4 Installing the Camera

You can install the Sarix Series IR dome camera using one of the following installation methods:

- **Surface Mount** (refer to ***2.3.4.1 Surface Installation***).
- **Pendant Mount** (refer to ***2.3.4.2 Pendant Installation***).
- **In-Ceiling Mount** (refer to ***2.3.4.3 In-Ceiling Installation***).

2.3.4.1 Surface Installation

The **Surface Installation** is mounting the camera to the wall with **IMPBB-ES**, a **Sarix Environmental Surface Mount** for Mini Environmental IR Dome White.

1. Pass all cables through the back box cable hole and attach the camera body (#2) to the back box (#1).
2. Attach the guide pattern which is used for surface mount to the wall or ceiling.

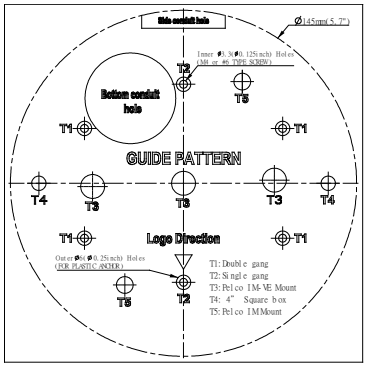


FIGURE 2-3: ATTACHING THE GUIDE PATTERN

3. According to the guide pattern (#1), drill a bottom conduit hole or side conduit hole and pull the wires through the hole**.**

4. Attach the mount plate (#2) of surface mount back plate to the mounting surface with proper screws.
5. Secure the back box (#3) to the mounting surface with three captive screws.
6. Position the camera as needed (refer to ***2.3.5 Positioning the Camera***).
7. Focus the lens (refer to ***2.3.6 Adjusting the Focus***).
8. Install the dome cover (#5) and complete the installation.

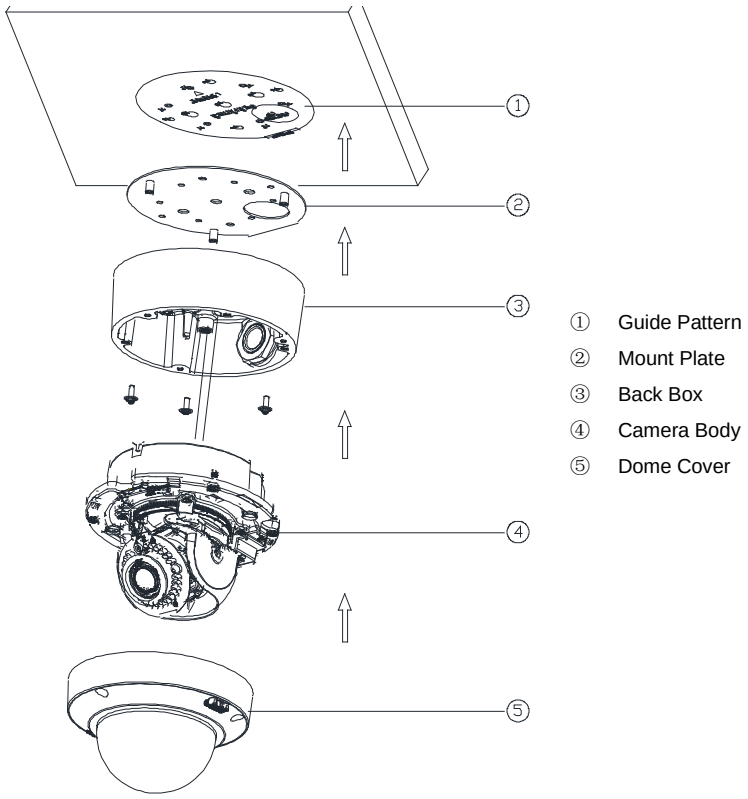


FIGURE 2-4: SURFACE INSTALLATION

2.3.4.2 Pendant Installation

The **Pendant Installation** involves mounting the camera to the wall with **IMPBB-EP Sarix Environmental Pendant Mount** for Mini Environmental IR Dome White. To attach the camera into the back box, it must be installed with a rain-tight compression connector and a lock nut as shown in Figure 2-5 are both provided.

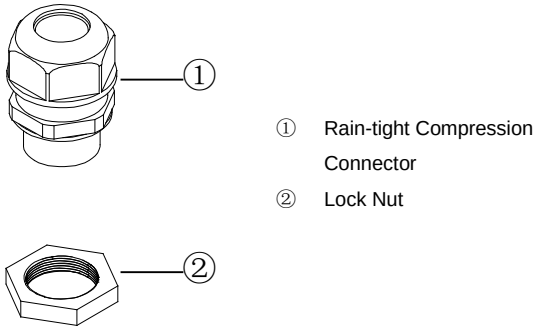


FIGURE 2-5: RAIN-TIGHT& LOCK NUT

Refer to **Figure 2-6** for pendant installation.

1. Pass all cables through the pendant pipe cable hole. Use mounting screws appropriate to your installation.
2. Screw the rain-tight compression connector onto the pipe until tight. Slide the back box (#1) onto the pipe until it rests on the underside of the rain-tight compression connector.
3. Screw the lock nut onto the pipe protruding from beneath the back box. Tighten until the back box is held firmly in place.
4. Mount the camera body (#2) to the back box (#1).
5. Use screws to attach the back box to the mounting surface.
6. Position the camera as needed (refer to ***2.3.5 Positioning the Camera***).
7. Focus the lens (refer to ***2.3.6 Adjusting the Focus***).
8. Install the dome cover (#3) and complete the installation.

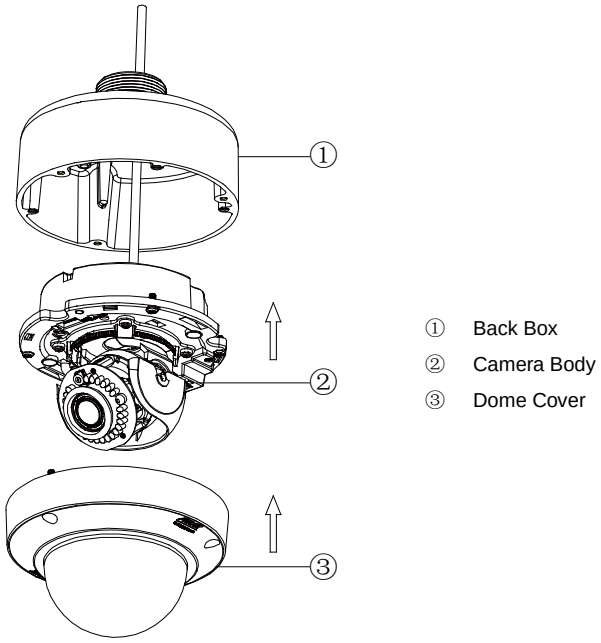


FIGURE 2-6: PENDANT INSTALLATION

2.3.4.3 In-Ceiling Installation

The **In-Ceiling Installation** involves mounting the camera into the ceiling with **IMPBB-EI Sarix Environmental In-Ceiling Mount** for Mini Environmental IR Dome.

1. Attach the guide pattern which is used for in-ceiling mount to the wall or ceiling.

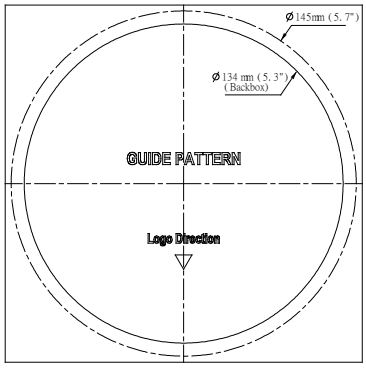


FIGURE 2-7: ATTACHING THE GUIDE PATTERN

2. According the guide pattern, cut a hole in the ceiling/wall.
3. Insert the back box into the hole and screw the two screws with a screwdriver so the antidropping claspers can slide out to chuck the back box into the ceiling (refer to *Figure2-8 & Figure2-9*).

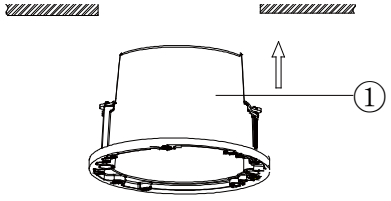


FIGURE 2-8: INSERTING THE BACK BOX

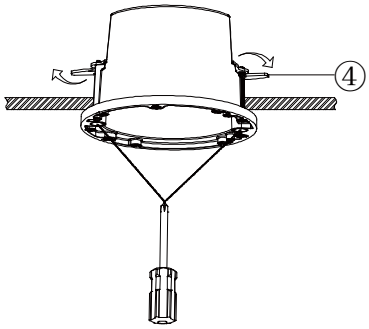


FIGURE 2-9: CHUCKING THE BACK BOX

4. Pass all cables through the back box cable hole and attach the camera body (#2) to the back box (#1).
5. Position the camera as needed (refer to ***2.3.5 Positioning the Camera***).
6. Focus the lens (refer to ***2.3.6 Adjusting the Focus***).
7. Install the dome cover (#3) and complete the installation.

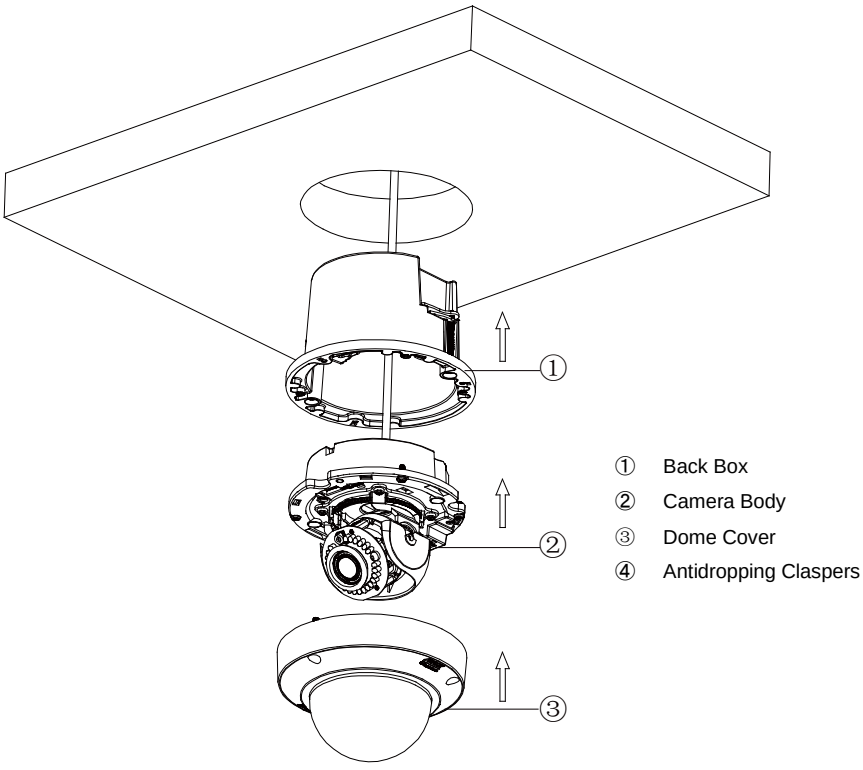
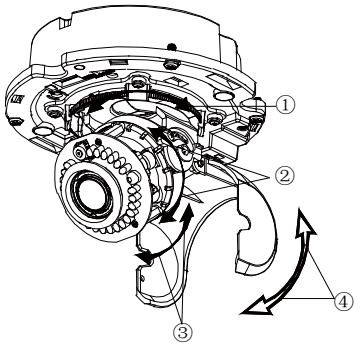


FIGURE 2-10: IN-CEILING INSTALLATION

2.3.5 Positioning the Camera

1. Retract the dome liner.
2. View the camera image using the browser (refer to ***2.4 Connection*** on page 20).
3. Use a small Phillips-head screwdriver to loose the screw (#5) for tilt adjustment.
4. Manually rotate and tilt the camera module to position the camera. Do not over-rotate the module.
   WARNING: Excessively turning the module in one direction could result in damage to the wiring.



① Pan = 355°
② Rotate = 360°
③ Tilt = 90°
④ Dome liner =90°

FIGURE 2-11: POSITIONING THE CAMERA

2.3.6 Adjusting the Focus

1. View the camera image using the browser (refer to ***2.4 Connection*** on page 20).
2. Use the settings in the Web interface (refer to ***3.2.3.3 Focus*** on page 37) to adjust the zoom and focus of the lens to the desired field of view.
3. Also the focus can be adjusted by moving the zoom slider and using the Focus options in the live webpage.
   NOTE: Focus adjustment is done exclusively with Web UI.

2.3.7 Network Topology

The camera can deliver video images and audio in real time using the Internet and Intranet. It's equipped with Ethernet RJ-45 network interface.

FIGURE 2-12: NETWORK TOPOLOGY TYPE Ⅰ

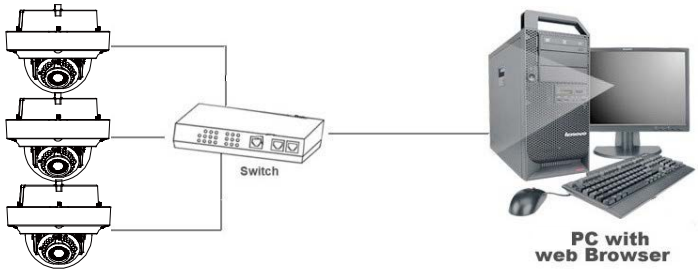


FIGURE 2-13: NETWORK TOPOLOGY TYPE Ⅱ

2.3.8 System Requirements

Below table lists the minimum requirement to implement and operate a unit. Network and processor bandwidth limitations might cause the video stream to pause or appear pixilated when additional Web-interface users connect to the camera. Decrease the images per second (ips), resolution, compression, or bit rate settings of the Web interface video streams to compensate for network/processor limitations.

TABLE 2-1: SYSTEM REQUIREMENTS

System Hardware	
CPU	Intel® Pentium® 4 microprocessor, 2.4GHz or equivalent
RAM	1 GB or above
Monitor	Minimum of 1024 x 768 resolution, 16- or 32-bit pixel color resolution
System Software	
Operating System	Microsoft Windows XP, Vista 32 and 64 bit, Win7 32 and 64 bit
Browser	Microsoft IE 8.0 and later
Media Player	Pelco Media Player or QuickTime® 7.6.5 for Windows XP, Windows Vista, and Windows 7; or QuickTime 7.6.4 for Mac OS X 10.4 (or later)
Unit	
Power Supply	AC 24V / PoE

Note

1. All the installation and operations should comply with your local electricity safety rules.
2. Pelco Media Player is recommended for control, smoothness, and reduced latency as compared to QuickTime. The PMP is downloadable from Pelco web site: www.pelco.com/mediaplayer.
3. This product is not compatible with QuickTime version 7.6.4 for Windows XP or Windows Vista. If you have this version installed on your PC, you will need to upgrade to QuickTime version 7.6.5.
4. Network and processor bandwidth limitations might cause the video stream to pause or appear pixelated when additional Web-interface users connect to the camera. Decrease the images per second (ips), resolution, compression, or bit rate settings of the Web interface video streams to compensate for network or processor limitations.

Caution To avoid damage to the unit, never connect more than one type of power supply (PoE IEEE802.3 Ethernet Class 3 or AC 24V power plug) at the same time.

2.4 Connection

2.4.1 Default IP address

The unit's default IP address is **192.168.0.20** and sub mask is **255.255.255.0**. When setting default IP address of 192.168.0.20 the camera will check to see if that address is already in use and will bump the last octet of the address by 1 if it is. The bump last octet of IP Address by 1 will continue until an unused IP address is found.

However, if you have a DHCP server in your network, the unit would obtain an IP address automatically from the DHCP server so that you don't need to change the camera's IP address. The factory default is DHCP **On** and 192.168.0.20 assignment only occurs when camera is set for DHCP but a DHCP server does not respond to request for an IP address.

2.4.2 Connecting from a computer & Viewing Preparation

2.4.2.1 Using Pelco Device Utility 2.2 Software to Get Camera's IP Address

Pelco Device Utility 2.2 software is a utility program that helps users to manage and configure the camera. Use the utility to find the IP address since the default option is to obtain an IP address via DHCP and therefore the IP address will NOT be known. Steps to get the utility program running are listed below.

1. According the installation instructions to finish installing the Device Utility 2.2 to the computer.
2. Log in to the Device Utility by entering the camera's User name and Password. In the window, enter the default user name: **admin** and password: **admin**, then click **Enter DU2** button to log in.
3. In the Manage Devices page, you can click Refresh Device List or Add New Device to search for the devices.
4. From the Device List, you can get series information about camera, IP Address included.

For more information about using DU2, click this green icon "  " on the upper-right corner of the Device Utility 2 page to get the **Device_ Utility_ 2_Help**.

2.4.2.2 Connecting from a computer

1. Check whether if the networking available between the unit and the computer by executing ping the default IP address. Start a command prompt (Windows: from the Start Menu, select Program. Select Accessories and choose Command Prompt.), and type "Ping 192.168.0.20". If the message "Reply from…" appears, it means the connection is available.
2. Start Internet Explorer and enter IP address: **192.168.0.20**. A login window should pop up. In the window, enter the default user name: **admin** and password: **admin** to log in.

NOTE: If you do not know the camera's IP address, you can locate it using the Pelco Device Utility 2.2 software (refer to **2.4.2.1 Using Pelco Device Utility 2.2 Software to Get Camera's IP Address** on page 20).

Further administration on the unit can be found in "3. Administration and Configuration".

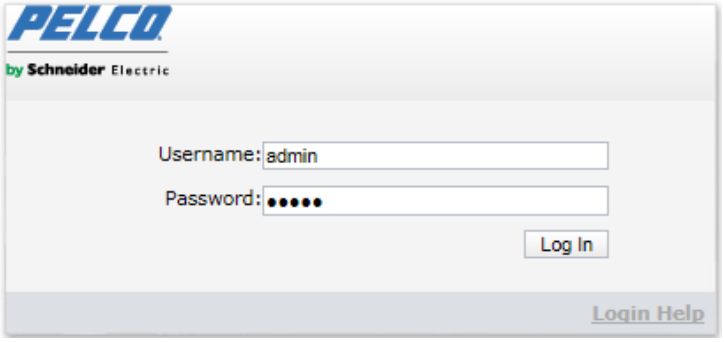


FIGURE 2-14: LOGIN WINDOW

2.4.2.3 Viewing Preparation

Images of the unit can be viewed through Microsoft Internet Explorer 8 or later. Before viewing, follow these steps to enable the display.

1. Enable Cookies On the **Privacy** tab, move the settings slider to **Low** or **Accept All Cookies**.
2. Change Security in **Internet options** and click **Custom Level** to open the **Security Settings** – **Internet Zone** screen.
   NOTE: If the camera operates inside of the intranet, click the **Intranet** icon. If the camera operates outside of the intranet, click the **Internet** icon.
3. Scroll down to the ActiveX controls and plug-ins radio buttons and set as follows:
   - 【Download signed ActiveX controls】➔ Prompt (recommended)
   - 【Download unsigned ActiveX controls】➔ Prompt
   - 【Automatic prompting for ActiveX controls】➔ Enable
   - 【Run ActiveX controls and plug-ins】➔ Enable
   - 【Script ActiveX controls marked safe for scripting*】➔ Enable
4. Press **OK** to save the settings.
5. Close all Microsoft Internet Explorer Windows and restart a new window. This will allow the new settings taking effect.
6. Type your setting IP address into the browser.
7. Then you should be able to see the camera image screen.

3. Administration and Configuration

3.1 Live

Simply click on **Live** on the top right side of the browser window while accessing the IP address of the unit, and a live video is displayed directly in the browser window. When clicked on **Settings**, a window will pop up for configuring "**System**", "**Network**", "**Imaging**", "**A/V Streams**", "**Users**", and "**Events**". Please refer to ***3.2 Settings*** on page 23 for more information. The current logged in identity shows to the right of the **Help**. Click on **Logout admin** of the administration window and configuration will return to the camera image screen.

* Figures of **3. Administration and Configuration** are taken from the 3MP model for web interface introduction purposes. Options within each item may differ slightly among series products and the differences will be marked in a **NOTE**.

Followings are explanations to the tabs on the **Live** window.

Select Stream: Selects the viewable video stream that is displayed in live view (primary or secondary) and selects unicast or multicast settings.

Maximize Viewing Area: Scales the image to the full size of the browser. To resize the video pane to normal view, click the Show Toolbar button in the upper-right corner of the window.

Open Stream in New Window: Opens the video in a scalable, independent window. Opening the video in a separate window allows you to view the video while other applications are running. This window can be minimized, maximized, or closed using the title bar buttons of the active window. The window can also be resized to your specifications by dragging the lower-right corner of the window.

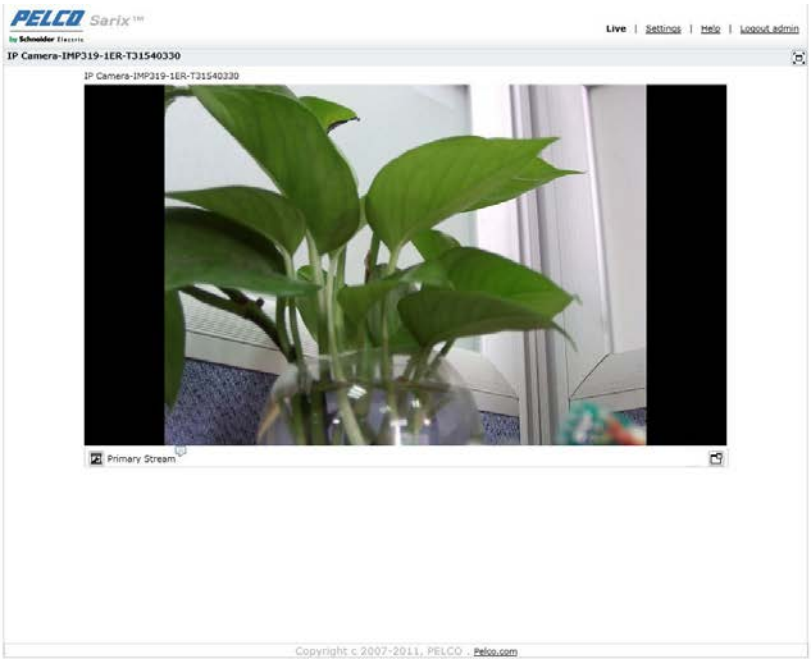


FIGURE 3-1: LIVE VIEW

3.2 Settings

Click on **Settings**, a window will pop up for configuring "**System**", "**Network**", "**Imaging**", "**A/V Streams**", "**Users**", and "**Events**".

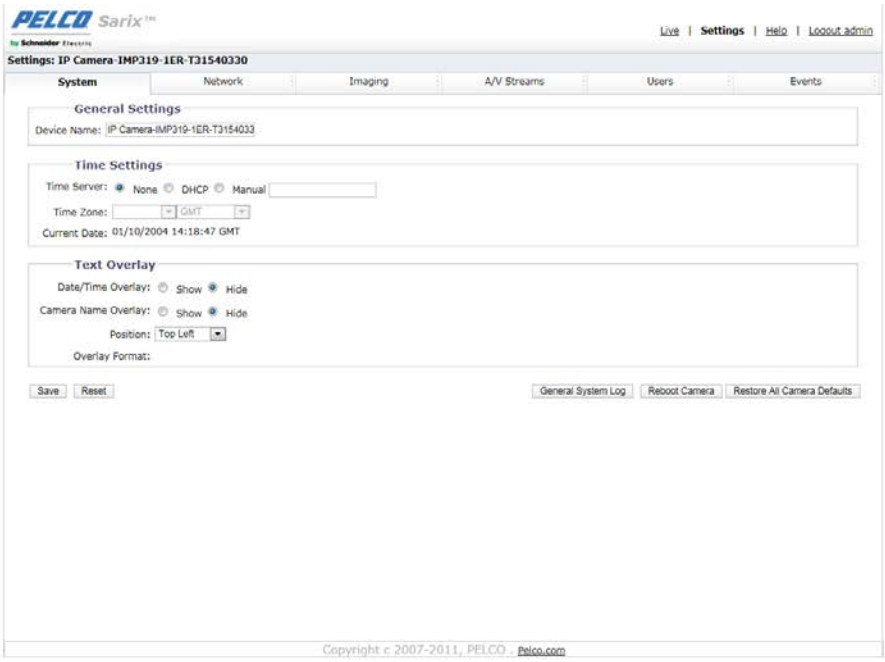


FIGURE 3-2: SETTINGS

3.2.1 System

Use the System tab to change the device name, configure the time settings, set up the text overlay for the live view, get backup, display system information and update firmware version. You can also use the System tab to generate a system log, reboot the camera, or to restore the camera's factory default settings.

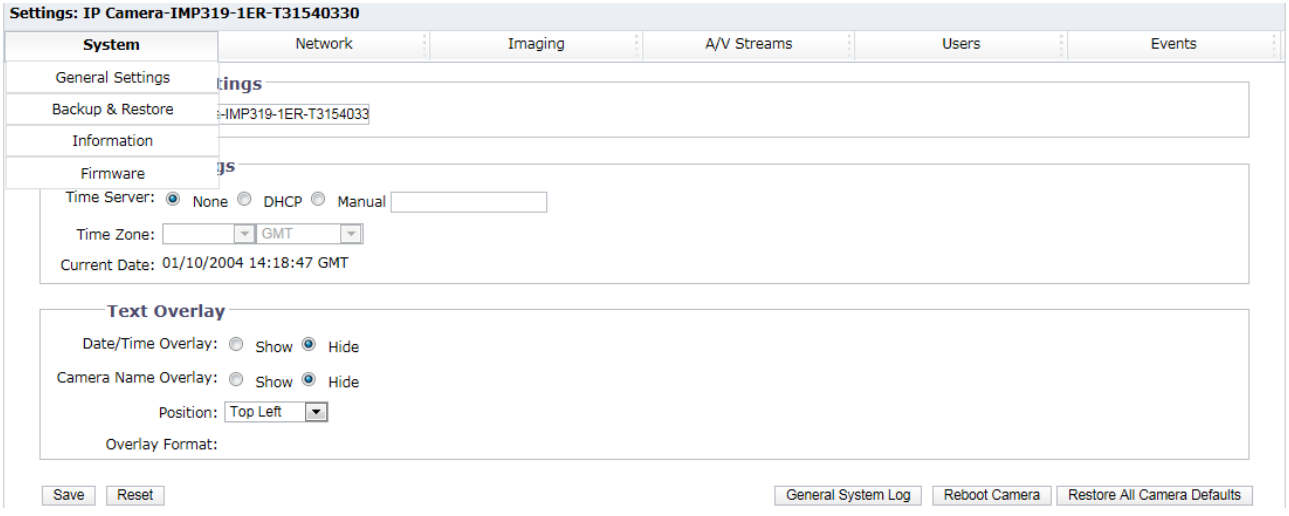


FIGURE 3-3: SYSTEM SETTINGS

General System Log

1. Click the System tab.
2. Click the General System Log button to create a system log that can be used by Pelco Product Support for troubleshooting.

Contact Pelco Product Support at 1-800-289-9100 (USA and Canada) or +1-559-292-1981 (international).

Reboot Camera

1. Click the System tab.
2. Click the Reboot Camera button to restart the camera. Rebooting the camera does not change the configured camera settings.

Restore All Camera Defaults

This process cannot be undone; all user and custom settings will be lost.

1. Click the System tab.
2. Click the Restore All Camera Defaults button to restore the camera's factory default settings.

NOTE: If the camera is not connected to a Dynamic Host Configuration Protocol (DHCP) network, the IP address settings for the camera will be lost and the server will not recognize the camera. DHCP On is the default setting for the camera IP address.

3.2.1.1 General Settings

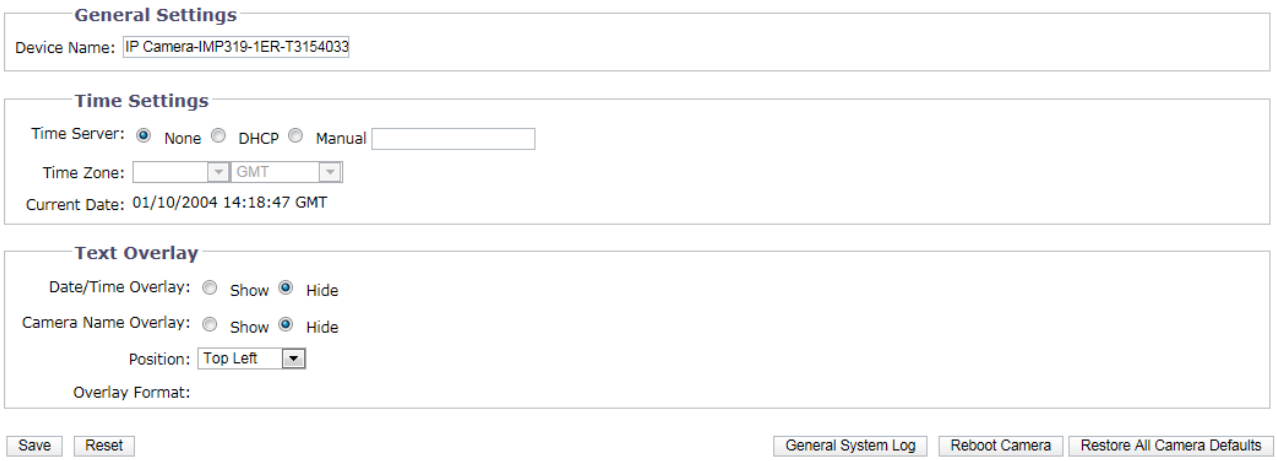


FIGURE 3-4: GENERAL SETTINGS

Device Name

Change the Device Name by following steps:

1. Click the **Device Name** box and highlight the text.
2. Type a user-friendly name into the **Device Name** box (2 to 64 characters). A user-friendly name makes it easier to recognize the device on the network. Examples of user-friendly names are Front Door, Lobby, or Parking Lot.
3. Click Save to save the new device name, or click Reset to restore to the previously saved device name.

Time Settings

If the camera is connected to a **Dynamic Host Configuration Protocol (DHCP)** network that has time server properties configured, the camera will synchronize automatically with the time server. If the DHCP network's time server properties are not configured or the network does not have a time server, you need to configure the time settings manually.

1. Type the IP address of the time server in the **Time Server** field. The time server is an external server that uses **Network Time Protocol (NTP)** to synchronize the camera date and time settings.

2. Select the **Time Zone** option. Select the continent and the region that are closest to the camera's location from the **Time Zone** drop-down menus.

NOTE: If your location observes a form of daylight saving time, the system will automatically change the time on the associated dates.

3. Click the Save button to save the settings, or click the Reset button to clear all of the information you entered without saving it.

Text Overlay

1. **Date/Time Overlay:** Select Show to display the date and time in the live view overlay. The default setting is **Hide**.
2. **Camera Name Overlay:** Select Show to display the device name in the live view overlay. The default setting is **Hide**.
3. *(Optional)* Select the display position for the overlay from the Position drop-down menu. Selections include **Top Left** and **Bottom Left**.
4. *(Optional)* Select the format in which the date and time will appear from the Overlay Format drop-down field if you have opted to show the Date/Time Overlay.

3.2.1.2 Backup & Restore

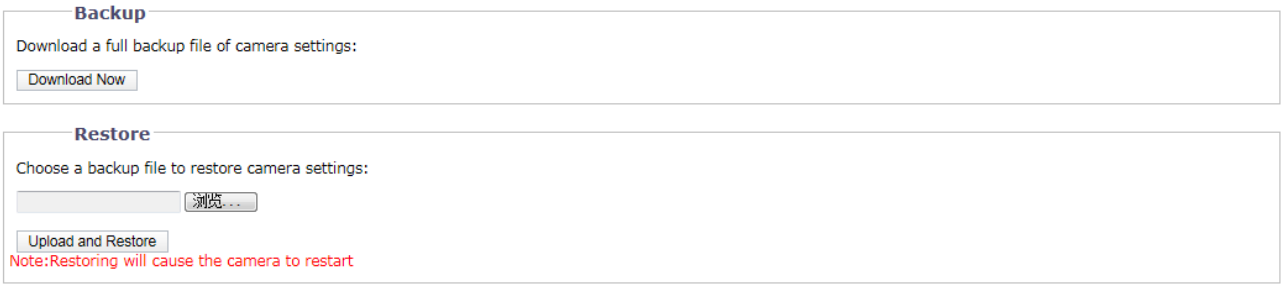


FIGURE 3-5: BACKUP AND RESTORE SETTINGS

Backup

Once the camera settings have been configured for optimal scene display, use the backup feature to save the camera settings.

Restore

If the camera settings are changed and inadvertently result in a less desirable image, use the restore setting to restore the camera to the previously saved settings.

NOTE: This feature is not intended for the configuration of multiple units or for firmware upgrades.

3.2.1.3 Information

The System Information page fields are read-only and include the firmware version, hardware version, model number, and serial number of the system are revealed here as below figure. This information is typically required by Pelco Product Support for troubleshooting purposes.

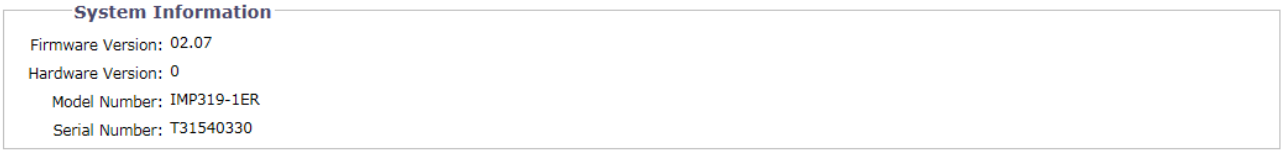


FIGURE 3-6: SYSTEM INFORMATION

3.2.1.4 Firmware

Users can update system firmware if available. All camera motions will shut down during firmware update. Please close any other screens before firmware update. Never disconnect power or LAN cable during the firmware update process. It takes approximately 3 minutes for the unit to reboot after firmware update process. Again, power can't be lost when updating firmware since it will cause the update failure and manufacturer maintenance will be required.

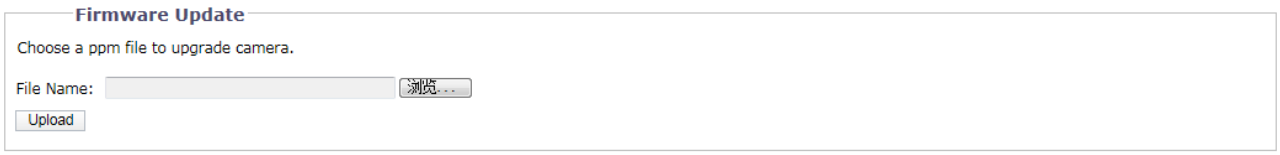


FIGURE 3-7: FIRMWARE UPDATE

3.2.2 Network

Use the Network tab to change the camera's general network settings, select the Secure Sockets Layer (SSL) settings, enable Secure Shell (SSH), configure 802.1x port security settings, choose SNMP Server Firewall mode and enable FTP access to this camera.

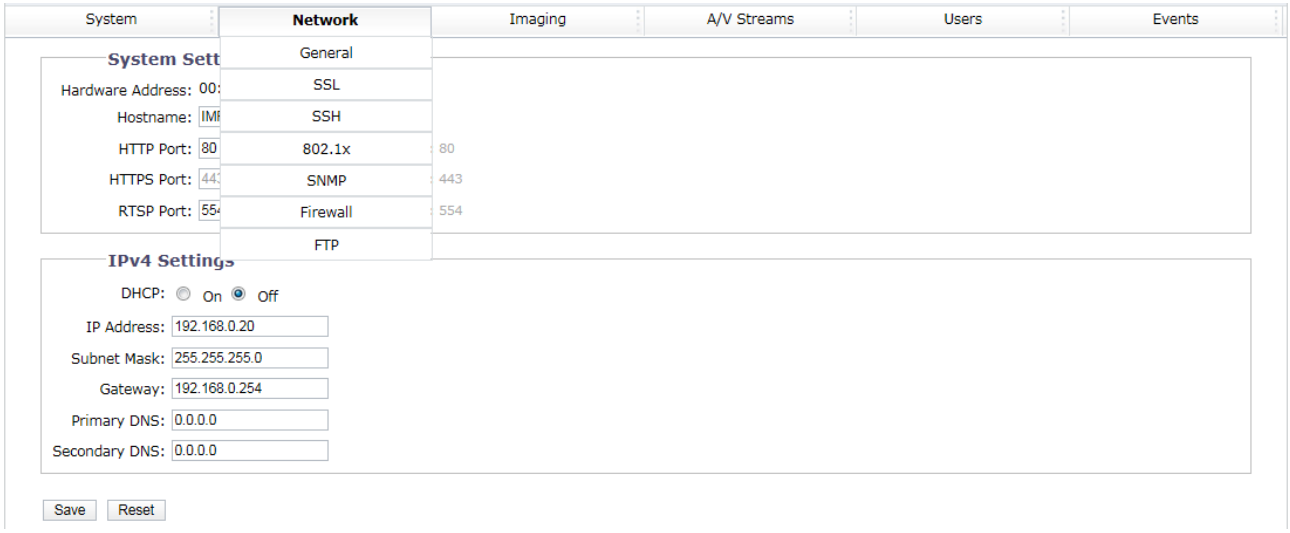


FIGURE 3-8: NETWORK CONFIGURATION

3.2.2.1 General

Set the General Network Settings for network communication settings.

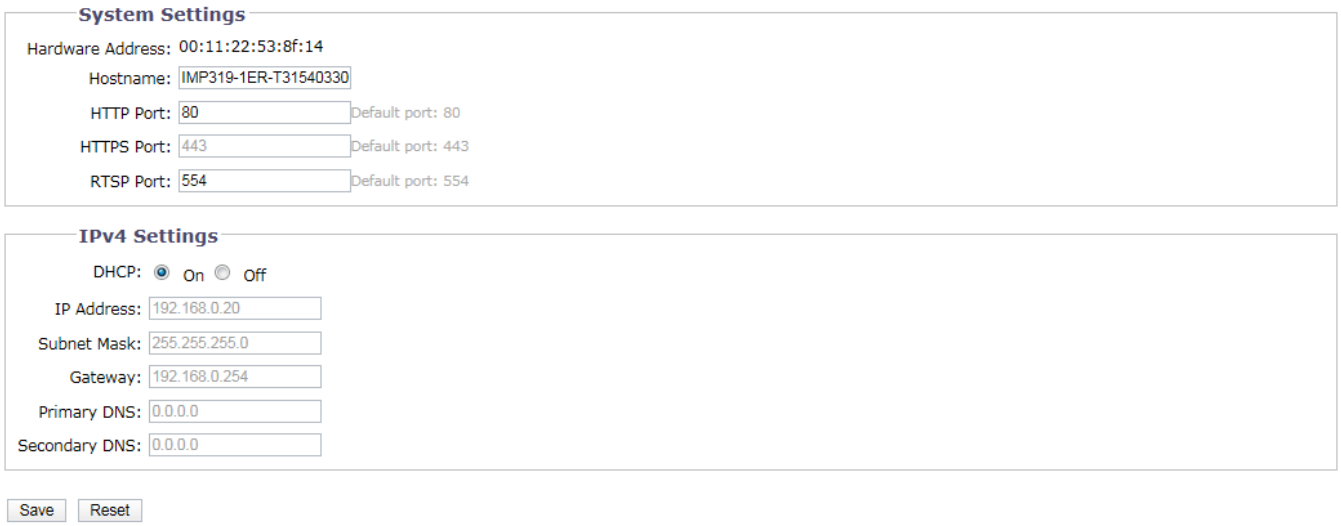


FIGURE 3-9: GENERAL NETWORK SETTINGS

System Settings

Settings under the System Settings are Hostname, HTTP Port, HTTPS Port, and RTSP Port. Contact your network administrator before changing port settings to ensure that your port settings do not conflict with your network infrastructure.

- **Hostname**
  1. Click in the **Hostname** box and highlight the text.
  2. Type a user-friendly name into the Hostname box (1 to 21 characters) using any combination of alphanumeric characters. A user-friendly name makes it easier to recognize the device on the network.
  3. Click the Save button to save the settings, or click the Reset button to clear all of the information you entered without saving it.

- **HTTP Port**

  NOTE: The HTTP port number must remain at the default setting (80) when connecting to a Pelco video management system (VMS) platform. If connecting to a Pelco VMS, do not change the HTTP port setting.
  1. Click in the **HTTP Port** box and highlight the text.
  2. Type the new port number in the **HTTP Port** field. The default port for HTTP communications is **80**.
  3. Click the Save button to save the settings, or click the Reset button to clear all of the information you entered without saving it.

- **HTTPS Port**

  NOTE: The HTTPS port is not configurable unless you have set SSL Mode to Optional or Required and installed a security certificate.
  1. Click in the **HTTPS Port** box and highlight the text.
  2. Type the new port number in the **HTTPS Port** field. The default port for HTTPS communications is **443**.
  3. Click Save. If you have changed the setting in error, you can click reset to revert to the previously saved setting.

- **RTSP Port**
  1. Click in the **RTSP Port** box and highlight the text.
  2. Type the new port number in the **RTSP Port** field. The default port for RTSP communications is **554**.
  3. Click the Save button to save the settings, or click the Reset button to clear all of the information you entered without saving it.

IPv4 Settings

Enable or disable the **Dynamic Host Configuration Protocol (DHCP)** server. DHCP automatically assigns an IP address to the device if there is a DHCP server on the network.

- **If DHCP is set to On,** the IP address, subnet mask, gateway, and DNS server settings are read-only text.
- **If DHCP is set to Off,** these settings must be manually changed.

  Change the following network settings as required:
  1. **IP Address:** The address of the camera connected to the network.
  2. **Subnet Mask:** The address that determines the IP network that the camera is connected to (relative to its address).
  3. **Gateway:** The router that accesses other networks.
  4. **DNS Servers:** The addresses of the dedicated servers that translate the names for Web sites and hostnames into numeric IP addresses.
  5. Click the Save button to save the settings, or click the Reset button to clear all of the information you entered without saving it.

3.2.2.2 SSL

To ensure security on the Internet, all Web browsers provide several security levels that can be adjusted for sites that use SSL technology to transmit data. **SSL** encrypts communications, making it difficult for unauthorized users to intercept and view user names and passwords.

SSL requires signed certificates to determine if the Web browser accessing the camera has the required authentication. The camera can generate a certificate signing request (CSR) that can be sent to a certificate authority for a signature (for example, VeriSign®), or it can generate a self-signed certificate using the **Generate Self-Signed Certificate** option.

FIGURE 3-10: SSL CONFIGURATION

SSL Configuration

Select one of the following modes:

- **Required:** A signed Secure Sockets Layer (SSL) certificate must be installed, and a secure URL that begins with the protocol name “https:” must be used to access the camera. Sensitive data is always encrypted during transmission. A URL that begins with the “http:” protocol rather than the “https:” protocol will be redirected to the secure URL automatically.

  NOTE: Beginning with firmware version 1.8.2, this field cannot be modified in the Web browser. To select or clear the

Required mode, you must use the ONVIF or Pelco API call. Doing so avoids placing the camera into a mode in which it would no longer work with a connected VMS system.

- **Optional:** A signed SSL certificate must be installed, but a secure URL that begins with the protocol name “https:” is optional when accessing the camera. You can also access the camera using a standard URL with the “http:” protocol, but sensitive data is not encrypted during transmission. To ensure that sensitive data is encrypted, you must use a secure URL with the “https:” protocol.

- **Disabled (default):** Turns off access to the Web client through SSL. Sensitive data will not be encrypted during transmission.
  NOTE: If the SSL mode is set to disabled, you cannot access the camera using a URL that begins with an “https:” protocol. Your Web browser displays an error message if you do not type the camera URL correctly.

Refer to the following sections for more information:

• ***Generating Self-Signed Certificate*** on page 29
• ***Generating Certificate Request*** on page 30

Certificate

- **Generating Self-Signed Certificate**

1. Click the **Install New Certificate** button located at the bottom of the **SSL** Configuration page. The Select Certificate Install Method option buttons appear on the page.

FIGURE 3-11: SELECT CERTIFICATE INSTALL METHOD OPTION

2. Select the “**Generate Self-signed Certificate**” option, and then click **Next**. The “**Self-signed Certificate Information Form**” opens.

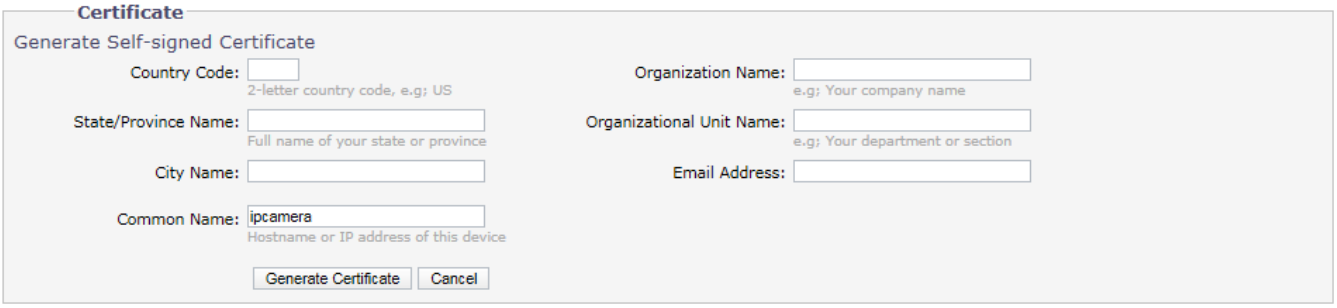


FIGURE 3-12: GENERATING SELF-SIGNED CERTIFICATE CONFIGURATION

3. Fill in all of the fields, and then click **Generate Certificate**. The following progress message appears on the page: “Loading data…” After a while, the certificate is uploaded to the device.
4. After the certificate is uploaded, select the desired mode.
5. Click Save.

NOTE: Self-signed certificates are valid for one year. The certificate’s expiration date is listed in the Installed Certificate

information section. If the certificate has expired and you attempt to access the camera using a secure URL, the Web browser displays a message. Repeat this procedure to generate and upload a new certificate.

- **Generating Certificate Request**

1. Click the **Install New Certificate** button located at the bottom of the SSL Configuration page. The Select Certificate Install Method option buttons appear on the page.
2. Select **Generate Certificate Request**, and then click **Next**. The "**Certificate Request Form**" opens.

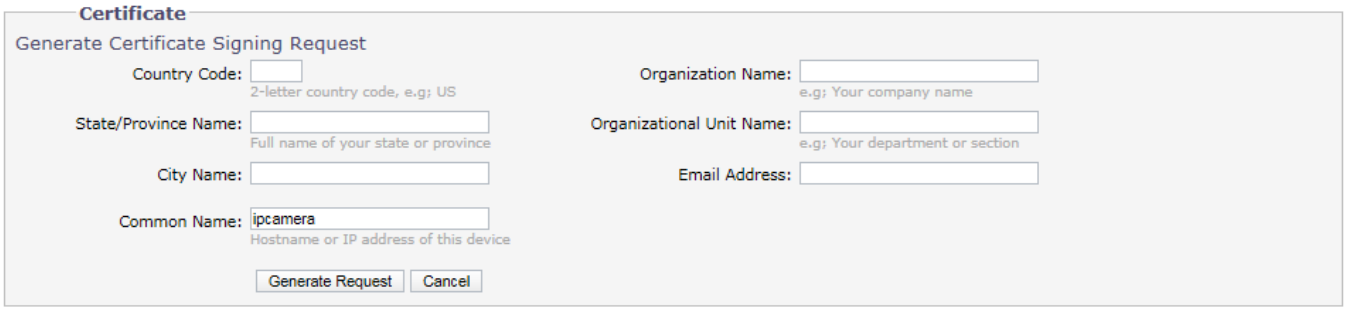


FIGURE 3-13: GENERATING CERTIFICATE REQUEST

3. Fill in all of the fields, and then click **Generate Request**. The following progress message appears on the page: "Generating certificate signing request, please wait…"
4. Send the CSR, which looks like an encrypted block of undecipherable text, to a third-party certificate authority of your choice for a signature.
5. After you receive the signed certificate, click the Install Certificate button to upload the signed certificate to the device.
6. After the certificate is uploaded, select the desired mode.
7. Click Save.

NOTE: Depending on the third-party certificate authority that signed your certificate, you might need to renew your certificate after a specified amount of time. Consult the certificate authority for more details.

- **Upload Certificate**

1. Click the **Install New Certificate** button located at the bottom of the SSL Configuration page. The Select Certificate Install Method option buttons appear on the page.
2. Select **Upload Certificate**, and then click **Next**. The "**Certificate**" opens.

FIGURE 3-14: UPLOAD CERTIFICATE

3. Choose the Certificate you want to upload and then click **Upload** button. The following progress message appears on the page: "Loading data…"
4. After the certificate is uploaded, select the desired mode.
5. Click Save.

- **Delete Certificate**
  1. Once you successfully upload a certificate, **Delete Certificate** button will appears at the bottom of the SSL Configuration page.
  2. If you want to delete the certificate, click the **Delete Certificate**, The following progress message appears on the page: “Deleting certificate file…”
  3. Click Save.

3.2.2.3 SSH

SSH is a user-enabled protocol that allows Pelco Product Support to log on to and service the camera for advanced troubleshooting purposes.

From this page, users with the appropriate permissions can enable or disable SSH access to the camera.

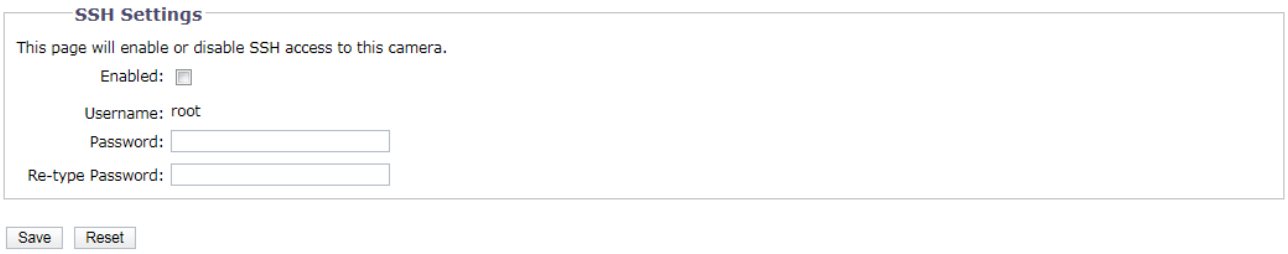


FIGURE 3-15: ENABLING SECURE SHELL

SSH Settings

1. Select the **Enabled** check box.
2. Click in the **Password** box and type a password (4 to 16 alphanumeric characters). Passwords are case-sensitive. **NOTE:** The default username is “root” and cannot be changed. The username and password are required when accessing the camera through a third-party SSH client.
3. Click in the “**Re-type Password**” box and retype your password.
4. Click the Save button to save the password and enable SSH, or click the Reset button to clear all of the information you entered without saving it.

3.2.2.4 802.1x

802.1x is a port security that authenticates devices that want to establish a point-to-point access through a wired or wireless port using Extensible Authentication Protocol (EAP). This port-based authentication method prevents unauthorized access to a Local Area Network (LAN) through a physical port. For example, when a device is connected to a network port, the network switch will ask the device for authentication.

If the credential is accepted when the device sends a credential to the network switch, the network switch will open the port for normal use.

If authentication fails, the device is prevented from accessing information on the port.

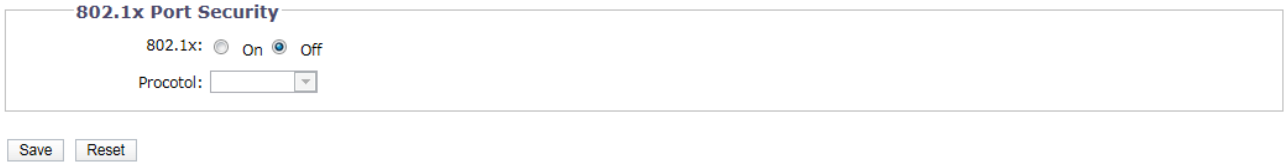


FIGURE 3-16: CONFIGURING THE 802.1X PORT SECURITY SETTINGS

802.1x Port Security

WARNING: To prevent network conflicts, contact your network administrator before configuring the 802.1x port security settings.

1. Select the **On** option for the 802.1x Port Security. The default setting for 802.1x is **Off**.
2. Select the Extensible Authentication Protocol (EAP) method from the Protocol drop-down menu. Supported EAP methods include **EAP-MD5**, **EAP-TLS**, **EAP-TTLS**, and **EAP-PEAP**.
3. Type the information required for the selected 802.1x authentication method.
4. Connect the PC to an 802.1x secured switch that has the same **EAP** method.
5. Click the Save button to save the settings, or click the Reset button to clear all of the information you entered without saving it.

3.2.2.5 SNMP

SNMP is an application layer protocol used to manage TCP/IP-based networks from a single workstation or several workstations. The camera supports SNMP versions 2c and 3 and can be configured to send data using a trap.

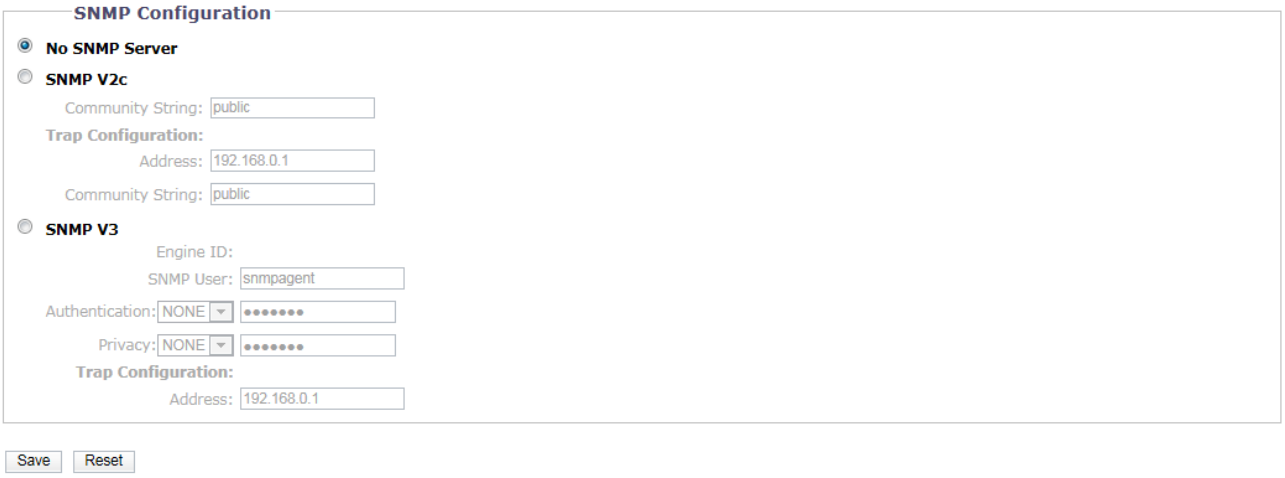


FIGURE 3-17: SNMP CONFIGURATION

SNMP Configuration

WARNING: The Simple Network Management Protocol (SNMP) settings are advanced controls. Consult your network administrator to obtain the required information to configure SNMP settings.

- **No SNMP Server**

  None disables the SNMP configuration and is the default setting.

- **CONFIGURING SNMP V2C**

  1. Select **V2c** as the SNMP Version.
  2. Type the community name in the Community String box. The default name for the Community String is “public.”
  3. Configure the Trap Configuration settings.
     - **Address:** Type the host name or IP address of the recipient of the trap message.
     - **Community String:** Type the name of the community that should receive the trap message.
  4. Click the Save button to save the settings, or click the Reset button to clear all of the information you entered without saving it.

- **CONFIGURING SNMP V3**

1. Select **V3** as the SNMP Version.
2. Type the SNMP user name in the **SNMP User** field.
3. Select the encryption algorithm for authentication from the **Authentication** drop-down menu: None, MD5, or SHA. If you use authentication method MD5 or SHA, type a password in the text box to the right of the selected Authentication encryption.
4. Select the privacy encryption algorithm setting from the **Privacy** drop-down menu: None, DES, or AES. If you use privacy method DES or AES, type a password in the text box to the right of the selected Privacy encryption.
5. Configure the address for the **Trap Configuration**. The Address is the host name or IP address of the recipient of the trap message.
6. Click the Save button to save the settings, or click the Reset button to clear all of the information you entered without saving it.

NOTE: SNMP V2c and SNMP V3 configuration settings are independent of each other, but only one SNMP version can be active at a time.

3.2.2.6 Firewall

Set the **Firewall** function. A firewall is a system or group of systems that manages access between two networks.

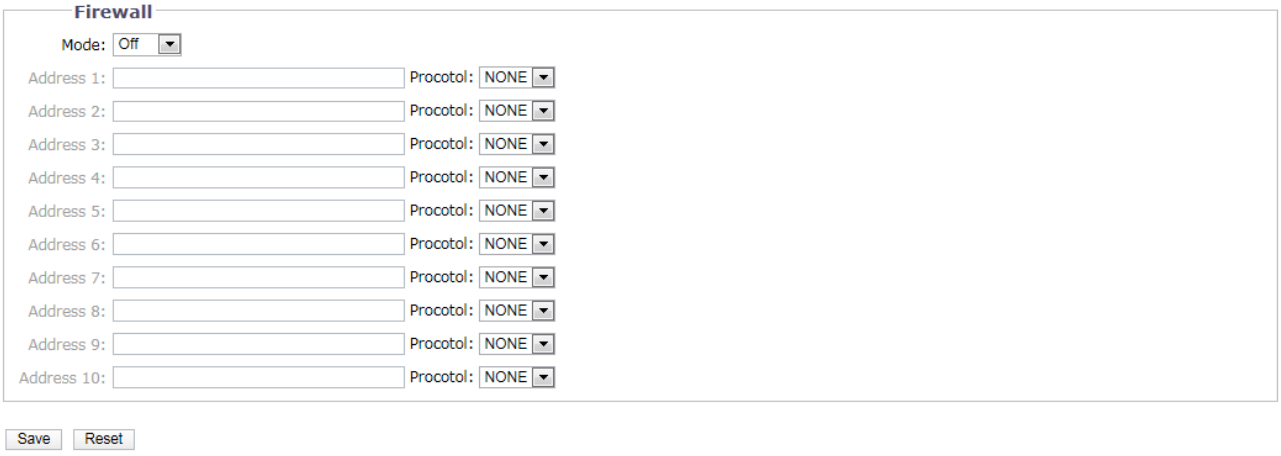


FIGURE 3-18: FIREWALL CONFIGURATION

Firewall

1. Select **Allow** or **Deny** mode to enable this function. The default setting is **Off**.
2. Type IP address in the **Address** field and select protocols. It is carried out over two transport layer protocols: TCP (Transmission Control Protocol) and UDP (User Datagram Protocol)
   - **TCP:** a connection-oriented, reliable-delivery, robust and high performance transport layer protocol.
   - **UDP:** a connectionless protocol, it is efficient protocol for some services and is resourceful but difficult to secure.
3. Click the Save button to save the settings, or click the Reset button to clear all of the information you entered without saving it.

3.2.2.7 FTP

This page will enable or disable **FTP** access to this camera. In this page, users can activate a FTP Server to access the SD card for recordings. **Enabled** the **FTP** and use this function.

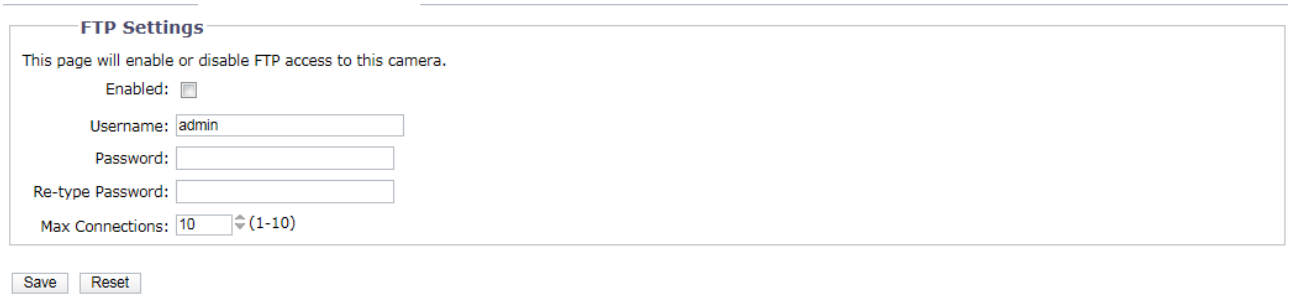


FIGURE 3-19: FTP SETTINGS

FTP Settings

1. Select the **Enabled** check box to activate the FTP function, and follow the following procedures to set up related settings.
2. Enter a **Username** if activated the FTP function.
3. Enter a **Password** associated with the **Username**.
4. **Re-type Password** to confirm it.
5. Set the number of maximum connections by entering a number in the **Max Connections** field.

   NOTE: This is the maximum of FTP Client connections, not the maximum of IE Window's connections.

3.2.3 Imaging

Use the Imaging tab to change the camera's general image settings, adjust the camera exposure, program the focus mechanism, or define window blanking privacy areas.

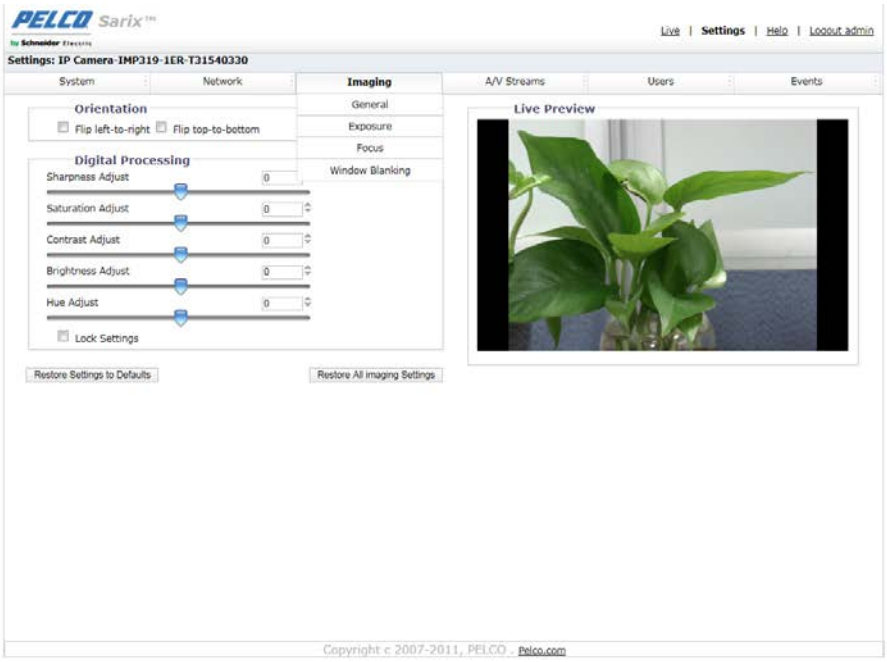


FIGURE 3-20: IMAGING SETTINGS

3.2.3.1 General

General imaging settings include adjustments for camera orientation and digital processing.

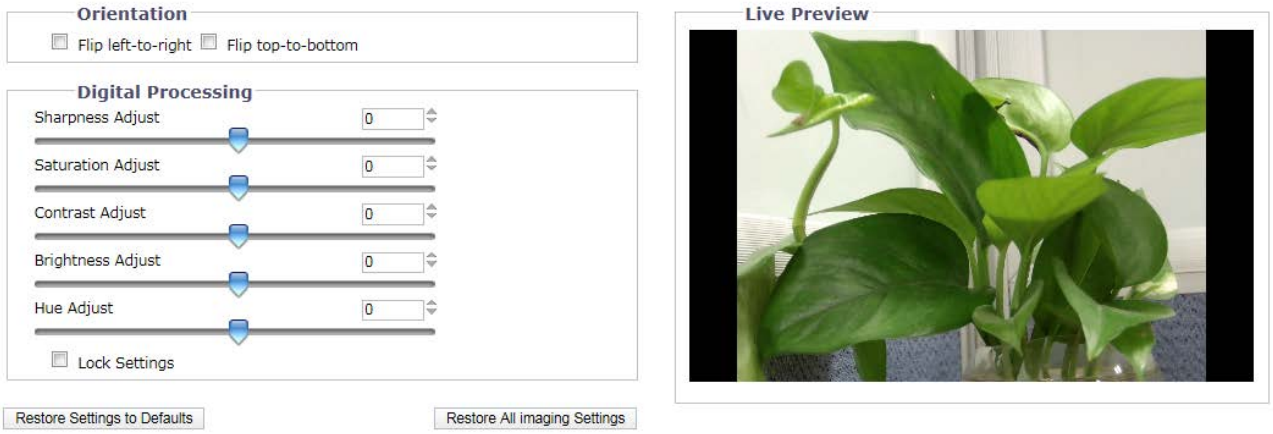


FIGURE 3-21: GENERAL IMAGING SETTINGS

Orientation

Use this setting when installing the camera in an inverted position. If the orientation is not adjusted, the image will display upside down and mirrored.

Select one of the following options:

1. Click the "**Flip left-to-right**" box to rotate the camera image 180 degrees horizontally.
2. Click the "**Flip top-to-bottom**" box to rotate the camera image 180 degrees vertically.

Digital processing

Digital processing settings can adjust the camera's sharpness, saturation, contrast, brightness and hue.

Move the slider to the left or right to change the following settings:

- **Sharpness:** Controls the clarity of detail in a scene. Move the slider to the right to increase the sharpness; move the slider to the left to decrease the sharpness. Increasing the sharpness also increases the image noise. The range of adjustment is –100 to 100; the default setting is 0 (zero).
- **Saturation:** Controls how intense or vivid the colors are in a scene. Move the slider to the right to increase the saturation level; move the slider to the left to decrease the saturation level. The range of adjustment is –100 to 100; the default setting is 0 (zero).
- **Contrast:** Controls gradations between the darkest and lightest portions of the scene. Move the slider to the right to increase the contrast; move the slider to the left to decrease the contrast. The range of adjustment is –100 to 100; the default setting is 0 (zero).
- **Brightness:** Controls the lighting detail in a scene. Move the slider to the right to lighten the image; move the slider to the left to darken the image. The range of adjustment is –100 to 100; the default setting is 0 (zero).
- **Hue:** Controls the color in a scene. Move the slider to the right to achieve a cool color image; move the slider to the left to achieve a warm color image. The range of adjustment is –100 to 100; the default setting is 0 (zero).

Check **Lock Settings** box to lock the above Digital processing settings.

3.2.3.2 Exposure

Exposure is the amount of light detected by the camera sensor. A scene with correct exposure settings has adequate detail and contrast between white and dark values. An image with too little or too much exposure eliminates detail in the scene. The camera features Exposure and Day/ Night settings.

NOTE: IR Illumination function is available in IR models only.

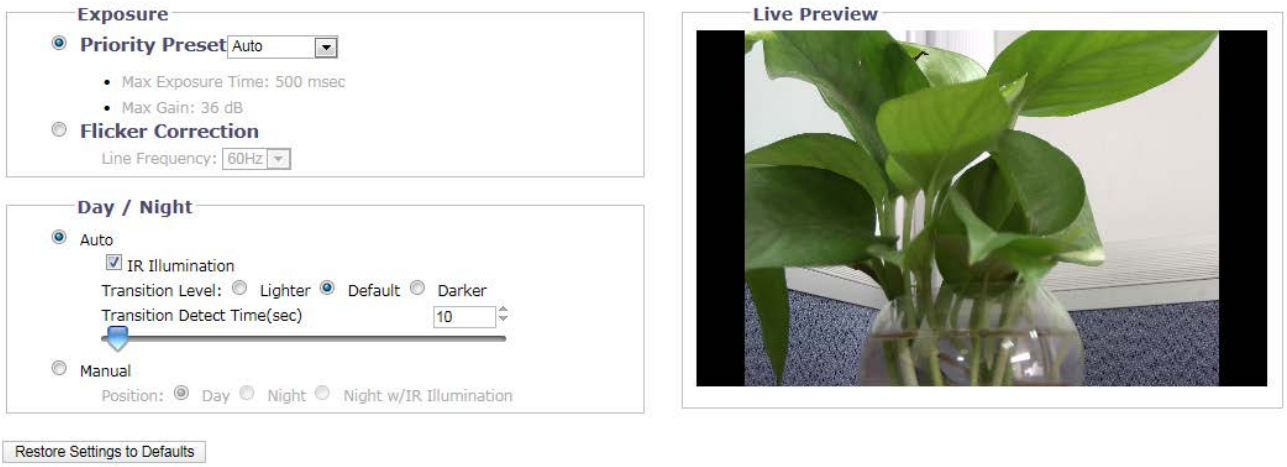


FIGURE 3-22: EXPOSURE SETTINGS

Exposure

- **Priority Preset**

  Select **Auto**, **Noise**, or **Frame Rate** to exposure in different value of **Max Exposure Time** and **Max Gain**.

- **Flicker Correction**

  Flickering by fluorescent light can be reduced by selecting “50Hz” if the power frequency is 50Hz, “60Hz”, if 60Hz.

Day/Night

The Day Night Auto mode setting automatically controls the IR cut filter depending on the Transition Level and Transition Detect Time settings.

- **Auto**

  1. **Transition Level:** Determines when the camera changes from day mode (color) to night mode (black-white). Move the slider to the left or right to change the transition level to a lighter or darker setting. Select a lighter transition level setting if you want the camera to change modes at a high lux setting. Use the default setting of 4 for normal day/night operation. Use a darker transition level to change modes at a low lux setting.

TABLE 3-1. LUX TRANSITION POINTS FOR INCANDESCENT LIGHTING

	Transition Level Setting	Day to Night Transition Point
Lighter ↓ Darker	1	1.0 ~ 2.0 lux
	2	0.50 ~ 1.0 lux
	3	0.25 ~ 0.50 lux
	4	0.125 ~ 0.25 lux
	5	0.0625 ~ 0.125 lux

Check **IR Illumination** box to enable IR Illumination.

2. **Transition Detect Time (sec):** Controls the length of time the camera is exposed to a light level before it changes to color or black-white mode.
   This setting is useful for dark scenes where a bright light is momentarily introduced in the scene (for example, when a car with its headlights turned on passes the camera scene).

- **Manual**
  1. **Day:** If **Day** mode selected, the camera is forced to stay in **Day** mode all day.
  2. **Night:** If **Night** mode selected, the camera is forced to stay in **Night** mode all day.
  3. **Night w/IR Illumination:** If **Night w/IR Illumination** mode selected, the camera is forced to stay in **Night w/IR Illumination** mode all day with **IR illumination** on.

3.2.3.3 Focus

Focus sets the back focus to the center focal point of the scene. The camera can be configured to back focus automatically or manually. Auto focus automatically back focuses the camera on the subject in the center of the scene. Manual focus turns off the auto focus mechanism and locks the camera at a user-specified position. The manual focus setting is recommended only for indoor applications that have a single, unchanging primary light source. The Focus page also includes **Full Range Auto-Focus**, **Quick Auto-Focus**, and a **Restore Settings to Defaults**.

FIGURE 3-23: FOCUS SETTINGS

Focus

- **Auto Focus**
  1. **Temperature Change Refocus:** The camera is programmed to run a quick automatic focus sequence when the internal temperature sensor of the camera detects an environmental temperature change of 41°F (5°C). This focus sequence adjusts the center focal point of the scene to maintain optimal focus. The default setting is **Off**; select **On** to turn on this setting.
  2. **Day/Night Switch Refocus:** The default setting for the Day/Night Switch Refocus is **Off**. Select **On** if the camera's focal length is greater than 25 mm or the night scene uses mostly IR lighting. The best method to determine if the day/night refocus should be enabled is to test the camera with the daytime light conditions, and then test it again with the nighttime light conditions.
     When enabled **On** this setting refocuses the camera when the camera changes from day mode (color) to night mode (black-white) or vice versa. For example, if the camera changes from day mode to night mode, the imager automatically adjusts the back focus for the change in light.

3. If required, use one of the following buttons to adjust the focus:
   a **Full Range Auto-Focus:** The camera starts a full-range search to find the optimal focal point for the scene.
   b **Quick Auto-Focus:** The camera searches for the optimal focal point in a limited range.
   c **Restore Settings to Defaults:** The camera resets the auto focus to the factory default setting.

- **Manual Focus**

  Select **Manual** Mode. Two sliders will appear, one for **Day Manual Focus Position**, the other for **Night Manual Focus Position**. Each slider will show a value that is the best focus position for the camera during the day and night.

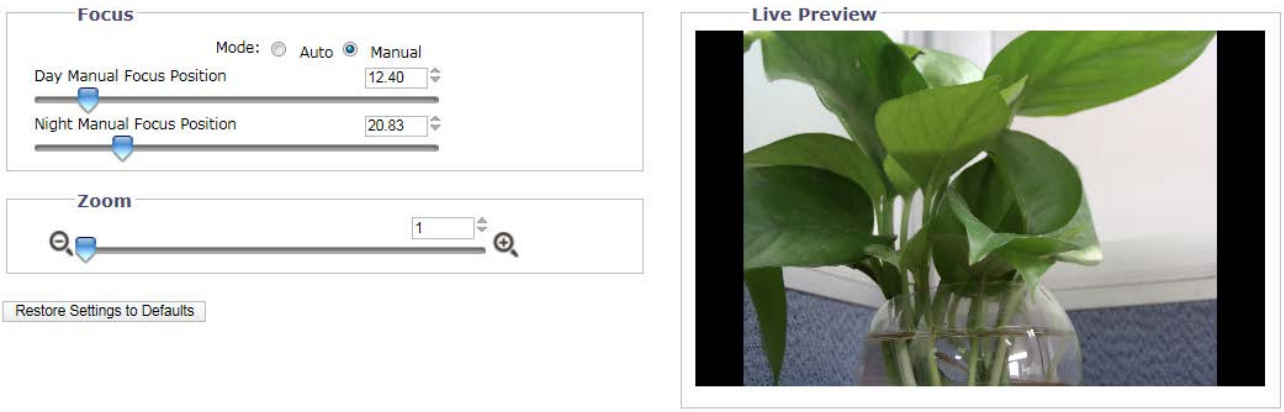


FIGURE 3-24: MANUAL FOCUS

1. **Day Manual Focus Position:** If you need to fine-tune the daytime focus, slightly move the **Day Manual Focus Position** slider to the left or right.
2. **Night Manual Focus Position:** If you need to fine-tune the nighttime focus, slightly move the **Night Manual Focus Position** slider to the left or right.
3. If required, click the **Restore Settings To Defaults** button to reset the focus to the factory default setting.

Zoom

Manually move the **Zoom** slider to the left or right to zoom in or zoom out the image, adjust the zoom value from 1.00~3.00 to get the desired field of view.

3.2.3.4 Window Blanking

Window blanking is used to conceal user-defined privacy areas. A blanked area appears on the screen as a solid gray window. The camera can handle up to four blanked windows as long as the total blanked area does not exceed 50 percent of the field of view.

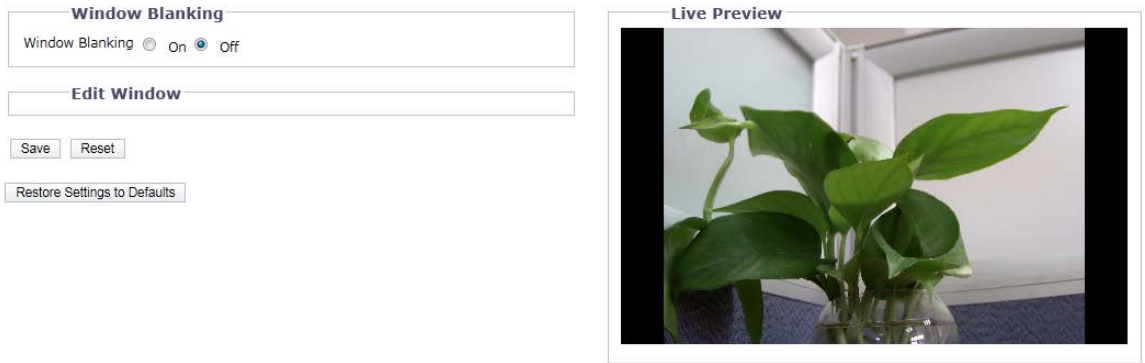


FIGURE 3-25: WINDOW BLANKING SETTINGS

Window Blanking

- **Window Blanking On**

  1. Draw a window in the Live Preview area of the page:
     a Hold down the left mouse button.
     b Drag the mouse diagonally across the area you want to blank.
     c A color-coded box appears in the Edit Window section of the page that is the same color as the window drawn in the Live Preview area.

FIGURE 3-26: WINDOW BLANKING ON

NOTE: Up to four blanked windows can be defined, but the blanked area cannot exceed 50 percent of the field of view.

  2. To resize the window, click and drag one or more of the points until the window is the desired shape and size.
  3. Click the Save button to save the settings, or click the Reset button to clear all of the information you entered without saving it.

- **Deleting a window blanking area**

  1. In the Edit Window area of the page, click the Delete button next to the window blanking area you want to delete.
  2. Click the Save button to save the settings, or click the Reset button to clear all of the information you entered without saving it.

- **Window Blanking Off**

  1. Select the Off option for Window Blanking.
  2. Click the Save button to save the settings, or click the Reset button to clear all of the information you entered without saving it.

3.2.4 A/V Streams

Use the A/V Streams tab to configure the video and audio streams for the camera. The A/V Streams tab includes a Video Configuration page and an Audio Configuration page.

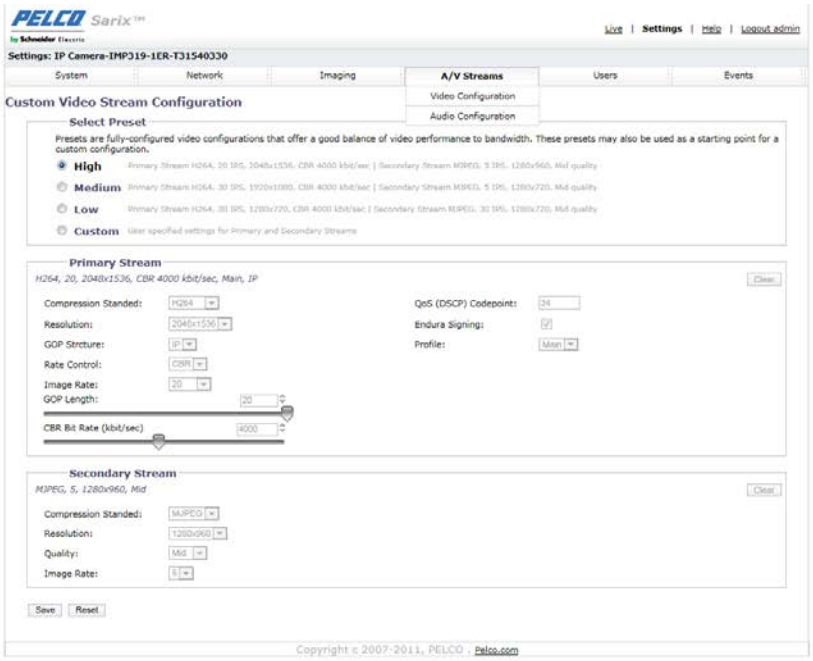


FIGURE 3-27: A/V STREAMS

3.2.4.1 Custom Video Stream Configuration

The Video Configuration page allows you to customize the compression, resolution, image rate, and bit rate of the video streams. The default names for the streams are Primary Stream and Secondary Stream. Although each stream can be configured independently, the settings of one stream can limit the options available to the other stream, depending on the processing power used.

NOTE: Always configure the primary stream before the secondary stream. The primary stream should always be the most resource-intensive of the streams.

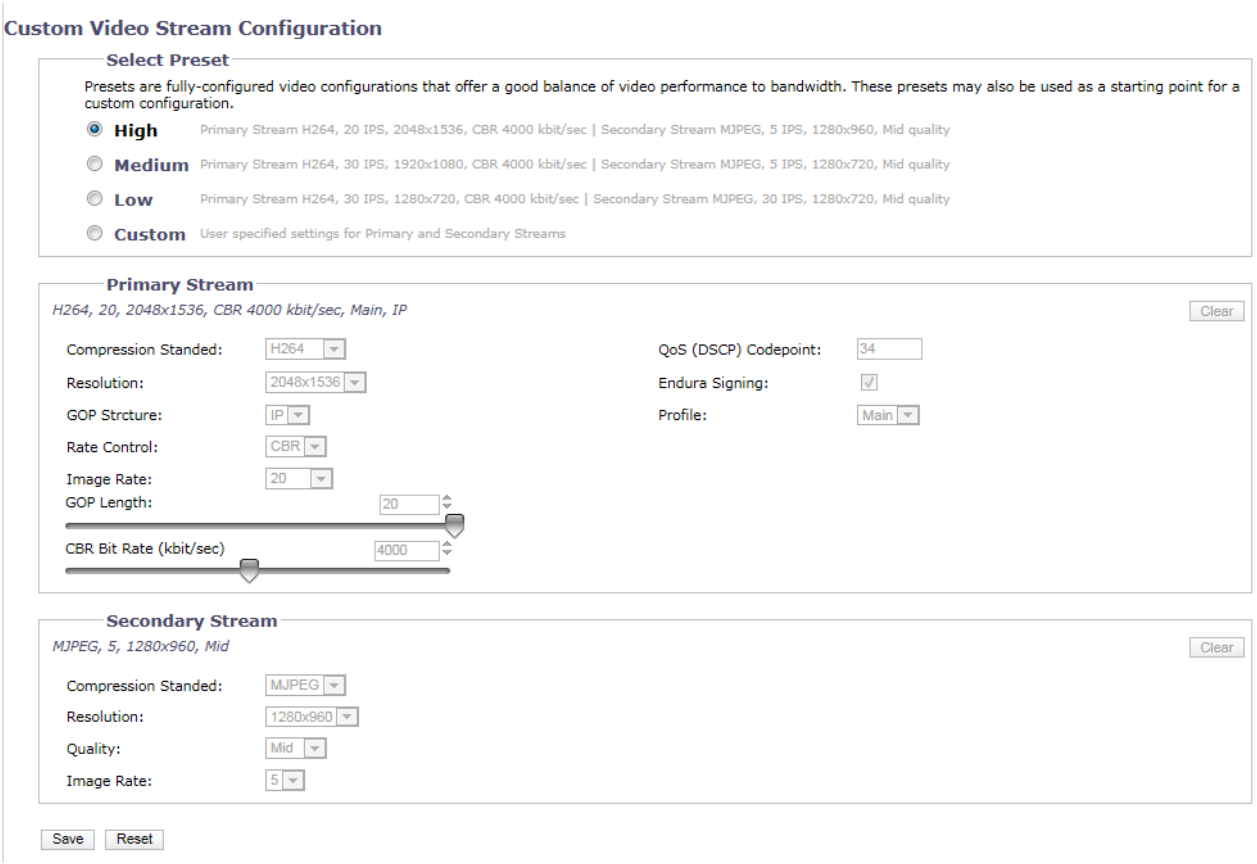


FIGURE 3-28: CUSTOM VIDEO STREAM CONFIGURATION

Select Preset

Presets are fully-configured video configurations that offer a good balance of video performance to bandwidth. These presets may also be used as a starting point for a custom configuration.

- **High:** Primary Stream H264, 20 IPS, 2048x1536, CBR 4000 kbit/sec | Secondary Stream MJPEG, 5 IPS, 1280x960, Mid quality.
- **Medium:** Primary Stream H264, 30 IPS, 1920x1080, CBR 4000 kbit/sec | Secondary Stream MJPEG, 5 IPS, 1280x720, Mid quality.
- **Low:** Primary Stream H264, 30 IPS, 1280x720, CBR 4000 kbit/sec | Secondary Stream MJPEG, 30 IPS, 1280x720, Mid quality.
- **Custom:** User specified settings for Primary and Secondary Streams.

Primary Stream

Select Custom in Select Preset and configure Primary Stream.

- **Compression Standard**
  1. **H264:** A new version of MPEG-4 compression used in high-definition video players such as Blu-ray™ and HD-DVD. H.264 is the most processor-intensive, but it requires the least amount of bandwidth.
  2. **MJPEG:** A commonly used video compression scheme. MJPEG has the least impact on the camera's processor, but it requires the most bandwidth.

- **Resolution**

  Refer to the following table for the resolution capabilities of your camera model.

TABLE 3-2. CORRELATIONS OF RESOLUTIONS/ COMPRESSIONS/ STREAMS

	Primary Stream		Secondary Stream	
Compression Standard / Available Resolutions	H264	MJPEG	H264	MJPEG
2592 x 1944*	2592x1944	N/A	800x600 640x480	800x600 640x480
2048x1536**	2048x1536	2048x1536	1280x960 800x600 640x480	1280x960 800x600 640x480
1920x1080	1920x1080	1920x1080	1280x720 1024x576	1280x720 1024x576
1600x1200	1600x1200	1600x1200	1280x960 800x600 640x480	1280x960 800x600 640x480
1280x960	1280x960	1280x960	1280x960 800x600 640x480	1280x960 800x600 640x480
1280x720	1280x720	1280x720	1280x720 1024x576	1280x720 1024x576
1024x576	1024x576	1024x576	1024x576	1024x576
800x600	800x600	800x600	800x600 640x480	800x600 640x480
640x480	640x480	640x480	640x480	640x480

***NOTE:** 2592 x 1944 supports **5MP Model** only.

** **NOTE:** 2048x1536 supports **5MP Model** and **3MP Model** only.

- **GOP Structure**

  The group of pictures (GOP) structure is the sequence in which frames are placed within a video stream.

  IP: A compression that uses only I-frames and P-frames to provide low latency and a high level of decoder support.

- **Rate Control**

  The rate control setting determines the bit rate and quality of each frame in the video stream.

  1. **CBR:** The constant bit rate (CBR) streams video at a fixed number of bits per second.
  2. **VBR:** The Variable Bit Rate (VBR) streams video at a variable number of bits per second.

     Select **VBR** Rate Control. VBR Bit Rate Min (kbit/sec) slider and VBR Bit Rate Max (kbit/sec) slider will appear.

Refer to the following section for more information:

- ***VBR Bit Rate Min (kbit/sec)*** on page 43
- ***VBR Bit Rate Max (kbit/sec)*** on page 43

- **Image Rate**

  The image rate is the number of images per second (ips) available for the video stream configuration. Available image rates are 30, 25, 20, 16.67, 15, 12.5, 10, 5, and 1.

  NOTE: The maximum image rate setting might not be obtainable due to the programmed compression standard and the resolution of the stream.

- **GOP Length**

  Select the GOP Length from 1 to 60. Recovery of the lost frames will be more difficult as the value gets bigger; on the contrary, it will increase the bite rate obviously and aggravate the network bandwidth.

- **CBR Bit Rate (kbit/sec)**

  Choose the bit rate control selection based on user requirements from 500 ~ 8000. A higher bit rate will consume higher network bandwidth.

- **VBR Bit Rate Min (kbit/sec)**

  Choose the bit rate control selection based on user requirements from 500 ~ 8000. A higher bit rate will consume higher network bandwidth.

- **VBR Bit Rate Max (kbit/sec)**

  Choose the bit rate control selection based on user requirements from 500 ~ 8000. A higher bit rate will consume higher network bandwidth.

- **QoS (DSCP) Codepoint**

  Quality of Service (QoS) for Differentiated Services Code Point (DSCP) is a code that allows the network to prioritize the transmission of different types of data. This setting is only available with H264.

  NOTES:

  1. If you are not familiar with DSCP, contact your network administrator before changing this setting.
  2. Your network must be configured to use QoS. If you are unsure if your network is QoS-aware, contact your network administrator.

- **Endura Signing**

  Enabling the Endura Signing feature allows an Endura® system to authenticate video from an Endura recorded stream. This setting is only available with H264.

- **Profile**

  The profile defines the subset of bit stream features in an H.264 stream, including color reproduction and additional video compression. It is important that the selected profile is compatible with the recording device so that a stream can be decoded and viewed.

  1. **Main:** An intermediate profile with a medium compression ratio. Main is the default profile setting. This profile is compatible with most recorders and uses fewer bits to compress video than the baseline profile; however, it uses more bits than the high profile. The main profile supports I-frames, P-frames, and B-frames.
  2. **High:** A complex profile with a high compression ratio. This is the primary profile for high-definition television

applications; for example this is the profile adopted for Blu-ray and HD-DVD. The high profile supports I-frames, P-frames, and B-frames.

Secondary Stream

Select Custom in Select Preset and configure Secondary Stream. Repeat Primary Stream setting steps for the Secondary Stream settings.

3.2.4.2 Audio Configuration

The Audio Configuration page allows you to setup the audio device. The default setting for Audio is disabled, which means that no audio is transmitted from the camera. When enabled, audio is transmitted from the camera to the PC. Based on your system configuration, images and audio may not be synchronized.

NOTE: Improper use of audio/visual recording equipment may subject you to civil and criminal penalties. Applicable laws regarding the use of such capabilities vary between jurisdictions and may require, among other things, express written consent from the recorded subjects. You are solely responsible for insuring strict compliance with such laws and for strict adherence to any/all rights of privacy and personality.

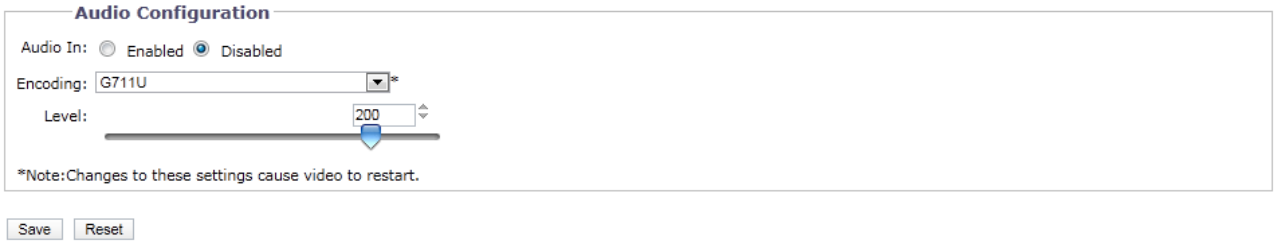


FIGURE 3-29: AUDIO CONFIGURATION

Audio In

- **Enabled**

  Set to **Enabled** when receiving audio from a microphone plugged into the unit.

- **Disabled**

  Set to **Disabled** to close **Audio In**.

Encoding

Two audio codecs **G711-Alaw/G711-Ulaw** can be chosen from.

Level

The sound levels are selectable from 1~255.

NOTE: Changes to these settings cause video to restart.

3.2.5 Users

Use the Users tab to create and manage user accounts and to change the way the camera manages the users settings.

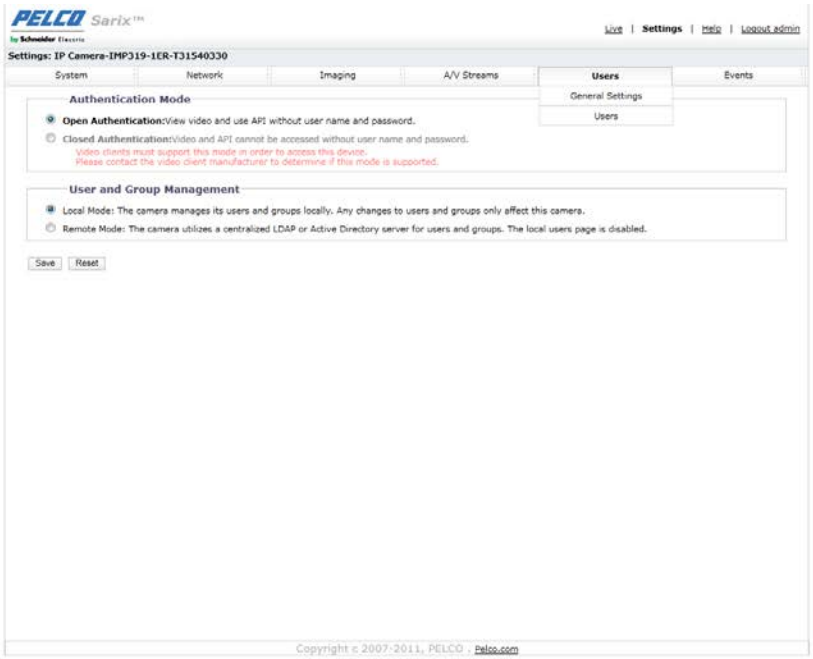


FIGURE 3-30: USERS CONFIGURATION

3.2.5.1 General Settings

Use the General Settings page to set the public user access level. This access level is a predefined set of user permissions that allows the camera to be accessed without logging on. Available permission levels depend upon the model of the device that you are using.

The General Settings page also allows you to change the way the camera manages users and groups settings. These settings can be managed on a camera-to-camera basis or by using a centralized server to apply changes to multiple cameras.

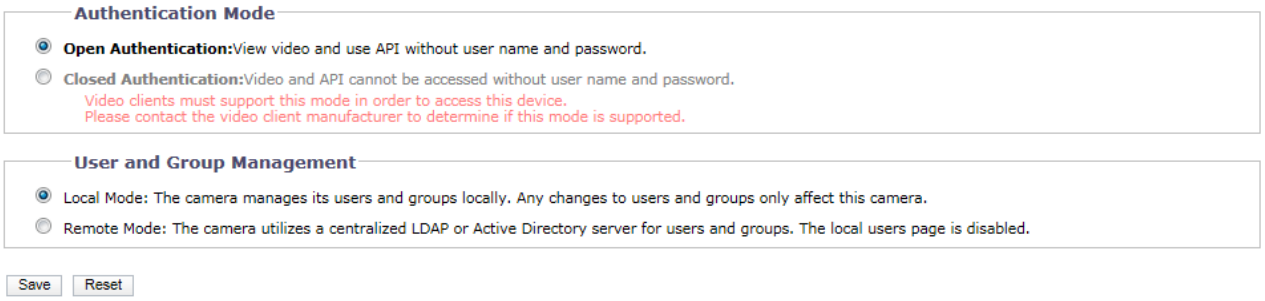


FIGURE 3-31: USERS GENERAL SETTINGS

Authentication Mode

- **Open Authentication**

  Allows users to view video and use the camera API without validating user credentials. With Open Authentication selected, you can select “Require password for PTZ” to limit PTZ control to authenticated users.

- **Closed Authentication**

  Requires users to possess valid credentials to view video and access the camera API. Before selecting Closed Authentication, ensure that your video management system supports Closed Authentication mode.

User and Group Management

Sarix cameras support two methods for managing the permissions of users and groups.

- **Local Mode**

  The camera manages users and groups locally. This is the default setting.

- **Remote Mode**

  The camera authenticates and manages users through an LDAP server supported by Microsoft® Active Directory®. This allows administrators to tie cameras and group permissions into existing single sign-on services (SSO). Selecting Remote Mode disables local user management settings.

  Enabling Remote Mode

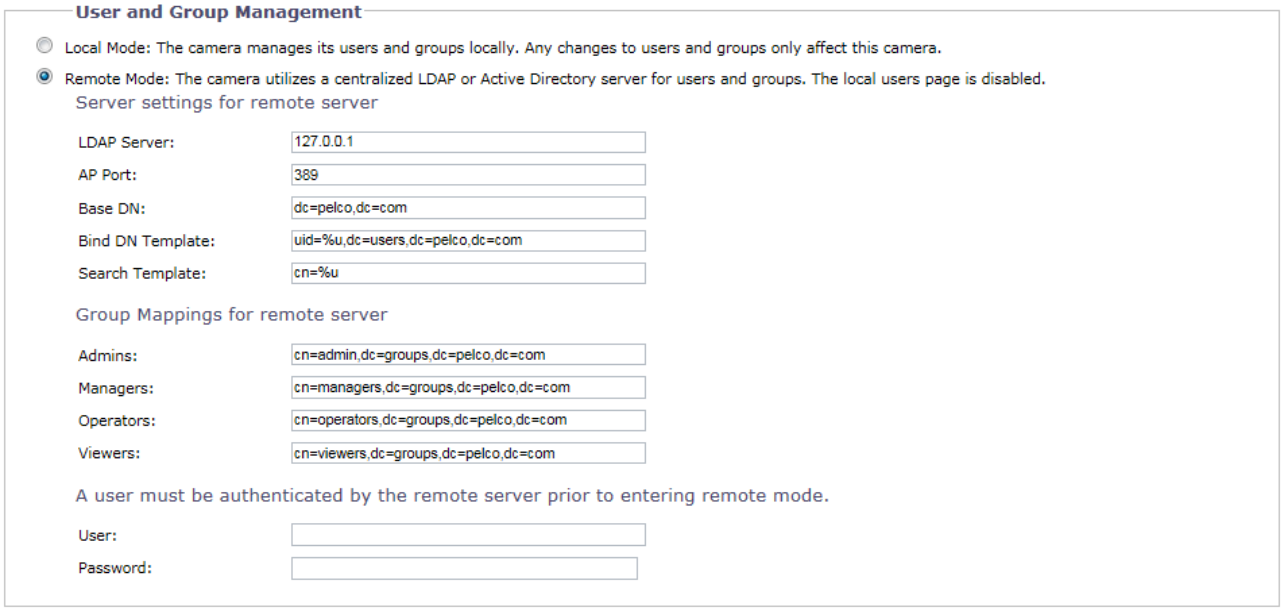


FIGURE 3-32: ENABLING REMOTE MODE

Select Remote Mode under User and Group Management.

1. **Server settings for remote server**
   a. Type the IP address or hostname of the LDAP server in the **LDAP Server** box.
   b. Type the port over which the camera will communicate with the LDAP server in the **AP Port** box. The default port for AP Communications is 389.
   c. Type the distinguished name (DN) that is the basis for LDAP searches in the **Base DN** box.
   d. Provide the template to format the username (provided when the user logs on to the camera) for searches in the LDAP directory in the **Bind DN Template** box.
   e. Provide the LDAP search query for users found in the base DN in the **Search Template** box. The search must match an entry in the LDAP user record to the bind name (username).

2. **Group Mappings for remote server**

   Input Group Mappings for each of the camera's four user groups:

   a. Input the common name (CN) and DN for the group of users to whom you want to grant admin access in the **Admins** box.

b Input the CN and DN for the group of users to whom you want to grant manager access in the **Managers** box.

c Input the CN and DN for the group of users to whom you want to grant operator access in the **Operators** box.

d Input the CN and DN for the group of users to whom you want to grant viewer access in the **Viewers** box.

3. **A user must be authenticated by the remote server prior to entering remote mode.**
   In the **User** and **Password** boxes, input the credentials of a user who can be authenticated through the LDAP server.

NOTE: Remote Mode (LDAP authentication) will not be enabled if you leave these fields blank or do not provide valid credentials; this ensures that you cannot lock yourself out of the camera with invalid or incorrect LDAP settings.

4. Click Save.

3.2.5.2 Users

User accounts are created to limit the permissions of individuals who are logged onto the camera. The Users page also includes four predefined access level settings that include Administrator, Manager, Operator, and Viewer permissions.

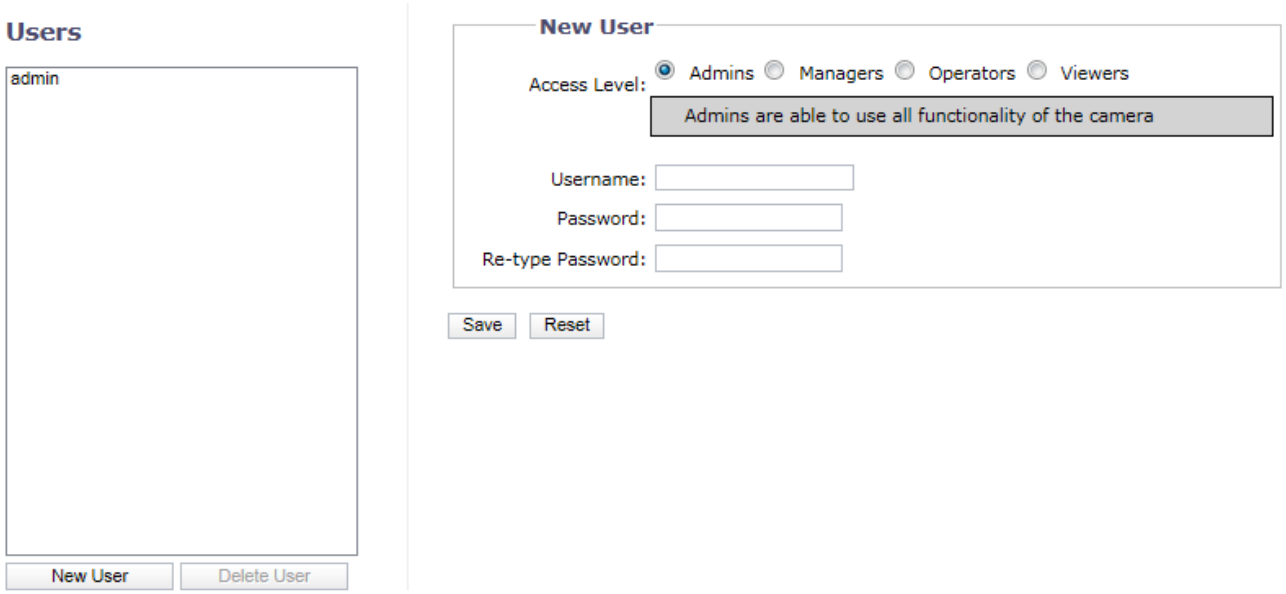


FIGURE 3-33: NEW USERS

Creating a New User

Click **New User** button below the left box and Select the Access Level for the new user.

- **Access Level**

1. Select the Access Level for the user.
   - **Admins:** This is the only defined group that cannot be deleted. This group has access to all permissions.
   - **Managers:** This defined group can be modified or deleted. This group has access to all permissions except the restore factory defaults, and API access permissions.
   - **Operators:** This defined group can be modified or deleted. The default permissions for this group are single stream view, stream selection, and multistream view.
   - **Viewers:** This defined group can be modified or deleted. The default permissions for this group are single stream view and multistream view.
2. Click the Save button to save the settings and create a new user. The new user profile appears in the box on the left side of the page. Click the Reset button to clear all of the information you entered without saving it.

- **Username**

  Click in the Username box and type a user name (2 to 23 alphanumeric characters). User names are not case-sensitive and are saved in lowercase characters.

- **Password**

  Click in the Password box and type a password (4 to 16 alphanumeric characters). Passwords are case-sensitive.

- **Re-type Password**

  Click in the Retype Password box and retype your password.

Click the Save button to save the settings and create a new user (the new user profile appears in the box on the left side of the page), or click the Reset button to clear all of the information you entered without saving it.

Deleting a User

1. Click the user profile that you want to delete from the defined users section located in the box on the left side of the page.
2. Click the Delete User button. A dialog box appears with the message “Are you sure you want to delete this user?”
3. Click OK. The user profile is deleted from the defined user profiles section.

NOTE: The “**admin**” user cannot be deleted.

3.2.6 Events

Use the Events tab to configure camera events and analytics.

Events are activated by user-defined event sources that tell the device how to react when an event occurs. Event handlers are the actions that the device takes when an event occurs. For example, a system source can be configured to send email to an operator if the system shuts-down and restarts.

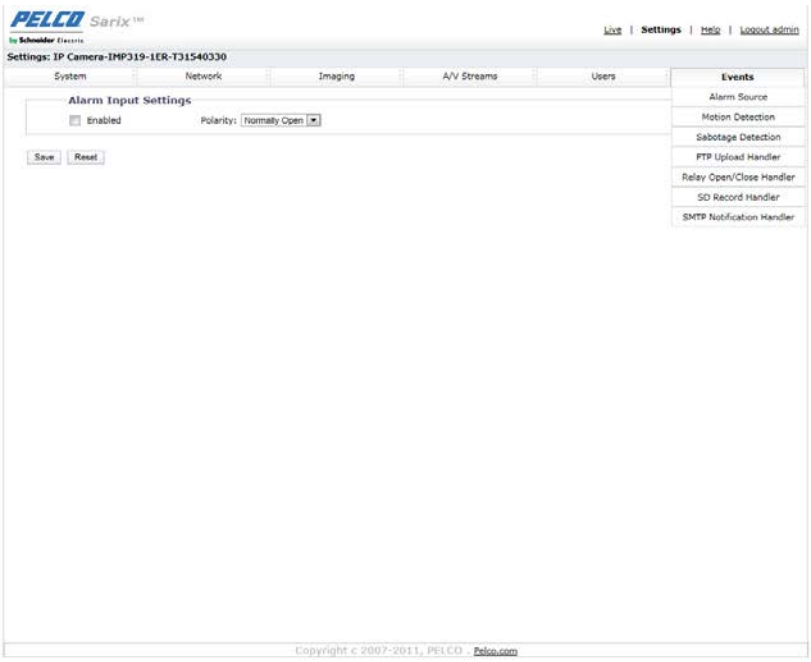


FIGURE 3-34: EVENTS SETTINGS

3.2.6.1 Alarm Source

The Alarm source is the camera input for an external signaling device, such as a door contact or motion detector. Both normally open and normally closed devices are supported.

FIGURE 3-35: ALARM SOURCE

Alarm Input Settings

1. Check **Enabled** button to enable **Alarm Input**.
2. Select either **Normally Open** or **Normally Closed** from the Polarity drop-down menu.
   - **Normally Open:** An alarm will be triggered when the external contact closes.
   - **Normally Closed:** An alarm will be triggered when the external contact opens.
3. Click the Save button to save the settings, or click the Reset button to clear all of the information you entered without saving it.

3.2.6.2 Motion Detection

This function is designed to record video once the unit detects a motion.

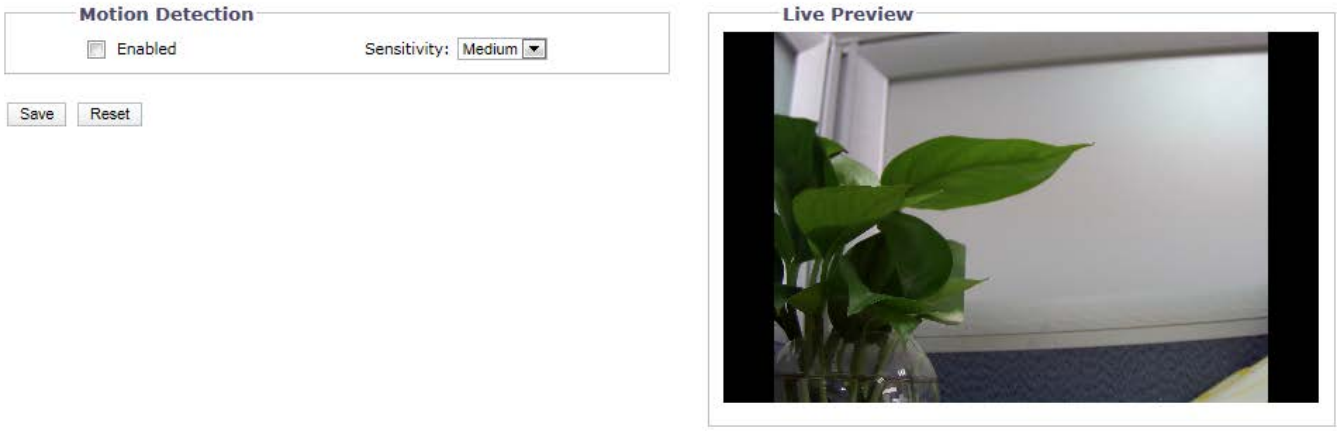


FIGURE 3-36: MOTION DETECTION SETTINGS

Motion Detection

1. Check **Enabled** button to enable **Motion Detection**.
2. **Sensitivity:** Choose different levels of sensitivity from **High**, **Medium**, and **Low**.
   - **High:** Motion is activated with slight changes in brightness or motion.
   - **Low:** Motion is activated with big changes in brightness or motion.
3. Set the desired area to trigger motion detection. The motion setup screen will be popped out for defining the detection area by dragging the mouse.

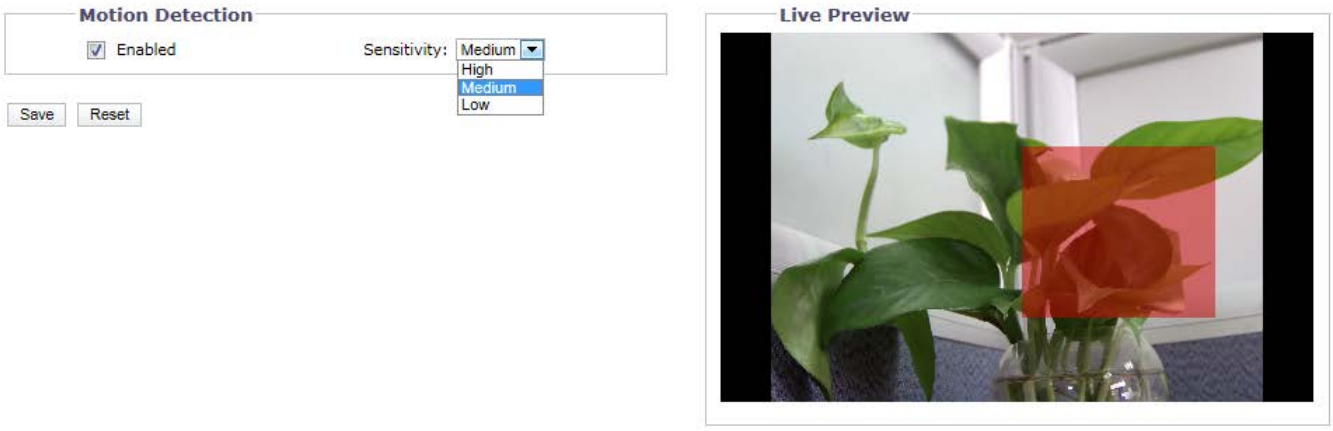


FIGURE 3-37: MOTION DETECTION ENABLED

4. Click the Save button to save the settings, or click the Reset button to clear all of the information you entered without saving it.

3.2.6.3 Sabotage Detection

The Camera Sabotage behavior detects scene changes or contrast changes in the field of view. An event or alarm is triggered if the lens is obstructed by spray paint, a cloth, or if it is covered with a lens cap. Any unauthorized repositioning of the camera also triggers an event or alarm.

FIGURE 3-38: SABOTAGE DETECTION

Scene Setup for Camera Sabotage

Install the camera in a high position, looking down on the scene. The field of view should be as large as possible. A small field of view could result in the view being blocked by an adjacent object.

Avoid scenes with a dark, uniform background; low lighting; and large moving objects.

Sabotage Detection

1. Check **Enabled** button to enable **Motion Detection**.
2. **Sensitivity:** Choose different levels of sensitivity from **High**, **Medium**, and **Low**.
   - **High:** Motion is activated with slight changes in the field of view.
   - **Low:** Motion is activated with big changes in the field of view.
3. Click the Save button to save the settings, or click the Reset button to clear all of the information you entered without saving it.

3.2.6.4 FTP Upload Handler

Users can save image files via FTP by setting FTP recording condition beforehand.

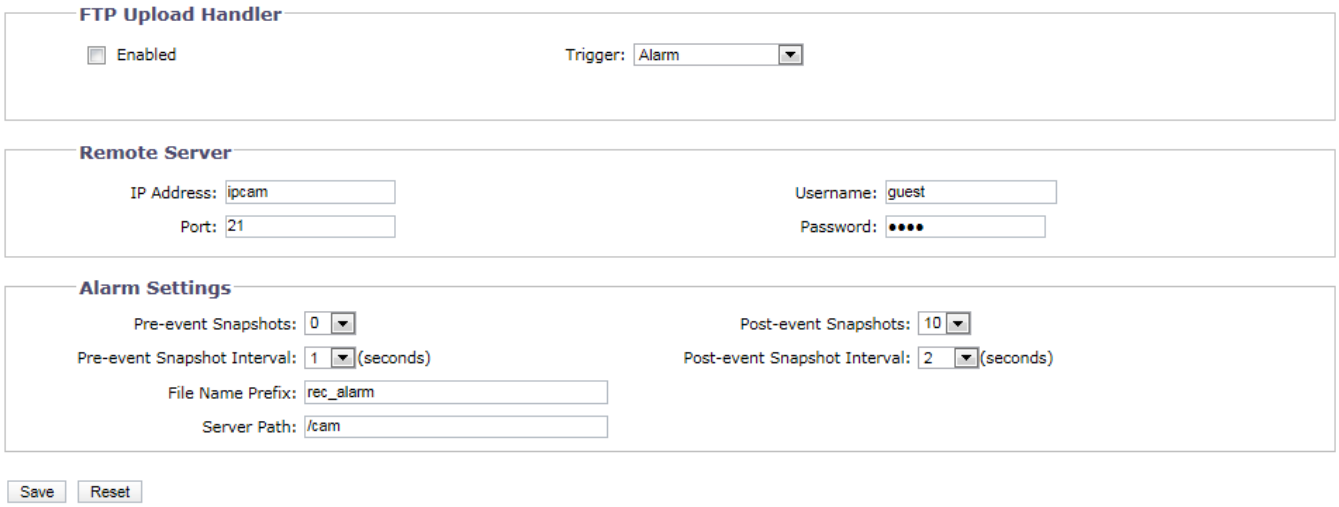


FIGURE 3-39: FTP UPLOAD HANDLER

FTP Upload Handler

You can store your image files base on the **Trigger** you've set.

1. Check **Enabled** button to enable **FTP Upload Handler**.
2. Select an event from the **Trigger** Drop-down menu and appears corresponding content under the **Remote Server**. Below are the Triggers configurations.
   - **Alarm:** Saves an image to a defined FTP server when **Alarm** event activated.

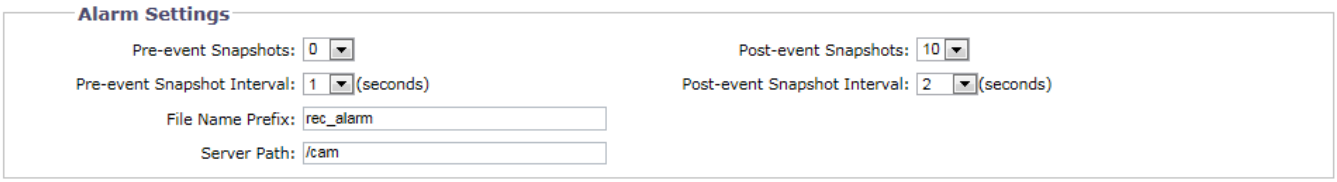


FIGURE 3-40: FTP UPLOAD HANDLER ALARM SETTINGS

   - **Motion Detection:** Saves an image to a defined FTP server when **Motion Detection** activated.

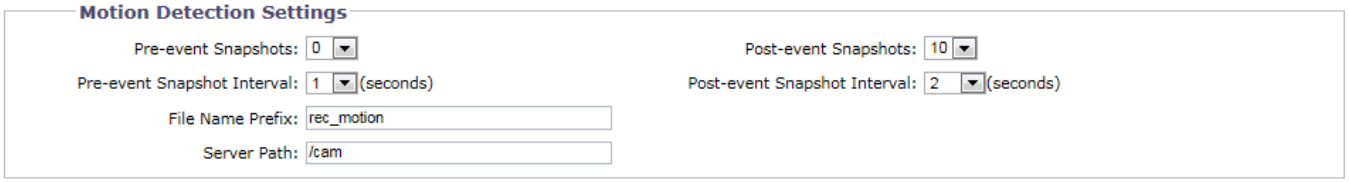


FIGURE 3-41: FTP UPLOAD HANDLER MOTION DETECTION SETTINGS

   - **Sabotage Detection:** Saves an image to a defined FTP server when **Sabotage Detection** activated.

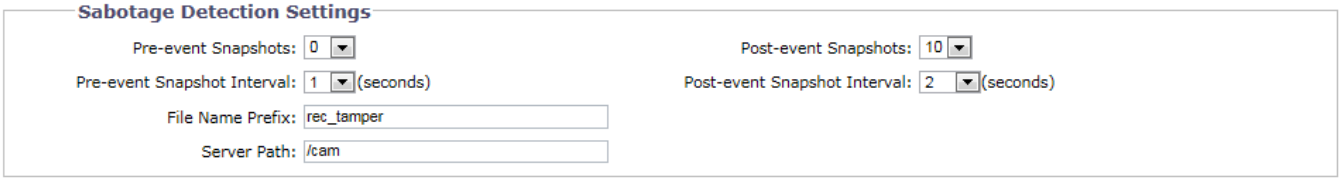


FIGURE 3-42: FTP UPLOAD HANDLER SABOTAGE DETECTION SETTINGS

- **Scheduled:** Saves an image to a defined FTP server when **Scheduled** event activated.

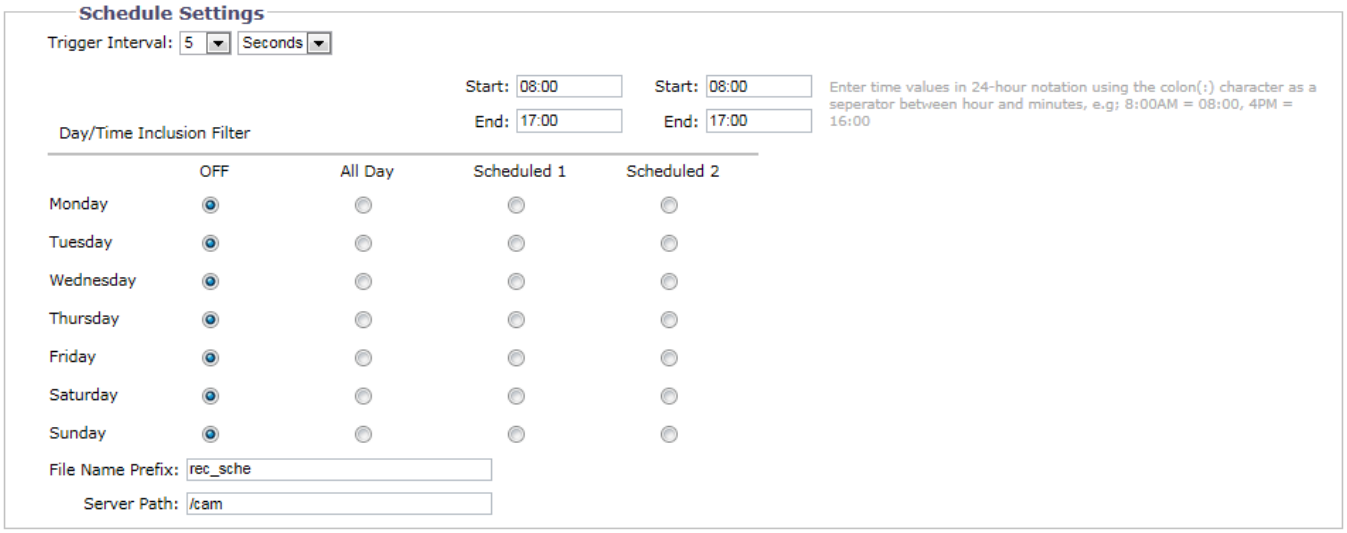


FIGURE 3-43: FTP UPLOAD HANDLER SCHEDULED SETTINGS

3. Click the Save button to save the settings, or click the Reset button to clear all of the information you entered without saving it.

Remote Server

Remote Server is used as a service component to transfer files by simply entering the IP address or hostname with the Login ID and password.

1. **IP Address:** Input a server name or address.
2. **Port:** Set "21" as default or change to dedicated number.
3. **Username:** Input a user name with privilege to access the server.
4. **Password:** Input the password associated with Username.

NOTE: The default **Username** and **Password** are "**guest**" and "**1234**".

Alarm Settings

1. Set **Pre-event Snapshots**, **Post-event Snapshots**, **Pre-event Snapshot Interval**, **Post-event Snapshot Interval**, **File Name Prefix**, and **Server Path** for **Alarm, Motion Detection, and Sabotage Detection**.
2. Set **Trigger Interval** time and determine the recording condition: **OFF**, **All Day**, **Schedule 1**, or **Schedule 2** from scheduled table during 24/7 for **Scheduled Trigger.**
3. Set the **Server Path** where the data is to be stored on the server.
4. Click the Save button to save the settings, or click the Reset button to clear all of the information you entered without saving it.

3.2.6.5 Relay Open/Close Handler

Send a signal to an external device when an alarm or relay is triggered.

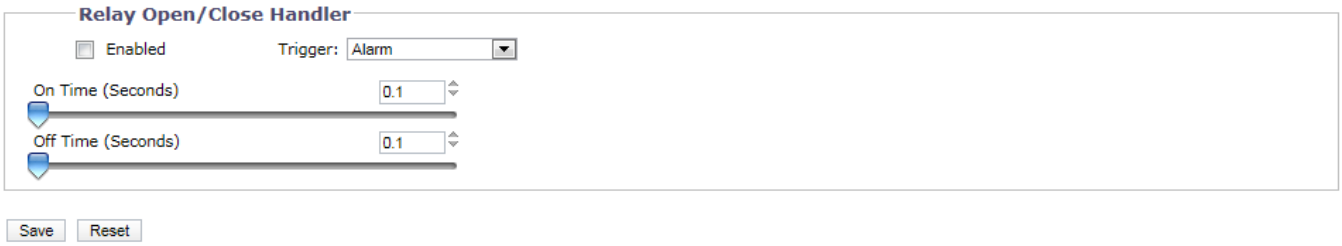


FIGURE 3-44: RELAY OPEN/CLOSE HANDLER SETTINGS

Relay Open/Close Handler

1. Check **Enabled** button to enable **Relay Open/Close Handler**.
2. Select the **Alarm**, **Motion Detection** or **Sabotage Detection** from the **Trigger** drop-down menu.
3. Move the **On Time** slider to set the amount of time that the relay will remain open. The time range is 0.1 to 200 seconds; the default setting is 0.1.
4. Move the **Off Time** slider to set the amount of time that the relay will remain closed. The time range is 0.1 to 200 seconds; the default setting is 0.1.
5. Click the Save button to save the settings, or click the Reset button to clear all of the information you entered without saving it.

3.2.6.6 SD Record Handler

Save video clips of the activated event to an SD card. Before use this function, an SD card must be installed in the device.

NOTE: The SD card must be formatted as FAT32. Other formats are not compatible with the camera.

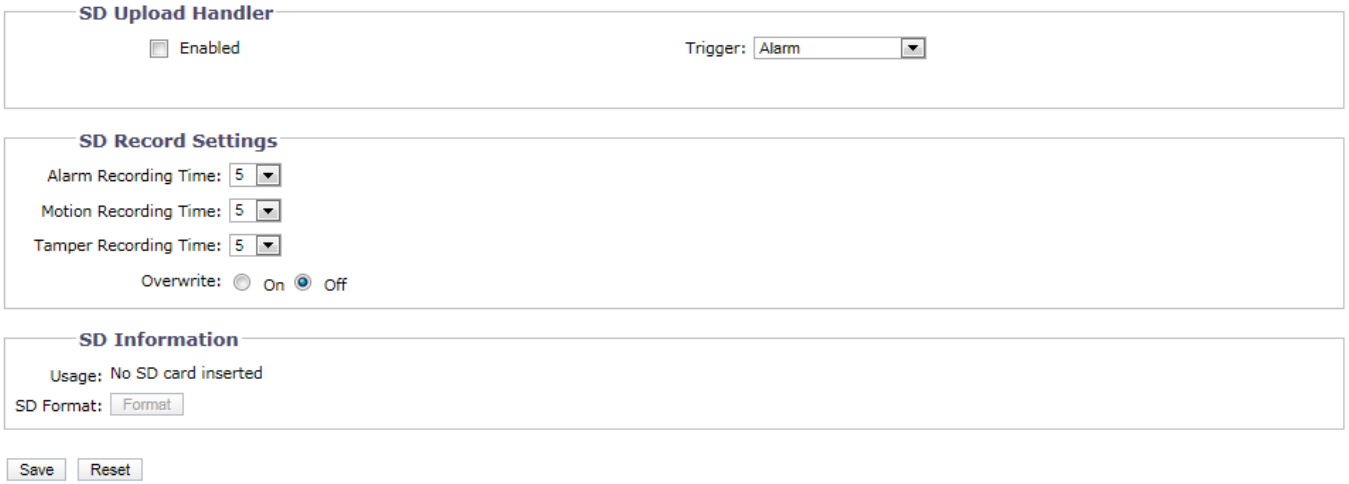


FIGURE 3-45: SD RECORD HANDLER SETTINGS

1. Check **Enabled** button to enable **SD Upload Handler**.
2. Select the **Alarm**, **Motion Detection**, Network Loss or **Sabotage Detection** from the **Trigger** drop-down menu.
3. Set a time interval for **Alarm Recording**, **Motion Recording**, and **Tamper Recording**.
4. Set overwrite **ON** or **Off** to enable or disable the SD card to be **overwritten** automatically when the SD card is full of recordings.

5. **Usage**: Information of SD card usage.
6. **SD Format:** Click Format to erase information off of the SD card.
7. Click the Save button to save the settings, or click the Reset button to clear all of the information you entered without saving it.

Format SD card as FAT32

1. Double click **guiformat.exe, the FAT32 Format** window will pop up as the figure shows below.
2. Select the hard disk/SD card you want to format as FAT32 from the **Drive** drop-down menus, and then click **Start** button to begin format the hard disk/SD card.

   NOTE: Format will erase all information off of the hard disk/SD card. Make sure you have any important files backed up before you format it.

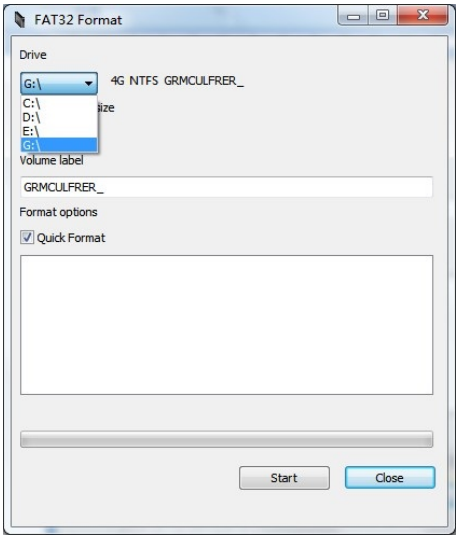


FIGURE 3-46: FAT32 FORMAT

3. When the progress bar is full, click **Close** to complete format and exit the format window.

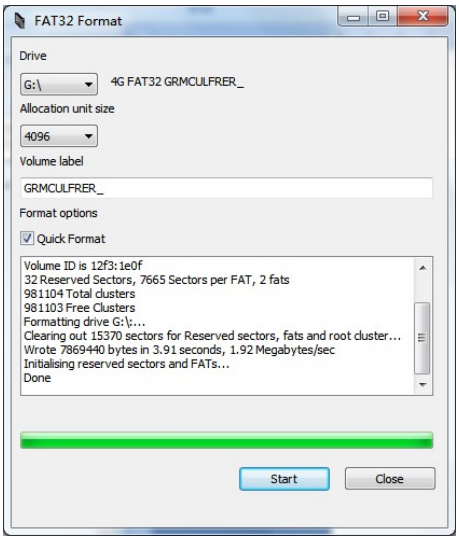


FIGURE 3-47: FAT32 FORMAT COMPLETE

3.2.6.7 SMTP Notification Handler

Set SMTP Notification Handler function and send an email to a defined email address when an event is activated.

NOTE: To use email notification, the camera must be connected to a local area network (LAN) that maintains an SMTP mail server. Consult your network administrator for information on configuring email notification on your local network.

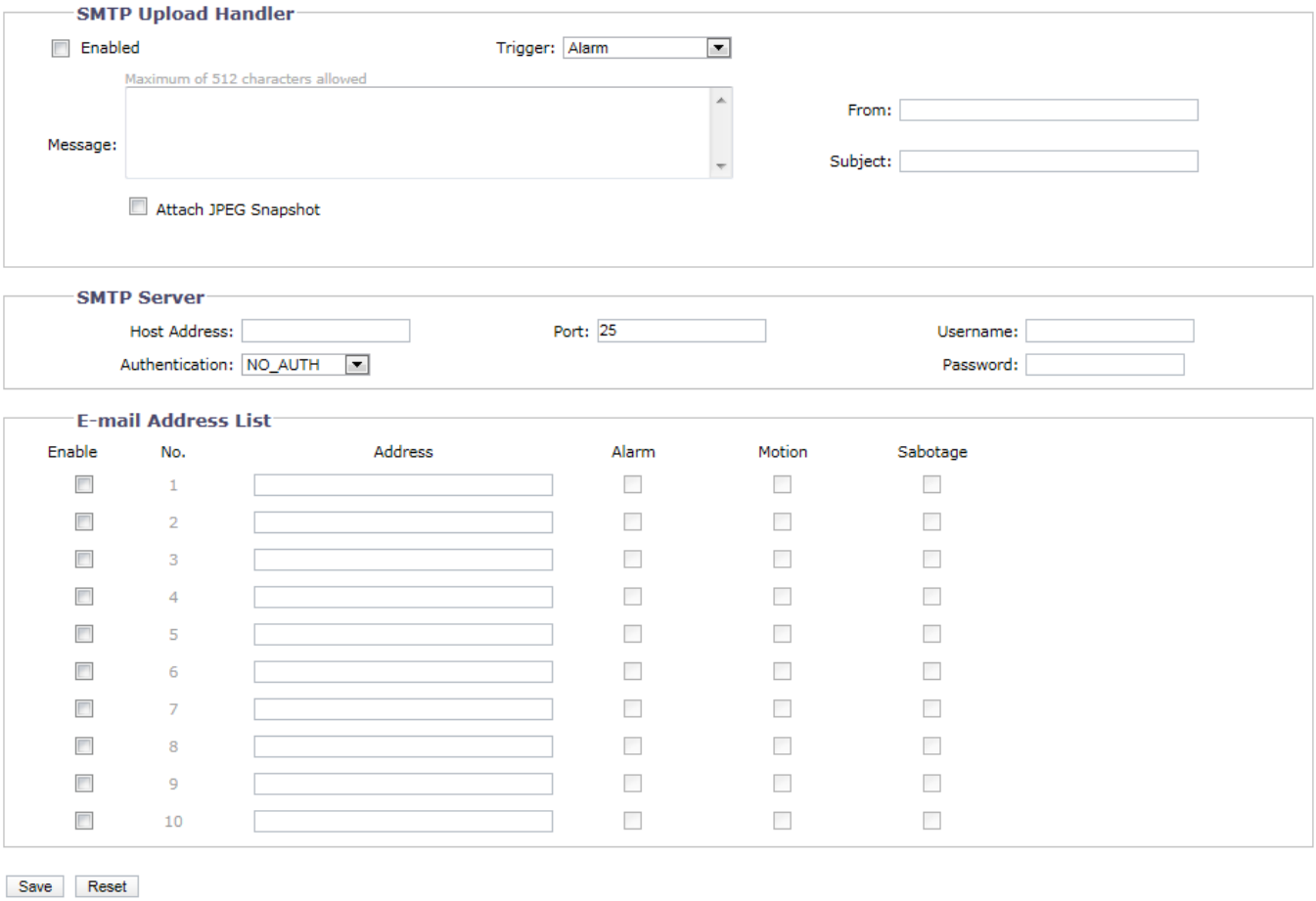


FIGURE 3-48: SMTP NOTIFICATION HANDLER SETTINGS

SMTP Upload Handler

1. Check **Enabled** button to enable **SMTP Upload Handler**.
2. Select the **Alarm**, **Motion Detection**, or **Sabotage Detection** from the **Trigger** drop-down menu.
   If choose **Alarm**, **Alarm** in event settings should be checked **Enabled**; if **Motion Detection**, **Motion Detection** in event settings should be checked **Enabled**; if **Sabotage Detection**, **Sabotage Detection** in event settings should be checked **Enabled** as pictures below.

FIGURE 3-49: ALARM ENABLED

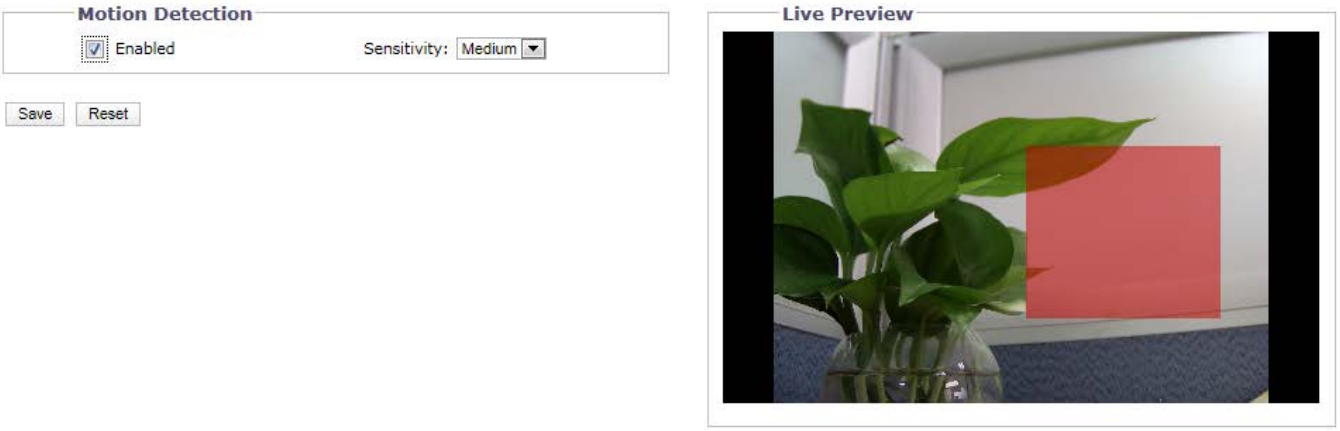


FIGURE 3-50: MOTION DETECTION ENABLED

FIGURE 3-51: SABOTAGE DETECTION ENABLED

3. Click in the text boxes (**Message**, **From**, and **Subject**), and then type the necessary information in each text box.
4. Select the **Attach JPEG Snapshot** box if you want to send a JPEG as an attachment.
5. Continue set the **SMTP Server** and **E-mail Address List**.

SMTP Server

Simple Mail Transfer Protocol (SMTP) is an Internet standard for electronic mail (e-mail) service across Internet Networking.

1. **Host Address:** Input a server name or address.
2. **Port:** set “25” as default or change to dedicated number.
3. **Username:** Input a user name with privilege to access the server.
4. **Password:** Input the password associated with Login ID.
5. **Authentication:** Select an authentication type.
   - **NO_AUTH:** Namely No Authentication, means no restriction.
   - **SMTP_PLAIN:** PLAIN is the name of a registered SASL authentication mechanism which serves as a parameter to the AUTH command. The PLAIN authentication mechanism is described in RFC 2595. PLAIN is the least secure of all the SASL authentication mechanisms since the password is sent unencrypted across the network.
   - **LOGIN:** The LOGIN mechanism is supported by Microsoft's Outlook Express as well as by some other clients.
   - **TLS_TTLS:** TLS is usually implemented on top of any of the Transport Layer protocols encapsulating the application-specific protocols such as HTTP, FTP, SMTP, NNTP and XMPP. The TLS protocol allows client-server applications to communicate across a network in a way designed to prevent eavesdropping and tampering. TLS can also be used to tunnel an entire network stack to create a VPN as is the case with OpenVPN.
6. Continue set the **E-mail Address List**.

E-mail Address List

This function is designed to notify multiple users via email when **Trigger** is set.

1. Check **Enable** and input the E-mail **Address** accordingly.
2. Select **Alarm**, **Motion** or **Sabotage** for sending E-mail.
3. Click the Save button to save the settings, or click the Reset button to clear all of the information you entered without saving it.

Specifications

CAMERA

Imaging Device

MPx	Sensor	Maximum Resolution
5 MPx	1/3.2-inch	2592 x 1944 (5.0 MPx)
3 MPx	1/3-inch	2048 x 1536 (3.1 MPx)
2 MPx	1/3-inch	1920 x 1080 (2.1 MPx)
1 MPx	1/4-inch	1280 x 720 (0.9 MPx)
SD	1/4-inch	800 x 600 (0.5 MPx)

Imager Type: CMOS

Imager Readout: Progressive scan

Electronic Shutter Range: 1/5 ~ 1/10,000 sec

Dynamic Range: 65 dB

White Balance Range: 2,500° to 8,000°K

Digital Noise Reduction: Yes (ON/OFF selectable)

Minimum Illumination

MPx	Sensitivity	Color		Mono- with IR Illumination	
		33 ms	200 ms	33 ms	200 ms
5 MPx	f/1.2	0.30 lux	0.02 lux	0.00 lux	0.00 lux
3 MPx	f/1.2	0.30 lux	0.02 lux	0.00 lux	0.00 lux
2 MPx	f/1.2	0.30 lux	0.02 lux	0.00 lux	0.00 lux
1 MPx	f/1.4	0.30 lux	0.02 lux	0.00 lux	0.00 lux
SD	f/1.4	0.30 lux	0.02 lux	0.00 lux	0.00 lux

Mechanical IR Cut Filter: Yes (AUTO/MANUAL selectable), with different set points on lux

IR Illumination: Adaptive IR up to 15 m; auto ON in night mode, or OFF

Lens: 2.8 to 10 mm or 3 to 9 mm remote zoom with DC iris

Focus: Autofocus

VIDEO

Video Streams: Up to 2 simultaneous streams, plus service stream; the secondary stream is variable based on the setup of the primary stream

Video Overlay: Camera name, time, date

Available Resolutions

MPx	Width	Height	Aspect Ratio
5.0	2592	1944	4:3
3.1	2048	1536	4:3
2.1	1920	1080	16:9
1.9	1600	1200	4:3
1.2	1280	960	4:3
0.9	1280	720	16:9
0.6	1024	576	16:9
0.5	800	600	4:3
0.3	640	480	4:3
0.1	320	240	4:3
0.1	320	180	16:9

Frame Rates

MPx	Images Per Second (ips)
5 MPx	12 (full), 10, 5, 1
3 MPx	20 (full), 16.67, 15, 12.5, 10, 5, 1
2 MPx	30 (full), 25, 20, 16.67, 15, 12.5, 10, 5, 1
1 MPx	30 (full), 25, 20, 16.67, 15, 12.5, 10, 5, 1
SD	30 (full), 25, 20, 16.67, 15, 12.5, 10, 5, 1

Note: Available frame rates are selectable for each independent stream depending on the coding, resolution, and stream configuration.

Video Encoding: H.264 high or main profiles; and MJPEG

Bit Rate Control: Constant bit rate (CBR), variable bit rate (VBR) with target range

Service Stream: 320 x 240 (0.1 MPx) or 320 x 180; 2 ips, MJPEG

Snapshot: JPEG capture at resolution of live view stream

Window Blanking: 4 configurable windows

ELECTRICAL

Network Port	RJ-45 connector for 100Base-TX
Power Input	PoE (IEEE 802.3af, Class 3) 24 VAC nominal, 18 to 32 VAC range
Power Consumption	<10.50 W
Local Storage	Up to 32 GB on Micro SDHC or SDXC card
Alarm	
Input	1
Output	1; PhotoMOS™ relay (30 V, 1 A)
Triggers	Unsupervised mode that detects switch closures (N.O. and N.C.)

ENVIRONMENTAL

Operating Temperature	–40° to 50°C (–40° to 122°F)*
Storage Temperature	–40° to 60°C (–40° to 140°F)
Operating Humidity	15% to 85%, RH noncondensing

*Thermostatically controlled heating provides ramped heating control between the initial heater on at 15°C (59°F) and full heating mode at –40°C (–40°F).

AUDIO

Streaming	Dual-channel
Input	Line in/terminal block
Output	Line out/terminal block
Encoding	G.711 A-law/G.711 U-law

GENERAL

Construction	Die-cast aluminum; polycarbonate bubble
Ingress Protection	IP66 per IEC 60529
Vandal Resistance	IK10 (20J impact) per IEC 62262
Finish	Light gray, RAL 7047; satin texture
Pan/Tilt Adjustment	Manual
Pan	355°
Tilt	75°
Rotate	360°
Weight	0.86 kg (1.90 lb)
Shipping Weight	1.07 kg (2.36 lb)

NETWORK

Supported Protocols	TCP/IP, UDP, ICMP, IPv4, SNMP v2c/v3, HTTP, HTTPS, SSL, SSH, SMTP, FTP, RTSP, UPnP, DNS, NTP, RTP, RTCP, LDAP
Users	
Unicast	1 administrator, up to 4 viewers
Multicast	Unlimited users H.264
Security Access	Multiple user access levels with password protection

INTEGRATION

Video Management	Digital Sentry 7.3 (or later); Endura 2.0 (or later); Third-party VMS through Pelco API 1.0 and ONVIF Profile S
Mobile Application	Integrated to Pelco Mobile App
Analytics	Simple motion detection and camera sabotage
Local Storage	Capture 5- or 10-second video clips on camera sabotage, motion detection, or alarm input; record video continuously in the case of network outage with option to overwrite; access video through FTP protocol
Camera Discovery and Firmware	Cameras discovered and firmware upgraded through Pelco Device Utility 2 version 2.2; cameras discovered and firmware upgrade through Endura Utilities
Web Browser Support	Microsoft® Internet Explorer® 8.0 and later

CERTIFICATIONS†

- CE - EN 55022 (Class A), EN 50130-4, EN 60950-1
- FCC (Class A) - 47 CFR Part 15
- UL and cUL Listed - UL 60950-1, CAN/CSA-C22.2 No. 60950-1-07
- ICES-003
- KCC
- NOM

† At the time of this publication, certifications are pending. Please consult the factory, our Web site (*www.pelco.com*), or the most recent B.O.S.S.® update for the current status of certifications.

MODELS

Type	Resolution	Lens	Model Number with Mount
In-Ceiling	5 MPx	3 to 9 mm	IMP519-1ERI
	3 MPx	3 to 9 mm	IMP319-1ERI
	2 MPx	3 to 9 mm	IMP219-1ERI
	1 MPx	2.8 to 10 mm	IMP1110-1ERI
	SD	2.8 to 10 mm	IMPS110-1ERI
Surface Mount	5 MPx	3 to 9 mm	IMP519-1ERS
	3 MPx	3 to 9 mm	IMP319-1ERS
	2 MPx	3 to 9 mm	IMP219-1ERS
	1 MPx	2.8 to 10 mm	IMP1110-1ERS
	SD	2.8 to 10 mm	IMPS110-1ERS
Pendant	5 MPx	3 to 9 mm	IMP519-1ERP
	3 MPx	3 to 9 mm	IMP319-1ERP
	2 MPx	3 to 9 mm	IMP219-1ERP
	1 MPx	2.8 to 10 mm	IMP1110-1ERP
	SD	2.8 to 10 mm	IMPS110-1ERP

RECOMMENDED MOUNTS

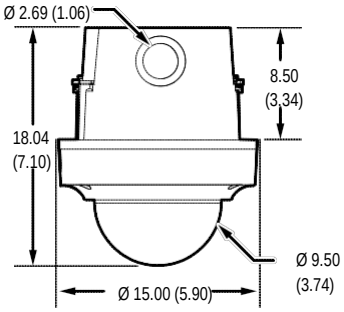
WMVE-SR — Wall mount, light gray; for use with the environmental pendant mount option

OPTIONAL ACCESSORIES

IPCT01 — Pelco IP camera tester*

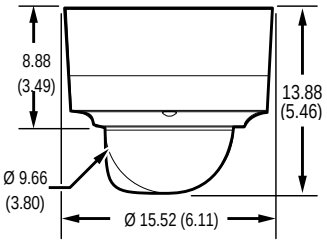
* Contact Pelco Product Support for more information about the use of the Pelco IP camera tester with cameras.

VALUES IN PARENTHESES ARE INCHES; ALL OTHERS ARE CENTIMETERS.



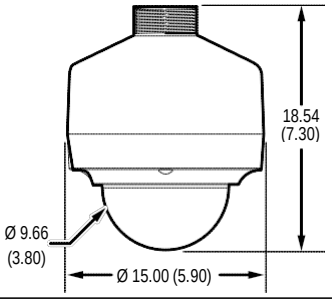
Environmental, In-Ceiling

- Clearance Above Ceiling 4 in.
- Maximum Ceiling Thickness 1.5 in.
- 3/4-Inch NPT or 25 mm Conduit Attachments On Back Box
- IP66 Ingress Protection
- IK10 (20J) Impact Resistance
- Plenum Rated Back Box



Environmental, Surface Mount

- Attaches to Standard 4-Inch Square Outlet Box and Standard 2-Gang Electrical Box
- 3/4-Inch NPT or 25 mm Conduit Attachments On Side and Top of Back Box
- IP66 Ingress Protection
- IK10 (20J) Impact Resistance



Environmental, Pendant

- 1.5-Inch NPT Thread for Use With Pelco Wall Mounts
- IP66 Ingress Protection
- IK10 (20J) Impact Resistance

Pelco Troubleshooting Contact Information

If the instructions provided fail to solve your problem, contact Pelco Product Support at 1-800-289-9100 (USA and Canada) or +1-559-292-1981 (international) for assistance. Be sure to have the serial number available when calling.

Do not try to repair the unit yourself. Leave maintenance and repairs to qualified technical personnel only.

Note for Dimension Drawings

NOTE: VALUES IN PARENTHESES ARE INCHES; ALL OTHERS ARE CENTIMETERS.

This equipment contains electrical or electronic components that must be recycled properly to comply with Directive 2002/96/EC of the European Union regarding the disposal of waste electrical and electronic equipment (WEEE). Contact your local dealer for procedures for recycling this equipment.

WARRANTY STATEMENT

For information about Pelco's product warranty and thereto related information, refer to www.pelco.com/warranty.

Pelco by Schneider Electric 3500 Pelco Way Clovis, California 93612-5699 United States
USA & Canada Tel (800) 289-9100 Fax (800) 289-9150
International Tel +1 (559) 292-1981 Fax +1 (559) 348-1120
www.pelco.com www.pelco.com/community