Sarix® Professional IWP Series Rugged Environmental Wedge Dome

User Manual

IWP121-1ES IWP221-1ES

C2298M-A-EN (10/20)

Contents

Important Notices Statement 5

Warranty Statement ..... **Error! Bookmark not defined.**

Preface 6

1. Product Overview 7

1.1 Dimensions 7

1.2 Models Introduction 8

1.3 Physical Characteristics 9

2. Installation and Connection 10

2.1 Unpacking Everything 10

2.2 Optional Accessories 10

2.3 Installation 10

2.3.1 Checking Appearance 10

2.3.2 Connecting the Wires 10

2.3.3 Disassembling the Camera 11

2.3.4 Installing the Camera 12

2.3.5 Adjusting the Camera Position 15

2.3.6 Sticking Desiccant 15

2.3.7 Completing the Installation 16

2.3.8 Network Topology 16

2.3.9 System Requirements 17

2.4 Connection 18

2.4.1 Default IP address 18

2.4.2 Connecting From a Computer & Viewing Preparation 18

3. Administration and Configuration 20

3.1 Live 20

3.2 Settings 21

3.2.1 System 22

3.2.2 Network 25
3.2.3 Imaging 36
3.2.4 A/V Streams 42
3.2.5 Users 47
3.2.6 Events 50
Pelco Troubleshooting Contact Information 60

Important Notices Statement

For information about Pelco's product-specific important notices and thereto related information, refer to *www.pelco.com/legal*.

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.

CAN ICES-3(A)/NMB-3(A)

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 .

Warranty Statement

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

UL SAFETY NOTICES

The product shall be installed by a qualified service person and the installation shall conform to all local codes.

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 following information:

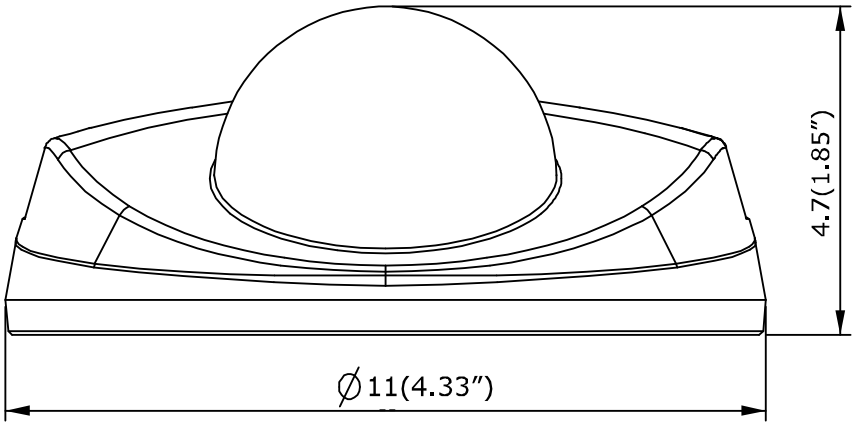
- **Product Overview:** The main functions and system requirements of the unit.
- **Installation and Connection:** Instructions on unit installation and wire connections.
- **Administration and Configuration**: The main menu navigation and controls explanations.

1. Product Overview

1.1 Dimensions

The dimension of the Sarix® Professional Series Rugged Environmental Wedge Dome camera is shown in the Figure 1-1 below.

VALUES IN PARENTHESES ARE INCHES; ALL OTHERS ARE CENTIMETERS.



RUGGED ENVIRONMENTAL WEDGE DOME

FIGURE 1-1: PHYSICAL DIMENSIONS

1.2 Models Introduction

The physical appearances and installation methods for the models indicated within the list below are, by and large, the same. Therefore, please use this manual where we use the example from IWP221-1ES as a reference to apply to all the models.

Model	Description
IWP121-1ES	1MP Rugged Environmental Wedge Dome Camera
IWP221-1ES	2MP Rugged Environmental Wedge Dome Camera

TABLE 1-1: MODELS LIST

1.3 Physical Characteristics

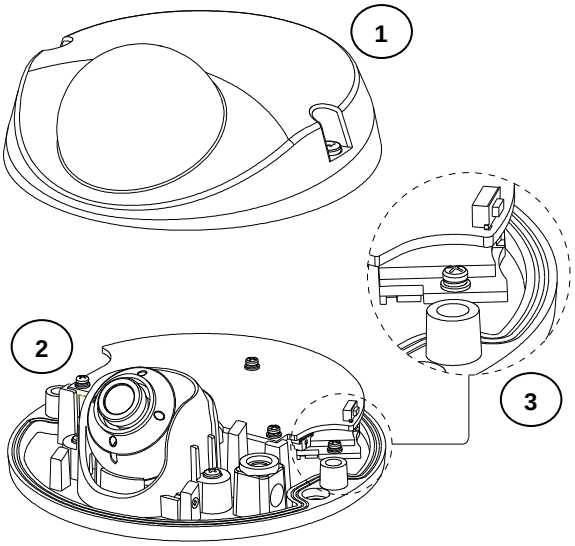


FIGURE 1-2: CAMERA CONNECTIONS AND FEATURES 1/3

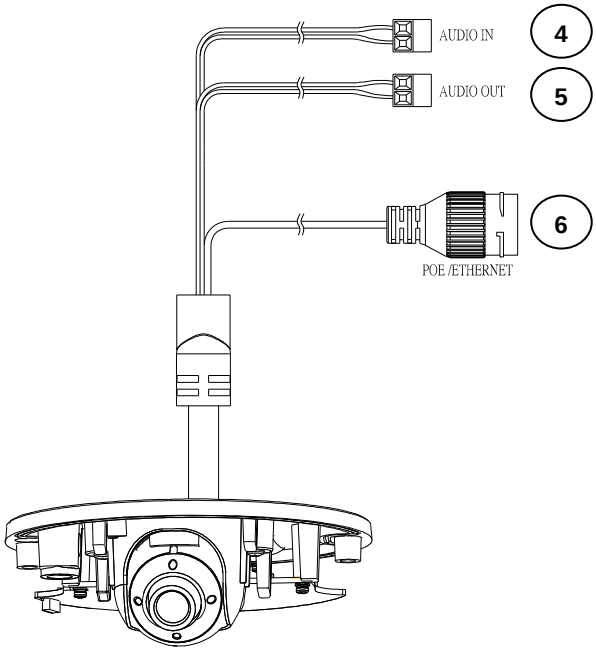


FIGURE 1-3: CAMERA CONNECTIONS AND FEATURES 2/3

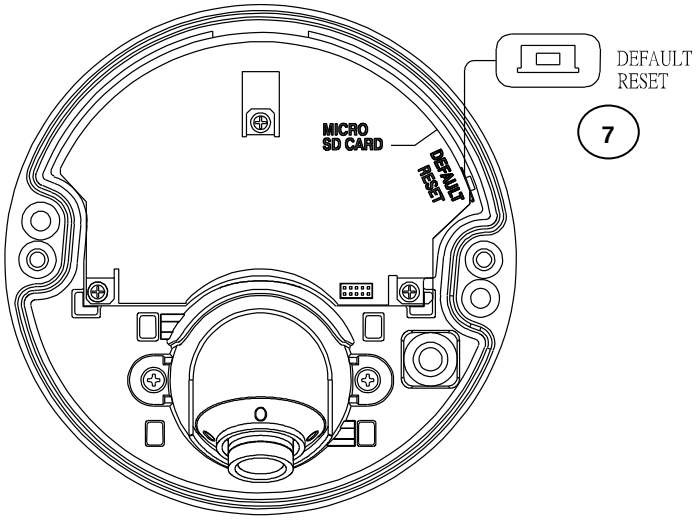


FIGURE 1-4: CAMERA CONNECTIONS AND FEATURES 3/3

1. **Dome Cover:** The upper dome cover of the camera.
2. **Camera Body:** The physical main body of the camera.
3. **Micro SD Card Slot:** The slot is for inserting micro SD card for file storage.
4. **Audio In:** Connect to an external microphone. White port: Audio in; Black port: GND.
5. **Audio Out:** Connect to a speaker. Red port: Audio out; Black port: GND.
6. **RJ-45 Network Port:** Connect the RJ-45 connector to this port with a PoE compatible network device that supplied power through the Ethernet cable.
7. **Default & Reset Button:**
   - **Default:** Press the button for 6 seconds to restore the camera's settings back to the factory default.
   - **Reset:** Press the button for below 1 second to reboot the camera.

2. Installation and Connection

2.1 Unpacking Everything

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

- Fixed Flat Dome Camera * 1
- Plastic Anchor * 2
- Flat Head Screw (Tapping Type) * 2
- Security Torx Wrench * 1
- Mounting Template * 1
- Printed Quick Installation Guide * 1
- Desiccant * 1

Please contact your dealer if any items are missing.

2.2 Optional Accessories

- IMPEBAP: a Sarix 4S electrical box adaptor for Wedge Dome
- IMPPMB-1I: a Sarix L-shape wall bracket mount for Wedge 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 Connecting the Wires

- Connect the PoE (IEEE 802.3af Class 0) port with a RJ-45 jack that links a PoE compatible network device that supplied power with networking capability through the Ethernet cable.
- Insert audio input/output cables to the connectors of unit if required.

  NOTE: To avoid the length deficiency, it's suggested 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.

2.3.3 Disassembling the Camera

1. Loosen the 2 screws on the cover by the supplied torx wrench.
2. Remove the dome cover gently.
3. Insert the optional micro SD card for file storage if necessary.

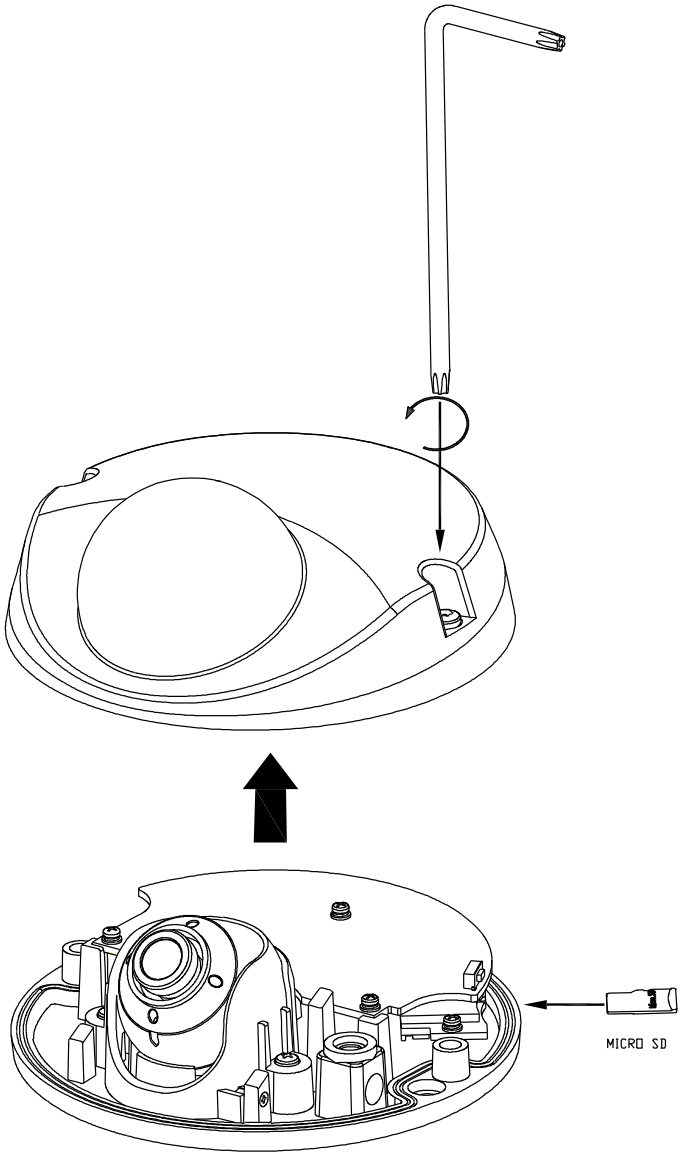
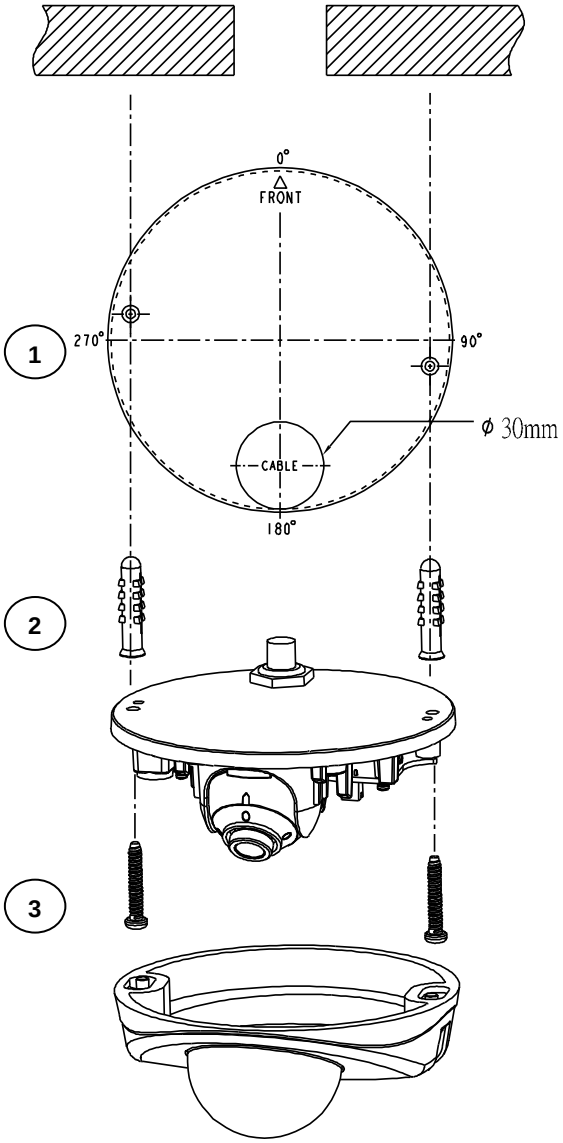


FIGURE 2 - 1: DISASSEMBLING THE CAMERA

2.3.4 Installing the Camera

2.3.4.1 Surface Installation - Ceiling or Wall

1. Attach the mounting template to the wall or ceiling.
2. Drill two holes indicated on the mounting surface and insert the plastic anchors into the holes.
3. Drill another hole with Ø30mm in diameter as indicated on the mounting template in the wall or ceiling and pass all the signal cables through the hole.
4. Secure the camera body to the wall or ceiling with the 2 flat head screws (tapping type).



1. Mounting Template
2. Plastic Anchors x 2
3. Flat Head Screws (Tapping Type) x 2

FIGURE 2 - 2: INSTALLING THE CAMERA

2.3.4.2 Surface Mount with IMPEBAP

You can mount the camera to a surface with **IMPEBAP**, a Sarix 4S electrical box adaptor mount for Wedge Dome. Refer to the figures below for surface installation with **IMPEBAP**.

1. Fix the adaptor plate to the surface embedded with 4S electrical box with 2 screws. Note the hole pattern with “4” indicators that represent the exact holes for 4S installation on the adaptor for proper mounting.
2. Pass all the cable thread from camera body into the adaptor plate and surface followed by wiring them if necessary. Fasten the camera body onto the adaptor plate with 2 screws. Note the hole pattern with “W” indicators that represent the exact holes for Wedge Dome installation on the adaptor for proper mounting.
3. Attach the dome cover to the camera body that was fixed with the adaptor plate already, and tightly secure the 2 screws of dome cover by torx wrench.
4. The Wedge Dome is eventually properly mounted on the surface with **IMPEBAP**.

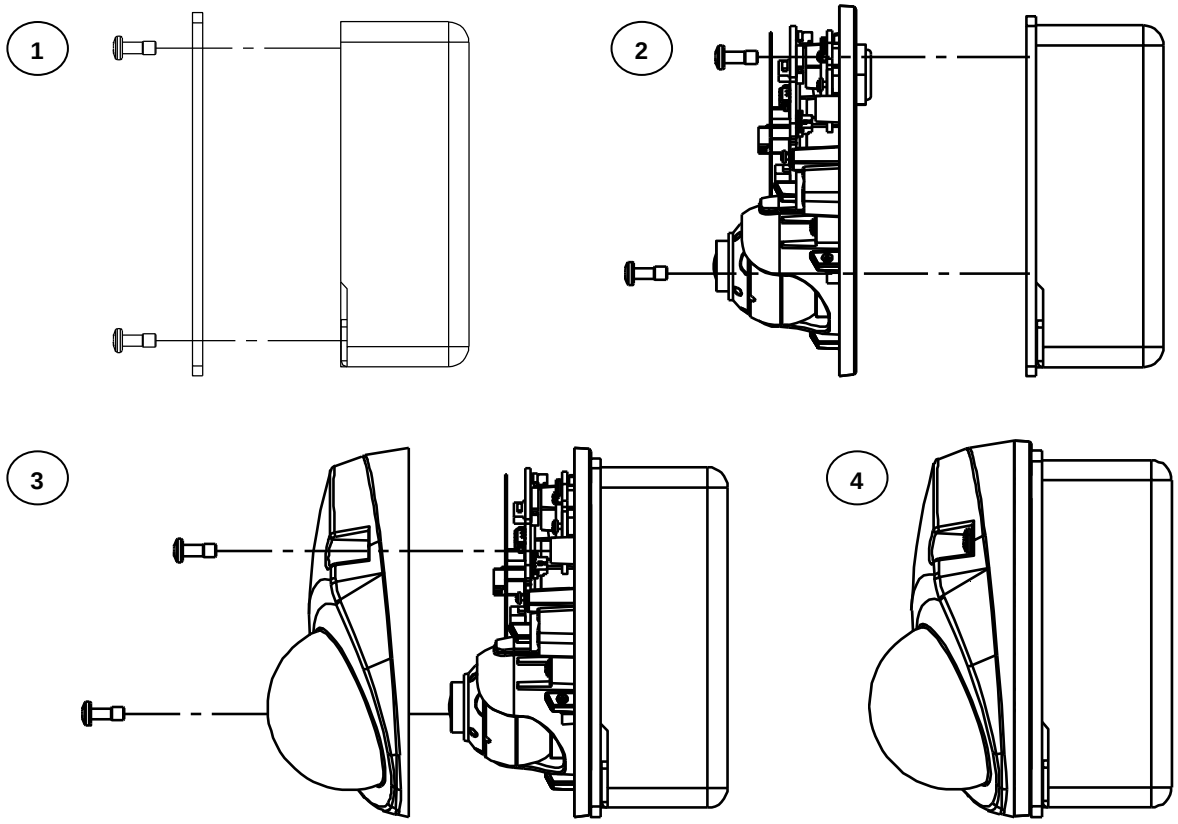


FIGURE 2-3: SURFACE MOUNT WITH IMPEBAP

2.3.4.3 Wall Mount with IMPPMB-1I

Wall mount with **IMPPMB-1I** requires both the L-shape bracket and the adaptor plate from **IMPEBAP**. Refer to the figures below for detailed process for Wall Mount with **IMPPMB-1I**.

1. Fasten the L-shape bracket onto the desired wall with 4 screws.
2. Further fix the adaptor plate from **IMPEBAP** onto the L-shape bracket with 2 screws. Note the hole pattern with "L" indicators that represent the exact holes for L-shape bracket assembly on the adaptor for proper installation.
3. Pass all the cable thread from camera body into the adaptor plate and L-shape bracket followed by wiring them if necessary. Fasten the camera body onto the adaptor plate with 2 screws. Note the hole pattern with "W" indicators that represent the exact holes for Wedge Dome installation on the adaptor for proper mounting.
4. Attach the dome cover to the camera body that was fixed with the adaptor plate already, and tightly secure the 2 screws of dome cover by torx wrench.
5. The Wedge Dome is eventually properly mounted on the wall with **IMPPMB-1I**.

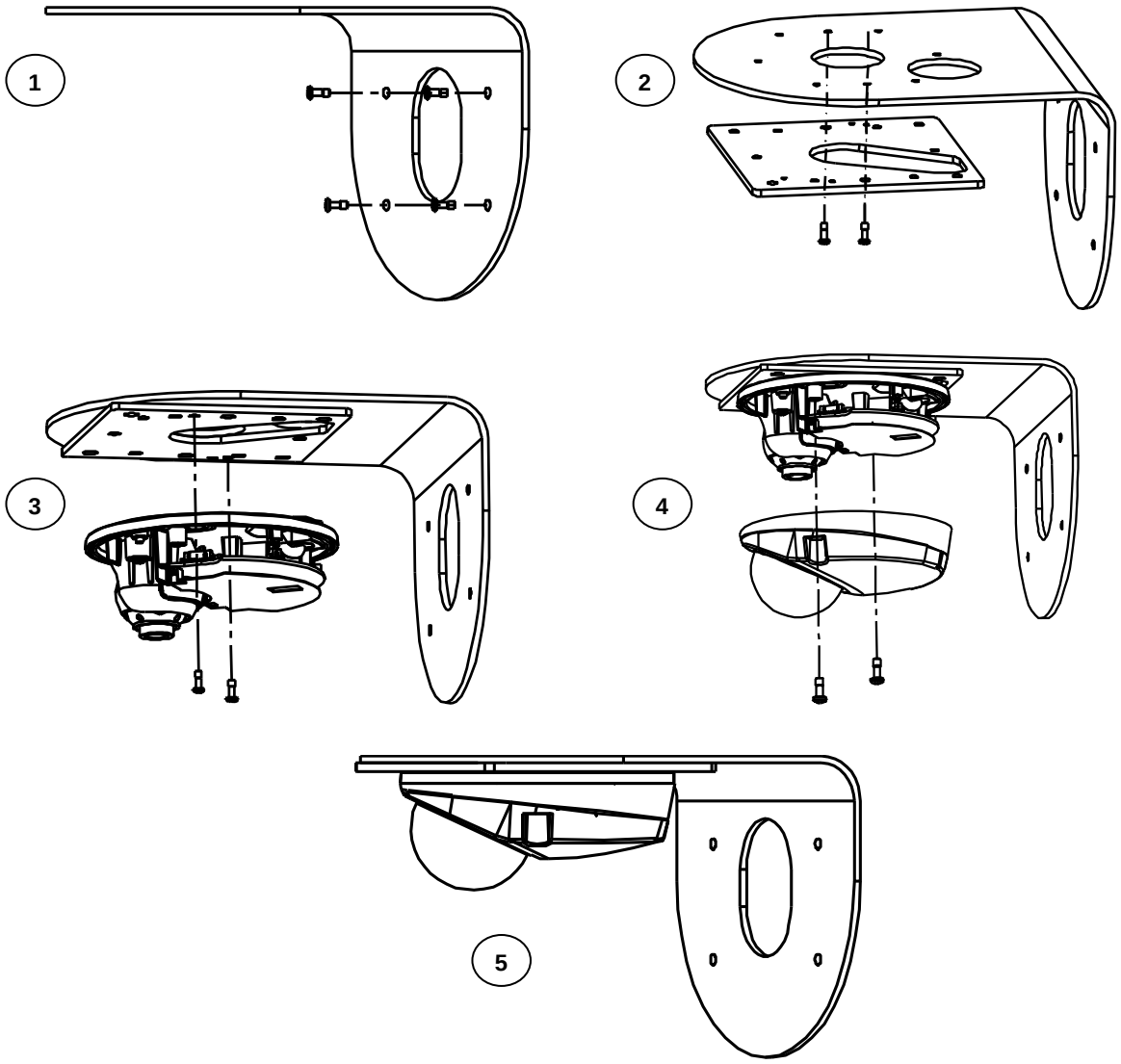
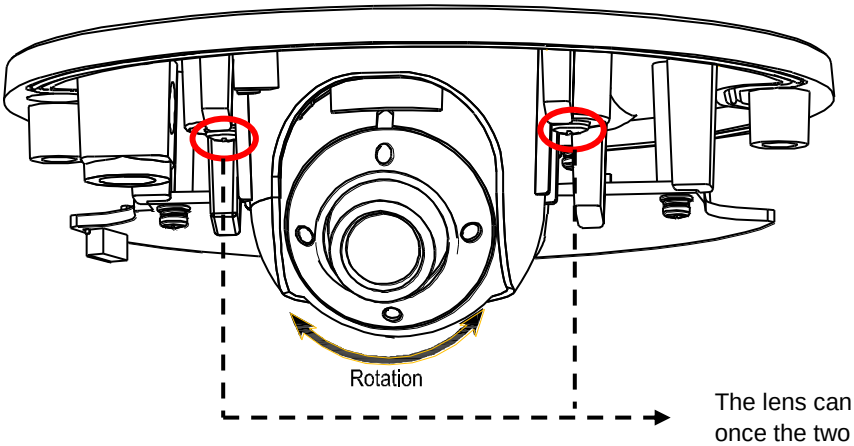


FIGURE 2-4: WALL MOUNT WITH IMPPMB-1I

2.3.5 Adjusting the Camera Position

1. Loosen the two screws beside the lens as figure shown below.
2. Adjust the lens to a desired shooting angle for suitable field of view.

NOTE: Make sure to relock the 2 screws tightly after adjustment.



The lens can be adjusted vertically & horizontally once the two screws are fully loosened.

FIGURE 2 - 5: ADJUSTING THE FOCUS POSITION

2.3.6 Sticking Desiccant

1. Take out the desiccant from the package.
2. Flip over the dome cover and stick desiccant to the rectangular recess as shown in the figure below.

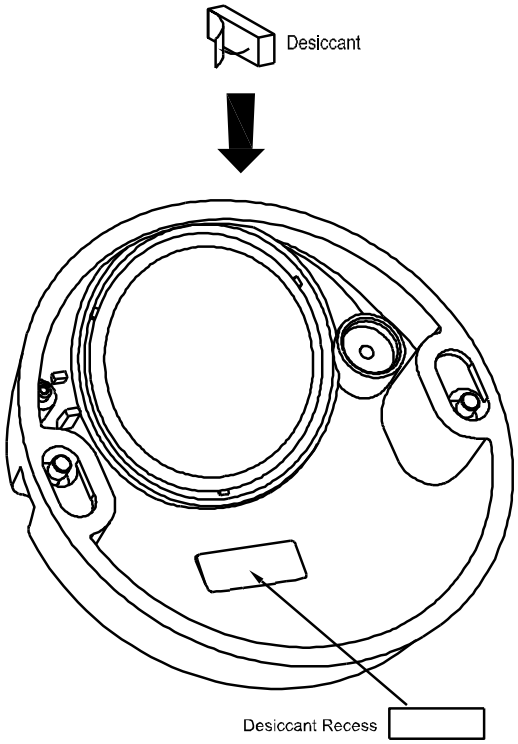


FIGURE 2 - 6: STICKING DESICCANT

2.3.7 Completing the Installation

1. After mounting the unit body to the surface, attach the dome cover with extra care on direction.

2. Fasten the dome cover with unit body by securing screws tightly via torx wrench to complete installation.

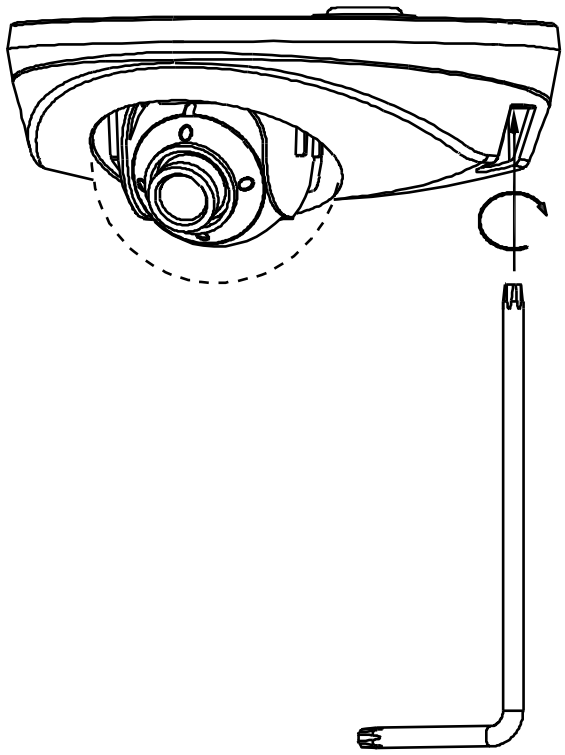


FIGURE 2 - 7: COMPLETING THE INSTALLATION

2.3.8 Network Topology

The unit, which is equipped with Ethernet RJ-45 network interface, can deliver video images in real time via either Internet or Intranet. Please refer to the skeleton drawings shown below to aid your understanding.

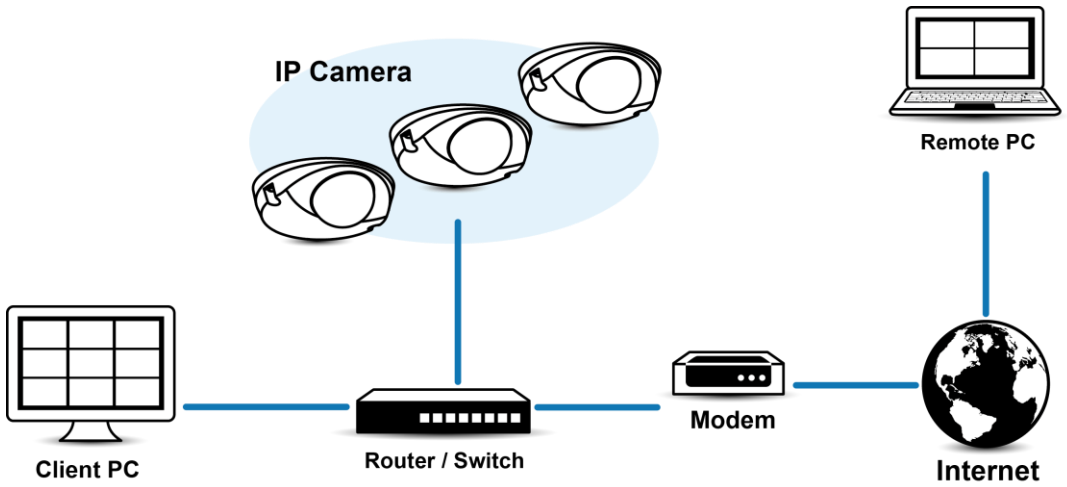


FIGURE 2 - 8: NETWORK TOPOLOGY

2.3.9 System Requirements

The table below lists the minimum requirements 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	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.

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 Software to Get Camera's IP Address

Pelco Device Utility 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. Finish installing the Device Utility to the computer according to the installation instructions.
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** 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 the Device Utility, click this green icon "?" on the upper-right corner of the Device Utility page.

2.4.2.2 Connecting from a computer

1. Check if there is 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 software (refer to **2.4.2.1 Using Pelco Device Utility Software to Get Camera's IP Address**).

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

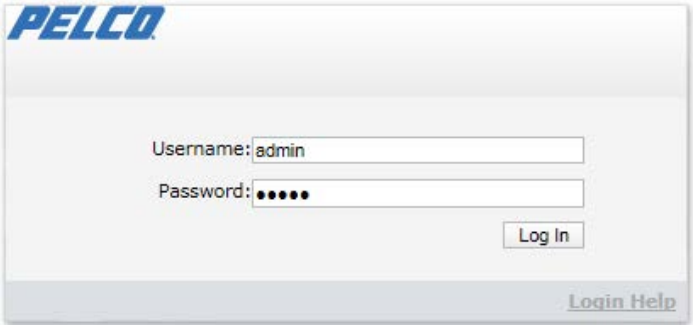


FIGURE 2 - 9: LOGIN WINDOW

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 ***21*** 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 of the options on the **Live** window.

Select Stream: Selects the viewable video stream that is displayed in live view (primary, secondary or quickview) and the transmission type (multicast or unicast) and the player type (Pelco Media Player and Quicktime) all available for selection by user.

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.

Snapshot: Capture a screenshot of what is seen currently on the live view image. A prompt message appears, after clicking the icon, to allow user to either open the screenshot or save the screenshot to a designated path.

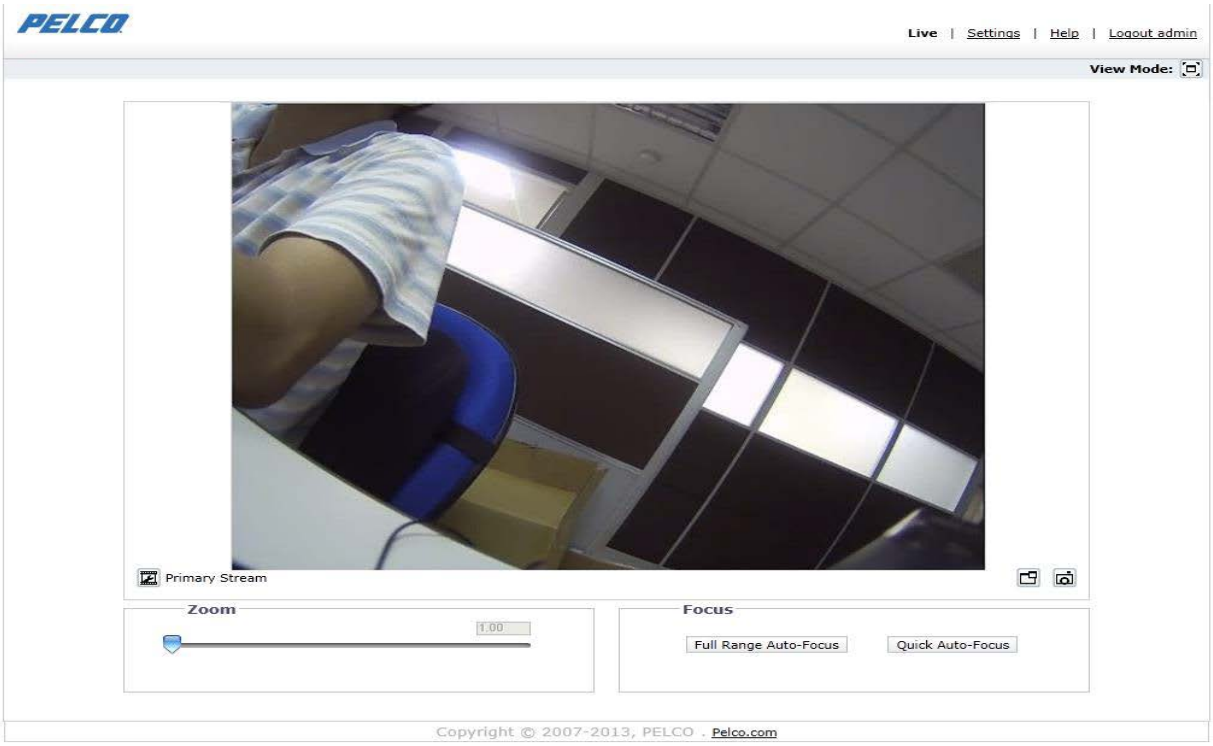


FIGURE 3-1: LIVE VIEW

3.2 Settings

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

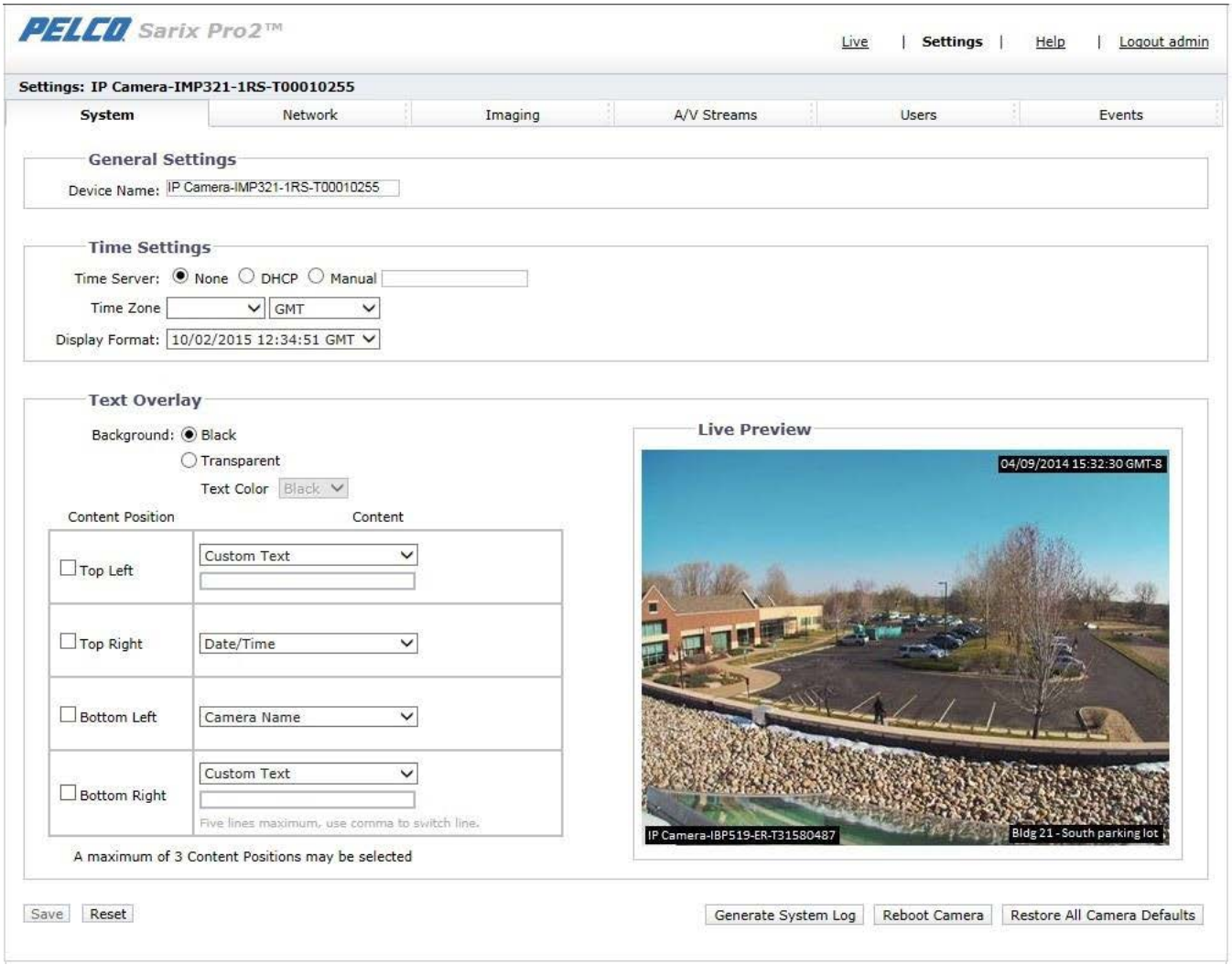


FIGURE 3-2: SYSTEM SETTINGS

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.

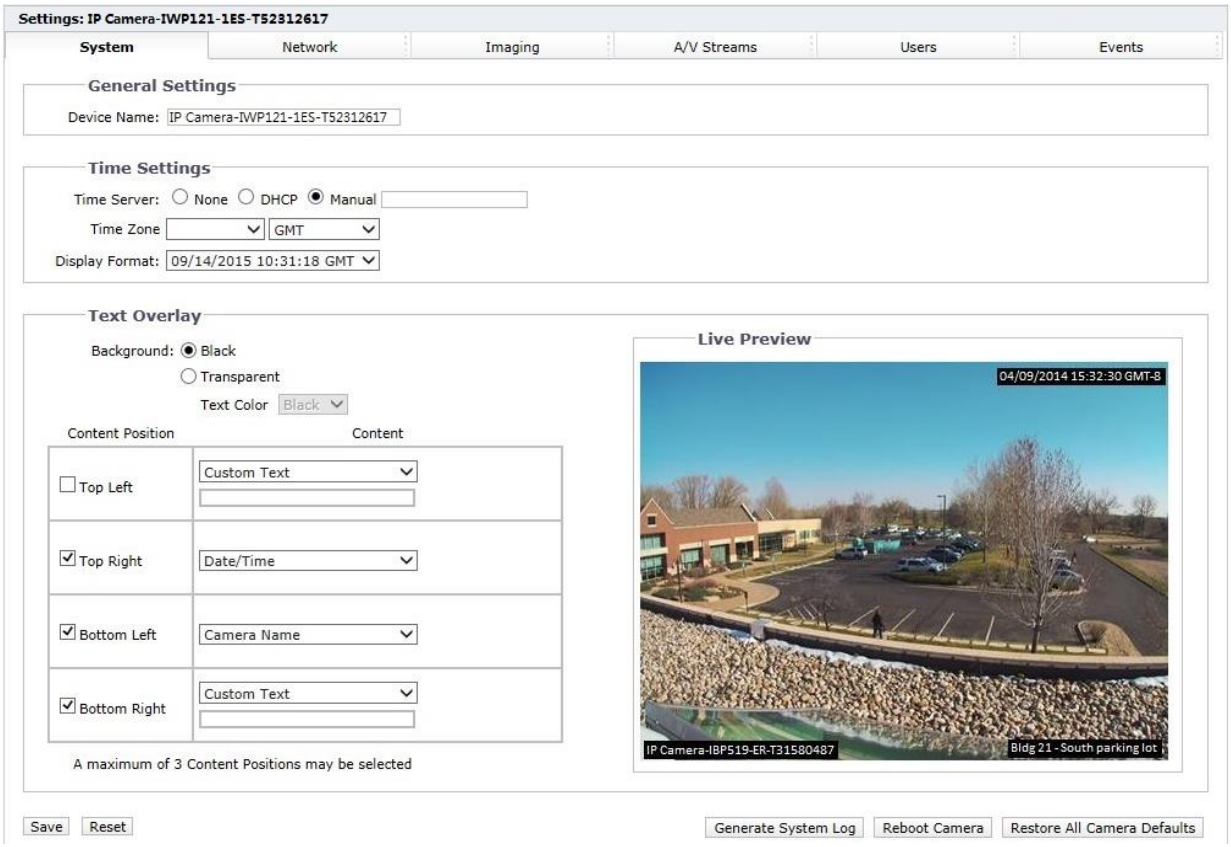


FIGURE 3-3: SYSTEM SETTINGS

Generate System Log

1. Click the System tab.
2. Click the Generate 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

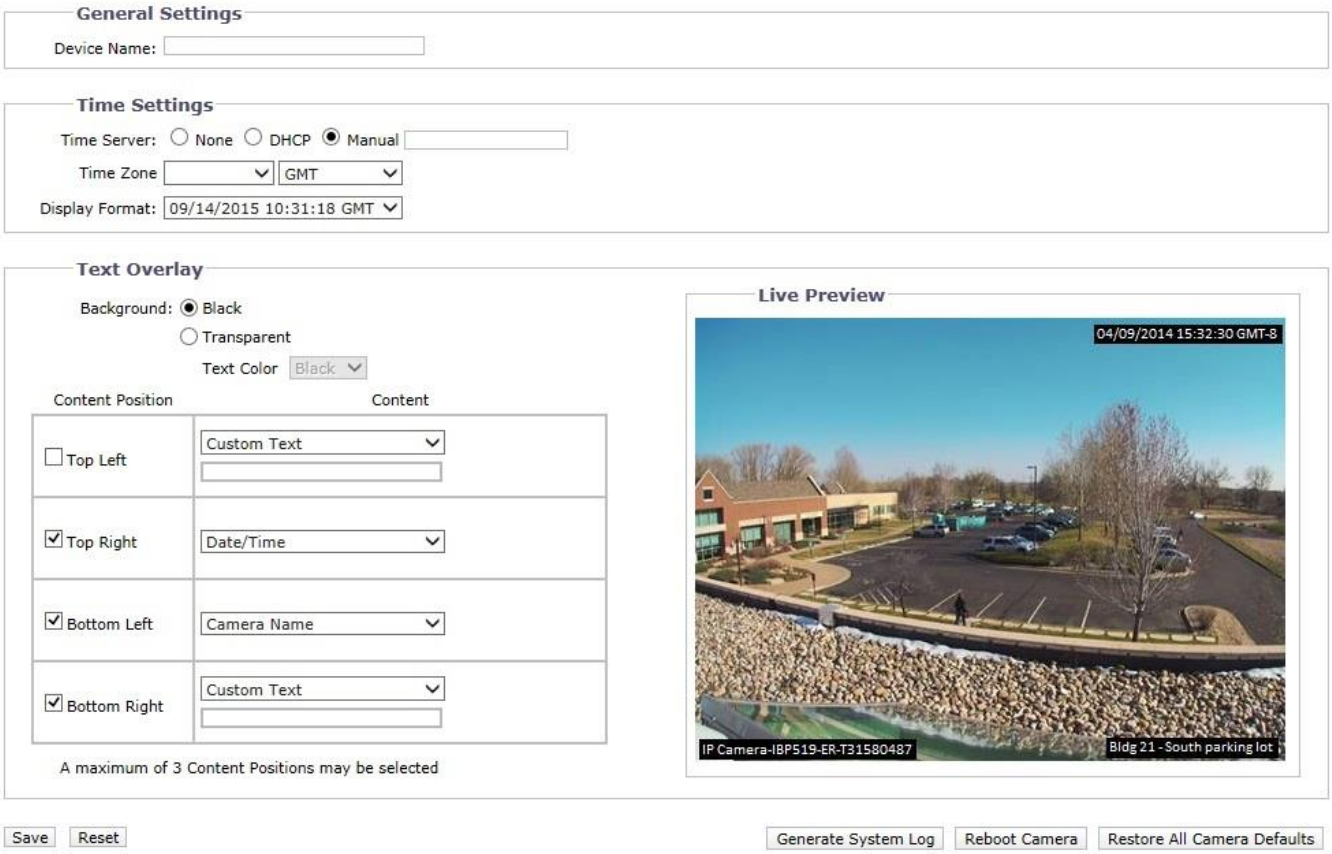


FIGURE 3-4: GENERAL SETTINGS

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. Select the format in which the date and time will appear from the Display Format drop-down field if you have opted to show the Date/Time Overlay.

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.

Text Overlay

1. Configure the text overlay settings:
   - **Background:** Set the background color for the text overlay as black or transparent. Text color for the transparent background can be also customized from the drop-down menu when the transparent background option is selected.
   - **Content:** Four content options can be selected to display from the drop-down menu: Date/Time, Camera Name, Camera Name + Date/Time, and Custom Text. The blank text field, which is for inputting desired text by users, shows only when Custom Text option is selected.
     NOTE: Multiple content options can display simultaneously.
   - **Content Position:** Four positions can be selected to display content overlays: Top Left, Top Right, Bottom Left, and Bottom Right. A maximum of three positions can be enabled simultaneously.
     NOTE: A maximum of 3 contents can be displayed simultaneously.
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.

3.2.1.2 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 System 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.

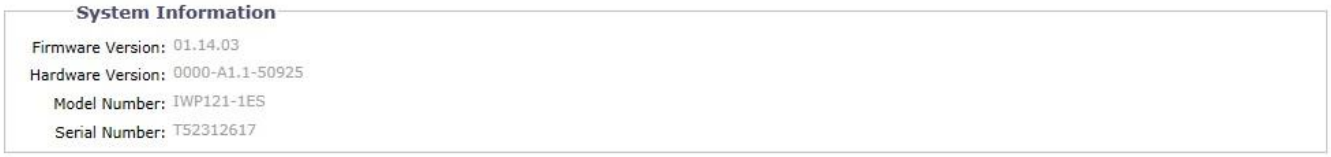


FIGURE 3-6: SYSTEM INFORMATION

3.2.1.4 Firmware Update

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. Disconnecting power during a firmware update will cause the update to fail. It takes approximately 3 minutes for the unit to reboot after firmware update process.

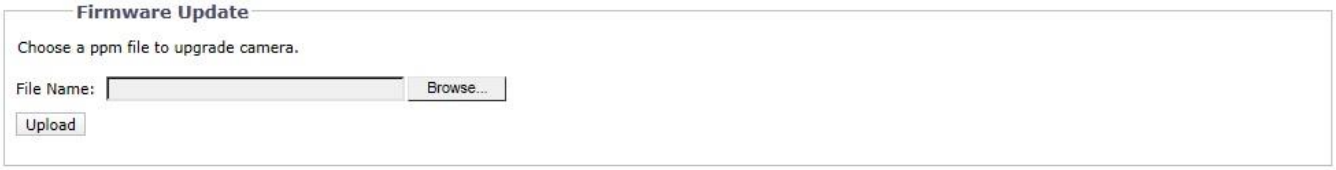


FIGURE 3-7: FIRMWARE UPDATE

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, enable FTP access to this camera and activate VMS Connectivity with the specific server.

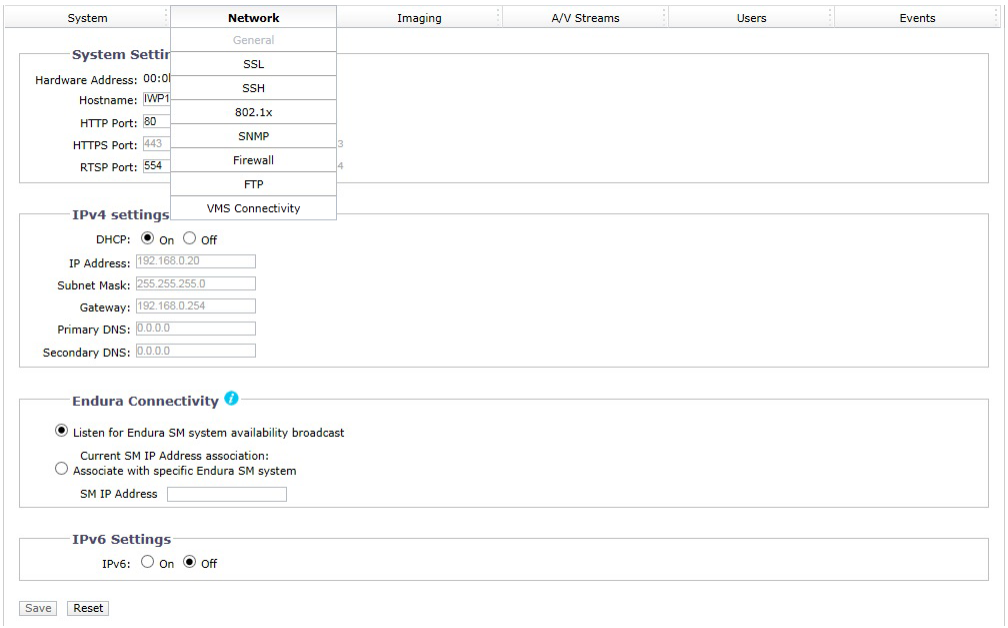


FIGURE 3-8: NETWORK CONFIGURATION

3.2.2.1 General

Set the General Network Settings for network communication settings.

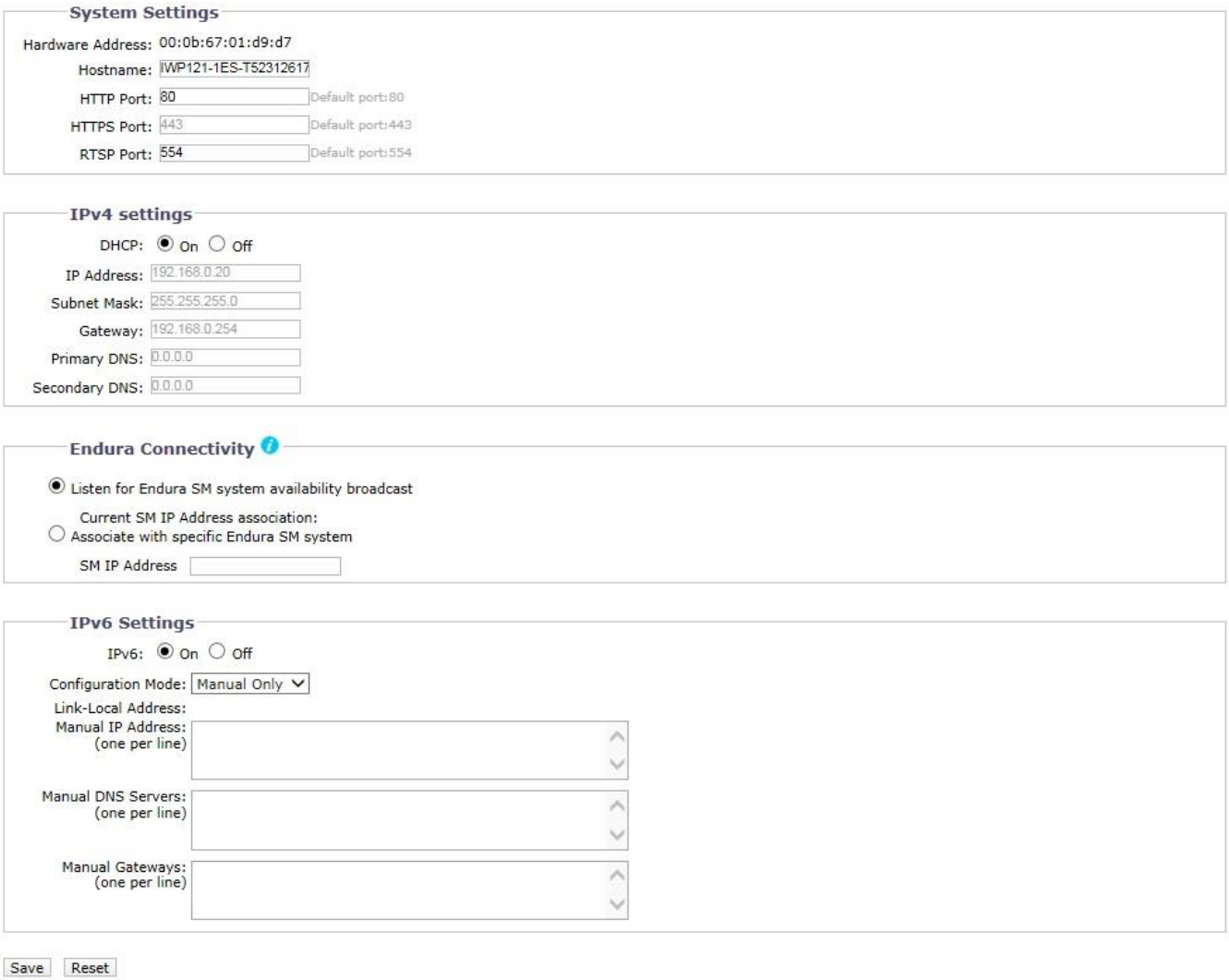


FIGURE 3-9: GENERAL NETWORK SETTINGS

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.

Endura Connectivity

In order to connect with the Pelco NVR Endura, please choose which communication method to be adopted for connectivity from the following 2 options:

- **Listen for Endura SM system availability broadcast:** In general, Endura broadcasts its SM IP Address to the camera so that a stable connection can be maintained between Endura system and the camera.
- **Associate with specific Endura SM system:** Under certain cases, the camera is unable to receive broadcast from Endura system and therefore is in need of a SM IP Address assigned specifically by user for connectivity.

Configuring IPv6 Settings

Your Sarix device supports IPv6 in conjunction with IPv4 configurations; the device does not support IPv6-only network deployments. The device will accept up to sixteen IPv6 addresses, three IPv6 DNS servers, and three IPv6 gateways.

There are two configuration modes for IPv6 address assignments:

Auto: Enables automatic configuration using router advertisement. Additional configuration can be provided over DHCPv6 (if available on your network). Selecting Auto mode still allows you to manually configure additional IPv6 addresses, DNS servers, and gateways.

Manual Only: Provides a link-local IPv6 address for the device and allows you to assign up to 16 static IPv6 addresses to the device.

1. Place your mouse pointer over the Network tab.

2. Select General from the drop-down menu.

3. Select On for IPv6.

4. Select a Configuration Mode from the drop-down box. Selecting Auto allows the device to configure the remaining IPv6 settings automatically, rendering the remaining steps optional.

5. *(Optional)* Provide static, unicast addresses in the Manual IP Addresses box. Each address requires a prefix, and it must be input using the format *prefix/IPv6Address*. Manual IP addresses without prefix information will be rejected.

6. *(Optional)* Provide the addresses of DNS servers that are not configured automatically in the Manual DNS Servers box.

7. *(Optional)* Provide the addresses of gateways that are not configured automatically in the Manual Gateways box.

NOTES:

• The device will not accept multicast, local host, or undefined IPv6 addresses.

• Link-local addresses are not supported for DNS.

• Manually specified DNS servers supersede automatically discovered DNS servers.

• Manually specified DNS servers are not validated by the device; verify any manually specified DNS servers before saving IPv6 settings.

• Manually specified gateways must be on the same network as the devices's IPv6 addresses. Behavior for a gateway that is not on the same network as the device's IPv6 addresses is undefined.

• Some video management systems (VMS), including Pelco VMS systems, do not support connections to cameras and encoders over IPv6.

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***

• ***Generating Certificate Request***

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.

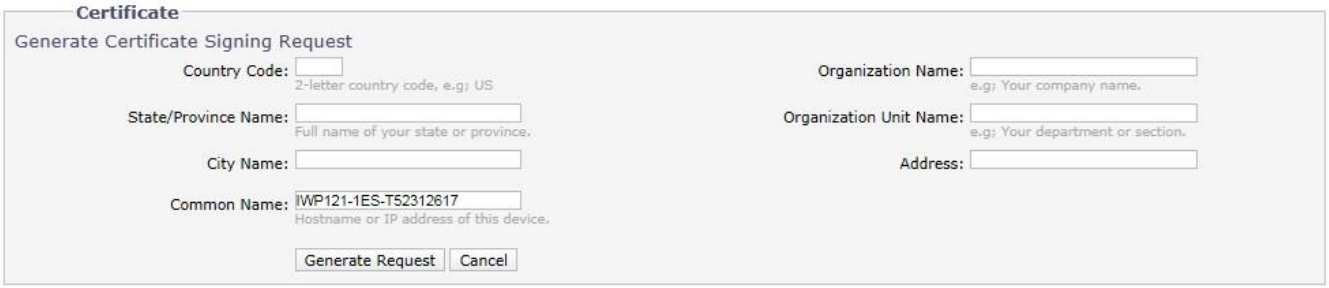


FIGURE 3-13: GENERATING CERTIFICATE REQUEST

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 appear 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.

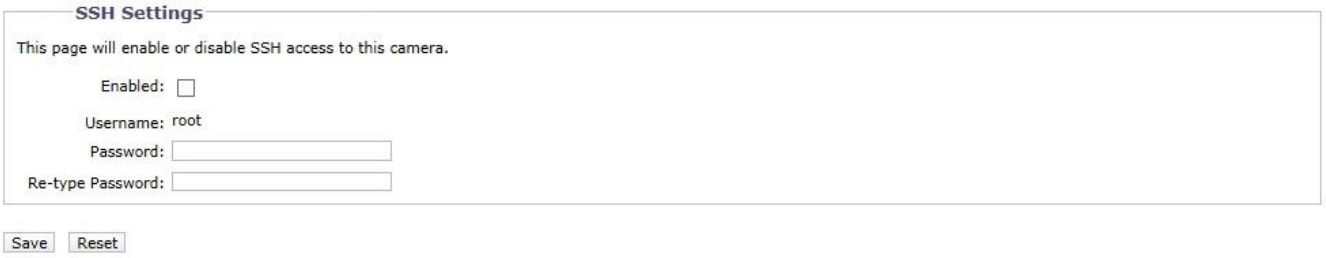


FIGURE 3-15: ENABLING SECURE SHELL

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.

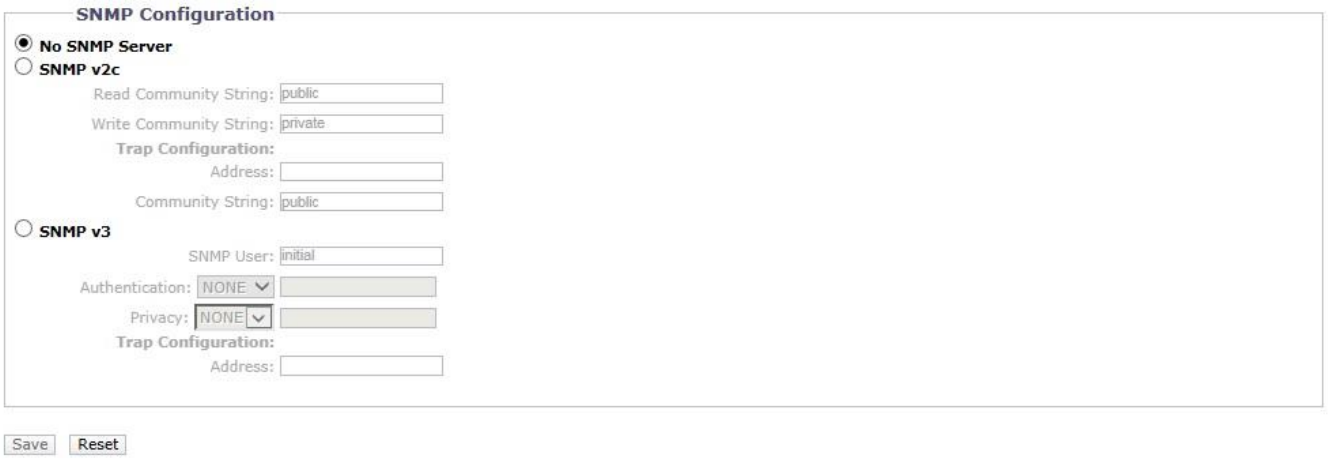


FIGURE 3-17: SNMP CONFIGURATION

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 both the Read and Write Community String box. The default name for each is “public” and “private” respectively.
  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. Enter 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. Check **Enabled** to enter IP address in the **Address** field. Up to ten addresses can be enabled for entry.
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.

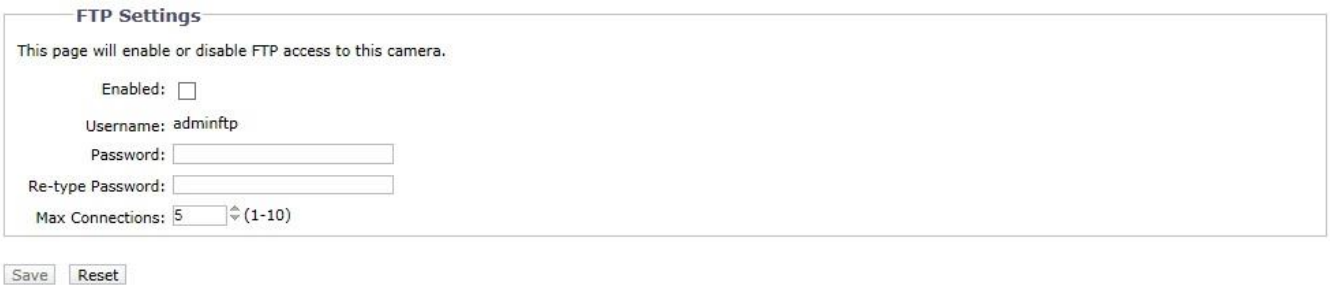


FIGURE 3-19: FTP SETTINGS

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.
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.

3.2.2.8 VMS Connectivity

This page relates to the standard protocol that conforms to the regulations of IP security surveillance data transmitting, transferring and monitoring within the PRC (People Republic of China) areas.

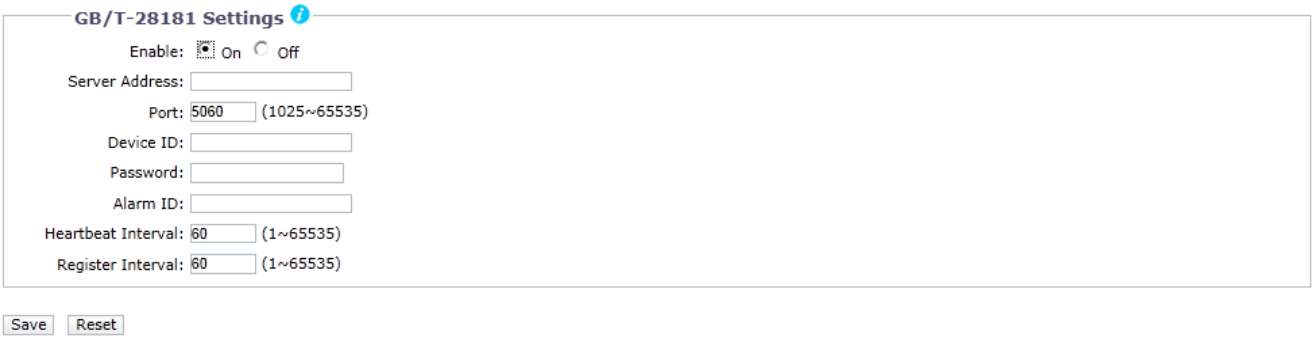


FIGURE 3-20: VMS CONNECTIVITY SETTINGS

GB/T-28181 Settings

1. Select the **Enable** check box to activate the VMS Connectivity function.
2. Enter an address for **Server Address** and a value for **Port** ranging from 1025 – 65535.
3. After registering the GB28181 service, enter a **Device ID** and an associated **Password**.
4. A set of alarm ID will be obtained after registering the GB28181 service. Input the provided alarm ID, which is for alarm notice, into the field here.
5. Set an interval value for Heartbeat and Register transmit with the server individually.

3.2.3 Imaging

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

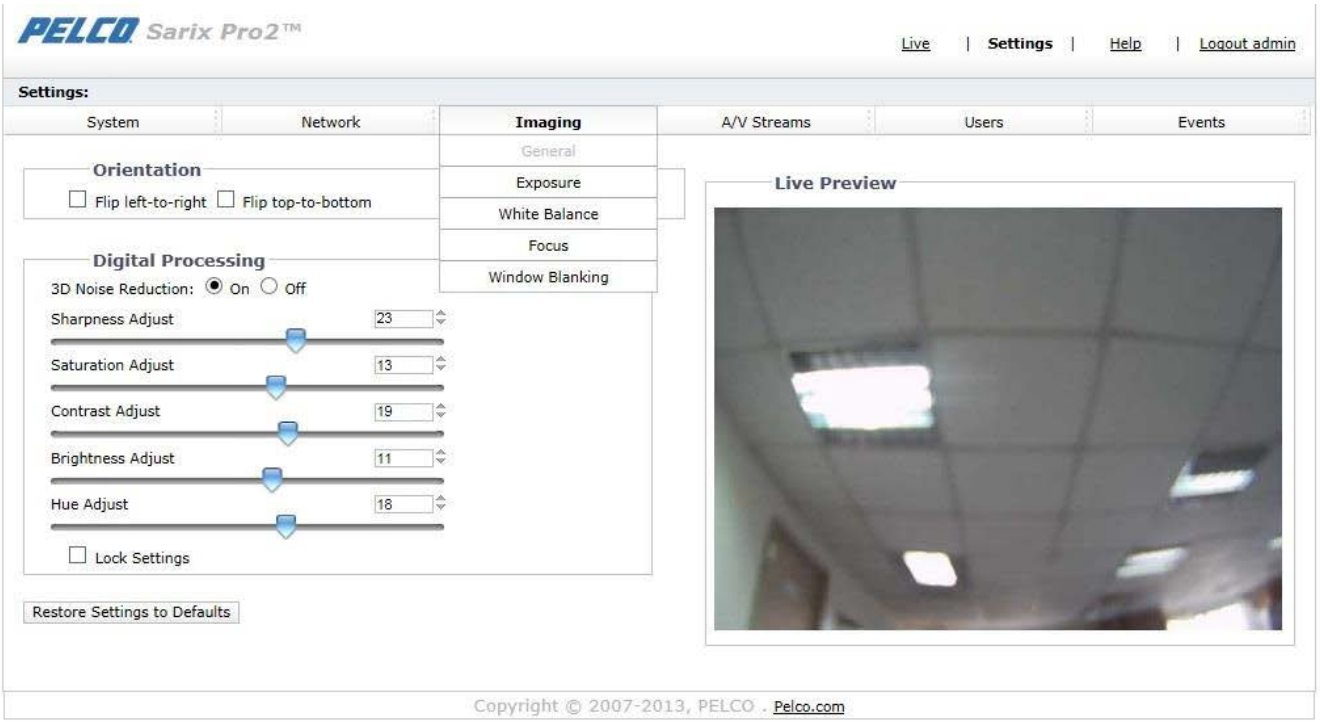


FIGURE 3-21: IMAGING SETTINGS

3.2.3.1 General

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

FIGURE 3-22: 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 noise reduction, sharpness, saturation, contrast, brightness and hue.

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

- **3D Noise Reduction**: Enable 3D Noise Reduction to improve video noise in low light scenes. Turn off 3D noise reduction if details are blurred in moving objects.
- **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.

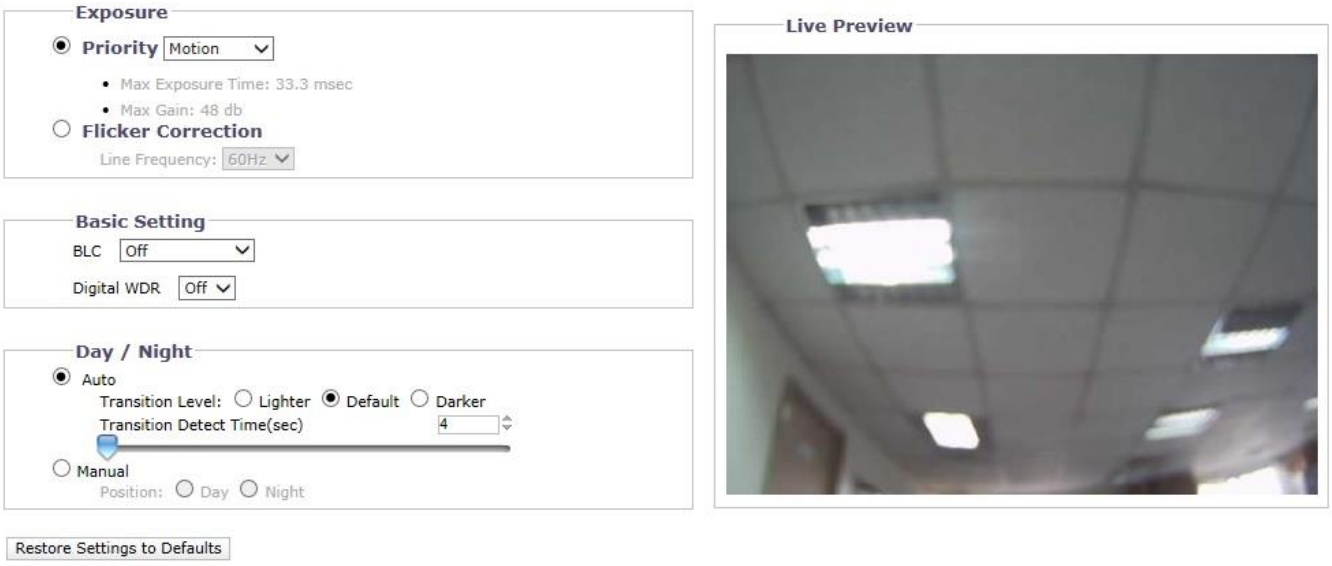


FIGURE 3-23: EXPOSURE SETTINGS

Exposure

- **Priority Preset**

  Select **Motion** or **Low Noise** as the exposure priority. The Motion setting increases exposure time to reduce motion blurring in low light. The Low Noise setting decreases exposure time and adjusts frame rate for improved noise reduction in low light scenes.

- **Flicker Correction**

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

Basic Setting

- **BLC**

  Select an area ranging from Upper, Lower, Central 1/3rd, Central 1/6th, Left, and Right for Backlight Compensation. Backlight Compensation is a function that sets the brightness of a selected area to an optimal level. This function is necessary when an auto iris lens tends to close quickly due to an intense light coming from the back of object in the area wished to view, resulting in the area being too dark and difficult to see. In this case, users may set the area corresponding to the portion they wish to see.

- **Digital WDR**

  Select On to enable Digital WDR. This feature is intended for providing clear images even under backlight where intensity of illumination can vary excessively, i.e. when both very bright and dark areas simultaneously come in the field of view. Digital WDR, via software algorithm, enables capture and display of both bright and dark areas in the same frame, in such a way that there are clear details in both areas, i.e. bright areas are not saturated and dark areas are not too dark.

Day/Night

The Day Night Auto mode setting automatically controls both the Transition Level and Transition Detect Time for the dynamic changes of light intensity between day time and night time.

- **Auto**
  1. **Transition Level:** Determines when the camera changes from day mode (color) to night mode (black-white). Select the "**Lighter**" transition level setting if you want the camera to change modes at a high lux setting. Use the "**Default**" setting for normal day/night operation. Use the "**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	10 lux
Default	2 lux
Darker	1 lux

  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.

3.2.3.3 White Balance

Under **White Balance**, choose from **ATW** (auto tracing white balance), **Auto**, and **Manual** modes of adjustment on white balance for the video. **ATW** offers continuous adjustments on camera color balance in accordance with any change in color temperature. **Auto** enables automatic controls on color temperature ranging from 2500°K to 10000°K.

FIGURE 3-24: WHITE BALANCE SETTINGS

Under **Manual** mode, the Red and Blue Gain adjustment bars with their scale boxes on their right will appear once the mode is selected. Base color of the video will change as the bars are adjusted left or right. Adjust to the ideal balance as appear fit. Click on **One Push** to have the camera adjust to the proper gain values rapidly depending on the ambient environment of area viewed, where its light source is constant, without adjusting for any change in light source or color temperature.

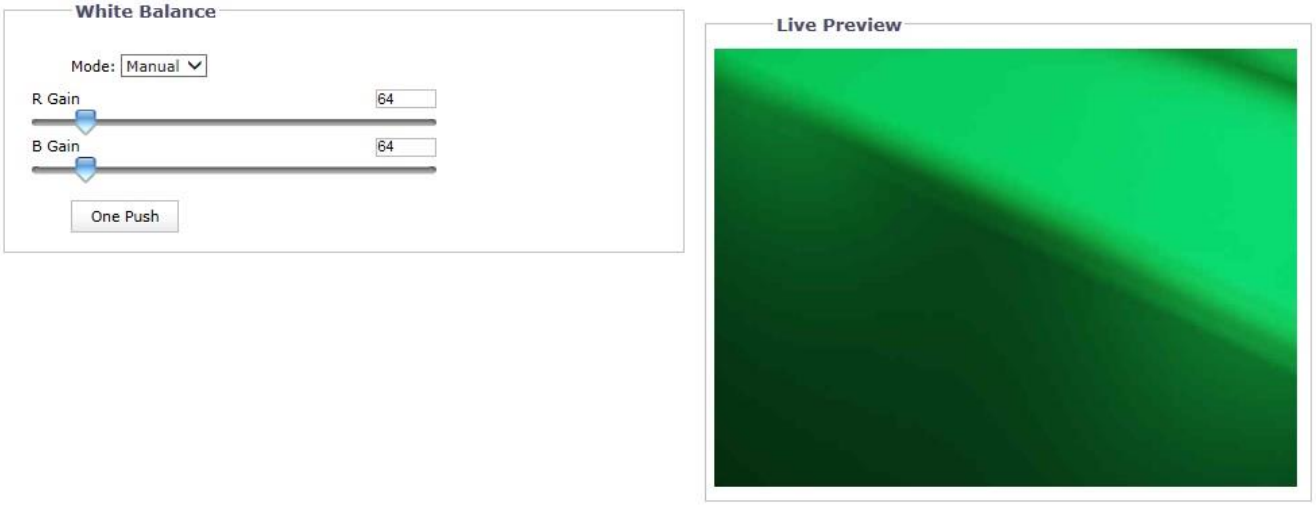


FIGURE 3-25: WHITE BALANCE SETTINGS – MANUAL

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 8 blanked windows as long as the total blanked area does not exceed 50 percent of the field of view.

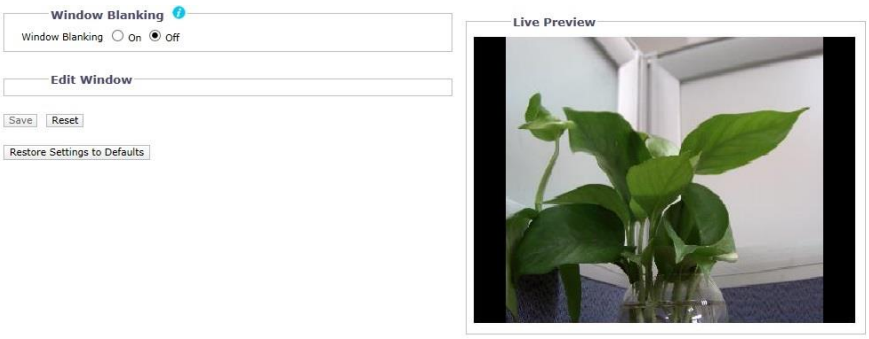


FIGURE 3-26: WINDOW BLANKING SETTINGS

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 3-27: WINDOW BLANKING ON

NOTE: Up to 8 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 as well as the Local Recording page.

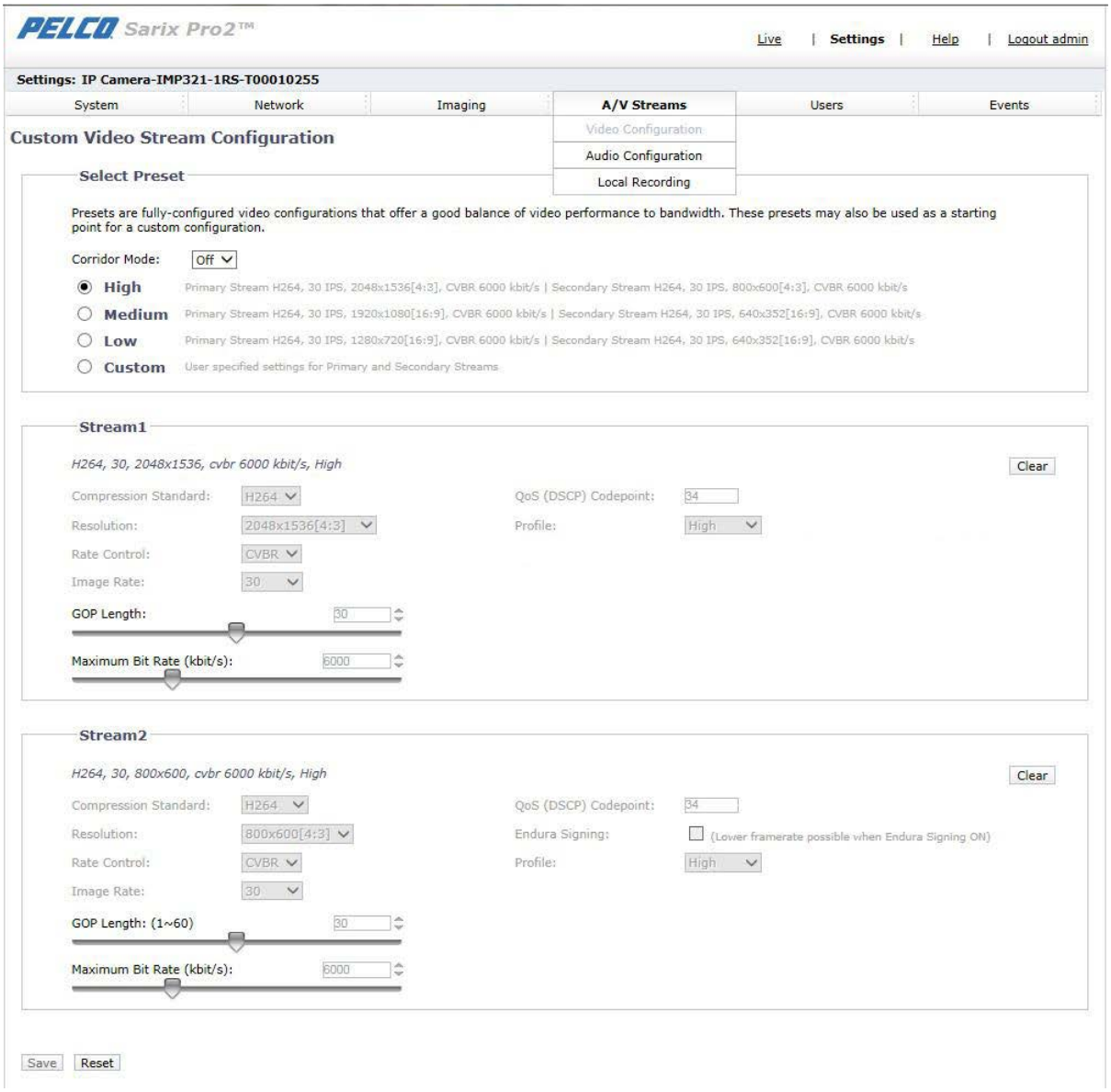


FIGURE 3-28: A/V STREAMS

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.

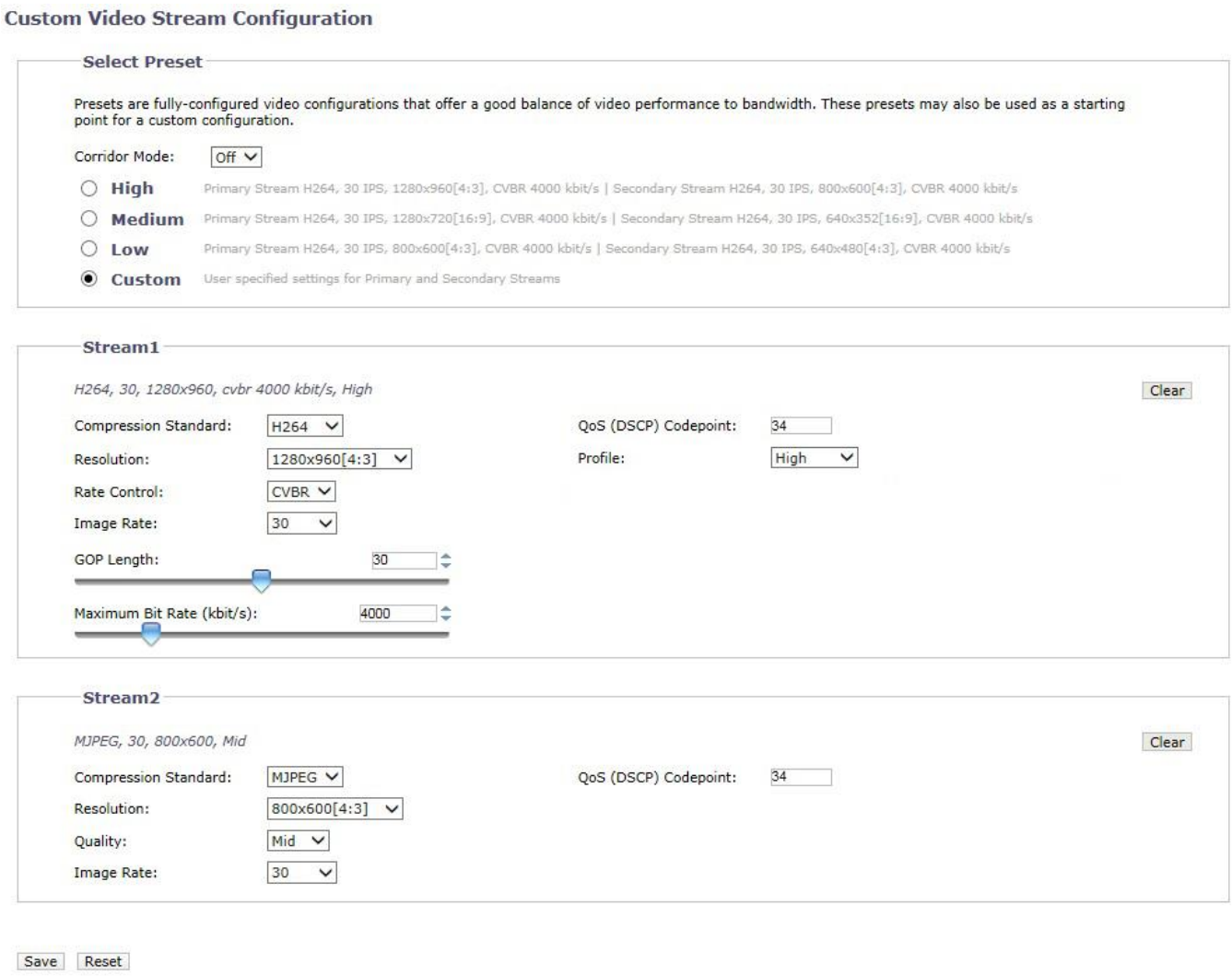


FIGURE 3-29: CUSTOM VIDEO STREAM CONFIGURATION

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. Choose to switch the Corridor Mode On or Off. Corridor Mode offers a vertically widened field of view in narrow spaces like hallways and tunnels.

NOTE: Corridor mode is not available when codec is MJPEG.

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		Service Stream
Compression Standard / Available Resolutions	H264	MJPEG	H264	MJPEG	MJPEG
2592 x 1944*	2592x1944	N/A	800x600 640x480 320x240	800x600 640x480 320x240	640x480
2048x1536**	2048x1536	2048x1536	800x600 640x480 320x240	800x600 640x480 320x240	640x480
1920x1080***	1920x1080	1920x1080	960x540	960x540	640x352
1920x1080***	1920x1080	1920x1080	640x352 320x180	640x352 320x180	640x352
1280x960	1280x960	1280x960	800x600 640x480 320x240	800x600 640x480 320x240	640x480
1280x720	1280x720	1280x720	640x352 320x180	640x352 320x180	640x352
1280x960****	1280x960	1280x960	1280x960 800x600 640x480 320x240	1280x960 800x600 640x480 320x240	640x480
1280x720****	1280x720	1280x720	1280x720 640x352 320x180	1280x720 640x352 320x180	640x352
800x600	800x600	800x600	800x600 640x480 320x240	800x600 640x480 320x240	640x480
640x480	640x480	640x480	640x480 320x240	640x480 320x240	640x480
320x240	320x240	320x240	320x240	320x240	640x480
320x180	320x180	320x180	320x180	320x180	640x352

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

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

*** **NOTE:** 1920x1080 supports **5MP Model** and **3MP Model** and **2MP Model** only.

**** **NOTE:** These resolution combinations are available for **1MP Model** only.

- **Rate Control**

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

  - **CBR:** The constant bit rate (CBR) streams video at a fixed number of bits per second. CBR uses the full capacity of the bit rate setting for scenes with or without motion. Video is always streamed at the user bit rate setting. Adjust the CBR Bit Rate slider that appears when CBR is selected to the optimal fixed number of bits per second.

  - **CVBR:** The constrained variable bit rate (CVBR) provides high-quality video and long recording time of variable bit rate while limiting variations in recording capacity consumption. Adjust the Maximum Bit Rate slider that appears when CVBR is selected to the optimal bit rate for your configuration.

- **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, 12, 10, 7.5, 5, 3, 2, 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. The upper limit depends on the selected image rate. Recovery of the lost frames will be more difficult as the value gets bigger. Smaller values will increase the bit rate and network bandwidth demands. This setting is only available with H264.

- **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.

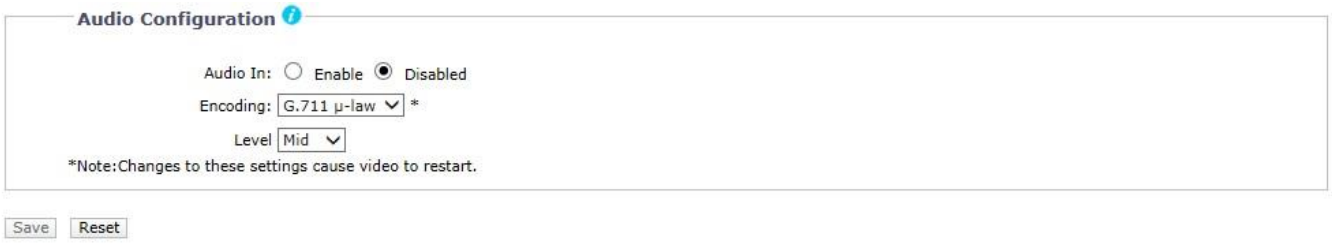


FIGURE 3-30: AUDIO CONFIGURATION

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 selectable sound levels are High, Mid, and Low.
NOTE: Changes to these settings cause video to restart.

3.2.4.3 Local Recording

Local Recording enables users to record and save video files locally on the SD card inserted, instead of recording and saving them over the network that will occupy a huge portion of memory and bandwidth. Check to enable this type of recording. Note that the oldest and previously-recorded video files on the card will be overwritten when the card is full.

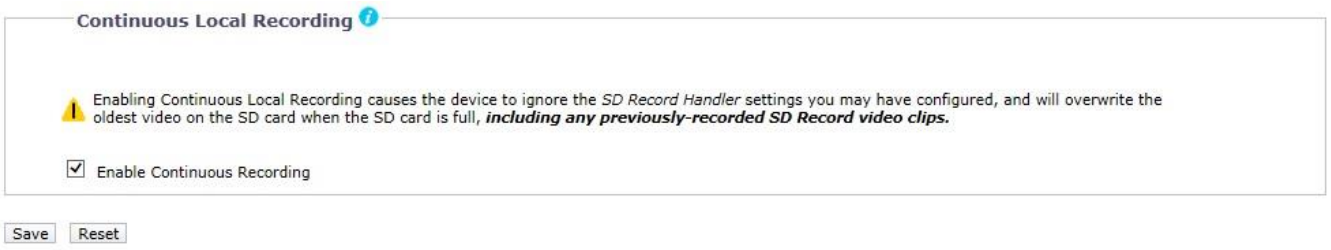


FIGURE 3-31: LOCAL RECORDING

3.2.5 Users

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

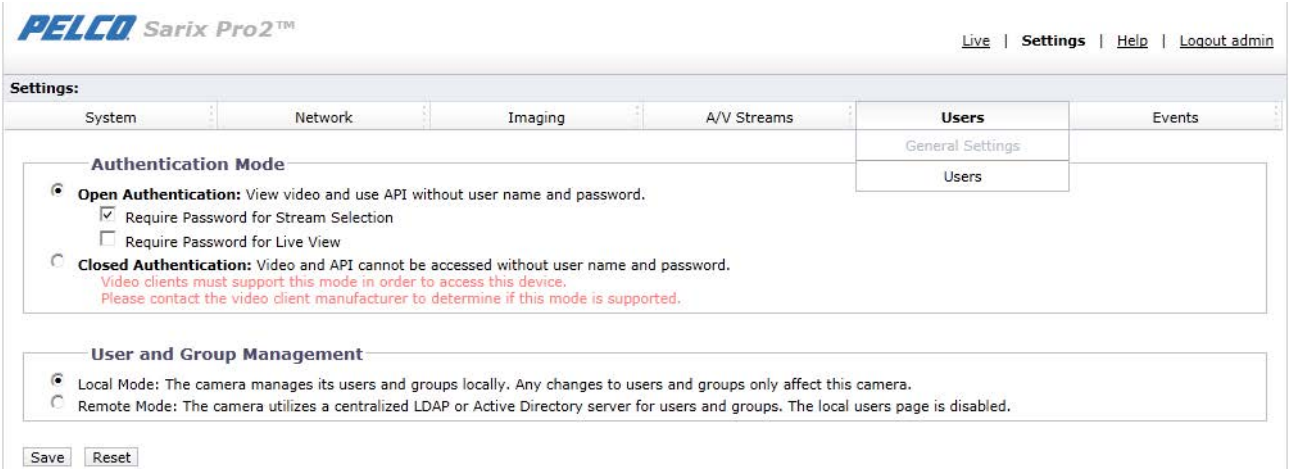


FIGURE 3-32: USERS CONFIGURATION

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.

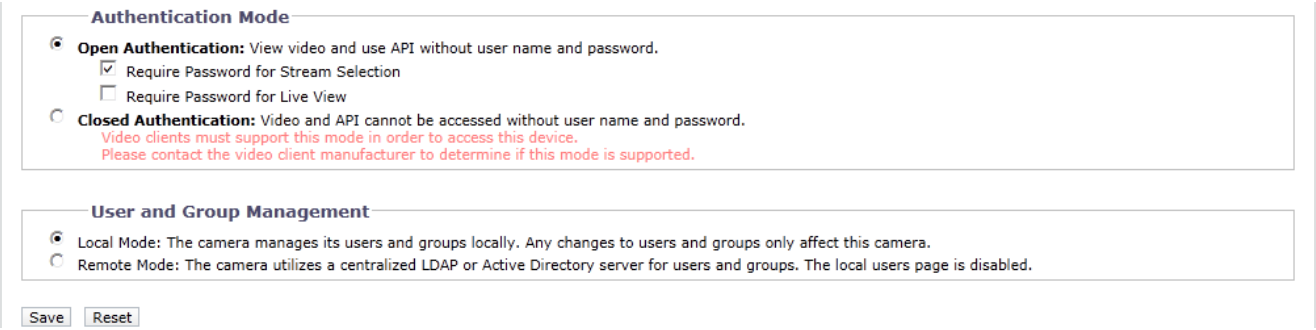


FIGURE 3-33: USERS GENERAL SETTINGS

Authentication Mode

- **Open Authentication**

  Allows users to view video and use the camera API without validating user credentials. With Open Authentication selected, you can check “Require password for Stream Selection” or “Require Password for Live View” or both to limit privileges 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

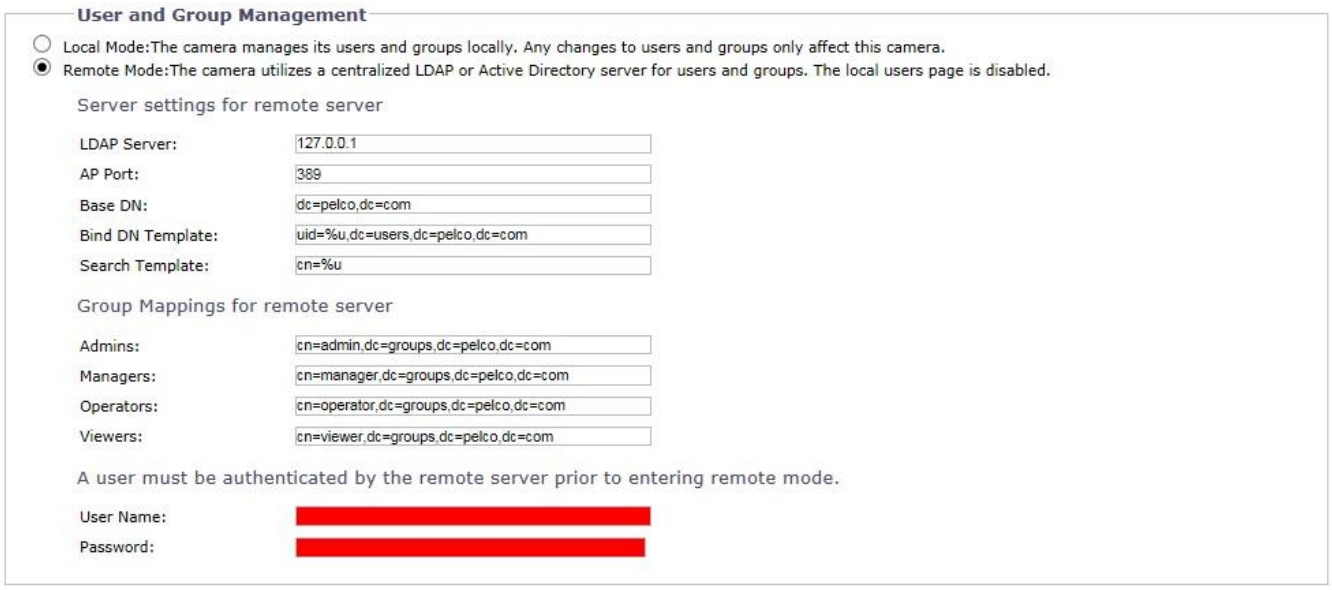


FIGURE 3-34: ENABLING REMOTE MODE

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

3.2.5.2 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.

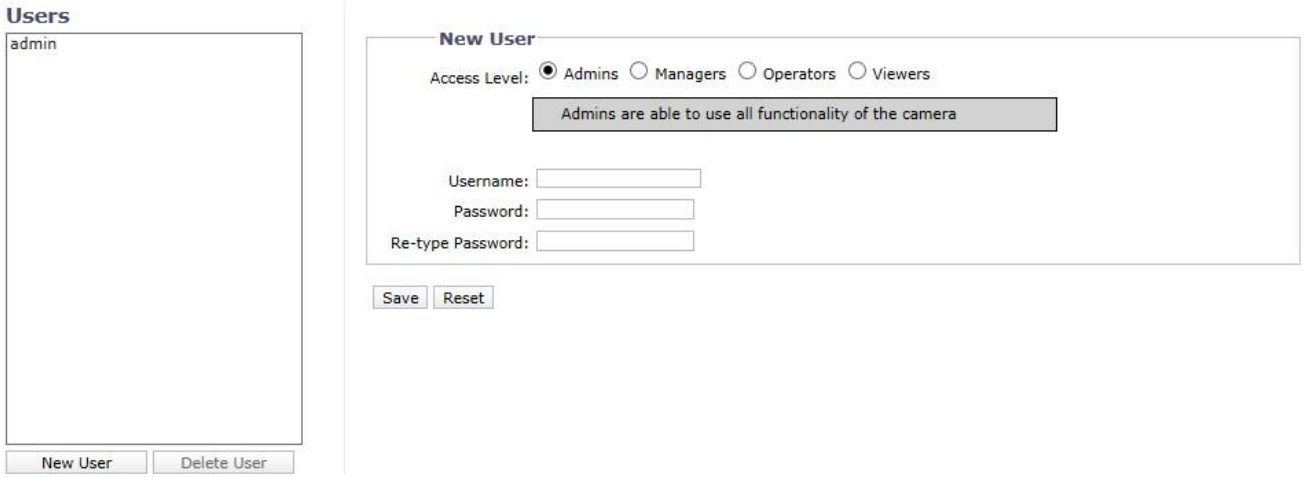


FIGURE 3-35: NEW USERS

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 permissions of access to Users page and the restore factory defaults.
   - **Operators:** This defined group can be modified or deleted. The default permissions for this group are video stream view, PTZ manipulation as well as the use of API.
     NOTE: PTZ manipulation permission varies by applicable models.
   - **Viewers:** This defined group can be modified or deleted. The default permissions for this group are limited within video stream view and the use of API.
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 case-sensitive.

- **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 default “**admin**” user cannot be deleted.

3.2.6 Events

Use the Events tab to configure camera events detections and the following handlers. Events detections are activated by user-defined event sources that tell the device how to react when a specific event occurs. Event handlers are the actions that the device takes when an event occurs. For example, an event source can be configured to alarm an operator via sending email notification if a motion occurs within the predefined camera’s coverage.

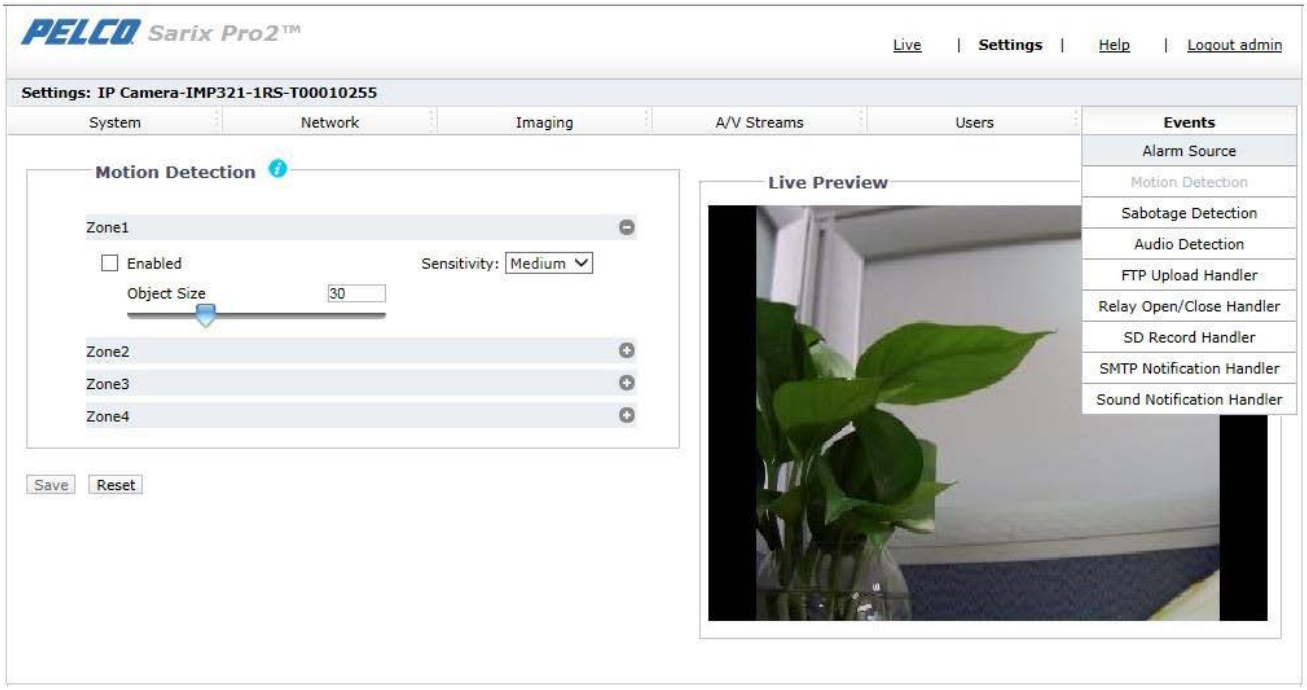


FIGURE 3-36: EVENTS SETTINGS

3.2.6.1 Motion

This page is designed to define multiple groups of motion detection zones with specific own thresholds for triggering.

FIGURE 3-37: MOTION ZONE AREA SETTING

Motion Zone Area Setting

1. Check **Enable** button to enable **Motion** for any or all of Zones 1 to 4.
   NOTE: Click on the button "⊕" to expand section of each zone setting, and click the button "⊖" to collapse each section.
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.
   - **Medium:** The threshold of sensitivity is in the middle between High and Low.
3. **Object Size** can be defined from the range 1 to 100 for detection on wanted objects.
4. Set the desired area to trigger motion detection. The red frame of motion setup will appear for defining the detection area by dragging the mouse.

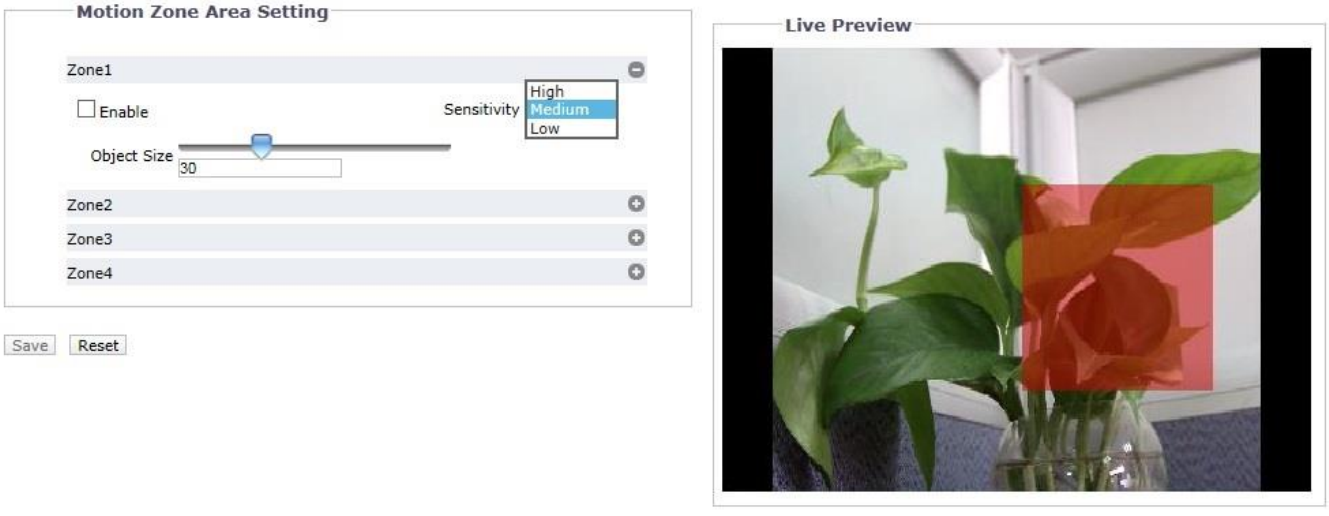


FIGURE 3-38: MOTION ZONE AREA ENABLING

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.

3.2.6.2 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.

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 **Enable** button to enable **Sabotage Detection**.
2. Configure the settings:
   - **Sensitivity:** Determines the triggering sensitivity for alarm. High sensitivity is triggered most easily but is prone to more false alarms. Low sensitivity will only trigger an alarm for major issues like blackout.
   - **Event logging (Profile) name:** Type a user-defined string name that will display within an alarm event to help users to easily distinguish among cameras.
   - **Alarm Severity:** Defines the severity of an alarm to allow the prioritization of alarms.

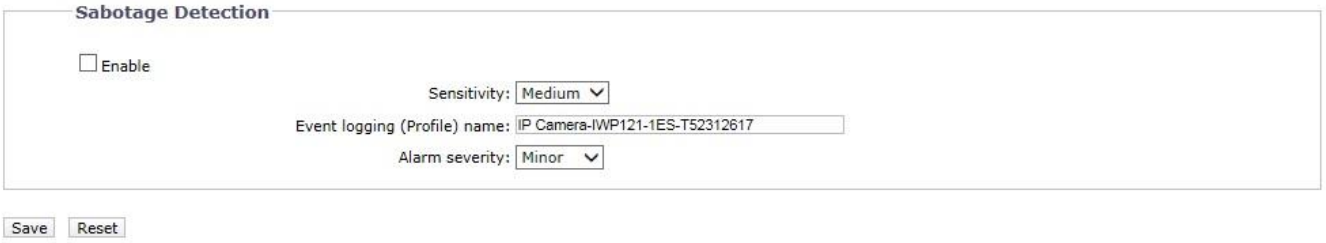


FIGURE 3-39: SABOTAGE DETECTION

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.

3.2.6.3 Audio Detection

This function is designed to define the detailed settings for triggering surrounding audio detection. Check to enable this function. Under **Sound Intensity Threshold**, adjust the threshold bar or input a number in the box right under it for the desired threshold level. A horizontal line, which indicates the exact threshold, in the box underneath will move up or down accordingly.

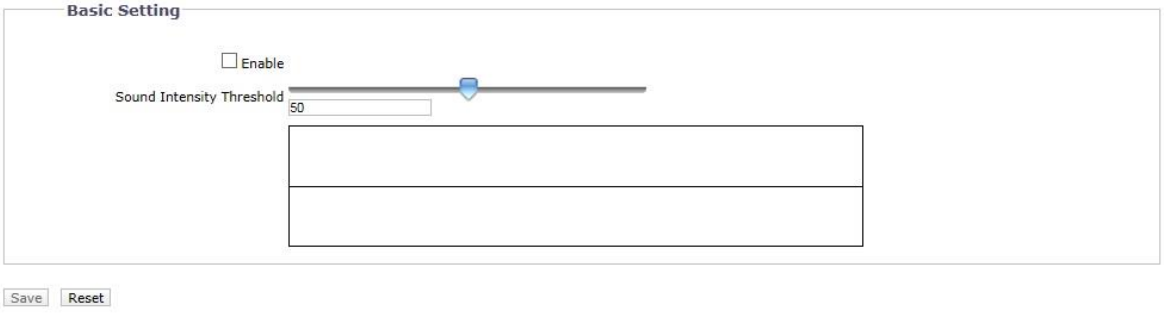


FIGURE 3-40: AUDIO DETECTION

3.2.6.4 FTP Upload Handler

Under this page, camera can record and send snapshot files via properly predefined FTP settings for different events composed of Motion, Sabotage, Schedule as well as Audio Detection.

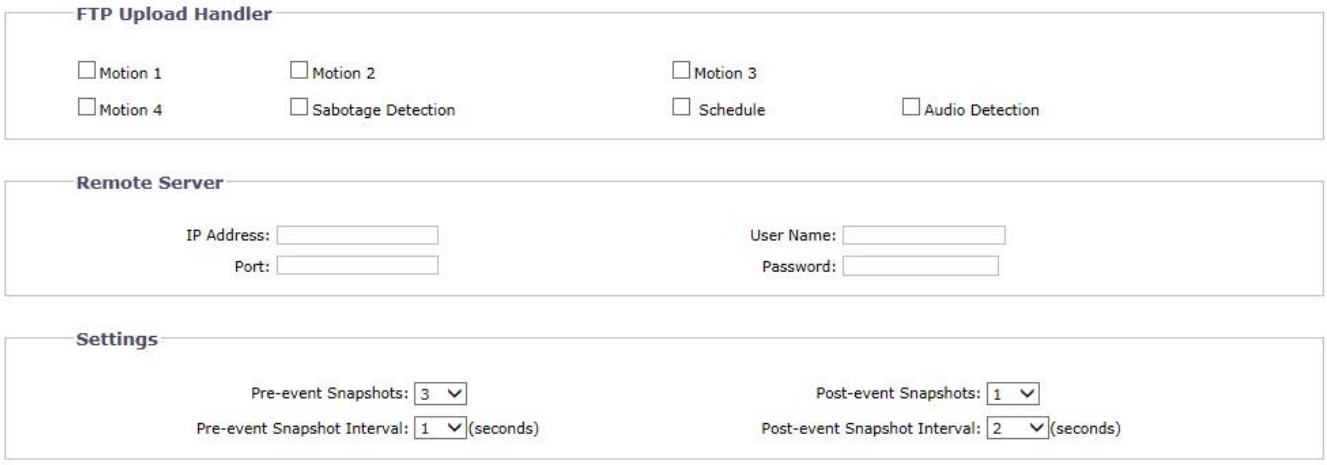


FIGURE 3-41: FTP UPLOAD HANDLER

FTP Upload Handler

You can record and send event image files based on the condition you have set previously.

1. Check to enable **FTP Upload Handler** for **Motions 1 through 4**, **Sabotage Detection**, **Schedule** as we as **Audio Detection**.
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.

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**".

Settings

1. Set **Pre-event Snapshots**, **Post-event Snapshots**, **Pre-event Snapshot Interval**, and **Post-event Snapshot Interval** for **Motions 1 through 4**, **Sabotage Detection**, **Schedule**, and **Audio Detection** selected.
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.

Snapshot Naming

By setting **File Name Prefix** and **Server Path** for **Motions 1 through 4**, **Sabotage Detection**, **Schedule**, and **Audio Detection** selected, you will be able to save an image to a defined FTP server when any of your selected events is activated. Set the **Server Path** where the data is to be stored on the server.

FIGURE 3-42: SNAPSHOT NAMING

You can also set **Trigger Interval** time and determine the recording condition: **OFF**, **All Day**, **Schedule 1**, or **Schedule 2** from scheduled table during 24/7 for **Schedule.** The trigger interval can be adjusted on a scale bar with its corresponding seconds shown in the box underneath.

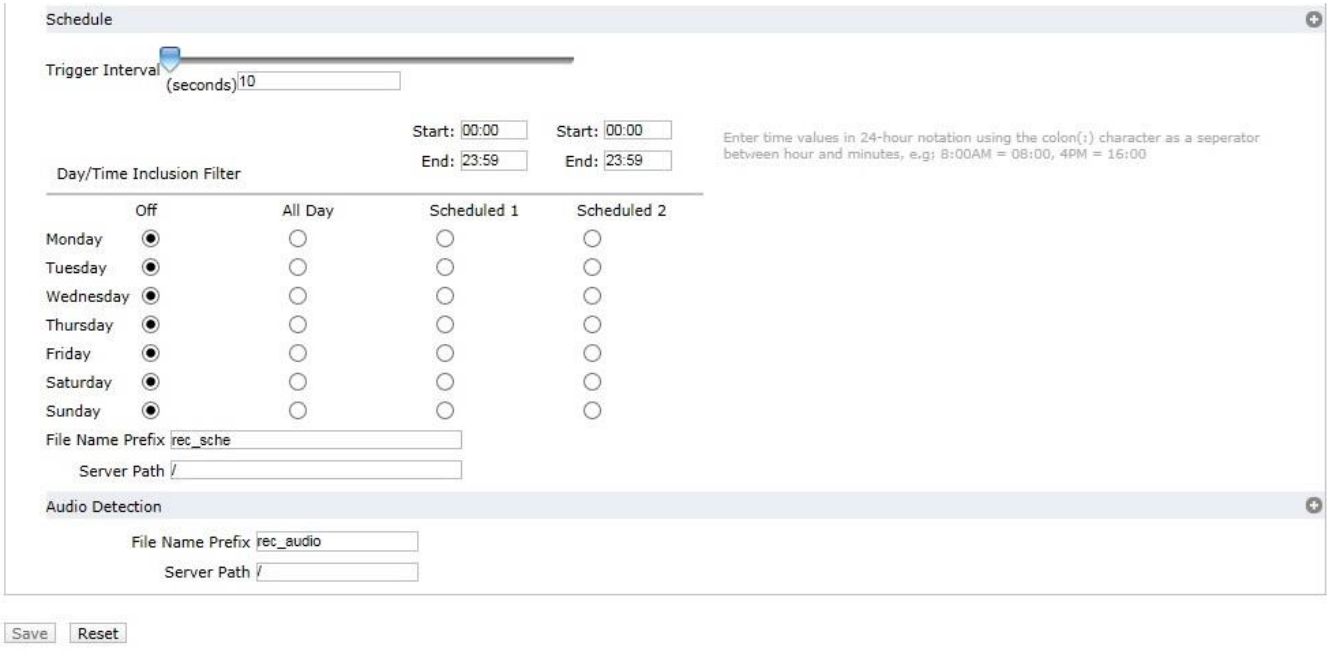


FIGURE 3-43: FTP UPLOAD HANDLER SCHEDULED SETTINGS

3.2.6.5 SD Record Handler

Save video clip backups from a variety of activated events to an SD card. Before using this function, a SD card must be installed in the camera beforehand.

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

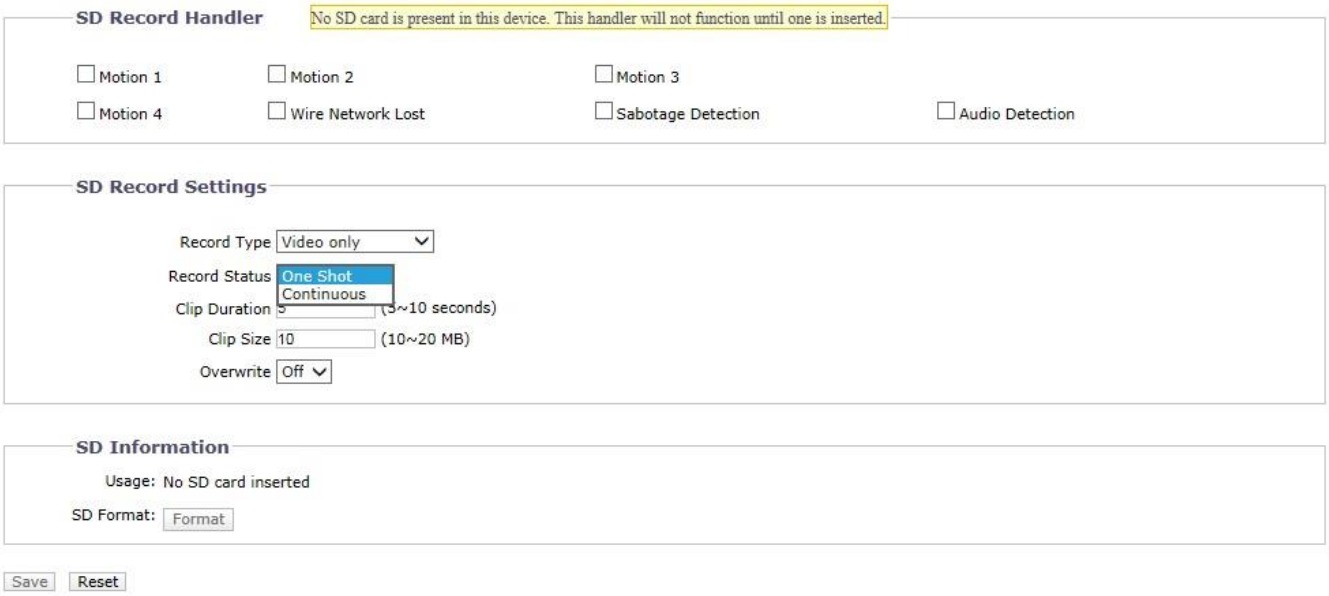


FIGURE 3-44: SD RECORD HANDLER SETTINGS

1. Check to enable **SD Record Handler** for **Motions 1 through 4**, **Wire Network Lost**, **Sabotage Detection**, and **Audio Detection**.
2. Choose either Video only or Audio and Video for **Record Type**, and choose One Shot or Continuous for **Record Status**. Then, set a **Clip Duration** (5~10 seconds) and **Clip Size** (10~20 MB).
   NOTE: It is required to define duration and size parameters for "One Shot" method, whilst only size value needs to be defined for "Continuous" method.
3. Set overwrite **ON** or **Off** to enable or disable the SD card to be **overwritten** automatically when the SD card is full of recordings.
4. **Usage**: Information of SD card usage.
5. **SD Format:** Click Format to erase information off from the SD card.
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.

Viewing SD Card Files from a Remote Server

1. Configure the **SD Record Handler** and **Motion** or **Sabotage Detection** settings.
2. Type "ftp://" followed by the IP address of the camera in a Web browser or Windows Explorer.
3. Right-click on a snapshot or recording from the SD card and save the file locally or open the file to view its content.

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.

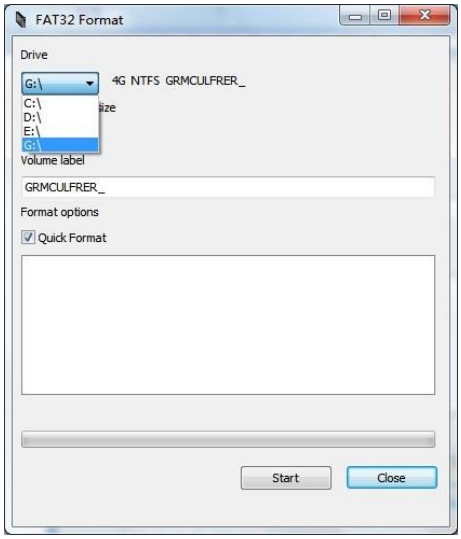


FIGURE 3-45: FAT32 FORMAT

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

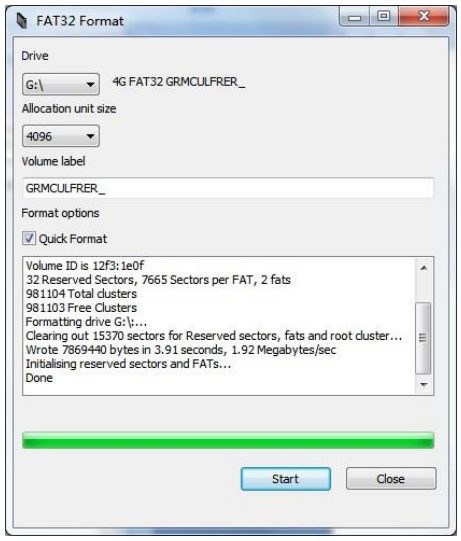


FIGURE 3-46: FAT32 FORMAT COMPLETE

3.2.6.6 SMTP Notification Handler

Set detailed SMTP Notification Handler function that will send an email to predefined email addresses when any or all the selected events are 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.

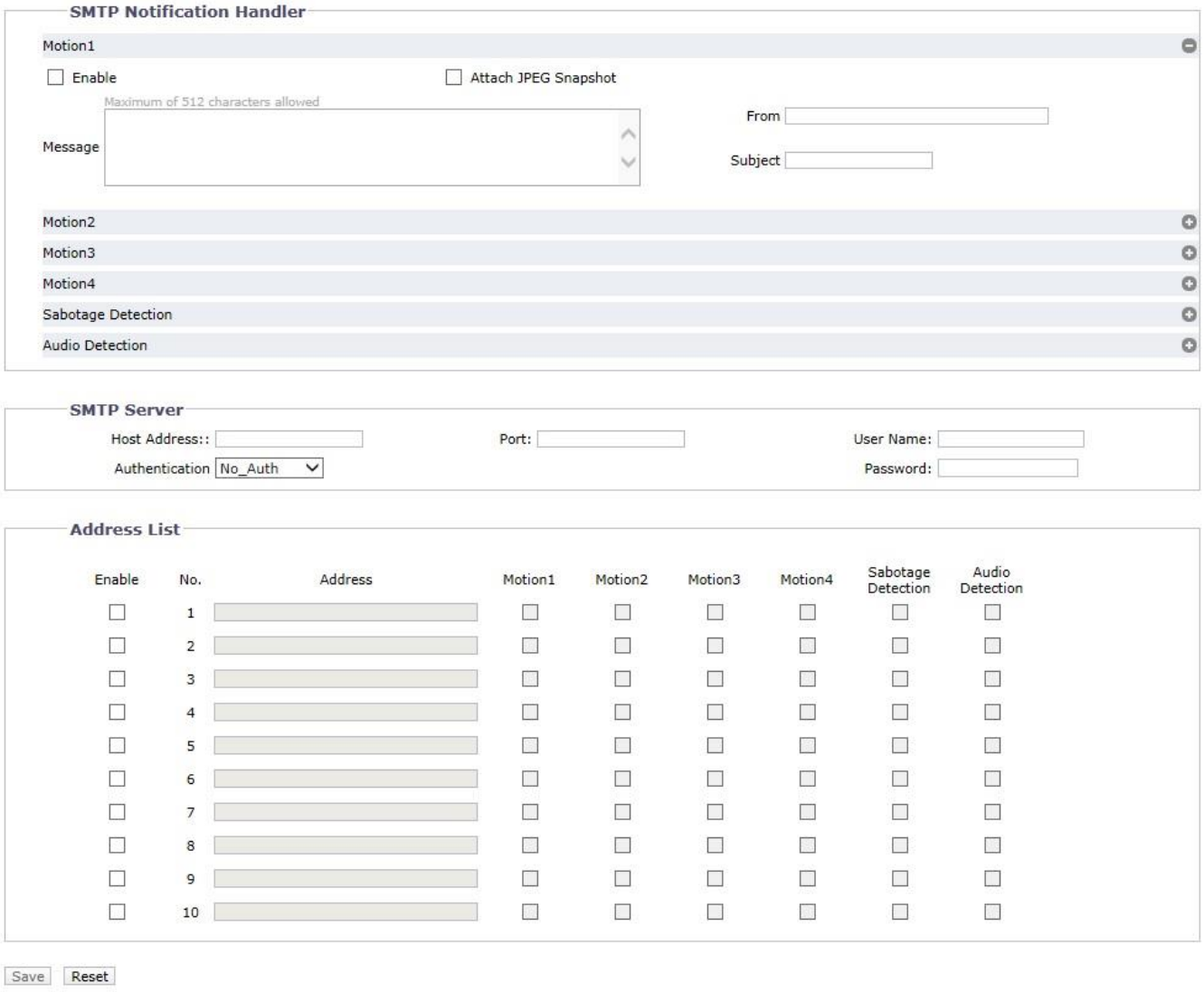


FIGURE 3-47: SMTP NOTIFICATION HANDLER SETTINGS

SMTP Notification Handler

1. Check **Enable** button to enable **SMTP Notification Handler** for **Motions 1 through 4**, **Sabotage Detection, and Audio Detection**.
2. Click in the text boxes (**Message**, **From**, and **Subject**), and then type the necessary information in each text box.
3. Select the **Attach JPEG Snapshot** box if you want to send a JPEG as an attachment.
4. Continue to set the **SMTP Server** and **Address List**.

SMTP Server

Set up Simple Mail Transfer Protocol (SMTP), the Internet standard for electronic mail (e-mail) service across Internet Networking, related settings under this section.

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**.

Address List

This section is designed to notify multiple users via email when the handler condition is set.

1. Check **Enable** and input the E-mail **Address** accordingly.
2. Select **Motions 1 through 4**, **Sabotage Detection**, or **Audio Detection** 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.

3.2.6.7 Sound Notification Handler

This page is designed for configuring detailed settings for sound notifications when an event occurs.

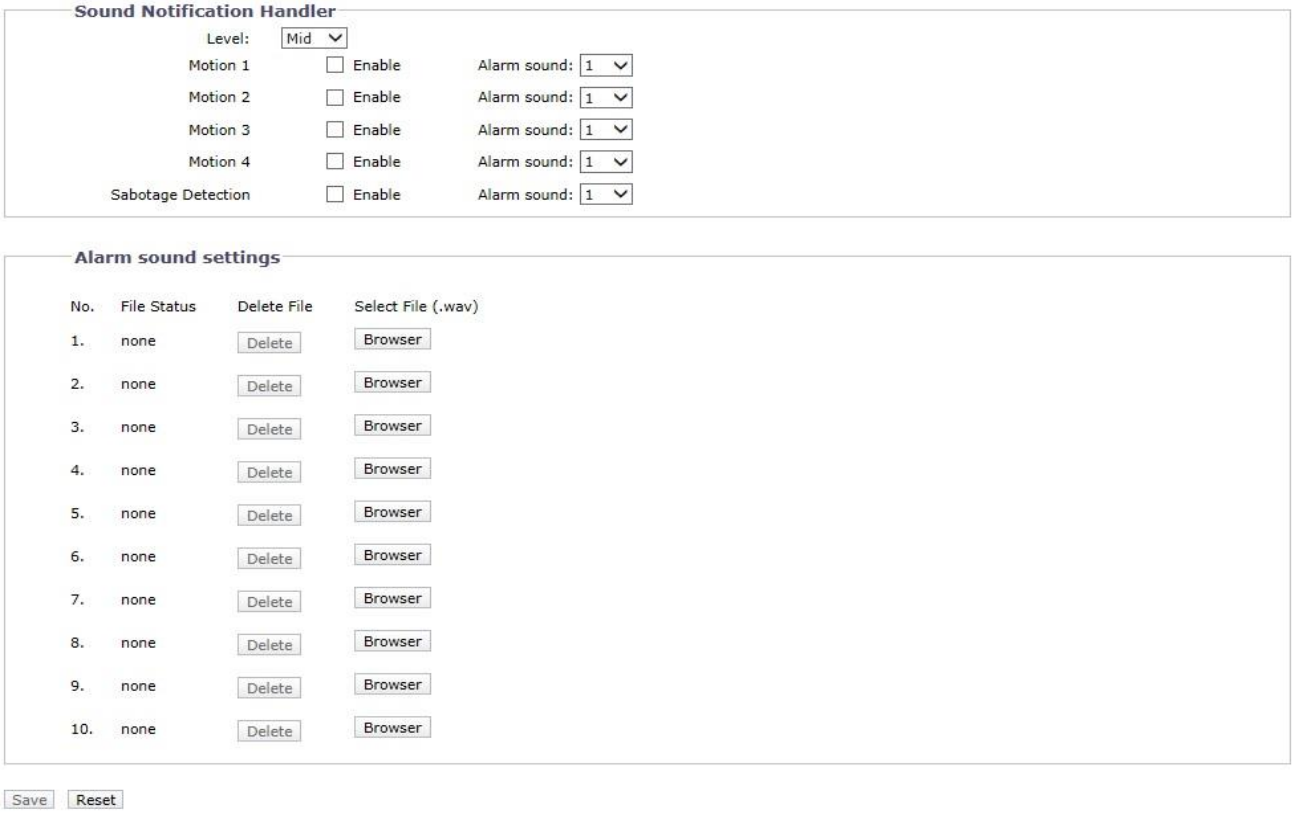


FIGURE 3-48: SOUND NOTIFICATION HANDLER SETTINGS

Sound Notification Handler

1. Select the level ranging from **High**, **Mid** to **Low** of sound notification handlers for different events.
2. Check to enable any or all of Motions 1 through 4 and Sabotage Detection and select one of the ten alarm sounds from the dropdown menu designated for the different events enabled.
3. Continue to set the **Alarm Sound Settings.**

Alarm Sound Settings

1. Customize up to 10 sound files for each event alarm. Click on the **Browser** and locate a desired sound file, which should be specific 8kHz 16bit .wav format, from your computer to upload to the camera. The number will correspond to that under Alarm sound to be selected for the Motion or Sabotage Detection enabled.
2. In the vicinity of each number from the list, the status of the uploaded sound will be displayed under **File Status** (with “none” displayed when no file is uploaded) and the **Delete** button will be enabled. Click on **Delete** to delete the file if necessary.
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.

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.

Pelco, Inc.
625 W. Alluvial Ave.
Fresno, CA 93711
+1 (559) 292-1981 International Phone
(800) 289-9100 USA & Canada Phone
(800) 289-9150 USA & Canada Fax
Pelco.com

Pelco, the Pelco logo, and other trademarks associated with Pelco products referred to in this publication are trademarks of Pelco, Inc. or its affiliates. ONVIF and the ONVIF logo are trademarks of ONVIF Inc. All other product names and services are the property of their respective companies. Product specifications and availability are subject to change without notice. ©Copyright 2019, Pelco, Inc. All rights reserved.