Fisheye Cameras

Operations Manual

Fisheye Cameras:

- Sarix Fisheye 3
- Pelco Fisheye

Document number: C6770M

Publication date: 2026-01-28

Pelco Corporation
pelco.com

C6770M
Revision: 4 – EN
2026-01-28

Contents

Camera Operations Manual

This Operations Manual provides instructions for setting up Fisheye Cameras and configuring their settings. The instructions in this Operations Manual refer to the camera's web interface to complete the steps. You will need the camera's IP address to access the web interface from a web browser.

You can only work on one camera at a time using the web interface. If you are setting up or configuring multiple cameras at once, you should use the Camera Configuration Tool (CCT) instead. See the Camera Configuration Tool User Manual for instructions.

The settings and features available in the web interface depend on the specific device and firmware version. The information in this guide is relevant to Fisheye Cameras using the latest firmware. You can download the latest firmware at https://www.pelco.com/updates.

System Requirements

You can access the web interface from any Windows, Mac, or mobile device using one of the following browsers:

- Microsoft Edge
- Mozilla Firefox
- Google Chrome

Configure your web browser to accept cookies or the web interface will not function correctly.

Other browsers might work but this has not been verified.

Initializing a Camera

The first time you log into a camera it will be in the factory default state. Cameras in the factory default state do not have a default username and password, and the system prompts you to create an account. You can also use a third-party VMS or CCT to initialize the camera and create the first administrator account.

Follow these steps to initialize the camera and create an administrator account:

1. Enter the camera's IP address into your web browser. The system will redirect you to the *Add user* page to create an account.
2. Enter a new **Username** or keep the default administrator name.
3. Enter a new **Username** for the user. We recommend you use a secure and complex password.
4. Confirm the new **Password** by re-entering it.
5. Make sure the **User name (Security group)** is set to Administrator.
6. Click **Save**.

You can now log into the camera.

Live Preview

On the *Live Preview* page, you can preview the live video, check storage status, download saved footage from the SD card and modify basic camera settings to enhance the image quality.

- Zoom in (top button)
- Zoom out
- Click and drag to pan across the scene
- Return to home position
- Zoom level (bottom button)
- Use auto focus
- Turn on or off analytic overlays
- Switch between video streams
- Download stills from camera
- SD card storage status

Downloading Saved Images

If the camera has an SD card installed and SD card storage is turned on, you can download saved images from on the *Live Preview* page.

- Click **Download** in the *Download Still from Camera* area.

The system downloads the files in .JPG format.

Enhancing Camera Image Quality

On the *Live Preview* page, users can enhance the overall image quality. For more image settings, see *Image & Display* on page 41.

Follow these steps to use the image controls:

1. To zoom in, move the **Zoom** slider to the right.
2. To zoom out, move the **Zoom** slider to the left.
3. Click **Auto Focus** to let the camera focus itself.
4. To focus the camera, move the **Focus** slider to the right or left.

Changes are saved automatically.

Enabling Analytics Overlays

On the *Live Preview* page, you can turn on analytics overlays to help visualize the analytic rules. When analytics overlays are turned on, overlays will appear around objects that meet the criteria defined by the analytic rules.

- To turn on analytics overlays, toggle the **Analytics Overlays** option. Changes are saved automatically.

NOTE

You must enable Analytics XML Metadata on the *Extended Settings* page before you can enable analytics overlays. See *Extended Settings* on page 67 for more information.

General

Under *General* settings, administrators can configure settings that apply to the camera's identity and essential functions, e.g., the camera's name, location, power state, and change the camera's mode.

See *Camera Mode* below for instructions on changing the camera's mode.

Editing the Camera's Name and Location

On the *General* page, you can change the camera's name and location. This helps identify the different cameras on the network. You will be able to filter cameras by location in tools like CCT or the VMS. The camera's name and location will appear in the VMS when the camera triggers analytic events and sends notifications.

1. Navigate to the *General* page in the camera's web interface.
2. Enter a new camera name in the **Name** field.
3. Enter a new location in the **Location** field.
4. Click **Save**.

The camera information will change to reflect the new name and location.

Changing the Camera's Power State

On the *General* page, you can change the camera's power state from Aux to PoE.

If the camera is connected to both PoE and an External Aux Power Supply, the camera will draw power from Aux. If you prefer the camera to use PoE, you can manually change the power state to use PoE.

- To change the camera's power state, select the **Force PoE** option from the **Device Power State** drop-down list. Click **Save**.

The camera will transition to using PoE instead of Aux power.

Camera Mode

On the *General* page, you can change the camera mode to prioritize different features on a per camera basis. For example, if you want to increase the framerate on a camera you can set it to High Framerate mode. However, High Framerate mode turns off other features.

You can only change the camera mode on cameras with higher bandwidth usage. You will not see this feature if the camera model does not support it.

1. Navigate to the *General* page in the camera's web interface.
2. In the *Settings* area, click the **Mode** drop-down list and select a different camera mode:
    a. Full feature: Offers the full functionality of the camera. Full feature is the default camera mode.
    b. High Frame Rate: Uses the maximum image rate possible but may disable some features on the camera.
    c. No Video Analytics: Turns off video analytics. This option is for deployments where camera-based video analytics would interfere with other analytics integrations.

d. Dynamic Privacy Masks: Enables dynamic privacy masks. Dynamic Privacy Masks can detect when the object, e.g., a person or vehicle, is moving and adjust so that the object remains masked.

3. Click **Save**.

The camera will reboot after you change the camera mode.

Refresh the browser and log in again once the camera has finished rebooting.

Dewarping Fisheye Cameras

On the *General* page, you can select a dewarp mode to create multiple views from the single Fisheye camera lens. Selecting a dewarp mode in the camera web ui will determine which views shown in a 3rd party VMS.

1. Navigate to the *General* page in the camera's web interface.
2. In the *Settings* area, click the **Mode** drop-down list and select a different mode:
   a. **Dewarp Streaming 90 x 4**: This dewarping mode will transmit 5 streams from the fisheye camera, including the default 360° fisheye stream plus four 90° streams. The four 90° streams comprise of the entire 360° view.
   b. **Dewarp Streaming 120 x 3**: This dewarping mode will transmit 4 streams from the fisheye camera, including the default 360° fisheye stream plus three 120° streams. The three 120° streams comprise of the entire 360° view.
   c. **Dewarp Streaming 180 x 2**: This dewarping mode will transmit 3 streams from the fisheye camera, including the default 360° fisheye stream plus two 180° streams. The two 180° streams comprise of the entire 360° view.
   d. **Dewarp Streaming 180 x 1**dewarp : This dewarping mode will transmit one 180° stream from the fisheye camera, including the default 360° fisheye stream. The 180° stream comprises one half of the entire 360° view. Only available on H6A Fisheye cameras.
3. Click the **Dewarp Streaming Rotation** option and select the rotation of the dewarped Fisheye streams. Calculated in degrees. This setting will only rotate the dewarped streams and will not change the default 360° stream's rotation. Available on H5A Fisheye cameras only.
4. Click **Save**.

Selecting a dewarping mode will produce multiple video streams. The streams are referred to as "heads" in the web interface. You can apply different camera settings to each head individually or to all the heads uniformly.

Time settings

On the *General* page, you can change the camera's time zone to align with its geographic location. This ensures that the camera can synchronize with other devices on the network. Clocks must be synchronized between all of the cameras, devices and servers on the network for the site to operate effectively.

1. Navigate to the *General* page in the camera's web interface.
2. In the *Time settings* area, click the **Time Zone** drop-down list and select the appropriate time zone.
3. You can toggle the **Automatically adjust clock for Daylight Savings Time** to the OFF position if required. However, we recommend keeping this ON.
4. Click **Save**.

The camera's clock will now show the time relative to its time zone.

GPS settings

On the *General* page, you can use the GPS settings to input the camera's geolocation information as decimal values. The GPS information can be useful for mapping and other location-based applications.

1. Navigate to the *General* page in the camera's web interface.
2. In the *GPS settings* area, enter a value in the **Latitude** (-90-90) field.
3. Enter a value for in the **Longitude** (-180-180) field.
4. Enter a value in the **Elevation (meters above sea level)** field, which is calculated in meters above sea level. Only takes positive values.
5. Click **Save**.

The camera will change its GPS coordinates to align with its geographic location.

Network & Security

Under *Network & Security* settings, administrators can change how the camera connects to the server network and camera time syncing behavior.

Changing the Hostname

On the *Network & Security* page, administrators can change the camera's Hostname.

1. Navigate to the *Network & Security* page in the camera's web interface.
2. Edit the text in the **Hostname** field.
3. Click **Save**.

The camera's hostname will be updated.

Turning off DHCP

On the *Network & Security* page, administrators can turn on or off DHCP. DHCP is enabled by default.

1. Navigate to the *Network & Security* page in the camera's web interface.
2. Toggle the **DHCP** button to the OFF position.
3. Click **Save**.

The camera will turn off DHCP.

Turning on IPv6

On the *Network & Security* page, administrators can turn on IPv6 to accommodate more devices on the network.

NOTE

Enabling IPv6 does not disable IPv4 settings.

Follow these steps to turn on IPv6:

1. Navigate to the *Network & Security* page in the camera's web interface.
2. In the **IPv6 Settings** area, select the **Enable** checkbox and click **Apply**. Additional settings will appear.
3. The **Accept Router Advertisements** checkbox should remain selected if you are using Auto as the DHCPv6 state.
4. Select the DHCPv6 State from the drop-down menu:
    a. Auto: DHCPv6 state is determined by router advertisements (RA). The Accept Router Advertisements setting is required for this setting to perform as expected.
    b. Stateless: The camera only receives DNS and NTP information from the DHCPv6 server. It

does not accept an IP address from the DHCPv6 server.

c. Stateful

d. Off

5. Enter the Static IPv6 Addresses.
6. Enter the Default Gateway.
7. Click **Save**.

The camera will turn on IPv6 and the camera will use the new DHCPv6 settings.

Turning Off WS Discovery

On the *Network & Security* page, administrators can turn off WS Discovery. WS Discovery is required for multicast communication and discovery. WS Discovery is enabled by default so cameras can be discovered by CCT or certain VMS's once they are added to the network.

1. Navigate to the *Network & Security* page in the camera's web interface.
2. Uncheck the **Enable WS Discovery Protocol** checkbox to turn off WS Discovery.
3. Click **Save**.

The camera will no longer be discoverable on the network.

TIP

Turn off WS Discovery after you add the camera to the network prevents unlawful actors from discovering the camera and accessing the live stream.

Configuring DNS Lookup Settings

Under *Network & Security* settings, administrators can change the camera's DNS Server address or assign the camera to alternate DNS server.

By default, cameras obtain a DNS Server address automatically.

1. Navigate to the *Network* page.
2. Select **Use the following DNS server address** to manually assign DNS servers.
3. Enter the server address for the Preferred DNS server. This is the first DNS server the camera will try to connect to.
4. Enter the server address for the Alternative DNS server 1. This is the first fall back server.
5. Enter the server address for the Alternative DNS server 2. This is the second fall back server.
6. Click **Save**.

The camera will use the new DNS server and DNS settings.

Configuring Control Ports

On the *Network & Security* page, administrators can configure the Control Port settings to assign certain connection types to certain ports.

Follow these steps to configure the control ports:

1. Navigate to the *Network & Security* page in the camera's web interface.
2. Make sure the **Enable HTTP connections** checkbox is turned on.
3. You can change the ports if required (1..65534). These are the default ports:
    a. HTTP port: 80
    b. HTTPS port: 443
    c. RTSP port: 554
    d. RTSP replay port: 555
    e. WebRTC port: 9090
4. Click **Save**.

The camera will use the new control port settings.

Configuring the NTP Server

On the *Network & Security* page, administrators can configure the External NTP Server Configuration settings so the camera's sync with the NTP server. This ensures the camera retains the correct date and time and prevents time synchronization issues.

Follow these steps to configure the NPT server:

1. Navigate to the *Network & Security* page in the camera's web interface.
2. Select the **Manual** button to manually assign an NTP server.
3. Enter the NTP Server address to assign the server.
4. Click **Save**.

The camera will use the new NPT server and settings.

Adjusting MTU size

On the *Network & Security* page, administrators can adjust the Maximum Transmission Unit (MTU) size to reduce network congestion.

1. Navigate to the *Network & Security* page in the camera's web interface.
2. To adjust the MTU size, enter a value (576 - 1500) in the **MTU size** field. The default is 1500.
3. Click **Save**.

TIP

If the network is slow, you can lower the MTU size to improve network performance.

Changing Ethernet Settings

On the *Network & Security* page, administrators can change the Ethernet settings to turn on duplex and adjust link tolerance.

Follow these steps to adjust the Ethernet settings:

1. Navigate to the *Network & Security* page in the camera's web interface.
2. Select the **Speed/Duplex** drop-down menu and choose **100M full duplex** if you want to turn on duplex.
   The Auto negotiation setting is preferred for most cameras, and will negotiate the optimal speed and duplex setting for your network connection.
3. Select the **Link tolerance** drop-down menu and change the link tolerance percentage. Increasing Link Tolerance means the network can tolerate a wider range of variations before resulting in an error.
4. Click **Save**.

The camera will use the new ethernet settings.

Changing Security Settings

On the *Network & Security* page, administrators can change the minimum TLS version and adjust the login session timeout.

Follow these steps to change the camera's security settings:

1. Navigate to the *Network & Security* page in the camera's web interface.
2. Select the **Minimum TLS version** drop-down list and choose TLS 1.3 if you want to restrict the camera to using a minimum TLS version.
   a. **TLS 1.3** is recommended for increased security.
   b. **TLS 1.2)** can be selected if it is required for backwards compatibility.
3. Enter a the max idle time (minutes) in the **Login session timeout** field before a user is logged out. This helps avoid unauthorized access.
4. Click **Save**.

The camera will use the new TLS version or session timeout.

Configuring SNMP

On the *SNMP* page, administrators can configure the device's SNMP settings and choose the status information that is sent to the management station page. Turning on the SNMP helps manage devices that are connected to the network.

For more details on the status information or traps that will be sent, see the device's Management Information Base (MIB) file on the Pelco website: www.pelco.com/updates.

Follow these steps to enable and configure SNMP:

1. Navigate to *Network & Security* > *SNMP* in the camera's web interface.
2. Toggle **Enable SNMP** to the ON position.
3. Select a different SNMP version from the **Version** drop-down list if required:
    a. SNMP v2c: Use SNMP v2c to make a request to the device for status information through an SNMP Get request and receive trap notifications from the device.
    b. SNMP v3: Use SNMP v2c to make a request to the camera for status information through an SNMP Get request and receive trap notifications from the camera. SNMP v3 offers greater security by allowing you to set a username and password for the camera. This camera uses SHA-1 type authentication and AES type encryption
4. If you selected SNMP v2c, complete these fields:
    a. Read community: Enter the read community name for the device. The name is used to authenticate SNMP traffic. Only SNMP management stations with the same read community name will receive a response from the device.
    b. Write community: Enter the IP address of the management station where the traps will be sent. In the *Available traps* area, select the traps that will be sent. For information on the different types of Traps, see *Available traps* below.
    c. Trap destination IP: Enter the IP address of the management station where the traps will be sent.
5. If you selected SNMP v3, complete the required fields:
    a. Username: Enter the username that the management station must use when sending the SNMP Get request to the camera.
    b. Password: Enter the password the management station must use with the chosen username.
6. Click **Save**.

Available traps

The following Traps are available:

- Temperature alert: A trap notification will be sent when the camera temperature rises above or falls below the supported threshold. A notification will also be sent when the camera temperature returns to normal.
- The camera will alert you when it is being tampered with.: A trap notification will be sent when the camera detects human tampering.
- The camera will alert you when its out of storage space.: A trap notification will be sent when the status of the SD card changes.

Configuring DSCP

On the *DSCP* page, administrators can turn the DSCP feature on or off, choose values for the traffic types listed below, and restore the default values. This helps manage network traffic and provides quality of service (QoS) on modern IP networks. DiffServ can be used to lower latency to critical network traffic, such as voice or streaming media, while providing simplified best-effort service to non-critical services, such as web traffic or file transfers.

For Primary, Secondary, Tertiary, and Replay Stream, it is very important to prepare and set up stream traffic. In case of stream over TCP (one common socket with RTSP), the DSCP value will be taken from the Primary stream and propagated to the other streams. Setting up a stream over UDP enables the user to specify different DSCP values for all streams.

Follow these steps to configure DSCP:

1. Navigate to *Network & Security* > *DSCP* in the camera's web interface.
2. Toggle **Activate feature** if it is not already enabled. DSCP is enabled by default.
3. In the **Onvif protocol** drop-down menu, click to select one of the options:
    a. DF (0)
    b. CS2 (16) (This is the default option)
4. In the **Web interface** drop-down menu, click to select one of the options:
    a. DF (0)
    b. AF21 (18) (This is the default option)
5. In the **SNMP** drop-down menu, click to select one of the options:
    a. DF (0)
    b. CS2 (16) (This is the default option)
6. In the **Primary stream** drop-down menu, click to select one of the options:
    a. CS3 (24)
    b. AF31 (26)
    c. CS4 (32)
    d. AF41 (34) (This is the default option)
7. In the **Secondary stream** drop-down menu, click to select one of the options:
    a. CS3 (24)
    b. AF31 (26)
    c. CS4 (32)
    d. AF41 (34) (This is the default option)
8. In the **Tertiary stream** drop-down menu, click to select one of the options:
    a. CS3 (24) (This is the default option)
    b. AF33 (30)
9. In the **Replay stream** drop-down menu, click to select one of the options:

a. CS3 (24) (This is the default option)
b. AF33 (30)
c. CS4 (32)
d. AF43 (38)

10. Click **Save**.

Restoring Defaults

- Administrators can use the **Restore Defaults** option if you need to restore the default settings. Click **Save**.

Configuring Firewall Settings

On the *Firewall* page, administrators can allow or deny access to certain IP addresses.

1. Navigate to *Network & Security* > *Firewall* in the camera's web interface.
2. Firewall is OFF by default. To allow access to certain IP addresses, select **Allow**.
3. To deny access to certain IP addresses, select Deny.
4. Enter an IP address into the field.
5. Click Add new address to add more IP addresses.
6. Click **Save**.

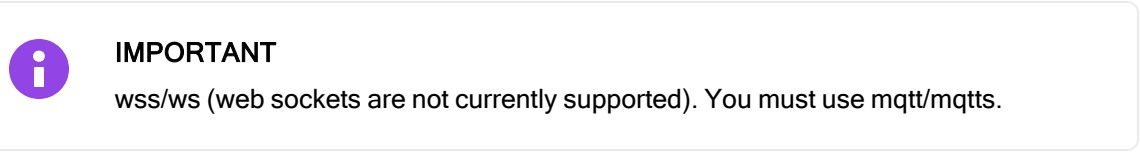
The Firewall settings will become active immediately.

Adding New MQTT Brokers

On the *MQTT Brokers* page, administrators can add new MQTT brokers. Using MQTT brokers will help in constrained environments when there are multiple sensors connected to the cameras.

Follow these steps to add a new broker:

1. Navigate to *Network & Security* > *MQTT Brokers* in the camera's web interface.
2. Click **Add new broker**.
3. For **AddressAddress**: enter the network address of the event broker. The format scheme://host:port indicates the protocol to be used (e.g., mqtt://, mqtts://), the hostname or IP address of the broker, and the port number for the connection.



4. For **Topic prefix**: enter the string that is prepended to all topics for events published to this broker. This allows for easier filtering and management of topics on the broker, especially in environments with multiple ONVIF devices. For example, if the prefix is onvif/device1, an event with the topic VideoSource/MotionAlarm would be published to onvif/device1/VideoSource/MotionAlarm.
5. For **Username** and **Password**: used for authentication with the event broker. If the broker requires a username and password for clients to connect, they should be entered here.

6. For **Certificate ID**: specifies the identifier of a client-side certificate to be used for TLS authentication with the broker. This is used when the broker requires clients to present a certificate to espagelish a secure connection.

   > **IMPORTANT**
   >
   > Certificates are selected from the list of saved Certificates under *Network & Security* > *Identity & Trust*.

7. For **QoS**: QoS stands for Quality of Service and is a setting that determines the guarantee of message delivery. It typically has the following levels: 0 (At most once): The message is sent once, with no confirmation of receipt. This is the fastest but least reliable level. 1 (At least once): The message is guaranteed to be delivered at least once, but it may be delivered more than once. 2 (Exactly once): The message is guaranteed to be delivered exactly once. This is the most reliable but also the slowest level.
8. For **Publish Filter**: allows you to select which categories of events will be sent to the broker. By checking the boxes next to event sources like Encryption Engine, Device, Video Source, etc., you can control the flow of event messages and reduce unnecessary network traffic.
9. For **Certificate Path Validation Policy**: specifies the identifier of a policy to be used for validating the certificate chain of the event broker. This is important for ensuring that the client is connecting to a trusted and authentic broker. Important: The ui allows you to select validation policies from the list of created/added on ui via certificates page.
10. Click **Add**.

The new broker will appear in the list. You can view the Address, Status and Actions in the *Brokers* list.

Publish Filters

Item	Description
Encryption Engine	Core component responsible for executing encryption/decryption operations.
Encryption Engine Update	An event or process indicating a firmware or software update to the encryption module.
Available Encryption Modes	A list of supported encryption protocols (e.g., AES, TLS versions).
Device	General representation of the physical unit itself.
Trigger	An input or signal that initiates a specific action or event.
Relay	An electrical output used to control external devices (e.g., lights, door locks).
Digital Input	An electrical input used to sense external signals (e.g., door contact, alarm sensor).
Digital Input	(Duplicate entry) Another instance of a digital input.
Illumination	Settings or status related to light sources (e.g., IR LEDs, white light).
User Configuration Update	A mechanism used to specify which events and configuration changes are published (sent out) to external subscribers/clients. It prevents unnecessary data traffic.
Logs	Records of system activities, errors, and events.
Configuration	The general settings or parameters of the device.
Schedule	Defined periods for specific actions (e.g., recording, event activation).
Changed	General notification that a parameter or state has been altered.
Removed	General notification that an item or configuration has been deleted.
Schedule	(Duplicate entry) Defined periods for specific actions.
State	The current operational status (e.g., running, idle, error).
Active	Indicates that a function, process, or setting is currently operational.
PTZ Controller	Component that manages Pan, Tilt, and Zoom movements of a camera.
PTZ Preset Tours	Defined sequence of preset camera positions for automatic tour.
Configuration	(Duplicate entry) General settings or parameters.
Video Source	The physical or logical channel providing video data (the camera lens).
Motion Alarm	An event triggered by the detection of movement in the video stream.
Global Scene Change	An event indicating a significant, broad change in the camera's field of view (e.g., camera moved).
Analytics Service	The subsystem responsible for video content analysis (e.g., detection, tracking).
Media	Refers to the video and audio streams themselves.

Item	Description
Profile Changed	Notification that a saved set of settings (profile) has been modified.
Configuration Changed	Publishes Configuration Changed information to external subscribers/clients, limiting unnecessary data traffic.
Media Control	Publishes Media Control information to external subscribers/clients, limiting unnecessary data traffic.
Configuration Update Profiles	Publishes Configuration Update Profiles to external subscribers/clients, limiting unnecessary data traffic.
Configuration Update Presets	Publishes Prohibited Direction information to external subscribers/clients, limiting unnecessary data traffic.
Configuration Update Preset Tours	Publishes Configuration Update Preset Tours information to external subscribers/clients, limiting unnecessary data traffic.
Configuration Update Network Protocols	Publishes Configuration Update Network Protocols information to external subscribers/clients, limiting unnecessary data traffic.
Configuration Update Led Enabled	Publishes Configuration Update Led Enabled information to external subscribers/clients, limiting unnecessary data traffic.
Configuration Update Ir Led Allowed	Publishes Configuration Update Ir Led Allowed information to external subscribers/clients, limiting unnecessary data traffic.
Configuration Update Ip Cam Mode	Publishes Configuration Update Ip Cam Mode information to external subscribers/clients, limiting unnecessary data traffic.
Configuration Update Profile	Publishes Configuration Update Profile information to external subscribers/clients, limiting unnecessary data traffic.
Configuration Update Video Src	Publishes Configuration Update Video Src information to external subscribers/clients, limiting unnecessary data traffic.
Configuration Update Video Src Cfg	Publishes Configuration Update Video Src Cfg information to external subscribers/clients, limiting unnecessary data traffic.
Configuration Update Video Src Cfg Options	Publishes Configuration Update Video Src Cfg Options information to external subscribers/clients, limiting unnecessary data traffic.
Configuration Update Video Enc Cfg	Publishes Configuration Update Video Enc Cfg information to external subscribers/clients, limiting unnecessary data traffic.
Configuration Update Video Enc Cfg Options	Publishes Configuration Update Video Enc Cfg Options information to external subscribers/clients, limiting unnecessary data traffic.
Configuration Update Audio Src	Publishes Configuration Update Audio Src information to external subscribers/clients, limiting unnecessary data traffic.
Configuration Update Audio Src Cfg	Publishes Configuration Update Audio Src Cfg information to external subscribers/clients, limiting unnecessary data traffic.
Configuration Update Audio Src Cfg Options	Publishes Configuration Update Audio Src Cfg Options information to external subscribers/clients, limiting unnecessary data traffic.
Configuration Update Audio Enc Cfg	Publishes Configuration Update Audio Enc Cfg information to external subscribers/clients, limiting unnecessary data traffic.
Configuration Update Audio Enc Cfg Options	Publishes Configuration Update Audio Enc Cfg Options information to external subscribers/clients, limiting unnecessary data traffic.
Configuration Update Audio Out	Publishes Configuration Update Audio Out information to external subscribers/clients, limiting unnecessary data traffic.
Configuration Update Audio Out Cfg	Publishes Configuration Update Audio Out Cfg information to external subscribers/clients, limiting unnecessary data traffic.
Configuration Update Audio Out Cfg Options	Publishes Configuration Update Audio Out Cfg Options information to external subscribers/clients, limiting unnecessary data traffic.

Item	Description
Configuration Update Audio Dec Cfg	Publishes Configuration Update Audio Dec Cfg information to external subscribers/clients, limiting unnecessary data traffic.
Configuration Update Audio Dec Cfg Options	Publishes Configuration Update Audio Dec Cfg Options information to external subscribers/clients, limiting unnecessary data traffic.
Configuration Update Metadata Cfg	Publishes Configuration Update Metadata Cfg information to external subscribers/clients, limiting unnecessary data traffic.
Configuration Update Metadata Cfg Options	Publishes Configuration Update Metadata Cfg Options information to external subscribers/clients, limiting unnecessary data traffic.
Configuration Update Video Analytics Cfg	Publishes Configuration Update Video Analytics Cfg information to external subscribers/clients, limiting unnecessary data traffic.
Configuration Update Ptz Cfg	Publishes Configuration Update Ptz Cfg information to external subscribers/clients, limiting unnecessary data traffic.
Configuration Update Ptz Cfg Options	Publishes Configuration Update Ptz Cfg Options information to external subscribers/clients, limiting unnecessary data traffic.
Configuration Update Scopes	Publishes Configuration Update Scopes information to external subscribers/clients, limiting unnecessary data traffic.
Configuration Update Digital Input	Publishes Configuration Update Digital Input information to external subscribers/clients, limiting unnecessary data traffic.
Configuration Update Relay Output	Publishes Configuration Update Relay Output information to external subscribers/clients, limiting unnecessary data traffic.
Configuration Update Imaging Settings20	Publishes Configuration Update Imaging Settings20 information to external subscribers/clients, limiting unnecessary data traffic.
Configuration Update Imaging Options20	Publishes Configuration Update Imaging Options20 information to external subscribers/clients, limiting unnecessary data traffic.
Configuration Update Thermal Cfg	Publishes Configuration Update Thermal Cfg information to external subscribers/clients, limiting unnecessary data traffic.
Configuration Update Network Protocol	Publishes Configuration Update Network Protocol information to external subscribers/clients, limiting unnecessary data traffic.
Configuration Update Patterns	Publishes Configuration Update Patterns information to external subscribers/clients, limiting unnecessary data traffic.
Configuration Update Serial Port Options	Publishes Configuration Update Serial Port Options information to external subscribers/clients, limiting unnecessary data traffic.
Configuration Update Serial Port Settings	Publishes Configuration Update Serial Port Settings information to external subscribers/clients, limiting unnecessary data traffic.
Configuration Update Video Src Ptz Settings	Publishes Configuration Update Video Src Ptz Settings information to external subscribers/clients, limiting unnecessary data traffic.
Configuration Update Preset Tour Options	Publishes Configuration Update Preset Tour Options information to external subscribers/clients, limiting unnecessary data traffic.
Configuration Update Radiometric Rule Overlay Cfg	Publishes Configuration Update Radiometric Rule Overlay Cfg information to external subscribers/clients, limiting unnecessary data traffic.

Item	Description
Recording Config	Settings that define how video/audio is recorded (e.g., quality, retention).
Job State	The current status of a defined task, such as a recording session.
Recording Configuration	(Duplicate entry) Settings for recording.
Track Configuration	Settings for managing and indexing recorded data segments (tracks).
Recording Job Configuration	Detailed setup for an automated recording task.
Delete Track Data	A command to remove a segment of recorded data.
Create Recording	A command to initiate a new recording job or session.
Delete Recording	A command to remove a recording job or its associated data.
Create Track	A command to define or start a new recorded track segment.
Delete Track	A command to remove a specific recorded track.
Rule Engine	The core component that processes events and triggers resulting actions based on defined rules.
Object Unusual Direction	Publishes Object Unusual Direction events to external subscribers/clients, limiting unnecessary data traffic.
Motion Detection	Publishes Motion Detection events to external subscribers/clients, limiting unnecessary data traffic.
Object Unusual Speed	Publishes Object Unusual Speed events to external subscribers/clients, limiting unnecessary data traffic.
Object Unusual Location	Publishes Object Unusual Location events to external subscribers/clients, limiting unnecessary data traffic.
Objects In Area Autotrack	Publishes Objects In Area Autotrack events to external subscribers/clients, limiting unnecessary data traffic.
Smart Motion	Publishes Smart Motion events to external subscribers/clients, limiting unnecessary data traffic.
Prohibited Direction	Publishes Prohibited Direction events to external subscribers/clients, limiting unnecessary data traffic.
Object Stops	Publishes Object Stops events to external subscribers/clients, limiting unnecessary data traffic.
Object Loitering	Publishes Object Loitering events to external subscribers/clients, limiting unnecessary data traffic.
Object Appears	Publishes Object Appears events to external subscribers/clients, limiting unnecessary data traffic.
Object Disappears	Publishes Object Disappears events to external subscribers/clients, limiting unnecessary data traffic.
Object Crosses	Publishes Object Crosses events to external subscribers/clients, limiting unnecessary data traffic.
Object Present	Publishes Object Present events to external subscribers/clients, limiting unnecessary data traffic.
Line Detector	Publishes Line Detector events to external subscribers/clients, limiting unnecessary data traffic.
Crossed	Publishes Crossed events to external subscribers/clients, limiting unnecessary data traffic.
Camera Tampering	Publishes Camera Tampering events to external subscribers/clients, limiting unnecessary data traffic.
Object Leaves	Publishes Object Leaves events to external subscribers/clients, limiting unnecessary data traffic.
Object Enters	Publishes Object Enters events to external subscribers/clients, limiting unnecessary data traffic.

Item	Description
Loitering Detector	Publishes Loitering Detector events to external subscribers/clients, limiting unnecessary data traffic.
Object Is Loitering	Publishes Object Is Loitering events to external subscribers/clients, limiting unnecessary data traffic.
Object Not Present	Publishes Object Not Present events to external subscribers/clients, limiting unnecessary data traffic.
Field Detector	Publishes Field Detector events to external subscribers/clients, limiting unnecessary data traffic.
Objects Inside	Publishes Objects Inside events to external subscribers/clients, limiting unnecessary data traffic.
Ip Filter	A rule set to allow or deny network traffic based on IP address.
Unauthorized Access Attempt	Publishes Unauthorized Access Attempt events to external subscribers/clients, limiting unnecessary data traffic.
Advancedsecurity	General component or settings related to enhanced security features.
Keystore	A repository for cryptographic keys and certificates.
Key Status	The current state of a cryptographic key (e.g., active, revoked, expired).

Configuring SMTP Settings

On the *SMTP* page, administrators can configure SMTP settings.

Follow these steps to configure SMTP settings:

1. Navigate to *Network & Security* > *SMTP* in the camera's web interface.
2. Enter the Server URL in this format: smtps://smtp.gmail.com:465, e.g., smtps://server.company.com:465.
3. Enter the Username and Password.
4. Enter the Sender Email Address, e.g., <user@example.com>.
5. Click **Save**.

The SMTP server settings will change.

Managing Network Access Using IP Filters

On the *IP Filter* page, administrators can control which IP addresses are able to connect to your camera. The IP filter limits access to certain IP addresses by either denying access to certain IP addresses or restricting access to certain IP addresses. You can also include deny or permit access to ranges of IP addresses.

> **IMPORTANT**
> If you choose to filter IP access using the Allow access option, make sure that you configure the correct addresses to be allowed or you may be locked out of your camera.

Administrators can configure 802.1x port-based authentication to set up the appropriate camera credentials so the video stream is not blocked by the switch.

Follow these steps to use the IP Filter:

1. Navigate to *Network & Security* > *IP Filter* in the camera's web interface.
2. Toggle the **Enable IP filter** button to enable IP filter.
3. Select the **Allow access** option to allow access to a limited number of IP addresses.
4. Select the **Deny access** option to deny access to a limited number of IP addresses.
5. In the IP filter entries area, click the **+** icon to add IP addresses.
6. Enter the IP address in the field.
7. Continue clicking the **+** icon to add IP addresses. You can add up to 256 IP filter entries.
8. You can select the **–** icon to remove IP addresses from the list of entries.
9. Click **Save**.

Restoring Defaults

- Administrators can use the **Restore Defaults** option if you need to restore the default settings. Click **Save**.

Configuring WebRTC

On the *WebRTC* page, administrators can enable WebRTC using either STUN or TURN servers. You can configure WebRTC by adding either STUN or TURN servers. Typically, you would use STUN servers unless client IP addresses or server port numbers are hidden on the network, i.e., firewalls.

Follow these steps to configure WebRTC:

1. Navigate to *Network & Security* > *WebRTC* in the camera's web interface.
2. In the *General Settings* area, select which type of servers you want to use:
   a. STUN servers: uses direct communication between WebRTC clients using public IP addresses and ports.
   b. TURN servers: provides a fallback when there is a lack of direct communication.

   > **NOTE**
   > You must turn off HTTP connections if you want to manage and use TURN servers.
3. If you are using STUN servers, enter the STUN server address using this format: stun[s] : <host> [:<port>]
4. If you are using TURN servers, enter the STUN server address using this format: turn[s]: <host> [: <port>] [?transport =<protocol>]
5. Use the **Add STUN Server** or **Add TURN Server** button to continue adding server addresses.
6. Click **Save**.

The new server will be added to the list.

Removing Servers

- Administrators can remove a server by selecting the 🗑 icon to remove it. Click **Save**.

Configuring 802.1x Profiles

On the *802.1x* page, administrators can configure profiles and manage saved 802.1x configurations. You can configure 802.1x port-based authentication to set up the appropriate camera credentials so the video stream is not blocked by the switch. This allows administrators to manage access to the video stream.

Follow these steps to configure 802.1x profiles:

1. Navigate to *Network & Security* > *802.1x* in the camera's web interface.
2. In the *Configure 802.1X profiles* area, click the **Protocol** drop-down list and select a different protocol:
   a. PEAP: For username and password authentication.
   b. EAP-TLS: For certificate authentication.
3. If you selected PEAP, complete the required fields:

   a. Configuration name**:** Give the profile a name.
   b. Identity: Enter the username that will be used to authenticate the camera.
   c. Password**:** Enter the password that will be used to authenticate the camera.
   d. Authenticate Server: check this box if you need to add a certificate.
4. If you selected EAP-TLS, complete the required fields:
   a. Configuration name**:** Give the profile a name.
   b. Identity: Enter the username that will be used to authenticate the camera.
   c. certTLS: Select the PEM-encoded certificate file to authenticate the camera.
   d. Private key: Select the PEM-encoded private key file to authenticate the camera.
   e. Private key password: If the private key has a password, enter the password here.
5. Click **Upload File** and the TLS client certificate and private key are uploaded to the camera. The uploaded files are used to generate a unique certificate to authenticate the camera. The unique certificate is displayed in the **Uploaded certificate** field.
6. Click **Save**.

If this is the first profile added to the camera, it is automatically enabled.

Saved configurations are listed under Saved 802.1X configurations. To switch between authentication profiles or delete them, see *Managing Saved 802.1x Configurations* below.

Managing Saved 802.1x Configurations

Administrators can manage your authentication profiles in the *Configure 802.1X profiles* area:

- To select a different authentication profile, select the saved configuration then click **Enable**.
- To delete one of the authentication profiles, select the saved configuration then click **Remove**.

These changes will be saved automatically.

Changing the Encryption Engine

On the *Encryption Engine* page, administrators can change encryption methods to enable FIPS compliance or NXP TPM.

Follow these steps to change the encryption engine:

1. Navigate to *Network & Security* > *Encryption Engine* in the camera's web interface.
2. In the *Security* area, select an option from the **Encryption Engine** drop-down list:
   a. Network: FIPS is not enabled. OpenSSL is enabled by default.
   b. FIPS 140-2: FIPS 140-2 is enabled.
   c. FIPS 140-3: FIPS 140-3 level 1 is enabled by putting the OpenSSL library into FIPS mode.
   d. NXP TPM: FIPS 140-2 level 3 is enabled by using the TPM. For newer cameras with FIPS 140-3 TPM, this option enables FIPS 140-3 level 3 instead.

   NOTE
   In the event of a TPM error, you will see the following message: "Trusted Platform Module tamper error. This camera is untrusted. Power cycle is required." You must reboot the camera to resolve the issue. The camera can still record footage until rebooted. See *System* on page 73 for instructions.
3. Click **Save**.

IMPORTANT
Changing this setting on your camera will require your camera to reboot and you will lose the video stream for that time. We recommend that you apply this setting during non-critical operating times.

Licensing FIPS

You must purchase a FIPS camera license to use these FIPS encryption engines:

- FIPS 140-2 Level 1
- FIPS 140-2 Level 3 on cameras with an onboard TPM
- FIPS 140-3 Level 3 on cameras with an onboard TPM

Contact Sales Representative at Pelco to provision additional licenses.

Managing Camera or Device Access Using Certificates

On the *Identity & Trust* page, administrators can add certificates, download certificates, view details, or download a Certificate Signing Request (CSR). Some certificates cannot be deleted, such as preloaded certificates provided with third-party libraries or those with a "preloaded" prefix from MPI (in the future).

Certificate Information

The *Certificates* pagele lists all certificates on the camera along with the following information:

- Name: The Certificate name.
- Type: The type of certificate, i.e., trusted or not trusted.
- Expiry Date: The date that the certificate will expire.

Adding a New Certificate

On the Certificates page, administrators can create new certificates for authentication.

Uploading a Self-Signed Certificate

You can upload a self-signed certificate for authentication.

1. Navigate to *Network & Security* > *Certificates* in the camera's web interface.
2. Click **Add new certificate**.
3. To create a self-signed certificate, click **Next**.
    a. Enter the Name: The certificate name. This field is required.
    b. Enter the Common Name: The primary hostname of the server. This field is required.
    c. Enter the Valid through (years): The number of years the certificate is valid for.
    d. Enter the Country: The Country where the organization is located.
    e. State or Province: The State (United States) or Province (Canada) associated with the organization.
    f. Enter the City or Locality (if required): The geographic locality of the organization.
    g. Enter the Organization (if required): The name of the organization requesting the certificates.
    h. Enter the Organizational Unit (if required): The name of the unit within the organization that is requesting the certificates.
    i. Select a Key Type: Select from the list of Key types.
4. Click **Next**.
5. If you want to create a new validation path using just this certificate, select the **Yes, create a new validation path upon Save** checkbox.

    NOTE

    If you want to create a Certificate Validation Path with additional certificates, switch to the *Certificate Validation Path* page. See *Certificate Validation Paths* on page 36 for instructions.

6. Click **Save**.

Activating the new certificate will deactivate any certificates that were being used by the same service.

Uploading a Client-Server Certificate Using a Signing Request

Administrators can upload a client-server certificate for authentication.

1. Click **Add new certificate**.
2. To create a self-signed certificate, click **Next**.
3. To upload a client-server certificate created using a signing request, select **Upload a client-server certificate created using a signing request** and click **Next**.
    a. Enter the Name: The certificate name. This field is required.
    b. Enter the Common Name: The primary hostname of the server. This field is required.
    c. Enter the Valid through (years): The number of years the certificate is valid for.
    d. Enter the Country: The Country where the organization is located.
    e. State or Province: The State (United States) or Province (Canada) associated with the organization.
    f. Enter the City or Locality (if required): The geographic locality of the organization.
    g. Enter the Organization (if required): The name of the organization requesting the certificates.
    h. Enter the Organizational Unit (if required): The name of the unit within the organization that is requesting the certificates.
    i. Select a Key Type: Select from the list of Key types.
4. Click **Next**.
5. If you want to create a new validation path using just this certificate, select the **Yes, create a new validation path upon Save** checkbox.

    NOTE

    If you want to create a Certificate Validation Path with additional certificates, use the *Certificate Validation Path* page. See *Certificate Validation Paths* on page 36 for instructions.
6. Click **Save**.

Activating the new certificate will deactivate any certificates that were being used by the same service.

Uploading a Client-Server Certificate Using PKCS#12

Administrators can upload a client-server certificate for authentication using PKCS#12.

1. Click **Add new certificate**.
2. To upload a client-server certificate with private key using PKCS#12, select **Upload a client-server certificate with private key using PKCS#12** and click **Next**.
3. Enter the Name: The certificate name. This field is required.
4. Select **Click to upload certificate file** and chose a file on the local machine.
5. Click **Next**.
6. Click the **Click to upload certificate file** button and select the .p12 or .pfx file on your local computer.
7. Enter the Password if required. If a password is not required, uncheck the **Password** button.
8. Click **Next**.
9. Click **Save**.

Activating the new certificate will deactivate any certificates that were being used by the same service.

Uploading a Client-Server Certificate Using PKCS8

Administrators can upload a client-server certificate for authentication using PKCS8:

1. Click **Add new certificate**.
2. To upload a client-server certificate with private key using PKCS8, select **Upload a client-server certificate with private key using PKCS8** and click **Next**.
3. Enter the Name: The certificate name. This field is required.
4. Select **Click to upload certificate file** and chose a file on the local machine.
5. Select **Click to upload a key file** and chose a file on the local machine.
6. Enter the password if required.
7. If a password is not required, deselect the **Password** checkbox.
8. Click **Next**.
9. Click the **Click to upload certificate file** button and select the .pem, .crt, .cer or .der file on your local computer.
10. Click the **Click to upload key file** button and select the .key, .pem, or .rsa file on your local computer.
11. Enter the Password if required. If a password is not required, uncheck the **Password** button.
12. Click **Next**.
13. Click **Save**.

Activating the new certificate will deactivate any certificates that were being used by the same service.

Uploading a CA Certificate

Administrators can upload a CA certificate for authentication.

1. Click **Add new certificate**.
2. To upload a CA certificate, select **CA certificate** and click **Next**.
3. Enter the Name: The certificate name. This field is required.
4. Select **Click to upload certificate file** and chose a file on the local machine.
5. Click **Next**.
6. Click the **Click to upload certificate file** button and select the .pem, .crt, .cer or .der file on your local computer.
7. Click **Next**.
8. Click **Save**.

Activating the new certificate will deactivate any certificates that were being used by the same service.

Downloading Certificate Signing Requests

On the *Identity & Trust* page, administrators can download certificate signing requests.

1. Navigate to *Network & Security* > *Identity & Trust* in the camera's web interface.
2. Click **Download CSR** and enter the following information:
   - Common Name: The primary hostname of the server. This field is required.
   - Subject Alternative Name (DNS): The alternative values associated with the certificate, e.g., email address, IP addresses, URIs, DNS names.
   - Organizational Unit: The name of the unit within the organization that is requesting the certificates.
   - Organization: The name of the organization requesting the certificates.
   - Locality: The geographic locality of the organization.
   - State or Province: The State (United States) or Province (Canada) associated with the organization.
   - Country: The Country where the organization is located.
3. Click the **Download** button to download the Certificate Signing Request.
4. Click **Save**.

The Certificate Signing Request will download as a .CSR file.

Certificate Validation Paths

On the *Certificate Validation Paths* page, administrators can add new paths and manage saved paths. Administrators can select from the saved certificate validation paths on the *TLS* page. See *Changing Certificate Validation Paths* on page 38 for more information. Access the *Certificate Validation Paths* page on the *Identity & Trust* page.

Add new certificate validation paths in the following order:

- Place Root CA first
- Place Intermediate CA in between (optional)
- Place End-Entity last

Adding a New Certificate Validation Path

Administrators can upload a new Certificate Validation Path.

1. Navigate to *Network* > *Identity & Trust* > *Certificate Validation Paths* in the camera's web interface.
2. Click **Add New Path**.
3. Enter a name for the path in the Path Details.
4. Search through the list of Available Certificates and select the certificates you want to add.
5. Use the > button to move the certificates to the Certificate Path Order area on the right.
6. Use the < button if you need to move certificates back to the Available Certificate area on the left.
7. Click and drag the ⠿ icon to reorder the list of certificates.
8. Click **Save**.

The new certificate validation path will be added to the list.

Managing Certificate Validation Paths

Administrators can manage Certificate Validation Paths using the options in the list:

- To view a Certificate Validation Paths, click the ⋮ icon and select **View**.
- To delete a Certificate Validation Paths, click the ⋮ icon and select **Delete**.

Administrators cannot delete a certificate validation path if the camera is currently using it.

Adding and Managing Certificate Validation Policies

On the *Certificate Validation Policies* page, you can add new policies and manage saved policies. You can access the *Certificate Validation Paths* page on the *Identity & Trust* page.

Follow these steps to add a new policy:

1. Navigate to *Network* > *Identity & Trust* > *Certificate Validation Policies* in the camera's web interface.
2. Click **Add New Policy**.
3. Enter a name for the path in the Policy Details.
4. Search through the list of Available Certificates and select the certificates you want to add.
5. Use the › button to move the certificates to the Selected Certificate area on the right.
6. Use the ‹ button if you need to move certificates back to the Available Certificate area on the left.
7. Click and drag the ⠿ button to reorder the list of certificates.
8. Click **Save**.

The new certificate validation policy will be added to the list.

Managing Certificate Validation Policies

You can manage Certificate Validation Policies using the options in the list:

- To view a Certificate Validation Policy, click the ⋮ icon and select **View**.
- To delete a Certificate Validation Policy, click the ⋮ icon and select **Delete**.

You will not be able to delete a certificate validation policy if the camera is currently using it.

Configuring 802.1x Profiles

On the *802.1x* page, administrators can configure profiles and manage saved 802.1x configurations. You can configure 802.1x port-based authentication to set up the appropriate camera credentials so the video stream is not blocked by the switch. This allows administrators to manage access to the video stream.

Follow these steps to configure 802.1x profiles:

1. Navigate to *Network & Security* > *802.1x* in the camera's web interface.
2. In the *Configure 802.1X profiles* area, click the **Protocol** drop-down list and select a different protocol:
    a. PEAP: For username and password authentication.
    b. EAP-TLS: For certificate authentication.
3. If you selected PEAP, complete the required fields:

a. Configuration name**:** Give the profile a name.
b. Identity: Enter the username that will be used to authenticate the camera.
c. Password**:** Enter the password that will be used to authenticate the camera.
d. Authenticate Server: check this box if you need to add a certificate.

4. If you selected EAP-TLS, complete the required fields:
   a. Configuration name**:** Give the profile a name.
   b. Identity: Enter the username that will be used to authenticate the camera.
   c. certTLS: Select the PEM-encoded certificate file to authenticate the camera.
   d. Private key: Select the PEM-encoded private key file to authenticate the camera.
   e. Private key password: If the private key has a password, enter the password here.
5. Click **Upload File** and the TLS client certificate and private key are uploaded to the camera. The uploaded files are used to generate a unique certificate to authenticate the camera. The unique certificate is displayed in the **Uploaded certificate** field.
6. Click **Save**.

If this is the first profile added to the camera, it is automatically enabled.

Saved configurations are listed under Saved 802.1X configurations. To switch between authentication profiles or delete them, see *Managing Saved 802.1x Configurations* below.

Managing Saved 802.1x Configurations

Administrators can manage your authentication profiles in the *Configure 802.1X profiles* area:

- To select a different authentication profile, select the saved configuration then click **Enable**.
- To delete one of the authentication profiles, select the saved configuration then click **Remove**.

These changes will be saved automatically.

Changing Certificate Validation Paths

On the *TLS* page, administrators can select from a list of saved certificate validation paths.

1. Navigate to *Network* > *TLS* in the camera's web interface.
2. Choose a saved Certificate Validation Path from the drop-down list.
3. Click **Save**.

NOTE

You must create the certificate validation path under *Identity & Trust* > *Certificate Validation Path* before it is available in the list. See *Certificate Validation Paths* on page 36 for more information.

Single Sign-On (SSO)

Single Sign-On (SSO) allows system administrators to configure cameras to use a single set of credentials for login. This simplifies access by having an external identity provider handle user authentication. The implementation relies on an OpenID Connect compliant authorization provider that uses JWT access tokens and supports an ONVIF roles claim.

Compatibility

The camera can be configured with most OpenID Connect-compliant authorization providers, provided they use JWT access tokens and support an ONVIF roles claim. While the compatibility has been verified with Keycloak, Ping One, Microsoft Entra ID, and Okta, other compliant providers are also expected to be compatible.

Authentication Requirements

Setting up SSO for the first time involves similar steps across platforms, though specific steps will differ. Cameras require these settings to authenticate users:

1. Register Cameras as Client Applications: The camera must be registered as a client application with the third-party authorization service.
2. Configure Parameters: You will need to configure parameters such as the Authorization Server address, Client ID, Client Secret, Scope, Certificate path validation policy, Audiences, JWT signature verification method and Custom claims (optional).
3. Token Validation: The camera validates the ID and Access Tokens by checking their signature, issuer, audience, expiration and any custom claims. For ID Tokens, a unique "nonce" value is used to prevent security risks like replay attacks.
4. ONVIF Roles for Authorization: User authorization is managed by mapping the user's identity to an ONVIF user level (e.g., onvif:Administrator, onvif:Operator, onvif:User). This mapping happens through a "roles" claim within the Access Token. Access will be denied if this claim is missing or invalid.

Setting Up SSO In The Camera Web Interface

Administrators can set up Single Sign-On (SSO) in the camera web interface with third-party OpenID Connect authorization providers. Administrator account permissions are required for both the camera and the third-party authorization provider.

The steps for configuring SSO for cameras depends on the third-party authorization set up and requirements. In general, the cameras must be set up as client applications with the authorization service, cameras will validate ID and access tokens, the access token must support ONVIF roles claims.

IMPORTANT

To configure Single Sign-On settings, you need to access the web interface via HTTPS.

Follow these steps to set up SSO:

1. Navigate to *Network* > *Single Sign-On* in the camera's web interface.
2. If required, click **Redirect to HTTPS** and re-enter your camera log in credentials.
3. In the *OIDC Authorization Server* area, enter the Authorization Server address.
4. In the *Authorization Code flow configuration* area, enter the following parameters:
    a. Client ID
    b. Client secret
    c. Scope
5. In the *Server certificate validation* area, select a **Certificate path validation policy** from the drop-down list.
6. In the *JWT validation* area, click **Add** to add the required policies:
    a. Supported audiences
    b. Custom claims
    c. Supported Values
7. Select a **JWT signature verification method** from the drop-down list.
8. Click **Save**.

Once these requirements are met, you can return to this section to complete the camera-side configuration.

Image & Display

Under *Image & Display* settings, you can edit General Image Settings, Day/Night settings, Exposure Settings and enable Advanced Filters, such as digital defog and image spageilization.

Live Preview

The Live Preview displays the live footage from the camera. Below the Live Preview you will find the following camera information:

- Current Exposure: The camera's current light exposure levels measured in milliseconds (ms).
- Current Iris: The camera's current iris shown as an F-number (f/#). The F-number measures the lens's focal length over the aperture's diameter. The smaller the f-number the larger the aperture opening relative to the focal length, meaning more light can enter the lens.
    - A small F-number means objects further away blur while the subject remains in focus.
    - A large F-number means better depth of field meaning more of the scene will be in focus.
- Current Gain: The camera's current gain controls the amplification of the signal from the camera sensor measured in decibels (dB).
- Last Known Light Level: The camera's exposure value (EV) at a recent high point.

TIP

Auto focus ROI is used to automatically focus the camera as temperature fluctuates. Ensure the ROI contains sufficient contrast during both the day and night.

Adjusting Image Settings

On the *Image & Display* page, administrators and operators can adjust image settings using the options under the Live Preview. You can also move and configure the Auto Focus Zone.

Follow these steps to adjust image settings:

1. Navigate to *Image & Display* in the camera's web interface.
2. To zoom in, move the **Zoom** slider to the right.
3. To zoom out, move the **Zoom** slider to the left.
4. Click **Auto Focus** to let the camera focus itself.
5. To focus the camera, move the **Focus** slider to the right or left.
6. To use Image Rotation, select the **Image Rotation** drop-down menu and select an option.
7. To use Temperature Refocus, toggle the **Enable Temperature Refocus** option to the ON position.
8. Click **Save**.

The camera will adjust based on the image controls.

Configuring the Auto Focus Zone

You can change the shape and location of the Auto Focus Zone using the Live View.

1. If you can not see the Auto Focus Zone on the Live View, toggle the Show Auto Focus Zone button to the **On** position. You should see a blue box in the middle of the Live View.
2. To move the Auto Focus Zone, click and drag the blue box.
3. To resize the Auto Focus Zone, click the blue box to highlight it and click and drag the four corners to change the shape.
4. Click **Save**.

Day/Night Settings

On the *Day/Night Settings* page, you can configure the camera's behavior when switching between day time and night time settings.

Changing Day / Night mode

You can change the camera's Day / Night mode to determine how the camera will switch between light and dark image settings. This improves the image for 24 hour visibility.

1. Navigate to *Image & Display* > *Day/Night Settings* in the camera's web interface.
2. Select an option from the *Day / Night mode* drop-down list:
   a. Automatic– When the light level is above the day/night threshold, the video image will be in color. When the light level goes below the day/night threshold, the camera will automatically open the IR cut filter and switch to monochrome mode. For camera with no IRCF, the camera will just switch to monochrome. If IR illuminators are enabled, they also turn on.
   When the Day / Night mode setting is set to Automatic you can use the slider to set the Day/Night Threshold. Move the slider to set the light level when the camera switches between day mode and night mode. The slider value is in Exposure Values (EV).
   In day mode, the last known light level is displayed under the image panel and is also shown as a blue bar on the Day/Night Threshold slider.
   b. Color: The video image will always be in color.
   c. Monochrome: The video image will always be monochrome.
   d. External: The camera will open the IR cut filter and switch to monochrome mode based on the digital input circuit state. For camera with no IRCF, the camera will just switch to monochrome.

   NOTE

   You can set the default digital input circuit state on the Digital IO page. See Digital Inputs and OutputsDigital Inputs & Outputs for more information.
3. Click **Save**.

Enabling IR LEDs

This feature allows you to manually enable or disable the IR illuminators that are installed on the camera.

- To enable IR LEDs in night mode, toggle the **IR Enable** button. Click **Save**.

Adjusting the Day/Night Threshold (EV)

To adjust the Day/Night Threshold (EV), use the slider to increase or decrease the minimum threshold required for the camera to change modes. Alternatively, you can enter a value (-8 and 8) in the EV field.

- Moving the slider to the right decreases the threshold required for the camera to switch to daytime settings.
- Moving the slider to the left decreases the threshold required for the camera to switch to night time settings.

Enabling Adaptive IR Compensation

Enabling automatic infrared adjustments through Adaptive IR Compensation allows the camera to automatically adjust the video image for saturation caused by IR illumination.

- To enable Adaptive IR Compensation, toggle the **Adaptive IR** button. Click **Save**.

Enabling Night Visibility Check

The night visibility check, when enabled, performs a periodic test switching between day/night mode to check if there is sufficient light level to switch from night mode to day mode. When turned off, the camera will use a less optimal method to determine if the light level is sufficient to switch to day mode.

- To enable Night Visibility Check, toggle the **Night Visibility Check** button. Click **Save**.

> **NOTE**
> Disabling the night visibility check could delay the camera from transitioning between night and day modes and make the transition time less optimal. For example, the camera stays in night mode 30 minutes longer than it needs to.

Adjusting Exposure Settings

On the *Exposure Settings* page, you can adjust the camera's exposure settings to optimize visibility in very bright or very dark environments. You can find the *Exposure Settings* by navigating to *Image & Display* > *Exposure Settings* in the camera's web interface.

Using Flicker Control

Use Flicker Control in scenes where the camera image appears to flicker. Flickering is often caused by fluorescent lights. You can reduce the flickering effect by setting the Flicker Control to the same frequency as the lights. Generally, Europe is 50Hz and North America is 60Hz.

- Click the **Flicker Control** drop-down list and select a frequency (Hz). Click **Save**.

The camera will start using the new frequency.

Changing Exposure

Exposure determines how much light reaches the camera's sensor. Exposure is set to Automatic by default which allows the camera to control the exposure. You can change the exposure rate to allow more light to hit the camera sensor which brightens the image. Alternatively, you can decrease the exposure to darken the image. Manually increasing the exposure time may affect the image rate.

- Click the **Exposure** drop-down list and select a value (milliseconds). Click **Save**.

The camera will adjust the sensor for the new exposure level.

Setting a Maximum Exposure Level

Maximum Exposure limits the exposure when the camera is set to Automatic. In low-light situations, set a maximum exposure level so you can manually control the camera's exposure time without creating blurry images.

The Maximum Exposure drop-down list is only available when the Exposure setting is set to Automatic.

- Click the **Maximum Exposure** drop-down list and select a value (milliseconds). Click **Save**.

The camera will apply the maximum exposure setting to avoid blurry images.

Setting a Maximum Gain

Maximum Gain limits the automatic gain setting by selecting a maximum gain level. In low-light situations, set a maximum gain to maximize the detail without creating excessive noise in the images.

- Click the **Maximum Gain** drop-down list and select a maximum gain level (milliseconds). Click **Save**.

The camera will apply the maximum gain setting to avoid excessive visual noise in the image.

Changing Priority

The Priority feature lets you prioritize Image Rate or Exposure. When Priority is set to Image Rate, the camera will maintain the set image rate as the priority and will not adjust the exposure beyond what can be recorded for the set image rate. When Priority is set to Exposure, the camera will maintain the exposure setting as the priority, and will override the set image rate to achieve the best image possible.

- Click the **Priority** drop-down list and select either Image Rate or Exposure. Click **Save**.

The camera will switch to prioritizing the selected option, either Image Rate or Exposure.

Changing Iris Mode

Iris Mode determines how the camera's iris is controlled. You can allow the camera to control the iris by selecting Auto. If you want to manually control the Iris, select either Open or Closed.

- If you want the camera to control the iris while you control other settings, select **Auto**.
- If you want the iris to open so you can manually start closing it, select **Open**.
- If you want the iris to close so you can manually start opening it, select **Open**.

Using WDR

Wide Dynamic Range (WDR) allows the camera to adjust the video image to accommodate scenes where bright light and dark shadow are clearly visible.

- Toggle the **WDR** button to the ON position. Click **Save**.

The camera will start using WDR.

Using Backlight Compensation Mode

Backlight Compensation helps brighten dark areas when there is strong background lighting, for example, a large window in the background. You can enable Backlight Compensation to brighten the dark areas and achieve a well exposed image.

- Toggle the **Backlight Compensation Mode** button to the ON position. Click **Save**.

The camera will start using backlight compensation.

Using Iris Priority

Iris Priority mode allows you to manually control the camera's F-stop (aperture) at a fixed setting. This means you determine how open or closed the lens's iris is, directly impacting the depth of field. While the F-stop remains constant, the camera automatically adjusts the shutter speed and gain to maintain proper exposure.

Features like Wide Dynamic Range (WDR) and Backlight Compensation are not available when Iris Priority mode is active.

- Toggle the **Iris Priority** button to the ON position. Click **Save**.

If you attempt to enable Iris Priority mode through an ONVIF call while simultaneously enabling WDR, auto exposure, or Backlight Compensation, those latter settings will take precedence, and Iris Priority mode will be ignored.

Advanced Filters

On the *Advanced Filters* page, you can enable digital defog and image stabilization features to improve visibility. You can find the *Advanced Filters* by navigating to *Image & Display* > *Advanced Filters* in the camera's web interface.

Digital Defog

If the camera is installed in a foggy environment, you can use Digital Defog increase the video contrast to help make objects more visible in the scene.

1. Toggle the **Enable Digital Defog** button to enable Digital Defog.
2. From the **Defog Level** drop-down list, select one of the available options: Low, Medium, High.
3. Click **Save**.

The camera will apply Digital Defog to help clarify foggy images.

Electronic Image Stabilization (EIS)

If the camera is mounted to a pole or other surface that is prone to shaking or vibrating, you can use image stabilization allows the camera's built-in image stabilization feature to compensate for the motion, improving the footage.

- Toggle the **Image Stabilization** button to enable image stabilization . Click **Save**.

The camera will apply electronic image stabilization to compensate for camera movement.

Adjustment

In the *Adjustment* area, you can adjust image settings to fine tune the image and optimize visibility. You can find the Adjustment area by navigating to *Image & Display* > *Adjustment* in the camera's web interface.

Image Rotation

Image Rotation rotates the camera image when the camera is installed upside down or sideways.

- To use Image Rotation, select the **Image Rotation** drop-down menu and select an option. Click **Save**.

You can rotate the image by 90°, 180° and 270°.

Adjusting Basic Image Settings

In the *Basic Settings* area, you can control the camera's image settings.

1. Use the sliders to adjust the following settings:
    a. Sharpness: increasing sharpness will help clarify fine details.
    Adjusting the sharpness will make the image blurry initially. Refocus the camera after adjusting the sharpness.
    b. Saturation: increasing saturation will enhance the color intensity. Lowering the saturation will reduce the intensity.
    c. Contrast: increasing contrast can emphasize certain aspects of the image. Lowering the contrast can make the image softer. The right level of contrast depends on the subjects you want to see clearly as well as the setting.
    d. Brightness: increasing brightness cam make dark scenes easier to see. If increasing brightness makes the dark areas harder to see, due to a strong back light for example, you can use Backlight Compensation Mode instead. See *Adjusting Exposure Settings* on page 43 for instructions.
2. Click **Save**.

Zoom & Focus

In the *Zoom & Focus* area, you can zoom and focus the camera.

1. To zoom in, move the **Zoom** slider to the right.
2. To zoom out, move the **Zoom** slider to the left.
3. Click **Auto Focus** to let the camera focus itself.
4. To focus the camera, move the **Focus** slider to the right or left.
5. Click **Save**.

White Balance

In the *White Balance* area, you can assign a White Balance mode to compensate for discoloration in the image. For example, florescent lights can cast a green hue on the scene. White Balance corrects this effect and makes objects in the field of view appear as they normally would.

1. Click the *White Balance* drop-down list and select one of the following modes:
    a. Automatic: Allows the camera to automatically control the red, green and blue color channels to neutralize the color cast and achieve a more accurate white.
    b. Manual: Allows you to manually set the Red and Blue levels.
2. You can select the Dominant Color Compensation checkbox if available. Select this option if the scene contains a large area in the field of view contains one color. For example, a large grassy area contains a lot of green.
3. If you selected Manual as the White Balance mode, use the Red and Blue sliders to manually compensate for discoloration in the image.
4. Click **Save**.

Temporal Filter Strength

Temporal Filter Strength reduces image noise by averaging the noise over several frames. This can reduce blurriness and decrease bandwidth usage.

> **TIP**
> Start by making small adjustments because applying excessive changes may degrade the overall image quality.

- Move the Temporal Filter Strength slider to the right to decrease the amount of visual noise in the scene.
- Move the Temporal Filter Strength slider to the left to decrease temporal strength filter. This will restore the image quality if the filter strength was too high but it will reintroduce visual noise in the image.

Overlays

On the *Overlays* page, you can add and customize overlays and toggle the display of the cross hair.

What are Overlays?

Overlays are text or symbols that are displayed directly on the camera's live video stream. They are used to add helpful information to the footage, such as the date and time. A key feature is that when you download still images from the camera, the resulting image files will include the displayed overlay information.

Adding New Overlays

On the *Overlays* page, you can create and configure multiple overlay types at the same time.

1. Navigate to *Image & Display* > *Overlays* in the camera's web interface.
2. Click **Add new Overlay**.
3. Select the **Location** drop-down menu and choose a location on the screen where the overlay will appear.
4. Select the **Overlay Type** drop-down menu and choose one or more options:
    a. Custom Text: Add a text field and enter the text you want shown.
    b. Date: Add the date.
    c. Time: Add the time.
    d. Camera Name: Add the camera's name. The camera's name is set on the General page, under Settings.
    e. Location: Add the location.
5. If you chose Custom Text, enter the text in the **Overlay Text** field. The limit is 64 plain-text characters.
6. If you chose Date, you can select a different date format from the **Date Format** drop-down menu.
7. If you chose Time, you can select a different time format from the **Time Format** drop-down menu.
8. To change the Font size, change the font value (between 12 - 80 pt) in the **Font size** field. The default font size is 24.
9. To change the Text Color, select the **Text Color** drop-down menu and choose a different color.
10. To change the Background Color, select the **Background Color** drop-down menu and choose a different color.
11. Click **Save**.

The overlay will appear on the live preview screen.

Compression & Image Rate

Under *Compression & Image Rate* settings, you can change the camera's compression and image quality settings.

Considerations when Configuring Compression & Image Rate Settings

- Image Quality vs. Bandwidth: Changing compression and image rate settings to image quality can increase bandwidth usage. Typically, settings that improve image quality will increase the bandwidth usage, due to the increased file size. The goal is to optimize image quality without causing network congestion.
- Self-Learning Video Analytics: Updating the image rate and compression settings can cause Self Learning progress to reset automatically.

Configuring Compression & Image Rate Settings

On the Compression & Image Rate page, you can configure the camera streaming settings to optimize video quality in light of network constraints. The camera will automatically adjust compression quality in order to abide by the bandwidth cap specified.

Cameras can have primary, secondary, tertiary and quaternary streams. Not all camera models have quaternary streams. Refer to the Pelco Camera Datasheets for your camera's specification.

To configure a camera stream, select the stream and edit the following settings:

1. In the **Compression Standard** drop-down list, select the preferred streaming format for compressing video files.
   If you are using Onboard Storage, make sure you select **H.264**.

   > **NOTE**
   > Changing the streaming format to H.264 or H.265 will only affect the footage in the VMS. You will not see a difference in the camera's Live Preview in the web interface.

2. For cameras that support Rate control, select one of the following options from the drop-down list:
   a. CVBR: Uses VBR to adjust the bitrate based on the complexity of the scene.
   b. CBR: Uses a fixed bitrate to produce smaller video files.
3. Select the **Resolution** drop-down list, and select the image resolution.
4. Select the **Frame rate** drop-down list, and select the frame rate. Choose a value between 1-30 seconds. This determines how many images per second you want the camera to stream over the network. The default frame rate is 30.
5. In the **Quality** drop-down list, select the desired image quality. Setting the Image quality to 1 will produce the highest quality video but will require the most bandwidth.

6. In the **Max Bitrate** field, enter the maximum bandwidth the camera can use. You can enter any number between 200-12000 kbps.
7. In the **Keyframe Interval** field, enter the number of frames between each keyframe. You can enter any number between 2-64.
8. To configure Multicast settings, see *Configuring Multicast Settings for Video* below.
9. You can check the RTSP Stream URLs or Still Image URIs on the Compression & Image Rate page, but you can not edit these values. To use the RTSP Stream URI to view the camera's video stream, see *Viewing the Camera Live Stream Using the RTSP Stream URI* on page 52.
10. Click **Save**.

This applies the compression and image rate settings to the camera stream.

You can configure these settings individually for primary, secondary, tertiary and quaternary streams if available. See *Enabling Cropped Quaternary Stream* below to access the quaternary stream.

Configuring Multicast Settings for Video

Follow these steps to configure Multicast behavior for the camera stream:

1. To configure Multicast, enter the required information in the following fields:
   a. Address: Enter the server address.
   b. Port: Enter the server port number (1024...65534). Only accepts even values.
   c. Time to live: Enter the number of seconds (1-255).
2. Click **Save**.

The camera will transmit the video stream to the server specified above and the camera feed should be viewable on the client(s) connected to that server, using the specified port number.

If you want to configure multicast streaming for audio, see *Configuring Multicast Settings for Audio* on page 76.

Enabling Maximum Secondary Stream Resolution

On the Compression & Image Rate page, you can enable the maximum Secondary Stream resolution.

- Select the **Enable Maximum Secondary Stream Resolution** checkbox to enable it. Click **Save**.

The camera will reboot.

The camera's secondary stream will use the maximum framerate that the camera can support. The maximum framerate depends on the camera model.

Enabling Cropped Quaternary Stream

On the Compression & Image Rate page, you can enable the camera's Quaternary Stream. This allows you to generate a specialized, fourth video stream (the quaternary stream) from your camera's output. This stream is cropped, meaning it focuses on a specific, smaller area of the original full-resolution video image.

Why Enable the Cropped Quaternary Stream?

- Enhanced Detail: By focusing on a smaller region of interest (ROI), the camera can allocate more processing power and bandwidth to that specific area. This allows you to transmit a cropped stream with a higher effective resolution or finer detail than the full-view stream, especially when zooming in digitally.
- Reduce Bandwidth and Storage: The cropped stream contains significantly less pixel data than the full-resolution stream. This allows the fourth stream to be recorded or viewed using less bandwidth and consuming less storage space, which is highly beneficial for remote monitoring or for saving resources when only a small area needs continuous, high-detail viewing.
- Privacy: While privacy masking is one option, a cropped stream can serve a similar purpose by only streaming the necessary area, effectively excluding sensitive peripheral content from being transmitted or recorded on that particular stream.

Cropped Quaternary Stream is only available on cameras that support a quaternary stream. However, the quaternary stream settings are hidden until you enable the cropped quaternary stream.

1. Navigate to the Compression & Image Rate page.
2. Select the **Enable Cropped Quaternary Stream** checkbox to enable it.
3. Click **Save**.

The camera will reboot and you will need to log in again.

Select the **quaternary** page to access the quaternary stream settings. You can adjust these settings the same way as the primary, secondary and tertiary streams. See *Configuring Compression & Image Rate Settings* on page 49 for instructions.

Advanced Compression & Image Rate Settings

On the *Advanced* page, you can configure more advanced streaming and image rate settings, like Smart Codec and Idle Scene Mode. These settings change the streaming behavior during periods of low activity to reduce bandwidth usage.

Using HDSM SmartCodec

You can enable and configure HDSM SmartCodec settings on the Video Configuration page. HDSM SmartCodec helps isolate objects from the background areas. This reduces the camera's bandwidth usage by concentrating on the subjects of interest.

HDSM SmartCodec is turned off by default.

1. In the *HDSM SmartCodec* area, toggle the **HDSM SmartCodec** option to enable it.
2. Click **Save**.

Enabling HDSM SmartCodec will turn on Idle Scene Mode. See *Using Idle Scene Mode* on the next page for instructions.

Turning Off Idle Scene Mode

If you want to continue using HDSM SmartCodec without Idle Scene mode you can turn it off.

- Toggle the **Idle Scene Mode** button to turn off this feature.

Using Idle Scene Mode

After you enable HDSM SmartCodec, Idle Scene mode is enabled automatically. Idle Scene mode conserves bandwidth by reducing the analytic functions during periods of inactivity. You can configure Idle Scene Mode to set the image quality standards when there is no activity in the scene.

1. In the On Idle Scenes area, you can configure the following settings:
    a. Min Image Rate: The encoding frame rate (images per second) when there is no motion in the scene.
    b. Keyframe Interval: The number of frames between each keyframe when there is no motion in the scene (between 1 and 254 frames).
    c. Post Motion Delay: The delay (in seconds) after motion has ended before the camera drops into idle scene settings (between 5 and 60).
    d. Quality: The compression quality when there is no motion in the scene (between 6 and 20).
    e. Max Bitrate: The maximum number of kilobytes per second when there is no motion in the scene.
2. Click **Save**.

Viewing the Camera Live Stream Using the RTSP Stream URI

You can view the camera's live video stream from any application that supports RTSP streams, including video players, by using the Real Time Streaming Protocol (RTSP) address.

1. To watch the camera's live video stream from an external video player, click the **Generate RTSP Stream URI** button. If the button is not available, the URI is auto-generated.
2. In the RTSP Stream URI area, the generated address is displayed at the bottom of the section. If the URIs are auto-generated, they are also shown here.
3. Select Unicast if you only plan to view the video stream from one video player at a time.
4. Select Multicast if you plan to view the video from more than one video player simultaneously.
5. Copy and paste the generated address into your video player. Do not open the live video stream yet.
6. Add your username and password to the beginning of the address in the following format:
   rtsp://<username>:<password>@<generated RTSP Stream URI>/.
   Example: rtsp://admin:admin@192.168.1.79/defaultPrimary?streamType=u.
7. Open the live video stream.

The live stream will show the live video stream from the camera.

Streaming Settings

On the *Streaming Settings* page, you can set the ONVIF Media Profile and configure Profile Settings.

1. Select an ONVIF Media Profile from the **Profiles** drop-down menu.
2. Select a profile from the **Video Source** drop-down menu.
3. Select a profile from the **Audio Source** drop-down menu.
4. To enable Metadata, select metadata0 from the **Metadata** drop-down menu.

5. To turn off Metadata, select None from the **Metadata** drop-down menu.
6. Select a profile from the **Video Encoder** drop-down menu.
7. Click **Save**.

Analytics

Under *Analytics* settings, you can create and manage analytic events.

Motion Detection

On the *Motion Detection* page, you can configure Motion Detection in two stages: defining the Motion Detection zones and then setting the sensitivity and threshold levels. Sensitivity determines how much each pixel must change before the analytic detects motion.

Follow these steps to configure Motion Detection:

1. To add Motion Detection zones:
    a. Make sure the **Select Zone** option is selected.
    b. Click an area on the Live Preview and drag your cursor to create a green square. This green square is a motion detection zone. Motion in this zone will trigger an event.
    c. Continue clicking and dragging to create zones where you want motion detected.
    d. If you want to start over, you can click **Select Full** to restore the motion detection zones.
2. To clear zones from within the Motion Detection zones:
    a. Select the **Clear Zone** option.
    b. Click an area on the Live Preview where you see green squares and drag your cursor to clear the area. This creates a hole in the Motion Detection zone. Motion in the cleared zone will not trigger an event.
    c. Continue clicking and dragging to clear the zones where you do not want motion to trigger an event.
    d. If you want to start over, you can click **Clear All Zones** to clear the motion detection zones.
3. To configure Sensitivity:
    a. Click and drag the **Sensitivity** slider to increase the Sensitivity(0-100). The higher the Sensitivity, the smaller the amount of pixel change is required before motion is detected. Sensitivity determines how many pixels must change before the image is considered to have motion. The default value is 50.
4. To configure Threshold:
    a. Click and drag the **Threshold** slider to increase the threshold (0-100). The higher the threshold, the higher the number of pixels must change before the image is considered to have motion. The default value is 20.
5. You can toggle the **Show Motion in Video** option to show motion in the Live Preview.
6. Click **Save**.
7. If you want to test the event, click the ►**Test** button on the top-right side of the screen.
   This will send a "Test" event to the Video Management System (VMS). Navigate to the VMS to verify that the event was received.

The analytic event will be saved and the camera will trigger an event if the activity is detected in the region (s) of interest. For instructions on editing the inclusion area, see *Modifying the Inclusion Area* on page 60.

Enabling ONVIF Motion Alarm Event

Enable ONVIF Motion Alarm Events so the camera can send ONVIF events. Many third-party Video Management Systems require the ONVIF protocol to process events.

- Toggle the **ONVIF Motion Alarm Enable** option to enable the ONVIF Motion Alarm Event protocol.

The camera will start sending ONVIF Motion Alarm Events.

Sabotage Detection

Under Sabotage Detection settings, you can create and edit Sabotage Detection events.

Sabotage Detection detects human tampering by detecting when the camera shakes or jerks from side to side in a way that is characteristic of human interference. Enabling Sabotage Detection allows the system to forward event notifications to an integrated system and send alarms to operators.

Configuring Classified Object Motion Detection

Classified Object Motion Detection analyzes the video footage but only reports the motion of vehicles or persons. This option is only available to Avigilon self-learning video analytics devices. The Classified Object Motion Detection event is listed on the *Events* page on the Analytics page. The default name is Smart Motion Rule. You can not edit the name of this rule.

Follow these steps to edit the Classified Object Motion Detection event:

1. Navigate to *Analytics* in the camera's web interface.
2. Click the ✎ icon next to Classified Object Motion Detection to edit the event.
3. Select the Object types you want the analytic to detect:
    a. Person
    b. Vehicle
4. If you selected Person under Object types, you can select which Person settings to monitor:
    a. Hard Hat: Detects either the presence or absence of a person wearing a hard hat.
    b. High-visibility Vest: Detects either the presence or absence of a person wearing a high-visability vest.
5. If you selected Vehicle under Object types, you can select which Vehicle settings to monitor:
    a. Bicycle
    b. Car
    c. Motorcycle
    d. Bus
    e. Large Truck
    f. Pickup Truck
    g. Van
6. Click and drag the **Sensitivity** slider to adjust the Sensitivity level. Lowering the sensitivity increases the chances of false negatives.
7. To configure **No. of objects**, enter the number of objects required to detect an alarm.

8. To configure **Threshold Time**, enter the minimum amount of time required before the event is triggered.
9. Click **Save**.
10. If you want to test the event, click the ►**Test** button on the top-right side of the screen.
    This will send a "Test" event to the Video Management System (VMS). Navigate to the VMS to verify that the event was received.

The analytic event will be saved and the camera will trigger an event if the activity is detected in the region (s) of interest. For instructions on editing the inclusion area, see *Modifying the Inclusion Area* on page 60.

Creating Motion Analytic Events

On the *Analytics* page, administrators and operators can create, edit and test motion analytic events.

Follow these steps to create a new analytic event:

1. Navigate to *Analytics* in the camera's web interface.
2. Click **Add Event** to add a motion analytic event.
3. Enter a name for the Analytic event. The event name will appear in the VMS when it is detected; so make sure it is descriptive.
4. To create an event based on Object Activity, select one of the following Detection types:
    a. Objects crossing beam: The event is triggered when the specified number of objects have crossed the directional beam that is configured over the camera's field of view. The beam can be unidirectional or bidirectional.
    b. Objects enter area: The event is triggered when the specified number of objects have entered the region of interest.
    c. Objects leave area: The event is triggered when the specified number of objects have left the region of interest.
    d. Object loitering: The event is triggered when the selected object type moves into the region of interest and then stays for an extended amount of time.
    e. Objects not present in area: The event is triggered when no objects are present in the region of interest.
    f. Object appears or enters area: The event is triggered by each object that enters the region of interest. The object can appear from within the region of interest or enter from outside.
    g. Objects in area: The event is triggered when objects are present in the region of interest.
    h. Object stops in area: The event is triggered when the object stops.
    i. Direction violated: The event is triggered when an object moves in the prohibited direction of travel.
5. To create an event based on Behavior Anomaly, select one of the following Detection types:
    a. Unusual Crowd Growth: This event is triggered when a crowd size grows unexpectedly.
    b. Unusual Crowd Size: This event is triggered when an unusual crowd size is detected.
    c. Crowd size: This event is triggered when the number of people is exceeded over a configurable duration.
6. Click and drag the **Sensitivity** slider to adjust the Sensitivity level. Lowering the sensitivity increases the chances of false negatives.

7. To configure **No. of objects**, enter the number of objects required to trigger an alarm.
8. To configure **Threshold Time**, enter the minimum amount of time required before the event is triggered.
9. To configure **Timeout**, enter the period of time before another the event is triggered.
10. Click **Save**.
11. If you want to test the event, click the ►**Test** button on the top-right side of the screen.
    This will send a "Test" event to the Video Management System (VMS). Navigate to the VMS to verify that the event was received.

The analytic event will be saved and the camera will trigger an event if the activity is detected in the region (s) of interest. For instructions on editing the inclusion area, see *Modifying the Inclusion Area* on page 60.

Creating Audio Analytics Events

> **IMPORTANT**
>
> In some countries or jurisdictions, there are strict rules about audio recording, particularly the recording of conversations, as this can be considered personally identifiable information (PII) under some privacy legislation. Before configuring these audio features, ensure that your use of these audio features complies with any applicable local and national laws and guidance.

On the *Analytics* page, you can enable Audio Analytics and create Audio detection events.

Prerequisites:

- The camera's microphone switch is turned off by default and must be physically switched on for Audio detection to work.
- A camera that supports audio analytics.
  Of the Pelco Fisheye Cameras cameras, only Sarix Fisheye 3 cameras support Audio detection.

Follow these steps to configure Audio detection:

1. Navigate to *Analytics* > *Audio Analytics*.
2. Toggle the **Enable** button.
3. Click **Save**.
4. A list of audio detection events will appear. Select a sound from the list.
5. Toggle the **Enabled** button to enable the Audio detection events.
6. Click the **Sensitivity** drop-down list to select an option:
   - Low: a lower setting means it requires a higher confidence level to trigger an alarm.
   - Medium: a medium setting means it requires a medium confidence level to trigger an alarm.
   - High: a higher setting means it requires a lower confidence level to trigger an alarm.
7. For **Timeout** enter a value (1-300) in seconds. Timeout is the minimum time interval after an audio event is detected before the system triggers an additional alarm.

> **IMPORTANT**
>
> During the Timeout interval, subsequent audio events. For example, multiple car alarms will not trigger separate alarms if they occur within the timeout interval. In some cases, like Gun shot detection, it would help to trigger multiple alarms. Consider reducing the Timeout setting for Gun shot detection.

8. Click **Save**.
9. If you want to test the event, click the ►**Test** button on the top-right side of the screen.
   This will send a "Test" event to the Video Management System (VMS). Navigate to the VMS to verify that the event was received.

Managing Audio Analytic Events

You can manage audio events on the *Audio Analytics* page. A green checkmark is shown next to the sounds that are being used for audio analytics events.

- Select the sound from the list and toggle the **Enable** button to the OFF position if you want to turn off an audio event. Click **Save**.

The audio analytic will no longer be detected.

Troubleshooting Audio Analytics *for Gunshot Detection*

If you need technical support when using the gunshot audio analytic feature, it can help to enable Gunshot Detection Diagnostic Logs. The logs contain diagnostic information that might help you locate the issue and troubleshoot. You can enable this functionality on the Audio Analytics Debug page located at https://*<enter camera ip address>*/web/setup-debug-audio-analytics.shtml. Audio debug information is not stored on the camera unless enabled.

Enabling Analytics Overlays

On the *Analytics* page, you can enable analytics overlays. Analytics Overlays include helpful analytic information on-screen when events are triggered.

> **NOTE**
>
> To be able to display Analytics Overlays, you must enable Analytics XML Metadata under *Extended Settings*. See *Extended Settings* on page 67 for instructions.

Follow these steps to enable analytics overlays:

1. Navigate to *Analytics* in the camera's web interface.
2. Toggle the **Display Object Confidence** button to include object confidence information in the overlay.
3. Toggle the **Display Object ID** button to include object ID in the overlay.
4. Click **Save**.

Analytic information will appear on-screen when an event is triggered.

Using Self Learning

On the *Analytics* page, you can configure Self Learning Analytics. Self Learning allows the camera to learn the scene and perform self adjustments based on the activity in the scene. Self Learning significantly improves the accuracy of classified object detection.

Scenes with less activity will require staging during the learning phase. Staging involves directed activity to show the camera what activity to detect. One example of staging would involve having a person walk through the field of view during learning.

Follow these steps to enable self-learning:

1. Navigate to *Analytics* in the camera's web interface.
2. Toggle the **Enable Self Learning** checkbox to enable Self Learning analytics.
3. Toggle the **Suspend Self Learning** checkbox to suspend Self Learning.
4. If you want to reset self learning, click the **Reset Self Learning** button. This erases previous self learning.

   > **IMPORTANT**
   >
   > This action can not be undone.

5. Click **Save**.

Self Learning will progress based on activity detected in the camera's field of view.

Suspending and Resetting Self Learning

Suspend Self Learning

Suspend the self-learning video analytics from continuing to learn the scene so that the camera continues to recognize objects correctly based on previous learnings and does not degrade its detection of objects when left to operate in sparse scenes.

The following scenarios are examples of when self learning should be suspended:

- People or vehicles are not expected in the device's field of view.
- Objects move at different heights. For example, overhead pedestrian bridges, train platforms, hills and underpasses.

Reset Self Learning

When the learning progress is reset, all learning data is cleared and the device needs to re-learn the scene. This prevents missed and false detections based on old data.

> **NOTE**
>
> Always reset Self Learning after a camera is physically moved or adjusted, or if the focus or zoom level is changed.

Changing Scene Mode

In the *Scene Mode* area, you can change the analytic scene mode. The right analytic scene mode will improve analytics results.

1. Navigate to *Analytics* in the camera's web interface.
2. Click the *Scene Mode* drop-down list and select on of the following options:
    a. Large Indoor Area
    b. Outdoors
3. Click **Save**.

The camera will change analytic scene modes.

For best practices on optimizing camera analytics, see the Designing a Site with Pelco Smart Analytics.

Modifying the Inclusion Area

You can edit the inclusion area to exclude areas that do not need to be monitored for the specific event.

The inclusion area looks like a green box on the Live Preview. Use your cursor to modify the shape and size of the inclusion area to make sure that every region you want to monitor for the event is monitored. After modifying the inclusion area, you can add one or more exclusion areas to ignore smaller regions in the camera's field of view.

Follow these steps to modify the inclusion area:

1. To edit the Inclusion Area:
    a. Click and drag the middle of the green square on the screen to move the inclusion area.
    b. Click and drag the Blue nodes to reshape the inclusion area.
    c. Click and drag the Green nodes to create additional Blue and Green nodes.
2. To add Exclusion Areas:
    a. Click **+ Add Exclusion Area** if you want to add a new exclusion area. The exclusion areas create holes in the inclusion area. Events in the exclusion zone will not trigger an event.
    b. Click and drag the middle of the green square on the screen to move the exclusion area.
    c. Reshape the exclusion area the same way you reshaped the inclusion area.
    d. Continue clicking and dragging to exclude the areas where you do not want the activity to trigger an event.
    e. Click **Delete Exclusion Area** to remove the selected exclusion area.
3. If you want to start over, click **Reset Areas** and select one of the following options:
    a. Reset Inclusion Area: Resets the inclusion area to cover the entire field of view.
    b. Reset Exclusion Areas: Deletes the exclusion areas.
    c. Reset All Areas: Resets the inclusion area and deletes the exclusion areas. You can not delete the inclusion area is required.
4. Click **Save**.

This updates the event so only events detected in the inclusion areas will trigger this particular event configuration.

Testing Analytics Events

There are two ways to test analytic events:

- After you save the event, you can test it by selecting the ►**Test** button on the top-right side of the screen.
- Alternatively, you can locate the analytic rule in the *Events* pagele and click the ►button.

Clicking the **Test** button will send a "Test" event to the Video Management System (VMS). Navigate to the VMS to verify that the event was received.

Analytic Event Types

Video Analytics

Motion Events	
Objects in area	The event is triggered when the selected object type moves into the region of interest
Objects crossing beam	The event is triggered when the specified number of objects have crossed the directional beam that is configured over the camera's field of view. The beam can be unidirectional or bidirectional.
Objects enter area	The event is triggered when the specified number of objects have entered the region of interest.
Objects leave area	The event is triggered when the specified number of objects have left the region of interest.
Object loitering	The event is triggered when the selected object type moves into the region of interest and then stays for an extended amount of time.
Object not present in area	The event is triggered when no objects are present in the region of interest.
Object appears or enters area	The event is triggered by each object that enters the region of interest. This event can be used to count objects
Object stops in area	The event is triggered when an object moves into a region of interest and then stops moving for the specified threshold time.
Objects too close	The event is triggered when two objects are too close together, based on the specified distance set for the event. Newer camera models only.
Direction violated	The event is triggered when an object moves in the prohibited direction of travel.
Unusual crowd size	This event is triggered when an unusual crowd size is detected
Unusual crowd growth	This event is triggered when a crowd size grows unexpectedly.
Crowd size	This event is triggered when the number of people is exceeded over a configurable duration.

Camera Automation

Under *Camera Automation* settings, administrators can create rules and assign actions that the camera will perform automatically in response to specific triggers.

Each rule specifies an action for the camera to perform each time the specified trigger occurs when a specified condition is true. Some actions come pre-defined and available to be used in rules, while others must be defined by the user before they can be used in rules.

IMPORTANT

Any changes you make to the actions will affect all of the camera rules using them.

Create Rules and Assign Actions

Rules define the trigger and conditions required to initiate actions. Administrators can create rules based on camera analytics, digital inputs, PTZ behavior and system status. You can create user-defined actions when creating rules or they can create the actions first.

Follow these steps to create a new rule:

1. Navigate to *Camera Automation* in the camera's web interface.
2. Click the **+ Add New** button to create a new Rule.
3. Enter the required information in the **Camera Automation** pop-up window:
    a. Enter a name for the Rule in the **Rule Name** field.
4. Define the Trigger in the *When the following trigger happens* area by selecting an option from the drop-down list:
    a. Analytics: Creates an Analytics rule.
    b. DigitalInput: Creates a Digital input rule.
    c. SystemStatus: Creates a System Status rule.
5. If you chose Analytics as the Trigger, select one of the saved Analytics types from the list. If you have created other analytic events, those will appear in the list as well.
    a. Smart Motion Rule: when the camera detects a specific motion event, e.g., classified objects in the scene. You can select from the list of motion rules you created on the *Analytics* page.
    b. Camera Tampering Rule: when the camera detects a person tampering with the camera itself.
    c. Motion Detector: when the camera detects motion in the scene.
6. If you chose SystemStatus as the Trigger, select **SystemBooted** from the drop-down list. This triggers an action when the camera reboots.
7. Click the **Simulate Trigger** button if you want to test any rules that you have already defined using that trigger.

> **NOTE**
>
> Simulate Trigger only causes the rules engine to execute the rules that depend on the chosen trigger. It does not simulate the underlying event that would cause the trigger to fire in real life.

8. Define the condition in the *And the following condition is true* area by selecting an option from the drop-down list:
    a. Always: the rule will perform the action every time the selected trigger occurs.
    b. Never: the rule will never perform the action, even if the selected trigger occurs. This can be used to temporarily disable a rule.
9. Click the **Evaluate** button if you want to check whether the selected condition is true or false.
10. Define the action in the *Then perform this action* area by selecting an option from the drop-down list:
    a. Digital Output: triggers a digital output. DigitalOutput only appears on cameras that have one or more digital outputs.
    b. Email: sends an email when the selected trigger occurs and the condition is true.
    c. FTP: triggers an FTP action sent to a subdirectory.
    d. Sequence: initiates a sequence of actions when the selected trigger occurs and the condition is true.
11. After you select from the list of available action categories, you can either chose from the available actions or create a new one. Select **+ Add New** and fill out the fields as described in the section titled *Create and Manage Sequences* under .
12. Click the **Invoke** button if you want to test the action.
13. Click **Save**.

The new rule will appear in the list of rules.

Managing Rules

Administrators can modify existing rules using the operations in the *Rules* pagele:

- Click the icon to edit a rule.
- Click the icon to delete a rule.

Editing or deleting rules will affect all the camera currently using the rule.

Adding New Sequences

Camera sequences automate a series of actions. These actions include digital outputs, sending emails, or transferring files via FTP. You can create and customize sequences, even setting delays between each step. You can use these sequences when creating camera rules.

Follow these steps to add a new sequence:

1. Navigate to *Camera Automation* > *User-Defined ActionsUser-Defined Actions* in the camera's web interface.
2. Select **Sequence** to show the settings area.
3. Click the **Add sequence** button.
4. Enter a name for the Sequence.
5. Select from the list of actions or click Add action to create one.
6. Enter the required information in the Sequence pagele:
    a. Delay: Enter the number of minutes you want the sequence to wait before performing the action.
    b. Category: Specifies a category, for example, "PTZ".
    c. Name– Specifies the specific action within the category, for example, "GoHome".
7. Click the **Test** button to test the sequence.
8. Click **Save**.

The new sequence will appear in the Sequence area and it will be listed as an option when creating or editing rules.

Managing Sequences

To modify a Sequence, use the operations in the pagele:

- Click and drag the ⠿ icon to reorder the Sequence.
- Click the 🗑 icon to delete a Sequence.

Editing or deleting sequences will affect all the camera rules currently using the sequence.

Adding New Email Actions

Email actions automate email outputs in response to camera rules, via the SMTP server. The email actions can be used as the User-Defined Actions when creating rules. You must configure SMTP server information before they can create email actions.

> **IMPORTANT**
> Any changes made to the SMTP server information will affect any rules that are already using that email.

Configuring SMTP Server Information

If you are adding the SMTP server for the first time, the button is labeled Configure SMTP. You must configure SMTP before you can access the **Add Email** option.

Follow these steps to configure SMTP Server information for the first time:

1. Navigate from *Camera Automation* > *Email Actions* in the camera's web interface.
2. Click the **Configure SMTP** button.
3. Enter the following information:
    a. Enter the SMTP Server URL.
    b. Enter the Username on the server url you provided.
    c. Enter User password or app password for the username.
    d. Enter an email address for the sender's email.
4. Click **Save**.

You can now add emails using this STMP server configuration.

Managing STMP Server Information

You can manage existing SMPT settings in the Email area:

- Click the **Edit SMTP** button to edit the SMTP server information and click **Apply**.

The SMTP server information will show the new configuration.

Adding an Email Action

Once an SMTP server has been set up, the Configure SMTP button changes to **Edit SMTP**, and the **Add Email** button becomes enabled.

Follow these steps to create a new email action:

1. Click the **Add Email** button.
2. Enter a name for the Email Action.
3. Enter a recipient email address in the **Email To** field.
4. You can enter another email address in the **Email Cc** field, if required.
5. Enter the text that you want to use for the email's subject line in the **Email Subject** field.
6. Enter the text that you want the email to contain into the **Email Body** section.
7. Click **Save**.

The new email action will be listed as an option when users create or edit rules.

Adding New FTP Actions

You can create FTP actions to use when assigning actions to the rules engine. Select the **FTP** row to show the FTP area. You can enable FTP by configuring FTP server information.

Configuring FTP Server Information

If you are adding the FTP server for the first time, the button is labeled **Configure FTP**. You must configure an FTP server before you can access the **Add FTP** option.

Follow these steps to configure FTP Server information:

1. Navigate to *Camera Automation* > *User-Defined Actions* in the camera's web interface.
2. Click **Configure FTP Server**.
3. Enter the Server URL.
4. Enter the Username for the Server URL you provided.
5. Enter the FTP user password associated with the Username.
6. Click **Save**.

You can add FTP actions using this FTP server configuration.

Managing FTP Server Information

You can manage existing FTP settings in the FTP area:

- Click the **Edit FTP** button to edit the FTPserver information and click **Apply**.

The FTP server information will show the new configuration.

Adding an FTP Action

After you add the FTP server information and enable FTP, you can create a new FTP action.

1. Click **Add FTP Action**.
2. Enter a name for the FTP Action.
3. Enter the Subdirectory.
4. Enter the Filename Pattern.
5. Select a File Type from the drop-down menu:
    a. Snapshot: Sends a JPEG image from the camera to the FTP server.
    b. hiResSnapshot: Sends a larger, higher-resolution image versus the smaller, downsized image that the Snapshot option produces.
6. Click **Save**.

The new FTP action will be listed as an option when users create or edit rules.

Cloud Connection

On the *Cloud Connection* page, you can connect the camera to Elevate using either the QR code in the camera's web interface or by entering the camera's serial number.

You will need to log into your Elevate account to connect cameras.

Follow these steps to connect a Pelco camera to the Elevate:

1. Navigate to Cloud Connection in the camera's web interface.
2. Click **Turn on provisioning mode**.
3. Cameras will use the QR Code method to connect by default. If you want to connect the camera using the serial number, select **Serial Number** from the drop-down menu.
4. Log in to your Pelco Elevate account.
5. Select the **Add camera** button.

6. If you are using the QR Code method:
    a. Choose the QR code method in your Elevate account.
    b. Scan the QR code below with your camera to connect it.
7. If you are using the Serial Number method:
    a. Choose the Serial Number method in your Elevate account.
    b. Enter the camera's serial number and click **Confirm**.
8. The camera will connect to Elevate.

The connection status indicator will update to show connected.

Extended Settings

On the *Extended Settings* page, you can configure ONVIF Settings. The ONVIF Settings allow you to enable certain features and capabilities that require specific ONVIF configurations.

1. Toggle the **Enable Multi-Packet XML Documents** button to reduce metadata size. Only for Video Management systems that support multi-packet XML documents.
2. Toggle the **Enable Analytics Options Requests** button to enable the GetAnalyticsModuleOptions and GetRuleOptions Requests.
3. Toggle the **Enable Analytics XML Metadata** button if you want to enable XML metadata. This is required to turn on bounding boxes.
4. Toggle the **Enable Run-Length Encoding of Motion Mask** button to enable run-length encoding of the motion mask. Only for Video Management Systems that do not require an un-encoded mask.
5. Toggle the **Enable Supplemental Events** button to send supplemental events not defined by ONVIF that may be useful to some Video Management Systems.
6. Toggle the **Enable Singleton Analytics Events** button to send singleton Analytics events instead of property events.
7. Click **Save**.

Privacy Zones

On the *Privacy Zones* page, you can create up to 64 privacy zones. Privacy zones can be applied to sensitive locations, such as residential areas, restrooms, or private offices, to prevent unauthorized viewing or recording of individuals in those spaces.

Creating Privacy Zones

Follow these steps to create Privacy Zones:

1. Navigate to *Privacy Zones* in the camera's web interface.
2. To add a privacy zone, click **Add**. The privacy zone will appear as a blue box on the Live Preview.
3. To define the privacy zone area, perform any of the following:
    a. Click and drag the blue box to move the privacy zone.
    b. Select the blue box to show the nodes on each corner. Click and drag the corner of the box to resize the privacy zone. Privacy Zones can only be rectangular in shape. Multiple privacy zones can be used to obscure other shapes.
4. For fine tuning, you can use the **Zoom** slider to zoom in or out.
5. Click **Save**.

The privacy zones will appear in designated areas.

Managing Privacy Zones

You can manage the saved Privacy Zones in the *Privacy Zones* list:

- If you want a privacy zone to appear blurry instead of opaque, select the **Blur** checkbox.
- If you want to delete a privacy zone, click the 🗑 icon.

Storage

On the *Storage* page, you can enable the onboard storage and download recorded video directly from the camera. Onboard storage is only available on cameras with an SD card or microSD card slot. The SD card will record from the highest resolution, non-tiled stream. Typically, the best stream to record from is the camera's primary stream.

Insert the SD card into the camera before you can use the onboard storage feature. Refer to the Camera's Installation Guide for the location of the SD card slot. For cameras with 2 microSD card slots, the camera will record video to SD cards in both slots. The total storage capacity of the system is the combined storage capacity of each of the two individual cards.

IMPORTANT

SD card failures can cause the camera to continuously reboot. To prevent this, the SD card will be disabled if persistent failures are detected. For more information, see *Troubleshooting SD Card Failures* on page 72.

Storage Information

In the *Onboard Storage* area, you can view device information and format the SD card.

Onboard Storage information:

- Status: The camera's storage status. For example: Recording, Recording when server connection is lost, etc.
- Total Capacity: The total storage capacity (GB) with one or more SD cards installed.
- Current Usage: The current storage (GB) usage.
- Remaining Capacity: The remaining storage capacity (hours).

Formatting The SD Card

On the *Storage* page, you can format the SD Card to reset it to its factory default state. This erases all data and sets up a new file system.

- Click **Format Card** in the *Onboard Storage* area.

The camera will reboot and footage stored on the card will be erased.

SD Card Information

On the *Storage* page, you can view the following SD card information:

- Model: The SD card model number.
- Serial Number: The SD card serial number.
- Capacity: The SD card's storage capacity (GB).
- Free Space: The available storage space on the SD card (MB).
- Measured Write Speed: The card's write speed (MB/s).

SD Card Encryption

On the *Storage* page, you can enable SD card encryption to encrypt the video files as a security precaution.

IMPORTANT

Enabling or disabling encryption will format all inserted cards and erase all files on them.

- Select the **Card Encryption** checkbox in the *Onboard Storage* area to enable card encryption. Click **Save**.

The SD card(s) will be reformatted and the files stored on them will be erased.

Configuring Recording Mode

On the *Storage* page, you can enable Onboard Storage and configure the recording mode, as well as the retention period.

Follow these steps to configure recording mode:

1. Toggle the **Enable Onboard Storage** button.
2. Toggle the **Recording when server connection is lost** button to have the camera record video to both the VMS and the SD card. By default, the camera will only record to the SD card when it is disconnected from the VMS.
3. Select one of the following recording modes:
    a. Continuous: The camera will record to the SD card continuously, without interuption.
    b. On Motion: The camera will record only when there is motion in the scene. The recorded video will be divided into files no more than five minutes in length or 100 MB in size.
    If you are configuring a video analytics camera, the On Motion setting will record either pixel change in the scene or analytics motion events depending on how the camera is configured in the VMS.
4. Toggle the **Enable Recording Retention** button to store recordings for a set amount of time (5 minutes to 2 years). You can assign the number of days, hours and minutes that the recordings will be stored.
5. Click **Save**.

After configuring the recording mode, check the Compression and Image Rate Settings to make sure the format is set to **H.264)** or **H.265)** to maximize the SD card recording capacity and performance.

Download Recordings From The Web Interface

On the *Storage* page, you can view and download the recorded footage on the SD card(s).

If the camera has two SD cards installed, select the SD card that you want to download video from. You may have to check both SD cards for the recording you want to download. The camera can record video to either SD card based on the remaining capacity of the SD cards.

We recommend that you download recorded video from the web interface. If your bandwidth is limited, you can choose to download the recorded video directly from the SD card. See *Downloading Recorded Video From The SD Card* below for instructions.

Follow these steps to download recorded video from the web interface:

1. In the Recording List, select the check box beside all the video files you want to download. To help you find the video you want, you can filter the videos by date and time. Select the **Filter** check box then select the time range.
2. Click **Download**.

The selected video files are automatically downloaded to your browser's default Downloads folder. If you are prompted by the browser, allow the download to occur.

> **NOTE**
> Do not close your browser window until the download is complete or the file may not download correctly. This is important if you are downloading multiple video files because the files are downloaded one by one.

Downloading Recorded Video From The SD Card

On the *Storage* page, you can download recorded video directly from the SD card if there is not enough bandwidth to download from the web interface.

To download recorded video directly from the SD card, perform the following:

1. In the *Settings* area, clear the **Enable Onboard Storage** check box to turn off Onboard Storage and then click **Apply**.
2. Remove the SD card from the camera.
3. Insert the SD card into a card reader.
4. When the Windows AutoPlay dialog box appears, select **Open folder** to view files.
5. Open the Camera Footage application. The Camera Footage window lists all the video files that are stored in the SD card.
    a. To download all the recorded videos, click **Download**.
    b. To download specific video, select the video files you want then click **Download Selected**.
6. When you are prompted, choose a location to save the video files.
7. The files start downloading from the SD card and are saved to the selected location.
8. When you are ready, eject the SD card.
9. Insert the SD card back into the camera then select **Enable Onboard Storage**.

The SD card will start recording again.

ONVIF Profile G

ONVIF Profile G allows video management systems to retrieve video from onboard storage when there is a gap in the VMS video due to a network outage or similar event.

- Cameras with firmware versions 4.4.0.X or later will have ONVIF Profile G already enabled.

Troubleshooting SD Card Failures

SD card failure can result in camera failure by causing the camera to continuously reboot. If the camera detects persistent failures, the SD card will be turned off automatically.

Once an SD card has been turned off, the camera and web interface will notify you of the issue:

- The video footage will show the following message: `SD card has failed. Format or replace the card`
  You can turn off video overlays on the *Storage* page by deselecting the **Enable SD disabled Overlay checkbox)** option.
- The *Storage* page will show the following message: `Storage Tab SD disabled Message`

Re-Enabling the SD Card

Follow these steps to re-enable the SD card:

1. Remove the SD card from the camera slot and replace it with a working SD card. A speed test will be run on the new card when it is inserted to determine if it will function without any issues.
2. You can also force the SD card to be re-enabled in the web interface by selecting **Force Enabled SD disabled** on the *Storage* page.

> **IMPORTANT**
> Forcing the SD card to be re-enabled is not recommended unless you are sure there are no problems with the card. If the card continues to fail, it may cause the camera to enter a reboot loop and after continued persistent failures, the SD card will be disabled again.

System

Under *System* settings, administrators can view system information, manually upgrade the firmware, reboot the device and restore the camera to the factory defaults.

You can view the following System information:

- Firmware Version: shows the firmware version installed on the camera.
- Model Number: the camera's model number will indicate whether it has certain functionalities, e.g, IR LEDs.
- Hardware Version: the hardware version number can help when contacting support with firmware related questions.
- Serial Number: the camera's unique serial number.

Updating Firmware

On the *System* page, administrators can upgrade the camera's firmware.

Follow these steps to manually upgrade the camera firmware:

1. Navigate to *System* in the camera's web interface.
2. Download the latest version of the firmware .bin file from the Pelco website at www.pelco.com/updates.
3. Click **Browse**, and then browse to and locate the firmware file on your computer.
4. Click **Firmware Update** and wait until the camera upgrade is complete.

The camera will reboot for 1 to 2 minutes.

When the camera is finished rebooting, refresh your browser and log in again.

Rebooting the Camera

If the camera is behaving strangely, an administrator can use the Reboot function to troubleshoot the issue.

1. Navigate to *System* in the camera's web interface.
2. Click **Reboot** to reboot the camera.

The camera will start rebooting. This can take several minutes.

TIP

Refresh your browser once the camera has finished rebooting. You will need to log in again.

Clearing All Settings

Administrators can clear all settings from the camera to restore the camera to factory default settings:

1. Navigate to *System* in the camera's web interface.
2. Select the **Preserve Network Configurations** checkbox if you want to keep the network settings configuration on the camera from being reset.
3. Click **Clear All Settings** to reset camera settings.
4. Click **Ok** in the confirmation dialog.

The camera will perform a factory reset.

Device Logs

On the *Device Logs* page, you can view, update or download the device log on the *Device Information* page. You can use the filters to narrow the logs shown in the pagele. You can filter by Log Type, Minimum Log Level and change the number of logs shown at one time.

Updating Device Logs

You can refresh the list of device logs.

- Refresh the list of device logs, click **Update**.

Any logs logged since the last refresh will be added to the pagele.

Downloading Log

You can download the current list of device logs.

- To download logs, click **Download Log**.

TIP

Make sure you have selected the right filters before downloading.

Audio

On the *Audio* page, you can adjust various audio settings to optimize audio quality and define the behavior of the Video Intercom's built-in microphone and speaker.

Follow these steps to configure the audio settings:

1. Navigate to *Audio* in the camera's web interface.
2. In the **Audio Settings** field, specify the audio encoder to use:
    - Opus: Default high-quality audio codec that generally produces superior sound. Use if you are running software Release 6.10 or later or using a third-party video management system that supports the Opus protocol.
    - G.711: Supported on various platforms. Use if your software version or third-party VMS does not support Opus.
3. Click **Save**.

The Audio settings will update.

Configuring Device Speaker

On the *Audio* page, you can configure the device's speaker.

Follow these steps to configure the device speaker:

- In the *Device Speaker* area, click and drag the **Speaker volume** slider to set the value (0-31 dB). The default value is 0. Click **Save**.

The Device Speaker settings will update.

Configuring Device Microphone

On the *Audio* page, you can configure the device's microphone.

Follow these steps to configure the device microphone:

- In the *Device Microphone* area, click and drag the **Gain for microphone** slider to set the value (0-31 dB). The default value is 0. Click **Save**.

Increasing the Gain for microphone value increases the volume.

Configuring Multicast Settings for Audio

Follow these steps to configure Multicast behavior for device audio:

1. To configure Multicast, enter the required information in the following fields:
    a. Address– Enter the server address.
    b. Port– Enter the server port number (1024...65534). Only accepts even values.
    c. Time to live: Enter the number of seconds (1-255).
2. Click **Save**.

The camera will transmit the audio to the server specified above and the audio should be accessible on the client(s) connected to that server, using the specified port number.

If you want to configure multicast streaming for video, see *Configuring Multicast Settings for Video* on page 50.

Users

On the *Users* page, administrators can add new user accounts and manage existing user accounts. You can choose to preserve user accounts and passwords when completing a firmware revert. Administrators can also change the password complexity requirements to make sure that users create complex passwords.

When creating new users, you must assign the user to a Security group: user, operator or administrator. The Security Groups are associated with different levels of access to camera settings. See *Security group* on page 79 for information on access and permissions.

Adding New Users

Follow these steps to add a new user:

1. Navigate to *Users* page in the camera web interface.
2. Click the **Add new user** button.
3. Enter a Username.
4. Enter a Password.

   > **TIP**
   >
   > The password must include uppercase characters, lowercase characters, numerical digits and symbols. Check the **Relative password strength** indicator to determine how strong the password is.

5. Re-enter the password to confirm.
6. Select a security group from the **Security group** drop-down menu.
7. Toggle the **Use PTZ controls** to grant the user permission to operate ptz camera controls.
8. Click **Save**.

The new user will appear in the Users list.

Managing Users

You can edit and delete user accounts on the *Users* page.

- To edit the account Username, click the icon and type the new Username into the field.
- To delete an account, click the icon and click **Delete** in the confirmation dialog.

Preserving User Accounts On Firmware Revert

On the *Users* page, administrators can perform firmware reverts as a part of troubleshooting camera issues. When completing a firmware revert, user accounts and passwords are wiped from the camera.

Make sure to select this option before completing a firmware revert. User accounts and passwords can not be restored after the camera settings are wiped.

- To keep the user accounts and passwords from being wiped, make sure you select the **Do not clear usernames or passwords on firmware revert** checkbox before completing a firmware revert.

You should be able to see the user accounts and passwords after the firmware revert.

Changing Password Complexity Requirements

On the *Users* page, administrators can change the password complexity requirements.

1. Enter the minimum password length (0-128 characters) in the **Minimum Length:** field.
2. Enter the minimum number of uppercase characters (0-128 characters) in the **Uppercase:** field.
3. Enter the minimum number of numerical characters (0-128 characters) in the **Number:** field.
4. Enter the minimum number of symbols (0-128 characters) in the **Symbols:** field.
5. Select the **Lock Password Complexity configuration** check box to prevent other users from editing it.
6. Click **Save**.

Users and operators will have to meet these requirements when changing their passwords.

Security group

Permissions	User	Operator	Administrator
Live Preview	Yes	Yes	Yes
PTZ Controls	Yes[1]	Yes	Yes
General Settings	No	No	Yes
Network Settings	No	No	Yes
Image and Display	No	Yes	Yes
Compression and Image Rate	No	Yes	Yes
Motion Detection	No	Yes	Yes
Tamper Detection	No	Yes	Yes
Analytics	No	Yes	Yes
Camera Automation	No	No	Yes
Privacy Zones	No	Yes	Yes
Digital Inputs and Outputs	No	Yes	Yes
Audio Settings	No	Yes	Yes
Storage	No	Yes[2]	Yes
Licensing	No	No	Yes
Users	No	No	Yes
System	No	No	Yes
Device Logs	No	No	Yes

[1] Users can use the PTZ controls if the administrator gives them permission.

[2] Operators can configure onboard storage settings but cannot delete video recordings or format the SD card.

About

Device Information	
Name	The camera's name.
Location	The camera's location
Part Number	The camera's part/model number.
Orderable Part Number	The camera's alternate part number.
Serial Number	The camera's unique serial number.
Device UUID	Universally unique identifier
Firmware Version	The firmware version running on the camera
Vasys Version	The Val System software version on the camera.
Build hash	A unique digital fingerprint for that specific software or firmware build.
MAC Address	The unique, hard-coded identifier assigned to a network interface controller (NIC) on the camera.
Licenses	The Third-Party License library for Third-Party Components and associated information.
ONVIF Conformance	The Onvif profiles supported by the camera.
Power Source	The power source currently supplying power to the camera.
Operation mode	The camera's current operating mode.

Account

Under *Users* settings, you can change your password or log out of the camera web interface. Click the icon to access the *Users* page.

Changing Your Password

If you remember your current password, you can change your password while logged into the camera web interface. If you do not remember your password, you will have to contact your system administrator.

1. Select the icon on the top-right corner of the window.
2. Enter your current password in the **Old Password** field.
3. Enter a new password in the **New Password** field.
4. Check the Relative password strength indicator to make sure your password is strong enough.
5. Re-enter the new password in the **Re-type password** field.
6. Click **Save**.

Your new password will take effect next time you log in.

Logging Out

Logging out of the web interface is straightforward.

1. To log out of the web interface, click the icon on the top-right corner of the window.
2. Click **Logout**.

NOTE

Users will be automatically logged out of the web interface after 15 minutes of inactivity.

Logging Out After Using SSO

When you log out, you are logged out of both the camera and the external login service at the same time.

More Information & Support

For additional product documentation and software and firmware upgrades, visit support.pelco.com.

Technical Support

Contact Pelco Technical Support at support.pelco.com/s/contactsupport.