Pelco Fisheye® Cameras
Operations Manual



Document number: C6708M-C
Publication date: 02/24

Table of Contents

Introduction 4
- System Requirements 4

Accessing Camera Settings 5
- Accessing the Camera Web Interface 5
- Creating the Initial User 5
- Logging In 5
- Logging Out 6

Using the Live View 7
- Navigating Through the Web Interface 7
- Saving a Still Image 7

Configuring the System Settings 8
- Configuring General Settings 8
- Managing the Camera Firmware 9
- Configuring Storage Management 10
  - Enabling Onboard Storage 10
  - Downloading Recorded Video from the Web Interface 11
  - Downloading Recorded Video from the SD Card 11
  - Deleting Recorded Video 11
- Extended Settings 12
- Configuring Diagnostics 12

Configuring the Network and Security Settings 14
- Configuring the Network Settings 14
  - Enabling SRTP Streaming 16
- Modifying Security Settings 16
- Configuring the Users 16
  - Adding a User 17
  - Modifying Users and Passwords 17
  - Removing a User 17
  - Keeping Usernames and Passwords After Firmware Revert 17
- Configuring 802.1x Port-Based Authentication 18
  - Configuring the 802.1X Port Security 18
  - Switching 802.1X Authentication Profiles 19
  - Removing an 802.1X Authentication Profile 19
  - Returning to the Network Page 19
- Configuring SNMP 19
- Configuring the IP Filter 20
- Managing Certificates 21
  - Downloading Certificates 21
  - Removing Certificates 21
  - Downloading Certificate Signing Requests 21

Uploading Certificates 21
Uploading CA Certificates 22

Configuring Imaging 23
Configuring General Imaging Settings 23
Understanding Backlight Compensation (BLC) and Wide Dynamic Range (WDR) 25
Adjusting White Balance Settings 25
Using Window Blanking 26
Setting a Window Blank 26
Deleting a Window Blank 27

Configuring A/V Streams 28
Compression and Image Rate 28
Enabling and Configuring Smart Compression 29
Viewing the RTSP Stream URI 29
Accessing the Still Image URI 30
Saving or Restoring Video Configurations 30
Setting Audio Configurations 30
Configuring Smart Compression Advanced Settings 30

Configuring Events 32
Configuring Motion Detection 32
Analytics Configuration 32
Configuring Digital Inputs and Outputs 33

Configuring Elevate 34
Connecting a Camera to Elevate 34
Viewing Image Health 34

Introduction

Pelco High Definition IP cameras include a web interface that allows you to view the live video and configure the camera through a web browser.

Before you access the web interface, make sure all the procedures described in the camera installation guide have been completed.

Note: Features and options are disabled if they are not supported by the camera.

System Requirements

The web interface can be accessed from any Windows, Mac, or mobile device using one of the following browsers:

- Microsoft Edge
- Mozilla Firefox
- Google Chrome™

Note: The web interface may work with older or unsupported browsers, but this has not been tested.

Accessing Camera Settings

Use the Motorola Camera Configuration Tool (CCT) https://www.pelco.com/camera-configuration-tool/ or the camera web user interface to access camera settings.

Note: Smart Analytics configuration requires the CCT.

Accessing the Camera Web Interface

After the camera has been installed, use the camera's IP address to access the web interface. The IP address can be found in the Motorola Camera Configuration Tool (CCT) — Click the **Network** tab to see the details of the selected cameras.

After you identify the IP address, complete the following procedure to access the web interface:

Note: The web browser must be configured to accept cookies or the camera web interface will not function correctly.

1. On a computer with access to the same network as the camera, enter the camera's IP address into a web browser in the format http://<*camera IP address*>/

   For example: http://192.168.1.40/

2. You will automatically be prompted to enter your username and password to access the camera. You will be asked to create a user with administrator privileges before the device will be operational. For more information, see *Adding a User*.

Creating the Initial User

Cameras do not have a default username and password and will be in a factory default state.

Caution: You must create a user with administrator privileges before the camera is operational.

If the camera is in the factory default state, you will be redirected to the New User page to create an administrator user:

1. Enter a new User Name or keep the default `administrator` name.
2. Enter a new Password for the user. It is recommended to use a secure and complex password.
3. Confirm the new password.
4. For the first user, Administrator must be selected in the Security Group drop-down menu.
5. Click Apply. After creating the user, you will be asked to login.

Logging In

You will automatically be prompted to enter your username and password to access the camera.

- If the camera is in the factory default state, you will be asked to create a user with administrator privileges before the camera will be operational. Use these credentials when logging in.

Note: Pelco recommends that you add a password after your first login. For more information, see *Modifying Users and Passwords*.

Logging Out

To log out of the camera, at the upper right corner of the window, click **Logout**.

Note: After 15 minutes of inactivity, the Web UI will automatically log the user out.

Using the Live View

After you log in, the first page you see is the *Live View*. The *Live View* contains an image panel that displays the live video stream.

Navigating Through the Web Interface

Use the tabs at the top of the window to navigate through the web interface. Click the **Live View** tab at any time to return to this page.

Saving a Still Image

To use this feature, the following settings are required for the camera:

- There is an SD card inserted in the camera. For more information, see the camera's installation guide.
- The camera's onboard storage settings are enabled on the *Storage Management* page. For more information, see *Configuring Storage Management*.
- The camera's video format must be set to MJPEG in the *Video Configurations* page. For more information, see *Compression and Image Rate*.

After all the requirements have been met, you can click **Save Still to SD Card** and the image that is displayed in the Live View page is automatically saved to the SD card.

To download the snapshot, see *Compression and Image Rate*.

Configuring the System Settings

Use the *System* tab to configuring *General Settings*, *Firmware*, *Storage Management*, and *Diagnostics*.

Configuring General Settings

The *General Settings* page allows you to set the camera's identity.

1. Click the **System** tab, and then click the **General Settings** button.
2. In the *Name* field, give the camera a meaningful name.
3. In the *Location* field, describe the camera's location.
4. From the *Mode* drop-down menu, select a dewarp streaming mode option to add additional dewarped fisheye video streams to the default 360° fisheye view. The following dewarping options are ideal options for dewarped views when connecting the Pelco Fisheye camera to a 3rd party VMS:

   - **Full Feature** — This is the standard operating mode that offers the full functionality of the camera. The dewarp streaming options are not available when *Full Feature* is selected.
   - **High Framerate** — This mode will use the maximum image rate possible but will disable self-learning video analytics and sabotage detection on 4K (8 MP), 12 MP Pelco Fisheye cameras.

     Note: If you select an in-camera dewarp streaming mode setting, the Pelco Fisheye camera will automatically disable self-learning video analytics and sabotage detection. The 12 MP Pelco Fisheye camera maximum frame rate will be reduced to 15 fps.

     After a dewarp streaming mode has been enabled, each stream can have camera settings applied to each stream or to all of the streams. Each stream will be referred to as a Head and can have settings applied to individual heads or to all heads.

   - **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.
   - **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 the entire 360° view.
   - **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.

5. When a *Dewarp Streaming Mode* is enabled, in the *Dewarp Streaming Rotation* field, set the rotation of the dewarped fisheye streams by degrees. This setting will only rotate the dewarped streams and will not change the default 360° stream's rotation.
6. From the *View Perspective* drop-down menu, select the mounting orientation that the camera is installed in.

   - **Ceiling** — The camera is mounted to a ceiling and is looking down on a scene.
   - **Wall** — The camera is mounted to a wall and is looking horizontally at a scene. Pelco Smart Analytics and camera Sabotage Detection are currently not supported on wall-mounted Pelco Fisheye cameras.

7. Select any of the *Overlay Settings* checkboxes to display and stamp that information on the camera's video stream. The options are:
   - **Display Date**—Selecting the *Display Date* checkbox also enables the *Date Format* drop-down menu. From the list, choose the date format.
   - **Display Time**
   - **Display GMT Offset**
   - **Display Name**
   - **Display Location**
8. In the *Device Power State* area, click to select the *Power State* from the drop-down menu.
   - **Auto** — The system automatically negotiates the power state; it might be set to PoE+, which is a higher wattage.
   - **Force PoE** — The camera will ask for PoE power standard only, which is lower wattage.
9. In the *Time Settings* area, select how the camera keeps time.
   - To manually set the camera's date and time, enter the time zone on this page.
   - Select the *Automatically adjust clock for Daylight Savings Time* checkbox, if required.
   - To auto-synchronize the camera's date and time with an NTP server, configure the NTP server on the *Network and Security* tab, *Network* page. See the section titled *Configuring the Network Settings*.

   Caution: The time setting must always be current. To ensure that the time is always current you should do one of the following:

   - Set up NTP on the DHCP server, if your VMS supports this feature.

   - Use a valid public NTP server.

   - Manually set the correct time in the Time Settings fields.
10. Click **Apply** to save the settings.

Managing the Camera Firmware

The *Firmware* page provides the current firmware version. From this page, you can also manually upgrade the firmware, reboot the device, and restore to the factory defaults.

- To manually upgrade the camera firmware:
  1. Download the latest version of the firmware .bin file from the Pelco website (www.pelco.com/training-support/).
  2. Click the **System** tab, and then click the **Firmware** button.
  3. Click **Choose File**, and then browse to and locate the downloaded firmware file.
  4. Click **Upgrade**. Wait until the camera upgrade is complete.
- To reboot the camera, in the *Reboot Device* area, click **Reboot**.
- To restore the camera to factory defaults, but preserve Network settings, in the *Restore to Factory Defaults* area, select the *Soft Reset* checkbox.
- To restore the camera to factory defaults, in the *Restore to Factory Defaults* area, click **Restore**.

Configuring Storage Management

On the *Storage Management* page, you can enable the camera's onboard storage feature and download recorded video directly from the camera.

Note: For cameras with 2 microSD card slots, you can now use one or both SD card slots. The camera will record video to both SD card slots simultaneously if two SD cards are inserted. The total storage capacity of the system is the combined storage capacity of each of the individual cards. The second microSD card slot is reserved for future use.

To access the *Storage Management* page, click the **System** tab, and then click the **Storage Management** button.

Current information about the camera is presented in the *Device Information* section at the top of the page. It includes *Status*, *Total Capacity*, *Current Usage*, and *Remaining Capacity*.

You can perform two actions in the **Device Information** area:

- To format the SD card, click **Format Card**.
- Click to select or deselect **Enable video alert overlay on severe SD card failure**. When enabled, this feature shows an overlay on the video stream when the card cannot record video. The functionality of enabling ONVIF Profile G is to allow the connected VMS system to be able to download recorded video from the camera's onboard storage when there are gaps to fill in the VMS video due to network outages.

Enabling Onboard Storage

To use the camera's onboard storage feature, you must first insert an SD card into the camera. Refer to the camera's installation manual for the location of the SD card slot.

The SD card will record from the camera's highest resolution stream. In most cases, this will be the primary stream.

Note: For cameras with 2 microSD card slots, you will only be able to configure the microSD card that is inserted first, in either card slot. The second microSD card slot is reserved for future features.

1. Click the **System** tab, and then click the **Storage Management** button.
2. In the **Settings** area, click to select the **Enable Onboard Storage** checkbox.
3. By default, the camera is set to only record to the SD card when it is unable to communicate with the network video management server. If you prefer to have the camera record video to both the network video management server and to the SD card, click to deselect the checkbox for the **Record only when server connection is interrupted** to disable the setting.
4. Select one of the following recording modes:
   - **Continuous:** the camera never stops recording to the SD card.
   - **On Motion:** the camera only records when there is motion in the scene.
     If you are configuring a Pelco 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.

   The recorded video will be divided into files no more than five minutes in length or 100 MB in size.
5. On the *Video Configurations* page, make sure the format is set to H.264 or H.265 to maximize the SD card recording capacity and performance. See the section titled *Compression and Image Rate*.

Downloading Recorded Video from the Web Interface

Listed in the *Export Recordings* section are all the videos that have been recorded to the SD card.

It is recommended that you download recorded video from the web interface. However, if your bandwidth is limited, you can choose to download the recorded video directly from the SD card. For more information, see *Downloading Recorded Video from the SD Card*.

To download recorded video from the web interface, perform the following:

1. Click the **System** tab, and then click the **Storage Management** button.
2. In the *Export Recordings* area, click to select the checkbox beside all the videos you want to download.
   To help you find the video you want, filter the videos by date and time. Click to select the checkbox for **Filter**, type in the dates in the *From* and *To* fields, and then select the *From* and *To* time range.
3. 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 might 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

If you do not have enough bandwidth to download recorded video directly from the web interface, you can choose to download the recorded video directly from the SD card.

To download recorded video directly from the SD card:

1. Click the **System** tab, and then click the **Storage Management** button.
2. In the **Settings** area, click to deselect the **Enable Onboard Storage** checkbox, and then click **Apply**.
3. Remove the SD card from the camera.
4. Insert the SD card into a card reader.
5. When the *Windows AutoPlay* dialog box appears, select **Open folder to view files**.
6. To download all the recorded videos, click **Download All**; to download specific video, select the video files you want then click **Download Selected**.
7. When you are prompted, choose a location to save the video files.
   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 click to select the checkbox for Enable Onboard Storage to begin recording to the SD card again.

Deleting Recorded Video

As the SD card becomes full, the camera automatically starts overwriting the oldest recorded video. You can also choose to manually delete video to make room for new recordings.

1. Click the **System** tab, and then click the **Storage Management** button.
2. Delete video by one of the following methods:

- To delete individual video files, in the *Recordings* section, select all of the files you want to delete from the *Recordings* list, click **Delete**, and then click **OK** in the confirmation dialog box.
- To delete all of the recorded video files, in the section, at the right of the information, click **Format Card** to format the SD card, and then click **OK** in the confirmation dialog box.

Extended Settings

On the Extended Settings page, you can configure ONVIF Settings.

1. Select the **Enable Multi-Packet XML Documents** checkbox to enable multi-packet XML documents to reduce metadata size. Only for Video Management systems that support multi-packet XML documents.

   Important: you must enable multi-packet XML when connecting to VideoXpert to ensure that bounding boxes align with their targets.

2. Select the **Enable Analytics Options Requests** checkbox to enable the GetAnalyticsModuleOptions and GetRuleOptions Requests.
3. Select the **Enable Analytics XML Metadata** checkbox to send analytics metadata in the XML metadata stream.
4. Select the **Enable Run-Length Encoding of Motion Mask** checkbox to enable run-length encoding of the motion mask. Only for Video Management Systems that do not require an un-encoded mask.
5. Select the **Enable Supplemental Events** checkbox to send supplemental events not defined by ONVIF that may be useful to some Video Management Systems.
6. Select the **Enable Singleton Analytics Events** checkbox to send singleton Analytics events instead of property events.
7. Click **Apply** to save your changes.

Configuring Diagnostics

The *Device Log* page allows you to view the camera system logs and the camera access logs.

1. Click the **System** tab, and then click the **Diagnostics** button.
2. In the **Type** drop-down menu, select one of the following:
   - **Access Logs** — Logs of users who have logged into the web interface.
   - **System Logs** — Logs of camera operations.
3. In the **Minimum Log Level** drop-down menu, select the minimum level of log message you want to see:
   - **Error** — Sent when the camera encounters a serious error. These are the highest level log messages.
   - **Warning** — Sent when the camera encounters a minor error such as an invalid username and password.
   - **Info** — Status information sent by the camera. These are the lowest level log messages.
4. In the **Maximum Number of Logs** drop-down menu, select the number of log messages you want displayed.
5. Click **Update**.

Note: There is also a Filter field with text that you can enter to search against.

The logs update to display the filtered information. The most recent log event is always displayed first.

Configuring the Network and Security Settings

Use the *Network and Security* tab to configure the *Network*, *Security*, *Users*, *802.1X*, *SNMP*, *DSCP*, and *IP Filter* settings.

Configuring the Network Settings

On the *Network* page, you can change how the camera connects to the server network and choose how the camera keeps time.

Note: You can only set the HTTPS port, the RTSP port, and the NTP Server in the camera web interface.

1. Click the **Network and Security** tab, and then click the **Network** button.
2. At the top of the page, select how the camera obtains an IP address:
   - **Obtain an IP address automatically**: select this option to connect to the network through an automatically assigned IP address.
     The IP address is obtained from a DHCP server. If it cannot obtain an address, the IP address will default to addresses in the 169.254.x.x range.
   - **Use the following IP address**: select this option to manually assign a static IP address.
     - **IP Address**: Enter the IP Address to use.
     - **Subnet Mask**: Enter the Subnet Mask to use.
     - **Default Gateway**: Enter the Default Gateway to use.
3. Click to select the checkbox for **Disable setting static IP address through ARP/Ping method** to disable the ARP/Ping method of setting an IP address.
4. In the *IPv6 Settings* area, click to select the checkbox for *Enable IPv6*, and then configure the following settings.

   Note: Enabling IPv6 does not disable IPv4 settings.

   a. Click to select the checkbox for **Accept Router Advertisements** if using Stateless Address Auto-Configuration.
   b. From the **DHCPv6 State** drop-down menu, select one of the following:
      - **Auto**: DHCPv6 state is determined by router advertisements (RA).

        Note: The Accept Router Advertisements setting must be enabled for this setting to perform as expected.
      - **Stateless**: the camera only receives DNS and NTP information from the DHCPv6 server. It does not accept an IP address from the DHCPv6 server.
      - **Stateful**: the camera receives IP address, DNS and NTP information from the DHCPv6 server.
      - **Off**: the camera does not communicate with the DHCPv6 server.
   c. In the **Static IPv6 Addresses** field, enter the preferred IPv6 address. Click the add icon (+) to add another address.

To change the prefix length, enter the preferred IPv6 address using Classless Inter-Domain Routing (CIDR) notation. For example, `2001:db8::1/32` would indicate the address prefix is 32-bits long.

By default, the prefix length is set to `/64`.

Note: The configured prefix length might not display correctly in the web interface, but the prefix used by the camera will be the configured length.

d. In the *Default Gateway* field, type the default gateway you prefer to use. You can only assign a default gateway if RA is disabled.

The IPv6 addresses that can be used to access the camera are listed under the *Current IPv6 Addresses* area.

5. To customize the hostname, enter it in the *Network Hostname* field.
6. In the *DNS Lookup* area, select how the camera will obtain a Domain Name System (DNS) server address.
   - Click to select the checkbox for *Obtain DNS server address automatically* to automatically find a DNS server.
   - Click to select the checkbox for *Use the following DNS server addresses* to manually set DNS server addresses. You can set up to three addresses:
     - In the *Preferred DNS server* field, type the address of the preferred DNS server.
     - (Optional) In the *Alternate DNS server 1* field, type the address of an alternate DNS server. If the preferred server is not available, the camera will attempt to connect to this server.
     - (Optional) In the *Alternate DNS server 2* field, type the address of another alternate DNS server. If both the preferred server and the first alternate server are unavailable, the camera will attempt to connect to this server.
7. In the Port Settings area, specify which control ports are used to access the camera. You can enter any port number between 1 and 65534. The default port numbers are:
   - *HTTP Port*: 80
   - *HTTPS Port*: 443
   - *RTSP Port*: 554
   - *RTSP Replay Port*: 555

   To limit camera access to secure connections only, click to deselect the checkbox for *Enable HTTP connections*. HTTP Port access is enabled by default.
8. In the NTP Server area, select the checkbox for how the server is configured—*DHCP* or *Manual*. If you select *Manual*, type the server address in the *NTP Server* field.
9. In the MTU area, set the Maximum Transmission Unit (MTU) size in bytes. Type a number in the *MTU size* field that is within the available range displayed on the right. Lower the MTU size if your network connection is slow.
10. In the *Link Settings* area, click to select an option from the Speed & Duplex drop-down menu. The Auto-negotiation (default) setting is the preferred setting for most cameras, and will negotiate the optimal speed and duplex setting for your network connection.

11. In the Security area, click to select from the drop-down menu the Minimum TLS version that the camera should to encrypt the communication between camera and server, and to block older TLS versions that should not be used.
    - TLS 1.2 is recommended for increased security.
    - TLS 1.1 can be selected if it is required for backwards compatibility.

    Note: Some cameras may also have the TLS 1.1 opttions, which can be selected if it is required for backwards compatibility.
12. Click **Apply** to save the settings.

Enabling SRTP Streaming

SRTP streaming allows the camera to stream via SRTP encryption to Video Management Systems that also support SRTP. To enable SRTP streaming, the camera must have the correct firmware installed.

Note: Using SRTP for third-party integrations may require additional steps. For information on configuring SRTP streaming when using third-party integrations, refer to the manufacturer's documentation.

Requirements

- SRTP streaming requires an HTTP connection.

  You can enable HTTP connections in your camera's web interface. For instructions, see *Configuring the Network Settings*.
- SRTP streaming requires an OpenSSL library connection and does not work with FIPS 140-2 or NXP TPM.

  You can change the encryption engine to use OpenSSL on the Security page in your camera's web interface. For instructions, see *Modifying Security Settings*.
- SRTP streaming requires a Unicast and Multicast over UDP connection.

Modifying Security Settings

1. Click the **Network and Security** tab, and then click the **Security** button.
2. In the **Encryption Engine** drop-down list, select the type of encryption to use.
   - Open SSL is the default option for encryption.
   - FIPS 140-2 enables FIPS 140-2 level 1 encryption.
3. Click **Apply** to save the settings.

Note: FIPS 140-2 Level 1 requires the purchase of a FIPS camera license.

Caution:Changing this setting on your camera will require your camera to reboot and you will lose the video stream for that time. Pelco recommends that you apply this setting during during non-critical operating times.

Configuring the Users

On the *Users* page, you can add new users, modify existing users, and remove users.

Adding a User

1. Click the **Network and Security** tab, and then click the **Users** button.
2. Click **Add...**.
3. On the *Add User* page, enter a *User Name* and *Password* for the new user.
4. In the *Security Group* drop-down menu, select the access permissions available to this new user.
   - The **User** has access to the Live View, but cannot access any of the setup pages.
   - The **Operator** has access to the Live View but limited access to the setup features. The user can access the *General Settings* page, *Imaging* page, *Video Configurations* page, *Motion Detection* page, *Window Blanking* page, and the *Digital Inputs and Outputs* page. The new user can also configure onboard storage settings but cannot delete video recordings or format the SD card.
   - The **Administrator** has full access to all the available features in the camera web interface.
5. Click **Apply** to add the user.

Modifying Users and Passwords

1. Click the **Network and Security** tab, and then click the **Users** button.
2. Click to select a user from the User Name (Security Group), and then click **Modify**.
3. To change the user's password, enter a new password for the user.
4. To change the user's security group, select a different group from the **Security Group** drop-down menu.

   Note: You cannot change the security group for the administrator account.
5. Click **Apply** to save the settings.

Removing a User

Note: You cannot remove the default Administrator user.

1. Click the **Network and Security** tab, and then click the **Users** button.
2. Click to select a user from the *User Name (Security Group)*, and then click **Remove**.

   Caution: There is no confirmation dialog box. The user is removed immediately.

Keeping Usernames and Passwords After Firmware Revert

To add a layer of security to protect the camera from theft, you have the option of keeping the camera's current usernames and passwords after a firmware revert.

Caution: If you have set your camera to use FIPS 140-2 encryption, we recommend that you do not choose to keep usernames and passwords after a firmware revert. The password and username is not stored in a FIPS 140-2 compliant manner and may affect your FIPS 140-2 compliance.

Normally if you restore the camera firmware back to the factory default settings, the camera returns to using the default username and password. When you enable this feature, the camera will continue to use the configured username and passwords, so the camera cannot connect to new servers without the appropriate credentials.

Caution: Forgetting your own username or password after enabling this setting voids your warranty. The primary method of restoring the factory default username and password will be disabled.

1. Click the **Network and Security** tab, and then click the **Users** button.
2. At the bottom of the Users page, click to select the checkbox for **Do not clear usernames or passwords on firmware revert** .
3. After you select the checkbox, the following popup message appears:

   Please store your administrator password in a safe place. Password recovery is not covered by warranty and loss of password voids your warranty.

4. Click **OK** if you agree to the feature limitations.

Always keep a copy of your password in a safe place to avoid losing access to your camera.

Configuring 802.1x Port-Based Authentication

If your network switch requires 802.1x port-based authentication, you can set up the appropriate camera credentials so that the video stream is not blocked by the switch. You can configure multiple profiles (Saved 802.1x Configurations); but be aware that you can only enable one profile at a time.

Configuring the 802.1X Port Security

1. Click the **Network and Security** tab, and then click the **802.1x** button.
2. From the *EAP Method* drop-down menu, select one of the following and complete the related fields:
   - Select **PEAP** for username and password authentication.
     - *Configuration Name:* enter a profile name.
     - *EAP Identity:* enter the username that will be used to authenticate the camera.
     - *Password:* enter the password that will be used to authenticate the camera.
   - Select **EAP-TLS** for certificate authentication.
     - *Configuration Name:* Enter a profile name.
     - *EAP Identity*: Enter the username that will be used to authenticate the camera.
     - *TLS Client Certificates*: Click **Choose File**, and then navigate to and select the PEM-encoded certificate file to authenticate the camera.
     - *Private Key*: Click **Choose File**, and then navigate to and select the PEM-encoded private key file to authenticate the camera.
     - *Private Key Password*: If the private key has a password, enter the password here.
     - *Upload Certificate*: 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.
3. If appropriate, click to select the checkbox for *Authenticate Server*.
4. Click **Save Config** to save the authentication profile.
   If this is the first profile added to the camera, it is automatically enabled.

   Saved configurations are listed under Saved 802.1x Configurations.

Switching 802.1X Authentication Profiles

To use a different authentication profile, select the saved configuration then click **Enable**.

Removing an 802.1X Authentication Profile

To delete one of the authentication profiles, select the saved configuration, and then click **Remove**.

Returning to the Network Page

To return to the *Network and Security* tab, *Network* page, click the **Back To Network Setup** button at the lower left of the page.

Configuring SNMP

You can use the Simple Network Management Protocol (SNMP) to help manage cameras that are connected to the network. When SNMP is enabled, camera status information can be sent to an SNMP management station.

On the *SNMP* page, you can configure the camera's SNMP settings and choose the status information that is sent to the management station page.

1. Click the **Network and Security** tab, and then click the **SNMP** button.
2. In the *SNMP Configuration* area:
   a. Click to select the checkbox for **Enable SNMP**.
   b. From the **Version** drop-down menu, select the preferred SNMP version. Be aware that both versions can be configured, but only one can be enabled at a time.
3. If you selected **SNMP v2c**, you can request camera status information through an SNMP Get request and receive trap notifications from the camera.
   a. In the *SNMP v2c Settings* area, click to select the checkbox for *Enable Traps* to enable traps from the camera.
   b. In the *Read/Write Community* field, enter the read community name for the camera. The name is used to authenticate SNMP traffic. Only SNMP management stations with the same read community name will receive a response from the camera.
   c. In the *Trap Destination IP* field, enter the IP address of the management station where the traps will be sent.
4. If you selected **SNMP v2c**, in the Available Traps area, select the traps that will be sent:
   - ***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.
   - ***Camera Tampering:*** a trap notification will be sent when the camera's video analytics detects a sudden scene change.
   - ***Edge Storage Status*****:** a trap notification will be sent when the status of the SD card changes.
5. If you selected **SNMP v3**, you can request status information through an SNMP Get request. SNMP v3 does not support traps. 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.

   In the SNMP v3 Settings area, complete the following:

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 **Apply** to save the settings.

Configuring the IP Filter

On the *IP Filter* page, you can control which IP addresses are able to connect to your camera.

1. Click the **Network and Security** tab, and then click the **IP Filter** button.
2. In the IP Filter area, click to select the checkbox for Enable IP Filter, to enable IP filtering.
3. Click to select how the camera should filter IP addresses—either by allowing or denying access:

- **Allow Access**: Select this option to only allow access to the specific IP address entries you will make below.

  Caution: 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 might be locked out of your camera.

- **Deny Access**: Select this option to deny access to the specific IP address entries you will make below. This is the default option.

4. Add all the *IP Filter Entries* to which access with be either allowed or denied:

   a. Click the add icon (+) to add an entry to the *IP filter Entries* list.

   b. In the IPv4, IPv6 or CIDR range field that appears, enter the IPv4, IPv6 or CIDR range of IP addresses that you would like to filter.

   c. Continue to add more entries to the list until you have added all of the necessary IP addresses to be filtered.

   You can add up to 256 *IP Filter Entries*.

5. Click **Apply** to save the settings.

Note: If you have denied or not allowed access to the IP address you are currently using to connect to your camera, your web interface connection will close after you click **Apply**.

Managing Certificates

On the *Certificates* page, administrators can manage certificates. Certificates are used to authenticate devices and encrypt communication over the network.

In the *Certificates* area, you can view the following information:

- *Cert ID*: Used to uniquely identify the certificate.
- *Subject*: The entity a certificate belongs to: a machine, an individual, or an organization.
- *Issuer*: The entity that verified the information and signed the certificate.
- *Algorithm*: This contain a hashing algorithm and a digital signature algorithm.
- *Expiry Date*: The date when the certificate expires.
- *Type*: The type of certificate, i.e., trusted or not trusted.

Downloading Certificates

1. To download a Certificate, select it from the list.
2. Click the **Download** button.

   Certificates are downloaded as .pem files.

Removing Certificates

1. To remove a Certificate, click the **Remove** button.
2. Click the **OK** button.

Downloading Certificate Signing Requests

1. To download the Certificate Signing Request (CSR), click the download **CSR button** and enter the following information:
   - *Common Name*: The primary hostname of the server.
   - *Alternative Name*: The alternative values associated with the certificate, e.g., email address, IP addresses, URIs, DNS names.
   - *(Optional) Organization*: The name of the organization requesting the certificates.
2. Click the **Download** button to download the CSR.

Uploading Certificates

1. To upload a certificate, click **Upload Cert**.
   a. *Certificate*: click **Choose File** to upload a certificate.
   b. *Private key*: click **Choose File** to upload a private key.
   c. *Private key password*: enter the private key password.
2. Click the **Upload** button to upload the Cert.

Uploading CA Certificates

1. Click the **Upload** button to upload the certificate.
2. To upload a CA certificate, click **Upload CA Cert**.
   a. *CA Certificate*: click **Choose File** to upload a CA certificate.
   b. *CA Certificate ID*: enter the CA certificate ID.
3. Click the **Upload** button to upload the CA certificate.

Configuring Imaging

On the *Imaging and Display* page, you can control the camera's day/night and exposure settings and view the camera's live video stream.

Configuring General Imaging Settings

You can set the camera's zoom and focus through this page.

1. Click the **Imaging** tab, and then click the **General** button.
2. View the following information:
   - *Current Exposure*
   - *Current Gain*
   - *Last Known Light Level*
3. To set how the camera compensates for the environmental lighting conditions, define the following *Day/Night Settings*:
   a. Use the *Day/Night Mode* drop-down menu to set how the video image switches between day and night mode.
      - **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.
      - **Color**: The video image will always be in color.
      - **Monochrome**: The video image will always be monochrome.

   b. If you selected the **Automatic** *Day/Night Mode*:
      - Use the *Day/Night Threshold (gain dB)* slider to set the day/night threshold. Move the slider to select the light level when the camera switches between day mode and night mode.The slider is only available when the Day/Night Mode setting is set to **Automatic**. The slider might display one of the following values:
        – **Day/Night Threshold (EV):** 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.
        – **Day/Night Threshold (gain dB):** The slider value is in decibels (dB).

   c. **Enable Adaptive IR Compensation:** You can enable automatic infrared adjustments through Adaptive IR Compensation.This allows the camera to automatically adjust the video image for saturation caused by IR illumination.
   d. **Enable Night Visibility Check:** You can manually enable or disable the night visibility check on a camera.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 disabled, the camera will use a less optimal method to determine if the light level is sufficient to switch to day mode.

      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.

4. To adjust the exposure of the image, adjust the *Exposure Settings*:
   - **Flicker Control:** If your video image flickers because of fluorescent lights around the camera, you can reduce the effects of the light by setting the Flicker Control to the same frequency as your lights. Generally, Europe is **50Hz** and North America is **60Hz**.

     Note: Resetting this control will stop the video stream for a few seconds.
   - **Exposure:** Click to select the appropriate exposure rate from the drop-down menu. Allow the camera to control the exposure by selecting **Automatic**. In some cases, **Automatic** is the only option available.

     Note: Increasing the manual exposure time might affect the image rate.
   - **Maximum Exposure:** If you selected **Automatic** as the *Exposure Offset*, you can limit the automatic exposure setting by selecting a maximum exposure level. The Maximum Exposure drop-down menu is only available when the Exposure setting is set to Automatic.
     By setting a maximum exposure level for low-light situations, you can control the camera's exposure time to let in the maximum amount of light without creating blurry images.
   - **Priority:** If you selected **Automatic** as the *Exposure Offset*, you can set **Image Rate** or **Exposure** as the priority.
     - When 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 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.
   - **Enable Wide Dynamic Range:** You can enable automatic color adjustments through Wide Dynamic Range (WDR). This allows the camera to adjust the video image to accommodate scenes where bright light and dark shadow are clearly visible. See the section titled *Understanding Backlight Compensation (BLC) and Wide Dynamic Range (WDR)*.
   - **Backlight Compensation:** If your scene has areas of intense light that cause the overall image to be too dark, click to select the checkbox for *Backlight Compensation*, and then enter a value (either by typing a number, or selecting one using the up and down arrows) that results in a well-exposed image. See the section titled *Understanding Backlight Compensation (BLC) and Wide Dynamic Range (WDR)*.
   - **Maximum Gain:** To limit the automatic gain setting, click to select the the appropriate *Maximum Gain* from the drop-down menu.
     By setting the maximum gain level for low-light situations, you can maximize the detail of an image without creating excessive noise in the images.
5. If the PTZ camera is installed upside down, you can get an upright image by configuring the "Image mirror settings":
   - **None**: no processing gets applied to the image.
   - **Flipped**: the image gets flipped by 180°.
6. Click **Apply** to save the settings.

Understanding Backlight Compensation (BLC) and Wide Dynamic Range (WDR)

- **BLC** is a feature that optimizes exposure in the foreground and background of security video. BLC uses a single exposure time for the whole image, and uses auto exposure to ignore very bright regions (or very dark, if set negative). You must choose whether the camera optimizes the foreground or the background.
- **WDR** enables advanced image processing, and helps draw out detail from both very bright and dark areas in a scene. For example: Use WDR in lobbies or store fronts with natural light streaming in through windows, where you also have dark areas in the same scene. WDR takes multiple exposures of the scene in a single time slice. Two scans are taken of each video frame, one with a short exposure optimized for brighter portions of the scene, the other longer to draw out detail in dark areas. The image processing combines the two images to form one view, incorporating the best detail and clarity across the entire scene.

If you enable both BLC and WDR, the camera will deliver the detail you will see in WDR-only mode, but will ignore optimization on the very brightest (or darkest) portions of the image.

Adjusting White Balance Settings

1. Click the **Imaging** tab, and then click the **White Balance** button.
2. View the following information:
   - *Current Exposure*
   - *Current Gain*
   - *Last Known Light Level*
3. Adjust the video image as required.
   You can either use a preset configuration, or you can create your own custom configuration. Use the **Preset** drop-down menu to select the preferred configuration:
   a. **Pelco:** This preset provides the recommended balance of brightness and color for video surveillance.
   b. **Standard:** This preset is configured for general day/night changes in an indoor or outdoor scene.
   c. **Vivid:** This preset provides increased color and brightness for a more saturated image.
   d. **Custom:** Select this option to manually adjust the following image settings:

      Note: The *Contrast* setting is disabled if you selected *Enable Wide Dynamic Range*. See the section titled *Configuring General Imaging Settings*

      - **Saturation:** You can adjust the video's color saturation by entering a percentage number.
        0 creates a black and white image, while 100 creates intense color images.
      - **Sharpness:** You can adjust the video's sharpness by entering a percentage number.
        0 applies the least amount of sharpening, while 100 applies the most sharpening to make the edges of objects more visible.
      - **Brightness:** You can adjust the video's brightness by entering a percentage number.
        0 applies the least amount of contrast, while 100 applies the most contrast between objects in the image.

- **Contrast:** You can adjust the video's contrast by entering a percentage number. 0 applies the least amount of contrast, while 100 applies the most contrast between objects in the image.

e. Move the *Temporal Filter Strength* slider slightly to the left or right to adjust the amount of noise vs. blur in the scene. This reduces image noise by averaging the noise over several frames.

Note: Start by making small adjustments only because applying excessive changes might degrade the overall image quality.

If the image looks noisy, move the slider to the right to reduce the amount of noise in the scene and decrease the bandwidth used.

If the image looks blurry, move the slider to the left to reduce the amount of blur in the scene and increase the bandwidth used.

By default, the slider is set to the middle, which is 50.

4. Use the **White Balance** drop-down menu to select how the white balance settings are controlled:
   - **Automatic**: The camera will automatically control the white balance.
   - **Custom**: Manually set the **Red** and **Blue** levels.
5. Click to select the checkbox for Dominant Color Compensation to enable an alternate auto white balance algorithm which should be used when a large area in the field of view contains one color. For example, a camera that is overlooking a grass field. For this example, the Dominant Color Compensation white balance mode will improve the white balance to a more neutral color.
6. Click **Apply** to save the settings.

Using Window Blanking

On the *Window Blanking* page, you can set window blanks (privacy zones) in the camera's field of view to block out areas that you do not want to see or record. The camera supports up to 64 window blanks.

Setting a Window Blank

1. Click the **Imaging** tab, and then click the **Window Blanking** button.
2. To add a window blank (privacy zone), click **Add**. A window blank box is added to the video image.
3. To define the window blanking box, perform any of the following:
   a. Drag any side of the box to resize the window blank. Window blank boxes can only be rectangular in shape.
   b. Click inside the box then drag to move the window blank box.
4. To set the window blank as removable:
   a. Click the **Enable** checkbox in the **Removable Blur** settings.
   b. Use the **Blurriness** slider to define the amount of blur in the privacy zones. All Blurriness settings will make the video from that zone completely obscured.
5. Click **Apply** to save the settings.

Deleting a Window Blank

1. Use one of the following methods to delete a window blank (privacy zone):
   - In the list of window blanks, click to select the name of the window blank to delete (**Privacy Zone [#]**), and then click **Remove**.
   - Click to select the window blank box to delete, click the **X** at the top-right corner of the gray box to delete the window blank box, and then click **OK** in the confirmation dialog box.
2. Click **Apply** to save the settings.
3. Click **OK** in the confirmation dialog box.

Configuring A/V Streams

Configure compression and image rate, smart compression, RTSP stream URI, Still Image URI, Audio Configurations, and advanced smart compression on the A/V Streams page.

Compression and Image Rate

On the *Compression and Image Rate* area, you can change the camera's compression and image quality settings for sending video over the network. You can change the camera's compression and image quality settings separately for primary, secondary, and tertiary streams.

Note: If a camera with video analytics is physically moved or adjusted, or if the focus or zoom level is changed, reset the learning progress to provide accurate results. If the camera's image rate and compression or display settings are updated, the learning progress might reset automatically.

To enable easy access and lower bandwidth usage, the web interface only displays video in JPEG format. The settings on this page only affect the video transmitted to the network video management software.

Note: The camera might automatically adjust compression quality in order to abide by the bandwidth cap specified.

Follow these steps for each of the primary, secondary, and tertiary streams to change the compression and image quality settings for each stream.

1. Click the **A/V Streams** tab, and then click the **Video Configurations** button.
2. In the *Compression and Image Rate* area:
   a. In the **Format** drop-down menu, select the preferred streaming format for displaying the camera video in the network video management software.

      If you are using the Onboard Storage feature, then **H.264** or **H.265** must be used. For more information, see *Enabling Onboard Storage*.

   b. In the **Max Image Rate** field, enter how many images per second you want the camera to stream over the network.

      Note: Adjusting the image rate across the maximum fps boundary will stop the video stream for a few seconds.

      If the camera is operating in High Framerate mode, then the maximum image rate is increased. For more information on the High Framerate mode, see *Configuring General Settings*.

   c. In the **Max Quality** drop-down menu, select the desired image quality level.

      Image quality setting of 1 will produce the highest quality video and require the most bandwidth.

   d. In the **Max Bitrate** field, enter the maximum bandwidth the camera can use.

   e. In the **Resolution** drop-down menu, select the preferred image resolution.

   f. In the **Min Keyframe Interval** field, enter the number of frames between each keyframe.

3. Click **Apply** to save the settings.

Enabling and Configuring Smart Compression

Smart Compression technology operates by separating foreground objects and background areas, then reduces bandwidth by increasing compression to the background areas. In this way, maximum quality is retained for subjects of interest while reducing bandwidth for unchanging backgrounds.

When enabled, the camera will automatically switch to idle scene mode settings when there are no motion events detected. A motion event is when the camera detects pixel motion in the scene. For more information, see the section titled *Configuring Motion Detection*.

The camera uses pixel change motion to detect foreground objects and therefore uses the standard Motion Detection sensitivity settings of the camera.

1. Click the **A/V Streams** tab, and then click the **Video Configurations** button.
2. In the *Smart Compression Settings* area, click to select the checkbox for *Enable* to enable *Smart Compression*.
3. In the **Min Image Rate** field, enter how many images per second you want the camera to stream when there is no motion in the scene.
4. In the **Idle Keyframe interval** field, enter the number of frames between each keyframe (between 1 and 254) when there is no motion in the scene.
5. In the *Bandwidth Reduction* drop-down menu, click to select one of the options:
   - **Low**
   - **Medium** (recommended)
   - **High**
   - **Custom**
6. Click **Apply** to save the settings.
7. If you chose **Custom** for the *Bandwidth Reduction*, see the section titled *Configuring Smart Compression Advanced Settings*.

Viewing the RTSP Stream URI

You can only view the RTSP stream address in the camera web interface. The RTSP Stream URI allows you to watch the camera's live video stream from any application that supports viewing RTSP streams, including many video players.

1. Click the **A/V Streams** tab, and then click the **Video Configurations** button.
2. View the auto-generated URIs in the RTSP Stream URI area:
   - **Unicast** — Use this URI to view the video stream from one video player at a time.
   - **Multicast** — Use this URI to view the video from more than one video player simultaneously.
3. To view the RTSP stream:
   a. Copy and paste the appropriate URI into your video player. DO NOT open the live video stream yet.
   b. Add your username and password to the beginning of the address in this format: rtsp://<username>:<password>@<generated RTSP Stream URI>/

      For example: rtsp://admin:admin@192.168.1.79/defaultPrimary?streamType=u
   c. Open the live video stream.

Accessing the Still Image URI

On the *A/V Streams* tab, *Video Configurations* page, you can access the last still image frame that the camera recorded.

1. Click the **A/V Streams** tab, and then click the **Video Configurations** button.
2. In the *Still Image URI* area, click the link.
   - The last recorded frame of video from the camera's tertiary stream is displayed if the encoding type is set to H.264 or H.265. The last frame comes from the primary stream, maximum resolution, if the encoding is set to MJPEG.
   - You can save or print the image directly from the browser.

Saving or Restoring Video Configurations

After you have updated all settings on the Video Configurations page, do one of the following:

- Click **Apply** to save the settings.
- Click **Restore Defaults** to restore all settings (saved and unsaved) to the default settings.

Setting Audio Configurations

Use the settings on the *Audio* page to adjust the audio quality of the Video Intercom.

For encoding the audio stream, you can choose from the Opus sound encoder, which produces high-quality sound, or the G.711 protocol sound encoder. Use the Opus encoder if you are using a video management system that supports the Opus protocol. Otherwise use the widely supported G.711 protocol.

1. Click the **A/V Streams** tab, and then click the **Audio Configurations** button.
2. In the *Audio Configuration* section, in the **Encoding** field, specify the audio encoder to use:
   - **Opus**: High quality audio codec is available if required.
   - **G.711**: This default setting is supported on various platforms.
3. In the *Device Speaker* section, use the **Volume** slider to adjust the volume on the speaker (from 0 to 100).
4. In the *Device Microphone* section:
   a. Use the *External Input Gain* slider to adjust the gain for any line-level audio input that is connected to the audio input connector on the I/O terminal block.
   b. Use the *Internal Mic Gain* slider to configure the gain for the microphone that is built into the camera.
5. Click **Apply** to save the settings.

Configuring Smart Compression Advanced Settings

If you enabled *Smart Compression* on the *Video Configuration* page (see the section titled *Enabling and Configuring Smart Compression*), configure the Smart Compression Advanced Settings.

1. Click the **A/V Streams** tab, and then click the **Smart Compression** button.
2. In the **On Motion** section, **Background Quality** field, enter the compression quality for the background (between the default of 6 and the lowest setting of 20).

3. In the **On Idle Scenes** section:
   - **Post-motion delay** field, enter the delay (in seconds) after motion has ended before the camera drops into idle scene settings (between 5 and 60)
   - **Image Rate** field, enter the encoding frame rate (images per second) when there is no motion in the scene.
   - **Quality** field, enter the compression quality when there is no motion in the scene (between 6 and 20).
   - **Max Bitrate** field, enter the maximum number of kilobytes per second when there is no motion in the scene.
   - **Keyframe Interval** field, enter the number of frames between each keyframe when there is no motion in the scene (between 1 and 254 frames).
4. Click **Apply** to save the settings.

Configuring Events

Use the *Events* tab to configure *Motion*, *Sabotage*, *Analytics Configuration*, and *DIO* settings.

Note: Other analytics events that are not available in the camera UI can be configured using CCT.

Configuring Motion Detection

On the *Motion Detection* page, you can define the green motion detection areas in the camera's field of view. Motion detection is ignored in areas not highlighted in green.

To help you define motion sensitivity and threshold, motion is highlighted in red in the image panel.

Note: This motion detection setting configures pixel change detection in the camera's field of view. If you are configuring a Pelco video analytics camera, you will need to configure the detailed analytics motion detection and other video analytics features through the Client software.

1. Click the **Events** tab, and then click the **Motion** button.
2. Define the motion detection area.
   The entire field of view is highlighted for motion detection by default. To define the motion detection area, use any of the following tools:
   - Click **Clear All** to remove all motion detection areas on the video image.
   - Click **Set All** to set the motion detection area to span the entire video image.
   - To set a specific motion detection area, click **Select Area** then click and drag anywhere on the video image.
   - To clear a specific motion detection area, click **Clear Area** then click and drag over any motion detection area.
   - Use the **Zoom In** and **Zoom Out** buttons to locate specific areas in the video image.
3. In the **Sensitivity** field, enter a percentage number to define how much each pixel must change before it is considered in motion.
   The higher the sensitivity, the smaller the amount of pixel change is required before motion is detected.
4. In the **Threshold** field, enter a percentage number to define how many pixels must change before the image is considered to have motion.
   The higher the threshold, the higher the number of pixels must change before the image is considered to have motion.
5. If the camera is connected to a third-party video management system (VMS), and then click to select the checkbox for *Enable Onvif MotionAlarm Event*.
   When it is enabled, the camera can send motion alarm information to the VMS according to the appropriate ONVIF protocol.
6. Click **Apply** to save the settings.

Analytics Configuration

On the *Analytics Configuration* page, you can enable, suspend, or reset Self Learning Analytics.

1. Click the **Events** tab, and then click the **Analytics Configuration** button.
2. Click to select the checkbox for **Enable Self Learning** to enable self learning analytics.

3. Click to select the checkbox for **Suspend Self Learning** to temporarily suspend self learning analytics.
4. Click **Apply** to save the settings.
5. Click Restore Defaults to restore the default settings.

Configuring Digital Inputs and Outputs

On the *Digital Inputs and Outputs* page, you can set up the external input and output devices that are connected to the camera. This option does not appear for cameras that do not support digital inputs and outputs.

1. Click the **Events** tab, and then click the **DIO** button.
2. To configure a digital input:
   a. Enter a name for the digital input in the **Name** field.
   b. Select the appropriate state from the **Circuit State** drop-down menu. The options are:
      - **Normally Open**
      - **Normally Closed**
   c. Click **Apply** to save the settings.
      After the digital input is connected to the camera, you will see the connection status in the **Circuit Current State** field. The status is typically *Open* or *Closed*.
3. To configure a digital output:
   a. Enter a name for *Digital Output 1* or *Digital Output 2* (if present) in the Name field.
   b. Select the appropriate state from the *Circuit State* drop-down menu.
   c. If appropriate, click to select the checkbox for *IRCF to Out* to allow the camera's IR Cut Filter to control the external output.
      This feature is typically used when the camera is connected to an external IR illuminator. After it is enabled, the IR illuminator is turned on when the camera's IR Cut Filter is in monochrome mode.
   d. If you did not select *IRCF to Out*, in the *Duration* field, enter how long the digital output is active when triggered. You can enter any number between 100 and 86,400,000 milliseconds.
   e. Click **Trigger** to manually trigger the digital output from the web interface.
   f. Click **Apply** to save the settings.

Configuring Elevate

Use the *Elevate* tab to connect a camera to Elevate and view *Image Health* settings.

Note: To connect a camera to Elevate, you must have an Elevate account. To create an account, visit elevate.pelco.com/register.

Connecting a Camera to Elevate

On the *Camera Connection* page, users can connect an Elevate-enabled camera to Elevate.

To connect a camera to Elevate, users must create a unique site token in their Pelco Elevate account. To login to Pelco Elevate, visit elevate.pelco.com/login. For instructions on creating a token, see the Pelco *Elevate User Guide*.

1. Click the **Elevate** tab, and then click the **Go to setup page** button.
2. If you are prompted to connect via HTTPS, click **Confirm**.

   Note: Connecting via HTTPS is required to connect to Elevate.

3. In the **Token:** field, paste the token from your Pelco Elevate account.
4. Click **Connect**.

Important: You must set the camera time to successfully connect the camera to Pelco Elevate. The camera time can be set up manually on the *System* tab, under *General Settings*, or be set to automatically sync with the NTP server. Syncing with the NTP server is the preferred method. To auto-synchronize the camera's date and time with an NTP server, you must configure the NTP server on the *Network and Security* tab, *Network* page. See the section titled *Configuring the Network Settings*.

Viewing Image Health

On the *Image Health* page, users can view the reference image for day time and night time.

The system uses these reference images to perform Image Health Checks twice a day, based on the timezone selected in the user's Pelco Elevate account. Ensure that the reference image for day time and night time have the ideal view. If the images shown in the *Reference Image* area are not a good representation of the camera's typical view, users can refresh images.

To view Image Health:

1. Click the **Elevate** tab, and then click the **Image Health** button.
2. View the reference image for day time and night time in the *Reference Image* area.

To refresh a Reference Image:

1. Click the **Refresh image** button found under the image.
2. A pop-up window will appear showing a preview of the updated reference image.
3. If you are satisfied with the preview, click **Update**.

Pelco Fisheye® Cameras Operations Manual

Manufacturer: Videotec s.r.l.
Address: Via Friuli, 6-I-36015 Schio (VI) - Italy
(+39) 0445 697411 Tel

Pelco, Inc.
625 W. Alluvial Ave., Fresno, California 93711 United States
(800) 289-9100 Tel
(800) 289-9150 Fax
+1 (559) 292-1981 International Tel
+1 (559) 348-1120 International Fax
www.pelco.com

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

© Copyright 2023, Pelco, Inc. All rights reserved.