



Standard Fixed Cameras

Operations Manual

Document number: C6774M

Publication date: 2025-01-10

Standard Fixed Cameras Operations Manual

© 2025, Pelco Corporation. All rights reserved. MOTOROLA, MOTO, MOTOROLA SOLUTIONS, and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners. Unless stated explicitly and in writing, no license is granted with respect to any copyright, industrial design, trademark, patent or other intellectual property rights of Pelco Corporation or its licensors.

This document has been compiled and published using product descriptions and specifications available at the time of publication. The contents of this document and the specifications of the products discussed herein are subject to change without notice. Pelco Corporation reserves the right to make any such changes without notice. Neither Pelco Corporation nor any of its affiliated companies: (1) guarantees the completeness or accuracy of the information contained in this document; or (2) is responsible for your use of, or reliance on, the information. Pelco Corporation shall not be responsible for any losses or damages (including consequential damages) caused by reliance on the information presented herein.

Pelco Corporation
pelco.com

PDF-STANDARD-OPS
Revision: 1 - EN
2025-01-10



MOTOROLA SOLUTIONS

Contents

Standard Fixed Cameras Operations Manual	1
Camera Web Interface System Requirements	1
Accessing the Camera Web Interface	2
Access the Camera Web Interface from the Camera Configuration Tool (CCT)	2
Creating the Initial User and Logging In	3
Logging In	3
Log Out	3
Live View	4
Configure Basic Settings	4
Using the Camera Focus Controls	4
Save a Still Image	4
System Settings	6
Configure General Settings	6
Manage Camera Firmware	7
Configure Storage Management	7
Enable Onboard Storage	8
Enable SD Card Encryption	9
Download Recorded Video from the Web Interface	9
Download Recorded Video from the SD Card	9
Delete Recorded Video	10
Activate Licenses	10
Automatic Activation	10
Manual Activation	11
Extended Settings	11
Access System Diagnostics using the Device Log	11
Network and Security Settings	13
Configure Network Settings	13
Enable SRTP Streaming	15
Requirements	15
Configure Security Settings	15
Manage Users	16
Add a New User	16
Modify User Settings	16
Remove a User	17
Keep Usernames and Passwords After Firmware Revert	17

Configure 802.1x Port-Based Authentication	18
Configure the 802.1X Port Security	18
Switch 802.1X Authentication Profiles	18
Remove an 802.1X Authentication Profile	18
Return to the Network Page	18
Enable SNMP	19
Activate DSCP	19
Configure the IP Filter	21
Manage Certificates	22
Downloading Certificates	22
Removing Certificates	22
Downloading Certificate Signing Requests	22
Uploading Certificates	23
Uploading CA Certificates	23
Creating Certificates	23
Imaging Settings	25
Configure Image and Display Settings	25
Adjust White Balance Settings	29
Use Window Blanking	31
Setting a Window Blank	31
Deleting a Window Blank	31
Dynamic Privacy Masks	31
Create Dynamic Privacy Masks	32
A/V Streams	34
Compression and Image Rate Settings	34
Enable and Configure Smart Compression	35
View the RTSP Stream Using URI	36
Access the Last Still Image Frame Using URI	36
Configure Multicast Streaming	36
Save or Restore Video Configurations Settings	37
Configure Streaming Settings	37
Configure Audio Setting	37
Configure Smart Compression Advanced Settings	38
Events	39
Enable and Configure Motion Detection	39
Enable and Configure Tamper Detection	40
Analytics Configuration	40

Standard Fixed Cameras Operations Manual

Change the Analytics Scene Mode	40
Create a Motion Event	41
Enable and Configure Self Learning Analytics	42
Suspend Self Learning	42
Reset Self Learning	43
Enable and Configure Audio Analytics	43
Configure Digital Inputs and Outputs	44
Camera Automation	45
Create and Manage Camera Rules	45
Manage Sequences and Email Actions	46
Create and Manage Sequences	47
Create and Manage Email Actions	47
Configure SMTP Server Information	47
Edit SMTP Server Information	47
Add Email	48
Create and Manage FTP Actions	48
Configure FTP Server	48
Add FTP Action	48
Pelco Elevate	50
Connect a Camera to Pelco Elevate	50
View Image Health	50
Camera Information	52
More Information & Support	53

Standard Fixed Cameras Operations Manual

You can use the camera's web interface to check the camera's online status and image quality, configure network settings, manage features and upgrade firmware. Make sure you have completed the installation procedure and added the camera to the network before you try to access the web interface.

The settings and features available in the web interface depend on the specific camera model. The information in this Operations Manual is relevant to Standard Fixed Cameras using the latest firmware. You can download the latest camera firmware at pelco.com/updates.

Camera Models:

- Sarix Enhanced 4 Bullet & Dome
- Sarix Enhanced 4P Bullet, Dome & Box
- Sarix Pro 4 Bullet & Dome
- Sarix Enhanced 3 Bullet & Dome
- Sarix Pro 3 Bullet & Dome
- Sarix Corner

Camera Web Interface 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 other browsers but this has not been verified.

Accessing the Camera Web Interface

You can access the camera web interface to configure camera settings after the camera is installed. You need to use a computer on the same network as your camera to access the camera web interface.



NOTE

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

1. 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 [Add a New User on page 16](#).

Access the Camera Web Interface from the Camera Configuration Tool (CCT)

You can also access the camera web interface from the Motorola Camera Configuration Tool (CCT)
<https://www.pelco.com/camera-configuration-tool/>

Creating the Initial User and Logging In

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



NOTE

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**. You will be prompted to log in.

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 log in. For more information, see [Modify User Settings on page 16](#).

Log 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.

Live View

On the *Live View* page, you can preview the live video stream and configure basic settings.

Configure Basic Settings

1. To manually zoom the camera, use the **Zoom** slider.
 - a. To zoom out, move the slider towards the left.
 - b. To zoom in, move the slider towards the right.
2. Click **Auto Focus** to let the camera focus itself.
3. To manually focus the camera, use the **Focus** slider.
 - a. To focus towards zero, move the slider towards the left.
 - b. To focus towards infinity, move the slider towards the right.
4. Select a Codec option from the drop-down list.
5. Use the **Analytics** options to turn on or off analytics.
6. Select the **Draw Object Bounding** if you want to enable bounding boxes around objects.
7. Click **Relearn background** to clear learning data and initiate relearning.

Using the Camera Focus Controls

Camera Focus controls are at the lower left of the application.

- To focus towards zero:
 - Click << to take a large step.
 - Click < to take a small step.
 - Click **0** to focus at zero.
- To focus towards infinity:
 - Click >> to take a large step.
 - Click > to take a small step.
 - Click **Inf** to focus at infinity.
- If the camera supports auto focusing, click **Auto Focus**.

Save a Still Image

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

Standard Fixed Cameras Operations Manual

- 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 [Configure Storage Management on page 7](#).
- The camera's video format must be set to MJPEG in the Video Configurations page. For more information, see [Compression and Image Rate Settings on page 34](#).

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.

See [Compression and Image Rate Settings on page 34](#) for instructions on how to download the snapshot.

System Settings

Use the System tab to configure General Settings, Firmware, Storage Management, Extended Settings and Diagnostics.

Configure General Settings

On the *General Settings* page you can update camera details, overlay settings and time settings.

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 the mode in which the camera will operate. This option is only applicable for select cameras.
 - Full Feature – This is the standard operating mode that offers the full functionality of the camera.
 - High Framerate – This mode will use the maximum image rate possible but will disable Analytics in order to achieve the maximum frame rate. WDR can be enabled up to 30 fps and should be disabled for frame rates higher than 30 fps.
 - Dynamic Privacy Masks – This mode will enable 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.
Only available on Sarix Enhanced 4 and 4P cameras at this time.



NOTE

When this mode is selected, the maximum frame rate will be limited to 15 fps.

- No Video Analytics – This mode will disable Video Analytics. This option is for deployments where camera based video analytics would interfere with other analytics integrations.
5. Select the Disable device status LEDs checkbox to disable the camera LED indicators.
 6. 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
 7. Use the **Font Size** field to make the font larger or smaller. The default font size is 24. You can make the font as small as 12 or as large as 120.
 8. 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 [Configure Network Settings on page 13](#).



IMPORTANT

The time setting must always be current. To ensure that the time is always current you can set up NTP on the DHCP server, if your VMS supports this feature. Otherwise, you can use a valid public NTP server. If required, you can manually set the correct time in the Time Settings fields.

9. To configure GPS Settings, enter the geolocation information as decimal values:
 - a. Latitude
 - b. Longitude
 - c. Elevation (meters above sea level)
10. Click **Apply** to save the settings.

Manage Camera Firmware

On the *Firmware* page, you can check the current firmware version, manually upgrade the firmware, reboot the device and restore the camera to the factory defaults.

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

Configure Storage Management

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

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 Profile G** to enable video 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.

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.

Enable 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 and Actions 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. Select the **Enable Recordings Retention** checkbox to enable the camera to store recordings for a set amount of time. You can assign the number of days, hours and minutes that the recordings will be stored.
6. 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 Settings on page 34](#).

Enable SD Card Encryption

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.

1. Select the **Card Encryption** checkbox in the *Onboard Storage* area to enable card encryption.
2. Click the **Apply** button.

Download 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 [Download Recorded Video from the SD Card below](#).

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.

Download 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.

Delete 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.

Delete video by one of the following methods:

1. 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.
2. To delete all of the recorded video files, in the Onboard Storage section, at the right of the information, click **Format Card** to format the SD card, and then click OK in the confirmation dialog box.

Activate Licenses

On the Licensing page you can use a license activation key to enable certain features.



NOTE

For licensing support, visit pelco.com/support.

1. Click the **Add License** button.
2. Enter a license activation key into the field.
3. Choose an activation method:
 - Automatic: use this option if the camera has Internet access.
 - Manual: use this option if the camera does not have Internet access.

Automatic Activation

Click Activate Now to activate your license.

Manual Activation

1. Click the **Save File** button to generate an activation request file.
2. Upload the activation request file to our licensing website:
flexnetoperations.com/flexnet/operationsportal/
Your license file will be available for download.
3. Save the license file.
4. Click the **Choose File** button and select the license file you saved in Step 3.

Extended Settings

You can configure ONVIF Settings on the *Extended Settings* page.

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.

Access System Diagnostics using the Device Log

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.

Standard Fixed Cameras Operations Manual

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.

Network and Security Settings

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

Configure 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. 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.
4. Uncheck the **Enable WS Discovery Protocol** checkbox to turn off the WS Discovery protocol. This option is enabled by default.
WS Discovery is used to scan and find cameras on the same network. This is required when using the Camera Configuration Tool and certain Video Management Systems. You can turn off WS Discovery after installation as a security precaution.
 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: 555To 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 LinkEthernet 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 options, which can be selected if it is required for backwards compatibility.

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

Enable SRTP Streaming

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



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 [Configure Network Settings on page 13](#).
- 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 [Configure Security Settings below](#).
- SRTP streaming requires a Unicast and Multicast over UDP connection.

Configure 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.



IMPORTANT

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 non-critical operating times.

Manage Users

You can add, modify, and remove users on the *Users* page.

Add a New 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.

Modify User Settings

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.

Remove 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**.



IMPORTANT

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

Keep 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.



IMPORTANT

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.



IMPORTANT

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.

Configure 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.

Configure 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.
 - Uploaded 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.

Switch 802.1X Authentication Profiles

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

Remove an 802.1X Authentication Profile

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

Return 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.

Enable 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.

Activate DSCP

Differentiated services or DiffServ is a computer networking architecture that specifies a simple and scalable mechanism for classifying and managing network traffic and providing quality of service (QoS) on

modern IP networks. DiffServ can, for example, be used to provide low-latency to critical network traffic, such as voice or streaming media, while providing simple best-effort service to non-critical services, such as web traffic or file transfers.

DiffServ uses a 6-bit differentiated services code point (DSCP) in the 8-bit differentiated services field (DS field) in the IP header for packet classification purposes. The DS field replaces the outdated IPv4 TOS field. Each DSCP value represents a QoS class, also known as a behavior aggregate. DiffServ is a coarse-grained, class-based mechanism for traffic management.

On the DSCP page you can activate the DSCP feature, choose values for the traffic types listed below, and restore values to default.

1. Click the Network and Security tab, and then click the DSCP button.
2. In the DSCP area, the **Activate feature** checkbox is selected by default. Clear the **Activate feature** checkbox to disable DSCP and reset all of the values on this page to DF(0).
3. In the **ONVIF protocol** drop-down menu, click to select one of the options:
 - DF(0)
 - CS2(16) (This is the default option.)
4. In the **Web interface** drop-down menu, click to select one of the options:
 - DF(0)
 - AF21 (18) (This is the default option.)
5. In the **SNMP** drop-down menu, click to select one of the options:
 - DF(0)
 - CS2 (16) (This is the default option.)
6. In the **Primary Stream** drop-down menu, click to select one of the options:
 - AF31(26)
 - CS4(32)
 - AF41(34) (This is the default option.)
7. In the **Secondary Stream** drop-down menu, click to select one of the options:
 - CS3(24),
 - AF31(26),
 - CS4(32),
 - AF41(34) (This is the default option.)
8. In the **Tertiary Stream** drop-down menu, click to select one of the options:
 - CS3(24) (This is the default option.)
 - AF33(30)
9. In the **Replay Stream** drop-down menu, click to select one of the options:
 - CS3(24) (This is the default option.)
 - AF33(30)
 - CS4(32)
 - AF43(38)
10. Click Restore Defaults and then click Apply to restore the DSCP values to their default settings.



NOTE

In case of Primary, Secondary, Tertiary and Replay Stream, it is very important to prepare and setup 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.

Configure 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.



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 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 will 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.

Manage 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. 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.
2. Click the **Download** button to download the CSR file.

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.

Creating Certificates

1. In the *Valid Not Before* field, enter the date that the certificate becomes valid in the format: mm/dd/yyyy. This field is required.



NOTE

You can also click the calendar icon to select a date using the calendar view.

2. In the *Valid Not After* field, enter the date that the certificate is no longer valid in the format: mm/dd/yyyy. This field is required.
3. 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.
4. Click the **Create** button.
5. Click the **Make Active** button.
6. Click the **OK** button in the pop-up message.



NOTE

If you activate the new certificate other certificates will be deactivated, and the page will be reloaded.

Imaging Settings

You can configure the image and display settings and privacy zones on the *Imaging* tab.



NOTE

You may need to reset the learning progress after modifying zoom or focus on cameras with video analytics. The learning progress might reset automatically if the camera's image rate, compression or display settings are updated.

Configure Image and Display 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. Use the **Zoom** slider to adjust the camera's zoom position.
 - To zoom out, move the slider towards the left.
 - To zoom in, move the slider towards the right.
3. To manually focus the camera, use the **Focus** buttons.
 - To focus towards zero:
 - Click << to take a large step.
 - Click < to take a small step.
 - Click 0 to focus at zero.
 - To focus towards infinity:
 - Click >> to take a large step.
 - Click > to take a small step.
 - Click Inf to focus at infinity.
 - Click **Auto Focus** to let the camera focus itself.



NOTE

After the focus is manually set, it will not change.

4. For Sarix Enhanced 4 and Sarix Pro 4 cameras, you can change the size and location of the **Auto Focus Zone** by clicking and dragging the orange **Auto Focus Zone** box on the camera's field of view.



NOTE

Auto Focus zones are visible by default. If the Auto Focus Zone is not visible on the camera's field of view, make sure the **Show Auto Focus Zones** checkbox is selected.

5. View the following information below the Focus buttons:
 - Current Exposure
 - Current Gain
 - Current Iris
 - Last Known Light Level
6. Use the Image Rotation drop-down menu to rotate the camera image as desired. The default option is None. The image can be rotated by 90 degrees, 180 degrees or 270 degrees. The camera will reboot when applying this setting and some encoding settings will revert to their default settings.
 - *None*
 - *90 degrees*
 - *180 degrees*
 - *270 degree*

Image rotation should not be combined between the camera and VMS image rotation settings. Perform the image rotation either in the camera or in the VMS, but not both.
7. If available, select the check box to enable **Temperature Refocus**. When enabled, the camera will automatically refocus as temperature fluctuates.



NOTE

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

8. 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.
 - **External:** The camera will open the IR cut filter and switch to monochrome mode based on the digital input circuit state.



NOTE

The default digital input circuit state is configured on the Digital Inputs and Outputs page. For more information, see [Configure Digital Inputs and Outputs on page 44](#).

- b. If you selected the Automatic Day/Night Mode:
 - i. 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.

9. To adjust the exposure of the image, adjust the Exposure Settings:
 - a. **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.

- b. **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.

- c. **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.
 - d. **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.
 - e. **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 \(WDR\)](#).
 - f. **Disable WDR in Low Light:** You can disable Wide Dynamic Range (WDR) in low-light environments for improved camera performance.
 - g. **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 \(WDR\)](#).
 - h. **Maximum Gain:** To limit the automatic gain setting, click to select 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.
 - i. **Iris:** You can allow the camera to control the iris by selecting **Automatic**, or you can manually set it to **Open** or **Closed**.
10. If you are configuring a Sarix Enhanced 4, 4P or Sarix Enhanced 4 Thermal camera, you can select the **Enable Digital Defog** checkbox to use digital defog. The camera will reduce fogginess in the camera view to improve image quality.
If you want to turn off Digital Defog without disabling the feature, you can select the **Off** button from the drop-down menu.
 11. If you are configuring a Sarix Enhanced 4 or 4P camera, you can select the **Enable Image Stabilization** checkbox in the Advanced Filters area to enable Electronic Image Stabilization (EIS). EIS automatically stabilizes the image whenever the camera shakes. This feature improves the image quality by compensating for camera movement.



NOTE

Image stabilization can not be enabled at the same time as: Wide Dynamic Range (WDR), Dynamic Privacy Masks or Privacy Zones on this camera.

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

Adjust White Balance Settings

1. Click the Imaging tab, and then click the **White Balance** button.
2. Use the **Zoom** slider to adjust the camera's zoom position.
 - To zoom out, move the slider towards the left.
 - To zoom in, move the slider towards the right.
3. To manually focus the camera, use the **Focus** buttons.
 - To focus towards zero:
 - Click **<<** to take a large step.
 - Click **<** to take a small step.
 - Click **0** to focus at zero.
 - To focus towards infinity:
 - Click **>>** to take a large step.
 - Click **>** to take a small step.
 - Click **Inf** to focus at infinity.
 - Click **Auto Focus** to let the camera focus itself.



NOTE

After the focus is manually set, it will not change.

4. View the following information below the Focus buttons:
 - Current Exposure
 - Current Gain
 - Current Iris
 - Last Known Light Level
5. 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 [Configure Image and Display Settings on page 25](#)

- **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.

6. 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.
7. 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.
8. Click **Apply** to save the settings.

Use 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.



NOTE

For Pelco PTZ cameras, the window blank might shift slightly when the camera performs an e-flip. If this is a concern, we recommend drawing a slightly larger box or disabling e-flip for that camera. For more information on disabling e-flip, see [Defining PTZ Limit Stops](#).

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.

Dynamic Privacy Masks



NOTE

The removable Dynamic Privacy Masks are only available on Sarix Enhanced 4 and 4P cameras at this time.

You can create and configure dynamic privacy masks on the *Dynamic Privacy Masks* page. Dynamic Privacy Masks blur certain objects from view in the live camera footage, recorded video and still images. The feature restricts access to sensitive information in the image.



NOTE

You must change the Camera Mode to Dynamic Privacy Masks before you can use dynamic privacy masks. You can change the camera mode on the General Settings page. You will not be able to use EIS when the camera mode is set to Dynamic Privacy Masks.

Create Dynamic Privacy Masks

You can define both blur zones and unblur zones when you create a Dynamic Privacy Mask. You must create at least one blur zone per mask. You have the option to create unblur zones to layer on top of the blur zones. Unblur zones cancel the blurring effect when layered on top of a blur zone. Adjust the unblur zones to cover smaller sections of the blur zones to use them effectively. You must also choose which objects get blurred by selecting one or more Class Filters. The Class Filters define the types of objects that will be blurred, e.g., Human or Vehicles.



IMPORTANT

Changing to Dynamic Privacy Mode on Pelco cameras will create a second camera head in the web interface: Head1 shows the unblurred stream and Head2 shows the blurred stream. You can only create masks on Head2.

1. Click **Create Mask** in the Mask Options area.
2. Click and drag the slider to increase the Blur Radius. This enhances the blurring effect.
3. Select one or more of the checkboxes to define which Class Filters to mask. The following class filters are currently available:
 - Human
 - Vehicle



NOTE

At least one class filter must be selected to create a mask. The Human class filter is selected by default.

4. Click **Add** in the Blur Zones column to add a new Blur Zone.



TIP

You can click the **Apply** button without creating any blur zones to quickly mask the entire area. Make sure to click **OK** to confirm.

Standard Fixed Cameras Operations Manual

5. Click **Add** in the Unblur Zones column to add a new Unblur Zone.
6. Click the zone to select it. The blue zone is the one you have currently selected.
7. Click and drag the middle of the zone to move it to a new location.
8. Click and drag the blue points to modify the size or shape of the zone.



NOTE

The zone must resemble a single valid polygon to apply effectively. Make sure the shape of the zone does not appear twisted.

9. Click on the edge of the zone to create a new point.
10. Select a zone from either column and use the **Remove** buttons if you want to delete it.



NOTE

Make sure you know which zone you have selected before you click Remove.

11. Click **Apply** to save the mask.
12. Click **Remove Mask** and then click **Apply** if you want to delete the mask.

A/V Streams

Use the *A/V Streams* tab to configure Video Configurations, Audio Configurations, Streaming Settings and Smart Compression.

Compression and Image Rate Settings

On the *Compression and Image Rate*, 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, tertiary and quaternary streams.



NOTE

Quaternary streams are only available on Sarix Pro 4 5MP camera models at this time.



NOTE

You may need to reset the learning progress after modifying zoom or focus on cameras with video analytics. The learning progress might reset automatically if the camera's image rate, compression or display settings are updated.

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 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 [Enable Onboard Storage on page 8](#).
 - 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 [Configure General Settings on page 6](#).

- 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.

Enable and Configure Smart Compression

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

Smart Compression is enabled by default.

1. Select the **Enable Idle Scene Mode** checkbox to enable Idle Scene Mode. Idle scene mode records video at a different frame rate and quality if there are no motion events detected in the scene. This lowers the bandwidth and storage used when the scene is idle. When motion events are detected, the camera automatically switches back to standard streaming mode.
2. 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.
3. 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.
4. In the Bandwidth Reduction drop-down menu, select one of the following options:
 - **Low**
 - **Medium** (recommended)
 - **High**
 - **Custom**
5. Click **Apply** to save the settings.
6. If you chose Custom for the Bandwidth Reduction, see the section titled [Configure Smart Compression Advanced Settings on page 38](#).

View the RTSP Stream Using 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.



NOTE

You can only generate the RTSP stream address in the camera web interface.

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.

Access the Last Still Image Frame Using 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.

Configure Multicast Streaming

Multicast streaming delivers a continuous stream of footage to multiple endpoints simultaneously. Cameras with multiple streams can stream to the multiple endpoints using different IP addresses and port numbers.

You can configure the primary, secondary and tertiary streams separately in the *Multicast* area on the *Video Configuration* page of the camera web interface. You can also adjust settings for a quaternary stream for the Sarix Pro 4 5MP camera models.

Follow these steps to configure multicast streaming settings for the camera streams as required:

1. Enter the IP address in the **Address** field.
2. Enter the port number in the **Port** field.
3. Enter a value between 1 and 255 seconds in the **Time To Live** field.

Save or Restore Video Configurations Settings

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.

Configure 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 **Video Encoder** drop-down menu.
4. Select a profile from the **Audio Source** drop-down menu.
5. To enable **Metadata**, select metadata0 from the drop-down menu.
6. To disable **Metadata**, select None.
7. Click the **Apply** button to apply your changes.

Configure Audio Setting

On the Audio Configurations page, you can adjust the audio settings for the device speaker and microphone.

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. 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.
2. In the **Device Speaker** section, use the **Volume** slider to adjust the volume on the speaker (from 0 to 100).
3. 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.

4. In the Device Microphone section, use the Line In 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.
5. Click **Apply** to save the settings.

Configure Smart Compression Advanced Settings

If you enabled Smart Compression on the Video Configuration page (see the section titled [Enable and Configure Smart Compression on page 35](#)), 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.

Events

Use the Events tab to configure Motion, Sabotage, Analytics , DIO settings and configure Camera Automation.



NOTE

Other analytics events, that are not available in the Camera's web interface, can be configured using the Camera Configuration Tool (CCT).

Enable and Configure 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.

Enable and Configure Tamper Detection

On the Sabotage page, you can enable and configure Tamper Detection. This enables the camera to send events when tampering is detected.

1. Make sure that the Enable Tamper Detection the checkbox is selected to enable Tamper Detection. Tamper Detection is enabled by default.
2. In the **Sensitivity** field, enter a number between 1 and 10 to determine the sensitivity level. The higher the setting, the more sensitive the camera is to a sudden change in the scene.



NOTE

A sudden change in the scene is usually caused by someone unexpectedly moving the camera. Lower the setting if small changes in the scene, like moving shadows, trigger too many tampering events. If the camera is installed indoors and the scene is unlikely to change, you can increase this setting to capture more unusual events.

3. In the **Trigger Delay (seconds)** field, enter the number of seconds between 2 and 30 that the tampering condition must occur in the scene before the Tamper Detection event is sent.

Analytics Configuration

You can use the *Analytics Configuration* page on the *Events* tab to create analytic events.

Change the Analytics Scene Mode

Set the camera to use the Analytics Scene Mode that best describes the scene. Some scene modes are not available on all camera models:

- **Outdoor** – suitable for most outdoor environments. This setting optimizes the camera to identify vehicles and people.
- **Large Indoor Area** – only detects people and is optimized to detect people around obstructions, like chairs and desks, if the head and torso are visible.

Create a Motion Event

You can create Motion Events on the *Analytics Configuration* page. Motion Events trigger alarms when a certain activity occurs in the inclusion area. You can add and arrange inclusion areas to make sure that the site is fully monitored.

1. Click **Add Event** in the Events area.
2. Enter a name for the Event in the Name field.
3. You can uncheck the **Enabled** checkbox if you want to enable it at a later time. The Enabled checkbox should remain checked if you want the event to be enabled immediately.
4. Select an activity type from the list:
 - Objects in area
 - Object loitering
 - Objects crossing beam
 - Object appears or enters area
 - Object not present in area
 - Objects enter area
 - Objects leave area
 - Object stops in area
 - Object removed from zone (Sarix Enhanced 4 and Sarix Pro 4 only)
 - Object abandoned in zone (Sarix Enhanced 4 and Sarix Pro 4 only)
 - Direction violated
5. Select one or more object types from the list of options. At least one object type is required.
 - Person
 - Vehicle
 - Car
 - Bus
 - Bicycle
 - Motorcycle
 - Pickup
 - Truck
 - Large
 - Truck
 - Van
6. Click and drag the slider to adjust the **Sensitivity** level. Lowering the sensitivity increases the chances of false negatives.
7. Use the up and down arrows to set the **No. of Objects** required to trigger an alarm.
8. Use the up and down arrows to set the **Threshold Time** required to trigger an alarm.
9. Objects within the Inclusion area for longer than the threshold time will trigger an alarm.
10. Use the up and down arrows to set the **Timeout** before another alarm is triggered.

11. Click and drag the middle of the green square on the screen to move the inclusion area.
12. Click and drag the points to reshape the inclusion area.
13. Click **Add Exclusion Area** to add a new exclusion area.
14. Click **Reset Inclusion Area** to reset the size and shape of the inclusion area.
15. Select an Inclusion Area and click **Delete Exclusion Area** if you want to delete it.



NOTE

At least one Inclusion area is required.

16. Click **Save**.
17. Click **Test** to trigger a mock event based on the saved settings. This event should appear in your VMS.

Enable and Configure Self Learning Analytics

On the Analytics Configuration page, you can configure Self Learning Analytics. The camera will perform self adjustments based on the activity in the field of view. This can significantly improve the accuracy of classified object detection.

Self-learning will progress based on activity detected in the field of view. Scenes with less activity will require staging during the learning phase. One example of staging would involve having a person walk through the field of view during learning.

Follow these steps to configure Self Learning in the camera's web interface:

1. Select the **Enable Self Learning** checkbox to enable self learning analytics.
2. Select the **Suspend Self Learning** checkbox to temporarily disable self learning analytics.
3. Click the **Reset Self Learning** button to reset self learning.



NOTE

This action can not be undone.

4. Click **Apply** to save your changes.

Suspend Self Learning

You can now stop 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.
- The device is in Indoor Overhead mode. Self-learning is not used, even if enabled. All detected objects are classified as people.

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.

Enable and Configure Audio Analytics

The Audio Analytics feature is only available on Sarix Enhanced 4 cameras at this time.



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 Audio Analytics page, you can enable and configure Audio Detection for different Audio Detection Events. This option is disabled by default.



NOTE

The camera's microphone is disabled by default and must be physically switched on for Audio Detection to work.

1. Select the **Enable Audio Detection** checkbox to enable the camera to detect Audio Detection Events.
2. Select a sound from the list:



NOTE

The sounds listed under **Basic Sounds** are available without a premium license. The sounds listed under **Premium Sounds** are only available with a premium license. For more information, see [Activate Licenses on page 10](#).

- Scream
 - Glass Break
 - Car Alarm
 - Fire Alarm
 - Dog Bark
 - Loud Noise
 - Ultrasound
 - Gunshot
3. Under Event Details, select the **Enabled** checkbox to enable Audio Detection Events.
 4. Select a Sensitivity level from the drop-down list:
 - 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.
 5. Adjust Timeout by entering a value between 1 and 300 seconds. Timeout refers to the minimum interval of time after an audio event is detected before the system triggers an additional alarm.



NOTE

During the Timeout interval, subsequent audio events, e.g., gunshots, will not trigger separate alarms.

6. Click the **Apply** button to save your changes.

Configure 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. Click **Trigger** to manually trigger the digital output from the web interface.
 - e. Click **Apply** to save the settings.

Camera Automation

You can create rules and assign actions to automate camera functions and responses on the *Automation* page, found on the *Events* tab.

Create and Manage Camera Rules

On the *Rules* tab, you can review the list of defined rules or create a new rule.

Follow these steps to create a new rule:



1. Click the **Add Rule** button.
2. Under *When the following trigger happens*, select the **Analytics** option if you want to create an Analytics rule and then select one of the following Analytics types:
 - 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. See [Create a Motion Event on page 41](#) for instructions.
 - Camera Tampering Rule – when the camera detects a person tampering with the camera itself.
 - Motion Detector – when the camera detects motion in the scene.
3. Alternatively, select the **SystemStatus** option if you want to create a system status rule and select one of the following options:
 - a. SystemBooted – triggers an action when the camera reboots.

4. You can click the **Simulate Trigger** button 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.

5. Under *And the following condition is true*, select an option:
 - Always – the rule will perform the action every time the selected trigger occurs.
 - Never – the rule will never perform the action, even if the selected trigger occurs. This can be used to temporarily disable a rule.
6. Under *Then perform this action*, select one of the following action types:
 - Console Output – displays a message.
 - Email – sends an email when the selected trigger occurs and the condition is true.
 - FTP – triggers an FTP action sent to a subdirectory.
 - Sequence – initiates a sequence of actions when the selected trigger occurs and the condition is true.
7. Click the **Test Action** button to test the action.
8. If you chose Email, select from the list of available email actions. If the email action you want isn't listed, you can create a new one by selecting Add New and filling out the form as described in the section titled Create and Manage Sequences under [Manage Sequences and Email Actions below](#).
9. If you chose Sequence, select from the list of available sequence actions. If the sequence you want isn't listed, you can create a new one by selecting Add New and filling out the form as described in the section titled Create and Manage Sequences under [Manage Sequences and Email Actions below](#).
10. You can click the **Test Action** button to test the action.
11. Enter a Rule Name.
12. Click the **Save** button. The rule will be added to the *Defined Rules* list.
13. Click the  icon to edit a rule.
14. Click the  icon to delete a rule.

Manage Sequences and Email Actions

On the *Actions* tab, you can create and configure the sequences or email actions that are used for the camera rules. This is helpful if you want to create reusable action types or edit the actions in one place.



IMPORTANT

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

Create and Manage Sequences

You can click the **Sequence** button to review, edit, delete or add new sequences. The new sequence will appear on the *Sequence* list. You can use these sequences when creating rules.

Follow these steps to create a new sequence:

1. Click the **Add Sequence** button.
2. On the *Add Sequence* page, enter the following information:
 - Sequence Name – enter a descriptive name for the sequence action. This name is shown on the Add Rule page.
 - Wait before – enter the number of minutes you want the sequence to wait before performing the action.
 - Then perform this action – select an action type and choose the action rule. If you select Email as the action type, see Step 5 for instructions on how to add a new email action.
3. Click the **Test** button to test the sequence.
4. Click the **Save** button to save it.

Create and Manage Email Actions

You can click the **Email** button to review, edit, delete or test email actions. You can also configure SMTP server information for the email actions.



IMPORTANT

Any changes you make to the SMTP server information will affect any rules that are already using that email.

Configure SMTP Server Information

If you are adding the SMTP server for the first time, the button is labeled **Configure SMTP** and the **Add Email** button is disabled and greyed out. See [Edit SMTP Server Information below](#) for instructions on how to edit SMTP server information for existing SMTP configurations.

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

1. Click the **Configure SMTP** button.
2. 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.
3. Click **Save**.

Edit SMTP Server Information

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

Standard Fixed Cameras Operations Manual

Follow these steps to edit the SMTP Server information:

1. Click the **Edit SMTP** button.
2. 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.
3. Click **Save**.

Add Email

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**.

Create and Manage FTP Actions

You can click the **FTP** button to configure an FTP server and create FTP actions.

Configure FTP Server

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

1. Click the **Configure FTP Server** button.
2. Enter the following information:
 - a. Enter the FTP Server URL.
 - b. Enter the Username on the server url you provided.
 - c. Enter the FTP user password or app password for the username.
3. Click **Save**.

Add FTP Action

Follow these steps to create a new FTP action:

1. Click the **Add FTP Action** button.
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:

Standard Fixed Cameras Operations Manual

- a. Snapshot – sends a saved image from the camera to the FTP server.
 - b. Syslogd – sends a system log to the FTP server.
 - c. ConsoleLog – sends a console log to the FTP server.
6. Click **Save**.

Pelco Elevate

You can use the *Elevate* tab to connect a Pelco Camera to Elevate. Check the [Elevate Supported Cameras List](#) to see the minimum firmware version required to connect a camera to Elevate.



NOTE

You must have an Elevate account to connect a camera to Elevate. Visit elevate.pelco.com/register to create an account.

Connect a Camera to Pelco Elevate

You can connect an Elevate-enabled camera to Elevate on the *Camera Connection* page located on the *Elevate* tab of the camera's web interface.

You must create a unique site token in your Pelco Elevate account before you can connect the camera through the web interface. To log in to Pelco Elevate, visit elevate.pelco.com/login. For instructions on creating a token, see the Pelco [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 Pelco Elevate.

3. In the **Token:** field, paste the token from your 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 [Configure Network Settings on page 13](#).

View Image Health

You can view the reference image for day time and night time on the *Image Health* page.



NOTE

Image Health is only available on fixed camera models at this time. PTZ models do not support Image Health.

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**.

Camera Information

You can access camera information by clicking the **About** button at the upper-right corner of the window. You will need this information when contacting product support.

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.

