ExSite® ExSite Pro PTZ
Operations Manual

Document number: C6758M

Publication date: 03/24

Table of Contents

Introduction

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

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

System Requirements

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

- Mozilla Firefox
- Google Chrome™

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

Accessing Camera Settings

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

Note: Smart Analytics configuration requires the CCT.

Accessing the Camera Web Interface

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

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

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

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

   For example: http://192.168.1.40/

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

Creating the Initial User

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

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

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

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

Logging In

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

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

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

Logging Out

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

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

Using the Live View

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

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

Saving a Still Image

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

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

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

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

Configuring the System Settings

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

Configuring General Settings

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

1. Click the **System** tab, and then click the **General Settings** button.
2. In the *Name* field, give the camera a meaningful name.
3. In the *Location* field, describe the camera's location.
4. 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**
5. In the *Time Settings* area, select how the camera keeps time.
   - To manually set the camera's date and time, enter the time zone on this page.
   - Select the *Automatically adjust clock for Daylight Savings Time* checkbox, if required.
   - To auto-synchronize the camera's date and time with an NTP server, configure the NTP server on the *Network and Security* tab, *Network* page. See the section titled *Configuring the Network Settings*.

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

   - Set up NTP on the DHCP server, if your VMS supports this feature.
   - Use a valid public NTP server.
   - Manually set the correct time in the Time Settings fields.
6. Click **Apply** to save the settings.

Managing the Camera Firmware

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

- To manually upgrade the camera firmware:
  1. Download the latest version of the firmware .bin file from the Pelco website (www.pelco.com/training-support/).
  2. Click the **System** tab, and then click the **Firmware** button.
  3. Click **Choose File**, and then browse to and locate the downloaded firmware file.
  4. Click **Upgrade**. Wait until the camera upgrade is complete.

- To reboot the camera, in the *Reboot Device* area, click **Reboot**.
- To restore the camera to factory defaults, but preserve Network settings, in the *Restore to Factory Defaults* area, select the *Soft Reset* checkbox.
- To restore the camera to factory defaults, in the *Restore to Factory Defaults* area, click **Restore**.

Configuring Storage Management

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

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*, *Remaining Capacity*.

Enabling Onboard Storage

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

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

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

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

Downloading Recorded Video from the Web Interface

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

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

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

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

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

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

Downloading Recorded Video from the SD Card

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

To download recorded video directly from the SD card:

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

Deleting Recorded Video

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

1. Click the **System** tab, and then click the **Storage Management** button.
2. Delete video by one of the following methods:
   - To delete individual video files, in the *Recordings* section, select all of the files you want to delete from the *Recordings* list, click **Delete**, and then click **OK** in the confirmation dialog box.
   - To delete all of the recorded video files, in the section, click **Format Card** to format the SD card, and then click **OK** in the confirmation dialog box.

Configuring Diagnostics

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

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

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

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

Configuring the Network and Security Settings

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

Configuring the Network Settings

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

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

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

   Note: Enabling IPv6 does not disable IPv4 settings.

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

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

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

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

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

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

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

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

   To limit camera access to secure connections only, click to deselect the checkbox for *Enable HTTP connections*. HTTP Port access is enabled by default.
8. In the NTP Server area, select the checkbox for how the server is configured—*DHCP* or *Manual*. If you select *Manual*, type the server address in the *NTP Server* field.
9. In the MTU area, set the Maximum Transmission Unit (MTU) size in bytes. Type a number in the *MTU size* field that is within the available range displayed on the right. Lower the MTU size if your network connection is slow.
10. In the *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.
12. Click **Apply** to save the settings.

Modifying Security Settings

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

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

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

Configuring the Users

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

Adding a User

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

Modifying Users and Passwords

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

menu.

Note: You cannot change the security group for the administrator account.

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

Removing a User

Note: You cannot remove the default Administrator user.

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

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

Keeping Usernames and Passwords After Firmware Revert

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

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

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

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

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

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

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

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

Configuring 802.1x Port-Based Authentication

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

Configuring the 802.1X Port Security

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

   Saved configurations are listed under Saved 802.1x Configurations.

Switching 802.1X Authentication Profiles

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

Removing an 802.1X Authentication Profile

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

Returning to the Network Page

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

Configuring SNMP

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

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

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

   In the SNMP v3 Settings area, complete the following:
   a. *Username*: enter the username that the management station must use when sending the SNMP Get request to the camera.
   b. *Password:* enter the password the management station must use with the chosen username.
6. Click **Apply** to save the settings.

Configuring 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 protcol** 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.

Configuring the IP Filter

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

1. Click the **Network and Security** tab, and then click the **IP Filter** button.
2. In the IP Filter area, click to select the checkbox for Enable IP Filter, to enable IP filtering.
3. Click to select how the camera should filter IP addresses—either by allowing or denying access:
   - **Allow Access**: Select this option to only allow access to the specific IP address entries you will make below.

     Caution: If you choose to filter IP access using the Allow Access option, make sure that you configure the correct addresses to be allowed or you might be locked out of your camera.
   - **Deny Access**: Select this option to deny access to the specific IP address entries you will make below. This is the default option.
4. Add all the *IP Filter Entries* to which access with be either allowed or denied:
   a. Click the add icon (+) to add an entry to the *IP filter Entries* list.
   b. In the IPv4, IPv6 or CIDR range field that appears, enter the IPv4, IPv6 or CIDR range of IP addresses that you would like to filter.
   c. Continue to add more entries to the list until you have added all of the necessary IP addresses to be filtered.

      You can add up to 256 *IP Filter Entries*.
5. Click **Apply** to save the settings.

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

Managing Certificates

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

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

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

Downloading Certificates

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

   Certificates are downloaded as .pem files.

Removing Certificates

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

Downloading Certificate Signing Requests

1. To download the Certificate Signing Request (CSR), click the download **CSR button** and enter the following information:
   - *Common Name*: The primary hostname of the server. 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/yyy. 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.

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

Configuring Imaging

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

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

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

Using Window Blanking

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

Setting a Window Blank

1. Click the **Imaging** tab, and then click the **Window Blanking** button.
2. To add a window blank (privacy zone), click **Add**. A window blank box is added to the video image.
3. To define the window blanking box, perform any of the following:
   a. Drag any side of the box to resize the window blank. Window blank boxes can only be rectangular in shape.
   b. Click inside the box then drag to move the window blank box.
4. Click **Apply** to save the settings.

Deleting a Window Blank

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

Configuring A/V Streams

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

Compression and Image Rate

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, and tertiary streams.

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

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

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

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

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

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

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

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

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

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

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

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

Configuring Smart Compression

Smart Compression technology separates foreground objects from background areas. This reduces the bandwidth required by increasing the image compression to the background areas. As a result, bandwidth is reserved for subjects of interest that require higher image quality.

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

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

1. In the *Smart Compression Settings* area, click to select the checkbox for *Enable* to enable *Smart Compression*.
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. 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, click to select one of the 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 *Configuring Smart Compression Advanced Settings*.

Viewing the RTSP Stream URI

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

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

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

Accessing the Still Image URI

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

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

Saving or Restoring Video Configurations

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

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

Configuring 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.

Configuring Smart Compression Advanced Settings

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

1. Click the **A/V Streams** tab, and then click the **Smart Compression** button.
2. In the **On Motion** section, **Background Quality** field, enter the compression quality for the background (between the default of 6 and the lowest setting of 20).
3. In the **On Idle Scenes** section:
   - **Post-motion delay** field, enter the delay (in seconds) after motion has ended before the camera drops into idle scene settings (between 5 and 60)
   - **Image Rate** field, enter the encoding frame rate (images per second) when there is no motion in the scene.
   - **Quality** field, enter the compression quality when there is no motion in the scene (between 6 and 20).
   - **Max Bitrate** field, enter the maximum number of kilobytes per second when there is no motion in the scene.
   - **Keyframe Interval** field, enter the number of frames between each keyframe when there is no motion in the scene (between 1 and 254 frames).
4. Click **Apply** to save the settings.

Configuring Events

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

Note: Other analytics events, that are not available in the camera UI, can be configured using the Camera Configuration Tool (CCT).

Configuring Motion Detection

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

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

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

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

Configuring 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.

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.

Suspending 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.

Resetting 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.

Note: The PTZ cameras currently only support analytics in their home position. Changing the home position of a PTZ camera effectively changes the camera's field of view and affects the video analytic results. It is recommended that learning progress is reset after a PTZ camera's home position is changed.

Configuring Digital Inputs and Outputs

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

1. Click the **Events** tab, and then click the **DIO** button.
2. To configure a digital input:
   a. Enter a name for the digital input in the **Name** field.
   b. Select the appropriate state from the **Circuit State** drop-down menu. The options are:
      - **Normally Open**
      - **Normally Closed**
   c. Click **Apply** to save the settings.
      After the digital input is connected to the camera, you will see the connection status in the **Circuit Current State** field. The status is typically *Open* or *Closed*.
3. To configure a digital output:
   a. Enter a name for *Digital Output 1* or *Digital Output 2* (if present) in the Name field.
   b. Select the appropriate state from the *Circuit State* drop-down menu.
   c. the *Duration* field, enter how long the digital output is active when triggered. You can enter any number between 100 and 86,400,000 milliseconds.
   d. Click **Trigger** to manually trigger the digital output from the web interface.
   e. Click **Apply** to save the settings.

ExSite® ExSite Pro PTZ Operations Manual

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

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