Pelco Camera Hardening

User Manual

Document number: C7000M

Publication date: 2025-09-15

© 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

C7000M
Revision: 1 – EN
20250915

Contents

About Pelco Camera Hardening 5
Purpose and Scope 5
Importance of Camera Hardening 5
Audience: IT or Site Administrators 5
Essential Camera Hardening Steps 6
Initial Setup and Controlling Access 7
Resetting Devices to Default Settings Before Deploying 7
Disabling HTTP and Enforcing HTTPS 7
Creating the Initial Administrator User and Logging In 7
Upgrading the Camera Firmware 8
Enabling FIPS Compliant Security Engine 8
Defining a Robust Password Policy 8
Practice Principle of Least Privilege 8
Using Secure Communications 10
Replacing the Self-signed Certificate 10
Configuring the TLS Minimum Version 10
Enabling Video Stream Encryption 10
Network Security 11
Disabling Discovery Services 11
Utilizing IP Filtering 11
Recommended Best Practices 13
User Account Management 14
Creating a Backup Admin Account 14
Keeping Usernames and Passwords After Firmware Revert 14
Network Configuration 15
Configuring 802.1X Port-Based Authentication 15
Securing SNMP 16
Activating DSCP 16
Advanced Configuration and Management 18
Certificate Management 19
Downloading a Certificate Signing Request (CSR) 19
Using CCT: 19

Using the Camera Web Interface: 20
Uploading Signed Certificates 20
Using CCT: 20
Using the Camera Web Interface: 20
Applying Certificates 20
Using CCT: 21
Using the Camera Web Interface: 21
Creating Self-Signed Certificates (via the Web Interface) 21
Deleting Certificates 22
Using CCT: 22
Using the Camera Web Interface: 22
Network Settings 23
Changing the HTTP or HTTPS Port 23
Using Camera Configuration Tool (CCT): 23
Using the Camera Web Interface: 23
Configuring IPv6 Settings 23
DNS Lookup Configuration 24
MTU Size Adjustment 24
Link Ethernet Settings 24
Conclusion 25
More Information & Support 26

About Pelco Camera Hardening

Camera hardening is critical for safeguarding against potential security threats and vulnerabilities in your Pelco camera systems. This guide provides essential steps and best practices for IT or Site Administrators to strengthen the security of your cameras, ensuring optimal protection against unauthorized access and malicious activities.

Purpose and Scope

This document serves as a comprehensive guide to enhance the security posture of Pelco Cameras. The guide is designed to provide actionable information for hardening camera devices by configuring various settings. While the Pelco Cameras Operations Manuals cover all configuration options for Pelco cameras, this hardening guide focuses specifically on security-related configurations, including network settings, access control, and encryption. It aims to reduce the risk of potential security breaches and unauthorized access by detailing both required hardening steps and recommended best practices.

Importance of Camera Hardening

Camera hardening is essential for safeguarding against potential security threats and vulnerabilities. By implementing the recommendations in this guide, you can significantly strengthen the security posture of your Pelco cameras, reducing the risk of unauthorized access, data breaches, and malicious activities. Staying vigilant and regularly reviewing and updating security measures is crucial to adapt to evolving threats and ensure continuous protection of your infrastructure.

Audience: IT or Site Administrators

This guide is primarily intended for IT or Site Administrators who are responsible for deploying, configuring, and maintaining Pelco cameras within a security system. A foundational understanding of network configurations, security principles, and camera operations will be beneficial for implementing the recommendations outlined in this document.

Essential Camera Hardening Steps

To establish a robust and secure foundation for your Pelco camera system, it is crucial to implement a series of essential hardening steps. These measures are designed to mitigate common vulnerabilities and significantly reduce the risk of unauthorized access and malicious activities, forming the baseline for optimal device security.

Initial Setup and Controlling Access

To establish a robust and secure foundation for your Pelco camera system, it is crucial to implement a series of essential hardening steps during initial setup and for ongoing access control. These measures are designed to mitigate common vulnerabilities and significantly reduce the risk of unauthorized access and malicious activities, forming the baseline for optimal device security.

Resetting Devices to Default Settings Before Deploying

Before deploying a camera, Pelco recommends resetting it to its factory default settings to ensure the device is in a known default state. This can be done remotely through the camera's web interface or physically at the camera by pressing and holding the factory revert button for 3 seconds. Refer to your specific camera's User Manual for instructions on locating the factory revert button and resetting it to factory default settings. After factory reset and initial user creation, the camera firmware should be updated to the latest firmware available on www.pelco.com. Then the rest of the users can be created.

Disabling HTTP and Enforcing HTTPS

HTTP poses significant security risks due to its lack of encryption. Disabling HTTP and enforcing the exclusive use of HTTPS helps to encrypt data transmission, which is crucial for preventing eavesdropping and man-in-the-middle attacks. HTTPS is enabled by default on Pelco cameras and cannot be disabled. However, HTTP Port access is enabled by default and should be disabled to limit camera access to secure connections only. The HTTPS port can be changed in the Camera Configuration Tool or the camera's web interface. All camera administrative tasks should be conducted over HTTPS. Camera hardening should be done in trusted environment via HTTPS (even though the camera by default uses a Self-Signed Certificate for HTTPS and the web browser shows a warning, it's better to have encrypted communication).

Creating the Initial Administrator User and Logging In

Pelco cameras do not have a default username and password and will be in a factory default state upon initial setup. You must create a user with administrator privileges before the camera becomes 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, ensuring it is secure and complex.
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 then be prompted to log in using these newly created credentials.

Upgrading the 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.

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.

Enabling FIPS Compliant Security Engine

By default, cameras will use a software-based OpenSSL library. On supported cameras, there are other encryption modes that will improve security and comply with Federal Information Processing Standards (FIPS). You have two primary options for enabling FIPS-compliant security:

1. Enable the FIPS-compliant software security engine.
2. Enable the FIPS-compliant secure element to achieve FIPS 140-2 or FIPS 140-3 Level 3 compliance, which will also store the private keys into the secure element.

You can select the encryption engine (Open SSL, FIPS 140-2, FIPS 140-3, or NXP TPM) in the camera's web interface under Security settings. Enabling these settings may cause your device to reboot, leading to a temporary loss of the video stream. NXP TPM enables the onboard trusted platform module to securely store encryption keys and is available on supported cameras.

Defining a Robust Password Policy

Establish a robust password policy that enforces minimum requirements for password strength and complexity. Consider factors such as password length, character types (e.g., uppercase, lowercase, numbers, symbols), and expiration intervals to enhance the overall security posture of your camera system.

Practice Principle of Least Privilege

The cameras allow for user accounts to be created at different privilege levels. To enhance security, limit users to the absolute minimum access required for their tasks. There are three available privilege levels:

- **Administrator**: Has full access to all available features in the camera web interface.
- **Operator**: Has access to the Live View but limited access to setup features. This user can access pages such as General Settings, Image and Display, Compression and Image Rate, Motion Detection, Privacy Zones, Digital Inputs and Outputs, Microphone, and Speakers.

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

- **User**: Has access only to the Live View and cannot access any of the setup pages.

Using Secure Communications

Establishing secure communication channels is fundamental to protecting your camera data from interception and unauthorized access.

Replacing the Self-signed Certificate

By default, Pelco cameras utilize a self-signed certificate for identification and SSL. While these provide basic encryption, it is highly recommended to replace the camera's self-signed certificate with one signed by a trusted Certificate Authority (CA). This ensures authenticity, prevents potential security risks associated with self-signed certificates, and allows the web browser to validate the certificate without warnings. You can manage and configure secure network connections in bulk using the Camera Configuration Tool (CCT), which facilitates downloading Certificate Signing Requests (CSRs) for each camera to be signed by a CA and subsequently uploading the signed certificates back to the cameras. For more information on setting up certificates, see *Certificate Management* on page 19.

Configuring the TLS Minimum Version

It is recommended to update the device configuration to support the best TLS version supported between the camera and the software client. This offers enhanced security features compared to previous versions and prevents downgrade attacks. For increased security, TLS 1.3 is recommended. TLS 1.2 can be selected if required for backwards compatibility. This setting can be found and configured in the Network section of the camera's web interface.

Enabling Video Stream Encryption

Encrypting the video stream helps prevent eavesdropping. Depending on the capabilities of your video management system (VMS), there are different methods available:

- Utilizing a VPN tunnel between the camera network and the VMS server.
- Tunneling Real-Time Protocol / Real-Time Streaming Protocol (RTP/RTSP) over HTTPS.
- Utilizing Secure Real-Time Protocol (SRTP).

For SRTP streaming, specific requirements must be met:

- SRTP streaming requires an HTTPS connection, which can be enabled in your camera's web interface.
- It requires an OpenSSL library connection and does not work with FIPS 140-2 or NXP TPM encryption engines. You can change the encryption engine to use OpenSSL on the Security page in your camera's web interface.
- SRTP streaming requires a Unicast and Multicast over UDP connection.

Network Security

Configuring network security settings is a critical component of hardening your camera system, controlling how devices communicate and preventing unauthorized network access.

Disabling Discovery Services

Discovery protocols are support services that make it easier to find cameras on the network. It is recommended to disable the WS Discovery protocol after deploying the devices and VMS as an additional hardening step to stop other services from discovering devices. Once auto-discovery is disabled, new devices can still be added to the system by manually discovering and adding them.

For Pelco cameras, you can uncheck the **Enable WS Discovery Protocol** checkbox on the Network page to turn off the WS Discovery protocol. This option is enabled by default.

Disabling discovery services can also be done on the VMS you are connecting your Pelco cameras to. Check your VMS documentation for more information.

Utilizing IP Filtering

Pelco cameras contain an IP filtering feature that allows you to control inbound and outbound traffic based on specified criteria, such as IP addresses, ports, and protocols. This helps mitigate risks associated with unauthorized access and network-based attacks.

To configure the IP Filter:

1. Navigate to the **Network and Security** tab, then click the **IP Filter** button.
2. Click to select the **Enable IP Filter** checkbox.
3. Choose 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 define. If you choose this option, ensure 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 define. This is the default option.
4. Add IP Filter Entries to which access will be either allowed or denied:
    - Click the add icon (+) to add an entry to the IP filter Entries list.
    - In the IPv4, IPv6, or CIDR range field that appears, enter the desired IP addresses or ranges to filter.
    - Continue to add more entries until you have included all necessary IP addresses to be filtered (up to 256 IP Filter Entries can be added).
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.

Recommended Best Practices

While the essential hardening steps provide a robust security baseline, implementing the following recommended best practices can further significantly enhance your camera system's resilience against evolving threats. These measures are not strictly mandatory for basic operation but offer additional layers of protection and improved operational security.

User Account Management

Effective user account management is crucial for maintaining control over who can access and configure your camera devices.

Creating a Backup Admin Account

Pelco recommends creating a backup administrator account for your device with a different password than the primary administrator account. This practice helps to protect the default admin account if it is compromised or the password is lost. You can choose to use the backup admin account for daily operations, or keep it as a backup in case the default administrator account is compromised. You can create a backup admin account using the Camera Configuration Tool (CCT) or additional user accounts with the camera web interface.

Keeping Usernames and Passwords After Firmware Revert

To add a layer of security to protect the device from theft, you have the option of keeping the device's current usernames and passwords after a firmware revert. Normally, if you restore the device firmware back to the factory default settings, the device returns to using the default username and password. When you enable this feature, the device will continue to use the configured username and passwords, so the device 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. Always keep a copy of your password in a safe place to avoid losing access to your device.

To enable this feature:

1. In the camera's web interface, navigate to 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 selecting the checkbox, a popup message will appear stating: `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.

Network Configuration

Optimizing network configurations beyond the basic setup can significantly enhance the security and performance of your camera system.

Configuring 802.1X Port-Based Authentication

If your network architecture supports it, enabling IEEE 802.1X authentication for wired and wireless networks will enhance network security by authenticating devices before they are granted access to the network. This ensures that only authorized cameras can connect and transmit data. You can configure multiple 802.1x profiles, but only one can be enabled at a time.

To set up 802.1X port-based authentication:

1. In the camera's web interface, navigate to Network > 802.1x.
2. From the EAP Method drop-down list, select the preferred authentication method and complete the related fields:
    - PEAP (for username and password authentication):
        - Configuration Name: Enter a profile name.
        - EAP Identity: Enter the username used to authenticate the camera.
        - Password: Enter the password used to authenticate the camera.
    - EAP-TLS (for certificate authentication):
        - Configuration Name: Enter a profile name.
        - EAP Identity: Enter the username used to authenticate the camera.
        - TLS Client Certificates: Select the PEM-encoded certificate file to authenticate the camera.
        - Private Key: Select the PEM-encoded private key file to authenticate the camera.
        - Private Key Password: If the private key has a password, enter it here.
        - The uploaded files are used to generate a unique certificate to authenticate the camera, which is displayed in the Uploaded Certificate field.
3. Click **Save Config** to save the authentication profile. If this is the first profile added, it is automatically enabled.
    - To use a different authentication profile, select the saved configuration then click **Enable**.
    - To delete an authentication profile, select the saved configuration then click **Remove**.

Securing SNMP

Simple Network Management Protocol (SNMP) can be used to manage cameras connected to the network and send camera status information to an SNMP management station. By default, SNMP is disabled. If SNMP is necessary, ensure it's configured securely, preferably using SNMP version 3 (SNMP v3) with strong authentication and encryption mechanisms. SNMP v3 offers greater security by allowing you to set a username and password for the camera, and it does not support traps.

To configure SNMP:

1. In the camera's web interface, navigate to the **Network and Security** tab, and then click the **SNMP** button.
2. In the SNMP Configuration area, click to select the checkbox for **Enable SNMP**.
3. From the **Version** drop-down menu, select the preferred SNMP version. Both versions can be configured, but only one can be enabled at a time.
    - **SNMP v2c**:
        - Click to select the checkbox for **Enable Traps** to enable traps from the camera.
        - In the **Read/Write Community** field, enter the read community name for the camera. Only SNMP management stations with the same read community name will receive a response.
        - In the **Trap Destination IP** field, enter the IP address of the management station where traps will be sent.
        - In the **Available Traps** area, select the traps that will be sent (e.g., Temperature Alert, Camera Tampering, Edge Storage Status).
    - **SNMP v3**: This camera uses SHA-1 type authentication and AES type encryption.
        - **Username**: Enter the username the management station must use for SNMP Get requests.
        - **Password**: Enter the password the management station must use with the chosen username.
4. Click **Apply** to save the settings.

Activating DSCP

Differentiated Services Code Point (DSCP) is a computer networking architecture that specifies a simple and scalable mechanism for classifying and managing network traffic, providing quality of service (QoS) on modern IP networks. It can 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. DSCP uses a 6-bit code point in the IP header for packet classification.

To activate and configure DSCP:

1. In the camera's web interface, navigate to the **Network and Security** tab, and then click the **DSCP** button.
2. The **Activate feature** checkbox is selected by default. Clearing it will disable DSCP and reset all values on the page to DF(0). DF(0) refers to Default Forwarding with a DSCP value of 0.
3. Select DSCP values from the drop-down menus for various traffic types:

- ONVIF protocol (default CS2(16)).
- Web interface (default AF21(18)).
- SNMP (default CS2(16)).
- Primary Stream (default AF41(34)).
- Secondary Stream (default AF41(34)).
- Tertiary Stream (default CS3(24)).
- Replay Stream (default CS3(24)).

4. Click **Apply** to save the settings. You can click **Restore Defaults** and then **Apply** to revert all DSCP values to their default settings.



NOTE

In the 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.

Advanced Configuration and Management

This section covers advanced configuration options that provide granular control over your camera system's security, network behavior, and streaming capabilities. While not always required for every deployment, these settings can be critical for specific environments, compliance requirements, or when integrating with complex video management systems.

Certificate Management

Certificates are essential for authenticating devices and encrypting communication over the network, providing a layer of trust and security. Administrators can manage these certificates to ensure secure connections.

You can view existing certificate information, including Cert ID, Subject, Issuer, Algorithm, Expiry Date, and Type (trusted or not trusted), in the Certificates area of the camera's web interface.

Downloading a Certificate Signing Request (CSR)

A Certificate Signing Request (CSR) is required for each camera to obtain a CA-signed certificate. This CSR must be signed by a certificate authority (CA) to be applied to a camera.

You can download a CSR using either the Camera Configuration Tool (CCT) or the camera's web interface. CCT can be used to perform this task on multiple cameras at one time, while the camera's web interface method must be done separately for each camera.

Using CCT:

1. Select the **TLS** tab in CCT.
2. In the **Download CSR** column, select the checkbox for the camera(s) you would like to download the CSR for.
3. Click **Apply**.
4. Enter the following information for the CSR(s):
    - **Common Name** for the CSRs (maximum 64 characters, including Prefix, Suffix, and Source of unique data). A preview is displayed as you enter a value. The Common Name cannot be empty, so you must enter a value for at least one of the Prefix, Suffix, and Source of unique data fields, or any combination of those fields.
        - **Prefix**: Enter a prefix for the Common Name.
        - **Source of unique data**: Select one camera identifier to append to the common name (for example: Counter, Name of the camera, IP address, MAC address, Serial number). This is useful when downloading CSRs for multiple cameras.
        - **Suffix**: Enter a suffix for the Common Name.
    - **Subject Alternative Name** for the CSRs. You can use user input or select a camera identifier (such as Hostname, or IP address).
    - Enter optional fields such as Organizational Unit, Organization, Locality, State or Province, and Country.
5. Click **Download CSR** and select where to save the zip file.

Using the Camera Web Interface:

1. Click the **Download CSR** button on the Certificates page.
2. Enter the required information: Common Name (primary hostname of the server), Subject Alternative Name (for example: email address, IP addresses, URIs, DNS names), Organizational Unit, Organization, Locality, State or Province, and Country.
3. Click the **Download** button to download the CSR file.

Uploading Signed Certificates

Once the CSRs have been signed by a Certificate Authority (CA), the signed certificates can be uploaded to the cameras. It is recommended to add the CA certificate file to the same zip file as the signed certificate(s) to properly display which cameras have trusted certificates in CCT. Signed certificate files must have specific file extensions such as .crt, .cer, or .pem.

Using CCT:

1. In the top-right corner of CCT, select the menu icon (typically three dots or lines) > **Upload Certificates**.
2. Select the zip file containing the signed certificates.
3. Review the summary of the signed certificates.
4. Click **Upload**. Only certificates for connected devices will be uploaded.
5. Click **OK**.

Using the Camera Web Interface:

1. To upload a certificate, click **Upload Cert**.
    a. Upload the **Certificate** file.
    b. Upload the **Private key** file.
    c. Enter the **Private key password**, if applicable.
2. Click the **Upload** button to upload the certificate.
3. To upload a CA certificate, click **Upload CA Cert**.
    a. Upload the **CA Certificate** file.
    b. Enter the **CA Certificate ID**.
4. Click the **Upload** button to upload the CA certificate.

Applying Certificates

After uploading signed certificates, you must apply them to their respective devices to activate them.

Using CCT:

1. Select the **TLS** tab.
2. In the **TLS Certificate Subject** column, select the desired certificate for each camera.
3. Click **Apply**.

> **TIP**
> Click **Manage** to view details about all available uploaded certificates before applying one to a camera.

Using the Camera Web Interface:

1. After creating or uploading a certificate, click the **Make Active** button.
2. Click **OK** in the pop-up message.

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

Creating Self-Signed Certificates (via the Web Interface)

You can create self-signed certificates directly from the camera's web interface if a CA-signed certificate is not immediately available.

> **IMPORTANT**
> While self-signed certificates can provide encryption, they do not offer the same level of trust and authentication as certificates signed by a trusted Certificate Authority (CA). Web browsers and some video management systems may display warnings about untrusted connections, and they do not verify the identity of the camera, which can impact the overall security of your system.

1. Navigate to the **Network and Security** tab, and then click the **Certificates** button.
2. In the **Valid Not Before** field, enter the date that the certificate becomes valid in the format `mm/dd/yyyy`. This field is required. You can also click the calendar icon to select a date.
3. 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.
4. Enter the following information:

- Common Name: The primary hostname of the server (required).
- Subject Alternative Name (DNS): Alternative values (such as email address, IP addresses, URIs, DNS names).
- Organizational Unit: The name of the unit within the organization.
- Organization: The name of the organization.
- 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.

5. Click the **Create** button.

Deleting Certificates

You can remove invalid, expired, self-signed, or unwanted certificates from a camera.

Using CCT:

1. Select the **TLS** tab.
2. In the Manage Certificates column, click **Manage**.
3. Click **Delete** next to the certificate you want to remove.
4. Click **Yes** to confirm.



NOTE

You cannot delete a certificate that is currently active. Apply a different certificate first, and then delete the unused certificate. You also cannot delete a certificate when editing other settings in CCT; apply or discard changes first.

Using the Camera Web Interface:

1. To remove a Certificate, click the **Remove** button.
2. Click the **OK** button in the confirmation dialog box.

Network Settings

This section details advanced network configurations that allow for fine-tuning how your camera connects and communicates within your network environment.

Changing the HTTP or HTTPS Port

You can select which ports the cameras should use to connect to the network over HTTP and HTTPS. The default port numbers are HTTP Port: 80, HTTPS Port: 443, RTSP Port: 554, RTSP Replay Port: 555, and WebRTC Port: 9090. You can enter any port number between 1 and 65534.

Using Camera Configuration Tool (CCT):

1. Select the **Network** tab.
2. In the **HTTP Port #** column, enter the new HTTP port number.
3. In the **HTTPS Port #** column, enter the new HTTPS port number.
4. Click **Apply**.

Using the Camera Web Interface:

1. Navigate to the Network and Security tab, and then click the **Network** button.
2. In the Port Settings area, specify which control ports are used to access the camera.
3. Enter the desired HTTP and HTTPS port numbers.
4. Click **Apply** to save the settings.

Configuring IPv6 Settings

You can enable IPv6 settings for your camera through the camera's web interface. Enabling IPv6 does not disable IPv4 settings.

1. On the Network page, in the IPv6 Settings area, click to select the checkbox for **Enable IPv6**.
2. Configure the following settings:
    - Click to select the checkbox for **Accept Router Advertisements** if using Stateless Address Auto-Configuration.
    - From the **DHCPv6 State** drop-down menu, select one of the following:
        - **Auto**: DHCPv6 state is determined by router advertisements (RA). 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.

3. You can also customize the **Network Hostname** in the provided field.
4. Click **Apply** to save the settings.

DNS Lookup Configuration

You can specify how the camera obtains a Domain Name System (DNS) server address in the camera's web interface.

1. In the **DNS Lookup** area of the Network page, select one of the following options:
   - 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.
2. Click **Apply** to save the settings.

MTU Size Adjustment

You can set the Maximum Transmission Unit (MTU) size in bytes.

1. In the MTU area of the Network page, type a number in the MTU size field that is within the available range displayed on the right.
2. Lower the MTU size if your network connection is slow.
3. Click **Apply** to save the settings.

Link Ethernet Settings

You can configure the Ethernet link settings for your camera.

1. In the Link Ethernet Settings area of the Network page, click to select an option from the **Speed & Duplex** drop-down menu.
2. The **Auto-negotiation (default)** setting is the preferred setting for most cameras, as it will negotiate the optimal speed and duplex setting for your network connection.
3. Click **Apply** to save the settings.

Conclusion

By following these guidelines for device hardening, you can significantly improve the security posture of your Pelco cameras, reducing the risk of potential security breaches and unauthorized access. It is imperative to stay vigilant and regularly review and update security measures to adapt to evolving threats and ensure continuous protection of your infrastructure.

More Information & Support

For additional product documentation, software, and firmware upgrades, and technical support, refer to the following resources:

- Camera Configuration Tool (CCT) download and User Guide.
- The Operations Manual(s) for your Pelco camera(s).

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.