Pelco Camera Hardening Guide

Version 3.0

February 21, 2020

This hardening guide is applicable to the current generation of IP cameras and video management solutions and is geared to the latest releases at the time of this publication.

This guide is geared to hardening configuration and practices of the IP Cameras but does not address general deployment recommendations already covered in camera operation manuals.

Contents

Secure Configuration Recommendations

Secure configuration for IP cameras will follow a basic methodology.

1. Initial Setup
2. Configure for Least Privilege.
3. Configure for Least Functionality.
4. Add Access Controls

Initial Setup

The initial camera setup should involve these configuration steps:

1. Account Setup
2. Update the camera firmware
3. Configure networking options
4. Configure authentication
5. Configure Encryption

Account Setup

To secure access to a new camera, an initial administrator account must be established.

Select 'Change Settings' and create an account. Reference the User and Admin Guides for the initial installation.

A longer password that is more complex (multiple character types – upper case, lower case, numerical, special characters) is much stronger and harder to crack.

Update the Camera Firmware

Download the latest versions from pelco.com to stay current with the latest available features, bug fixes, and security patches.

www.pelco.com/updates

Authentication

Pelco cameras support digest authentication. Passwords are not transmitted in clear text during authentication.

After the initial account is created, log into the camera with the new credential and configure 'Closed Authentication' for Pelco API and 'Require Authentication' for RTSP/JPEG. Video clients must support closed authentication and enabling RTSP authentication will disabled multicast on boot.

Network

IP Cameras support core network services to function properly. These core services include:

- Dynamic Host Configuration Protocol (DHCP) – allows hosts to be connected to a network and have an IP address allocated automatically. If your network utilizes DHCP, configure the DHCP server(s) to issue reservations for all cameras and VMS components. For IPv4, DHCP is enabled by default. IPv6 is set to auto configuration mode. Both can be modified to manual settings.
- Domain Name System (DNS) – provides for resolution of a human readable/memorable hostname to an IP address. Use a consistent naming convention and utilize fully qualified domain names with A records mapped to the IP address. Name servers can be configured in the camera through DHCP options.
- Network Time Protocol (NTP) – ensures all hosts on a network have a common clock to support logging and timestamps. Time servers can be configured in the camera through DHCP options or set manually.

Encryption

Encrypt administrator access to the camera by enabling TLS. Pelco cameras support TLS version 1.2 with support for strong cipher suites.

There are 3 TLS configuration modes – disabled (default), optional (HTTP+HTTPS enabled), and required (HTTPS only, recommended).

Pelco cameras can generate self-signed certificates or accepts upload of digital certificates signed by external PKI. Optionally, the camera can generate a Certificate Signing Request to ease support external PKI.

Configure for Least Privilege

Create a system account, or accounts, and apply the least privilege role necessary for the job duties.

The Principle of Least Privilege is a best practice tenet that requires a system user is granted only the lowest permission level necessary to perform their job function.

Pelco products ship with pre-configured roles and permissions to support enforcement of the principle of least privilege. Pelco IP Cameras have 4 built-in roles with associated permissions.

- Admins – full control of all camera features and functions
- Managers – full control except for user management and restoring factory default settings
- Operators – have access to view video, control PTZ
- Viewers – can only view the video

It is common for a single individual to support multiple roles. In the case of administrators, Pelco recommends that a separate non-admin level account be created for use with any less-privileged functions. For example, the admin may also be an operator for day to day function. A separate operator account could be used for normal operation.

Configure for Least Functionality

Disable any services that are not needed for your environment.

SNMP, SSH, and FTP are examples of services that may exist on some camera models that can be optionally enabled. If they are not necessary for your environment, they should remain disabled. If SNMP is needed, SNMPv3 does support authentication and encryption.

Once TLS is configured on the device, HTTP access can be disabled with the HTTP-only option.

Many environments use IPv4. Pelco cameras do support IPv6, which can be optionally disabled.

Add Access Controls

Historically, video surveillance has been conducted over separate media (CCTV, coaxial cables, etc.). With the advent of IP cameras, it became possible to share network resources with the enterprise IT infrastructure. Many organizations continue to keep the video network isolated from the IT network in order to support the principle of separation of duties. While this isolation may be provided by either physical or logical separation, this guide addresses a logical means separation for video infrastructure. Certainly, these practices may also be employed within a physically separate network.

With modern converged IP networks, it is often possible to emulate network isolation with VLANs and network-based access control lists. It is a good practice to maintain VLAN separation for the IP camera network and to control access to surveillance assets.

Camera 802.1X

While network access control (NAC) is outside the scope of this hardening guide, Pelco does recommend the use of 802.1x for those organizations that can support it.

802.1x allows device authenticated to a connected network. This does add some initial administrative overhead, but can be used to prevent rogue devices on the network.

Cameras support several EAP modes, including:

- EAP-MD5
- EAP-PEAP
- EAP-TLS
- EAP-TTLS

Camera Firewall

Pelco cameras have a firewall feature that allow an administrator to control access to the camera. This may be used to augment network-based access controls. Exercise caution when configuring the camera firewall as it is possible to block administrative network access. Recovery would require use of the physical reset button on the camera to restore defaults. Please consult the admin guide for your model of camera.

The firewall allows either allow or deny one or more IP addresses. The firewall evaluates each line, top-down looking for an IP address match.

The 'allow' list implements a whitelist of IP addresses followed by an implicit 'deny all'. Any IP address not included on the list will be denied. Use caution to avoid removing your ability to administer the camera.

The 'deny' list implements a blacklist of IP addresses to be blocked followed by an implicit 'allow all'. Any IP address not on the deny list would be allowed.

Should the camera firewall be enabled, Pelco recommends a whitelist of systems that must administer and operate the video solution. These addresses should include, but are not limited to:

- VMS(s)
- Recording/Storage Device(s)
- Multicast Address(es)
- Monitoring system(s)
- Operator Console(s)
- Security Administrator Workstation(s)
- Any other authorized system requiring access to video directly from the camera

Be cognizant of dynamically assigned addresses that may change over time. Although DHCP server administration outside the scope of this document, it is a good practice to create DHCP reservations for devices that may be included in a camera firewall.

Additional Network-based Controls for Consideration

Multicasting

With multicast streaming, a video need only be sent once and can be received by multiple recipients (clients, recorders, etc.). This is efficient and less burdensome than sustaining multiple unicast streams.

There is trade-off for this efficiency in terms of added complexity and potentially reduced confidentiality. Multicast routing must be configured to function across a network layer3 boundary. As multicast video is a one-to-many communication, the stream is visible to any system that has registered as a member of the multicast group. With some network switches, the multicast may be visible to all devices in a VLAN.

To restrict access to a multicast stream, some form of network level access control must be implemented. Consult your network vendor product documentation for proper configuration of multicast routing and multicast access control.

Ultimately, the decision to employ multicast or unicast is a network design decision to be made based on the pros and cons and abilities of the network environment.

VLANs

A VLAN (Virtual Local Area Network) is a useful means of logical network isolation. IP surveillance assets may be placed in a separate VLAN than other IT assets to augment access control and confidentiality.

QOS

Media streams require lower latency and jitter than typical data applications. While an IP surveillance network often works just fine on a converged network, network congestion may impact real-time streaming performance and possibly availability. Enter Quality of Service (QOS). QOS may be used to "mark" packets from the camera so that network switches may prioritize the traffic. Please refer to your network equipment manufacturers guidance for configuration of QOS.

Operation and Maintenance Recommendations

Beyond camera configuration, there are some practices that can help improve your security:

Stay up to date. Pelco periodically releases firmware updates to address bugs and vulnerabilities. Subscribe to pelco.com for notification of new software and firmware releases. Check for patches and updates and keep your products up to date. Stay abreast of product lifecycles, plan and coordinate upgrades.

Maintain procedures to safeguard configuration backups and to restore a device from backups as necessary.

Please report potential product vulnerabilities through the web portal (https://www.pelco.com/report) of by email (cybersecurity@pelco.com).