PELCO®

VideoXpert

v 3.9 System Hardening Guide

VideoXpert™

Document number: C6672M-A

Publication date: 06/20

Table of Contents

Introduction

This hardening guide is applicable to the current generation of Pelco video management solutions and is geared towards the latest versioned release. At the time of this publication, VideoXpert v 3.9 is the most current release.

This guide is geared to hardening and best practices of VMS configurations, but does not address general deployment recommendations already covered in VMS operation manuals.

Note: Prior to making any configuration changes recommended by this guide, please refer to any organizationally specific policies and standards that may be applicable. Pelco's recommendations are implementation suggestions based on industry best practices and are in no way intended to replace an organization's pre-existing IT directives.

Using Default Security Features

VideoXpert includes a myriad of build-in security features to accommodate and support the hardening of your VMS. Some of these capabilities include configurable roles and permissions for application users. Upon initial configuration of the system, default passwords are required to be changed. These passwords are then stored with cryptographic functions in order to protect their confidentiality. Additionally, VideoXpert supports auditing capabilities through its logging and user action reports. Communication between VideoXpert components is also encrypted over TLS and configurations are supported to enforce validation of digital certificates prior to connecting to the VMS; ensuring proper authentication is performed. By default, Pelco uses a self-signed certificate, but allows for an organization to configure and upload their own certificate. For further instruction on enabling certificate validation and managing these certificates for VideoXpert, please refer to the operations manual that applies to your installed VideoXpert component and version. These are available at https://www.pelco.com/docs/.

Following Secure Configuration Recommendations—Initial Setup

Ensuring Secure Installation

Prior to making any changes to the system at all, ensure adequate backup and recovery procedures are in place. Pelco recommends that you create backups of essential files/data and system and application configuration settings. Backup procedures specific to VideoXpert can be found in the corresponding operations manual available for download from Pelco's Document Center at https://www.pelco.com/docs/.

If installing a VMS on your own hardware, Pelco recommends that a clean version of Windows be installed fresh on the system using a valid Microsoft image. Previously used systems might have pre-existing malware, spyware, or other unknown exploitable vulnerabilities.

Even in fresh installations of Windows, a system likely has unnecessary programs installed. These programs expand the attack surface and become potential points of entry for system compromise. Installed programs should be reviewed, with the resulting unneeded programs being completely removed/uninstalled. Verify that all installed programs are legitimate and required for functionality.

Updating the System

Ensure that each installed application and the underlying OS of each server and computer on your system has the latest updates that address the current known vulnerabilities. For Windows, you can check for updates directly through the OS. For VideoXpert, the latest patches and versions of software releases can be located at https://www.pelco.com/updates/.

On a continual basis:

- Frequently update the OS and the necessary installed applications to ensure newly discovered vulnerabilities are patched as soon as a patch is available.
- Frequently update anti-virus libraries with the latest patches and definitions.

Note: Updates can often require a restart. This can be a problem if high availability is required (which is often the case for surveillance systems) because the server cannot receive data from devices when it is restarting. There are a number of options to minimize this impact on availability. For example, you can download updates to the system first, and then apply them at a time when a restart will not disrupt operations significantly. Pelco recommends that you verify the updates in a test environment before implementing the changes across the entire organization or VMS.

Setting-up the Account

To secure access to a new VMS, you must configure an initial administrator account.

Configuration of the initial VMS administrator account will be invoked upon first use of the VMS application. For the initial installation, see the current version of the following documents:

- For VideoXpert Enterprise Systems: VideoXpert Enterprise System Configuration Guide, VideoXpert Enterprise Installation Manual, and the VxToolbox Operations Manual
- For VideoXpert Professional Systems: VxToolbox section of the VideoXpert Professional Operations Manual

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

Configuring Authentication

Authentication is a process for verifying the identity of an object, service, or person. When you authenticate an object, the goal is to verify that the object is genuine. When you authenticate a service or person, the goal is to verify that the credentials presented are authentic.

Pelco recommends that, whenever possible, you use Windows users in combination with Active Directory (AD) to authorize access to the underlying system. This allows you to enforce:

- A password policy that requires users to change their password regularly and prevents older passwords from being used.
- Brute force protection, so that the Windows AD account is blocked after a predefined number of consecutive failed authentication attempts, again in line with the organizational password policy.
- Multi-factor authentication into the system, particularly for administrators.
- Role-based permissions, so you can apply access controls across your domain.

Overall, AD allows for a more consistent Windows authentication baseline that can be tracked and enforced across the entire network for both users and computers.

Note: If your organization does not use Active Directory or if the VMS is isolated from your IT network as a standalone system, local group policy can be modified to address secure authentication by configuring your organizationally specific policies in the *Windows Local Group Policy Editor*, under **Computer Configuration** > **Windows Settings** > **Security Settings**.

Using Windows Defender Credential Guard

As a built-in Windows solution for safeguarding credentials, Pelco strongly encourages you to enable Windows Defender Credential Guard. This feature uses virtualization-based security to isolate secrets so that only privileged system software can access them. Unauthorized access to these secrets can lead to credential theft attacks, such as Pass-the-Hash or Pass-The-Ticket. Windows Defender Credential Guard prevents these attacks by protecting NTLM password hashes, Kerberos Ticket Granting Tickets, and credentials stored by applications as domain credentials.

By enabling Windows Defender Credential Guard, the following features and solutions are provided:

- **Hardware security**: NTLM, Kerberos, and Credential Manager take advantage of platform security features, including Secure Boot and virtualization, to protect credentials.
- **Virtualization-based security**: Windows NTLM and Kerberos derived credentials and other secrets run in a protected environment that is isolated from the running operating system.
- **Better protection against advanced persistent threats**: When Credential Manager domain credentials, NTLM, and Kerberos derived credentials are protected using virtualization-based security, the credential theft attack techniques and tools used in many targeted attacks are blocked. Malware running in the operating system with administrative privileges cannot extract secrets that are protected by virtualization-based security. Although Windows Defender Credential Guard is a powerful mitigation method, persistent threat attacks will likely shift to new attack techniques. You should incorporate other security strategies and architectures.

Enable Windows Defender Credential Guard by using Group Policy:

1. From the *Group Policy Management Console* (“gpedit.msc”), select **Computer Configuration** > **Administrative Templates** > **System** > **Device Guard**.
2. Double-click **Turn On Virtualization Based Security**, and then click **Enabled**.
3. In the *Select Platform Security Level* box, select **Secure Boot** or **Secure Boot and DMA Protection**.
4. In the *Credential Guard Configuration* box, click **Enabled with UEFI lock**, and then click **OK**. To be able to turn off Windows Defender Credential Guard remotely, select **Enabled without lock**.
5. In the *Secure Launch Configuration* box, select **Enabled**.
6. To enforce processing of the group policy, you can run “gpupdate /force” in Command Prompt (“cmd.exe”).

Using Device Authentication

Another consideration for achieving a more robust authentication baseline involves the practice of secure device authentication through the use of digital certificates. For instance, implementing 802.1x authentication (within the underlying Windows system) as a network access control (NAC). A NAC will securely authenticate authorized devices and prevent rogue devices from connecting to the network. Device whitelisting techniques, such as implementing a host-based security system (HBSS), are also effective for preventing rogue devices from connecting to both networks and standalone systems. More information concerning HBSS features and configurations can be found later in this guide, in the section titled *Considering Additional Security Controls*. Ensure that you consult with your network and/or end-point security vendor for implementation of these solutions.

Configuring the Network Protocols, Ports, and Services (PPS)

All VideoXpert components and their associated network ports, protocols, and services (PPS) are listed in individual tables below. In order to determine which network services to enable on a particular system, you must consider all services required to run on said system. For example, to ensure that the network blocks only unwanted traffic, specify rules that allow for the necessary traffic of each VideoXpert component installed. Keep in mind that this guide is specific to VideoXpert; additional network traffic rules can be created in order to ensure overall functionality. This functionality is dependent upon other necessary or required applications and services running on your system that are separate from the VMS. More on access control and how to prevent unwanted network connections/traffic will be addressed later in this guide.

Table 1: VideoXpert ProServer Protocols and Ports

Protocol	Ports	Service
TCP/HTTPS	443	REST API
UDP/SSDP	1900	SSDP Discovery
TCP/RTSP	5544	Video and audio command and control
TCP/SSH	6666	Application-specific debugging
TCP/HTTP	9091	REST API
TCP/psql	15432	PostrgeSQL database (localhost service)
UTP/RTP	41950-61000	Receiving streamed video and audio
UDP/RTCP	41950-61000	Receiving metadata regarding the media streams

Table 2: VxOpsCenter protocols and ports

Protocol	Ports	Service
UDP/syslog	34543	Logging
TCP/RTP	43421	Decoder command and control (localhost service)
UDP/RTP	random	Receiving streamed video and audio

Table 3: VxToolbox protocols and ports

Protocol	Ports	Service
UDP/SNMP	161	VxSNMP service
TCP/SSH	6667	VxToolbox debugging
TCP/JMX	6660	Java debugging interface (localhost service)
TCP/Telnet	7777	Application-specific debugging (localhost service)
TCP/GRPC/TLS	31457	Internal application communication (localhost service)
TCP/HTTP	31458	Software updating cameras
TCP/debug	>49000	VxToolbox opens a random ephemeral port >49000 for debug functionality with JVisualVM. Removal of this feature is under investigation for a future release.

Table 4: Core protocols and ports

Protocol	Ports	Service
TCP/HTTP	80	HTTP, used for camera configuration as necessary
TCP/HTTPS	443	HTTPS
UDP/SSDP	1900	SSDP discovery target on 239.255.255.250
TCP/Hazelcast	6001	Hazelcast communications, before cluster configuration
TCP/Hazelcast	6002	VxDatabase Hazelcast communications, before cluster configuration
TCP/Postgres	15432	Database
TCP/Hazelcast SSL	16011	Hazelcast SSL communications, after cluster configuration
TCP/Hazelcast	16012	VxDatabase Hazelcast TLS communications, after cluster configuration

Table 5: Media Gateway protocols and ports

Protocol	Ports	Service
UDP/RTP/RTSP	All	When streaming Unicast from cameras, the Media Gateway uses ports in the range 41950-65535 to receive the data, but the client may request data on any port. Multicast data will use the port configured on the camera, thus all UDP ports must be available.
TCP/RSTP	554	RTSP
TCP/HTTPS	5443	Internal API, HTTPS (MJPEG and other communication)
TCP/Hazelcast	6002	Hazelcast communications, before cluster configuration
TCP/HTTP	8090	Internal API, HTTPS (MJPEG) not used by the system
TCP/Hazelcast SSL	16002	Hazelcast SSL communications, after cluster configuration

Table 6: VxStorage protocols and ports

Protocol	Ports	Service
UDP/SSDP	1900	SSDP discovery
TCP/RTSP	5544	RTSP video and audio command and control
TCP/Hazelcast	6003	Hazelcast communications
TCP port/ HTTP	9091	HTTP, API calls
TCP/HTTPS	9443	HTTPS, API calls
UDP/RTP	41950-65535	Receiving streamed video and audio
UDP/RTCP	41950-65535	Receiving media streams metadata

If recording in multicast mode, the required UDP port range is determined by the cameras.

Configuring Encryption

Encryption has become a staple in the security world as a fortifying tool for controlling access to privileged and/or sensitive information. There are numerous supported features and capabilities that Pelco recommends implementing with respect to the use of encryption.

By default, VideoXpert account credentials are protected with cryptographic functions. Furthermore, the VMS includes a forced encryption setting on exports of recorded camera streams. This setting can be enabled any time after initial setup of VideoXpert within VxToolbox, under the “System” tab. Another default security feature is the encryption of VideoXpert database columns containing sensitive information.

Using Data At Rest

As an additional layer of security, Pelco recommends that you use some form of data at rest (DAR) solution by implementing whole disk encryption (WDE). VideoXpert is capable of supporting certain WDE programs, such as the built-in Windows feature, BitLocker. To enable and manage BitLocker, navigate to the *Control Panel* and select **BitLocker Drive Encryption**.

In line with enabling DAR protection, Pelco also recommends that you verify the existence of a Trusted Platform Module (TPM) and Unified Extensible Firmware Interface (UEFI) firmware compatibility (as opposed to legacy BIOS) with Secure Boot enabled.

Using Trusted Platform Module (TPM) Technology

TPM technology is designed to provide hardware-based, security-related functions. A TPM chip is a secure crypto-processor that is designed to carry out cryptographic operations. The chip includes multiple physical security mechanisms to make it tamper resistant, and malicious software is unable to tamper with the security functions of the TPM. Some of the key advantages of using TPM technology are that you can:

- Generate, store, and limit the use of cryptographic keys.
- Use TPM technology for platform device authentication by using the TPM’s unique RSA key, which is burned into itself.
- Help ensure platform integrity by taking and storing security measurements.

The TPM must be enabled in the system firmware during system boot. To verify your current TPM configuration, run "tpm.msc" when logged in to Windows.

Using UEFI with Secure Boot

UEFI provides additional security features in comparison to legacy BIOS firmware, including Secure Boot—a standard that ensures systems boot only to a trusted operating system. UEFI is required to support additional security features in Windows, including Virtualization Based Security and Credential Guard. Systems with UEFI that are operating in Legacy BIOS mode will not support these security features.

To verify your system firmware, run **System Information**. Under *System Summary*, *BIOS Mode* displays your current firmware specification. To verify Secure Boot configuration, in the same *System Summary* window, look under *Secure Boot State*. Just like TPM, Secure Boot must be enabled within the system firmware during reboot.

Using FIPS Cryptographic Modules

Pelco VideoXpert supports the enforcement of FIPS 140 validated cryptographic modules. The United States Federal Information Processing Standard (FIPS) defines security and interoperability requirements for computer systems that are used by the U.S. federal government. The FIPS 140 standard defines approved cryptographic algorithms. The FIPS 140 standard also sets forth requirements for key generation and for key management. The National Institute of Standards and Technology (NIST) uses the Cryptographic Module Validation Program (CMVP) to determine whether a particular implementation of a cryptographic algorithm is compliant with the FIPS 140 standard. An implementation of a cryptographic algorithm is considered FIPS 140-compliant only if it has been submitted for and has passed NIST validation.

Enforcing the use of FIPS compliant algorithms will help ensure the system does not accept nor allow the use of weak or antiquated ciphers.

To force FIPS compliant algorithms in Windows:

1. Open the *Local Group Policy Editor* (run “gpedit.msc”).
2. Navigate to **Computer Configuration** > **Windows Settings** > **Security Settings** > **Local Policies** > **Security Options**.
3. In the right panel, scroll to and double-click **System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing**, and then click to select the radio button for *Enabled*.
4. Click **Apply**.
5. Close *Local Group Policy Editor*.
6. In order to apply new group policy, do one of the following:
   - Reboot the system.
   - Open Command Prompt (run “cmd.exe”) as administrator and execute the command: “gpupdate /force”.

   When the group policy change has taken effect, the system will configure itself to use FIPS 140 cryptographic libraries.

Updating Browsers

To reinforce the use of stronger algorithms, ensure any web browsers installed on the system are up to date with the latest version installed. Also confirm that the browsers are configured to check for publisher’s certificate revocation status. This enforces a policy that all PKI signed objects shall be validated.

Configuring for Least Privilege

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

A role is a group of permissions that define abilities and responsibilities within a system. A user must be assigned at least one role to perform actions within the system. Create a system account, or accounts, and apply the least privilege role necessary for the job duties.

Configuring VideoXpert Roles and Permissions

If you are authenticating using LDAP, you are not required to manage accounts and roles, but you can in order to control settings that are not specified in LDAP. For more instruction on how to sync VideoXpert roles when using LDAP, please see the applicable VideoXpert Operations Manual.

Pelco products ship with pre-configured roles and permissions to support enforcement of the principle of least privilege.

There are four default roles within VideoXpert:

- **Administrator** has full rights to the system.
- **Manager** has all Supervisor rights and the ability to configure recorders and devices within the system, including tags, recorder assignment, etc. Managers can also assign roles to users. (This role is available on VxPro Systems only.)
- **Supervisor** has advanced access to live and recorded video including investigations, PTZ control, and plug-ins. Supervisors can use plug-ins, configure events, and access workspaces configured by other users. (This role is available on VxPro Systems only.)
- **User** has basic rights to view live and recorded video. (This role is available on VxPro Systems only.)

Custom roles can also be created and assigned to organizationally unique users. VideoXpert contains some hard-coded user accounts that are integral to the system. You cannot edit, disable, or delete these accounts, nor can you change roles or permissions for these users. However, you can change the password for these accounts and Pelco strongly recommends that you change the “admin” password from the default. The “rule_engine” and “snmp” account passwords are randomly generated and Pelco only recommends changing these passwords in cases where a known password is required. VideoXpert asserts this by enforcing default password changes upon initial configuration of the VMS components. These hard-coded accounts are listed in the table, below.

User	Description
admin	This is the basic administrative user for VideoXpert. This user account possesses the “administrator” role, so is granted all available permissions within the system.
rule_engine	This role supports the rules engine.
snmp	This role is used to collect diagnostic information for the SNMP service that is available on the product.

For further instruction on how to manage users and roles within VideoXpert, please see the current version of the applicable VideoXpert operations manual.

Following Additional Least Privilege Best Practices

Using Separate Accounts for Privileged Functions

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 administrator may also be a basic user for day to day function. A separate user account could be used for basic rights to view live and recorded video. Apply this same concept to Windows accounts- Users with administrative privileges should have separate accounts for administrative duties and normal operational tasks.

Preventing Privilege Escalation

To prevent privilege escalation within the OS environment, Pelco recommends that you run administrative tasks and processes “separately” or “individually” when logged into a non-privileged Windows account—as opposed to logging in to the operating system with a privileged account to run all administrative functions. In the latter scenario, if a privileged account is compromised when the administrator is logged in, the malicious actor would then be granted privileged access to the entire system.

Performing Account Reviews

A process that can greatly reinforce the Least Privilege best practices can entail conducting regular account reviews of all users (privileged and non-privileged). This also helps prevent users who change roles or job duties from accumulating permissions that they no longer require.

Configuring for Least Functionality on VideoXpert Systems

The principle of least functionality states that systems are configured to provide only essential capabilities and to prohibit or restrict the use of non-essential functions, such as ports, protocols, and/or services that are not integral to the operation of that system. Pelco strongly recommends that you evaluate which services are currently running, and determine which are unnecessary and can be disabled. The overarching goal of least functionality is to reduce the attack surface within a given environment. It is best practice to maintain VideoXpert as a dedicated system by only allowing it to be used as a VMS.

Minimizing the Use of Essential Protocols, Ports, and Services

To apply least functionality for VideoXpert, start with the PPS tables provided within the Network section of this guide (as a baseline for essential Pelco VMS services). See *Configuring the Network Protocols, Ports, and Services (PPS)*. Disable any services you deemed unessential to the system’s intended purpose. If SNMP is needed, SNMPv3 (as used in the optional VxSNMP Agent) supports authentication and encryption.

Minimizing Essential Roles and Features

Another vital area to assess when implementing least functionality is the removal of any Windows Roles and Features that are not required for the environment. “Roles” refer to the roles that your device can play on your network - roles including a file server, a web server, or a DHCP or DNS server. “Features” refer to additional capabilities of the Windows operating system itself, for example: .NET Framework or Windows Backup. To manage these settings, search for and open either *Server Manager* or *Turn Windows features on or off*.

Windows Features and Roles can easily and efficiently be enabled/disabled by running Command Prompt ("cmd.exe") as administrator and executing one of the following commands:

- DISM /online /disable-feature /featurename:NameOfRoleOrFeature
- DISM /online /enable-feature /featurename:NameOfRoleOrFeature

A system restart may be required after all changes are applied.

The following is a list of recommended roles and features to be disabled on any VideoXpert system (due to know exploits and weaknesses):

- IIS-WebServerRole
- IIS-HostableWebCore
- TelnetClient
- TFTP
- SimpleTCP
- IIS-FTPServer
- FaxServiceConfigRole
- FaxServiceRole
- P2P-PnrpOnly
- MicrosoftWindowsPowerShellV2Root
- MicrosoftWindowsPowerShellV2
- SMB1Protocol

Pelco recommends that the following minimum/baseline roles and features be enabled on VideoXpert systems.

- For client systems:
  - SearchEngine-Client-Package
  - NetFx4-AdvSrvs
  - ServicesForNFS-ClientOnly
  - ClientForNFS-Infrastructure
  - NFS-Administration
  - Internet-Explorer-Optional-amd64
  - WorkFolders-Client
  - Microsoft-Windows-NetFx3-OC-Package
  - Microsoft-Windows-NetFx4-US-OC-Package
  - Microsoft-Windows-Client-EmbeddedExp-Package
  - Microsoft-Windows-NetFx3-WCF-OC-Package
  - Microsoft-Windows-NetFx4-WCF-US-OC-Package
- For servers:
  - NetFx4ServerFeatures
  - NetFx4
  - MicrosoftWindowsPowerShellRoot
  - MicrosoftWindowsPowerShell
  - KeyDistributionService-PSH-Cmdlets
  - TlsSessionTicketKey-PSH-Cmdlets
  - Tpm-PSH-Cmdlets
  - Server-Psh-Cmdlets

- MicrosoftWindowsPowerShellISE
- ServerCore-WOW64
- ServerCore-EA-IME-WOW64
- Server-Shell
- Internet-Explorer-Optional-amd64
- Server-Gui-Mgmt
- Windows-Defender-Gui
- Microsoft-Windows-Client-EmbeddedExp-Package
- ServicesForNFS-ServerAndClient
- ServerForNFS-Infrastructure
- ClientForNFS-Infrastructure
- Windows-Defender-Features
- Windows-Defender
- ServerCore-EA-IME
- Server-Drivers-General
- SearchEngine-Client-Package
- FileAndStorage-Services
- Storage-Services
- File-Services
- CoreFileServer
- ServerCore-Drivers-General
- ServerCore-Drivers-General-WOW64

Proper account management can similarly promote your stance on least functionality. Just as it is sensible to change default passwords on built-in accounts, it is equally important to disable any unused accounts. Built-in Windows accounts, specifically the default “Administrator” and “Guest” accounts, should also be disabled and renamed. Separate and unique administrator or guest accounts should be created instead. Again, regular account reviews can help reinforce these concepts.

Configuring for Interoperability

Certain considerations should be made when commissioning cameras and accessories (such as encoders) in VideoXpert. Refer to the product user and admin guides for configuring VideoXpert and cameras to work together. Pelco recommends that you only commission devices that have authentication enforced. For further instruction on hardening cameras, please refer to the current version of the *Pelco Camera Hardening Guide*.

Adding Access Controls

Access control is a fundamental component of security that dictates who can access and use certain information and resources. These policies make sure users are who they say they are, and that they have the appropriate level of availability to an organization's assets. In fact, the practice of access control is so imperative to maintaining an effective security program that, in many ways, a significant number of other concepts and principles covered in this guide can also be associated with implementing proper access control methods. Although this guide focuses primarily on technical/logical means for system hardening, physical security controls can also be quite effective in limiting access to valued resources.

Isolating the Network

Numerous precautions can be taken when it comes to the general configuration of access controls. The include firewalls, user rights assignment/group policy, and file system permissions; and can also include techniques to segment or isolate the network in order to control access to the servers, clients, and applications. Many organizations prefer to keep their video network isolated from their IT network in order to support the principle of separation of duties.

With modern converged IP networks, it is often possible to emulate network isolation with Virtual Local Area Network (VLAN) and network-based access control lists. It is a good practice to maintain VLAN separation for the VMS network, and to control access to surveillance assets. Again, to consult with your network vendor for implementation of this solution.

Using Windows Firewall

Use firewalls to limit or filter internal and external network communication between servers, client computers, along with programs and their associated services. Pelco highly recommends layering your security through a combination of both network-based and host-based firewalls, to achieve a "Defense-in-Depth" approach. Although there are a myriad of options for firewall solutions, this guide focuses primarily on Windows Firewall (a host-based firewall solution) because it comes standard on Windows operating systems. Certainly, other host-based firewall solutions can be used in combination with a network-based firewall, depending on your specific organizational needs and IT infrastructure.

To manage Windows Firewall through local group policy, run the *Local Group Policy Editor* (“gpedit.msc”) and navigating to **Computer Configuration** > **Windows Settings** > **Security Settings** > **Windows Defender Firewall with Advanced Security**. From here, most of your configuration options can be found in the right panel.

Here are some general recommendations when configuring Windows Firewall:

- First and foremost, ensure that the *Firewall state* for each profile (*Domain*, *Private*, and *Public*) is turned on. This can be modified under *Windows Defender Firewall Properties* within the group policy location stated above.
- Unsolicited inbound connections, for which there is no rule allowing the connection, should be blocked within each profile. Create custom inbound rules for authorized traffic. Instructions on how to apply VideoXpert specific rules are provided below, following these recommendations.
- Outbound connections should be allowed unless a rule explicitly blocks the connection. This allows normal outbound communication, which could be restricted as necessary with additional rules.
- Inbound and outbound rules can be defined by program, port, predefined rule templates, or a custom rule which can be based upon a combination of factors (program, service, port/ protocol). Assess what traffic you require in addition to VideoXpert, and create rules as necessary.
- Local firewall rules should not be merged with Group Policy settings on a public network. This prevents Group Policy settings from being changed by non-privileged or unauthorized users. Under *Windows Defender Firewall Properties*, this can be set by clicking **Customize** next to *Settings*. Click **No** for both rule merging drop down menus and repeat for each profile tab.
- Proper logging for Windows Firewall should also be configured. Click **Customize** next to *Logging* within the *Windows Defender Firewall Properties* window. Enable logging and repeat for each profile tab.

Importing VideoXpert Firewall Rules

Export VideoXpert rules required for VMS functionality from the local firewall policy, then import them into a Group Policy.

1. With VideoXpert installed, open the local Windows Firewall management console (run “wf.msc”) and click **Inbound Rules** in the left panel.
2. Highlight all of the VideoXpert rule names that are present and right-click to select **Copy**.
3. Open the *Local Group Policy Editor* (“gpedit.msc”) and navigate to **Computer Configuration** > **Windows Settings** > **Security Settings** > **Windows Defender Firewall with Advanced Security** > **Inbound Rules**.
4. In the *Inbound Rules* panel, right-click and select **Paste**. The appropriate VideoXpert firewall rules are imported into Group Policy.

Note: By using this import method, you can avoid having to use the above provided VideoXpert PPS tables to manually create VideoXpert specific rules in Windows Firewall.

Using Additional Group Policy Settings

While making changes within the *Local Group Policy Editor*, additional access control recommendations include reviewing the settings within *User Rights Assignment*, *Account Lockout Policy*, and the *User Account Control* settings under *Security Options*.

Configuring User Rights Assignment

Open the *Local Group Policy Editor* (“gpedit.msc”), and then navigate to **Computer Configuration** > **Windows Settings** > **Security Settings** > **Local Policies** > **User Rights Assignment**. Review the settings and ensure that they align with your organization’s standards. Best practice configurations include:

- Configure the policy value for *Access this computer from the network* to only include the **Administrators** and **Authenticated Users** groups.
- Configure the policy value for *Allow log on locally* to only include the **Administrators** and **Users** groups.
- Configure the *Deny access to this computer from the network* and *Deny log on through Remote Desktop Services* user rights to prevent access from unauthenticated users, such as the **Guest** group.
- Configure the *Deny log on as a batch job*, *Deny log on as a service*, and *Deny log on locally* user rights to prevent access from highly privileged domain accounts (**Enterprise Admins** and **Domain Admins** groups) on domain systems and from unauthenticated access (**Guest** group) on all systems.

Configuring the Account Lockout Policy

After you configure User Rights Assignment (see the section titled *Configuring User Rights Assignment*), while still in the *Local Group Policy Editor* window, navigate to **Computer Configuration** > **Windows Settings** > **Security Settings** > **Account Policies** > **Account Lockout Policy**. Prior to making changes, refer to your organization’s Account Management Plan for account lockout policies. General recommendations for these settings include:

- Configure the policy value for *Account lockout threshold*. Anywhere between 3-5 successive failed attempts is a reasonable threshold.
- After this setting is configured, default values for *Account lockout duration* and *Reset account lockout counter after* are set to 30 minutes. Ordinarily, 15 to 30 minutes is a rational duration for these policies.

Note: Ensure that steps are taken and procedures are in place to prevent a denial of service from a system lockout. Having a backup/alternate administrator to unlock application or system accounts is one approach for avoiding loss of availability to resources due to lockout.

Configuring Security Options

To configure *User Account Control* settings, navigate to **Computer Configuration** > **Windows Settings** > **Security Settings** > **Local Policies** > **Security Options**. Review the policy settings and ensure that they align with organizational policy. Commonly, the default Windows settings suffice.

Under *Security Options* verify that the value for *Interactive logon: Machine inactivity limit* is configured and meets your organization's policy standards. As an industry standard, this is typically set somewhere around 15 minutes (900 seconds) for non-privileged users and 10 minutes (600 seconds) for privileged users. Avoid a value of "0", because this will cause a denial of service.

Configuring File System Permissions

Though relating to the previously discussed topic of least privilege, note that in order to maintain an effective posture on access control, the review of folder permissions and their inheritance attributes to subsequent files/folders is also crucial to maintaining a secure baseline. This is especially important for areas in your file system that contain sensitive information (for example: PII or confidential/proprietary data), system critical files, configuration files, and audit logs.

Verify these permissions in File Explorer. To do so:

1. Right click on the appropriate folder, and then click **Properties**.
2. Click the "**Security** tab.
3. Click **Advanced**.
4. Review and modify various parameters for permissions on that folder and any objects it contains.

Note: One benefit of implementing a role-based permissions scheme in Windows is that it can simplify certain account management tasks, which includes verifying user permissions on items such as your file system. Tracking the role(s) assigned to each group and managing which accounts are assigned to those groups is a far more effective and efficient approach than having to manage and track separate permissions for individual users. In other words, assigning file or folder permissions by individual user instead of by group can lead to a daunting endeavor when it comes time for an account review. This method also simplifies managing and tracking which actions or processes a user can invoke. For example, imagine having to review all permissions in the *Local Group Policy Editor* if the values on every setting also contained individual users instead of groups.

Access control covers a wide range of topics concerning security. The primary goal to keep in mind is to provide reliable access to those that are authorized, and at the same time, restricting access to those that are not.

Considering Additional Security Controls

The following additional security controls are considered supplements to baseline VideoXpert hardening. Refer to any relevant local policy or guidance before applying any of the proceeding controls, because their implementation requires organizationally specific decisions to be made based on the unique environment.

Using a Host Based Security System (HBSS)

In addition to providing a device whitelisting solution (as mentioned earlier), HBSS delivers value through a full range of other endpoint protection capabilities. A few of these core features include: antivirus, a host intrusion prevention system (HIPS), data loss prevention (DLP), file integrity monitoring (FIM), and policy auditing.

Using an Antivirus Agent

Malicious software can establish a base on individual desktops and servers. Employing an automated mechanism to detect this type of software will aid in elimination of the software from the operating system.

An antivirus agent is a critical tool for any device—designed to prevent, search for, detect, and remove software viruses, and other malicious software including worms, trojans, adware, and more. Ensure that your antivirus agent is up to date, because today's malicious software can change appearance in order to avoid being discovered. Moreover, Pelco highly recommends scheduling regular scans in order to assist with anything potentially missed from real-time malware detection.

Note: When installing antivirus software on a machine that is running VideoXpert software, the admin must exclude scanning from certain file types and locations, and certain network traffic. Without implementing these exceptions, antivirus scanning will use a considerable amount of system resources that impacts memory, hard drives, and CPU. Also, the scanning process can temporarily lock files which will likely result in a disruption in the recording process and/or database corruption. For specifics on these exclusions, please refer to our knowledge base article located at https://support.pelco.com/s/article/How-to-use-AntiVirus-Software-in-the-VxE-and-VxPro-Systems-1538586730289.

Using a Host Intrusion Prevention System (HIPS)

HIPS is an installed software package which monitors a single host for suspicious activity by analyzing events occurring within that host. In other words an HIPS aims to stop malware by monitoring the behavior of code. This makes it possible to help keep your system secure without depending on a specific threat definition to be added to a detection update.

Using Data Loss Prevention (DLP)

DLP is a strategy for making sure that end users do not send sensitive or critical information outside the private network. DLP uses custom rules to classify and protect confidential or critical information, so that unauthorized end users cannot accidentally or maliciously share data that , if disclosed, could put the organization at risk. This includes automated processes such as scanning outgoing emails and their attachments or blocking the use of removable media devices to protect against unauthorized sharing of sensitive information.

Using File Integrity Monitoring (FIM)

FIM is a technology that monitors and detects changes in files that may indicate a cyber-attack. As part of change control, file integrity monitoring involves examining files to see if and when they change, how they change, who changed them, and what can be done to restore those files if those modifications are unauthorized. The scope of files being monitored is defined at the organization's discretion. This is especially important for areas in your file system that contain sensitive information (for example: PII or confidential/proprietary data), system critical files, configuration files, and audit logs.

Using Policy Auditing

Policy Auditor is an agent-based IT audit solution that leverages the Security Content Automation Protocol (SCAP) to automate the processes required for tracking compliance with mandates such as: Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act of 1996 (HIPAA), and Federal Information Security Management Act of 2002 (FISMA). This tool can also assist in maintaining and monitoring any changes to your configuration baseline. Helping to ensure configurations are secure and align with organizational policy.

Using Audit Logging and Event Management

VideoXpert offers a built-in event logging feature specific to events occurring within the VMS. Refer to the current version of the *VideoXpert Toolbox Operations Manual* (for Enterprise systems) or the *VideoXpert Professional Operations Manual* (for VideoXpert Professional systems) for detailed instruction on how to configure and manage these events.

Using Log Collection

For a more holistic approach to event management, Pelco highly recommends that you enable logging for the system itself, and for any other installed applications. The Windows OS has a native feature for system level event logging known as Event Viewer. Run *Event Viewer* (“eventvwr.msc”) and verify that *System*, *Application*, and *Security* events are all enabled. This enables logging where possible. Proper implementation also includes regular reviews and analysis of logs collected, other maintenance activities relating to log retention policies, and offloading/backing up your audit logs.

Regular log reviews are important because sometimes logging records are the only evidence of a successful attack. Many organizations keep audit records for compliance purposes, but attackers rely on the fact that such organizations rarely look at the audit logs, and they do not know that their systems have been compromised. Because of poor or nonexistent log analysis processes, attackers sometimes control victim machines for months or years without anyone in the target organization knowing, even though the evidence of the attack has been recorded in unexamined log files.

Using Log Retention

Defining the retention period for logged events is an organizational decision; it should take into account any industry or government regulatory requirements concerning data retention with which the organization must stay in compliance. After a retention period is defined, ensure adequate disk space is allotted in order to accommodate these requirements.

Using Log Protection

Routinely backing up and offloading audit records helps ensure their protection from accidental loss or deletion, and from malicious manipulation that would compromise log integrity or availability.

Where possible, Pelco recommends that you offload log data in real time, or weekly if real time is not feasible (such as in the case of standalone systems).

Determining the Scope of an Event

When determining the scope of information to be logged, consider taking the following actions.

- Generate audit records for these events, whether successful or unsuccessful:
  - Access to security objects or configurations
  - Modified security objects or configurations
  - Logon/connection attempts
  - Logoffs/disconnect/session timeouts
  - Account management functions: create/read/update/delete/assign functions for users, organizationss, contact groups, roles/privileges, etc.
  - Access to confidential or sensitive data objects
  - Any privileged system functions
  - Alert on concurrent logons (Simultaneous logon sessions from the same account occurring on separate systems)
- Audit records should use a consistent format and contain sufficient information to facilitate troubleshooting and investigations, such as:
  - Timestamp
  - Event type
  - Event result (success/fail)

  - Originating IP/hostname
  - User ID or Device ID

Using Data Backup and Recovery

Backup and recovery describes the process of creating and storing copies of data that can be used to protect organizations against data loss. Recovery from a backup typically involves restoring the data to the original location, or to an alternate location where it can be used in place of the lost or damaged data. Data failures can be the result of hardware or software failure, data corruption, or a human-caused event, such as accidental deletion of data or a malicious attack (virus or malware). In recent years, ransomware has gained a strong presence in the cybersecurity threat landscape. This type of malicious attack is designed to extort money from a victim. Often, ransomware will demand a payment in order to undo changes that the malware has made to the victim's computer.

These changes can include:

- Encrypting data that is stored on the victim's disk – so the victim can no longer access the information.
- Blocking normal access to the victim's system.

Maintaining an adequate backup strategy can assist in alleviating the impact to an incident resulting in lost or corrupt data. At a fundamental level, a typical backup plan includes:

- What is being backed up (Give highest priority to crucial data.)
- Where backups are stored (Rotate a set of backups off-site, usually once a week.)
- How often backups will occur
- The type(s) of backups to be performed (ex. full, incremental, differential)
- The personnel responsible for performing backups
- The personnel responsible for monitoring the success of these backups (Test your backups before you need them.)

Configuring Data Execution Prevention (DEP)

DEP is a security feature that can help prevent damage to your computer from viruses and other security threats. Harmful programs try to attack Windows by attempting to run (also known as execute) code from system memory locations reserved for Windows and other authorized programs. These types of attacks can harm your programs and files.

DEP can help protect your computer by monitoring your programs to make sure that they use system memory safely. If DEP notices a program on your computer using memory incorrectly, it closes the program and notifies you.

To configure DEP:

1. Search for *View advanced system setting.*
2. Under *Performance*, click **Settings**.
3. Click the **Data Execution Prevention** tab, and then select *Turn on DEP for all programs and services except those I select*.
4. Add any programs to which you do not want DEP to apply (if any).

Following Operation and Maintenance Recommendations

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

- Stay up-to-date. 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 current with product lifecycles, and plan and coordinate upgrades.
- Maintain procedures to safeguard configuration backups and to restore a device from backups as necessary.
- Report potential product vulnerabilities through the web portal at https://www.pelco.com/report or by email at cybersecurity@pelco.com.

Pelco, Inc.
625 W. Alluvial, 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