AVIGILON™

Avigilon System Hardening Guide

For Avigilon Unity Video and Avigilon Control Center Systems

MOTOROLA SOLUTIONS

Copyright

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. Avigilon Corporation reserves the right to make any such changes without notice. Neither Avigilon 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. Avigilon Corporation shall not be responsible for any losses or damages (including consequential damages) caused by reliance on the information presented herein.

Avigilon Corporation
avigilon.com

PDF-HARDEN-UNITY

Revision: 1 - EN

20240207

Contents

Introduction

Hardening refers to configuring a video security system to be more secure and less susceptible to cyberattacks. Video security systems are a crucial aspect of securing a location but, they are also a prime target for hackers due to their ability to collect and store sensitive information.

This guide is intended to offer recommendations for hardening an AvigilonControl Center (ACC) System including the following components:

This guide is intended to offer recommendations for hardening an Avigilon Unity Video System or Avigilon Control Center (ACC) System including the following components:

- ACC Server(s)
- Unity Video or ACC Server(s)
- ACC Client(s)
- Unity Video or ACC Client(s)
- Avigilon or third-party devices

NOTE

Most of the instructions in this guide are common between Avigilon Unity Video Systems and ACC Systems. Common instructions will refer to Systems, Servers, and Clients, which imply that they are using one of these two Avigilon softwares. Differences between Unity Video and ACC will be called out where appropriate.

This guide references Security Technical Implementation Guidelines (STIGs) from the US Defense Information Systems Administration (DISA), Federal Information Processing Standards (FIPS), Center for Internet Security (CIS), the Internet Engineering Task Force (IETF), and the United States National Institute of Standards and Technology (NIST). It commonly references the "Security and Privacy Controls for Information Systems and Organizations" that are found at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

Secure Avigilon System Checklist

A hardened Avigilon System consists of three components. The following checklist provides the necessary steps needed to harden these components:

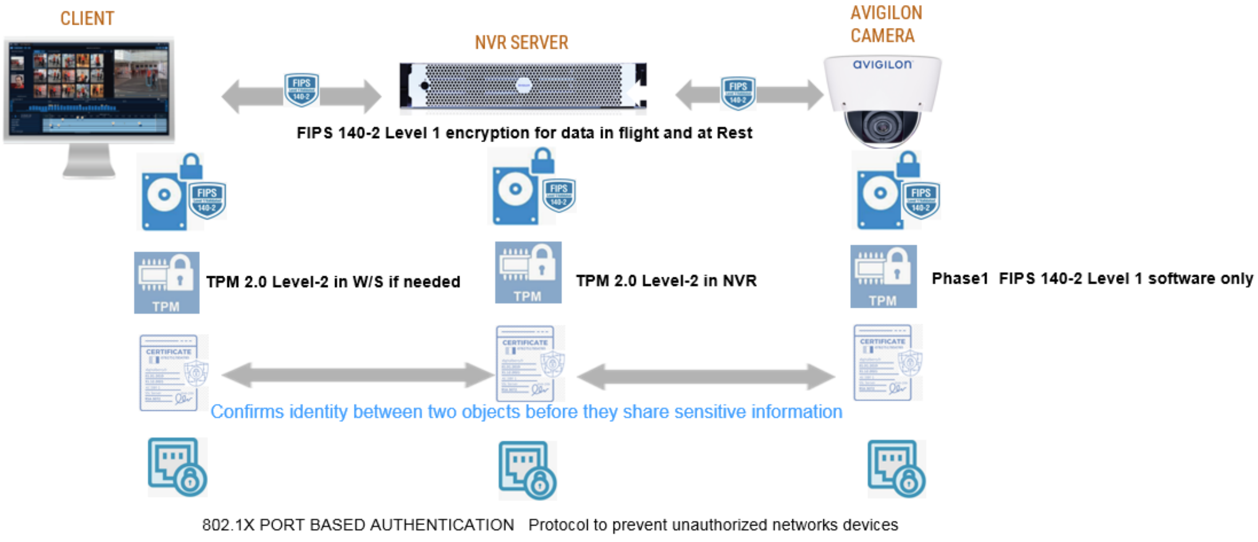
1. Avigilon NVR Premium FIPS Series recorder (see *Securing Servers* on page 26):
    - Deploy the NVR. Upon first boot, the system will enable BitLocker encryption and apply a new secure password to your administrator account. For more information, see the appropriate NVR Installation Guide, which can be found at help.avigilon.com.
    - Deploy and configure the Server.
    - Download the recovery image and the USB creation tool provided. Create a bootable USB key.
    - Back up the BitLocker recovery keys for both the OS and data volumes.
    - Disable the USB ports.
2. Avigilon Secure cameras (see *Securing Devices* on page 52):
    - Install and setup the camera.
    - Create a strong and complex password for the camera's administrator account.
    - Upgrade the camera to the latest firmware.
    - Set up a trusted CA-signed certificate. For more information, see *Enabling Video Stream Encryption* on page 57.
    - Enable FIPS 140-2 encryption. For more information, see *Enabling FIPS 140-2 Camera Communications* on page 54.
3. Unity Video or ACC Clients (see *Securing Avigilon Remote Workstations* on page 63):
    - Set up a trusted CA-signed certificate on the Server and Clients. For more information, see *Securing Network Communications* on page 38.
    - Enable FIPS 140-2 encryption for server and client communications. For more information, see *Configuring FIPS Compliance* on page 45.
    - Enable WAN (secure) communications between the server and cameras and between clients and servers. For more information, see *Encrypting Video* on page 50.

Video Security System Data Flow

The Avigilon System is an end-to-end solution, meaning it runs with Avigilon FIPS-enabled cameras and NVR Premium FIPS Series recorders. Workstations are optional. If you will be using workstations, we recommend that you purchase Avigilon Remote Monitoring workstations and follow the instructions provided in this guide to harden your workstations.

The typical data flow of the a video security system can be broken down in the following steps:

1. Video is captured by the camera.
2. Video data is streamed over the network to the recording Server.
3. Video data is stored by the recording Server.
4. Video data is backed up to an archive System.
5. Live and recorded video is streamed to the Client.
6. Recorded video is exported by the Client.


CLIENT
NVR SERVER
AVIGILON CAMERA
avigilon
FIPS 140-2
FIPS 140-2 Level 1 encryption for data in flight and at Rest
TPM
TPM 2.0 Level-2 in W/S if needed
TPM 2.0 Level-2 in NVR
Phase1 FIPS 140-2 Level 1 software only
CERTIFICATE
Confirms identity between two objects before they share sensitive information
802.1X PORT BASED AUTHENTICATION Protocol to prevent unauthorized networks devices

Cyber Risk Management Overview

Avigilon recommends that you apply the Cyber-Kill Chain and Cyber Risk Management Framework explained below to your System. Understanding these concepts will give a contextual understanding of how and why cyber attackers access vulnerable Systems, and steps you can take to prevent them from doing so.

Cyber-Kill Chain

The cyber-kill chain was developed by Lockheed Martin to outline the steps that a typical cyber attacker takes to carry out their attack successfully. The cyber-kill chain is made up of seven stages that the attacker takes to achieve their objectives, which are typically to gain unauthorized access to a System, steal information, or disrupt System operations. The seven stages of the cyber-kill chain are as follows:

1. **Reconnaissance**: Just like burglars and thieves, cyber attackers need to plan their attacks. They research, identify and select their targets, often using phishing tactics or by extracting public information from an employee's LinkedIn profile or corporate website. These attackers also scan for network vulnerabilities and services or applications they can exploit.
2. **Weaponization**: Once the attacker has identified a target System, they develop a weapon, which is typically a piece of malware, that can exploit the vulnerabilities they've discovered in the reconnaissance stage.
3. **Delivery**: After the weapon has been developed, the attacker needs to deliver it to the target System. Various delivery methods could be used, including email attachments, phishing emails, or social engineering attacks.
4. **Exploitation**: Once attackers gain access to an organization, they can activate attack code on the victim's host and take control of the target machine.
5. **Installation**: Attackers will seek to establish privileged operations, root kit, escalate privileges, and establish persistence.
6. **Command-and-Control**: Attackers establish a command channel back through the Internet to a specific Server so they can communicate and pass data back and forth between infected devices and their Server.
7. **Actions on the Objective**: Attackers may have many different motivations for attack, and it's not always for profit. Their reasons could be data exfiltration, destruction of critical infrastructure, or to deface web property or create fear/extortion.

Understanding the cyber-kill chain is essential for security professionals, as it allows them to detect and mitigate attacks at various stages before they are successful. By breaking down and analyzing each stage of the cyber-kill chain, security professionals can develop effective security controls and strategies to safeguard their networks and Systems from sophisticated cyber threats.

For more information

The following documents can provide additional guidance:

- lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

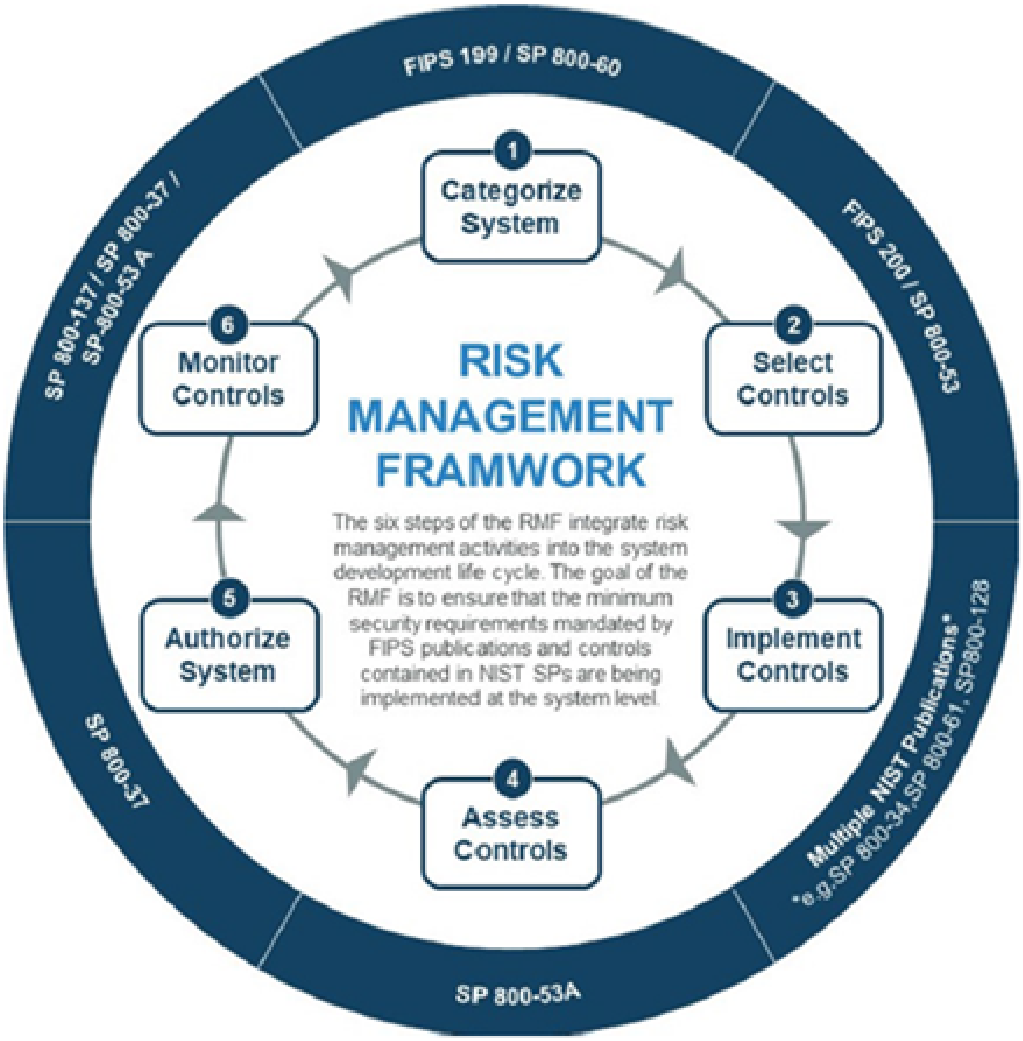
Cyber Risk Management Framework

The Cyber Risk Management Framework is an adaptable set of guidelines that organizations can use to iteratively manage and mitigate cybersecurity risks. Its goal is to help organizations maintain the security authorization of the information System over time in a highly dynamic operating environment.

The primary document describing the Cyber Risk Management Framework is the NIST Special Publication (SP) 800-37 Revision 2, which is available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf.

The Cyber Risk Management Framework is based on six core functions as documented in this publication:

1. **Categorization of information Systems** (identification of risk level). An administrative step that involves understanding the organization and defining System boundaries. Based on the System boundaries, all information types associated with the System should be identified. Relevant information may include the organization's mission, roles and responsibilities, operating environent, intended use, and connections with other Systems.
2. **Selection of security and privacy controls**. These controls are the management, operational, and technical safeguards or countermeasures employed within an organizational information System. They help to protect the confidentiality, integrity, and availability of the System and its information.
3. **Implementation of security and privacy controls**. Requires the implementation of the controls selected in step 2, and should describe how the controls are employed within the information System and its environment of operation.
4. **Assessment of the effectiveness of security controls**. Use appropriate assessment procedures to determine the extent that the controls are correctly implemented, operating as intended, and producing the desired outcome, as defined in the security requirements.
5. **Authorize the information System**. Create an Authority to Operate (ATO). Authorization is based on a determination of the risk to organizational operations, and individuals, assets, other organizations, and the nation that would result from the operation of the information System. If the previous steps were adequate and successful, this would lead to the decision that the risk is acceptable.
6. **Monitoring and evaluating security controls through iterations**. Continuous monitoring programs should be used to allow the organization to maintain the security authorization of the information System over time in a highly dynamic operating System, where Systems adapt to changing threats, vulnerabilities, technologies, and mission/business processes.


FIPS 199 / SP 800-60
FIPS 200 / SP 800-53
Multiple NIST Publications*
*e.g.SP 800-34,SP 800-61, SP800-128
SP 800-53A
SP 800-37
SP 800-137 / SP 800-37 / SP-800-53 A
1 Categorize System
2 Select Controls
3 Implement Controls
4 Assess Controls
5 Authorize System
6 Monitor Controls
RISK MANAGEMENT FRAMWORK
The six steps of the RMF integrate risk management activities into the system development life cycle. The goal of the RMF is to ensure that the minimum security requirements mandated by FIPS publications and controls contained in NIST SPs are being implemented at the system level.

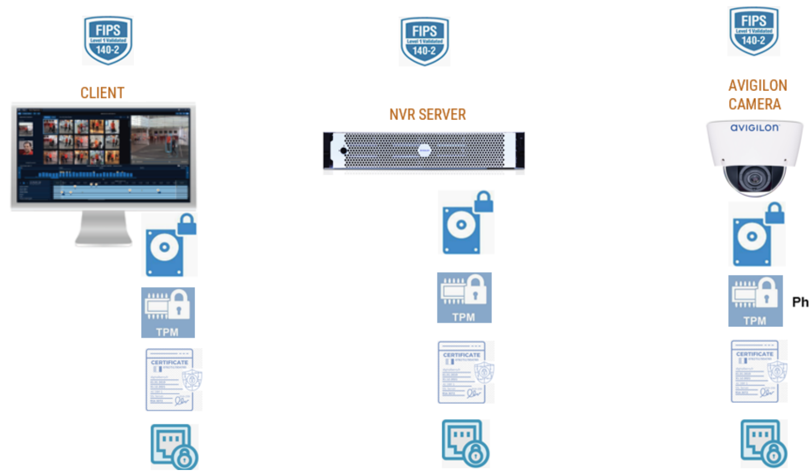
Start the RMF process as descibed in step 1. Your selection of security and privacy controls (step 2) will depend on what is found during step 1.

Avigilon provides an out-of-the-box solution baseline, as described in this Hardening Guide, on how to implement the security controls for unclassified information. We have performed Nessus and STIGs scans for our solutions, and will provide documentation on our scan results upon request.

General Guidelines

Avigilon recommends the following actions to secure your System, and lists their corresponding control tasks from NIST SP 800-53 Revision 5. It's important to note that these guidelines are just a starting point and should be evaluated based on the specific needs and risks of the Avigilon video security System being secured.

Action	Control Task
Establish baseline configurations for the System	CM-2 (Baseline Configurations)
Implement security-related System configuration settings	CM-6 (Configuration Settings)
Enforce secure password policies	AC-2 (Account Management)
Identify and authenticate System users	IA-2 (Identification and Authentication)
Log and track changes to System configurations	CM-3 (Configuration Change Control)
Monitor System activity for security events	AU-2 (Audit Events)
Collect and analyze audit information to detect inappropriate activity	AU-12 (Audit Generation)
Monitor physical access to System components	PE-6 (Monitoring Physical Access)
Implement access controls to limit access to authorized individuals	AC-2 (Account Management) AC-3 (Access Enforcement) AC-6 (Least Privilege)
Use multifactor authentication for remote access	AC-17 (Remote Access)
Control user access to information flow within the System	AC-4 (Information Flow Enforcement) AC-3 (Access Enforcement)
Control wireless access to the System	AC-18 (Wireless Access)
Control access to portable and mobile devices	AC-19 (Access Control for Portable and Mobile Devices)
Implement cryptographic key establishment and management controls	SC-12 (Cryptographic Key Establishment and Management)



Phase1 FIPS 140-2 Level 1 software only

Establishing a Security Plan

By establishing security objectives and creating a strong security policy, you will be able to protect your System from potential attacks and keep your organization and its assets safe.

The first step towards establishing a security plan is to identify your security objectives. Start by assessing the scope and reach of your surveillance System. Think about what information you want to protect and what potential risks exist for your System.

Some common security objectives include maintaining the confidentiality, integrity, and availability of your System, restricting access to authorized users, preventing unauthorized changes to System configurations, and ensuring data backup and recovery mechanisms are in place. Once you have identified your objectives, it is important to involve all stakeholders in the security plan development process. This includes security personnel, IT staff, business units, and any other relevant parties. Communication is vital in developing an effective security plan, and all stakeholders should be aware of the goals and objectives of the plan.

The next step is to create an effective security policy. This should be based on your security objectives and take into consideration any regulations or compliance standards that apply to your System. A solid security policy will provide the framework for protecting your organization from potential security breaches as outlined in *Cyber Risk Management Overview* on page 8.

Refer to nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.pdf for guidance on meeting your policy requirements.

NOTE

Tools such as the Microsoft Security Configuration Manager (SCCM) with the Security Content Automation Protocol (SCAP) can be utilized to automate parts of the security policy.

Adhering to Security Standards

As part of your security plan, Avigilon recommends aligning your security System with the guidance available from the following sources.

National Institute of Standards and Technology Guides

The National Institute of Standards and Technology (NIST) is responsible for developing standards and guidelines, including minimum requirements, and for providing adequate information security for all agency operations and assets. Their guidelines have been prepared for use by federal agencies, but may also be used by nongovernmental organizations on a voluntary basis and are not subject to copyright regulations.

Their publications can be found on their website www.nist.gov/publications. These documents in particular will be helpful when hardening your System:

- NIST SP 800-53 Rev 5: nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
- NIST SP 800-128: nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-128.pdf
- NIST SP 800-41 Rev 1 (specific to firewalls): nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf

CISA's Industrial Control Systems Standards and References

The Cybersecurity & Infrastructure Security Angency (CISA) offers several products and services that assist in cybersecurity risk management efforts.

Their recommendations can be found in the ICS-CERT Standards and References (general list): www.us-cert.gov/ics.

Use a FIPS-Certified Cryptographic Library

Avigilon recommends that you use a Federal Information Processing Standard (FIPS) 140-2 certified cryptographic software library to encrypt all in-transit data for your Avigilon software between Server and Clients. In the Avigilon software, you have the option to select the level of FIPS 140-2 compliance. Select the **Strict** setting to ensure your security System's communications are secure.

The FIPS 140-2 publication can be found at nvlpubs.nist.gov/nistpubs/fips/nist.fips.140-2.pdf.

The following NIST documentation can provide further information:

- NIST SP 800-53 SI-7: Software, Firmware, and Information Security
- NIST SP 800-53 IA-7: Cryptographic Module Authentication
- NIST SP 800-53 SC-8: Transmission Confidentiality and Integrity
- NIST SP 800-53 SC-12: Cryptographic Key Establishment and Management
- NIST SP 800-53 SC-13: Cryptographic Protection

Microsoft Security Update Guide

The Microsoft Security Response Center (MSRC) investigates all reports of security vulnerabilities affecting Microsoft products and services, and releases these documents as part of the ongoing effort to help you manage security risks and help keep your Systems protected.

Their recommendations can be found in the Microsoft Security Update Guide (docs.microsoft.com/en-us/security-updates).

Updating the System Components

Avigilon recommends that you keep your operating System, software and firmware up-to-date in your System. Security patches and updates are released regularly to address vulnerabilities and improve System performance. Failure to install these updates could leave the System more vulnerable to cyber attacks or malfunctions that could compromise the integrity of the surveillance System.

Updating Windows

Avigilon recommends that you install the latest Windows Updates on all System components (Servers, recorders, and workstations). Avigilon NVR Premium FIPS Series recorders are Windows-based, so installing security updates from Windows Update is critical.

Updates often include bug fixes, stability improvements, and new features that could benefit the System's performance. For example, an update that improves video encoding or decoding capabilities could lead to better video quality or smoother playback.

CAUTION

Updating Windows requires the System to be restarted, which can cause interruptions to the System. To avoid these interruptions, it is important to plan maintenance tasks during off-peak hours or schedule automatic updates during times when the System is least active. It is also important to ensure that the System is properly shut down and restarted, as failing to do so could result in file corruption or other issues that could affect System stability. Avigilon recommends that you verify updates in a test environment before updating your System.

For more information

The following documents can provide additional guidance:

- NIST SP 800-53 SI-2: Flaw Remediation
- NIST SP 800-53 CM-8: System Component Inventory

Updating Software and Device Firmware

Avigilon recommends that you use the latest software and device firmware. This ensures that you get all released security updates and bug fixes. You can use the Camera Configuration Tool, the Avigilon Client, or the Camera Web Interface to upgrade your devices.

Updates can be found at avigilon.com/support.

NOTE

Before upgrading firmware, read the upgrade instructions in the appropriate device Camera Web Interface Guide, which can be found at help.avigilon.com.

Protecting Your System with Anti-virus Software

Avigilon recommends that you use anti-virus software on all components possible in your System. Using antivirus software on a System is essential to protect the System from malware, viruses, and other threats.

To avoid degraded System performance during virus scanning, Avigilon recommends that you follow these guidelines when setting up the files and directories to scan on your Server and failover Server.

> **IMPORTANT**
>
> Adding folders and EXE files to the exclusion list of the anti-virus software can have implications to your IT security.
> You may want to set up a maintenance window where you can scan programs for malware. Consult your IT security administrator.

Depending on the anti-virus software you are using, the procedure to exclude files and folders will be different. Exclude the following locations from being automatically scanned by your anti-virus software:

- `AvigilonData` folders, which are located on each of the Avigilon data volumes (Primary and Secondary volumes).
- `AvigilonConfig` folders, which are located on each of the Avigilon Config volumes.
- Program Files, located at `C:\Program Files\Avigilon`.

Some anti-virus software packages come with live process scanning or incorporated firewalls, which may cause communication failures between cameras and Servers, or between Servers and Clients. To prevent this, exclude the following applications and folders from being scanned.

Server Applications

Software	Folder Filepath	Applications to exclude
ACC	`C:\Program Files\Avigilon\Avigilon Control Center Server\`	• `VmsAdminPanel.exe` • `VmsAdminPanelLauncher.exe` • `VmsDaemonService.exe` • `LprDaemonApp.exe` (if installed) • `%programdata%/avigilon` This is usually `C:\ProgramData\Avigilon` (entire folder)
Unity Video	`C:\Program Files\Avigilon\Avigilon Unity Server\`	

Analytics Service

Software	Folder Filepath	Applications to exclude
ACC	`C:\Program Files\Avigilon\Avigilon Control Center Analytics Service\`	• `AnalyticsDaemonService.exe`
Unity Video	`C:\Program Files\Avigilon\Avigilon Unity Analytics Service\`	

Client and Virtual Matrix Application

Software	Folder Filepath	Applications to exclude
ACC	`C:\Program Files\Avigilon\Avigilon Control Center Client\`	- `VmsClientApp.exe`
Unity Video	`C:\Program Files\Avigilon\Avigilon Unity Client\`	

Virtual Matrix Application

Software	Folder Filepath	Applications to exclude
ACC	`C:\Program Files\Avigilon\Avigilon Control Center Virtual Matrix\`	- `VmsVirtualMatrixApp.exe`
Unity Video	`C:\Program Files\Avigilon\Avigilon Unity Virtual Matrix\`	

Gateway Application

Software	Folder Filepath	Applications to exclude
ACC	`C:\Program Files\Avigilon\Avigilon Control Center Gateway\`	- `VmsWebGateway.exe`
Unity Video	`C:\Program Files\Avigilon\Avigilon Unity Gateway\`	

Web Endpoint Application

Software	Folder Filepath	Applications to exclude
ACC	`C:\Program Files\Avigilon\Avigilon Control Center Web Endpoint\`	- `WebEndpointService.exe`
Unity Video	`C:\Program Files\Avigilon\Avigilon Unity Web Endpoint\`	

Avigilon Player Application

Software	Folder Filepath	Applications to exclude
ACC	64-bit version: `C:\Program Files\Avigilon\Avigilon Player\VmsPlayerApp.exe` 32-bit version: `C:\Program Files (x86)\Avigilon\Avigilon Control Center Player\VmsPlayerApp.exe`	- `VmsPlayerApp.exe`
Unity Video	64-bit version: `C:\Program Files\Avigilon\Avigilon Player\` 32-bit version: `C:\Program Files`	

```
(x86)\Avigilon\Avigilon Unity
Player\VmsPlayerApp.exe
```

For more information

The following documents can provide additional guidance:

- NIST SP 800-53 PL-8: Security and Privacy Architecture
- NIST SP 800-53 SI-2: Flaw Remediation
- NIST SP 800-53 SI-3: Malicious Code Protection
- NIST SP 800-53 SI-4: System Monitoring

Securing User Accounts

Avigilon recommends that you take steps to secure the accounts that are used to access your System components. Complete the following steps to create strong passwords for your accounts and to create group policies for account management.

Using Strong Passwords

Use strong passwords in your System to maintain confidentiality and prevent unauthorized access. Strong passwords are designed to be complex and difficult to guess, whereas weak ones make the System vulnerable to attacks. A strong password should be at least 14 character requirement, using a mix of upper and lower cases, numerals, and special characters.

Enforce strong password policies and regularly remind users to create secure passwords and change them every few months.

For more information

The following documents can provide additional guidance:

- STIG V-73229 from Windows Server 2016 STIG, V1R12
- STIG V-205661 from Windows Server 2019 STIG, V2R4
- NIST 800-53 IA-5: Authenticator Management
- NIST 800-53 IA-6: Authenticator Feedback
- NIST 800-53 SI-11: Error Handling

Securing Server User Accounts

There are three types of user accounts that you can use with your System:

- **Windows user**: A Windows User account in an Active Directory provides full administrative access to the System. The user can install new programs, manage System settings, and make System-wide changes. Windows users can be authenticated through the Active directory as a single authoritative source and enterprise service for the network as opposed to being authenticated through their local machine. This allows you to use role-based access controls and assign permissions to users and groups consistently across the domain and devices on the network.

- **Basic user**: A basic user account managed individually or in a Windows Workgroup provides limited administrative access to System settings and permissions. Basic users cannot install new programs or make any System-wide changes.

- **Network service**: Network service accounts interact with the network and perform tasks such as accessing files and connecting to databases, without having access to the Windows graphical user interface or other resources that may not be required for the service to operate. These accounts are created to provide a secure way for services to interact with the network and other resources without compromising System security. See *Running Software as a Network Service* on page 46 for more information.

After determining the user accounts your System requires, consider grouping them based on their function or the privileges they are assigned. Grouping user accounts allows for management through Active Directory or a Windows Workgroup, and subnets can be created for each group to connect to the Server separately. See *Managing Subnets* on page 47 for more information.

For more information

The following documents can provide additional guidance:

- NIST SP 800-53 CM-6: Configuration Settings
- NIST SP 800-53 SA-5: System Documentation
- NIST SP 800-53 SA-8: Security and Privacy Engineering Principles

Active Directory

There are two types of supported deployments of the System: **Joining an Active Directory** or **Creating a Standalone Peer-to-peer Windows Workgroup environment**. The difference between the two lies in their purpose, functionality, and security. Active Directory provides centralized management and control over user accounts, resources, and security policies, whereas Workgroup environments are self-managed and require manual configuration on each computer.

- **Joining an Active Directory**. Active Directory is a service provided by Microsoft Windows that acts as a centralized directory service, used to manage resources and users within a network. Avigilon recommends that you use Windows users in combination with an Active Directory to authorize access to the System. Active Directory provides a hierarchical structure for managing and organizing resources and users in a network. Joining a computer to an active directory allows for centralized management of user accounts, permissions, and security policies.

  Active Directory also provides additional features such as Group Policy management, which allows for easier configuration of settings like security policies and application settings throughout the network.

- **Create a Standalone Peer-to-peer Windows Workgroup environment**. Creating a standalone peer-to-peer Windows Workgroup environment is typically done in a smaller environment or home network, but not exclusively. In this deployment, each computer is self-managed, and there is no centralized user account management or security policy management. Instead, each computer is responsible for managing its own user accounts, resources, and security policies. In a Workgroup environment, sharing files and resources like printers and folders is done on a case-by-case basis and requires explicit authorization from each computer.

Importing Active Directory Users

Avigilon software has several ways to manage Systems for large organizations. Avigilon recommends synchronizing with your organization's Active Directory to quickly import users and groups. This will allow Windows Active Directory users to log in with their Windows credentials. Members of an imported Active Directory group are automatically added as users to the site.

Changes to users in the Active Directory are synchronized with accounts in the software.

> **NOTE**
>
> User information, including credentials, is maintained by the Active Directory. You can only disable an imported user, assign the user to a group, or configure the user's Login Timeout in the software.

Enabling Active Directory

Before you can import users and groups, you need to enable and log in to Active Directory.

The default port is or 389 UDP in ACC. Ensure that this port is open on all Servers and Active Directory Servers used for authentication. Your AD administrator may choose to use a non-default IP port for better security. This is already transparent to the System.

The default port is 38883 UDP in Unity Video, or 389 UDP in ACC. Ensure that this port is open on all Servers and Active Directory Servers used for authentication. Your AD administrator may choose to use a non-default IP port for better security. This is already transparent to the System.

1. In the New Task menu (☰), click **Site Setup**.
2. Click the site name, then click **Users and Groups**.
3. In the External Directory tab, select **Active Directory** from the drop-down list.

   > **IMPORTANT**
   >
   > If your site is connected to an ACM appliance, enabling Active Directory will disable previously imported ACM roles. To use Active Directory, configure remote authentication from external domains in the ACM appliance first. For more information, see the ACM help files.

4. Click **Edit**.
5. Select the **Use ACC Server account** checkbox to use those credentials, or enter your domain credentials.

   Select the **Use Unity Video Server account** or **Use ACC Server account** checkbox to use those credentials, or enter your domain credentials.

   The service account is either the Local System account or the account specified in Windows Service under the Service Properties in the Log On tab on the computer running the Server software.

6. Click **OK**.

Importing Groups

After Active Directory is enabled, you can import groups and nested groups from trusted domains within the same forest. All users in the group are automatically imported, and will belong to the same permissions group.

1. Click **Add Group**.
2. Select a permission group template and click **OK**. You can change the group's permissions later.
3. To import a group from a different domain, click **Locations...** and select a domain.
4. Enter the name of the Windows group or click **Advanced...** to search for the group.
5. Click **OK**. All users in the group are automatically imported.
6. Update the imported group's settings and permissions.

Importing Users

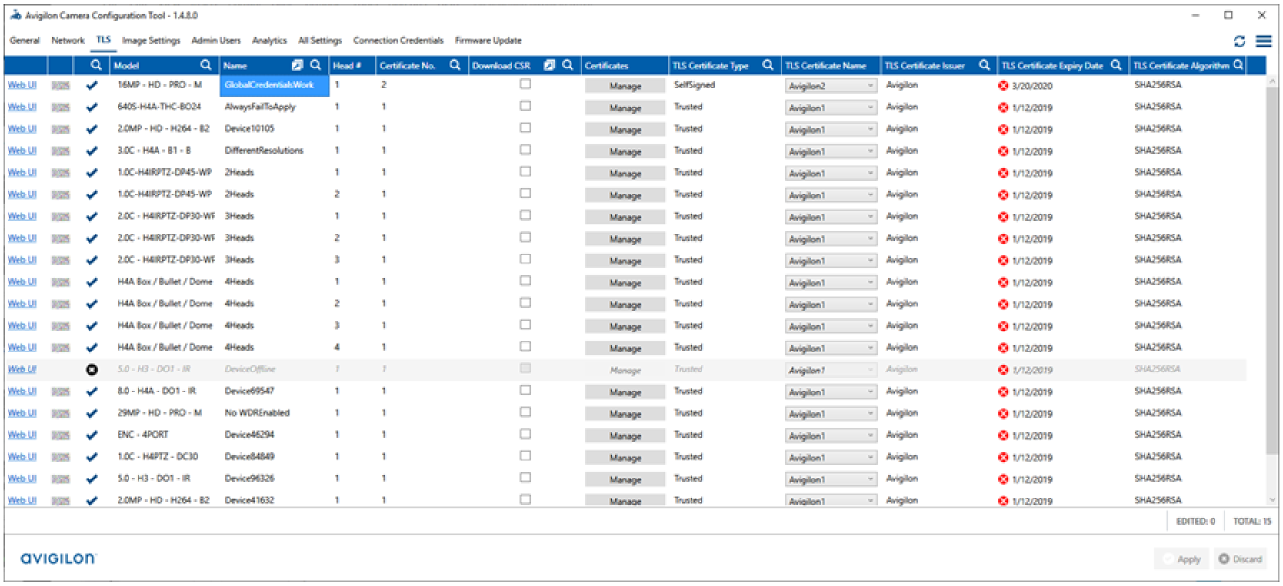
After Active Directory is enabled, you can import users from trusted domains within the same forest.

1. Click **Add User**.
2. To import a user from a different domain, click **Locations...** and select a domain.
3. Enter the name of the Windows user or click **Advanced...** to search for the user.
4. Click **OK**.
5. Assign the imported user to a group:
    a. In the Users tab, select the imported user and click **Edit User**.
    b. Select the **Member Of** tab.
    c. Select the access group checkboxes to assign the user to that group.
    d. Click **OK**.

Securing Device User Accounts

There are three types of device users with different levels of permissions. Not all users require Administrator permissions to perform their duties, but the account used to connect to the System should be an Administrator account. Add necessary users with modified permissions to each of your devices. Avigilon recommends that you change the default username and password of all device user accounts and assign individual accounts to each user of the device.

> **TIP**
>
> You can also use the Camera Configuration Tool to add a secondary or backup Admin user. For more information, see *Creating a Backup Admin Account on page 54*



			Model	Name	Head #	Certificate No.	Download CSR	Certificates	TLS Certificate Type	TLS Certificate Name	TLS Certificate Issuer	TLS Certificate Expiry Date	TLS Certificate Algorithm
Web UI	[redacted]	✓	16MP - HD - PRO - M	GlobalCredentialsWork	1	2	□	Manage	SelfSigned	Avigilon2	Avigilon	☒ 3/20/2020	SHA256RSA
Web UI	[redacted]	✓	640S-H4A-THC-BO24	AlwaysFailToApply	1	1	□	Manage	Trusted	Avigilon1	Avigilon	☒ 1/12/2019	SHA256RSA
Web UI	[redacted]	✓	2.0MP - HD - H264 - B2	Device10105	1	1	□	Manage	Trusted	Avigilon1	Avigilon	☒ 1/12/2019	SHA256RSA
Web UI	[redacted]	✓	3.0C - H4A - B1 - B	DifferentResolutions	1	1	□	Manage	Trusted	Avigilon1	Avigilon	☒ 1/12/2019	SHA256RSA
Web UI	[redacted]	✓	1.0C-H4IRPTZ-DP45-WP	2Heads	1	1	□	Manage	Trusted	Avigilon1	Avigilon	☒ 1/12/2019	SHA256RSA
Web UI	[redacted]	✓	1.0C-H4IRPTZ-DP45-WP	2Heads	2	1	□	Manage	Trusted	Avigilon1	Avigilon	☒ 1/12/2019	SHA256RSA
Web UI	[redacted]	✓	2.0C - H4IRPTZ-DP30-WF	3Heads	1	1	□	Manage	Trusted	Avigilon1	Avigilon	☒ 1/12/2019	SHA256RSA
Web UI	[redacted]	✓	2.0C - H4IRPTZ-DP30-WF	3Heads	2	1	□	Manage	Trusted	Avigilon1	Avigilon	☒ 1/12/2019	SHA256RSA
Web UI	[redacted]	✓	2.0C - H4IRPTZ-DP30-WF	3Heads	3	1	□	Manage	Trusted	Avigilon1	Avigilon	☒ 1/12/2019	SHA256RSA
Web UI	[redacted]	✓	H4A Box / Bullet / Dome	4Heads	1	1	□	Manage	Trusted	Avigilon1	Avigilon	☒ 1/12/2019	SHA256RSA
Web UI	[redacted]	✓	H4A Box / Bullet / Dome	4Heads	2	1	□	Manage	Trusted	Avigilon1	Avigilon	☒ 1/12/2019	SHA256RSA
Web UI	[redacted]	✓	H4A Box / Bullet / Dome	4Heads	3	1	□	Manage	Trusted	Avigilon1	Avigilon	☒ 1/12/2019	SHA256RSA
Web UI	[redacted]	✓	H4A Box / Bullet / Dome	4Heads	4	1	□	Manage	Trusted	Avigilon1	Avigilon	☒ 1/12/2019	SHA256RSA
Web UI		●	5.0 - H3 - DO1 - IR	DeviceOffline	1	1	□	Manage	Trusted	Avigilon1	Avigilon	☒ 1/12/2019	SHA256RSA
Web UI	[redacted]	✓	8.0 - H4A - DO1 - IR	Device69547	1	1	□	Manage	Trusted	Avigilon1	Avigilon	☒ 1/12/2019	SHA256RSA
Web UI	[redacted]	✓	29MP - HD - PRO - M	No WDREnabled	1	1	□	Manage	Trusted	Avigilon1	Avigilon	☒ 1/12/2019	SHA256RSA
Web UI	[redacted]	✓	ENC - 4PORT	Device46294	1	1	□	Manage	Trusted	Avigilon1	Avigilon	☒ 1/12/2019	SHA256RSA
Web UI	[redacted]	✓	1.0C - H4PTZ - DC30	Device84849	1	1	□	Manage	Trusted	Avigilon1	Avigilon	☒ 1/12/2019	SHA256RSA
Web UI	[redacted]	✓	5.0 - H3 - DO1 - IR	Device96326	1	1	□	Manage	Trusted	Avigilon1	Avigilon	☒ 1/12/2019	SHA256RSA
Web UI	[redacted]	✓	2.0MP - HD - H264 - B2	Device41632	1	1	□	Manage	Trusted	Avigilon1	Avigilon	☒ 1/12/2019	SHA256RSA

EDITED: 0 TOTAL: 15

Adding a Device User with the Camera's Web Interface

Use the device's web interface to add a user:

1. On the Users page, click **Add...**.
2. On the Add User page, enter a Username and Password for the new user.
3. In the Security Group drop-down list, select the access permissions available to this new user.
    - **Administrator**: full access to all available features in the camera web interface, including PTZ controls.
    - **Operator**: has access to the live view and PTZ controls but limited access to device setup. For example, this user can configure onboard SD card storage settings, but cannot delete video recordings or format the SD card.
    - **User**: has access to the live view and optional access to PTZ controls, but no access to device setup. To enable PTZ controls, select the Use PTZ Controls checkbox.
4. Click **Apply** to add the user.

For more information

The following documents can provide additional guidance:

- NIST SP 800-53 AC-5: Separation of Duties
- NIST SP 800-53 CM-9: Configuration Management Plan

Monitoring Logs

Avigilon recommends that you monitor logs on your security System to track and investigate security incidents, identify potential security breaches, identify misconfigurations or vulnerabilities in the System, and improve the overall security posture of the System. All the activities and events that occur on the System, including user logins, file access, network connections, System errors are logged. By reviewing logs, security administrators can detect unusual activity or patterns that may indicate a security breach or perform a post-incident analysis.

Servers using Avigilon software include Windows Event logs that are enabled by default to log Windows events on your Server. The Client also has site logs for user, access, and device events. Camera and device logs can also be accessed through the Camera Configuration Tool or the device's web interface.

For more information

The following documents can provide additional guidance:

- NIST SP 800-53 AU-3: Content of Audit Records
- NIST SP 800-53 RA-5: Vulnerability Monitoring and Scanning
- NIST SP 800-53 AU-6: Audit Record Review, Analysis, and Reporting

Windows Event Logs

You can view application error logs on the Server using the Windows Event logs.

1. In the Admin Tool, select **General** > (icon needed).
2. In the Applications Logs dialog box, double-click an error to view the details.
3. Click OK to close the dialog box.

ACC Site Logs

Unity Video or ACC Site Logs

Using the Client, you can view site logs for Servers, devices, users and access events. See the Client User Guide for a full list of the types of events that can be logged for each category, such as users logging in or out, exporting files, and modified a site setting. Site logs can only be accessed from the Client.

To view site logs:

1. In the New Task (☰) menu, click ( ) **Site Logs**.
2. In the top-left area, select the types of events and their details to search.
3. Select the site, Server, or devices you want to search.
4. Set the date and time range to search.
5. Click **Search**.
6. Select a column header to sort the results by Time, Type, or Message.
7. Click a search result to display the event details at the bottom of the tab. You may need to scroll down to view the entire event details.

Device Logs

Using the Camera Configuration Tool, you can access the device logs for connected Avigilon devices. These logs include access and operation events.

TIP

You can also use a device's web interface to view its log entries.

Device logs can only be accessed from the device's web interface or the Camera Configuration Tool.

To view a device's logs:

1. In Camera Configuration Tool, filter the camera list to only display the cameras you want to log.
2. In the top-right corner, select ☰ > **Device Logs**.
3. In the Device Logs window, click **Write Logs to File**.
4. Select a location to save the log file.

   The existing camera logs are automatically downloaded. The System continues to stream and record the live camera logs until you click **Stop** or close the Device Logs window.

NOTE

In the Device Logs window:

- You can reference what device is referenced in the log message by the Serial Number.
- If a camera goes offline it will stop logging until it returns online.
- The log file is saved in .txt format and can be reviewed in text reader.
- Each time you open the Device Logs window the previous log is displayed. Click Write Logs to File to refresh the devices list and save a new log file.

Using Simple Network Management Protocol (SNMP)

Avigilon recommends the use of Simple Network Management Protocol (SNMP) to help manage cameras that are connected to the network. When SNMP is enabled, camera status information can be sent to an SNMP management station including temperature alerts, camera tampering notifications, and SD card status. From there, this status information can be monitored.

See the Configuring SNMP section of the Camera Web Interface User Guide for more information about configuring SNMP for your device. For more details about the status information or traps that will be sent, see the device's Management Information Base (MIB) file. The MIB files are available at avigilon.com/support and the Camera Web Interface Guide can be found at help.avigilon.com.

For more information

The following documents can provide additional guidance:

- NIST SP 800-53 SI-4: System Monitoring

Creating Backup Files

As a best practice for your security system, Avigilon recommends that you create backup files in case there is a need to recover your system at a later date. Having a clear backup workflow can save you time and effort later if there is a crisis. Keep the following in mind when creating your backup workflow:

- Check your backup reports to make sure they are successful.
- Regularly perform manual test restores.
- Create a schedule that includes archiving your backup files.

The following types of backups will be useful for a video security system:

- Backup your server OS drive.
- Create a failover connection to a backup server ensure secure video storage.
- Backup your site settings.
- Backup camera settings using the Camera Configuration Tool.
- Keep a back-up copy of your licenses.
- Export a Site Health Report to PDF or CSV file.

For more information

The following documents can provide additional guidance:

- NIST SP 800-53 CP-6: Alternate Storage Site
- NIST SP 800-53 CP-9: System Backup
- NIST SP 800-53 CP-10: System Recovery and Reconstitution

Setting the Date and Time

Having the correct date and time setup on each device is important from a security point-of-view. For example, this will ensure that System logs for devices are time-stamped with the correct information.

Avigilon recommends that you synchronize the camera clock with a Network Time Protocol (NTP) Server. If there are no NTP Servers on the System, use a public NTP Server or the Avigilon NTP Server. Without NTP synchronization, the date and time must be set manually. Most cameras have a battery backup RTC (Real-Time Clock) that will maintain the time without power.

IMPORTANT

The time setting of your Server and other devices in your System should always be synchronized to prevent data loss or a camera's video stream from being rejected. Using an NTP Server will prevent this issue.

Server Date and Time

The Server gets its time from the operating System. The Server OS must be configured to get its time from an accurate time source. If the Server is joined to a Windows Domain, its OS time will automatically be synchronized with the domain. If the Server is not joined to a Windows Domain, the OS should be configured to use another accurate time source such as an NTP Server, configured using Windows NTP settings.

Camera Date and Time

Avigilon cameras automatically get their time from the Server. This is done using NTP on port 38884. If this port is firewalled, another time source is required and must be manually configured for each camera. See the procedure below for more information.

> **NOTE**
>
> Third party cameras must be manually configured to use an accurate time source. Some cameras are able to use the Server's 38884 NTP port, but many cameras must use the default NTP port 123. These camera must be manually configured to use a time source that uses this default port.

Use the Camera Configuration Tool to configure the NTP Server:

1. In the Camera Configuration Tool, select the **Network** tab
2. In the NTP Server Mode column, select **DHCP** or **Manual**.
3. If you select Manual, in the NTP Server column, enter the NTP Server address.
4. Click **Apply**.

Securing Servers

NVR Premium FIPS Series recorders are built and tested to meet 90% of the STIG requirements of the Windows Server 2019 STIG V2R4 (May-2022), or Windows Server 2016 STIG V1R10 (Jan-2020) for NVR4X, after initial setup when deployed as a standalone or member Server. The remaining 10% are either covered in this guide, or are left to your organization's policies. STIG rules are periodically updated for the latest findings and requirements. Your organization may want to follow the latest edition of the Windows Server STIG to ensure you meet the latest requirements and guidelines.

Complete the steps in the following sections to harden Servers connected your System.

Using Physical Access Control

Physical access control involves restricting access to physical spaces, hardware, and devices to authorized personnel only through the use of physical barriers and other mechanisms. Avigilon software supports integration with ACM as well as other 3rd party access control Systems. Avigilon recommends that you make use of physical access control in your security System to accomplish the following goals:

- **Prevent Unauthorized Access**: Physical access control prevents unauthorized individuals from gaining entry into restricted areas or sensitive spaces, such as Server rooms, thereby protecting valuable assets from theft, damage or sabotage. This can include securing entrances, exits, doors, windows, and other points of entry.
- **Comply with Regulations**: Businesses often need to comply with regulatory standards for physical security, such as in the healthcare or finance sectors, where access to patient records or financial information must be highly restricted.
- **Enhance Cybersecurity**: Physical access control helps prevent cyber threats by ensuring that unauthorized individuals cannot gain access to computer Systems, Servers, and other sensitive equipment. Allowing full administrative access to all internal users can increase the risk of information being compromised in an attack. By preventing users with no need to access System components from doing so, such risk can be mitigated.
- **Accountability and Tracking**: Physical access control allows for accountability and tracking of individuals' movements within a building or campus. Access logs can be used to identify individuals who may be responsible for security breaches, theft, or other criminal activities. See *Monitoring Logs* on page 21 for more information.

Physical access control can also be applied to USB and SD card ports to mitigate risks associated with these ports. The NVR Premium FIPS Series recorder's USB ports are recommended to be disabled during initial setup and deployment. The ports will need to be enabled to use the recovery USB to restore the System. For more information, see *Enabling and Disabling USB Ports* on page 32.

For more information

The following documents can provide additional guidance:

- NIST SP 800-53 PE-1: Physical and Environmental Protection Policy and Procedures
- NIST SP 800-53 PE-2: Physical Access Authorizations
- NIST SP 800-53 PE-3: Physical Access Control
- NIST SP 800-53 AC-6: Least Privilege
- NIST SP 800-53 MP-7: Media Use

Using Dedicated Networks and Servers

Avigilon recommends the use of dedicated networks and Servers, which operate in isolation from other networks and Systems, to reduce the risk of unauthorized access and protect against malware infections. Using dedicated networks and servers with no other services running also minimizes the potential for disruption from other applications or network traffic. Dedicated networks accomplish the following goals:

- **Increase Security**: When all the components of a security System are on a dedicated network and Server, it reduces the attack surface, which makes it more difficult for attackers to gain access or exploit vulnerabilities. This helps to prevent unauthorized access to critical data, sensitive information, and confidential materials.
- **Improve Performance**: Dedicated networks and Servers provide higher performance, as they are designed specifically for the intended purpose. This reduces ottlenecks and resource contention, which ensures that the System can operate at maximum efficiency.
- **Efficient Administration**: When all the components of a security System are on a dedicated network and Server, it simplifies administration, making it easier to manage and maintain. This allows for efficient allocation of resources and more effective application of security policies.

To further limit communication between Client machines and devices connected to the network, Avigilon recommends the use of dedicated network cards. Using separate network interface cards to connect Servers, Client machines, and devices ensures that there is no direct communication between those components. For example, the devices would have a separate network interface card that is dedicated to communication with the security Server. Set up rules that allow only communication between the Client machines and the Server, and do the same for devices and the Server. Encrypt any necessary communication using VPN tunnels and HTTPS encryption.

If there is a network-based archive storage, use a separate and dedicated network for this as well.

For more information

The following documents can provide additional guidance:

- NIST SP 800-53 CA-3: Information Exchange
- NIST SP 800-53 SC-7: Boundary Protection

Setting Up Recording and Storage Settings

If you are running the Server software on a network video recorder, enable the Storage Management feature with the Admin Tool. See the Server User Guide for more information on using the Admin Tool to:

- Set the Primary Data volume location, path, and size
- Add a secondary data volume
- Select which data volume will be the Primary volume
- Change the location of the Config volume

TIP

Avigilon recommends that Config volume and Primary Data volume should be hosted on the same storage volume that is separate from the OS volume.

See the Client User Guide for more information on using the Client to configure Continuous Archiving and Failover Connections.

For more information

The following documents can provide additional guidance:

- Unity Video Server User Guide
- Unity Video Client User Guide
- ACC Server User Guide
- ACC Client User Guide

Changing the Default iDRAC Password

Each NVR has a factory-generated iDRAC password that is printed on the bottom of the luggage tag attached to the unit. To avoid risk of attackers using these unique passwords physically printed on the unit, all passwords for default accounts created during the initial system build should be changed.

> **TIP**
>
> If iDRAC is reset at any time, the root password will revert back to the unique password printed on the luggage tag and should be changed again. Any other non-default accounts will be lost and will have to be re-added.

1. Press the `F2` key while the server is booting up to open System Setup.
2. Go to **iDRAC Settings** > **User Configuration**.
3. Ensure *root* is the current User Name.
4. Enter a new root password in the **Change Password** field and press **Enter**.

   > **IMPORTANT**
   >
   > Avigilon recommends to always use strong passwords that are unique to a single device or service. For more information, see *Securing User Accounts* on page 17.

5. Repeat this procedure for any other default iDRAC accounts.

Getting Started with Deployment

There are two options deploy a ACC system: standalone deployment or Active Directory deployment.

There are two options deploy a Unity Video or ACC system: standalone deployment or Active Directory deployment.

Standalone Deployment

A standalone deployment is the standard deployment as documented in the Client User Guide. Refer to the Client User Guide to set up a standalone deployment.

Active Directory Deployment

Avigilon recommends that you use Windows users in combination with an Active Directory (AD) to authorize access to the System, whenever possible.

There are different options for joining your NVR to an Active Directory, but the general steps are:

1. Note down the IP address of the DNS server.
2. On the NVR, open the **Network and Sharing Center**.
3. Select **NIC** > **Properties** > **Internet Protocol Version 4 (TCP/IP)** > **Properties** > **Use the following DNS server addresses**. Select the NIC that is connected to your local network.
4. Enter the IP address of the DNS server noted in step 1 as the **Preferred DNS server**.

   If you have an alternate or backup DNS server, you can enter that as the Alternate DNS server.
5. Click **OK**.
6. Logout and then log back in to the NVR.

Refer to the Client User Guide to continue setting up your Active Directory deployment.

For more information

The following documents can provide additional guidance:

- Initial Unity Video System Setup and Workflow Guide
- Unity Video Help Center
- Unity Video Server User Guide
- Initial ACC System Setup and Workflow Guide
- ACC 7 Help Center
- ACC 7 Server User Guide

Creating the OS Recovery USB Drive

FOR NVR PREMIUM FIPS SERIES RECORDERS

As part of your initial setup, Avigilon recommends that you create an OS recovery USB drive in case it is needed to recover your system in the future.

> **TIP**
>
> Make sure your USB drive is at least 32 GB to contain all of the recovery files. Be aware that any stored files will be deleted as part of the creation process.

To create the recovery USB, you will need to follow this procedure on a workstation or laptop that is running Windows 10 (1703) or later.

1. Download a USB recovery image and the USB recovery creation tool, *USB_Recovery_Creation_Tool.exe*, to your workstation or laptop. The USB creation tool and recovery image are available at avigilon.com.
2. Run the **USB_Recovery_Creation_Tool.exe** file.
3. Select your USB device from the **Recovery USB** drop-down list.

4. Browse to the downloaded recovery image file and select it.
5. Click **Create USB**. Wait for the USB creation process to finish. This can take up to 20 minutes.
6. Remove the USB from the workstation or laptop and store it in a secure location.

> **NOTE**
>
> Once the USB has been created, you will need to copy the BitLocker recovery keys to the root of the recovery USB drive. For more information, see *Backing Up the BitLocker Recovery Keys* below. This step is only required for NVR Premium FIPS Series recorders. Other Avigilon NVRs do not use BitLocker encryption.

Backing Up the BitLocker Recovery Keys

FOR NVR PREMIUM FIPS SERIES RECORDERS

Avigilon recommends that you back up your BitLocker recovery key as part of your initial NVR Premium FIPS Series recorder setup. The BitLocker recovery key is backed up as a BEK file. This process can also be done at any time after initial setup using the command line procedure, in case the original backup is lost.

The recovery key BEK files need to be copied to the root of the recovery USB device so it can be used to unlock the drives if a recovery is needed. For more information, see *Creating the OS Recovery USB Drive* on the previous page.

The following section describes copying the BEK recovery key files to the root of the recovery USB device.

Copying BEK Recovery Keys to the Recovery USB Device

The BitLocker BEK recovery keys are automatically created when the NVR is deployed. These files need to be copied to the root of the USB recovery device.

1. Plug the USB recovery device into the recorder.

> **NOTE**
>
> USB ports must be enabled to access the USB device. For more information, see *Enabling and Disabling USB Ports on page 32*.

2. The BEK files are hidden by default. You will need to view the files in order to copy them. The folder should contain 2 BEK files.
   a. Open Window Explorer.
   b. Go to **View** > **Options** > **Folder Options** and deselect the **Hide protected operating system files (Recommended)** checkbox. Click **Yes** on the warning message that appears.
   c. Click **Apply** and **OK**.
   d. Go to **View** > **Options** > **Folder Options** and select the **Show hidden files, folders, and drives** option under *Hidden files and folders*.
   e. Click **Apply** and **OK**. The BEK files should now display.
3. Copy the BEK BitLocker recovery key files located in `C:\Avigilon\BitLockerRecovery` to the root of the USB device.

4. Ensure that the files were copied successfully, and then delete the **BitLockerRecovery** folder from `C:\Avigilon`.
5. Store the USB recovery device in a secure location.

Using the Command Prompt to Back Up BEK Recovery Key Files

1. Plug the USB recovery device into the recorder.
2. Open the Command Prompt as administrator.
3. Enter the following command and press `Enter`:

```
manage-bde -protectors -get <encrypted drive letter>: -SaveExternalKey <USB
drive letter>:\
```

> **TIP**
>
> In the example above, choose which encrypted drive you want to back up the recovery file for, either **C:** or **D:**, and enter the drive letter for the USB device. Remove < and > from the command after entering your drive letters.

4. The BEK recovery key file for that drive will be saved to the root of the USB device.
5. Repeat this procedure so that you have backed up both the C: and D: recovery key files, and save the USB device in a secure location.

Setting Clients to WAN Mode

FOR NVR PREMIUM FIPS SERIES RECORDERS

As part of hardening the NVR Premium FIPS Series recorder, LAN mode live streaming to a Client is not supported. Instead, secure live streaming is supported in WAN mode. Set any Clients connecting to the NVR Premium FIPS Series recorder to WAN mode to ensure secure live streaming.

For more information about setting WAN mode, see *Encrypting Video* on page 50.

Starting Windows Credential Guard Services

FOR NVR PREMIUM FIPS SERIES RECORDERS

On an Avigilon NVR Premium FIPS Series recorder that will be joining a domain, you must start running Windows Credential Guard services to meet STIG requirements. You will need to perform this fix by editing a group policy:

1. Open the Local Group Policy Editor and go to the policy for **Computer Configuration** > **Administrative Templates** > **System** > **Device Guard**.
2. Set the **Turn On Virtualization Based Security** option to **Enabled**, with the following settings:
   - **Enabled with UEFI lock** selected for the **Credential Guard Configuration** setting.
   - **Secure Boot** or **Secure Boot and DMA Protection** selected for the **Select Platform Security Level:** setting.
3. Click **Apply** and **OK**.

NOTE

After updating the group policy, use the command line to run **gpupdate** and then restart the machine for the settings to take effect. In some cases, the settings may not apply until the machine is restarted a second time.
For more information on using gpupdate, see Microsoft's documentation.

Enabling and Disabling USB Ports

FOR NVR PREMIUM FIPS SERIES RECORDERS

To help keep your NVR Premium FIPS Series recorder safe from the threat of individuals accessing the USB ports on your NVR, there is a configuration tool for enabling and disabling the USB ports on your NVR. In cases where you need to enable the USB port in order to recover your system, and your system is in a state where you can't access the configuration tool, you can enable the USB ports using BIOS after rebooting the NVR.

For more information

The following documents can provide additional guidance:

- NIST SP 800-53 MP-7: Media Use

Using the Configuration Tool for USB Ports

To increase the security of your NVR Premium FIPS Series recorder, Avigilon recommends that you disable the USB ports on the NVR:

TIP

If you disable the USB ports on a workstation, you will need a secure shared network drive or something similar for exporting clips and images to. If you disable the USB ports on your NVR Premium FIPS Series recorder and want to set up archiving, you will need a secure shared network drive or something similar for writing the archives to.

1. Launch **UsbPortConfigurationTool.exe** as administrator. It is located at: `C:\Avigilon\3rdPartyInstallers\UsbPortConfigurationTool.exe`.
2. The tool will display the current USB port configuration and give you the following configuration options:
   - **[A] All Ports On**. Type `A` and `Enter` to enable all of the USB ports.
   - **[O] All Ports Off**. Type `O` and `Enter` to disable all of the USB ports.
   - **[B] Back Ports On and Front Ports Off**. Type `B` and `Enter` to disable the front ports and leave the back ports enabled.
   - **[C] Cancel**. Type `C` and `Enter` to cancel making any changes to your USB port configuration.

   NOTE

   The selections that use yellow text are the default selections and will be executed if you press `Enter` without entering any other letter.

3. Type `Y` to confirm the configuration or `N` to cancel. Press `Enter`.
4. Changing the USB port configuration will require a system restart. Type `Y` and `Enter` to restart now or `N` and `Enter` to restart later.

Enabling USB Ports During Startup

If you have disabled the USB ports on your NVR Premium FIPS Series recorder and require the port to do an OS recovery, you may not be able to use the configuration tool to re-enable the USB ports. In this case you can use the following steps to enable the USB ports using BIOS Settings during system startup:

1. Press the `F2` key while the server is booting up to open System Setup BIOS Settings.
2. Go to **System BIOS Settings** > **Integrated Devices**.
3. Select **All Ports On** or **Only Back Ports On** from the **User Accessible USB Ports** drop-down list.

   Either all of the USB ports or the USB ports on the back of the unit will now be available to use with the USB recovery device.
4. Click **Exit** to save your setting.

Enabling iDRAC Networking

FOR NVR PREMIUM FIPS SERIES RECORDERS

The out of band management port (OOBM) on the NVR Premium FIPS Series recorder that is used for iDRAC is disabled by default from the factory. It is disabled according to the hardening policies.

In cases where you want to use iDRAC with your NVR, despite the security risk, you will need to enable iDRAC networking before you can connect to the NVR with iDRAC. See Dell's iDRAC documentation for more information.

IMPORTANT

If you are using iDRAC with your NVR Premium FIPS Series recorder, it is strongly recommended that you follow Dell's Guidelines for Hardening iDRAC to ensure it is used securely.

1. Turn on the NVR.
2. Press <**F2**> during the Power-on Self-test (POST).
3. In the **System Setup Main Menu** page, click **iDRAC Settings**.
4. Click **Network**.
5. Enable and specify the network settings.
6. Click **Back**, click **Finish**, and then click **Yes**. The network information is saved and the system reboots.

Enabling Windows Error Reporting Service

FOR NVR PREMIUM FIPS SERIES RECORDERS

As part of hardening the NVR Premium FIPS Series recorders, Windows Error Reporting Service has been disabled on the NVR. This service is a low risk and should be safe to enable on your system should you want to collect error reporting and crash dump information on your NVR Premium FIPS Series recorder.

Set the Windows Error Reporting Service to *Manual* if you want to enable this service.

Disabling the Sending of Additional Data

To keep your NVR secure, you should Enable the option to *Do Not Send Additional Data* when additional data is requested by Microsoft in response to Windows error reports. Enabling this setting will automatically decline any additional data requests from Microsoft.

1. Open the Group Policy Management Console by running **gpmc.msc**.
2. Navigate to `Computer Configuration > Policies > Administrative Templates > Windows Components > Windows Error Reporting`.
3. Set the **Do Not Send Additional Data** option to **Enabled**.

Enabling Server Administrator Software

FOR NVR PREMIUM FIPS SERIES RECORDERS

Addresses STIG V-223042 on NVR5, or V-64717 on NVR4X

The Server Administrator software is pre-installed on the NVR Premium FIPS Series recorders to provide information about the system operation status and give you remote access to the NVR for recovery operations. To comply with hardening policies, the NVR Premium FIPS Series recorders will not allow the Server Administrator software to open with its default self-signed certificate.

You have the following two options to enable the Server Administrator software:

- Obtain a CA-signed certificate. This will replace the risky self-signed certificate and allow you to use the Server Administrator software as intended.
- Use the Windows Registry Editor to work around the self-signed certificate. This method is not recommended as a permanent solution, but may be an acceptable risk for a one-time use of the Server Administrator software.

> **IMPORTANT**
>
> Once you have finished using the Server Administrator software with this workaround, you must restore the registry file to its original configuration or you will risk leaving your system vulnerable to attack.

Certificate Management for the Server Administrator Software

To safely use the Server Administrator software on your NVR Premium FIPS Series recorder on a regular basis, you will need a certificate signed by a well-known and trusted Certificate Authority (CA) to replace the default self-signed certificate. You can do this by following the steps below. For more detailed information, refer to Dell's documentation on this process.

1. Use the Server Administrator Web interface to generate a Certificate Signing Request (CSR) with your company's information.
2. Submit the CSR to a trusted Certificate Authority such as VeriSign.

   The CA can be a root CA or an intermediate CA.

3. After receiving the CA-signed SSL certificate, upload it to the Server Administrator.

   The SSL certificate for each Server Administrator must be placed in the certificate store of the management station. After the SSL certificate is installed on the management station, you can access the Server Administrator software without certificate warnings.

Server Administrator Software Registry Key Workaround

If you only need to use the Server Administrator software for a single action, you can use the Windows Registry Editor to edit a registry key to temporarily allow use of the default self-signed certificate.

> **IMPORTANT**
>
> Using this workaround will leave your system vulnerable to cyber attacks and should only be done temporarily. Once you have performed the required action with the Server Administrator software, Avigilon highly recommends that you return the registry key to its original setting.

1. Open the Windows Registry Editor:
   a. Press the **Windows** key and **R** key at the same time.
   b. Type `regedit` in the **Open** field and click **OK**.
2. Navigate to the following registry key:
   `HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings`
3. Change the **PreventIgnoreCertErrors** value to **REG_DWORD** = **0**.

   This will allow the Server Administrator software to load, but will fail STIG compliance.

4. Perform any actions needed with the Server Administrator software. When complete, use the Windows Registry Editor to return **PreventIgnoreCertErrors** to its original state.

When Resetting the NVR to Default Settings

FOR NVR PREMIUM FIPS SERIES RECORDERS

If you are required at any point to reset your Avigilon NVR Premium FIPS Series recorder to its default settings, you will need to change some other settings after resetting the unit to ensure the Avigilon NVR Premium FIPS Series recorder is reset in the correct state.

After using BIOS to reset to default settings, the following settings need to be manually applied in the System BIOS interface:

- TPM Security turned **ON**. This setting is located in System BIOS Settings > System Security.
- The CPU's Virtualization Technology set to **Enabled**. This setting is located in System BIOS Settings > Processor Settings.
- PXE Devices are set to **Disabled**. These settings are located in System BIOS Settings > Network Settings.

The iDRAC FIPS Mode and iDRAC Enable NIC settings should not be affected by the BIOS reset. However, after resetting to default settings you should confirm that these two settings are set correctly to ensure your system is secure.

- Verify that the iDRAC FIPS Mode is set to **Enabled**. This setting is accessed through the iDRAC web interface, in iDRAC Settings > Connectivity > Network > Advanced Network Settings > Federal Information Processing Standards.
- Verify that the iDRAC Enable NIC is set to **Disabled**. This setting is located in System BIOS iDRAC Settings > Network Settings.

Securing the Network

Complete the steps in the following sections to harden the network in your System.

Setting Up Basic Network Settings

Use the device's web interface to setup its basic network settings:

> **TIP**
>
> The Camera Configuration Tool can also be used to set static IP addresses for connected cameras.

1. Go to the Network setup page.
2. At the top of the page, select how the camera obtains an IP address:
    - **Obtain an IP address automatically**: select this option to connect to the network through an automatically assigned IP address.

      The IP address is obtained from a DHCP Server. If it cannot obtain an address, the IP address will default to addresses in the 169.254.x.x range.
    - **Use the following IP address**: select this option to manually assign a static IP address.
        - **IP Address**: Enter the IP address you want to use.
        - **Subnet Mask**: Enter the subnet mask you want to use.
        - **Default Gateway**: Enter the default gateway you want to use.
3. Select the **Disable setting static IP address through ARP/Ping method** checkbox to disable the ARP/Ping method of setting an IP address.
4. If the camera supports IPv6, select the **Enable IPv6** checkbox to configure the following settings.

    > **NOTE**
    >
    > Enabling IPv6 does not disable IPv4 settings.

    a. Select the **Accept Router Advertisements** checkbox if using Stateless Address Auto-Configuration.

    b. From the DHCPv6 State drop-down list, select one of the following:
    - **Auto**: DHCPv6 state is determined by router advertisements (RA).

      > **NOTE**
      >
      > The Accept Router Advertisements setting must be enabled for this setting to perform as expected.
    - **Stateful**: the camera receives IP address, DNS and NTP information from the DHCPv6 Server.

- **Stateless**: the camera only receives DNS and NTP information from the DHCPv6 Server. It does not accept an IP address from the DHCPv6 Server.
- **Off**: the camera does not communicate with the DHCPv6 Server.

c. In the **Static IPv6 Addresses** field, enter the preferred IPv6 address. Click + for additional addresses.

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

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

> **NOTE**
>
> The configured prefix length may not display correctly in the web interface, but the prefix used by the camera will be the configured length.

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

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

5. If you need to customize the hostname, enter it in the **Hostname** field.
6. In the Control Ports area, you can specify which control ports are used to access the camera. Clear the the **Enable HTTP connections** checkbox to limit the camera to secure connections only. HTTP Port access is enabled by default.

   You can change the default ports to any port number between 1 and 65534. The default port numbers are:

   - **HTTP Port**: 80
   - **HTTPS Port**: 443
   - **RTSP Port**: 554
7. Click **Apply** to save your settings.

Securing Network Communications

Implement strong network security measures to ensure the reliability and effectiveness of your security System. Security Systems need to be protected by network security protocols, such as the following:

- **VPN tunnels and HTTPS encryption**: Secures communication channels between Client devices and Servers.
- **IEEE 802.1x standard**: Ensures that only authorized devices are allowed access to the network via port-based access control.
- **Transport Layer Security (TLS)**: Encrypts data in transit and protects it from interception and tampering.

With these protocols in effect, unused network protocols can be disabled:

- **Servers**: Obsolete versions of SSL/TLS protocols can be disabled.
- **Devices**: ARP and HTTP can be disabled. IPv6 can also be disabled if not in use.

NOTE

For new FIPS-enabled cameras, these services and protocols will be disabled out of the box. For deployed devices that are being upgraded with hardened firmware, these services and protocols will need to be disabled manually. For more information, see the appropriate device Camera Web Interface Guide, which can be found at help.avigilon.com.

When connecting wireless devices to the System, Avigilon recommends protecting those communications following the IEEE 802.11 security objectives established by NIST in NIST SP 800-48 revision 1, Guide to Securing Legacy IEEE 802.11 Wireless Networks (nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-48r1.pdf).

For more information

The following documents can provide additional guidance:

- Public-Key Infrastructure: datatracker.ietf.org/wg/ipsec/documents
- CA/Browser Forum: cabforum.org
- NIST SP 800-53 SI-2: Flaw Remediation
- NIST SP 800-53 CM-6: Configuration Settings
- NIST SP 800-53 CM-7: Least Functionality
- NIST SP 800-53 SC-23: Session Authenticity
- NIST SP 800-53 AC-17: Remote Access (Disable Nonsecure Network Protocols)
- NIST SP 800-53 AC-18: Wireless Access
- NIST SP 800-53 IA-2: Identification and Authentication (Organizational Users)
- NIST SP 800-53 SA-9: External System Services

Using Self-Signed Certificates

The following sections will provide information on the steps needed to generate a CA-signed certificate, disable Avigilon's default certificate, and verify that the new certificate is functioning correctly.

Managing Certificates on the Server

By default, the Server uses a self-signed certificate for verifying Client communications. Avigilon recommends using a trusted CA-signed certificate or other intermediate certificate, such as a Windows CA or custom CA certificate. You must be a Windows Administrator to make these changes.

If you are using a CA-signed certificate, you will need to disable trust of the default Avigilon certificates after setting up your CA-signed certificates to ensure the default certificate can no longer be used.

If you are managing certificates on a machine running both Client and the Server, follow the instructions starting with *Generating the Certificate* on the next page. If the machine is only running the Client, skip to *Importing the Certificate Authorities* on page 41.

IMPORTANT

After generating a new Server certificate or importing new Certificate Authorities, the Avigilon Unity Orchestrator Service will need to be restarted from the *services.msc* tool.
If you are manually logging into a Server after setting up your certificate instead of using auto-discovery, use the full Server hostname, including domain.

NOTE

The instructions below are an example workflow for users of a small cluster that can physically access each Server to manually set them up.
If you are using custom certification or remotely pushing certificates, ensure that the certificates meet the following criteria:

- Resides in the Server machine's LocalMachine/Personal certificate store
- Friendly name is ***AccServerCert***.
- Friendly name is ***AccServerCert***. ***UnityServerCert*** can also be used on Unity Servers.
- **Make private key exportable** is enabled
- **Alternative Name** corresponds to the Server's fully-qualified hostname
- Has a secure signature algorithm (not SHA1)
- Certificate authorities are present on all Server and Client machines in **Trusted Root Certification Authorities** and **Intermediate Certification Authorities** certificate stores, as appropriate

Generating the Certificate

1. Open the Certificate Manager. Select **Run** in the **Start** menu and enter *certlm.msc*.
2. Navigate to the **Personal** > **Certificates** folder.
3. Right-click in the folder contents area and select **All Tasks** > **Request New Certificate...**.
4. Click **Next**.
5. In the Select Certificate Enrollment Policy window, select the **Active Directory Enrollment Policy** and click **Next**.
6. In the Request Certificates window, select the appropriate policy checkbox, then expand the **Details** drop-down arrow and click **Properties**.
7. On the **General** tab, enter the **Friendly Name** as ***AccServerCert***.

IMPORTANT

Make sure to enter the correct Friendly Name, ***AccServerCert***. Otherwise, the Server and Clients will not recognize the certificate and will fail to connect.

8. On the **General** tab, enter the **Friendly Name** as ***AccServerCert***. ***UnityServerCert*** can also be used on Unity Video Servers.

> **IMPORTANT**
>
> Make sure to enter the correct Friendly Name, ***AccServerCert*** or ***UnityServerCert***. Otherwise, the Server and Clients will not recognize the certificate and will fail to connect.

9. On the **Subject** tab, in the **Alternative Name** area, expand the drop-down arrow and click **DNS**.
10. Fill in the full Server hostname, including domain name, and click **Add**.
11. On the **Private Key** tab, in the **Key options** area, fill the **Make private key exportable** check box.
12. If your software is running as a specific user account, configure permissions on the private key:
    a. On the **Private Key** tab, in the **Key permissions** area, fill the **Use custom permissions** check box.
    b. Click **Set permissions...** and add the corresponding user account to the group or user list.
13. Click **OK**.
14. On the Request Certificates window, click **Enroll**. Click **Finish** when the operation is complete.

Exporting the Certificate Authorities

> **NOTE**
>
> Exporting and importing should only be done if other Servers in the cluster, or the machines where the Client is run, do not already have the Root and Intermediate Certificate Authorities of the generated certificate.

1. Using the certlm.msc tool, double-click the new certificate and select the **Certification Path** tab.
2. For each certificate authority above the new certificate:
    a. Click **View Certificate**.
    b. On the **Details** tab, click **Copy to File...**.
3. Click **Next**.
4. If you are asked whether to export the private key, select **No (default)** and click **Next**.
5. Leave the Export File Format settings as default and click **Next**.
6. Enter the name and location for the exported certificate, or click **Browse** to navigate to the location where you want to save the exported certificate. Click **Next**.
7. Click **Finish** to export the certificate and private key.

Importing the Certificate Authorities

This procedure should be performed on the Client or Server without the Certificate Authorities of the new Server certificate:

1. Using the certlm.msc tool, right-click in the **Trusted Root Certification Authorities** > **Certificates** folder contents area. Click the **Action** menu and select **All Tasks** > **Import...**.
2. Click **Next**.
3. On the File to Import window, enter the certificate name and path in the **File name** field or click **Browse** to navigate to the exported root certificate authority. Click **Next**.
4. Select the Import option to **Mark the key as exportable** and **Include all extended properties**, then click **Next**.
5. Leave the settings as default and click **Next**.
6. Click **Finish**.
7. Repeat the above steps for each exported Intermediate Certificate Authority. In Step 1, chose **Intermediate Certification Authorities** instead of **Trusted Root Certification Authorities**.

Disabling Default Avigilon Certificates

Once you have set up your trusted CA-signed certificates, you will need to disable trusting of the default Avigilon certificates for the sites and Clients that will be using CA-signed certificates.

IMPORTANT

Make sure that you have set up trusted certificates on your Servers and Clients before disabling trust for the Avigilon certificate authority.

Site Settings

1. In the New Task menu ☰, click **Site Setup**.
2. Select a site, then click **Security** 🔒 .
3. Select the **Require trusted server certificates** checkbox.
4. Click **OK**.

Client Settings

1. In the top-right corner of the Client, select ⚙ > **Client Settings**.
2. In the Security tab, select the **Require trusted server certificates** checkbox.
3. Click **OK**.

Verifying the Certificate

Once you have created the Active Directory certificate and imported the private key, you can verify that it is functioning correctly on your Server:

1. Open a web browser and enter https://[localhost name]:38881

   Locahost name is the localhost of the created certificate with the domain.
2. Click the lock icon to the left of the URL.
3. The message *Connection is secure* and *Certificate (Valid)* indicates the certificate is working correctly.
4. Click **Certificate (Valid)** to display the details of the certificate. The name of the certificate you have just created should be displayed.

Configuring Endpoint Security Settings

When end-point security software runs an automated scan on a heavily used Avigilon NVR or workstation, it may prevent video data from being written. Some endpoint security software is equipped with live process scanning and incorporated firewalls. These features may cause communication failures between cameras and NVRs or between NVRs and clients.

To minimize performance issues, you should set up exceptions in the endpoint security running on NVRs, workstations or clients within the Avigilon Unity Video system. For more information on how to exclude locations and applications from being scanned, see your endpoint security manual.

To enable communication between Unity Cloud and Unity Video Server, see the *Safelisting Services* used by Unity Cloud in the Unity Cloud User Guide.

Preventing Data Write Issues

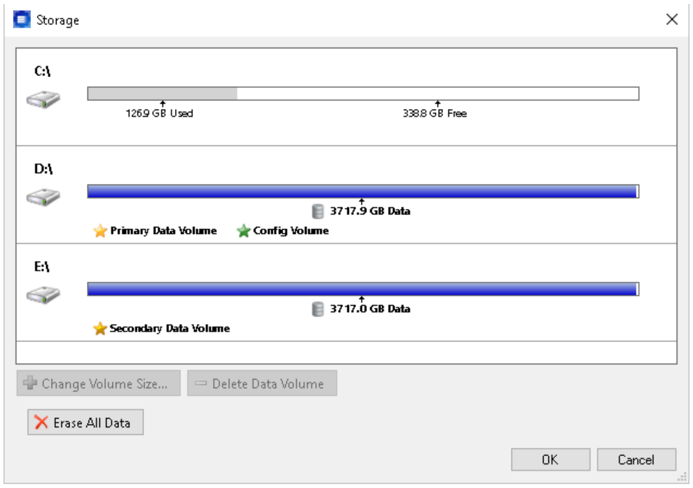
To ensure endpoint security software does not interfere with the Avigilon Unity Video software's ability to write video data and other important files, exclude the following locations from being scanned:

AvigilonData	Located on each of the Primary and Secondary Data Volumes.*
AvigilonConfig	Located on each of the Config Volumes.*

*Do not use the C drive or an OS drive for these volumes. To see which drives are configured as the Primary and Secondary Data Volumes and Config Volumes, use the Avigilon Unity Video Admin Tool.

- In the Admin Tool, click **Settings** > **Storage**.

  The Primary and Secondary Data Volumes and Config Volumes are displayed.



Preventing Execution Issues

There are two ways to prevent Avigilon applications from being flagged by endpoint security software:

1. (recommended): If you endpoint security software supports certificate-based whitelisting, add Avigilon's certificate to your endpoint security software’s approved list.

2. Add the following process exclusions to your approved list:

- C:\Program Files\Avigilon\Avigilon Unity Server\VmsAdminPanel.exe
- C:\Program Files\Avigilon\Avigilon Unity Server\VmsAdminPanelLauncher.exe
- C:\Program Files\Avigilon\Avigilon Unity Server\VmsDaemonService.exe
- C:\Program Files\Avigilon\Avigilon Unity Web Endpoint\WebEndpointService.exe*
- C:\Program Files\Avigilon\Avigilon Unity Server\LPR6\LprDaemonApp.exe*
- C:\Program Files\Avigilon\Avigilon Unity Analytics Service\AnalyticsDaemonService.exe*
- C:\Program Files\Avigilon\Avigilon Unity Cloud Bridge\VmsCloudBridge.exe
- C:\Program Files\Avigilon\Avigilon Unity Orchestrator Service\VmsOrchestratorService.exe
- C:\Program Files\Avigilon\Avigilon Unity API Gateway\VmsApiGateway.exe
- C:\Program Files\Avigilon\Avigilon Unity Core\VmsCore.exe
- C:\Program Files\Avigilon\Avigilon Unity Client\CefSharp.BrowserSubprocess.exe
- C:\Program Files\Avigilon\Avigilon Unity Core\bin\pgbouncer\pgbouncer.exe
- C:\Program Files\Avigilon\Avigilon Unity Core\bin\pgsql\bin\clusterdb.exe
- C:\Program Files\Avigilon\Avigilon Unity Core\bin\pgsql\bin\createdb.exe
- C:\Program Files\Avigilon\Avigilon Unity Core\bin\pgsql\bin\createuser.exe
- C:\Program Files\Avigilon\Avigilon Unity Core\bin\pgsql\bin\dropdb.exe
- C:\Program Files\Avigilon\Avigilon Unity Core\bin\pgsql\bin\dropuser.exe
- C:\Program Files\Avigilon\Avigilon Unity Core\bin\pgsql\bin\ecpg.exe
- C:\Program Files\Avigilon\Avigilon Unity Core\bin\pgsql\bin\initdb.exe
- C:\Program Files\Avigilon\Avigilon Unity Core\bin\pgsql\bin\isolationtester.exe
- C:\Program Files\Avigilon\Avigilon Unity Core\bin\pgsql\bin\libpq_pipeline.exe
- C:\Program Files\Avigilon\Avigilon Unity Core\bin\pgsql\bin\libpq_testclient.exe
- C:\Program Files\Avigilon\Avigilon Unity Core\bin\pgsql\bin\libpq_uri_regress.exe
- C:\Program Files\Avigilon\Avigilon Unity Core\bin\pgsql\bin\oid2name.exe
- C:\Program Files\Avigilon\Avigilon Unity Core\bin\pgsql\bin\pgbench.exe
- C:\Program Files\Avigilon\Avigilon Unity Core\bin\pgsql\bin\pg_amcheck.exe
- C:\Program Files\Avigilon\Avigilon Unity Core\bin\pgsql\bin\pg_archivecleanup.exe
- C:\Program Files\Avigilon\Avigilon Unity Core\bin\pgsql\bin\pg_basebackup.exe
- C:\Program Files\Avigilon\Avigilon Unity Core\bin\pgsql\bin\pg_checksums.exe
- C:\Program Files\Avigilon\Avigilon Unity Core\bin\pgsql\bin\pg_config.exe
- C:\Program Files\Avigilon\Avigilon Unity Core\bin\pgsql\bin\pg_controldata.exe
- C:\Program Files\Avigilon\Avigilon Unity Core\bin\pgsql\bin\pg_ctl.exe
- C:\Program Files\Avigilon\Avigilon Unity Core\bin\pgsql\bin\pg_dump.exe
- C:\Program Files\Avigilon\Avigilon Unity Core\bin\pgsql\bin\pg_dumpall.exe
- C:\Program Files\Avigilon\Avigilon Unity Core\bin\pgsql\bin\pg_isolation_regress.exe
- C:\Program Files\Avigilon\Avigilon Unity Core\bin\pgsql\bin\pg_isready.exe
- C:\Program Files\Avigilon\Avigilon Unity Core\bin\pgsql\bin\pg_receivewal.exe
- C:\Program Files\Avigilon\Avigilon Unity Core\bin\pgsql\bin\pg_recvlogical.exe

- C:\Program Files\Avigilon\Avigilon Unity Core\bin\pgsql\bin\pg_regress.exe
- C:\Program Files\Avigilon\Avigilon Unity Core\bin\pgsql\bin\pg_regress_ecpg.exe
- C:\Program Files\Avigilon\Avigilon Unity Core\bin\pgsql\bin\pg_resetwal.exe
- C:\Program Files\Avigilon\Avigilon Unity Core\bin\pgsql\bin\pg_restore.exe
- C:\Program Files\Avigilon\Avigilon Unity Core\bin\pgsql\bin\pg_rewind.exe
- C:\Program Files\Avigilon\Avigilon Unity Core\bin\pgsql\bin\pg_test_fsync.exe
- C:\Program Files\Avigilon\Avigilon Unity Core\bin\pgsql\bin\pg_test_timing.exe
- C:\Program Files\Avigilon\Avigilon Unity Core\bin\pgsql\bin\pg_upgrade.exe
- C:\Program Files\Avigilon\Avigilon Unity Core\bin\pgsql\bin\pg_verifybackup.exe
- C:\Program Files\Avigilon\Avigilon Unity Core\bin\pgsql\bin\pg_waldump.exe
- C:\Program Files\Avigilon\Avigilon Unity Core\bin\pgsql\bin\postgres.exe
- C:\Program Files\Avigilon\Avigilon Unity Core\bin\pgsql\bin\psql.exe
- C:\Program Files\Avigilon\Avigilon Unity Core\bin\pgsql\bin\reindexdb.exe
- C:\Program Files\Avigilon\Avigilon Unity Core\bin\pgsql\bin\psql.exe
- C:\Program Files\Avigilon\Avigilon Unity Core\bin\pgsql\bin\reindexdb.exe
- C:\Program Files\Avigilon\Avigilon Unity Core\bin\pgsql\bin\vacuumdb.exe
- C:\Program Files\Avigilon\Avigilon Unity Core\bin\pgsql\bin\vacuumlo.exe
- C:\Program Files\Avigilon\Avigilon Unity Core\bin\pgsql\bin\zic.exe
- C:\Program Files\Avigilon\Avigilon Unity Player\CefSharp.BrowserSubprocess.exe
- C:\Program Files\Avigilon\Avigilon Unity VirtualbMatrix\CefSharp.BrowserSubprocess.exe
- C:\Program Files\Avigilon\Avigilon Control Center Server\VmsUpgraderApp.exe
- C:\Program Files\Avigilon\Avigilon Control Center Client\VmsClientApp.exe
- C:\Program Files\Avigilon\Avigilon Control Center Web Endpoint\node.exe
- C:\Program Files\Avigilon\Avigilon Control Center Gateway\VmsWebGateway.exe
- C:\Program Files\Avigilon\Avigilon Control Center Virtual Matrix\VmsVirtualMatrixApp.exe
- C:\Program Files\Avigilon\Avigilon Player\VmsPlayerApp.exe
- C:\Program Files\Avigilon\Avigilon Platform Monitor Service\AvigilonPlatformMonitorService.exe
- C:\Program Files (x86)\Avigilon\Avigilon Control Center Player\VmsPlayerApp.exe
- D:\AvigilonData
- D:\AvigilonConfig

Configuring FIPS Compliance

FOR NVR PREMIUM FIPS SERIES RECORDERS

You can select the level of compliance with the Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules for server and client communication.

Server Communication

Define the level of compliance for cryptographic modules used for server communication.

Servers added to a multi-server site will use the same setting as the site.

1. In the New Task menu ☰, click **Site Setup**.
2. Select a site, then click **Security** 🔒 .
3. Select the **FIPS 140-2 Mode:**
   - **Off** — Only uses non-FIPS compliant cryptographic modules.
   - **Relaxed** — Prefers communication using FIPS 140-2-compliant cryptographic modules, but allows non-compliant cryptographic modules.
   - **Strict** — Allows communication using only FIPS 140-2-compliant cryptographic modules.
4. Click **OK**.

> **TIP**
>
> Use **Relaxed** mode for:
>
> - The initial configuration of a distributed System, especially if using a laptop.
> - Systems with components that have not been upgraded to version 7.8 or later.
> - Systems with third-party integrations that are not FIPS 140-2-compliant.

Client Communication

Define the level of compliance for cryptographic modules used when the client logs in to sites.

1. In the top-right corner of the Client, select ⚙ > **Client Settings**.
2. In the Security tab, select the **FIPS 140-2 Mode:**
   - **Off** — Allows log in using the default Secure Remote Password protocol (SRP).
   - **Relaxed** — Allows log in using FIPS 140-2-compliant cryptographic modules and fallback modules. SRP will not be used.
   - **Strict** — Allows log in using only FIPS 140-2-compliant cryptographic modules.
3. Click **OK**.

> **TIP**
>
> The client setting does not need to match the site setting. The client can log in to sites that use a different FIPS mode.

Running Software as a Network Service

It may be beneficial to run your Avigilon software service as a network service account instead of using a regular user account. The network service account can be set up to only have the relevant permissions to run the required services.

To switch the service to run as a network service account:

1. Open the **Windows Services** app.
2. In the list of services, find the service with Avigilon software as both the Name and Description. Right-click the Avigilon software service and select **Properties**.
3. Click the **Log On** tab.
4. If not already selected, select the **This Account** radial button.

   Enter `NT AUTHORITY\NetworkService` in the **This Account** field. Leave the **Password** field blank.
5. Click **OK**.

Changing from LAN to WAN

The Server will not be able to detect connected cameras in local area network (LAN) mode if the Internet Control Message Protocol (ICMP) on your network is disabled or blocked.

Change the camera's network type to wide area network (WAN) mode before disabling ICMP to keep cameras connected to the server.

Selecting WAN mode will encrypt communications with your device.

1. In the site Setup tab, click .
2. Select the device connections you want to edit from the Connected Devices list.
3. Click **Edit...**.
4. In the Network Type: drop-down list, select **WAN**.
5. Click **OK**.

Managing Subnets

Subnets can be created for groups of users that allow them to connect to the Server through separate network connections. Avigilon recommends dividing users into groups based on the privileges they are assigned and managing them through either Active Directory or a Windows Workgroup. Each group can then connect to the Server through their respective subnet. Subnets can also be used to limit a device or component to only communicate with the Server and not have access to the wider network.

For more information

The following documents can provide additional guidance:

- CIS CSC 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches (cisecurity.org/controls/)
- NIST SP 800-53 AC-2: Account Management
- NIST SP 800-53 SC-7: Boundary Protection

Configuring the Firewall

Only enable the ports needed for services being used on your System. Any open unused ports pose a security risk.

CAUTION

Avigilon does not recommend connecting your System to the internet. If internet connection is a necessity for your System, use a well configured firewall.

Camera Ports

Default Port	Services	Transport	Encrypted
443	Web Interface, ONVIF	HTTPS	Yes
3702	ONVIF Device Discovery	UDP Multicast 239.255.255.250	No
51000-54999*	RTP/RTCP	UDP	No
554	RTSP	TCP	No
161	SNMP	UDP	No

* These default ports will depend on the Server settings, which are configurable. If the Server settings for RTP/RTCP are changed, the camera ports will require the same update.

Server Ports

These ports apply to both Unity and ACC Systems.

Default Port	Services	Transport	Encrypted	Optional
38880*	(limited)	HTTP	No	Yes
38881	Video (WAN) Rest API PBRPC API	HTTPS	Yes with forward secrecy TLS-SRP (mutual) with self-signed certificate TLS with self-signed certificate (pinned) TLS with user certificate (Client or mutual)	No
38882	Synchrony for Server to other Servers (reliable ordered broadcast)	UDP	No	No
38883*	Server Discovery for Clients	UDP Multicast 239.255.255.250	No	Yes‡
38884	NTP	UDP	No	Yes**
3702	ONVIF Device Discovery	UDP Multicast 239.255.255.250	No	Yes

Default Port	Services	Transport	Encrypted	Optional
51000-55000	RTP/RTCP	UDP	No	Yes‡‡
59595	Pelco device driver (SOAP)	HTTP	No	Yes
39990	REST	HTTP	No	No
8443	Web Endpoint for Mobile app	HTTPS	Connections negotiated using trusted certificates. Traffic is encrypted using SSL / TLS 1.2	Yes
8444	Web Endpoint for Server	HTTPS	Connections negotiated using trusted certificates. Traffic is encrypted using SSL / TLS 1.2	Yes
443	ACS initial connection and WebRTC signaling	HTTPS	Connections negotiated using trusted certificates. Traffic is encrypted using SSL / TLS 1.2	No
25	SMTP	HTTPS	Connections negotiated using trusted certificates. Traffic is encrypted using SSL / TLS 1.2	Yes

* These ports are closed by default on Avigilon's hardened NVRs. If you are hardening your own System, make sure to block these ports.

‡ This port is optional if you are not using site families to group multiple Servers. When site families are created with multiple Servers, this port should be open for Server to Server communication.

** The camera and Server times must be synchronized to connect. The simplest method for this is through the NTP Server. If you choose to close this NTP port, you will have to use another method to synchronize the camera and Server times. For more information, see *Setting the Date and Time* on page 24.

‡‡ These RTP/RTCP ports are used for streaming camera video over LAN. If you disable these ports, you must enable camera streaming over WAN to access your camera video. For more information, see *Changing from LAN to WAN* on page 47, and *Encrypting Video* on the next page.

NOTE

Changing the base HTTP port, 38880, will also update the service ports used by the Server software (38881 and 38882).
Changing the base RTP port, 51000, will also update the related RTP ports used by the Server software (51000-55000).

Unity Video Server Ports

These ports apply to Unity Video Servers in addition to the ports in the previous table.

Default Port	Services	Transport	Encrypted	Optional
38980	Database replication	Postgres	Yes with forward secrecy	No
38981	Database	Postgres	TLS-SRP (mutual) with self-signed certificate	No
38982	Clustering (Gossip)	HTTPS	TLS with self-signed certificate (pinned)	No
38983	Clustering (MQTT)	MQTT	TLS with user certificate (Client or mutual)	No

For more information

The following documents can provide additional guidance:

- CIS CSC 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches (cisecurity.org/controls/)
- NIST SP 800-53 CA-3: Information Exchange
- NIST SP 800-53 CM-6: Configuration Settings
- NIST SP 800-53 AC-2: Account Management
- NIST SP 800-53 SC-7: Boundary Protection

Encrypting Video

To improve the security of your System you have the option of encrypting live video that your Client receives from sites. Recorded video is always encrypted. You can encrypt video from all sites, or choose specific sites that will use encrypted video.

IMPORTANT

While it improves the security of the video communication, encrypting video will also increase the load on your Network Video Recorder, which can negatively impact the throughput performance of the NVR by up to 30%.

Encrypting Video from All Sites

1. In the top-right corner of the Client, select ⚙ > **Client Settings**.
2. In the Security tab, select the **Encrypt video from all sites** checkbox.
3. Click **OK**.

This setting will enforce encrypted video for any new video streams on your Client. Any previously established connections will continue using their configured settings.

Encrypting Video from Specific Sites

1. In the top-right corner of the Client, select ⚙ > **Client Settings**.
2. In the Site Networking tab, find and select a site that will use encrypted video from the list.
3. In the **Connection Type:** drop-down list, select **WAN (Secured)**.

   Repeat this step for any other sites that should use encrypted video.

4. Click **OK**.

Securing Devices

Complete the steps in the following sections to harden devices connected to your security System.

Using the Camera Configuration Tool to Apply Settings to Multiple Cameras

The Camera Configuration Tool allows you to configure all Avigilon cameras that are discovered on your network. You can apply common settings to multiple cameras at the same time, or adjust individual cameras to fit your site requirements.

You will need the following to use this tool:

- All the cameras you are configuring have been installed and are physically connected to the network.
- The Camera Configuration Tool is installed on a computer that has access to the same network as the cameras.
- You know the password for all the cameras.

For more information, see the Camera Configuration Tool User Guide.

By default, the Camera Configuration Tool will try to connect to cameras using secure HTTPS. If a secure connection is unavailable, the tool will use HTTP. You can manage these network settings.

Securely connected cameras will display one of the icons 🔒, 🔒, 🔓 or ❌ next to their camera status.

Disabling HTTP Connections in the Camera Configuration Tool

By default, the Camera Configuration Tool will try to connect to cameras using secure HTTPS. If a secure connection is unavailable, the tool will use HTTP.

For increased security, you can prevent the Camera Configuration Tool from connecting over HTTP if secure connections are unavailable. Cameras that cannot connect over HTTPS will appear offline.

1. Close the Camera Configuration Tool application.
2. In Windows Explorer, navigate to the installation folder. By default, this is `C:\Program Files (x86)\Motorola Solutions\Camera Configuration Tool`.
3. Double-click `CCT_DisableHttp.reg` to prevent the application from using HTTP.
4. Click **Yes**, then **OK**.
5. Open the Camera Configuration Tool application.

To re-enable connections over HTTP:

1. Close the Camera Configuration Tool application.
2. In Windows Explorer, navigate to the installation folder. By default, this is `C:\Program Files (x86)\Motorola Solutions\Camera Configuration Tool`.

3. Double-click `CCT_EnableHttp.reg`.
4. Click **Yes**, then **OK**.
5. Open the Camera Configuration Tool application.

Resetting Devices to Default Settings Before Deploying

Before deploying a device, Avigilon recommends that you reset the device to its factory default settings to ensure that the device is in a known default state. You can do this remotely through the camera's web interface, or physically at the camera by using a paperclip or similar tool to press and hold the factory revert button for 3 seconds

See your device's User Manual for instructions on locating the factory revert button and resetting it to factory default settings.

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.

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

Normally if you restore the 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.

1. At the bottom of the Users page, select the **Do not clear usernames or passwords on firmware revert** check box.
2. After you select the check box, the following popup message appears:

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

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

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

Creating a Backup Admin Account

Avigilon recommends creating a backup admin account for your device with a different password than the primary administrator account. This will help 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 with the Camera Configuration Tool (CCT):

> **NOTE**
>
> You can also create additional user accounts with the camera web interface. For more information, see *Securing User Accounts* on page 17.

1. In the Camera Configuration Tool, select the **Admin Users** tab.
2. In the Secondary Admin User Name column, enter a new username.

   If you want to use the same username for all cameras, click (icon) then enter the username.
3. In the Secondary Admin Password column, enter a password for the new user.

   If you want to use the same password for all cameras, click (icon) then enter the password.

   > **TIP**
   >
   > Select the checkbox next to the password field to see your entry.
4. Click **Apply**.

You can add more admin users with the camera web interface, however the Camera Configuration Tool will only display the default administrator user and one other admin user on this tab.

Enabling FIPS 140-2 Camera Communications

You can enable compliance with the Federal Information Processing Standard (FIPS) 140-2 Level 1 Security Requirements for Cryptographic Modules for Server and camera communication as an option to the standard OpenSSL cryptographic engine in the Client, the Camera Configuration Tool, or the camera's web interface.

> **NOTE**
>
> FIPS 140-2 Level 1 requires the purchase of a FIPS camera license.

Setting the Encryption Mode in the Client

The following steps are completed using the Client.

FIPS 140-2 Level 1 encryption requires that you have the CAM-FIPS license in addition to the standard camera channel license for each camera.

To select an encryption engine to be used on an Avigilon device:

1. In the New Task menu , click **Site Setup**.
2. Select a device, then click **Network**.
3. Select **FIPS 140-2 Level 1** from the Encryption Mode: list to enable encrypted communications for the device. Enabling FIPS 140-2 Level 1 may cause your device to reboot.
4. Click **OK**.

For more information

The following documents can provide additional guidance:

- Unity Video Help Center
- ACC 7 Help Center

Setting the Encryption Mode in CCT

The following steps are completed using the Camera Configuration Tool. For more information about using the Camera Configuration Tool, see the Camera Configuration Tool User Guide.

1. Select the **TLS** tab.
2. In the **Encryption Mode** column, use the drop-down list for each camera to select the type of encryption to use:
   - **OpenSSL** is the default option for encryption.
   - **FIPS 140-2 Level 1** enables FIPS 140-2 level 1 encryption.
3. At the bottom-right corner of the window, click **Apply**.

> **IMPORTANT**
>
> Changing this setting on your camera will require your camera to reboot and you will lose the video stream for that time. Avigilon recommends that you apply this setting during non-critical operating times. Applying this setting on a single camera can take from 1 to 5 minutes.

The new encryption mode settings are implemented on the cameras.

Setting the Encryption Mode in the Camera Web UI

The following steps are completed using the camera's web interface. For more information about using the camera's web interface, see the appropriate device Camera Web Interface Guide, which can be found at help.avigilon.com.

1. Go to the AdvancedNetwork setup page.
2. In the Encryption Engine drop-down list, select the type of encryption to use:
   - **Open SSL** is the default option for encryption.
   - **FIPS 140-2** enables FIPS 140-2 level 1 encryption.

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

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

Configuring 802.1x Port-Based Authentication

If your network requires 802.1x port-based authentication, you can set up the appropriate camera credentials in the camera's web interface so that the video stream is not blocked.

1. In the left-menu pane, select **Network** > **802.1x**.
2. On the Configure 802.1x Profiles page, select the preferred authentication method. You can configure multiple profiles. Be aware that you can only enable one profile at a time.

   From the **EAP Method** drop-down list, select one of the following and complete the related fields:

   - Select **PEAP** for username and password authentication.
     - **Configuration Name:** give the profile a name.
     - **EAP Identity:** enter the username that will be used to authenticate the camera.
     - **Password:** enter the password that will be used to authenticate the camera.
   - Select **EAP-TLS** for certificate authentication.
     - **Configuration Name:** give the profile a name.
     - **EAP Identity:** enter the username that will be 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 the password here.
     - Click **Upload Files** and the TLS client certificate and private key are uploaded to the camera. The uploaded files are used to generate a unique certificate to authenticate the camera. The unique certificate is displayed in the Uploaded Certificate field.
3. Click **Save Config** to save the authentication profile.

   If this is the first profile added to the camera, it is automatically enabled.

   Saved configurations are listed under **Saved 802.1x Configurations**.

> **NOTE**
>
> 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**.

Disabling Discovery Services

Discovery protocols are support services that make it easier to find the cameras on the network. Avigilon recommends disabling the auto-discovery protocol, the UDP Multicast discovery protocol, after deploying the cameras and System as an additional hardening step to stop the Server from scanning the network for new devices.

After disabling auto-discovery new devices can be added to the System by manually discovering and adding them. For more information on manually discovering devices, see the Help Center.

To disable auto-discovery services:

1. On your Server, find the **VmsDaemonConfig.cfg** file, located in the same folder as Server installer.
2. Open the **VmsDaemonConfig.cfg** file with a text editor such as notepad.
3. Add the following lines inside of the *<Root>* element of the XML data:

```
<DevClient>
 <DeviceDriverAvigilon>
  <ConfigItem name="AvigilonDiscoveryEnable" type="Boolean" value="0"/>
 </DeviceDriverAvigilon>
 <DeviceDriverOnvif>
  <ConfigItem name="OnvifDiscoveryEnable" type="Boolean" value="0"/>
 </DeviceDriverOnvif>
</DevClient>
```

TIP

Value 1 = enabled. Value 0 = disabled.

4. Save the changes to the **VmsDaemonConfig.cfg** file.
5. Reboot the Server to have the changes take effect.

For more information

The following documents can provide additional guidance:

- Unity Video Help Center
- ACC 7 Help Center

Enabling Video Stream Encryption

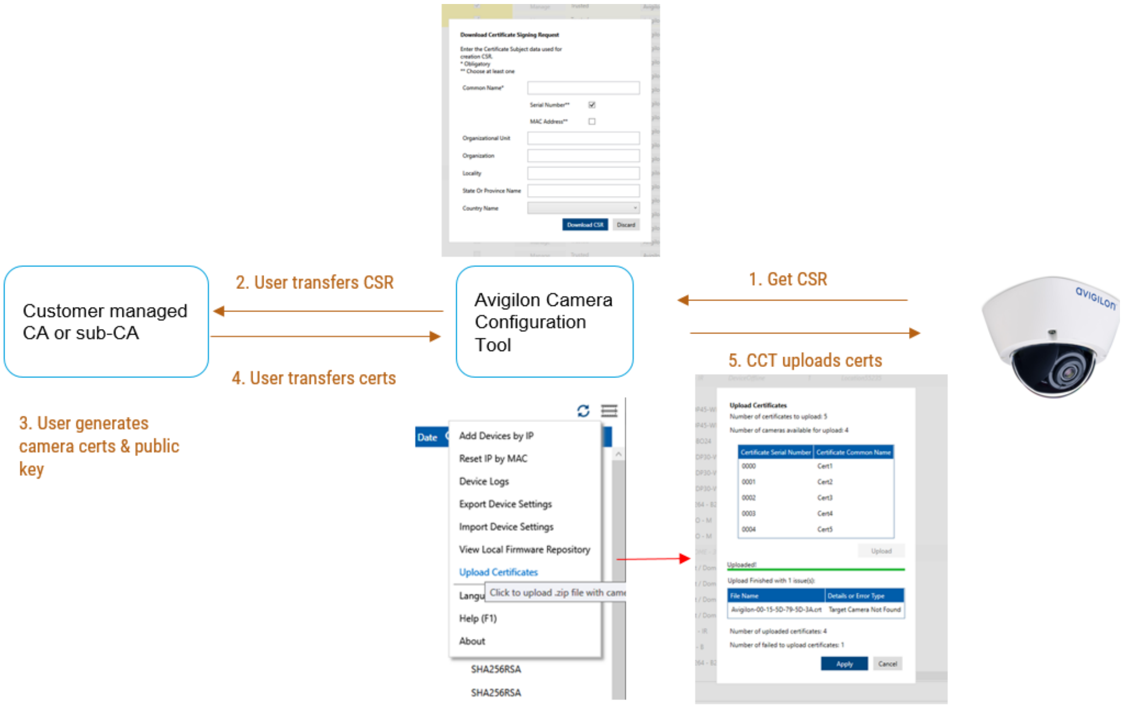
Avigilon recommends accessing the camera using HTTPS, which encrypts the traffic between the Client and the camera. All camera administrative tasks should go through HTTPS. Video streamed over RTP/RTSP is still unencrypted. If the video stream contains sensitive data, tunnel RTP/RTSP over HTTPS.

A self-signed certificate is sufficient for providing encryption, but the web browser will warn that the certificate cannot be validated. A CA-signed certificate is needed for the Server to authenticate that it is accessing the correct camera. If these types of secure network communication are not used, credentials may get compromised and attackers might use them to access the System.

For more information, see *Using Self-Signed Certificates* on page 39 and *Encrypting Video* on page 50.

Managing Camera Certificates with CCT

You can manage and configure secure network connections in bulk using the Camera Configuration Tool. The diagram below shows the basic workflow for setting up CA or sub-CA certificates with CCT on your Avigilon cameras.



Download Certificate Signing Request

Enter the Certificate Subject data used for creation CSR.
* Obligatory
** Choose at least one

Common Name*

Serial Number** ☑

MAC Address** ☐

Organizational Unit

Organization

Locality

State Or Province Name

Country Name

Download CSR | Discard

Upload Certificates

Number of certificates to upload: 5

Number of cameras available for upload: 4

Certificate Serial Number	Certificate Common Name
0000	Cert1
0001	Cert2
0002	Cert3
0003	Cert4
0004	Cert5

Upload

Uploaded!

Upload Finished with 1 issue(s):

File Name	Details or Error Type
Avigilon-00-15-5D-79-5D-3A.crt	Target Camera Not Found

Number of uploaded certificates: 4

Number of failed to upload certificates: 1

Apply | Cancel

Downloading a Certificate Signing Request

Download a Certificate Signing Request (CSR) for each camera, or multiple cameras. The CSR must be signed by a certificate authority (CA) to apply it to a camera.

1. Select the **TLS** tab.
2. In the Download CSR column, select the checkbox for the camera(s).
3. Click **Apply**.
4. Enter a **Common Name** for the CSRs. Maximum 64 characters, including the 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. This is a useful identifier when downloading CSRs for multiple cameras. Options are: None, Counter, Name of the camera, Location of the camera, Hostname of the camera, IP address of the camera, MAC address of the camera, Serial number of the camera, Common Name of the current certificate, or Autogenerated hex number.
   - **Suffix**: Enter a suffix for the Common Name.

5. Enter a **Subject Alternative Name** for the CSRs. A preview is displayed as you enter a value.
   - To enter a user specified Subject Alternative Name, select **User input** as the **Source of data** and enter the name in **Value of Subject Alternative Name** field.
   - To enter a camera identifier as the Subject Alternative Name, select one of the following options from the **Source of data** drop-down list: A copy of the Common Name, Hostname of the camera, IP address of the camera, or First Subject Alternative Name of the current certificate.
6. Enter the following optional fields:
   - **Organizational Unit** — The division of an organization.
   - **Organization** — The organization name.
   - **Locality** — The city where the organization is located.
   - **State or Province** — The state or province where the organization is located.
   - **Country** — The 2-letter country code.
7. Click **Download CSR** and select where to save the CSR.

The CSR will be downloaded as a zip file. Submit this to a CA to be signed.

Uploading Signed Certificates

Once the CSRs have been signed by a CA, zip up all the certificates to upload into the Camera Configuration Tool.

> **NOTE**
>
> - Signed certificate files that you add to the zip file must have specific file extensions such as *.crt*, *.cer*, or *.pem*.
> - To see which cameras have trusted certificates in the Camera Configuration Tool, you will also need to add the CA certificate file to the same zip file as the signed certificate(s).

1. In the top-right corner, select ☰ > **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**.

The uploaded certificates can now be applied to their respective devices.

Applying Certificates

After you upload signed certificates, you can select which certificate to use for each device.

1. Select the **TLS** tab.
2. In the TLS Certificate Subject column, select a certificate.
3. Click **Apply**.

TIP

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

Deleting Certificates

You can remove invalid, expired, self-signed or unwanted certificates from a camera connected with the Camera Configuration Tool.

NOTE

- You cannot delete a certificate that is Currently Active. Apply a different certificate, and then delete the unused certificate.
- You cannot delete a certificate when you are editing other settings in the Camera Configuration Tool. Apply or Discard your changes before deleting a certificate.

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

Managing Device Certificates in Avigilon Software

Once you have set up CA or sub-CA certificates on your cameras and devices, you will need to add those certificates to the Trust Store of your Sites. Once the devices and System have been set up to use custom trusted certificates, you should disable trusting the Avigilon certificate authority and the default self-signed certificates. It is recommended to use the Device certificate report to verify if any connected devices do not have trusted certificates properly set up before disabling trust of the default Avigilon certificate authority.

Adding Device Certificates

Each custom camera and device signing certificate, intermediate certificate, or root certificate authority should be installed on the Server's local computer certificate Trust Store. Install your device certificates using the Microsoft Management Console (MMC):

1. Select **Run** in the **Start** menu and enter *mmc*.
2. In MMC, click the **File** menu and select **Add/Remove Snap-in**.
3. Select the **Certificates** option in the left panel and click **Add**.
4. Select to the manage the certificates for the **Computer account** and click **Next**.
5. Select **Local computer** and click **Next**.

6. In the right panel, ensure that `Certificates (Local Computer)` is selected and click **OK**.
7. Right-click on one of the following options. Make sure to choose the option that applies to your certificate:
   - **Intermediate Certification Authorities**: For certificates issued by Intermediate CAs.
   - **Trusted Root Certification Authorities**: For certificates issued by Trusted Root CAs.
8. Select **All Tasks** > **Import**.
9. Use **Browse** to locate and select the intermediate or root certificate you are installing. Then click **Next**.
10. Choose the option to `Automatically select the certificate store based on the type of certificate` and click **Next**.
11. Click **Finish**.

Disabling the Default Device Certificates

Once you have set up CA or sub-CA certificates on your cameras and devices and added those certificates to the Trust Store of your Sites, disable trust in the default device certificates to ensure that the custom certificates are the only ones that can be used.

> **IMPORTANT**
>
> Make sure that you have set up trusted certificates on your devices before disabling trust for the Avigilon certificate authority. If any connected devices do not have trusted certificates properly setup, you will receive an error message and won't be able to select this checkbox.
>
> Click **Device certificate report** to generate a report of all devices that do not meet the certificate requirements.

1. In the New Task menu , click **Site Setup**.
2. Select a site, then click **Security**.
3. Select the **Require trusted device certificates:** checkbox under Device Security Settings.
4. Click **OK**.

Troubleshooting Device Certificates

You can use the Device certificate report button to generate a report of all devices that do not meet the trusted certificate requirements.

1. In the New Task menu , click **Site Setup**.
2. Select a site, then click **Security**.
3. Click **Device certificate report**.
4. Use the generated report to identify any cameras that require certificate maintenance because of incorrect or expired certificates.

Enabling HTTPS

Users with administration rights should encrypt traffic between the Clients and the camera. This will require that the Client supports HTTPS.

HTTPS is enabled by default and cannot be disabled. The HTTPS port can be changed in the Camera Configuration Tool or the camera's web interface.

Changing the HTTP or HTTPS Port with CCT

You can select which ports the cameras should use to connect to the network over HTTP and HTTPS.

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

Changing the HTTP or HTTPS Port with the Camera Web Interface

For instructions about changing the HTTPS port with the web interface, see *Setting Up Basic Network Settings* on page 37.

Securing Avigilon Remote Workstations

If you are using Avigilon Remote Monitoring Workstations as clients to connect to the NVR Premium FIPS Series recorder, complete the steps in the following sections to harden the remote monitoring workstation to the same Windows STIG guidelines that the NVR Premium FIPS Series recorder uses.

After enabling the TPM, encrypting your drives with BitLocker and running the Avigilon Workstation Hardening Kit, your Avigilon remote monitoring workstation will be hardened to a certain point and will pass 90% of the applicable STIG scan checklist. The remaining 10%, which can be found at must be hardened manually to achieve full STIG compliance.

> **NOTE**
>
> Avigilon tested the NVR against the STIG versions identified in the guide. It is the responsibility of the end user to determine any additional configuration required for full compliance. Avigilon cannot guarantee the performance of the NVR as specified will remain unchanged after implementing additional hardening changes mandated by the policies of the body governing security for your organization.

Supported Avigilon remote monitoring workstations:

- RM5-WKS-4MN: Remote monitoring workstation for up to 4 monitors.
- RM5-WKS-2MN: Remote monitoring workstation for up to 2 monitors.

For more information

The following documents can provide additional guidance:

- www.stigviewer.com/stigs

Enabling the Trusted Platform Module (TPM)

1. Restart the Avigilon workstation. Press `F2` while the workstation is booting to open the System Setup BIOS Settings.
2. In the left-hand pane, navigate to **Security** > **TPM 2.0 Security**.
3. Select the **TPM On** checkbox.
4. Click **Exit** and then click **Yes** to save your settings.
5. The system will automatically restart. The TPM will now be enabled.

Changing Administrator Account Name and Password

Addresses STIG V-220745 on NVR5, or V-63423 on NVR4X

Before applying the hardening kit, change your Administrator password to meet the 14 character requirement, using a mix of upper and lower cases, numerals, and special characters. Update any other account passwords that are used on the Avigilon workstation to meet the same requirements.

IMPORTANT

After applying the hardening kit, your built-in Administrator account name will be automatically changed to **motosec** to meet STIG compliance. The administrator account created when deploying the workstation, and any other administrator accounts created will be unaffected and can still be used. **Your built-in Administrator account password will not change**, only the account name will be updated. This default built-in account will then be disabled as required by Windows.

Set Passwords to Expire

Addresses STIG V-220716 on NVR5, or V-63371 on NVR4X

To reduce the risk of a password being discovered and used to compromise the system, make sure your account passwords are all set to expire. If an account password is set to never expire, this will be a STIG finding.

1. Run **Computer Management**.
2. Navigate to **System Tools** > **Local Users and Groups** > **Users**.
3. Check each active account by double-clicking it and ensuring the **Password never expires** checkbox is unchecked for all accounts.

Running the Avigilon Workstation Hardening Kit

Avigilon provides a hardening kit to help harden your Avigilon remote monitoring workstation to the same STIG rules as the NVR Premium FIPS Series recorder.

1. Download the **AvigilonSecureWorkstation-X.X.X.X-win10.zip** hardening kit file from the Avigilon Partner Community. Login to the resource center, search for `AvigilonSecureWorkstation-X.X.X.X-win10.zip` and download the file to your remote monitoring workstation.
2. Unzip the workstation hardening kit. Note the location where the hardening kit files will be unzipped.
3. Right-click the **AvigilonSecureWorkstation.bat** file that was unzipped from the hardening kit and select to **Run as Administrator**. This will start the process of hardening your Avigilon workstation and may take up to 5 minutes.
4. Once the batch file has finished running, restart your workstation for the hardening changes to take effect.

IMPORTANT

After running the hardening kit, there will be some remaining STIG vulnerabilities that you must manually comply with if you want the Avigilon workstation to be fully STIG-compliant. See *Remaining STIGs Vulnerabilities to be Addressed* on page 67 for a list of the remaining STIG vulnerabilities.

Encrypting with BitLocker

As part of hardening your Avigilon workstation, you will encrypt your OS drive and data drive using BitLocker. Perform this step after applying the workstation hardening kit.

Before encrypting your drives, ensure that the TPM is enabled by right-clicking the Start menu and selecting **Device Manager**. *Trusted Platform Module* with the version number should display under **Security devices**. If the TPM is not enabled, see *Enabling the Trusted Platform Module (TPM)* on page 63.

Enabling the BitLocker Startup PIN

Addresses STIG V-220703 and V-220704 on NVR5, or V-94859 and V-94861 on NVR4X

Avigilon recommends configuring your BitLocker Drive Encryption group policy for the OS drive to require a PIN for additional authentication on startup:

1. Open the Local Group Policy Editor and go to the policy for **Computer Configuration** > **Administrative Templates** > **Windows Components** > **BitLocker Drive Encryption** > **Operating System Drives**.
2. Double-click **Require additional authentication at startup** and set it to **Enabled**.
3. Ensure the **Allow BitLocker without a compatible TPM** checkbox is not checked.
4. Select **Do not allow TPM** from the **Configure TPM startup** drop-down list.
5. Select **Require startup PIN with TPM** from the **Configure TPM startup PIN** drop-down list.
6. Select **Do not allow startup key with TPM** from the **Configure TPM startup key** drop-down list.
7. Select **Do not allow startup key and PIN with TPM** from the **Configure TPM startup key and PIN** drop-down list.
8. Click **Apply** and **OK**.
9. Double-click **Configure minimum PIN length for startup** and set it to **Enabled**.
10. Set the **Minimum characters** for the PIN to **6** or more characters.
11. Click **Apply** and **OK**

NOTE

After updating the group policy, use the command line to run **gpupdate** and then restart the machine for the settings to take effect. For more information on using gpupdate, see Microsoft's documentation.

Encrypting the OS Drive

1. Use the **Windows key** + **S** to open the search bar. Search for and open the **Control Panel**.
2. Click **System and Security** > **BitLocker Drive Encryption**.

   NOTE

   You will be asked to set a 6-20 character PIN for your BitLocker OS drive. Enter your PIN and click **Set PIN** to save it. This PIN will be required when you startup your system. Save this PIN in a secure location.

3. Click **Turn on BitLocker** for the *Operating system drive*.This will be your C: drive.

4. Choose how you would like to back up your recovery key, and click **Next**.

> **NOTE**
>
> Whatever method you choose to back up the recovery key, make sure to store it securely, as this key will be needed to recover the data if there is a system failure.

5. Select an encryption option of either **Encrypt used disk space only** or **Full Disk Encryption** and click **Next**.

   Selecting to encrypt the full disk is recommended for workstations that have already been in use for some time. Be aware that the full disk encryption could take approximately 10-12 hours.

6. Select **New encryption mode** and click **Next**.
7. Check the **Run BitLocker system check** checkbox and click **Continue**.
8. Restart the Avigilon workstation to start the encryption process.

   You can check the status of the drive encryption at **Control Panel** > **System and Security** > **Manage BitLocker**.

Encrypting the Data Drive

1. Use the **Windows key** + **S** to open the search bar. Search for and open the **Control Panel**..
2. Click **System and Security** > **Manage BitLocker**.
3. Click **Turn on BitLocker** for the data volume you want to encrypt under *Fixed data drives*. This will be your D: drive.
4. Select to **Automatically unlock this drive on this computer** and click **Next**.
5. Choose how you would like to back up your recovery key, and click **Next**.

> **NOTE**
>
> Whatever method you choose to back up the recovery key, make sure to store it securely, as this key will be needed to recover the data if there is a system failure.

6. Select an encryption option of either **Encrypt used disk space only** or **Full Disk Encryption** and click **Next**.

   Selecting to encrypt the full disk is recommended for workstations that have already been in use for some time. Be aware that the full disk encryption could take approximately 10-12 hours.

7. Select **New encryption mode** and click **Next**.
8. Click **Start encrypting** to start the encryption process. This process may take several hours depending on the drive size.

Enabling Secure Boot

Addresses STIG V-220700 on NVR5, or V-77085 on NVR4X

To enable your Avigilon workstation to use Secure Boot:

1. Use the **Windows key** + **S** to open the search bar. Search for and open **System Information**.
2. Under **System Summary**, locate the **Secure Boot State** line and check its status. If the **Secure Boot State** is set to **Off**, use the following steps to turn it on.
3. Use the **Windows key** + **S** to open the search bar. Search for and open **Settings**.
4. Go to **Update and Security** > **Recovery**. Under **Advanced Startup**, click **Restart Now**.
5. Once prompted, select **Troubleshoot** > **UEFI Firmware Settings** > **Restart** and click **Next**.
6. Under **Settings**, locate **Secure Boot**.
7. Select the **Secure Boot Enable** checkbox.
8. Click **Apply** and **Exit** to continue restarting the system and apply the setting.

   After restarting, repeat steps 1 and 2 to check that Secure Boot is now enabled.

Starting Windows Credential Guard Services

On an Avigilon remote monitoring workstation that will be joining a domain, you must start running Windows Credential Guard services to meet STIG requirements. You will need to perform this fix by editing a group policy:

1. Open the Local Group Policy Editor and go to the policy for **Computer Configuration** > **Administrative Templates** > **System** > **Device Guard**.
2. Set the **Turn On Virtualization Based Security** option to **Enabled**, with the following settings:
   - **Enabled with UEFI lock** selected for the **Credential Guard Configuration** setting.
   - **Secure Boot** or **Secure Boot and DMA Protection** selected for the **Select Platform Security Level:** setting.
3. Click **Apply** and **OK**.

NOTE

After updating the group policy, use the command line to run **gpupdate** and then restart the machine for the settings to take effect. In some cases, the settings may not apply until the machine is restarted a second time.
For more information on using gpupdate, see Microsoft's documentation.

Remaining STIGs Vulnerabilities to be Addressed

After enabling the TPM, encrypting your drives with BitLocker and running the Avigilon Workstation Hardening Kit, your Avigilon remote monitoring workstation will be hardened to a certain point and will pass 90% of the applicable STIG scan checklist. The remaining 10% must be hardened manually to achieve full STIG compliance.

NOTE

Avigilon tested the NVR against the STIG versions identified in the guide. It is the responsibility of the end user to determine any additional configuration required for full compliance. Avigilon cannot guarantee the performance of the NVR as specified will remain unchanged after implementing additional hardening changes mandated by the policies of the body governing security for your organization.

For more information

The following documents can provide additional guidance:

- www.stigviewer.com/stigs

Windows 10 STIG Vulnerabilities

The following STIG vulnerabilities were found using the Windows 10 STIG V2R4, SCAP 1.2 for NVR5, or V1R17 SCAP 1.2 for NVR4X.

	Vuln ID	Title, Description, and Fix Text	Resolution
1	**NVR5:** V-220702 **NVR4X:** V-63337	**Windows 10 information Systems must use BitLocker to encrypt all disks to protect the confidentiality and integrity of all information at rest.** Description: If data at rest is unencrypted, it is vulnerable to disclosure. Even if the operating System enforces permissions on data access, an adversary can remove non-volatile memory and read it directly, thereby circumventing operating System controls. Encrypting the data ensures that confidentiality is protected even when the operating System is not running. Fix: Enable full disk encryption on all information Systems (including SIPRNet) using BitLocker. BitLocker, included in Windows, can be enabled in the Control Panel under "BitLocker Drive Encryption" as well as other management tools. NOTE: An alternate encryption application may be used in lieu of BitLocker providing it is configured for full disk encryption and satisfies the pre-boot authentication requirements (WN10-00-000031 and WN10-00-000032).	Resolved using fix text instructions.
2	**NVR5:** V-220717 **NVR4X:** V-63373	**Permissions for System files and directories must conform to minimum requirements.** Description: Changing the System's file and directory permissions allows the possibility of unauthorized and anonymous modification to the operating System and installed applications. Fix: Maintain the default file System permissions and configure the Security Option: "Network access: Let everyone	Resolved using fix text instructions.

	Vuln ID	Title, Description, and Fix Text	Resolution
		permissions apply to anonymous users" to "Disabled" (WN10-SO-000160).	
3	**NVR5:** V-220719 **NVR4X:** V-63381	**Simple Network Management Protocol (SNMP) must not be installed on the System.** Description: Some protocols and services do not support required security features, such as encrypting passwords or traffic. Fix: Uninstall "Simple Network Management Protocol (SNMP)" from the System. Run "Programs and Features". Select "Turn Windows Features on or off". De-select "Simple Network Management Protocol (SNMP)".	Resolved using fix text instructions.
4	**NVR5:** V-220740 **NVR4X:** V-63409	**The number of allowed bad logon attempts must be configured to 3 or less.** Description: The account lockout feature, when enabled, prevents brute-force password attacks on the System. The higher this value is, the less effective the account lockout feature will be in protecting the local System. The number of bad logon attempts must be reasonably small to minimize the possibility of a successful password attack, while allowing for honest errors made during a normal user logon. Fix: Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Account Policies >> Account Lockout Policy >> "Account lockout threshold" to "3" or less invalid logon attempts (excluding "0" which is unacceptable).	Resolved using fix text instructions.
5	**NVR5:** V-220745 **NVR4X:** V-63423	**Passwords must, at a minimum, be 14 characters.** Description: Information Systems not protected with strong password schemes (including passwords of minimum length) provide the opportunity for anyone to crack the password, thus gaining access to the System and compromising the device, information, or the local network. Fix: Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Account Policies >> Password Policy >> "Minimum password length" to "14" characters.	Resolved using fix text instructions.
6	**NVR5:** V-250319 **NVR4X:** V-63577	**Hardened UNC Paths must be defined to require mutual authentication and integrity for at least the \\*\SYSVOL and \\*\NETLOGON shares.** Description: Additional security requirements are applied to Universal Naming Convention (UNC) paths specified in	Resolved using fix text instructions.

	Vuln ID	Title, Description, and Fix Text	Resolution
		Hardened UNC paths before allowing access them. This aids in preventing tampering with or spoofing of connections to these paths. Fix: Configure the policy value for Computer Configuration >> Administrative Templates >> Network >> Network Provider >> "Hardened UNC Paths" to "Enabled" with at least the following configured in "Hardened UNC Paths:" (click the "Show" button to display). Value Name: \\*\SYSVOL Value: RequireMutualAuthentication=1, RequireIntegrity=1 Value Name: \\*\NETLOGON Value: RequireMutualAuthentication=1, RequireIntegrity=1	
7	**NVR5:** V-220903 **NVR4X:** V-63579	**The DoD Root CA certificates must be installed in the Trusted Root Store.** Description: To ensure secure DoD websites and DoD-signed code are properly validated, the System must trust the DoD Root Certificate Authorities (CAs). The DoD root certificates will ensure the trust chain is established for Server certificates issued from the DoD CAs. Fix: Install the DoD Root CA certificates: • DoD Root CA 3 • DoD Root CA 4 • DoD Root CA 5 The certificates can be installed using the InstallRoot tool. The InstallRoot tool is available on Cyber Exchange at https://public.cyber.mil/pki-pke/pkipke-document-library/	https://public.cyber.mil/pki-pke/pkipke-document-library/ Search "InstallRoot".
8	**NVR5:** V-220904 **NVR4X:** V-63583	**The External Root CA certificates must be installed in the Trusted Root Store on unclassified Systems.** Description: To ensure secure websites protected with External Certificate Authority (ECA) Server certificates are properly validated, the System must trust the ECA Root CAs. The ECA root certificates will ensure the trust chain is established for Server certificates issued from the External CAs. This requirement only applies to unclassified Systems. Fix: Install the ECA Root CA certificates on unclassified Systems: • ECA Root CA 2 • ECA Root CA 4	https://public.cyber.mil/pki-pke/pkipke-document-library/ Search "InstallRoot".

	Vuln ID	Title, Description, and Fix Text	Resolution
		The certificates can be installed using the InstallRoot tool. The InstallRoot tool is available on Cyber Exchange at https://public.cyber.mil/pki-pke/pkipke-document-library/	
9	**NVR5:** V-220905 **NVR4X:** V-63587	**The DoD Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified Systems.** Description: To ensure users do not experience denial of service when performing certificate-based authentication to DoD websites due to the System chaining to a root other than DoD Root CAs, the DoD Interoperability Root CA cross-certificates must be installed in the Untrusted Certificate Store. This requirement only applies to unclassified Systems. Fix: Install the DoD Interoperability Root CA cross-certificates on unclassified Systems. Issued To - Issued By - Thumbprint • DoD Root CA 3 - DoD Interoperability Root CA 2 - AC06108CA348CC03B53795C64BF84403C1DBD341 • DoD Root CA 3 - DoD Interoperability Root CA 2 - 49CBE933151872E17C8EAE7F0ABA97FB610F6477 The certificates can be installed using the InstallRoot tool. The InstallRoot tool is available on Cyber Exchange at https://public.cyber.mil/pki-pke/pkipke-document-library/	https://public.cyber.mil/pki-pke/pkipke-document-library/ Search "InstallRoot".
10	**NVR5:** V-220906 **NVR4X:** V-63589	**The US DoD CCEB Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified Systems.** Description: The US DoD CCEB Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified Systems. Fix: Install the US DoD CCEB Interoperability Root CA cross-certificate on unclassified Systems. Issued To - Issued By - Thumbprint • DoD Root CA 3 - US DoD CCEB Interoperability Root CA 2 - AF132AC65DE86FC4FB3FE51FD637EBA0FF0B12A9 The certificates can be installed using the InstallRoot tool. The InstallRoot tool ais available on Cyber Exchange at https://public.cyber.mil/pki-pke/pkipke-document-library/	https://public.cyber.mil/pki-pke/pkipke-document-library/ Search "InstallRoot".
11	**NVR5:** V-220799 **NVR4X:** V-63597	**Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain Systems.** Desription: A compromised local administrator account can provide means for an attacker to move laterally between	Resolved using fix text instructions.

	Vuln ID	Title, Description, and Fix Text	Resolution
		domain Systems. With User Account Control enabled, filtering the privileged token for built-in administrator accounts will prevent the elevated privileges of these accounts from being used over the network. Fix: Configure the policy value for Computer Configuration >> Administrative Templates >> MS Security Guide >> "Apply UAC restrictions to local accounts on network logons" to "Enabled". This policy setting requires the installation of the SecGuide custom templates included with the STIG package. "SecGuide.admx" and "SecGuide.adml" must be copied to the \Windows\PolicyDefinitions and \Windows\PolicyDefinitions\en-US directories respectively.	
12	**NVR5:** V-220820 **NVR4X:** V-63633	**Local users on domain-joined computers must not be enumerated.** Description: The username is one part of logon credentials that could be used to gain access to a System. Preventing the enumeration of users limits this information to authorized personnel. Fix: This requirement is applicable to domain-joined Systems, for standalone Systems this is NA. Configure the policy value for Computer Configuration >> Administrative Templates >> System >> Logon >> "Enumerate local users on domain-joined computers" to "Disabled".	Resolved using fix text instructions.
13	**NVR5:** V-220920 **NVR4X:** V-63669	**The machine inactivity limit must be set to 15 minutes, locking the System with the screensaver.** Description: Unattended Systems are susceptible to unauthorized use and should be locked when unattended. The screen saver should be set at a maximum of 15 minutes and be password protected. This protects critical and sensitive data from exposure to unauthorized personnel with physical access to the computer. Fix: Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> "Interactive logon: Machine inactivity limit" to "900" seconds" or less, excluding "0" which is effectively disabled.	Resolved using fix text instructions.
14	**NVR5:** V-220921 **NVR4X:** V-63675	**The required legal notice must be configured to display before console logon.** Description: Failure to display the logon banner prior to a logon attempt will negate legal proceedings resulting from unauthorized access to System resources.	Resolved using fix text instructions.

	Vuln ID	Title, Description, and Fix Text	Resolution
		Fix: Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> "Interactive logon: Message text for users attempting to log on" to the following: You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions: • The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations. • At any time, the USG may inspect and seize data stored on this IS. • Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose. • This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy. • Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.	
15	**NVR5:** V-220922 **NVR4X:** V-63681	**The Windows dialog box title for the legal banner must be configured.** Description: Failure to display the logon banner prior to a logon attempt will negate legal proceedings resulting from unauthorized access to System resources. Fix: Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> "Interactive logon: Message title for users attempting to log on" to "DoD Notice and Consent Banner", "US Department of Defense Warning Statement", or a site-defined equivalent.	Resolved using fix text instructions.

	Vuln ID	Title, Description, and Fix Text	Resolution
		If a site-defined title is used, it can in no case contravene or modify the language of the banner text required in WN10-SO-000075.	
16	**NVR5:** V-220849 **NVR4X:** V-63731	**Local drives must be prevented from sharing with Remote Desktop Session Hosts.** Description: Preventing users from sharing the local drives on their Client computers to Remote Session Hosts that they access helps reduce possible exposure of sensitive data. Fix: Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Remote Desktop Services >> Remote Desktop Session Host >> Device and Resource Redirection >> "Do not allow drive redirection" to "Enabled".	Resolved using fix text instructions.
17	**NVR5:** V-220968 **NVR4X:** V-63871	**The Deny access to this computer from the network user right on workstations must be configured to prevent access from highly privileged domain accounts and local accounts on domain Systems and unauthenticated access on all Systems.** Description: Inappropriate granting of user rights can provide System, administrative, and other high-level capabilities. The "Deny access to this computer from the network" right defines the accounts that are prevented from logging on from the network. In an Active Directory Domain, denying logons to the Enterprise Admins and Domain Admins groups on lower trust Systems helps mitigate the risk of privilege escalation from credential theft attacks, which could lead to the compromise of an entire domain. Local accounts on domain-joined Systems must also be assigned this right to decrease the risk of lateral movement resulting from credential theft attacks. The Guests group must be assigned this right to prevent unauthenticated access. Fix: Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> "Deny access to this computer from the network" to include the following. Domain Systems Only: • Enterprise Admins group • Domain Admins group Local account (see Note below)	Resolved using fix text instructions.

	Vuln ID	Title, Description, and Fix Text	Resolution
		All Systems: • Guests group Privileged Access Workstations (PAWs) dedicated to the management of Active Directory are exempt from denying the Enterprise Admins and Domain Admins groups. (See the Windows Privileged Access Workstation STIG for PAW requirements.) Note: "Local account" is a built-in security group used to assign user rights and permissions to all local accounts.	
18	**NVR5:** V-220969 **NVR4X:** V-63873	**The Deny log on as a batch job user right on domain-joined workstations must be configured to prevent access from highly privileged domain accounts.** Description: Inappropriate granting of user rights can provide System, administrative, and other high level capabilities. The "Deny log on as a batch job" right defines accounts that are prevented from logging on to the System as a batch job, such as Task Scheduler. In an Active Directory Domain, denying logons to the Enterprise Admins and Domain Admins groups on lower trust Systems helps mitigate the risk of privilege escalation from credential theft attacks which could lead to the compromise of an entire domain. Fix: This requirement is applicable to domain-joined Systems, for standalone Systems this is NA. Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> "Deny log on as a batch job" to include the following. Domain Systems Only: • Enterprise Admin Group • Domain Admin Group	Resolved using fix text instructions.
19	**NVR5:** V-220970 **NVR4X:** V-63875	**The Deny log on as a service user right on Windows 10 domain-joined workstations must be configured to prevent access from highly privileged domain accounts.** Description: Inappropriate granting of user rights can provide System, administrative, and other high level capabilities. The "Deny log on as a service" right defines accounts that are denied log on as a service. In an Active Directory Domain, denying logons to the Enterprise Admins and Domain Admins groups on lower trust Systems	Resolved using fix text instructions.

	Vuln ID	Title, Description, and Fix Text	Resolution
		helps mitigate the risk of privilege escalation from credential theft attacks which could lead to the compromise of an entire domain. Incorrect configurations could prevent services from starting and result in a DoS. Fix: This requirement is applicable to domain-joined Systems, for standalone Systems this is NA. Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> "Deny log on as a service" to include the following. Domain Systems Only: • Enterprise Admins Group • Domain Admins Group	
20	**NVR5:** V-220971 **NVR4X:** V-63877	**The Deny log on locally user right on workstations must be configured to prevent access from highly privileged domain accounts on domain Systems and unauthenticated access on all Systems.** Description: Inappropriate granting of user rights can provide System, administrative, and other high-level capabilities. The "Deny log on locally" right defines accounts that are prevented from logging on interactively. In an Active Directory Domain, denying logons to the Enterprise Admins and Domain Admins groups on lower trust Systems helps mitigate the risk of privilege escalation from credential theft attacks, which could lead to the compromise of an entire domain. The Guests group must be assigned this right to prevent unauthenticated access. Fix: Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> "Deny log on locally" to include the following. Domain Systems Only: • Enterprise Admins Group • Domain Admins Group Privileged Access Workstations (PAWs) dedicated to the management of Active Directory are exempt from denying the Enterprise Admins and Domain Admins groups. (See the Windows Privileged Access Workstation STIG for PAW	Resolved using fix text instructions.

	Vuln ID	Title, Description, and Fix Text	Resolution
		requirements.) All Systems: • Guests Group	
21	**NVR5:** V-220972 **NVR4X:** V-63879	**The Deny log on through Remote Desktop Services user right on Windows 10 workstations must at a minimum be configured to prevent access from highly privileged domain accounts and local accounts on domain Systems and unauthenticated access on all Systems.** Description: Inappropriate granting of user rights can provide System, administrative, and other high-level capabilities. The "Deny log on through Remote Desktop Services" right defines the accounts that are prevented from logging on using Remote Desktop Services. If Remote Desktop Services is not used by the organization, the Everyone group must be assigned this right to prevent all access. In an Active Directory Domain, denying logons to the Enterprise Admins and Domain Admins groups on lower trust Systems helps mitigate the risk of privilege escalation from credential theft attacks, which could lead to the compromise of an entire domain. Local accounts on domain-joined Systems must also be assigned this right to decrease the risk of lateral movement resulting from credential theft attacks. The Guests group must be assigned this right to prevent unauthenticated access. Fix: Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> "Deny log on through Remote Desktop Services" to include the following. If Remote Desktop Services is not used by the organization, assign the Everyone group this right to prevent all access. Domain Systems Only: • Enterprise Admins group • Domain Admins group • Local account (see Note below) All Systems: • Guests group Privileged Access Workstations (PAWs) dedicated to the	Resolved using fix text instructions.

	Vuln ID	Title, Description, and Fix Text	Resolution
		management of Active Directory are exempt from denying the Enterprise Admins and Domain Admins groups. (See the Windows Privileged Access Workstation STIG for PAW requirements.) Note: "Local account" is a built-in security group used to assign user rights and permissions to all local accounts.	
22	**NVR5:** V-220732 **NVR4X:** V-74719	**The Secondary Logon service must be disabled on Windows 10.** Description: The Secondary Logon service provides a means for entering alternate credentials, typically used to run commands with elevated privileges. Using privileged credentials in a standard user session can expose those credentials to theft. Fix: Configure the "Secondary Logon" service "Startup Type" to "Disabled".	Resolved using fix text instructions.
23	**NVR5:** V-220861 **NVR4X:** V-102617	**The Windows Explorer Preview pane must be disabled for Windows 10.** Description: A known vulnerability in Windows 10 could allow the execution of malicious code by either opening a compromised document or viewing it in the Windows Preview pane. Organizations must disable the Windows Preview pane and Windows Detail pane. Fix: Ensure the following settings are configured for Windows 10 locally or applied through group policy. Configure the policy value for User Configuration >> Administrative Templates >> Windows Components >> File Explorer >> Explorer Frame Pane "Turn off Preview Pane" to "Enabled". Configure the policy value for User Configuration >> Administrative Templates >> Windows Components >> File Explorer >> Explorer Frame Pane "Turn on or off details pane" to "Enabled" and "Configure details pane" to "Always hide".	Resolved using fix text instructions.
24	**NVR5:** V-220946 **NVR4X:** V-102627	**Windows 10 must use multifactor authentication for local and network access to privileged and non-privileged accounts.** Description: Without the use of multifactor authentication, the ease of access to privileged and non-privileged functions is greatly increased. All domain accounts must be enabled for multifactor authentication with the exception of local emergency accounts.	Resolved using fix text instructions.

	Vuln ID	Title, Description, and Fix Text	Resolution
		Multifactor authentication requires using two or more factors to achieve authentication. Factors include: 1. Something a user knows (e.g., password/PIN); 2. Something a user has (e.g., cryptographic identification device, token); and 3. Something a user is (e.g., biometric). A privileged account is defined as an information System account with authorizations of a privileged user. Network access is defined as access to an information System by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, or the internet). Local access is defined as access to an organizational information System by a user (or process acting on behalf of a user) communicating through a direct connection without the use of a network. The DoD CAC with DoD-approved PKI is an example of multifactor authentication. Satisfies: SRG-OS-000106-GPOS-00053, SRG-OS-000107-GPOS-00054, SRG-OS-000108-GPOS-00055 Fix: For non-domain joined Systems, configuring Windows Hello for sign-on options is suggested based on the organization's needs and capabilities.	

Windows Defender STIG Vulnerabilities

The following STIG vulnerabilities were found using the MS Windows Defender Antivirus STIG V2R4.

	Vuln ID	Title, Description, and Fix Text	Resolution
25	**NVR5:** V-213426 **NVR4X:** V-75147	**Microsoft Defender AV must be configured to block the Potentially Unwanted Application (PUA) feature.** Description: After enabling this feature, PUA protection blocking takes effect on endpoint Clients after the next signature update or computer restart. Signature updates take place daily under typical circumstances. PUA will be blocked and automatically quarantined. Fix: Set the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Microsoft Defender Antivirus >> "Configure Detection for Potentially Unwanted Applications" to "Enabled" and "Block".	Resolved using fix text instructions.

	Vuln ID	Title, Description, and Fix Text	Resolution
26	**NVR5:** V-213450 **NVR4X:** V-75237	**Microsoft Defender AV must be configured to perform a weekly scheduled scan.** Description: This policy setting allows you to specify the day of the week on which to perform a scheduled scan. The scan can also be configured to run every day or to never run at all. This setting can be configured with the following ordinal number values: (0x0) Every Day (0x1) Sunday (0x2) Monday (0x3) Tuesday (0x4) Wednesday (0x5) Thursday (0x6) Friday (0x7) Saturday (0x8) Never (default). If you enable this setting a scheduled scan will run at the frequency specified. If you disable or do not configure this setting a scheduled scan will run at a default frequency. Fix: Set the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Microsoft Defender Antivirus >> Scan >> "Specify the day of the week to run a scheduled scan" to "Enabled " and select anything other than "Never" in the drop-down box.	Resolved using fix text instructions.
27	**NVR5:** V-213452 **NVR4X:** V-75241	**Windows Defender AV spyware definition age must not exceed 7 days.** Description: C4 This policy setting allows defining the number of days that must pass before spyware definitions are considered out of date. If definitions are determined to be out of date, this state may trigger several additional actions, including falling back to an alternative update source or displaying a warning icon in the user interface. By default this value is set to 14 days. If this setting is enabled, spyware definitions will be considered out of date after the number of days specified have passed without an update. If this setting is disabled or not configured, spyware definitions will be considered out of date after the default number of days have passed without an update. Fix: Set the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Windows Defender Antivirus >> Signature Updates >> "Define the number of days before spyware definitions are considered out of date" to "Enabled" and select "7" or less in the drop-down box. Do not select a value of 0. This disables the option.	Resolved using fix text instructions.
28	**NVR5:** V-213453 **NVR4X:** V-75243	**Microsoft Defender AV virus definition age must not exceed 7 days.** Description: This policy setting allows defining the number of days that must pass before virus definitions are considered out of date. If definitions are determined to be out of date, this state	Resolved using fix text instructions.

	Vuln ID	Title, Description, and Fix Text	Resolution
		may trigger several additional actions, including falling back to an alternative update source or displaying a warning icon in the user interface. By default, this value is set to 14 days. If this setting is enabled, virus definitions will be considered out of date after the number of days specified have passed without an update. If this setting is disabled or not configured, virus definitions will be considered out of date after the default number of days have passed without an update. Fix: Set the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Microsoft Defender Antivirus >> Signature Updates >> "Define the number of days before virus definitions are considered out of date" to "Enabled" and select "7" or less in the drop-down box. Do not select a value of 0. This disables the option.	

Microsoft Internet Explorer 11 STIG Vulnerabilities

The following STIG vulnerabilities were found using the Microsoft Internet Explorer 11 STIG V2R1, Benchmark.

	Vuln ID	Title, Description, and Fix Text	Resolution
29	**NVR5:** V-223016 **NVR4X:** V-46477	**Check for publishers certificate revocation must be enforced.** Description: Check for publisher's certificate revocation options should be enforced to ensure all PKI signed objects are validated. Fix: If the System is on the SIPRNet, this requirement is NA. Open Internet Explorer. From the menu bar, select "Tools". From the "Tools" drop-down menu, select "Internet Options". From the "Internet Options" window, select the "Advanced" tab from the "Advanced" tab window, scroll down to the "Security" category, and select the "Check for publisher's certificate revocation" box. Note: Manual entry in the registry key: HKCU\Software\Microsoft\Windows\Current Version\WinTrust\Trust Providers\Software Publishing for the value "State", set to "REG_DWORD = 23C00", may first be required.	Resolved using fix text instructions.
30	**NVR5:** V-223071 **NVR4X:** V-46609	**Configuring History setting must be set to 40 days.** Description: This setting specifies the number of days that Internet Explorer keeps track of the pages viewed in the History List. The delete Browsing History option can be accessed using Tools, Internet Options, "General" tab, and then click Settings under Browsing History.	Resolved using fix text instructions.

	Vuln ID	Title, Description, and Fix Text	Resolution
		If you enable this policy setting, a user cannot set the number of days that Internet Explorer keeps track of the pages viewed in the History List. The number of days that Internet Explorer keeps track of the pages viewed in the History List must be specified. Users will not be able to delete browsing history. If you disable or do not configure this policy setting, a user can set the number of days that Internet Explorer tracks views of pages in the History List. Users can delete browsing history. Fix: Set the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Delete Browsing History -> 'Disable Configuring History' to 'Enabled', and enter '40' in 'Days to keep pages in History'.	
31	**NVR5:** V-223122 **NVR4X:** V-46807	**AutoComplete feature for forms must be disallowed.** Description: This AutoComplete feature suggests possible matches when users are filling in forms. It is possible that this feature will cache sensitive data and store it in the user's profile, where it might not be protected as rigorously as required by organizational policy. If you enable this setting, the user is not presented with suggested matches when filling in forms. If you disable this setting, the user is presented with suggested possible matches when filling forms. If you do not configure this setting, the user has the freedom to turn on the auto-complete feature for forms. To display this option, the user opens the Internet Options dialog box, clicks the "Contents" tab, and clicks the "Settings" button. Fix: Set the policy value for User Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> 'Disable AutoComplete for forms' to 'Enabled'.	Resolved using fix text instructions.
32	**NVR5:** V-223124 **NVR4X:** V-46815	**Turn on the auto-complete feature for user names and passwords on forms must be disabled.** Description: This policy setting controls automatic completion of fields in forms on web pages. It is possible that malware could be developed which would be able to extract the cached user names and passwords from the currently logged on user, which an attacker could then use to compromise that user's online accounts. If you enable this setting, the user cannot change the 'User name and passwords on forms' or 'prompt me to save passwords'. The Auto Complete feature for" User names and passwords on forms" will be turned on. If you disable this setting, the user cannot change the 'User name and passwords on forms' or 'prompt me to save passwords'. The Auto Complete feature for "User names and passwords on forms" is turned off. The user also cannot opt to be prompted to save passwords. If you do not configure this setting, the user has the freedom of turning on Auto Complete for "User name and passwords on forms", and the option of prompting to save passwords.	Resolved using fix text instructions.

	Vuln ID	Title, Description, and Fix Text	Resolution
		Fix: Set the policy value for User Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> 'Turn on the auto-complete feature for user names and passwords on forms' to 'Disabled'.	
33	**NVR5:** V-223126 **NVR4X:** V-46829	**Browser must retain history on exit.** Description: Delete Browsing History on exit automatically deletes specified items when the last browser window closes. Disabling this function will prevent users from deleting their browsing history, which could be used to identify malicious websites and files that could later be used for anti-virus and Intrusion Detection System (IDS) signatures. Furthermore, preventing users from deleting browsing history could be used to identify abusive web surfing on government Systems. Fix: Set the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Internet Explorer >> Delete Browsing History >> 'Allow deleting browsing history on exit' to 'Disabled'.	Resolved using fix text instructions.
34	**NVR5:** V-223127 **NVR4X:** V-46841	**Deleting websites that the user has visited must be disallowed.** Description: This policy prevents users from deleting the history of websites the user has visited. If you enable this policy setting, websites the user has visited will be preserved when the user clicks "Delete". If you disable this policy setting, websites that the user has visited will be deleted when the user clicks "Delete". If you do not configure this policy setting, the user will be able to select whether to delete or preserve websites the user visited when the user clicks "Delete". Fix: Set the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Internet Explorer >> Delete Browsing History >> 'Prevent Deleting Web sites that the User has Visited' to 'Enabled'.	Resolved using fix text instructions.
35	**NVR5:** V-223131 **NVR4X:** V-46857	**Internet Explorer Processes for Notification Bars must be enforced (Reserved).** Description: This policy setting allows you to manage whether the Notification Bar is displayed for Internet Explorer processes when file or code installs are restricted. By default, the Notification Bar is displayed for Internet Explorer processes. If you enable this policy setting, the Notification Bar will be displayed for Internet Explorer processes. If you disable this policy setting, the Notification Bar will not be displayed for Internet Explorer processes. If you do not configure this policy setting, the Notification Bar will be displayed for Internet Explorer processes. Fix: Set the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Internet Explorer >> Security Features >> Notification Bar >> 'Internet Explorer Processes' to 'Enabled'.	Resolved using fix text instructions.

	Vuln ID	Title, Description, and Fix Text	Resolution
36	**NVR5:** V-223133 **NVR4X:** V-46861	**Internet Explorer Processes for Notification Bars must be enforced (Explorer).** Description: This policy setting allows you to manage whether the Notification Bar is displayed for Internet Explorer processes when file or code installs are restricted. By default, the Notification Bar is displayed for Internet Explorer processes. If you enable this policy setting, the Notification Bar will be displayed for Internet Explorer processes. If you disable this policy setting, the Notification Bar will not be displayed for Internet Explorer processes. If you do not configure this policy setting, the Notification Bar will be displayed for Internet Explorer processes. Fix: Set the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Internet Explorer >> Security Features >> Notification Bar >> 'Internet Explorer Processes' to 'Enabled'.	Resolved using fix text instructions.
37	**NVR5:** V-223135 **NVR4X:** V-46869	**Internet Explorer Processes for Notification Bars must be enforced (iexplore).** Description: This policy setting allows you to manage whether the Notification Bar is displayed for Internet Explorer processes when file or code installs are restricted. By default, the Notification Bar is displayed for Internet Explorer processes. If you enable this policy setting, the Notification Bar will be displayed for Internet Explorer processes. If you disable this policy setting, the Notification Bar will not be displayed for Internet Explorer processes. If you do not configure this policy setting, the Notification Bar will be displayed for Internet Explorer processes. Fix: Set the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Internet Explorer >> Security Features >> Notification Bar >> 'Internet Explorer Processes' to 'Enabled'.	Resolved using fix text instructions.
38	**NVR5:** V-223041 **NVR4X:** V-64715	**Prevent per-user installation of ActiveX controls must be enabled.** Description: This policy setting allows you to prevent the installation of ActiveX controls on a per-user basis. If you enable this policy setting, ActiveX controls cannot be installed on a per-user basis. If you disable or do not configure this policy setting, ActiveX controls can be installed on a per-user basis. Fix: Set the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Internet Explorer >> 'Prevent per-user installation of ActiveX controls' to 'Enabled'.	Resolved using fix text instructions.

Adobe Acrobat Reader STIG Vulnerabilities

The following STIG vulnerabilities were found using the Adobe Acrobat Reader DC Continuous Track STIG V2R1.

	Vuln ID	Title, Description, and Fix Text	Resolution
39	**NVR5:** V-213123 **NVR4X:** V-64937	**The Adobe Acrobat Pro DC Continuous Send and Track plugin for Outlook must be disabled.** Description: When enabled, the Adobe Send and Track button appears in Outlook. When an email is composed it enables the ability to send large files as public links through Outlook. The attached files can be uploaded to the Adobe Document Cloud and public links to the files are inserted in the email body. Fix: Configure the following registry value: Note: The Key Name "cCloud" is not created by default in the Acrobat Pro DC install and must be created. Registry Hive: HKEY_LOCAL_MACHINE Registry Path: \Software\Policies\Adobe\Adobe Acrobat\DC\FeatureLockDown\cCloud Value Name: bAdobeSendPluginToggle Type: REG_DWORD Value: 1 Configure the policy value for Computer Configuration > Administrative Templates > Adobe Acrobat Pro DC Continuous > Preferences > 'Send and Track plugin' to 'Disabled'.	Resolved using fix text instructions.