AXIS Camera Station Pro

Cybersecurity: Quick reference guide

Oct 2024
Author: Erik Richardson

1. Introduction

As cybersecurity threats continue to evolve, protecting video surveillance systems like AXIS Camera Station is critical to ensuring data privacy, integrity, and availability. This document serves as a guide to help users understand the key cybersecurity measures and best practices for securing AXIS Camera Station Pro, with a specific focus on version 6. It highlights important considerations such as secure communication, authentication methods, and protecting both data in transit and data at rest.

2. Cybersecurity related development methods within Axis

Axis adheres to the Axis Security Development Model (ASDM) to ensure software security. Regular vulnerability scans are conducted using open-source and commercial tools before product releases and during scheduled intervals for services. These scans help identify and address vulnerabilities, reducing risks for customers.

All release notes for AXIS Camera Station include the version of the Microsoft Windows Defender Security Intelligence scanner used to scan the installer.

3. Security on the local server

AXIS Camera Station operates as a Windows service, relying on Windows account and OS security. It's essential to maintain an updated environment and manage user rights appropriately.
Related documentation:
AXIS Camera Station Pro Microsoft Windows Update Management
AXIS Camera Station Pro User Management

- Sensitive Data: Usernames, passwords (e.g., device credentials), and other sensitive information in databases are encrypted with AES-256.
- Encrypted Storage: Recording storage can be secured using BitLocker, though additional hardware resources may be required.
- Performance Considerations: To improve performance, add AXIS Camera Station-related folders to your antivirus "allow list" to prevent scanning delays. Refer to the FAQ on what to include in the allow list. FAQ: What to include in an Antivirus allow list for AXIS Camera Station Pro.

4. Security between server and client

All communication between the server and client is secured using TLS 1.2 or newer standards. Video streams are encrypted with AES-256. For enhanced security, AXIS Camera Station supports Zero Trust architecture by providing a server certificate ID that can be verified when connecting for the first time.

Ensure your firewall is configured with the appropriate port openings: Port list

5. Client server authentication method

AXIS Camera Station supports both **Kerberos** and **NTLM** for client-server authentication, with **Kerberos** being the default where available. **NTLM** is used for local accounts or when Kerberos is not an option. We recommend enabling Kerberos for its superior security and mutual authentication in Active Directory environments.

6. Security between server and device

Communication between the server and AXIS devices uses **TLS 1.2 or newer**, assuming proper device configuration. For devices with **AXIS OS firmware 5.70 or higher**, **HTTPS** is enabled by default, with a self-signed certificate generated by AXIS Camera Station. You can also use certificates from your own **Certificate Authority (CA)**.

For information on how to configure your HTTPS settings or certificates, please visit the following page: AXIS Camera Station Pro User Manual – Certificates

For securing third-party devices (such as ONVIF profile S devices), it may be necessary to manually add certificates. Contact the device manufacturer for specific instructions. More details on securing AXIS devices can be found in the AXIS OS Hardening Guide User manual

Firewall port configuration is required to allow proper connection: Port list

7. Security between server and online services

All communications with Axis online services are encrypted using **TLS 1.2 or newer**. Access to these services requires an authenticated **MyAxis account**: MyAxis page.

8. Other security considerations

AXIS Camera Station requires **TLS 1.2** to be enabled, though it does not enforce this across your OS or network. Disabling older TLS versions increases security without impacting AXIS Camera Station functionality.

Audit logs are generated by AXIS Camera Station and can be reviewed for monitoring user activity: AXIS Camera Station Pro User Manual - Logs

For additional security recommendations, consult the AXIS Camera Station Pro System Hardening Guide