AXIS Camera Station

Cybersecurity
Quick reference guide

June 2023

*<span>**PLEASE NOTE**</span> that Axis doesn't take any responsibility for how this configuration may affect your system. If the modification fails or if you get other unexpected results, you may have to restore the settings.*

1. Introduction

The following document is to help you understand the Cybersecurity considerations with AXIS Camera Station in focus.
Note this document is based on AXIS Camera Station version 5.50 and the information may change over time.

2. Cybersecurity related development methods within Axis

Axis works with software security according to the ASDM model;
More information can be found on this page: Axis Security Development Model

Regular vulnerability scanning allows the development teams to identify and patch software vulnerabilities before products are released to the public, reducing the customer's risk when deploying the product or service. Scanning is performed prior to each release (hardware, software) or on a running schedule (services) using both open-source and commercial vulnerability scanning packages.

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

3. Security on the local server

Since AXIS Camera Station is running as a Microsoft Windows service, we are depending on Microsoft Windows Account and Operating System security. Keeping your environment and user rights up to date is highly recommended.
Related documentation:
AXIS Camera Station Microsoft Windows Update Management
AXIS Camera Station User Management

Sensitive data like usernames and passwords (such as device credentials) in the databases is AES256 encrypted.

Storing recorded video on encrypted disks with BitLocker is supported but might require extra hardware resources due to increased hard disk input/output usage.

Adding certain folders related to AXIS Camera Station to your "allow list" within your security software is advised to improve performance. Certain scanners will scan all recording data which can result in delays or errors in the actual video data. Find more information here: FAQ: What to include in an Antivirus allow list for AXIS Camera Station.

4. Security between server and client

All communication supports TLS 1.2 or newer standards.

The video-stream connection between AXIS Camera Station server and the client is AES-256 encrypted.

To support Zero Trust architecture AXIS Camera Station provides a server certificate ID which can be confirmed, when connecting to a server for the first time.

Firewall requires the following ports to be opened to allow connection: Port list

5. Security between server and device

All communication supports TLS 1.2 or newer standards if the AXIS device is configured correctly.
HTTPS communication is enabled by default for AXIS devices with AXIS OS firmware 5.70 and higher.
AXIS Camera Station generates a self-signed HTTPS certificate by default but can be supplied by your own CA certificate.
For information on how to configure your HTTPS settings or certificates, please visit the following page: AXIS Camera Station User Manual – Certificates

Secure communications with third party devices such as ONVIF profile S, can in some cases (depending on the device) be achieved by manually adding certificates to the device. Please contact the device manufacturer for more information.

More information about security within AXIS devices, can be found here: AXIS OS Hardening Guide User manual

Firewall requires the following ports to be opened to allow connection: Port list

6. Security between server and online services

All HTTPS communication with our online services supports TLS 1.2 or newer standards.

Axis's online services require an authenticated MyAxis account: MyAxis page.

7. Other security considerations

AXIS Camera Station requires TLS 1.2 to be enabled but we do not enforce TLS 1.2 within your Operating System and/or network.
Disabling older TLS versions will increase security and does not affect AXIS Camera Station.

AXIS Camera Station records audit logs that can be reviewed to help identify activities: AXIS Camera Station User Manual - Logs

For further recommendations, please read the AXIS Camera Station System Hardening Guide