AXIS Camera Station Recorder Series Hardening Guide

Table of Contents

Introduction

The reason for system hardening is to remove as many security risks as possible. Hardening is the process of securing a device and or system by reducing its attack surface. A system or device has a larger vulnerability surface the more functions it fulfills; in theory, a single-function system is more secure than a multipurpose one. Removing available vectors of attack typically includes the removal of unnecessary applications, unnecessary usernames or logins and the disabling or removal of unnecessary services and or protocols. Other measures like applying updates to the software, closing open network ports, setting up intrusion-detection systems, firewalls and intrusion-prevention systems are also considered as part of the system hardening process.

Axis applies cyber hardening best practices in the design, development and testing of our devices to minimize the risk of flaws that could be exploited in an attack. We make it as easy and as cost-efficient as possible to apply appropriate security controls and our devices support encryption and security management.

This guide provides information on how to harden AXIS Network Video Recorder’s (NVR) against possible malicious attacks that may potentially allow an adversary to compromise a NVR and extract sensitive information or use it as a platform to launch other malicious attacks. The guide will describe how to harden the Microsoft Windows operating environment and on best practices that can be applied to AXIS Camera Station.

Physical NVR Security Hardening

Physical Protection

When it comes to IT security, physical protection is the foundation for the overall security strategy. It is very important to make sure that all devices have been protected at the physical layer.

The following methods are recommended to be used to increase the physical security of the NVR as well as the other key components to the network infrastructure for example switches and routers.

Physical Location

- Install the NVR in a secured room with limited access.
- If possible, rack mount the NVR, use the provided rails or ears or purchase a separate shelf.
- Make sure to lock the server cabinet door for added security.
- If the NVR has a lockable lid, cover or bezel, make sure to lock it and secure the key.
- Try to avoid exposed network or power cables.

Limit Port Access

USB Ports

To prevent information being copied on to removable media, or possibly exposing the machine to potential virus, malware, spyware or even ransomware you can disable USB ports. Simply by disconnecting the USB cables or disabling the feature via the BIOS or disabling via Windows with the use of group policies.

Network Ports

Make sure to disable or lock any unused network ports on the NVR. This can be accomplished via the BIOS or other imbedded management system.

BIOS

- The security section of the BIOS is used to keep unauthorized people from making any changes to the BIOS. Because settings in the BIOS are so critical to correct PC operation, it’s recommended to secure with an administration password.

- Disabling the ability to boot from bootable USB, DVD or CD is also highly recommended.

- Upgrading the BIOS version to the latest is highly recommended.

Microsoft Windows Hardening

Windows User Accounts

It’s advisable to create multiple user accounts with different levels of privileges, this approach is an important part of the defensive strategy. This approach ensures that users log on with privileges limited to their roles. If multiple administrators will be administrating the NVR then its best practise to create multiple accounts rather than share a single account, this helps with account auditing.

A recommendation is to configure multiple windows accounts to be used by different users to use/manage the windows environment.

Below are some typical examples of this;

Account Names	***Windows Account roles***
Admin	Administrator
ACS Operator	User
ACS Viewer	User

Admin

The Windows administrator should have full privileges to install software, create accounts etc. After deployment, only a selected number of individuals within the organization should have access to the Administrator account. This is the account that installers, integrators will use during Deployment, configuration or maintenance.

Important: *If multiple individuals need to have Windows Administrator privileges it is recommended to setup multiple administrator accounts. The passwords to these accounts should be limited to single individuals, not shared within the organization. This will help track who-did-what.*

ACS Operator / ACS Viewer

The ACS Operator and the ACS Viewer users should not have Windows administrative privileges and should be configured to be users. Their privileges should be limited and they should not be allowed to install software, add/remove accounts or modify the Windows settings. The main purpose of these accounts is to login to AXIS Camera Station.

Local Account & User Policies

The most common method to authenticate a user's identity is to use a secret passphrase or password. A secure network environment requires all users to use **strong passwords**. These passwords help prevent the compromise of user accounts and administrative accounts by unauthorized people who use either manual methods or automated tools to guess weak passwords.

To ensure that **strong passwords** are being used specific account policies can be applied for example password complexity. Account policies can also be used to lock out an account if the wrong password has been entered too many times.

Windows Updates

Make sure to always download and install the latest updates from Microsoft to protect the NVR against known vulnerabilities in the operating system. Updates will require an internet connection, take the appropriate measures to secure and monitor this connection.

In some case windows updates, will require a restart. This may in some cases be a problem if the NVR is a mission critical resource. To reduce the impact on the availability of the NVR maintenance windows should be planned during off peak hours when the server can be taken down.

Set Date and Time

From a security perspective, it is important that the date and time are correct so that, for example, the system logs are properly time-stamped.

It is recommended that the NVR clock be synchronized with a Network Time Protocol (NTP) server. For individuals and small organizations that do not have a local NTP server, you can use a public NTP server. Check with your ISP to see whether they provide NTP or use a public NTP servers. By default Windows will use time.windows.com however if no internet access is available then an internal NTP server should be used if available.

Logging

Logging is a vital part of cyber security, capturing the correct data in the logs and then monitoring those logs closely. Application and system logs are important also monitoring AXIS Camera Station server and client logs.

Server logs provide the following;

- Alerts to suspicious activities that require further investigation.
- Tracking attacker's activities.
- Assistance in post-event investigation.
- Evidence for legal proceedings.

The logs should be reviewed in set intervals however the frequency depends on certain factors;

- Amount of traffic the server receives.
- General threat level.
- Specific threats.
- Vulnerability of the server.

Anti-Virus

Anti-Virus software is always recommended to be installed to protect the system against viruses and malware which may get inside the network or system that may potentially lock, encrypt or otherwise compromise data on the NVR and or other network devices.

Antivirus software should be deployed on all hosts for which antivirus software is available. Antivirus software should be installed as soon after OS installation as possible and then updated with the latest signatures and antivirus software patches. The antivirus software should then perform a complete scan of the host to identify any potential infections. To support the security of the host, the antivirus software should be configured and maintained properly so that it continues to be effective at detecting and stopping malware

When using an Anti-Virus application please make sure to whitelist and or Allow AXIS Camera Station Client and Server, and do not allow Anti-Virus scanning on the recording directories as this may impact potential new recordings and lower system performance.

What to include in an Ant-Virus white list for AXIS Camera Station to work as expected FAQ116307

Windows Firewall

A firewall is a network security device designed to block unauthorized access to or from a private network. Software firewalls are installed on the NVR and of course can be customized; allowing you some control over its function and protection features. A software firewall will help protect the NVR from outside attempts to control or gain access to the NVR.

Ports and protocols to excluded in firewall rules to allow AXIS Camera Station to work as expected FAQ116306

802.1X Network Authentication

It is also highly recommended to use 802.1x. 802.1X which is a port-based network access control which provides a method to restrict user's access to network resources by using authentication. This restricts users from gaining access to the network resources through an 802.1x-enabled port without authentication.

If a user wants to access the network through a port under 802.1x control, the user must first input an account name for authentication and then wait for authorization before sending or receiving any data from an 802.1x-enabled port.

Windows IP address filtering

IP Address filtering is a good first step in controlling the flow of information to and from specific IP addresses. IP filtering is simply a process that decides which types of IP addresses will be processed normally and which will be deleted and completely ignored, as if it had never been received. Many different sorts of criteria can be used to determine which IP addresses you wish to filter.

IP address filtering can be achieved by using the windows firewall or by using Windows IP security policy. IP filtering can also be configured on routers and switches.

Windows Remote Administration

Remote administration of a machine is a common task that an administrator must perform. However, consider the security aspects when opening protocols and or service to allow a remote connection to be made to the server. Ideally never expose NVR's to the public internet for remote administration but if you do ensure it's in a controlled manner as this increases the possibility of a malicious attack on the system and or NVR.

If remote administration is necessary, consider the points below.

- Use SSL VPN technology to create a connection to the network to make sure that the remote access is authenticated and encrypted. Understand where users authorized for remote desktop access are connecting from, and limit internet access to fixed IP address ranges using IP filters or other methodology. **Do not open access to all Internet hosts**.

- Using two-factor authentication for remote access through VPN.

- Only company-issued hardware devices can connect to the internal corporate network.

- Remote desktop access. If access is essential, ensure there are good reasons why a remote desktop session is needed before even considering allowing access.

If all that is needed is to connect to the NVR to view and playback live and or recorded video, then you can achieve this by connecting to AXIS Camera Station by using AXIS Camera Station secure remote access.

AXIS Camera Station Security Hardening

Camera Hardening

It's also highly recommended to install Axis Device Management, to be able to manage devices and to pre-configure devices prior to them being connected to AXIS Camera Station. To do so follow the *AXIS Camera Hardening Guide* for further information.

AXIS Camera Station Account Management

When using AXIS Camera Station, it is always best practice to create multiple windows users and then give them the appropriate permissions within AXIS Camera Station (to view certain cameras restrict them from viewing recordings etc.). This is even the case if only one user should be using the system. Users and or groups can be created locally on the NVR or be connected to a Domain controller with active directory.

The following table is an example of user roles in AXIS Camera Station

Account Names	***Windows Account roles***	***AXIS Camera Station User Roles***
System Installer	Full Windows Administrator	None
AXIS Camera Station Administrator account	ACS Operator	Administrator
Axis Camera Station Users	ACS User	User

Remote Access

In some occasions, remote access is required to be able to monitor live video or playback of recordings from a remote location. To be able to achieve this remote access is required to the NVR. A secure way to achieve this is to deploy and use AXIS Camera Station Secure Remote Access *Technical Paper.*

Another solution would be a VPN solution which establishes a secure tunnel between the remote location and the NVR installation.

AXIS Camera Station Mobile APP

Any device that is connected to the network should follow the same security standards as applied in computer and network environments, this is also true for smart phones. Smart phones should follow the company's security policies that have been put into place for example; users are unable to install applications from unsecure sources.

The AXIS Camera Station mobile app should only be downloaded from one of these authorized sources;

- Google Play Store*
- Apple App Store*

**Unless an enterprise app store is being used.*

Software Updates

It’s always highly recommended to update the AXIS Camera Station software every time a new version becomes available. Updates often bring user and system improvements and address possible security vulnerabilities. To check what the latest update offers by checking the release notes which are available next to the update.

To reduce the impact on the availability of the NVR, maintenance windows should be planned during off peak hours when the server can be taken offline. This is essential as the system will not be available for recording during this time frame. All software updates are accompanied by an MD5 checksum which is used for file integrity verification, such as when downloading an application installer, there is a MD5 checksum provided along with the download. This is used to verify the file is the original and or uncorrupted.

Firmware Updates

Firmware controls how the device behaves. Axis recommends updating the product firmware whenever new firmware becomes available. New firmware often fixes bugs, contains new features, and protects from security vulnerabilities. AXIS Camera Station can automatically check for new firmware and download it, or it can be used to manually check and download new firmware. Take into consideration to schedule a maintenance window for any type of firmware/software or hardware upgrade. Having a maintenance window is essential as during firmware upgrades the camera will not be available during this time frame.

System notifications

System notifications are generated within the AXIS Camera Station application and show up in the notification area and as a small popup. These notifications are intended to warn the user of certain conditions that have occurred for example;

- Lost connection to device.
- Unexpected server shutdown.
- Failed to execute rule.
- Recording error.

Email alerts can be configured to notify an administrator if a system notification is triggered.

About this document

This guide explains how to harden devises and it can also be used as collateral for deployment teams dealing with local network policy, configurations and specification.

All settings described in this document are available in the product's webpages. To access the webpages, see the User Manual of the specific product.

This document has been prepared carefully, if you identify any inaccuracies or omissions, please inform your local AXIS office. AXIS Communications AB is not responsible for any technical or typographical errors in this document and reserves the right to make changes to the product and manuals without prior notice.

AXIS Communications AB makes no warranty of any kind with regard to the material contained within this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose.

AXIS Communications AB shall not be liable nor responsible for incidental or consequential damages in connection with the furnishing, performance or use of this material. This product is only to be used for its intended purpose.

Intellectual property rights

AXIS AB has intellectual property rights relating to technology embodied in the product described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the patents listed at www.AXIS.com/patent.htm and one or more additional patents or pending patent applications in the US and other countries.

This product contains licensed third-party software. See the menu item "About" in the product's user interface for more information.

This product contains source code copyright Apple Computer, Inc., under the terms of Apple Public Source License 2.0 (see www.opensource.apple.com/apsl). The source code is available from https://developer.apple.com/bonjour/

Trademark acknowledgments

AXIS COMMUNICATIONS and AXIS are registered trademarks or trademark applications of AXIS AB in various jurisdictions. All other company names and products are trademarks or registered trademarks of their respective companies. Apple, Boa, Apache, Bonjour, Ethernet, Internet Explorer, Linux, Microsoft, Mozilla, Real, SMPTE, QuickTime, UNIX, Windows, Windows Vista and WWW are registered trademarks of the respective holders. Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates. UPnPTM is a certification mark of the UPnPTM Implementers Corporation.

Contact information

AXIS Communications AB
Emdalavägen 14
223 69 Lund
Sweden
Tel: +46 46 272 18 00
Fax: +46 46 13 61 30
www.AXIS.com

Support

For technical assistance, please contact your AXIS reseller. If your questions cannot be answered immediately, your reseller will forward your queries through the appropriate channels to ensure a rapid response.
If you are connected to the Internet, you can:

- Download user documentation and software updates.
- Find answers to resolved problems in the FAQ database. Search by product, category or phrase.
- Report problems to AXIS support staff by logging in to your private support area.
- Chat with AXIS support staff.
- Visit AXIS Support at www.AXIS.com/techsup/