Hardening Guide

Cameras

Table of contents

1. Introduction

Axis strives to apply cybersecurity best practices in the design, development and testing of our devices to minimize the risk of flaws that could be exploited in an attack. However, securing a network, its devices, and the services it supports requires active participation by the entire vendor supply chain, as well as the end-user organization. A secure environment depends on its users, processes, and technology. Therefore, we created this guide to support you in securing your network, devices and services.

The guide provides technical advice for anyone involved in deploying Axis video solutions. It establishes a baseline configuration as well as a hardening guide that deals with the evolving threat landscape. Like that of many other security organizations, the Axis baseline uses the CIS Controls - Version 6.1, see www.cisecurity.org/critical-controls.cfm. *These controls were previously known as SANS Top 20 Critical Security Controls.* This document refers to these CSC (Critical Security Control) by marking CSC#.

You may need the product's User Manual to learn how to configure specific settings. Axis provides ACM (AXIS Camera Management) www.axis.com/products/axis-camera-management free of charge that helps manage a number of security controls more cost-efficiently.

Note: This document, contact information and security advisories can be found at **www.axis.com/support/product-security**

1.1 Security cameras in a network environment

The most apparent threats to a network camera are physical sabotage, vandalism and tampering. To protect the product from these threats, it is important to select a vandal-resistant model or casing, to mount it in the recommended way, and to protect the cables.

From an IT/network perspective, the camera is a network endpoint similar to business laptops, desktops and mobile devices. Unlike a business laptop, a network camera is not exposed to the common threat of users visiting potentially harmful websites, opening malicious email attachments, or installing untrusted applications. However, the camera is a network device with an interface that may expose the system to risks. This guide focuses on reducing the exposure area of these risks.

1.2 Limit Internet exposure

It is not recommended to expose the camera as a public web server, allowing unknown clients to get network access to the camera. For Individuals and small organizations that do not operate a VMS (Video Management System) and need to access video from remote locations, Axis recommends using AXIS Companion. AXIS Companion is a Windows/IOS/Android client software, free of charge, that provides an easy way to access video in a more secure way without exposing the camera to the Internet. Information and download for AXIS Companion can be found at **www.axis.com/companion.** Large organizations using a VMS should consult the VMS vendor for remote video access.

1.3 Limit local network exposure

In a VMS environment, the clients will always access live and recorded video through the VMS server. Placing the VMS server and cameras on an isolated network, through physical or virtual isolation, is a common and recommended measure to reduce exposure and risks.

2. About the protection levels

This guide uses different protection levels depending on system size and needs. Each level assumes that the previous level's recommendations are followed.

Protection level		Recommended for	Procedures
0	Default protection	Only recommended for demo purposes and test scenarios.	N/A
1	Standard protection	Minimum recommended level of protection. This level is adequate for small businesses or office installations where, typically, the operator is also the administrator.	> Factory default settings > Use latest firmware > Set the master password > Create a video client account > Configure network settings > Set time and date > Disable audio when applicable > Edge Storage Encryption
2	Enterprise protection	Recommended settings for corporations that have a dedicated system administrator.	> HTTP digest authentication > Domain and host name > Disable unused services > IP Address filter > HTTPS Encryption
3	Managed enterprise protection	Large network infrastructure with an IT/IS department. For environments where cameras may need to be integrated into an enterprise network infrastructure.	> IEEE 802.1X Network Access Control > SNMP monitoring > Remote system log

3. Default protection

Cameras are delivered with predefined default settings and a default password. It is not recommended to use these settings for daily operations.

4. Standard protection

The standard protection level is the minimum recommended level of protection. This level is adequate for small businesses and small organizations where, typically, the operator is also the administrator.

4.1 Factory default settings

CSC #3: Secure configuration for hardware and software.

Before starting, make sure that the product is in a known factory default state. If you are unsure of the state, go to *System Options > Maintenance* and click Default.

4.2 Use latest firmware

CSC #2: Inventory of authorized and unauthorized software.

When new vulnerabilities are discovered, most are either not critical or are very costly to exploit. Occasionally a critical vulnerability is discovered, and device, computer, and systems services need to be patched. Patching software and firmware is an important process of cybersecurity. An attacker will often try to exploit common (known) vulnerabilities, and if they gain network access to an unpatched service, they may succeed. Make sure you always use the latest firmware because it may include security patches for known vulnerabilities. The release notes for a specific firmware may explicitly mention a critical security fix but not all the general ones.

Download the latest firmware file to your computer. The latest version is always available free of charge at **www.axis.com/techsup/firmware.php.** Before upgrading the firmware, read the instructions in the User Manual.

4.3 Set master password

CSC #5: Controlled use of administrative privileges.

The password is the most important means of protection for a network camera. Make sure to use a strong password and keep it protected. On a multi-camera installation, the cameras can have the same password or unique passwords. Using the same password simplifies management but increases the risk if one camera's security is compromised.

Create a hard-to-guess password of at least 8 characters, preferably using a password generator.

4.4 Create a video client account

CSC #5: Controlled use of administrative privileges.
CSC #11: Limitation and control of network ports, protocols, and services.

The default root account has full privileges and should be reserved for administrative tasks. It is recommended to create a client user account with limited privileges for daily operation. This reduces the exposure of the administrator password.

Go to *System Options > Security > Users* and create an account for daily operation. Depending on what camera services the client will use, you need to select Viewer or Operator. A Video Management System (VMS) should normally use the Operator privileges group but may in some cases require administrator privileges. Check with the VMS vendor.

4.5 Configure network settings

CSC #3: Secure configuration for hardware and software.

The device IP configuration depends on the network configuration, such as IPv4/IPv6, static or dynamic (DHCP) network address, subnet mask and default router.

Go to System Options > Network > TCP/IP > Basic/Advanced to configure network settings

4.6 Set time and date

CSC #3: Secure configuration for hardware and software.

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

It is recommended that the camera clock be synchronized with a Network Time Protocol (NTP) server. For individuals and small organizations that do not have a local NTP server, a public NTP server may be used. Check with your Internet service provider or use a public NTP server such as pool.ntp.org.

Go to *System Options > Date & Time* to configure the time settings including time zone and daylight savings time.

4.7 Disable audio

CSC #11: Limitation and control of network ports, protocols, and services.
CSC #13: Data protection.

Audio is enabled by default in camera models that support it. Audio will typically have a higher data classification compared to video due to privacy and integrity. It is recommended to check local regulations before allowing audio streaming.

Go to *System Options > Security> Audio Support* to prevent clients from requesting audio.

4.8 Edge Storage Encryption

CSC #13: Data protection.

If the camera has support for SD Card and video is recorded to this storage device, it is recommended to apply encryption. This will prevent unauthorized individuals that may have removed the SD card to play the stored video. If a Network Attached Storage (NAS) is used as a recording device, it should be protected in a locked area and its accounts/credentials need to be properly configured.

Go to *System Options > Storage > SD Card > Encrypt* and set a passphrase. The encryption used is AES-128.

5. Enterprise protection

For medium and large organizations that deploy a professional video surveillance system, it is recommended to use a Video Management System (VMS) software or NVR. The enterprise protection level involves minimizing risks by reducing the possible attack area of the network camera. It is important to follow the VMS manufacturers' cybersecurity recommendations.

Some of the settings described in this section are already preset at the factory. Make sure that they are correct by following the instructions below.

5.1 Open ports

For reference, the cameras have the following open port pre-configuration.

Port	Service
TCP-21	FTP Server
TCP-80	HTTP Server
TCP-554	RTSP Server
TCP-49152	UPnP (Discovery Protocol)
TCP-1900	UPnP Simple Service Discovery Protocol (SSDP)
UDP-3702	Web Service Dynamic Discovery
UDP-4815	Bonjour Discovery Protocol (mDNS)
UDP-57143	Bonjour (mDNSResponderPosix)

5.2 HTTP digest authentication

CSC #3: Secure configuration for hardware and software.
CSC #13: Data Protection.

In order to prevent clients from sending login passwords in clear text over the network, it is recommended to allow only digest authentication (encrypted passwords).

Go to *System Options > Users > Allow Password type* and select Encrypted Only. If you have a client that does not support digest authentication, you should select Encrypted & Unencrypted.

5.3 Domain and host name

CSC #1: Inventory of authorized and unauthorized devices.

If your network infrastructure has support for local Domain Name System (DNS), it is recommended that cameras are accessed using an Fully Qualified Domain Name (FQDN) instead of its IP address. This makes it easier to manage and keep track of cameras.

Go to *System Options > Network > Advanced > Host Name configuration* to align the system with your DNS infrastructure.

5.4 Disable unused services

Even though unused services are not an immediate security threat, it is a good practice to disable unused service to reduce unnecessary risks. Below are some services that could be disabled if not used:

5.4.1 FTP server

The FTP server is default enabled and typically used for advanced maintenance and troubleshooting. The FTP server should be disabled after camera deployment.

Note that later camera firmware may have this service disabled by default, but we recommend that you check the setting.

Go to *System Options > Network > Advanced > FTP.*

5.4.2 SSH – Secure Shell

SSH command line interface is disabled by default. SSH can be helpful for advanced maintenance and troubleshooting, but during normal operations SSH should be disabled. We recommend making sure that it is.

Go to *System Options > Plain Config* and select the group Network. The checkbox for SSH can be found near the bottom.

5.4.3 ARP/Ping setting of IP address

ARP/Ping is a legacy service that allows an administrator to set a static IP address using a command line terminal to send an ARP/Ping command combination. The service is only available for two minutes after the camera has been restarted. This service has been removed in later firmware, but if you have older firmware, it is recommended that you disable the service completely.

Go to *System Options > Network > Basic under section Services.*

5.4.4 AXIS Device Dispatcher – AVHS

AVHS (AXIS Video Hosting Systems) is a cloud-based video management service. Pressing the control button on the camera registers the camera on the hosting service dispatcher. The dispatcher will allow a user who has access to the camera and provides the correct OAK (Owner Authentication Key) to claim the camera. To stop the camera from connecting to the dispatcher when the physical control button is pressed, go to *System Options > Network > Basic* and uncheck Enable AVHS.

Note that some VMS vendors may support Axis Device Dispatcher when deploying cameras into the system. Check with the VMS vendor.

Read more about AVHS at **www.axis.com/products/hosted-video**

5.4.5 Network discovery protocols

Discovery protocols are support services that make it easier to find the camera and its services on the network. After deployment, once the camera device IP address is known and the camera is added to the VMS, it is recommended that you disable the discovery protocol to stop the camera from announcing its presence on the network.

> UPnP (Universal Plug and Play)
Go to *System Options > Network > UPnP*

> Bonjour
Go to *System Options > Network > Bonjour*

> Link-local address (Zero Conf)
Go to *System Options > Network > Advanced Link-Local IPv4 Address*

5.4.6 SOCKS

SOCKS is disabled by default and used only for specific purposes, to allow the camera to reach network services (e.g. HTTP or FTP image upload) on the other side of a firewall/proxy server.

Go to *System Options > Network > SOCKS*

5.4.7 Always multicast video

Always multicast video is disabled by default. The service is used for specific environments to broadcast video on the local network without clients requesting multicast video.

Go to *System Options > Network > RTP > Multicast*

5.4.8 QoS – Quality Of Service

If the network infrastructure does not support QoS, go to *System Options > Network > QoS* and set all DCSP settings to 0.

Go to *System Options > Network > QoS*

5.5 IP address filter (IP tables)

CSC #1: Inventory of Authorized and Unauthorized Devices
CSC #13: Boundary defense.
CSC #15: Controlled access based on the need to know.

Enabling IP filtering only for authorized clients will prevent the camera from responding to network traffic from any other clients. Make sure to add all authorized clients (VMS server and administrative clients) to the white list.

Go to *System Options > Security > IP Address Filter*

5.6 HTTPS Encryption

CSC #13: Data protection.

HTTPS encrypts the traffic between the client and the camera. It is recommended to use HTTPS for all administrative tasks on the camera. Note that enabling HTTPS will not automatically encrypt video sent over RTP/RTSP. If video is classified as restricted and needs to be protected with encryption, the video client needs to request RTP/RTSP video tunneled over HTTPS. This is controlled by (and depends on) the video client/VMS capabilities.

A self-signed certificate is adequate for providing encryption but will not protect from man-in-the-middle-attack. Clients (e.g., web browsers) will warn that the certificate is not trusted.

A CA-signed certificate (private or public CA) is needed for the client to authenticate that it is accessing the correct camera and thereby mitigate the risk of an attacking computer impersonating a camera.

6. Managed enterprise protection

Managed enterprise networks are systems that typically have additional management tools and services that the cameras need to be aligned with.

6.1 IEEE 802.1X network access control

CSC #1: Inventory of authorized and unauthorized devices.
CSC #13: Boundary defense.

To be accepted in a network infrastructure that is protected by IEEE 802.1X, the cameras need to have appropriate certificates and settings.

Go to *System Options > Security > Certificates* to manage certificates and install the CA root certificate.
Go to System Options > Security > IEEE 802.1X

6.2 SNMP monitoring

CSC #14: Maintenance, monitoring, and analysis of audit logs.

Axis cameras support the following SNMP protocols:

> SNMP v1: Supported only for legacy reasons and should not be used.

> SNMP v2c: May be used on a protected network segment.

> SNMP v3: Recommended for monitoring purposes.

The cameras support monitoring MIB-II and Axis Video MIB. Axis Video MIB can be downloaded at **www.axis.com/support/downloads/axis-video-mib**

For more information about SNMP, see the User Manual.

6.3 Remote System Log

CSC #4: Continuous vulnerability assessment and remediation.
CSC #6: Maintenance, monitoring, and analysis of audit logs.
CSC #16: Account monitoring and control.
CSC #18: Incident response and management.

A syslog server collects all the log messages generated by all cameras. This simplifies audits and prevents log messages from being destructed in the camera either intentionally/maliciously or unintentionally (by a camera reboot overwrite caused by the max log size being reached).

To enable remote syslog, a camera configuration file must be edited. *Go to System Options > Advanced > Scripting > Open Script Editor.*

Camera firmware up to version 5.70
Using the built-in script editor, select the file /etc/rsyslog.conf and add a line at the bottom including the IP address of the syslog server (e.g. *.*@10.2.0.2).

Camera firmware 5.80 and later
A text file with one row containing the IP address of the syslog server (e.g. *.*@10.2.0.2) needs to be added under /etc/rsyslog.d/.

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 web-pages, 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/

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/**

70424/EN/R1/1704

About Axis Communications

Axis offers intelligent security solutions that enable a smarter, safer world. As the market leader in network video, Axis is driving the industry by continually launching innovative network products based on an open platform - delivering high value to customers through a global partner network. Axis has long-term relationships with partners and provides them with knowledge and ground-breaking network products in existing and new markets.

Axis has more than 2,600 dedicated employees in more than 50 countries around the world, supported by a global network of over 90,000 partners. Founded in 1984, Axis is a Sweden-based company listed on NASDAQ Stockholm under the ticker AXIS.

For more information about Axis, please visit our website www.axis.com.

AXIS® COMMUNICATIONS