WHITE PAPER

Hardening guide

June 2020

AXIS COMMUNICATIONS

Table of Contents

Table of Contents

1 Introduction

Axis Communications 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. The purpose of this guide is to support you in securing your network, devices, and services.

The guide provides technical advice for anyone involved in deploying Axis solutions. It establishes a baseline configuration as well as a hardening guide that deals with the evolving threat landscape. Like many other security organizations, Axis follows the methods outlined by CIS Controls - Version 7.1, see *www.cisecurity.org/controls*. These controls were previously known as SANS Top 20 Critical Security Controls. This document refers to these CSC (Critical Security Controls) by marking CSC#.

You may need the product's user manual to learn how to configure specific settings. Note that Axis devices updated the user interface in firmware version 7.10.

Firmware < 7.10: *http://<IP address>/admin/config.shtml*

Firmware >= 7.10: *https://<IP address>/#settings/system/tools/plainconfig*

The document refers to modifying device settings using the "Plain config" page with referrals marked as:

Plain config group

2 System and environment

2.1 Web browser access

Axis devices have a web server that allows users to access the device using a standard web browser. The web interface is intended for configuration, maintenance, and troubleshooting. It is not intended to be used for daily operations, i.e., as a client to view video. The only clients that should be allowed to interact with cameras during daily operations are a video management system (VMS) or device administration and management tools, such as AXIS Device Manager. System users should never be allowed to access Axis devices directly.

2.2 AXIS Device Manager

AXIS Device Manager is a device administration and management tool that streamlines deployment and maintenance of Axis devices. The tool provides an efficient way to manage all major installation, security, and maintenance tasks as well as life-cycle management of several security controls. AXIS Device Manager is available as a free download at *www.axis.com/products/axis-device-manager*

2.3 Security cameras in a network environment

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

From an IT/network perspective, the camera is a network endpoint similar to any other, such as laptop and desktop computers or mobile devices. Unlike a laptop computer, however, a network camera does not have users visiting potentially harmful websites, opening malicious email attachments, or installing untrusted applications. Nevertheless, a network camera is a device with an interface that may expose risks to the system it is connected to. This guide focuses on reducing the exposure to these risks.

2.4 Limit Internet exposure

It is not recommended to expose the camera as a public web server, allowing unknown clients to gain network access to the camera. Axis recommends using AXIS Companion for individuals and small organizations that do not operate a VMS nor need to access video from remote locations. AXIS Companion employs Windows/IOS/Android client software, is free of charge, and provides an easy way to access video in a more secure way without exposing the camera to the Internet. More information about AXIS Companion can be found at *www.axis.com/companion*. All organizations that use a VMS should consult the VMS vendor for remote video access.

2.5 Limit local network exposure

In a VMS environment, 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.

3 Protection levels

According to CIS Controls, the CIS Controls Implementation Groups (IGs) are self-assessed categories for organizations based on relevant cybersecurity attributes. Each IG identifies a subset of the CIS Controls that the community has broadly assessed to be reasonable for an organization with a similar risk profile and resources to strive to implement. This guide is based on those while further adding more default levels.

Protection level	Implementation Group	Description
Default	N/A	A set of security controls that do not require any action from users.
Basic	Group 1	An organization with limited resources and cybersecurity expertise available to implement sub-controls
Foundational	Group 2	An organization with moderate resources and cybersecurity expertise to implement sub-controls
Organizational	Group 3	A mature organization with significant resources and cybersecurity experience to allocate sub-controls

4 Default protection

Cameras are delivered with predefined default settings. It is not recommended to use default settings for daily operations. There are several security controls that you do not need to configure.

4.1 Disabled by default

CSC #5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

The camera will not operate until the administration password is set.

4.2 Disabled services

The following services are disabled by default and should only be enabled if needed.

Service	Usage
FTP Server (port 21)	FTP is only used for specific maintenance or troubleshooting.
SSH (port 22)	SSH is used for specific maintenance or troubleshooting.
Audio	Audio in/out is disabled by default. Check local regulations before enabling.
SOCKS	SOCKS allows the camera to reach network services (e.g. HTTP or FTP image upload) on the other side of a firewall/proxy server.
Always Multicast Video	Used for specific environments to broadcast video on the local network without clients requesting multicast video.
Quality of Service	Used to prioritize selected network traffic.
ONVIF	ONVIF is a standardized protocol for video surveillance systems. Most video systems support Axis VAPIX® Network video Application Programming Interfaces (APIs).

4.3 Signed firmware

CSC #2: Inventory and Control of Software Assets

All Axis firmware is signed. When upgrading the device with a new firmware the device will check the integrity of the firmware and reject tampered firmware. This will prevent attackers from luring users to install a compromised firmware.

4.4 Secure boot

CSC #2: Inventory and Control of Software Assets

Selected devices have secured the boot sequence. This secures the integrity of the device by ensuring that only un-tampered devices can be deployed.

4.5 Trusted platform module (TPM)

CSC #14: Controlled Access Based on the Need to Know

Selected devices have a dedicated module for secure key storage. This increases the protection of encryption keys stored on the device.

4.6 HTTPS enabled

CSC #16: Account Monitoring and Control

HTTPS is enabled by default with a self-signed certificate. This enables setting the device password in a secure way.

4.7 Digest authentication

CSC #16: Account Monitoring and Control

Clients accessing the device will authenticate with a password that is encrypted when sent over the network. This reduces the risk of network sniffers getting hold of the password.

5 Basic protection

The basic protection level is the minimum recommended level of protection. This level is adequate for small businesses and small organizations where typically: 1) the operator is also the administrator; and 2) the organization has limited resources and cybersecurity expertise available to implement sub-controls.

5.1 Factory default settings

CSC #5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers.

Before starting, make sure that the product is in a known factory default state. Read the user manual in order to factory default the device.

5.2 Upgrade to latest firmware

CSC #2: Inventory and Control of Software Assets

When new vulnerabilities are discovered, most are either not critical or are very costly to exploit. Occasionally a critical vulnerability is discovered which demand connected network devices, computers, systems, and services to be patched. Patching software and firmware is an important aspect of cybersecurity. An attacker will often try to exploit commonly 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.

Axis maintains two types of firmware tracks: active track and long-term support (LTS) tracks. While both types include the latest critical patches, LTS does not include new features in order to minimize the risk of compatibility issues. If the firmware has the features, Axis recommends to use the LTS track.

Download the latest firmware file to your computer. The latest version is always available as a free download at *www.axis.com/support/firmware*. Before upgrading the firmware, read the instructions in the user manual.

5.3 Set device password

CSC #4: Controlled Use of Administrative Privileges

The device root account is a device administration account. The password needs to be set for the device for it to become operational. Make sure to use a strong password and keep it protected. For multi-camera installations, the cameras can either use the same password or unique passwords. Using the same password for multiple cameras simplifies management but increases the risk if one camera's security is compromised.

5.4 Create a video client account

CSC #4: Controlled Use of Administrative Privileges

CSC #9: 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 risk of compromising the device administrator password.

5.5 Configure network settings

CSC #11: Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches

The device IP configuration depends on the network configuration, such as IPv4/IPv6, static or dynamic (DHCP) network address, subnet mask and default router. It is recommended to review your network topology when adding new types of components.

5.6 Set time and date

CSC #6: Maintenance, Monitoring and Analysis of Audit Logs

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, preferably two. 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.

5.7 Edge storage encryption

CSC #13: Data Protection

If the camera has support for Secure Digital (SD) cards and video is recorded to this storage device, it is recommended to apply encryption. This will prevent unauthorized individuals from being able to play the stored video from a removed SD card. 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.

6 Foundational 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 network video recorder (NVR). The foundational protection level involves minimizing risks by reducing the possible attack area of the network camera. Typically, this level is applicable for organizations with moderate resources and cybersecurity expertise to implement sub-controls. It is important to follow the VMS manufacturers' cybersecurity recommendations.

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

6.1 Open ports

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

Port	Service
TCP-80	HTTP Server
TCP-443	HTTPS Server
TCP-554	RTSP Server
TCP-49152	UPnP (Discovery Protocol)
UDP-1900	SSDP/UPnP
UDP-3702	Web Service Dynamic Discovery
UDP-5353	mDNSResponder

6.2 Disable web browser access

CSC #5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

After the device is deployed into a system (or added to AXIS Device Manager) it is recommended to prevent people within the organization from using a web browser to access the camera. This adds protection if the device account password is spread within the organization.

Plain config group System [Web Interface Disabled]

6.3 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:

6.3.1 One click cloud connect (O3C)

O3C is a service to deploy cameras to cloud-based video management services. 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 Owner Authentication Key (OAK) to claim the camera.

Consult the user manual to prevent cameras from connecting to the dispatcher when the physical control button is pressed.

6.3.2 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.

Plain config group Network [UPnP, Bonjour, ZeroConf]

6.4 IP address filter

CSC #1: Inventory and Control of Hardware Assets

CSC #12: Boundary Defense

CSC #14: 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.

Plain config group Network [Filter, Input]

6.5 HTTPS with self-signed certificates

CSC #13: Data Protection

HTTPS is available by default for administrative operations. 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 video is only encrypted when a client requests video (RTP/RTSP) is tunneled over HTTPS or when SRTP (Secure RTP) is used.

A self-signed certificate is adequate for providing encryption but will not protect from man-in-the-middle attack. Clients may need to be configured to accept untrusted certificates. Browsers will warn that the certificate is not trusted.

7 Organizational protection

The organizational protection level is for mature organizations with significant resources and cybersecurity experience to allocate to sub-controls. These typically encompass systems that have additional management tools and services that the devices need to be aligned with.

7.1 HTTPS with CA-signed certificates

CSC #13: Data Protection

A CA-signed certificate (private or public CA) is needed for the client to authenticate that it is accessing the correct camera. This mitigates the risk of an attacking computer impersonating a camera. Note that AXIS Device Manager has a built-in CA service that can be used to issue signed certificates to cameras.

7.2 IEEE 802.1X network access control

CSC #1: Inventory and Control of Hardware Assets

CSC #12: Boundary Defense

Cameras need to have appropriate certificates and settings in order to be accepted in a network infrastructure that is protected by IEEE 802.1X.

7.3 SNMP monitoring

CSC #6: 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*.

7.4 Remote system log

CSC #6: Maintenance, Monitoring and Analysis of Audit Logs

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, i.e. by a camera reboot overwrite caused by the max log size being reached.

For details about how to enable remote syslog server in different camera firmware versions, see *www.axis.com/support/technical-notes*

8 About this document

The intended use of this guide is to harden devices and also provide collateral for deployment teams to deal with local network policy, configurations and specification.

All settings described in this document are made in the product's webpages. To access the webpages, see the user manual of the specific product.

8.1 Liability

Every care has been taken in the preparation of this document. Please inform your local Axis office of any inaccuracies or omissions. Axis Communications AB cannot be held responsible for any technical or

typographical errors 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.

8.2 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 *axis.com/patent* 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 *opensource.apple.com/apsl*). The source code is available from *developer.apple.com/bonjour/*.

9 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*

10 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*

About Axis Communications

Axis enables a smarter and safer world by creating network solutions that provide insights for improving security and new ways of doing business. As the industry leader in network video, Axis offers products and services for video surveillance and analytics, access control, and audio systems.

Axis has more than 3,500 dedicated employees in over 50 countries and collaborates with partners worldwide to deliver customer solutions. Axis was founded in 1984 and has its headquarters in Lund, Sweden.

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