AXIS OS

Hardening guide

AXIS OS Lifecycle guide | *AXIS OS Forensics guide* | *AXIS OS Vulnerability scanner guide* | *Security advisories* | *AXIS OS Release notes* | *AXIS OS Knowledge base* | *AXIS OS YouTube playlist*

Introduction

The AXIS OS Hardening guide provides practical guidance for strengthening the security of Axis devices running AXIS OS. It describes recommended configuration settings, features, and operational practices that help reduce the attack surface, protect data, and ensure reliable operation throughout the device lifecycle. The guide is intended for system administrators, integrators, and security professionals who want to deploy and maintain Axis products in a secure and resilient manner, in line with industry best practices.

Web interface configuration
The guide refers to configuring device settings within the web interface of the Axis device. The configuration path differs according to the AXIS OS version installed on the device:

AXIS OS version	Web interface configuration path
< 7.10	Setup > System Options > Security > IEEE 802.1X
≥ 7.10	Settings > System > Security
≥ 10.9	System > Security

Scope

This guide applies to all AXIS OS-based products running AXIS OS (LTS or active track), as well as legacy products running device software 4.xx and 5.xx.

AXIS OS-based products are intended for use in professional security or business intelligence systems and are intended to be integrated with other products, such as video management systems (VMS) and device management applications.

The product may be used in non-professional settings by technically skilled individuals, but it is not designed or intended for home use by individual consumers.

The product follows a secure-by-default approach, but to achieve higher security levels, it is important to follow this Hardening Guide. For selected integrated systems, exemplified secure system design guides are available and can be found at *help.axis.com*.

CIS protection levels

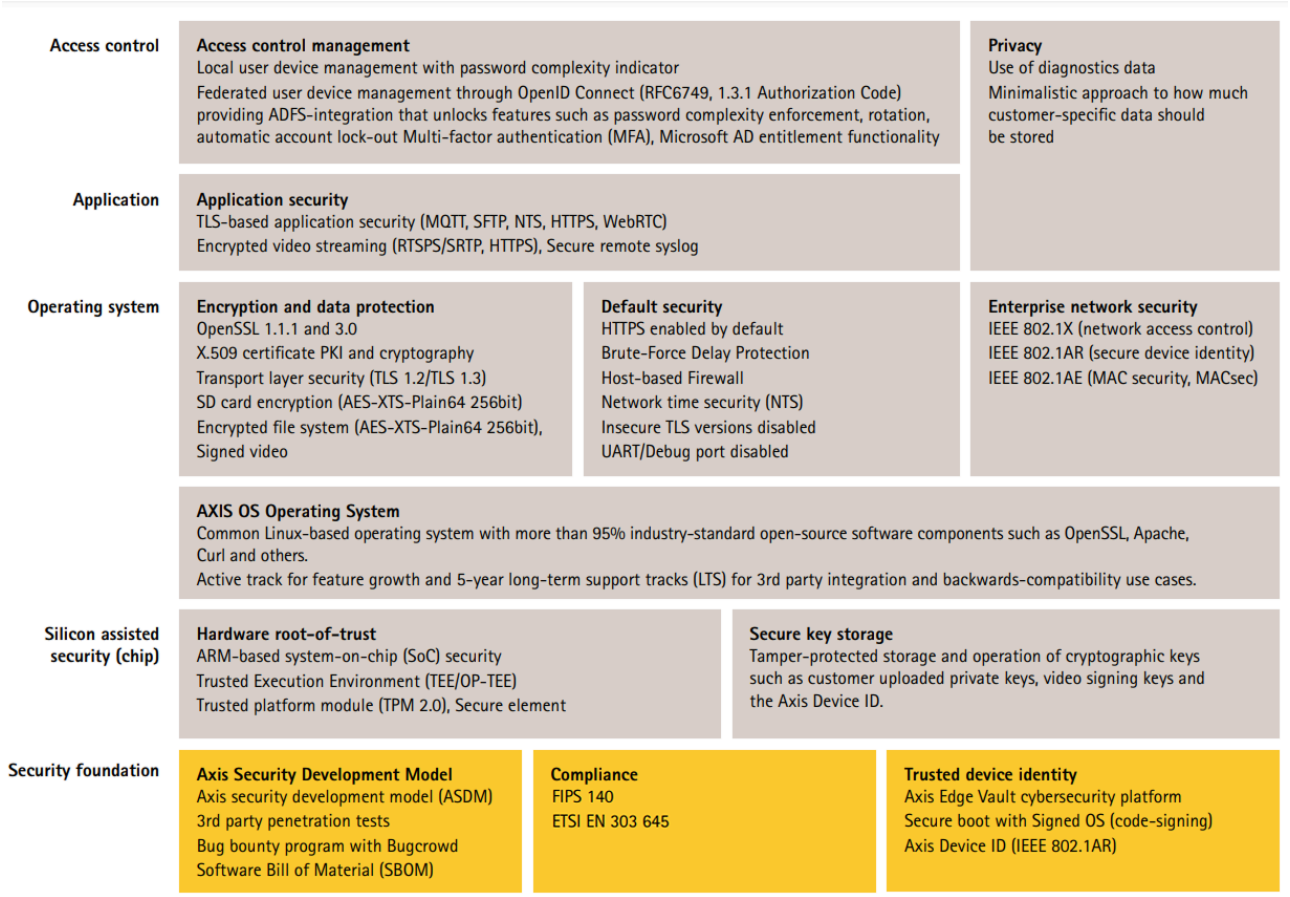
We follow the methods outlined in the Center for Internet Safety (CIS) Controls Version 8 to structure our cybersecurity framework recommendations. The CIS Controls, formerly known as the SANS Top 20 Critical Security Controls, provide 18 categories of Critical Security Controls (CSC) focused on addressing the most common cybersecurity risk categories in an organization.

This guide refers to the Critical Security Controls by adding the CSC number (**CSC #**) for each hardening topic. For more information about the CSC categories, see the *18 CIS Critical Security Controls* at cisecurity.org.

Default protection

Axis devices come with default protection settings. There are several security controls that you don't need to configure. These controls provide a base level of device protection and serve as the foundation for more extensive hardening.

The AXIS OS Security Architecture diagram outlines AXIS OS cybersecurity capabilities across various layers. It provides a comprehensive overview of the security foundation, silicon-assisted security, AXIS OS operating system, and the application and access control layer.



Right click and open the image in a new tab for a better visual experience.

Authentication

Disabled by default

CSC #4: Secure Configuration of Enterprise Assets and Software

The Axis device will not operate until the administrator password has been set.

After setting the administrator password, access to administrator functions and/or video streams is only possible via authentication of valid username and password credentials. We don't recommend that you use features that enable unauthenticated access such as anonymous viewing and always multicast mode.

To learn how to configure device access, see *Device access* in AXIS OS Knowledge base.

Digest authentication

CSC #3: Data Protection

Clients accessing the device will authenticate with a password that should be encrypted when sent over the network. We recommend that you enable HTTPS as described here. If this is not possible, we recommend that

you only use Digest authentication instead of Basic or both Basic and Digest. This reduces the risk of network sniffers getting hold of the password.

AXIS OS version	Web interface configuration path
< 7.10	Setup > System Options > Advanced > Plain Config > Network > Network HTTP Authentication policy
≥ 7.10	Settings > System > Plain config > Network > Network HTTP Authentication policy
≥ 10.9	System > Plain config > Network > Network HTTP Authentication policy

ONVIF replay attack protection

CSC #3: Data Protection

Replay attack protection is a standard security feature enabled by default in Axis devices. Its purpose is to sufficiently secure ONVIF-based user authentication by adding an additional security header, which includes the UsernameToken, valid timestamp, nonce and password digest. The password digest is calculated from the password (which is already stored in the system), nonce, and timestamp. The purpose of the password digest is to validate the user and prevent replay attacks, which is why digests are cached. We recommend that you keep this setting enabled.

AXIS OS version	Web interface configuration path
< 7.10	Setup > System Options > Advanced > Plain Config > System > Enable Replay Attack Protection
≥ 7.10	Settings > System > Plain config > WebService > Enable Replay Attack Protection
≥ 10.9	System > Plain config > WebService > Enable Replay Attack Protection

Prevent brute-force attacks

CSC #4: Secure Configuration of Enterprise Assets and Software
CSC #13: Network Monitoring and Defense

Axis devices feature a prevention mechanism to identify and block brute-force attacks coming from the network such as password-guessing. The feature, called brute-force delay protection, is available in AXIS OS 7.30 and later.

Brute-force delay protection is enabled by default starting from AXIS OS 11.5. For detailed configuration examples and recommendations, see *Brute force delay protection* in AXIS OS Knowledge base.

AXIS OS version	Web interface configuration path
< 7.10	N/A
≥ 7.10	Settings > System > Plain config > System > PreventDosAttack
≥ 10.9	System > Security > Prevent brute-force attacks

Audit log

CSC #1: Inventory and Control of Enterprise Assets

CSC #8: Audit Log Management

Audit logs are used for cybersecurity-related purposes such as incident handling, and helping to establish long-term monitoring of relevant events and actions. We recommend using a remote syslog server or some other network monitoring application so the Axis device can send its logs to a central logging environment. This simplifies the storage of log messages and their retention time.

For more information, see *Audit Log* in AXIS OS Knowledge base.

AXIS OS Version	Web interface configuration path
< 7.10	N/A
≥ 7.10	N/A
≥ 12.5	System > Logs

Edge storage

CSC #4: Secure Configuration of Enterprise Assets and Software

CSC #3: Data Protection

Starting from AXIS OS 12.0, the noexec mount option has been added as a default option for mounted network shares. This will disable any direct execution of binaries from the mounted network share. SD cards already had this option added in earlier versions of AXIS OS.

Additionally Axis devices with AXIS OS 10.10 and later versions support encrypted export of edge recordings. We recommend that you use this feature as it prevents unauthorized individuals from being able to play exported video material.

AXIS OS version	Web interface configuration path
< 7.10	N/A
≥ 7.10	N/A
≥ 10.9	Recordings

Network security

Network protocols

CSC #4: Secure Configuration of Enterprise Assets and Software

Only a minimal number of network protocols and services are enabled by default in Axis devices, as listed below.

Protocol	Port	Transport	Comments
HTTP	80	TCP	General HTTP traffic such as web interface access, VAPIX and ONVIF API interface or edge-to-edge communication.*
HTTPS	443	TCP	General HTTPS traffic such as web interface access, VAPIX and ONVIF API interface or edge-to-edge communication.*

Protocol	Port	Transport	Comments
RTSP	554	TCP	Used by the Axis device for video/audio streaming.
RTP	Ephemeral port range**	UDP	Used by the Axis device for video/audio streaming.
UPnP	49152	TCP	Used by third-party applications to discover the Axis device via UPnP discovery protocol. **NOTE:** Disabled by default from AXIS OS 12.0.
Bonjour	5353	UDP	Used by third-party applications to discover the Axis device via mDNS discovery protocol (Bonjour).
SSDP	1900	UDP	Used by third-party applications to discover the Axis device via SSDP (UPnP). **NOTE:** Disabled by default from AXIS OS 12.0.
WS-Discovery***	3702	UDP	Used by third-party applications to discover the Axis device via WS-Discovery protocol (ONVIF).

* For more information about edge-to-edge, see the white paper *Edge-to-edge technology*.

** Allocated automatically within a predefined range of port numbers according to RFC 6056. For more information, see the Wikipedia article *Ephemeral port*.

*** The WebService Discovery (WS-Discovery) protocol is disabled by default in AXIS OS 12.1 and later.

We recommend that you disable unused network protocols and services wherever possible. For a complete list of services that are used by default or that can be enabled based on configuration, see *Commonly used network ports* in AXIS OS Knowledge base.

For instance, you need to manually enable audio in/out and microphone functionality in Axis video surveillance products such as network cameras, while in Axis intercoms and network speakers, audio in/out and microphone functionality are key features and are enabled by default.

HTTPS enabled

CSC #3: Data Protection

Starting from AXIS OS 7.20, HTTPS has been enabled by default with a self-signed certificate which enables setting the device password in a secure way. In AXIS OS 10.10 and later versions, the self-signed certificate was replaced by the IEEE 802.1AR secure device ID certificate.

AXIS OS has the most common security-related HTTP(S) headers enabled by default to improve the base level of cybersecurity in the factory default state. In AXIS OS 9.80 and later versions, you can use the custom HTTP header VAPIX API to configure additional HTTP(S) headers.

For more information about the HTTP header VAPIX API, see the *VAPIX Library*.

To read more about default HTTP(S) headers, see *Default HTTP(S) headers* in AXIS OS Knowledge base.

AXIS OS version	Web interface configuration path
< 7.10	Setup > System Options > Security > HTTPS
≥ 7.10	Settings > System > Security > HTTP and HTTPS
≥ 10.9	System > Network > HTTP and HTTPS

IEEE 802.1X network access control

CSC #6: Access Control Management
CSC #13: Network Monitoring and Defense

Axis devices support IEEE 802.1X port-based network access control through the EAP-TLS method. For optimal protection, we recommend that you use client certificates signed by a trusted certificate authority (CA) when you authenticate your Axis device.

AXIS OS version	Web interface configuration path
< 7.10	Setup > System Options > Security > IEEE 802.1X
≥ 7.10	Settings > System > Security > IEEE 802.1X
≥ 10.9	System > Security > IEEE 802.1X

In AXIS OS 12.6 we added 802.1x authentication to the S3008 and S3008 MK II recorders. If you're connecting devices with an Axis device ID, but no MACsec support – go to **System > Network ports**, and under **Security** for the port(s), select "Authentication required". This ensures that only devices with an Axis device ID are allowed to connect.

IEEE 802.1AE MACsec

CSC #3: Data Protection
CSC #6: Access Control Management

Axis devices support 802.1AE MACsec which is a well-defined network protocol that cryptographically secures point-to-point ethernet links on network layer 2 ensuring the confidentiality and integrity of data transmissions between two hosts. As MACsec operates at the low layer 2 of the network stack, it adds an additional layer of security to network protocols that do not offer native encryption capabilities (ARP, NTP, DHCP, LLDP, CDP...) as well as ones that do offer it alike (HTTPS, TLS).

The IEEE 802.1AE MACsec standard describes two modes of operation, a manually configurable Pre-Shared Key (PSK)/Static CAK mode and an automatic Master Session/Dynamic CAK mode using IEEE 802.1X EAP-TLS sessions. Axis device supports both two modes.

In AXIS OS 12.6 we added 802.1AE MACsec support to the S3008 and S3008 MK II recorders. If you're connecting devices with an Axis device ID and MACsec support – go to **System > Network ports**, and under **Security** for the port(s), select "MACsec secured required". This enforces both 802.1x authentication and MACsec encryption.

For more information about 802.1AE MACsec and how to configure it in AXIS OS devices, see *IEEE 802.1AE* in the AXIS OS knowledge base.

IEEE 802.1AR secure device identity

CSC #1: Inventory and Control of Enterprise Assets
CSC #13: Network Monitoring and Defense

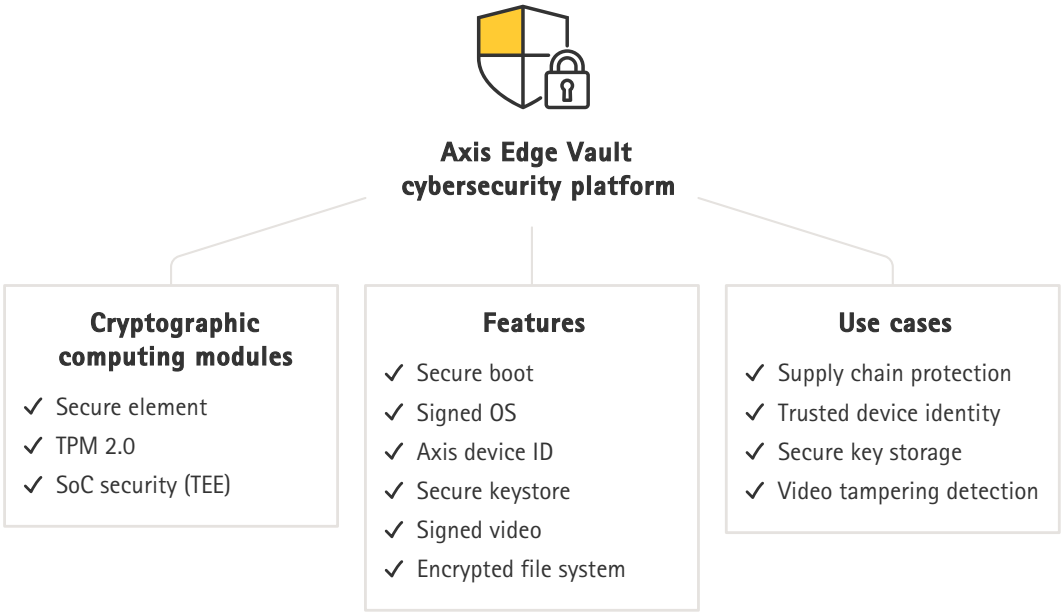
Axis devices with Axis Edge Vault support the network standard IEEE 802.1AR. This allows for automated and secure onboarding of Axis devices into the network through Axis device ID, a unique certificate installed in the device during production. For an example of secure device onboarding, please read more in *Secure integration of Axis devices into Aruba networks*.

For more information, see the white paper *Axis Edge Vault*. To download the Axis Device ID certificate chain, which is used to validate the device identity of Axis devices, see the *Public Key Infrastructure Repository* on axis.com.

Axis Edge Vault

Axis Edge Vault provides a hardware-based cybersecurity platform that safeguards Axis devices. It relies on a strong foundation of cryptographic computing modules (secure element and TPM) and SoC security (TEE and secure boot), combined with expertise in edge device security. Axis Edge Vault is based on a strong root of trust established by secure boot and signed OS. These features enable an unbroken chain of cryptographically validated software for the chain of trust that all secure operations depend on.

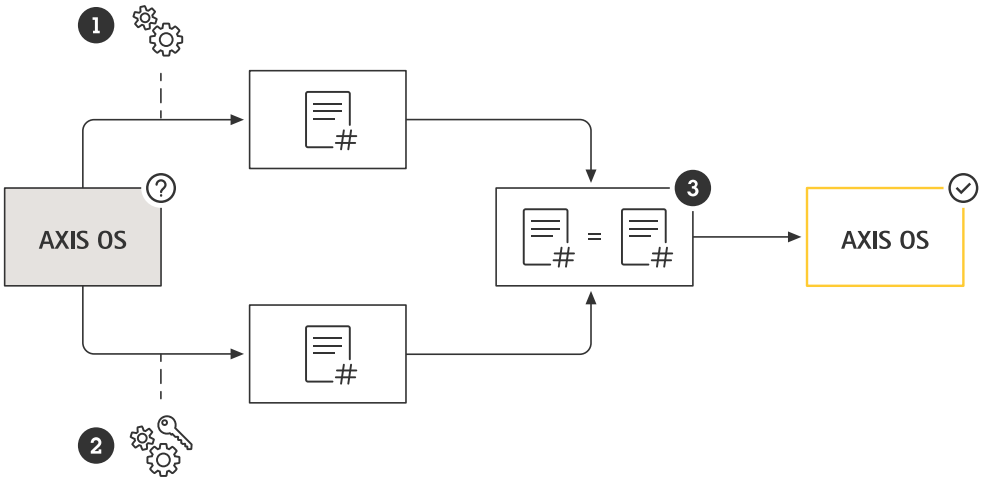
Devices with Axis Edge Vault minimize exposure to cybersecurity risks by preventing eavesdropping and the malicious extraction of sensitive information. Axis Edge Vault also ensures that the Axis device is a trusted and reliable unit on the network.



Signed OS

CSC #2: Inventory and Control of Software Assets

AXIS OS is signed as of version 9.20.1. When you upgrade the version, the device will check the integrity of the update files through cryptographic signature verification and will reject any files that have been tampered with. This prevents attackers from tricking users into installing compromised files.



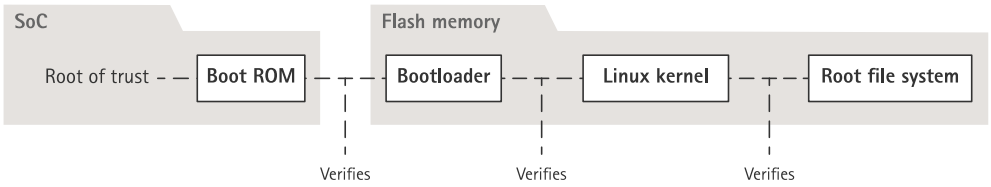
1) The device computes the hash value of the AXIS OS. 2) The device uses the public key to decrypt the signature, obtaining the hash value. 3) If the results match, the OS signature is verified.

For more information, see the white paper *Axis Edge Vault*.

Secure boot

CSC #2: Inventory and Control of Software Assets

Most Axis devices have a secure boot sequence to safeguard the integrity of the device. Secure boot prevents you from deploying Axis devices that have been tampered with.

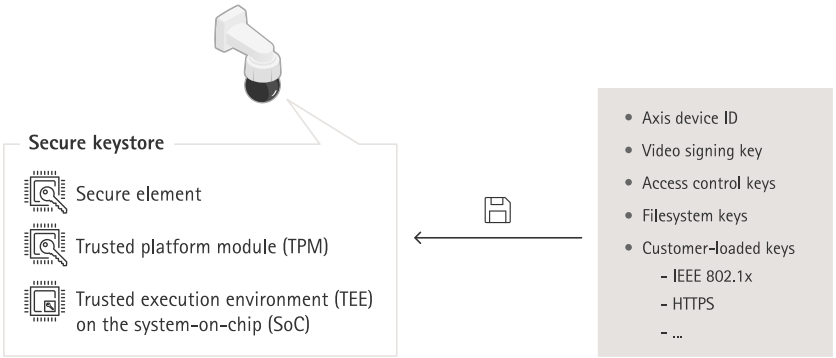


For more information, see the white paper *Axis Edge Vault*.

Secure keystore

CSC #6: Access Control Management

The secure keystore provides hardware-based, tamper-protected storage of cryptographic information. It protects the Axis device ID as well as cryptographic information uploaded by the customer, while also preventing unauthorized access and malicious extraction in the event of a security breach. Depending on security requirements, an Axis device can have one or multiple such modules, like a TPM 2.0 (Trusted Platform Module), a secure element, and/or a TEE (Trusted Execution Environment).



For more information, see the white paper *Axis Edge Vault*.

Signed video

CSC #3: Data Protection

Starting from AXIS OS 13.0, signed video is enabled by default. With signed video, Axis devices add a signature to their video stream to make sure the video is intact and to verify its origin by tracing it back to the device that produced it. Your Video Management System (VMS) or Evidence Management System (EMS) can also verify the authenticity of the video from an Axis device.

Axis supplies the tool *Axis Signed media verifier*, which you can use to verify the authenticity of recorded videos from an Axis device. We offer these three sample files that you can use to explore the tool.

- *Original but unsigned video*
- *Original and signed video*
- *Manipulated video*

The video management system (VMS) or evidence management system (EMS) can also verify the authenticity of video provided by an Axis device.

For more information, see the white paper *Axis Edge Vault*. To find the Axis root certificates used to validate the signed video authenticity, see *Device access* in AXIS OS Knowledge base.

AXIS OS version	Web interface configuration path
< 7.10	N/A
≥ 7.10	N/A
≥ 10.9	System > Plain config > Image > SignedVideo

Encrypted filesystem

CSC #3: Data Protection

A malicious adversary could try to extract information from the filesystem by demounting the flash memory and accessing it through a flash reader device. However, the Axis device can protect the filesystem against malicious data exfiltration and configuration tampering in the event of someone gaining physical access to or stealing it. When the Axis device is powered off, the information on the filesystem is AES-XTS-Plain64 256bit encrypted. During the secure boot process, the read-write filesystem is decrypted and can be mounted and used by the Axis device.

For more information, see the white paper *Axis Edge Vault*.

Software Bill of Materials (SBOM)

CSC #1: Inventory and Control of Enterprise Assets

The Software Bill of Materials (SBOM) for managing vulnerabilities and enhancing supply chain transparency is a vital tool to increase trust in Axis products. The SBOM is supplied with every device software release published on axis.com.

Decommissioning

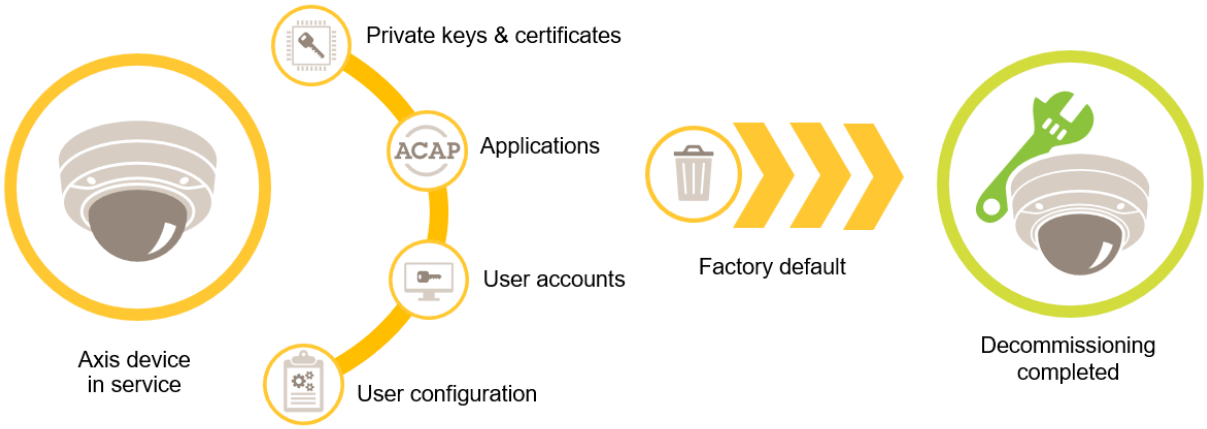
CSC #3: Data Protection

Axis devices use both volatile and non-volatile memory. The volatile memory is erased whenever you unplug the device from its power source, whereas information stored in the non-volatile memory is retained and available again at start-up. We avoid the common practice of simply removing the data pointers to make the stored data invisible to the file system, which is why a factory reset is required. For NAND-flash memory, the UBI function "Remove Volume" is used. The equivalent function is used for eMMC-flash memory, which signals that storage blocks are not used anymore. The storage controller will then wipe those storage blocks accordingly.

When decommissioning an Axis device, we recommend you reset the device to factory default settings, which will erase any data stored in the device's non-volatile memory.

Note that issuing a factory default command will not immediately erase the data, instead the device will reboot and the data erasure will occur during system boot. It is thus not sufficient to merely issue the factory default command – the device must also be allowed to reboot and complete its boot before being powered off, to guarantee that the data erase has completed.

This procedure of erasing customer data follows the "Clear" sanitization technique described in NIST SP-800-88 Revision 1.



AXIS OS version	Web interface configuration path
< 7.10	Setup > System Options > Maintenance > Default
≥ 7.10	Settings > System > Maintenance > Default
≥ 10.9	Maintenance > Default

This table contains more information about data stored in the non-volatile memory.

Information and data	**Erased after factory default**
VAPIX and ONVIF usernames and passwords	Yes
Certificates and private keys	Yes
Self-signed certificate	Yes
TPM and Axis Edge Vault stored information	Yes
WLAN settings and users/passwords	Yes
Custom certificates*	No
SD card encryption key	Yes
SD card data**	No
Network share settings and users/passwords	Yes
Network share data**	No
User configuration***	Yes

Uploaded applications (ACAPs)****	Yes
Production data and lifetime statistics*****	No
Uploaded graphics and overlays	Yes
RTC clock data	Yes

* The signed OS process uses custom certificates that allow users to upload (among other things) AXIS OS.
** Recordings and images stored on edge storage (SD card, network share) have to be deleted by the user separately. Erasing customer data on the SD card is done according to NIST SP-800-88 Revision 1 Cryptographic Erase (CE) and for data on HDDs (S30-Recorder Series) it is NIST SP-800-88 Revision 1 Clear. For more information, see in AXIS OS Knowledge base.
*** All user-made configurations, from creating accounts to network, O3C, event, image, PTZ and system configurations.
**** The device retains any pre-installed applications but deletes all user-made configurations to them
***** Production data (calibration, 802.1AR production certificates) and lifetime statistics include non-sensitive and non-user-related information.

Basic hardening

Basic hardening is the minimum recommended level of protection for Axis devices. The basic hardening topics are "configurable on the edge". This means that they can be directly configured in the Axis device without further dependencies to third-party network infrastructure, video, or evidence management systems (VMS, EMS), equipment or applications.

Commissioning

Factory default settings

CSC #4: Secure Configuration of Enterprise Assets and Software

Before you configure your device, make sure that it's in a factory default state. It's also important to reset the device to factory default settings when you need to clear it from user data or decommission it. For more information, see *Decommissioning, on page 11*.

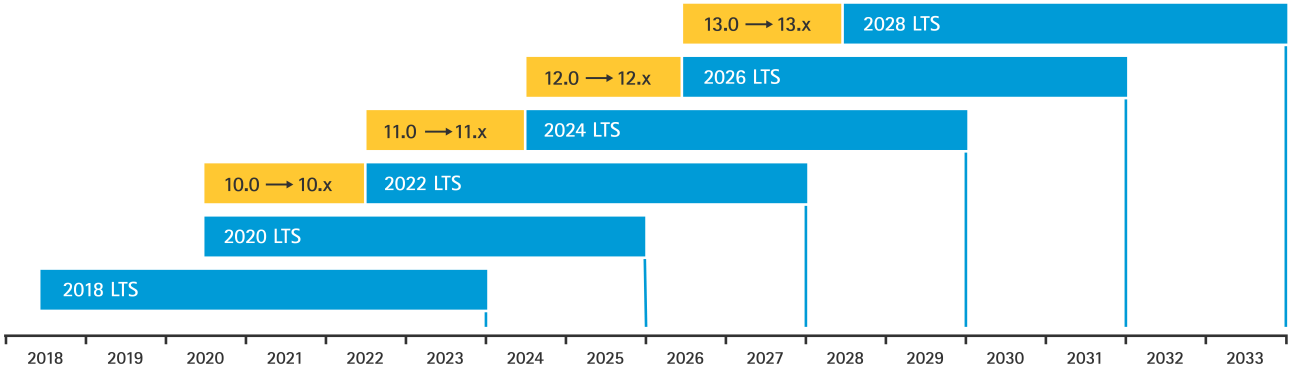
AXIS OS version	Web interface configuration path
< 7.10	Setup > System Options > Maintenance > Default
≥ 7.10	Settings > System > Maintenance > Default
≥ 10.9	Maintenance > Factory default

Upgrade to latest AXIS OS

CSC #2: Inventory and Control of Software Assets

Patching software is an important aspect of cybersecurity. Attackers will often try to exploit commonly known vulnerabilities and may succeed if they gain network access to an unpatched service. Make sure you always use the latest AXIS OS version, as it may include security patches for known vulnerabilities. The release notes for a specific version may explicitly mention a critical security fix, but not all general fixes.

Axis maintains two types of AXIS OS tracks: active tracks and long-term support (LTS) tracks. While both include the latest critical vulnerability patches, LTS tracks do not include new features, as the aim is to minimize the risk of compatibility issues. For more information, see *AXIS OS lifecycle* in AXIS OS Information.



Axis provides a forecast for upcoming releases with information about important new features, bug fixes and security patches. To read more, see *Upcoming releases* in AXIS OS Information. Visit *Device software* at axis.com to download AXIS OS for your device.

AXIS OS version	Web interface configuration path
< 7.10	Setup > System Options > Maintenance > Upgrade Server
≥ 7.10	Settings > System > Maintenance > Firmware upgrade
≥ 10.9	Maintenance > AXIS OS upgrade

Create dedicated accounts

CSC #4: Secure Configuration of Enterprise Assets and Software
CSC #5: Account Management

Axis devices can have two types of accounts: an administrator account and a client user account. The administrator account is the primary account for managing your device, and it's essential to reserve it for administrative tasks only. When setting up your device, you'll need to create a username and password for the administrator account.

In addition to the administrator account, create a client user account with limited privileges for daily operation. This allows you to manage your device securely, reducing the risk of compromising the device administrator password. You should use the client user account for tasks that don't require full administrative privileges.

When creating passwords for either account, we recommend that you implement guidelines such as the NIST or BSI password recommendations, which require new passwords to be sufficiently long and complex. Axis devices support passwords up to 64 characters. Passwords shorter than 8 characters are considered weak. For more information, see *Identity and access management* in AXIS OS Knowledge base.

Axis devices running AXIS OS 11.6 or higher support OAuth 2.0, which allows centralized Identity and Access Management (IAM) and federated identities for authenticating to the device. This eliminates the need for local device user management. For more information, see *OAuth 2.0, on page 26*.

AXIS OS version	Web interface configuration path
< 7.10	Setup > Basic Setup > Users
≥ 7.10	Settings > System > Users
≥ 10.9	System > Users
≥ 11.6	System > Accounts

Configure network, date, and time settings

CSC #4: CSC #8: Audit Log Management
CSC #12: Network Infrastructure Management

It's important to correctly configure the device's network, date, and time settings to keep your Axis device functional and secure. These settings affect various aspects of the device's behavior, including network communication, logging, and certificate validation.

The device IP configuration depends on the network configuration, such as IPv4/IPv6, static or dynamic (DHCP) network address, subnet mask, and default router. Review your network topology whenever you add new components. We recommend that you use static IP address configuration to ensure network reachability and minimize dependencies to network servers that might be vulnerable to attacks, such as DHCP servers.

AXIS OS version	Web interface configuration path
< 7.10	Setup > Basic Setup > TCP/IP
≥ 7.10	Settings > System > TCP/IP
≥ 10.9	System > Network

Accurate timekeeping is essential to maintain system logs, validate digital certificates, and enable services like HTTPS, IEEE, and 802.1x. We recommend that you synchronize your device's clock with Network Time Protocol (NTP) or Network Time Security (NTS) servers. Network Time Security (NTS), an encrypted and secure variant of Network Time Protocol (NTP), was added in AXIS OS 11.1 We recommend that you configure multiple time servers for higher accuracy and to account for potential failures. If you can't host local time servers, consider using public NTP or NTS servers. For more information about NTP/NTS in Axis devices, see*NTP and NTS* in Axis OS Knowledge base.

AXIS OS version	Web interface configuration path
< 7.10	Setup > Basic Setup > Date & Time
≥ 7.10	Settings > System > Date and time
≥ 10.9	System > Date and time
≥ 11.6	System > Time and location

Edge storage encryption

CSC #3: Data Protection

SD card
If the Axis device supports and uses Secure Digital (SD) cards to store video recordings, we recommend that you apply encryption. This will prevent unauthorized individuals from being able to play the stored video from a removed SD card.

To learn more about SD card encryption in Axis devices, see *SD card support* in AXIS OS Knowledge base.

AXIS OS version	Web interface configuration path
< 7.10	Setup > System Options > Storage
≥ 7.10	Settings > System > Storage
≥ 10.9	System > Storage

Network share (NAS)
If you use a Network Attached Storage (NAS) as a recording device, we recommend that you keep it in a locked area with limited access and enable hard disc encryption on it. Axis devices utilize SMB as network protocol for connecting to a NAS to store video recordings. While earlier versions of SMB (1.0 and 2.0) don't provide any security or encryption, later versions (2.1 and later) do, which is why we recommend that you use later versions during production.

To learn more about proper SMB configuration when you connect an Axis device to a network share, see *Network share* in AXIS OS Knowledge base.

AXIS OS version	Web interface configuration path
< 7.10	Setup > System Options > Storage
≥ 7.10	Settings > System > Storage
≥ 10.9	System > Storage

Applications (ACAPs)

CSC #4: Secure Configuration of Enterprise Assets and Software

You can upload applications onto the Axis device to extend its functionality. Many of them come with their own user interface for interacting with a certain feature. Applications may use security functionality that's provided by AXIS OS.

Axis devices are preloaded with several applications developed by Axis according to the *Axis security development model (ASDM)*. For more information about Axis applications, see *Analytics* at axis.com.

For third-party applications, we recommend that you contact the vendor for proof points regarding the security of the application in terms of operation and testing and if it has been developed according to common best-practice security development models. Vulnerabilities found in third-party applications must be reported to the third-party vendor directly.

We recommend that you only operate trusted applications and remove unused applications from Axis devices.

AXIS OS version	Web interface configuration path
< 7.10	Setup > Applications
≥ 7.10	Settings > Apps
≥ 10.9	Apps

As of AXIS OS 12.0 (Sept 2024), ACAP-signing is required and enabled by default, with the option to disable it. As of AXIS OS 13.0 (Sept 2026), ACAP-signing will be mandatory, with no option to disable it. ACAPs are signed in the ACAP portal using SHA-512 and a 4096-bit RSA private key that is stored securely in a Thales Luna Network HSM 7 in the Axis data center in Lund, Sweden. Axis network devices are pre-loaded with the 4096-bit RSA public key in order to validate the ACAP signature prior to ACAP-installation. The public key is stored on the Axis network device on the Linux file system.

Disable unused services/functions

CSC #4: Secure Configuration of Enterprise Assets and Software

Even though unused services and functions are not an immediate security threat, it's good practice to disable unused services and functions to reduce unnecessary risks. Keep reading to learn more about services and functions you can disable if they are not in use.

Web interface access

CSC #4: Secure Configuration of Enterprise Assets and Software

CSC #5: Account Management

Axis devices have a web server that allows users to access the device via a standard browser. The web interface is intended for configuration, maintenance, and troubleshooting, and not for daily operations, for example, as a client to view video.

The only clients that should be allowed to interact with Axis devices during daily operations are video management systems (VMS) or device administration and management tools such as AXIS Device Manager. System users should never be allowed to access Axis devices directly.

As of AXIS OS 9.50, it's possible to disable the web interface of an Axis device. Once you deploy an Axis device into a system (or add it to AXIS Device Manager), we recommend that you remove the option for people within the organization to access the device via a web browser. This creates an additional layer of security if the device account password is shared within the organization. The safer option is to exclusively set up access to Axis devices through dedicated applications that offer advanced identity access management (IAM) architecture, more traceability, and safeguards to avoid account leakage.

AXIS OS version	Web interface configuration path
< 7.10	N/A
≥ 7.10	Settings > System > Plain config > System > Web Interface Disabled
≥ 10.9	System > Plain config > System > Web Interface Disabled

Network discovery protocols

Discovery protocols, such as Bonjour, UPnP, ZeroConf, WS-Discovery, and LLDP/CDP, are support services that make it easier to find the Axis device and its services on the network. After you have deployed the device and added it to the VMS, we recommend that you disable the discovery protocol to stop the Axis device from announcing its presence on the network.

AXIS OS version	Web interface configuration path
< 7.10	Setup > System Options > Advanced > Plain Config > Network > Network Bonjour Enabled, Network UPnP Enabled, Network ZeroConf Enabled, Network UPnP NATTraversal Enabled*
	N/A
≥ 7.10	Settings > System > Plain config > Network > Network Bonjour Enabled, Network UPnP Enabled, Network ZeroConf Enabled, Network UPnP NATTraversal Enabled*
	Settings > System > Plain config > WebService > Discovery Mode
≥ 10.9	Settings > Plain config > Network > Bonjour Enabled, UPnP Enabled, ZeroConf Enabled
	System > Plain config > WebService > DiscoveryMode > Enable WS-Discovery discoverable mode
≥ 11.11	System > Network > Network discovery protocols > Bonjour, UPnP, WS-Discovery, LLDP and CDP**
	Settings > Plain config > Network > ZeroConf Enabled
≥12.1***	System > Network > Network discovery protocols >Bonjour, LLDP and CDP**

* Functionality was removed from AXIS 10.12 and is not available in later versions.

** Disabling LLDP and CDP may impact the PoE power negotiation.
*** By default as of this version, disabling ZeroConf is no longer required. A link-local address is used as a fallback when DHCP is unavailable and no static IP address is configured.

Information disclosure

By default, Axis devices announce basic software versions of their current Apache, OpenSSL, and AXIS OS software versions either during HTTP(S) connections with clients on the network, or through the Basic Device Info VAPIX API (*https://developer.axis.com/vapix/network-video/basic-device-information/*).

This information is essential for network security scanners or network monitoring systems such as Rapid7, Tenable Nessus and others to scan Axis devices for outstanding vulnerabilities. Without this information, these applications might not work correctly on Axis devices. In general, Axis recommends having information disclosure enabled and functional, as it helps to maintain software updates, situational awareness, monitoring and the secure operation of Axis devices.

However, some cybersecurity approaches require that information disclosure is kept to a minimum or is completely disabled. To comply with this requirement, configuration parameters are in place to disable the information disclosure. However, we only recommend that you disable this if you operate your device according to our recommendations and keep it up to date at all times.

Apache/OpenSSL versions

The option to disable the HTTP(S) server headers to reduce information exposure during HTTP(S) connections is available as of AXIS OS 10.6.

AXIS OS version	Web interface configuration path
< 7.10	N/A
≥ 7.10	Settings > System > Plain config > System > HTTP Server Header Comments

≥ 11.11	*https://IP_OR_HOSTNAME/config/web-ui/swagger-ui/?url=/config/discover/apis/basic-device-info/v2/openapi.json#/basic-device-info.v2beta/patch_basic_device_info_v2beta_allowAnonymous*
	
	{
	"data": false
	}

Audio

In Axis video surveillance-oriented products, such as the network cameras, audio in/out and microphone functionality are disabled by default. If you require audio capabilities, you must enable them before use. In Axis products where audio in/out and microphone functionality are key features, such as in Axis intercoms and network speakers, audio capabilities are enabled by default.

We recommend that you disable audio capabilities if you don't use them.

AXIS OS version	Web interface configuration path
< 7.10	Setup > System Options > Advanced > Plain Config > Audio > Audio A* > Enabled
≥ 7.10	Settings > Audio > Allow audio
≥ 10.9	Audio > Device settings

SD card slot(s)

Axis devices usually have support for at least one SD card to provide local edge storage of video recordings. We recommend that you disable the SD card slot entirely if you don't use SD cards. The option to disable the SD card slot is available from AXIS OS 9.80

For more information, see *Disabling the SD card* in AXIS OS Knowledge base.

AXIS OS version	Web interface configuration path
< 7.10	N/A
≥ 7.10	Settings > System > Plain config > Storage > SD Disk Enabled
≥ 10.9	System > Plain config > Storage > SD Disk Enabled

SSH access

SSH is a secure communication protocol used for troubleshooting and debugging purposes only. It's supported by Axis devices starting from AXIS OS 5.50. We recommend that you disable SSH access.

For more information about debugging options using SSH, see *SSH access* in AXIS OS Knowledge base.

AXIS OS version	Web interface configuration path
< 7.10	Setup > System Options > Plain Config > Network > SSH Enabled
≥ 7.10	Settings > System > Plain config > Network > SSH Enabled
≥ 10.9	System > Plain config > Network > SSH Enabled

Interfaces

UART/Debug

CSC #4: Secure Configuration of Enterprise Assets and Software

Every Axis device comes with a so-called physical UART (Universal Asynchronous Receiver Transmitter) interface, sometimes referred to as a 'debug port' or 'serial console'. The interface itself is only physically accessible through extensive dismantling of the Axis device. The UART/debug is used only for product development and debugging purposes during internal R&D engineering projects within Axis.

The UART/debug is enabled by default in Axis devices with AXIS OS 10.10 and earlier versions, but it requires authenticated access and doesn't expose any sensitive information while being unauthenticated. Starting from AXIS OS 10.11, the UART/debug is disabled by default. The only way to enable the interface is by unlocking it through a device-unique custom certificate provided by Axis.

Network ports

Starting from AXIS OS 11.2, devices with multiple network ports, such as AXIS S3008, come with the option to disable both the PoE and network traffic of their network ports. Leaving unused network ports unattended and active poses a severe security risk.

AXIS OS version	Web interface configuration path
< 7.10	N/A
≥ 7.10	N/A
≥ 11.2	System > Power over Ethernet

USB

Starting from AXIS OS 12.1, the AXIS D1110 comes with the option to disable the USB port. Leaving unused USB ports unattended and active poses a severe security risk.

AXIS OS version	Web interface configuration path
< 7.10	N/A
≥ 7.10	N/A
≥ 12.1	System > > Accessories > USB Configuration

Wi-Fi capabilities

Selected Axis devices provide Wi-Fi capabilities using a built-in access point through a USB Wi-Fi Dongle. Wi-Fi is only activated upon pressing the physical WLAN setup button when no physical RJ45 network connection is present. This is true regardless of whether the device is in the factory-default state or is operational. The user can connect to the access point using the SSID and device-unique SSID-password found on the product label.

Please see the user manual for the setup of your Axis device and its Wi-Fi capabilities. The following explains the workings of the built-in access point capabilities in selected Axis products with Wi-Fi support:

- The built-in access point can only be enabled by pressing the physical WLAN setup button, on condition that no Wi-Fi SSID/password is configured and no physical RJ45 network connection is present. This is true regardless of whether the device is in the factory-default state or operational.
- The built-in access point is disabled once the camera connects to a user-configured access point. Alternatively, it is disabled automatically 15 minutes after the user presses the physical WLAN setup button during installation.

If the device uses a connected Wi-Fi dongle, it is recommended to configure Wi-Fi capabilities appropriately, using an SSID + password during the initial configuration of the device, for the strongest security.

Bluetooth

Selected Axis devices provide built-in Bluetooth capability, which you can use for a smooth user experience when setting up the device in its initial state after factory default, e.g. to adjust the image and lenses.

Please see the user manual for your device, for its setup and and Bluetooth capabilities. The descriptions below explain the general Bluetooth capabilities in Axis products:

- Bluetooth is automatically enabled in the factory default state as long as there is no user configured, and for up to a maximum of 2 hours after initial boot-up. Bluetooth is automatically disabled when a user is configured or 2 hours after initial boot-up, regardless of whether a physical RJ45 network connection is present or not.

- After Bluetooth has been disabled, it cannot be enabled manually by the user. You can only restore Bluetooth functionality by resetting the device to the factory default state again.
- The Bluetooth connection from your device to the Axis device uses an HTTPS tunnel that uses the latest TLS 1.2/1.3 encryption. Axis products use Bluetooth Security Mode 1 Level 2 (Encryption with unauthenticated pairing, Just Works).

Limit network access

CSC #1: Inventory and Control of Enterprise Assets
CSC #4: Secure Configuration of Enterprise Assets and Software
CSC #13: Network Monitoring and Defense

AXIS OS 11.9 saw the introduction of a host-based firewall, a security feature that allows you to create rules regulating incoming traffic by IP address and/or TCP/UDP port numbers. This helps prevent unauthorized access to the device or its services.

If you set the default policy to "Drop", be sure to add all authorized clients (VMS and administrative clients) and/or ports to your list.

AXIS OS version	Web interface configuration path
≥ 11.9	System > Security > Firewall

IP address filtering

Devices with AXIS OS 11.8 and earlier versions use IP address filtering to prevent access from unauthorized clients. We recommend that you either configure your device to allow authorized network host IP addresses, or you can deny unauthorized ones.

If you choose to allow IP addresses, make sure to add all authorized clients, including VMS servers and administrative clients, to your list.

AXIS OS version	Web interface configuration path
< 7.10	Setup > System Options > Security > IP Address Filter
≥ 7.10	Settings > System > TCP/IP > IP address filter
10.9 — 11.8	Settings > Security > IP address filter

Note

You can enable more detailed logs of network access attempts to help you identify undesired access attempts from other network hosts. To do so, go to **System** > **Plain config** > **Network** and the Network Filter Log.

HTTPS

CSC #3: Data Protection

HTTP and HTTPS are enabled by default in Axis devices starting from AXIS OS 7.20. While HTTP access is insecure with no encryption at all, HTTPS encrypts the traffic between the client and the Axis device. We recommend that you use HTTPS for all administrative tasks on the Axis device.

For configuration instructions, see *HTTPS only, on page 29* and *HTTPS ciphers, on page 22*.

HTTPS ciphers

Axis devices support and use TLS 1.2 and TLS 1.3 cipher suites to securely encrypt HTTPS connections. The specific TLS version and cipher suite used depends on the client that connects to the Axis device and will be negotiated accordingly. Throughout regular AXIS OS updates, the list of available ciphers of the Axis device may

receive updates without the actual cipher configuration being changed. A change of cipher configurations must be user-initiated, either by performing a factory default of the Axis device or via manual user configuration. From AXIS OS 10.8 and later, the list of ciphers is automatically updated when the user performs an AXIS OS update.

TLS 1.2 and lower

When using TLS 1.2 or lower, you can specify the HTTPS ciphers to be used by the Axis device once it restarts. There are no restrictions to the ciphers you can choose, but we recommend that you select any or all of the following strong ciphers:

```
ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-
AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-
POLY1305:ECDHE-RSA-CHACHA20-POLY1305
```

AXIS OS version	Web interface configuration path
< 7.10	Setup > System Options > Advanced > Plain Config > HTTPS > Ciphers
≥ 7.10	Settings > System > Plain config > HTTPS > Ciphers
≥ 10.9	System > Plain config > HTTPS > Ciphers

TLS 1.3

By default, only strong cipher suites according to the TLS 1.3 specifications are available:

```
TLS_AES_128_GCM_SHA256:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_256_GCM_
SHA384
```

These suites can't be configured by the user.

Extended hardening

The instructions for extended hardening build on the hardening topics described in *Default protection, on page 4* and *Basic hardening, on page 14*. But while you can apply the default and basic hardening instructions directly on your Axis device, the extended hardening requires active participation by the entire vendor supply chain, the end-user organization, and the underlying IT- and/or network infrastructure.

Limit internet and network exposure

CSC #12: Network Infrastructure Management

We recommend that you avoid exposing any Axis device as a public web server or in any other way allow unknown clients network access to the device. For small organizations and individuals that don't use video management software (VMS) or need to access video from remote locations, AXIS Camera Station Edge is a good option.

AXIS Camera Station Edge is available on Windows, iOS, and Android, free of charge, and provides an easy way to access video securely without exposing your device to the internet. For more information, see *axis.com/products/axis-camera-station-edge*.

Note

If your organization uses a VMS, consult your VMS vendor for best practices about remote video access.

Isolating network devices and related infrastructure and applications reduces the risk of network exposure.

We recommend isolating your Axis devices and related infrastructure and applications on a local network that is segregated from your production and business network.

To apply basic hardening, protect the local network and its infrastructure (router, switches) from unauthorized access using multiple network-security mechanisms. These can include VLAN segmenting, limited routing capabilities, VPN for site-to-site or WAN access, network layer 2/3 firewalling, and access control lists (ACL).

To extend basic hardening, apply advanced network inspection techniques, such as deep packet inspection and intrusion detection. This enhances threat protection within the network. Note that extended network hardening typically requires specialized software and/or hardware appliances.

Network vulnerability scanning

CSC #1: Inventory and Control of Enterprise Assets
CSC #12: Network Infrastructure Management

You can use network security scanners to perform vulnerability assessments of your network devices. The purpose of a vulnerability assessment is to provide a systematic review of potential security vulnerabilities and misconfigurations.

We recommend that you perform regular vulnerability assessments of your Axis devices and their related infrastructure. Before you start the scan, make sure that your Axis devices have been updated to the latest available AXIS OS version, on the LTS or the active track.

We also recommend that you review the scanning report and filter out known false positives for Axis devices, which you can find in the *AXIS OS Vulnerability Scanner Guide*. Submit the report and any additional remarks in a ticket to *Axis support* at axis.com.

Trusted public key infrastructure (PKI)

CSC #3: Data Protection
CSC #12: Network Infrastructure Management

We recommend that you deploy web server and client certificates to your Axis devices that are trusted and signed by a public or private certificate authority (CA). A CA-signed certificate with a validated trust chain helps to remove browser certificate warnings when you connect over HTTPS. A CA-signed certificate also ensures the

authenticity of the Axis device when you deploy a network access control (NAC) solution. This mitigates the risk of attacks from a computer impersonating an Axis device.

You can use AXIS Device Manager, which comes with a built-in CA service, to issue signed certificates to Axis devices.

Remote syslog

CSC #8: Audit Log Management

You can configure an Axis device to send all its log messages encrypted to a central syslog server. This makes audits easier and prevents log messages from being deleted in the Axis device, either intentionally/maliciously or unintentionally. Depending on company policies, it can also provide extended retention time of device logs.

For more information about how you enable the remote syslog server in different AXIS OS versions, see *Syslog* in AXIS OS Knowledge base.

AXIS OS version	Web interface configuration path
< 7.10	For instructions, see *Syslog* in AXIS OS Lifecycle guide
≥ 7.10	Settings > System > TCP/IP
≥ 10.9	System > Logs

SNMP

CSC #3: Data Protection
CSC #8: Audit Log Management

You can configure an Axis device to send encrypted SNMP health monitoring data to a central SNMP server through SNMPv3. SNMP-based network monitoring allows for creating alerts and monitoring the device over an extended period of time. Please note that only SNMPv3 offers encryption and privacy, which is why we strongly recommended its use over SNMPv1 and SNMPv2c.

Read more about *SNMP* in AXIS OS Knowledge base.

AXIS OS version	**Web interface configuration path**
< 7.10	For instructions, see *SNMP* in AXIS OS Knowledge base.
≥ 7.10	Settings > System > Network > SNMP
≥ 10.9	System > Network > SNMP

Secure video streaming (SRTP/RTSPS)

CSC #3: Data Protection

Starting from AXIS OS 7.40, Axis devices support secure video streaming over RTP, also referred to as SRTP/RTSPS. SRTP/RTSPS uses a secure end-to-end encrypted transportation method to make sure that only authorized clients receive the video stream from the Axis device. We recommend that you enable SRTP/RTSPS if your video management system (VMS) supports it. If available, use SRTP instead of unencrypted RTP video streaming.

Note

SRTP/RTSPS only encrypts the video stream data. For administrative configuration tasks, we recommend that you enable HTTPS only to encrypt this type of communication.

AXIS OS version	Web interface configuration path
< 7.10	Setup > System Options > Advanced > Plain Config > Network > RTSPS
≥ 7.10	Settings > System > Plain config > Network > RTSPS
≥ 10.9	System > Plain config > Network > RTSPS

OAuth 2.0

CSC #4: Secure Configuration of Enterprise Assets and Software
CSC #5: Account Management

With OAuth 2.0, you can integrate AXIS OS devices running AXIS OS 11.6 or higher into an IT infrastructure with a centralized Identity and Access Management (IAM) service. This lets you use federated identities to authenticate to the Axis device, eliminating the need for local device user management.

OAuth mitigates CSRF attacks by using a unique token to ensure each request is valid.

Depending on the service provider's features, you can use the following security mechanisms for enhanced identity-based authentication to the Axis device:

- Multi-Factor Authentication (MFA)
- Password complexity enforcement
- Password rotation
- Time-limited authentication
- Centralized identity (user/service account) management

For more information about how to enable and configure OAuth 2.0 in AXIS OS devices, see *OAuth 2.0 OpenID Connect* in AXIS OS Knowledge base.

AXIS OS version	**Web interface configuration path**
< 7.10	N/A
≥ 7.10	N/A
≥ 11.6	System > Accounts > OpenID Configuration

Physical anti-tampering accessories

CSC #1: Inventory and Control of Enterprise Assets
CSC #12: Network Infrastructure Management

Axis offers physical intrusion and/or tampering switches as optional accessories to enhance the physical protection of Axis devices. These switches can trigger an alarm which makes it possible for Axis devices to send a notification or an alarm to selected clients.

For more information about available anti-tampering accessories, see:

- *AXIS TA8501 Physical Tampering Switch*
- *AXIS Dome Intrusion Switch C*
- *AXIS Door Switch A*

Legacy hardening

This section covers hardening instructions for securing configurations on parameters found in legacy AXIS OS versions or products. These parameters are not found in the more recent or latest LTS-tracks or the Active track.

Script editor environment

We recommend that you disable access to the script editor environment. The script editor is used for troubleshooting and debugging purposes only.

The script editor was removed from AXIS OS 10.11 and is not available in later versions.

AXIS OS version	Web interface configuration path
< 7.10	N/A
≥ 7.10	Settings > System > Plain config > System > Enable the script editor (editcgi)
≥ 10.9	System > Plain config > System > Enable the script editor (editcgi)

FTP access

FTP is an insecure communication protocol used for troubleshooting and debugging purposes only. FTP access was removed from AXIS OS 11.1 and is not available in later versions. We recommend that you disable FTP access and use secure SSH access for troubleshooting purposes.

For more information about SSH, see *SSH access* in AXIS OS Lifecycle guide. For information about debugging options using FTP, see *FTP access* in AXIS OS Lifecycle guide.

AXIS OS version	Web interface configuration path
< 7.10	Setup > System Options > Plain Config > Network > FTP Enabled
≥ 7.10	Settings > System > Plain config > Network > FTP Enabled
≥ 10.9	System > Plain config > Network > FTP Enabled

Telnet access

Telnet is an insecure communication protocol used for troubleshooting and debugging purposes only. It's supported by Axis devices with earlier versions than AXIS OS 5.50. We recommend that you disable Telnet access.

AXIS OS version	Web interface configuration path
< 5.50	For instructions, see *Device access* in AXIS OS Knowledge base.
< 7.10	N/A
≥ 7.10	N/A
≥ 10.9	N/A

ARP/Ping

ARP/Ping was a method for setting the Axis device's IP address using tools like AXIS IP Utility. The functionality was removed from AXIS OS 7.10 and is not available in later versions. We recommend that you disable the feature in Axis devices with AXIS OS 7.10 and earlier versions.

AXIS OS version	Web interface configuration path
< 7.10	Setup > System Options > Advanced > Plain Config > Network > ARP/Ping
≥ 7.10	N/A
≥ 10.9	N/A

Outdated TLS versions

We recommend that you disable old, outdated, and insecure TLS versions before you put your Axis device in production. Outdated TLS versions are usually disabled by default, but it is still possible to enable them in Axis devices to provide backwards compatibility to third-party applications that haven't yet implemented TLS 1.2 and TLS 1.3.

The outdated TLS versions were removed as of AXIS OS 12.0 and are not available in later versions.

AXIS OS version	Web interface configuration path
< 7.10	Setup > System Options > Advanced > Plain Config > HTTPS > Allow TLSv1.0 and/or Allow TLSv1.1
≥ 7.10	Settings > System > Plain config > HTTPS > Allow TLSv1.0 and/or Allow TLSv1.1
≥ 10.9 – 11.11.X	System > Plain config > HTTPS > Allow TLSv1.0 and/or Allow TLSv1.1

Access log

CSC #1: Inventory and Control of Enterprise Assets
CSC #8: Audit Log Management

The access log provides detailed logs of users accessing the Axis device, which makes both audits and access control management easier. We recommend that you enable this feature and combine it with a remote syslog server so that the Axis device can send its logs to a central logging environment. This simplifies the storage of log messages and their retention time.

For more information, see *Device access logging* in AXIS OS Knowledge base.

AXIS OS version	Web interface configuration path
< 7.10	Setup > System Options > Advanced > Plain Config > System > Access log
≥ 7.10	Settings > System > Plain config > System > Access log
≥ 10.9	System > Plain config > System > Access log

HTTPS only

We recommend that you configure your Axis device to use HTTPS only (with no HTTP access possible). This will automatically enable HSTS (HTTP Strict Transport Security), which will improve the security of the device further.

As of AXIS OS 7.20, Axis devices come with a self-signed certificate, which is valid until 2038-01-19. While a self-signed certificate isn't trusted by design, it's adequate to securely access the Axis device during initial configuration and when there's no public key infrastructure (PKI) available. If available, the self-signed certificate should be removed and replaced with proper signed client certificates issued by a PKI authority of choice. Starting from AXIS OS 10.10, the self-signed certificate was replaced by the IEEE 802.1AR secure device ID certificate.

AXIS OS version	Web interface configuration path
< 7.10	Setup > System Options > Security > HTTPS
≥ 7.10	Settings > System > Security > HTTP and HTTPS
≥ 10.9	System > Network > HTTP and HTTPS

Quickstart guide

The quickstart guide provides a brief overview of settings you should configure when you harden Axis devices with AXIS OS 5.51 and later versions. It covers the hardening topics you can read about in *Basic hardening, on page 14*, however, it doesn't cover the topics in *Extended hardening, on page 24* since they require extensive and customer-specific configuration on a case-by-case basis.

We recommend that you use AXIS Device Manager to harden multiple Axis devices in a quick and cost-efficient way. If you need to use another application for device configuration, or only need to harden a few Axis devices, we recommend that you use the VAPIX API.

Common configuration mistakes

Note

The common configuration mistakes listed below potentially increase the attack surface of the Axis device and reduce its cybersecurity defense layers, resulting in a higher risk of exploitation, misuse, or insecure operation of the device.

Internet-exposed devices
CSC #12: Network Infrastructure Management

We don't recommend that you expose the Axis device as a public web server or that you in any other way give unknown clients network access to the device. For more information, see .

Common password
CSC #4: Secure Configuration of Enterprise Assets and Software
CSC #5: Account Management

We strongly advise you to use a unique password for each device instead of a generic password for all devices. For instructions, see *Identity and access management* in AXIS OS Knowledge base and *Create dedicated accounts, on page 15*.

Anonymous access
CSC #4: Secure Configuration of Enterprise Assets and Software
CSC #5: Account Management.

We don't recommend that you allow anonymous users to access video and configuration settings in the device without having to provide login credentials. For more information, see *Disabled by default, on page 4*.

Secure communication disabled
CSC #3: Data Protection

We don't recommend that you operate the device using insecure communication and access methods, such as HTTP or basic authentication where passwords are transferred without encryption. For more information, see *HTTPS enabled, on page 7*. For configuration recommendations, see *Digest authentication, on page 4*.

Outdated AXIS OS version
CSC #2: Inventory and Control of Software Assets

We strongly advise you to operate the Axis device using the latest available AXIS OS version, either on the LTS or active track. Both tracks provide the latest security patches and bug fixes. For more information, see *Upgrade to latest AXIS OS, on page 14*.

Basic hardening via VAPIX API

You can use the VAPIX API to harden your Axis devices based on the topics covered in *Basic hardening, on page 14*. In this table, you can find all basic hardening configuration settings regardless of the AXIS OS version of your Axis device.

It's possible that some configuration settings are no longer available in your device's AXIS OS version since some functionality has been removed over time to increase security. If you receive an error when you issue the VAPIX call, it could be an indication that the functionality is no longer available in the AXIS OS version.

Purpose	VAPIX API call
*Disable POE in unused network ports**	`http://ip-address/axis-cgi/nvr/poe/setportmode.cgi?port=X&enabld=no`
*Disable network traffic in unused network ports***	`http://ip-address/axis-cgi/network_settings.cgi { "apiVersion": "1.17", "method": "setDeviceConfiguration", "params": { "deviceName": "eth1.1", "staticState": "down" } }`
Disable Bonjour discovery protocol	`https://ip-address/axis-cgi/param.cgi?action=update&Network.Bonjour.Enabled=no`
Disable UPnP discovery protocol	`https://ip-address/axis-cgi/param.cgi?action=update&Network.UPnP.Enabled=no` `https://ip-address/axis-cgi/param.cgi?action=update&Network.UPnP.NATTraversal.Enabled=no`
Disable WebService discovery protocol	`https://ip-address/axis-cgi/param.cgi?action=update&WebService.DiscoveryMode.Discoverable=no`
Disable one-click-cloud connection (O3C)	`https://ip-address/axis-cgi/param.cgi?action=update&RemoteService.Enabled=no`
Disable device SSH maintenance access	`https://ip-address/axis-cgi/param.cgi?action=update&Network.SSH.Enabled=no`
Disable device FTP maintenance access	`https://ip-address/axis-cgi/param.cgi?action=update&Network.FTP.Enabled=no`
Disable ARP-Ping IP address configuration	`https://ip-address/axis-cgi/param.cgi?action=update&Network.ARPPingIPAddress.Enabled=no`
Disable Zero-Conf IP address configuration	`http://ip-address/axis-cgi/param.cgi?action=update&Network.ZeroConf.Enabled=no`
Enable HTTPS only	`https://ip-address/axis-cgi/param.cgi?action=update&System.BoaGroupPolicy.admin=https` `https://ip-address/axis-cgi/param.cgi?action=update&System.BoaGroupPolicy.operator=https` `https://ip-address/axis-cgi/param.cgi?action=update&System.BoaGroupPolicy.viewer=https`
Enable TLS 1.2 and TLS 1.3 only	`https://ip-address/axis-cgi/param.cgi?action=update&HTTPS.AllowTLS1=no` `https://ip-address/axis-cgi/param.cgi?action=update&HTTPS.AllowTLS11=no`

Purpose	VAPIX API call
TLS 1.2 secure cipher configuration	`https://ip-address/axis-cgi/param.cgi?action=update&HTTPS.Ciphers=ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305`

*Enable brute force attack protection****	`https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.ActivatePasswordThrottling=on`
	`https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.DoSBlockingPeriod=10`
	`https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.DoSPageCount=20`
	`https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.DoSPageInterval=1`
	`https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.DoSSiteCount=20`
	`https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.DoSSiteInterval=1`

Disable script editor environment	`https://ip-address/axis-cgi/param.cgi?action=update&System.EditCgi=no`
Enable improved user access logging	`https://ip-address/axis-cgi/param.cgi?action=update&System.AccessLog=On`
Enable ONVIF replay attack protection	`https://ip-address/axis-cgi/param.cgi?action=update&WebService.UsernameToken.ReplayAttackProtection=yes`
Disable device web interface access	`https://ip-address/axis-cgi/param.cgi?action=update&System.WebInterfaceDisabled=yes`
Disable HTTP/OpenSSL server header	`https://ip-address/axis-cgi/param.cgi?action=update&System.HTTPServerTokens=no`

Disable anonymous viewer and PTZ access	`https://ip-address/axis-cgi/param.cgi?action=update&root.Network.RTSP.ProtViewer=password`
	`https://ip-address/axis-cgi/param.cgi?action=update&root.System.BoaProtViewer=password`
	`https://ip-address/axis-cgi/param.cgi?action=update&root.PTZ.BoaProtPTZOperator=password`

Purpose	VAPIX API call
Prevent installation of root-privilege requiring ACAP applications	`http://ip-address/axis-cgi/applications/config.cgi?action=set&name=AllowRoot&value=false`
Prevent the installation of unsigned ACAP applications	`http://ip-address/axis-cgi/applications/config.cgi?action=set&name=AllowUnsigned&value=false`

* Replace "X" with the actual port number in "port=X". Examples: "port=1" will disable port 1 and "port=2" will disable port 2.
** Replace "1" with the actual port number in "eth1.1". Examples: "eth1.1" will disable port 1 and "eth1.2" will disable port 2.
*** After 20 failed login attempts within one second, the client IP address is blocked for 10 seconds. Every following failed request within the 30 seconds page interval will result in the DoS blocking period being extended by another 10 seconds.

Basic hardening via AXIS Device Manager (Extend)

You can use AXIS Device Manager and AXIS Device Manager Extend to harden your Axis devices based on the topics covered in *Basic hardening, on page 14*. Use this *configuration file*, which consists of the same configuration settings listed in *Basic hardening via VAPIX API, on page 30*.

It's possible that some configuration settings are no longer available in your device's AXIS OS version since some functionality has been removed over time to increase security. AXIS Device Manager and AXIS Device Manager Extend will automatically remove these settings from the hardening configuration.

Note

After you upload the configuration file, the Axis device will be configured to HTTPS only and the web interface will be disabled. You can modify the configuration file according to your needs, for example by removing or adding parameters.

Security notifications

We recommend that you subscribe to *Axis security notification service* to receive information about newly discovered vulnerabilities in Axis products, solutions, and services as well as how to keep your Axis devices secure.

T10177717

2026-07 (M69.2)

© 2022 – 2026 Axis Communications AB