

AXIS OS Hardening Guide

AXIS OS Hardening Guide

[AXIS OS Portal](#) | [AXIS OS Release Notes](#) | [AXIS OS Knowledge base](#) | [AXIS OS YouTube playlist](#) | [Security Advisories](#)

AXIS OS Hardening Guide

Introduction

Introduction



AXIS OS Hardening Guide for Axis edge devices

Axis Communications strives to apply cybersecurity best practices in the design, development, and testing of our devices to minimize the risk of flaws that hackers could exploit in an attack. However, the entire vendor supply chain and end-user organization must be involved in securing a network, its devices, and the services it supports. A secure environment depends on its users, processes, and technology. The purpose of this guide is to help you keep your network, devices, and services secure.

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

Axis devices are network endpoints just like computers and mobile phones. Many of them have a web interface that can expose vulnerabilities to connected systems. In this guide, we explain how you can reduce those risks.

The guide provides technical advice for anyone involved in deploying Axis solutions. It includes a recommended baseline configuration as well as a hardening guide that takes the evolving threat landscape into account. You may need to consult the product's user manual to learn how to configure specific settings. Note that Axis devices got a web interface update in AXIS OS 7.10 and 10.9, which changed the configuration path.

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 4.xx and 5.xx.







The operating system for Axis edge devices.

AXIS OS Security Architecture

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

AXIS OS Hardening Guide

Introduction

 <p>Access control</p>	<p>Access control management Local user device management with password complexity indicator Federated user device management through OpenID Connect (RFC6749, 1.3.1 Authorization Code) providing ADFS-integration that unlocks features such as Password complexity enforcement, rotation, automatic account lock-out Multi-factor authentication (MFA), Microsoft AD entitlement functionality</p>	<p>Privacy Use of diagnostics data Minimalistic approach to how much customer-specific should be stored</p>				
 <p>Application</p>	<p>Application security TLS-based application security (MQTT, SFTP, NTS, HTTPS, WebRTC) Encrypted video streaming (RTSPS/SRTP, HTTPS), Secure remote syslog</p>					
 <p>Operating system</p>	<p>Encryption and data protection</p> <ul style="list-style-type: none"> OpenSSL 1.1.1 and 3.0 X.509 certificate PKI and cryptography Transport layer security (TLS 1.2/TLS 1.3) SD card encryption (AES-XTS-Plain64 256bit) Encrypted file system (AES-XTS-Plain64 256bit), Signed video 	<p>Default security</p> <ul style="list-style-type: none"> HTTPS enabled by default Brute-Force Delay Protection Host-based Firewall Network time security (NTS) Insecure TLS versions disabled UART/Debug port disabled 	<p>Enterprise network security</p> <ul style="list-style-type: none"> IEEE 802.1X (network access control) IEEE 802.1AR (secure device identity) IEEE 802.1AE (MAC security, MACsec) 			
<p>AXIS OS Operating System Common Linux-based operating system with more than 95% industry-standard open-source software components such as OpenSSL, Apache, Curl and others. Active track for feature growth and 5-Year Long-Term Support tracks (LTS) for 3rd party integration and backwards-compatibility use cases.</p>						
 <p>Silicon assisted security (chip)</p>	<p>Hardware root-of-trust ARM-based system-on-chip (SoC) security Trusted Execution Environment (TEE/OP-TEE) Trusted platform module (TPM 2.0), Secure element</p>	<p>Secure key storage Tamper-protected storage and operation of cryptographic keys such as customer uploaded private keys, video signing keys and the Axis Device ID.</p>				
<p>Security foundation</p> <table border="1"> <tr> <td data-bbox="459 833 783 929"> <p>Secure software development Axis security development model (ASDM) 3rd party penetration tests Bug bounty program with Bugcrowd Software Bill of Material (SBOM)</p> </td> <td data-bbox="783 833 1107 929"> <p>Certification Common criteria CC EAL4+ / EAL6+ FIPS 140-2 ETSI EN 303 645</p> </td> <td data-bbox="1107 833 1449 929"> <p>Trusted device identity Axis Edge Vault cybersecurity platform Secure boot with Signed Firmware (code-signing) Axis Device ID (IEEE 802.1AR)</p> </td> </tr> </table>				<p>Secure software development Axis security development model (ASDM) 3rd party penetration tests Bug bounty program with Bugcrowd Software Bill of Material (SBOM)</p>	<p>Certification Common criteria CC EAL4+ / EAL6+ FIPS 140-2 ETSI EN 303 645</p>	<p>Trusted device identity Axis Edge Vault cybersecurity platform Secure boot with Signed Firmware (code-signing) Axis Device ID (IEEE 802.1AR)</p>
<p>Secure software development Axis security development model (ASDM) 3rd party penetration tests Bug bounty program with Bugcrowd Software Bill of Material (SBOM)</p>	<p>Certification Common criteria CC EAL4+ / EAL6+ FIPS 140-2 ETSI EN 303 645</p>	<p>Trusted device identity Axis Edge Vault cybersecurity platform Secure boot with Signed Firmware (code-signing) Axis Device ID (IEEE 802.1AR)</p>				

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

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.

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](https://www.cisecurity.org).

AXIS OS Hardening Guide

Default protection

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.

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.

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

Edge storage

CSC #4: Secure Configuration of Enterprise Assets and Software

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.

Credentialed access

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.

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. In this table you can see which these are.

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.*
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.

AXIS OS Hardening Guide

Default protection

Protocol	Port	Transport	Comments
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*.

We recommend that you disable unused network protocols and services whenever possible. For a complete list of services that are used by default or 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 therefore enabled by default.

UART/Debug interface

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 interface is used only for product development and debugging purposes during internal R&D engineering projects within Axis.

The UART/debug interface 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 interface is disabled by default. The only way to enable the interface is by unlocking it through a device-unique custom certificate provided by Axis.

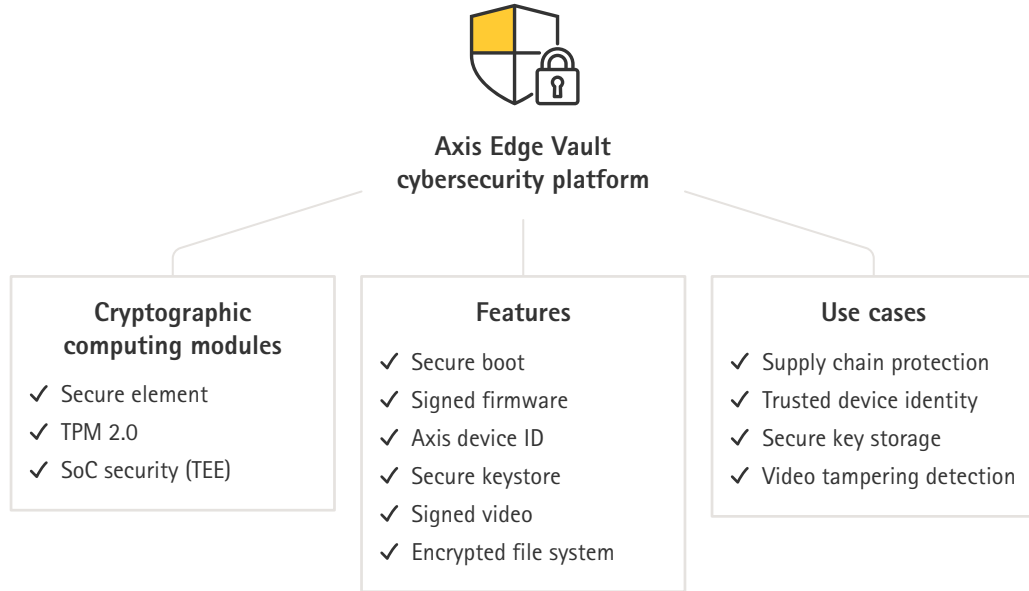
Axis Edge Vault

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 firmware. These features enable an unbroken chain of cryptographically validated software for the chain of trust that all secure operations depend on.

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

AXIS OS Hardening Guide

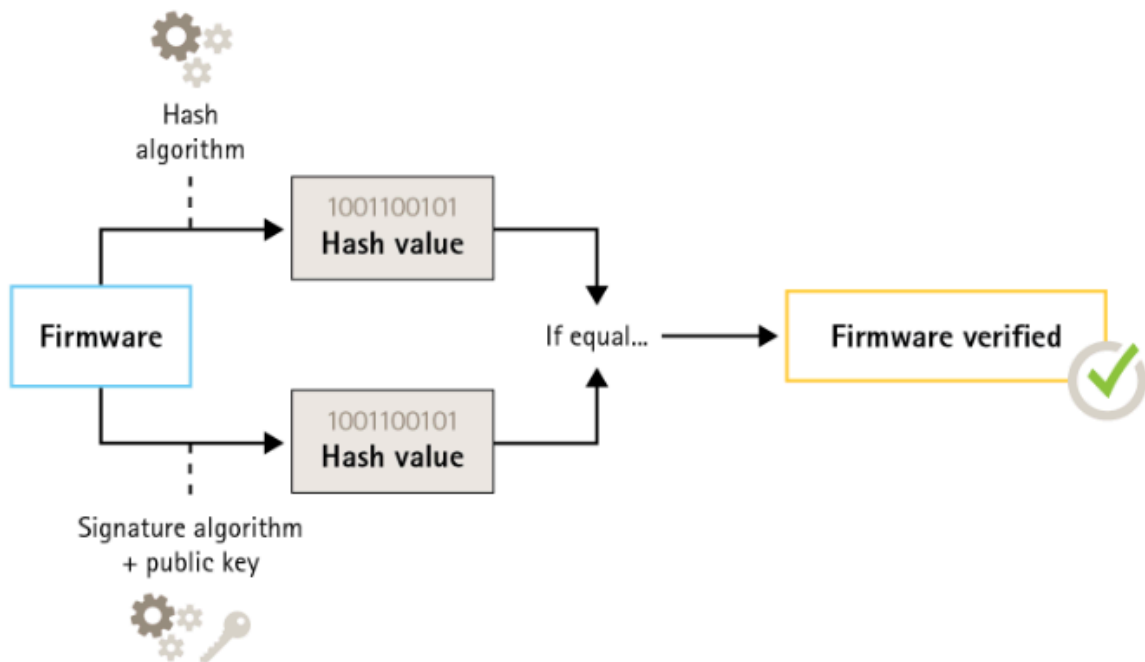
Default protection



Signed firmware

CSC #2: Inventory and Control of Software Assets

AXIS OS is signed from version 9.20.1. Whenever you upgrade the AXIS OS version on device, the device will check the integrity of the update files through cryptographic signature verification and reject any tampered files. This prevents attackers from luring users into installing compromised files.



AXIS OS Hardening Guide

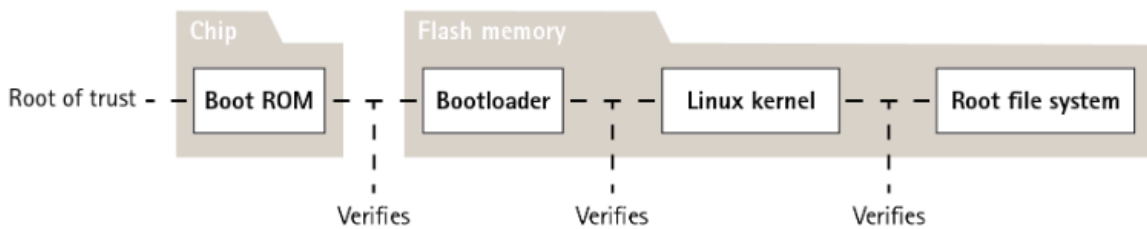
Default protection

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*.

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-Plain64256bit encrypted. During the secure boot process, the read-write filesystem is decrypted and can be mounted and used by the Axis device.

AXIS OS Hardening Guide

Default protection

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

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. 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

Default HTTP(S) headers

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. Starting from AXIS OS 9.80, 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.

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 therefore 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 Hardening Guide

Default protection

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

Decommissioning

CSC #3: Data Protection

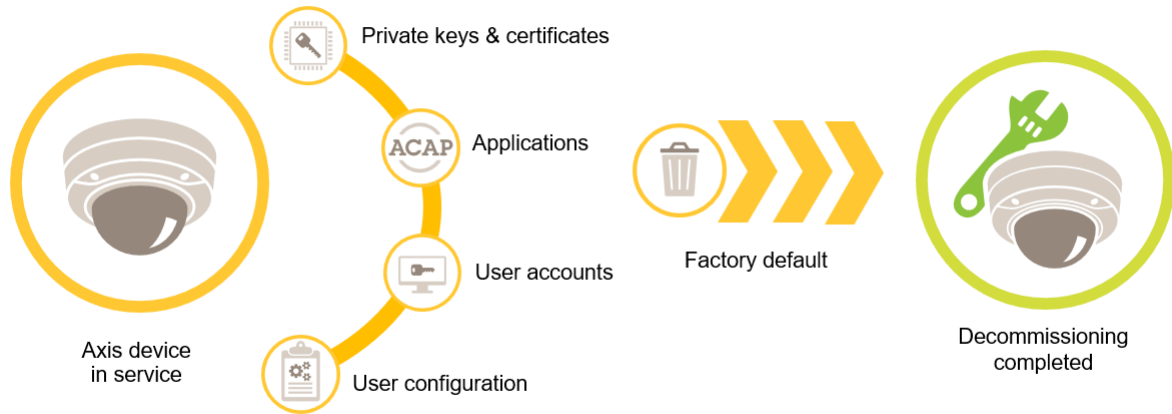
Axis devices use both volatile and non-volatile memory, and while the volatile memory is erased whenever you unplug the device from its power source, information stored in the non-volatile memory remains and is made available again at start-up. We avoid the common practice of simply removing the data 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 that signalizes that storage blocks are not used anymore. The storage controller then will wipe those storage blocks accordingly.

When decommissioning an Axis device, we recommend that you reset the device to factory default settings, which will erase any data stored on 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 therefore not sufficient to merely issuing 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.

AXIS OS Hardening Guide

Default protection



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 firmware 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. For more

AXIS OS Hardening Guide

Default protection

information, see Formatting Axis SD cards 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.*

AXIS OS Hardening Guide

Basic hardening

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.

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 .

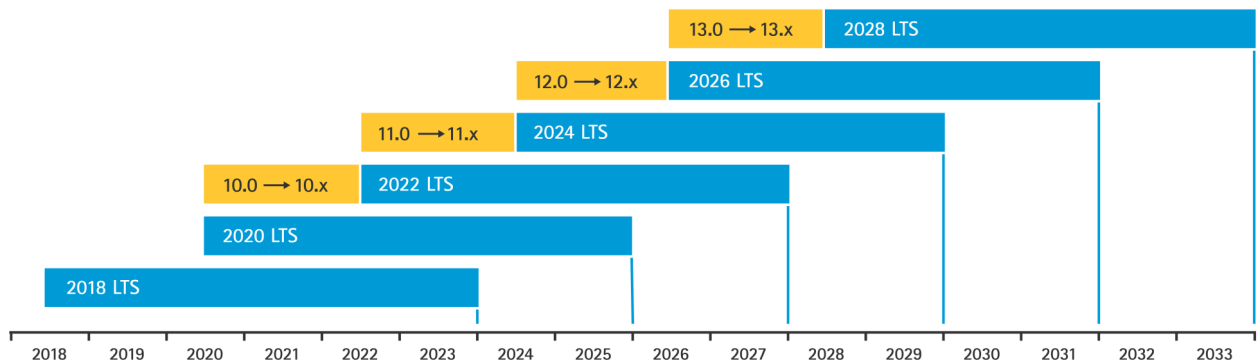
AXIS OS version	Web interface configuration path
< 7.10	Setup > System Options > Maintenance > Default
≥ 7.10	Settings > System > Maintenance > Default
≥ 10.9	Maintenance > Default

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 since 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: the active track and the long-term support (LTS) tracks. While both types include the latest critical vulnerability patches, the 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*.

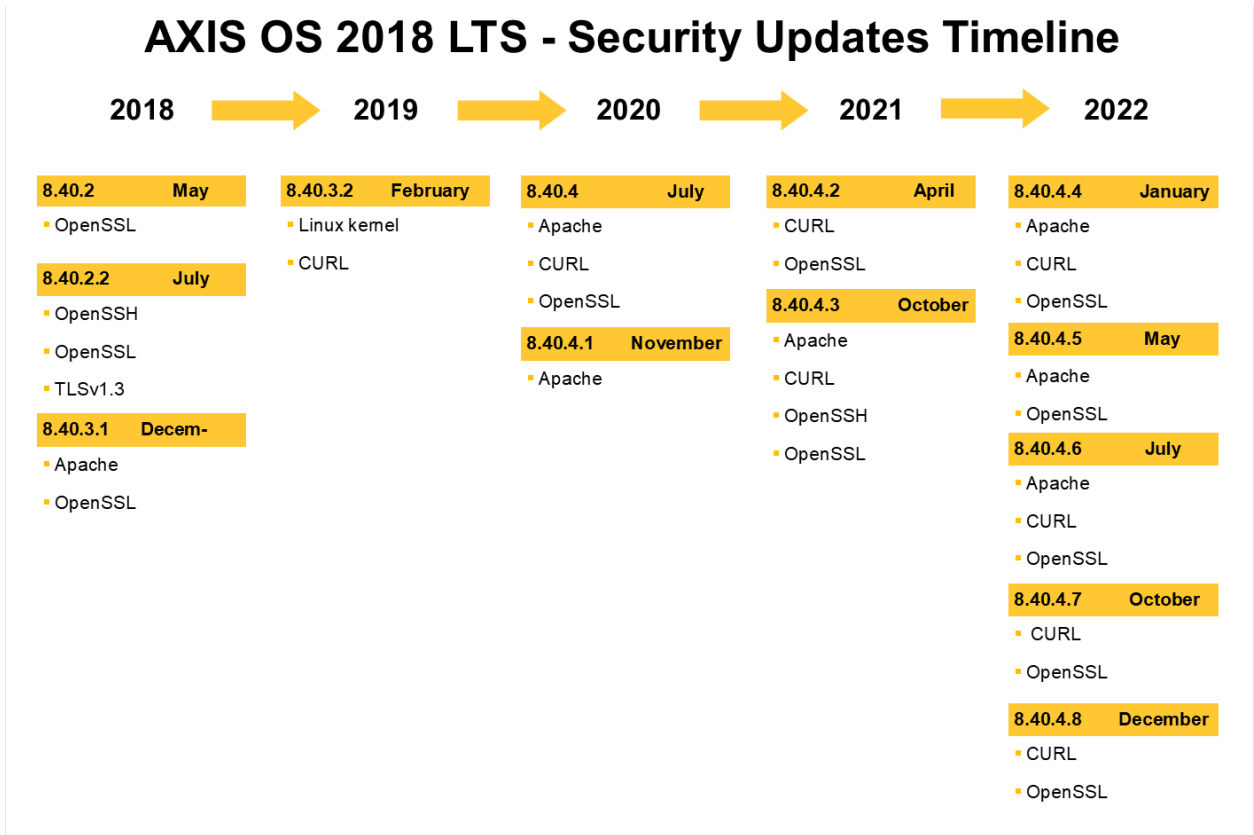


Axis provides a forecast for upcoming releases with information about important new features, bug fixes and security patches. To read more, see *Upcoming releases* in *AXIS OS Information*. Visit *Firmware* at axis.com to download AXIS OS for your device.

This chart illustrates the importance of keeping Axis devices up to date.

AXIS OS Hardening Guide

Basic hardening



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 > Firmware upgrade

Configure administrator account

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

The administrator account is the primary account for managing your Axis device. When setting up your device, you'll need to create a username and password. Use a strong password and reserve this account for administrative tasks only. To maintain security, we advise against using the administrator account for daily operations.

When operating Axis devices, using the same password simplifies management but increases your vulnerability to breaches and data leaks. Using unique passwords for each single Axis device provides high security but makes device management more complex.

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.

AXIS OS Hardening Guide

Basic hardening

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

Create dedicated accounts

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

Administrator accounts have full privileges and should be reserved for administrative tasks. We recommend that you create a client user account with limited privileges for daily operation. This reduces the risk of compromising the device administrator password.

For more information, see the *identity and access management* section in the *AXIS OS Knowledge Base*.

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

Limit web interface access

CSC #5: *Account Management*

Axis devices have a web server that allows users to access the device via a standard web browser. The web interface is intended for configuration, maintenance, and troubleshooting. It's not intended 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. For more information, see .

Disable web interface access

CSC #4: *Secure Configuration of Enterprise Assets and Software*

Starting from 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

AXIS OS Hardening Guide

Basic hardening

Configure network settings

CSC #12: Network Infrastructure Management

The device IP configuration depends on the network configuration, such as IPv4/IPv6, static or dynamic (DHCP) network address, subnet mask, and default router. We recommend that you review your network topology whenever you add new types of components.

We also recommend that you use static IP address configuration on your Axis devices to ensure network reachability and disentangle the dependency to servers in the network (such as DHCP servers) that might be a target for attacks.

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

Configure date and time settings

CSC #8: Audit Log Management

From a security perspective, it's important that you set the correct date and time. This ensures, for example, that system logs are correctly time-stamped and that digital certificates can be validated and used during runtime. Without proper time-sync, services that rely on digital certificates such as HTTPS, IEEE and 802.1x may not work correctly.

We recommend that you keep the Axis device clock synchronized with Network Time Protocol (NTP, unencrypted) servers or - preferably - Network Time Security (NTS, encrypted) 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 time-sync accuracy but also to account for a failover scenario where one of the configured time servers might be unavailable.

Using public NTP or NTS servers can be an alternative for individuals and small organizations that can't facilitate local time server instances themselves. 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

AXIS OS Hardening Guide

Basic hardening

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

Export recording encryption

CSC #3: Data Protection

Starting from AXIS OS 10.10, Axis devices 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

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

Disable unused services/functions

CSC #4: Secure Configuration of Enterprise Assets and Software

AXIS OS Hardening Guide

Basic hardening

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.

Unused physical 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

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 > LLDP and CDP**

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

** Disabling LLDP and CDP could impact the PoE power negotiation.

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's 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.

AXIS OS Hardening Guide

Basic hardening

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

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)

HTTP(S) server headers

By default, Axis devices announce their current Apache and OpenSSL versions during HTTP(S) connections with clients on the network. This information is useful when you use network security scanners on a regular basis since it provides a more detailed report of outstanding vulnerabilities in a particular AXIS OS version.

It's possible to disable the HTTP(S) server headers to reduce information exposure during HTTP(S) connections. However, we only recommend that you disable the headers if you operate your device according to our recommendations and keep it up to date at all times.

The option to disable the HTTP(S) server headers is available starting from 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
≥ 10.9	System > Plain config > System > HTTP Server Header Comments

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 Hardening Guide

Basic hardening

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

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 Portal. For information about debugging options using FTP, see *FTP access* in AXIS OS Portal.

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

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

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 Hardening Guide

Basic hardening

AXIS OS version	Web interface configuration path
< 5.50	For instructions, see <i>Device access</i> 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

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

IP address filter

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

IP address filtering prevents unauthorized clients from accessing the Axis device. We recommend that you configure your device to either allow the IP addresses of authorized network hosts or to deny the IP addresses of unauthorized network hosts.

If you choose to allow IP addresses, make sure to add all authorized clients (VMS server 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*	Settings > Security > IP address filter

* In AXIS OS 11.9 and later versions, the IP address filter has been replaced by the new host-based firewall.

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

AXIS OS Hardening Guide

Basic hardening

Host-based firewall

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

Users can use the firewall to create rules to regulate the ingress traffic toward the devices by IP address and/or TCP/UDP port numbers. Thus, it can prevent unauthorized clients from accessing the Axis device or particular services on the device.

If you set the default policy to "Deny", make 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	Setup > Security > Firewall

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 [and](#) .

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.

Starting from AXIS OS 7.20, Axis devices come with a self-signed certificate. 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

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 Hardening Guide

Basic hardening

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.

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

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*

AXIS OS Hardening Guide

Extended hardening

Extended hardening

The instructions for extended hardening build on the hardening topics described in and . 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 exposure

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 small organizations and individuals that don't operate a VMS or need to access video from remote locations, we recommend using AXIS Companion.

AXIS Companion employs Windows/iOS/Android client software, is free of charge, and provides an easy way to access video securely without exposing the Axis device to the Internet. For more information about AXIS Companion, see axis.com/companion.

Note

All organizations that use a VMS should consult the VMS vendor for best practices about remote video access.

Limit network exposure

CSC #12: Network Infrastructure Management

A common way to reduce the risks of network exposure is to physically and virtually isolate network devices and related infrastructure and applications. Examples of such infrastructure and applications are video management software (VMS), network video recorders (NVR), and other types of surveillance equipment.

We recommend that you isolate your Axis devices and related infrastructure and applications on a local network that isn't connected to your production and business network.

To apply basic hardening, protect the local network and its infrastructure (router, switches) from unauthorized access by adding a multilayer of network-security mechanisms. Examples of such mechanisms are VLAN segmenting, limited routing capabilities, virtual private network (VPN) for site-to-site or WAN access, network layer 2/3 firewalling, and access control lists (ACL).

To extend the basic hardening, we recommend that you apply more advanced network inspection techniques, such as deep packet inspection and intrusion detection. This will add consistent and comprehensive threat protection within the network. Extended network hardening requires dedicated 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, either on the LTS or 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 helpdesk ticket to *Axis support* on axis.com.

AXIS OS Hardening Guide

Extended hardening

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.

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

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.

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.

SNMP monitoring

CSC #8: Audit Log Management

AXIS OS Hardening Guide

Extended hardening

Axis devices support the following SNMP protocols:

- **SNMP v1**: supported for legacy reasons only, do not use.
- **SNMP v2c**: can be used on a protected network segment.
- **SNMP v3**: recommended for monitoring purposes.

Axis devices also support monitoring MIB-II and Axis Video MIB. To download Axis Video MIB, see *Axis Video MIB* in AXIS OS Knowledge base.

To learn more about how you configure SNMP in AXIS OS, see *SNMP (Simple Network Management Protocol)* in AXIS OS Knowledge base.

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

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 <i>Syslog</i> in AXIS OS Portal
≥ 7.10	Settings > System > TCP/IP
≥ 10.9	System > Logs

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

AXIS OS Hardening Guide

Extended hardening

Signed video

CSC #3: Data Protection

Starting from AXIS OS 10.11, Axis devices with Axis Edge Vault support signed video. With signed video, Axis devices can 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. The video management system (VMS) or evidence management system (EMS) can also verify the authenticity of the 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

AXIS OS Hardening Guide

Quickstart guide

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 , however, it doesn't cover the topics in 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

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 and .

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 .

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 . For configuration recommendations, see .

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 .

Basic hardening via VAPIX API

You can use the VAPIX API to harden your Axis devices based on the topics covered in . 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.

AXIS OS Hardening Guide

Quickstart guide

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

AXIS OS Hardening Guide

Quickstart guide

Purpose	VAPIX API call
<i>TLS 1.2 secure cipher configuration</i>	<pre>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:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384</pre>
<i>Enable brute force attack protection***</i>	<pre>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</pre>
<i>Disable script editor environment</i>	<pre>https://ip-address/axis-cgi/param.cgi?action=update &System.EditCgi=no</pre>
<i>Enable improved user access logging</i>	<pre>https://ip-address/axis-cgi/param.cgi?action=update &System.AccessLog=On</pre>
<i>Enable ONVIF replay attack protection</i>	<pre>https://ip-address/axis-cgi/param.cgi?action=update &WebService.UsernameToken.ReplayAttackProtection=yes</pre>
<i>Disable device web interface access</i>	<pre>https://ip-address/axis-cgi/param.cgi?action=update &System.WebInterfaceDisabled=yes</pre>
<i>Disable HTTP/OpenSSL server header</i>	<pre>https://ip-address/axis-cgi/param.cgi?action=update &System.HTTPServerTokens=no</pre>
<i>Disable anonymous viewer and PTZ access</i>	<pre>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</pre>

AXIS OS Hardening Guide

Quickstart guide

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

* 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 . Use this *configuration file*, which consists of the same configuration settings listed in .

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.

