AXIS OS Hardening Guide

Introduction

Introduction

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

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

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

The guide provides technical advice for anyone involved in deploying Axis solutions. It establishes a baseline configuration as well as a hardening guide that deals with the evolving threat landscape. You may need the product's user manual to learn how to configure specific settings. Note that Axis devices updated the user interface in firmware versions 7.10 and 10.9.

Web interface configuration
The guide refers to modifying device settings within the web interface of the Axis device according to the following instructions:

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

Changelog for AXIS OS Hardening Guide

Date & time	Version	Changes
March 2022	2.0	Overhaul of current hardening guide

Scope

The hardening instructions outlined in this guide are written for, and can be applied to, all AXIS OS-based products that are running an AXIS OS LTS or active track firmware. Legacy products running 4.xx and 5.xx firmware are also in scope.

AXIS OS Hardening Guide

Introduction

Security notifications

It is recommended to subscribe to *Axis security notification service* to receive information about newly discovered vulnerabilities in Axis products, solutions and services and other security-related technical information that contribute to operating Axis devices in a secure manner.

CIS protection levels

As a means of structuring our recommendations in the context of a cybersecurity framework, Axis has chosen to follow the methods outlined in Center for Internet Safety (CIS) Controls - Version 8. The CIS controls, previously known as 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 item. For more information on the CSC categories, see *https://www.cisecurity.org/controls/cis-controls-list*.

Default protection

Axis devices are delivered with predefined default protection settings. There are several security controls that you do not need to configure. These controls allow for basic device protection and serve as the fundament for more extended hardening.

Disabled by default

CSC #4: Secure Configuration of Enterprise Assets and Software

The Axis device will not operate until the administration password is set.

For more guidance on how to configure device access, see *https://help.axis.com/axis-os#device-access*.

Credentialed access

After setting the administration password, access to administrative functions and/or video streams is only provided via authentication using valid username/password credentials. It is not recommended to enable e.g. anonymous viewer and/or always multicast video/audio functionality, which would allow for the opposite.

Network protocols

CSC #4: Secure Configuration of Enterprise Assets and Software

Only a minimum number of network protocols and services are enabled by default in Axis devices. In the table below 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	UDP	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 3rd party applications to discover the Axis device via UPnP discovery protocol
Bonjour	5353	UDP	Used by 3rd party applications to discover the Axis device via mDNS discovery protocol (Bonjour)

Default protection

Protocol	Port	Transport	Comments
SSDP	1900	UDP	Used by 3rd party applications to discover the Axis device via SSDP (UPnP)
WS-Discovery	3702	UDP	Used by 3rd party applications to discover the Axis device via WS-Discovery protocol (ONVIF)

** Allocated automatically within a predefined range of port numbers according to RFC 6056. More information can be found here.*

It is recommended to 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 *https://help.axis.com/axis-os#commonly-used-network-ports*.

For instance, audio in/out and microphone functionality are disabled by default and must be enabled before use in Axis video surveillance-oriented products, such as the network cameras. In Axis intercoms and network speakers on the other hand, where audio in/out and microphone functionality are main features, audio capabilities are enabled by default.

UART/Debug interface

CSC #4: Secure Configuration of Enterprise Assets and Software

Every Axis device incorporates a so called physical UART (Universal Asynchronous Receiver Transmitter) interface, sometimes referred to as a debug port or serial console. The interface itself is not easily accessible. To gain physical access, extensive dismantling of the Axis device is required. The UART/debug interface is used only for product development and debugging purposes during internal R&D engineering projects within Axis.

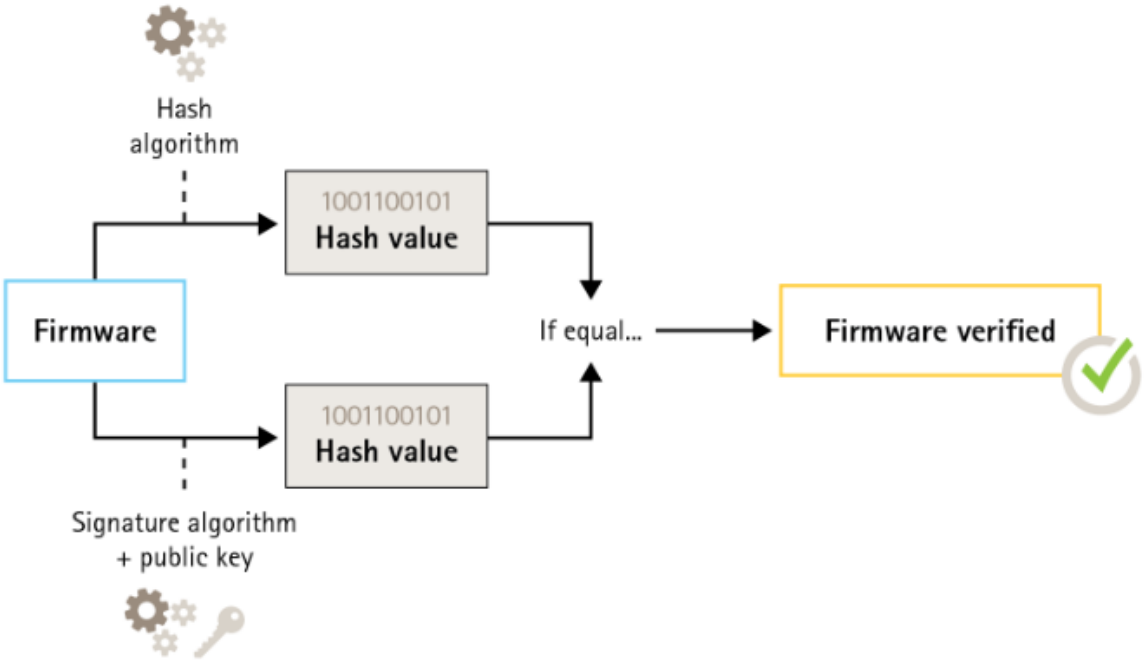
For Axis devices with AXIS OS 10.10 and lower, the UART/debug interface is enabled by default, but it requires authenticated access and does not expose any sensitive information while being unauthenticated. From AXIS OS 10.11 and onwards, the UART/debug interface is disabled by default and can only be enabled by unlocking it via a device-unique custom firmware certificate. This is provided by Axis only and cannot be generated in any other way.

Signed firmware

CSC #2: Inventory and Control of Software Assets

All Axis firmware is signed from version 9.20.1. When upgrading the device with a new firmware the device will check the integrity of the firmware and reject tampered firmware. This will prevent attackers from luring users to install a compromised firmware.

Default protection

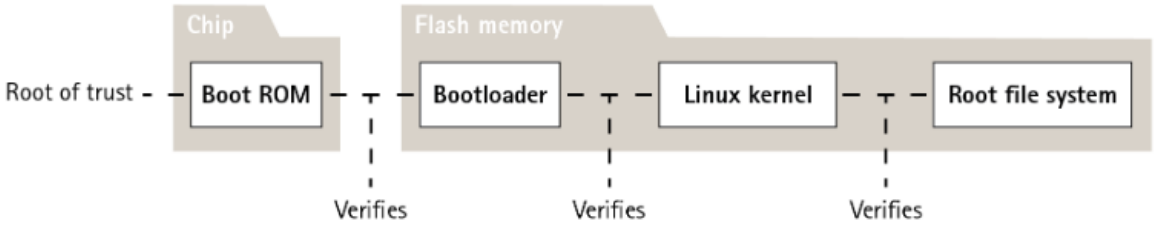


For more information about Axis signed firmware, see the *Cybersecurity features in Axis products* white paper.

Secure boot

CSC #2: Inventory and Control of Software Assets

Most Axis devices have secured the boot sequence. This secures the integrity of the device by ensuring that only untampered devices can be deployed.



For more information about secure boot, see the *Cybersecurity features in Axis products* white paper.

Secure key store

CSC #6: Access Control Management

Axis Edge Vault (AEV)
Selected Axis devices have a dedicated hardware security module for secure key storage, sensitive login credentials as well as more secure features.

Trusted platform module (TPM)
Selected Axis devices have a dedicated hardware security module for secure key storage. This increases the protection of encryption keys stored on the device.

For more information about trusted platform modules in Axis products, see the *Cybersecurity features in Axis products* white paper.

HTTPS enabled

CSC #3: Data Protection

HTTPS is enabled by default with a self-signed certificate since AXIS OS 7.20. This enables setting the device password in a secure way. In AXIS OS 10.10 and higher, the self-signed certificate has been 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

Digest authentication

CSC #3: Data Protection

Clients accessing the device will authenticate with a password that should be encrypted when sent over the network. Therefore it is recommended to use Digest authentication only instead of Basic or Basic & 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 with the purpose to ensure that ONVIF-based user authentication is sufficiently secured 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 password digest is used to both validate the user and to avoid replay attacks, and due to this digests are cached. It is recommended to 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

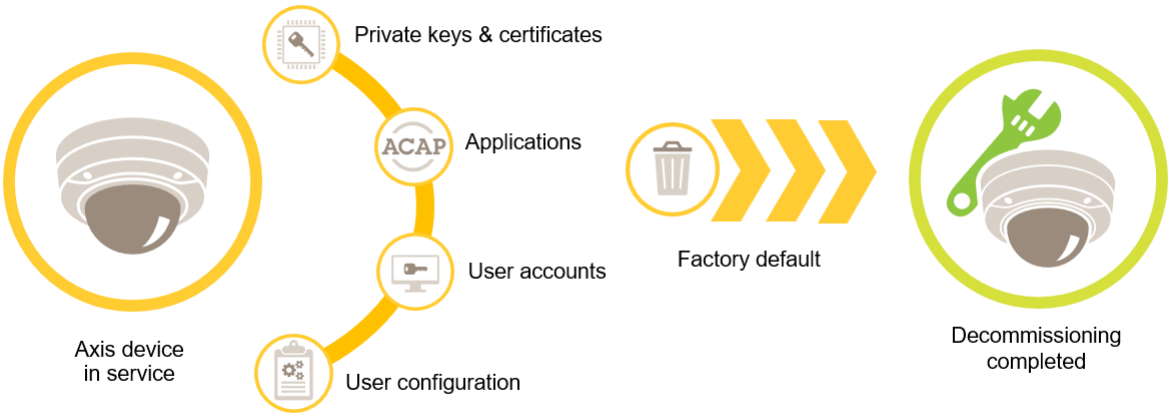
Default protection

Decommissioning

CSC #3: Data Protection

When decommissioning an Axis device, a factory default should be performed. After the factory default, all data is erased by overwriting/sanitization.

Axis devices use both volatile and non-volatile memory, and while the volatile memory is erased when removing the power, information stored in the non-volatile memory remains and is made available again at start-up. The commonly known concept of just removing the data pointers in order to make the current data invisible for the filesystem is not applied, which is why a factory default is required.



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

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

Information and data	Erased after factory default
VAPIX and ONVIF users/passwords	Yes
Root user/password	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 firmware certificates*	No
SD card encryption key	Yes
SD card data**	No

Default protection

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

** Custom firmware certificates are used in the signed firmware process to allow the user to e.g. upload Axis official firmware.*
*** Recording and images stored on edge storage (SD card, network share) have to be deleted by the user separately. For more information, see .*
**** All user-made configurations, from setting the initial root password to network-, O3C-, event-, image-, PTZ- and system configurations.*
***** Applications that are pre-installed are kept but their configuration is erased nevertheless.*
****** Production data (calibration, 802.1AR production certificates) as well as lifetime statistics include non-sensitive and non-user related information.*

Basic hardening

The basic hardening is the minimum level of protection recommended for Axis devices. The below listed hardening items are "configurable on the edge", meaning they can be directly configured in the Axis device without having further dependencies to any 3rd party network infrastructure, video or evidence management systems (VMS, EMS), or other 3rd party equipment or application.

Factory default settings

CSC #4: Secure Configuration of Enterprise Assets and Software

Before starting, make sure that the device is in a known factory default state. The factory default is important when decommissioning devices as well as clearing user-data. For more information, see *Decommissioning on page 8*.

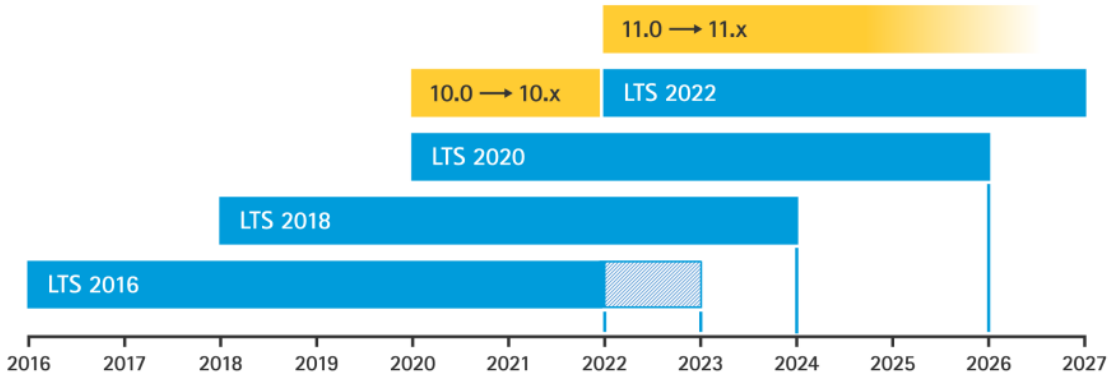
AXIS OS version	Web interface configuration path
< 7.10	Setup > System Options > Maintenance > Default
>= 7.10	Settings > System > Maintenance > Default
>= 10.9	Maintenance > Default

Upgrade to latest firmware

CSC #2: Inventory and Control of Software Assets

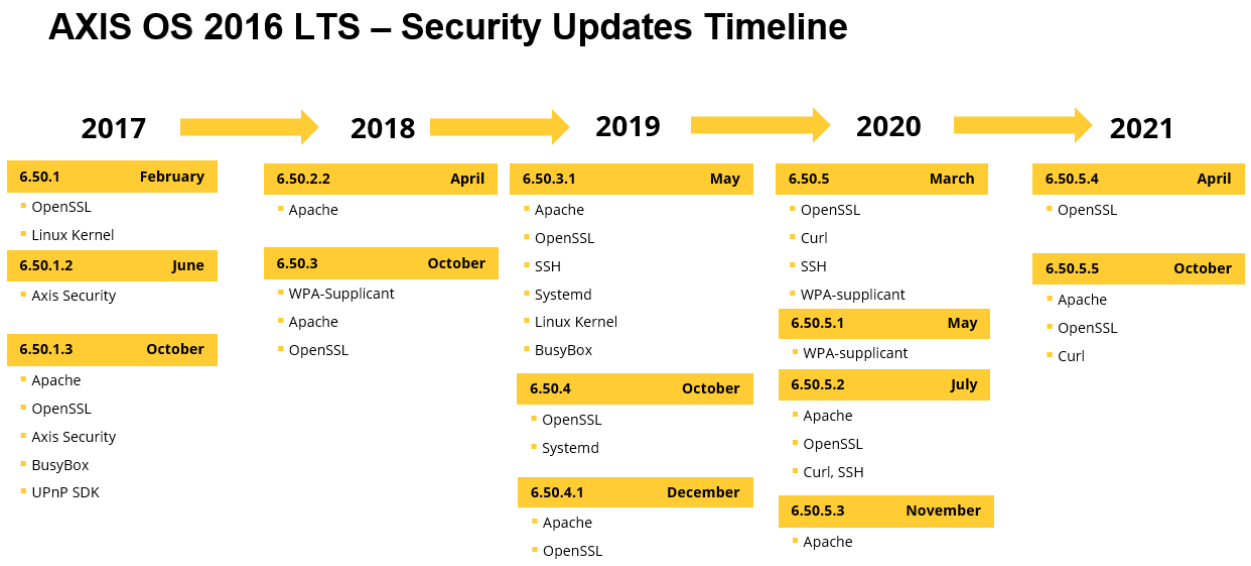
Patching software and firmware is an important aspect of cybersecurity. An attacker will often try to exploit commonly known vulnerabilities, and if they gain network access to an unpatched service, they may succeed. Make sure you always use the latest firmware since it may include security patches for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

Axis maintains two types of firmware 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 in order to minimize the risk of compatibility issues.



Axis provides a forecast for upcoming releases outlining important new features, bug fixes and security patches at *https://help.axis.com/axis-os#upcoming-releases*. Firmware for AXIS OS-capable devices can be downloaded at *https://www.axis.com/support/firmware*.

The below chart illustrates the importance of keeping the firmware of the Axis devices up to date.



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

Set device root password

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

The device root account is the main device administration account. The device password needs to be set before it becomes operational. Make sure to use a strong password and limit the usage of the root account to administration tasks only. It is not recommended to use the root account in daily production.

When operating Axis devices, using the same password simplifies management but lowers the security in case of breach or data leak. Using unique passwords for each single Axis device provides high security but comes with an increased complexity to device management. Password rotation is recommended.

It is recommended to implement sufficient password complexity and length, such as *NIST password recommendations*. Axis devices support passwords up to 64 characters. Passwords **shorter than 8 characters** are considered weak.

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

Create a video client account

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

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

For more information about identity and access management in video surveillance systems, see the following *white paper*.

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

Limit web interface access

CSC #5: Account Management

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

The only clients that should be allowed to interact with 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. *Disable web interface access on page 12* outlines the possibility to disable the web interface of the Axis device.

Disable web interface access

CSC #4: Secure Configuration of Enterprise Assets and Software

From AXIS OS 9.50 and onwards, the web interface of Axis devices can be disabled. After an Axis device is deployed into a system (or added to AXIS Device Manager), it is recommended to prevent people within the organization from using a web browser to access the device. This adds protection if the device account password is spread within the organization.

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

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. It is recommended to review your network topology when adding new types of components.

It is recommended to use static IP address configuration on Axis devices to ensure network reachability and disentangle the dependency to e.g. a DHCP server in the network 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

Basic hardening

Configure date and time settings

CSC #8: Audit Log Management

From a security perspective, it is important that the date and time are correct so that, for example, the system logs are time-stamped with the right information, and digital certificates can be validated and used during runtime. Without proper time-sync, services that rely on digital certificates such as HTTPS, IEEE 802.1x, and others may not work correctly.

It is recommended that the Axis device clock is synchronized with Network Time Protocol (NTP, unencrypted) servers or preferably with Network Time Security (NTS, encrypted) servers. Network Time Security (NTS) as encrypted and secure variant of the Network Time Protocol (NTP) was added in AXIS OS 11.1. It is advised to configure multiple time servers for higher time-sync accuracy but also account for a fail-over scenario where one of the configured time servers might be unavailable.

Using a public NTP or NTS servers can be an alternative for individuals and small organizations that cannot facilitate a local time server instances themselves. For more information about NTP/NTS in Axis devices,, see *Network Time Protocol*.

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

Edge storage encryption

CSC #3: Data Protection

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

To learn more about SD card encryption in Axis devices, see *https://help.axis.com/axis-os#sd-card-support*.

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 a Network Attached Storage (NAS) is used as a recording device, it should be protected in a locked area with limited access and have hard disc encryption enabled. Axis devices utilize SMB as network protocol for connecting to a NAS in order to store video recordings. While earlier versions of SMB (1.0 and 2.0) do not provide any security or encryption, later versions (2.1 and higher) do, which is why later versions are recommended to use during production

To learn more about proper SMB configuration when connecting an Axis device to a network share, see *https://help.axis.com/axis-os#network-share*.

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

From AXIS OS 10.10 and onwards, Axis devices have support for encrypted export of edge recordings. This is recommended to use since it will prevent unauthorized individuals from being able to play the 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

Applications can be uploaded onto the Axis device to extend its functionality and can even provide their own user interface for interacting with a certain feature. Applications may use security functionality that is provided by the AXIS OS operating system on the device.

Axis devices are preloaded with several *Axis developed applications (ACAPs)*, which are developed according to the *Axis security development model (ASDM)*. For 3rd party applications it is recommended to contact the vendor to learn the proof points on how securely a 3rd party application is being operating, tested and if it has been developed according to common best-practices security development models. Vulnerabilities that are found in 3rd party applications have to be reported to the 3rd party vendor directly.

It is recommended to only operate trusted applications and to 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

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

One-click cloud connection (O3C, AVHS)

O3C is a service used to deploy Axis devices to cloud-based video management services. Pressing the control button on the Axis device registers the device on the hosting service dispatcher. The dispatcher will allow a user who has access to the Axis device and provides the correct Owner Authentication Key (OAK) to claim the Axis device.

To prevent the Axis device from connecting to the dispatcher when the physical control button is pressed, consult the user manual.

AXIS OS version	Web interface configuration path
< 7.10	Setup > Basic Setup > Services > Enable AVHS
>= 7.10	Settings > System > O3C
>= 10.9	System > Network > One-click cloud connection

Basic hardening

Network discovery protocols

Discovery protocols, such as Bonjour, UPnP, ZeroConf and WebService Discovery, are support services that make it easier to find the Axis device and its services on the network. After deployment, once the Axis device IP address is known and the Axis device is added to the VMS, it is recommended to 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 > Network Bonjour Enabled, Network UPnP Enabled, Network ZeroConf Enabled
	System > Plain config > WebService > Discovery Mode Enabled

** Functionality has been removed in AXIS OS 10.2 and onwards*

Outdated TLS versions

It is recommended to make sure that older, outdated, and insecure TLS versions are disabled before the product is put in production. The outdated versions are usually disabled per default, but Axis devices offer the possibility to enable them to allow backwards-compatibility to 3rd party applications that have not yet implemented TLS 1.2 and TLS 1.3.

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	System > Plain config > HTTPS > Allow TLSv1.0 and/or Allow TLSv1.1

Script editor environment

It is recommended to make sure that the script editor environment access is disabled. The script editor is used for troubleshooting and debugging purposes only.

The script editor has been removed in AXIS OS 11.1 and onwards.

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)

Basic hardening

HTTP(S) server headers

By default, the Axis device announces its current running Apache and OpenSSL versions during HTTP(S) connections with clients on the network. This information is useful when a customer is utilizing a network security scanner on a daily or weekly basis to allow for more detailed reporting of outstanding vulnerabilities in a particular firmware version.

It is always recommended to keep the Axis device up-to-date. However, if the Axis device is operated as recommended by Axis and is ensured to always be up-to-date, these headers may be disabled to reduce the information exposure by the Axis device upon HTTP(S) connections. This option is available from AXIS OS 10.6 and onwards.

AXIS OS version	Web interface configuration path
< 7.10	N/A
>= 7.10	Settings > System > Plain config > System > HTTP Server Headers Comments
>= 10.9	System > Plain config > System > HTTP Server Headers Comments

Audio

Audio in/out and microphone functionality are disabled by default and must be enabled before use in Axis video surveillance-oriented products, such as the network cameras. In products where audio in/out and microphone functionality are main features, such as Axis intercoms and network speakers, audio capabilities are enabled by default. It is recommended to disable audio capabilities if not used.

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, but possibly more SD cards, to allow for local edge storage recording of video footage. It is recommended to disable the SD card slot entirely if no SD card is used. This option is available from AXIS OS 9.80 and onwards.

For further reading, see *https://help.axis.com/axis-os#disabling-the-sd-card*.

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

It is recommended to make sure that the FTP access is disabled. FTP is an insecure communication protocol used for troubleshooting and debugging purposes only. FTP access has been removed in AXIS OS 11.1 and onwards. For troubleshooting purposes it is recommended to use secure SSH access, see https://help.axis.com/axis-os#ssh-access.

For more guidance on the debugging possibilities using FTP, see *https://help.axis.com/axis-os#ftp-access*.

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 supported by Axis devices with firmware 5.50 and higher. It is recommended to make sure that the SSH access is disabled. SSH is a secure communication protocol used for troubleshooting and debugging purposes only.

For more guidance on the debugging possibilities using SSH, see *https://help.axis.com/axis-os#ssh-access*.

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 supported by Axis devices with firmware versions below 5.50. It is recommended to make sure that the Telnet access is disabled. Telnet is an insecure communication protocol used for troubleshooting and debugging purposes only.

AXIS OS version	Web interface configuration path
< 5.50	Instructions can be found *here*
< 7.10	N/A
>= 7.10	N/A
>= 10.9	N/A

ARP/Ping

ARP/Ping was a method for setting the Axis device IP address using e.g. AXIS IP Utility. The functionality was removed in AXIS OS 7.10 and it is recommended to disable the feature in Axis devices running lower AXIS OS 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

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

Enabling IP filtering only for authorized clients will prevent the Axis device from responding to network traffic from any other clients. It is recommended to either allow or block the IP addresses of network hosts to ensure that only hosts that are authorized can access the Axis device. Make sure to add all authorized clients (VMS server and administrative clients) to your allowlist.

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

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, e.g. to password-guess the login credentials. The feature called *brute-force delay protection* is available from AXIS OS 7.30 and onwards.

For detailed configuration examples and recommendations, see *https://help.axis.com/axis-os#brute-force-delay-protection*.

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

HTTPS

CSC #3: Data Protection

Axis devices have HTTP and HTTPS enabled by default since 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. It is recommended to use HTTPS for all administrative tasks on the Axis device. Please follow the instructions below to configure the Axis device properly for HTTPS and corresponding cipher settings.

HTTPS only

It is recommended to configure the Axis device for HTTPS only (no HTTP access possible). Having HTTPS only enabled will also automatically enable HSTS (HTTP Strict Transport Security) to further enhance device security.

While a self-signed certificate is not trusted by design, it is adequate for secure access to the Axis device during initial configuration and for when no public key infrastructure (PKI) is available at hand. If available, the self-signed certificate should be removed and replaced with proper signed client certificates of the PKI-authority of choice.

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 a variety of ciphers that are used to securely encrypt HTTPS connections from the Axis device into the network. After factory defaulting the Axis device, the list of ciphers may be updated automatically according to the configuration of the firmware the Axis device is running. Please refer to the below list of secure and strong ciphers only, which should be configured and used during production (as of February 2022):

TLS 1.2 and lower

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

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
Per default, only strong ciphers according to the TLS 1.3 specification will be selected. These are not user configurable. Currently (as of February 2022) these ciphers are:

TLS_AES_128_GCM_SHA256:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_256_GCM_SHA384

Access log

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

Enabling the access log will yield more detailed logging of user access towards the Axis device, which will simplify audits and access control. It is recommended to use this feature in combination with setting up a remote syslog server so that the Axis device can send its logs to a central logging environment, which simplifies storage of log messages and their retention time.

For more information about device logging in Axis devices, see *https://help.axis.com/axis-os#device-access-logging*.

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 accessories in order to enhance the physical tampering protection of Axis devices. When in place, these anti-tampering accessories trigger an alarm that enables the Axis device to send out a notification or an alarm to selected clients.

For more information about available anti-tampering accessories for Axis devices, go to:

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

Extended hardening

The hardening instructions outlined in this section are an extension that build on the default and basic hardening described in previous sections. While the default and basic hardening can be configured and enabled directly in the Axis device, the extended hardening of Axis devices require active participation by the entire vendor supply chain, as well as the end-user organization and the underlying IT- and/or network infrastructure.

Limit internet exposure

CSC #12: Network Infrastructure Management

It is not recommended to expose the Axis device as a public web server or public network access of any kind, allowing unknown clients to gain network access to the device. Axis recommends using AXIS Companion for individuals and small organizations that do not operate a VMS nor need to access video from remote locations.

AXIS Companion employs Windows/iOS/Android client software, is free of charge, and provides an easy way to access video in a secure way without exposing the Axis device to the Internet. More information about AXIS Companion can be found at *www.axis.com/companion*. All organizations that use a VMS should consult the VMS vendor for their best practices regarding remote video access.

Limit network exposure

CSC #12: Network Infrastructure Management

It is recommended to segment and place Axis devices and corresponding infrastructure/applications, such as the video management system (VMS), network video recorders (NVR) and other types of surveillance equipment, on an isolated local network that is decoupled from the production and business network. Physical and virtual isolation is a common and recommended counter measure to reduce exposure and risks.

As for basic hardening, the local network and its infrastructure (router, switches) should be access-protected by a multilayer of network-security mechanism, such as VLAN segmenting, limited routing capabilities, virtual private network (VPN) for site-to-site or WAN access, as well as network layer 2/3 firewalling and access control lists (ACL).

To extend the basic hardening, it is recommended to apply more advanced network inspection techniques, such as deep packet inspection and intrusion detection, to apply 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

It is recommended to perform regular vulnerability assessments of the infrastructure the Axis device is part of as well as of the Axis device itself. These vulnerability assessments are usually performed by network security scanners.

The purpose of a vulnerability assessment is to provide a systematic review of potential security vulnerabilities and misconfigurations. Please make sure that the Axis device being tested is updated to the latest available LTS or active track firmware before starting the scan.

It is recommended to review the scanning report and filter out known false-positives for Axis devices stated *here*.

The report and remaining remarks that are left should be submitted in a helpdesk ticket to *Axis support*.

Trusted public key infrastructure (PKI)

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

Extended hardening

It is recommended to deploy web server and client certificates in Axis devices that are trusted and signed by a public or private Certificate Authority (CA) of choice. A CA-signed certificate whose trust chain can be validated helps to remove browser certificate warnings when connecting over HTTPS and ensures the authenticity of the Axis device when deploying a Network Access Control (NAC) solution. This mitigates the risk of an attacking computer impersonating an Axis device. Note that AXIS Device Manager has a built-in CA service that can be used 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 have support for IEEE 802.1x port-based network access control utilizing the EAP-TLS method. For optimal protection, authentication of Axis devices must utilize client certificates signed by a trusted Certificate Authority (CA) of choice.

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 802.1AR 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 new network standard IEEE 802.1AR, which allows for automated and secure onboarding of Axis devices into the network via the Axis device ID, a globally unique certificate installed in the device during production. For more information, see the *Cybersecurity features in Axis products* white paper.

The Axis root certificates used to validate the device identity of Axis devices can be downloaded here: *https://help.axis.com/axis-os#device-access*.

SNMP monitoring

CSC #8: Audit Log Management

Axis devices support the following SNMP protocols:

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

Axis devices support monitoring MIB-II and AXIS Video MIB. AXIS Video MIB can be downloaded here: *https://help.axis.com/axis-os#axis-video-mib*. For more guidance on how to configure SNMP in AXIS OS, see *https://help.axis.com/axis-os#simple-network-management-protocol-snmp*.

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

Extended hardening

Remote syslog

CSC #8: Audit Log Management

Axis devices can be configured to send all log messages encrypted to a central syslog server. This simplifies audits and prevents log messages from being deleted in the Axis device either intentionally/maliciously or unintentionally. It also allows for extended retention time of device logs depending on company policies.

For details about how to enable remote syslog server in different AXIS OS versions, see *https://help.axis.com/axis-os#syslog*.

AXIS OS version	Web interface configuration path
< 7.10	Instructions can be found *here*
>= 7.10	Settings > System > TCP/IP
>= 10.9	System > Logs

Secure video streaming (SRTP/RTSPS)

CSC #3: Data Protection

From AXIS OS 7.40 and onwards, Axis devices support secure video streaming over RTP, referred to as SRTP or RTSPS. It is recommended to enable SRTP/RTSPS if the video management system (VMS) supports it. The Axis device's video stream will then be received via a secure end-to-end encrypted transportation method by authorized clients only. If available, SRTP should be used in favor over unencrypted RTP video streaming.

Note that SRTP/RTSPS is only encrypting the video stream data. For administrative configuration tasks performed on the Axis device, it is recommended to 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

Signed video

CSC #3: Data Protection

From AXIS OS 10.11 and onwards, Axis devices with support for Axis Edge Vault can add a signature to its video stream to make sure the video is intact and to verify its origin by tracing it back to the Axis device that produced it. Signed video allows the video management system (VMS) or evidence management system (EMS) to verify the authenticity of the video provided by an Axis device.

For more information, see the *Cybersecurity features in Axis products* white paper. The Axis root certificates used to validate the signed video authenticity can be found here: *https://help.axis.com/axis-os#device-access*.

AXIS OS version	Web interface configuration path
< 7.10	N/A
>= 7.10	N/A
>= 10.9	System > Plain config > Image > Signed video

Quickstart guide

The quickstart guide provides a short and effective overview of settings that should be configured for hardening Axis devices with AXIS OS 5.51 and onwards. The hardening items that are covered in the quickstart guide covers the *Basic hardening on page 10* section. The *Extended hardening on page 20* section is excluded since this requires extensive and customer-specific configuration on a case-by-case basis.

It is recommended to use AXIS Device Manager to harden multiple Axis devices in a quick and cost-efficient way. If another application needs to be used for device configuration, or if only a few number of devices need to be hardened directly, the VAPIX API is the recommended way to harden Axis devices.

Basic hardening via VAPIX API

See the below VAPIX API configuration samples on how to harden the Axis device according to the corresponding items in *Basic hardening on page 10*. The list includes all basic hardening configuration settings independently of the firmware version of the Axis device. It is possible that some configuration settings are not present in the AXIS OS version your device is running since some functionality has been removed to increase security. Receiving an error while issuing the VAPIX call would be an indication of the functionality no longer being present in the Axis device firmware.

Purpose	VAPIX API call
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`

Quickstart guide

Purpose	VAPIX API call

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`
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:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384`

*Enable brute force attack protection**	`https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.ActivatePasswordThrottling=c`
	`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=9`
	`https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.DoSPageInterval=30`
	`https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.DoSSiteCount=9`
	`https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.DoSSiteInterval=30`

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`

Purpose	VAPIX API call
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`

** After 10 failed login attempts within 30 seconds, the client IP address gets 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)

This *configuration file* can be used to harden Axis devices using AXIS Device Manager and AXIS Device Manager Extend according to the corresponding items in *Basic hardening on page 10*. The configuration file consists of the same items as listed in *Basic hardening via VAPIX API on page 23*. It is possible that some configuration settings are not present in the AXIS OS version your device is running since some functionality has been removed to increase security. AXIS Device Manager and AXIS Device Manager Extend will automatically remove settings from the hardening configuration that are no longer relevant.

Note

The Axis device will be configured to HTTPS only and the web interface will be disabled after uploading the configuration file. The example configuration file can be modified accordingly to desired needs by e.g. removing or adding parameters.

AXIS OS Hardening Guide
Ver. M14.2
Date: 2022
Part No.