

AXIS OS Portal

Table of Contents

.....	3
About	4
Release schedule.....	5
Breaking changes.....	6
Changes in AXIS OS 13	6
Security.....	6
API changes	10
ACAP applications	13
Miscellaneous	16
Changes in AXIS OS 14	16
Applied	17
Changes in AXIS OS 12.1	17
Changes in AXIS OS 12.0	19
Changes in AXIS OS 11.....	30
Next AXIS OS version	34
Current AXIS OS version	36
Open source library support	37
Software Bill of Materials	38
AXIS OS lifecycle management.....	39
Active track.....	39
Long-term support track.....	40
Product-specific support.....	40
Suggested track	40
Upgrade path.....	41
General recommendations.....	43
Downloading AXIS OS.....	44
AXIS OS versioning.....	45
AXIS OS Support	46

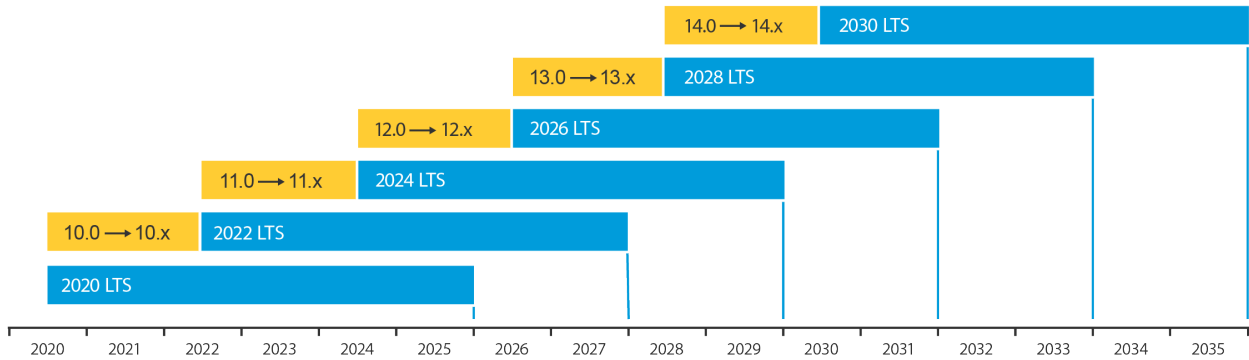
AXIS OS Release Notes | AXIS OS Knowledge base | AXIS OS YouTube playlist | AXIS OS Hardening Guide | Security Advisories

About

AXIS OS is our operating system for edge devices. It's used in more than 400 products with the broadest partner application reach in the security industry. It's a Linux-based OS that's built around openness, transparency and cybersecurity.

We have three support tracks: , , and .
See for more details.

AXIS OS support overview



The active track releases a new version every 2–3 months where only the latest version is supported. The LTS tracks are created every two years and are supported and maintained for about 5 years.

Release schedule

In the schedule below you can find information about upcoming releases on the active track and the LTS tracks.

Version	Track	Preliminary release date	Planned features and updates
12.5	Active	June 2025	• Apache version 2.4.63 • AXIS CVEs – CVE-2025-30027 – CVE-2025-3892
11.11	LTS 2024	May 2025	• AXIS CVEs – CVE-2025-0325
10.12	LTS 2022	May/June 2025	• time zone database version 2025b • Product specific corrections
9.80	LTS 2020	June 2025	• More info to come.
8.40	Product-specific support	May 2025	• AXIS CVEs – CVE-2025-0325 • cURL version 8.12.1 • OpenSSL version 1.1.1zb • OpenSSH version 9.9p2
6.50	Product-specific support	August/September 2025	• AXIS CVEs – CVE-2023-5677 – CVE-2025-0325 • cURL version 8.12.1 • OpenSSL version 1.1.1zb • OpenSSH version 9.9p2

- For highlights and detailed release notes on AXIS OS releases, visit *AXIS OS Release Notes*.
- For downloads, visit *Download device software* page.

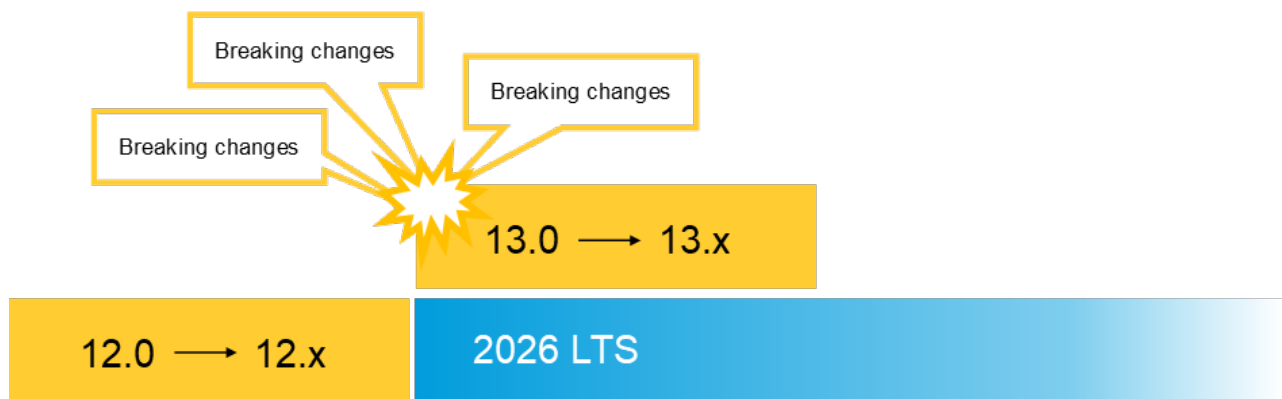
Subscriptions

- Axis provides a new email notification service for AXIS OS release updates and other important information. You can find the subscription link *here*.
- Subscribe to the *AXIS OS YouTube playlist* to conveniently stay updated and informed.
- If you are using RSS feed, you can subscribe to our  *product firmware feed*.

Breaking changes

Every two years, Axis introduces a new active track, transitioning the previous active track into a long-term support (LTS) phase. In September 2026, AXIS OS 12 will enter the LTS 2026 phase, while we introduce the new active track, AXIS OS 13.

In our active tracks, we focus on delivering innovative features to advance AXIS OS and enhance its cybersecurity. At the start of the new track, we introduce pre-announced breaking changes, communicating them well in advance, with further changes during the lifecycle of the active track taking place but with limited impact.



A breaking change is a deliberate modification that breaks backward compatibility. Although Axis makes every effort to ensure consistency, breaking changes are occasionally required in order to:

- **Improve cybersecurity:** Axis may remove obsolete features or modify existing features to enhance security.
- **Update functionality and improve usability:** Axis enhances existing functionality by implementing new default settings, change behavior, or introducing more advanced features to expand use cases.

In both scenarios, Axis provides an alternative method for accomplishing the same tasks and communicates these changes in advance. Furthermore, *** the active track is the only place where these changes can be made, as maintaining compatibility is the primary focus of LTS tracks.** Usually, these changes are implemented on the new active track after establishing a new LTS track, providing users with a reasonable timeframe to adjust their systems while maintaining security measures.

* An exception may apply if we are required to make changes due to a legal obligation.

Note

If you experience issues after upgrading to AXIS OS 13, utilize the rollback option to let the device revert back to its previous AXIS OS version. See guidelines [here](#). We recommend that you keep at least one device running AXIS OS 13, generate a server report and contact Axis Technical Support for troubleshooting assistance or guidance.

Changes in AXIS OS 13

Below is a list of changes that apply to the first version of AXIS OS 13, coming in September 2026. Please note that the changes can be adjusted in the future.

In late Q1 2026, you'll be able to download a version with all breaking changes available so you can test and verify them. More information to come.

Security

- **Password complexity enforcement**
Password complexity enforcement is considered best-practice when managing account credentials. Therefore, Axis will provide the possibility to enforce password complexity upon SSH, VAPXI, ONVIF account creation via profile selection:

Profile 1: Length-based according to NIST recommendations, whereas 15 characters will be required without further complexity requirements.

Profile 2: Complexity-based requiring 12 characters minimum, including at least 1 numbers, 1 capital, 1 small, 1 special.

See a preliminary screenshot of the new password complexity enforcement profile selection below

Add account

Account

New password ⓘ

Repeat password

Password Complexity Profile ⓘ

Length-based

- ✓ Length-based ⓘ
- Complexity-based
-

This profile complies with NIST-800b and Japan JC-Star requirements.

On upgrade or after a factory default: This change will affect upgrades and the factory defaulted state. For upgrades, only accounts created after the upgrade need to meet password complexity requirements. Existing accounts will not be considered and need to be adjusted manually.

Reason for change: Password complexity enforcement is considered best-practice to ensure better device security and increased protection against dictionary and brute-force attacks, especially for internet-connected devices that are exposed to a greater threat surface. This change will also shorten the hardening guide where password complexity needs to be taken into consideration.

Total Brute Force time in an online password attack without delay protection - 720 requests/sec*		
Number of characters	Only lower-case letters	Upper- and lower-case letters, and 0 to 9
4	~11 minutes	~ 6 hours
5	~ 5 hours	~ 14 days
8		~ 9615 years
10		~ 6.3 million years
14		~ 546.191 billion years

*Actual rate may vary and is depending on product performance.

The impacts: As a user, password complexity requirements entail a higher organizational burden when managing passwords and accounts on multiple devices. Password complexity needs to be taken into

consideration when onboarding unconfigured devices directly into Video Management Systems and other applications. Devices may require pre-configuration.

- HTTPS-only enforcement as default**

In AXIS OS 13, network connections to the device from factory will only be allowed using secure HTTPS/443 connections. In AXIS OS 12 and earlier, the device would allow both HTTPS/443 secure as well as HTTP/80 insecure connections.

HTTP and HTTPS

Allow access through

HTTPS

HTTPS port

443

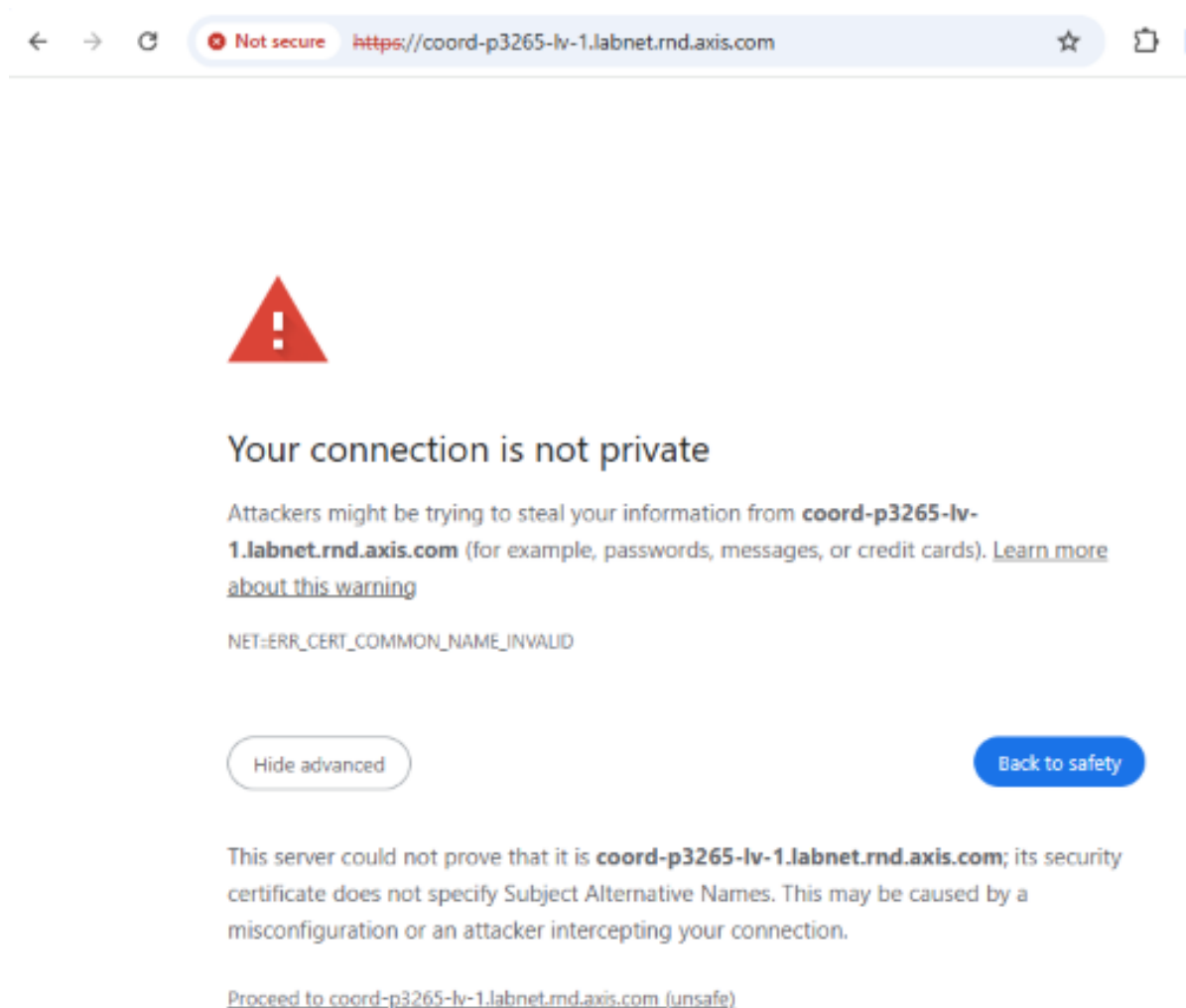
Certificate

Axis device ID ECC-P256 (802.1AR)

On upgrade or after a factory default: After a factory default.

Reason for change: To increase the overall device security following the secure-by-default strategy and reduce the hardening guide configuration steps for the user.

The impacts: By default, network connections to the device will only be allowed on HTTPS port 443. To use HTTP port 80, you must enable it first; otherwise, no network connection can be established. Even with a secure HTTPS connection, your browser might still show a warning due to issues validating the certificate. This is expected behavior, as IoT device certificates aren't compatible with most browsers. When accessing the Axis device's web interface via HTTPS, your web browser might display a warning message. This happens because the browser checks the certificate's information against the device's URL, which doesn't match due to the default certificate used in Axis devices. Device manufacturers can't resolve this issue, as it's inherent to how browsers verify certificates.



Affected VAPIX parameters:

The default values will change from:

System.BoaGroupPolicy.admin=both

System.BoaGroupPolicy.operator=both

System.BoaGroupPolicy.viewer=both

To:

System.BoaGroupPolicy.admin=https

System.BoaGroupPolicy.operator=https

System.BoaGroupPolicy.viewer=https

- **Signed Video enabled**

Signed Video was added as a feature in AXIS OS 11.10 to allow cryptographic verification of video authenticity and therefore strengthen the trust in video footage. Axis has decided to enable Signed Video in order to allow users to benefit from this layer of security out-of-the-box.

On upgrade or after a factory default: After a factory default.

Reason for change: Enabling signed video from factory allows users to take advantage of Signed Video out-of-the-box without requiring any pre-configuration and also removing the need of taking this into consideration during device hardening.

The impacts: No compatibility issues are to be expected with Video Management Systems such as AXIS Camera Station, Genetec, Milestone. The cryptographic signature introduced is part of the optional H.264 payload that, when not used, is ignored by clients. A slight increase in video bitrate can be observed in specific situations.

Affected VAPIX parameters:

The default values will change from:

Image.IO.MPEG.SignedVideo.Enabled=no

To:

Image.IO.MPEG.SignedVideo.Enabled=yes

- **Removal of loopback interfaces**

The following IPv4/IPv6 loopback interfaces are currently configured in AXIS OS:

127.0.0.1 [::1]
 127.0.0.2 [::2]
 127.0.0.3 [::3]
 127.0.0.4 [::4]
 127.0.0.5 [::5]
 127.0.0.11 [::11]
 127.0.0.12 [::12]

This list will be reduced to three IPv4 loopback interfaces only with h2c (HTTP2 unencrypted) support:

127.0.0.1
 127.0.0.4
 127.0.0.12

On upgrade or after a factory default On upgrade.

Reason for change: Reduce complexity and increase performance.

How can it affect me? Since only internal services use these loopback interfaces, no impact is expected for "VMS like" integrations. However, ACAP applications may rely on certain loopback interfaces being unavailable on OS 13. To ensure compatibility, these applications might need adaptation to handle this change gracefully, such as providing appropriate error messages to users.

- **RTSP tunnelled over HTTP(S) Authentication**

Currently, the RTSP server authenticates RTSP tunneled HTTP(S) streaming requests in factory defaulted state while all other streaming requests are managed by the HTTP(S) server as the major authentication interface. This change is about the HTTP(S) server handling authenticating when RTSP streams are requested that shall be tunneled over HTTP(S).

On upgrade or after a factory default: After factory default.

Reason for change: Instead of clients need to handle different authentication schemes for different RTSP/HTTP(S) server. This change unifies the behaviour and selects the HTTP(S) server being the major authentication interface in AXIS OS, especially for RTSP tunneled HTTP(S) network traffic. This change as well improves long-term stability and security authentication in AXIS OS.

The impacts: Client applications should not notice any significant impact when it comes to authentication.

Affected VAPIX parameters:

The default values will change from:

System.HTTPAuthRTSPOverHTTP=no

Network.RTSP.AuthenticateRTSPOverHTTP=yes

To:

System.HTTPAuthRTSPOverHTTP=yes

Network.RTSP.AuthenticateRTSPOverHTTP=no

API changes

- **Removal of PTZ.Support VAPIX API**

The parameters PTZ.Support.S#.JoyStickEmulation and PTZ.Support.S#.GenericHTTP will be removed.

These parameters were never officially documented nor supported. For more general information on PTZ product support and corresponding VAPIX APIs, see *VAPIX Library*.

On upgrade or after a factory default: On upgrade.

Reason for change: The PTZ.Support VAPIX API is not used anymore and considered obsolete.

The impacts: These parameters were officially never documented nor supported so no immediate impact would be expected.

Affected VAPIX parameters:

The following VAPIX parameters will be removed:

PTZ.Support.S#.JoyStickEmulation

PTZ.Support.S#.GenericHTTP

S# refers to S0, S1, S2 etc.. and refers to the number of image sensors/view areas supported by the product.

- **Removal of PTZ.Variou.V#.HomePresetSet VAPIX API**

The PTZ.Variou.V#.HomePresetSet VAPIX was used to indicate if a home preset was configured. The new parameter is PTZ.Preset.HomePosition, for more information, see *PTZ VAPIX API*.

On upgrade or after a factory default: On upgrade.

Reason for change: The PTZ.Various.V#.HomePresetSet VAPIX API is not used anymore and considered obsolete.

The impacts: This API and its parameters were never officially documented nor supported, so no immediate impact is expected.

Affected VAPIX parameters:

The following VAPIX parameters will be removed:

PTZ.Various.V#.HomePresetSet

whereas V# indicates the image/view area source.

- **Removal of PTZ-Autotracking 2.x legacy URLs**

This change will remove some legacy URLs that are currently available in the PTZ-Autotracking 2.x application. The officially supported URLs that should be used can be found in the *VAPIX Library*.

On upgrade or after a factory default: On upgrade.

Reason for change: Removing these legacy URLs that are not supported anymore will improve and streamline user experience and make the installation more robust.

The impacts: Client applications that have been implementing these API parameters and expect it to be available in AXIS OS 13 may stop working or provide the user with error messages that API parameter configuration was not successful.

Affected VAPIX parameters:

The following PTZ-Autotracking 2.x URLs:

http://<ip-address>/local/axis-ptz-autotracking/settings.fcgi

http://<ip-address>/local/axis-ptz-autotracking/operator.fcgi

http://<ip-address>/local/axis-ptz-autotracking/viewer.fcgi

will change to the below respectively for each user type:

http://<ip-address>/axis-cgi/ptz-autotracking/admin.cgi

http://<ip-address>/axis-cgi/ptz-autotracking/operator.cgi

http://<ip-address>/axis-cgi/ptz-autotracking/viewer.cgi

- **Remove unofficial SSH v1 API**

The *SSH Management API* is a device configuration API allowing for the creation and management of SSH users and access to the device. This API is officially released as version 2. The older, development version of the API, version 1, will be removed in AXIS OS 13 as it was never officially released.

On upgrade or after a factory default: On upgrade.

Reason for change: Only supporting the officially published version 2 of the SSH Management API and its documentation will streamline API behavior and user experience, preventing misunderstandings and confusing different API behaviors.

The impacts: Client applications that have been implementing these API parameters on this specific version and expect it to be available in AXIS OS 13 may stop working or provide the user with error messages that API parameter configuration was not successful.

- **Removal of legacy Streaming VAPIX API**

These VAPIX API parameters have been previously used to configure streaming related settings.

On upgrade or after a factory default: On upgrade.

Reason for change: These VAPIX API parameters are not used anymore and considered obsolete.

The impacts: Client applications that have been implementing these API parameters and expect it to be available in AXIS OS 13 may stop working or provide the user with error messages that API parameter configuration was not successful.

Affected VAPIX parameters:

The following VAPIX parameters will be removed:

Image.RFCCompliantMulticastEnabled

Image.ReferersEnabled

Image.Referers

Image.IX.MaxFrameSize

Image.IX.MPEG.ConfigHeaderInterval

Image.IX.MPEG.ICount

Image.IX.MPEG.Complexity

Audio.DSCP

Network.RTSP.AuthenticateOverHTTP

whereas IX indicates the image/view area source.

- **Removal of legacy SNMP VAPIX API**

The legacy parameter configuration for SNMP will be removed and replaced by a more feature-rich *SNMP VAPIX API*.

On upgrade or after a factory default: On upgrade.

Reason for change: Reducing complexity, improving user and API experience by providing a single SNMP VAPIX API for configuration that is also more feature rich than the legacy API. This change will also streamline device behavior since the S30 Recorder Series does not support the old legacy parameters to start with.

The impacts: Client applications that have been implementing these API parameters and expect it to be available in AXIS OS 13 may stop working or provide the user with error messages that API parameter configuration was not successful.

Affected VAPIX parameters:

The following VAPIX parameters will be removed:

SNMP.DSCP
 SNMP.Enabled
 SNMP.EngineBoots
 SNMP.InitialUserPasswd
 SNMP.InitialUserPasswdSet
 SNMP.TransportProtocol
 SNMP.V1
 SNMP.V1ReadCommunity
 SNMP.V1WriteCommunity
 SNMP.V2c
 SNMP.V3
 SNMP.Trap.Enabled
 SNMP.Trap.TO.Address
 SNMP.Trap.TO.Community
 SNMP.Trap.TO.AuthFail.Enabled
 SNMP.Trap.TO.ColdStart.Enabled
 SNMP.Trap.TO.LinkUp.Enabled
 SNMP.Trap.TO.WarmStart.Enabled

- **Removal of Layout VAPIX API**

The Layout VAPIX API contains parameters that have been used by the Axis device web interface only to provide certain functionality in the *classic AXIS OS web interface*.

On upgrade or after a factory default: On upgrade.

Reason for change: These VAPIX parameters are considered obsolete and haven't had an effect since 2017 and the introduction of newer versions of Axis device web interfaces.

The impacts: There is no immediate impact to the user as these parameters are non-functional and serve no purpose.

Affected VAPIX parameters:

The following VAPIX APIs will be removed:

Layout.ViewerIE
 Layout.ViewerOther
 Layout.PlainConfigEnabled
 Layout.H264InstallationEnabled
 Layout.AACInstallationEnabled
 Layout.EnableBasicSetup
 Layout.ShowVideoFormatDropDown
 Layout.DefaultStreamProfile
 Layout.ShowPaletteSelector
 Layout.ShowRelCrossEnabled
 Layout.DefaultJoystickMode

- **Removal of HTTP Network Authentication VAPIX API**

The Network.HTTP.AuthenticationPolicy controls whether HTTP(S) and RTSP server on the device are operated in Basic, Digest or partially both authentication modes. The Network.HTTP.

AuthenticationWithQop has been a non-functional parameter since 2016 (AXIS OS 2016 LTS, 6.50).

On upgrade or after a factory default: On upgrade.

Reason for change: These VAPIX parameters are considered obsolete, and the *Virtual Host VAPIX API* represents a more feature-rich configuration interface that will allow better, tailored use case

configurations based on user needs. Currently in AXIS OS 12, the NetworkHTTPAuthentication parameters alongside the Virtual Host VAPIX API allow for a contradicting and confusing device state. **The impacts:** Auto-Migration of the configuration of the Network.HTTP.AuthenticationPolicy into the virtual host VAPIX API will be in place so upgrades do not affect the current configuration. The *Virtual Host VAPIX API* should be used for configuration instead. However, client applications that have been implementing these API parameters and expect it to be available in AXIS OS 13 may stop working or provide the user with error messages that API parameter configuration was not successful.

Affected VAPIX parameters:

The following VAPIX APIs will be removed:

Network.HTTP.AuthenticationPolicy

Network.HTTP.AuthenticationWithQop

- **Changes to List recordings Edge Storage VAPIX API**

A number of response changes to the *List Recordings* argument within the Edge Storage API will be introduced.

- The response will no longer include starttime, stoptime, locked, numberofrecordings, recordingtype, eventtrigger.

- The API will use ISO 8601 basic format instead of ISO 8601 extended format.

- Removed the hidden option "useactualtimes" and make it the default instead.

On upgrade or after a factory default: On upgrade.

Reason for change: This change will improve product performance when requesting large chunks of recordings from the device. Also, some information that will be stripped from the API response was deprecated before and is considered obsolete.

The impacts: Client applications that have been implementing these API parameters and expect it to be available in AXIS OS 13 may stop working or provide the user with error messages that API operation was not successful.

- **Changes to View Area VAPIX API**

Today, view areas and digital PTZ sync their view areas/home preset position between each other. If the digital PTZ home position is updated, the view area service setting for the corresponding view area is updated accordingly, and vice versa.

On upgrade or after a factory default: On upgrade.

Reason for change: This change will remove the complex dependency between view areas and digital PTZ and improve user experience.

The impacts: Future behavior will mean that a set Home preset would not update the view area settings in the view area service and the other way around. When combining digital PTZ and view areas, the digital PTZ home position will take precedence over configured view areas.

- **Removal of Time.POSIXTimeZone and Time.DST.Enabled VAPIX parameters**

The *Time.POSIXTimeZone* and *Time.DST.Enabled* parameters are used to set time zone/daylight savings time and have been deprecated and are considered obsolete. The new Time API to configure these use cases can be found in the *VAPIX Library*.

On upgrade or after a factory default: On upgrade.

Reason for change: These VAPIX API parameters don't cover the all-time configuration in the device and have been considered obsolete and deprecated since AXIS OS 9.30. A more feature-rich VAPIX API for time configuration is available.

The impacts: Client applications that have been implementing these API parameters and expect it to be available in AXIS OS 13 may stop working or provide the user with error messages that API parameter configuration was not successful.

Affected VAPIX parameters:

The following VAPIX APIs will be removed:

Time.POSIXTimeZone

Time.DST.Enabled

ACAP applications

- **Signed ACAP applications**

Starting from AXIS OS 13.0, the option to allow unsigned applications has been removed and only signed ACAP applications are allowed.

Apps

 **Add app** [Find more apps](#)

Allow unsigned apps ☐ 



AXIS Video Motion Detection
☐

Version: 4.5-8
 Axis Communications

[Open](#)




AXIS Object Analytics
☐

Version: 1.13.11
 Axis Communications

[Open](#)


If an unsigned ACAP application is installed on the device, it must be removed or replaced with a signed version before upgrading to AXIS OS 13. This replacement must be done while the device is still running AXIS OS 12. Support for retaining the application signature will be introduced later in AXIS OS 12.

On upgrade or after a factory default: On upgrade.

Reason for change: To increase trust in ACAP applications and comply with international regulations and best practices for secure software delivery.

The impact: All ACAP applications to be installed in AXIS OS 13 must be signed, otherwise the ACAP installation will fail.

Affected VAPIX parameters:

The following VAPIX API parameters will be removed :

`/axis-cgi/applications/config.cgi?action=set&name=AllowUnsigned&value=true`

`/axis-cgi/applications/config.cgi?action=set&name=AllowUnsigned&value=false`

- **Removal of ACAP package.conf**

Package.conf and Manifest.json are part of an ACAP application and its configuration and needed for ACAP application installation on Axis devices. From AXIS OS 13.0, all ACAP applications must contain a manifest.json file that describes their configuration. The old way of using a package.conf file will not be supported. If an ACAP application without a manifest.json file has been installed on the device, it needs to be removed or replaced before upgrading to AXIS OS 13.

On upgrade or after a factory default: On upgrade.

Reason for change: : The package.conf format lacks the structure and ease of validation that manifest.json and the associated JSON schema provides. ACAP applications using package.conf are handled by an older version of the ACAP framework in AXIS OS. Removing this version improves the overall cybersecurity posture of the AXIS OS architecture and reduces its attack surface. More information about the manifest.json can be found in *Develop ACAP applications*.

The impact: An ACAP application that does not contain a manifest.json file needs to be given one, e.g. by following these *instructions*.

- **ACAP manifest compatibility declaration**

In AXIS OS 12.x, we're introducing an optional field in the application manifest that specifies the AXIS OS major versions the application supports. To adapt to this change, ACAP developers must include compatibility information in the ACAP manifest. This field will become mandatory in AXIS OS 13 and only ACAP with this explicit compatibility information will be supported on OS 13.

Note that package.conf doesn't support this feature. As a result, an ACAP application with only a package.conf file (and no manifest) won't meet the AXIS OS 13 requirements.

On upgrade or after a factory default: On upgrade.

Reason for change: To improve usability and the ACAP application experience for both ACAP developers and users operating Axis devices. It also prevents installation of incompatible ACAP applications and situations where ACAP applications would stop working. It improves the user experience by detecting error states while attempting the upgrade, improving the safety of the device and ACAP application.

The impact: An ACAP application can only be installed or upgraded if it declares compatibility with the current AXIS OS version. Likewise, an upgrade will only proceed if all installed applications are

compatible with the target AXIS OS version. AXIS OS also checks application compatibility at boot. If any application lacks a valid compatibility declaration, the upgrade will be refused or rolled back. This safeguard ensures system stability, especially when upgrading from older AXIS OS versions that don't support compatibility checks.

- **Rollback upon ACAP installation during AXIS OS upgrade**

When performing an AXIS OS upgrade, all ACAP applications in the background are re-installed as part of the process. If a re-installation of an ACAP results in an error, be it from lack of compatibility declaration, a failing post-install script, or something else that would cause a regular installation to fail, AXIS OS will initiate a rollback to the previous version.

On upgrade or after a factory default: On upgrade.

Reason for change: This improvement will improve the user experience and prevent ACAP applications from becoming non-functional after AXIS OS upgrades.

The impact: An ACAP application that cannot be installed successfully during an AXIS OS upgrade will cause the device to revert to the original AXIS OS version. As a user, you would see that the upgrade failed, meaning that server report and logs would have to be analyzed to understand the root cause.

- **Changed rules for ACAP application install/uninstall scripts**

- The scripts files must have executable permissions.
- The scripts must complete within X minutes.
- If they are shell scripts, they must start with `#!/bin/sh`.
- If the post-install script exits with anything else than zero, installation will fail.
- The umask will be 022 when the script starts.

On upgrade or after a factory default: On upgrade.

Reason for change: To prevent ACAP applications with faulty scripts from being installed.

The impact: An ACAP application that uses a post-install or pre-uninstall script needs to be modified so that these scripts comply with the stricter rules. Installation or upgrade will be aborted if the post-install script of an ACAP application fails.

- **Restrictions on ACAP application device access**

Additional restrictions will limit application access on the device. Applications will be allowed to run only as the dynamic user created specifically for them or as the "sdk" user. They will be granted access only to the groups and D-Bus APIs required to use the officially supported APIs.

On upgrade or after a factory default: On upgrade.

Reason for change: To prevent ACAP applications from bypassing the AXIS OS security model.

The impact: An ACAP application will be blocked from installation if it specifies a user other than "sdk" in its manifest, or if it requests groups or D-Bus APIs not required by officially supported APIs. To be accepted, the application must be updated to use only supported APIs. Its manifest must also comply with schema version 2.0 or later, where these restrictions are enforced.

- **Removal of .larod model format**

Support for the .larod model format will be removed. The .larod API is part of the Native SDK and used by ACAP applications that want to use their own deep learning models for analytics.

On upgrade or after a factory default: On upgrade.

Reason for change: The successor to the obsolete .larod format (now considered obsolete) is the .tflite format, which offers more features and capabilities.

The impact: ACAP applications and other services that use the .larod format won't work anymore. Those applications will have to switch to using the standard .tflite model format instead. Migrating to the tflite format should be very easy since the .tflite file is already provided as an input when generating .larod files. Using .tflite files directly has been supported since AXIS OS 10.7, and the .larod format has been marked as deprecated in the larod documentation since AXIS OS 10.9.

- **Removal of uint16_t for VDO_TIMESTAMP in VDO ACAP API**

Currently both uint16_t and uint32_t are supported for choosing timestamp type when creating a stream. Using the uint32_t variant is more consistent and future proof. The ACAP documentation with support for uint32_t will be included in the AXIS OS 12.4 release. Once the SDK 12.4 release is ready for the ACAP, it will be [here](#).

On upgrade or after a factory default: On upgrade.

Reason for change: Easier maintenance and more future-proof solution for ACAP developers.

The impact: ACAP applications should be adapting to uint32_t VDO_timestamps and might break if they expect uint16_t timestamps that are not available anymore in AXIS OS 13. UTC will remain the default custom timestamp type. The only impact will be on debug use-cases such as CLIENT_SERVER_DIFF.

- Stopping ACAPs that uses DLPU without disabling VOD**
 DLPU in Axis products are not able to serve different applications unless the model is specifically optimized for that application. If another ACAP besides AOA tries to use the DLPU and does not disable VOD, it will be stopped in AXIS OS 13.
On upgrade or after a factory default: On upgrade.
Reason for change: This increases device stability and performance and ensures the quality of Axis' internal analytics services.
The impact: Your incompatible ACAP application may stop working after the upgrade, or it may block the upgrade.

Miscellaneous

- AXIS OS image file compression** The AXIS OS file image will be compressed with zstd instead of gzip.
On upgrade or after a factory default: On upgrade but will not affect the device itself.
Reason for change: ZSTD-compression of the AXIS OS file images are smaller in size, which require less storage and less data being sent over networks to distribute the AXIS OS images and perform upgrades.
The impacts: The metadata that was previously available in gzip-compressed images such as software version, HWID, and product model are still available, but the parsing of that information needs to be adapted towards zstd. The format of the information itself is not changing either, but it is required that external clients that parse the metadata of the image file change the parsing to zstd-standard. Clients that don't adapt will not be able to parse the metadata of the AXIS OS image file. Clients can automatically identify the compression format since gzip-compressed files always start with 0x1F, 0x8B, 0x03. Zstd-compressed files, on the other hand, start with 0x2B, 0xB5, 0x2F, 0xFD.
- PTZ continuous pan control** The current default behavior for continuous pan is to keep moving until a pan limit is reached. For products with unlimited pan, this means that a continuous pan movement will keep going if no stop command is received or the product is restarted. In AXIS OS 13, the PTZ camera will no longer pan indefinitely. Instead, it will automatically stop after 10 minutes if the operator hasn't issued any pan movements. It will be possible to disable this timeout or change the value of the timeout
On upgrade or after a factory default: On upgrade.
Reason for change: The current behavior potentially wears out the mechanics of the product, so this change was introduced to improve the product lifetime.
The impacts: The PTZ camera will no longer pan indefinitely. Instead, it will automatically stop after 10 minutes if the operator hasn't issued any pan movements.

Changes in AXIS OS 14

Changes that apply to the first version of AXIS OS 14, coming in September 2028. Please note that the changes can be adjusted in future.

API changes:

- Removal of unofficial certificate management**
 The unofficial and externally undocumented custom certificate management API with the VAPIX endpoints `/axis-cgi/certappmgmt.cgi` and `/axis-cgi/certmgmt.cgi` will be removed. For supported AXIS OS certificate management and enrollment APIs, please refer to the *VAPIX Library*.
Reason for change: Unofficial and undocumented APIs shall not be used due to the security risk. Thus, it is removed since there are other VAPIX APIs that can be used instead.
The impact: If you have third party software using this API, it will not work correctly with AXIS OS 14 or higher.
- Removal of time.cgi VAPIX API**
 The `time.cgi` is deprecated and considered obsolete. A more feature-rich Time API to configure time-related settings can be found in the *VAPIX Library*.
On upgrade or after a factory default: On upgrade.
Reason for change: Only supporting the officially supported Time VAPIX API and its documentation will streamline API behavior and the user experience, preventing misunderstandings and confusing different API behaviors. The new API is part of the export-import functionality of AXIS OS and can be used for multi-device configuration.

How can it affect me? Client applications that have been implementing these API parameters and expect it to be available in AXIS OS 13 may stop working or provide the user with error messages that API parameter configuration was not successful.

Affected VAPIX parameters:

The `time.cgi` and its parameters.

ACAP applications

- **Removal of axhttp library for ACAP applications**

The axhttp library for ACAP applications will be removed. The manifest schema will remove the option `transferCgi` to configure `transfer-cgi` for ACAP applications.

On upgrade or after a factory default: On upgrade.

Reason for change: The axhttp is considered obsolete and is replaced with better modern alternatives. ACAP developers will use the FastCGI or reverse proxy option, which will be the successor and receive official long-term support.

The impact: An ACAP application build with SDK 3.x (that utilizes the `transferCGI`, used by axhttp) will not work after upgrading to AXIS OS 14. ACAP applications need to be rewritten and rebuilt to use FastCGI or reverse proxy (option `reverseProxy` in manifest) instead.

Applied

Changes in AXIS OS 12.1

Edge Storage:

- **Removal of vFAT**

The ability to format SD cards to the vFAT system file will be removed. However, they can still be used as before. A long time ago, SD cards were delivered with vFAT as the standard file system for cards up to 32GB. Since such SD cards are no longer used, the usefulness of vFAT is very limited.

Why is this change introduced? Axis has since start recommended Ext 4. vFat should never be used.

How can it affect me? If necessary, you will need to format the SD card outside the device.

Onboard storage

SD card 1 (55.2 GB)

Free: 100%

Status: Mounted

File system: ext4

Encrypted: No

Wear: 4%

Retention time

As long as possible

Number of days 7 [1..7000]

Tools

Check

Repair

Format

Encrypt

Format storage device

Erase all recordings and format the storage device.

File system

ext4 (recommended)

vfat

Cancel

Format

Safely remove the storage device:

Unmount

Autoformat

Write protect

Network & Discovery:

- **Disabled UPnP discovery protocol**

Axis devices currently have UPnP and Bonjour enabled in factory defaulted state for general device discovery. The Bonjour protocol allows for device detection within the local subnet where the device is

located (example: 192.168.1.0/24). The UPnP protocol allows device discovery across networks (example: 192.168.1.0/24 and 192.168.2.0/24) but only if multicast-routing is properly configured. Axis believes that the device detection within the local subnet is the main use case for a discovery protocol and therefore will disable UPnP in factory defaulted devices moving forward. This will also lower the attack surface of the device and increase the overall network security. The UPnP protocol remains available in Axis devices with the option for the user to enable it if needed.

VAPIX API parameter: root.Network.UPnP.Enabled

Network discovery protocols

Bonjour® ☒ ⓘ Bonjour name AXIS P3265-LV	UPnP® ☐ ⓘ UPnP name AXIS P3265-LV - B8A44F281DB4
WS-Discovery ☐ ⓘ	

Save

Why is this change introduced? To lower the attack surface of the device and increase the overall device security.

How can it affect me? If you have third party software only using UPnP for device discovery, it will not work correctly with AXIS OS 12.1 or higher and users need to enable UPnP first on the Axis device.

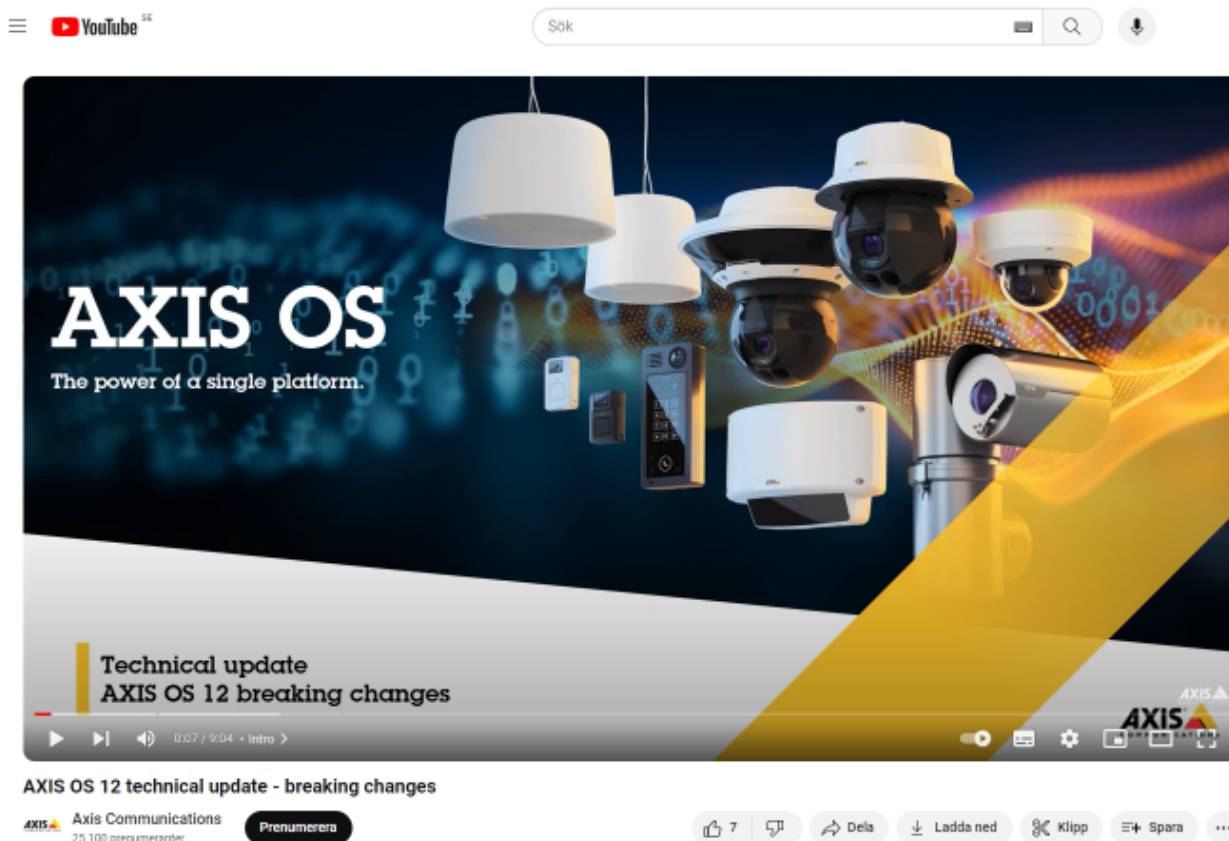
Security:

- Basic authentication for HTTPS connections**
 Axis devices perform digest authentication when serving both HTTP and HTTPS connections. Since HTTPS connections are preferred for increased security, Axis will change the default behavior so that basic authentication is used for HTTPS connections only by introducing a new authentication policy mode called "Recommended". The authentication policy for HTTP & the RTSP server will not change in this mode. More information about the authentication policy can be found in the *VAPIX Library*. Using basic authentication in HTTPS connections is IT-industry standard and allows Axis devices to operate in a well-defined and common practice as well. Digest authentication will still be kept for serving for unencrypted HTTP connections. Using HTTPS only is the recommended operational mode for Axis devices.

Why is this change introduced? To follow the IT-industry standard.

How can it affect me? If you use digest authentication for HTTPS connection, it will not work correctly with AXIS OS 12.1 or higher.

Changes in AXIS OS 12.0



Check out the *AXIS OS 12 Technical Update - Breaking Changes* video, to learn more about the upcoming changes.

- Removal of the old web interface**
 The old web interface, also called "*AXIS OS web version B*", will be removed.
Why is this change introduced? The old web interface is no longer needed since the *new interface* has all implemented features. It is removed to save memory space on the device and to simplify both usage and maintenance. Additionally, the old web interface used a number of outdated libraries and removing it will make the device more secure.
How can it affect me? The new web interface will be displayed after upgrade.

Security:

- Disabled HTTP Port 80 redirects**
 In previous security penetration tests, Axis was advised to disable HTTP Port 80 redirects in order to enhance security and to prevent information leakage. Currently, Axis devices are configured for HTTPS-only, but the HTTP port 80 redirects are enabled to inform users/clients that communication is not permitted on port 80 and redirecting them automatically to port 443 instead. Axis will follow the general recommendation provided by third-party penetration test laboratories and will deactivate HTTP port 80 redirects when the device is set to HTTPS-only mode.

No.	Time	UTC Time	Package Delta	Source MAC	Source	Source Port	Destination MAC	Destination	Destination Port	Protocol	Length	Info
1	0.000000	07:43:22.487823	0.000000	Micro-St_e2:48:b5	172.25.201.50	60346	AxisComm_d9:10:b9	172.25.201.191	80	TCP	66	60346 → 80 [SYN] Seq=0 Win=64240 Len=0
2	0.000079	07:43:22.487902	0.000079	Micro-St_e2:48:b5	172.25.201.50	60347	AxisComm_d9:10:b9	172.25.201.191	80	TCP	66	60347 → 80 [SYN] Seq=0 Win=64240 Len=0
3	0.000556	07:43:22.488379	0.000477	AxisComm_d9:10:b9	172.25.201.191	80	Micro-St_e2:48:b5	172.25.201.50	60346	TCP	66	80 → 60346 [SYN, ACK] Seq=0 Ack=1 Win=0
4	0.000613	07:43:22.488436	0.000057	Micro-St_e2:48:b5	172.25.201.50	60346	AxisComm_d9:10:b9	172.25.201.191	80	TCP	54	60346 → 80 [ACK] Seq=1 Ack=1 Win=21022
5	0.000627	07:43:22.488450	0.000014	AxisComm_d9:10:b9	172.25.201.191	80	Micro-St_e2:48:b5	172.25.201.50	60347	TCP	66	80 → 60347 [SYN, ACK] Seq=0 Ack=1 Win=0
6	0.000653	07:43:22.488476	0.000026	Micro-St_e2:48:b5	172.25.201.50	60347	AxisComm_d9:10:b9	172.25.201.191	80	TCP	54	60347 → 80 [ACK] Seq=1 Ack=1 Win=21022
7	0.027298	07:43:22.515121	0.026645	Micro-St_e2:48:b5	172.25.201.50	60346	AxisComm_d9:10:b9	172.25.201.191	80	HTTP	602	GET / HTTP/1.1
8	0.027733	07:43:22.515556	0.000435	AxisComm_d9:10:b9	172.25.201.191	80	Micro-St_e2:48:b5	172.25.201.50	60346	TCP	60	80 → 60346 [ACK] Seq=1 Ack=549 Win=303
9	0.028136	07:43:22.515959	0.000403	AxisComm_d9:10:b9	172.25.201.191	80	Micro-St_e2:48:b5	172.25.201.50	60346	HTTP	617	HTTP/1.1 302 Found (text/html)
10	0.031251	07:43:22.519074	0.003115	Micro-St_e2:48:b5	172.25.201.50	60353	AxisComm_d9:10:b9	172.25.201.191	443	TCP	66	60353 → 443 [SYN] Seq=0 Win=64240 Len=0
11	0.031658	07:43:22.519491	0.000417	AxisComm_d9:10:b9	172.25.201.191	443	Micro-St_e2:48:b5	172.25.201.50	60353	TCP	66	443 → 60353 [SYN, ACK] Seq=0 Ack=1 Win=0
12	0.031732	07:43:22.519555	0.000064	Micro-St_e2:48:b5	172.25.201.50	60353	AxisComm_d9:10:b9	172.25.201.191	443	TCP	54	60353 → 443 [ACK] Seq=1 Ack=1 Win=21022
13	0.031887	07:43:22.519710	0.000155	Micro-St_e2:48:b5	172.25.201.50	60353	AxisComm_d9:10:b9	172.25.201.191	443	TLSv1.3	571	Client Hello
14	0.032157	07:43:22.519980	0.000270	AxisComm_d9:10:b9	172.25.201.191	443	Micro-St_e2:48:b5	172.25.201.50	60353	TCP	60	443 → 60353 [ACK] Seq=1 Ack=518 Win=30
15	0.051470	07:43:22.539293	0.019313	AxisComm_d9:10:b9	172.25.201.191	443	Micro-St_e2:48:b5	172.25.201.50	60353	TLSv1.3	1382	Server Hello, Change Cipher Spec, Appl
16	0.057340	07:43:22.545163	0.005870	Micro-St_e2:48:b5	172.25.201.50	60353	AxisComm_d9:10:b9	172.25.201.191	443	TLSv1.3	84	Change Cipher Spec, Application Data

To test the possible impact, configure your Axis device for HTTPS only and configure a firewall rule in AXIS OS 11.9 as shown below, where the Axis device would effectively block communication on port 80 for a specific client trying to connect.

AXIS P3265-LV Dome Camera

HTTP and HTTPS

Allow access through: **HTTPS**

HTTPS port: **443**

Certificate: **Axis device ID ECC-P256 (802.1AR)**

Save

AXIS P3265-LV Dome Camera

Firewall

Activate: **On**

Default Policy: **Allow**

Address	Rule type	Protocol	Port	Policy
172.25.201.150	Filter	TCP	80	Deny

Add rules

Why is this change introduced? To lower the attack surface of the device and increase the overall device security.

How can it affect me? If you access the Axis device via HTTP, it will not work correctly with AXIS OS 12.0 or higher. Please use HTTPS instead.

- Removed support for TLS 1.0/1.1 HTTPS connections**
 Axis devices support modern encryption technology through TLS 1.2/1.3, which is used by default for HTTPS connections. However, there is also an option to enable older, outdated and insecure TLS 1.0/1.1 versions for backward compatibility with legacy systems that cannot support more secure HTTPS connections. Axis will completely remove TLS 1.0/1.1 versions for HTTPS connections to increase overall security and prevent users from accidentally enabling these protocol versions.
 VAPIX API Parameter: root.HTTPS.AllowTLS1 and root.HTTPS.AllowTLS11

Plain config

⚠ Plain config is for expert users only. Only change the settings if you know what you're doing.

Select group: None Search for parameters by ID: TLS

ⓘ To see the effect of your changes, you might have to refresh the webpage or restart the device.

HTTPS

☐ Allow TLSv1.0 (deprecated, implies Allow TLSv1.1)

☐ Allow TLSv1.1 (deprecated)

Network / Interface / 10 / dot1x / EAPTLS

Identity: axis-acc8ec656f3

Private key password: *****

Why is this change introduced? It is obsolete, and keeping it might be a security threat.

How can it affect me? If you have third party software using TLS 1.0/1.1 HTTPS connections, it will not work correctly with AXIS OS 12.0 or higher.

- **Removed support for OpenSSL 1.1.1**

Since AXIS OS 11.6 (August 2023), Axis devices support simultaneously version 1.1.1 and 3.0 of the cryptographic software backend OpenSSL. To allow for smooth transition, OpenSSL 1.1.1 will still be supported until LTS 2024 track is launched and in that track. With AXIS OS 12, OpenSSL 1.1.1 support will be removed. Patches and security updates of OpenSSL 1.1.1 will still be supported on active AXIS OS long-term support tracks as Axis has signed a support contract with the OpenSSL foundation to receive prolonged support.

Note that upcoming changes may affect ACAP applications. To ensure compatibility and security, it is recommended to use *OpenSSL 3.X*, which is available in ACAP Native SDK 1.14 / AXIS OS 11.10.

Alternatively, ACAP applications can *embed a custom cryptographic library* to meet their specific needs.

Why is this change introduced? It is obsolete as the active track runs a newer version.

How can it affect me? If you have third party software using OpenSSL 1.1.1, it will not work correctly with AXIS OS 12.0 or higher.

Network & Discovery:

- **IPv4 address changes**

To date, Axis devices have never been IPv4 compliant following the corresponding RFC framework. That resulted in the Axis device having a default IP-address which is 192.168.0.90/24. This circumstance leads to network related issues that we want to resolve. For instance, if no DHCP server is available on the network, the default IP address of Axis devices currently is 192.168.0.90/24 regardless of whether anyone on the same network segment already uses the same IP address. This may cause service interruptions for other devices if such IP address conflict occurs. At the same time, the link-local address (169.254.x.x/16) is enabled by default regardless of whether it's used, which is not in compliance with the RFC standard.

With the above changes in place, there will be no default IP addresses of AXIS OS devices anymore. The Axis OS devices will use the IP addresses either from a DHCP server or statically configured address. The devices will only fall back to link-local addresses if there is an IP address conflict detected, or a DHCP server is unavailable in the network. More information regarding the IPv4 addressing change can be found [here](#).

Why is this change introduced?

- To be completely RFC IPv4 compliant.
- Disable link-local address when it is not used.
- Better user experience for our customers when multiple factory-defaulted Axis devices are placed on the same network simultaneously.
- Increase robustness and detect IP address conflicts.

- **How can it affect me?** Affects during installation, AXIS devices will request IP address from the network it attaches to etc DHCP.
- **Disabled WS-Discovery protocol**
Axis devices currently have the WS-Discovery (WebService-Discovery) protocol enabled in factory defaulted state as additional option for ONVIF-related device discovery. However, the ONVIF interface is not enabled in factory defaulted state which makes the availability of the WS-Discovery protocol by default obsolete. Axis will adapt the default behavior and will disable the WS-discovery protocol in factory defaulted state. This means a user need to enable the WS-discovery protocol if desired.
VAPIX API parameter: WebService.DiscoveryMode.Discoverable

Network discovery protocols

Bonjour® ☒ ⓘ Bonjour name AXIS P3265-LV	UPnP® ☐ ⓘ UPnP name AXIS P3265-LV - B8A44F281DB4
WS-Discovery ☐ ⓘ	

Save

Why is this change introduced? To lower the network footprint and increase the cybersecurity level of an Axis device when ONVIF is not being used.

How can it affect me? You will not be able to discover the device until WS-Discovery has been enabled.

- **Possibility to disable Basic Device Info VAPIX API**The *Basic Device Information* VAPIX API allows to retrieve general information about the Axis product with no authentication. This is useful for device discovery and profiling during network and application onboarding. Axis will implement an additional VAPIX parameter that will allow the user to disable the basic device information API if needed. The ability for the user to disable this VAPIX API may be considered a behavioral change if unknown.
Why is this change introduced? Provide the ability to reduce the attack surface and information leakage of the device, increasing the overall security resilience of the network.
How can it affect me? If you have third party software using this API after onboarding, it will not work correctly with AXIS OS 12.0 or higher.
- **Removal of releaseinfo.cgi**The axis-release/releaseinfo.cgi VAPIX API has been removed. It is recommended to use the Basic Device Information VAPIX API instead, see more info in the *VAPIX Library*.
Example output of axis-release/releaseinfo.cgi:
part=6975649029
version:11.2.53
Why is this change introduced? It is obsolete and replaced by a different API.
How can it affect me? If you have third party software using this API, it will not work correctly with AXIS OS 12.0 or higher.
- **Removal of getBrand.cgi**The previously deprecated VAPIX API axis-cgi/prod_brand_info/getbrand.cgi has been removed. It is recommended to use the Basic Device Information VAPIX API instead, see more info in the *VAPIX Library*. Please find below an example output of the information that was possible to receive through getBrand.cgi, all the information is still available and covered in the referenced Basic Device Information VAPIX API.
Example output of getBrand.cgi:
Brand.Brand=AXIS
Brand.ProdFullName=AXIS P3265-LV Dome Camera
Brand.ProdNbr=P3265-LV
Brand.ProdShortName=AXIS P3265-LV
Brand.ProdType=Dome Camera
Brand.ProdVariant=

Brand.WebURL=http://www.axis.com

Why is this change introduced? It is obsolete and replaced by a different API.

How can it affect me? If you have third party software using this API, it will not work correctly with AXIS OS 12.0 or higher.

- **Removal of network filter API**

The current IP-filtering VAPIX API will be replaced by a more feature-rich firewall application that can be configured through JSON REST API. The new firewall service will be available in AXIS OS 11.8 (January 2024) and can be used from there on.

IP address filter

☐ Use filter

Policy

☒ Allow

☐ Deny

Addresses ⓘ

Save

The legacy network filter API with the following below parameters will be removed in AXIS OS 12:

Network.Filter.Enabled

Network.Filter.Input.AcceptAddresses

Network.Filter.Input.Policy

Network.Filter.Log.Enabled

Why is this change introduced? It is obsolete and replaced by the new host-based firewall.

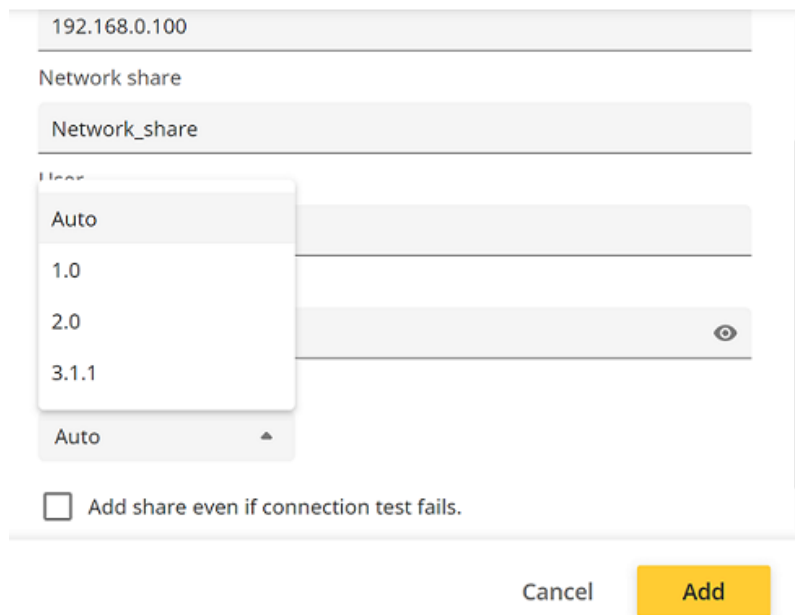
How can it affect me? If you have third party software using this API, it will not work correctly with AXIS OS 12.0 or higher.

Edge Storage:

- **Removed support for SMB 1.0 and 2.0**

The Server Message Block Protocol (SMB) is widely used for mounting network shares when storing recordings. While secure versions of the SMB protocol are supported and available in Axis devices (2.1, 3.0, 3.02 and 3.1.1), the insecure versions (1.0 and 2.0) are still available to use but disabled in factory defaulted state. Axis will remove version 1.0 and 2.0 completely to increase the overall security and to prevent users from enabling these protocol versions by mistake.

Add network storage



192.168.0.100

Network share

Network_share

Version

Auto

1.0

2.0

3.1.1

Auto

☐ Add share even if connection test fails.

Cancel Add

Why is this change introduced? It is obsolete, and keeping it might be a security threat.
How can it affect me? If you have a storage connection requiring these versions, they will not work anymore.

ACAP application related changes:

NOTICE

Before upgrading to AXIS OS 12.0 or higher, note that certain applications require updates. See the respective documentation for more information.

- **AXIS Perimeter Defender 3.6.0 required.** Versions 3.5.1 and earlier are not compatible with AXIS OS 12.0 or higher. Follow these *instructions* to perform the upgrade correctly.
- **AXIS License Plate Verifier 2.12.8 required.** Versions 2.8.4 or earlier are not compatible with AXIS 12 or higher. Follow these *instructions* to perform the upgrade correctly.
- **AXIS People Counter 5.0.5 required.** Versions 4.6.108 and earlier are not compatible with AXIS OS 12 or higher. Follow these *instructions* to perform the upgrade correctly.

- **Removal of root-privileges**

Root-privileged access to Axis products and ACAP applications has been removed indefinitely without the possibility to enable it. The previously available parameter in AXIS OS 11 to enable root privileges has been removed. This change applies to the factory default settings as well as when upgrading to AXIS OS 12 from any previous version of AXIS OS.

This change increases ACAP applications confidentiality by better protecting their data and secrets, preventing information leakage and increasing AXIS OS system integrity. Please read the *full guide* for more information.

Why is this change introduced? To increase the security on the device.

How can it affect me? ACAP applications that do not use root-privileges are not affected.

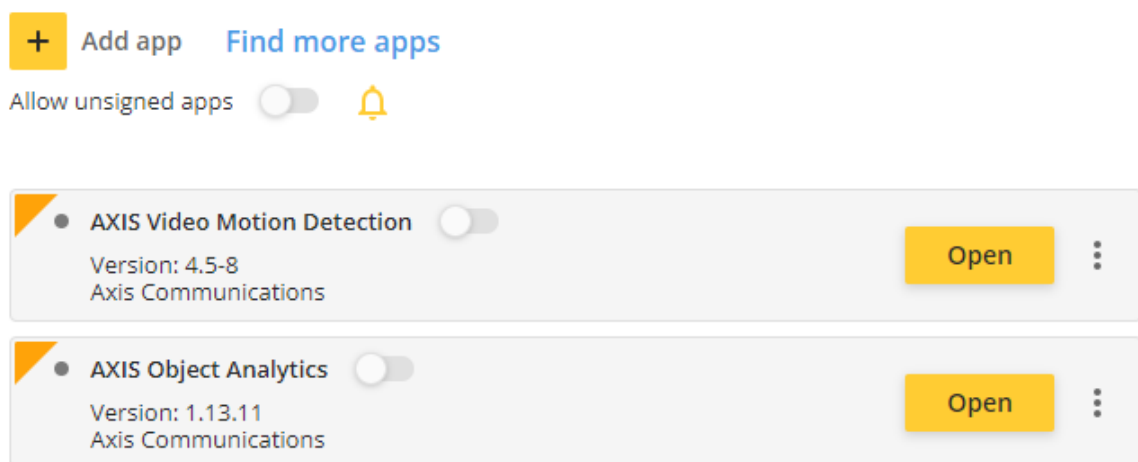
ACAP applications with root privileges, will not work with AXIS OS 12.0 or higher. Check the installed ACAP applications carefully! Make sure they are working properly. If possible, select the LTS 2024 track.

Possible scenarios where failures could be expected are:

- The ACAP application cannot run because it tries to use the previously available root user with root privileges.

- The post-install script may be using root-privileges, which prevents the ACAP application from being installed or run.
 - The pre-uninstall script may be using root-privileges, which may prevent ACAP application data from being cleaned up at installation.
 - The ACAP application tries to access file system resources or functionality that is locked behind root-privileges.
 - The ACAP application that include or need access to security-sensitive functionality will not work anymore. For example, VPN-capable solutions based on Tailscale, ZeroTier, IPsec, OpenVPN and WireGuard that may have been deployed as an ACAP application previously, will not work in AXIS OS 12. Axis is looking into how and if a VPN-client can be embedded into the AXIS OS operating system natively.
- **Signed ACAP applications** From AXIS OS 12.0, the option to allow unsigned apps will be disabled in factory defaulted state. To upload unsigned ACAP applications, users must enable this option. This only applies to factory-defaulted products running AXIS OS 12 or higher.

Apps



VAPIX API parameters:

`/axis-cgi/applications/config.cgi?action=set&name=AllowUnsigned&value=true`

`/axis-cgi/applications/config.cgi?action=set&name=AllowUnsigned&value=false`

Running unsigned ACAP applications from any previous version of AXIS OS when upgrading to AXIS OS 12 will have no impact and the ACAP application will continue to function normally. For more information and a timeline, see *Additional security in AXIS OS and ACAP applications*.

Why is this change introduced? To lower the attack surface of the device and increase the overall device security.

How can it affect me? For factory default devices, you will need to enable Allow unsigned apps.

- **ACAP installation behaviour**
The ACAP installation is now aborted if the post-install script exit on EX_NOPERM (77). Previously, the ACAP applications is installed nevertheless and warnings were printed in the log files. Uninstall will happen regardless of pre-uninstall script error and will write the error code to the log.
Why is this change introduced? To increase the ACAP applications reliability on the market.
How can it affect me? ACAP application vendors are informed and should compile a new ACAP application version without errors if affected.
- **Removal of Basic analytics ACAP applications**
Due to updates to our framework, it is not possible to support some older types of ACAP applications and they will therefore be removed.
This applies to Axis Basic Enter-Exit, Axis Basic Object Counter and Axis Basic Object Removed

Why is this change introduced? Due to architectural changes.

How can it affect me? If you are using any of these ACAP applications, do not upgrade until the system has a verified replacer.

- **Removal of libcapture library**

The libcapture library for ACAP applications is obsolete and will be removed. It is recommended to use the Video capture API instead. For more information, visit the [ACAP SDK Documentation](#).

Why is this change introduced? It is obsolete, and keeping it might be a security threat.

How can it affect me? If you have an ACAP application using this library, it will not work correctly with AXIS OS 12.0 or higher.

- **Removal of vaconfig.cgi**

The ACAP applications managed by the vaconfig.cgi API is no longer supported, this configuration and management API is therefore obsolete and will be removed.

Why is this change introduced? It is obsolete, and keeping it might be a security threat.

How can it affect me? If you have an ACAP application using this library, it will not work correctly with AXIS OS 12.0 or higher.

- **Removal of ACAP Computer Vision SDK support**

The ability to enable ACAP Computer Vision SDK support will be removed for the listed products because they only have 1 GB of memory.

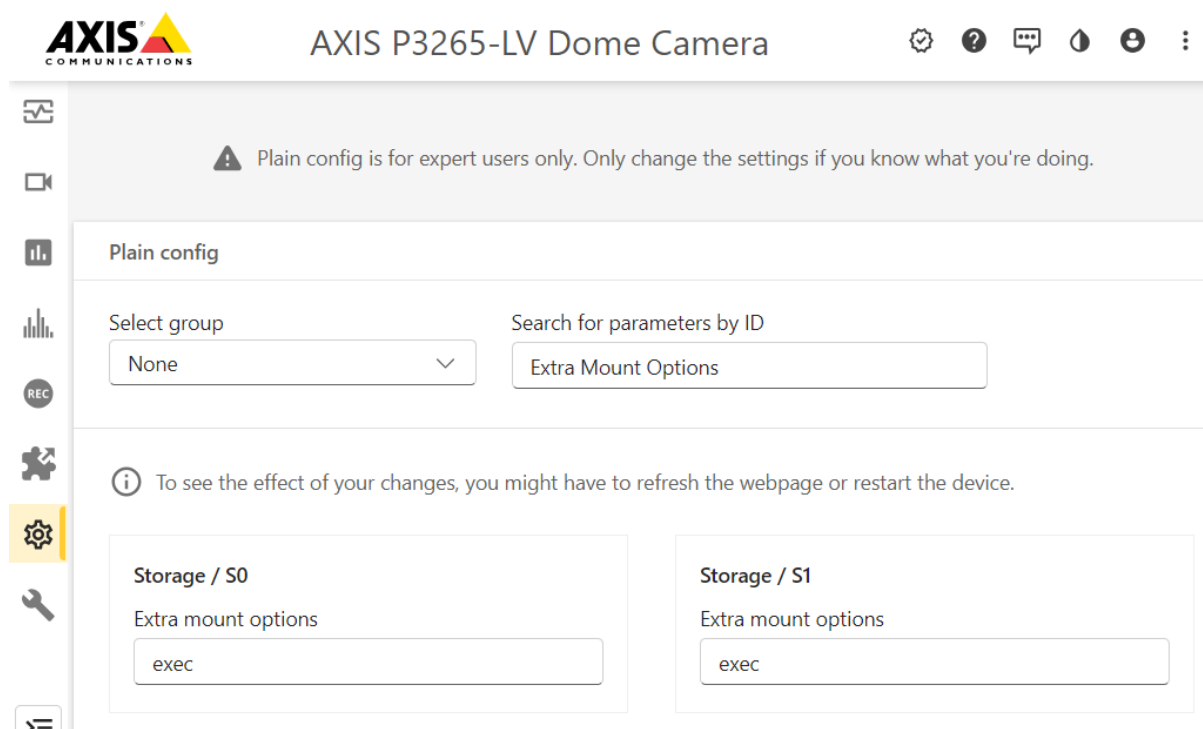
Applies to: AXIS D2210-VE, AXIS M3215-LVE, AXIS M3216-LVE, AXIS M5526-E, AXIS P1465-LE, AXIS P1465-LE-3, AXIS P3265-LV/-LVE/-V and AXIS P3265-LVE-3

Why is this change introduced? Running the Computer Vision SDK on the product will consume too much memory and may render the product inoperable.

How can it affect me? If you have an ACAP application using the Computer Vision SDK, it will not work correctly with AXIS OS 12.0 or higher.

- **File execution on edge storage**

In AXIS OS 12, to allow ACAP applications to execute files or binaries from edge storage (such as an SD card or network share), the user must explicitly configure the Axis device. This can be achieved by setting up the Extra Mount Options in Plain Config, as described below.



The screenshot shows the AXIS P3265-LV Dome Camera configuration web interface. At the top, the AXIS logo and camera model are displayed. A warning message states: "Plain config is for expert users only. Only change the settings if you know what you're doing." Below this, the "Plain config" section is active. It includes a "Select group" dropdown menu set to "None" and a search bar labeled "Search for parameters by ID" containing the text "Extra Mount Options". A note below the search bar says: "To see the effect of your changes, you might have to refresh the webpage or restart the device." The main configuration area is divided into two columns: "Storage / S0" and "Storage / S1". Each column has a label "Extra mount options" and a text input field containing the value "exec". A sidebar on the left contains various icons for navigation, with the settings gear icon highlighted.

As a result of this change, in the factory default state of AXIS OS 12, file execution from edge storage is disabled and must be explicitly configured.

Why is this change introduced? To increase the security on the device.

How can it affect me? ACAP applications requiring file execution on edge storage may not function properly if the device is not configured accordingly.

API changes:

- **Rate Control changes for RTSPs** As the VAPIX Rate Control API has evolved over the years, the relationship between some of the URL options and param.cgi parameters has become complicated. This will be simplified in upcoming versions of Axis OS. This was communicated earlier [here](#).

Why is this change introduced? To simplify the Rate control API.

How can it affect me? The new API is supported by the product when Properties.Image.RateControl.Version is 2.0 and higher. videobitrate and Image.I#.RateControl.TargetBitrate are deprecated from now. No changes are made when it comes to Average Bitrate (ABR).

- **Remove Legacy Overlays**
The possibility to create overlays via the parameter CGI will be completely deprecated. This was communicated earlier [here](#). An example of the old overlay is provided below.



Why is this change introduced? Overlays have their own API, dynamicoverlay CGI, with direct access to the overlay system. There for should this old way be deprecated.

How can it affect me? If you have third party software using this API, it will not work correctly with AXIS OS 12.0 or higher.

- **Added path restrictions for dynamicoverlay.cgi**
The *Dynamic Overlay* VAPIX API that allows to configure the path to the overlay image to display has been limited to `/etc/overlays/`. It is not possible anymore to alter the path through VAPIX API.
Why is this change introduced? Supporting to alter the path trough API is not best practice and keeping it might be a security threat.
How can it affect me? If you have third party software using this API, it will not work correctly with AXIS OS 12.0 or higher.
- **Changes in dynamicoverlay.cgi**
Optional values, "source" and "sensor" will be removed from the *Dynamic Overlay* in AXIS OS 12.

Why is this change introduced? The options are obsolete and no longer used and should therefore be removed to follow best practice.

How can it affect me? If you have third party software using this API, it will not work correctly with AXIS OS 12.0 or higher.

- **New version of `privacymask.cgi`.**
Unused functionality or parameters have been removed, while those utilized in the previous version have been preserved.

The following will be removed in `privacymask.cgi`:

`preview_on`
`preview_off`
`query list`
`query position`
`ptpolygon`
`imagerotation`
`imageresolution`
`zoomlowlimit`

The following will be removed in `param.cgi`:

parameter `Image.I[source].Overlay.MaskWindows.PtPolygon`

Why is this change introduced? Supporting capabilities that are not used is not best practice and keeping them might be a security threat.

How can it affect me? If you have third party software using this API, it will not work correctly with AXIS OS 12.0 or higher.

- **Removal of "ClassCandidate" from Analytics Scene description for ONVIF**
In the analytics scene description, both "`tt:ClassDescriptor/tt:ClassCandidate`" and "`tt:ClassDescriptor/tt:Type`" are used today for backward comparability, but they say the same information. ONVIF recommends the use of "`tt:ClassDescriptor/tt:Type`", see *metadastream.xsd*—
AXIS OS 11.11 and lower

```
<tt:Object ObjectId="101">
  <tt:Appearance>
    <tt:Shape>
      <tt:BoundingBox left="-0.6" top="0.6" right="-0.2" bottom="0.2"/>
      <tt:CenterOfGravity x="-0.4" y="0.4"/>
      <tt:Polygon>
        <tt:Point x="-0.6" y="0.6"/>
        <tt:Point x="-0.6" y="0.2"/>
        <tt:Point x="-0.2" y="0.2"/>
        <tt:Point x="-0.2" y="0.6"/>
      </tt:Polygon>
    </tt:Shape>
    <tt:Class>
      <tt:ClassCandidate>
        <tt:Type>Vehical</tt:Type>
        <tt:Likelihood>0.75</tt:Likelihood>
      </tt:ClassCandidate>
      <tt:Type Likelihood="0.75">Vehicle</tt:Type>
    </tt:Class>
    <tt:VehicleInfo>
      <tt:Type Likelihood="0.75">Bus</tt:Type>
    </tt:VehicleInfo>
  </tt:Appearance>
</tt:Object>
```

AXIS OS 12.0 and higher

```
<tt:Object ObjectId="101">
  <tt:Appearance>
    <tt:Shape>
      <tt:BoundingBox left="-0.6" top="0.6" right="-0.2" bottom="0.2"/>
      <tt:CenterOfGravity x="-0.4" y="0.4"/>
      <tt:Polygon>
        <tt:Point x="-0.6" y="0.6"/>
        <tt:Point x="-0.6" y="0.2"/>
        <tt:Point x="-0.2" y="0.2"/>
        <tt:Point x="-0.2" y="0.6"/>
      </tt:Polygon>
    </tt:Shape>
    <tt:Class>
      <tt:Type Likelihood="0.75">Vehicle</tt:Type>
    </tt:Class>
    <tt:VehicleInfo>
      <tt:Type Likelihood="0.75">Bus</tt:Type>
    </tt:VehicleInfo>
  </tt:Appearance>
</tt:Object>
```

Why is this change introduced? Axis should be in compliant with ONVIF.

How can it affect me? If you have third party software using this API, it will not work correctly with AXIS OS 12.0 or higher.

- Updating terminology from "Vehical" to "Vehicle" for ONVIF**
 Due to an error in the ONVIF Metadata Spec, "Vehicle" has been incorrectly represented as "Vehical", in the Analytics Scene description. As of AXIS OS 12, the correct term "vehicle" will be used instead. See code example at *Changes in the analytics metadata stream in AXIS OS 12.0*.
Why is this change introduced? Axis should be in compliant with ONVIF.
How can it affect me? If you have third party software using this API, it will not work correctly with AXIS OS 12.0 or higher.
- Updating terminology from "Bicycle" to "Bike" in VehicleType for ONVIF**
 Currently in the Analytics Scene description, the term "Bicycle" is used to describe both a bicycle and a motorcycle within the context of "VehicleType". As of AXIS OS 12.0, "Bike" will be used instead of "Bicycle" to describe both bicycles and motorcycles according to the ONVIF Standard, and it will be represented as an "ObjectType". See code example at *Changes in the analytics metadata stream in AXIS OS 12.0*.
Why is this change introduced? Axis should be in compliant with ONVIF.
How can it affect me? If you have third party software using this API, it will not work correctly with AXIS OS 12.0 or higher.
- Removal of the lightcontrol web service API**
 The lightcontrol web service API (implemented in ws/wsd/impl/ali) has been deprecated for many years and is replaced by the lightcontrol-cgi JSON API. Information about this change has been sent out previously to partners.
Why is this change introduced? It is obsolete, and keeping it might be a security threat.
How can it affect me? If you have third party software using this API, it will not work correctly with AXIS OS 12.0 or higher.

Product specific:

- Remove support for AXIS T6101/T6112**
 Support for AXIS T6101 and AXIS T6112 will be removed. Read more about compatible products on axis.com

Why is this change introduced? AXIS T6101 and AXIS T6112 are discontinued.

How can it affect me? AXIS T6101 and AXIS T6112 does not work with Axis devices running AXIS OS 12.0 or higher. Please use AXIS OS LTS 2024 instead.

Changes in AXIS OS 11

Please note that some breaking was done AXIS OS 11, but with limited impact.

The changed default behavior in AXIS OS 11 will affect the product after a **factory reset**, as well as new products launched with that specific version, but will not affect an upgrade, i.e. if you upgrade AXIS OS without a factory reset, your products will not change their behavior.

Security:

- **Remove access via FTP protocol**
 Since AXIS OS 11.1, we have removed the possibility to access the device via the FTP protocol, to increase overall minimum cybersecurity level.
 For troubleshooting purposes it is recommended to use secure SSH access. Note that upload from the device to an FTP server is still possible. For more information, visit SSH access in the AXIS OS Knowledge base.
Why is this change introduced? To increase overall security.
How can it affect me? If you have third party software using this feature, it will not work correctly with AXIS OS 11.1 or higher.
- **Removed support for proxy SOCKS version 4 and 5**
 Since AXIS OS 11.0, support for proxy SOCKS version 4 and 5 has been removed.
Why is this change introduced? It is obsolete, and keeping it might be a security threat.
How can it affect me? If you have third party software using this feature, it will not work correctly with AXIS OS 11.0 or higher.
- **No dedicated root user in factory defaulted state**
 Since AXIS OS 11.5, no dedicated root user is pre-configured in factory defaulted state. To ease O3C-related integrations and to allow time to adapt, Axis made a modification that currently creates this root user for O3C onboarding/integration. From LTS 2024, O3C integrations shall not rely on the previously available admin user named "root". If a separate (admin) user is deemed necessary for some purpose, this user shall be specifically created during the initial onboarding/integration.
Why is this change introduced? To lower the attack surface of the device and increase the overall device security.
How can it affect me? If you have third party software using root as hardcoded username, it will not work correctly with AXIS OS 11.5 or higher unless you create a user root.
- **Root-privilege is disabled in factory defaulted state**
 Root-privileged access is disabled by default in Axis products and ACAP applications to increase ACAP confidentiality by better protecting their data and secrets, to prevent information leakage and to increase AXIS OS system integrity by removing system-wide root-privileged access for users and applications. In AXIS OS 11, this can still be enabled by parameter if required, see screenshots below for reference:

Apps

+

Add app

Find more apps

Allow unsigned apps

Allow root-privileged apps

●

AXIS Video Motion Detection

Version: 4.5-8

Axis Communications

Open

●

AXIS Object Analytics

Version: 1.13.11

Axis Communications

Open

SSH accounts

+

Add SSH account

Restrict root access

Enable SSH

Account

Comment

root

root

Please read the *full guide* for more information. The changes in AXIS OS 11 are summarized below.

Why is this change introduced? To increase the security on the device.

How can it affect me? Affected ACAP applications has been communicated about this and should create a new version if they are affected regarding this change.

AXIS OS	Timeline	Changes
11.5	June 2023	– –
11.6	September 2023	–
11.8	January 2024	– –
11.11	June 2024	–
LTS 2024	H2 2024	Support: 2024–2029. Can be used as a stop-gap solution until an ACAP application is fully adapted. – –

VAPIX API changes:

- PTZ VAPIX API version 2

31

Since AXIS OS 11.0, there is a new version of the PTZ VAPIX API. For more information, visit the *VAPIX library*.

- **Removal of date.cgi**
 Since AXIS OS 11.0, the date.cgi has been removed and replaced by time.cgi. For more information, visit the *VAPIX library*.
Why is this change introduced? It is obsolete, and keeping it might be a security threat.
How can it affect me? If you have third party software using this API, it will not work correctly with AXIS OS 11.0 or higher.

- **Support removed for BMP format**
 Since AXIS OS 11.0, support to request an image in BMP file format has been removed. For more information, visit the *VAPIX library*.
Why is this change introduced? It is obsolete, and keeping it might be a security threat.
How can it affect me? If you have third party software using this feature, it will not work correctly with AXIS OS 11.0 or higher.

- **Removed support of recording mediaclip through Mediaclip API**
 Since AXIS OS 11.0, support to record a mediaclip using the Mediaclip API has been removed. For more information, visit the *VAPIX library*.
Why is this change introduced? It is obsolete, and keeping it might be a security threat.
How can it affect me? If you have third party software using this feature, it will not work correctly with AXIS OS 11.0 or higher.

- **Parameters in the root.PTZ parameter group changes**
 Since AXIS OS 11.0, changed access for a number of parameters in the root.PTZ parameter group. For more information, visit the *VAPIX library*.
Why is this change introduced? Due to architectural changes.
How can it affect me? If you have third party software using this, it will not work correctly with AXIS OS 11.0 or higher.

- **Removal of edit.cgi**
 Since AXIS OS 11.1, the edit.cgi has been removed. For more information, visit the *VAPIX library*.
Why is this change introduced? It is obsolete, and keeping it might be a security threat.
How can it affect me? If you have third party software using this API, it will not work correctly with AXIS OS 11.1 or higher.

- **Removal of libvidcap**
 The libvidcap has been removed. Use Video capture API instead. For more information, visit the *ACAP developer guide*.
Why is this change introduced? It is obsolete, and keeping it might be a security threat.
How can it affect me? If you have third party software using this API, it will not work correctly with AXIS OS 11.1 or higher.

- **Removal of overlay-cgi.**
 The overlay-cgi has been removed in AXIS OS 11.10. It is recommended to use overlayimage-cgi instead, see more info in the *VAPIX Library*.
 VAPIX API parameter affected:
 call_overlay_upload.cgi
 call_overlay_del.cgi
 call_overlay_set.cgi
 create_overlay.cgi
 overlay_list.cgi
 overlay_image_formats.cgi
Why is this change introduced? It is obsolete and replaced by a different API.

How can it affect me? If you have third party software using this API, it will not work correctly with AXIS OS 12.0 or higher.

Other changes:

- **Removal of the built in motion detection**
In AXIS OS 11.2 the old built in motion detection, also known as VMD1, was removed.
Why is this change introduced? It is obsolete, and keeping it might be a security threat.
How can it affect me? If you have third party software using this application, it will not work correctly with AXIS OS 11.2 or higher.
- **Removed installable decoder AAC**
Since AXIS OS 11.0, the installable audio decoder for AAC has been removed and is no longer downloadable from the cameras web interface.
- **Removed installable decoder H.264**
Since AXIS OS 11.0, the installable decoder for H.264 has been removed and is no longer downloadable from the cameras web interface.

Next AXIS OS version

Please note that this schedule is preliminary and that both time schedule and included features are subject to change as work progresses.

For the Developer News articles, visit the *Developer Community*.

AXIS OS 12.5

Scheduled for: June 2025

Features for all products

- Added support to set custom headers for HTTP-based video streaming cgi.
- The Power settings API has been updated with a new "powerState" value in the PowerStatus object, indicating whether the power supplied by the PSE supports full or limited device functionality.
- A new "Type" option has been added to Remote Syslog configuration (System -> Logs -> Remote system log), allowing users to choose between sending all logs ("All") or only audit logs ("Audit").

Cybersecurity updates

- Updated Apache to version 2.4.63 to improve cybersecurity.

Analytics updates

- If an ACAP application installed on the device can't be re-installed on the new AXIS OS version, a rollback occurs. For example, upgrading from AXIS OS 11.11 to 12.5 will trigger a rollback if an ACAP application runs as the root user. Previously, the failing application would be dropped, resulting in lost settings after the upgrade.
- Both the device system-on-chip (SOC) and architecture are displayed in "Install an app", in the web interface.
- AXIS License Plate Verifier
 - Added support for PTZ cameras: AXIS P5676-LE, AXIS Q6135-LE, AXIS Q6225-LE, AXIS Q6315-LE, AXIS Q6318-LE, AXIS Q6355-LE and AXIS Q6358-LE. Pairing is supported for up to two preset positions.
 - Added support for AXIS A9210
 - Corridor mode has been added to supported AXIS ARTPEC-7, AXIS ARTPEC-8, and AXIS ARTPEC-9 products.
 - License plate recognition has been improved for various regions, including Dubai, New Zealand, Latvia, and Canada.
 - The event retention behavior has been changed when no SD card is present, affecting full frame, downsized frame, and vehicle crop selections.
 - Corrected an issue with the maximum retained events on SD cards.
 - Corrected an issue with umlaut display on text overlays.
 - Corrected an issue with the Area of Interest, when there are too many polygons are set in the upper part of the zone.
 - Corrected an issue with the Test button under Push Event menu related to VAPIX events
- AXIS Audio AnalyticsApplies to: AXIS D4200-VE, AXIS M3086-V, AXIS P1465-LE, AXIS P1467-LE, AXIS P1468-LE, AXIS P9117-PV, AXIS Q1656/-B/-DLE, AXIS Q1728, AXIS Q1805-LE, AXIS Q1806-LE and AXIS Q9307-LV
 - Sound pressure level: New feature that measures how loud a sound is in decibels.
 - Audio classification: Added speech and coughing fit.
- AXIS Scene Metadata

Applies to: All products with AXIS Scene Metadata support.

- Added support for detecting the "human carries bag" relation.
- Relation detection is available through the Analytics Scene description producer via RTSP.
- When a human is detected carrying a bag, a Bag element is added to the Appearance/ HumanBody/Belonging element.
- Enabling the "metadata_fusion_experimental_classes" feature flag allows tracking of bags as objects, including their relation to humans, bounding box, and type (via the non-standardized BagInfo element).

Product specific features

- Hardware modifications have been made to proactively prepare for the new NDAA 23 regulations that will be required in 2028. You will find more information about NDAA Compliance on axis.com. In AXIS OS knowledge base, you will find more about the hardware changes. The hardware ID can be found in Plain config > Properties > System > Hardware ID.
 - Products with Hardware IDs A45 only support active track 12.5.xx and later..

Applies to: AXIS Q1728

- Added the possibility to enable the PTZ legacy mode for optics control and PTZ presets .

Applies to: AXIS Q1800-LE, AXIS Q1800-LE-3, AXIS Q1805-LE, AXIS Q1806-LE, AXIS Q1808-LE and AXIS Q1809-LE

Current AXIS OS version

AXIS OS 12.4

Release date: April 2025

- **Features for all products**
 - Added support to set custom headers for HTTP-based video streaming cgi.
- **Cybersecurity updates**
 - Added support for Crypto-Policy setting to chose between standard OpenSSL cipher suite or FIPS 140-2 cipher suites. The Crypto-Policy setting can be adjusted from the Security tab in the web-interface or through VAPIX API.
 - Added support for OAuth 2.0 RFC6749 Client Credential Flow for token-based machine-to-machine communication that provides better overall security as traditional digest/basic authentication schemes.
- **Product specific features and changes**
 - Zipstream storage profiles for AV1 format now support B-frames, allowing for more efficient video compression.

Applies to: All products based on *AXIS ARTPEC-9*

- Hardware modifications have been made to proactively prepare for the new NDAA 23 regulations that will be required in 2028. You will find more information about NDAA Compliance on axis.com. In AXIS OS knowledge base, you will find more about the *hardware changes*. The hardware ID can be found in Plain config > Properties > System > Hardware ID.
 - Products with Hardware ID A1D and A1E only support active track 12.4.XX and later, as well as coming LTS 2024 11.11 version and LTS 2022 10.12 version, and later.

Applies to: AXIS M7116 and AXIS P7316

Open source library support

AXIS OS-based network products use a variety of open source libraries. Therefore, it is critical that changes to these libraries are reflected in AXIS OS. Libraries are updated in the AXIS OS Active and LTS tracks in conjunction with the release. If there are no software restrictions, they are also updated in the PSS track.

If an open source library becomes end-of-life (EOL) by the upstream community, Axis aims to replace the library in a timely manner or provide support in a different way depending on its use within the AXIS OS-based network product. An example is listed below.

OpenSSL is used for cryptographic operations. The currently used OpenSSL 1.1.1 version is a long-term support (LTS) release which has reached its *EOL during September 2023* as announced by the OpenSSL foundation.

- From AXIS OS 11.6.89 and onwards, the newest OpenSSL 3.0 library (LTS) is supported in addition to the current OpenSSL 1.1.1, which will be deprecated but still usable.
- Axis plans to remove OpenSSL 1.1.1 support in AXIS OS 12 after LTS 2024.
- To support AXIS OS LTS tracks, Axis has a support contract agreement with the OpenSSL foundation for continued patching of OpenSSL 1.1.1.

ACAP related information

Starting from ACAP SDK version 4.14, we're integrating the latest openssl Version 3 into the Native ACAP SDK. Please read more in the *release notes* and explore API examples on *GitHub* for details.

What needs to be done:

If any Axis-owned ACAP relies on the OpenSSL 1.1.1 runtime dependency provided by the platform, it requires refactoring and rebuilding with OpenSSL 3 libraries. We recommend utilizing the latest ACAP SDK (4.14) to ensure compatibility with the correct library version.

Software Bill of Materials

A Software Bill of Materials (SBOM) is an inventory of all components included in the software. It has become an increasingly important and common part of software development lifecycle and processes. It allows IT Operations and Security staff to determine which third-party or open-source software is packaged with your software. Having an SBOM is important when it comes to securing your IT systems and protecting user data.

Why do Axis publish an SBOM?

Axis works actively with the principles of openness and building trust through transparency, the SBOM is a valued addition to these principles. It provides our customers with the information necessary to know whether or not the products we have provided may be vulnerable to cyber attacks.

For which AXIS OS versions?

Axis will provide an SBOM for all AXIS OS releases on active track starting with release 11.2.

What is included?

The Axis SBOM contains information about Axis-Proprietary components and Opensource software used to assemble AXIS OS.

What is excluded and why?

Due to current licensing/legal limitations we cannot provide information about third-party proprietary software. Our aim is to cover all the third-party components as legally possible if third-party vendors agree. Furthermore, some components like the Linux Kernel needs to be enriched further for more granular sub-components.

Where can I find the SBOM?

The SBOM is located together with the AXIS OS version it is based on. AXIS OS can be found in the product support or at the [download page](#).

What format and why?

The Axis SBOM is produced in accordance with the CycloneDX SBOM specification. This format seems to be the most usable in other systems and strives to be a minimalist format easy to work with. Advantages of this format can be found [here](#).

What is the difference between a SBOM and the Third party software licenses document?

The Third party software licenses document is meant to list all legal agreements and licenses with third parties related to any intellectual property that allows us to use, market and incorporate this into our products.

What about SBOM for other AXIS software?

This is a start, and we are looking into how SBOM is applicable to other software from Axis.

Where can I find more information about SBOM in general?

The *National Telecommunications and Information Administration* provides more educational information about SBOM.

- *Framing Software Component Transparency: Establishing a Common Software Bill of Material (SBOM)*
- *Software Bill of Material FAQ*

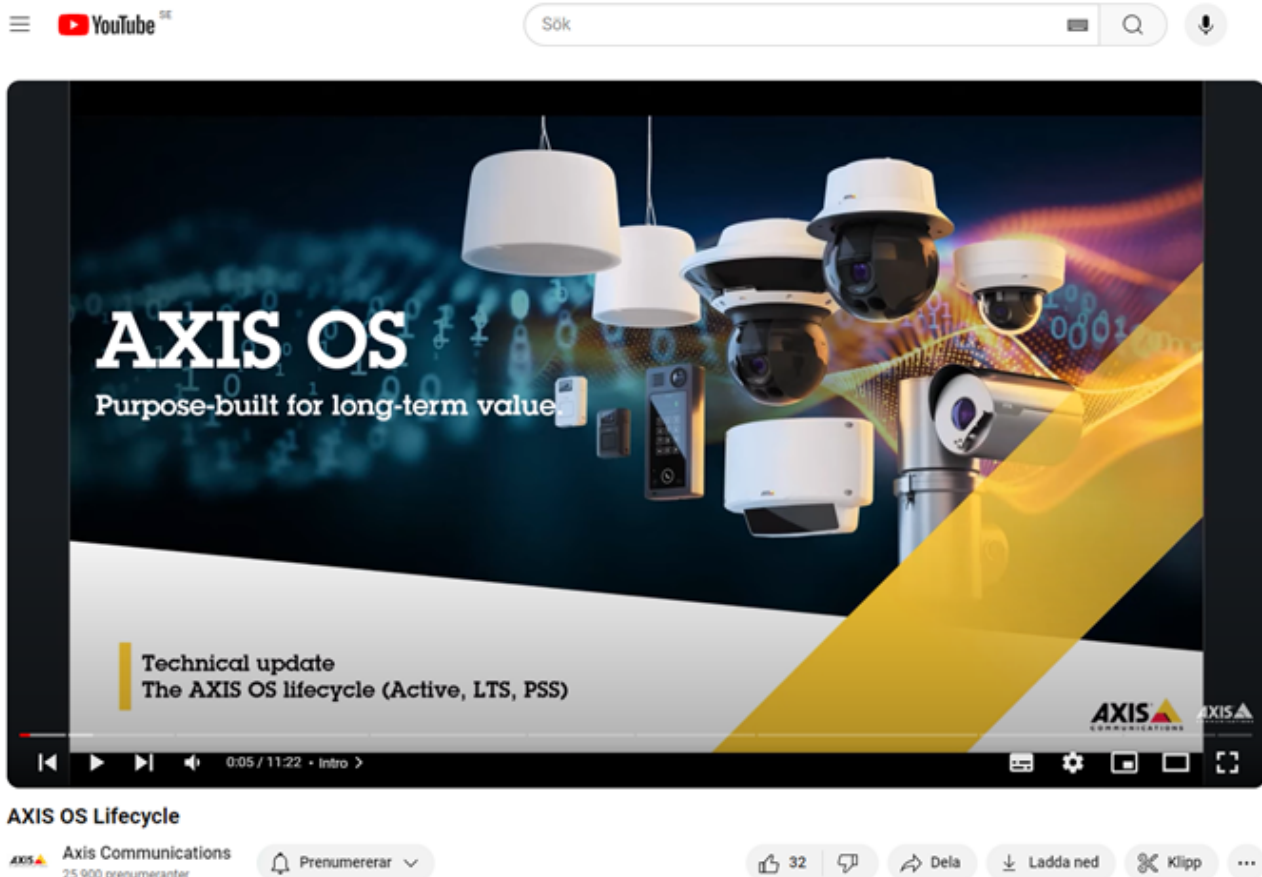
How can I use the SBOM to analyze the software?

The Axis SBOM contains information about Axis-Proprietary and Opensource software used to assemble AXIS OS. The Axis SBOM can be used by third party vulnerability scanners to highlight known vulnerabilities in software packages. A vulnerability that applies to a certain module or feature in a software package needs to be loaded and used by the Axis device. Vulnerabilities in modules that are not loaded are not relevant but may still be flagged by the vulnerability scanner or SBOM information. For more information on how to work with the result of a security scanner see: *AXIS OS Vulnerability Scanner Guide*.

AXIS OS lifecycle management

AXIS OS supplies three types of tracks: **active**, **long-term support (LTS)** and **product-specific support (PSS)** track.

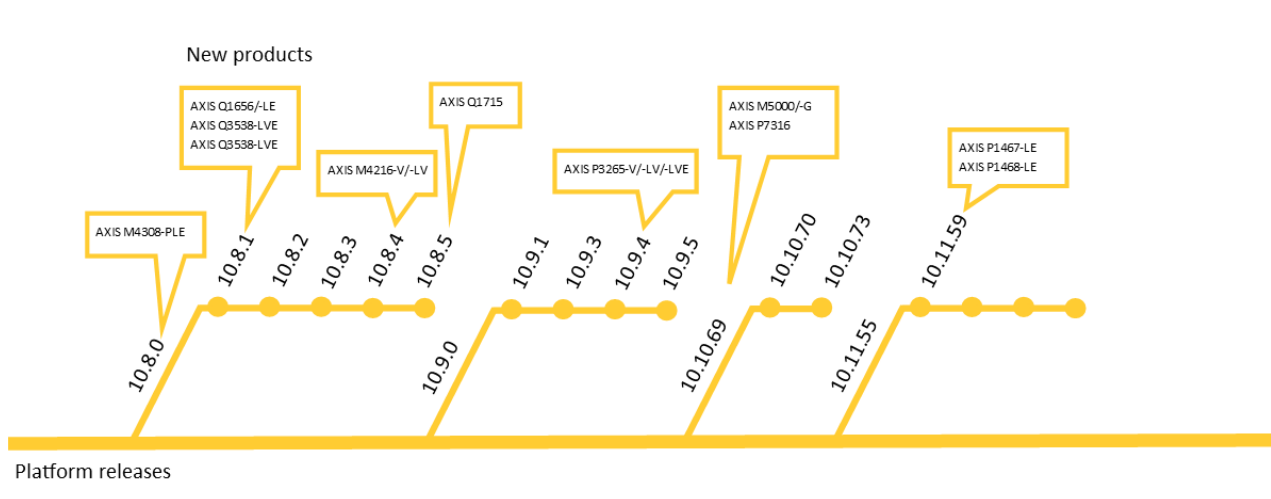
In the active track, we consistently add new features while also improving cybersecurity. In LTS, we refrain from introducing new features, prioritizing to maintain cybersecurity and ensuring compatibility. PSS will receive updates less frequently compared to our other two tracks, but we remain committed to addressing bug corrections and upholding cybersecurity measures.



There's a *YouTube video* that explains the AXIS OS lifecycle in more detail. It covers our different tracks, version management and upgrade recommendations.

Active track

The most updated and feature progressive track of AXIS OS, that is suitable for customers who want access to the newest features and improvements. New products are launched on this track, which means the most immediate access to any new features and updates.



Long-term support track

The focus of the long-term support (LTS) track is to keep the products well integrated with third-party equipment or software, and still get necessary bug fixes and cybersecurity updates. An LTS track has a fixed feature set and a new track is created every two years and maintained for 5 years. No new products or features are added to the LTS track.

Product-specific support

Product-specific support (PSS), is a rare track used when a product needs support after an LTS track has expired. The products on this track will still receive necessary bug fixes and cybersecurity updates. Each product is on its own track, the tracks are not connected with one another. Also, other non-Axis OS products have similar support tracks.

	Active Track	LTS	PSS
Pace	6 major releases/year	Differs between LTS	Differs between products
Supported	Latest version	Latest version in each track	Latest version
Focus on	Feature growth	Compatibility	Compatibility
Vulnerability patches	✓	✓	✓
New security features	✓	✗	✗
New features	✓	✗	✗
New product launch	✓	✗	✗
Product discontinue	✗	✓	✓
Example releases	11.1.70, 11.2.53, 11.3.71, 11.4.5	8.40.x, 9.80.x, 10.12.x	6.50.5.16, 7.10.3026, 8.45.4.3

Suggested track

Below is a list of system characteristics and goals to help you choose the right track.

Highest level of cybersecurity – AXIS OS active

AXIS OS active track provides security patches and the latest enhancements including security.

Need for specific new features – AXIS OS active

AXIS OS active track offers the latest features. In some areas, such as analytics, the gap between Active, LTS and newer products may be greater.

Satisfied with current features and cybersecurity level – AXIS OS LTS

LTS tracks has focus on compatibility and adding new cyber security patches. AXIS OS LTS track do not introduce new features or breaking changes.

Extensive internal verification process when accepting new software updates – AXIS OS LTS

Updates within the same AXIS OS LTS track shouldn't require recertification. If validating new releases is costly or time-consuming, the AXIS OS LTS track is recommended.

Existing processes involve frequent updates of VMS and system components. – AXIS OS active or AXIS OS LTS

Both AXIS OS Active and LTS track may be used. Each new Axis release is validated with Milestone, Genetec and AXIS Camera Station.

Make sure your VMS is validated before upgrading.

Current processes lack frequent updates for VMS and system components – AXIS OS LTS

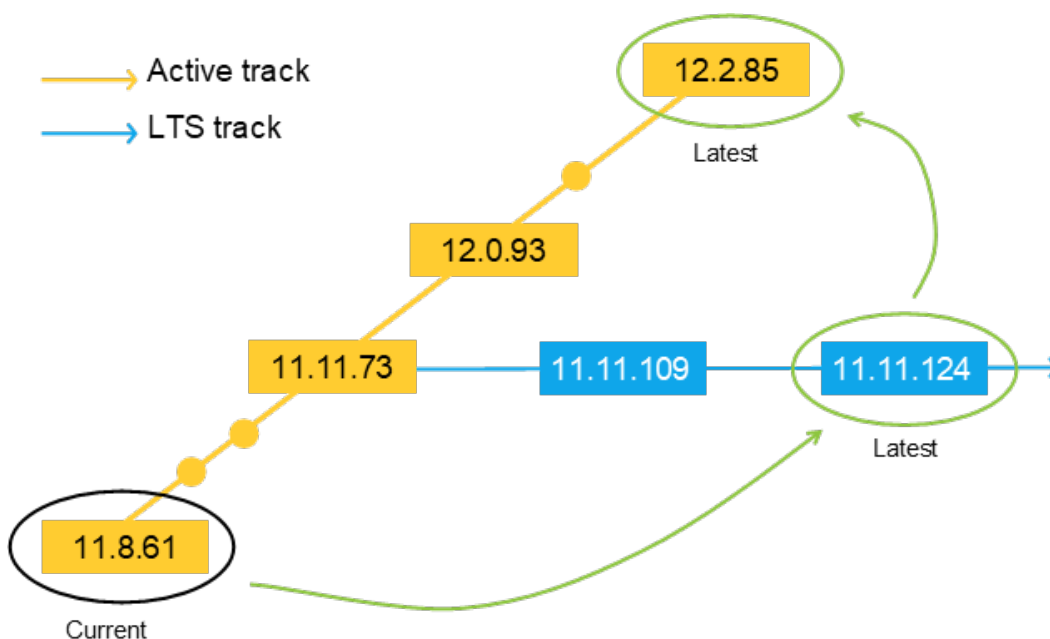
Verify with your VMS and ACAP provider which versions they test and recommend. AXIS OS LTS is the recommended choice for optimal compatibility.

Upgrade path

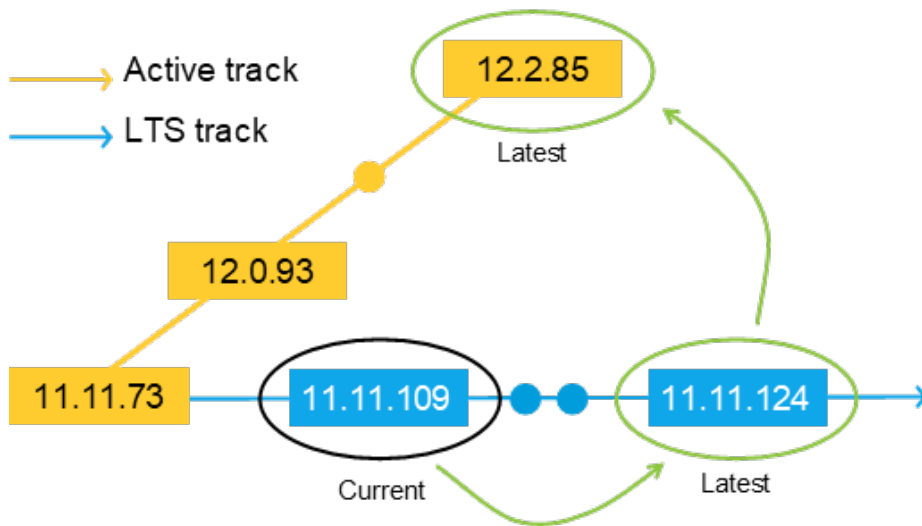
You can upgrade your devices using the web interface or various device management tools, such as AXIS Device Manager, AXIS Camera Station Pro, and AXIS Camera Station Edge. AXIS Device Management Extend simplifies the upgrade process by providing built-in backend upgrade paths. Read more about *How to upgrade* in AXIS OS Knowledge base.

Here are some recommendations for how to upgrading:

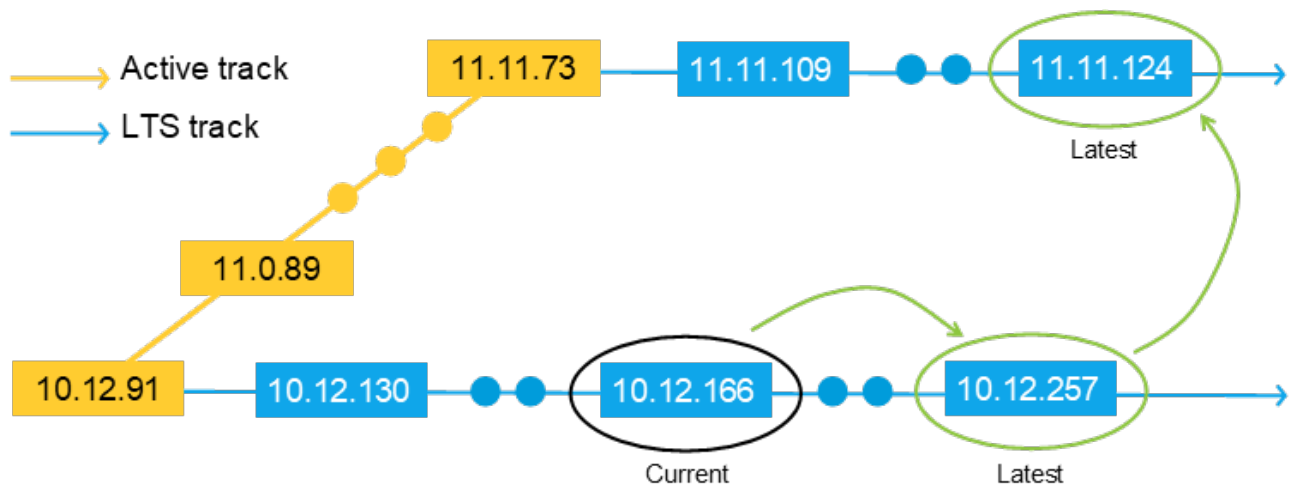
- Upgrading from an older active track to the latest active: Upgrade to the latest version of the intermediate LTS.



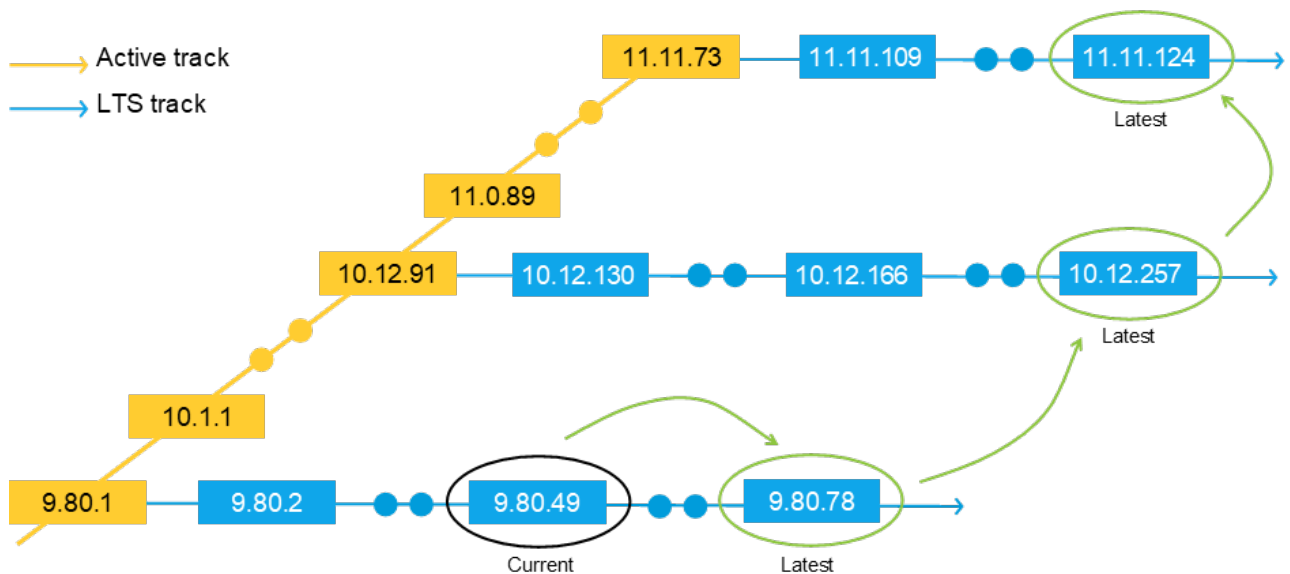
- Upgrading from the latest LTS track to the active track: Start by upgrading to the latest version of your current LTS.



- Upgrading from an older LTS to the next LTS version: First, update to the latest version of your current LTS



- Upgrading from an older LTS to two newer LTS versions: Upgrade to the intermediate LTS version first.



Considerations

A new active track always means that something has changed. To move AXIS OS forward we deliberately introduce breaking changes to keep our software up-to-date due to cybersecurity and feature growth. When you upgrade to a newer track please keep in mind we may have introduced new features, changed the default settings, and performance enhancements can affect compatibility with your existing system.

Over time, multiple LTS tracks become available for a product. Each LTS track is designed to provide long-term consistency by focusing on bug fixes without introducing new features. However, it's a good idea to upgrade to the latest LTS track.

Therefore, product upgrades should be performed in a controlled and monitored manner to ensure that the version is performing as expected in your environment before proceeding. It is always recommended to have a group of devices that represent your inventory in a test environment and validate the upgrade before the actual installation. Grouping and testing please read more [here](#).

Stay current with AXIS OS upgrades

Maintaining a consistent upgrade strategy is essential for ensuring your Axis products benefit from ongoing enhancements. Axis Technical Services also advises upgrading to the latest version when addressing issues with an Axis product.

Selecting the right latest version

With multiple upgrade options available, it's important to choose the appropriate "latest" version. Here's some guidance:

- For Long-term support (LTS), we recommend to choose the newest LTS track if available for your product.
- On any track (Active or LTS), we recommend upgrading to the latest available version.

By following this approach, you'll keep your Axis products up-to-date with optimal performance and cybersecurity.

Additional Q&A

- **If my Axis product is running on the LTS 2022 (10.12) track, should I consider upgrading to the latest AXIS OS active track?** It depends on third-party dependencies and compatibility with the active track. Generally, we recommend remaining on the LTS 2022 (10.12) track and updating within that track as long as it's supported. If you need features only on the active track, upgrading might be worth considering.
- **I would like to run my Axis product on an LTS track, but there is currently no LTS track available?** If your product was released between two LTS tracks, it's recommended to keep it updated on the active track until a new LTS track is available. New LTS tracks are introduced every two years.
- **If there are multiple LTS tracks available, which LTS track should I choose?** We recommend using the latest LTS track supported by your third-party software. This ensures compatibility, reduces the need to switch tracks, and provides access to the latest cybersecurity updates and features.
- **What should I do if my VMS states that it requires a specific version of the LTS track, such as version 9.80.3.2 on LTS 2020, but I cannot find it on axis.com?** If your VMS specifies a specific LTS version, it will also be compatible with subsequent releases within that track. VMS systems typically list one version because it was certified with it, but compatibility remains consistent within each LTS track. It's generally safe to use other versions.
- **When upgrading from an old LTS to a new LTS, is it necessary to upgrade to the intermediate versions?** To preserve settings, we recommend upgrading in incremental steps. If resetting the device to factory defaults, however, intermediate versions are not necessary.

General recommendations

Follow the below recommendations to optimize AXIS OS performance, ensure cybersecurity, and simplify updates and lifecycle management.

Always use the latest supported AXIS OS version:

- Always run the latest version within your selected AXIS OS track.

- Ensure that all models in your system are running the same AXIS OS version, if possible.
- If you have products with different HWIDs for the same model, make sure you are still running the same version, see *Hardware Changes* in the AXIS OS Knowledge Base.
- If AXIS OS LTS track is preferred, choose the latest available LTS version for each product.
- The LTS track provides robust cybersecurity measures and allows time to plan for upgrading to a newer LTS track when needed.

Simplify software updates and lifecycle planning using device management tools:

- E.g. *AXIS Device Manager* and *AXIS Device Manager Extend*.
- Plan for device replacement before software reaches end-of-support.

Stay up-to-date on cybersecurity recommendations:

- Subscribe to *cybersecurity notifications* for the latest updates.
- Apply recommendations from *AXIS OS hardening guide* to secure your devices.
- Use network security scanners (e.g., Tenable, Rapid7) to identify potential vulnerabilities.

Upgrading between AXIS OS LTS tracks:

- If you are changing AXIS OS tracks (LTS or active), please read the .
- Read the *release notes*, changes has been done between the different tracks.

Verification of new releases:

- When updating within the same AXIS OS LTS track additional certification or compatibility testing is usually not required.
- For large systems using AXIS OS active track, it's recommended to pre-test new releases in a staging environment before deploying them to production. This ensures a smooth transition and minimizes potential disruptions.
- To stay ahead of the curve, take advantage of *AXIS OS active track beta releases* to test upcoming features and enhancements in your staging environment prior to the official release.
- Axis verifies all new AXIS OS releases against the latest versions of AXIS Camera Station, Genetec and Milestone. If you are using older VMS versions or VMS solutions from other vendors, we recommend pre-validating new AXIS OS active track releases to ensure compatibility.
- Ensure that all components in the system supports the new version before changing LTS tracks or major versions on AXIS OS Active track.

Downloading AXIS OS

Which AXIS OS tracks are available for an Axis edge device can be obtained when downloading AXIS OS from the *download page*.

AXIS OS can also be found on the product support page for each product, where you can find all available supported versions and some older. Older unsupported versions will periodically be removed due to known bugs and cybersecurity vulnerabilities that are corrected in later releases. It is recommend to only AXIS OS versions that are supported.

Download device software

Find the right software (previously firmware) releases by searching for your device.

P3265-LV



Product	End of support ⓘ	Version		
AXIS P3265-LV	2031-12-31	12.1.64 - AXIS OS active	RELEASE NOTES	🔒 DOWNLOAD ▼
		11.11.124 - AXIS OS LTS 2024	RELEASE NOTES	🔒 DOWNLOAD ▼
		10.12.262 - AXIS OS LTS 2022	RELEASE NOTES	🔒 DOWNLOAD ▼

Please see below a list of common tags that indicate different AXIS OS tracks as seen in the picture above.

Tag example	Explanation
12.1.64 - AXIS OS active	AXIS OS active track providing new features, security and other improvements.
11.11.124 - AXIS OS LTS 2024 10.12.262 - AXIS OS LTS 2022 9.80.66 - AXIS OS LTS 2020	AXIS OS long-term support track (LTS) providing security and maintain compatibility.
8.40.59 - PSS 6.50.5.19 - PSS 5.51.4.7	With and without PSS tag. Product-specific support (PSS) track.

AXIS OS versioning

AXIS OS releases are denoted by a unique number combination. Older releases were named by the year and type of the release but since release 10.10 we changed the versioning. The differences and the significance of each number is explained in the figures below.

In some cases, you may also notice an additional number at the end. This version builds on the main AXIS OS release with additional features, such as AXIS Access Control products.

11.5.64



Major
release
version

Minor
release
version

Patch
number

- The major version is incremented after a new active track has been created. This happens every two years when the active track becomes an LTS track.
- The minor version is indicating what feature set is included and updated with each feature release approximately 6 times per year.
- The patch number is increased more often, it's used for adding patches and bugfixes, and only final versions will be available to customers. This means that this number is only a number to mirror the external version with the internal version.

Previous versioning .

7.10.1.2



Year:
6 = 2016
7 = 2017
8 = 2018
9 = 2019
10 = ...

Yearly release:
10 = release 1
20 = release 2
30 = release 3
40 = release 4
50 = ...
(X)5 = PFW

Major
release
version

Minor
release
version

AXIS OS Support

When a product has an AXIS OS support date, what does that mean?

The product will be supported during this period with bug fixes as well as critical security updates, and with focus on compatibility and consistency.

What is required to get the full support period?

To benefit from the full support period of AXIS OS, the device must be upgraded to the latest active, LTS or PSS version. For more information on upgrade strategies, see .

How long can I expect to get AXIS OS support for my product?

Axis generally provides 5 years of Axis OS support from the product's discontinuation date. This policy was introduced in 2016, ensuring that our customers receive extended support for their devices. To view the exact support date for your product, please visit the product's support page.

Why do some products display only the date for Hardware support and not AXIS OS support, or vice versa?

The dates displayed depend on investigated information and the product's lifecycle stage. For older products, no dates may be shown, while in other cases, two different dates might be displayed. If the product has a defined end-of-support date for hardware and AXIS OS, both dates will be shown.

What accounts for the diverse end-of-software support dates across different products?

Each product's end of software support date is determined based on its unique hardware characteristics, including system-on-chip (SoC) type, memory capacity, and market segment.

Why do some products lack an AXIS OS support date?

Some products are not included in the development of AXIS OS, and therefore some old products have no software support dates. However, dates will be available for more products in the Axis portfolio over time. For further questions, please contact *Axis Technical Support Helpdesk*.

What happens once the AXIS OS support has expired for a product?

No further updates, improvements or security patches will be released. There are limits to how long we can maintain software currency and implement changes to an older version. Modifying software that is limited by hardware resources becomes increasingly challenging and complicated over time. Eventually, we reach a stage where it is no longer possible to guarantee the cybersecurity of the product. This signals that it is time to replace the device.

Where can I find further information on the current forecast for AXIS OS, upcoming changes and which tracks are currently supported?

Please follow and monitor the .

Example of AXIS OS Support:

Throughout its product lifecycle, the AXIS Q1656-LE will continue to receive new features, increased cybersecurity, improvements and security updates until 2028. Between 2028 and the end of 2033, it will receive some improvements along with all security updates through LTS 2028, with a focus on compatibility.

