# AXIS OS Portal

## Table of Contents

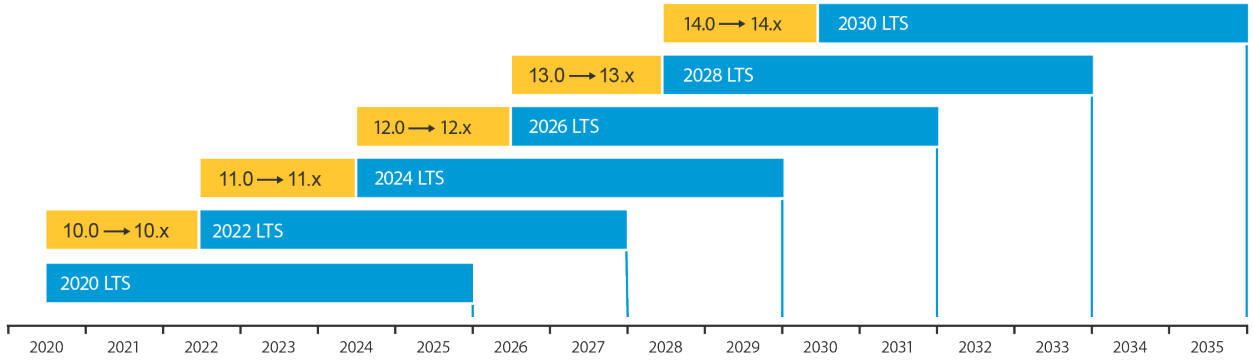
*AXIS OS Release Notes* | *AXIS OS Knowledge base* | *AXIS OS YouTube playlist* | *AXIS OS Hardening Guide* | *Security Advisories*

# 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: *Active track, on page 45*, *Long-term support track, on page 46*, and *Product-specific support, on page 46*.
See *AXIS OS lifecycle management, on page 45* 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 |
|---|---|---|---|
| 12.10 | Active | April 2026 | • OpenSSL to version 3.5.5<br>• OpenSSL version 3.0.19 |
| 11.11 | LTS 2024 | May 2026 | • OpenSSL version 3.0.19<br>• OpenSSL version 1.1.1zf |
| 10.12 | LTS 2022 | June 2026 | • OpenSSL version 1.1.1zf |
| 9.80 | Product-specific support | June 2026 | • OpenSSL version 1.1.1zf |
| 8.40 | Product-specific support | May/June 2026 | • OpenSSL version 1.1.1zf |
| 6.50 | Product-specific support | May 2026 | • OpenSSL version 1.1.1zf |

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

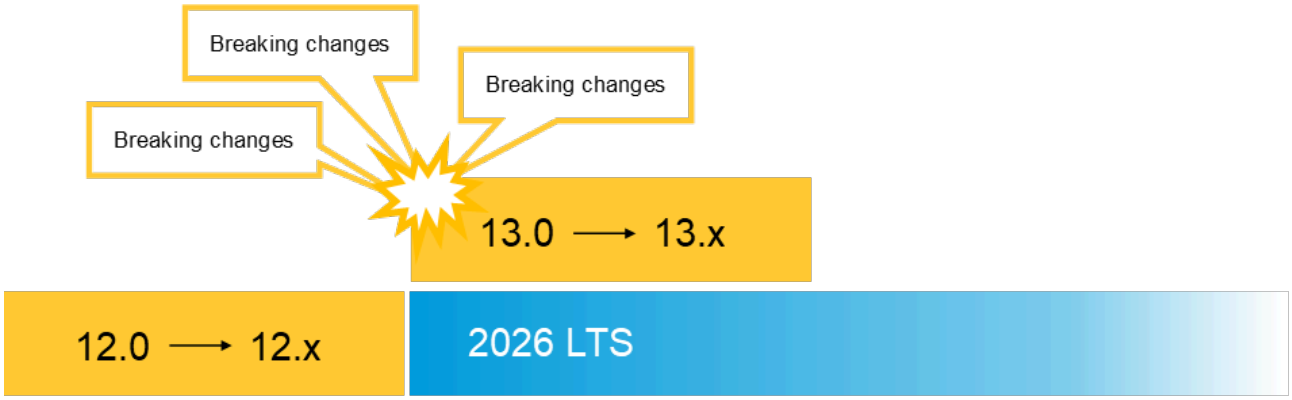
**Subscriptions**

- 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 planned for the first version of AXIS OS 13, scheduled for release in September 2026.

Please note that while the list may be adjusted, **no new changes will be added**. Some breaking changes may be postponed to AXIS OS 14 or removed entirely.

In April 2026, a preview version including all breaking changes will be available for download so you can test and verify them. More information will follow.

### Year 2038 problem (Y2038)

The widely known *Year 2038 problem* (Y2038) needs to be addressed proactively, well before 2038.
This issue is related to time computation: any reference beyond 2038 will fail, and problems can occur even before the exact date.

AXIS OS 13 will be 2038-ready, which requires both internal services and ACAP applications running on AXIS OS to adapt.

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

**Reason for change:**To proactively solve the Year 2038 problem and avoid faulty device states. Addressing it now ensures a smooth transition to 64-bit timing, considering the expected 10-year lifespan of our devices. The Y2038 problem affects computations involving dates beyond 19 January 2038 (03:14:07 UTC). On 32-bit systems, the system clock would otherwise wrap back to 13 December 1901 (20:45:52 UTC) when the counter overflows.

AXIS OS 13 serves as the essential architectural foundation for Y2038 resolution. By switching to a 64-bit time_t and updating the kernel and glibc APIs, we are building the infrastructure necessary to eventually achieve full compliance.

Achieving full Y2038 compliance is an iterative process involving extensive testing and bug-fixing. This work will be carried out across two tracks:

- **AXIS OS 13 (32-bit and 64-bit products):** This track provides the 64-bit timing variables required for future-proofing. Fixes for time-related bugs will be rolled out as they are identified.
- **AXIS OS 12 (64-bit products):** For products already on a 64-bit architecture, applicable Y2038 patches and bug fixes will be backported to the AXIS OS 12 track.

While the system is not automatically compliant upon the initial release of AXIS OS 13.0, this change initiates the transition. All subsequent fixes and optimizations will be handled by Axis and delivered transparently via standard OS updates.

**The impacts:** AXIS OS will switch to 64-bit `time_t` and 64-bit time APIs in `glibc` and the Linux kernel. This is an ABI (Application Binary Interface) break, meaning ACAP applications and other internal services must be recompiled to run on AXIS OS 13. Regardless of whether the product is 32-bit or 64-bit, if there is an incompatible ACAP application, the upgrade to AXIS OS 13 will fail. To be able to upgrade the incompatible ACAP application must be removed first.

However, it is more challenging for 32-bit products (*ARTPEC-7* and *i.MX6SX*).

**32-bit products:**

- If an ACAP application is not compatible, the upgrade to AXIS OS 13 will fail, and the device will roll back to AXIS OS 12.
- To upgrade to AXIS OS 13, any incompatible ACAP must first be removed.
- In order to perform a seamless upgrade, ACAP application must not have any dependency on 32-bit time. This is hard to achieve and requires extensive testing; therefore, a seamless upgrade may be difficult to accomplish.

**64-bit products:**

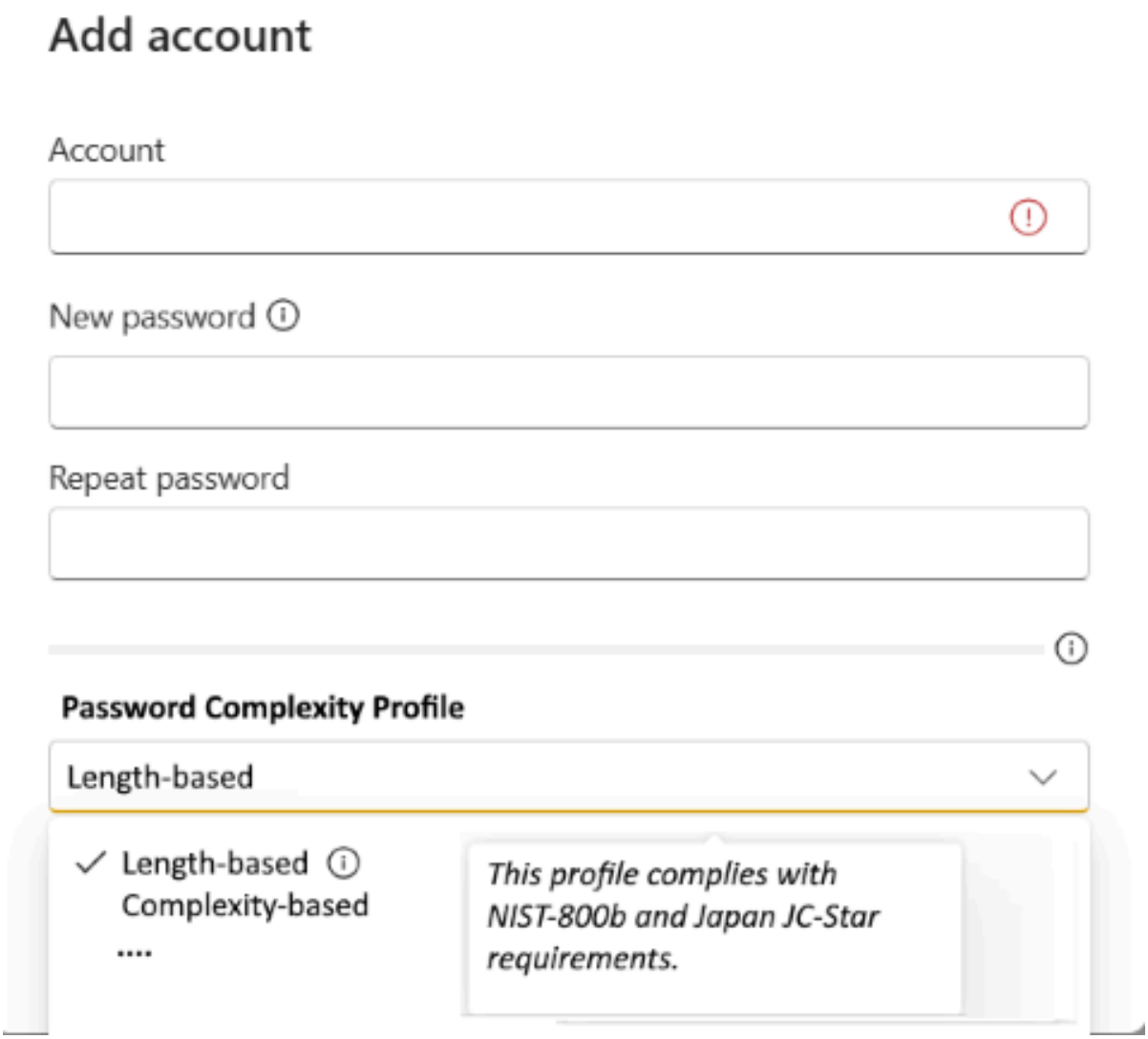
- ACAP applications compatible with AXIS OS 13 can run on AXIS OS 12, making the upgrade process smoother.

**Affected products (32-bit that will get AXIS OS 13):** AXIS A1210/-B, AXIS A1214, AXIS A1610/-B, AXIS A1710-B, AXIS A1711, AXIS A1810-B, AXIS A1811, AXIS A9210, AXIS C1210-E, AXIS C1211-E, AXIS C1510, AXIS C1511, AXIS C1610-VE, AXIS C8110, AXIS C8210, AXIS F9104-B, AXIS F9111, AXIS F9114/-B, AXIS I8016-LVE, AXIS M3057-PLR Mk II, AXIS M5000/-G, AXIS M5074, AXIS M5075/-G, AXIS M7104, AXIS M7116, AXIS P3925-LRE, AXIS P3925-R, AXIS P3935-LR, AXIS AXIS P5654-E, AXIS P5654-E Mk II, AXIS P5655-E, AXIS P5676-LE, AXIS P7304, AXIS P7316, AXIS Q6074/-E, AXIS Q6075/-E/-S/-SE, AXIS Q6078-E, AXIS Q6135-LE, AXIS Q6225-LE, AXIS Q6315-LE, AXIS Q6318-LE, AXIS Q8615-E, AXIS Q8752-E & Mk II, AXIS V5925, AXIS V5938, D201-S XPT Q6075 and ExCam XPT Q6075.

## Security

- **Password complexity enforcement**
  Password complexity enforcement is considered best practice when managing account credentials. Axis will introduce the option to enforce password complexity in an upcoming AXIS OS 12 release. Starting

with AXIS OS 13, password complexity enforcement will be enabled by default for new/edited accounts created via SSH, VAPIX, ONVIF and SNMP profile selection—and this behavior cannot be disabled. This change also applies to the web interface
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



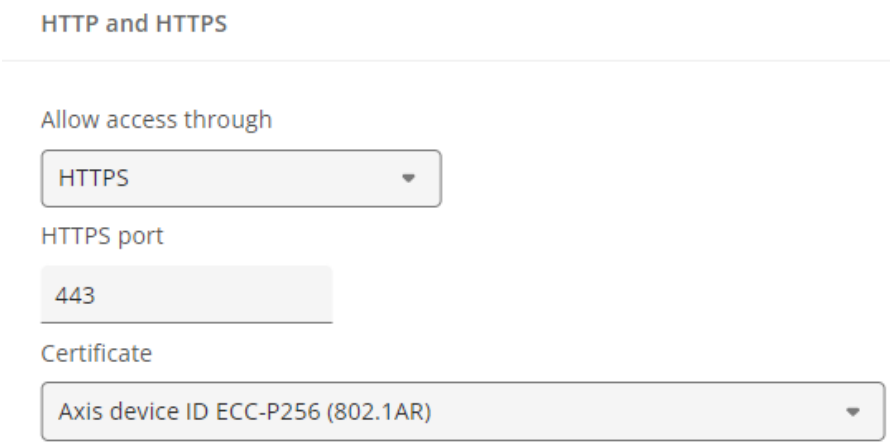

**On upgrade or after a factory default:** This change will affect upgrades and the factory defaulted state. For upgrades, only new/edited accounts created after the upgrade need to meet password complexity requirements. Existing accounts will not be considered and need to be adjusted manually.
**Reason 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.
**To comply with the following regulations and certifications:** France ANSSI CSPN, Spain Lince CPSTIC, Japan JC-Star level 3 and higher, South Korea NIS, E.U. CRA, Singapore CLS level 3 and higher

| 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 |

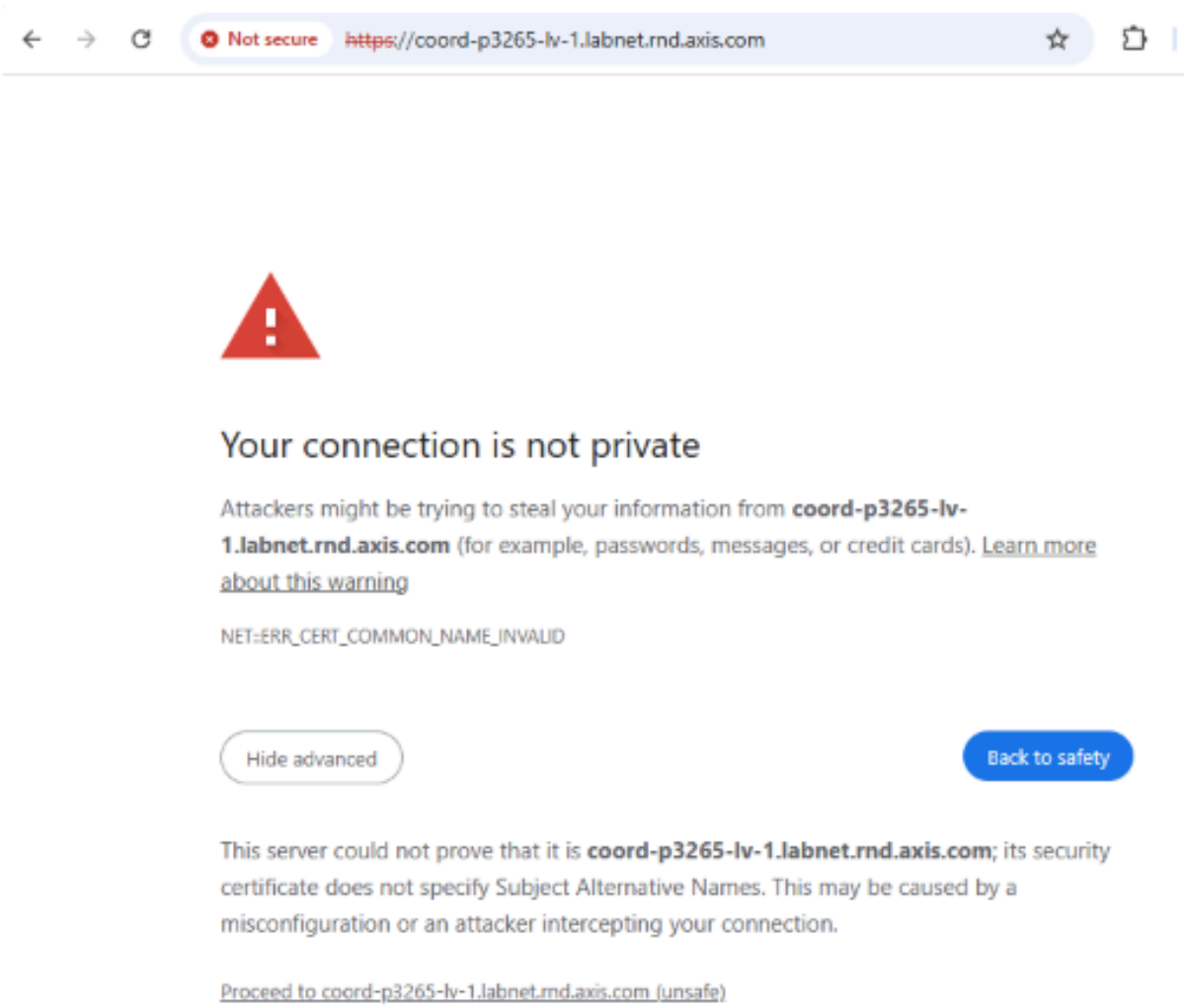
*Actual rate may vary and is depending on product performance.

**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.

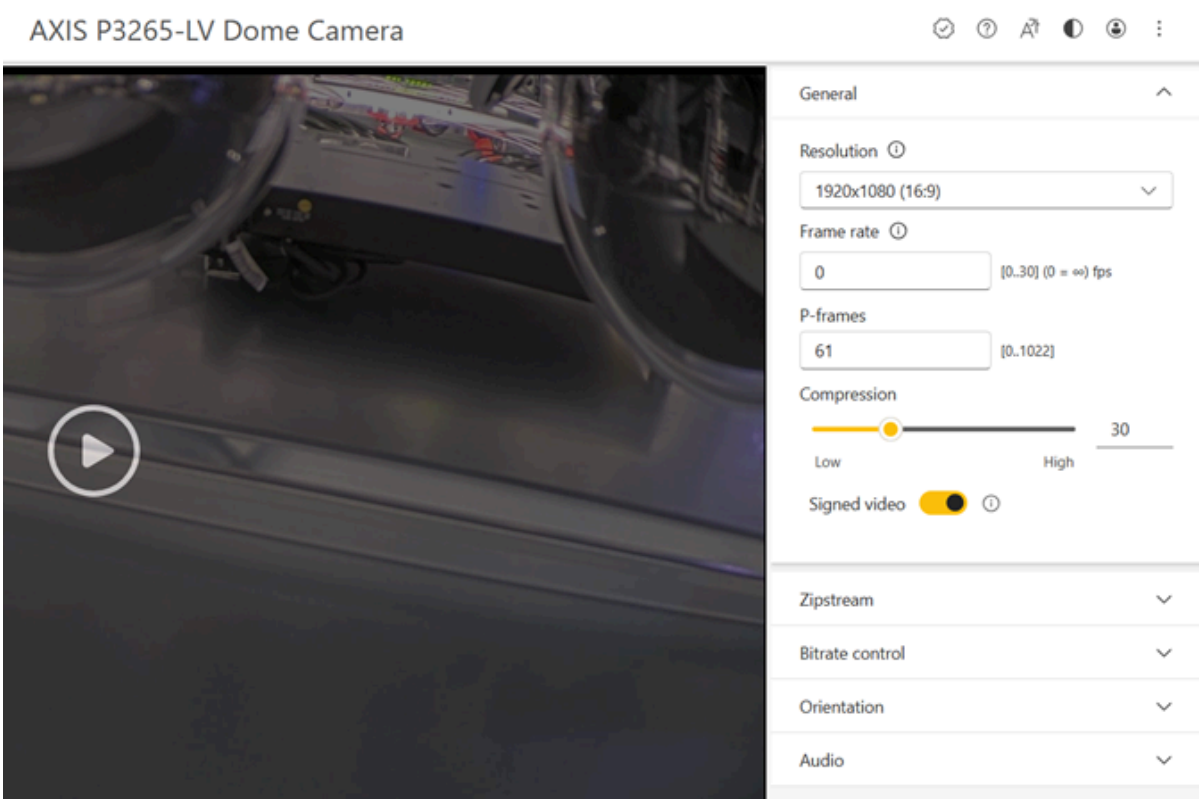



**On upgrade or after a factory default:** After a factory default.
**Reason for change:** To increase the overall device security following the secure-by-default strategy and reduce the hardening guide configuration steps for the user.
**To comply with the following regulations and certifications:** Japan JC-Star level 3 and higher, South Korea NIS, E.U. CRA, Singapore CLS level 3 and higher.
**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.I0.MPEG.SignedVideo.Enabled=no
To:
Image.I0.MPEG.SignedVideo.Enabled=yes

- **Removal of UPnP Discovery**
  UPnP Discovery has been disabled since AXIS OS 12.0 and onwards to lower the network attack service, increase overall security of the device and to reduce hardening guide configuration steps for the user. Since then, the preferred device discovery method is Bonjour which allows for device detection within the local subnet where the device is located (example: 192.168.1.0/24). Now UPnP will be removed completely as a feature from AXIS OS.
  **On upgrade or after a factory default** On upgrade.
  **Reason for change:** Axis considers Bonjour to cover all device discovery use cases and therefore UPnP is seen as obsolete. Removing UPnP will also shorten the hardening guide as users do not need to take UPnP further into account.
  **The impacts:** If UPnP is used in production after initial device deployment and configuration, upgrading to AXIS OS 13 and higher will make the device not discoverable via UPnP.
  **Affected VAPIX parameters:**
  The following parameter will be removed: Network.UPnP.Enabled

- **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.
**The impacts:** 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

- **Prevent Stack Execution**
  Starting in AXIS OS 13, the Linux kernel will block any process that has its stack marked as executable. This type of setup is very uncommon and typically only occurs by mistake. If a process with an executable stack tries to run, it will crash immediately with a segmentation fault (SIGSEV), and the kernel log will show an error such as: `not starting process [PROCESS] with executable stack`
  For more information: *https://wiki.gentoo.org/wiki/Hardened/GNU_stack_quickstart*
  **On upgrade or after a factory default:** On upgrade.
  **Reason for change:** Allowing executable stacks makes it easier for attackers to exploit memory vulnerabilities such as buffer overflows. By enforcing non-executable stacks, AXIS OS further strengthens system security and reduces the risk of such exploits. All internal AXIS OS components are already built with non-executable stacks, so this change mainly acts as an additional safeguard.
  **The impacts:** This change is not expected to affect normal device operation, as all AXIS OS components are already built with non-executable stacks. Most ACAP applications will continue to function without modification for the same reason. Only in rare cases—if an ACAP was previously compiled with an executable stack—it will fail to start after the upgrade. In such cases, the application must be recompiled with a non-executable stack. No special actions are required for integrators unless they are using custom-built ACAPs with unusual build configurations.

- **Removal of TLS 1.0/1.1 for SIP-communication (UPDATED! Already removed in 12.10)**
  In AXIS OS 12.10 we have updated to OpenSSL 3.5.5 to increase overall cybersecurity, addressing one high-severity, two medium-severity, and seven low-severity issues. OpenSSL 3.5.5 do not support TLS 1.0/1.1 and therefor the breaking change has taken place in AXIS OS 12.10 already.
  **Note:** In the factory default state TLS 1.0/1.1 SIP communication is no longer supported as the use of RSA 1024-bit keys is prohibited. It does not affect upgrades, to maintain backwards compatibility.
  **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**: Third-party SIP clients or servers that only support TLS 1.0/1.1 will no longer work with Axis products that require TLS 1.2/1.3.

## API changes

- **Updated Recording System**
  The AXIS OS Recording system has been re-implemented and is mostly fully backward compatible, except for the changes listed below.
  **On upgrade or after a factory default:** On upgrade.
  **Reason for change:** Improves the optimization of video cache and RAM consumption, but also added more features. Enables simultaneous recording for both cloud and local storage.

  1. **Multiple recording ids**
     In the recording system a recording id is used to identify a sequence of recorded media. The number of recording ids and the length of the sequence they identify will change with the new recording system.
     **Existing recording system:** A recording id has no upper limit on the length of the recording sequence it identifies. For a continuous recording a new recording id will only be generated at the start of the recording, for example at boot.
     **New recording system:** A recording id is time restricted to maximum 24 hours, (1 hour default). An ongoing recording can thus span over multiple recording ids. As default for a continuous recording there will thus be 24 recording ids during a day.
     Note that this behavior is not limited to continuous recordings, as triggered recordings can also run for extended periods depending on the trigger.
     1.1. The axis-cgi/record/list.cgi API is used to list recording ids and this will thus return more ids than before. To identify if two sequential recording ids are part of the same recording sequence the start and stop time of each id can be compared. If the stop time of the first recording id is identical to the start time of the second, then these two recording ids are both part of the same recording sequence.
     1.2. The axis-cgi/record/export/exportrecording.cgi API is used to export parts of a recording sequence. Currently this API can only export recorded media belonging to a single recording id. To make it easier to export longer recording sequences in the new recording system this API will be extended so that the stop time given in the API call may extend into trailing recording ids.
     1.3. Same as for export.cgi, RTSP playback is performed on one recording id only.

  2. **Time stamps in H.264 header.**
     As described here, the monolith can be configured to insert product information and timestamps into H.264 header data *here*. This feature is not currently implemented in the new recording system.

  3. **Removing ongoing recordings**
     The axis-cgi/record/remove.cgi API can be used to remove one or more recordings.
     **Existing recording system:** If trying to remove an ongoing recording the recording would first be stopped and then removed.
     **New recording system:** Trying to remove an ongoing recording will result in an error reply. The caller is expected to stop a recording before removing it.

  4. **Recording files have changed location and format on disk**
     Accessing the recording files directly on disk has never been publicly supported. Due to lack of public API's for ACAPs we are aware though that some partners has done this anyway. It is therefore worth mentioning that all recording files have moved to new a location on disk and are using a new naming scheme and different format.
     Any ACAP needing access to recording files shall do that via the public DBUS API's that have been available since AXIS OS 11.11 however documentation is missing at the moment. We will update this text as soon as they are a public.

  5. **RTSP "failoverrecordinglength=<duration>" no longer supported**
     With the URL option "failoverrecordinglength", the camera would automatically start a recording on the camera if an RTSP session got timeout. For clients the following will change:
     * "failoverrecordinglength" URL option will be ignored.
     * RTSP GET_PARAMETER for parameter "Failover-Recording-ID" will result in 451 Parameter Not Understood.

6. **EstimatedFileSize property is removed**
   In the axis-cgi/record/export/properties.cgi CGI belonging to the *Export Recording API*, the EstimatedFileSize property is removed from the response.

- **Removal of deprecated functions in VDO**
  Crop Settings isn't intended for ACAPs and has been deprecated since 11.11. The functions vdo_buffer_is_complete, vdo_frame_get_fd, and vdo_frame_get_opaque have been deprecated since 10.12.
  **On upgrade or after a factory default:** On upgrade.
  **Reason for change:** The deprecated functions in *libvdo* will be removed.
  **The impacts:** ACAP applications using these APIs may stop working after upgrade to AXIS OS 13.
  **Affected VAPIX parameters:** *libvdo: Deprecated List*

- **Removal of the statistics field from VDO Stream Info**
  The statistics fields in the VDO stream info map include framerate and other data for a VDO stream.
  **On upgrade or after a factory default:** On upgrade.
  **Reason for change:** The statistics field has been removed for maintenance reasons. Additionally, even when not actively used, the feature negatively impacts performance, making its removal beneficial overall.
  **The impacts:** If an ACAP uses the statistics fields in the VDO stream info, all retrieved values will be 0. The ACAP will still function except for the statistics. If an ACAP uses VDO, it will have all this information from the VDO stream it has started.
  **Affected VAPIX parameters:** *VDO stream info*
  The following VAPIX parameters will be removed:
  statistics.duration

  statistics.framerate

  statistics.bitrate

  statistics.frame_count

  statistics.idrframe_count

  statistics.bit_count

  statistics.failed_frames

  statistics.accumulated_bytes

  statistics.accumulated_idrbytes

- **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.Various.V#.HomePresetSet VAPIX API**
  The PTZ.Various.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

- **Removal of ptzcoordcalc.cgi VAPIX API**
  The ptzcoordcalc.cgi VAPIX was used to transform picture coordinates to and from pan/tilt coordinates.
  **On upgrade or after a factory default:** On upgrade.
  **Reason for change:** The ptzcoordcalc.cgi VAPIX API is not used anymore and considered obsolete.
  **The impacts:** This API and its parameters were officially never documented nor supported so no immediate impact would be expected.

- **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.ReferrersEnabled
  Image.Referrers
  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.

- **Update receive.cgi API for HTTP/1.1 Compliance (NEW!)**
  The change routes receive.cgi through the Apache server, which applies chunked transfer coding. This means the data will now be sent as a sequence of length-delimited buffers.vSee *RFC 9112 7.1* for more information.
  **On upgrade or after a factory default:** On upgrade.
  **Reason for change:** This change ensures compliance with HTTP/1.1 and supports improved security, high availability, load balancing, and centralized authentication and authorization.
  **The impacts:** Clients relying on static parsing of the data will require updates to align with the Chunked Transfer Coding handling described in RFC 9112.
  **Affected VAPIX parameters:** It is a behavioral change.
  Example usage with httptype singlepart - RFC 9110 15.3.7.1 - (implicit when no httptype option is given):
  http://<servername>/axis-cgi/audio/receive.cgi?audiocodec=g711&audiobitrate=64000&audiosamplerate=8000
  This currently gives the following respons header:respons header (along with the first part of the message body):
  HTTP/1.0: 200 OK
  Cache-Control: no-cache
  Pragma: no-cache
  Expires: Thu, 01 Dec 1994 16:00:00 GMT
  Connection: close
  Content-Type: audio/basic
  .....}xsomkigeca_^^]\\\[ZZYYXXXXWWWWWWWWWXYYYZZ
  With the change the respons header will look as follows (**updates in bold**):
  **HTTP/1.1** 200 OK
  **Date**: Mon, 17 Nov 2025 14:24:45 GMT
  **Server**: Apache/2.4.65 (Unix) OpenSSL/3.0.18
  **X-Content-Type-Options**: nosniff
  **X-Frame-Options**: SAMEORIGIN
  **X-XSS-Protection**: 1; mode=block
  **Content-Security-Policy**: default-src 'self'; frame-ancestors 'self'; connect-src 'self' https://*.google-analytics.com https://*.analytics.google.com https://*.googletagmanager.com https://*.axis.com mediastream: blob:; script-src 'self' https://*.googletagmanager.com https://www.google-analytics.com https://ssl.google-analytics.com https://*.axis.com; style-src 'self' 'unsafe-inline'; img-src 'self' https://*.google-analytics.com https://*.googletagmanager.com https://*.axis.com data: blob:; media-src 'self' mediastream: blob:; object-src 'none'
  **Referrer-Policy**: strict-origin-when-cross-origin
  Cache-Control: no-cache
  Pragma: no-cache
  Expires: Thu, 01 Dec 1994 16:00:00 GMT
  Content-Type: audio/basic
  **Keep-Alive**: timeout=5, max=99
  **Connection**: Keep-Alive
  **Transfer-Encoding**: chunked
  **1fd**
  fWXXXZ[\^aehkmoqsvxz~.....\{vsomkigeb`_^]\\
  \[ZYYXXWWWWWWWWWWXXXYYYZ[\\]]]\\\\\\\\\]]]]{}{}{}
  ````abcegjms~.....}wtqnkgeca_{^}
  [ZZYYXWVVUUUUUTTTTTTTUUUUVVWWWWXXYZZ[]_cfiloquwz}.....
  **200** .....}wqljigdb`_]]
  [ZZYXXWWVVUUUUUTUUTTTTTTUUVVVVWWXXYYYZ[]^``dgknruyz Unknown macro:
  {.....} xsqnkhfeb`_]\\\[ZZYYYXXXXXXWWWWXXXYYYZZZ
  [[\\\\]adgkov{.....}xtqnljgeca_]]
  [[[ZZYYYYXXXXXXXXXXXYYYZ[[ ]|file:///]^_behlqy.....
  **200**
  ````

Example usage with httptype multipart - RFC 9110 15.3.7.2 - http://<servername>/axis-cgi/audio/receive.cgi?httptype=multipart&audiocodec=g711&audiobitrate=64000&audiosamplerate=8000
This currently gives the following respons header (along with the first part of the message body):
HTTP/1.0 200 OK
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Dec 1994 16:00:00 GMT
Connection: close
Content-Type: multipart/x-mixed-replace; boundary=myboundary
–myboundary
Content-Type: audio/basic
Content-Length: 509
.....}}}}|}}|{}||}~}}}{|{z
{||||{|||{{{|{{{{{||{zyzzzzzy{zz{{{yyz|zyzzyzzyyyyyyzz{{{zyyzxzyyxxxwwxzzzyyyyyyzxwy
{zxzyyyzyxxyyxyyxzwxyxxyyyywx{yyyxxyyzzzzz|{zyyyzzyz{{z{{zzz{{yyzyz{zzzzzyyzzz{zzzz{zzzzz{{yy
{|{{{{{zzyzyz{{yzzzz{{{{zzzyzz{{{z{|{{||||
Unknown macro: {|}
zy{}|{|{||}}||}}{}}|{{||}}||{||{|}}..|{}}|||..}}....}}|{|}{}{}{}{}{}}}}.}....{}{}.....{~}...
–myboundary
Content-Type: audio/basic
Content-Length: 512
With the change the respons header will look as follows (**updates in bold**):
**HTTP/1.1** 200 OK
**Date**: Mon, 17 Nov 2025 14:26:07 GMT
**Server**: Apache/2.4.65 (Unix) OpenSSL/3.0.18
**X-Content-Type-Options**: nosniff
**X-Frame-Options**: SAMEORIGIN X-XSS-Protection: 1; mode=block
**Content-Security-Policy**: default-src 'self'; frame-ancestors 'self'; connect-src 'self' https://*.google-analytics.com https://*.analytics.google.com https://*.googletagmanager.com https://*.axis.com mediastream: blob:; script-src 'self' https://*.googletagmanager.com https://www.google-analytics.com https://ssl.google-analytics.com https://*.axis.com; style-src 'self' 'unsafe-inline'; img-src 'self' https://*.google-analytics.com https://*.googletagmanager.com https://*.axis.com data: blob:; media-src 'self' mediastream: blob:; object-src 'none'
**Referrer-Policy**: strict-origin-when-cross-origin
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Dec 1994 16:00:00 GMT
Content-Type: multipart/x-mixed-replace; boundary=myboundary
**Keep-Alive**: timeout=5, max=99
**Connection**: Keep-Alive
**Transfer-Encoding**: chunked
**40**
–myboundary
Content-Type: audio/basic
Content-Length: 509
**1fd**
.....|wsomjgeb`{}^]]]] [[\]]]{}^{}`abbcddeefgggghikmou
{.....|}}}}|||{zzzzyzyz||~.....|vqnlkihfdb`{_}]
[[ZZYXWWVVVUUUUUUUUUUUVVVWWXYYZZ[[\]
^adhknqvy}.....~wqmkhfca_]]
[ZYYYXXXWWVVVVWWWWWWWWWXXYZZZ\\]^^__acfimqw|.....
**2**

- **Removal of legacy privacy mask type parameter**
  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:** This parameter may currently be used by some partners to determine whether a product supports privacy masks when onboarding devices into their systems. However, it is no longer relevant to the masking functionality, and its value is no longer evaluated. Partners should instead use the parameter root.Properties.PrivacyMask.PrivacyMask to identify privacy mask support:

**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 parameter will be removed:Image.PrivacyMaskType

- **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.NTCIP.Enabled
  SNMP.Trap.Enabled
  SNMP.Trap.T0.Address
  SNMP.Trap.T0.Community
  SNMP.Trap.T0.AuthFail.Enabled
  SNMP.Trap.T0.ColdStart.Enabled
  SNMP.Trap.T0.LinkUp.Enabled
  SNMP.Trap.T0.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 (UPDATED!)**
  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.
  Additional impact: The parameters are also used to control the RTSP and RTSPS server authentication mode. By removing these parameters, clients will no longer be able to configure the authentication modes. Instead, the authentication mode will be hardcoded as follows:

| Protocol | Policy | qop |
|---|---|---|
| RTSP | Digest | qop=auth |
| RTSPS | Basic | - |

  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 (Cancelled)**
  Decision to keep existing API. We will communicate any upcoming changes to list.cgi following the AXIS OS lifecycle on the Active and LTS tracks.

- **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

- **Removal of record.cgi & stop.cgi**
  The *record.cgi & stop.cgi* will be removed since alternative recording methods are available.
  As replacement API, clients have two options. To set up a *recording using the event system* or use *record/continuous/addconfiguration.cgi* .
  **On upgrade or after a factory default:** On upgrade.
  **Reason for change:** We believe these legacy APIs are not widely used. This change aims to unify recording methods. Additionally, these legacy APIs are not persistent after a reboot, causing recordings to stop if the camera restarts or encounters a problem.
  **The impacts:** The old method of starting/stopping recordings will not work with AXIS OS 13.
  **Affected VAPIX parameters:**
  The following APIs will be removed from the Edge Storage API:
  record.cgi
  stop.cgi
- **Changes in param.cgi parameter configuration of the Storage group**
  Legacy parameters will be removed and this change aims to streamline storage device configuration. After the removal only the following parameters of the group will remain:
  Storage.Sn.DiskID, Storage.Sn.Enabled, Storage.Sn.ExtraMountOptions, Storage.Sn.FriendlyName and Storage.Sn.MountOnBoot
  **On upgrade or after a factory default:** On upgrade.
  **Reason for change:** We believe these legacy parameters are not widely used. This change aims to streamline storage device configuration, increasing simplicity and consistency.
  **The impacts:** The old configuration method will not work with AXIS OS 13.
  **Affected VAPIX parameters:**

| Removed | Replaced by |
|---|---|
| Storage.MountDir | N/A |
| Storage.Sn.AutoRepair | Running disk repair automatically at mount is needed for robust filesystem operation. Is skipped if disk is locked, see below for locked. Manual repair in *disks/repair.cgi*. |
| Storage.Sn.CleanupLevel | CleanupLevel is an obsolete, since FW 5.50, parameter and have no effect. Read in cleanuplevel in *disks/list.cgi*. |
| Storage.Sn.CleanupMaxAge | Read in cleanupmaxage in *disks/list.cgi* and update in *disks/properties/setcleanupmaxage.cgi*. |
| Storage.Sn.CleanupPolicyActive | Read in cleanuppolicy in *disks/list.cgi* and update in *disks/properties/setcleanuppolicy.cgi*. |
| Storage.Sn.DeviceNode | Internal information about where to find the hardware, set at build time. |
| Storage.Sn.FileSystem | *disks/getcapabilities.cgi* |
| Storage.Sn.Locked | *disks/lock.cgi* |
| Storage.Sn.MountPointPermissions | Set at FW build time to allow services more access to storage. Examples are Body Worn (BW) cameras where a BW service uploads recordings to System Control Unit (SCU) and recorders, like S3008, where the NetworkShare server needs direct access to storage. |
| Storage.Sn.MountPointPermissions | Read in requiredfilesystem in *disks/list.cgi* and update in *disks/properties/setrequiredfs.cgi*. |

- **Removal of legacy parameter audiooutput from Media clip API**

Support for legacy parameter audiooutput will be removed from Media clip API. More information can be found in *VAPIX Library*.
**On upgrade or after a factory default:** On upgrade.
**Reason for change:** audiooutput has been deprecated since November 2023 and is not used anymore. audiooutput has been replaced with audiodeviceid and audioouputid.
**The impacts:** Using audiooutput will not work with AXIS OS 13.
**Affected VAPIX parameters:**
The following parameters will be removed from the Media Clip API:
audiooutput

- **Removal of tenBandGraphicDspEqualizer from Audio mixer API**
  The Audio mixer plugin "tenBandGraphicDspEqualizer" will be replaced by "tenBandGraphicEqualizer" on network speaker products. See the *VAPIX Library* for further information on the API.
  **On upgrade or after a factory default:** On upgrade.
  **Reason for change:** Reduce complexity for clients where equalizer plugin has different name between network speakers and cameras, so simplifying by harmonizing the plugin name by replacing "tenBandGraphicDspEqualizer".
  **The impacts:** The Audio mixer plugin tenBandGraphicDspEqualizer is not supported in AXIS OS 13.

- **Removal of File Upload VAPIX API**
  The file upload VAPIX API is a legacy feature from version 5.60, which allowed users to upload custom web content in *AXIS OS web version A (Classic)*. Since the introduction of *AXIS OS web version B* in 2017, uploading custom web content has not been supported.
  **On upgrade or after a factory default:** On upgrade.
  **Reason for change:** The File Upload VAPIX API has been considered obsolete since 2017, as its use case for uploading custom web content has been replaced. Since then, ACAP applications have taken over the functionality of providing custom web content. This change further increases cybersecurity robustness by removing a way to upload files or content onto the device, and more appropriate solutions for this use case are now available.
  **The impacts:** Client applications that have implemented these APIs and expect them to be available in AXIS OS 13 may stop working or display error messages indicating that file content management was unsuccessful.
  **Affected VAPIX parameters:**
  The following VAPIX APIs will be removed:
  upload_file.cgi
  local_del.cgi
  local_list.cgi
  file_upload.cgi

- **Removal of legacy Properties.Image.Rotation, Properties.Image.I#.Rotation and Image.I#.Rotation parameters**
  Artpec-7 and newer products no longer support stream-specific rotation. You can now handle rotation globally using `ImageSource.I#.Rotation` and `ImageSource.I#.SourceRotation`. We temporarily retained the legacy parameters for backward compatibility. On Artpec-7 and newer products, any changes you make to these parameters are automatically mapped to the new parameters.
  **On upgrade or after a factory default:** On upgrade.
  **Reason for change:** AXIS OS 13 won't support Artpec-6 products. Since a replacement API has been available for some time, keeping the old parameters only causes confusion and increases maintenance complexity. Additionally, you can no longer reliably map legacy parameters for all channels, especially in multi-channel products that now include view area support.
  **The impacts:** A client that is expecting the VAPIX parameters and tries to configure them will most likely stop working or fail to do the wanted configuration.
  **Affected VAPIX parameters:**
  The following VAPIX APIs will be removed, note that I# could be I0, I1, I2 etc.. for products with multiple image/view sources:
  Properties.Image.Rotation
  Properties.Image.I#.Rotation
  Image.I#.Rotation
  More information about the Image Source Rotation can be found in the *VAPIX Library*.

- **Removal of "Camera Tampering" Detector**

The legacy Camera Tampering detector will be removed. Its functionality is replaced by AXIS Image Health Analytics, which provides more advanced and reliable capabilities.
**On upgrade or after a factory default:** On upgrade.
**Reason for change:** AXIS Image Health Analytics delivers superior performance and expanded capabilities compared to the old Camera Tampering detector, making the legacy feature redundant.
**The impact:** Tampering events via MotionRegionDetector/Motion will stop working. Switch to Image Health Analytics. **Note:** For products that do not support AXIS Image Health Analytics, a dedicated tampering event is introduced in AXIS OS 13 to ensure continued ONVIF Profile T compliance and basic tampering detection functionality.
**Affected VAPIX parameters:**
The API endpoint for the Camera Tampering detector will be removed. Specifically, the MotionRegionDetector/Motion event will no longer be available. For more information see the *VAPIX Library*.

- **Replacement of the Best Snapshot Configuration VAPIX API**
  The Best Snapshot API will be renamed to Object Snapshot API for alignment with established naming conventions.
  **On upgrade or after a factory default:** On upgrade.
  **Reason for change:** The name of the API will be changed to "object snapshot" to align with established naming conventions.
  **The impact:** Client applications that have implemented the API and expect it to be available in AXIS OS 13 may stop working or display error messages.
  **Affected VAPIX parameters:**
  The name of the API end-points will be replaced:
  From: /config/rest/best-snapshot
  To: /config/rest/object-snapshot

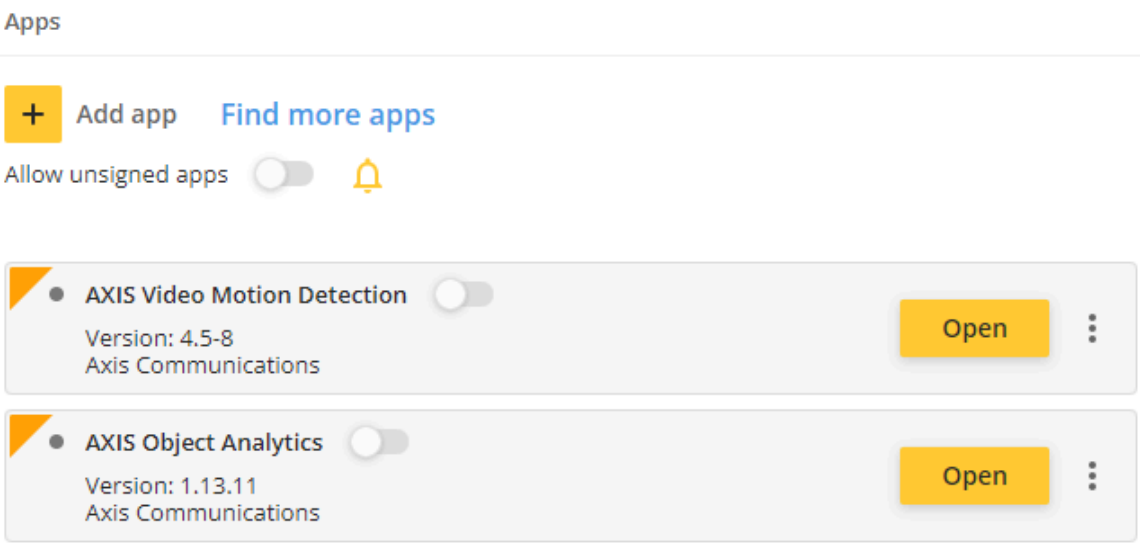
- **Changes to View Area VAPIX API (UPDATED!)**
  Today the view area service and digital ptz driver syncs their view areas/home preset position between each other. If the digital PTZ home position is updated, the view area service setting for the corresponding view area is updated accordingly, and vice versa. The parameter root.PTZ.Various.V#.Locked, where '#' is the channel number, has two function. It is used for enabling/disabling digital PTZ on a channel and it also updates the PTZ home position to the current position when set to true.
  **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 impact:** 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. Parameter root.PTZ.Various.V2.Locked will no longer update the PTZ home position when set to true. Its only function will be to enable/disable digital PTZ for a channel. Instead the channel will go back to the configured view area when digital PTZ is disabled.
  **Affected VAPIX parameters:**
  The parameters will not change but behavior will. Please read more in the *View Area API* documentation.

## ACAP applications

Note

If the upgrade fails, it may be due to an incompatible third-party ACAP application installed on the device. Remove the application and try again, or contact the ACAP vendor for further assistance.

- **Enforcement of ACAP signing**
  Starting with AXIS OS 13.0, unsigned applications are no longer permitted — only signed ACAP applications will be accepted.




ACAP applications are required to go through a signing process provided by the ACAP Portal on axis.com. The application archive and its signature will now be kept after installation so that the signature can be validated again after an OS upgrade. The proper upgrade path that will be recommended towards AXIS OS 13 is to go through AXIS OS 12 LTS (exact version TBD), re-install existing applications including re-doing their configuration and then perform the upgrade to AXIS OS 13.
**On upgrade or after a factory default:** On upgrade.
**Reason for change:**
— The user can be certain that the application has not been tampered with, be certain from whom the ACAP is provided and that a chain of authenticity is established since contact details from the ACAP portal are transparently available.
— An application cannot pretend to be another application (for instance, to steal its data) since the application identity can be checked by Axis before signing.
— Axis can inspect and approve the application's access rights before signing which will increase overall cybersecurity in AXIS OS and its devices.
— Pro-active communication regarding ACAP-related matters will be improved Axis can communicate given the contact details of each ACAP application from the ACAP Portal.
— Axis, its partners and individual ACAP developers will be meeting international legal requirements and best-practices when it comes to secure software delivery and code-signing.
**The impact:** Attempting to upgrade to AXIS OS 13 while having unsigned applications installed will trigger a rollback to ensure device safety.
**Affected VAPIX parameters:**
The following VAPIX parameters will be removed that were previous available to allow the installation of unsigned ACAP applications :
/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.

- **AXIS OS 13 Requires DLPU Usage Declaration in the ACAP Manifest**
  DLPUs in Axis products cannot serve different applications if the model is not optimized specifically for those applications. To improve the user experience, AXIS OS 13 requires DLPU usage declaration in the ACAP manifest. This will allow the WebGUI visualizations and server reports to present information about DLPU usage.
  **On upgrade or after a factory default:** On upgrade.
  **Reason for change:** To improve the user experience and show how the device performs.
  **The impact:** Your incompatible ACAP may stop working after an upgrade, or it may block the upgrade.

- **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**
  If an ACAP application contains a post-install script or a pre-uninstall script, the following rules will apply:
  · 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.

- **Enforcement of ACAP manifest schema v2**
  Starting with AXIS OS 13, ACAP applications must use **manifest schema v2** to declare their access rights. This requirement is enforced during mandatory ACAP signing, which is addressed separately as another breaking change.
  Applications will be restricted to run only as their own dynamically created user or as the sdk user — all other users are no longer permitted. Access will also be limited to a predefined set of system groups and D-Bus interfaces, aligned with officially supported APIs.
  **On upgrade or after a factory default:** On upgrade.

**Reason for change:** This enforcement prevents ACAP applications from bypassing AXIS OS security layers and is part of hardening the overall ecosystem. It also ensures that only officially supported APIs and libraries are used, leading to a more secure and consistent developer experience.
**The impact:** Devices with ACAPs that do not use manifest schema v2 will be blocked from upgrading to prevent them from entering an unsupported or broken state.

- **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 Larod version 1&2**
  The larod API is part of the the Native SDK and is used by ACAPs that want to use their own deep learning models for analytics.
  **On upgrade or after a factory default:** On upgrade.
  **Reason for change:** Streamlining and improving ACAP developer experience by only supporting the latest supported version of Larod. Reduced need for testing testing and reduced cost of maintenance.
  **The impact:** ACAPs and platform services that use version 1 and 2 of the Larod API will not work anymore. Those ACAP's will have to migrate to version 3 of the API. A migration guide is included in *the Larod documentation*. Migration is expected to be easy since the basic structure of the API hasn't changed.
- **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.
- **Removal of overlay enums from VDO ACAP API**
  Non-functional enums in the VDO ACAP API will be removed to improve ACAP API experience and avoid false expectations that these enums would be working. The complete list of enums that will be removed can be found *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:** No impact is expected, as the enums in this ACAP API have not been functional for a long time.
- **Message-Broker will be removed and replaced by Nexus**
  ACAP applications that use Message-Broker will no longer work starting with AXIS OS 13.0. The same data previously provided via Message-Broker will be available through the Nexus API in the same format. No VAPIX parameters will change. The new API is part of the ACAP SDK.
  **On upgrade or after a factory default:** On upgrade.
  **Reason for change:** Cleaning up the VDO ACAP API from legacy functionality that has not been functional since at least AXIS OS 10.12.
  **The impact:** Your incompatible ACAP application will stop working after the upgrade.
- **Removal of the ACAP applications AXIS Motion Guard, AXIS Fence Guard, AXIS Loitering Guard**
  The applications AXIS Motion Guard, AXIS Fence Guard, and AXIS Loitering Guard will be removed. Their functionality is replaced by AXIS Object Analytics.
  **On upgrade or after a factory default:** On upgrade.
  **Reason for change:** AXIS Object Analytics provides enhanced capabilities and a broader feature set.

**The impact:** Client applications that have implemented the ACAP application and their API and expect them to be available in AXIS OS 13 may stop working or display error messages.
**Affected VAPIX parameters:**
The APIs for the applications will be removed:
*Motion Guard*
*Fence Guard*
*Loitering Guard*

- **Removal of AXIS Removed object detection (NEW)**
  The legacy ACAP application AXIS Removed object detection will be removed. Its functionality will not be replaced.
  **On upgrade or after a factory default:** On upgrade.
  **Reason for change:** The legacy ACAP is considered obsolete and does not comply with the cybersecurity standards required in AXIS OS 13.
  **The impact:** Client applications that have implemented the ACAP application and their API and expect them to be available in AXIS OS 13 may stop working or display error messages.
- **Stop supporting the ability to install and run ACAPs on SD card (NEW!)**
  This is a beta feature that has never been officially supported or documented in the VAPIX documentation. For security reasons it will be removed in Axis OS 13. A rework is planned for the future.
  **On upgrade or after a factory default:** On upgrade.
  **Reason for change:** To enhance the security of the ACAP.
  **The impact:** It will not be possible to install or run an ACAP from an SD card in AXIS OS 13.

### 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.
- **Removal of SMB support for S30 and S40 series**
  SMB support will be removed from S30 and S40 devices. SMB is an older technology, and we now provide more scalable and robust alternatives through stream options and the new recording system.
  **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.

**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:** Newer and better option exist.
  **The impact:** Client applications that have been implementation based on SMB and expect it to be available in AXIS OS 14 may stop working or provide the user with error messages that the configuration was not successful.

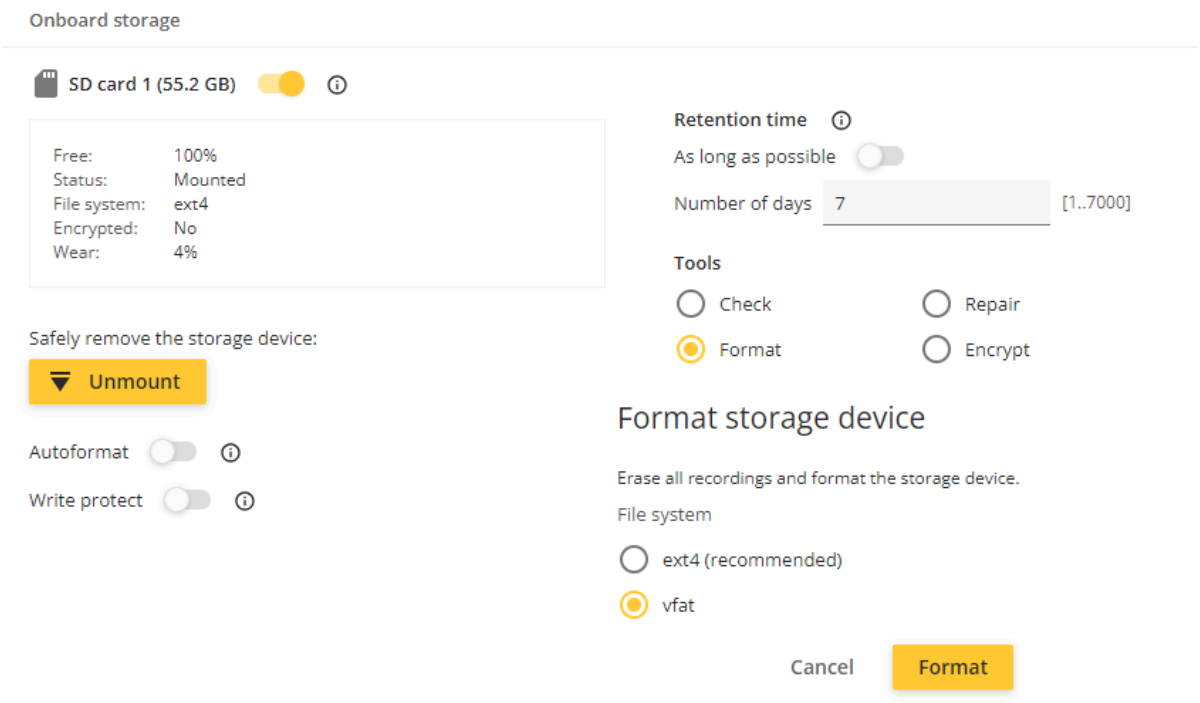
## Applied

### Changes in AXIS OS 12.1

**Edge Storage:**

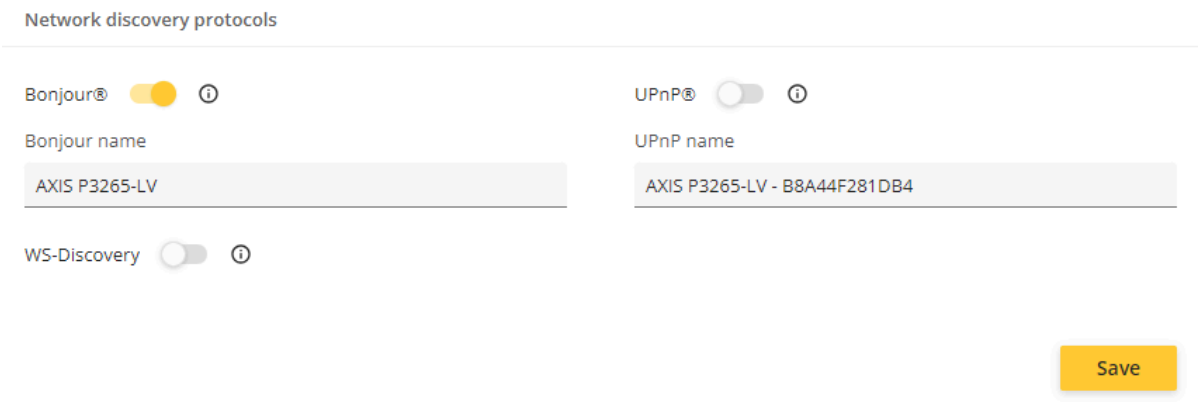
- **Removal of vFAT**
  The ability to format SD cards to the vFAT system file will be removed. However, they can still be used as before. A long time ago, SD cards were delivered with vFAT as the standard file system for cards up to 32GB. Since such SD cards are no longer used, the usefulness of vFAT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




**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




  **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.

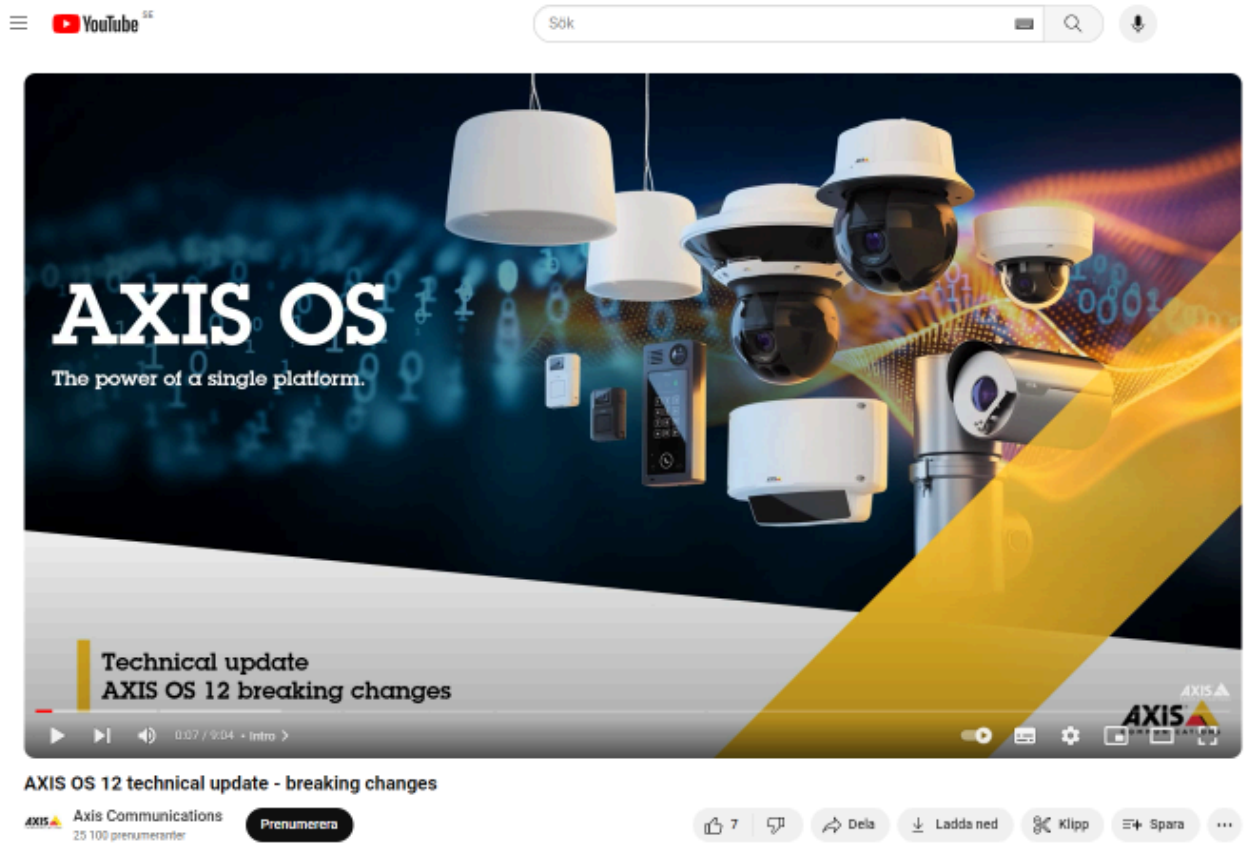
**Security:**

- **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



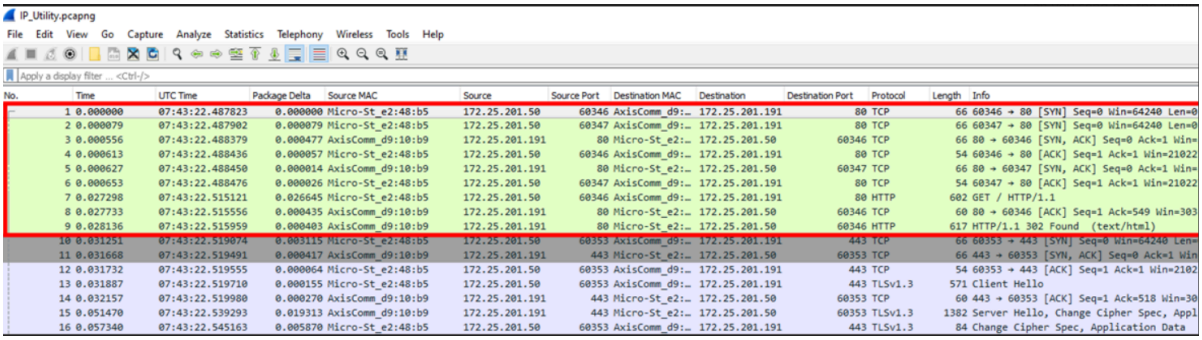

Check out the *AXIS OS 12 Technical Update - Breaking Changes* video, to learn more about the upcoming changes.

- **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.

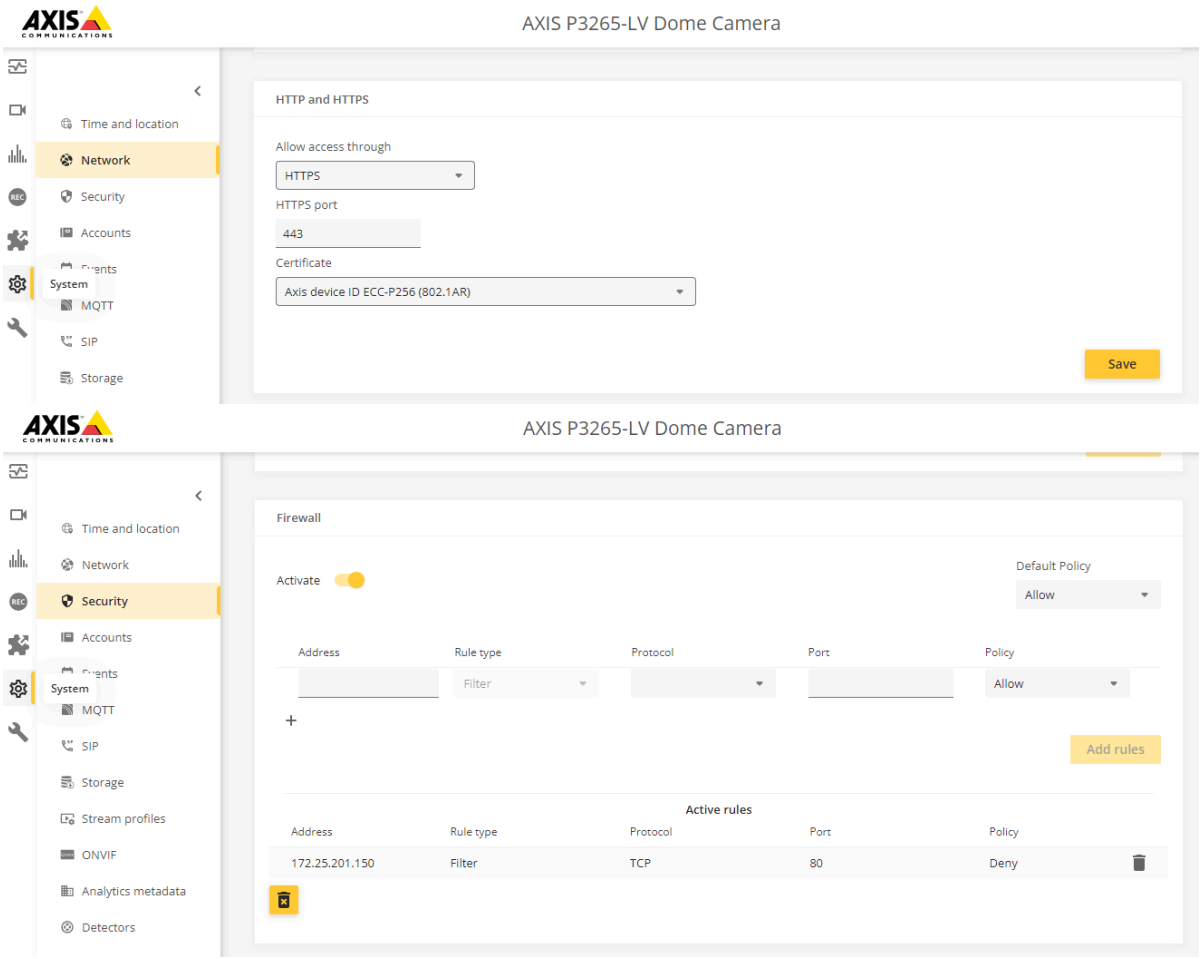
**Security:**

- **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.



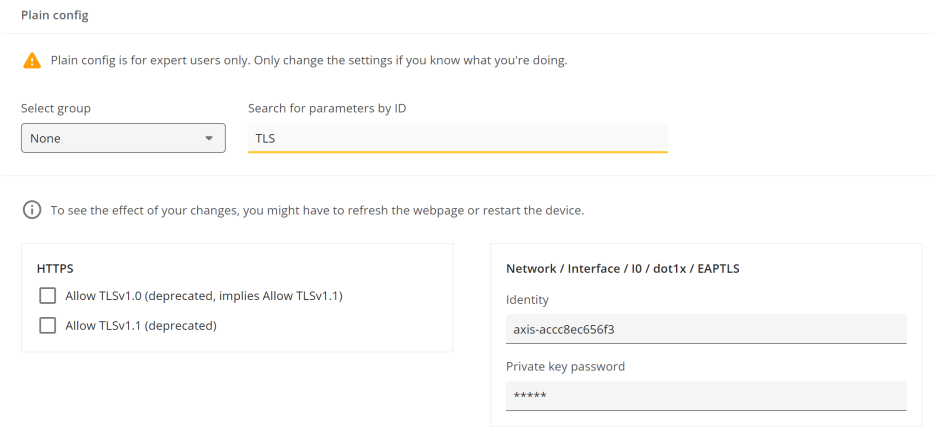

To test the possible impact, configure your Axis device for HTTPS only and configure a firewall rule in AXIS OS 11.9 as shown below, where the Axis device would effectively block communication on port 80 for a specific client trying to connect.




**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




**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.

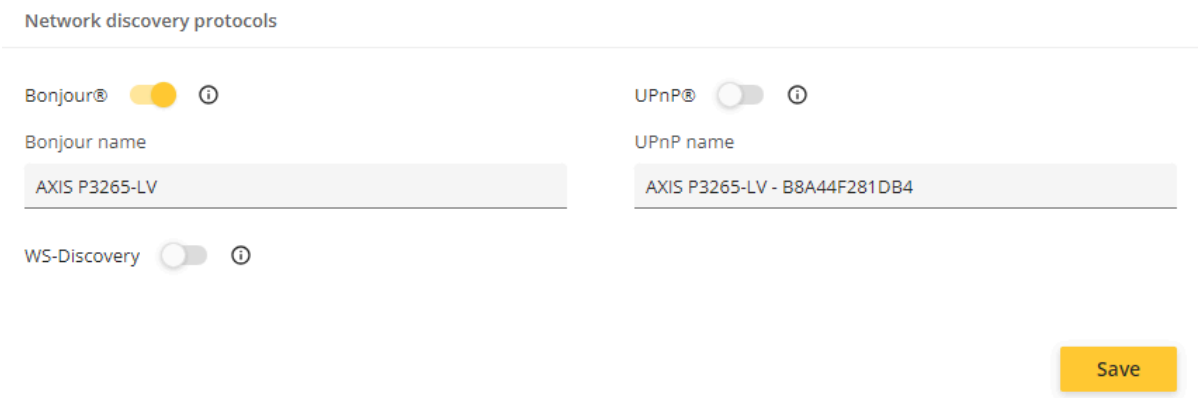
- **Removed support for OpenSSL 1.1.1**
  Since AXIS OS 11.6 (August 2023), Axis devices support simultaneously version 1.1.1 and 3.0 of the cryptographic software backend OpenSSL. To allow for smooth transition, OpenSSL 1.1.1 will still be supported until LTS 2024 track is launched and in that track. 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 adress 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




  **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.

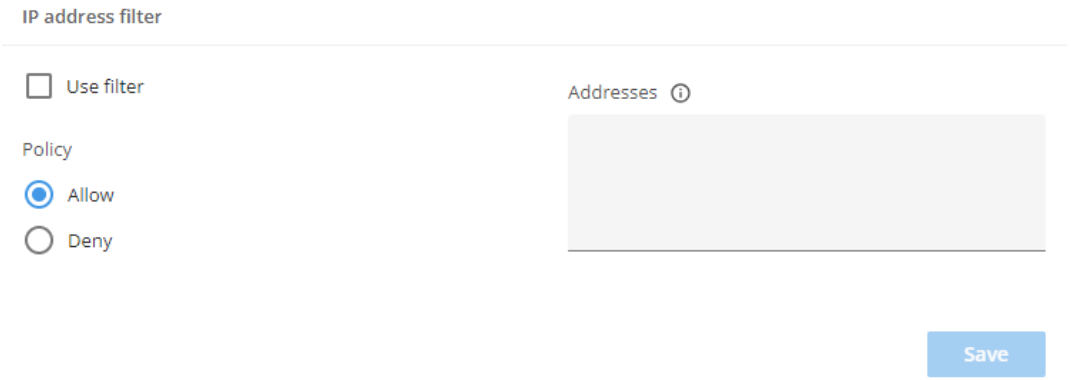
- **Possibility to disable Basic Device Info VAPIX API**The *Basic Device Information* VAPIX API allows to retrieve general information about the Axis product with no authentication. This is useful for device discovery and profiling during network and application onboarding. Axis will implement an additional 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.

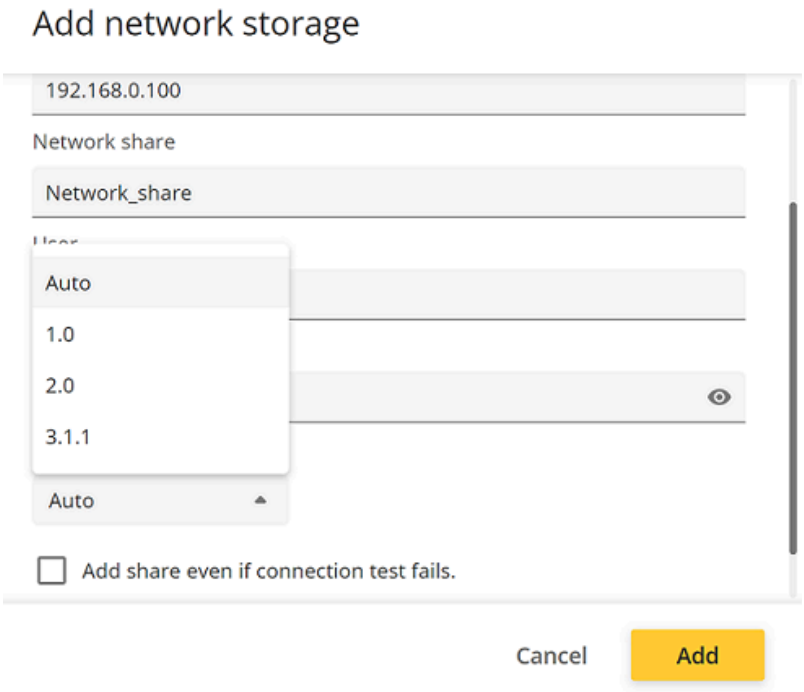
- **Removal of network filter API**
  The current IP-filtering VAPIX API will be replaced by a more feature-rich firewall application that can be configured through JSON REST API. The new firewall service will be available in AXIS OS 11.8 (January 2024) and can be used from there on.




  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.




**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.

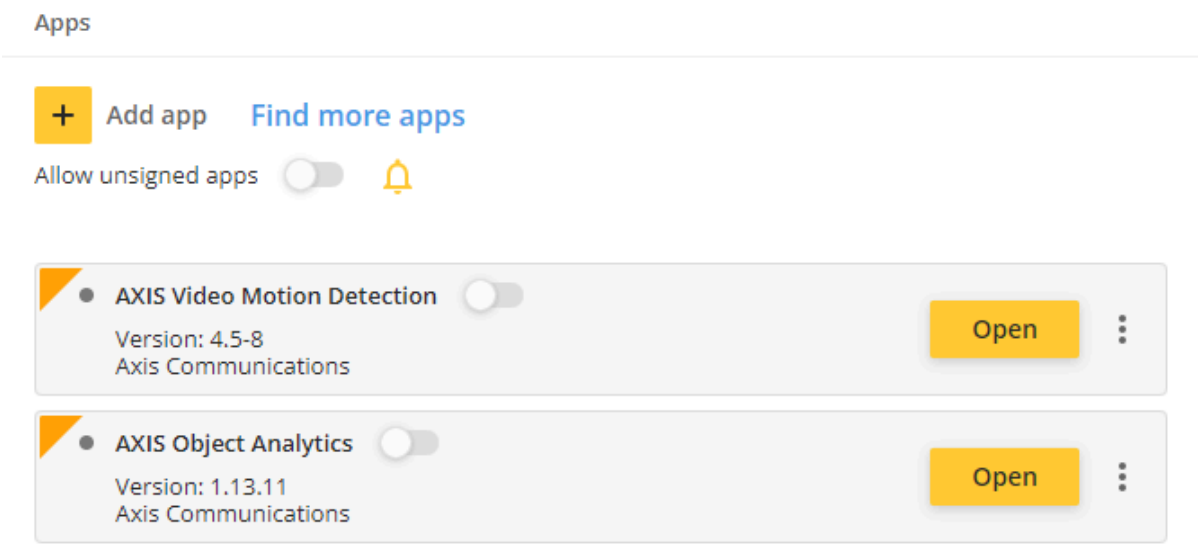
- **AXIS Perimeter Defender 3.6.0 required.** Versions 3.5.1 and earlier are not compatible with AXIS OS 12.0 or higher. Follow these *instructions* to perform the upgrade correctly.
- **AXIS License Plate Verifier 2.12.8 required.** Versions 2.8.4 or earlier are not compatible with AXIS 12 or higher.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




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

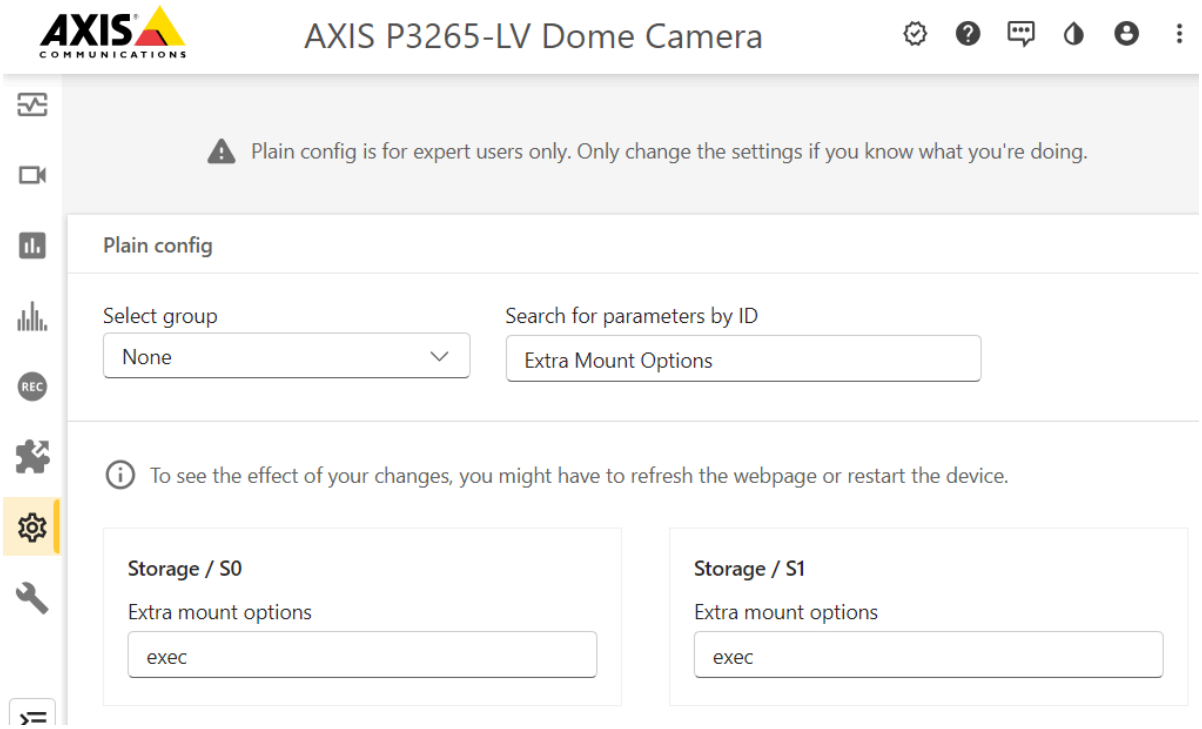
**Why is this change introduced?** Due to architectural changes.
**How can it affect me?** If you are using any of these ACAP applications, do not upgrade until the system has a verified replacer.

- **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.



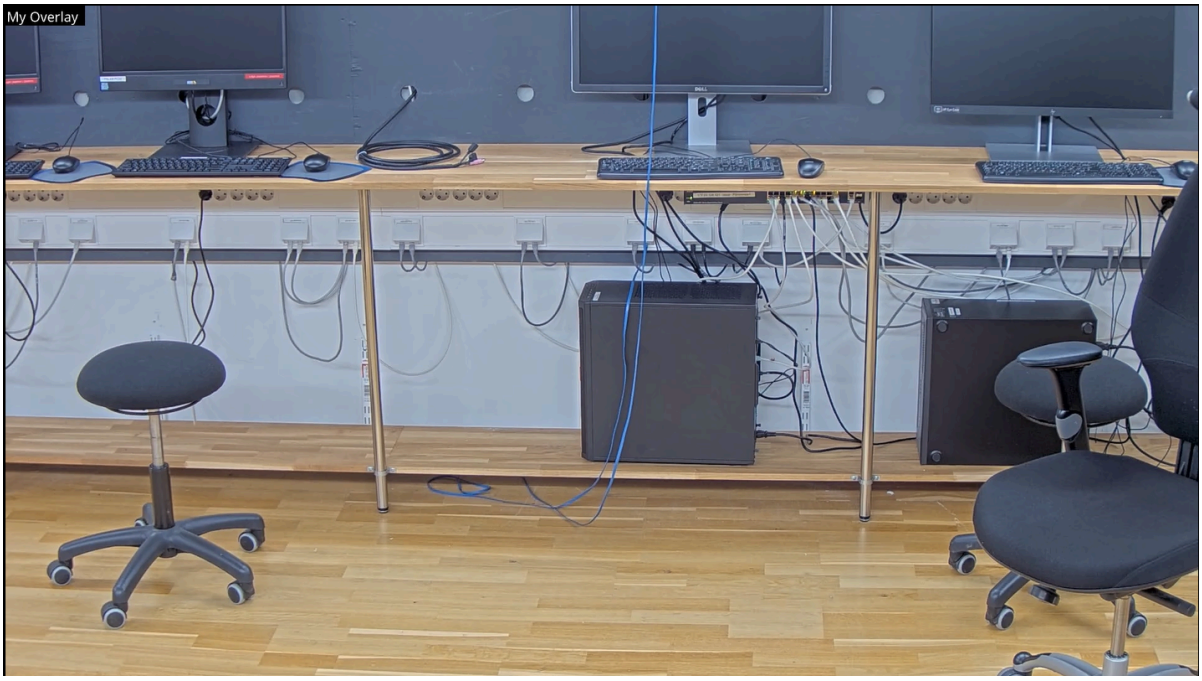
As a result of this change, in the factory default state of AXIS OS 12, file execution from edge storage is disabled and must be explicitly configured.
**Why is this change introduced?** To increase the security on the device.
**How can it affect me?** ACAP applications requiring file execution on edge storage may not function properly if the device is not configured accordingly.

**API changes:**

- **Rate Control changes for RTSP**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 *metadatastream.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.

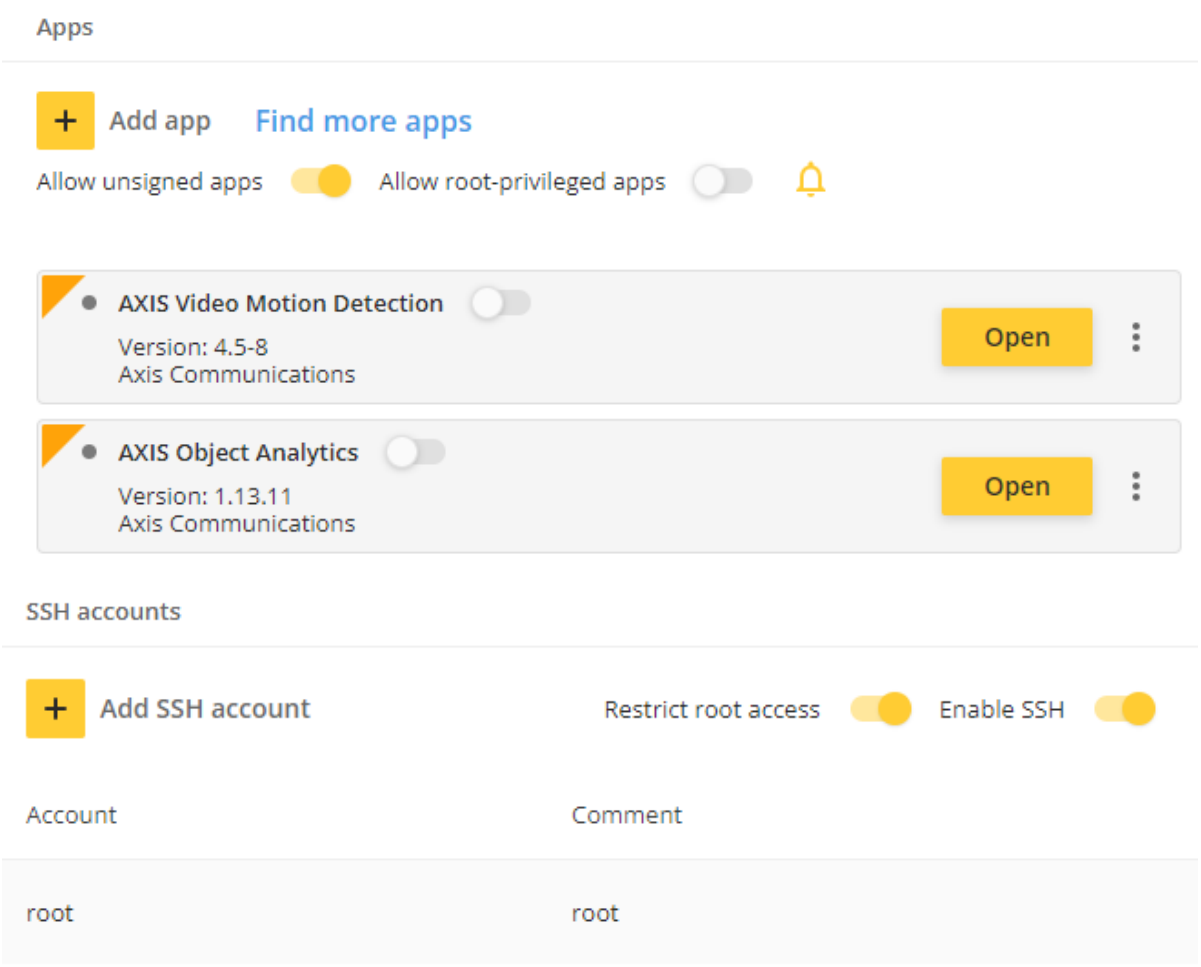
**Security:**

- **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:




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 | –<br>– |
| 11.6 | September 2023 | – |
| 11.8 | January 2024 | –<br>– |
| 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.<br><br>–<br>– |

**VAPIX API changes:**

- **PTZ VAPIX API version 2**

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*.

Information about current and other releases is available in the *AXIS OS release notes*.

### AXIS OS 12.10

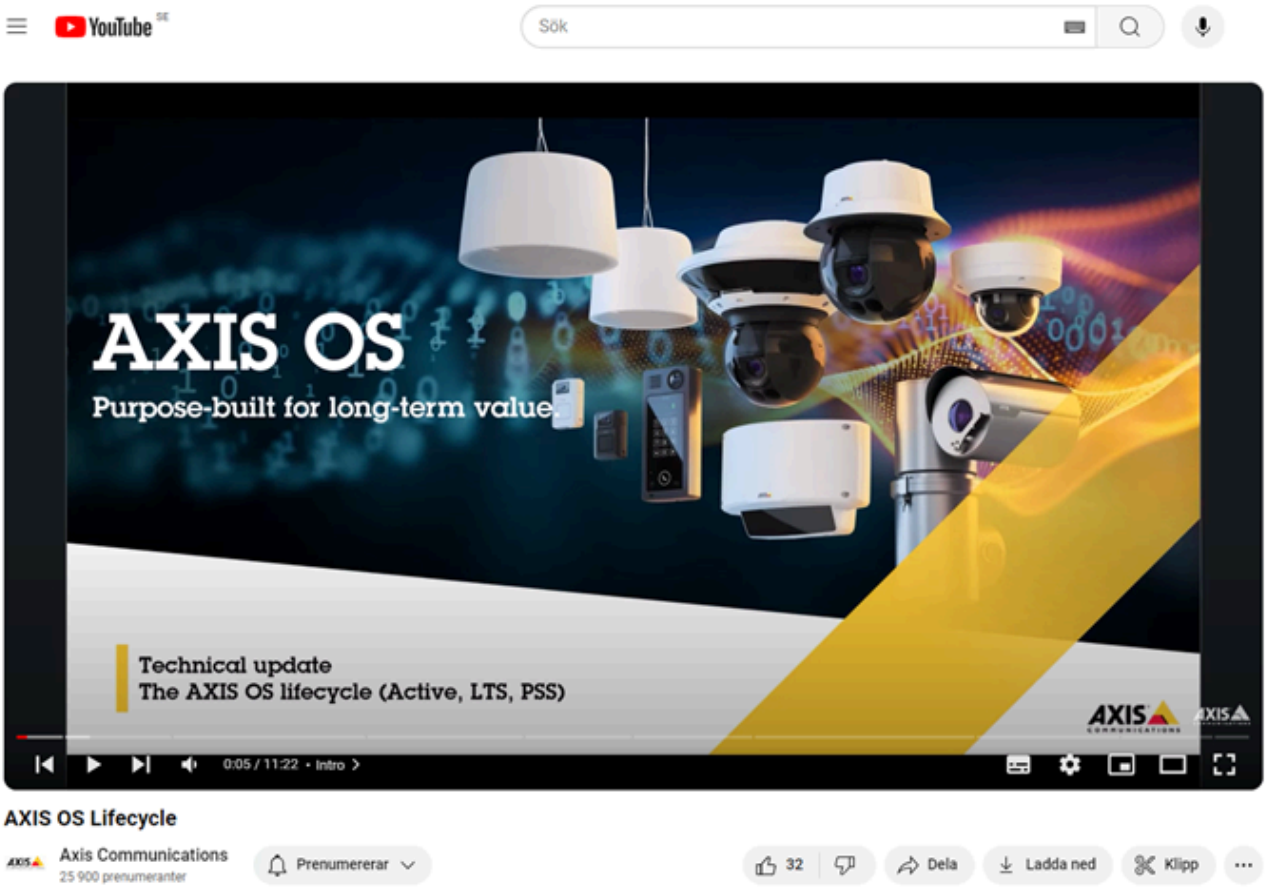
Scheduled for: April 2026

- Added support for RFC 7030 Enrollment over Secure Transport (EST) for IT-policy managed, automated lifecycle of certificates and their renewal. EST can be used to manage certificates for TLS-bearing services such as IEEE 802.1X, HTTPS, MQTT and others. Read more in the *AXIS OS Knowledge base*.
- Updated to OpenSSL 3.5.5 to increase overall cybersecurity, addressing one high-severity, two medium-severity, and seven low-severity issues.
  **Note:** In the factory default state TLS 1.0/1.1 SIP communication is no longer supported as the use of RSA 1024-bit keys is prohibited. **This is a breaking change for SIP**. Support for TLS 1.0/1.1 HTTPS connections was removed in AXIS OS 12.0. It does not affect upgrades, to maintain backwards compatibility.
- Device Configuration API: Added the possibility to set system-wide passphrase complexity before registering the first account.
- Web interface: Added support to select a passphrase complexity profile on the initial account setup page.
- AXIS Audio Manager Edge: Added API support for paging audio clips from the library.Applies to: AXIS C1110-E, AXIS C1111-E, AXIS C1210-E, AXIS C1211-E, AXIS C1510, AXIS C1511, AXIS C1610-VE, AXIS C1710, AXIS C1720, AXIS C8110, AXIS C8210, AXIS D4200-VE and AXIS D6310

## 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.

For a visual explanation, watch the YouTube video *Life of a Product*, which shows the product lifecycle from the AXIS OS point of view.

### 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.

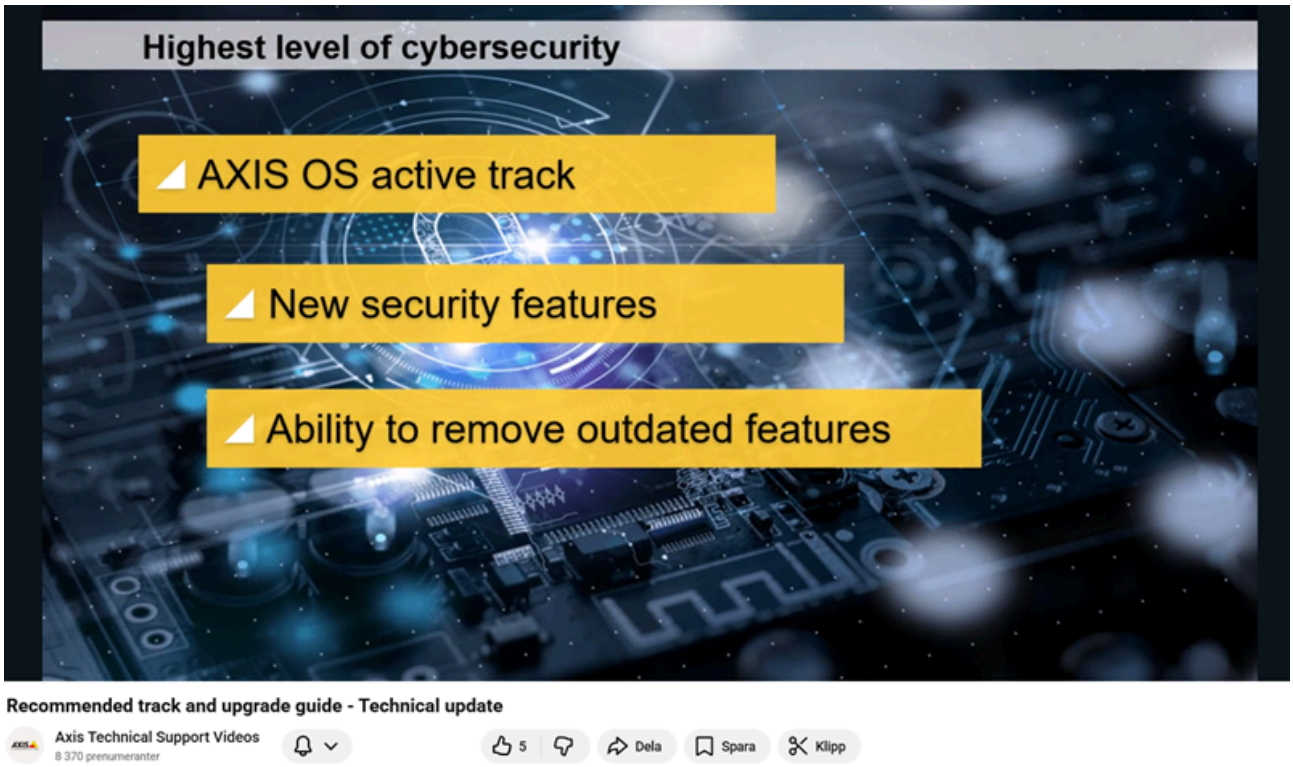
**Existing processes involve frequent updates of VMS and system components. – AXIS OS active or AXIS OS LTS**

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**

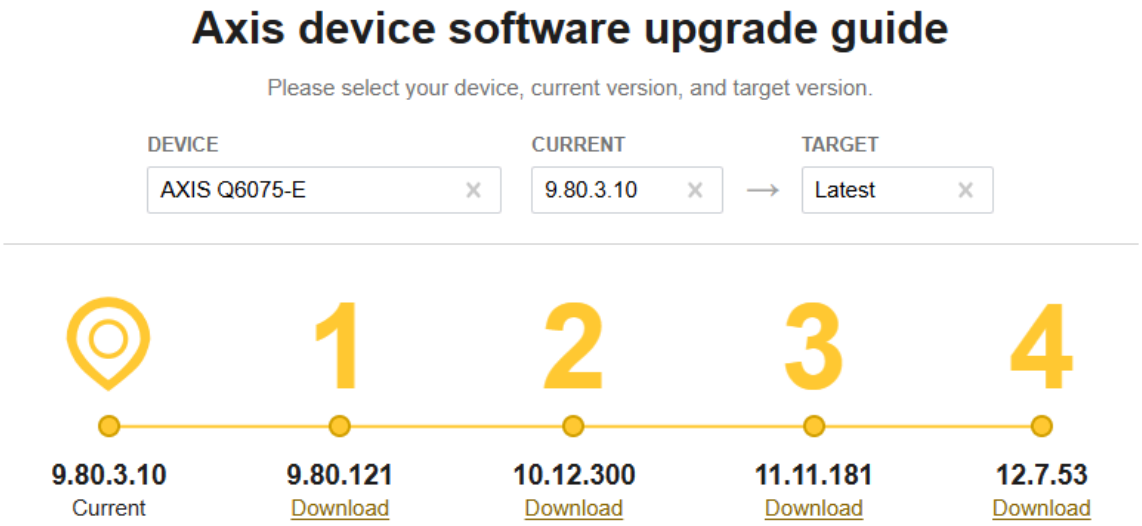
Verify with your VMS and ACAP provider which versions they test and recommend. AXIS OS LTS is the recommended choice for optimal compatibility.




Please watch the YouTube *video*. It is about recommended tracks, and it also covers the Axis device software upgrade guide.

## Upgrade path

You can upgrade your devices using the web interface or various device management tools, such as AXIS Device Manager and AXIS Camera Station Pro. AXIS Device Management Extend simplifies the upgrade process by providing built-in backend upgrade tracks.




Go to *Upgrade guide*, where you can select your device, current and target AXIS OS versions to get step by step instructions.
Detailed information about *How to upgrade* is available in AXIS OS Knowledge base.

Important

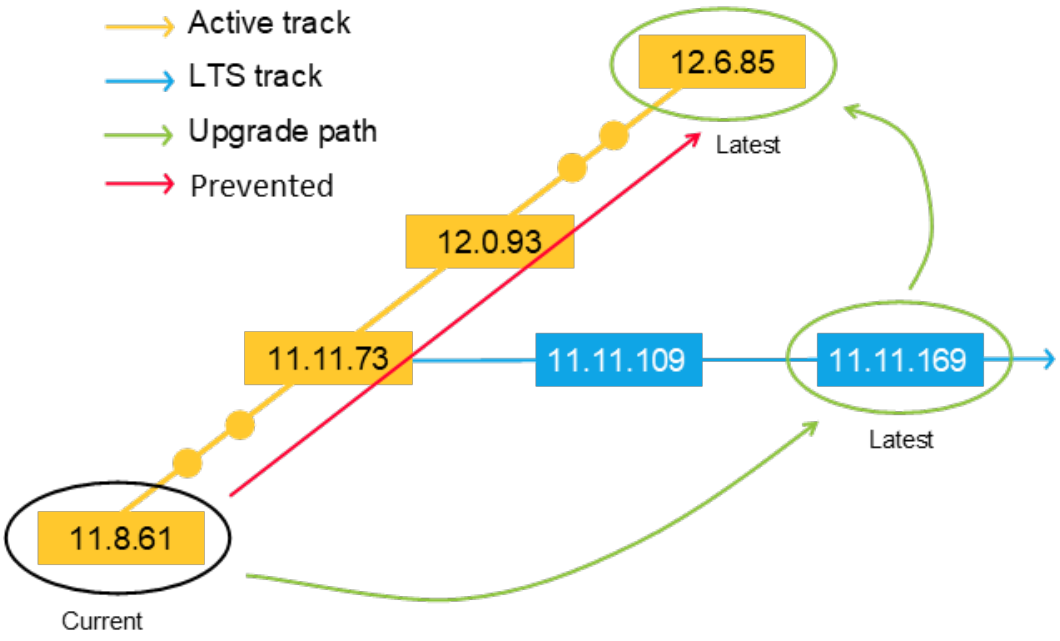
Starting with **AXIS OS 12.6.85** and **11.11.169**, recommended upgrade paths are enforced by the device software to prevent incompatible upgrades and protect device configuration.

- AXIS OS active 12.6.85 can only be upgraded to later versions.
- AXIS OS LTS 2024 (11.11.169) can only be upgraded to AXIS OS 12 or later 11.11 versions.

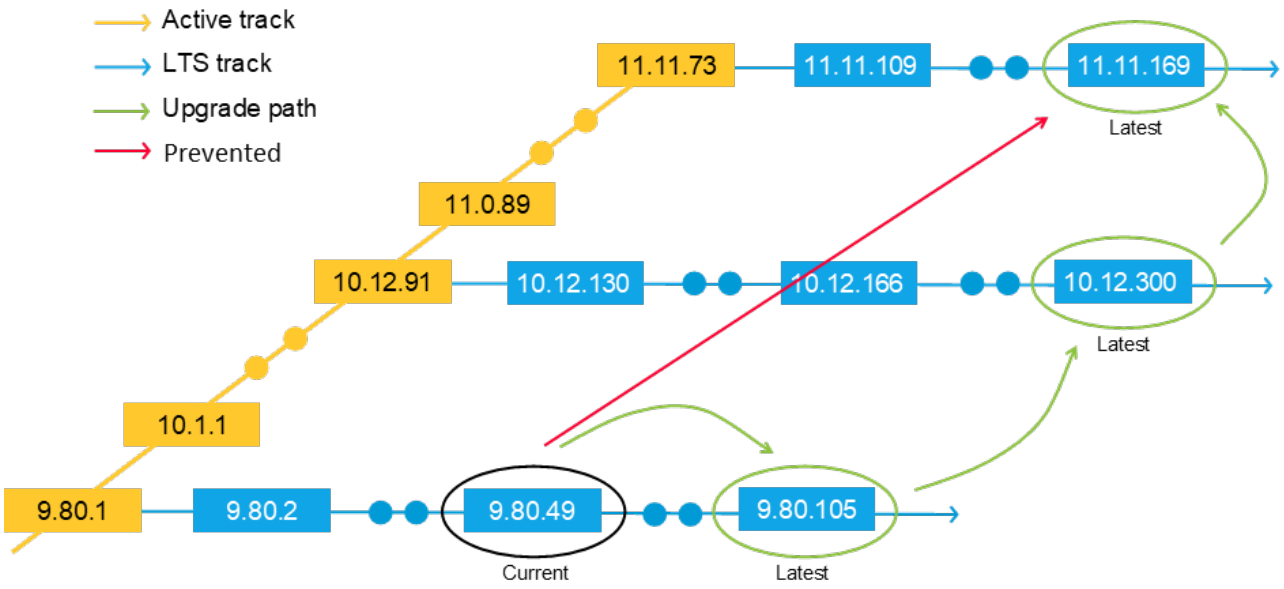
These recommendations and enforcements are not required if the upgrade is performed with a factory default.

Please follow the upgrade path below:

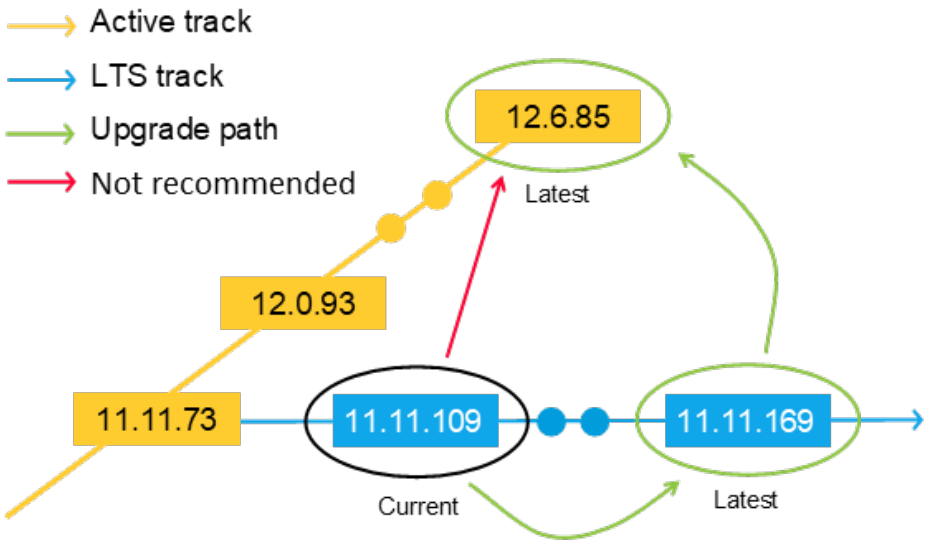
- **Upgrading from an older active track to the latest active**: Upgrade to the latest version of the intermediate LTS.



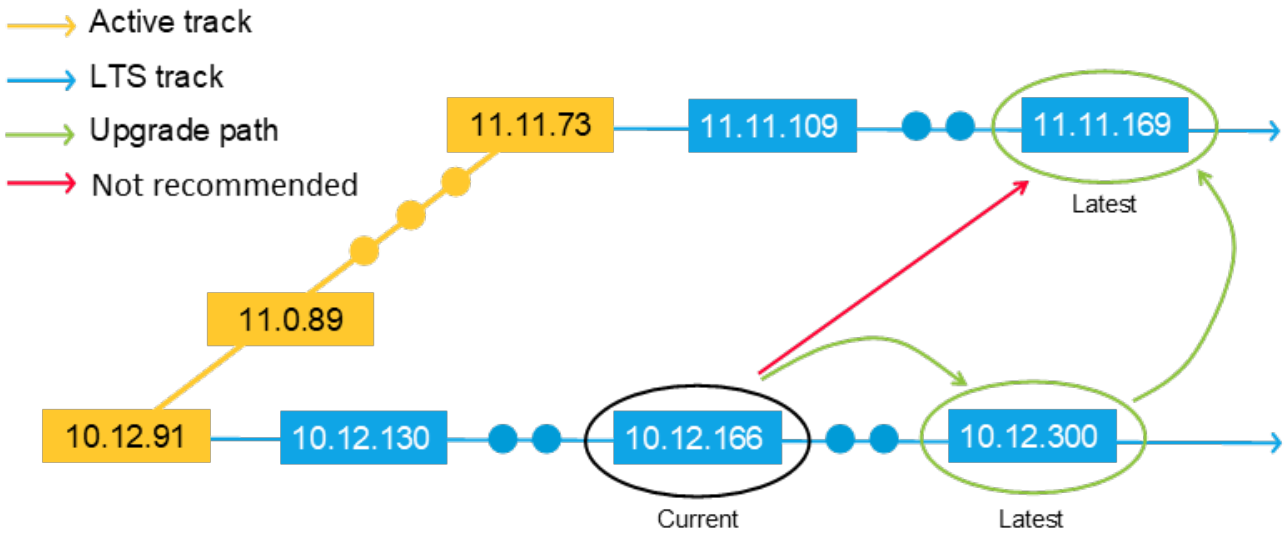

- **Upgrading from an older LTS to two newer LTS versions**: Upgrade to the intermediate LTS version first.




- **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



**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 made performance enhancements that might 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 chose the newest LTS track if available for you 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 *Upgrade path, on page 47*.
- Read the *release notes*, changes has been done between the different tracks.

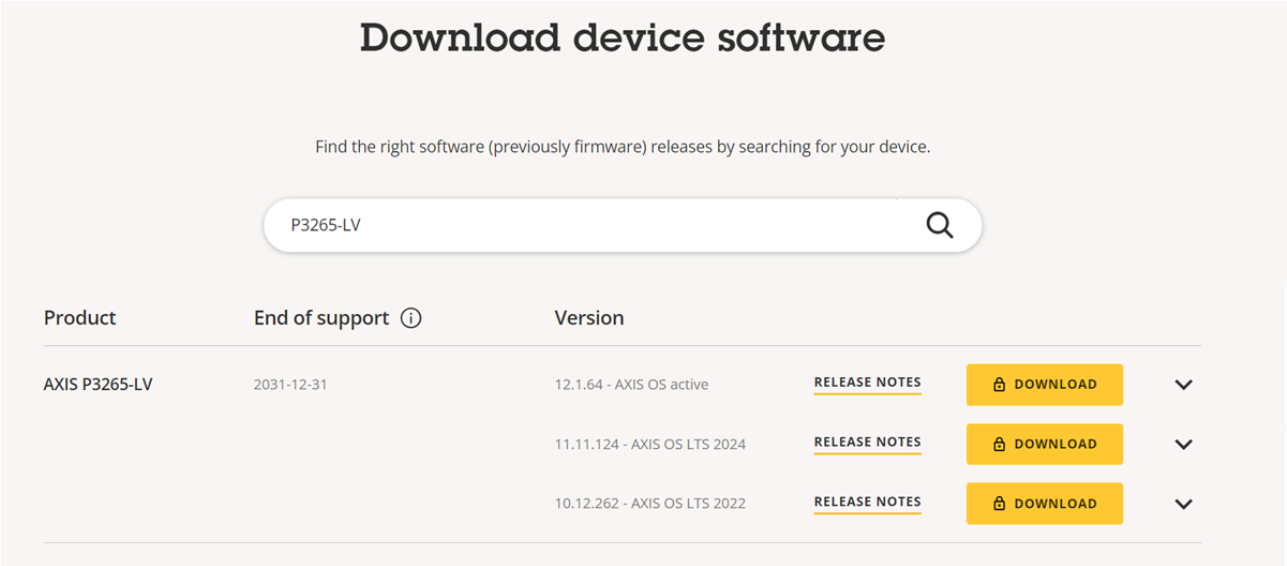
**Verification of new releases:**

- 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.



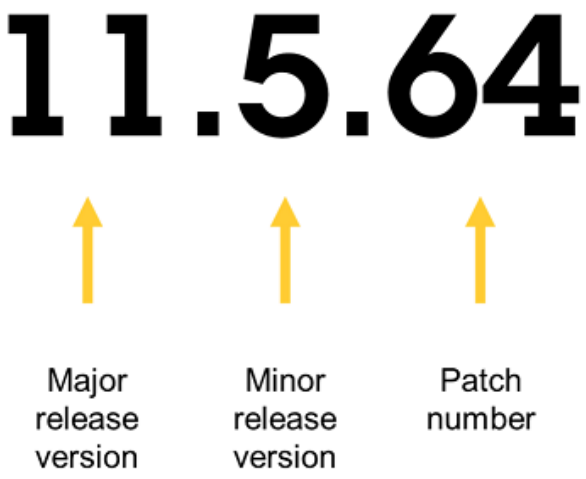

Please see below a list of common tags that indicate different AXIS OS tracks as seen in the picture above.

| 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<br><br>10.12.262 - AXIS OS LTS 2022 | AXIS OS long-term support track (LTS) providing security and maintain compatibility. |
| 9.80.140 - PSS<br><br>8.40.93 - PSS<br>6.50.5.21 - PSS<br>5.51.4.7 | With and without PSS tag. Product-specific support (PSS) track. |

## AXIS OS versioning

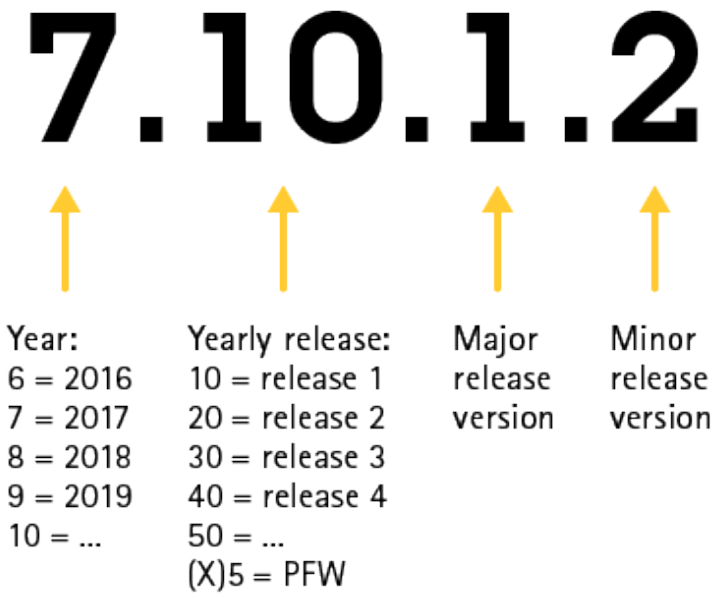
AXIS OS releases are denoted by a unique number combination. Older releases where named by the year and type of the release but since release 10.10 we changed the versioning. The differences and the significance of each number is explained in the figures below.

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.




- 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 .




## 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 *Upgrade path, on page 47*.

### 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*.

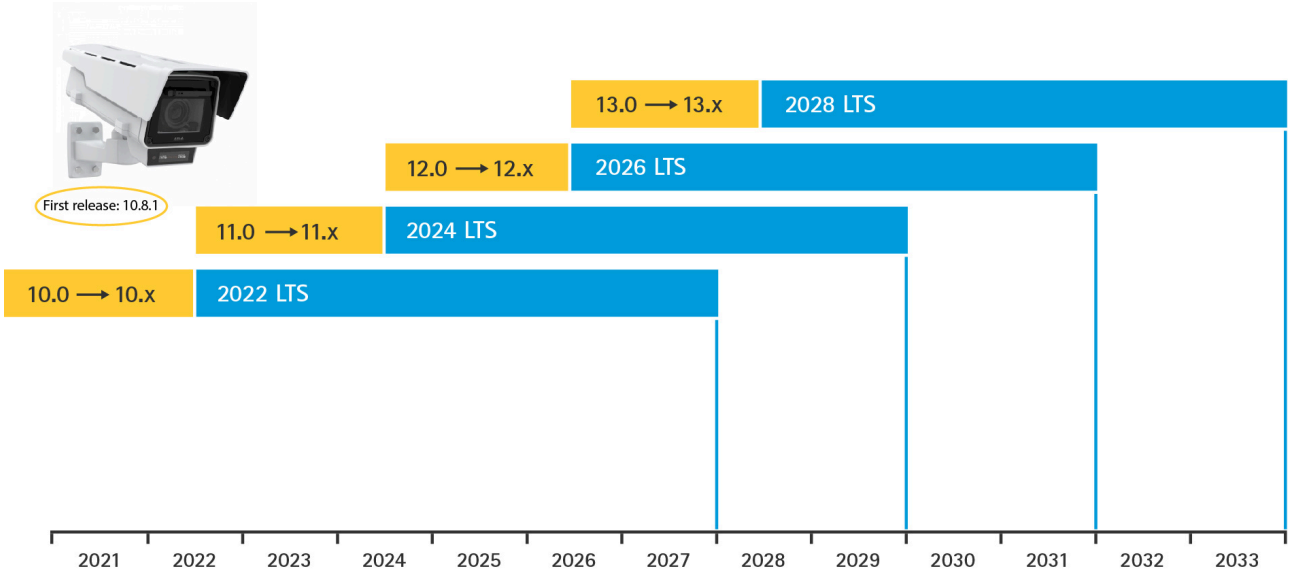
### What happens once the AXIS OS support has expired for a product?

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 *Release schedule, on page 5*.

**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.



# Software Composition

## 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*.

T10202650

- (M37.2)