

AXIS OS Portal

AXIS OS Portal

Table of Contents

About	4
Release schedule	5
Upcoming breaking changes	6
Planned	6
Applied	19
Additional information	22
Next AXIS OS version	22
Current AXIS OS version	22
Open source library support	23
Software Bill of Materials	25
AXIS OS lifecycle management	26
Active track	26
Long-term support track	26
Product-specific support	27
Upgrade recommendations	27
Downloading AXIS OS	28
AXIS OS versioning	29
AXIS OS Support	30
Knowledge base	32

About

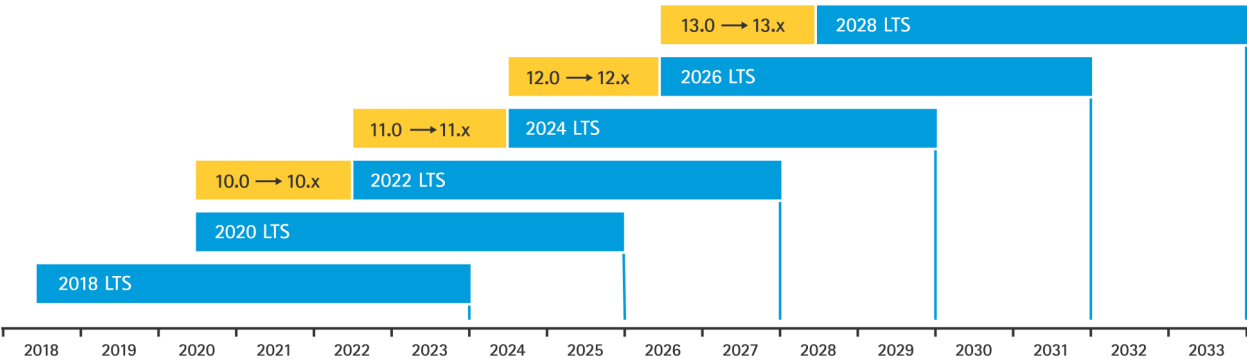


The operating system for Axis edge devices.

AXIS OS is our operating system for edge devices. It's used in more than 300 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.

AXIS OS features different tracks depending on your needs. The **long-term support (LTS)** tracks maximize stability and focus on keeping a well-integrated 3rd party system by providing bug fixes and security patches. The **active track** on the other hand provides access to the newest state-of-the-art features and functionalities as well as bug fixes and security patches, which defines the active track as the software-development-focused track.

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
11.9	Active	February/March 2024	<ul style="list-style-type: none">• cURL version 8.5.0
10.12	LTS 2022	February/March 2024	<ul style="list-style-type: none">• OpenSSL 1.1.1x
9.80	LTS 2020	February 2024 and March 2024	<ul style="list-style-type: none">• February – Apache version 2.4.58.• March – OpenSSL 1.1.1x
8.40	LTS 2018	February/March 2024	<ul style="list-style-type: none">• Apache version 2.4.58.• OpenSSL 1.1.1x• Last release on LTS 2018. Read more here.
11.11	Upcoming LTS 2024	August/September 2024	<ul style="list-style-type: none">• More information will come.
12.0	Upcoming Active	September 2024	<ul style="list-style-type: none">• See <i>Changes in AXIS OS 12.0</i> on page 6 for more information.

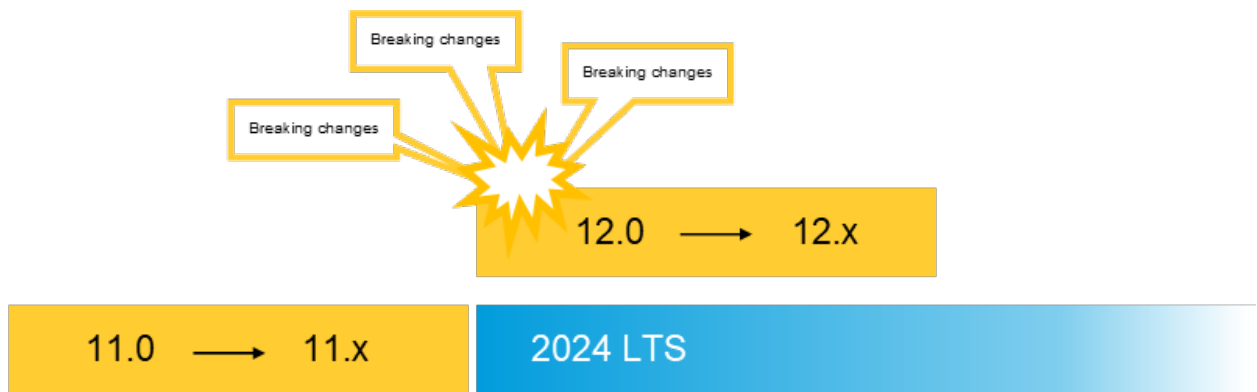
- For highlights and detailed release notes on AXIS OS releases, visit [AXIS OS Release Notes](#).
- Go to *Additional information on page 22* to read more about scheduled and current AXIS OS releases.
- For downloads, visit [Download device software](#) page.
- To get the latest updates to your RSS feed, subscribe to the  [product firmware feed](#).

Upcoming breaking changes

Upcoming breaking changes

AXIS OS 11 active track will transit to LTS 2024 which will be launched in Q3 2024. The new active track will be AXIS OS 12 in which the announced breaking changes will be implemented. The majority of the breaking changes will be introduced at the beginning of the new active track, and the remaining breaking changes will come in the lifetime of AXIS OS 12 and will be communicated in advance.

Please note that some changes will already take place in AXIS OS 11, but with limited impact. Changed default behavior in AXIS OS 11 will affect the product after a factory default as well as new products that are launched with that specific version, but not when doing an upgrade i.e. if you upgrade the AXIS OS without factory default, your products will not change their behavior.



Axis always strives for providing the backward compatibility. However, introducing breaking changes are sometimes inevitable in order to:

- **Improve cybersecurity:** Axis might remove an outdated feature or change the behavior of an existing feature in order to improve the security.
- **Update existing functionality and improve usability:** Axis updates the existing functionality with new default settings or supersedes them with more advanced functionality to extend use cases.

In both cases, we have introduced an alternative way of doing the same things and communicated it in advance. Axis tries to make these changes mostly after creating a new LTS track, to give more time to adjust while maintaining the security.

Note

If you experience issues after upgrading to AXIS OS 12, utilize the rollback option to let the device revert back to its previous AXIS OS version. See guidelines [here](#).

Planned

Changes in AXIS OS 12.0

Important

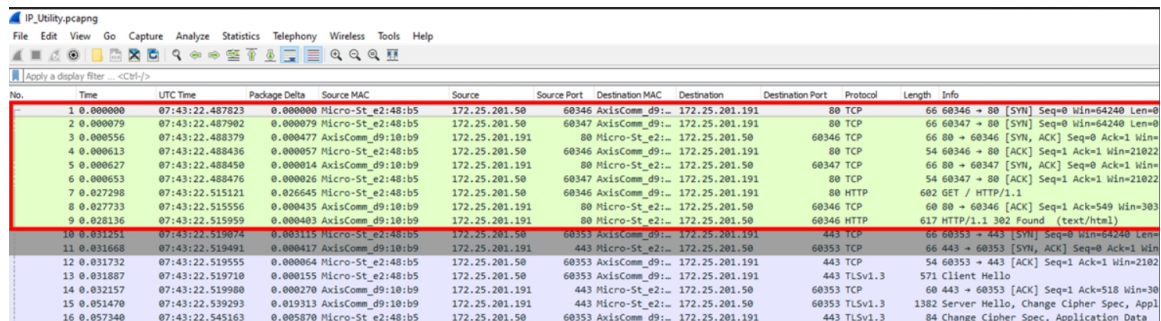
Changes that apply to the first version of the upcoming active track, AXIS OS 12.0. Please note that the changes can be adjusted in future.

- **Disabled HTTP Port 80 redirects**

In previous security penetration tests, it was emphasized to Axis to disable HTTP Port 80 redirects for increased security and to avoid information leakage. Axis devices are currently configured to HTTPS-only, HTTP port 80 redirects are enabled informing accessing clients that no communication is allowed onto port 80 and redirect the accessing client to port 443 instead. Axis will follow the general recommendation from third party penetration test laboratories and will disable HTTP port 80 redirects when the device is configured to HTTPS-only.

AXIS OS Portal

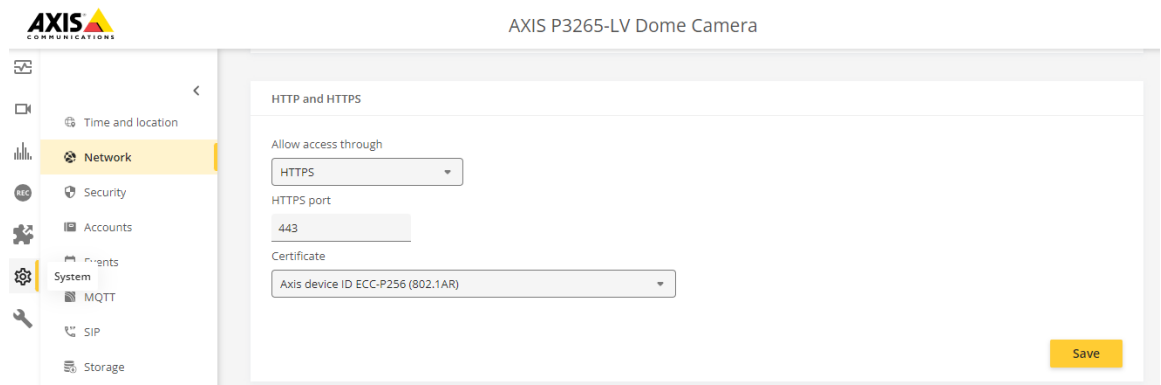
Upcoming breaking changes



The image shows a Wireshark packet capture of network traffic. The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help) and a toolbar. Below the toolbar is a filter bar with 'Apply a display filter' and '<Ctrl>/>'. The main packet list table is as follows:

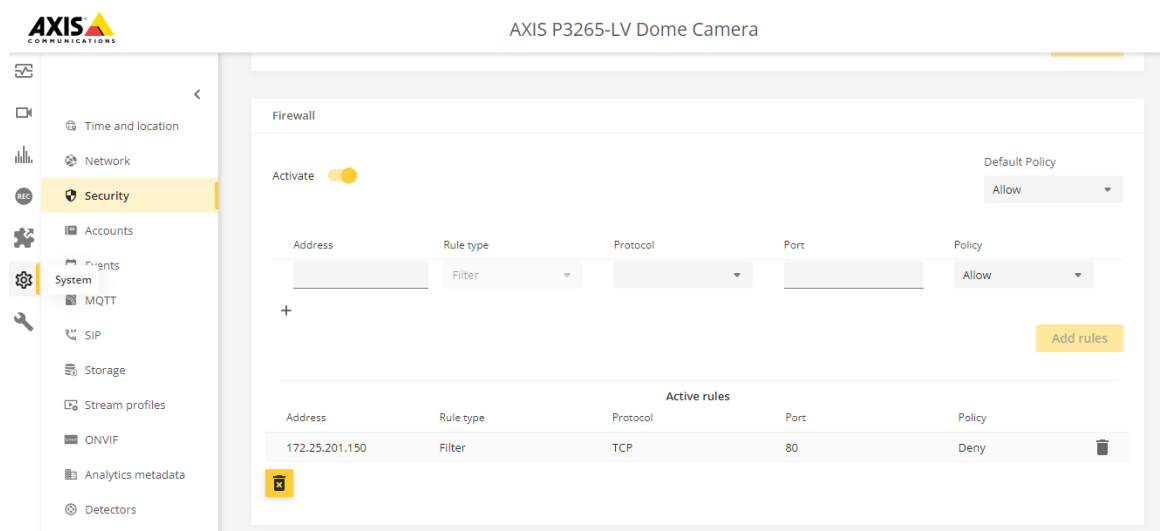
No.	Time	UTC Time	Package Delta	Source MAC	Source	Source Port	Destination MAC	Destination	Destination Port	Protocol	Length	Info
1	0.000000	07:43:22.487823	0.000000	Micro-St_e2:48:b5	172.25.201.50	60346	AxisComm_d9:10:b9	172.25.201.191	80	TCP	66	60346 → 80 [SYN] Seq=0 Win=64240 Len=0
2	0.000079	07:43:22.487902	0.000079	Micro-St_e2:48:b5	172.25.201.50	60347	AxisComm_d9:10:b9	172.25.201.191	80	TCP	66	60347 → 80 [SYN] Seq=0 Win=64240 Len=0
3	0.000556	07:43:22.488379	0.000477	AxisComm_d9:10:b9	172.25.201.191	80	Micro-St_e2:48:b5	172.25.201.50	60346	TCP	66	80 → 60346 [SYN, ACK] Seq=0 Ack=1 Win=0 Len=0
4	0.000613	07:43:22.488436	0.000057	Micro-St_e2:48:b5	172.25.201.50	60348	AxisComm_d9:10:b9	172.25.201.191	80	TCP	54	60348 → 80 [ACK] Seq=1 Ack=1 Win=21022 Len=0
5	0.000627	07:43:22.488450	0.000014	AxisComm_d9:10:b9	172.25.201.191	80	Micro-St_e2:48:b5	172.25.201.50	60347	TCP	66	80 → 60347 [SYN, ACK] Seq=0 Ack=1 Win=0 Len=0
6	0.000653	07:43:22.488476	0.000026	Micro-St_e2:48:b5	172.25.201.50	60347	AxisComm_d9:10:b9	172.25.201.191	80	TCP	54	60347 → 80 [ACK] Seq=1 Ack=1 Win=21022 Len=0
7	0.027298	07:43:22.515121	0.026645	Micro-St_e2:48:b5	172.25.201.50	60346	AxisComm_d9:10:b9	172.25.201.191	80	HTTP	602	GET / HTTP/1.1
8	0.027733	07:43:22.515556	0.000435	AxisComm_d9:10:b9	172.25.201.191	80	Micro-St_e2:48:b5	172.25.201.50	60346	TCP	60	80 → 60346 [ACK] Seq=1 Ack=549 Win=303 Len=0
9	0.028136	07:43:22.515959	0.000403	AxisComm_d9:10:b9	172.25.201.191	80	Micro-St_e2:48:b5	172.25.201.50	60346	HTTP	617	HTTP/1.1 302 Found (text/html)
10	0.031251	07:43:22.519074	0.003115	Micro-St_e2:48:b5	172.25.201.50	60353	AxisComm_d9:10:b9	172.25.201.191	443	TCP	66	60353 → 443 [SYN] Seq=0 Win=64240 Len=0
11	0.031668	07:43:22.519491	0.000417	AxisComm_d9:10:b9	172.25.201.191	443	Micro-St_e2:48:b5	172.25.201.50	60353	TCP	66	443 → 60353 [SYN, ACK] Seq=0 Ack=1 Win=0 Len=0
12	0.031732	07:43:22.519555	0.000064	Micro-St_e2:48:b5	172.25.201.50	60353	AxisComm_d9:10:b9	172.25.201.191	443	TCP	54	60353 → 443 [ACK] Seq=1 Ack=1 Win=21022 Len=0
13	0.031887	07:43:22.519710	0.000155	Micro-St_e2:48:b5	172.25.201.50	60353	AxisComm_d9:10:b9	172.25.201.191	443	TLSv1.3	571	Client Hello
14	0.032157	07:43:22.519980	0.000270	AxisComm_d9:10:b9	172.25.201.191	443	Micro-St_e2:48:b5	172.25.201.50	60353	TCP	60	443 → 60353 [ACK] Seq=1 Ack=518 Win=30 Len=0
15	0.051470	07:43:22.539293	0.019313	AxisComm_d9:10:b9	172.25.201.191	443	Micro-St_e2:48:b5	172.25.201.50	60353	TLSv1.3	1382	Server Hello, Change Cipher Spec, Appl
16	0.057340	07:43:22.545163	0.005870	Micro-St_e2:48:b5	172.25.201.50	60353	AxisComm_d9:10:b9	172.25.201.191	443	TLSv1.3	84	Change Cipher Spec, Application Data

In order to test your client for possible impact, configure your Axis device for HTTPS-only and configure a Firewall rule in AXIS OS 11.9 as seen below where the Axis device would effectively block port 80 communication for a specific client that tries to connect.



The image shows the 'Network' settings screen for an AXIS P3265-LV Dome Camera. The left sidebar contains icons for Time and location, Network (selected), Security, Accounts, Parents, System, MQTT, SIP, and Storage. The main content area is titled 'HTTP and HTTPS' and contains the following settings:

- Allow access through: HTTPS (dropdown menu)
- HTTPS port: 443 (text input)
- Certificate: Axis device ID ECC-P256 (802.1AR) (dropdown menu)
- Save button



The image shows the 'Firewall' settings screen for an AXIS P3265-LV Dome Camera. The left sidebar contains icons for Time and location, Network, Security (selected), Accounts, Parents, System, MQTT, SIP, Storage, Stream profiles, ONVIF, Analytics metadata, and Detectors. The main content area is titled 'Firewall' and contains the following settings:

- Activate: ☒ (toggle switch)
- Default Policy: Allow (dropdown menu)
- Table with columns: Address, Rule type, Protocol, Port, Policy. The table is currently empty.
- + button (to add rules)
- Add rules button
- Active rules section with a table containing one rule:

Address	Rule type	Protocol	Port	Policy
172.25.201.150	Filter	TCP	80	Deny

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

AXIS OS Portal

Upcoming breaking changes

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 SMB 1.0 and 2.0**

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

Add network storage

192.168.0.100

Network share

Network_share

Here

Auto

1.0

2.0

3.1.1

Auto

☐ Add share even if connection test fails.

Cancel Add

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

- **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 up until and including the upcoming LTS 2024 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.

Why is this change introduced? It is obsolete for the active track as the active track run 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.

Upcoming breaking changes

- Removed support for TLS 1.0/1.1 HTTPS connections

Axis devices have support for modern encryption technology through TLS 1.2/1.3 that are used by default for HTTPS connections with the option to enable older, outdated and insecure TLS 1.0/1.1 versions for establishing backwards compatibility to legacy systems not being capable of supporting more secure HTTPS connections. Axis will remove TLS 1.0/1.1 versions for HTTPS connections completely to increase overall security and to prevent users from enabling these protocol versions by mistake.

VAPIX API Parameter: *root.HTTPS.AllowTLS1* and *root.HTTPS.AllowTLS11*

The screenshot shows the 'Plain config' section of the Axis OS Portal. At the top, there is a warning icon and text: 'Plain config is for expert users only. Only change the settings if you know what you're doing.' Below this, there is a 'Select group' dropdown menu set to 'None' and a search bar labeled 'Search for parameters by ID' containing the text 'TLS'. A yellow underline is visible under the 'TLS' search term. Below the search bar, there is an information icon and text: 'To see the effect of your changes, you might have to refresh the webpage or restart the device.' The main content area is divided into two panels. The left panel, titled 'HTTPS', contains two checkboxes: 'Allow TLSv1.0 (deprecated, implies Allow TLSv1.1)' and 'Allow TLSv1.1 (deprecated)', both of which are unchecked. The right panel, titled 'Network / Interface / IO / dot1x / EAPTLS', contains two fields: 'Identity' with the value 'axis-acc8ec656f3' and 'Private key password' with the value '*****'.

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.

- 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. 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 using digest authentication for HTTPS connection, it will not work correctly with AXIS OS 12.0 or higher.

- Removal of vFAT

The possibility to use vFAT as file system for SD cards will be removed. 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 you are using the not recommended vFat file system, it will not work anymore with AXIS OS 12.0 or higher.

AXIS OS Portal

Upcoming breaking changes

- Removal of the old web interface

The old web interface, also called "*AXIS OS web version B*", will be removed.

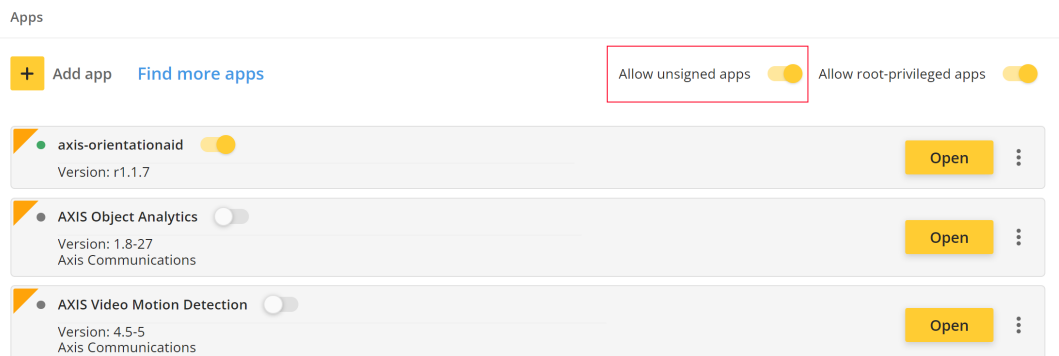
Why is this change introduced? The old web interface is no longer needed since the *new interface* now have all features implemented. It is removed to save memory space on the device and to simplify both usage and maintenance. Additionally, the old web interface used a number of outdated libraries and removing it will make the device more secure.

How can it affect me? The new web interface will be displayed after upgrade.

- ACAP related changes:

- Signed ACAP applications only

From AXIS OS 12.0, the below parameter that allows to install unsigned applications will be removed and it becomes mandatory to use signed applications. However, for development purposes there will be a possibility to bypass the ACAP signature requirement by unlocking individual products. For more information and timeline, go to *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? If you are trying to install unsigned ACAP, it will not work correctly with AXIS OS 12.0 or higher.

- ACAP installation behaviour

The ACAP installation is now aborted if the post-install script exits with an error code. Previously, the ACAP is installed nevertheless and warnings were printed in the log files.

Why is this change introduced? To increase the ACAPS reliability on the market.

How can it affect me? ACAP vendors are informed and should compile a new ACAP version without errors if affected.

- Removal of Basic analytics ACAP applications

Upcoming breaking changes

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 ACAPs, do not upgrade until the system has a verified replacer.

- **Removed support for Add-On applications**

Add-On applications are no longer supported. All applications of this type should have replacements in the form of ACAP applications or the equivalent functionality is now built into the device software itself.

Why is this change introduced? Unofficial and undocumented formats for application packages shall not be used due to the security risk. Thus, it is removed since the ACAP application format can be used instead.

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

- **Removal of libcapture library**

The libcapture library for ACAPs 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 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 using this library, it will not work correctly with AXIS OS 12.0 or higher.

- **VAPIX 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).

Upcoming breaking changes

- **Disabled basic device information**

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 change the default behavior so that the Basic Device Information VAPIX API will be automatically disabled after the Axis product is initialized. The product initialization is completed when the first initial account with password is created.

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

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 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 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.

AXIS OS Portal

Upcoming breaking changes

- **PTZ tilt coordinates are not handled correctly in metadata**

PTZ tilt coordinates are not handled correctly in metadata. From AXIS OS 12, VAPIX Metadata for pan and tilt position will be calculated with physical constraints in tilt and pan when using Generic Pan/Tilt Position Space, in the same way as calculated in ONVIF already. A new parameter will be introduced: *root.Properties.API.Metadata.PTZ.GenericPanTiltPosition=truelimitations*

Why is this change introduced? Because the PTZ generic Pan/tilt metadata was presented wrongly.

How can it affect me? If using the PTZ generic Pan/tilt metadata the information is not correct. New parameter should be used to get the correct PTZ generic Pan/tilt metadata.

- **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.

- **Event and Action Services VAPIX API changes**

The Event and Action Services VAPIX API has been hardened and will not disclose sensitive recipient connection details anymore such as username and password.

Previously, those information were available by authenticated administrator-privileged accounts only. Recipients in the Event and Action Services VAPIX API are used so that Axis networked devices can connect to a server. Moving forward, It is expected from clients that receive the recipient configuration that they do not require this specific information and store it pro-actively themselves prior to recipient configuration.

Upcoming breaking changes

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


How can it affect me? There should be no impact as it is expected from clients that receive the recipient configuration that they do not require this specific information and store it pro-actively themselves prior to recipient configuration.

- 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*

Plain config


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

Select group

None

Search for parameters by ID

upnp

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

Network / UPnP

☒ Enabled

Friendly name

AXIS P1375 - ACCC8EC656F3

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 12.0 or higher and users need to enable UPnP first on the Axis device.


- 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 and configured in factory defaulted state which makes the availability of the WS-Discovery protocol obsolete. Axis will adapt the default behavior and will disable the WS-discovery protocol in factory defaulted state. The WS-discovery will be enabled only when an ONVIF user is configured on the Axis device. This will also lower the attack surface of the device and increase overall network security. However, the WS-Discovery protocol can be disabled per user's discretion after device detection and onboarding through a parameter.

Upcoming breaking changes

VAPIX API parameter: *WebService.DiscoveryMode.Discoverable*

Plain config


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

Select group

None

Search for parameters by ID

DiscoveryMode

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

WebService / DiscoveryMode

☒ Enable WS-Discovery discoverable mode

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 an ONVIF user has been created on the Axis device.

- **Added path restrictions for dynamicoverlay.cgi**

The *Dynamic Overlay* VAPIX API that allows to configure the patch 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 through 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.

- **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

AXIS OS Portal

Upcoming breaking changes

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.

Changes during AXIS OS 12

Important

Changes taking place among the first versions of the upcoming active track, AXIS OS 12. Please note that the changes can be adjusted in future.

- Password complexity enforcement

The user is currently supported with a password strength indicator for selecting secure passwords for service accounts. However, the user might select insecure passwords anyway. At some point in time in AXIS OS 12, it is planned to introduce a password complexity enforcement to enforce using secure-considered passwords when accessing an Axis device.

Afterward, it will not be possible to use insecure password combinations. It is expected that the password complexity enforcement will be standardized and will require a minimum password length of 14 characters including small and big letters, special signs and numbers, alternatively small and big letters with a password length of 64-characters. More information to come. The decision on when to introduce password complexity has not been made yet but will be communicated in time.

The screenshot shows the 'Add user' form in the AXIS OS Portal. The form is titled 'Add user' and contains the following fields and elements:

- Username:** A text input field containing 'MyUser'.
- New password:** A password input field with masked characters (dots) and a toggle icon (eye) to show/hide the password.
- Repeat password:** A password input field with masked characters (dots) and a toggle icon (eye) to show/hide the password.
- Password strength indicator:** A green progress bar indicating the strength of the password, accompanied by an information icon (i).
- Role:** A dropdown menu currently set to 'Administrator'.
- Buttons:** 'Cancel' and 'Save' buttons at the bottom right.

Upcoming breaking changes

Why is this change introduced? To increase the cybersecurity level.

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.

How can it affect me? Will be updated shortly.

- HTTPS-only enforcement**

The current default behavior of Axis devices in factory defaulted state is that HTTP and HTTPS are both enabled allowing for a flexible choice on which protocol to use to connect to the Axis device. Axis, since many years, has given the recommendation to configure the Axis device to HTTPS-only during initial configuration according to the *AXIS OS Hardening Guide*. Please see the current default settings below.

HTTP and HTTPS

Allow access through

HTTP and HTTPS

HTTP port

80

HTTPS port

443

Certificate

Axis device ID ECC-P256 (802.1AR)

This default behavior is likely to change at some point in time in AXIS OS 12 to increase overall default security and protect communication between the Axis device and the human user as well as applications. Axis has plans to change the default behavior so that HTTP communication will be disabled, and HTTPS-only communication is the only enabled protocol to be used in factory defaulted state.

AXIS OS Portal

Upcoming breaking changes

HTTP and HTTPS

Allow access through

HTTPS

HTTPS port

443

Certificate

Axis device ID ECC-P256 (802.1AR)

Why is this change introduced? To increase the cybersecurity level.

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

- **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*.

Why is this change introduced? 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.

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.

- **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.

Why is this change introduced?

- To be completely RFC IPv4 compliant.
- Disable link-local address when it is not used.

AXIS OS Portal

Upcoming breaking changes

- Better user experience for our customers when multiple factory-defaulted Axis devices are placed on the same network simultaneously.
- Increase robustness and detect IP address conflicts.

How can it affect me? Affects during installation, AXIS devices will request IP address from the network it attaches to etc DHCP.

- 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.

Applied

Changes during AXIS OS 11

Breaking changes done in AXIS OS 11.

- 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*.

Upcoming breaking changes

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.

- 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.

- 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.

- 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*.

- 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.

- 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 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.

Upcoming breaking changes

- 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 12.0 or higher unless you create a user root.

- Signed ACAP applications as default and removed root-privileged access

Axis will require ACAP applications to be signed upon installing them onto the Axis device to increase overall security. We will also remove root-privileged access to Axis products and ACAP applications to increase ACAP confidentiality by better protecting their data and secrets, prevent information leakage as well as elevated AXIS OS system integrity through the removal of system-wide root-privileged access for users and applications. 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 ACAPs 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	<ul style="list-style-type: none">• VAPIX/Web Access: The user "root" is an ordinary administrator.• ACAP Privileges: Root privileges can be disabled.
11.6	September 2023	<ul style="list-style-type: none">• SSH Access: Root user access can be disabled.
11.8	January 2024	<ul style="list-style-type: none">• SSH Access: Root user access is disabled by default but can be enabled.• ACAP Privileges: Root privileges is disabled by default but can be enabled.
11.x	Q3 2024	<ul style="list-style-type: none">• Axis devices only accept installation of signed ACAP applications by default. Devices can be configured to accept unsigned applications
LTS 2024	H2 2024	Support: 2024-2029. Can be used as a stop-gap solution until an ACAP application is fully adapted. <ul style="list-style-type: none">• SSH Access: Root user access is disabled by default but can be enabled.• ACAP Privileges: Root privileges is disabled by default but can be enabled.

Additional information

In this section you can read about updates and features in upcoming AXIS OS releases. For more information about:

- Previous releases, visit [AXIS OS Release Notes](#).
- Developer News articles, visit [Developer Community](#).

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.

AXIS OS 11.9

Scheduled for: February/March 2024

- Updated user-management API. In version 1.2, it is possible to retrieve information from the device if it supports admin users named anything else than "root".
- Enabled Radar and Camera Autocalibration for automatically learning scene elevation.
Applies to: AXIS Q1656-DLE
- Added support for Network radar pairing (Edge-to-edge technology). The radar view will use the second view area to show the radar view when pairing is enabled.
Applies to: AXIS P1465-LE-3 and AXIS P3265-LVE-3
- Analytics
 - Improved object detection and added support for new object classes; HumanFace, LicensePlate, and vehicle sub-classes Bus, Car and Truck. These classes have been added to the RTSP video analytics metadata stream. More information is provided [here](#).
Applies to: AXIS P3727-PLE

To see which classes are supported on your device, use `getSupportedMetadata` which is documented in the *The Analytics Metadata Producer Configuration API*. More information is provided in the *AXIS Developer Community* and the *AXIS OS Knowledge base*.
- Cybersecurity
 - Updated to increase overall cybersecurity level.
 - The Trusted Execution Environment (TEE) is selectable as a secure keystore, providing higher performance and lower latency compared to the high-security and certified TPM 2.0 and Secure Element. More information and guidance can be found [here](#).
Applies to: Products on *ARTPEC-8*, *CV25*, *S6L* and *6SX*
- VAPIX
 - Added a new VAPIX REST API to be able to write a custom message into the system log of the device.

Current AXIS OS version

AXIS OS 11.8

Release date: January 2024

- Added support for host-based firewall to improve network security. The legacy "IP-Filtering"-service is deprecated and will be removed after AXIS OS 2024 LTS.

Additional information

- Added support for EventBroker MQTT capability in ONVIF profile M.
Applies to: All product with support for metadata.
- Added MQTT Graph overlays.
- Added support for WLAN country code.
Applies to: AXIS M1075-L
- Added support for IEEE 802.1AE MAC Security (MACsec) with Static CAK/Pre-Shared Key (PSK) and Dynamic CAK/EAP-TLS. Dynamic CAK/EAP-TLS is enabled by default. MACsec can be configured from the security tab in the web-interface and allows for complete layer-2 network encryption between the Axis device and network switch. Read more in the *AXIS OS Knowledge base*.
Applies to: All products except AXIS S30-series
- Added a new Log API via the device config framework. A way to see if a device supports Log API is by running `http://{device}/config/discover/apis/log/v1`.
- **ACAP**
 - Added support for Reverse Proxy in the ACAP manifest/installation framework.
 - Added support for accessibility of static HTML files for operators and viewers in the *new manifest schema*.
 - ACAP applications using the axaudio lib will be able to get raw (pcm) audio streams even if the input is disabled.
Applies to: All products with audio and ACAP support
- **Root-Privileges**
 - Root-privileged installation of ACAP applications is disabled in the factory defaulted state. To allow the installation of root-privilege ACAPs, it must be enabled in Settings > Apps > Allow root-privileges apps. Upgrade without factory default will not affect the setting. For more information see *Additional security in AXIS OS and ACAP applications* and *Upcoming breaking changes on page 6*.
 - Root-privileged access through the SSH-interface is disabled in factory defaulted state. To allow root-privileged access through SSH, it must be enabled in Settings > Accounts > SSH accounts. Upgrade without factory default will not affect the setting. For more information see *Additional security in AXIS OS and ACAP applications* and *Upcoming breaking changes on page 6*.
- **VAPIX**
 - A new VAPIX REST API for saving/clearing all severity logs in one single persistent file.
 - Added a new VAPIX REST API to thermography-cgi.

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.

Additional information

- 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.

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?

Initially, due to current licensing and technical limitations we cannot provide information about third-party proprietary software and Axis-proprietary components with dependencies. In addition to this some of the packages in the software consist of pre-compiled bundles such as our web interface and ACAPS, which have not in their turn provided an SBOM. Over time our aim is to cover all the third-party components and as much of the Axis-proprietary components as legally possible.

Where can I find the SBOM?

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

What format and why?

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

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

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

What about SBOM for other AXIS software?

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

Where can I find more information about SBOM in general?

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

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

How can I use the SBOM to analyze the software?

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

AXIS OS lifecycle management

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

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

	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

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.

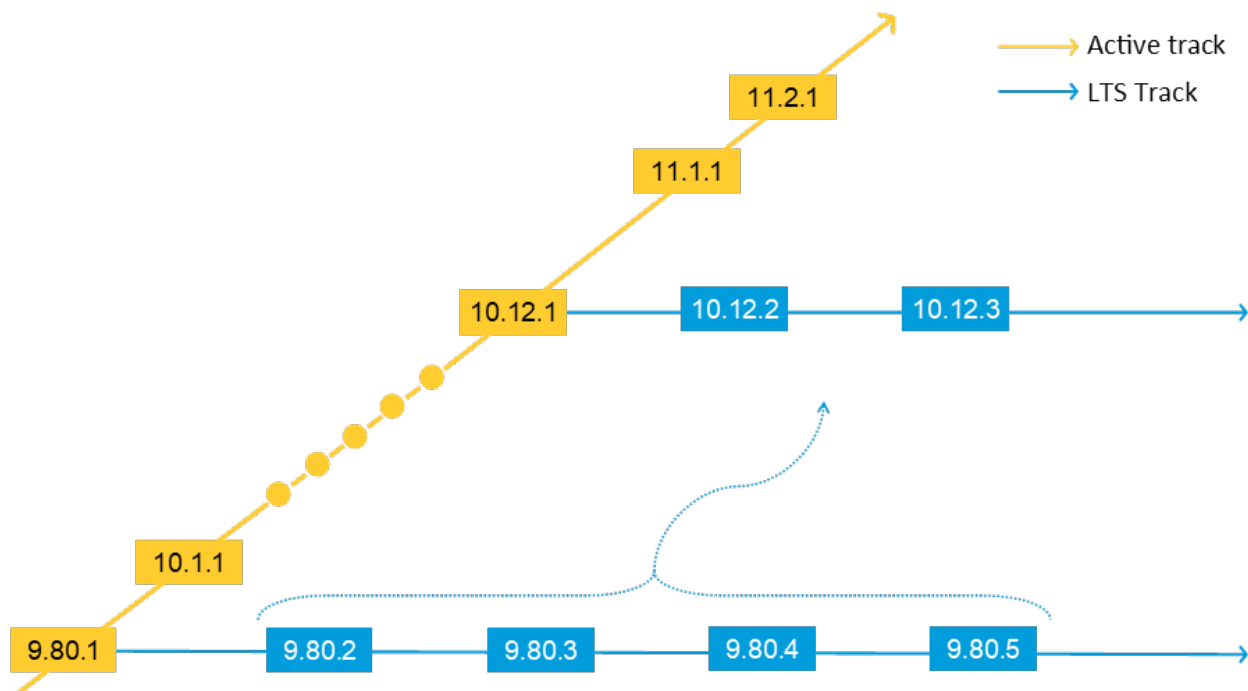
Upgrade recommendations

If upgrading via the web interface it is required to always go through each major LTS track. (9.60 => 9.80 LTS => 10.6). It is also recommended to avoid upgrading with longer version gaps, such as upgrading directly from AXIS OS 10.5 to AXIS OS 10.9. Instead, use all available releases in-between your actual AXIS OS version and the target release of the Axis device. An upgrade from AXIS OS 10.5 to AXIS OS 10.9 should be performed by upgrading through the available AXIS OS 10.6, 10.7 and 10.8 if they are available on www.axis.com.

Maintaining a upgrade strategy ensures that your Axis product receives continuous improvements. Axis Technical Services will also recommend that you update to the latest when reporting issues related to an Axis product. But since there may be several coexisting tracks, which "latest" should you choose? If you use an LTS track, you should normally update to the latest version on the same AXIS LTS track. If you intend to use the AXIS OS active track, you should update to the latest available.

- Question:** With my Axis product running on the LTS 2020 (9.80) track, should I consider updating to the latest AXIS OS active track?
Answer: It is recommended to stay on the LTS 2020 (9.80) track but update to the latest version on that track as long as it is maintained, unless there is a need for new features available from the AXIS OS active track.
- Question:** I would like to run my Axis product on an LTS track, but currently there is no LTS track available?
Answer: Your product was launched between two LTS tracks. It is recommended to continuously update the product on the AXIS OS active track until an LTS track is available. A new LTS track is available every two years.
- Question:** With my Axis product running on the LTS 2020 (9.80) track, should I consider updating to the new LTS track?
Answer: Yes, but you should coordinate the change with your other schedules, e.g., VMS upgrade, network maintenance, and camera replacement cycle.
- Question:** My VMS states that it must use a certain version of the LTS track, e.g. version 9.80.3.2 on LTS 2020, but I can't find that on axis.com. What do I do?
Answer: If a VMS is compatible with one version on the LTS track, it is also compatible with the upcoming releases on that track. The reason most VMS's only list one version is because that's the version they've been certified with. Since compatibility is maintained within each LTS tracks, it's safe to use other versions on that track as well.

With time, there will be several LTS tracks available for a product. All LTS tracks maintain a high level of stability through long-term bug fixing without adding new features. At some point though, technical limitations may make it impossible to update certain components in AXIS OS. In a long-term perspective, it is therefore recommended to switch to a newer LTS track. Please note that a newer LTS track may include new features, changes to default settings, and performance adjustments that could affect compatibility with your system. The products should be updated in a controlled and supervised manner after verification that the new LTS track works as expected in your environment.



Recommended upgrade path for switching LTS tracks when a new LTS track is available. Note that actual notation may differ from those in the diagram.

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.

Firmware

Find the firmware you are looking for by searching for your product.

AXIS M1137-E

Product	Version			
AXIS M1137-E Mk II	10.12.104 - AXIS OS LTS 2022	RELEASE NOTES	DOWNLOAD	▼
AXIS M1137-E	9.80.3.13 - AXIS OS LTS 2020	RELEASE NOTES	DOWNLOAD	▼
AXIS M1137-E	10.12.91 - AXIS OS	RELEASE NOTES	DOWNLOAD	▼

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

Tag example	Explanation
11.4.63 - AXIS OS	AXIS OS active track providing new features, security and other improvements.
10.12.166 - AXIS OS LTS 2022 9.80.28 - AXIS OS LTS 2020 8.40.19 - AXIS OS LTS 2018	AXIS OS long-term support track (LTS) providing security and maintain compatibility.
6.50.5.10 5.51.4.7	Without tag. Not part of AXIS OS Active or LTS track. Only maintained during hardware warranty.

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.

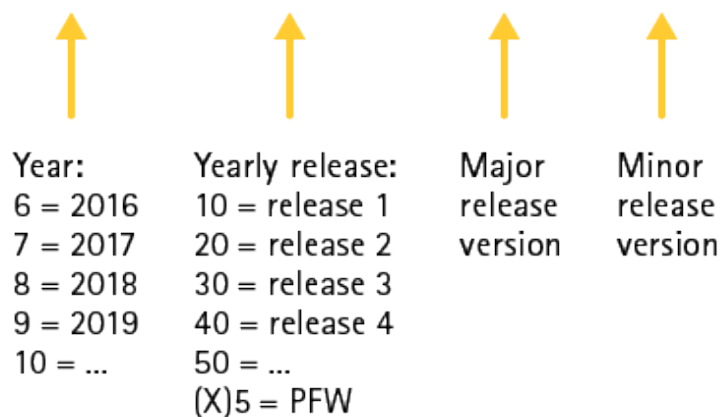
11.5.64



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

Previous versioning .

7.10.1.2



AXIS OS Support

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

AXIS OS lifecycle management

The product will be supported during this period with stability and security releases.

What is required to get the full support period?

The device needs to be upgraded to the latest supported LTS version. For more information on upgrade strategy, see *Upgrade recommendations on page 27*.

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

Which dates will be shown depends on what information have been investigated and where the product is in its lifecycle. In some cases no dates are shown, and in other cases two different dates can be shown. If the product has a set end of support date for hardware and AXIS OS, they will both be shown.

Why do the products have such varied end of support dates?

The support dates will be set per product as each product has its own hardware configuration regarding SoC (system-on-chip), memory, etc. Since the portfolio adds new products all the time, we need also to limit the total number of products supported, otherwise the level of support would have to be reduced.

Why do some products lack an AXIS OS maintenance date?

A support date is only available for products that have a determined support period. It will be available for more products in the AXIS portfolio over time. Please contact the *Axis Technical Support Helpdesk* for further questions.

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

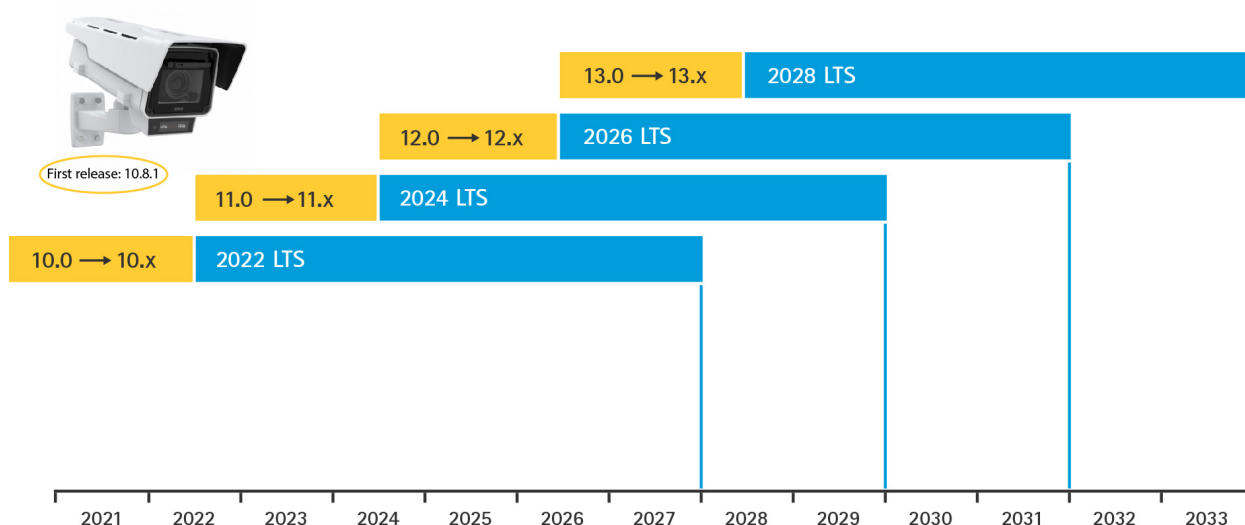
There will be no further updates, improvements, or security patches. There are limitations on how long we can keep a software up-to-date and make changes in an older version. It gets more difficult and complicated to make changes on software that is limited by hardware resources, and there comes a point when we no longer can keep the product cyber secure.

Where do I find out more about the current AXIS OS release forecast, upcoming changes and currently supported tracks?

Please follow and monitor the *Release schedule on page 5* in the AXIS OS portal.

Example of AXIS OS Support:

During its product lifecycle, AXIS Q1656-LE Box Camera will receive new features, higher cybersecurity, improvements and security patches up until 2028. From 2028 until 2033, it will get some improvements and all security patches through LTS 2028, with focus on compatibility.



AXIS OS Portal

Knowledge base

Knowledge base

The AXIS OS Knowledge base has moved to its own online manual. Please got *AXIS OS Knowledge base*.

