

AXIS OS Portal

Table of Contents

.....	3
About	4
Release schedule.....	5
Breaking changes.....	6
Planned.....	6
Changes in AXIS OS 13.....	6
Changes in AXIS OS 14.....	9
Applied	9
Changes in AXIS OS 12.1	9
Changes in AXIS OS 12.0	11
Changes in AXIS OS 11.....	22
Next AXIS OS version	26
Current AXIS OS version	27
Open source library support	28
Software Bill of Materials	29
AXIS OS lifecycle management.....	31
Active track.....	31
Long-term support track.....	32
Product-specific support.....	32
Suggested track	32
Upgrade path.....	33
General recommendations.....	35
Downloading AXIS OS.....	36
AXIS OS versioning.....	37
AXIS OS Support	38

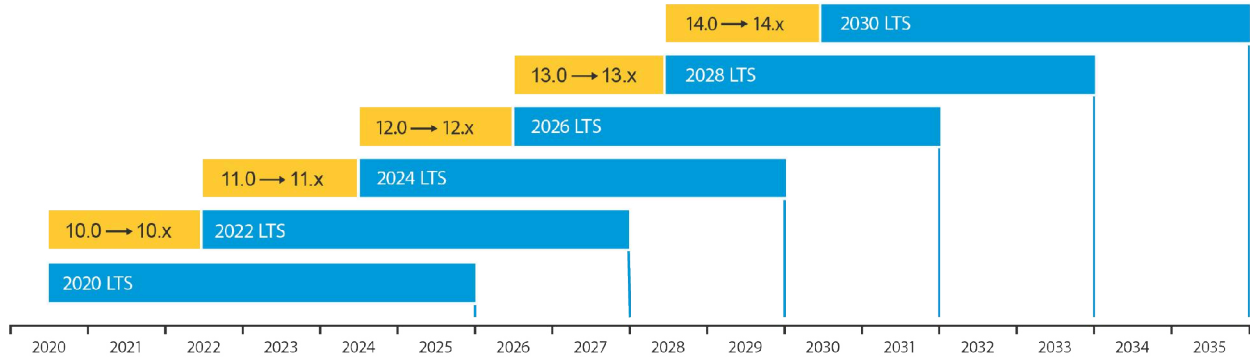
AXIS OS Release Notes | AXIS OS Knowledge base | AXIS OS YouTube playlist | AXIS OS Hardening Guide | Security Advisories

About

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

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

AXIS OS support overview




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

Release schedule

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

Version	Track	Preliminary release date	Planned features and updates
12.4	Active	April 2025	<ul style="list-style-type: none"> cURL version 8.12.0 AXIS CVE: CVE-2025-0325
11.11	LTS 2024	March 2025	<ul style="list-style-type: none"> OpenSSL vesion 3.0.16 and 1.1.1zb cURL version 8.12.0 AXIS CVE: CVE-2025-0324, CVE-2025-0361 and CVE-2024-47261
10.12	LTS 2022	March/April 2025	<ul style="list-style-type: none"> OpenSSL vesion 1.1.1zb cURL version 8.12.0 AXIS CVE: CVE-2024-47261
9.80	LTS 2020	April 2025	<ul style="list-style-type: none"> OpenSSL version 1.1.1zb cURL version 8.12.0 AXIS CVE: CVE-2024-47261
8.40	Product-specific support	May 2025	<ul style="list-style-type: none"> cURL version 8.12.0 OpenSSL version 1.1.1zb AXIS CVE: CVE-2025-0325
6.50	Product-specific support	March 2025	<ul style="list-style-type: none"> cURL version 8.11.1 AXIS CVE: CVE-2024-47262

- For highlights and detailed release notes on AXIS OS releases, visit *AXIS OS Release Notes*.
- Subscribe to the *AXIS OS YouTube playlist* to conveniently stay updated and informed.
- Go to 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*.

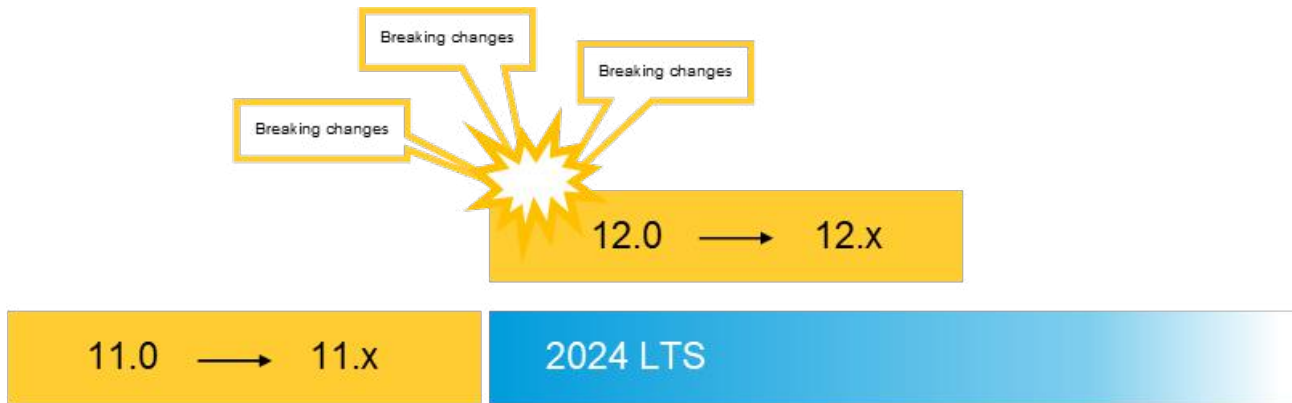
Breaking changes

Axis launches a new active track every two years, transitioning the previous active track into a long-term support (LTS) phase.

In September 2024, AXIS OS 11 entered the LTS 2024 phase, while the new active track, AXIS OS 12, was introduced.

Each new active track focuses on delivering innovative features to advance AXIS OS and enhance its cybersecurity.

In addition, pre-announced breaking changes are introduced at the start of the new track, communicated well in advance, with further changes during the lifecycle of the active track taking place but with limited impact.



A breaking change is an intentional modification which will break backwards compatibility. While Axis consistently strives to maintain backward compatibility, introducing breaking changes is sometimes necessary 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 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.** These changes are usually implemented after a new LTS track has been established, giving users sufficient time to adapt while maintaining security measures.

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](#). We recommend that you keep at least one device running AXIS OS 12, generate a server report and contact Axis Technical Support for troubleshooting assistance or guidance.

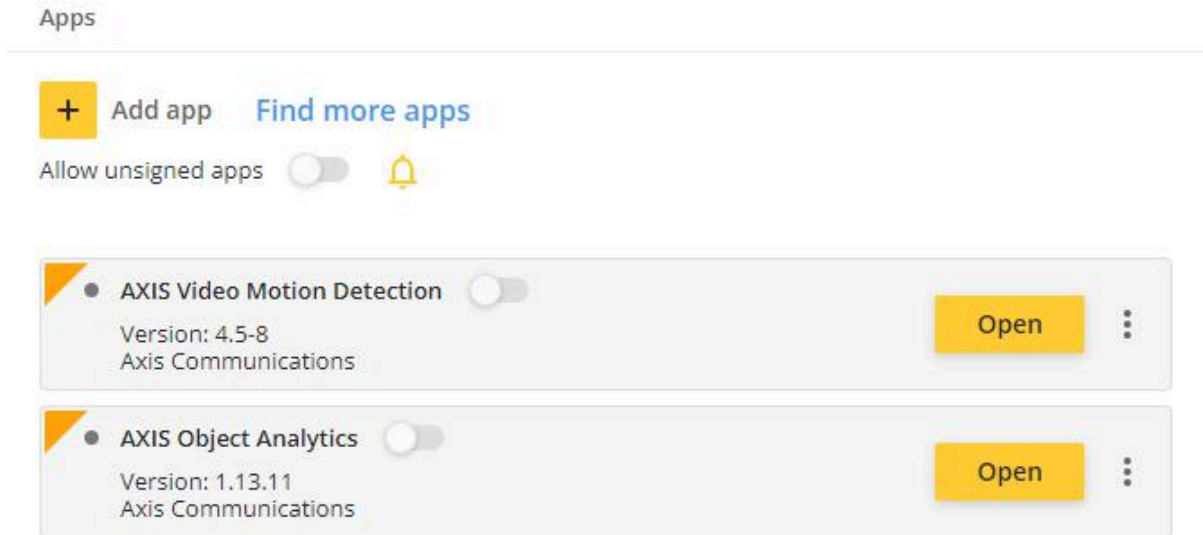
Planned

Changes in AXIS OS 13

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

ACAP related changes:

- **Signed ACAP applications**
From AXIS OS 13.0, the option to allow unsigned applications is removed and only signed ACAP applications are allowed.



VAPIX API parameters that will be removed :

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

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

Running unsigned ACAPs from any previous version of AXIS OS when upgrading to AXIS OS 13 will not be affected and the ACAP will continue to function normally. Only new ACAP installations in AXIS OS 13 are affected.

Why is this change introduced? To increase trust in ACAP applications and comply with international regulations and best practices for secure software delivery.

How can it affect me? New ACAPs to be installed in AXIS OS 13 must be signed, otherwise the ACAP installation will fail.

Security:

- **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. 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.

Add user

Username

New password

Repeat password

Role

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 port

HTTPS port

Certificate

This default behavior is likely to change in order 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.

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 13 or higher.

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*.
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 14 or higher.

Applied

Changes in AXIS OS 12.1

Edge Storage:

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

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

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

Onboard storage

SD card 1 (55.2 GB) ● ⓘ

Free: 100%
 Status: Mounted
 File system: ext4
 Encrypted: No
 Wear: 4%

Safely remove the storage device:

▼ Unmount

Autoformat ⓘ

Write protect ⓘ

Retention time ⓘ

As long as possible

Number of days [1..7000]

Tools

Check Repair

Format Encrypt

Format storage device

Erase all recordings and format the storage device.

File system

ext4 (recommended)

vfat

Cancel Format

Network & Discovery:

- Disabled UPnP discovery protocol**

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

VAPIX API parameter: root.Network.UPnP.Enabled

Network discovery protocols

Bonjour® ● ⓘ

Bonjour name

UPnP® ⓘ

UPnP name

WS-Discovery ⓘ

Save

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

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

Security:

- Basic authentication for HTTPS connections**

Axis devices perform digest authentication when serving both HTTP and HTTPS connections. Since HTTPS connections are preferred for increased security, Axis will change the default behavior so that basic

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

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

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

Changes in AXIS OS 12.0



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

- **Removal of the old web interface**

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

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

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

Security:

- **Disabled HTTP Port 80 redirects**

In previous security penetration tests, Axis was advised to disable HTTP Port 80 redirects in order to enhance security and to prevent information leakage. Currently, Axis devices are configured for HTTPS-only, but the HTTP port 80 redirects are enabled to inform users/clients that communication is not

permitted on port 80 and redirecting them automatically to port 443 instead. Axis will follow the general recommendation provided by third-party penetration test laboratories and will deactivate HTTP port 80 redirects when the device is set to HTTPS-only mode.

No.	Time	UTC Time	Package Delta	Source MAC	Source	Source Port	Destination MAC	Destination	Destination Port	Protocol	Length	Info
1	0.000000	07:43:22.487823	0.000000	Micro-St_e2:48:b5	172.25.201.50	60346	AxisComm_d9:10:b9	172.25.201.191	80	TCP	66	60346 → 80 [SYN] Seq=0 Win=64240 Len=0
2	0.000079	07:43:22.487902	0.000079	Micro-St_e2:48:b5	172.25.201.50	60347	AxisComm_d9:10:b9	172.25.201.191	80	TCP	66	60347 → 80 [SYN] Seq=0 Win=64240 Len=0
3	0.000556	07:43:22.488379	0.000477	AxisComm_d9:10:b9	172.25.201.191	80	Micro-St_e2:48:b5	172.25.201.50	60346	TCP	66	80 → 60346 [SYN, ACK] Seq=0 Ack=1 Win=0 Len=0
4	0.000613	07:43:22.488436	0.000057	Micro-St_e2:48:b5	172.25.201.50	60346	AxisComm_d9:10:b9	172.25.201.191	80	TCP	54	60346 → 80 [ACK] Seq=1 Ack=1 Win=21022 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	0.032733	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	07:43:22.515599	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	0.031115	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=2102 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

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.

The top screenshot shows the 'HTTP and HTTPS' configuration page. Under 'Allow access through', 'HTTPS' is selected. The 'HTTPS port' is set to '443'. The 'Certificate' dropdown is set to 'Axis device ID ECC-P256 (802.1AR)'. A 'Save' button is visible at the bottom right.

The bottom screenshot shows the 'Firewall' configuration page. The 'Activate' toggle is turned on. A table of active rules is shown below:

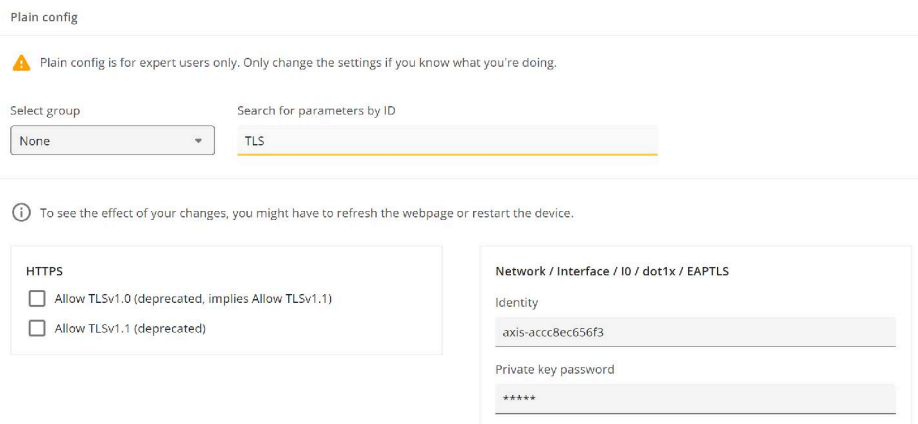
Address	Rule type	Protocol	Port	Policy
172.25.201.150	Filter	TCP	80	Deny

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

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 ACAPs. 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, ACAPs can *embed a custom cryptographic library* to meet their specific needs.

Why is this change introduced? It is obsolete as the active track runs a newer version.
How can it affect me? If you have third party software using OpenSSL 1.1.1, it will not work correctly with AXIS OS 12.0 or higher.

Network & Discovery:

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

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

Why is this change introduced?

- To be completely RFC IPv4 compliant.
- Disable link-local address when it is not used.
- Better user experience for our customers when multiple factory-defaulted Axis devices are placed on the same network simultaneously.
- Increase robustness and detect IP address conflicts.
- **How can it affect me?** Affects during installation, AXIS devices will request IP address from the network it attaches to etc DHCP.

- **Disabled WS-Discovery protocol**

Axis devices currently have the WS-Discovery (WebService-Discovery) protocol enabled in factory defaulted state as additional option for ONVIF-related device discovery. However, the ONVIF interface is not enabled in factory defaulted state which makes the availability of the WS-Discovery protocol by default obsolete. Axis will adapt the default behavior and will disable the WS-discovery protocol in factory defaulted state. This means a user need to enable the WS-discovery protocol if desired.
 VAPIX API parameter: `WebService.DiscoveryMode.Discoverable`



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

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

- **Possibility to disable Basic Device Info VAPIX API** The *Basic Device Information* VAPIX API allows to retrieve general information about the Axis product with no authentication. This is useful for device discovery and profiling during network and application onboarding. Axis will implement an additional VAPIX parameter that will allow the user to disable the basic device information API if needed. The ability for the user to disable this VAPIX API may be considered a behavioral change if unknown.

Why is this change introduced? Provide the ability to reduce the attack surface and information leakage of the device, increasing the overall security resilience of the network.

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

- **Removal of `releaseinfo.cgi`** The `axis-release/releaseinfo.cgi` VAPIX API has been removed. It is recommended to use the Basic Device Information VAPIX API instead, see more info in the *VAPIX Library*. Example output of `axis-release/releaseinfo.cgi`:

```
part=6975649029
version:11.2.53
```

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

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

- **Removal of `getBrand.cgi`** The previously deprecated VAPIX API `axis-cgi/prod_brand_info/getbrand.cgi` has been removed. It is recommended to use the Basic Device Information VAPIX API instead, see more info in the *VAPIX Library*. Please find below an example output of the information that was possible to

receive through getBrand.cgi, all the information is still available and covered in the referenced Basic Device Information VAPIX API.

Example output of getBrand.cgi:

```
Brand.Brand=AXIS
Brand.ProdFullName=AXIS P3265-LV Dome Camera
Brand.ProdNbr=P3265-LV
Brand.ProdShortName=AXIS P3265-LV
Brand.ProdType=Dome Camera
Brand.ProdVariant=
Brand.WebURL=http://www.axis.com
```

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

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

- **Removal of network filter API**

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

IP address filter

Use filter

Policy

Allow

Deny

Addresses ⓘ

[Save](#)

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

```
Network.Filter.Enabled
Network.Filter.Input.AcceptAddresses
Network.Filter.Input.Policy
Network.Filter.Log.Enabled
```

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

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

Edge Storage:

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

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

Add network storage

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 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?

ACAPs that do not use root-privileges are not affected.

ACAPs 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.

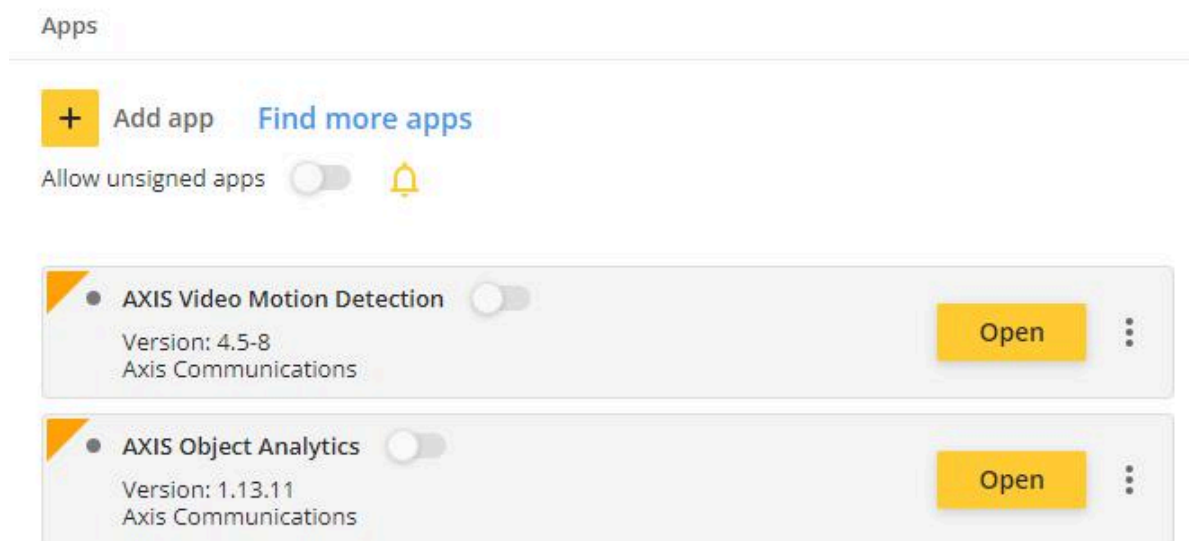
Possible scenarios where failures could be expected are:

The ACAP 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 from being installed or run.

The pre-uninstall script may be using root-privileges, which may prevent ACAP data from being cleaned up at installation.

The ACAP tries to access file system resources or functionality that is locked behind root-privileges. The ACAP applications 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 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 ACAPs, 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 ACAPs from any previous version of AXIS OS when upgrading to AXIS OS 12 will have no impact and the ACAP 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 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 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**
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.

- **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.

- **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.

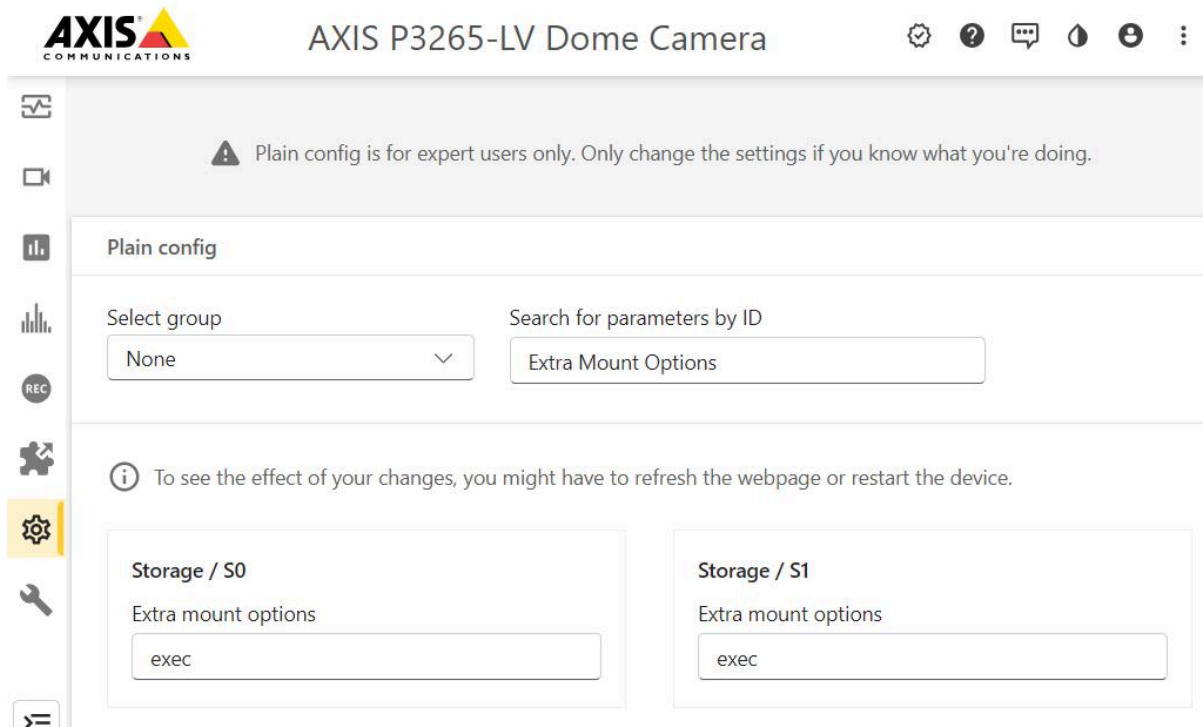
Applies to: AXIS D2210-VE, AXIS M3215-LVE, AXIS M3216-LVE, AXIS M5526-E, AXIS P1465-LE, AXIS P1465-LE-3, AXIS P3265-LV/-LVE/-V and AXIS P3265-LVE-3

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 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 ACAPs 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? ACAPs requiring file execution on edge storage may not function properly if the device is not configured accordingly.

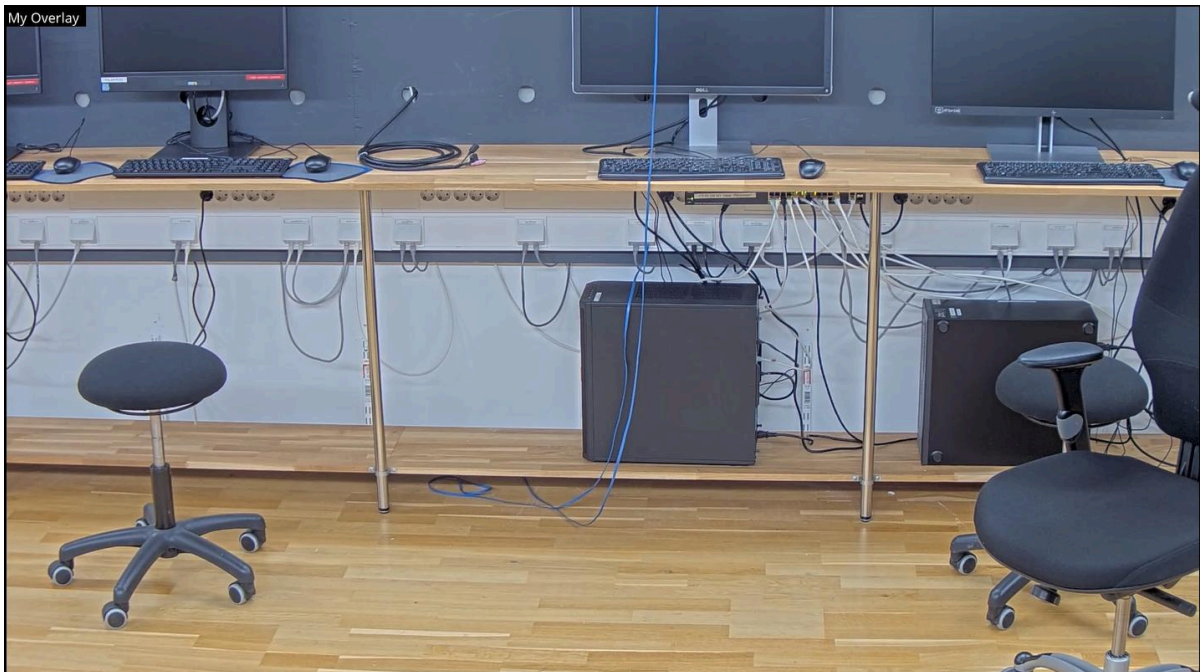
API changes:

- **Rate Control changes for RTSPAs** 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.l#.RateControl.TargetBitrate are deprecated from now. No changes are made when it comes to Average Bitrate (ABR).

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



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

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

- **Added path restrictions for dynamicoverlay.cgi**
The *Dynamic Overlay* VAPIX API that allows to configure the path to the overlay image to display has been limited to `/etc/overlays/`. It is not possible anymore to alter the path through VAPIX API.

Why is this change introduced? Supporting to alter the path trough API is not best practice and keeping it might be a security threat.

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

- **Changes in dynamicoverlay.cgi**
Optional values, "source" and "sensor" will be removed from the *Dynamic Overlay* in AXIS OS 12.

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

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

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

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

preview_on
 preview_off
 query list
 query position
 ptpolygon
 imagerotation
 imageresolution
 zoomlowlimit

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

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

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

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

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

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

AXIS OS 12.0 and higher

```

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

```

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

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

- **Updating terminology from "Vehical" to "Vehicle" for ONVIF**

Due to an error in the ONVIF Metadata Spec, "Vehicle" has been incorrectly represented as "Vehical", in the Analytics Scene description. As of AXIS OS 12, the correct term "vehicle" will be used instead. See code example at *Changes in the analytics metadata stream in AXIS OS 12.0*.

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

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

- **Updating terminology from "Bicycle" to "Bike" in VehicleType for ONVIF**

Currently in the Analytics Scene description, the term "Bicycle" is used to describe both a bicycle and a motorcycle within the context of "VehicleType". As of AXIS OS 12.0, "Bike" will be used instead of "Bicycle" to describe both bicycles and motorcycles according to the ONVIF Standard, and it will be represented as an "ObjectType".

See code example at *Changes in the analytics metadata stream in AXIS OS 12.0*.

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

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

- **Removal of the lightcontrol web service API**

The lightcontrol web service API (implemented in ws/wsd/impl/ali) has been deprecated for many years and is replaced by the lightcontrol-cgi JSON API. Information about this change has been sent out previously to partners.

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

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

Product specific:

- **Remove support for AXIS T6101/T6112**

Support for AXIS T6101 and AXIS T6112 will be removed. Read more about compatible products on axis.com

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

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

Changes in AXIS OS 11

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

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

Security:

- **Remove access via FTP protocol**

Since AXIS OS 11.1, we have removed the possibility to access the device via the FTP protocol, to increase overall minimum cybersecurity level.

For troubleshooting purposes it is recommended to use secure SSH access. Note that upload from the device to an FTP server is still possible. For more information, visit SSH access in the AXIS OS Knowledge base.

Why is this change introduced? To increase overall security.

How can it affect me? If you have third party software using this feature, it will not work correctly with AXIS OS 11.1 or higher.

- **Removed support for proxy SOCKS version 4 and 5**

Since AXIS OS 11.0, support for proxy SOCKS version 4 and 5 has been removed.

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

How can it affect me? If you have third party software using this feature, it will not work correctly with AXIS OS 11.0 or higher.

- **No dedicated root user in factory defaulted state**

Since AXIS OS 11.5, no dedicated root user is pre-configured in factory defaulted state. To ease O3C-related integrations and to allow time to adapt, Axis made a modification that currently creates this root user for O3C onboarding/integration. From LTS 2024, O3C integrations shall not rely on the previously available admin user named "root". If a separate (admin) user is deemed necessary for some purpose, this user shall be specifically created during the initial onboarding/integration.

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

How can it affect me? If you have third party software using root as hardcoded username, it will not work correctly with AXIS OS 11.5 or higher unless you create a user root.

- **Root-privilege is disabled in factory defaulted state**

Root-privileged access is disabled by default in Axis products and ACAP applications to increase ACAP confidentiality by better protecting their data and secrets, to prevent information leakage and to increase AXIS OS system integrity by removing system-wide root-privileged access for users and applications. In AXIS OS 11, this can still be enabled by parameter if required, see screenshots below for reference:

Apps

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

Allow unsigned apps Allow root-privileged apps

● **AXIS Video Motion Detection**

Version: 4.5-8
Axis Communications

Open ⋮

● **AXIS Object Analytics**

Version: 1.13.11
Axis Communications

Open ⋮

SSH accounts

+ [Add SSH account](#) Restrict root access Enable SSH

Account	Comment
root	root

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

Why is this change introduced? To increase the security on the device.
How can it affect me? Affected 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	- -
11.6	September 2023	-
11.8	January 2024	- -
11.11	June 2024	-
LTS 2024	H2 2024	Support: 2024-2029. Can be used as a stop-gap solution until an ACAP application is fully adapted. - -

VAPIX API changes:

- **PTZ VAPIX API version 2**
Since AXIS OS 11.0, there is a new version of the PTZ VAPIX API. For more information, visit the *VAPIX library*.
- **Removal of date.cgi**
Since AXIS OS 11.0, the date.cgi has been removed and replaced by time.cgi. For more information, visit the *VAPIX library*

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

How can it affect me? If you have third party software using this API, it will not work correctly with AXIS OS 11.0 or higher.

- **Support removed for BMP format**
Since AXIS OS 11.0, support to request an image in BMP file format has been removed. For more information, visit the *VAPIX library*.

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

How can it affect me? If you have third party software using this feature, it will not work correctly with AXIS OS 11.0 or higher.

- **Removed support of recording mediaclip through Mediaclip API**
Since AXIS OS 11.0, support to record a mediaclip using the Mediaclip API has been removed. For more information, visit the *VAPIX library*.

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

How can it affect me? If you have third party software using this feature, it will not work correctly with AXIS OS 11.0 or higher.

- **Parameters in the root.PTZ parameter group changes**
Since AXIS OS 11.0, changed access for a number of parameters in the root.PTZ parameter group. For more information, visit the *VAPIX library*.

Why is this change introduced? Due to architectural changes.

How can it affect me? If you have third party software using this, it will not work correctly with AXIS OS 11.0 or higher.

- **Removal of edit.cgi**
Since AXIS OS 11.1, the edit.cgi has been removed. For more information, visit the *VAPIX library*.

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

How can it affect me? If you have third party software using this API, it will not work correctly with AXIS OS 11.1 or higher.

- **Removal of libvidcap**
The libvidcap has been removed. Use Video capture API instead. For more information, visit the *ACAP developer guide*

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

How can it affect me? If you have third party software using this API, it will not work correctly with AXIS OS 11.1 or higher.

- **Removal of overlay-cgi.**
The overlay-cgi has been removed in AXIS OS 11.10. It is recommended to use overlayimage-cgi instead, see more info in the *VAPIX Library*.

VAPIX API parameter affected:

call_overlay_upload.cgi
call_overlay_del.cgi
call_overlay_set.cgi
create_overlay.cgi
overlay_list.cgi
overlay_image_formats.cgi

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

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

Other changes:

- **Removal of the built in motion detection**

In AXIS OS 11.2 the old built in motion detection, also known as VMD1, was removed.

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

How can it affect me? If you have third party software using this application, it will not work correctly with AXIS OS 11.2 or higher.

- **Removed installable decoder AAC**

Since AXIS OS 11.0, the installable audio decoder for AAC has been removed and is no longer downloadable from the cameras web interface.

- **Removed installable decoder H.264**

Since AXIS OS 11.0, the installable decoder for H.264 has been removed and is no longer downloadable from the cameras web interface.

Next AXIS OS version

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

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

AXIS OS 12.4

Scheduled for: April 2025

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

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

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

Applies to: AXIS M7116 and AXIS P7316

Current AXIS OS version

AXIS OS 12.3

Release date: February-March 2025

- **Features for all products**
 - Added Time API to Device Configuration API, as beta.
 - Updated the Certificate, Firewall, SNMP, and LLDP APIs in the Device Configuration API to remove the beta designation, indicating they are now stable and ready for production use.
 - IPv6 support is now enabled by default, which includes IPv6 Link-Local Address, DHCPv6, and Router Advertisement capabilities.
- **Cybersecurity updates**
 - Updated cURL to version 8.11.0, addressing *CVE-2024-9681*.
 - Updated cURL to version 8.11.1 to increase overall cybersecurity level.
- **Analytics updates**
 - AXIS Object Analytics: Added the ability to copy the scenario ID in the web interface.
 - AXIS Scene Metadata: Reduced the frequency of sending empty frames from Analytics Scene Description. If no objects are detected in the scene, an empty frame is now sent every other second (instead of approximately 10 times per second). This change affects both the ONVIF producer 'Analytics Scene Description' and the message broker topic 'com.axis.analytics_scene_description.v0.beta'. Applies to: All products with AXIS Scene Metadata support.
- **Product specific features and changes**
 - Hardware modifications have been made to proactively prepare for the new NDAA 23 regulations that will be required in 2028. You will find more information about NDAA Compliance on *axis.com*. In AXIS OS knowledge base, you will find more about the *hardware changes*. The hardware ID can be found in Plain config > Properties > System > Hardware ID.
 - Products with Hardware ID A16, A17 and A18 only support active track 12.3.XX and later, as well as coming LTS 2024 11.11 version and LTS 2022 10.12 version, and later.

Applies to: AXIS M5074, AXIS M5075 and AXIS M5075-G
 - AXIS Image Health Analytics is added as pre-installed application.

Applies to: AXIS Q1686-DLE
 - Add unknown object filter which hides all tracks that are not classified as "human" or "vehicle"

Applies to: AXIS D2110-VE, AXIS D2210-VE, AXIS Q1656-DLE and AXIS Q1686-DLE

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?

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?

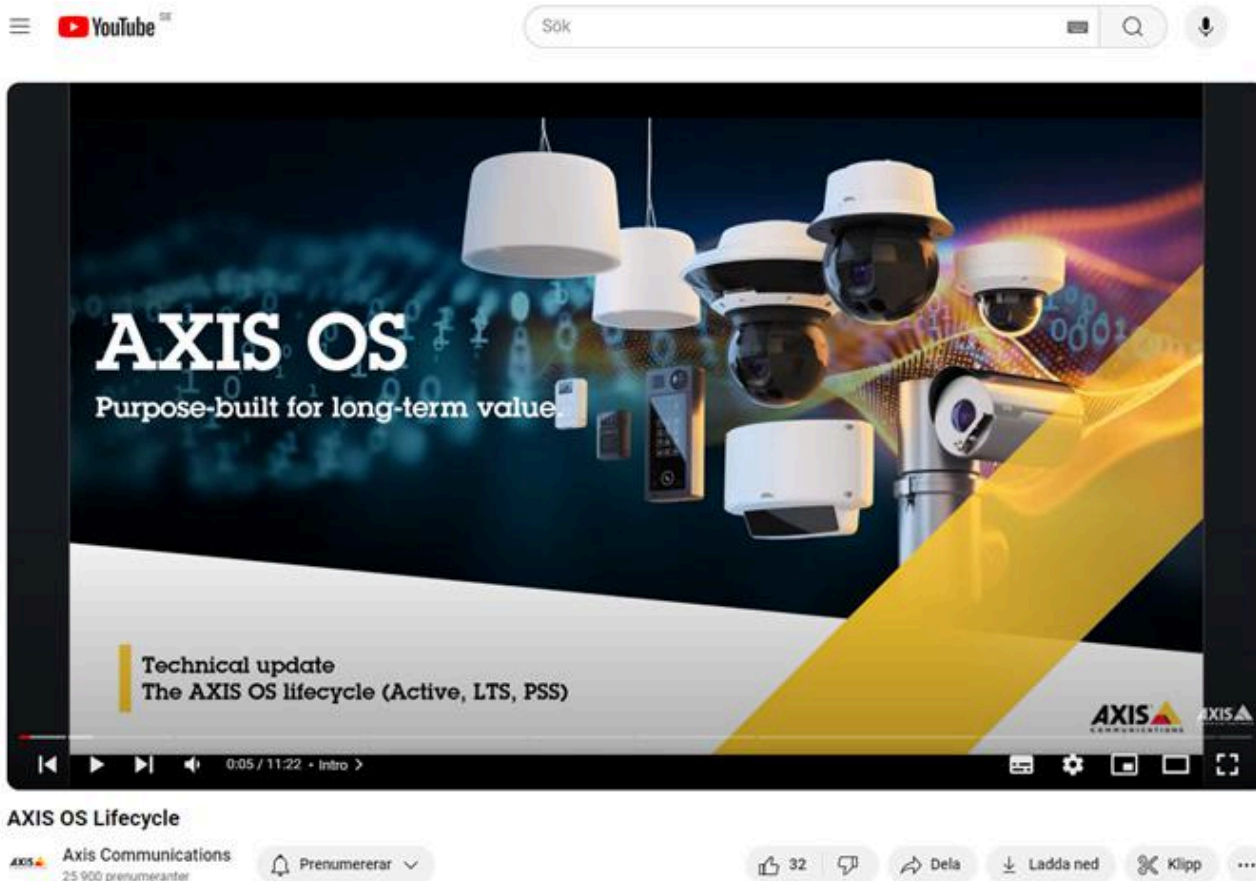
The Axis SBOM contains information about Axis-Proprietary and Opensource software used to assemble AXIS OS. The Axis SBOM can be used by third party vulnerability scanners to highlight known vulnerabilities in software packages. A vulnerability that applies to a certain module or feature in a software 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.



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

Active track

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



Long-term support track

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

Product-specific support

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

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

Suggested track

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

Highest level of cybersecurity – AXIS OS active

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

Need for specific new features – AXIS OS active

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

Satisfied with current features and cybersecurity level – AXIS OS LTS

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

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

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

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

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

Make sure your VMS is validated before upgrading.

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

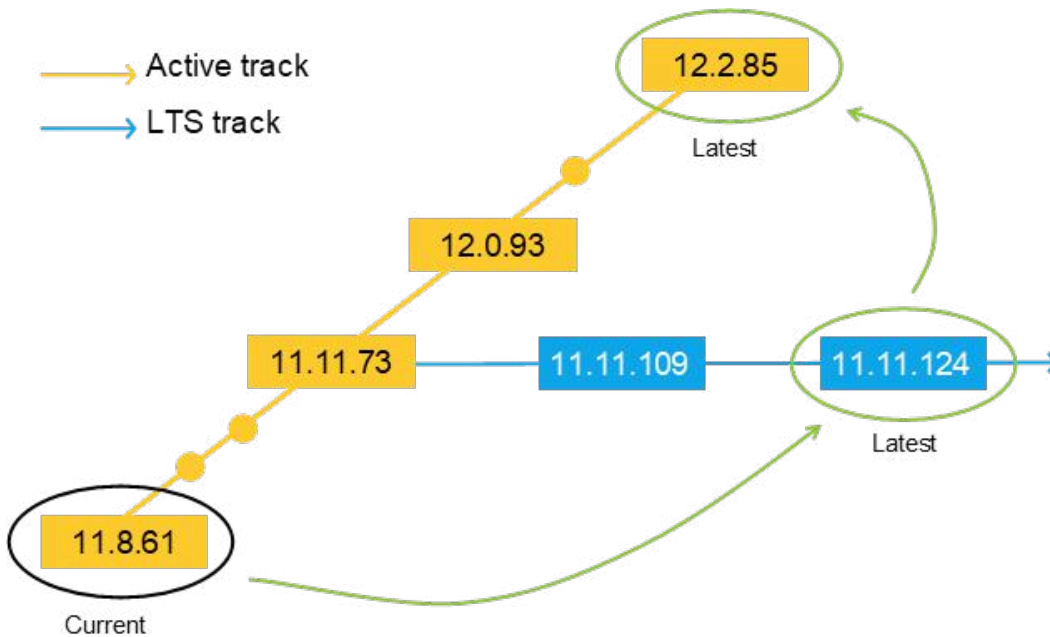
Verify with your VMS and ACAP provider which versions they test and recommend. AXIS OS LTS is the recommended choice for optimal compatibility.

Upgrade path

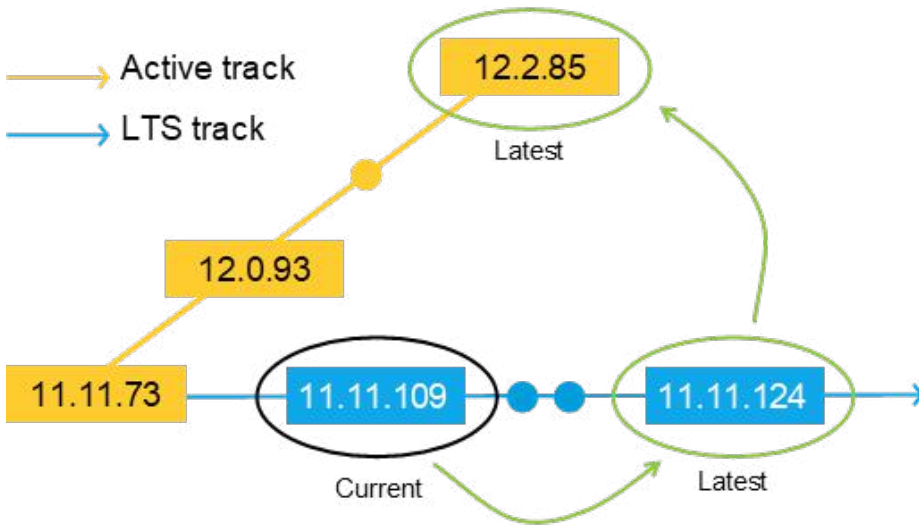
You can upgrade your devices using the web interface or various device management tools, such as AXIS Device Manager, AXIS Camera Station Pro, and AXIS Camera Station Edge. AXIS Device Management Extend simplifies the upgrade process by providing built-in backend upgrade paths. Read more about *How to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

Here are some recommendations for how to upgrading:

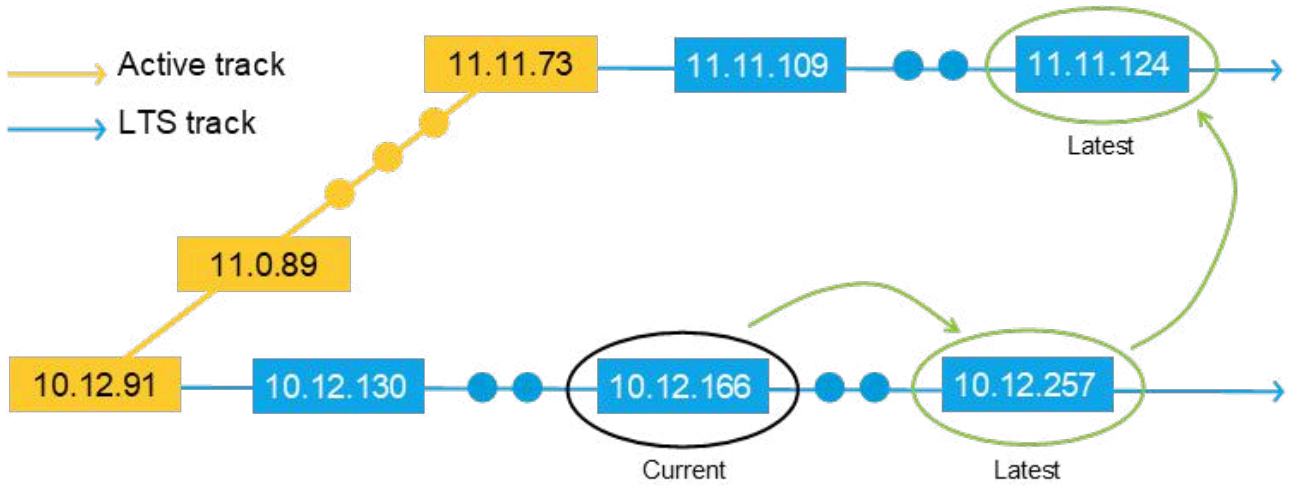
- **Upgrading from an older active track to the latest active:** Upgrade to the latest version of the intermediate LTS.



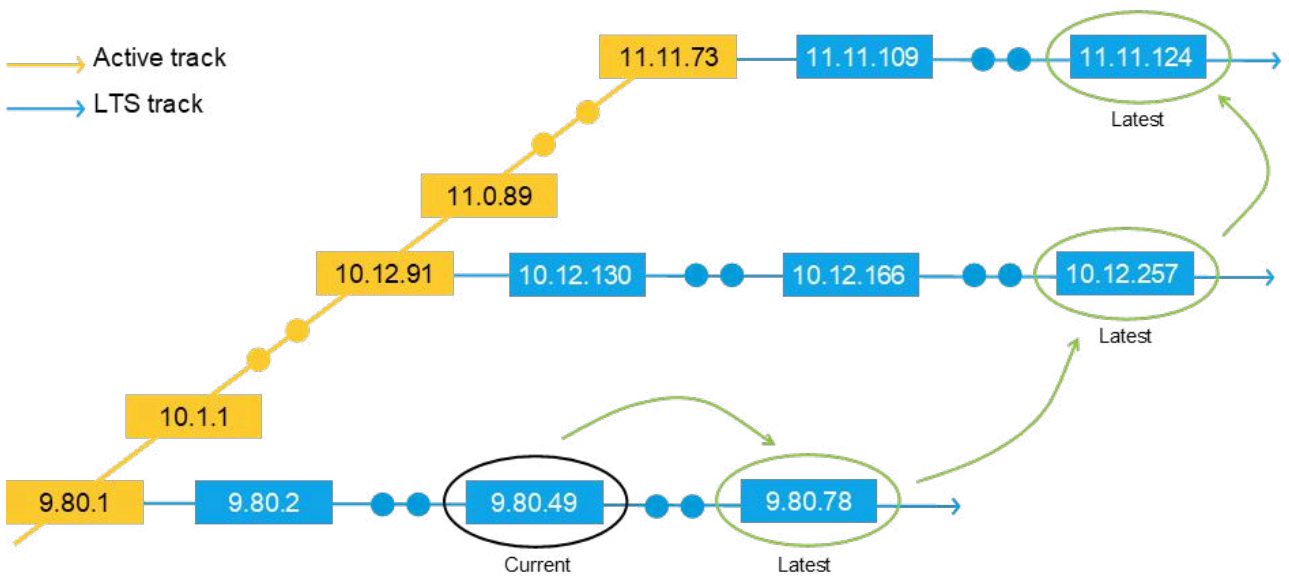
- **Upgrading from the latest LTS track to the active track:** Start by upgrading to the latest version of your current LTS.



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



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



Considerations

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

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

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

Stay current with AXIS OS upgrades

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

Selecting the right latest version

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

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

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

Additional Q&A

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

General recommendations

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

Always use the latest supported AXIS OS version:

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

Simplify software updates and lifecycle planning using device management tools:

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

Stay up-to-date on cybersecurity recommendations:

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

Upgrading between AXIS OS LTS tracks:

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

Verification of new releases:

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

Downloading AXIS OS

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

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

Download device software

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

🔍

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

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

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

AXIS OS versioning

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

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

11.5.64

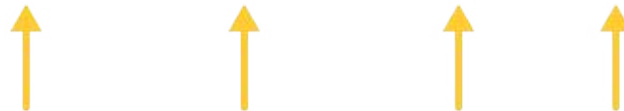


Major release version Minor release version Patch number

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

Previous versioning .

7.10.1.2



Year:	Yearly release:	Major release version	Minor release version
6 = 2016	10 = release 1		
7 = 2017	20 = release 2		
8 = 2018	30 = release 3		
9 = 2019	40 = release 4		
10 = ...	50 = ...		
	(X)5 = PFW		

AXIS OS Support

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

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

What is required to get the full support period?

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

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

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

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

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

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

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

Why do some products lack an AXIS OS support date?

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

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

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

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

Please follow and monitor the .

Example of AXIS OS Support:

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

