AXIS OS

Release notes

AXIS OS Lifecycle guide | *AXIS OS Knowledge base* | *AXIS OS YouTube playlist*| *AXIS OS Hardening guide* | *Security advisories*

About

Welcome to the AXIS OS Release notes, a repository for the release notes about new features, security and other improvements for different AXIS OS tracks. *AXIS OS* is the Linux-based operating system used in most of your Axis network devices. It's purpose-built to live up to the most important criteria(s) for network devices: high standards for cybersecurity, ease of integration, quality, and long-term value.

Note

- The release notes provide details about the new features, cybersecurity patches and reported customer issues. Technical improvements to the device software are mentioned as general improvements without specifics since they are not relevant to customers.
- Only the latest AXIS OS version in each track is supported.
- Some AXIS OS versions may no longer be available on axis.com. See the *AXIS OS lifecycle guide* for more information.
- Release notes for the archived AXIS OS releases are accessible in the *AXIS OS Release Notes Archive*.
- More information about the AXIS OS upgrade recommendations and upgrade strategy can be found in the *AXIS OS Lifecycle guide*.
- In the *AXIS OS Knowledge base* you will find more information about AXIS OS features and functionality.

AXIS OS 13

Go to *Products on active track - AXIS OS 13, on page 87* for a list of products on this track.

AXIS OS 13.0

Note

The release of AXIS OS 13.0 is delayed and is estimated to be at the end of October.

Breaking changes

Read more about the breaking changes at *Changes in AXIS OS 13* in AXIS OS lifecycle guide.

- Switched to 64-bit time types to enable Y2038 compatibility.

  Applies to: All products based on *AXIS ARTPEC-7, on page 85* and *I.MX 6SX, on page 87* that have AXIS OS 13.
- Password complexity enforcement is enabled by default for new/edited accounts created via SSH, VAPIX, ONVIF and SNMP profile selection. This behavior cannot be disabled. This change also applies to the web interface.
  - Profile 1: Length-based according to NIST recommendations, whereas 15 characters will be required without further complexity requirements.
  - Profile 2: Complexity-based requiring 12 characters minimum, including at least 1 numbers, 1 capital, 1 small, 1 special.
- Signed Video is enabled by default.
- HTTPS-only is enforcement as default. To use HTTP port 80, you must enable it first.
- Removed the UPnP discovery protocol.
- The AXIS OS recording system has been updated. The following changes may affect integrations: .
  - Recording IDs are limited to 24 hours, with one hour as the default. Continuous and long-running triggered recordings can span multiple IDs.
  - `axis-cgi/record/list.cgi` returns more recording IDs. Use matching start and stop times to identify consecutive IDs in the same recording sequence. Export and RTSP playback apply to a single recording ID.
  - The updated recording system does not support inserting product information and timestamps into H.264 header data.
  - `axis-cgi/record/remove.cgi` returns an error when removing an ongoing recording. Stop the recording before removing it.
  - Recording files use a new on-disk location, naming scheme, and format. ACAP integrations must use the public recording D-Bus APIs instead of direct file access.
  - The RTSP `failoverrecordinglength` URL option is no longer supported.
  - The `EstimatedFileSize` property is removed from `axis-cgi/record/export/properties.cgi`.
  - The `root.StreamCache.Size` parameter is removed on non-video products
- ACAP application changes
  - *ACAP applications must be signed*. If the application was originally installed in AXIS OS 12.7 or earlier, it must be reinstalled on AXIS OS 12.8 or later before upgrading to AXIS OS 13.
  - To install unsigned ACAP applications during development, developers must request and install the *Developer Mode application*. It also enables SSH access for ACAP application users through a dynamic user. Disabling Developer Mode uninstalls all unsigned ACAP applications and removes the SSH users created for them.
  - ACAP applications must include a *manifest.json file* to define their configuration, as the legacy package.conf is no longer supported.

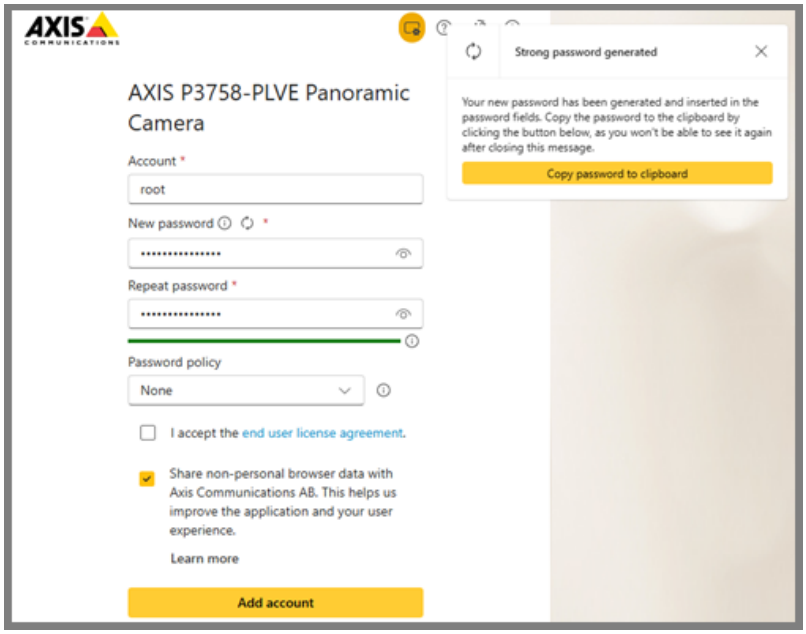
  - ACAP applications can no longer request support from the host system for *running containers*. The Computer Vision SDK is no longer supported.
  - Every ACAP application must *declare the range of AXIS OS versions* it is compatible with and will be prevented from being installed on AXIS OS versions outside of that range.
  - ACAP applications using DLPU resources must declare this usage in *manifest.json*. This enables correct resource management and DLPU usage reporting in the WebGUI and server reports.
  - ACAP applications are only allowed to access *D-Bus methods* and *groups* required by the official APIs. ACAP applications must run either as an application-specific user or as the sdk user.
  - ACAP applications can no longer request support from the host system for running containers.
  - Removed the ability to install and run ACAP applications on SD card.
  - Installation of an *ACAP application will fail* if it contains a post-install script that exits with a non-zero exit code, or if the script runs for too long.
- The legacy Camera Tampering detector is removed. Its functionality is replaced by AXIS Image Health Analytics, which provides more advanced and reliable capabilities.
- New light tamper detector, for those products that do not support AXIS Image Health Analytics.Applies to: AXIS F9104-B, AXIS F9104-B Mk II, AXIS F9111, AXIS F9111-R Mk II, AXIS F9114, AXIS F9114-B, AXIS F9114-B Mk II, AXIS F9114-R Mk II, AXIS I8016-LVE, AXIS I8116-E , AXIS I8307-VE, AXIS I8407-LVE, AXIS M1055-L, AXIS M1075-L-Mk II, AXIS M2035-LE, AXIS M2036-LE, AXIS M3057-PLR Mk II, AXIS M3085-V, AXIS M3086-V, AXIS M3088-V, AXIS M3125-LVE, AXIS M3126-LVE, AXIS M3128-LVE, AXIS M3905-R, AXIS M3945-R, AXIS M4215-V/-LV, AXIS M4216-V/-LV , AXIS M4218-V/-LV, AXIS M4225-LVE, AXIS M4227-LVE, AXIS M4228-LVE, AXIS M4348-PLR, AXIS M5000, AXIS M5000-G, AXIS M5526-E, AXIS M7104, AXIS M7116, AXIS P1245 Mk II, AXIS P1265 Mk II, AXIS P1275 Mk II, AXIS P1468-XLE, AXIS P1518-E/-LE, AXIS P3735-PLE, AXIS P3737-PLE, AXIS P3738-PLE, AXIS P3747-PLVE, AXIS P3748-PLVE, AXIS P3818-PVE, AXIS P3827-PVE, AXIS P3905-R Mk III, AXIS P3925-LRE, AXIS P3925-R, AXIS P3935-LR, AXIS P3945-R, AXIS P3947-R, AXIS P4705-PLVE, AXIS P4707-PLVE, AXIS P4708-PLVE, AXIS P7304, AXIS P7316, AXIS Q1809-LE, AXIS Q1961-TE, AXIS Q1961-XTE, AXIS Q1971-E, AXIS Q1972-E, AXIS Q2101-TE, AXIS Q2111-E, AXIS Q2112-E, AXIS Q3839-PVE, AXIS Q3839-SPVE, AXIS Q4809-PVE, AXIS Q8752-E, AXIS Q8752-E-Mk II, AXIS Q9307-LV, AXIS V5925 and AXIS V5938
- Removed the ACAP application AXIS Removed Object Detection. The functionality is not replaced.
- AXIS OS image file compression - changed the device software image format from a gzipped tar archive to a zstd compressed tar archive for better compression rate.
- HTTP(S) server will handle authenticating when RTSP streams are requested that shall be tunneled over HTTP(S).
- Removed .larod model, format, as well as Larod version 1 & 2.
- Changed the device software image format from a gzipped tar archive to a zstd compressed tar archive for better compression rate.
- Implemented prevention of Stack Execution.
- Removed loopback interfaces to reduce complexity and increase performance.
- The current default behavior for continuous pan has been changed to automatically stop after 10 minutes.
- Message-Broker has be removed and replaced by *device data hub*.
- Removed the statistics field from *VDO Stream Info*.
- API changes
  - Removed API endpoint for Camera Tampering detector.
  - Removed `ptzcoordcalc.cgi`.
  - Removed `upload_file.cgi`.
  - Removed `local_del.cgi`.

- Removed `local_list.cgi`.
- Removed `file_upload.cgi`.
- Removed `record.cgi`.
- Removed `stop.cgi`.
- Removed `Time.POSIXTimeZone` and `Time.DST.Enabled` parameters in `param.cgi`.
- Removed `PTZ.Various.V#.HomePresetSet`.
- Removed `PTZ.Support.S#.JoyStickEmulation` and `PTZ.Support.S#.GenericHTTP` PTZ.Support.
- Removed `ptzcoordcalc.cgi`.
- Removed legacy `Image.I#.Appearance.Rotation` and `Image.I#.Appearance.AutoRotationEnabled` parameters.
- Removed legacy privacy mask type parameter `Image.PrivacyMaskType`.
- Removed `vdo_frame_get_is_last_buffer`, `vdo_frame_get_fd` and `vdo_frame_get_opaque` in the VDO ACAP API.
- Removed non-functional enums `VdoOverlayAlign`, `VdoOverlayColor` and `VdoOverlayTextSize` in the VDO ACAP API.
- Removed `uint16_t` for `VDO_TIMESTAMP` in VDO ACAP API.
- Removed legacy `Image.I#.Appearance.Rotation` and `Image.I#.Appearance.AutoRotationEnabled` parameters.
- Removed the unofficial SSH v1 API.
- Removed the Layout VAPIX API.
- Removed HTTP Network Authentication VAPIX API.
- Removed legacy SNMP VAPIX API.
- Removed legacy Streaming VAPIX API.
- Removed PTZ-Autotracking 2.x legacy URLs.
- Removed legacy parameter `audiooutput` from Media clip API.
- Removed the UPnP discovery protocol.
- Removed legacy parameters in param.cgi parameter configuration of the Storage group.
- Changes to View Area VAPIX API, removed the complex dependency between view areas and digital PTZ and improved user experience.
- Replaced of the Best Snapshot Configuration VAPIX API. The name of the API will be changed to "object snapshot" to align with established naming conventions.
- Removed the tenBandGraphicDspEqualizer Audio Mixer API. Its replacement is the tenBandGraphicEqualizer Audio Mixer API.
- Non-functional enums, `VdoOverlayAlign`, `VdoOverlayColor` and `VdoOverlayTextSize`, in the VDO ACAP API are removed.
- Updated `receive.cgi` API for HTTP/1.1 compliance. The data will now be sent in multiple chunks, each chunk preceded by a length. See *RFC 9112 7.1*.
- HTTP(S) server will handle authenticating when RTSP streams are requested that shall be tunneled over HTTP(S). The default configuration when factory defaulted in AXIS OS 13 are: `System.HTTPAuthRTSPOverHTTP="yes"` and `Network.RTSP.AuthenticateRTSPOverHTTP="no"`. Updating from AXIS OS 12 or lower towards AXIS OS 13 and higher should not change the parameters.

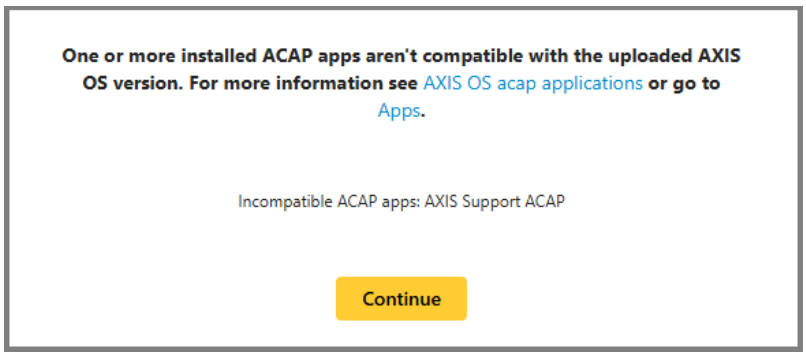
Features for all products

- Web interface

- Added the possibility to autogenerate password and ability to copy the password to clipboard.



- Improved upgrade failure message in the web interface. This is one of the new messages:



- Added a dedicated Night mode settings page that brings all night-related settings together in one place.
- Introduced tab navigation do decrease the need for scrolling and improve the user experience.
- Added the possibility to configure exclude areas for PVM scenarios.
- Enrollment over Secure Transport: The maximum number of EST profiles are shown.

- Object Store Recording (OSR) is now used as default for recordings.
- Added OPUS as encoder and decoder when using ONVIF streaming and audio backchannel.
- Open Set is to be released as a preview which requires Occupancy in Area to include static objects.
- Updated tzdata to version 2026c to ensure accurate time zone and daylight saving time transitions.
- Added support for brute force protection configuration in Firewall API v1. Read more *here*.
- Added support for Precision Time Protocol (PTP) software timestamping, enabling synchronization on devices without hardware timestamping support. Devices with hardware timestamping capabilities continue to use hardware mode by default for optimal accuracy.
- Added support for specifying the NTP max distance value, this allows the device to accept NTP servers with higher root dispersion than the default threshold allows.
- Added both radar, and audio pairing for speaker and microphone, to networkpairing_v1 API.
- Added support for edge storage in recording group v2 API.

- Data transformation API is no longer in beta, meaning they are now stable and ready for production use. Read more *here*.

Cybersecurity updates

- Updated OpenSSH to version 10.4 to increase overall cybersecurity level.
- Updated cURL to version 8.21.0 to increase overall cybersecurity level.
- Added support for Post-Quantum Crypto (PQC) ML-KEM hybrid scheme for TLS 1.3 communication providing store now, decrypt later protection for increased cybersecurity. Supporting clients can make use of it for e.g. HTTPS, MQTT, RTSPS, 802.1X and other services.
- Addressed *CVE-2026-9063*, *CVE-2026-13409*, *CVE-2026-14542*, *CVE-2026-14543* and *CVE-2026-63282*. These CVEs will be externally disclosed on 10 November 2026, more detailed information will follow then. For more information, please visit the *Security advisories*.
- Addressed *CVE-2026-4757* and *CVE-2026-6505*. For more information, please visit the *Security advisories*.
- Addressed *CVE-2026-46433* in `lldpd version 1.0.17`.
- Addressed *CVE-2026-56109* in `alsa-lib version 1.2.15.3`.
- Addressed *CVE-2026-39879* in `syslog-ng version 4.11.0`.
- Addressed *CVE-2026-50292* in `libinput version 1.30.2`.
- Addressed *CVE-2025-13151* in `libtasn1 version 4.21.0`.
- Addressed *CVE-2026-11979* in `libxml2 version 2.15.3`.
- Addressed *CVE-2026-26157*, *CVE-2026-26158* and *CVE-2026-29004* in `busybox version 1.38.0`.
- Addressed *CVE-2026-58015* in `glib version 2.88.1`.
- Addressed *CVE-2026-58016* in `glib version 2.89.1,`.
- Addressed *CVE-2026-58010*, *CVE-2026-58011*, *CVE-2026-58012*, *CVE-2026-58013* and *CVE-2026-58014* in `glib version 2.88.2`.
- Addressed *CVE-2026-40612*, *CVE-2026-41256*, *CVE-2026-41257*, *CVE-2026-43894*, *CVE-2026-43895*, *CVE-2026-43896* and *CVE-2026-44777* in `jq version 1.8.1`.
- Addressed *CVE-2026-56131*, *CVE-2026-56403*, *CVE-2026-56404*, *CVE-2026-56405*, *CVE-2026-56406*, *CVE-2026-56407*, *CVE-2026-56408*, *CVE-2026-56409*, *CVE-2026-56410*, *CVE-2026-56411* and *CVE-2026-56412* in `libexpat version 2.8.1`.
- Addressed *CVE-2026-72522* in `libexpat version 2.8.2`.
- Updated `quick-xml to version 0.39.2`, addressing *RUSTSEC-2026-0194* and *RUSTSEC-2026-0195*.
- Updated `ca-certificates`, addressing *CLSA-2026-1773684237*.
- Improved system security in the system's naming service by using safe memory handling functions, ensuring compliance cybersecurity standards.
- Updated Remote Syslog to utilize stronger encryption ciphers for improved data transmission security.

Analytics updates

- Improved the native analytics capability in object tracking used in e.g. AXIS Object Analytics and AXIS Scene Metadata:

  Applies to: All products based on *Ambarella CV25, on page 86*, *Ambarella CV75, on page 86*, *AXIS ARTPEC-8, on page 84* and *AXIS ARTPEC-9, on page 83*

  - Reduce the number of false tracks from duplicated overlapping detections
  - Keeps object tracks better for fast moving objects, e.g. vehicles on highway
  - Reduce effect of false positive tracks floating away when predicted.

- AXIS Object Analytics
  - Added Analytic space - dashboard for all native analytic on camera
  - Added Status field for scenarios
  - Corrected issues with overlays during configuration
  - Added new Device Configuration Scenario API
  - Added Heatmap feature to the new analytic space

    Applies to: All products based on *AXIS ARTPEC-9, on page 83*
- AXIS Perimeter Defender

  Applies to: AXIS Q1971-E, AXIS Q1972-E, AXIS Q2111-E, AXIS Q2112-E and AXIS Q6411-LE Kit
  - Added as pre-installed application.
  - Added Vapix/Onvif Diagnostic Event for "analytics stopped".
  - Added Audit log.
  - Corrected an issue with scenario zone display scale.
  - Corrected an issue when log or telemetry files could not be written.
  - Improved cybersecurity in API calls.
  - Improved stability.
- AXIS License Plate Verifier

  Applies to: AXIS P1485-LE Kit, AXIS P1486-LE-Kit, AXIS P3285-LVE Kit and AXIS Q1800-LE-3
  - Corrected FÜ symbol reading in German 2-line license plates.
  - Corrected Swiss plates with VS series reading (were reading as WS often).
  - Added DX format series for Poland plates.
  - Corrected US Pennsylvanian plates reading of the new 0 symbol.
  - Corrected capture_timestamp in UPDATE events.
  - Corrected an issue with plates added to a list that would have had an incorrect "Created" timestamp.
  - Corrected an issue with From and To timestamp filters when Last hour is applied.
  - Switched to vdo_frame_get_utc_timestamp API.
  - Corrected license error handling when a license is not activated.
  - Corrected an issue with Secure Entry when access is granted for not assigned AOI when Direction = Any.
  - Corrected an issue when clicking on "Reset configuration", does not return Controller and Relay settings to defaults.
  - Corrected an issue with A9210 Network I/O Relay Module that fails the connection.
  - Corrected special symbols handling in input fields (Test integrations).
  - Corrected Push Events when inserting vehicle_info.coordinates.
  - Corrected the Setup Assistant when applying new rotation values that are not applied immediately after setting.
  - Corrected Import list operation which did not filter out license plates containing invalid characters.
  - Corrected UTMC: fix InstanceId field according to the schema (UInteger).
  - Corrected UTMC: add MMR (Make Model Recognition) related fields even when no MMR recognition results.

- Added Conditional event status handling to UTMC.
- Corrected when importing large licens plate list files which caused critical error.
- Corrected import lists with licens plates that contains only numerical symbols.
- Corrected duplicate check that causes data loss during an import of the list.
- Corrected List Synchronization when the main camera contains large amount of plates.
- Corrected incorrect Content-Type headers in multiple ALPV APIs.
- Corrected infinite loading of the 'Apply filters' button in the Search.
- Corrected sending '%' symbol in Test integrations returns 500 Internal Server Error.
- Corrected possible plate text update from the occluded license plate if overall confidence is higher.
- Corrected an issue with activating Text Overlays that was only activated on a second attempt.

Product specific features

- Axis Scene Intelligence

  Applies to: All products based on *AXIS ARTPEC-9, on page 83*
  - Added support for Background Appearance.
  - For background appearance it's possible to toggle Sharpness reduction and Saturation reduction for the feature.
- AXIS Scene Annotations

  Applies to: AXIS Q6088-E and AXIS Q6358-LE
  - Added text annotations for roads and buildings.
  - Added pinned text that remains fixed during PTZ camera movement.
  - Added support for text and icons.
  - Added zoom-based Level of Detail (LOD) support.
  - Introduced a new 3D interface for placing scene annotations.
- Added support for using AVIF format for snapshots.

  Applies to: All products based on *AXIS ARTPEC-9, on page 83*
- Added the possibility to connect to a private 4G/5G network, when using AXIS TP3604-E. Read more about which products that support AXIS TP3604-E on *axis.com*
- AXIS Audio Manager Edge

  Applies to: AXIS C1110-E, AXIS C1111-E, AXIS C1210-E, AXIS C1211-E, AXIS C1310-E Mk II, AXIS C1410 Mk II, AXIS C1510, AXIS C1511, AXIS C1610-VE, AXIS C1710, AXIS C1720, AXIS C8110, AXIS C8210, AXIS D3110 Mk II, AXIS D4200-VE and AXIS D6310
  - Removed functionality of "Allowed content". From now all content types are visible
  - Updated the algorithm for sending audio between devices. Limitation: Update all devices in audio site to latest version available for each device.
  - Utilizes TLS by default in the initial communication when adding a device to the audio site.
  - Updated the user managment solution to follow the device account rights structure of Administrator, Operator and Viewer. The mapping to audio use cases can be found in AXIS Audio Manager Edge user interface.
- Added the possibility to select the device sound profile in the web configuration page. Note that the sound profile can also be set from Audio Manager systems and will then override what is set on device level. SoundProfile API available via Audio mixer API.

Applies to: AXIS C1110-E, AXIS C1111-E, AXIS C1210-E, AXIS C1211-E, AXIS C1510, AXIS C1511, AXIS C1610-VE, AXIS C8210, AXIS C8110, AXIS C1310-E Mk II, AXIS C1410 Mk II, AXIS C1710, AXIS C1720, AXIS D4200-VE and AXIS XC1311

- Display brightness will automatically be set to max brightness when text notification is shown on display and signaling LED is active. The increased brightness will temporarily override the configured display brightness settings.

  Applies to: AXIS C1710 and AXIS C1720

- Increased the number of possible in-call actions from 3 to 6.

  Added hebrew language option for the physical display.

  Added a settings menu to enable users to adjust display brightness, change display language, customize the clock, and read info about the device.

  Applies to: AXIS C6110

- Add Feature Flag that activates Human classification outside the Human Recognition Zone.

  Added the support to connect the same radar to a supported ptz camera and a supported panoramic camera via Edge to edge.

  Applies to: AXIS D2122-VE and AXIS D2123-VE

- Improved road profile, added radar Traffic Assistant and radar lanes configuration.

  Applies to: AXIS D2210-VE and AXIS Q1656-DLE

- Increase max speed for oncoming vehicles to 360 km/h.

  Add new profile for departing vehicles with a max speed of 280 km/h.

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

- Added making state in the Vaping detection card, in the web interface.

  Added a new condition in Action rules to support masking detection.

  Applies to: AXIS D6310

- Changed the area opacity and line width of not triggered areas.

  Applies to: AXIS F9104-B Mk II, AXIS F9111-R Mk II, AXIS F9114-R/-B Mk II, AXIS Q1961-TE, AXIS Q2101-TE and AXIS Q2802-E

- Updated internal files handling to improve security and ensure that only the correct system files are accessed.

  Applies to: AXIS I8307-VE

- Products with Hardware ID AAC only support active track version 13.0.88 and later, as well as upcoming LTS 2026, LTS 2024 and LTS 2022 versions and later.

  Applies to: AXIS M3085-V, AXIS M3086-V and AXIS M3088-V

- Added support for tampering detection. (Investigate)

  Applies to: AXIS M3905-R and AXIS P3905-R Mk III

- Two new scene profiles added to the web interface:License plate, optimized for capturing license plates, and Traffic overview, optimized for monitoring vehicle traffic. These can be selected under Video > Image > Appearance > Scene profile. Traffic camera installation assistance under Video > Installation, which provides camera-setting recommendations based on the installation environment and selected

surveillance scenario. Applies to: AXIS P3275-LVE, AXIS P3285-LVE, AXIS Q3546-LVE and AXIS Q3556-LVE

- Added adaptive illumination to reduce power consumption by optimizing IR light usage based on motion detection.

  Applies to: AXIS P3275-LV, AXIS P3275-LVE, AXIS P3275-V, AXIS P3277-LV, AXIS P3277-LVE, AXIS P3278-LV, AXIS P3278-LVE, AXIS P3285-LV, AXIS P3285-LVE, AXIS P3287-LV, AXIS P3287-LVE, AXIS P3288-LV and AXIS P3288-LVE
- Added support for toggling wide dynamic range (WDR) through an action.

  Applies to: AXIS P3735-PLE, AXIS P3737-PLE, AXIS P3738-PLE, AXIS P4705-PLVE, AXIS P4707-PLVE, AXIS P4708-PLVE and AXIS F9114
- Products with Hardware ID A67, A68, A69 and A6A only support active track version 13.0.88 and later, as well as LTS 2026 version 12.11.118 and later, LTS 2024 version 11.11.220 and later, and LTS 2022 version 10.12.345 and later. Applies to: AXIS Q1656, AXIS Q1656-LE, AXIS Q1656-DLE and AXIS Q1686-DLE.
- Added the possibility to get fused speed and AXIS License Plate Verifier for low speeding vehicles use-cases, via LicensePlate event..

  Applies to: AXIS Q1656-DLE
- Added support for AXIS TU8003.

  Applies to: AXIS Q1971-E, AXIS Q2112-E and AXIS Q2802-E
- Added support for background overlays. Scene annotation overlays may toggle if foreground objects (humans & vehicles) should be shown in front of the overlay.

  Applies to: AXIS Q6088-E and AXIS Q6358-LE
- Increased the upper temperature limit of the S3 sensor from +80C to +85C, to remove false warnings. Applies to:AXIS Q6315-LE and AXIS Q6318-LE

AXIS OS 13.0.88

Release date: 2026-09-22

Corrections

- Strengthened the input validation in stream profile settings.
- Corrected an issue where some devices failed to obtain an IPv6 address via DHCPv6.
- Corrected an issue where SNMP v1 and v2c were not functioning correctly.
- Corrected an issue where sensor and optics modifiers for overlays was not working correctly.
- Corrected an issue where it was possible to set multiple ONVIF text overlays.
- Corrected an issue the data-transformer service that could cause the system to restart unexpectedly.
- Increased the upper temperature limit of the S3 sensor from +80C to +85C, to remove false warnings.
- Corrected a vulnerability where secure RTSP streams could be initiated without encryption.
- Corrected an issue where memory usage increased in audio services, improving overall system stability.
- Corrected an issue where audio services consumed excessive memory, improving overall system stability.
- Corrected an issue where ONVIF text overlays were not correctly displayed on view areas.
- Corrected an issue where incorrect respond was sent for ExportFormat in /axis-cgi/record/export/properties.cgi?.
- Updated Remote Syslog to utilize stronger encryption ciphers for improved data transmission security.

- Corrected an issue where the Record video action failed to trigger events associated with the Recording ongoing condition.
- Corrected an issue where RTSP and RTSPS settings were reset to default values during a firmware upgrade.
- Corrected an issue where HTTPS connectivity could be lost after updating and deleting certificates via the API.
- Corrected an issue where the system failed to send a 'Ready' event after a continuous recording had stopped.
- Correct an issue where the Content-Type does not match the payload when send images to email via the event rules.
- Corrected an issue where a normally closed I/O input could incorrectly become active after a device restart.
- Corrected an issue where entering an overly long MACsec identity in the network configuration settings could cause the system to become unresponsive.
- Improved system security in the system's naming service by using safe memory handling functions, ensuring compliance cyber security standards.
- Corrected an issue where SFTP recipients failed to connect due to a fingerprint mismatch when the server supported multiple host key algorithms.
- Corrected an issue where action engine is not reconstructing the message content filter correctly when returning the rules with GetActionRules APIs.
- Corrected an issue where video playback could stop, requiring a device restart.

  Applies to: AXIS AXIS D1110
- Corrected an issue where proxy credentials were not handled correctly and could be exposed in a system log.

  Corrected an issue where URL-embedded credentials were not sanitized correctly and could be exposed in a system log.

  Applies to: AXIS C6110,
- Corrected an issue where toggling Wide Dynamic Range (WDR) could cause system instability and affect image settings.

  Applies to: AXIS F9104-B-MKIII, AXIS F9111-R-MKII, AXIS F9114-R-MKIII
- Corrected an issue where the measurement type of a thermometry data source was not updated on the dashboard after being changed.

  Applies to: AXIS F9111, AXIS F9111-R Mk II, AXIS F9114, AXIS F9114-R Mk II
- Corrected the status LED behavior to ensure consistency across different intercom models.

  Updated internal files handling to improve security and ensure that only the correct system files are accessed.

  Applies to: AXIS I8307-VE,
- Corrected an issue with broken image.

  Applies to: AXIS M3088-V, AXIS M3125-LVE and AXIS M4218-LV/-V
- Corrected an issue where the PTZ functionally to was not working correctly together with Pelco driver installed.

  Applies to: AXIS Q2112-E

- Added the support to connect the same radar to a supported ptz camera and a supported panoramic camera via Edge to edge.

  Applies to: AXIS D2122-VE and AXIS D2123-VE
- Corrected an issue where rotating or mirroring views in picture-in-picture mode could cause display instability.

  Applies to: AXIS F9102-R
- Corrected an issue where H.264 video streams failed to use hardware decoding in Chromium-based browsers.

  Applies to: AXIS M3098-LV
- Corrected an issue where continuous recording to an SD card could lead to metadata storage errors and prevent the removal of recordings.

  Applies to: AXIS P1518-LE, AXIS Q2802-E
- Corrected an issue where widget overlays could not be added to non-default view areas.

  Applies to: AXIS P3277-LVE-MIC
- Corrected an issue where video source and queue owner could not be configured for certain PTZ event rules.

  Applies to: AXIS P5654-E, AXIS Q6325-LE, AXIS Q6358-LE
- Corrected an issue where AXIS License Plate Verifier could crash during startup.

  Applies to: AXIS Q1686-DLE and AXIS Q6358-LE
- Corrected an issue where the Maintenance view failed to load.

  Applies to: AXIS Q2802-E
- Corrected an issue where the zoom does not stop.

  Applies to: AXIS Q6355-LE and AXIS Q6358-LE
- Corrected an issue where the radar menu disappeared from Autotracking, which limited the creation of autotracking profiles to AXIS Object Analytics.

  Applies to: AXIS Q6086-E, AXIS Q6088-E, AXIS Q6325-LE, AXIS Q6355-LE, AXIS Q6358-LE and AXIS Q6411-LE when paired with AXIS D2122-VE or AXIS D2123-VE
- Corrected an issue where privacy masks move and tilt- or pan-position change without user interaction.

  Applies to: AXIS Q6135-LE

LTS 2026 - 12.11

Support phase: 2026 – 2031-12-31

Go to *Products on LTS 2026 - 12.11, on page 89* for a list of products on this track.

Note

- When upgrading from LTS 2024 or LTS 2022, please review the breaking changes implemented in AXIS OS 12.

  These can be found in *Changes in AXIS OS 12* in the AXIS OS Lifecycle guide.
- Release notes for previous versions of AXIS OS 12 are available *here*.

AXIS OS 12.11.118

Release date: 2026-09-07

Analytics updates

- AXIS Perimeter Defender

  Applies to: AXIS Q1971-E, AXIS Q1972-E, AXIS Q2111-E, AXIS Q2112-E and AXIS Q6411-LE-KIT
  - Corrected an issue where scenarios with duplicate names are accepted.
  - Corrected an issue where Analytics run-time parameters are not restored from backup.
- AXIS License Plate Verifier

  Applies to: AXIS Q1686-DLE and AXIS Q6358-LE
  - Corrected an issue where AXIS License Plate Verifier could crash during startup.

Features and product specific

- Strengthened the input validation in stream profile settings.
- Improved the upgrade process for ACAP applications to ensure provisioning settings are preserved.
- Updated Remote Syslog to utilize stronger encryption ciphers for improved data transmission security.
- Improved system memory efficiency by optimizing audio service resource usage when audio functionality is not in use.
- Updated tzdata to version 2026c to ensure accurate time zone and daylight saving time transitions.
- Improved system security in the system's naming service by using safe memory handling functions, ensuring compliance cyber security standards.
- Data transformation API is no longer in beta, meaning they are now stable and ready for production use. Read more *here*.
- Added support for specifying the NTP max distance value, this allows the device to accept NTP servers with higher root dispersion than the default threshold allows.
- AXIS Audio Manager Edge

  Applies to: AXIS C1110-E, AXIS C1111-E, AXIS C1210-E, AXIS C1211-E, AXIS C1310-E Mk II, AXIS C1410 Mk II, AXIS C1510, AXIS C1511, AXIS C1610-VE, AXIS C1710, AXIS C1720, AXIS C8110, AXIS C8210, AXIS D3110 Mk II, AXIS D4200-VE and AXIS D6310
  - Updated the algorithm for sending audio between devices.

    Limitation: Update all devices in audio site to latest version available for each device.
- Updated internal files handling to improve security and ensure that only the correct system files are accessed.

  Applies to: AXIS I8307-VE

- Products with Hardware ID A67, A68, A69 and A6A only support active track version 13.0..xx and later, as well as LTS 2026 version 12.11.118 and later, LTS 2024 version 11.11.220 and later, and LTS 2022 version 10.12.345 and later. Applies to: AXIS Q1656, AXIS Q1656-LE, AXIS Q1656-DLE and AXIS Q1686-DLE.
- Improved the responsiveness of the remote view setup GUI when configuring PTZ motors.

  Applies to: AXIS Q3716-PLVE

Cybersecurity updates

- Updated OpenSSH to version 10.4 to increase overall cybersecurity level.
- Updated cURL to version 8.21.0 to increase overall cybersecurity level.
- Added support for Post-Quantum Crypto (PQC) ML-KEM hybrid scheme for TLS 1.3 communication providing store now, decrypt later protection for increased cybersecurity. Supporting clients can make use of it for e.g. HTTPS, MQTT, RTSPS, 802.1X and other services.
- Addressed *CVE-2026-9063*, *CVE-2026-13409* and *CVE-2026-14543*. These CVEs will be externally disclosed on 10 November 2026, more detailed information will follow then. For more information, please visit the *Security advisories*.
- Addressed *CVE-2026-40612*, *CVE-2026-41256*, *CVE-2026-41257*, *CVE-2026-43894*, *CVE-2026-43895*, *CVE-2026-43896* and *CVE-2026-44777* in `jq version 1.8.1`.
- Addressed *CVE-2026-26157*, *CVE-2026-26158* and *CVE-2026-29004* in `busybox version 1.38.0`.
- Addressed *CVE-2026-58016* in `glib version 2.89.1`.
- Addressed *CVE-2026-50292* in `libinput version 1.30.2`.
- Updated `glib to version 2.88.2`, addressing *BELL-CVE-2026-58010*, *BELL-CVE-2026-58011*, *BELL-CVE-2026-58012*, *BELL-CVE-2026-58013* and *BELL-CVE-2026-58014*.
- Updated `jq to version 1.8.1`, addressing *ECHO-8a1c-e3df-ae5b*, *ECHO-b834-a843-3668* and *ECHO-dfa5-57c7-ba16*.
- Updated `ca-certificates`, addressing *CLSA-2026-1773684237*.

Corrections

- Corrected an issue where sensor and optics modifiers for overlays was not working correctly.
- Corrected an issue where SNMP v1 and v2c were not functioning correctly.
- Corrected an issue where it was possible to set multiple ONVIF text overlays.
- Corrected an issue where some devices failed to obtain an IPv6 address via DHCPv6.
- Corrected an issue the data-transformer service that could cause the system to restart unexpectedly.
- Corrected an issue where entering an overly long MacSec identity in the network configuration settings could cause the system to become unresponsive.
- Corrected an issue where ONVIF text overlays were not correctly displayed on view areas.
- Corrected an issue where memory usage increased in audio services, improving overall system stability.
- Corrected an issue where audio services consumed excessive memory, improving overall system stability.
- Corrected an issue where incorrect respond was sent for ExportFormat in `/axis-cgi/record/export/properties.cgi?`.
- Corrected an issue where the Record video action failed to trigger events associated with the Recording ongoing condition.
- Correct an issue where the Content-Type does not match the payload when send images to email via the event rules.
- Corrected an issue where RTSP and RTSPS settings were reset to default values during a firmware upgrade.

- Corrected an issue where HTTPS connectivity could be lost after updating and deleting certificates via the API.
- Corrected an issue where the system failed to send a 'Ready' event after a continuous recording had stopped.
- Corrected an issue where SFTP recipients failed to connect due to a fingerprint mismatch when the server supported multiple host key algorithms.
- Corrected an issue where action engine is not reconstructing the message content filter correctly when returning the rules with GetActionRules APIs.
- Addressed Teams provisioning failures by properly parsing Teams server responses.

  Applies to: AXIS A8207-VE Mk II, AXIS I7010-VE, AXIS I7020, AXIS I8016-LVE, AXIS I8116-E and AXIS I8307-VE
- Corrected an issue where video playback could stop, requiring a device restart.

  Applies to: AXIS D1110
- Corrected an issue where the dynamic LED strip functionality behaved inconsistently during radar disconnect and reconnect scenarios.

  Applies to: AXIS D2123-VE and AXIS Q6358-LE
- Corrected an issue where 180-degree rotation was not applied to the main view when using PIP mode.

  Corrected a memory leak when switching Picture-in-Picture sources to improve system stability.

  Applies to: AXIS F9102
- Corrected an issue where toggling Wide Dynamic Range (WDR) could cause system instability and affect image settings.

  Applies to: AXIS F9102-B, AXIS F9104-B Mk III, AXIS F9111-R Mk II and AXIS F9114-R Mk III
- Corrected an issue where image file sources in an HDMI playlist could not be mirrored or rotated.

  Corrected an issue where rotating or mirroring views in picture-in-picture mode could cause display instability.

  Corrected an issue where frame rate drops occurred when using Picture-in-Picture with certain sensor combinations.

  Applies to: AXIS F9102-R
- Corrected an issue where the measurement type of a thermometry data source was not updated on the dashboard after being changed.

  Applies to: AXIS F9111, AXIS F9111-R Mk II, AXIS F9114 and AXIS F9114-R Mk II
- Corrected the status LED behavior to ensure consistency across different intercom models.

  Applies to: AXIS I8027-LVE, AXIS I8307-VE and AXIS I8407-LVE
- Corrected an issue where video streaming could fail during mid-call negotiation in certain SIP configurations.

  Applies to: AXIS I8116-E
- Corrected an issue where H.264 video streams failed to use hardware decoding in Chromium-based browsers.

  Applies to: AXIS M2046-LE, AXIS M3097-V and AXIS M3098-LV

- Corrected an issue where continuous recording to an SD card could lead to metadata storage errors and prevent the removal of recordings.

  Applies to: AXIS P1518-LE and AXIS Q2802-E
- Corrected an issue where widget overlays could not be added to non-default view areas.

  Applies to: AXIS P3277-LVE-MIC
- Corrected an issue where the radar menu disappeared from Autotracking, which limited the creation of autotracking profiles to AXIS Object Analytics.

  Applies to: AXIS Q6086-E, AXIS Q6088-E, AXIS Q6325-LE, AXIS Q6355-LE, AXIS Q6358-LE and AXIS Q6411-LE when paired with AXIS D2122-VE or AXIS D2123-VE
- Corrected an issue where some search results were missing from Smart Search when using cloud storage.

  Applies to: AXIS Q1656 and AXIS Q1656-B
- Corrected an issue where the PTZ functionally to was not working correctly together with Pelco driver installed.

  Applies to: AXIS Q2112-E
- Corrected an issue where the Maintenance view failed to load.

  Applies to: AXIS Q2802-E
- Corrected an issue where privacy masks move and tilt- or pan-position change without user interaction.

  Applies to: AXIS Q6135-LE

AXIS OS 12 Archived Release Notes

If you're looking for release notes from earlier versions of AXIS OS 12 active track, you can find them *here*.

LTS 2024 - 11.11

Support phase: 2024 – 2029-12-31

Go to *Products on LTS 2024 - 11.11, on page 91* for a list of products on this track.

Note

- When upgrading from LTS 2022 or LTS 2020, please review the breaking changes implemented in AXIS OS 11.

  These can be found in *Changes in AXIS OS 11* in the AXIS OS Lifecycle guide.
- Release notes for previous versions of AXIS OS 11 are available *here*.

AXIS OS 11.11.220

Release date: 2026-07-23

Product specific features

- Updated the End User License Agreement.
- Added the possibility to add a custom subject alternative name (SAN) during the CSR-generation in the web interface.
- Products with Hardware ID A67, A68, A69 and A6A only support active track version 13.0.88 and later, as well as LTS 2026 version 12.11.118 and later, LTS 2024 version 11.11.220 and later, and LTS 2022 version 10.12.345 and later. Applies to: AXIS Q1656, AXIS Q1656-LE, AXIS Q1656-DLE and AXIS Q1686-DLE.

Cybersecurity updates

- Updated OpenSSL to version 3.0.21 to increase overall cybersecurity level.
- Updated OpenSSL to version 1.1.1zh to increase overall cybersecurity level.
- Updated cURL to version 8.21.0 to increase overall cybersecurity level.
- Addressed *CVE-2026-13409* . This CVE will be externally disclosed on 10 Nov 2026, more detailed information will follow at that time. For more information, please visit the *Axis vulnerability management portal*.
- Adressed *CVE-2026-53614* in util-linux version 2.42.2.
- Addressed *CVE-2025-13151*, *CVE-2026-40612*, *CVE-2026-41256*, *CVE-2026-41257*,*CVE-2026-43894*, *CVE-2026-43895*, *CVE-2026-43896*, *CVE-2026-44777*, *CVE-2026-45614* and *CVE-2026-58016*.
- Addressed *ECHO-8a1c-e3df-ae5b*, *ECHO-b834-a843-3668* and *ECHO-dfa5-57c7-ba16* in jq-1.8.1.
- Addressed *CLSA-2026-1773684237* in ca-certificates-20260223.

Corrections

- Corrected an issue with wrong validity for client-server certificate, displayed in the web interface.
- Corrected an issue where a normally closed I/O input could incorrectly become active after a device restart.
- Corrected an issue where privacy masks move and tilt- or pan-position change without user interaction.

  Applies to: AXIS Q6135-LE
- Corrected an issue that could cause the audio service to crash, improving overall system stability.

  Applies to: AXIS Q9216-SLV

AXIS OS 11.11.215

Release date: 2026-06-23

Corrections

- Corrected an issue where privacy masks move and tilt- or pan-position change without user interaction.

  Applies to: AXIS Q6135-LE

AXIS OS 11.11.212

Release date: 2026-06-08

Cybersecurity updates

- Updated OpenSSL to version 3.0.20 to increase overall cybersecurity level.
- Updated Apache to version 2.4.67 to increase overall cybersecurity level.
- Addressed *CVE-2026-31431*, known as *Copy Fail*. For more information, please visit the *Axis vulnerability management portal*.

Corrections

- Updated tzdata to version 2026a to ensure accurate time zone and daylight saving time transitions.
- Corrected a security vulnerability to ensure only signed application packages can be installed.
- Corrected an issue where firmware upgrades could fail when device memory was nearly full.

  Applies to: AXIS C1110-E and AXIS C1111-E
- Improved IR-cut filter motor control to increase hardware reliability and longevity.

  Applies to: AXIS P1375/-E, AXIS P1377/-LE and AXIS P1378/-LE
- Improved AI model support for INT8 quantized models.

  Applies to: AXIS P1465-LE, AXIS P1467-LE and AXIS P1468-LE
- Corrected an issue where connection to an attached PTZ could be blocked.

  Applies to: AXIS Q6020-E and AXIS Q6300-E
- Corrected an issue where the IR-cut filter could end up in an incorrect position.

  Applies to: AXIS Q6225-LE, AXIS Q6315-LE, AXIS Q6318-LE and AXIS Q8615-E
- Corrected a resource leak to improve long-term system stability when using PTZ functions.

  Applies to: AXIS Q6300-E

AXIS OS 11.11.205

Release date: 2026-05-04

Cybersecurity updates

- Updated OpenSSL to version 3.0.19 and 1.1.1zf to increase overall cybersecurity level.
- Updated cURL to version 8.19.0 to increase overall cybersecurity level.
- Addressed *CVE-2026-1965*, *CVE-2026-3783*, *CVE-2026-3784* and *CVE-2026-3805* in curl-8.18.0.
- Addressed *CVE-2026-2921*, *CVE-2026-3083* and *CVE-2026-3085* in gstreamer-1.26.7.
- Addressed *CVE-2025-13601* and *CVE-2025-14087* in glib-2.86.3.
- Addressed *CVE-2024-12243* and *CVE-2025-9820* in gnutls-3.8.10.
- Addressed *CVE-2025-59375* in expat-2.7.2.
- Addressed *CVE-2025-13151* in libtasn1-4.20.0.

- Addressed *CVE-2025-68615* in net-snmp-5.9.4

Corrections

- Updated the End User License Agreement.
- Added 1000BASE-T connection type in the PlainConfig settings.
- Corrected an issue where system action configuration was being overwritten.
- Corrected an issue where bitrate mode overrides were not consistently applied.
- Corrected an issue where 802.1x EAP-TLS reauthentication could cause recording gaps due to temporary network disconnections.
- Corrected an 802.1X authentication issue affecting multiple devices on a single switch port by introducing a new multi-auth mode.
- Corrected an issue that caused the device to loose network connection when the network speed was manually set to 1Gbps/full duplex.

  Applies to: All products that support 1Gbps network speed
- Corrected an issue where rzoom and rfocus commands were not available for Pelco driver.

  Applies to: AXIS Q1656, AXIS Q1656-B, AXIS Q1656-BE, AXIS Q1656-BLE and AXIS Q1656-LE
- Corrected a focus issue due to a lens calibration offsets. Only models with the hardware IDs A20 and 9FB are affected.

  Applies to: AXIS Q1805-LE and AXIS Q1806-LE
- Enhanced the robustness of the NTP service during system shutdown and firmware update.

  Applies to: AXIS Q6010-E

AXIS OS 11.11.198

Release date: 2026-03-03

Corrections

- Internal quality improvements.

  Applies to: AXIS P3818-PVE

AXIS OS 11.11.195

Release date: 2026-02-18

Corrections

- Corrected a focus issue due to a lens calibration offsets. Only models with the hardware IDs A20 and 9FB are affected.

  Applies to: AXIS Q1805-LE and AXIS Q1806-LE

AXIS OS 11.11.194

Release date: 2026-02-18

Corrections

- Improved stability and memory optimization.

  Applies to: AXIS M7104, AXIS M7116, AXIS P7304 and AXIS P73116

AXIS OS 11.11.192

Release date: 2026-02-23

Cybersecurity updates

- Upgrading curl to version 8.18.0 to improve cybersecurity.
- Addressed *DEBIAN-CVE-2025-49014* in jq-1.8.1.
- Addressed *BELL-CVE-2024-2236* in libgcrypt-1.11.0.
- Updated cURL to version 8.17.0 to increase overall cybersecurity level.
- Updated ntfs-3g to address *CVE-2023-52890*.

  Applies to: AXIS D1110, AXIS S3008, AXIS S3008 MK II, AXIS S3016 and AXIS W800
- Updated Apache to version 2.4.66, addressing *CVE-2025-55753*, *CVE-2025-58098*, *CVE-2025-59775*, *CVE-2025-65082*, *CVE-2025-66200 CVE-2025-55753*, *CVE-2025-58098*, *CVE-2025-59775*, *CVE-2025-65082* and *CVE-2025-66200*

Corrections

- Corrected an issue in the storage manager that caused a crash during disk status updates.
- Corrected an issue where the MTU limit was exceeded when streaming via SIP.

  Applies to: AXIS A8207-VE, AXIS A8207-VE MK II, AXIS I8016-LVE and AXIS I8116-E
- Corrected a memory leaks in audio_conf service during.

  Applies to: AXIS C1110-E, AXIS C1111-E, AXIS C1210-E, AXIS C1211-E, AXIS C1510, AXIS C1511 and AXIS C8110
- Corrected an issue where focus was lost after an upgrade or restart.

  Applies to: AXIS M1135 MK II, AXIS M1135-E MK II, AXIS M1137 MK II, AXIS M1137-E MK II, AXIS Q1615 MK III, AXIS Q1615-LE MK III, AXIS Q1656 and AXIS Q1656-B
- Corrected an issue with status LED indicator was not turned off. Applies to: AXIS M2035-LE.

  Applies to: AXIS M2035-LE and AXIS M2036-LE
- Corrected an issue where the overlay disappeared if the image was mirrored.

  Applies to: AXIS M3905-R and AXIS P3905-R MK III
- Corrected an issue where PTZ control in double panorama stream did not work. Applies to: AXIS M4308-PLE, AXIS M4327-P, AXIS M4328-P, AXIS M4317-PLVE and AXIS M4318-PLVE.
- Corrected a Radar-Camera pairing issue.

  Applies to: AXIS P3265-LVE-3
- Corrected an issue where starting a Dual View streaming would hang.

  Applies to: AXIS P4705-PLVE, AXIS P4707-PLVE and AXIS P4708-PLVE
- Corrected an issue where custom focus area in presets was not working correctly.

  Applies to: AXIS Q1715 and AXIS Q1798-LE

AXIS OS 11.11.181

Release date: 2025-11-03

Cybersecurity updates

- Updated OpenSSH to version 10.1 to increase overall cybersecurity level.
- Updated OpenSSL to version 3.0.18 to increase overall cybersecurity level.
- Updated glib, addressing *CVE-2025-6052*
- Addressed *CVE-2025-8998*, *CVE-2025-9055* and *CVE-2025-9524*. These CVEs will be externally disclosed on 11 November 2025, more detailed information will follow then. For more information, please visit the *Axis vulnerability management portal*.

Corrections

- Corrected an issue where zoom modifiers (#z and #Z) was not working correctly with upload image and video upload to ftp or http.
- Corrected an issue where Always Multicast stopped working after a device upgrade.
- Corrected a memory leak in the dynamicoverlay-cgi.
- Improved log messages for upload images to FTP.
- Added support in the web interface to use FQDN for SNMP Trap address.
- Corrected an issue where Privacy mask not working correctly.

  Applies to: AXIS P3248-LVE
- Resolved an issue that caused failure of the ONVIF conformance test.

  Applies to: AXIS D2210-VE
- Corrected an issue where it sometimes takes up to 30 seconds to connect via AMC.

  Applies to: AXIS Q9307-LV and AXIS V5925
- Corrected an issue where Always Multicast would stop and not recover when a sensor signal was lost over the serial link.

  Applies to: AXIS F9114 and AXIS F9114-B

AXIS OS 11.11.176

Release date: 2025-10-06

Cybersecurity updates

- Updated cURL to version 8.16.0 to increase overall cybersecurity level.
- updated redis to version 7.2.10, addressing *CVE-2025-48367*.
- Corrected an issue where AXIS License Plate Verifier was not working correctly with cURL version 8.14.1.

Corrections

- Corrected an issue where the GetSegment D-Bus reply was zero for recordings.
- Corrected an issue where the date format in email headers was inconsistent for the first 9 days of the month.
- Corrected an issue where zoom modifiers (#z and #Z) were not supported in videoclip upload filenames.
- Corrected a memory leak in the Axis parameter handler service.
- Improved TLS Handshake Performance with TPM Keys.
- Improved media player handling.

  Applies to: AXIS D1110, AXIS S3008 and AXIS S3016
- Corrected an issue where PTZ autotracker stopped working after restart.

  Applies to: AXIS D201-S XPT Q6075 and AXIS Q6075-E

- Corrected a bootloader issue after updating to AXIS OS 11.11.160.

  Applies to: AXIS M3085-V, AXIS M3088-V, AXIS M3125-LVE, AXIS M3126-LVE, AXIS M3128-LVE, AXIS M4215-LV, AXIS M4215-V, AXIS M4218-LV and AXIS M4218-V

AXIS OS 11.11.169

Release date: 2025-09-08

Features for all products

- Enabled the enforcement of upgrade paths. More information can be found in the *AXIS OS Lifecycle guide*.

  This feature is now integrated in the web interface, so in case of failed upgrade attempt, an error message is shown in the logs.

Cybersecurity updates

- Addressed *CVE-2025-6571*. This CVE will be externally disclosed on 11 November 2025, more detailed information will follow then. For more information, please visit the *Axis vulnerability management portal*.
- Updated OpenSSL to version 3.0.17, addressing *CVE-2025-4575*.
- Updated OpenSSL to version 1.1.1zc to increase overall cybersecurity level.
- Updated Apache to version 2.4.64 to increase overall cybersecurity level.
- Updated Apache to version 2.4.65 to increase overall cybersecurity level.
- Addressed *CVE-2024-23337*, *CVE-2025-48060* and *CVE-2024-53427* in jq-1.7.1.
- Addressed *BIT-redis-2025-21605* in redis-7.2.7.

Corrections

- Corrected an issue where capital letters were not supported in account usernames.
- Corrected an issue with HTTP notifications failing due to permission errors.
- Corrected an issue where Always Multicast would stop and not recover when a sensor signal was lost over the serial link.

  Applies to: AXIS F9114 and AXIS F9114-B
- Improved Cold Boot Stability for i-CS system lens.

  Applies to: AXIS M1135 MK II, AXIS M1135-E MK II, AXIS M1137 MK II and AXIS M1137-E MK II
- Corrected an issue with RTSP stream not being displayed correctly at restart. If you change the Quad view configuration the stream will be restarted.

  Applies to: AXIS M3077-PLVE and AXIS M4327-P
- Corrected an issue where changes to Smoke Alert Analytics settings had no effect.

  Applies to: AXIS P1468-XLE, AXIS XFQ1656 and AXIS XPQ1785
- Corrected a freeze issue caused by electrostatic discharge (ESD) events. The device now automatically recovers without needing manual restart.

  Applies to: AXIS Q1951-E and AXIS Q1952-E

AXIS OS 11.11.164

Release date: 2025-07-17

Corrections

- Corrected an issue where capital letters were not supported in account usernames.
- Corrected an issue where changes to Smoke Alert Analytics settings had no effect.

  Applies to: AXIS P1468-XLE, AXIS XFQ1656 and AXIS XPQ1785

AXIS OS 11.11.161

Release date: 2025-07-07

Corrections

- Corrected an issue where FPS drops from 15 to 11 when opening an 8th stream.

  Applies to: AXIS Q6010-E and AXIS Q6100-E

AXIS OS 11.11.160

Release date: 2025-07-07

Analytics updates

- AXIS License Plate Verifier 11.11

  Applies to: AXIS P1445-LE-3, AXIS P1455-LVE-3, AXIS P1465-LE-3, AXIS P3245-LVE-3 and AXIS P3265-LVE-3
  - Added support for PTZ cameras, supporting pairing for up to two preset positions.

    Applies to: AXIS P5676-LE, AXIS Q6135-LE, AXIS Q6225-LE, AXIS Q6315-LE, AXIS Q6318-LE, AXIS Q6355-LE and AXIS Q6358-LE
  - Added support for AXIS A9210.
  - Added corridor mode to the supported *AXIS ARTPEC-7, on page 85*, *AXIS ARTPEC-8, on page 84* and *AXIS ARTPEC-9, on page 83* products.
  - License plate recognition has been improved for various regions, including Dubai, New Zealand, Latvia, and Canada.
  - Improved the event retention behavior when no SD card is present, affecting full frame, downsized frame, and vehicle crop selections.
  - Corrected an issue with the maximum retained events on SD cards.
  - Corrected an issue with umlaut display on text overlays.
  - Corrected an issue with the Area of Interest when there are too many polygons set in the upper part of the zone.
  - Corrected an issue with the Test button under Push Event menu related to VAPIX events.
- AXIS Audio Analytics
  - Restored AXIS Audio Analytics. The application went missing after upgrading to AXIS OS version 11.11.148.

    Applies to: AXIS D3110, AXIS M3086-V, AXIS P9117-PV and AXIS W400

Cybersecurity updates

- Improved password validation for network shares.
- Updated cURL to version 8.14.1.
- Updated OpenSSH to version 10.0p1.
- Addressed *CVE-2025-32728*.

- Addressed *CVE-2025-6298*. This CVE will be externally disclosed later. More detailed information will follow then. For more information, please visit the *Axis vulnerability management portal*.

Product specific features

- Hardware modifications have been made to proactively prepare for the new NDAA 23 regulations that will be required in 2028. You will find more information about on axis.com. In AXIS OS knowledge base, you will find more about the . The hardware ID can be found in Plain config > Properties > System > Hardware ID.
  - Products with Hardware ID A2D only support active track version 12.5.56 and later, as well as LTS 2024 version 11.11.160 and later, and LTS 2022 version 10.12.270 and later.

    Applies to: AXIS M3088–V

Corrections

- Corrected an issue with the description of the modifier in the text overlay.
- Corrected an issue where API-Discovery triggered a memory leak, improving system stability.
- Corrected an issue causing high memory usage in the httpd process, optimizing the web server performance.
- Increased the number of simultaneous connections the web server can handle to prevent device reboots during high traffic.
- Corrected an issue where remounting an encrypted SD card could cause an illegal state if done incorrectly.
- Corrected an issue where SMTP DATA messages did include additional not needed null characters.
- Corrected an issue with the disk event triggers where they were not triggering again after restarting the device.
- Corrected an issue with delay in the audio streaming when using line-in paging source in AXIS Audio Manager Edge.

  Applies to: AXIS C1110-E, AXIS C1111-E, AXIS C1210-E, AXIS C1211-E, AXIS C1510, AXIS C1511, AXIS C1610-VE, AXIS C8110 and AXIS C8210
- Corrected an issue where the device would fail to boot in high temperature environments.

  Applies to: AXIS M1135 MK II, AXIS M1135-E MK II, AXIS M1137 MK II and AXIS M1137-E MK II
- Corrected an issue where the device could not pan due to ice build-up in cold weather conditions.

  Applies to: AXIS Q6215-LE and AXIS Q6225-LE
- Updated the behavior of the front LED so that it no longer lights up during product start-up and that the color of the LED is according to the pre-defined events for SIP, live stream active and recording.

  Applies to: AXIS C1310-E MK II

AXIS OS 11.11.155

Release date: 2025-06-03

Corrections

- Corrected an issue where the device would fail to boot in high temperature environments.

  Applies to: AXIS M1135 MK II, AXIS M1135-E MK II, AXIS M1137 MK II and AXIS M1137-E MK II

AXIS OS 11.11.148

Release date: 2025-04-29

Cybersecurity updates

- Updated expat-2.6.4, addressing OpenSource *CVE-2024-8176*.
- Addressed Axis *CVE-2025-0325*. This CVE will be externally disclosed on 2 June 2025, more detailed information will follow then. For more information, please visit the *Axis vulnerability management portal*.

Product specific features

Hardware modifications have been made to proactively prepare for the new NDAA 23 regulations that will be required in 2028. You will find more information about *NDAA Compliance* on axis.com. In AXIS OS knowledge base, you will find more about the *hardware changes*. The hardware ID can be found in Plain config > Properties > System > Hardware ID.

- Products with Hardware IDs A1D and A1E only support active track 12.4.59 and later, as well as LTS 2024 version 11.11.148 and later, and LTS 2022 version 10.12.280 and later.

  Applies to: AXIS M7116 and AXIS P7316

Corrections

- Updated time zone database version to 2025b.
- Improved stability of the “focusd” and “maskd” daemons when handling oversized messages.
- Corrected a logging out issue when using an OpenID Connect user.
- Corrected an issue where the password was not hidden in the input field for ACAP applications.
- Corrected memory leaks in the mdns-sd-confd process, reducing memory consumption and improving system stability.
- Corrected an issue in recording-indexer caused by corrupt database version.
- Corrected an issue where the RTSPS certificate was changed after a standard software upgrade.
- Corrected an issue where weak ciphers were used in SMTP mail notifications, improving the security of email communications.
- Corrected an issue where SMTP DATA messages were incorrectly terminated, causing compatibility issues with strict SMTP servers like Postfix.
- Improved stability of the "lightlogic" daemon.
- Improved system stability by addressing a potential memory leak in the Video-Object-Detection process.

  Applies to: AXIS I7010-VE, AXIS I7010-VE SAFETY, AXIS I7020, AXIS I8116-E, AXIS M1055-L, AXIS M1075-L, AXIS M2035-LE, AXIS M2036-LE, AXIS M3085-V, AXIS M3086-V, AXIS M3088-V, AXIS M3125-LVE, AXIS M3126-LVE, AXIS M3128-LVE, AXIS M4215-LV/-V, AXIS M4216-LV/-V and AXIS M4218-LV/-V
- Corrected an issue where manual calibration web page failed to load.

  Applies to: AXIS D101-A XF P3807, AXIS EXCAM XF P3807 and AXIS P3807-PVE
- Solved an issue with z-wave event not working correctly.

  Applies to: AXIS M5000-G and AXIS M5075-G
- Corrected an issue where PTZ Autocalibration would sometimes fail despite showing success in the web GUI.

  Applies to: AXIS Q6010-E and AXIS Q6100-E
- Corrected an issue preventing PTZ from functioning after a restart when IR is enabled.

  Applies to: AXIS Q6315-LE and AXIS Q6318-LE
- Corrected An Issue With SIP Settings Page Accessibility.

Corrected an issue preventing the SIP page from loading, ensuring users can access the page without interruption.

Applies to: AXIS C8110

- Corrected an issue preventing the units from being reachable after a soft restart, requiring a hard restart to recover.

  Applies to: AXIS D3110

- Corrected an issue where changing the radar position/orientation was not registered in the paired camera, ensuring accurate calibration.

  Corrected an issue where radar tracks were not accurately interpreted, resulting in incorrect angle displays on paired camera products.

  Applies to: AXIS P3265-LVE-3

AXIS OS 11.11.141

Release date: 2025-03-17

Features for all products

- Updated the End User License Agreement.

Analytics

- AXIS License Plate Verifier
  - Added the ability to disable VAPIX events.
  - Added SD card status for heartbeat event.
  - Improved handling of SD card storage.
  - Resolved an issue related to HTTPS when integrated with AXIS A91xx I/O Relay Modules, if both the relay module and the camera are set to HTTPS.
  - Improved data caching from older versions.
  - Corrected an issue with 2N integration and direction status events.

Product specific features

- Hardware modifications have been made to proactively prepare for the new NDAA 23 regulations that will be required in 2028. You will find more information about *NDAA Compliance* on axis.com. In AXIS OS knowledge base, you will find more about the hardware changes. The hardware ID can be found in Plain config > Properties > System > Hardware ID.
  - Products with Hardware ID A20 only support active track 12.2.61 and later, as well as LTS 2024 version 11.11.141 and later.

    Applies to: AXIS Q1806-LE
  - Products with Hardware ID A21 and A22 only support active track 12.2.61 and later, as well as LTS 2024 version 11.11.141 and later.

    Applies to: AXIS P1387/-B/-BE/-LE and AXIS P1388/-B/-BE/-LE

Cybersecurity updates

- Updated OpenSSL to version 1.1.1zb and 3.0.16 to increase overall cybersecurity level.
- Updating OpenSSH to version 9.9p2, addressing *CVE-2025-26466*.
- Updated libxml2 to version 2.13.3, addressing *CVE-2024-56171*, *CVE-2025-24928* and *CVE-2025-27113*.
- Updated cURL to version 8.12.0, addressing *CVE-2025-0725*, *CVE-2025-0665* and *CVE-2025-0167*.

- Updated cURL to version 8.12.1 to improve cybersecurity.
- Addressed *CVE-2025-0361* and *CVE-2024-47261*. These CVEs will be externally disclosed on 8 April 2025, more detailed information will follow then. For more information, please visit the *Axis vulnerability management portal*.
- Addressed *CVE-2025-0324*. This CVE will be externally disclosed on 2 June 2025, more detailed information will follow then. For more information, please visit the *Axis vulnerability management portal*.
- Addressed *CVE-2024-46981*.
- Addressed *CVE-2024-51741*.
- Addressed *BIT-redis-2024-51741*.

Corrections

- Corrected a Recording Page Crash on Invalid Filter Input.
- Corrected an issue with incorrect headers when sending image via proxy.
- Updated time zone database version to 2025a.
- Corrected an issue where audio stopped working when using transmit.cgi and a content length of zero.
- Corrected an issue that prevented manual IR light activation in certain situations.
- Corrected an issue where the browser selected Simplified Chinese automatically while it should have selected the Traditional Chinese.
- Updated the behavior of the front LED so that it no longer lights up during product start-up.

  Applies to: AXIS C1310-E
- Corrected an issue where shock detected event was triggered when IR-cut filter was turned on/off.

  Applies to: AXIS Q1805-LE and AXIS Q1806-LE

AXIS OS 11.11.136

Release date: 2025-02-10

Cybersecurity updates

- Addressed *CVE-2024-47261*. This CVE will be externally disclosed on 4 March 2025, more detailed information will follow then. For more information, please visit the *Axis vulnerability management portal*.

Product specific features

- Updated the End User License Agreement.

  Applies to: AXIS A8207-VE/Mk II, AXIS I7010-VE, AXIS I7020, AXIS I8016-LVE and AXIS I8116-E

AXIS OS 11.11.135

Release date: 2025-02-10

Features for all products

- The beta tag is removed from the Certificate APIs in the Device Configuration API.

Cybersecurity updates

- Addressed *CVE-2025-0359*, *CVE-2025-0360* and *CVE-2024-47259*. These CVEs will be externally disclosed on 4 March 2025, more detailed information will follow then. For more information, please visit the *Axis vulnerability management portal*.
- Updated glib, addressing *CVE-2024-52533*.

- Updated cURL to version 8.11.1 to increase overall cybersecurity level.

Analytics updates

- AXIS License Plate Verifier

  Applies to: AXIS P1445-LE-3, AXIS P1455-LVE-3, AXIS P1465-LE-3, AXIS P3245-LVE-3 and AXIS P3265-LVE-3

  - Added plate confidence to VAPIX events.
  - Updated the Genetect Integration with new data, vehicle direction, device location Latitude/Longitude, vehicle type and color, country and region.
  - Corrected an issue with Update status event images and storage.
  - Corrected an issue where Push Events were not received in TCP, in combination with proxy function.
  - Corrected an issue with Slovakian plates where a T would be read as an I.
  - Corrected an issue with country classification for Canadian number plates.
  - Corrected an issue with User Interface cached pages.

Product specific features

- Hardware modifications have been made to proactively prepare for the new NDAA 23 regulations that will be required in 2028. You will find more information about *NDAA Compliance* on axis.com. In AXIS OS knowledge base, you will find more about the *hardware changes*. The hardware ID can be found in Plain config > Properties > System > Hardware ID.
  - Products with Hardware ID A16, A17 and A18 only support upcoming active track 12.3 and later, as well as LTS 2024 version 11.11.135 and later, and LTS 2022 version 10.12.291 and later.

    Applies to: AXIS M5074, AXIS M5075 and M5075-G
  - Products with Hardware ID A14 and A15 only support active track AXIS OS 12.1 and later, as well as LTS 2024 version 11.11.135 and later.

    Applies to: AXIS P3738-PLE and AXIS P4708-PLVE
- Added support for AXIS T61 Mk II Audio and I/O Interface module.

  Applies to: AXIS P3245-LVE-3

Corrections

- Corrected an issue in the Auto Speaker Test when performing Re-calibration.
- Corrected problem where WebRTC streaming did not work in some situations.
- Improved time.cgi API to only display valid time zones, removing obsolete options.
- Corrected an issue causing high RAM usage of the metadata process, improving overall system performance.
- Corrected an issue where configuring both PTZ unit and Multidirectional camera to "HTTPS only" prevented manual PTZ positioning calibration.
- Corrected an issue when midspan is used, the device network interface doesn't go up again after MACsec is deactivated on the switch.
- Corrected an issue that occurred when importing ECC keys using Trusted Platform Module (TPM) for secure key storage.

  Applies to: All products with SecureKeystore feature
- Corrected an issue with dark image in low light.

  Applies to: AXIS M3125-LVE, AXIS M3126-LVE, AXIS M3128-LVE, AXIS M4215-LV/-V and AXIS M4218-LV/-V

- Updated support for AXIS T61 Mk II Audio and I/O Interface devices.

  Applies to: AXIS P3265-LVE-3
- Corrected an issue that allowed the heater to start in low power mode after an upgrade.

  Applies to: AXIS Q1805-LE, AXIS Q1806-LE and AXISQ1808-LE
- Corrected an intermittent focus issue that sometimes caused blurry images when using wide-angle or partial zoom modes.

  Applies to: AXIS Q6315-LE and AXIS Q6318-LE
- Corrected an issue where the device would reboot unexpectedly when enabling IR (Infrared) and using optical zoom simultaneously.

  Applies to: AXIS Q6315-LE
- Corrected an issue where the camera could move out of control if it received multiple rapid preset calls.

  Applies to: AXIS Q8752-E

AXIS OS 11.11.131

Release date: 2024-12-27

Corrections

- Corrected an intermittent focus issue that sometimes caused blurry images when using wide-angle or partial zoom modes.

  Applies to: AXIS Q6315-LE

AXIS OS 11.11.128

Release date: 2024–12–18

Product specific features

- Hardware modifications have been made to proactively prepare for the new NDAA 23 regulations that will be required in 2028. You will find more information about *NDAA Compliance* on axis.com. In AXIS OS knowledge base, you will find more about the *hardware changes*. The hardware ID can be found in Plain config > Properties > System > Hardware ID.
  - Products with Hardware ID A09 only support active track 12.1.60 and later, as well as LTS 2024 version 11.11.128 and later.

    Applies to: AXIS M3128-LVE

Corrections

- Increased the default amount of audio clips from 10 to 20

  Applies to: AXIS D3110.
- Corrected an occasional problem with Wide Dynamic Range (WDR) functionality.

  Applies to: AXIS M3088-V, AXIS M3128-LVE and AXIS M4218-LV/-V
- Corrected an issue with dark image in low light.

  Applies to: AXIS M3125-LVE, AXIS M3126-LVE, AXIS M3128-LVE, AXIS M4215-LV/-V and AXIS M4218-LV/-V

AXIS OS 11.11.127

Release date: 2025–12–06

Product specific features

Hardware modifications have been made to proactively prepare for the new NDAA 23 regulations that will be required in 2028. You will find more information about *NDAA Compliance* on axis.com. In AXIS OS knowledge base, you will find more about the *hardware changes*. The hardware ID can be found in Plain config > Properties > System > Hardware ID.

- Products with Hardware ID A08 only support active track 12.1.60 and later, as well as LTS 2024 version 11.11.127 and later, and LTS 2022 version 10.12.270 and later.

  Applies to: AXIS M3088-V
- Products with Hardware ID A07 only support active track 12.1.60 and later, as well as LTS 2024 version 11.11.127 and later.

  Applies to: AXIS M4218-V and AXIS M4218-LV

Corrections

- Corrected an occasional problem with Wide Dynamic Range (WDR) functionality.

  Applies to: AXIS M3088-V , AXIS M3128-LVE and AXIS M4218-V/-LV

AXIS OS 11.11.126

Release date: 2024–12–02

Corrections

- Added support for AXIS T61 Mk II Audio and I/O Interface module.

  Applies to: AXIS P3245-LVE-3
- AXIS Audio Manager Edge: Corrected an issue where certain music sources could be unintentionally muted during volume adjustment.

  Applies to: AXIS C1110-E, AXIS C1111-E, AXIS C1210-E, AXIS C1211-E, AXIS 1510, AXIS C1511, AXIS C1610-VE, AXIS C8110 and AXIS C8210

AXIS OS 11.11.124

Release date: 2024-11-25

Cybersecurity updates

- Addressed *CVE-2024-8772*. This CVE will be externally disclosed on 26 November 2024 as part of our ongoing commitment to cybersecurity. Detailed information will follow then. For more information, please visit the *Axis vulnerability management portal*.
- Updated wpa-supplicant to version 2.11 to increase overall cybersecurity level.
- Restricted access to param.cgi so that only authorized administrators can configure privacy masks.

Analytics updates

- AXIS License Plate Verifier

  Applies to: AXIS P1445-LE-3, AXIS P1455-LE-3, AXIS P1465-LE-3, AXIS P3245-LVE-3 and AXIS P3265-LVE-3
  - Improved on Australian libraries with extended plate formats to increase license plate reads for Custom/Personalized plates.

- Improved on Mexican libraries with characters that are situated very close to the frame of the license plate.
- Corrected a stability issue related to Australia and New Zealand region number plates.
- Corrected an issue with max character filter.
- Corrected an issue with Singapore region which was not listed in some camera models.

Product specific features

Hardware modifications have been made to proactively prepare for the new NDAA 23 regulations that will be required in 2028. You will find more information about *NDAA Compliance* on axis.com. In AXIS OS knowledge base, you will find more about the *hardware changes*. The hardware ID can be found in Plain config > Properties > System > Hardware ID.

- Products with Hardware ID 9FA and 9F9 only support LTS 2024 11.11.124 and later.

  Applies to: AXIS P1385, AXIS P1385-B, AXIS P1385-BE and AXIS P1385-E
- Products with Hardware ID 9FC, 9FD and 9FE only support active track 12.1.60 and later, as well as LTS 2024 version 11.11.124 and later.

  Applies to: AXIS P1465-LE 9mm, AXIS P1465-LE 29mm and AXIS P1465-LE-3
- Products with Hardware ID 9FB only support active track 12.0.91 and later, as well as LTS 2024 11.11.124 and later.

  Applies to: AXIS Q1805-LE

Corrections

- Corrected an issue where SSH and network share users were removed after upgrade.
- Corrected an issue where the image upload file naming was not correct.
- Corrected a problem with gaps in the exported Matroska files when they were recorded at 50/60 FPS.
- Improved "Start Recording" functionality to prevent simultaneous continuous recording.
- Corrected an issue with virtual inputs.

  Applies to: AXIS I8016-LVE
- Corrected an issue with audio microphone pairing.

  Applies to: AXIS P1385, AXIS P1387 and AXIS P1388
- Corrected an intermittent issue with low image quality and bitrate in RTSP-streams, when using Zipstream in combination with PTZ commands.

  Applies to: All products based on *AXIS ARTPEC-7, on page 85* and *AXIS ARTPEC-8, on page 84* with PTZ support.
- Corrected an issue where the incorrect MAC address was shown.

  Applies to: AXIS Q1808-LE

AXIS OS 11.11.120

Release date: 2024-10-28

Corrections

- Corrected an issue with playing profiles with durations, ensuring consistent behavior for light and sound effects.

  Applies to: AXIS D4100-E

- Corrected an issue that caused devices to stop sending video to the VMS after a restart.

  Corrected an issue that could cause the device to stop responding if the video processing system was stopped unexpectedly.

  Applies to: AXIS M1075–L
- Corrected an issue where recording stopped after upgrade if global proxy was set on the recorder.

  Corrected a issue where SSH and network share users were removed after an upgrade.

  Applies to: AXIS S3008. AXIS S3008 MK IIand AXIS S3016

AXIS OS 11.11.117

Release date: 2024-10-11

Corrections

- Corrected an issue with virtual inputs.

  Applies to: AXIS A8207-VE, AXIS A8207-VE Mk II, AXIS I7010-VE, AXIS I8016-LVE and AXIS I8116-E

AXIS OS 11.11.116

Release date: 2024-10-11

Cybersecurity updates

- Updated cURL to version 8.10.1 to increase overall cybersecurity level.
- Updated OpenSSL to version 3.0.15, addressing *CVE-2024-6119* and *CVE-2024-5535*
- Updated OpenSSL to version 1.1.1za, addressing *CVE-2024-5535*.
- Addressed *CVE-2024-8160*. This CVE will be externally disclosed on 26 November 2024, as part of our ongoing commitment to cybersecurity. Detailed information will follow then. For more information, please visit the *Axis vulnerability management portal*.
- Updated expat (libexpat1) to version 2.6.2, addressing *CVE-2024-45490*, *CVE-2024-45491* and *CVE-2024-45492*.
- Updated h2 servers, addressing *RUSTSEC-2024-0332*.
- Updated libxml2 to version 2.12.8, addressing *CVE-2024-34459*.
- Updated ncurses (libtinfo5), addressing *CVE-2023-45918*.
- Updated ncurses (libncursesw5), addressing *CVE-2023-50495*.
- Improved stability and reliability of the certificate management service.

Analytics updates

- AXIS Object Analytics
  - Improved the number of false alarms for static scenes in Axis Object Analytics.

    Applies to: D201-S XPT Q6075, ExCam XPT Q6075, AXIS F9104-B Main Unit, AXIS F9111 Main Unit, AXIS F9114/-B Main unit,AXIS P3245-LV/-LVE, AXIS P5654-E/-E Mk II, AXIS P5655-E, AXIS P5676-LE, AXIS Q1951-E, AXIS Q1952-E, AXIS Q6074/-E, AXIS Q6075/-E/-S/-SE, AXIS Q6078-E, AXIS Q6135-LE, AXIS Q6225-LE, AXIS Q6315-LE, AXIS Q6318-LE and AXIS Q8615-E

Note that not all products support AXIS Object Analytics. Note that not all products support AXIS Object Analytics. For more information on compatible products and features, visit the *AXIS Object Analytics*.

Corrections

- Corrected an issue with malformed XML data in the metadata stream.
- Corrected an issue where it was not possible to enable DST using root.Time.DST.Enabled.
- Increased the possible maximum length of the MQTT overlay key.
- Changed the indicated LED from green to off during normal operation.

  Applies to: AXIS C1110-E, AXIS C1111-E, AXIS C1210-E, AXIS C1211-E, AXIS C1310-E Mk II, AXIS C1410 Mk II, AXIS C1510, AXIS C1511, AXISC1610-VE and AXIS XC1311
- Improved system stability by resolving memory leaks in audio service during RTSP connection openings and closures, reducing the risk of crashes.

  Applies to: AXIS C1110-E, AXIS C1111-E, AXIS C1310-E, AXIS C1310-E Mk II, AXIS C1410, AXIS C1410 Mk II, AXIS C1610-VE, AXIS C8110, AXIS C8210 and AXIS XC1311
- Corrected an issue where the camera stopped streaming and the web interface became inaccessible.

  Applies to: AXIS M3085-V, AXIS M3088-V, AXIS M4215-LV/-V and AXIS M4218-LV/-V
- Corrected an issue which caused timestamps of analytics scene description frames to be out of sync with the video.

  Applies to: AXIS Q1656-DLE and AXIS Q1686-DLE
- Corrected an issue with the video not being updated using the new web interface.

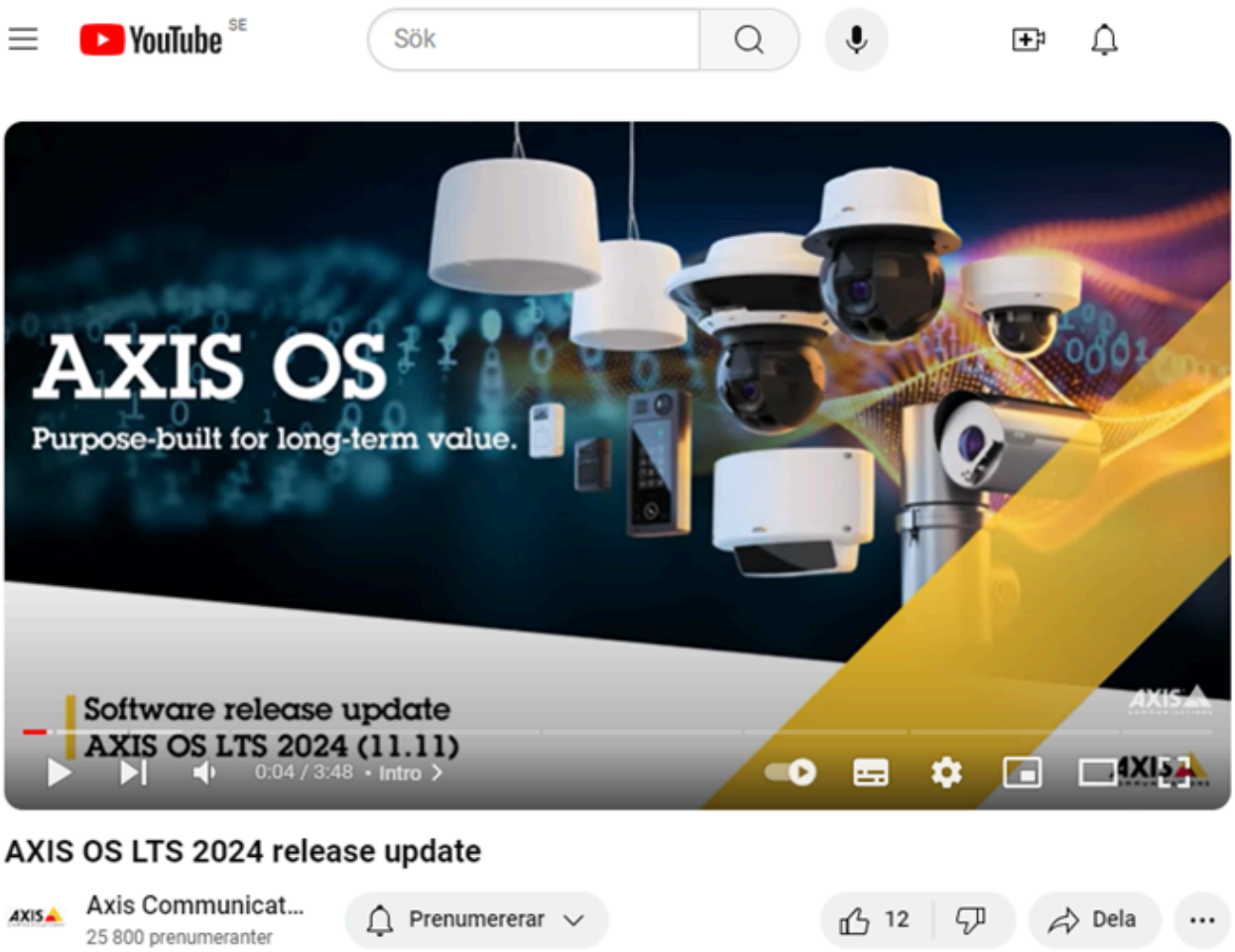
  Applies to: AXIS Q6215-LE
- Corrected an issue where the product could become unavailable over the network after a reboot or a firmware upgrade.

  Applies to: AXIS S3016
- Corrected an issue where the camera could move out of control if it received multiple rapid preset calls.

  Applies to: AXIS Q8752-E

AXIS OS 11.11.109

Release date: 2024-09-10 – 2024-09-18



The first release of AXIS OS LTS 2024 is out. Watch the *release update video* that summarizes the highlights, or read through the complete list of changes below.

Important

A critical issue has been identified when upgrading from latest AXIS OS LTS 2022 10.12.252 to any version other than LTS 2024 11.11.109, on certain Axis products.

This affects: AXIS D3110, AXIS W400, AXIS D4100-E, AXIS M3215-LVE, AXIS M3216-LVE, AXIS P1467-LE, AXIS P1468-LE, AXIS P3265-LV, AXIS P3265-LVE, AXIS P3265-V, AXIS P3267-LV, AXIS P3267-LVE, AXIS P3268-LV, AXIS P3268-LVE, AXIS P3268-SLVE, AXIS Q1656, AXIS Q1656-B AXIS Q1656-BE, AXIS Q1656-BLE, AXIS Q1656-LE, AXIS Q3536-LVE, AXIS Q3538-LVE, AXIS Q3538-SLVE and AXIS S3008.

Example: If you upgrade from 10.12.252 to 11.11.73, the product will become unusable and completely inaccessible. To minimize the damages, we have unpublished AXIS OS 10.12.252 for the above products.

Upgrading from 10.12.252 to 11.11.109 directly works fine. We are working to solve this issue.

After upgrading to 11.11.109, do not perform a factory default and try to downgrade to another version. This will render your product unusable and inaccessible. A fix for this issue is planned for the upcoming 11.11 LTS release.

If you are experiencing this matter with your device please contact *Axis Technical Services* for help.

New products

- AXIS M3125-LVE
- AXIS M3126-LVE
- AXIS M3128-LVE

Features for all products

- Changed the firewall default policy to "Allow" to prevent accidental lockouts when activating the firewall.
- Added support for selecting MQTT client status as a condition when creating event rules.

Cybersecurity updates

- Updated Apache to version 2.4.62, addressing *CVE-2024-40725* and *CVE-2024-40898*.
- Updated libssh2 to version 1.11.0, addressing *CVE-2023-48795*.
- Updated OpenSSH to version 9.8p1, addressing *CVE-2024-6387*.
- Addressed *CVE-2024-6509* and *CVE-2024-6979*. For more information, please visit the *Axis vulnerability management portal*.
- Addressed *CVE-2024-7784*. For more information, please visit the *Axis vulnerability management portal*.

  Note that downgrading the product to an older AXIS OS version is not possible.

  Applies to: Products base on *AXIS ARTPEC-8, on page 84*, *I.MX 6SX, on page 87*, *I.MX 6ULL, on page 87*, *I.MX 8M-Mini, on page 87*, *I.MX 8M-NANO, on page 87* and *I.MX 8QP/M, on page 87*

Analytics updates

- AXIS License Plate Verifier 2.12.8
  - Improved stability and memory optimization.
  - Improved on state recognition for USA number plates where stuck letters such as FT or LR could affect the state recognition of the plate.
  - Improved the libraries for Austrian number plates.
  - Added support for Singapore license plates.
  - Added support for the new license plate prefix region MUC for German license plates.
  - Corrected an issue with too many descriptor files open in buffered events.
  - Corrected an issue for Push Events, wrong value in the Lost event in Unicode filed (umlauts).
  - Corrected an issue when saving sensitivity setting value.
  - Corrected an issue when camera switches between day and night mode.
  - Corrected an issue when the default HTTP/HTTPS port is changed on the camera.

Product specific features

- AXIS Audio Manager Edge: Corrected an issue where streaming from Royal Streaming was not working correctly.
- Improved Radar pairing function stability and introducing automatic reconnect if the connection between the radar and camera drops. Applies to: AXIS D2210-VE, AXIS P1465-LE-3, AXIS P3265-LE-3 and AXIS Q1700-LE

Corrections

- Removed example private keys, previously intended for demonstration purposes only, to address security scanner findings.
- Corrected an issue where it was not possible to upgrade from AXIS OS version 8.20 or older.Applies to: Products based on *AXIS ARTPEC-6, on page 85*

- Changed the indicated LED from green to off during normal operation.Applies to: AXIS C1110-E, AXIS C1111-E, AXIS C1210-E, AXIS C1211-E, AXIS C1310-E Mk II, AXIS C1410 Mk II, AXIS C1510, AXIS C1511, AXIS C1610-VE and AXIS XC1311
- Corrected an issue with radar stream orientation when the camera video stream was rotated.Limitation: The radar video stream will always match the camera rotation. If the camera stream is rotated, the radar live view will rotate as well.Applies to: AXIS D2110-VE, AXIS D2210-VE, AXIS P1465-LE-3, AXIS P3265-LE-3 and AXIS Q1700-LE
- Corrected an issue where AXIS TU8003 was not working correctly. Applies to: AXIS P3737-PLE, AXIS P3747-PLVE and AXIS P3748-PLVE
- Corrected an issue where a3dpc API did not work correctly from the DAX ACAP. Applies to: AXIS P8815-2
- Corrected an issue where recordings stopped working when global proxy was set on the recorder. Applies to: AXIS S3008, AXIS S3008 Mk II and AXIS S3016
- Corrected an issue where audio was not being transmitted correctly over HDMI.Applies to: AXIS Q1715
- Corrected an issue where the focus calibration did not work correctly in the web interface. Applies to: AXIS Q6010-E and AXIS Q6100-E

The following products will remain on LTS 2024, which means they will have this track as their final track and will not receive AXIS OS 12.

• AXIS A8207-VE • AXIS C1310-E • AXIS C1410 • AXIS M3057-PLVE Mk II • AXIS M3068-P • AXIS M3067-P • AXIS P1375/-E • AXIS P1377/-LE • AXIS P1378/-LE • AXIS P1445-LE/-LE-3 • AXIS P1447-LE • AXIS P1448-LE • AXIS P1455-LE/-LE-3 • AXIS P3227-LV/-LVE • AXIS P3228-LV/-LVE	• AXIS P3245-LV/-LVE/-LVE-3 • AXIS P3245-V/-VE • AXIS P3247-LV/-LVE • AXIS P3248-LV/-LVE • AXIS P3255-LVE • AXIS P3715-PLVE • AXIS P3717-PLE • AXIS P3719-PLE • AXIS P3727-PLE • AXIS P3807-PVE • AXIS P8815-2 • AXIS Q1645/-LE • AXIS Q1647/-LE • AXIS Q1659 • AXIS Q1700-LE	• AXIS Q1785-LE • AXIS Q1786-LE • AXIS Q3515-LV/-LVE • AXIS Q3517-LV/-LVE/SLVE • AXIS Q3518-LVE • AXIS Q3527-LVE • AXIS Q6010-E • AXIS Q6100-E • AXIS Q6215 • D101-A XF P3807 • ExCam XF P1377 • ExCam XF Q1645 • ExCam XF P3807 • F101-A XF P1377 • F101-A XF Q1785 • XP40-Q1785

The following products will remain on LTS 2024, meaning they will have this track as their final track and will not receive AXIS OS 12. However, they will continue to receive Product-specific support (PSS) after the end of LTS 2024 until 2031-12-31.

• AXIS D3110 • AXIS D4100 • AXIS M3077-PLVE	• AXIS Q1951-E • AXIS Q1952-E • AXIS Q9216-SLV

AXIS OS 11 Archived Release Notes

If you're looking for release notes from earlier versions of AXIS OS 11 active track, you can find them *here*.

LTS 2022 - 10.12

Support phase: 2022 – 2027-12-31

Go to *Products on LTS 2022 - 10.12, on page 94* for a list of products on this track.

Release notes for older versions of AXIS OS 10 can be found *here*.

AXIS OS 10.12.345

Release date: 2026-07-13

Product specific features

- Products with Hardware ID A67, A68, A69 and A6A only support active track version 13.0.88 and later, as well as LTS 2026 version 12.11.118 and later, LTS 2024 version 11.11.220 and later, and LTS 2022 version 10.12.345 and later. Applies to: AXIS Q1656, AXIS Q1656-LE, AXIS Q1656-DLE and AXIS Q1686-DLE.

Corrections

- Corrected an issue where IPv4 zero settings were not applied correctly, ensuring better compliance with network standards.Applies to: AXIS P7304

AXIS OS 10.12.338

Release date: 2026-06-09

Cybersecurity updates

- Updated OpenSSH to version 10.3 to increase overall cybersecurity level.
- Updated OpenSSL to version 1.1.1zg to increase overall cybersecurity level.
- Addressed *CVE-2026-31431*, known as *Copy Fail*. For more information, please visit the *Axis vulnerability management portal*.
- Addressed *CVE-2025-13601* and *CVE-2025-14087* in glib-2.86.3.
- Addressed *CVE-2025-68615* in net-snmp-5.9.4.
- Addressed *CVE-2026-2921*, *CVE-2026-3083* and *CVE-2026-3085* in gstreamer-1.26.7.
- Addressed *CVE-2026-7598* and *CVE-2025-5987* in libssh2-1.11.1.
- Addressed *CVE-2026-22184* in zlib-1.3.1.
- Addressed *CVE-2026-41989* in libgcrypt.
- Addressed *ECHO-8a1c-e3df-ae5b*, *ECHO-b834-a843-3668* , *ECHO-dfa5-57c7-ba16* and *CVE-2025-48060* in jq-1.8.1.
- Addressed *MINI-2gpr-cw8q-9r9p* in libcap-2.76.
- Addressed *ALSA-2025:7512* and *RLSA-2025:7512* in expat-2.7.1.
- Addressed *CVE-2025-59375* in expat-2.7.2.
- Addressed *CVE-2025-48060* in ntfs-3g-2022.10.3

Corrections

- Updated tzdata to version 2026a to ensure accurate time zone and daylight saving time transitions.
- Updated the End User License Agreement.
- Corrected an issue where system action configuration was being overwritten.
- Corrected an issue where the password was not hidden in the input field for ACAP applications.
- Corrected an issue where 802.1x EAP-TLS reauthentication could cause recording gaps due to temporary network disconnections.

- Corrected an 802.1X authentication issue affecting multiple devices on a single switch port by introducing a new multi-auth mode.

AXIS OS 10.12.323

Release date: 2026-02-18

Cybersecurity updates

- Updated Apache to version 2.4.66 to increase overall cybersecurity level.
- Updated cURL to version 8.17.0 to increase overall cybersecurity level.
- Updated OpenSSH to version 10.1 to increase overall cybersecurity level.
- Updated OpenSSL to version 1.1.1zd to increase overall cybersecurity level.
- Addressed *CVE-2025-8998*, *CVE-2025-9055* and *CVE-2025-9524*. For more information, please visit the *Axis vulnerability management portal*.
- Addressed *CVE-2024-7784*. Note that downgrading the product to an older AXIS OS version other than the latest supported 11.11 LTS or 10.12 LTS track release is not possible. For more information, please visit the *Axis vulnerability management portal*.

  Applies to: AXIS D3110, AXIS D4100-E, AXIS M3215-LVE, AXIS M3216-LVE, AXIS P1467-LE, AXIS P1468-LE, AXIS P3265-LV, AXIS P3265-LVE, AXIS P3265-V, AXIS P3267-LV, AXIS P3267-LVE, AXIS P3268-LV, AXIS P3268-LVE, AXIS P3268-SLVE, AXIS P4705-PLVE, AXIS P4707-PLVE, AXIS Q1656, AXIS Q1656-B, AXIS Q1656-BE, AXIS Q1656-BLE, AXIS Q1656-LE, AXIS Q3536-LVE, AXIS Q3538-LVE, AXIS Q3538-SLVE and AXIS W400
- Addressed *CVE-2023-21414*. Note that downgrading the product to an older AXIS OS version other than the latest supported 10.12 LTS track release is not possible. For more information, please visit the *Axis vulnerability management portal*.

  Applies to: AXIS M3215-LVE, AXIS M3216-LVE, AXIS P1467-LE, AXIS P1468-LE, AXIS P3265-LV, AXIS P3265-LVE, AXIS P3265-V, AXIS P3267-LV, AXIS P3267-LVE, AXIS P3268-LV, AXIS P3268-LVE, AXIS P3268-SLVE, AXIS P4705-PLVE, AXIS P4707-PLVE, AXIS Q1656, AXIS Q1656-B, AXIS Q1656-BE, AXIS Q1656-BLE, AXIS Q1656-LE, AXIS Q3536-LVE, AXIS Q3538-LVE and AXIS Q3538-SLVE
- Updated libxml2 to version 2.13.8, addressing:
  - *CVE-2025-6021*
  - *CVE-2025-27113*
  - *CVE-2025-32414*
  - *CVE-2025-32415*
  - *CVE-2025-49794*
  - *CVE-2025-49795*
  - *CVE-2025-49796*
- Updated ntfs-3g to to version 2022.10.3, addressing *CVE-2022-40284* and *CVE-2023-52890*.

  Applies to: AXIS S3008 and AXIS W800

Corrections

- Updated the End User License Agreement.
- Ensured continuity in system monitoring by preserving critical logs after upgrades.
- Corrected an issue where zoom modifiers (#z and #Z) were not supported in video clip upload filenames.
- Corrected an issue where zoom modifiers (#z and #Z) was not working correctly with upload image and video upload to ftp or http.
- Corrected an issue where focus was lost after an upgrade or restart.

Applies to: AXIS M1135 MK II, AXIS M1135-E MK II, AXIS M1137 MK II, AXIS M1137-E MK II, AXIS Q1615 MK III, AXIS Q1615-LE MK III, AXIS Q1656 and AXIS Q1656-B

- Corrected an issue with status LED indicator was not turned off..

  Applies to: AXIS M2035-LE and AXIS M2036-LE

AXIS OS 10.12.300

Release date: 2025-08-25

Cybersecurity updates

- Updated OpenSSL to version 1.1.1zc to increase overall cybersecurity level.
- Updated cURL to version 8.14.1, addressing *CVE-2025-5399*.
- Updated Apache to version 2.4.65 to increase overall cybersecurity level.
- Updated FFmpeg versions to version 4.4.6 to increase overall cybersecurity level.

Corrections

- Corrected an issue with HTTP notifications failing due to permission errors.
- Corrected an issue where remounting an encrypted SD card could cause an illegal state if done incorrectly.
- Corrected an issue where SMTP DATA messages did include additional not needed null characters.
- Corrected an issue where Always Multicast would stop and not recover when a sensor signal was lost over the serial link.

  Applies to: AXIS F9114 MAIN UNIT and AXIS F9114-B MAIN UNIT
- Improved Cold Boot Stability for i-CS system lens.

  Corrected an issue where the device would fail to boot in high temperature environments.

  Applies to: AXIS M1135 MK II, AXIS M1135-E MK II, AXIS M1137 MK II and AXIS M1137-E MK II

AXIS OS 10.12.291

Release date: 2025-06-19

Product specific features

- Hardware modifications have been made to proactively prepare for the new NDAA 23 regulations that will be required in 2028. You will find more information about *NDAA Compliance* on axis.com. In AXIS OS knowledge base, you will find more about the *hardware changes*. The hardware ID can be found in Plain config > Properties > System > Hardware ID.
  - Products with Hardware IDs A16, A17 and A18 only support active track 12.3.56 and later, as well as LTS 2024 version 11.11.135 and later, and LTS 2022 10.12.291 and later.

    Applies to: AXIS M5074, AXIS M5075 and AXIS M5075-G

AXIS OS 10.12.289

Release date: 2025-06-02

Features for all products

- Updated time zone database version to 2025b.

Cybersecurity updates

- Updated OpenSSH to version 10.0p1.
- Addressed *CVE-2025-32728*.

Corrections

- Improved stability of the focus daemon when handling oversized messages.
- Corrected an issue in recording-indexer caused by corrupt database version.
- Corrected an issue with the disk event triggers where they were not triggering again after restarting the device.
- Corrected an issue where SMTP DATA messages were incorrectly terminated, causing compatibility issues with strict SMTP servers like Postfix.
- Corrected an issue preventing the units from being reachable after a soft restart, requiring a hard restart to recover.

  Applies to: AXIS D3110 and AXIS W400
- Improved stability of the "lightlogic" daemon.

AXIS OS 10.12.280

Release date: 2025-03-24

Features for all products

- Updated the End User License Agreement.

Cybersecurity updates

- Updated cURL to version 8.12.1 to improve cybersecurity.
- Updated OpenSSL to version 1.1.1zb to increase overall cybersecurity level.
- Updated OpenSSH to version 9.9p2, addressing *CVE-2025-26466*.
- Updated libxml2 to version 2.13.3, addressing *CVE-2024-56171* and *CVE-2025-24928*.
- Addressed *CVE-2024-47261*. This CVE will be externally disclosed on 8 April 2025. More detailed information will follow then. For more information, please visit the *Axis vulnerability management portal*.
- Addressed *CVE-2025-0325*. This CVE will be externally disclosed on 2 June 2025, more detailed information will follow then. For more information, please visit the *Axis vulnerability management portal*.

Product specific features

Hardware modifications have been made to proactively prepare for the new NDAA 23 regulations that will be required in 2028. You will find more information about *NDAA Compliance* on axis.com. In AXIS OS knowledge base, you will find more about the *hardware changes*. The hardware ID can be found in Plain config > Properties > System > Hardware ID.

- Products with Hardware IDs A1D and A1E only support active track 12.4.59 and later, as well as LTS 2024 version 11.11.148 and later, and LTS 2022 version 10.12.280 and later.

  Applies to: AXIS M7116 and AXIS P7316

Corrections

- Fixed Always Multicast Startup Failure.
- Corrected an issue with events using IPv6 recipient.
- Corrected an issue with incorrect headers when sending image via proxy.
- Updated time zone database version to 2025a.
- Corrected an issue where audio stopped working when using transmit.cgi and a content length of zero.

- Improved system stability by addressing a potential memory leak in the Video-Object-Detection process.

  Applies to: AXIS M2035-LE, AXIS M2036-LE, ÄXIS M3085-V, AXIS M3086-V, AXIS M3088-V and M4216-LV/-V
- Corrected an issue where the camera could move out of control if it received multiple rapid preset calls.

  Applies to: AXIS Q8752-E

AXIS OS 10.12.270

Release date: 2025-01-27

Product specific features

- Hardware modifications have been made to proactively prepare for the new NDAA 23 regulations that will be required in 2028. You will find more information about *NDAA Compliance* on axis.com. In AXIS OS knowledge base, you will find more about the *hardware changes*. The hardware ID can be found in Plain config > Properties > System > Hardware ID.
  - Products with Hardware ID A2D only support active track version 12.5.56 and later, as well as LTS 2024 version 11.11.160 and later, and LTS 2022 version 10.12.270 and later.

    Applies to: AXIS M3088–V

Cybersecurity updates

- Updated cURL to version 8.11.1 to increase overall cybersecurity level.
- Updated glib, addressing *CVE-2024-52533*.
- Addressed *CVE-2024-47260* and *CVE-2024-47262*. These CVEs will be externally disclosed on 4 March 2025. More detailed information will follow then. For more information, please visit the *Axis vulnerability management portal*.

Corrections

- Improved "Start Recording" functionality to prevent simultaneous continuous recording.
- Corrected an issue that occurred when importing ECC keys using Trusted Platform Module (TPM) for secure key storage.

  Applies to: All products with SecureKeystore feature
- Corrected a focus issue.

  Applies to: AXIS P1377/-E
- Corrected an intermittent focus issue that sometimes caused blurry images when using wide-angle or partial zoom modes.

  Applies to: AXIS Q6315-LE and AXIS Q6318-LE
- Corrected an issue where the device would reboot unexpectedly when enabling IR (Infrared) and using optical zoom simultaneously.

  Applies to: AXIS Q6315-LE
- Corrected an issue with unexpected reboots when enabling IR and using optical zoom simultaneously.

  Applies to: AXIS Q6315-LE
- Corrected an issue where the device would display a black screen when switching from wall to ceiling mounting mode.

  Applies to: AXIS Q3819-PVE

AXIS OS 10.12.262

Release date: 2024-11-18

Cybersecurity updates

- Addressed *CVE-2024-8772*. This CVE will be externally disclosed on 26 November 2024 as part of our ongoing commitment to cybersecurity. Detailed information will follow then. For more information, please visit the *Axis vulnerability management portal*.
- Addressed *CVE-2023-21418*. For more information, please visit the *Axis vulnerability management portal*.
- Updated libxml2, addressing *CVE-2023-45322* and *CVE-2024-25062*.
- Updated busybox, addressing *CVE-2022-48174*.
- Updated zlib (libz1), addressing *CVE-2023-45853*.
- Restricted access to param.cgi so that only authorized administrators can configure privacy masks.
- Updated wpa-supplicant to version 2.11 to increase overall cybersecurity level.
- Corrected an issue with certificates, where the certificate name was used as the identity.

Corrections

- Corrected an issue where Client Stream Data showed wrong FPS as viewer.

  Limitation: FPS restriction is removed when adaptive stream is enabled for viewers.
- Corrected an issue where # in network sharing passwords was not supported.
- Corrected an issue where mounting network share with 'space' character in the name was not working correctly.
- Corrected an issue where network share recipient hostname with '-' character was not working correctly.
- Corrected an issue where it sometimes was not possible to change encryption password after reset and format of the edge storage.
- Corrected a focus setting issue that prevented users from accessing certain functionalities, such as open iris to set focus, autofocus, and resetting functions, when using a DC iris with the camera.

  Applies to: AXIS P1375, AXIS P1377, AXIS P1378, AXIS Q1645, AXIS Q1645-LE, ExCam XF P1377, ExCam XF Q1645 and F101-A XF P1377
- Addressed unintended presence of Electronic Image Stabilization (EIS) settings in the web interface.

  Applies to: AXIS Q1659

AXIS OS 10.12.257

Release date: 2024-10-11

Cybersecurity updates

- Updated cURL to version 8.10.1 to increase overall cybersecurity level.
- Updated OpenSSL to version 1.1.1za to increase overall cybersecurity level.
- Addressed *CVE-2024-8160*. This CVE will be externally disclosed on 26 November 2024, more detailed information will follow then. For more information, please visit the *Axis vulnerability management portal*.
- Updated expat (libexpat1) version 2.6.2, addressing *CVE-2024-45492*, *CVE-2024-45490* and *CVE-2024-45491*.
- Updated ncurses (libncursesw5), addressing *CVE-2023-50495*and *CVE-2023-29491*.

- Updated ncurses (libtinfo5), addressing *CVE-2023-45918*.
- Improved stability and reliability of the certificate management service.

Corrections

- Corrected an issue where the camera could move out of control if it received multiple rapid preset calls.

  Applies to: AXIS Q8752-E

AXIS OS 10.12.252

Release date: 2024-09-02

Cybersecurity updates

- Updated Apache to version 2.4.62 to increase overall cybersecurity level.
- Updated cURL to version 8.9.0 to increase overall cybersecurity level.
- Updated libssh2 to version 1.11.0 to increase overall cybersecurity level.
- Updated OpenSSL to version 1.1.1y to increase overall cybersecurity level.
- Updated OpenSSH to version 9.8p1 to increase overall cybersecurity level.
- Addressed a vulnerability allowing DHCPv6 lease injection through unvalidated input parameters.
- Removed example private keys, previously intended for demonstration purposes only, to address security scanner findings.
- Addressed CVE-2023-52160 in wpa-supplicant to increase overall cybersecurity level.
- Addressed CVE-2024-0067, CVE-2024-6173, CVE-2024-6509. For more information, please visit the *Axis vulnerability management portal* .
- Addressed CVE-2024-7784. Please note that downgrading the product to an older AXIS OS version is not possible. For more information, please visit the *Axis vulnerability management portal.*Applies to: All products base on *AXIS ARTPEC-8, on page 84*, *I.MX 6SX, on page 87*, *I.MX 6ULL, on page 87*, *I.MX 8M-Mini, on page 87*, *I.MX 8M-NANO, on page 87* and *I.MX 8QP/M, on page 87*

Corrections

- Corrected an issue causing stream crashes via CGI input with invalid float values.Applies to: AXIS Q3515-LV/-LVE, AXIS Q3517-LV/-LVE/-SLVE and AXIS Q3527-LVE
- Corrected an issue that was preventing images from being successfully sent via SFTP.Applies to: AXIS Q6075-E and AXIS Q6135-LE
- Corrected an issue in the Event system where a faulty event topic filter could cause log messages to flood as well as prevent RTSP metadata streams from opening correctly.
- Corrected an issue with malformed XML data in the metadata stream.

AXIS OS 10.12.240

Release date: 2024-06-17

Cybersecurity updates

- Updated Apache to version 2.4.59 to increase overall cybersecurity level.

Corrections

- Corrected an issue where SSH users who used ssh-copy-id to install their SSH key as authorized on the device would unintentionally still have SSH access after a factory default with keeping IP settings.
- Corrected memory problems for products utilizing AXIS O3C Dispatcher service.
- Corrected an issue where invalid data could crash the Remote Syslog cgi.

AXIS OS 10.12.236

Release date: 2024-05-27

Cybersecurity updates

- Addressed CVE-2024-0066. For more information, please visit the *Axis vulnerability management portal*.
- Updated *cURL to version 8.7.1* to increase overall cybersecurity level.

Corrections

- Corrected an issue where mounting network share with 'space' character in the name was not working correctly.
- The parameter RemoteService.ProxyPassword that controls the proxy password has been masked and made unreadable for security reasons.
- Improved stability of the WSDD (Web Services Dynamic Discovery) by addressing potential unexpected crashes.
- Added DNS cache for O3C client to reduce the DNS lookup.
- Corrected an issue causing gradual increase in Snapshot CGI response time.
- Corrected an issue where # in network sharing passwords was not supported.
- Addressed unintended presence of Electronic Image Stabilization (EIS) settings in the web interface. Applies to: AXIS Q1659
- Corrected an issue where IR light setting was not preserved after camera upgrades.Applies to: AXIS M3057-PLVE, AXIS M3058-PLVE, AXIS P1445-LE, AXIS P1445-LE-3, AXIS P1447-LE, AXIS P1448-LE, AXIS P3227-LV, AXIS P3227-LVE, AXIS P3228-LV, AXIS P3228-LVE, AXIS P3245-LV, AXIS P3245-LVE, AXIS P3717-PLE, AXIS P3719-PLE, AXIS Q1700-LE, AXIS Q1785-LE, AXIS Q1786-LE, AXIS Q3515-LV, AXIS Q3515-LVE, AXIS Q3517-LV, AXIS Q3517-LVE, AXIS Q3517-SLVE, AXIS Q3518-LVE, AXIS Q3527-LVE, and AXIS Q6215-LE

AXIS OS 10.12.228

Release date: 2024-03-12

Cybersecurity updates

- Addressed CVE-2024-0055. For more information, please visit the *Axis vulnerability management portal*.
- Updated OpenSSL to version 1.1.1x to increase overall cybersecurity level.
- Updated *cURL to version 8.6.0* to increase overall cybersecurity level.

Corrections

- Updated mDNS Responder Daemon (mDNSResponder) to version 2200.60.25.0.4, enhancing overall system stability.
- Updated time zone database version to 2024a.
- Corrected an issue where the camera did not return to the start position after being physically forced to pan.
- Extended the number of preset positions for the built-in Pelco driver from 32 to 100. Additionally, introduced a new config option in plain configuration (UserAdv parameter).

AXIS OS 10.12.221

Release date: 2024–01–29

Cybersecurity updates

- Addressed CVE-2023-5800. For more information, please visit the *Axis vulnerability management portal*.

- Updated *cURL to version 8.5.0* to increase overall cybersecurity level.
- Updated *Apache to version 2.4.58* to increase the overall cybersecurity level.

Corrections

- Corrected an issue where it was not possible to add license if the ACAP uses semantic versioning.
- Corrected an issue causing slight waves/vibrations in the image.Applies to: AXIS Q6225-LE
- Addressed various stability issues in the SIP daemon.Applies to: AXIS A8207-VE, AXIS A8207-VE Mk II and AXIS I8016-LVE

AXIS OS 10.12.213

Release date: 2023–11–09

Cybersecurity updates

- Addressed CVE-2023-21418. For more information, please visit the *Axis vulnerability management portal*.
- Addressed CVE-2023-4911. For more information, please visit the *Axis vulnerability management portal*.
- Addressed CVE-2023-5553. Note that downgrading the product to an older LTS 2022 version is not possible. For more information, please visit the *Axis vulnerability management portal*. Applies to: All products based on *AXIS ARTPEC-8, on page 84*.
- Updated *cURL to version 8.4.0* to increase overall cybersecurity level.

Corrections

- Corrected an issue preventing I/O notifications to be received from AXIS Companion mobile app.
- Corrected a Pan Tilt Zoom issue using Coaxitron driver.Applies to: AXIS P7304 and AXIS P7316

AXIS OS 10.12.208

Release date: 2023–10-11

Cybersecurity updates

- Updated *cURL to version 8.3.0* to increase overall cybersecurity level.
- Updated OpenSSL to version 1.1.1w to increase the overall cybersecurity level.
- Addressed CVE-2023-21414. Note that downgrading the product to an older LTS 2022 version is not possible except for Q3527-LVE that has support for 9.80 LTS. For more information, please visit the *Axis vulnerability management portal*.Applies to: AXIS A8207-VE Mk II, AXIS Q3527-LVE and all products based on *AXIS ARTPEC-8, on page 84*
- Addressed CVE-2023-21415. For more information, please visit the *Axis vulnerability management portal*.
- Addressed CVE-2023-21417. For more information, please visit the *Axis vulnerability management portal*.

Corrections

- Corrected an issue where the Web interface was unintentionally modifying the timezone upon loading, even if the device had been previously configured outside of the Web interface.
- Corrected an issue where focus and zoom option was not available in the web interface.Applies to: AXIS P3245-LV/-LVE
- Radar track IDs now persist across reboots, preventing collisions with previous boots.Increased the maximum track ID limit significantly to prevent track ID repetition from prolonged radar detector usage. Applies to: AXIS D2050-VE

- Corrected an issue that caused slow-motion pattern playback when starting two light profiles simultaneously.Applies to: AXIS D4100-E

AXIS OS 10.12.199

Release date: 2023–08-21

Features

- Added support for AXIS T6101/T6112 Mk II with the same audio and I/O functionality as when combined with AXIS T6101/T6112.Applies to: AXIS M3115-LVE, AXIS M3116-LVE, AXIS M3064-V, AXIS M3065-V, AXIS M3066-V and AXIS M3075-V

Cybersecurity updates

- Updated *cURL to version 8.2.0* to increase overall cybersecurity level.
- Updated OpenSSL to version 1.1.1v to increase the overall cybersecurity level.

Corrections

- Corrected CVE-2023-21413. For more information, please visit the *Axis vulnerability management portal*.
- Added the possibility to Netd Service to preserve the static resolver configuration even after a soft restore, safeguarding static DNS/Search domain settings.
- Updated the mDNS Responder Daemon (mDNSResponder) to version 1790.80.10 to improve system stability.
- Corrected an issue with incorrect trigger of I/O ports, that occurs at upgrade if an AXIS T6101 or AXIS T6112 is connected to the device. Applies to: All products with support for *AXIS T6101 and AXIS T6112*
- Corrected microphone power type when the product is used in combination with AXIS T6101 audio module.Applies to: AXIS P3255-LVE
- Improved stability by addressing a potential memory leak in the remote camera control service.Applies to: AXIS P3818-PVE, AXIS Q3819-PVE, AXIS Q6010-E and AXIS Q6100-E
- Corrected an issue where manual focus was not working correctly via ONVIF command, if using third-party driver.Applies to: AXIS Q1656 and AXIS Q1656-B
- Corrected an issue with Orientation Aid ACAP to be able to move the compass bar correctly via ONVIF commands.Applies to: AXIS Q6135-LE and AXIS Q6315-LE
- Corrected an issue where wiper was not possible to run through ONVIF command.Applies to: AXIS Q8752-E

AXIS OS 10.12.197

Release date: 2023–08-04

Corrections

- Corrected an issue that could bring the camera in an out of focus state. To activate the correction on affected units, an additional restart is required after the upgrade.Applies to: AXIS Q3536-LVE and AXIS Q3538-LVE

AXIS OS 10.12.193

Release date: 2023–07-20

Features

- Improved SNMP Monitoring by adding support for the ipAddressTable OID.
- Updated AXIS License Plate Verifier to version 2.8.4.Applies to: AXIS P3245-LVE-3, AXIS P1455-LE-3 and AXIS P1445-LE-3

- Corrected CVE-2023-21407, CVE-2023-21408, CVE-2023-21409, CVE-2023-21410, CVE-2023-21411, CVE-2023-21412. For more information, please visit the *Axis vulnerability management portal*.
- Added extra polygons to the Area of Interest for a more flexible coverage of the area.
- Added the possibility for 2N integration to select the type of event by direction, any, in or out which it can be send to 2N IP device.
- Added the possibility to set image parameters according to the manual for none AXIS License Plate Verifier kit cameras.
- Added the possibility to send two images with Push Event, one image will be the license plate crop and the other image will be the same frame as used to be saved with the event under **Settings > Image > Save Full Frame**.
- Added a new VAPIX event ALPV.Update. This event will be triggered together with metadata for every updated event.

Corrections

- Corrected the focal length limits when using a CS-mount lens with DC-iris.Applies to: AXIS Q1647, AXIS Q1647-LE, AXIS Q1645, AXIS Q1645-LE and ExCam XF Q1645

AXIS OS 10.12.182

Release date: 2023–06-19

Features

- Added support for more than 7 identical streams. The maximum identical streams is equal to the MaxViewers parameter value.
- Enhanced SNMP Monitoring: We resolved a missing TCP sub-tree OID issue in NET-SNMP by adding support for the SNMP TCP MIB object .1.3.6.1.2.1.6. This improvement ensures a smooth and uninterrupted SNMP monitoring experience.
- Improved UPnP compliance by updating the SSDP (Simple Service Discovery Protocol) SERVER header in the standard "OS/version UPnP/1.0 product/version" format and USN (Unique Service Name) field with a UUID in the standard format. This enhances consistency and compatibility.
- Added proxy configuration support to the Owner Authentication Key (OAK) cgi using group root. RemoteService, simplifying setup on networks requiring proxy servers for Internet access and improving the authentication process.
- Updated time zone database version to 2023c.
- Added support for Network speaker pairing (Edge-to-edge technology), enabling synchronization of audio playback.Applies to: AXIS Q6225-LE

Cybersecurity updates

- Updated *Apache to version 2.4.57* to increase the overall cybersecurity level.
- Updated *cURL to version 8.1.0* to increase overall cybersecurity level.
- Updated OpenSSL to version 1.1.1u to increase the overall cybersecurity level.

Corrections

- Corrected an issue with OAK (owner authentication key). It now only produces warnings in the log instead of errors if the device is not able to connect to the internet.
- Corrected an issue where sequence ID modifiers #s and #S were not displaying the expected values.
- Improved performance for video streams when using same configurations.
- Corrected an issue in VDO Api, related to orientation when rotation has been changed.
- Corrected an issue where ONVIF recordings resumed after factory default.
- Updated libupnp to version 1.14.16, fixing a memory leak and improving overall stability.

- Corrected a memory leak in the video service, resulting in improved stability for streaming videos.
- Improved the syslog system stability by fixing a memory leak.
- Corrected an issue where artifacts could appear in the image when WDR is enabled and panning and tilting between different lighting conditions.Applies to: AXIS Q6315-LE
- Improved system reliability. To ensure uninterrupted streaming, we have optimized the response time of requests and increased the MCU's IWDG timeout to prevent restarts caused by unreliable communication.Applies to: AXIS M3205-LVE and AXIS M3206-LVE
- Corrected a focus setting issue that prevented users from accessing certain functionalities, such as open iris to set focus, autofocus, and resetting functions, when using a DC iris with the camera.Applies to: AXIS P1375, AXIS P1377, AXIS P1378, AXIS Q1645, AXIS Q1645-LE, ExCam XF P1377, ExCam XF Q1645 and F101-A XF P1377
- Corrected CVE-2023-21405. For more information, please visit the *Axis vulnerability management portal*.Applies to: AXIS A8207-VE and AXIS A8207-VE Mk II
- Corrected an auto focus issue causing inaccurate coordinates on set focus window.Applies to: AXIS M5074, AXIS M5075/-G, AXIS P3245-LV/-LVE/-V/-VE, AXIS P3245-LVE-3, AXIS P3247-LV/-LVE, AXIS P3248-LV/-LVE, AXIS P3255-LVE, AXIS P5654-E, AXIS P5655-E, AXIS Q1700-LE, AXIS Q1715, AXIS Q1785/-LE, AXIS Q1786-LE, AXIS Q1798-LE, AXIS Q3515-LV/-LVE, AXIS Q3517-LV/-LVE/-SLVE, AXIS Q3518-LVE, AXIS Q3527-LVE, AXIS Q6135-LE, AXIS Q8752-E, ExCam XF Q1785, F101-A XF Q1785, XF40-Q1785 and XP40-Q1785

AXIS OS 10.12.166

Release date: 2023–04–17

Features

- Updated *cURL to version 8.0.1* to increase overall cybersecurity level.
- Updated *Apache to version 2.4.56* to increase the overall cybersecurity level.
- Improved the manager client certificates and added support for installing multiple trust certificates and requesting/installing a second client certificate.
- Products with Hardware ID 971 only support active track 11.4.52 and later, as well as LTS 2022 version 10.12.166 and later. The hardware ID can be found in **Plain config > Properties > System > Hardware ID**. Applies to: AXIS M5075-G
- Added detailed health information from SD cards to the server report, including power cycle statistics and flash wear rates. This improvement allows for a better monitoring of the system's health that can prevent downtime or data loss.

Corrections

- Corrected an issue in mDNS discovery that caused the reported port to be incorrect due to the network byte order not being properly handled. The correct port is now being printed.
- Improved network interface handling to prevent memory leaks and crashes by automatically restarting the web service discovery client daemon (wsdd) when network changes occur, ensuring uninterrupted service.
- Added fallback mode for network hardware that is limited to 10BASE-T and 100BASE-TX transmission. Applies to: All *AXIS ARTPEC-7, on page 85* products
- Corrected low-light image quality issues.Applies to: AXIS Q1700-LE, AXIS Q1785-LE, AXIS Q1786-LE, ExCam XF Q1785, F101-A XF Q1785, XF40-Q1785 and XP40-Q1785
- Corrected a focus setting issue that prevented users from accessing certain functionalities, such as open iris to set focus, autofocus, and resetting functions, when using a DC iris with the camera.Applies to: AXIS P1375, AXIS P1377, AXIS P1378, AXIS Q1645, AXIS Q1645-LE, ExCam XF P1377, ExCam XF Q1645 and F101-A XF P1377

- Corrected an issue where live view via HDMI could be accessed without setting a password. To enhance security, it is now mandatory to set up a password before being able to access live feed on a TV or monitor via HDMI.Applies to: AXIS V5925

AXIS OS 10.12.153

Release date: 2023-02-20

Features

- Updated *Apache to version 2.4.55* to increase the overall cybersecurity level.
- Updated OpenSSL to version 1.1.1t to increase overall cybersecurity level.
- Updated *cURL to version 7.87.0* to increase overall cybersecurity level.
- The Security level for 'AutoRepair', 'FileSystem' and 'RequiredFileSystem' parameters has been lowered.

Corrections

- Disabled secure redirects from other network hosts net.ipv4.conf.all.secure_redirects & net.ipv4.conf.default.secure_redirects to increase overall minimum cybersecurity level.
- Corrected an issue where audio was not working correctly in the Companion and AXIS Camera Station iOS apps. Correction was also needed in the iOS apps, therefore requires iOS Companion version 7.11.14 or later, and iOS AXIS Camera Station 4.6.12 or later.Applies to: All products with audio out.
- Corrected an issue where is was not possible to install an application using manifest.json if an older application using package.conf was already installed.
- Corrected an issue affecting some O3C clients, that caused internal authentication requests to fail after a few days of uptime.
- Corrected an issue where it was not possible to save images using compression set to 10 or below to a network share when SMB 3.1.1 was used.
- Updated time zone database version to 2022g.
- Improved stability of syslog system by addressing a potential memory leak.
- Improved system stability during roll-back.
- Improved stability of the multicast DNS (mDNS) services.
- Corrected ONVIF reply for MaximumRetentionTime
- Corrected an issue with simultaneous PTZ Onvif requests.Applies to: All products with PTZ support.
- Corrected an issue where the IR led was turned off during the download of the server report.Applies to: AXIS Q6135-LE
- Corrected an IR-LED issue causing temperatures and image degradation in high ambient temperatures above 35°C, when IR light is activated at full power.Applies to: AXIS Q6318-LE
- Improved QuickZoom functionality to switch only during longer continuous zoom movements, ensuring smoother zoom experience with the mouse scroll wheel.Applies to: AXIS Q6135-LE and AXIS Q6318-LE
- Corrected an issue with focus being lost over time.Applies to: AXIS M3215-LVE, AXIS M3216-LVE, AXIS P1467-LE, AXIS P1468-LE, AXIS P3265-V/-LV/-LVE, AXIS P3267-LV/-LVE, AXIS P3268-LV/-LVE, AXIS P4705-PLVE, AXIS P4707-PLVE, AXIS Q1656/-B/-BE/-BLE/-LE, AXIS Q3536-LVE and AXIS Q3538-LVE
- Corrected an issue that caused pre-defined controls buttons to appear in the wrong place on the onscreen control panel.Applies to: All products with onscreen control support.
- Corrected an issue where autofocus needed to be re-applied when the ambient temperature changed. Applies to: AXIS P3265-V/-LV/-LVE, AXIS P3267-LV/-LVE, AXIS P3268-LV/-LVE, AXIS Q3536-LVE and AXIS Q3538-LVE

AXIS OS 10.12.145

Release date: 2023–02–02

- Improved day/night switching stability. After upgrade a power off/on of the camera is required.Applies to: AXIS M3205-LVE and AXIS M3206-LVE

AXIS OS 10.12.135

Release date: 2022-12-08

Features

- Products with Hardware 9A0.1, 9A0.2 and 9A0.3 only support LTS 2022 version 10.12.135 and later. Products with hardware ID 796, 7C3.1 and 7C3.2 support all AXIS OS versions.The hardware ID can be found in **Plain config > Properties > System > Hardware ID**.Applies to: AXIS P1375–E, AXIS P1377–LE and AXIS P1378–LE

AXIS OS 10.12.130

Release date: 2022–12–05

Features

- Updated cURL to version 7.86.0 to increase overall cybersecurity level.
- Updated OpenSSL to version 1.1.1s to increase the overall cybersecurity level.

Corrections

- Corrected an issue where the metadata producer was disabled after upgrade when upgrading from AXIS OS 10.6 or 10.7 to 10.12.
- Corrected an issue that caused the wrong file size to be reported for recordings larger than 50MB when using FTP.
- Corrected an issue where ACAP application parameters were reset after AXIS OS upgrade.
- Corrected an issue to make it possible to create certificates with Common Name up to 64 characters.
- The vdo_stream_get_info capture API now returns the resulting channel.
- Corrected an issue with video streaming when using dynamic fps in Zipstream.Applies to: AXIS M3064-V, AXIS M3065-V, AXIS M3066-V, AXIS M3075-V, AXIS M3205-LV, AXIS M3206-LVE and AXIS Q9216-SLV
- Corrected an issue with broken image that could happen after start up.Applies to: AXIS M2035-LE and AXIS M2036-LE
- Corrected an issue where the Iris value was not shown when using Auto Iris.Applies to: AXIS V5925
- Corrected an issue which could cause audio clips not to play to completion.Applies to: AXIS Q6215-LE
- Corrected an issue that caused privacy masks to shift when using pan and tilt.Applies to: AXIS P1375
- Corrected an issue with loss of focus in wide infinity, that could occur after upgrading from 10.9.Applies to: AXIS P1448-LE
- Corrected an issue where the camera was not getting enough power when using certain POE switches. Applies to: AXIS Q6075 and ExCam XPT Q6075

AXIS OS 10.12.122

Release date: 2022-11-03

Corrections

- Corrected an issue where upgrade from 10.9.4 to 10.12 was not possible.Applies to: AXIS P3265-LVE 22mm, AXIS 3267-LV/-LVE and AXIS P3268-LV/-LVE.

AXIS OS 10.12.114

Release date: 2022-10–06

Features

- Updated cURL to version 7.85.0 to increase overall cybersecurity level.
- Added support for RFC8200 IPv6.

Corrections

- Corrected an issue to make it possible to create certificates with Common Name up to 64 characters.
- Corrected an issue that caused no video stream after upgrading from 9.80 LTS.Applies to: AXIS Q3527-LVE
- Improved the IR cut filter switching.Applies to: All products with IR cut filter.
- Corrected an issue where image processing could fail to work properly after 248 days of uptime.Applies to: AXIS Q1645/-LE and ExCam XF Q1645
- Corrected an issue where the new web interface was not showing streaming settings.Applies to: AXIS M2035-LE, AXIS M2036-LE, AXIS M3057-PLVE, AXIS M3058-PLVE, AXIS M3064-V, AXIS M3065-V, AXIS M3066-V, AXIS M3067-P, AXIS M3068-P, M3075-V, AXIS M3085-V, AXIS M3086-V, AXIS M3115-LVE, AXIS M3116-LVE, AXIS M3205-LVE, AXIS M3206-LVE, AXIS M4216–V/-LV, AXIS P3719-PLE

Limitations

- When upgrading AXIS OS from versions below 10.10.69 and metadata producers are used, the metadata producers must be enabled manually via **System > Analytics metadata**.

AXIS OS 10.12.104

Release date: 2022-09-13

Features

- Updated cURL to version 7.84.0 to increase overall cybersecurity level.
- Added setting in Action rules for how many times an audio clip should be repeated when played.
- Products with hardware ID 998 only support active track 10.12.104 and later, as well as LTS 9.80.3.14 and later. Products with hardware ID 7CA support all AXIS OS versions. The hardware ID can be found in **Plain config > Properties > System > HardwareID**.Applies to: AXIS P3925-R
- Products with hardware ID 999 only support active track 10.12.104 and later, as well as LTS 9.80.3.14 and later. Products with hardware ID 7CC support all AXIS OS versions. The hardware ID can be found in **Plain config > Properties > System > HardwareID**. Applies to: AXIS P3925-LRE
- Products with hardware ID 99A.1 and 99A.2 only support active track 10.12.104 and later, as well as LTS 9.80.3.14 and later. Products with hardware ID 91A only support active track 10.10.69 and later, as well as LTS 2020 version 9.80.3.8. Products with hardware ID 7CC support all AXIS OS versions. The hardware ID can be found in **Plain config > Properties > System > HardwareID**. Applies to: AXIS P3935-LR
- Added the possibility to detect tailgating, if more than one person passes under a counter during a predefined time interval.Applies to: AXIS P8815-2.

Corrections

- Improved system stability.
- Corrected an issue that prevented the use of audio clips in action rules. Applies to: AXIS A8207-VE and AXIS A8207-VE Mk II
- Improved IR LED dimming algorithm.Applies to: AXIS Q3536-LVE and AXIS Q3538-LVE
- Corrected an issue to make WDR enabled as default. Applies to: AXIS M1135/-E Mk II and AXIS M1137/-E Mk II

- Corrected an issue where focus is lost over time.Applies to: AXIS P3727-PLE
- Corrected an issue in swaying object filters that made video stream flicker and metadata stream fail. Corrected an issue where ignore swaying objects was disabled after restart. Improved tracking at large angles. Improved general radar performance and stability.Applies to: AXIS D2110-VE

AXIS OS 10 Archived Release Notes

If you're looking for release notes from earlier versions of AXIS OS 10 active track, you can find them *here*.

PSS 9.80

Support phase: 2020 – 2025-12-31

Go to *Products on PSS 9.80, on page 95* for a list of products on this track.

AXIS OS 9.80.146

Release date: 2026-06-29

Important

AXIS P1435-LE will not receive future updates since it has reached its end of software support.

Cybersecurity updates

- Updated Apache to version 2.4.67 to increase overall cybersecurity level.
- Updated OpenSSH to version 10.3 to increase overall cybersecurity level.
- Updated OpenSSL to version 1.1.1zh to increase overall cybersecurity level.
- Updated libssh2 to version 1.11.1 to address *CVE-2026-7598* and *CVE-2025-5987*.
- Addressed *CVE-2025-59375*, *CVE-2026-41989* and *CVE-2025-14087*.
- Addressed *CLSA-2026-1773684237* in ca-certificates-20260223.
- Addressed *ALSA-2025:7512* in expat-2.7.1.

Corrections

- Updated the End User License Agreement.
- Corrected an issue where multiline parameters were not accepted for ACAP applications.
- Corrected an issue where specially crafted inputs could cause high CPU utilization, improving overall system stability and security.
- Corrected truncated response issue in param.cgi when XML content is requested, which previously caused AXIS Device Manager to fail retrieving device configurations.

AXIS OS 9.80.132

Release date: 2026-01-12

Cybersecurity updates

- Updated cURL to version 8.17.0 to increase overall cybersecurity level.
- Updated OpenSSH to version 10.1 to increase overall cybersecurity level.
- Updated OpenSSL to version 1.1.1zd to increase overall cybersecurity level.
- Updated libxml2 to version 2.14.6, addressing *CVE-2025-27113*.
- Updated libxml2 to version 2.13.8, addressing *CVE-2025-6021*, *CVE-2025-49794*, *CVE-2025-49795*, *CVE-2025-49796*, *CVE-2025-32414* and *CVE-2025-32415*.
- Addressed *CVE-2025-8998*, *CVE-2025-9055* and *CVE-2025-9524*. These CVEs will be externally disclosed on 11 November. Detailed information will follow then. For more information, please visit the *Axis vulnerability management portal*.

Important

This is the last release on the AXIS OS LTS 2020 track.

- The following products will not receive any further releases as their hardware warranty and software support period has expired:
- The following products will continue to receive releases until their hardware warranty and software support period expires:

All other products have the later LTS tracks. See the for a complete list of products and their support status.

AXIS OS 9.80.121

Release date: 2025-09-22

Cybersecurity updates

- Updated OpenSSH to version 10.0p1.
- Updated cURL to version 8.14.1, addressing *CVE-2025-5399*.
- Updated OpenSSL to version 1.1.1zc to increase overall cybersecurity level.
- Updated Apache to version 2.4.65 to increase overall cybersecurity level.
- Updated FFmpeg to version 4.2.11 to increase overall cybersecurity level.
- Addressed *CVE-2025-32728*.

Corrections

- Corrected an issue with HTTP notifications failing due to permission errors.
- Corrected an issue in recording-indexer caused by corrupt database version.
- Corrected an issue where SMTP DATA messages did include additional not needed null characters.
- Corrected an issue where remounting an encrypted SD card could cause an illegal state if done incorrectly.
- Corrected an issue with recording to encrypted SD card while streaming RTSPS.

  Applies to: All products based on ARTPEC-5

AXIS OS 9.80.105

Release date: 2025-04-22

Cybersecurity updates

- Updated cURL to version 8.12.1 to increase overall cybersecurity level.
- Updated OpenSSL to version 1.1.1zb to increase overall cybersecurity level.
- Updated OpenSSH to version 9.9p2, addressing *CVE-2025-26466*.
- Updated libxml2 to version 2.13.3, addressing *CVE-2025-24928* and *CVE-2024-56171*.
- Updated ffmpeg to version 4.2.10, addressing *CVE-2019-13312*, *CVE-2019-13390*, *CVE-2019-15942*, *CVE-2020-12284*, *CVE-2020-13904*, *CVE-2020-20446*, *CVE-2020-20448*, *CVE-2020-20451*, *CVE-2020-20453*, *CVE-2020-20891*, *CVE-2020-20892*, *CVE-2020-20896*, *CVE-2020-20902*, *CVE-2020-21041*, *CVE-2020-22015*, *CVE-2020-22016*, *CVE-2020-22019*, *CVE-2020-22020*, *CVE-2020-22021*, *CVE-2020-22022*, *CVE-2020-22023*, *CVE-2020-22025*, *CVE-2020-22026*, *CVE-2020-22027*, *CVE-2020-22028*, *CVE-2020-22031*, *CVE-2020-22032*, *CVE-2020-22036*, *CVE-2020-22037*, *CVE-2020-22041*, *CVE-2020-22044*, *CVE-2020-22046*, *CVE-2020-22048*, *CVE-2020-23906*, *CVE-2020-35964*, *CVE-2020-35965*, *CVE-2021-38114*, *CVE-2021-38171*, *CVE-2021-38291*, *CVE-2022-3109* and *CVE-2023-47342*.
- Addressed *CVE-2024-47261*. For more information, please visit the *Axis vulnerability management portal*.
- Addressed *CVE-2025-0325*. This CVE will be externally disclosed on 2 June 2025 as part of our ongoing commitment to cybersecurity. Detailed information will follow then. For more information, please visit the *Axis vulnerability management portal*.

Corrections

- Updated the End User License Agreement.
- Updated time zone database to version 2025b.

- Corrected an issue where SMTP DATA messages were incorrectly terminated, causing compatibility issues with strict SMTP servers like Postfix.
- Corrected an issue with incorrect headers when sending image via proxy.
- Corrected an issue where Always Multicast stopped working after a device upgrade.
- Improved stability of "focusd", "maskd", and "blinkenlights" daemons when handling oversized messages.
- Added AXIS TQ1818-E Positioning Unit Support enabling compatibility with various PT Mount and camera models.

  Applies to: AXIS P1364, AXIS P1365 Mk II, AXIS P1367/-E, AXIS P1368-E, AXIS P1375/-E, AXIS P1377/-LE, AXIS P1378/-LE, AXIS Q1615 Mk II, AXIS Q1645, AXIS Q1647, AXIS Q1659, AXIS Q1785, AXIS Q1941, AXIS Q1942, AXIS Q8641-E and AXIS Q8642-E
- Improved stability of the "lightlogic" daemon.

  Applies to: AXIS M1065-LW

AXIS OS 9.80.95

Release date: 2025-02–25

Cybersecurity updates

- Addressed *CVE-2024-47260* and *CVE-2024-47262*. This CVE will be externally disclosed on 4 March 2025 as part of our ongoing commitment to cybersecurity. Detailed information will follow then. For more information, please visit the *Axis vulnerability management portal*.
- Updated glib, addressing *CVE-2024-52533*.
- Updated libexpat to version 2.6.4, addressing *CVE-2024-50602*.
- Updated cURL to version 8.11.1 to increase overall cybersecurity level.

Corrections

- Corrected issue preventing AXIS Companion mini cameras from configuring storage during AXIS Camera Station Edge site creation wizard setup.
- Improved "Start Recording" functionality to prevent simultaneous continuous recording.
- Corrected an issue where the Wireless 802.1X EAP-TLS authentication is not working if the CA certificate is not configured.

  Applies to: AXIS M1065-LW and AXIS M3045-WV

AXIS OS 9.80.85

Release date: 2024-11–19

Cybersecurity updates

- Addressed *CVE-2024-8772*. This CVE will be externally disclosed on 26 November 2024 as part of our ongoing commitment to cybersecurity. Detailed information will follow then. For more information, please visit the *Axis vulnerability management portal*.
- Updated ncurses (libncursesw5 and libtinfo5), addressing *CVE-2023-50495*, *CVE-2023-45918* and *CVE-2023-29491*.
- Updated expat (libexpat1) version 2.6.2, addressing *CVE-2024-45492*, *CVE-2024-45490* and *CVE-2024-45491*.
- Updated libxml2, addressing *CVE-2023-45322* and *CVE-2024-25062*.
- Updated busybox, addressing *CVE-2022-48174*.
- Updated zlib (libz1), addressing *CVE-2023-45853*.

- Updated util-linux, addressing *CVE-2024-28085*.
- Updated syslog-ng, addressing *CVE-2022-38725*.
- Updated Dbus to version 1.12.28, addressing *CVE-2023-34969*.
- Updated cURL to version 8.10.1 to increase overall cybersecurity level.
- Updated OpenSSL to version 1.1.1za to increase overall cybersecurity level.
- Updated wpa-supplicant to version 2.11 to increase overall cybersecurity level.
- Improved stability and reliability of the certificate management service.

Corrections

- Corrected an issue with Malformed XML data in the metadata stream.
- Corrected an issue limiting audio sampling rate selection to 8kHz in ONVIF media profile, now supporting rates of 8/16/32/44.1/48 kHz.

  Applies to: AXIS P1364/-E

AXIS OS 9.80.78

Release date: 2024-08–26

Cybersecurity updates

- Updated Apache to version 2.4.62 to increase overall cybersecurity level.
- Updated cURL to version 8.9.0 to increase overall cybersecurity level.
- Updated OpenSSL to version 1.1.1y to increase overall cybersecurity level.
- Updated OpenSSH to version 9.8p1 to increase overall cybersecurity level.
- Updated libssh2 to version 1.11.0 to increase overall cybersecurity level.
- Addressed CVE-2023-52160 in wpa-supplicant to increase overall cybersecurity level.
- Addressed CVE-2024-0067, CVE-2024-6173, CVE-2024-6509. For more information, please visit the *Axis vulnerability management portal*.

Corrections

- Added DNS cache for O3C client to reduce the DNS lookup.
- Corrected an issue causing stream crashes via CGI input with invalid float values.Applies to: AXIS Q3515-LV/-LVE, AXIS Q3517-LV/-LVE/-SLVE and AXIS Q3527-LVE

AXIS OS 9.80.72

Release date: 2024-06-17

Corrections

- Corrected an issue where SSH users who used ssh-copy-id to install their SSH key as authorized on the device would unintentionally still have SSH access after a factory default with keeping IP settings.
- Corrected memory problems for products utilizing AXIS O3C Dispatcher service.

AXIS OS 9.80.69

Release date: 2024–05–28

Cybersecurity updates

- Addressed CVE-2024-0066. For more information, please visit the *Axis vulnerability management portal*.

- The parameter RemoteService.ProxyPassword that controls the proxy password has been masked and made unreadable for security reasons.

AXIS OS 9.80.66

Release date: 2024–05–06

Cybersecurity updates

- Addressed CVE-2024-0054. For more information, please visit the *Axis vulnerability management portal*.
- Updated OpenSSH to version 9.6p1 to increase overall cybersecurity level.
- Updated *cURL to version 8.7.1* to increase overall cybersecurity level.
- Updated OpenSSL to version 1.1.1x to increase overall cybersecurity level.
- Removed legacy overlay image CGIs i.e. create_overlay, overlay_set, overlay_del, overlay_image_ formats, overlay_list.

Corrections

- Updated time zone database version to 2024a.

AXIS OS 9.80.55

Release date: 2024–02–05

Cybersecurity updates

- Updated *cURL to version 8.5.0* to increase overall cybersecurity level.
- Updated *Apache to version 2.4.58* to increase the overall cybersecurity level.
- Addressed CVE-2023-5800. For more information, please visit the *Axis vulnerability management portal*.

AXIS OS 9.80.49

Release date: 2023–11–01

Cybersecurity updates

- Updated *cURL to version 8.4.0* to increase overall cybersecurity level.

Corrections

- Corrected CVE-2023-21417 and CVE-2023-21418. For more information, please visit the *Axis vulnerability management portal*.
- Corrected critical Kernel crashes for improved system stability.Applies to: AXIS M2026-LE Mk II, AXIS M3015, AXIS M3016, AXIS M3106-L/-LVE Mk II, AXIS Q6125-LE and ExCam XF M3016

AXIS OS 9.80.47

Release date: 2023–10–13

Cybersecurity updates

- Updated *cURL to version 8.3.0* to increase overall cybersecurity level.
- Updated OpenSSL to version 1.1.1w to increase the overall cybersecurity level.

Corrections

- Corrected CVE-2023-21415. For more information, please visit the *Axis vulnerability management portal*.
- Improved stability of the WSDD (Web Services Dynamic Discovery) by addressing a potential memory leak and crashes associated with network interface rebinding on network changes.

AXIS OS 9.80.42

Release date: 2023–08–22

Cybersecurity updates

- Updated *cURL to version 8.2.0* to increase overall cybersecurity level.
- Updated OpenSSL to version 1.1.1v to increase the overall cybersecurity level.

Corrections

- Added proxy configuration support to the Owner Authentication Key (OAK) cgi using group root. RemoteService, simplifying setup on networks requiring proxy servers for Internet access and improving the authentication process.
- Added the possibility to Netd Service to preserve the static resolver configuration even after a soft restore, safeguarding static DNS/Search domain settings.
- Improved stability of UPnP (Universal Plug and Play) service.
- Updated the mDNS Responder Daemon (mDNSResponder) to version 1790.80.10 to improve system stability.
- Improved stability of the syslog system by addressing a potential memory leak.

AXIS OS 9.80.34

Release date: 2023–06–26

Features

- Improved UPnP compliance by updating the SSDP (Simple Service Discovery Protocol) SERVER header in the standard "OS/version UPnP/1.0 product/version" format and USN (Unique Service Name) field with a UUID in the standard format. This enhances consistency and compatibility.
- Updated time zone database version to 2023c.

Cybersecurity updates

- Updated *Apache to version 2.4.57* to increase the overall cybersecurity level.
- Updated *cURL to version 8.1.0* to increase overall cybersecurity level.
- Updated OpenSSL to version 1.1.1u to increase the overall cybersecurity level.
- Updated libupnp to version 1.14.16, solving a memory leak and improving overall stability.

Corrections

- Corrected an issue with OAK (owner authentication key). It now only produces warnings in the log instead of errors if the device is not able to connect to the internet.
- Improved the handling of SD card timeouts, ensuring that processes no longer hang for prolonged periods when a faulty SD card is detected. Applies to: All products with SD card support

AXIS OS 9.80.28

Release date: 2023–04–24

Features

- Updated *Apache to version 2.4.56* to increase the overall cybersecurity level.
- Updated *cURL to version 8.0.1* to increase overall cybersecurity level.
- Improved the manager client certificates and added support for installing multiple trust certificates and requesting/installing a second client certificate.
- Products with Hardware 9A0.1, 9A0.2 and 9A0.3 only support active track version 11.2.53 and later, LTS 2022 version 10.12.135 and later, as well as LTS 2020 version 9.80.28 and later.Products with hardware

ID 796, 7C3.1 and 7C3.2 support all AXIS OS versions. The hardware ID can be found in **Plain config > Properties > System > Hardware ID**. For more information, read the related *FAQ*.Applies to: AXIS P1375-E, AXIS P1377-LE and AXIS P1378-LE

Corrections

- Added detailed health information from SD cards to the server report, including power cycle statistics and flash wear rates. This improvement allows for a better monitoring of the system's health that can prevent downtime or data loss.
- Corrected low-light image quality issues.Applies to: AXIS Q1700-LE, AXIS Q1785-LE, AXIS Q1786-LE, ExCam XF Q1785, F101-A XF Q1785, XF40-Q1785 and XP40-Q1785
- Added fallback mode for network hardware that is limited to 10BASE-T and 100BASE-TX transmission. Applies to: All *AXIS ARTPEC-7, on page 85* products
- Corrected an issue where the "Turn on/off camera heater" option was appearing in the on-screen control dropdown, even though the product does not have a heater.Applies to: AXIS P1375-E, AXIS P1377-LE and AXIS P1378-LE

AXIS OS 9.80.22

Release date: 2023-03-07

Features

- Updated *Apache to version 2.4.55* to increase the overall cybersecurity level.
- Updated *cURL to version 7.88.1* to increase overall cybersecurity level.
- Updated OpenSSL to version 1.1.1t to increase overall cybersecurity level.
- Updated time zone database version to 2022g.
- Receiving ICMP secure redirects from other network hosts are now disabled to increase overall minimum cyber security level.

Corrections

- Corrected an issue affecting some O3C clients, that caused internal authentication requests to fail after a few days of uptime.
- Improved stability of syslog system by addressing a potential memory leak.
- Improved stability of the PTZ VAPIX parser.Applies to: AXIS M3115-LVE and AXIS M3116-LVE
- Corrected an issue that caused privacy masks to remain the same size during zooming after a restart. The privacy masks will now adjust their size in relation to the rest of the image during zooming, which is the expected behavior.Applies to: AXIS Q1700-LE
- Corrected an issue with simultaneous PTZ ONVIF requests.Applies to: AXIS P5654-E, AXIS P5655-E, AXIS Q1700-LE, AXIS Q1785-LE, AXIS Q1786-LE, AXIS Q6010-E, AXIS Q6074/-E, AXIS Q6075/-E/-S, AXIS Q6125-LE, AXIS Q6215-LE, AXIS Q8641-E, AXIS Q8642-E, D201-S XPT Q6075, ExCam XF Q1785, ExCam XPT Q6075, F101-A XF Q1785, XF40-Q1785 and XP40-Q1785

AXIS OS 9.80.12

Release date: 2022-12-15

Corrections

General improvements.

AXIS OS 9.80.10

Release date: 2022-11-29

Features

- New versioning on AXIS OS LTS 2020. For more information, see *AXIS OS versioning*.
- Updated cURL to version 7.86.0 to increase overall cybersecurity level.
- Updated OpenSSL to version 1.1.1s to increase the overall cybersecurity level.
- Updated time zone database version to 2022d. This version has some common time zones, such as Europe/Amsterdam, Europe/Copenhagen, Europe/Oslo, Europe/Stockholm, and more, removed from the recommended list of time zones.
- Products with Hardware ID 9A1 only support LTS 2020 version 9.80.10 and later. Products with hardware ID 756 support all AXIS OS versions. The hardware ID can be found in **Plain config > Properties > System > Hardware ID**. Applies to: AXIS Q6215-LE
- Products with hardware ID 97A.1 and 97A.2 only support AXIS OS 10.12.73 and later, as well as LTS 2020 version 9.80.10 and later. Products with hardware ID 7CF.1 and 7CF.2 support all AXIS OS versions. The hardware ID can be found in **Plain config > Properties > System > HardwareID**. Applies to: AXIS Q6010-E

Corrections

- Corrected an issue that caused a wrong file size to be reported for recordings larger than 50MB when using FTP.
- Corrected an issue that prevented the possibility to change manual IR Illumination angle from the web interface.Applies to: AXIS Q1785-LE, AXIS Q1786-LE and AXIS Q1798-LE
- Corrected an issue that on rare occasions caused the image to show horizontal lines or an over-saturated image.Applies to: AXIS M3064-V, AXIS M3065-V, AXIS M3066-V, AXIS M3075-V, AXIS M3205-LVE, AXIS M3206-LVE and AXIS Q9216-SLV

AXIS OS 9.80.3.14

Release date: 2022-09-12

Features

- Updated cURL to version 7.84.0 to increase overall cybersecurity level.
- Products with hardware ID 998 only support active track 10.12.104 and later, as well as LTS 9.80.3.14 and later. Products with hardware ID 7CA support all AXIS OS versions. The hardware ID can be found in **Plain config > Properties > System > HardwareID**.Applies to: AXIS P3925-R
- Products with hardware ID 999 only support active track 10.12.104 and later, as well as LTS 9.80.3.14 and later. Products with hardware ID 7CC support all AXIS OS versions. The hardware ID can be found in **Plain config > Properties > System > HardwareID**. Applies to: AXIS P3925-LRE
- Products with hardware ID 99A.1 and 99A.2 only support active track 10.12.104 and later, as well as LTS 9.80.3.14 and later. Products with hardware ID 91A only support active track 10.10.69 and later, as well as LTS 2020 version 9.80.3.8. Products with hardware ID 7CC support all AXIS OS versions. The hardware ID can be found in **Plain config > Properties > System > HardwareID**. Applies to: AXIS P3935-LR

Corrections

- Corrected an issue that caused audio via external VMS to stop working.
- Improved focus behavior after an upgrade. When upgrade is finished, perform also calibration **System > Maintenance > Optics > Calibrate** and autofocus **Image > Autofocus**.Applies to: AXIS P3245-LV/-LVE, AXIS P3247-LV/-LVE and AXIS P3248-LV/-LVE.

AXIS OS 9.80.3.13

Release date: 2022-07-22

Features

- Updated Apache web server to version 2.4.54 to increase overall cybersecurity level.
- Updated OpenSSL to version 1.1.1q to increase overall cybersecurity level.

- Updated cURL to version 7.83.1 to increase overall cybersecurity level.
- Products with hardware ID 991 and 992 only support active track 10.11.87 and later, as well as LTS track 9.80.3.13 and later. Products with hardware ID 7BD and 7C0 support all AXIS OS versions. The hardware ID can be found in **Plain config > Properties > System > HardwareID**.Applies to: AXIS M3067-P and AXIS M3068-P
- Products with hardware ID 993.1, 993.2, 994.1 and 994.2 only support active track 10.11.89 and later, as well as LTS track 9.80.3.13 and later. Products with hardware ID 985.1, 985.2, 986.1 and 986.2 only support active track 10.11.85 and later, as well as LTS track 9.80.3.13 and later. Products with hardware ID 956.1, 956.2, 956.3 and 956.4 only support active track 10.8.3 and later, as well as LTS track 9.80.3.9 and later. Products with hardware ID 91E.1, 91E.2, 91F.1 and 91F.2 only support active track 10.4.0 and later, as well as LTS track 9.80.3.1 and later. Products with hardware ID 7BE.1, 7BE.2, 7BF.1 and 7BF.2 support all AXIS OS versions. The hardware ID can be found in **Plain config > Properties > System > HardwareID**. Applies to: AXIS P3247-LV/-LVE and AXIS P3248-LV/-LVE
- Products with hardware ID 990 only support active track 10.12.65 and later, as well as LTS track 9.80.3.13 and later. Products with hardware ID 7AF support all AXIS OS versions. The hardware ID can be found in **Plain config > Properties > System > HardwareID**. Applies to: AXIS Q1798-LE
- Products with hardware ID 981 and 982 only support active track version 10.11.85 and later, as well as LTS track 9.80.3.13 and later. Products with hardware ID 7BB and 7BC support all AXIS OS versions. The hardware ID can be found in **Plain config > Properties > System > HardwareID**. Applies to: AXIS M3115-LVE and AXIS M3116-LVE
- Products with hardware ID 98E.1, 98E.2, 98E.3, 98D.1, 98D.2 and 98D.3 only support active track 10.12.65 and later, as well as LTS track 9.80.3.13 and later. Products with hardware ID 795, 796, 7C2.1, 7C2.2, 7C3.1 and 7C3.2 support all AXIS OS versions. The hardware ID can be found in **Plain config > Properties > System > HardwareID**. For more information, read the related *FAQ*.Applies to: AXIS P1375/-E, AXIS P1377/-LE, AXIS P1378/-LE, F101-A XF P1377 and ExCam XF P1377
- Products with hardware ID 983.1 an 983.2 only support AXIS OS 10.11.85 and later, as well as LTS track 9.80.3.13 and later. Products with hardware ID 90F.1 and 90F.2 support AXIS OS versions from 10.3.01 and LTS versions from 9.80.3.1. Products with hardware ID 79E.1 and 79E.2 support all AXIS OS versions. The hardware ID can be found in **Plain config > Properties > System > HardwareID**. Applies to: AXIS P3245-V/-VE
- Products with hardware ID 984.1 and 984.2 only support active track 10.11.85 and later, as well as LTS track 9.80.3.13 and later. Products with hardware ID 910.1 and 910.2 only support active track 10.3.0.1 and later, as well as LTS track 9.80.3.1 and later. Products with hardware ID 79F.1, 79F.2, 79F.3 and 79F.4 support all AXIS OS versions. The hardware ID can be found in **Plain config > Properties > System > HardwareID**. Applies to: AXIS P3245-LV/-LVE
- Products with hardware ID 987.1, 987.2, 988.1, 988.2, 989.1, 989.2, 98A.1, 98A.2, 98B.1 and 98B.2 only support active track 10.11.87 and later, as well as LTS track 9.80.3.13 and later. Products with hardware ID 917.1, 917.2, 918.1, 918.2, 914.1, 914.2, 915.1, 915.2, 916.1 and 916.2 support AXIS OS version 10.6.5 and later, and as well as LTS track 9.80.3.4 and later. Products with hardware ID 7D9.1, 7D9.2, 7DA.1, 7DA.2, 7B0, 7B1, 7FA.1 and 7FA.2 support all AXIS OS versions. The hardware ID can be found in **Plain config > Properties > System > HardwareID**. Applies to: AXIS Q6074/-E, AXIS Q6075/-E, D201-S XPT Q6075 and ExCam XPT Q6075

Corrections

- ONVIF recordings are now continued automatically after disruptions.

AXIS OS 9.80.3.12

Release date: 2022-06-09

Features and corrections

- Updated OpenSSL to version 1.1.1o to increase the overall cybersecurity level.
- General improvements to the LTS 2020 platform.
- Corrected an issue that would cause the AXIS OS upgrade to fail on rare occasions.

- Corrected *CVE-2018-25032*.

AXIS OS 9.80.3.11

Release date: 2022-05-09 (to be rolled out within 3 weeks of release date)

Features

- Updated OpenSSL to version 1.1.1n to increase overall minimum cybersecurity level.
- Updated Apache to version 2.4.53 to increase overall cybersecurity level.
- Updated wpa-supplicant to version 2.10 to increase overall cybersecurity level.

Corrections

- General improvements to the LTS 2020 platform.
- Receiving ICMP redirects from other network hosts is now disabled to increase overall minimum cybersecurity level.
- Updated the certificate management API's to handle camera models that do not support Real-Time Streaming Protocol over SSL (RTSPS).
- Corrected *CVE-2021-29462*.
- Corrected *CVE-2021-33910*.
- Improved memory management in the network services daemon.
- On some units focus might drift over time. Lens control has been improved to reduce this type of issues. Calibrate and autofocus the camera after upgrade.Applies to: AXIS P3245-V/-VE/-LV/-LVE

AXIS OS 9.80.3.10

Release date: 2022-03-16

Features

- Updated OpenSSL to version 1.1.1m to increase overall cybersecurity level.
- Updated Apache to version 2.4.52 to increase overall cybersecurity level.

Corrections

- Improved HDMI video output. Applies to: AXIS M3065-V, AXIS M3066-V and AXIS M3075-V
- Corrected an issue that caused the send images event to stop uploading towards an FTP server when the filename included a space (" ").
- Corrected *CVE-2020-13848*.
- Corrected an issue that prevented the Axis device to stream a 3rd unique video stream in rare conditions. Applies to: AXIS Q6125-LE
- Improved handling of empty recordings.
- Support for a new audio codec - ADAU1361 - has been added. Applies to: AXIS P3935-LR
- Corrected an issue that caused the IR-cut filter to get stuck halfway.Applies to: AXIS P3925-R/-LRE and AXIS P3935-LR

AXIS OS 9.80.3.9

Release date: 2022-02-01

Only for AXIS P3245-LV/-LVE, AXIS P3247-LV/-LVE and AXIS P3248-LV/-LVE.

Features

- Updated Apache to version 2.4.52 to increase overall cybersecurity level.

- Updated OpenSSL to version 1.1.1m to increase the overall cybersecurity level.
- Products with hardware ID 956.x only support 10.8.3 and later, as well as 9.80.3.9 on LTS 2020.Products with hardware ID 91E.x and 91F.x support 10.4.0 and later, as well as LTS 2020 9.80.3.1 and later. Products with hardware ID 7BE.x and 7BF.x support all AXIS OS versions. The hardware ID can be found in **Plain config > Properties > System > HardwareID**.

Corrections

- Corrected an issue that caused the send images event to stop uploading towards an FTP server when the filename included a space (" ").
- Corrected *CVE-2020-13848*.

AXIS OS 9.80.3.8

Release date: 2021-12-20

Features

- Updated Apache to version 2.4.51 to increase overall cybersecurity level.
- Updated OpenSSL to version 1.1.1l to increase overall cybersecurity level.
- Updated cURL to version 7.79.1 to increase overall cybersecurity level.
- Support for a new audio codec - ADAU1361 - has been added. Products with hardware ID 91A will now support the new codec. The hardware ID can be found via
  Plain config > Properties > System > HardwareID Applies to: AXIS P3935-LR

Corrections

- General improvements to the LTS 2020 platform.
- Corrected an issue that caused active recordings to be restarted when adding a new recording rule.
- Improved system stability of the Network Services.
- The remote syslog configuration is now preserved during a AXIS OS update within the same track.
- Corrected an issue that caused overlay text flickers when used in conjunction with an event triggered by the **recording ongoing** condition.
- Adjusted the default tilt to range between 0 to -180 degrees.Applies to: AXIS Q6074-E
- Improved response time of the I/O port monitoring cgi **/axis-cgi/io/input.cgi?monitor=1**.Applies to: AXIS D2050-VE, AXIS FA54, AXIS P1364/-E, AXIS P1365/-E Mk II, AXIS P1367/-E, AXIS P1368-E, AXIS P5655-E, AXIS Q1615/-LE Mk II, AXIS Q1645/-LE, AXIS Q1647/-LE, AXIS Q1659, AXIS Q1700-LE, AXIS Q1785-LE, AXIS Q1786-LE, AXIS Q1798-LE, AXIS Q1941-E, AXIS Q1942-E, AXIS Q3515-LV/-LVE, AXIS Q3517-LV/-LVE/-SLVE, AXIS Q3518-LVE, AXIS Q3527-LVE, AXIS Q6074, AXIS Q6075, AXIS Q6075-S/-SE, AXIS Q8641-E, AXIS Q8642-E, ExCam XF Q1645, ExCam XF Q1785, F101-A XF Q1785, XP40-Q1785 and XP40-Q1942
- Corrected *CVE-2021-3658*.Applies to: AXIS Companion Cube LW, AXIS Companion Dome WV, AXIS M1045-LW, AXIS M1065-LW, AXIS M3044-WV and AXIS M3045-WV
- Improved stability of the imaging processing to prevent crashes during darkness.Applies to: AXIS Companion Dome V
- Corrected an issue that could cause 'transmit.cgi' to close the connection prematurely when transmitting audio to the camera.Applies to: AXIS Companion Bullet LE, AXIS Companion Cube L/-LW, AXIS Companion Dome V/-WV, AXIS Companion Eye L, AXIS Companion Bullet mini LE, AXIS Companion Dome mini LE, AXIS Companion Eye mini L, AXIS Companion Recorder, AXIS D2050-VE, AXIS FA54, AXIS M1045-LW, AXIS M1065-L/-LW, AXIS M1124/-E, AXIS M1125/-E, AXIS M1134, AXIS M1135/-E, AXIS M1137/-E, AXIS M2025-LE, AXIS M2026-LE, AXIS M2026-LE Mk II, AXIS M3015, AXIS M3016, AXIS M3044-V/-WV, AXIS M3045-V/-WV, AXIS M3046-V, AXIS P9106-V, AXIS M3057-PLVE, AXIS M3058-PLVE, AXIS M3064-V, AXIS M3065-V, AXIS M3066-V, AXIS M3075-V, AXIS M3067-P, AXIS M3068-P, AXIS M3104-L/-LVE, AXIS M3105-L/-LVE, AXIS M3106-L/-LVE, AXIS M3106-L/-LVE Mk II, AXIS M3115-LVE, AXIS M3116-LVE, AXIS M3205-LVE, AXIS M3206-LVE, AXIS P1244, AXIS P1245, AXIS P1254, AXIS

P1264, AXIS P1265, AXIS P1275, AXIS P1280-E, AXIS P1290-E, AXIS P1364/-E, AXIS P1365/-E Mk II, AXIS P1367/-E, AXIS P1368-E, AXIS P1375/-E, AXIS P1377/-LE, AXIS P1378/-LE, AXIS P1435-E, AXIS P1435-LE, AXIS P1445-LE, AXIS P1445-LE-3, AXIS P1447-LE, AXIS P1448-LE, AXIS P3224-V/-VE/-LV/-LVE Mk II, P3225-V/-VE/-LV/-LVE Mk II, AXIS P3227-LV/-LVE, AXIS P3228-LV/-LE, AXIS P3235-LV/-LVE, AXIS P3245-V/-VE/-LV/-LVE, AXIS P3247-LV/-LVE, AXIS P3248-LV/-LVE, AXIS P3374-V/-LV, AXIS P3375-V/-VE/-LV/-LVE, AXIS P3717-PLE, AXIS P3807-PVE, AXIS P3925-R/-LRE, AXIS P3935-LR, AXIS P5654-E, AXIS P5655-E, AXIS Q1615/-LE Mk II, AXIS Q1645/-LE, AXIS Q1647/-LE, AXIS Q1659, AXIS Q1700-LE, AXIS Q1785-LE, AXIS Q1786-LE, AXIS Q1798-LE, AXIS Q1941-E, AXIS Q1941-E PT Mount, AXIS Q1942-E, AXIS Q1942-E PT Mount, AXIS Q3515-LV/-LVE, AXIS Q3517-LV/-LVE/-SLVE, AXIS Q3518-LVE, AXIS Q3527-LVE, AXIS Q3615-VE, AXIS Q3617-VE, AXIS Q6010-E, AXIS Q6074/-E, AXIS Q6075/-E/-S/-SE, AXIS Q6125-LE, AXIS Q6215-LE, AXIS Q8641-E, AXIS Q8642-E, AXIS Q9216-SLV, ExCam XF Q1645, ExCam XF Q1785, F101-A XF Q1785, XP40-Q1785 and XP40-Q1942

- Corrected an issue in the temperature controller that caused warnings in the logs after a factory reset. Applies to: AXIS P3245-V/-VE
- Updated the header for H.265 streams to not include delay information to avoid that some video clients may mistake it for B-frames.Applies to: AXIS M1134, AXIS M1135/-E, AXIS M1137/-E, AXIS M3067-P, AXIS M3068-P, AXIS M3115-LVE, AXIS M3116-LVE, AXIS P1375/-E, AXIS P1377/-LE, AXIS P1378/-LE, AXIS P3245-V/-VE/-LV/-LVE, AXIS P3247-LV/-LVE, AXIS P3247-LVE/-LVE, AXIS P3925-R/-LRE, AXIS P3935-LR, AXIS P5654-E, AXIS P5655-E, AXIS Q1798-LE, AXIS Q6074/-E and AXIS Q6075/-E/-S/-SE
- Corrected an issue where the camera sometimes did not recover from night mode. Please power off/on the camera after upgrade for this correction to take effect.Applies to: AXIS M3205-LVE and AXIS M3206-LVE

AXIS OS 9.80.3.5

Release date: 2021-09-07 (to be rolled out within three weeks of release date)

Features

- Updated Apache to version 2.4.48 to increase overall cybersecurity level.
- Updated cURL to version 7.78.0 to increase overall cybersecurity level.

Corrections

- The porttest-cgi is not used and is now removed from the platform.
- Corrected an issue that could cause an RTSP stream to stop after 60+ seconds if streamed to an openRTSP client.
- Corrected an issue that interrupted the NTP-time-sync between the Axis device and NTP-server when the NTP-server was unstable and suffered fluctuating time-changes.
- Made sure audio and video frames are grouped correctly in exportrecording.cgi.
- Corrected the following CVEs:
  - *CVE-2021-31988*
  - *CVE-2021-31987*
  - *CVE-2021-31986*
  - *CVE-2021-27219*
  - *CVE-2021-27218*
  - *CVE-2020-26558*
- Corrected an issue that prevented the mute signal to be properly transmitted to the audio controller. Applies to: AXIS Companion Cube L/-LW and AXIS M1065-L/-LW

AXIS OS 9.80.3.4

Release date: 2021-06-29

Only for AXIS Q6074/-E, AXIS Q6075/-E, D201-S XPT Q6075 and ExCam XPT Q6075.

Features and corrections

- General improvements to the LTS 2020 platform.
- Products with hardware ID 918, 917, 916, 915 and 914 only support 10.6.5 and later, or 9.80.3.4 and later on LTS 2020.Products with hardware ID 7D9, 7DA, 7B0, 7B1 and 7FA support all AXIS OS versions. The hardware ID can be found in **Plain config > Properties > System > HardwareID**.

AXIS OS 9.80.3.3

Release date: 2021-06-28 (to be rolled out within three weeks of release date)

Features

- Updated OpenSSH to version 8.6p1 to increase the overall minimum cyber security level.
- Added support for dynamic power allocation via Link Layer Discovery Protocol (LLDP) in addition to PoE-class based power allocation. This allows the switch to allocate less power to the camera and potentially a greater number of PoE devices can be connected to the switch. LLDP can be enabled in **Settings > System > PlainConfig > Network > LLDP POE > LLDP Send Max PoE**.Applies to: AXIS M3115-LVE and AXIS M3116-LVE

Corrections

- Corrected an issue that did not account for MTU packet fragmentation for IEEE 802.1x authentication. Previously the Axis device was not able to authenticate properly against an 802.1x network when the MTU was configured to 1410 or lower.
- Corrected an issue that prevented the device to stream in always-multicast mode after the video stream processing was restarted.
- Extended the 802.1x EAP-Identity field character limit from 32 to 128 characters.
- Increased the number of characters allowed in the name of an Action Event Condition, from 80 to 512.
- Corrected an issue that caused already established secure connections such as HTTPS or One-Click Cloud Connections to be interrupted.Applies to: AXIS Q6074/-E and AXIS Q6075/-E/-S
- Corrected an issue that caused distorted images in cropped corridor mode.Applies to: AXIS D2050-VE, AXIS FA54, AXIS M3057-PLVE, AXIS M3058, AXIS P1367/-E, AXIS P1368-E, AXIS P1445-LE, AXIS P1445-LE-3, AXIS P1447-LE, AXIS P1448-LE, AXIS P3227-LV/-LVE, AXIS P3228-LV/-LVE, AXIS P3717-PLE, AXIS P3807-PVE, AXIS Q1645/-LE, AXIS Q1647/-LE, AXIS Q1659, AXIS Q1700-LE, AXIS Q1785-LE, AXIS Q1786-LE, AXIS Q3515-LV/-LVE, AXIS Q3517-LV/-LVE/-SLVE, AXIS Q3518-LVE, AXIS Q3527-LVE, AXIS Q6215-LE, ExCam XF Q1785, F101-A Q1785 and XP40-Q1785

PSS 8.40

Go to *Products on PSS 8.40, on page 96* for a list of products on this track.

AXIS OS 8.40.104

Release date: 2026-06-30

Cybersecurity updates

- Updated Apache to version 2.4.67 to increase overall cybersecurity level.
- Updated OpenSSL to version 1.1.1zg to increase overall cybersecurity level.
- Updated OpenSSH to version 10.3 to increase overall cybersecurity level.
- Updated libssh2 to version 1.11.1 to address *CVE-2026-7598* and *CVE-2025-5987*
- Addressed *CVE-2026-41989* in libgcrypt

Corrections

- Updated the End User License Agreement.
- Corrected truncated response issue in param.cgi when XML content is requested, which previously caused AXIS Device Manager to fail retrieving device configurations.
- Corrected an issue where specially crafted inputs could cause high CPU utilization, improving overall system stability and security.

AXIS OS 8.40.93

Release date: 2025-12-02

Cybersecurity updates

- Updated cURL to version 8.17.0 to increase overall cybersecurity level.
- Updated OpenSSH to version 10.1 to increase overall cybersecurity level.
- OpenSSL Update to version 1.1.1zd to increase overall cybersecurity level.
- Updated Apache to version 2.4.65 to increase overall cybersecurity level.
- Addressed *CVE-2025-8998* and *CVE-2025-9524* .These CVEs will be externally disclosed on 11 November. For more information, please visit the *Axis vulnerability management portal*.

Corrections

- Corrected an issue with HTTP notifications failing due to permission errors.
- Corrected an issue where SMTP DATA messages did include additional not needed null characters.

AXIS OS 8.40.78

Release date: 2025-05-19

Features for all products

- Updated the End User License Agreement.

Product specific features

- Added support for AXIS TQ1818-E Positioning Unit.

  Applies to: AXIS Q8685-E and AXIS Q8685-LE

Cybersecurity updates

- Updated OpenSSH to version 9.9p2, addressing *CVE-2025-26466*.

- Updated OpenSSL to version 1.1.1zb to increase overall cybersecurity level.
- Updated cURL to version 8.12.1 to increase overall cybersecurity level.
- Addressed *CVE-2025-0325* . This CVE will be externally disclosed on 2 June 2025, more detailed information will follow then. For more information, please visit the Axis vulnerability management portal.

Corrections

- Corrected an issue where SMTP DATA messages were incorrectly terminated, causing compatibility issues with strict SMTP servers like Postfix.

AXIS OS 8.40.68

Release date: 2025–01–17

Cybersecurity updates

- Addressed *CVE-2024-47262*. These CVEs will be externally disclosed on 4 March 2025. More detailed information will follow then. For more information, please visit the *Axis vulnerability management portal*.
- Updated OpenSSL to version 1.1.1za to increase overall cybersecurity level.
- Updated cURL to version 8.11.1 to increase overall cybersecurity level.
- Updated wpa-supplicant to version 2.11 to increase overall cybersecurity level.

Corrections

- Improved "Start Recording" functionality to prevent simultaneous continuous recording.
- Improved stability and reliability of the certificate management service.

AXIS OS 8.40.59

Release date: 2024-09-10

Cybersecurity updates

- Updated Apache to version 2.4.62 to increase overall cybersecurity level.
- Updated OpenSSL to version 1.1.1y to increase overall cybersecurity level.
- Updated OpenSSH to version 9.8p1 to increase overall cybersecurity level.
- Updated cURL to version 8.9.0 to increase overall cybersecurity level.
- Updated libssh2 to version 1.11.0 to increase overall cybersecurity level.
- Updated Nettle cryptographic library to version 3.6 to increase overall cybersecurity level.
- Addressed vulnerability allowing unauthorized command execution via param.cgi.
- Addressed a vulnerability allowing DHCPv6 lease injection through unvalidated input parameters.
- Addressed vulnerabilities in GnuTLS: CVE-2024-28834 and CVE-2024-28835.
- Addressed CVE-2023-52160 in wpa-supplicant to increase overall cybersecurity level.
- Addressed CVE-2024-0067, CVE-2024-6173, CVE-2024-6509. For more information, please visit the *Axis vulnerability management portal*.

Corrections

- Resolved an issue where SSH users could retain access after a factory default with kept IP settings.
- Corrected a stream crash caused by invalid float values in CGI input.
- Implemented DNS cache for O3C client to reduce DNS lookups.

AXIS OS 8.40.48

Release date: 2024-05-29

Cybersecurity updates

- Addressed CVE-2024-0066. For more information, please visit the *Axis vulnerability management portal*.
- The parameter RemoteService.ProxyPassword that controls the proxy password has been masked and made unreadable for security reasons.

AXIS OS 8.40.43

Release date: 2024-03-04

Cybersecurity updates

- Addressed CVE-2024-0054. For more information, please visit the *Axis vulnerability management portal*.
- Addressed CVE-2023-5800. For more information, please visit the *Axis vulnerability management portal*.
- Updated OpenSSL to version 1.1.1x to increase overall cybersecurity level.
- Updated OpenSSH to version 9.6p1 to increase overall cybersecurity level.
- Updated *Apache to version 2.4.58* to increase overall cybersecurity level.

Important

This is the last release on the AXIS OS LTS 2018 track.

- The following products will not receive any further releases as their hardware warranty and software support period has expired:
- The following products will continue to receive releases until their hardware warranty and software support period expires:

All other products have the later LTS tracks. See the *Products on PSS 8.40, on page 96* for a complete list of products and their support status.

AXIS OS 8.40.37

Release date: 2023–11–01

Cybersecurity updates

- Updated *cURL to version 8.4.0* to increase overall cybersecurity level.

Corrections

- Corrected CVE-2023-21418. For more information, please visit the *Axis vulnerability management portal*.

AXIS OS 8.40.35

Release date: 2023–10–09

Cybersecurity updates

- Updated *cURL to version 8.3.0* to increase overall cybersecurity level.
- Updated OpenSSL to version 1.1.1w to increase the overall cybersecurity level.

Corrections

- Corrected CVE-2023-21415. For more information, please visit the *Axis vulnerability management portal*.

AXIS OS 8.40.31

Release date: 2023–09–05

Cybersecurity updates

- Updated *cURL to version 8.2.0* to increase overall cybersecurity level.
- Updated OpenSSL to version 1.1.1v to increase the overall cybersecurity level.

Corrections

- Netd Service preserves the static resolver configuration even after a soft restore, safeguarding static DNS/Search domain settings.

AXIS OS 8.40.26

Release date: 2023–06–26

Features

- Improved UPnP compliance by updating the SSDP (Simple Service Discovery Protocol) SERVER header in the standard "OS/version UPnP/1.0 product/version" format and USN (Unique Service Name) field with a UUID in the standard format. This enhances consistency and compatibility.

Cybersecurity updates

- Updated *Apache to version 2.4.57* to increase the overall cybersecurity level.
- Updated *cURL to version 8.1.0* to increase overall cybersecurity level.
- Updated OpenSSL to version 1.1.1u to increase the overall cybersecurity level.
- Updated libupnp to version 1.14.16, solving a memory leak and improving overall stability.

Corrections

- Corrected an issue with OAK (owner authentication key). It now only produces warnings in the log instead of errors if the device is not able to connect to the internet.

AXIS OS 8.40.19

Release date: 2023–04–26

Features

- Updated *Apache to version 2.4.56* to increase the overall cybersecurity level.
- Updated *cURL to version 8.0.1* to increase overall cybersecurity level.
- Improved the manager client certificates and added support for installing multiple trust certificates and requesting/installing a second client certificate.

AXIS OS 8.40.15

Release date: 2023-03-13

Features

- Updated *Apache to version 2.4.55* to increase the overall cybersecurity level.
- Updated *cURL to version 7.88.1* to increase overall cybersecurity level.
- Updated OpenSSL to version 1.1.1t to increase overall cybersecurity level.
- Receiving ICMP secure redirects from other network hosts are now disabled to increase overall minimum cyber security level.

Corrections

- Corrected an issue affecting some O3C clients, that caused internal authentication requests to fail after a few days of uptime.
- Improved stability of syslog system by addressing a potential memory leak.
- Corrected an issue with the audio transmit function where the response to /axis- cgi/audio/transmit.cgi is returning a '400 Bad Request' error.Applies to: All products with audio support
- Corrected an issue with simultaneous PTZ ONVIF requests.Applies to: AXIS P5514-E, AXIS P5515, AXIS M5525-E, AXIS P5624-E Mk II, AXIS P5635-E Mk II, AXIS Q1785-LE, AXIS Q1786-LE, AXIS Q6052/-E, AXIS Q6054/-E, AXIS Q6054/-E Mk II, AXIS Q6054/-E Mk III, AXIS Q6055/-E/-C/-S, AXIS Q6124-E, AXIS Q6125-LEAXIS Q8641-E, AXIS Q8642-E, D201-S XPT Q6055 and ExCam XPT Q6055

AXIS OS 8.40.8

Release date: 2022-12-12

Features

- New versioning on AXIS OS LTS 2018. For more information, see *AXIS OS versioning*.
- Updated OpenSSL to version 1.1.1s to increase the overall cybersecurity level.
- Updated cURL to version 7.86.0 to increase overall cybersecurity level.

Corrections

- Corrected an issue that caused a wrong file size to be reported for recordings larger than 50MB when using FTP.
- Corrected an issue that prevented streaming in always-multicast mode when the device was started without network connection.
- Corrected an issue in the bootloader that prevented upgrade to AXIS OS LTS 2020 - 9.80.Applies to: AXIS P1435-E/-LE, AXIS P3904-R Mk II and AXIS P3905-R Mk II
- Increase the number of audio files for pre-configured sounds from 10 to 50.Applies to: AXIS M5525-E

AXIS OS 8.40.4.7

Release date: 2022-10-18

Features and corrections

- Updated cURL to version 7.85.0 to increase overall cybersecurity level.
- Updated OpenSSL to version 1.1.1q to increase the overall cybersecurity.

Corrections

- General improvements to the LTS-2018 platform.
- Corrected an issue that caused audio via external VMS to stop working.
- Improved wide zoom (optical zoom 1x) Autofocus quality during night time conditions.Applies to: AXIS Q6155-E and AXIS Q6154-E

AXIS OS 8.40.4.6

Release date: 2022-07-21

Features

- Updated Apache web server to version 2.4.54 to increase overall cybersecurity level.
- Updated OpenSSL to version 1.1.1p to increase overall cybersecurity level.
- Updated cURL to version 7.83.1 to increase overall cybersecurity level.

Corrections

- Corrected an issue where the time tooltip was not displaying the correct date after passing midnight. Also, the date in the recordings list and the export was sometimes 1 day off.
- Corrected an issue where 802.1X would not trust the intermediate certificate authority (CA).
- Corrected an issue that caused time-out while reading boot block parameters.

AXIS OS 8.40.4.5

Release date: 2022-05-18 (to be rolled out within 3 weeks of release date)

Features

- Updated Apache to version 2.4.53 to increase overall cybersecurity level.
- Updated OpenSSL to version 1.1.1o to increase the overall cybersecurity level.
- Updated wpa-supplicant to version 2.10 to increase overall cybersecurity level.

Corrections

- General improvements to the LTS 2018 platform.
- Receiving ICMP redirects from other network hosts is now disabled to increase overall minimum cybersecurity level.
- Improved memory management in the network services daemon.
- Corrected an issue that caused the send images event to stop uploading towards a FTP server when the filename included a space (" ").
- Corrected *CVE-2018-25032*.

AXIS OS 8.40.4.4

Release date: 2022-01-24 (to be rolled out within 3 weeks of release date)

Features

- Updated Apache to version 2.4.52 to increase overall cybersecurity level.
- Updated OpenSSL to version 1.1.1m to increase overall cybersecurity level.
- Updated cURL to version 7.79.1 to increase overall cybersecurity level.

Corretions

- The remote syslog configuration is now preserved during a AXIS OS update within the same track.
- Improved handling of empty recordings.
- Corrected an issue that prevented AXIS OS upgrade from LTS 2016 (6.50).
- Corrected *CVE-2021-3658*.Applies to: AXIS Companion Cube LW, AXIS M1045-LW, AXIS M1065-LW, AXIS M3044-WV and AXIS M3045-W
- Improved stability of the imaging processing to prevent crashes in some darkness conditions.Applies to: AXIS Companion Dome V
- Corrected an issue that could cause 'transmit.cgi' to close connection prematurely when transmitting audio to the camera.Applies to: AXIS Companion Cube L/-LW, AXIS FA54, AXIS M1065-L/-LW, AXIS P1364/-E, AXIS P1365/-E Mk II, AXIS P1367/-E, AXIS P1368-E, AXIS P1445-LE, AXIS P1445-LE-3, AXIS P1447-LE, AXIS P1448-LE, AXIS P3235-LV/-LVE, AXIS P3374-V/-LV, AXIS P3375-V/-VE/-LV/-LVE, AXIS Q1615/-E Mk II, AXIS Q1645/-LE, AXIS Q1647/-LE, AXIS Q1659, AXIS Q1785-LE, AXIS Q1786-LE, AXIS Q1941-E, AXIS Q1942-E, AXIS Q3515-LV/-LVE, AXIS Q3517-LV/-LVE/-SLVE, AXIS Q3518-LVE, ExCam XF Q1645 and XP40-Q1942

AXIS OS 8.40.4.3

Release date: 2021-10-04 (to be rolled out within 3 weeks of release date)

Features

- Updated Apache to version 2.4.48 to increase overall cybersecurity level.
- Updated OpenSSL to version 1.1.1l to increase overall cyber security level.
- Updated cURL to version 7.78.0 to increase overall cybersecurity level.
- Updated OpenSSH to version 8.6p1 to increase the overall minimum cybersecurity level.

Corrections

- Corrected an issue that in combination with some VMSes and low resolution could cause brief disconnections in the video stream.
- Improved memory management in the network services daemon.
- Improved memory management in the DHCP lease update daemon.
- Corrected an issue that prevented the Axis device to respond with "HTTP 403 Forbidden" when the source-ip address was blocked when using PreventDOSAttack in **Plain Config > System**. Previously "HTTP 401 Unauthorized" was returned.
- Corrected nice names for the PreventDoSAttack parameters in **Settings > System > Plain Config > System > PreventDoSAttack**.
- Corrected an issue that did not account for MTU packet fragmentation for IEEE 802.1x authentication. Previously the Axis device was not able to authenticate properly against an 802.1x network when the MTU was configured to 1410 or lower.
- Corrected an issue that prevented streaming in always-multicast mode on rare occasions.
- Extended the 802.1x EAP-Identity field character limit from 32 to 128 characters.
- Corrected an issue that interrupted the NTP-time-sync between the Axis device and NTP-server when the NTP-server was unstable and suffered fluctuating time-changes.
- Corrected an issue that could cause an RTSP stream to stop after 60+ seconds if streamed to an openRTSP client.
- Corrected the following CVE:s
  - *CVE-2021-31988*
  - *CVE-2021-31987*
  - *CVE-2021-31986*
  - *CVE-2021-27219*
  - *CVE-2021-27218*
  - *CVE-2020-26558*Affected products: AXIS M1045-LW, AXIS M1065-LW, AXIS M3045-WV, AXIS M3044-WV, AXIS Companion Cube LW and AXIS Companion Dome WV
  - *CVE-2019-12450*
- Corrected an issue that caused images to be unusually dark when using WDR mode.Applies to: AXIS Companion Bullet LE, AXIS Companion Eye L/-LVE, AXIS M1124/-E, AXIS M1125/-E, AXIS M2025-LE, AXIS M3104-L/-LVE, AXIS M3105-L/-LVE, AXIS P1244, AXIS P1245, AXIS P1254, AXIS P1264, AXIS P1265, AXIS P1275, AXIS P1280-E, AXIS P1290-E, AXIS P1364/-E, AXIS P1365/-E Mk II, AXIS P1435-E/-LE, AXIS P3224-V/-VE/-LV/-LVE Mk II, AXIS P3225-V/-VE/-LV/-LVE Mk II, AXIS P3235-LV/-LVE, AXIS P3374-V/-LV, AXIS P3375-V/-VE/-LV/-LVE, AXIS Q1615/-E Mk II, AXIS Q1941-E, AXIS Q1941-E PT Mount, AXIS Q1942-E, AXIS Q1942-E PT Mount, AXIS Q3615-VE, AXIS Q3617-VE, AXIS Q6154-E, AXIS Q8641-E, AXIS Q8642-E and XP40-Q1942
- Corrected an issue that caused installation of ACAP using packagemanager.cgi to fail.Applies to: AXIS M3045-V
- Improved system stability when streaming multiple video streams at the same time.Applies to: AXIS FA54

- Improved stability in recording management.Applies to: AXIS Companion Cube L/-LW, AXIS Companion Dome V/-WV, AXIS M1045-LW, AXIS M1065-L/-LW, AXIS M2026-LE, AXIS M3044-V/-WV, AXIS M3045-V/-WV, AXIS M3046-V, AXIS P9106-V, AXIS M3106-L/-LVE

AXIS OS 8.40.4.2

Release date: 2021-04-19 (to be rolled out within 3 weeks of release date)

Features

- Updated OpenSSL to version 1.1.1k to fix *CVE-2021-3449* and *CVE-2021-3450*.
- Updated cURL to version 7.73.0 to increase overall cybersecurity level.

Corrections

- Improved Link Layer Discovery Protocol (LLDP) system stability.
- Corrected an issue that caused IEEE 802.1x network authentication to fail sometimes after unexpected reboots.
- Corrected an issue in oak.cgi that could cause invalid requests.
- Corrected an issue that caused the value of Quality of Service (QoS) to not be respected in always multicast mode.
- Corrected an issue that caused PKCS#12-formatted certificate uploads to fail when certain special characters were used as a password.
- Corrected an issue that caused video clients to not display a low-FPS video stream due to missing base FPS info in VUI timing info.Applies to: AXIS FA54, AXIS M3057-PLVE, AXIS M3058-PLVE, AXIS P1367/-E, AXIS P1368-E, AXIS P1445-LE, AXIS P1445-LE-3, AXIS P1447-LE, AXIS P1448-LE, AXIS P3227-LV/-LVE, AXIS P3228-LV/-LVE, AXIS Q1645/-LE, AXIS Q1647/-LE, AXIS Q1659, AXIS Q1785-LE, AXIS Q1786-LE, AXIS Q3515-LV/-LVE, AXIS Q3517-LV/-LVE/-SLVE and AXIS Q3518-LVE
- Corrected an issue that could cause live image to blink in dark conditions on rare occasions.Applies to: AXIS FA54, AXIS M3057-PLVE, AXIS M3058-PLVE, AXIS P1367/-E, AXIS P1368-E, AXIS P1445-LE, AXIS P1445-LE-3, AXIS P1447-LE, AXIS P1448-LE, AXIS P3227-LV/-LVE, AXIS P3228-LV/-LVE, AXIS Q1645/-LE, AXIS Q1647/-LE, AXIS Q1659, AXIS Q1785-LE, AXIS Q1786-LE, AXIS Q3515-LV/-LVE, AXIS Q3517-LV/-LVE/-SLVE and AXIS Q3518-LVE
- Corrected an issue with pause-frame handling that could cause network disconnections if pause-frames were enabled and used in the network.Applies to: AXIS FA54, AXIS M3057-PLVE, AXIS M3058-PLVE, AXIS P1367/-E, AXIS P1368-E, AXIS P1445-LE, AXIS P1445-LE-3, AXIS P1447-LE, AXIS P1448-LE, AXIS P3227-LV/-LVE, AXIS P3228-LV/-LVE, AXIS Q1645/-LE, AXIS Q1647/-LE, AXIS Q1659, AXIS Q1785-LE, AXIS Q1786-LE, AXIS Q3515-LV/-LVE, AXIS Q3517-LV/-LVE/-SLVE and AXIS Q3518-LVE
- Corrected an issue that prevented the device to utilize the available network bandwidth in high-latency networks such as 4G cellular network.Applies to: AXIS FA54, AXIS M3057-PLVE, AXIS M3058-PLVE, AXIS P1367/-E, AXIS P1368-E, AXIS P1445-LE, AXIS P1445-LE-3, AXIS P1447-LE, AXIS P1448-LE, AXIS P3227-LV/-LVE, AXIS P3228-LV/-LVE, AXIS Q1645/-LE, AXIS Q1647/-LE, AXIS Q1659, AXIS Q1785-LE, AXIS Q1786-LE, AXIS Q3515-LV/-LVE, AXIS Q3517-LV/-LVE/-SLVE and AXIS Q3518-LVE

AXIS OS 8.40.4.1

Release date: 2020-11-16 (to be rolled out within 3 weeks of release date)

Features

- Updated Apache to version 2.4.46 to increase overall cybersecurity level.
- Added support for HTTP Strict Transport Security (HSTS) when using HTTPS.
- Reduced time to build-up an RTSP video stream by 30% and more.

Corrections

- Corrected an issue that caused an error message to pop up when pressing the test button of an event using HTTP recipients.
- Corrected an issue that caused distorted H.265 streams on rare occasions.Applies to: AXIS M2026-LE Mk II, AXIS M3015, AXIS M3016, and AXIS M3106-L/-LVE Mk II
- Corrected an issue that could cause image to shake when Electronic Image Stabilization (EIS) was activated during high zoom (x32) operations.Applies to: AXIS Q1785-LE and AXIS Q1786-LE

PSS 6.50

Go to *Products on PSS 6.50, on page 96* for a list of products that will continue to receive updates.
The list will be modified over time as the expiry date of the products varies, and it is only valid for the latest release.
Although supported products are planned to receive updates twice a year, they will receive security patches whenever it is deemed necessary.

AXIS OS 6.50.5.22

Release date: 2026-06-24

Cybersecurity updates

- Updated Apache to version 2.4.67 to increase overall cybersecurity level.
- Updated cURL to version 8.17.0 to increase overall cybersecurity level.
- Updated OpenSSL to version 1.1.1zg to increase overall cybersecurity level.
- Updated OpenSSH to version 10.3 to increase overall cybersecurity level.
- Updated libssh2 to version 1.11.1 to address *CVE-2026-7598* and *CVE-2025-5987*.

Corrections

- Improve overall stability and security of the policykit-cert service.
- Corrected truncated response issue in param.cgi when XML content is requested, which previously caused Axis Device Manager to fail retrieving device configurations.

AXIS OS 6.50.5.21

Release date: 2025-10-20

Cybersecurity

- Updated Apache to version 2.4.65 to increase overall cybersecurity level.
- Updated cURL to version 8.16.0 to increase overall cybersecurity level.
- Updated OpenSSH to version 10.0p1 to increase overall cybersecurity level.
- Updated OpenSSL to version 1.1.1zc to increase overall cybersecurity level.
- Updated OpenSSH to version 9.9p2, addressing *CVE-2025-26466*.
- Addressed *CVE-2025-0325*, *CVE-2023-5677* and *CVE-2025-32728*. For more information, please visit the *Axis vulnerability management portal*.
- Addressed *CVE-2025-9524*. This CVE will be externally disclosed on 11 November 2025, more detailed information will follow then. For more information, please visit the *Axis vulnerability management portal*.

Corrections

- Corrected an issue where SMTP DATA messages were incorrectly terminated, causing compatibility issues with strict SMTP servers like Postfix.
- Corrected an issue where SMTP DATA messages did include additional not needed null characters.

AXIS OS 6.50.5.20

Release date: 2025-03-05

Cybersecurity

- Addressed *CVE-2024-47262*. This CVE will be externally disclosed on 4 March 2025, more detailed information will follow then. For more information, please visit the *Axis vulnerability management portal*.
- Updated wpa-supplicant to version 2.11 to increase overall cybersecurity level.
- Updated cURL to version 8.11.1 to increase overall cybersecurity level.

Corrections

- Improved "Start Recording" functionality to prevent simultaneous continuous recording.

AXIS OS 6.50.5.19

Release date: 2024-11-13

Cybersecurity updates

- Updated cURL to version 8.10.1 to increase overall cybersecurity level.
- Updated OpenSSL to version 1.1.1za, addressing *CVE-2024-5535*.
- Updated OpenSSH to version 9.8p1, addressing *CVE-2024-6387*.
- Updated Apache to version 2.4.62, addressing *CVE-2024-40725* and *CVE-2024-40898*.
- Updated libssh2 to version 1.11.0, addressing *CVE-2023-48795*.
- Addressed *CVE-2023-52160* in wpa-supplicant to increase overall cybersecurity level.
- Addressed *CVE-2024-47257*. This CVE will be externally disclosed on 26 November 2024 as part of our ongoing commitment to cybersecurity. Detailed information will follow then. For more information, please visit the *Axis vulnerability management portal*.
- Improved certificate management service stability and reliability.

Corrections

- Corrected issue with SSH user access after factory default with kept IP settings.
- Added DNS cache for O3C client to reduce DNS lookup times.

AXIS OS 6.50.5.18

Release date: 2024-05-28

Cybersecurity updates

- Addressed CVE-2024-0066. For more information, please visit the *Axis vulnerability management portal*.
- Updated *cURL to version 8.7.1* to increase overall cybersecurity level.
- Updated OpenSSH to version 9.6p1 to increase overall cybersecurity level.

AXIS OS 6.50.5.17

Release date: 2024-03-19

Cybersecurity updates

- Updated *cURL to version 8.6.0* to increase overall cybersecurity level.
- Updated OpenSSL to version 1.1.1x to increase overall cybersecurity level.

AXIS OS 6.50.5.16

Release date: 2024-01-29

Cybersecurity updates

- Updated Apache to version 2.4.58 to increase the overall cybersecurity level.

Corrections

- Netd Service now preserves the static resolver configuration even after a soft reset, protecting static DNS/Search domain settings.

AXIS OS 6.50.5.15

Release date: 2023-11-08

Cybersecurity updates

- Updated *cURL to version 8.4.0* to increase overall cybersecurity level.
- Addressed CVE-2023-21418. For more information, please visit the *Axis vulnerability management portal*.

AXIS OS 6.50.5.14

Release date: 2023-10-19

Cybersecurity updates

- Updated *cURL to version 8.3.0* to increase overall cybersecurity level.
- Updated OpenSSL to version 1.1.1w to increase the overall cybersecurity level.

Corrections

- Corrected CVE-2023-21415. For more information, please visit the *Axis vulnerability management portal*.

AXIS OS 6.50.5.13

Release date: 2023-08-28

Cybersecurity updates

- Updated *cURL to version 8.2.0* to increase overall cybersecurity level.
- Updated OpenSSL to version 1.1.1v to increase the overall cybersecurity level.

Corrections

- Resolved an issue where the respawn daemon incorrectly managed restarts for ACAP services, notably in situations with multiple acaps running simultaneously.

AXIS OS 6.50.5.12

Release date: 2023-08-02

Features

- General improvements to the platform.

Cybersecurity updates

- Added proxy configuration support to the Owner Authentication Key (OAK) cgi using group root. RemoteService, simplifying setup on networks requiring proxy servers for Internet access and improving the authentication process.
- Updated *Apache to version 2.4.57* to increase the overall cybersecurity level.
- Updated OpenSSL to version 1.1.1u to increase the overall cybersecurity level.

AXIS OS 6.50.5.11

Release date: 2023-05-29

Features

- Updated *Apache to version 2.4.56* to increase the overall cybersecurity level.
- Updated *cURL to version 8.0.1* to increase overall cybersecurity level.
- Added support for a second client certificate.

AXIS OS 6.50.5.10

Release date: 2023-04-04

Features

- Updated *Apache to version 2.4.55* to increase the overall cybersecurity level.
- Updated OpenSSL to version 1.1.1t to increase overall cybersecurity level.
- Updated *cURL to version 7.88.1* to increase overall cybersecurity level.

Corrections

- Corrected an issue affecting some O3C clients, that caused internal authentication requests to fail after a few days of uptime.

AXIS OS 6.50.5.8

Release date: 2023-02-09

Corrections

- Disabled secure redirects from other network hosts net.ipv4.conf.all.secure_redirects & net.ipv4.conf.default.secure_redirects, to increase overall minimum cybersecurity level.
- Corrected a restart issue caused by tilting the PTZ camera to 90 degrees. The issue was introduced in version 6.50.5.5 and 6.50.5.6.Applies to: AXIS Q6128-E
- Corrected an issue with the audio transmit function where the response to /axis- cgi/audio/transmit.cgi is returning a '400 Bad Request' error.Applies to: All products with audio support

Important

This is the last release on the AXIS OS LTS 2016 track.

The following product will continue to receive releases until the hardware warranty and software maintenance period has expired:
AXIS F34, AXIS F41, AXIS F44 Dual audio input, AXIS M1145/-L, AXIS M3026-VE, AXIS M3027-PVE, AXIS M7011, AXIS P1427-E/-LE, AXIS P3353, AXIS P3354, AXIS P3363-V/-VE, AXIS P3364-V/-VE/-LV/-LVE, AXIS P3365-V/-VE, AXIS P3367-V/-VE, AXIS P3384-V/-VE, AXIS P3707-PE, AXIS P3904-R, AXIS P3905-R/-RE, AXIS P3915-R, AXIS P5414-E, AXIS P5415-E, AXIS P7224, AXIS P8535, AXIS P8804, AXIS P8804-2, AXIS Q1615/-E, AXIS Q1635/-E, AXIS Q1765-LE PT Mount, AXIS Q1765-LE, AXIS Q2901-E PT Mount, A XIS Q2901-E, AXIS Q6000-E/ MK II, AXIS Q6114-E, AXIS Q6115-E, AXIS Q6128-E, AXIS Q7411, AXIS Q7436, AXIS Q8414-LV, AXIS Q8665-E/-LE, XF40-Q1765, XF40-Q2901, XF60-Q1765, XF60-Q2901 and XP40-Q1765

The following products have later LTS tracks. Please upgrade to the latest version to increase cybersecurity:
AXIS M1124/-E, AXIS M1125/-E, AXIS P1364/-E, AXIS P1365/-E Mk II, AXIS P1435-E/-LE, AXIS P3904-R Mk II, AXIS P3905-R Mk II, AXIS P3915-R Mk II, AXIS P5514/-E, AXIS P5515/-E, AXIS P5624-E Mk II, AXIS P5635-E Mk II, AXIS Q1775/-E, AXIS Q6052/-E, AXIS Q6054/-E, AXIS Q6055/-E, AXIS Q6155-E, D201-S XPT Q6055 and ExCam XPT Q6055

The following products will not receive any more releases since the hardware warranty and software maintenance period has expired:
AXIS F44 Main unit, AXIS M3006-V, AXIS M3007-P/-PV, AXIS P1354/-E, AXIS P1353/-E, AXIS P1357/-E, AXIS P1365/-E, AXIS P1405-E/-LE, AXIS P1425-E/-LE, AXIS P3214-V/-VE, AXIS P3215-V/-VE,

AXIS P3224-LV/-LVE, AXIS P3225-LV/-LVE, AXIS P5624-E, AXIS P5635-E, AXIS Q1604/-E, AXIS Q1614/-E, AXIS Q1931-E, AXIS Q1931-E PT Mount, AXIS Q1932-E, AXIS Q1932-E PT Mount, AXIS Q3505-V/-VE, AXIS Q6042/-E/-C/-S, AXIS Q6044/-E/-C/-S, AXIS Q6045/-E/-C/-S Mk II, AXIS Q8631-E and AXIS Q8632-E

AXIS OS 6.50.5.7

Release date: 2022-12-19

Features and corrections

- Updated Apache to version 2.4.54 to increase overall cybersecurity level.
- Updated OpenSSL to version 1.1.1s to increase the overall cybersecurity level.
- Updated cURL to version 7.86.0 to increase overall cybersecurity level.
- Corrected an issue that caused audio via external VMS to stop working.
- Corrected an issue that caused the wrong file size to be reported for recordings larger than 50MB when using FTP.
- Corrected an issue where 802.1X would not trust the intermediate certificate authority (CA).

AXIS OS 6.50.5.6

Release date: 2022-05-11 (to be rolled out within three weeks of release date)

Features

- Updated OpenSSL to version 1.1.1o to increase overall cybersecurity level.
- Updated Apache to version 2.4.53 to increase overall cybersecurity level.
- Updated cURL to version 7.79.1 to increase overall cybersecurity level.
- Updated wpa-supplicant to version 2.10 to increase overall cybersecurity level.

Corrections

- General improvements to the LTS 2016 platform.
- Receiving ICMP redirects from other network hosts is now disabled to increase overall minimum cybersecurity level.
- Improved handling of empty recordings.
- Corrected an issue with uploading RSA certificate with PKCS#8 formatted private keys.
- Corrected an issue that caused the send images event to stop uploading towards an FTP server when the filename included a space (" ").
- Corrected an issue with file permission when using disk encryption
- Corrected an issue that caused ONVIF AbsoluteMove commands to return a 500 Internal Server Error.
- Corrected *CVE-2021-29462*.
- Corrected *CVE-2020-13848*.
- Corrected *CVE-2019-15916*.

AXIS OS 6.50.5.5

Release date: 2021-10-25 (to be rolled out within three weeks of release date)

Features

- Updated Apache to version 2.4.48 to increase overall cybersecurity level.
- Updated OpenSSH to version 8.6p1 to increase the overall minimum cybersecurity level.
- Updated cURL to version 7.78.0 to increase overall cybersecurity level.

- Updated OpenSSL to version 1.1.1l to increase overall minimum cybersecurity level.

Corrections

- Corrected the following CVEs:
  - *CVE-2021-31988*
  - *CVE-2021-31987*
  - *CVE-2021-31986*
  - *CVE-2021-27219*
  - *CVE-2021-27218*
  - *CVE-2019-12450*
- Corrected an issue that caused video clients such as VLC to not display a low-FPS video stream due to missing base FPS info in VUI timing info.

AXIS OS 6.50.5.4

Release date: 2021-05-17 (to be rolled out within three weeks of release date)

Features

- Updated OpenSSL to version 1.1.1k to fix *CVE-2021-3449* and *CVE-2021-3450*.

Corrections

- Corrected an issue that caused the value of Quality of Service (QoS) to not be respected in always multicast mode.

AXIS OS 6.50.5.3

Release date: 2020-11-09 (to be rolled out within three weeks of release date)

Features

- Updated Apache to version 2.4.46 to increase overall cyber security level.

Corrections

- Corrected an issue that caused a test button in the web interface to not work when mounting network-attached atorage (NAS) configured with SMB v3.
- Added a sensitivity parameter for tampering detection in PlainConfig that can now be adjusted by the user.Applies to: AXIS P1244, AXIS P1245, AXIS P1254, AXIS P1264, AXIS P1265, AXIS P1275, AXIS P1364/-E, AXIS P1365/-E Mk II and AXIS P1435-E/-LE
- Corrected an issue that caused a failure to send images with action rules to email recipients.Applies to: AXIS P1244, AXIS P1245, AXIS P1254, AXIS P1264, AXIS P1265, AXIS P1275, AXIS P1364/-E, AXIS P1365/-E Mk II and AXIS P1435-E/-LE

Product groups

System-on-chip (SoC)

Features or corrections are sometimes applied to a group of products based on the system-on-chip (SoC). These groups are listed below and are sometimes referenced in the release notes.

For more information, visit *System-on-chip*.

AXIS ARTPEC-9

• AXIS D2122-VE	• AXIS P1487-LE	• AXIS Q1726/-LE
• AXIS D2123-VE	• AXIS P1488-LE	• AXIS Q1728/-LE
• AXIS M4337-PLVE/-SPLVE	• AXIS P3275-LV/-LVE/-V	• AXIS Q3546-LVE
• AXIS M4338-PLVE	• AXIS P3277-LV/-LVE	• AXIS Q3548-LVE
• AXIS M4347-PLVE	• AXIS P3277-LVE Mic	• AXIS Q3556-LVE
• AXIS M4348-PLVE	• AXIS P3278-LV/-LVE	• AXIS Q3558-LVE
• AXIS P1475-LE	• AXIS P3285-LV/-LVE	• AXIS Q6086-E
• AXIS P1485-LE	• AXIS P3285-LVE Kit	• AXIS Q6088-E
• AXIS P1485-LE Kit	• AXIS P3287-LV/-LVE	• AXIS Q6325-LE
• AXIS P1486-LE	• AXIS P3288-LV/-LVE	• AXIS Q6355-LE
• AXIS P1486-LE Kit	• AXIS P3407-VE	• AXIS Q6358-LE
	• AXIS P3408-VE	• AXIS Q6411-LE

AXIS ARTPEC-8

- AXIS D2210-VE
- AXIS F9104-B Mk II Main Unit
- AXIS F9111-R Mk II Main Unit
- AXIS F9114-B/-R Mk II Main Unit
- AXIS I8307-VE
- AXIS M3215
- AXIS M3216
- AXIS M4225-LVE
- AXIS M4227-LVE
- AXIS M4228-LVE
- AXIS M4317-PLR/-PLVE
- AXIS M4318-PLR/-PLVE
- AXIS M4327-P
- AXIS M4328-P
- AXIS M5526-E
- AXIS P1385/-B/-BE/-E
- AXIS P1387/-B/-BE/-LE
- AXIS P1388/-B-BE/-LE
- AXIS P1465-LE
- AXIS P1465-LE-3
- AXIS P1467-LE
- AXIS P1468-LE
- AXIS P1468-XLE
- AXIS P1518-E/-LE
- AXIS P3265-V/-LV/-LVE
- AXIS P3265-LVE-3
- AXIS P3267-LV/-LVE/-LVE Mic
- AXIS P3268-LV/-LVE/-SLVE
- AXIS P3735-PLE
- AXIS P3737-PLE
- AXIS P3738-PLE
- AXIS P3747-PLVE
- AXIS P3748-PLVE
- AXIS P3827-PVE
- AXIS P4705-PLVE
- AXIS P4707-PLVE
- AXIS P4708-PLVE
- AXIS P9117-PV
- AXIS Q1656/-B/-BE/-BLE/-DLE/-LE
- AXIS Q1686-DLE
- AXIS Q1800-LE
- AXIS Q1800-LE-3
- AXIS Q1805-LE
- AXIS Q1806-LE
- AXIS Q1808-LE
- AXIS Q1809-LE
- AXIS Q1961-TE/-XTE
- AXIS Q1971-E
- AXIS Q1972-E
- AXIS Q2101-TE
- AXIS Q2111-E
- AXIS Q2112-E
- AXIS Q2802-E
- AXIS Q3536-LVE
- AXIS Q3538-LVE
- AXIS Q3626-VE
- AXIS Q3628-VE
- AXIS Q3839-PVE/-SPVE
- AXIS Q4809-PVE
- AXIS Q6020-E
- AXIS Q6300-E
- AXIS Q9227-SLV
- AXIS Q9307-LV
- AXIS XFQ1656

AXIS ARTPEC-7

- AXIS D2110-VE
- AXIS F9104-B Main Unit
- AXIS F9111 Main Unit
- AXIS F9114 Main Unit
- AXIS F9114-B Main Unit
- AXIS I8016-LVE
- AXIS M1134
- AXIS M1135/-E
- AXIS M1137/-E
- AXIS M3057-PLVE Mk II
- AXIS M3067-P
- AXIS M3068-P
- AXIS M3077-PLVE
- AXIS M3115-LVE
- AXIS M3116-LVE
- AXIS M4308-PLE
- AXIS M5000/-G
- AXIS M5074
- AXIS M5075/-G
- AXIS M7104
- AXIS P1375/-E
- AXIS P1377/-LE
- AXIS P1378/-LE
- AXIS P1455-LE
- AXIS P1455-LE-3
- AXIS P3245-V/-VE/-LV/-LVE
- AXIS P3245-LVE-3
- AXIS P3247-LV/-LVE
- AXIS P3248-LV/-LVE
- AXIS P3255-LVE
- AXIS P3727-PLE
- AXIS P3818-PVE
- AXIS P3925-R/-LRE
- AXIS P3935-LR
- AXIS P5654-E
- AXIS P5654-E Mk II
- AXIS P5655-E
- AXIS P5676-LE
- AXIS P7304
- AXIS P7316
- AXIS Q1715
- AXIS Q1798-LE
- AXIS Q1951-E
- AXIS Q1952-E
- AXIS Q3819-PVE
- AXIS Q6074/-E
- AXIS Q6075/-E/-S/-SE
- AXIS Q6078-E
- AXIS Q6078-E Mk II
- AXIS Q6135-LE
- AXIS Q6225-LE
- AXIS Q6315-LE
- AXIS Q6318-LE
- AXIS Q8615-E
- AXIS Q8752-E
- AXIS V5925
- AXIS V5938
- D201-S XPT Q6075
- ExCam XPT Q6075
- ExCam XF P1377
- F101-AXF P1377

AXIS ARTPEC-6

- AXIS A8207-VE
- AXIS A8207-VE Mk II
- AXIS D2050-VE
- AXIS FA54
- AXIS M3057-PLVE
- AXIS M3058-PLVE
- AXIS P1367/-E
- AXIS P1368-E
- AXIS P1445-LE
- AXIS P1445-LE-3
- AXIS P1447-LE
- AXIS P1448-LE
- AXIS P3227-LV/-LVE
- AXIS P3228-LV/-LVE
- AXIS P3715-PLVE
- AXIS P3717-PLE
- AXIS P3807-PVE
- AXIS P8815-2
- AXIS Q1645/-LE
- AXIS Q1647/-LE
- AXIS Q1659
- AXIS Q1700-LE
- AXIS Q1785-LE
- AXIS Q1786-LE
- AXIS Q3515-LV/-LVE
- AXIS Q3517-LV/-LVE/-SLVE
- AXIS Q3518-LVE
- AXIS Q3527-LVE
- AXIS Q6215-LE
- AXIS XPQ1785
- D101-A XF P3807
- ExCam XF P1367
- ExCam XF P3807
- ExCam XF Q1645
- ExCam XF Q1785
- F101-A XF P1367
- F101-A XF Q1785
- XF40-Q1785
- XP40-Q1785

AXIS ARTPEC-5

• AXIS A9161 • AXIS A9188/-VE • AXIS C1004-E • AXIS C2005 • AXIS C8033 • AXIS F34 Main Unit • AXIS F41 Main Unit • AXIS F44 Dual Audio Input • AXIS M2025-LE • AXIS M5525-E • AXIS M7011 • AXIS P1244 • AXIS P1245	• AXIS P1254 • AXIS 1264 • AXIS 1265 • AXIS 1275 • AXIS P1280-E • AXIS P1290-E • AXIS P3374-LV/-V • AXIS P3375-LV/-LVE/-V/-VE • AXIS P3904-R Mk II • AXIS P3905-R Mk II • AXIS Q1941-E • AXIS Q1941-E PT Mount • AXIS Q1942-E	• AXIS Q1942-E PT Mount • AXIS Q3615-VE • AXIS Q3617-VE • AXIS Q6055-C • AXIS Q6154-E • AXIS Q6155-E • AXIS Q7436 Blade • AXIS Q8641-E • AXIS Q8642-E • AXIS Q8685-E • AXIS Q8685-LE • D201-S XPT Q6055 • XP40-Q1942

Ambarella CV25

• AXIS I7010-VE • AXIS I7010-VE Safety • AXIS I7020 • AXIS I8116-E • AXIS M1055-L • AXIS M1075-L • AXIS M1075-L Mk II	• AXIS M2035-LE • AXIS M2036-LE • AXIS M3085-V • AXIS M3086-V • AXIS M3086-V Mic • AXIS M3088-V • AXIS M3125-LVE • AXIS M3126-LVE	• AXIS M3128-LVE • AXIS M4215-LV/-V • AXIS M4216-LV/-V • AXIS M4218-LV/-V • AXIS P1245 Mk II • AXIS P1265 Mk II • AXIS P1275 Mk II

Ambarella CV75

• AXIS M2048-LE • AXIS M3098-H/-LV/-V • AXIS M3138-LVE	• AXIS M3945-R • AXIS P3945-R • AXIS P3947-R

Ambarella S5

• AXIS P3719-PLE	• AXIS Q6010-E	• AXIS Q6100-E

Ambarella S5L

• AXIS M3064-V • AXIS M3065-V • AXIS M3066-V	• AXIS M3075-V • AXIS M3205-LVE • AXIS M3206-LVE	• AXIS Q9216-SLV • AXIS W100 • AXIS W101

Ambarella S6LM

• AXIS D6310 • AXIS M3905-R • AXIS P3905-R Mk III	• AXIS W102 • AXIS W110 • AXIS W111	• AXIS W120 • AXIS W401

I.MX 6SX

• AXIS A1210/-B • AXIS A1214 • AXIS A1601 • AXIS A1610/-B • AXIS A1710-B • AXIS A1711	• AXIS A1810-B • AXIS A1811 • AXIS A9210 • AXIS C1210-E • AXIS C1211-E	• AXIS C1510 • AXIS C1511 • AXIS C1610-VE • AXIS C8110 • AXIS C8210

I.MX 6ULL

• AXIS C1310-E • AXIS C1410	• AXIS D3110 • AXIS D4100-E	• AXIS W400

I.MX 8M-NANO

• AXIS C1110-E • AXIS C1111-E • AXIS C1310-E Mk II	• AXIS C1410 Mk II • AXIS D3110 Mk II • AXIS D4100-VE Mk II	• AXIS D4200-VE • AXIS TP3604-E • AXIS XC1311

I.MX 8M-Mini

• AXIS C1710	• AXIS C1720	• AXIS C6110

I.MX 8QP/M

• AXIS D1110 • AXIS S3008	• AXIS S3008 Mk II • AXIS S3016	• AXIS S4000 • AXIS W800

Products per track

The product groups below are based on the active track and the available LTS tracks.

Products on active track – AXIS OS 13

Note

The product list is subject to change, new products will be added over time.

- AXIS C1110-E
- AXIS C1111-E
- AXIS C1210-E
- AXIS C1211-E
- AXIS C1310-E Mk II
- AXIS C1410 Mk II
- AXIS C1510
- AXIS C1511
- AXIS C1610-VE
- AXIS C1710
- AXIS C1720
- AXIS C6110
- AXIS C8110
- AXIS C8210
- AXIS D1110
- AXIS D2110-VE
- AXIS D2122-VE
- AXIS D2123-VE
- AXIS D2210-VE
- AXIS D3110 Mk II
- AXIS D4100-VE Mk II
- AXIS D4200-VE
- AXIS D6310
- AXIS F9104-B/-B Mk II
- AXIS F9111/-R Mk II
- AXIS F9114/-B/-B Mk II/-R Mk II
- AXIS I7010-VE/-VE Safety
- AXIS I7020
- AXIS I8016-LVE
- AXIS I8116-E
- AXIS I8307-VE
- AXIS M1055-L
- AXIS M1075-L Mk II
- AXIS M2035-LE
- AXIS M2036-LE
- AXIS M2048-LE
- AXIS M3057-PLR Mk II
- AXIS M3085-V
- AXIS M3086-V
- AXIS M3086-V Mic
- AXIS M5074
- AXIS M5075/-E
- AXIS M5526-E
- AXIS M7104
- AXIS M7116
- AXIS P1245 Mk II
- AXIS P1265 Mk II
- AXIS P1275 Mk II
- AXIS P1385/-B/-BE/-E
- AXIS P1387/-B/-BE/-LE
- AXIS P1388/-B/-BE/-LE
- AXIS P1468-XLE
- AXIS P1475-LE
- AXIS P1485-LE
- AXIS P1485-LE Kit
- AXIS P1486-LE
- AXIS P1486-LE Kit
- AXIS P1487-LE
- AXIS P1488-LE
- AXIS P1518-E/-LE
- AXIS P3275-LV/-LVE/-V
- AXIS P3277-LV/-LVE/-LVE Mic
- AXIS P3278-LV/-LVE
- AXIS P3285-LV/-LVE
- AXIS P3285-LVE Kit
- AXIS P3287-LV/-LVE
- AXIS P3288-LV/-LVE
- AXIS P3407-VE
- AXIS P3408-VE
- AXIS P3735-PLE
- AXIS P3737-PLE
- AXIS P3738-PLE
- AXIS P3747-PLVE
- AXIS P3748-PLVE
- AXIS P3827-PVE
- AXIS P3905-R Mk III
- AXIS P3925-R/-LRE
- AXIS P3935-LR
- AXIS P3945-R
- AXIS P3947-R
- AXIS Q1800-LE/-LE-3
- AXIS Q1805-LE
- AXIS Q1806-LE
- AXIS Q1808-LE
- AXIS Q1809-LE/-LE 150 mm
- AXIS Q1961-TE/-XTE
- AXIS Q1971-E
- AXIS Q1972-E
- AXIS Q2101-TE
- AXIS Q2111-E
- AXIS Q2112-E
- AXIS Q2802-E
- AXIS Q3538-SLVE
- AXIS Q3546-LVE
- AXIS Q3548-LVE
- AXIS Q3556-LVE
- AXIS Q3558-LVE
- AXIS Q3626-VE
- AXIS Q3628-VE
- AXIS Q3839-PVE/-SPVE
- AXIS Q4809-PVE
- AXIS Q6020-E
- AXIS Q6074/-E
- AXIS Q6075/-E/-S/-SE
- AXIS Q6078-E
- AXIS Q6086-E
- AXIS Q6088-E
- AXIS Q6225-LE
- AXIS Q6300-E
- AXIS Q6315-LE
- AXIS Q6318-LE
- AXIS Q6325-LE
- AXIS Q6355-LE
- AXIS Q6358-LE
- AXIS Q6411-LE
- AXIS Q8615-E
- AXIS Q8752-E
- AXIS Q8752-E Mk II
- AXIS Q9227-SLV
- AXIS Q9307-LV

• AXIS M3098-H/-LV/-V • AXIS M3125-LVE • AXIS M3126-LVE • AXIS M3138-LVE • AXIS M3905-R • AXIS M3945-R • AXIS M4215-LV/-V • AXIS M4216-LV/-V • AXIS M4317-PLR/-PLVE • AXIS M4318-PLR/-PLVE • AXIS M4327-P • AXIS M4328-P • AXIS M4337-PLVE/-SPLVE • AXIS M4338-PLVE • AXIS M4347-PLVE • AXIS M4348-PLVE • AXIS M5000/-G	• AXIS P4705-PLVE • AXIS P4707-PLVE • AXIS P4708-PLVE • AXIS P5654-E • AXIS P5654-E MK II • AXIS P5655-E • AXIS P5676-LE • AXIS P7304 • AXIS P7316 • AXIS P9117-PV • AXIS Q1656/-B/-BE/-BLE/-DLE/-LE • AXIS Q1686-DLE • AXIS Q1715 • AXIS Q1726/-LE • AXIS Q1728/-LE	• AXIS S3008 • AXIS S3008 Mk II • AXIS S3016 • AXIS S4000 • AXIS V5925 • AXIS V5938 • AXIS TP3604-E • AXIS W102 • AXIS W111 • AXIS W120 • AXIS W401 • AXIS W800 • AXIS XC1311 • AXIS XFQ1656 • D201-S XPT Q6075 • ExCam XPT Q6075

The following products will also receive AXIS OS 13. However, they do not follow the same lifecycle as the above products.

• AXIS A1210/-B • AXIS A1214 • AXIS A1610/-B	• AXIS A1710-B • AXIS A1711 • AXIS A1810-B	• AXIS A1811 • AXIS A9210

Products on LTS 2026 - 12.11

Note

LTS 2026 is supported until 2031-12-31.

- AXIS A8207-VE Mk II
- AXIS C1110-E
- AXIS C1111-E
- AXIS C1210-E
- AXIS C1211-E
- AXIS C1310-E Mk II
- AXIS C1410 Mk II
- AXIS C1510
- AXIS C1511
- AXIS C1610-VE
- AXIS C1710
- AXIS C1720
- AXIS C6110
- AXIS C8110
- AXIS C8210
- AXIS D1110
- AXIS D2110-VE
- AXIS D2210-VE
- AXIS D3110 Mk II
- AXIS D4100-VE Mk II
- AXIS D4200-VE
- AXIS D6310
- AXIS FA51/-B
- AXIS FA54
- AXIS F9104-B
- AXIS F9104-B Mk II
- AXIS F9111
- AXIS F9111-R Mk II
- AXIS F9114/-B
- AXIS F9114-B Mk II
- AXIS F9114–R Mk II
- AXIS I7010-VE
- AXIS I7010-VE Safety
- AXIS I7020
- AXIS I8016-LVE
- AXIS I8116-E
- AXIS I8307-VE
- AXIS M1055-L
- AXIS M1075-L
- AXIS M1075-L Mk II
- AXIS M4337-PLVE/-SPLVE
- AXIS M4338-PLVE
- AXIS M4347-PLVE
- AXIS M4348-PLVE
- AXIS M5000/-G
- AXIS M5074
- AXIS M5075/-G
- AXIS M5526-E
- AXIS M7104
- AXIS M7116
- AXIS P1245 Mk II
- AXIS P1265 Mk II
- AXIS P1275 Mk II
- AXIS P1385/-B/-BE/-E
- AXIS P1387/-B/-BE/-LE
- AXIS P1388/-B/-BE/-LE
- AXIS P1465-LE
- AXIS P1465-LE-3
- AXIS P1467-LE
- AXIS P1468-LE/-XLE
- AXIS P1475-LE
- AXIS P1485-LE
- AXIS P1485-LE Kit
- AXIS P1486-LE
- AXIS P1486-LE Kit
- AXIS P1487-LE
- AXIS P1488-LE
- AXIS P1518-E/-LE
- AXIS P3265-V/-LV/-LVE
- AXIS P3265-LVE-3
- AXIS P3267-LV/-LVE
- AXIS P3267-LVE Mic
- AXIS P3268-LV/-LVE/-SLVE
- AXIS P3275-LV/-LVE/-V
- AXIS P3277-LV/-LVE
- AXIS P3277-LVE Mic
- AXIS P3278-LV/-LVE
- AXIS P3285-LV/-LVE
- AXIS P3285-LVE Kit
- AXIS P3287-LV/-LVE
- AXIS Q1728/-LE
- AXIS Q1798-LE
- AXIS Q1800-LE
- AXIS Q1800-LE-3
- AXIS Q1805-LE
- AXIS Q1806-LE
- AXIS Q1808-LE
- AXIS Q1809-LE
- AXIS Q1809-LE 150 mm
- AXIS Q1961-TE/-XTE
- AXIS Q1971-E
- AXIS Q1972-E
- AXIS Q2101-TE
- AXIS Q2111-E
- AXIS Q2112-E
- AXIS Q2802-E
- AXIS Q3536-LVE
- AXIS Q3538-LVE/-SLVE
- AXIS Q3626-VE
- AXIS Q3546-LVE
- AXIS Q3548-LVE
- AXIS Q3556-LVE
- AXIS Q3558-LVE
- AXIS Q3628-VE
- AXIS Q3819-PVE
- AXIS Q3839-PVE/-SPVE
- AXIS Q4809-PVE
- AXIS Q6020-E
- AXIS Q6074/-E
- AXIS Q6075/-E/-S/-SE
- AXIS Q6078-E
- AXIS Q6086-E
- AXIS Q6088-E
- AXIS Q6135-LE
- AXIS Q6225-LE
- AXIS Q6300-E
- AXIS Q6315-LE
- AXIS Q6318-LE
- AXIS Q6325-LE
- AXIS Q6355-LE

• AXIS M1135 Mk II • AXIS M1135-E Mk II • AXIS M1137 Mk II • AXIS M1137-E Mk II • AXIS M2035-LE • AXIS M2036-LE • AXIS M2048-LE • AXIS M3057-PLR Mk II • AXIS M3085-V • AXIS M3086-V • AXIS M3086-V Mic • AXIS M3088-V • AXIS M3098-H/-LV/-V • AXIS M3125-LVE • AXIS M3126-LVE • AXIS M3128-LVE • AXIS M3138-LVE • AXIS M3215-LVE • AXIS M3216-LVE • AXIS M3905-R • AXIS M3945-R • AXIS M4215-LV/-V • AXIS M4216-LV/-V • AXIS M4218-LV/-V • AXIS M4225-LVE • AXIS M4227-LVE • AXIS M4228-LVE • AXIS M4308-PLE • AXIS M4317-PLR/-PLVE • AXIS M4318-PLR/-PLVE • AXIS M4327-P • AXIS M4328-P	• AXIS P3288-LV/-LVE • AXIS P3407-VE • AXIS P3408-VE • AXIS P3735-PLE • AXIS P3737-PLE • AXIS P3738-PLE • AXIS P3747-PLVE • AXIS P3748-PLVE • AXIS P3818-PVE • AXIS P3827-PVE • AXIS P3905-R Mk III • AXIS P3925-R/-LRE • AXIS P3935-LR • AXIS P3945-R • AXIS P3947-R • AXIS P4705-PLVE • AXIS P4707-PLVE • AXIS P4708-PLVE • AXIS P5654-E • AXIS P5654-E MK II • AXIS P5655-E • AXIS P5676-LE • AXIS P7304 • AXIS P7316 • AXIS P9117-PV • AXIS Q1615 Mk III • AXIS Q1615-LE Mk III • AXIS Q1656/-B/-BE • AXIS Q1656-BLE/-DLE/-LE • AXIS Q1686-DLE • AXIS Q1715 • AXIS Q1726/-LE	• AXIS Q6358-LE • AXIS Q6411-LE • AXIS Q8615-E • AXIS Q8752-E • AXIS Q8752-E Mk II • AXIS Q9227-SLV • AXIS Q9307-LV • AXIS S3008 • AXIS S3008 Mk II • AXIS S3016 • AXIS S4000 • AXIS V5925 • AXIS V5938 • AXIS TP3604-E • AXIS XC1311 • AXIS XFQ1656 • AXIS XPQ1785 • AXIS W100 • AXIS W101 • AXIS W102 • AXIS W110 • AXIS W111 • AXIS W120 • AXIS W401 • AXIS W800 • D201-S XPT Q6075 • ExCam XF Q1785 • ExCam XPT Q6075 • F101-A XF Q1785 • XF40-Q1785

Products on LTS 2024 – 11.11

Note

LTS 2024 is supported until 2029-12-31. After the end-of-support date, the following occurs:

- A number of products will continue to receive product-specific support (PSS) until their software support period expires.
- Certain products will have LTS 2024 as their final track and receive updates until end of software support on 2029-12-31.
- Some products have newer LTS track and will not receive further updates on LTS 2024 after 2029–12–31.

The following products will continue to receive releases after 2029-12-31 until the software support period expires.

• AXIS D4100-E • AXIS M3077-PLVE • AXIS P1455-LE	• AXIS P8815-2 • AXIS Q1951-E • AXIS Q1952-E	• AXIS Q6010-E • AXIS Q9216-SLV

The following products will not receive further releases after 2029-12-31 since the software support period expires then.

• AXIS A8207-VE • AXIS C1310-E • AXIS D3110 • AXIS M3057-PLVE Mk II • AXIS M3067-P • AXIS M3068-P • AXIS P1245 Mk II • AXIS P1265 Mk II • AXIS P1275 Mk II • AXIS P1375/-E • AXIS P1377/-LE • AXIS P1378/-LE • AXIS P1445-LE/-LE-3 • AXIS P1447-LE	• AXIS P1448-LE • AXIS P1455-LE-3 • AXIS P3247-LV/-LVE • AXIS P3248-LV/-LVE • AXIS P3255-LVE • AXIS P3715-PLVE • AXIS P3717-PLE • AXIS P3719-PLE • AXIS P3727-PLE • AXIS P3807-PVE • AXIS Q1645/-LE • AXIS Q1647/-LE • AXIS Q1659 • AXIS Q1700-LE	• AXIS Q3518-LVE • AXIS Q3527-LVE • AXIS Q6100-E • AXIS Q6215-LE • D101-A XF P3807 • F101-A XF P1377 • F101-A XF Q1785 • ExCam XF P1377 • ExCam XF P3807 • ExCam XF Q1645 • XP40-Q1785 • AXIS W400

The following products have newer LTS track. Please upgrade to newer LTS to improve cybersecurity.

- AXIS A8207-VE Mk II
- AXIS C1110-E
- AXIS C1111-E
- AXIS C1210-E
- AXIS C1211-E
- AXIS C1310-E Mk II
- AXIS C1410/Mk II
- AXIS C1510
- AXIS C1511
- AXIS C1610-VE
- AXIS C8110
- AXIS C8210
- AXIS D1110
- AXIS D2110-VE
- AXIS D2210-VE
- AXIS FA51/-B
- AXIS FA54
- AXIS F9104-B
- AXIS F9111
- AXIS F9114/-B
- AXIS I7010-VE
- AXIS I7010-VE Safety
- AXIS I7020
- AXIS I8016-LVE
- AXIS I8116-E
- AXIS M1055-L
- AXIS M1075-L
- AXIS M1135 Mk II
- AXIS M1135-E Mk II
- AXIS M1137 Mk II
- AXIS M1137-E Mk II
- AXIS M2035-LE
- AXIS M2036-LE
- AXIS M3057-PLR Mk II
- AXIS M3077-PLVE
- AXIS M3085-V
- AXIS M3086-V
- AXIS M3086-V Mic
- AXIS M3088-V
- AXIS M3125-LVE
- AXIS M3216-LVE
- AXIS M3905-R
- AXIS M4215-LV/-V
- AXIS M4216-LV/-V
- AXIS M4218-LV/-V
- AXIS M4308-PLE
- AXIS M4317-PLR/-PLVE
- AXIS M4318-PLR/-PLVE
- AXIS M4327-P
- AXIS M4328-P
- AXIS M5000/-G
- AXIS M5074
- AXIS M5075/-G
- AXIS M5526-E
- AXIS M7104
- AXIS M7116
- AXIS P1385/-B/-BE/-E
- AXIS P1387/-B/-BE/-LE
- AXIS P1388/-B/-BE/-LE
- AXIS P1465-LE/-LE-3
- AXIS P1467-LE
- AXIS P1468-LE/-XLE
- AXIS P3265-V/-LV/-LVE
- AXIS P3265-LVE-3
- AXIS P3267-LV/-LVE
- AXIS P3267-LVE Mic
- AXIS P3268-LV/-LVE
- AXIS P3268-SLVE
- AXIS P3735-PLE
- AXIS P3737-PLE
- AXIS P3738-PLE
- AXIS P3818-PVE
- AXIS P3827-PVE
- AXIS P3905-R Mk III
- AXIS P3925-R/-LRE
- AXIS P3935-LR
- AXIS P4705-PLVE
- AXIS P4707-PLVE
- AXIS P4708-PLVE
- AXIS P5654-E
- AXIS P7304
- AXIS P7316
- AXIS P9117-PV
- AXIS Q1615 Mk III
- AXIS Q1615-LE Mk III
- AXIS Q1656/-B/-BE/-BLE
- AXIS Q1656-DLE/-LE
- AXIS Q1715
- AXIS Q1798-LE
- AXIS Q1805-LE
- AXIS Q1806-LE
- AXIS Q1808-LE
- AXIS Q1809-LE 150 mm
- AXIS Q1961-TE/-XTE
- AXIS Q2101-TE
- AXIS Q3536-LVE
- AXIS Q3538-LVE/-SLVE
- AXIS Q3626-VE
- AXIS Q3628-VE
- AXIS Q3819-PVE
- AXIS Q6074/-E
- AXIS Q6075/-E/-S/-SE
- AXIS Q6078-E
- AXIS Q6135-LE
- AXIS Q6225-LE
- AXIS Q6315-LE
- AXIS Q6318-LE
- AXIS Q8615-E
- AXIS Q8752-E
- AXIS Q9307-LV
- AXIS S3008
- AXIS S3008 Mk II
- AXIS S3016
- AXIS V5925
- AXIS V5938
- AXIS XC1311
- AXIS XPQ1785
- AXIS XFQ1656
- AXIS W100
- AXIS W101

• AXIS M3126-LVE • AXIS M3128-LVE • AXIS M3215-LVE • AXIS P3227-LV/-LVE • AXIS P3228-LV/-LVE • AXIS P3245-LV/-LVE • AXIS P3245-LVE-3 • AXIS P3245-V/-VE	• AXIS P5654-E MK II • AXIS P5655-E • AXIS Q1785-LE • AXIS Q1786-LE • AXIS Q3515-LV/-LVE • AXIS Q3517-LV/-LVE • AXIS Q3517-SLVE • AXIS P5676-LE	• AXIS W800 • D201-S XPT Q6075 • ExCam XF Q1785 • ExCam XPT Q6075 • F101-A XF Q1785 • XF40-Q1785

Products on LTS 2022 - 10.12

Note

LTS 2022 is supported until 2027-12-31. After the end-of-support date, the following occurs:

- A number of products will continue to receive product-specific support (PSS) until their software support period expires.
- Certain products will have LTS 2022 as their final track and receive updates until end of software support on 2027-12-31.
- Some products have newer LTS track and will not receive further updates on LTS 2022 after 2027–12–31.

The following products will continue to receive releases after 2027-12-31 until the software support period expires.

• AXIS M3058-PLVE	• AXIS M3115-LVE	• AXIS M3116-LVE • AXIS Q9216-SLV

The following products will not receive further releases after 2027-12-31 since the software support period expires then.

• AXIS D2050-VE • AXIS M1134 • AXIS M1135/-E • AXIS M1137/-E • AXIS M3057-PLVE	• AXIS M3064-V • AXIS M3065-V • AXIS M3066-V • AXIS M3075-V • AXIS M3205-LVE	• AXIS Q1798-LE • AXIS M3206-LVE • AXIS P1367/-E • AXIS P1368-E • F101-A XF P1367 • ExCam XF P1367

The following products have at least one newer LTS track. Please upgrade to newer LTS to improve cybersecurity.

- AXIS A8207-VE/-VE Mk II
- AXIS D2110-VE Security Radar
- AXIS D3110 Connectivity Hub
- AXIS D4100-E Network Strobe Siren
- AXIS F9104-B
- AXIS F9111
- AXIS F9114/-B
- AXIS FA51/-B
- AXIS FA54
- AXIS I8016-LVE
- AXIS M1135 Mk II/-E Mk II
- AXIS M1137 Mk II/-E Mk II
- AXIS M2035-LE
- AXIS M2036-LE
- AXIS M3057-PLVE Mk II/-PLR Mk II
- AXIS M3067-P
- AXIS M3068-P
- AXIS M3077-PLVE
- AXIS M3085-V
- AXIS M3086-V
- AXIS M3088-V
- AXIS M3215-LVE
- AXIS M3216-LVE
- AXIS M4216-LV/-V
- AXIS M4308-PLE
- AXIS M5000/-G
- AXIS M5074
- AXIS M5075/-G
- AXIS M7104
- AXIS M7116
- AXIS P1375/-E
- AXIS P1377/-LE
- AXIS P1378/-LE
- AXIS P1445-LE/-LE-3
- AXIS P1447-LE
- AXIS P1448-LE
- AXIS P1455-LE/-LE-3
- AXIS P1467-LE
- AXIS P3268-LV/-LVE/-SLVE
- AXIS P3715-PLVE
- AXIS P3717-PLE
- AXIS P3719-PLE
- AXIS P3727-PLE
- AXIS P3807-PVE
- AXIS P3818-PVE
- AXIS P3925-LRE
- AXIS P3925-R
- AXIS P3935-LR
- AXIS P5654-E
- AXIS P5655-E
- AXIS P7304
- AXIS P7316
- AXIS P8815-2 3D People Counter
- AXIS Q1615 Mk III
- AXIS Q1615-LE Mk III
- AXIS Q1645/-LE
- AXIS Q1647/-LE
- AXIS Q1656/-B/-BE/-BLE/-LE
- AXIS Q1659
- AXIS Q1951-E
- AXIS Q1952-E
- AXIS Q1700-LE
- AXIS Q1715
- AXIS Q1785-LE
- AXIS Q1786-LE
- AXIS Q3515-LV/-LVE
- AXIS Q3517-LV/-LVE/-SLVE
- AXIS Q3518-LVE
- AXIS Q3527-LVE
- AXIS Q3536-LVE
- AXIS Q3538-LVE/-SLVE
- AXIS Q3819-PVE
- AXIS Q6010-E
- AXIS Q6074/-E
- AXIS Q6075/-E/-S/-SE
- AXIS Q6078-E
- AXIS Q6100-E
- AXIS Q6135-LE
- AXIS Q6215-LE
- AXIS Q6225-LE
- AXIS Q6315-LE
- AXIS Q6318-LE
- AXIS Q8752-E
- AXIS S3008
- AXIS V5925
- AXIS V5938
- D101-A XF P3807
- D201-S XPT Q6075
- ExCam XF P1377
- ExCam XF P3807
- ExCam XF Q1645
- ExCam XF Q1785
- ExCam XPT Q6075
- F101-A XF P1377
- F101-A XF Q1785
- AXIS W100
- AXIS W101
- AXIS W800
- XF40-Q1785
- XP40-Q1785

Products on PSS 9.80

The following products will continue to receive releases until the software support period expires.

• AXIS M1045-LW • AXIS M1065-L/-LW • AXIS M2025-LE • AXIS M2026-LE Mk II • AXIS M3015 • AXIS M3016 • AXIS M4206-V/-LV • AXIS P1244 • AXIS P1245 • AXIS P1254	• AXIS P1264 • AXIS P1265 • AXIS P1275 • AXIS P1280-E • AXIS P1290-E • AXIS P3374-V/-LV • AXIS P3375-V/-VE/-LV/-LVE • AXIS P3904-R Mk II • AXIS P3905-R Mk II	• AXIS P9106-V • AXIS Q1941-E/-E PT Mount • AXIS Q1942-E/-E PT Mount • AXIS Q3615-VE • AXIS Q3617-VE • AXIS Q8641-E • AXIS Q8642-E • ExCam XF M3016 • XP40-Q1942

Products on PSS 8.40

The following products will continue to receive releases until the software support period expires.

• AXIS M5525-E • AXIS Q6055-C	• AXIS Q6154-E • AXIS Q6155-E	• AXIS Q8685-E/-LE • D201-S XPT Q6055

Products on PSS 6.50

The following product will continue to receive releases until the software support period expires.

• AXIS F34 • AXIS F41 • AXIS F44 Dual Audio Input • AXIS M1145-L • AXIS M7011	• AXIS P3367-V/-VE • AXIS P5414-E • AXIS P5415-E • AXIS Q2901-E • AXIS Q2901-E PT Mount	• AXIS Q6128-E • AXIS Q7411 • AXIS Q7436 • XF40-Q2901 • XF60-Q2901

Unsupported products

The following products are not supported any longer.

Note

This list is subject to change, since more products will be added when their software support period expire.

- AXIS Companion
  - 360
  - Bullet LE
  - Bullet mini LE
  - Cube L/LW
  - Dome mini LE
  - Dome V/WV
  - Eye L/LVE
  - Eye mini L
  - Recorder 4CH
  - Recorder 8CH
- AXIS C3003-E
- AXIS F44 Main Unit
- AXIS M1124/-E
- AXIS M1125/-E
- AXIS M2026-LE
- AXIS M3006-V
- AXIS M3007-P/-PV
- AXIS M3027-PVE
- AXIS M3044-V/-WV
- AXIS M3045-V/-WV
- AXIS M3047-P
- AXIS M3048-P
- AXIS M3046-V
- AXIS M3104-L/-LVE
- AXIS M3105-L/-LVE
- AXIS M3106-L/-LVE
- AXIS M3106-L Mk II
- AXIS M3106-LVE Mk II
- AXIS P1353/-E
- AXIS P1354/-E
- AXIS P1357/-E
- AXIS P1364/-E
- AXIS P1365/-E
- AXIS P1365 Mk II
- AXIS P1365-E Mk II
- AXIS P1367/-E
- AXIS P1368-E
- AXIS P1405-E/-LE
- AXIS P1405-LE Mk II
- AXIS P1425-E/-LE
- AXIS P1425-LE Mk II
- AXIS P1427-E/-LE
- AXIS P1428-E
- AXIS P1435-E/-LE
- AXIS P3214-V/-VE
- AXIS P3215-V/-VE
- AXIS P3224-LV/-LVE
- AXIS P3224-V Mk II
- AXIS P3224-VE Mk II
- AXIS P3224-LV Mk II
- AXIS P3224-LVE Mk II
- AXIS P3225-LV/-LVE
- AXIS P3225-V Mk II
- AXIS P3225-VE Mk II
- AXIS P3225-LV Mk II
- AXIS P3225-LVE Mk II
- AXIS P3235-LV/-LVE
- AXIS P3353
- AXIS P3354
- AXIS P3363-V/-VE
- AXIS P3364-V/-VE
- AXIS P3364-LV/-LVE
- AXIS P3365-V/-VE
- AXIS P3384-V/-VE
- AXIS P3707-PE
- AXIS P3904-R
- AXIS P3905-R/-RE
- AXIS P3915-R
- AXIS P3915-R Mk II
- AXIS P5514/-E
- AXIS P5515/-E
- AXIS P5624-E
- AXIS P5624-E Mk II
- AXIS P5635-E
- AXIS P5635-E Mk II
- AXIS P8804
- AXIS P8804-2
- AXIS Q1604/-E
- AXIS Q1614/-E
- AXIS Q1615 Mk II
- AXIS Q1615-E Mk II
- AXIS Q1635/-E
- AXIS Q1765-LE
- AXIS Q1765-LE PT Mount
- AXIS Q1775/-E
- AXIS Q1931-E
- AXIS Q1931-E PT Mount
- AXIS Q1932-E
- AXIS Q1932-E PT Mount
- AXIS Q3504-V/-VE
- AXIS Q3505-V/-VE
- AXIS Q3505-V Mk II
- AXIS Q3505-VE Mk II
- AXIS Q3505–SVE Mk II
- AXIS Q6000-E
- AXIS Q6000-E Mk II
- AXIS Q6042/-E/-C/-S
- AXIS Q6044/-E/-C/-S
- AXIS Q6045/-C/-E/-S
- AXIS Q6045 Mk II
- AXIS Q6045 -C Mk II
- AXIS Q6045-E Mk II
- AXIS Q6045-E -S Mk II
- AXIS Q6052/-E
- AXIS Q6054/-E
- AXIS Q6054 Mk II
- AXIS Q6054-E Mk III
- AXIS Q6055/-E/-S
- AXIS Q6114-E
- AXIS Q6115-E
- AXIS Q6124-E
- AXIS Q6125-LE
- AXIS Q8414-LVS
- AXIS Q8631-E
- AXIS Q8632-E
- AXIS Q8665-E/-LE
- ExCam XPT Q6055
- XF40-Q1765
- XF60-Q1765

	• AXIS Q1615/-E	• XP40-Q1765

Downgrade restrictions

Downgrade is not supported in certain AXIS OS versions, mainly for security reasons e.g. when a vulnerability has been addressed in the current version but still exists in earlier versions. Please see the release notes for the specific AXIS OS version for more information.
The table below shows when the restriction was introduced as well as possible downgrade paths.

Affected AXIS OS version	Affected products	Can be downgraded to
12.0.91	All products based on: • *AXIS ARTPEC-8, on page 84* • *I.MX 6SX, on page 87* • *I.MX 6ULL, on page 87* • *I.MX 8M-NANO, on page 87* • *I.MX 8M-Mini, on page 87* • *I.MX 8QP/M, on page 87*	• 11.11.109 or later • 10.12.252 or later
11.11.109	All products based on: • *AXIS ARTPEC-8, on page 84* • *I.MX 6SX, on page 87* • *I.MX 6ULL, on page 87* • *I.MX 8M-NANO, on page 87* • *I.MX 8M-Mini, on page 87* • *I.MX 8QP/M, on page 87*	• 10.12.252 or later
11.7.57	All products based on: • *AXIS ARTPEC-8, on page 84*	–
11.6.94	All products based on: • *AXIS ARTPEC-8, on page 84* As well as: • AXIS A8207-VE Mk II • AXIS Q3527-LVE.	• 10.12.208 or later
10.12.323	• AXIS D3110 • AXIS D4100-E • AXIS M3215-LVE • AXIS M3216-LVE • AXIS P1467-LE • AXIS P1468-LE • AXIS P3265-LV/-LVE/-V • AXIS P3267-LV/-LVE • AXIS P3268-LV/-LVE/-SLVE • AXIS P4705-PLVE • AXIS P4707-PLVE	–

	• AXIS Q1656/-B/-BE/-BLE/-LE • AXIS Q3536-LVE • AXIS Q3538-LVE/-SLVE • AXIS W400	
10.12.252	All products based on: • *AXIS ARTPEC-8, on page 84* • *I.MX 6SX, on page 87* • *I.MX 6ULL, on page 87* • *I.MX 8M-NANO, on page 87* • *I.MX 8M-Mini, on page 87* • *I.MX 8QP/M, on page 87*	–
10.12.213	All products based on: • *AXIS ARTPEC-8, on page 84*	–
10.12.208	All products based on: • *AXIS ARTPEC-8, on page 84* As well as: • AXIS A8207-VE Mk II • AXIS Q3527-LVE	–

T10228770

- (M70.2)

© 2021 – 2026 Axis Communications AB