AXIS OS 13.0

What's new in AXIS OS?

This flyer covers selected features and updates in AXIS OS 13.0. A complete overview is available in the **release notes.**



The list of Axis devices that can be updated to AXIS OS 13.0 active track release is available **here.**

GENERAL

Feature / update	Function	Value
Year 2038 (Y2038) problem addressed	Y2038 problem refers to a time computing problem that will occur after 19th January 2038. For 32-bits Axis devices, significant software adjustments have been made to shift into 64-bit timing.	Prevents time calculation error and failure, caused by Y2038 problem.
Background appearance	AI driven imaging feature for ARTPEC-9 single channel cameras.	Reduces the bitrate without reducing the image quality.
Autogenerated passwords	Added the possibility to autogenerate password and ability to copy the password to clipboard. Now available in the web interface.	Saves time for end user.

CYBERSECURITY

Feature / update	Function	Value
Password complexity enforcement	Enabled by default, and cannot be disabled, for new or edited accounts created via SSH, VAPIX, ONVIF and SNMP profile selection. This change also applies to the web interface.	Password complexity enforcement is considered best practice when managing account credentials.
HTTPS-only enforcement	By default, and after a factory default, network connections to the device will only be allowed on HTTPS port 443.	To increase the overall device security following the Secure by Default approach.
Signed video enabled by default	With signed video feature it's possible to verify the authenticity of the video.	Enabling signed video from factory allows users to take advantage of signed video without requiring any pre-configuration.
Enforcement of ACAP signing	All ACAPS must now be digitally signed. If the ACAP 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.	Increased cybersecurity. Ensures authenticity of the ACAP and identity of the software provider.

CYBERSECURITY

Feature / update	Function	Value
Added support for Post-Quantum Crypto (PQC) ML-KEM hybrid scheme for TLS 1.3 communication	ML-KEM (Module-Lattice-based Key Encapsulation Mechanism) is a standardized cryptographic algorithm designed to secure data against the threat of future quantum computers. Provides "store now, decrypt later" protection. Can be used by supporting clients when using services such as HTTPS, MQTT, RTSPS, and 802.1X.	Increased protection for future PQC computers.
CVEs addressed	Addressed CVE-2026-9063, CVE-2026-13409, CVE-2026-14542 CVE-2026-14543 and CVE-2026-63282 which will be externally disclosed 10th November. Addressed CVE-2026-81709 and CVE-2026-84751, which will be externally disclosed 9th February.	Increased overall cybersecurity level.
Software components updates	Updated OpenSSH to version 10.4 and cURL to version 8.21.0.	Increased overall cybersecurity level.

ANALYTICS

Feature / update	Function	Value
AXIS Audio Analytics: Human presence detection classification now available	A new AI-based classification that detects indications of human presence by recognizing sounds people make. Provides an additional signal when people enter or are active in a monitored environment.	Useful in situations where video analytics alone may not provide the complete picture.
AXIS Object Analytics: New Analytics Space	Analytics Space provides a single, intuitive interface for managing analytics across different devices. Enhanced metadata visualization allows for live detections and identified objects directly within the video stream.	Easier and faster interaction with the analytics.

TERMS

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

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

Software Bill Of Material (SBOM)
An inventory list of all the components that make up a software resource.

Common Vulnerabilities & Exposures (CVE)
A public database that identifies and catalogs known cybersecurity vulnerabilities. All entries are scored using the Common Vulnerability Scoring System (CVSS) to evaluate the threat level.

Breaking change
A change in functionality that can break or disrupt the previously known and intended behavior. Typically implemented to improve usability and increase security.

LINKS

AXIS OS | AXIS OS FOR IT INFRASTRUCTURE | AXIS OS SUPPORT | AXIS OS NOTIFICATION SERVICE

VIDEOS | AXIS SECURITY ADVISORY | RELEASE NOTES

©2026 Axis Communications AB. AXIS COMMUNICATIONS, AXIS, ARTPEC and VAPIX are registered trademarks of Axis AB in various jurisdictions. All other trademarks are the property of their respective owners.