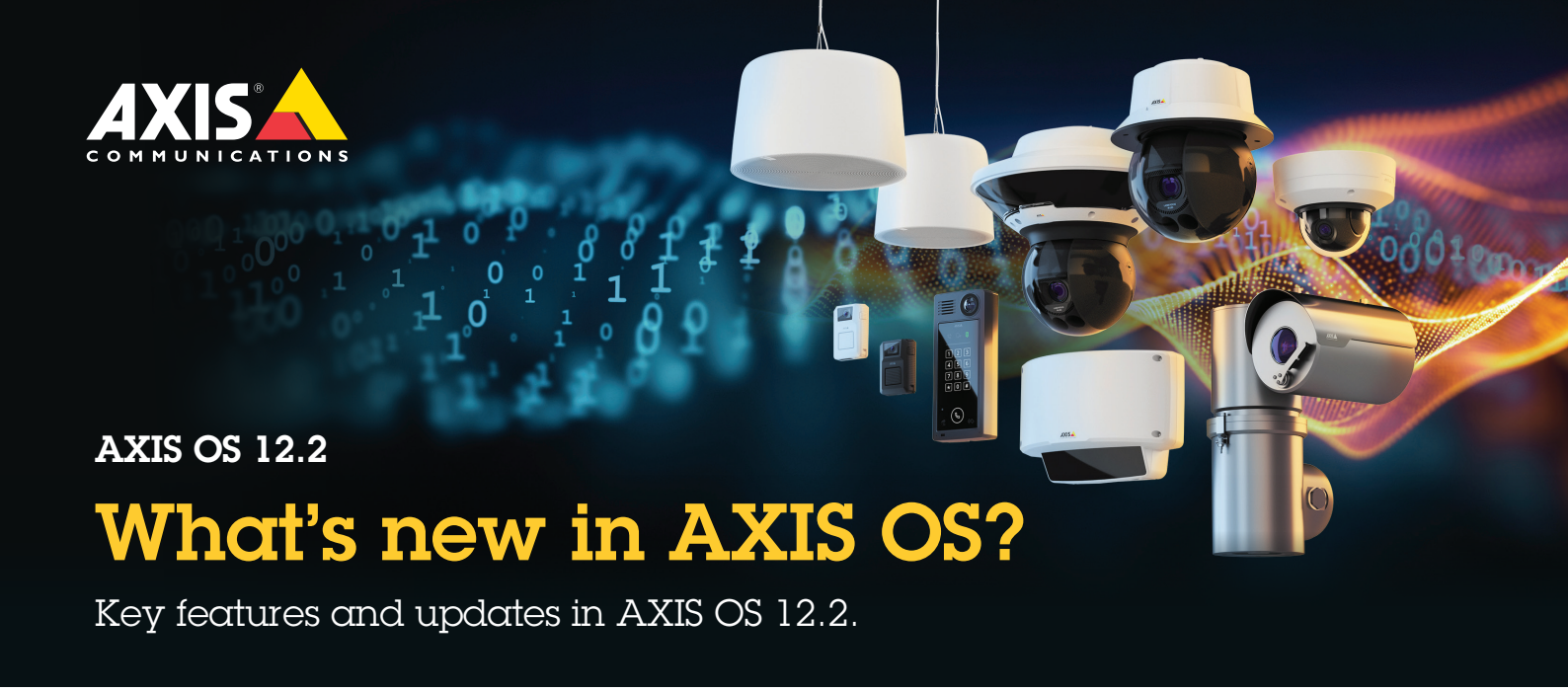

AXIS OS 12.2

What's new in AXIS OS?

Key features and updates in AXIS OS 12.2.

GENERAL

The list of Axis devices that can be updated to AXIS OS 12.2 active track release is available here.

Feature / update	Function	Value
Added support for trouble shooting in the web interface	In addition to the existing possibility to download network trace file for Axis device, it's now also possible to ping and port check the hosts on the network.	Easier and faster trouble shooting of network issues for system integrators and IT teams.
DDNS update parameter now included in the web interface	Dynamic Domain Name System (DDNS) update parameter is now included in the web interface.	Increased accessibility - now easier to find for everyone.
"Best snapshot" overlay in the metadata stream now included in the web interface	"Best snapshot" overlay and object attributes in the metadata stream for moving objects is now available in the web interface.*	Increased efficiency for search, easy to find for everyone in the web interface.
Custom file name for sending video clips	Added the possibility to choose a custom file name for sending video clips in the action rules.	Convenient file handling.

*** For products based on ARTPEC-9. ARTPEC-8, ARTPEC-7 and AMBARELLA-CV25**

CYBERSECURITY

Feature / update	Function	Value
Added support for Public key authentication with SSH	Public key authentication uses a pair of computer-generated keys, one public and one private. SSH is a network protocol that gives users a secure way to access a computer over an unsecured network.	Increased overall cybersecurity, easier configuration and handling of accessing the device for ACAP-developers.
Patched vulnerabilities	Through AXIS OS bug bounty program, along with two newly performed AXIS OS penetration tests, three vulnerabilities have been addressed and patched: CVE-2025-0359, CVE-2025-0360 and CVE-2024-47259. In addition, we have updated open source package libraries to patch two other vulnerabilities: CVE-2024-52533 and CVE-2023-52424.	Increased cybersecurity.
Extended Firewall VAPIX API	The Firewall VAPIX API added in AXIS OS 11.8 is now enhanced with the possibilities of filtering and more granular access to the device. It's now possible to filter for MAC-addresses and IP- and port-ranges.	Increased cybersecurity, increased flexibility for configuration. IT teams can increase network security with Axis devices.

PRODUCT-SPECIFIC

Feature / update	Function	Value
Added basic SNMP support in the web interface*	Settings for Simple Network Management Protocol (SNMP) is now added to the web interface. With SNMP the user can easier monitor the system.	Increased accessibility - now easier to find for everyone. IT teams can now easier access the settings.

*** It applies to AXIS S3008, AXIS S3008 MK II and AXIS S3016 network recorders.**

TERMS

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.

AXIS OS product-specific support (PSS) track
The AXIS OS product-specific support (PSS) track is a rare track for when a product requires support after an LTS track expires. The products on this track continue to receive necessary bug fixes and cybersecurity updates. Each product sits on its own track and the track is not connected to other product tracks. Non-AXIS OS products have similar support tracks.

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.

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

RELEASE NOTES | VIDEOS | WEBPAGE