WHITE PAPER

Cybersecurity with Axis network audio

September 2025

AXIS COMMUNICATIONS

Summary

In today's interconnected world, securing audio communication systems is vital for protecting sensitive information and maintaining operational efficiency. Networked audio systems face numerous threats, including unauthorized access, eavesdropping, denial-of-service attacks, malware, and software exploits. Axis addresses these risks with state-of-the-art security solutions that integrate seamlessly with existing infrastructures, offering reliability, scalability, and robust protection.

Axis employs a security-by-design approach, incorporating encryption, authentication, secure software updates, access control, system hardening, and event logging. Secure protocols such as SIPS, SRTP, HTTPS, and IEEE 802.1AE enable secure communication and data transmission.

Axis audio management software provides role-based access control, secure onboarding, and comprehensive event logging, catering to both on-premises and cloud-based deployments.

By leveraging these layers of security, Axis network audio systems deliver end-to-end protection against cyber threats.

Table of Contents

1 Introduction

Audio systems play a crucial part for communication, security, and operational efficiency in various industries such as retail, transportation, public safety, and education. These systems are also attractive targets for cyber attacks, so robust security measures are essential. A compromised audio system can have serious and far-reaching consequences.

This white paper explores the main layers of security that Axis speakers and audio systems employ to address these challenges.

2 Understanding the risks

With the increasing deployment of networked audio solutions across industries, the potential risks associated with unsecured systems have grown significantly.

Networked audio systems can be exposed to several types of threats.

- **Unauthorized access.** Unprotected audio devices can be accessed remotely by malicious actors who could then take control of speakers, issue unauthorized announcements, or disrupt operations.
- **Eavesdropping and data interception.** Networked audio systems sometimes transmit sensitive voice data over wired or wireless networks. Without encryption, attackers could intercept and record conversations, leading to privacy breaches, industrial espionage, or misuse of confidential information.
- **Denial-of-service (DoS) attacks.** Attackers can flood networked speakers or audio servers with excessive traffic, causing system overload and disruption of services. Such attacks could render emergency communication systems inoperable at critical moments.
- **Malware and ransomware attacks.** Just like traditional IT infrastructure, networked audio devices can be compromised by malware or ransomware. Attackers could lock down devices, demand ransom payments, or use the compromised system as an entry point to attack the broader network.
- **Software exploits and supply chain vulnerabilities.** Outdated operating systems with unpatched security flaws can be exploited to gain control over audio devices. Additionally, insecure supply chain practices can introduce vulnerabilities before deployment, making systems susceptible from the start.

3 Benefits of Axis network audio

Axis provides state-of-the-art speaker and system security solutions that seamlessly integrate with existing infrastructures. Open architecture provides compatibility with diverse systems and protocols. An Axis system is flexible and designed to grow with your organization's needs, from small deployments to enterprise-scale networks. Axis offers both on-premises and cloud-based audio management systems.

Axis uses a security-by-design approach for software development. Our framework Axis Security Development Model (ASDM) defines processes and tools that make sure we integrate security throughout the entire software development lifecycle and reduce the risk of vulnerabilities. ASDM is continuously improved.

One of many inputs to the improvement is that we perform regular evaluations of various security-related standards and map them to ASDM. Our software meets stringent industry standards for data privacy and security, including the EU's GDPR (General Data Protection Regulation).

4 Key features of speaker and system security

With Axis network audio, security is built into the devices as well as the management systems.

Encryption and authentication

- Encryption provides secure transmission of audio data through TLS 1.2 and 1.3, preventing unauthorized parties from intercepting and accessing the information.
- Authentication makes sure that only authorized devices and users can access the devices but also the overall solution.

Secure device software updates

- Secure boot (in most products) and digitally signed patches make sure that only verified device software is installed. This protects systems from malicious code.

Access control

- AXIS Audio Manager Pro and AXIS Audio Manager Center use role-based access control (RBAC), which limits system access to authorized personnel only.
- Centralized management enables IT administrators to monitor and control permissions effectively.

System hardening

- Default settings are optimized for security out of the box, reducing vulnerabilities.
- Additional configuration options allow for customization based on specific use cases. AXIS OS Hardening Guide at *help.axis.com/axis-os-hardening-guide* provides technical advice.

Event logging and monitoring

- Comprehensive logging provides visibility into system activities. This can provide help in real-time threat detection and forensic analysis.

5 Security throughout the system

With Axis network audio, security is built into the devices and management systems. Secure protocols enable a high level of security in the communication between devices and management software.

5.1 Device security

All Axis speakers operate on AXIS OS, our purpose-built device software for Axis devices. It enables long-term value, cybersecurity, and world-class integration. With AXIS OS, all our speakers inherit robust security features from the Axis ecosystem. This provides consistency and reliability across all devices and offers end-to-end protection for every deployment. The security features include encrypted file systems and the hardware-based cybersecurity platform Axis Edge Vault (*axis.com/solutions/edge-vault*).

Axis Edge Vault safeguards the integrity of Axis devices and enables the execution of secure operations based on cryptographic keys. It enables the IEEE 802.1AR-compliant Axis device ID to be verified and leveraged for secure onboarding of the device in zero trust networks through IEEE 802.1X and HTTPS. With Axis Edge Vault, you can securely boot the device, integrate it, and be sure sensitive information like cryptographic keys is protected.

With Axis Edge Vault you can be sure that the Axis device you've received hasn't been tampered with or compromised in the physical supply chain. Axis Edge Vault establishes a chain of trust and ensures an unbroken chain of cryptographically validated software. For instance, the feature *signed OS* guarantees that the device software is from Axis and only updates that are signed by Axis can be installed.

5.2 Security protocols

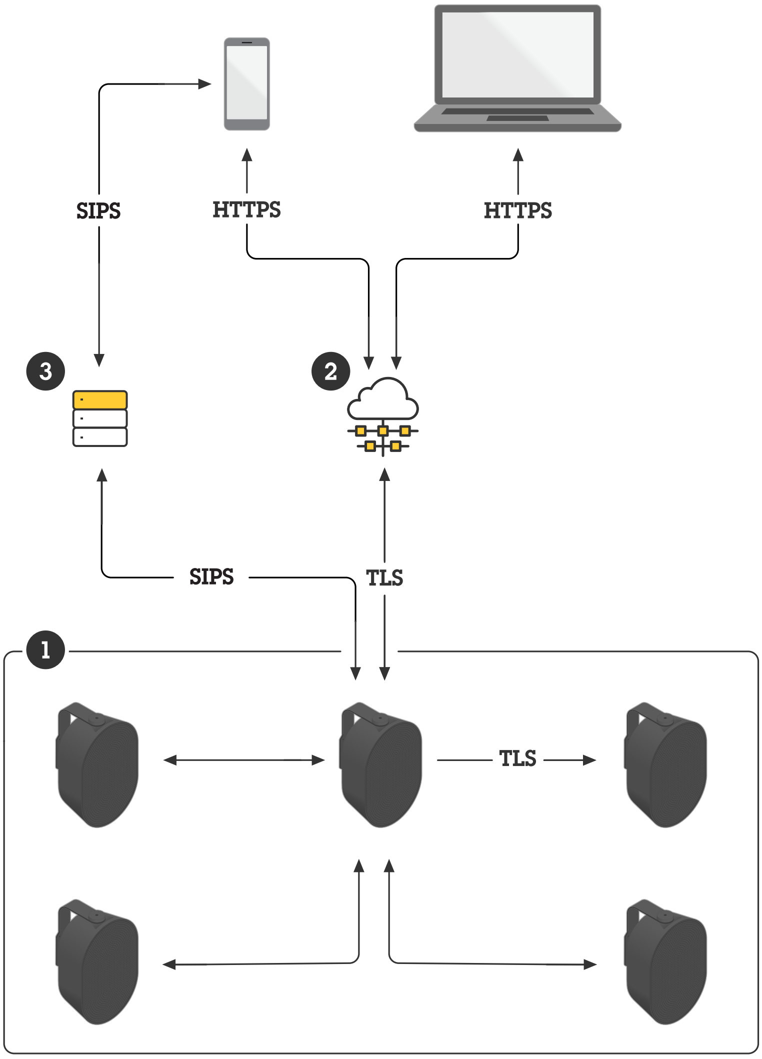
Axis devices and systems use open protocols for secure communication, transmission, and streaming.

- **SIPS** (SIP Secure): enhances the standard SIP (Session Initiation Protocol) by incorporating TLS (Transport Layer Security). This establishes a secure connection between an IP PBX and a VoIP telephone. Once the secure connection is set up, SRTP (Secure Real-Time Transport Protocol) encrypts voice data into secure IP packets for transmission over the internet. This provides end-to-end encryption from the transmitter (IP phone system) to the receiver (speaker).

  By leveraging SIPS and SRTP, Axis systems secure both the audio data and the connection setup itself. This means that the audio stream and connection details (such as caller identity and recipient) are fully encrypted and the peer-to-peer secure communication channel is robust.

- **Multicast controller**: a multicast controller feature in Axis speakers allows secure reception of multicast audio streams sent via SRTP. This makes sure that group communication is encrypted.

- **Transmit.cgi** and **receive.cgi**: These VAPIX APIs provide a secure method to send and receive audio streams in encrypted point-to-point communication via HTTPS. CGI (Common Gateway Interface) is a standard protocol that specifies communication between a web server and external programs.
- **RTSPS** (Real-Time Streaming Protocol Secure): a network control protocol used to establish and manage real-time media streams between a server and a client. This is supported for secure audio streaming, utilizing encryption to prevent unauthorized access.
- **HTTPS**: All APIs are secured with HTTPS to maintain confidentiality and integrity in all communications.
- **IEEE 802.1AE**: also known as MACsec (Media Access Control Security), a network protocol that AES-128 encrypts network communication fundamentally on network layer 2. If combined with HTTPS, RTSPS, and SIPS, network traffic is essentially double-encrypted and network security significantly enhanced.



A network audio system with secure communication thanks to several open protocols.

1 *AXIS Audio Manager Edge: on-premises audio management integrated in Axis speakers*
2 *AXIS Audio Manager Center: hybrid-cloud centralized audio management*
3 *Partner PBX*

5.3 Security in audio management software

5.3.1 On-premises solutions

Axis on-premises solutions are designed to manage zoning, prioritization, and secure communication across multiple speakers on-site.

AXIS Audio Manager Edge. This management software is built into every network audio speaker from Axis. It makes each speaker a complete, all-in-one sound system with no need for a separate software management server. AXIS Audio Manager Edge is intended to manage low-complexity projects that consist of up to 200 devices in up to 20 zones.

- Has support for encryption between devices. The default encryption method is TLS with self-signed certificates, but we recommend that you install trusted certificates on your devices and enable TLS authentication in the site's system settings. This provides protection against man-in-the-middle attacks.
- Enables secure onboarding of devices to local site. Initial setup is done over HTTPS with device credentials. After that MQTT (TLS-PSK) is used for communication between devices and SRTP is used to send encrypted RTP data such as audio streams between the devices.
- Provides external system access for operational use cases via HTTPS API.

AXIS Audio Manager Pro. This management software is intended for larger and more advanced projects. It can handle large numbers of zones (500+) and thousands of devices (5000+) in a single interface.
AXIS Audio Manager Pro facilitates long-term scheduling and advanced priority settings.

- Includes role-based access control, which limits system access to authorized personnel only, with support for Active Directory integration.
- Enables secure onboarding of devices.
- Includes a detailed event and audit log. This provides a comprehensive record of system activity, which can help administrators track changes, monitor behavior, and troubleshoot issues.

5.3.2 Cloud-based solution

AXIS Audio Manager Center is a service for remote management and monitoring of multisite systems, scaling from a few sites to several thousands. It is used together with AXIS Audio Manager Edge at each local site. Employing both cloud-based and on-premises components, this is a convenient and stable hybrid cloud solution.

AXIS Audio Manager Center simplifies management, gives centralized control, and handles secure onboarding of devices. User workload is significantly reduced, with a single sign-on to schedule announcements, background music, ads, and more for selected sites or zones. The main security features include:

- Role-based access control (RBAC): limits system access to authorized personnel only.
- Centralized user management: supports *My Axis* or Active Directory users/groups for streamlined administration. No need for local users.
- Secure onboarding: simplifies the secure onboarding of devices with trust from the cloud, using unique certificates installed on each device.
- Simplifies secured E2E configurations: enables secure configuration of SIPS, including certificate handling.
- Health monitoring and notifications: offers centralized monitoring for system health and immediate alerts for potential issues.
- Secure communication: all communication between the cloud and devices is encrypted via TLS, with mutual TLS (two-way authentication) ensuring robust security.
- Remote access: enables secure remote access to local site from anywhere.

T10225475/EN/M1.13/2509

About Axis Communications

Axis enables a smarter and safer world by improving security, safety, operational efficiency, and business intelligence. As a network technology company and industry leader, Axis offers video surveillance, access control, intercoms, and audio solutions. These are enhanced by intelligent analytics applications and supported by high-quality training.

Axis has around 5,000 dedicated employees in over 50 countries and collaborates with technology and system integration partners worldwide to deliver customer solutions. Axis was founded in 1984, and the headquarters are in Lund, Sweden.