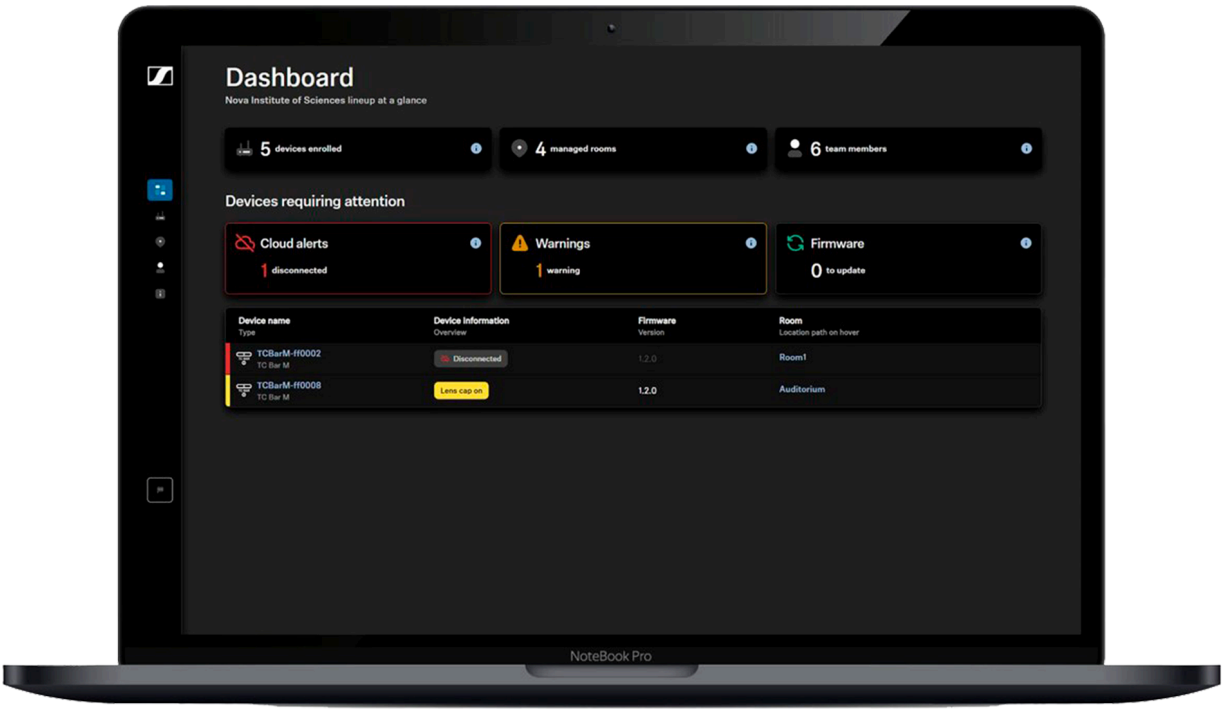


DeviceHub

Security white paper

PDF Export of the Original HTML Manual

Contents

1. Introduction

This document aims to provide information about the security and data privacy of DeviceHub to facilitate the onboarding in our customers' IT environments.

Sennheiser DeviceHub is a cloud-based platform for managing and monitoring Sennheiser AV devices across locations. It provides centralized visibility, configuration, and control from any browser, supporting both on-site and remote workflows.

Designed for AV and IT professionals, DeviceHub helps maintain system reliability, streamline operations, and enable secure collaboration across distributed environments.

The Sennheiser DeviceHub platform is built following security by design principles to ensure the confidentiality, integrity, and availability of your AV infrastructure. Hosted on Microsoft Azure, it leverages enterprise-grade identity controls, encrypted communications, and compliance frameworks to protect user data and device interactions.

2. Security at Sennheiser

Overview of Sennheiser's integrated security approach and the key measures used to ensure secure, standards-compliant products for customers.

At Sennheiser, we prioritize our customers' security and are dedicated to being a dependable and trustworthy partner. We are committed to addressing the security needs of our customers, particularly our corporate and higher education clients, while staying ahead of upcoming security regulations. Our security features are being progressively integrated into our portfolio and will be included in relevant new solutions.

Our approach to integrated security:

- Our dedicated product security team establishes security requirements and standards, overseeing their conceptualization and implementation.
- At Sennheiser we implement the **Security by Design** approach into our development life cycle and treat security as a core business requirement.
- We utilize **Security by Default**, while aiming to balance robust security in our products' default settings with user-friendly design.
- We follow best practices for a secure Software Development Life Cycle (SDLC) and information security.
- We perform internal and external security evaluations and penetration testing, along with continuous efforts to identify potential vulnerabilities while providing security patches as fast as possible to our customers.
- We have a vulnerability handling process that ensures prompt and effective response to, and mitigation of, security incidents.
- We follow best practices and comply with relevant security standards and regulations. For more details, please see chapter Compliance.

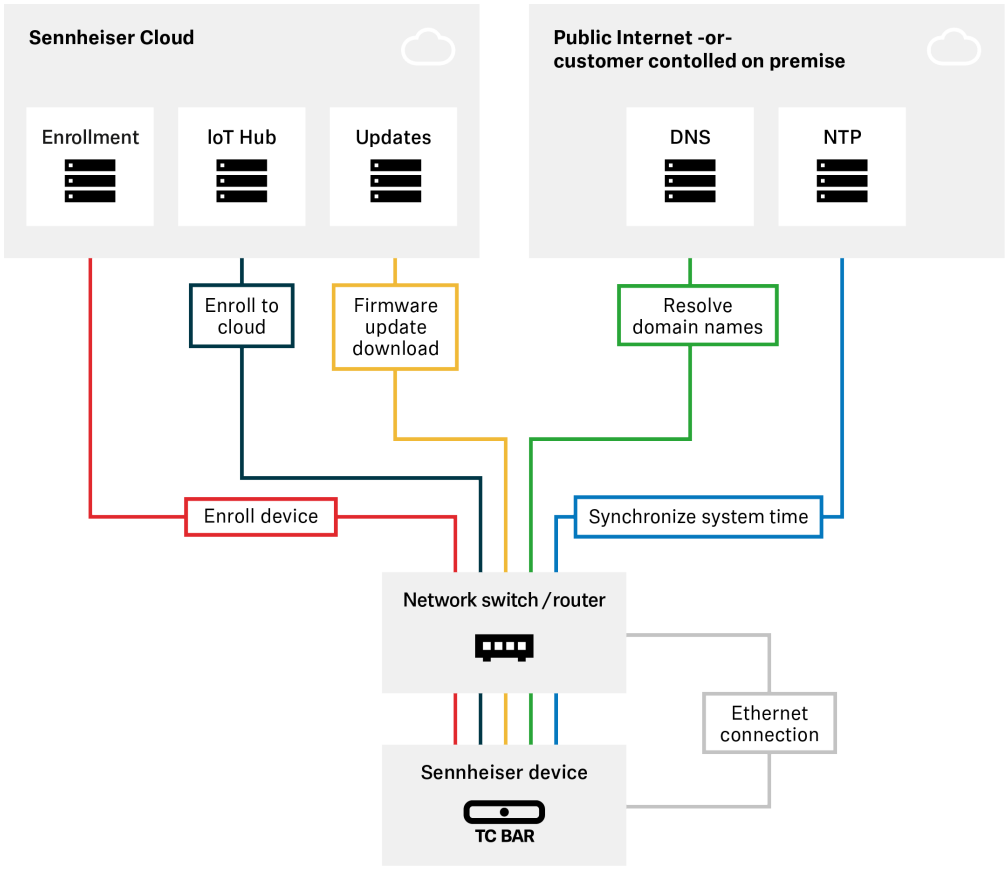
We are also continuously adapting our requirements to cover upcoming regulations such as the EU Cyber Resilience Act.

3. Communication flows

Overview of the communication flows between Sennheiser devices and DeviceHub.

> **i** The connection to DeviceHub is disabled by default on the Sennheiser devices in order limit the attack surfaces of a device in a factory default state.

Below you can find relevant information for understanding the communication flows between devices and Sennheiser DeviceHub.



Sennheiser DeviceHub utilizes Microsoft Azure IoT Hub for connections established by the Sennheiser devices. The following network protocols and ports are required for the Sennheiser cloud connectivity over the device control network.

> **i** All device communication over HTTPS and MQTT is secured with TLS 1.2 or higher.

IPv4	Port	Protocol	Service / FQDN
Device Enrollment Service	443	HTTPS	api.cloud.sennheiser.com

IPv4	Port	Protocol	Service / FQDN
Azure IoT Hub, **EMEA** (Europe, Middle East and Africa)	443	MQTT over WebSockets	iot-sennheiser-prod-emea.azure-devices.net
Azure IoT Hub, **APAC** (Asia and Pacific regions)	443	MQTT over WebSockets	iot-sennheiser-prod-apac.azure-devices.net
Azure IoT Hub, **AMER** (Americas)	443	MQTT over WebSockets	iot-sennheiser-prod-amer.azure-devices.net
Firmware Update Service	443	HTTPS	updates.sennheiser.com
Network Time Synchronization	123	NTP	Default: time.cloudflare.com, time.nist.gov
Domain Name Service	53	DNS	User configurable

4. Authentication & authorization

User authentication, access control, and secure device enrollment in DeviceHub.

To safeguard your data, DeviceHub employs a comprehensive security framework grounded in industry-standard authentication and authorization.

This framework incorporates a range of security features that ensure only verified and appropriately authorized users can access DeviceHub, namely:

Identity & Access Management:

DeviceHub uses the **Microsoft Entra** service for authentication. Organizations can enable Single-Sign-On (SSO) or allow users to register for the service with an email address.

- Single-Sign-On (SSO) is supported with the following protocols: SAML 2.0, OpenID Connect, OAuth 2.0.

Multi-factor Authentication (MFA):

Multi-factor authentication (MFA) is available to all users through single sign-on (SSO). Support via Sennheiser's own solution, using a second email verification code, will follow soon.

Role-Based Access Control (RBAC):

Assign roles to users to control permissions. Current roles include **Organization Owner** and **Location Admin**, with more coming soon. For a detailed description, please refer to the DeviceHub user documentation.

Device Enrollment:

Devices can be securely enrolled in Sennheiser DeviceHub to enable cloud-based device control, using a time-limited enrollment code.

5. Data protection

Sennheiser applies a comprehensive data protection strategy that ensures robust encryption controls for both data at rest and data in transit.

Encryption in transit

All communication between users, DeviceHub, and devices uses HTTPS, MQTT and WSS network protocols. For both the communication is authenticated and encrypted using Transport Layer Security (TLS) version 1.2 or higher.

Encryption at rest

Customer data—including user credentials or organization and device configurations—is encrypted using **AES256.** For more information on Azure data encryption at rest, please visit Microsoft's Documentation.

6. Data privacy

Overview of how Sennheiser DeviceHub collects, stores, and protects private and non-private data in compliance with GDPR.

> **i** All processing of private data is carried out in compliance with GDPR. For more information, see the privacy policy.

Private data

Sennheiser needs to store a minimum set of **private data** to offer the user login & authentication for DeviceHub, namely:

- User email address
- First and last name of the user

Microsoft Azure services are utilized for storage of private data, hosted on EU data servers.

Non-private data

Sennheiser also stores **non-private data** to offer the cloud monitoring and configuration service, such as:

- Organization name
- Location names
- Device configuration

Microsoft Azure services are utilized for storage of non-private data, hosted across AMER, EMEA and APAC for redundancy and availability.

No audio or video data is ever sent from a Sennheiser device to the Sennheiser DeviceHub. Only control information is transmitted to the cloud, namely device configuration and monitoring status.

7. Security testing and vulnerability management

DeviceHub undergoes continuous security testing and structured vulnerability management to help ensure robust protection against emerging threats.

Security testing

Sennheiser's internal product security team performs regular security testing of DeviceHub. In addition, DeviceHub has undergone independent third-party testing through means of an external penetration test.

An external security assessment, including thread modelling and security concept reviews, was executed. Sennheiser is committed to regularly testing the security of our products.

Vulnerability management

Sennheiser's dedicated product security team investigates vulnerabilities and determines their applicability, severity, and impact. Sennheiser responds within 7 working days upon receiving reported vulnerabilities and will provide updates on the status of confirmed vulnerabilities in a timely manner.

i If you want to report a vulnerability in a Sennheiser product:

- Open the form: Vulnerability report.
- In the field **How can we help you?***, select **Report a security issue: Product/Software**.

8. Monitoring & incident response

DeviceHub monitors security-related events and defines processes for efficient incident detection, analysis, and response.

Continuous cloud security monitoring

We operate centralized security monitoring for our cloud environment to quickly detect, assess, and respond to threats.

- **Centralized telemetry & SIEM aggregation**

  Security signals from our Microsoft cloud services are collected and analyzed within a Security Information and Event Management (SIEM) platform to provide real-time visibility and alerting.

- **Automated detection & analytics**

  We employ automated detections—combining rule-based alerts and behavioral analytics—to identify anomalous activity and potential threats, with continuous tuning to reduce false positives.

- **Log retention**

  Security logs, including audit and login events, are retained for 365 days in line with our policy to support investigations and compliance.

- **Incident response**

  A dedicated Incident Response (IR) team follows a documented process with defined escalation paths.

- **Monitoring scope**

  Our monitoring is presently focused on identity and access telemetry from Microsoft Entra (sign in and audit events).

- **Resilience & Recovery**

  We leverage Microsoft services to protect data and sustain operations in the event of an incident.

9. Compliance

DeviceHub compliance with security-related certifications and standards.

DeviceHub complies with the following security regulations:

- General Data Protection Regulation (GDPR)
- NIS2, compliance when it comes into force in Germany in 2026
- Cyber Resilience Act (CRA), compliance when it comes into force 2027

10. Additional resources

Find more information, documentation, and support options related to Sennheiser DeviceHub.

- Sennheiser DeviceHub product page – all the latest features and documentation
- Sennheiser DeviceHub User documentation
- Sennheiser DeviceHub connectivity guide
- Sennheiser DeviceHub – Customer Support Form
- Security @ Sennheiser

Sennheiser electronic SE & Co. KG | Am Labor 1 | 30900 Wedemark | Germany