# TeamConnect Ceiling M Plus

## Cybersecurity white paper

# Contents

1. Introduction ..... 3
2. Cybersecurity at Sennheiser ..... 4
3. Product overview and cybersecurity features ..... 5
    Product components in a nutshell ..... 5
    Cybersecurity features ..... 7
4. List of network ports ..... 9
5. Security recommendations ..... 11
6. Compliance ..... 12
7. Conclusion ..... 13

# 1. Introduction

This white paper aims to provide IT professionals with an in-depth understanding of the TeamConnect Ceiling M Plus (TCC M Plus), its components, and its security features.

In the rapidly evolving digital landscape, cybersecurity has become a paramount concern for businesses worldwide. As hybrid meetings and remote collaboration continue to shape modern workplaces, the demand for secure, reliable, and high-quality audio solutions is greater than ever. Sennheiser addresses this need with the TeamConnect Ceiling M Plus (TCC M Plus) microphone - a cutting-edge solution designed to deliver exceptional audio clarity while maintaining robust security standards. This whitepaper provides IT and AV professionals with an understanding of the TCC M Plus microphone, its architecture, and the security mechanisms that safeguard your communication environment.

# 2. Cybersecurity at Sennheiser

**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 new relevant 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.

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

# 3. Product overview and cybersecurity features

TeamConnect Ceiling M Plus offers flexible conferencing solutions with multiple operating modes, control options, and interfaces.

## Product components in a nutshell

TeamConnect Ceiling M Plus is a state-of-the-art ceiling microphone, designed to deliver secure, seamless collaboration in modern meeting environments.

Built on Sennheiser's commitment to reliable audio, it combines advanced audio performance with robust safeguards to protect sensitive communication. Featuring adaptive, intelligent beamforming technology, the system ensures crystal-clear speech capture while minimizing unauthorized access risks. It offers streamlined integration options, including single cable mode and flexible installation designs.

### Sennheiser control software

The TeamConnect Ceiling M Plus can be configured via:

- The device's Local Web UI, which is accessible over its local IP address or host name via any modern browser. It allows for easy and quick device configuration in the local network or on your desk.
- DeviceHub, which is a cloud-based platform for managing and monitoring Sennheiser AV devices across locations.

### PartnerLink

PartnerLink is a Sennheiser integration capability that enables supported products to be configured directly within selected third-party AV platforms. It is designed to simplify audio integration and accelerate configuration and commissioning.

The TeamConnect Ceiling M Plus provides a PartnerLink | Q-SYS mode, which allows devices to be discovered by and configured via Q-SYS Designer software. During the paring process of the TCC M Plus with a Q-SYS AV&C processor, the TCC M Plus shares a dedicated password with the Q-SYS device and receives a unique password in return. The TCC M Plus is muted until the pairing is completed. This ensures only authenticated devices can establish a PartnerLink connection, and communication remains secure.

Audio streams from the TCC M Plus are stopped, as soon as the device is disconnected from the Q-SYS core via the device's web interface. This ensures that no audio stream remains active without being actively managed.

The PartnerLink configuration can be deactivated or set back by switching the TCC M Plus to the Default (Dante®) mode. This removes all connectivity to the Qsys system.

PartnerLink is built as a scalable framework for future partner platform integrations.

### 3rd-Party control modules

Beyond stand-alone operation, the TeamConnect Ceiling M Plus can serve as the gateway to a highly integrated meeting room. Compatibility with various 3rd party modules enables flexible customization and expanded functionality, allowing the TeamConnect Ceiling M Plus to integrate seamlessly with existing systems and software.

For more details, please visit the webiste 3rd Party API for Sennheiser devices and explore the 3rd party integration modules for TCC M Plus.

### Network modes

All Sennheiser products support multiple network ports for network isolation. Sennheiser TeamConnect Ceiling M Plus comes with two RJ-45 sockets, which can be configured via Sennheiser Control Cockpit for the following network modes:

- Single cable mode: control and AoIP routing as well as PoE on the same port. If your network switch supports PoE+ you can allow up to three units of TCC M Plus to be daisy chained in an installation with a single cable run.
- Split mode: this option allows to split the operation, with PoE control on one port and AoIP on the other.

### List of interfaces

The Sennheiser TeamConnect Ceiling M Plus provides the following interfaces and network protocols to ensure seamless connectivity and communication:

- Ethernet, used for:
    - Control Data: For control and monitoring, a REST/HTTPS API is used.
    - Dante®: Audio over IP solution, allowing transmission of multiple audio channels over Ethernet and replacing traditional analog audio distribution.
    - PartnerLink Audio Streaming: Transmission of audio channels over Ethernet, utilized when the device is configured in PartnerLink mode.
- Analog Audio Output, allowing a balanced analog audio out for legacy or non-networked systems.

# Cybersecurity features

Built-in security features protect TCC M Plus devices, data, and communications across network, firmware, access control, and privacy aspects.

## Encryption and authentication

To meet the increasing demand for security in AV and IT projects, Sennheiser developed the secure Sennheiser Sound Control Protocol (SSCv2). Among other security features, this protocol defines a REST API that allows the user to control the device using an end-to-end encrypted connection via TLS1.2 / TLS1.3 (HTTPS). In addition to encryption, SSCv2 also provides an authentication scheme. By using HTTP basic authentication, a compatible and well-established mechanism of username and password is employed to ensure that no unauthorized changes are made to the device's settings and that no data is read from it. The SSCv2 protocol is used for local on-premises connections to the TeamConnect Ceiling M Plus to allow for secure configuration of the device.

The communication between the TeamConnect Ceiling M Plus and the Sennheiser DeviceHub cloud-based monitoring device management tool uses MQTT network protocols over HTTPS. The communication is authenticated and encrypted using TLS 1.2 and above. Devices must be enrolled to Sennheiser DeviceHub, using an enrollment code for device authentication.

The TeamConnect Ceiling M Plus supports Dante® Media Encryption, allowing to safeguard media from interception or unauthorized access. The feature protects the content of media flows using AES-256 encryption. Visit the Dante® documentation for more on how to configure and use it.

## Password protection

Sennheiser implements authentication methods on devices and software, to ensure that only authenticated users can access the devices on the network.

- The TeamConnect Ceiling M Plus device is protected with a strong password and requires authentication in the form of claiming on the device's local web UI before use. When the device is used for the first time with the local web UI, the default password must be changed before allowing configuration or monitoring.
- Sennheiser DeviceHub is protected by its own dedicated user authentication mechanisms and requires separate credentials, independent of the device password.
- 3rd party integrations are disabled by default. They must be explicitly enabled and authorized by the user and require authentication using credentials defined within the respective 3rd party module.
- Audio streams shared via Sennheiser PartnerLink are authenticated by a password exchange between the TeamConnect Ceiling M Plus and the partner device.

### Firmware updates

The TeamConnect Ceiling M Plus can be updated, ensuring that future vulnerabilities are resolved by providing security patches. The devices implement a secure firmware update, ensuring that only authorized firmware is installed and protecting against malicious tampering.

### Brute force prevention

To safeguard against brute force attacks, the device implements a brute force prevention mechanism designed to limit unauthorized access attempts. This includes blocking IP addresses after repeated access attempts with invalid credentials.

### Factory State Mute

The device is muted in the factory default state, to ensure it cannot be operated unsecure in the network.

### Protect personal data

The TeamConnect Ceiling M Plus does not store any personal data, ensuring that your privacy is protected.

Sennheiser DeviceHub stores only the required personal data for sign up and logging in. No audio or video data is ever sent from a Sennheiser device to Sennheiser DeviceHub. Only control information is transmitted to the cloud, namely device configuration and monitoring status. All Sennheiser DeviceHub private data processing is carried out in compliance with GDPR. For more information, please see the Sennheiser DeviceHub Privacy Policy.

# 4. List of network ports

This table lists the network ports required for device operation, depending on the selected operating mode and configuration.

The following tables provide an overview of the network ports and services used by the TeamConnect Ceiling M Plus for local device management, cloud connectivity, audio networking, and integration with third-party platforms. Depending on the selected operating mode and enabled features, additional ports may be required.

### Inbound Connections

| Port | Protocol | Interface | Purpose |
|---|---|---|---|
| 80 | TCP | Control | HTTP redirect to HTTPS |
| 443 | TCP | Control | Local Web UI, SSCv2 API, device management, audio routing and control |
| 5353 | UDP | Control/AoIP | mDNS device discovery |

### Inbound Connections

| Port | Protocol | Interface | Purpose |
|---|---|---|---|
| 53 | UDP | Control/AoIP | DNS name resolution |
| 67 | UDP | Control/AoIP | Automatic IP configuration (DHCP) |
| 123 | UDP | Control | NTP time synchronization |
| 443 | TCP | Control | Firmware updates, cloud communication, certificate validation and secure device management |

### Dante®

If Default Operating Mode with Dante® is enabled, additional TCP and UDP ports are required for audio transport, clock synchronization, device discovery, and Dante® management services.

Refer to the Audinate Dante® documentation for the complete and current list of required ports and protocols.

### PartnerLink (Q-SYS Mode)

The following ports are only required when the device is operated in Q-SYS Mode (PartnerLink enabled).

**Required Outbound Connections**

| Port | Protocol | Interface | Purpose |
|---|---|---|---|
| 2467 | UDP | Control | Device Discovery |
| 5004 | UDP | AoIP | PartnerLink Audio Streaming |
| 31920 | UDP | AoIP | PTP |

# 5. Security recommendations

Follow these recommendations to ensure the security of your devices.

## Limit attack surfaces

It is good practice to limit the possible attack surfaces of a device to the absolute minimum needed to fulfill the requirements of the use case. To support this Sennheiser allows the configuration of:

- Cloud connection to Sennheiser DeviceHub - disabled by default
- 3rd party access - disabled by default
- mDNS - enabled by default

Additionally, the user can opt out of using audio over IP (Dante®) by connecting the TeamConnect Ceiling M Plus analog audio outputs instead.

## Keep software up to date

Sennheiser releases firmware updates for security issues in a timely manner. Users of TeamConnect Ceiling M Plus should keep their devices updated to the latest version. Users can manually trigger the device update via the local web UI or DeviceHub at their convenience. In addition, DeviceHub will notify automatically once a new firmware update is available.

Please always keep your systems up to date.

## Use strong passwords

To protect control access over the network, you must choose a strong password with at least 10 characters that includes at least one of each of the following:

- lowercase letter: a, b, c, ..., x, y, z
- uppercase letter: A, B, C, ..., X, Y, Z
- digit: 0, ..., 9
- at least one special character that is present on a standard US-layout keyboard: !#$ %&()*+,-./:;<=>?@[]^_{|}~

To protect each individual user installation, whenever a TeamConnect Ceiling M Plus is controlled over the network, the passwords used are chosen by the user.

It is recommended to use a unique password for each device, as well as separate passwords for access to 3rd party API.

# 6. Compliance

The TeamConnect Ceiling M Plus complies with the following security standards and regulations:

- California SB 327: Security of connected devices
- PSTI: UK Product Security and Telecommunications Infrastructure

# 7. Conclusion

**The TCC M Plus is a comprehensive video conferencing solution with high-quality audio, video, and advanced security.**

In conclusion, the TeamConnect Ceiling M Plus is a comprehensive solution for your audio conferencing needs, delivering exceptional speech intelligibility, advanced features, and robust security. Whether you are a small business or a large enterprise, the TeamConnect Ceiling M Plus can enhance your communication and collaboration, making your meetings more productive and efficient. For more information about the TeamConnect Ceiling M Plus, visit the website: sennheiser.com/tccmplus.

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