TeamConnect Ceiling Medium

Security white paper

Contents

1. Introduction

This white paper aims to provide IT professionals with an in-depth understanding of the TCC M, 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 Medium microphone - a cutting-edge solution designed to deliver exceptional audio clarity while maintaining robust security standards. This whitepaper provides IT professionals with an understanding of the TeamConnect Ceiling microphone, its architecture, and the security mechanisms that safeguard your communication environment.

2. Security 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 security features

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

Product components in a nutshell

TeamConnect Ceiling Medium 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 Medium can be configured via the Sennheiser Control Cockpit software. It is an on-premises centralized management software that allows you to configure and monitor the settings of your device. For more, please visit the product documentation.

3rd-Party control modules

Beyond stand-alone operation, the TeamConnect Ceiling Medium 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 Medium 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.

Network modes

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

- Single cable mode: control and Dante® flow as well as PoE on the same port. If your network switch supports PoE+ you can allow up to three units of Team Connect Ceiling Medium 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 Dante® on the other.

List of interfaces

The Sennheiser TeamConnect Ceiling Medium 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.
- Analog Audio Output, allowing a balanced analog audio out for legacy or non-networked systems.

4. List of network ports

This table lists the network ports, protocols, and services required for device communication, discovery, and control.

Port	Protocol	Service	Product
53	UDP	DNS	Translates domain names to IP addresses.
68	UDP	DHCP	Automatically assigns IP addresses to devices.
443	TCP	SSC Sound Control Protocol v2 (SSCv2)	Sennheiser Sound Control Protocol v2 is an HTTPS-based protocol used for control communication between the control application (Sennheiser Control Cockpit or 3rd Party Access) and the device.
443	TCP	Update	Used for updating the device firmware.
5353	UDP	mDNS (Multicast 224.0.0.251)	mDNS (Multicast 224.0.0.251) is used by Sennheiser Control Cockpit to discover devices. You can disable this port in the Control Cockpit web interface and add devices manually instead.
28800, 28700-28708, 38800, 38700-38708, 14336-15359, 34336-34600, 4440, 4444, 4455, 24440, 24441, 24444, 24455, 4777, 8850, 28900, 24445, 8850, 38900, 8899, 8000, 8001, 8002, 8029, 8751, 8800, 61440-61951, 123, 8702, 69, 6969, 9005, 67, 6700	UDP	Dante®	These ports may be open, depending on your Dante® configuration. For more information about Dante® ports, please refer to the Audinate website.
4777, 8028, 8753, 4778, 443, 80, 8001, 8443, 8081, 27017	TCP	Dante®	These ports may be open, depending on your Dante® configuration. For more information about Dante® ports, please refer to the Audinate website.
4321, 5004, 319, 320, 5353, 8700-8708, 9998, 9875	TCP/ UDP	Dante®	These ports may be open, depending on your Dante® configuration.

Port	Protocol	Service	Product
			For more information about Dante® ports, please refer to the Audinate website.
n/a	ICMP	Ping	Error messages and operational information.

5. Security features

Built-in security features protect TCC M 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 Medium to allow for secure configuration of the device.

The TeamConnect Ceiling Medium supports **Dante Media Encryption**, allowing to safeguard media from interception or unauthorized access. The feature is available since firmware version 1.1.1. and 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 Medium device is protected with a strong password and requires authentication in the form of claiming of the device in Control Cockpit before use. When the device is used for the first time with the Sennheiser Control Cockpit, the default password must be changed before allowing configuration or monitoring. The device is muted in the factory default state, to ensure it cannot be operated unsecure in the network.

- Sennheiser control software Control Cockpit user interface, which can be accessed on the network, is password protected by default.
- 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.

IEEE 802.1x

Sennheiser TeamConnect Ceiling Medium supports IEEE 802.1X, a port-based network access control mechanism that ensures devices obtain network access only after successful authentication. This mitigates unauthorized network use during installation and daily operation. TeamConnect Ceiling Medium implements 802.1X as a supplicant and can be onboarded into secured networks that enforce identity-based access. IEEE 802.1X can be configured via SSH and supports two authentication methods: EAP-TLS and EPA-PEAPv0/ EAP-MSCHAPv2. For further information on configuration of 802.1X, please refer to TCC 802.1X Config Guide.

Firmware updates

The TeamConnect Ceiling Medium 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.

Physical security

To reduce the risk of theft, tampering, or accidental damage to the TeamConnect Ceiling Medium, the device's mounting kit comes with secure mechanical fixation points and a safety ceiling fastener, which can be screwed to a suitable anchor.

Protect personal data

The TeamConnect Ceiling Medium does not store any personal data, ensuring that your privacy is protected. The Sennheiser Control Cockpit software does not store any personal data.

6. Security recommendations

Follow these recommendations to enhance 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:

- 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 Medium analog audio outputs instead.

Keep software up to date

Sennheiser releases firmware updates for security issues in a timely manner. Users of TeamConnect Ceiling Medium should keep their devices updated to the latest version. Control Cockpit is checking daily for new updates. The user can then update the device at their convenience.

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 Medium 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.

7. Conclusion

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

In conclusion, the TeamConnect Ceiling Medium 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 Medium can enhance your communication and collaboration, making your meetings more productive and efficient. For more information about the TeamConnect Ceiling Medium, visit the website: sennheiser.com/teamconnect-ceiling-medium.

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