TeamConnect Bar

Security White Paper

Sennheiser electronic SE & Co. KG

Am Labor 1, 30900 Wedemark, Germany, www.sennheiser.com

v1.2

SENNHEISER

Contents

Introduction

In the rapidly evolving digital landscape, cybersecurity has become a paramount concern for businesses worldwide. As video conferencing becomes increasingly integral to our professional lives, the need for secure, reliable, and high-quality communication tools is more pressing than ever.

Sennheiser, a renowned name in the audio industry, has stepped into this domain with the TeamConnect Bar, a state-of-the-art video meeting bar. Designed with advanced features, user-friendly interface, and robust security measures, the TC Bar is set to redefine the video conferencing experience.

This white paper aims to provide IT professionals with an in-depth understanding of the TC Bar, its components, and its security features. Join us as we explore how the TC Bar, a product of Sennheiser's commitment to excellence and innovation, is shaping the future of secure video conferencing.

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 requirements and security standards, and oversees 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 secure Software Development Life Cycle (SDLC) and information security.
- We perform internal and external security evaluations and testing, and continuously work to identify potential vulnerabilities while offering security patches as early as possible to our customers.
- We have a vulnerability handling process (link) to act promptly on vulnerabilities in our products.
- We follow best practices and comply with relevant security standards and regulations:
  - ETSI EN 303 645: Cyber Security for IoT devices
  - EU Radio Equipment Directive (RED)
  - EU CEN/Cenelec EN 18031
  - PSTI: UK Product Security and Telecommunications Infrastructure
  - California SB 327: Security of connected devices

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

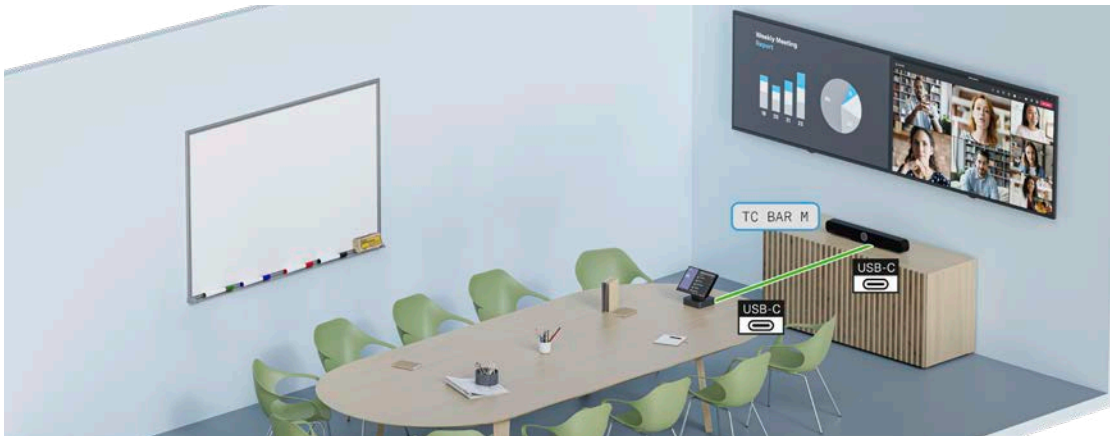
Product overview and security features

Product components in a nutshell

The TeamConnect Bar Solutions are scalable, all-in-one conferencing devices, designed to meet modern meeting demands with built-in camera, microphones and speakers.

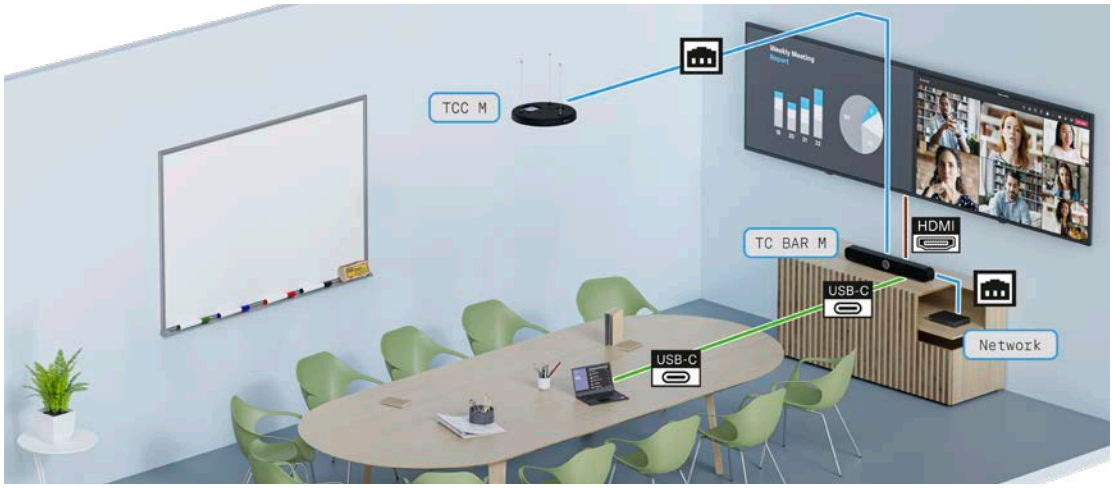
The TC Bar can be operated either as a stand-alone conference system at the workplace or as a networked conference system in a meeting room.

Stand-alone solution



The TC Bar is connected via USB-C® directly to a notebook or or via other UVC- and UAC-capable USB host devices. There is no need for a network connection. In this mode, only restricted functions are available.

Network solution



The TC Bar can be connected to an existing network infrastructure and controlled remotely by the Sennheiser or 3rd party control software.

Sennheiser Control Cockpit

The Sennheiser Control Cockpit is a centralized management software that allows you to control and monitor the settings of the TC Bar, ensuring optimal performance. The Control Cockpit provides you with complete control over your video conferencing experience. For more, please visit the product page: Sennheiser Control Cockpit

3rd-Party control modules

Expanding possibilities the TC Bar is not just a stand-alone device; it's a gateway to a highly integrated meeting room. With its compatibility with various 3rd party modules, you can customize and enhance its functionality according to your needs. This feature allows you to integrate the TC Bar with your existing systems and software, providing a seamless and efficient video conferencing solution.

For more details, please visit the website sennheiser/tc-bar-m or sennheiser/tc-bar-s and explore the 3rd party integration modules under **Downloads ▸ 3rd Party Integration**.

List of interfaces

The TC Bar supports a variety of interfaces and network protocols to ensure seamless connectivity and communication. These include:

- Ethernet: the interface is used for:
  - Control data: For control and monitoring the TC Bar, a REST/HTTPS API can be used
  - Dante®: Audio over IP solution, allowing transmission of multiple audio channels over Ethernet and replacing traditional analog audio distribution
  - PoE: Power over Ethernet
  - The TC Bar products support different network modes, allowing separating the control and Dante® data. For more, please refer to the user manual.
- HDMI®: For high-definition video and audio output
- USB: The video bar is a peripheral and an USB hub
  - USB devices plugged into the TC Bar are usable by the connected client PC
- Bluetooth®: The video bar can be paired via Bluetooth® and supports the following profiles:
  - A2DP (Advanced Audio Distribution Profile)
  - HFP (Handsfree Profile)
  - AVRCP (Audio Video Remote Control Profile)
- IR Control: An infrared remote control allows to control a subset of commands (muting, volume, Bluetooth®, camera) when being in line of sight. The IR control system is not tied to a specific TC Bar, providing flexibility and adaptability across multiple setups.

List of network ports

Port	Protocol	Service	Details
53	UDP	DNS	Translates domain names to IP addresses
68	UDP	DHCP	Automatically assigns IP addresses
443	TCP	SSCv2	Sennheiser Sound Control Protocol v2 is a HTTPS based protocol, used for the control communication between the control software (Sennheiser Control Cockpit) or 3rd party integration) and the device
443	TCP	Update	Used for updating the device firmware
5353	UDP	mDNS	mDNS (Multicast 224.0.0.251) is used for discovery of the device by the Sennheiser Control Cockpit. This port can be disabled, using the Control Cockpit web interface and devices can be added manually instead
4321, 5004, 319, 320, 5353, 9998, 9875, 5000,4440,4444, 4455, 4777, 8000:8899, 28700, 28800, 38700, 38800, 14336:14591	UDP	Dante®	For more information about Dante® ports, please refer to the Audinate website.
5000, 4777, 8753, 16100:16131, 4778	TCP	Dante®	For more information about Dante® ports, please refer to the Audinate website.
n/a	ICMP	Ping	Error messages and operational information

Security features

Encryption and authentication

To meet the increasing demand for security in AV and IT projects, Sennheiser developed the secure Sennheiser Sound Control Protocol (SSCv2). It is an encrypted REST API allowing the user to control the device using HTTPS commands and to integrate products in every IT environment. It offers end-to-end security, utilizing HTTPS (TLS 1.3).

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.

Password protection

Sennheiser implements authenticated methods on our devices and software, to ensure that only authenticated users can access the devices on the network and devices are secured end-to-end.

Security features:

- The Sennheiser Control Cockpit user interface, which can be accessed on the network, is password protected by default.
- The TC Bar device has a strong unique default password in the factory default state, which is printed on the device label. 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.
- 3rd party integrations are disabled by default. They must be explicitly enabled and authorized by the user and authenticated in the 3rd party module with a 3rd party password.

Firmware updates

The TC Bars 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.

Advanced networking options

The TC Bars support different network modes and in the case of the TC Bar M, multiple network ports to allow IT and AV professionals to utilize network isolation. In complex customer networks, the Sennheiser device can be connected to separate networks, isolating control from media communication.

Physical security

The TC Bar is designed with physical security features, this includes a lens cap to protect the camera when not in use, and a Kensington lock slot to secure the device against theft.

Protect personal data

The TC Bar is designed with privacy in mind. It does not store any personal data, ensuring that your privacy is protected. Similarly, the Sennheiser Control Cockpit software does not store any personal data.

Security recommendations

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 several TC Bar features:

- The following interfaces and protocols are configurable and disabled by default:
  - Bluetooth®

  - Dante®
  - 3rd party access
- The following interfaces and protocols are configurable and enabled by default:
  - IR remote control
  - mDNS
  - HDMI®

Recommendations for stand-alone (USB) setup

To facilitate secure connections and interactions with the bar using only USB, the TC Bar includes a unique 12-character initial password for its control interface. This secures the control access in case the device is accidentally connected to a network, while a pure USB setup is intended.

- If you are using a room PC (e.g. Microsoft Teams Room/MTR) you should configure it to apply updates to the TC Bar using the regular Windows Update process. The update will be carried out automatically and silently through the connected USB link without any user interaction. This process will not use Ethernet, as is done with SCC.
- If you are setting up an BYOD setup, where users connect their own devices to the TC Bar for the meeting, you should plan a regular schedule to apply updates to the TC Bar to ensure an optimal security level.

Recommendations for network setup

In case the TC Bar is connected to a network, make sure to change the default device password. To do so, simply install the Sennheiser Control Cockpit software, connect to the same network the TC Bar is connected to, discover the device and claim it. During the claiming process, you will be guided to change the device password.

In addition, you can use Control Cockpit to enable or disable interfaces and protocols as well as configure your device's network settings.

Keep software up to date

Sennheiser is releasing firmware updates for security issues in a timely manner. Users of TC Bars should keep their devices updated to the latest version. Control Cockpit is checking daily for new updates and is informing the user once an update is found. The user can then update the device whenever there is some downtime. Please always keep your systems up to date.

Use strong passwords

To protect control access to the network, the user must choose a strong password of at least 10 characters and containing at least one of:

- 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, there are no generic passwords. Whenever a TC Bar is controlled over the network, the passwords used are chosen by the user.

Conclusion

In conclusion, the TC Bar is a comprehensive solution for your video conferencing needs, providing high-quality video and audio, advanced features, and robust security. Whether you are a small business or a large corporation, the TC Bar can enhance your communication and collaboration, making your meetings more productive and efficient.

For more information about the TC Bar, visit the product page.