TeamConnect Bar

Security white paper

Contents

1. Introduction

This white paper aims to provide IT professionals with an in-depth understanding of the TC Bar, its components, and its security features.

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.

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. For more product specific details, please see Compliance.

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

3. Product overview and security features

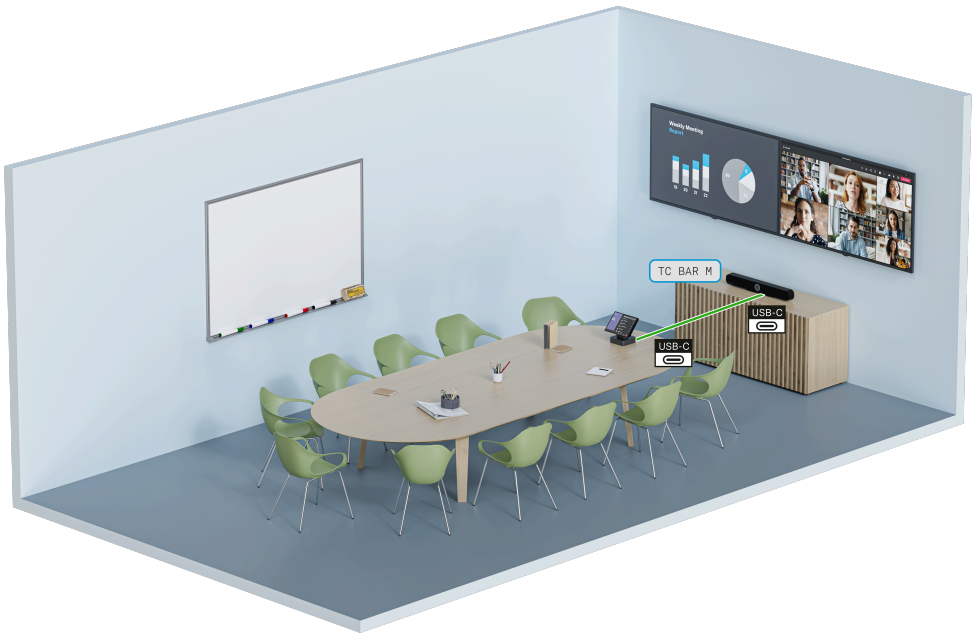
TC Bar offers flexible conferencing solutions with multiple operating modes, control options, and interfaces.

Product components in a nutshell

TeamConnect Bar Solutions are scalable, all-in-one conferencing devices designed to meet modern meeting requirements, with an integrated camera, microphones, and speakers. They can be used as stand-alone systems or deployed as networked conferencing solutions in meeting rooms.

Stand-alone solution

The TC Bar is connected via USB-C® directly to a notebook or via other UVC- and UAC-capable USB host devices. A network connection is not required. In this mode, only limited functions are available.

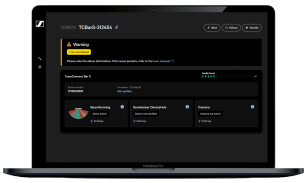
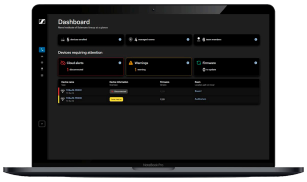
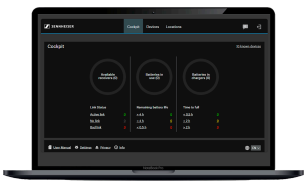


Network solution

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

Sennheiser control software

The TC Bar can be configured via various software tools, namely:

Application	Description
Local Web UI (LUI) 	LUI is a browser-based interface for easy and quick device configuration in the local network and is accessible over the device IP address or host name. LUI is available as of firmware version 2.0.0. • Online manual: Local Web UI
DeviceHub 	Cloud-based platform for managing and monitoring Sennheiser AV devices across locations. DeviceHub compatibility is available as of firmware version 2.0.0. • Online manual: DeviceHub • Product info: sennheiser.com/devicehub • Software: https://devicehub.sennheiser.com
Control Cockpit 	On-premise centralized management software that allows you to configure your TC Bar. • Online manual: Control Cockpit • Product info: sennheiser.com/control-cockpit

3rd Party control modules

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

For more details, visit the website sennheiser.com/tc-bar-m or sennheiser.com/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:

- Gigabit Ethernet: the interface is used for:
    - Control data: For control and monitoring of the TC Bar, a REST API over HTTPS is used on-premises and MQTT API over HTTPS is used for cloud monitoring and configuration, if enabled.
    - Dante®: Audio over IP solution, allowing transmission of multiple audio channels over Ethernet and replacing traditional analog audio distribution.
    - The TC Bar products support different network modes, allowing separating the control and Dante® data. For more details, please refer to the user manual.
- HDMI®: For high-definition video and audio output.
- USB 3.1 Gen 1: The video bar is a peripheral and a 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.

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.
80	TCP	HTTP	Purely used for securely redirecting communication to port 443.
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.
443	TCP	MQTT	HTTPS based protocol, used for the control communication between the control software (Sennheiser DeviceHub) and the device.
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®	For more information about Dante® ports, please refer to the Audinate website.

Port	Protocol	Service	Product
4777, 8028, 8753, 4778, 443, 80, 8001, 8443, 8081, 27017	TCP	Dante®	For more information about Dante® ports, please refer to the Audinate website.
4321, 5004, 319, 320, 5353, 8700-8708, 9998, 9875	TCP/ UDP	Dante®	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 TC Bar 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 secure communication from all Sennheiser Control Software and 3rd party API to the TC Bar.

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

The TC Bar supports Dante Media Encryption, allowing to safeguard media from interception or unauthorized access. The feature is available from firmware version 1.3.8 onwards and protects the content of media flows using AES-256 encryption. Visit the Dante documentation for more information.

Password protection

Sennheiser implements authentication methods on devices and software, to ensure that only authenticated users can access the devices on the network. The TC Bar is delivered with a strong, unique default password in the factory default state. This password is printed on the device label and is required for initial access. When accessing the TC Bar for the first time via the Local Web UI or during claiming of the device in Control Cockpit the default password must be changed before any configuration or monitoring.

- The Local Web UI of the TC Bar device is protected by the current device password and requires authentication for access.
- Sennheiser control software (Control Cockpit and 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.

Firmware updates

The TC Bars can be updated, ensuring that future vulnerabilities are resolved by providing security patches. To guard against malicious tempering, the devices implement a secure firmware update mechanism, ensuring that only authorized firmware signed by Sennheiser can be installed.

From firmware version 1.3.8 onwards, device downgrades are prevented to ensure security.

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.

Secure boot

The TC Bars are designed to start only with verified, trusted firmware, preventing execution of unauthorized code during the boot process.

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 implement network isolation. In complex customer networks, the Sennheiser device can be connected to separate networks, isolating control traffic from media communication.

Physical security and privacy

The TC Bar is designed with physical security features, including a lens cap to protect the camera when it is 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. The device does not store any personal data, helping to ensure that your privacy is protected. The Sennheiser Control Cockpit software also does not store any personal data.

The Sennheiser DeviceHub cloud monitoring tool stores only the personal data required for sign-up and login. 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. All Sennheiser DeviceHub processing of private data is carried out in compliance with GDPR. For more information, please see the Sennheiser DeviceHub privacy policy.

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 several TC Bar features:

- The following interfaces and protocols are configurable and disabled by default:
    - Cloud connection to Sennheiser DeviceHub
    - 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, contrary to all other communication to Sennheiser Control Software.
- 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 connect to the same network the TC Bar is connected to, and access the Local Web UI or Sennheiser Control Cockpit to discover the device and claim it. During the claiming process, you are guided to change the device password.

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

Keep software up to date

Sennheiser releases firmware updates for security issues in a timely manner. Users of TC Bars should keep their devices updated to the latest version. The user can manually trigger the device update in DeviceHub or Control Cockpit 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, there are no generic passwords. Whenever a TC Bar is controlled over the network, the passwords used are always chosen by the user.

7. Compliance

The Sennheiser TC Bars comply with the following security standards and regulations:

- EU Radio Equipment Directive (RED)
- EU CEN/Cenelec EN 18031
- PSTI: UK Product Security and Telecommunications Infrastructure
- California SB 327: Security of connected devices

8. Conclusion

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

The TC Bar is a comprehensive solution for video conferencing, delivering high-quality video and audio, advanced features, and robust security. Whether you are a small business or a large corporation, the TC Bar can improve communication and collaboration, making your meetings more productive and efficient. For more information about the TC Bar, visit the product page sennheiser.com/tc-bar.

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