TeamConnect Bar

Cloud connectivity guide

PDF export of the original HTML instructions

Contents

1. Product information

This document provides AV /IT professionals with step-by-step guidance on enabling cloud connectivity for the TeamConnect Bar (TC Bar) and preparing it for integration with **Sennheiser DeviceHub,** Sennheiser's cloud-based device management platform.

Content

The document covers the following topics for setup of the device and the network configuration to ensure seamless operation with Sennheiser DeviceHub:

- Preparing your network for cloud connectivity
- Installing the firmware
- Known issues and limitations of the beta firmware

Prerequisites

You will need:

- TeamConnect Bar S or M
- Sennheiser Control Cockpit v9.1.2 or higher
- Firmware image with "Local Web UI" (LUI) supporting Sennheiser DeviceHub firmware v2.0.2 or higher
- Network access with mandatory firewall configuration

2. Preparing the TC Bar for cloud connectivity

To enable cloud connectivity for TC Bar devices, ensure the latest firmware is installed and configure the necessary network settings and outbound ports as specified.

For the device to operate in a cloud environment it needs to be updated to the latest firmware version provided for this device (2.0.2 or higher). To update your device to the new firmware via Control Cockpit, follow the steps in the chapter Installing the firmware.

Network modes

This chapter outlines the network communication options for TC Bars S and M, including Single Domain, Dual Domain, and Split Modes, along with guidance for configuration.

The TC Bars S and M provide the option to configure different network modes namely:

- Single Domain Mode: single cable, one network (TC Bar S and M)
- Dual Domain Mode: single cable, two separate networks for control and Dante (for both TC Bar S and M)
- Split Mode: two cables, two separate networks for control and Dante (for TC Bar M)

For a detailed guide on how to select and configure the network modes, please refer to the Network Guide.

To connect any of the TC Bar devices to the cloud, please configure the control network accordingly.

Required outbound ports (DeviceHub)

Sennheiser DeviceHub relies on Microsoft Azure IoT Hub for connections established by the TC Bars.

The following network protocols and ports are required for the Sennheiser cloud connectivity over the TC Bar control network.

IPv4	Port	Protocol	Service / FQDN	Service Tag
52.166.23.94 (EMEA) 104.211.55.78 (AMER) 20.239.51.210 (APAC)	443	HTTPS	Device Enrollment Service **api.cloud.sennheiser.com**	N/A
Dynamic*	443	MQTT over WebSockets	IoT Region **EMEA** **iot-senn heiser-prod-emea.azure-devices.net**	AzureIoTHub.WestEurope
Dynamic*	443	MQTT over WebSockets	IoT Region **APAC** **iot-sennheiser-prod-apac.azure-devices.net**	AzureIoTHub.EastAsia
Dynamic*	443	MQTT over WebSockets	IoT Region **AMER** **iot-sennheiser-prod-amer.azure-devices.net**	AzureIoTHub.EastAsia

All device communication is secured with current TLS/SSL.

*Dynamic IPv4:
The IP addresses of Azure IoT Hubs are dynamic and may change without prior notice.

▶ Use FQDNs (fully qualified domain names) if supported by your firewall or
▶ check the Microsoft Azure Service Tags to retrieve the current IP ranges by searching for the specified Service Tag:
  ▶ Download the complete Service-Tags list from www.microsoft.com/download.
  ▶ In the downloaded `.json` file, search for the Service Tag corresponding to your IoT Hub region. If you are unsure or operating in multiple regions, you may enable all three IoT Hub regions.

Currently, only direct connection (MQTT; port 443) is supported. The connection type "behind HTTPS proxy" is not supported by the TC Bar. The URLs provided are for reference only.

> **ℹ** **Important:** IPv6 connectivity is not yet supported. Devices must use IPv4 for all outbound communication. This is particularly relevant for environments where IPv6 is common, such as mobile networks (e.g., SG). Please ensure your network allows IPv4 traffic for the required ports and domains.

Optional ports (Control Cockpit)

Enable specific firewall ports to perform firmware updates of the TC Bar using Sennheiser Control Cockpit software.

In case you would like to perform a firmware update of the TC Bar using the Sennheiser Control Cockpit software, make sure to enable the following ports in your firewall for the control network.

Optional ports:

Port	Protocol	Service
5353	UDP	Optionally allow mDNS (Multicast 224.0.0.251) to discover devices automatically with Control Cockpit. As an alternative, you can disable mDNS and add devices manually by their IP address.
443	HTTPS	SSC Sound Control Protocol v2 for communication to Control Cockpit/ Firmware Update.

Installing the firmware

Follow these steps to install the firmware for the TC Bar using Sennheiser Control Cockpit on Windows, ensuring to remove any previous firmware versions to avoid conflicts.

> **i**   This step is only required if the device does not yet have cloud-enabled firmware installed. If such a firmware update has already been performed, no further update is necessary.

To install the firmware:

- ▶ Download and install Sennheiser Control Cockpit v9.1.2 or higher under sennheiser.com/control-cockpit (Windows only).
- ▶ In Control Cockpit, navigate to **Device** > **Firmware Info**.
- ▶ Select the firmware v2.0.2 or higher from the drop-down and perform the update.

> ✓   The firmware has been installed successfully.

3. Known Issues

This document outlines known issues and pitfalls related to firmware, time synchronization, third-party access, and provides supportive links for troubleshooting TC Bars.

Supportive links

Sennheiser DeviceHub

- User manual

TC Bar

- TC Bar user manual
- Product information
- Knowledge Base
- Product security at Sennheiser

TC Bar requires an external time source

Condition

The TC Bar requires an external time source after booting.

Cause

The TC Bar requires an external time source. Accurate system time is necessary for proper enrollment and communication with Sennheiser DeviceHub. For persistent time synchronization, use a valid NTP server.

After a factory reset, the device defaults to Manual NTP mode and automatically preloads two predefined time servers.

Mode switching:

- Manual to Auto
  - Server fields are cleared and disabled (Auto uses network-provided time).
- Auto to Manual
  - Default servers are reinserted and fields become editable.

Manual changes:

- Any user-entered servers remain active in Manual mode unless switched to Auto, which clears them.

▶ Enrollment can be performed using the "Use browser time" option in the LUI. The devices does not store time persistently e.g. during a reboot. The system time is saved periodically and restored after reboot, significantly reducing time drift. However, if no valid NTP server or time source is available, the system time will still drift over time after multiple reboots. Larger deviations between system time and actual time may cause enrollment to fail. Therefore, it is important to ensure that a valid NTP server is always configured and reachable.

NTP server is not validated

Condition

The NTP server is not validated and shows an error.

Cause

This is by design: the device accepts any address provided via DHCP or entered manually, without checking its reachability or validity.

▶ If time synchronization issues occur, please verify that the configured NTP server is accessible and delivering a valid time signal.

Third-party access cannot be disabled

Condition

Third-party access cannot be disabled once enabled in the firmware v2.0.x.

Cause

The function is not implemented in the beta firmware version of DeviceHub yet.