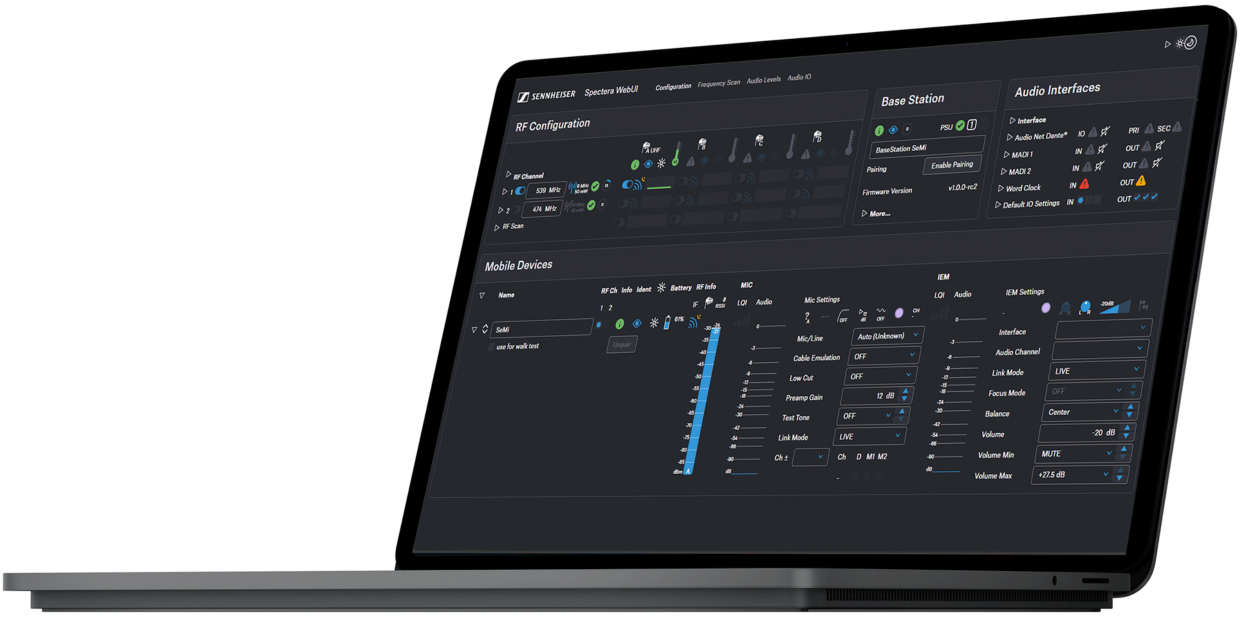


Spectera WebUI

WebUI Control Software

PDF Export of the Original HTML Manual

Contents

1. Preface

PDF Export of the Original HTML Manual

This PDF document is an automatic export of an interactive set of HTML manuals. Some content and interactive elements may not be included in the PDF because they cannot be displayed in this format. In addition, automatically generated page breaks may cause related content to be slightly shifted. We can therefore only guarantee the completeness of the information in the HTML manual and recommend using it. You can find it in the Documentation Portal at www.sennheiser.com/documentation.

2. Product Information

Information about supported devices, design, functionality and the main features of the software at a glance.

Spectera WebUI is a self-hosted, browser-based and user-friendly interface for the dedicated control and monitoring of Spectera devices.

The WebUI offers you an intuitive **Configuration** with essential remote control and monitoring functions, such as IEM volume, latency, audio level and settings, RF status, battery status and much more. The **Frequency Scan** provides a continuous spectrum scan via Spectera's innovative DAD antenna. Plus, the **Audio Levels view** shows all inputs and outputs of the connected interfaces on one page. All audio channels and links are summarized in the **Audio IO** view and can be easily adjusted.

Key Features

- Self-hosted, browser-based and user-friendly interface for the dedicated control and monitoring of Spectera devices.
- Online interface for full system management.
- A tool-tip provides contextual additional information that appears when hovering over an element with the mouse.
- Complete remote control and monitoring of all Spectera ecosystem components, including the Base Station, DAD antenna, and SEK bodypacks, all on a single page.
- Unprecedented remote control and monitoring capabilities, plus visibility of:
    - Interference Level (IF)
    - Receive Signal Strength Indication (RSSI)
    - Link Quality Input (LQI)
    - IEM settings (Interface, CH, Mode, Balance, Volume)
    - MIC settings (Mic/Line, Cable Emulation, Low Cut, Preamp Gain, Test Tone, Mode, CH)
- Continuous spectrum scanning via DAD antenna available.
- Regional license key for activating the Base Station.

3. User Manual

Detailed description of the WebUI navigation and configuration.

> i Please navigate to the desired chapters by clicking on the related information.

Getting Started

Starting the WebUI for the first time, including device authentication and license entitlement.

When adding the Base Station for the first time, three intermediate steps are required:

1. Identifying the Base Station via IP (see **Network**).
2. Authenticating the Base Station using the configured password (see Claiming single device (WebUI)).
3. Activating the Base Station license (see Activating a license (webUI)).

> i If the Base Station IP is used via LinkDesk at the same time, the control buttons in the WebUI are deactivated. In this case, the user can monitor, but can no longer intervene actively.

> i Operational data is collected to continuously improve the stability and functionality of Spectera. The data is pseudonymized to ensure there is no direct personal reference. Tracking can be disabled in the settings (see chapter Enabling/disabling data collection).

Identifying Base Station via IP

In order to add a Base Station, its IP address is required.

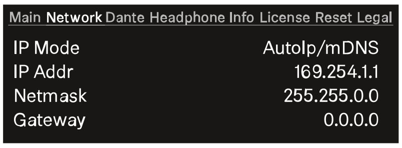
You can read the IP address on the display of the device.

To identify the IP of your Base Station:

▶ On the Base Station, rotate the jog-dial and navigate to the menu **Network**.

▶ Press the jog-dial to enter the menu.

✓ The network data will be displayed.



IP Mode	AutoIp/mDNS
IP Addr	169.254.1.1
Netmask	255.255.0.0
Gateway	0.0.0.0

- Note the displayed IP of your device.

✓ The IP address of your Base Station has been identified.

Claiming single device (WebUI)

Instructions for claiming a single device in Spectera WebUI.

To claim your Base Station:

▶ Depending on the firmware version, enter the following URL into your browser:

- Firmware 0.8.x: `https://deviceIP/specteracontrol/index.html`
- Firmware ≥1.0.0: `https://deviceIP/specterawebui/index.html`

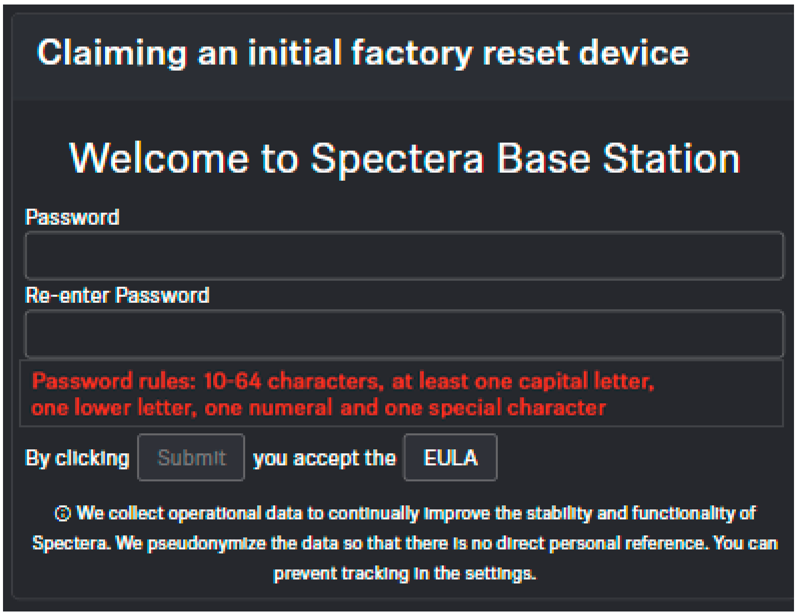
> **i** Since the certificate is unknown to your browser, a security warning is displayed the first time you run the application. The security warning depends on the browser you are using.

▶ Depending on your browser, click on **Advanced** and then on:

- **Continue to localhost (unsafe)** (Microsoft Edge)
- **Proceed to localhost (unsafe)** (Google Chrome)
- **Accept the Risk and Continue** (Firefox)
- or similar (other browsers).

✓ The WebUI displays the following options depending on the state of the device:

If•the device is in a factory default state and the original password is still assigned, it will be automatically detected and applied. Next, a new password has to be set:



Claiming an initial factory reset device

Welcome to Spectera Base Station

Password

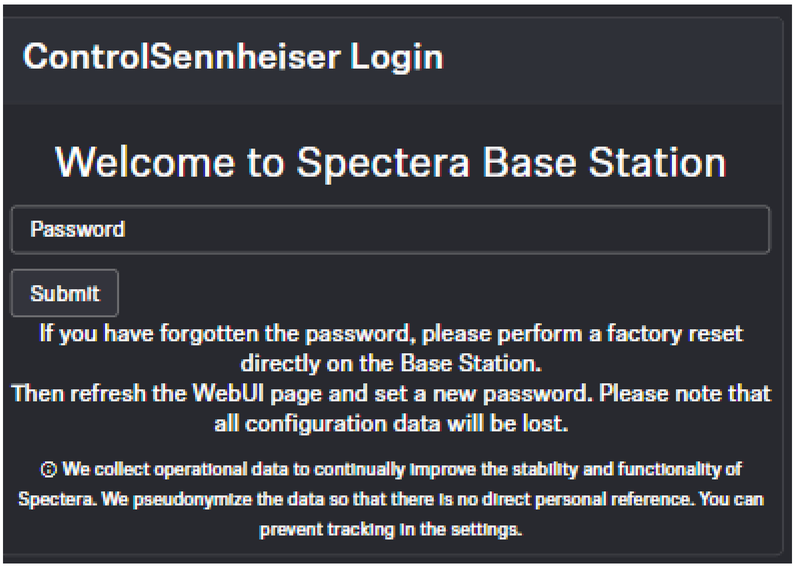
Re-enter Password

Password rules: 10-64 characters, at least one capital letter, one lower letter, one numeral and one special character

By clicking Submit you accept the EULA

ⓘ We collect operational data to continually improve the stability and functionality of Spectera. We pseudonymize the data so that there is no direct personal reference. You can prevent tracking in the settings.

If•the device was previously claimed by another Sennheiser LinkDesk or Spectera WebUI instance, the previously set password must be entered:



ControlSennheiser Login

Welcome to Spectera Base Station

If you have forgotten the password, please perform a factory reset directly on the Base Station.
Then refresh the WebUI page and set a new password. Please note that all configuration data will be lost.

ⓘ We collect operational data to continually improve the stability and functionality of Spectera. We pseudonymize the data so that there is no direct personal reference. You can prevent tracking in the settings.

i If you cannot remember the previously set password, please perform a factory reset of the device. After the reset, the default password for Spectera will be automatically applied by the software.

▶ Set a new device password (if you are logging in for the first time) or enter the password you have already assigned for authentication (if you have already logged in).

▶ Click on **Submit**.

✓ Your Base Station has been claimed successfully.

Activating a license (webUI)

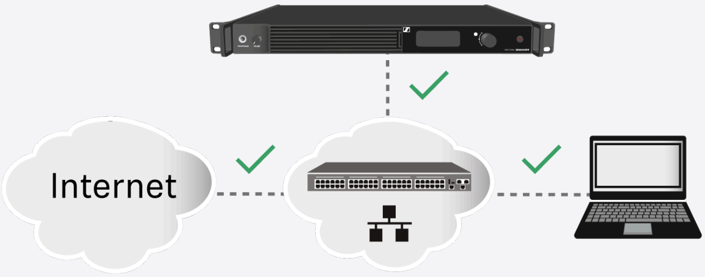
Under Entitlement, you can enter and activate the current license for the frequency spectrum.

i The purchased license (included in the product) is only valid for the region for which the product was designed and approved. The license may not be used in other regions.

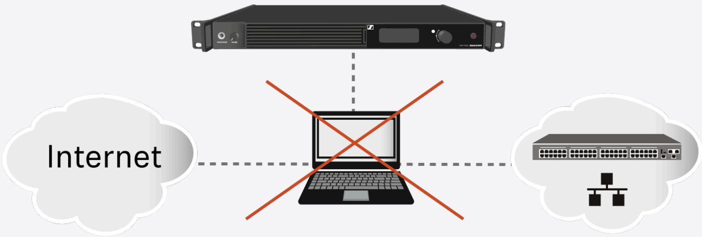
NOTICE

License activation requires a direct Internet connection to the device

In order to activate the Base Station using the 18-digit license code, a direct Internet connection is required.

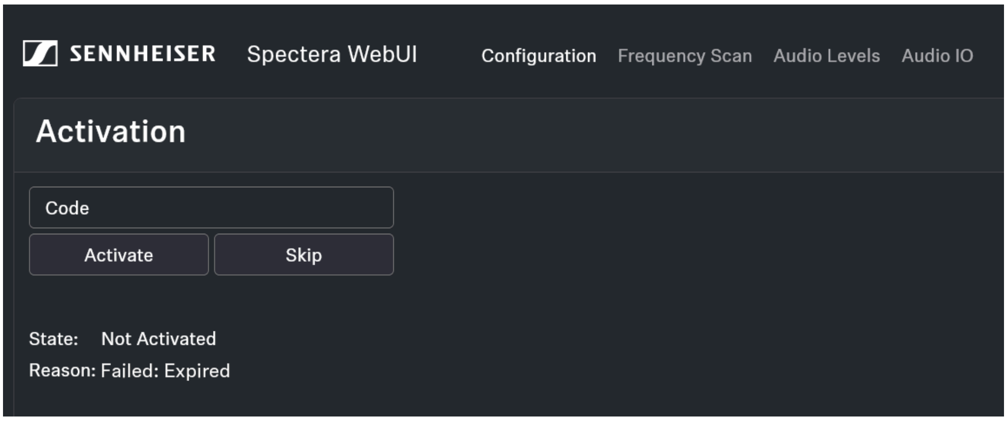


- ▶ Please connect your Base Station directly to a network with Internet access via a switch or router. For more information, refer to the chapter Connecting to a network.
- ▶ Direct connections via laptop etc. are not supported for activation!



- ▶ The Internet is only required once for activation.

When you start the device for the first time, your license key is requested.



State: Not Activated

Reason: Failed: Expired

To activate the license:

▶ Enter the acquired license and click on **Activate** or on **Skip** to proceed with activation later.

✓ Your license has been activated.

Resetting the device password

You can reset the assigned device password on your Base Station to its factory settings.

> i To change or reset the device password, the device must be reset to factory settings.

> **NOTICE**
>
> ⚠ **Data loss during the factory reset**
>
> All audio devices will be unpaired and all audio routes will be deleted.
>
> All settings (including the device password) are reset to the default values. The license remains activated.
>
> After the reset, the device is restarted automatically.
>
> ▶ Do not reset the Base Station during an active live audio transmission.

To reset the password to factory settings, you have two options available:

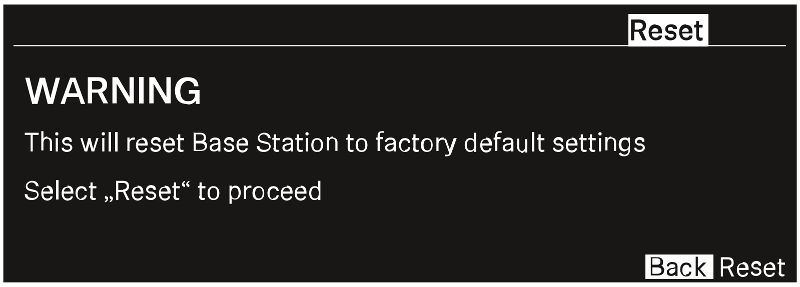
- Reset via the device (see below)
- Reset via the WebUI interface (see Resetting the Base Station)

To reset the Base Station to its factory default settings using the device:

▶ On the Base Station, rotate the jog-dial and navigate to the menu **Reset**.

▶ Press the jog-dial to enter the menu.

✓ A warning will appear.



WARNING

This will reset Base Station to factory default settings

Select „Reset“ to proceed

▶ Rotate the jog-dial to **Reset**.

▶ Press the jog-dial again.

✓ The Base Station will be set back to factory settings and reboot.

> i After rebooting, check the IP address as it may have changed.

✓ The Base Station has been reset to its factory default settings.

Basic configuration

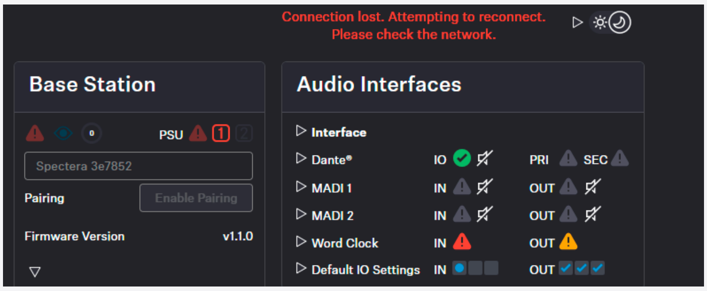
Start your basic configuration with the recommended steps.

> i If the Base Station IP is used via LinkDesk at the same time, the control buttons in the WebUI are deactivated. In this case, the user can monitor, but can no longer intervene actively.

When setting up the WebUI for the first time, we recommend following these first steps to successfully configure the system from the outset:

- Activating a license (webUI)
- Enabling/disabling data collection
- Scanning the RF frequency
- Configuring RF channels
- Assigning an antenna to an RF channel
- Pairing/unpairing mobile devices
- Selecting audio link mode (IEM)
- Selecting audio link mode (Mic/Line)
- Assigning an RF channel
- Selecting the Mic/Line input

> i If the connection to the device is lost (no power supply or no network connection), the live status will be displayed based on an error message.



Connection lost. Attempting to reconnect.
Please check the network.

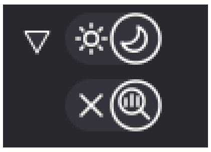
Enabling/disabling data collection

Spectera collects operational data to enhance stability and functionality.

The data is pseudonymized to ensure there is no direct personal reference.

To enable/disable data collection:

- ▶ On the start page, navigate to the top navigation at the top right.
- ▶ Click on the triangle to expand the settings.



- Click on:
  - the X to stop data collection
  - the magnifying glass to enable data collection.

✓ Data collection has been enabled/disabled.

Scanning the RF frequency

You can run a frequency scan to check the current frequency situation in your surrounding area.

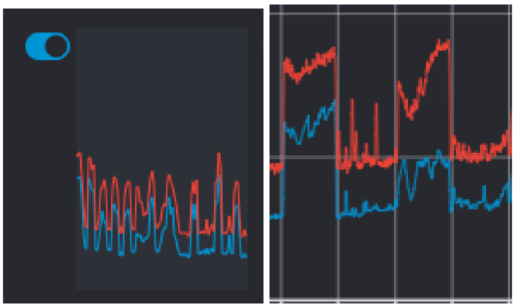
The frequency scan provides an overview of the frequency situation in your location. You can save the antenna configuration as a .csv info file. This file can be used as a backup file to recapitulate your settings or as local frequency information for your specific environment. You can scan the frequencies of all antennas connected to the Base Station.

The scan can be initiated:

- via the RF configuration tab to see a small extract without any details or
- via the Frequency Scan tab for a detailed overview of the frequency situation.

The scan results will be displayed in two different curves:

- **Peak** (red) = Maximum value
- **RMS** (blue) = Average power or strength

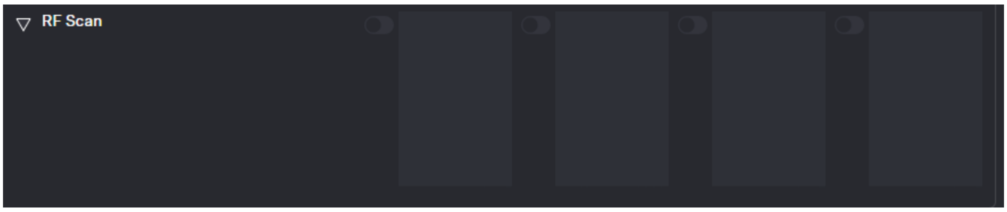


i Please note that the antenna must not be assigned to an RF channel before scanning (see Assigning an antenna to an RF channel).

To scan the RF frequency via the RF configuration tab:

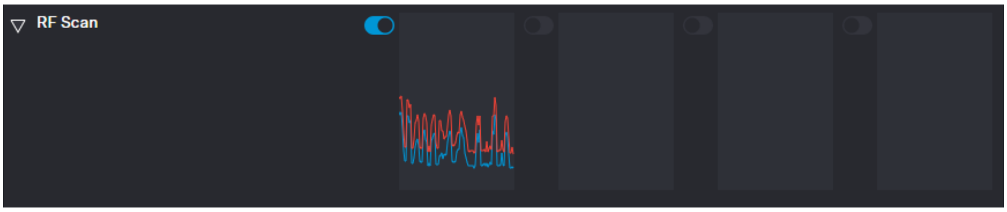
▶ In the top bar, navigate to **Configuration** > **RF Configuration**.

✓ Under the **RF Scan** drop-down menu, there are four toggle switches that enable and disable the scan function for each connected antenna.



▶ Click on the toggle switch of the antenna to be scanned in order to start an immediate scan.

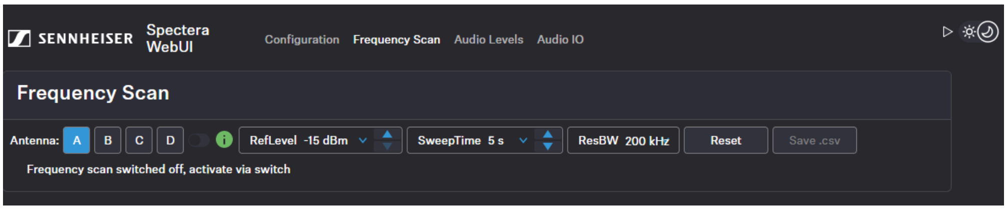
✓ The square is highlighted with a blue dot and the scan result is displayed in a small frequency curve after approx. 5 seconds.



- In order to view the results,
  - click on the small frequency icon or
  - navigate to **Frequency Scan** in the top bar.

To scan the RF frequency via the Frequency Scan tab:

- In the top bar, navigate to the tab **Frequency Scan**.



RefLevel -15 dBm

SweepTime 5 s

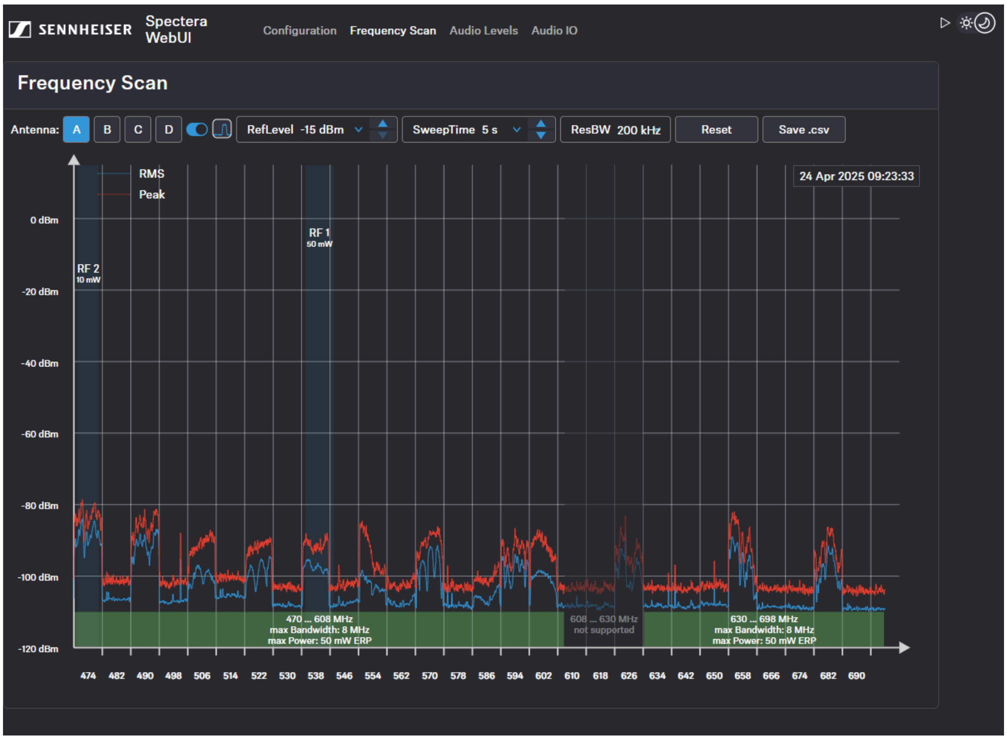
ResBW 200 kHz

Frequency scan switched off, activate via switch

- Select your antenna to be scanned and adjust your desired settings.

- Switch on the toggle to start the scan.

✓ The frequency scan is started and the result is displayed in a detailed frequency diagram. Supported frequency ranges are shown in green and unsupported ranges in gray.



Frequency Scan

Antenna: A

RefLevel -15 dBm

SweepTime 5 s

ResBW 200 kHz

24 Apr 2025 09:23:33

To reset a scan:

▶ Click on **Reset**.

✓ The current scan will be reset.

To save the scan results as `.csv`:

▶ Click on **Save.csv**.

✓ The antenna configuration has been downloaded locally to your computer as a `.csv` file.

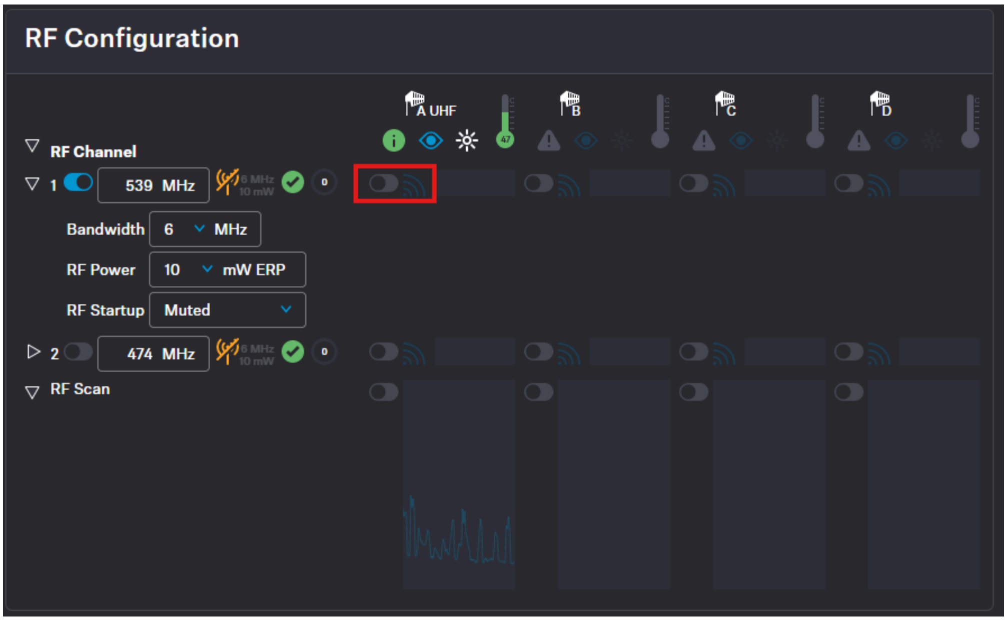
✓ The frequency of your connected antenna has been scanned.

Assigning an antenna to an RF channel

You can choose between up to four connected antennas to assign them to your two possible RF channels.

> i For additional reliability in terms of redundancy or to extend your range, you can assign up to four antennas per channel and use them simultaneously.

The antennas can be assigned and unassigned, e.g. to perform an RF scan or to switch between the configured RF channels.



RF Configuration

RF Channel

1 539 MHz

Bandwidth 6 MHz

RF Power 10 mW ERP

RF Startup Muted

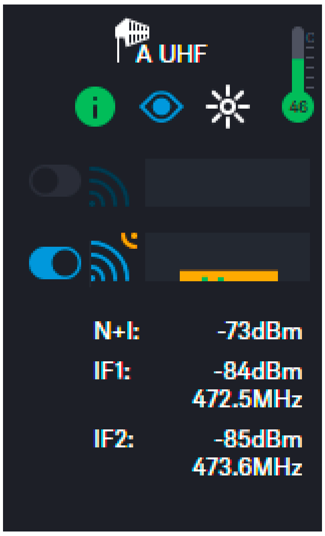
2 474 MHz

RF Scan

To assign an antenna for an RF channel:

- In the top bar, navigate to **Configuration** > **RF Configuration**.
- In your RF channel row, click on the toggle switch next to the utilization and interference icon .

✓ The toggle switch turns blue . The antenna has been assigned to the RF channel and any potential interference is indicated by the icon.



N+I: -73dBm
IF1: -84dBm 472.5MHz
IF2: -85dBm 473.6MHz

✓ The antenna has been assigned to a specific RF channel.

Pairing/unpairing mobile devices

In the WebUI, you can pair up to 128 mobile devices to a Base Station within one RF channel.

Mobile devices can only be paired and operated with one Base Station at a time. If a mobile device is to be used with another Base Station, it must first be paired again.

> **i** Please unmute at least one RF channel before pairing if this was not done automatically.

To pair a mobile device:

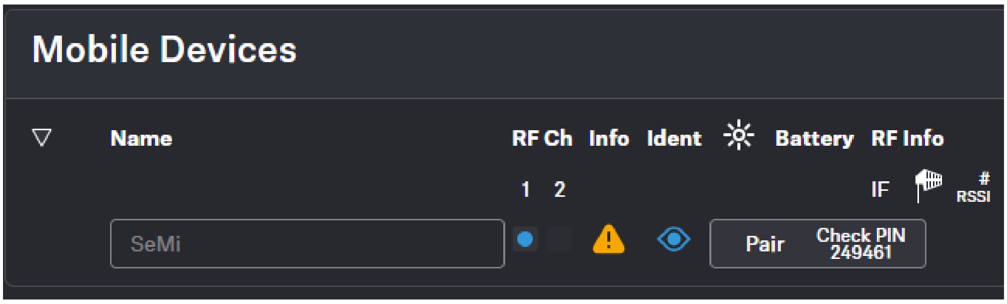
▶ In the top bar, navigate to **Configuration** > **Base Station**.

▶ Click on **Enable Pairing**.

✓ The Base Station starts the pairing process for 300 seconds.

▶ Switch on your mobile device and activate **Pairing Mode** if it has not been activated automatically (Switching the SEK on and off).

✓ After a few seconds, the available mobile devices are displayed in the list below under **Mobile Devices**. A verification PIN is displayed on the mobile device and in the WebUI.



Mobile Devices

▽	Name	RF Ch		Info	Ident	Battery	RF Info	
		1	2				IF	# RSSI
	SeMi	●		⚠	👁	Pair	Check PIN 249461	

▶ Verify the PIN on the mobile device and click on **Pair**.

✓ The mobile device has been paired successfully. The device state color changes to:

ⓘ green (successfully paired)

⚠ gray (assigned RF channel not on air)

⚠ yellow (firmware mismatch) or

⚠ red (unconnected, no RF channel selected, not available)

To unpair a mobile device:

> **i** To unpair a paired device, the audio links must first be deactivated.

- ▶ In the top bar, navigate to **Configuration** > **Mobile Devices**.
- ▶ Click on the button **Unpair** > **Confirm** in the line of the mobile device to be unpaired.
  - ✓ The mobile device has been successfully unpaired.

> ✓ The mobile devices have been successfully paired/unpaired.

Selecting audio link mode (Mic/Line)

You can select the audio mode for your Mic/Line link.

> i Please note that the bandwidth utilization varies depending on the link mode.

The following modes are available:

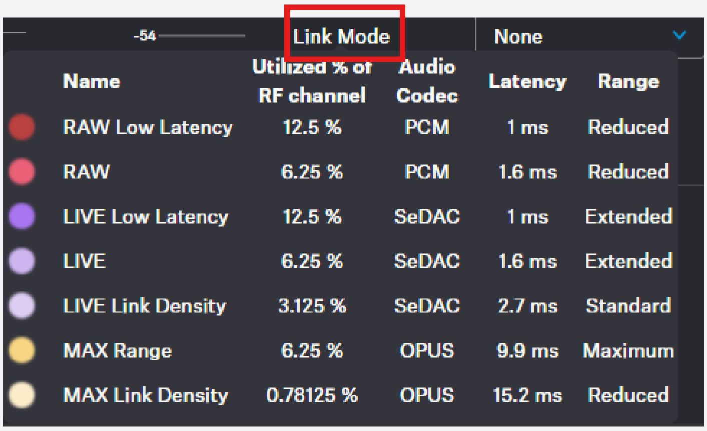
- ● Max Range
- ● Max Link Density
- ● Live Link Density
- ● LIVE
- ● Live Low Latency
- ● RAW
- ● RAW Live Low Latency

To select the audio mode:

▶ In the top bar, navigate to **Configuration** > **Mobile Devices** > **Mic Settings**.

▶ Select the audio mode from the drop-down list **Link Mode**.

> i Hover your mouse over the word **Link Mode** to display a tabular listing of possible modes.



Link Mode None

	Name	Utilized % of RF channel	Audio Codec	Latency	Range
●	RAW Low Latency	12.5 %	PCM	1 ms	Reduced
●	RAW	6.25 %	PCM	1.6 ms	Reduced
●	LIVE Low Latency	12.5 %	SeDAC	1 ms	Extended
●	LIVE	6.25 %	SeDAC	1.6 ms	Extended
●	LIVE Link Density	3.125 %	SeDAC	2.7 ms	Standard
●	MAX Range	6.25 %	OPUS	9.9 ms	Maximum
●	MAX Link Density	0.78125 %	OPUS	15.2 ms	Reduced

✓ The audio mode has been selected.

Selecting audio link mode (IEM)

You can select the audio mode for your IEM link.

> **i** Please note that the bandwidth utilization varies depending on the link mode.

The following modes are available:

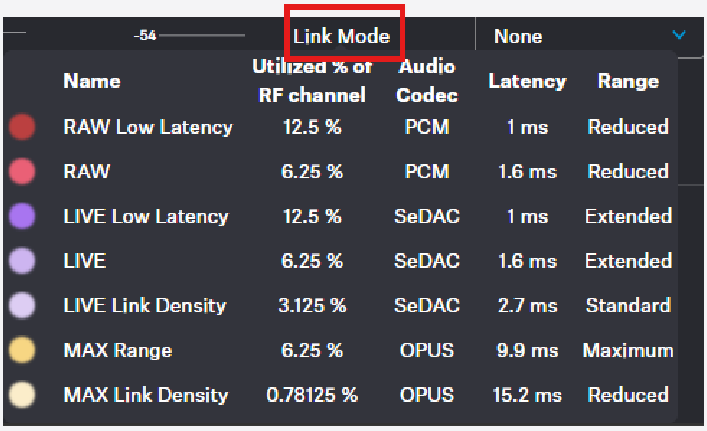
- ● Max Range
- ● Max Link Density
- ● Live Link Density Range
- ● Live Link Density Range
- ● Live Low Latency
- ● Live Ultra Low Latency

To select the audio mode:

▶ In the top bar, navigate to **Configuration** > **Mobile Devices** > **IEM Settings**.

▶ Select the audio mode from the drop-down list **Link Mode**.

> **i** Hover your mouse over the word **Link Mode** to display a tabular listing of possible modes.



Link Mode None

	Name	Utilized % of RF channel	Audio Codec	Latency	Range
●	RAW Low Latency	12.5 %	PCM	1 ms	Reduced
●	RAW	6.25 %	PCM	1.6 ms	Reduced
●	LIVE Low Latency	12.5 %	SeDAC	1 ms	Extended
●	LIVE	6.25 %	SeDAC	1.6 ms	Extended
●	LIVE Link Density	3.125 %	SeDAC	2.7 ms	Standard
●	MAX Range	6.25 %	OPUS	9.9 ms	Maximum
●	MAX Link Density	0.78125 %	OPUS	15.2 ms	Reduced

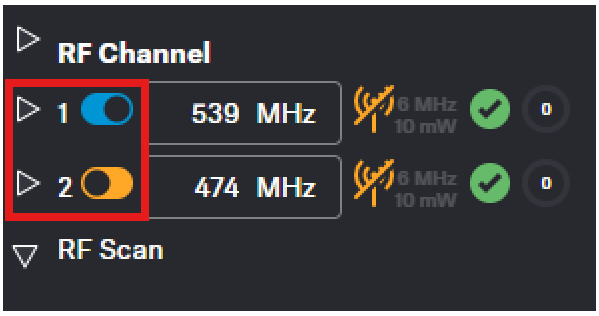
> ✓ The audio mode has been selected.

Assigning an RF channel

You can assign a configured RF channel to your mobile device.

To assign the RF channel:

- In the top bar, navigate to **Configuration** > **Mobile Devices**.
- Select your configured channel under **RF Channel**.



- Enable the toggle switch of the configured RF channel.

✓ The RF channel has been assigned to your mobile device.

Selecting the Mic/Line input

You can select the audio input as the signal source for your Mic/Line link.

i For a smooth system configuration, we recommend first selecting the link modes and afterwards assigning the channels:

- Selecting audio link mode (Mic/Line)
- Selecting audio link mode (IEM)
- Adding/removing an audio channel (Mic/Line)
- Selecting an audio channel (IEM link)
- Selecting the IEM audio interface

i You can route audio links to several channels. Routing can be performed easily via the routing matrix (see Audio inputs and outputs).

The following input signals are available:

- Auto (unknown)
- Mic
- Line

i The automatic mic/line detection is based on power consumption and is optimized for use with Sennheiser microphones. Because third-party microphones vary widely, reliable detection cannot always be ensured.

To choose the audio input:

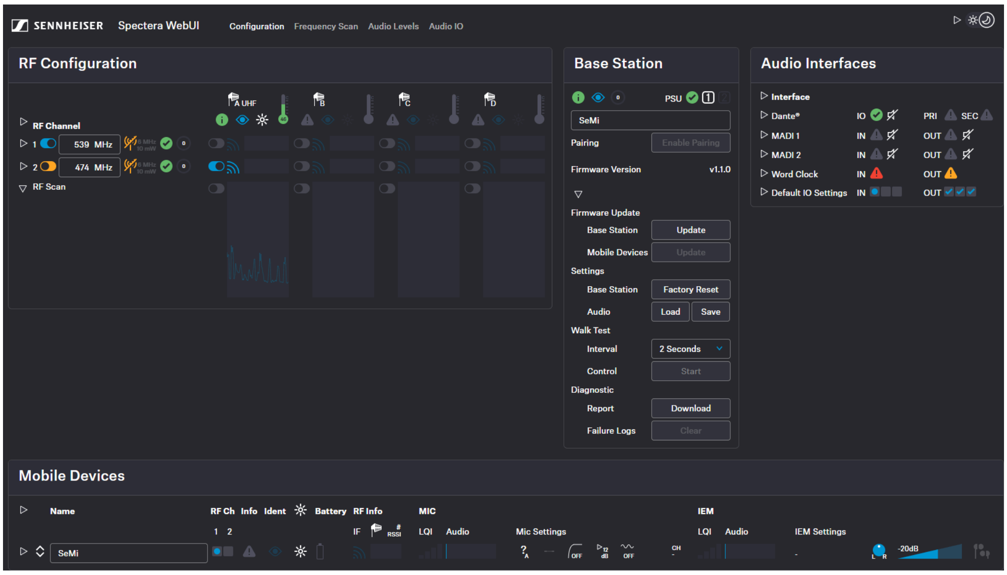
▶ In the top bar, navigate to **Configuration** > **Mobile Devices** > **Mic Settings**.

▶ Select the audio input from the drop-down list **Mic/Line**.

✓ The audio input has been selected.

Configuration

Under Configuration, you can set the essential settings for the RF channel, antenna, Base Station and mobile devices.



RF Channel 1: 539 MHz, 6 MHz, 10 mW

RF Channel 2: 474 MHz, 6 MHz, 10 mW

Base Station: SeMi

Firmware Version v1.1.0

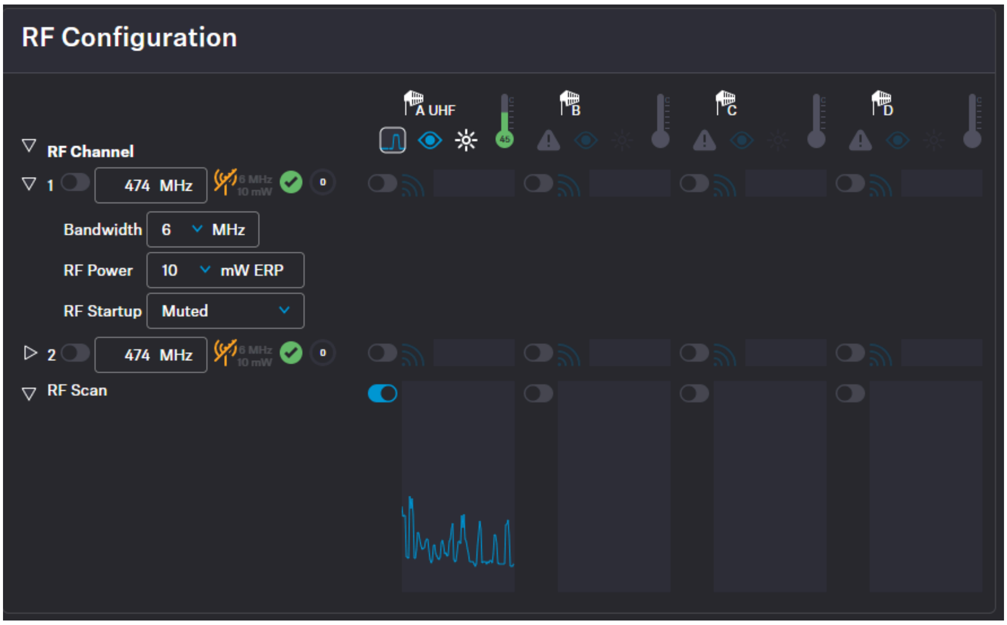
Walk Test Interval: 2 Seconds

Mobile Devices: SeMi

i Please navigate to the desired chapters by clicking on the related information.

RF configuration

Here you can set up your RF channel and check the status of local permissions, your connected antenna, and any potential frequency interference in the surrounding area.



RF Channel 1: 474 MHz, 6 MHz, 10 mW

Bandwidth 6 MHz

RF Power 10 mW ERP

RF Startup Muted

RF Channel 2: 474 MHz, 6 MHz, 10 mW

RF Channel

- Display of two possible configurable RF channels **RfC 1** and **RfC 2**
- Display of the antenna (A-D) assigned to the RF channel

Frequency

- Settings for frequency of the RF channel
- The input is accepted via the **ENTER** key

> **i** The input cannot be accepted by switching with
> **TAB**
> .

- 📡 Status indication of the RF channel with current settings
- Permission indication for local country based on RF channel settings
  - ✅ Valid properties acc. to the license and local regulations
  - ⚠ Invalid properties acc. to the license and local regulations

  > **i** The frequency and bandwidth must comply with local regulations.

- 13 Capacity utilization of the entire RF bandwidth in %

Bandwidth

- Settings for bandwidth of the RF channel

> **i** The input cannot be accepted by switching with
> **TAB**
> .

> **i** The frequency and bandwidth must comply with local regulations. Permission is displayed via the icons ✅ (valid) and ⚠ (invalid).

RF Power

- Setting for the transition power of the transmitter

> **i** The frequency and bandwidth must comply with local regulations. Permission is displayed via the icons ✅ (valid) and ⚠ (invalid).

RF Startup

- Settings for the first RF start after switching off the device or when waking up the device after it has been in standby mode.

Antenna

- 📡 Display of available antennas (A-D)
- ⓘ Readiness status of the RF channel
  - ⓘ green (successfully paired and ready)
  - ⚠ gray (assigned RF channel not on air)
  - ⚠ yellow (high temperature or packet jitter)
  - ⚠ red (error, for example: PoE malfunction, critical temperature)
  - ⚠ red flashing (unconnected: antenna is configured but not connected)
- 👁 Identification button for configured antenna (flashes white 3x)
- ☀ LED brightness of the antenna LED (off, dim, standard, bright)
- 🌡 46 Current antenna temperature (switch between Celsius and Fahrenheit)
- ● Indication for active RF
- 📶 Frequency indication without any interference
- 📶 Frequency indication with interference in the surrounding area

Scanning the RF frequency

You can run a frequency scan to check the current frequency situation in your surrounding area.

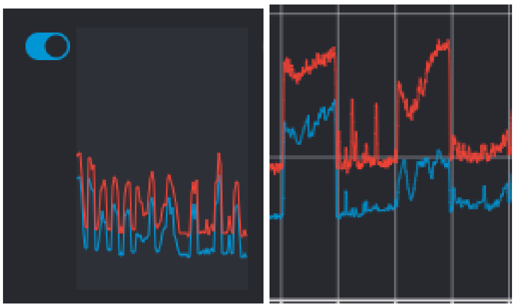
The frequency scan provides an overview of the frequency situation in your location. You can save the antenna configuration as a .csv info file. This file can be used as a backup file to recapitulate your settings or as local frequency information for your specific environment. You can scan the frequencies of all antennas connected to the Base Station.

The scan can be initiated:

- via the RF configuration tab to see a small extract without any details or
- via the Frequency Scan tab for a detailed overview of the frequency situation.

The scan results will be displayed in two different curves:

- **Peak** (red) = Maximum value
- **RMS** (blue) = Average power or strength

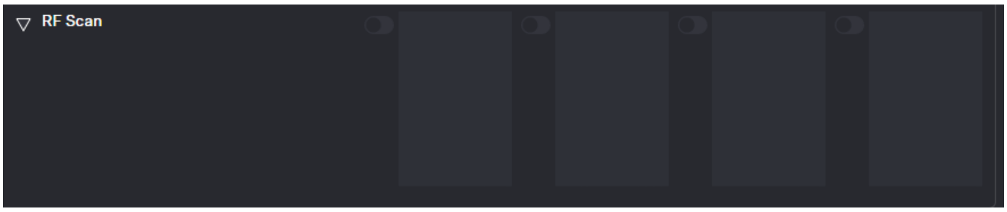


i Please note that the antenna must not be assigned to an RF channel before scanning (see Assigning an antenna to an RF channel).

To scan the RF frequency via the RF configuration tab:

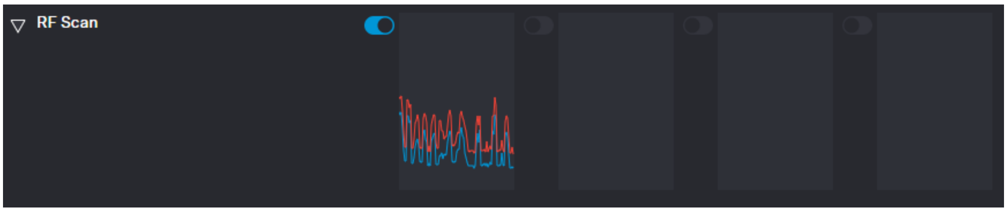
▶ In the top bar, navigate to **Configuration** > **RF Configuration**.

✓ Under the **RF Scan** drop-down menu, there are four toggle switches that enable and disable the scan function for each connected antenna.



▶ Click on the toggle switch of the antenna to be scanned in order to start an immediate scan.

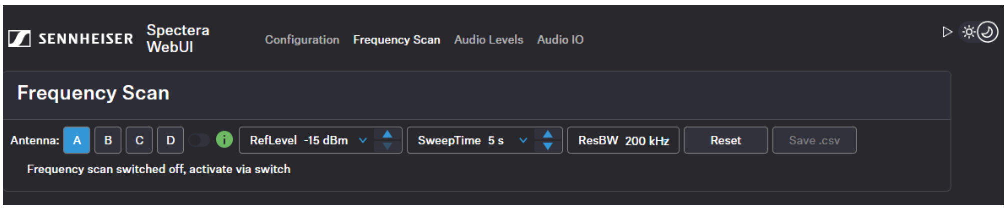
✓ The square is highlighted with a blue dot and the scan result is displayed in a small frequency curve after approx. 5 seconds.



- In order to view the results,
  - click on the small frequency icon or
  - navigate to **Frequency Scan** in the top bar.

To scan the RF frequency via the Frequency Scan tab:

- In the top bar, navigate to the tab **Frequency Scan**.



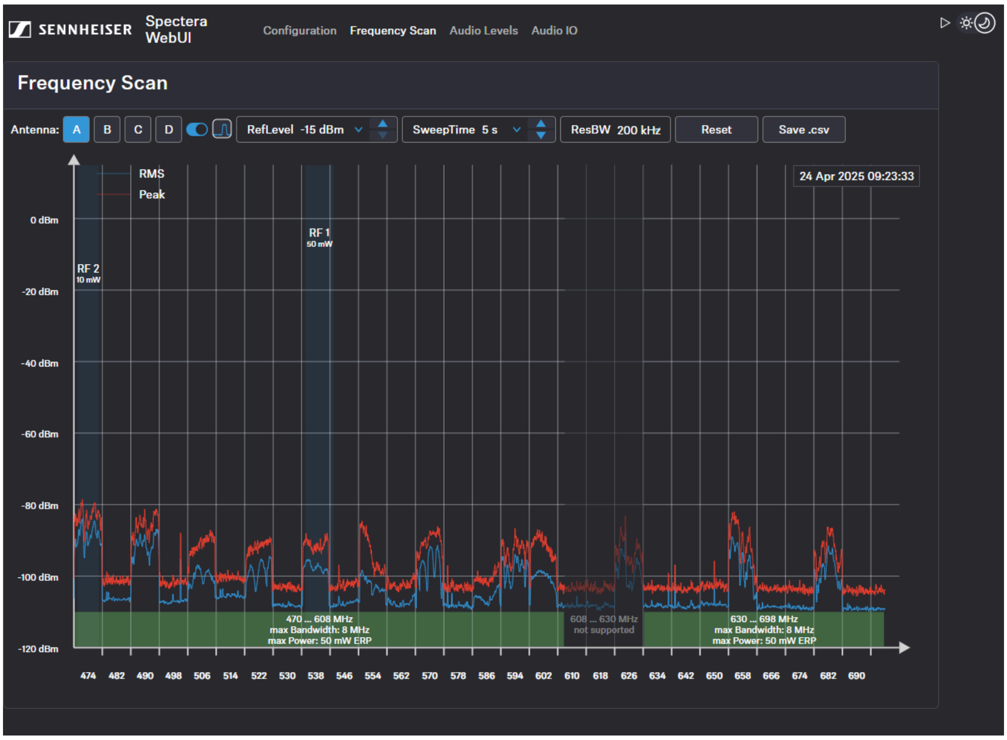
Frequency Scan

Antenna: A B C D RefLevel -15 dBm SweepTime 5 s ResBW 200 kHz

Frequency scan switched off, activate via switch

- Select your antenna to be scanned and adjust your desired settings.
- Switch on the toggle to start the scan.

✓ The frequency scan is started and the result is displayed in a detailed frequency diagram. Supported frequency ranges are shown in green and unsupported ranges in gray.



Frequency Scan

Antenna: A B C D RefLevel -15 dBm SweepTime 5 s ResBW 200 kHz

To reset a scan:

▶ Click on **Reset**.

✓ The current scan will be reset.

To save the scan results as `.csv`:

▶ Click on **Save.csv**.

✓ The antenna configuration has been downloaded locally to your computer as a `.csv` file.

✓ The frequency of your connected antenna has been scanned.

Configuring RF channels

Here you can find out how to configure the RF channel correctly from the outset.

> **i** The current local permissions are displayed when the frequency is selected.

To configure an RF channel:

▶ In the top bar, navigate to **Configuration** > **RF Configuration**.

▶ For channel RF1, enter the frequency under **1** and confirm with **ENTER**.

▶ Next, select the **Bandwidth** and the **RF Power** for your location.

✓ The applicability of your settings is indicated by an icon:

✅ green: applicable

⚠ red: not applicable

▶ Under **RF Startup**, select the mute option for the configured RF channel:

- Active
- Muted
- Last state = When switching on or leaving standby mode, the last used RF state is restored

✓ The RF Channel has been assigned to the operating antenna.

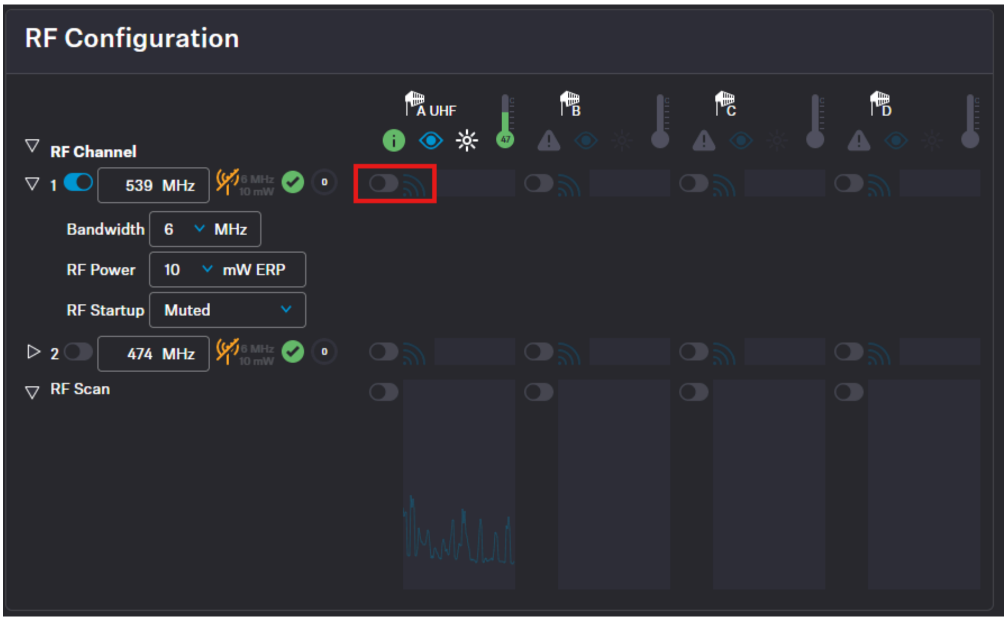
> ✓ The RF Channel has been configured.

Assigning an antenna to an RF channel

You can choose between up to four connected antennas to assign them to your two possible RF channels.

> i For additional reliability in terms of redundancy or to extend your range, you can assign up to four antennas per channel and use them simultaneously.

The antennas can be assigned and unassigned, e.g. to perform an RF scan or to switch between the configured RF channels.



RF Configuration

RF Channel

1 539 MHz

Bandwidth 6 MHz

RF Power 10 mW ERP

RF Startup Muted

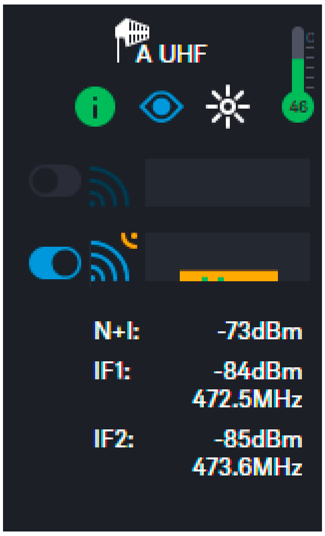
2 474 MHz

RF Scan

To assign an antenna for an RF channel:

- In the top bar, navigate to **Configuration** > **RF Configuration**.
- In your RF channel row, click on the toggle switch next to the utilization and interference icon .

✓ The toggle switch turns blue . The antenna has been assigned to the RF channel and any potential interference is indicated by the icon.

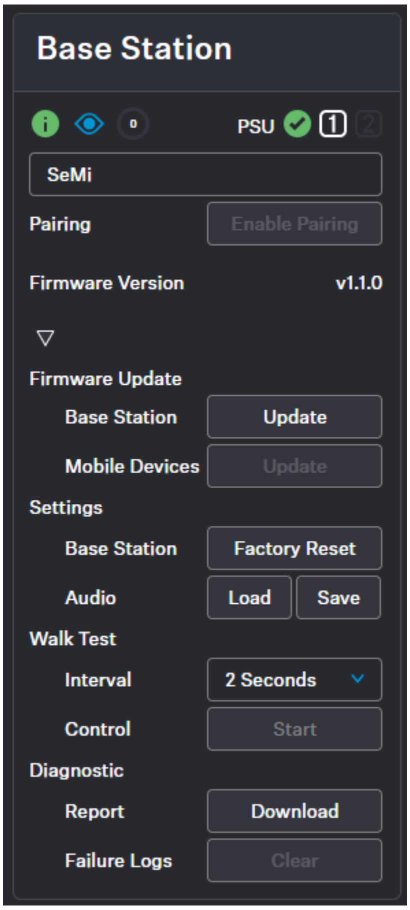


N+I: -73dBm
IF1: -84dBm
472.5MHz
IF2: -85dBm
473.6MHz

✓ The antenna has been assigned to a specific RF channel.

Base Station

Here, you can check the basic settings of the Base Station and easily perform tasks such as firmware updates, walk tests, or restoring it to factory settings.



Base Station

ⓘ ◉ 0 PSU ✓ 1 2

SeMi

Pairing: Enable Pairing

Firmware Version: v1.1.0

▽

Firmware Update
- Base Station: Update
- Mobile Devices: Update

Settings
- Base Station: Factory Reset
- Audio: Load | Save

Walk Test
- Interval: 2 Seconds
- Control: Start

Diagnostic
- Report: Download
- Failure Logs: Clear

General

- ⓘ Device state color
- ◉ Identify button (see Identifying the Base Station)
- 0 Indication for pending actions
- ✓ 1 Connection status and number of connected power supply units
- Name of your Base Station (see Changing the device name)

Enable Pairing

- Triggers the Pairing function of the Base Station for 300 sec. (see Pairing/unpairing mobile devices)

Firmware Update

- Base Station
    - Update service for the Base Station (see Updating the firmware (Base Station))
- Mobile Devices
    - Update service for mobile devices (see Updating the firmware (mobile devices))

Settings

- Base Station
    - Factory Reset - resets the Base Station to the factory defaults (see Resetting the Base Station)
- Audio
    - Saving/loading audio settings as `.json` file (Saving/loading audio settings)

Walk Test

- Interval: interval of the walk test (see Performing a walk test)
- Control: Starting/Stopping the walk test

Diagnostic

- **Report**: Provides archived support information of the product as a download.

  > **i** The automatically generated file contains basic information about the product and the last saved product configuration before a potential failure. In case of support, this file should be saved and sent to the support team.

- **Failure Logs**: Deletes all error messages saved under "Report" that occurred during runtime.

Changing the device name

You can change the device name for your Base Station.

> **i** For security reasons, please do not enter any sensitive personal data as the device name.

To change the device name:

- ▶ In the top bar, navigate to **Configuration** > **Base Station**.
- ▶ Edit the name under **Name** and confirm with **ENTER**.
  - ✓ The name is immediately transmitted to the Base Station and saved.

✓ The device name has been changed.

Updating the firmware (Base Station)

The firmware version of the Base Station can be downloaded and updated manually.

The firmware version for the Base Station also includes the latest versions for the antennas and the mobile devices. While the antennas are updated automatically, the updates for the mobile devices must be started explicitly.

> i Please download the latest firmware version for your Base Station under: sennheiser.com/spectera-base-station.

NOTICE

⚠ **Data loss during firmware update**

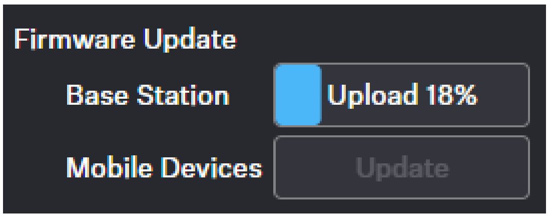
The audio transmission is interrupted during the firmware update of the Base Station, the antenna or the mobile device.

After the firmware update, the device is restarted automatically.

- ▶ Do not update the firmware during an active live audio transmission.

To update your Base Station firmware:

- ▶ In the top bar, navigate to **Configuration** > **Base Station**.
- ▶ Under **Firmware Update** > **Base Station** click on **Update**.
  - ✓ A new upload window opens.
- ▶ Select the manually downloaded `.sennpkg` file.
  - ✓ The firmware file has been selected. The firmware starts the update automatically. The update process is indicated by the current percentage value.


Firmware Update

Base Station: Upload 18%

Mobile Devices: Update

> i After the successful update, the Base Station restarts and automatically begins the update on the connected antennas. Please refresh your browser after the entire update process.

✓ The firmware has been updated once the update is installed.

Updating the firmware (mobile devices)

The update of the firmware version of mobile devices can be initiated using the Update button.

The latest firmware version for the mobile devices will be delivered with the latest firmware version of the Base Station. To update to a new version, the update process must be initialized individually.

> **i** Please note that firmware versions are not backward compatible. The latest compatible version is included in the firmware update package for the Base Station.

NOTICE

Data loss during firmware update

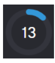
The audio transmission is interrupted during the firmware update of the Base Station, the antenna or the mobile device.

After the firmware update, the device is restarted automatically.

- Do not update the firmware during an active live audio transmission.

To update your mobile device firmware:

- In the top bar, navigate to **Configuration** > **Base Station**.
- Under **Firmware Update** > **Mobile Devices** click on **Update**.

✓ The update process will start automatically and show the progress as a percentage . After a successful update, the mobile device is restarted and paired automatically.

> **i** The firmware update is a disruptive process. The mobile devices will update and reboot in sequence. This process will take roughly 20 seconds: during this time audio will be lost. Please stay in reach of the Base Station, do not remove the battery from the mobile devices during the process and do not close the application.

✓ The firmware has been updated.

Resetting the Base Station

You can reset the Base Station to the factory settings remotely.

> i You can also reset the Base Station to the factory settings directly via the device.

NOTICE

Loss of data after resetting to factory settings

All settings are reset to the factory settings!

All devices will be unpaired and all audio routes will be deleted!

The user password will be reset!

The entitlement will remain.

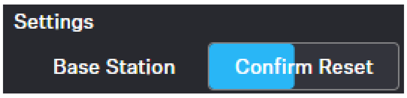
▶ Make sure that no connections are being actively used at the time of the reset.

To reset the Base Station remotely:

▶ In the top bar, navigate to **Configuration** > **Base Station**.

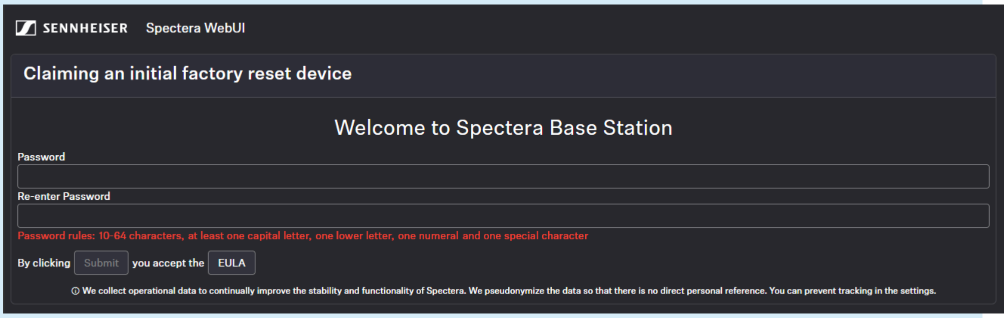
▶ Click on **Settings** and then on **Factory Reset**.

✓ A countdown timer will be displayed (highlighted in blue).



▶ Press **Confirm Reset** to confirm the factory reset.

✓ The Base Station has been reset. Upon re-login, you will be prompted to set a new password for the device.



Claiming an initial factory reset device

Welcome to Spectera Base Station

Password

Re-enter Password

Password rules: 10-64 characters, at least one capital letter, one lower letter, one numeral and one special character

By clicking Submit you accept the EULA

ⓘ We collect operational data to continually improve the stability and functionality of Spectera. We pseudonymize the data so that there is no direct personal reference. You can prevent tracking in the settings.

Pairing/unpairing mobile devices

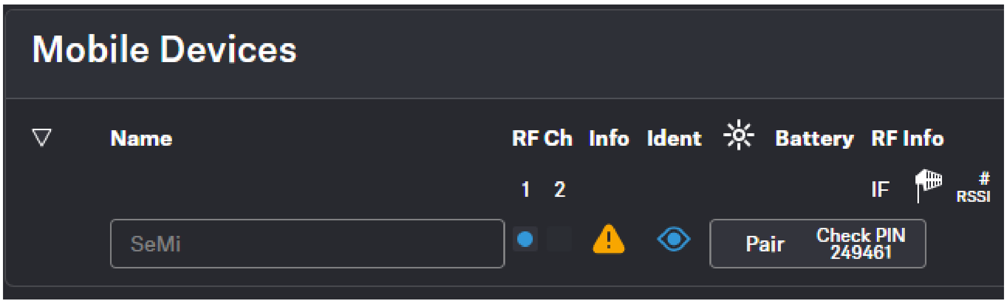
In the WebUI, you can pair up to 128 mobile devices to a Base Station within one RF channel.

Mobile devices can only be paired and operated with one Base Station at a time. If a mobile device is to be used with another Base Station, it must first be paired again.

> **i** Please unmute at least one RF channel before pairing if this was not done automatically.

To pair a mobile device:

- In the top bar, navigate to **Configuration** > **Base Station**.
- Click on **Enable Pairing**.
  - ✓ The Base Station starts the pairing process for 300 seconds.
- Switch on your mobile device and activate **Pairing Mode** if it has not been activated automatically (Switching the SEK on and off).
  - ✓ After a few seconds, the available mobile devices are displayed in the list below under **Mobile Devices**. A verification PIN is displayed on the mobile device and in the WebUI.



- Verify the PIN on the mobile device and click on **Pair**.
  - ✓ The mobile device has been paired successfully. The device state color changes to:
    - ⓘ green (successfully paired)
    - ⚠ gray (assigned RF channel not on air)
    - ⚠ yellow (firmware mismatch) or
    - ⚠ red (unconnected, no RF channel selected, not available)

To unpair a mobile device:

i To unpair a paired device, the audio links must first be deactivated.

- ▶ In the top bar, navigate to **Configuration** > **Mobile Devices**.
- ▶ Click on the button **Unpair** > **Confirm** in the line of the mobile device to be unpaired.
  - ✓ The mobile device has been successfully unpaired.

✓ The mobile devices have been successfully paired/unpaired.

Identifying the Base Station

You can remotely identify your Base Station.

To identify the Base Station:

- ▶ In the top bar, navigate to **Configuration** > **Base Station**.
- ▶ Click on the 👁 **Identify** icon.
  - ✓ The icon on the Base Station card flashes. The Base Station display shows "Identify".

✓ The Base Station has been identified.

Saving/loading audio settings

You can save your audio settings and load them at a later time.

> **i** In order to apply the audio settings, a familiar ID of the previously assigned mobile device is expected in connection with the hardware configuration of the Base Station described in this document. Unknown IDs of the mobile device or unknown hardware configurations will result in the settings not being accepted successfully.

The audio settings can be exported in a `.json` file.

To save your audio settings:

▶ In the top bar, navigate to **Configuration** > **Base Station**.

▶ Under **Settings** click on **Save**.

✓ Your audio settings have been exported as a `.json` file.

To load your saved audio settings:

▶ In the top bar, navigate to **Configuration** > **Base Station**.

▶ Under **Settings** click on **Load**.

✓ A new upload window opens.

▶ Select your saved file and click on **Open**.

✓ Your audio settings file has been successfully loaded.

✓ The audio settings have been successfully saved/loaded.

Performing a walk test

A walk test allows you to check the reception quality of your radio links within the operating environment.

The automatically generated data is used to provide an overview of the frequency behavior with the simulated devices and their configuration under the intended conditions. The result is represented as plain data in a `.json` file. The implementation of a graphical representation of the result is in planning.

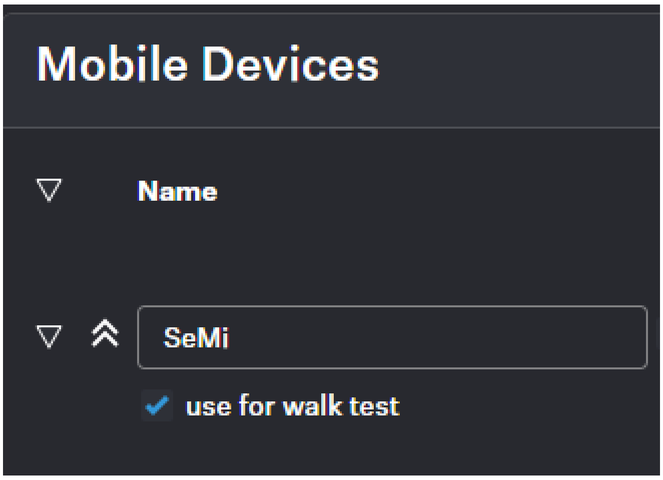
You can specify the measurement interval of the walk test in seconds:

- 1
- 2
- 3
- 4
- 5
- 10
- 20
- 30

> **i** If the total data rate is too high, individual values are omitted.

To perform a walk test:

- ▶ Switch on the transmitter and the receiver of the radio link you want to check.
- ▶ In addition, switch on all other devices that you want to use in the operating environment.
- ▶ Navigate to **Configuration** > **Mobile Devices** and select the checkbox **use for walk test** for the device to be tested.



Mobile Devices

▽ Name

▽ ⌃ SeMi

☑ use for walk test

▶ Navigate to **Configuration** > **Base Station**, select the measuring interval for the walk test and click on **Start**.

✓ The walk test has been started.

▶ Walk the operating environment with the mobile device.

▶ Click on **Stop** as soon as the walk test has been performed.

✓ The results of the walk test are automatically downloaded locally to your computer as a `.json` file.

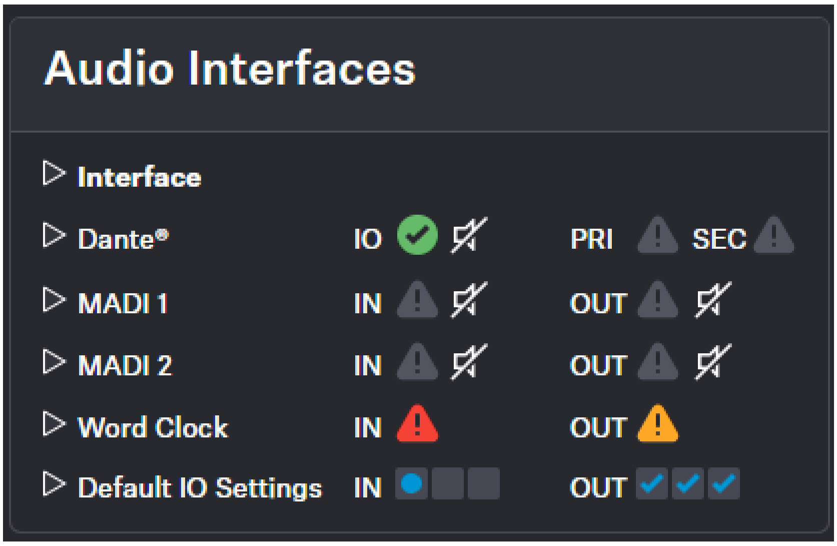
✓ The walk test has been performed successfully.

Audio interfaces

Here you can monitor all available interfaces and manage the outputs.

A built-in sample rate converter can be used to convert the outputs to predetermined frequencies and generate a custom sample rate for any audio channel. The following settings are available for MADI 1, MADI 2 and Word Clock interfaces:

- Leader 48 kHz
- Leader 96 kHz
- Follow MADI 1 Input
- Follow MADI 2 Input
- Follow World Clock Input
- Follow Audio Network



Audio Interfaces

▷ Interface

▷ Dante® IO ✓ PRI ⚠ SEC ⚠

▷ MADI 1 IN ⚠ OUT ⚠

▷ MADI 2 IN ⚠ OUT ⚠

▷ Word Clock IN ⚠ OUT ⚠

▷ Default IO Settings IN ● □ □ OUT ☑ ☑ ☑

The interface status is indicated by the following colors:

- ⓘ: OK
- ⚠: Not used
- ⚠: Attention, e.g.: "fallback active"
- ⚠: Warning, e.g.: "input not toggling"

Audio Network

- Dante®
- Dante® Primary
- Dante® Secondary

MADI 1

- Input
- Output

MADI 2

- Input
- Output

Word Clock BNC

- Input
- Output

Default Input Interface

- Dante®
- MADI 1
- MADI 2

Selecting the default audio input/output source

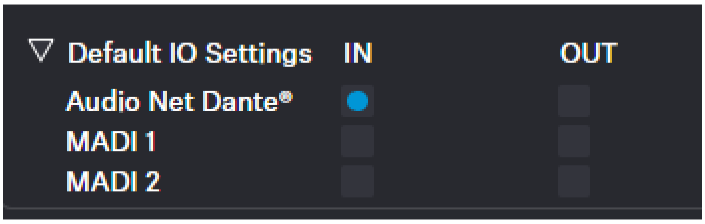
You can select the default source for the audio input and output of your audio interface.

To select the default input interface:

▶ In the top bar, navigate to **Configuration RF** > **Audio Interfaces**.

▶ Select the input interface under **Default IO Settings**.

✓ The default input interface has been selected.



▽ Default IO Settings	IN	OUT
Audio Net Dante®	●	□
MADI 1	□	□
MADI 2	□	□

To select the clock source output:

▶ Select the desired setting for the clock source under:

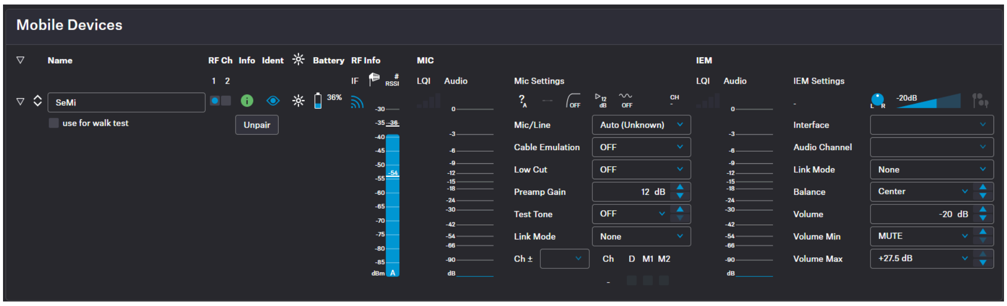
- **MADI 1**
- **MADI 2**
- **Word Clock BNC**

✓ The clock source output has been selected.

✓ The audio interfaces have been selected.

Mobile Devices

Here you can configure specific settings for mobile devices.



□ use for walk test

Mic/Line: Auto (Unknown)
Cable Emulation: OFF
Low Cut: OFF
Preamp Gain: 12 dB
Test Tone: OFF
Link Mode: None
Ch ±

Interface
Audio Channel
Link Mode: None
Balance: Center
Volume: -20 dB
Volume Min: MUTE
Volume Max: +27.5 dB

The following interactions can be made for each mobile device:

General

- Changing the name of the device (see Changing the device name)
- Assigning an RF channel (see Assigning an RF channel)
- Monitoring the status of the device (connection status, temperature, entitlement, data-transition etc)
- Changing the LED brightness (see Setting the LED brightness)
- Identifying the device (see Identifying your mobile device)
- Pairing/unpairing the device (see Pairing/unpairing mobile devices)
- Monitoring the battery status
- Interference level at mobile device
- Receive Single Strength Indication at the dominant antenna
- Link Quality Input (LQI)

MIC

- Link Quality Input (LQI) (see Selecting audio link mode (Mic/Line))
- Input Mic/Line (see Selecting the Mic/Line input)
- Cable Emulation (see Activating/deactivating cable emulation)
- OFF Low Cut (see Activating/deactivating Low Cut)
- 12 dB Preamp Gain (see Setting the Preamp Gain)
- OFF Test Tone (see Activating/deactivating Test Tone)

- ● Link Mode (color depends on the mode) (see Selecting audio link mode (Mic/Line))
- CH 1 Assigned channel (see Assigning an RF channel)

In-Ear Monitoring (IEM)

- Interface (see Selecting the default audio input/output source)
- Channel (see Selecting an audio channel (IEM link))
- Mode (see Selecting audio link mode (IEM))
  - ● Max Range
  - ● Max Link Density
  - ● Live Link Density Range
  - ● Live Link Density Range
  - ● Live Low Latency
  - ● Live Ultra Low Latency
- L ● R Balance / Center (see Adjusting the balance)
- -34.5dB Volume (see Setting the volume)
- 🎧 Headphone

Pairing/unpairing mobile devices

In the WebUI, you can pair up to 128 mobile devices to a Base Station within one RF channel.

Mobile devices can only be paired and operated with one Base Station at a time. If a mobile device is to be used with another Base Station, it must first be paired again.

> **i** Please unmute at least one RF channel before pairing if this was not done automatically.

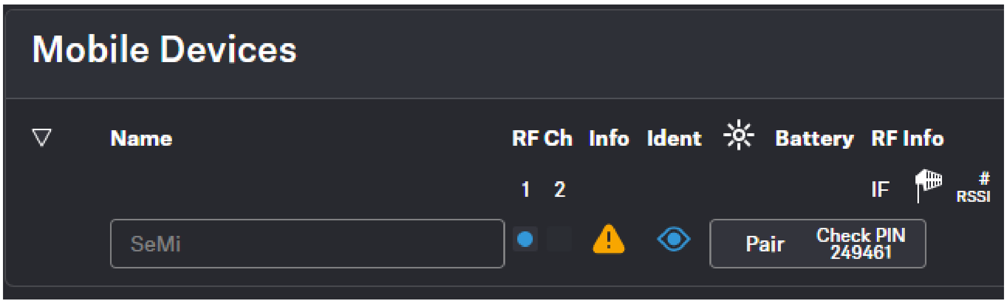
To pair a mobile device:

▶ In the top bar, navigate to **Configuration** > **Base Station**.

▶ Click on **Enable Pairing**.

✓ The Base Station starts the pairing process for 300 seconds.

- Switch on your mobile device and activate **Pairing Mode** if it has not been activated automatically (**Switching the SEK on and off**).
  - ✓ After a few seconds, the available mobile devices are displayed in the list below under **Mobile Devices**. A verification PIN is displayed on the mobile device and in the WebUI.



Mobile Devices

▽	Name	RF Ch	Info	Ident	☼	Battery	RF Info
		1 2					IF # RSSI
	SeMi	●	⚠	👁		Pair	Check PIN 249461

- Verify the PIN on the mobile device and click on **Pair**.
  - ✓ The mobile device has been paired successfully. The device state color changes to:
    - ⓘ green (successfully paired)
    - ⚠ gray (assigned RF channel not on air)
    - ⚠ yellow (firmware mismatch) or
    - ⚠ red (unconnected, no RF channel selected, not available)

To unpair a mobile device:

> **i** To unpair a paired device, the audio links must first be deactivated.

- In the top bar, navigate to **Configuration** > **Mobile Devices**.
- Click on the button **Unpair** > **Confirm** in the line of the mobile device to be unpaired.
  - ✓ The mobile device has been successfully unpaired.

> ✓ The mobile devices have been successfully paired/unpaired.

Identifying your mobile device

You can remotely identify your mobile device.

To identify the mobile device:

- ▶ In the top bar, navigate to **Configuration** > **Mobile Devices**.
- ▶ Click on the 👁**Identify** icon.
  - ✓ The LED on the mobile device flashes white alternately for 5 seconds.

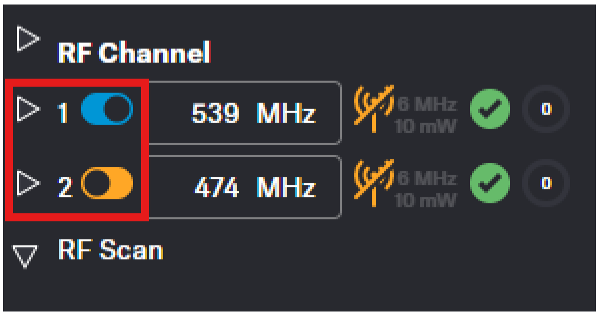
✓ The mobile device has been identified.

Assigning an RF channel

You can assign a configured RF channel to your mobile device.

To assign the RF channel:

- In the top bar, navigate to **Configuration** > **Mobile Devices**.
- Select your configured channel under **RF Channel**.



RF Channel

1 539 MHz 6 MHz 10 mW 0

2 474 MHz 6 MHz 10 mW 0

RF Scan

- Enable the toggle switch of the configured RF channel.

✓ The RF channel has been assigned to your mobile device.

Selecting audio link mode (IEM)

You can select the audio mode for your IEM link.

> Please note that the bandwidth utilization varies depending on the link mode.

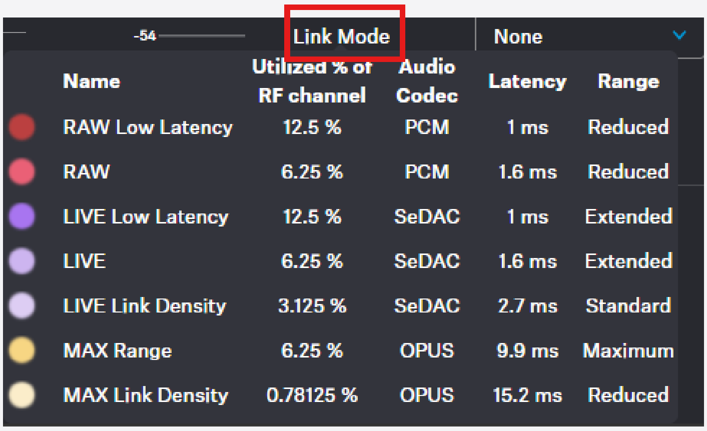
The following modes are available:

- ● Max Range
- ● Max Link Density
- ● Live Link Density Range
- ● Live Link Density Range
- ● Live Low Latency
- ● Live Ultra Low Latency

To select the audio mode:

- In the top bar, navigate to **Configuration** > **Mobile Devices** > **IEM Settings**.
- Select the audio mode from the drop-down list **Link Mode**.

> Hover your mouse over the word **Link Mode** to display a tabular listing of possible modes.



	Name	Utilized % of RF channel	Audio Codec	Latency	Range
●	RAW Low Latency	12.5 %	PCM	1 ms	Reduced
●	RAW	6.25 %	PCM	1.6 ms	Reduced
●	LIVE Low Latency	12.5 %	SeDAC	1 ms	Extended
●	LIVE	6.25 %	SeDAC	1.6 ms	Extended
●	LIVE Link Density	3.125 %	SeDAC	2.7 ms	Standard
●	MAX Range	6.25 %	OPUS	9.9 ms	Maximum
●	MAX Link Density	0.78125 %	OPUS	15.2 ms	Reduced

✓ The audio mode has been selected.

Selecting audio link mode (Mic/Line)

You can select the audio mode for your Mic/Line link.

i Please note that the bandwidth utilization varies depending on the link mode.

The following modes are available:

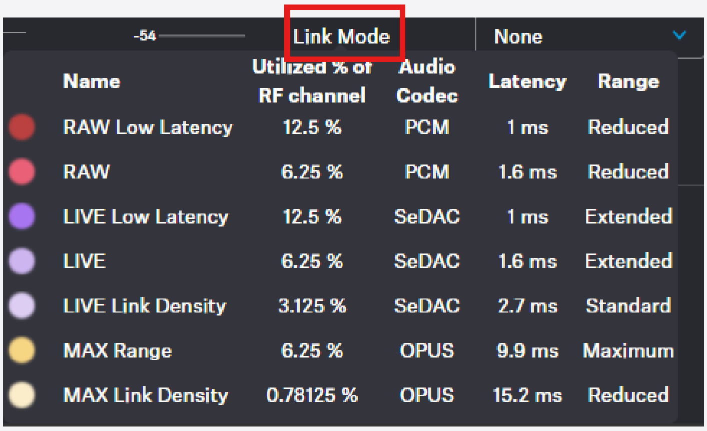
- ● Max Range
- ● Max Link Density
- ● Live Link Density
- ● LIVE
- ● Live Low Latency
- ● RAW
- ● RAW Live Low Latency

To select the audio mode:

▶ In the top bar, navigate to **Configuration** > **Mobile Devices** > **Mic Settings**.

▶ Select the audio mode from the drop-down list **Link Mode**.

i Hover your mouse over the word **Link Mode** to display a tabular listing of possible modes.



-54 Link Mode None

	Name	Utilized % of RF channel	Audio Codec	Latency	Range
●	RAW Low Latency	12.5 %	PCM	1 ms	Reduced
●	RAW	6.25 %	PCM	1.6 ms	Reduced
●	LIVE Low Latency	12.5 %	SeDAC	1 ms	Extended
●	LIVE	6.25 %	SeDAC	1.6 ms	Extended
●	LIVE Link Density	3.125 %	SeDAC	2.7 ms	Standard
●	MAX Range	6.25 %	OPUS	9.9 ms	Maximum
●	MAX Link Density	0.78125 %	OPUS	15.2 ms	Reduced

✓ The audio mode has been selected.

Selecting the Mic/Line input

You can select the audio input as the signal source for your Mic/Line link.

i For a smooth system configuration, we recommend first selecting the link modes and afterwards assigning the channels:

- Selecting audio link mode (Mic/Line)
- Selecting audio link mode (IEM)
- Adding/removing an audio channel (Mic/Line)
- Selecting an audio channel (IEM link)
- Selecting the IEM audio interface

i You can route audio links to several channels. Routing can be performed easily via the routing matrix (see Audio inputs and outputs).

The following input signals are available:

- Auto (unknown)
- Mic
- Line

i The automatic mic/line detection is based on power consumption and is optimized for use with Sennheiser microphones. Because third-party microphones vary widely, reliable detection cannot always be ensured.

To choose the audio input:

▶ In the top bar, navigate to **Configuration** > **Mobile Devices** > **Mic Settings**.

▶ Select the audio input from the drop-down list **Mic/Line**.

✓ The audio input has been selected.

Adding/removing an audio channel (Mic/Line)

You can assign an audio channel number and the interface output for your Mic/Line link.

> i You can route audio links to several channels. Routing can be performed easily via the routing matrix (see Audio inputs and outputs).

To add an audio channel:

- ▶ In the top bar, navigate to **Configuration** > **Mobile Devices** > **Mic Settings**.
- ▶ Select the channel number from the drop-down list **Channel** which is indicated with a plus in front of it (e.g. **+1**).

To remove the link channel:

- ▶ Select the channel number from the drop-down list **Channel** which is indicated with a minus in front of it (e.g. **-1**).

To select the output interface of the assigned link channel:

- ▶ Activate/deactivate the check-boxes under **D** (for DANTE®), **M1** (for MADI 1) and/or **M2** (for MADI 2).

> ✓ The audio channel and the audio interface output has been added/removed.

Performing a walk test

A walk test allows you to check the reception quality of your radio links within the operating environment.

The automatically generated data is used to provide an overview of the frequency behavior with the simulated devices and their configuration under the intended conditions. The result is represented as plain data in a `.json` file. The implementation of a graphical representation of the result is in planning.

You can specify the measurement interval of the walk test in seconds:

- 1
- 2
- 3
- 4
- 5
- 10
- 20
- 30

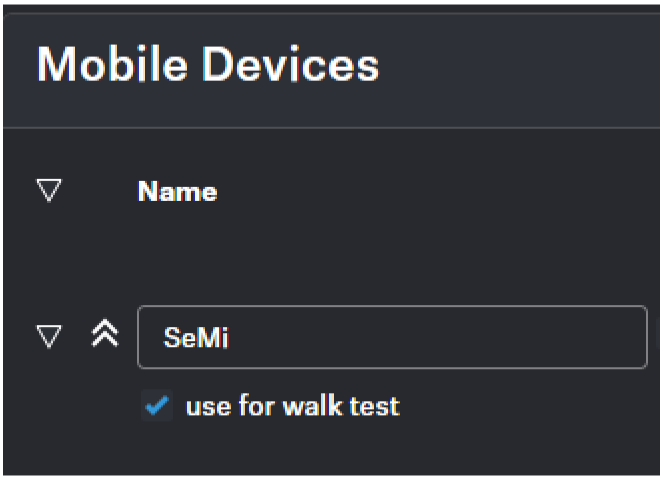
> i If the total data rate is too high, individual values are omitted.

To perform a walk test:

▶ Switch on the transmitter and the receiver of the radio link you want to check.

▶ In addition, switch on all other devices that you want to use in the operating environment.

▶ Navigate to **Configuration** > **Mobile Devices** and select the checkbox **use for walk test** for the device to be tested.



Mobile Devices

Name: SeMi

☑ use for walk test

- ▶ Navigate to **Configuration** > **Base Station**, select the measuring interval for the walk test and click on **Start**.

  ✓ The walk test has been started.

- ▶ Walk the operating environment with the mobile device.

- ▶ Click on **Stop** as soon as the walk test has been performed.

  ✓ The results of the walk test are automatically downloaded locally to your computer as a `.json` file.

✓ The walk test has been performed successfully.

Changing the device name

You can change the device name for your mobile device.

> **i** For security reasons, please do not enter any sensitive personal data as the device name.

To change the device name:

- ▶ In the top bar, navigate to **Configuration** > **Mobile Devices**.
- ▶ Edit the name under **Name** and confirm with **ENTER**.
  - ✓ The name is immediately transmitted to the mobile device and saved.

✓ The device name has been changed.

Setting the LED brightness

You can adjust the brightness of your LED on the mobile device.

There are four settings for the LED brightness:

- ☀ OFF
- ☀ Dim
- ☀ Standard
- ☀ Bright

To change the LED brightness:

▶ In the top bar, navigate to **Configuration** > **Mobile Devices**.

▶ Click on the ☀ icon multiple times to set the LED to your desired brightness.

✓ The LED brightness has been set.

Selecting the IEM audio interface

You can select the desired audio interface as the signal source for your IEM link.

The following interfaces are available:

- Dante®
- MADI 1
- MADI 2

To choose the audio interface:

▶ In the top bar, navigate to **Configuration** > **Mobile Devices** > **IEM Settings**.

▶ Select the audio interface from the drop-down list **Interface**.

✓ The audio interface has been selected.

Selecting an audio channel (IEM link)

You can assign an audio channel number for your IEM link.

i For a smooth system configuration, we recommend first selecting the link modes and afterwards assigning the channels:

- Selecting audio link mode (Mic/Line)
- Selecting audio link mode (IEM)
- Adding/removing an audio channel (Mic/Line)
- Selecting an audio channel (IEM link)
- Selecting the IEM audio interface

i It is also possible to select an existing link (marked with *), as long as it is using the same RF channel.

To add an audio channel:

▶ In the top bar, navigate to **Configuration** > **Mobile Devices** > **IEM Settings**.

▶ Select the channel number from the drop-down list **Audio Channel**.

✓ The audio channel has been selected.

Adjusting the balance

You can change the balance for your IEM link.

The following values can be selected directly and adjusted individually in steps of 1%:

- 100% Left
- 75% Left
- 50% Left
- 25% Left
- Center
- 25% Right
- 50% Right
- 75% Right
- 100% Right

To change the balance:

▶ In the top bar, navigate to **Configuration** > **Mobile Devices** > **IEM Settings**.

▶ Select the balance mode from the drop-down list **Balance**.

✓ The balance mode has been changed.

Setting the volume

The volume can be controlled directly from the device as well as from the WebUI.

If the volume value is changed on the device, this change is displayed in the WebUI in real time.

WARNING

Hearing damage due to high volumes

This product is capable of producing sound pressure levels exceeding 85 dB (A). Volume levels that are too high may damage your hearing.

- Reduce the volume and the microphone amplification, if applicable, before using the product.

To set the volume:

- In the top bar, navigate to **Configuration** > **Mobile Devices** > **IEM Settings**.
- Enter the desired volume level in dB under **Volume**.

✓ The volume has been set.

Setting the min volume

You can set a predefined min volume for your IEM link.

The volume set here is the minimum level that is sent to your dedicated mobile device.

The following values can be selected directly and adjusted individually in steps of 0.5 dB:

- -6 dB
- -12 dB
- -18 dB
- -24 dB
- -30 dB
- -36 dB
- -42 dB
- -48 dB
- -54 dB
- -60 dB
- MUTE

WARNING

⚠ **Hearing damage due to high volumes**

This product is capable of producing sound pressure levels exceeding 85 dB (A). Volume levels that are too high may damage your hearing.

▶ Reduce the volume and the microphone amplification, if applicable, before using the product.

To set the min volume:

▶ In the top bar, navigate to **Configuration** > **Mobile Devices** > **IEM Settings**.

▶ Select the min volume level in dB under **Volume min**.

✓ The min volume has been set.

Setting the max volume

You can set a predefined max volume for your IEM link.

The volume set here is the maximum level that is transmitted to your connected mobile device.

The following values can be selected directly and adjusted individually in steps of 0.5 dB:

- -27.5 dB
- -24 dB
- -18 dB
- -12 dB
- -6 dB
- 0 dB
- +6 dB
- +12 dB
- +18 dB
- +24 dB
- +27.5 dB

WARNING

Hearing damage due to high volumes

This product is capable of producing sound pressure levels exceeding 85 dB (A). Volume levels that are too high may damage your hearing.

▶ Reduce the volume and the microphone amplification, if applicable, before using the product.

To set the max volume:

▶ In the top bar, navigate to **Configuration** > **Mobile Devices** > **IEM Settings**.

▶ Select the max volume level in dB under **Volume max**.

✓ The max volume has been set.

Activating/deactivating cable emulation

You can emulate the capacitance of connected cables and influence the sound of your mic/ line input.

> i Cable emulation is only applicable for the line input.

The following presets are available:

- OFF
- Short
- Mid
- Long

To activate cable emulation:

▶ In the top bar, navigate to **Configuration** > **Mobile Devices** > **Mic Settings**.

▶ Select the value from the drop-down list **Cable Emulation**.

To deactivate cable emulation:

▶ Select the value **OFF**.

✓ The cable emulation value has been activated/deactivated.

Activating/deactivating Low Cut

You can reduce or remove low frequencies in the audio signal while allowing high frequencies to pass through.

This allows low-frequency ambient noise to be filtered out of the audio signal, thereby improving the clarity of the audio.

The following presets are available:

- OFF
- 30 Hz
- 60 Hz
- 80 Hz
- 100 Hz
- 120 Hz

To activate Low Cut:

▶ In the top bar, navigate to **Configuration** > **Mobile Devices** > **Mic Settings**.

▶ Select the value from the drop-down list **Low Cut**.

To deactivate Low Cut:

▶ Select the value **OFF**.

✓ Low Cut has been activated/deactivated.

Setting the Preamp Gain

With the preamp you can increase the audio level for your Mic/Line output.

To set the gain:

- ▶ In the top bar, navigate to **Configuration** > **Mobile Devices** > **Mic Settings**.
- ▶ Enter the desired preamp gain level in 1 dB increments under **Preamp Gain**.

✓ The Preamp Gain has been set.

Activating/deactivating Test Tone

With a constant test tone, you can simulate and test the performance of your audio devices in different dB levels.

The following values can be selected directly and adjusted individually in steps of 1 dB:

- OFF
- -60 dB
- -54 dB
- -48 dB
- -42 dB
- -36 dB
- -30 dB
- -24 dB
- -18 dB
- -12 dB
- -6 dB
- 0 dB

To activate the Test Tone:

▶ In the top bar, navigate to **Configuration** > **Mobile Devices** > **Mic Settings**.

▶ Select the value from the drop-down list under **Test Tone**.

To deactivate the Test Tone:

▶ Select the value **OFF**.

✓ The Test Tone has been activated/deactivated.

Activating a license (webUI)

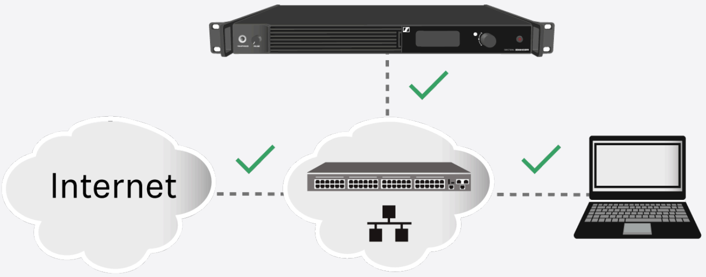
Under Entitlement, you can enter and activate the current license for the frequency spectrum.

i The purchased license (included in the product) is only valid for the region for which the product was designed and approved. The license may not be used in other regions.

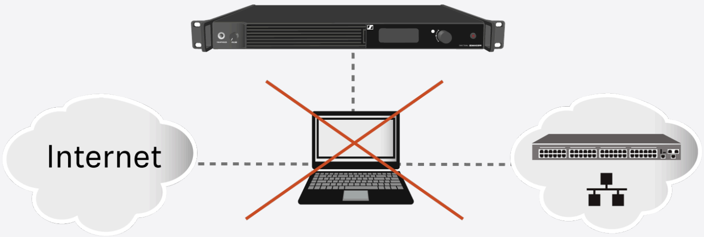
NOTICE

⚠ **License activation requires a direct Internet connection to the device**

In order to activate the Base Station using the 18-digit license code, a direct Internet connection is required.

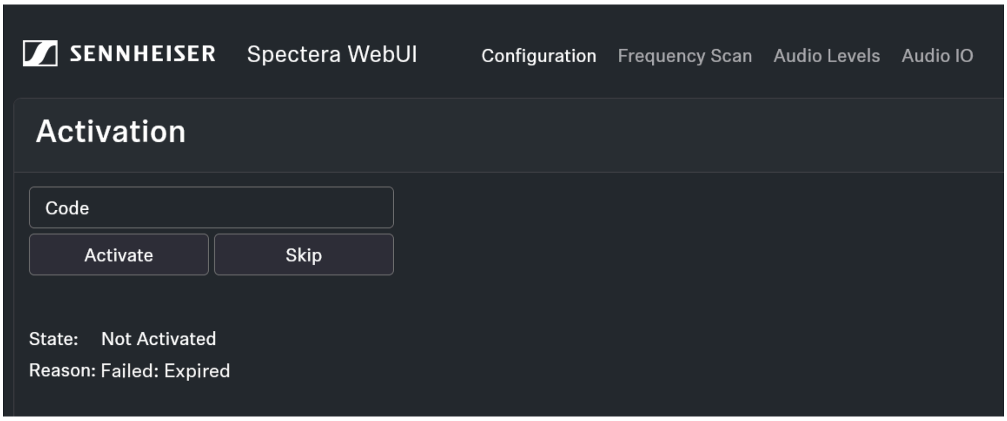


- ▶ Please connect your Base Station directly to a network with Internet access via a switch or router. For more information, refer to the chapter Connecting to a network.
- ▶ Direct connections via laptop etc. are not supported for activation!



- ▶ The Internet is only required once for activation.

When you start the device for the first time, your license key is requested.



State: Not Activated

Reason: Failed: Expired

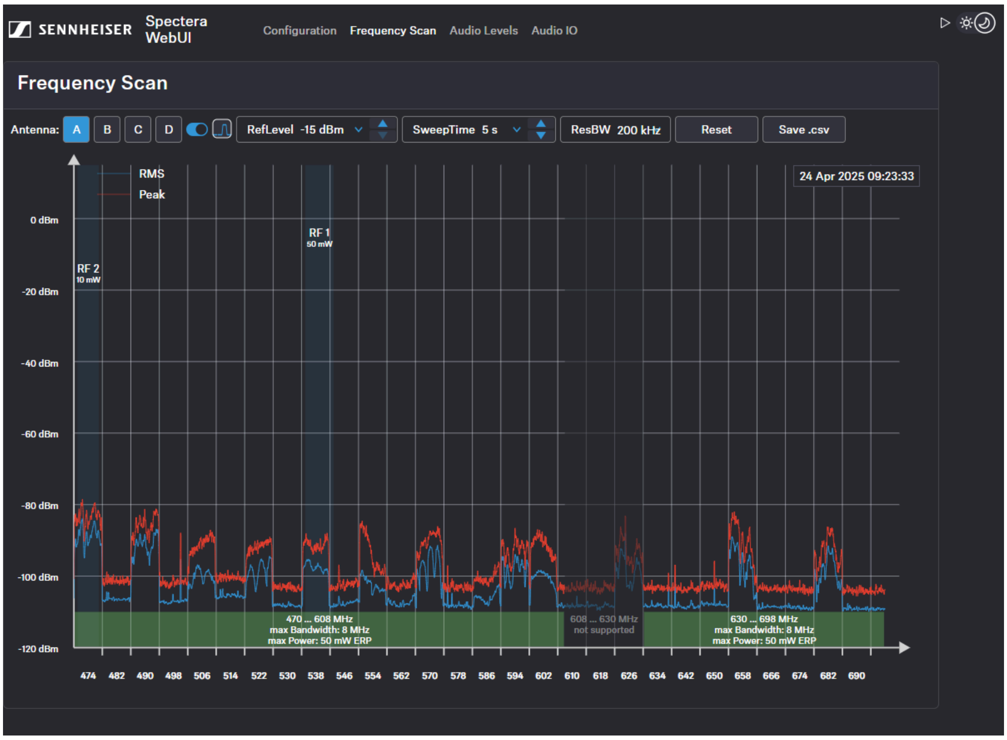
To activate the license:

- ▶ Enter the acquired license and click on **Activate** or on **Skip** to proceed with activation later.

✓ Your license has been activated.

Frequency Scan

You can use an RF scan to examine the current frequency situation of your connected antenna.



Frequency Scan

Antenna: A B C D

RefLevel -15 dBm

SweepTime 5 s

ResBW 200 kHz

24 Apr 2025 09:23:33

i Make sure that no antenna is activated!

You can monitor and control the following settings in the Frequency Scan menu:

- Selecting the antenna (A-D) connected to the Base Station
- Setting the RefLevel (reference level for frequency scan)
- Setting the Sweep time for frequency scan between 2s (fast update rate) and 60s (slow update rate)
- Setting the resolution bandwidth
- Resetting the peak trace
- Saving all settings to a `.csv` file

Scanning the RF frequency

You can run a frequency scan to check the current frequency situation in your surrounding area.

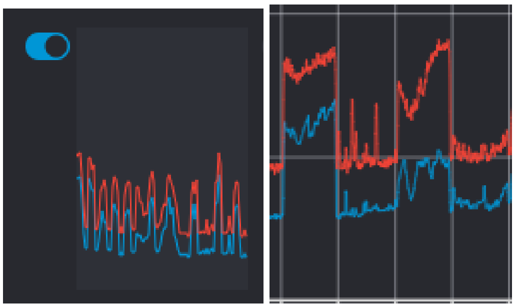
The frequency scan provides an overview of the frequency situation in your location. You can save the antenna configuration as a .csv info file. This file can be used as a backup file to recapitulate your settings or as local frequency information for your specific environment. You can scan the frequencies of all antennas connected to the Base Station.

The scan can be initiated:

- via the RF configuration tab to see a small extract without any details or
- via the Frequency Scan tab for a detailed overview of the frequency situation.

The scan results will be displayed in two different curves:

- **Peak** (red) = Maximum value
- **RMS** (blue) = Average power or strength

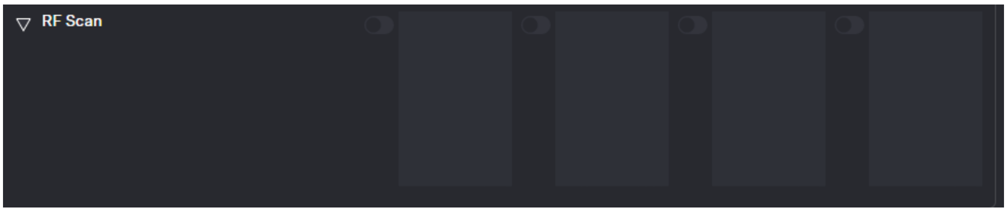


i Please note that the antenna must not be assigned to an RF channel before scanning (see Assigning an antenna to an RF channel).

To scan the RF frequency via the RF configuration tab:

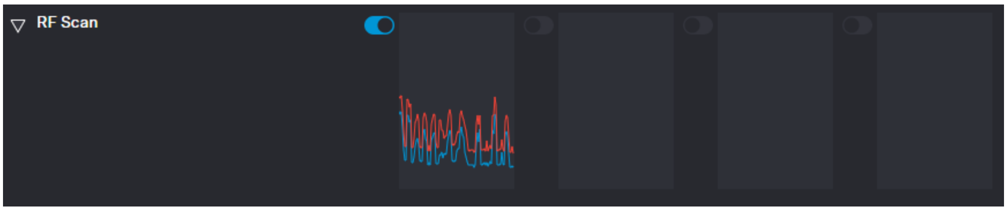
▶ In the top bar, navigate to **Configuration** > **RF Configuration**.

✓ Under the **RF Scan** drop-down menu, there are four toggle switches that enable and disable the scan function for each connected antenna.



▶ Click on the toggle switch of the antenna to be scanned in order to start an immediate scan.

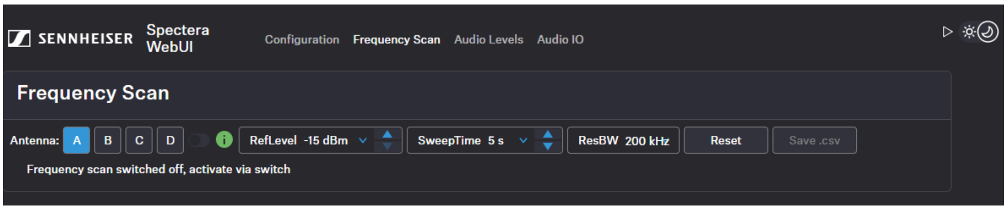
✓ The square is highlighted with a blue dot and the scan result is displayed in a small frequency curve after approx. 5 seconds.



- In order to view the results,
  - click on the small frequency icon or
  - navigate to **Frequency Scan** in the top bar.

To scan the RF frequency via the Frequency Scan tab:

- In the top bar, navigate to the tab **Frequency Scan**.



Frequency Scan

Antenna: A B C D

RefLevel -15 dBm

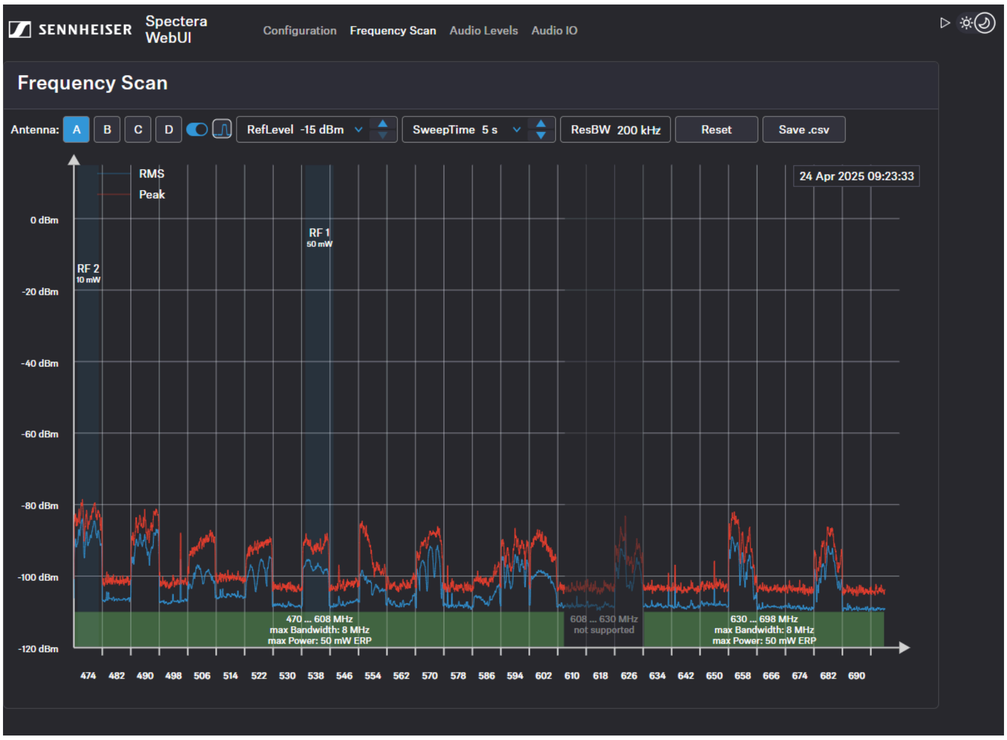
SweepTime 5 s

ResBW 200 kHz

Frequency scan switched off, activate via switch

- Select your antenna to be scanned and adjust your desired settings.
- Switch on the toggle to start the scan.

✓ The frequency scan is started and the result is displayed in a detailed frequency diagram. Supported frequency ranges are shown in green and unsupported ranges in gray.



Frequency Scan

Antenna: A B C D

RefLevel -15 dBm

SweepTime 5 s

ResBW 200 kHz

24 Apr 2025 09:23:33

To reset a scan:

- Click on **Reset**.

✓ The current scan will be reset.

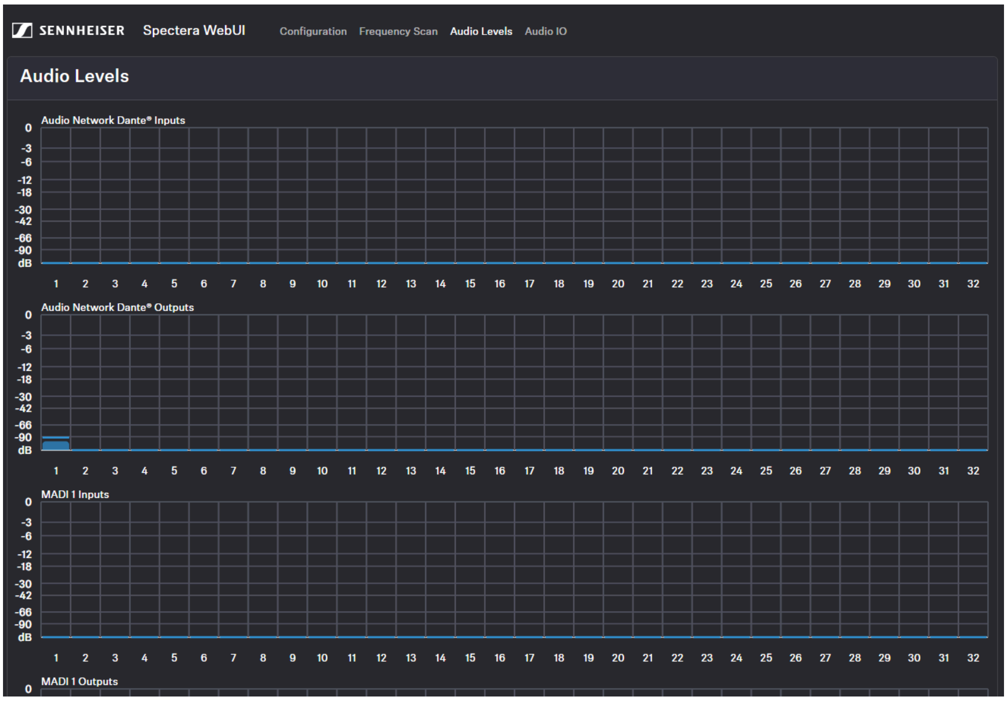
To save the scan results as `.csv`:

- ▶ Click on **Save.csv**.
  - ✓ The antenna configuration has been downloaded locally to your computer as a `.csv` file.

✓ The frequency of your connected antenna has been scanned.

Audio levels

Under Audio Levels you can monitor all interfaces at a glance.



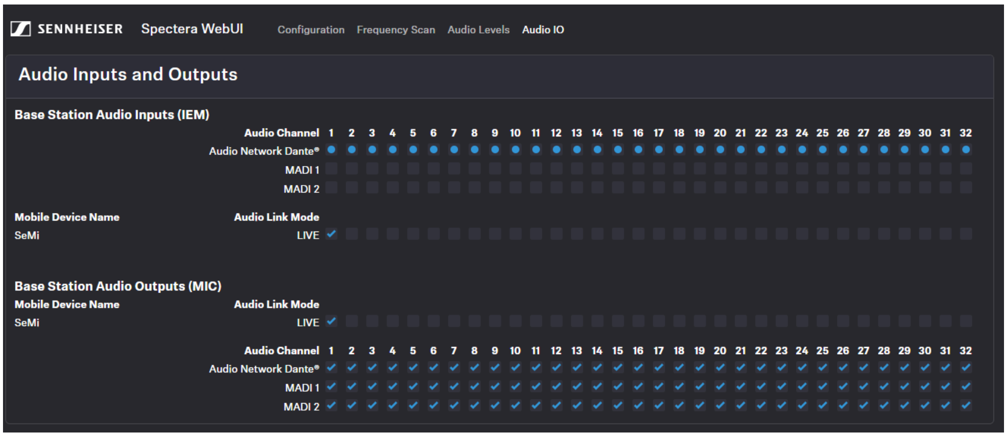
All interfaces are sorted according to their inputs and outputs and displayed visually with a frequency response:

- Dante® Inputs
- Dante® Outputs
- MADI 1 Inputs
- MADI 1 Outputs
- MADI 2 Inputs
- MADI 2 Outputs

Audio inputs and outputs

Here you have an overview of all channels at a glance and can assign the audio network input and output for the link channels directly and easily.

The link modes assigned in the mobile devices are displayed here. You can select the desired channels directly and assign them to your audio network input or output.



Audio Inputs and Outputs

Base Station Audio Inputs (IEM)

Audio Channel	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
Audio Network Dante®	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
MADI 1	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
MADI 2	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

Mobile Device Name	Audio Link Mode																																
SeMi	LIVE	✓	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

Base Station Audio Outputs (MIC)

Mobile Device Name	Audio Link Mode																																
SeMi	LIVE	✓	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

Audio Channel	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
Audio Network Dante®	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
MADI 1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
MADI 2	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

4. Knowledge Base

Central hub for information, resources, and guides with further content on the product and/ or service.

Network guide

This network guide is intended for IT administrators, system integrators and event technicians and serves as an planning and configuration guide for integrating components of the Spectera offering into diverse network environments from small home networks up to enterprise networks.

The guide contains recommendations on network setup for transmission of control data and audio content (via Dante®).

Introduction

This network guide is intended for IT administrators, system integrators and event technicians and serves as an planning and configuration guide for integrating components of the Spectera offering into diverse network environments from small home networks up to enterprise networks.

The guide contains recommendations on network setup for transmission of control data and audio content (via Dante®).

General requirements

Operating systems

The Spectera Base Station as network device is able to be controlled by network-capable PC or Mac devices.

The following system requirements apply for operation with Spectera WebUI and Sennheiser LinkDesk:

System requirements

- Intel i5 Dual Core processor/M1 Mac/or similar
- 16 GB RAM
- At least 4 GB hard disk space (5 GB for Mac devices)
- Gigabit LAN interface
- Windows® 10, 11, Server 2019, Server 2022 (x64) or higher
- Mac OS Big Sonoma or later
- IPv4 network

Supported web browsers for Spectera WebUI

- Google Chrome: 125 or later
- Microsoft Edge: 125 or later
- Mozilla Firefox: 128 or later
- Apple Safari: 17 or later
- JavaScript must be activated

Network

Bandwidth and speed

When it comes to bandwidth requirements for high-quality audio, there are a number of factors that can affect the input and output of the audio. The network speed required for especially audio transmission via Dante® should be as high as possible to ensure a smooth listening experience. As a rule, the minimum bandwidth for transmitting and receiving audio at the Spectera Base Station is approximately the following:

> “The majority of audio used in professional settings is PCM (uncompressed), sampled at 48 kHz and a bit depth (word length) of 24 bits. Dante® audio is unicast by default but can be set to use multicast for cases of one-to-many distribution.
>
> - Dante® packages audio into flows to save on network overhead.
> - Unicast Audio flows contain up to 4 channels. The samples-per-channel can vary between 4 and 64, depending on the latency setting of the device. Bandwidth usage is about 6 Mbps per typical unicast audio flow.
> - Bandwidth for multicast flows is dependent on the number of audio channels used. Bandwidth is about 1.5 Mbps per channel.
>
> ”

Source: Audinate Dante Information for Network Administrators (PDF)

Internet access

For both components Spectera Base Station and Sennheiser LinkDesk we recommend to provide permanent Internet access. Please refer to chapter Ports, protocols and services to get more details about used Internet services.

i At least for the initial product activation of the Spectera Base Station and for the use of the optional Sennheiser Account Login in Sennheiser LinkDesk it is mandatory to have a direct Internet access and DNS support.

i At the moment it is not possible to manually configure any network proxy and DNS server at Spectera Base Station. Please make sure to provide direct Internet access e.g. via white-listing the device and any used port, protocol and domain and using DHCP to provide DNS server settings.

Network infrastructure (switches/cables)

Generally any kind of unmanaged or managed network switch can be used for control and audio data transmission. For proper operation of Dante® some fundamental requirements need to be fulfilled:

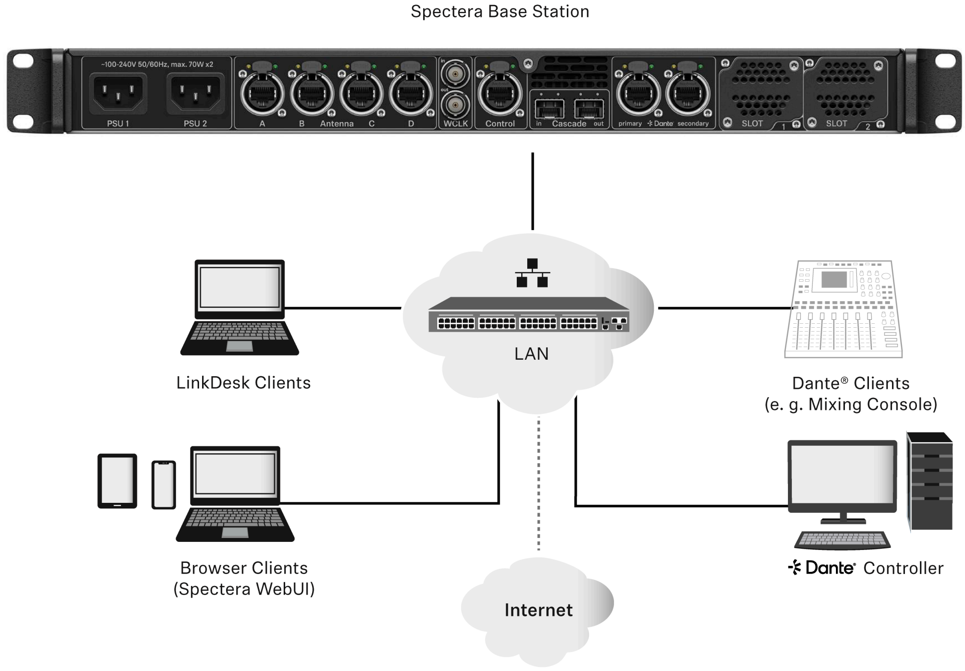
- When using managed switches, ensure that they allow EEE (Energy Efficient Ethernet or "Green Ethernet") to be disabled. Make sure that EEE is disabled on all ports used for real-time Dante traffic.
- When using unmanaged switches, do not use switches that support the EEE function, because it cannot be disabled.
- Make sure that the switch supports Quality of Service (QoS) and that it is enabled.
- For larger networks, consider using VLANs to segment audio traffic from other types of network traffic.

> i For further information about that topic, please refer to the: Audinate FAQ - Networks and Switches. Additionally, there is a list of incompatible switches available at Audinate: Audinate List of incompatible EEE switches (PDF)

To ensure a reliable transmission speed of audio and control data with the Spectera Base Station, please use an RJ45 network cable with the CAT5e S/FTP standard or higher.

Network setups

To operate the several components of the Spectera offering they need to be integrated into a network setup, either existing or new. Following figure shows a general overview of the network setup and their participants.



Spectera Base Station

This Sennheiser device has 3 network interfaces. One interface dedicated for control data and two interfaces for audio data (specifically Dante®). There is a primary and a secondary interface for redundancy of the audio transmission.

Sennheiser LinkDesk client

This client can be any host computer (PC or Mac), with the LinkDesk software application installed.

Browser Client (Spectera WebUI)

This client can be any host computer (PC, Mac, Tablet, Smartphone), with a supported web browser installed, accessing the Spectera WebUI.

Dante® client

This can be any device with a Dante® network interface installed. This ranges from Virtual Dante® Soundcards installed on a host computer up to dedicated devices like a Mixing Console.

Dante® Controller

This is typically host computer (PC or Mac), with the Dante® Controller software application installed. This application configures and controls all the Dante® devices and audio streams inside the network.

LAN with network switches and router

This can be any network switch for routing the network communication inside the Local Area Network (LAN) and any network router providing the gateway to other networks and to the Internet.

Spectera Base Station - network configuration

Depending on the desired network address configuration all network interface (Control and both Dante®) can be operated in following IP Modes with IPv4 only:

- Fixed/Static IP
- Auto IP (DHCP or Zeroconf)

Additionally it can be configured if mDNS/DNS-SD information shall be published by the device or not.

i **Dante® restrictions**

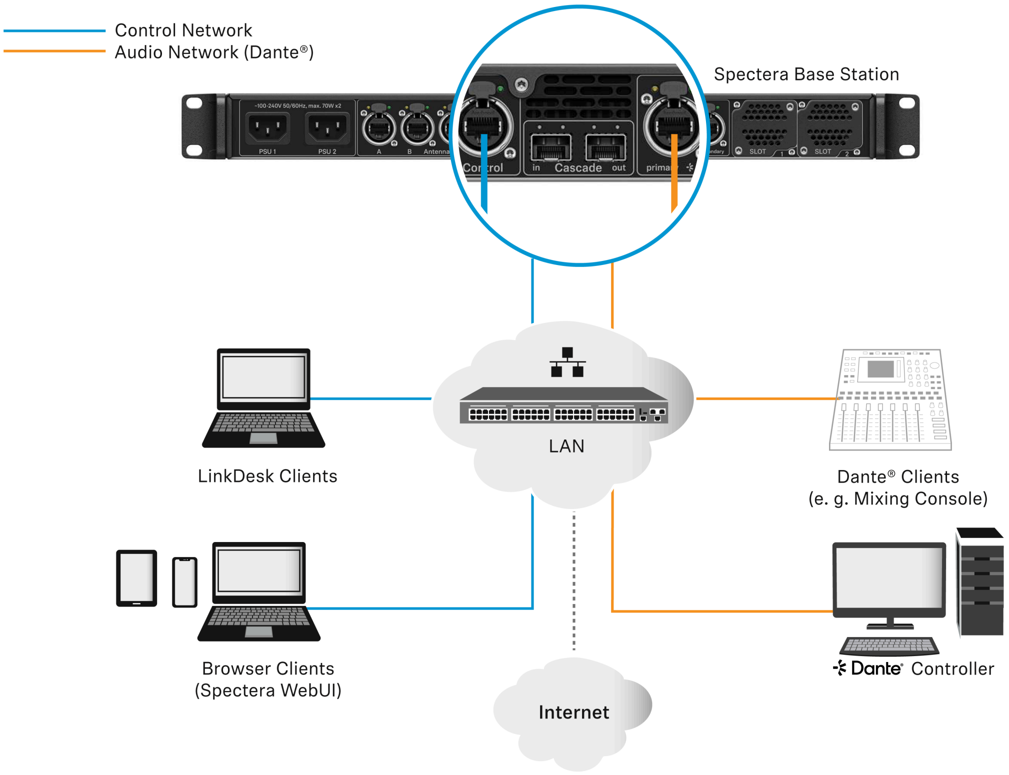
- It is not possible to deactivate the Dante® functionality for the both Dante® ports.
- Dante® ports are shutdown when the device is in standby mode.
- Network configuration of Dante® ports can only be done via Dante® Controller software application.
- By default the Dante® ports are configured to Auto IP. If Fixed/Static IPs have been configured and the device cannot be reached anymore, the IP Mode can only be reset to Auto IP by a Factory Reset of the device.
- The Dante primary and secondary networks must not be directly connected to each other (network loop). Make sure you always connect the Base Station Dante network ports to two different networks that do not run via a common switch.

Shared Network Mode

In Shared Network Mode both networks for Control and Dante® are using the same physical network infrastructure.

- Configure both Control and Dante® networks over one switch / router.
- Use two different IPs to address the Control network and the Dante® network separately.

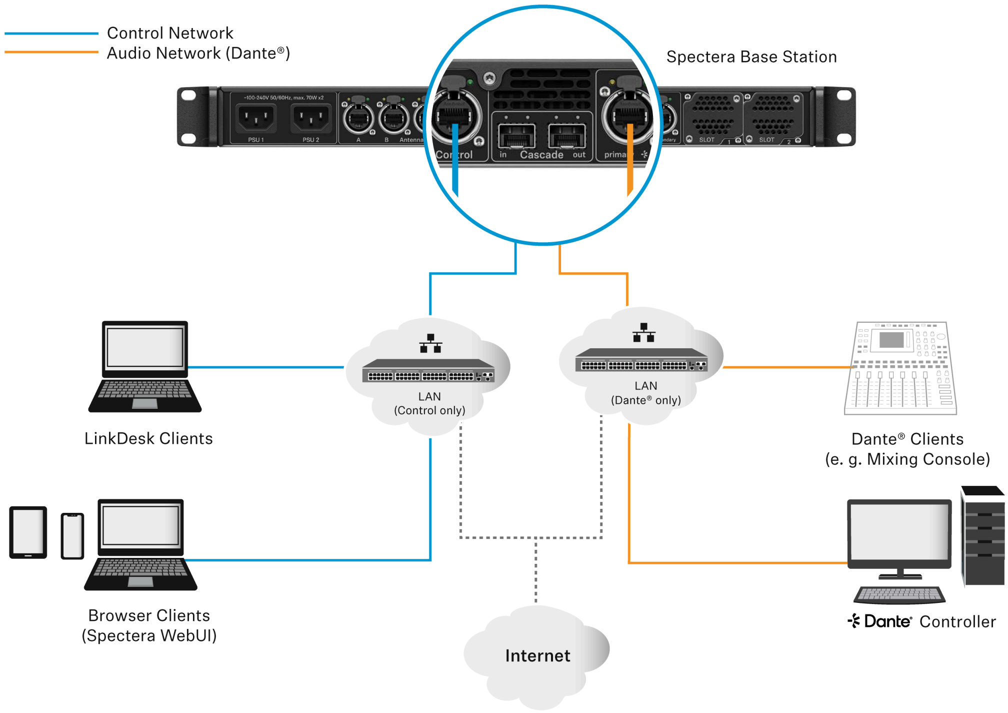
i The Spectera Base Station can not be configured to use VLAN tagging (IEEE 802.1Q) at its network ports. Still it is possible to use network switches that support VLANs to separate the Control and Dante® traffic within the same physical network. Please make sure that the switch is configured to forward untagged traffic from both networks to the respective ports of the Base Station. Additionally, make sure that the switch is configured to forward multicast traffic for the Dante® network.



Split Network Mode

In Split Network Mode both networks for Control and Dante® are using different physical network infrastructure.

- Configure both Control and Dante® networks over two different switches / routers.
- Use two different IPs to address the Control network and the Dante® network separately.


Control Network
Audio Network (Dante®)
Spectera Base Station
Control
in Cascade out
primary
LAN
(Control only)
LAN
(Dante® only)
LinkDesk Clients
Dante® Clients
(e. g. Mixing Console)
Browser Clients
(Spectera WebUI)
Internet
Dante® Controller

Ports, protocols and services

Spectera Base Station

In order to use the Spectera Base Station device in a network, certain ports must be enabled (especially for the organization/enterprise firewall) for communication between software and devices.

> i If necessary, please contact the local administrator to configure the required ports.

Ports - Base Station Control Network Interface

Address	Port	Protocol	Type	Service	Usage
Requests from device to ...					
Sennheiser License Server address[1]	80	HTTPS (TCP)	Unicast	Sennheiser License Server	Activation of devices
ANY address of time server (see list of **NTP time server pools**)	123	NTP	Unicast	NTP Time Server	Synchronize system time
224.0.0.251	5353	mDNS (UDP)	Multicast	mDNS, DNS-SD	(optional - if desired) Device/Service Discovery
Requests to device from ...					
ANY IP of SSCv2 client	443	HTTPS (TCP)	Unicast	SSCv2 - Spectera Base Station API	Monitor+Control communication from clients
[1] my.nalpeiron.com					

NTP servers

To correctly operate with licenses and certificates, the Spectera Base Station needs a correct system time. The device will use the well-established NTP mechanism from the IP protocol stack to synchronize clock between a time server in a network and the client inside the device.

Currently for an IT administrator or system integrator it is not possible to manually configure a dedicated NTP server to be used by the Spectera Base Station. Being able to configure a dedicated NTP server manually is a planned feature for an upcoming release.

The device behaves the following way:

- If a time server configuration has been provided via DHCP or manually, it tries to connect and sync to that time server first.
- Otherwise the device is trying to access any server of following list of time server pools worldwide publicly available.

> i An IT administrator has to assure to provide Internet access to at least one of the server pools and to provide DNS settings via DHCP to the device.

List of NTP time server pools:

- pool.ntp.org
- time.nist.gov
- time.aws.com
- time.cloudflare.com

Ports - Base Station Dante® Network Interfaces

Spectera Base Station requires several ports to be opened for both Dante® Network Interfaces to operate properly. For the list of ports and more detailed information, please refer directly to the Dante® website: Audinate FAQ - Networks and Switches.

Spectera WebUI

In order to use the Spectera WebUI, certain ports must be enabled (especially for the organization/enterprise firewall) for communication between software and devices.

> i If necessary, please contact the local administrator to configure the required ports.

Port requirements

Address	Port	Protocol	Type	Service	Usage
Requests from host to ...					
ANY IP of a Base Station	443	HTTPS (TCP)	Unicast	SSCv2 - Spectera Base Station API	Monitor+Control communication to devices
Sennheiser User Insights addresses [1]	443	HTTPS (TCP)	Unicast	Sennheiser User Insights	Analytics of usage and operational data

[1] sennheiseruserinsights.matomo.cloud

cdn.matomo.cloud

Sennheiser LinkDesk

In order to use the Sennheiser LinkDesk software, certain ports must be enabled (especially for the organization/enterprise firewall) for communication between software and devices.

> i If necessary, please contact the local administrator to configure the required ports.

Port requirements

Address	Port	Protocol	Type	Service	Usage
Host Internal					
LOCALHOST	54352	HTTPS (TCP)	Unicast	LinkDesk backend	Internal backend communication
Requests from host to ...					
ANY IP of a Base Station	443	HTTPS (TCP)	Unicast	SSCv2 - Spectera Base Station API	Monitor+Control communication to devices
Sennheiser CIAM addresses [1]	443	HTTPS (TCP)	Unicast	Sennheiser CIAM	Sennheiser account Sign-in/Log-in
Sennheiser User Insights addresses [2]	443	HTTPS (TCP)	Unicast	Sennheiser User Insights	Analytics of usage and operational data
Requests to host from ...					
224.0.0.251	5353	mDNS (UDP)	Multicast	mDNS, DNS-SD	(optional - if desired) Device/service discovery

[1] accounts-pro-emea.sennheiser-cloud.com

b2c-config.sennheisercloud.com

[2] sennheiseruserinsights.matomo.cloud

cdn.matomo.cloud

Best practice

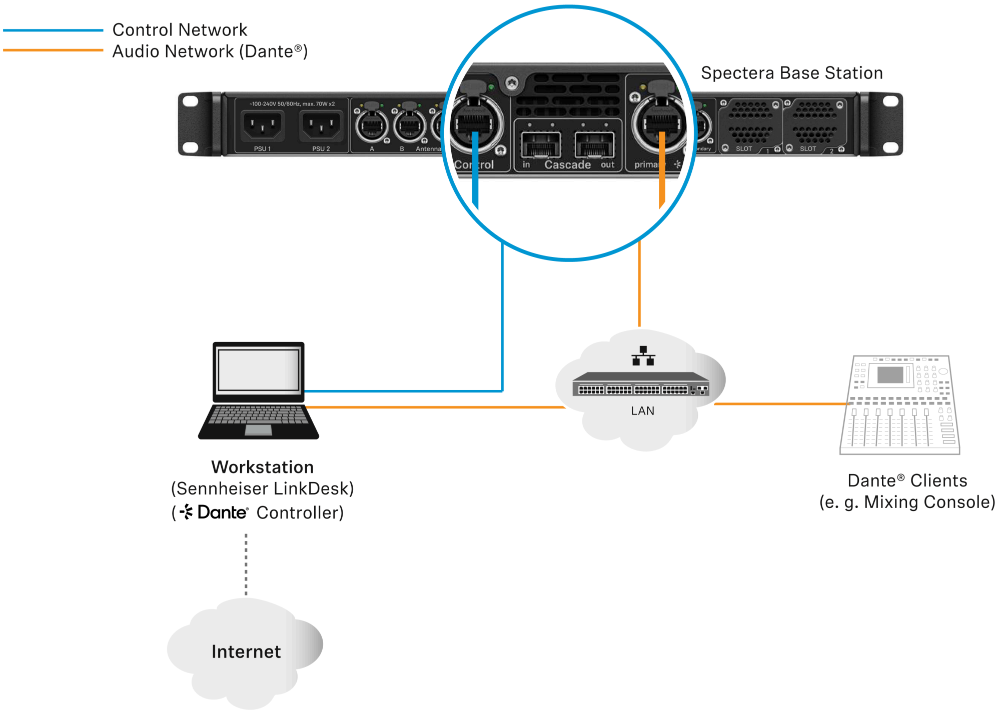
Sharing Internet connection in small network setups

It is possible to operate the Spectera offering without dedicated router networks e.g. in really small setups, but we do recommend to always use some kind of home network router for trouble-free usage.

Especially for providing Internet access to Spectera Base Station it is possible to use the builtin functionality of Windows and MacOS for Internet Connection Sharing.

> **i** For enterprise networks we DO NOT RECOMMEND the usage of Internet Connection Sharing. Most of the times it is even prohibited by enterprise IT policy to use such service.

The network setup might look like this:



Inside this setup one workstation is used for all client software applications (Sennheiser LinkDesk, Spectera WebUI, Dante® Controller). Either two separated wired network interface are used for control and audio (Dante®) or one interface gets shared. Please be aware that in such setups (typically) no DHCP service is activated. Use either manual IP settings or ZeroConf configuration.

For Internet Connection Sharing typically an existing network connection (Wi-Fi or Ethernet) with Internet access gets shared with another selected network interface of the host.

In order to share your Internet connection on Windows:

- Connect your client device to your host PC using an Ethernet cable. If either device doesn't have a free Ethernet port, use a USB-to-Ethernet adapter.
- Go to the **Network Connections** menu. The easiest way to get there is by searching for "Network Connections" in the Windows Search box.
- Right-click on the network adapter connected to the Internet (for example, Wi-Fi or modem), and then select **Properties**.
- Toggle **Allow other network users to connect** to **ON** from the Sharing tab and select the relevant Ethernet port from the pull-down menu.

> i Note that, if you have VPN software installed, you may see a lot of virtual Ethernet ports on your list and you'll need to pick the real one.

✓ After you click OK, Internet should flow to your client device over its Ethernet port. For more details on sharing an Internet connection please refer to the Microsoft Support page.

In order to share your Internet connection on MacOS:

- On your Mac, choose **Apple menu** > **System Settings**.
- Click on **General** in the sidebar and then on **Sharing** (you may need to scroll down).
- Turn on **Internet Sharing** and click on **Configure**.
- Click the **Share your connection** from pop-up menu.
- Choose the Internet connection you want to share ((For example, if you're connected to the Internet over Wi-Fi, choose Wi-Fi).
- Under **To devices using**, turn on the port other devices can use to access the shared internet connection. (For example, if you want to share your Internet connection over Ethernet, select Ethernet).

> i If you're sharing to devices using Wi-Fi, configure the Internet-sharing network, then click **OK**.

- Click on **Done**.

> i For more details on sharing an Internet connection please refer to the Apple Support page.

✓ Your Internet connection will be shared on MacOS/Windows.

Security guide

This security guide provides essential information and best practices for IT administrators, system integrators, and event technicians to ensure robust security measures are implemented effectively.

Professional audio systems, extensively deployed in environments such as broadcasting, live events, and corporate settings, are increasingly integrated into enterprise networks — making them susceptible to threats like unauthorized access, data interception, and signal interference. To ensure secure deployment and system integrity, Sennheiser enforces the highest security standards across all products, supported by robust protective measures and comprehensive management practices.

- **Security Principles and System Design:**

  Sennheiser embeds security from product development through regular risk assessments and secure configurations, following a “security by design” approach. Compliance with international standards ensures consistent protection and proactive threat mitigation.

- **Communication Security and Encryption:**

  Industry-standard encryption protocols like AES-256 and TLS protect audio and control data from interception and unauthorized access. Secure methods such as HTTPS and REST APIs are used for networked and third-party integrations.

- **Authentication and Access Control:**

  Role-based authentication and device claiming validate users and devices before granting access. b credentials and regular updates maintain system integrity and prevent unauthorized access.

- **Network Configuration and Interfaces:**

  Enable only essential ports, segment networks, and apply firewall rules for secure operation. Proper configuration of protocols like Dante®, mDNS, and Bluetooth® is critical for a robust network infrastructure.

This guide provides comprehensive measures to protect professional audio systems from threats through secure design, encryption, authentication, and best practices throughout the system lifecycle.

Introduction

This security guide provides essential information and best practices for IT administrators, system integrators, and event technicians to ensure robust security measures are implemented effectively.

Professional audio systems, extensively deployed in environments such as broadcasting, live events, and corporate settings, are increasingly integrated into enterprise networks — making them susceptible to threats like unauthorized access, data interception, and signal interference. To ensure secure deployment and system integrity, Sennheiser enforces the

highest security standards across all products, supported by robust protective measures and comprehensive management practices.

- **Security Principles and System Design:**

  Sennheiser embeds security from product development through regular risk assessments and secure configurations, following a “security by design” approach. Compliance with international standards ensures consistent protection and proactive threat mitigation.

- **Communication Security and Encryption:**

  Industry-standard encryption protocols like AES-256 and TLS protect audio and control data from interception and unauthorized access. Secure methods such as HTTPS and REST APIs are used for networked and third-party integrations.

- **Authentication and Access Control:**

  Role-based authentication and device claiming validate users and devices before granting access. b credentials and regular updates maintain system integrity and prevent unauthorized access.

- **Network Configuration and Interfaces:**

  Enable only essential ports, segment networks, and apply firewall rules for secure operation. Proper configuration of protocols like Dante®, mDNS, and Bluetooth® is critical for a robust network infrastructure.

This guide provides comprehensive measures to protect professional audio systems from threats through secure design, encryption, authentication, and best practices throughout the system lifecycle.

Key product security features

Key security features of Spectera devices and software tools are detailed, emphasizing best practices for IT administrators to ensure secure communication and data protection.

Spectera devices (Base Station, DAD, and Mobile Devices (SEK)) and software tools such as **Spectera Base Station WebUI** and **Sennheiser LinkDesk** support enhanced security measures, ensuring both a secure connection between devices via radio and secure data transfer over the network. It offers the following security features:

- **AES-256 Link Encryption:**

  The AES-256 Link Encryption protects audio and control communication between devices.
- **Control Protocol Encryption:**

  The WebUI is always using encrypted HTTPS communication. The SSCv2 protocol secures the communication between devices and software tools via HTTPS.
- **Device Claiming & Authentication:**

  The Device Claiming & Authentication feature ensures authorized control access using passwords.
- **Dante® Media Encryption:**

  The Dante® Media Encryption is an optional channel encryption for Dante networks

AES-256 Link Encryption

All wireless communication between the Spectera devices will be protected with AES-256, a top-tier encryption standard designed to safeguard sensitive data.

Link Encryption includes the following interfaces:

- The connection between the Base Station and Mobile Devices for audio transmission.
- The connection between the Base Station and Mobile Devices for device setting synchronization.

i The AES-256 Link Encryption is always enabled and can not be disabled.

Control Protocol Encryption

All control communication over the network to the Base Station is encrypted and authenticated.

It offers end-to-end security, utilizing HTTPS (TLS 1.3). Communication to the Sennheiser license server is encrypted on application level.

The Protocol Encryption is always enabled and can not be disabled.

Device Claiming & Authentication

Device claiming and authentication enhance security by requiring password protection for device access and ensuring only authorized users can modify settings through encrypted connections.

The device access via network control API and WebUI of Spectera Base Station and via Sennheiser LinkDesk is password protected, to avoid configuring the device by unauthorized actors inside the network.

The Device Authentication is always enabled and can not be disabled.

Benefits of device claiming

- **Device Claiming Feature:**

  Device claiming is a feature of the Sennheiser LinkDesk and Spectera Base Station WebUI that allows the user to claim ownership of their Sennheiser devices, providing an extra layer of security and control.
- **Device Assignment:**

  It allows assigning a device to one or more remote installations, which prevents any unauthenticated device control within the network.
- **Initial Configuration:**

  As part of the initial configuration, users claim a device by configuring a mandatory device password.
- **Usability:**

  Within an installation, multiple software applications can be used simultaneously with this device password for optimal usability
- **Security Measures:**

  Once a device is claimed, its settings can only be viewed and modified via an encrypted connection, which requires entry of the configuration password.

Dante® Media Encryption (available as of Spectera Dante® firmware Brooklyn3 version 1.1.0)

Dante® Media Encryption extends the security benefits of using Dante® on your network by concealing the media content during transmission between devices.

Dante® utilizes the Advanced Encryption Standard (AES) with a 256-bit key to provide industry-leading media protection.

Concealing the contents of media packets prevents malicious or unauthorized users eavesdropping or interfering with Dante media traffic.

i By default, Dante Media Encryption is disabled, since encryption can only be configured by using the Dante Director application. Please refer to the Audinate documentation for detailed information on Dante® encryption, on how to enable and configure encryption and to update the Dante® firmware:

- Dante Media Encryption: Audinate/Media Encryption
- Updating Dante® firmware: Dante Updater

How to use the security features

The following section explains how you can use the various security features both via the device itself and via supported software applications.

Certificates

Spectera Base Station is using a self-signed certificate for network communication.

The certificate is generated in factory and will be renewed with every factory reset.

> i Currently it is not possible to replace the certificate with a CA-signed certificate.

When accessing the Spectera WebUI with a browser for the first time you will get a security warning informing about an unknown certificate. The security warning depends on the browser you are using. Depending on your browser, click on Advanced or Show Details (Safari) and then on:

- Microsoft Edge: **Continue to localhost (unsafe)**
- Google Chrome: **Proceed to localhost (unsafe)**
- Firefox: **Accept the Risk and Continue**
- Apple Safari: **[...] visit this Website** > **Visit Website**
- or similar (other browsers)

In order to prevent man-in-the-middle (MITM) attacks, Sennheiser LinkDesk has some built-in security measures. Because of these measures, you might receive a certificate mismatch warning while working with a Base Station. In some cases, these can occur even though there is actually no security issue. These are:

- The Base Station has been factory reset since the last connect. In this case you can safely confirm the connection and proceed when encountering the mismatch warning.
- A different Base Station has been connected via the same IP address. In this case please verify if the IP Address you are using is indeed the correct IP Address of the intended Base Station.

Device authentication

The devices access via network is password protected and the device must be claimed in the control software before use.

You can claim the Base Station via:

- LinkDesk (see Claiming single device (LinkDesk)) or
- WebUI (see Claiming single device (WebUI)).

i Please note that the new password must meet the following requirements:

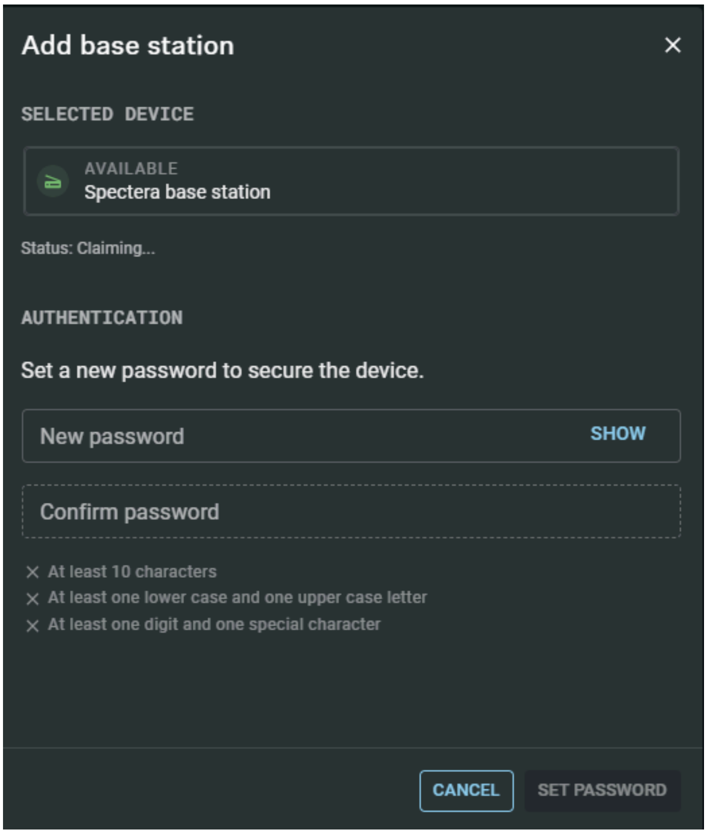
- At least ten characters
- At least one lowercase letter
- At least one uppercase letter
- At least one number
- At least one special character: !#$%&()*+,-./:;<=>?@[]^_{|}~
- Maximum length: 64 characters

Claiming single device (LinkDesk)

Instructions for claiming a single device in Sennheiser LinkDesk.

To claim your Base Station:

- In your production card, activate the function **DEVICE SYNCHRONIZATION** on the left-hand side of the top bar.
- Click on the + symbol in the **BASE STATIONS** bar on the right.
- Enter the correct IP address of the Base Station and click on **Search**.
  - If the device is in a factory default state and the original password is still assigned, it will be automatically detected and applied. Next, a new password has to be set:



Add base station

SELECTED DEVICE

AVAILABLE
Spectera base station

Status: Claiming...

AUTHENTICATION

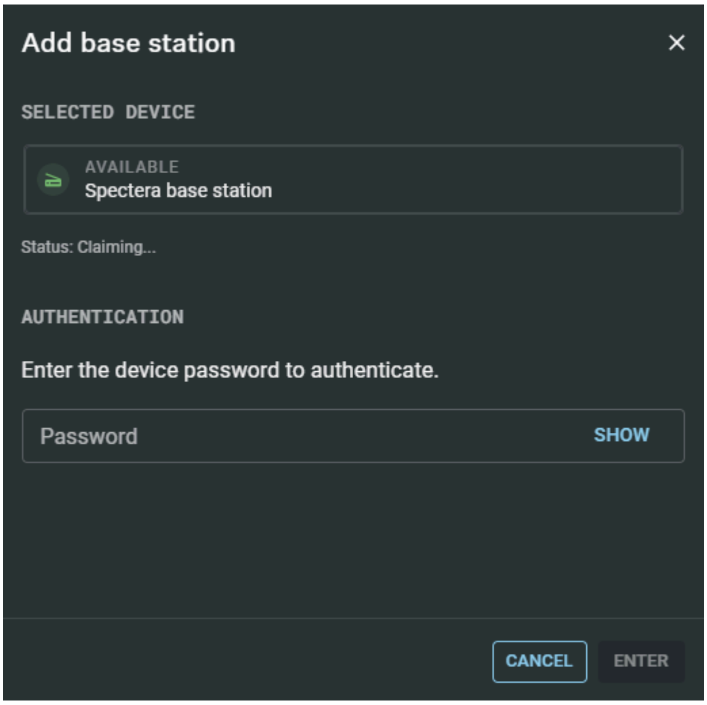
Set a new password to secure the device.

New password

Confirm password

✕ At least 10 characters
✕ At least one lower case and one upper case letter
✕ At least one digit and one special character

  - If the device was previously claimed by another Sennheiser LinkDesk or Spectera WebUI instance, the previously set password must be entered:



Add base station

SELECTED DEVICE

AVAILABLE
Spectera base station

Status: Claiming...

AUTHENTICATION

Enter the device password to authenticate.

i If you cannot remember the previously set password, please perform a factory reset of the device. After the reset, the default password for Spectera will be automatically applied by the software.

▶ Set a new device password (if you are logging in for the first time) or enter the password you have already assigned for authentication (if you have already logged in).

i Please note that the new password must meet the following requirements:

- At least ten characters
- At least one lowercase letter
- At least one uppercase letter
- At least one number
- At least one special character: !#$%&()*+,-./:;<=>?@[]^_{|}~
- Maximum length: 64 characters

✓ Your Base Station has been claimed successfully.

Claiming single device (WebUI)

Instructions for claiming a single device in Spectera WebUI.

To claim your Base Station:

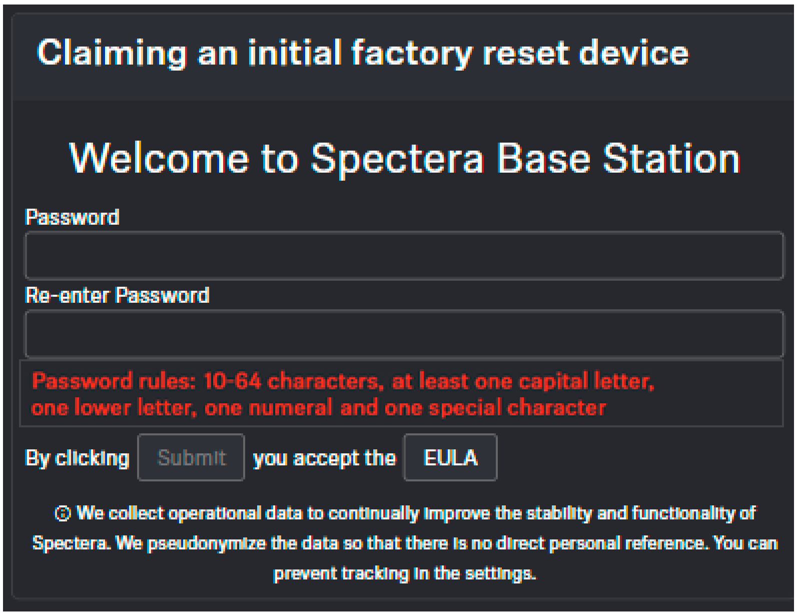
▶ Depending on the firmware version, enter the following URL into your browser:
- Firmware 0.8.x: `https://deviceIP/specteracontrol/index.html`
- Firmware ≥1.0.0: `https://deviceIP/specterawebui/index.html`

> **i** Since the certificate is unknown to your browser, a security warning is displayed the first time you run the application. The security warning depends on the browser you are using.

▶ Depending on your browser, click on **Advanced** and then on:
- **Continue to localhost (unsafe)** (Microsoft Edge)
- **Proceed to localhost (unsafe)** (Google Chrome)
- **Accept the Risk and Continue** (Firefox)
- or similar (other browsers).

✓ The WebUI displays the following options depending on the state of the device:

If•the device is in a factory default state and the original password is still assigned, it will be automatically detected and applied. Next, a new password has to be set:



Claiming an initial factory reset device

Welcome to Spectera Base Station

Password

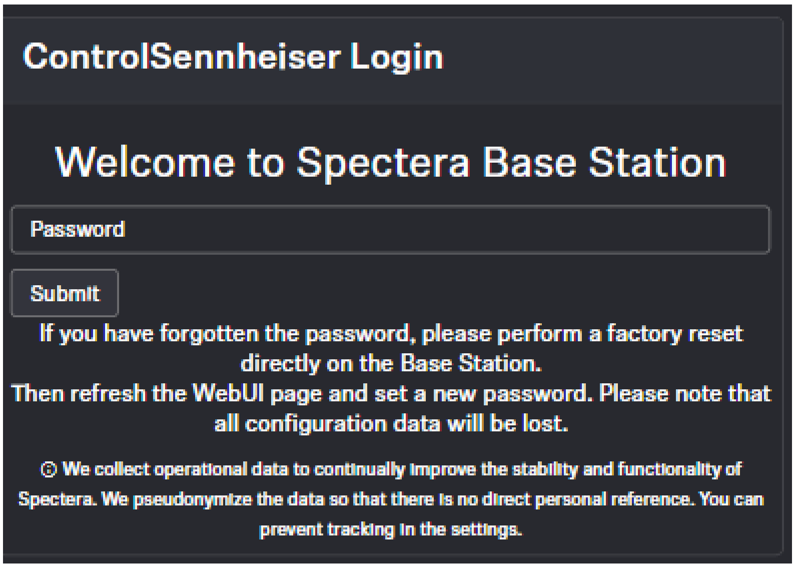
Re-enter Password

Password rules: 10-64 characters, at least one capital letter, one lower letter, one numeral and one special character

By clicking Submit you accept the EULA

ⓘ We collect operational data to continually improve the stability and functionality of Spectera. We pseudonymize the data so that there is no direct personal reference. You can prevent tracking in the settings.

If•the device was previously claimed by another Sennheiser LinkDesk or Spectera WebUI instance, the previously set password must be entered:



ControlSennheiser Login

Welcome to Spectera Base Station

If you have forgotten the password, please perform a factory reset directly on the Base Station.
Then refresh the WebUI page and set a new password. Please note that all configuration data will be lost.

ⓘ We collect operational data to continually improve the stability and functionality of Spectera. We pseudonymize the data so that there is no direct personal reference. You can prevent tracking in the settings.

i If you cannot remember the previously set password, please perform a factory reset of the device. After the reset, the default password for Spectera will be automatically applied by the software.

▶ Set a new device password (if you are logging in for the first time) or enter the password you have already assigned for authentication (if you have already logged in).

▶ Click on **Submit**.

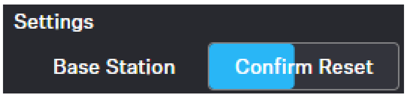
✓ Your Base Station has been claimed successfully.

Resetting the device password (Spectera Base Station)

The device password can only be reset through a factory reset (either performed directly on the device or remotely via WebUI):

To reset the Base Station remotely:

- ▶ In the top bar, navigate to **Configuration** > **Base Station**.
- ▶ Click on **Settings** and then on **Factory Reset**.
  - ✓ A countdown timer will be displayed (highlighted in blue).

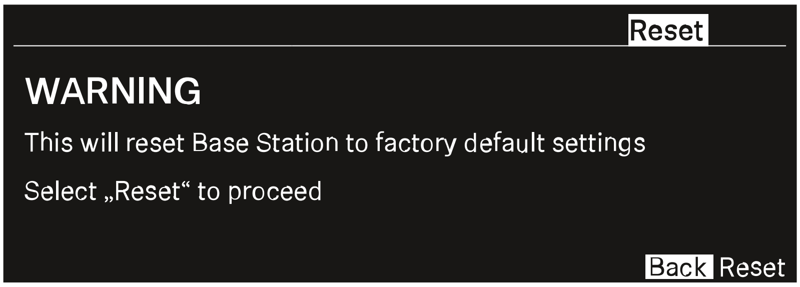


Settings

- ▶ Press **Confirm Reset** to confirm the factory reset.

To reset the Base Station to its factory default settings using the device:

- ▶ On the Base Station, rotate the jog-dial and navigate to the menu **Reset**.
- ▶ Press the jog-dial to enter the menu.
  - ✓ A warning will appear.



Reset

WARNING

This will reset Base Station to factory default settings

Select „Reset“ to proceed

- ▶ Rotate the jog-dial to **Reset**.
- ▶ Press the jog-dial again.
  - ✓ The Base Station will be set back to factory settings and reboot.

> **i** After rebooting, check the IP address as it may have changed.

Troubleshooting

This chapter provides a systematic approach for identifying and resolving issues that may occur during the startup or operation of Spectera.

Depending on the specific problem, click on the relevant chapter to identify possible causes and apply potential solutions.

License activation fails

Condition

An error occurs during license activation.

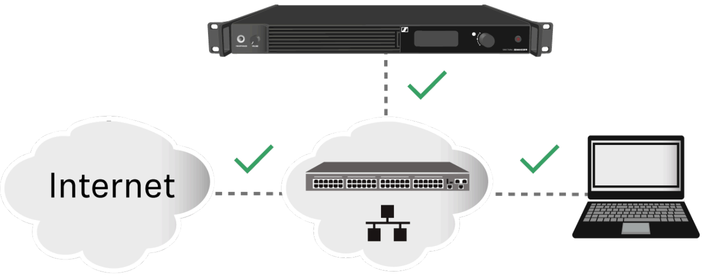
Causes

The three most common causes of activation errors are as follows:

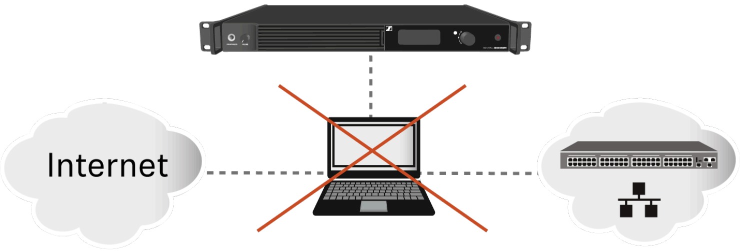
1. The Base Station was not connected properly and has no Internet connection (see Solution 1: Establish a proper connection of the Base Station to the Internet).
2. The license server and/or NTP time server are/is unreachable due to missing port permissions, preventing license key authorization and system clock synchronization (see Solution 2: Open required ports for license activation and system clock synchronization).
3. The license key was entered incorrectly or has already been activated and is in use with another Base Station (see Solution 3: Check the activation code and contact support if necessary).

Solution 1: Establish a proper connection of the Base Station to the Internet

▶ Please connect the Base Station directly to a network with Internet access via a switch or router.



- Direct connections via laptop etc. are only supported in certain network configuration (see Sharing Internet connection in small network setups). To eliminate this issue, please avoid a direct connection with your device for license activation.



Solution 2: Open required ports for license activation and system clock synchronization

- Please contact your IT administrator to provide Internet access to the License Server and any NTP server by opening the required network ports and to provide DNS settings via DHCP to the device.

Address	Port	Protocol	Type	Service	Usage
my.nalpeiron.com	80	HTTPS (TCP)	Unicast	Sennheiser License Server	Activation of devices
ANY (see list of NTP servers)	123	NTP	Unicast	NTP Time Server	Synchronize system time

i You can find the complete overview of all ports at Ports, protocols and services.

Solution 3: Check the activation code and contact support if necessary

- Please verify that you have correctly entered the Activation Code, or check if someone else has already used the code to activate another Base Station.
- If the code has already been used for activation, please reach out to Sennheiser Customer Support.

No device access via the WebUI

Condition

The device cannot be accessed via the self-hosted WebUI.

Cause

The wrong device IP or URL schema is being used in the browser.

Solution

▶ Find out the correct IP of the Base Station (see **Network**).

▶ Enter the correct IP using the correct URL schema depending on the initial firmware version:

- Firmware ≤ 0.8.x use `https://deviceIP/specteracontrol/index.html`.
- Firmware ≥ 1.x.x use `https://deviceIP/`.

✓ In some cases the internet browser might have trouble showing the page. Please use the LinkDesk software sennheiser.com/linkdesk.

The Base Station cannot be found

Condition

The Base Station cannot be found via LinkDesk / WebUI / Dante Manager.

Cause

The required ports for communication with the Base Station have not been made accessible.

Solution

▶ Depending on the use case, please make the necessary ports available for the Base Station, so that data traffic can flow unrestricted:

- Spectera Base Station
- Sennheiser LinkDesk
- Dante®

5. Technical Specifications

System requirements and ports requirements for inbound and outbound traffic.

System requirements

- Intel i5 Dual Core processor/M1 Mac/or similar
- 16 GB RAM
- Gigabit LAN interface
- Windows® 10 or higher
- Mac OS Big Sonoma or later
- IPv4 network

Supported web browsers for Spectera WebUI

- Google Chrome: 125 or later
- Microsoft Edge: 125 or later
- Mozilla Firefox: 128 or later
- Apple Safari: 17 or later
- JavaScript must be activated

Port requirements

Address	Port	Protocol	Type	Service	Usage
Requests from host to ...					
ANY IP of a Base Station	443	HTTPS (TCP)	Unicast	SSCv2 - Spectera Base Station API	Monitor+Control communication to devices
Sennheiser User Insights addresses [1]	443	HTTPS (TCP)	Unicast	Sennheiser User Insights	Analytics of usage and operational data

[1] sennheiseruserinsights.matomo.cloud

cdn.matomo.cloud

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