
# LinkDesk

## Software for Spectera Wireless Solution

PDF export of the original HTML instructions

# Contents

# 1. Preface

### PDF export of the original HTML instructions

This PDF document is an automated export of an interactive set of HTML instructions. It may be the case that not all contents and interactive elements are contained in the PDF as they cannot be presented in this format. Furthermore, automatically generated page breaks may cause coherent contents to be moved slightly. We can therefore only guarantee the completeness of the information in the HTML instructions, and recommend that you use these. You can find this in the documentation portal at www.sennheiser.com/documentation.

# 2. Product information

Software for the world's first wideband bidirectional wireless solution — Spectera.

With LinkDesk and Spectera, you get an intuitive workflow and unprecedented remote control and monitoring capabilities, plus visibility of IEM volume, latency, audio level and settings, RF health, battery status, and more.

The software's RF manager provides a continuous spectrum scan via Spectera's innovative DAD antenna. Plus, LinkDesk's assistive behaviors allow for quick and easy system management, and its production handling allows you to manage, store, and recall multiple Base Station configurations instantly.

## Key features

- Intuitive desktop application for full system management
- Notification system to expedite workflows and troubleshooting
- Assistive behaviors for fast and easy system management
- Production handling: manage, store and recall multiple Base Station configurations instantly
- Full remote control and monitoring of all Spectera ecosystem components including Base Station, DAD antenna, SEK bodypacks
- Unprecedented remote control and monitoring capabilities, plus visibility of IEM volume, latency, audio level and settings, RF health, battery status, and more
- RF manager for continuous spectrum scan via DAD antenna
- License activation for Base Station

## Operating System

- Windows®
- MacOS

## Product Support

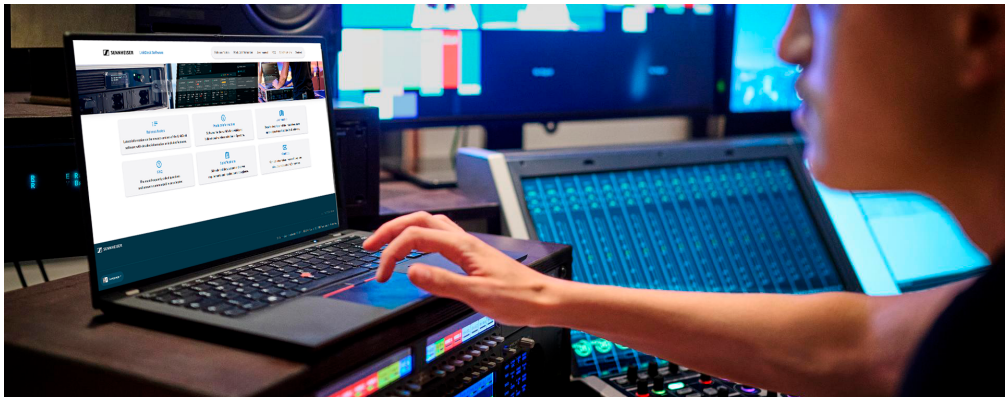
- Base Station
- DAD antenna
- SEK bodypacks

## Language Support

- English

# 3. User manual

Detailed description of the installation, start-up and operation of the LinkDesk software.



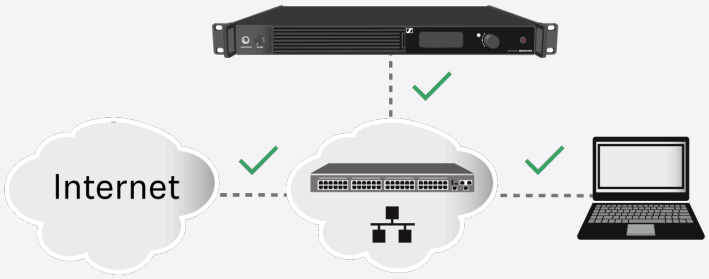
### Important Information on License Activation

> **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.

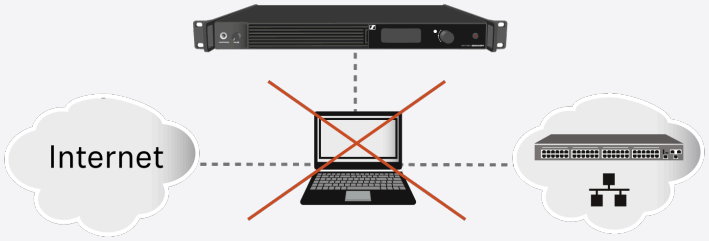
**NOTICE**

**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.

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

# Get started

Please navigate to the desired chapters by clicking on the corresponding information.

## Downloading and installing

The application is freely available and can be downloaded directly from the Sennheiser website.

**To download LinkDesk:**

- Navigate to the software product page of Sennheiser.
- Navigate to **Download**.
- Accept the listed **Terms and Conditions** and click on **Download**.
  - ✓ The download of the latest software version will be started.

**To install the software:**

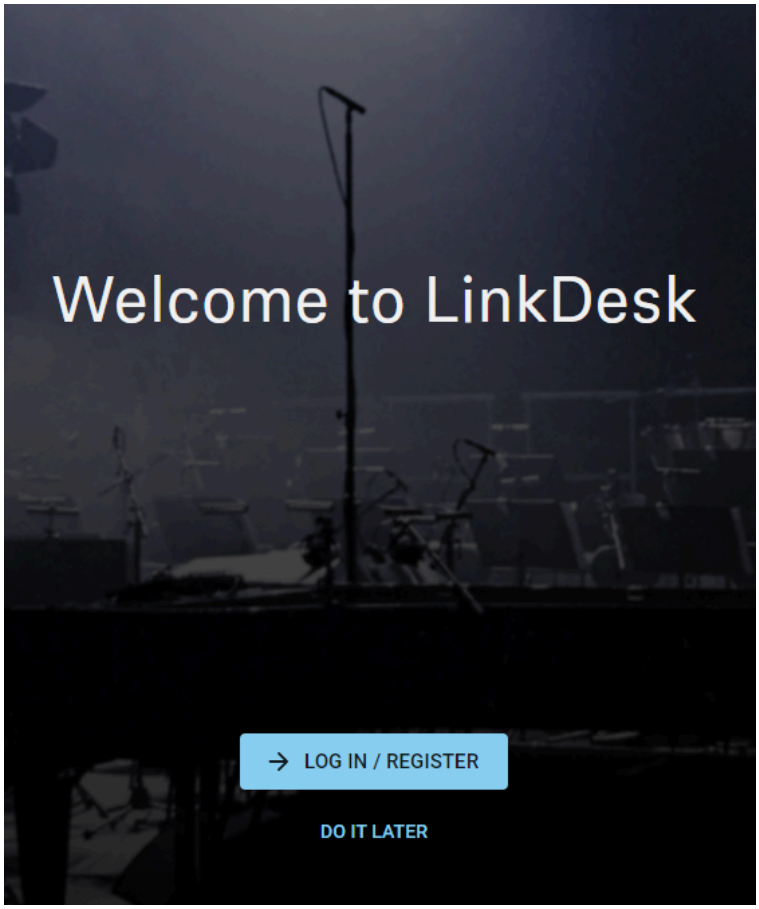
Please note that you need admin rights to complete the installation.

- Navigate to the folder of the downloaded software package.
- Double click on the application and follow the setup instructions.

You have successfully downloaded and installed the software.

## Signing in

To start the application, you can sign up for a new account or log in with an existing account.




When you start the software, you will be redirected to a log-in window. Here you can sign up and log in with your new account.

When you sign up for Sennheiser, your credentials will be valid for all brands within the Sennheiser Group.

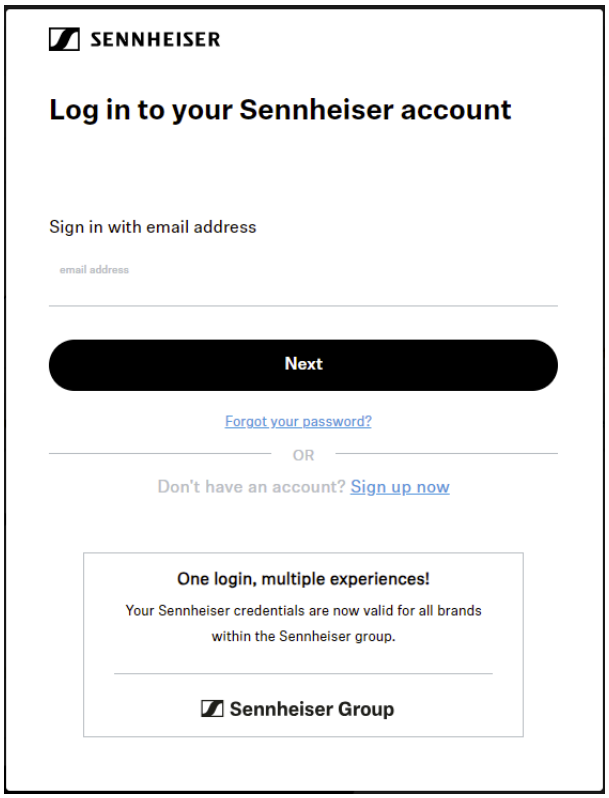
> **i** You can also skip the log-in and start the software without registration. You can then sign up or log in from the application at any time.

> **i** The login and account data assigned to your account are saved as long as your user account exists. You can delete your user account at any time. Further information can be found in the **consent to the processing of personal data**, which you must read and confirm during the registration process.

**To sign up and log in:**

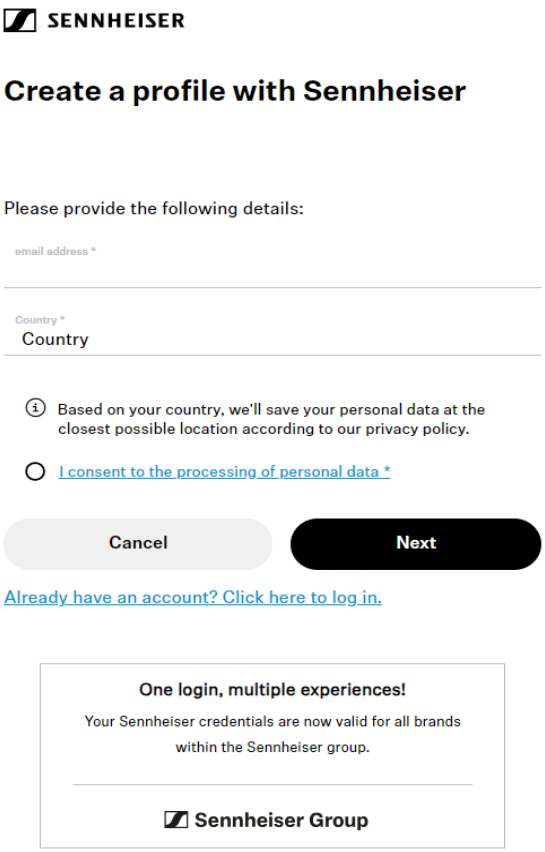
- Click on **LOG IN / REGISTER**.

  You will be redirected to the registration window. You can log in here if you already have an account.

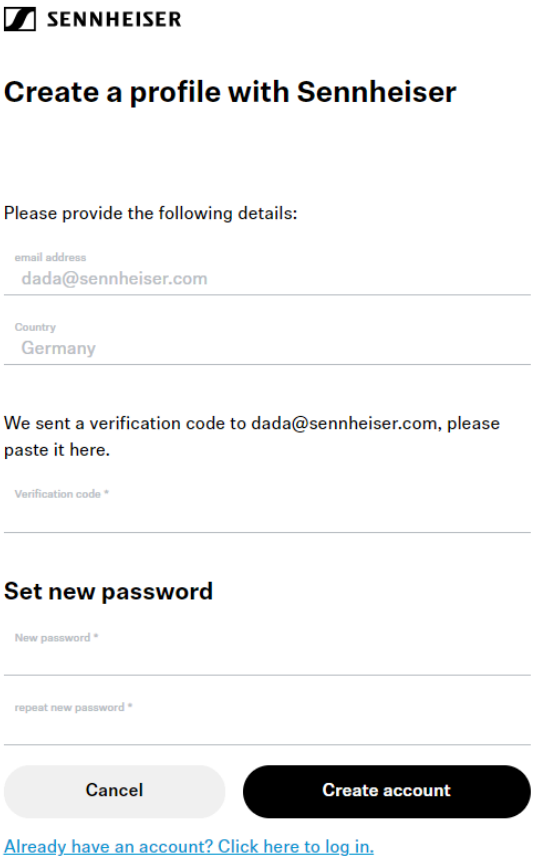



- If you do not yet have an account, click on **Sign up now** and fill in your registration data:
  - e-mail address*
  - country

  A confirmation code will be sent to your registered e-mail address.
- Confirm your consent to the processing of personal data and click on **Next**.




- In the second step, enter your personal data. Mandatory fields are marked with an asterisk*:
  - user name*,
  - surname,
  - family name,
  - phone number.
- Next, set your new password and enter the confirmation code from your e-mail.




- Click **Create account** to log in with your credentials.

> Your Sennheiser credentials are now valid for all brands within the Sennheiser Group. This ensures that you only need one log-in name and one password.

**To start directly without signing up / logging in:**

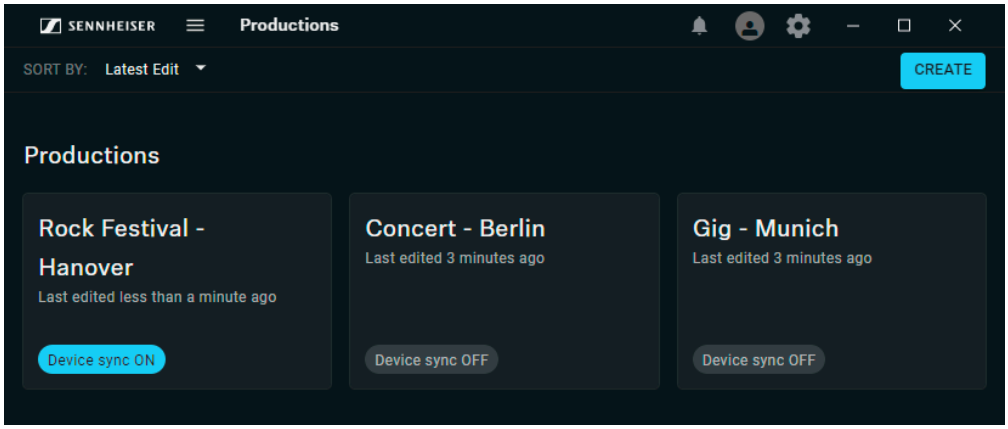
- Click on **DO IT LATER**.

  The application is started immediately. In order to sign up or log in later, click on the user icon at the top right and then on **Log in**.

You have successfully signed up and/or logged in.

## Main views and cards

The main view of the application shows general settings and cards that have already been created.




The top bar contains general settings that can be customized.

Beneath this, all production cards are displayed that are active or inactive depending on the sync status. The production cards can be sorted by:

- Latest edit
- Oldest edit
- Alphabetically A-Z
- Alphabetically Z-A

## Settings

Under **Settings**, various customizations can be configured for the user and the software.

### General

- Setting the user's current country
- Setting the time zone
- Setting the date format

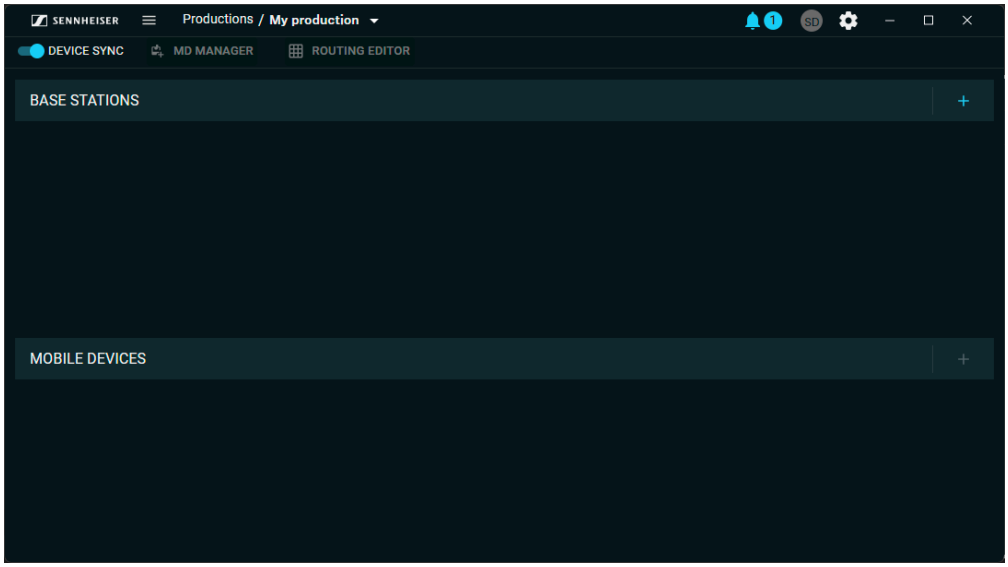
### User

- Sign in/registration

## Productions

Productions contain a virtual configuration set of devices and settings that are prepared for an upcoming event.

Within a production card, all the required components are clearly visualized in a structural sequence, which enables easy handling and quick access to the important elements.




Each production is divided into sections (only visible once the Base Station and an antenna have been added):

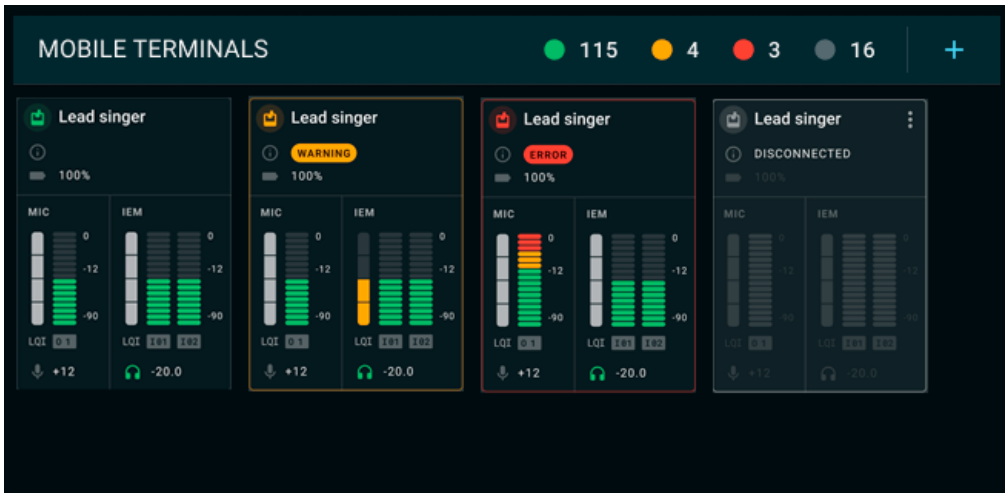
- **Frequency Information Visualization**
  - Live display of the current frequency spectrum with occupied and free frequencies
  - Scanning RF Spectrum
- **Base Stations**
  - Summary of all connected or planned Base Stations
- **Mobile devices**
  - Summary of all connected or planned mobile devices

## Device state colors

The displayed colors of the device symbols provide a visual indication of the current status of the device.

In addition to the colors, associated messages/warnings are displayed. The following colors may occur:

| Icon | Color | Meaning |
|---|---|---|
| | GREEN | successful status (e. g. normal operation mode) |
| | YELLOW | warning (e.g. device not configured properly(e.g. no audio links)) |
| | RED | error (e.g. firmware mismatch) |
| | WHITE | neutral status (e.g. not connected / offline device) |



# Basic configuration

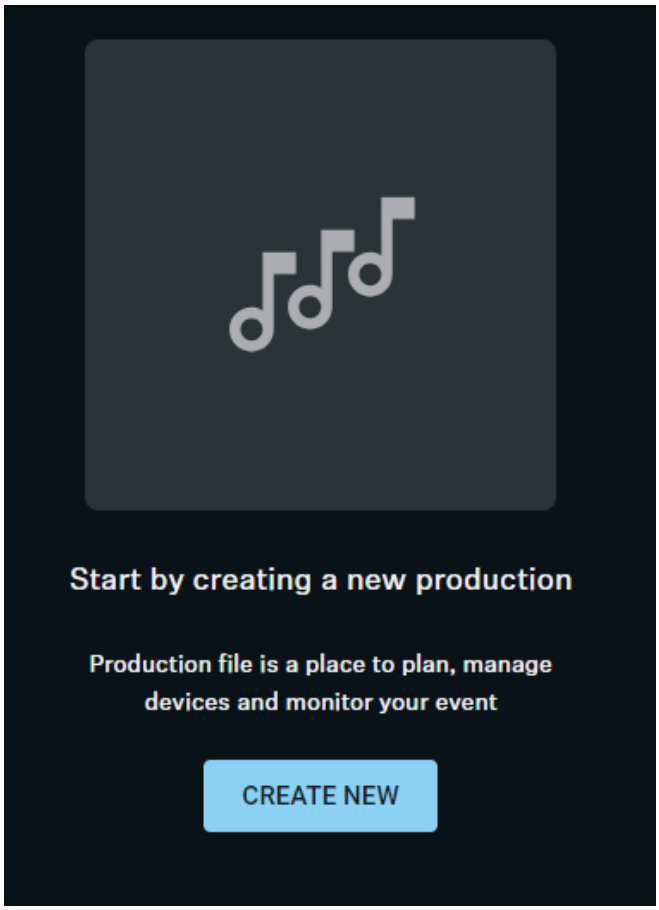
Start your basic configuration with the recommended steps.

For an initial setup, we recommend following these first steps to successfully configure the system from the outset:

- Creating new productions
- 
- Activating a license (LinkDesk)
- Activating antennas
- Scanning the RF spectrum
- Adding RF channels
- Pairing/unpairing mobile devices

## Creating new productions

With productions, you can create a virtual workplace to plan, manage and monitor your real devices for the upcoming event.



**To create a new production:**

- Click on **CREATE NEW** to start a new production.
- Enter a name under **Production Information** and click on **CREATE**.

**To create a further production:**

- In the task bar at the top click on **Productions** > **Create**.

> Please note that the new production will take lead access to devices in the network, while the other productions will lose access.

- Enter a name under **Production Information** and click on **CREATE**.

✓ The production has been created.

## Adding Base Station

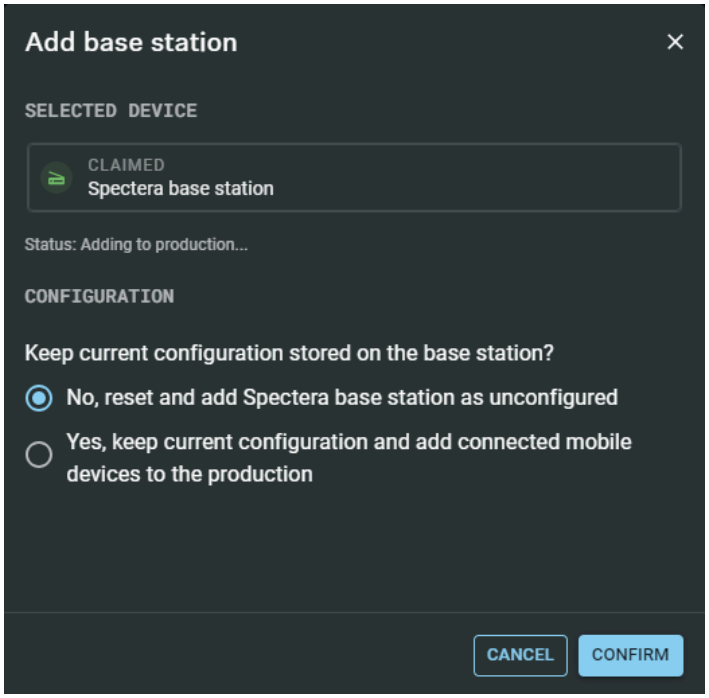
To add a Base Station, you must identify it via its IP address, authenticate it with a password, and activate its license.

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 (LinkDesk)).
3. Activating the Base Station license (see Activating a license (LinkDesk)).

**To add a Base Station (claiming single device):**

- 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**.
  - The Base Station has been identified and is displayed in the results.




> **i** If the Base Station has already been used with a previous configuration, this will be retrieved when it is added. You will be asked whether you want to keep the current configuration on the Base Station or continue with an unconfigured Base Station.

- 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).

  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 added successfully and is displayed on the Base Station card on the top left. If external antennas are connected to the Base Station, they automatically appear on the card (see Activating antennas).

You will then be prompted to activate the license (Activating a license (LinkDesk)) for your region (if it has not yet been activated), or to configure at least one broadband channel to enable pairing and communication between the Base Station and mobile devices.

## Identifying Base Station via IP

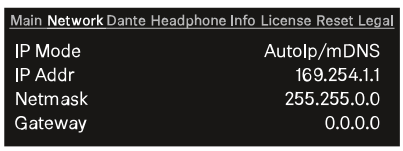
In order to add a Base Station, its IP address is required.

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.




- Note the displayed IP of your device.

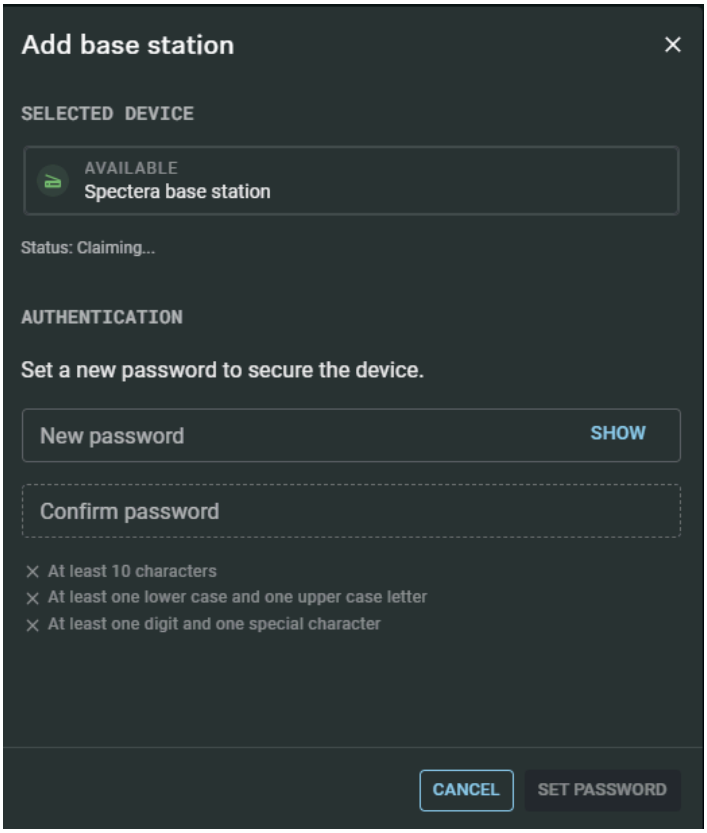
✓ The IP address of your Base Station has been identified.

## Claiming single device (LinkDesk)

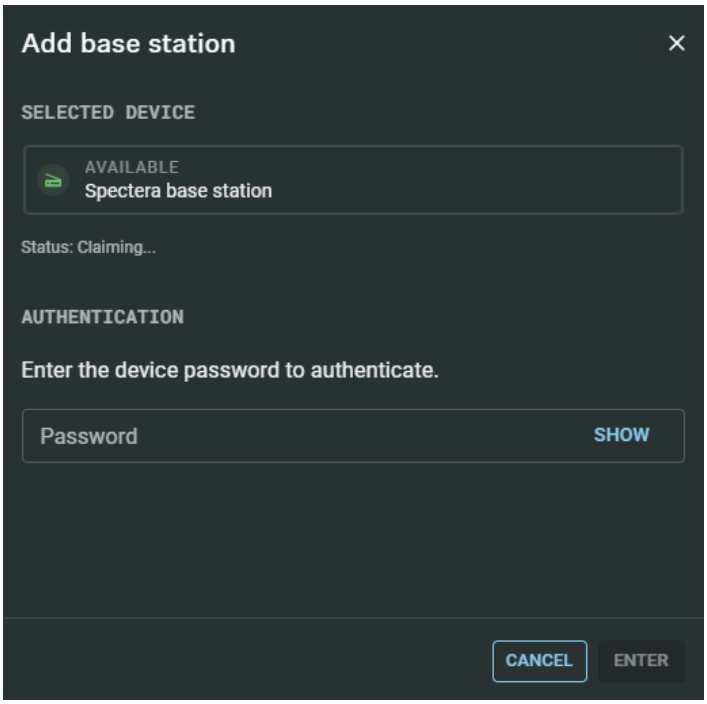
Instructions for claiming a single device in Sennheiser LinkDesk.

**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:




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




> **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.

## Activating a license (LinkDesk)

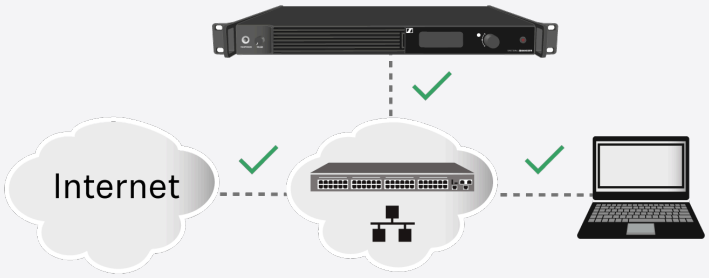
Here you will learn how to activate your region-specific license for your Base Station.

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.

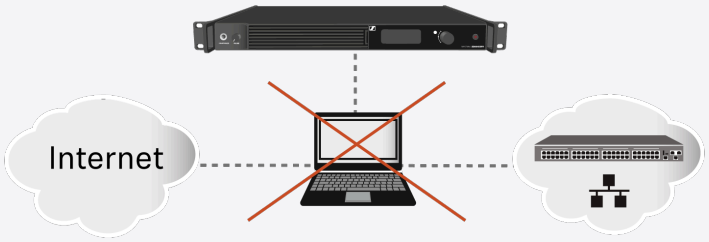
**NOTICE**

**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!

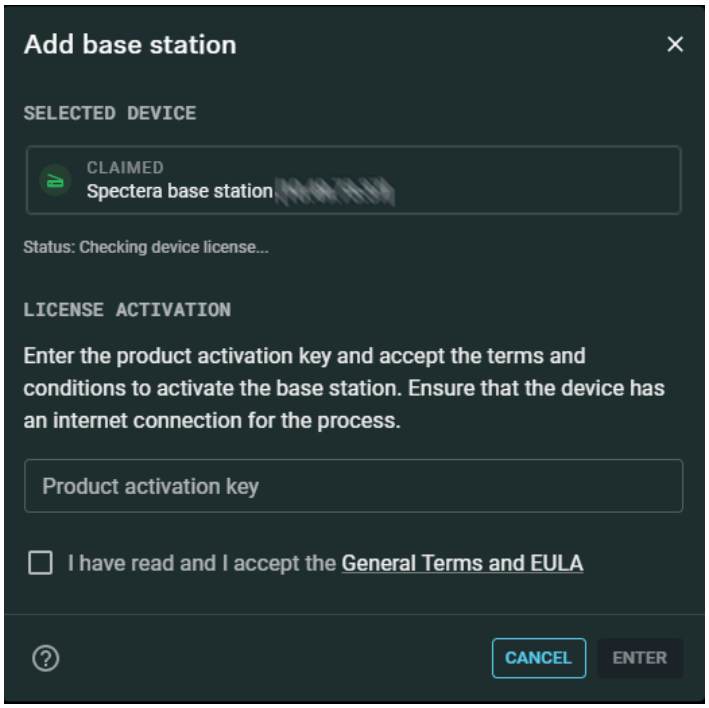



- The Internet is only required once for activation.

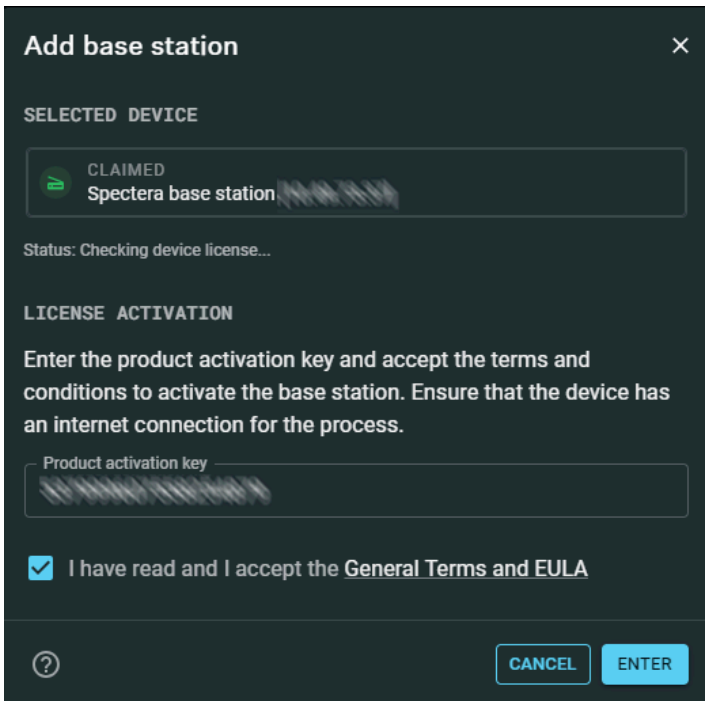
After you have successfully added and claimed your Base Station (see Adding Base Station) you will be prompted to activate the license.

**To activate the license:**

- Add a new Base Station to your production (see Adding Base Station).
  - A new license activation window appears:




- Enter your purchased product activation key.
- Read and acknowledge the general terms and the end-user license agreement:



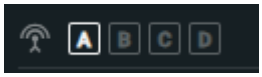

- Click **ENTER** to activate the license.

✓ Your license has been activated successfully.

## Activating antennas

Antennas connected to a Base Station must be selected and activated before use.

The connected antennas are displayed with a white marking in the overview card of the Base Station:




> For detailed information on how to connect the antennas to the Base Station, please refer to the chapter **Connecting antennas**.

**To assign one or more connected antennas to the Base Station:**

- Click on your Base Station card.
  - An additional navigation menu will appear on the right-hand side of the window.
- Select the RF channel to which you want to add an additional antenna.
- Under **ANTENNAS** click on **+ ADD ANTENNA**.
  - All connected antennas are displayed.
- Select the antenna that you want to assign to your RF channel.

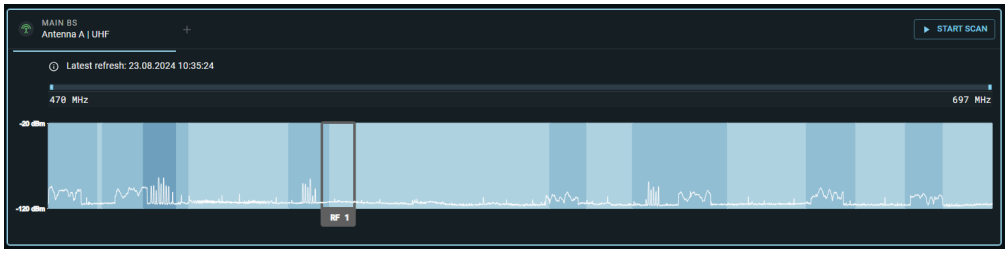
> The antenna has been assigned and is displayed in the overview of the Base Station card.

## Scanning the RF spectrum

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

You can scan the frequency environment of all antennas connected to the Base Station.

> **i** Make sure that no antenna is activated! If the scan is started with an active antenna, the RF channel is automatically muted until the scan is completed.




Before activating the connected antenna, you can check the occupancy of the frequency spectrum and examine the surroundings for possible frequency interference.

**To start the RF scan:**

- From your production card dashboard, click **START SCAN** on the right side of the top bar.

  The connected antenna scans the environment and displays a live graphic within the configured RF channel.

  > **i** You can zoom into the spectrum by pressing CMD and using the scroll function of your mouse. If the scan is started with an active antenna, the RF channel is automatically muted until the scan is completed.

**To start the RF scan for another antenna:**

- In the main window of the RF SCAN click on **+** to select your antenna and then on **START SCAN**.

  > **i** Via the Context Tray of the scan, you can adapt the resolution bandwidth and sweep time for each scanning DAD.

✓ The RF spectrum of your connected antennas has been scanned.

## Adding RF channels

You can configure an RF channel and assign it to the available devices.

> **i** To configure an RF channel, at least one antenna must be connected to the BS station (see **Connecting antennas**).

**In order to add an RF channel:**

- Click on your Base Station card.
  - ✓ An additional navigation menu will appear on the right-hand side of the window.
- Click on:
  - the symbol  **Add RF channel** on the Base Station card **OR**
  - the Base Station card and navigate in the right-hand tab to **RF CHANNEL** > **RF SETTINGS** > **EDIT**.
  - ✓ A configuration menu for RF channels appears.
- Select the operating antenna.
- Select the RF power and enter your available frequency and bandwidth.
- Click on **SAVE** to create the RF channel.

✓ The RF channel has been successfully added and the antenna has been muted.

## Pairing/unpairing mobile devices

In LinkDesk 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.

> **i** The order of mobile device cards cannot be changed. Please add devices in the desired order. Newly added devices are always added in the last position to the right.

**To pair a mobile device:**

- In your production card, activate the function **DEVICE SYNCHRONIZATION** on the left-hand side of the top bar.
- Click on the button **MD Manager** on the left-hand side of the top bar.
  - A new window **Add mobile devices** opens.
- Select your Base Station from the drop down list on the left-hand side and activate **PAIRING MODE**.
- 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.
- Click on the button in the line of the mobile device to be paired.
  - A confirmation code is displayed both in LinkDesk and on the mobile device.
- Compare the displayed code at both endpoints.
- In LinkDesk, click on **Confirm** to pair the selected mobile device.
  - The mobile device has been paired successfully. The device state color changes to:
    - green: successful operation, or
    - yellow: warning (e.g. if the audio links have not yet been assigned (see also Device state colors)).

**To unpair a mobile device:**

- You can either
  - click on the  **unpair** button of the corresponding device in the MD Manager or
  - click on the three dots  of the mobile device card and select the  **unpair** function.
- The mobile device has been unpaired successfully.

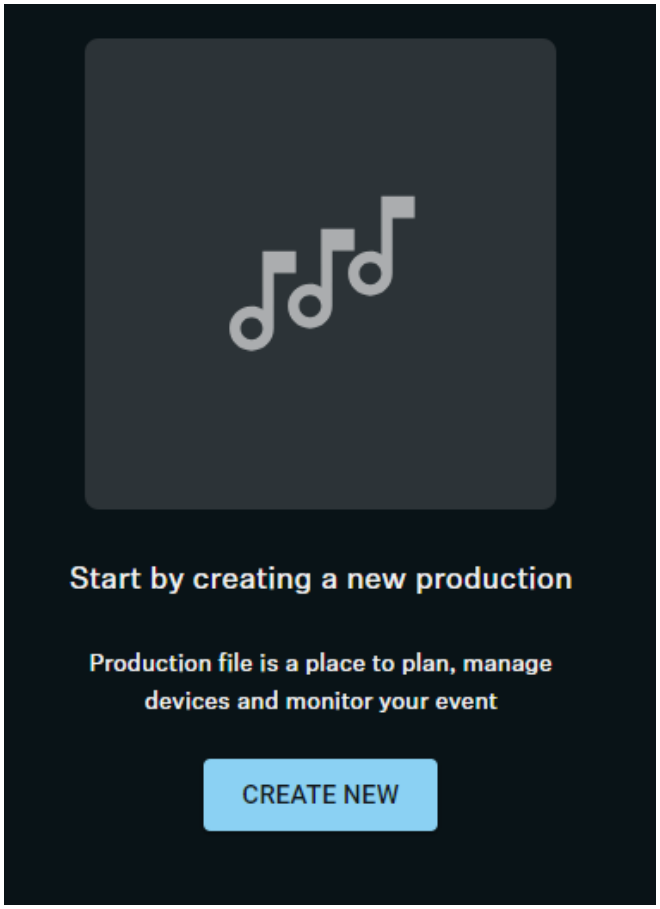
The mobile devices have been successfully paired/unpaired.

# Productions

In this chapter you will learn the basic information about productions.

## Creating new productions

With productions, you can create a virtual workplace to plan, manage and monitor your real devices for the upcoming event.




**To create a new production:**

- Click on **CREATE NEW** to start a new production.
- Enter a name under **Production Information** and click on **CREATE**.

**To create a further production:**

- In the task bar at the top click on **Productions** > **Create**.

  > Please note that the new production will take lead access to devices in the network, while the other productions will lose access.

- Enter a name under **Production Information** and click on **CREATE**.

✓ The production has been created.

## Editing meta information

You can edit the meta information of your previously created production card.

**To edit a production:**

- Navigate to **Productions** and click on the three dots  of the production card.
- Select **Edit** to edit the meta information of the production.

> You can edit a description with up to 32 characters. Special characters in general and spaces at the beginning and end of the description are not permitted.

The meta information has been edited.

## Activating device synchronization

Device synchronization connects all your devices like a network hub, making it essential for both existing and newly added devices to work together smoothly.

**When you turn on device synchronization, it automatically starts the matching process for Base Stations that are already in use and configured. You will be guided step-by-step through the process.**

**To activate device synchronization:**

- Click on your created production card.
- Click on the button  **DEVICE SYNCHRONIZATION** at the top left of the product card.
  - A message appears with the following options:
    - [PUSH] - replace all settings currently on the Base Station with those stored in LinkDesk, or
    - [PULL] - pull the current settings from the Base Station to LinkDesk.
- Select an option and click **OK**.

Device synchronization has been activated.

You can now add new components such as Base Stations, mobile devices and antennas to your card.

## Deleting productions

The previously created productions can simply be deleted.

**CAUTION**

**This production card will be permanently deleted.**

Deleted production cards can no longer be restored.

- Only delete the production card if you are certain it is no longer needed.

**To delete a production:**

- Navigate to **Productions** and click on the three dots  of the production to be deleted.
- Select  **Delete** to permanently delete the production.

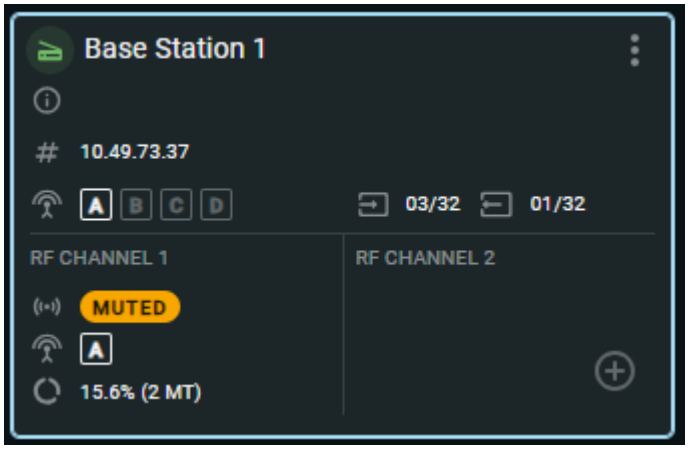
✓ The production has been deleted permanently.

# Base Station

The Base Station is the central hardware for managing and monitoring all compatible Spectera products.

The Base Station is used to connect, configure and monitor antennas and mobile devices all in one.

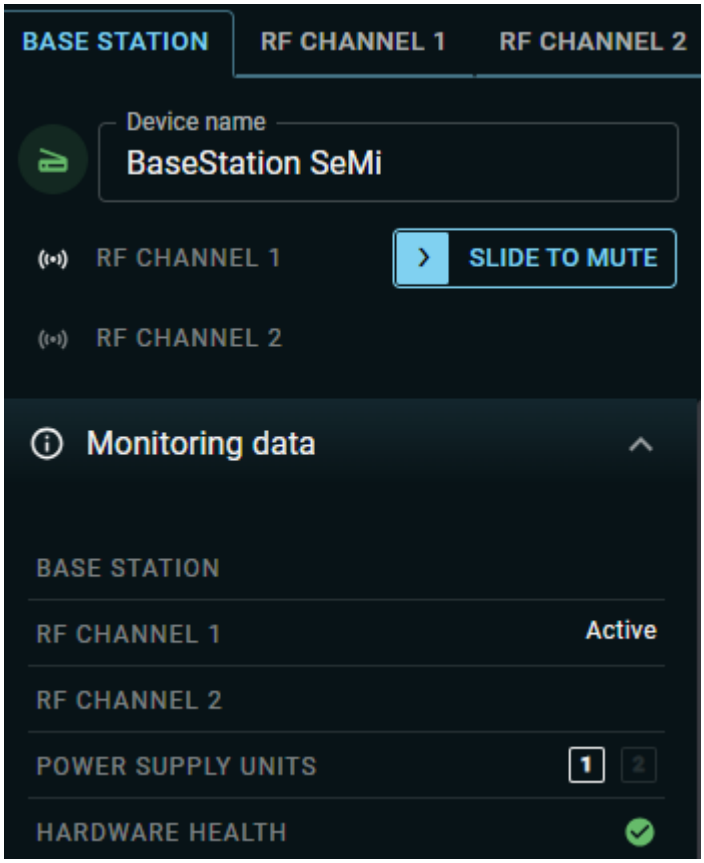
## Summarized view




Depending on the configuration, a Base Station can provide the following summarized device information:

- the device state color
- the current warnings about the status of the device
- the IP address
- the connected antennas
- the configured RF channels
- the status of the RF channel, e.g. muted, antenna loss or antenna update
- the number of routed IEF/IFB inputs
- the number of routed MIC/LINE outputs
- the capacity utilization of the entire RF bandwidth

### Details view




By clicking on the Base Station card, a details page appears on the right-hand side of the navigation menu. The page shows detailed information about the device and allows you to edit and monitor the settings for ongoing operation:

- **BASE STATION**
  - Name and status of the Base Station
    - Device state colors
    - Identifying Base Stations
  - Status of the RF channel
    - Muting/unmuting RF signals
- **Device information:**
  - Changing the device name
  - Updating the firmware (Base Station)
- **Monitoring data**
  - Here you can monitor the hardware health-state, the configured RF channels, the number of connected power supply units, and occurring interference.
- **Interface settings**
  - Overview of all available interfaces for incoming and outgoing links and connections
- **Antenna ports**
  - Overview of all connected antennas and available antenna ports

- **Paired devices**
    - Overview of all known devices within the RF channels with the number of linked routes
- **Hardware details**
    - Detailed information about the Base Station

## Identifying Base Stations

You can remotely identify your Base Station.

**To identify the Base Station:**

▶ On your Base Station card, click on the 3 dots  and then on  **Identify** under the section **Base Station**.

✓ The icon on the Base Station card flashes. The display of the Base Station shows **Identify**.

✓ The Base Station has been identified.

## Adding Base Station

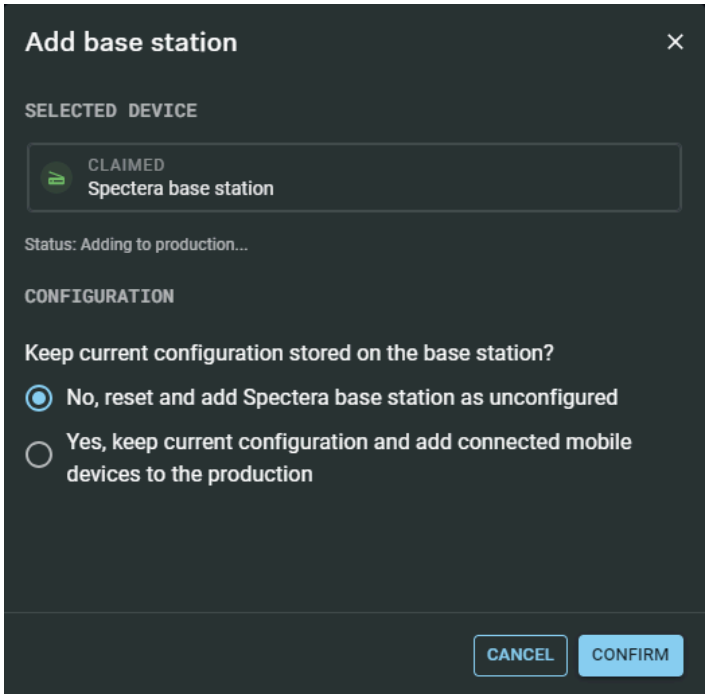
To add a Base Station, you must identify it via its IP address, authenticate it with a password, and activate its license.

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 (LinkDesk)).
3. Activating the Base Station license (see Activating a license (LinkDesk)).

**To add a Base Station (claiming single device):**

- 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**.
  - The Base Station has been identified and is displayed in the results.




> **i** If the Base Station has already been used with a previous configuration, this will be retrieved when it is added. You will be asked whether you want to keep the current configuration on the Base Station or continue with an unconfigured Base Station.

- 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).

  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 added successfully and is displayed on the Base Station card on the top left. If external antennas are connected to the Base Station, they automatically appear on the card (see Activating antennas).

You will then be prompted to activate the license (Activating a license (LinkDesk)) for your region (if it has not yet been activated), or to configure at least one broadband channel to enable pairing and communication between the Base Station and mobile devices.

## Activating a license (LinkDesk)

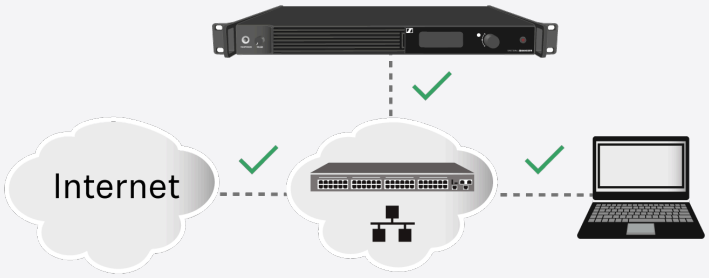
Here you will learn how to activate your region-specific license for your Base Station.

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.

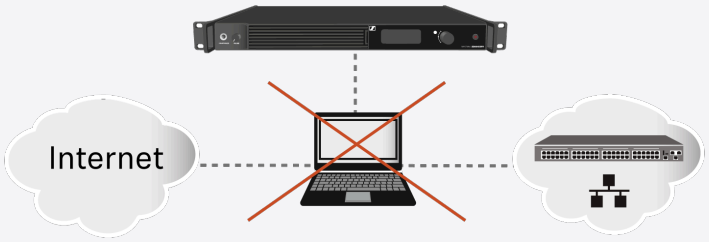
**NOTICE**

**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!

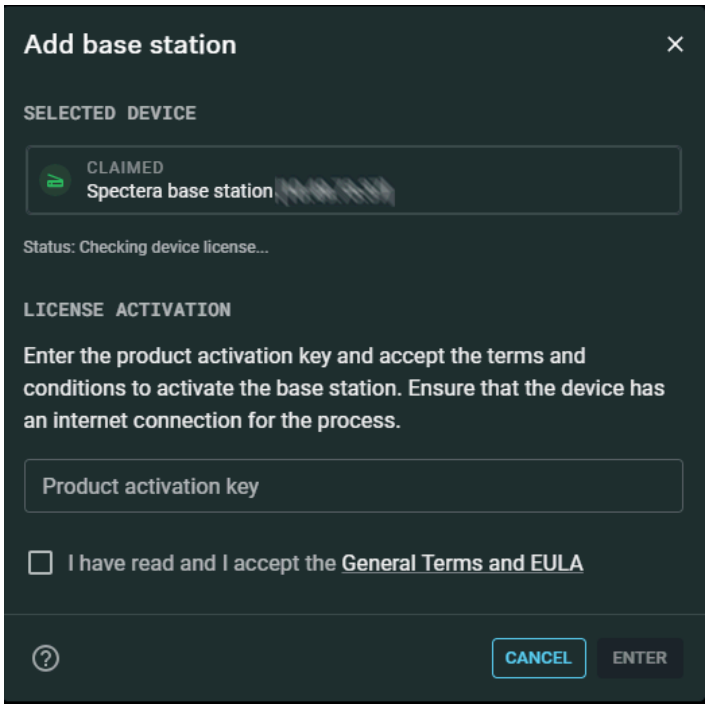



- The Internet is only required once for activation.

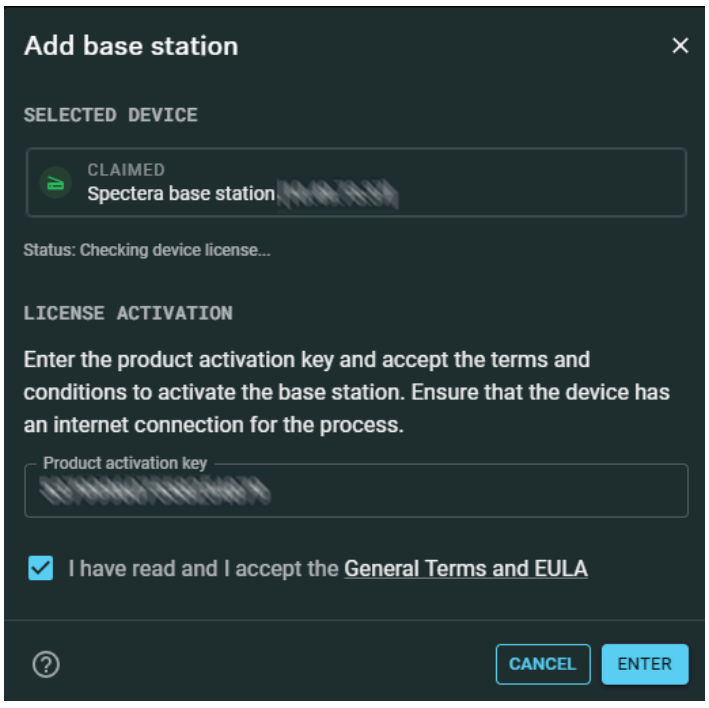
After you have successfully added and claimed your Base Station (see Adding Base Station) you will be prompted to activate the license.

**To activate the license:**

- Add a new Base Station to your production (see Adding Base Station).
  - A new license activation window appears:




- Enter your purchased product activation key.
- Read and acknowledge the general terms and the end-user license agreement:



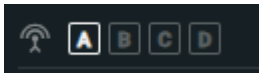

- Click **ENTER** to activate the license.

✓ Your license has been activated successfully.

## Activating antennas

Antennas connected to a Base Station must be selected and activated before use.

The connected antennas are displayed with a white marking in the overview card of the Base Station:




> For detailed information on how to connect the antennas to the Base Station, please refer to the chapter **Connecting antennas**.

**To assign one or more connected antennas to the Base Station:**

- Click on your Base Station card.
  - An additional navigation menu will appear on the right-hand side of the window.
- Select the RF channel to which you want to add an additional antenna.
- Under **ANTENNAS** click on **+ ADD ANTENNA**.
  - All connected antennas are displayed.
- Select the antenna that you want to assign to your RF channel.

> The antenna has been assigned and is displayed in the overview of the Base Station card.

## Adding RF channels

You can configure an RF channel and assign it to the available devices.

> **i** To configure an RF channel, at least one antenna must be connected to the BS station (see **Connecting antennas**).

**In order to add an RF channel:**

- Click on your Base Station card.
  - ✓ An additional navigation menu will appear on the right-hand side of the window.
- Click on:
  - the symbol  **Add RF channel** on the Base Station card **OR**
  - the Base Station card and navigate in the right-hand tab to **RF CHANNEL** > **RF SETTINGS** > **EDIT**.
  - ✓ A configuration menu for RF channels appears.
- Select the operating antenna.
- Select the RF power and enter your available frequency and bandwidth.
- Click on **SAVE** to create the RF channel.

✓ The RF channel has been successfully added and the antenna has been muted.

## Configuring RF channels

You can adjust the RF channel in terms of its antenna selection, frequency and bandwidth.

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

**To configure an RF channel:**

- Click on your Base Station card.
  - An additional navigation menu will appear on the right-hand side of the window.
- Navigate to the tab **RF CHANNEL 1** or **RF CHANNEL 2**.
- Specify under the **RF AT STARTUP** function whether, after powering up the Base Station:
  - the channel should start muted by default [**muted**], or
  - it should start unmuted [**active**], or
  - it should retain its last status [**last**].
- Under **ANTENNAS** please select the operating antenna on which the RF channel is to configured.
  - The antenna has been selected.
- Adjust the desired frequency and bandwidth under: **Channel settings** > **RF SETTINGS** > **EDIT**.

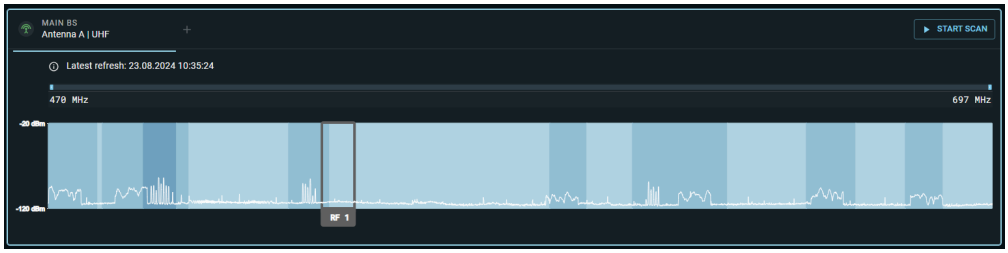
✓ The RF Channel has been configured.

## Scanning the RF spectrum

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

You can scan the frequency environment of all antennas connected to the Base Station.

> **i** Make sure that no antenna is activated! If the scan is started with an active antenna, the RF channel is automatically muted until the scan is completed.




Before activating the connected antenna, you can check the occupancy of the frequency spectrum and examine the surroundings for possible frequency interference.

**To start the RF scan:**

- From your production card dashboard, click **START SCAN** on the right side of the top bar.

  The connected antenna scans the environment and displays a live graphic within the configured RF channel.

  > **i** You can zoom into the spectrum by pressing CMD and using the scroll function of your mouse. If the scan is started with an active antenna, the RF channel is automatically muted until the scan is completed.

**To start the RF scan for another antenna:**

- In the main window of the RF SCAN click on **+** to select your antenna and then on **START SCAN**.

  > **i** Via the Context Tray of the scan, you can adapt the resolution bandwidth and sweep time for each scanning DAD.

✓ The RF spectrum of your connected antennas has been scanned.

## Adding mobile devices

You can add mobile devices to your connected Base Station.

> When adding mobile devices for the first time, they need to be paired. Devices that have already been paired and removed will be displayed in the MD Manager and can easily be added back to production using the + button.

**To add a mobile device:**

- In your production card, activate the function **DEVICE SYNCHRONIZATION** on the left-hand side of the top bar.
- Click on the button **MD Manager** on the left-hand side of the top bar.
  - A new window opens and shows a list of all known and connected mobile devices.
- Click on **PAIRING MODE** to set the Base Station to pairing mode.
  - The Base Station remains in pairing status for 5 minutes.
- Switch on your mobile device and activate **Pairing Mode** if it has not been activated automatically (**Switching the SEK on and off**, **Pairing the SEK to the Base Station**).
  - After a few seconds, the available mobile devices are displayed in the list.
- Click on the **Add** button in the line of the mobile device to be added.
  - A confirmation code is displayed both in LinkDesk and on the mobile device.
- Compare the displayed code at both endpoints.
- In LinkDesk, click on **Confirm** to pair the selected mobile device.

> The mobile device has been added to the Base Station and is indicated as a separate card. The card shows the connected Base Station and the occupied RF channel. The device state color changes to:
>
> - green: successful operation, or
> - yellow: warning (e.g. if the audio links have not yet been assigned (see also Device state colors and Routing editor).

## Pairing/unpairing mobile devices

In LinkDesk 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.

> **i** The order of mobile device cards cannot be changed. Please add devices in the desired order. Newly added devices are always added in the last position to the right.

**To pair a mobile device:**

- In your production card, activate the function **DEVICE SYNCHRONIZATION** on the left-hand side of the top bar.
- Click on the button **MD Manager** on the left-hand side of the top bar.
  - A new window **Add mobile devices** opens.
- Select your Base Station from the drop down list on the left-hand side and activate **PAIRING MODE**.
- 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.
- Click on the button in the line of the mobile device to be paired.
  - A confirmation code is displayed both in LinkDesk and on the mobile device.
- Compare the displayed code at both endpoints.
- In LinkDesk, click on **Confirm** to pair the selected mobile device.
  - The mobile device has been paired successfully. The device state color changes to:
    - green: successful operation, or
    - yellow: warning (e.g. if the audio links have not yet been assigned (see also Device state colors)).

**To unpair a mobile device:**

- You can either
  - click on the  **unpair** button of the corresponding device in the MD Manager or
  - click on the three dots  of the mobile device card and select the  **unpair** function.
- The mobile device has been unpaired successfully.

✓ The mobile devices have been successfully paired/unpaired.

## Displaying device information

You can display detailed information relating to your Spectera device.

Find out here which device information can be displayed in the details view for mobile devices or for the Base Station.

**In order to display detailed information:**

- Click on the card of your Spectera device (Base Station or mobile device).
  - An additional navigation menu will appear on the right-hand side of the window.
- Observe all the details in the menu by scrolling up and down.

Detailed information is displayed.

## Changing the device name

You can change the device name for your Base Station.

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

**To change the device name:**

- Click on your Base Station card.
  - An additional navigation menu will appear on the right-hand side of the window.
- Navigate to **BASE STATION** > **Device information**.
- Edit the name under **Device name**.
  - The name is immediately transmitted to the Base Station and saved.

✓ The device name has been changed.

## Configuring interface settings

You can configure the interfaces of the inputs and outputs on the device individually.

The following interfaces are available for the Base Station:

- AUDIO NETWORK (DANTE)
- MADI 1
- MADI 2
- WORD CLOCK

> **i** Once you select the DANTE interface, configuration must be completed through either the Dante Controller or the Domain Manager.

**To select and assign an available interface:**

1. Click on your Base Station card.
   - ✓ An additional navigation menu will appear on the right-hand side of the window.
2. Navigate to **BASE STATION** > **Interface Settings**.
3. Assign the desired audio connections to the available interfaces.

✓ The interface settings have been configured.

## Muting/unmuting RF signals

You can mute/unmute the RF signals of the configured channels.

The following RF statuses are possible:

- 

muted RF channel
- 

unmuted RF channel

**In order to mute/unmute the RF signal:**

> Attention: Signal transmission will be stopped immediately on all routed links!

1. Click on your Base Station card.
   - An additional navigation menu will appear on the right-hand side of the window.
2. On the **BASE STATION** tab, slide the arrow symbol in the displayed direction to change the mute:
   - 

to mute the RF channel
   - 

to unmute the RF channel

✓ The RF signal has been muted/unmuted.

## Resetting RF channels

You can reset or remove your configured RF channel from the current production.

**NOTICE**

**By resetting the RF channel, the connected mobile devices are also removed from this production.**

The audio signal of connected devices will be interrupted immediately!

- Only remove the channel if no active audio is being used.

**To reset the RF channel:**

- On your Base Station Card, click on the 3 dots  and then on **Reset RF Ch 1** under the section **RF CHANNEL 1**.
- Click on **REMOVE**.

> This function can also be accessed via the RF Channel context tray (click on the Base Station card and navigate to the context tray menu on the right).

✓ The RF channel has been reset.

## 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.

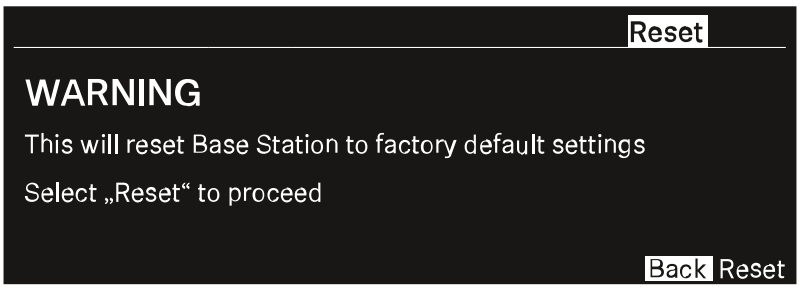
- ▶ Do not reset the Base Station during an active live audio transmission.

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.




- ▶ 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.

## Removing the Base Station

You can delete your configured Base Station from the current production.

**NOTICE**

**By removing the Base Station, the connected mobile devices are also removed from this production.**

The audio signal of connected devices will be interrupted immediately!

- Only remove the Base Station if no active audio is being used.

**To remove the Base Station:**

- On your Base Station Card, click on the 3 dots  and then on **Delete** under the section **Base Station**.
- Click on **OK**.

✓ The Base Station has been removed.

## Updating the firmware (Base Station)

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

The DAD antenna updates automatically (about 20 seconds) after the BS is updated or when the DAD is plugged in. RF signals will pause during the update. You will see the update status on the BS card.

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

**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:**

- Click on your Base Station card.
  - ✓ An additional navigation menu will appear on the right-hand side of the window.
- Navigate to **BASE STATION** > **Device information**.
- Under the current Base Station click on **UPDATE** and then on **Update Version**  .
- Click on **UPLOAD FILE** and select the manually downloaded `.sennpkg` file.
  - ✓ The firmware file has been selected.
- Click on **UPDATE** to start the update process.
  - ✓ The firmware starts the update automatically.

> **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.

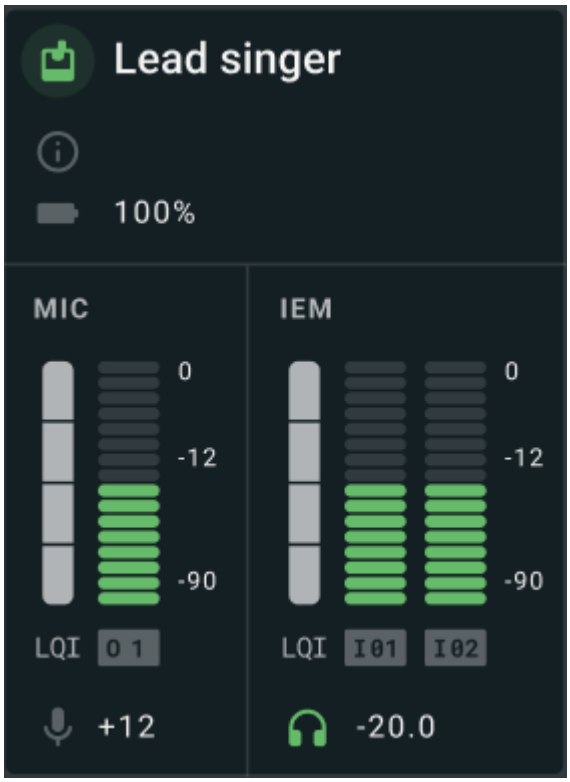
# Mobile devices

Mobile devices are bodypack transmitters and/or receivers that are assigned to a Base Station.

On a mobile device, both incoming in-ear signals and outgoing microphone signals can be sent with one device. To do this, the audio link mode must be set.

> The order of mobile device cards cannot be changed. Please add devices in the desired order. Newly added devices are always added in the last position to the right.

### Summarized view

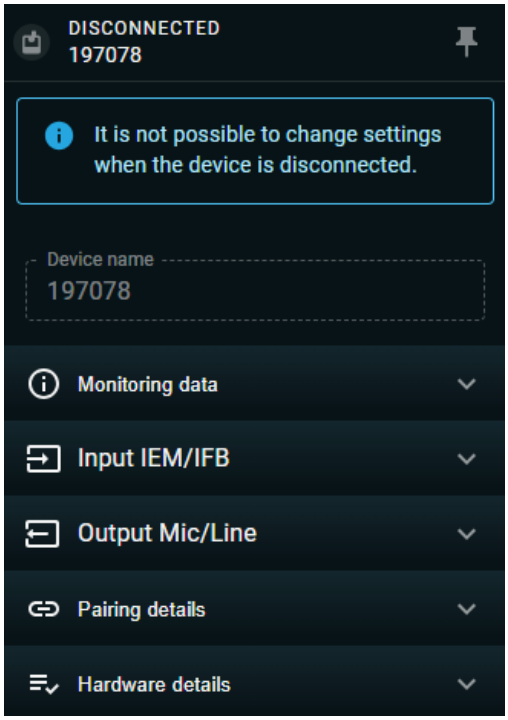



Depending on the configuration, a mobile device can provide the following summarized device information:

- the device state color and the name of the device
- the current warnings about the status of the device
- the connected RF channels and Base Station
- the battery status

- the `IEF/IFB` input information:
  - `LQI` Link Quality Input (LQI)
  - `I1` input channel number (e.g. "I 1" for mono or "I 2" and "I 3" for stereo)
-  `MIC/LINE` the output information
-  Colored indication of headphone status (red - not connected; green = connected) and the current volume status

### Detail view




By clicking on the card of the mobile device, a details page appears on the right-hand side of the navigation menu. The page shows detailed information about the device and allows you to edit important settings for ongoing operation:

- **Name** and **status** of the devices
  - Changing the device name
-  **Monitoring data**
  - Monitoring the readiness state, the battery status of your mobile device and occurring interference.
-  **Input IEM/IFB**
  - Changing the balance
  - Changing the headphone volume
  - Changing the headphone volume limiter
  - Monitoring the selected audio link mode
  - Monitoring the configured audio channel
  - Changing the routing configuration with **EDIT ROUTES**

- **Output Mic/Line**
  - Changing the **MIC/LINE SELECTION**
  - Enabling /disabling **TEST TONE**
  - Enabling /disabling **CABLE EMULATION**
  - Changing the **PREAMP GAIN** for the microphone output
  - Changing the low cut value in order to minimize the wind noise
  - Monitoring the selected audio link mode
  - Monitoring the configured audio channel
- **Pairing details**
  - Details about the connected Base Station
  - Details about the active RF channel and
  - Details about the capacity utilization of the entire RF bandwidth
- **Hardware details**
  - Product name
  - Type
  - Serial number
  - FCC number
  - Firmware version
  - If a firmware update is available, you can start the update here (Updating the firmware (Base Station))

## Pairing/unpairing mobile devices

In LinkDesk 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.

> **i** The order of mobile device cards cannot be changed. Please add devices in the desired order. Newly added devices are always added in the last position to the right.

**To pair a mobile device:**

- In your production card, activate the function **DEVICE SYNCHRONIZATION** on the left-hand side of the top bar.
- Click on the button **MD Manager** on the left-hand side of the top bar.
  - A new window **Add mobile devices** opens.

- Select your Base Station from the drop down list on the left-hand side and activate  **PAIRING MODE**.
- 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.
- Click on the  button in the line of the mobile device to be paired.
  - ✓ A confirmation code is displayed both in LinkDesk and on the mobile device.
- Compare the displayed code at both endpoints.
- In LinkDesk, click on **Confirm** to pair the selected mobile device.
  - ✓ The mobile device has been paired successfully. The device state color changes to:
    - green: successful operation, or
    - yellow: warning (e.g. if the audio links have not yet been assigned (see also Device state colors)).

**To unpair a mobile device:**

- You can either
  - click on the  **unpair** button of the corresponding device in the MD Manager or
  - click on the three dots  of the mobile device card and select the  **unpair** function.
  - ✓ The mobile device has been unpaired successfully.

✓ The mobile devices have been successfully paired/unpaired.

## Adding mobile devices

You can add mobile devices to your connected Base Station.

> When adding mobile devices for the first time, they need to be paired. Devices that have already been paired and removed will be displayed in the MD Manager and can easily be added back to production using the + button.

**To add a mobile device:**

- In your production card, activate the function **DEVICE SYNCHRONIZATION** on the left-hand side of the top bar.
- Click on the button **MD Manager** on the left-hand side of the top bar.
  - A new window opens and shows a list of all known and connected mobile devices.
- Click on **PAIRING MODE** to set the Base Station to pairing mode.
  - The Base Station remains in pairing status for 5 minutes.
- Switch on your mobile device and activate **Pairing Mode** if it has not been activated automatically (**Switching the SEK on and off**, **Pairing the SEK to the Base Station**).
  - After a few seconds, the available mobile devices are displayed in the list.
- Click on the **Add** button in the line of the mobile device to be added.
  - A confirmation code is displayed both in LinkDesk and on the mobile device.
- Compare the displayed code at both endpoints.
- In LinkDesk, click on **Confirm** to pair the selected mobile device.

> The mobile device has been added to the Base Station and is indicated as a separate card. The card shows the connected Base Station and the occupied RF channel. The device state color changes to:
>
> - green: successful operation, or
> - yellow: warning (e.g. if the audio links have not yet been assigned (see also Device state colors and Routing editor).

## Displaying device information

You can display detailed information relating to your Spectera device.

Find out here which device information can be displayed in the details view for mobile devices or for the Base Station.

**In order to display detailed information:**

- Click on the card of your Spectera device (Base Station or mobile device).
  - An additional navigation menu will appear on the right-hand side of the window.
- Observe all the details in the menu by scrolling up and down.

Detailed information is displayed.

## Changing the device name

You can change the device name for your mobile device.

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

**To change the device name:**

- Click on your mobile device card.
  - An additional navigation menu will appear on the right-hand side of the window.
- Edit the name under **Device name**.
  - The name is immediately transmitted to the mobile device and saved.

The device name has been changed.

## Configuring IEM/IFB input

You can adjust the **BALANCE** and **VOLUME** of the IEM/IFB input.

**WARNING**

**Danger due to high volume levels**

Volume levels that are too high may damage your hearing.

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

**To configure the IEM/IFB input:**

- Click on your mobile device card.
  - An additional navigation menu will appear on the right-hand side of the window.
- Click on the drop-down menu **Input IEM/IFB** and adapt the settings for:
  - BALANCE
  - HEADPHONE VOLUME
  - HEADPHONE VOLUME LIMITER
- Click on **EDIT ROUTES** to configure the audio link mode.

## Configuring MIC/LINE output

You can adjust the **PREAMP GAIN** and **LOW CUT** of the MIC/ LINE output.

**WARNING**

**Danger due to high volume levels**

Volume levels that are too high may damage your hearing.

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

**To configure the MIC/LINE output:**

- Click on your mobile device card.
  - An additional navigation menu will appear on the right-hand side of the window.
- Click on the drop-down menu **Output MIC/LINE** and adapt the settings for:
  - **TEST TONE**, to simulate and test the performance of your audio devices in different dB levels,
  - **CABLE EMULDATION**, to emulate the capacitance of connected cables and influence the sound of your mic/line input,
  - **PREAMP GAIN**, to adjust the pre amplification OR
  - **LOW CUT**, to minimize wind noise.
- Click on **EDIT ROUTES** to configure the audio link mode.

## Removing a mobile device

You can remove your mobile devices from your current production.

When you remove a mobile device from the production card, LinkDesk will still remember and keep it paired. You can re-add this device to your production card at any time through the MD Manager.

**NOTICE**

**The audio signal will be interrupted immediately!**

By removing the connected mobile devices, the audio signal of connected devices will be interrupted immediately!

- Only remove mobile devices if no active audio is being used.

**To remove the mobile device:**

- On your mobile device card, click on the 3 dots and then on **Delete**.
- Click on **OK**.

✓ The mobile device has been removed.

## Updating the firmware (mobile devices)

The firmware version of the mobile devices can be downloaded and updated manually.

The Base Station update typically ensures that all components are included so no manual downloads are required. Once the Base Station firmware is updated, the user will be guided through the process of updating the mobile devices (MDs). MDs with an older firmware version cannot be used until they are updated.

If the user pairs a mobile device with outdated firmware, it will not work until the update is performed. The update can be started from the mobile device context file.

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

**NOTICE**

**Loss of data if the firmware transfer is interrupted**

If the transfer is interrupted, this may lead to a loss of data. The devices may be damaged by this.

- Do not remove any connections to the stationary devices during firmware updates.
- Do not disconnect the devices from the mains power. For portable devices, use fully charged batteries where possible!
- Place the portable devices in a stable position in front of the infrared interface for the duration of the update.

**To update your mobile device firmware:**

- Click on your mobile device card.
  - ✓ An additional navigation menu will appear on the right-hand side of the window.
- Navigate to the drop-down menu **Hardware details**.
- Click on **UPLOAD FILE** and select the manually downloaded firmware.
  - ✓ The firmware file has been selected.
- Click on **UPDATE** to start the update process.

> **i** The update is carried out as a broadcast, meaning all mobile devices with outdated firmware will be recognized and updated one by one.

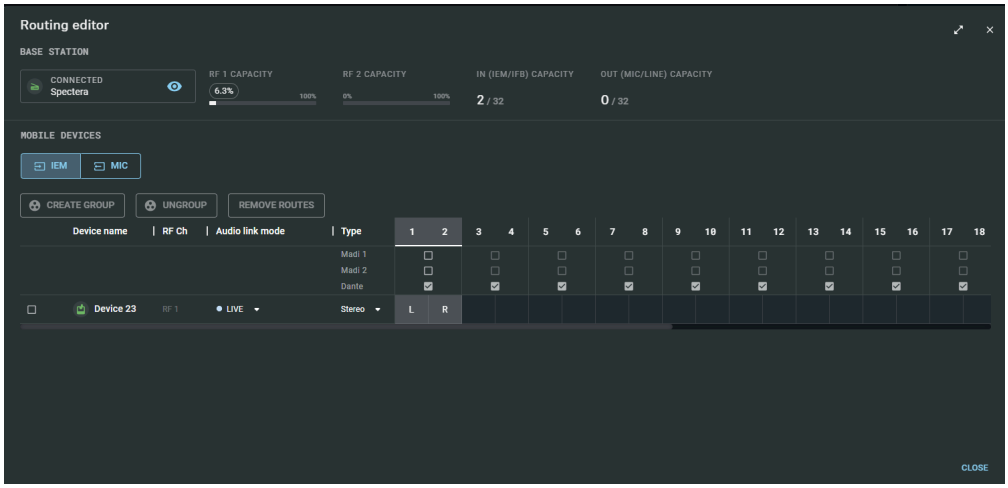
The firmware has been updated.

# Routing editor

The editor serves as a basic configurator for mobile devices and also provides an overview of all connected devices with their total capacity utilization within an RF spectrum.

The editor can be used to:

- Select connected Base Stations and show up the configured RF channels
- Assign RF channels to mobile devices;
- Configure audio link modes for mobile devices;
- Configure audio types for mobile devices
- Assign up to 32 audio links for IEM/IFB input and MIC output




1. Routing settings

## Base Station

- Summarized view of the selected base station with the configured channels and inputs/outputs.

## Mobile devices

- Selection and display of a mobile device by signal type (IEM or MIC).

## Groups

- Possibility to group devices and remove groups or the defined routes.

> **i** You can group IEM links to listen to the same mix and economize RF resources. Any IEM link on a mobile device can be freely moved in and out of a group, and groups can even be merged together.

### Routing settings

- The customized configuration of individual paired mobile devices.
- **Device name**
    - Display of all paired mobile devices.
- **RF channel**
    - Display of the channel assignment of the individual mobile device.
- **Audio link mode**
    - Selection of preset audio link modes with indication of their capacity impact:
        - Not set
        - LIVE Link Density
        - LIVE
        - LIVE Low Latency
        - LIVE Ultra Low Latency
- **Mode Type**
    - Type of the available mode (stereo/mono).
- **Audio Links**
    - Assignment of individual links for IEM/MIC, with specification of the existing sound type (stereo/mono).

## Defining audio routes

With the routing editor, you can easily route the audio of your connected devices and monitor the capacity impact.

The following settings must be made to route the audio:

- Select the affected input or output
- Select a suitable audio link mode
- Select the audio type
- Assign the audio link number

**To select the setting for your IEM or MIC channel:**

▶ Under **MOBILE DEVICES** click on  IEM or  MIC.

✓ The channel has been selected.

**To select the Audio Link Mode:**

- Navigate to the row of the mobile device to be configured and select the desired mode in the **Audio link mode** column.

  i Depending on the selected mode, the capacity utilization of the HF channel will be adapted and the influence on important parameters will be shown.

  ✓ The Audio Link mode has been selected.

**NOTICE**

**This action will reset the audio channel assignment and audio link mode for this device**

The audio might be interrupted.

- Make sure that no live audio is being used.

- Navigate to the row of the mobile device to be configured and select the desired mode in the **Type** column.

  ✓ The audio type has been selected.

**To assign the audio link:**

- Navigate to the row of the mobile device to be routed and select the desired link in the numbering column.

  ✓ The audio link has been assigned.

✓ The audio links have been routed.

## Removing audio routes

You can remove defined audio routes from the routing editor.

**NOTICE**

**This action will reset the audio channel assignment and audio link mode for this device**

The audio might be interrupted.

- Make sure that no live audio is being used.

**To remove defined audio routes:**

- In your production card, navigate to **ROUTING EDITOR**.
- Activate the check-box of the mobile devices for which the audio routes are to be deleted.
- Click on the button **REMOVE ROUTES** > **OK**.

The defined audio routes have been removed.

# Error Handling

Summary of the typical error messages that can occur and how to resolve them.

## Base Station cannot be claimed

### Condition

A failure occurs during the claiming process.

### Cause

Base Station is currently in-use and cannot be claimed.

### Remedy

- Use a different Base Station or deactivate the sync status in a running production (Activating device synchronization).

## Mobile devices cannot be paired

### Condition

The pairing function is deactivated.

### Cause

The RF channel of the Base Station is muted.

### Remedy

- Unmute the RF channel (see Muting/unmuting RF signals).

# 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:

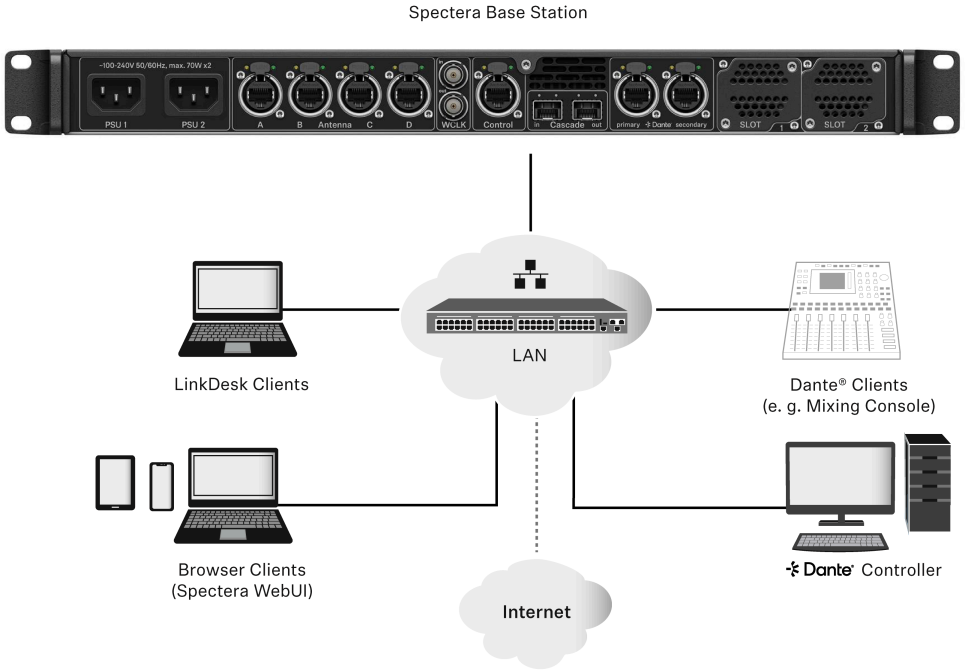
- When using managed switches, ensure that they allow EEE (Energy Efficient Ethernet or "Green Ethernet") to be disabled. Make sure that EEE is disabled on all ports used for real-time Dante traffic.
- When using unmanaged switches, do not use switches that support the EEE function, because it cannot 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.

**Dante® restrictions**

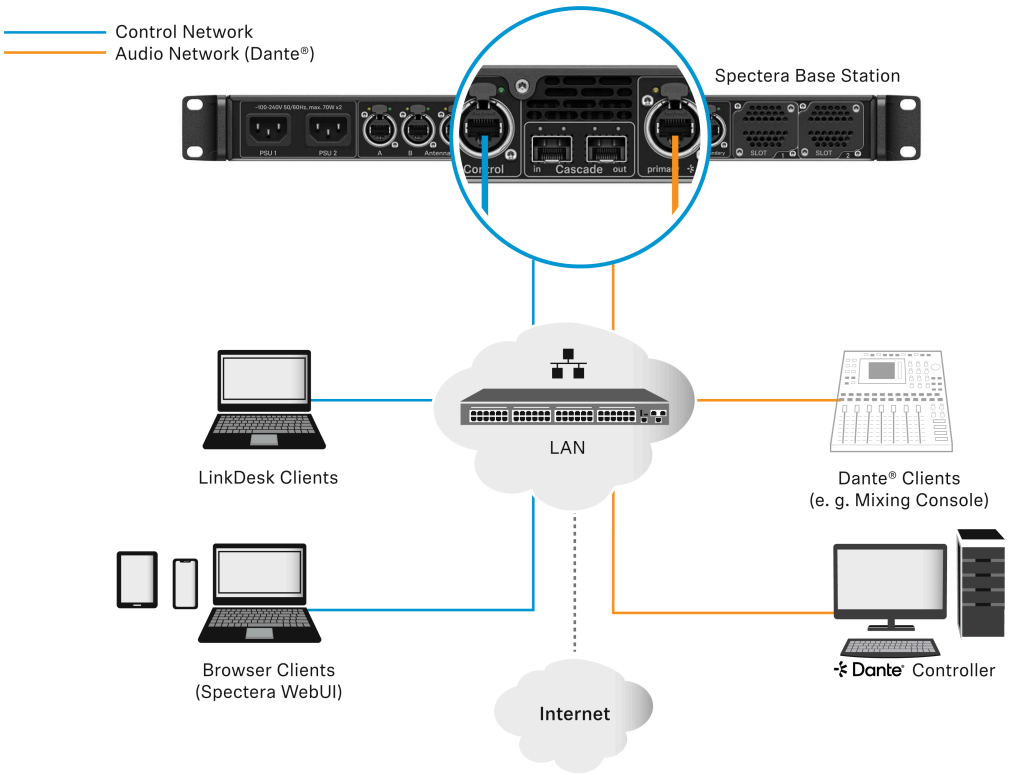
- It is not possible to deactivate the Dante® functionality for the both Dante® ports.
- Dante® ports are shutdown when the device is in standby mode.
- Network configuration of Dante® ports can only be done via Dante® Controller software application.
- By default the Dante® ports are configured to Auto 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.

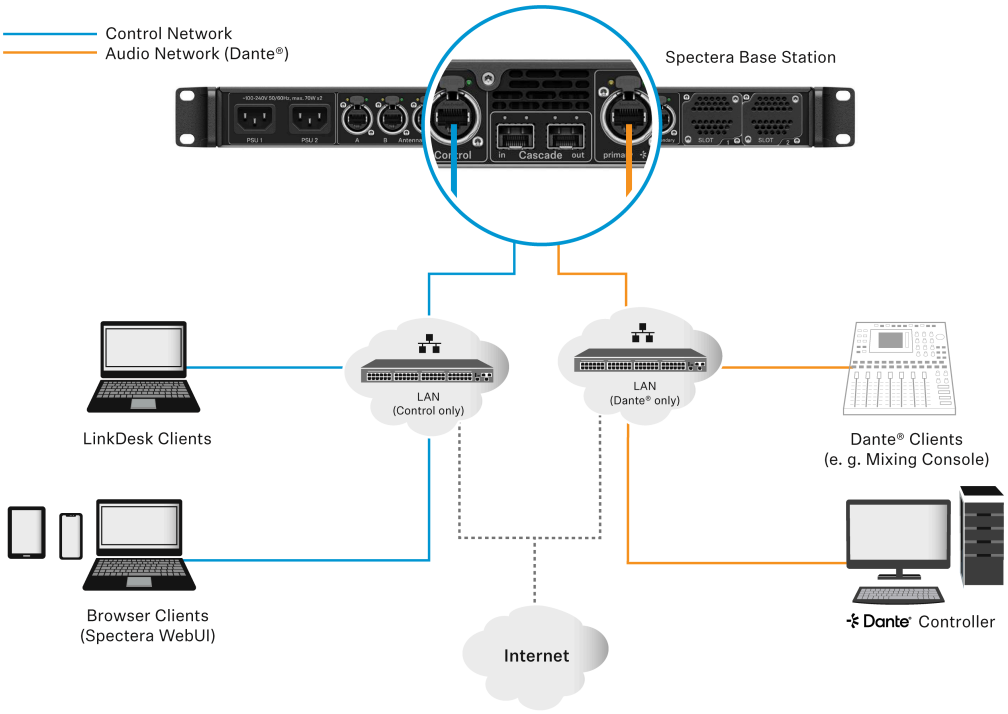
The Spectera Base Station can not be configured to use VLAN tagging (IEEE 802.1Q) at its network ports. Still it is possible to use network switches that support VLANs to separate the Control and Dante® traffic within the same physical network. Please make sure that the switch is configured to forward 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
LAN
(Control only)
LAN
(Dante® only)
LinkDesk Clients
Dante® Clients
(e. g. Mixing Console)
Browser Clients
(Spectera WebUI)
Dante Controller
Internet

# 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<br>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

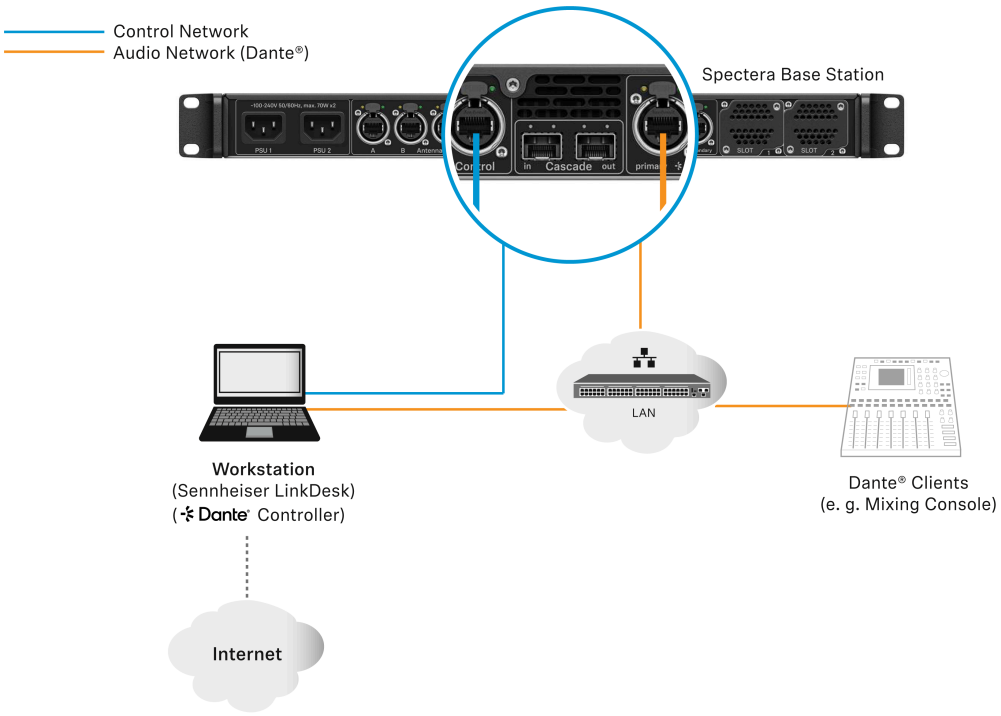
## Sharing Internet connection in small network setups

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)).

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

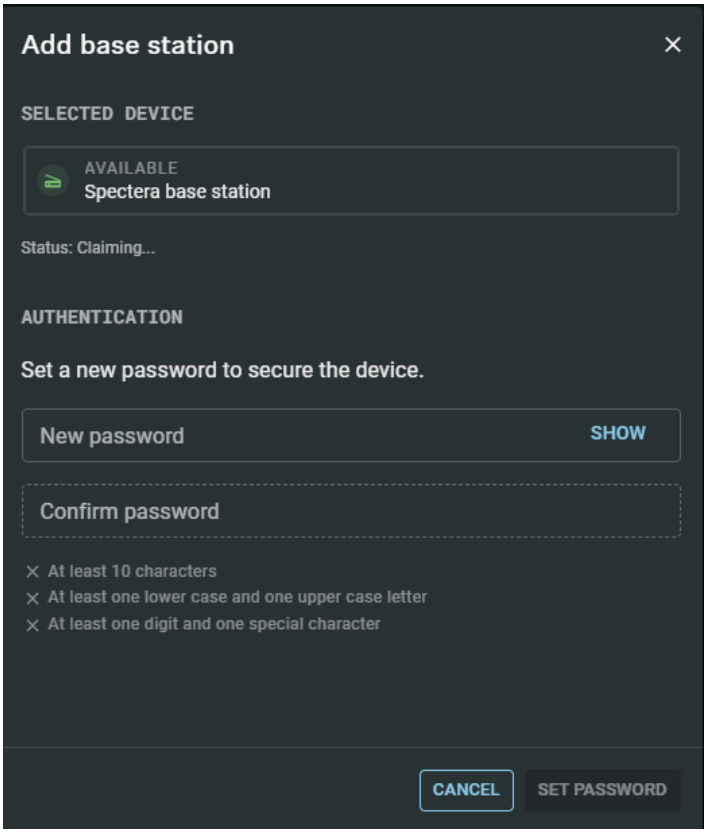
- At least ten characters
- At least one lowercase letter
- At least one uppercase letter
- At least one number
- At least one special character: !#$%&()*+,-./:;<=>?@[]^_{|}~
- Maximum length: 64 characters

## Claiming single device (LinkDesk)

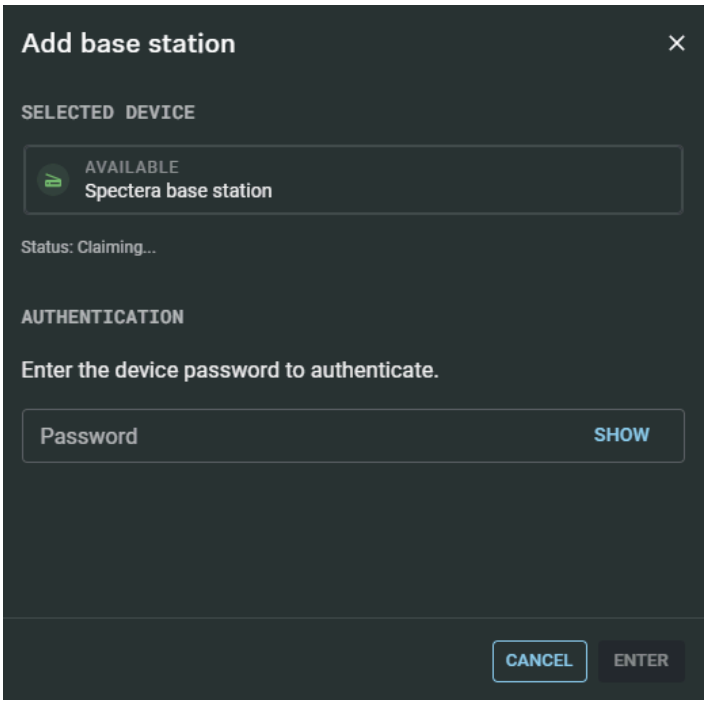
Instructions for claiming a single device in Sennheiser LinkDesk.

**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:




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




> **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:**

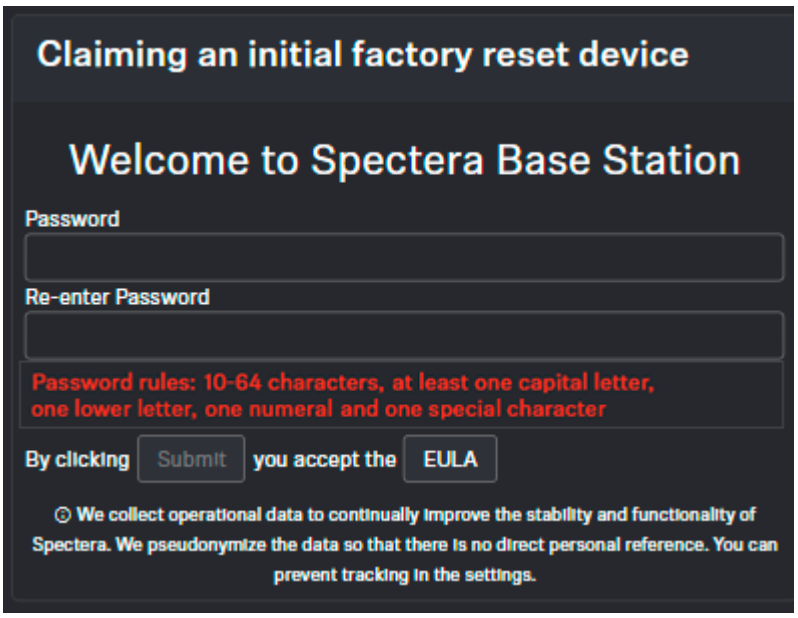
- Depending on the firmware version, enter the following URL into your browser:
  - Firmware 0.8.x: `https://deviceIP/specteracontrol/index.html`
  - Firmware ≥1.0.0: `https://deviceIP/specterawebui/index.html`

> **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.

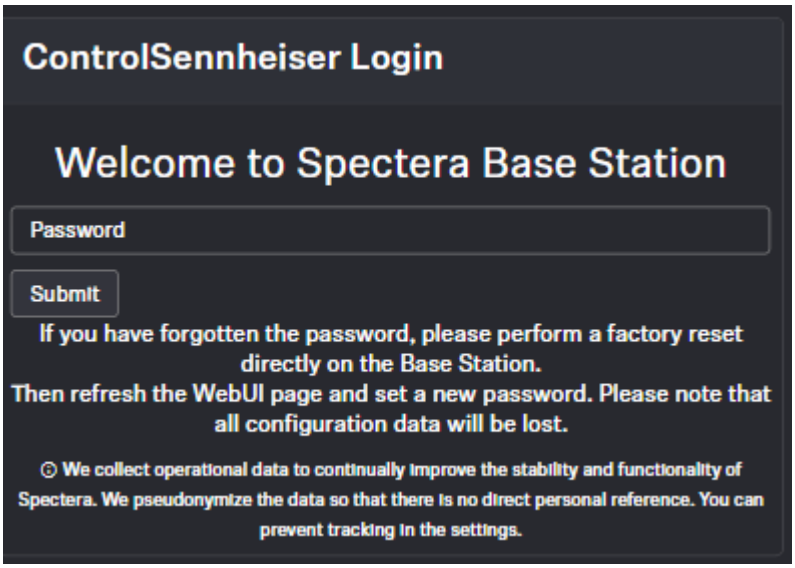
- Depending on your browser, click on **Advanced** and then on:
  - **Continue to localhost (unsafe)** (Microsoft Edge)
  - **Proceed to localhost (unsafe)** (Google Chrome)
  - **Accept the Risk and Continue** (Firefox)
  - or similar (other browsers).

✓ 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:




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




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**.

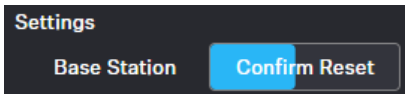
✓ Your Base Station has been claimed successfully.

## 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:**

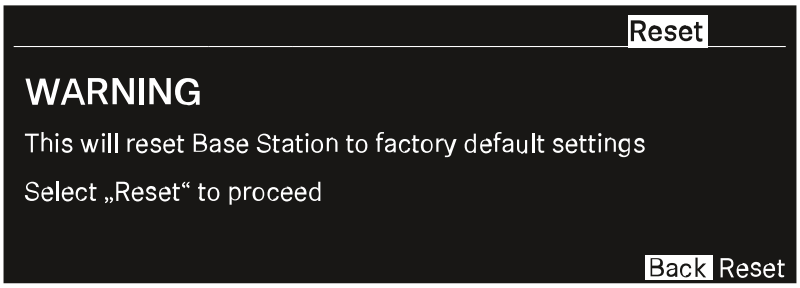
- In the top bar, navigate to **Configuration** > **Base Station**.
- Click on **Settings** and then on **Factory Reset**.
  - A countdown timer will be displayed (highlighted in blue).




- 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.




- 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.

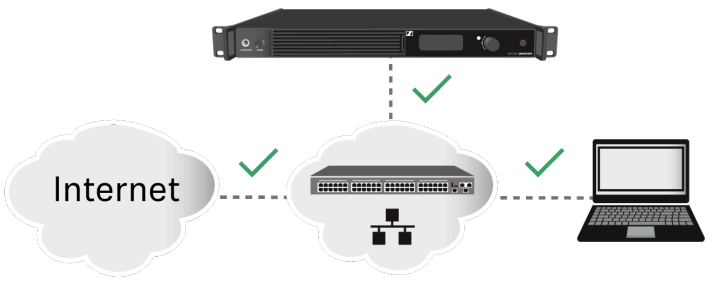
### Causes

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

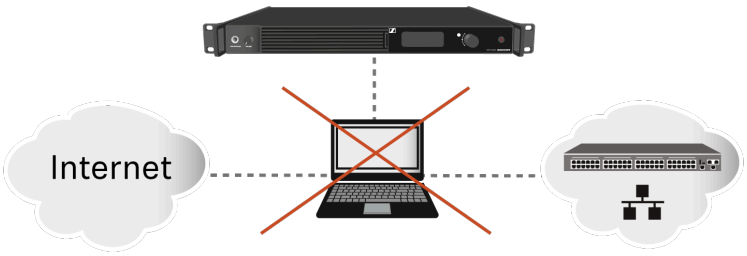
1. The Base Station was not connected properly and has no Internet connection (see Solution 1: Establish a proper connection of the Base Station to the Internet).
2. The license server and/or NTP time server are/is unreachable due to missing port permissions, preventing license key authorization and 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. Specifications

All technical data, system and server requirements and required ports at a glance.

## 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

## 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<br>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

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