Spectera

Security Guide for IT Administrators, System Integrators and Event Technicians

PDF export of the original HTML instructions

Contents

1. Introduction 3
2. Key product security features 4
AES-256 Link Encryption 4
Control Protocol Encryption 5
Device Claiming & Authentication 6
Dante® Media Encryption (available as of Spectera Dante® firmware Brooklyn3 version 1.1.0) 7
3. How to use the security features 8
Certificates 8
Device authentication 9
Claiming single device (LinkDesk) 10
Claiming single device (WebUI) 12
Resetting the device password (Spectera Base Station) 14

1. 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.

2. 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

3. How to use the security features

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

Certificates

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

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

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

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

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

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

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

Device authentication

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

You can claim the Base Station via:

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

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

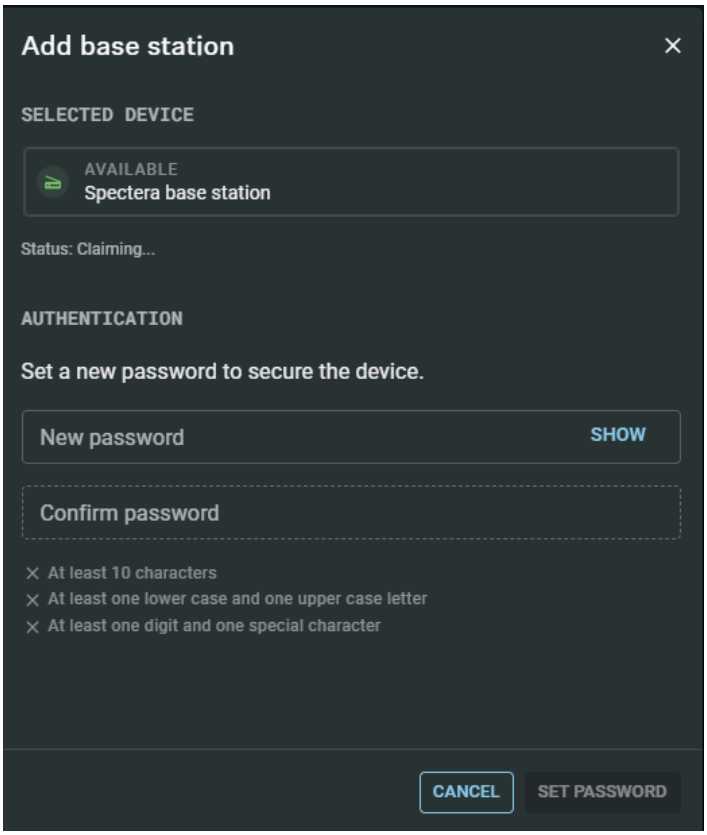
- At least ten characters
- At least one lowercase letter
- At least one uppercase letter
- At least one number
- At least one special character: !#$%&()*+,-./:;<=>?@[]^_{|}~
- Maximum length: 64 characters

Claiming single device (LinkDesk)

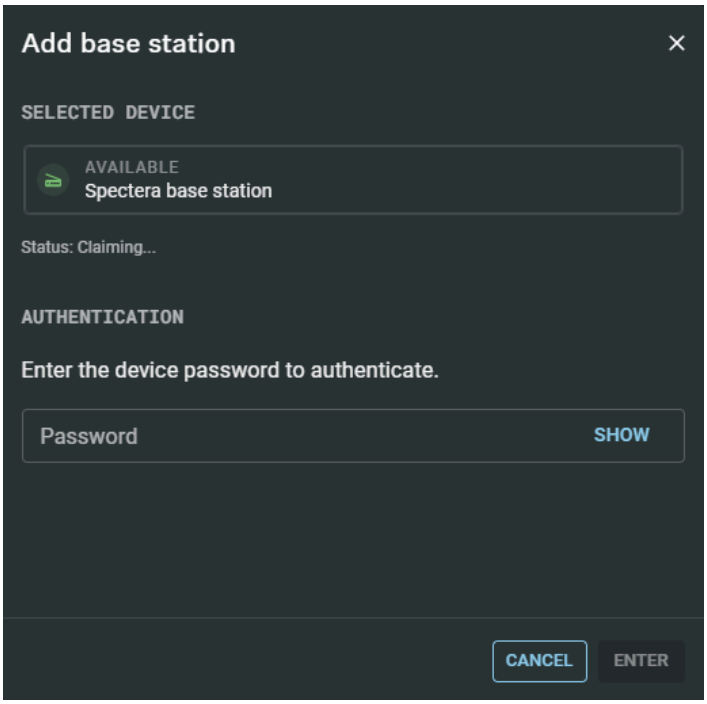
Instructions for claiming a single device in Sennheiser LinkDesk.

To claim your Base Station:

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



  - 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:

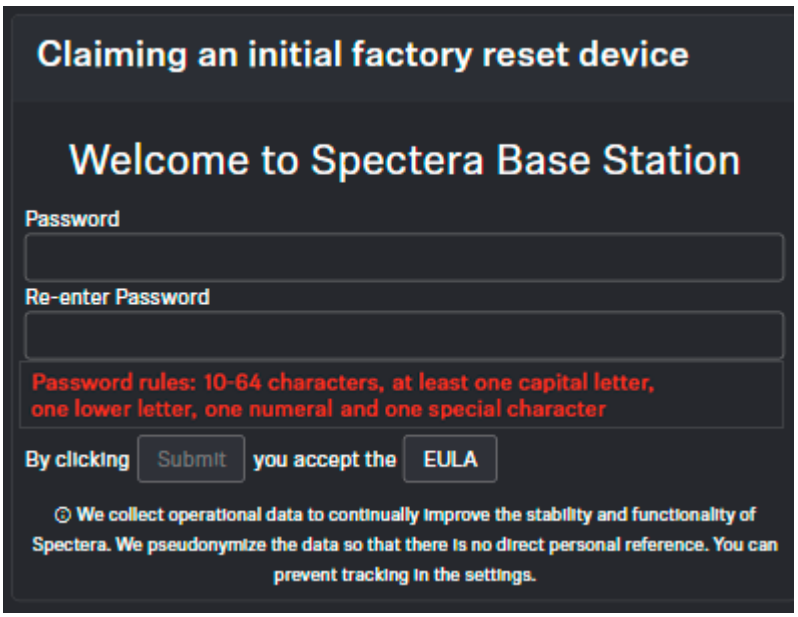
- Depending on the firmware version, enter the following URL into your browser:
  - Firmware 0.8.x: `https://deviceIP/specteracontrol/index.html`
  - Firmware ≥1.0.0: `https://deviceIP/specterawebui/index.html`

> **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.

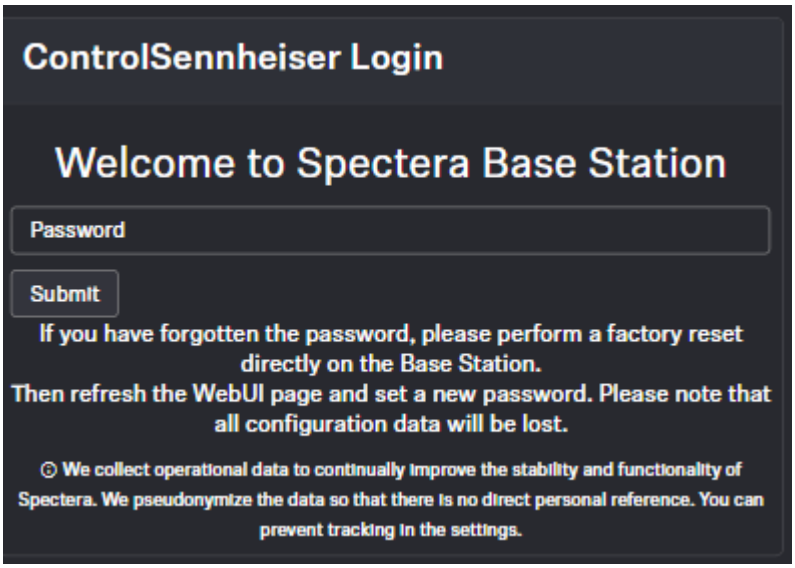
- Depending on your browser, click on **Advanced** and then on:
  - **Continue to localhost (unsafe)** (Microsoft Edge)
  - **Proceed to localhost (unsafe)** (Google Chrome)
  - **Accept the Risk and Continue** (Firefox)
  - or similar (other browsers).

✓ 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**.

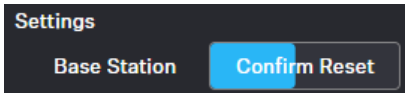
✓ Your Base Station has been claimed successfully.

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:

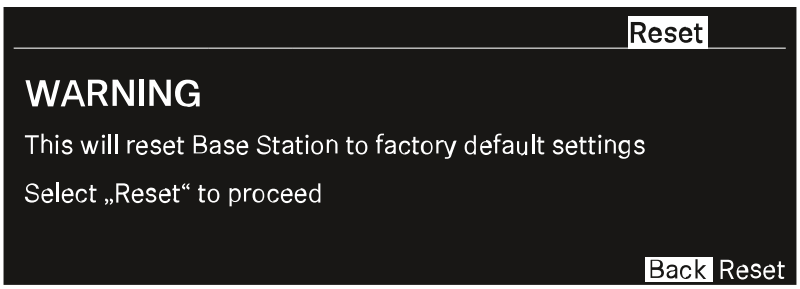
- In the top bar, navigate to **Configuration** > **Base Station**.
- Click on **Settings** and then on **Factory Reset**.
  - A countdown timer will be displayed (highlighted in blue).



- 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.

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