Spectera

Sicherheitsleitfaden für IT-Administratoren, Systemintegratoren und Veranstaltungstechniker

PDF-Export der Original-HTML-Anleitung

Inhalt

Kapitel 1. Sicherheitsleitfaden

Dieser Sicherheitsleitfaden bietet wichtige Informationen und bewährte Praktiken für IT-Administratoren, Systemintegratoren und Veranstaltungstechniker, um sicherzustellen, dass robuste Sicherheitsmaßnahmen effektiv umgesetzt werden.

Professionelle Audiosysteme, die umfangreich in Umgebungen wie Rundfunk, Live-Events und Unternehmenssettings eingesetzt werden, sind zunehmend in Unternehmensnetzwerke integriert – was sie anfällig für Bedrohungen wie unbefugten Zugriff, Datenabfang und Signalstörungen macht. Um eine sichere Bereitstellung und Systemintegrität zu gewährleisten, setzt Sennheiser die höchsten Sicherheitsstandards für alle Produkte durch, unterstützt von robusten Schutzmaßnahmen und umfassenden Managementpraktiken.

- **Sicherheitsprinzipien und Systemdesign:**

  Sennheiser integriert Sicherheit von der Produktentwicklung über regelmäßige Risikoanalysen bis hin zu sicheren Konfigurationen und verfolgt einen Ansatz der „Sicherheit durch Design“. Die Einhaltung internationaler Standards gewährleistet konsistenten Schutz und proaktive Bedrohungsabwehr.

- **Kommunikationssicherheit und Verschlüsselung:**

  Branchenübliche Verschlüsselungsprotokolle wie AES-256 und TLS schützen Audio- und Steuerdaten vor Abfang und unbefugtem Zugriff. Sichere Methoden wie HTTPS und REST-APIs werden für netzwerkbasierte und Drittanbieter-Integrationen verwendet.

- **Authentifizierung und Zugriffskontrolle:**

  Rollenbasierte Authentifizierung und Geräteansprüche validieren Benutzer und Geräte, bevor der Zugriff gewährt wird. Regelmäßige Aktualisierungen und sichere Anmeldeinformationen erhalten die Systemintegrität und verhindern unbefugten Zugriff.

- **Netzwerkkonfiguration und Schnittstellen:**

  Aktivieren Sie nur essentielle Ports, segmentieren Sie Netzwerke und wenden Sie Firewall-Regeln für einen sicheren Betrieb an. Eine ordnungsgemäße Konfiguration von Protokollen wie Dante®, mDNS und Bluetooth® ist entscheidend für eine robuste Netzwerk-Infrastruktur.

Dieser Leitfaden bietet umfassende Maßnahmen zum Schutz professioneller Audiosysteme vor Bedrohungen durch sicheres Design, Verschlüsselung, Authentifizierung und bewährte Praktiken während des gesamten Systemlebenszyklus.

Wichtige Sicherheitsmerkmale des Produkts

Die wichtigsten Sicherheitsmerkmale von Spectera-Geräten und Software-Tools werden detailliert beschrieben und betonen bewährte Verfahren für IT-Administratoren, um eine sichere Kommunikation und den Schutz von Daten zu gewährleisten.

Die Spectera-Geräte (Basisstation, DAD und mobile Geräte (SEK)) sowie Software-Tools wie **Spectera Basisstation WebUI** und **Sennheiser LinkDesk** unterstützen verbesserte

Sicherheitsmaßnahmen, die sowohl eine sichere Verbindung zwischen Geräten über Funk als auch einen sicheren Datentransfer über das Netzwerk gewährleisten. Es bietet die folgenden Sicherheitsmerkmale:

- **AES-256 Link-Verschlüsselung:**

  Die AES-256 Link-Verschlüsselung schützt Audio- und Steuerkommunikation zwischen Geräten.

- **Verschlüsselung des Steuerprotokolls:**

  Die WebUI verwendet immer verschlüsselte HTTPS-Kommunikation. Das SSCv2-Protokoll sichert die Kommunikation zwischen Geräten und Software-Tools über HTTPS.

- **Geräteanspruch und Authentifizierung:**

  Die Funktion Geräteanspruch und Authentifizierung gewährleistet den autorisierten Zugriff auf die Steuerung mithilfe von Passwörtern.

- **Dante® Medienverschlüsselung:**

  Die Dante® Medienverschlüsselung ist eine optionale Kanal Verschlüsselung für Dante-Netzwerke.

AES-256 Link-Verschlüsselung

Alle drahtlosen Kommunikationen zwischen den Spectera-Geräten werden mit AES-256, einem erstklassigen Verschlüsselungsstandard zum Schutz sensibler Daten, gesichert.

Die Link-Verschlüsselung umfasst die folgenden Schnittstellen:

- Die Verbindung zwischen der Basisstation und mobilen Geräten für die Audioübertragung.
- Die Verbindung zwischen der Basisstation und mobilen Geräten zur Synchronisierung der Geräteeinstellungen.

> **i** Die AES-256 Link-Verschlüsselung ist immer aktiviert und kann nicht deaktiviert werden.

Verschlüsselung des Steuerprotokolls

Alle Steuerkommunikationen über das Netzwerk zur Basisstation sind verschlüsselt und authentifiziert.

Es bietet End-to-End-Sicherheit und nutzt HTTPS (TLS 1.3). Die Kommunikation mit dem Sennheiser Lizenzserver ist auf Anwendungsebene verschlüsselt.

Die Protokollverschlüsselung ist immer aktiviert und kann nicht deaktiviert werden.

Geräteanspruch & Authentifizierung

Der Geräteanspruch und die Authentifizierung verbessern die Sicherheit, indem sie einen Passwortschutz für den Gerätezugriff erfordern und sicherstellen, dass nur autorisierte Benutzer die Einstellungen über verschlüsselte Verbindungen ändern können.

Der Gerätezugriff über die Netzwerksteuerungs-API und die WebUI der Spectera Basisstation sowie über Sennheiser LinkDesk ist passwortgeschützt, um zu verhindern, dass unbefugte Akteure im Netzwerk das Gerät konfigurieren.

Die Geräteauthentifizierung ist immer aktiviert und kann nicht deaktiviert werden.

Vorteile des Geräteanspruchs

- **Geräteanspruchsfunktion:**

  Der Geräteanspruch ist eine Funktion der Sennheiser LinkDesk und der Spectera Basisstation WebUI, die es dem Benutzer ermöglicht, das Eigentum an seinen Sennheiser-Geräten zu beanspruchen und eine zusätzliche Sicherheitsebene und Kontrolle zu bieten.

- **Gerätezuweisung:**

  Es ermöglicht die Zuweisung eines Geräts zu einer oder mehreren Remote-Installationen, was eine nicht authentifizierte Gerätesteuerung im Netzwerk verhindert.

- **Erstkonfiguration:**

  Im Rahmen der Erstkonfiguration beanspruchen Benutzer ein Gerät, indem sie ein obligatorisches Gerätepasswort konfigurieren.

- **Benutzerfreundlichkeit:**

  Innerhalb einer Installation können mehrere Softwareanwendungen gleichzeitig mit diesem Gerätepasswort für optimale Benutzerfreundlichkeit verwendet werden.

- **Sicherheitsmaßnahmen:**

  Sobald ein Gerät beansprucht wurde, können seine Einstellungen nur über eine verschlüsselte Verbindung angezeigt und geändert werden, die die Eingabe des Konfigurationspassworts erfordert.

Dante® Medienverschlüsselung (verfügbar ab Spectera Dante® Firmware Brooklyn3 Version 1.1.0)

Dante® Medienverschlüsselung erweitert die Sicherheitsvorteile der Verwendung von Dante® in Ihrem Netzwerk, indem der Medieninhalt während der Übertragung zwischen Geräten verborgen wird.

Dante® verwendet den Advanced Encryption Standard (AES) mit einem 256-Bit-Schlüssel, um branchenführenden Schutz für Medien zu bieten.

Das Verbergen des Inhalts von Medienpaketen verhindert, dass böswillige oder unbefugte Benutzer den Dante-Medienverkehr abhören oder stören.

i Standardmäßig ist die Dante Medienverschlüsselung deaktiviert, da die Verschlüsselung nur über die Dante Director-Anwendung konfiguriert werden kann. Bitte beziehen Sie sich auf die Audinate Dokumentation für detaillierte Informationen zur Dante® Verschlüsselung, wie Sie die Verschlüsselung aktivieren und konfigurieren und die Dante® Firmware aktualisieren:

- Dante Medienverschlüsselung: Audinate/Medienverschlüsselung
- Aktualisierung der Dante® Firmware: Dante Updater

Wie man die Sicherheitsfunktionen nutzt

Der folgende Abschnitt erklärt, wie Sie die verschiedenen Sicherheitsfunktionen sowohl über das Gerät selbst als auch über unterstützte Softwareanwendungen nutzen können.

Zertifikate

Die Spectera Base Station verwendet ein selbstsigniertes Zertifikat für die Netzwerkkommunikation.

> **i** Derzeit ist es nicht möglich, es durch ein von der Zertifizierungsstelle signiertes Zertifikat zu ersetzen. Das Zertifikat wird werkseitig generiert und bei jedem Werksreset erneuert.

Wenn Sie zum ersten Mal mit einem Browser auf die Spectera WebUI zugreifen, erhalten Sie eine Sicherheitswarnung, die über ein unbekanntes Zertifikat informiert. Die Sicherheitswarnung hängt vom verwendeten Browser ab. Klicken Sie je nach Browser auf **Erweitert** oder **Details anzeigen** (Safari) und dann auf:

- Microsoft Edge: **Weiter zu localhost (unsicher)**
- Google Chrome: **Weiter zu localhost (unsicher)**
- Firefox: **Risiko akzeptieren und fortfahren**
- Apple Safari: **[...] diese Website besuchen** > **Website besuchen**
- oder ähnlich (andere Browser)

Um Man-in-the-Middle-Angriffe (MITM) zu verhindern, verfügt Sennheiser LinkDesk über einige integrierte Sicherheitsmaßnahmen. Aufgrund dieser Maßnahmen erhalten Sie möglicherweise eine Warnung zu einem Zertifikatkonflikt, wenn Sie mit einer Base Station arbeiten. In einigen Fällen können diese auftreten, obwohl tatsächlich kein Sicherheitsproblem vorliegt. Diese sind:

- Die Base Station wurde seit der letzten Verbindung auf die Werkseinstellungen zurückgesetzt. In diesem Fall können Sie die Verbindung sicher bestätigen und fortfahren, wenn eine Konfliktwarnung auftritt.
- Eine andere Base Station wurde über dieselbe IP-Adresse verbunden. Überprüfen Sie in diesem Fall, ob die verwendete IP-Adresse tatsächlich die richtige IP-Adresse der vorgesehenen Base Station ist.

Geräteauthentifizierung

Der Zugriff auf die Geräte über das Netzwerk ist passwortgeschützt und das Gerät muss in der Steuerungssoftware vor der Nutzung beansprucht werden.

Sie können die Basisstation über:

- LinkDesk (siehe Einzelgerät claimen (LinkDesk)) oder
- WebUI (siehe Einzelgerät claimen (WebUI)).

i Bitte beachten Sie, dass das neue Passwort die folgenden Anforderungen erfüllen muss:

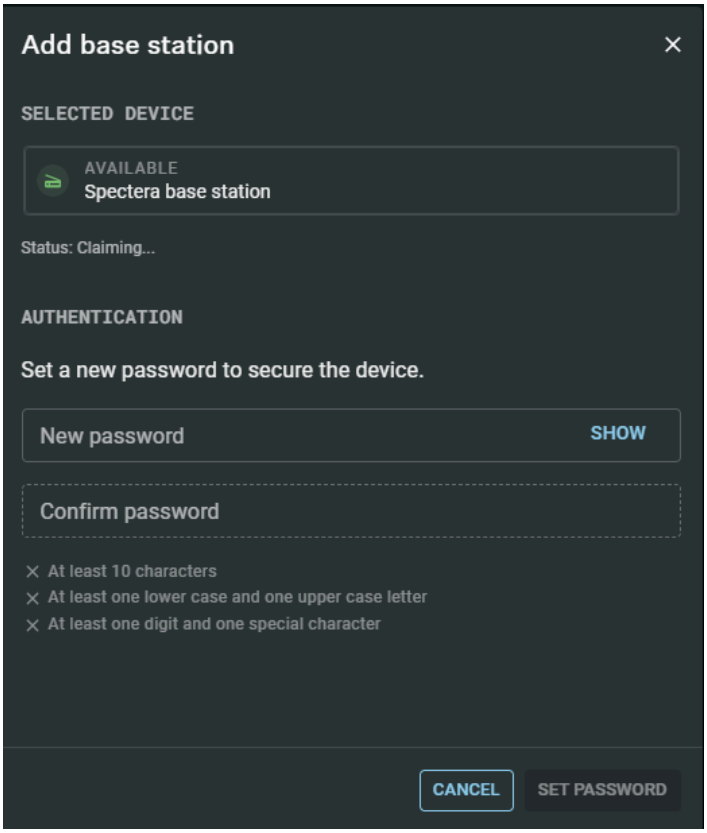
- Mindestens zehn Zeichen
- Mindestens ein Kleinbuchstabe
- Mindestens ein Großbuchstabe
- Mindestens eine Zahl
- Mindestens ein Sonderzeichen: !#$%&()*+,-./:;<=>?@[]^_{|}~
- Maximale Länge: 64 Zeichen

Einzelgerät claimen (LinkDesk)

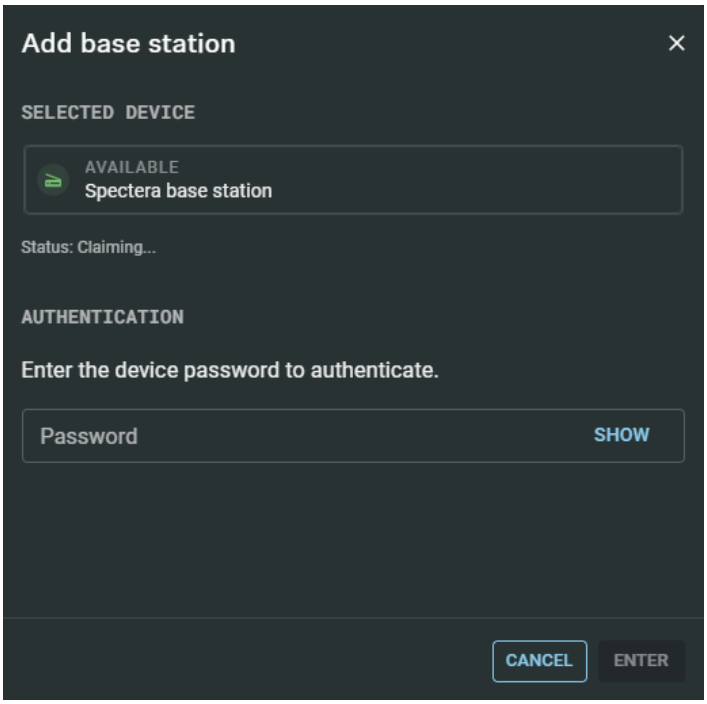
Anweisungen zum Beanspruchen eines einzelnen Geräts in Sennheiser LinkDesk.

Um Ihre Base Station zu beanspruchen:

- Aktivieren Sie in Ihrer Produktionskarte die Funktion **GERÄTESYNCHRONISIERUNG** auf der linken Seite der oberen Leiste.
- Klicken Sie auf das + Symbol in der **BASE STATIONS** Leiste auf der rechten Seite.
- Geben Sie die korrekte IP-Adresse der Base Station ein und klicken Sie auf **Suche**.
    - Wenn das Gerät sich im Werkszustand befindet und das ursprüngliche Passwort noch zugewiesen ist, wird es automatisch erkannt und angewendet. Als nächstes muss ein neues Passwort festgelegt werden:



    - Wenn das Gerät zuvor von einer anderen Sennheiser LinkDesk- oder Spectera WebUI-Instanz beansprucht wurde, muss das zuvor festgelegte Passwort eingegeben werden:



> **i** Wenn Sie sich nicht an das zuvor festgelegte Passwort erinnern können, führen Sie bitte einen Werksreset des Geräts durch. Nach dem Reset wird das Standardpasswort für Spectera automatisch von der Software angewendet.

- Legen Sie ein neues Gerätepasswort fest (wenn Sie sich zum ersten Mal anmelden) oder geben Sie das Passwort ein, das Sie bereits zur Authentifizierung zugewiesen haben (wenn Sie sich bereits angemeldet haben).

> **i** Bitte beachten Sie, dass das neue Passwort die folgenden Anforderungen erfüllen muss:
>
> - Mindestens zehn Zeichen
> - Mindestens ein Kleinbuchstabe
> - Mindestens ein Großbuchstabe
> - Mindestens eine Zahl
> - Mindestens ein Sonderzeichen: !#$%&()*+,-./:;<=>?@[]^_{|}~
> - Maximale Länge: 64 Zeichen

✓ Ihre Base Station wurde erfolgreich beansprucht.

Einzelgerät claimen (WebUI)

Anleitungen zum Beanspruchen eines einzelnen Geräts in der Spectera WebUI.

Um Ihre Basisstation zu beanspruchen:

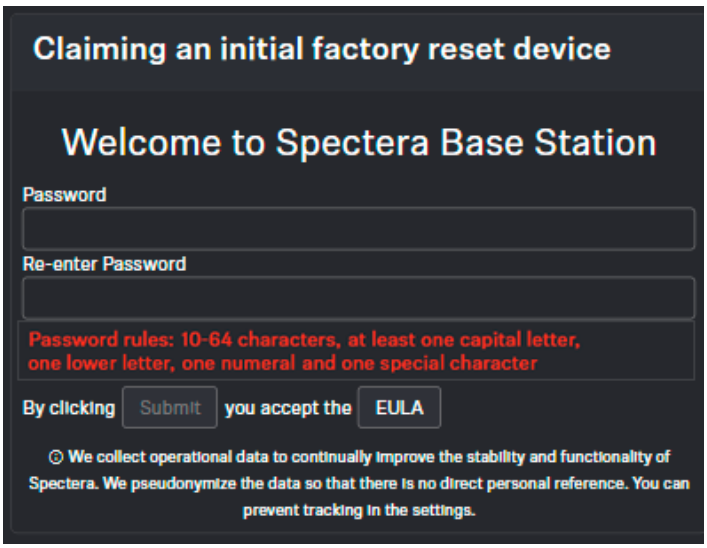
- Je nach Firmware-Version geben Sie die folgende URL in Ihren Browser ein:
  - Firmware 0.8.x: `https://deviceIP/specteracontrol/index.html`
  - Firmware ≥1.0.0: `https://deviceIP/specterawebui/index.html`

> **i** Da das Zertifikat Ihrem Browser unbekannt ist, wird beim ersten Ausführen der Anwendung eine Sicherheitswarnung angezeigt. Die Sicherheitswarnung hängt von dem Browser ab, den Sie verwenden.

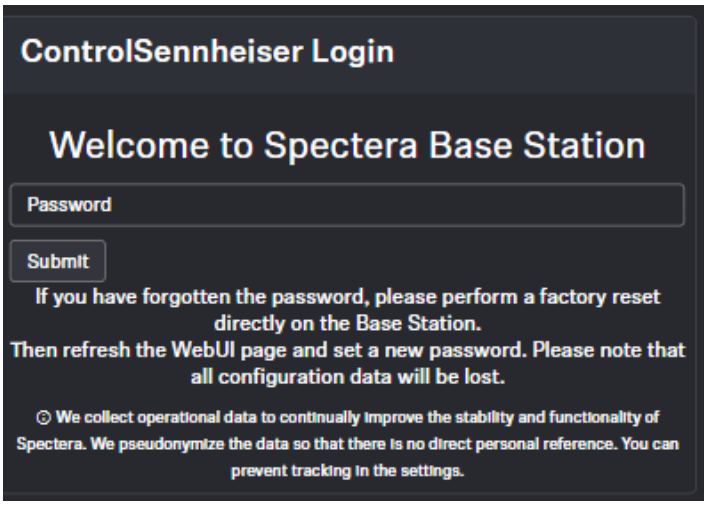
- Je nach Ihrem Browser klicken Sie auf **Erweitert** und dann auf:
  - **Weiter zu localhost (unsicher)** (Microsoft Edge)
  - **Fortfahren zu localhost (unsicher)** (Google Chrome)
  - **Das Risiko akzeptieren und fortfahren** (Firefox)
  - oder ähnlich (andere Browser).

✓ Die WebUI zeigt die folgenden Optionen abhängig vom Zustand des Geräts an:

- Wenn das Gerät sich im Werkszustand befindet und das ursprüngliche Passwort noch zugewiesen ist, wird es automatisch erkannt und angewendet. Als Nächstes muss ein neues Passwort festgelegt werden:



- Wenn das Gerät zuvor von einem anderen Sennheiser LinkDesk oder Spectera WebUI-Instanz beansprucht wurde, muss das zuvor festgelegte Passwort eingegeben werden:



> **i** Wenn Sie sich nicht an das zuvor festgelegte Passwort erinnern können, führen Sie bitte einen Werksreset des Geräts durch. Nach dem Reset wird das Standardpasswort für Spectera automatisch von der Software angewendet.

- Legen Sie ein neues Gerätepasswort fest (wenn Sie sich zum ersten Mal anmelden) oder geben Sie das Passwort ein, das Sie bereits zur Authentifizierung zugewiesen haben (wenn Sie sich bereits angemeldet haben).
- Klicken Sie auf **Absenden**.

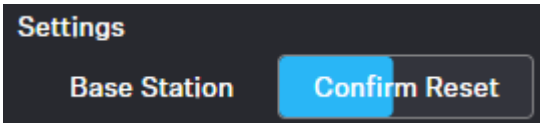
✓ Ihre Base Station wurde erfolgreich beansprucht.

Zurücksetzen des Gerätepassworts (Spectera Basisstation)

Das Gerätepasswort kann nur durch einen Werksreset zurückgesetzt werden (entweder direkt am Gerät oder remote über die WebUI):

Zurücksetzen der Base Station:

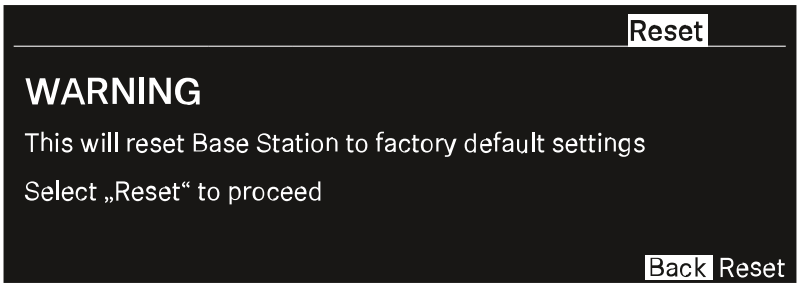
- Navigieren Sie in der oberen Leiste zu **Konfiguration** > **Base Station**.
- Klicken Sie unter **Settings**(Einstellungen) auf **Factory Reset** (Werkseinstellungen).
  - Es wird eine ablaufende Zeitleiste angezeigt (blau hinterlegt).



- Drücken Sie auf **Confirm Reset**, um das Zurücksetzen auf Werkseinstellungen zu bestätigen.

So setzen Sie die Base Station auf die Werkseinstellungen zurück:

- Drehen Sie an der Base Station das Jog-Dial und navigieren Sie zum Menü **Reset**.
- Drücken Sie das Jog-Dial, um das Menü zu öffnen.
  - Eine Warnung wird angezeigt.



- Drehen Sie das Jog-Dial auf **Reset**.
- Drücken Sie das Jog-Dial erneut.
  - Die Base Station wird auf die Werkseinstellungen zurückgesetzt und neu gestartet.

> **i** Überprüfen Sie nach dem Neustart die IP-Adresse, da sie sich möglicherweise geändert hat.

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