Spectera

Guía de Seguridad para Administradores de TI, Integradores de Sistemas y Técnicos de Eventos

Exportación a PDF de las instrucciones originales en HTML

Contents

Capítulo 1. Guía de seguridad

Esta Guía de Seguridad proporciona información esencial y mejores prácticas para los administradores de TI, integradores de sistemas y técnicos de eventos para garantizar que se implementen medidas de seguridad robustas de manera efectiva.

Los sistemas de audio profesional, ampliamente desplegados en entornos como la radiodifusión, eventos en vivo y entornos corporativos, están cada vez más integrados en redes empresariales, lo que los hace susceptibles a amenazas como el acceso no autorizado, la interceptación de datos y la interferencia de señales. Para garantizar un despliegue seguro y la integridad del sistema, Sennheiser aplica los más altos estándares de seguridad en todos los productos, respaldados por medidas de protección robustas y prácticas de gestión integrales.

- **Principios de Seguridad y Diseño del Sistema:**

  Sennheiser incorpora la seguridad desde el desarrollo del producto a través de evaluaciones de riesgos regulares y configuraciones seguras, siguiendo un enfoque de "seguridad por diseño". El cumplimiento de estándares internacionales garantiza una protección consistente y una mitigación proactiva de amenazas.

- **Seguridad de la Comunicación y Cifrado:**

  Protocolos de cifrado estándar de la industria como AES-256 y TLS protegen los datos de audio y control de la interceptación y el acceso no autorizado. Se utilizan métodos seguros como HTTPS y REST APIs para integraciones en red y de terceros.

- **Autenticación y Control de Acceso:**

  La autenticación basada en roles y la reclamación de dispositivos validan a los usuarios y dispositivos antes de otorgar acceso. Las credenciales y actualizaciones regulares mantienen la integridad del sistema y previenen el acceso no autorizado.

- **Configuración de Red e Interfaces:**

  Habilitar solo los puertos esenciales, segmentar redes y aplicar reglas de firewall para un funcionamiento seguro. La configuración adecuada de protocolos como Dante®, mDNS y Bluetooth® es crítica para una infraestructura de red robusta.

Esta guía proporciona medidas integrales para proteger los sistemas de audio profesional de amenazas a través de un diseño seguro, cifrado, autenticación y mejores prácticas a lo largo del ciclo de vida del sistema.

Características clave de seguridad del producto

Se detallan las características clave de seguridad de los dispositivos y herramientas de software de Spectera, enfatizando las mejores prácticas para que los administradores de TI aseguren la comunicación segura y la protección de datos.

Los dispositivos de Spectera (Base Station, DAD y Dispositivos Móviles (SEK)) y herramientas de software como **Spectera Base Station WebUI** y **Sennheiser LinkDesk** apoyan medidas de seguridad mejoradas, asegurando tanto una conexión segura entre dispositivos a través

de radio como una transferencia de datos segura a través de la red. Ofrece las siguientes características de seguridad:

- **Cifrado de Enlace AES-256:**

  El Cifrado de Enlace AES-256 protege la comunicación de audio y control entre dispositivos.

- **Cifrado de Protocolo de Control:**

  El WebUI siempre utiliza comunicación HTTPS cifrada. El protocolo SSCv2 asegura la comunicación entre dispositivos y herramientas de software a través de HTTPS.

- **Reclamación de Dispositivos y Autenticación:**

  La función de Reclamación de Dispositivos y Autenticación asegura el acceso de control autorizado utilizando contraseñas.

- **Cifrado de Medios Dante®:**

  El Cifrado de Medios Dante® es un cifrado de canal opcional para redes Dante.

Cifrado de Enlace AES-256

Toda la comunicación inalámbrica entre los dispositivos Spectera estará protegida con AES-256, un estándar de cifrado de primer nivel diseñado para salvaguardar datos sensibles.

El cifrado de enlace incluye las siguientes interfaces:

- La conexión entre la Base Station y los Dispositivos Móviles para la transmisión de audio.
- La conexión entre la Base Station y los Dispositivos Móviles para la sincronización de la configuración del dispositivo.

i El cifrado de enlace AES-256 está siempre habilitado y no se puede desactivar.

Cifrado del Protocolo de Control

Toda la comunicación de control a través de la red hacia la Base Station está cifrada y autenticada.

Ofrece seguridad de extremo a extremo, utilizando HTTPS (TLS 1.3). La comunicación con el servidor de licencias de Sennheiser está cifrada a nivel de aplicación.

El cifrado del protocolo está siempre habilitado y no se puede desactivar.

Reclamación y Autenticación de Dispositivos

La reclamación y autenticación de dispositivos mejoran la seguridad al requerir protección por contraseña para el acceso al dispositivo y asegurar que solo los usuarios autorizados puedan modificar la configuración a través de conexiones cifradas.

El acceso al dispositivo a través de la API de control de red y WebUI de la Base Station de Spectera y a través de Sennheiser LinkDesk está protegido por contraseña, para evitar la configuración del dispositivo por actores no autorizados dentro de la red.

La autenticación del dispositivo está siempre habilitada y no se puede desactivar.

Beneficios de la reclamación de dispositivos

- **Función de Reclamación de Dispositivos:**

  La reclamación de dispositivos es una función del Sennheiser LinkDesk y la WebUI de la Base Station de Spectera que permite al usuario reclamar la propiedad de sus dispositivos Sennheiser, proporcionando una capa adicional de seguridad y control.

- **Asignación de Dispositivos:**

  Permite asignar un dispositivo a una o más instalaciones remotas, lo que previene cualquier control de dispositivo no autenticado dentro de la red.

- **Configuración Inicial:**

  Como parte de la configuración inicial, los usuarios reclaman un dispositivo configurando una contraseña de dispositivo obligatoria.

- **Usabilidad:**

  Dentro de una instalación, múltiples aplicaciones de software pueden usarse simultáneamente con esta contraseña de dispositivo para una usabilidad óptima.

- **Medidas de Seguridad:**

  Una vez que un dispositivo es reclamado, su configuración solo puede ser vista y modificada a través de una conexión cifrada, que requiere la entrada de la contraseña de configuración.

Cifrado de Medios Dante® (disponible a partir de la versión 1.1.0 del firmware Brooklyn3 de Spectera Dante®)

El cifrado de medios Dante® extiende los beneficios de seguridad de usar Dante® en su red al ocultar el contenido de los medios durante la transmisión entre dispositivos.

Dante® utiliza el Estándar de Cifrado Avanzado (AES) con una clave de 256 bits para proporcionar protección de medios líder en la industria.

Ocultar el contenido de los paquetes de medios previene que usuarios maliciosos o no autorizados escuchen o interfieran con el tráfico de medios de Dante.

i Por defecto, el cifrado de medios Dante está deshabilitado, ya que el cifrado solo puede ser configurado utilizando la aplicación Dante Director. Por favor, consulte la documentación de Audinate para obtener información detallada sobre el cifrado de Dante®, sobre cómo habilitar y configurar el cifrado y actualizar el firmware de Dante®:

- Cifrado de Medios Dante: Audinate/Cifrado de Medios
- Actualización del firmware de Dante®: Actualizador de Dante

Cómo usar las funciones de seguridad

La siguiente sección explica cómo puede utilizar las diversas funciones de seguridad tanto a través del dispositivo en sí como a través de aplicaciones de software compatibles.

Certificados

La Base Station Spectera utiliza un certificado autofirmado para la comunicación de red.

> **i** Actualmente, no es posible reemplazarlo con un certificado firmado por CA. El certificado se genera en fábrica y se renueva al restablecer los ajustes de fábrica.

Al acceder a la Spectera WebUI con un navegador por primera vez, se le mostrará un aviso de seguridad que indica que hay un certificado desconocido. Dicho aviso dependerá del navegador que use. Dependiendo de su navegador, haga clic en **Avanzado** o **Mostrar detalles** (Safari) y, posteriormente, en:

- Microsoft Edge: **Continuar a localhost (no seguro)**
- Google Chrome: **Acceder a localhost (sitio no seguro)**
- Firefox: **Aceptar el riesgo y continuar**
- Safari de Apple: **[...] visitar este sitio web** > **Visitar este sitio web**
- o similar (en otros navegadores)

Para evitar ataques de tipo «hombre en el medio» (MITM por su sigla en inglés), LinkDesk de Sennheiser incorpora ciertas medidas de seguridad que pueden generar advertencias de error por coincidencia de certificados al utilizar una Base Station. En algunos casos, esto puede ocurrir aunque en realidad no haya ningún problema de seguridad. Los casos más comunes son los siguientes:

- Se han restablecido los ajustes de fábrica de la Base Station desde la última conexión. En este caso, puede confirmar de forma segura la conexión y continuar cuando le aparezca el aviso de no coincidencia.
- Se ha conectado una Base Station diferente a través de la misma dirección IP. En este caso, compruebe si la dirección IP que está utilizando es realmente la dirección IP correcta de la Base Station prevista.

Autenticación de Dispositivos

El acceso a los dispositivos a través de la red está protegido por contraseña y el dispositivo debe ser reclamado en el software de control antes de su uso.

Puede reclamar la Base Station a través de:

- LinkDesk (ver Reclamación de un solo dispositivo (LinkDesk)) o
- WebUI (ver Reclamando un dispositivo único (WebUI)).

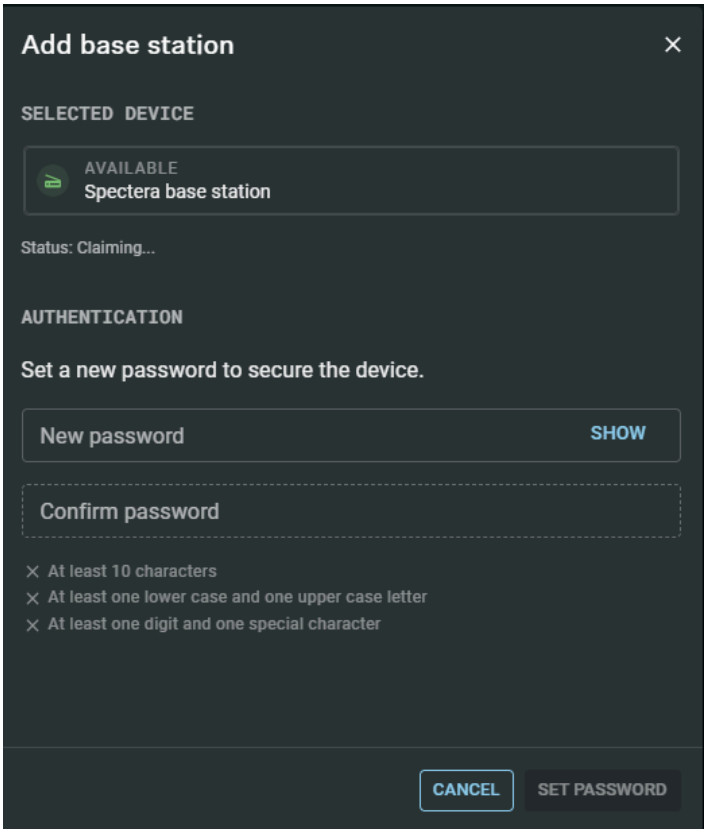
> **i** Tenga en cuenta que la nueva contraseña debe cumplir con los siguientes requisitos:
>
> - Al menos diez caracteres
> - Al menos una letra minúscula
> - Al menos una letra mayúscula
> - Al menos un número
> - Al menos un carácter especial: !#$%&()*+,-./:;<=>?@[]^_{|}~
> - Longitud máxima: 64 caracteres

Reclamación de un solo dispositivo (LinkDesk)

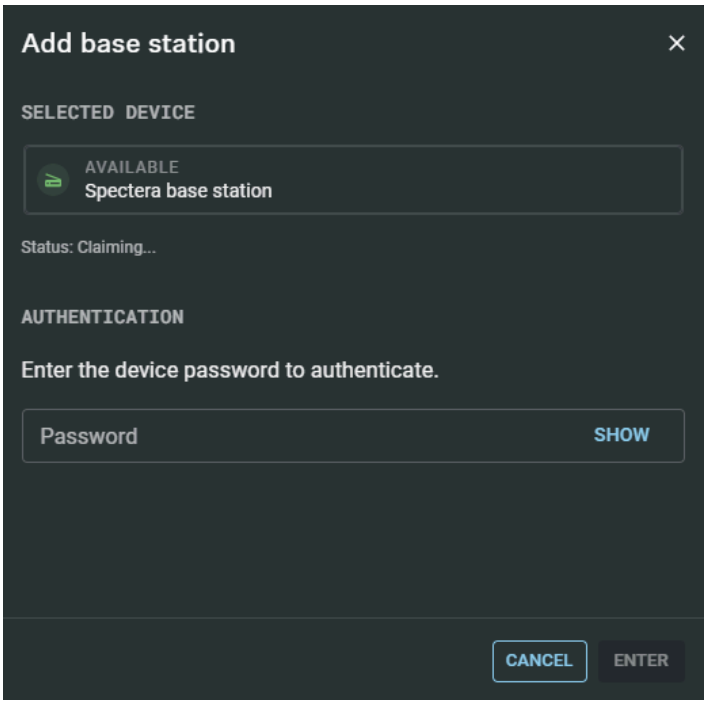
Instrucciones para reclamar un solo dispositivo en Sennheiser LinkDesk.

Para reclamar su Base Station:

- En su tarjeta de producción, active la función **SINCRONIZACIÓN DE DISPOSITIVOS** en el lado izquierdo de la barra superior.
- Haga clic en el símbolo en la barra de **BASE STATIONS** a la derecha.
- Ingrese la dirección IP correcta de la Base Station y haga clic en **Buscar**.
  - Si el dispositivo está en un estado de fábrica y la contraseña original aún está asignada, será detectado y aplicado automáticamente. A continuación, se debe establecer una nueva contraseña:



  - Si el dispositivo fue reclamado previamente por otra instancia de Sennheiser LinkDesk o Spectera WebUI, se debe ingresar la contraseña previamente establecida:



> **i** Si no puede recordar la contraseña previamente establecida, realice un restablecimiento de fábrica del dispositivo. Después del restablecimiento, la contraseña predeterminada para Spectera será aplicada automáticamente por el software.

- Establezca una nueva contraseña para el dispositivo (si está iniciando sesión por primera vez) o ingrese la contraseña que ya ha asignado para la autenticación (si ya ha iniciado sesión).

> **i** Tenga en cuenta que la nueva contraseña debe cumplir con los siguientes requisitos:
>
> - Al menos diez caracteres
> - Al menos una letra minúscula
> - Al menos una letra mayúscula
> - Al menos un número
> - Al menos un carácter especial: !#$%&()*+,-./:;<=>?@[]^_{|}~
> - Longitud máxima: 64 caracteres

✓ Su Base Station ha sido reclamada con éxito.

Reclamando un dispositivo único (WebUI)

Instrucciones para reclamar un único dispositivo en Spectera WebUI.

Para reclamar su Base Station:

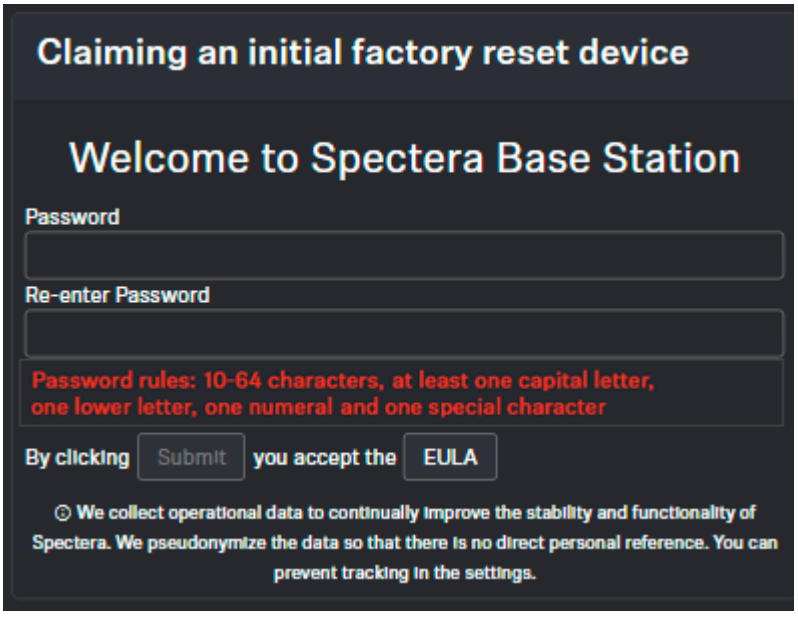
- Dependiendo de la versión del firmware, ingrese la siguiente URL en su navegador:
  - Firmware 0.8.x: `https://deviceIP/specteracontrol/index.html`
  - Firmware ≥1.0.0: `https://deviceIP/specterawebui/index.html`

> **i** Dado que el certificado es desconocido para su navegador, se muestra una advertencia de seguridad la primera vez que ejecuta la aplicación. La advertencia de seguridad depende del navegador que esté utilizando.

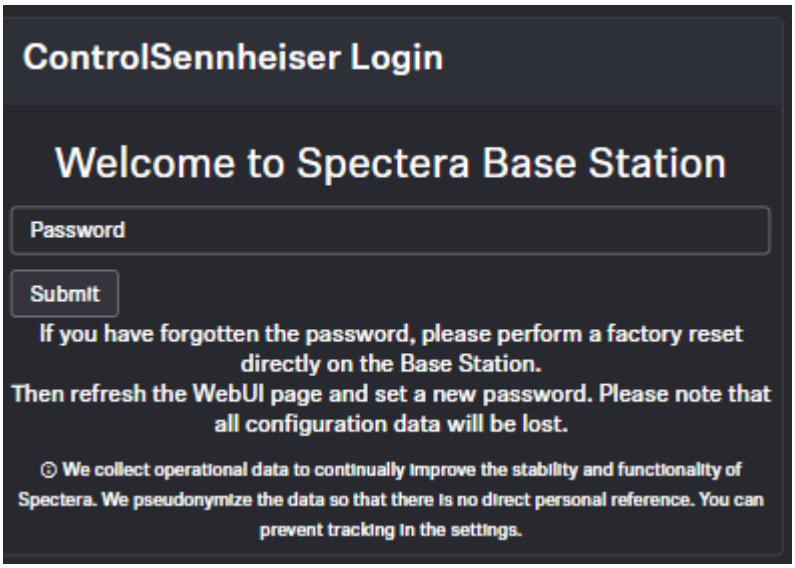
- Dependiendo de su navegador, haga clic en **Avanzado** y luego en:
  - **Continuar a localhost (no seguro)** (Microsoft Edge)
  - **Proceder a localhost (no seguro)** (Google Chrome)
  - **Aceptar el riesgo y continuar** (Firefox)
  - o similar (otros navegadores).

✓ La WebUI muestra las siguientes opciones dependiendo del estado del dispositivo:

- Si el dispositivo está en un estado de fábrica y la contraseña original está aún asignada, se detectará y aplicará automáticamente. A continuación, se debe establecer una nueva contraseña:



- Si el dispositivo fue reclamado previamente por otra instancia de Sennheiser LinkDesk o Spectera WebUI, se debe ingresar la contraseña previamente establecida:



i Si no puede recordar la contraseña previamente establecida, realice un restablecimiento de fábrica del dispositivo. Después del restablecimiento, la contraseña predeterminada para Spectera será aplicada automáticamente por el software.

- Establezca una nueva contraseña para el dispositivo (si está iniciando sesión por primera vez) o ingrese la contraseña que ya ha asignado para la autenticación (si ya ha iniciado sesión).
- Haga clic en **Enviar**.

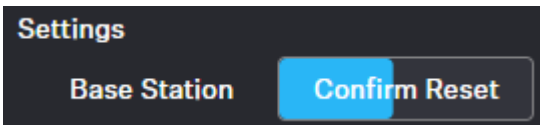
✓ Su Base Station ha sido reclamada con éxito.

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):

Para restablecer la Base Station:

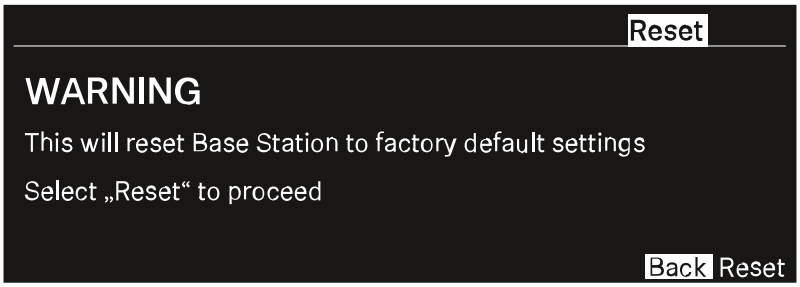
- En la barra superior, vaya a **Configuración** > **Base Station**.
- Haga clic en **Settings** (Configuración) y luego en **Factory Reset** (Restablecimiento de fábrica).
  - Se mostrará una línea de tiempo en cuenta regresiva (resaltada en azul).



- Presione **Confirm Reset** para confirmar el restablecimiento a los valores de fábrica.

Para restablecer los ajustes de fábrica de la Base Station:

- En la Base Station, gire el dial selector hasta llegar al menú **Reset**.
- Pulse el dial selector para entrar en el menú.
  - Aparecerá una advertencia.



- Gire el dial selector hasta llegar a **Reset**.
- Pulse de nuevo el dial selector.
  - La Base Station se restablecerá a sus ajustes de fábrica y se reiniciará.

> **i** Compruebe la dirección IP después del reinicio, ya que puede haber cambiado.

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