Spectera

Guia de Segurança para Administradores de TI, Integradores de Sistema e Técnicos de Evento

Exportar PDF do manual original HTML

Índice

Capítulo 1. Guia de Segurança

Este Guia de Segurança fornece informações essenciais e melhores práticas para administradores de TI, integradores de sistemas e técnicos de eventos para garantir que medidas de segurança robustas sejam implementadas de forma eficaz.

Sistemas de áudio profissionais, amplamente utilizados em ambientes como transmissões, eventos ao vivo e configurações corporativas, estão cada vez mais integrados a redes empresariais — tornando-os suscetíveis a ameaças como acesso não autorizado, interceptação de dados e interferência de sinal. Para garantir a implantação segura e a integridade do sistema, a Sennheiser impõe os mais altos padrões de segurança em todos os produtos, apoiados por medidas de proteção robustas e práticas de gestão abrangentes.

- **Princípios de Segurança e Design do Sistema:**

  A Sennheiser incorpora segurança desde o desenvolvimento do produto por meio de avaliações de risco regulares e configurações seguras, seguindo uma abordagem de "segurança por design". A conformidade com padrões internacionais garante proteção consistente e mitigação proativa de ameaças.

- **Segurança da Comunicação e Criptografia:**

  Protocolos de criptografia padrão da indústria, como AES-256 e TLS, protegem dados de áudio e controlo contra interceptação e acesso não autorizado. Métodos seguros, como HTTPS e APIs REST, são utilizados para integrações em rede e de terceiros.

- **Autenticação e Controle de Acesso:**

  A autenticação baseada em funções e a reivindicação de dispositivos validam usuários e dispositivos antes de conceder acesso. Credenciais e atualizações regulares mantêm a integridade do sistema e previnem acesso não autorizado.

- **Configuração de Rede e Interfaces:**

  Ative apenas portas essenciais, segmente redes e aplique regras de firewall para operação segura. A configuração adequada de protocolos como Dante®, mDNS e Bluetooth® é crítica para uma infraestrutura de rede robusta.

Este guia fornece medidas abrangentes para proteger sistemas de áudio profissionais contra ameaças por meio de design seguro, criptografia, autenticação e melhores práticas ao longo do ciclo de vida do sistema.

Principais características de segurança do produto

As principais características de segurança dos dispositivos e ferramentas de software Spectera são detalhadas, enfatizando as melhores práticas para administradores de TI garantirem comunicação segura e proteção de dados.

Os dispositivos Spectera (Base Station, DAD e Dispositivos Móveis (SEK)) e ferramentas de software como **Base Station WebUI** e **Sennheiser LinkDesk** suportam medidas de segurança aprimoradas, garantindo tanto uma conexão segura entre dispositivos via

rádio quanto transferência de dados segura pela rede. Oferece os seguintes recursos de segurança:

- **Criptografia de Link AES-256:**

  A Criptografia de Link AES-256 protege a comunicação de áudio e controle entre dispositivos.

- **Criptografia de Protocolo de Controle:**

  O WebUI utiliza sempre comunicação HTTPS criptografada. O protocolo SSCv2 protege a comunicação entre dispositivos e ferramentas de software via HTTPS.

- **Reivindicação e Autenticação de Dispositivos:**

  A funcionalidade de Reivindicação e Autenticação de Dispositivos garante acesso de controle autorizado usando senhas.

- **Criptografia de Mídia Dante®:**

  A Criptografia de Mídia Dante® é uma criptografia de canal opcional para redes Dante.

Criptografia de Link AES-256

Todas as comunicações sem fio entre os dispositivos Spectera serão protegidas com AES-256, um padrão de criptografia de alto nível projetado para proteger dados sensíveis.

A Criptografia de Link inclui as seguintes interfaces:

- A conexão entre a Base Station e Dispositivos Móveis para transmissão de áudio.
- A conexão entre a Base Station e Dispositivos Móveis para sincronização de configurações do dispositivo.

> **i** A Criptografia de Link AES-256 está sempre ativada e não pode ser desativada.

Criptografia do Protocolo de Controle

Toda a comunicação de controle pela rede para a Base Station é encriptada e autenticada.

Oferece segurança de ponta a ponta, utilizando HTTPS (TLS 1.3). A comunicação com o servidor de licenças da Sennheiser é encriptada a nível de aplicação.

A Criptografia do Protocolo está sempre ativada e não pode ser desativada.

Reivindicação e Autenticação de Dispositivos

A reivindicação e autenticação de dispositivos aumentam a segurança ao exigir proteção por senha para acesso ao dispositivo e garantir que apenas usuários autorizados possam modificar configurações através de conexões criptografadas.

O acesso ao dispositivo via API de controle de rede e WebUI da Base Station Spectera e via Sennheiser LinkDesk é protegido por senha, para evitar a configuração do dispositivo por atores não autorizados dentro da rede.

A Autenticação de Dispositivo está sempre ativada e não pode ser desativada.

Benefícios da reivindicação de dispositivos

- **Recurso de Reivindicação de Dispositivo:**

  A reivindicação de dispositivo é um recurso do Sennheiser LinkDesk e da WebUI da Base Station Spectera que permite ao usuário reivindicar a propriedade de seus dispositivos Sennheiser, proporcionando uma camada extra de segurança e controle.

- **Atribuição de Dispositivo:**

  Permite atribuir um dispositivo a uma ou mais instalações remotas, o que impede qualquer controle de dispositivo não autenticado dentro da rede.

- **Configuração Inicial:**

  Como parte da configuração inicial, os usuários reivindicam um dispositivo configurando uma senha de dispositivo obrigatória.

- **Usabilidade:**

  Dentro de uma instalação, múltiplas aplicações de software podem ser usadas simultaneamente com esta senha de dispositivo para uma usabilidade ideal.

- **Medidas de Segurança:**

  Uma vez que um dispositivo é reivindicado, suas configurações só podem ser visualizadas e modificadas via uma conexão criptografada, que requer a entrada da senha de configuração.

Criptografia de Mídia Dante® (disponível a partir da versão 1.1.0 do firmware Brooklyn3 da Base Station Dante®)

A Criptografia de Mídia Dante® estende os benefícios de segurança do uso do Dante® na sua rede ao ocultar o conteúdo da mídia durante a transmissão entre dispositivos.

O Dante® utiliza o Padrão de Criptografia Avançada (AES) com uma chave de 256 bits para fornecer proteção de mídia líder da indústria.

Ocultar o conteúdo dos pacotes de mídia impede que usuários maliciosos ou não autorizados escutem ou interfiram no tráfego de mídia Dante.

i Por padrão, a Criptografia de Mídia Dante está desativada, uma vez que a criptografia só pode ser configurada usando o aplicativo Dante Director. Consulte a documentação da Audinate para obter informações detalhadas sobre a criptografia Dante®, como habilitar e configurar a criptografia e atualizar o firmware Dante®:

- Criptografia de Mídia Dante: Audinate/Criptografia de Mídia
- Atualizando o firmware Dante®: Atualizador Dante

Como usar os recursos de segurança

A seção a seguir explica como você pode usar os vários recursos de segurança tanto através do próprio dispositivo quanto através de aplicativos de software suportados.

Certificados

A Spectera Base Station utiliza um certificado autoassinado para a comunicação de rede.

> **i** De momento não é possível substituir este por um certificado assinado pela CA (Autoridade Certificadora). O certificado é gerado de fábrica e será renovado a cada reset de fábrica.

Ao aceder à Spectera WebUI pela primeira vez com um navegador será apresentado um aviso de segurança sobre um certificado desconhecido. O aviso de segurança depende do navegador utilizado. Dependendo do seu navegador, clique em **Advanced** (Definições avançadas) ou em **Show Details** (Mostrar detalhes) (Safari) e depois em:

- Microsoft Edge: **Continue to localhost (unsafe) (Continuar para localhost (inseguro))**
- Google Chrome: **Proceed to localhost (unsafe) (Avançar para localhost (inseguro))**
- Firefox: **Accept the Risk and Continue (Aceitar o risco e continuar)**
- Apple Safari: **[...] visit this Website ([...] visitar este website)** > **Visit Website (Visitar website)**
- ou semelhante (outros navegadores)

Para prevenir ataques “man-in-the-middle” (MITM), o Sennheiser LinkDesk tem algumas medidas de segurança integradas. Devido a estas medidas, pode receber um aviso de incompatibilidade de certificados durante o trabalho com uma Base Station. Em alguns casos, tal pode ocorrer mesmo não havendo qualquer problema de segurança. Estes são:

- A Base Station foi reposta às configurações de fábrica desde a última ligação. Neste caso, pode confirmar com segurança a ligação e avançar quando encontrar o aviso de incompatibilidade.
- Foi ligada uma Base Station diferente através do mesmo endereço IP. Neste caso, verifique se o endereço IP que está a usar é realmente o endereço IP correto da Base Station pretendida.

Autenticação de Dispositivos

O acesso aos dispositivos via rede é protegido por senha e o dispositivo deve ser reivindicado no software de controle antes do uso.

Você pode reivindicar a Base Station via:

- LinkDesk (veja Reivindicando um único dispositivo (LinkDesk)) ou
- WebUI (veja Reivindicando um único dispositivo (WebUI)).

i Por favor, note que a nova senha deve atender aos seguintes requisitos:

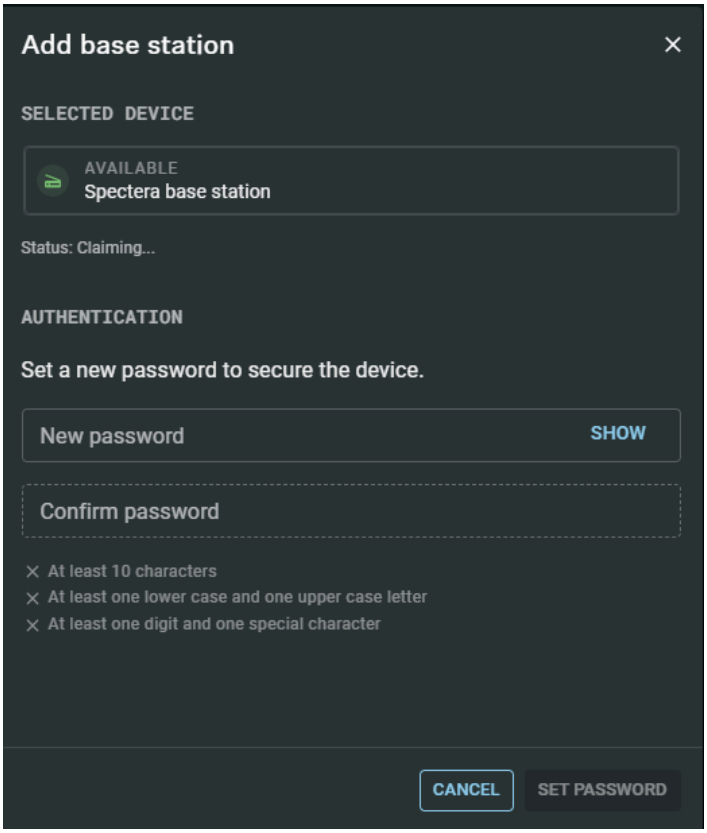
- Pelo menos dez caracteres
- Pelo menos uma letra minúscula
- Pelo menos uma letra maiúscula
- Pelo menos um número
- Pelo menos um caractere especial: !#$%&()*+,-./:;<=>?@[]^_{|}~
- Comprimento máximo: 64 caracteres

Reivindicando um único dispositivo (LinkDesk)

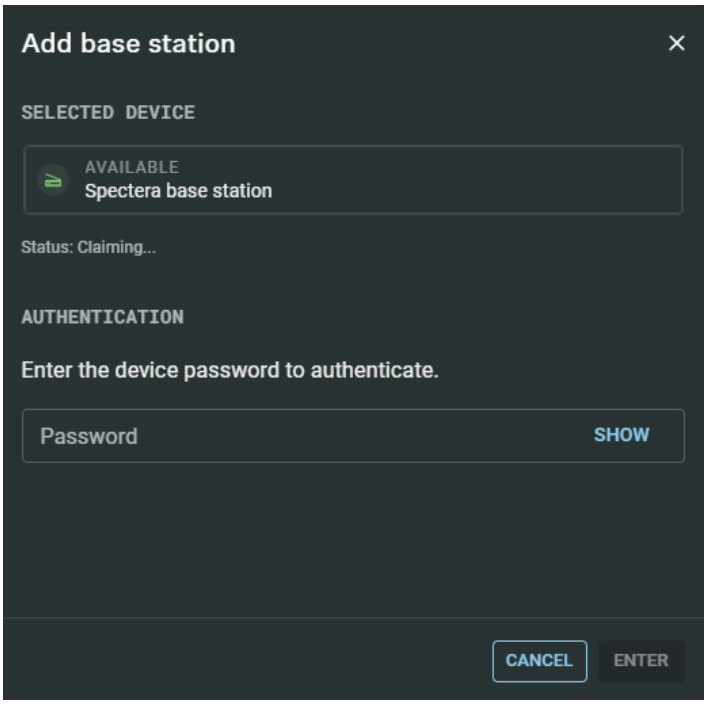
Instruções para reivindicar um único dispositivo no Sennheiser LinkDesk.

Para reivindicar sua Base Station:

- Na sua placa de produção, ative a função **SINCRONIZAÇÃO DE DISPOSITIVOS** no lado esquerdo da barra superior.
- Clique no símbolo + na barra **BASE STATIONS** à direita.
- Digite o endereço IP correto da Base Station e clique em **Pesquisar**.
    - Se o dispositivo estiver em estado de fábrica e a senha original ainda estiver atribuída, ele será automaticamente detectado e aplicado. Em seguida, uma nova senha deve ser definida:



    - Se o dispositivo foi anteriormente reivindicado por outra instância do Sennheiser LinkDesk ou Spectera WebUI, a senha previamente definida deve ser inserida:



ℹ Se você não consegue se lembrar da senha previamente definida, por favor, realize um reset de fábrica do dispositivo. Após o reset, a senha padrão para Spectera será automaticamente aplicada pelo software.

- Defina uma nova senha para o dispositivo (se você estiver fazendo login pela primeira vez) ou insira a senha que você já atribuiu para autenticação (se você já tiver feito login).

ℹ Por favor, note que a nova senha deve atender aos seguintes requisitos:
- Pelo menos dez caracteres
- Pelo menos uma letra minúscula
- Pelo menos uma letra maiúscula
- Pelo menos um número
- Pelo menos um caractere especial: !#$%&()*+,-./:;<=>?@[]^_{|}~
- Comprimento máximo: 64 caracteres

✓ Sua Base Station foi reivindicada com sucesso.

Reivindicando um único dispositivo (WebUI)

Instruções para reivindicar um único dispositivo na WebUI Spectera.

Para reivindicar a sua Base Station:

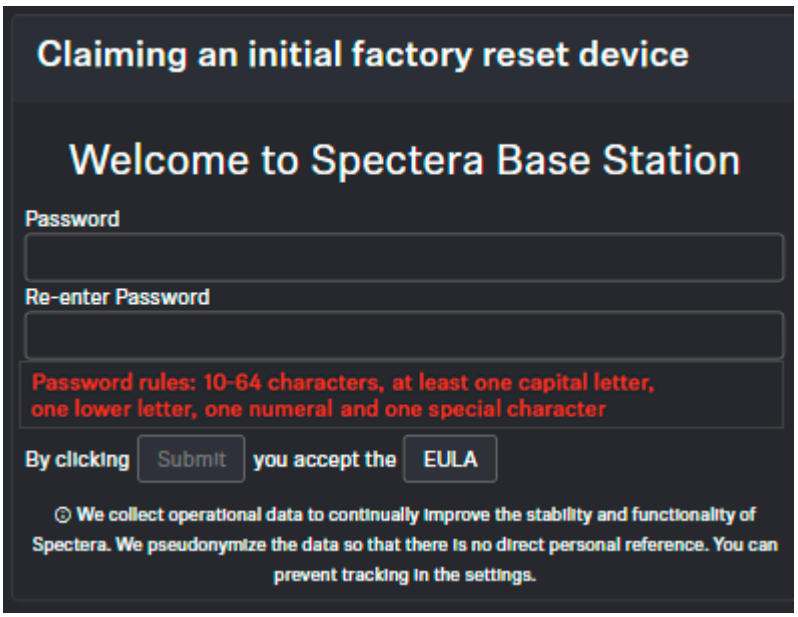
- Dependendo da versão do firmware, insira a seguinte URL no seu navegador:
  - Firmware 0.8.x: `https://deviceIP/specteracontrol/index.html`
  - Firmware ≥1.0.0: `https://deviceIP/specterawebui/index.html`

> **i** Como o certificado é desconhecido para o seu navegador, um aviso de segurança é exibido na primeira vez que você executa o aplicativo. O aviso de segurança depende do navegador que você está usando.

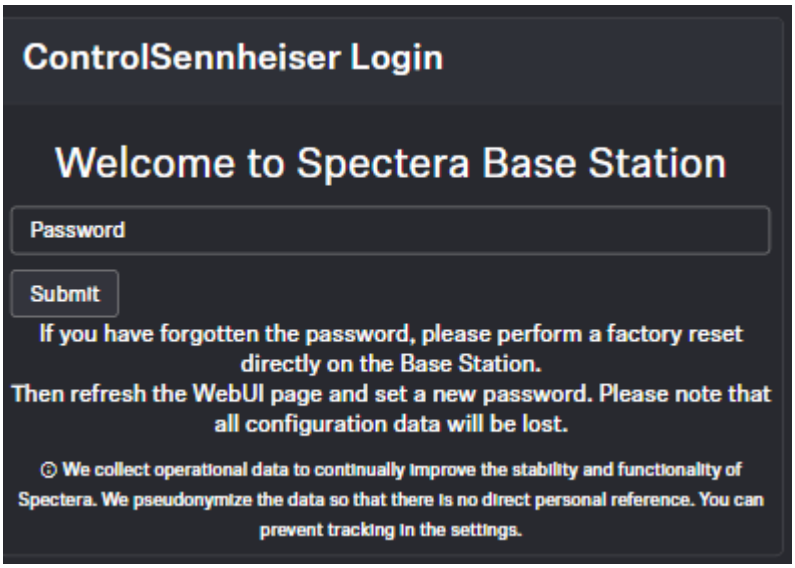
- Dependendo do seu navegador, clique em **Avançado** e depois em:
  - **Continuar para localhost (não seguro)** (Microsoft Edge)
  - **Prosseguir para localhost (não seguro)** (Google Chrome)
  - **Aceitar o Risco e Continuar** (Firefox)
  - ou similar (outros navegadores).

✓ A WebUI exibe as seguintes opções dependendo do estado do dispositivo:

- Se o dispositivo estiver em estado de fábrica e a senha original ainda estiver atribuída, ele será automaticamente detectado e aplicado. Em seguida, uma nova senha deve ser definida:



- Se o dispositivo foi anteriormente reivindicado por outra instância do Sennheiser LinkDesk ou WebUI Spectera, a senha previamente definida deve ser inserida:



i Se você não consegue se lembrar da senha previamente definida, por favor, realize um reset de fábrica do dispositivo. Após o reset, a senha padrão para Spectera será automaticamente aplicada pelo software.

- Defina uma nova senha para o dispositivo (se você estiver fazendo login pela primeira vez) ou insira a senha que você já atribuiu para autenticação (se você já tiver feito login).
- Clique em **Enviar**.

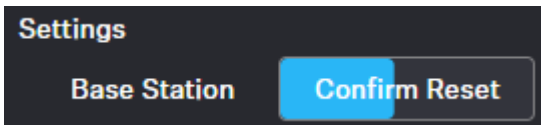
✓ Sua Base Station foi reivindicada com sucesso.

Redefinindo a senha do dispositivo (Base Station Spectera)

A senha do dispositivo só pode ser redefinida através de uma redefinição de fábrica (realizada diretamente no dispositivo ou remotamente via WebUI):

Para repor a Base Station:

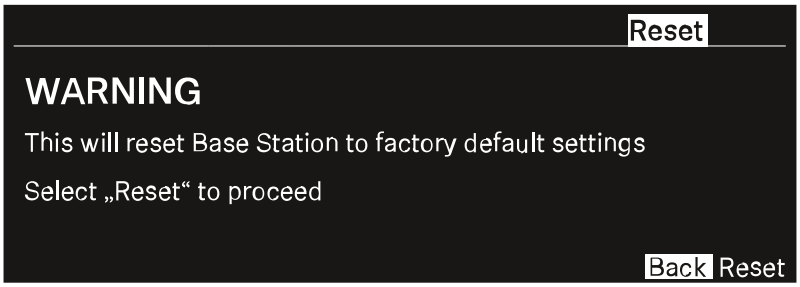
- Na barra superior, navegue para **Configuração** > **Base Station**.
- Clique em **Settings** (Configurações) e depois em **Factory Reset** (Restaurar Padrões de Fábrica).
  - Uma linha do tempo em contagem regressiva será exibida (destacada em azul).



- Pressione **Confirm Reset** para confirmar a restauração para os padrões de fábrica.

Para repor a Base Station para as predefinições de fábrica:

- Na Base Station, rode o botão rotativo e navegue para o menu **Reset**.
- Prima o botão rotativo para aceder ao menu.
  - É apresentado um aviso.



- Rode o botão rotativo até **Reset**.
- Volte a premir o botão rotativo.
  - A Base Station será reposta para as definições de fábrica e reiniciada.

> Após o reinício, verifique o endereço IP pois este pode ter sido alterado.

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