Spectera

IT管理员、系统集成商和事件技术人员的安全指南

原始HTML手册的PDF导出

内容

第1 章. 安全指南

本安全指南为IT管理员、系统集成商和事件技术人员提供了确保有效实施强大安全措施的基本信息和最佳实践。

专业音频系统广泛应用于广播、现场活动和企业环境等场所，越来越多地集成到企业网络中——使其容易受到未经授权的访问、数据拦截和信号干扰等威胁。为了确保安全部署和系统完整性，Sennheiser在所有产品中执行最高的安全标准，并配备强大的保护措施和全面的管理实践。

- **安全原则和系统设计：**

  Sennheiser在产品开发过程中嵌入安全性，通过定期风险评估和安全配置，遵循“设计即安全”的方法。遵守国际标准确保了一致的保护和主动的威胁缓解。

- **通信安全和加密：**

  行业标准的加密协议如AES-256和TLS保护音频和控制数据免受拦截和未经授权的访问。使用HTTPS和REST API等安全方法进行网络和第三方集成。

- **身份验证和访问控制：**

  基于角色的身份验证和设备声明在授予访问权限之前验证用户和设备。凭证和定期更新维护系统完整性，防止未经授权的访问。

- **网络配置和接口：**

  仅启用必要的端口，划分网络，并应用防火墙规则以确保安全操作。正确配置Dante®、mDNS和Bluetooth®等协议对于构建强大的网络基础设施至关重要。

本指南提供了全面的措施，通过安全设计、加密、身份验证和系统生命周期中的最佳实践来保护专业音频系统免受威胁。

关键产品安全特性

详细介绍了Spectera设备和软件工具的关键安全特性，强调IT管理员确保安全通信和数据保护的最佳实践。

Spectera设备（基站、DAD和移动设备（SEK））以及软件工具如 **Spectera Base Station WebUI**和**Sennheiser LinkDesk**支持增强的 安全措施，确保设备之间通过无线电的安全连接和网络上的安全数据传输。它提供以下安全特性：

- **AES-256链路加密：**

  AES-256链路加密保护设备之间的音频和控制通信。

- **控制协议加密：**

  WebUI始终使用加密的HTTPS通信。SSCv2协议通过HTTPS保护设备和软件工具之间的通信。

- **设备声明与认证：**

  设备声明与认证功能确保使用密码进行授权控制访问。

- **Dante®媒体加密：**

  Dante®媒体加密是Dante网络的可选通道加密。

AES-256 链接加密

所有 Spectera 设备之间的无线通信将受到 AES-256 的保护，这是一种旨在保护敏感数据的顶级加密标准。

链接加密包括以下接口：

- 基站与移动设备之间用于音频传输的连接。
- 基站与移动设备之间用于设备设置同步的连接。

> **i** AES-256 链接加密始终启用，无法禁用。

控制协议加密

所有通过网络到基站的控制通信都是加密和认证的。

它提供端到端的安全性，利用HTTPS（TLS 1.3）。与Sennheiser许可证服务器的通信在应用层上是加密的。

协议加密始终启用，无法禁用。

设备声明与认证

设备声明和认证通过要求设备访问的密码保护以及确保只有授权用户可以通过加密连接修改设置来增强安全性。

通过Spectera基站的网络控制API和WebUI以及Sennheiser LinkDesk访问设备是受密码保护的，以避免网络内未经授权的行为者配置设备。

设备认证始终启用，无法禁用。

设备声明的好处

- **设备声明功能：**

  设备声明是Sennheiser LinkDesk和Spectera基站WebUI的一个功能，允许用户声明对其Sennheiser设备的所有权，提供额外的安全性和控制层。

- **设备分配：**

  它允许将设备分配给一个或多个远程安装，防止网络内任何未经认证的设备控制。

- **初始配置：**

  作为初始配置的一部分，用户通过配置强制设备密码来声明设备。

- **可用性：**

  在一个安装中，可以同时使用多个软件应用程序与此设备密码，以实现最佳可用性。

- **安全措施：**

  一旦设备被声明，其设置只能通过加密连接查看和修改，这需要输入配置密码。

Dante® 媒体加密（自 Spectera Dante® 固件 Brooklyn3 版本 1.1.0 起可用）

Dante® 媒体加密通过在设备之间传输时隐藏媒体内容，扩展了在网络上使用 Dante® 的安全性。

Dante® 使用 256 位密钥的高级加密标准（AES）提供行业领先的媒体保护。

隐藏媒体数据包的内容可以防止恶意或未经授权的用户窃听或干扰 Dante 媒体流量。

默认情况下，Dante 媒体加密是禁用的，因为加密只能通过使用 Dante Director 应用程序进行配置。有关 Dante® 加密的详细信息，包括如何启用和配置加密以及更新 Dante® 固件，请参阅 Audinate 文档：

- Dante 媒体加密：Audinate/媒体加密
- 更新 Dante® 固件：Dante 更新程序

如何使用安全功能

以下部分解释了如何通过设备本身和支持的软件应用程序使用各种安全功能。

证书

Spectera Base Station使用自签名证书进行网络通信。

> **i** 当前无法将其替换为CA签名证书。证书在出厂时生成，每次恢复出厂设置时都会更新。

首次通过浏览器访问Spectera WebUI时，您将收到关于未知证书的安全警告。安全警告内容取决于您使用的浏览器。根据浏览器类型，单击高级或显示详细信息(Safari)，然后选择：

- Microsoft Edge: **继续访问本地主机（不安全）**
- Google Chrome: **继续前往本地主机（不安全）**
- Firefox: **接受风险并继续**
- Apple Safari: **[...] 访问此网站** > **访问网站**
- 或类似选项（其他浏览器）

为防止中间人(MITM)攻击，Sennheiser LinkDesk内置了多项安全措施。由于这些措施，您在操作Base Station时可能会收到证书不匹配警告。在某些情况下，即使实际不存在安全问题，也可能出现此类警告。具体情形包括：

- Base Station自上次连接后已恢复出厂设置。在此情况下，您可安全确认连接并在遇到不匹配警告时继续操作。
- 通过相同IP地址连接了其他Base Station。此时请验证您使用的IP地址是否确为目标Base Station的正确IP地址。

设备认证

通过网络访问的设备是密码保护的，设备在使用前必须在控制软件中进行声明。

您可以通过以下方式声明基站：

- LinkDesk（请参见 声明单个设备（LinkDesk））或
- WebUI（请参见 声明单个设备（WebUI））。

i 请注意，新密码必须满足以下要求：

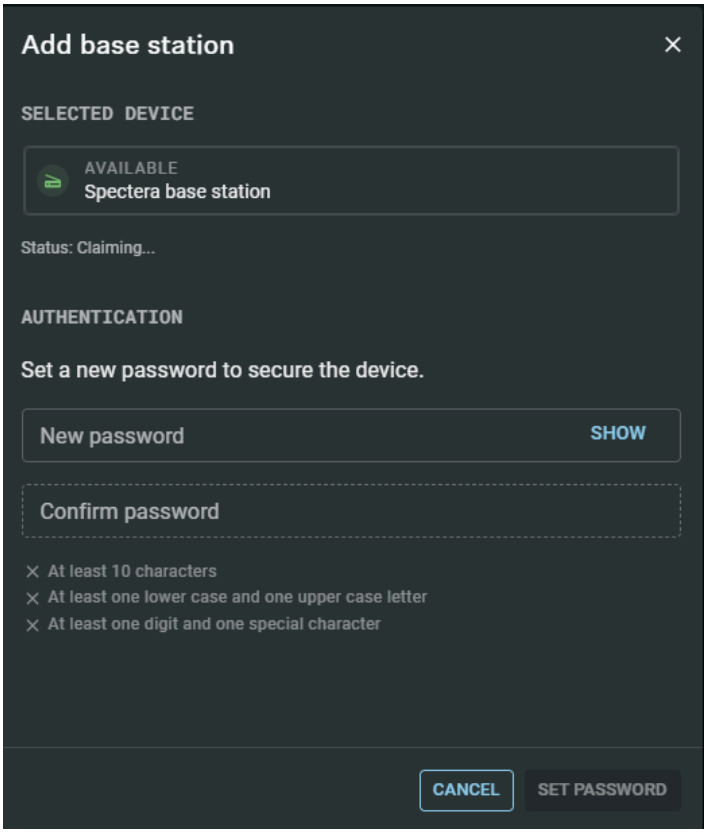
- 至少十个字符
- 至少一个小写字母
- 至少一个大写字母
- 至少一个数字
- 至少一个特殊字符： !#$%&()*+,-./:;<=>?@[]^_{|}~
- 最大长度：64个字符

声明单个设备（LinkDesk）

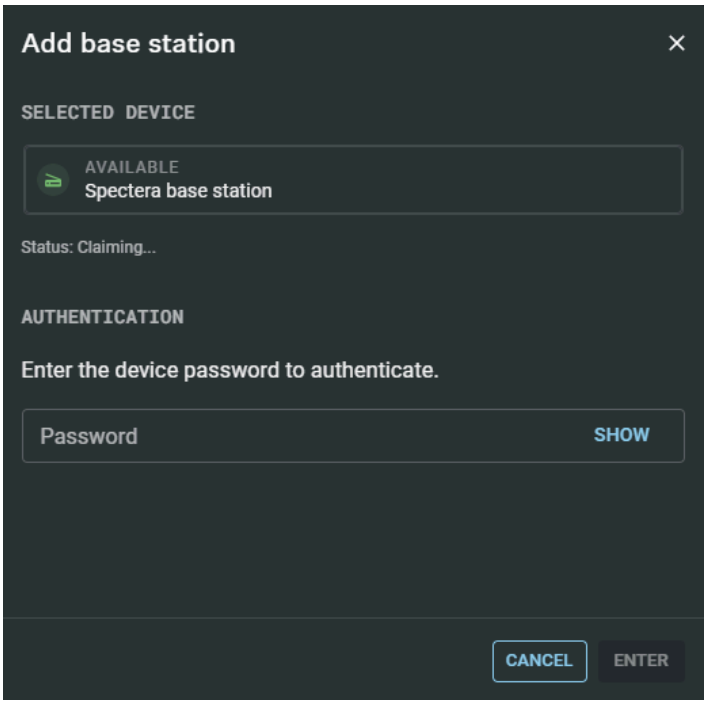
在 Sennheiser LinkDesk 中声明单个设备的说明。

要声明您的 Base Station：

- 在您的 生产卡中，在顶部栏的左侧激活功能 **设备同步**。
- 点击右侧 **Base Stations** 栏中的 符号。
- 输入 Base Station 的正确IP地址并点击 **搜索**。
  - 如果设备处于出厂默认状态并且原始密码仍然分配，则会自动检测并应用。接下来，必须设置新密码：



  - 如果设备之前已被其他 Sennheiser LinkDesk 或 Spectera WebUI 实例声明，则必须输入之前设置的密码：



i 如果您无法记住之前设置的密码，请对设备执行出厂重置。重置后，Spectera 的默认密码将由软件自动应用。

▶ 设置新设备密码（如果您是第一次登录）或输入您已分配的用于身份验证的密码（如果您已登录）。

i 请注意，新密码必须满足以下要求：
- 至少十个字符
- 至少一个小写字母
- 至少一个大写字母
- 至少一个数字
- 至少一个特殊字符： !#$%&()*+,-./:;<=>?@[]^_{|}~
- 最大长度：64个字符

✓ 您的 Base Station 已成功声明。

声明单个设备（WebUI）

在 Spectera WebUI 中声明单个设备的说明。

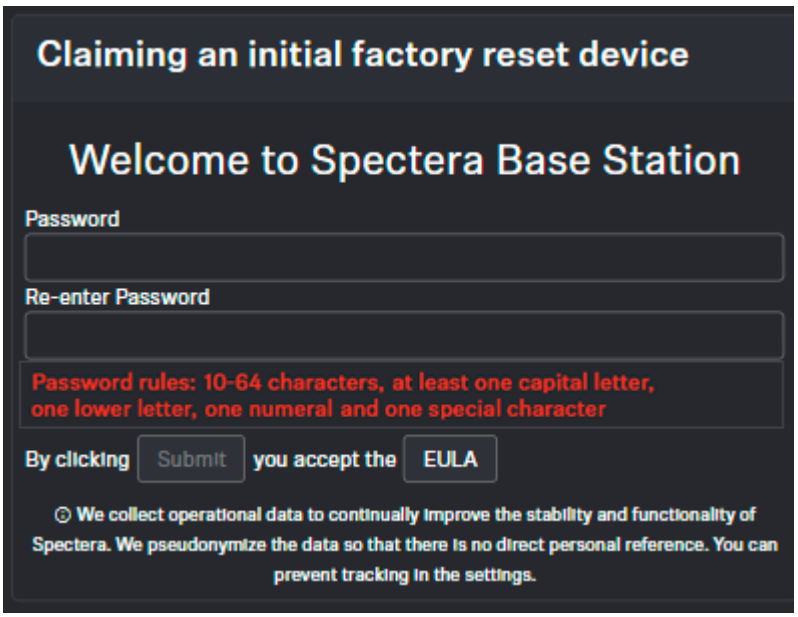
要声明您的基站：

▶ 根据固件版本，将以下 URL 输入到您的浏览器中：
- 固件 0.8.x: `https://deviceIP/specteracontrol/index.html`
- 固件 ≥1.0.0: `https://deviceIP/specterawebui/index.html`

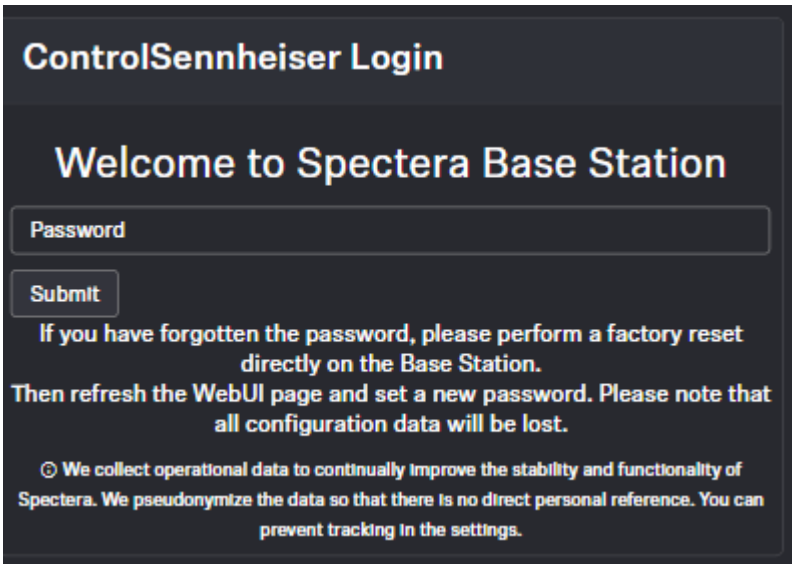
> **i** 由于证书对您的浏览器未知，首次运行应用程序时会显示安全警告。安全警告取决于您使用的浏览器。

▶ 根据您的浏览器，点击 **高级**，然后点击：
- **继续访问 localhost（不安全）**（Microsoft Edge）
- **继续访问 localhost（不安全）**（Google Chrome）
- **接受风险并继续**（Firefox）
- 或类似（其他浏览器）。

✓ WebUI 根据设备的状态显示以下选项：
- 如果设备处于出厂默认状态并且原始密码仍然分配，则会自动检测并应用。接下来，必须设置新密码：



- 如果设备之前已被其他 Sennheiser LinkDesk 或 Spectera WebUI 实例声明，则必须输入之前设置的密码：



i 如果您无法记住之前设置的密码，请对设备执行出厂重置。重置后，Spectera 的默认密码将由软件自动应用。

- 设置新设备密码（如果您是第一次登录）或输入您已分配的用于身份验证的密码（如果您已登录）。
- 点击 **提交**。

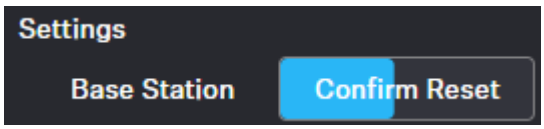
✓ 您的 Base Station 已成功声明。

重置设备密码（Spectera 基站）

设备密码只能通过恢复出厂设置来重置（可以直接在设备上执行或通过 WebUI 远程执行）：

恢复Base Station的出厂设置：

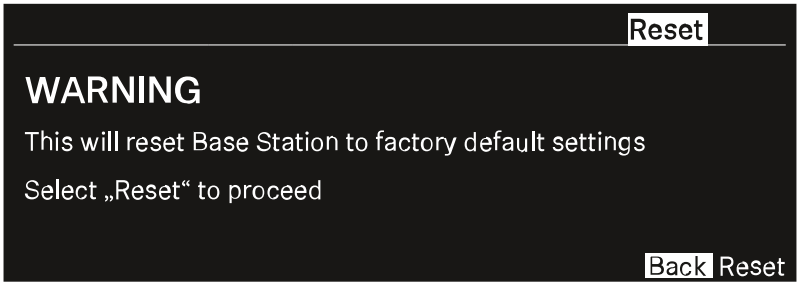
- 在顶部菜单栏中，进入**配置** > **基站**。
- 在**设置**中点击**恢复出厂设置**。
  - 将显示一个倒计时时间线（蓝色背景）。



- 按**确认重置**以确认恢复出厂设置。

恢复Base Station出厂设置：

- 在Base Station上旋转操控旋钮，导航至**Reset**菜单。
- 按下操控旋钮进入菜单。
  - 将出现警告提示。



- 旋转操控旋钮选择**Reset**。
- 再次按下操控旋钮。
  - Base Station将恢复出厂设置并重启。

> 重启后请检查可能发生变化的IP地址。

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