Spectera

Guide de sécurité pour les administrateurs et techniciens

Exportation au format PDF du manuel HTML d’origine

Table des matières

1. Introduction

Ce guide de sécurité fournit des informations essentielles et des meilleures pratiques pour les administrateurs informatiques, les intégrateurs de systèmes et les techniciens d'événements afin d'assurer que des mesures de sécurité robustes soient mises en œuvre efficacement.

Les systèmes audio professionnels, largement déployés dans des environnements tels que la diffusion, les événements en direct et les entreprises, sont de plus en plus intégrés dans des réseaux d'entreprise — les rendant susceptibles à des menaces telles que l'accès non autorisé, l'interception de données et l'interférence de signal. Pour garantir un déploiement sécurisé et l'intégrité du système, Sennheiser applique les normes de sécurité les plus élevées à tous ses produits, soutenues par des mesures de protection robustes et des pratiques de gestion complètes.

- **Principes de sécurité et conception du système :**

  Sennheiser intègre la sécurité dès le développement du produit à travers des évaluations de risques régulières et des configurations sécurisées, suivant une approche de « sécurité par conception ». La conformité aux normes internationales garantit une protection cohérente et une atténuation proactive des menaces.

- **Sécurité de la communication et cryptage :**

  Des protocoles de cryptage conformes aux normes de l'industrie tels que AES-256 et TLS protègent les données audio et de contrôle contre l'interception et l'accès non autorisé. Des méthodes sécurisées telles que HTTPS et les API REST sont utilisées pour les intégrations réseau et tierces.

- **Authentification et contrôle d'accès :**

  L'authentification basée sur les rôles et la revendication de dispositifs valident les utilisateurs et les dispositifs avant d'accorder l'accès. Les mises à jour régulières des identifiants maintiennent l'intégrité du système et préviennent l'accès non autorisé.

- **Configuration du réseau et interfaces :**

  Activez uniquement les ports essentiels, segmentez les réseaux et appliquez des règles de pare-feu pour un fonctionnement sécurisé. Une configuration appropriée des protocoles tels que Dante®, mDNS et Bluetooth® est essentielle pour une infrastructure réseau robuste.

Ce guide fournit des mesures complètes pour protéger les systèmes audio professionnels contre les menaces grâce à une conception sécurisée, un cryptage, une authentification et des meilleures pratiques tout au long du cycle de vie du système.

2. Fonctionnalités de sécurité clés des produits

Les principales fonctionnalités de sécurité des appareils et des outils logiciels Spectera sont détaillées, en mettant l'accent sur les meilleures pratiques pour les administrateurs informatiques afin d'assurer une communication sécurisée et une protection des données.

Les appareils Spectera (Base Station, DAD et appareils mobiles (SEK)) et les outils logiciels tels que **Spectera Base Station WebUI** et **Sennheiser LinkDesk** prennent en charge des mesures de sécurité renforcées, garantissant à la fois une connexion sécurisée entre les appareils via radio et un transfert de données sécurisé sur le réseau. Il offre les fonctionnalités de sécurité suivantes :

- **Chiffrement de lien AES-256 :**

  Le chiffrement de lien AES-256 protège la communication audio et de contrôle entre les appareils.
- **Chiffrement du protocole de contrôle :**

  Le WebUI utilise toujours une communication HTTPS chiffrée. Le protocole SSCv2 sécurise la communication entre les appareils et les outils logiciels via HTTPS.
- **Revendication de dispositif et authentification :**

  La fonctionnalité de revendication de dispositif et d'authentification garantit un accès de contrôle autorisé à l'aide de mots de passe.
- **Chiffrement des médias Dante® :**

  Le chiffrement des médias Dante® est un chiffrement de canal optionnel pour les réseaux Dante.

Chiffrement de lien AES-256

Toute communication sans fil entre les appareils Spectera sera protégée par AES-256, une norme de chiffrement de premier ordre conçue pour protéger les données sensibles.

Le chiffrement de lien comprend les interfaces suivantes :

- La connexion entre la Base Station et les appareils mobiles pour la transmission audio.
- La connexion entre la Base Station et les appareils mobiles pour la synchronisation des paramètres des appareils.

> **i** Le chiffrement de lien AES-256 est toujours activé et ne peut pas être désactivé.

Chiffrement du protocole de contrôle

Toute communication de contrôle sur le réseau vers la Base Station est chiffrée et authentifiée.

Il offre une sécurité de bout en bout, utilisant HTTPS (TLS 1.3). La communication vers le serveur de licence Sennheiser est chiffrée au niveau de l'application.

Le chiffrement du protocole est toujours activé et ne peut pas être désactivé.

Revendication de dispositif et authentification

La revendication de dispositif et l'authentification renforcent la sécurité en exigeant une protection par mot de passe pour l'accès aux dispositifs et en garantissant que seuls les utilisateurs autorisés peuvent modifier les paramètres via des connexions chiffrées.

L'accès au dispositif via l'API de contrôle réseau et le WebUI de la Base Station Spectera et via Sennheiser LinkDesk est protégé par mot de passe, afin d'éviter la configuration du dispositif par des acteurs non autorisés à l'intérieur du réseau.

L'authentification des dispositifs est toujours activée et ne peut pas être désactivée.

Avantages de la revendication de dispositif

- **Fonctionnalité de revendication de dispositif :**

  La revendication de dispositif est une fonctionnalité du Sennheiser LinkDesk et du WebUI de la Base Station Spectera qui permet à l'utilisateur de revendiquer la propriété de ses dispositifs Sennheiser, offrant une couche supplémentaire de sécurité et de contrôle.

- **Attribution de dispositif :**

  Elle permet d'attribuer un dispositif à une ou plusieurs installations distantes, ce qui empêche tout contrôle de dispositif non authentifié au sein du réseau.

- **Configuration initiale :**

  Dans le cadre de la configuration initiale, les utilisateurs revendiquent un dispositif en configurant un mot de passe obligatoire pour le dispositif.

- **Utilisabilité :**

  Au sein d'une installation, plusieurs applications logicielles peuvent être utilisées simultanément avec ce mot de passe de dispositif pour une utilisabilité optimale.

- **Mesures de sécurité :**

  Une fois qu'un dispositif est revendiqué, ses paramètres ne peuvent être consultés et modifiés que via une connexion chiffrée, ce qui nécessite l'entrée du mot de passe de configuration.

Chiffrement des médias Dante® (disponible à partir de la version 1.1.0 du firmware Dante® Brooklyn3)

Le chiffrement des médias Dante® étend les avantages de sécurité de l'utilisation de Dante® sur votre réseau en dissimulant le contenu des médias lors de la transmission entre les dispositifs.

Dante® utilise la norme de chiffrement avancé (AES) avec une clé de 256 bits pour fournir une protection des médias de premier plan dans l'industrie.

Dissimuler le contenu des paquets de médias empêche les utilisateurs malveillants ou non autorisés d'écouter ou d'interférer avec le trafic multimédia Dante.

i Par défaut, le chiffrement des médias Dante est désactivé, car le chiffrement ne peut être configuré qu'en utilisant l'application Dante Director. Veuillez vous référer à la documentation d'Audinate pour des informations détaillées sur le chiffrement Dante®, sur la façon d'activer et de configurer le chiffrement et de mettre à jour le firmware Dante® :

- Chiffrement des médias Dante : Audinate/Chiffrement des médias
- Mise à jour du firmware Dante® : Mise à jour de Dante

3. Comment utiliser les fonctionnalités de sécurité

La section suivante explique comment vous pouvez utiliser les différentes fonctionnalités de sécurité à la fois via l'appareil lui-même et via des applications logicielles prises en charge.

Certificats

a Base Station Spectera utilise un certificat auto-signé pour la communication réseau.

> **i** Actuellement, il n'est pas possible de le remplacer par un certificat signé par une autorité de certification. Le certificat est généré en usine et sera renouvelé à chaque réinitialisation des réglages d'usine.

Lorsque vous accédez pour la première fois à Spectera WebUI à l'aide d'un navigateur, vous recevez un avertissement de sécurité vous informant de l'existence d'un certificat inconnu. L'avertissement de sécurité dépend du navigateur que vous utilisez. En fonction de votre navigateur, cliquez sur **Avancé** ou **Afficher les détails** (Safari), puis sur :

- Microsoft Edge: **Continuer vers l'hôte local (non sécurisé)**
- Google Chrome: **Poursuivre vers l'hôte local (non sécurisé)**
- Firefox: **Accepter le risque et continuer**
- Apple Safari: **[...] consulter ce site Web** > **Consulter ce site Web**
- ou toute autre option similaire (autres navigateurs)

Afin d'éviter les attaques de type « man-in-the-middle » (MITM), le Sennheiser LinkDesk dispose de certaines mesures de sécurité intégrées. En raison de ces mesures, il se peut que vous receviez un avertissement d'incompatibilité de certificat lorsque vous travaillez avec une Base Station. Dans certains cas, ces problèmes peuvent survenir même s'il n'y a pas de problème de sécurité. Il s'agit de :

- Les réglages d'usine de la Base Station ont été réinitialisés depuis la dernière connexion. Dans ce cas, vous pouvez confirmer la connexion en toute sécurité et continuer lorsque vous rencontrez l'avertissement d'incompatibilité.
- Une autre Base Station a été connectée au moyen de la même adresse IP. Dans ce cas, veuillez vérifier si l'adresse IP que vous utilisez est bien l'adresse IP correcte de la Base Station prévue.

Authentification des dispositifs

L'accès aux dispositifs via le réseau est protégé par un mot de passe et le dispositif doit être revendiqué dans le logiciel de contrôle avant utilisation.

Vous pouvez revendiquer la Base Station via :

- LinkDesk (voir Revendiquer un appareil unique (LinkDesk)) ou
- WebUI (voir Réinitialisation du mot de passe de l'appareil (Base Station Spectera)).

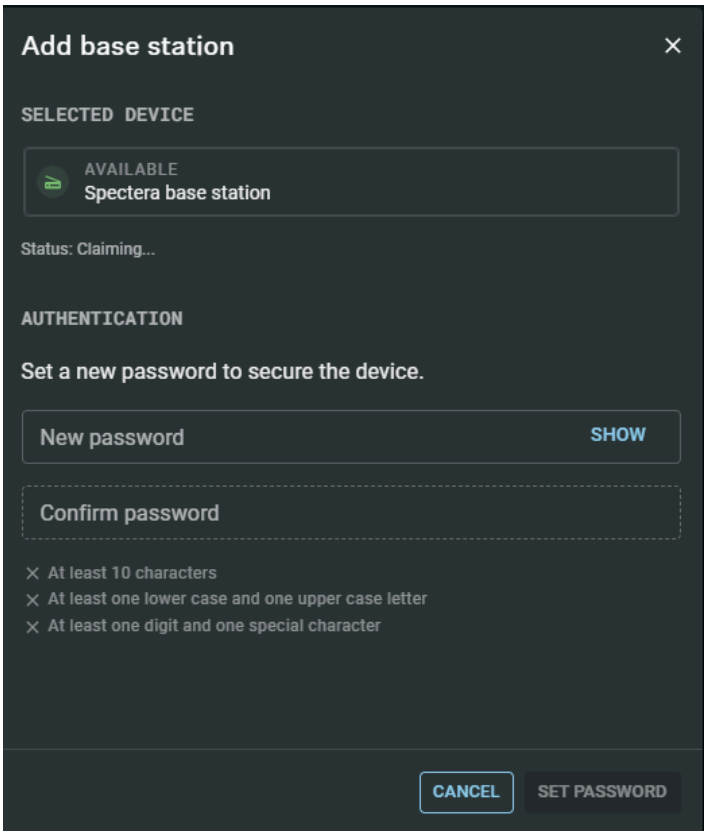
> **i** Veuillez noter que le nouveau mot de passe doit répondre aux exigences suivantes :
>
> - Au moins dix caractères
> - Au moins une lettre minuscule
> - Au moins une lettre majuscule
> - Au moins un chiffre
> - Au moins un caractère spécial : !#$%&()*+,-./:;<=>?@[]^_{|}~
> - Longueur maximale : 64 caractères

Revendiquer un appareil unique (LinkDesk)

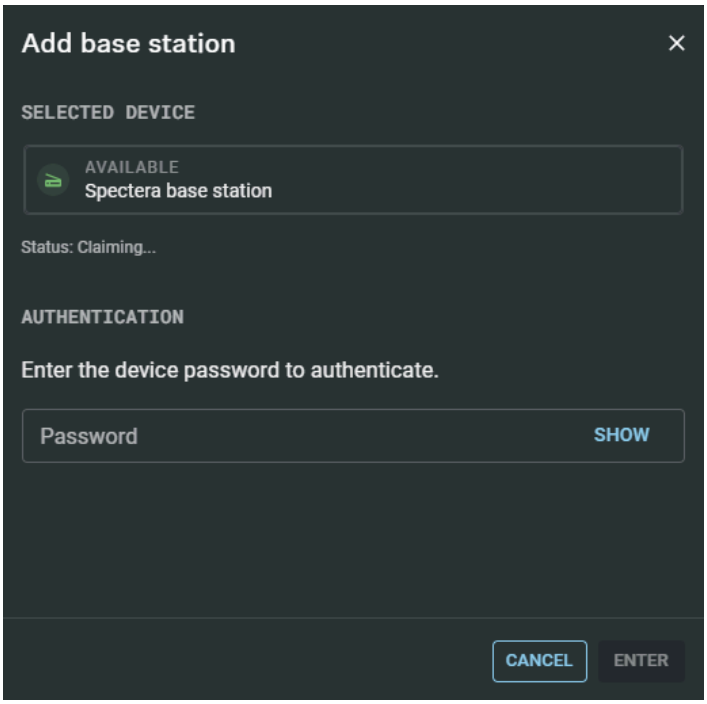
Instructions pour revendiquer un appareil unique dans Sennheiser LinkDesk.

Pour revendiquer votre Base Station :

- Dans votre carte de production, activez la fonction **SYNCHRONISATION DES APPAREILS** sur le côté gauche de la barre supérieure.
- Cliquez sur le symbole + dans la barre **BASE STATIONS** à droite.
- Entrez l'adresse IP correcte de la Base Station et cliquez sur **Rechercher**.
  - Si l'appareil est dans un état par défaut d'usine et que le mot de passe d'origine est toujours attribué, il sera automatiquement détecté et appliqué. Ensuite, un nouveau mot de passe doit être défini :



  - Si l'appareil a été précédemment revendiqué par une autre instance Sennheiser LinkDesk ou Spectera WebUI, le mot de passe précédemment défini doit être saisi :



> **i** Si vous ne vous souvenez pas du mot de passe précédemment défini, veuillez effectuer une réinitialisation d'usine de l'appareil. Après la réinitialisation, le mot de passe par défaut pour Spectera sera automatiquement appliqué par le logiciel.

- Définissez un nouveau mot de passe pour l'appareil (si vous vous connectez pour la première fois) ou entrez le mot de passe que vous avez déjà attribué pour l'authentification (si vous vous êtes déjà connecté).

> **i** Veuillez noter que le nouveau mot de passe doit répondre aux exigences suivantes :
>
> - Au moins dix caractères
> - Au moins une lettre minuscule
> - Au moins une lettre majuscule
> - Au moins un chiffre
> - Au moins un caractère spécial : !#$%&()*+,-./:;<=>?@[]^_{|}~
> - Longueur maximale : 64 caractères

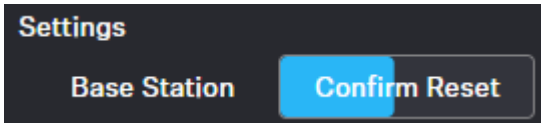
✓ Votre Base Station a été revendiquée avec succès.

Réinitialisation du mot de passe de l'appareil (Base Station Spectera)

Le mot de passe de l'appareil ne peut être réinitialisé que par une réinitialisation d'usine (effectuée directement sur l'appareil ou à distance via WebUI) :

Pour réinitialiser la Base Station :

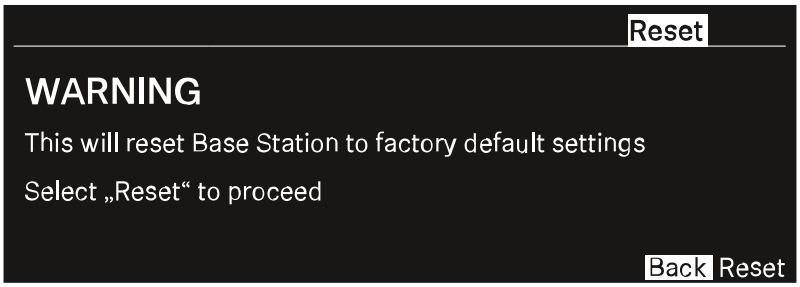
- Dans la barre de navigation supérieure, accédez à **Configuration** > **Base Station**.
- Cliquez sur **Settings** (Paramètres) puis sur **Factory Reset** (Réinitialisation d'usine).
  - Une chronologie défilante s'affiche (en surbrillance bleue).



- Appuyez sur **Confirm Reset** pour confirmer la réinitialisation aux paramètres d'usine.

Pour réinitialiser les réglages d'usine de la Base Station :

- Sur la Base Station, tourner la molette et naviguer jusqu'au menu **Reset**.
- Appuyez sur la molette pour entrer dans le menu.
  - Un avertissement va apparaître.



- Tourner la molette sur **Reset**.
- Appuyez à nouveau sur la molette.
  - Les réglages d'usine de la Base Station seront restaurés, puis la Base Station redémarrera.

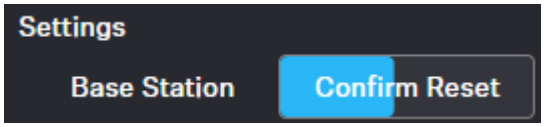
> **i** Après le redémarrage, vérifiez l'adresse IP, cette dernière ayant pu changer.

Réinitialisation du mot de passe de l'appareil (Base Station Spectera)

Le mot de passe de l'appareil ne peut être réinitialisé que par une réinitialisation d'usine (effectuée directement sur l'appareil ou à distance via WebUI) :

Pour réinitialiser la Base Station :

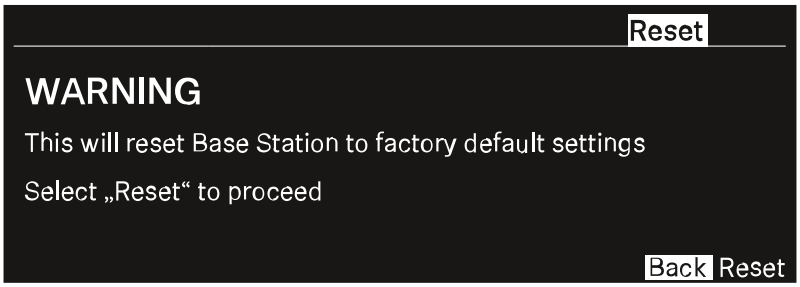
- Dans la barre de navigation supérieure, accédez à **Configuration** > **Base Station**.
- Cliquez sur **Settings** (Paramètres) puis sur **Factory Reset** (Réinitialisation d'usine).
  - Une chronologie défilante s'affiche (en surbrillance bleue).



- Appuyez sur **Confirm Reset** pour confirmer la réinitialisation aux paramètres d'usine.

Pour réinitialiser les réglages d'usine de la Base Station :

- Sur la Base Station, tourner la molette et naviguer jusqu'au menu **Reset**.
- Appuyez sur la molette pour entrer dans le menu.
  - Un avertissement va apparaître.



- Tourner la molette sur **Reset**.
- Appuyez à nouveau sur la molette.
  - Les réglages d'usine de la Base Station seront restaurés, puis la Base Station redémarrera.

> **i** Après le redémarrage, vérifiez l'adresse IP, cette dernière ayant pu changer.

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