Fonction de clé prépartagée personnelle dans le point d'accès CBW

Objectif

Cet article explique la fonction de clé prépartagée personnelle (PSK) du microprogramme Cisco Business Wireless (CBW) Access Point (AP) version 10.6.1.0.

Périphériques pertinents | Version du logiciel

- Point d'accès Cisco Business Wireless 140AC | 10.6.1.0 (Télécharger la dernière version)
- Point d'accès Cisco Business Wireless 145AC | 10.6.1.0 (Télécharger la dernière version)
- Point d'accès Cisco Business Wireless 240AC | 10.6.1.0 (Télécharger la dernière version)

Introduction

Si votre réseau est équipé de matériel CBW, vous pouvez désormais utiliser la fonction PSK personnelle dans la version 10.6.1.0 du micrologiciel !

Personal PSK, également appelé Personal PSK (iPSK), est une fonction qui permet à un administrateur d'émettre des clés pré-partagées uniques à des périphériques individuels pour le même réseau local sans fil (WLAN) Wi-Fi Protected Access II (WPA2) personnel. L'unique clé d'alimentation est liée à l'adresse MAC du périphérique. Ceci n'est pas pris en charge dans les WLAN où la stratégie WPA3 est activée.

Cette fonctionnalité authentifie le client à l'aide d'un serveur RADIUS. Il est généralement destiné aux appareils IoT, aux ordinateurs portables et aux appareils mobiles de l'entreprise.

Table des matières

Conditions préalables

- Vérifiez que vous avez mis à niveau le micrologiciel du point d'accès CBW vers 10.6.1.0. Cliquez sur si vous souhaitez obtenir des instructions détaillées sur la mise à jour du micrologiciel.

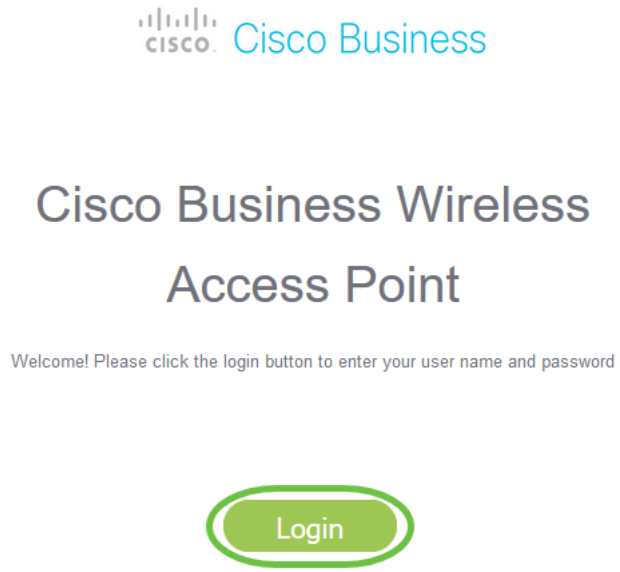
- Vous aurez besoin d'un serveur RADIUS où la clé PSK personnelle et l'adresse MAC du périphérique doivent être configurées.
- Cette fonctionnalité CBW est prise en charge avec trois serveurs RADIUS différents : FreeRADIUS, NPS de Microsoft et ISE de Cisco. La configuration varie en fonction du serveur RADIUS utilisé.

Configuration des paramètres RADIUS CBW

Pour configurer les paramètres RADIUS sur le point d'accès CBW, procédez comme suit.

Étape 1

Connectez-vous à l'interface utilisateur Web du point d'accès CBW.

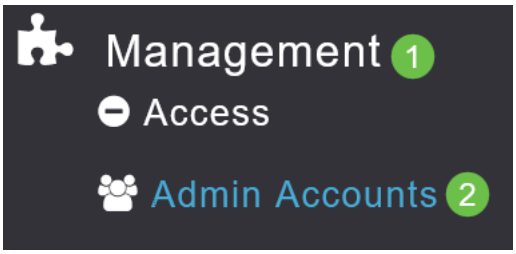


Étape 2

Cliquez sur le symbole **fléché bidirectionnel** pour passer en mode expert.

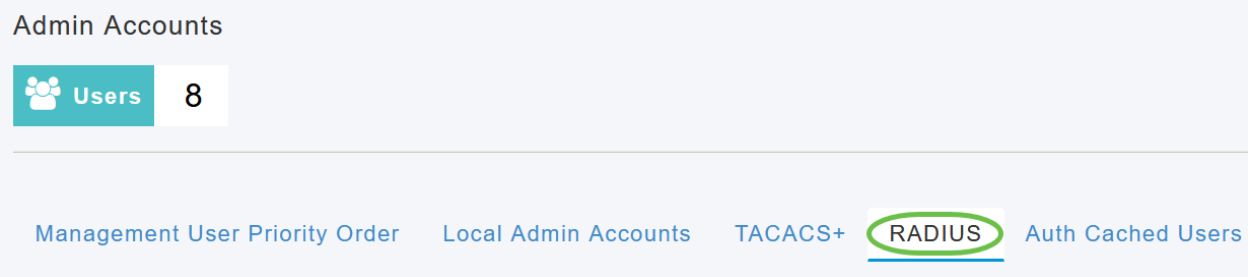
Étape 3

Accédez à **Management > Admin Accounts.**



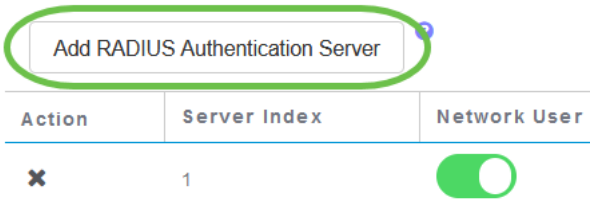
Étape 4

Sélectionnez l'onglet **RADIUS**.



Étape 5

Cliquez sur **Add RADIUS Authentication Server**.

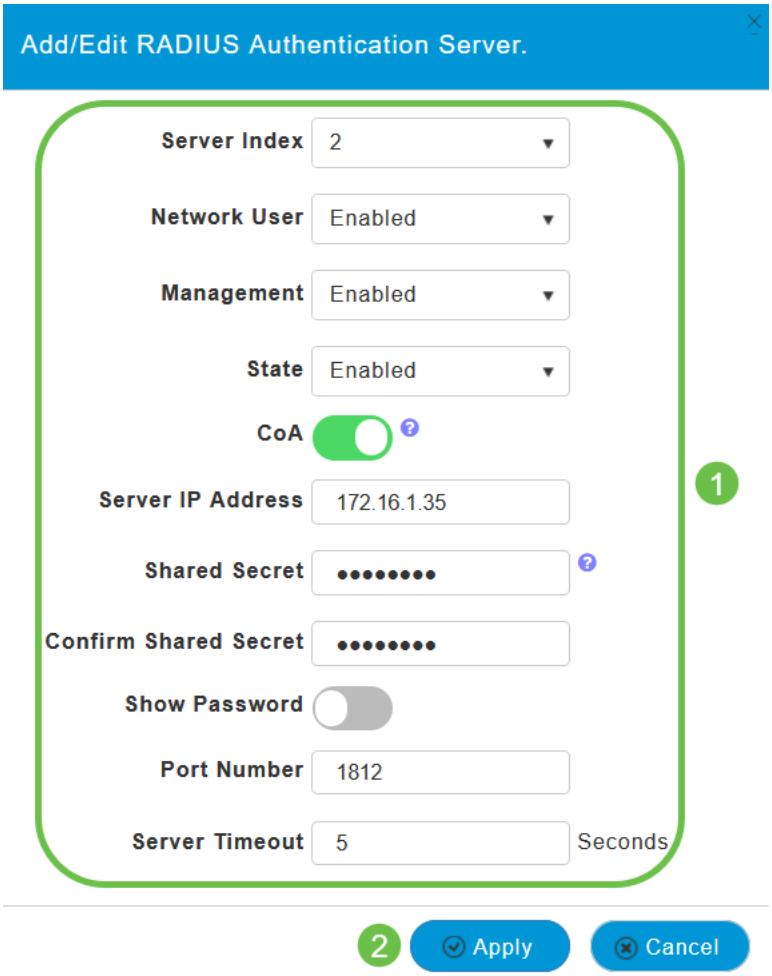


Étape 6

Configurez les éléments suivants :

- *Index de serveur* - Sélectionner 1 à 6
- *Network User* - Activez l'état. Par défaut, cette option est activée
- *Gestion* - Activez l'état. Par défaut, cette option est activée
- *State* - Activez l'état. Par défaut, cette option est activée
- *CoA* - Assurez-vous que la charge d'autorité (CoA) est activée.
- *Adresse IP du serveur* : saisissez l'adresse IPv4 du serveur RADIUS.
- *Shared Secret* - Entrez la clé secrète partagée.
- *Port Number* - Entrez le numéro de port utilisé pour communiquer avec le serveur RADIUS.
- *Délai d'attente du serveur* - Entrez le délai d'attente du serveur.

Cliquez sur Apply.



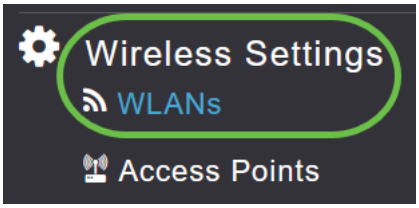
Configuration des paramètres WLAN

Créez un WLAN en tant que WLAN sécurisé WPA2 personnel standard.

La clé pré-partagée ne sera pas utilisée pour les périphériques PSK personnels. Ceci ne serait utilisé que pour les périphériques qui ne sont PAS authentifiés sur le serveur RADIUS. Vous devez ajouter les adresses MAC de N'IMPORTE QUEL périphérique qui se connectera à ce WLAN à la liste d'autorisation de ce périphérique.

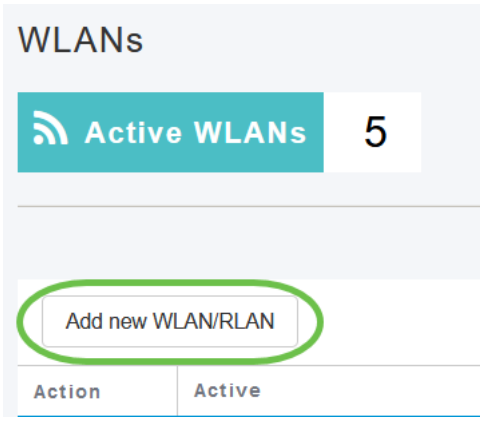
Étape 1

Accédez à **Wireless Settings > WLAN**.



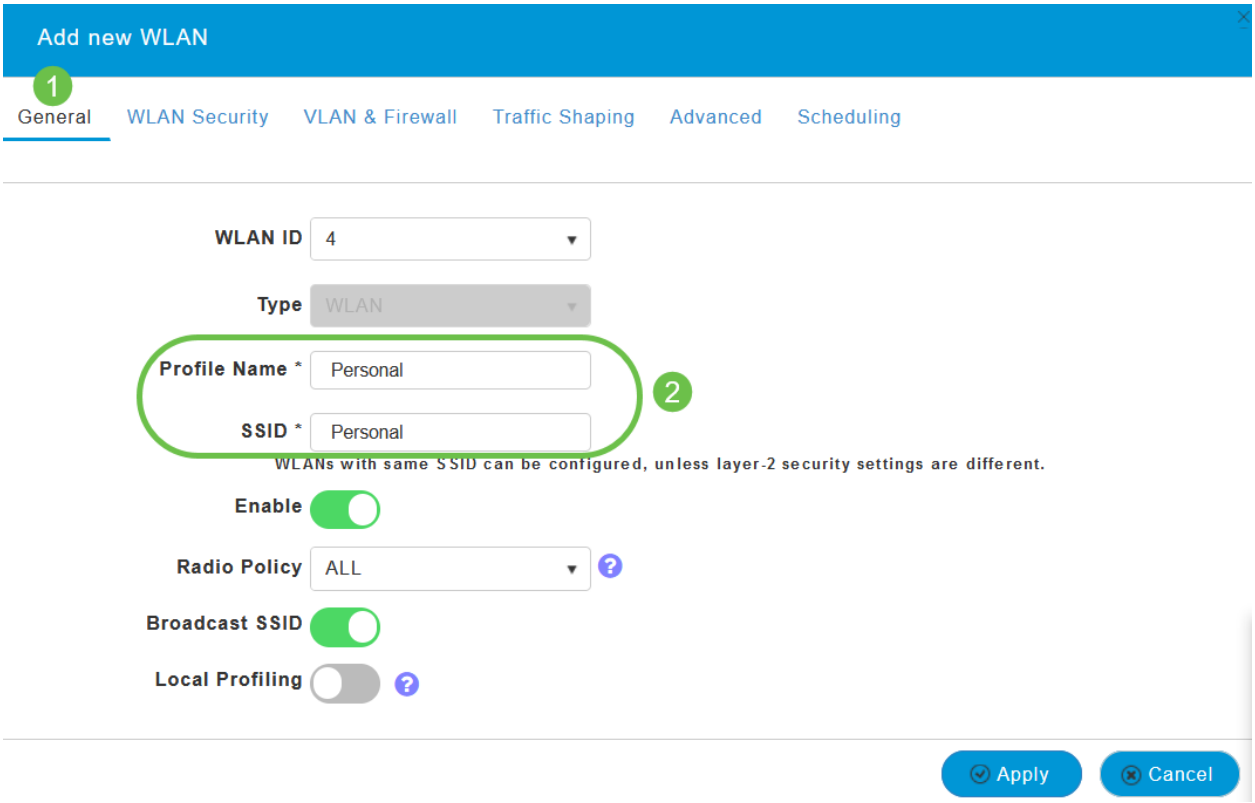
Étape 2

Cliquez sur **Ajouter un nouveau WLAN/RLAN**.



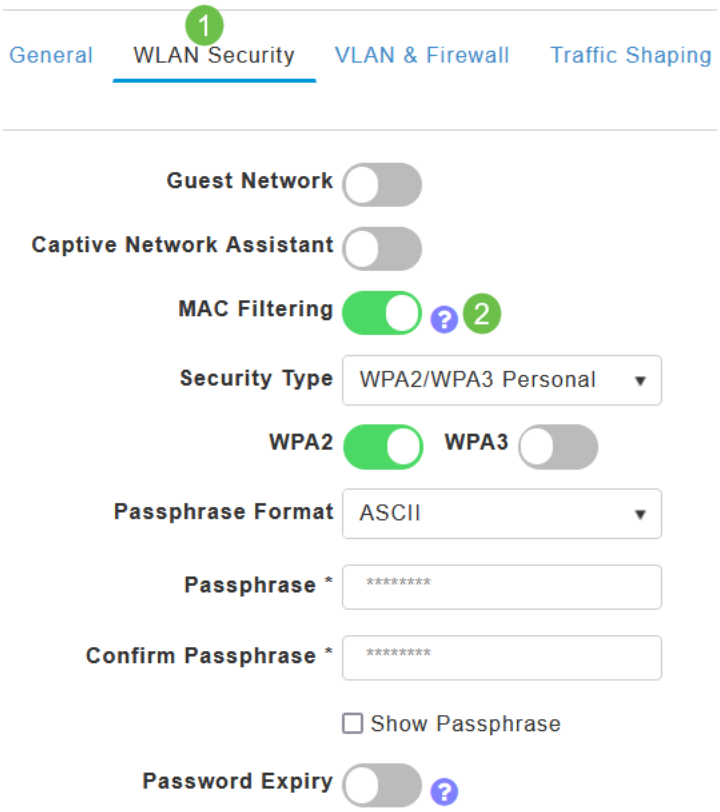
Étape 3

Sous l'onglet *Général*, saisissez un *nom de profil* pour le WLAN.



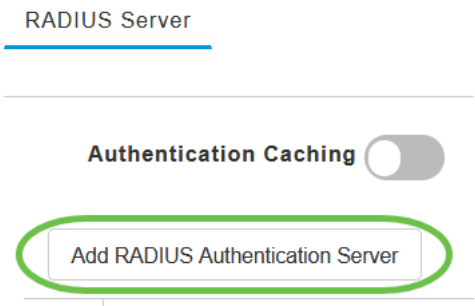
Étape 4

Accédez à l'onglet **Sécurité WLAN** et activez le **filtrage MAC** en faisant glisser la bascule.



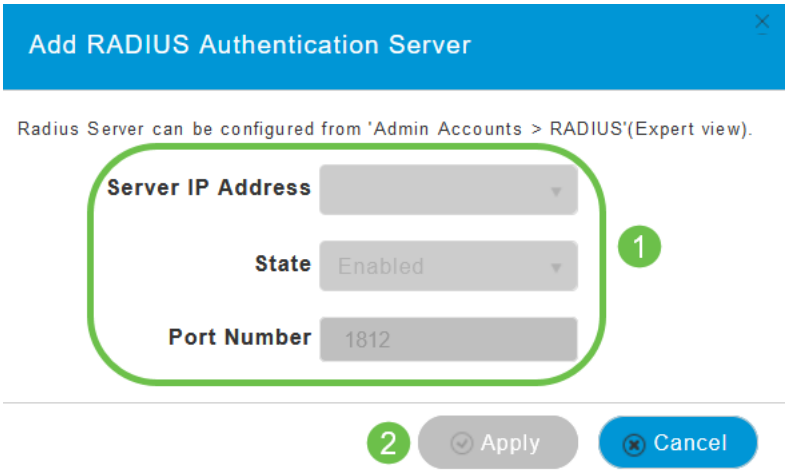
Étape 5

Cliquez sur **Add RADIUS Authentication Server** pour ajouter le serveur RADIUS configuré dans la section précédente pour fournir l'authentification pour ce WLAN.



Étape 6

Une fenêtre contextuelle s'affiche. Entrez l'*adresse IP, l'état et le numéro de port du serveur*. Cliquez sur Apply.

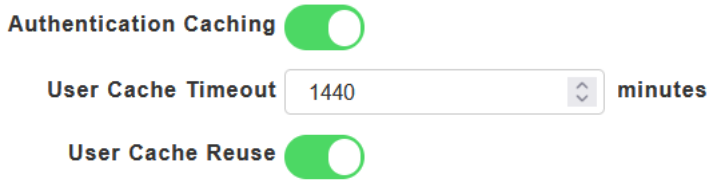


Étape 7

(Facultatif)

Activez *la mise en cache d'authentification*. Lorsque vous activez cette option, les champs suivants s'affichent.

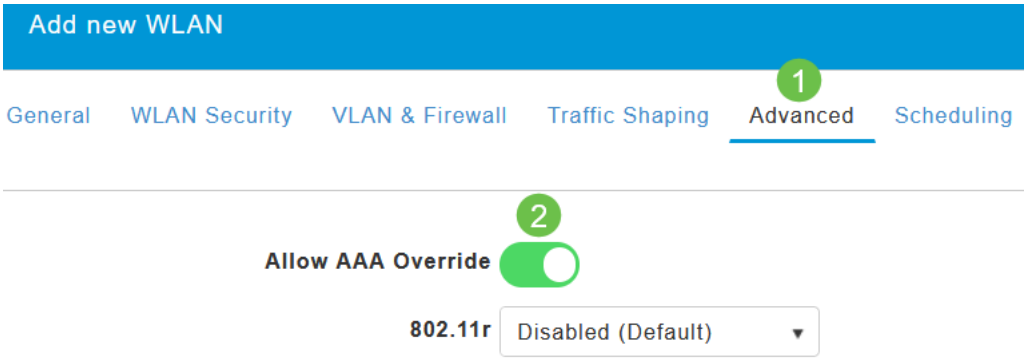
- *Expiration du cache utilisateur* - Spécifie la période à laquelle les informations d'identification authentifiées dans le cache expirent.
- *Réutilisation du cache utilisateur* - Utilisez les informations du cache des informations d'identification avant le délai d'expiration du cache. Par défaut, ceci est désactivé.



Si cette fonctionnalité est activée, un client qui a déjà été authentifié sur ce serveur ne sera pas tenu de transmettre des données au serveur RADIUS lorsqu'il se reconnectera à ce WLAN dans les 24 heures qui suivent.

Étape 8

Accédez à l'onglet Avancé. Activez **Allow AAA Override** en faisant glisser la bascule.

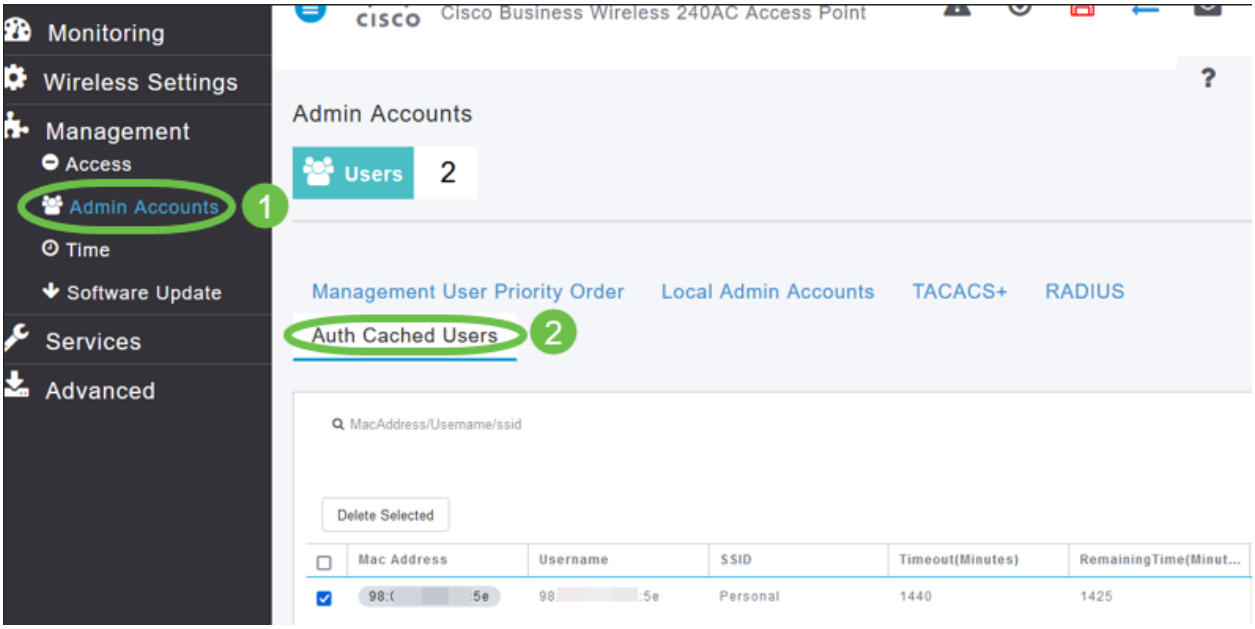


L'onglet *Avancé* ne s'affiche que si vous êtes en *mode Expert*.

Étapes suivantes

Une fois que vous avez configuré les paramètres sur votre point d'accès CBW et configuré votre serveur RADIUS, vous devriez pouvoir connecter votre périphérique. Saisissez la clé PSK personnalisée configurée pour cette adresse MAC et elle se connectera au réseau.

Si vous avez configuré la mise en cache de l'authentification, vous pourrez voir les périphériques qui ont rejoint le WLAN en accédant à l'onglet *Auth Cached Users* sous *Comptes d'administration*. Si nécessaire, il peut être supprimé.



Conclusion

Voilà ! Vous pouvez désormais profiter des avantages de la fonction PSK personnelle sur votre point d'accès CBW.