Configurer RADIUS dans le point d'accès sans fil professionnel Cisco

Objectif

L'objectif de ce document est de vous montrer comment configurer RADIUS dans le point d'accès Cisco Business Wireless (CBW).

Périphériques pertinents | Version du micrologiciel

- 140AC (fiche technique) | 10.4.1.0 (Télécharger la dernière version)
- 145AC (fiche technique) | 10.4.1.0 (Télécharger la dernière version)
- 240AC (fiche technique) | 10.4.1.0 (Télécharger la dernière version)

Introduction

Si vous souhaitez configurer RADIUS dans votre point d'accès CBW, vous êtes au bon endroit ! Les points d'accès CBW prennent en charge la dernière norme 802.11ac de phase 2 pour des réseaux plus performants, plus accessibles et plus denses. Ils offrent des performances de pointe avec des connexions sans fil hautement sécurisées et fiables, pour une expérience utilisateur mobile et robuste.

RADIUS (Remote Authentication Dial-In User Service) est un mécanisme d'authentification permettant aux périphériques de se connecter et d'utiliser un service réseau. Il est utilisé à des fins d'authentification, d'autorisation et de comptabilité centralisées. Un serveur RADIUS régule l'accès au réseau en vérifiant l'identité des utilisateurs à l'aide des identifiants de connexion saisis. Par exemple, un réseau Wi-Fi public est installé sur un campus universitaire. Seuls les étudiants disposant du mot de passe peuvent accéder à ces réseaux. Le serveur RADIUS vérifie les mots de passe entrés par les utilisateurs et accorde ou refuse l'accès au réseau local sans fil (WLAN), le cas échéant.

Si vous êtes prêt à configurer RADIUS sur votre point d'accès CBW, commençons !

Table des matières

Configurer RADIUS sur votre point d'accès CBW

Cette section vous propose des conseils pour les débutants.

Connexion

Connectez-vous à l'interface utilisateur Web du point d'accès principal. Pour ce faire, ouvrez un navigateur Web et saisissez https://ciscobusiness.cisco. Vous pouvez recevoir un avertissement avant de continuer. Entrez vos informations d'identification.Vous pouvez également accéder au point d'accès principal en entrant https://[adresse IP] (du point d'accès principal) dans un

navigateur Web.

Conseils

Si vous avez des questions sur un champ de l'interface utilisateur, recherchez une info-bulle qui ressemble à ceci : 

Trouver l'icône Développer le menu principal pose problème ?

Accédez au menu situé à gauche de l'écran. Si le bouton de menu ne s'affiche pas, cliquez sur cette icône pour ouvrir le menu de la barre latérale. 

Application Cisco Business

Ces périphériques disposent d'applications complémentaires qui partagent certaines fonctions de gestion avec l'interface utilisateur Web. Toutes les fonctionnalités de l'interface utilisateur Web ne seront pas disponibles dans l'application.

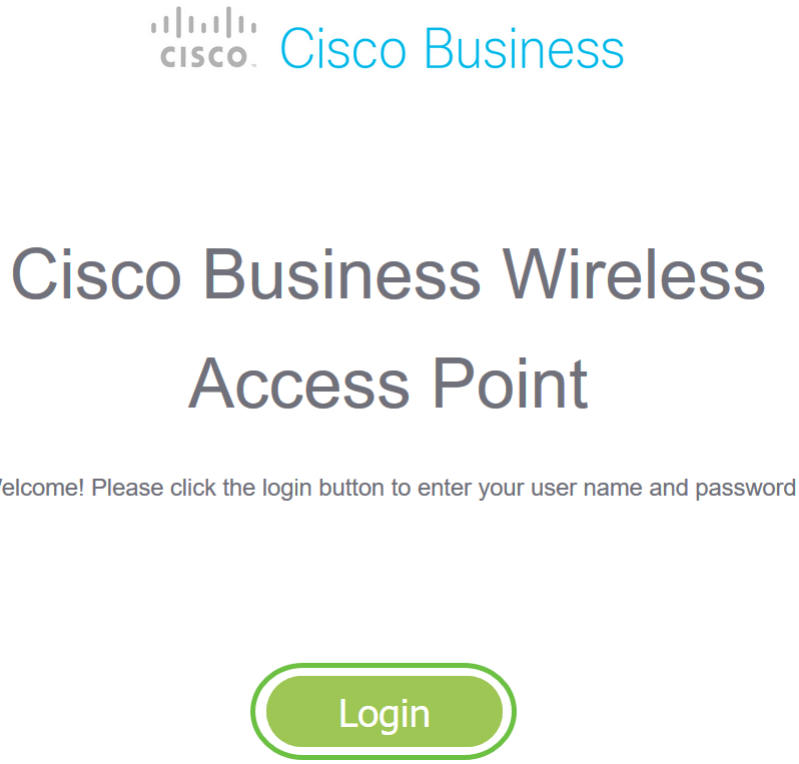
Télécharger l'application iOS Télécharger l'application Android

Forum aux questions

Si vous avez encore des questions sans réponse, vous pouvez consulter notre foire aux questions . Forum aux questions

Étape 1

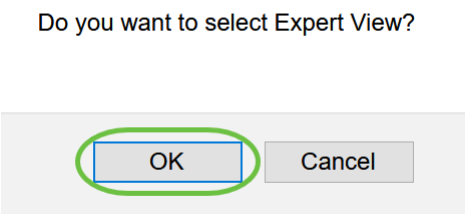
Connectez-vous à votre point d'accès CBW à l'aide d'un nom d'utilisateur et d'un mot de passe valides.



Étape 2

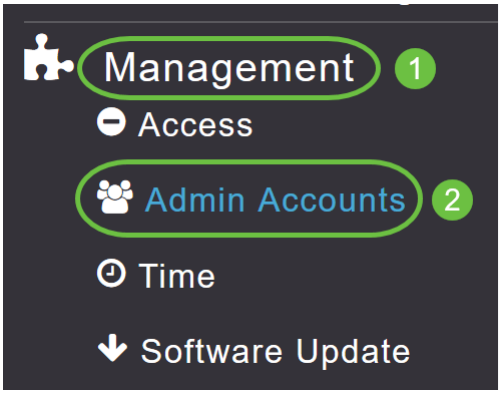
Cliquez sur le symbole de **flèche bidirectionnelle** en haut de l'interface utilisateur Web pour *basculer en mode Expert*.

L'écran contextuel suivant s'affiche. Cliquez sur **OK** pour continuer.



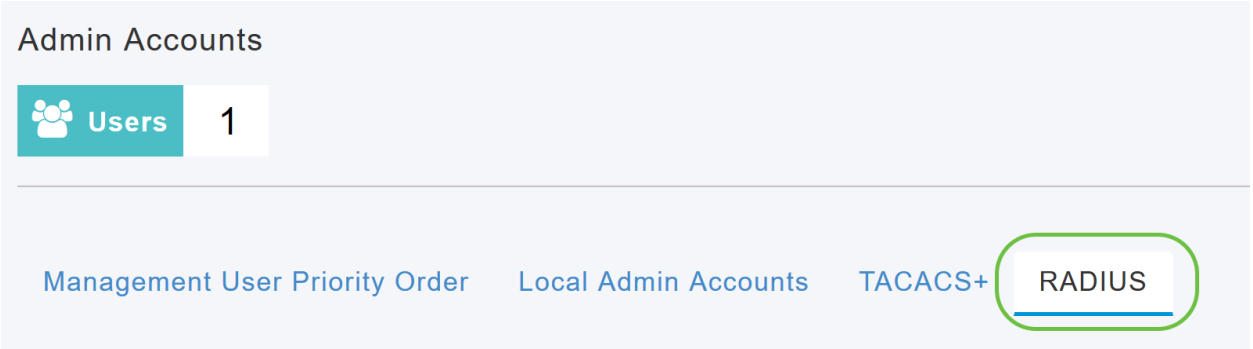
Étape 3

Accédez à **Management > Admin Accounts**.



Étape 4

Pour ajouter les serveurs RADIUS, cliquez sur l'onglet **RADIUS**.

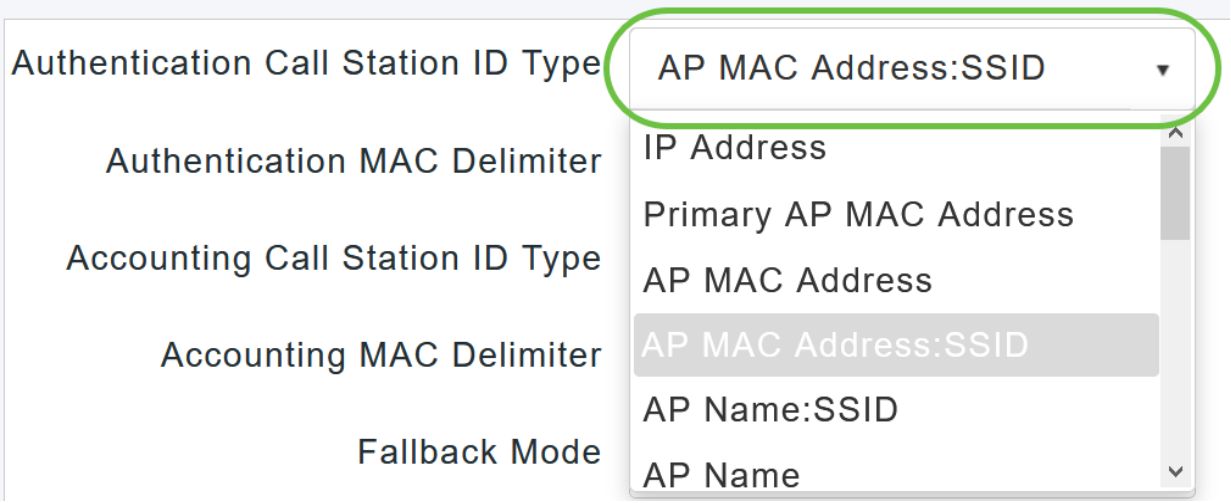


Étape 5

Dans la liste déroulante *Authentication Call Station ID Type*, sélectionnez l'option qui est envoyée

au serveur RADIUS dans le message Access-Request. Les options suivantes sont disponibles :

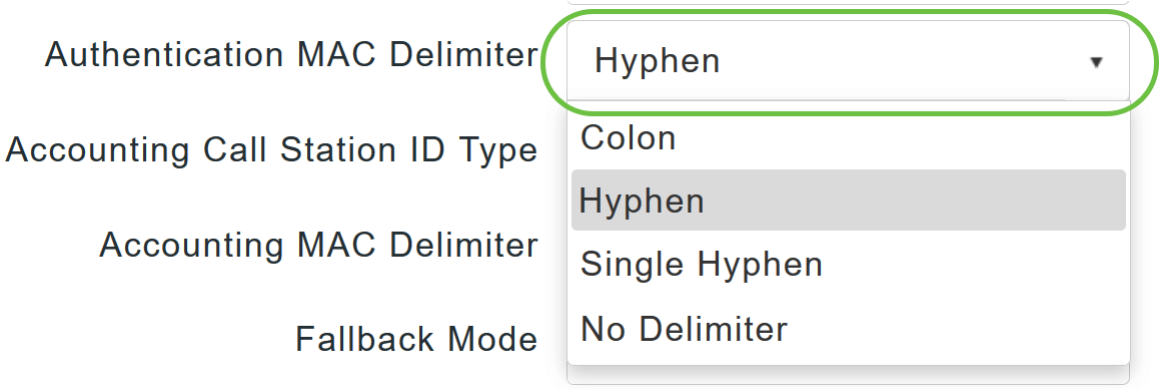
- *Adresse IP*
- *Adresse MAC du point d'accès principal*
- *Adresse MAC de l'AP*
- *Adresse MAC de l'AP:SSID*
- *Nom du point d'accès:SSID*
- *Nom du point d'accès*
- *Groupe AP*
- *Groupe flexible*
- *Emplacement du point d'accès*
- *ID de VLAN*
- *Adresse MAC Ethernet du point d'accès*
- *Adresse MAC Ethernet du point d'accès:SSID*
- *Adresse de l'étiquette AP*
- *Adresse de l'étiquette du point d'accès:SSID*
- *AP MAC:SSID AP Group*
- *AP Eth MAC:SSID AP Group*



Étape 6

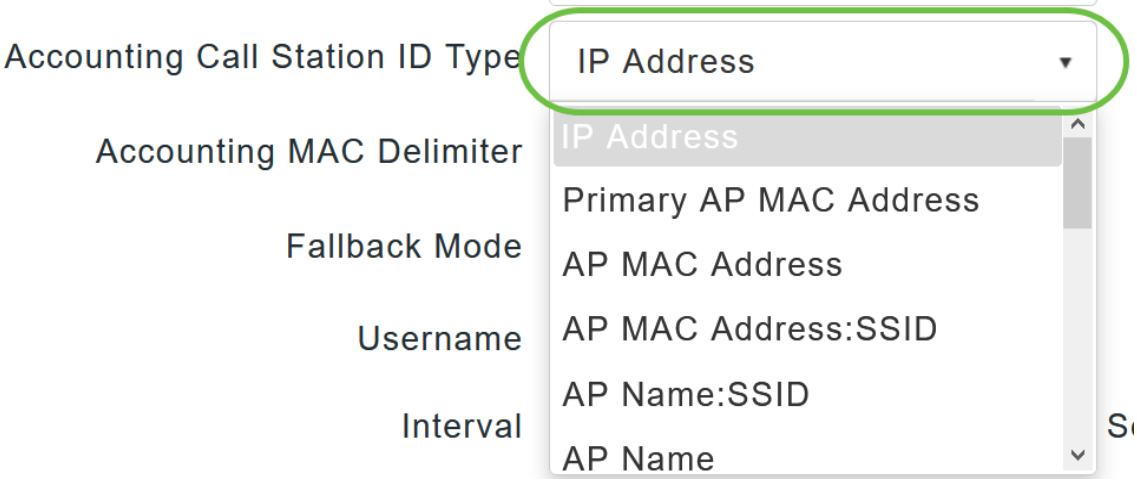
Sélectionnez *Authentication MAC Delimiter* dans la liste déroulante. Les options sont les suivantes :

- *Colon*
- *Hyphène*
- *Tiret unique*
- *Aucun délimiteur*



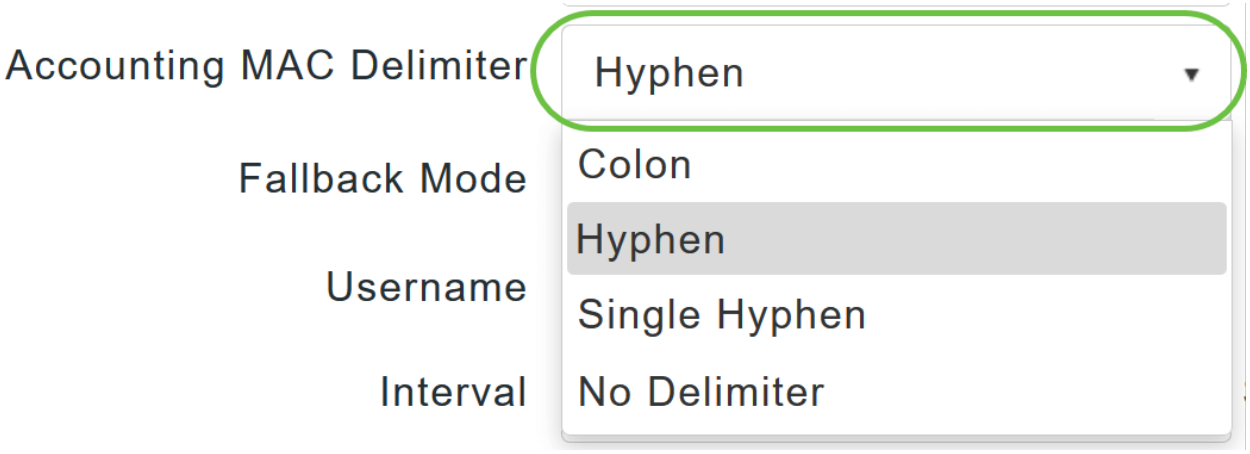
Étape 7

Sélectionnez le *type d'ID de poste d'appel comptable* dans la liste déroulante.



Étape 8

Choisissez le *délimiteur MAC comptable* dans la liste déroulante.



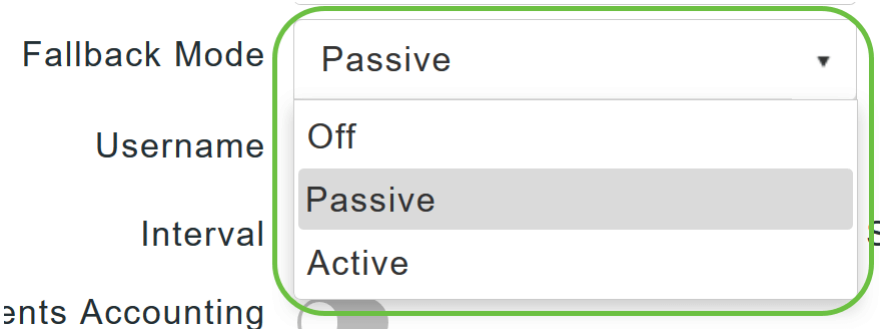
Étape 9

Spécifiez le *mode de secours* du serveur RADIUS dans la liste déroulante. Il peut s'agir de l'un des éléments suivants :

- *Éteint* - Désactive la restauration du serveur RADIUS. C'est la valeur par défaut.
- *Passif* : force le point d'accès principal à revenir à un serveur avec une priorité inférieure à

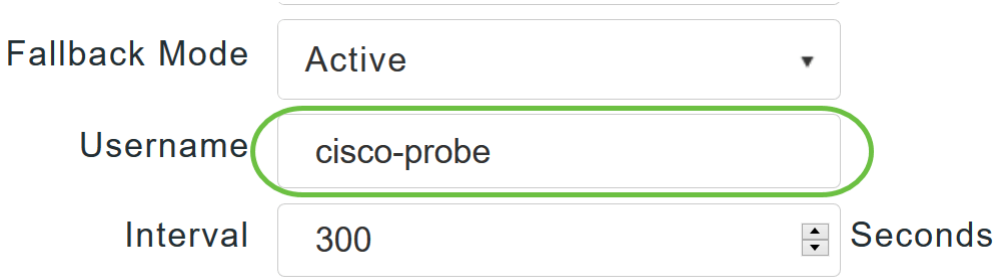
partir des serveurs de sauvegarde disponibles sans utiliser de messages d'analyse superflus. Le point d'accès principal ignore tous les serveurs inactifs pendant une période de temps et recommence plus tard lorsqu'un message RADIUS doit être envoyé.

- *Actif* : force le point d'accès principal à revenir à un serveur avec une priorité inférieure des serveurs de sauvegarde disponibles en utilisant des messages d'analyse RADIUS pour déterminer de manière proactive si un serveur marqué comme inactif est de nouveau en ligne. Le point d'accès principal ignore tous les serveurs inactifs pour toutes les requêtes RADIUS actives. Une fois que le serveur principal reçoit une réponse du serveur ACS récupéré, le serveur RADIUS de secours actif n'envoie plus de messages de sonde au serveur demandant l'authentification de sonde active.



Étape 10

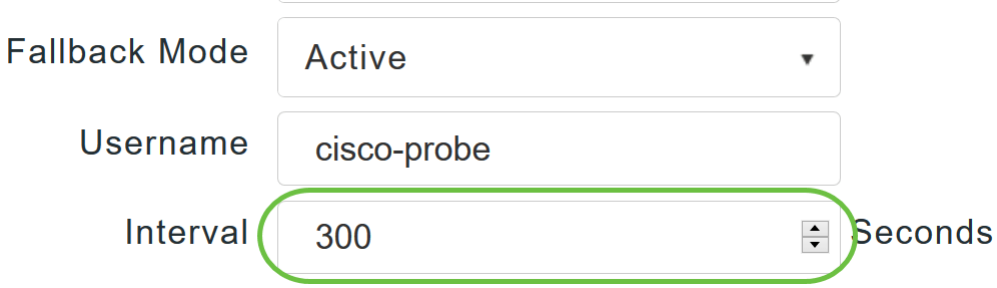
Si vous avez activé le *mode de secours actif*, entrez le nom à envoyer dans les sondes du serveur inactif dans le champ *Nom d'utilisateur*.



Vous pouvez saisir jusqu'à 16 caractères alphanumériques. La valeur par défaut est **cisco-probe**.

Étape 11

Si vous avez activé le *mode de secours actif*, saisissez la valeur de l'intervalle d'analyse (en secondes) dans le champ Intervalle. L'intervalle sert de temps inactif en mode passif et d'intervalle de sonde en mode actif.

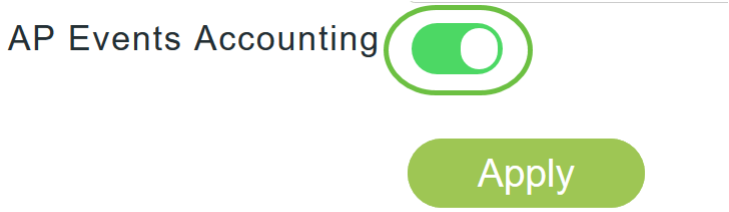


La plage valide est comprise entre 180 et 3 600 secondes et la valeur par défaut est **300** secondes.

Étape 12

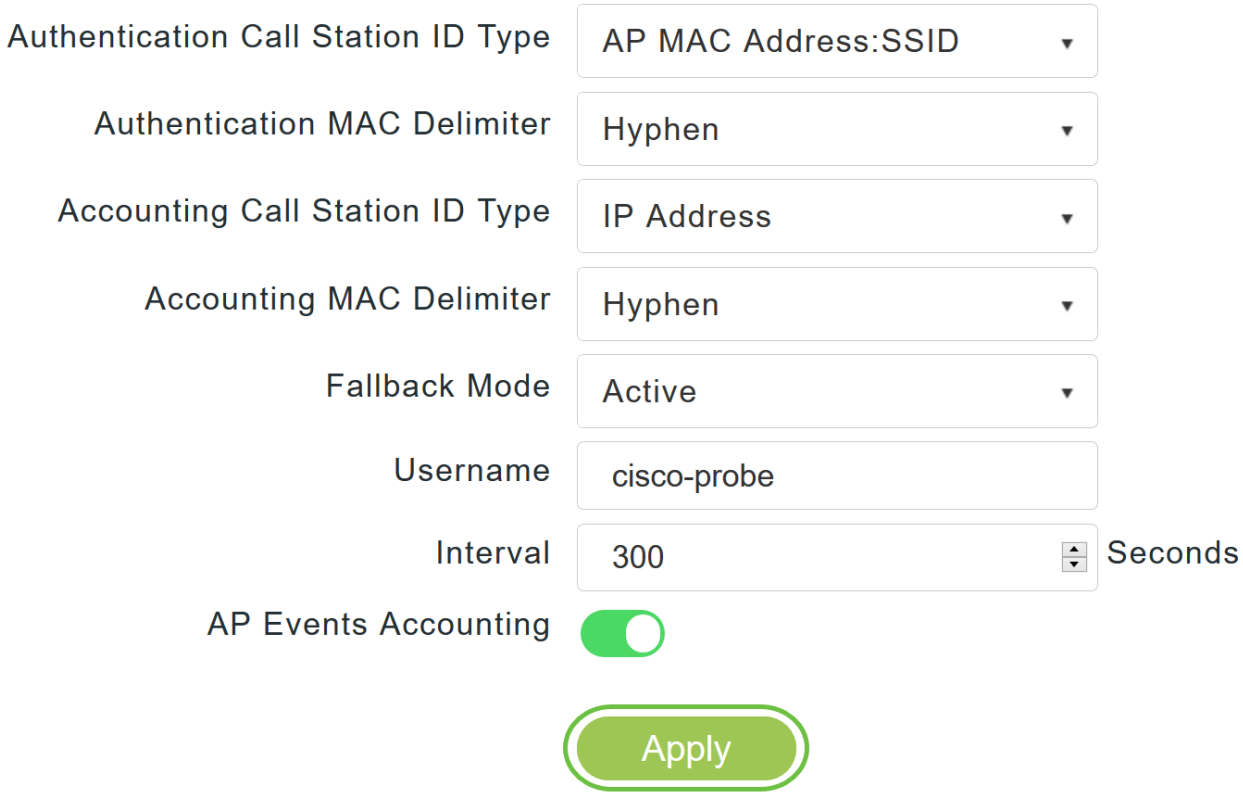
Activez le bouton de curseur *AP Events Accounting* pour activer l'envoi de demandes de comptabilité au serveur RADIUS.

Pendant les problèmes de réseau, les points d'accès se joignent/se déconnectent du point d'accès principal. L'activation de cette option garantit que ces événements sont surveillés et que les demandes de comptabilité sont envoyées au serveur RADIUS pour vous aider à détecter les problèmes de réseau.



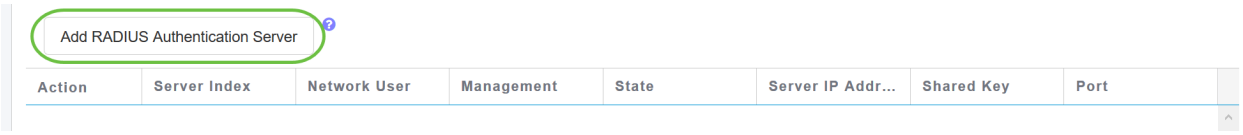
Étape 13

Cliquez sur Apply.



Étape 14

Pour configurer le serveur d'authentification RADIUS, cliquez sur **Add RADIUS Authentication Server**.

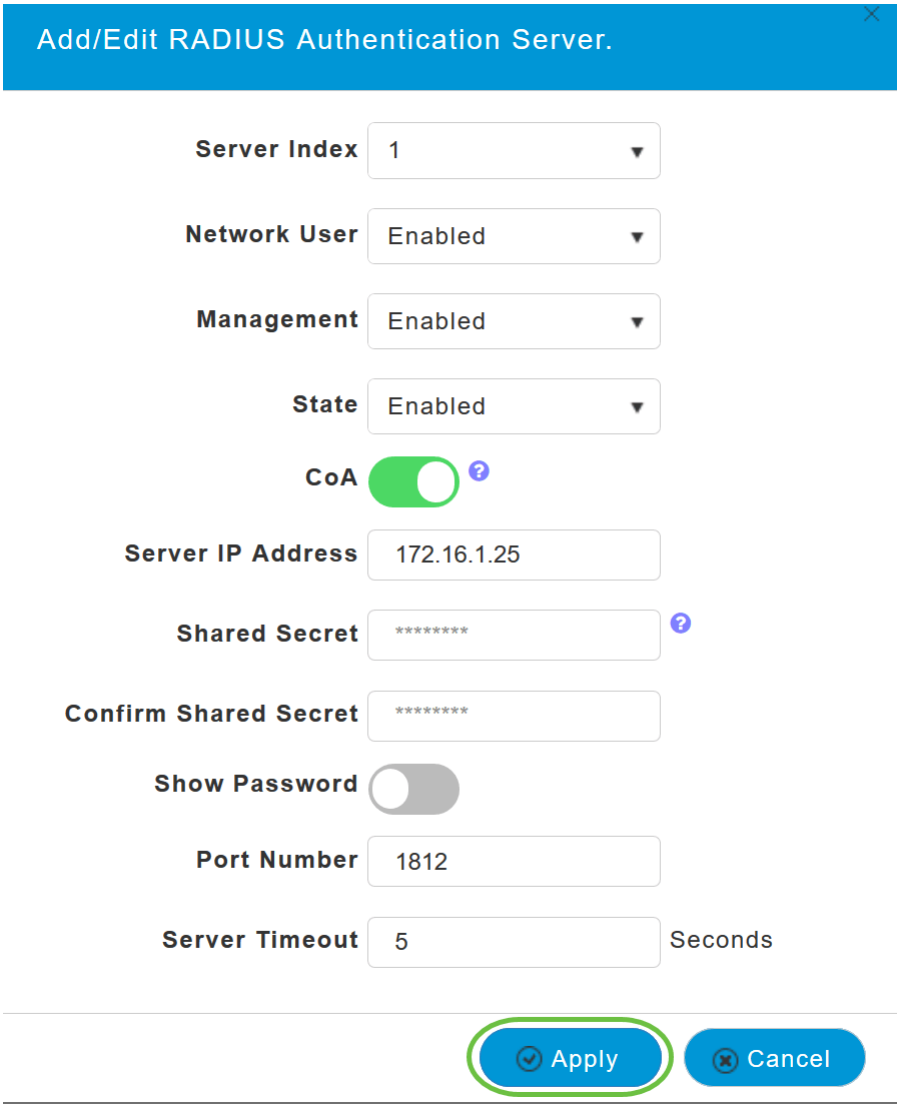


Étape 15

Dans la fenêtre contextuelle *Add/Edit RADIUS Authentication*, configurez les éléments suivants :

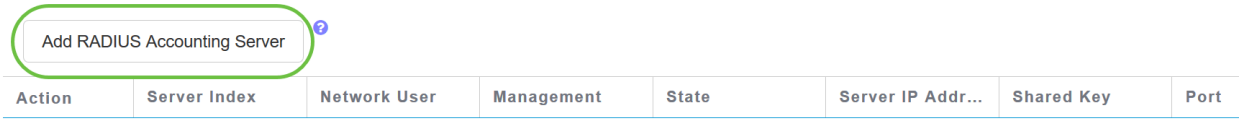
- *Index de serveur* - Sélectionner 1 à 6
- *Network User* - Activez l'état. Par défaut, cette option est activée
- *Gestion* - Activez l'état. Par défaut, cette option est activée
- *State* - Activez l'état. Par défaut, cette option est activée
- *CoA* - Vous pouvez choisir d'activer cette option en déplaçant le bouton du curseur
- *Adresse IP du serveur* : saisissez l'adresse IPv4 du serveur RADIUS.
- *Secret partagé* - Entrez le secret partagé
- *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.



Étape 16

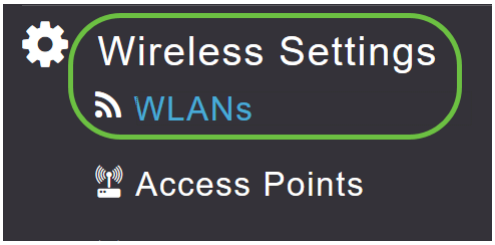
Pour ajouter *RADIUS Accounting Server*, suivez les mêmes étapes que celles de l'étape 15 car la page contient des champs similaires.



Configurer WLAN

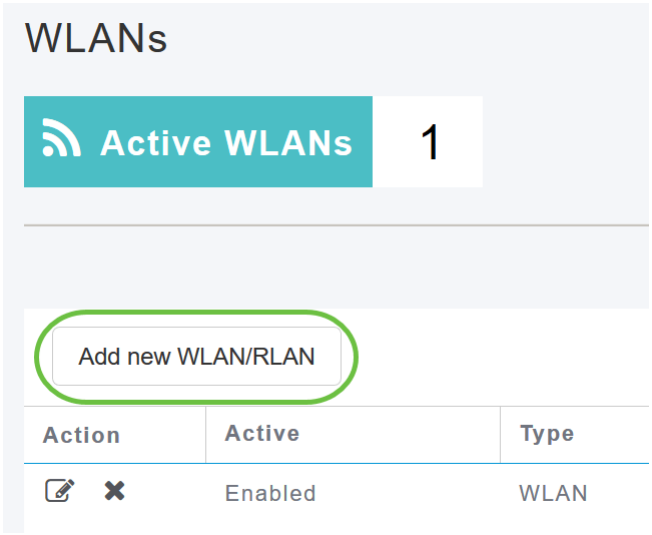
Étape 1

Pour configurer un WLAN qui va gérer l'authentification WPA2 avec RADIUS, accédez à **Wireless settings > WLAN**.



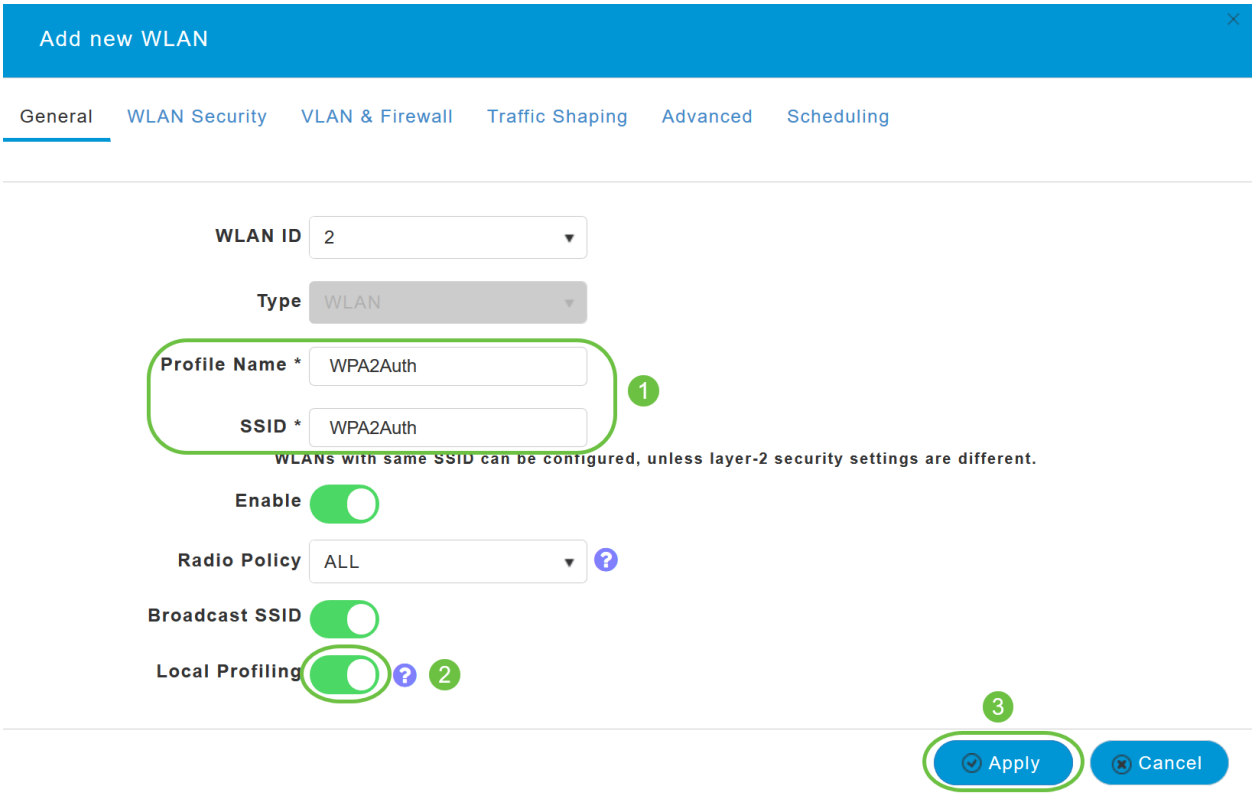
Étape 2

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



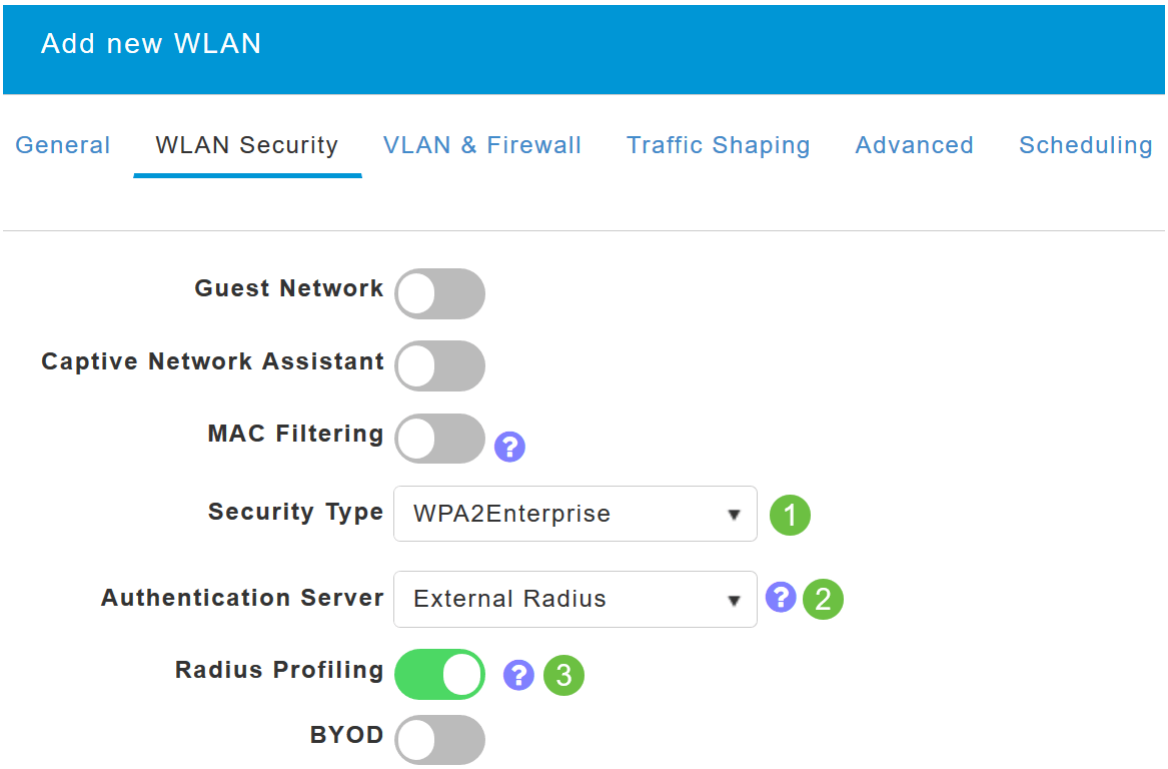
Étape 3

Dans l'onglet *Général*, saisissez le *nom du profil*. Le champ *SSID* est renseigné automatiquement. Vous pouvez choisir d'activer le *profilage local*. Cliquez sur Apply.



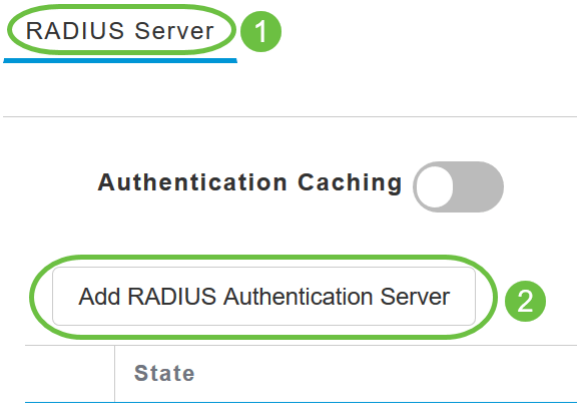
Étape 4

Accédez à l'onglet *Sécurité WLAN*. Dans le menu déroulant *Security Type*, sélectionnez **WPA2Enterprise**. Sélectionnez **Radius externe** comme *serveur d'authentification*. Vous pouvez choisir d'activer le *profilage Radius*.



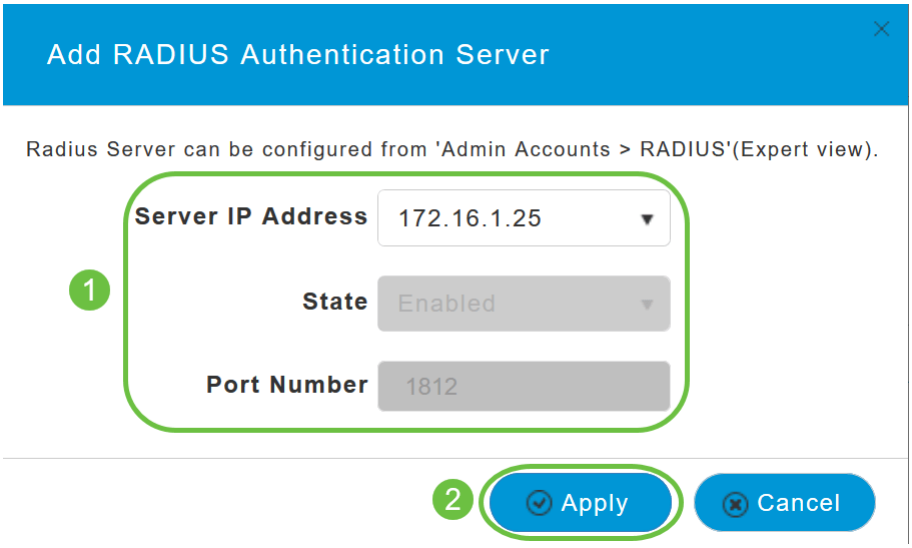
Étape 5

Accédez à la section *Serveur RADIUS*. Cliquez sur **Add RADIUS Authentication Server**.



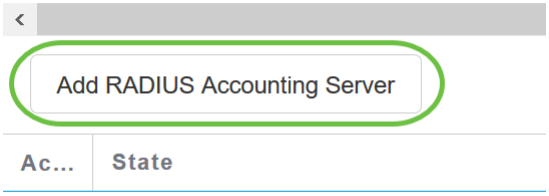
Étape 6

Vérifiez les détails du serveur d'authentification RADIUS que vous avez configuré et cliquez sur **Apply**.



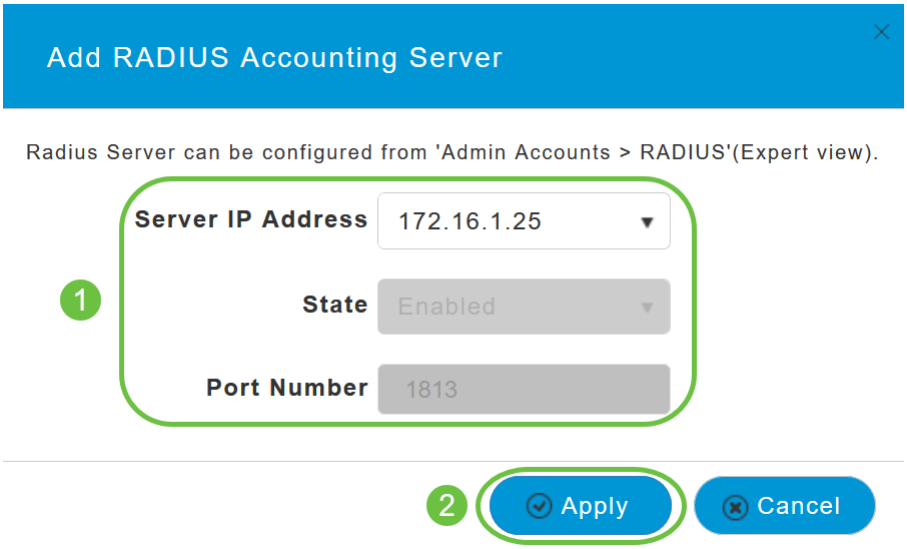
Étape 7

Cliquez sur **Add RADIUS Accounting Server**.



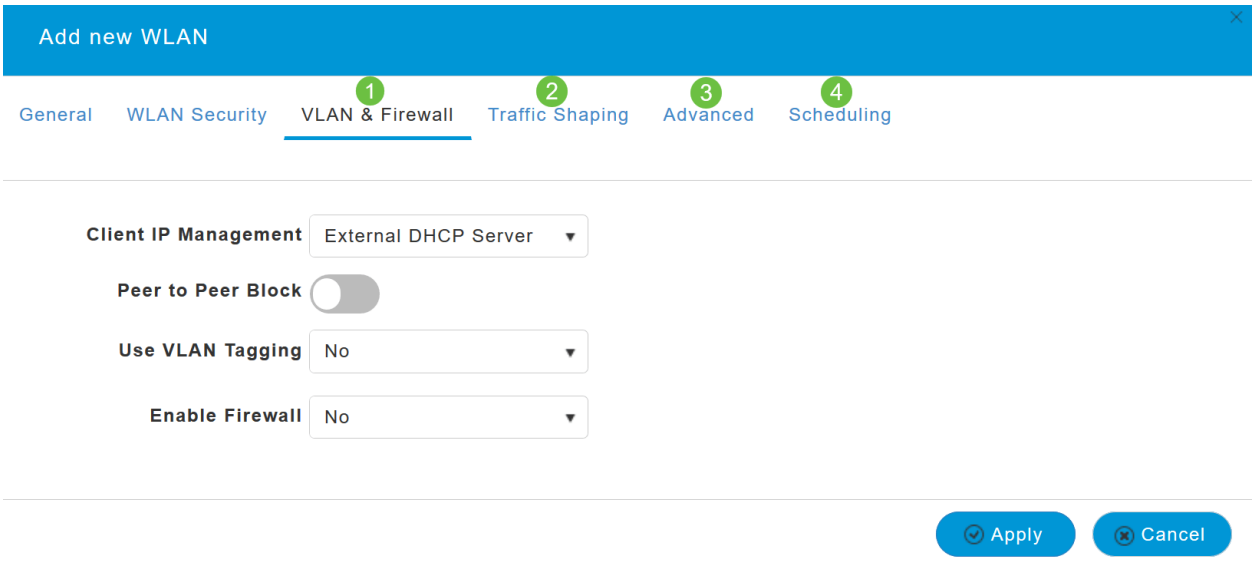
Étape 8

Vérifiez les détails du serveur de comptabilité RADIUS que vous avez configuré et cliquez sur **Apply**.



Étape 9

Accédez aux onglets *VLAN & Firewall*, *Traffic Shaping*, *Advanced* et *Scheduling* pour configurer les paramètres en fonction de vos préférences réseau. Cliquez sur Apply.

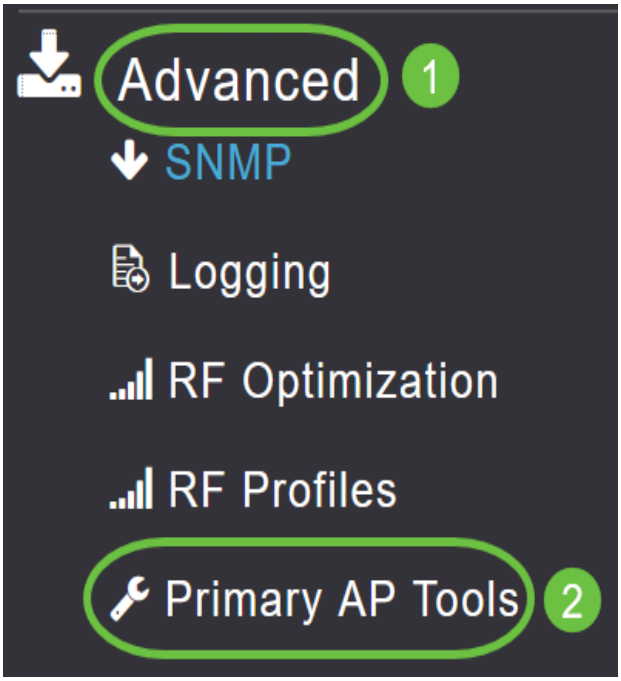


Vérification

Pour tester l'authentification RADIUS, procédez comme suit :

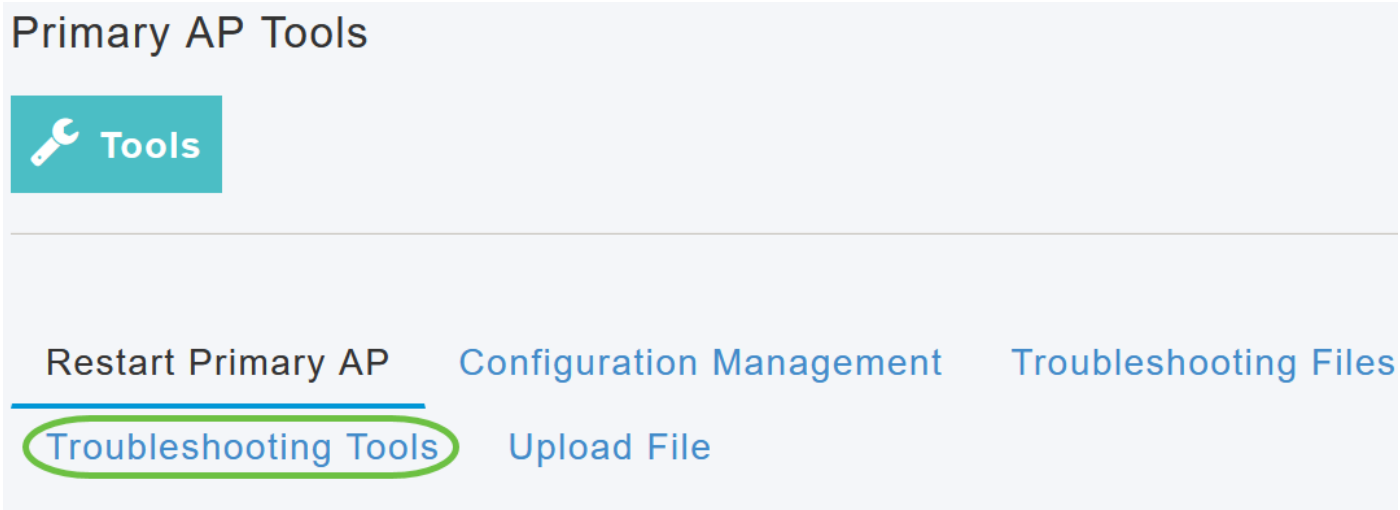
Étape 1

Accédez à **Advanced > Primary AP Tools**.



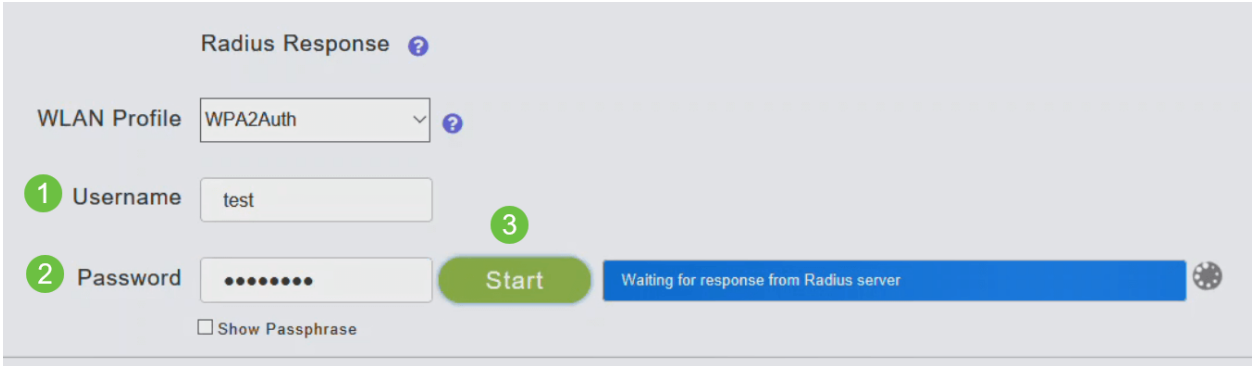
Étape 2

Cliquez sur **Outils de dépannage**.



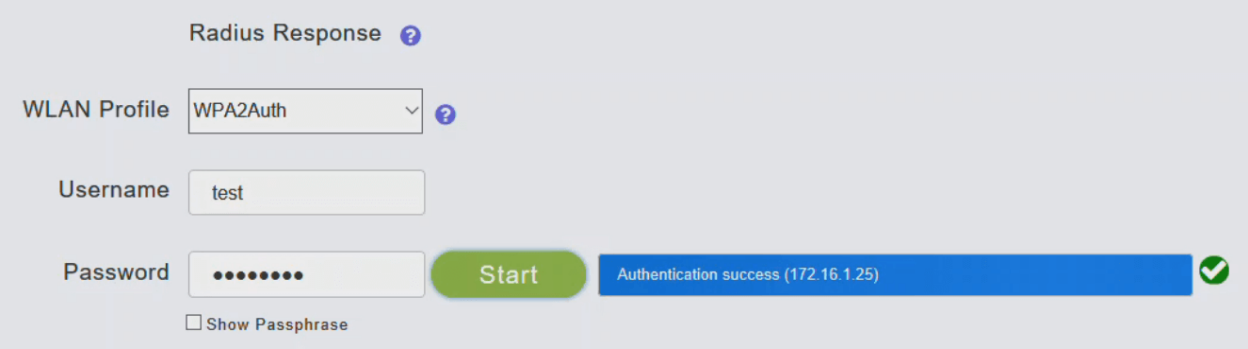
Étape 3

Dans la section *Réponse Radius*, saisissez le *nom d'utilisateur* et le *mot de passe* du profil WLAN que vous avez configuré précédemment et cliquez sur **Démarrer**.



Étape 4

Une fois la vérification terminée, la notification suivante s'affiche à l'écran.



Conclusion

Voilà ! Vous avez maintenant appris les étapes de configuration de RADIUS sur votre point d'accès CBW. Pour obtenir des configurations plus avancées, reportez-vous au *Guide d'administration des points d'accès sans fil Cisco Business.*

Forum aux questions Mise à niveau du micrologiciel RLAN Profilage des applications Profilage client Outils PA principaux Umbrella Utilisateurs WLAN Journalisation Modélisation du trafic Rogues Interféreurs Gestion de la configuration Mode de maillage de configuration de port