Configurez les paramètres de sécurité sans fil sur un WAP

Introduction

Configurer la Sécurité Sans fil sur votre point d'accès sans fil (WAP) est haut-essentiel pour protéger votre réseau Sans fil contre les intrus qui peuvent compromettre l'intimité de vos périphériques sans fil aussi bien que des données transmettant au-dessus de votre réseau Sans fil. Vous pouvez configurer la Sécurité Sans fil sur votre réseau Sans fil en installant le filtre d'adresses MAC, l'accès protégé par Wi-Fi (WPA/WPA2) personnel, et l'entreprise WPA/WPA2.

Le filtrage MAC est utilisé pour filtrer les clients sans fil pour accéder au réseau utilisant leurs adresses MAC. Une liste de client sera configurée à permettent ou bloquent aux adresses sur la liste pour accéder au réseau, selon votre préférence. Pour se renseigner plus sur le filtrage MAC, a cliquez ici.

L'entreprise WPA/WPA2 personnel et WPA/WPA2 sont des protocoles de Sécurité utilisés pour protéger l'intimité en chiffrant les données transmises au-dessus du réseau Sans fil. WPA/WPA2 est compatible avec les normes ieees 802.11E et 802.11i. Comparé au protocole de Sécurité de Confidentialité équivalente aux transmissions par fil (WEP), WPA/WPA2 ont amélioré l'authentification et les fonctionnalités de chiffrement.

WPA/WPA2 personnel est pour l'entreprise à la maison d'utiliser-et WPA/WPA2 est pour le réseau entreprise-mesuré. L'entreprise WPA/WPA2 fournit la sécurité accrue et le contrôle centralisé au-dessus du réseau comparé à WPA/WPA2 personnel.

Dans ce scénario, la Sécurité Sans fil va être configurée sur le WAP pour protéger le réseau contre des intrus utilisant WPA/WPA2 les configurations personnelles et d'entreprise.

Objectif

Ce buts de l'article de t'afficher comment configurer WPA/WPA2 protocoles personnelle et d'entreprise de Sécurité pour améliorer la sécurité et confidentialité de votre réseau Sans fil.

Note: Cet article suppose qu'un Identifiant SSID (Service Set Identifier) ou un réseau local sans fil (WLAN) a été déjà créé sur votre WAP.

Périphériques applicables

- Gamme WAP100
- Gamme WAP300
- Gamme WAP500

Version de logiciel

- 1.0.2.14 – WAP131, WAP351
- 1.0.6.5 – WAP121, WAP321
- 1.3.0.4 – WAP371

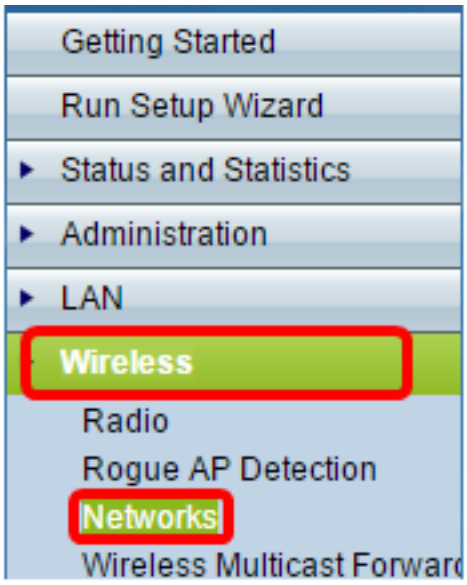
- 1.1.0.7 – WAP150, WAP361
- 1.2.1.5 - WAP551, WAP561
- 1.0.1.11 – WAP571, WAP571E

Configurez les paramètres de sécurité sans fil

Configurez WPA/WPA2 personnel

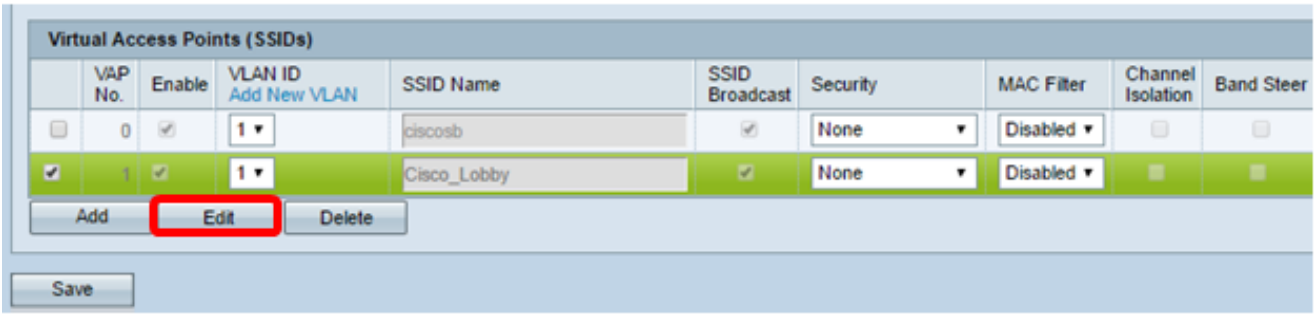
Étape 1. Ouvrez une session à l'utilitaire basé sur le WEB de votre Point d'accès et choisissez la **radio > les réseaux**.

Note: Dans l'image ci-dessous, l'utilitaire basé sur le WEB du WAP361 est utilisé comme exemple. Les options du menu peuvent varier selon le modèle de votre périphérique.

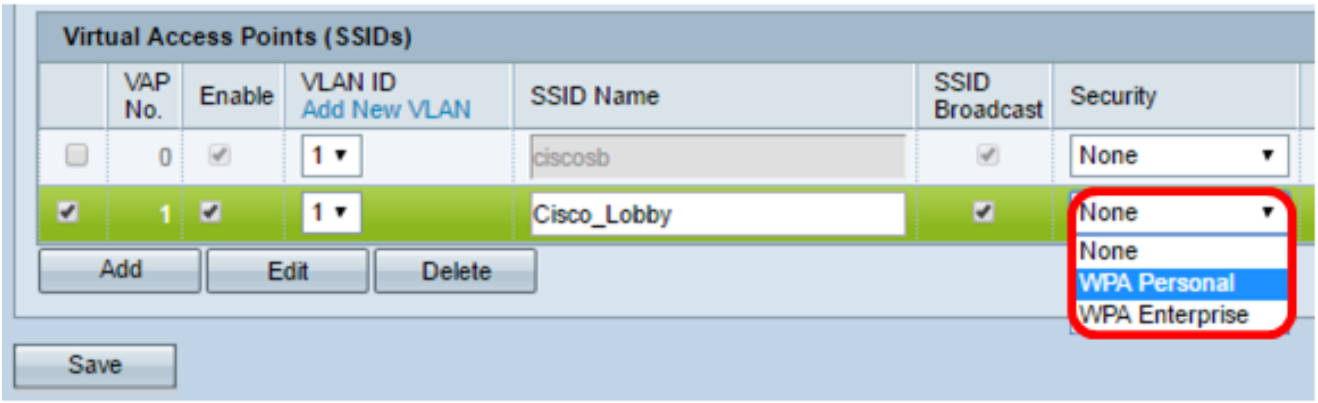


Étape 2. Sous la région virtuelle des Points d'accès (SSID), cochez la case du SSID que vous voulez configurer et cliquer sur Edit.

Remarque: Dans cet exemple, VAP1 est choisi.



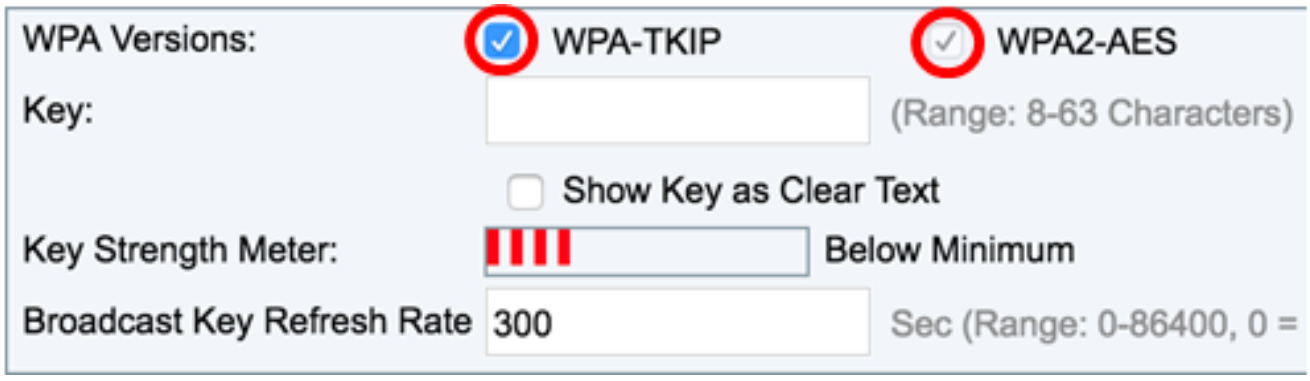
Étape 3. Clic **WPA personnel de la** liste déroulante de Sécurité.



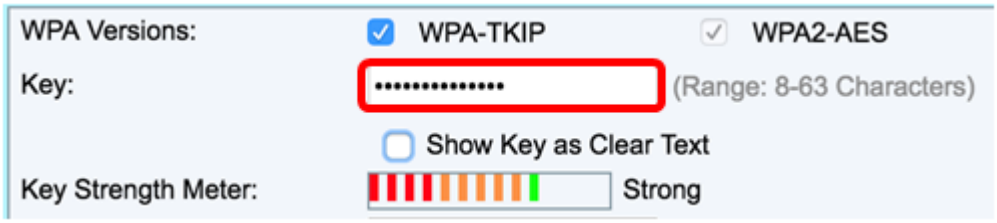
Étape 4. Choisissez la version WPA (WPA-TKIP ou WPA2-AES) en cochant la case. Deux peuvent être choisis immédiatement.

- WPA-TKIP — Outil principal Access-temporel d'intégrité de Wi-Fi Protected. Le réseau a quelques stations client qui prennent en charge seulement le protocole de l'original WPA et de Sécurité TKIP. Notez qu'on ne permet pas choisir seulement WPA-TKIP pour le Point d'accès selon la dernière condition requise de Wi-Fi Alliance.
- WPA2-AES — Norme de chiffrement Access-avancée de Wi-Fi Protected. Toutes les stations client sur le support réseau WPA2 et AES-CCMP chiffrent/protocole de Sécurité. Cette version WPA fournit la meilleure Sécurité par norme d'IEEE 802.11i. Selon la dernière condition requise de Wi-Fi Alliance, le WAP doit prendre en charge ce mode tout le temps.

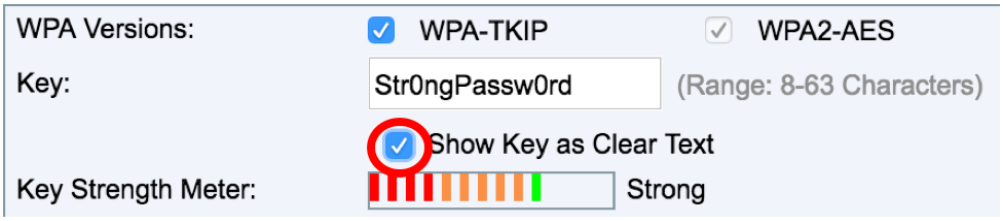
Remarque: Pour cet exemple, les deux cases sont vérifiées.



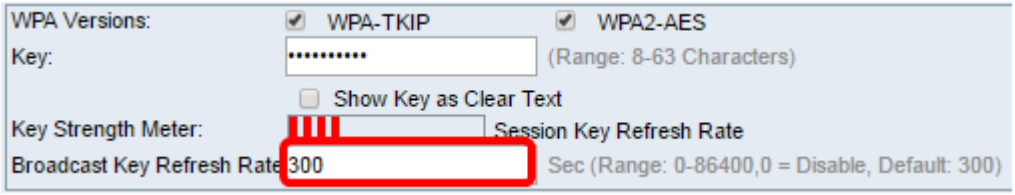
Étape 5. Créez un mot de passe se composant de 8-63 caractères et écrivez-le dans la zone de tri.



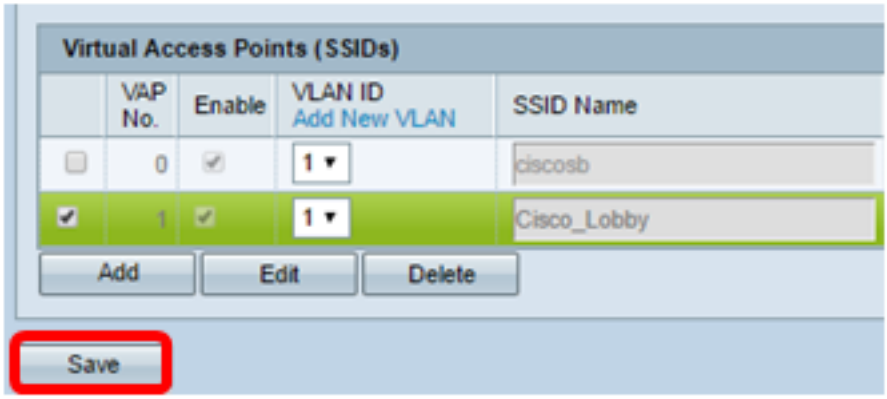
Note: Vous pouvez cocher la **clé d'exposition comme clairement zone de texte** pour afficher le mot de passe que vous avez créé.



Étape 6. (facultative) dans le domaine de *fréquence d'actualisation de clé d'émission*, écrivent une valeur ou l'intervalle auxquels la clé d'émission (groupe) est régénérée pour des clients associés avec ce VAP. Le par défaut est de 300 secondes et la plage valide est de 0 à 86400 secondes. Une valeur de 0 indique que la clé d'émission n'est pas régénérée.



Étape 7. **Sauvegarde de** clic.

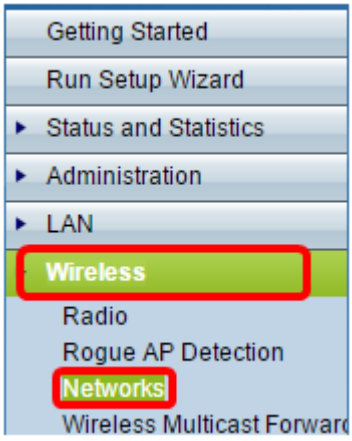


Vous maintenant avez configuré le WPA personnel sur votre WAP.

Configurez l'entreprise WPA/WPA2

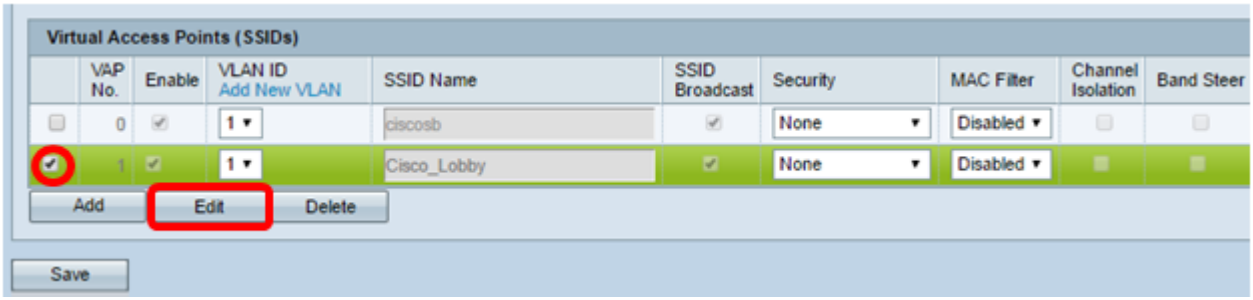
Étape 1. Ouvrez une session à l'utilitaire basé sur le WEB de votre Point d'accès et choisissez la **radio > les réseaux**.

Note: Dans l'image ci-dessous, l'utilitaire basé sur le WEB du WAP361 est utilisé comme exemple.

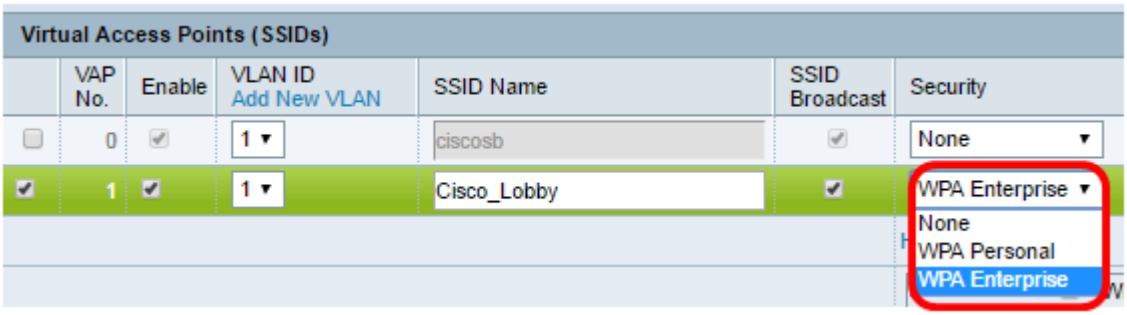


Étape 2. Sous la région virtuelle des Points d'accès (SSID), vérifiez le SSID que vous voulez

configurer et cliquer sur le bouton d'**éditer** au-dessous de elle.



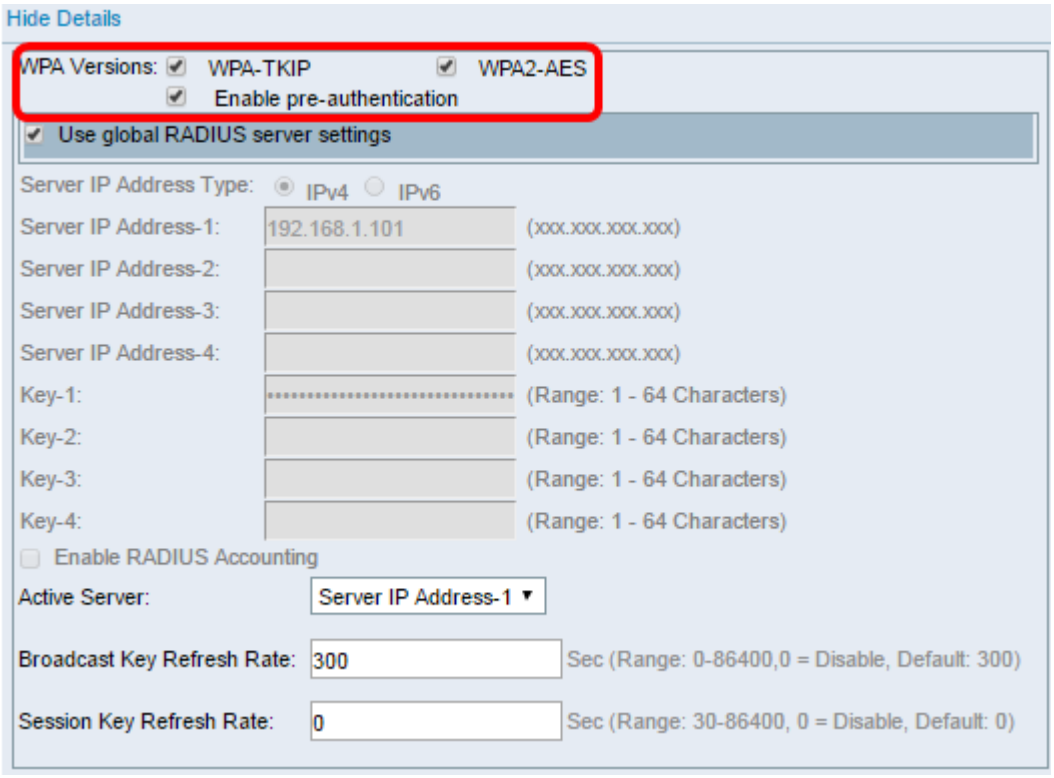
Étape 3. Choisissez le **WPA Enterprise de la** liste déroulante de Sécurité.



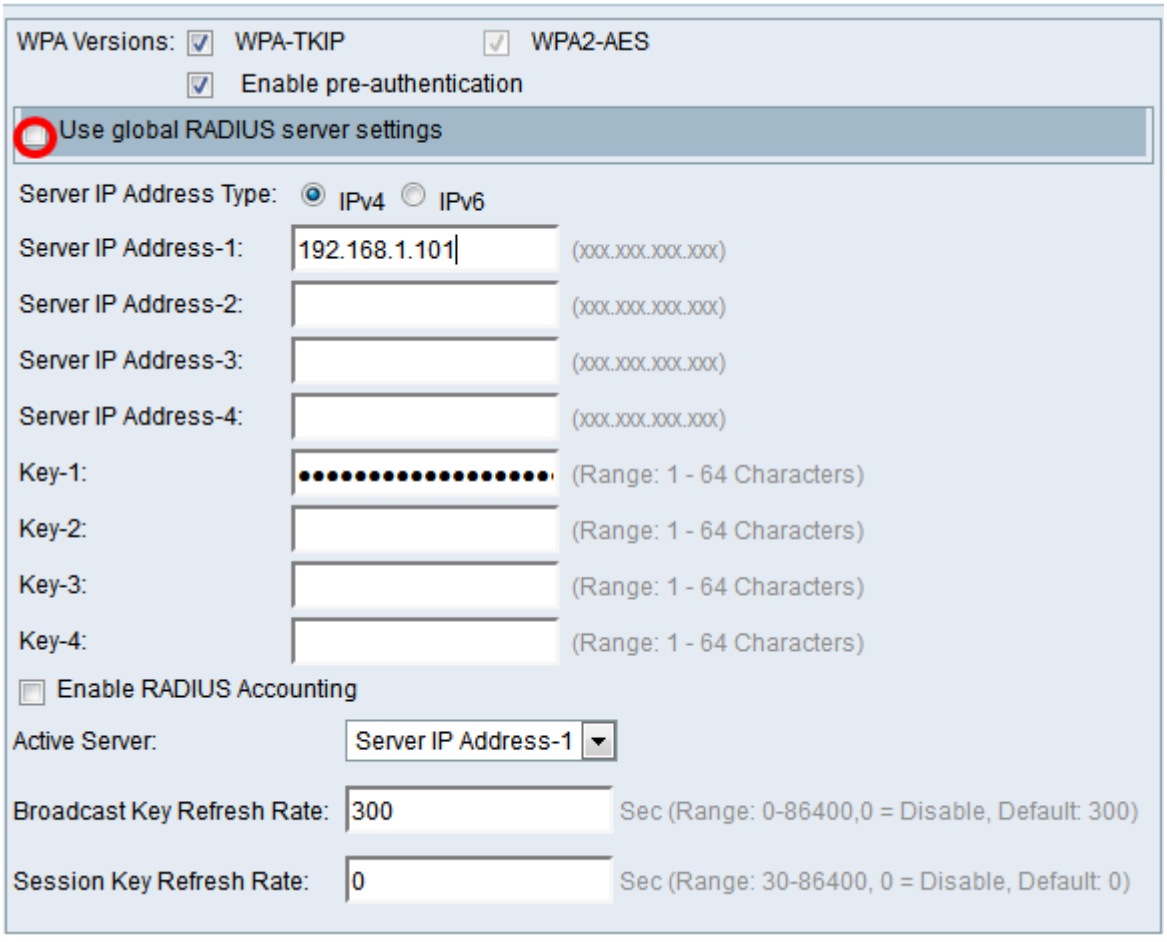
Étape 4. Choisissez la version WPA (WPA-TKIP, WPA2-AES, et pré-authentification d'enable).

- Pré-authentification d'enable — Si vous choisissez WPA2-AES seulement ou WPA-TKIP et WPA2-AES comme version WPA, vous pouvez activer la pré-authentification pour les clients WPA2-AES. Vérifiez cette option si vous voulez que les clients sans fil WPA2 envoient les paquets de pré-authentification. Les informations de pré-authentification sont transmises par relais du périphérique WAP que le client utilise actuellement au périphérique de la cible WAP. L'activation de cette caractéristique peut aider à accélérer l'authentification pour les clients errants qui se connectent aux plusieurs points d'accès (AP).

Remarque: Cette option ne s'applique pas si vous sélectionniez WPA-TKIP pour des versions WPA parce que l'original WPA ne prend en charge pas cette caractéristique.

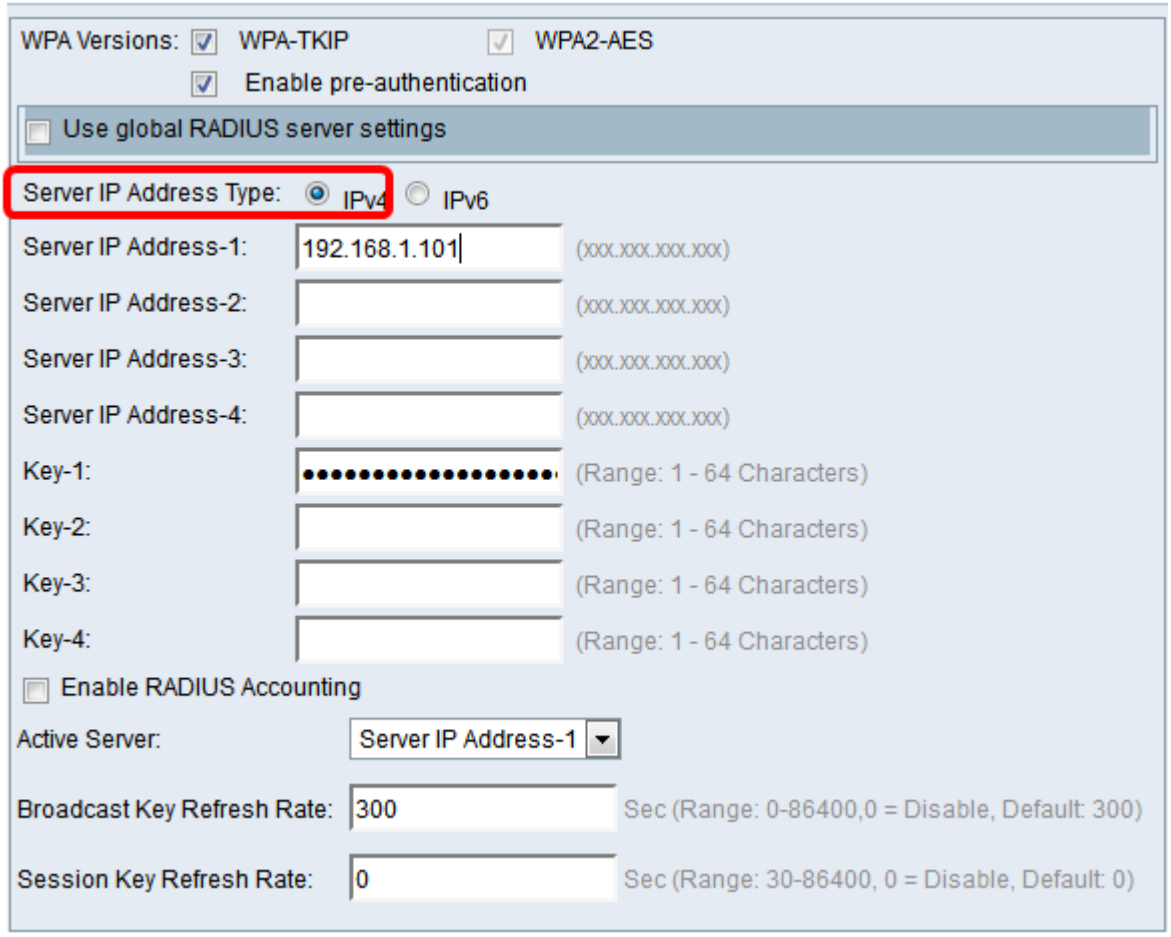


Étape 5. (facultative) décochent la case **globale de configurations de serveur de RADIUS d'utilisation** pour éditer les configurations.



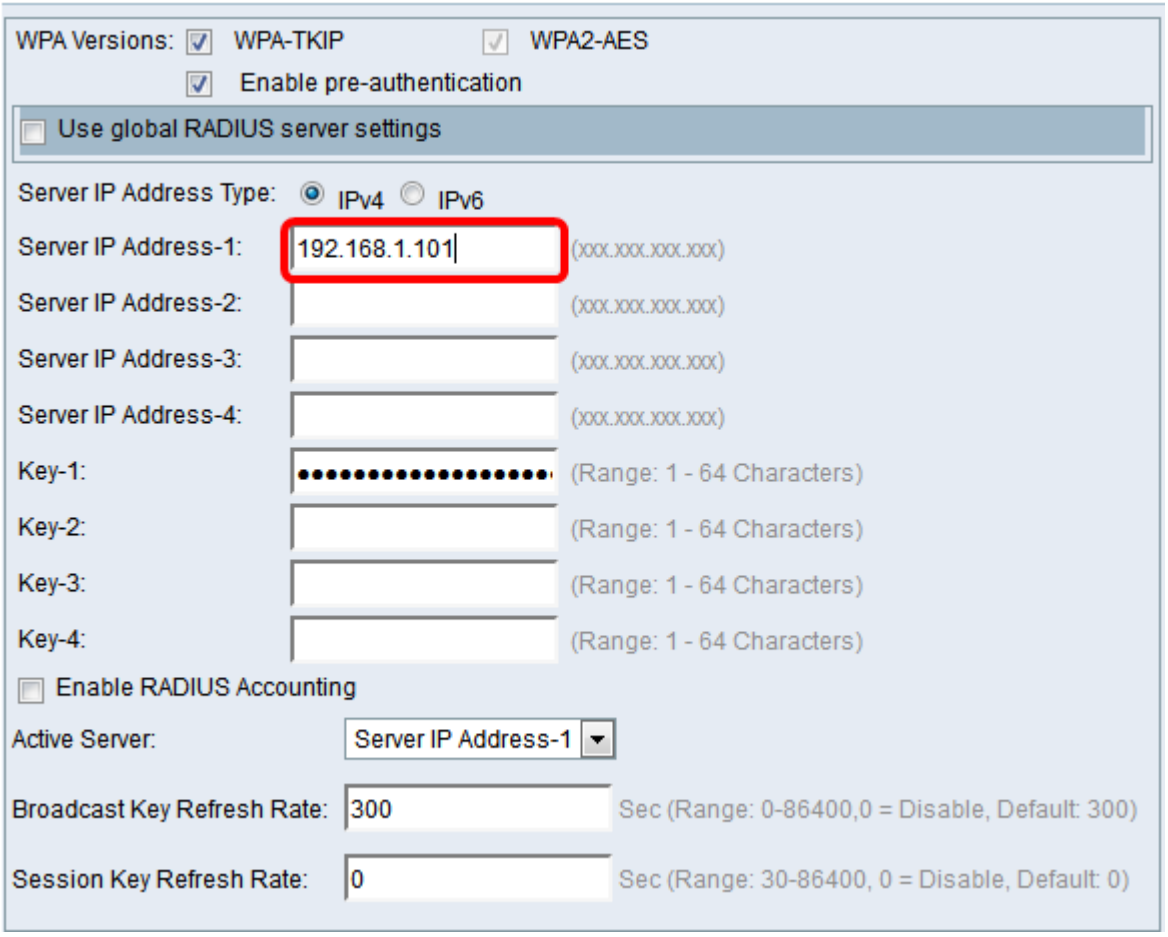
Clic (facultatif) d'étape 6. la case d'option pour le **type** correct d'**adresse IP du serveur**.

Remarque: Pour cet exemple, l'ipv4 est choisi.



Étape 7. Écrivez l'adresse IP du serveur de RADIUS dans le domaine d'*adresse IP du serveur*.

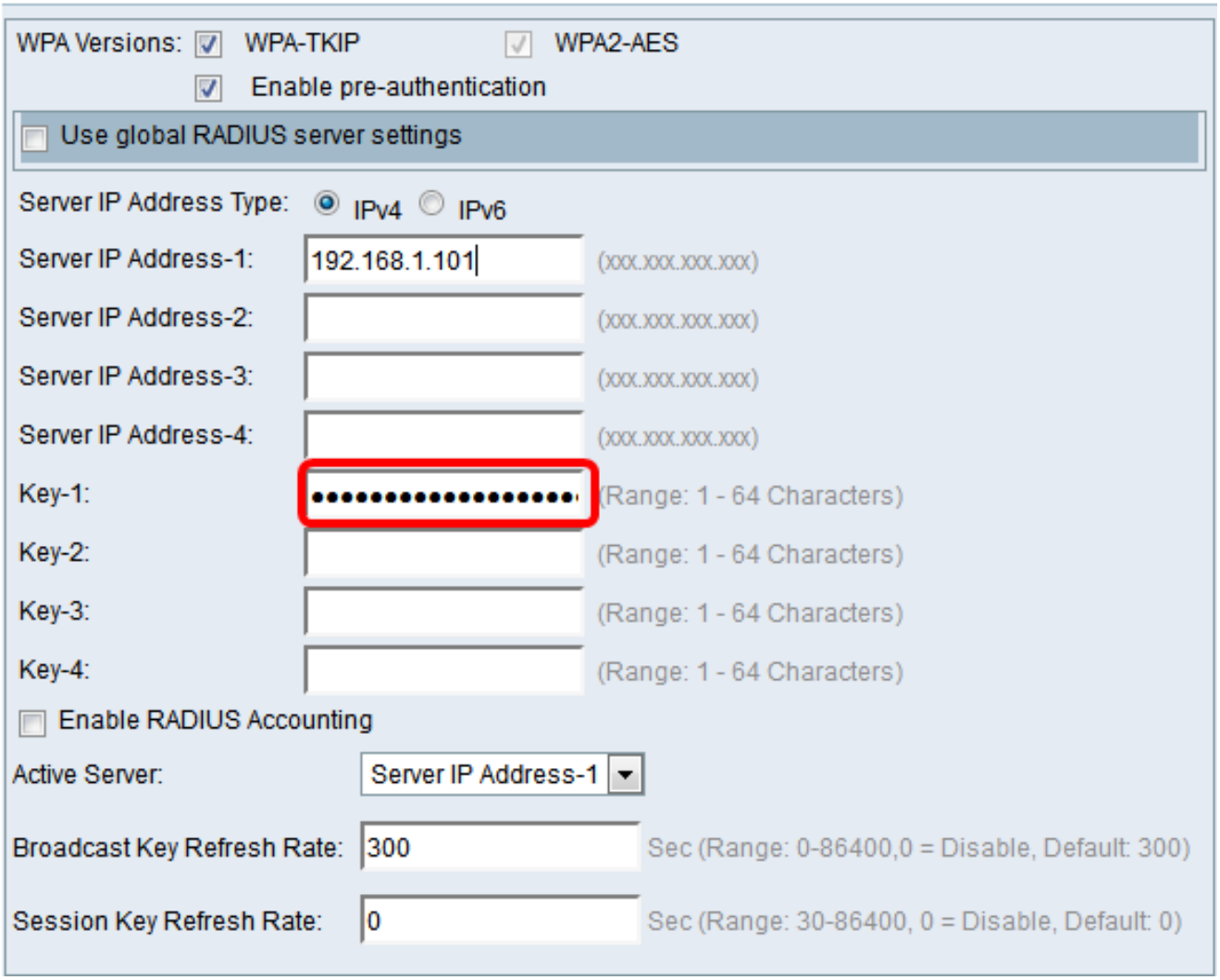
Remarque: Pour cet exemple 192.168.1.101 est utilisé.



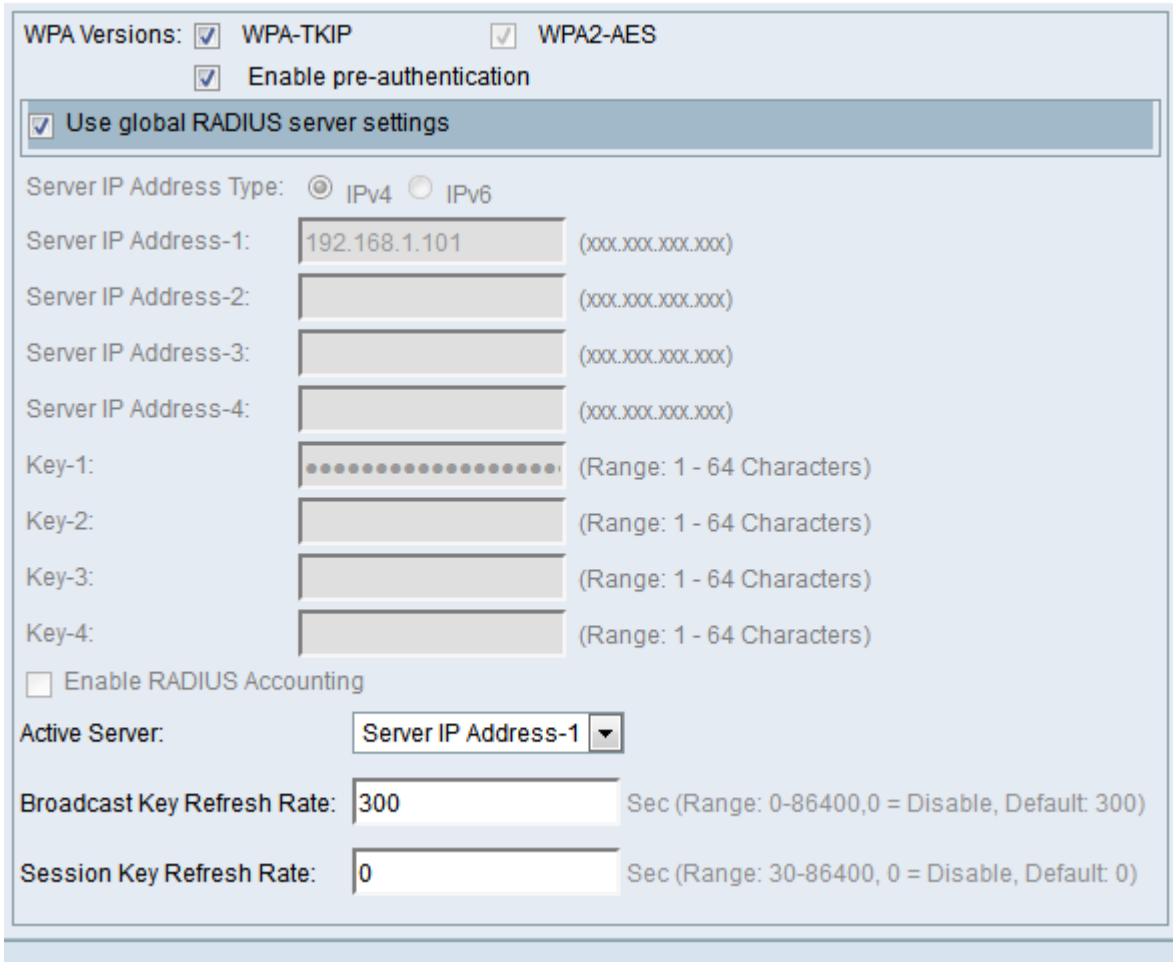
Étape 8. Dans la zone de tri, écrivez la correspondance principale de mot de passe à votre serveur de RADIUS que le WAP l'utilise pour authentifier à RADIUS le serveur. Vous pouvez utiliser de 1 à 64 alphanumériques standard et des caractères particuliers.

Note: Les clés distinguent les majuscules et minuscules et doivent apparier le clé configuré sur le serveur de RADIUS.

Étape 9. (facultative) répètent des étapes 7-8 pour chaque serveur de RADIUS dans votre réseau que vous voulez que le WAP communique avec.



Contrôle (facultatif) d'étape 10. la case de **comptabilité d'EnableRADIUS** pour activer le cheminement et la mesure des ressources qu'un utilisateur a consommées (heure système, la quantité de données transmises). L'activation de cette caractéristique permettra RADIUS expliquant les serveurs primaires et de sauvegarde.



Étape 11. Clic Save.

Vous avez maintenant avec succès configuré la Sécurité de l'entreprise WPA/WPA2 sur votre WAP.