Configurez les paramètres de sécurité sans fil sur le WAP125 et le WAP581

Objectif

La sécurité sans fil te permet pour protéger le réseau Sans fil contre l'accès non autorisé. Le WAP125 et le WAP 581 Points d'accès de charge statique de supports ont câblé la protection équivalente (WEP), le Protocole WPA (Wi-Fi Protected Access) personnel, et le WPA Enterprise. Ces configurations peuvent être configurées par Point d'accès virtuel (VAP). Mettre ces configurations en place fournit la sécurité des réseaux par VAP. Il est typiquement configuré quand le Point d'accès est d'abord déployé, ou quand des mises à jour sont faites aux paramètres de sécurité sans fil du réseau.

Ce buts de l'article de t'afficher comment configurer la Sécurité Sans fil sur un Point d'accès WAP125 ou WAP581.

Périphériques applicables

- WAP125
- WAP581

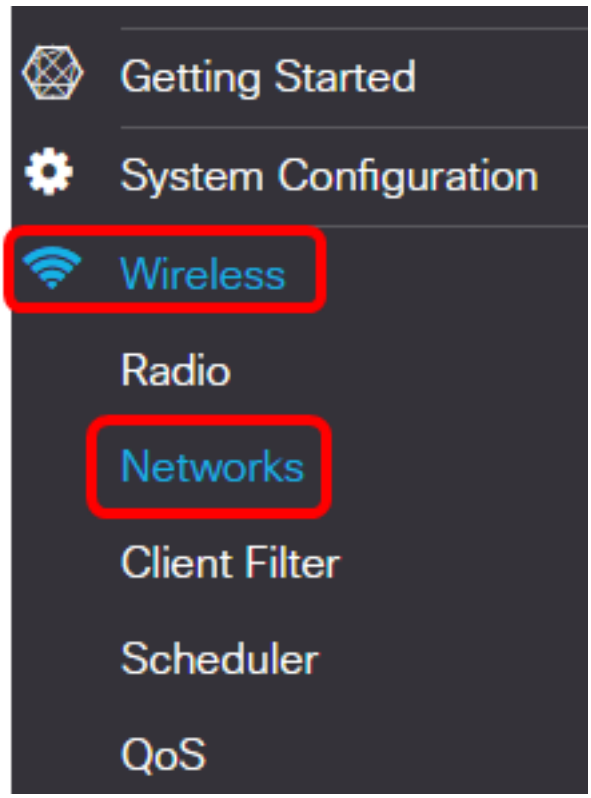
Version de logiciel

- WAP125 - 1.0.0.3
- WAP581 - 1.0.0.4

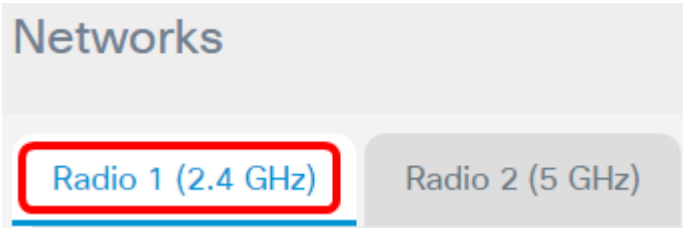
Configurez les paramètres de sécurité sans fil

Configurez le Personal Security WPA

Étape 1. La procédure de connexion à l'utilitaire basé sur le WEB du WAPand choisissent la **radio > les réseaux**.

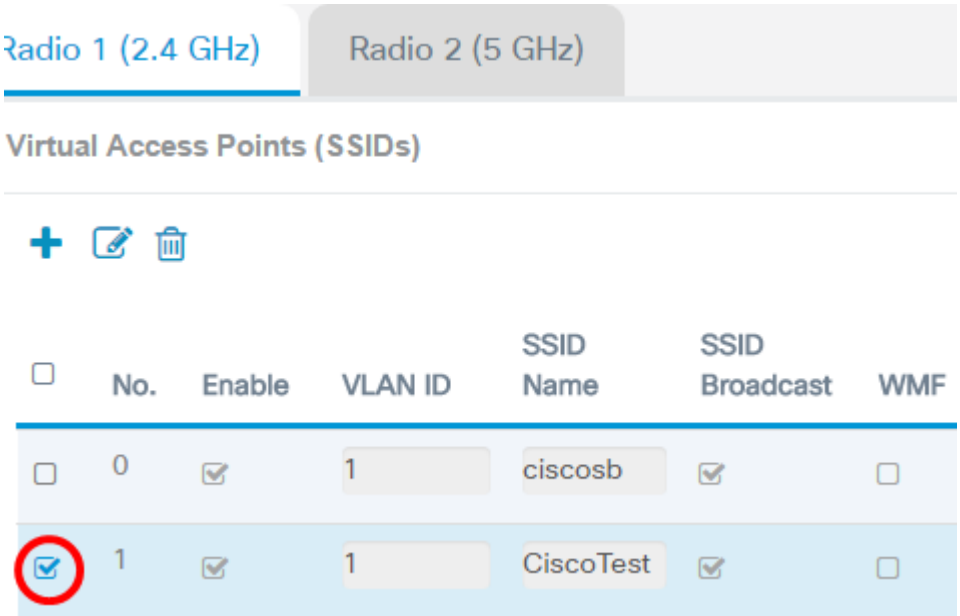


Étape 2. Choisissez la radio dont les paramètres de sécurité sans fil doivent être configurés.



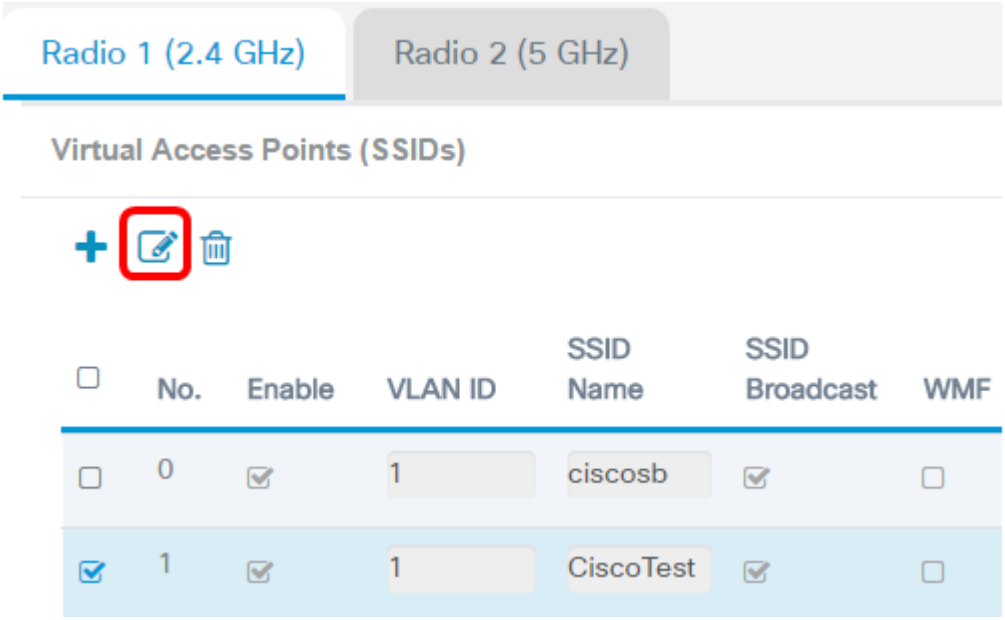
Remarque: Dans cet exemple, la radio 1 (2.4 gigahertz) est choisie.

Étape 3. Cochez la case pour le VAP dont les paramètres de sécurité sans fil doivent être configurés.



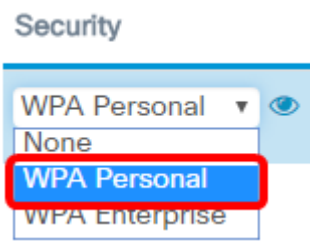
Remarque: Dans cet exemple, VAP 1 est choisi.

Étape 4. Cliquez sur Edit.



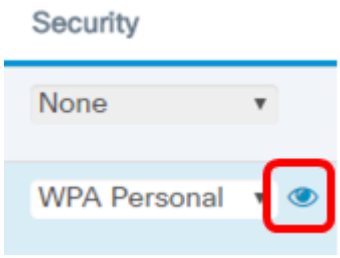
Étape 5. Choisissez une security mode de la liste déroulante de Sécurité. Les options sont :

- Aucun — Cette option désactive les paramètres de sécurité sans fil du VAP sélectionné. Désactiver la security mode ouvre le réseau Sans fil et permet à quiconque avec un périphérique sans fil pour se connecter à votre réseau, et à ses ressources. Tandis que ce mode n'est pas recommandé, il peut être utile aux réseaux dans les sites distants.
- WPA personnel — Cette option implémente la sécurité WPA au réseau Sans fil. Il te permet pour utiliser le Protocole TKIP (Temporal Key Integrity Protocol) ou les algorithmes de Norme AES (Advanced Encryption Standard). Quand mélangé, il permettra les périphériques qui ne prennent en charge pas l'algorithme AES pour se connecter au réseau. Le WPA personnel te permet pour utiliser un mot de passe alphanumérique jusqu'à 64 caractères longs. Le WPA personnel est typiquement utilisé dans les bureaux où un serveur de Service RADIUS (Remote Authentication Dial-In User Service) n'est pas utilisé.
- WPA Enterprise — Cette option vous permet de combiner les fonctionnalités de sécurité offertes par WPA, alors qu'aussi utilisant un serveur de RADIUS. Ceci est typiquement utilisé dans les environnements où un serveur de RADIUS est utilisé. Si vous choisissez cette option, a cliquez ici.



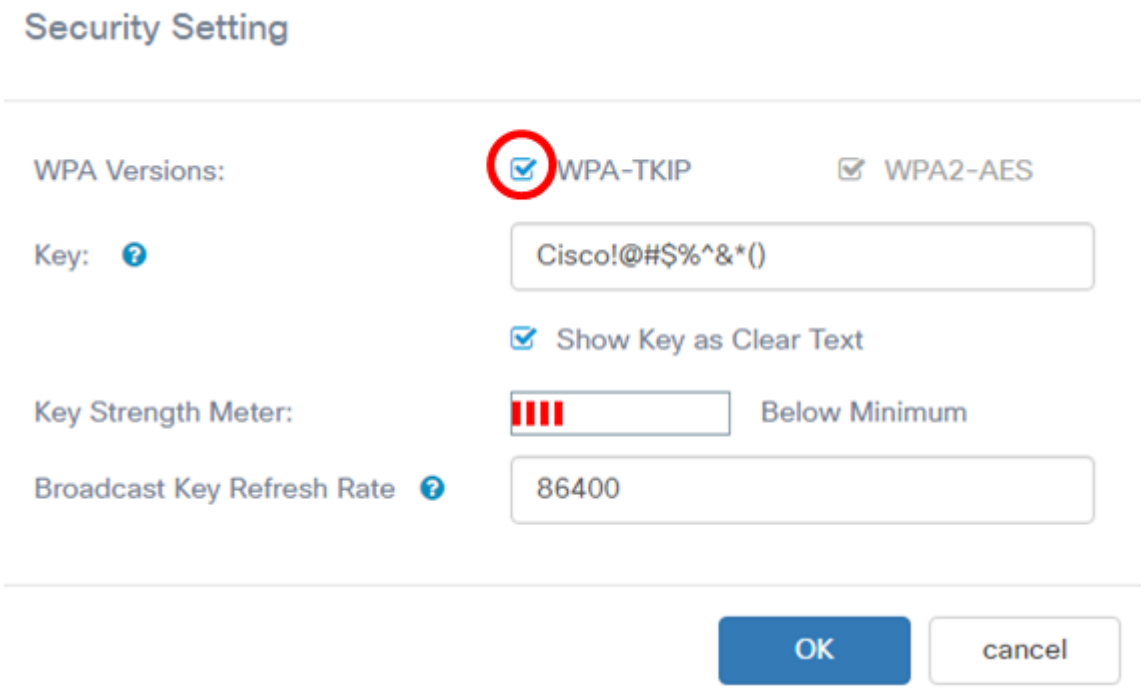
Remarque: Dans cet exemple, le WPA personnel est choisi.

Étape 6. Cliquez sur le bouton de vue pour configurer les paramètres personnels WPA.



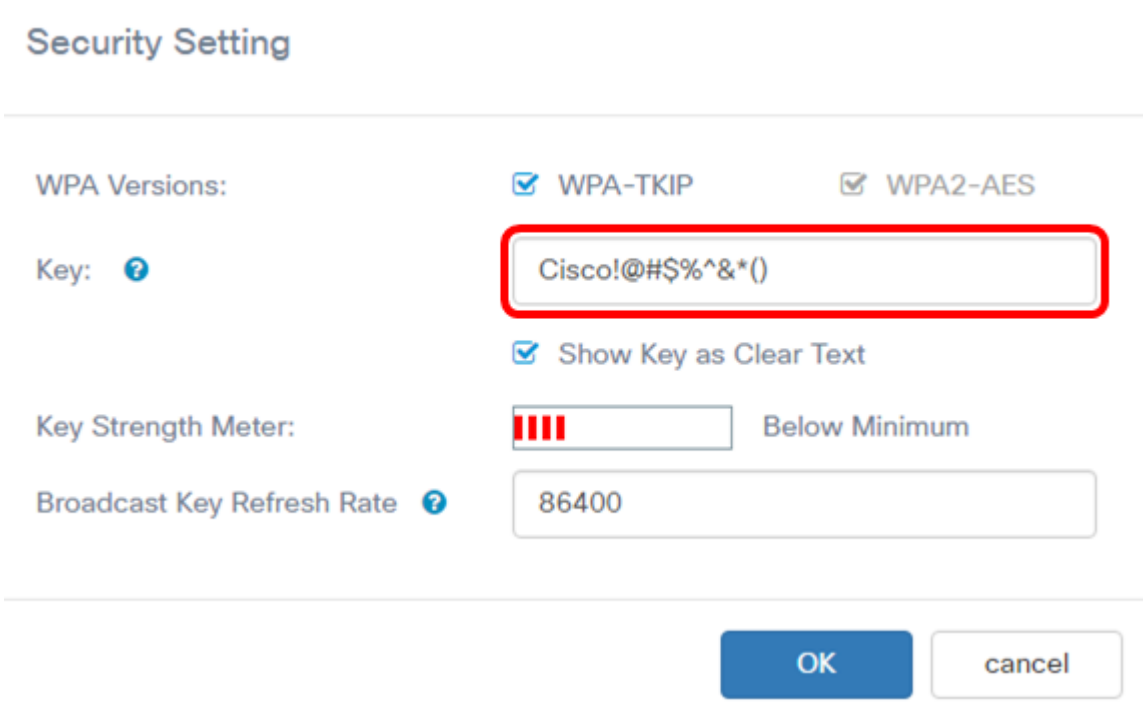
Étape 7. Choisissez votre version WPA dans la région de versions WPA. Les options sont :

- WPA-TKIP — Cette option implémente la Sécurité mélangée sur le réseau Sans fil. Il est idéal pour des réseaux avec les clients sans fil mélangés. Cette option est désactivée par défaut.
- WPA2-AES — Cette option implémente la Sécurité WPA2-AES sur le réseau. C'est idéal pour les réseaux Sans fil avec les clients qui prennent en charge la Sécurité WPA2.



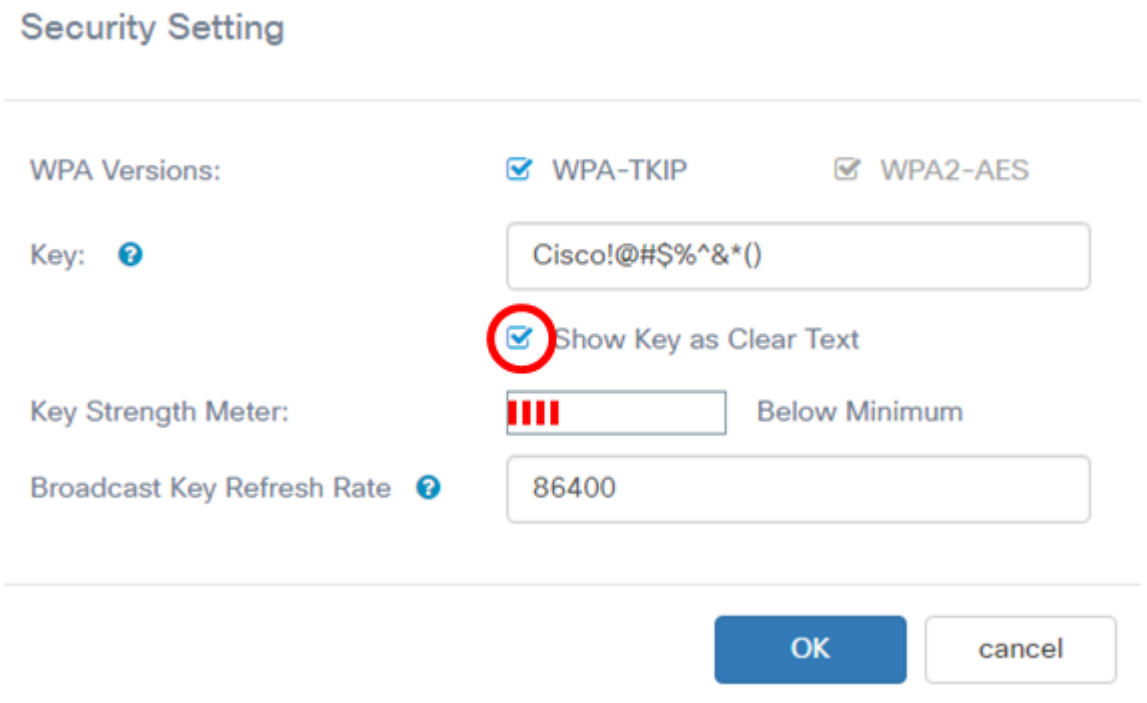
Remarque: Dans cet exemple, WPA-TKIP est vérifié.

Étape 8. Entrez le mot de passe réseau dans la zone de tri. La clé peut être une combinaison des lettres et numéro, de 8 à 63 caractères de longueur.



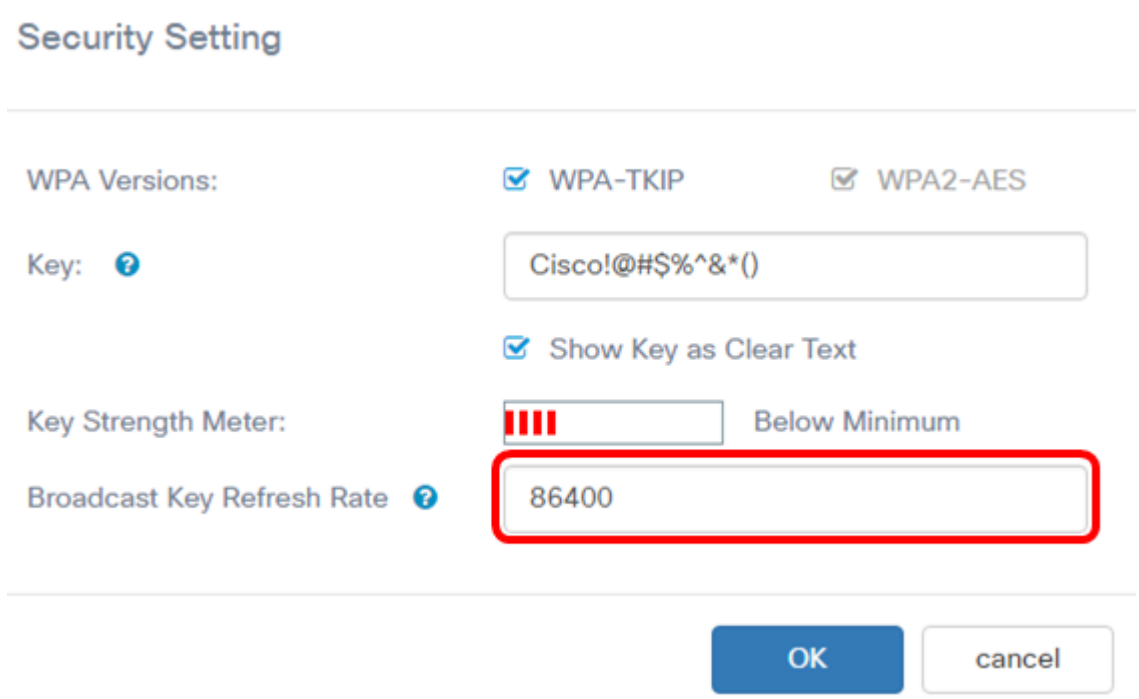
Remarque: Dans cet exemple, Cisco ! @#$%^&* () est écrit.

Contrôle (facultatif) d'étape 9. la **clé d'exposition en tant que** case des **textes clairs** pour visualiser la clé en texte brut.

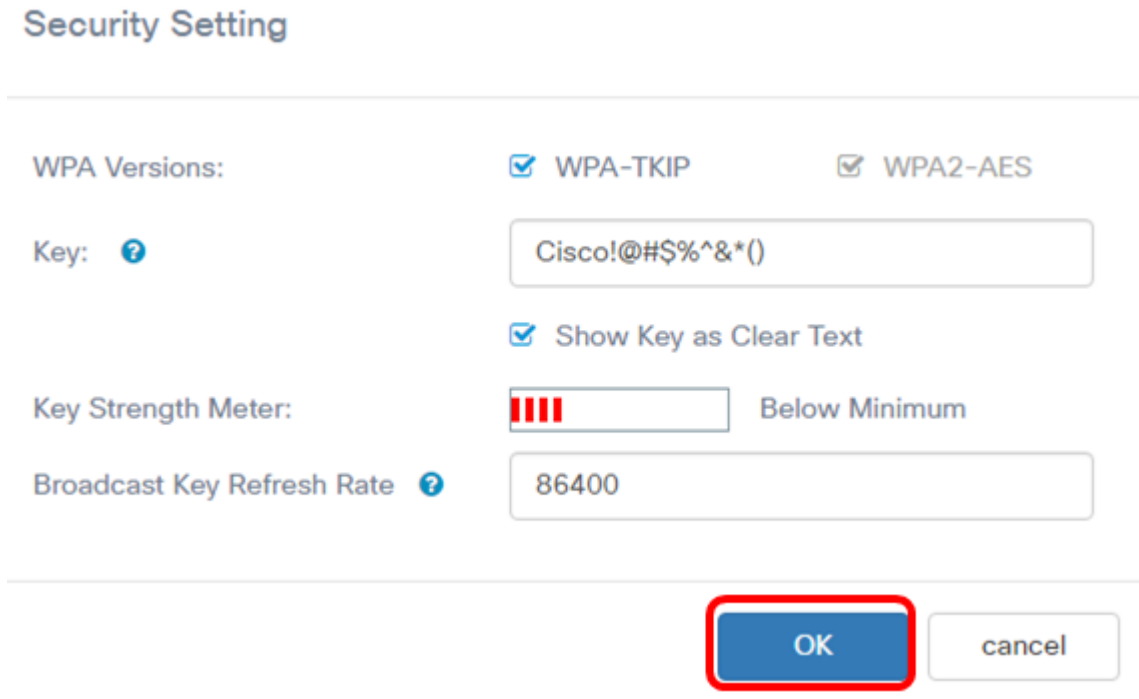


Remarque: Dans cet exemple, la clé d'exposition en tant que texte clair est vérifiée.

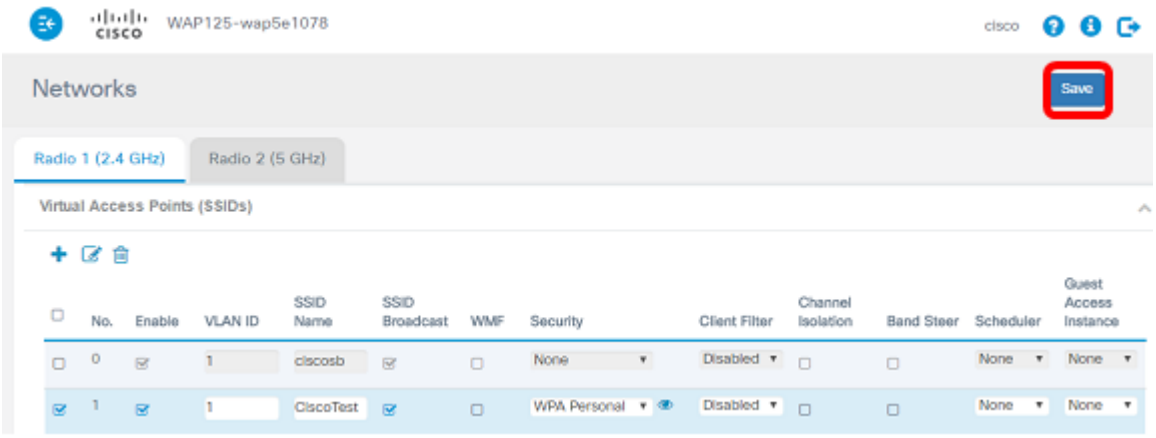
Étape 10. Écrivez le nombre de secondes jusqu'à ce que votre clé de Sécurité soit remplacée par nouvellement une clé générée dans le domaine de *fréquence d'actualisation de clé d'émission*. La valeur par défaut est 86400.



Étape 11. Cliquez sur OK.



Étape 12. Cliquez sur **Save**.

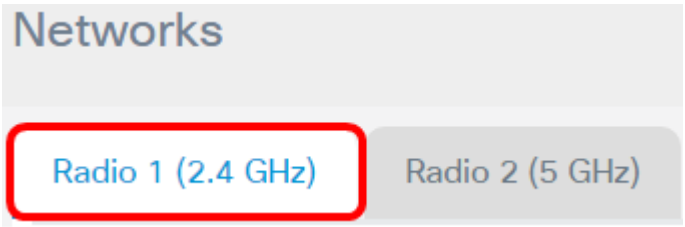


Étape 13. Cliquez sur **OK**.

Les paramètres de sécurité sans fil personnels WPA ont été maintenant configurés sur votre WAP125.

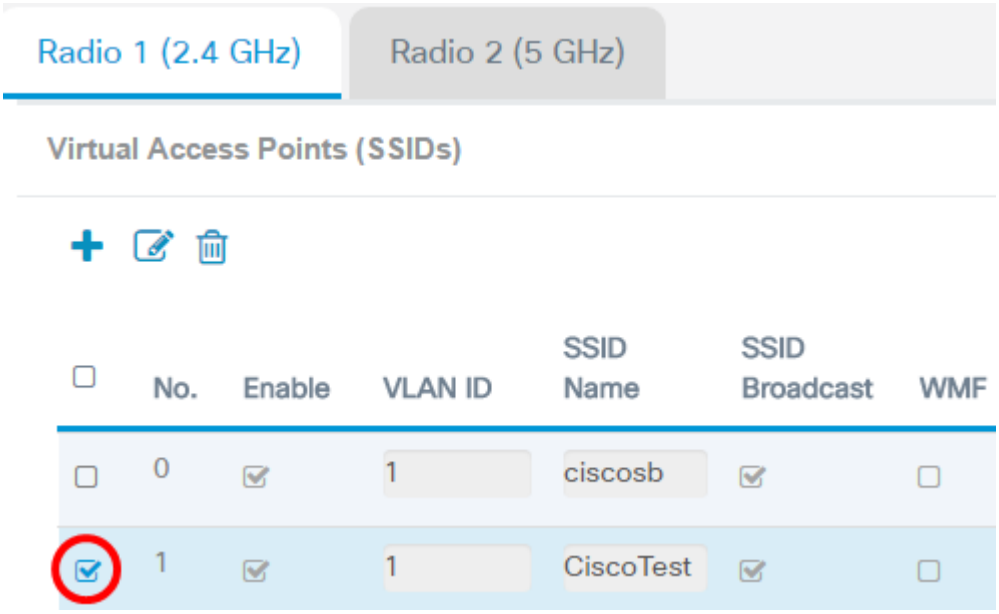
Configurez la Sécurité de WPA Enterprise

Étape 1. Choisissez la radio dont les paramètres de sécurité sans fil doivent être configurés.



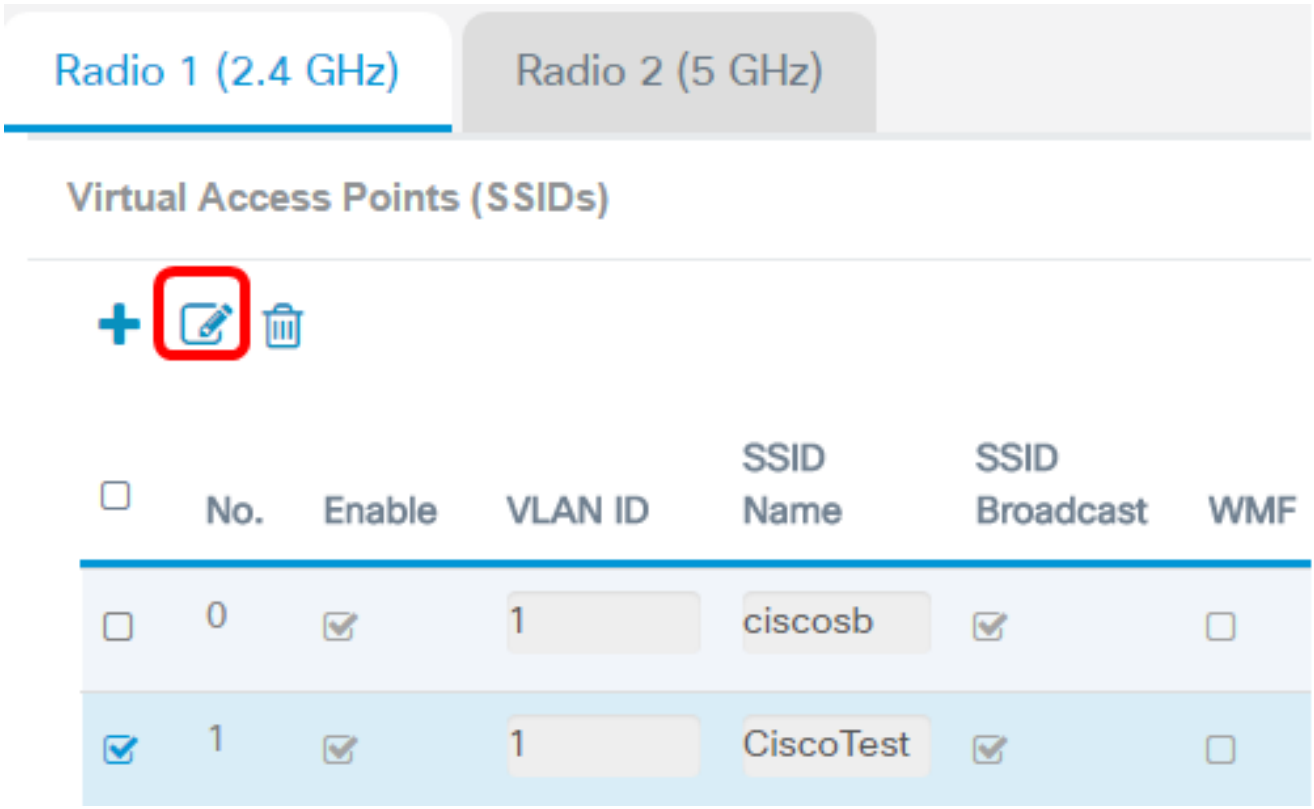
Remarque: Dans cet exemple, la radio 1 (2.4 gigahertz) est choisie.

Étape 2. Cochez la case pour le VAP dont les paramètres de sécurité sans fil doivent être configurés.

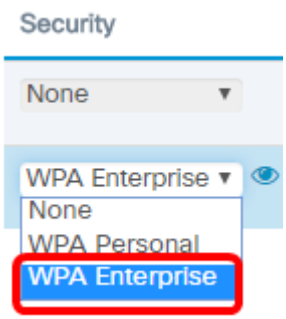


Remarque: Dans cet exemple, VAP 1 est choisi.

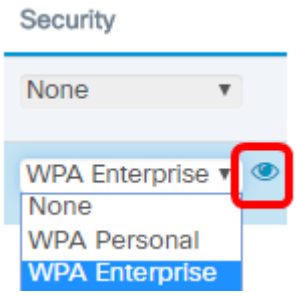
Étape 3. Cliquez sur Edit.



Étape 4. Choisissez le WPA Enterprise de la liste déroulante de Sécurité.

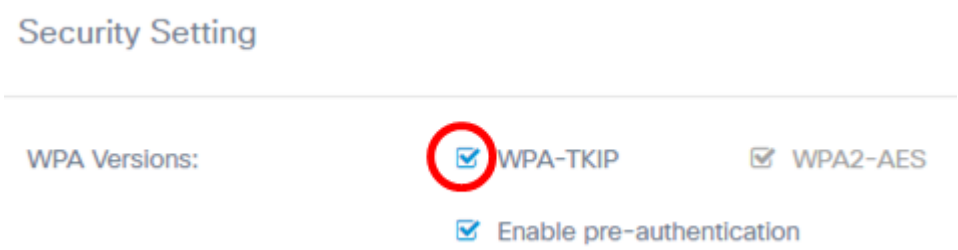


Étape 5. Cliquez sur le bouton de vue pour configurer les paramètres de WPA Enterprise.



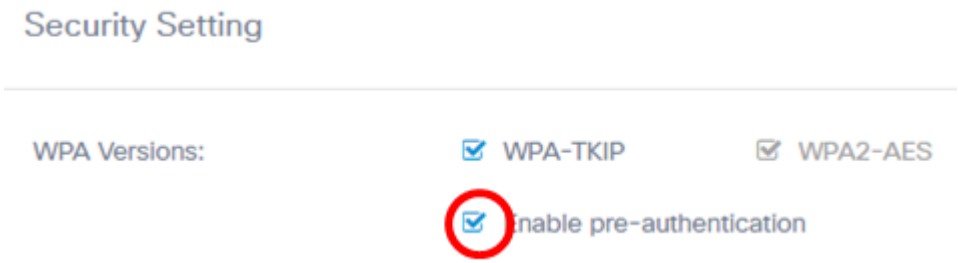
Étape 6. Choisissez votre version WPA dans la région de versions WPA. Les options sont :

- WPA-TKIP — Cette option implémente la Sécurité mélangée sur le réseau Sans fil. Il est idéal pour des réseaux avec les clients sans fil mélangés. Cette option est désactivée par défaut.
- WPA2-AES — Cette option implémente la Sécurité WPA2-AES sur le réseau. C'est idéal pour les réseaux Sans fil avec les clients qui prennent en charge la Sécurité WPA2.

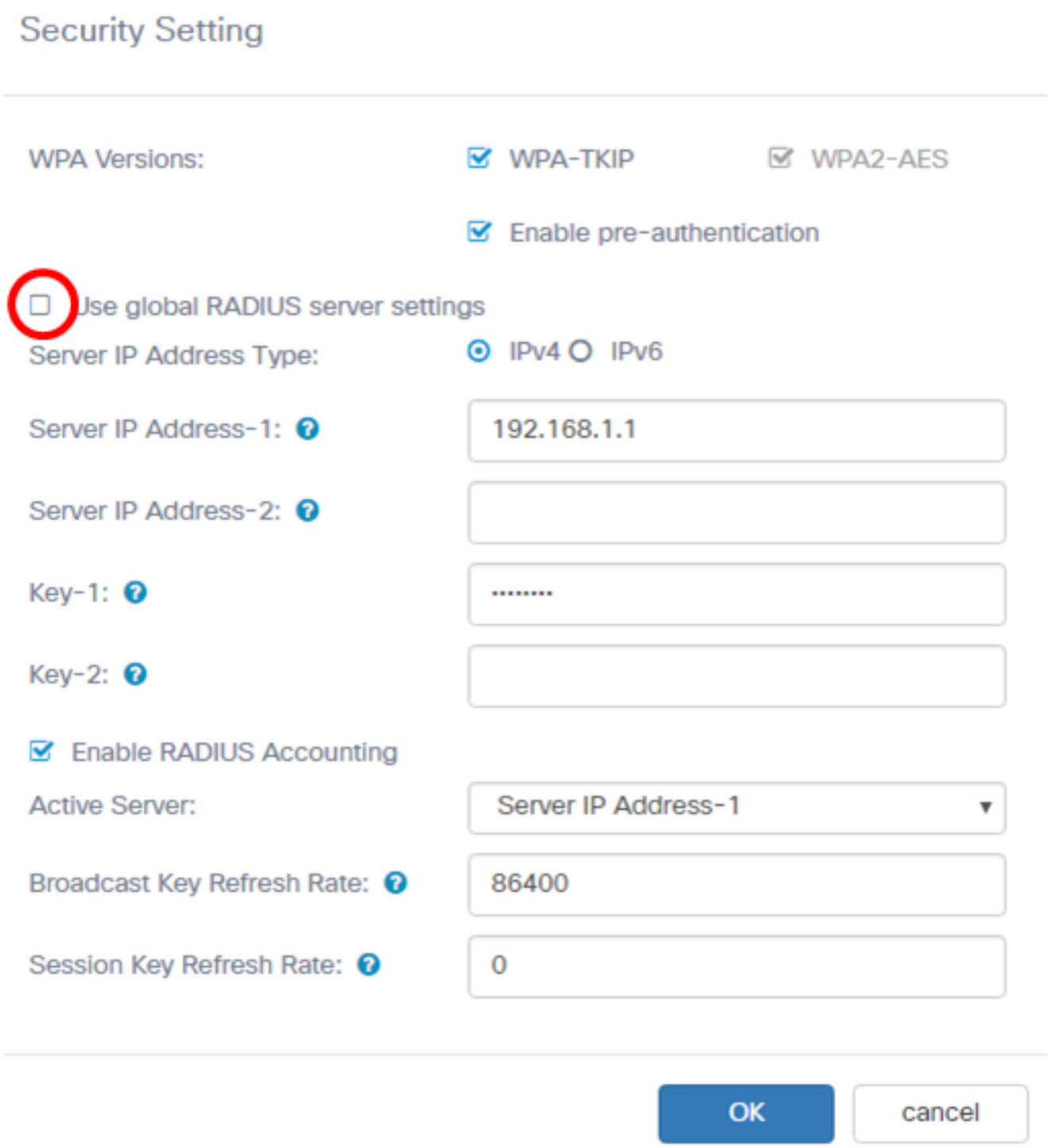


Remarque: Dans cet exemple, WPA-TKIP est vérifié.

Contrôle (facultatif) d'étape 7. la case de pré-**authentification d'enable** pour lancer la caractéristique. Une fois cochées, les informations de pré-authentification sont transmises par relais du WAP que le client sans fil est actuellement connecté à 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. Quand la security mode est désactivée, cette option est également désactivée et ne peut pas être éditée.



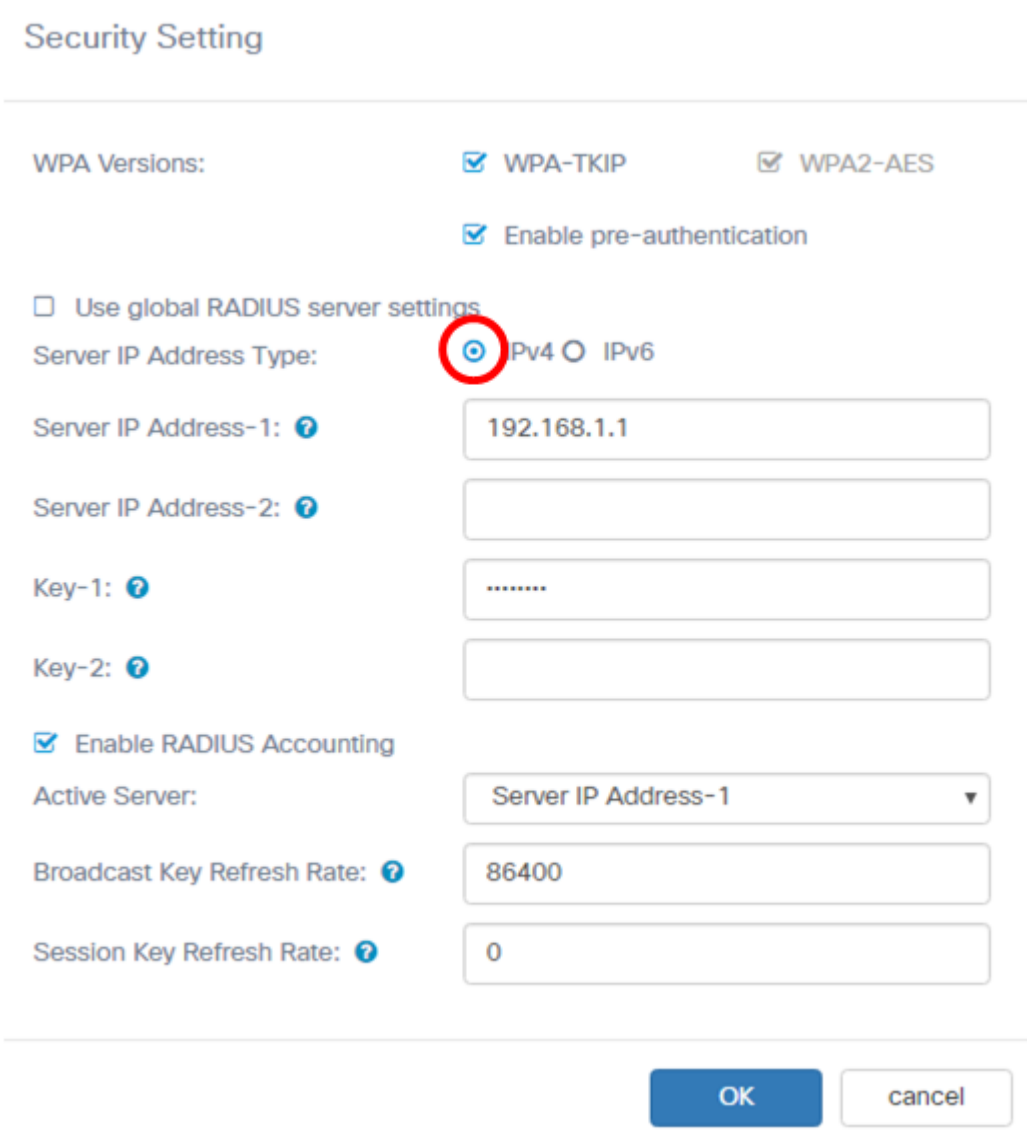
Étape 8. (facultative) décochent la case globale de configurations de serveur de RADIUS d'utilisation pour pouvoir spécifier un ensemble différent de serveurs de RADIUS. Par défaut, chaque VAP utilise les configurations globales de RADIUS définies pour le WAP.



Remarque: Dans cet exemple, utilisez le serveur global de RADIUS que des configurations n'est pas vérifiées. Si ceci est vérifié,

Étape 9. (facultative) choisissent un type d'adresse IP du serveur. Les options sont :

- Ipv4 — Cette option permet le contact WAP le serveur de RADIUS d'ipv4.
- IPv6 — Cette option permet le contact WAP le serveur de RADIUS d'IPv6.



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

Étape 10. (facultative) entrent dans l'adresse IP du serveur primaire de RADIUS pour le VAP dans le domaine de l'*adresse IP du serveur -1*.

Remarque: Dans cet exemple, 192.168.1.1 est entré.

Étape 11. (facultative) entrent dans l'adresse IP du serveur de sauvegarde de RADIUS pour le VAP dans le domaine de l'*adresse IP du serveur -2*.

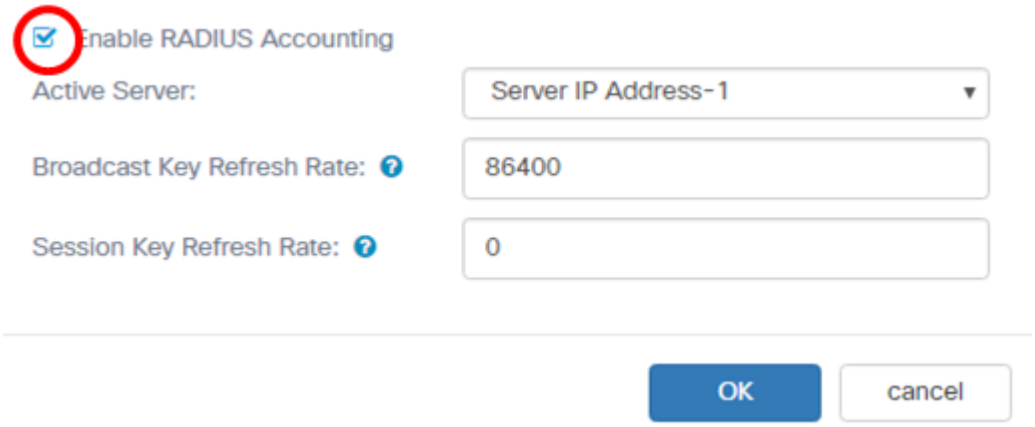
Remarque: Dans cet exemple, aucune adresse IP de sauvegarde n'est écrite.

Étape 12. (Facultatif) entrez un mot de passe pour l'adresse du serveur primaire dans le domaine *Key-1*.

Étape 13. (Facultatif) entrez un mot de passe pour l'adresse du serveur de sauvegarde dans le domaine *Key-2*.

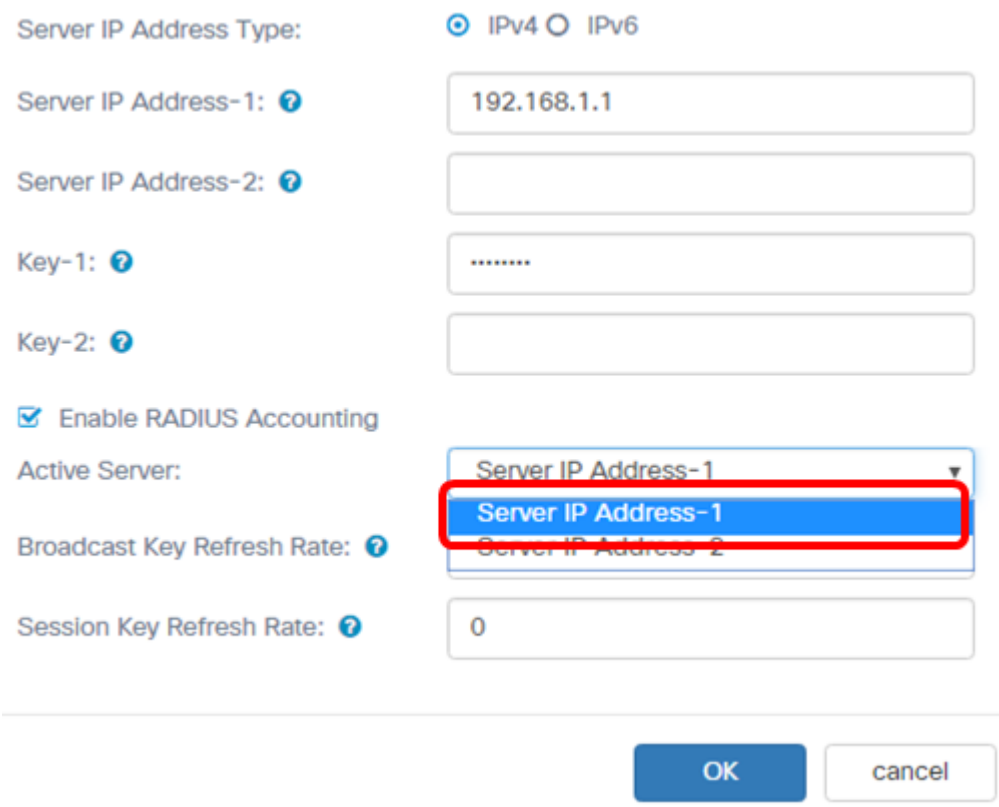
Remarque: Dans cet exemple, aucun mot de passe n'est entré.

Étape 14.(Optional) Cochez la case de **comptabilité de RADIUS d'enable**. Cette option dépiste et mesure les ressources qu'un utilisateur particulier a consommées comme l'heure système et la quantité de données transmises et reçues. Quand activé, il sera activé pour les serveurs primaires et de sauvegarde.



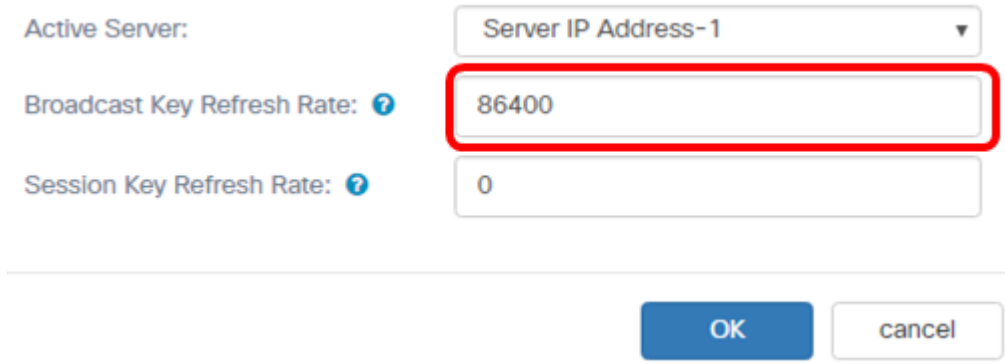
Remarque: Dans cet exemple, la comptabilité de RADIUS d'enable est vérifiée.

Étape 15. (Facultatif) choisissez un serveur actif de la liste déroulante active de serveur.



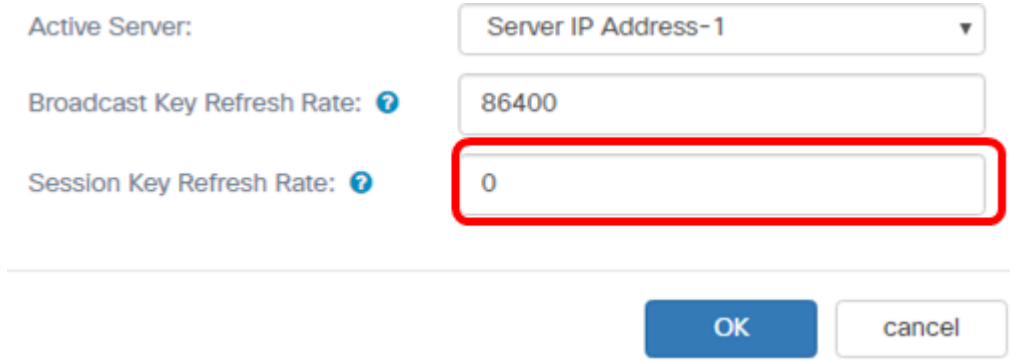
Remarque: Dans cet exemple, IP Address-1 de serveur est choisi.

Étape 16. (Facultatif) écrivez le nombre de secondes jusqu'à ce que votre clé de Sécurité soit remplacée par nouvellement une clé générée dans le domaine de *fréquence d'actualisation de clé d'émission*. La valeur par défaut est 86400.

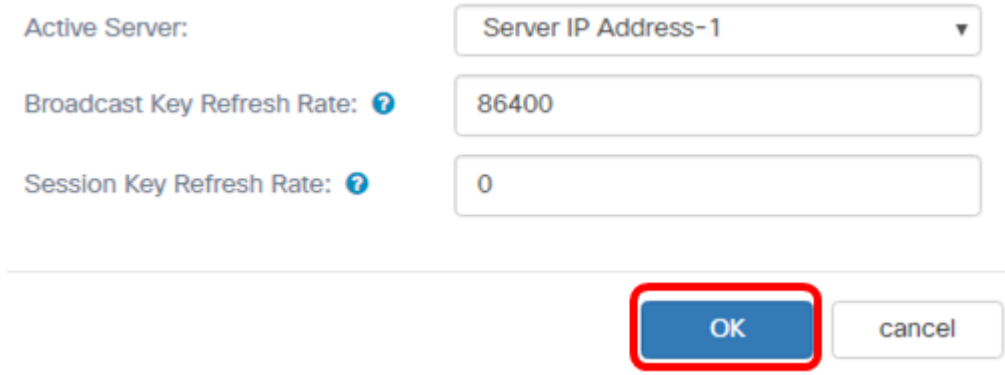


Remarque: Dans cet exemple, la fréquence d'actualisation de clé d'émission est laissée à sa valeur par défaut.

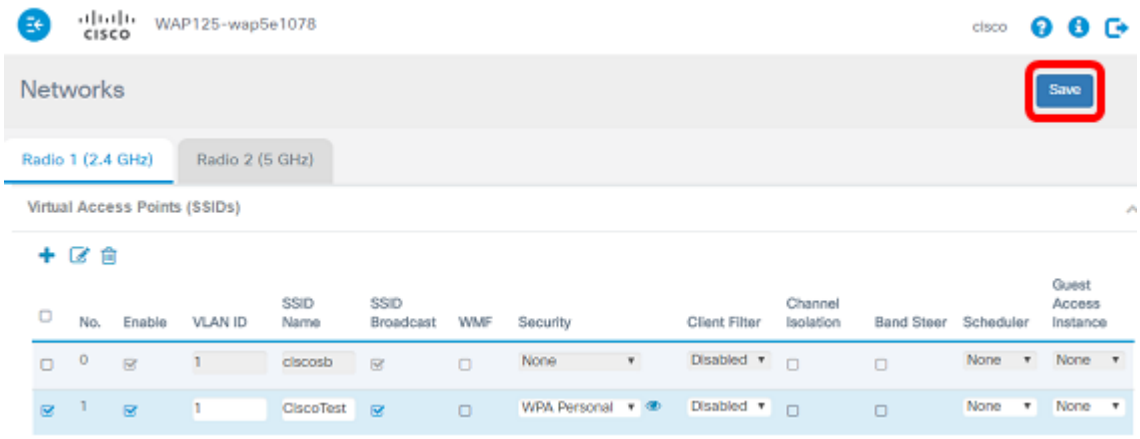
Étape 17. Écrivez l'intervalle auquel le WAP régénère des clés de session pour chaque client associé avec le VAP. Il peut être de 30 à 86400 secondes.



Étape 18. Cliquez sur **OK**.



Étape 19. Cliquez sur **Save**.



Vous devriez maintenant avoir configuré la Sécurité de WPA Enterprise sur votre réseau Sans fil.

Visualisez un vidéo lié à cet article…

A cliquez ici pour visualiser d'autres entretiens de tech de Cisco