Configurer la table d'instance d'accès invité sur le point d'accès WAP125

Objectif

La fonctionnalité d'accès invité du point d'accès WAP125 fournit une connectivité sans fil aux clients sans fil temporaires de la plage du périphérique. Il fonctionne en demandant au point d'accès de diffuser deux SSID différents : l'une pour le réseau principal et l'autre pour le réseau invité. Les invités sont ensuite redirigés vers un portail captif où ils doivent saisir leurs informations d'identification. En effet, cela permettrait de sécuriser le réseau principal tout en donnant aux invités accès à Internet.

Les paramètres du portail captif tels que le délai d'attente de session et l'URL (Uniform Resource Locator) de redirection sont configurés dans la table d'instances d'accès invité de l'utilitaire Web du WAP125. La fonction d'accès invité a été particulièrement utile dans les halls d'hôtels et de bureaux, les restaurants et les centres commerciaux.

Cet article vise à vous montrer comment configurer la table d'instance d'accès invité du point d'accès WAP125. Il suppose que les paramètres de la table des paramètres régionaux du portail Web et de la table des groupes d'invités sont déjà configurés. Pour obtenir des instructions sur la configuration de ces deux paramètres, cliquez ici.

Périphériques pertinents

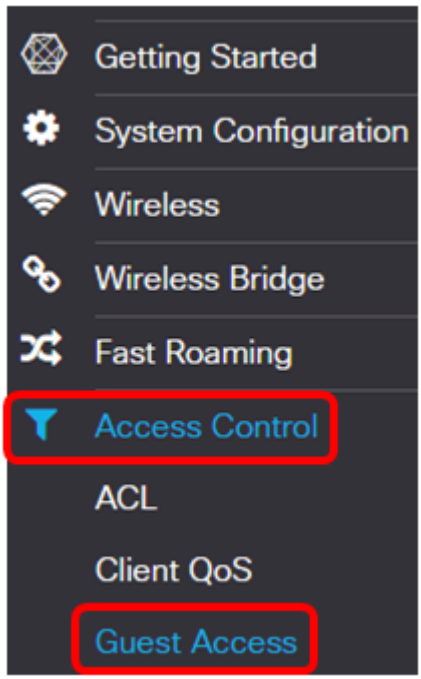
- WAP125

Version du logiciel

- 1.0.0.4 : WAP581
- 1.0.0.5 : WAP125

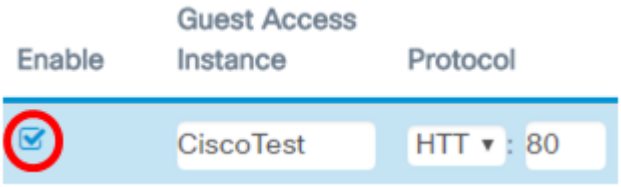
Configurer la table d'instances d'accès invité

Étape 1. Connectez-vous à l'utilitaire Web du WAP125 et choisissez **Access Control > Guest Access**.

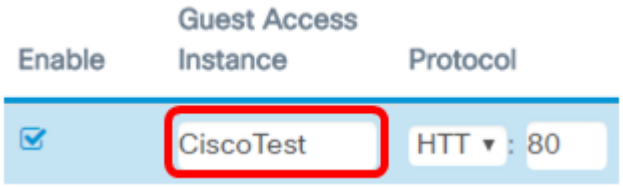


Note: Les images de cet article proviennent du WAP125. Les options de menu peuvent varier en fonction du modèle de votre périphérique.

Étape 2. Vérifiez que la case à cocher **Activer** l'instance d'accès invité est activée pour vous assurer que l'accès invité est actif.



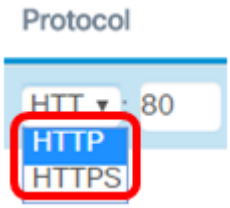
Étape 3. Entrez un nom pour l'instance dans le champ *Instance d'accès invité*. Il peut contenir jusqu'à 32 caractères alphanumériques.



Note: Dans cet exemple, CiscoTest est entré.

Étape 4. Sélectionnez un protocole pour l'instance d'accès invité. Les options sont les suivantes :

- HTTP : cette option est également appelée HTTP (HyperText Transfer Protocol). Il ne fournit pas de chiffrement lors de la vérification de la page Web demandée.
- HTTPS : cette option est également appelée HyperText Transfer Protocol Secure (HTTPS). Cela signifie que toutes les communications entre l'ordinateur et le site Web qu'il contacte sont chiffrées.



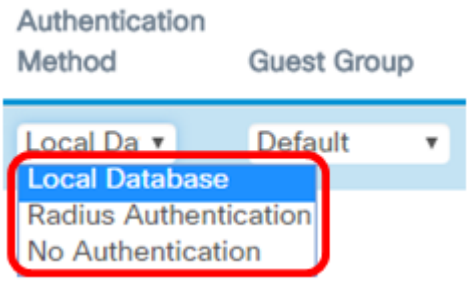
Note: Dans cet exemple, HTTP est choisi.

Étape 5. Entrez un numéro de port en regard du champ Protocol. Le numéro de port permet d'identifier le protocole lorsqu'il atteint un serveur.

Note: Dans cet exemple, 80 est entré.

Étape 6. Choisissez une méthode d'authentification dans la liste déroulante Authentication Method. Ce paramètre sera utilisé par le point d'accès lorsque les clients s'authentifient via le portail captif. Les options sont les suivantes :

- Local Database : cette option permet au périphérique WAP de vérifier les informations d'identification de l'utilisateur à partir d'un fichier stocké localement. Si cette option est sélectionnée, passez aux étapes 7 à 10, puis configurez la table de groupe d'invités.
- RADIUS Authentication : cette option permet au point d'accès de vérifier les utilisateurs via un serveur RADIUS (Remote Authentication Dial-In User Service). Si cette option est sélectionnée, passez aux étapes 7 à 10, puis passez à la configuration de l'authentification RADIUS.
- No Authentication : cette option désactive l'authentification et permet aux clients sans fil de se connecter au réseau invité sans entrer leurs informations d'identification. Si cette option est sélectionnée, passez à l'étape 11.

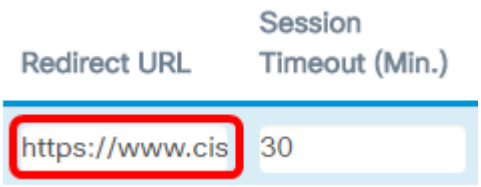


Note: Dans cet exemple, la base de données locale est sélectionnée.

Étape 7. Sélectionnez un groupe dans la liste déroulante Groupe d'invités.

Note: Dans cet exemple, Default est automatiquement sélectionné.

Étape 8. Entrez l'adresse à rediriger après avoir saisi les informations d'identification dans le champ *URL de redirection*.

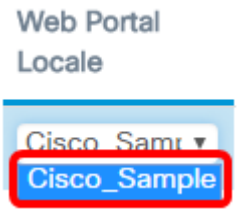


Note: L'adresse doit commencer par HTTP ou HTTPS. Dans cet exemple, https://www.cisco.com est entré.

Étape 9. Entrez le nombre de minutes avant l'expiration d'une session dans le champ *Délai d'expiration de session (min.)*.

Note: Dans cet exemple, 30 est entré.

Étape 10. Sélectionnez un profil de portail Web dans la liste déroulante Paramètres régionaux du portail Web.



Note: Dans cet exemple, Cisco_Sample est sélectionné automatiquement. Pour obtenir des instructions sur la configuration des paramètres régionaux du portail Web, cliquez ici.

La table d'instances d'accès invité doit maintenant être configurée.

Configurer la table de groupe d'invités

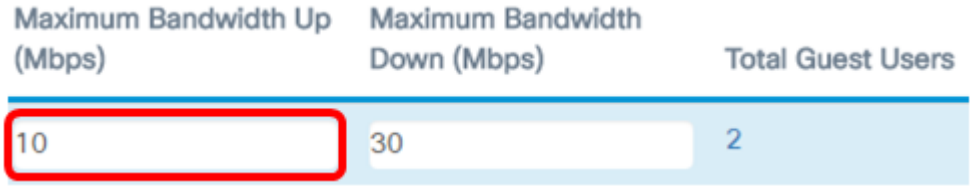
Étape 7. Entrez un nom pour le groupe invité dans le champ *Nom du groupe invité*. Le nom du groupe d'invités peut comporter jusqu'à 32 caractères.

Note: Dans cet exemple, CiscoInvités est saisi.

Étape 8. Saisissez le nombre de minutes avant l'expiration de l'invite dans le champ *Délai d'inactivité (min.)*.

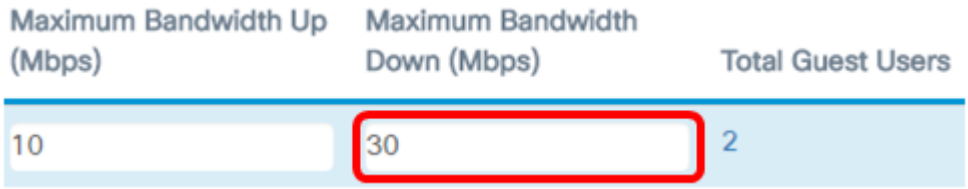
Note: Dans cet exemple, 5 est entré.

Étape 9. Entrez la vitesse de chargement maximale dans le champ *Bande passante maximale ascendante (Mbits/s)*. Il s'agit de la bande passante maximale, en Mbits/s, qu'un client sans fil peut envoyer lors de l'utilisation du portail captif. La bande passante maximale peut être comprise entre 0 et 300, où 0 est la valeur par défaut.



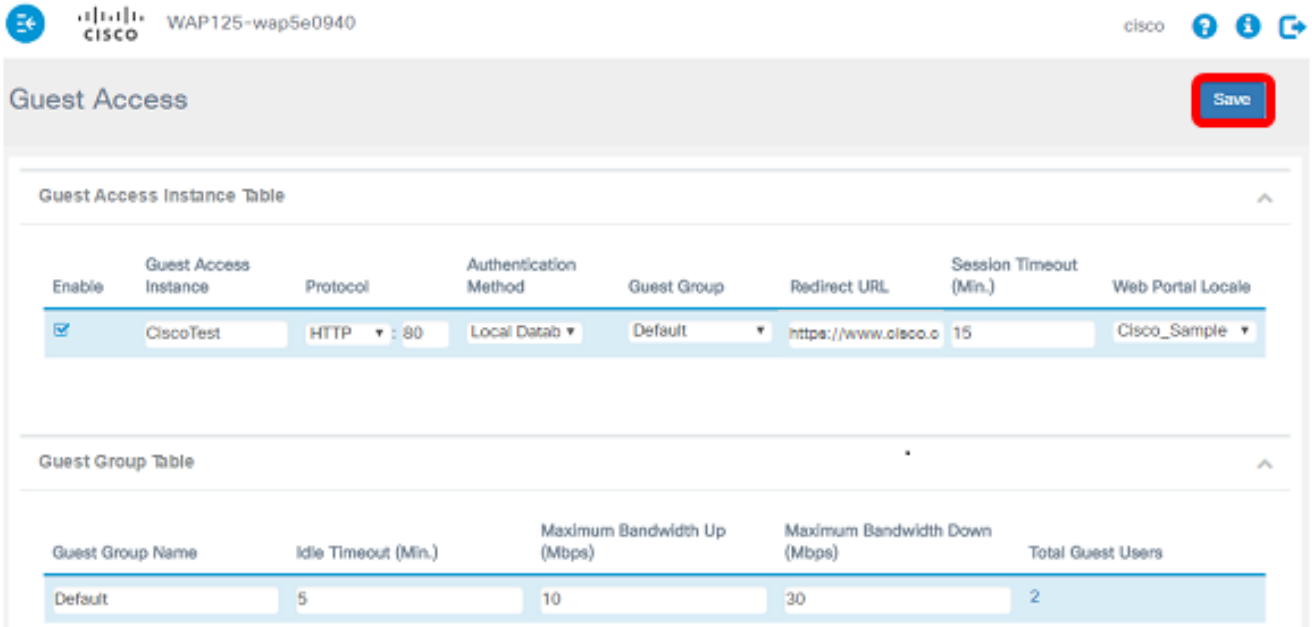
Note: Dans cet exemple, 10 est entré.

Étape 10. Entrez la vitesse de téléchargement maximale dans le champ *Bande passante maximale descendante (Mbits/s)*. Il s'agit de la bande passante maximale, en Mbits/s, qu'un client sans fil peut recevoir lors de l'utilisation du portail captif. La bande passante maximale peut être comprise entre 0 et 300, où 0 est la valeur par défaut.



Note: Dans cet exemple, 30 est entré.

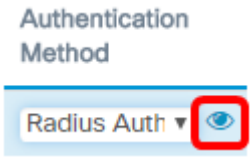
Étape 11. Click **Save**.



La table d'instance d'accès invité doit maintenant être configurée avec l'authentification de base de données locale.

Authentification RADIUS

Étape 1. Cliquez sur le bouton View (Afficher).

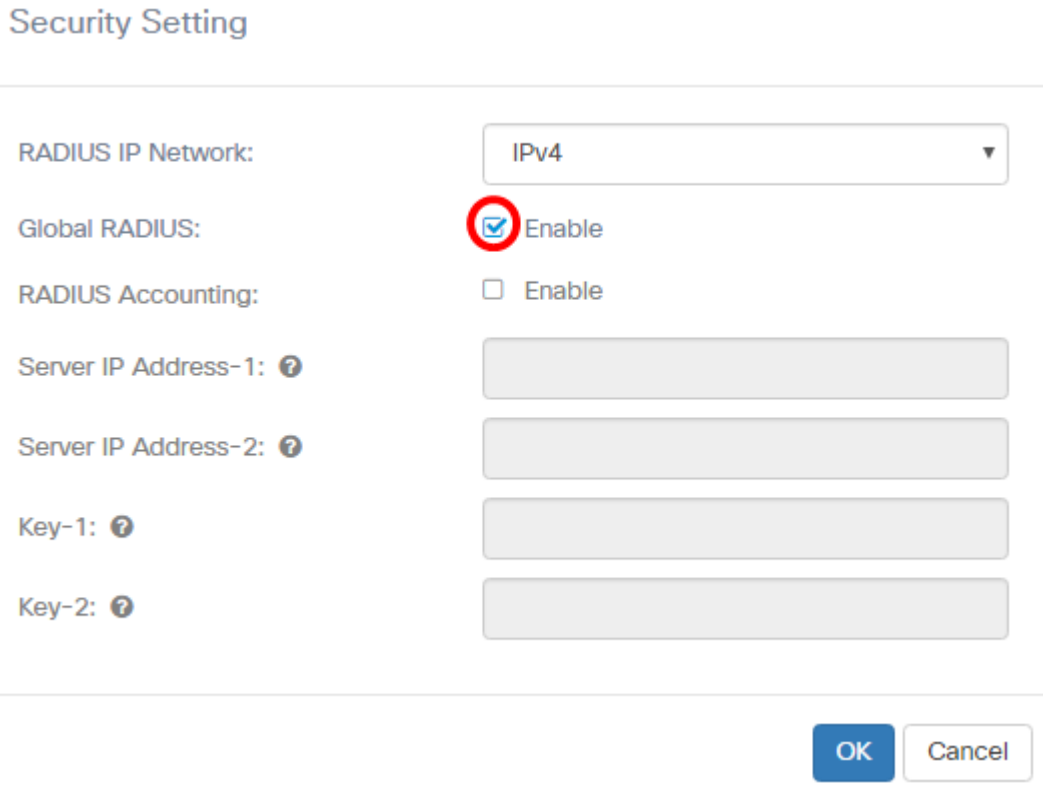


Étape 2. Dans la fenêtre contextuelle Security Setting, sélectionnez le réseau IP radius dans la liste déroulante RADIUS IP Network. Les options sont les suivantes :

- IPv4 : cette option est la forme d'adressage IP la plus couramment utilisée sur un réseau. Il utilise un format 32 bits pour identifier les hôtes sur un réseau.
- IPv6 : cette option est la norme d'adresse IP de nouvelle génération destinée à remplacer le format IPv4. IPv6 résout le problème de pénurie d'adresses en utilisant un système d'adressage 128 bits au lieu du 32 bits utilisé dans IPv4.

Note: Dans cet exemple, IPv4 est choisi.

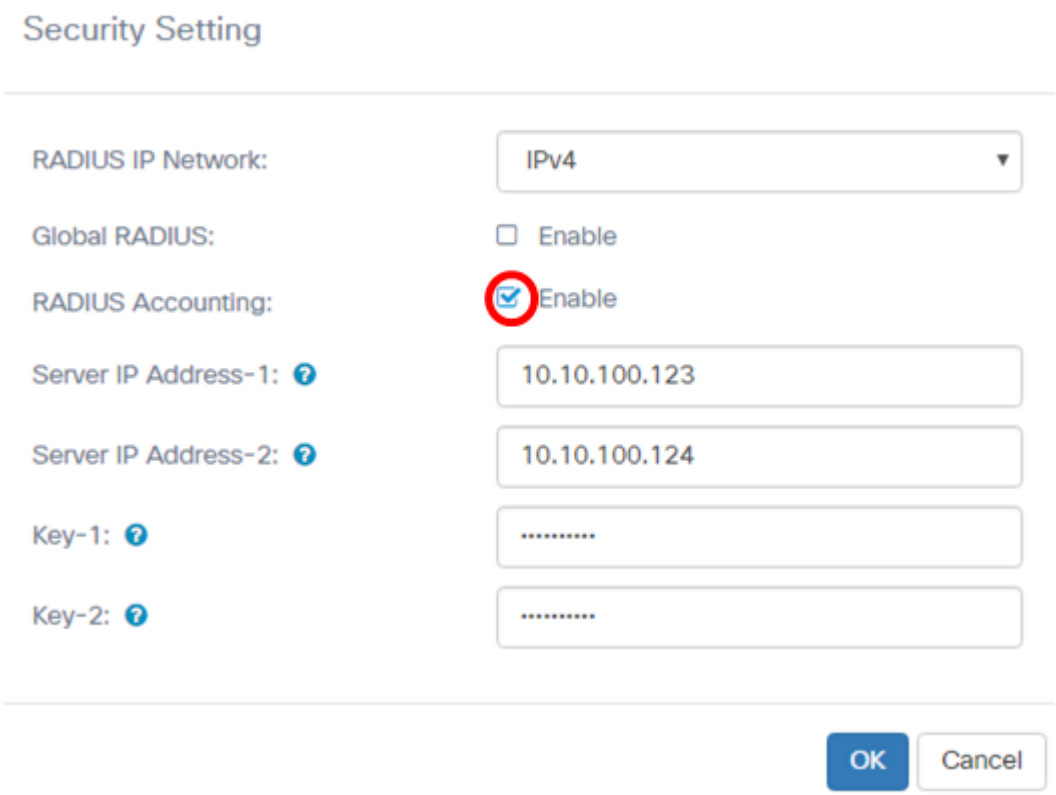
Étape 3. (Facultatif) Cochez la case **Activer** RADIUS global pour permettre au portail captif d'utiliser un autre ensemble de serveurs RADIUS.



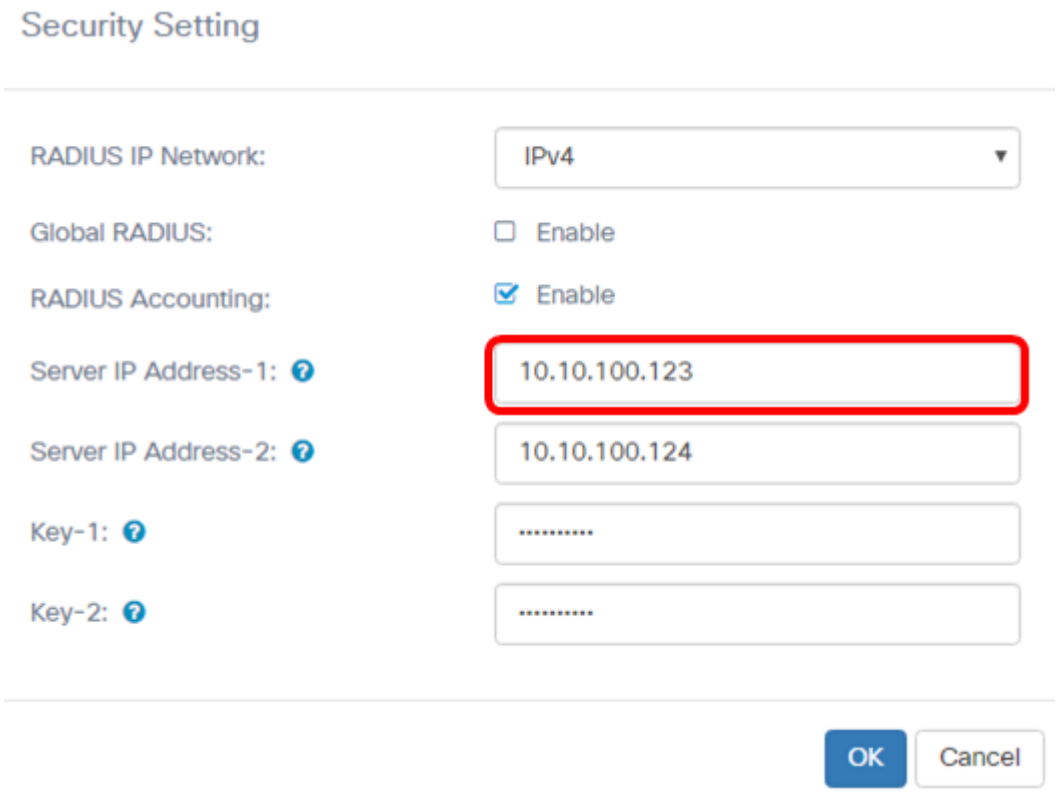
Note: Lorsqu'elle est activée, aucune autre configuration de la zone Paramètres de sécurité

n'a besoin d'être configurée. Passez à l'étape 9. Dans cet exemple, Global RADIUS est activé.

Étape 4. (Facultatif) Cochez la case **Activer** la comptabilité RADIUS pour permettre au point d'accès de suivre et de mesurer les ressources qu'un utilisateur particulier a consommées, telles que le temps système et la quantité de données transmises et reçues.

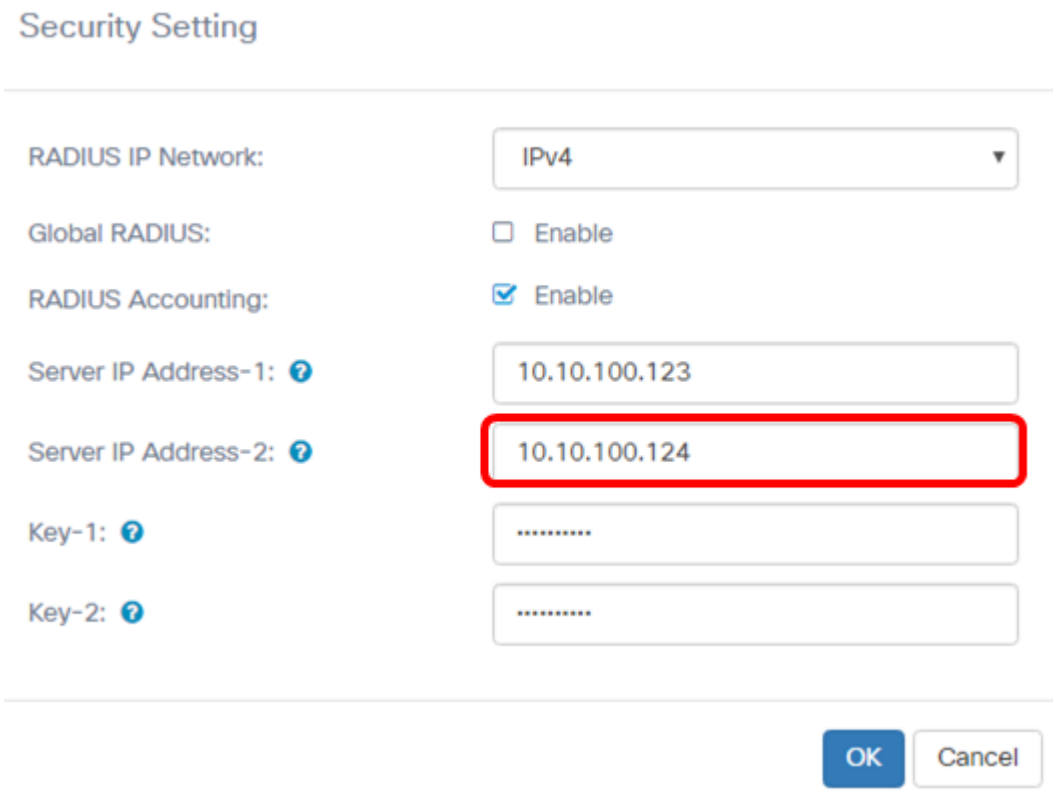


Étape 5. (Facultatif) Entrez l'adresse IPv4 ou IPv6 du serveur RADIUS principal dans le champ *Server IP Address-1*.



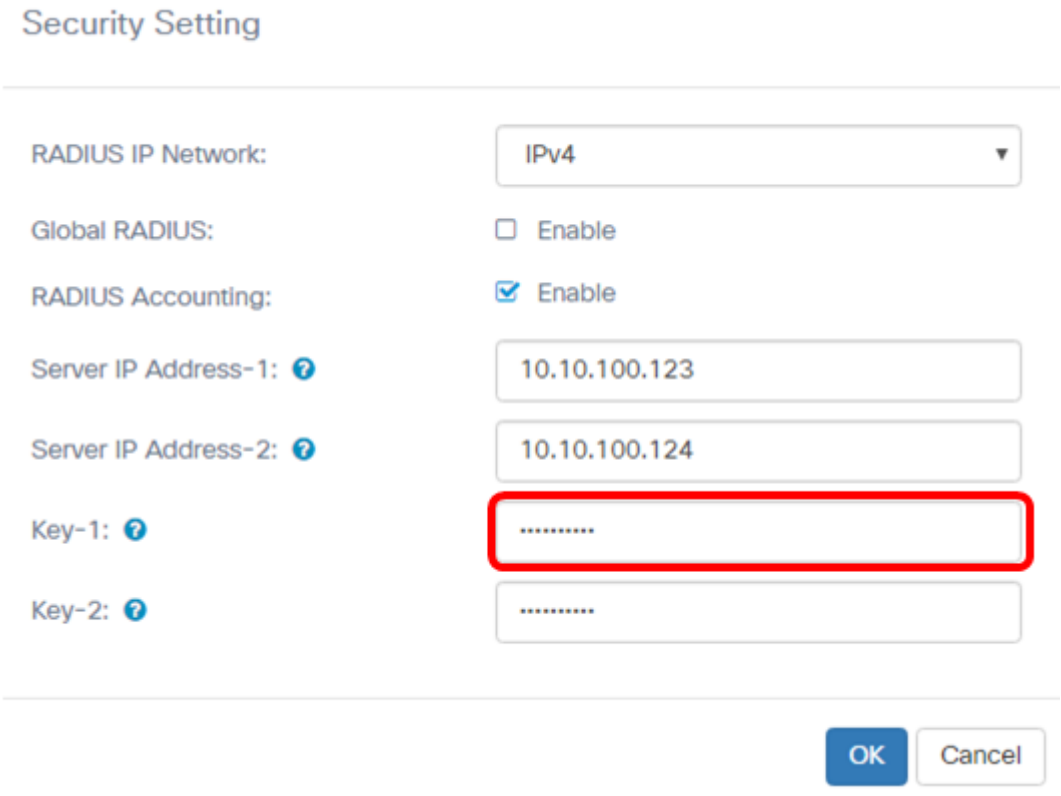
Note: Dans cet exemple, 10.10.100.123 est entré.

Étape 6. (Facultatif) Entrez l'adresse IPv4 ou IPv6 du serveur RADIUS de sauvegarde dans le champ *Server IP Address-2*.



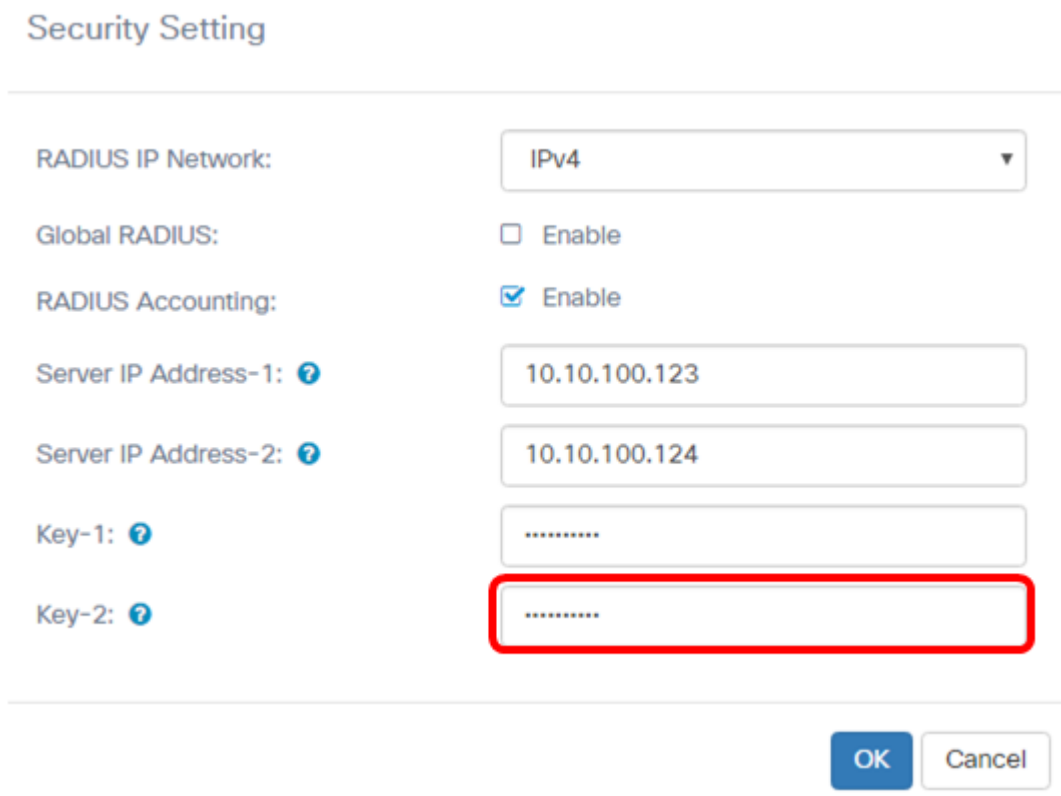
Note: Dans cet exemple, 10.10.100.124 est entré.

Étape 7. (Facultatif) Entrez le mot de passe utilisé par le point d'accès pour authentifier le serveur RADIUS principal dans le champ *Key-1*. L'entrée de ce champ est sensible à la casse et doit correspondre à l'entrée configurée sur le serveur RADIUS principal. La clé peut comporter jusqu'à 63 caractères alphanumériques.

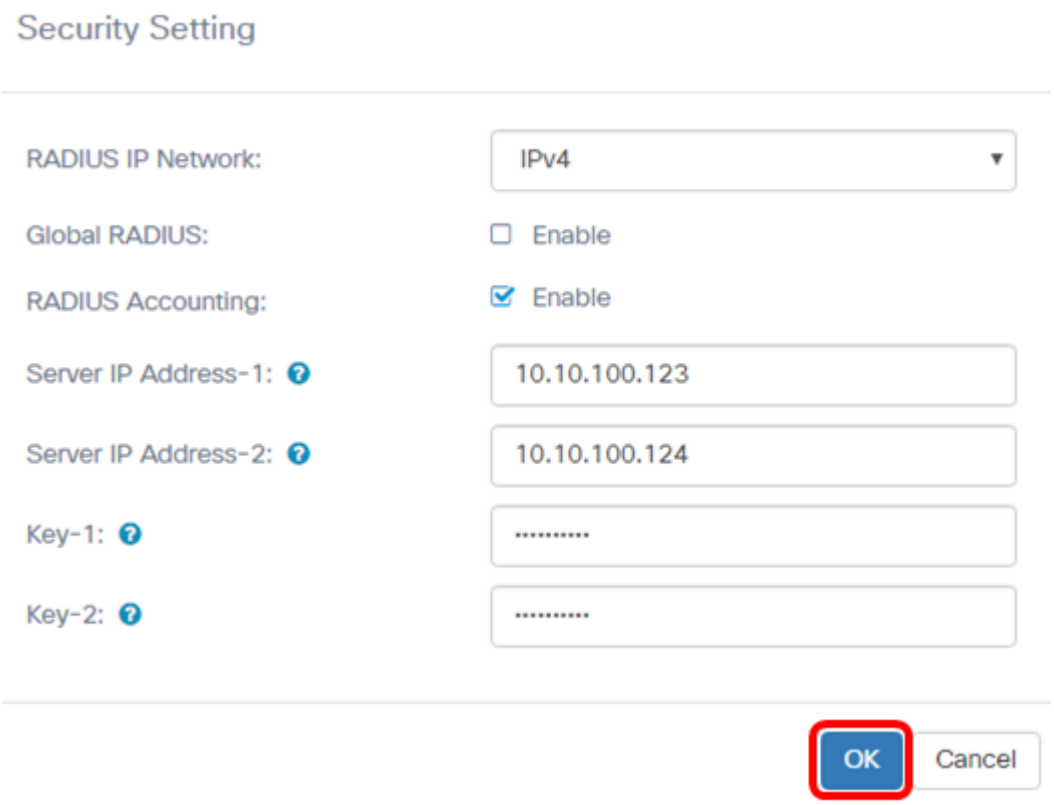


Étape 8. (Facultatif) Entrez le mot de passe utilisé par le point d'accès pour authentifier le

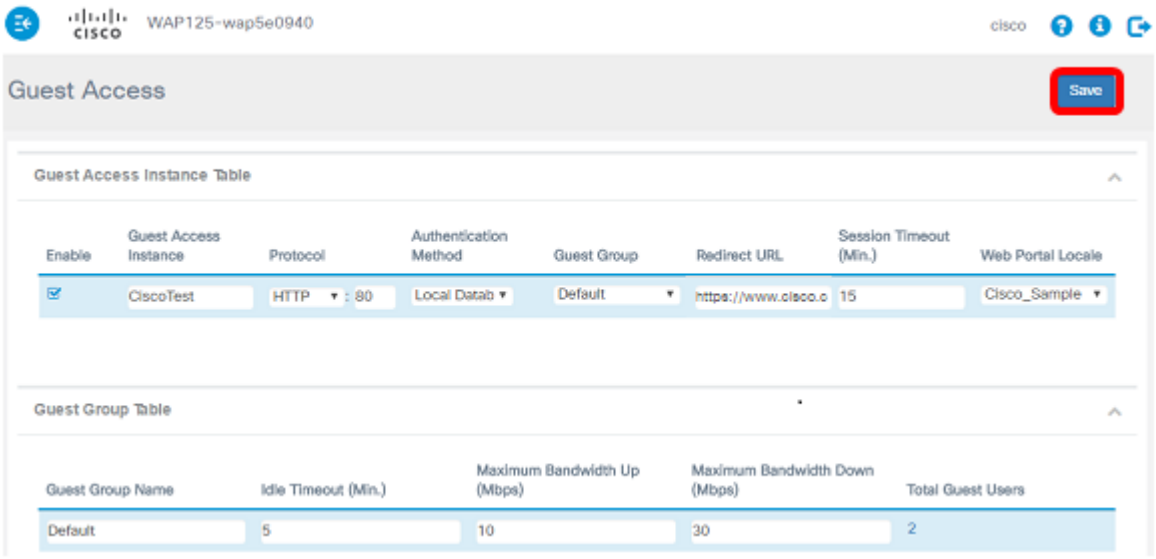
serveur RADIUS secondaire dans le champ *Key-2*. L'entrée de ce champ est sensible à la casse et doit correspondre à l'entrée configurée sur le serveur RADIUS principal. La clé peut comporter jusqu'à 63 caractères alphanumériques.



Étape 9. Click OK.



Étape 10. Click **Save**.



La table Instance d'accès invité doit maintenant être configurée avec la méthode d'authentification RADIUS.