# Configuration d'instance de portail captif sur le point d'accès WAP321

## Objectif

Le portail captif vous permet de bloquer les clients connectés au réseau WAP. Les clients consultent une page Web spéciale à des fins d'authentification avant d'être autorisés à utiliser Internet normalement. La vérification du portail captif est destinée aux invités et aux utilisateurs authentifiés, et utilise le navigateur Web en le transformant en périphérique d'authentification. Les instances de portail captif sont un ensemble défini de configurations qui sont utilisées pour authentifier les clients sur le réseau WAP. Différentes instances (maximum deux) peuvent être configurées pour répondre différemment aux utilisateurs lorsqu'ils tentent d'accéder au point d'accès virtuel associé. Les portails captifs sont utilisés dans de nombreux points d'accès Wi-Fi pour charger les utilisateurs d'accéder à Internet.

Ce document explique comment configurer la configuration globale du portail captif sur le point d'accès WAP321.

## Périphériques pertinents

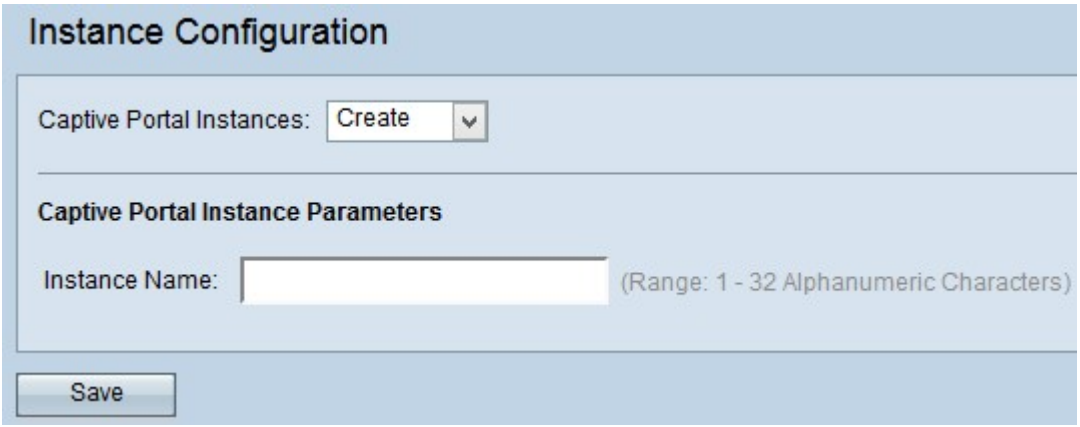
·WAP321

## Version du logiciel

•1.0.3.4

## Configuration d'instance de portail captif

Étape 1. Connectez-vous à l'utilitaire de configuration Web et choisissez **Captive Portal > Instance Configuration**. La page *Configuration de l'instance* s'ouvre :




Étape 2. Choisissez **Créer** dans la liste déroulante Instances du portail captif si vous voulez créer une nouvelle configuration. Pour modifier la configuration actuelle, sélectionnez l'instance actuelle dans la liste déroulante et passez à l'étape 5.

**Note**: Vous pouvez créer jusqu'à deux configurations.

Étape 3. Entrez un nom pour la configuration dans le champ Nom de l'instance. La plage est

comprise entre 1 et 32 caractères alphanumériques.


Étape 4. Cliquez sur **Enregistrer** pour enregistrer les modifications apportées. La page s'affiche à nouveau avec des champs supplémentaires pour la configuration de l'instance.

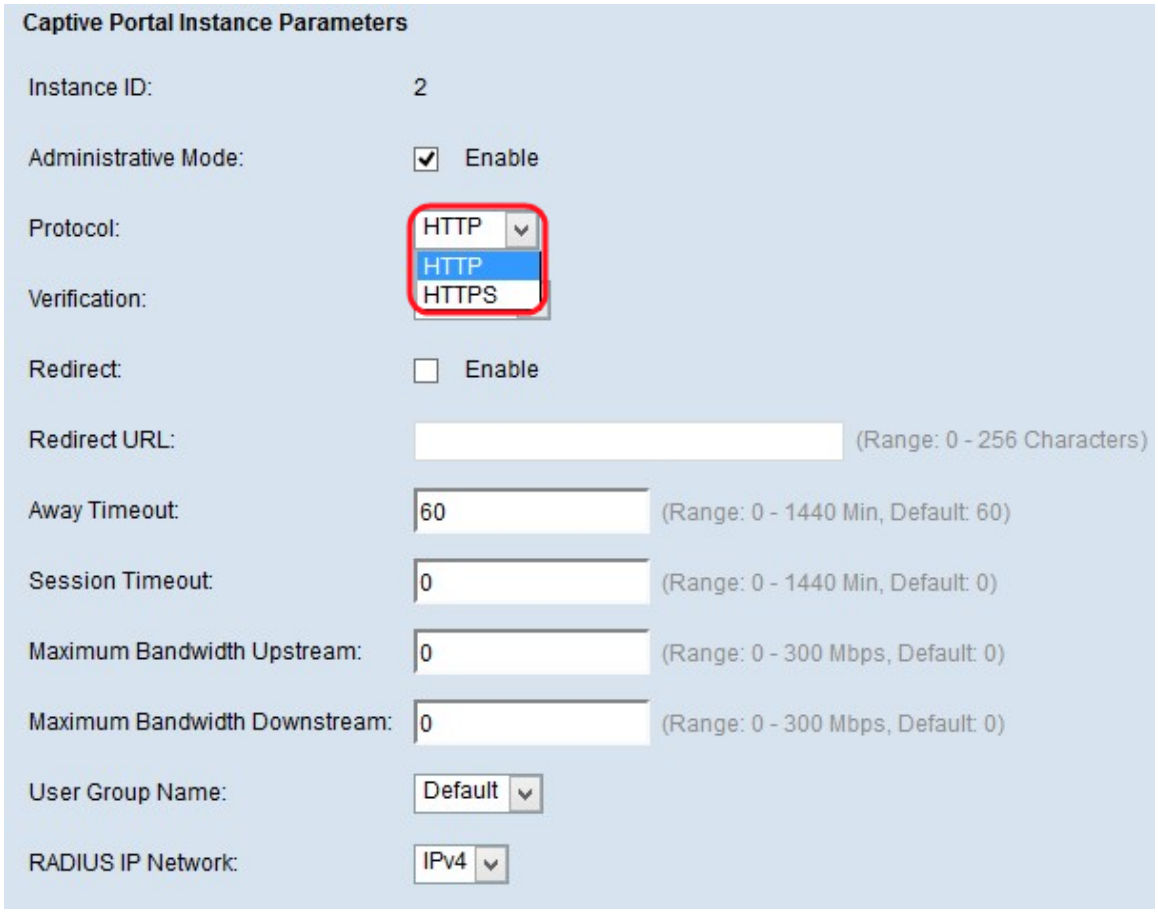

La page *Configuration de l'instance* comporte des champs non configurables qui affichent les informations suivantes :

·Instance ID : spécifie le numéro de rang de l'instance CP actuellement configurée sur le périphérique WAP.

·Nombre de paramètres régionaux : spécifie le nombre de paramètres régionaux (jeu de

paramètres de langue et de pays spécifiques des préférences utilisateur) associés à l'instance.

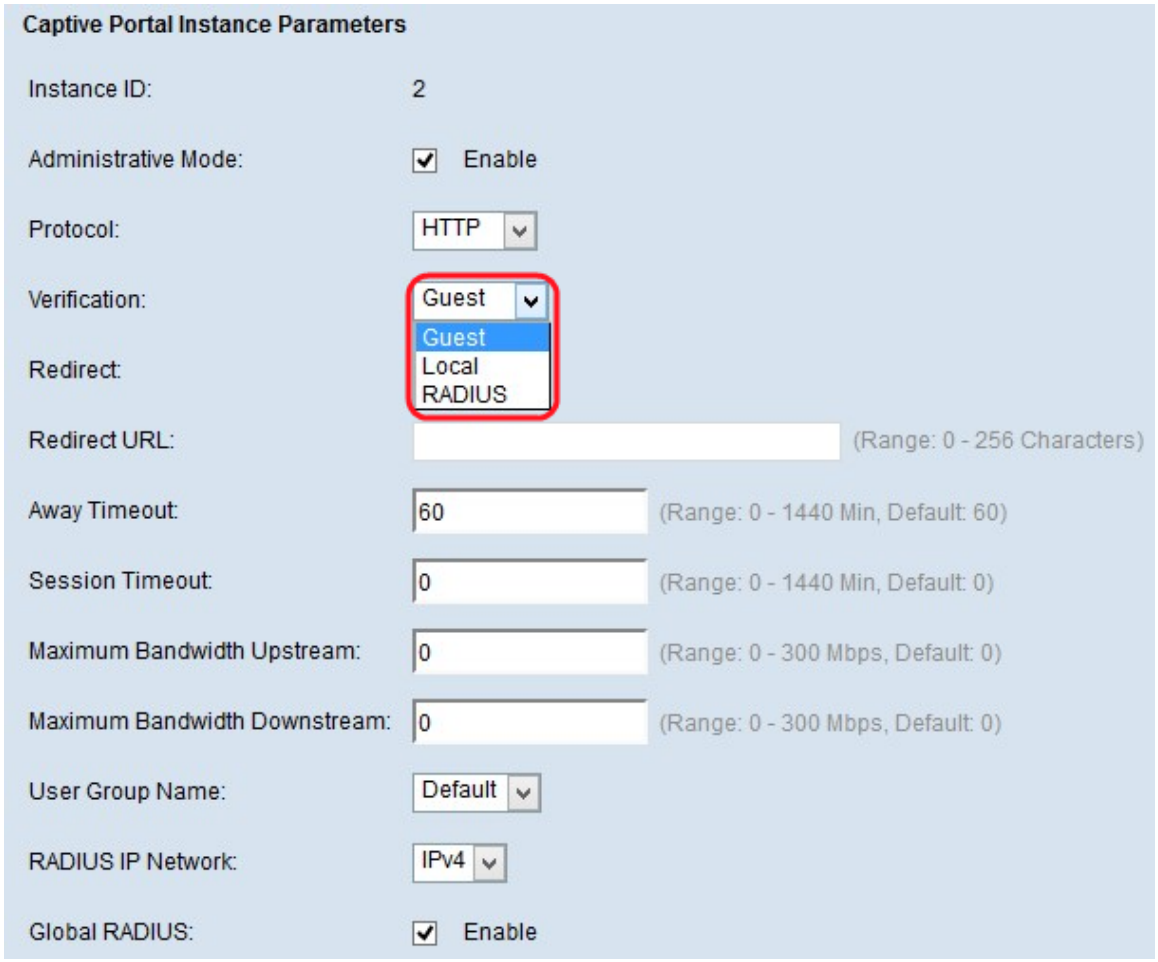
Étape 5. Cochez la case **Enable** pour activer l'instance CP dans le champ Administrative Mode.




Étape 6. Sélectionnez le protocole que l'instance CP doit utiliser pour vérification dans le champ Protocol. Les valeurs possibles sont les suivantes :

·HTTP : ne chiffre pas les informations pour le processus de vérification.

·HTTPS : utilise le protocole SSL (Secure Sockets Layer), qui nécessite un certificat pour fournir le chiffrement utilisé dans le processus d'authentification.

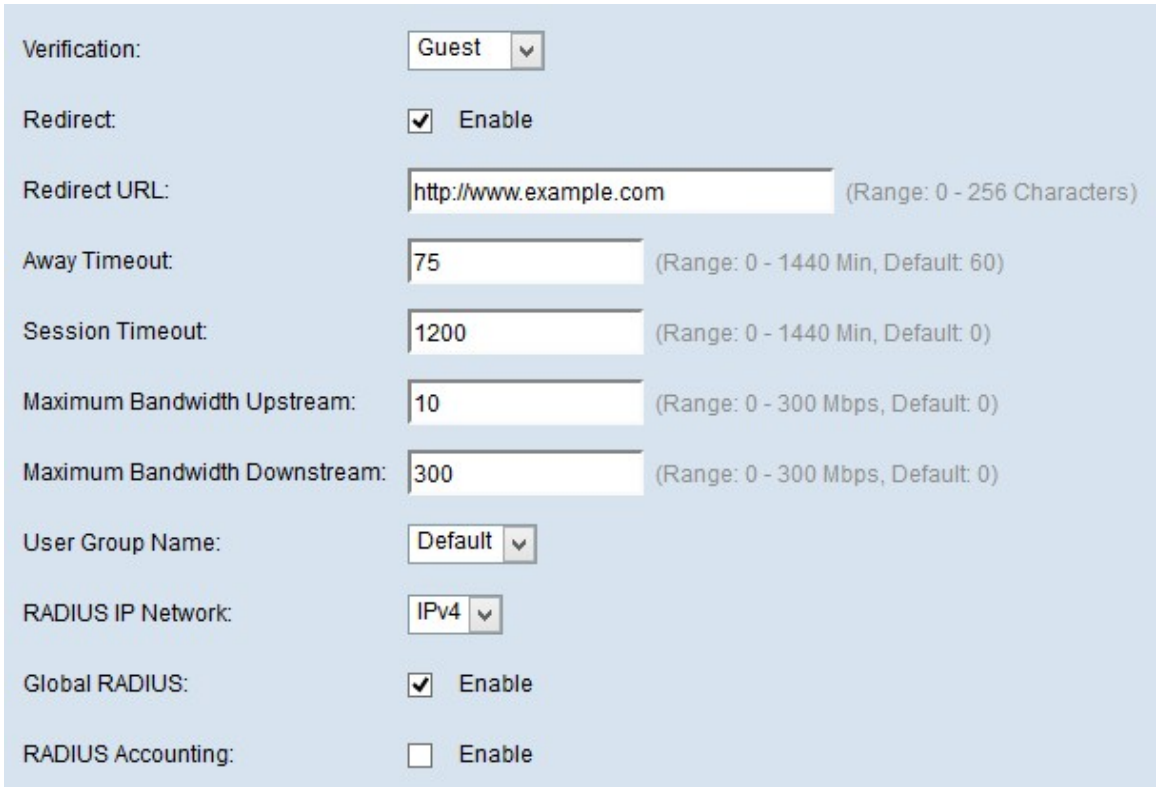



Étape 7. Choisissez la méthode d'authentification que le PC doit utiliser pour la vérification dans la liste déroulante Vérification. Les méthodes d'authentification sont utilisées pour refuser l'accès des utilisateurs malveillants au périphérique. La méthode d'authentification choisie est utilisée pour vérifier les clients. Les valeurs possibles sont les suivantes :

·Guest : n'utilise aucune authentification.

·Local : utilise une base de données locale pour l'authentification.

·RADIUS : utilise une base de données serveur RADIUS distante pour l'authentification.




Étape 8. Cochez la case **Activer** dans le champ Redirection si vous voulez rediriger le client nouvellement authentifié vers une URL configurée.

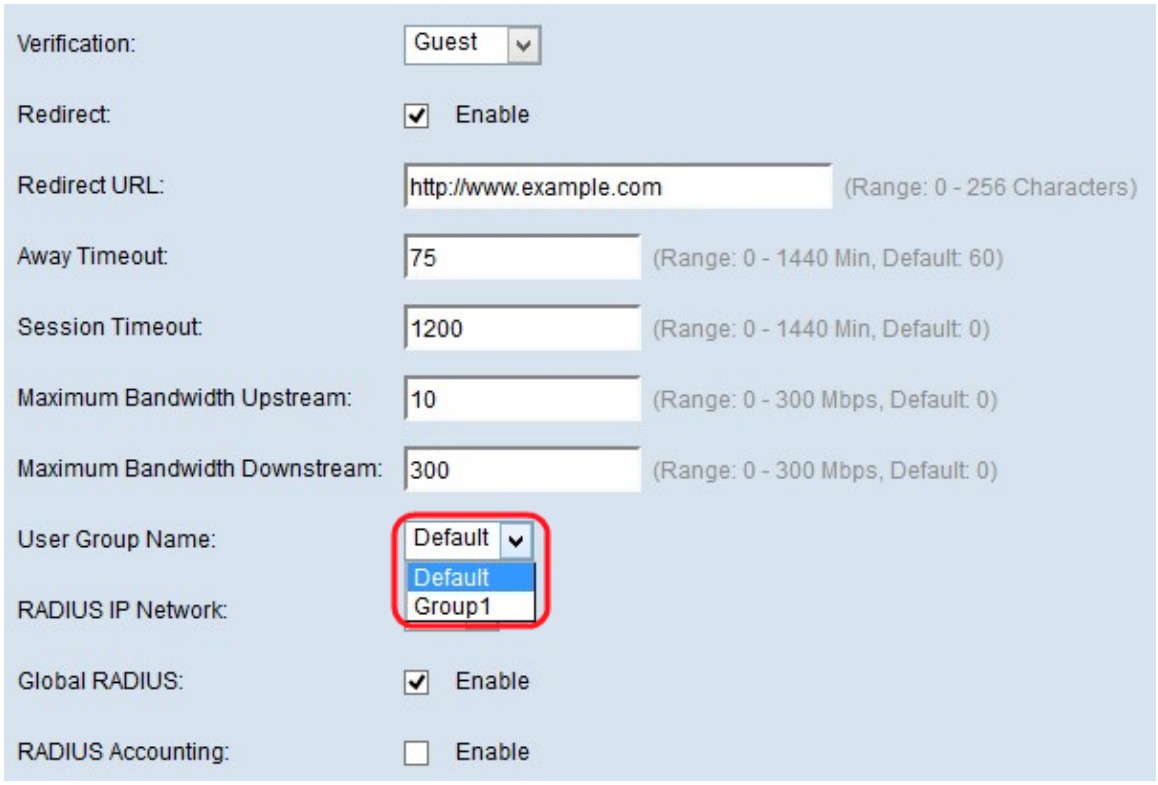
Étape 9. Entrez l'URL avec le préfixe "http://" vers lequel le client nouvellement authentifié sera redirigé dans le champ Redirect URL. La plage est comprise entre 0 et 256 caractères.

Étape 10. Saisissez la durée pendant laquelle un utilisateur peut rester inactif avant d'être automatiquement déconnecté dans le champ Away Timeout. Si la valeur est définie sur 0, le délai d'attente n'est pas appliqué. La plage est comprise entre 0 et 1 440 minutes. La valeur par défaut est 60 minutes.

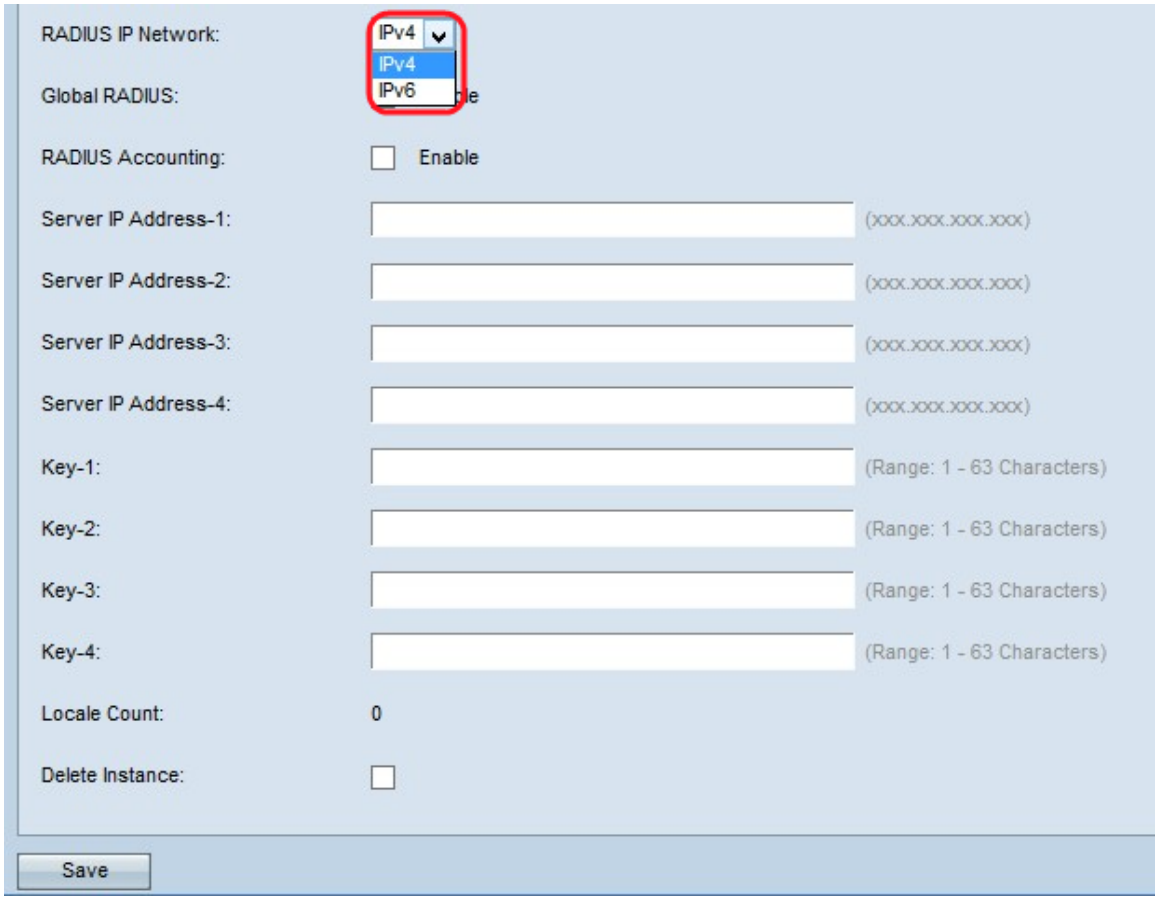
Étape 11. Saisissez le délai d'attente avant la fin de la session dans le champ Session Timeout. La plage est comprise entre 0 et 1 440 minutes. La valeur par défaut est 0, ce qui signifie que le délai d'attente n'est pas appliqué.

Étape 12. Saisissez la vitesse de téléchargement maximale qu'un client peut envoyer des données via le portail captif dans le champ Maximum Bandwidth Upstream. La plage est comprise entre 0 et 300 Mbits/s. La valeur par défaut est 0.

Étape 13. Saisissez la vitesse de téléchargement maximale à laquelle un client peut recevoir des données via le portail captif dans le champ Maximum Bandwidth Downstream. La plage est comprise entre 0 et 300 Mbits/s. La valeur par défaut est 0.




Étape 14. Choisissez le groupe souhaité dans le champ Nom du groupe d'utilisateurs que vous souhaitez affecter à l'instance CP dans la liste déroulante des groupes préconfigurés.

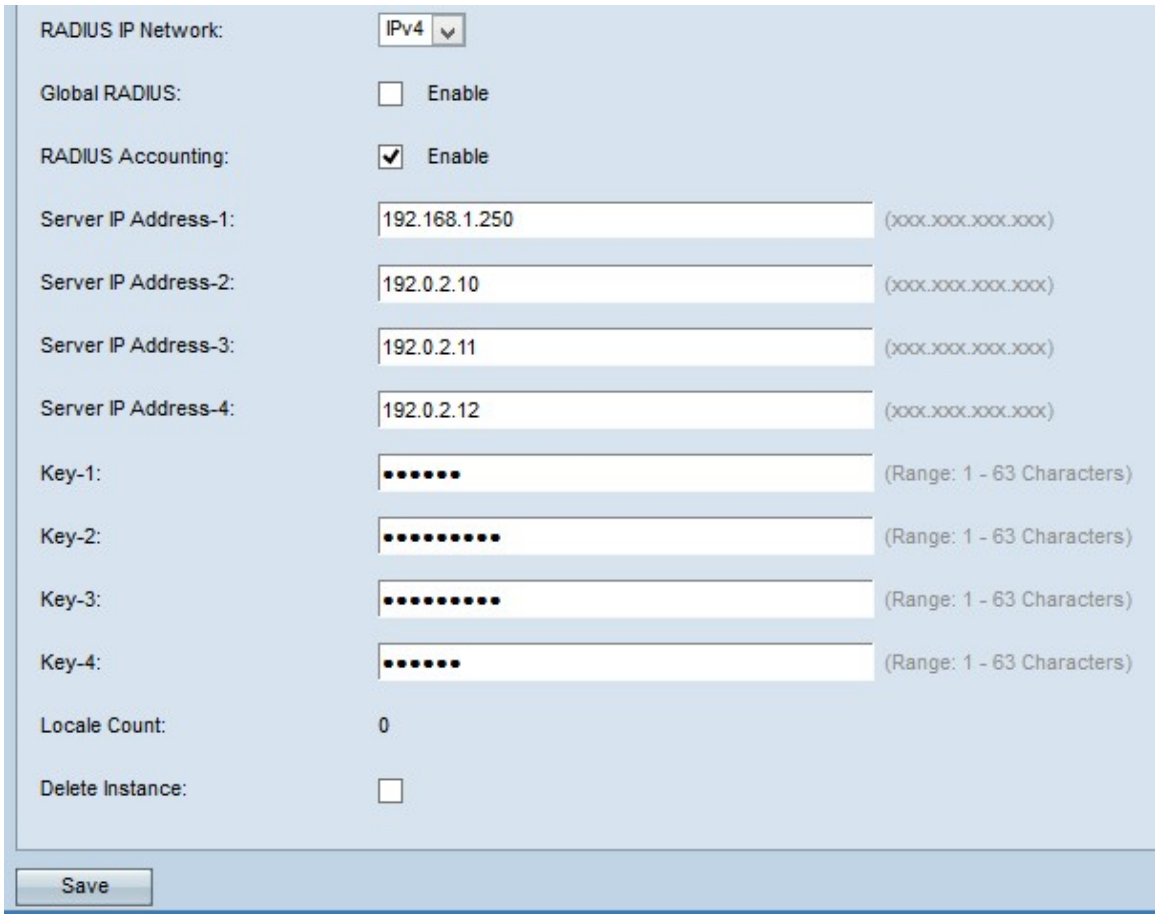



Étape 15. Sélectionnez le type de protocole Internet dans le champ RADIUS IP Network (Réseau IP RADIUS), qui sera utilisé par l'instance CP dans la liste déroulante RADIUS IP network (Réseau IP RADIUS). Les valeurs possibles sont les suivantes :

·IPv4 : l'adresse du client RADIUS se trouve dans la quatrième version d'IP avec le format

d'adresse xxx.xxx.xxx.xxx (192.0.2.10).

·IPv6 — L'adresse du client RADIUS se trouve dans la sixième version de l'adresse IP au format xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (2001:DB8::CAD5:7D91).




Étape 16. Cochez la case **Activer** dans le champ RADIUS global si vous voulez utiliser la liste de serveurs RADIUS globaux pour l'authentification.

**Économiseur de temps :** Passez à l'étape 22 si vous choisissez RADIUS global. Vous n'avez pas besoin d'entrer l'adresse IP du serveur RADIUS si vous avez activé l'option RADIUS global, car la fonctionnalité CP utilise les serveurs RADIUS globaux préconfigurés.

Étape 17. Cochez la case **Activer** dans le champ Comptabilité RADIUS si vous voulez suivre et mesurer le temps et l'utilisation des données des clients sur le réseau WAP.

Étape 18. Saisissez l'adresse IP du serveur RADIUS que vous souhaitez utiliser comme serveur principal dans le champ Server IP Address-1. L'adresse IP doit être au format IPv4 ou IPv6 selon ce que vous avez choisi dans le réseau IP RADIUS à l'étape 15.

Étape 19. (Facultatif) Entrez les adresses IP du serveur RADIUS de sauvegarde dans les champs Server IP Address-2 to Server IP Address-4. Ces serveurs sont utilisés si l'authentification échoue avec le serveur principal. Vous pouvez configurer jusqu'à trois serveurs IP de sauvegarde qui seront authentifiés dans l'ordre si le prédécesseur échoue.

Étape 20. Saisissez la clé secrète partagée dans le champ Key-1 que le périphérique WAP utilise pour s'authentifier auprès du serveur RADIUS principal. Vous pouvez utiliser jusqu'à 63 caractères alphanumériques et spéciaux standard. La clé est sensible à la casse.

Étape 21. (Facultatif) Entrez la clé secrète partagée dans les champs Key 2 to 4 que le périphérique WAP utilise pour s'authentifier auprès des serveurs RADIUS de sauvegarde

respectifs.

Le champ Nombre de paramètres régionaux affiche le nombre de paramètres régionaux associés à l'instance actuelle. Trois paramètres régionaux différents peuvent être créés et affectés à chaque instance à partir de la page de personnalisation Web.

Étape 22. (Facultatif) Si vous voulez supprimer l'instance actuellement configurée, cochez la case **Supprimer l'instance** pour supprimer l'instance actuellement configurée.

Étape 23. Cliquez sur **Enregistrer** pour enregistrer toutes les modifications apportées.