Configurer la tâche de service HTTP/HTTPS sur un point d'accès WAP125 ou WAP581

Objectif

HyperText Transfer Protocol Secure (HTTPS) est un protocole de transfert plus sécurisé que HTTP. Le point d'accès peut être géré via des connexions HTTP et HTTPS lorsque les serveurs HTTP/HTTPS sont configurés. Certains navigateurs Web utilisent HTTP tandis que d'autres utilisent HTTPS. Un point d'accès doit posséder un certificat SSL (Secure Socket Layer) valide pour utiliser les services HTTPS.

Pourquoi devons-nous configurer la tâche de service HTTP/HTTPS ?

Cette fonctionnalité est utile pour empêcher les hôtes indésirables d'accéder à l'utilitaire Web. À l'aide de la liste de contrôle d'accès à la gestion, vous pouvez spécifier jusqu'à 10 adresses IP, cinq pour IPv4 et cinq pour IPv6 pour avoir accès à l'utilitaire Web.

L'objectif de ce document est de vous montrer comment renforcer votre réseau en vous montrant comment configurer la tâche de service HTTP/HTTPS sur le WAP125.

Périphériques pertinents

- WAP125
- WAP581

Version du logiciel

- 1.0.0.4 - WAP581
- 1.0.0.5 - WAP125

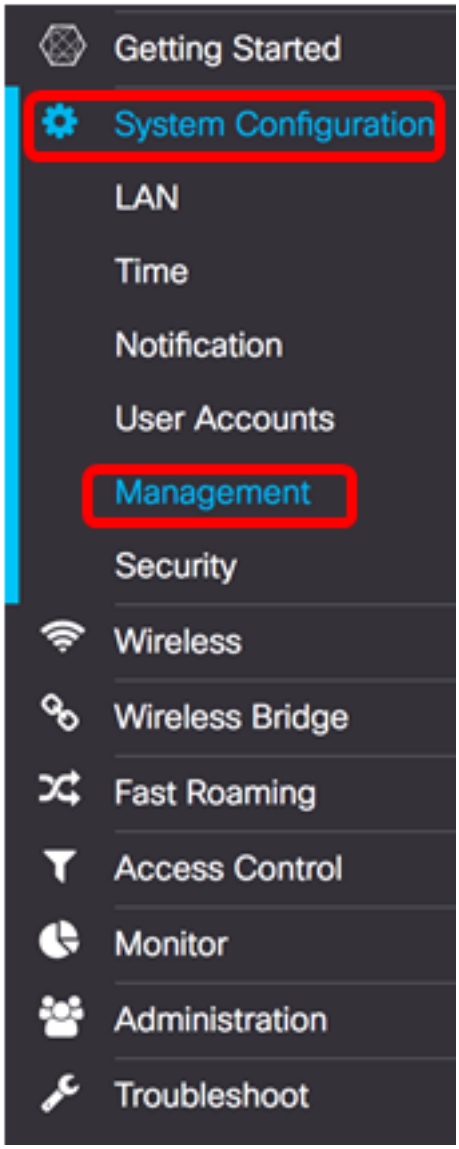
Collecte des informations d'assistance

Étape 1. Connectez-vous à l'utilitaire Web de votre WAP. Le nom d'utilisateur et le mot de passe par défaut sont cisco/cisco.

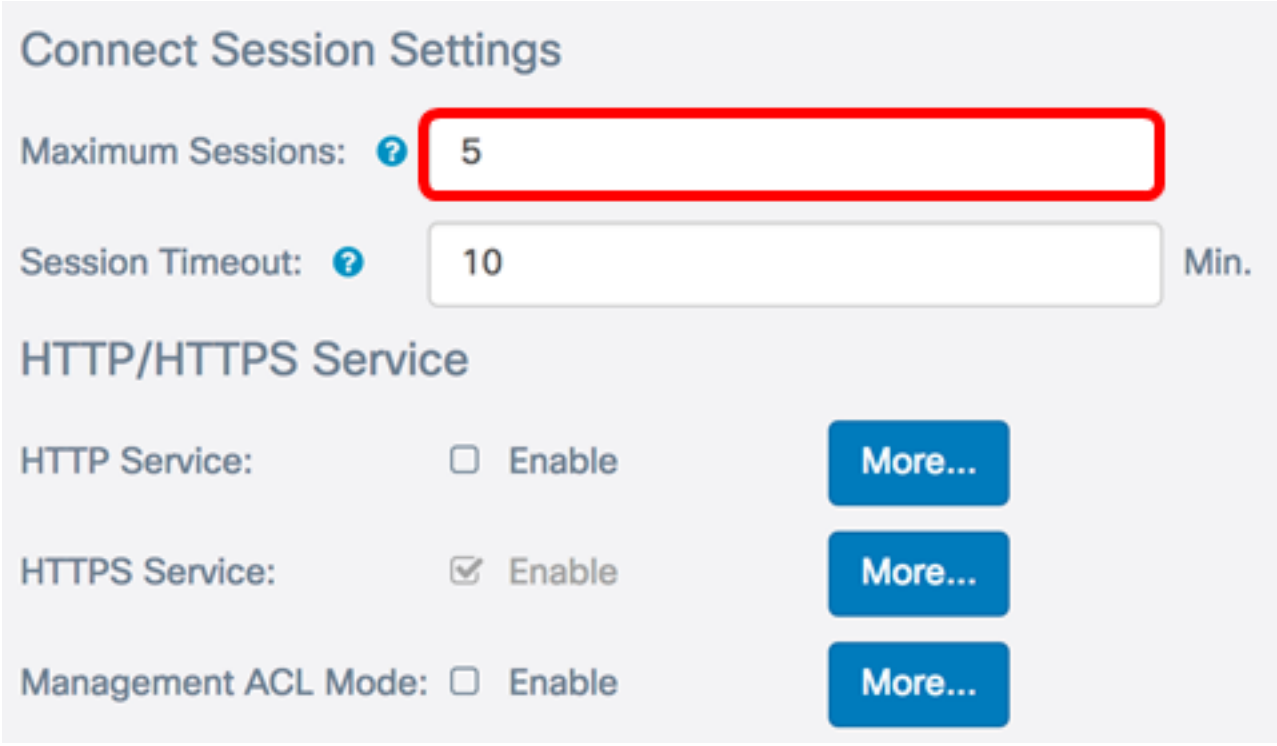
Note: Si vous avez déjà modifié le mot de passe ou créé un nouveau compte, saisissez plutôt vos nouvelles informations d'identification.

Étape 2. Choisissez **Configuration du système > Gestion**.

Note: Les options disponibles peuvent varier en fonction du modèle exact de votre périphérique. Dans cet exemple, WAP125 est utilisé.

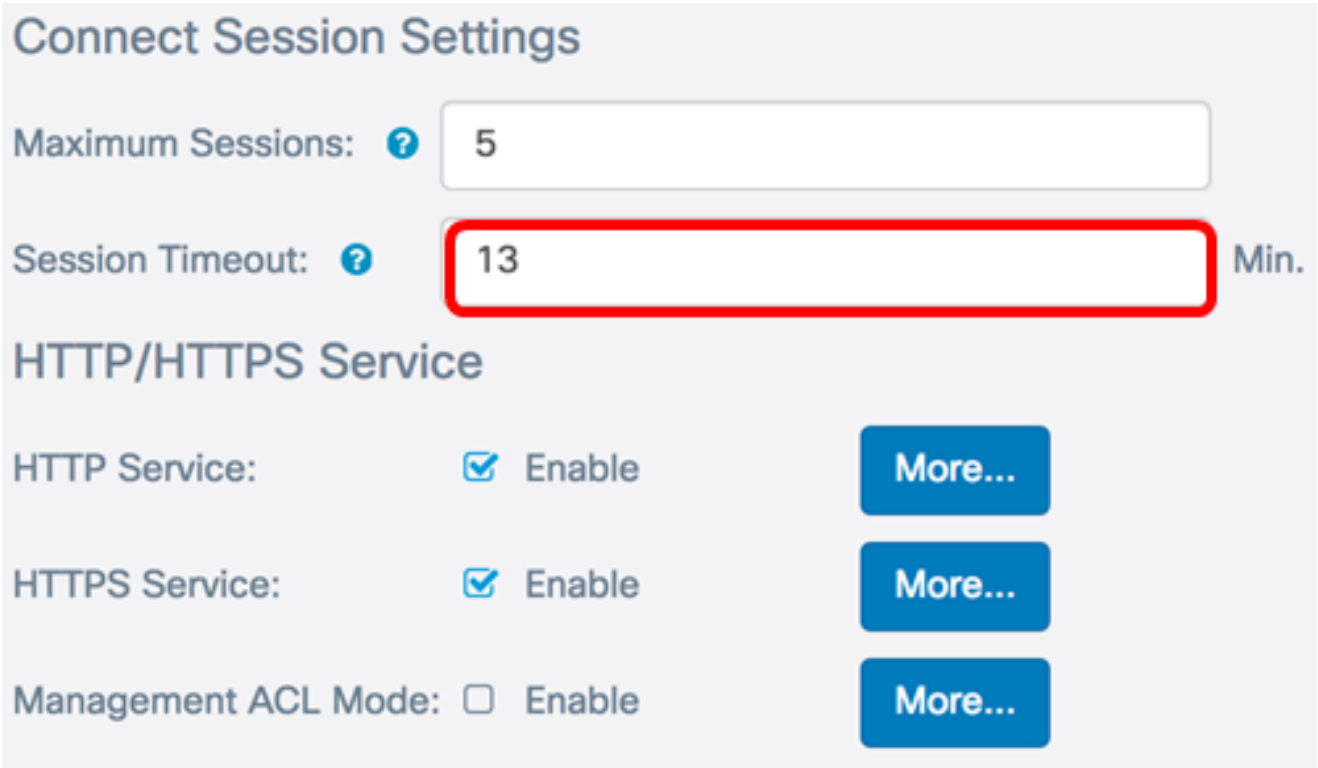


Étape 3. Dans le champ *Nombre maximal de sessions* sous Paramètres de session de connexion, saisissez une valeur comprise entre 1 et 10 pour définir le nombre maximal de sessions Web simultanées. Une session est créée chaque fois qu'un utilisateur se connecte au périphérique. Si la session maximale est atteinte, l'utilisateur suivant qui tente de se connecter au périphérique avec le service HTTP ou HTTPS est rejeté. 5 est établi par défaut.



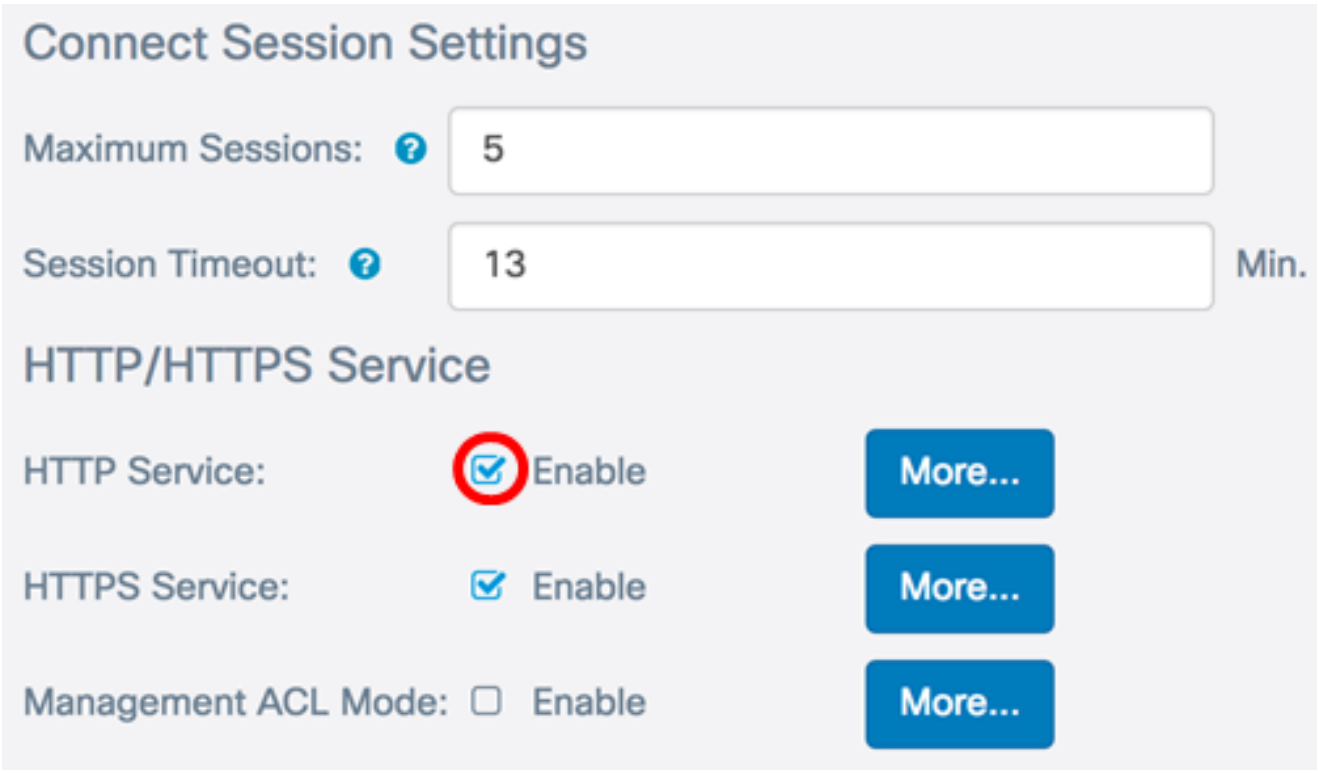
Étape 4. Dans le champ *Session Timeout*, saisissez une valeur comprise entre 2 et 60 minutes pour définir l'heure à laquelle la session Web peut rester inactive. La valeur par défaut est 10 minutes.

Note: Dans cet exemple, 13 est utilisé.

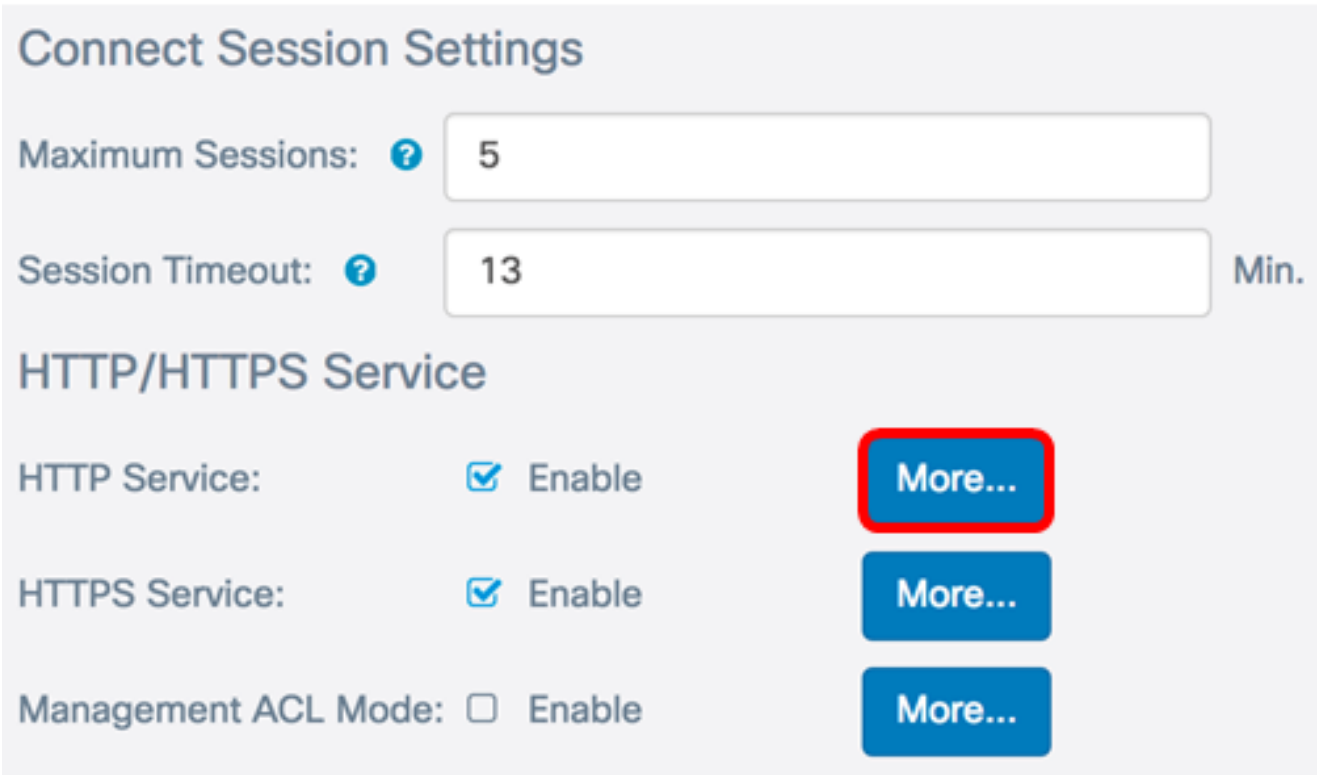


Service HTTP

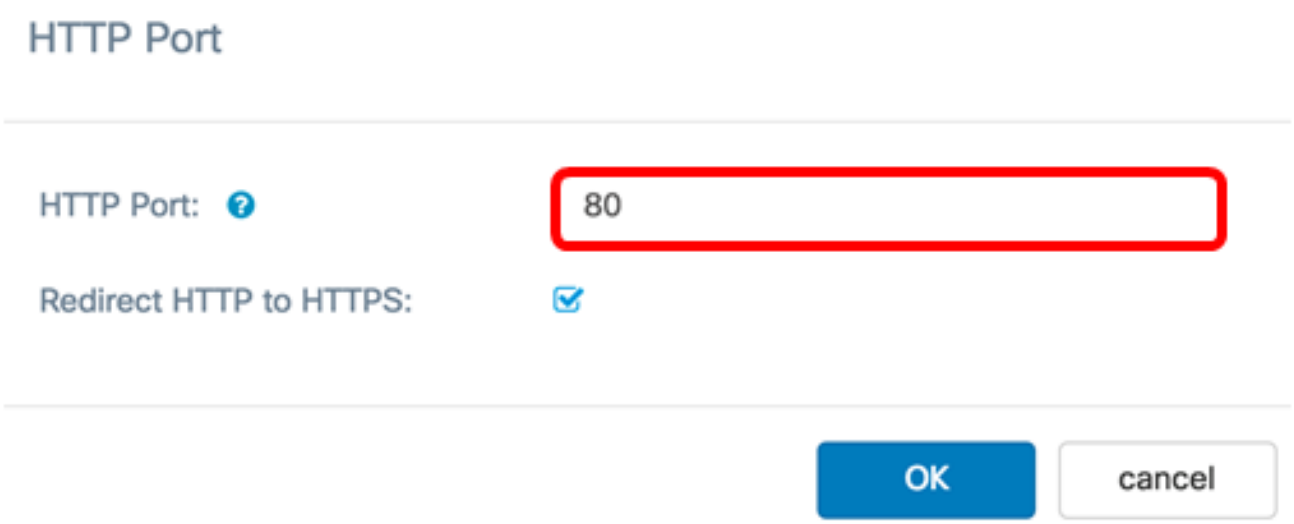
Étape 5. Cochez la case **Activer** le service HTTP pour autoriser la connexion de sessions Web via HTTP.



Étape 6. (Facultatif) Cliquez sur **More** pour afficher d'autres options et configurer un numéro de port.

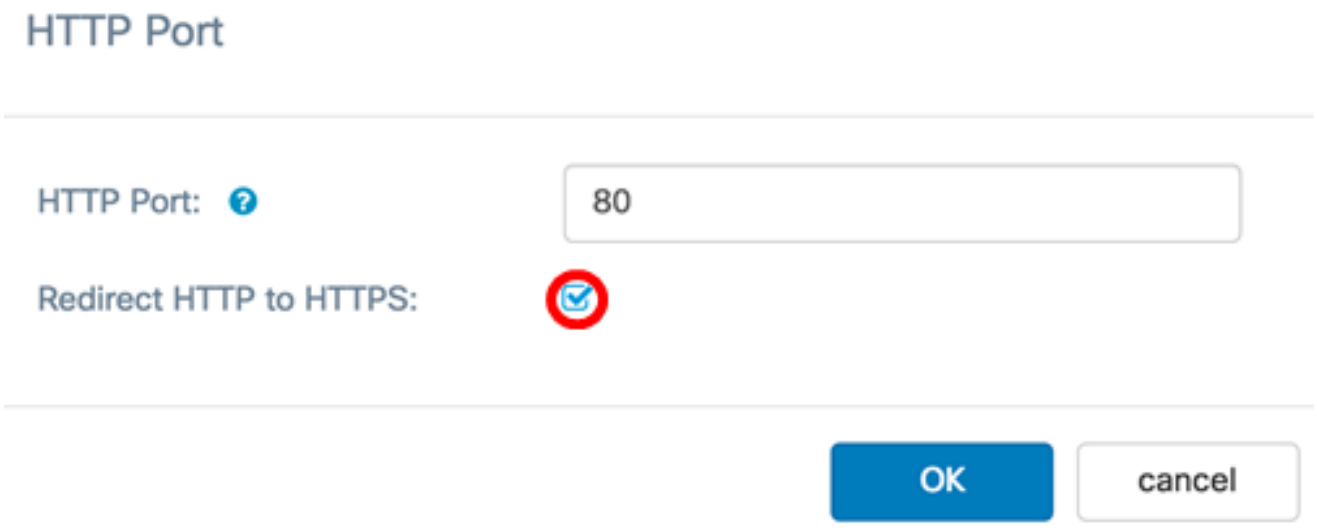


Étape 7. Dans le champ *Port HTTP*, saisissez un numéro de port logique à utiliser pour les connexions HTTP. La valeur du port est comprise entre 1025 et 65535. Le port par défaut réservé aux connexions HTTP est 80.

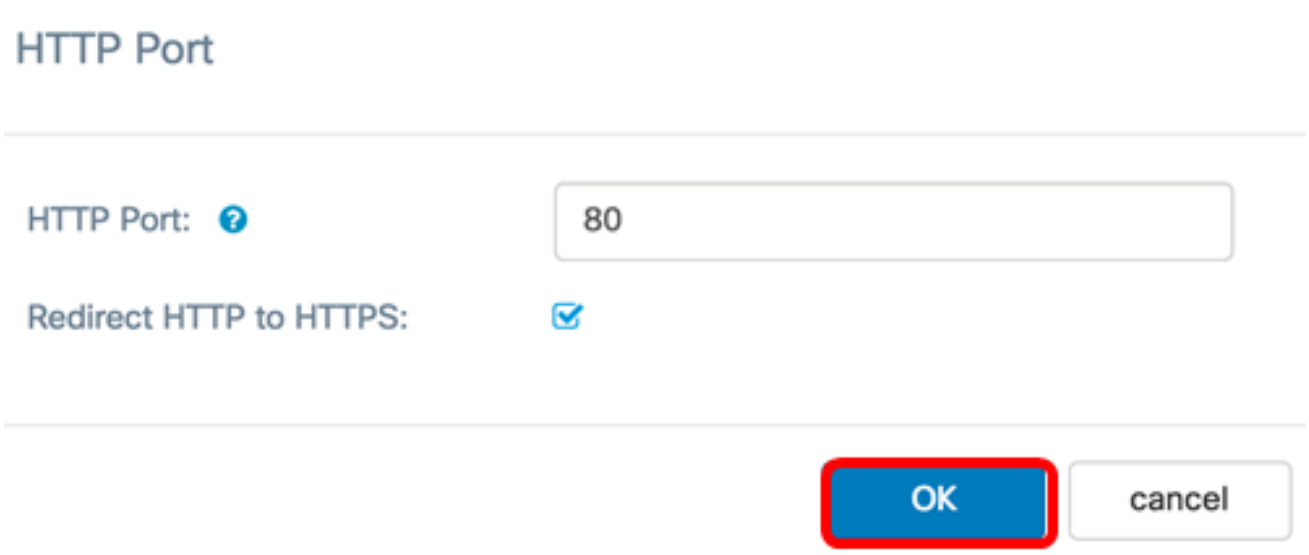


Étape 8. (Facultatif) Cochez la case **Rediriger HTTP vers HTTPS** pour permettre au navigateur de vous rediriger vers un protocole plus sécurisé, HTTPS, lors de l'établissement d'une session Web.

Note: Cette option n'est disponible que si la case à cocher Service HTTP est désactivée à l'étape 4. Dans cet exemple, cette option est cochée.



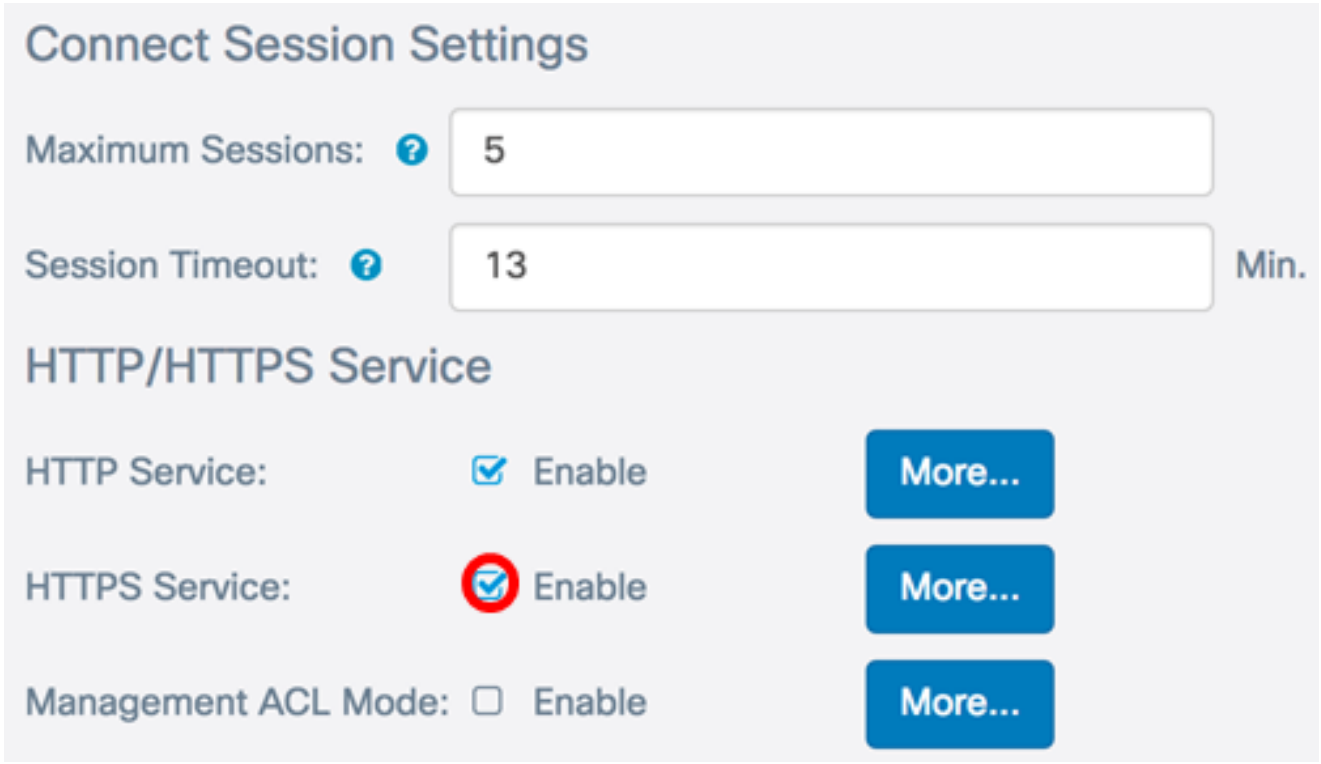
Étape 9. Cliquez sur **OK** pour revenir à la page Gestion et poursuivre la configuration.



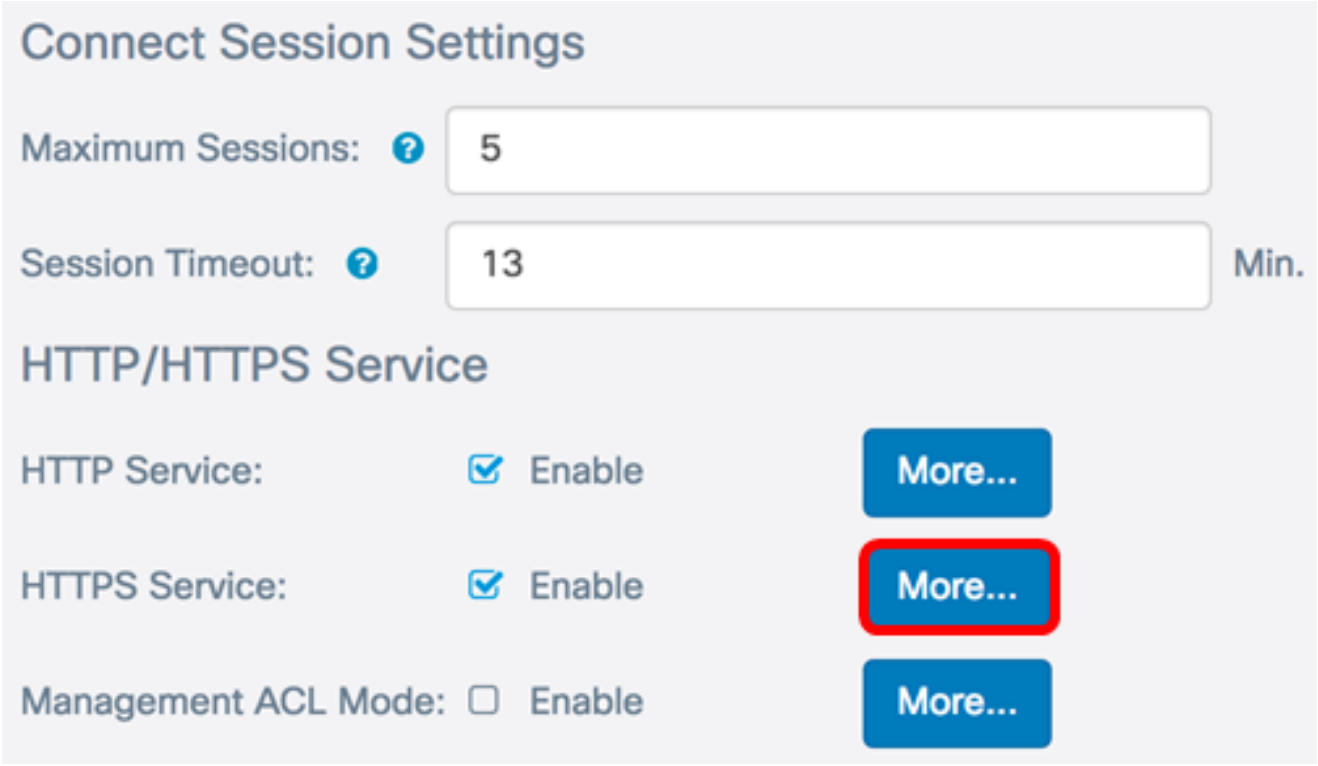
Service HTTPS

Étape 10. Cochez la case **Activer** le service HTTPS pour permettre l'établissement de sessions Web via un protocole sécurisé, HTTPS. Cette option est activée par défaut.

Note: Si cette option est désactivée, toutes les connexions existantes utilisant HTTPS sont déconnectées.



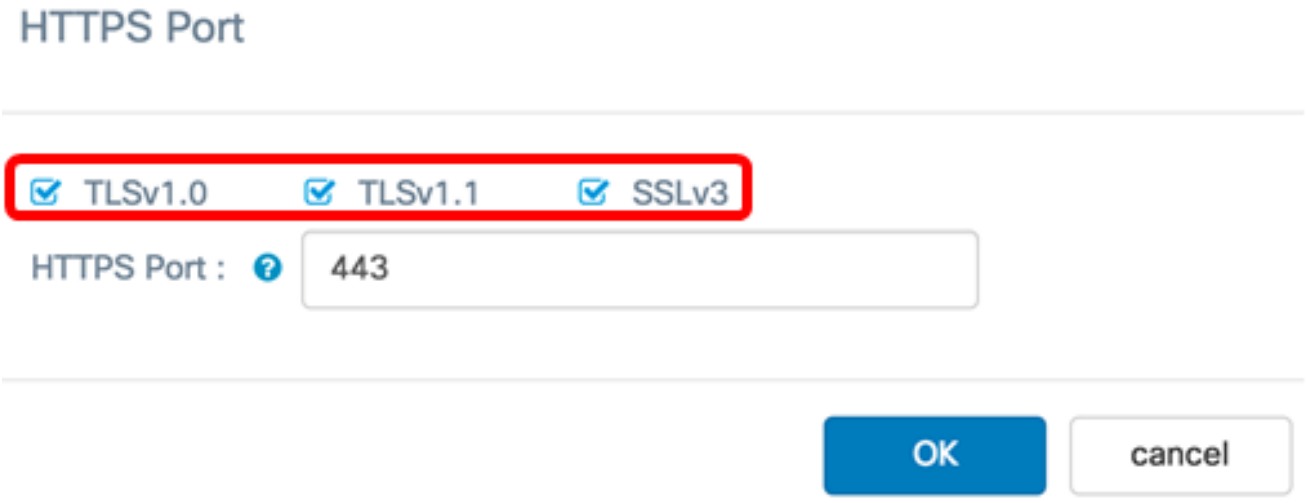
Étape 11. Cliquez sur **More** pour définir un port à utiliser par HTTPS et pour sélectionner Transport Layer Security Versions à utiliser sur HTTPS.



Étape 12. Sous la zone HTTPS Port, cochez les cases des protocoles de sécurité suivants utilisés sur HTTPS :

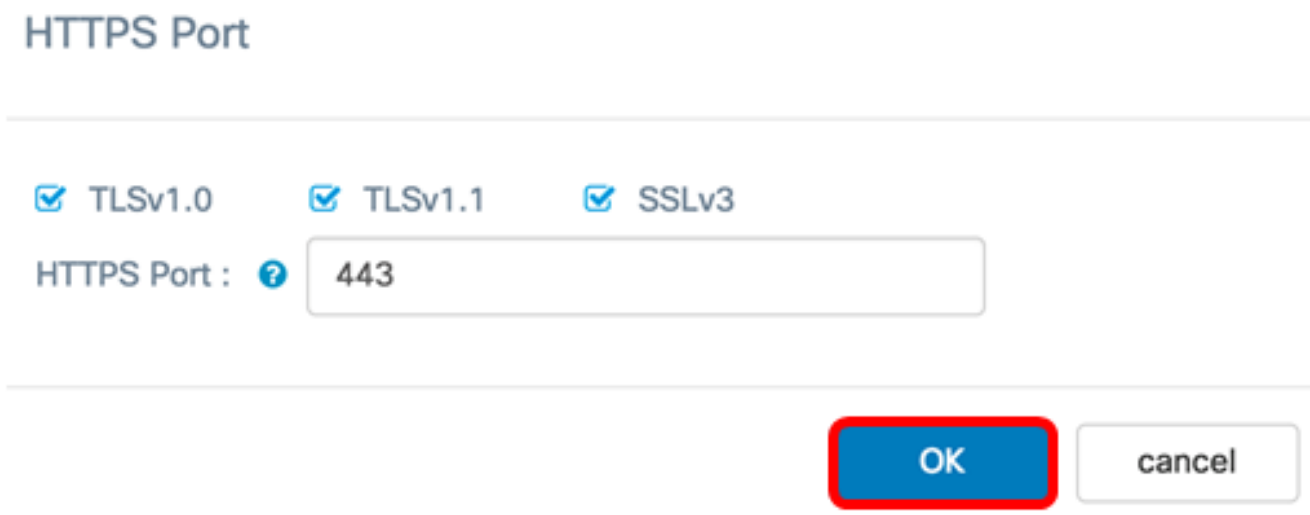
- TLSv1.0 — TLSv1 (Transport Layer Security version 1) est un protocole cryptographique qui fournit la sécurité et l'intégrité des données pour la communication sur Internet.
- TLSv1.1 - Une version améliorée de la première version de TSLv1 améliore la sécurité et l'intégrité des données pour la communication.
- SSLv3 - SSLv3 (Secure Socket Layer version 3) est un protocole utilisé sur HTTPS pour établir des sessions sécurisées et des communications sur Internet.

Note: Dans cet exemple, toutes les cases à cocher sont cochées.



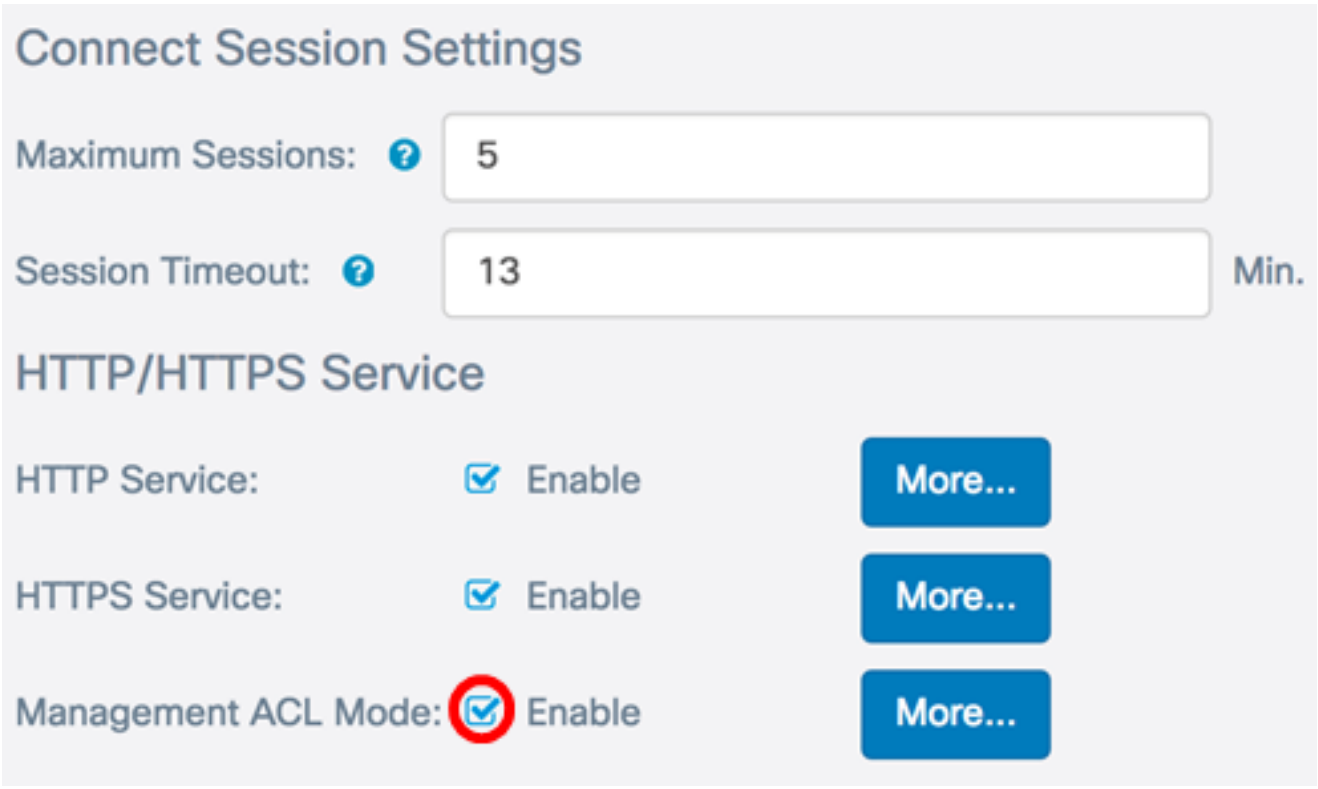
Étape 13. Dans le champ *Port HTTPS*, saisissez un numéro de port logique à utiliser pour les connexions HTTPS. Le port réservé par défaut est 443.

Étape 14. Cliquez sur **OK pour continuer.**

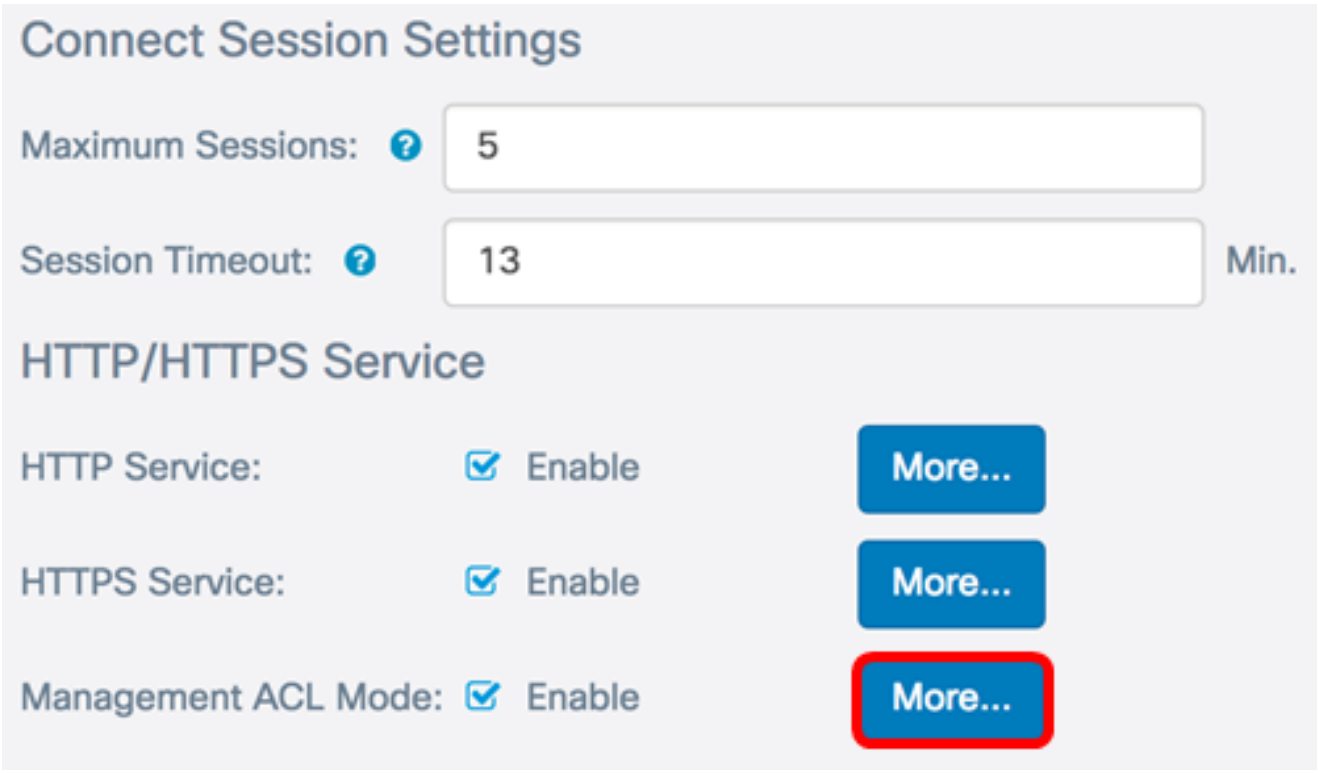


Mode ACL de gestion

Étape 15. Cochez la case **Activer** le mode ACL pour spécifier une liste de contrôle d'accès (ACL) des adresses IP autorisées à accéder à l'utilitaire Web. Si cette fonctionnalité est désactivée, elle autorise l'accès à l'utilitaire Web.



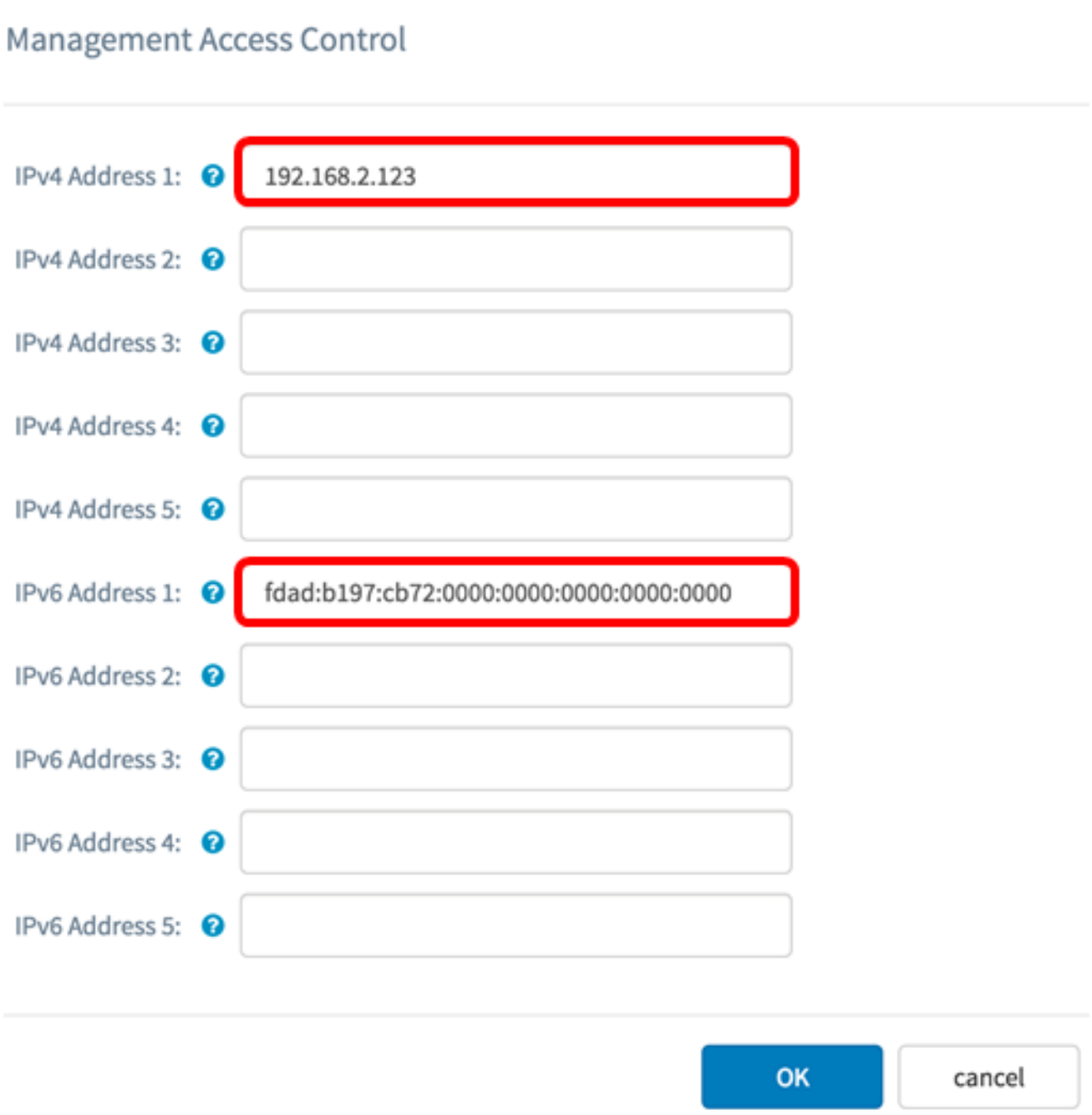
Étape 16. Cliquez sur **More** pour spécifier une liste d'adresses IPv4 et IPv6 autorisées à accéder à l'utilitaire Web.



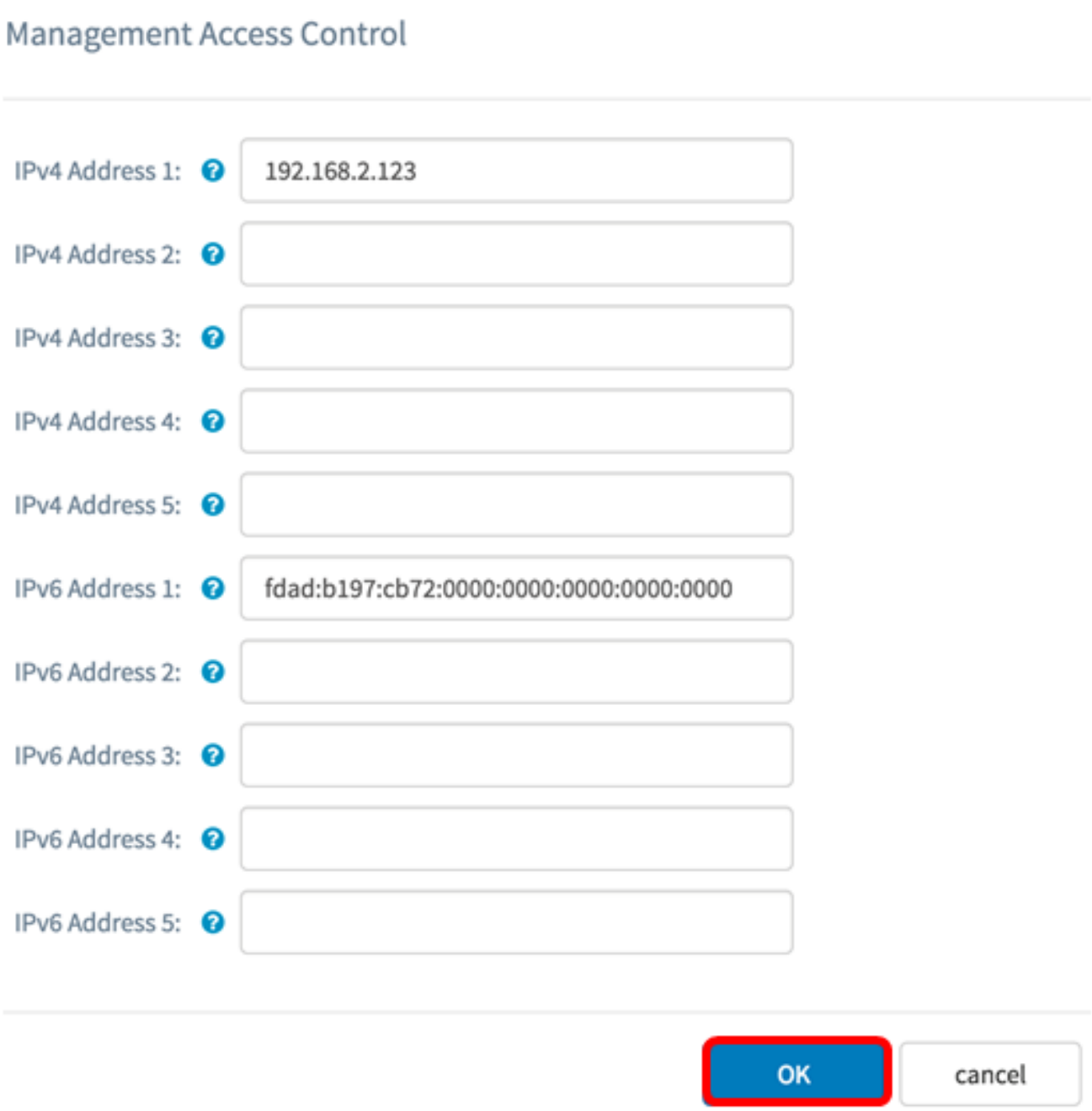
Étape 17. Dans les champs *IPv4 Address* et *IPv6 Address*, saisissez les adresses IP administratives dans les formats respectifs auxquels l'accès à l'utilitaire Web sera accordé.

Astuce : Attribuez des adresses IP statiques aux adresses IP administratives.

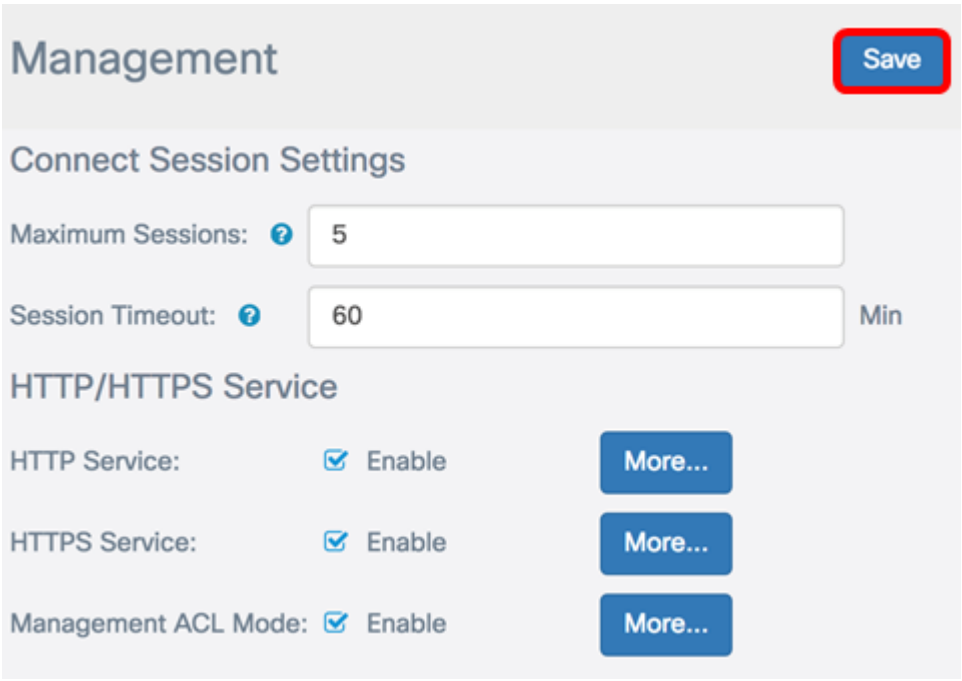
Note: Dans cet exemple, 192.168.2.123 est utilisé comme adresse d'administration IPv4 et fdad:b197:cb72:0000:0000:0000:0000:0000 est utilisé comme adresse d'administration IPv6 adresse.



Étape 18. Click OK.



Étape 19. Cliquez sur le bouton **Enregistrer** pour enregistrer les paramètres configurés.



Vous devez maintenant avoir correctement configuré la tâche de service HTTP/HTTPS sur votre point d'accès WAP125 ou WAP581.