Configuration de service HTTP/HTTPS et Gestion de certificat de Protocole SSL (Secure Socket Layer) sur les Points d'accès WAP121 et WAP321

Objectif

Le Point d'accès peut être géré par les deux connexions sécurisées de HTTP et de HTTP (HTTPS) quand les serveurs HTTP/HTTPS sont configurés. Le texte hyper Transfer Protocol sécurisé (HTTPS) est un plus protocole sécurisé de transfert que le HTTP. Quelques navigateurs Web utilisent le HTTP tandis que d'autres utilisent HTTPS. Un Point d'accès doit avoir un certificat ssl valide pour utiliser le service HTTPS. Un certificat ssl est un certificat digitalement signé par une autorité de certification qui permet au navigateur Web pour avoir une transmission chiffrée sécurisée avec le web server.

Cet article explique comment configurer le service HTTP/HTTPS sur les Points d'accès WAP121 et WAP321.

Périphériques applicables

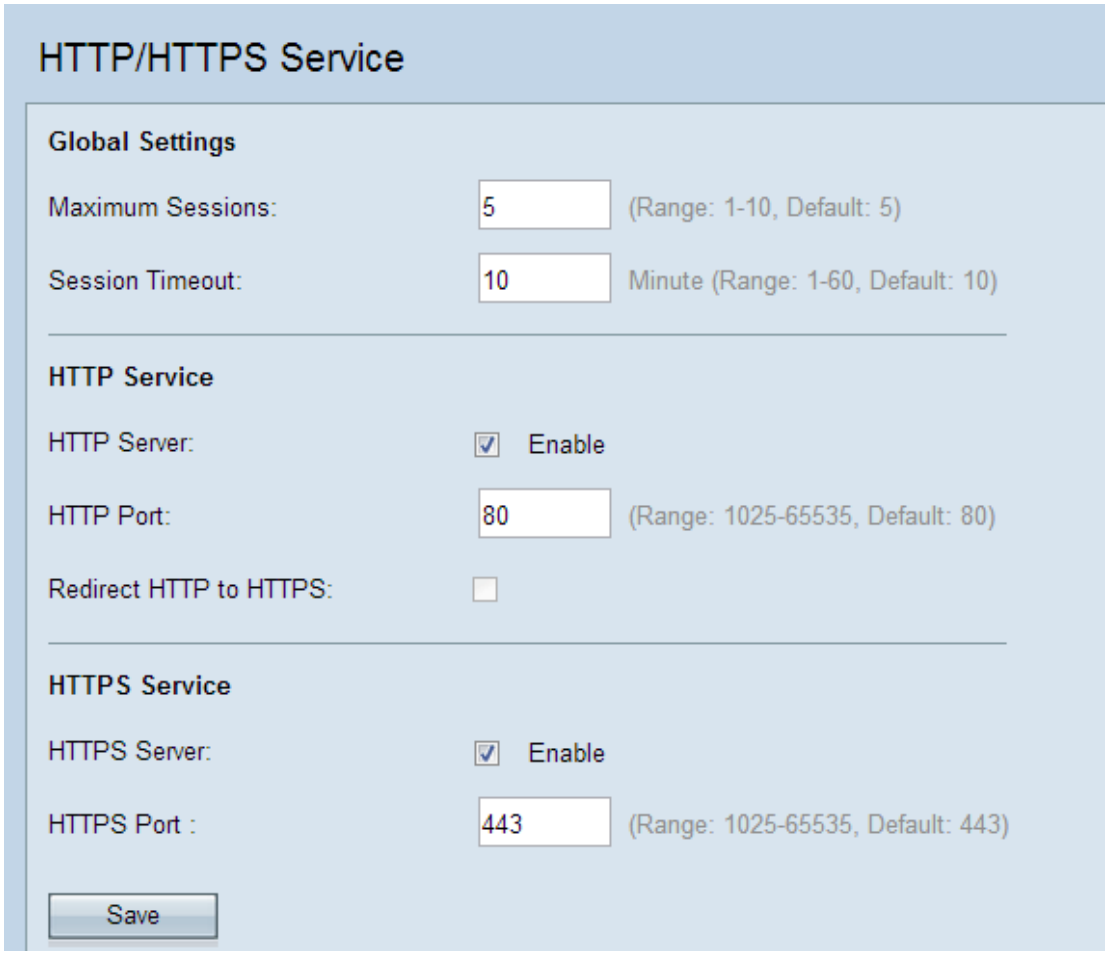
- WAP121
- WAP321

Version de logiciel

- 1.0.3.4

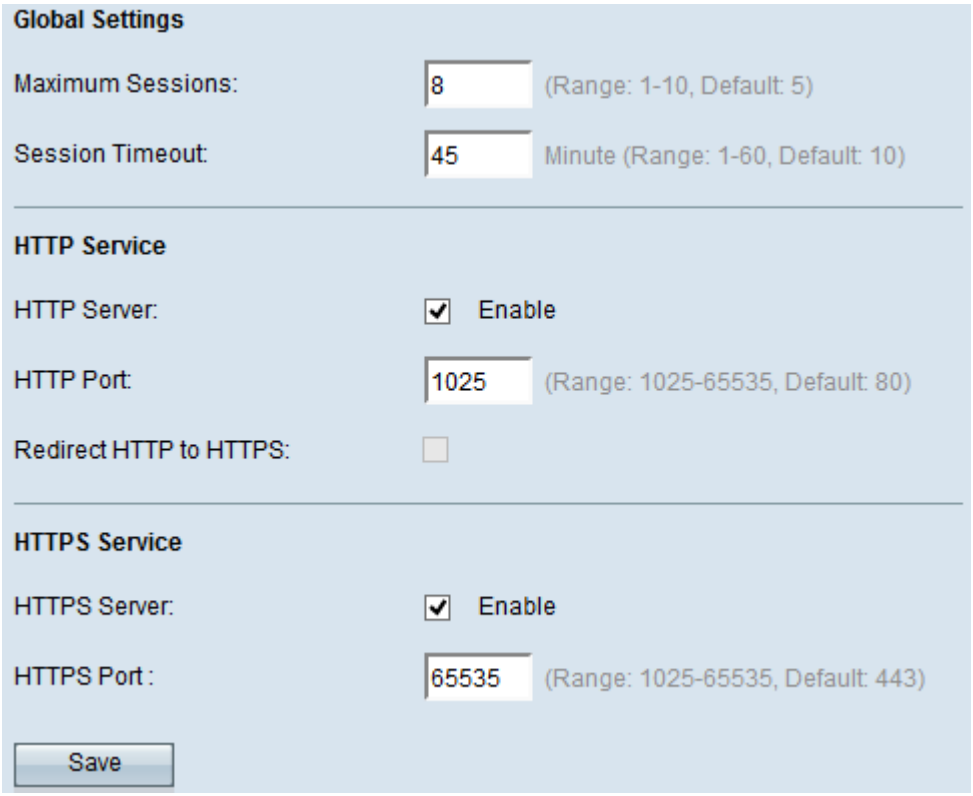
Service HTTP/HTTPS

Étape 1. Ouvrez une session à l'utilitaire de configuration Web et choisissez la **gestion > le service HTTP/HTTPS**. La page de *service HTTP/HTTPS* s'ouvre :



Étape 2. Présentez le nombre maximal de sessions Web qui inclut le HTTP et session HTTPS à être dans utilisé en même temps en sessions maximum mettent en place. Une session est chaque fois créés les logins d'un utilisateur au périphérique. Si la session maximum est atteinte alors le prochain utilisateur qui tente d'ouvrir une session dans le périphérique avec le service de HTTP ou HTTPS est rejeté.

Étape 3. Écrivez la durée maximale en quelques minutes que les restes inactifs d'un utilisateur ont ouvert une session à l'interface web AP dans le domaine de Session Timeout.



Étape 4. Cochez la case d'**enable** dans le domaine de serveur HTTP pour activer l'accès de Web par l'intermédiaire du HTTP.

Remarque: Si le serveur HTTP est désactivé, toutes les connexions en cours qui utilisent le HTTP seront déconnectées.

Étape 5. Introduisez le numéro de port pour l'utiliser pour des connexions HTTP dans le domaine de port HTTP. Le numéro de port s'étend à partir de 1025 à 65535.

Étape 6. (facultative) pour réorienter des tentatives d'accès HTTP de Gestion sur le port HTTP au HTTPS mettent en communication, cochent le **HTTP de réorientation dans la** case **HTTPS**. Ce champ est disponible seulement quand l'accès HTTP est désactivé.

Étape 7. Cochez la case d'**enable du** serveur HTTPS pour activer l'accès de Web par l'intermédiaire de HTTPS.

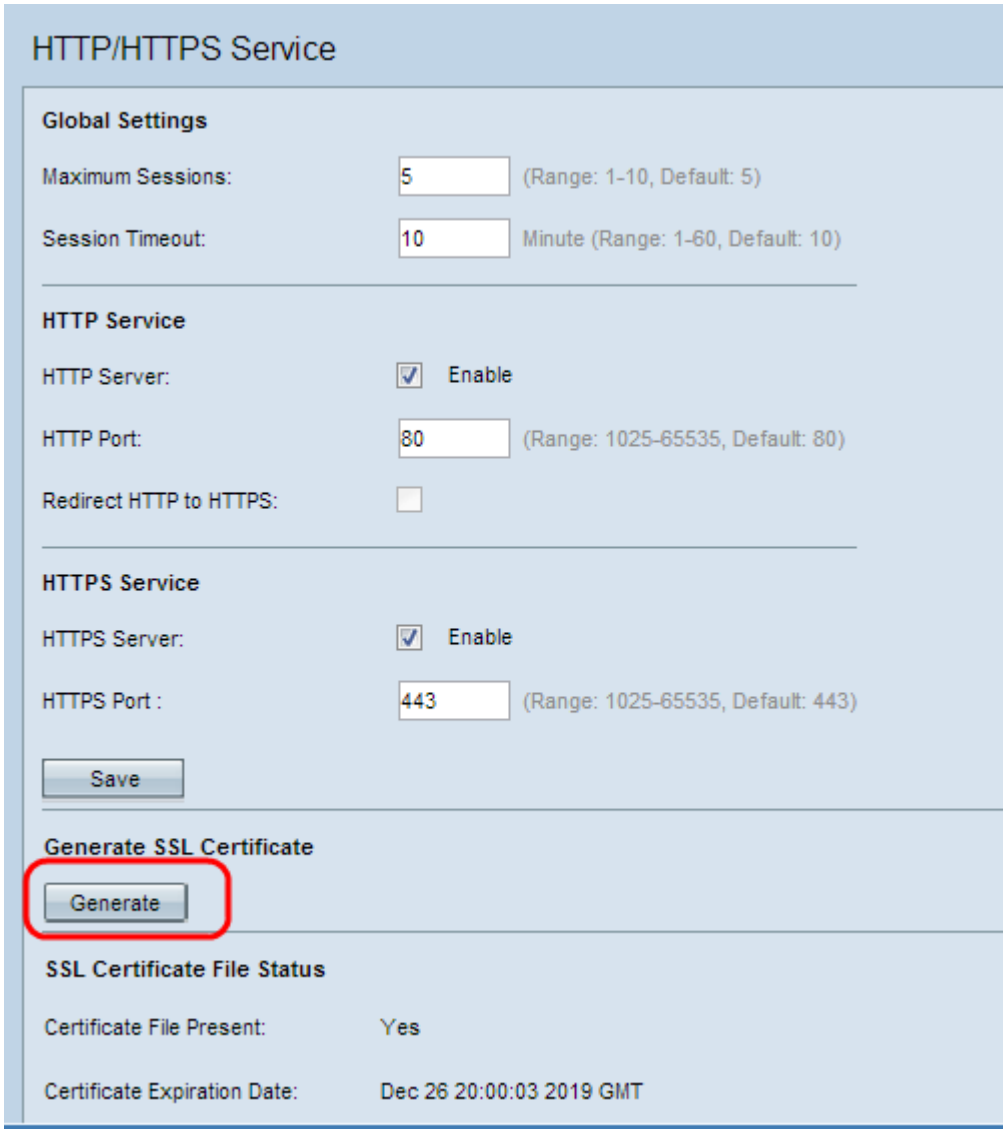
Remarque: Si le serveur HTTPS est désactivé, toutes les connexions en cours qui utilisent HTTPS seront déconnectées.

Étape 8. Introduisez le numéro de port pour l'utiliser pour des connexions HTTPS dans le domaine de port HTTPS. Le numéro de port s'étend à partir de 1025 à 65535.

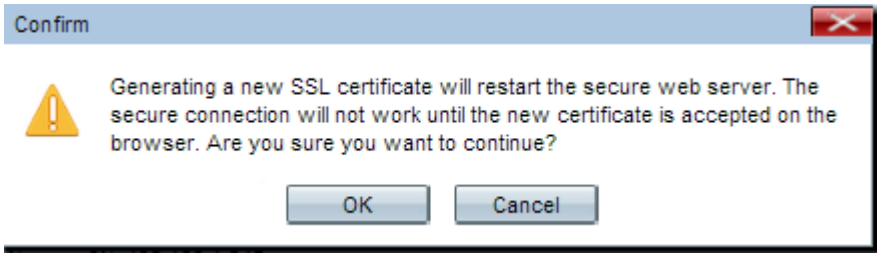
Étape 9. **Sauvegarde de** clic pour sauvegarder les configurations.

Génération d'un certificat ssl

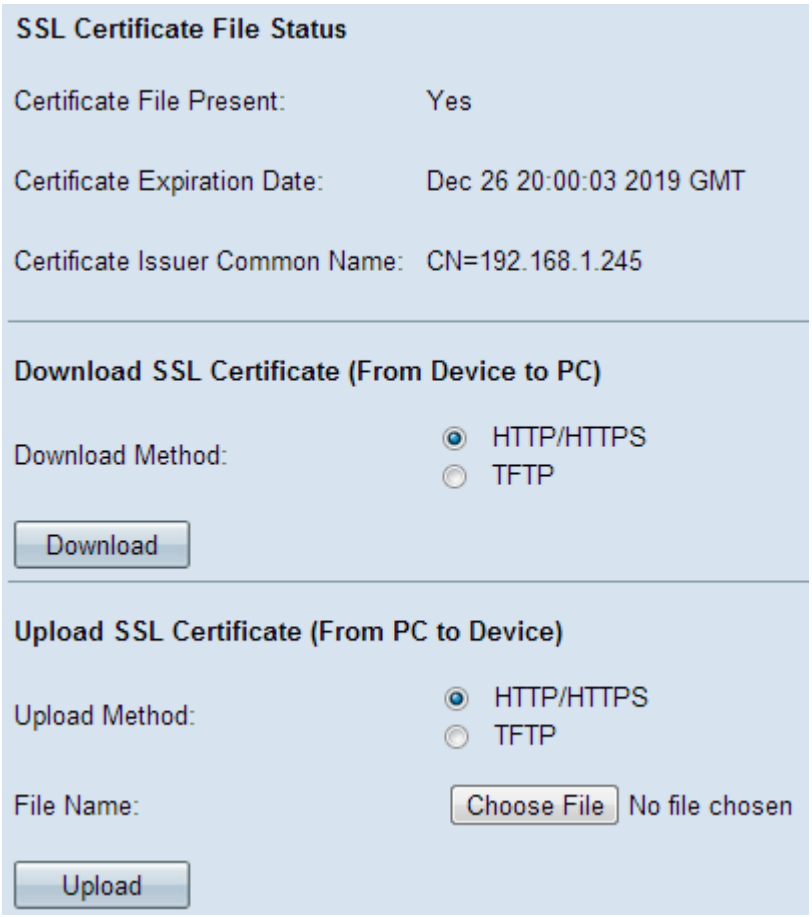
La génération d'un nouveau certificat ssl de HTTP pour le web server sécurisé devrait être faite après qu'AP ait saisi une adresse IP. Ceci s'assure que le nom commun pour le certificat apparie l'adresse IP d'AP. La génération d'un nouveau certificat ssl redémarre le web server sécurisé. La connexion sécurisée ne fonctionne pas jusqu'à ce que le nouveau certificat soit reçu sur le navigateur. Suivez les étapes données ci-dessous pour générer le certificat ssl.



Étape 1. Le clic **se produisent** pour générer un nouveau certificat ssl. Le message d'alerte apparaît.



Étape 2. Cliquez sur OK **pour continuer la génération du certificat ssl.**



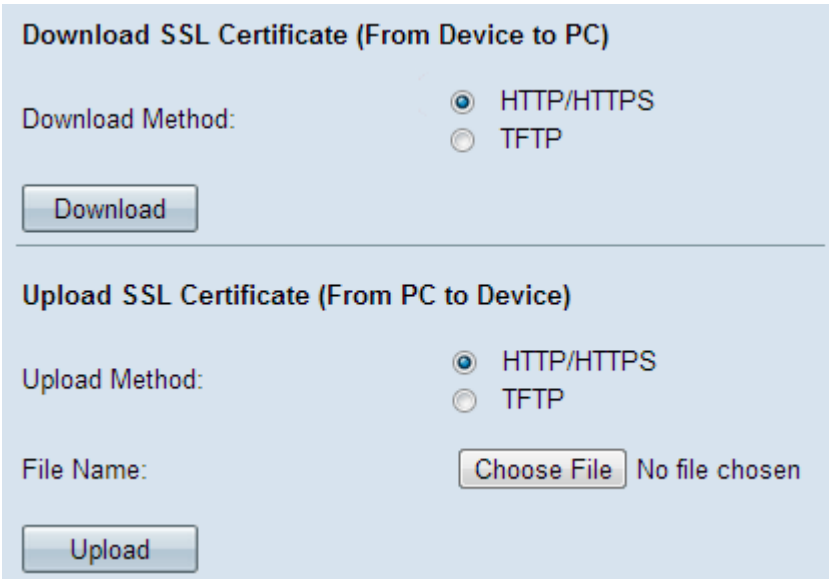
La région d'état de fichier de certificat ssl affiche les informations suivantes :

• Fichier du certificat actuel — Indique si le fichier de certificat ssl de HTTP est présent ou pas. Non est établi par défaut.

• Date d'expiration de certificat — Affiche la date d'expiration du certificat ssl de HTTP.

• Nom commun d'émetteur de certificat — Affiche le nom commun de l'émetteur de certificat.

Téléchargez le certificat ssl



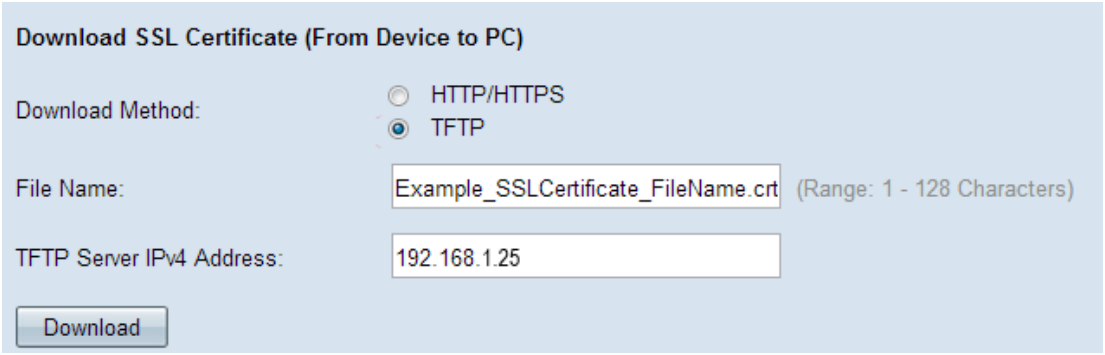
Étape 1. Cliquez sur le fichier approprié de certificat ssl de la case d'option de méthode de

téléchargement dans la région de certificat ssl de téléchargement (du périphérique au PC).

• HTTP/HTTPS — Cliquez sur cette case d'option si le certificat ssl doit être téléchargé d'un web server.

• TFTP — Cliquez sur cette case d'option si le certificat ssl doit être téléchargé d'un serveur TFTP.

Remarque: Ignorez à l'étape 4 si HTTP/HTTPS est cliqué sur dans l'étape précédente.



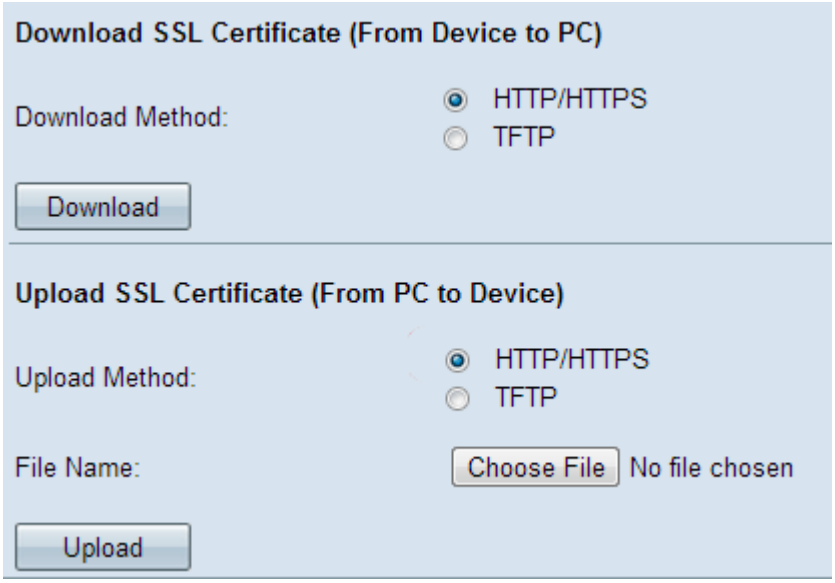
Étape 2. Si le TFTP est cliqué sur dans l'étape 2, alors écrivez le nom du fichier dans le domaine de nom du fichier.

Étape 3. Introduisez l'adresse du serveur TFTP dans le domaine d'ipv4 addres de serveur TFTP.

Étape 4. Cliquez sur Download pour télécharger le fichier du certificat.

Téléchargez le certificat ssl

Suivez les étapes données ci-dessous pour télécharger le certificat ssl.



Étape 1. Cliquez sur la case d'option appropriée de méthode de téléchargement dans la région de certificat ssl de téléchargement (du PC au périphérique).

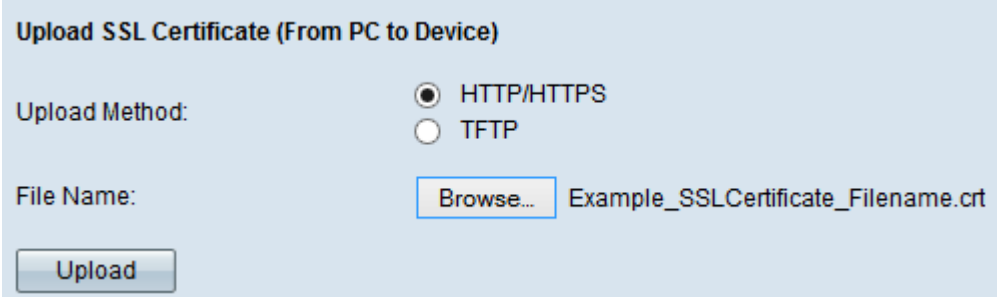
• HTTP/HTTPS — Cliquez sur cette case d'option si le certificat ssl doit être téléchargé avec un web server.

• TFTP — Cliquez sur cette case d'option si le certificat ssl doit être téléchargé avec un

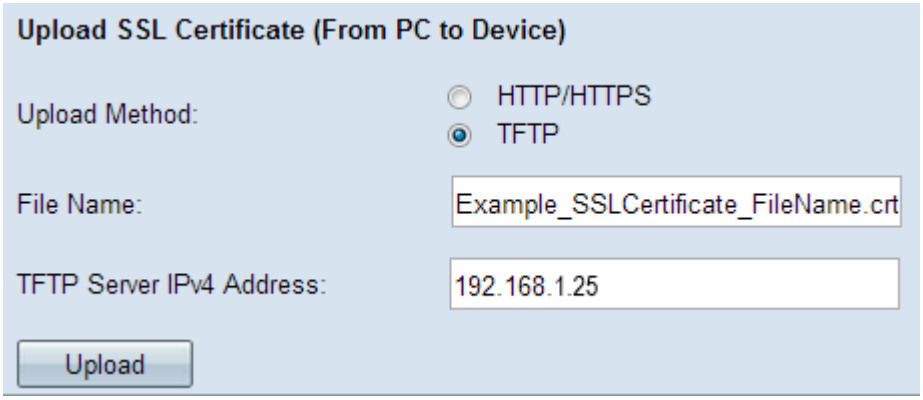
serveur TFTP.

Remarque: Ignorez à l'étape 4 si le TFTP est cliqué sur dans l'étape précédente.

Étape 2. Si HTTP/HTTPS est cliqué sur, alors cliquez sur **choisissent le fichier** ou **Browse** basé sur votre navigateur pour rechercher le fichier.



Étape 3. Cliquez sur Upload **pour télécharger le fichier qui est choisi.** Ignorez les dernières étapes comme ces étapes s'appliquent seulement au TFTP.



Étape 4. Si le TFTP est cliqué sur dans l'étape 2, alors écrivez le nom du fichier dans le domaine de nom du fichier.

Étape 5. Introduisez l'adresse du serveur TFTP dans le domaine d'ipv4 addres de serveur TFTP.

Étape 6. Cliquez sur Upload pour télécharger le fichier du certificat.