Gestion des utilisateurs VPN et configuration de Quick VPN sur les routeurs VPN RV016, RV042, RV042G et RV082

Objectif

Un réseau privé virtuel (VPN) est un moyen de connecter des points d'extrémité sur différents réseaux sur un réseau public, tel qu'Internet. Une application utile des VPN est qu'un utilisateur distant avec un logiciel client VPN peut accéder en toute sécurité aux informations sur un réseau privé tant qu'il a accès à Internet. Les routeurs VPN de la gamme RV0xx peuvent être configurés pour permettre aux utilisateurs de QuickVPN de créer un tunnel VPN avec le routeur. Cisco QuickVPN est un logiciel développé pour l'accès à distance à un réseau privé virtuel (VPN).

Un certificat VPN est un moyen d'améliorer la sécurité dans le tunnel VPN. Les certificats sont générés par le routeur et sont utilisés pour s'assurer que le routeur et l'utilisateur QuickVPN sont sécurisés. À partir du routeur, vous pouvez exporter le certificat qui peut être utilisé par le client QuickVPN.

Cet article explique comment configurer un utilisateur VPN et gérer les certificats VPN sur les routeurs VPN de la gamme RV0xx.

Remarque : vous devez configurer un tunnel VPN avant de configurer des utilisateurs VPN. Pour en savoir plus sur la façon de configurer le VPN passerelle à passerelle, consultez Configuration du VPN passerelle à passerelle sur les routeurs VPN RV016, RV042, RV042G et RV082. Pour en savoir plus sur la façon de configurer un VPN de client à passerelle, référez-vous à Configurer un tunnel d'accès à distance (client à passerelle) pour les clients VPN sur les routeurs VPN RV016, RV042, RV042G et RV082. Après avoir configuré les utilisateurs VPN, vous devez configurer Quick VPN sur le PC de l'utilisateur pour accéder au tunnel VPN.

Périphériques pertinents

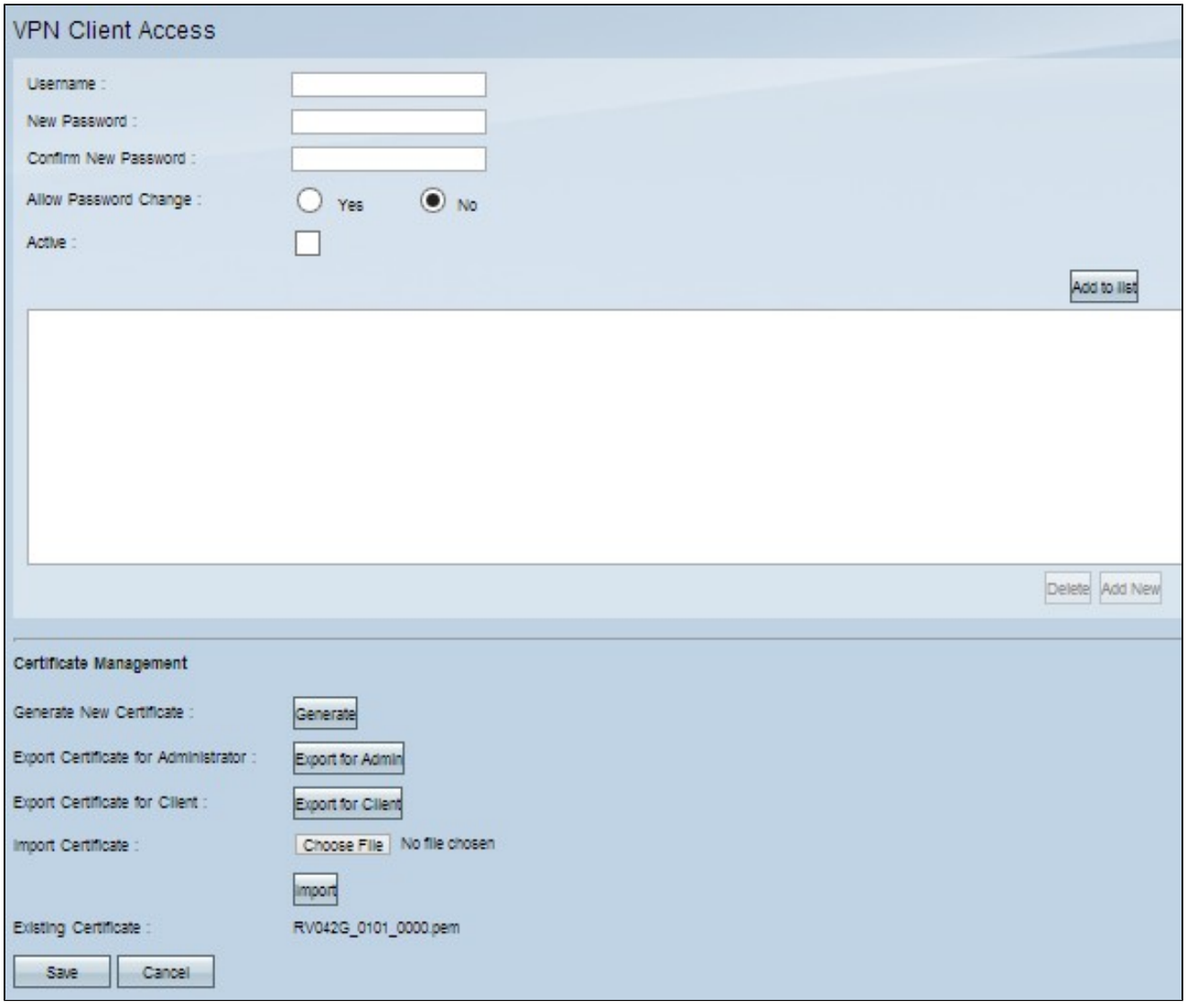
- RV016
- RV042
- RV042G
- RV082

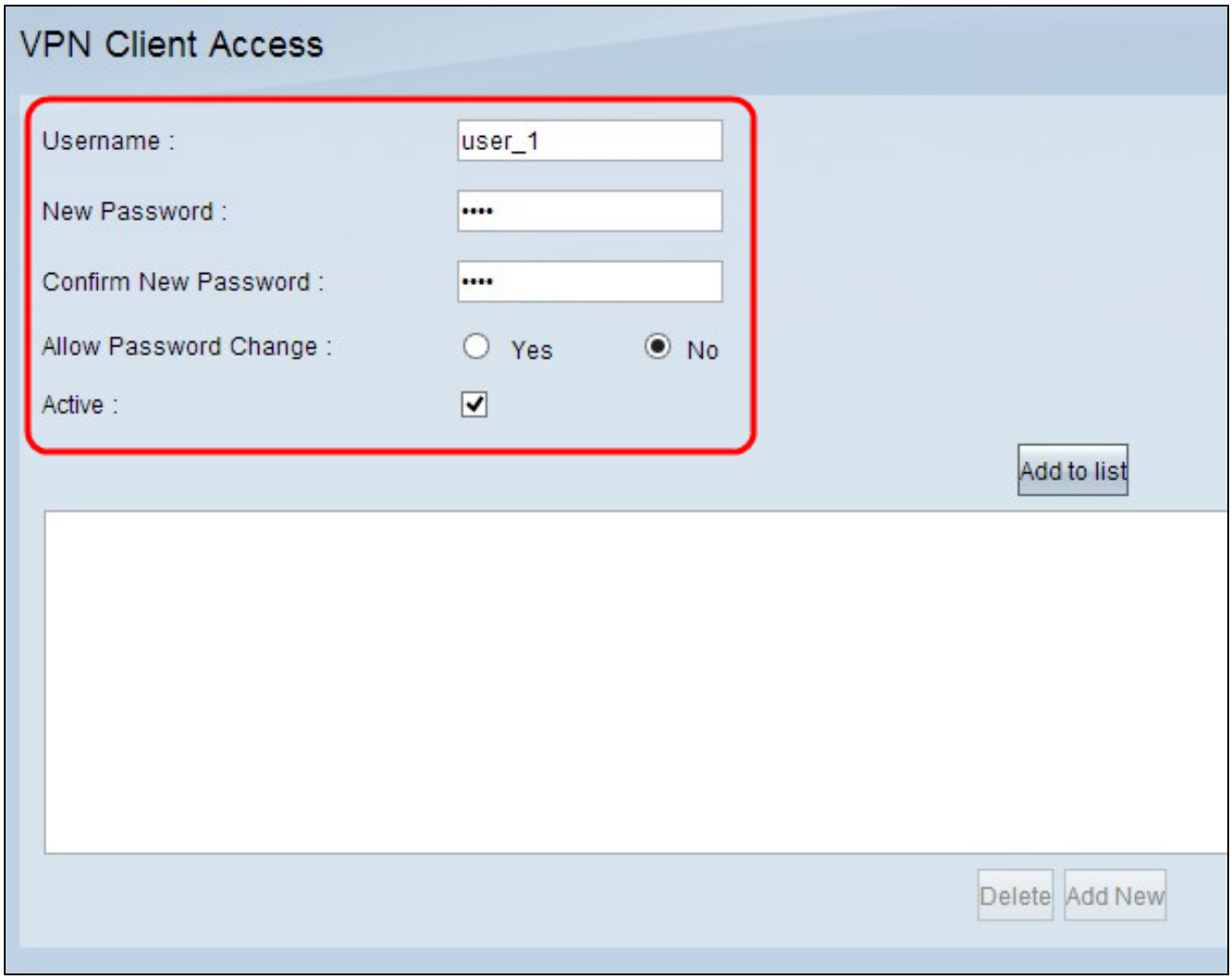
Version du logiciel

· v4.2.2.08 [Routeurs VPN de la gamme RV]
· 1.4.2.1 [Cisco QuickVPN]

Configuration des utilisateurs VPN

Étape 1. Connectez-vous à l'utilitaire de configuration du routeur et choisissez VPN > VPN Client Access.La page VPN Client Access s'ouvre :





Étape 2. Saisissez le nom d'utilisateur du client VPN dans le champ Username.

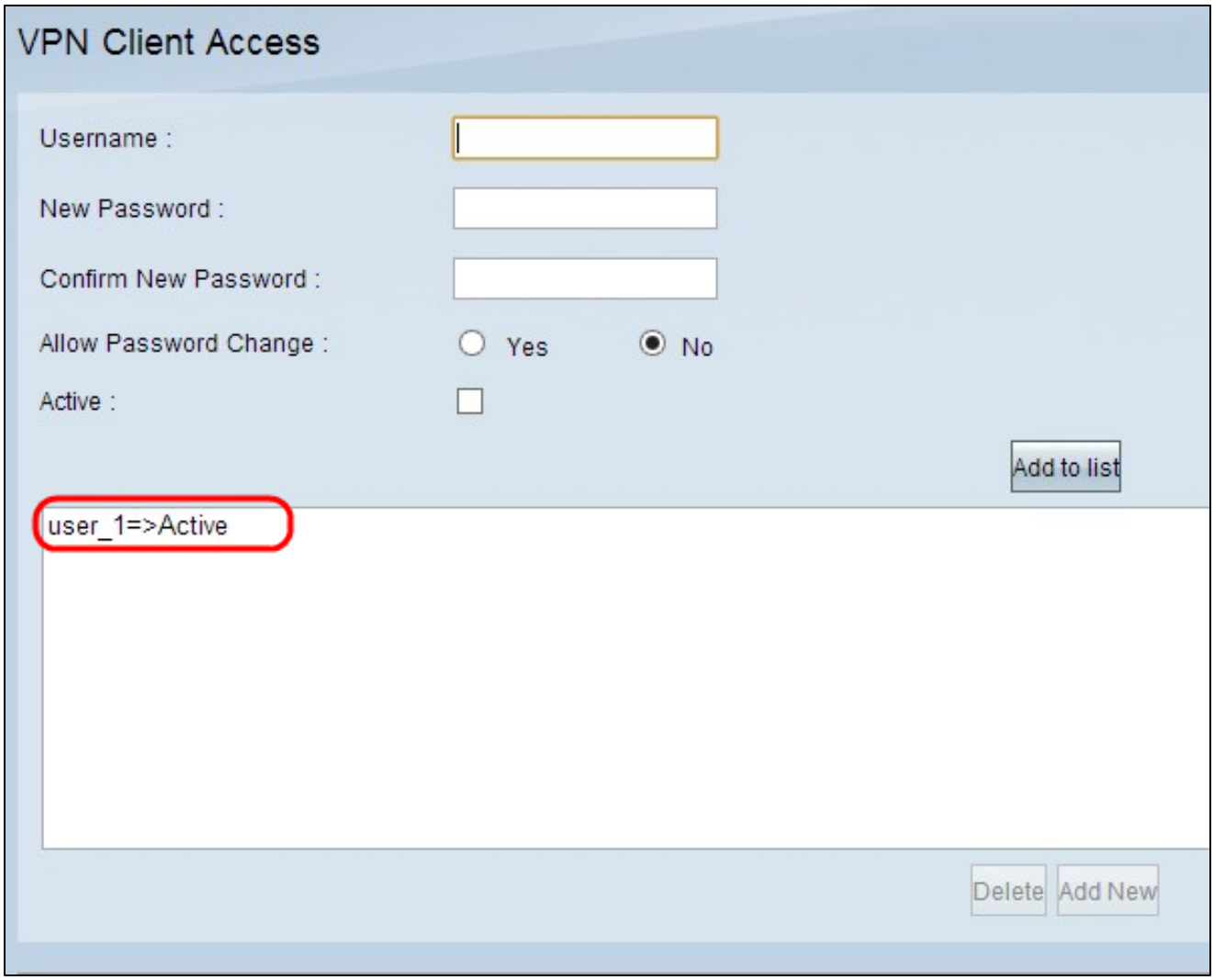
Étape 3. Saisissez le mot de passe de l'utilisateur dans le champ Nouveau mot de passe.

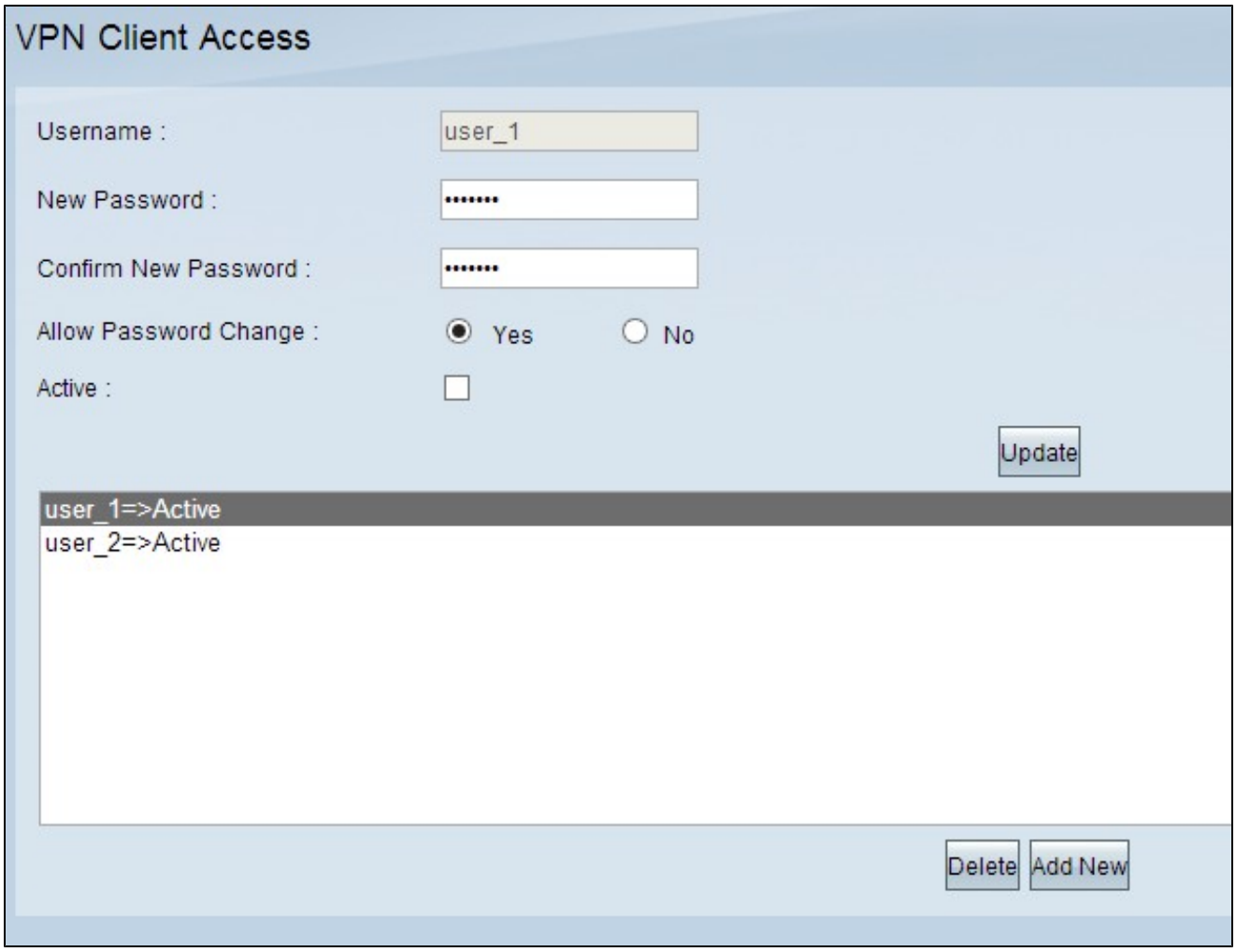
Étape 4. Saisissez à nouveau le mot de passe pour le confirmer dans le champ Confirmer le nouveau mot de passe.

Étape 5. (Facultatif) Pour autoriser l’utilisateur à modifier son mot de passe, cliquez sur la case d’option Yes.

Étape 6. Cochez la case Active pour rendre l'utilisateur VPN actif.

Étape 7. Cliquez sur Add to list pour ajouter l'utilisateur à la table.


VPN Client Access
Username :
New Password :
Confirm New Password :
Allow Password Change :
Yes
No
Active :
Add to list
user_1=>Active
Delete
Add New



Étape 8. (Facultatif) Pour modifier les informations relatives à un utilisateur, cliquez sur l'utilisateur spécifique dans le tableau. Modifiez les informations nécessaires, puis cliquez sur Update. Vous ne pouvez pas modifier le nom d'utilisateur.

Étape 9. (Facultatif) Pour supprimer un utilisateur de la table, cliquez sur l'utilisateur spécifique dans la table, puis cliquez sur Supprimer.

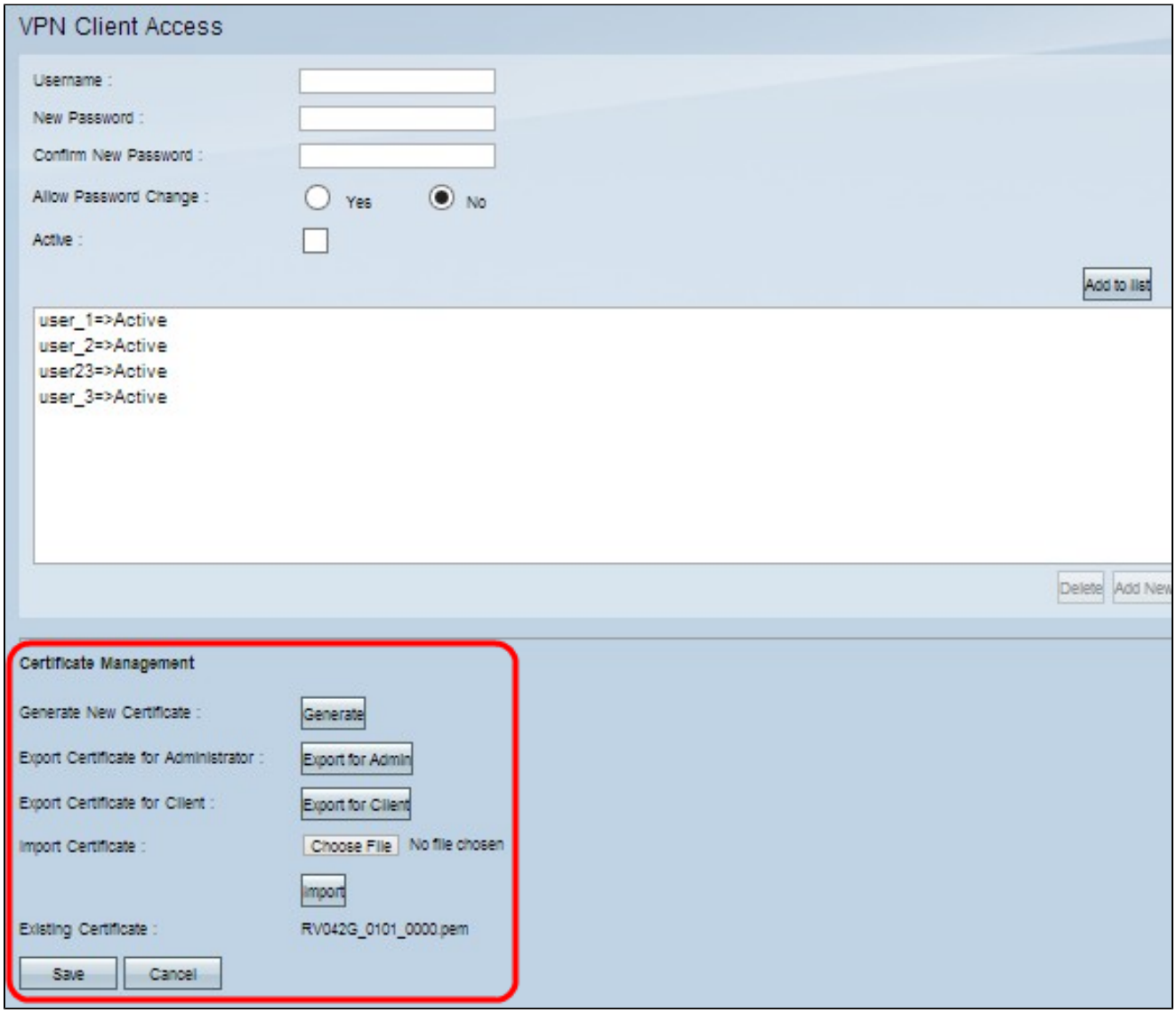
Étape 10. (Facultatif) Pour ajouter un nouvel utilisateur VPN, cliquez sur Add New et suivez les étapes 1 à 7.

Étape 11. Cliquez sur Save pour enregistrer les paramètres.

Gestion des certificats

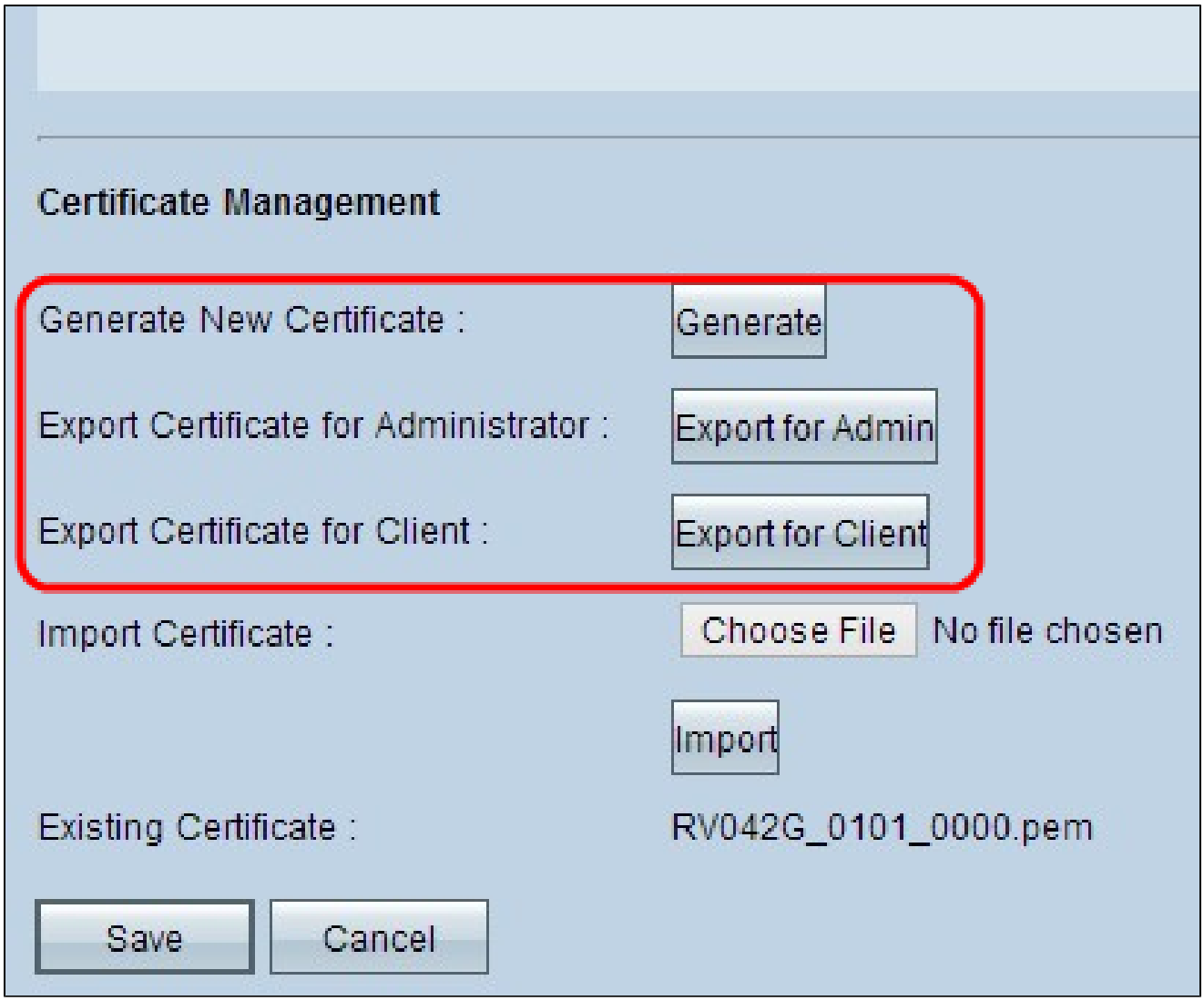
Remarque : il est possible d'avoir une connexion VPN sans certificat sur le PC. Cependant, un certificat augmentera la sécurité du VPN.

Étape 1. Connectez-vous à l'utilitaire de configuration du routeur et choisissez VPN > VPN Client Access. La page VPN Client Access s'ouvre. Faites défiler jusqu'à la zone Certificate Management.

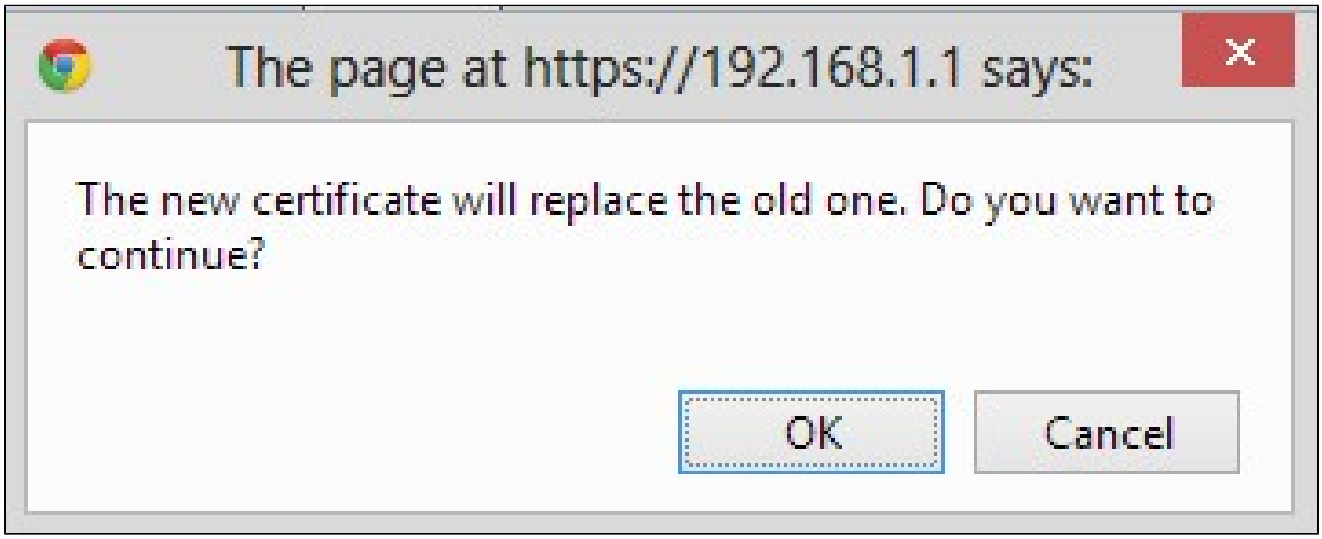


Le certificat actuel s'affiche dans le champ Certificat existant. Si vous souhaitez exporter un certificat vers votre PC, allez à la section Export Certificate. Si vous souhaitez importer un certificat de votre PC vers le routeur, allez à la section Import Certificate.

Exporter le certificat



Étape 1. (Facultatif) Pour générer un nouveau certificat pour le routeur, cliquez sur Generate. Le certificat précédent est remplacé par le nouveau certificat. Une fenêtre de message d'avertissement s'affiche :



Étape 2. Cliquez sur OK pour continuer avec un nouveau certificat et remplacer l'ancien certificat par le nouveau.

Étape 3. (Facultatif) Pour télécharger et enregistrer un certificat en tant que sauvegarde sur votre ordinateur, cliquez sur Export for Admin. Un certificat administratif contient la clé privée et est utilisé comme sauvegarde lors de la réinitialisation d'usine.

Étape 4. Cliquez sur Export for Client pour télécharger un certificat client et l'enregistrer sur votre PC. Il est utilisé lorsque l'utilisateur accède au tunnel VPN. Le routeur enregistre un fichier .pem sur votre ordinateur.

Remarque : pour enregistrer un fichier .pem dans le magasin de certificats sous Windows, il doit être converti en fichier .pfx ou .p12.

Importer un certificat

Étape 1. Cliquez sur Choose File et choisissez le certificat que vous souhaitez importer. Le type de fichier doit être .pem.

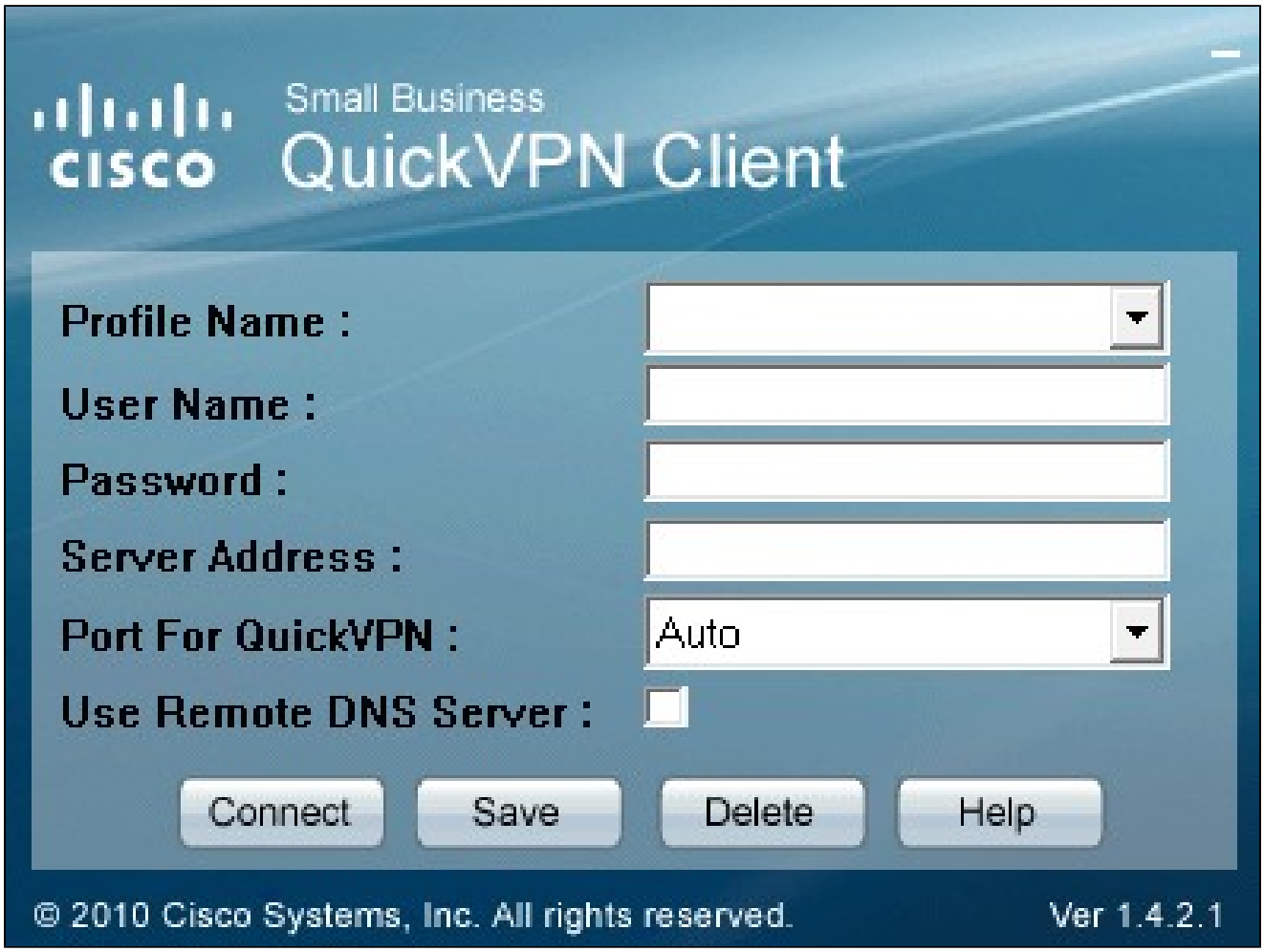
Étape 2. Cliquez sur Import pour importer le certificat.

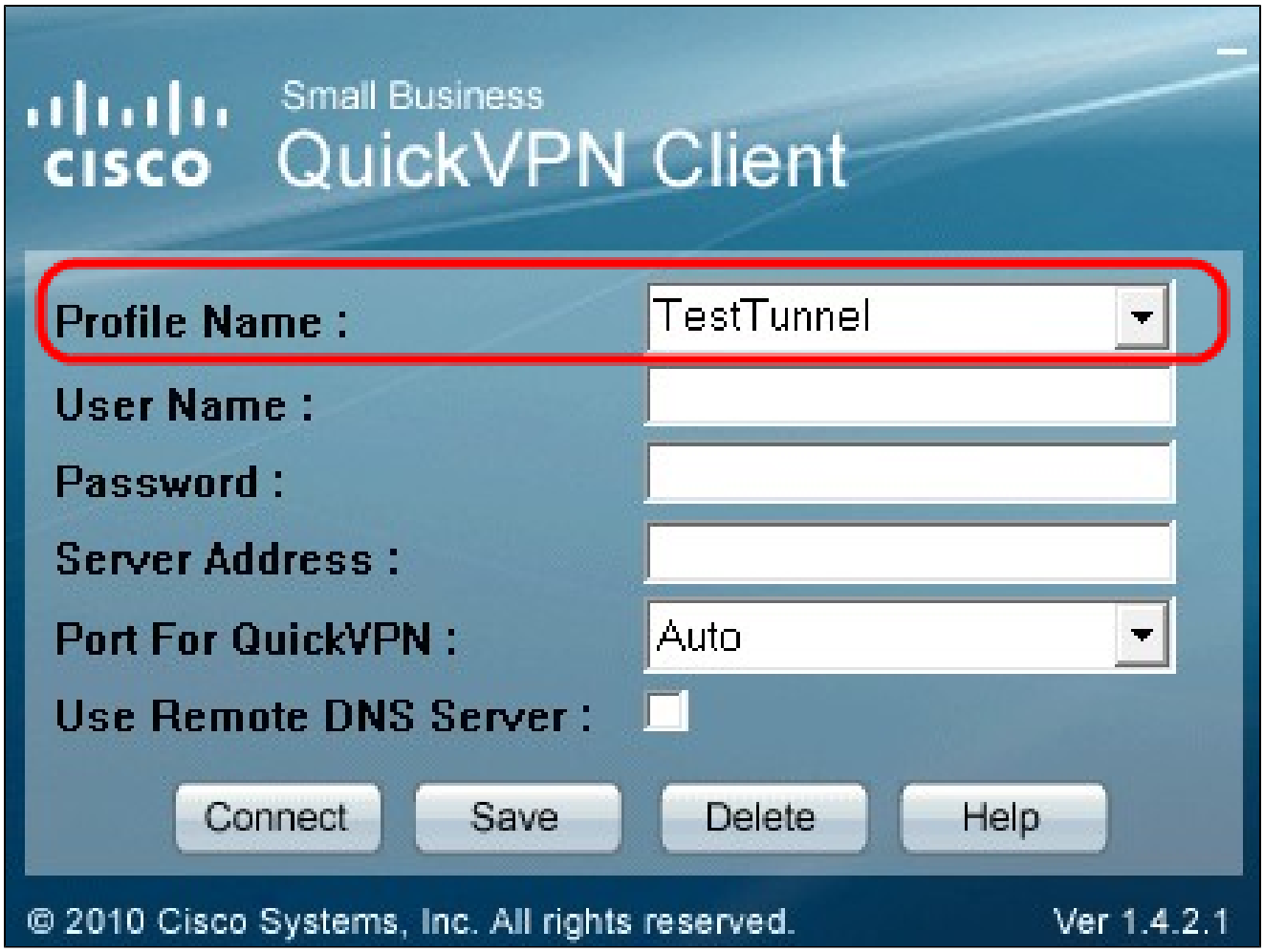
Étape 3. Cliquez sur Save pour enregistrer les paramètres.

Configuration de Cisco QuickVPN

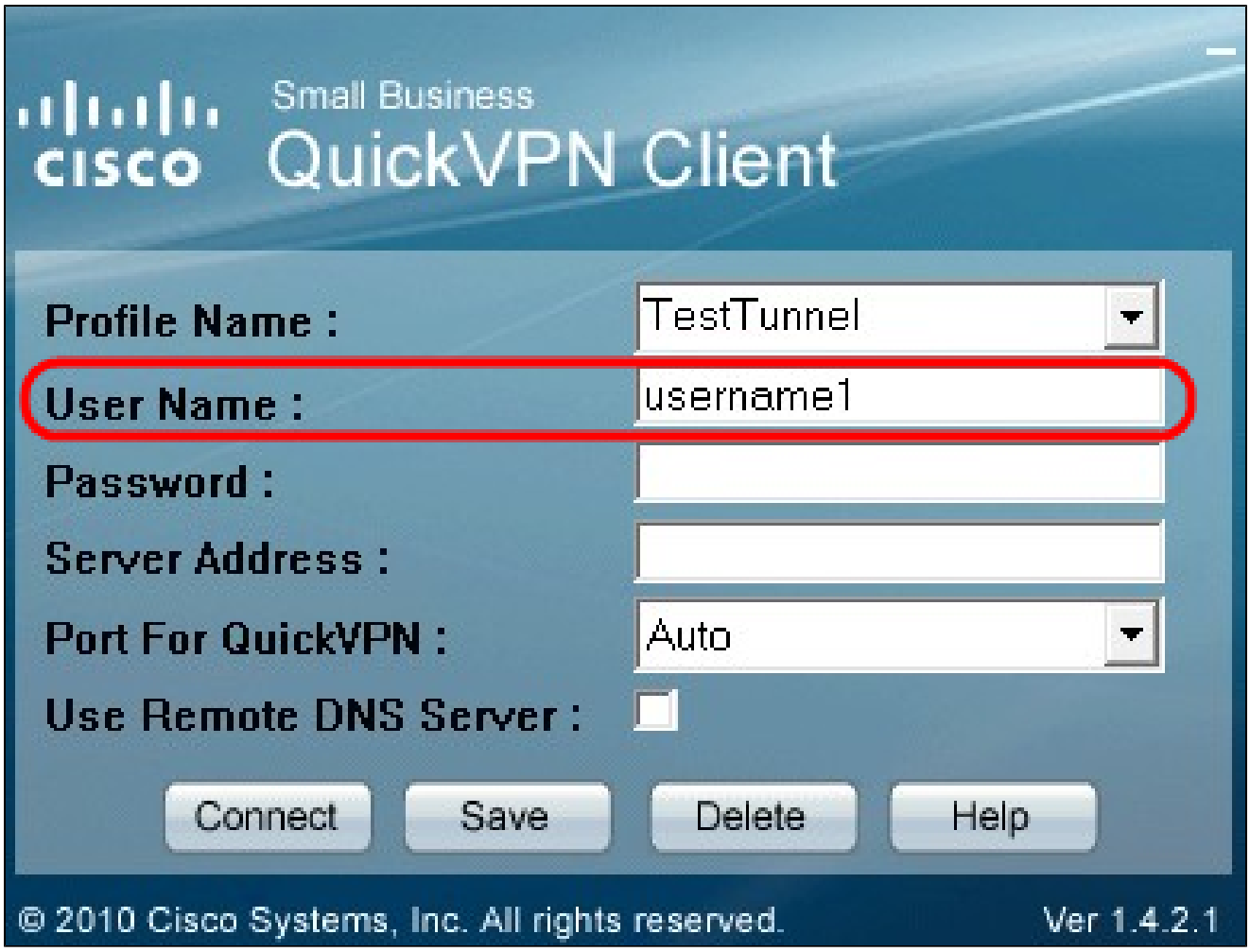
Remarque : ce logiciel est uniquement pris en charge par les systèmes d'exploitation Windows. Vous pouvez télécharger ce logiciel sur le site Web officiel de Cisco (www.cisco.com).

Étape 1. Ouvrez le logiciel Cisco QuickVPN.

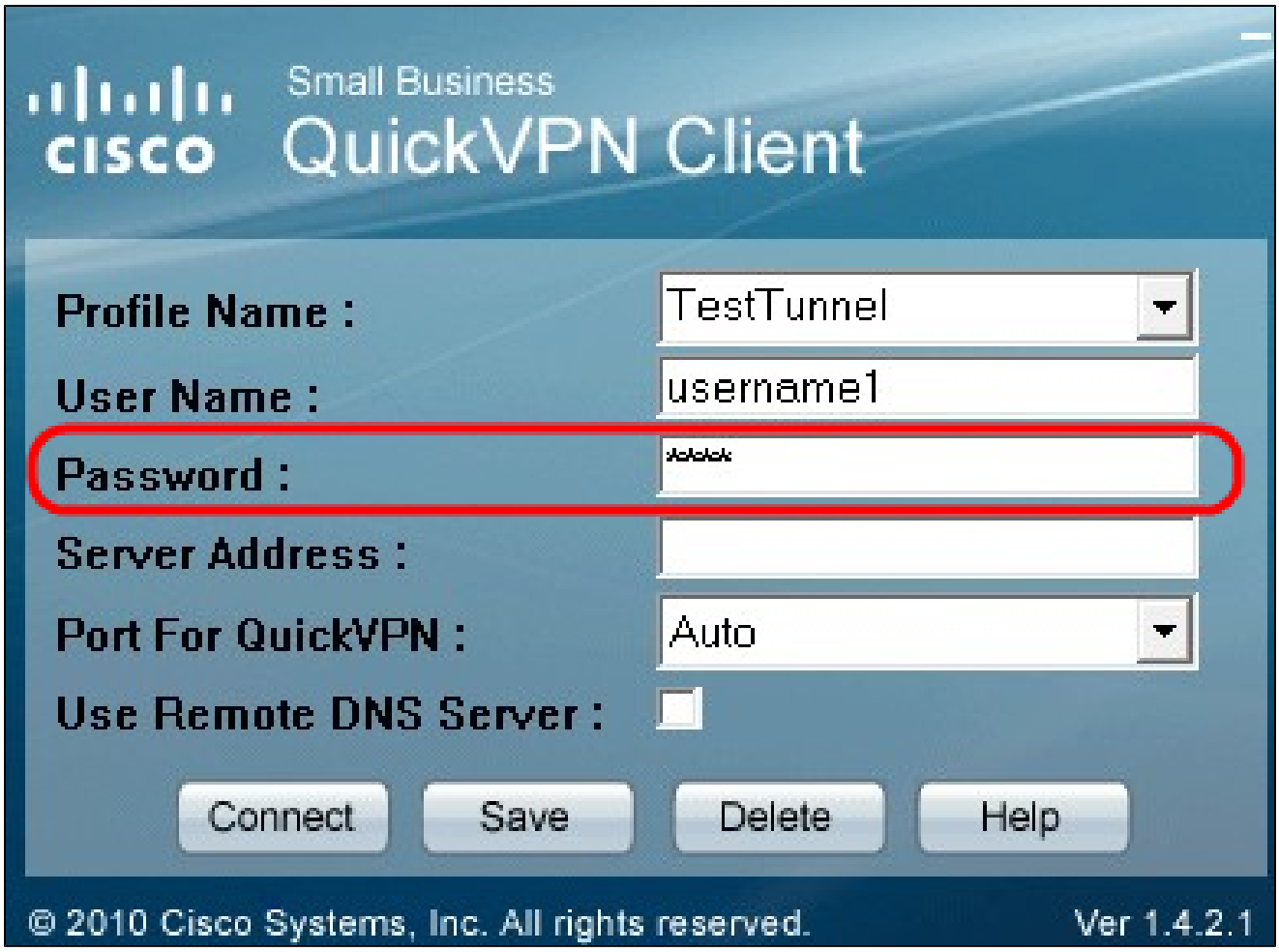




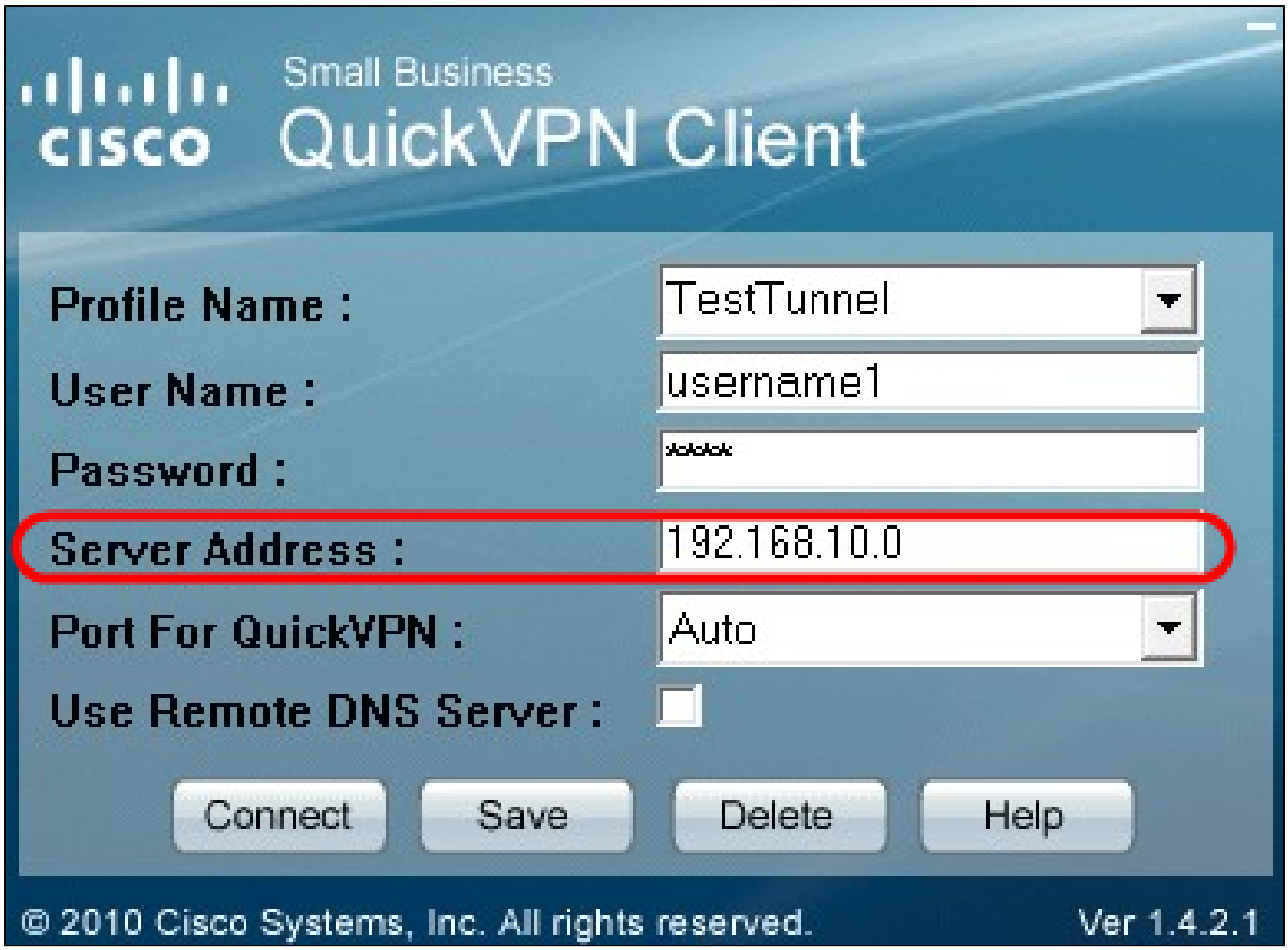
Étape 2. Dans le champ Profile Name, saisissez le nom du tunnel VPN créé sur le routeur filaire RV.



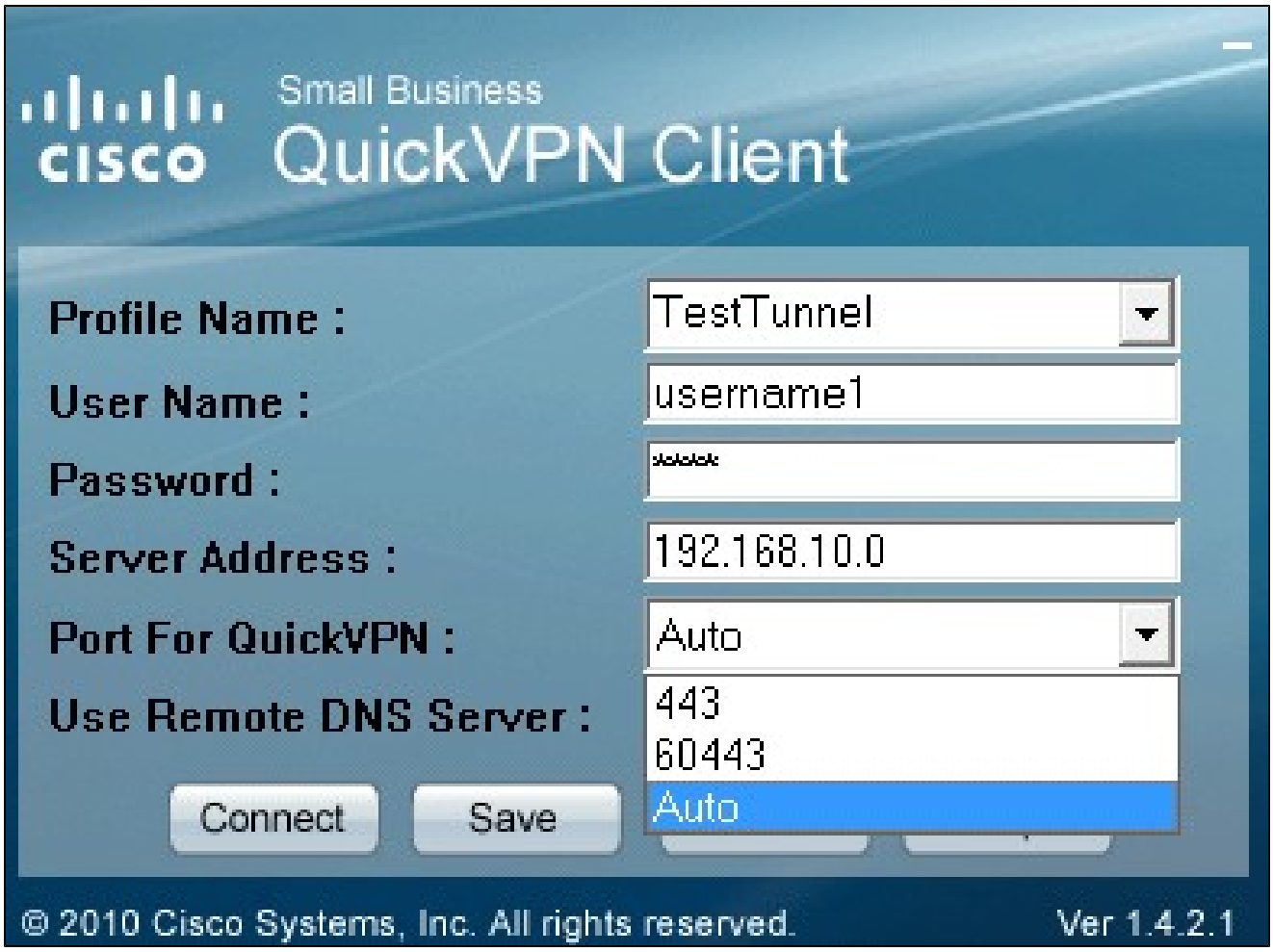
Étape 3. Dans le champ User Name (Nom d'utilisateur), saisissez le nom d'utilisateur attribué au routeur.



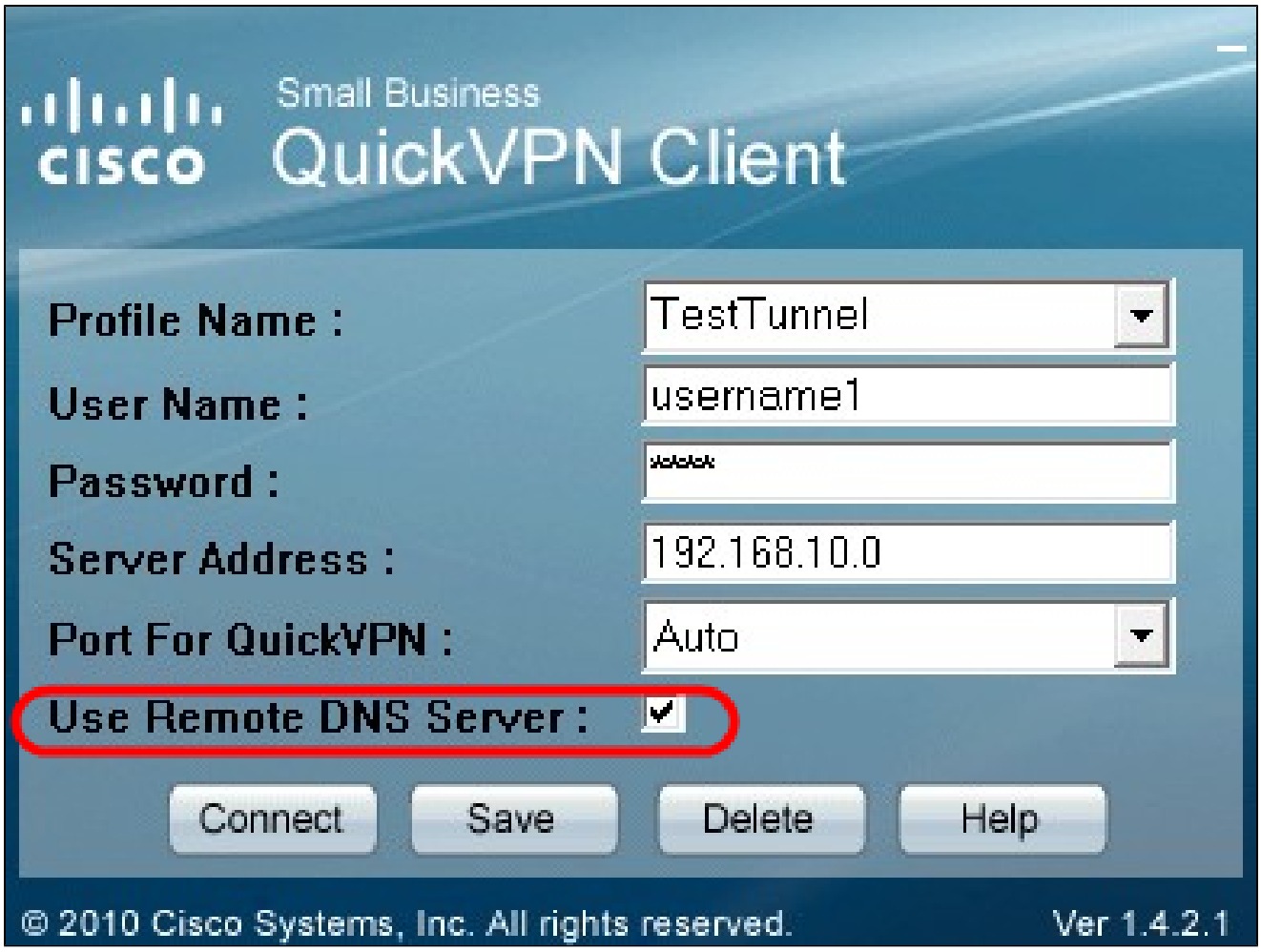
Étape 4. Dans le champ Mot de passe, saisissez le mot de passe attribué au routeur.



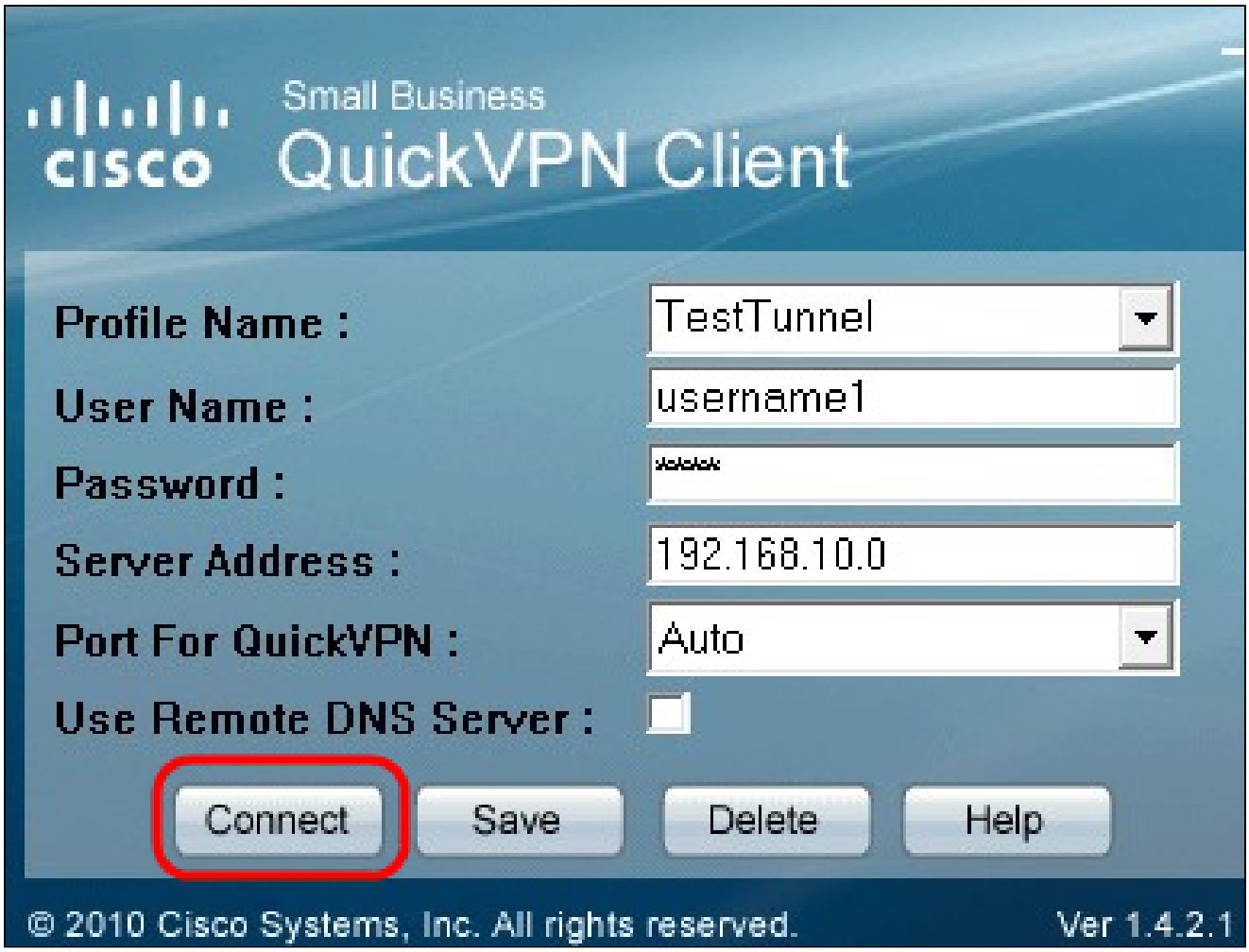
Étape 5. Dans le champ Server Address, saisissez l'adresse IP du routeur utilisé pour le VPN.



Étape 6. Dans la liste déroulante Use Remote DNS Server, sélectionnez le numéro de port approprié. Auto est la valeur par défaut, qui sélectionne automatiquement le numéro de port en fonction des paramètres VPN.



Étape 7. Cochez la case Use Remote DNS Server si vous avez un serveur DNS qui peut résoudre des noms de domaine ; sinon, décochez-la et utilisez vos paramètres de réseau VPN.



Étape 8. Cliquez sur Connect pour accéder au VPN.

Étape 9. (Facultatif) Pour enregistrer la configuration, cliquez sur Save.

Étape 10. (Facultatif) Pour supprimer une configuration enregistrée, cliquez sur Delete.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.