# Exemple de configuration de Cisco Secure Services Client avec WPA PEAP/GTC

## Contenu



## Introduction

Ce document décrit comment configurer le Protocole WPA (Wi-Fi Protected Access) symbolique de la carte du Protected Extensible Authentication Protocol (PEAP) /Generic (GTC) sur le Cisco Secure Services Client.

## Conditions préalables

### Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Version 4.0 de Cisco Secure Services ClientLe Cisco Secure Services Client est disponible pour le téléchargement du centre de logiciel de Cisco.com (clients enregistrés seulement).
- Windows XP SP2 ou 2000 minimum SP4

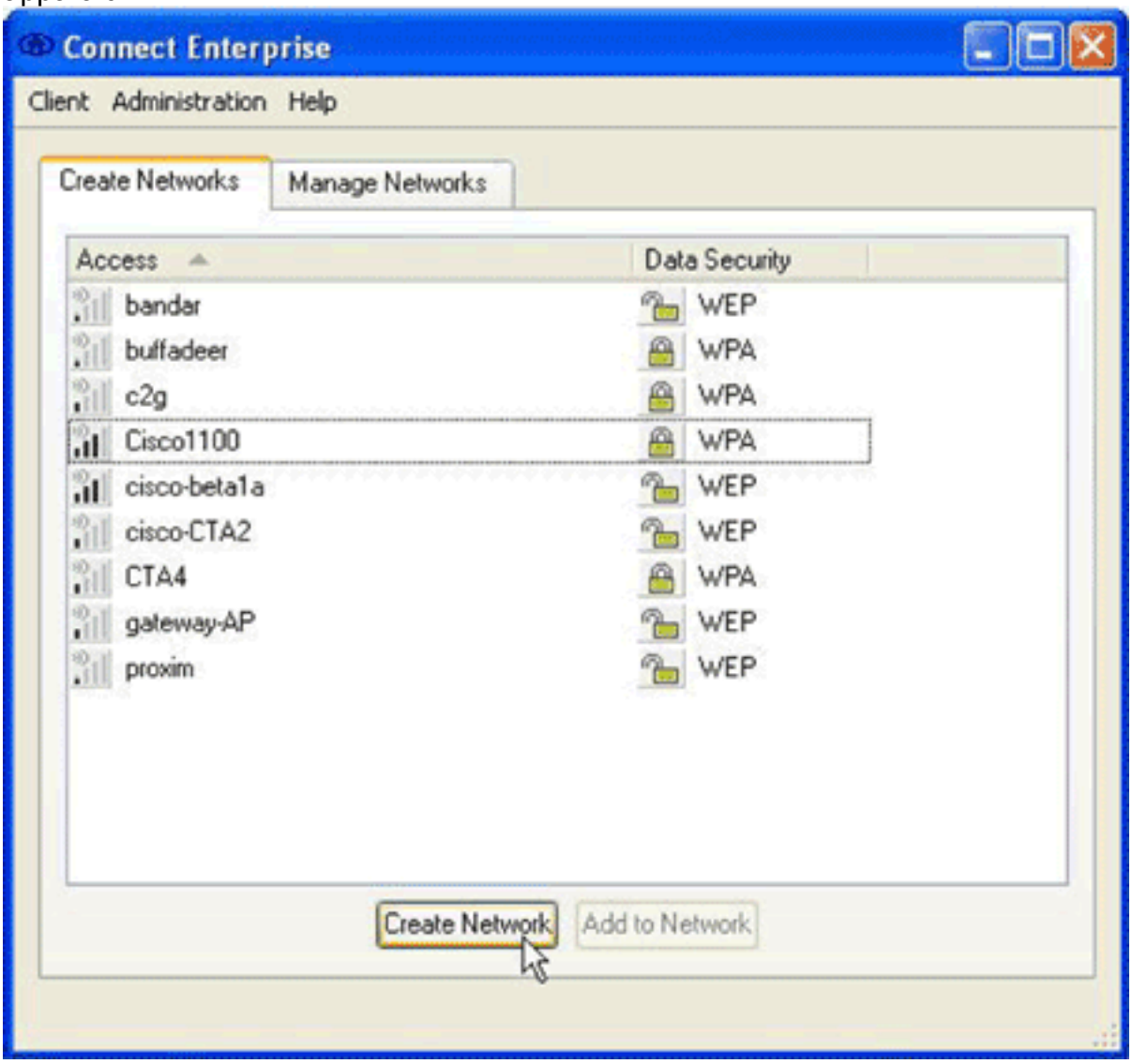
### Conventions

Pour plus d'informations sur les conventions des documents, reportez-vous au document Conventions relatives aux conseils techniques Cisco.

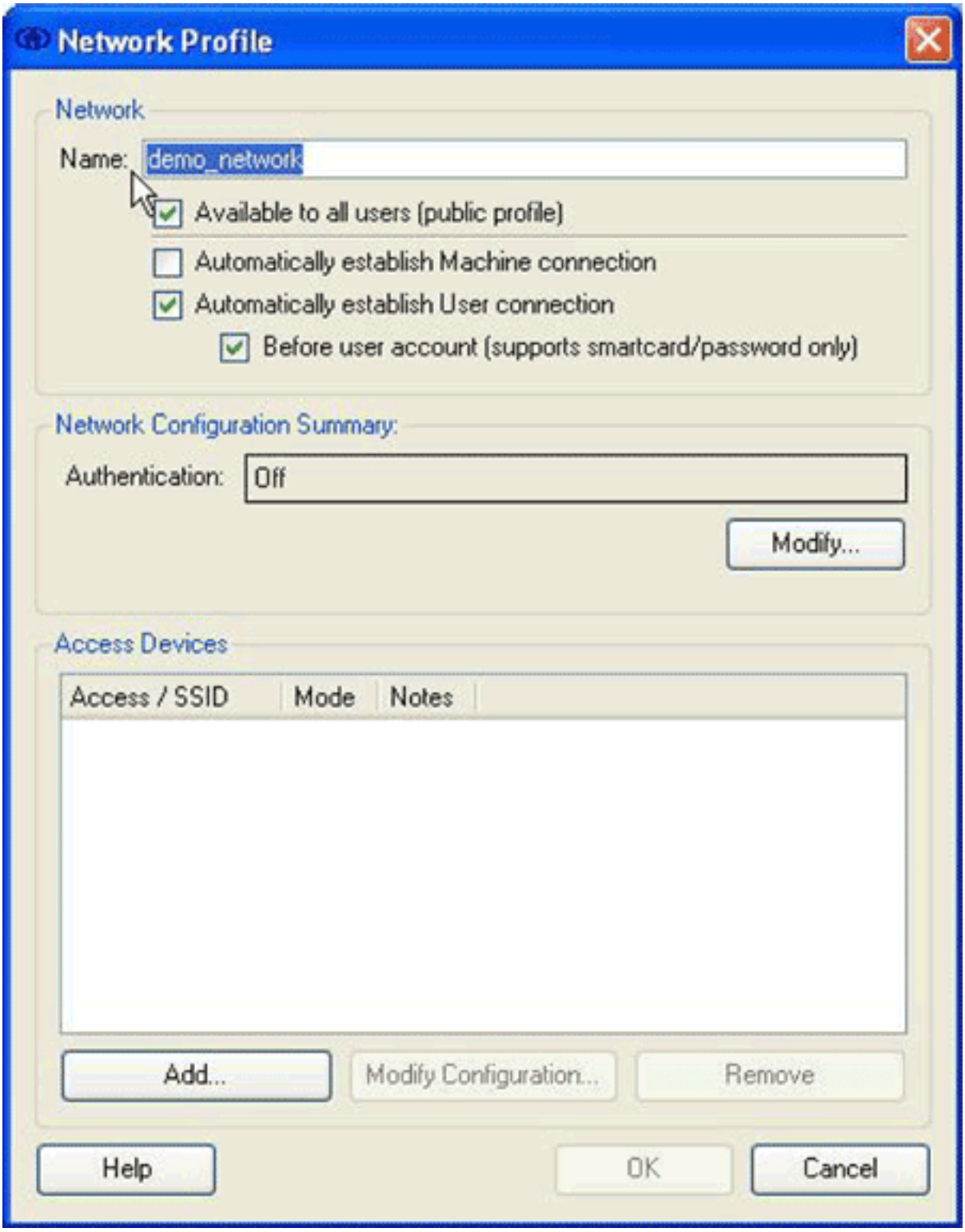
## Configurez le Cisco Secure Services Client avec PEAP/GTC WPA

Pour configurer le Cisco Secure Services Client avec PEAP/GTC WPA, terminez-vous ces étapes :

1. Cliquez avec le bouton droit l'icône de la barre d'état système de Cisco Secure Services Client, et choisissez **ouvert**.**Remarque:** Si vous n'êtes pas connecté à un réseau, votre icône de la barre d'état système est faible.La boîte de dialogue d'entreprise de connecter apparaît.



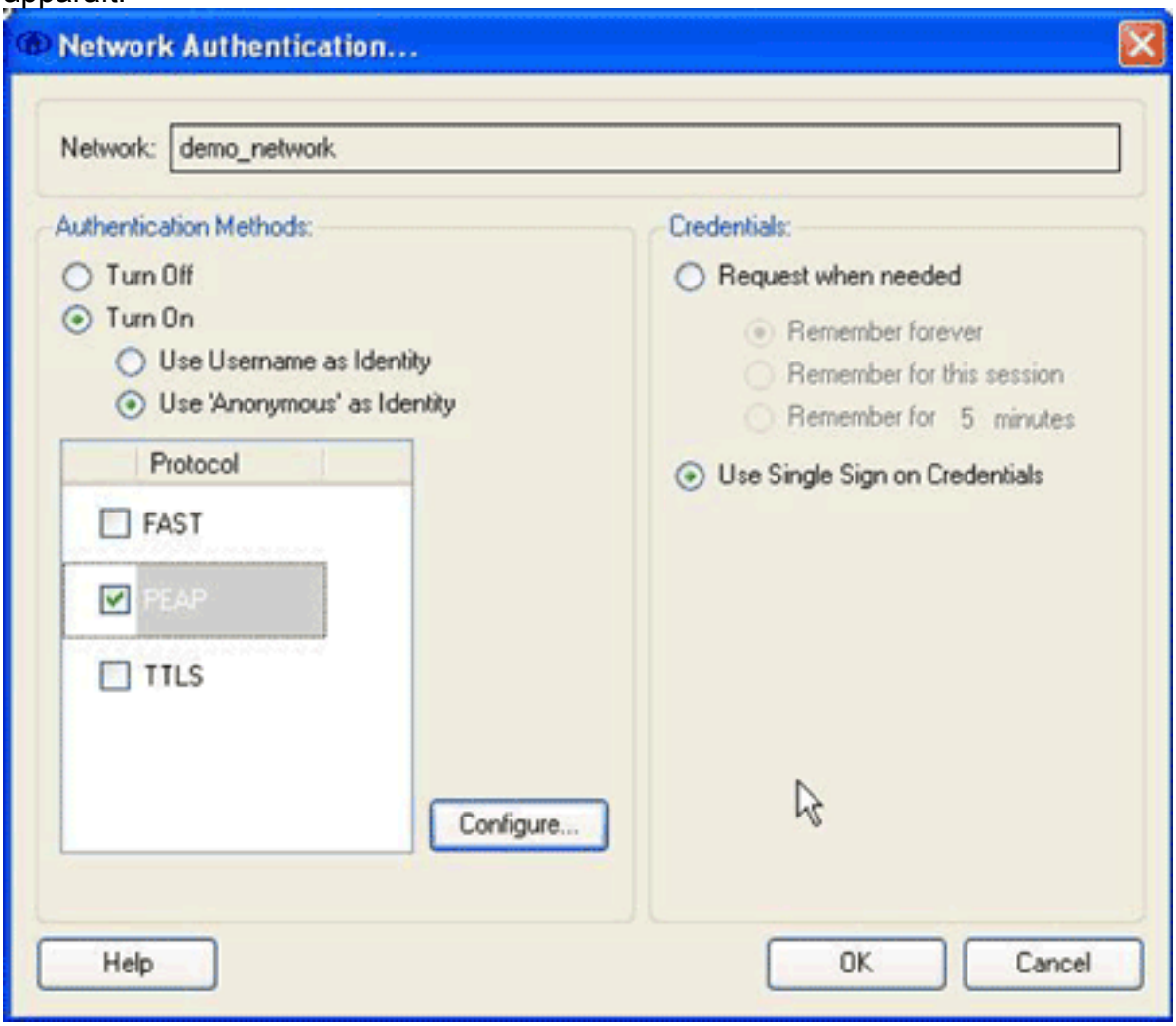

2. Cliquez sur l'onglet de **réseaux de création**.La région de réseaux de création affiche les réseaux qui annoncent leur Identifiant SSID (Service Set Identifier).
3. Cliquez sur le bouton de **réseau de création**.La boîte de dialogue de profil réseau apparaît.



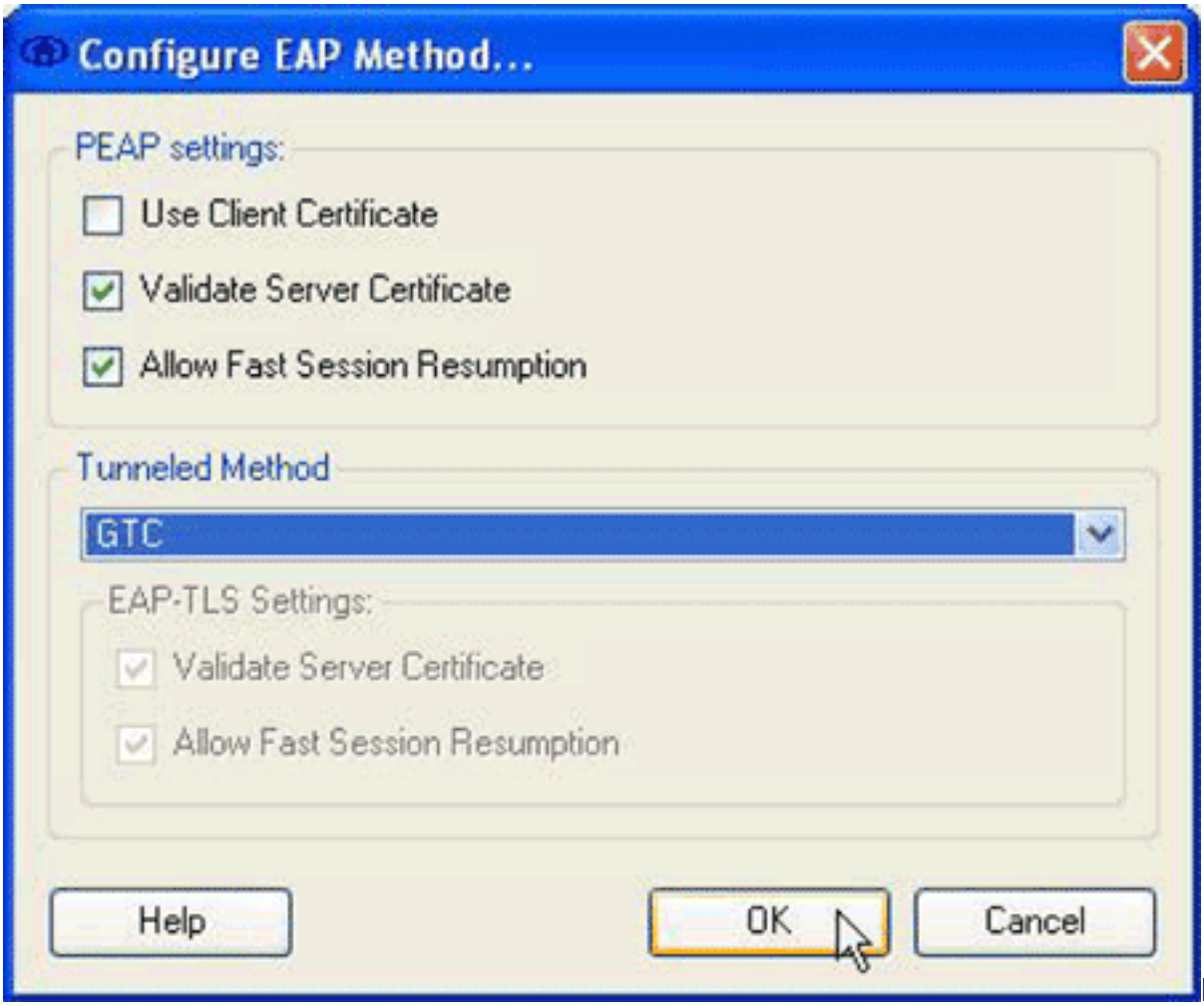

4. Dans la région de réseau, configurez ces options :Dans la zone d'identification, écrivez un nom pour votre réseau.Ce nom apparaît comme SSID pour ce réseau. Pour cet exemple, le nom est *demo_network*.Cochez le **disponible dans toute la** case d'**utilisateurs (profil public)**.Cochez **automatiquement la** case de **connexion utilisateur d'établissement**, et vérifiez automatiquement la case de connexion d'ordinateur d'établissement n'est pas coché.Cochez **avant** case de **compte utilisateur (carte à puce/mot de passe de supports seulement)**.**Remarque:** Quand **avant que la** case de **compte utilisateur (carte à puce/mot de passe de supports seulement)** soit cochée, l'authentification poursuit juste après que des qualifications sont entrées, mais avant que la connexion de domaine se produit. Si vous utilisez des certificats utilisateurs, ne cochez pas **avant** case de **compte utilisateur (carte à puce/mot de passe de supports seulement)**. Puisqu'ils ne sont pas disponibles avant la connexion de Windows, vous ne pouvez pas utiliser des certificats utilisateurs avec des

connexions de domaine.

5. Dans le secteur récapitulatif de configuration réseau, cliquez sur le bouton de **modifier**.La boîte de dialogue d'authentification de réseau apparaît.

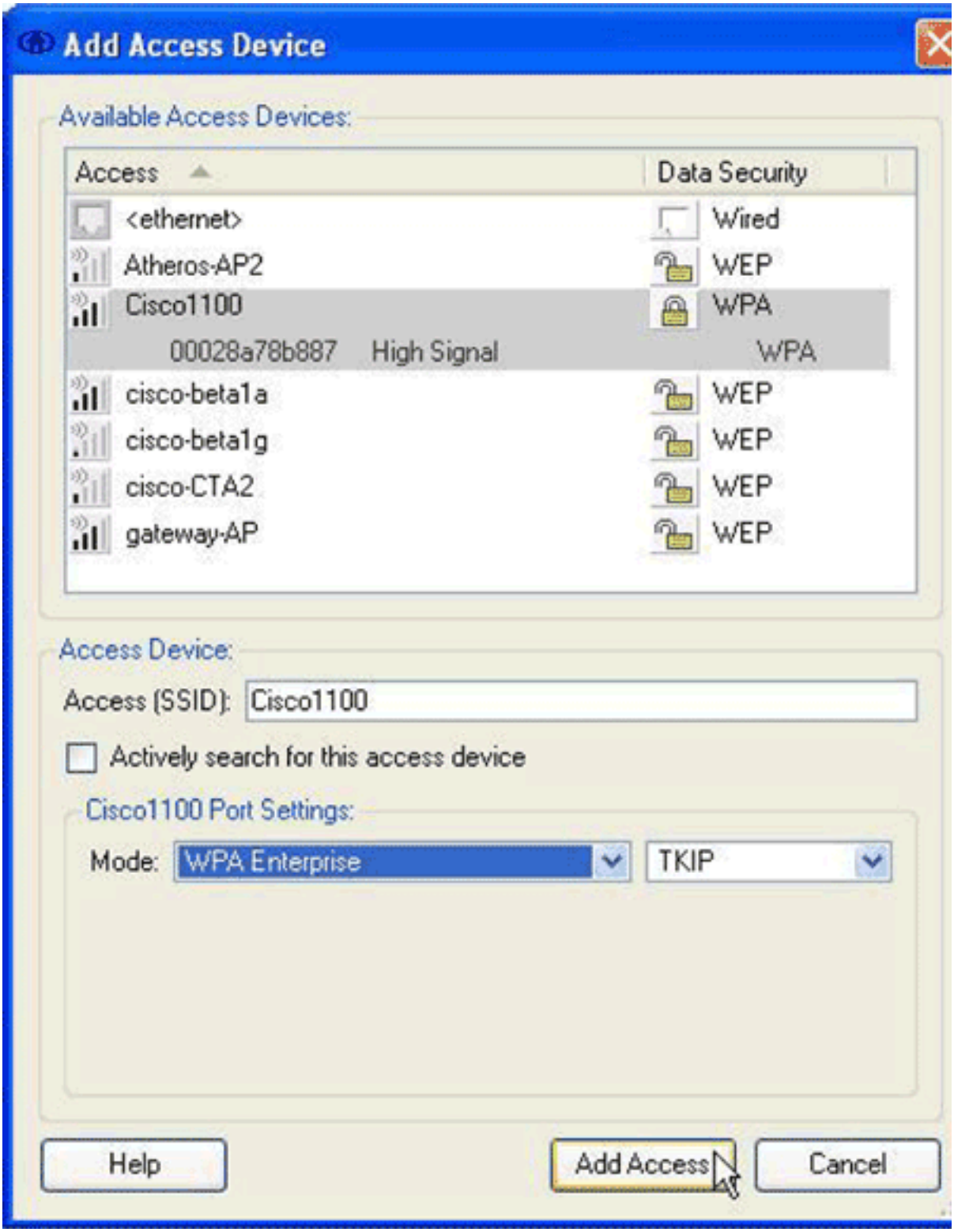



6. Dans la boîte de dialogue d'authentification de réseau, configurez ces options :Dans la région de qualifications, cliquez sur l'**utilisation simple se connectent la** case d'option de **qualifications**.Dans la région de méthodes d'authentification, cliquez sur la case d'option d'**activer**, et puis cliquez sur l'**utilisation « anonyme » comme identité**.La case d'option d'activer remplit liste de protocole affichée dans la région de méthodes d'authentification. L'utilisation « anonyme » comme la case d'option d'identité limite la liste seulement aux Protocoles d'authentification percés un tunnel.Cochez la case **PEAP**, et puis cliquez sur Configure.La boîte de dialogue de méthode d'EAP de configurer apparaît.



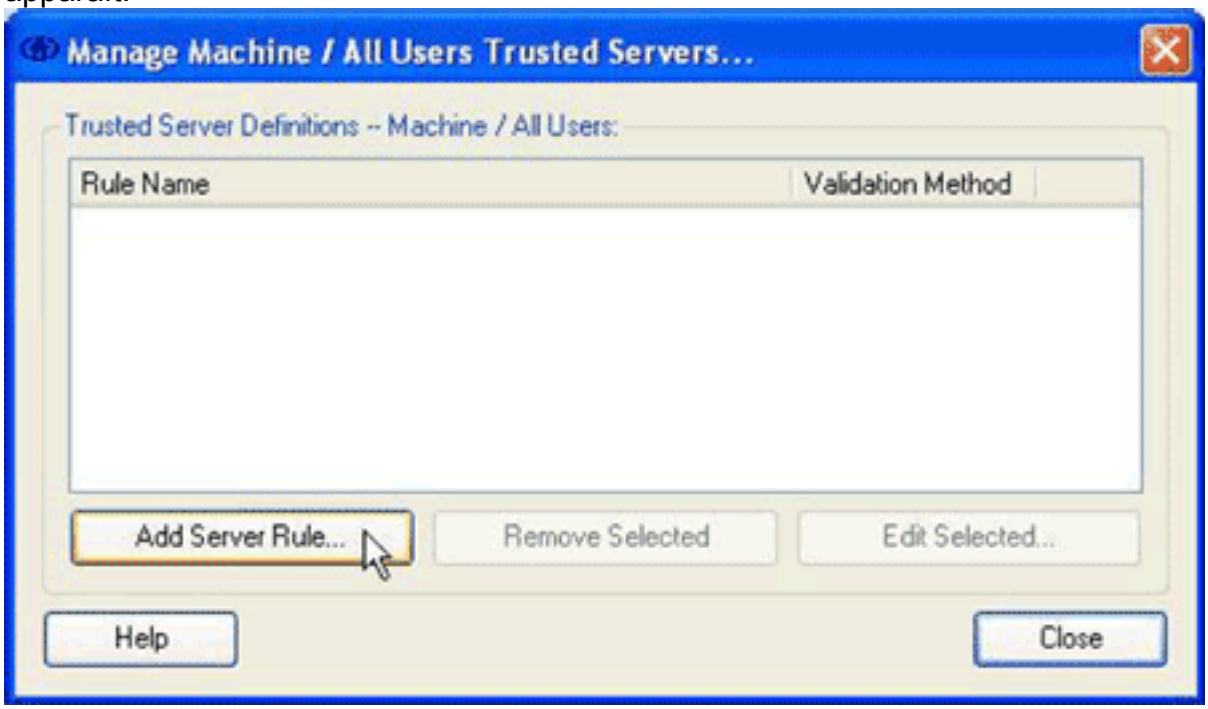
Décochez la case de **certificat client d'utilisation**.Vérifiez le **certificat de serveur de validation** et **permettez les** cases **rapides de reprise de session**.Du menu déroulant percé un tunnel de méthode, choisissez **GTC**.Cliquez sur OK pour retourner dans la boîte de dialogue d'authentification de réseau, et puis cliquez sur OK pour retourner dans la boîte de dialogue de profil réseau.

7. Dans la région de périphériques d'Access de la boîte de dialogue de profil réseau, cliquez sur Add.La boîte de dialogue de périphérique d'Access d'ajouter apparaît.

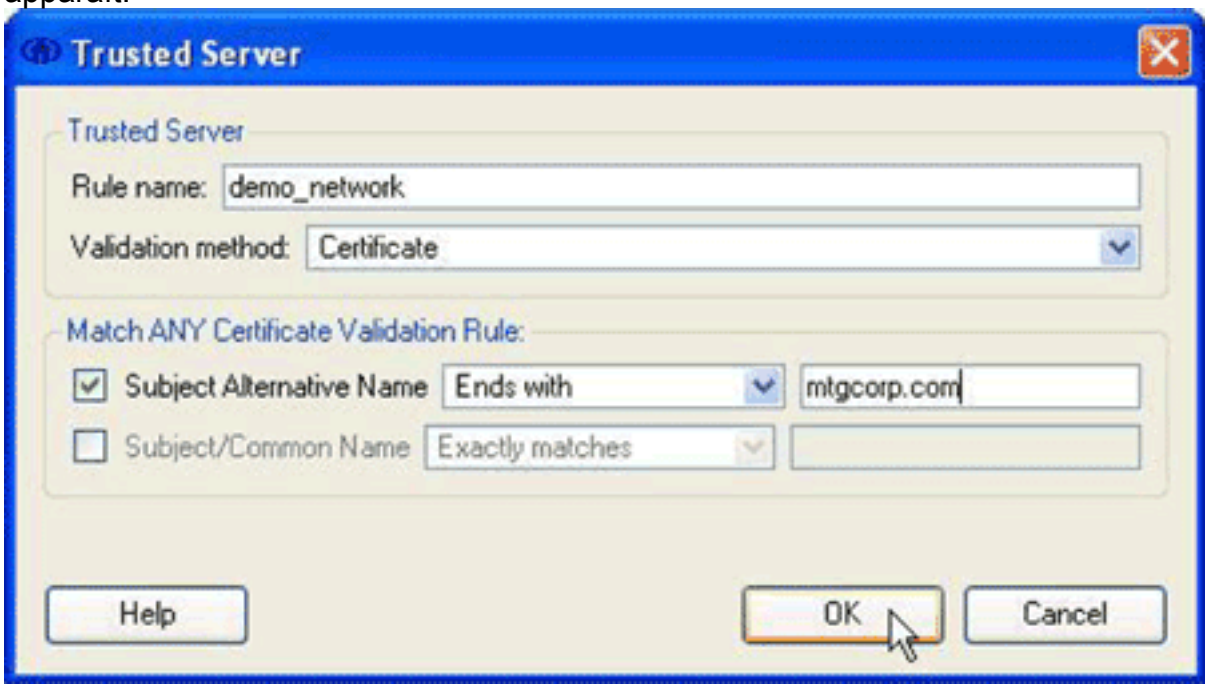



8. Dans la boîte de dialogue de périphériques d'Access d'ajouter, choisissez le périphérique que vous voulez configurer, et puis cliquez sur Add **Access.Remarque:** Si le périphérique que vous voulez configurer est dans la marge, le SSID pour ce périphérique apparaît dans la liste de périphériques disponible d'Access. Si le périphérique n'apparaît pas, écrivez le SSID pour le périphérique dans le domaine d'Access (SSID), écrivez les configurations de port dans la région de configurations de port de Cisco 1100, et puis cliquez sur Add **Access**.
9. Dans la boîte de dialogue de profil réseau, cliquez sur OK pour retourner dans la boîte de dialogue d'entreprise de connecter.
10. Dans la boîte de dialogue d'entreprise de connecter, choisissez **fait confiance que les serveurs > gèrent l'ordinateur/tous les utilisateurs faits confiance des serveurs du** menu de client.L'ordinateur de gérer/tous utilisateurs a fait confiance que boîte de dialogue de

serveurs
apparaît.




11. Cliquez sur Add la **règle de serveur**.La boîte de dialogue de confiance de serveur apparaît.



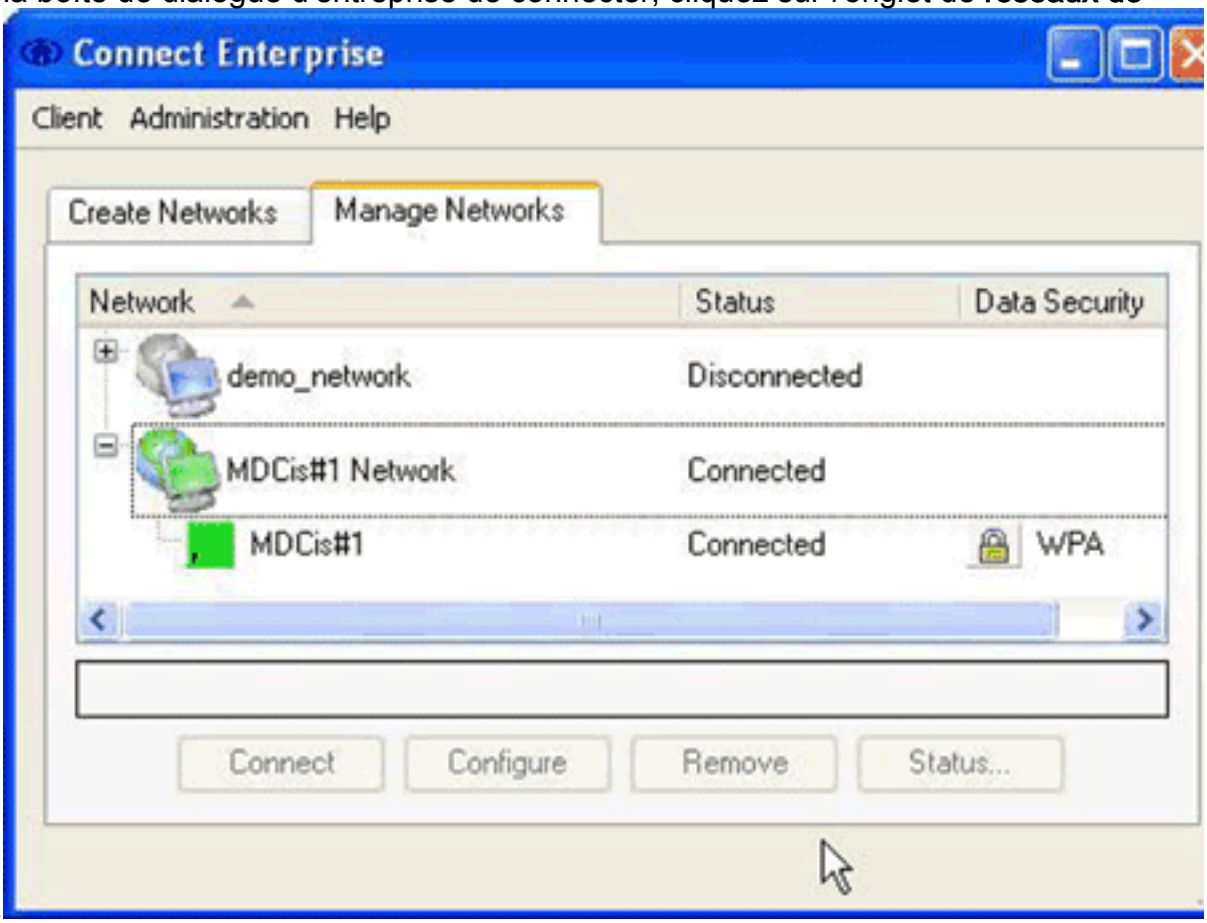

12. Dans la boîte de dialogue de confiance de serveur, configurez ces options :Dans la zone d'identification de règle, écrivez un nom pour la règle.Du menu déroulant de méthode de validation, choisissez le **certificat**.Dans la région de règle de validation de certificat de match any, configurez les options pour la règle.Pour construire une règle, vous devez savoir que le contenu du certificat de serveur et écrire ces valeurs dans la validation de certificat de match any ordonne la zone. Par exemple, si le nom alternatif soumis contient le nom de domaine d'un serveur, *mtgcorpserver.mtgcorp.com*, choisissent des **extrémités avec du** menu déroulant alternatif soumis de nom, et puis entrent dans **mtgcorp.com** dans le champ texte.Cliquez sur OK pour retourner dans l'ordinateur de gérer/tous boîte de dialogue de serveurs de confiance par utilisateurs.
13. Dans l'ordinateur de gérer/tous utilisateurs a fait confiance à la boîte de dialogue de

serveurs, cliquent sur **près du** retour dans la boîte de dialogue d'entreprise de connecter. La configuration est complète, et vous pouvez se connecter au réseau.

## Connectez au réseau

Pour se connecter à votre nouveau réseau, terminez-vous ces étapes :

1. Dans la boîte de dialogue d'entreprise de connecter, cliquez sur l'onglet de **réseaux de gérer**.




2. Le démonter de n'importe quel réseau qui est connecté à l'adaptateur l'a utilisé par votre nouveau réseau.
3. De la liste des réseaux, sélectionnez le nouveau profil réseau, et le clic **se connectent**.

Sur la configuration et la connexion réussies, les affichages d'icône de la barre d'état système de Cisco Secure Services Client verdissent.

**Remarque:** Si le logiciel de protection antivirus est installé sur votre ordinateur et il est configuré pour analyser le répertoire de log de Cisco Secure Services Client, vous pouvez éprouver les cycles CPU élevés avec l'authentification de Cisco Secure Services Client. Pour améliorer la représentation, configurez votre logiciel de protection antivirus pour exclure le répertoire de log de Cisco Secure Services Client.

## Informations connexes

- Support et documentation techniques - Cisco Systems