# Exemple de configuration d'un serveur EAP local dans un réseau sans fil unifié Cisco

## Contenu



## Introduction

Ce document décrit la configuration d'un serveur local Extensible Authentication Protocol (EAP) dans un contrôleur de réseau local sans fil de Cisco (WLC) pour l'authentification des utilisateurs sans fil.

L'authentification EAP locale est une méthode qui permet d'authentifier localement des utilisateurs et des clients sans fil. Il est conçu pour être utilisé dans les bureaux distants qui souhaitent maintenir la connectivité aux clients sans fil lorsque le système principal est perturbé ou que le serveur d'authentification externe tombe en panne. Lorsque vous activez le protocole EAP local, le contrôleur sert de serveur d'authentification et de base de données utilisateur locale, supprimant ainsi la dépendance à l'égard d'un serveur d'authentification externe. Le protocole EAP local récupère les informations d'identification des utilisateurs de la base de données locale des utilisateurs ou de la base de données principale LDAP (Lightweight Directory Access Protocol) pour authentifier les utilisateurs. Le protocole EAP local prend en charge les protocoles LEAP (Lightweight EAP), EAP-Flexible Authentication via Secure Tunneling (EAP-FAST) et EAP-Transport Layer Security (EAP-TLS) entre le contrôleur et les clients sans fil.

Notez que le serveur EAP local n'est pas disponible s'il existe une configuration de serveur RADIUS externe globale dans le WLC. Toutes les demandes d'authentification sont transmises au RADIUS externe global jusqu'à ce que le serveur EAP local soit disponible. Si le WLC perd la connectivité au serveur RADIUS externe, le serveur EAP local devient actif. S'il n'y a pas de configuration globale du serveur RADIUS, le serveur EAP local devient immédiatement actif. Le serveur EAP local ne peut pas être utilisé pour authentifier les clients, qui sont connectés à d'autres WLC. En d'autres termes, un WLC ne peut pas transférer sa demande EAP à un autre WLC pour l'authentification. Chaque WLC doit avoir son propre serveur EAP local et sa base de données individuelle.

**Remarque :** utilisez ces commandes afin d'empêcher WLC d'envoyer des requêtes à un serveur RADIUS externe .

```
config wlan disable
        config wlan radius_server auth disable
        config wlan enable
```

Le serveur EAP local prend en charge ces protocoles dans la version du logiciel 4.1.171.0 et ultérieure :

- LEAP
- EAP-FAST (nom d'utilisateur/mot de passe et certificats)
- EAP-TLS

# Conditions préalables

## Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance de la configuration des WLC et des points d'accès légers (LAP) pour le fonctionnement de base
- Connaissance du protocole LWAPP (Lightweight Access Point Protocol) et des méthodes de sécurité sans fil
- Connaissance de base de l'authentification EAP locale.

## Components Used

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

- Windows XP avec carte adaptateur CB21AG et Cisco Secure Services Client Version 4.05
- Contrôleur LAN sans fil Cisco 4400 4.1.171.0
- Autorité de certification Microsoft sur le serveur Windows 2000

## Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

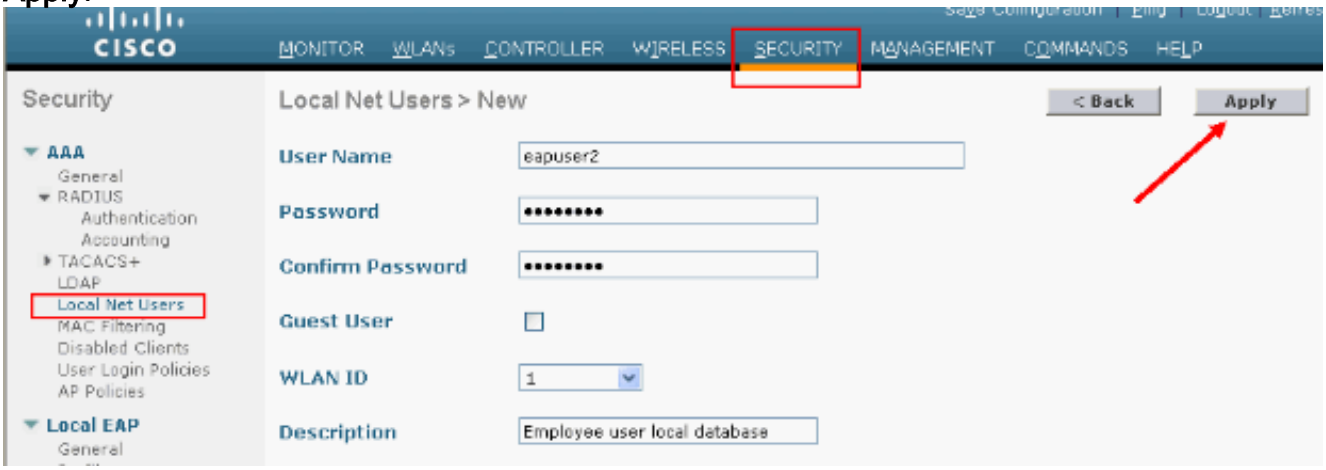
# Configurer le protocole EAP local sur le contrôleur LAN sans fil Cisco

Ce document suppose que la configuration de base du WLC est déjà terminée.

## Configuration EAP locale

Complétez ces étapes afin de configurer le protocole EAP local :

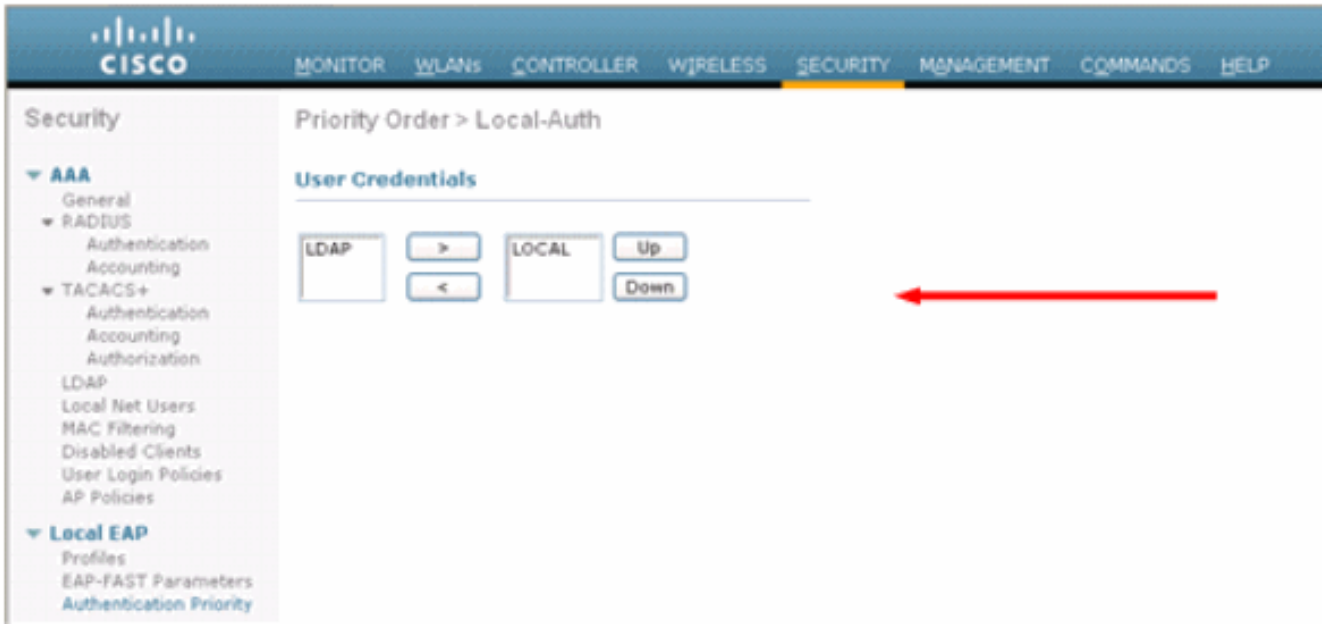
1. Ajouter un utilisateur réseau local :Àpartir de l'interface utilisateur graphique. choisissez **Security > Local Net Users > New**, saisissez le nom d'utilisateur, le mot de passe, l'utilisateur invité, l'ID WLAN et la description, puis cliquez sur **Apply**.




Àpartir de l'interface de ligne de commande, vous pouvez utiliser la commande **config netuser add** *<username>*<password><WLAN id><*description*> **:Remarque :** cette commande a été réduite à une deuxième ligne pour des raisons spatiales.

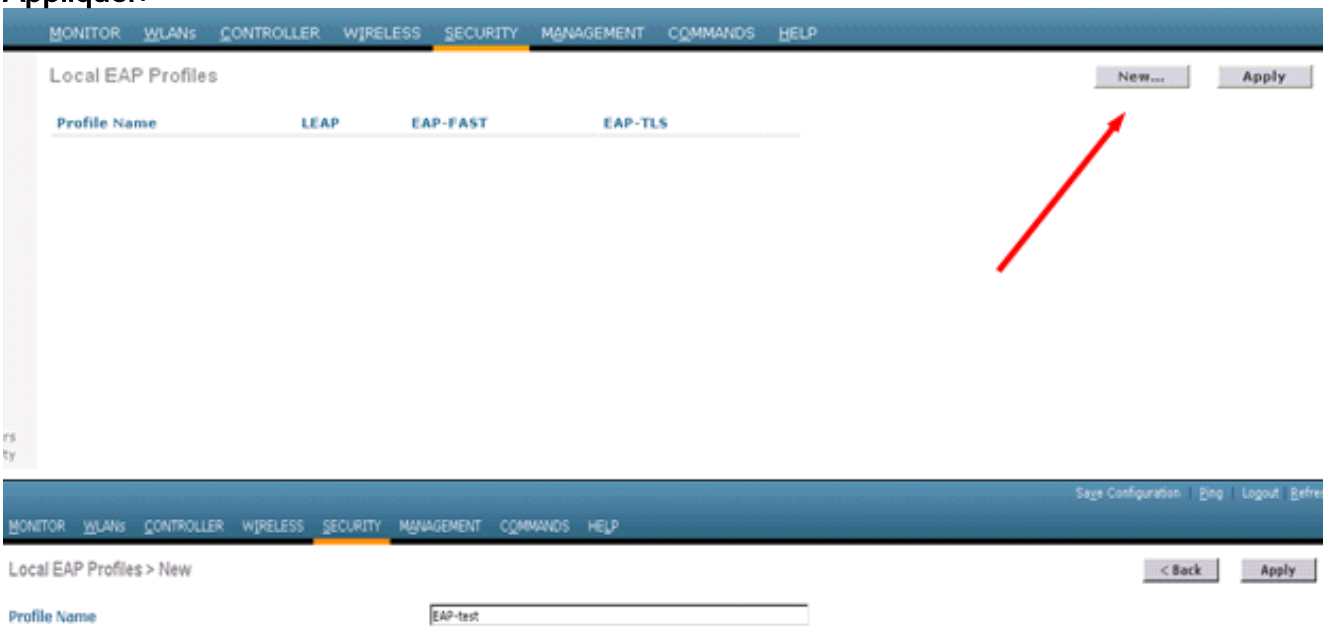
```
(Cisco Controller) >config netuser add eapuser2 cisco123 1 Employee user local database
```

2. Spécifiez l'ordre de récupération des informations d'identification de l'utilisateur.Dans l'interface utilisateur graphique, sélectionnez **Security > Local EAP > Authentication Priority**. Sélectionnez ensuite LDAP, cliquez sur le bouton "**<**" et cliquez sur **Appliquer**. Ceci place d'abord les informations d'identification de l'utilisateur dans la base de données locale.



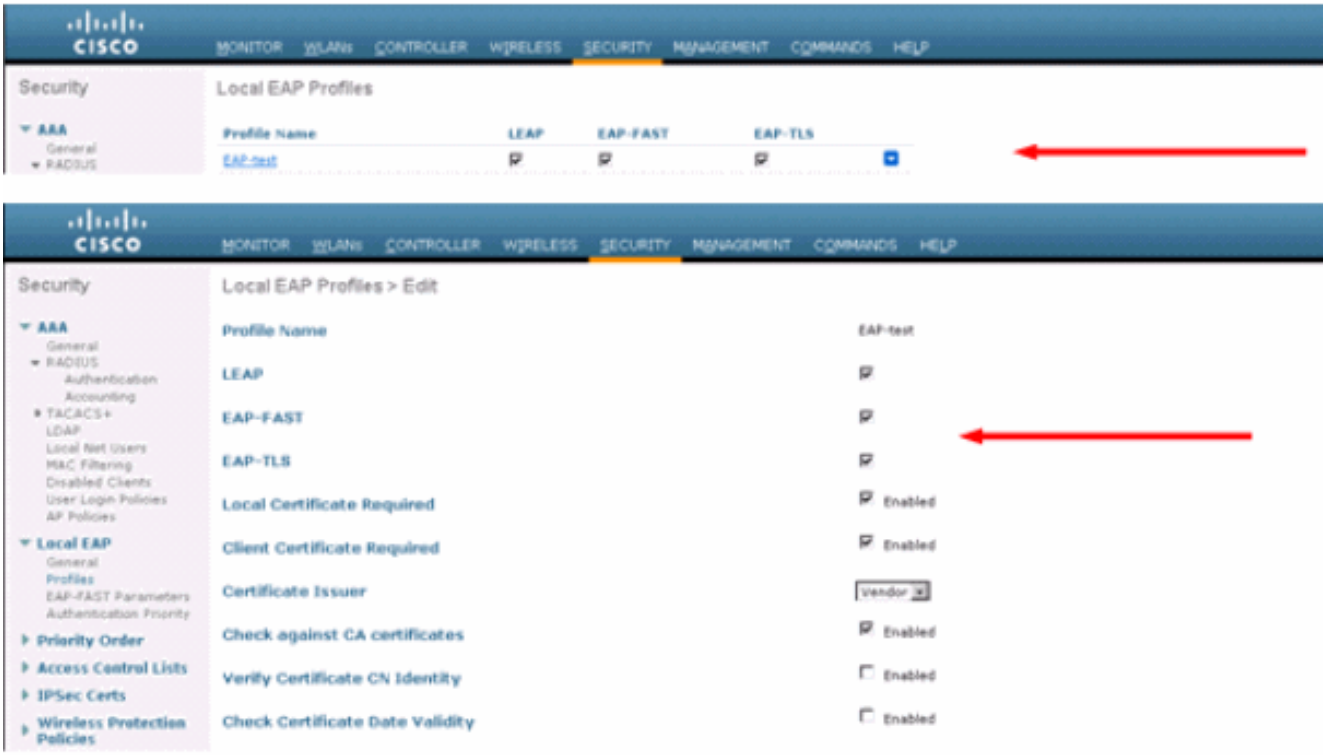

Àpartir de l'interface de ligne de commande :
`(Cisco Controller) >`**`config local-auth user-credentials local`**

3. Ajouter un profil EAP :Pour ce faire à partir de l'interface utilisateur graphique, choisissez **Security > Local EAP > Profiles** et cliquez sur **New**. Lorsque la nouvelle fenêtre apparaît, tapez le nom du profil et cliquez sur **Appliquer**.




Vous pouvez également le faire à l'aide de la commande CLI **config local-auth eap-profile add *<profile-name>*.** Dans notre exemple, le nom du profil est *EAP-test*.
`(Cisco Controller) >`**`config local-auth eap-profile add`** *`EAP-test`*

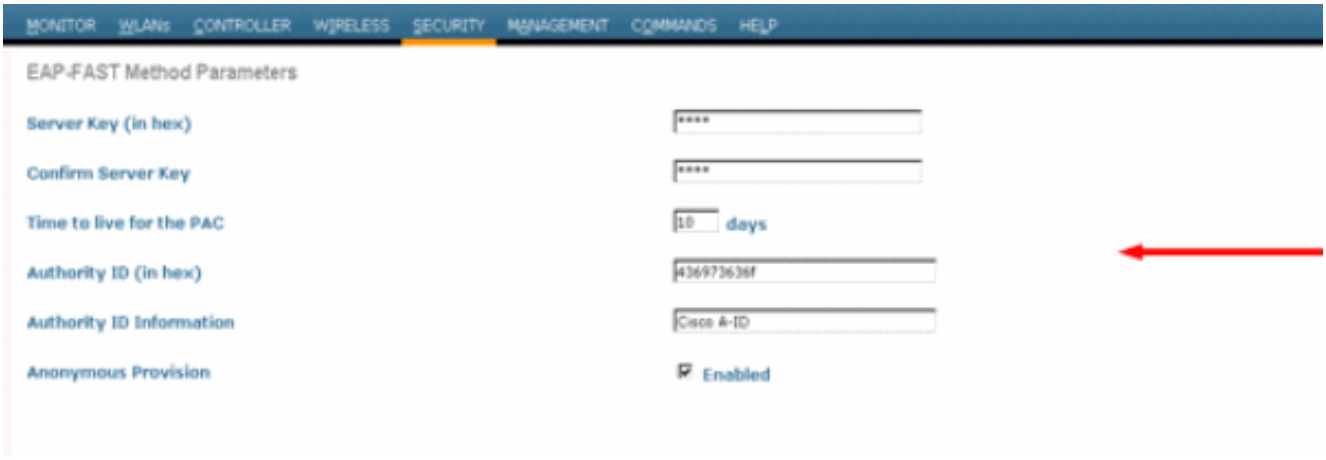
4. Ajoutez une méthode au profil EAP.Dans l'interface utilisateur graphique, choisissez **Security > Local EAP > Profiles** et cliquez sur le nom du profil pour lequel vous voulez ajouter les méthodes d'authentification. Cet exemple utilise LEAP, EAP-FAST et EAP-TLS. Cliquez sur **Apply** afin de définir les méthodes.




Vous pouvez également utiliser la commande CLI **config local-auth eap-profile method add *<method-name>*<profile-name>.** Dans notre exemple de configuration, nous ajoutons trois méthodes au test EAP du profil. Les méthodes sont LEAP, EAP-FAST et EAP-TLS dont les noms de méthode sont *leap, fast* et *tls* respectivement. Ce résultat montre les commandes de configuration CLI :

```
(Cisco Controller) >config local-auth eap-profile method add leap EAP-test
(Cisco Controller) >config local-auth eap-profile method add fast EAP-test
(Cisco Controller) >config local-auth eap-profile method add tls EAP-test
```

5. Configurez les paramètres de la méthode EAP. Ceci est uniquement utilisé pour EAP-FAST. Les paramètres à configurer sont les suivants :**Server Key (clé de serveur)** : clé de serveur permettant de chiffrer/déchiffrer les certificats d'accès protégé (PAC) (au format hexadécimal).**Time to Live for PAC (pac-ttl)** : définit l'heure de vie du PAC.**ID d'autorité (id d'autorité)** : définit l'identificateur d'autorité.**Disposition anonyme (anon-provn)** : détermine si une disposition anonyme est autorisée. Ceci est activé par défaut.Pour la configuration via l'interface utilisateur graphique, choisissez **Security > Local EAP > EAP-FAST Parameters** et entrez la clé de serveur, Time to live pour le PAC, l'ID d'autorité (en hexadécimal) et les valeurs d'ID
d'autorité.

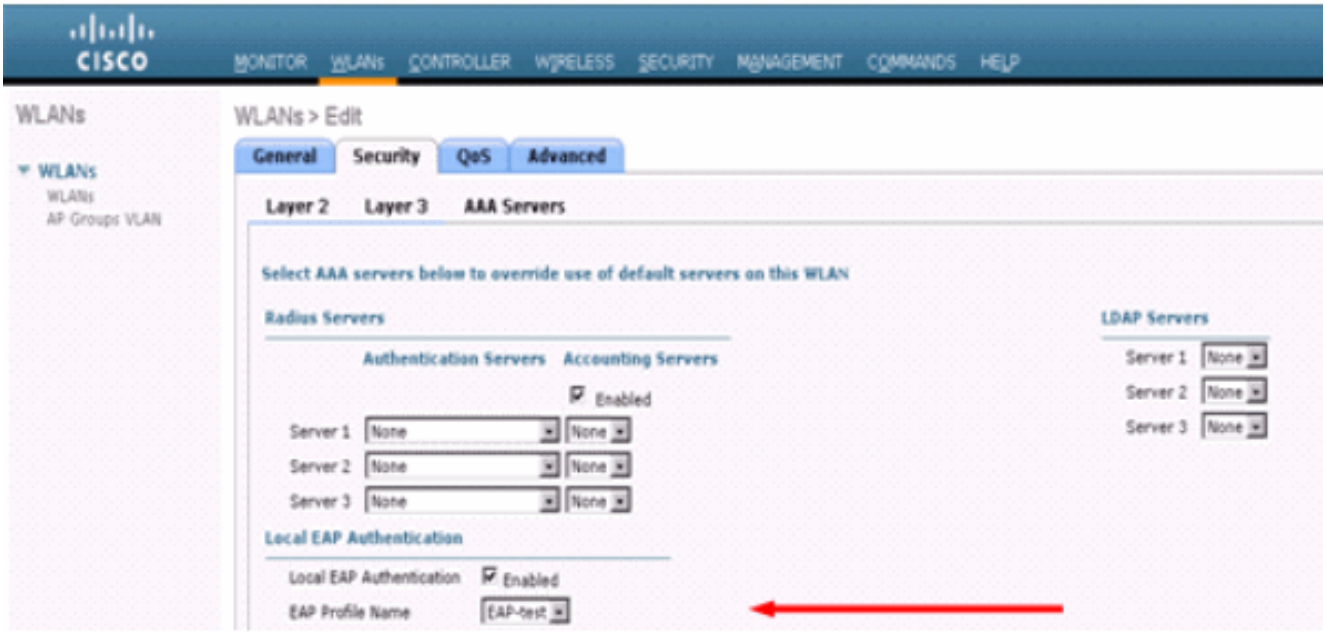



Voici les commandes de configuration CLI à utiliser afin de définir ces paramètres pour EAP-

FAST :

```
(Cisco Controller) >config local-auth method fast server-key 12345678
(Cisco Controller) >config local-auth method fast authority-id 43697369f1 CiscoA-ID
(Cisco Controller) >config local-auth method fast pac-ttl 10
```

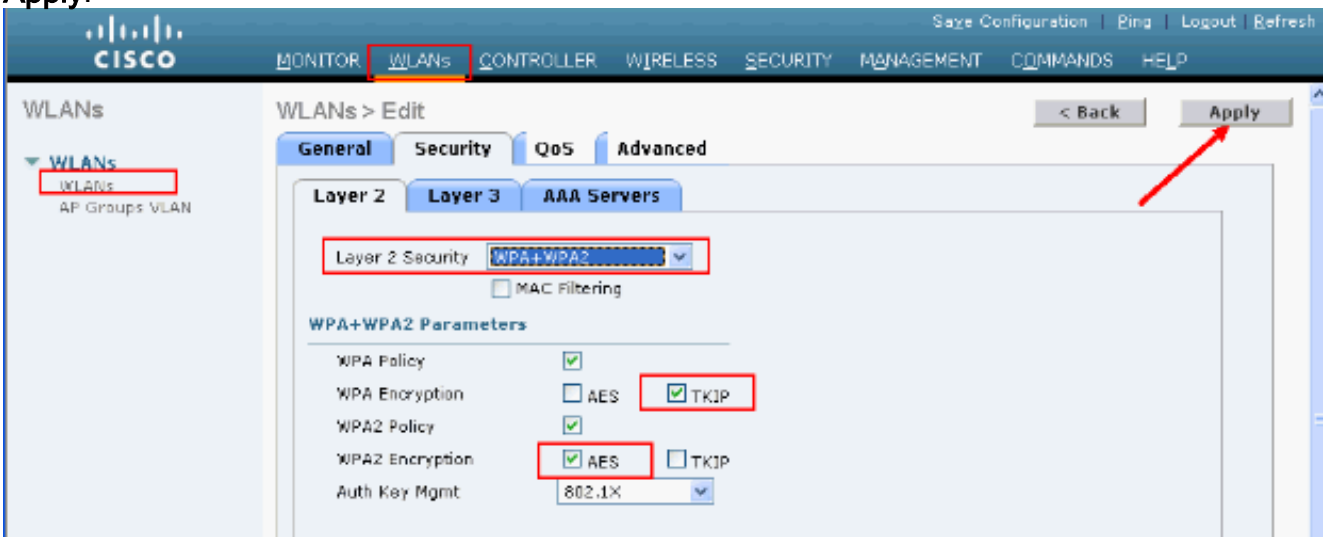
6. Activer l'authentification locale par WLAN :Dans l'interface utilisateur graphique, sélectionnez **WLAN** dans le menu supérieur et sélectionnez le WLAN pour lequel vous voulez configurer l'authentification locale. Une nouvelle fenêtre apparaît. Cliquez sur les onglets **Security > AAA**. Cochez **Local EAP authentication** et sélectionnez le nom de profil EAP approprié dans le menu déroulant comme indiqué dans cet exemple
:




Vous pouvez également émettre la commande de **configuration de configuration** CLI **wlan local-auth enable *<profile-name>*<wlan-id>** comme indiqué ici :

```
(Cisco Controller) >config wlan local-auth enable EAP-test 1
```

7. Définissez les paramètres de sécurité de couche 2.Àpartir de l'interface graphique utilisateur, dans la fenêtre WLAN Edit, accédez aux onglets **Security > Layer 2** et sélectionnez **WPA+WPA2** dans le menu déroulant Layer 2 Security. Dans la section WPA+WPA2 Parameters, définissez le cryptage WPA sur **TKIP** et le cryptage WPA2 **AES**. Cliquez ensuite sur
**Apply**.



Àpartir de l'interface de ligne de commande, utilisez les commandes suivantes :

```
(Cisco Controller) >config wlan security wpa enable 1
(Cisco Controller) >config wlan security wpa wpa1 ciphers tkip enable 1
(Cisco Controller) >config wlan security wpa wpa2 ciphers aes enable 1
```

8. Vérifiez la configuration :

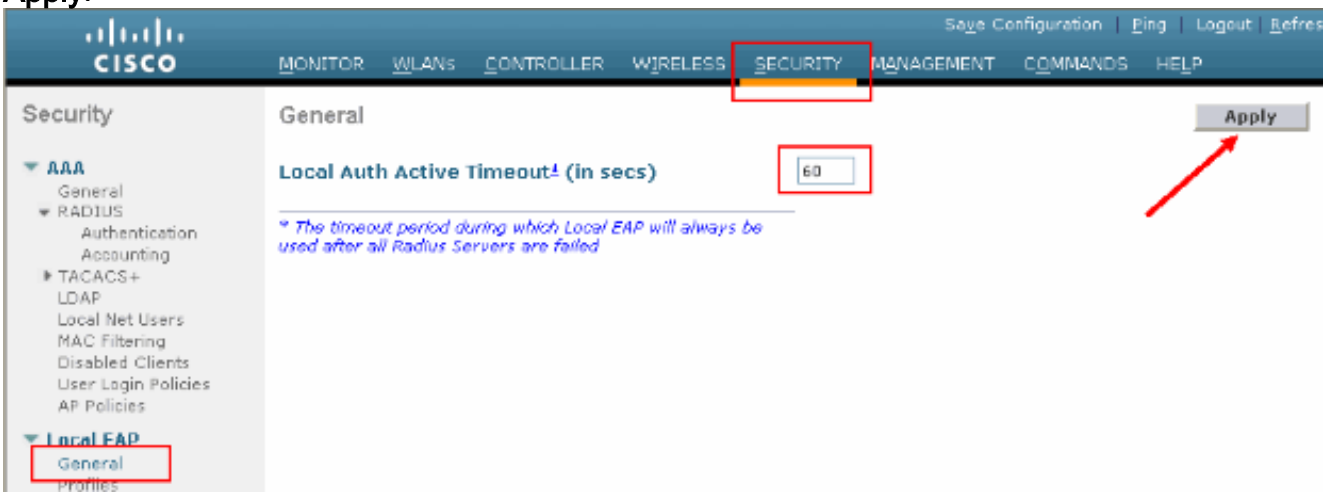
```
(Cisco Controller) >show local-auth config

User credentials database search order:
    Primary ..................................... Local DB

Timer:
    Active timeout .............................. Undefined

Configured EAP profiles:
    Name ........................................ EAP-test
      Certificate issuer ........................ cisco
      Peer verification options:
        Check against CA certificates ........... Enabled
        Verify certificate CN identity .......... Disabled
        Check certificate date validity ......... Enabled
      EAP-FAST configuration:
        Local certificate required .............. No
        Client certificate required ............. No
      Enabled methods ........................... leap fast tls
      Configured on WLANs ....................... 1

EAP Method configuration:
    EAP-FAST:
--More-- or (q)uit
      Server key ................................ <hidden>
      TTL for the PAC ........................... 10
      Anonymous provision allowed ............... Yes
      Authority ID .............................. 43697369f10000000000000000000000
      Authority Information ..................... CiscoA-ID
```

Vous pouvez voir les paramètres spécifiques de wlan 1 avec la commande **show wlan *<wlan id>*** :

```
(Cisco Controller) >show wlan 1


WLAN Identifier.................................. 1
Profile Name..................................... austinlab
Network Name (SSID).............................. austinlab
Status........................................... Disabled
MAC Filtering.................................... Disabled
Broadcast SSID................................... Enabled
AAA Policy Override.............................. Disabled
Number of Active Clients......................... 0
Exclusionlist Timeout............................ 60 seconds
Session Timeout.................................. 1800 seconds
Interface........................................ management
WLAN ACL......................................... unconfigured
DHCP Server...................................... Default
DHCP Address Assignment Required................. Disabled
Quality of Service............................... Silver (best effort)
WMM.............................................. Disabled
CCX - AironetIe Support.......................... Enabled
CCX - Gratuitous ProbeResponse (GPR)............. Disabled
Dot11-Phone Mode (7920).......................... Disabled
Wired Protocol................................... None
--More-- or (q)uit
IPv6 Support..................................... Disabled
Radio Policy..................................... All
```

```
Local EAP Authentication..... Enabled (Profile 'EAP-test')
Security

   802.11 Authentication:..... Open System
   Static WEP Keys..... Disabled
   802.1X..... Disabled
   Wi-Fi Protected Access (WPA/WPA2)..... Enabled
      WPA (SSN IE)..... Enabled
         TKIP Cipher..... Enabled
         AES Cipher..... Disabled
      WPA2 (RSN IE)..... Enabled
         TKIP Cipher..... Disabled
         AES Cipher..... Enabled
                                                Auth Key Management
         802.1x..... Enabled
         PSK..... Disabled
         CCKM..... Disabled
   CKIP ..... Disabled
   IP Security..... Disabled
   IP Security Passthru..... Disabled
   Web Based Authentication..... Disabled
--More-- or (q)uit
   Web-Passthrough..... Disabled
   Conditional Web Redirect..... Disabled
   Auto Anchor..... Disabled
   Cranite Passthru..... Disabled
   Fortress Passthru..... Disabled
   H-REAP Local Switching..... Disabled
   Infrastructure MFP protection..... Enabled
                                    (Global Infrastructure MFP Disabled)
   Client MFP..... Optional
   Tkip MIC Countermeasure Hold-down Timer..... 60

 Mobility Anchor List
 WLAN ID     IP Address       Status
```

Il existe d'autres paramètres d'authentification locale qui peuvent être configurés, en particulier le temporisateur d'expiration actif. Ce compteur configure la période pendant laquelle le protocole EAP local est utilisé après l'échec de tous les serveurs RADIUS.Dans l'interface utilisateur graphique, sélectionnez **Security > Local EAP > General** et définissez la valeur temporelle. Cliquez ensuite sur **Apply**.



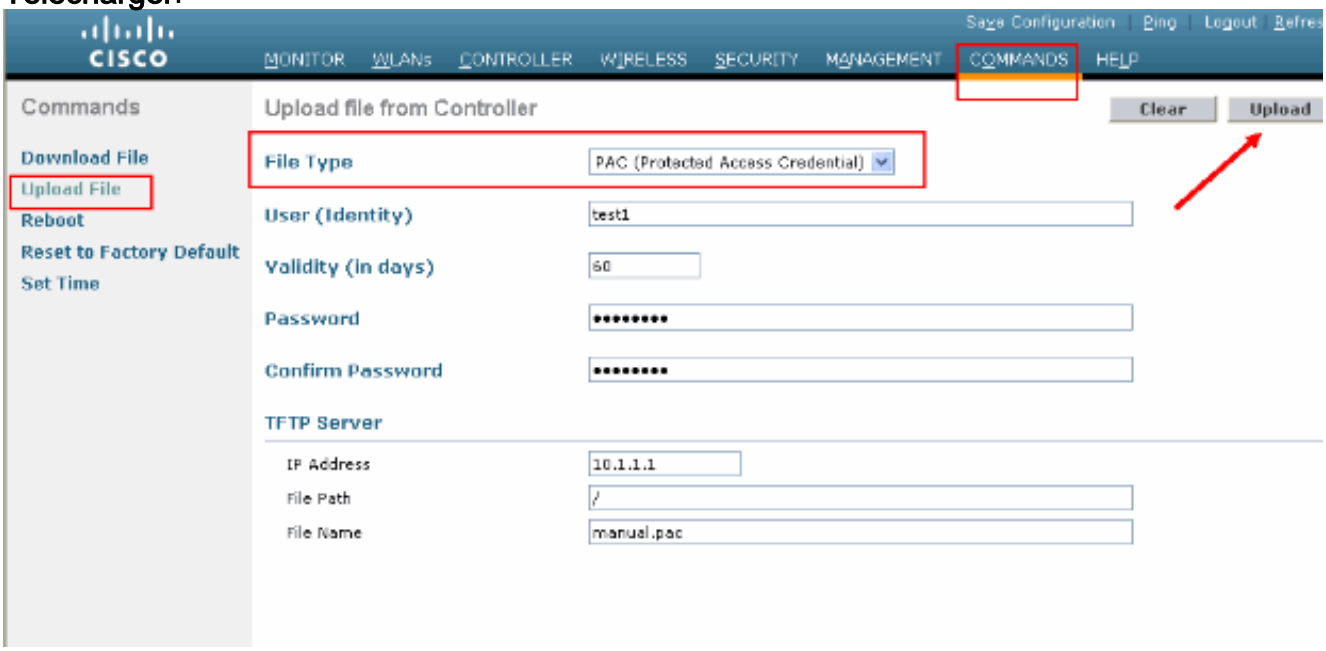

Àpartir de l'interface de ligne de commande, exécutez les commandes suivantes :

```
(Cisco Controller) >config local-auth active-timeout ?
<1 to 3600> Enter the timeout period for the Local EAP to remain active,
in seconds.
(Cisco Controller) >config local-auth active-timeout 60
```

Vous pouvez vérifier la valeur à laquelle ce minuteur est configuré lorsque vous émettez la commande **show local-auth config**.

```
(Cisco Controller) >show local-auth config

User credentials database search order:
    Primary ..................................... Local DB

Timer:
    Active timeout ............................. 60

Configured EAP profiles:
    Name ........................................ EAP-test
... Skip
```

9. Si vous devez générer et charger le PAC manuel, vous pouvez utiliser l'interface utilisateur graphique ou l'interface de ligne de commande.Dans l'interface utilisateur graphique, sélectionnez **COMMANDES** dans le menu supérieur et choisissez **Télécharger le fichier** dans la liste à droite. Sélectionnez **PAC (Protected Access Credential)** dans le menu déroulant Type de fichier. Entrez tous les paramètres et cliquez sur **Télécharger**.




Àpartir de l'interface de ligne de commande, entrez les commandes suivantes :

```
(Cisco Controller) >transfer upload datatype pac
(Cisco Controller) >transfer upload pac ?

username     Enter the user (identity) of the PAC

 (Cisco Controller) >transfer upload pac test1 ?

<validity>     Enter the PAC validity period (days)

(Cisco Controller) >transfer upload pac test1 60 ?

<password>     Enter a password to protect the PAC

 (Cisco Controller) >transfer upload pac test1 60 cisco123

(Cisco Controller) >transfer upload serverip 10.1.1.1

(Cisco Controller) >transfer upload filename manual.pac
```

```
(Cisco Controller) >transfer upload start

Mode..................................................... TFTP
TFTP Server IP........................................... 10.1.1.1
TFTP Path................................................ /
TFTP Filename............................................ manual.pac
Data Type................................................ PAC
PAC User................................................. test1
PAC Validity............................................. 60 days
PAC Password............................................. cisco123

Are you sure you want to start? (y/N) y
PAC transfer starting.
File transfer operation completed successfully.
```

# Autorité de certification Microsoft

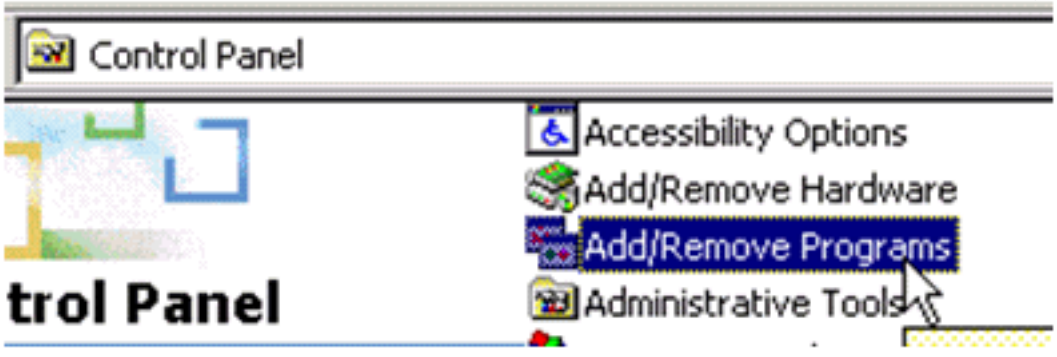
Pour utiliser l'authentification EAP-FAST version 2 et EAP-TLS, le WLC et tous les périphériques clients doivent avoir un certificat valide et doivent également connaître le certificat public de l'autorité de certification.

## Installation

Si Windows 2000 Server ne dispose pas déjà de services d'autorité de certification, vous devez l'installer.

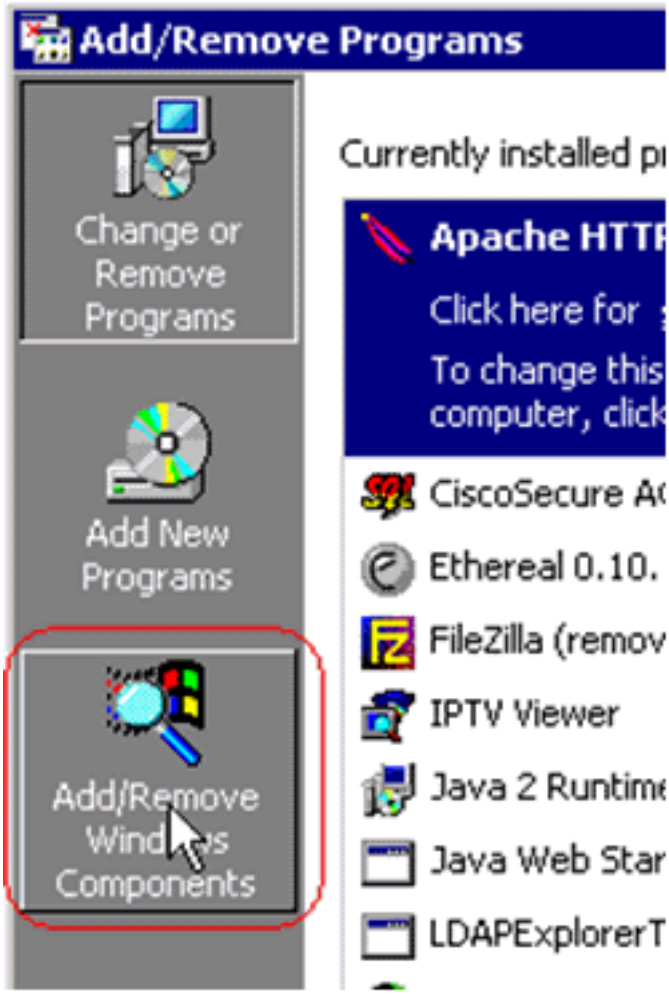
Complétez ces étapes afin d'activer l'autorité de certification Microsoft sur un serveur Windows 2000 :

1. Dans le Panneau de configuration, sélectionnez **Ajout/Suppression de programmes**.



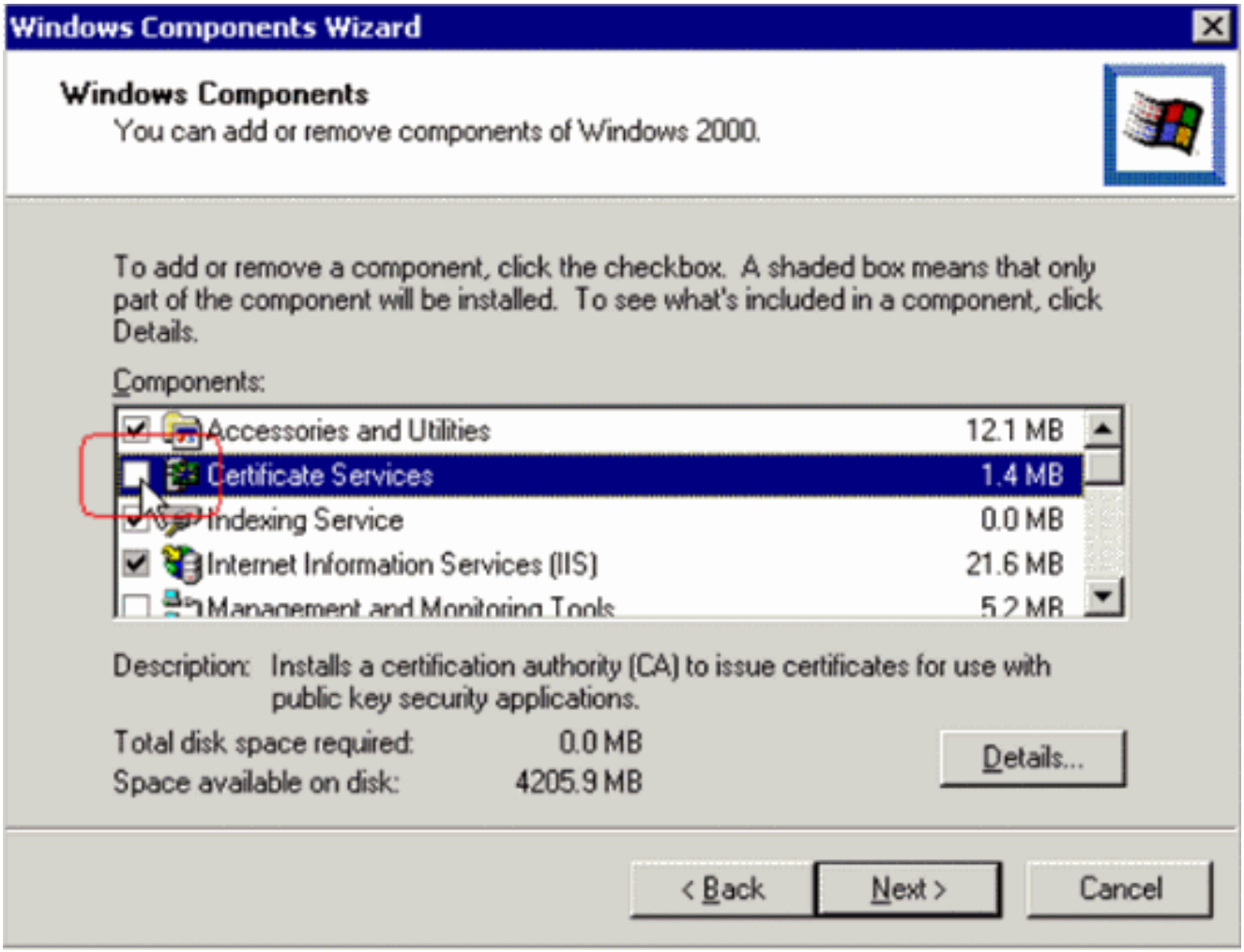

::

2. Sélectionnez **Ajouter/Supprimer des composants Windows** sur le côté

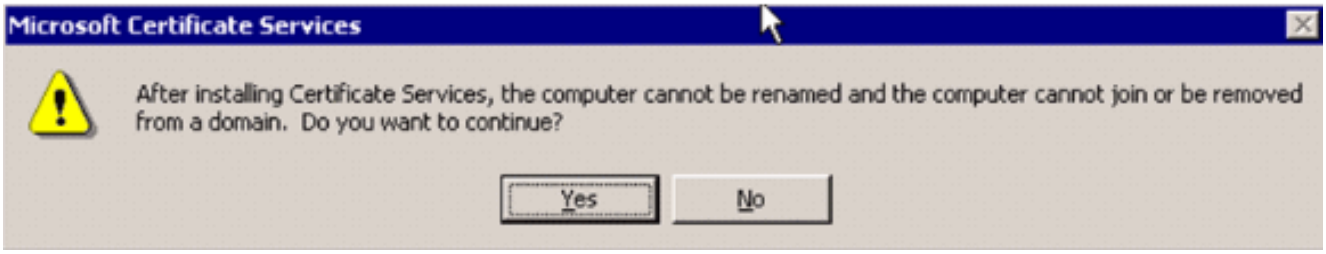



gauche.

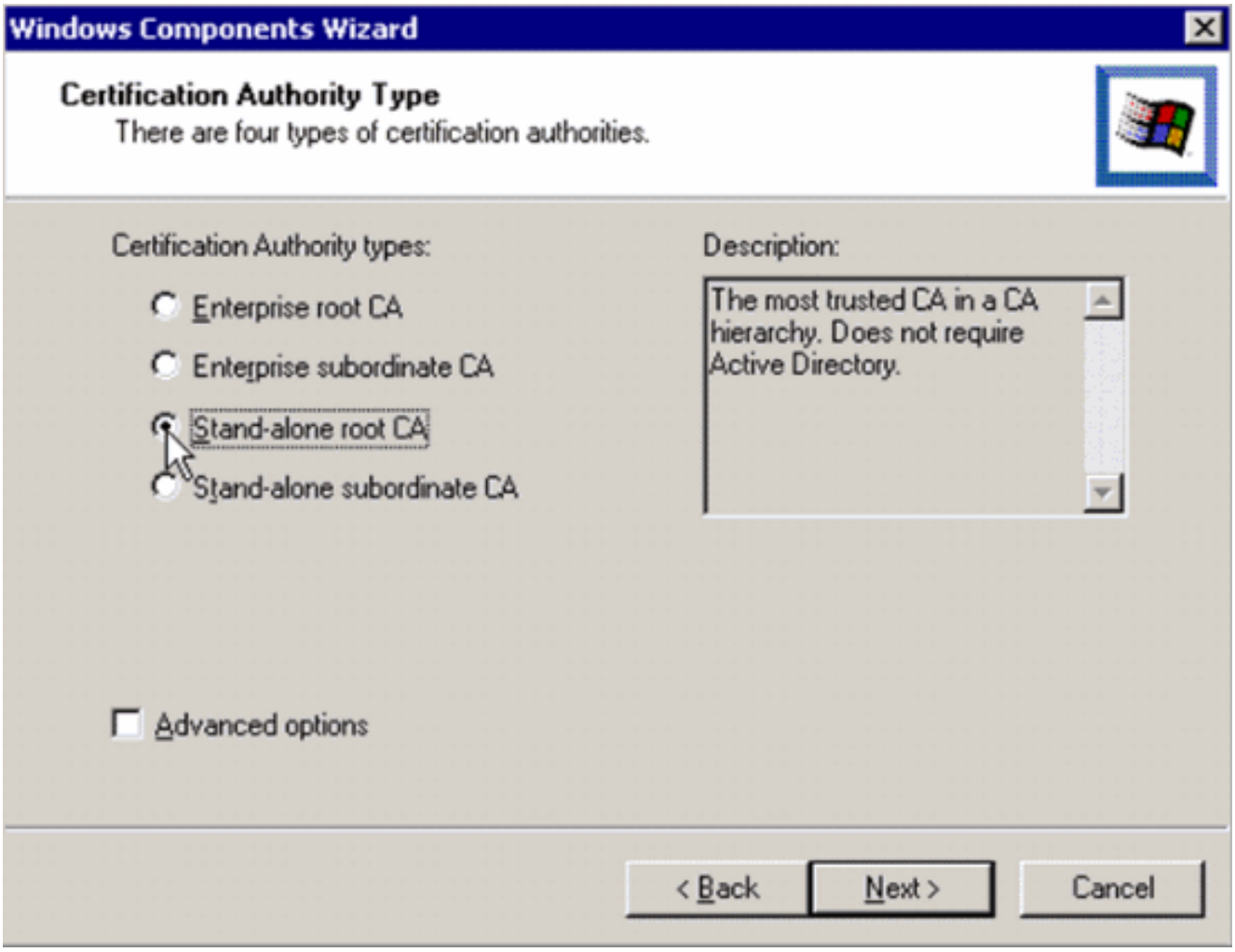
3. Vérifier **les services de certificats**.



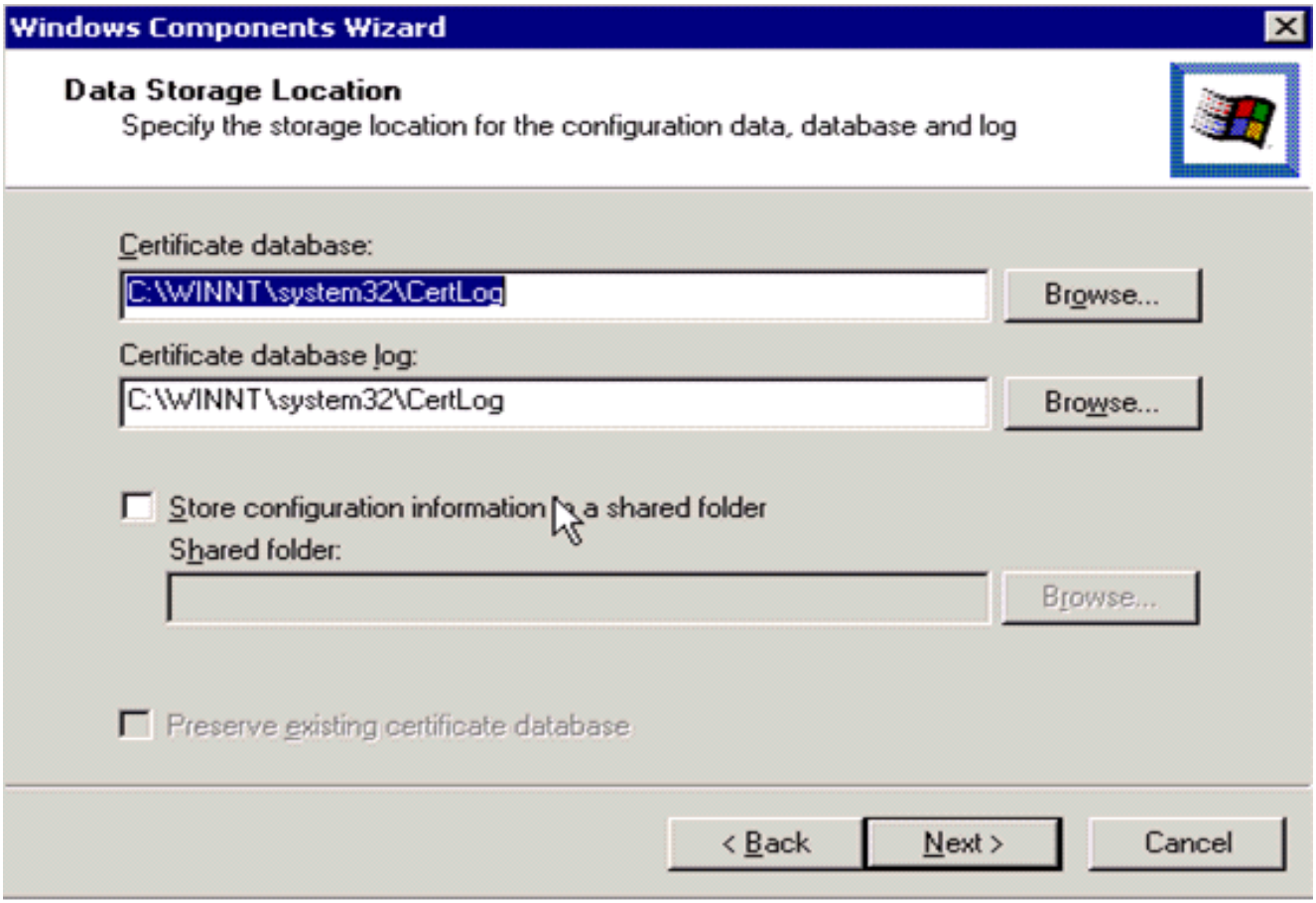

Vérifiez cet avertissement avant de continuer
:



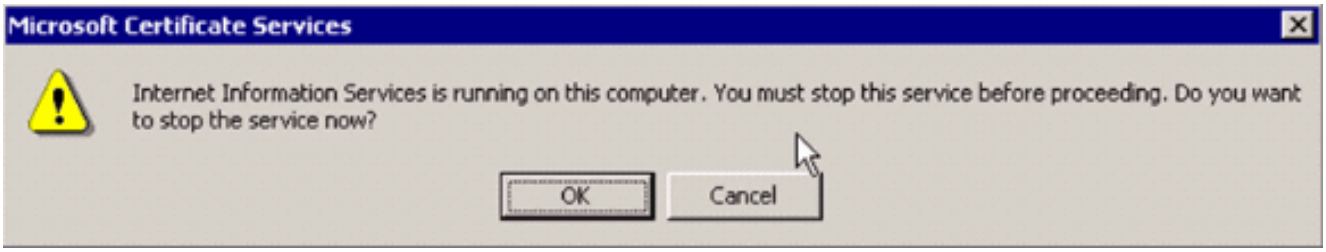

4. Sélectionnez le type d'autorité de certification à installer. Afin de créer une autorité autonome simple, sélectionnez **Autorité de certification racine autonome**.




5. Saisissez les informations nécessaires concernant l'autorité de certification. Ces informations créent un certificat auto-signé pour votre autorité de certification. N'oubliez pas le nom de l'autorité de certification que vous utilisez.L'autorité de certification stocke les certificats dans une base de données. Cet exemple utilise la configuration par défaut proposée par Microsoft :




6. Les services de l'Autorité de certification Microsoft utilisent le serveur Web Microsoft IIS afin de créer et de gérer des certificats client et serveur. Il doit redémarrer le service IIS pour ceci :




Microsoft Windows 2000 Server installe maintenant le nouveau service. Vous devez disposer du CD d'installation de Windows 2000 Server pour installer de nouveaux composants Windows.L'autorité de certification est maintenant installée.

## Installer le certificat dans le contrôleur de réseau local sans fil Cisco

Afin d'utiliser EAP-FAST version 2 et EAP-TLS sur le serveur EAP local d'un contrôleur LAN sans fil Cisco, procédez comme suit :

1. Installez le certificat du périphérique sur le contrôleur de réseau local sans fil.
2. Téléchargez un certificat CA du fournisseur sur le contrôleur LAN sans fil.
3. Configurez le contrôleur de réseau local sans fil pour utiliser EAP-TLS.

Notez que dans l'exemple présenté dans ce document, Access Control Server (ACS) est installé sur le même hôte que Microsoft Active Directory et Microsoft Certification Authority, mais la configuration doit être identique si le serveur ACS se trouve sur un autre serveur.

## Installer le certificat de périphérique sur le contrôleur de réseau local sans fil

Procédez comme suit :

1. . Complétez ces étapes afin de générer le certificat à importer dans le WLC :Accédez à **http://<serverIpAddr>/certsrv**.Choisissez **Demander un certificat** et cliquez sur **Suivant**.Choisissez **Demande avancée** et cliquez sur **Suivant**.Choisissez **Soumettre une demande de certificat à cette autorité de certification à l'aide d'un formulaire** et cliquez sur **Suivant**.Choisissez **Web server** pour Certificate Template et entrez les informations pertinentes. Marquez ensuite les clés comme **exportables**.Vous recevez maintenant un certificat que vous devez installer sur votre machine.
2. Complétez ces étapes afin de récupérer le certificat à partir du PC :Ouvrez un navigateur Internet Explorer et choisissez **Outils > Options Internet >**Contenu.Cliquez sur **Certificats**.Sélectionnez le nouveau certificat installé dans le menu déroulant.Cliquez sur **Exporter**.Cliquez deux fois sur **Suivant** et choisissez **Oui exporter la clé privée**. Ce format est PKCS#12 (.format PFX).Sélectionnez **Activer la protection renforcée**.Tapez un mot de passe.Enregistrez-le dans un fichier **<tme2.pfx>**.
3. Copiez le certificat au format PKCS#12 sur n'importe quel ordinateur sur lequel Openssl est installé afin de le convertir au format PEM.
```
openssl pkcs12 -in tme2.pfx -out tme2.pem
!--- The command to be given, -in Enter Import Password: !--- Enter the password given
previously, from step 2g. MAC verified OK Enter PEM pass phrase: !--- Enter a phrase.
Verifying - Enter PEM pass phrase:
```
4. Téléchargez le certificat de périphérique au format PEM converti sur le WLC.
```
(Cisco Controller) >transfer download datatype eapdevcert

(Cisco Controller) >transfer download certpassword password
!--- From step 3. Setting password to <cisco123> (Cisco Controller) >transfer download
filename tme2.pem

(Cisco Controller) >transfer download start

Mode..................................... TFTP
Data Type................................ Vendor Dev Cert
TFTP Server IP........................... 10.1.1.12
TFTP Packet Timeout...................... 6
TFTP Max Retries......................... 10
TFTP Path................................ /
TFTP Filename............................ tme2.pem

This may take some time.
Are you sure you want to start? (y/N) y

TFTP EAP Dev cert transfer starting.

Certificate installed.
  Reboot the switch to use new certificate.
```
5. Une fois redémarré, vérifiez le certificat.
```
(Cisco Controller) >show local-auth certificates

Certificates available for Local EAP authentication:

Certificate issuer ..................... vendor
  CA certificate:
    Subject: C=US, ST=ca, L=san jose, O=cisco, OU=wnbu, CN=tme
     Issuer: C=US, ST=ca, L=san jose, O=cisco, OU=wnbu, CN=tme
      Valid: 2007 Feb 28th, 19:35:21 GMT to 2012 Feb 28th, 19:44:44 GMT
```

```
Device certificate:
  Subject: C=US, ST=ca, L=san jose, O=cisco, OU=wnbu, CN=tme2
   Issuer: C=US, ST=ca, L=san jose, O=cisco, OU=wnbu, CN=tme
    Valid: 2007 Mar 28th, 23:08:39 GMT to 2009 Mar 27th, 23:08:39 GMT
```

## Télécharger un certificat d'autorité de certification fournisseur sur le contrôleur LAN sans fil

Procédez comme suit :

1. Complétez ces étapes afin de récupérer le certificat CA du fournisseur :Accédez à **http://<serverIpAddr>/certsrv**.Choisissez **Récupérer le certificat CA** et cliquez sur **Suivant**.Sélectionnez le certificat CA.Cliquez sur **codage DER**.Cliquez sur **Télécharger le certificat de l'Autorité de certification** et enregistrez le certificat en tant que **rootca.cer**.
2. Convertissez l'autorité de certification du fournisseur du format DER au format PEM avec la commande **openssl x509 -in rootca.cer -informer DER -out rootca.pem -outform PEM**.Le fichier de sortie est rootca.pem au format PEM.
3. Télécharger le certificat CA du fournisseur :

```
(Cisco Controller) >transfer download datatype eapcacert

(Cisco Controller) >transfer download filename ?

<filename>     Enter filename up to 16 alphanumeric characters.

(Cisco Controller) >transfer download filename rootca.pem

(Cisco Controller) >transfer download start ?

(Cisco Controller) >transfer download start

Mode..................................................... TFTP
Data Type................................................ Vendor CA Cert
TFTP Server IP........................................... 10.1.1.12
TFTP Packet Timeout...................................... 6
TFTP Max Retries......................................... 10
TFTP Path................................................ /
TFTP Filename............................................ rootca.pem

This may take some time.
Are you sure you want to start? (y/N) y

TFTP EAP CA cert transfer starting.

Certificate installed.
  Reboot the switch to use new certificate.
```

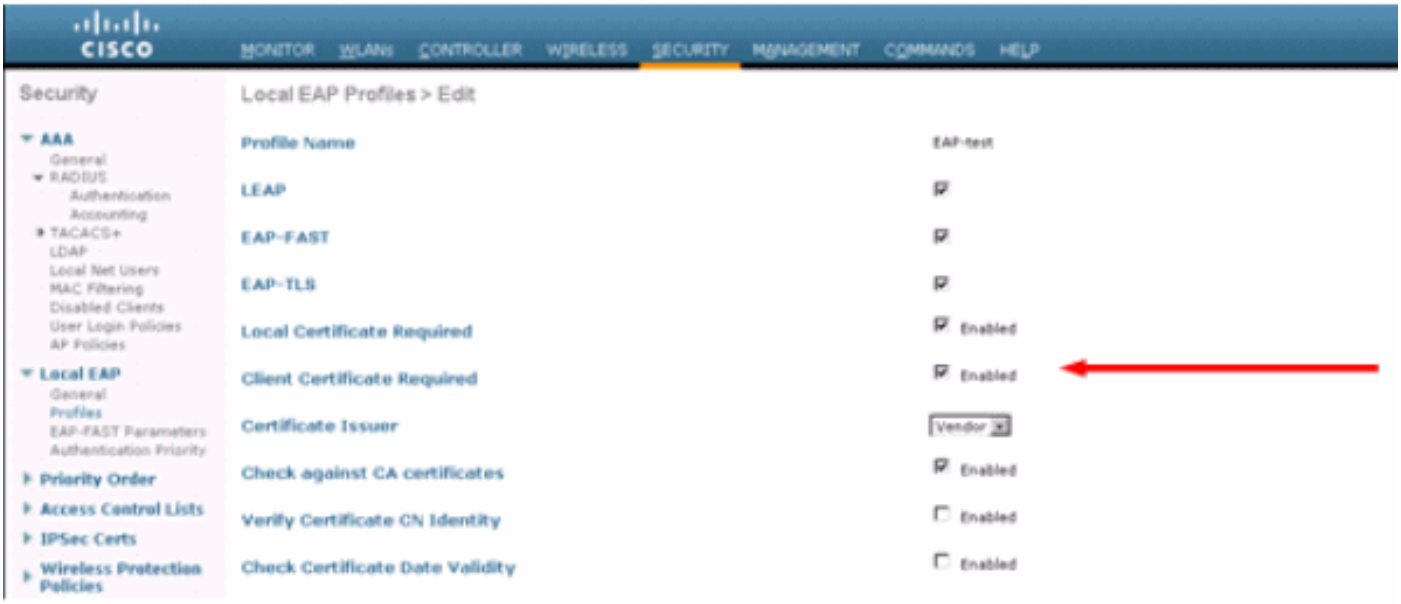
## Configurer le contrôleur de réseau local sans fil pour utiliser EAP-TLS

Procédez comme suit :

Dans l'interface utilisateur graphique, sélectionnez **Security > Local EAP > Profiles**, choisissez le profil et vérifiez les paramètres suivants :

- Le certificat local requis est activé.
- Le certificat client requis est activé.
- L'émetteur du certificat est Fournisseur.

- La vérification des certificats CA est activée.



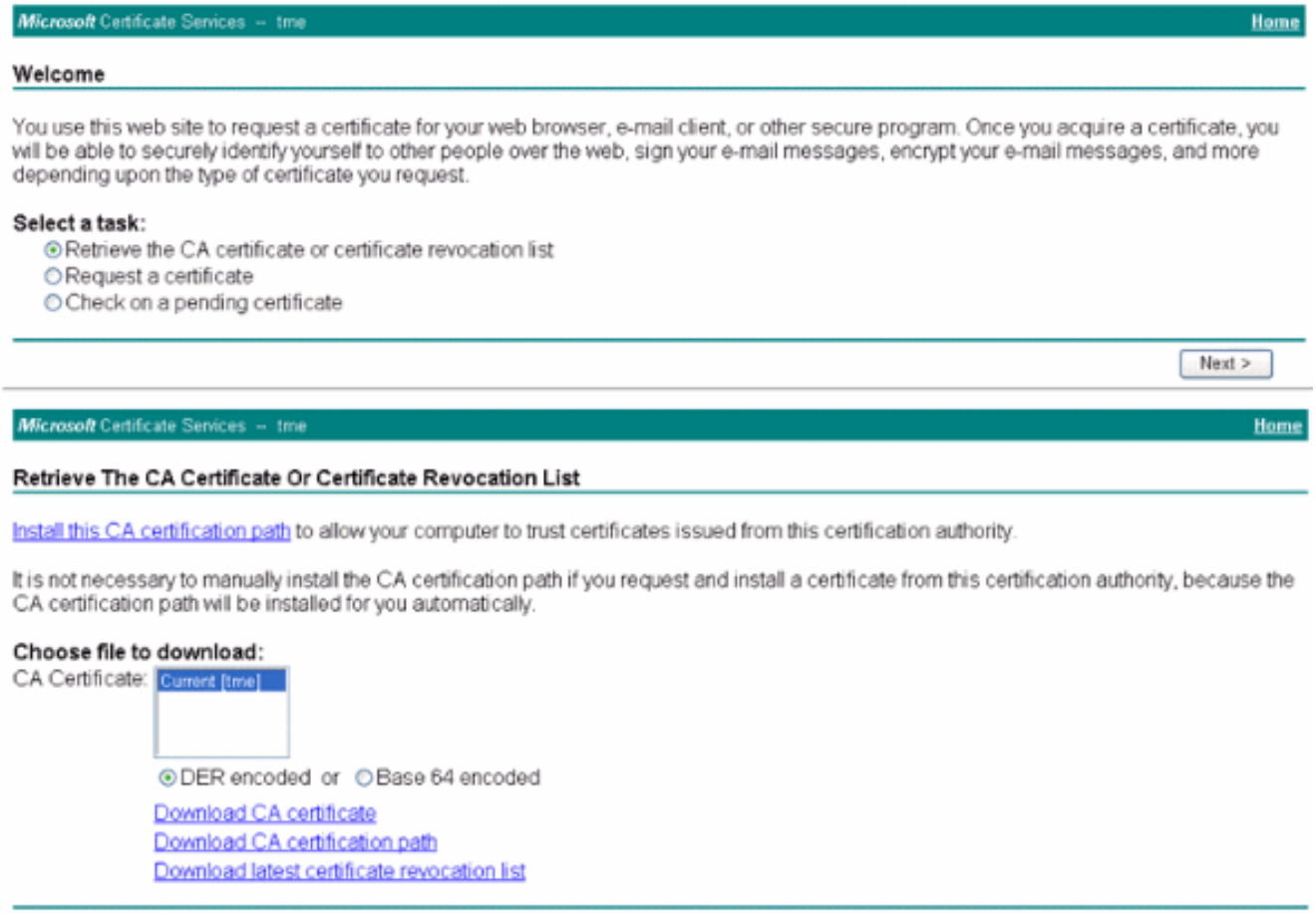

# Installer le certificat d'autorité de certification sur le périphérique client

## Télécharger et installer un certificat d'autorité de certification racine pour le client

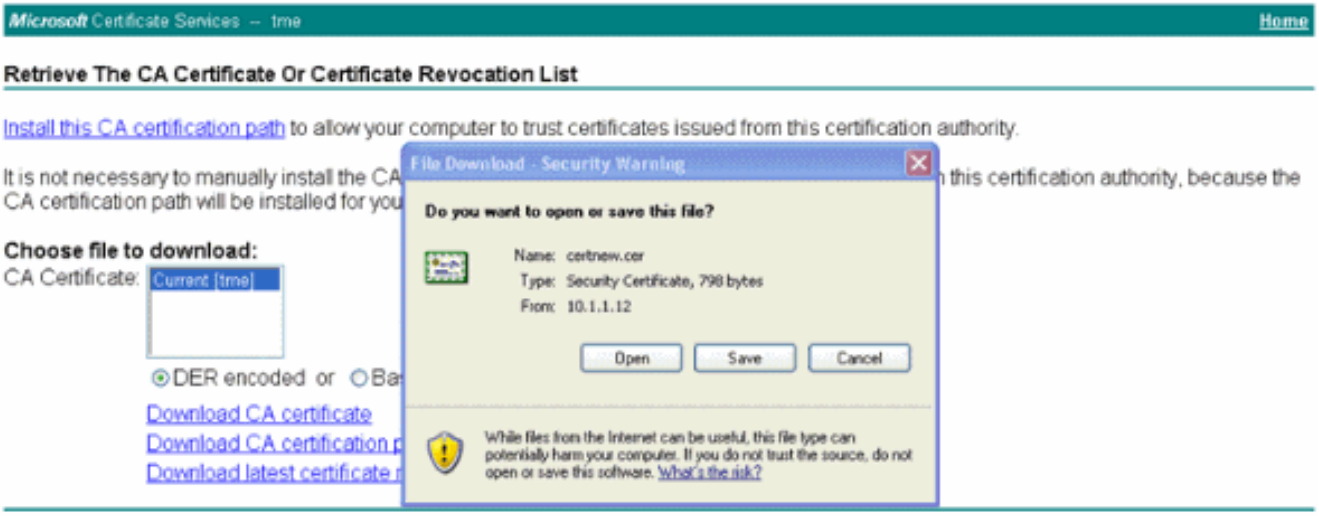
Le client doit obtenir un certificat d'autorité de certification racine auprès d'un serveur d'autorité de certification. Vous pouvez utiliser plusieurs méthodes pour obtenir un certificat client et l'installer sur l'ordinateur Windows XP. Pour obtenir un certificat valide, l'utilisateur Windows XP doit être connecté à l'aide de son ID utilisateur et doit disposer d'une connexion réseau.

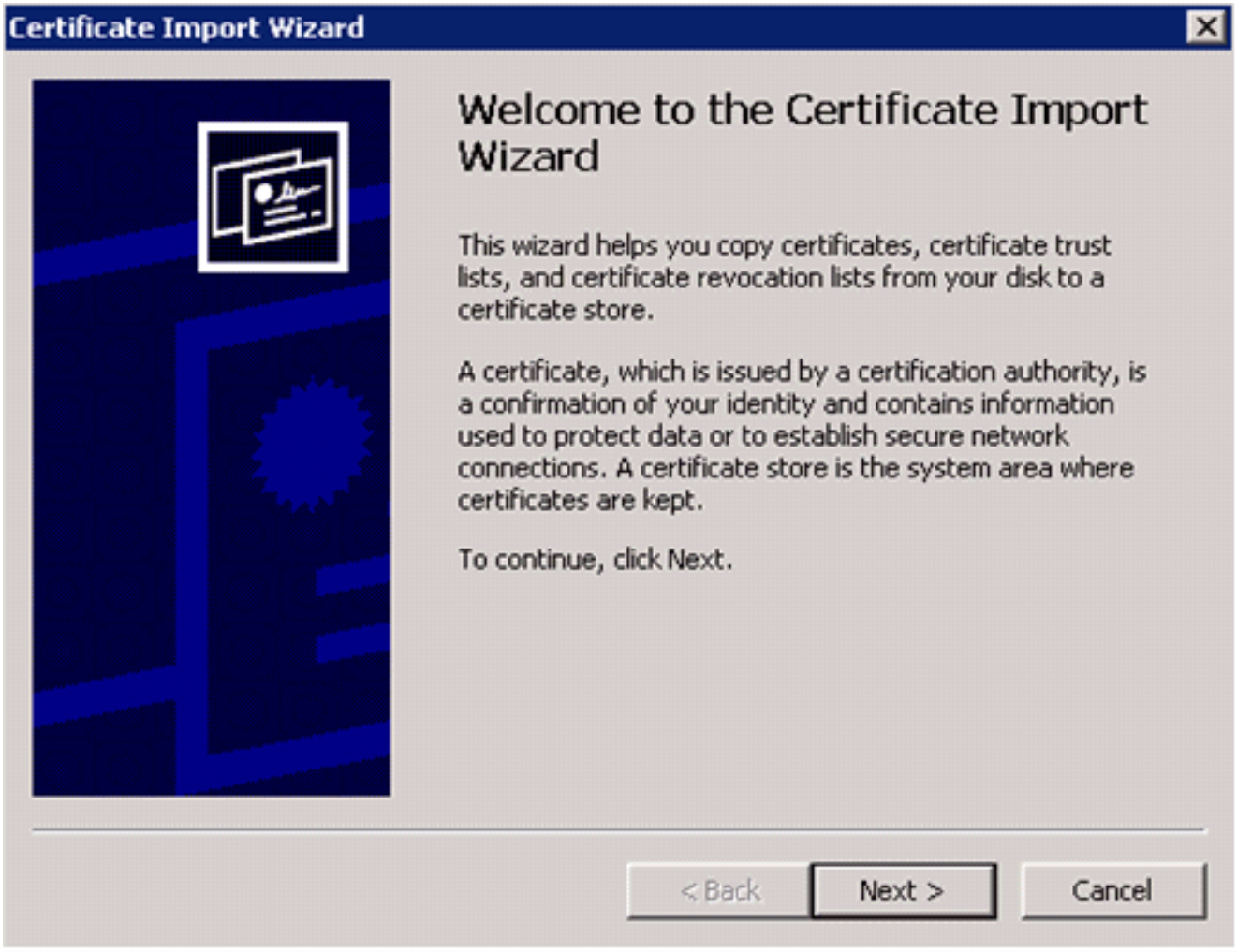
Un navigateur Web sur le client Windows XP et une connexion câblée au réseau ont été utilisés pour obtenir un certificat client auprès du serveur privé de l'autorité de certification racine. Cette procédure est utilisée pour obtenir le certificat client d'un serveur de l'Autorité de certification Microsoft :

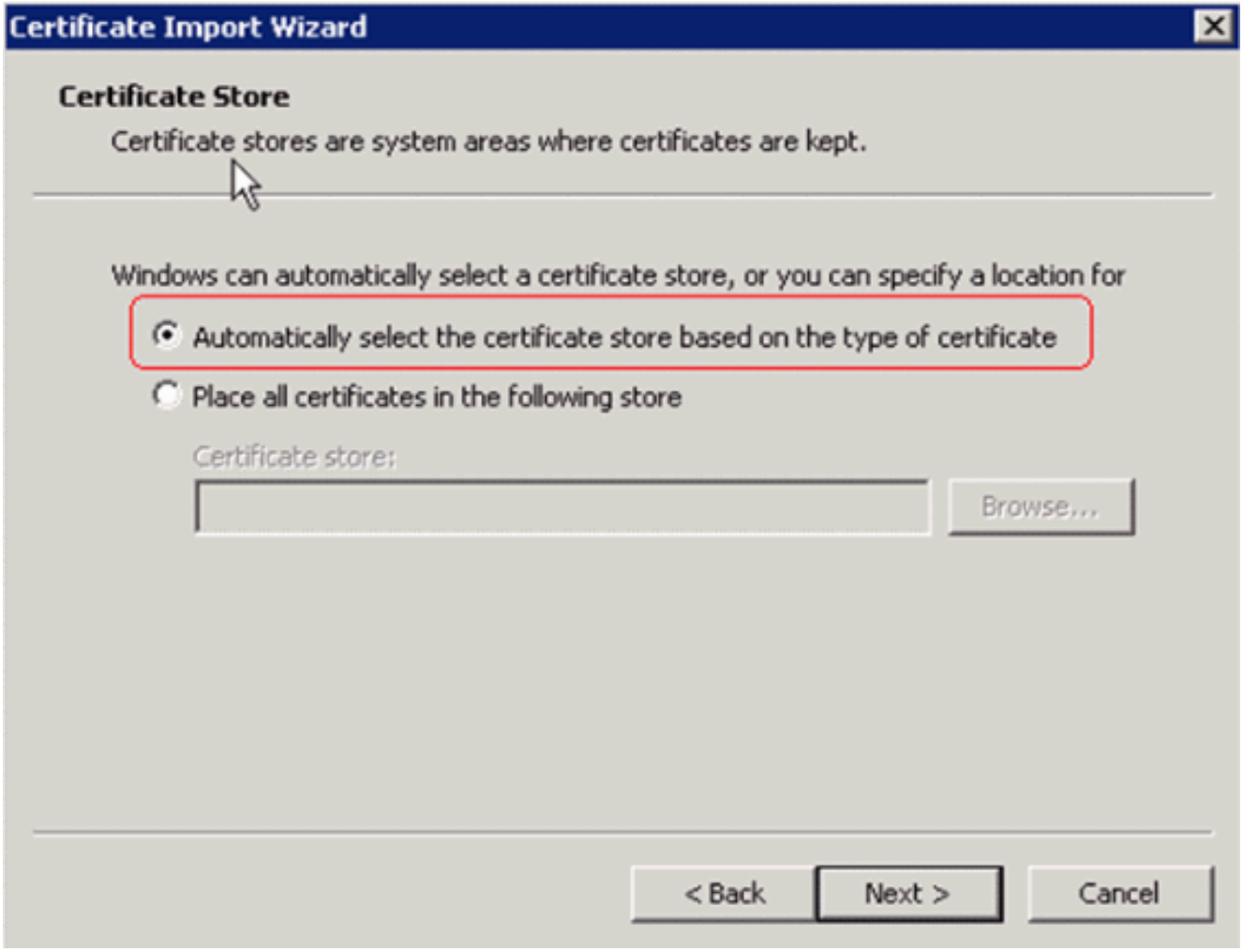
1. Utilisez un navigateur Web sur le client et pointez le navigateur sur le serveur de l'autorité de certification. Pour ce faire, saisissez **http://IP-address-of-Root-CA/certsrv**.
2. Connectez-vous à l'aide de **Domain_Name\user_name**. Vous devez vous connecter à l'aide du nom d'utilisateur de la personne qui doit utiliser le client XP.
3. Dans la fenêtre Bienvenue, sélectionnez **Récupérer un certificat CA** et cliquez sur **Suivant**.
4. Sélectionnez **Codage Base64** et **Télécharger le certificat CA**.
5. Dans la fenêtre Certificat émis, cliquez sur **Installer ce certificat** et cliquez sur **Suivant**.
6. Choisissez **Automatically select the certificate store** et cliquez sur **Next**, pour afficher le message Import réussi.
7. Se connecter à l'autorité de certification pour récupérer le certificat de l'autorité de certification
   :



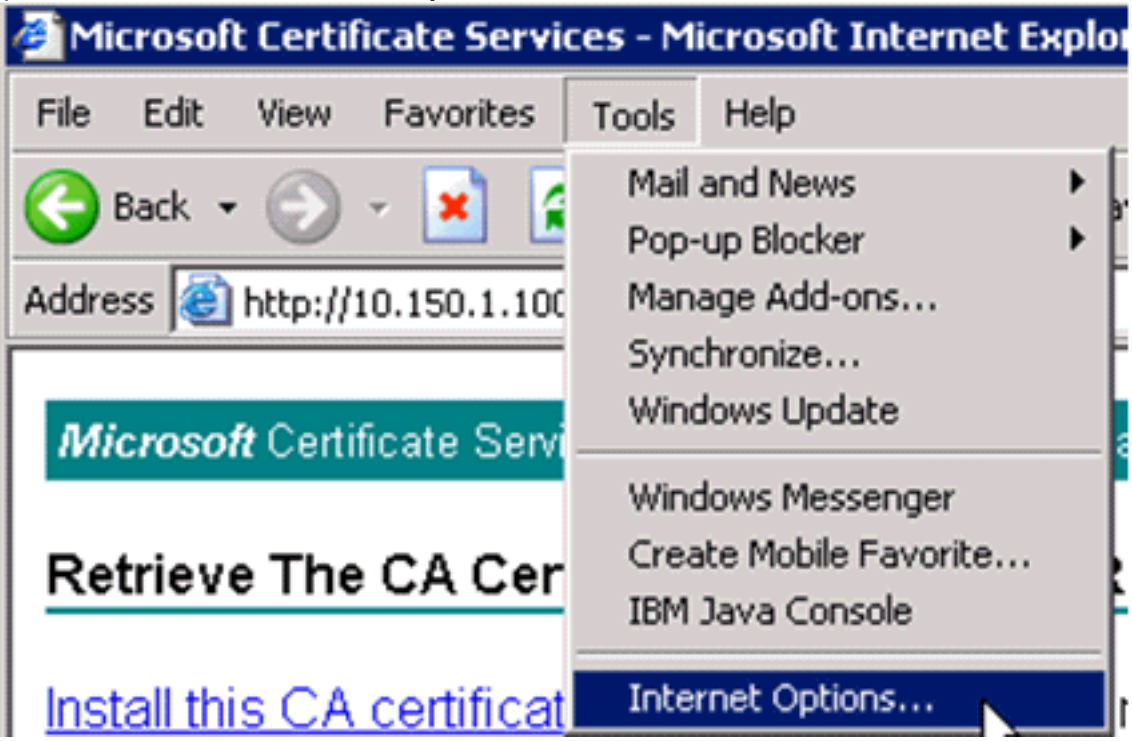

8. Cliquez sur **Download CA certificate**.

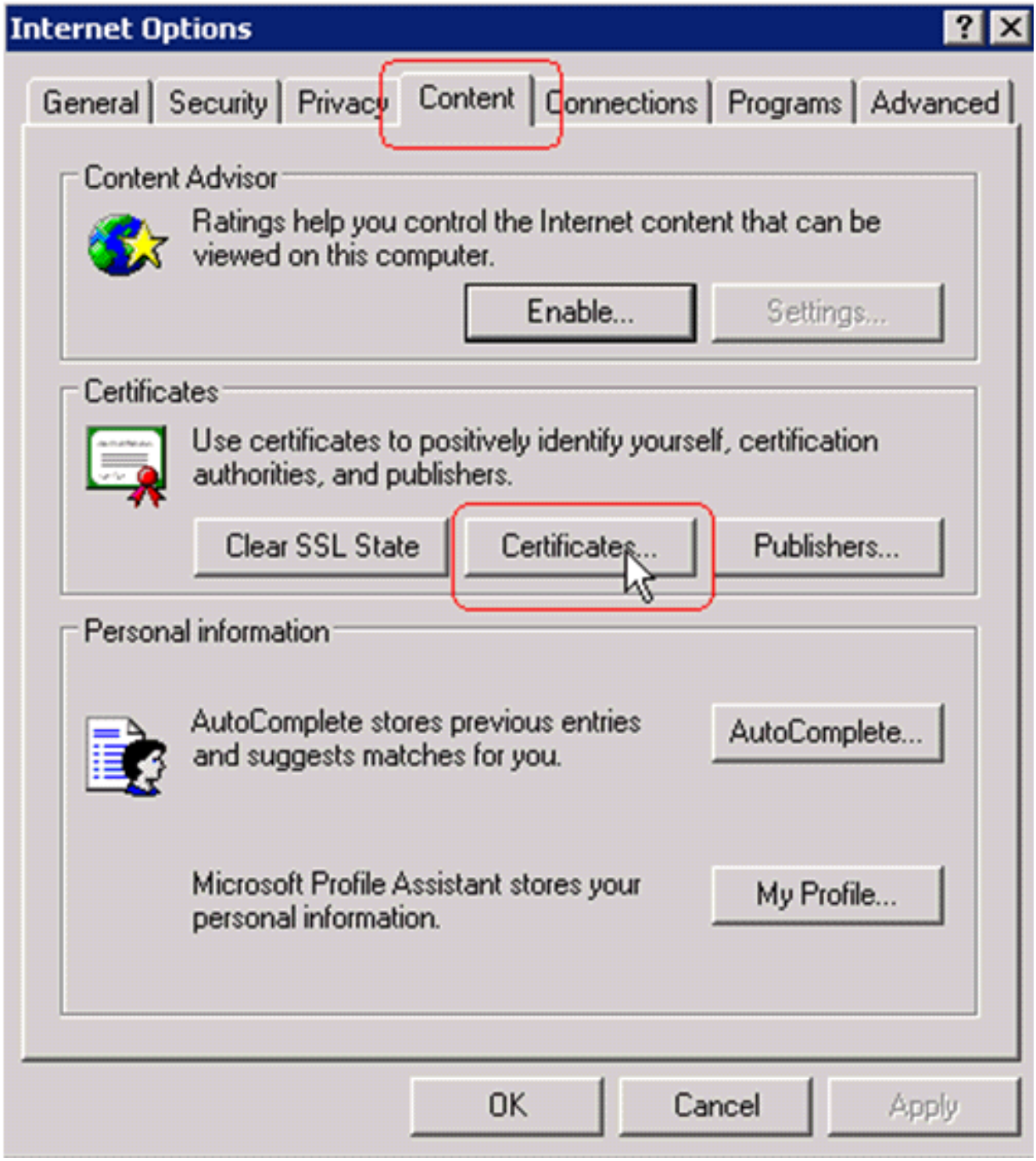



Certificate Import Wizard
Welcome to the Certificate Import Wizard
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
To continue, click Next.
< Back
Next >
Cancel

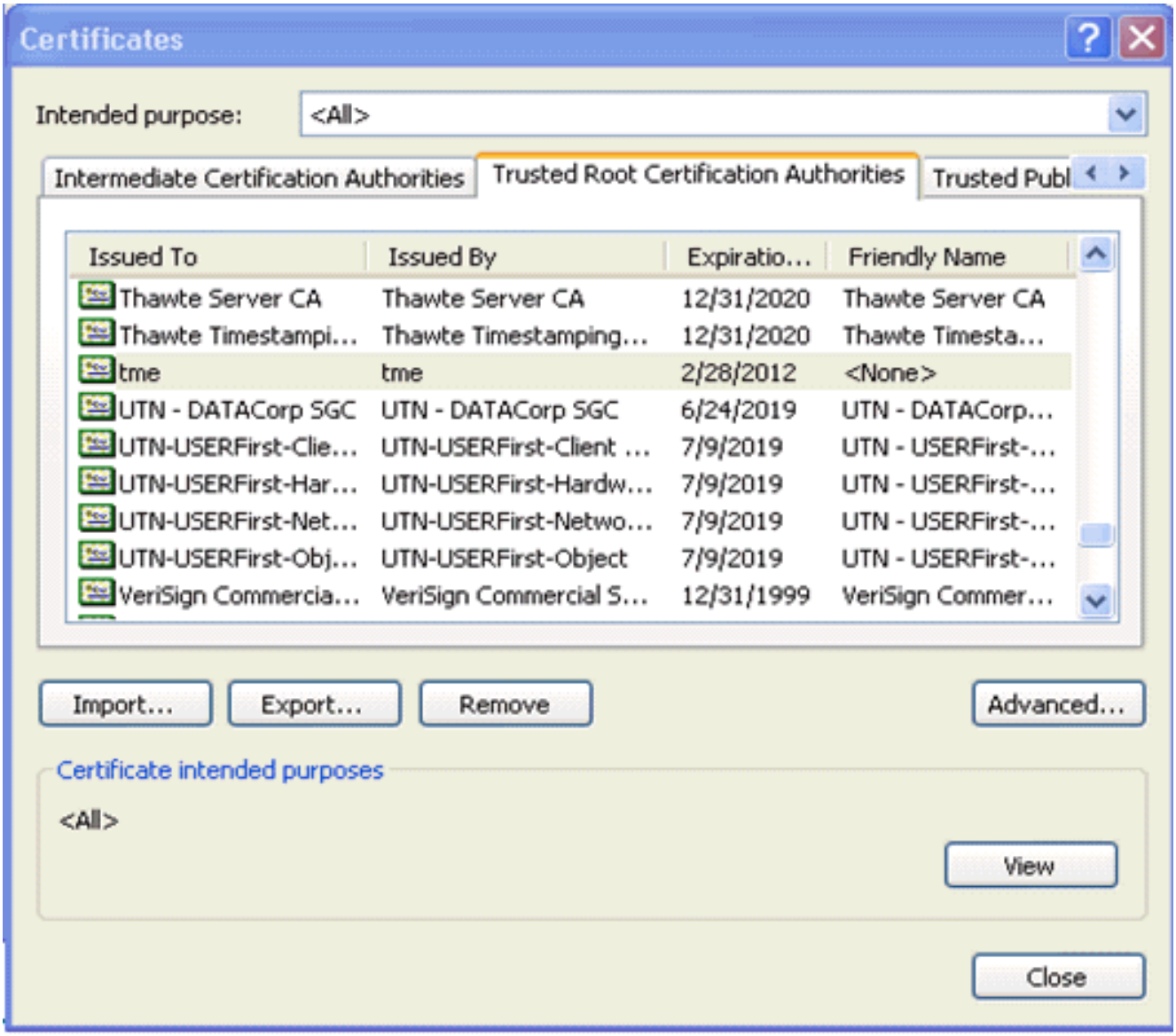

Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for
Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Certificate store:
Browse...
< Back
Next >
Cancel


9. Afin de vérifier que le certificat de l'autorité de certification est correctement installé, ouvrez Internet Explorer et choisissez **Outils > Options Internet > Contenu > Certificats**.






Dans Trusted Root Certification Authority (Autorité de certification racines de confiance), vous devriez voir votre autorité de certification nouvellement installée
:



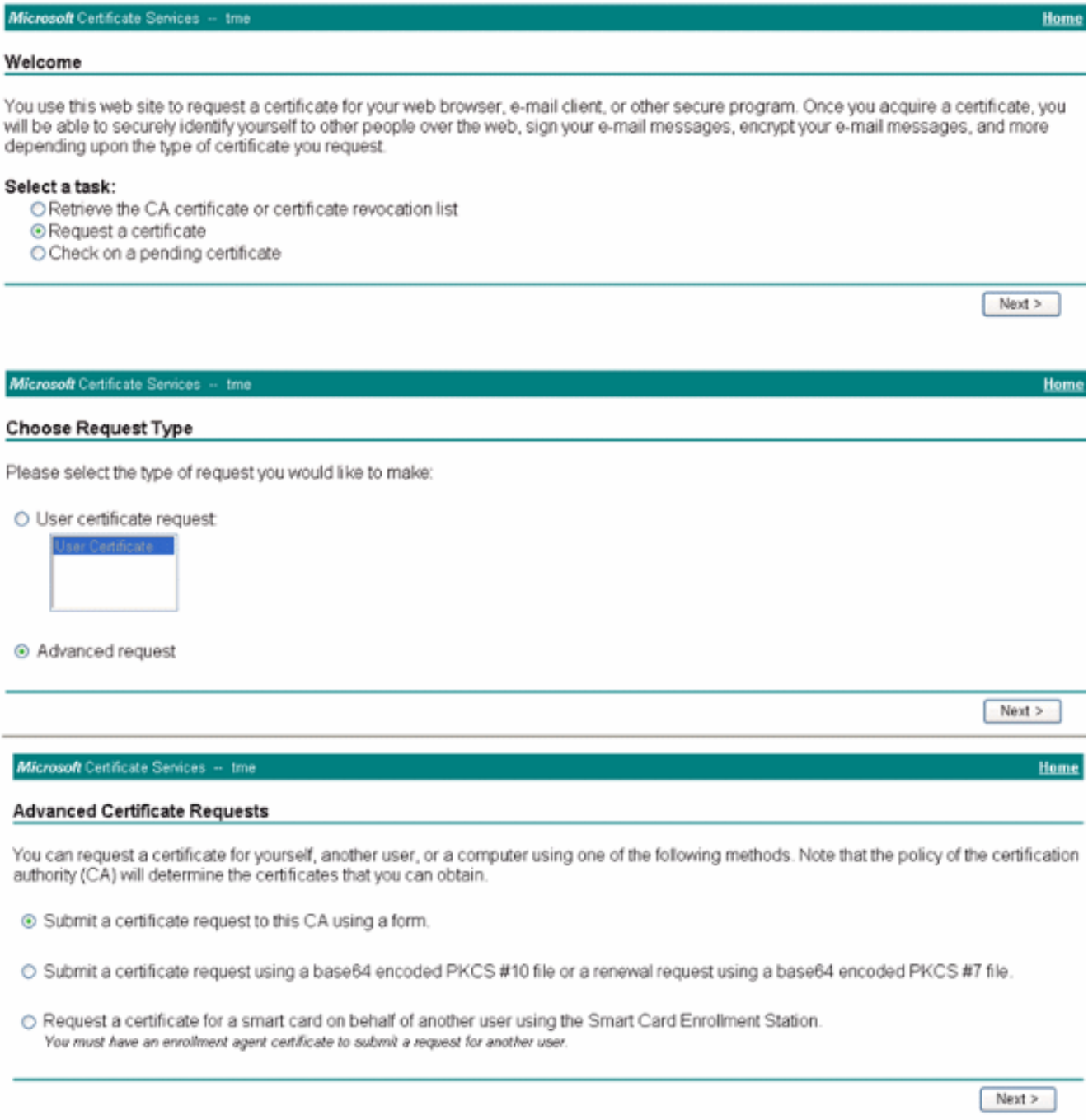

## Générer un certificat client pour un périphérique client

Le client doit obtenir un certificat d'un serveur d'autorité de certification pour le WLC pour authentifier un client EAP-TLS WLAN. Vous pouvez utiliser plusieurs méthodes pour obtenir un certificat client et l'installer sur l'ordinateur Windows XP. Pour obtenir un certificat valide, l'utilisateur Windows XP doit être connecté à l'aide de son ID utilisateur et doit disposer d'une connexion réseau (soit une connexion filaire, soit une connexion WLAN avec sécurité 802.1x désactivée).

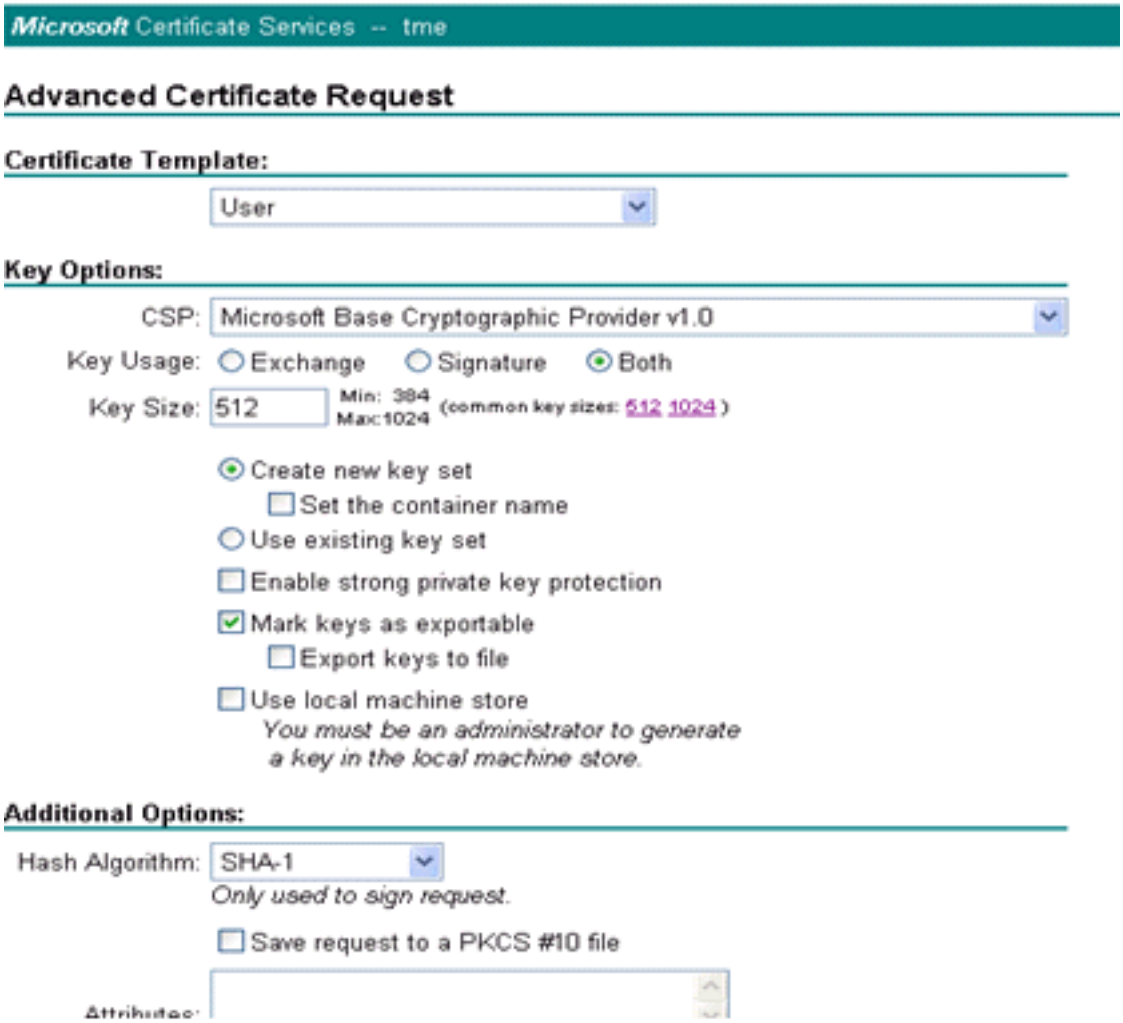
Un navigateur Web sur le client Windows XP et une connexion câblée au réseau sont utilisés pour obtenir un certificat client auprès du serveur de l'autorité de certification racine privé. Cette procédure est utilisée pour obtenir le certificat client d'un serveur de l'Autorité de certification Microsoft :

1. Utilisez un navigateur Web sur le client et pointez le navigateur sur le serveur de l'autorité de certification. Pour ce faire, saisissez **http://IP-address-of-Root-CA/certsrv**.
2. Connectez-vous à l'aide de **Domain_Name\user_name**. Vous devez vous connecter à l'aide du nom d'utilisateur de la personne qui utilise le client XP. (Le nom d'utilisateur est incorporé au certificat client.)
3. Dans la fenêtre Bienvenue, sélectionnez **Demander un certificat** et cliquez sur **Suivant**.
4. Choisissez **Demande avancée** et cliquez sur **Suivant**.

5. Choisissez **Soumettre une demande de certificat à cette autorité de certification à l'aide d'un formulaire** et cliquez sur **Suivant**.
6. Dans le formulaire Demande de certificat avancée, sélectionnez le modèle de certificat en tant qu'**utilisateur**, spécifiez la taille de clé **1024** et cliquez sur **Soumettre**.
7. Dans la fenêtre Certificat émis, cliquez sur **Installer ce certificat**. Cela aboutit à l'installation réussie d'un certificat client sur le client Windows XP.

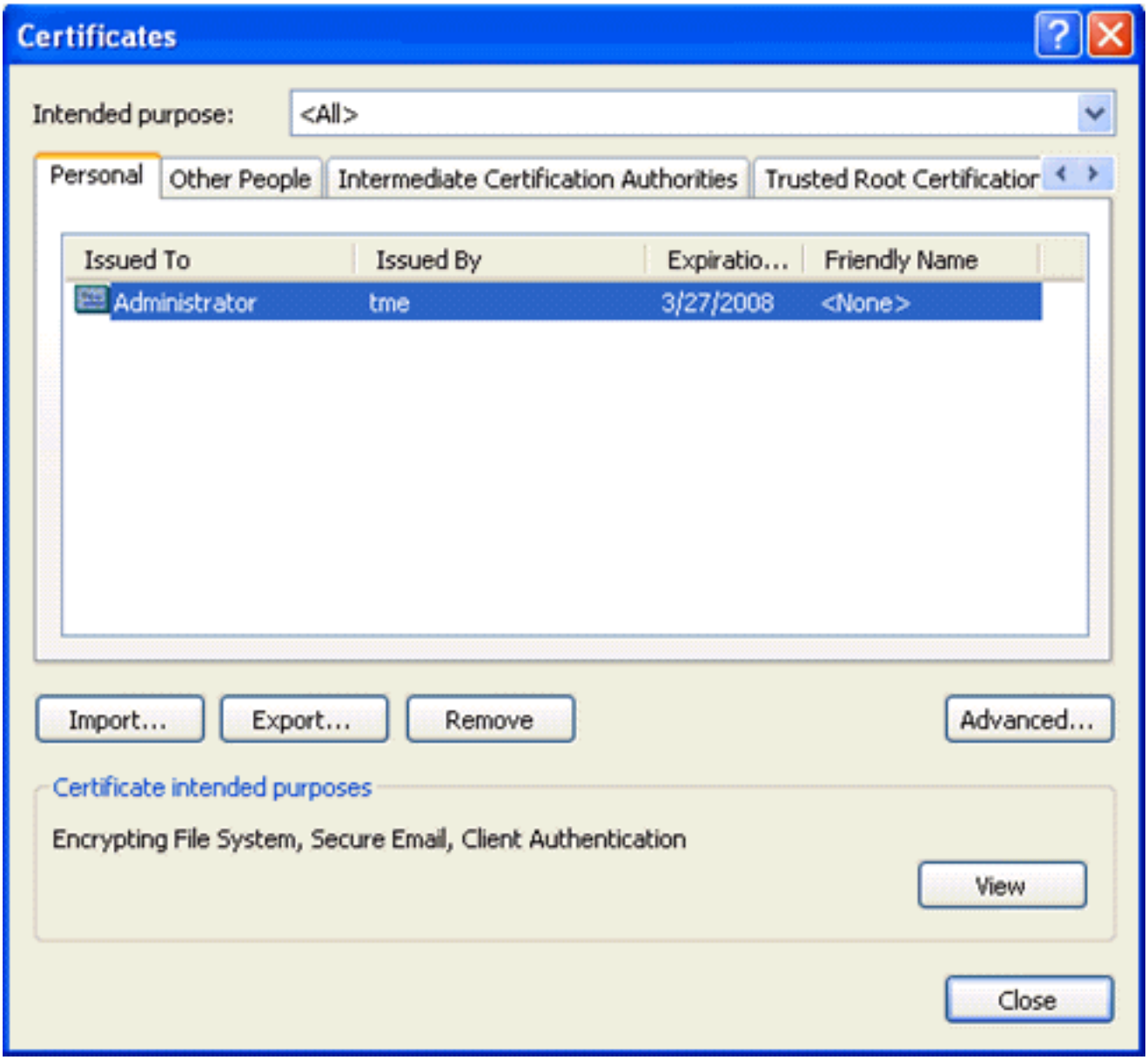



8. Sélectionnez **Client Authentication**




**Certificate**. Le certificat client est maintenant créé.

9. Afin de vérifier que le certificat est installé, accédez à Internet Explorer et choisissez **Outils > Options Internet > Contenu > Certificats**. Dans l'onglet Personnel, vous devriez voir le certificat.

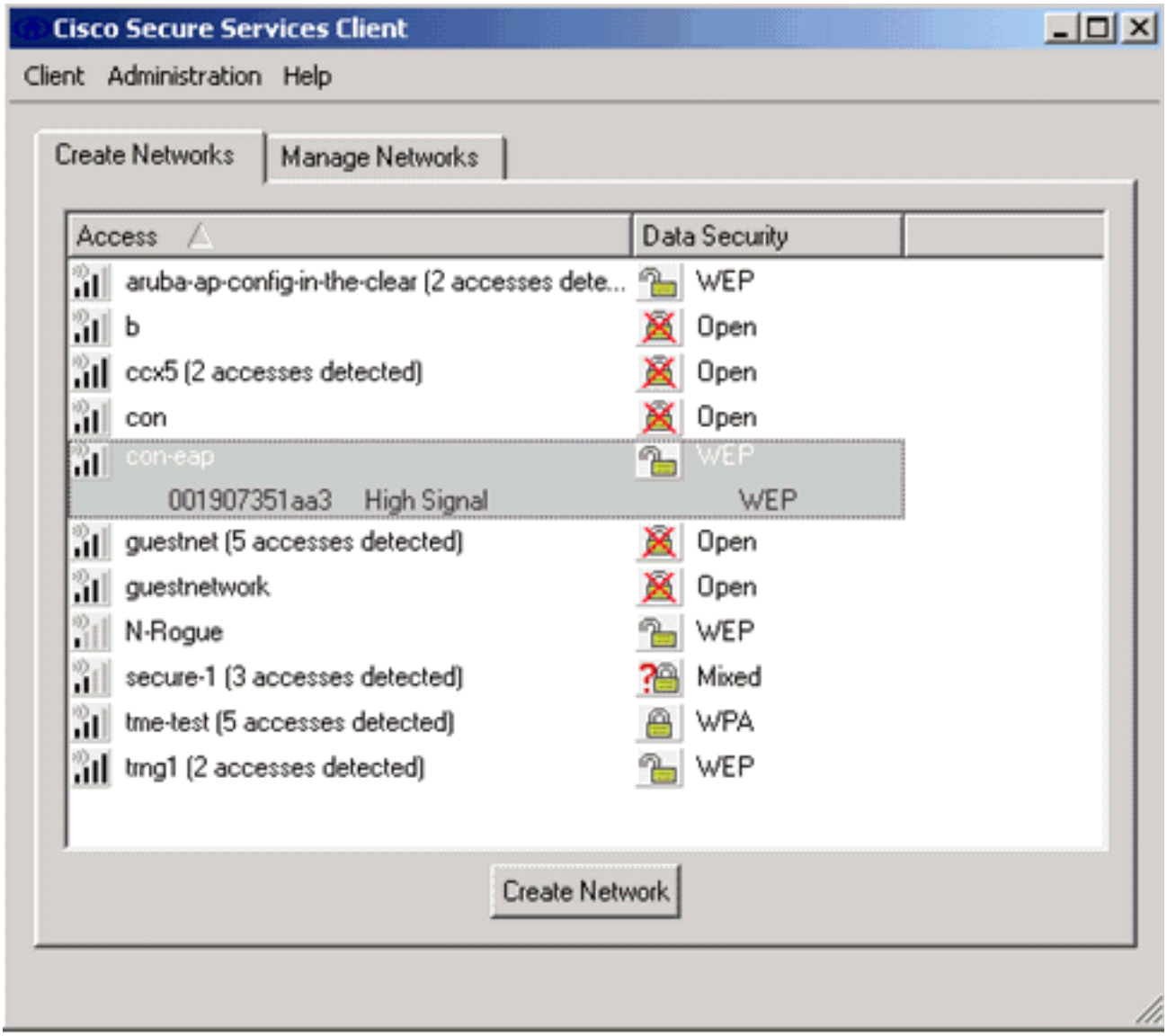



## EAP-TLS avec Cisco Secure Services Client sur le périphérique client

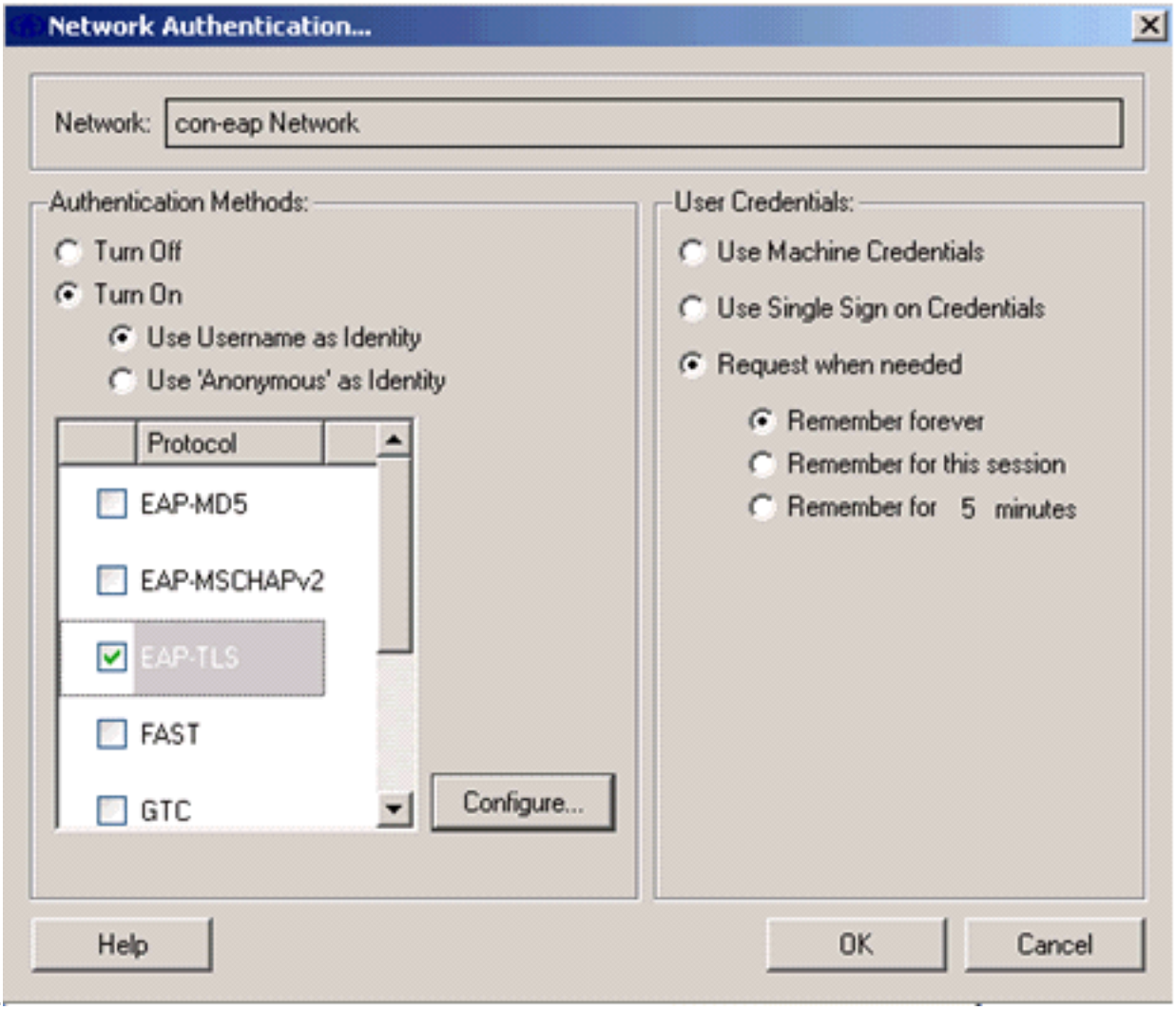
Procédez comme suit :

1. Par défaut, le WLC diffuse le SSID, de sorte qu'il est affiché dans la liste Créer des réseaux de SSID analysés. Afin de créer un profil réseau, vous pouvez cliquer sur le SSID dans la liste (Entreprise) et cliquer sur **Créer un réseau**.Si l'infrastructure WLAN est configurée avec le SSID de diffusion désactivé, vous devez ajouter manuellement le SSID. Pour ce faire, cliquez sur **Ajouter** sous Périphériques d'accès et saisissez manuellement le SSID approprié (par exemple, Entreprise). Configurez le comportement de la sonde active pour le client. C'est-à-dire que le client recherche activement son SSID configuré. Spécifiez **la recherche active de ce périphérique d'accès** après avoir entré le SSID dans la fenêtre Ajouter un périphérique d'accès.**Remarque :** Les paramètres de port ne permettent pas les modes d'entreprise (802.1X) si les paramètres d'authentification EAP ne sont pas configurés pour le profil.
2. Cliquez sur **Créer un réseau** afin de lancer la fenêtre Profil réseau, qui vous permet d'associer le SSID choisi (ou configuré) à un mécanisme d'authentification. Attribuez un nom

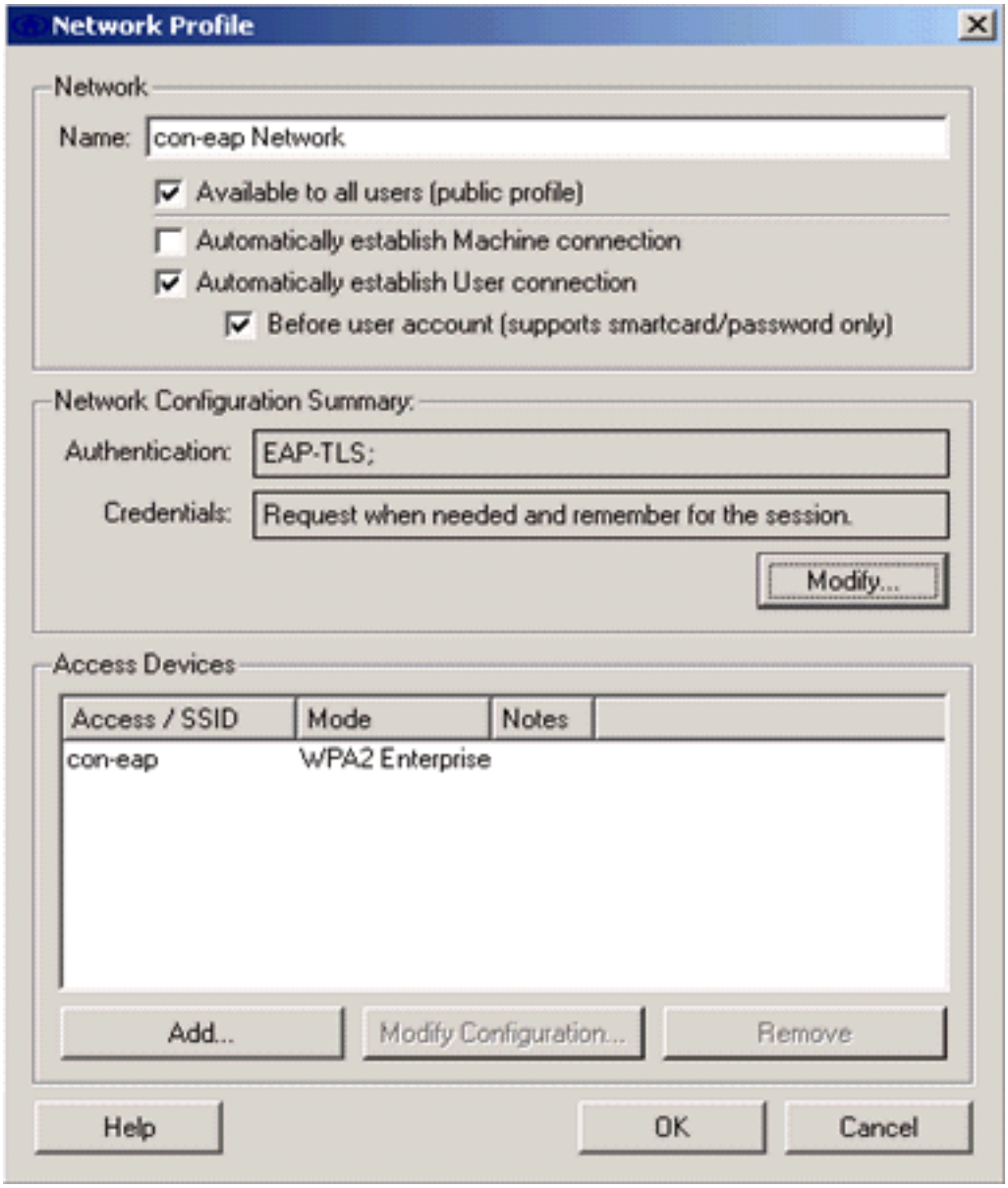
descriptif au profil.**Remarque :** Plusieurs types de sécurité WLAN et/ou SSID peuvent être associés sous ce profil
d'authentification.



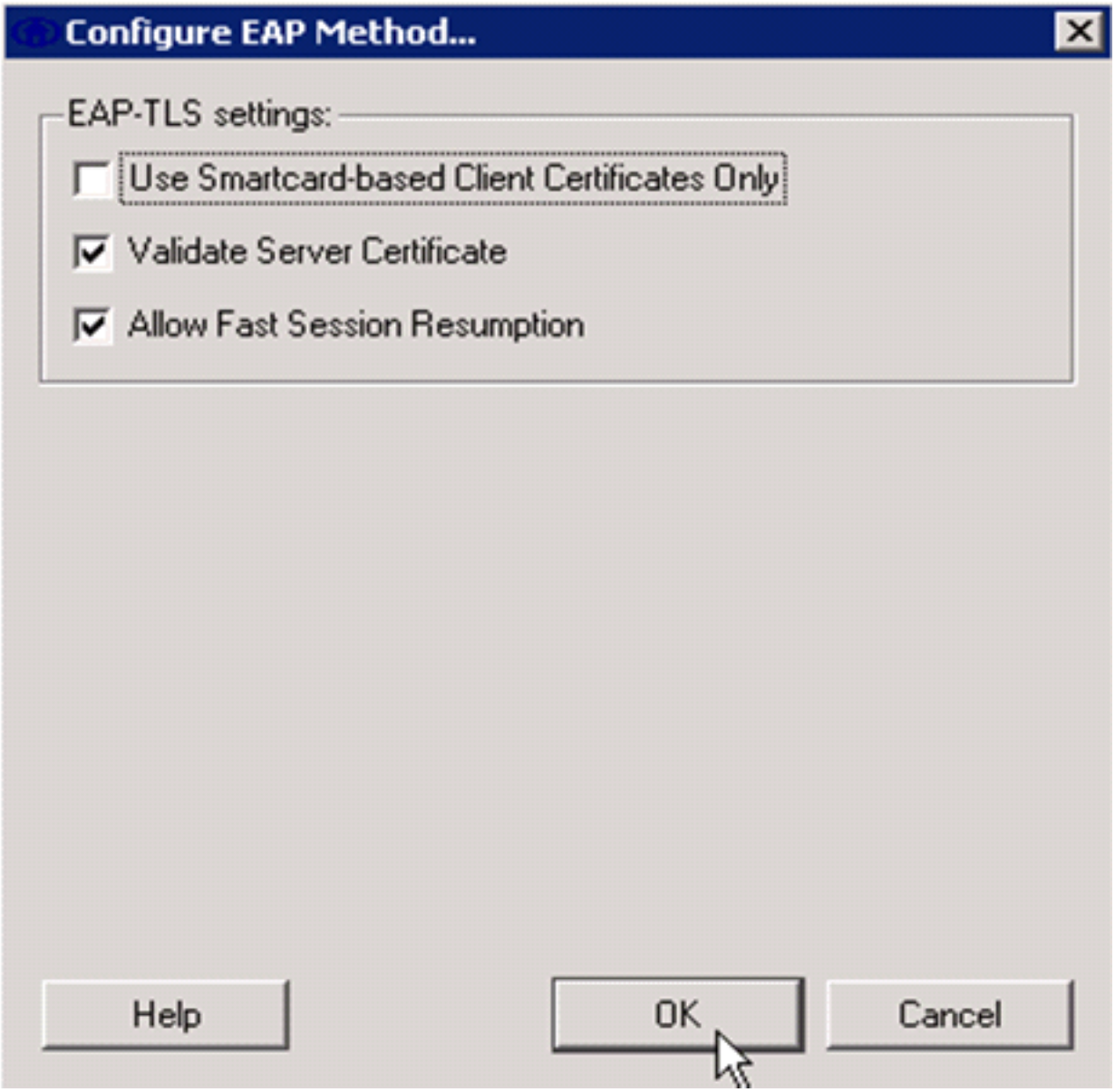

3. Activez l'authentification et vérifiez la méthode EAP-TLS. Cliquez ensuite sur **Configurer** afin de configurer les propriétés EAP-TLS.
4. Sous Network Configuration Summary, cliquez sur **Modify** afin de configurer les paramètres EAP / d'informations d'identification.
5. Spécifiez **Activer l'authentification**, choisissez **EAP-TLS** sous Protocole, et choisissez **Nom d'utilisateur** comme identité.
6. Spécifiez **Utiliser les informations d'identification de connexion unique** pour utiliser les informations d'identification de connexion pour l'authentification réseau. Cliquez sur **Configurer** pour configurer les paramètres EAP-


Network Authentication...
Network:
con-eap Network
Authentication Methods:
Turn Off
Turn On
Use Username as Identity
Use 'Anonymous' as Identity
Protocol
EAP-MD5
EAP-MSCHAPv2
EAP-TLS
FAST
GTC
Configure...
User Credentials:
Use Machine Credentials
Use Single Sign on Credentials
Request when needed
Remember forever
Remember for this session
Remember for 5 minutes
Help
OK
Cancel

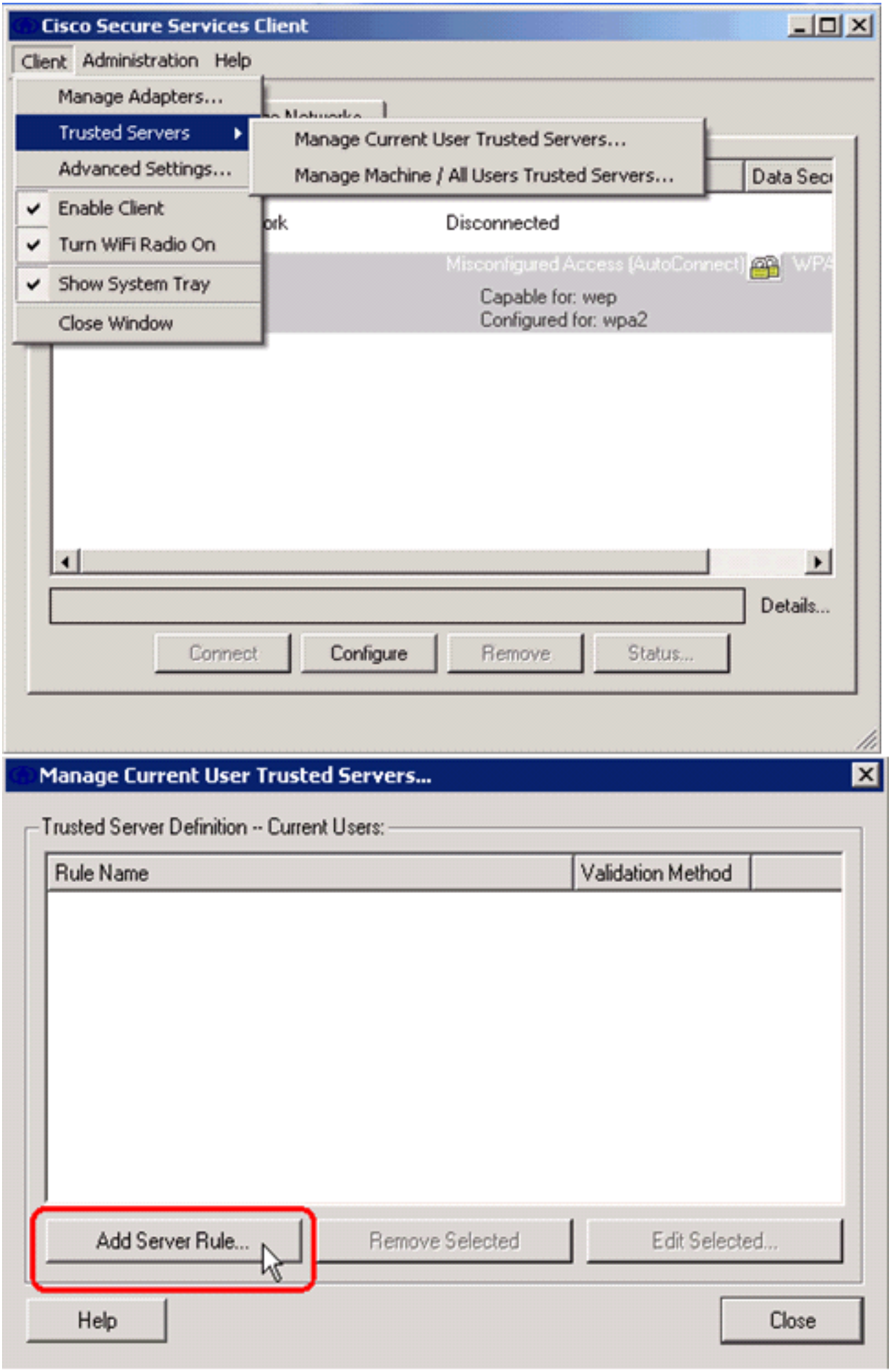
TLS.




7. Pour disposer d'une configuration EAP-TLS sécurisée, vous devez vérifier le certificat du serveur RADIUS. Pour ce faire, cochez la case **Valider le certificat du serveur**.

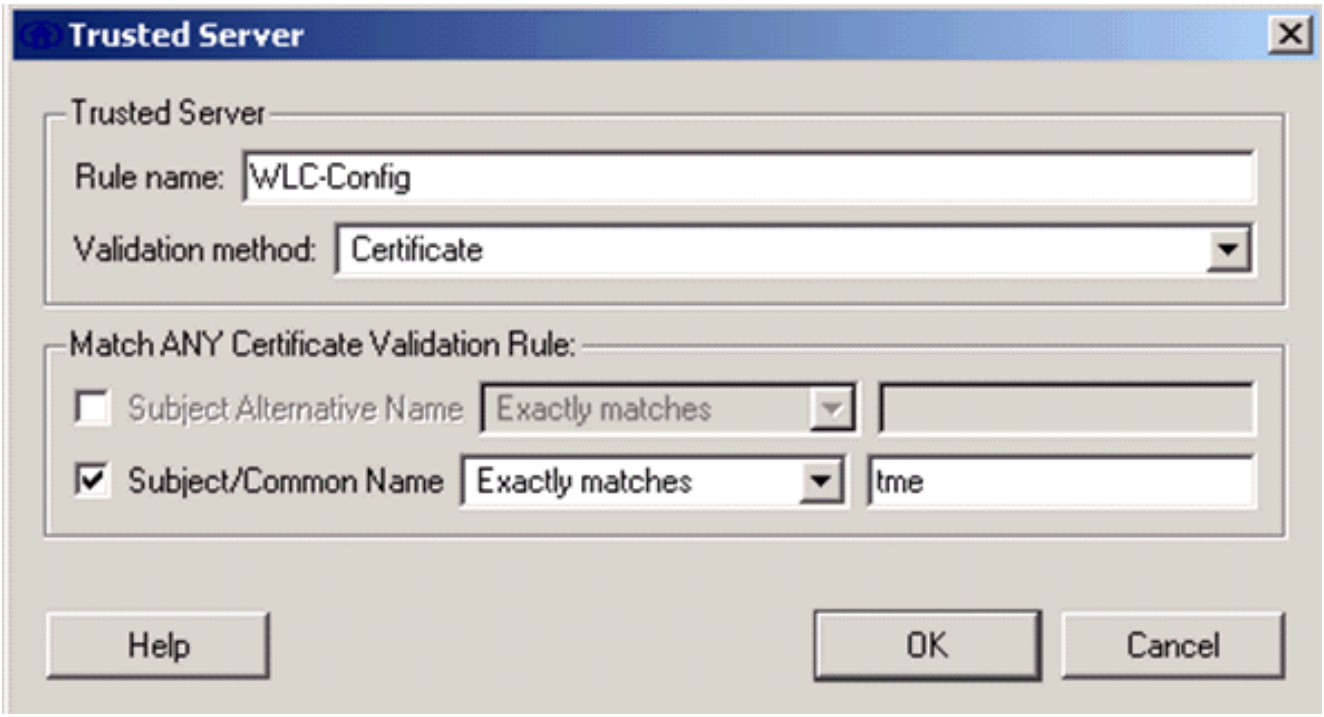



8. Pour valider le certificat du serveur RADIUS, vous devez fournir les informations du client Cisco Secure Services afin d'accepter uniquement le bon certificat. Choisissez **Client > Serveurs approuvés > Gérer les serveurs approuvés de l'utilisateur actuel**.



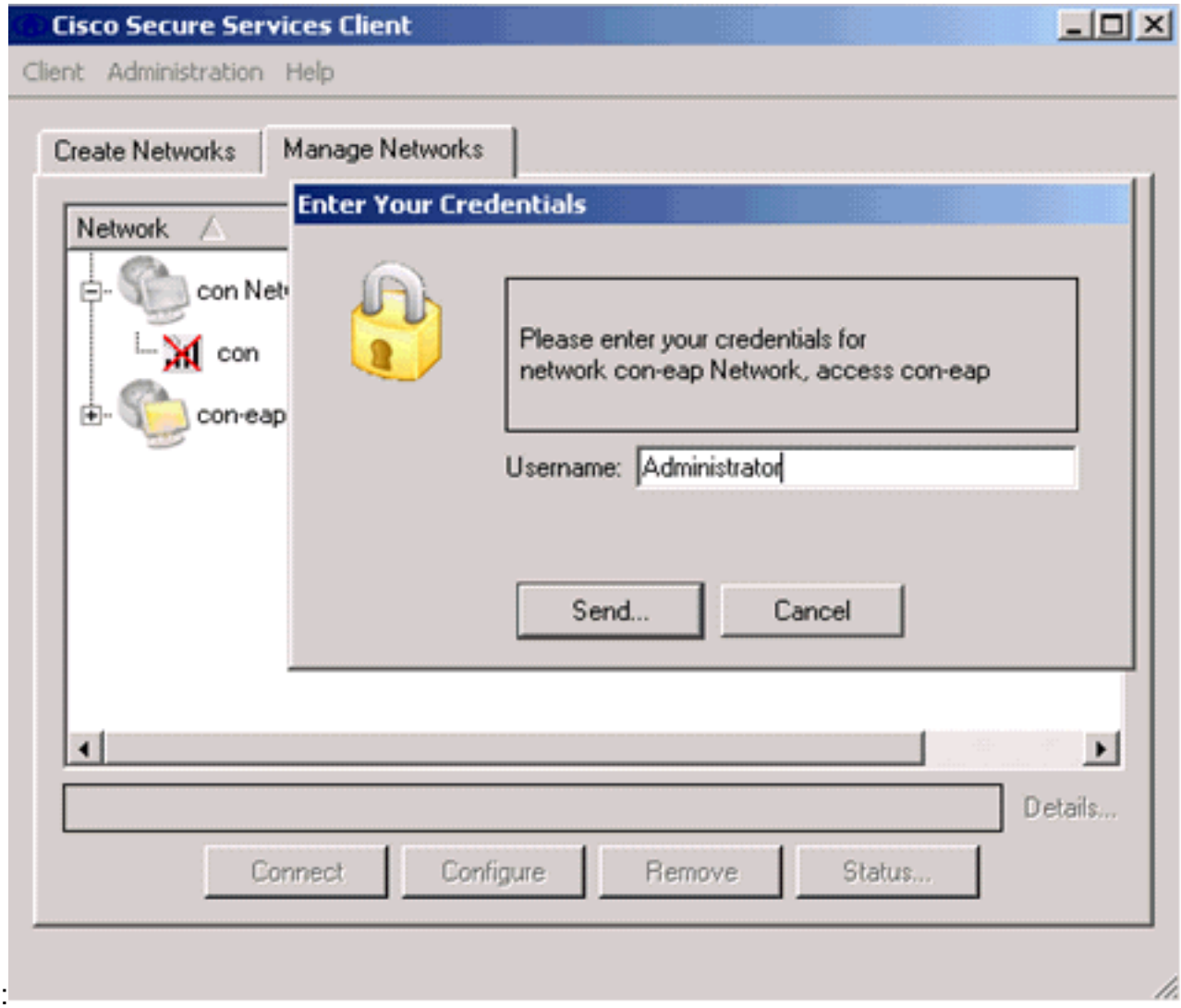

9. Donnez un nom à la règle et vérifiez le nom du certificat du

serveur.




La configuration EAP-TLS est terminée.

10. Connectez-vous au profil de réseau sans fil. Le client Cisco Secure Services demande la connexion de l'utilisateur

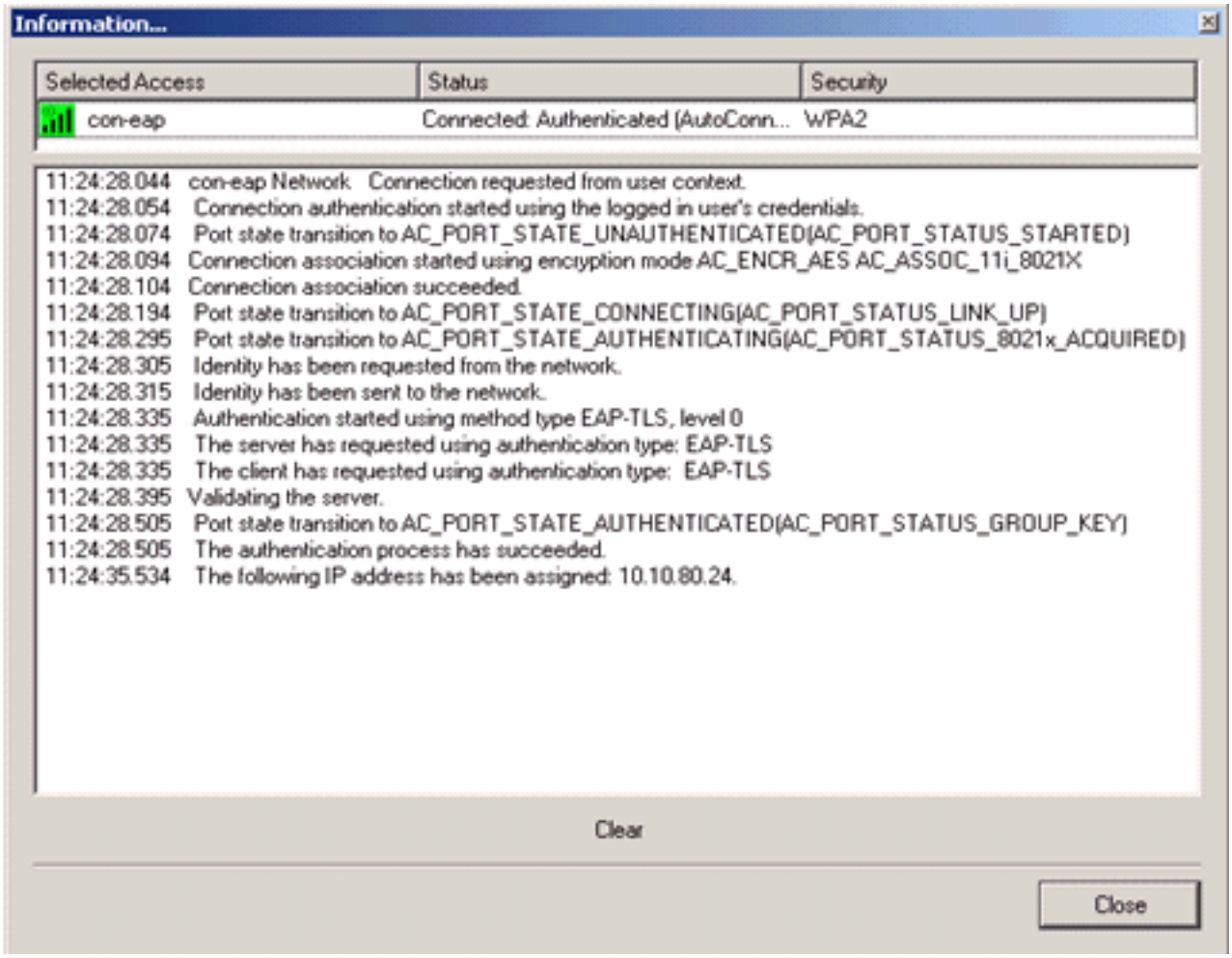


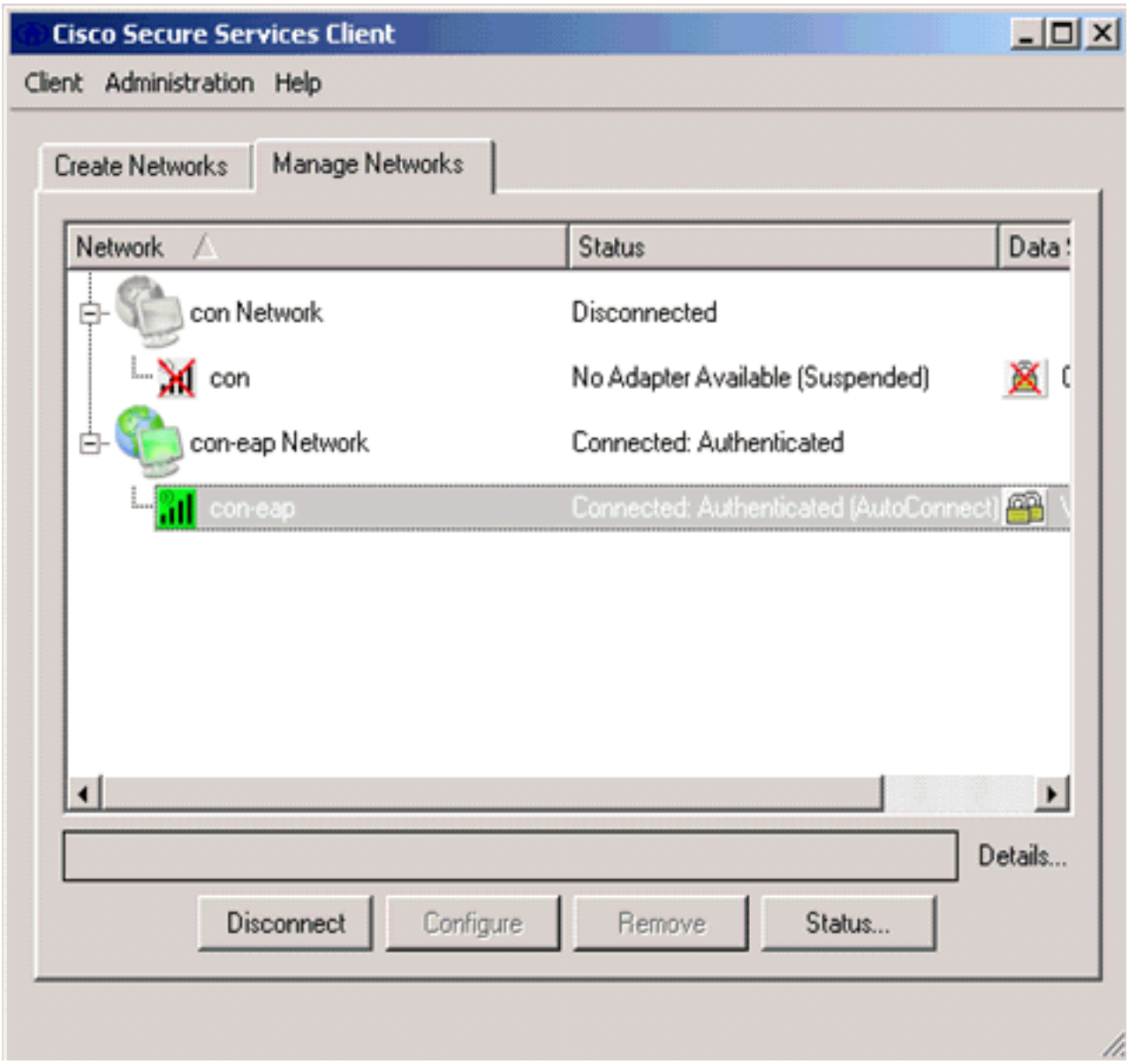

:L

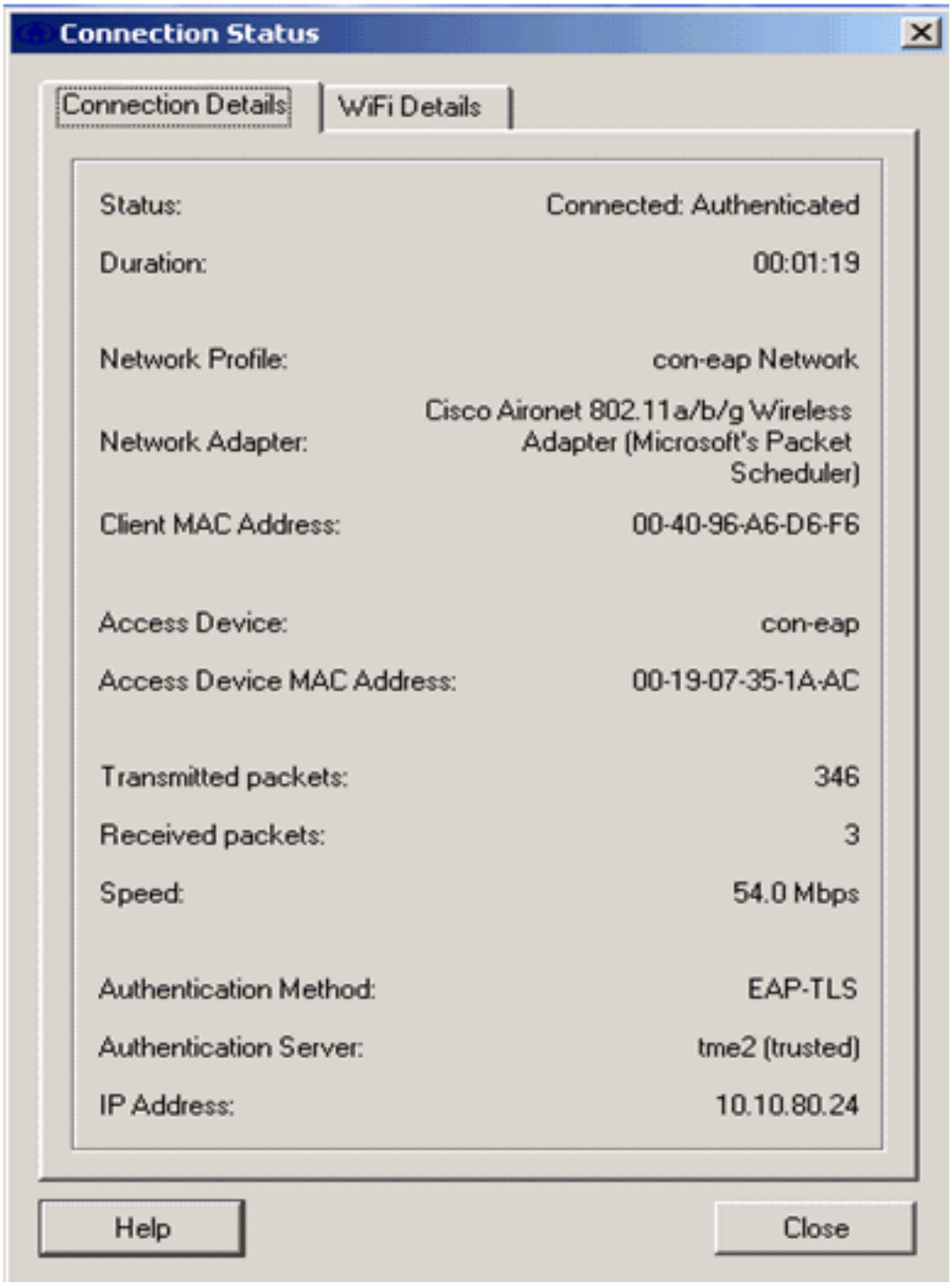
e client Cisco Secure Services reçoit le certificat du serveur et le vérifie (avec la règle

configurée et l'autorité de certification installée). Il demande ensuite l'utilisation du certificat pour l'utilisateur.

11. Une fois le client authentifié, sélectionnez **SSID** sous Profil dans l'onglet Gérer les réseaux et cliquez sur **État** pour interroger les détails de connexion.La fenêtre Détails de la connexion fournit des informations sur le périphérique client, l'état et les statistiques de la connexion, ainsi que la méthode d'authentification. L'onglet WiFi Details (Détails WiFi) fournit des détails sur l'état de la connexion 802.11, qui inclut le RSSI, le canal 802.11 et l'authentification/chiffrement.




Cisco Secure Services Client
Client
Administration
Help
Create Networks
Manage Networks
Network
Status
Data
con Network
Disconnected
con
No Adapter Available (Suspended)
con-eap Network
Connected: Authenticated
con-eap
Connected: Authenticated (AutoConnect)
Details...
Disconnect
Configure
Remove
Status...




## Commandes de débogage

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes show. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show .**

**Remarque :** reportez-vous à Informations importantes sur les commandes de débogage avant d'utiliser les commandes **de débogage**.

Ces commandes de débogage peuvent être utilisées au niveau du WLC pour surveiller la progression de l'échange d'authentification :

- **debug aaa events enable**
- **debug aaa detail enable**
- **debug dot1x events enable**

- debug dot1x states enable
- debug aaa local-auth eap events enableOU
- debug aaa all enable

## Informations connexes

- Guide de configuration du contrôleur LAN sans fil Cisco, version 4.1
- Prise en charge de la technologie WLAN
- Support et documentation techniques - Cisco Systems