

Configuratievoorbeeld voor Unified Wireless Network Local EAP-server

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[Local EAP op Cisco draadloze LAN-controller configureren](#)

[Local EAP-configuratie](#)

[Microsoft certificeringsinstantie](#)

[Installatie](#)

[Installeer het certificaat in de Cisco draadloze LAN-controller](#)

[Installeer het apparaatcertificaat op de draadloze LAN-controller](#)

[Download een leveranciercertificaat aan de draadloze LAN-controller](#)

[Configureer de draadloze LAN-controller voor het gebruik van EAP-TLS](#)

[Installeer het certificaatcertificaat op het clientapparaat.](#)

[Download en Installeer een Root CA-certificaat voor de client](#)

[Een clientcertificaat genereren voor een clientapparaat](#)

[EAP-TLS met Cisco Secure Services-client op het clientapparaat](#)

[Opdrachten debug](#)

[Gerelateerde informatie](#)

[Inleiding](#)

Dit document beschrijft de configuratie van een lokale MAP-server (Extensible Authentication Protocol) in een Cisco Wireless LAN Controller (WLC) voor de verificatie van draadloze gebruikers.

Plaatselijke MAP is een authenticatiemethode die het mogelijk maakt dat gebruikers en draadloze klanten lokaal worden geauthentiseerd. Het is ontworpen voor gebruik in afgelegen kantoren die verbindingen willen onderhouden met draadloze klanten wanneer het back-end systeem verstoord raakt of de externe authenticatieserver daalt. Wanneer u lokale EAP toelaat, dient de controller als de authenticatieserver en de lokale gebruikersdatabase, waarmee de afhankelijkheid van een externe verificatieserver wordt verwijderd. Plaatselijke MAP haalt gebruikersaanmeldingsgegevens uit de lokale gebruikersdatabase of de Lichtgewicht Directory Access Protocol (LDAP) back-end database om gebruikers echt te maken. Lokale EAP ondersteunt lichtgewicht EAP (LEAP), EAP-Flexibele verificatie via Secure Tunneling (EAP-FAST) en EAP-Transport Layer Security (EAP-TLS)-verificatie tussen de controller en draadloze klanten.

Merk op dat de lokale EAP-server niet beschikbaar is als er een globale externe RADIUS-

serverconfiguratie in de WLC is. Alle verificatieverzoeken worden naar de globale externe RADIUS doorgestuurd totdat de lokale MAP-server beschikbaar is. Als de WLC de connectiviteit op de externe RADIUS-server verliest, wordt de lokale EAP-server actief. Als er geen algemene RADIUS-serverconfiguratie is, wordt de lokale EAP-server onmiddellijk actief. De lokale EAP-server kan niet gebruikt worden om cliënten te authenticeren, die verbonden zijn met andere WLC's. Met andere woorden, het ene WLC kan zijn EAP-verzoek niet aan een andere WLC doorsturen voor authenticatie. Elke WLC zou zijn eigen lokale EAP server en individuele database moeten hebben.

Opmerking: gebruik deze opdrachten om te voorkomen dat WLC verzoeken naar een externe straal server verstuurt.

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

De lokale EAP-server ondersteunt deze protocollen in 4.1.171.0 softwarerelease en later:

- LEAP
- EAP-FAST (zowel gebruikersnaam/wachtwoord als certificaten)
- EAP-TLS

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Kennis van het configureren van WLC's en lichtgewicht access points (LAP's) voor gebruik als basiseenheid
- Kennis van Lichtgewicht Access Point Protocol (LWAPP) en draadloze beveiligingsmethoden
- Basiskennis van lokale MAP-authenticatie.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Windows XP met CB21AG adapterkaart en Cisco Secure Services client versie 4.0
- Cisco 4400 draadloze LAN-controller 4.1.17.0
- Microsoft Certified Authority op Windows 2000-server

Conventies

Raadpleeg [Cisco Technical Tips Conventions \(Conventies voor technische tips van Cisco\) voor meer informatie over documentconventies.](#)

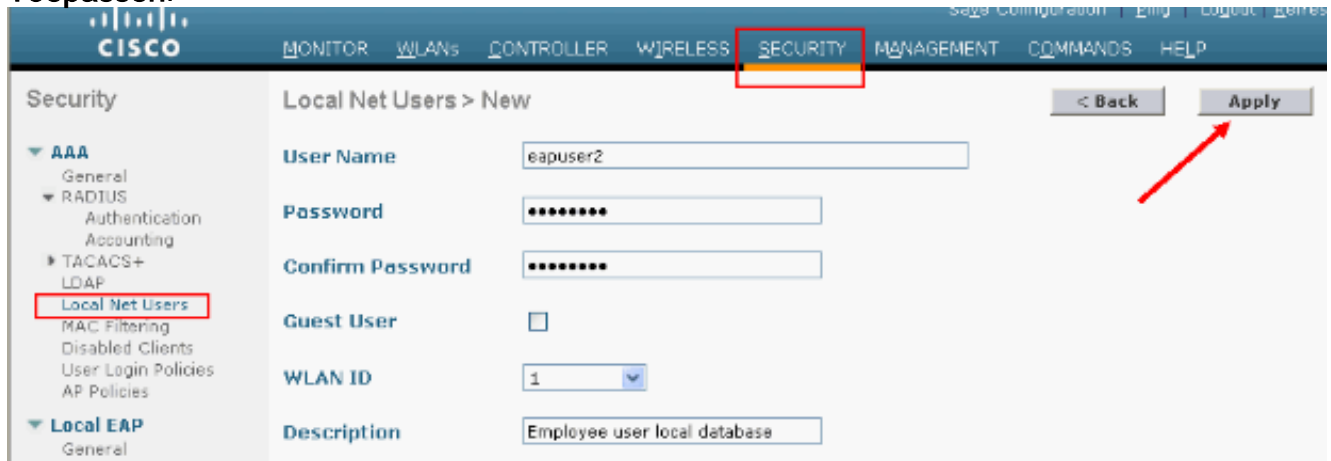
Local EAP op Cisco draadloze LAN-controller configureren

Dit document gaat ervan uit dat de basisconfiguratie van de WLC al is voltooid.

Local EAP-configuratie

Voltooi deze stappen om lokale MAP te configureren:

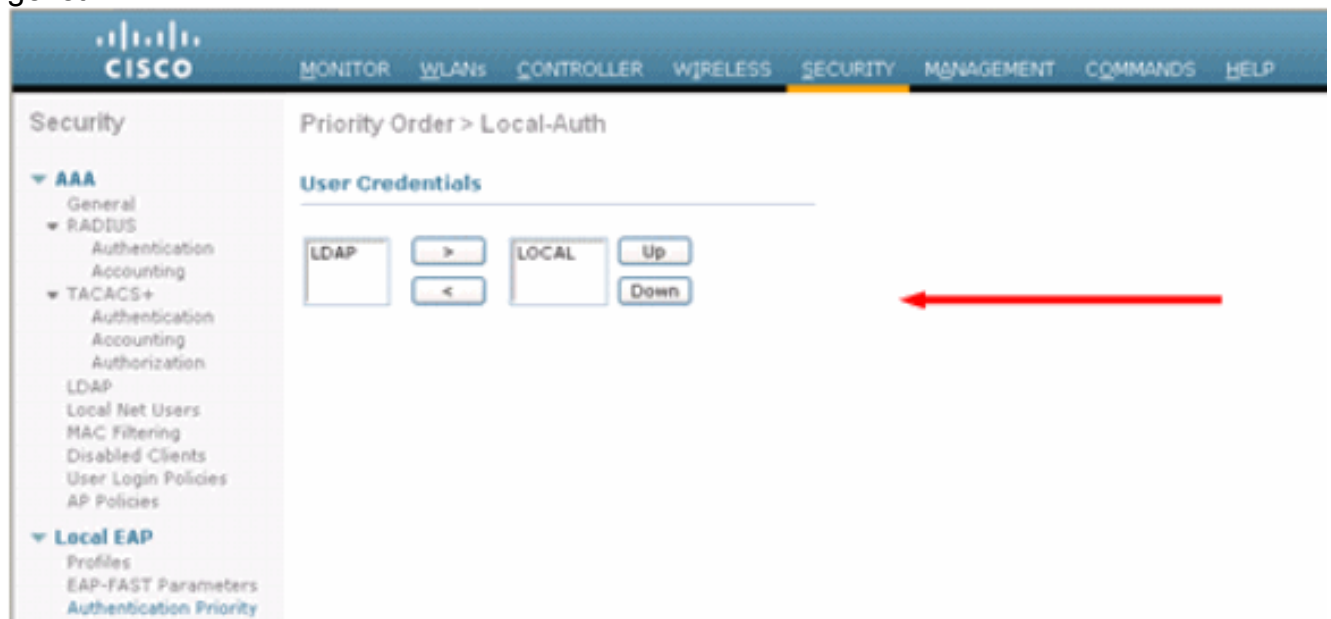
1. Voeg een lokale netgebruiker toe: Kies in de GUI. **Beveiliging > Lokale Net-gebruikers > Nieuw**, voer de gebruikersnaam, het wachtwoord, de gastgebruiker, WLAN-id en de beschrijving in en klik op **Toepassen**.



Vanuit de CLI kunt u het **configuratieset** gebruiken om **<gebruikersnaam><wachtwoord><WLAN id><beschrijving>opdracht toe te voegen**: **Opmerking**: deze opdracht is vanwege ruimtelijke redenen naar een tweede regel teruggebracht.

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

2. Specificeer de terugwinningsvolgorde voor gebruikersinterface. Kies in de GUI **Security > Local EAP > Accounting Priority**. Selecteer LDAP en klik op "<" en klik op **Toepassen**. Hiermee worden de gebruikersreferenties in de lokale database eerst gezet.

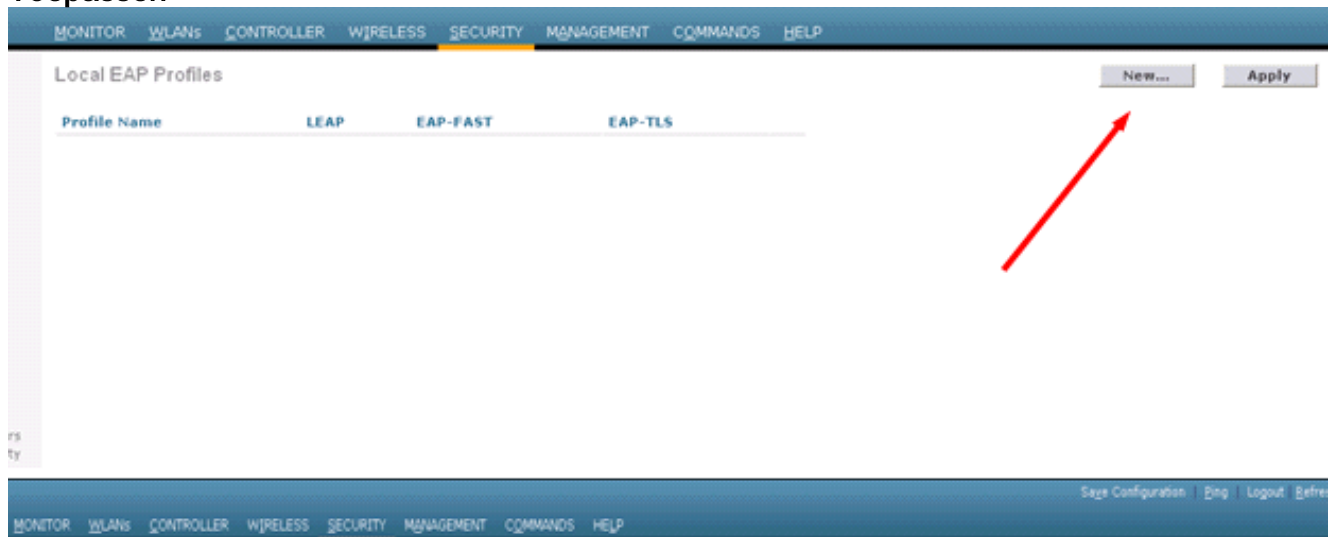


Van de CLI:

```
(Cisco Controller) >config local-auth user-credentials local
```

3. Een MAP-profiel toevoegen: Om dit vanuit de GUI te doen, kiest u **Beveiliging > Local EAP > Profiles** en klikt u op **New**. Wanneer het nieuwe venster verschijnt, typt u de Profile Name en

klikt u op
Toepassen.



U kunt dit ook doen door de CLI-opdracht **configuratie van de lokale auth-eap-profile add <profile-name> te gebruiken.** In ons voorbeeld is de profielnaam een *EAP-test*.

(Cisco Controller) **>config local-auth eap-profile add EAP-test**

- Voeg een methode toe aan het MAP-profiel. Kies in de GUI **Security > Local EAP > Profiles** en klik op de profielnaam waarvoor u de authenticatiemethoden wilt toevoegen. In dit voorbeeld wordt gebruik gemaakt van LEAP, EAP-FAST en EAP-TLS. Klik op **Toepassen** om de methoden in te stellen.

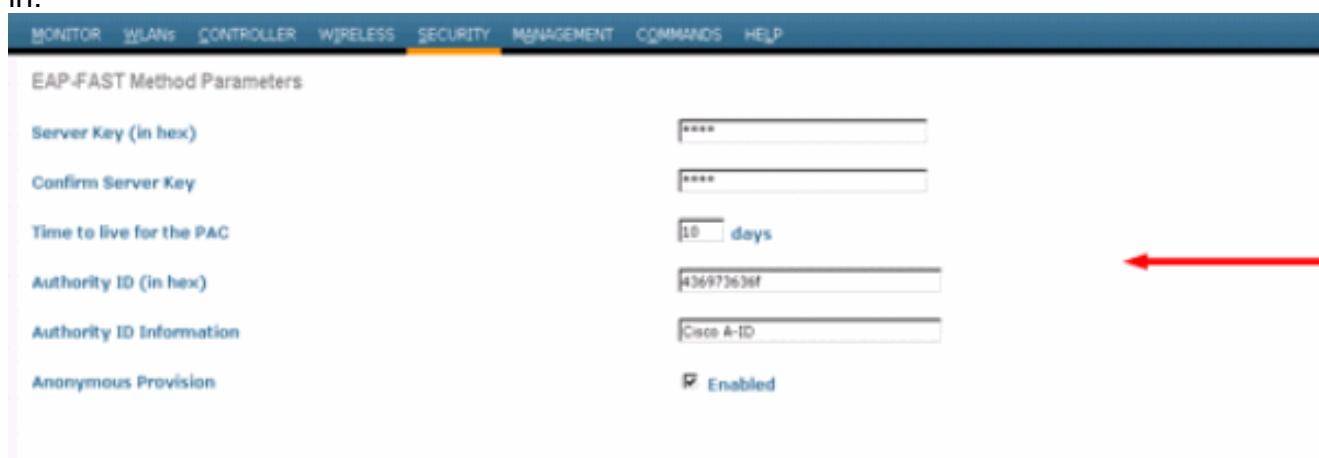


U kunt ook de CLI opdracht **mede-configuratie van de lokale auth-eap-profile methode gebruiken om <methode-name><profile-name> toe te voegen.** In onze voorbeeldconfiguratie voegen we drie methoden toe aan de MAP-profieltest. De methoden zijn LEAP, EAP-FAST en EAP-TLS, waarvan de methodenamen respectievelijk *springen* en *hoog* zijn. Deze uitvoer

toont de CLI configuratieopdrachten:

```
(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. Configureer de parameters van de MAP-methode. Dit wordt alleen gebruikt voor EAP-FAST. De parameters die moeten worden ingesteld zijn: **Server Key (server-key)**-serversleutel om beschermde toegangsgegevens (PAC's) te versleutelen/decrypteren (in hexadecimaal). **Tijd om te leven voor PAC (pac-tl)** Hiermee wordt de tijd ingesteld om te leven voor de PAC. **Bevoegde autoriteit-id** —Hiermee stelt u de autoriteit-identificator in. **Anonymous Voorziening (anon-provn)** - vormt of anonieme bepaling wordt toegestaan. Dit is standaard ingeschakeld. Voor configuratie via de GUI, kies **Beveiliging > Lokaal MAP > EAP-FAST-parameters** en voer de servertoets, de tijd om voor de PAC te leven, autoriteit-ID (in hex) en de waarde van de autoriteit-ID in.



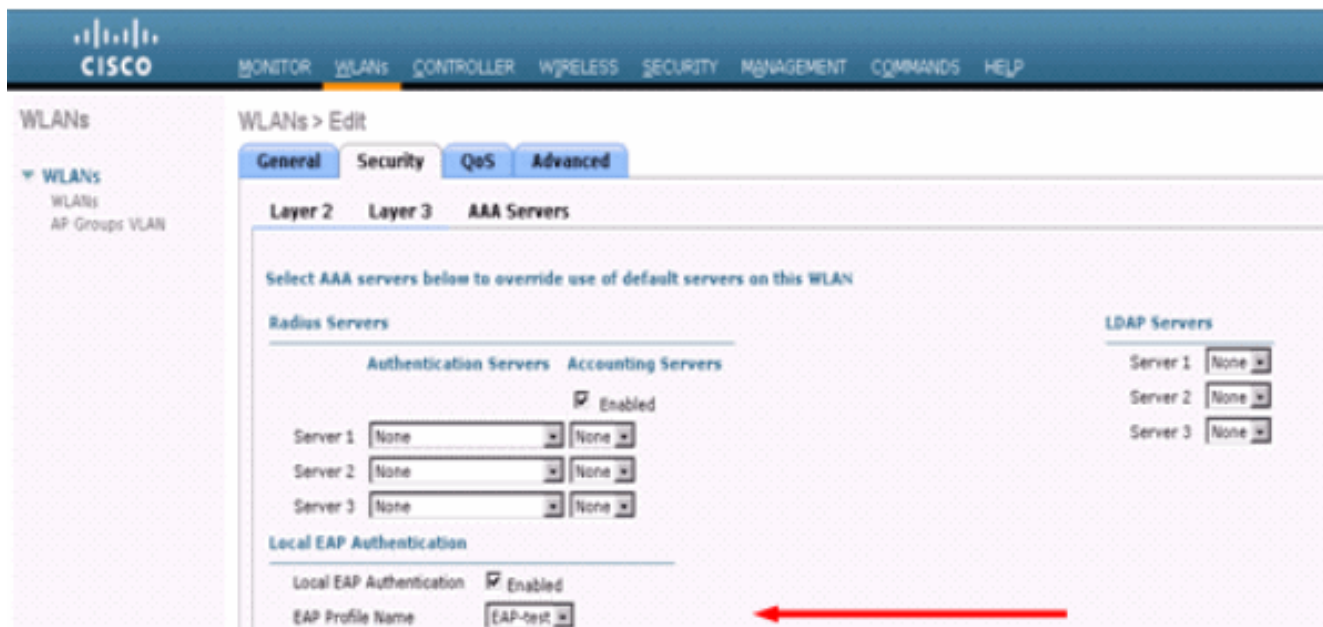
The screenshot shows the 'EAP-FAST Method Parameters' configuration page. The fields are as follows:

Parameter	Value
Server Key (in hex)	****
Confirm Server Key	****
Time to live for the PAC	10 days
Authority ID (in hex)	43697363f1
Authority ID Information	Cisco A-ID
Anonymous Provision	<input checked="" type="checkbox"/> Enabled

Dit zijn de CLI-configuratieopdrachten die moeten worden gebruikt om deze parameters voor EAP-FAST in te stellen:

```
(Cisco Controller) >config local-auth method fast server-key 12345678  
(Cisco Controller) >config local-auth method fast authority-id 43697363f1 CiscoA-ID  
(Cisco Controller) >config local-auth method fast pac-ttl 10
```

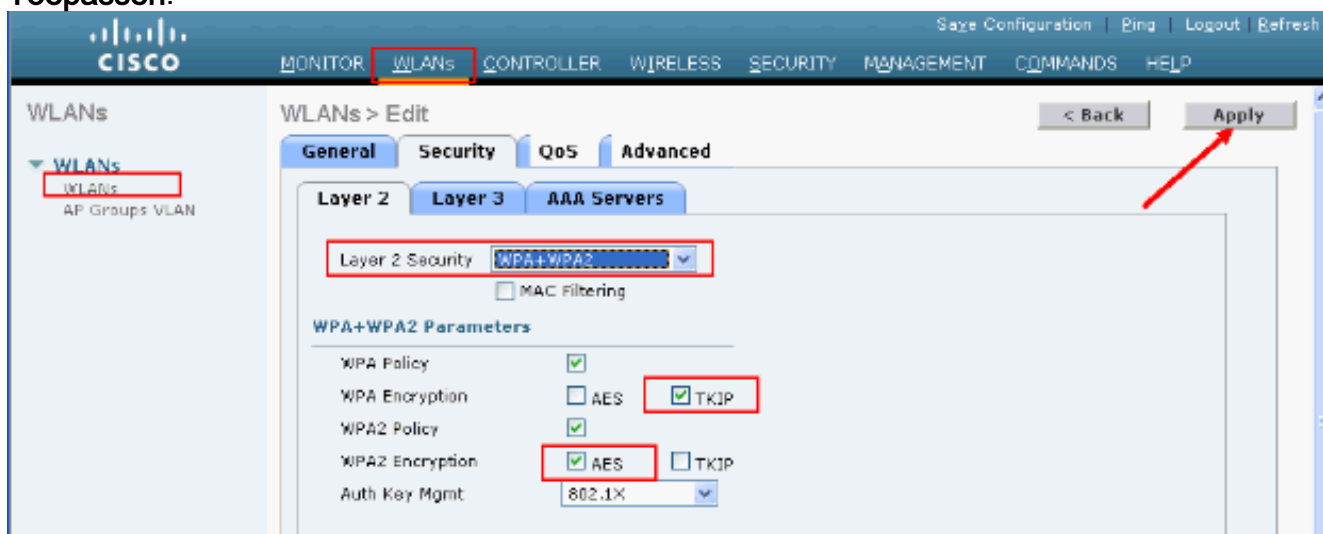
6. Lokale verificatie per WLAN inschakelen: Kies in de GUI **WLAN's** in het bovenste menu en selecteer de WLAN's waarvoor u lokale verificatie wilt configureren. Er verschijnt een nieuw venster. Klik op de tabbladen **Security > AAA**. Controleer **lokale MAP-verificatie** en selecteer de juiste MAP-profielnaam in het keuzemenu zoals in dit voorbeeld wordt weergegeven:



U kunt ook het CLI **Config-lokaal-auth** uitvoeren om **<profiel-naam><WLAN-id>** configuratieopdracht zoals hieronder wordt getoond, uit te geven:

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

7. Stel Layer 2 security parameters in. Vanuit de GUI-interface gaat in het venster WLAN-bewerking naar de tabbladen **Security > Layer 2** en kiest u **WPA+WAP2** uit het keuzemenu Layer 2 Security. Stel onder het gedeelte WPA+WAP2-parameters de WPA-encryptie in op **TKIP** en WAP2-encryptie **AES**. Klik vervolgens op **Toepassen**.



Gebruik vanuit CLI deze opdrachten:

```
(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. Controleer de configuratie:

```
(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

```

U kunt specifieke parameters van VLAN 1 zien met de opdracht Show WLAN <wlan>:

(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

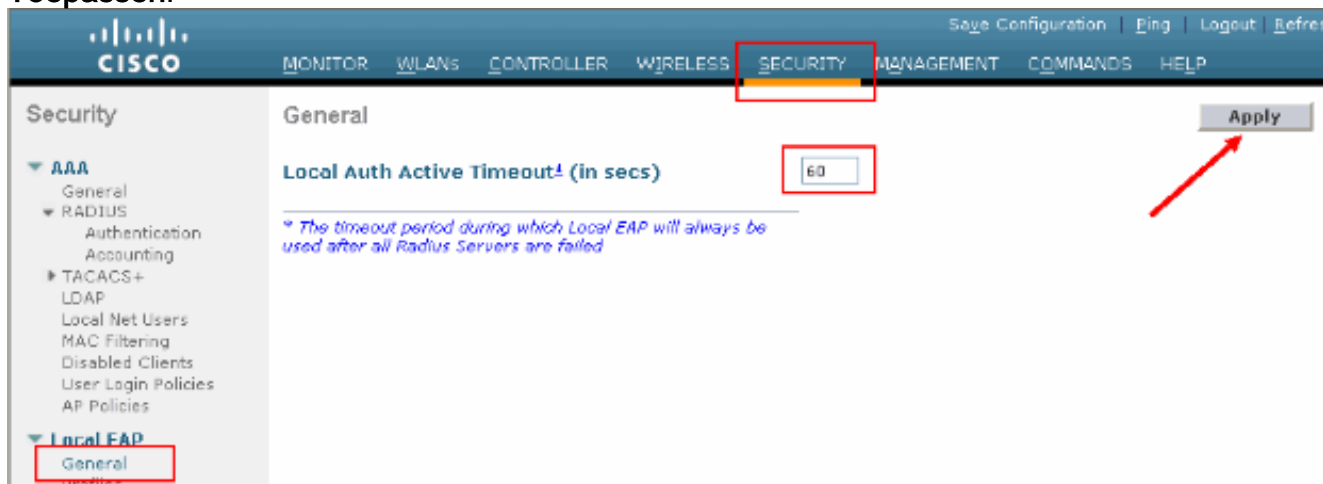
```

```

Mobility Anchor List
WLAN ID      IP Address      Status

```

Er zijn andere lokale authenticatieparameters die kunnen worden geconfigureerd, in het bijzonder de actieve time-out timer. Deze timer vormt de periode waarin lokale EAP wordt gebruikt nadat alle RADIUS-servers zijn mislukt. Kies in de GUI, **Security > Local EAP > General** en stel de tijdwaarde in. Klik vervolgens op **Toepassen**.



Geef deze opdrachten vanuit CLI uit:

```

(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

```

U kunt de waarde verifiëren waaraan deze timer is ingesteld wanneer u het opdracht **lokaal-auth** configuratie afgeeft.

```

(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. Als u de handleiding voor PAC wilt genereren en laden, kunt u de GUI of de CLI gebruiken. Selecteer in de GUI de optie **OPDRACHTEN** in het bovenste menu en kies de

optie **Bestand uploaden** in de lijst aan de rechterkant. Selecteer **PAC (Protected Access Credentials)** in het keuzemenu van het bestandstype. Voer alle parameters in en klik op **Upload**.

Voer vanuit CLI deze opdrachten in:

```
(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.

Om de MAP-FAST versie 2 en MAP-TLS-authenticatie te kunnen gebruiken, moeten de WLC en alle clientapparaten over een geldig certificaat beschikken en tevens het publieke certificaat van de certificeringsinstantie kennen.

Installatie

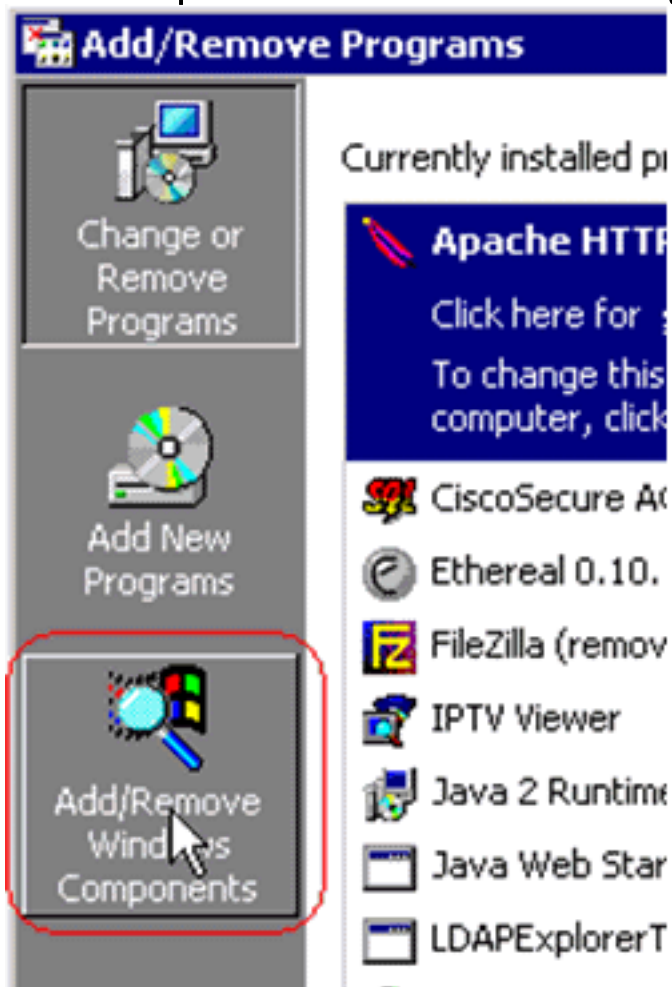
Als de Windows 2000 Server niet reeds de diensten van de certificeringsinstantie geïnstalleerd heeft, moet u het installeren.

Voltooi deze stappen om de Microsoft certificeringsinstantie in te schakelen op een Windows 2000-server:

1. Kies in het Configuratiescherm de optie **Software**.



2. Selecteer **Windows-componenten aan de linkerkant toevoegen of**

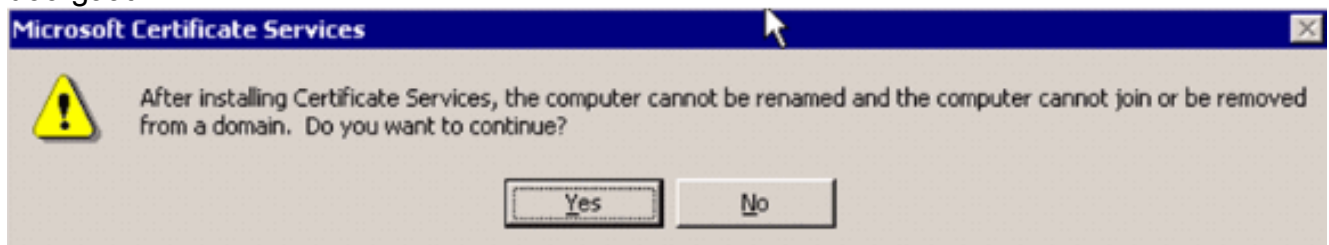


verwijderen.

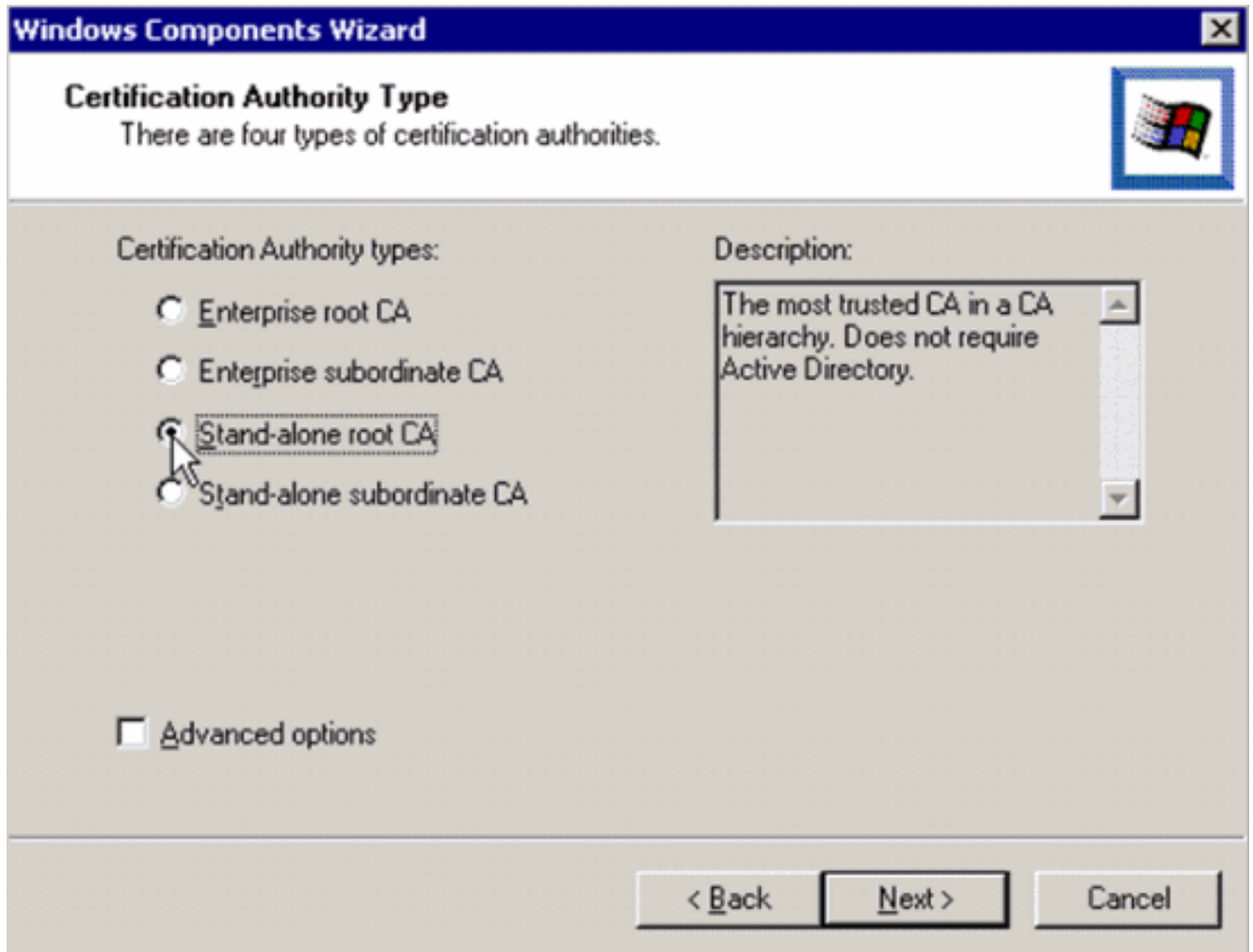
3. Controleer de **certificaatservices**.



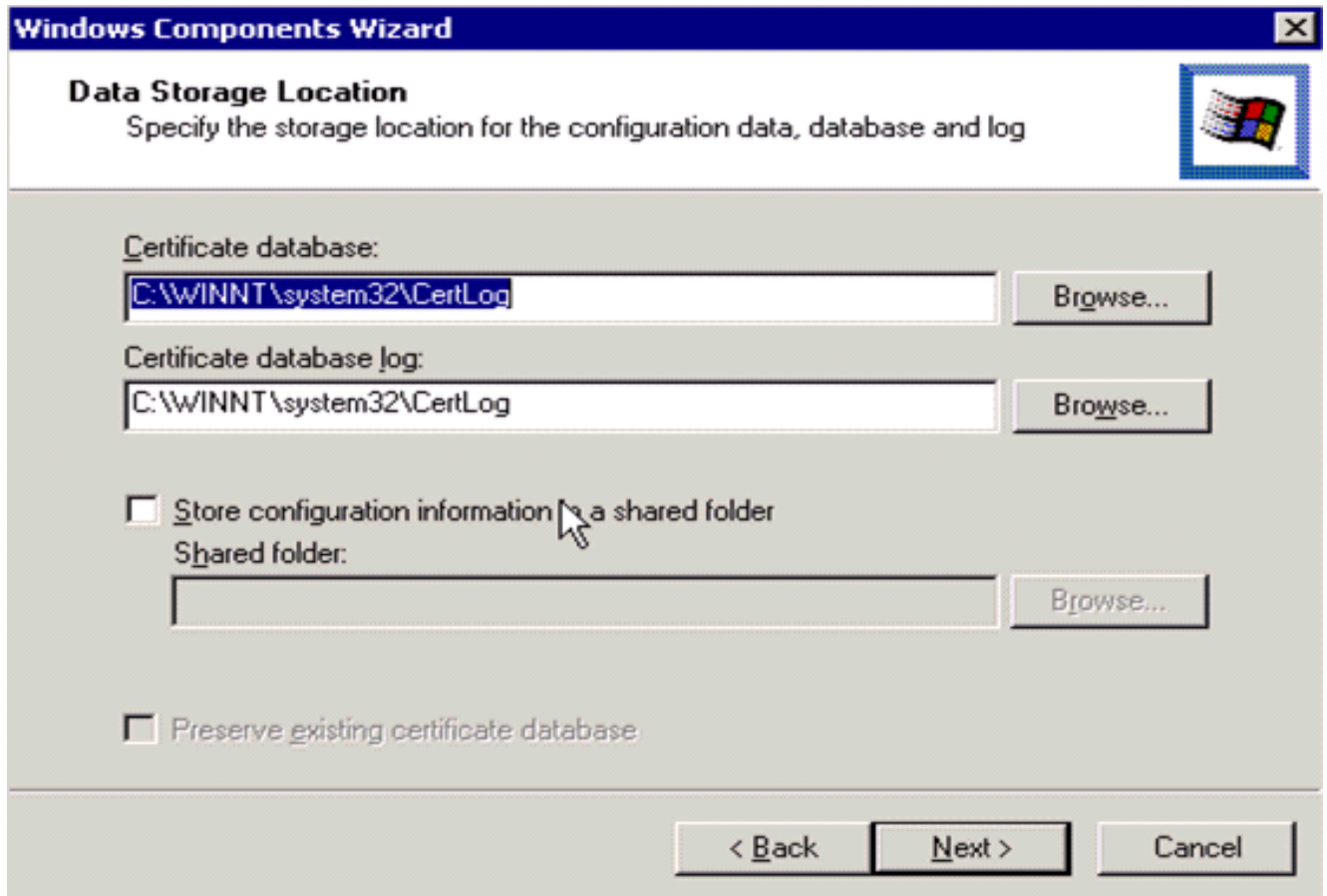
Controleer deze waarschuwing voordat u doorgaat:



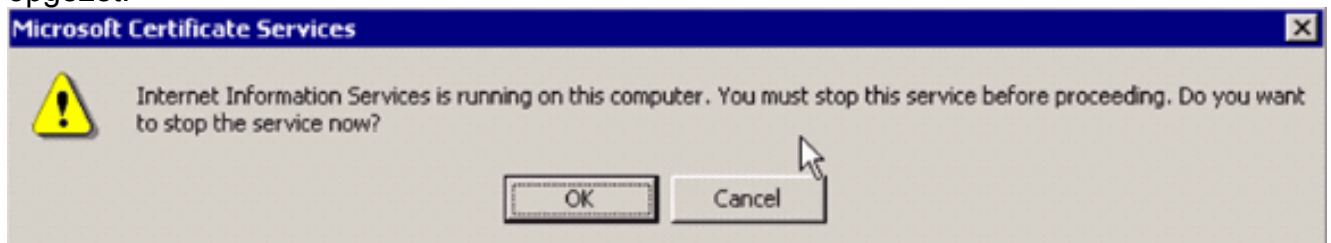
4. Selecteer welk type certificeringsinstantie u wilt installeren. Om een eenvoudig op zichzelf staand gezag te creëren, selecteert u **Afstand-alone wortel CA**.



5. Voer de nodige informatie in over de certificeringsinstantie. Deze informatie creëert een zelf-ondertekend certificaat voor uw certificeringsinstantie. Onthoud de CA-naam die u gebruikt. De certificeringsinstantie slaat de certificaten op in een database. In dit voorbeeld wordt de standaardinstelling gebruikt die door Microsoft is voorgesteld:



6. De diensten van de certificeringsinstantie van Microsoft gebruiken de server van het ISIS Microsoft om client- en servercertificaten te creëren en te beheren. De IS-dienst moet hiervoor opnieuw worden opgezet:



De Microsoft Windows 2000 Server installeert nu de nieuwe service. U hebt uw installatie-cd voor Windows 2000-servers nodig om nieuwe Windows-onderdelen te installeren. De certificeringsinstantie is nu geïnstalleerd.

[Installeer het certificaat in de Cisco draadloze LAN-controller](#)

Om EAP-FAST versie 2 en EAP-TLS op de lokale MAP server van een Cisco draadloze LAN controller te gebruiken, volgt u deze drie stappen:

1. [Installeer het apparaatcertificaat op de draadloze LAN-controller.](#)
2. [Download een leveranciercertificaat aan de draadloze LAN-controller.](#)
3. [Configureer de draadloze LAN-controller voor het gebruik van EAP-TLS.](#)

Merk op dat in het voorbeeld in dit document, de Access Control Server (ACS) op dezelfde host is geïnstalleerd als de Microsoft Active Directory en Microsoft Certification Authority, maar de configuratie dient hetzelfde te zijn als de ACS-server op een andere server is.

Installeer het apparaatcertificaat op de draadloze LAN-controller

Voer de volgende stappen uit:

1. . Voltooi deze stappen om het certificaat voor invoer in de WLC te genereren: Ga naar **http://<serverIpAddress>/certsrv**. Kies een certificaat aanvragen en klik op **Volgende**. Klik op **Geavanceerde aanvraag** en klik op **Volgende**. Kies een certificaataanvraag bij deze CA indienen met behulp van een formulier en klik op **Volgende**. Kies **webserver** voor certificaatsjabloon en voer de relevante informatie in. Merk de sleutels vervolgens op als **uitvoerbaar**. U ontvangt nu een certificaat dat u in uw machine moet installeren.
2. Voltooi deze stappen om het certificaat van de pc terug te halen: Open een browser van Internet Explorer en kies **Gereedschappen > Internet-opties > Content**. Klik op **Certificaten**. Selecteer het nieuwe geïnstalleerde certificaat in het keuzemenu. Klik op **Exporteren**. Klik tweemaal op **Volgende** en kies **Ja exporteren de privé-toets**. Dit formaat is het PKCS#12 (PFX-formaat). Kies **sterke bescherming inschakelen**. Typ een wachtwoord. Opslaan in een bestand <tme2.pfx>.
3. Kopieer het certificaat in de PKCS#12-indeling naar een computer waarop u OpenSSL hebt geïnstalleerd, zodat het naar PEM-indeling wordt geconverteerd.

```
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. Download het geconverteerde PEM-formaat certificaat op de 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. Controleer het certificaat zodra u het hebt herstart.

```
(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

[Download een leveranciercertificaat aan de draadloze LAN-controller](#)

Voer de volgende stappen uit:

1. Voltooi deze stappen om het CA-certificaat van de verkoper terug te halen: Ga naar **http://<serverIpAddress>/certsrv**. Kies **Ophalen het CA-certificaat** en klik op **Volgende**. Kies het CA-certificaat. Klik op **DER gecodeerd**. Klik op **CA-certificaat downloaden** en het certificaat opslaan als **rootca.cer**.
2. De verkoper CA van het DER-formaat converteren naar het PEM-formaat met de **openssl x509-in rootca.cer -informeert DER-out rootca.pem -buiten PEM-opdracht**. Het uitvoerbestand is **rootca.pem** in de PEM-indeling.
3. Download het CA-certificaat van verkoper:

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

```
(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.
```

[Configureer de draadloze LAN-controller voor het gebruik van EAP-TLS](#)

Voer de volgende stappen uit:

Kies in de GUI, **Security > Local EAP > Profiles**, kies het profiel en controleer op deze instellingen:

- Lokaal certificaat vereist is ingeschakeld.
- Clientcertificaat vereist is ingeschakeld.
- Certificaat-uitgever is verkoper.
- Controleer tegen CA-certificaten is ingeschakeld.

The screenshot shows the Cisco SCA interface for configuring a Local EAP Profile. The profile name is 'EAP-test'. The configuration table is as follows:

Configuration Item	Value / Status
Profile Name	EAP-test
LEAP	<input type="checkbox"/>
EAP-FAST	<input type="checkbox"/>
EAP-TLS	<input type="checkbox"/>
Local Certificate Required	<input checked="" type="checkbox"/> Enabled
Client Certificate Required	<input checked="" type="checkbox"/> Enabled
Certificate Issuer	Vendor
Check against CA certificates	<input checked="" type="checkbox"/> Enabled
Verify Certificate CN Identity	<input type="checkbox"/> Enabled
Check Certificate Date Validity	<input type="checkbox"/> Enabled

[Installeer het certificaatcertificaat op het clientapparaat.](#)

[Download en Installeer een Root CA-certificaat voor de client](#)

De client moet een basiscertificaat van CA van een server van de certificeringsinstantie verkrijgen. Er zijn meerdere methoden die u kunt gebruiken om een client-certificaat te verkrijgen en het in de Windows XP-machine te installeren. Om een geldig certificaat te kunnen verkrijgen, moet de Windows XP-gebruiker zijn aangemeld bij het gebruik van zijn gebruikersidentificatie en moet er een netwerkverbinding zijn.

Een webbrowser op de Windows XP client en een bekabelde verbinding met het netwerk werden gebruikt om een client certificaat te verkrijgen van de server van de Private root Certified Authority. Deze procedure wordt gebruikt om het client-certificaat te verkrijgen van een server van de Microsoft certificeringsinstantie:

1. Gebruik een webbrowser op de client en plaats de browser naar de server van de certificeringsinstantie. Voer hiervoor **http://IP-address-of-Root-CA/certsrv** in.
2. Meld u aan bij gebruik van **Domain_Name\user_name**. U moet inloggen met behulp van de gebruikersnaam van het individu dat de XP-client moet gebruiken.
3. Kies in het venster Welcome **een CA-certificaat ophalen** en klik op **Next**.
4. Selecteer **Base64 Encoding** en **Download CA certificaat**.
5. Klik in het venster certificaatuitgifte op **Installeer dit certificaat** en klik op **Volgende**.
6. Kies **Automatisch de certificaatopslag selecteren** en klik op **Volgende**, voor een succesvol importbericht.
7. Connect met de certificeringsinstantie voor het opvragen van het certificaat van de certificeringsinstantie:

Welcome

You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.

Select a task:

- Retrieve the CA certificate or certificate revocation list
- Request a certificate
- Check on a pending certificate

[Next >](#)

Retrieve The CA Certificate Or Certificate Revocation List

[Install this CA certification path](#) to allow your computer to trust certificates issued from this certification authority.

It is not necessary to manually install the CA certification path if you request and install a certificate from this certification authority, because the CA certification path will be installed for you automatically.

Choose file to download:

CA Certificate:

DER encoded or Base 64 encoded

[Download CA certificate](#)

[Download CA certification path](#)

[Download latest certificate revocation list](#)

8. Klik op CA-certificaat downloaden.

Retrieve The CA Certificate Or Certificate Revocation List

[Install this CA certification path](#) to allow your computer to trust certificates issued from this certification authority.

It is not necessary to manually install the CA certification path if you request and install a certificate from this certification authority, because the CA certification path will be installed for you automatically.

Choose file to download:

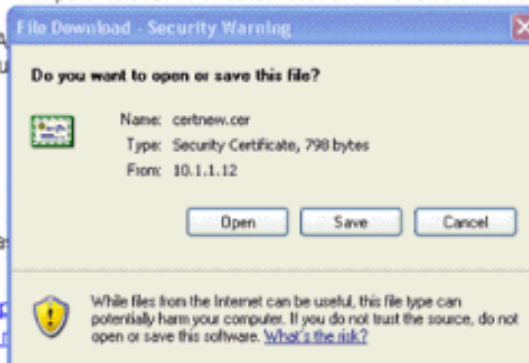
CA Certificate:

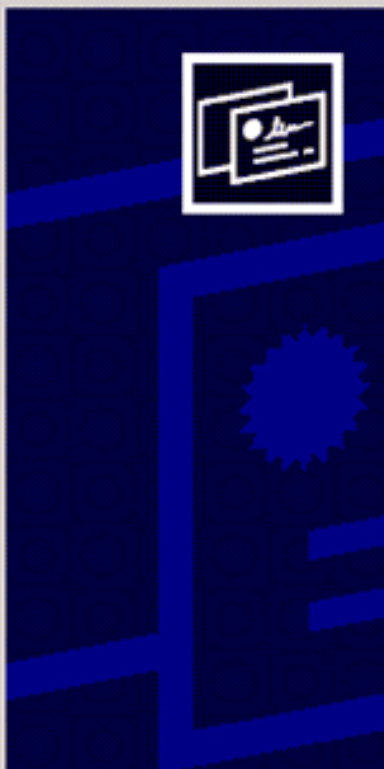
DER encoded or Base 64 encoded

[Download CA certificate](#)

[Download CA certification path](#)

[Download latest certificate revocation list](#)





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 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...

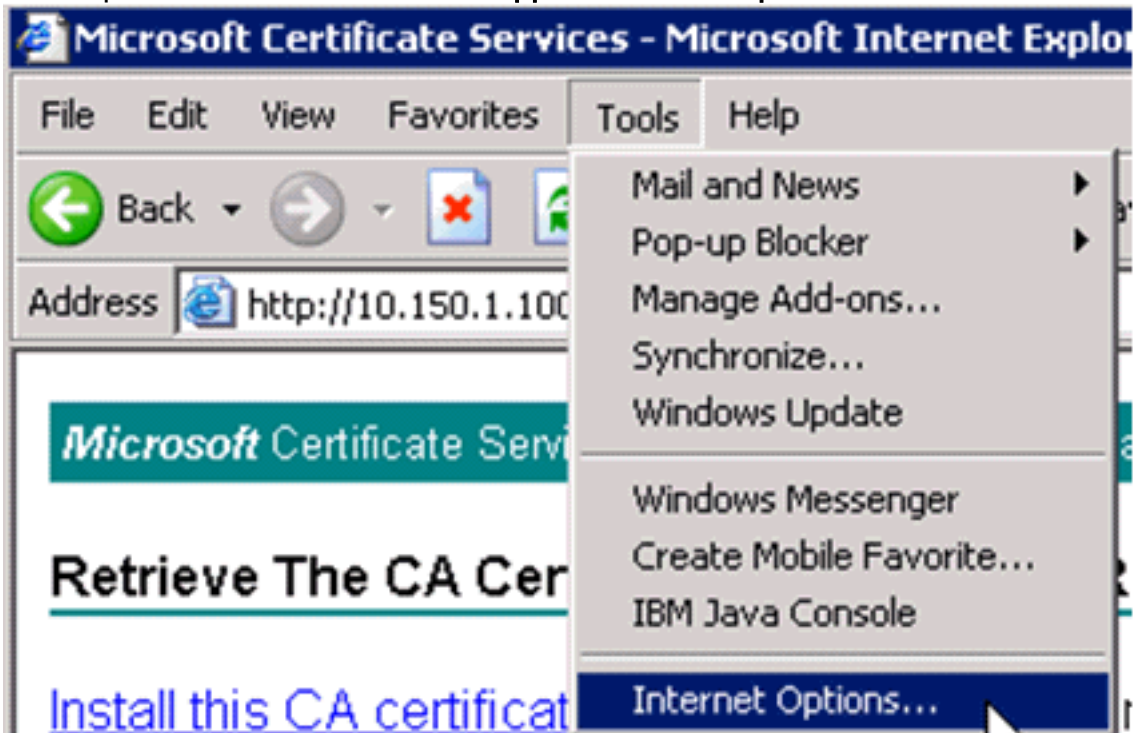
< Back

Next >

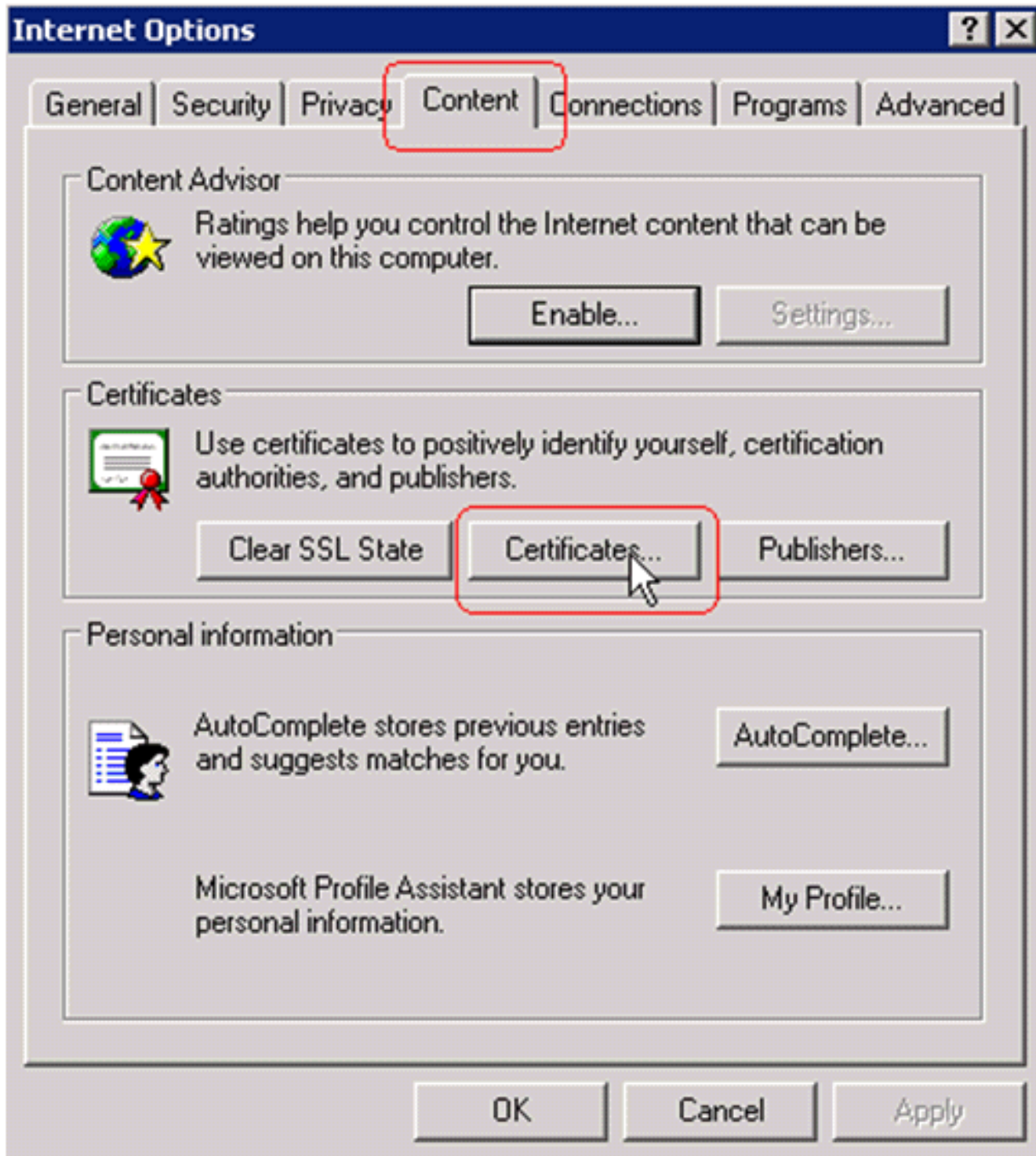
Cancel



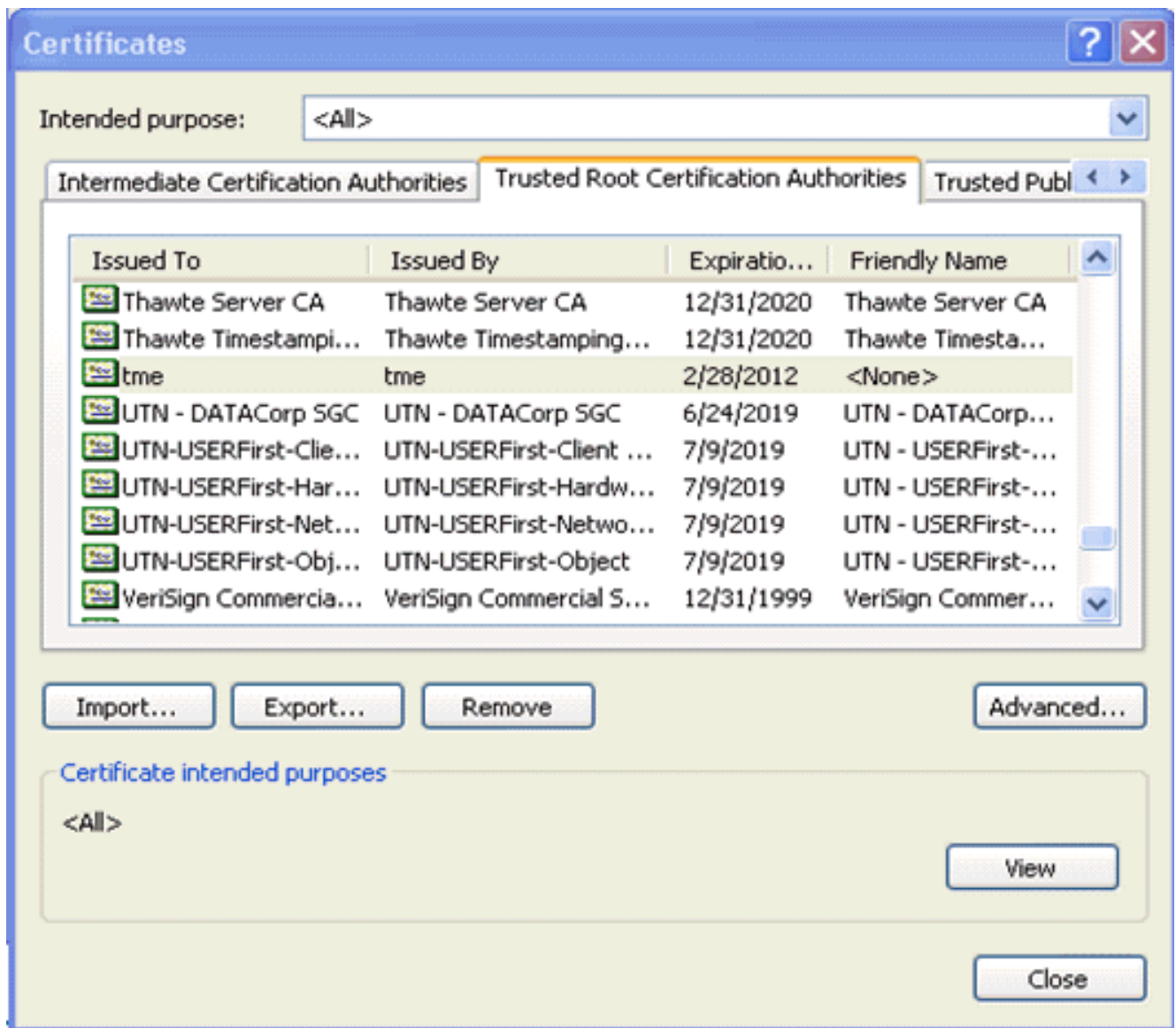
9. Om te controleren of het certificaat van de certificeringsinstantie correct is geïnstalleerd, opent u Internet Explorer en kiest u **Gereedschappen > Internet-opties > Content >**



Certificaten.



Bij Trusted Root-certificeringsinstantie dient u uw nieuwe geïnstalleerde certificeringsinstantie te raadplegen:



Een clientcertificaat genereren voor een clientapparaat

De client moet een certificaat van een server van de certificeringsinstantie verkrijgen voor de WLC om een WLAN EAP-TLS-client te authenticeren. Er zijn meerdere methoden die u kunt gebruiken om een client-certificaat te verkrijgen en het in de Windows XP-machine te installeren. Om een geldig certificaat te kunnen verkrijgen, moet de Windows XP-gebruiker zijn aangemeld bij het gebruik van zijn gebruikersidentificatie en moet hij een netwerkverbinding hebben (een bekabelde verbinding of een WLAN-verbinding met een 802.1x-beveiliging uitgeschakeld).

Een webbrowser op de Windows XP client en een bekabelde verbinding met het netwerk worden gebruikt om een client certificaat te verkrijgen van de server van de Private root Certified Authority. Deze procedure wordt gebruikt om het client-certificaat te verkrijgen van een server van de Microsoft certificeringsinstantie:

1. Gebruik een webbrowser op de client en plaats de browser naar de server van de certificeringsinstantie. Voer hiervoor **http://IP-address-of-Root-CA/certsrv** in.
2. Meld u aan bij gebruik van **Domain_Name\user_name**. U moet inloggen met behulp van de gebruikersnaam van het individu dat de XP-client gebruikt. (De gebruikersnaam wordt in het client-certificaat opgenomen.)
3. Kies in het venster Welcome een **certificaat aanvragen** en klik op **Volgende**.
4. Kies **Geavanceerde aanvraag** en klik op **Volgende**.

5. Kies een certificaataanvraag bij deze CA indienen met behulp van een formulier en klik op **Volgende**.
6. Kies in het formulier Geavanceerd certificaataanvraag de sjabloon als **gebruiker**, specificeer de grootte van het certificaat als **1024** en klik op **Indienen**.
7. Klik in het venster certificaatgifte op **Installeer dit certificaat**. Dit resulteert in de succesvolle installatie van een client certificaat op de Windows XP-client.

Microsoft Certificate Services -- tme [Home](#)

Welcome

You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.

Select a task:

- Retrieve the CA certificate or certificate revocation list
- Request a certificate
- Check on a pending certificate

[Next >](#)

Microsoft Certificate Services -- tme [Home](#)

Choose Request Type

Please select the type of request you would like to make:

- User certificate request

User Certificate
- Advanced request

[Next >](#)

Microsoft Certificate Services -- tme [Home](#)

Advanced Certificate Requests

You can request a certificate for yourself, another user, or a computer using one of the following methods. Note that the policy of the certification authority (CA) will determine the certificates that you can obtain.

- Submit a certificate request to this CA using a form.
- Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file.
- Request a certificate for a smart card on behalf of another user using the Smart Card Enrollment Station.
You must have an enrollment agent certificate to submit a request for another user.

[Next >](#)

8. Selecteer **Clientverificatiecertificaat**.

Advanced Certificate Request

Certificate Template:

User

Key Options:

CSP: Microsoft Base Cryptographic Provider v1.0

Key Usage: Exchange Signature Both

Key Size: 512 Min: 384 (common key sizes: 512 1024) Max: 1024

- Create new key set
 - Set the container name
- Use existing key set
- Enable strong private key protection
- Mark keys as exportable
 - Export keys to file
- Use local machine store
You must be an administrator to generate a key in the local machine store.

Additional Options:

Hash Algorithm: SHA-1
Only used to sign request.

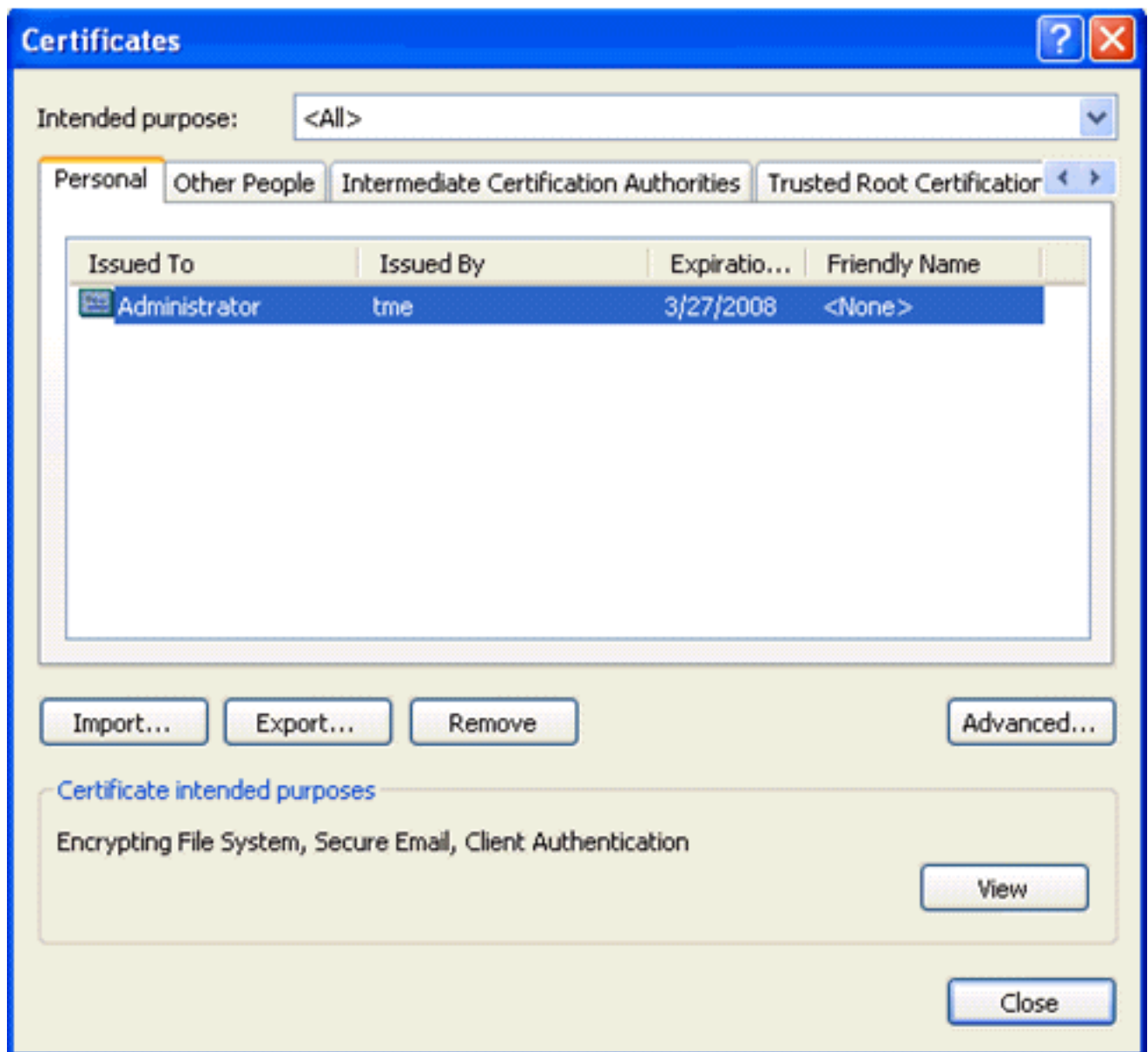
Save request to a PKCS #10 file

Attributes:

Het client-

certificaat is nu gemaakt.

9. Om te controleren of het certificaat is geïnstalleerd, gaat u naar Internet Explorer en kiest u **Gereedschappen > Internet-opties > Content > Certificaten**. In het tabblad Persoonlijk kunt u het certificaat bekijken.

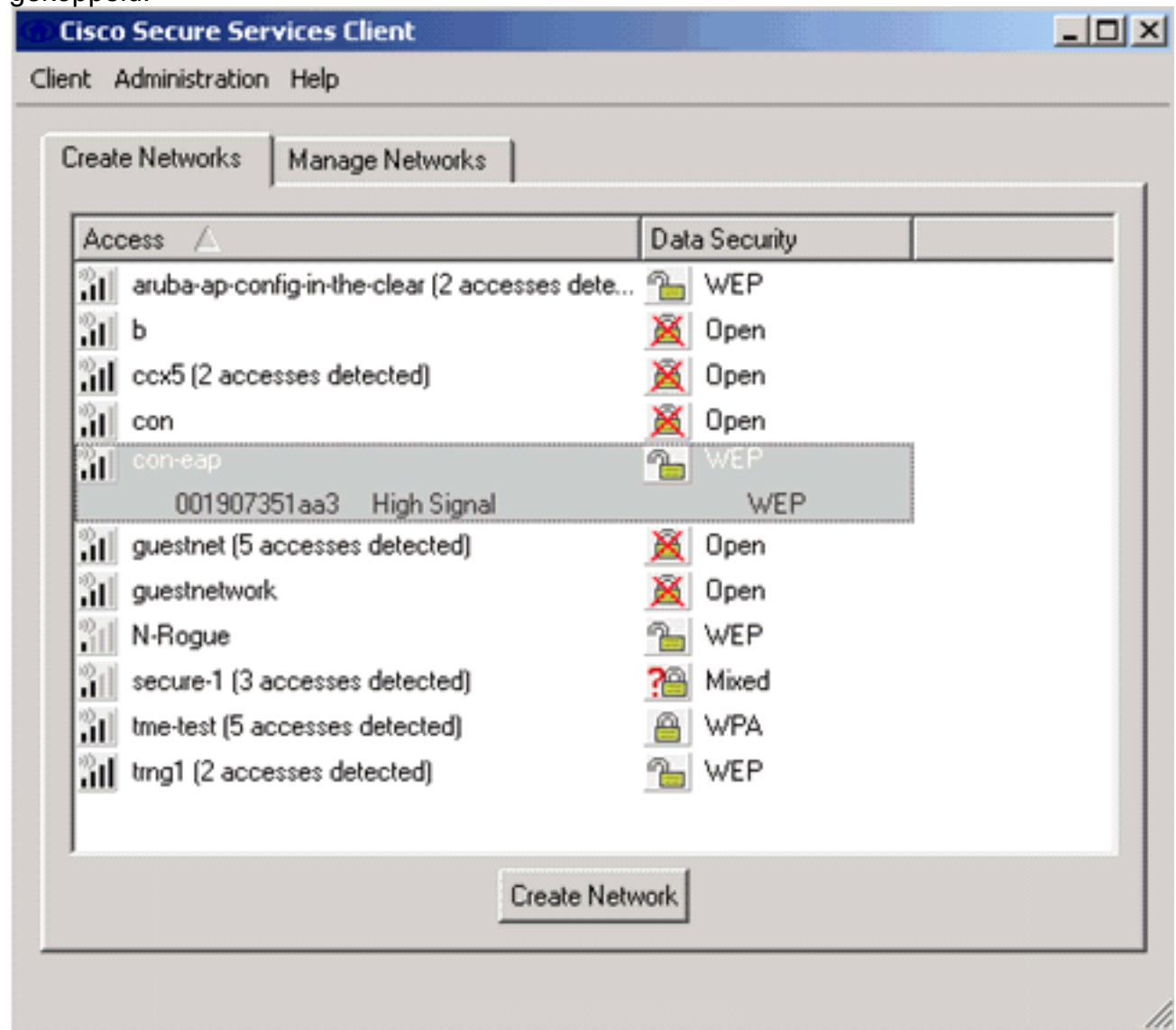


EAP-TLS met Cisco Secure Services-client op het clientapparaat

Voer de volgende stappen uit:

1. De WLC zendt standaard de SSID uit, dus wordt deze weergegeven in de lijst Network maken van gescande SSID's. U kunt een netwerkprofiel maken door op SSID in de lijst (Enterprise) te klikken en op **Netwerk maken** te klikken. Als de WLAN-infrastructuur is geconfigureerd met SSID dat wordt uitgeschakeld, moet u handmatig de SSID toevoegen. Om dit te doen, klik op **Add** onder Access Devices en voer handmatig de juiste SSID's (bijvoorbeeld Enterprise) in. Configureer actief probe gedrag voor de client. Dat is, waar de klant actief voor zijn gevormd SSID probeert. Specificeer **actief zoekactie naar dit toegangsapparaat** nadat u SSID in het venster Toevoegen toegangsapparaat hebt ingevoerd. **Opmerking:** de poortinstellingen staan geen bedrijfsmodi toe (802.1X) indien de MAP-echtheidsinstellingen niet voor het profiel zijn ingesteld.
2. Klik op **Netwerk maken** om het venster Network Profile te starten, dat u toestaat om de gekozen (of geconfigureerde) SSID te associëren met een verificatiemechanisme. Geef een beschrijvende naam voor het profiel toe. **Opmerking:** Meerdere WLAN-beveiligingstypen en/of SSID's kunnen bij dit verificatieprofiel worden

gekoppeld.



3. Schakel de authenticatie in en controleer de EAP-TLS-methode. Klik vervolgens op **Configureren** om de EAP-TLS-eigenschappen te configureren.
4. Klik onder Samenvatting van de Netwerkconfiguratie op **Wijzigen** om de instellingen EAP / geloofsbrieven te configureren.
5. Specificeer **Inschakelen-verificatie**, kies **EAP-TLS** onder Protocol en kies **Gebruikersnaam** als Identity.
6. Specificeer **Gebruik Single Sign on Credentials** om logaanmeldingsgegevens voor netwerkverificatie te gebruiken. Klik op **Configureren** om de EAP-TLS-parameters in te stellen.

Network Authentication...



Network: con-eap Network

Authentication Methods:

- Turn Off
- Turn On
 - Use Username as Identity
 - Use 'Anonymous' as Identity

Protocol
<input type="checkbox"/> EAP-MD5
<input type="checkbox"/> EAP-MSCHAPv2
<input checked="" type="checkbox"/> EAP-TLS
<input type="checkbox"/> FAST
<input type="checkbox"/> GTC

Configure...

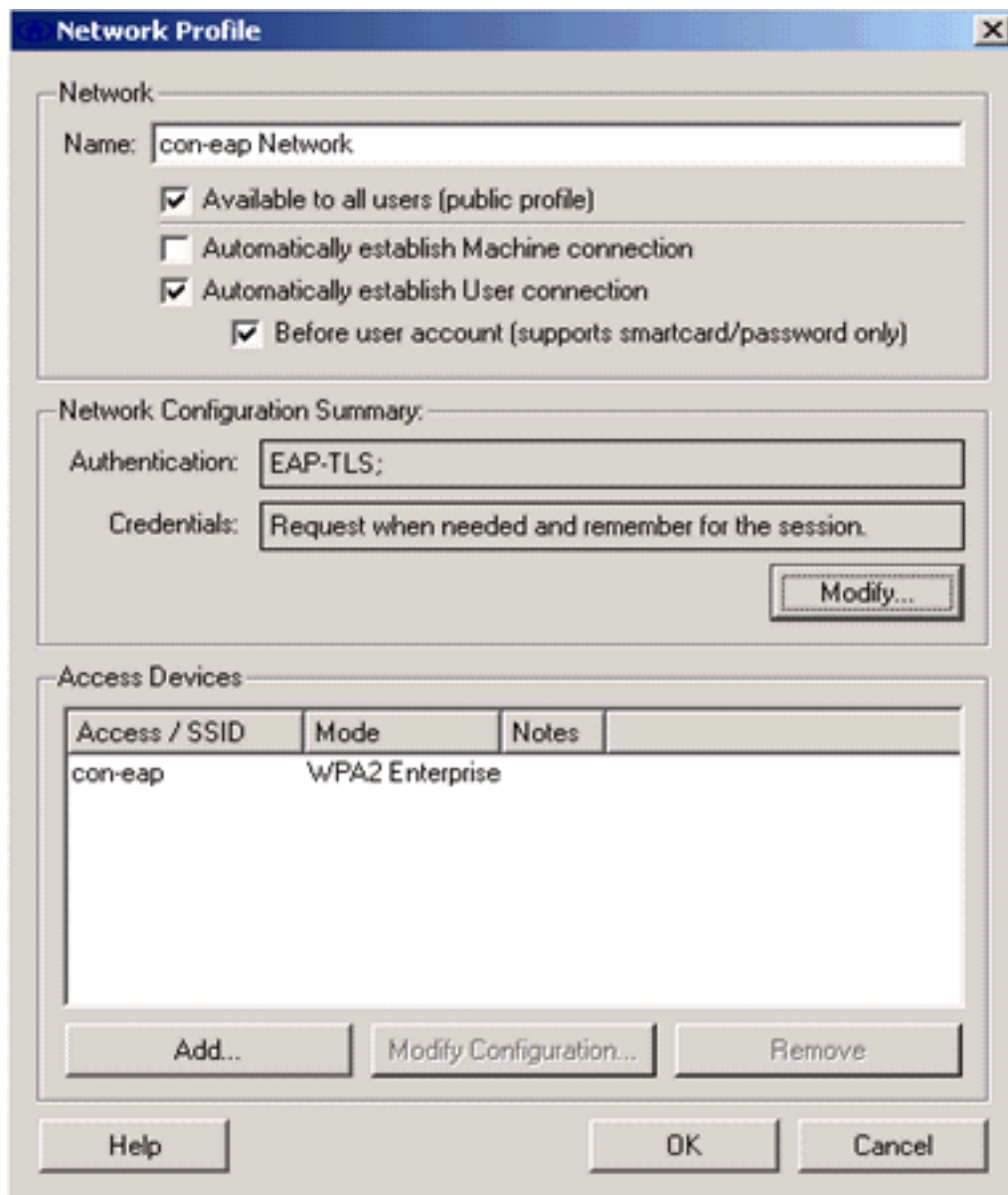
User Credentials:

- Use Machine Credentials
- Use Single Sign on Credentials
- Request when needed
 - Remember forever
 - Remember for this session
 - Remember for 5 minutes

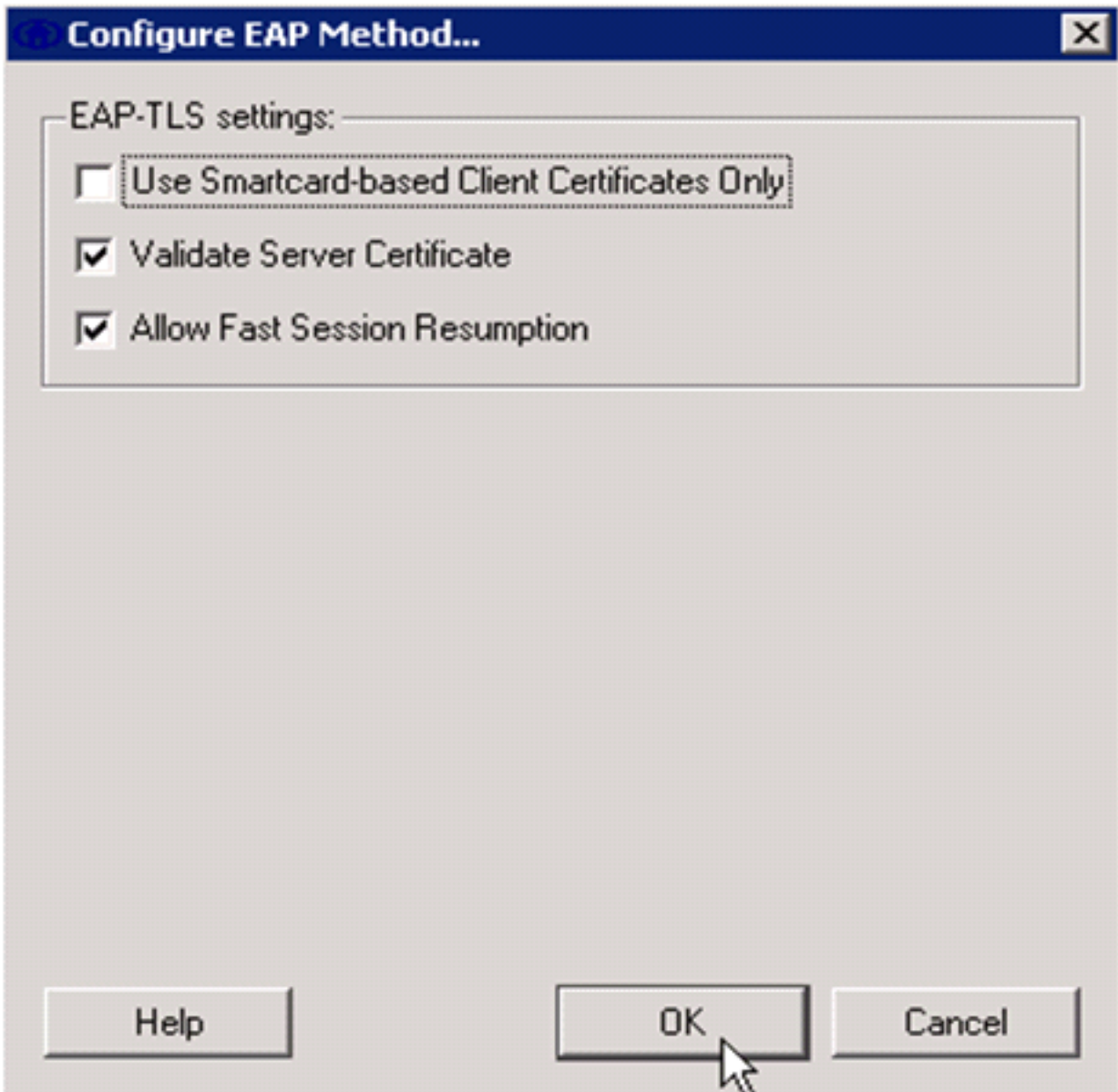
Help

OK

Cancel

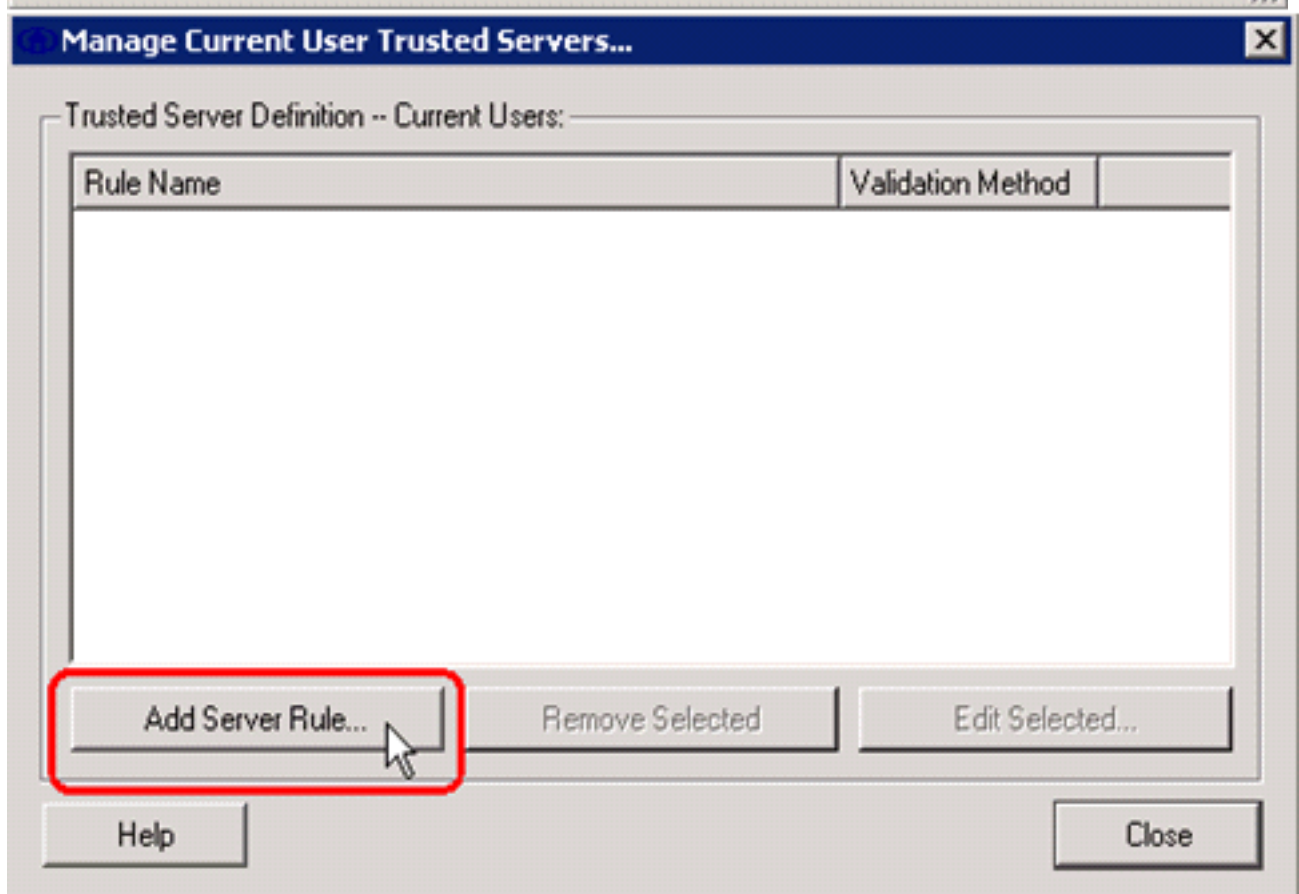
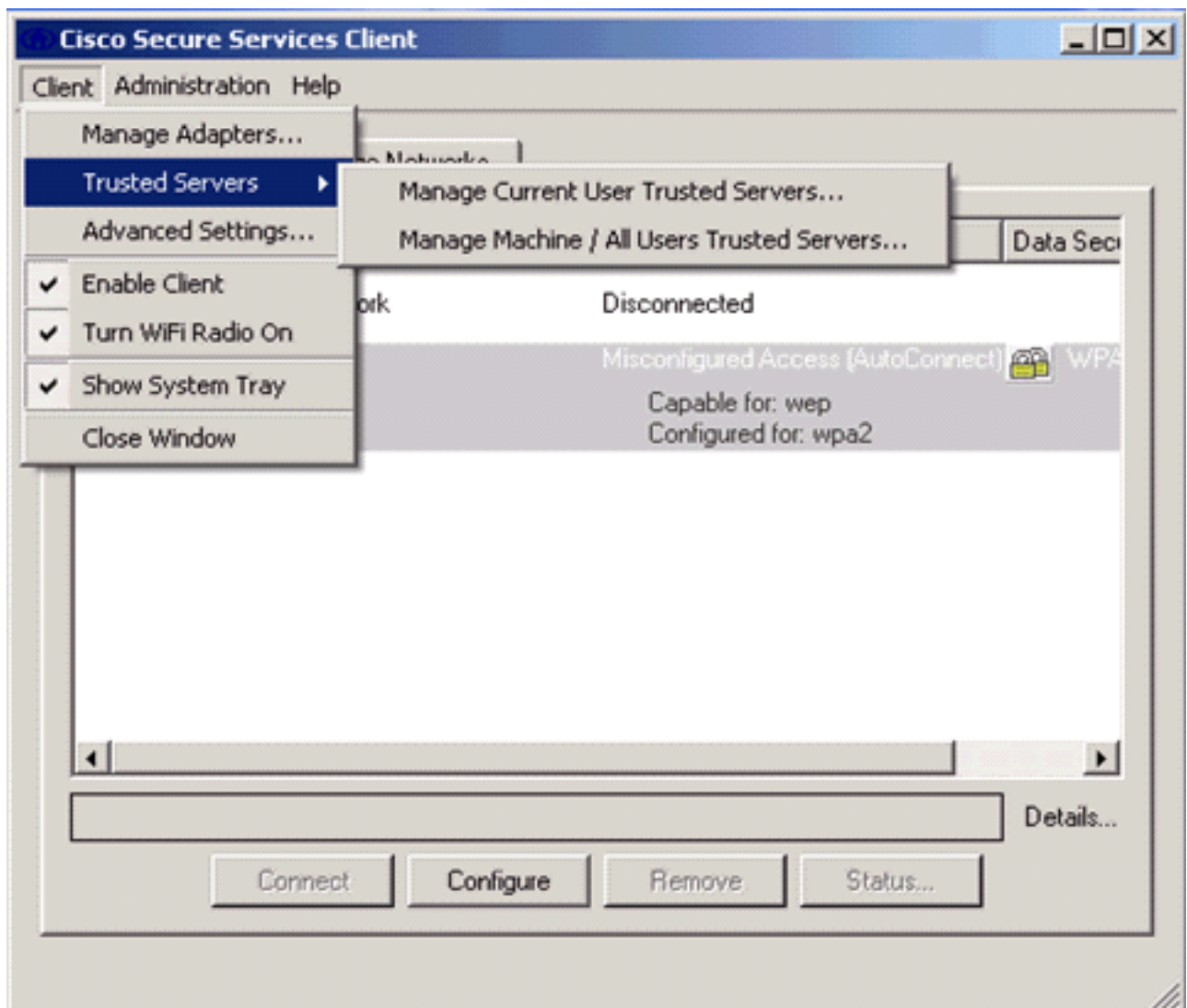


7. Om een beveiligde EAP-TLS-configuratie te hebben, moet u het RADIUS-servercertificaat controleren. Controleer hiervoor **het servercertificaat**



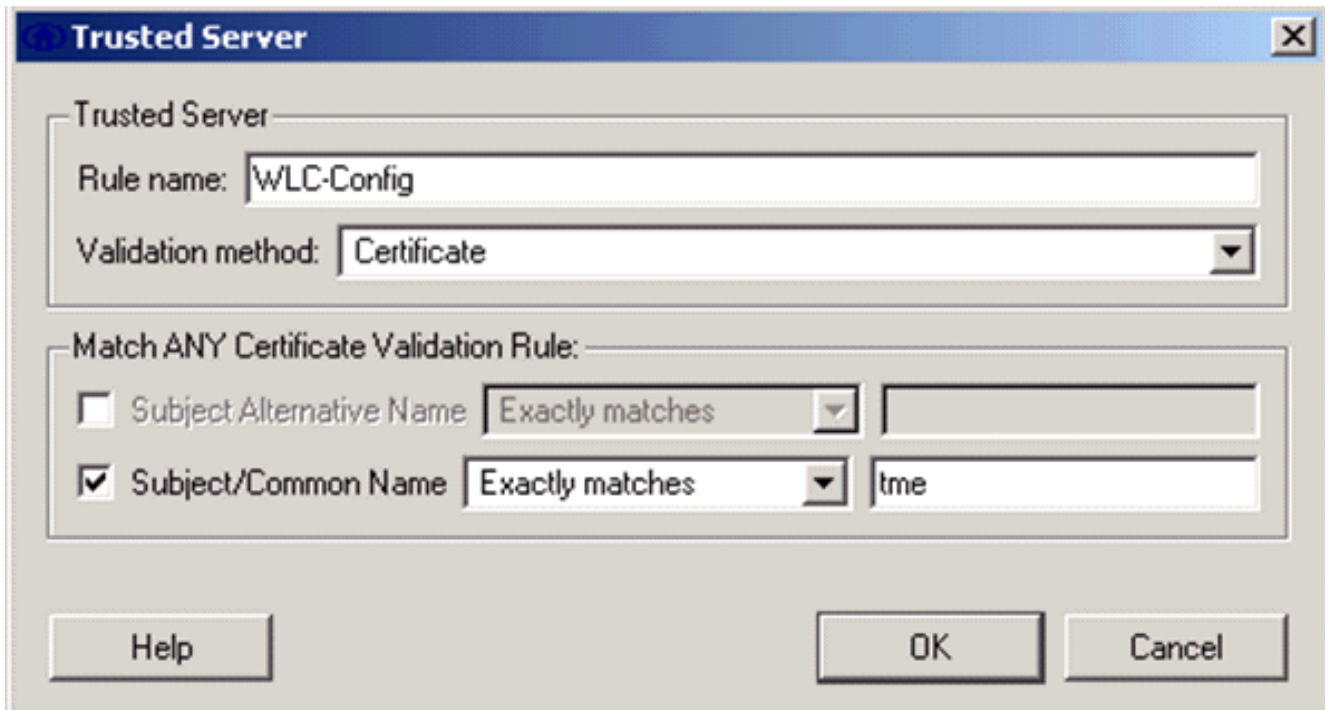
op.

8. Om het RADIUS-servercertificaat te valideren, moet u Cisco Secure Services Client-informatie geven om alleen het juiste certificaat te aanvaarden. Kies **client > Vertrouwde servers > Huidige op gebruikers vertrouwde servers** beheren.



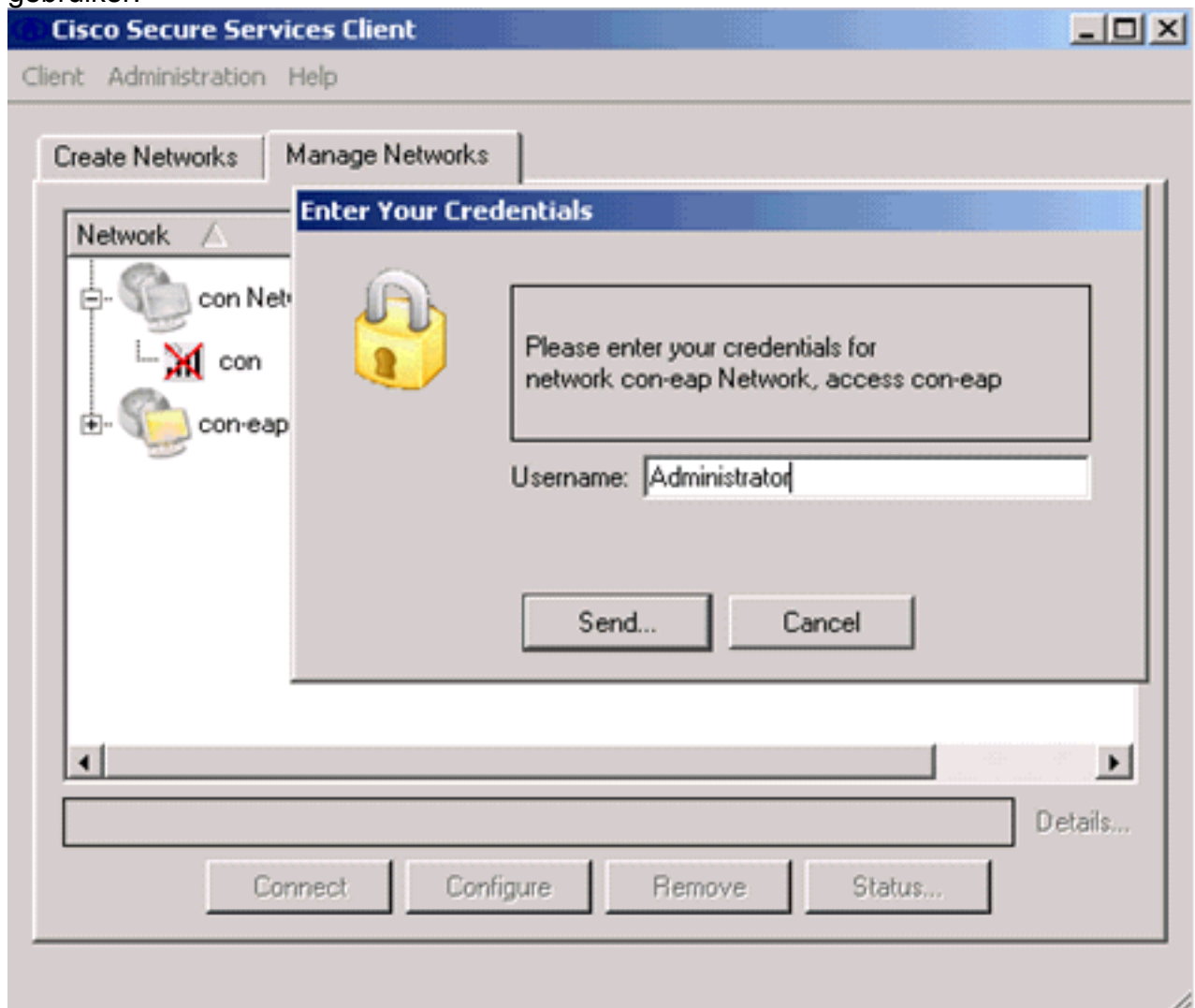
9. Geef een naam voor de regel en controleer de naam van het

servercertificaat.



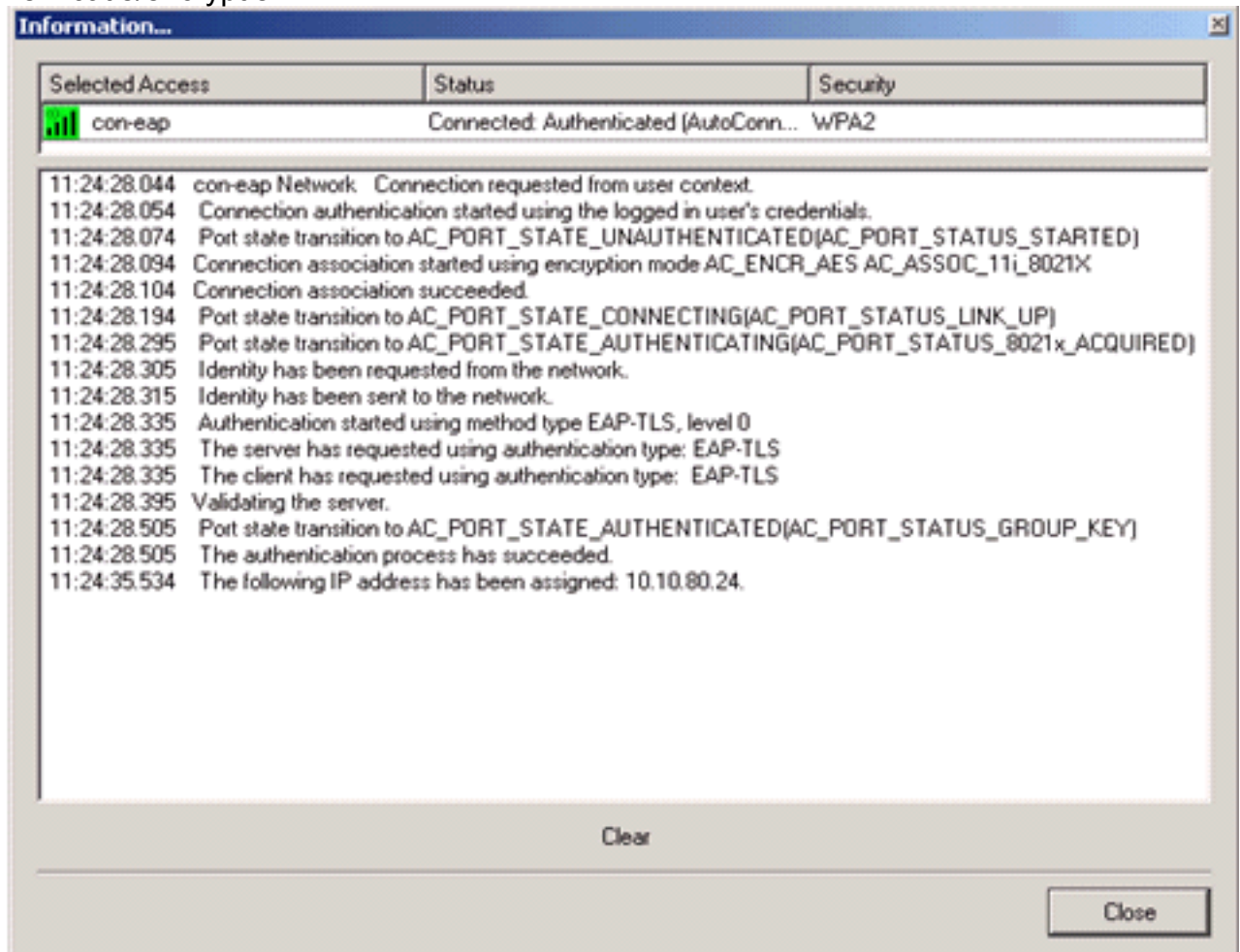
De configuratie van het MAP-TLS is voltooid.

10. Sluit aan op het draadloze netwerkprofiel. De Cisco Secure Services Client vraagt om inloggen van de gebruiker:









e Cisco Secure Services Client ontvangt het servercertificaat en controleert dit (met de regel ingesteld en de certificeringsinstantie geïnstalleerd). Vervolgens wordt gevraagd het certificaat te gebruiken voor de gebruiker.

11. Nadat de client voor authenticatie is geselecteerd, kiest u **SSID** onder het profiel in het tabblad Oplossingen beheren en klikt u op **Status** om verbindingdetails te vragen. Het venster Connection Details geeft informatie over het clientapparaat, de verbindingstatus en de statistieken en de verificatiemethode. Het tabblad WiFi biedt details over de 802.11-verbindingstatus, waaronder RSSI, 802.11-kanaal en verificatie/encryptie.



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)	

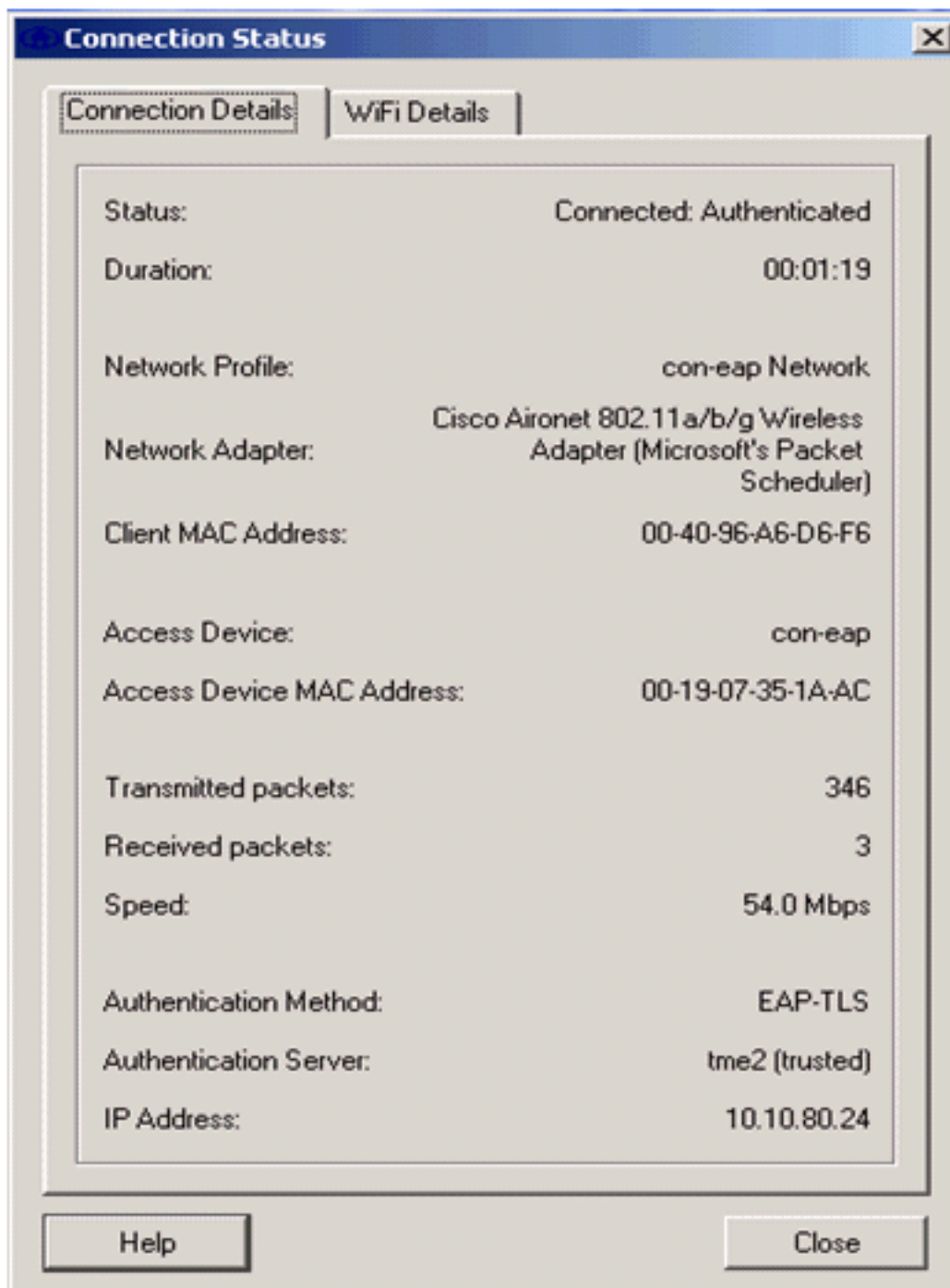
 Details...

Disconnect

Configure

Remove

Status...



Opdrachten debug

Het [Uitvoer Tolk](#) ([uitsluitend geregistreeerde](#) klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

Opmerking: Raadpleeg [Belangrijke informatie over debug Commands](#) voordat u **debug**-opdrachten gebruikt.

Deze debug opdrachten kunnen bij de WLC worden gebruikt om de voortgang van de authenticatie-uitwisseling te bewaken:

- debug aaaaaathedingen activeren
- u kunt gegevens debug a
- debug dot1x gebeurtenissen in staat stellen

- debug dot1x-staten
- debug a local-auth-gebeurtenissen activerenOF
- debug a allen activeren

Gerelateerde informatie

- [Configuratie-gids voor Cisco draadloze LAN-controllers, release 4.1](#)
- [WLAN-technologieondersteuning](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)