Unified Wireless Network Local EAP-Server - Konfigurationsbeispiel

Inhalt

Einleitung

Dieses Dokument beschreibt die Konfiguration eines lokalen EAP-Servers (Extensible Authentication Protocol) in einem Cisco Wireless LAN Controller (WLC) für die Authentifizierung von Wireless-Benutzern.

Lokaler EAP ist eine Authentifizierungsmethode, mit der Benutzer und Wireless-Clients lokal authentifiziert werden können. Sie ist für die Verwendung in Außenstellen ausgelegt, die die Verbindung zu Wireless-Clients aufrechterhalten möchten, wenn das Back-End-System ausfällt oder der externe Authentifizierungsserver ausfällt. Wenn Sie lokalen EAP aktivieren, fungiert der Controller als Authentifizierungsserver und als lokale Benutzerdatenbank. Dadurch entfällt die Abhängigkeit von einem externen Authentifizierungsserver. Der lokale EAP ruft Benutzeranmeldeinformationen aus der lokalen Benutzerdatenbank oder der Backend-Datenbank des Lightweight Directory Access Protocol (LDAP) ab, um Benutzer zu authentifizieren. Lokaler EAP unterstützt Lightweight EAP (LEAP), EAP-Flexible Authentication via Secure Tunneling (EAP-FAST) und EAP-Transport Layer Security (EAP-TLS)-Authentifizierung zwischen Controller und Wireless Clients.

Beachten Sie, dass der lokale EAP-Server nicht verfügbar ist, wenn der WLC eine globale externe RADIUS-Serverkonfiguration enthält. Alle Authentifizierungsanforderungen werden an den globalen externen RADIUS weitergeleitet, bis der lokale EAP-Server verfügbar ist. Wenn der WLC die Verbindung zum externen RADIUS-Server verliert, wird der lokale EAP-Server aktiviert. Wenn keine globale RADIUS-Serverkonfiguration vorliegt, wird der lokale EAP-Server sofort aktiviert. Der lokale EAP-Server kann nicht zur Authentifizierung von Clients verwendet werden, die mit anderen WLCs verbunden sind. Anders ausgedrückt: Ein WLC kann seine EAP-Anforderung zur Authentifizierung nicht an einen anderen WLC weiterleiten. Jeder WLC muss über einen eigenen lokalen EAP-Server und eine eigene Datenbank verfügen.

Hinweis: Verwenden Sie diese Befehle, um zu verhindern, dass WLC Anfragen an einen externen Radius-Server sendet.

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

Der lokale EAP-Server unterstützt diese Protokolle ab Version 4.1.171.0:

- LEBEN
- EAP-FAST (Benutzername/Kennwort und Zertifikate)
- EAP-TLS

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Kenntnisse der Konfiguration von WLCs und Lightweight Access Points (LAPs) für den Basisbetrieb
- Kenntnis der LWAPP- (Lightweight Access Point Protocol) und Wireless-Sicherheitsmethoden
- Grundkenntnisse der lokalen EAP-Authentifizierung.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Windows XP mit CB21AG Adapterkarte und Cisco Secure Services Client Version 4.05
- Cisco Wireless LAN Controller 4.1.171.0 der Serie 4400
- Microsoft-Zertifizierungsstelle für Windows 2000-Server

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Konfigurieren des lokalen EAP auf dem Cisco Wireless LAN

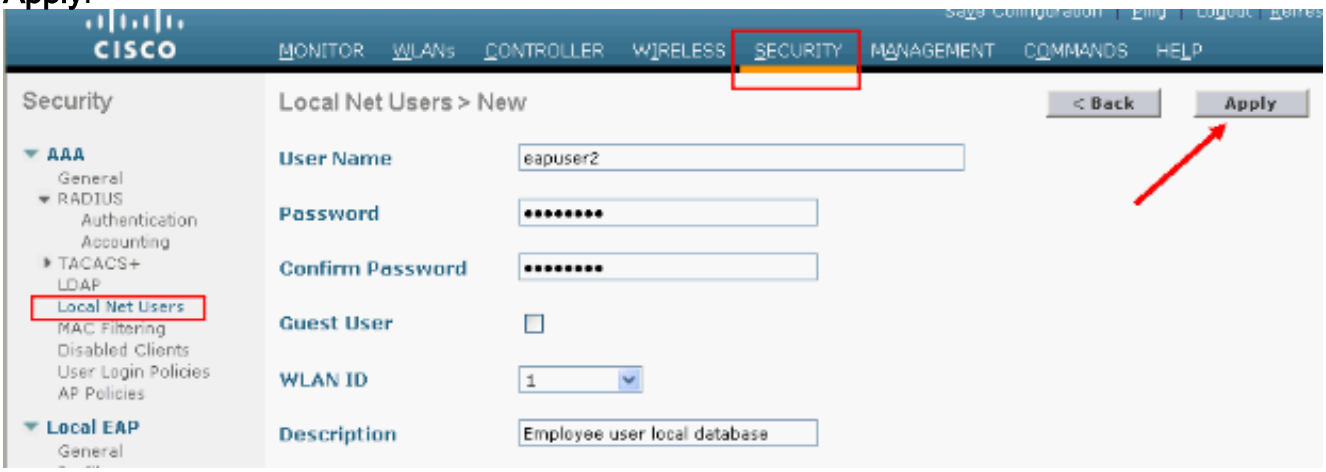
Controller

In diesem Dokument wird davon ausgegangen, dass die grundlegende Konfiguration des WLC bereits abgeschlossen ist.

Lokale EAP-Konfiguration

Gehen Sie wie folgt vor, um den lokalen EAP zu konfigurieren:

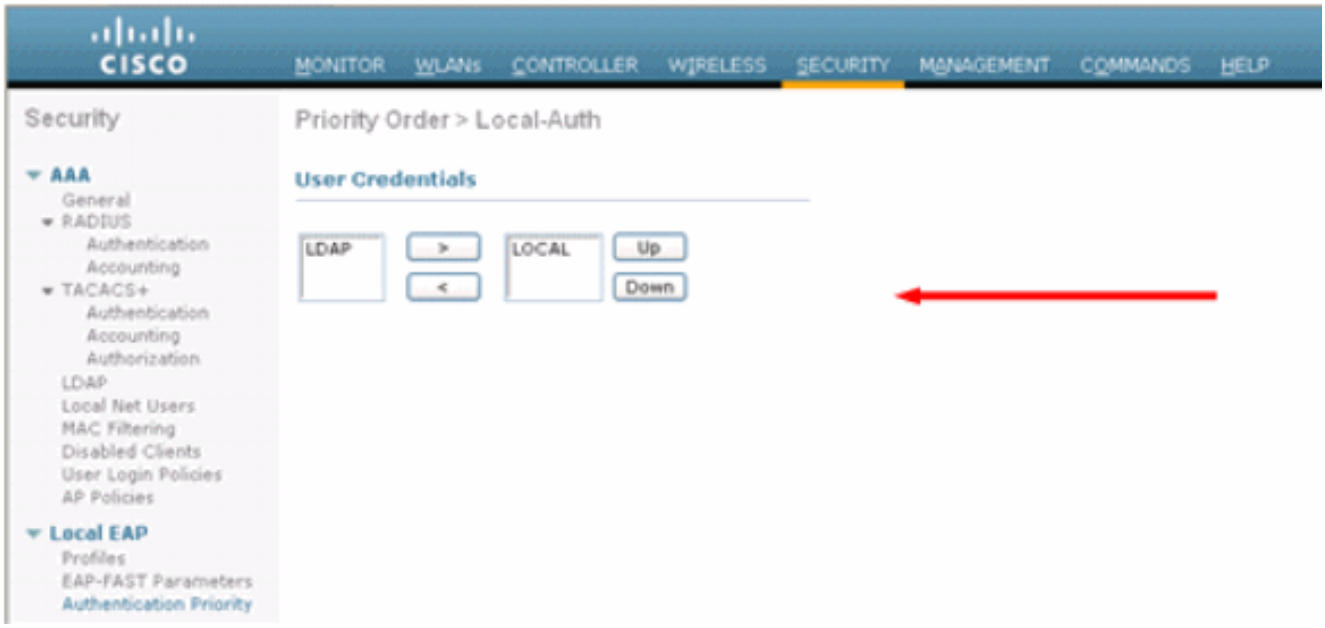
1. Hinzufügen eines lokalen Netzbenutzers:Über die GUI. wählen Sie **Security > Local Net Users > New aus**, geben Sie den Benutzernamen, das Kennwort, den Gastbenutzer, die WLAN-ID und die Beschreibung ein, und klicken Sie auf **Apply**.



Über die CLI können Sie den Befehl **config netuser add *<username> <password> <WLAN ID> <description>*** verwenden:**Hinweis:** Dieser Befehl wurde aus räumlichen Gründen auf eine zweite Zeile herabgesetzt.

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

2. Geben Sie die Bestellung zum Abrufen von Benutzeranmeldeinformationen an.Wählen Sie in der GUI **Security > Local EAP > Authentication Priority (Sicherheit > Lokaler EAP > Authentifizierungspriorität)**. Wählen Sie dann LDAP aus, klicken Sie auf die Schaltfläche **"<" und dann auf Übernehmen**. Dadurch werden die Benutzeranmeldeinformationen zuerst in die lokale Datenbank eingegeben.



Über die CLI:

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

3. EAP-Profil hinzufügen:Wählen Sie dazu in der GUI **Security > Local EAP > Profiles (Sicherheit > Lokaler EAP > Profile) aus,** und klicken Sie auf **New (Neu)**. Wenn das neue Fenster angezeigt wird, geben Sie den Profilnamen ein, und klicken Sie auf **Übernehmen**.

Sie können dies auch mit dem CLI-Befehl **config local-auth eap-profile add *<profile-name>* *tun.*** In unserem Beispiel lautet der Profilname *EAP-test*.

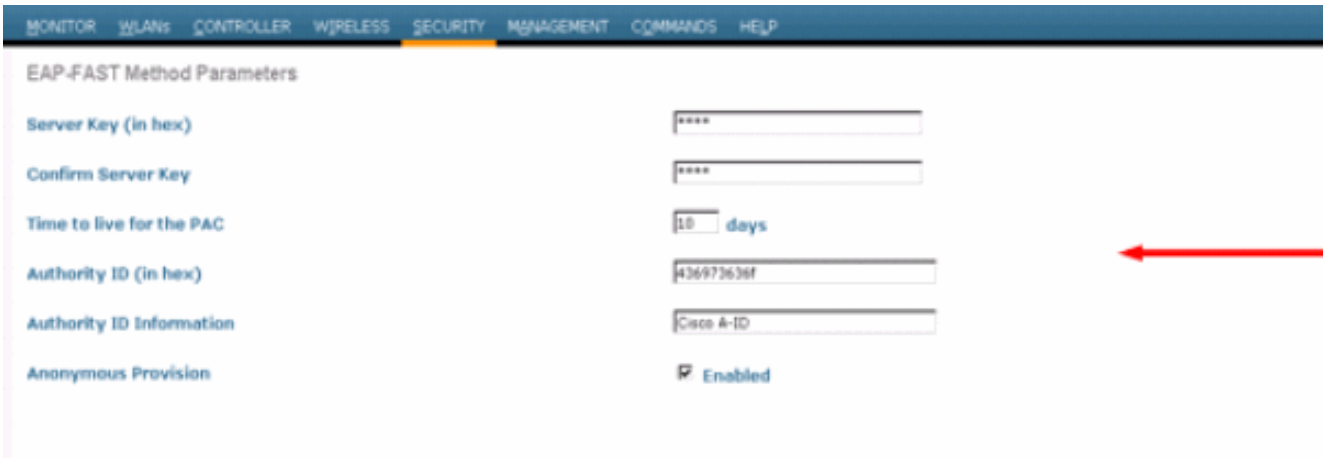
```
(Cisco Controller) >config local-auth eap-profile add EAP-test
```

4. Fügen Sie dem EAP-Profil eine Methode hinzu.Wählen Sie in der GUI **Security > Local EAP > Profiles** aus, und klicken Sie auf den Profilnamen, für den Sie die Authentifizierungsmethoden hinzufügen möchten. In diesem Beispiel werden LEAP, EAP-FAST und EAP-TLS verwendet. Klicken Sie auf **Apply**, um die Methoden festzulegen.

Sie können auch den CLI-Befehl **config local-auth eap-profile method add *<method-name>* *<profile-name>*** verwenden. In unserer Beispielkonfiguration fügen wir dem Profil-EAP-Test drei Methoden hinzu. Die Methoden sind LEAP, EAP-FAST und EAP-TLS, deren Methodennamen *Sprung, Fast* und *TLS* sind. Diese Ausgabe zeigt die CLI-Konfigurationsbefehle:

```
(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
```

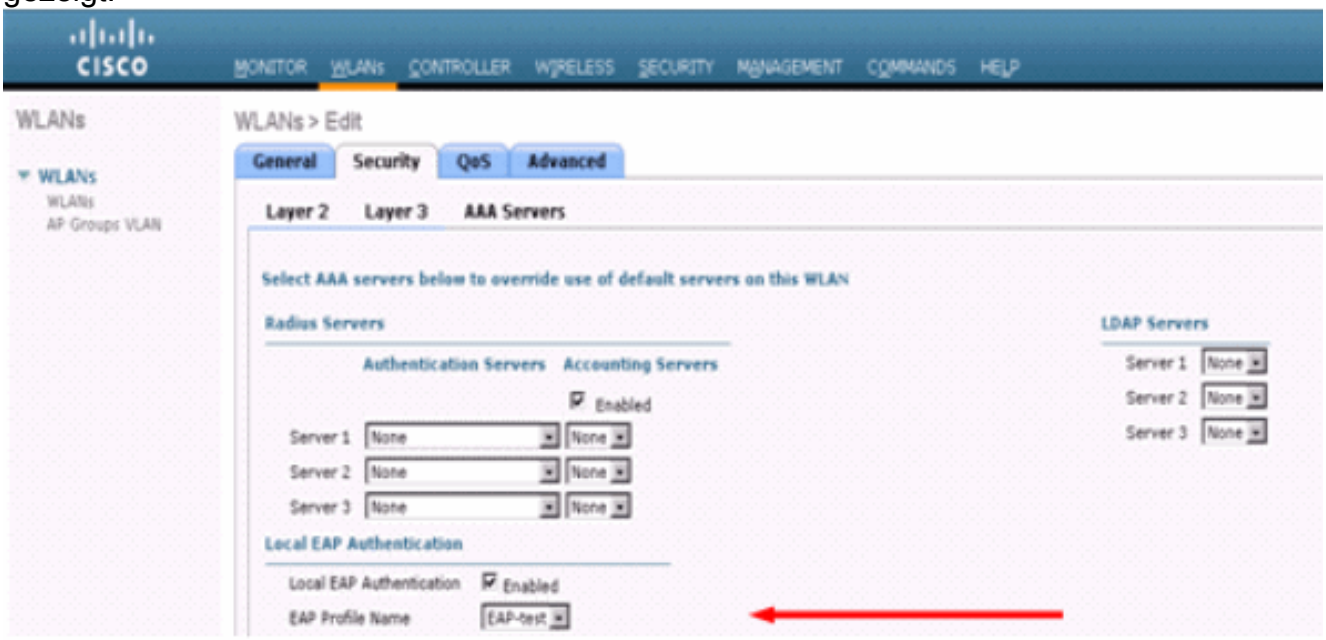
5. Konfigurieren Sie die Parameter der EAP-Methode. Dies wird nur für EAP-FAST verwendet. Die zu konfigurierenden Parameter sind:**Server Key (Server-Key)** - Serverschlüssel zum Verschlüsseln/Entschlüsseln von PACs (Protected Access Credentials) (hexadezimal).**Time to Live for PAC (pac-ttl)**: Legt die Zeit bis zum Live-Betrieb für die PAC fest.**Authority ID (Authority-ID) (Autoritäts-ID)** - Legt die Autoritätskennung fest.**Annonymous Provivision (anon-provn)**: Konfiguriert, ob anonyme Rückstellungen zulässig sind. Dies ist standardmäßig aktiviert.Wählen Sie für die Konfiguration über die GUI **Security > Local EAP > EAP-FAST Parameters (Sicherheit > Lokaler EAP > EAP-FAST-Parameter)**, und geben Sie den Serverschlüssel, Time to live für die PAC, Authority ID (in Hex) und Authority ID Information (Informationen zur Behörde-ID)
ein.



Dies sind die CLI-Konfigurationsbefehle zum Festlegen der folgenden Parameter für 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
```

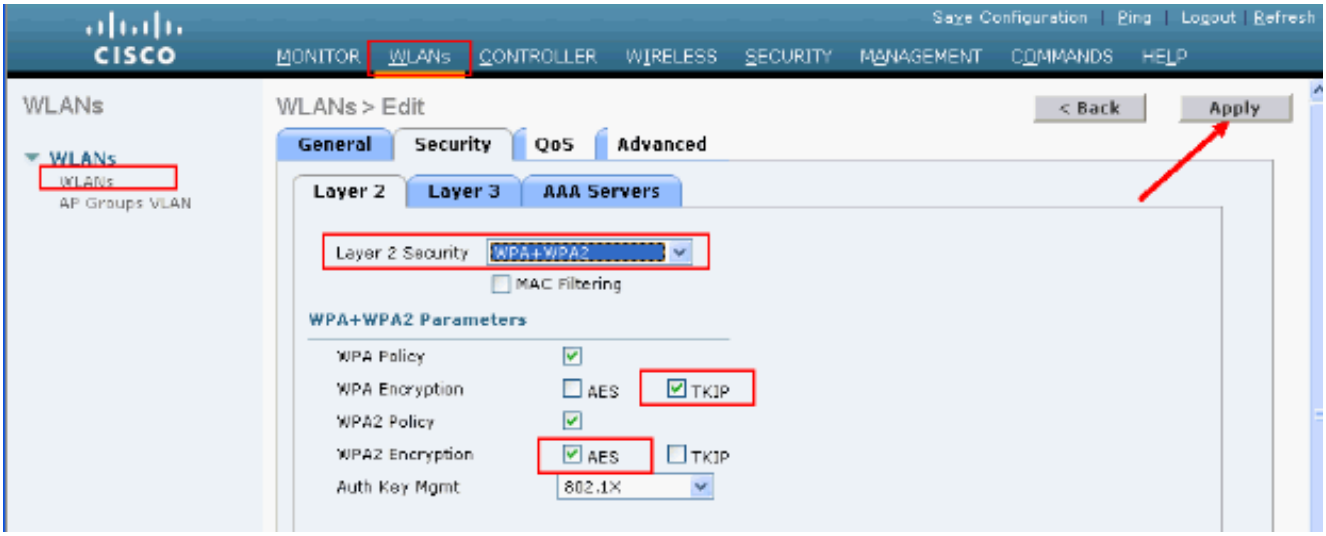
6. Lokale Authentifizierung pro WLAN aktivieren:Wählen Sie in der GUI im oberen Menü **WLANs** aus, und wählen Sie das WLAN aus, für das Sie die lokale Authentifizierung konfigurieren möchten. Ein neues Fenster wird angezeigt. Klicken Sie auf die Registerkarten **Security > AAA**. Überprüfen Sie die **lokale EAP-Authentifizierung**, und wählen Sie im Pulldown-Menü den richtigen EAP-Profilnamen aus, wie in diesem Beispiel gezeigt:



Sie können auch den Konfigurationsbefehl **CLI config wlan local-auth enable *<profile-name>* *<wlan-id>*** wie folgt ausgeben:

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

7. Legen Sie die Layer-2-Sicherheitsparameter fest.Gehen Sie in der GUI-Oberfläche im Fenster WLAN Edit (WLAN-Bearbeitung) zu den Registerkarten **Security > Layer 2** und wählen Sie **WPA+WPA2** aus dem Pulldown-Menü Layer 2 Security (Layer-2-Sicherheit). Legen Sie im Abschnitt WPA+WPA2-Parameter die WPA-Verschlüsselung auf **TKIP** und WPA2 Encryption **AES fest**. Klicken Sie anschließend auf **Übernehmen**.



Verwenden Sie in der CLI die folgenden Befehle:

```
(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. Überprüfen Sie die Konfiguration:

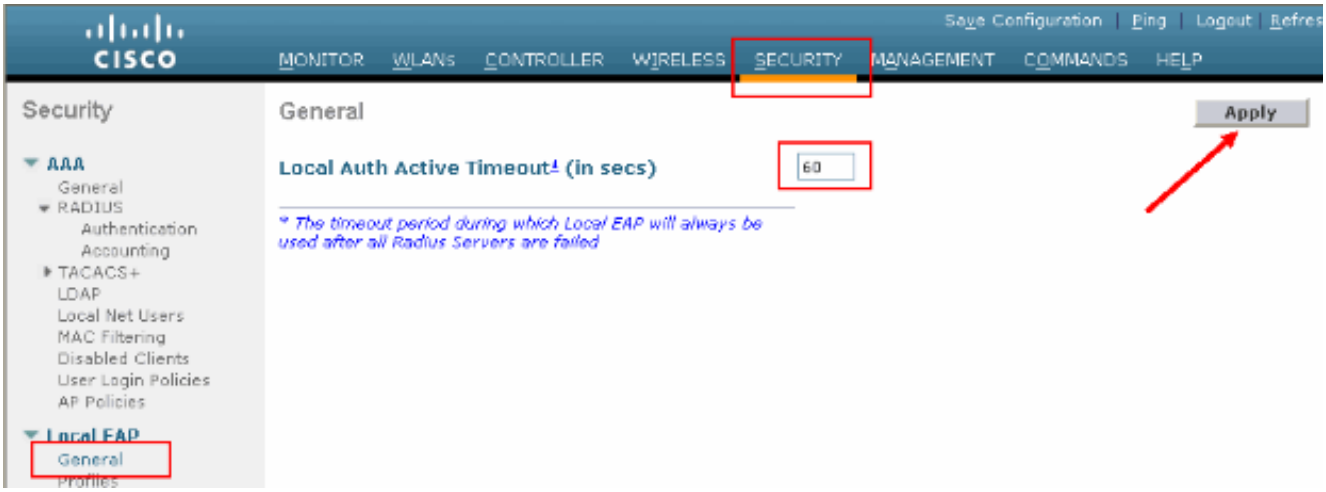
```
(Cisco Controller) >show local-auth config

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 .............................. 43697369f10000000000000000000
      Authority Information ..................... CiscoA-ID
```

Mithilfe des Befehls **show wlan *<wlan id> können*** Sie bestimmte Parameter von wlan 1 sehen:

```
(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
```

Es gibt weitere lokale Authentifizierungsparameter, die konfiguriert werden können, insbesondere den aktiven Timeout-Timer. Dieser Timer konfiguriert den Zeitraum, in dem lokales EAP verwendet wird, nachdem alle RADIUS-Server ausgefallen sind.Wählen Sie in der GUI **Security > Local EAP > General (Sicherheit > Lokaler EAP > Allgemein) aus,** und legen Sie den Zeitwert fest. Klicken Sie anschließend auf **Übernehmen**.



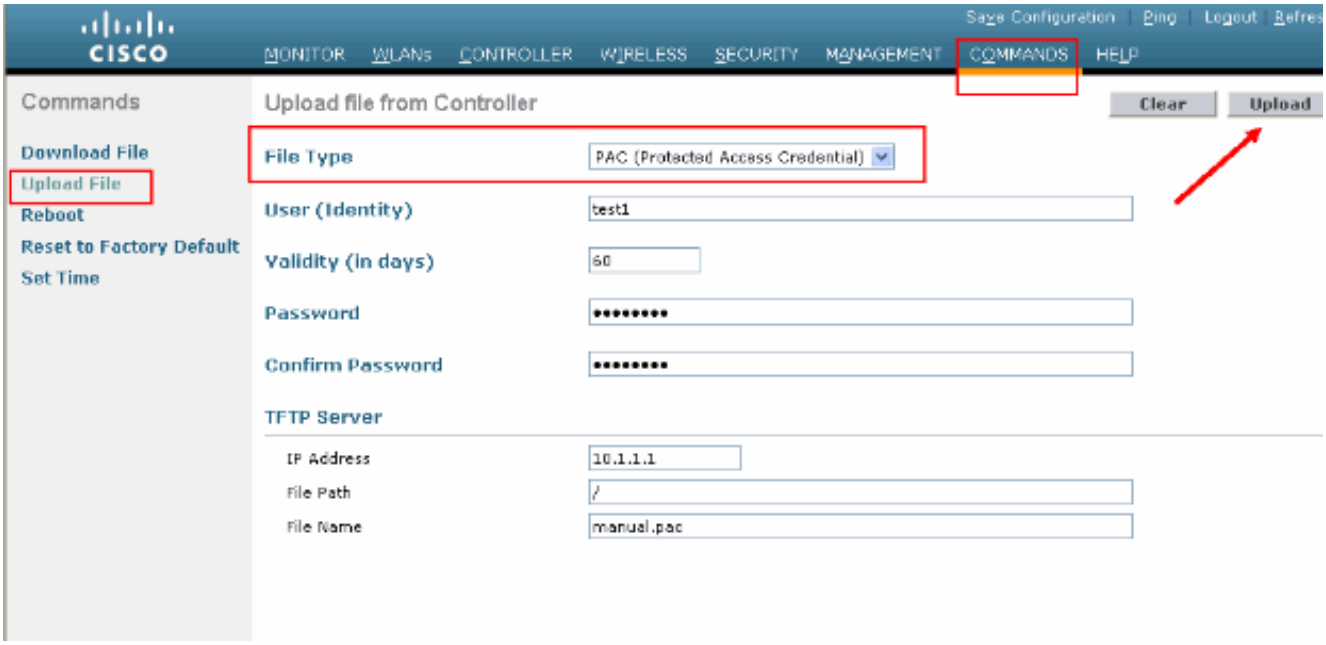
Führen Sie über die CLI die folgenden Befehle aus:

```
(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
```

Sie können den Wert, für den dieser Timer eingerichtet ist, überprüfen, wenn Sie den Befehl **show local-auth config** ausführen.

```
(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. Wenn Sie die manuelle PAC erstellen und laden müssen, können Sie entweder die GUI oder die CLI verwenden.Wählen Sie in der GUI **COMMANDS** im oberen Menü aus und wählen Sie **Upload File** aus der Liste rechts. Wählen Sie **PAC (Protected Access Credential)** aus dem Dropdown-Menü Dateityp aus. Geben Sie alle Parameter ein und klicken Sie auf **Hochladen**.



Geben Sie in der CLI die folgenden Befehle ein:

```
(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.
```

Microsoft-Zertifizierungsstelle

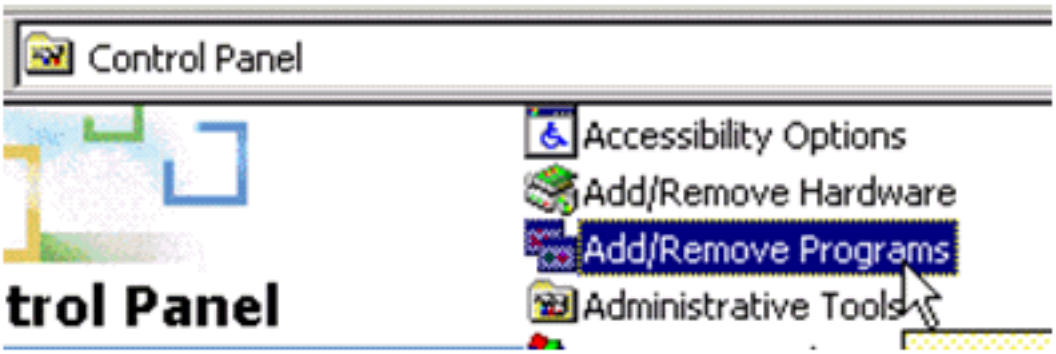
Um die EAP-FAST Version 2 und die EAP-TLS-Authentifizierung zu verwenden, müssen der WLC und alle Client-Geräte über ein gültiges Zertifikat verfügen und das öffentliche Zertifikat der Zertifizierungsstelle kennen.

Installation

Wenn auf dem Windows 2000-Server noch keine Zertifizierungsstellen installiert sind, müssen Sie diese installieren.

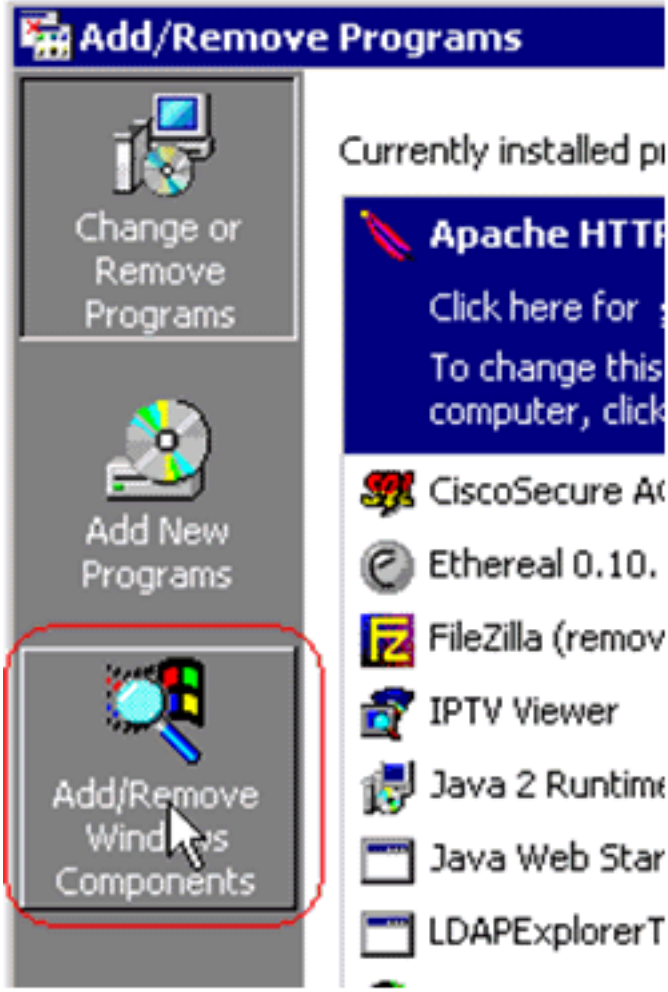
Gehen Sie wie folgt vor, um die Microsoft Certification Authority auf einem Windows 2000-Server zu aktivieren:

1. Wählen Sie in der Systemsteuerung **Software aus**.



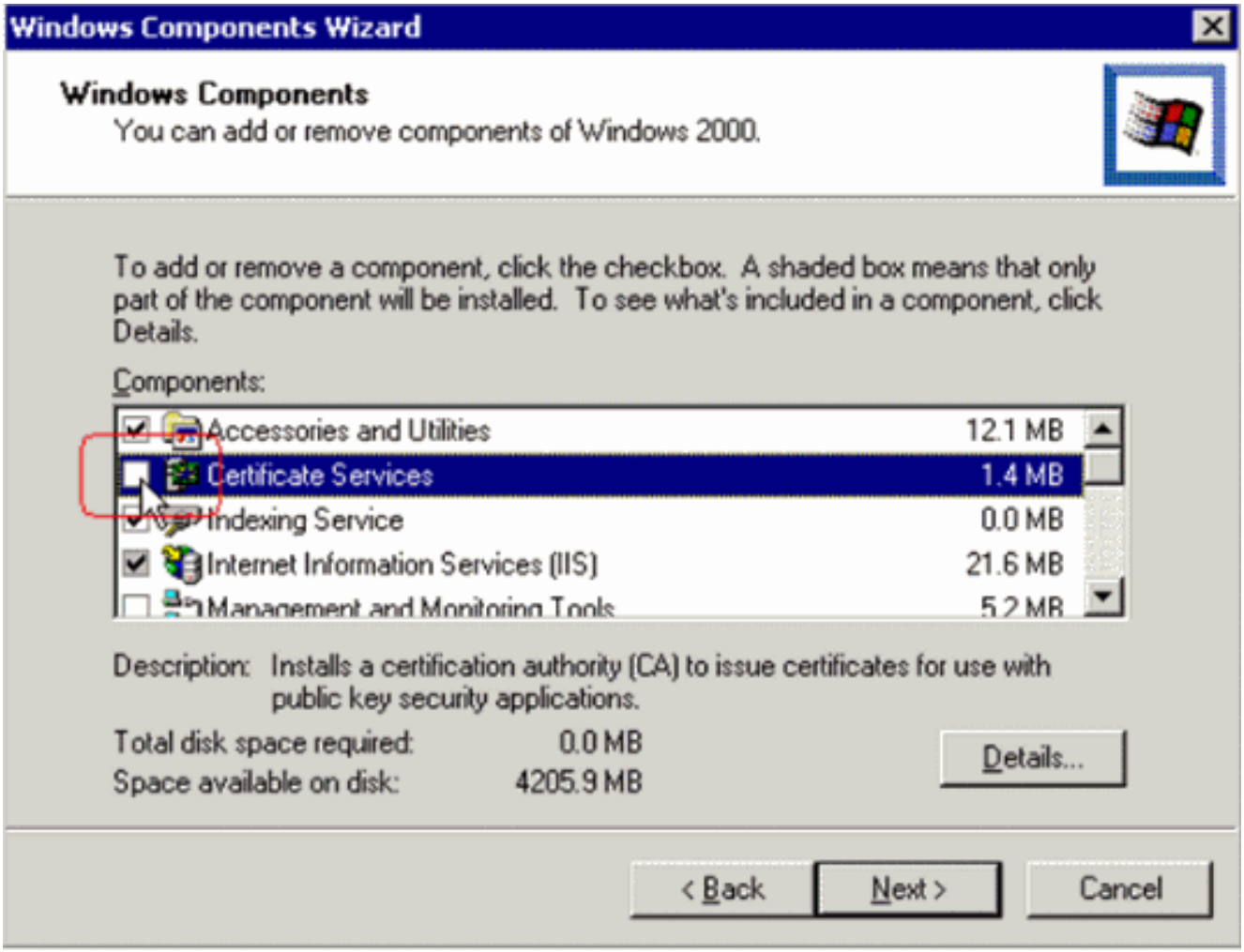
:

2. Wählen Sie links **Windows-Komponenten hinzufügen/entfernen**

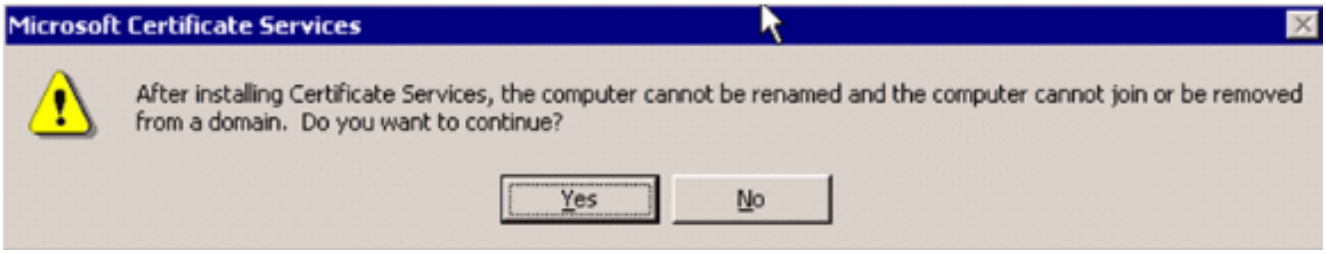


aus.

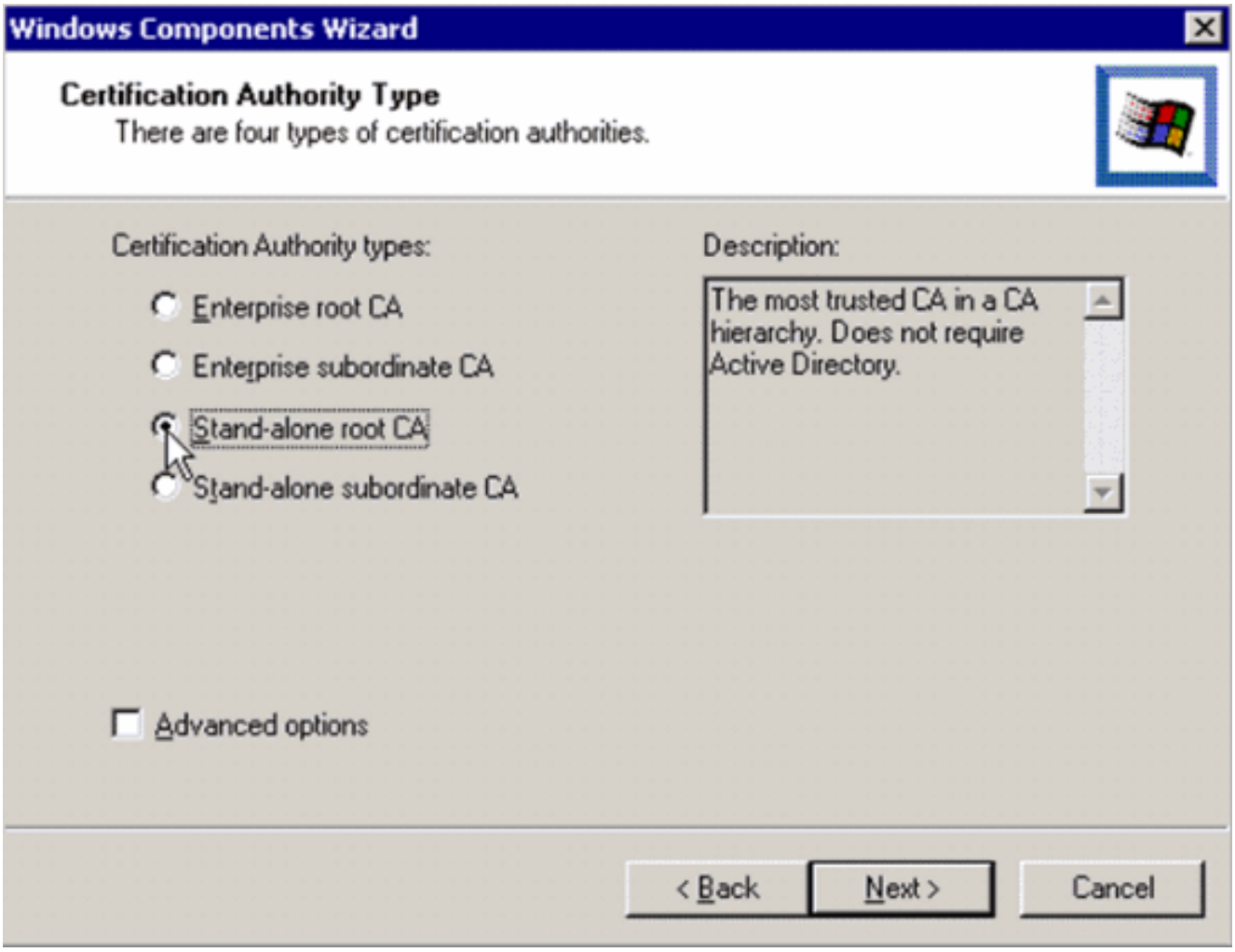
3. Aktivieren Sie **Zertifizierungsdienste**.



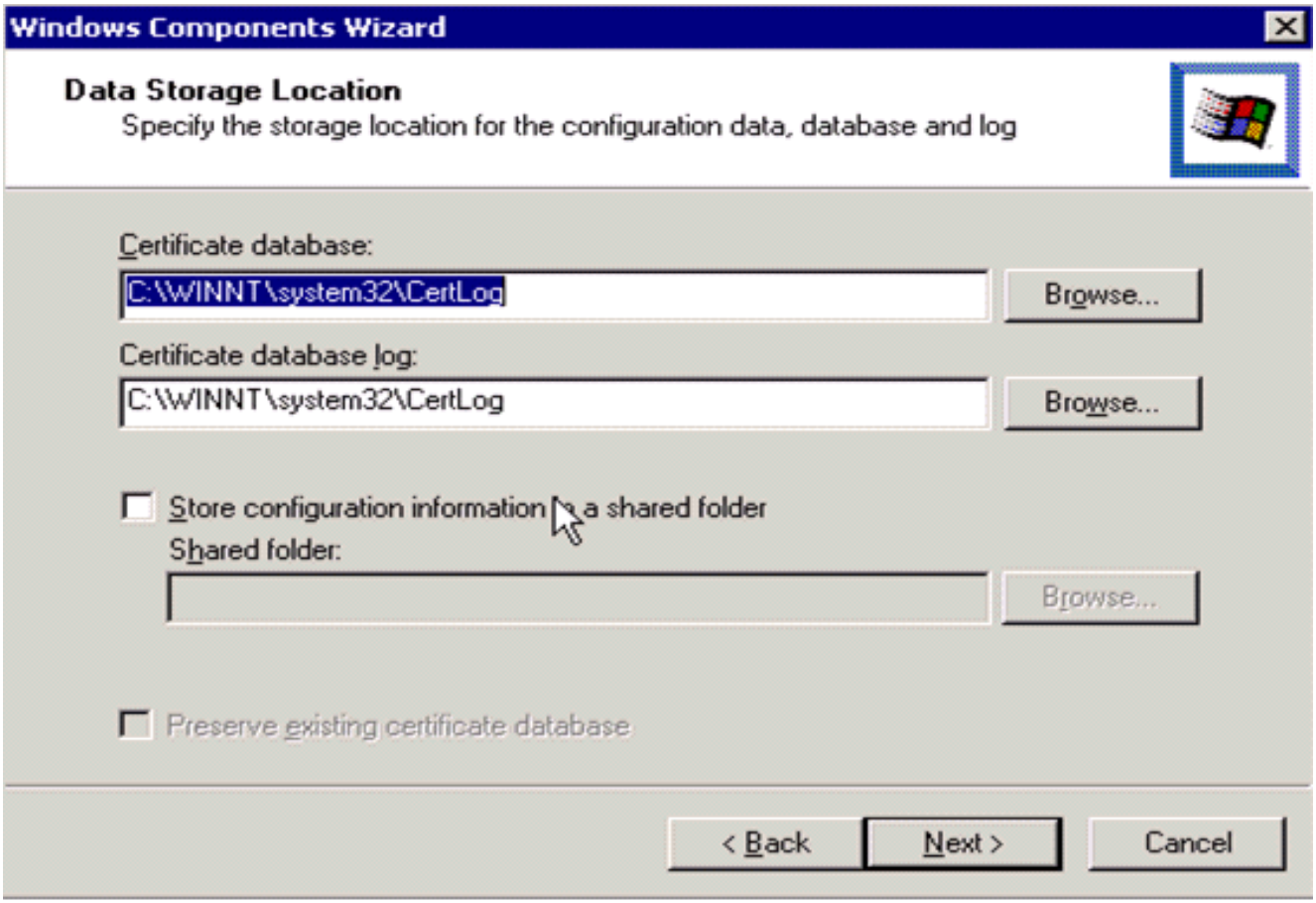
Überprüfen Sie diese Warnung, bevor Sie fortfahren:



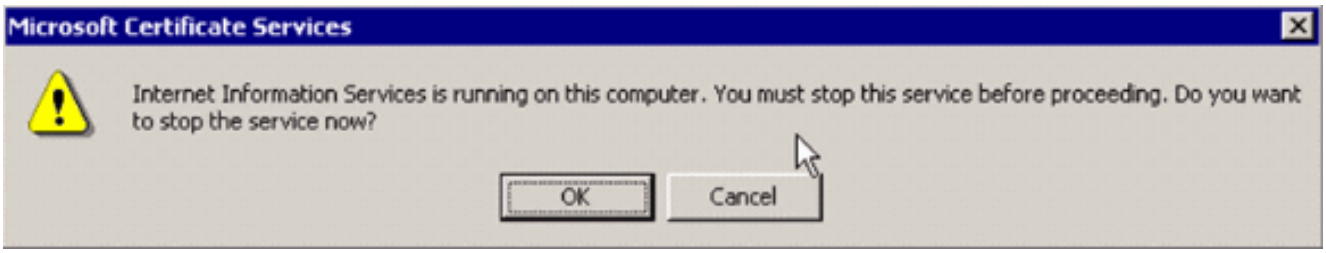
4. Wählen Sie die Zertifizierungsstelle aus, die Sie installieren möchten. Um eine einfache eigenständige Autorität zu erstellen, wählen Sie die **eigenständige Stammzertifizierungsstelle aus**.



5. Geben Sie die erforderlichen Informationen zur Zertifizierungsstelle ein. Mit diesen Informationen wird ein selbstsigniertes Zertifikat für Ihre Zertifizierungsstelle erstellt. Beachten Sie den Namen der CA, den Sie verwenden.Die Zertifizierungsstelle speichert die Zertifikate in einer Datenbank. In diesem Beispiel wird die von Microsoft vorgeschlagene Standardeinrichtung
verwendet:



6. Microsoft Certification Authority-Dienste verwenden den IIS Microsoft Web Server, um Client- und Serverzertifikate zu erstellen und zu verwalten. Der IIS-Dienst muss für diesen Vorgang neu gestartet
werden:



Der Microsoft Windows 2000 Server installiert den neuen Dienst jetzt. Sie benötigen Ihre Windows 2000 Server-Installations-CD, um neue Windows-Komponenten installieren zu können.Die Zertifizierungsstelle ist jetzt installiert.

Installieren des Zertifikats im Cisco Wireless LAN Controller

Um EAP-FAST Version 2 und EAP-TLS auf dem lokalen EAP-Server eines Cisco Wireless LAN Controllers zu verwenden, gehen Sie wie folgt vor:

1. Installieren Sie das Gerätezertifikat auf dem Wireless LAN Controller.
2. Laden Sie ein Zertifikat der Anbieterzertifizierungsstelle auf den Wireless LAN Controller herunter.
3. Konfigurieren Sie den Wireless LAN Controller für die Verwendung von EAP-TLS.

Beachten Sie, dass im Beispiel in diesem Dokument der Access Control Server (ACS) auf demselben Host wie Microsoft Active Directory und die Microsoft Certification Authority installiert ist. Die Konfiguration sollte jedoch identisch sein, wenn sich der ACS-Server auf einem anderen

Server befindet.

Installieren Sie das Gerätezertifikat auf dem Wireless LAN-Controller.

Führen Sie diese Schritte aus:

1. . Gehen Sie wie folgt vor, um das Zertifikat für den Import in den WLC zu generieren:Gehen Sie zu **http://<serverIpAddr>/certsrv**.Wählen Sie **Zertifikat anfordern aus**, und klicken Sie auf **Weiter**.Wählen Sie **Erweiterte Anforderung** aus, und klicken Sie auf **Weiter**.Wählen Sie **eine Zertifikatsanforderung an diese Zertifizierungsstelle mithilfe eines Formulars senden aus,** und klicken Sie auf **Weiter**.Wählen Sie **Webserver** für Zertifikatsvorlage aus, und geben Sie die entsprechenden Informationen ein. Markieren Sie dann die Tasten als **exportierbar**.Sie erhalten nun ein Zertifikat, das Sie auf Ihrem Computer installieren müssen.
2. Gehen Sie wie folgt vor, um das Zertifikat vom PC abzurufen:Öffnen Sie einen Internet Explorer-Browser, und wählen Sie **Extras > Internetoptionen > Inhalt aus**.Klicken Sie auf **Zertifikate**.Wählen Sie das neu installierte Zertifikat aus dem Dropdown-Menü aus.Klicken Sie auf **Exportieren**.Klicken Sie zweimal auf **Weiter** und wählen Sie **Yes export the private key (Privater Schlüssel exportieren)**. Dieses Format ist PKCS#12 (PFX-Format).Wählen Sie **Starken Schutz aktivieren aus**.Geben Sie ein Kennwort ein.Speichern Sie die Datei in einer Datei <tme2.pfx>.
3. Kopieren Sie das Zertifikat im PKCS#12-Format auf einen Computer, auf dem Sie OpenSSL installiert haben, um es in das PEM-Format zu konvertieren.
```
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. Laden Sie das konvertierte Gerätezertifikat im PEM-Format auf den WLC herunter.
```
(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. Überprüfen Sie nach dem Neustart das Zertifikat.
```
(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
```

Laden Sie ein Zertifikat der Anbieterzertifizierungsstelle auf den Wireless LAN Controller herunter.

Führen Sie diese Schritte aus:

1. Gehen Sie wie folgt vor, um das Zertifizierungsstellenzertifikat des Anbieters abzurufen:Gehen Sie zu **http://<serverIpAddr>/certsrv**.Wählen Sie **Zertifikat abrufen aus**, und klicken Sie auf **Weiter**.Wählen Sie das CA-Zertifikat aus.Klicken Sie auf **DER codiert**.Klicken Sie auf **Zertifizierungsstellenzertifikat herunterladen** und speichern Sie das Zertifikat als **rootca.cer**.
2. Konvertieren Sie die Anbieter-CA aus dem DER-Format in das PEM-Format mit dem **Befehl openssl x509 -in rootca.cer -notify DER -out rootca.pem -out PEM**.Die Ausgabedatei ist rootca.pem im PEM-Format.
3. Laden Sie das Zertifizierungsstellenzertifikat des Anbieters herunter:

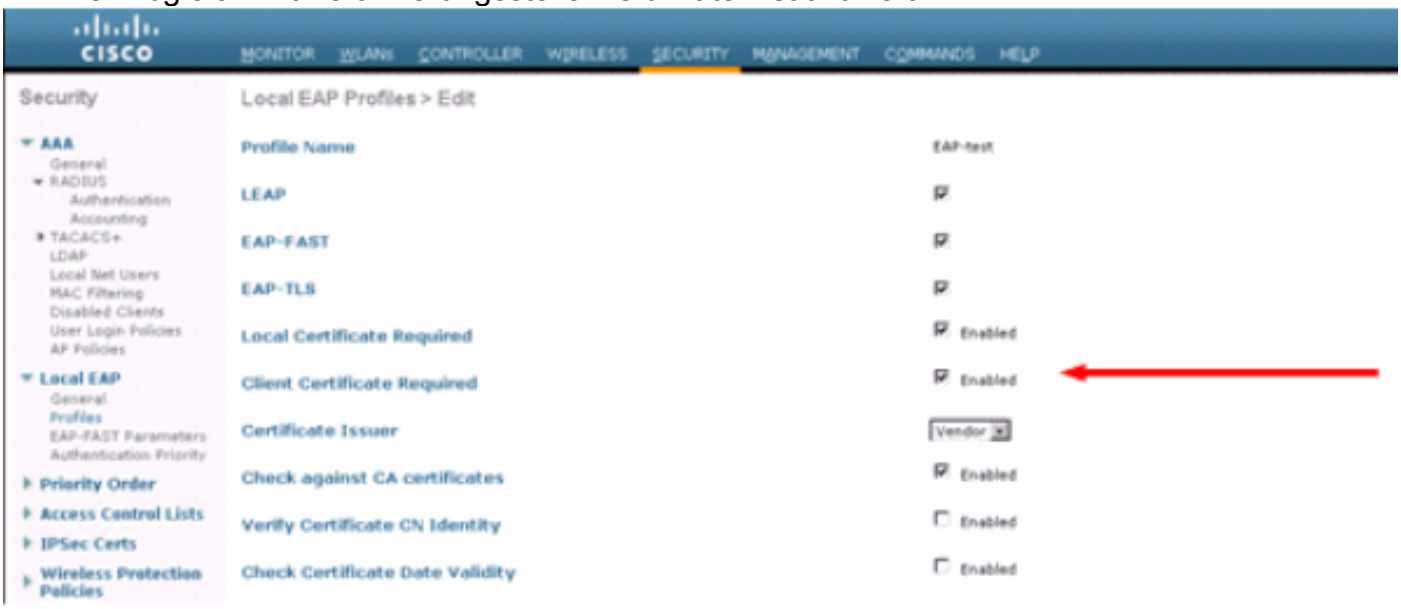
```
(Cisco Controller) >transfer download datatype eapcacert

(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.
```

Konfigurieren des Wireless LAN-Controllers für die Verwendung von EAP-TLS

Führen Sie diese Schritte aus:

Wählen Sie in der GUI **Security > Local EAP > Profiles**, wählen Sie das Profil aus, und prüfen Sie, ob diese Einstellungen vorhanden sind:

- Lokales Zertifikat erforderlich ist aktiviert.
- Client-Zertifikat erforderlich ist aktiviert.
- Zertifikataussteller ist Anbieter.
- Der Abgleich mit Zertifizierungsstellenzertifikaten ist aktiviert.



Installieren des Zertifikats der Zertifizierungsstelle auf dem Client-Gerät

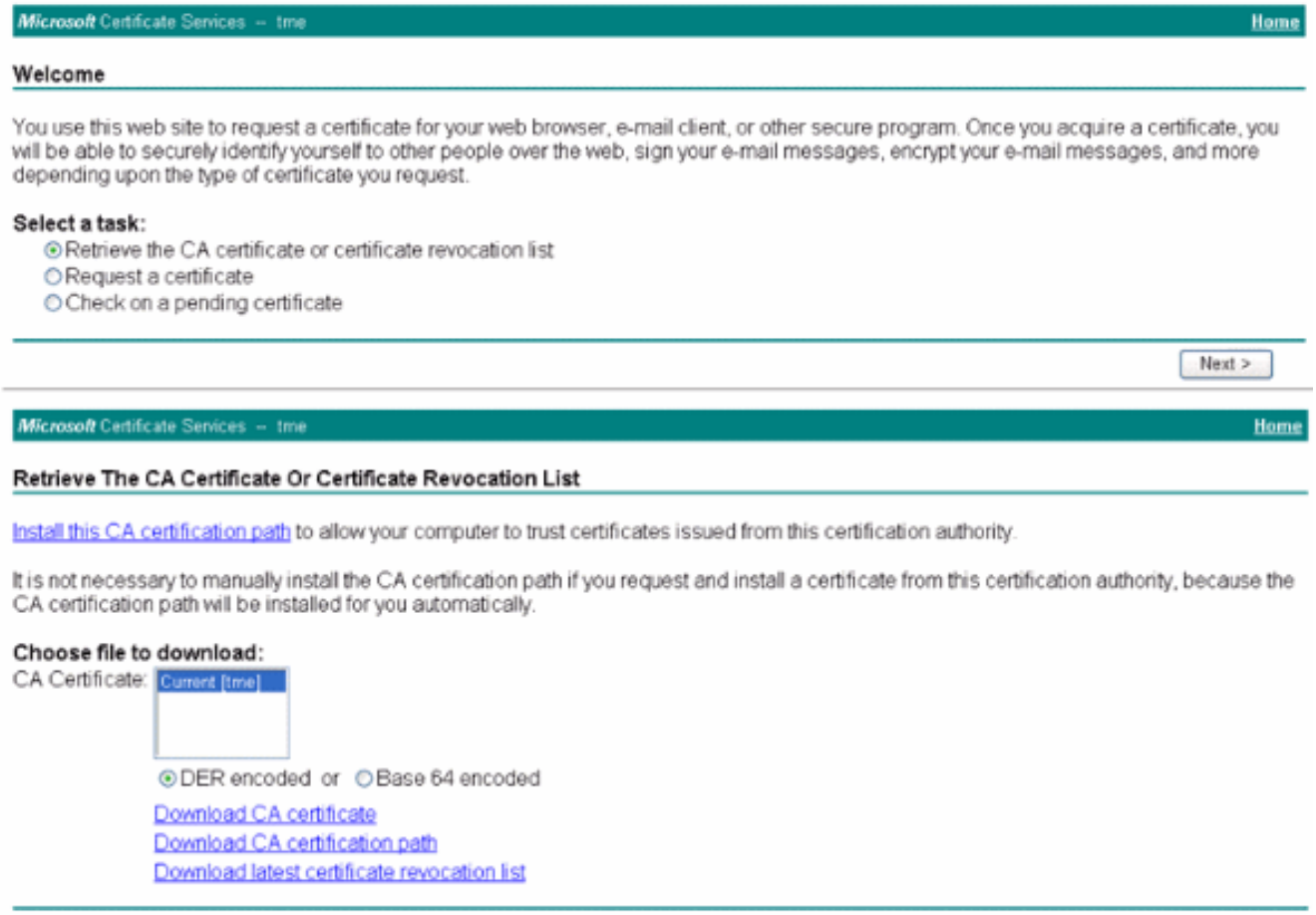
Herunterladen und Installieren eines Zertifikats der Stammzertifizierungsstelle für den Client

Der Client muss ein Root-Zertifizierungsstellenzertifikat von einem Zertifizierungsstellen-Server beziehen. Es gibt mehrere Methoden, mit denen Sie ein Clientzertifikat abrufen und auf dem Windows XP-Computer installieren können. Um ein gültiges Zertifikat zu erhalten, muss der Windows XP-Benutzer mit seiner Benutzer-ID angemeldet sein und über eine Netzwerkverbindung verfügen.

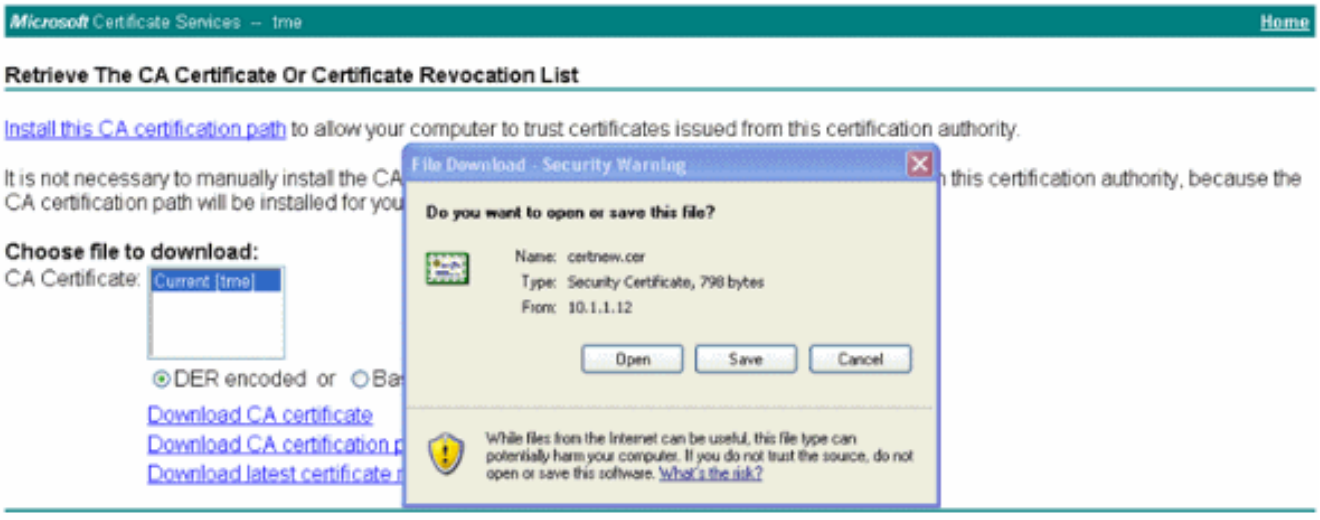
Ein Webbrowser auf dem Windows XP-Client und eine kabelgebundene Verbindung zum Netzwerk wurden verwendet, um ein Client-Zertifikat vom privaten Root Certification Authority-Server zu erhalten. Dieses Verfahren wird verwendet, um das Clientzertifikat von einem Microsoft Certification Authority-Server zu erhalten:

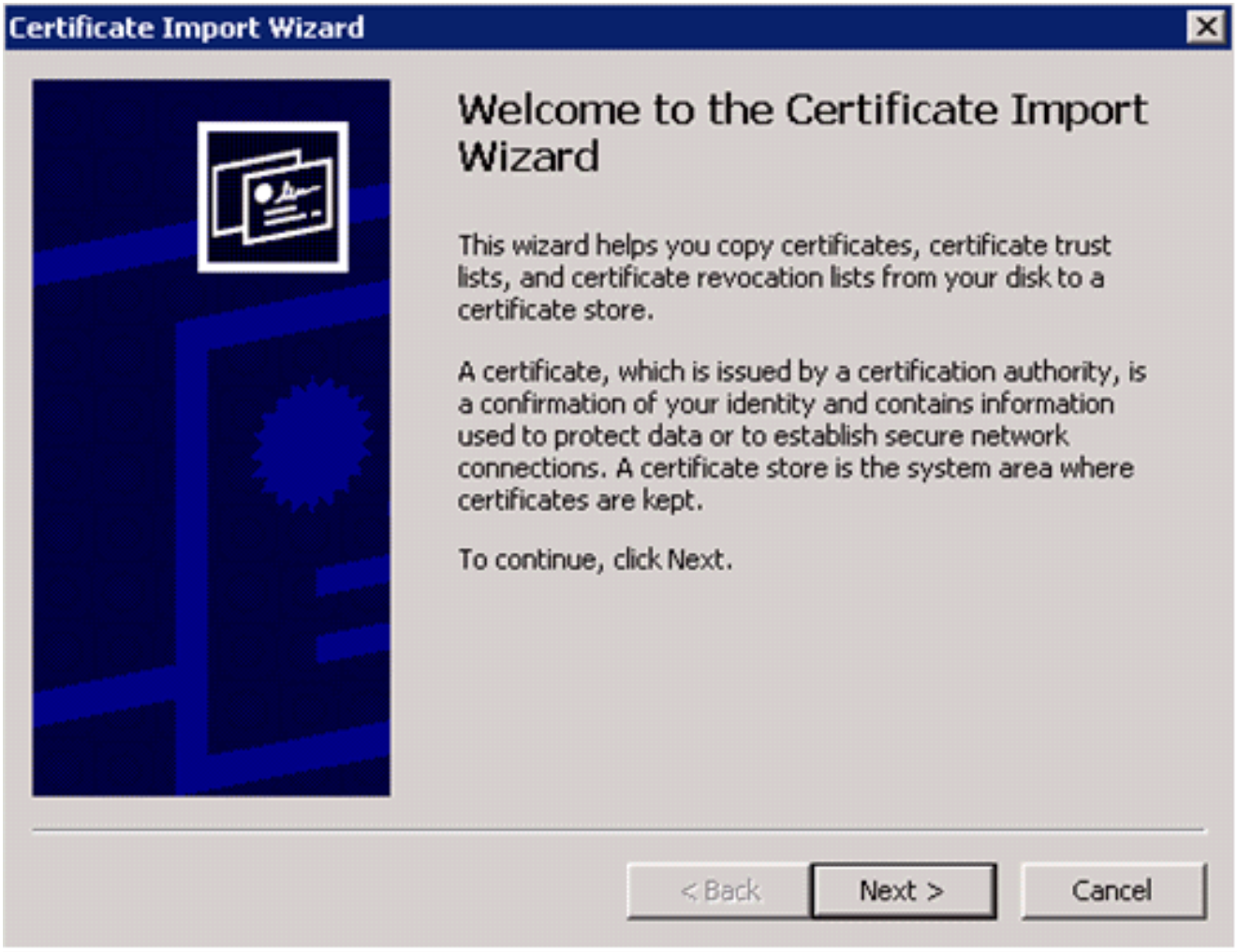
1. Verwenden Sie einen Webbrowser auf dem Client, und verweisen Sie den Browser auf den Zertifizierungsstellen-Server. Geben Sie dazu **http://IP-address-of-Root-CA/certsrv** ein.
2. Melden Sie sich mit **Domain_Name\user_name an**. Sie müssen sich mit dem Benutzernamen der Person anmelden, die den XP-Client verwenden soll.
3. Wählen Sie im Welcome-Fenster die Option **Retrieve a CA certificate (Zertifikat der Zertifizierungsstelle abrufen) aus,** und klicken Sie auf **Next (Weiter)**.
4. Wählen Sie **Base64 Encoding** und **Download CA Certificate aus**.
5. Klicken Sie im Fenster Zertifikat ausgegeben auf **Dieses Zertifikat installieren** und dann auf **Weiter**.
6. Wählen Sie **Automatisch den Zertifikatsspeicher aus**, und klicken Sie auf **Weiter**, um eine erfolgreiche Importmeldung zu erhalten.

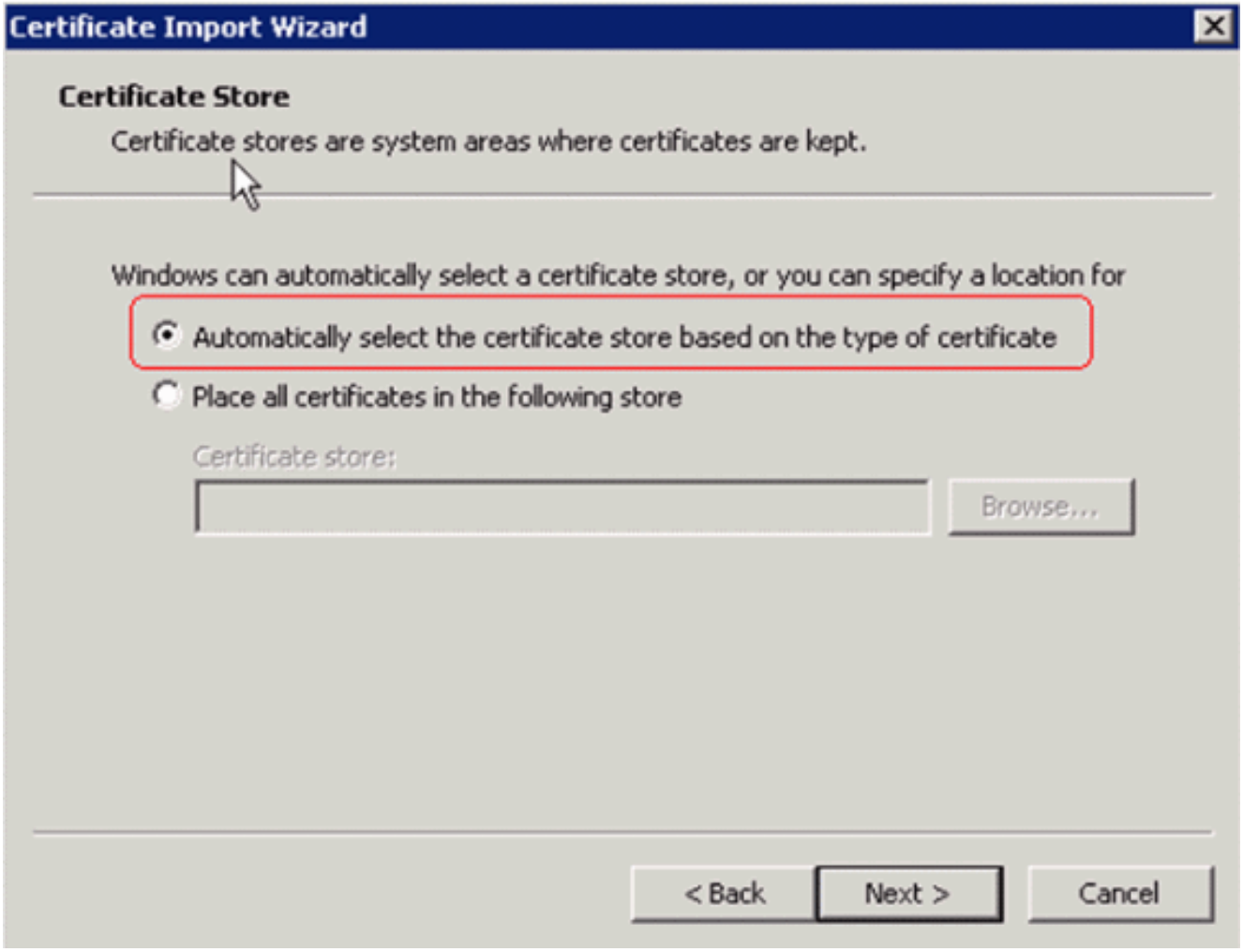
7. Stellen Sie eine Verbindung zur Zertifizierungsstelle her, um das Zertifikat der Zertifizierungsstelle
   abzurufen:



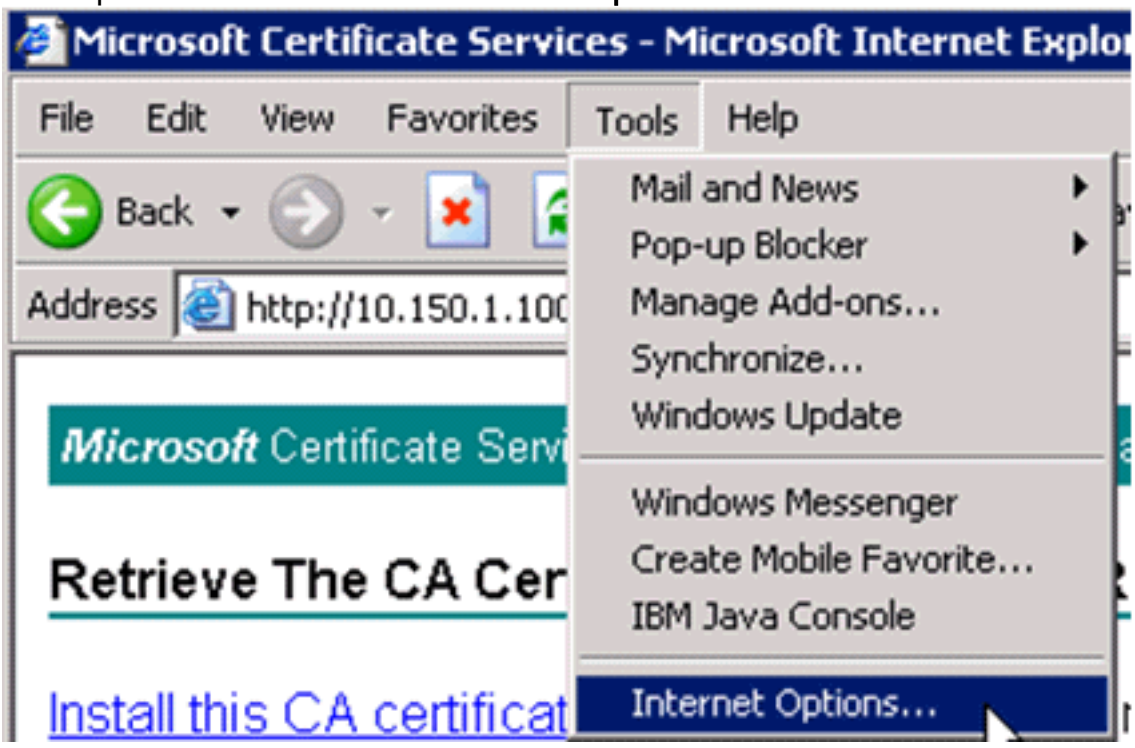
8. Klicken Sie auf **Zertifizierungsstellenzertifikat herunterladen**.

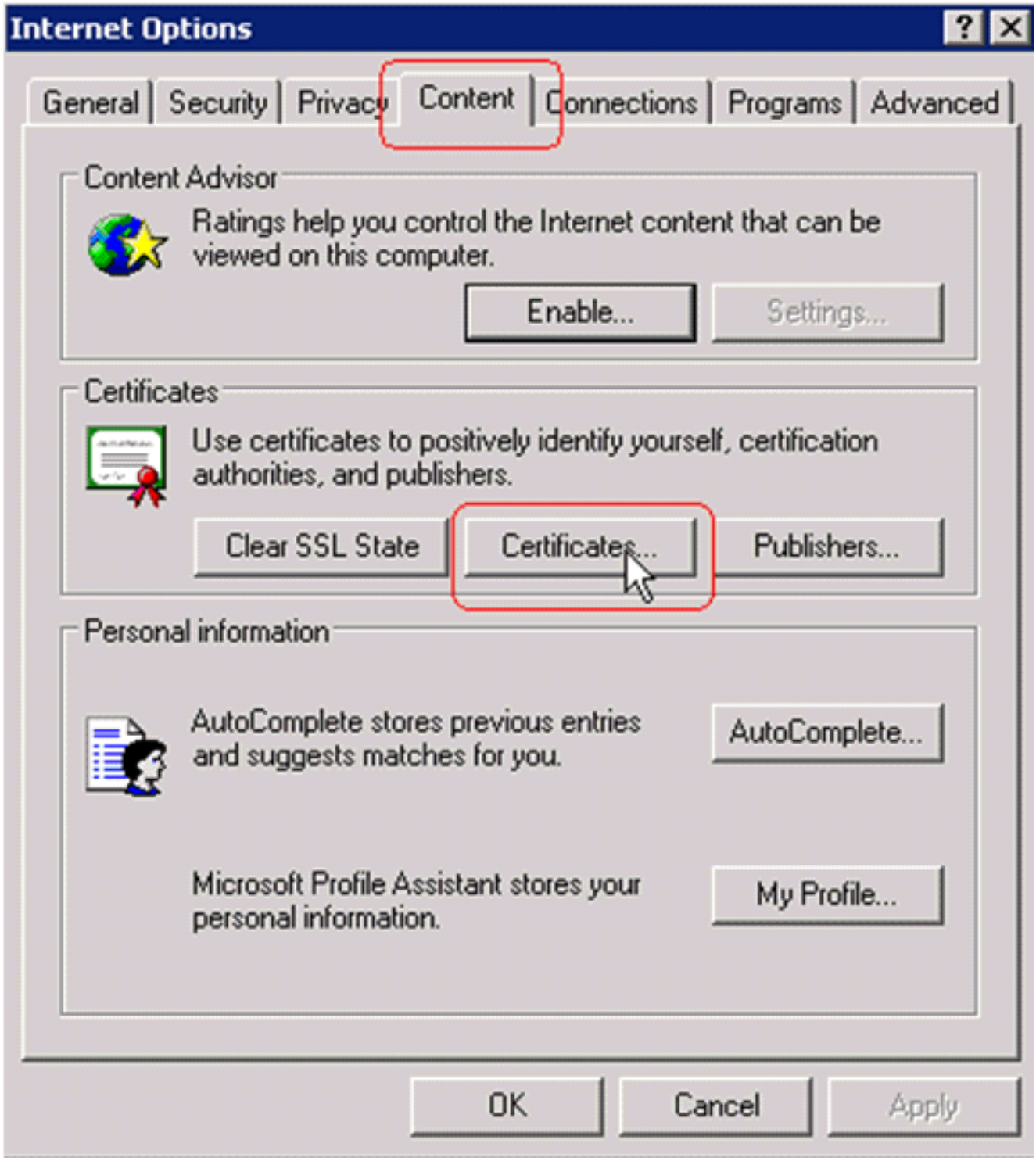



Certificate Import Wizard
Welcome to the Certificate Import Wizard
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
A certificate, which is issued by a certification authority, is a confirmation of your identity 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

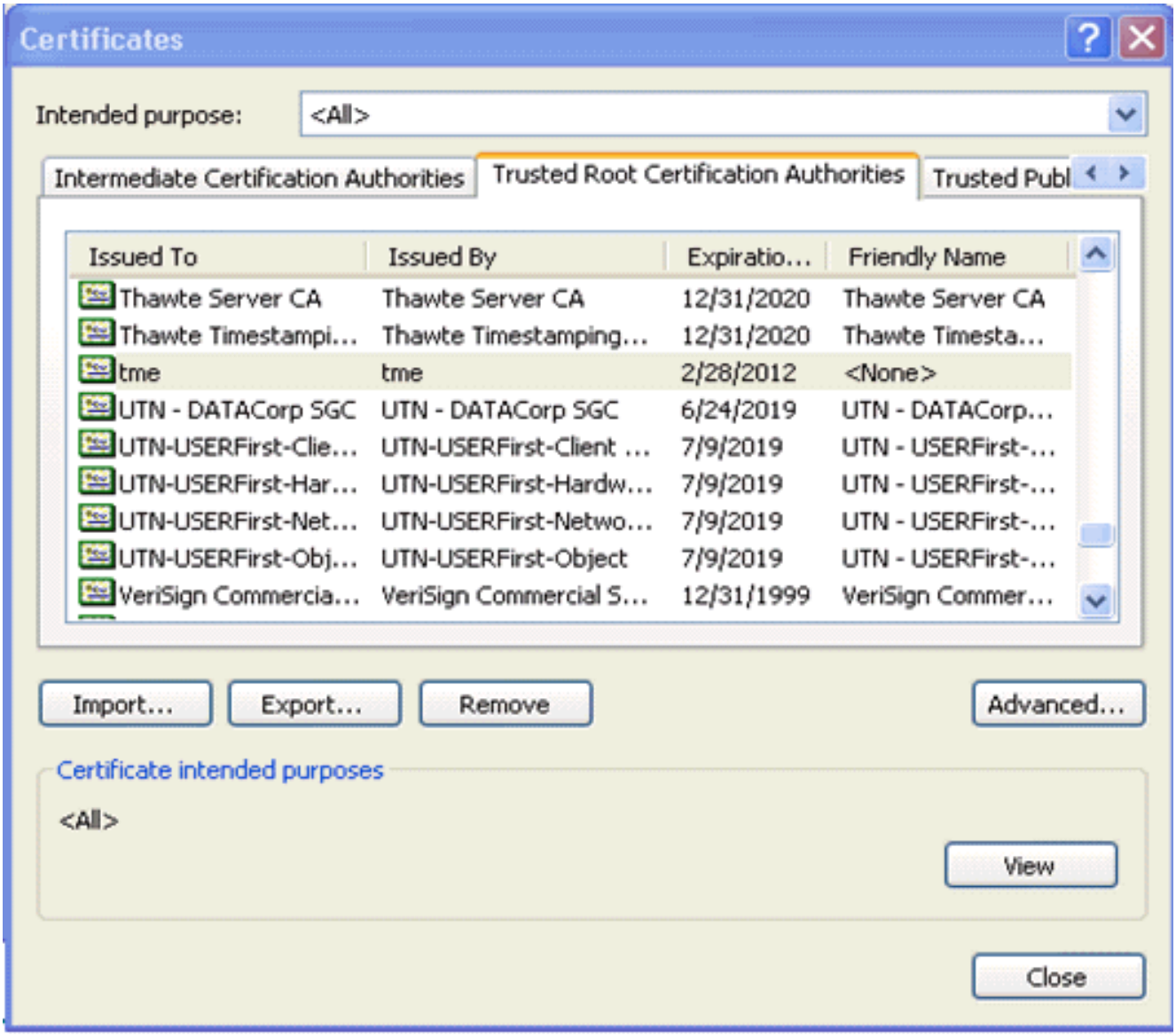

Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for
Automatically select the certificate store based on the type of certificate
Place all certificates in the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

9. Um zu überprüfen, ob das Zertifikat der Zertifizierungsstelle korrekt installiert ist, öffnen Sie Internet Explorer und wählen **Extras > Internetoptionen > Inhalt > Zertifikate** aus.





In der Trusted Root Certification Authority sollten Sie Ihre neu installierte Zertifizierungsstelle sehen:



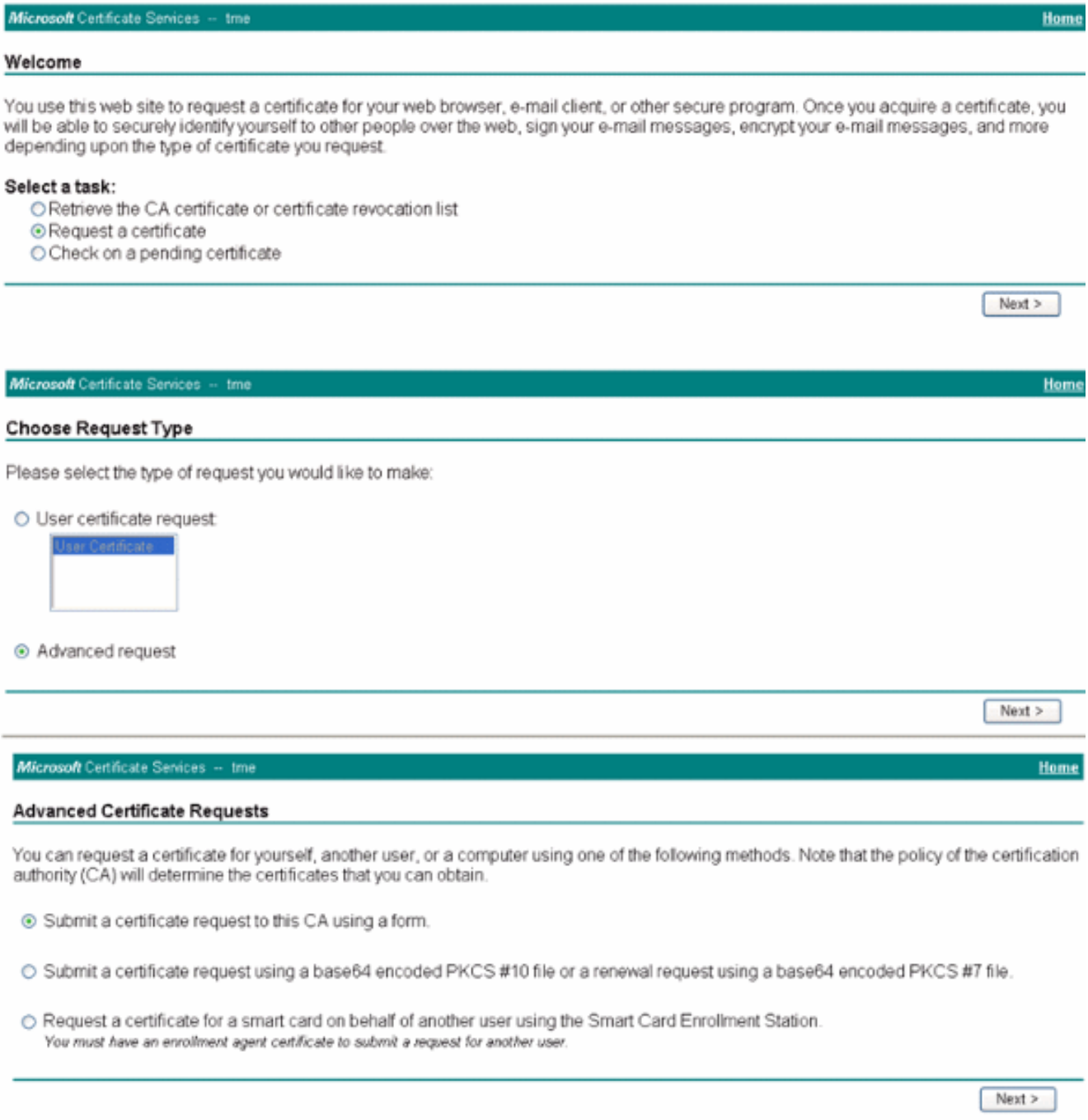
Generieren eines Clientzertifikats für ein Clientgerät

Der Client muss ein Zertifikat von einem Zertifizierungsstellen-Server für den WLC erhalten, um einen WLAN EAP-TLS-Client zu authentifizieren. Es gibt mehrere Methoden, mit denen Sie ein Clientzertifikat abrufen und auf dem Windows XP-Computer installieren können. Um ein gültiges Zertifikat zu erwerben, muss der Windows XP-Benutzer mit seiner Benutzer-ID angemeldet sein und über eine Netzwerkverbindung verfügen (entweder eine kabelgebundene Verbindung oder eine WLAN-Verbindung mit 802.1x-Sicherheit deaktiviert).

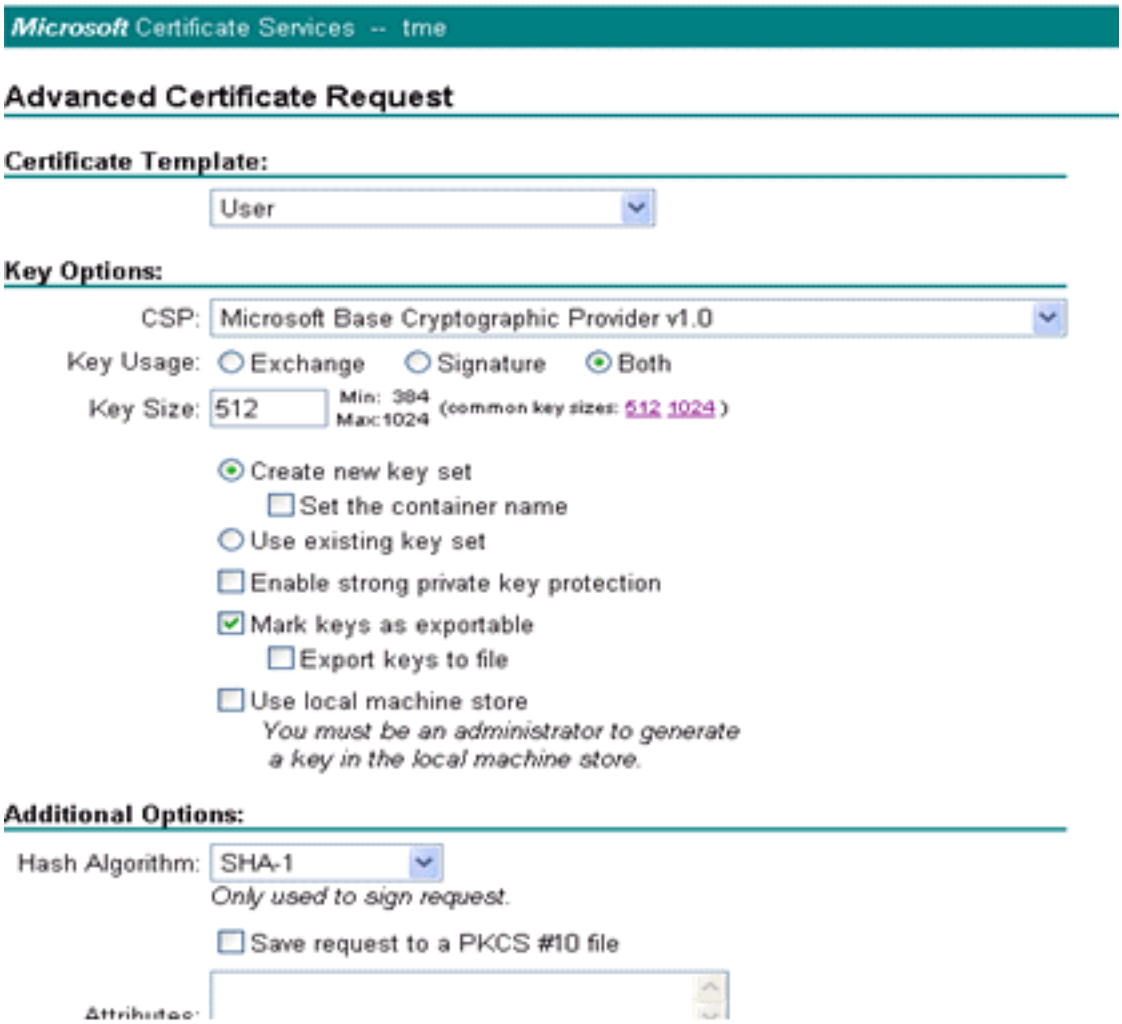
Ein Webbrowser auf dem Windows XP-Client und eine kabelgebundene Verbindung zum Netzwerk werden verwendet, um ein Client-Zertifikat vom privaten Root Certification Authority-Server zu erhalten. Dieses Verfahren wird verwendet, um das Clientzertifikat von einem Microsoft Certification Authority-Server zu erhalten:

1. Verwenden Sie einen Webbrowser auf dem Client, und verweisen Sie den Browser auf den Zertifizierungsstellen-Server. Geben Sie dazu **http://IP-address-of-Root-CA/certsrv** ein.
2. Melden Sie sich mit **Domain_Name\user_name an**. Sie müssen sich mit dem Benutzernamen der Person anmelden, die den XP-Client verwendet. (Der Benutzername wird in das Clientzertifikat eingebettet.)
3. Wählen Sie im Willkommensfenster **Zertifikat anfordern aus** und klicken Sie auf **Weiter**.
4. Wählen Sie **Erweiterte Anforderung aus**, und klicken Sie auf **Weiter**.

5. Wählen Sie **eine Zertifikatsanforderung an diese Zertifizierungsstelle mithilfe eines Formulars senden aus,** und klicken Sie auf **Weiter**.
6. Wählen Sie im Formular Erweiterte Zertifikatsanforderung die Zertifikatsvorlage als **Benutzer aus**, geben Sie die Schlüsselgröße als **1024** an, und klicken Sie auf **Senden**.
7. Klicken Sie im Fenster Zertifikat ausgegeben auf **Dieses Zertifikat installieren**. Dies führt zur erfolgreichen Installation eines Clientzertifikats auf dem Windows XP-Client.

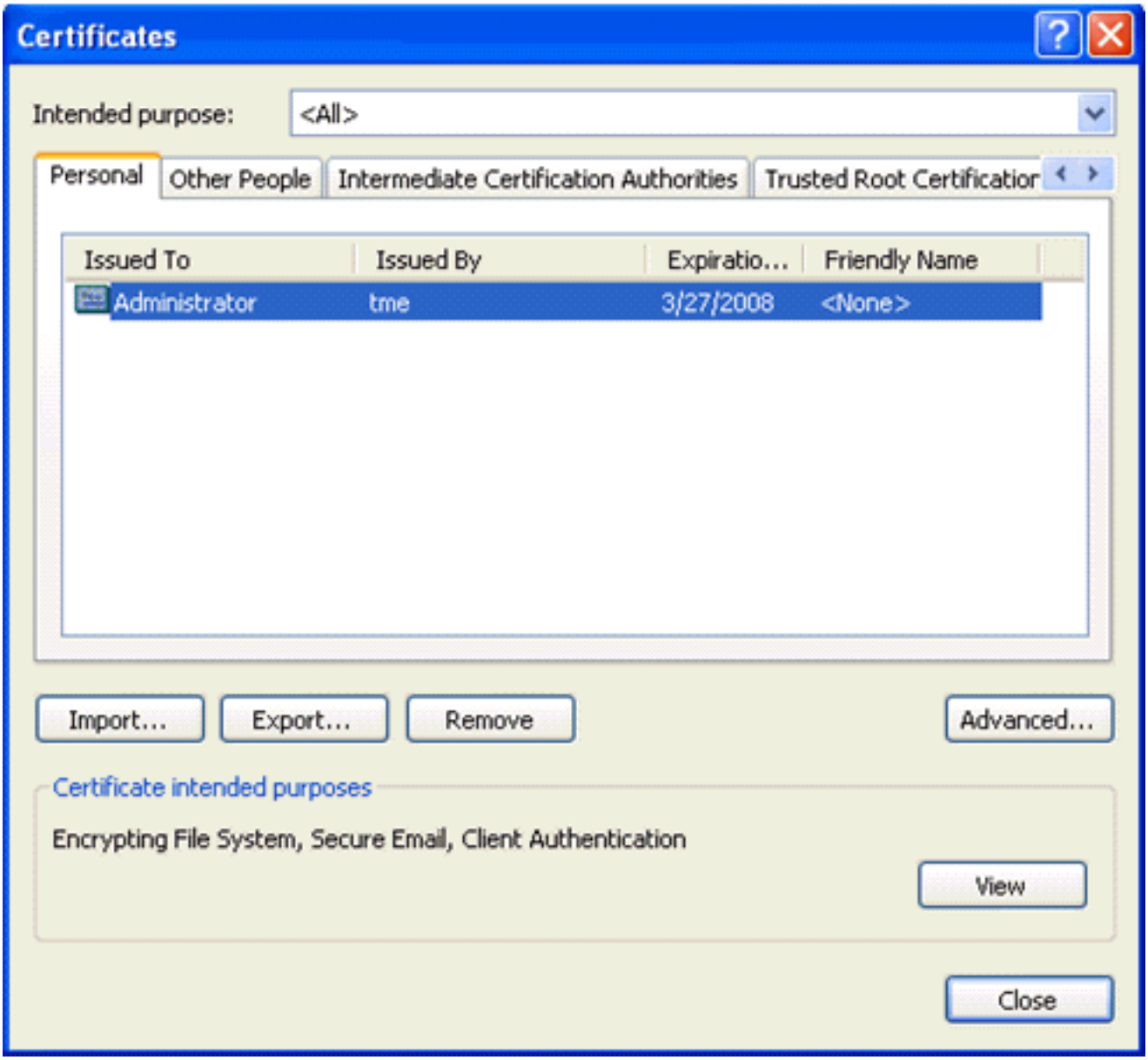


8. Wählen Sie **Client Authentication Certificate**



aus. Das Clientzertifikat wurde jetzt erstellt.

9. Um zu überprüfen, ob das Zertifikat installiert ist, gehen Sie zu Internet Explorer, und wählen Sie **Extras > Internetoptionen > Inhalt > Zertifikate aus**. Auf der Registerkarte Personal sollte das Zertifikat angezeigt werden.

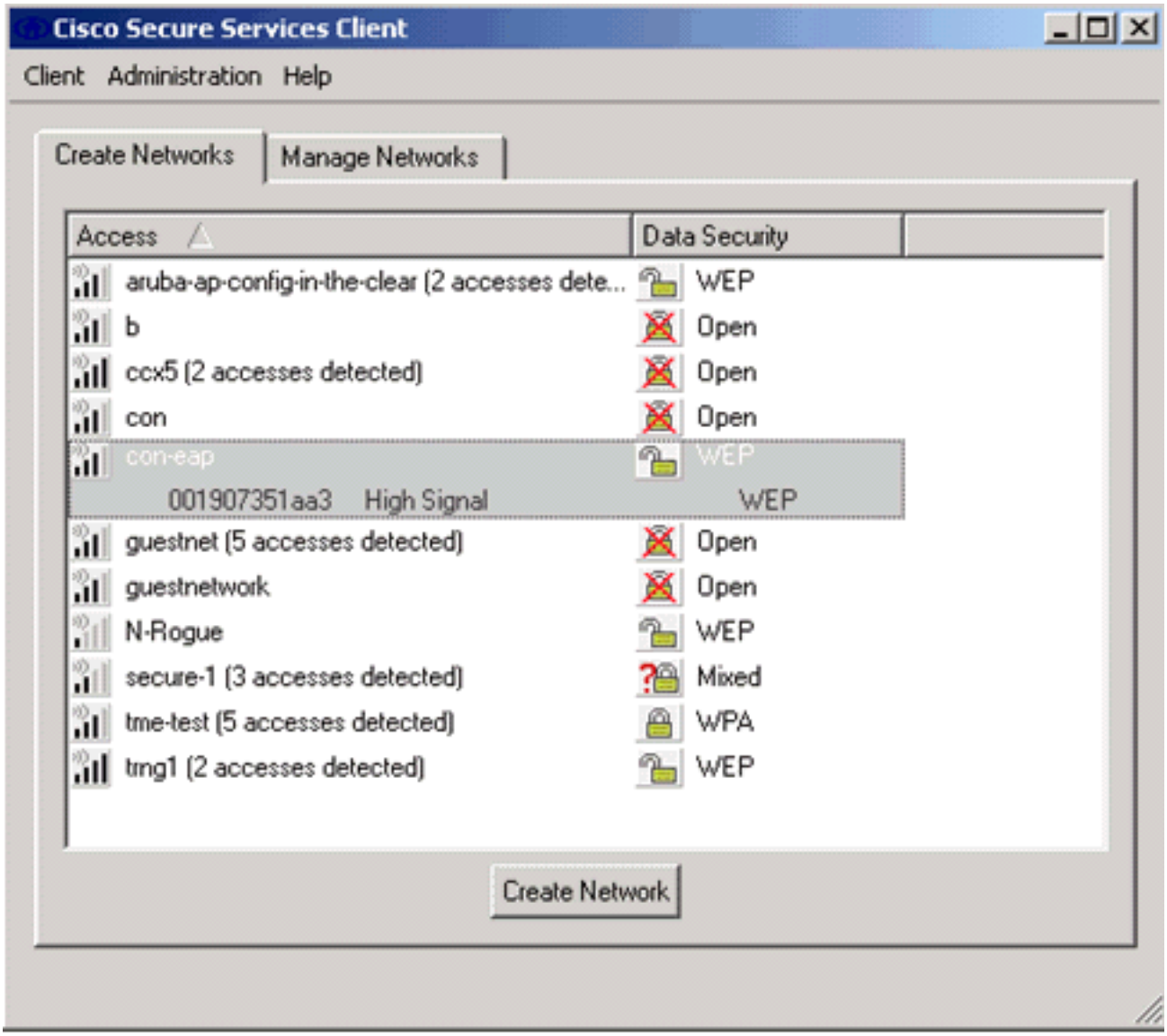


EAP-TLS mit Cisco Secure Services Client auf Client-Gerät

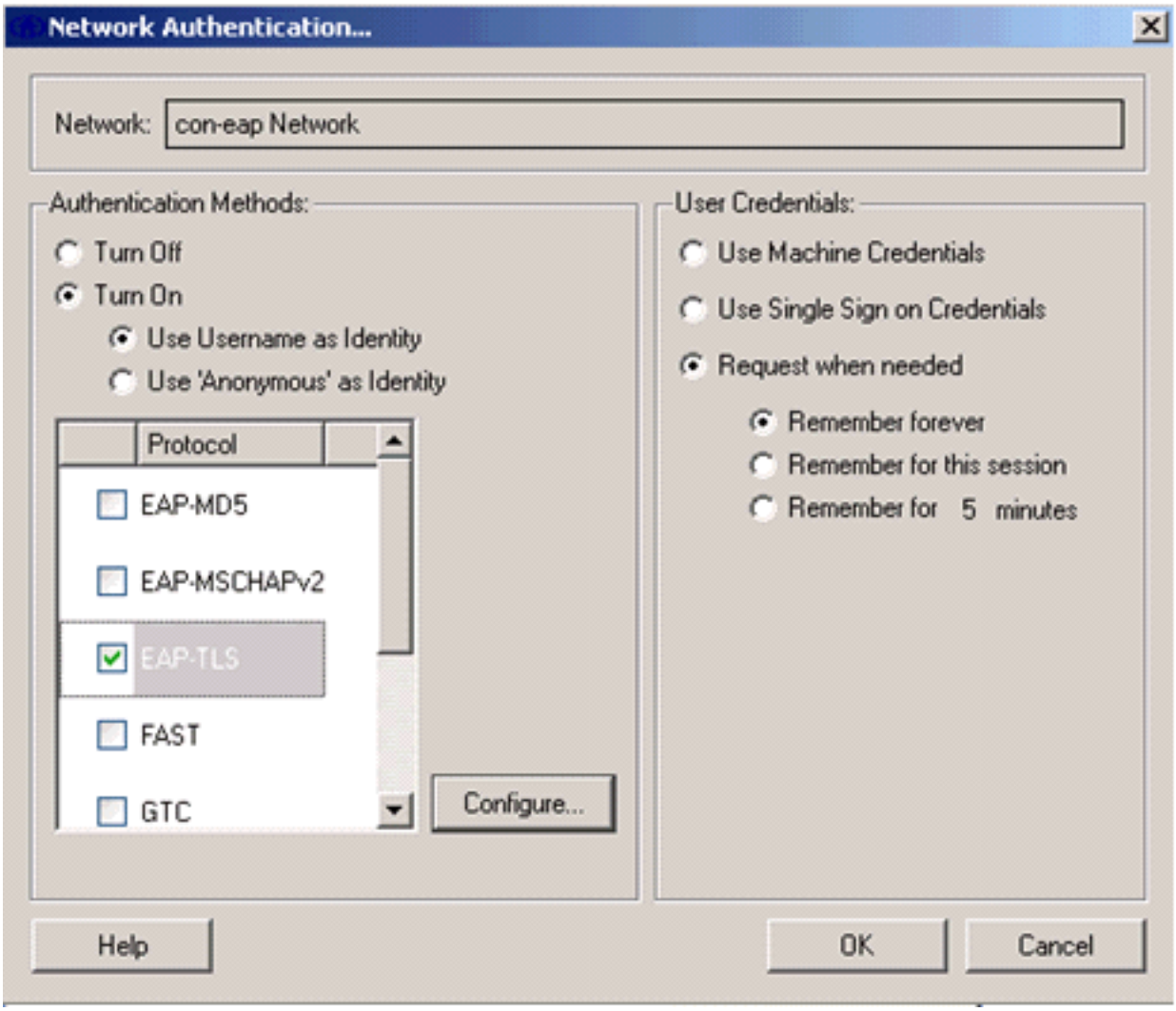
Führen Sie diese Schritte aus:

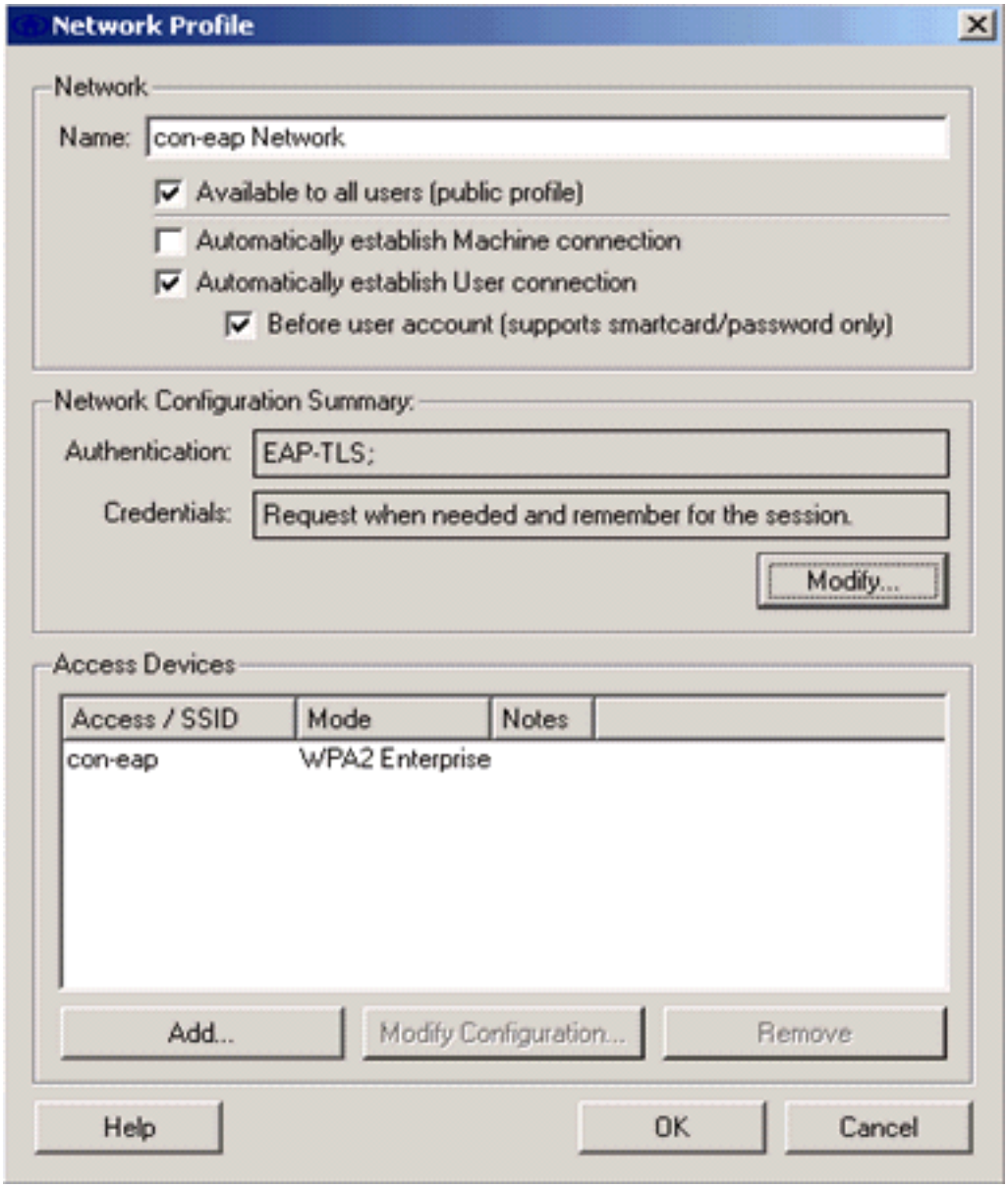
1. Der WLC sendet die SSID standardmäßig, sodass sie in der Liste "Create Networks" (Netzwerke erstellen) der gescannten SSIDs angezeigt wird. Um ein Netzwerkprofil zu erstellen, können Sie auf die SSID in der Liste (Enterprise) klicken und auf **Netzwerk erstellen**.Wenn die WLAN-Infrastruktur so konfiguriert ist, dass die Broadcast-SSID deaktiviert ist, müssen Sie die SSID manuell hinzufügen. Klicken Sie dazu unter Zugriffsgeräte auf **Hinzufügen** und geben Sie manuell die entsprechende SSID ein (z. B. Enterprise). Konfigurieren Sie das aktive Testverhalten für den Client. In diesem Fall sucht der Client aktiv nach seiner konfigurierten SSID. Geben Sie **Aktiv nach diesem Zugriffsgerät suchen** an, nachdem Sie die SSID im Fenster Zugriffsgerät hinzufügen eingegeben haben.**Hinweis:** Die Porteinstellungen lassen keine Enterprise-Modi (802.1X) zu, wenn die EAP-Authentifizierungseinstellungen nicht zuerst für das Profil konfiguriert wurden.
2. Klicken Sie auf **Create Network (Netzwerk erstellen)**, um das Fenster Network Profile (Netzwerkprofil) zu öffnen, in dem Sie die ausgewählte (oder konfigurierte) SSID einem Authentifizierungsmechanismus zuordnen können. Weisen Sie dem Profil einen

beschreibenden Namen zu.**Hinweis:** Mehrere WLAN-Sicherheitstypen und/oder SSIDs können diesem Authentifizierungsprofil zugeordnet
werden.

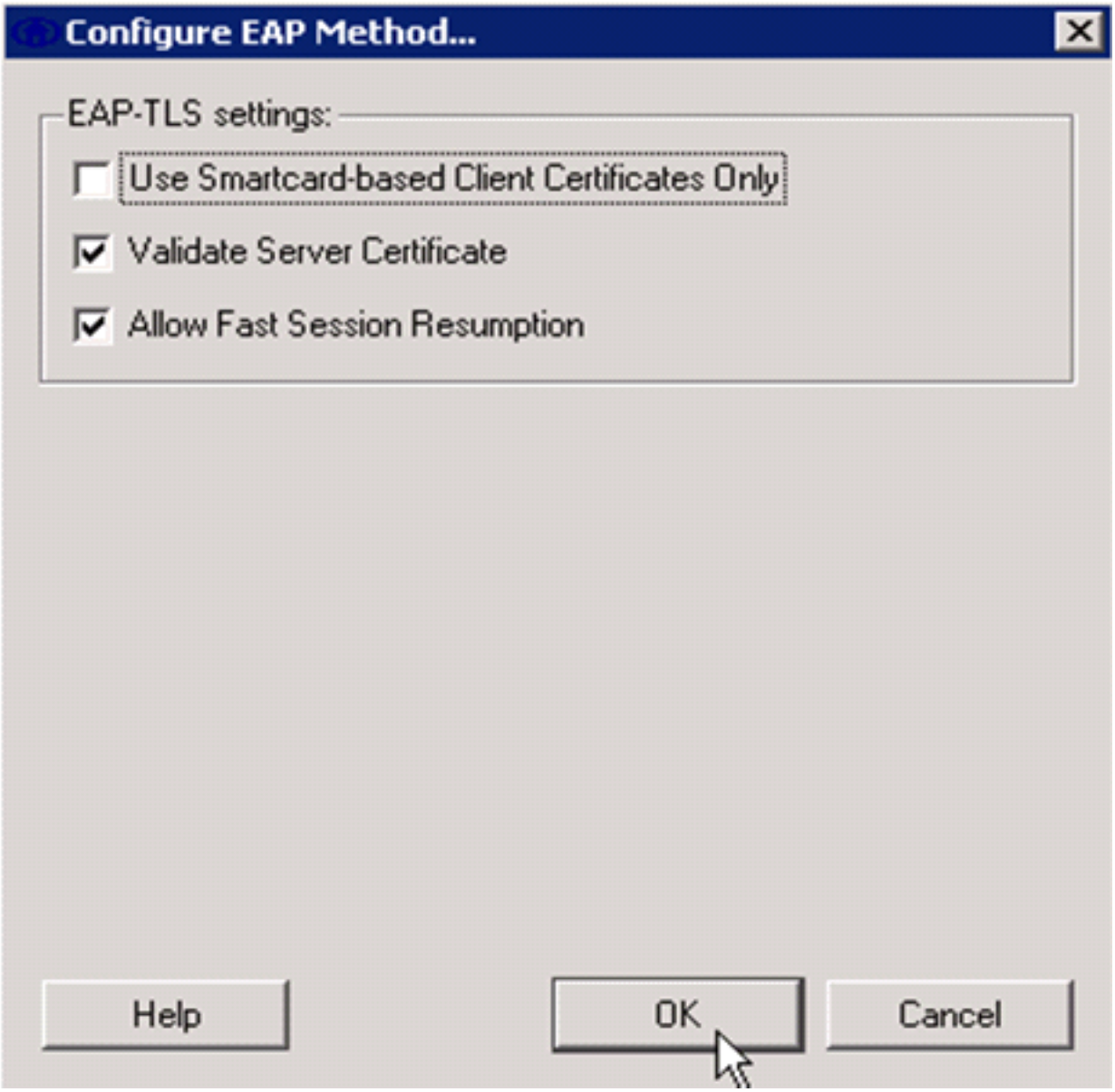


3. Aktivieren Sie die Authentifizierung, und überprüfen Sie die EAP-TLS-Methode. Klicken Sie anschließend auf **Konfigurieren**, um die EAP-TLS-Eigenschaften zu konfigurieren.
4. Klicken Sie unter "Übersicht über die Netzwerkkonfiguration" auf **Ändern**, um die EAP-/Anmeldeinformationseinstellungen zu konfigurieren.
5. Geben Sie **Authentifizierung einschalten**, wählen Sie **EAP-TLS** unter Protokoll aus, und wählen Sie **Benutzername** als Identität aus.
6. Geben Sie **Single Sign on Credentials (Single-Sign-on-Anmeldeinformationen verwenden**, um Anmeldeinformationen für die Netzwerkauthentifizierung zu verwenden. Klicken Sie auf **Konfigurieren**, um EAP-TLS-Parameter
einzurichten.

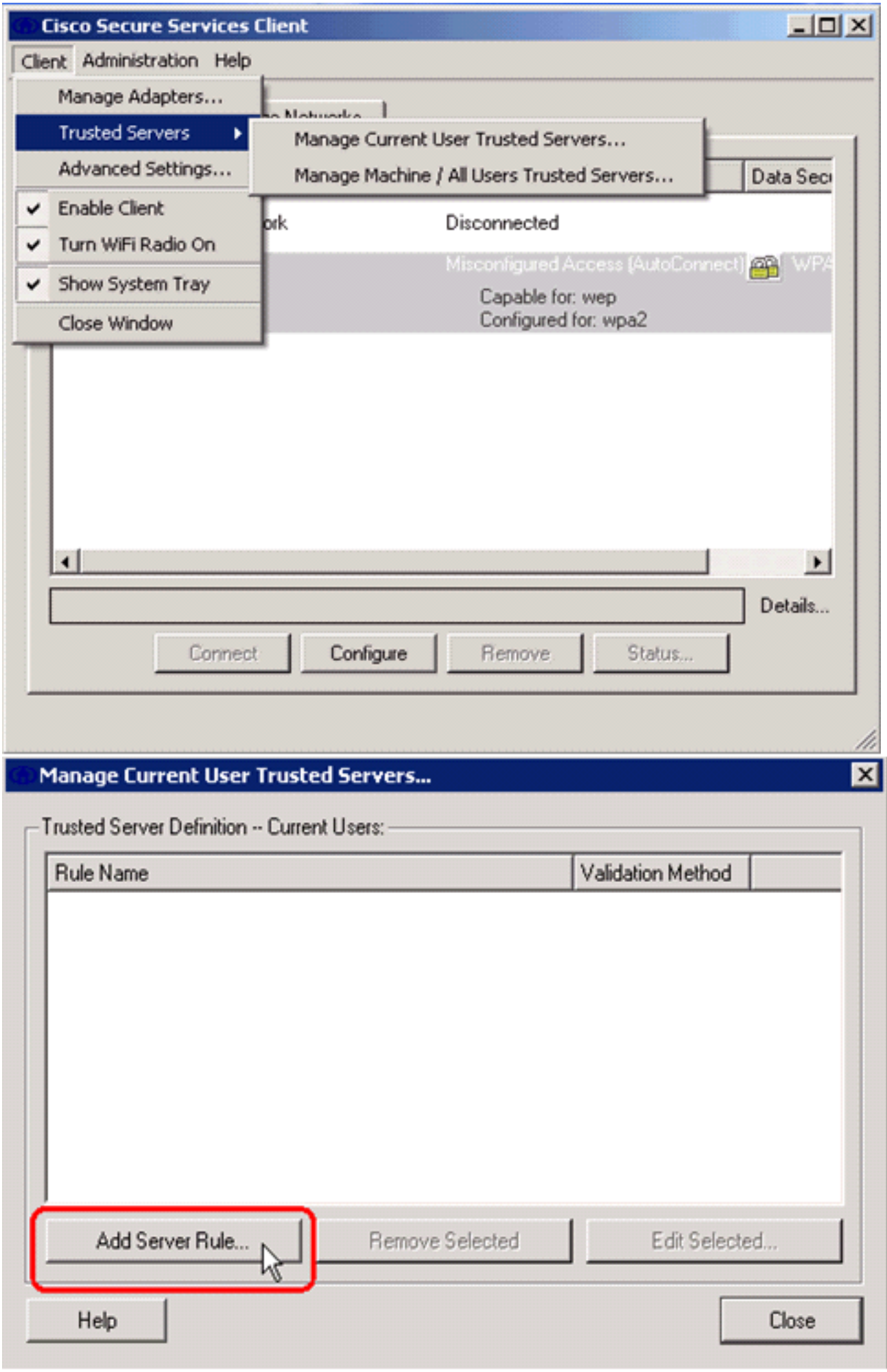

Network Authentication...
Network:
con-eap Network
Authentication Methods:
Turn Off
Turn On
Use Username as Identity
Use 'Anonymous' as Identity
Protocol
EAP-MD5
EAP-MSCHAPv2
EAP-TLS
FAST
GTC
Configure...
User Credentials:
Use Machine Credentials
Use Single Sign on Credentials
Request when needed
Remember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



7. Um eine gesicherte EAP-TLS-Konfiguration zu erhalten, müssen Sie das RADIUS-Serverzertifikat überprüfen. Aktivieren Sie dazu die Option **Serverzertifikat validieren**.

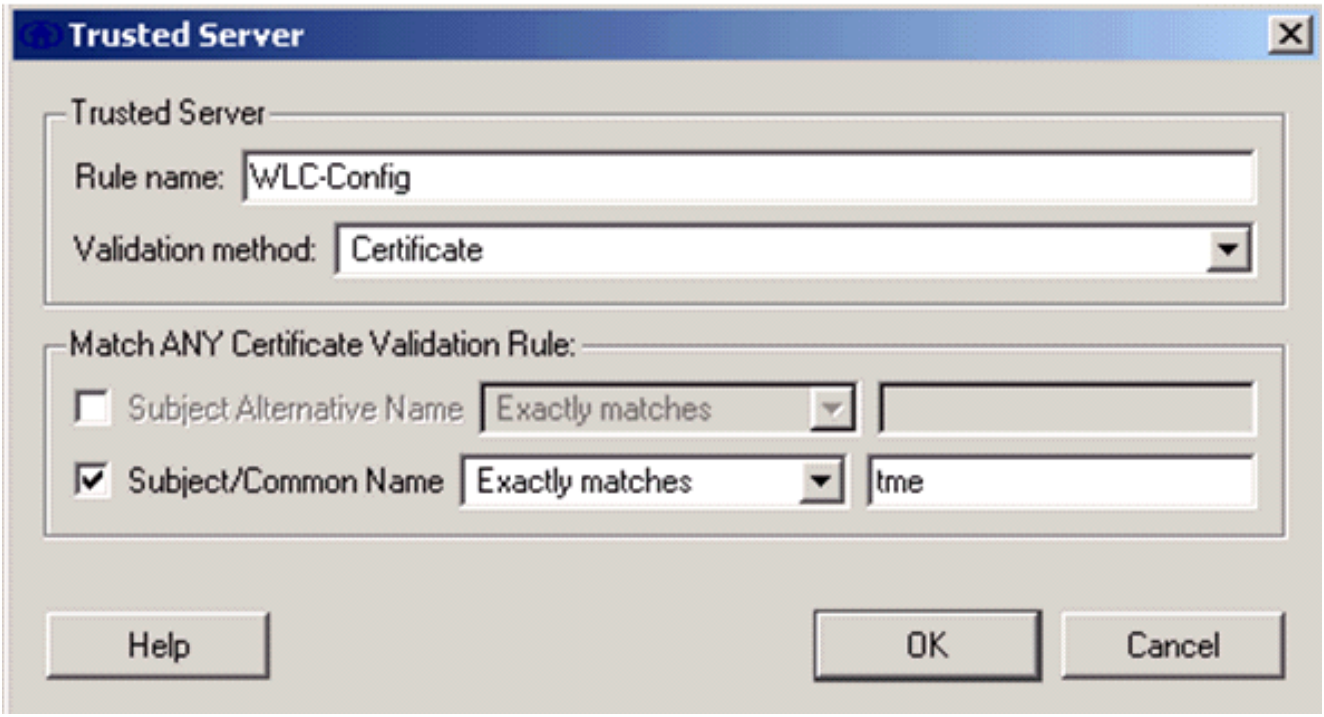


8. Um das RADIUS-Serverzertifikat zu validieren, müssen Sie den Cisco Secure Services Client angeben, damit nur das richtige Zertifikat akzeptiert werden kann. Wählen Sie **Client > Trusted Servers (Client > vertrauenswürdige Server) > Manage Current User Trusted Servers (Aktuelle vertrauenswürdige Server verwalten)**.



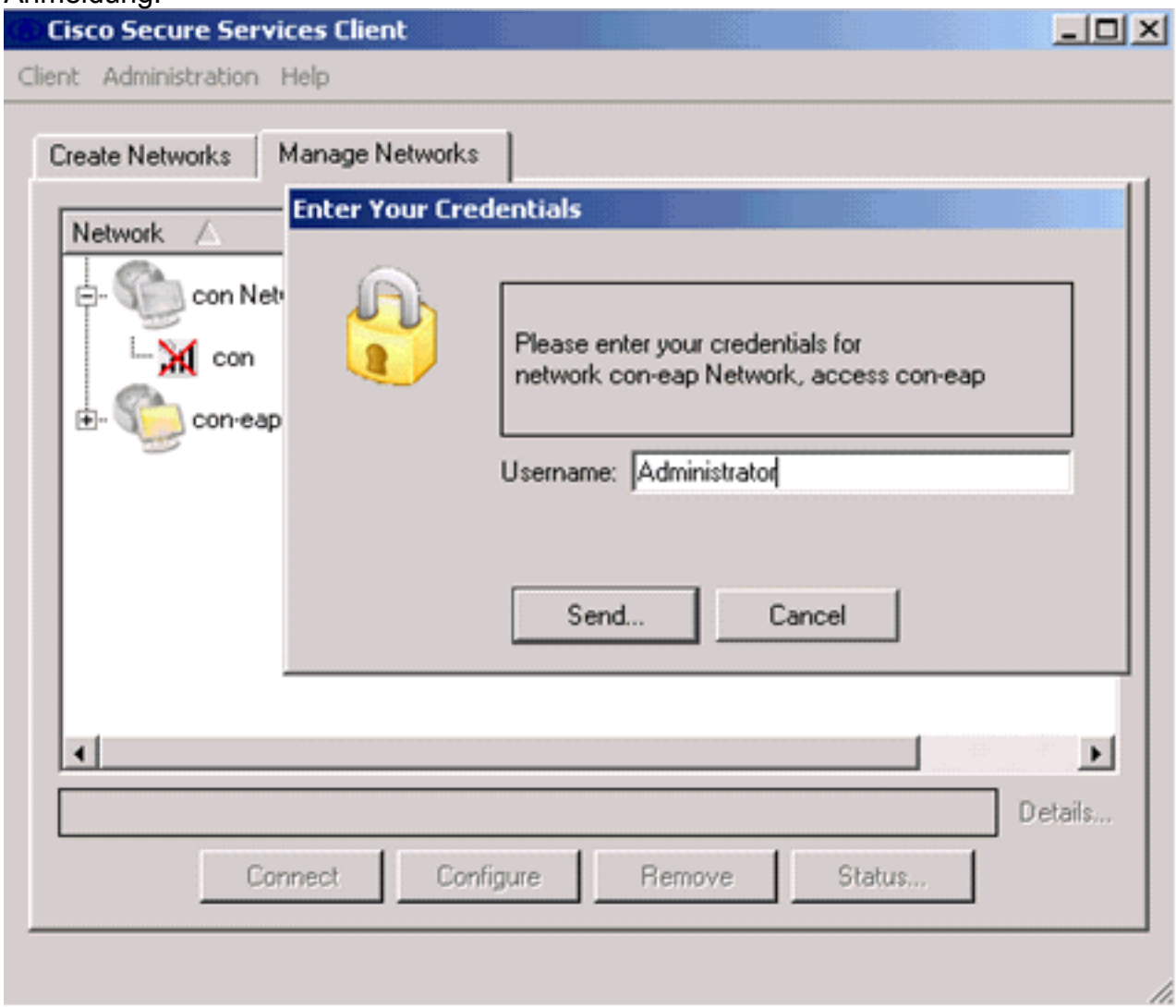
9. Geben Sie einen Namen für die Regel ein, und überprüfen Sie den Namen des

Serverzertifikats.



Die EAP-TLS-Konfiguration ist abgeschlossen.

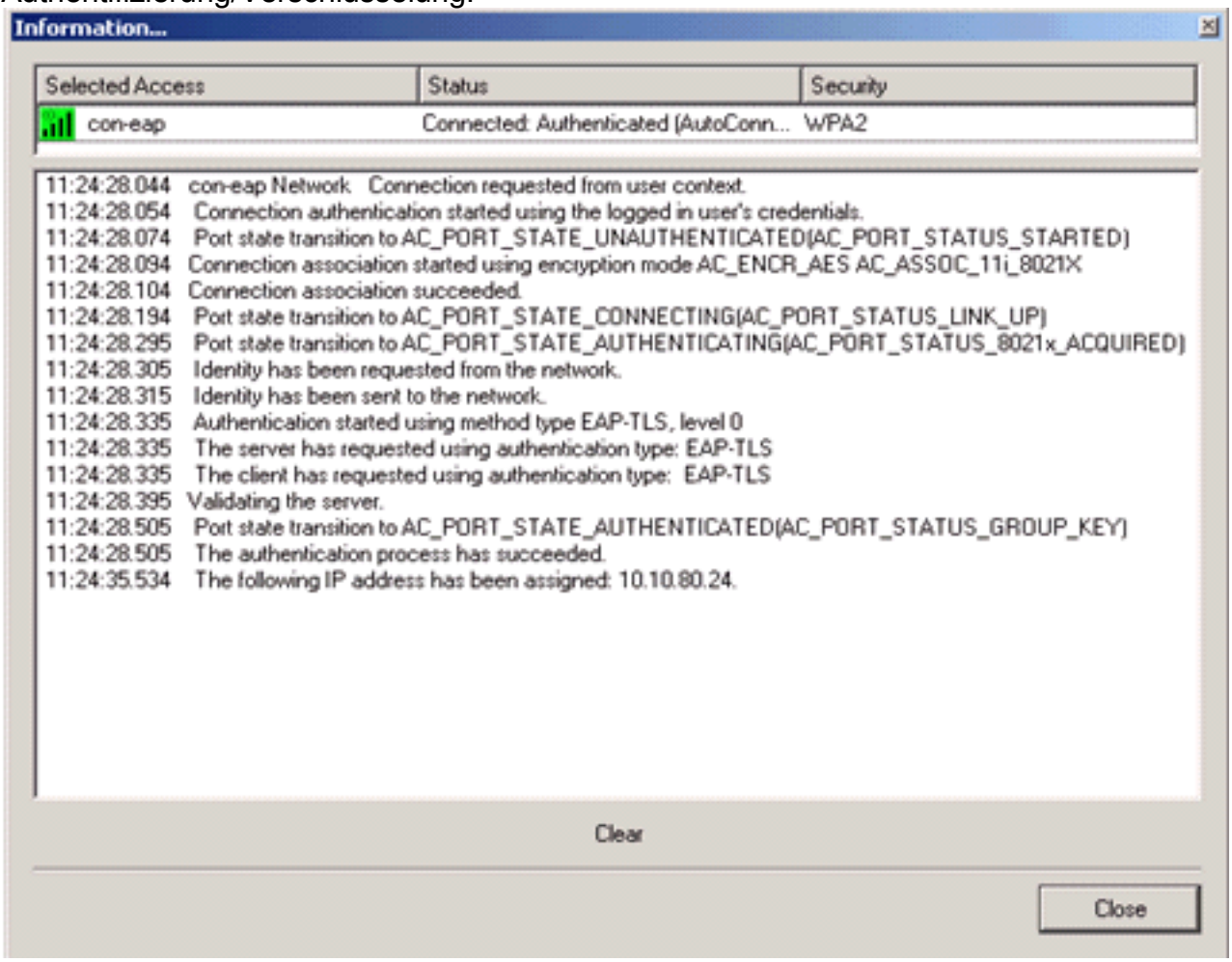
10. Stellen Sie eine Verbindung zum Wireless-Netzwerkprofil her. Der Cisco Secure Services Client bittet um
    Anmeldung:

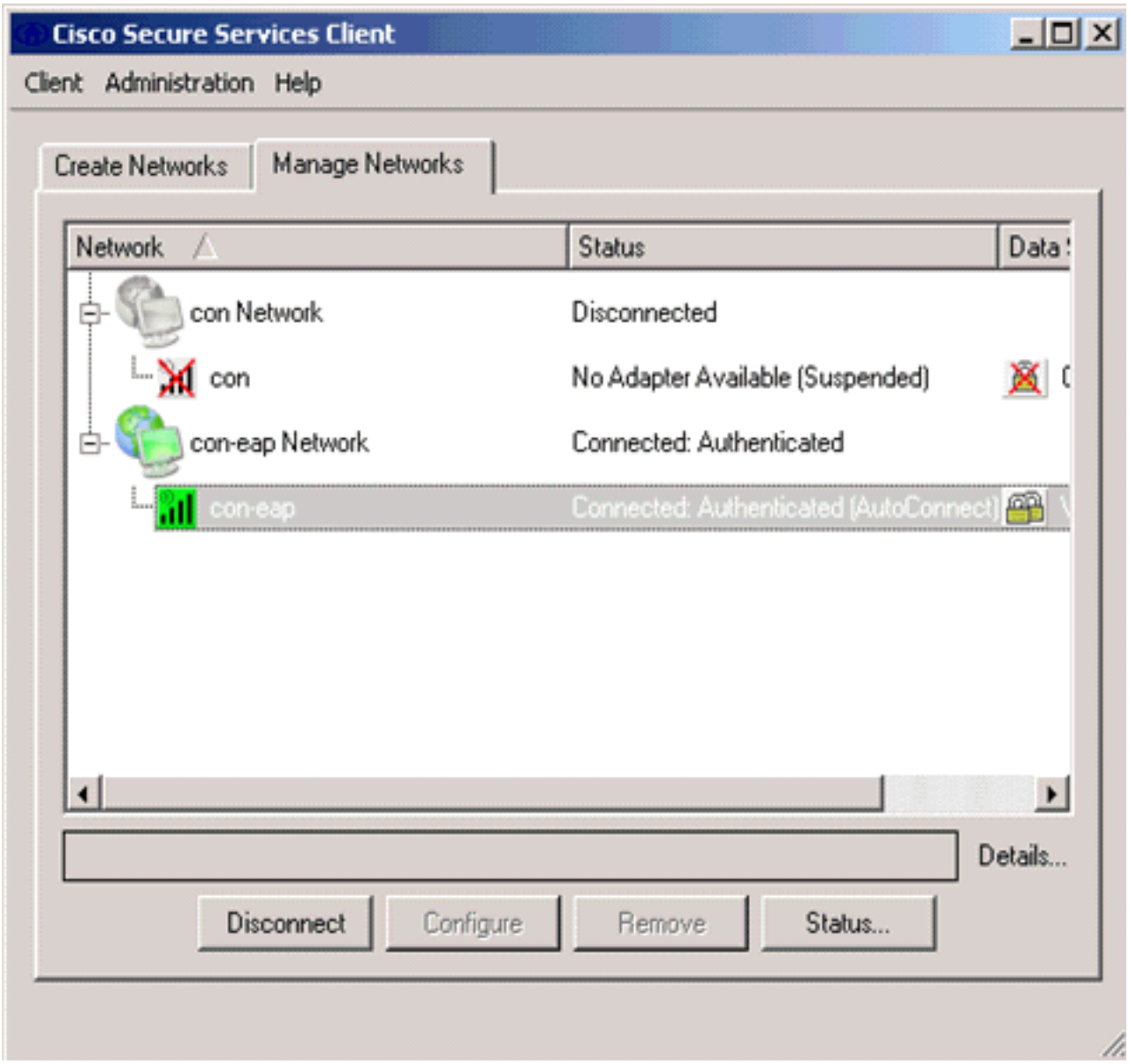


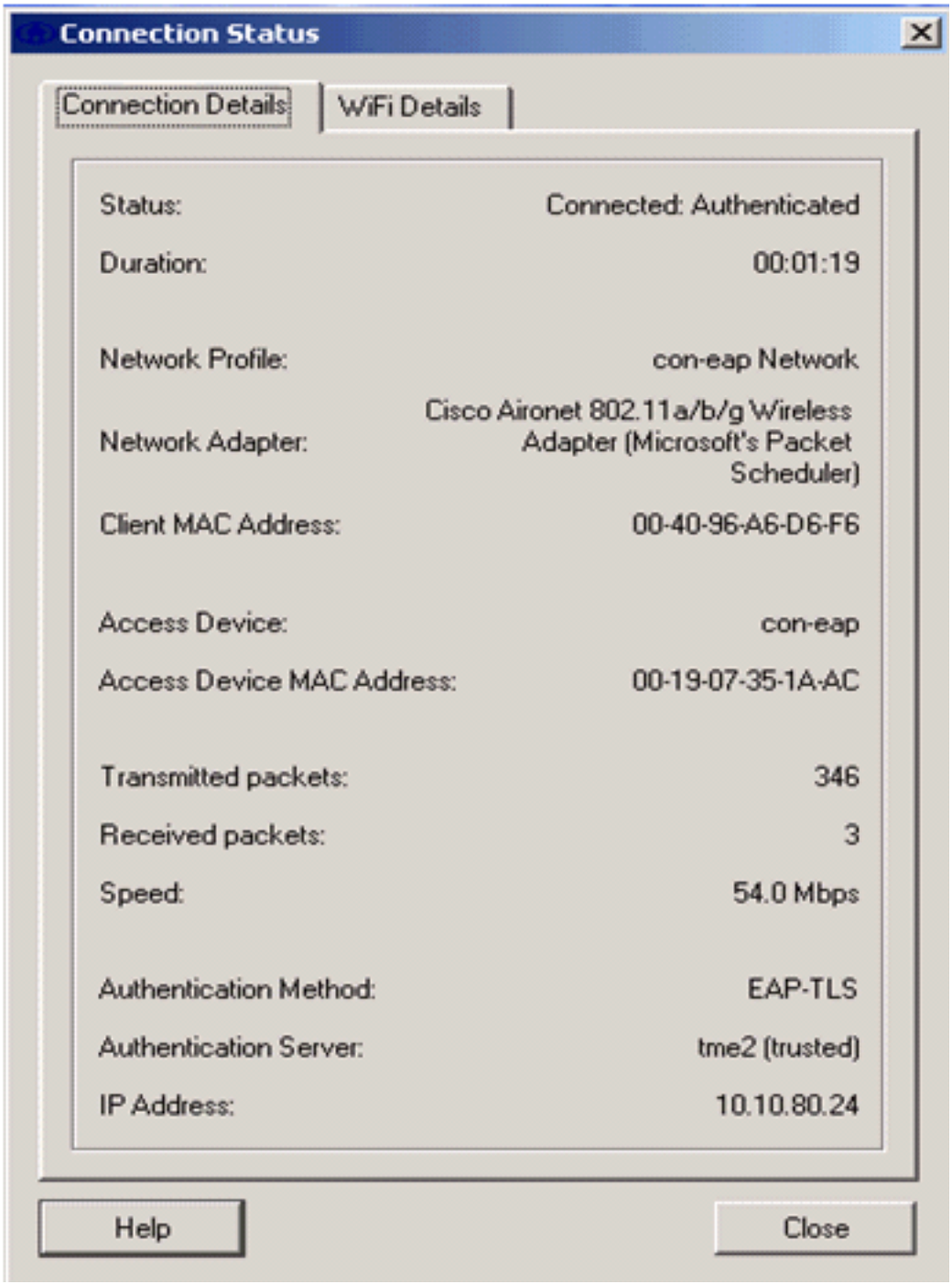
D

er Cisco Secure Services Client empfängt das Serverzertifikat und überprüft es (mit konfigurierter Regel und installierter Zertifizierungsstelle). Anschließend wird die Verwendung des Zertifikats für den Benutzer angefordert.

11. Nachdem der Client sich authentifiziert hat, wählen Sie auf der Registerkarte "Netzwerke verwalten" unter **SSID** aus, und klicken Sie auf **Status**, um Verbindungsdetails abzufragen.Das Fenster Verbindungsdetails enthält Informationen zum Client-Gerät, zum Verbindungsstatus, zu Statistiken und zur Authentifizierungsmethode. Die Registerkarte WiFi Details enthält Details zum Verbindungsstatus für 802.11, einschließlich RSSI, 802.11-Kanal sowie Authentifizierung/Verschlüsselung.




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...



Debugbefehle

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

Hinweis: Beachten Sie vor der Verwendung von **Debug-**Befehlen die Informationen zu Debug-Befehlen.

Diese Debug-Befehle können am WLC verwendet werden, um den Fortschritt des Authentifizierungsaustauschs zu überwachen:

- **debug aaa events enable**
- **debuggen aaa detail enable**
- **debug dot1x-Ereignisse aktivieren**

- debug dot1x status enable
- debuaa local-auth eap events enableODER
- debug aaa all enable

Zugehörige Informationen

- Konfigurationsleitfaden für Cisco Wireless LAN Controller, Version 4.1
- Unterstützung von WLAN-Technologie
- Technischer Support und Dokumentation für Cisco Systeme