统一无线网络本地EAP服务器配置示例

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[规则](#)
[在思科无线局域网控制器上配置本地EAP](#)
[本地EAP配置](#)
[Microsoft认证中心](#)
[安装](#)
[在思科无线局域网控制器中安装证书](#)
[在无线局域网控制器上安装设备证书](#)
[将供应商CA证书下载到无线局域网控制器](#)
[配置无线LAN控制器以使用EAP-TLS](#)
[在客户端设备上安装证书颁发机构证书](#)
[下载并安装客户端的根CA证书](#)
[为客户端设备生成客户端证书](#)
[客户端设备上思科安全服务客户端的EAP-TLS](#)
[调试命令](#)
[相关信息](#)

简介

本文档介绍在思科无线局域网控制器(WLC)中配置本地可扩展身份验证协议(EAP)服务器以对无线用户进行身份验证。

本地 EAP 是允许用户和无线客户端在本地进行身份验证的身份验证方法。它设计用于远程办公室，当后端系统中断或外部身份验证服务器关闭时，远程办公室希望保持与无线客户端的连接。启用本地EAP时，控制器充当身份验证服务器和本地用户数据库，从而消除对外部身份验证服务器的依赖。本地EAP从本地用户数据库或轻量目录访问协议(LDAP)后端数据库检索用户凭证以对用户进行身份验证。本地EAP支持控制器和无线客户端之间的轻量级EAP(LEAP)、通过安全隧道的EAP灵活身份验证(EAP-FAST)和EAP传输层安全(EAP-TLS)身份验证。

请注意，如果WLC中有全局外部RADIUS服务器配置，则本地EAP服务器不可用。所有身份验证请求都会转发到全局外部RADIUS，直到本地EAP服务器可用。如果WLC失去与外部RADIUS服务器的连接，则本地EAP服务器变为活动状态。如果没有全局RADIUS服务器配置，本地EAP服务器将立即变为活动状态。本地EAP服务器无法用于验证连接到其他WLC的客户端。换句话说，一个WLC无法将其EAP请求转发到另一个WLC进行身份验证。每个WLC都应有自己的本地EAP服务器和单个数据库。

注意：使用这些命令可阻止WLC向外部radius服务器发送请求。

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

本地EAP服务器在4.1.171.0软件版本及更高版本中支持以下协议：

- LEAP
- EAP-FAST（用户名/密码和证书）
- EAP-TLS

先决条件

要求

Cisco 建议您了解以下主题：

- 关于如何为基本操作配置 WLC 和轻量接入点 (LAP) 的知识
- 轻量级接入点协议(LWAPP)和无线安全方法知识
- 本地EAP身份验证的基本知识。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Windows XP，装有 CB21AG 适配器卡和 Cisco 安全服务客户端 4.05 版
- 思科4400无线LAN控制器4.1.171.0
- Windows 2000服务器上的Microsoft认证中心

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

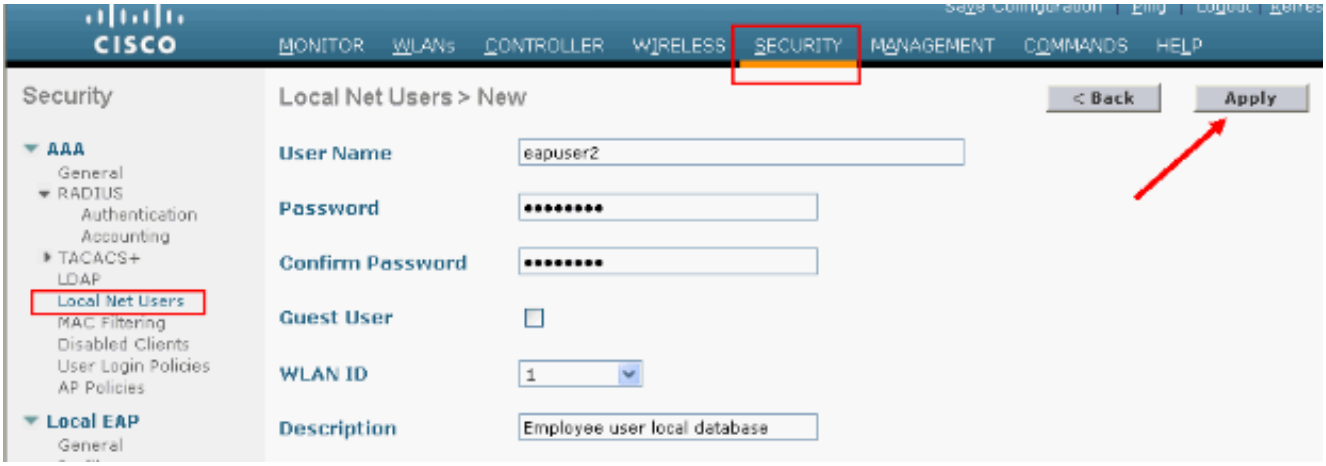
在思科无线局域网控制器上配置本地EAP

本文档假设 WLC 的基本配置已完成。

本地EAP配置

要配置本地EAP，请完成以下步骤：

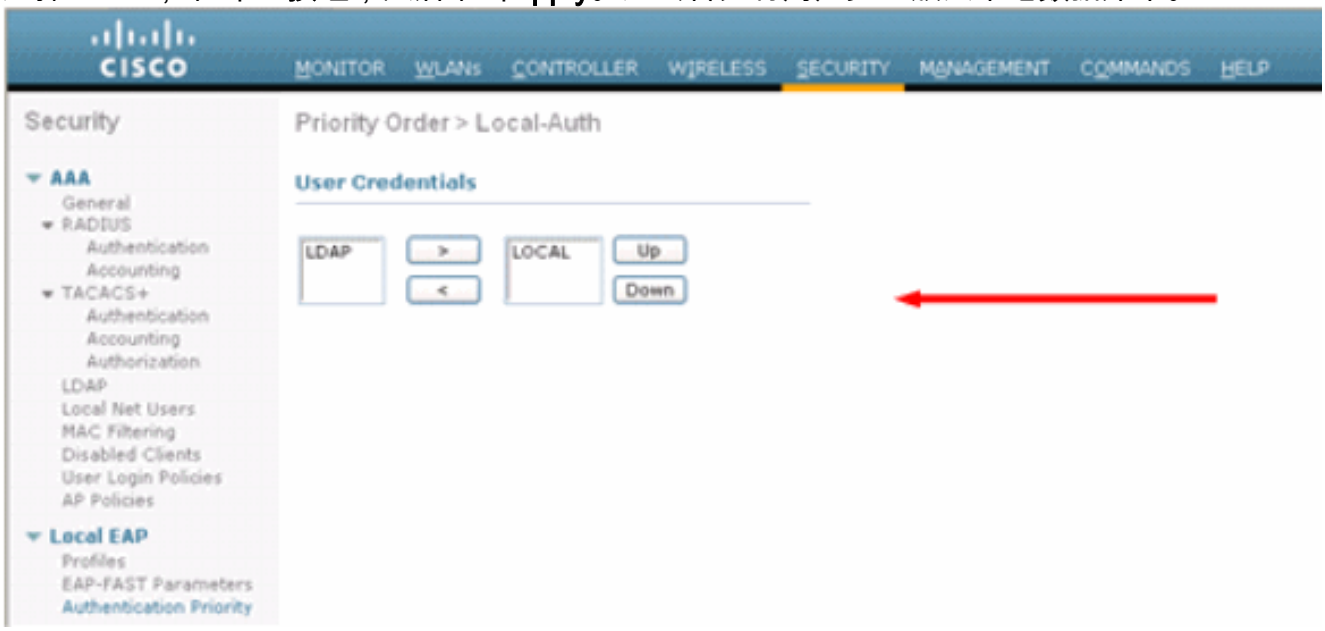
1. 添加本地网络用户：从GUI中。选择**Security > Local Net Users > New**，输入User Name、Password、Guest User、WLAN ID和Description，然后单击**Apply**。



在CLI中，您可以使用config netuser add *<username> <password> <WLAN id> <description>*命令：**注意：**由于空间原因，此命令已降级到第二行。

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

2. 指定用户凭据检索顺序。从GUI中，选择Security > Local EAP > Authentication Priority。然后选择LDAP，单击“**>**”按钮，然后单击**Apply**。这会首先将用户凭证放入本地数据库中。



从CLI:

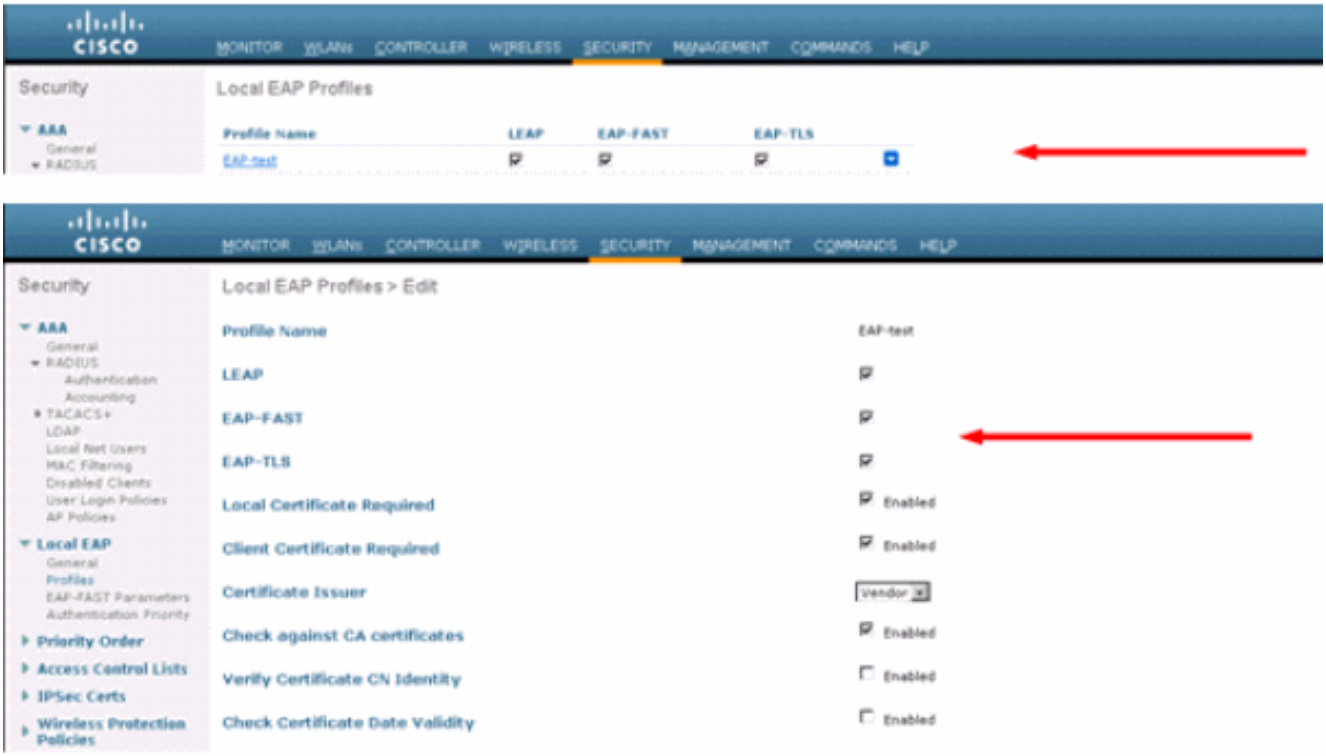
```
(Cisco Controller) >config local-auth user-credentials local
```

3. 添加EAP配置文件：要从GUI执行此操作，请选择Security > Local EAP > Profiles，**然后单击New**。当出现新窗口时，键入“配置文件名称”(Profile Name)，然后单击“**应用”(Apply)**。

您也可以使用CLI命令**config local-auth eap-profile add *<profile-name>执行此操作。*** 在我们的示例中，配置文件名*称为EAP-test*。

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

4. 向EAP配置文件添加方法。从GUI中选择**Security > Local EAP > Profiles**，然后单击要为其添加身份验证方法的配置文件名称。本示例使用LEAP、EAP-FAST和EAP-TLS。单击**Apply**以设置方法。

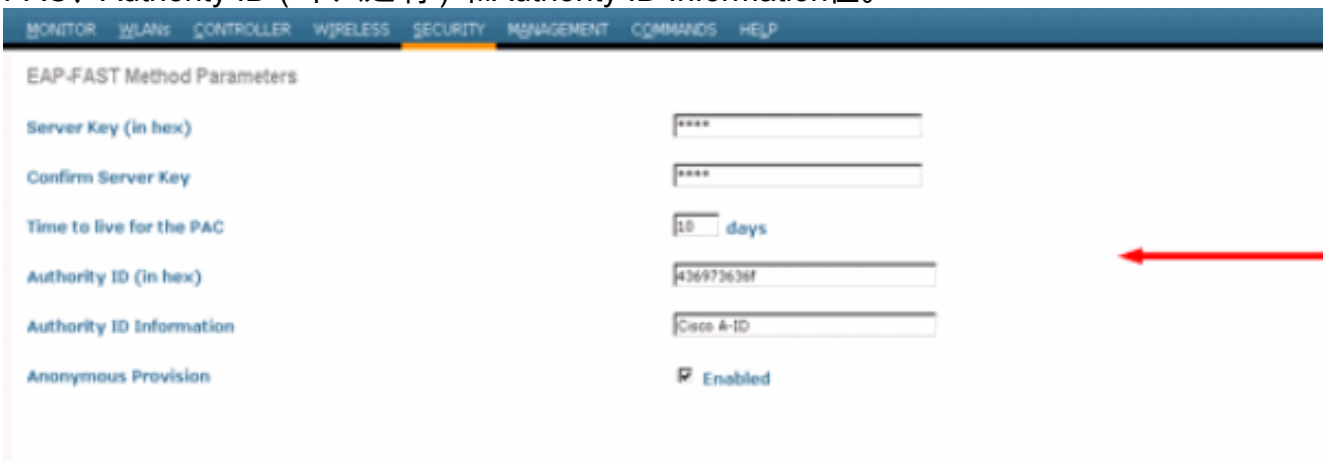


您还可以使用CLI命令**config local-auth eap-profile method add *<method-name> <profile-name>***。在示例配置中，我们向配置文件EAP测试添加三种方法。方法为LEAP、EAP-FAST和EAP-TLS，其方法名称分*别为leap*、*fast*和*tls*。此输出显示CLI配置命令：

```
(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. 配置EAP方法的参数。这仅用于EAP-FAST。要配置的参数包括：**Server Key(server-key)** —

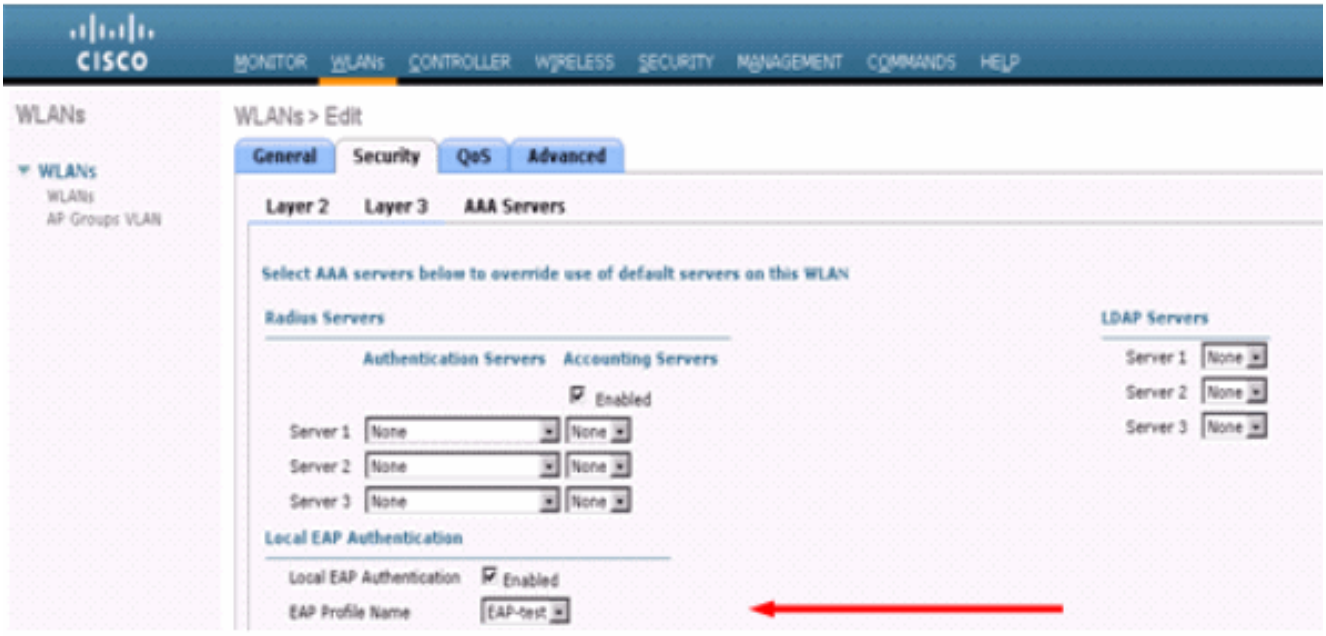
用于加密/解密受保护访问凭证(PAC)（十六进制）的服务器密钥。**PAC的生存时间(pac-ttl)** — 设置PAC的生存时间。**授权ID（授权ID）** — 设置授权标识符。**匿名调配（匿名调配）** — 配置是否允许匿名调配。默认情况下启用该接口。对于通过GUI进行的配置，请选择**Security > Local EAP > EAP-FAST Parameters**，然后输入PAC的Server key、Time to live for the PAC、Authority ID（十六进制）和Authority ID Information值。



以下是用于为EAP-FAST设置这些参数的CLI配置命令：

```
(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
```

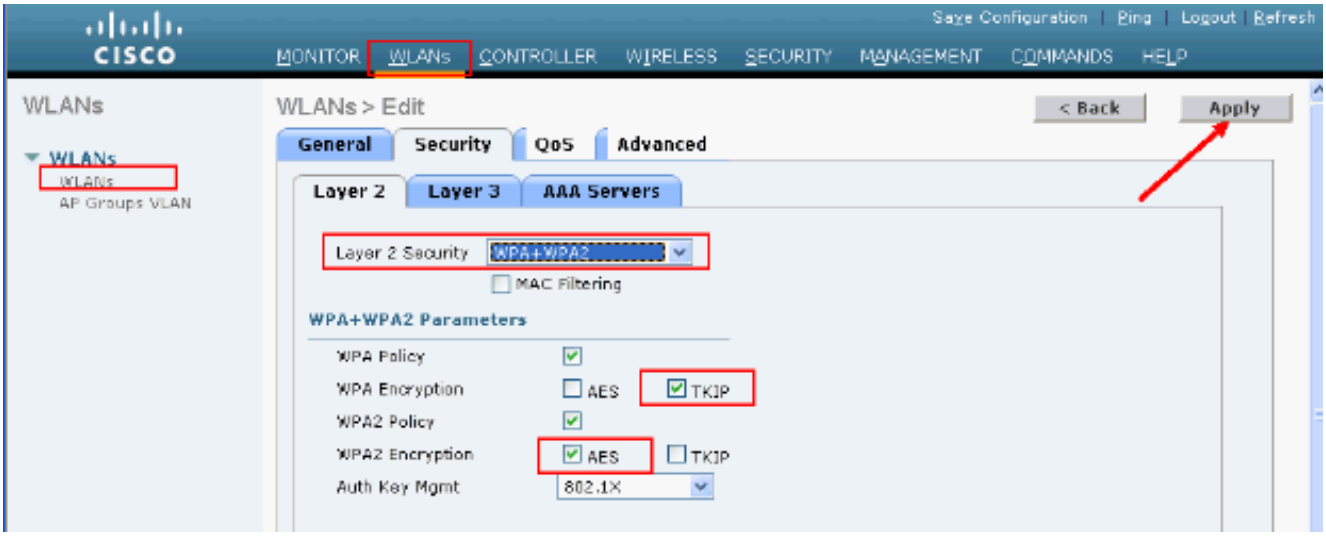
6. 启用每个WLAN的本地身份验证：从GUI中，在顶**部**菜单上选择WLAN，然后选择要为其配置本地身份验证的WLAN。系统将显示新窗口。单击“安**全”>“AAA”**选项卡。选**中Local EAP Authentication**，然后从下拉菜单中选择正确的EAP Profile Name，如以下示例所示：



您还可以发出CLI config **wlan local-auth enable *<profile-name> <wlan-id>*配**置命令，如下所示：

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

7. 设置第2层安全参数。在GUI界面中，在“WLAN编辑”窗口中转到“安全”**>“第2层”**选项卡，并从**“第2层**安全”下拉菜单中选择**WPA+WPA2。**在“WPA+WPA2参数”部分下，将WPA加密设置为**TKIP**和WPA2加密**AES**。然后单击 Apply。**



在CLI中，使用以下命令：

```
(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. 检查配置:

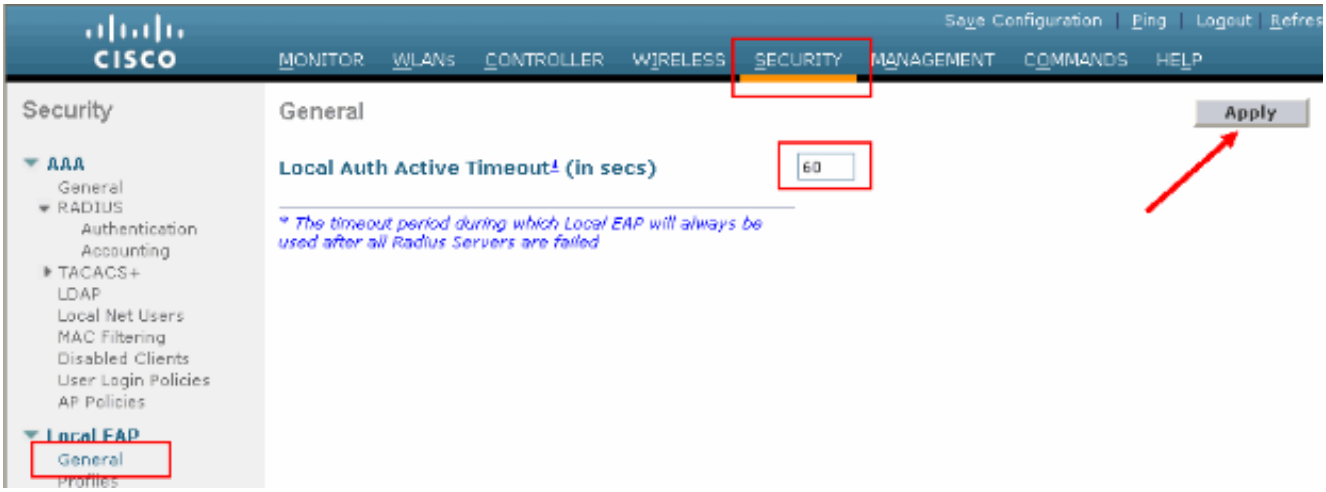
```
(Cisco Controller) >show local-auth config

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
```

使用show wlan <wlan id>命令可以看到wlan 1*的特定*参数：

```
(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
```

还可以配置其他本地身份验证参数，特别是活动超时计时器。此计时器配置在所有RADIUS服务器发生故障后使用本地EAP的时间段。从GUI中，选择**Security > Local EAP > General**并设置时间值。然后单击 **Apply**。



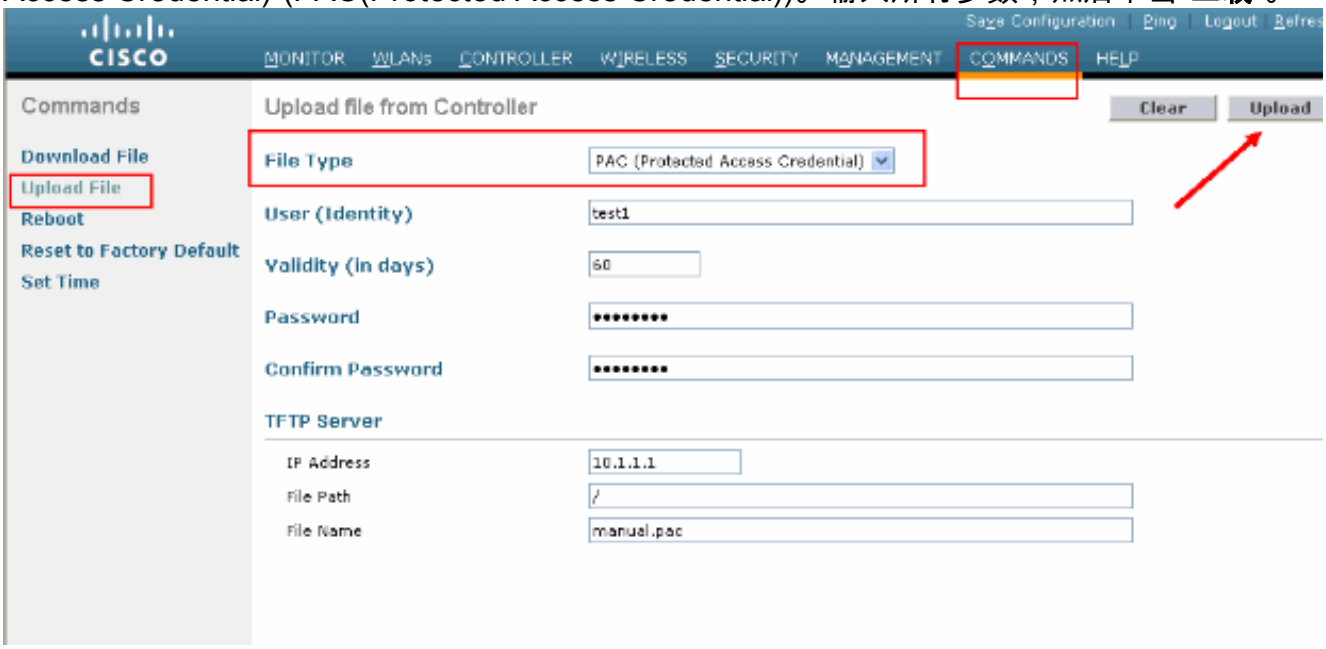
从CLI发出以下命令：

```
(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
```

当您发出show local-auth config命令时，可以验证此计时器设置到的值。

```
(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. 如果需要生成并加载手动PAC，可以使用GUI或CLI。从GUI中，从顶部菜单中选择“命令”，然后从右侧列表中选择“上传文件”。从“文件类型”(File Type)下拉菜单中选择“PAC(Protected Access Credential)”(PAC(Protected Access Credential))。输入所有参数，然后单击“上载”。



在CLI中输入以下命令：

```
(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认证中心

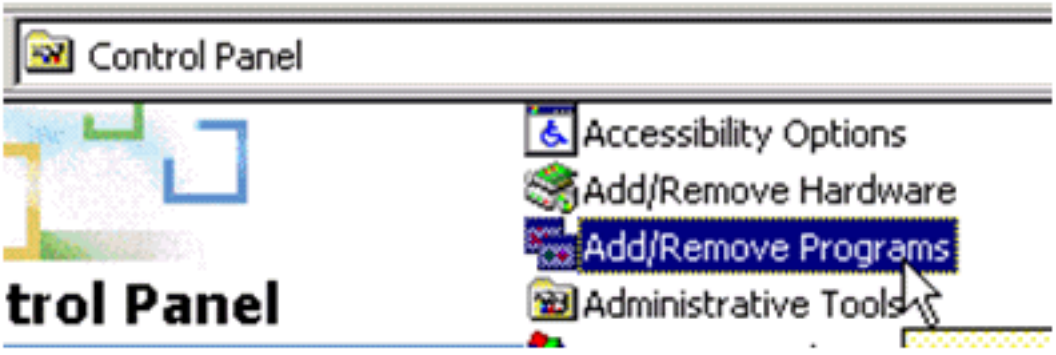
要使用EAP-FAST第2版和EAP-TLS身份验证，WLC和所有客户端设备必须具有有效的证书，并且还必须知道证书颁发机构的公共证书。

安装

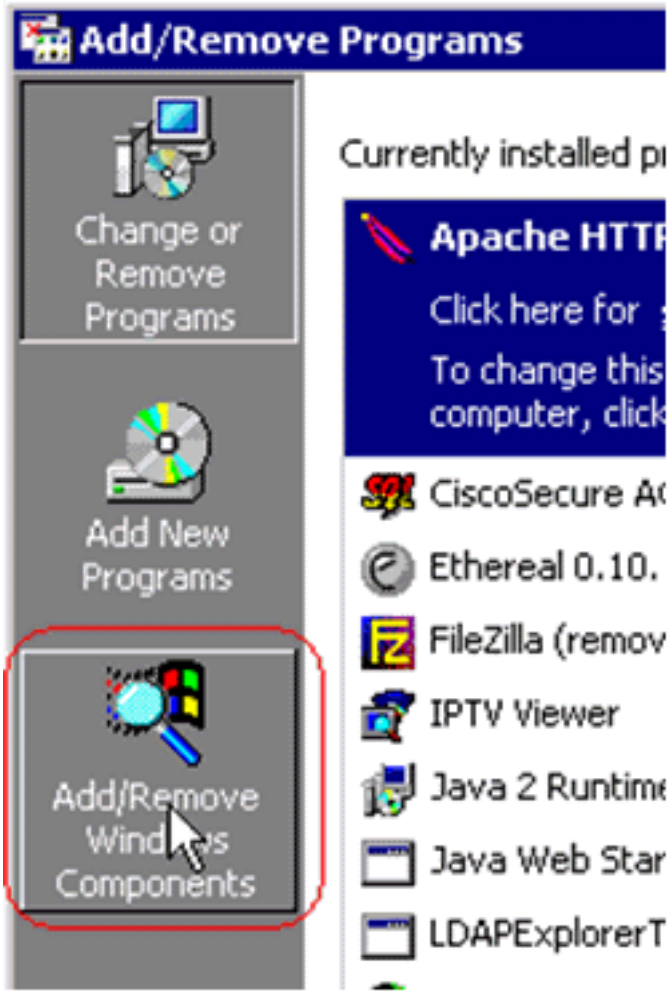
如果Windows 2000 Server尚未安装证书颁发机构服务，则需要安装它。

要在Windows 2000 Server上激活Microsoft证书颁发机构，请完成以下步骤：

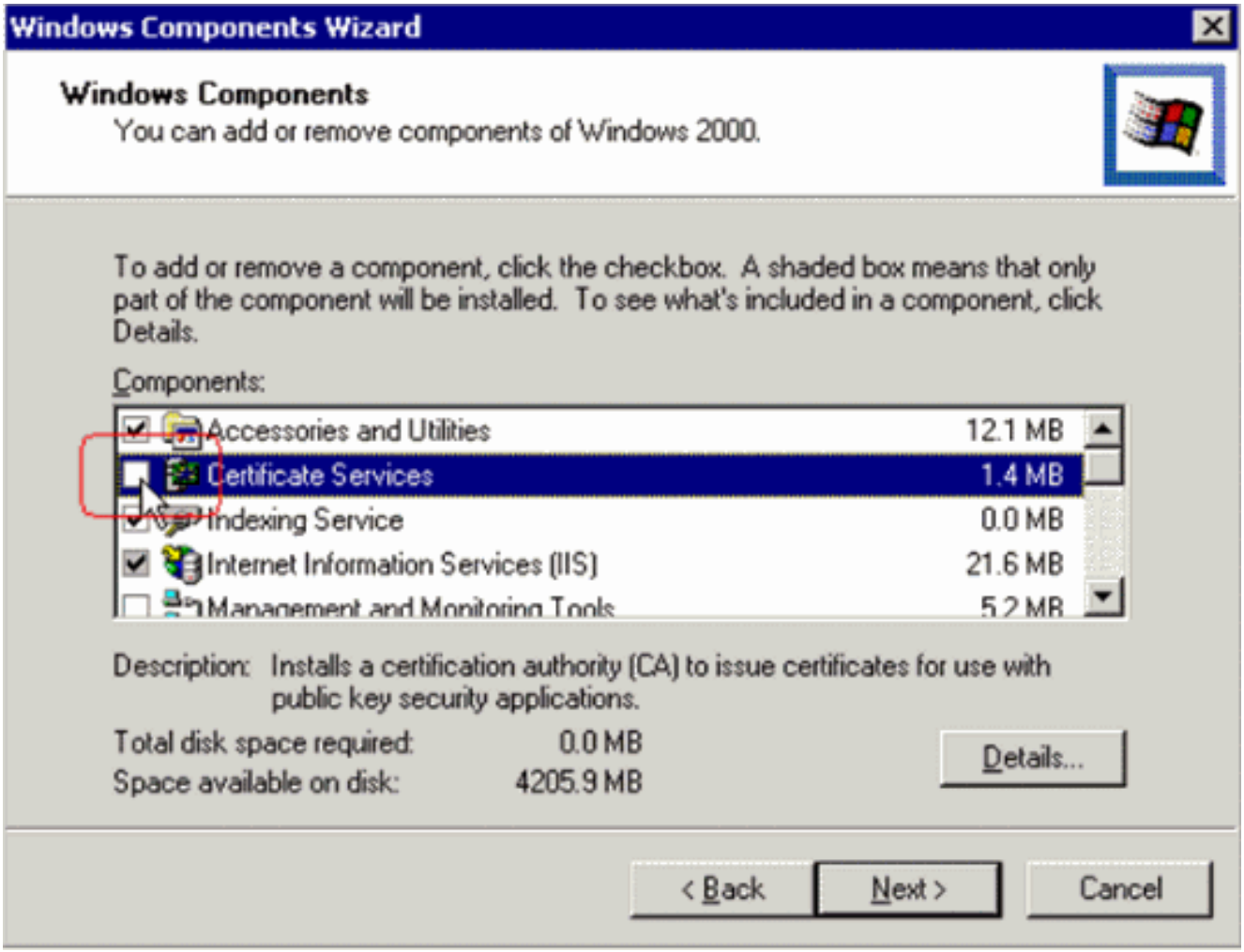
1. 从“控制面板”中，选择“**添加/删除程序**”。



:

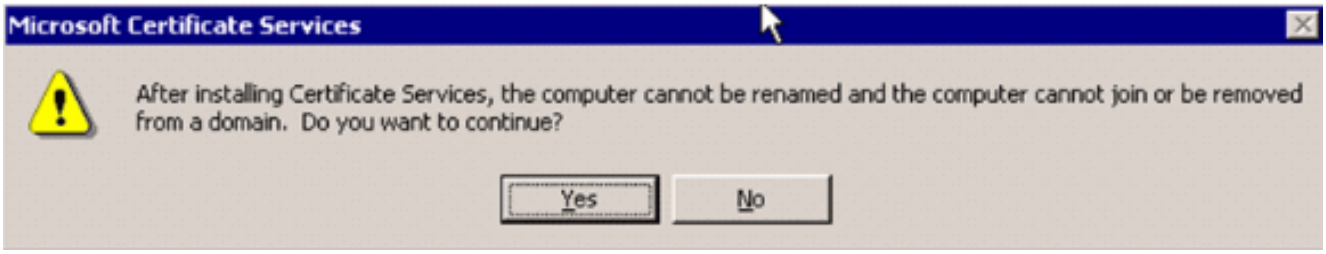


2. 在左**侧选择添加/删**除Windows组件。
3. 检查**证书服务**。

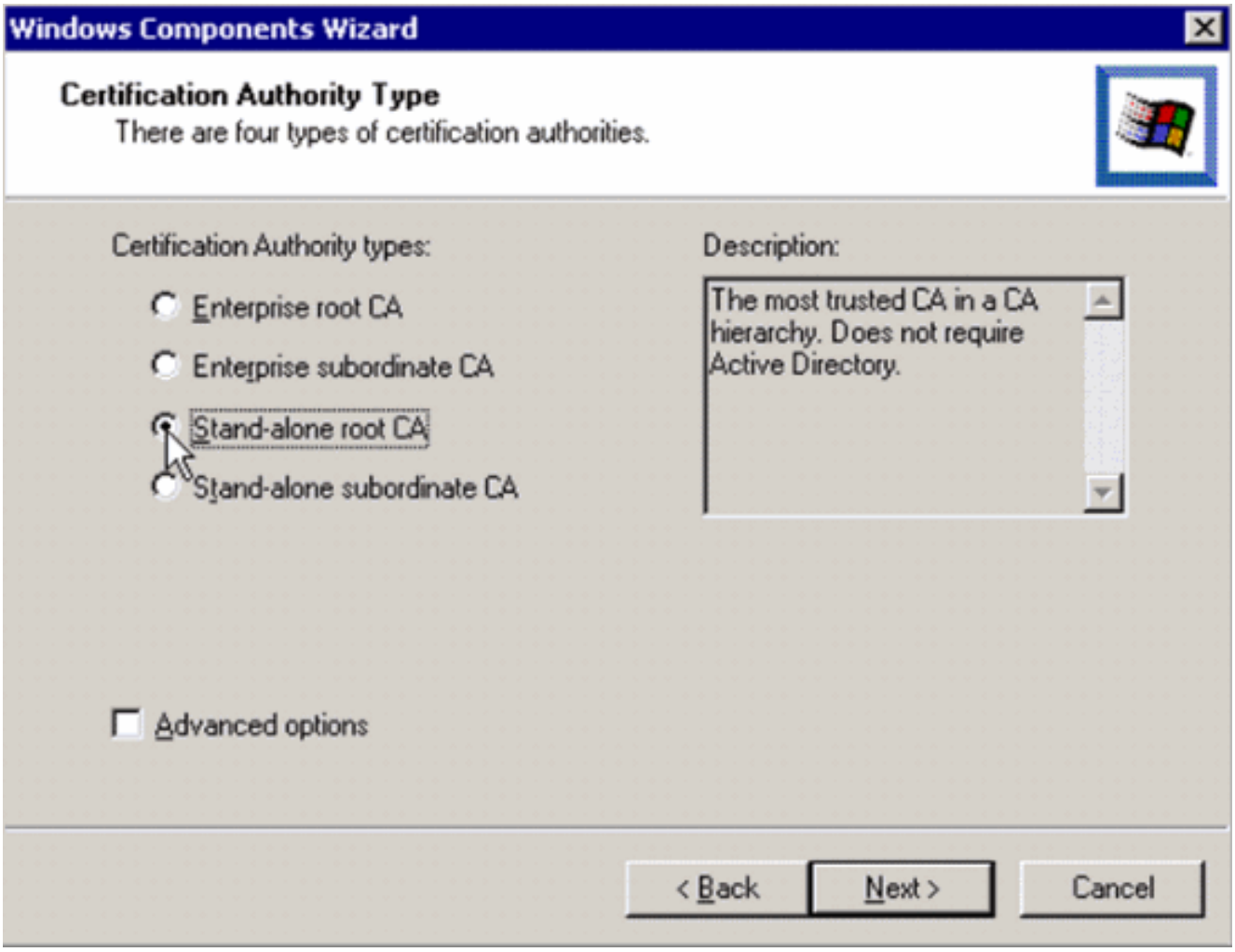


在继续之前，请查看此警告

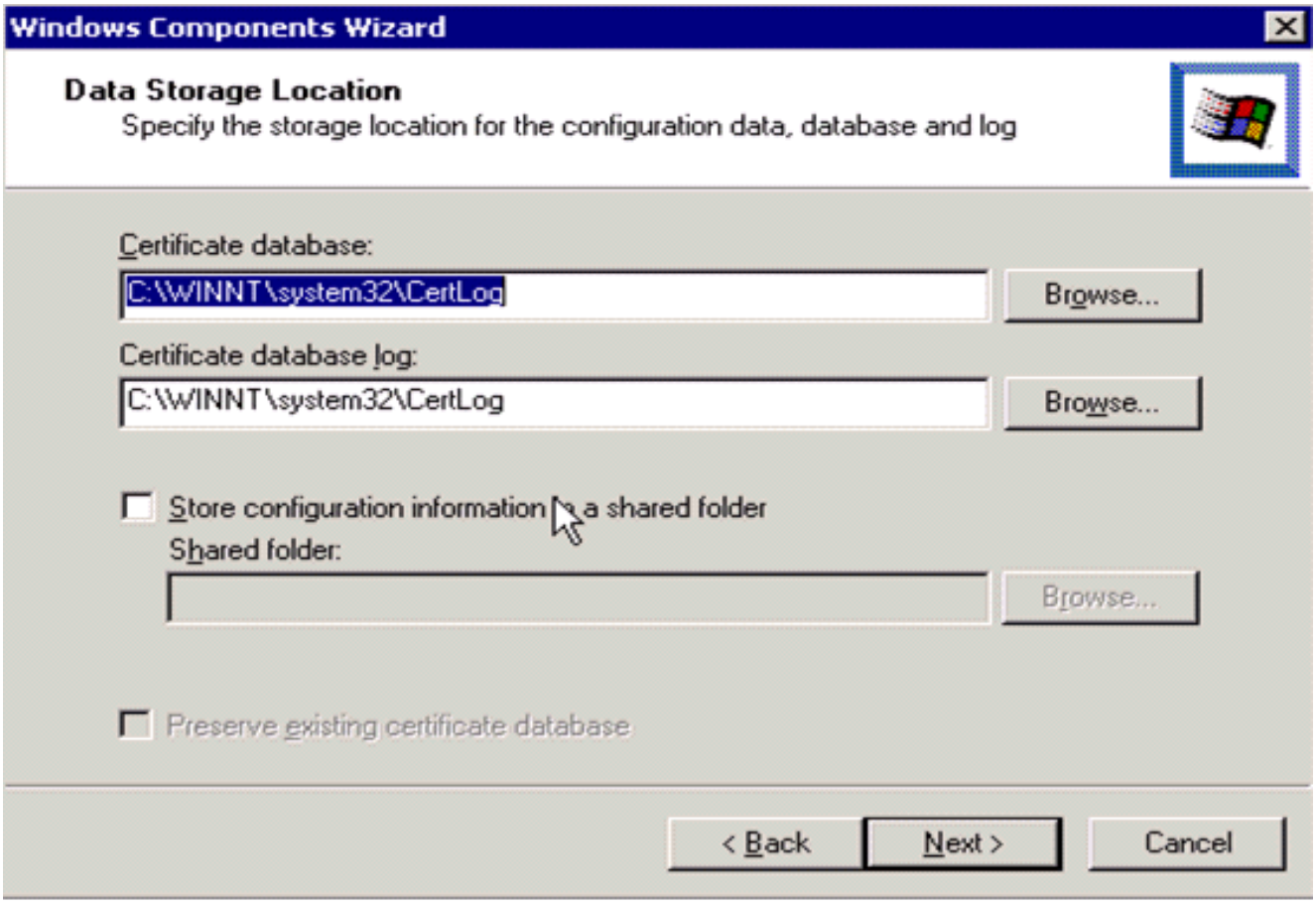
：



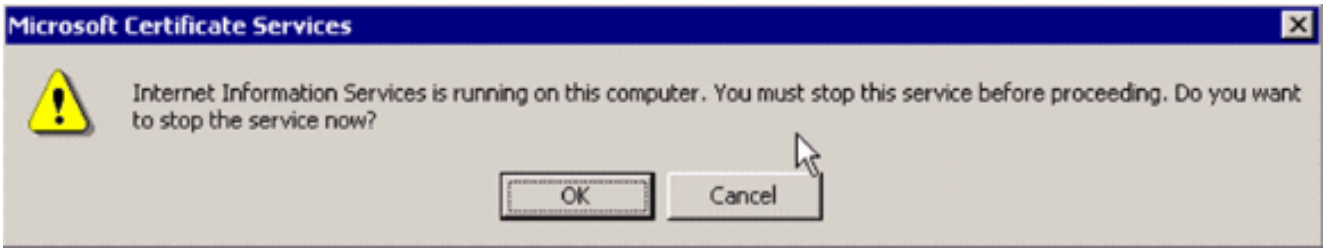
4. 选择要安装的证书颁发机构类型。要创建简单的独立机构，请选择Stand-alone root CA。



5. 输入有关认证中心的必要信息。此信息为您的证书颁发机构创建自签名证书。记住您使用的CA名称。证书颁发机构将证书存储在数据库中。本示例使用Microsoft建议的默认设置：



6. Microsoft证书颁发机构服务使用IIS Microsoft Web Server来创建和管理客户端和服务器证书。它需要为此重新启动IIS服务
：



Microsoft Windows 2000 Server现在安装新服务。您需要有Windows 2000 Server安装光盘才能安装新的Windows组件。现在已安装证书颁发机构。

在思科无线局域网控制器中安装证书

要在思科无线局域网控制器的本地EAP服务器上使用EAP-FAST第2版和EAP-TLS，请执行以下步骤：

1. 在无线LAN控制器上安装设备证书。
2. 将供应商CA证书下载到无线局域网控制器。
3. 将无线LAN控制器配置为使用EAP-TLS。

请注意，在本文档所示的示例中，访问控制服务器(ACS)与Microsoft Active Directory和Microsoft证书颁发机构安装在同一台主机上，但如果ACS服务器位于其他服务器上，则配置应相同。

在无线局域网控制器上安装设备证书

请完成以下步骤：

1. 。要生成要导入到WLC的证书，请完成以下步骤：转到**http://<serverIpAddr>/certsrv**。选择**申请一个证书，然后单击"下一步"。**选择**高级请求并单击"下一步"。**选择**使用表单向此 CA 提交证书请求并单击"下一步"。**为Certificate Template(**证书模**板)选择Web服务器并输入相关信息。然后将密钥标记为可**导出**。现在，您将收到需要在计算机中安装的证书。
2. 要从PC检索证书，请完成以下步骤：打开Internet Explorer浏览器，然后选择"**工具**"**>"Internet选项">"内容"。**单击**Certificates**。从下拉菜单中选择新安装的证书。单击**Export**。单击**Next**两次，然后选**择Yes export the private key**。此格式为PKCS#12（.PFX格式）。选择**启用强保护**。键入密码。将其保存到文件<tme2.pfx>中。
3. 将PKCS#12格式的证书复制到安装了Openssl的任何计算机，以将其转换为PEM格式。

```
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. 将转换的PEM格式设备证书下载到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. 重新启动后，检查证书。

```
(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
```

将供应商CA证书下载到无线局域网控制器

请完成以下步骤：

1. 要检索供应商CA证书，请完成以下步骤：转到**http://<serverIpAddr>/certsrv**。选择**Retrieve the CA Certificate(检索CA证书)**，然后单击**Next**。选择CA证书。单击**DER encoded**。单击“**Download CA certificate(下载CA证书)**”，将证书保存为**rootca.cer**。
2. 使用**openssl x509 -in rootca.cer -inform DER -out rootca.pem -outform PEM命令将供应商CA从DER格式转换为PEM格式。**输出文件为PEM格式的rootca.pem。
3. 下载供应商CA证书：

```
(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
```

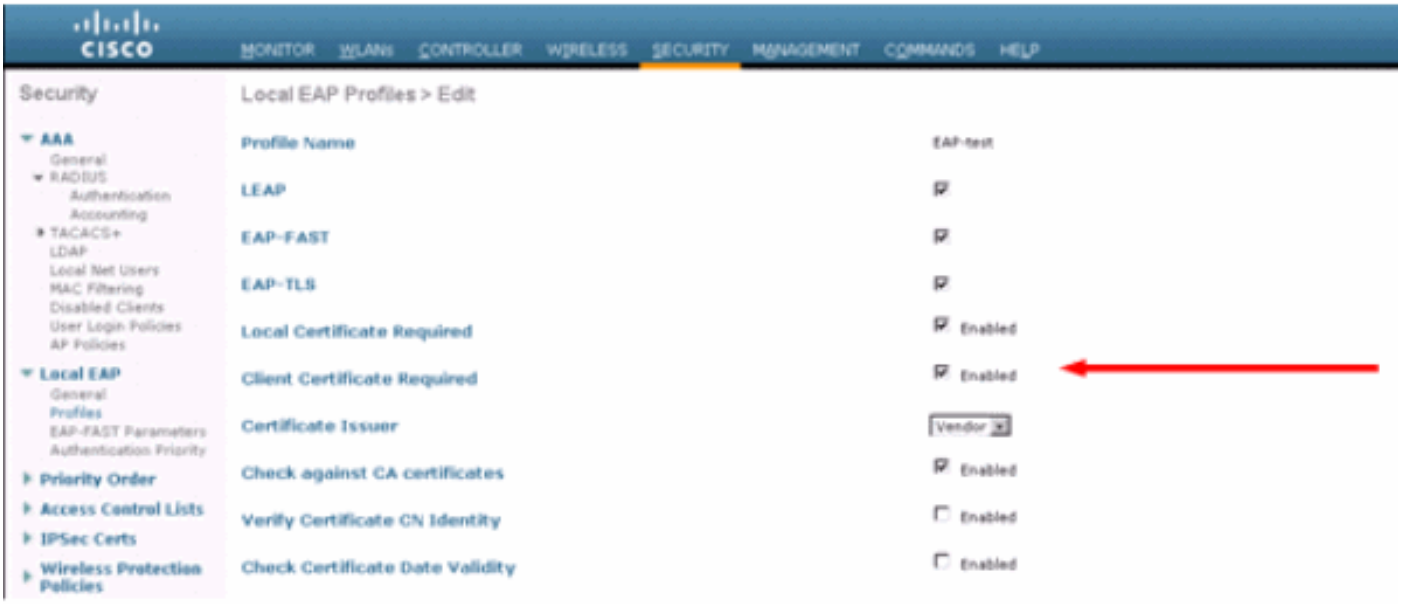
```
TFTP EAP CA cert transfer starting.

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

配置无线LAN控制器以使用EAP-TLS

请完成以下步骤：

在GUI中，选择**Security > Local EAP > Profiles**，选择配置文件并检查以下设置：

- 已启用“需要本地证书”。
- 已启用“需要客户端证书”。
- 证书颁发者为供应商。
- 已启用针对CA证书的检查。



在客户端设备上安装证书颁发机构证书

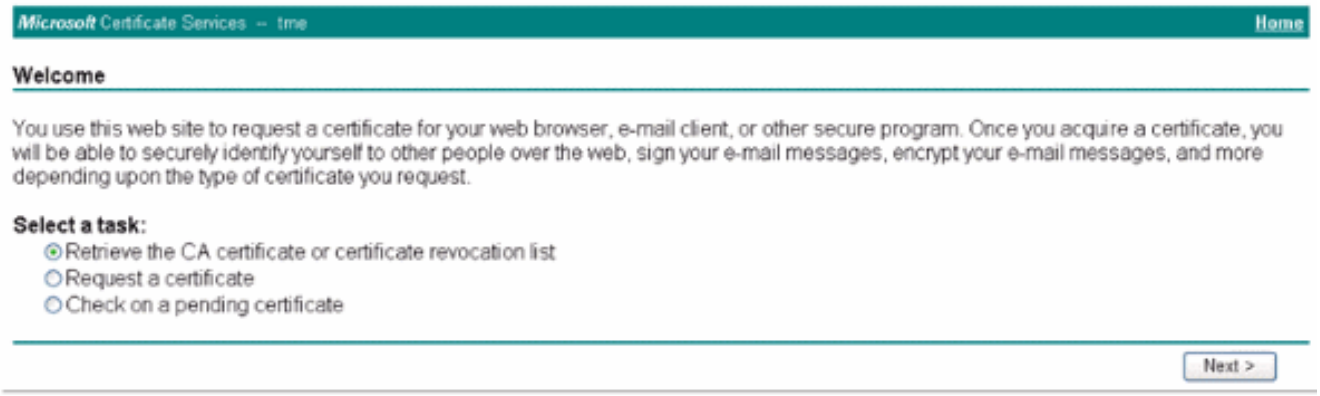
下载并安装客户端的根CA证书

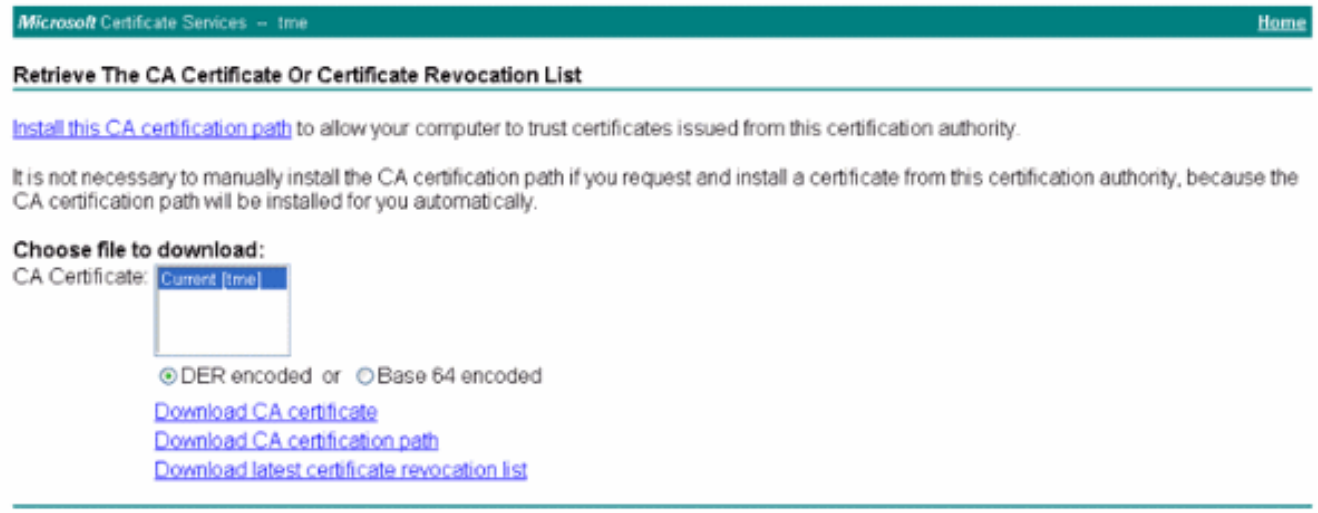
客户端必须从证书颁发机构服务器获取根CA证书。您可以使用多种方法获取客户端证书并将其安装在Windows XP计算机上。要获取有效证书，Windows XP用户必须使用其用户ID登录，并且必须具有网络连接。

Windows XP客户端上的Web浏览器和网络的有线连接用于从专用根证书颁发机构服务器获取客户端证书。此过程用于从Microsoft证书颁发机构服务器获取客户端证书：

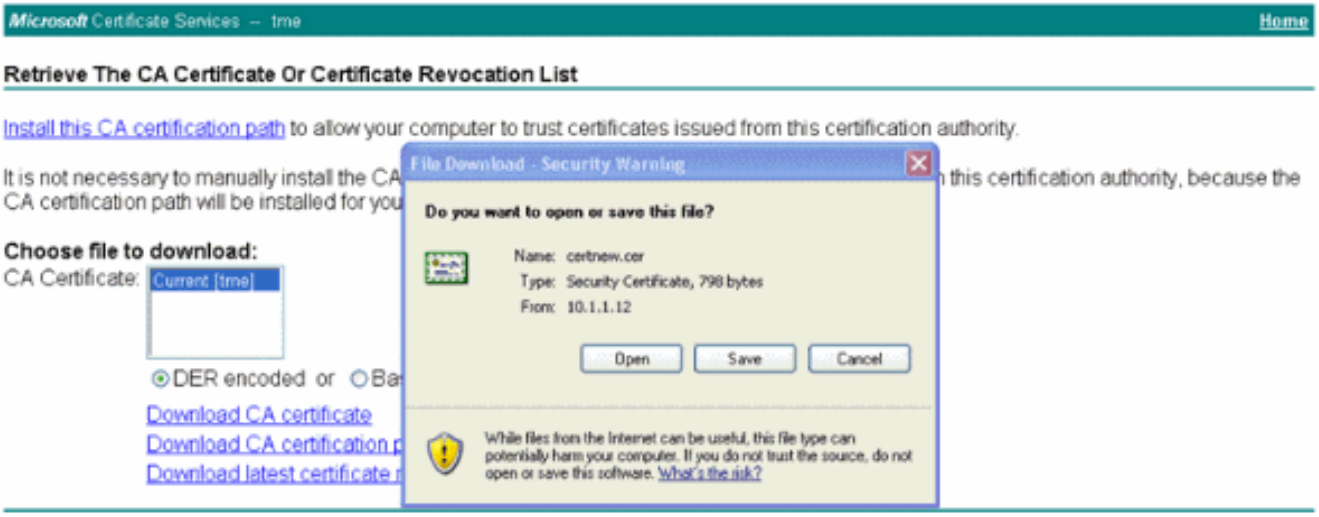
1. 在客户端上使用Web浏览器，并将浏览器指向证书颁发机构服务器。为此，请输入**http://IP-address-of-Root-CA/certsrv**。
2. 使用域**名\用户名登录**。您必须使用要使用XP客户端的个人的用户名登录。
3. 在“欢迎”窗口中，选择**检索CA证书，然**后单击**下一步**。
4. 选择**Base64 Encoding**和**Download CA certificate**。
5. 在“Certificate Issued（颁发的证书）”窗口中，单**击“Install this certificate(安装此证**书)”，然**后单击“Next(下**一步)”。

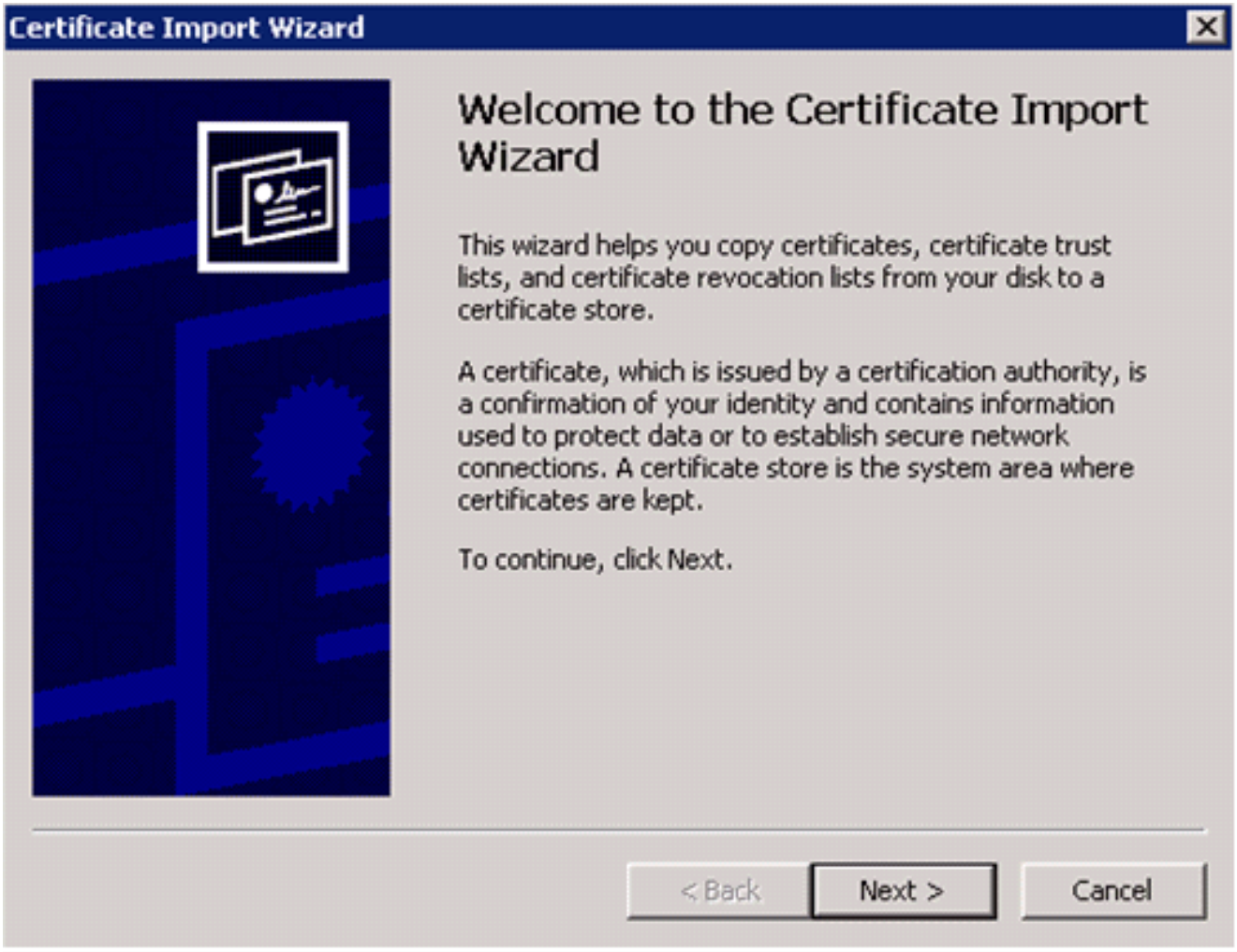
6. 选择**自动选择证书存储**，然后单击**下一步**，以获得成功的导入消息。
7. 连接到证书颁发机构以检索证书颁发机构证书
:

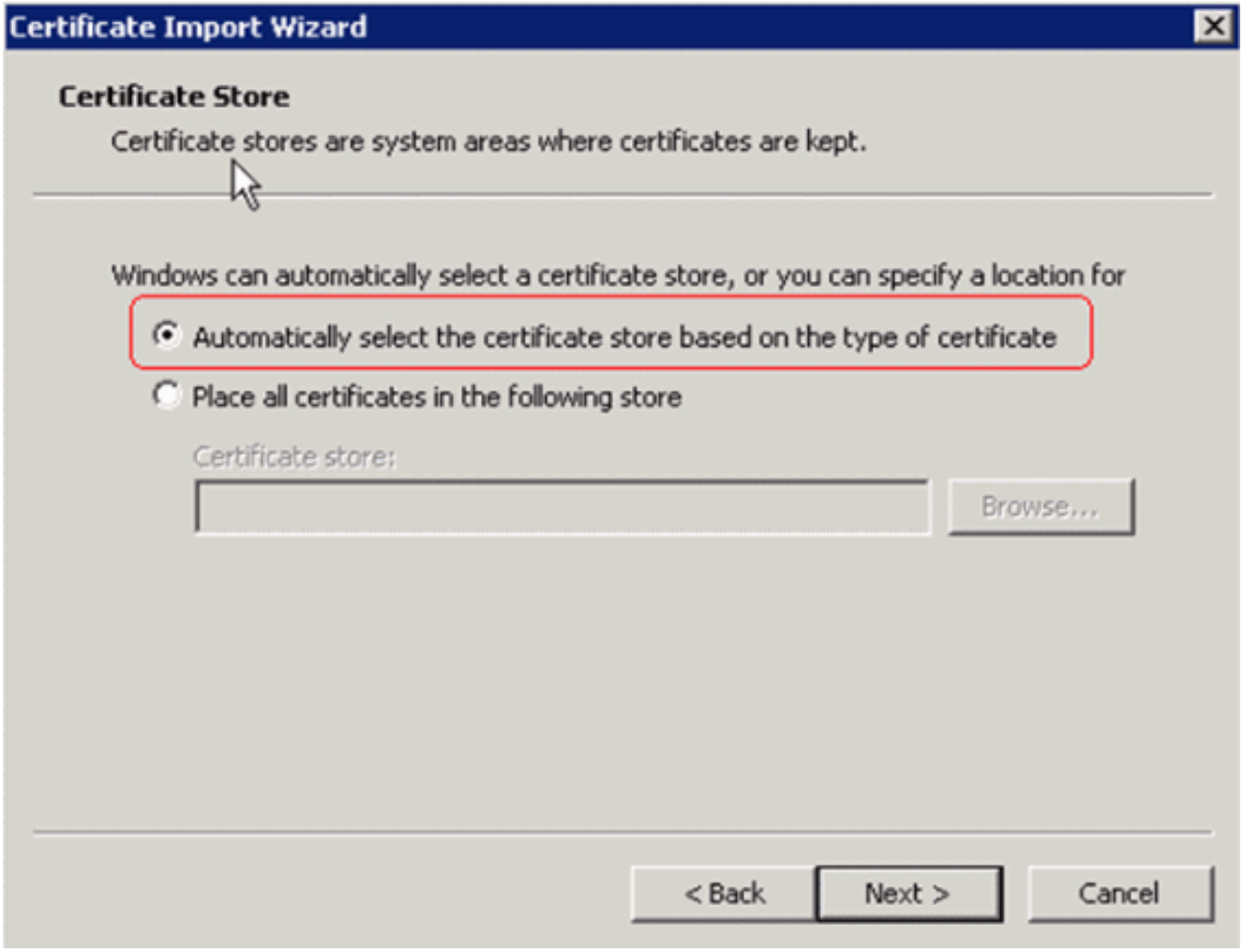




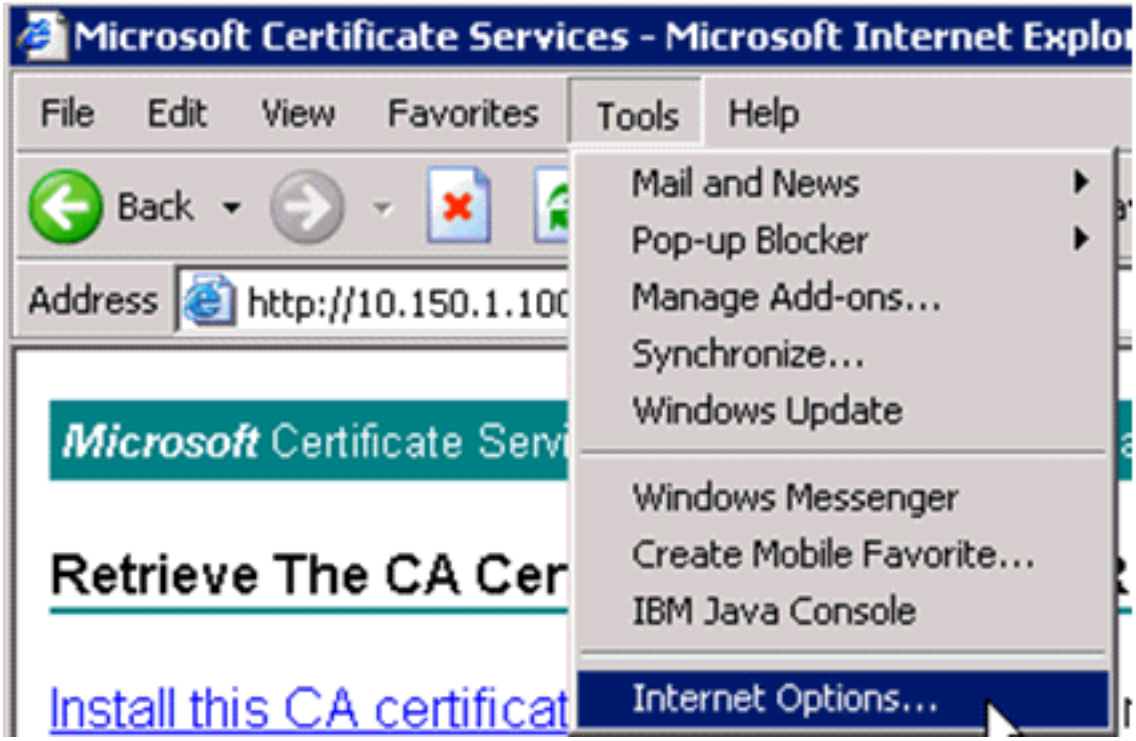
8. 单击**下载 CA 证书**。

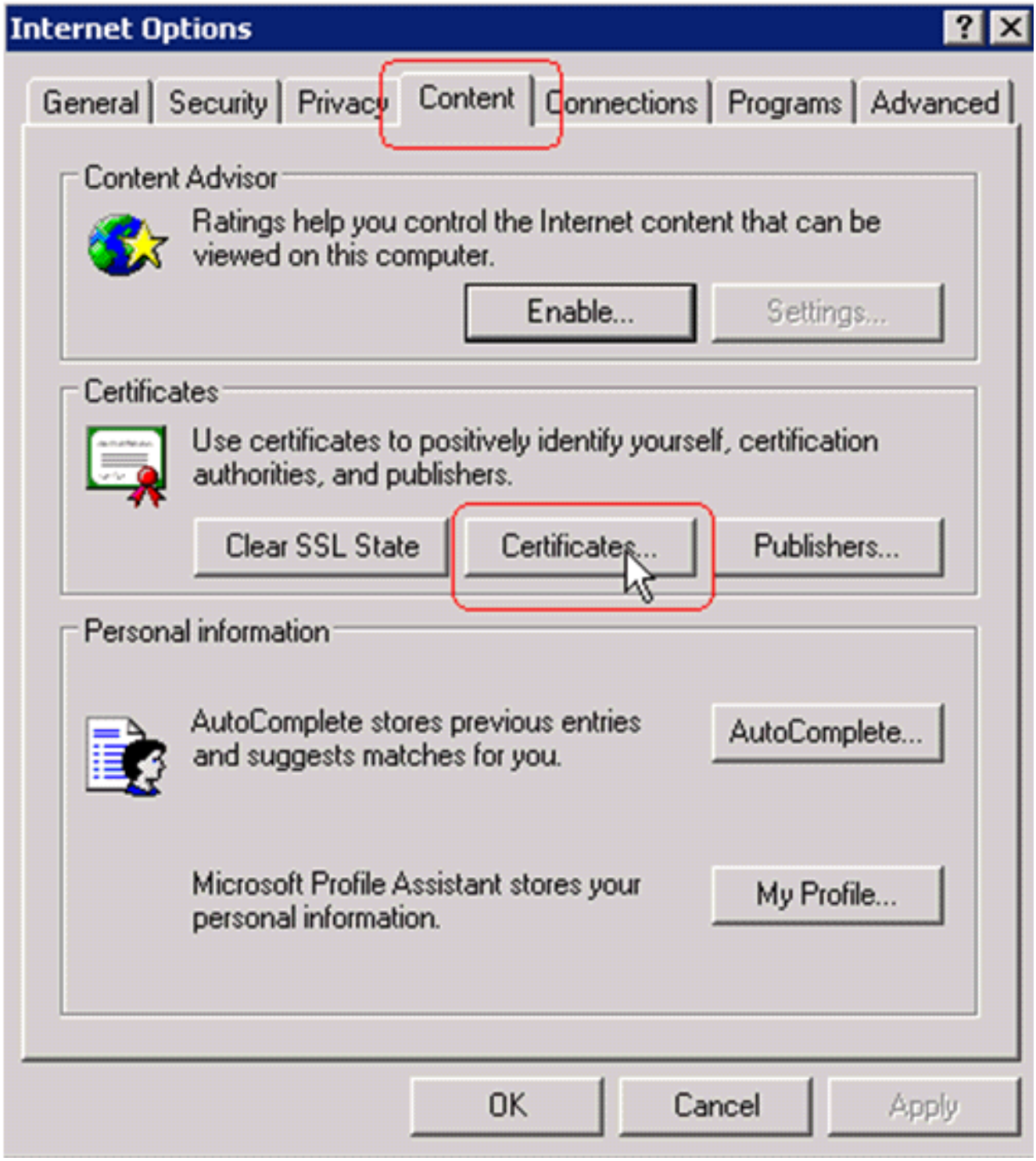



Certificate Import Wizard
Welcome to the Certificate Import Wizard
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
A certificate, which is issued by a certification authority, is a confirmation of your identity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

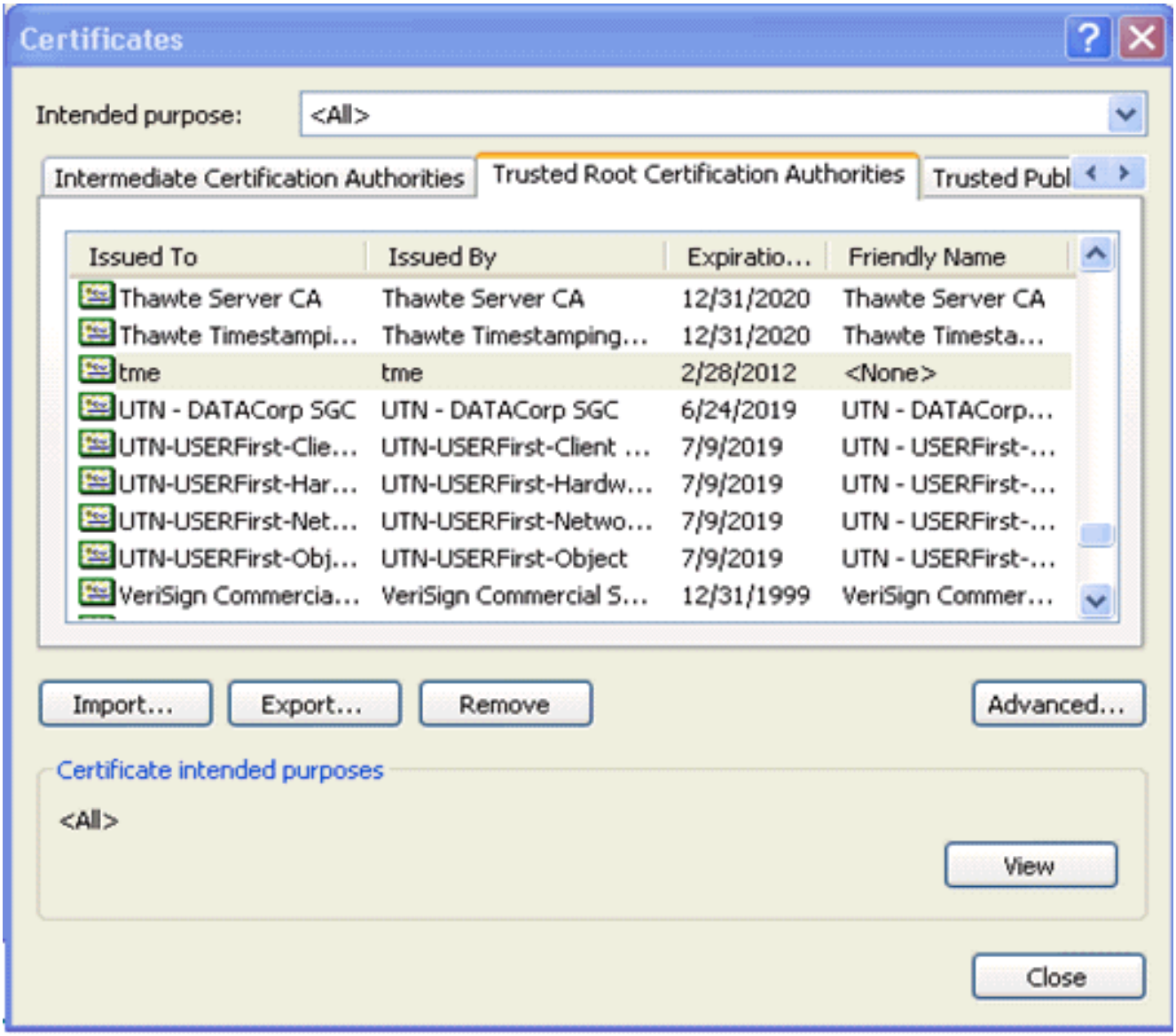

Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for
Automatically select the certificate store based on the type of certificate
Place all certificates in the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

9. 要检查证书颁发机构证书是否已正确安装，请打开Internet Explorer并选择“工具”>“Internet选项”>“**内容**”>“**证书**”。





在受信任的根证书颁发机构中，您应看到新安装的证书颁发机构：



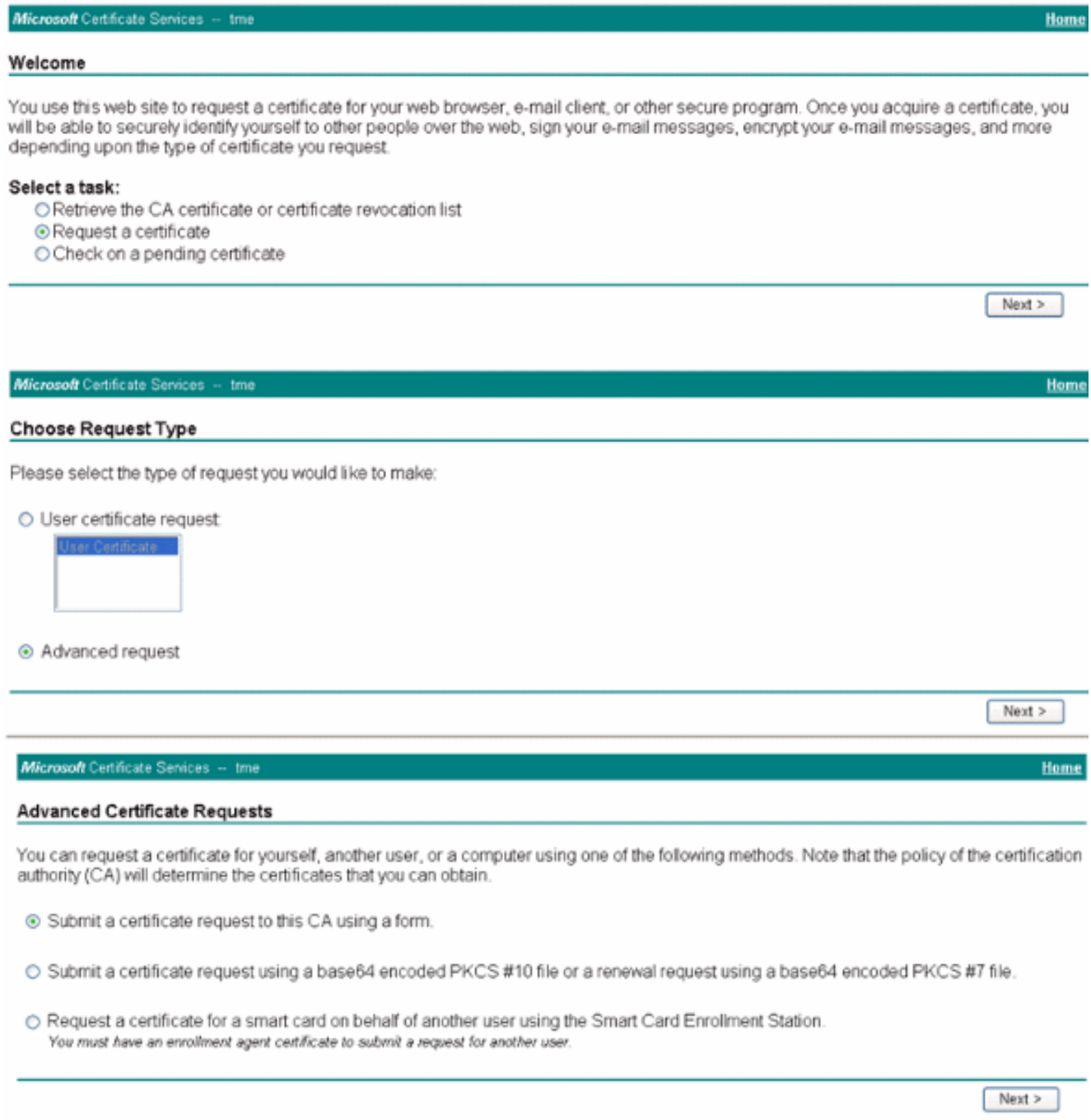
为客户端设备生成客户端证书

客户端必须从证书颁发机构服务器获取证书，WLC才能对WLAN EAP-TLS客户端进行身份验证。您可以使用多种方法来获取客户端证书并将其安装在Windows XP计算机上。要获取有效证书，Windows XP用户必须使用其用户ID登录，并且必须具有网络连接（有线连接或禁用了802.1x安全的WLAN连接）。

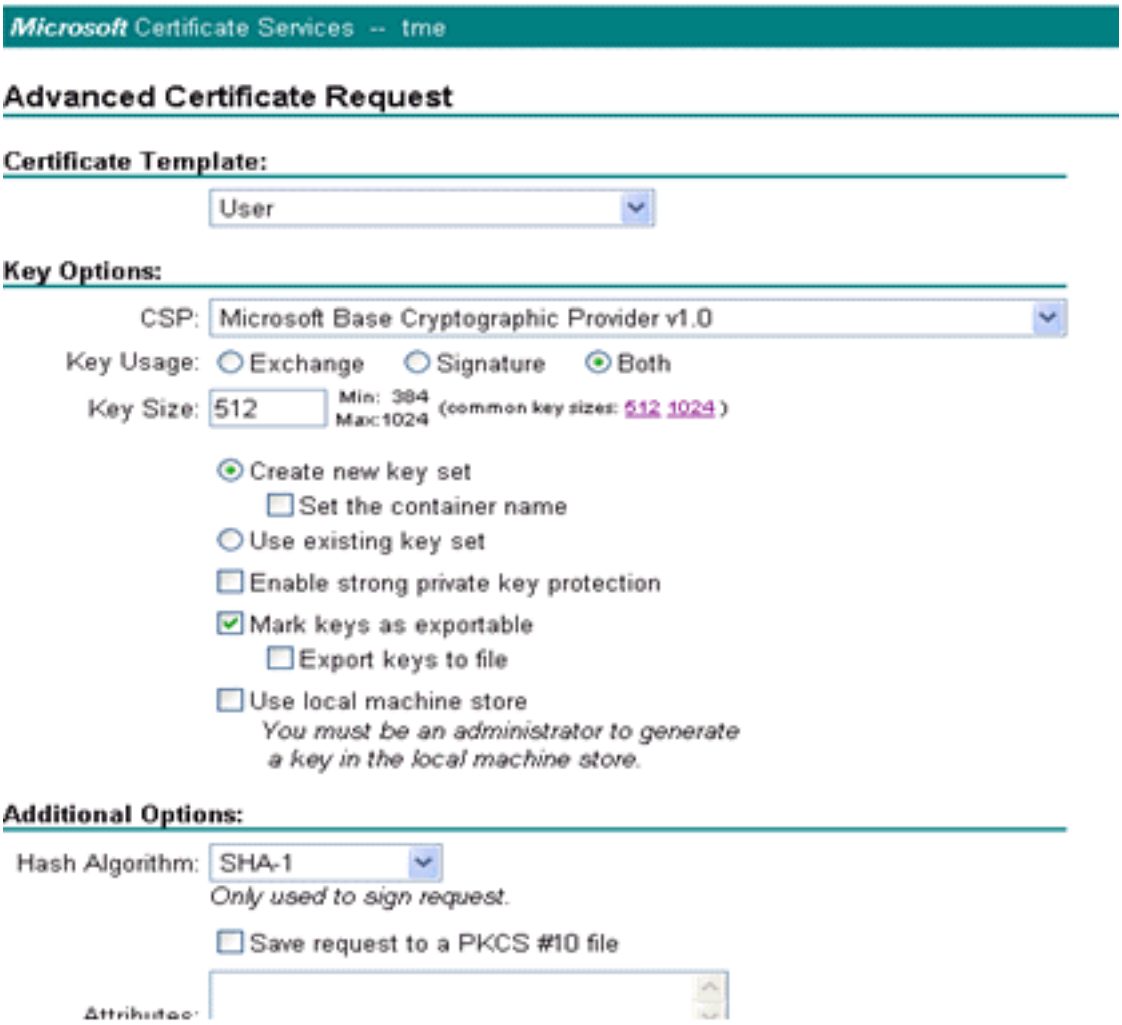
Windows XP客户端上的Web浏览器和网络的有线连接用于从专用根证书颁发机构服务器获取客户端证书。此过程用于从Microsoft证书颁发机构服务器获取客户端证书：

1. 在客户端上使用Web浏览器，并将浏览器指向证书颁发机构服务器。为此，请输入**http://IP-address-of-Root-CA/certsrv**。
2. 使用域**名\用户名登录**。必须使用使用XP客户端的个人的用户名登录。（用户名嵌入到客户端证书中。）
3. 在“欢迎”窗口中，选择“**请求证书”**，然后单**击“下一步**”。
4. 选择**高级请求并单击“下一步”。**
5. 选择**使用表单向此 CA 提交证书请求并单击“下一步”。**
6. 在“高级证书请求”(Advanced Certificate Request)表单中，选择“证书模板”(Certificate Template)作为“用户”(User)，将“密钥大小”(Key Size)指定**为1024，然**后单击“**提交”(Submit)**。
7. 在Certificate Issued（颁发的证书）窗口中，单击**Install this certificate(安装此证**书)。这会导

致在Windows XP客户端上成功安装客户端证书。

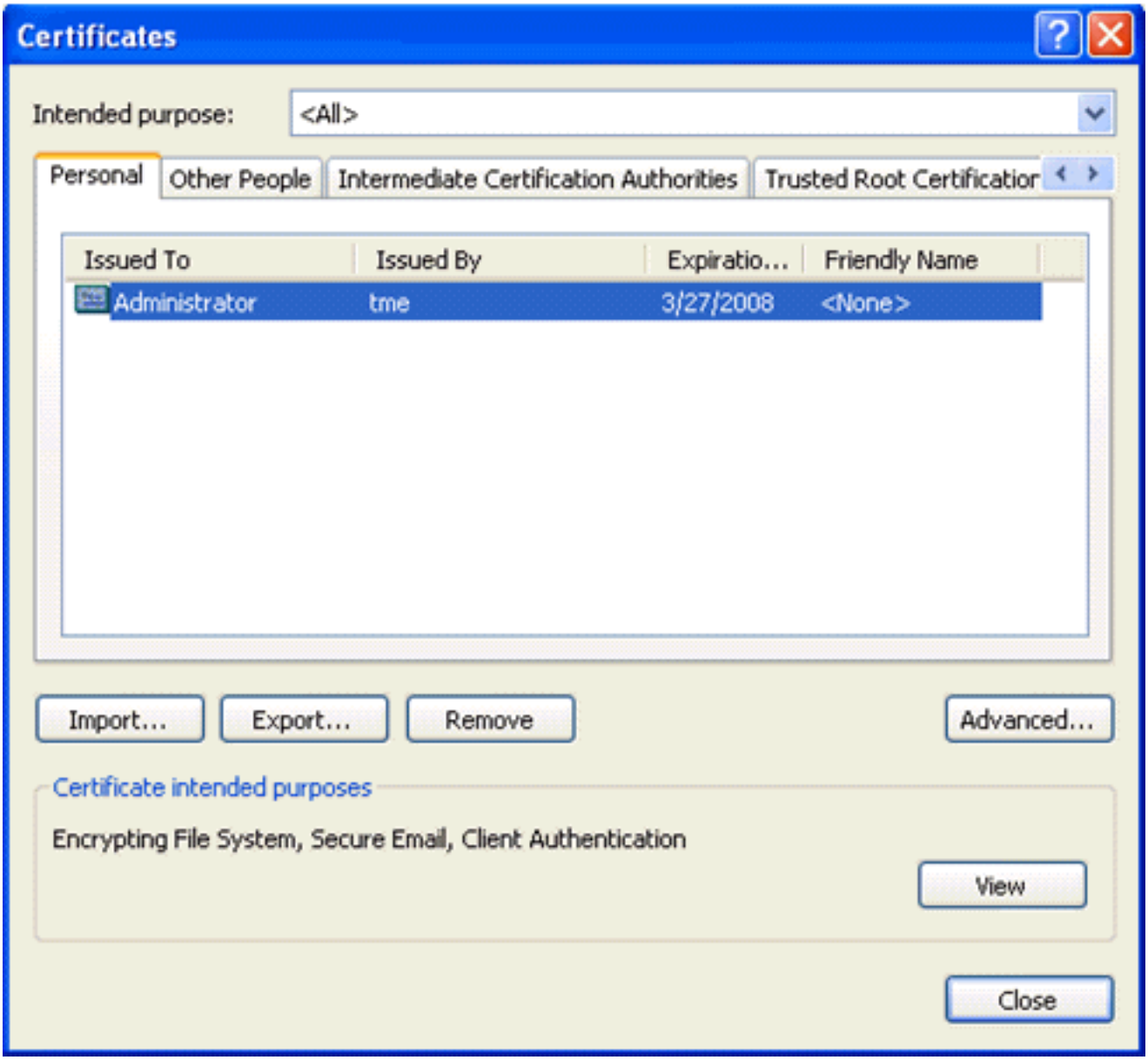


8. 选择“Client Authentication Certificate”。



客户端证书现已创建。

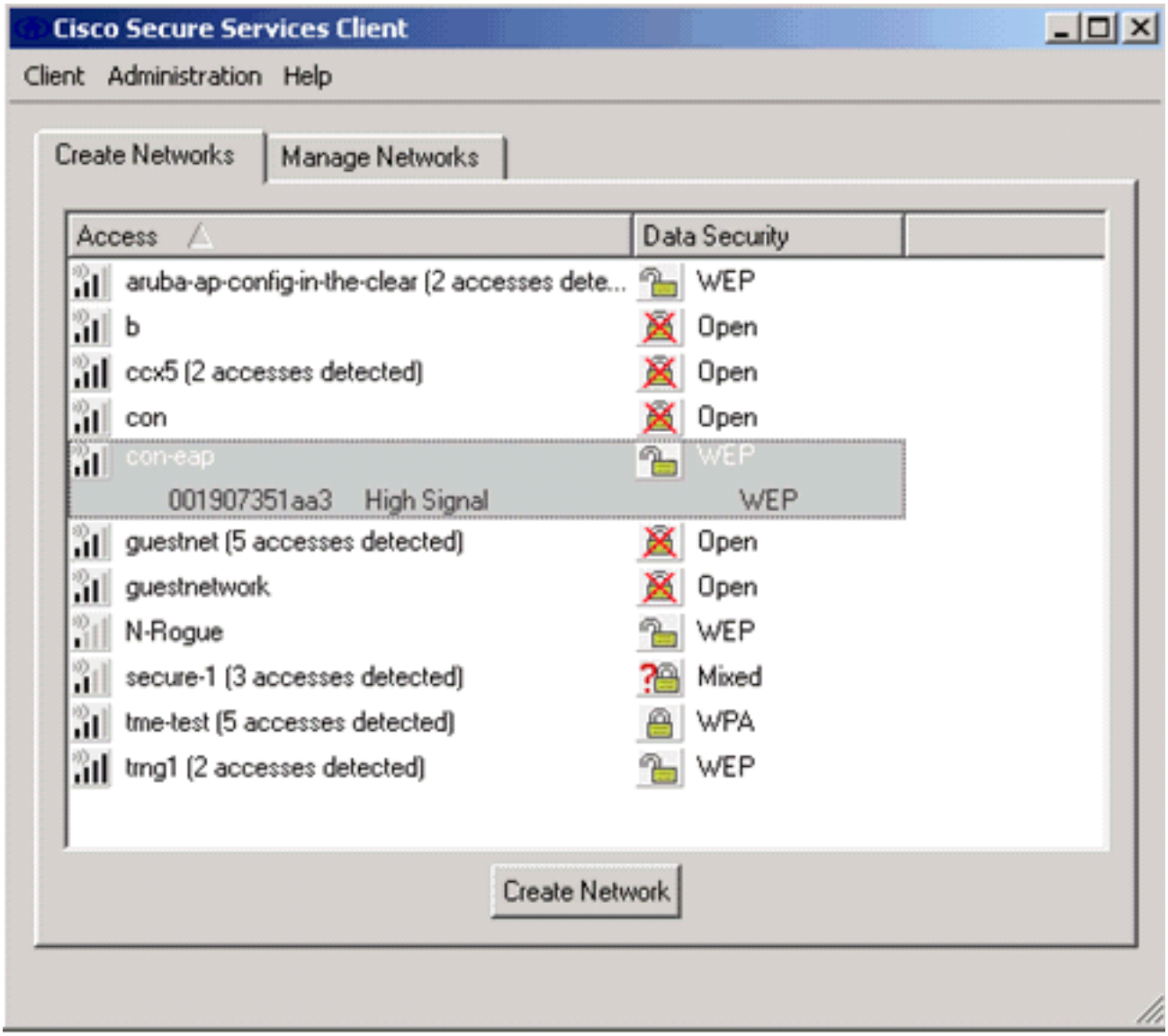
9. 要检查证书是否已安装，请转到Internet Explorer，然后选择“工具”>“Internet选项”>“内容”>“证书”。在“个人”选项卡中，您应该看到证书。



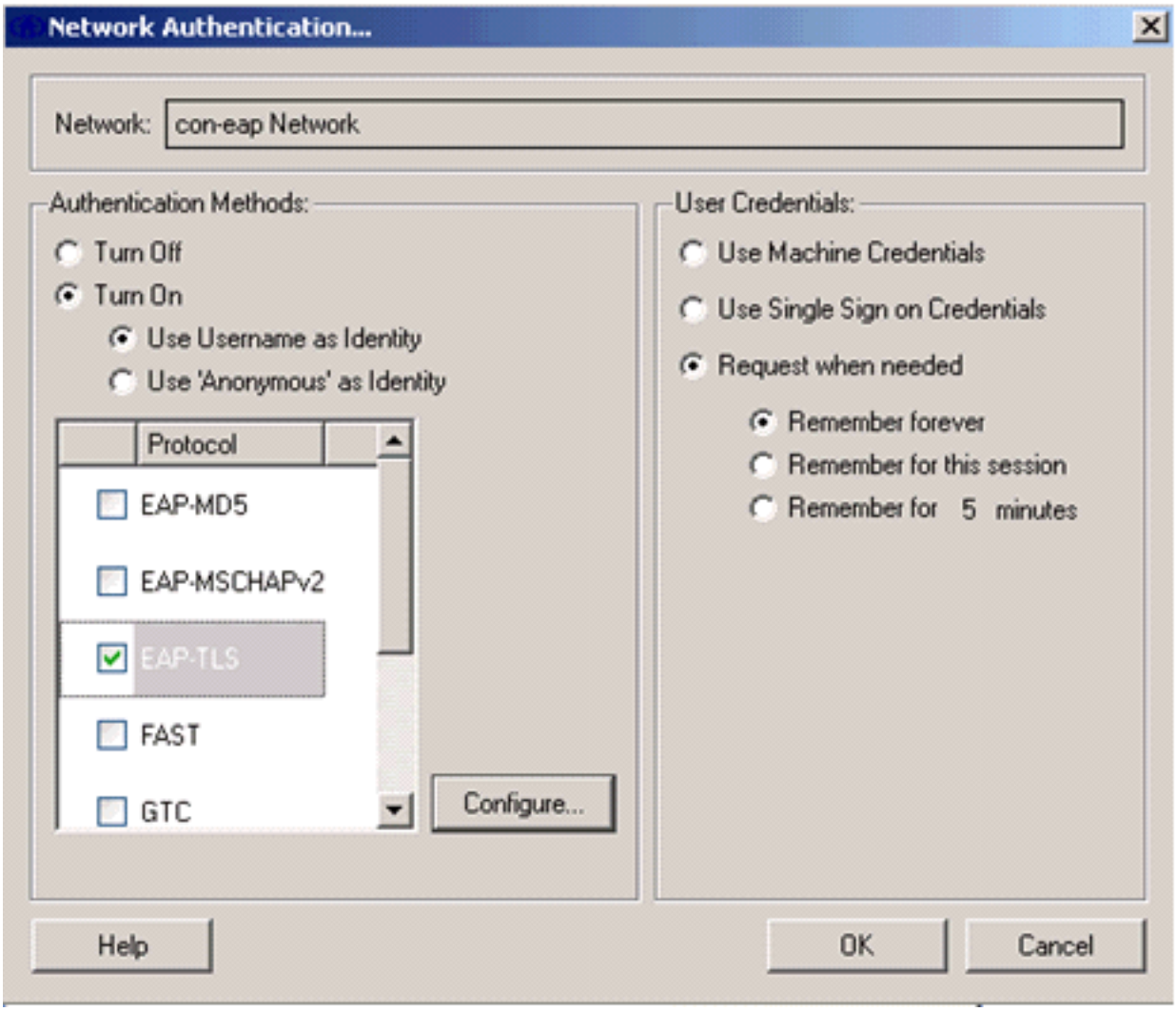
客户端设备上思科安全服务客户端的EAP-TLS

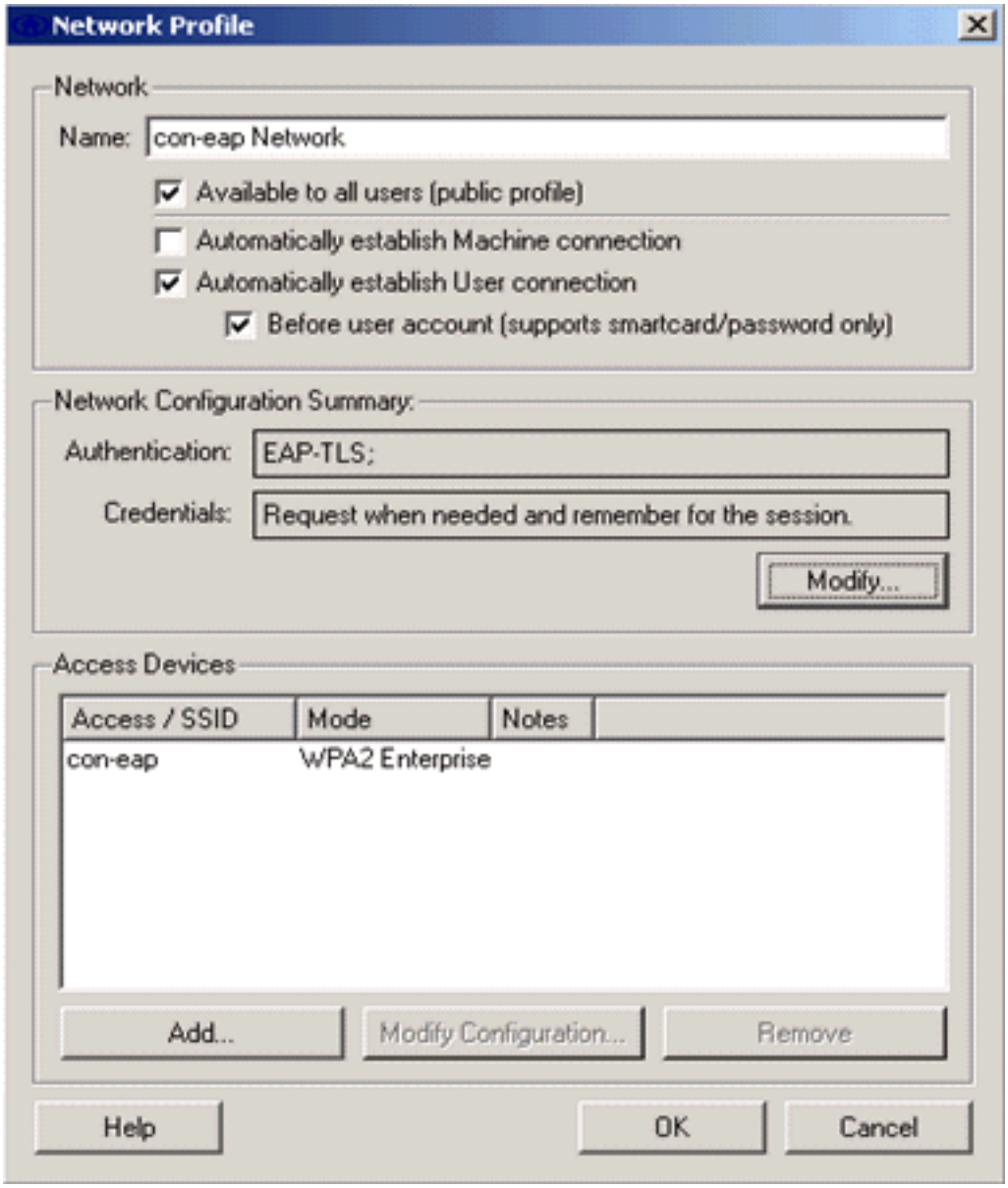
请完成以下步骤：

1. 默认情况下，WLC广播SSID，因此它显示在已扫描SSID的Create Networks列表中。要创建网络配置文件，可以点击列表（企业）中的SSID，然后点击创建**网络**。如果WLAN基础设施配置了禁用广播SSID，则必须手动添加SSID。为此，请单击“Access Devices”下的**Add**，然后手动输入适当的SSID（例如，Enterprise）。 为客户端配置活动探测行为。也就是说，客户端主动探查其已配置的SSID。在“Add Access Device”窗口中输入 SSID 之后，指定 **Actively search for this access device。注意：**如果EAP身份验证设置未首先为配置文件配置，则端口设置不允许企业模式(802.1X)。
2. 单击**Create Network**以启动“Network Profile”窗口，该窗口允许您将所选（或已配置）SSID与身份验证机制相关联。为配置文件指定描述性名称。**注意：在**此身份验证配置文件下可以关联多个WLAN安全类型和/或SSID。

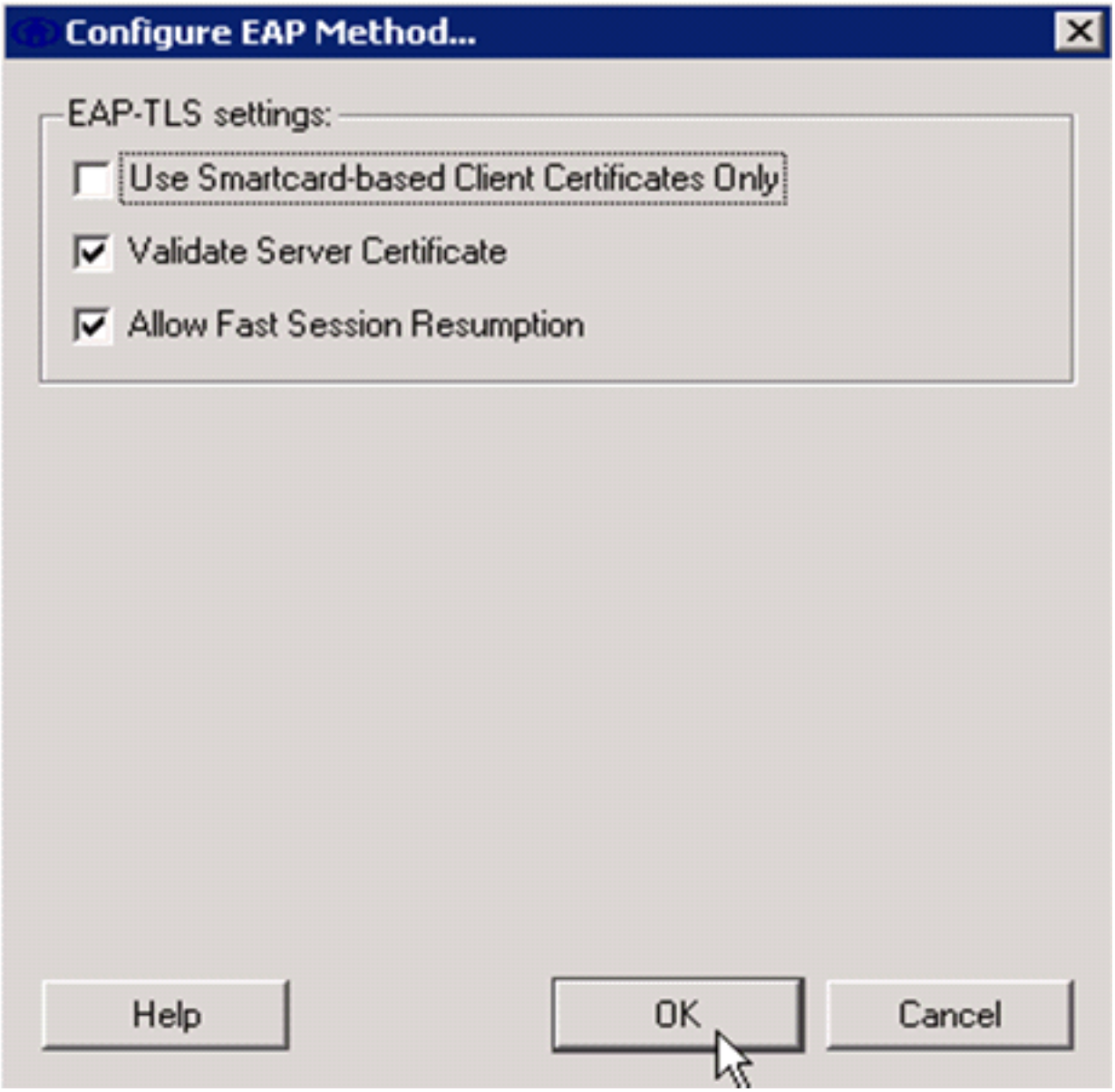


3. 打开身份验证并检查EAP-TLS方法。然后单击**Configure**以配置EAP-TLS属性。
4. 在Network Configuration Summary（网络配置摘要）下，单击**Modify**以配置EAP /凭据设置。
5. 指**定Turn On Authentication**，在Protocol**下选择EAP-TLS**，然后选择**Username**作为Identity。
6. 指定 **Use Single Sign on Credentials，以使用登录凭据进行网络身份验证。**单击**Configure**以设置EAP-TLS参数。


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

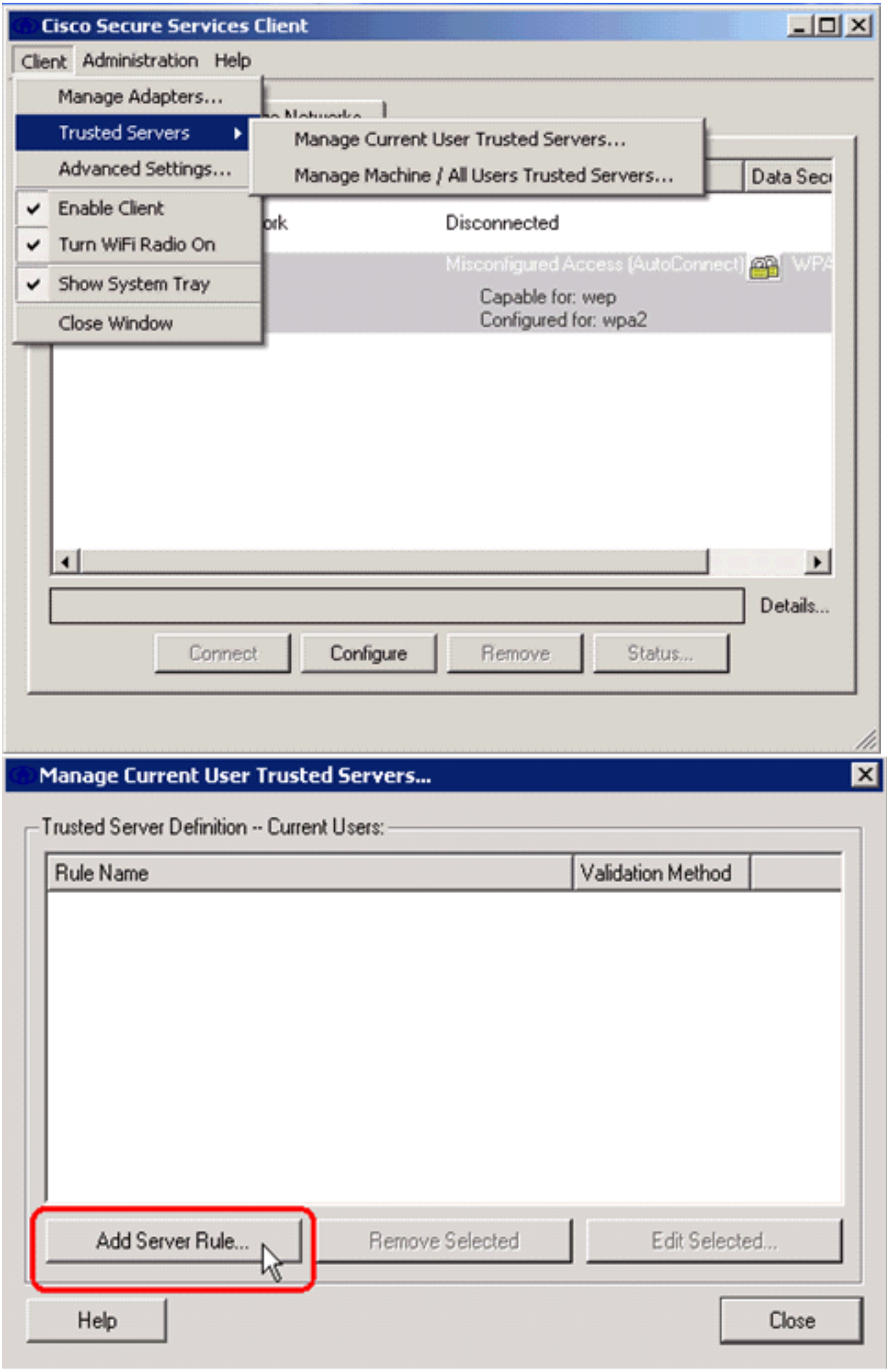


7. 要获得安全的EAP-TLS配置，您需要检查RADIUS服务器证书。为此，请选中验证服**务器证书**

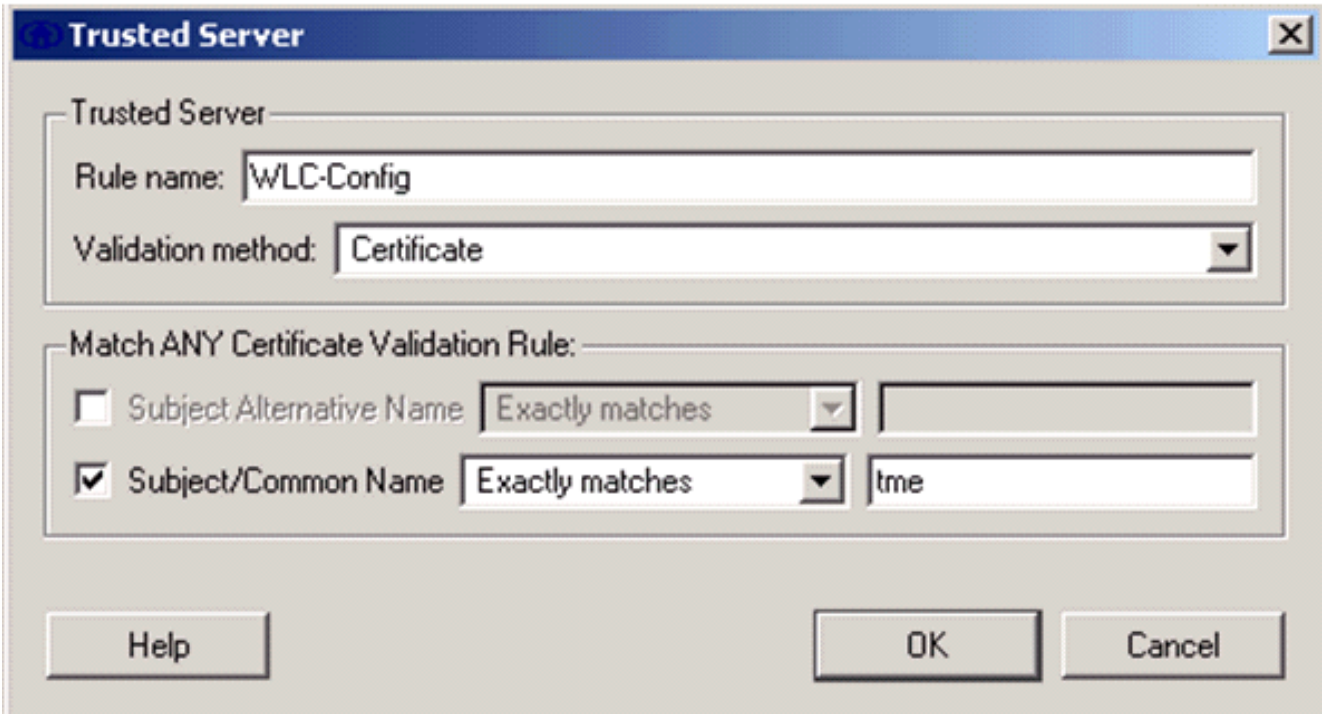


。

8. 要验证RADIUS服务器证书，您需要提供思科安全服务客户端信息，以便仅接受正确的证书。选择**Client > Trusted Servers > Manage Current User Trusted Servers**。

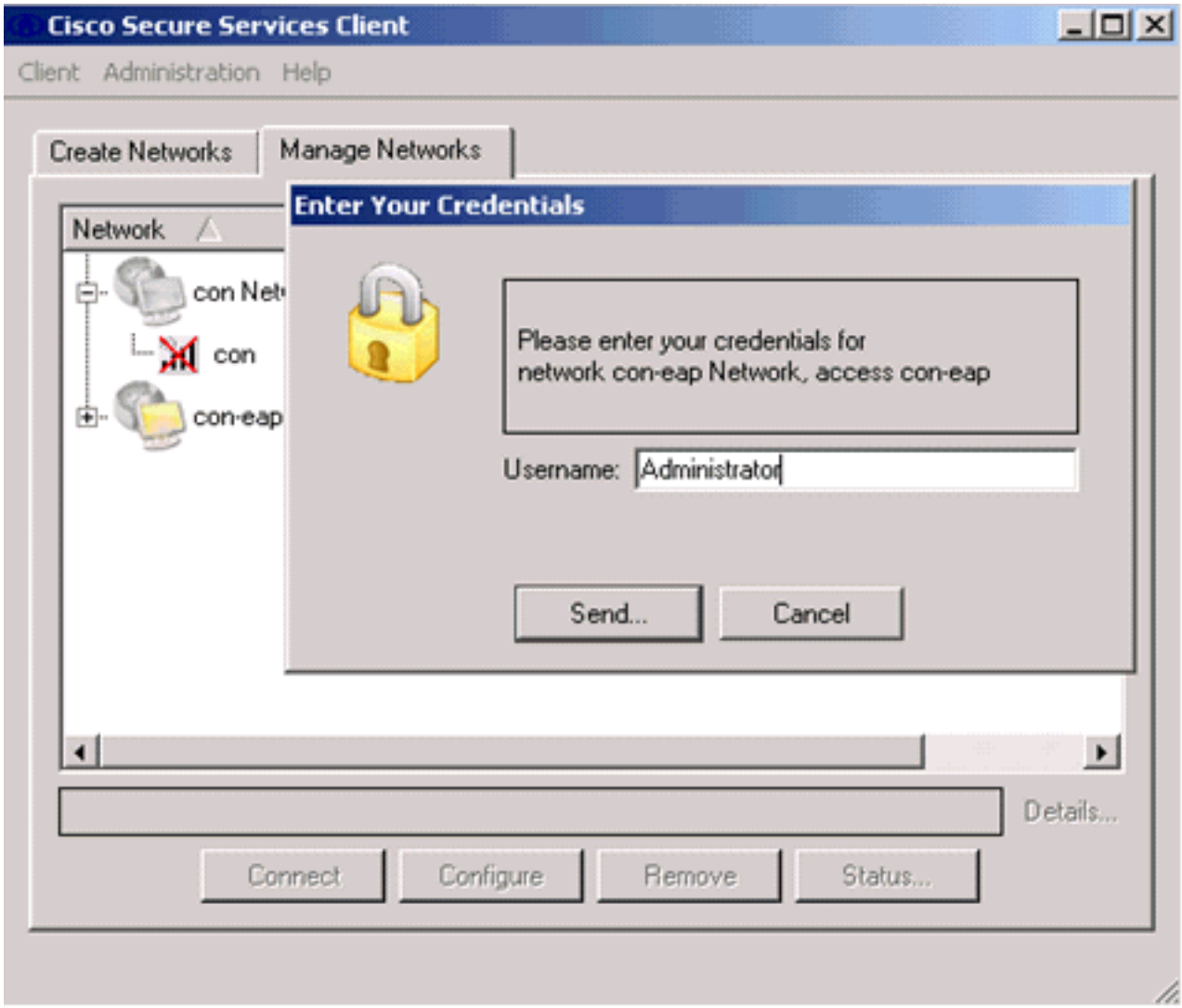


9. 为规则指定名称并检查服务器证书的名称。



EAP-TLS配置已完成。

10. 连接到无线网络配置文件。思科安全服务客户端要求用户登录

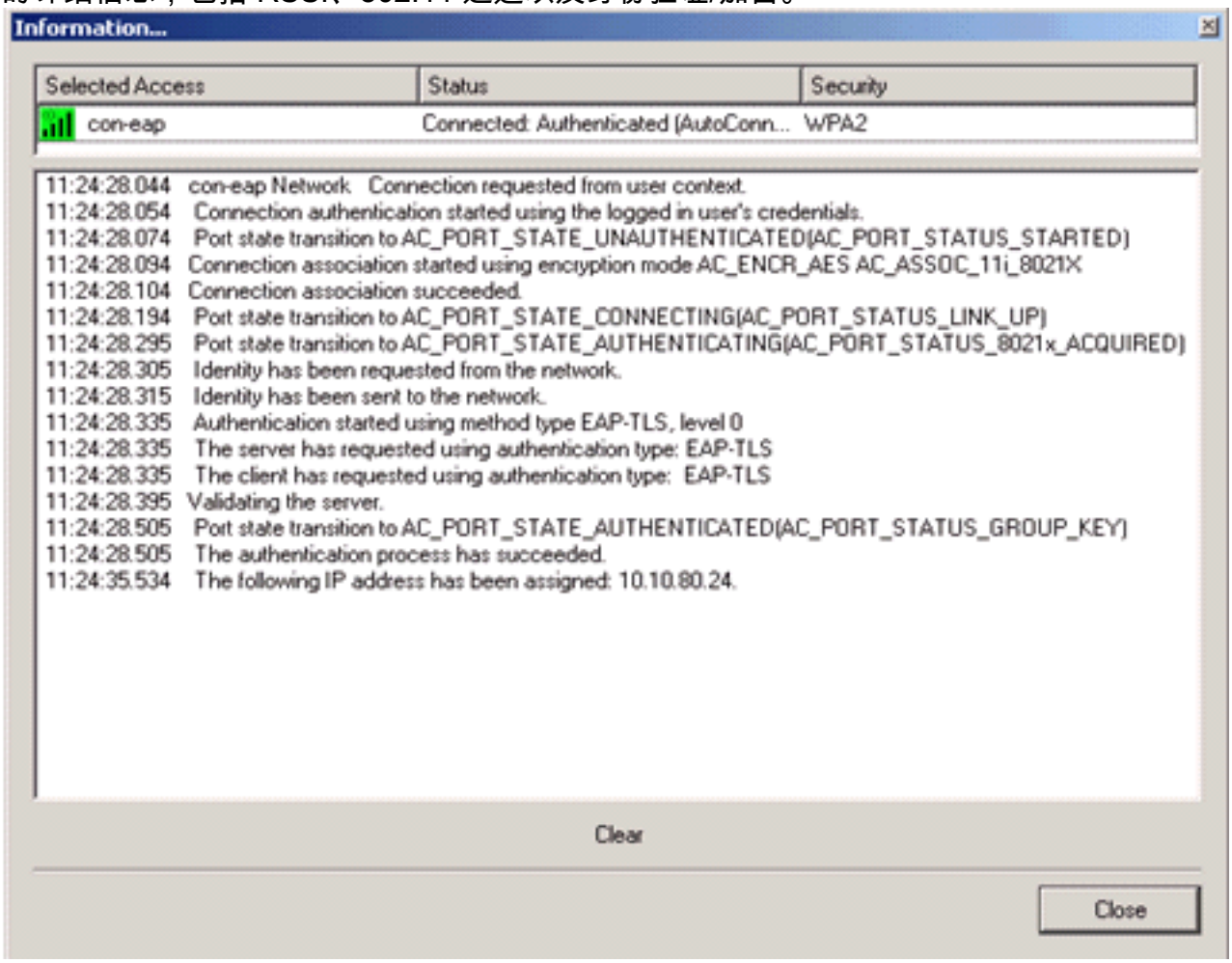


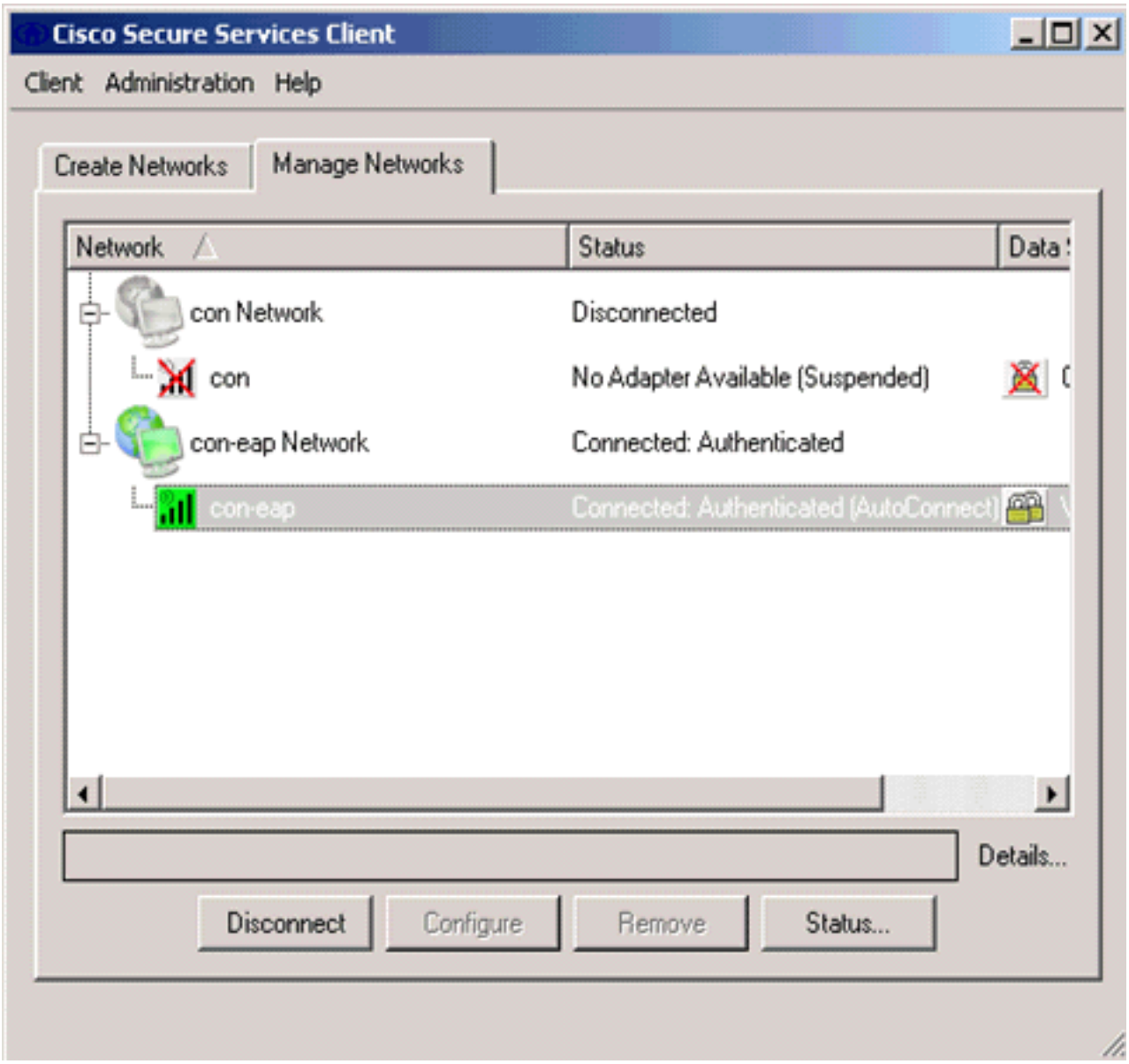
：

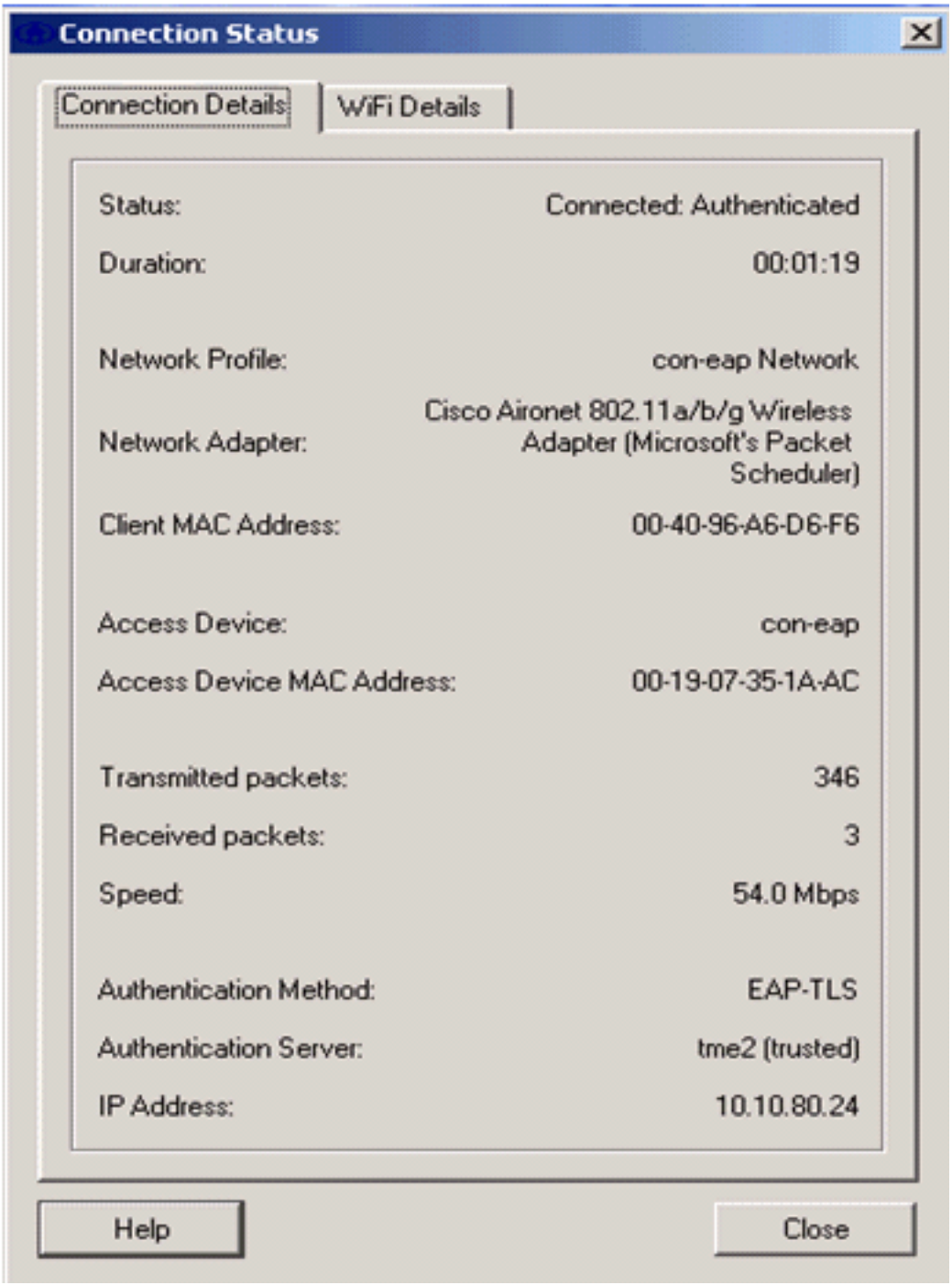
思科安全服务客户端接收服务器证书并对其进行检查（配置规则并安装证书颁发机构）。 然后，它要求用户使用证书。

11. 在客户端验证之后，在“Manage Networks”选项卡中的“Profile”下选择 **SSID，然后单击**

“Status”以查询有关连接的详细信息。“Connection Details”窗口提供了有关客户端设备、连接状态和统计信息以及身份验证方法的信息。“WiFi Details”选项卡提供了有关 802.11 连接状态的详细信息，包括 RSSI、802.11 通道以及身份验证/加密。




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...



调试命令

命令输出解释程序（仅限注册用户）(OIT) 支持某些 show 命令。使用 OIT 可查看对 show 命令输出的分析。

注意：在使用debug命令之前，请参阅有关Debug命**令的**重要信息。

在WLC上可以使用以下debug命令来监控身份验证交换的进度：

- **debug aaa events enable**
- **debug aaa detail enable**
- **debug dot1x events enable**
- **debug dot1x states enable**
- **debug aaa local-auth eap events enable**或者

- debug aaa all enable

相关信息

- Cisco 无线局域网控制器配置指南 4.1 版
- WLAN 技术支持
- 技术支持和文档 - Cisco Systems