统一无线网络本地EAP服务器配置示例

目录

简介

本文描述一个本地可扩展的认证协议(EAP)服务器的配置在一个Cisco无线LAN控制器(WLC)的无线用户的验证的。

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。它设计用于要维护连接对无线客户端的远程办公室，当后端系统变得打乱时或外部验证服务器断开。当您启用本地EAP时，控制器担当，从而删除在外部验证服务器的认证服务器和本地用户数据库依赖因素。本地EAP从本地用户数据库或轻量级目录访问协议(LDAP)支持者数据库获取用户凭证验证用户。本地EAP通过获取建立隧道(EAP-FAST)支持轻量级EAP (LEAP)， EAP灵活验证和传输层在控制器和无线客户端之间的安全(EAP-TLS)验证。

注意本地EAP服务器不是可用的，如果有在WLC的一全局外部RADIUS服务器配置。所有认证请求转发对全局外部RADIUS，直到本地EAP服务器是可用的。如果WLC疏松连接到外部RADIUS服务器，则本地EAP服务器变得激活。如果没有全局RADIUS服务器配置，本地EAP服务器变得激活立即。本地EAP服务器不可能用于验证客户端，连接对其他WLCs。换句话说，一WLC不能转发其EAP请求到验证的另一WLC。每WLC应该有其自己的本地EAP服务器和个人数据库。

注意： 请使用这些命令为了从发送请求终止WLC对外部RADIUS服务器。

```
config wlan disable
        config wlan radius_server auth disable
        config wlan enable
```
本地EAP服务器支持在4.1.171.0软件版本的这些协议和以后：

- LEAP
- EAP-FAST (两用户名/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验证基础知识。

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无线局域网控制器4.1.171.0
- Windows 2000服务器的Microsoft证书颁发机构

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

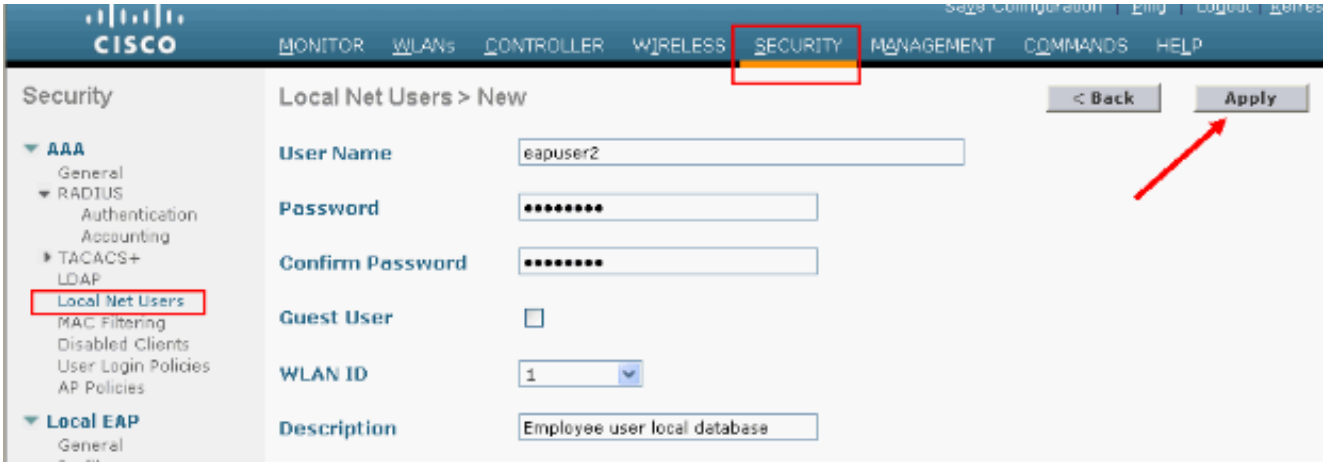
配置在Cisco无线LAN控制器的本地EAP

本文档假设 WLC 的基本配置已完成。

本地EAP配置

完成这些步骤为了配置本地EAP ：

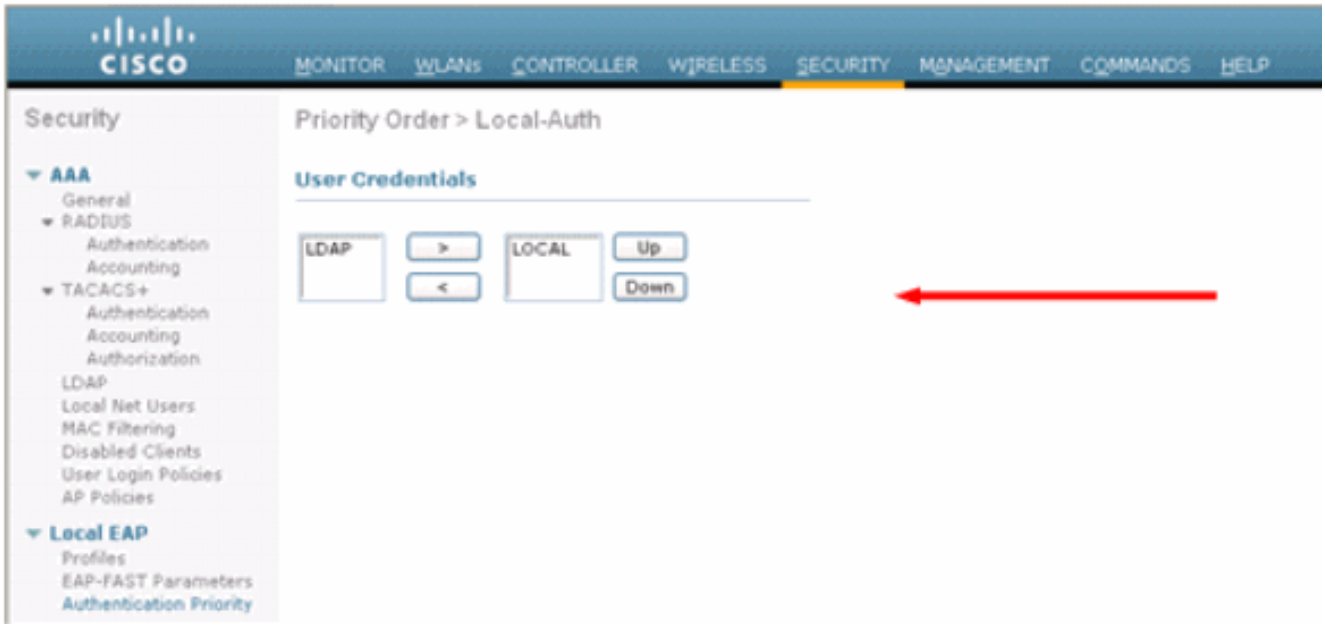
1. 添加一个本地净用户：从GUI。选择**安全>本地捕网用户>New**，输入用户名、密码、来宾用户、WLAN ID和说明并且单击**应用**。



从CLI您能使用**设置netuser添加*<username> <password> <WLAN id> <description>***命令：**注意：** 此命令给第二条线路减少了由于空间的原因。

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

2. 指定用户凭证检索顺序。从GUI，请选择**安全>本地EAP >验证优先级**。然后请选择LDAP，单击“**<**”按钮并且单击**应用**。这在本地数据库首先放置用户凭证。



从CLI ：

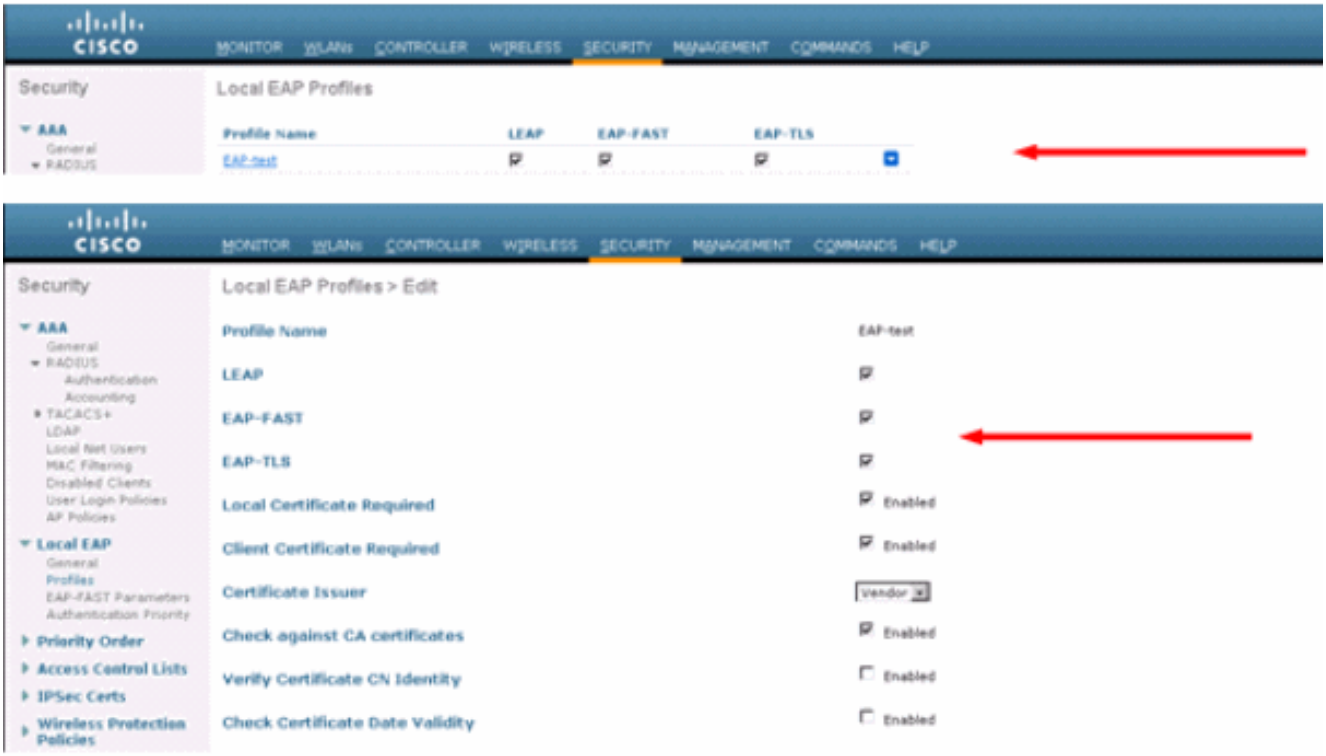
```
(Cisco Controller) >config local-auth user-credentials local
```

3. 添加一Eap profile ：为了从GUI执行此，选择**安全>本地EAP >配置文件**和点击**新**。当新窗口出现时，请键入配置文件名称并且单击**应用**。

您能也执行此使用CLI命令**config local-auth eap-profile添加*<profile-name>*。**在我们的示例中，配置文件名称是*EAP测试*。

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

4. 添加一个方法到Eap profile。从GUI请选择**安全>本地EAP >配置文件**并且点击您想要添加认证方法的配置文件名称。此示例使用LEAP、EAP-FAST和EAP-TLS。单击**应用**为了设置方法。

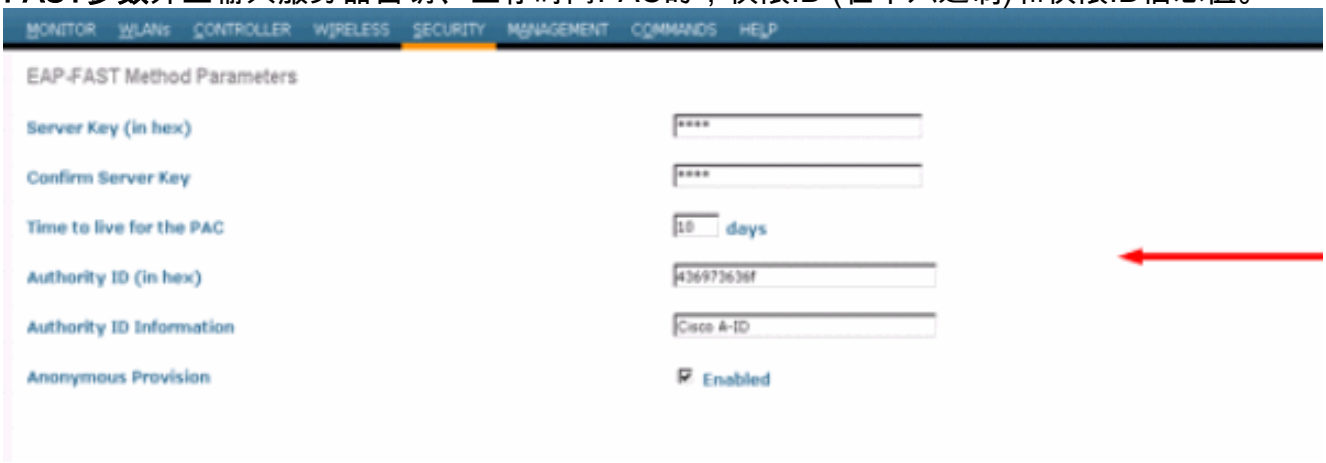


您能也使用CLI命令**config local-auth eap-profile方法添加*<method-name> <profile-name>***。在我们的配置示例中我们添加三个方法到配置文件EAP测试。方法是方法名称分别为闰年，*快速*和*tls的*LEAP、EAP-FAST和TLS。此输出显示CLI配置命令：

```
(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。这只使用EAP-FAST。将配置的参数是：**服务器密钥(服务器密钥)** —服务器密钥加密的/解密受保护的访问凭证(PACs) (在十六进制)。**PAC的(pac-ttl)生存时间**—设置

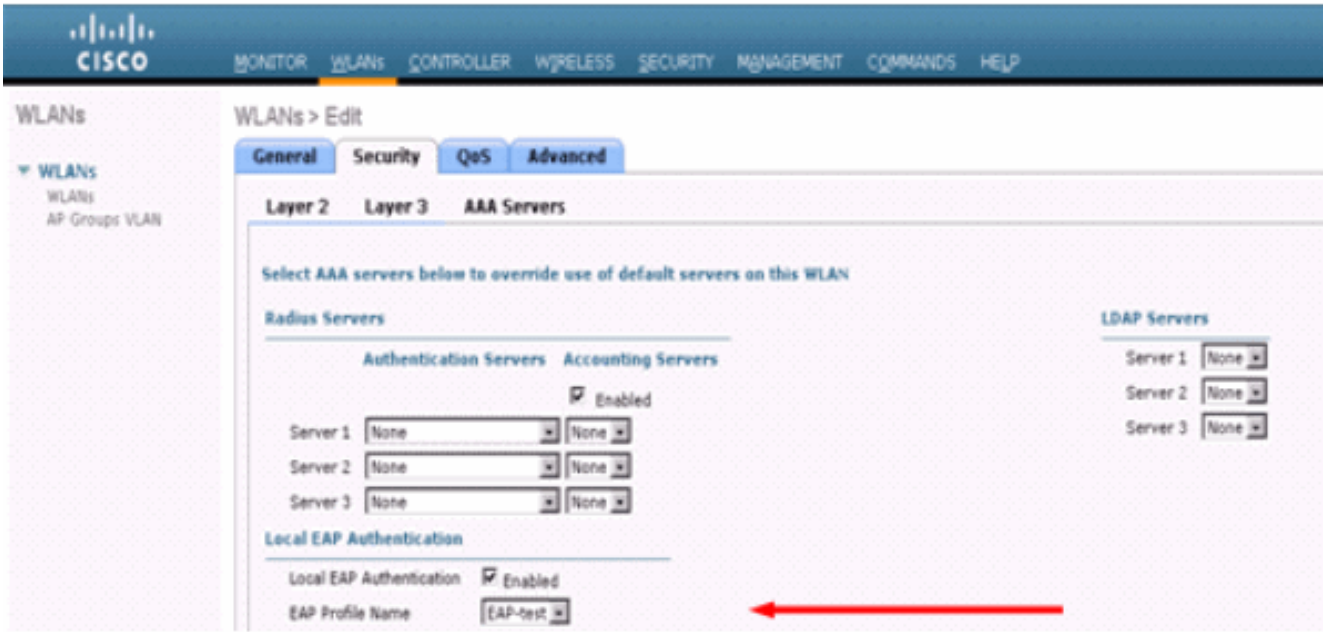
PAC的生存时间。**权限ID (权限id)** —设置权限标识符。**匿名提供(anon-provn)** —配置匿名提供是否允许。默认情况下启用该接口。对于配置通过GUI，请选择**安全>本地EAP > EAP-FAST参数**并且输入服务器密钥、生存时间PAC的，权限ID (在十六进制)和权限ID信息值。



这些是CLI配置命令使用为了设置EAP-FAST的这些参数：

```
(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
```

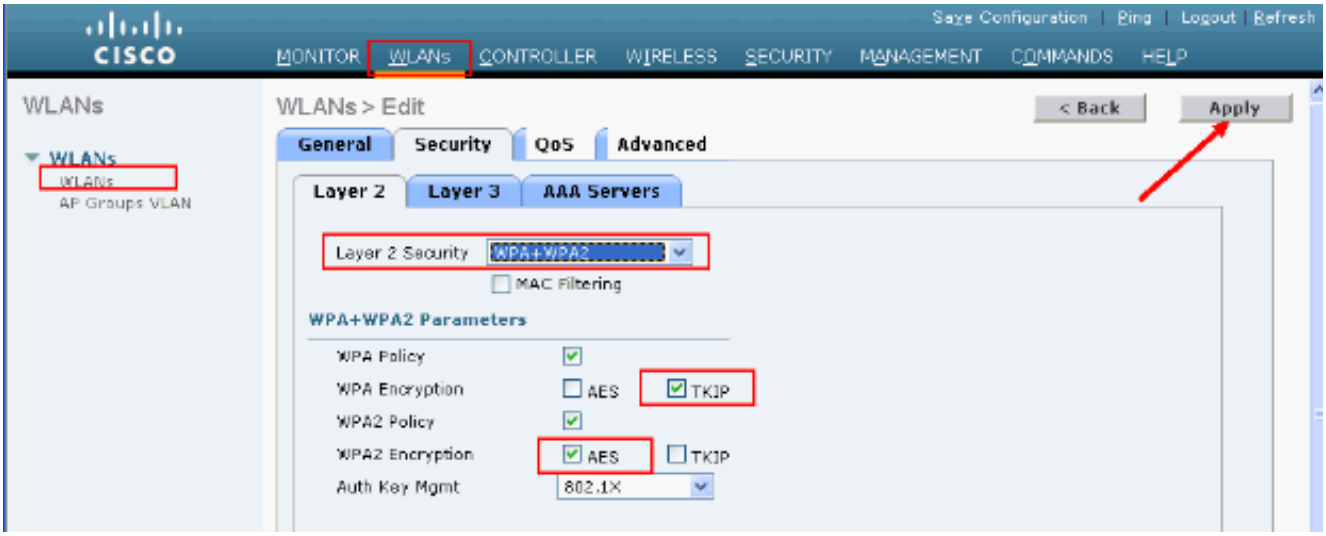
6. Enable (event)本地认证每WLAN ：从GUI请选择在顶部菜单的**WLAN**并且选择您要配置本地认证的WLAN。新窗口出现。点击**安全>AAA**选项卡。检查**本地EAP验证**并且选择从下拉菜单的正确的Eap profile名称，此示例显示
：



您能也发出CLI来设置**wlan本地验证enable (event)** *<profile-name>* *<wlan-id>*配置命令如显示此处：

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

7. 设置第2层安全参数。从GUI界面，在Edit窗口的WLAN请去**安全> Layer2**选项卡并且从第2层安全下拉菜单选择**WPA+WPA2**。在WPA+WPA2参数部分下，设置WPA加密为**TKIP**和WPA2加密**AES**。然后单击 **Apply**。



从CLI，请使用这些命令：

```
(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. 验证配置：

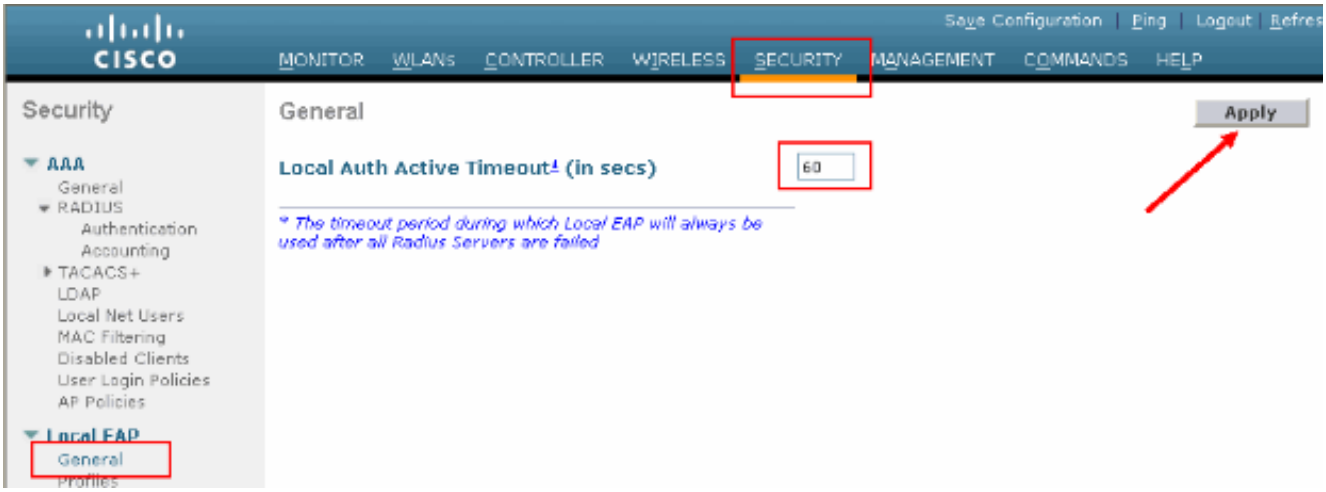
```
(Cisco Controller) >show local-auth config

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

您能看到特定参数WLAN 1用显示wlan <wlan id>命令：

```
(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
```

有可以配置的其他本地认证参数，特别是活动超时计时器。此计时器配置期间本地EAP使用的期限在，在所有RADIUS服务器失败后。从GUI，请选择**安全>本地EAP >General**并且设置时间值。然后单击 **Apply**。



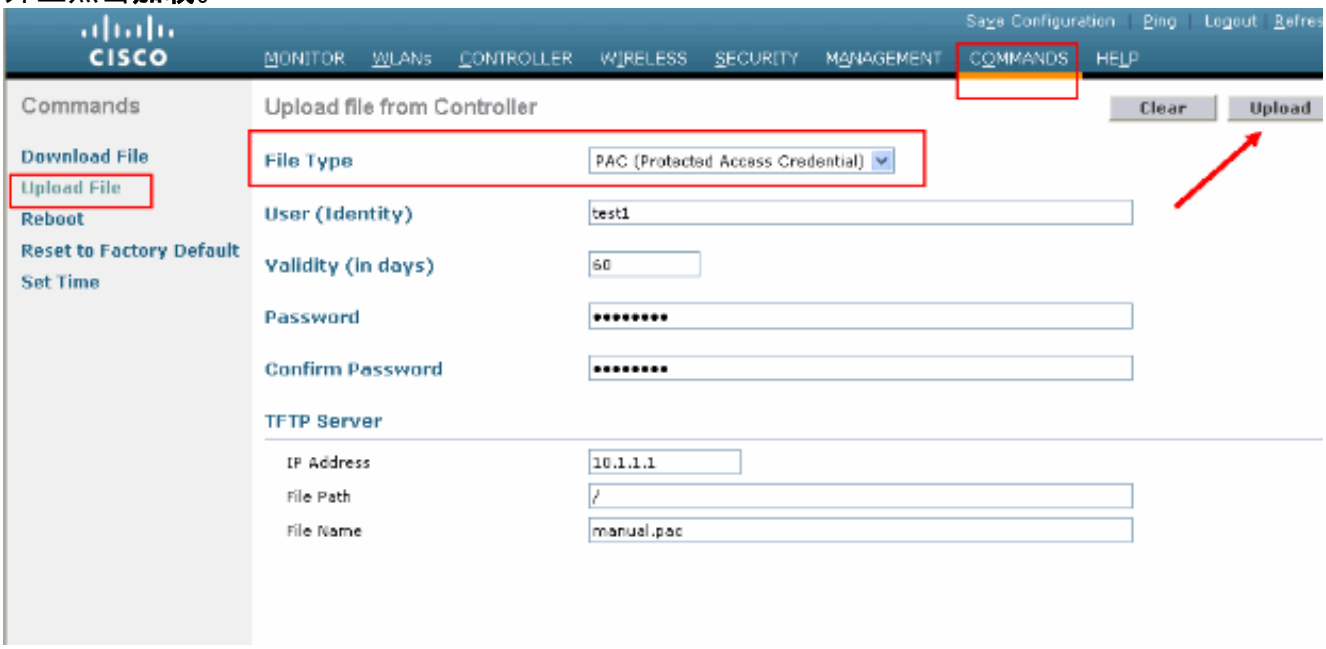
从CLI，请发出这些命令：

```
(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
```

您能验证此计时器设置的值，当您发出**config命令时显示的本地验证。**

```
(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. 如果需要生成和装载手工的PAC，您能使用GUI或CLI。从GUI，从顶部菜单的挑选**命令**和从在右边的列表选择**上传文件**。挑选**PAC (受保护的访问凭证)**从文件类型下拉菜单。输入所有参数并且点击**加载**。



从CLI，请输入这些命令：

```
(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证书颁发机构

为了使用EAP-FAST版本2和EAP-TLS验证， WLC和所有客户端设备必须有有效证书，并且必须也认识证书颁发机构的公共证书。

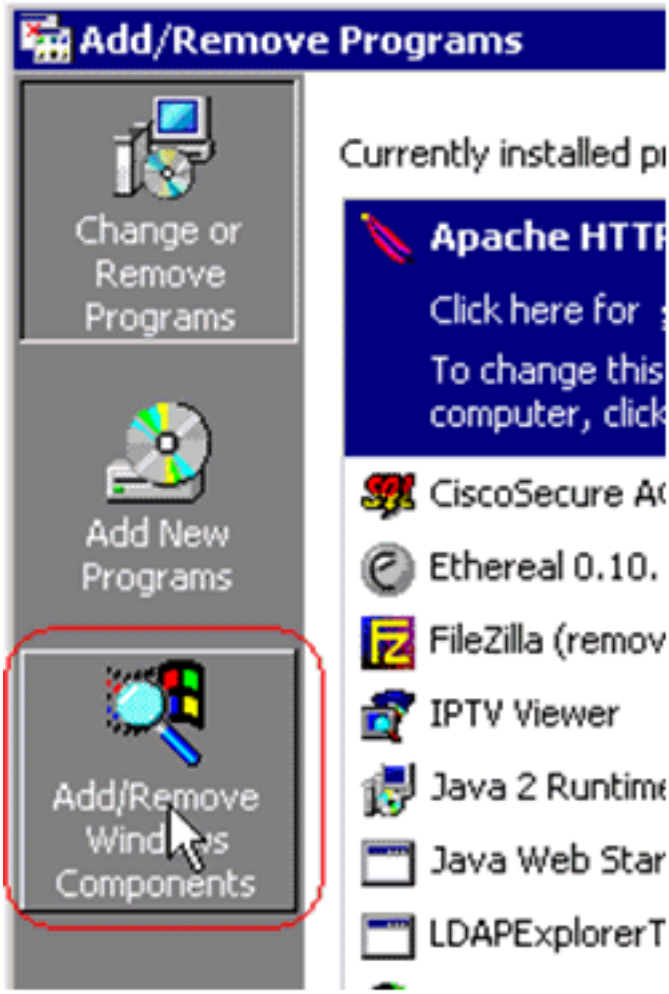
安装

如果Windows 2000服务器已经没有安装的证书颁发机构服务，您需要安装它。

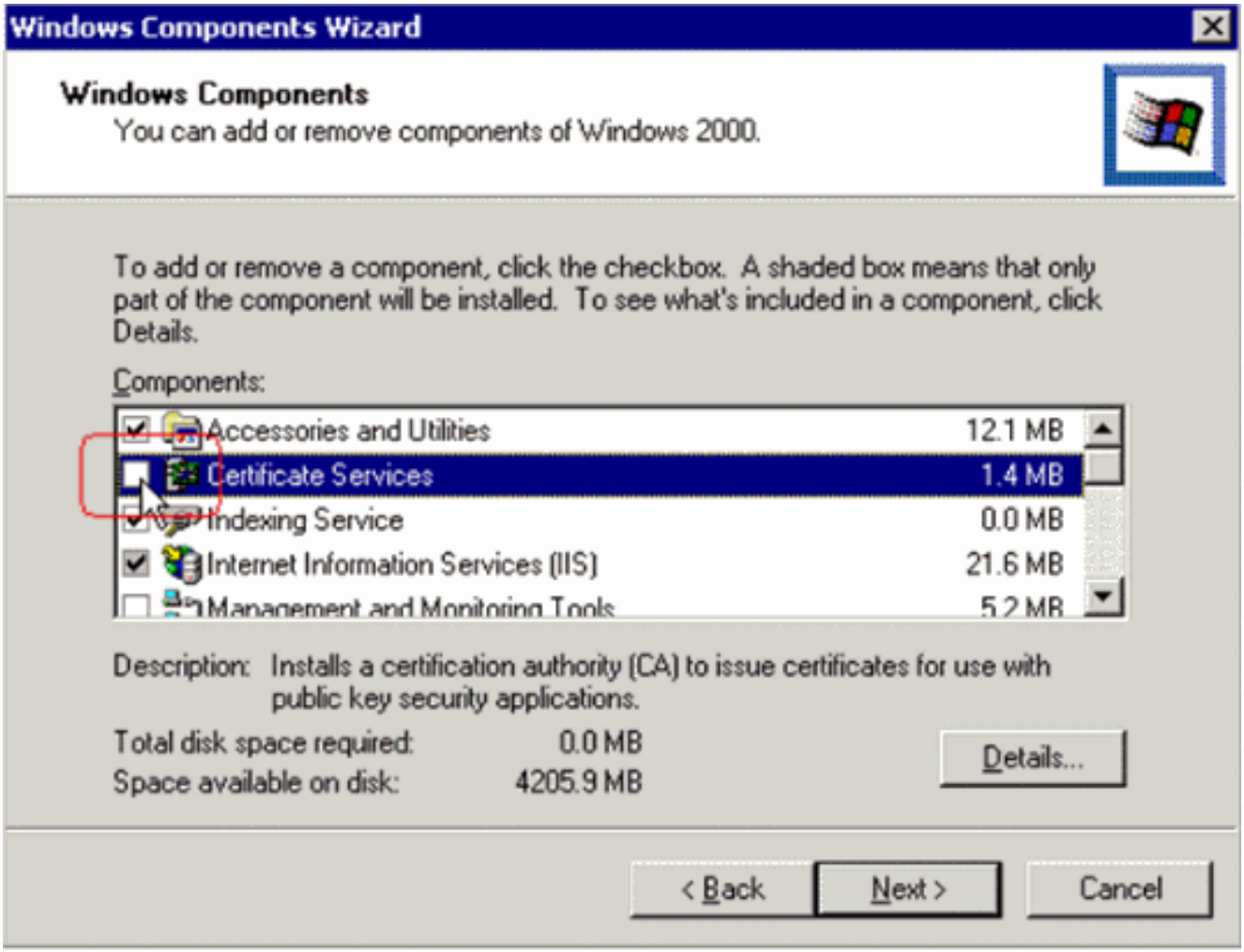
完成这些步骤为了激活Windows 2000服务器的Microsoft证书颁发机构：

1. 从控制面板，请选择**添加/删除程序**。

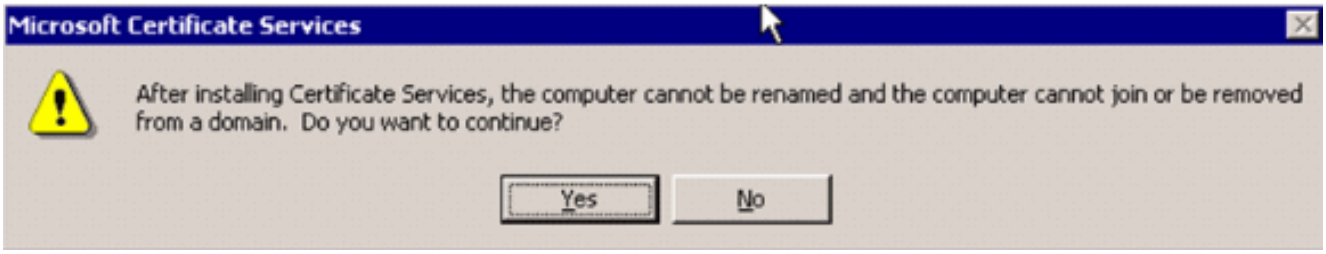
::



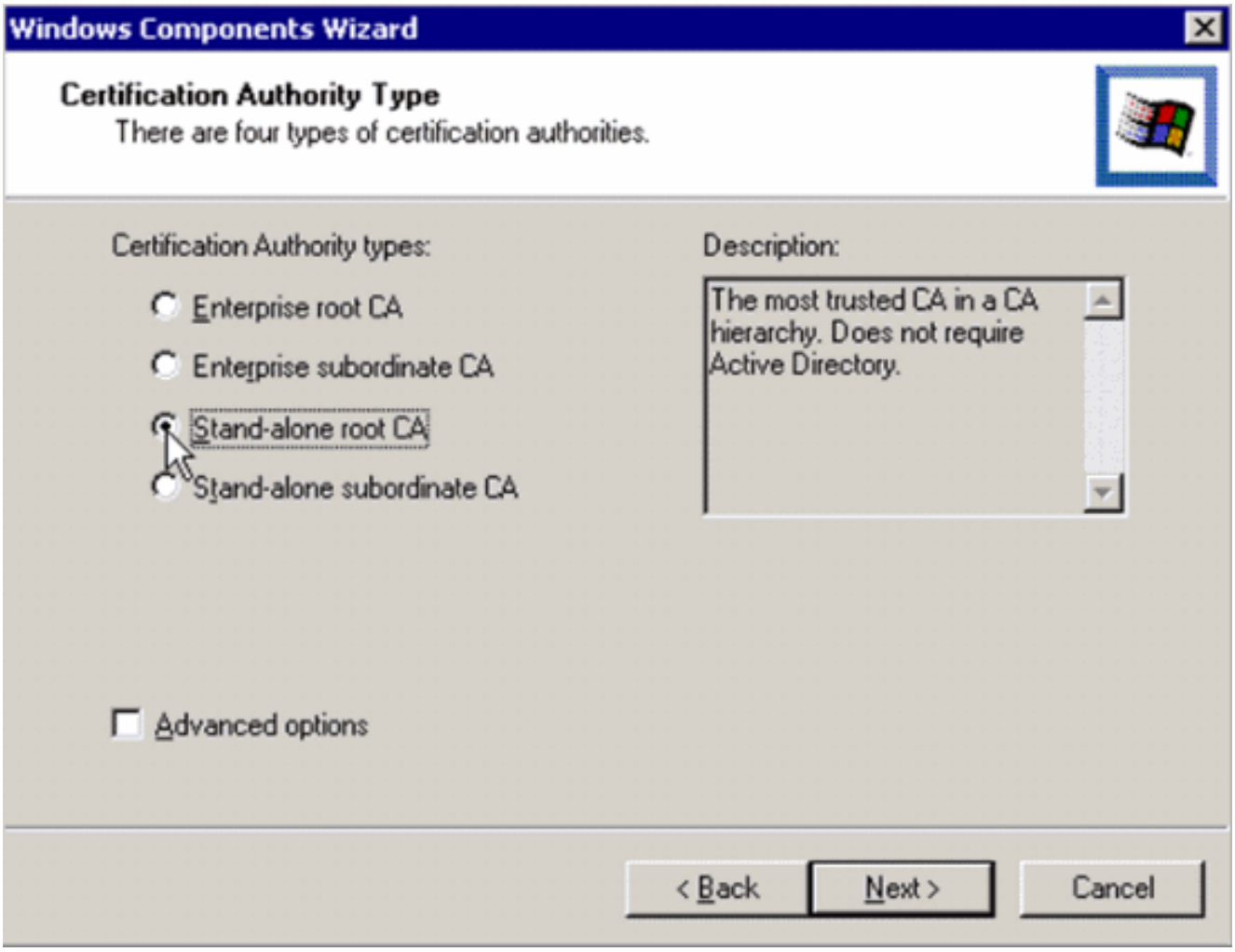
2. 选择**添加/删除**在左侧的**Windows组件**。
3. 检查**证书服务**。



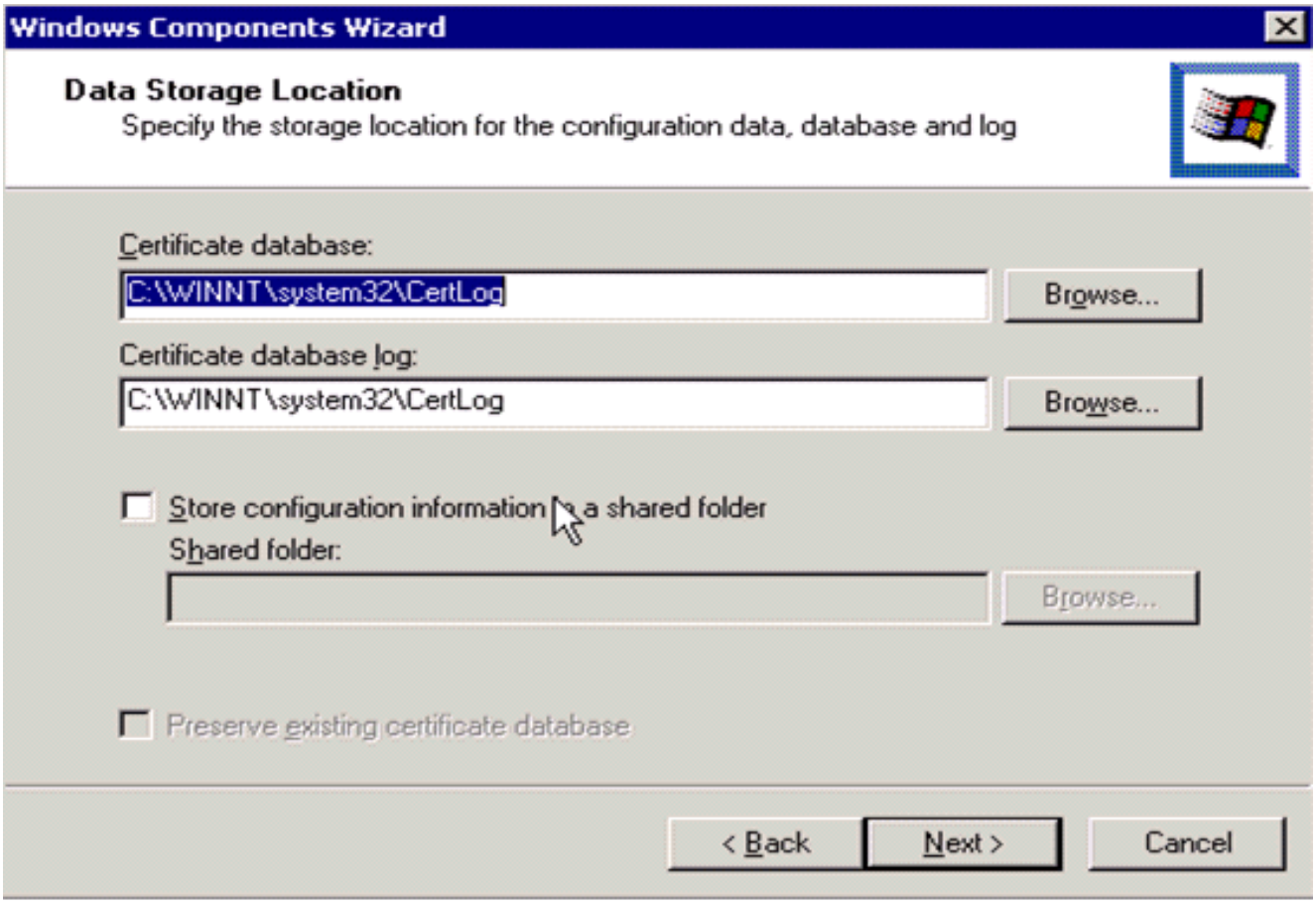
在您继续前，请查看此警告
：



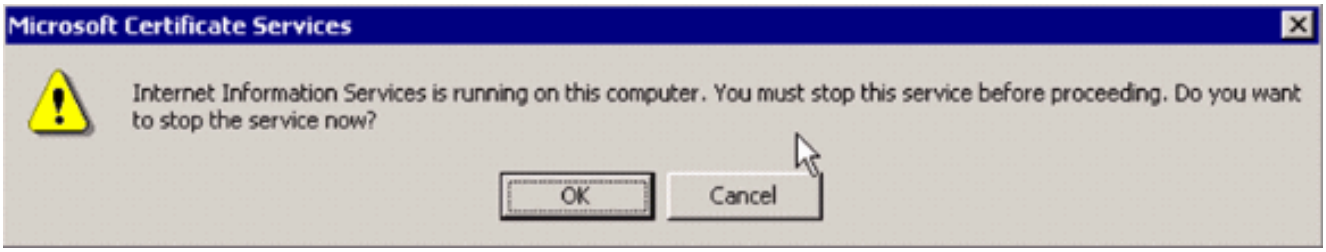
4. 选择证书颁发机构的类型您要安装。为了创建一种简单独立权限，请选择**独立根CA。**



5. 进入关于证书颁发机构的必要信息。此信息创建您的证书颁发机构的一自签名证书。切记您使用的CA名称。证书颁发机构存储在数据库的证书。此示例使用默认设置报价由Microsoft
:



6. Microsoft证书颁发机构服务使用IIS Microsoft Web服务器为了创建和管理客户端和服务器证书。它需要重新启动此的IIS服务
：



Microsoft Windows 2000服务器当前安装新的服务。您需要有您的Windows 2000服务器安装CD为了安装新窗口组件。证书颁发机构当前安装。

安装在Cisco无线LAN控制器的证书

为了使用EAP-FAST版本2和EAP-TLS在Cisco无线LAN控制器的本地EAP服务器，请遵从这三个步骤：

1. 安装在无线局域网控制器的设备证书。
2. 下载供应商CA证书到无线局域网控制器。
3. 配置无线局域网控制器使用EAP-TLS。

注意在本文显示的示例，访问控制服务器(ACS)在主机和Microsoft Active Directory一样和Microsoft证书颁发机构安装，但是配置应该是相同的，如果ACS服务器在一个不同的服务器。

安装在无线局域网控制器的设备证书

完成这些步骤：

1. .。完成这些步骤为了生成证书导入到WLC ：去**http:// <serverIpAddr>/certsrv**。选择**申请一个证书**，然后单击“下一步”。选择**高级请求**并且**其次**点击。选择**使用表单向此 CA 提交证书请求**并单击“下一步”。选择认证模板的**Web服务器**并且输入相关信息。然后请标记密钥如**可导出**。您当前接收您在您的计算机需要安装的证书。
2. 完成这些步骤为了从PC:获取证书打开Internet Explorer浏览器并且选择**工具> Internet选项>内容**。点击**证书**。最近选择从下拉菜单的预装证书。点击**出口**。**其次**两次单击并且选择**是出口专用密钥**。此格式是PKCS-12 (.PFX格式)。选择**Enable (event)强保护**。键入密码。保存它在文件<tme2.pfx>。
3. 复制在PKCS-12格式的证书到您安排Openssl安装为了转换它到PEM格式的所有计算机。

```
(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.
```

4. 下载在WLC上的已转换PEM格式化设备证书。

```
(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. 一旦重新启动，请检查证书。

```
(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
```

下载供应商CA证书到无线局域网控制器

完成这些步骤：

1. 完成这些步骤为了获取供应商CA证书：去http:// <serverIpAddr>/certsrv。选择**获取CA证书**并

且**其次**单击。选择CA证书。点击**编码的DER**。点击**下载CA证书**并且保存证书作为**rootca.cer**。

2. 转换从DER格式的CA到与**openssl x509的**PEM格式里的供应商**-在rootca.cer -通知DER - rootca.pem - outform PEM命令**。输出文件是在PEM格式的rootca.pem。
3. 下载供应商CA证书：

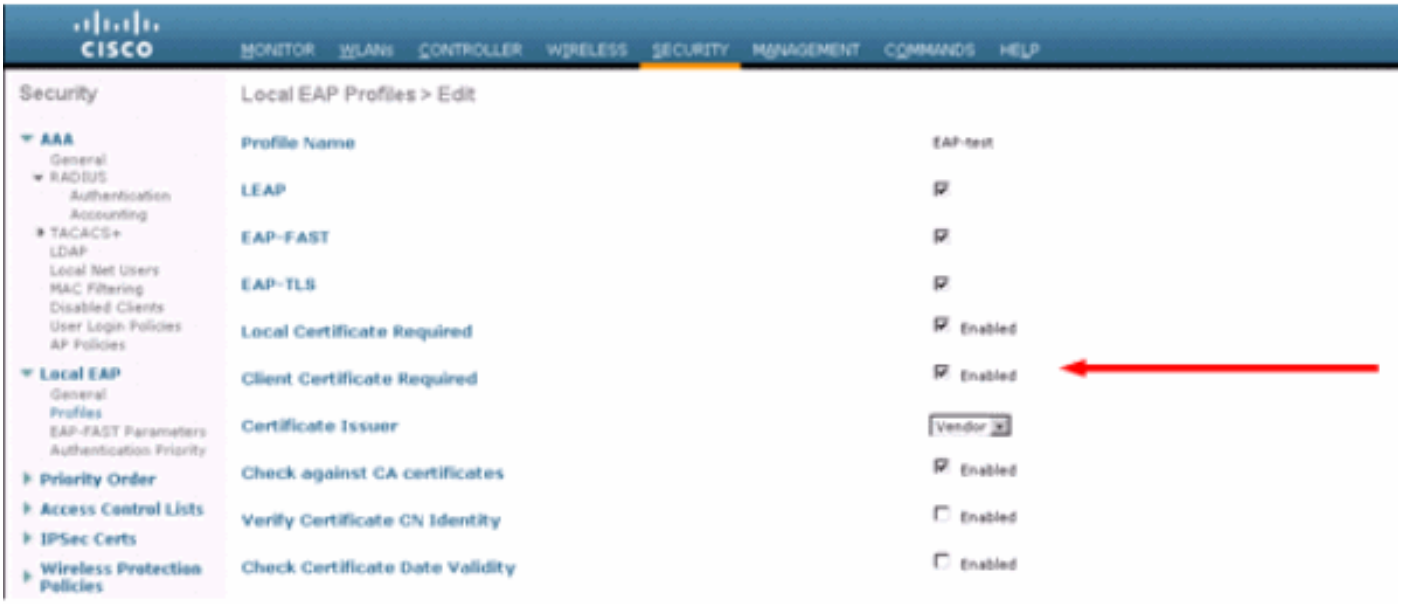
```
(Cisco Controller) >transfer download datatype eapcacert

(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.
```

配置无线局域网控制器使用EAP-TLS

完成这些步骤：

从GUI，请选择**安全>本地EAP >配置文件**，选择配置文件并且检查这些设置：

- 要求的本地证书启用。
- 要求的客户端证书启用。
- 证书发布者是供应商。
- CA证书的检查启用。



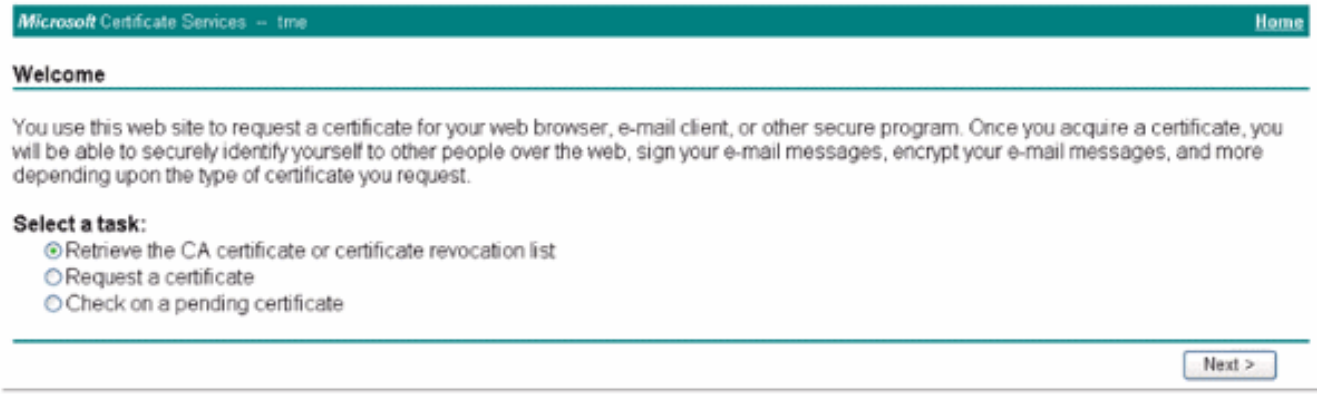
安装在客户端设备的认证机关证书

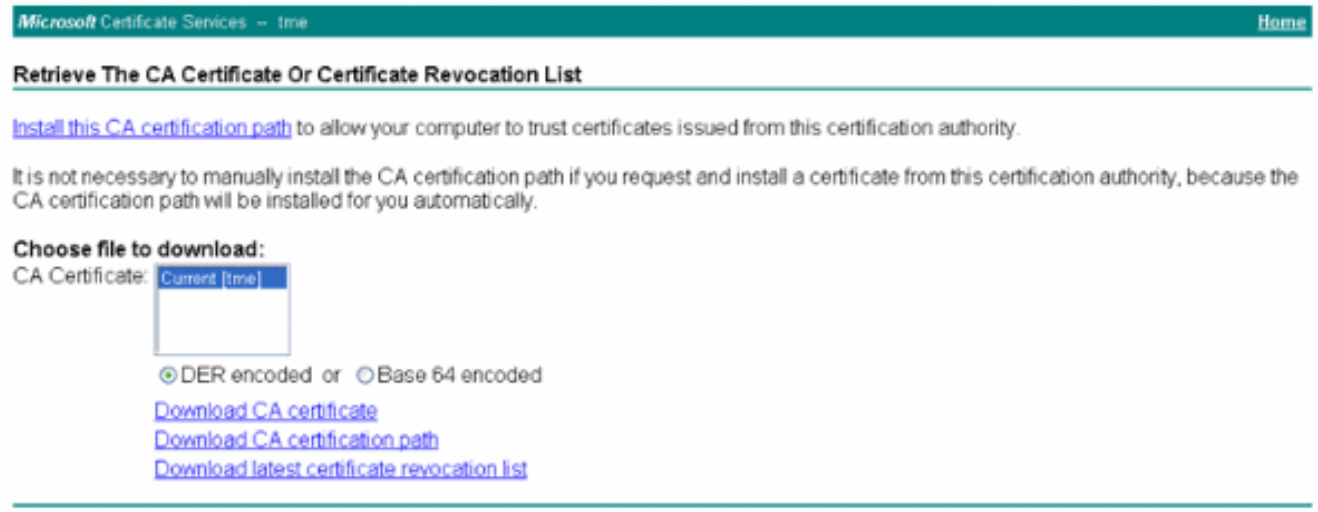
下载并且安装客户端的根CA证书

客户端必须从认证授权服务器获取根CA证书。有您在Windows XP计算机能使用获取客户端证书和安装它的几个方法。为了获取有效证书， Windows XP用户必须登陆使用他们的用户ID，并且必须有网络连接。

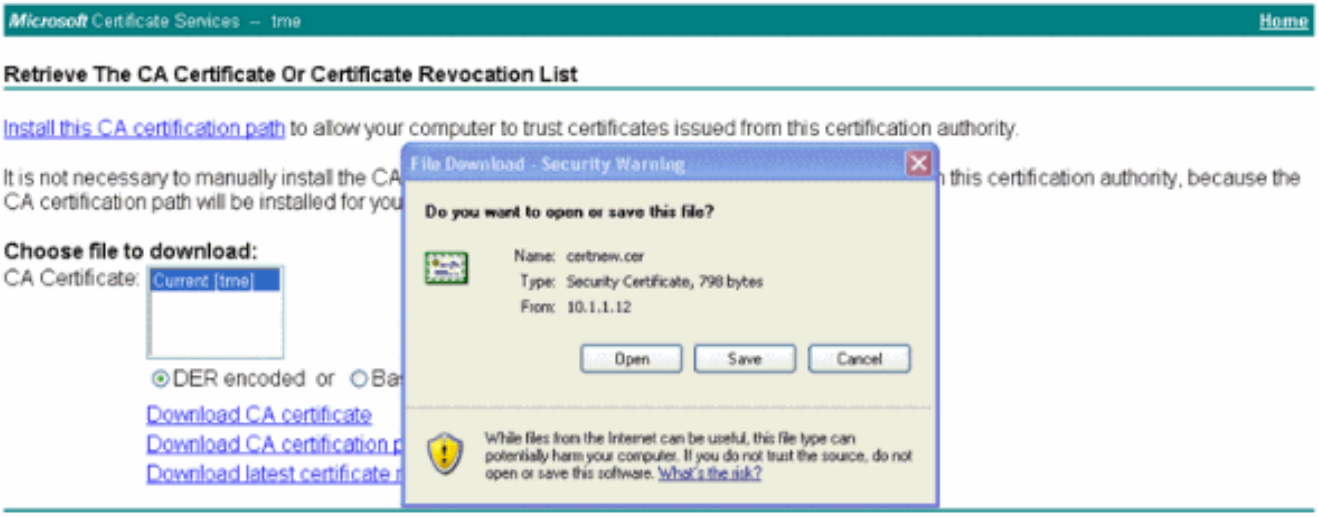
在Windows XP客户端的一Web浏览器和对网络的一个有线连接使用从专用根认证中心服务器获取客户端证书。此步骤使用从Microsoft认证授权服务器获取客户端证书：

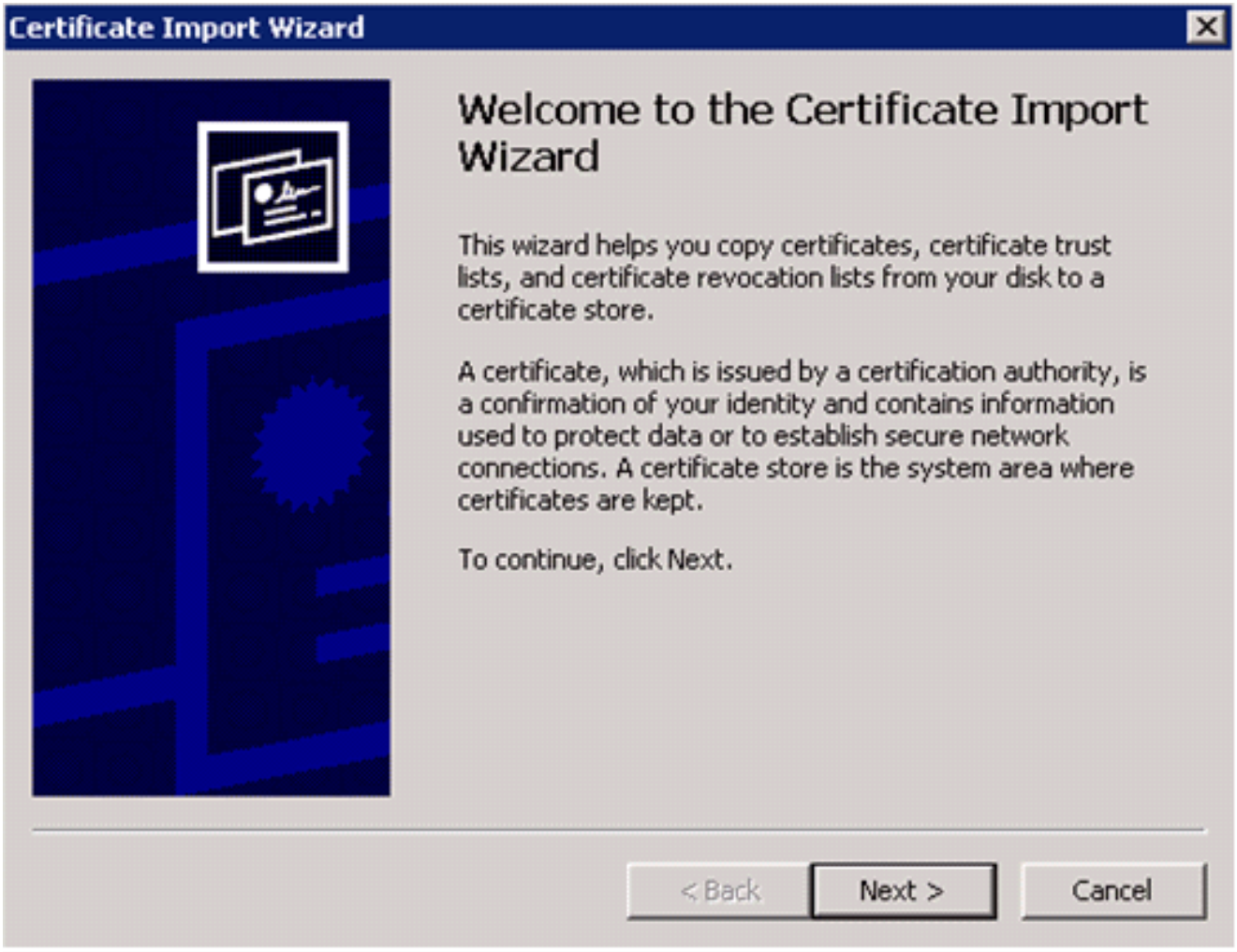
1. 请使用在客户端的一Web浏览器并且点浏览器认证授权服务器。为了执行此，请输入**http://IP-address-of-Root-CA/certsrv**。
2. 登陆使用**Domain_name \ user_name**。您必须登陆使用是使用XP客户端人的用户名。
3. 在Welcome窗口，请选择**获取CA证书**并且**其次**单击。
4. 选择**编码的Base64**并且**下载CA证书**。
5. 在证书发出的窗口，请点击**安装此证书**并且**其次**单击。
6. **自动地**选择**精选证书存储**并且为成功的导入消息**其次**单击。
7. 连接给获取的认证机关证书证书颁发机构
   ：

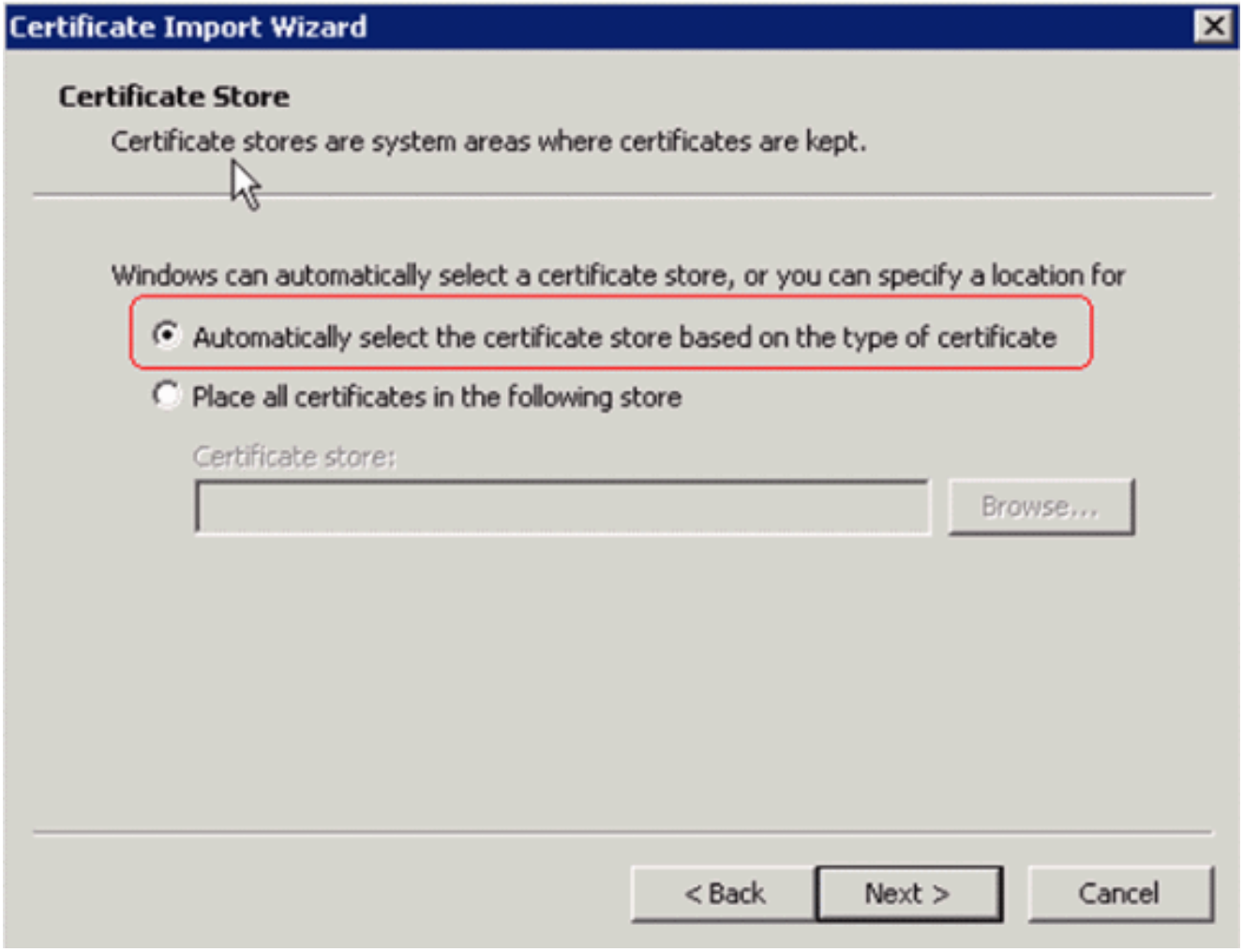

Microsoft Certificate Services -- tme
Home
Welcome
You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt 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
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:
Current [tme]
DER encoded or Base 64 encoded
Download CA certificate
Download CA certification path
Download latest certificate revocation list

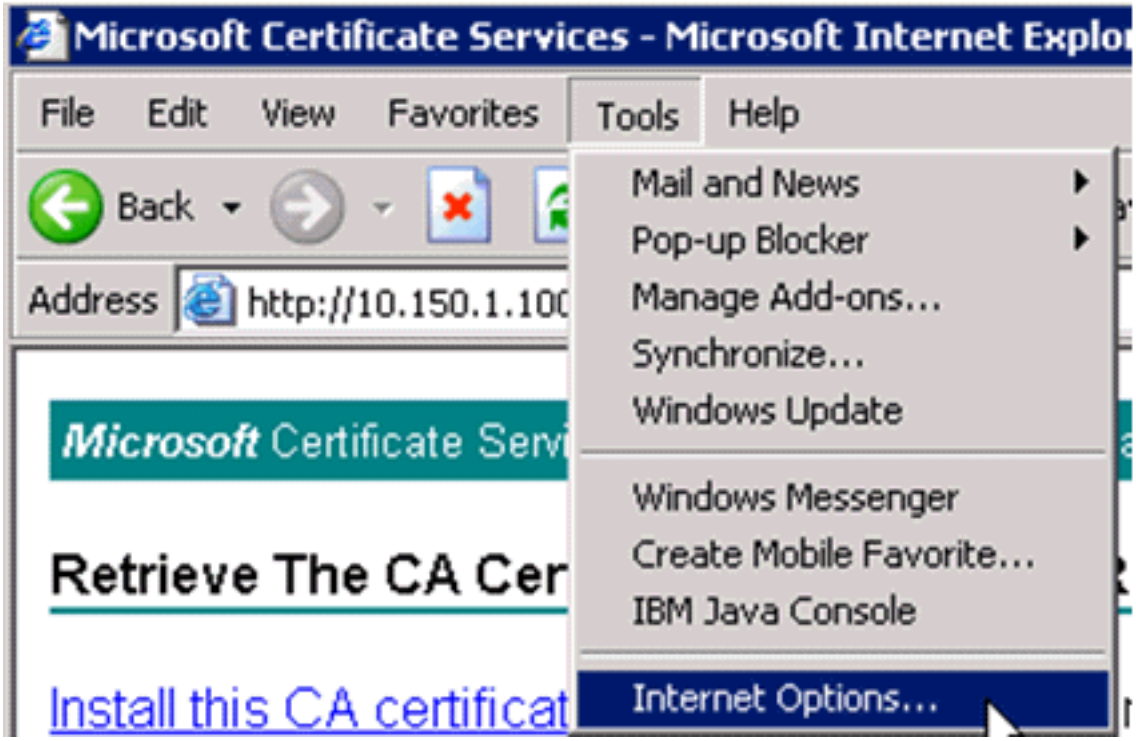
8. 单击**下载 CA 证书**。

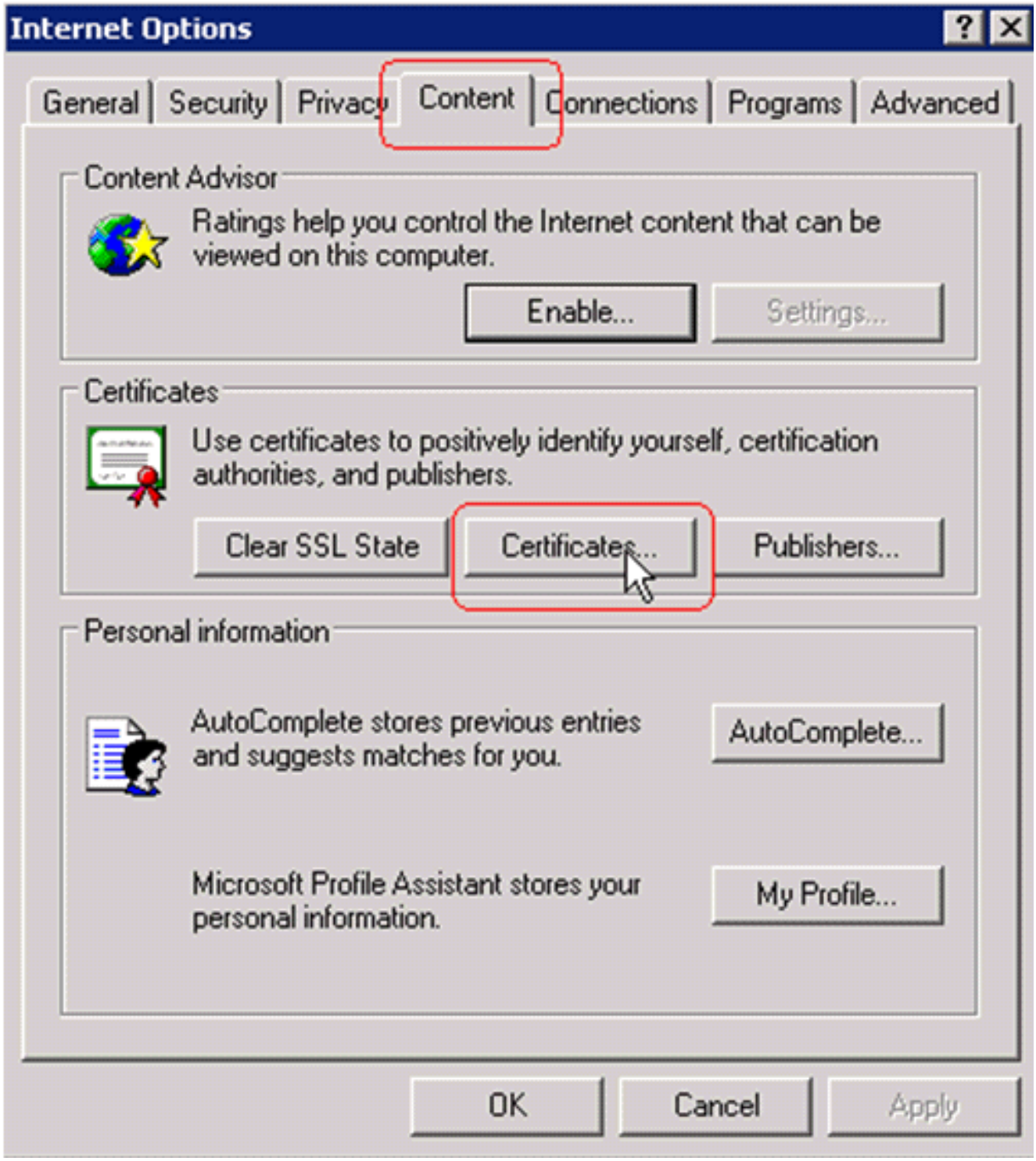

Microsoft Certificate Services -- tme
Home
Retrieve The CA Certificate Or Certificate Revocation List
Install this CA certification path to allow your computer to trust certificates issued from this certification authority.
Choose file to download:
CA Certificate:
Current [tme]
Download CA certificate
File Download - Security Warning
Do you want to open or save this file?
Name: certnew.cer
Type: Security Certificate, 798 bytes
From: 10.1.1.12
Open
Save
Cancel
While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open or save this software. What's the risk?


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

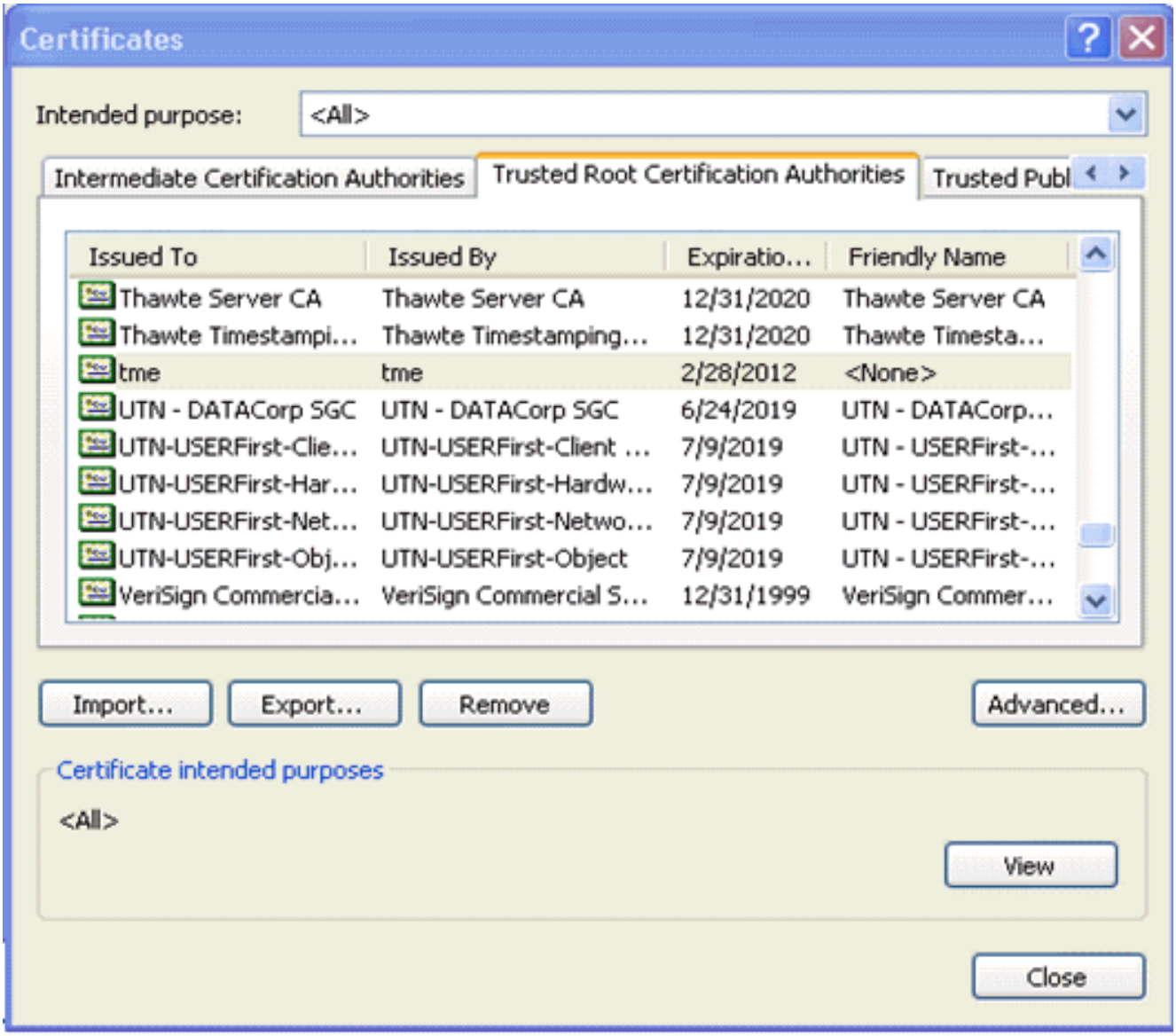

Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for
Automatically select the certificate store based on the type of certificate
Place all certificates in the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

9. 为了检查认证机关授权正确地安装，开放Internet Explorer和选择**工具> Internet选项>内容>证书**。





在可靠的根证书颁发机构，您应该看到您的最近安装的证书颁发机构：



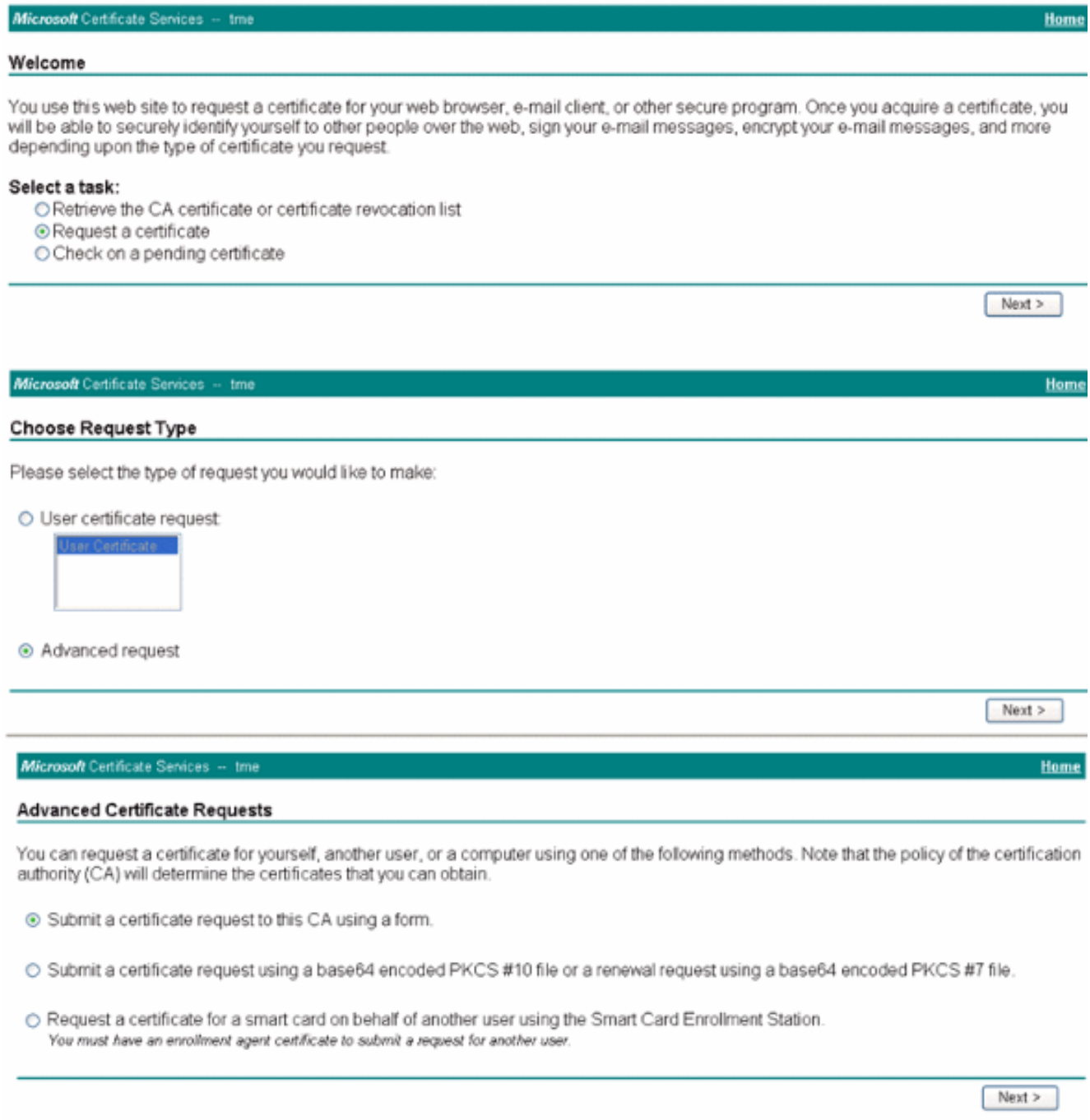
生成客户端设备的客户端证书

客户端必须从WLC的一个认证授权服务器获取证书能验证WLAN EAP-TLS客户端。有您在Windows XP计算机能使用为了获取客户端证书和安装它的几个方法。为了获取有效证书，Windows XP用户必须登陆使用他们的用户ID，并且必须有网络连接(一个有线连接或一WLAN连接与禁用的802.1x安全)。

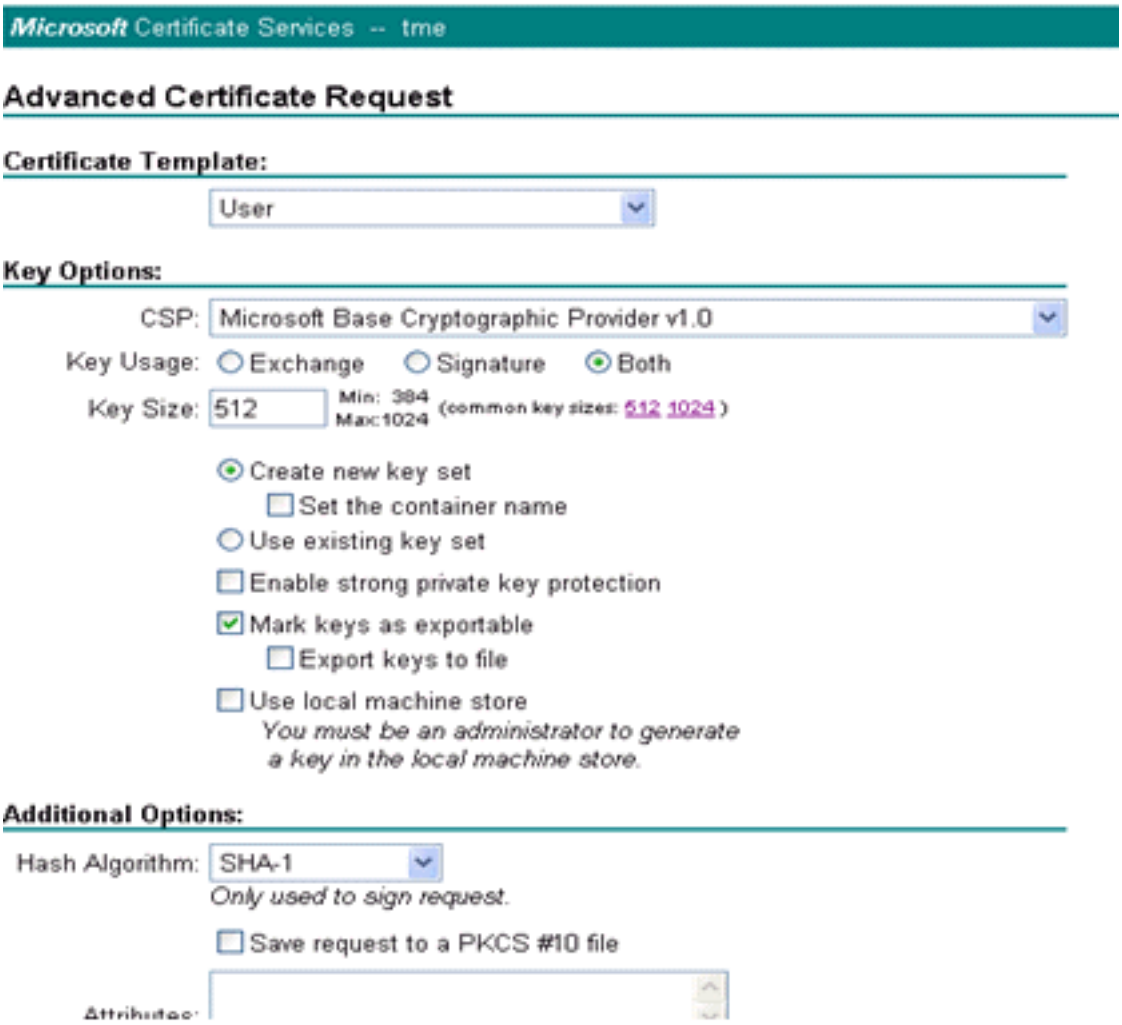
在Windows XP客户端的一Web浏览器和对网络的一个有线连接用于从专用根认证中心服务器获取客户端证书。此步骤使用从Microsoft认证授权服务器获取客户端证书：

1. 请使用在客户端的一Web浏览器并且点浏览器认证授权服务器。为了执行此，请输入**http://IP-address-of-Root-CA/certsrv**。
2. 登陆使用**Domain_name \ user_name**。您必须登陆使用使用XP客户端人的用户名。(用户名获得被嵌入到客户端证书。)
3. 在Welcome窗口，请选择**请求证书**并且**其次**单击。
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Advanced Certificate请求表，请选择认证模板作为**用户**，指定密钥大小， **1024**并且单击**提交**。
7. 在证书发出的窗口，请点击**安装此证书**。这一个客户端证书的成功的安装在Windows XP客户

端的导致。

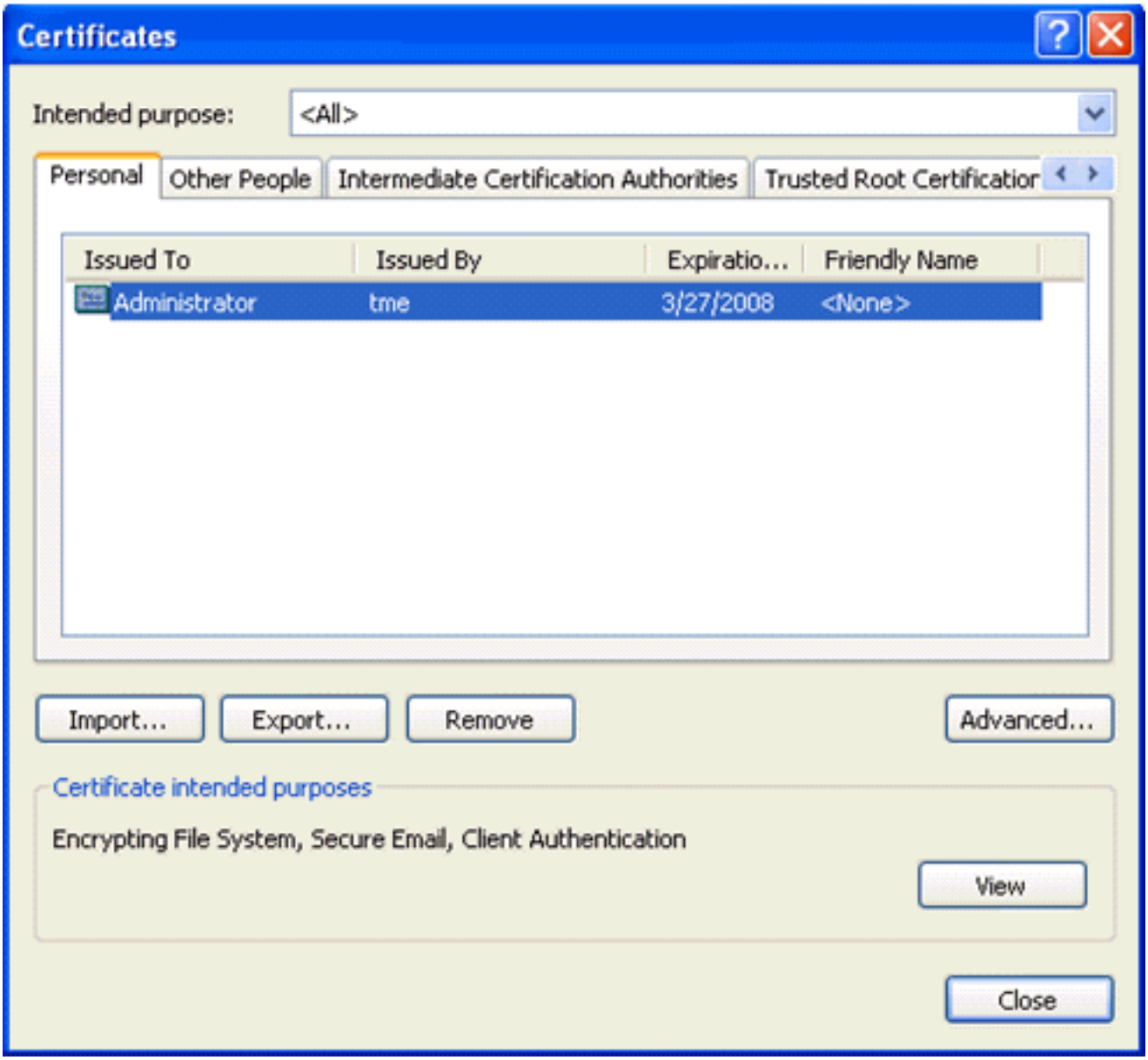


8. 选择**客户端身份验证证书**。



客户端证书当前创建。

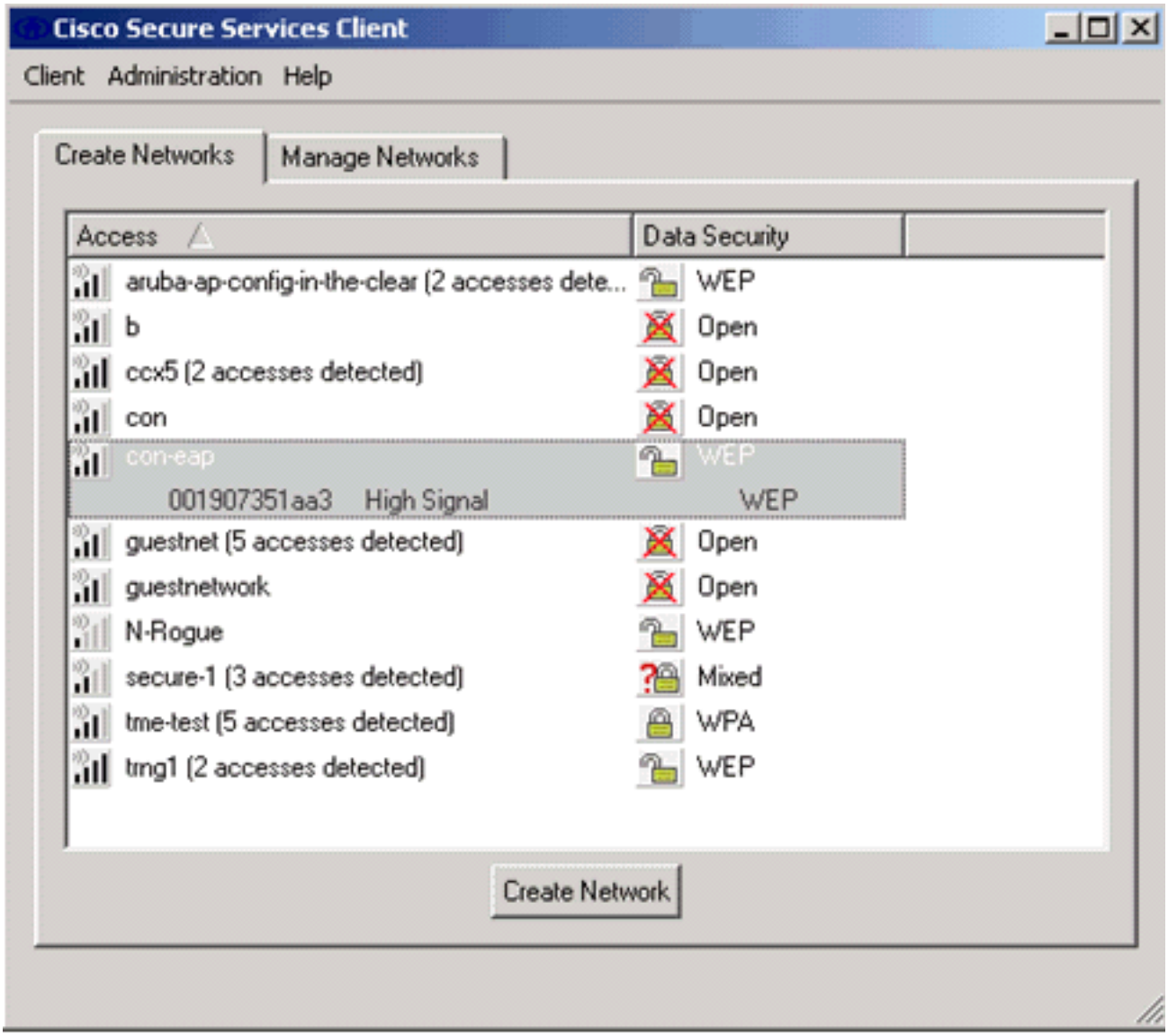
9. 为了检查证书安装，请去Internet Explorer并且选择**工具> Internet选项>内容>证书**。在个人选项，您应该看到证书。



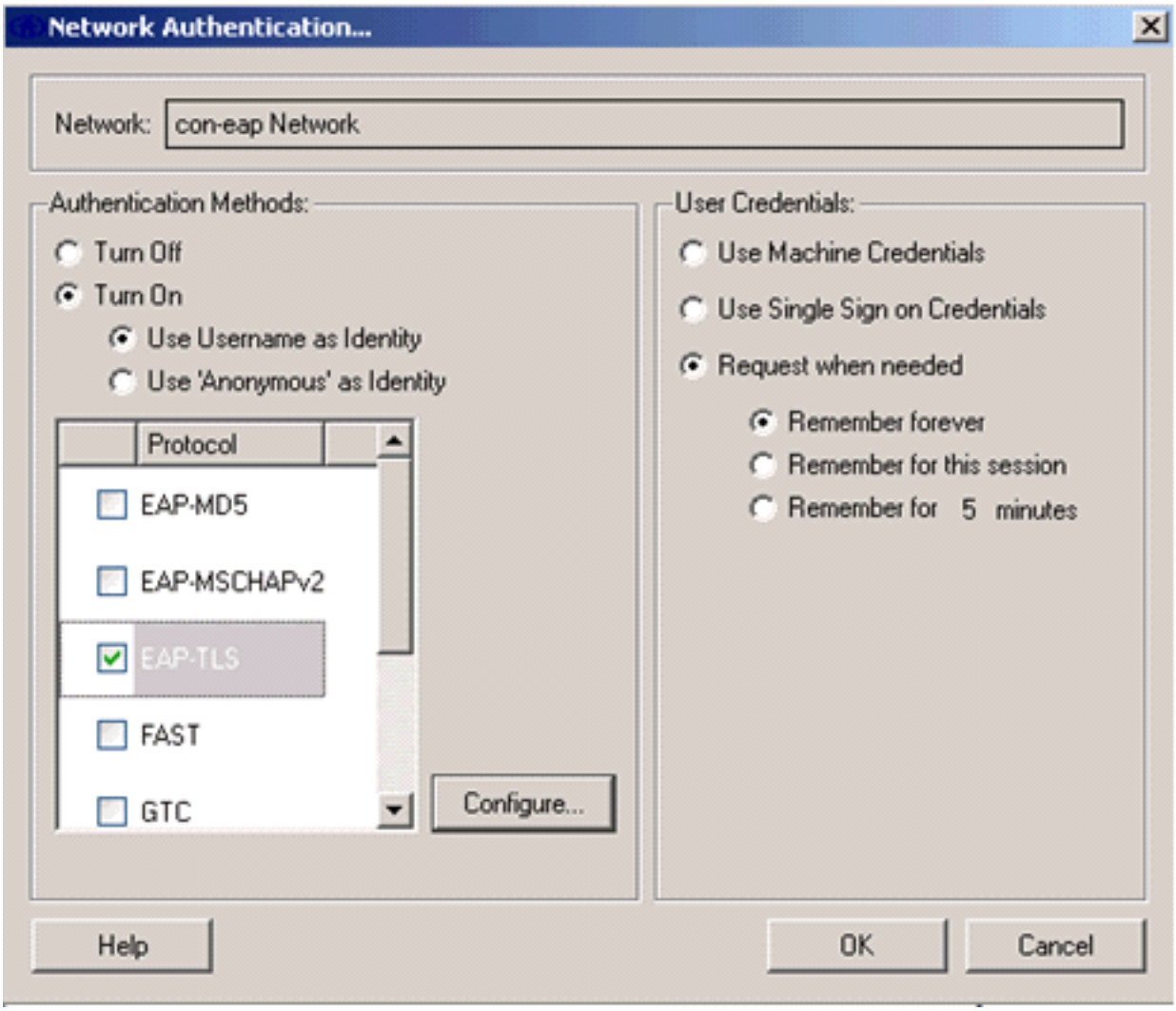
与思科安全服务客户端的EAP-TLS客户端设备的

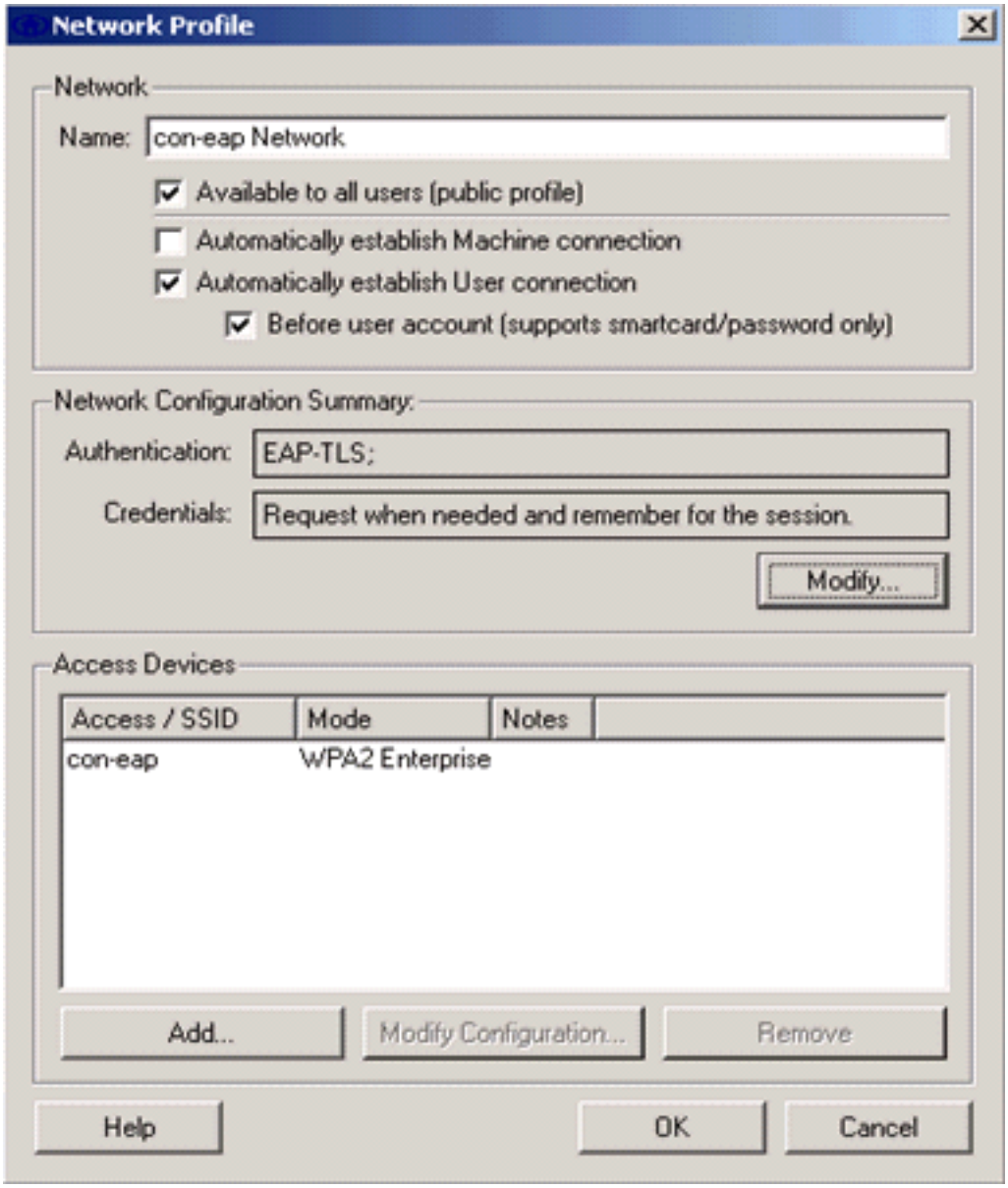
完成这些步骤：

1. 默认情况下， WLC广播SSID，因此在被扫描的Ssid创建网络列表显示。为了创建网络配置文件，您能点击在列表(企业)的SSID并且单击**创建网络**。如果WLAN基础设施配置与禁用的广播SSID，您必须手工添加SSID。为了执行此，请单击**添加**在接入设备下和手工输入适当的SSID (例如，企业)。配置客户端的活动探测器行为。即其中其已配置的SSID的积极地客户端探测器。在“Add Access Device”窗口中输入 SSID 之后，指定 **Actively search for this access device**。**注意：** 如果不是首次为配置文件配置 EAP 身份验证设置，则端口设置不允许企业模式 (802.1X)。
2. 单击**创建网络**为了启动网络配置文件窗口，允许您连结选定的(或配置) SSID与认证机制。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，可以关联多种 WLAN 安全类型和/或 SSID。

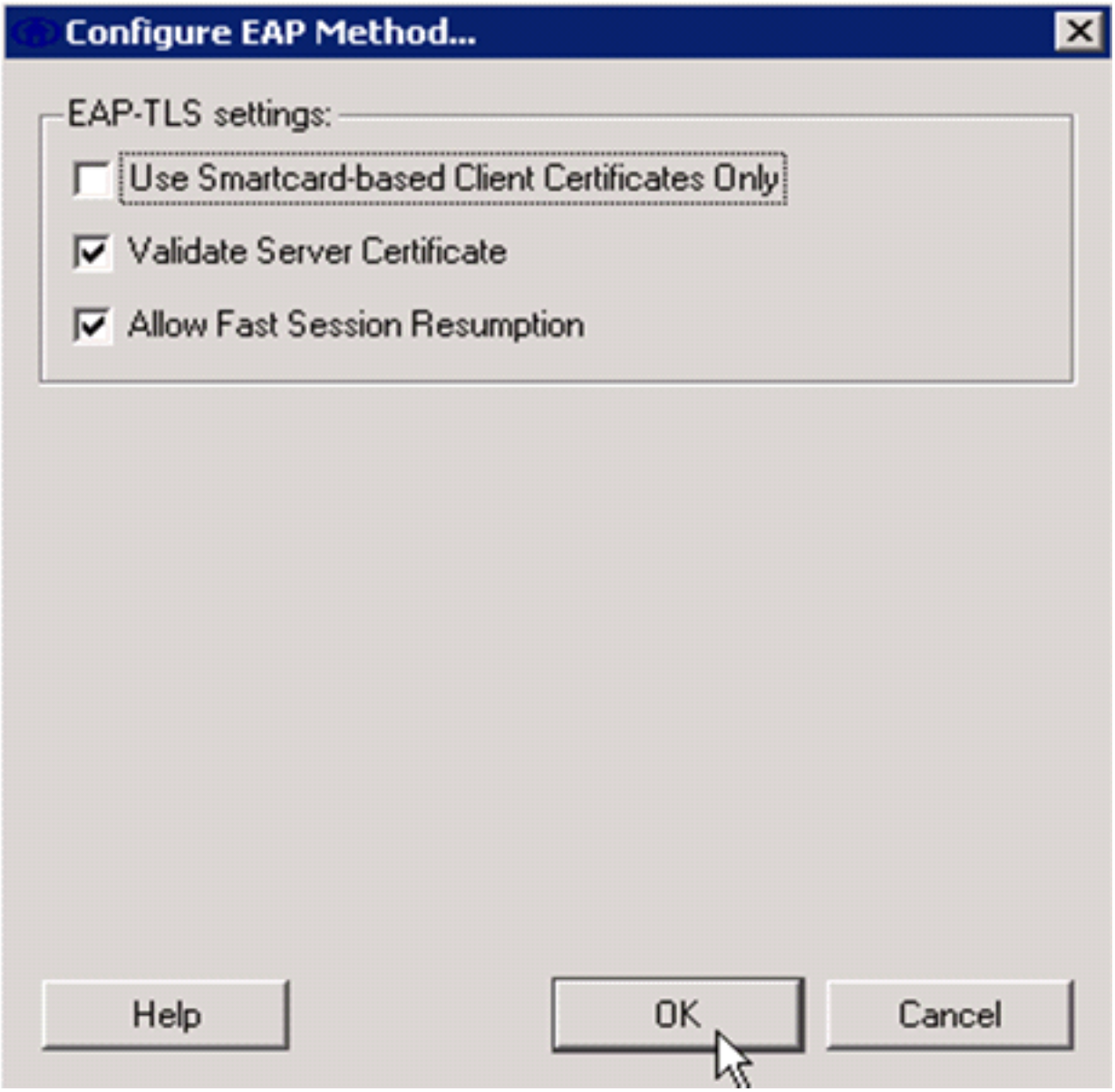


3. 打开验证并且检查EAP-TLS方法。然后请单击**配置**为了配置EAP-TLS属性。
4. 在网络配置摘要下，请点击**修改**为了配置EAP/凭证设置。
5. 指定**打开验证**，选择**EAP-TLS**在协议下，并且选择**用户名**作为标识。
6. 指定 **Use Single Sign on Credentials**，以使用登录凭据进行网络身份验证。单击**配置**设置EAP-TLS参数。

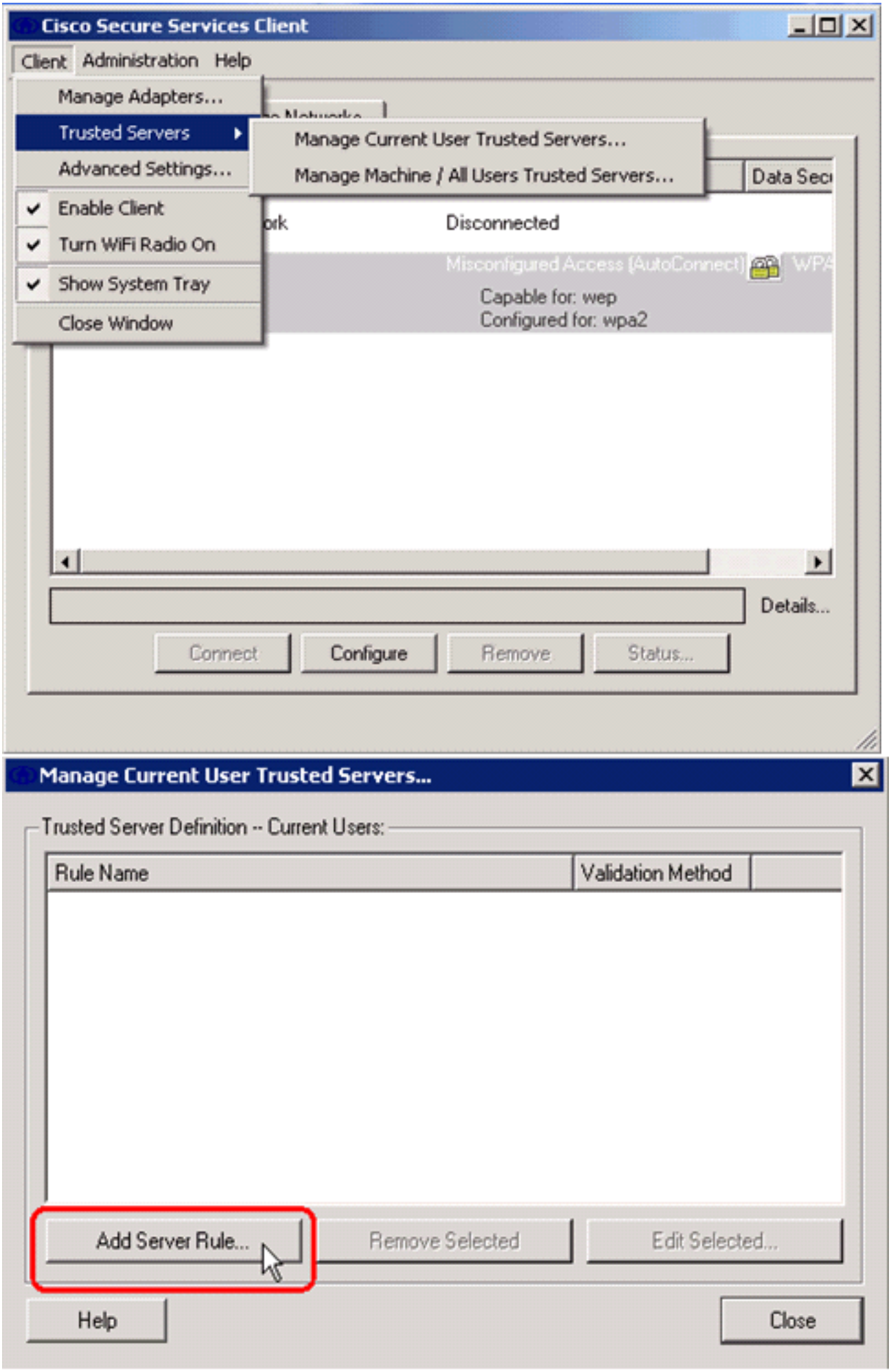

Network Authentication...
Network:
con-eap Network
Authentication Methods:
Turn Off
Turn On
Use Username as Identity
Use 'Anonymous' as Identity
Protocol
EAP-MD5
EAP-MSCHAPv2
EAP-TLS
FAST
GTC
Configure...
User Credentials:
Use Machine Credentials
Use Single Sign on Credentials
Request when needed
Remember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



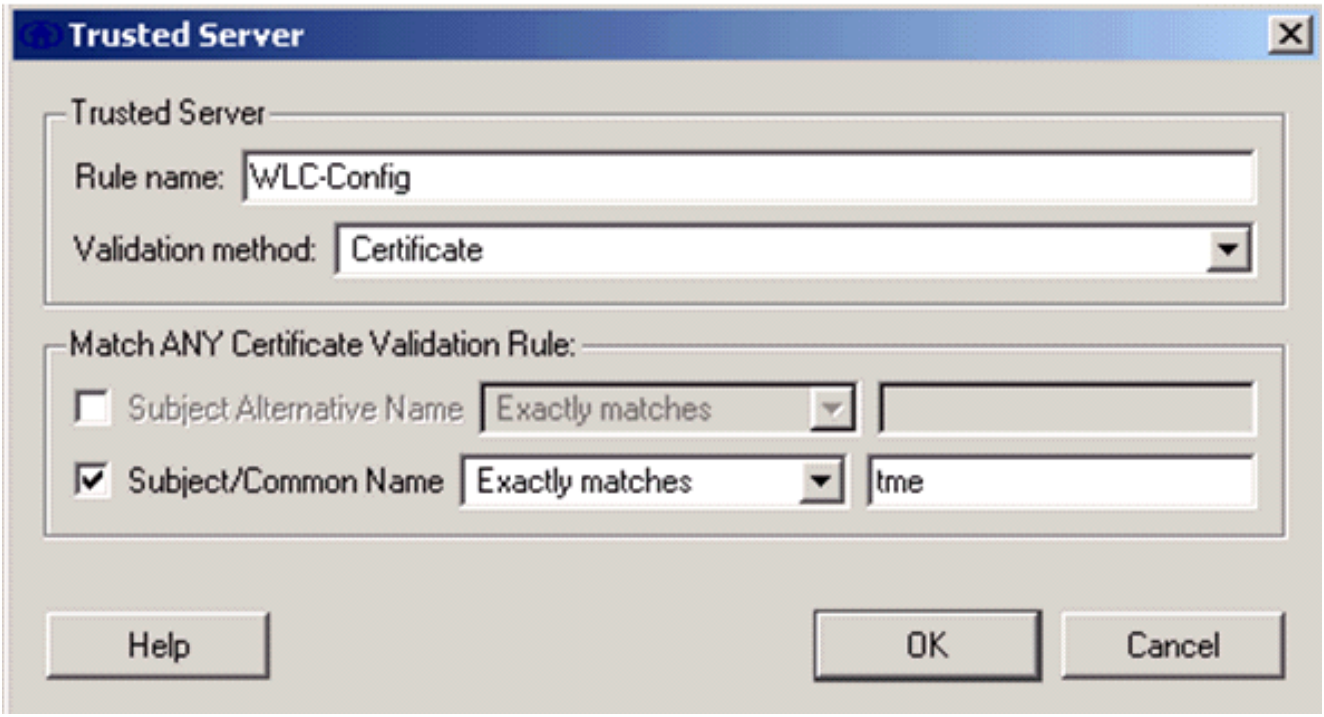
7. 为了有您需要检查RADIUS服务器证书的一获取的EAP-TLS配置。为了执行此，检查**验证服务器证书**。



8. 为了验证RADIUS服务器证书，您需要提供思科安全服务客户端信息为了接受仅正确证书。选择**Client>委托服务器>管理当前用户委托服务器。**

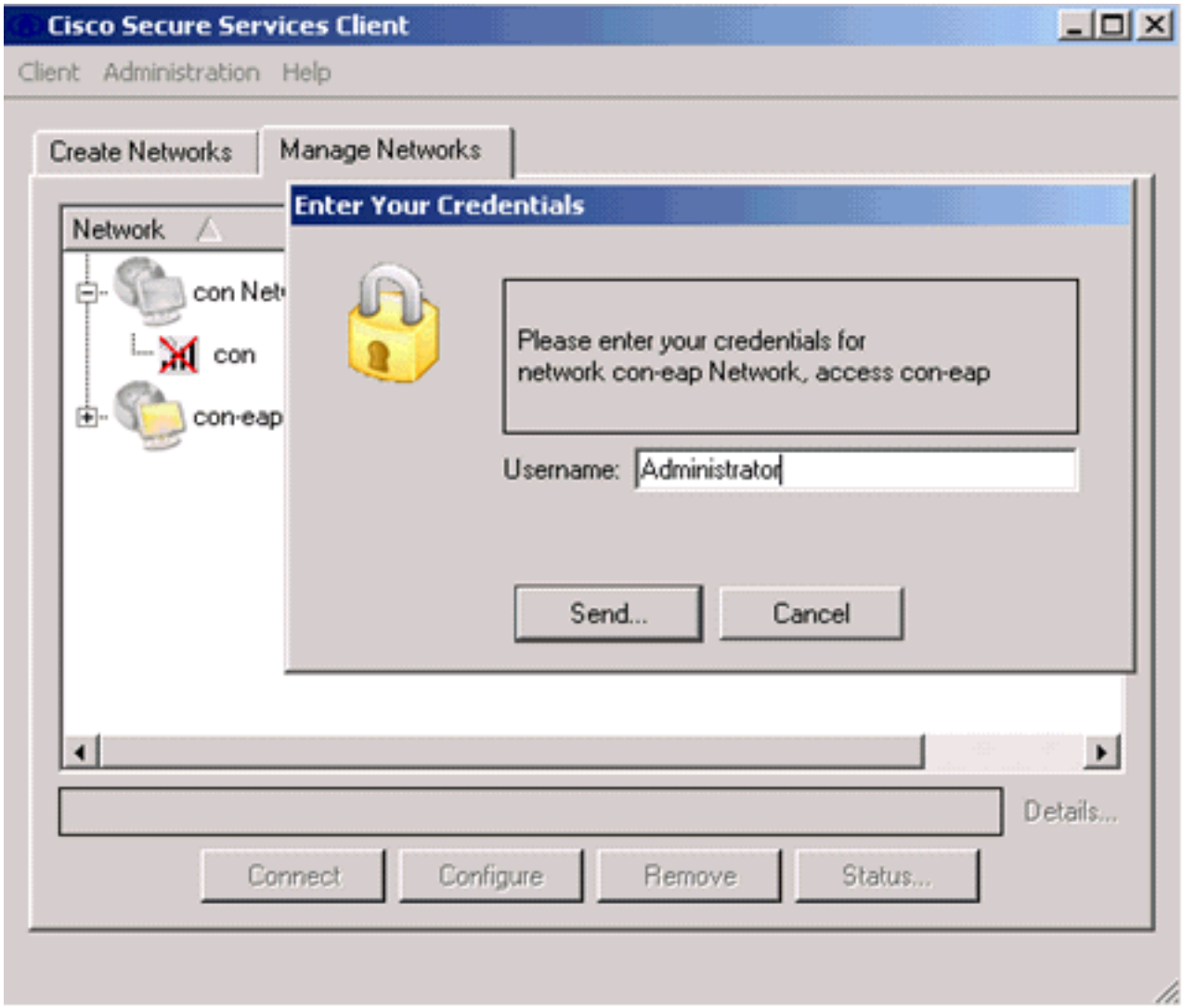


9. 给予一名称对于规则并且检查服务器证书的名称。



EAP-TLS配置完成。

10. 对无线网络配置文件的连接。思科安全服务客户端请求用户登录

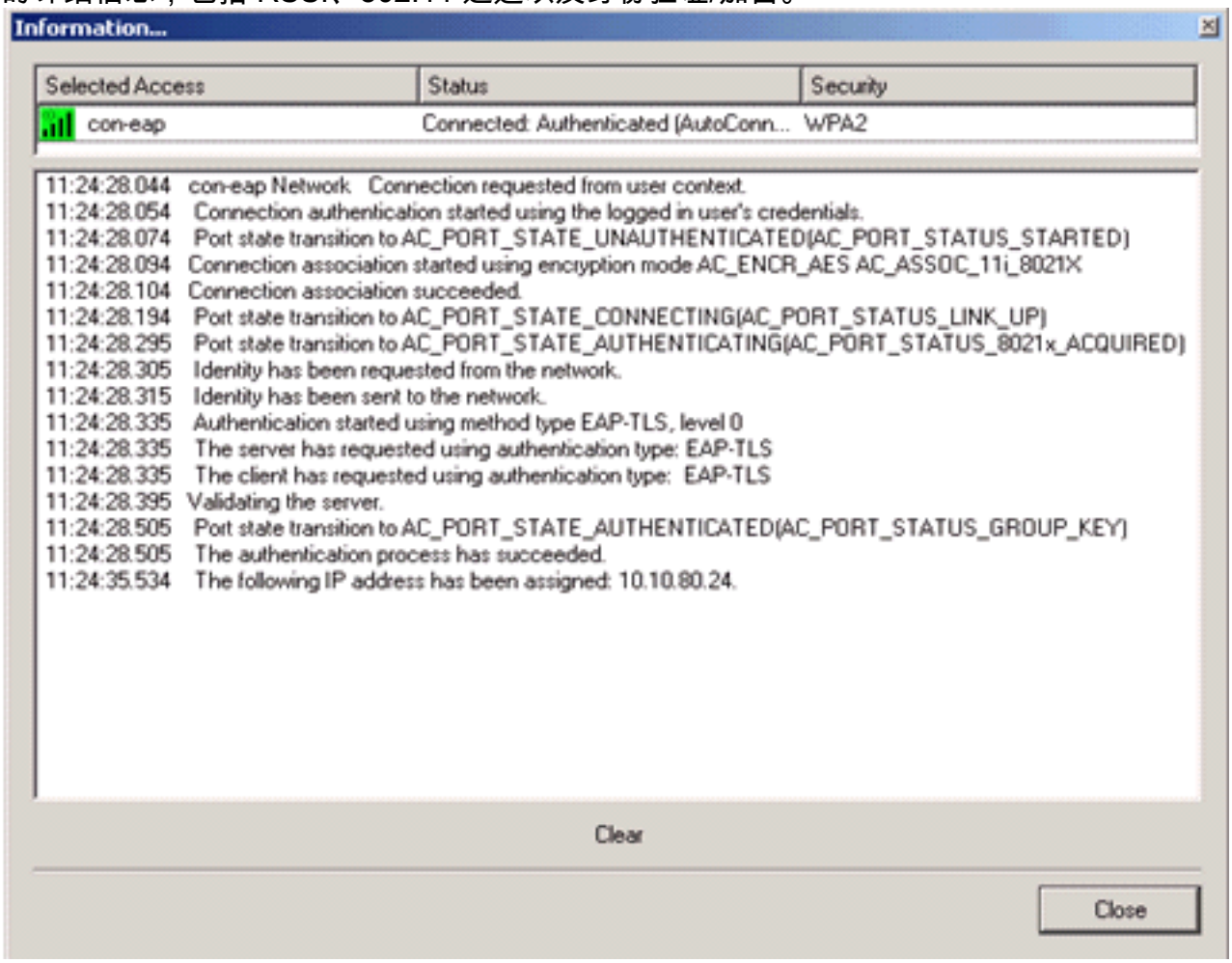


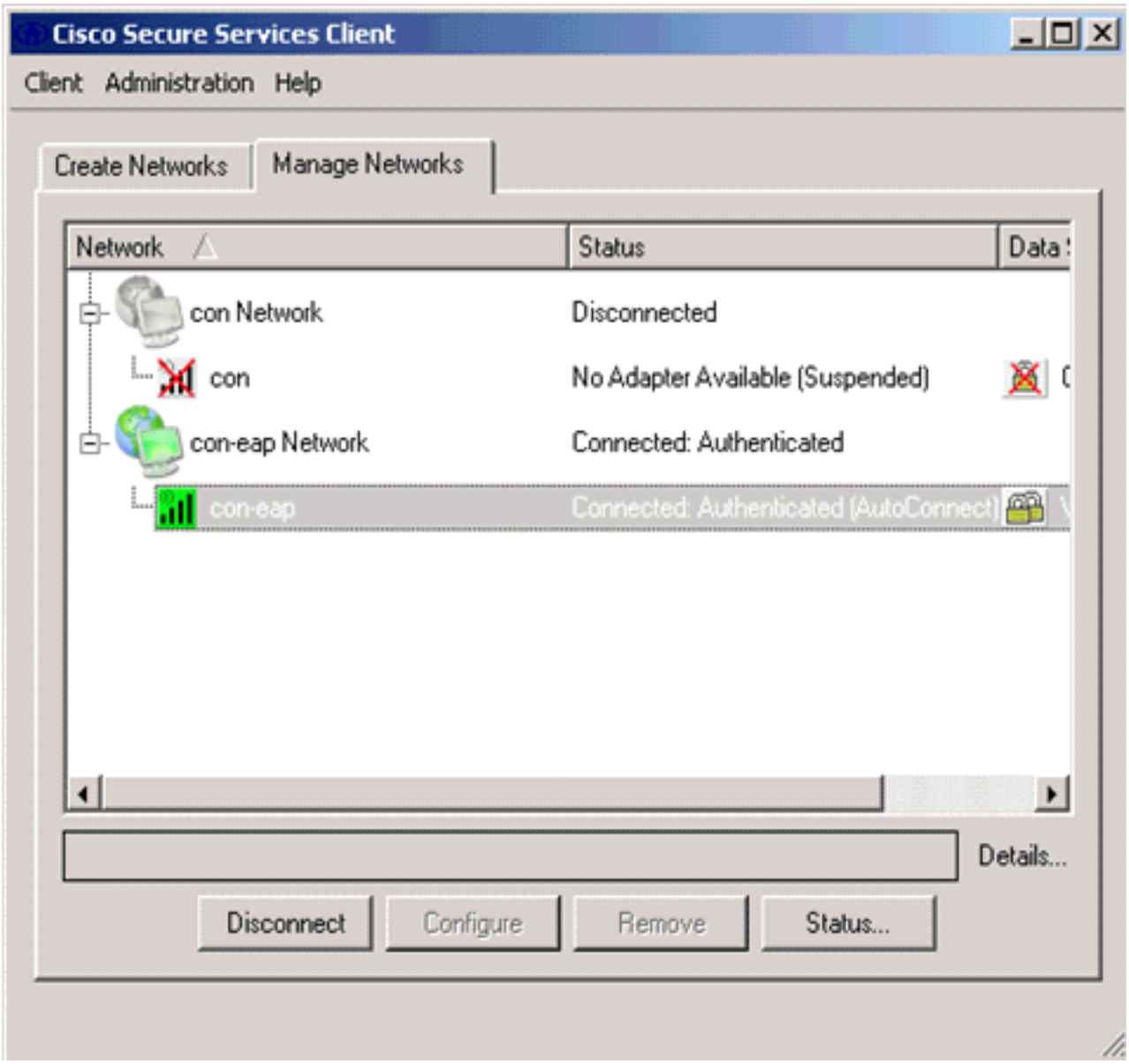
：

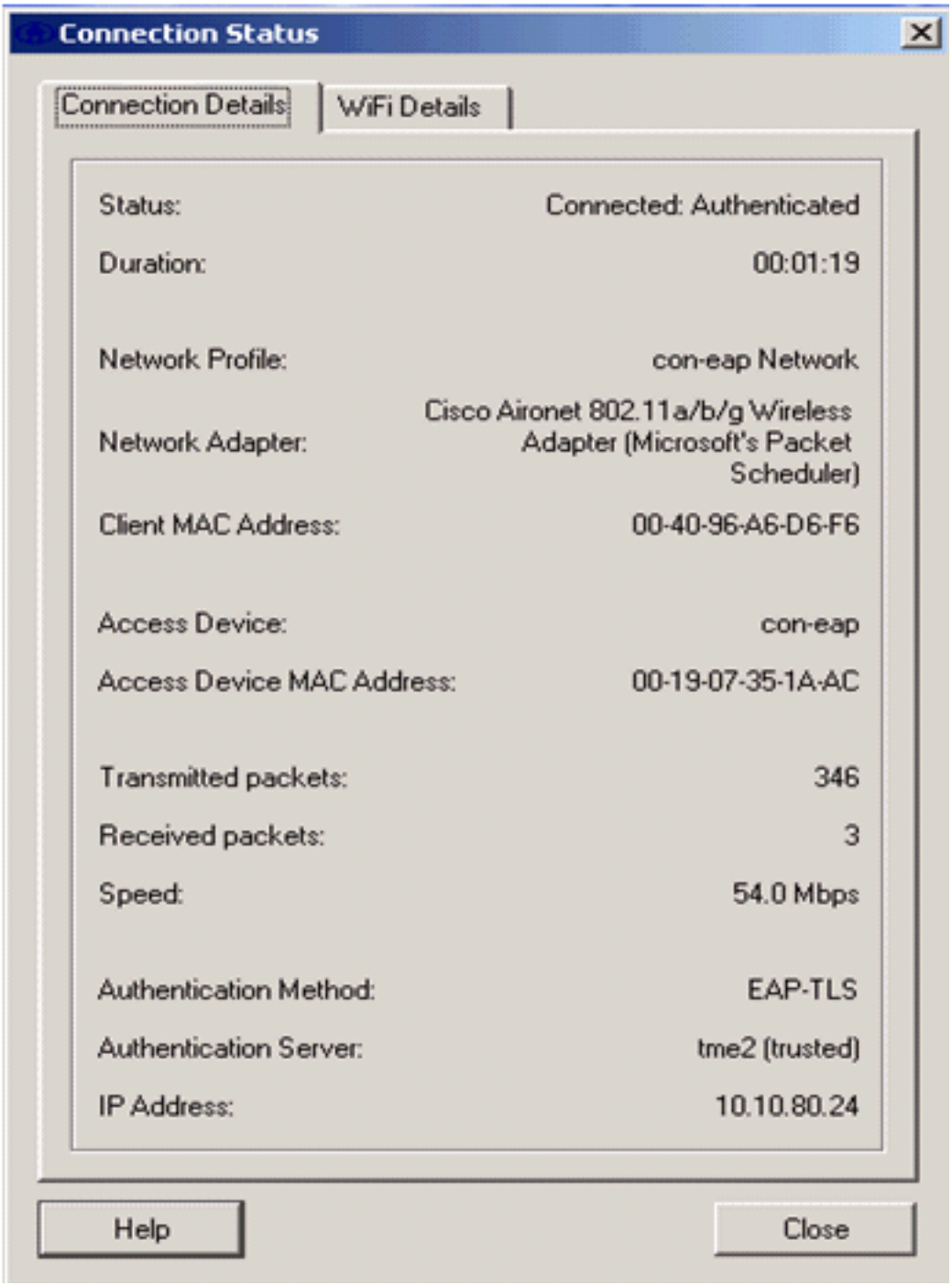
思科安全服务客户端接收服务器证书并且检查它(当规则配置的和证书颁发机构安装)。它然后请求证书使用用户。

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...



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

这些调试指令可以被使用在WLC监控认证交换的进度：

- **debug aaa events enable**
- **debug aaa detail enable**
- **debug dot1x events enable**
- **debug dot1x states enable**
- **debug aaa local-auth eap事件enable (event)**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