Exemplo de configuração de servidor EAP local de rede sem fio unificada

Contents

Introduction

Este documento descreve a configuração de um servidor local de Extensible Authentication Protocol (EAP) em um Controlador de LAN Wireless (WLC) da Cisco para a autenticação dos usuários sem fio.

O EAP local é um método de autenticação que permite que usuários e clientes sem fio sejam autenticados localmente. Ele foi projetado para uso em escritórios remotos que desejam manter a conectividade com clientes sem fio quando o sistema back-end for interrompido ou o servidor de autenticação externo for desativado. Quando você habilita o EAP local, o controlador serve como o servidor de autenticação e o banco de dados de usuário local, removendo assim a dependência de um servidor de autenticação externo. O EAP local recupera as credenciais do usuário do banco de dados de usuário local ou do banco de dados back-end LDAP (Lightweight Diretory Access Protocol) para autenticar usuários. O EAP local suporta EAP Lightweight (LEAP), autenticação EAP-Flexible via Secure Tunneling (EAP-FAST) e autenticação EAP-Transport Layer Security (EAP-TLS) entre o controlador e os clientes sem fio.

Observe que o servidor EAP local não está disponível se houver uma configuração de servidor

RADIUS externo global na WLC. Todas as solicitações de autenticação são encaminhadas para o RADIUS externo global até que o Servidor EAP local esteja disponível. Se a WLC perder conectividade com o servidor RADIUS externo, o servidor EAP local se tornará ativo. Se não houver configuração global do servidor RADIUS, o servidor EAP local se tornará imediatamente ativo. O servidor EAP local não pode ser usado para autenticar clientes, que estão conectados a outras WLCs. Em outras palavras, uma WLC não pode encaminhar sua solicitação de EAP para outra WLC para autenticação. Cada WLC deve ter seu próprio servidor EAP local e banco de dados individual.

Observação: use estes comandos para impedir que o WLC envie solicitações a um servidor radius externo .

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

O servidor EAP local suporta estes protocolos na versão de software 4.1.171.0 e posterior:

- LEAP
- EAP-FAST (nome de usuário/senha e certificados)
- EAP-TLS

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento de como configurar WLCs e pontos de acesso lightweight (LAPs) para operação básica
- Conhecimento de Lightweight Access Point Protocol (LWAPP) e métodos de segurança sem fio
- Conhecimento básico da autenticação EAP local.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Windows XP com placa de adaptador CB21AG e Cisco Secure Services Client versão 4.05
- Controlador de LAN sem fio Cisco 4400 4.1.171.0
- Autoridade de Certificação da Microsoft no servidor Windows 2000

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

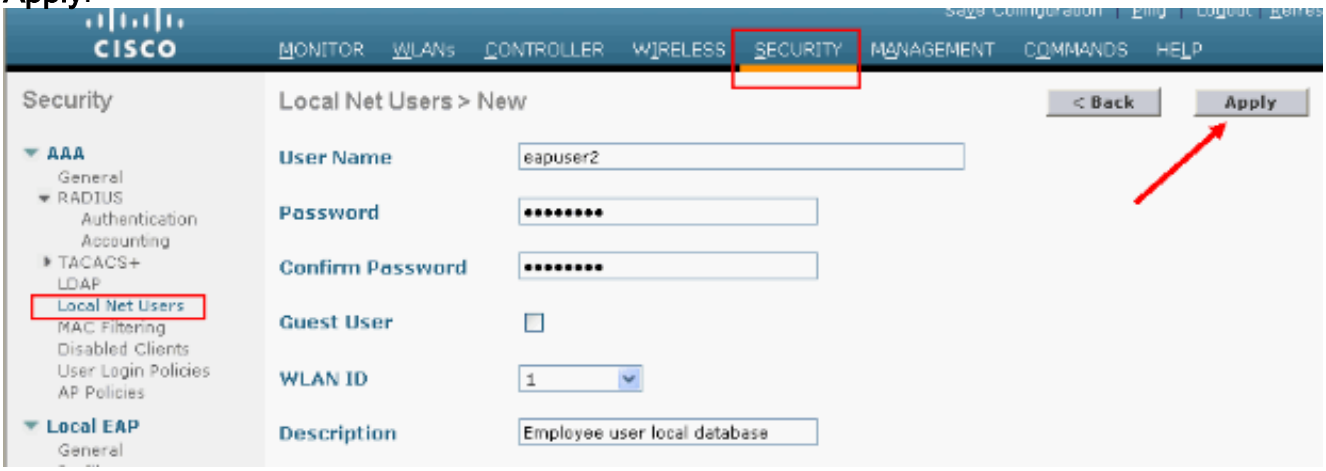
Configurar o EAP local no Cisco Wireless LAN Controller

Este documento pressupõe que a configuração básica da WLC já está concluída.

Configuração de EAP local

Conclua estes passos para configurar o EAP local:

1. Adicionar um usuário de rede local:Na GUI. escolha **Security > Local Net Users > New**, insira User Name, Password, Guest User, WLAN ID e Description e clique em **Apply**.



Na CLI, você pode usar o **comando config netuser add *<username>* *<password>*<WLAN id>*<description>*:Observação:** esse comando foi reduzido para uma segunda linha devido a razões espaciais.

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

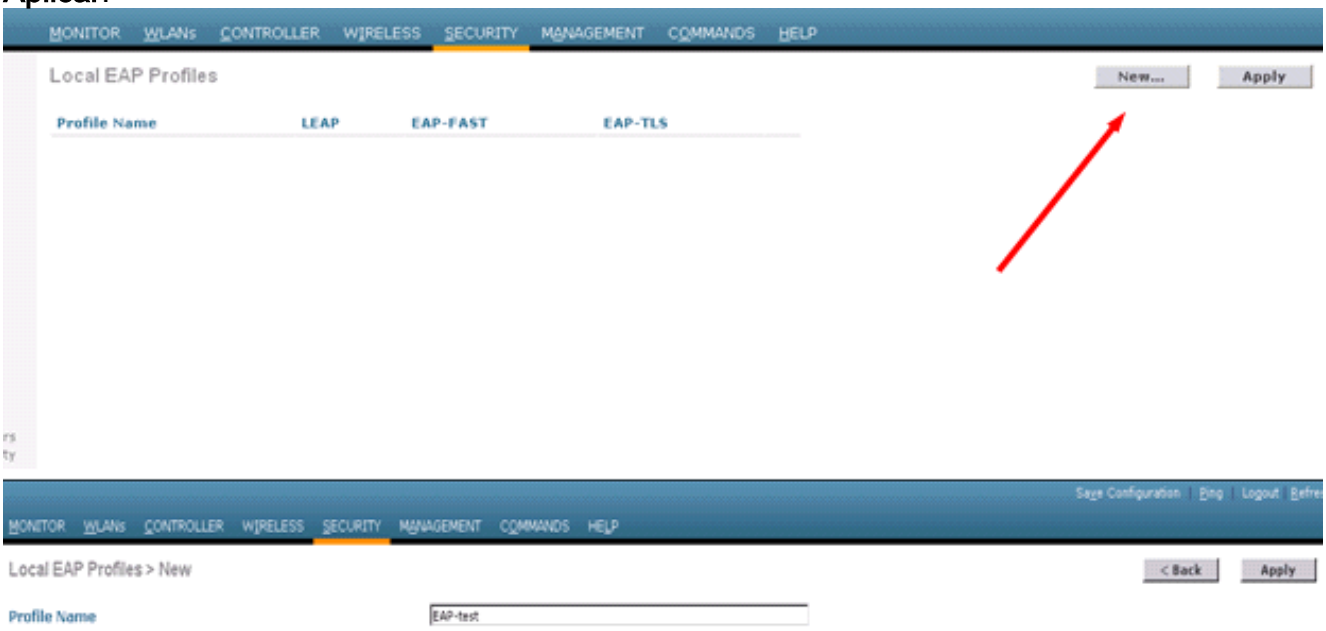
2. Especifique a ordem de recuperação de credenciais do usuário.Na GUI, escolha **Security > Local EAP > Authentication Priority**. Em seguida, selecione LDAP, clique no botão "<" e clique em **Apply**. Isso coloca as credenciais do usuário no banco de dados local primeiro.

Na CLI:

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

3. Adicionar um perfil EAP:Para fazer isso na GUI, escolha **Security > Local EAP > Profiles** e clique em **New**. Quando a nova janela for exibida, digite o Nome do perfil e clique em

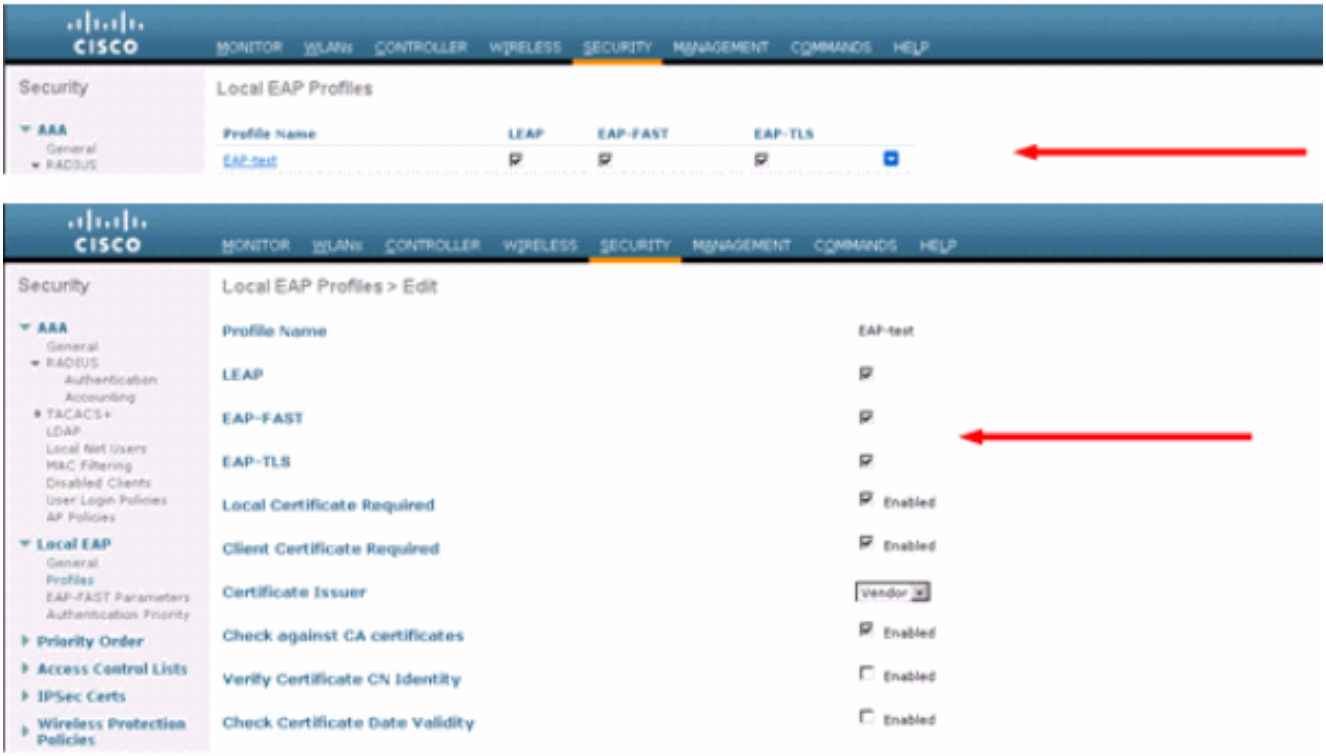
Aplicar.



Você também pode fazer isso usando o comando CLI **config local-auth eap-profile add *<profile-name>*.** No nosso exemplo, o nome do perfil é *EAP-test*.

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

4. Adicione um método ao perfil EAP.Na GUI, escolha **Security > Local EAP > Profiles** e clique no nome do perfil para o qual deseja adicionar os métodos de autenticação. Este exemplo usa LEAP, EAP-FAST e EAP-TLS. Clique em **Apply** para definir os métodos.

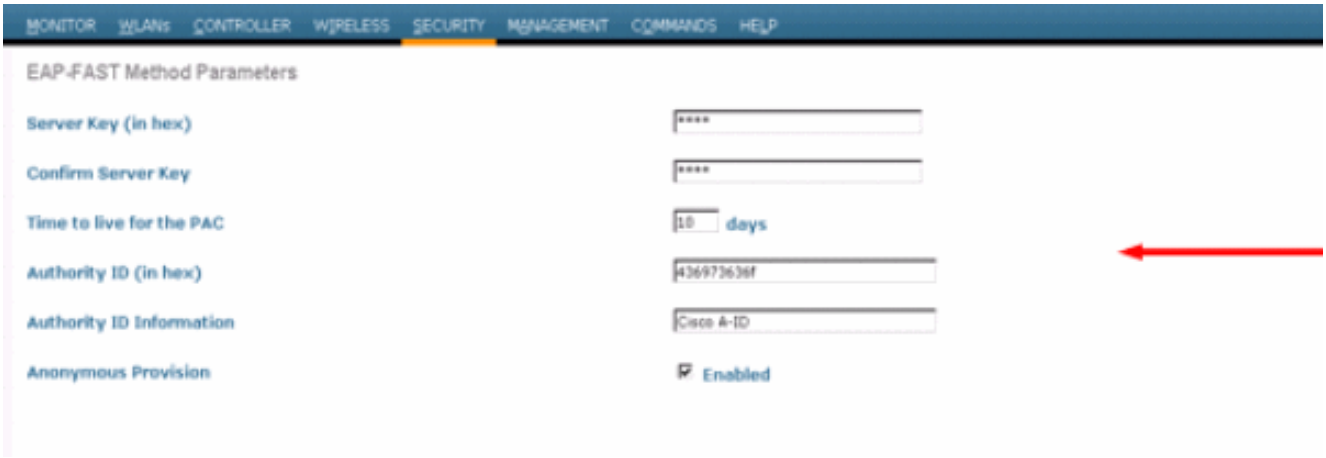


Você também pode usar o comando CLI **config local-auth eap-profile method add *<method-name> <profile-name>*.** Em nosso exemplo de configuração, adicionamos três métodos ao teste EAP de perfil. Os métodos são LEAP, EAP-FAST e EAP-TLS cujos nomes de método são *leap, fast* e *tls* respectivamente. Esta saída mostra os comandos de configuração CLI:

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

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

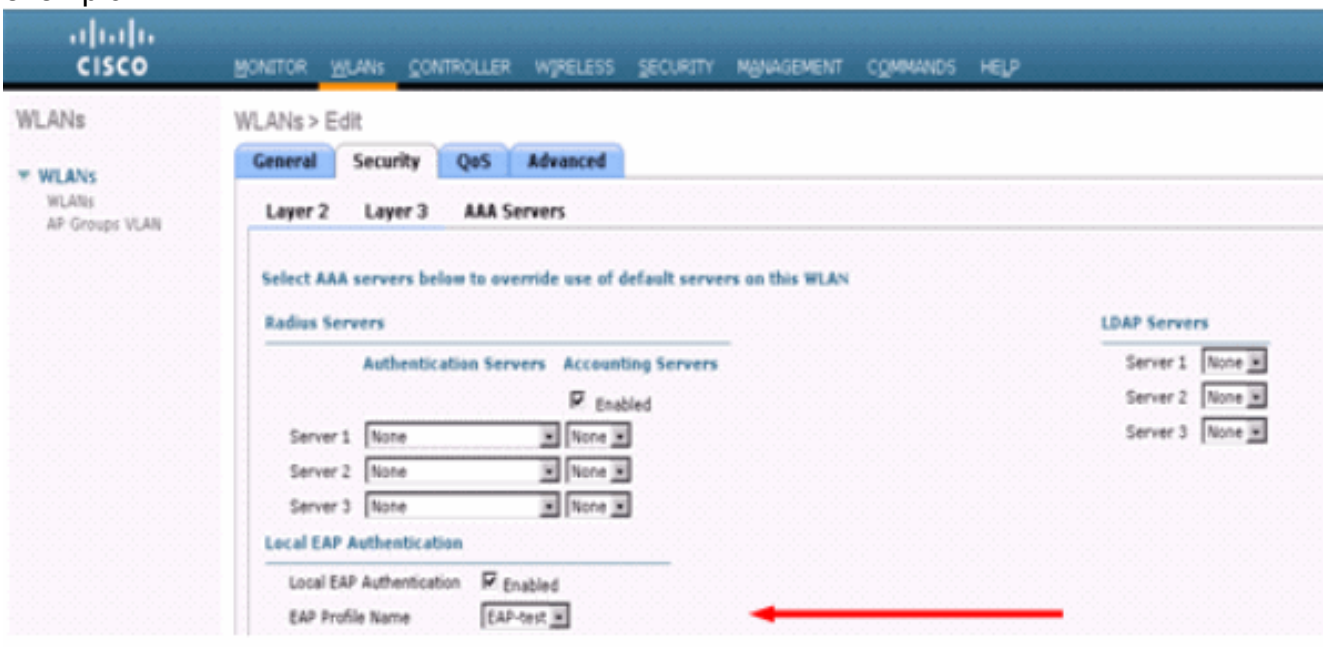
5. Configure os parâmetros do método EAP. Só é utilizado para EAP-FAST. Os parâmetros a serem configurados são:**Server Key (server-key)** — Chave do servidor para criptografar/descriptografar PACs (Protected Access Credentials) (em hexadecimal).**Time to Live for PAC (pac-ttl)** — Define o tempo de vida da PAC.**ID da autoridade (id da autoridade)** —Define o identificador da autoridade.**Provisão anônima (não comprovada)** — Configura se a provisão anônima é permitida. Iss está habilitado por padrão.Para configuração por meio da GUI, escolha **Security > Local EAP > EAP-FAST Parameters** e insira a chave do servidor, Time to live para a PAC, Authority ID (em hexadecimal) e Authority ID Information values.



Estes são os comandos de configuração CLI a serem usados para definir estes parâmetros para 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
```

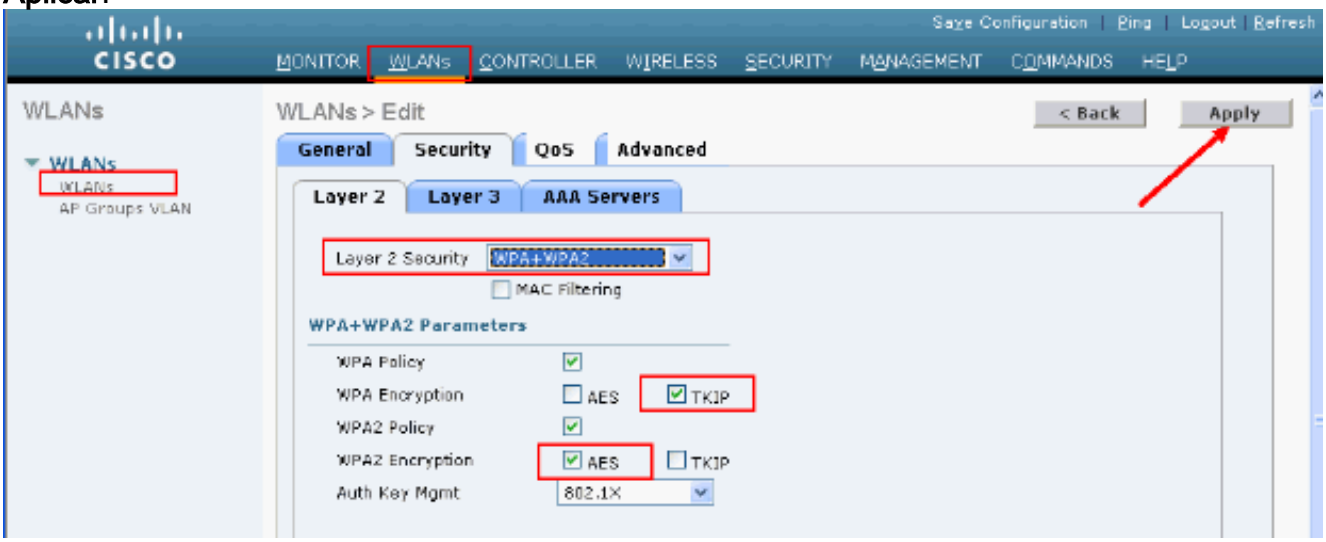
6. Ativar autenticação local por WLAN:Na GUI, escolha **WLANs** no menu superior e selecione a WLAN para a qual deseja configurar a autenticação local. Uma nova janela é exibida. Clique nas guias **Security > AAA**. Verifique a **autenticação** EAP **local** e selecione o nome de perfil EAP correto no menu suspenso como mostrado neste exemplo:



Você também pode executar o comando de configuração CLI **config wlan local-auth enable *<profile-name>* *<wlan-id>* como mostrado aqui:**

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

7. Defina os parâmetros de segurança da camada 2.Na interface GUI, na janela WLAN Edit, vá para as guias **Security > Layer 2** e escolha **WPA+WPA2** no menu suspenso Layer 2 Security. Na seção Parâmetros WPA+WPA2, defina a Criptografia WPA como **AES TKIP** e Criptografia WPA2. Em seguida, clique em **Aplicar**.



Na CLI, use estes comandos:

```
(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. Verifique a configuração:

```
(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
```

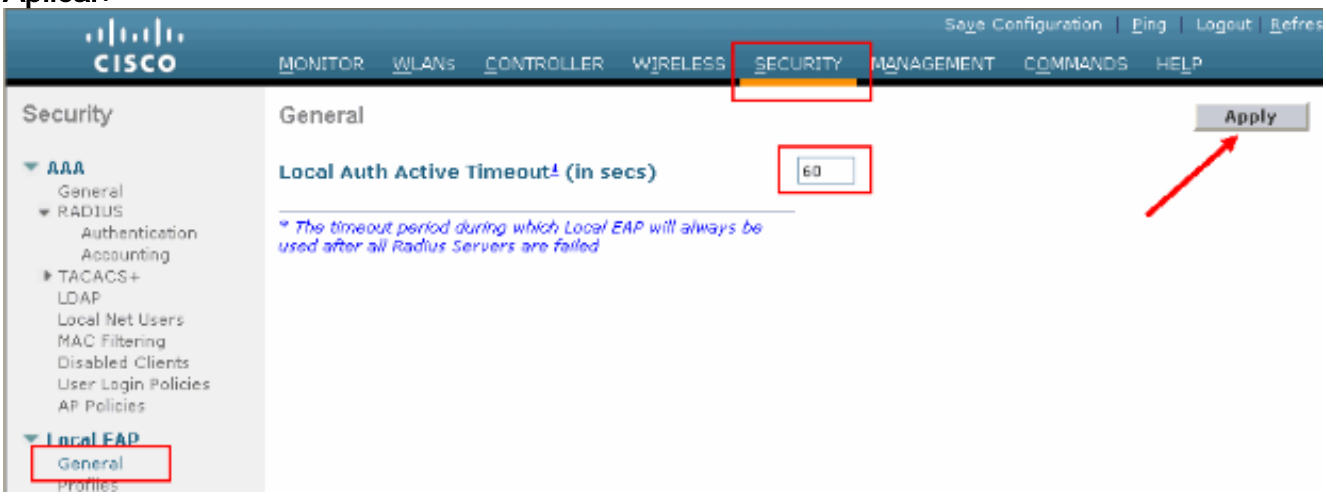
Você pode ver parâmetros específicos da wlan 1 com o **comando show wlan *<wlan id>*:**

```
(Cisco Controller) >show wlan 1
```

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

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

 Mobility Anchor List
 WLAN ID     IP Address       Status
```

Há outros parâmetros de autenticação local que podem ser configurados, em particular o temporizador de timeout ativo. Esse temporizador configura o período durante o qual o EAP local é usado depois que todos os servidores RADIUS falharam.Na GUI, escolha **Security >**

Local EAP > General e defina o valor de hora. Em seguida, clique em **Aplicar**.



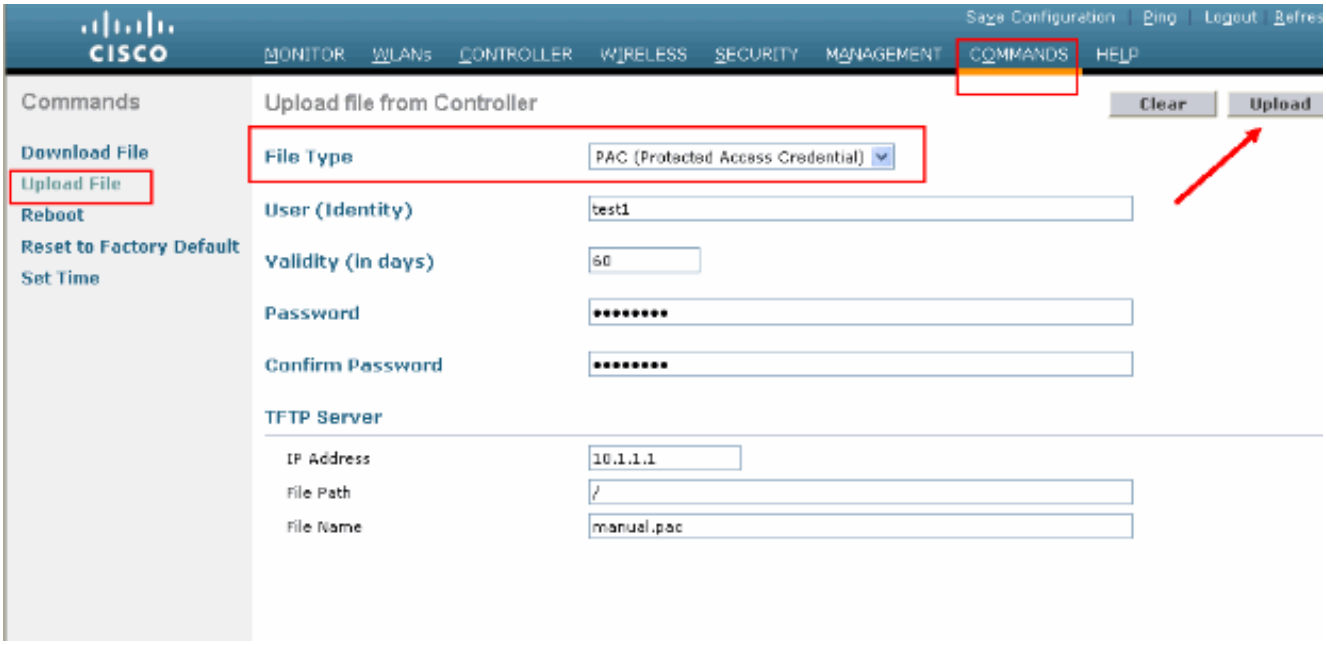
Na CLI, emita estes comandos:

```
(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
```

Você pode verificar o valor ao qual esse temporizador está configurado ao emitir o comando **show local-auth config**.

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

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

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

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

9. Se precisar gerar e carregar a PAC manual, você pode usar a GUI ou a CLI.Na GUI, selecione **COMMANDS** no menu superior e escolha **Upload File** na lista no lado direito. Selecione **PAC (Protected Access Credential)** no menu suspenso Tipo de arquivo. Insira todos os parâmetros e clique em **Upload**.



Na CLI, insira estes comandos:

```
(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.
```

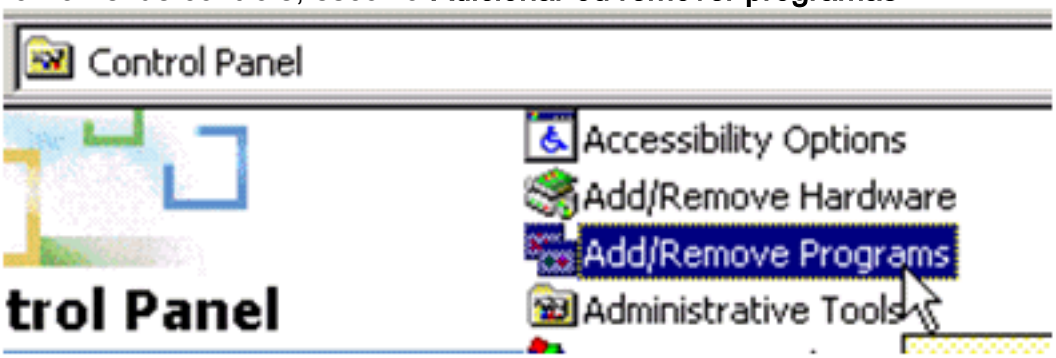
Autoridade de Certificação Microsoft

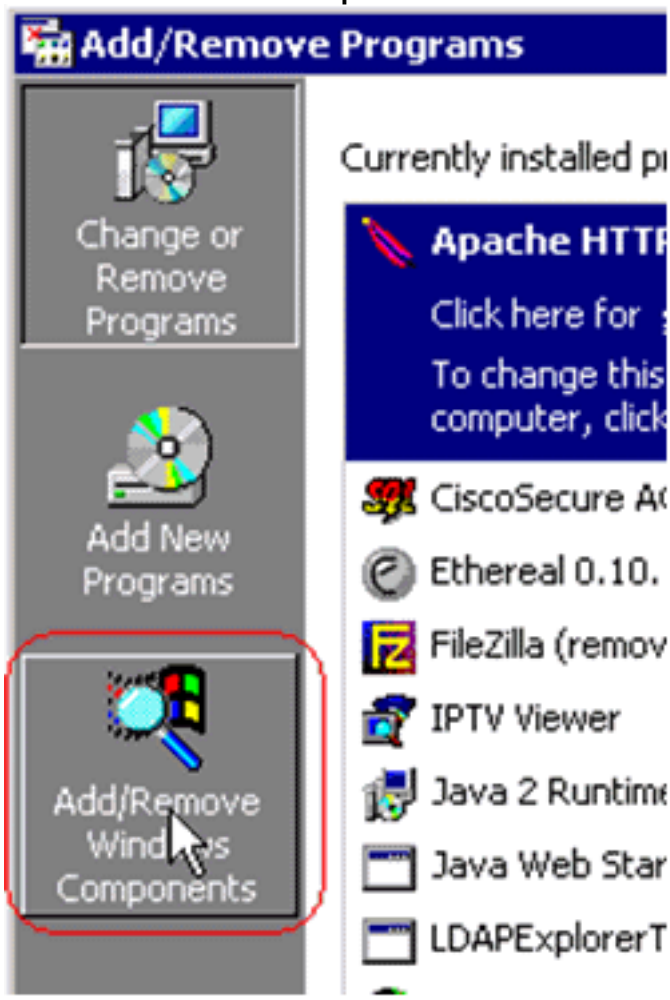
Para usar a autenticação EAP-FAST versão 2 e EAP-TLS, a WLC e todos os dispositivos clientes devem ter um certificado válido e também devem saber o certificado público da Autoridade de Certificação.

Instalação

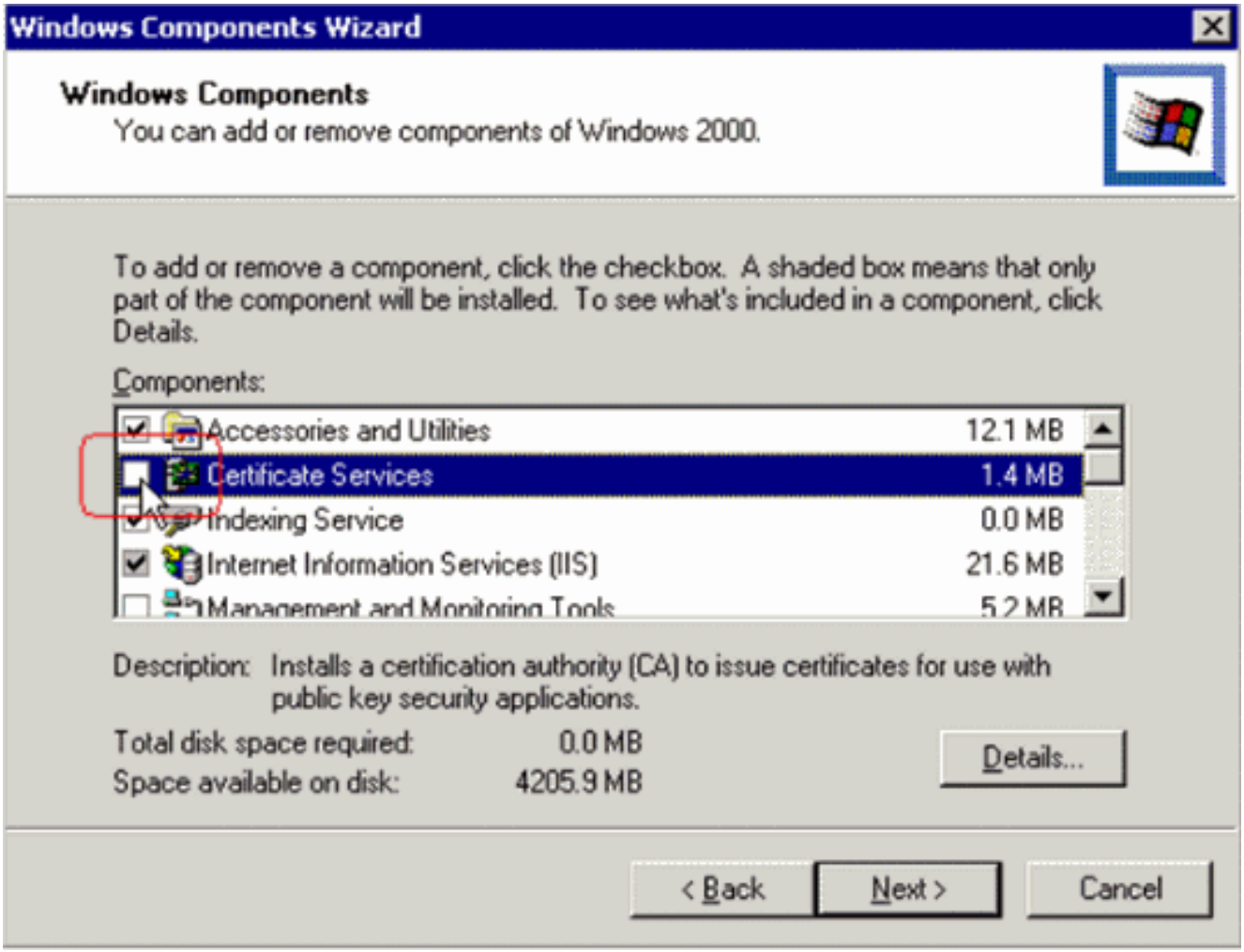
Se o Windows 2000 Server ainda não tiver serviços de Autoridade de Certificação instalados, é necessário instalá-lo.

Conclua estes passos para ativar a Autoridade de Certificação da Microsoft em um Windows 2000 Server:

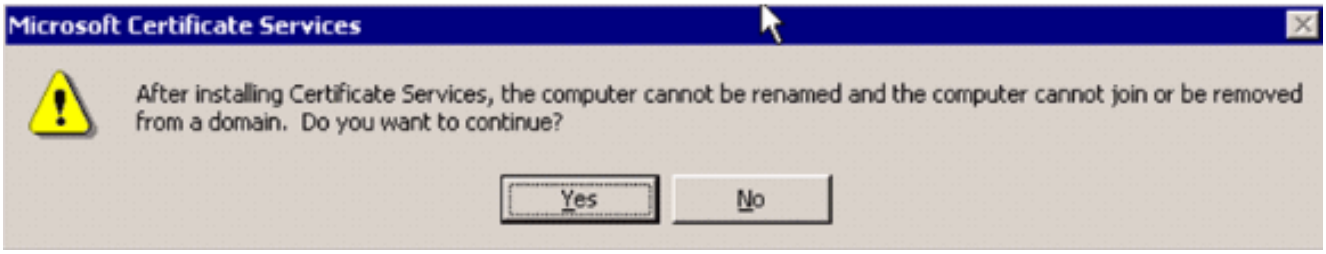
1. No Painel de controle, escolha **Adicionar ou remover programas**.


:
2. Selecione **Adicionar/remover componentes do Windows** no lado


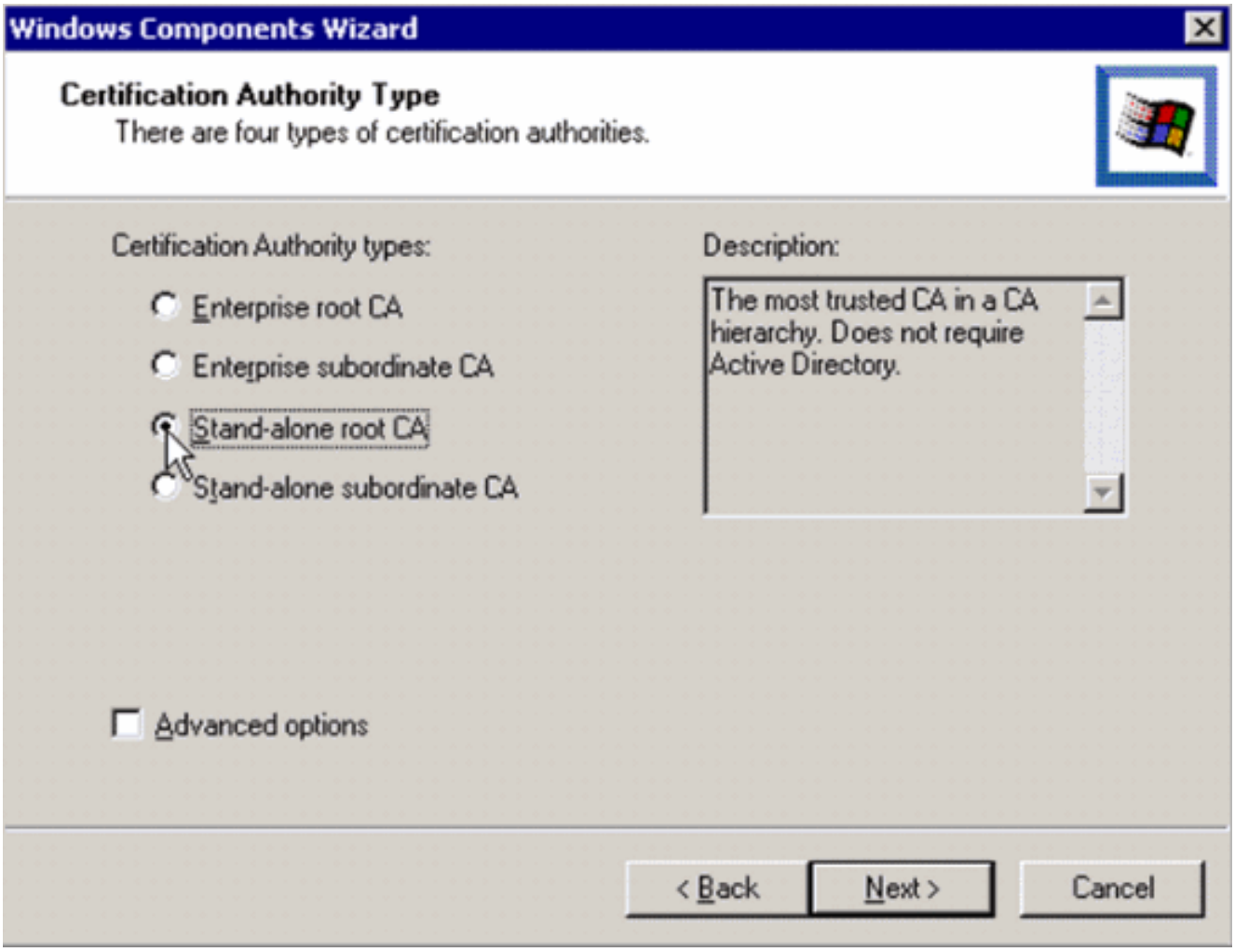
esquerdo.
3. Verificar **serviços de certificado**.



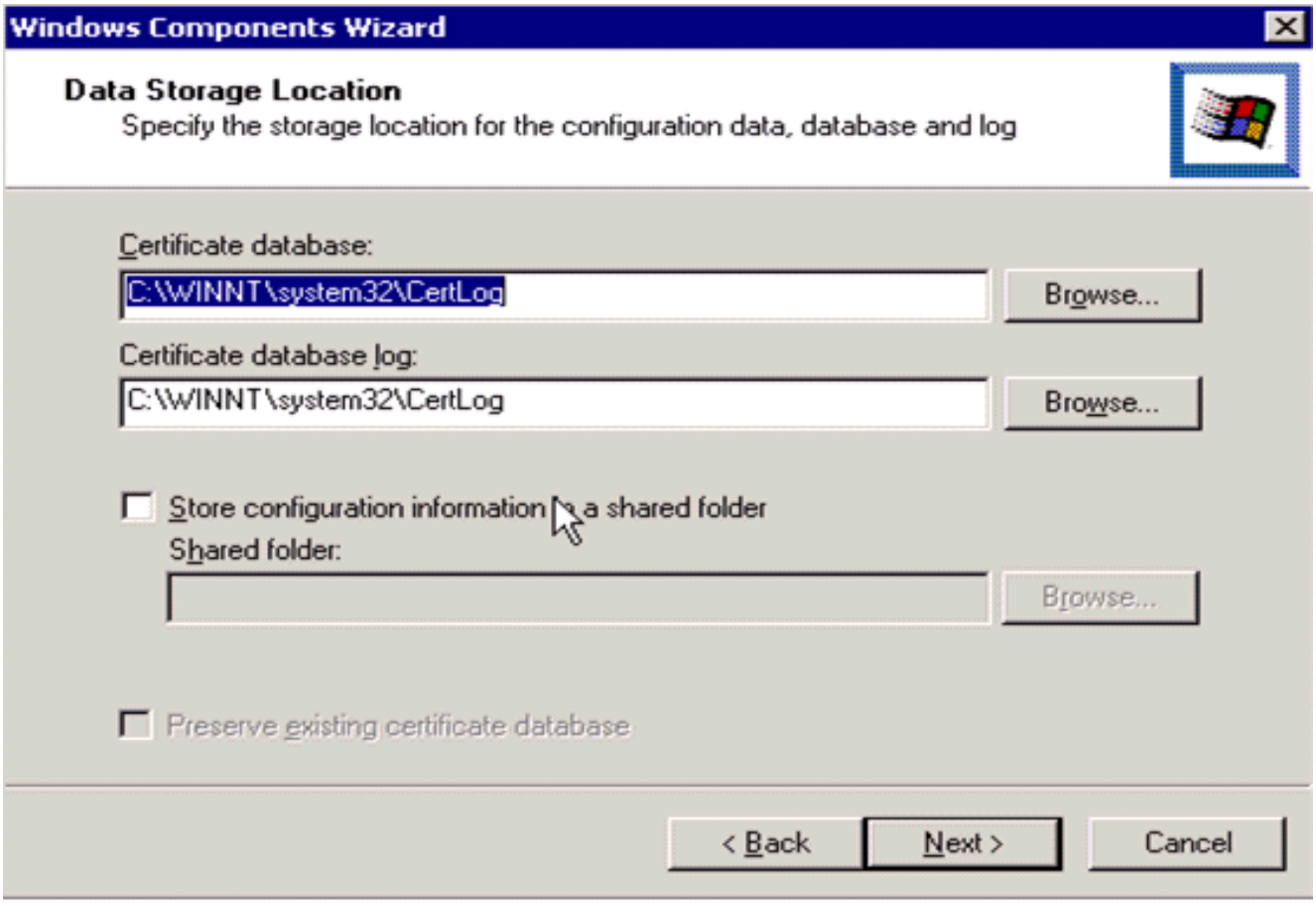
Revise este aviso antes de continuar:



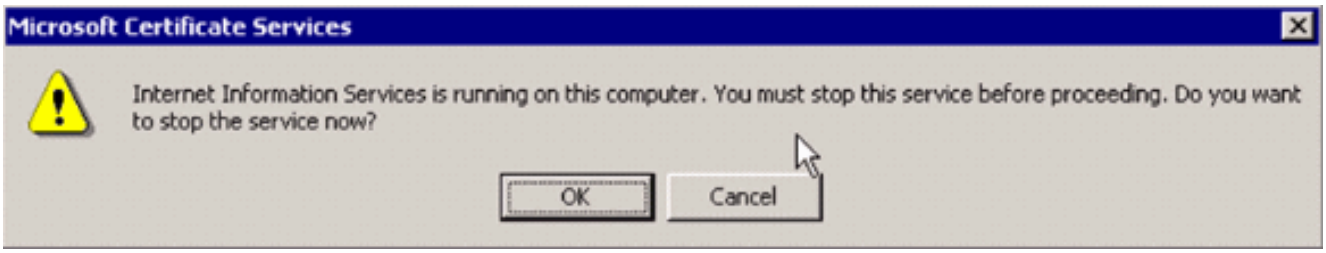
4. Selecione o tipo de autoridade de certificação que deseja instalar. Para criar uma autoridade independente simples, selecione **CA raiz autônoma**.



5. Insira as informações necessárias sobre a autoridade de certificação. Essas informações criam um certificado autoassinado para sua Autoridade de Certificação. Lembre-se do nome da AC que você usa.A Autoridade de Certificação armazena os certificados em um banco de dados. Este exemplo usa a configuração padrão proposta pela
Microsoft:



6. Os serviços da Autoridade de Certificação Microsoft usam o Microsoft Web Server do IIS para criar e gerenciar certificados de cliente e servidor. Ele precisa reiniciar o serviço IIS para
isso:



O Microsoft Windows 2000 Server agora instala o novo serviço. Você precisa ter o CD de instalação do Windows 2000 Server para instalar novos componentes do Windows.A Autoridade de Certificação está agora instalada.

Instalar o certificado no Cisco Wireless LAN Controller

Para usar EAP-FAST versão 2 e EAP-TLS no servidor EAP local de um Cisco Wireless LAN Controller, siga estas três etapas:

1. Instale o certificado do dispositivo no controlador de LAN sem fio.
2. Baixe um certificado CA do fornecedor no controlador de LAN sem fio.
3. Configure o Wireless LAN Controller para usar EAP-TLS.

Observe que no exemplo mostrado neste documento, o Access Control Server (ACS) está instalado no mesmo host que o Microsoft Ative Diretory e a Autoridade de Certificação Microsoft, mas a configuração deve ser a mesma se o servidor ACS estiver em um servidor diferente.

Instale o certificado do dispositivo no controlador de LAN sem fio

Conclua estes passos:

1. . Conclua estes passos para gerar o certificado a importar para a WLC:Vá para **http://<serverIpAddr>/certsrv**.Escolha **Solicitar um certificado** e clique em **Avançar**.Escolha **Solicitação avançada** e clique em **Avançar**.Escolha **Submeter uma solicitação de certificado a esta AC usando um formulário** e clique em **Avançar**.Escolha **Servidor Web** para Modelo de Certificado e insira as informações relevantes. Em seguida, marque as chaves como **exportáveis**.Agora você recebe um certificado que precisa instalar na sua máquina.
2. Conclua estes passos para recuperar o certificado do PC:Abra um navegador Internet Explorer e escolha **Ferramentas > Opções da Internet > Conteúdo**.Clique em **Certificados**.Selecione o certificado recém-instalado no menu suspenso.Clique em **Exportar**.Clique em **Next** duas vezes e escolha **Yes export the private key**. Este formato é PKCS#12 (formato .PFX).Escolha **Ativar proteção forte**.Digite uma senha.Salve-o em um arquivo <tme2.pfx>.
3. Copie o certificado no formato PKCS#12 para qualquer computador no qual você tenha o Openssl instalado para convertê-lo no formato PEM.
```
openssl pkcs12 -in tme2.pfx -out tme2.pem
!--- The command to be given, -in Enter Import Password: !--- Enter the password given
previously, from step 2g. MAC verified OK Enter PEM pass phrase: !--- Enter a phrase.
Verifying - Enter PEM pass phrase:
```
4. Faça o download do certificado do dispositivo de formato PEM convertido para a 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. Depois de reinicializar, verifique o certificado.
```
(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
```

Baixe um certificado CA do fornecedor no controlador de LAN sem fio

Conclua estes passos:

1. Conclua estes passos para recuperar o certificado CA do fornecedor:Vá para **http://<serverIpAddr>/certsrv**.Escolha **Recuperar o certificado CA** e clique em **Avançar**.Escolha o certificado CA.Clique em **DER codificado**.Clique em **Download CA certificate** e salve o certificado como **rootca.cer**.
2. Converta a CA do fornecedor do formato DER em formato PEM com o comando **openssl x509 -in rootca.cer -information DER -out rootca.pem -outform PEM**.O arquivo de saída é rootca.pem no formato PEM.
3. Faça o download do certificado CA do fornecedor:

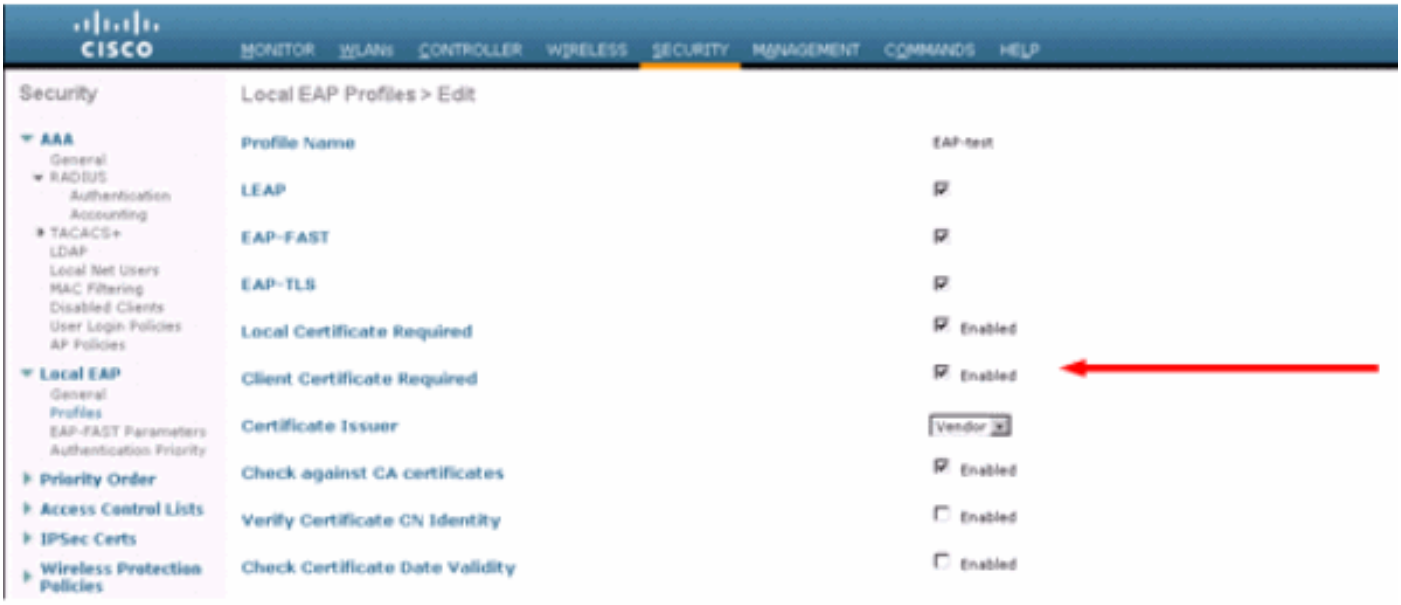
```
(Cisco Controller) >transfer download datatype eapcacert

(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.
```

Configure o controlador de LAN sem fio para usar EAP-TLS

Conclua estes passos:

Na GUI, escolha **Security > Local EAP > Profiles**, escolha o perfil e verifique estas configurações:

- Certificado local obrigatório habilitado.
- Certificado do cliente obrigatório ativado.
- O emissor do certificado é o fornecedor.
- Verifique se os certificados CA estão habilitados.



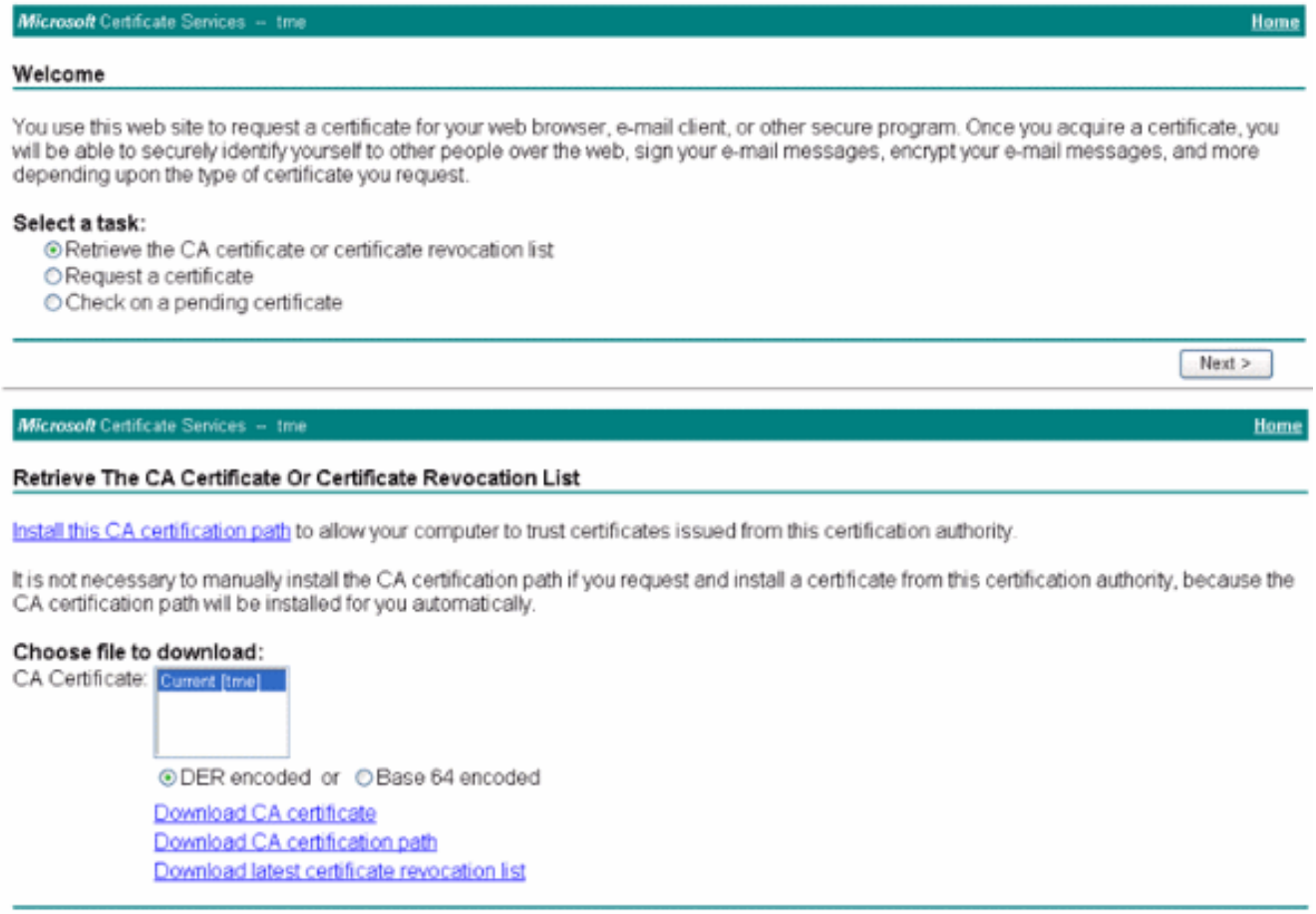
Instalar o certificado da autoridade de certificação no dispositivo cliente

Baixar e instalar um certificado CA raiz para o cliente

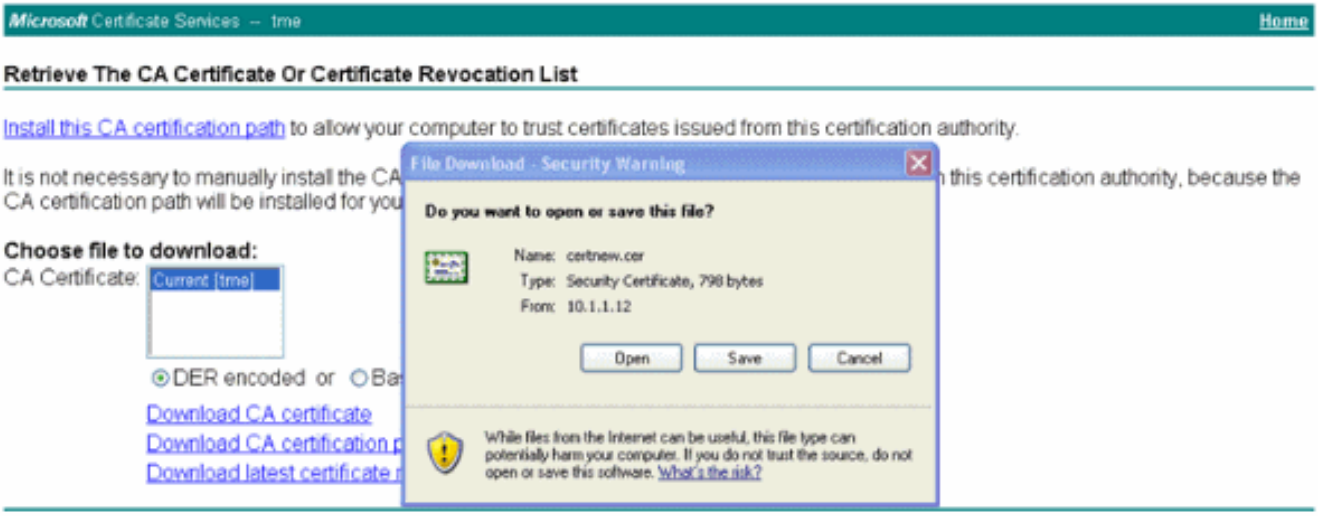
O cliente deve obter um certificado CA raiz de um servidor de Autoridade de Certificação. Há vários métodos que você pode usar para obter um certificado de cliente e instalá-lo na máquina do Windows XP. Para adquirir um certificado válido, o usuário do Windows XP precisa estar conectado usando sua ID de usuário e deve ter uma conexão de rede.

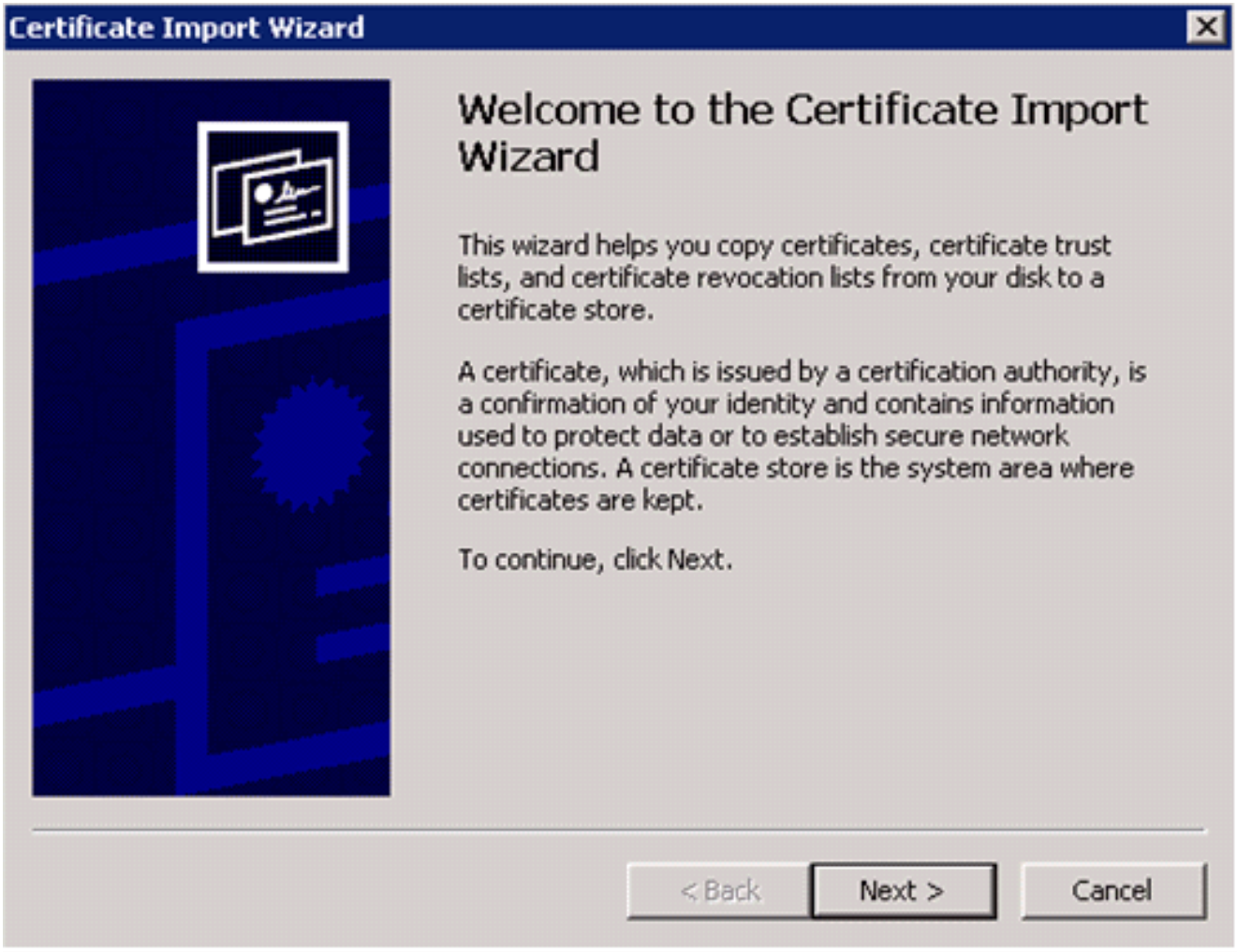
Um navegador da Web no cliente Windows XP e uma conexão com fio à rede foram usados para obter um certificado de cliente do servidor da Autoridade de Certificação raiz privada. Este procedimento é usado para obter o certificado do cliente de um servidor da Autoridade de Certificação da Microsoft:

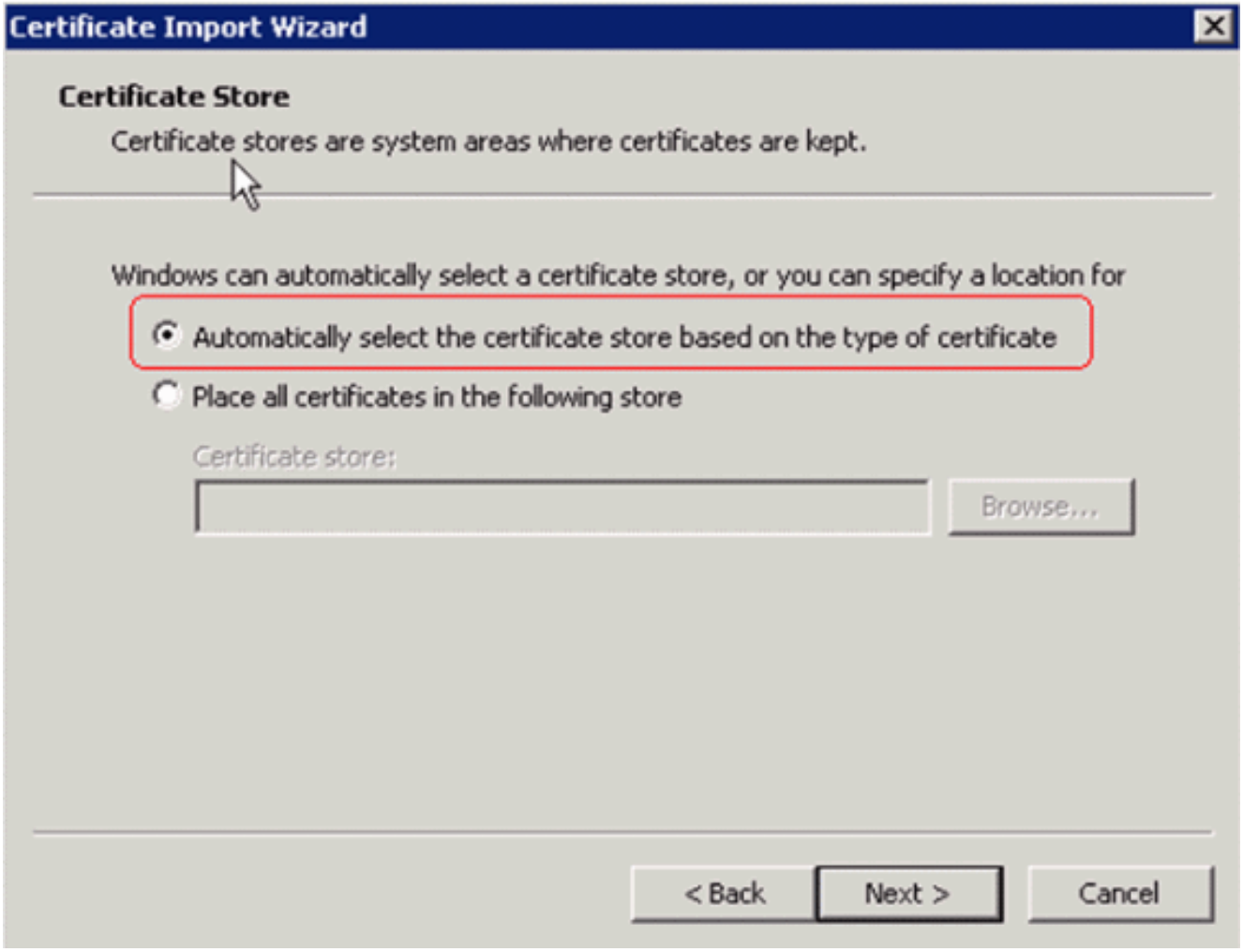
1. Use um navegador da Web no cliente e aponte o navegador para o servidor da Autoridade de Certificação. Para fazer isso, digite **http://IP-address-of-Root-CA/certsrv**.
2. Faça login usando **Domain_Name\user_name**. Você deve fazer login usando o nome de usuário da pessoa que deve usar o cliente XP.
3. Na janela Bem-vindo, escolha **Recuperar um certificado CA** e clique em **Avançar**.
4. Selecione **Base64 Encoding** e **Download CA certificate**.
5. Na janela Certificado emitido, clique em **Instalar este certificado** e clique em **Avançar**.
6. Escolha **Selecionar automaticamente o repositório de certificados** e clique em **Avançar** para a mensagem de importação bem-sucedida.
7. Ligar à Autoridade de Certificação para obter o certificado da Autoridade de Certificação:



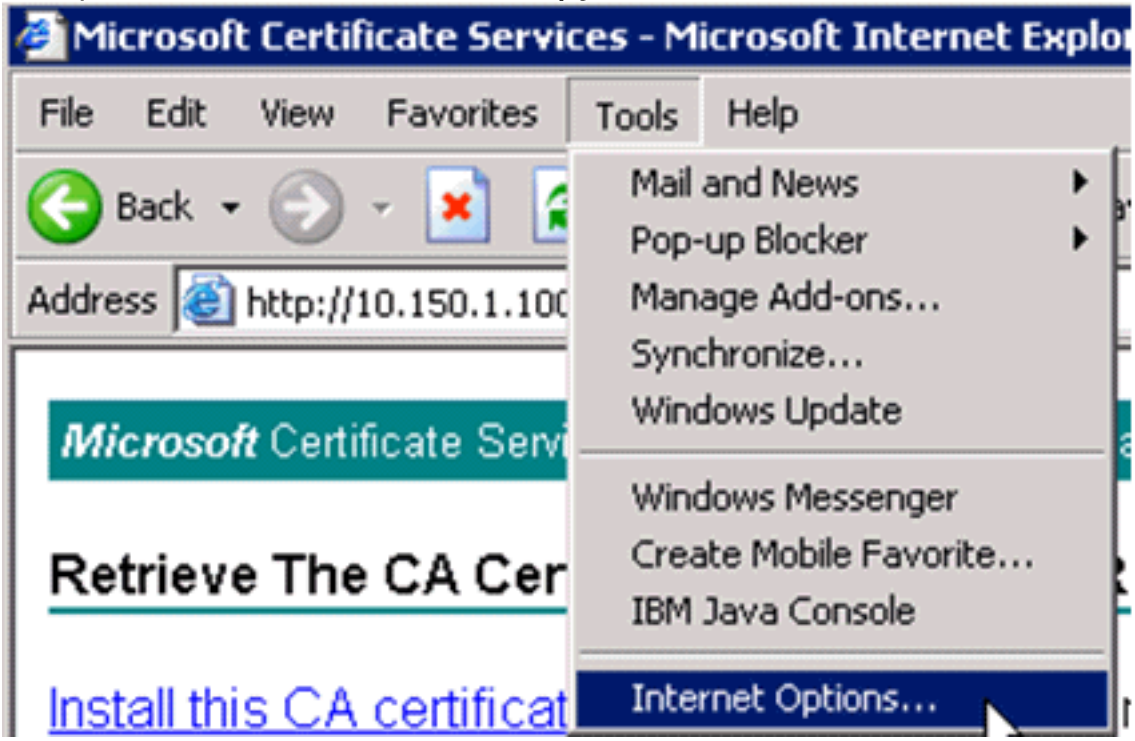
8. Clique em **Transferir certificado CA**.

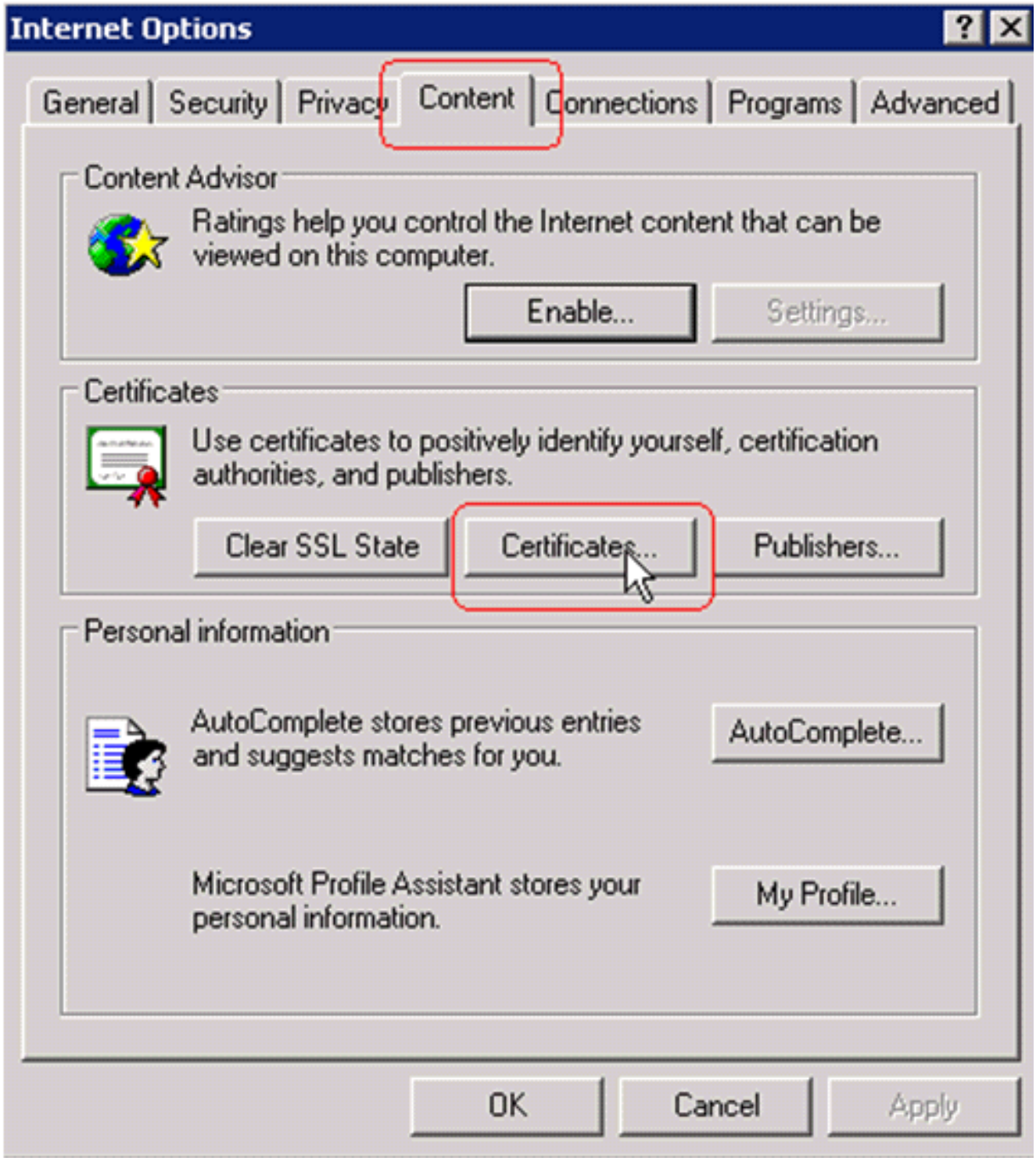



Certificate Import Wizard
Welcome to the Certificate Import Wizard
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
A certificate, which is issued by a certification authority, is a confirmation of your identity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

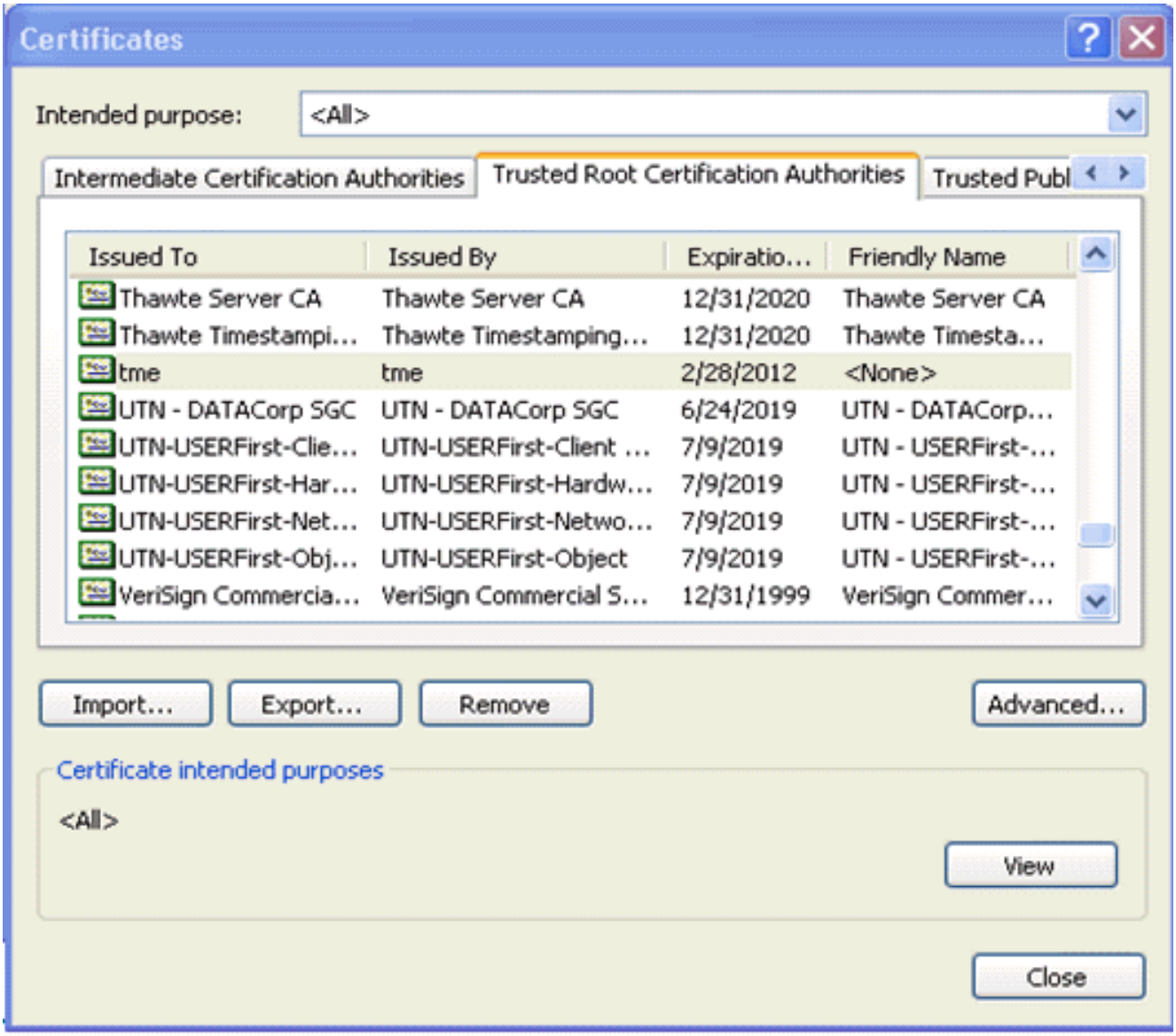

Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for
Automatically select the certificate store based on the type of certificate
Place all certificates in the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

9. Para verificar se o certificado da Autoridade de Certificação está instalado corretamente, abra o Internet Explorer e escolha **Ferramentas > Opções da Internet > Conteúdo > Certificados**.





Na Trusted Root Certification Authority (Autoridade de Certificação de Raiz Confiável), você deve ver sua Autoridade de Certificação recém-instalada:



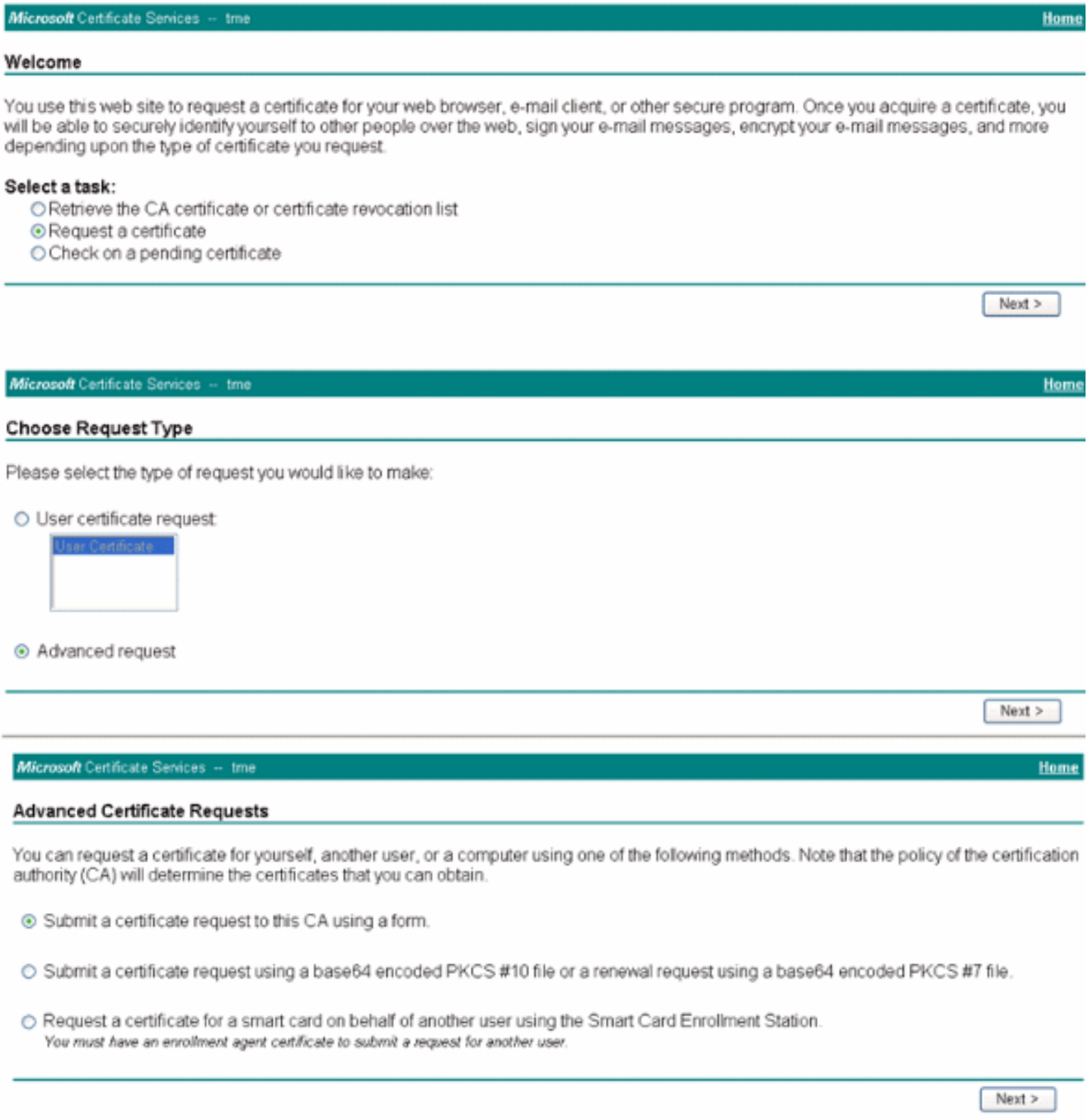
Gerar um certificado de cliente para um dispositivo cliente

O cliente deve obter um certificado de um servidor de Autoridade de Certificação para que a WLC autentique um cliente WLAN EAP-TLS. Há vários métodos que você pode usar para obter um certificado de cliente e instalá-lo na máquina do Windows XP. Para adquirir um certificado válido, o usuário do Windows XP precisa estar conectado usando sua ID de usuário e deve ter uma conexão de rede (uma conexão com fio ou uma conexão WLAN com segurança 802.1x desabilitada).

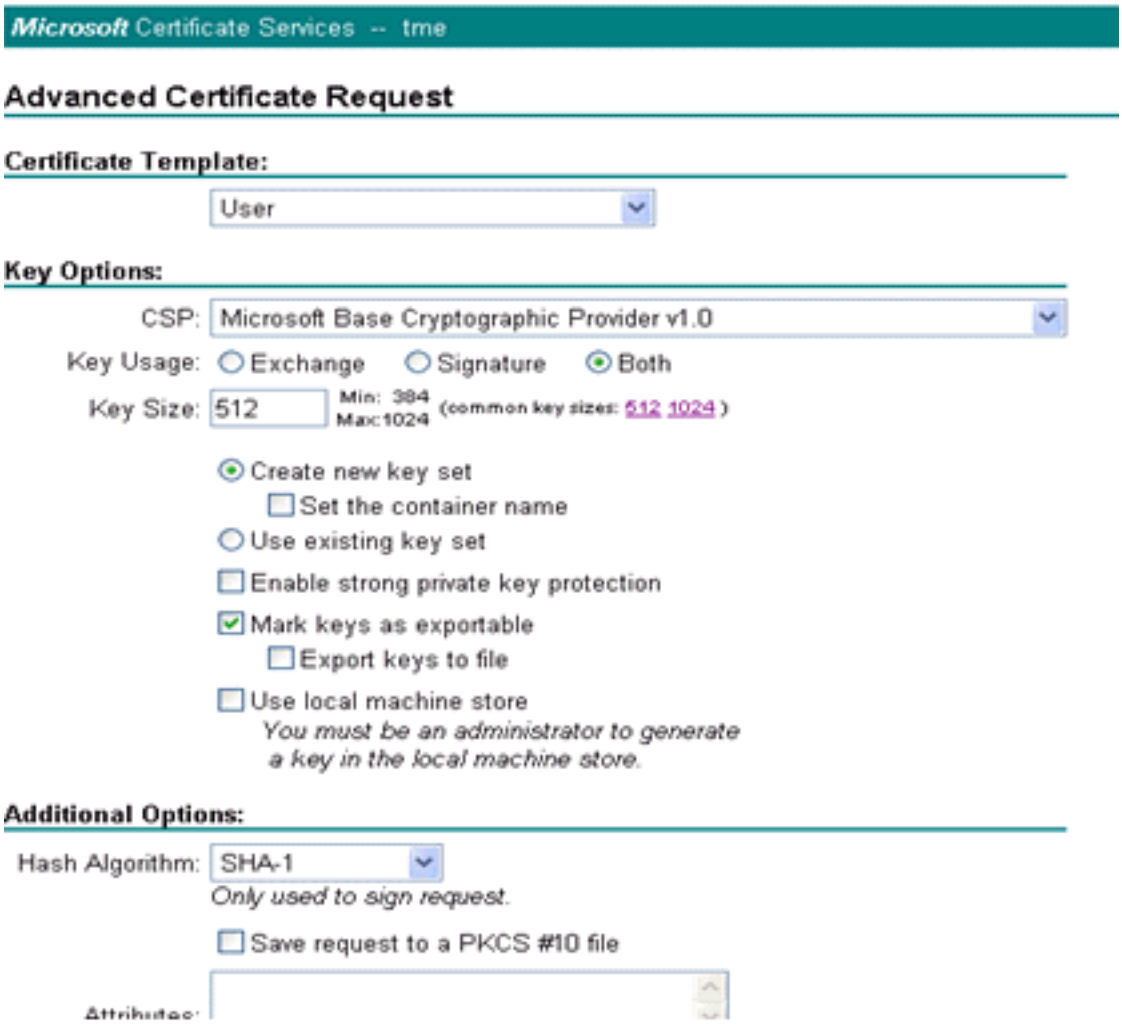
Um navegador da Web no cliente Windows XP e uma conexão com fio à rede são usados para obter um certificado de cliente do servidor da Autoridade de Certificação raiz privada. Este procedimento é usado para obter o certificado do cliente de um servidor da Autoridade de Certificação da Microsoft:

1. Use um navegador da Web no cliente e aponte o navegador para o servidor da Autoridade de Certificação. Para fazer isso, digite **http://IP-address-of-Root-CA/certsrv**.
2. Faça login usando **Domain_Name\user_name**. Você deve fazer login usando o nome de usuário da pessoa que usa o cliente XP. (O nome de usuário é incorporado ao certificado do cliente.)
3. Na janela Bem-vindo, escolha **Solicitar um certificado** e clique em **Avançar**.
4. Escolha **Solicitação avançada** e clique em **Avançar**.

5. Escolha **Submeter uma solicitação de certificado a esta AC usando um formulário** e clique em **Avançar**.
6. No formulário Solicitação de certificado avançado, escolha Modelo de certificado como **usuário**, especifique o tamanho da chave como **1024** e clique em **Enviar**.
7. Na janela Certificado emitido, clique em **Instalar este certificado**. Isso resulta na instalação bem-sucedida de um certificado de cliente no cliente Windows XP.

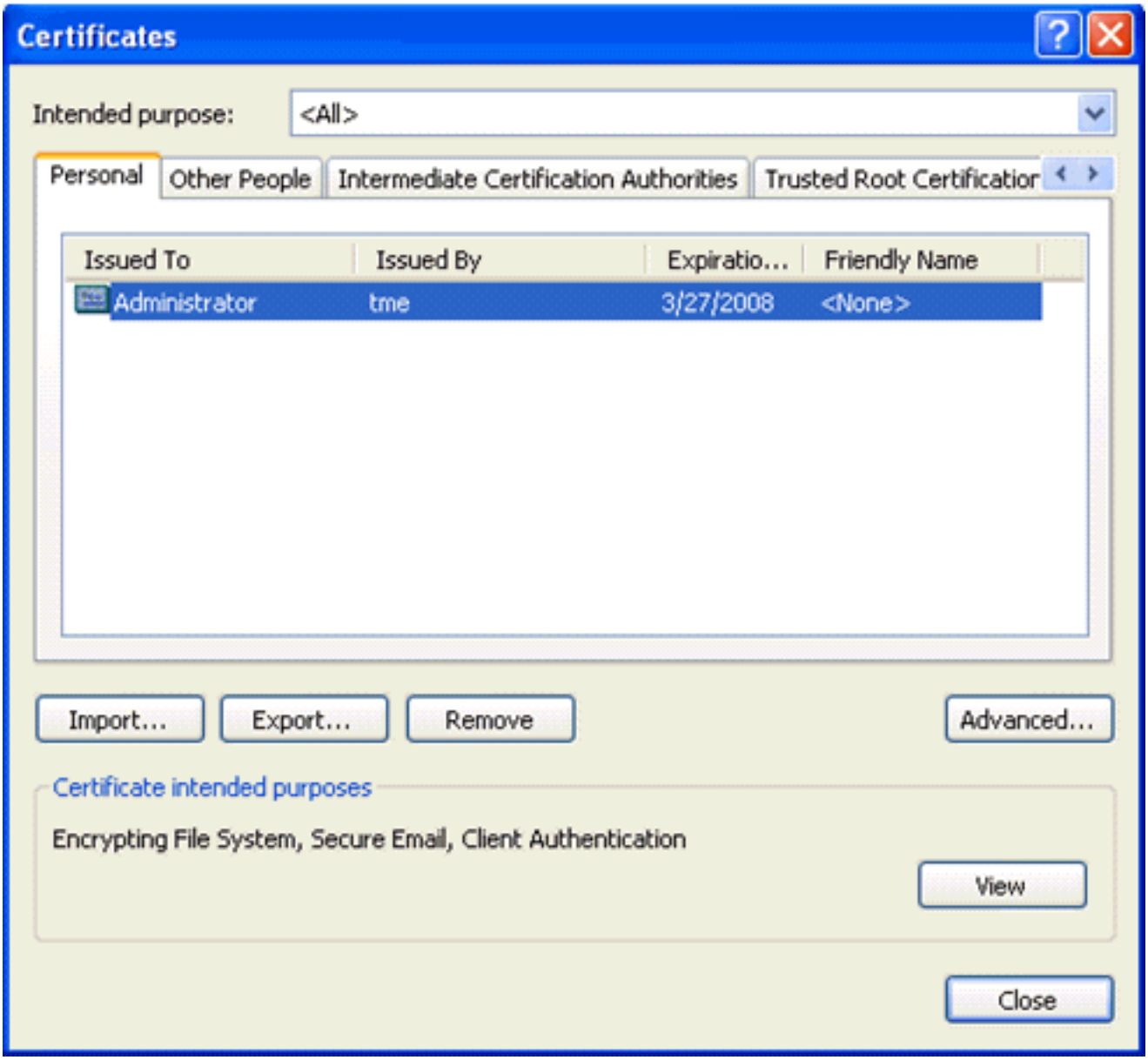


8. Selecione **Certificado de Autenticação de**



Cliente. O certificado do cliente foi criado agora.

9. Para verificar se o certificado está instalado, vá para o Internet Explorer e escolha **Ferramentas > Opções da Internet > Conteúdo > Certificados**. Na guia Pessoal, você deve ver o certificado.

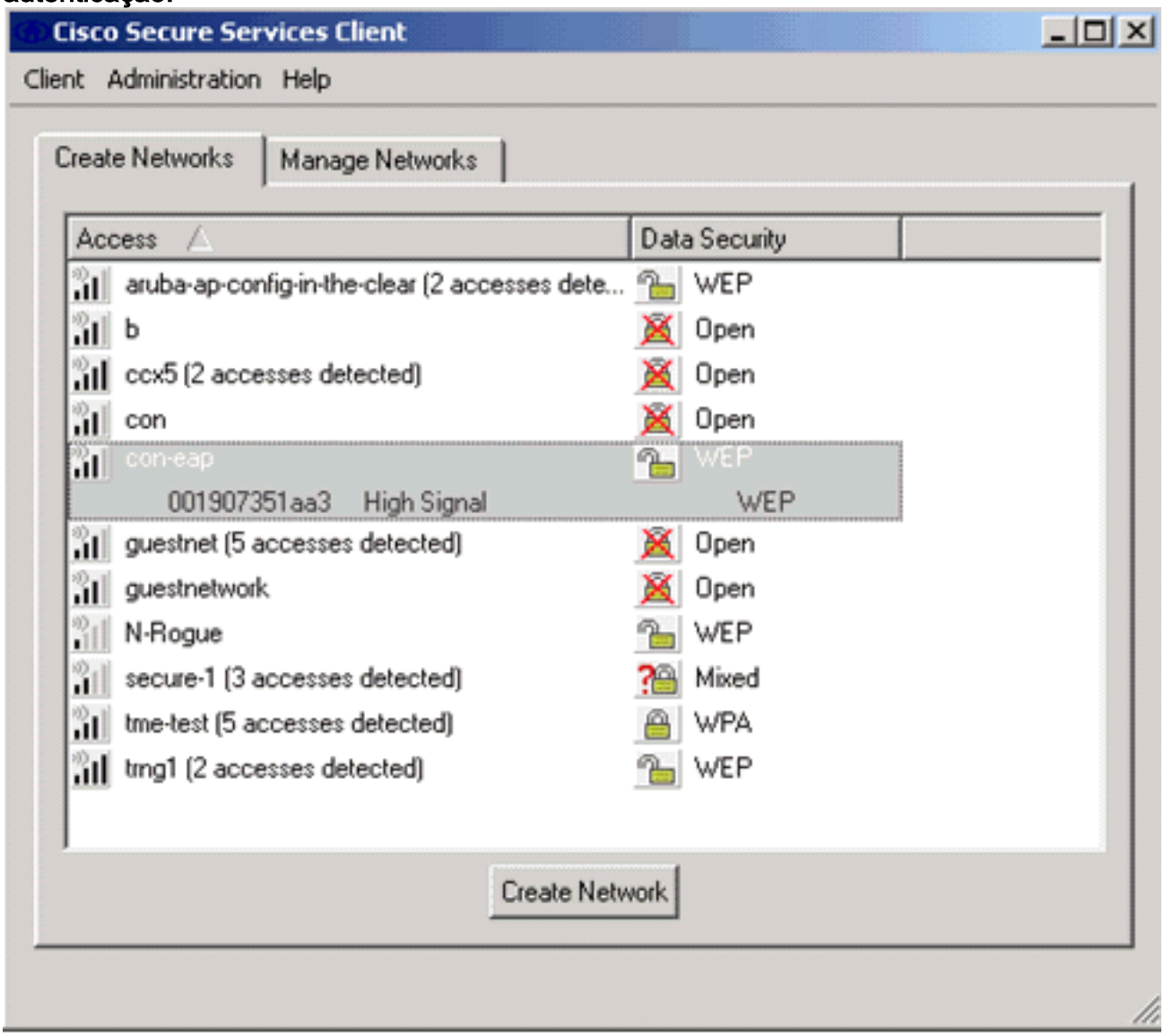


EAP-TLS com Cisco Secure Services Client no dispositivo cliente

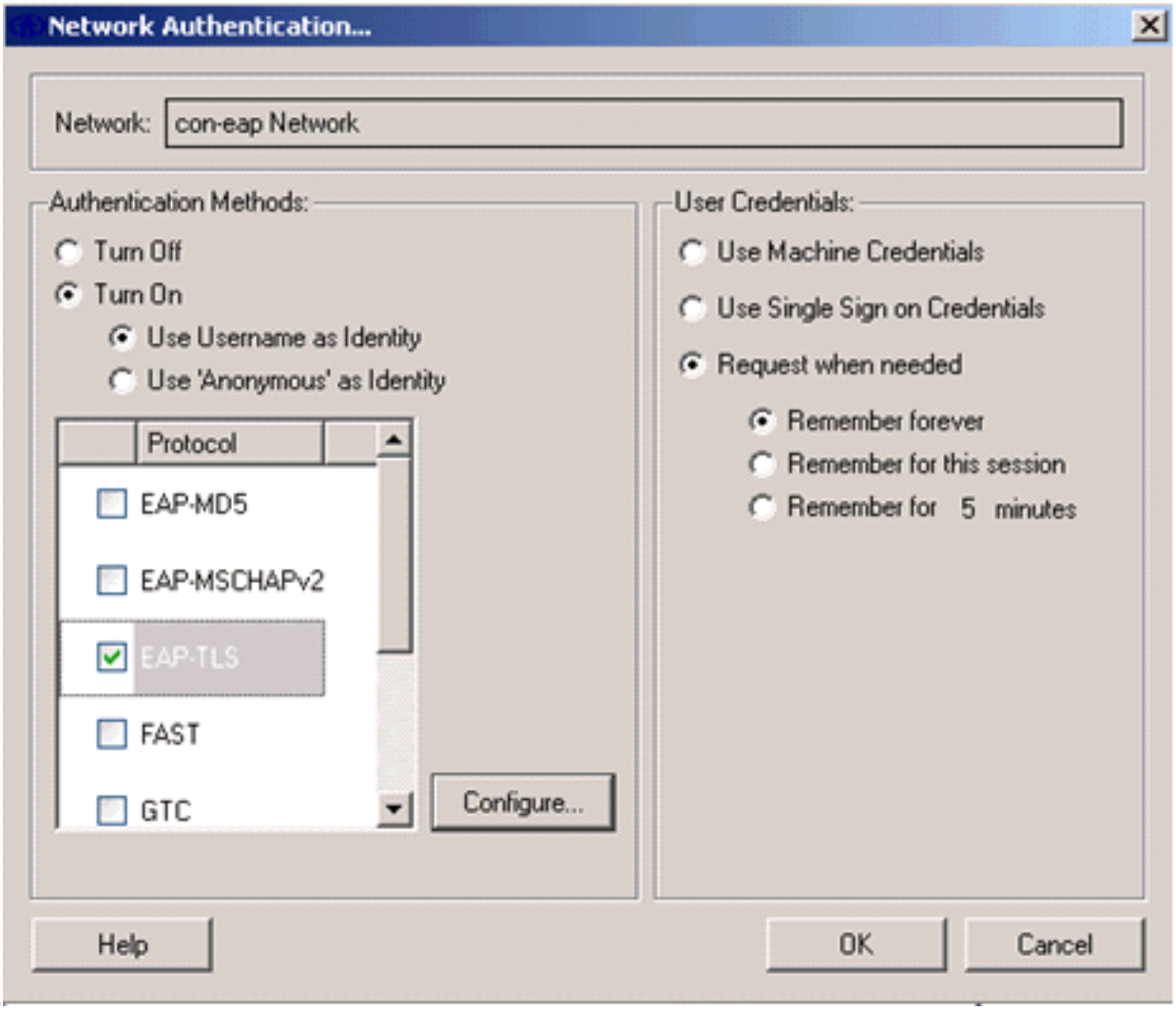
Conclua estes passos:

1. A WLC, por padrão, transmite o SSID, de modo que ele seja exibido na lista Criar redes de SSIDs digitalizados. Para criar um perfil de rede, clique no SSID na lista (Empresa) e clique em **Criar rede**.Se a infraestrutura de WLAN estiver configurada com o SSID de broadcast desabilitado, você deverá adicionar manualmente o SSID. Para fazer isso, clique em **Adicionar** em Dispositivos de acesso e insira manualmente o SSID apropriado (por exemplo, Empresa). Configure o comportamento de sondagem ativo para o cliente. Ou seja, onde o cliente procura ativamente seu SSID configurado. Especifique **Atively search for this access device** depois de inserir o SSID na janela Add Access Device.**Nota:As configurações de porta não permitirão modos corporativos (802.1X) se as configurações de autenticação EAP não forem primeiro configuradas para o perfil.**
2. Clique em **Create Network** para abrir a janela Network Profile, que permite associar o SSID escolhido (ou configurado) a um mecanismo de autenticação. Atribua um nome descritivo para o perfil.**Nota:Vários tipos de segurança de WLAN e/ou SSIDs podem ser associados neste perfil de**

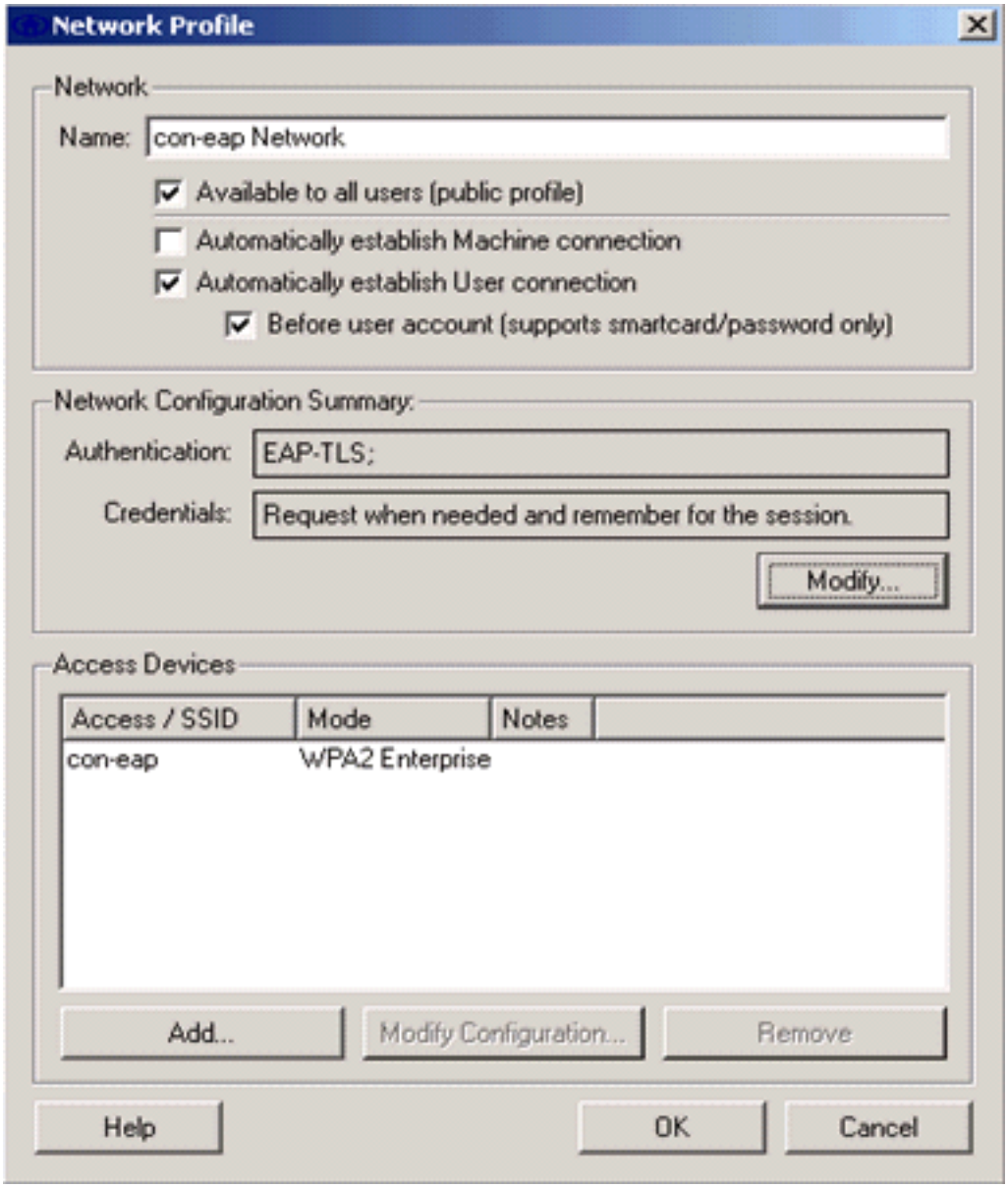
autenticação.



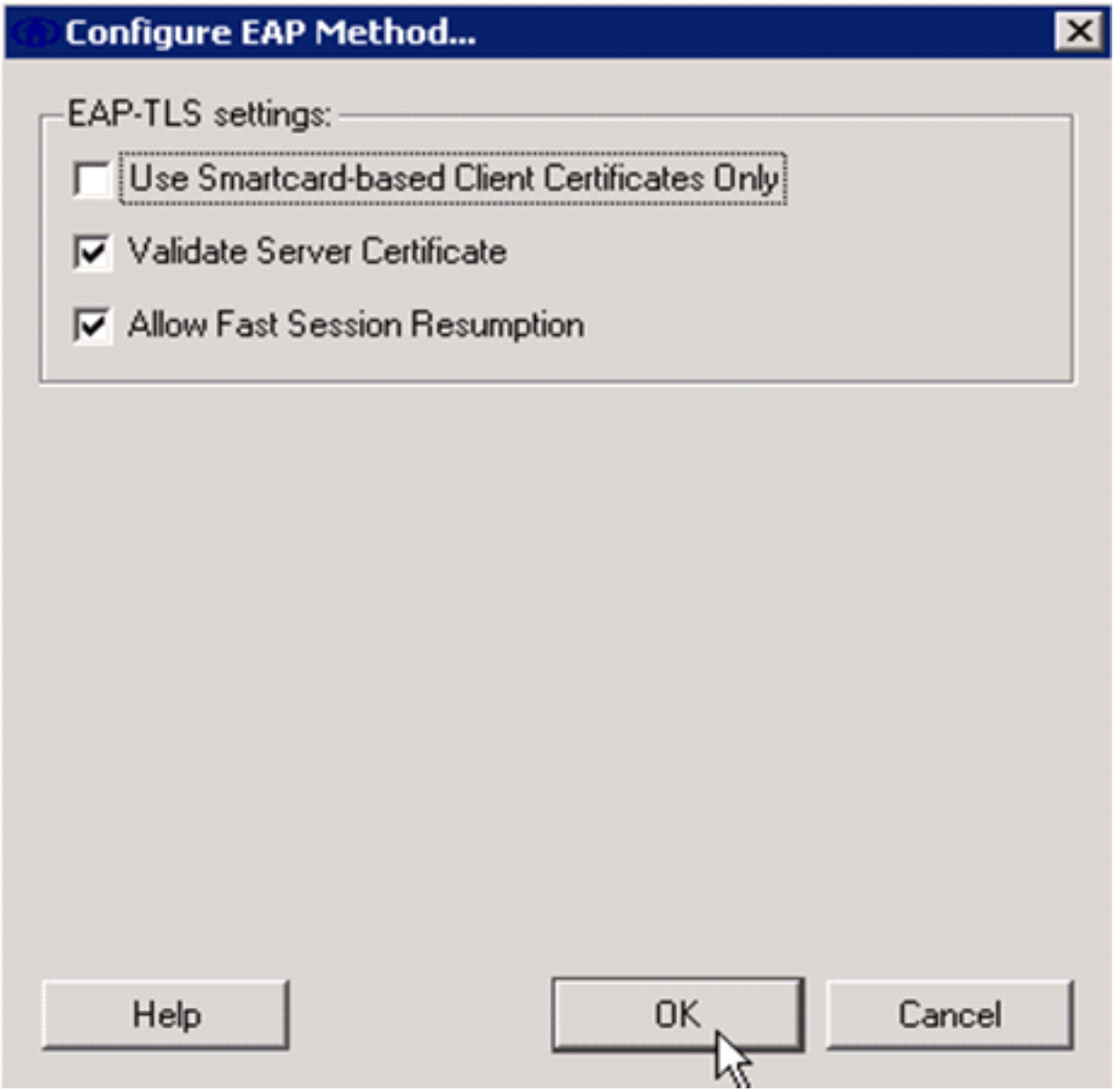
3. Ative a autenticação e verifique o método EAP-TLS. Em seguida, clique em **Configurar** para configurar as propriedades EAP-TLS.
4. Em Network Configuration Summary (Resumo da configuração da rede), clique em **Modify (Modificar)** para definir as configurações de EAP/credenciais.
5. Especifique **Turn On Authentication**, escolha **EAP-TLS** em Protocol e escolha **Username** como a Identity.
6. Especifique **Utilizar Credenciais de Início de Sessão Único** para utilizar credenciais de início de sessão para autenticação de rede. Clique em **Configurar** para configurar parâmetros EAP-


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

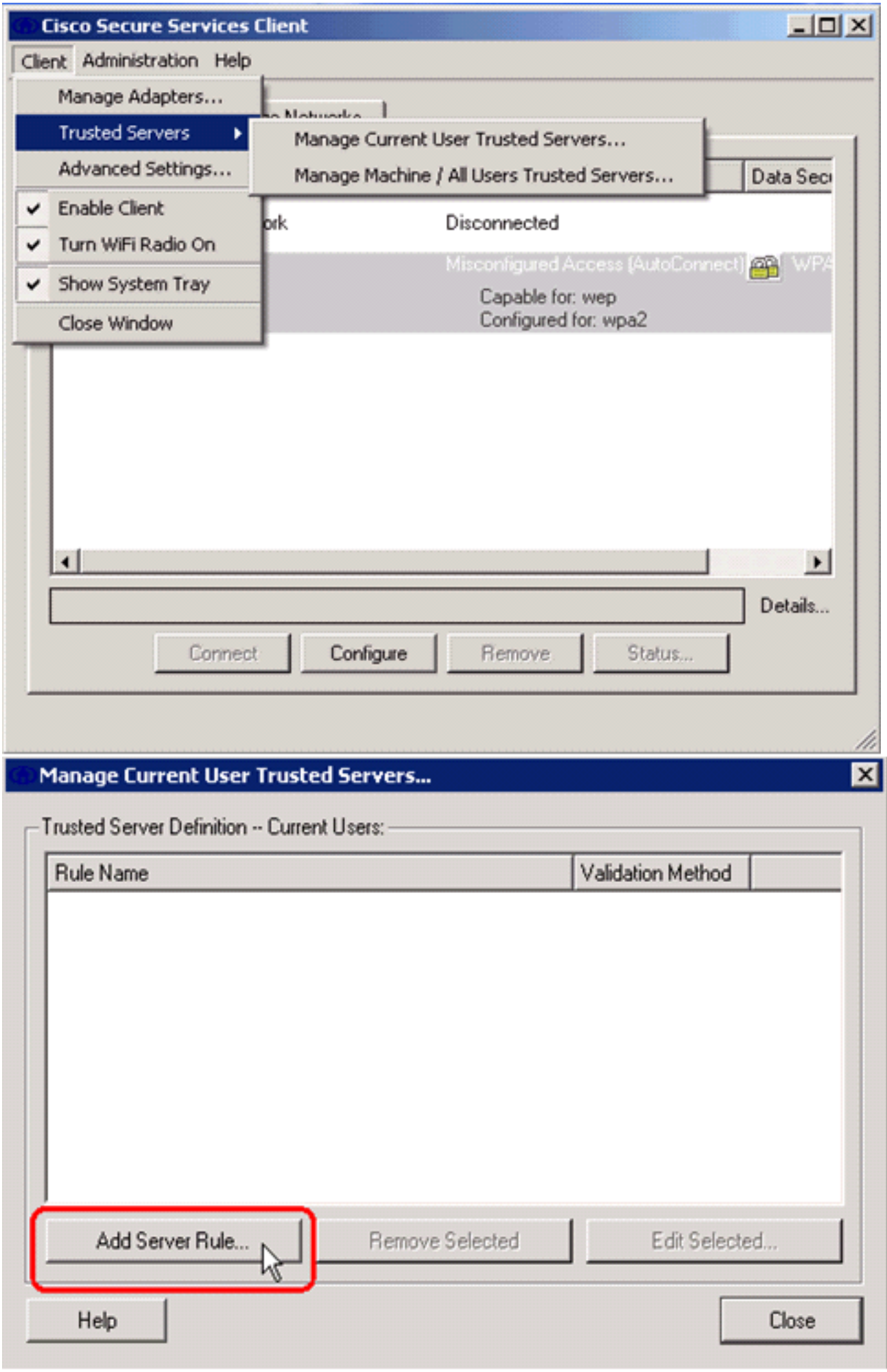
TLS.



7. Para ter uma configuração EAP-TLS segura, você precisa verificar o certificado do servidor RADIUS. Para fazer isso, marque **Validar certificado do servidor**.

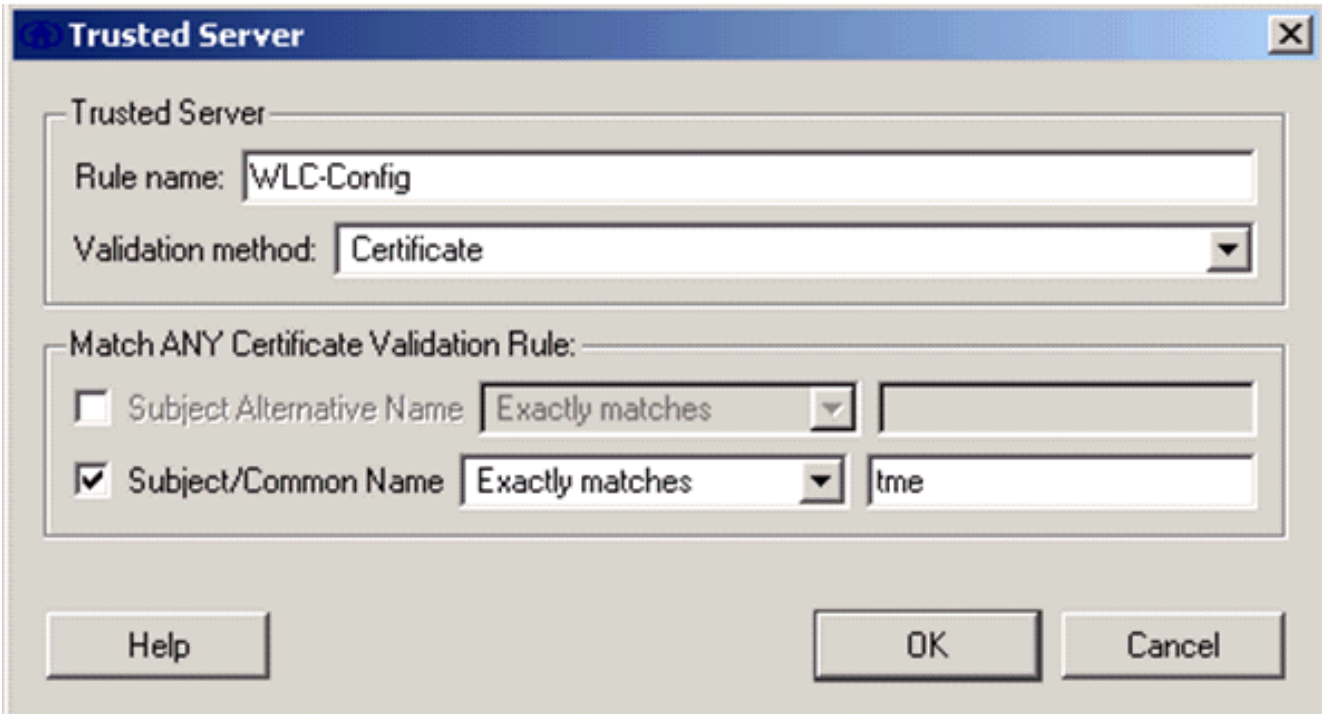


8. Para validar o certificado do servidor RADIUS, você precisa fornecer informações do Cisco Secure Services Client para aceitar apenas o certificado correto. Escolha **Cliente > Servidores Confiáveis > Gerenciar Servidores Confiáveis de Utilizadores Atuais**.



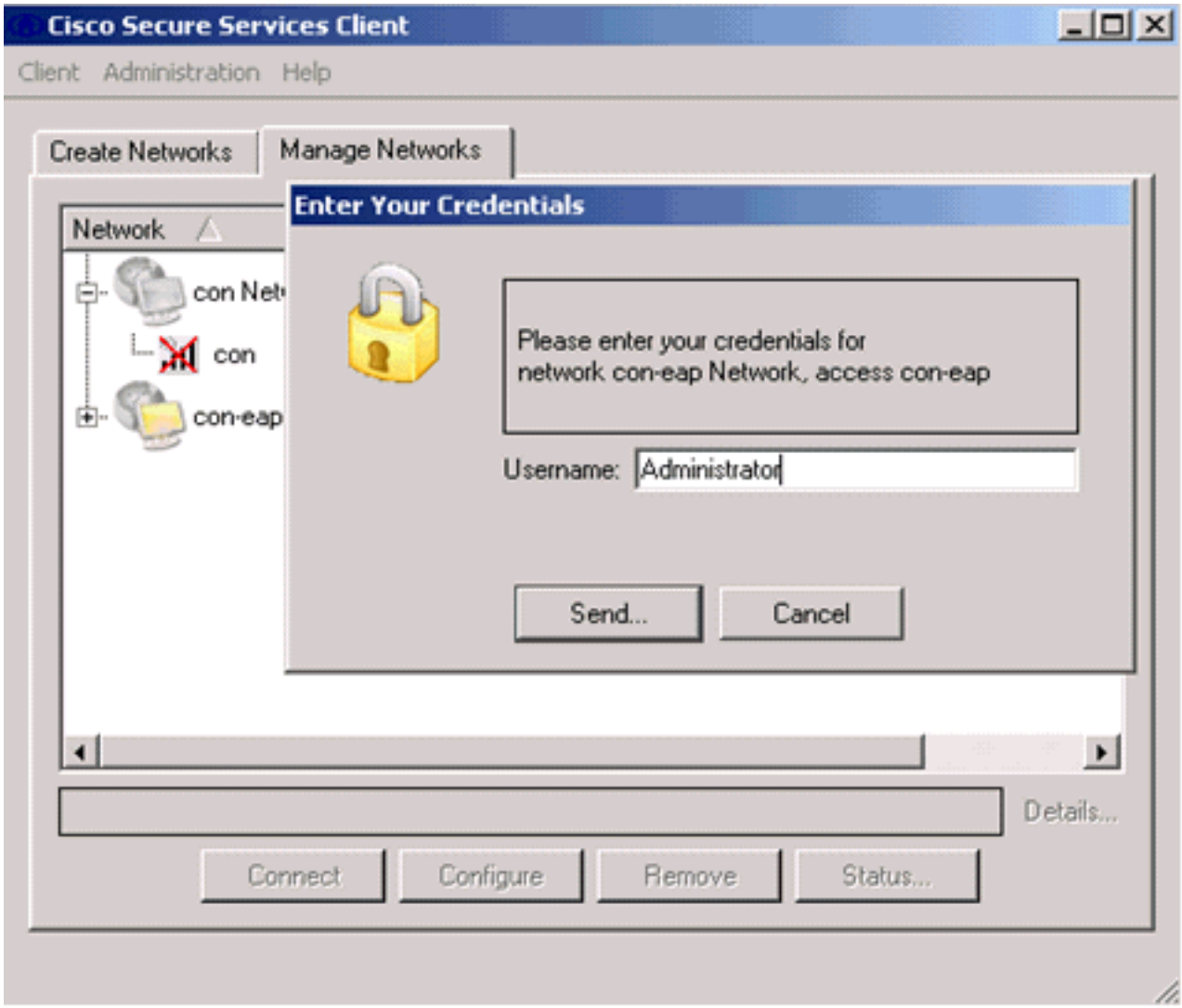
9. Forneça um nome para a regra e verifique o nome do certificado do

servidor.



A configuração EAP-TLS foi concluída.

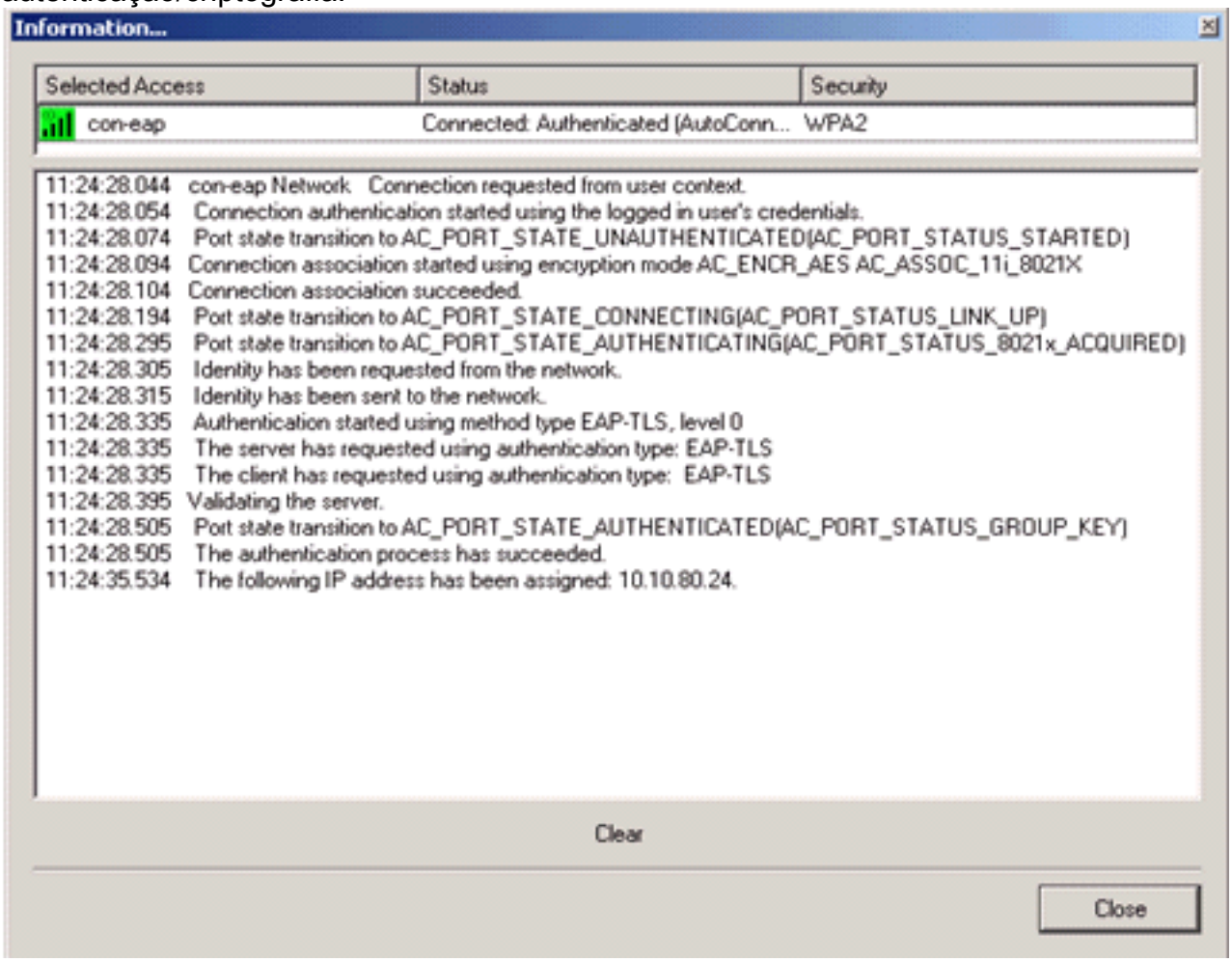
10. Conecte-se ao perfil da rede sem fio. O Cisco Secure Services Client solicita o login do usuário:

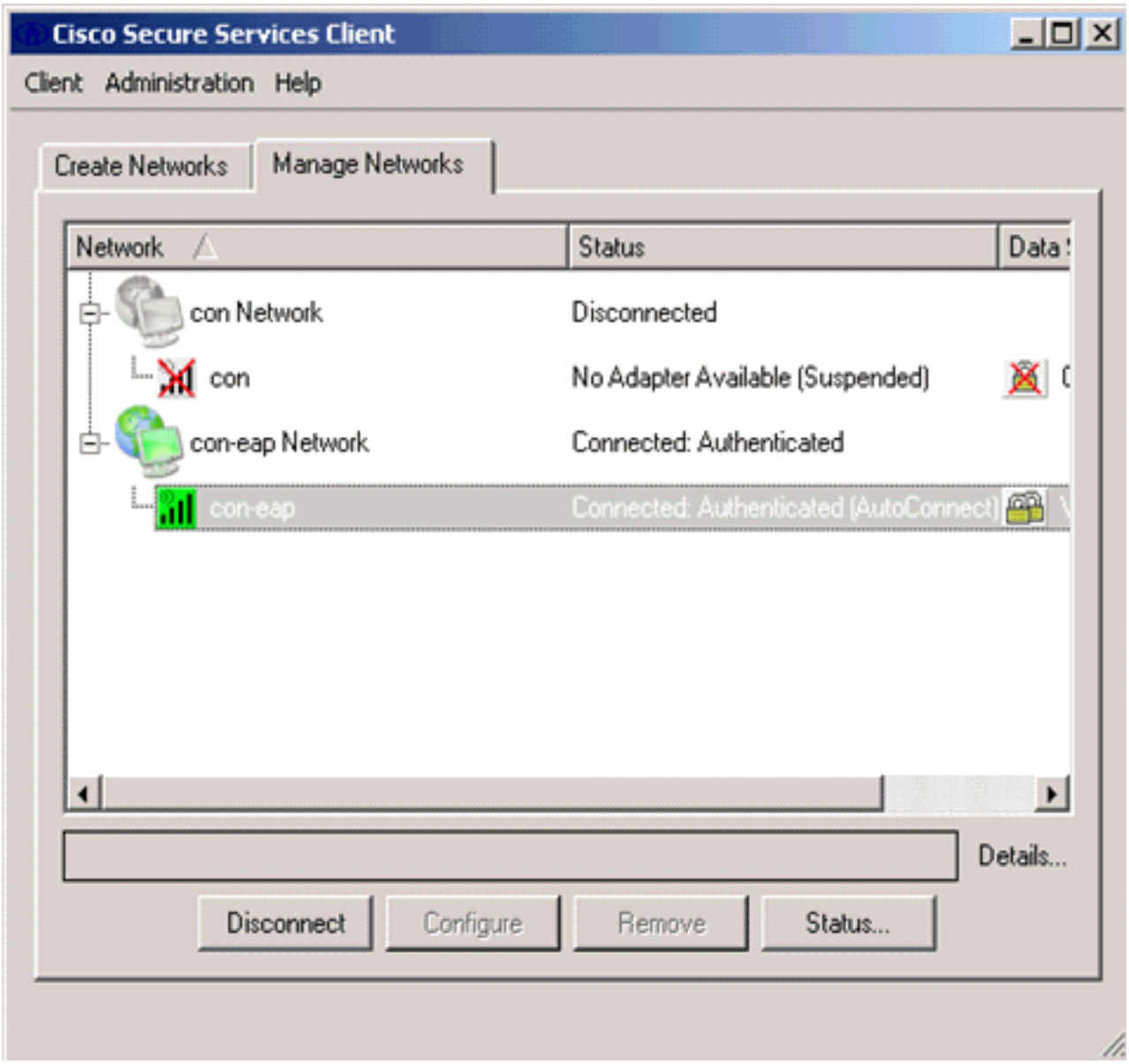


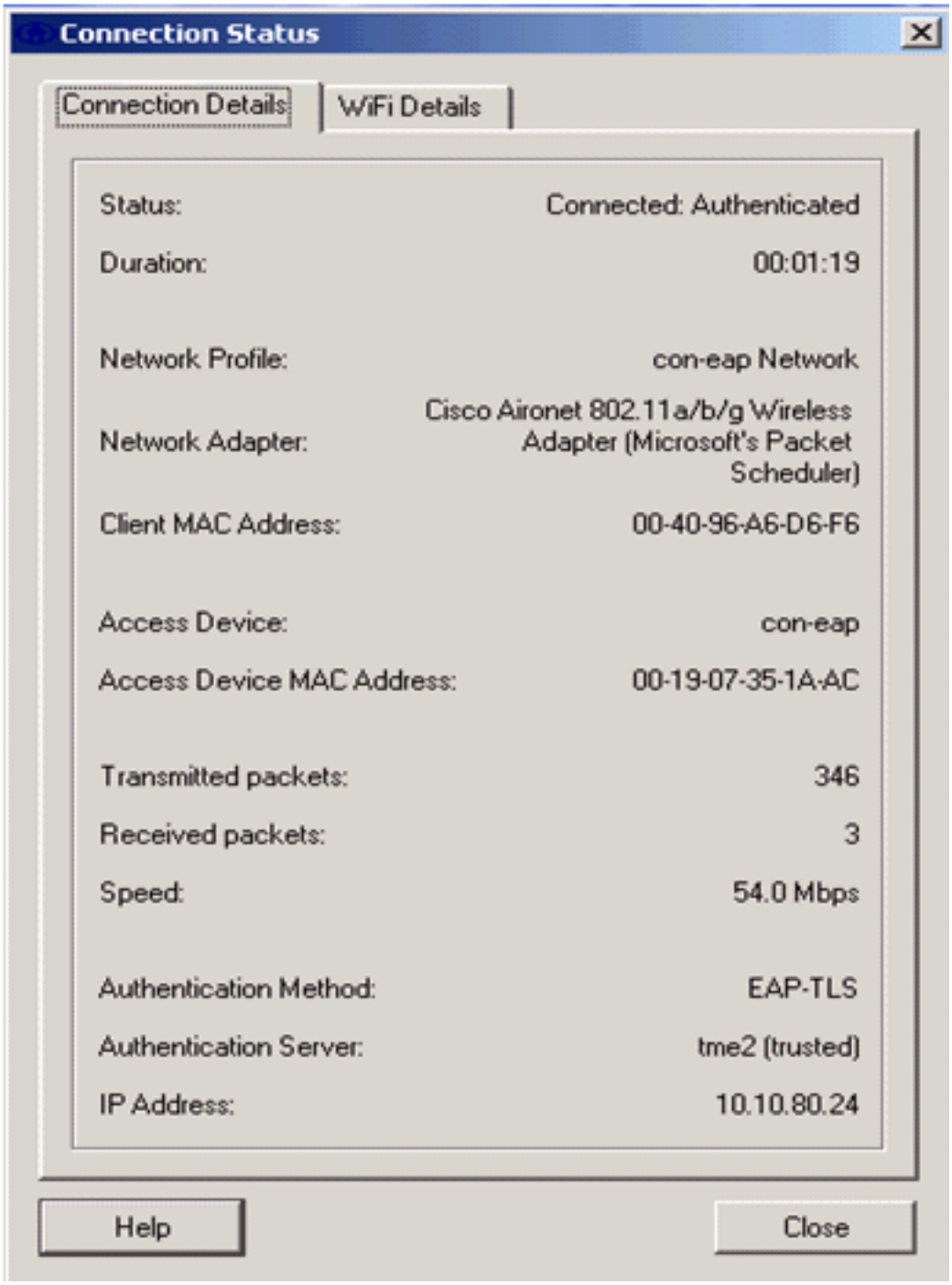
O Cisco Secure Services Client recebe o certificado do servidor e o verifica (com a regra

configurada e a Autoridade de Certificação instalada). Em seguida, solicita que o certificado seja usado para o usuário.

11. Depois que o cliente autenticar, escolha **SSID** na guia Profile (Perfil) na guia Manage Networks (Gerenciar redes) e clique em **Status** para consultar os detalhes da conexão.A janela Detalhes da conexão fornece informações sobre o dispositivo cliente, status e estatísticas da conexão e método de autenticação. A guia Detalhes do WiFi fornece detalhes sobre o status da conexão 802.11, que inclui o RSSI, o canal 802.11 e a autenticação/criptografia.




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...



Comandos debug

A Output Interpreter Tool (somente clientes registrados) (OIT) oferece suporte a determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Nota:Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos debug.

Esses comandos debug podem ser empregados na WLC para monitorar o progresso da troca de autenticação:

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

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

Informações Relacionadas

- Guia de configuração do Cisco Wireless LAN Controller, versão 4.1
- Suporte à tecnologia WLAN
- Suporte Técnico e Documentação - Cisco Systems