Exemplo de configuração de servidor local unificado da rede Wireless EAP

Índice

Introdução

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 permita os usuários e os clientes Wireless a ser autenticados localmente. É projetado para o uso nos escritórios remotos que querem manter a Conectividade aos clientes Wireless quando o sistema no final do processo se torna interrompido ou o servidor de autenticação externa vai para baixo. Quando você permite o EAP local, o controlador serve como o Authentication Server e a base de dados de usuário local, removendo desse modo a dependência em um servidor de autenticação externa. O EAP local recupera credenciais do usuário da base de dados de usuário local ou do base de dados no final do processo do Lightweight Directory Access Protocol (LDAP) para autenticar usuários. O EAP local apoia EAP de pouco peso (PULO), Autenticação Flexível de EAP através do Tunelamento seguro (EAP-FAST), e autenticação da Segurança da camada do EAP-transporte (EAP-TLS) entre o controlador e os clientes Wireless.

Note que o server local EAP não está disponível se há uma configuração de servidor de raio externo global no WLC. Todos os pedidos de autenticação estão enviados ao RAIO externo global até que o server local EAP esteja disponível. Se o WLC afrouxa a Conectividade ao servidor de raio externo, a seguir o server local EAP torna-se ativo. Se não há nenhuma configuração de servidor RADIUS global, o server local EAP torna-se imediatamente ativo. O server local EAP não pode ser usado para autenticar os clientes, que são conectados a outros WLC. Ou seja um WLC não pode enviar seu pedido EAP a um outro WLC para a autenticação. Cada WLC deve ter seus próprios server local EAP e base de dados individual.

Nota: Use estes comandos a fim parar o WLC de enviar pedidos a um servidor de raio externo.

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

Os suportes de servidor locais EAP estes protocolos no software release de 4.1.171.0 e mais tarde:

- PULO
- EAP-FAST (ambo username/senha, e Certificados)
- EAP-TLS

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento de como configurar WLC e Lightweight Access Points (regaços) para a operação básica
- Conhecimento de métodos de pouco peso do protocolo (LWAPP) e da segurança Wireless do Access point
- Conhecimento básico da autenticação de EAP local.

Componentes Utilizados

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

- Windows XP com placa de adaptadores CB21AG e versão 4.05 do Cisco Secure Services Client
- Controlador 4.1.171.0 do Wireless LAN de Cisco 4400
- Autoridade de certificação de Microsoft no servidor do Windows 2000

Convenções

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

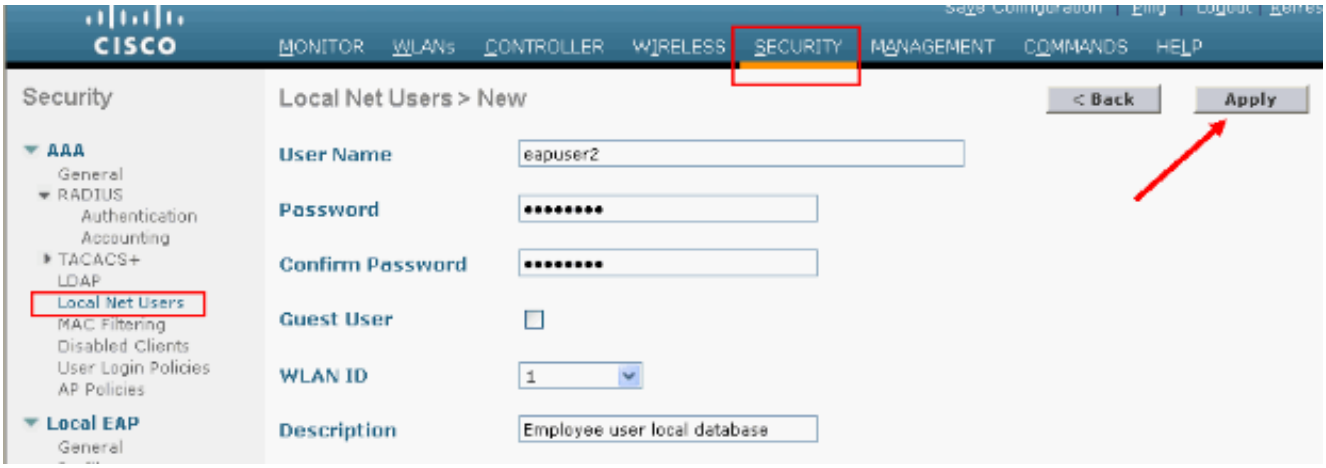
Configurar o EAP local no controlador de LAN do Cisco Wireless

Este documento supõe que a configuração básica do WLC está terminada já.

Configuração local EAP

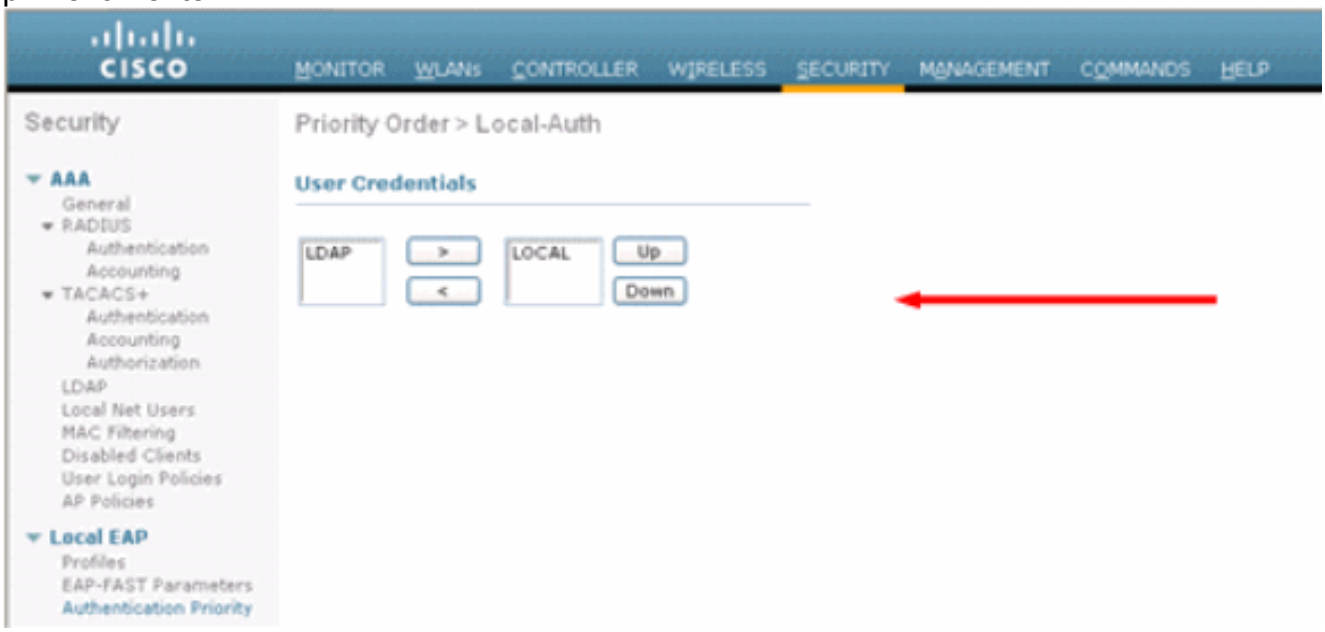
Termine estas etapas a fim configurar o EAP local:

1. Adicionar um usuário líquido local:Do GUI. escolha a **Segurança > usuários líquidos locais > novo**, dê entrada com o nome de usuário, senha, usuário convidado, ID de WLAN, e a descrição e o clique **aplicam-se**.



   Do CLI você pode usar o **netuser da configuração adiciona o** comando do *<description> do id> do <password> <WLAN do <username>*:**Nota:** Este comando foi derrubado a uma segunda linha devido às razões espaciais.`(Cisco Controller) >`**`config netuser add`** *`eapuser2 cisco123 1 Employee user local database`*

2. Especifique a ordem de recuperação credencial do usuário.Do GUI, escolha a **Segurança > local EAP > prioridade da autenticação**. Selecione então o LDAP, clicam "**<**" o botão e o clique **aplica-se**. Isto põe as credenciais do usuário no base de dados local primeiramente.

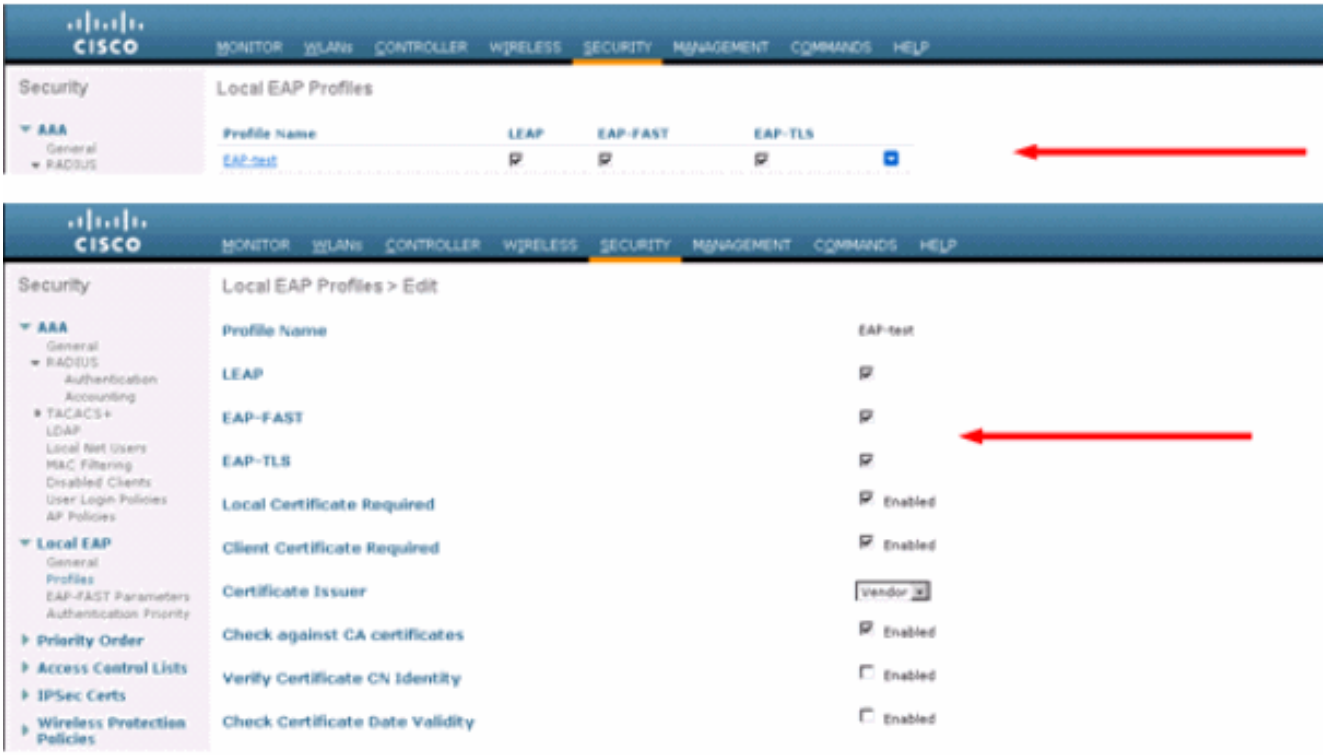


   Do CLI:`(Cisco Controller) >`**`config local-auth user-credentials local`**

3. Adicionar um perfil EAP:A fim fazer isto do GUI, escolha a **Segurança > local EAP > perfis** e clique **novo**. Quando a nova janela aparece, datilografe o nome de perfil e o clique **aplica-se**.

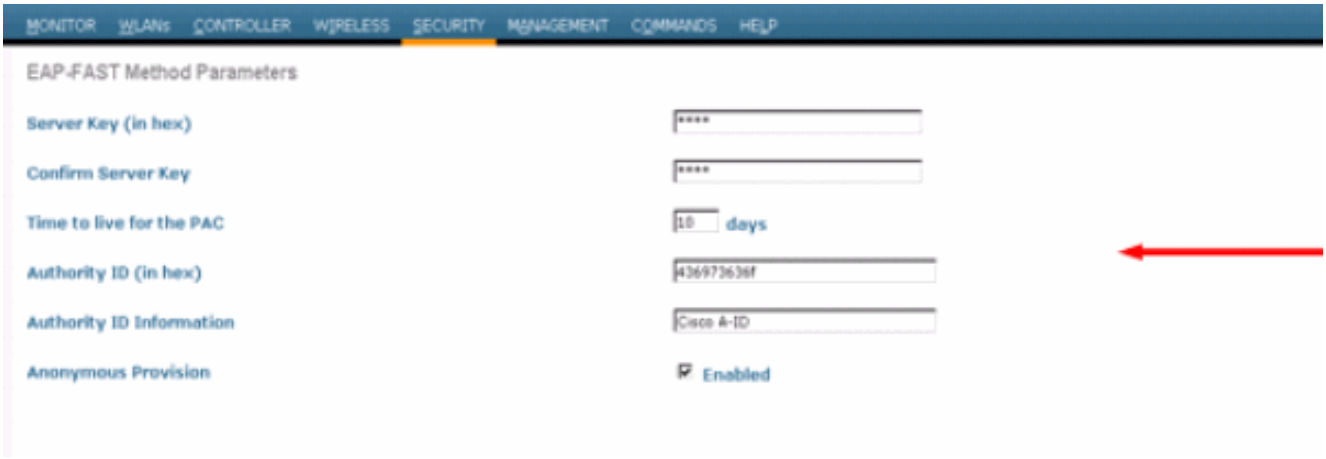
Você pode igualmente fazer este que usa o comando CLI o EAP-**perfil do local-AUTH que da configuração adiciona o** *<profile-name>.* Em nosso exemplo, o nome de perfil é EAP-*teste.*`(Cisco Controller) >`**`config local-auth eap-profile add`** *`EAP-test`*

4. Adicionar um método ao perfil EAP.Do GUI escolha a **Segurança > local EAP > perfis** e clique sobre o nome de perfil para que você quer adicionar os métodos de autenticação. Este exemplo usa o PULO, EAP-FAST, e o EAP-TLS. O clique **aplica-se** a fim ajustar os métodos.



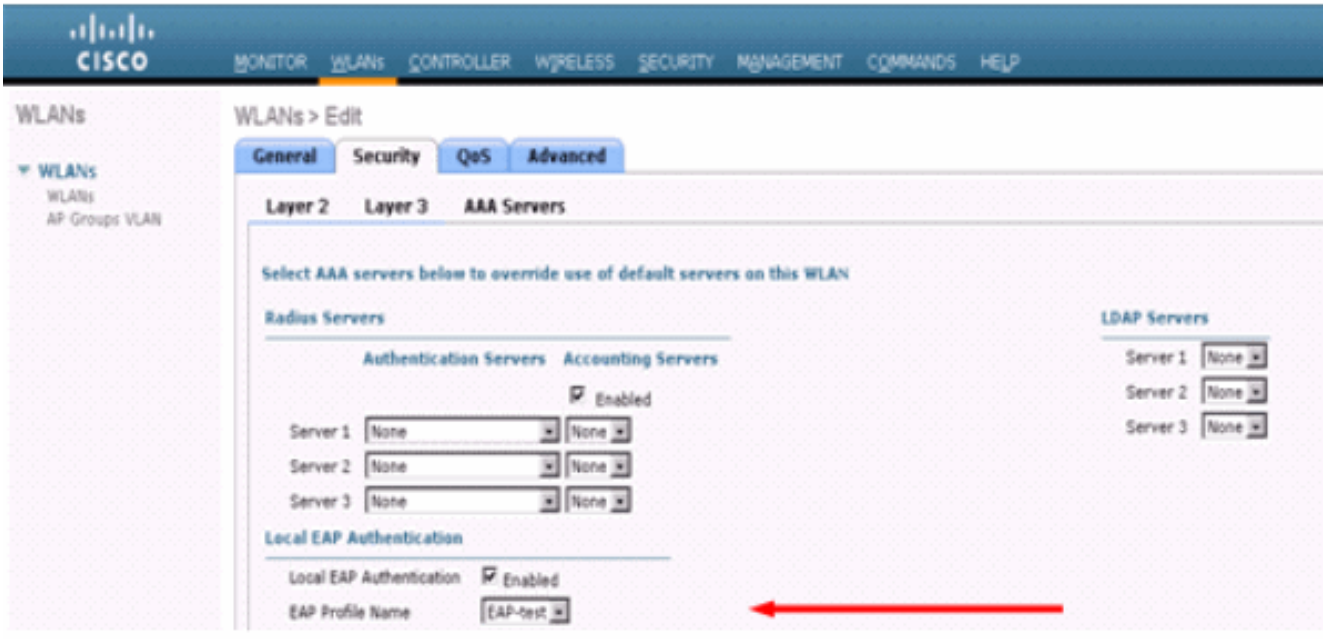
Você pode igualmente usar o comando CLI o **método do EAP-perfil que do local-AUTH da configuração adiciona o** *<profile-name> do <method-name>*. Em nosso exemplo de configuração nós adicionamos três métodos ao EAP-teste do perfil. Os métodos são o PULO, EAP-FAST, e o EAP-TLS cujos os nomes do método são pulo*, rápido,* e *tls* respectivamente. Esta saída mostra os comandos de configuração de 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. Configurar os parâmetros do método de EAP. Isto é usado somente para EAP-FAST. Os parâmetros a ser configurados são:**Chave de servidor (chave de servidor)** — Cifrar da chave de servidor/credenciais protegidas decrypt do acesso (PAC) (no hexadecimal).**Time to Live para PAC (PAC-TTL)** — Ajusta o Time to Live para o PAC.**Autoridade ID (autoridade-identificação)** — Ajusta o identificador da autoridade.**Disposição de Annonymous (anon-provn)** — Configura se a disposição anônima está permitida. Iss está habilitado por padrão.Para a configuração com o GUI, escolha a **Segurança > local EAP > parâmetros EAP-FAST** e incorpore a chave de servidor, o Time to Live para o PAC, a autoridade ID (em encantar), e os valores de informação de ID da autoridade.



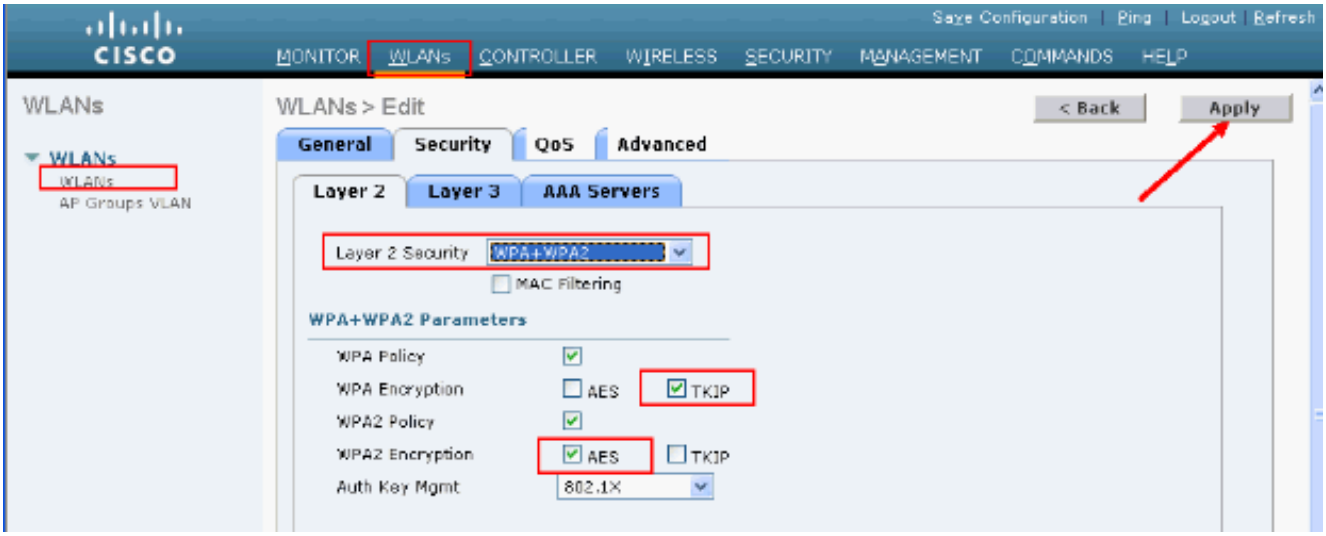
Estes são os comandos de configuração de CLI usar-se a fim ajustar estes parâmetros para EAP-FAST:`(Cisco Controller) >`**`config local-auth method fast server-key 12345678`** `(Cisco Controller) >`**`config local-auth method fast authority-id 43697369f1 CiscoA-ID`** `(Cisco Controller) >`**`config local-auth method fast pac-ttl 10`**

6. Permita a autenticação local pelo WLAN:Do GUI escolha **WLAN no** menu superior e selecione o WLAN para que você quer configurar a autenticação local. Uma nova janela aparece. Clique a **Segurança >** abas **AAA**. Verifique a **autenticação de EAP local** e selecione o nome de perfil direito EAP do menu de destruição como este exemplo mostra:



Você pode igualmente emitir a **configuração que** CLI o local-**AUTH wlan permite o** comando configuration do *<wlan-id> do <profile-name>* como mostrado aqui:`(Cisco Controller) >`**`config wlan local-auth enable EAP-test 1`**

7. Ajuste os parâmetros de segurança da camada 2.Da interface GUI, no WLAN edite o indicador vão às abas da **Segurança > da camada 2** e escolheu **WPA+WPA2 do** menu de destruição da Segurança da camada 2. Sob os parâmetros WPA+WPA2 secione, ajuste a criptografia WPA **TKIP** e WPA2 à criptografia **AES**. Clique então **aplicam-se**.

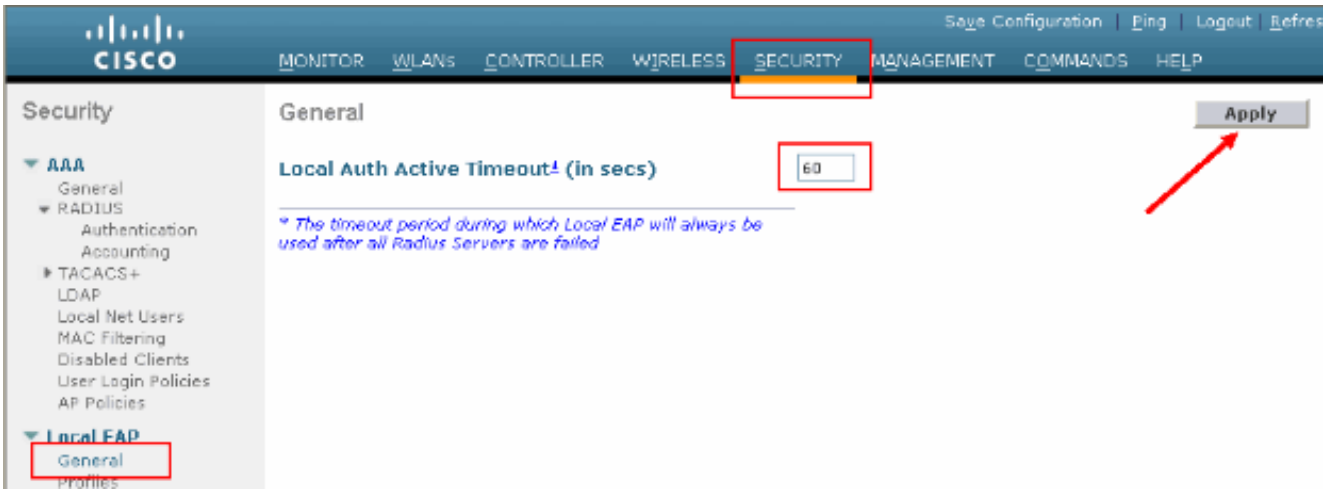


Do CLI, use estes comandos:(Cisco Controller) >**config wlan security wpa enable 1** (Cisco Controller) >**config wlan security wpa wpa1 ciphers tkip enable 1** (Cisco Controller) >**config wlan security wpa wpa2 ciphers aes enable 1**

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 ..... 43697369f10000000000000000000 Authority Information ..... CiscoA-ID Você pode ver parâmetros específicos de 1 wlan com o comando **<*wlan* wlan do *id*> *da* mostra**:(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.....

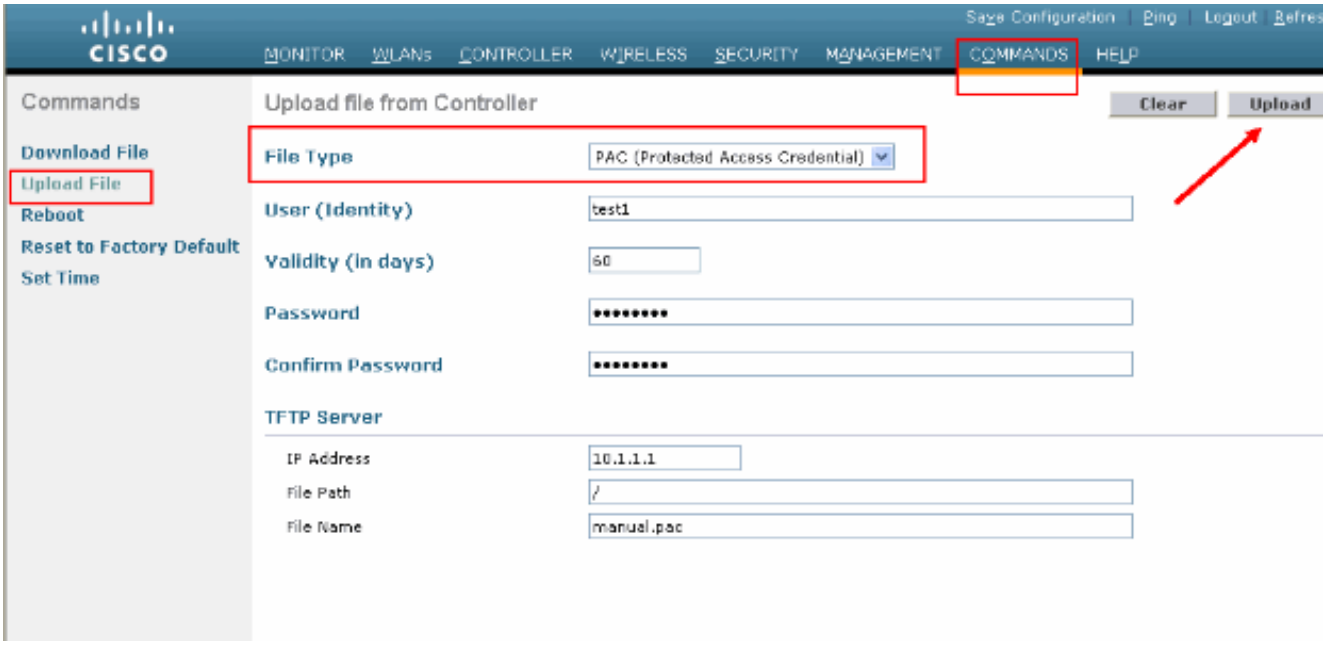
```
Disabled Wi-Fi Protected Access (WPA/WPA2)..... Enabled WPA (SSN
IE)..... Enabled TKIP Cipher..... Enabled
AES Cipher..... Disabled WPA2 (RSN
IE)..... Enabled TKIP Cipher..... Disabled
AES Cipher..... Enabled Auth Key Management
802.1x..... Enabled PSK.....
Disabled CCKM..... Disabled CKIP
..... 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 da autenticação local que podem ser configurados, em particular o temporizador ativo do intervalo. Este temporizador configura o período durante que o EAP local é afinal servidores Radius usados falhou.Do GUI, escolha a **Segurança > local EAP > geral** e ajustado o valor do tempo. Clique então **aplicam-se**.



Do 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 a que este temporizador se estabelece quando você emite o **comando config do local-AUTH da mostra**.`(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 você precisa de gerar e carregar o PAC manual, você pode usar o GUI ou o CLI.Do GUI, os **COMANDOS** seletos do menu superior e escolheram o **arquivo da transferência de arquivo pela rede da** lista no lado direito. **PAC** seleto **(credenciais protegidas do acesso) do** menu de destruição do tipo de arquivo. Incorpore todos os parâmetros e clique sobre a **transferência de arquivo pela rede**.



Do CLI, incorpore 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 de Microsoft

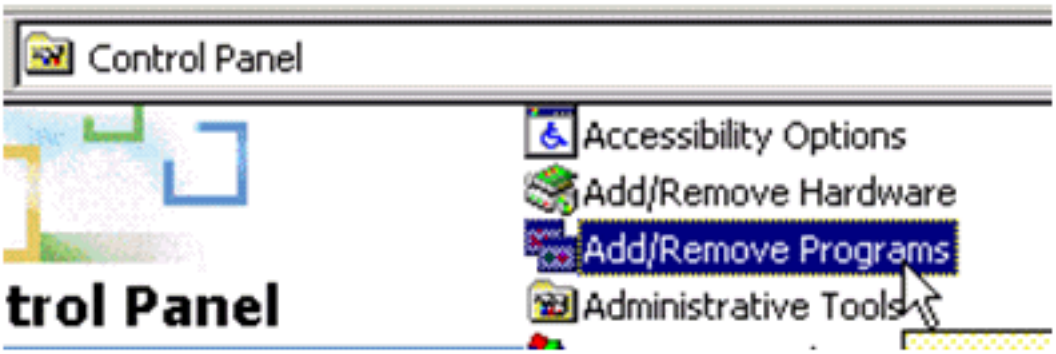
A fim usar a versão 2 EAP-FAST e a autenticação EAP-TLS, WLC e todos os dispositivos do cliente devem ter um certificado válido e devem igualmente conhecer o certificado público da autoridade de certificação.

Instalação

Se o servidor do Windows 2000 já não tem serviços da autoridade de certificação instalado, você precisa de instalá-lo.

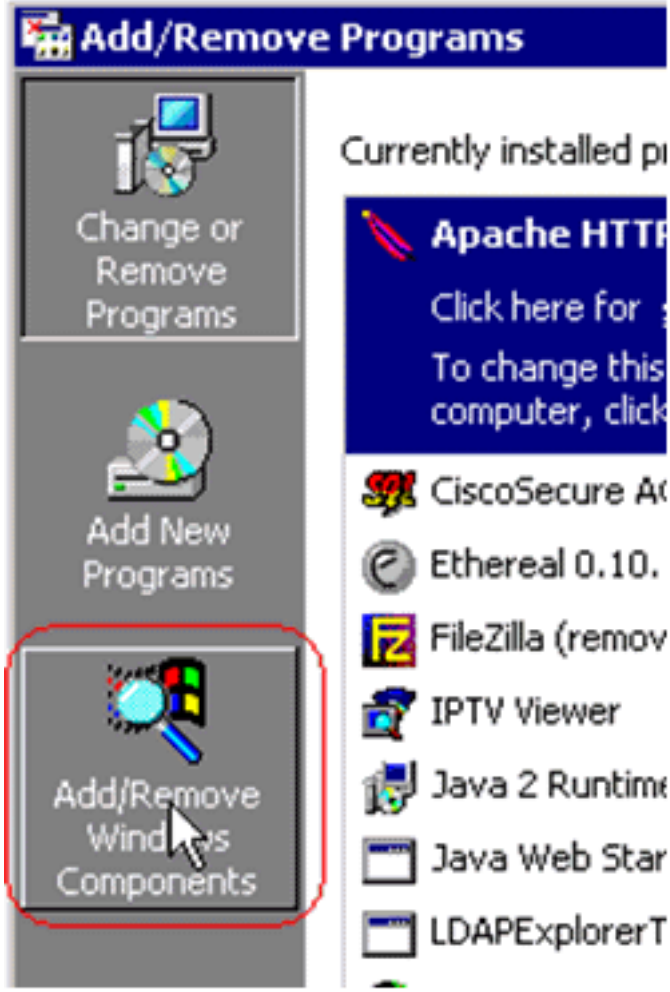
Termine estas etapas a fim ativar a autoridade de certificação de Microsoft em um servidor do Windows 2000:

1. Do Control Panel, escolha **adicionar/removeres programar**.



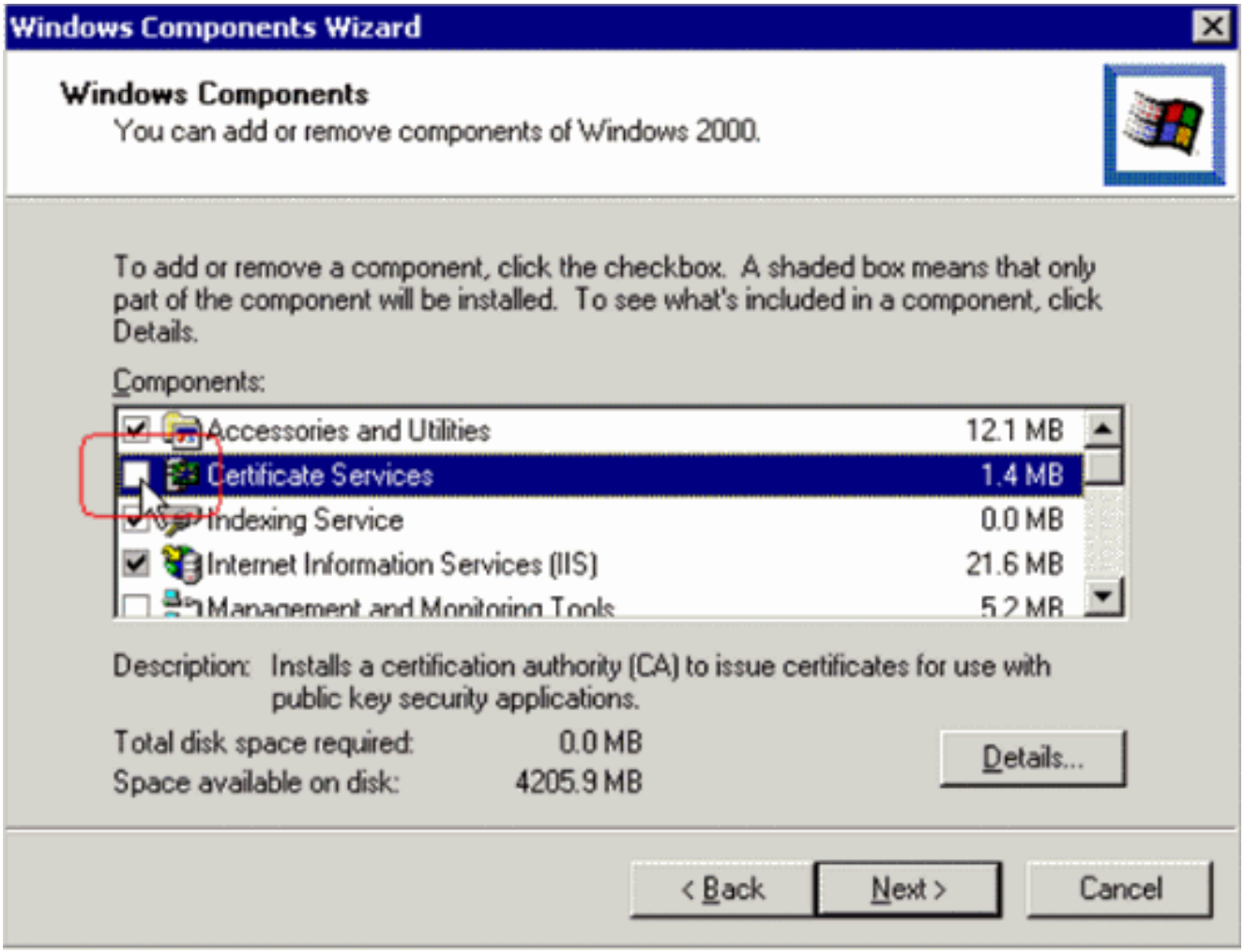
:

2. Seleto **adicionar/remova componentes do Windows no** lado

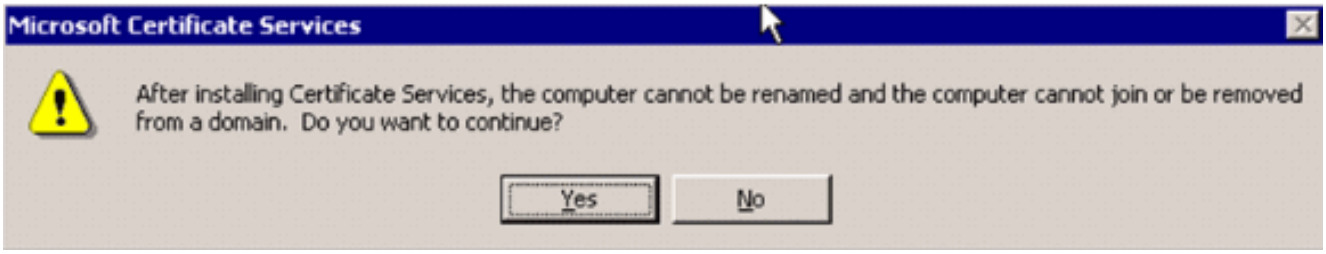


esquerdo.

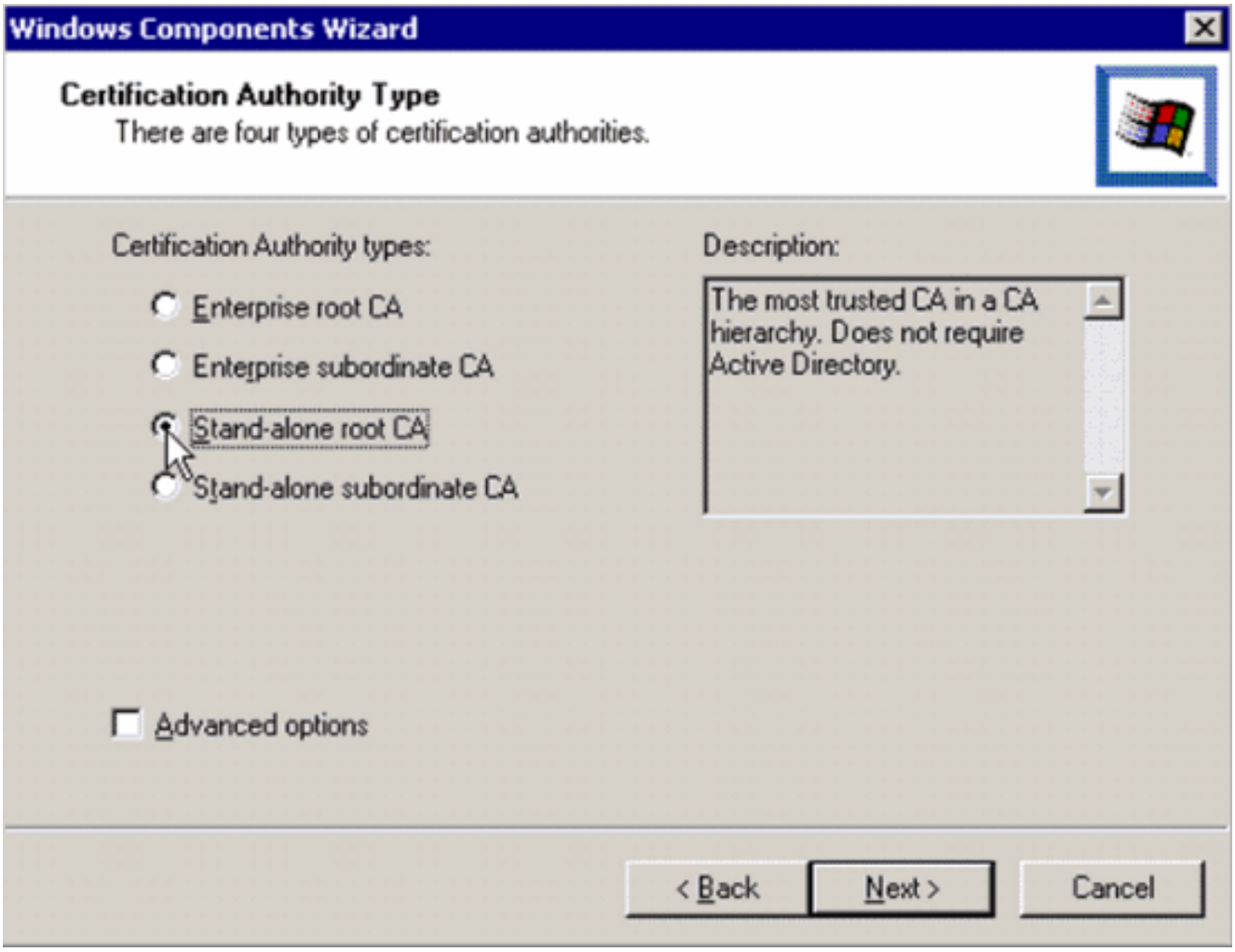
3. Verifique **serviços certificados**.



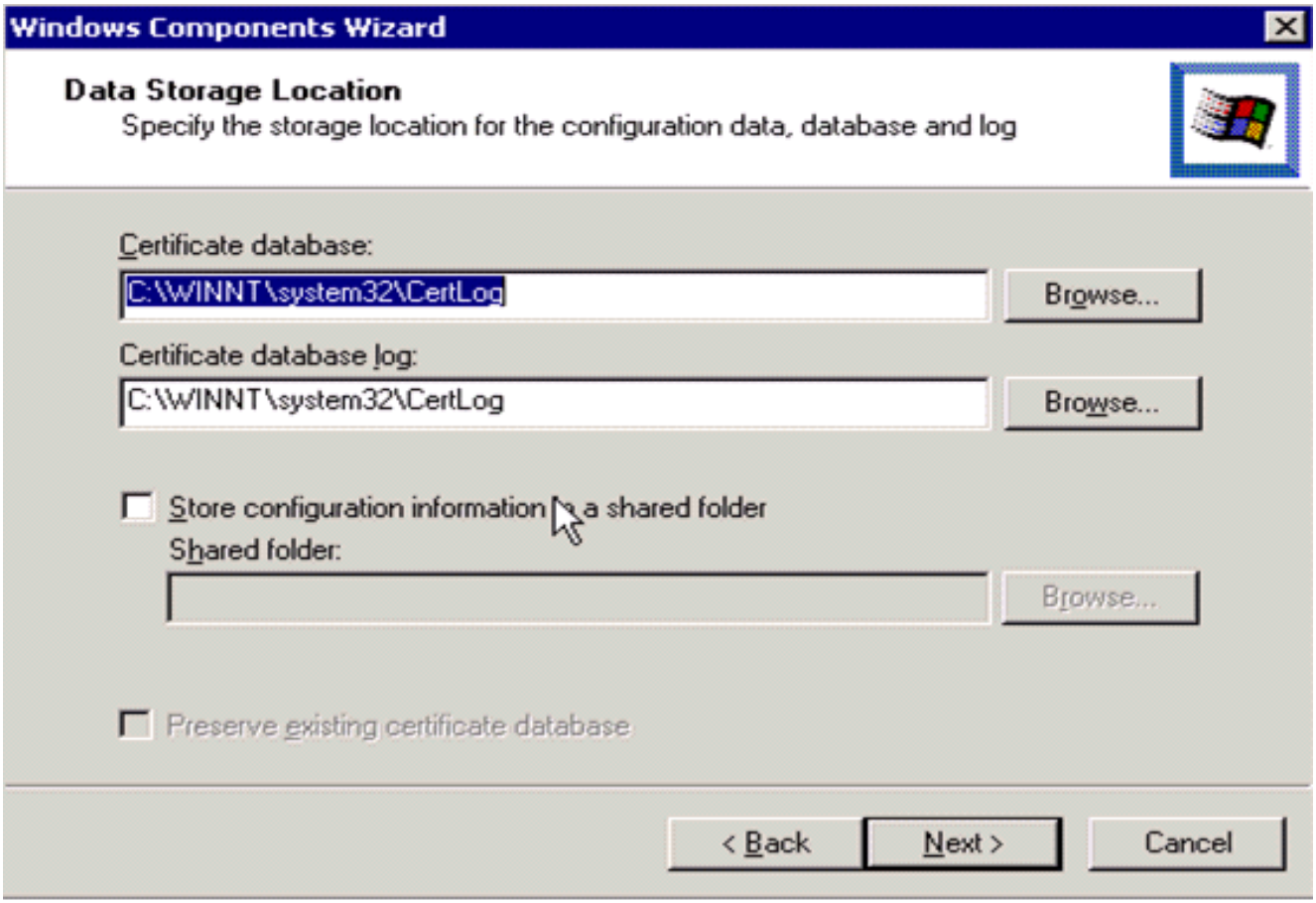
Reveja este aviso antes que você continue:



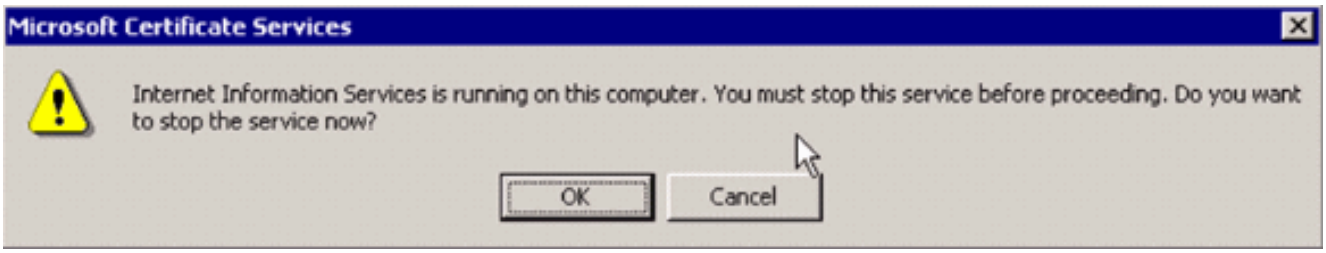
4. Selecione que o tipo de autoridade de certificação você quer instalar. A fim criar uma autoridade autônoma simples, selecione a **CA raiz autônoma.**



5. Incorpore a informação necessária sobre a autoridade de certificação. Esta informação cria um certificado auto-assinado para sua autoridade de certificação. Recorde o nome de CA que você usa.A autoridade de certificação armazena os Certificados em um base de dados. Este exemplo usa a instalação do padrão proposta por
Microsoft:



6. Os serviços da autoridade de certificação de Microsoft usam o servidor de Web IIS Microsoft a fim criar e controlar Certificados de cliente e servidor. Precisa de reiniciar o serviço IIS para
este:



O Servidor do Microsoft Windows 2000 instala agora o serviço novo. Você precisa de ter seu CD de instalação do servidor do Windows 2000 a fim instalar componentes das novas janelas.A autoridade de certificação é instalada agora.

Instale o certificado no controlador de LAN do Cisco Wireless

A fim usar a versão 2 EAP-FAST e o EAP-TLS no server local EAP de um controlador de LAN do Cisco Wireless, siga estas três etapas:

1. Instale o certificado do dispositivo no controlador do Wireless LAN.
2. Transfira um certificado de CA do vendedor ao controlador do Wireless LAN.
3. Configurar o controlador do Wireless LAN para usar o EAP-TLS.

Note que no exemplo mostrado neste documento, o Access Control Server (ACS) está instalado no mesmo host que o microsoft ative directory e na autoridade de certificação de Microsoft, mas a configuração deve ser a mesma se o servidor ACS está em um server diferente.

Instale o certificado do dispositivo no controlador do Wireless LAN

Conclua estes passos:

1. . Termine estas etapas a fim gerar o certificado para importar ao WLC:Vá a **http://<serverIpAddr>/certsrv**.Escolha o **pedido um certificado** e clique-o **em seguida**.Escolha o **pedido avançado** e clique-o **em seguida**.Escolha **submetem um pedido de certificado para este CA usando um formulário** e clicam-no **em seguida**.Escolha o **servidor de Web** para o molde de certificado e incorpore a informação relevante. Marque então as chaves como **exportable**.Você recebe agora um certificado que você precise de instalar em sua máquina.
2. Termine estas etapas a fim recuperar o certificado do PC:Abra um navegador do internet Explorer e escolha **ferramentas > opções de internet > índice**.Clique **Certificados**.Selecione o certificado recentemente instalado do menu de destruição.Clique a **exportação**.Clique **em seguida** duas vezes e escolha **sim a exportação a chave privada**. Este formato é o PKCS-12 (formato do .PFX).Escolha **permitem a proteção forte**.Datilografe uma senha.Salvar a em um arquivo <tme2.pfx>.
3. Copie o certificado no formato do PKCS-12 a todo o computador onde você tem o OpenSSL instalado a fim o converter ao formato PEM.`openssl pkcs12 -in tme2.pfx -out tme2.pem` *!--- The command to be given, -in <inputfilename>.* `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. Transfira o certificado convertido do dispositivo de formatação PEM no 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. Uma vez que recarregado, 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`

Transfira um certificado de CA do vendedor ao controlador do Wireless LAN

Conclua estes passos:

1. Termine estas etapas a fim recuperar o certificado de CA do vendedor:Vá a **http://<serverIpAddr>/certsrv**.Escolha **recuperam o certificado de CA** e clicam-no **em seguida**.Escolha o certificado de CA.Clique o **DER codificado**.Clique sobre o **certificado de CA da transferência** e salvar o certificado como **rootca.cer**.
2. Converta o vendedor que CA do formato DER no formato PEM com o **OpenSSL x509 - em rootca.cer - informa o DER - para fora rootca.pem - comando do outform PEM**.O arquivo de saída é rootca.pem no formato PEM.
3. Transfira o certificado de CA do vendedor:`(Cisco Controller) >`**`transfer download datatype`**

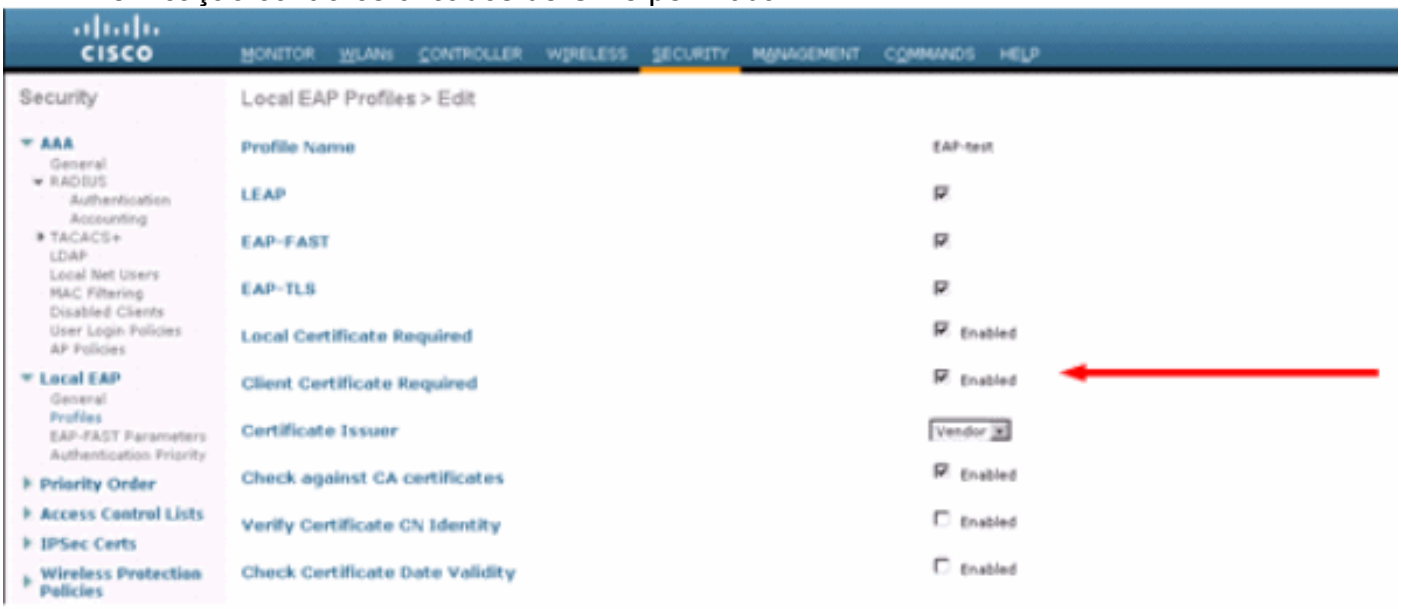
```
eapcacert (Cisco Controller) >transfer download filename ? <filename> Enter filename up to
16 alphanumeric characters. (Cisco Controller) >transfer download filename rootca.pem
(Cisco Controller) >transfer download start ? (Cisco Controller) >transfer download start
Mode..................................... 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.
```

Configurar o controlador do Wireless LAN para usar o EAP-TLS

Conclua estes passos:

Do GUI, escolha a **Segurança > local EAP > perfis**, escolha o perfil e verifique-o para ver se há estes ajustes:

- O certificado local exigido é permitido.
- O certificado de cliente exigido é permitido.
- O expedidor do certificado é vendedor.
- A verificação contra certificados de CA é permitida.



Instale o certificado do Certificate Authority no dispositivo do cliente

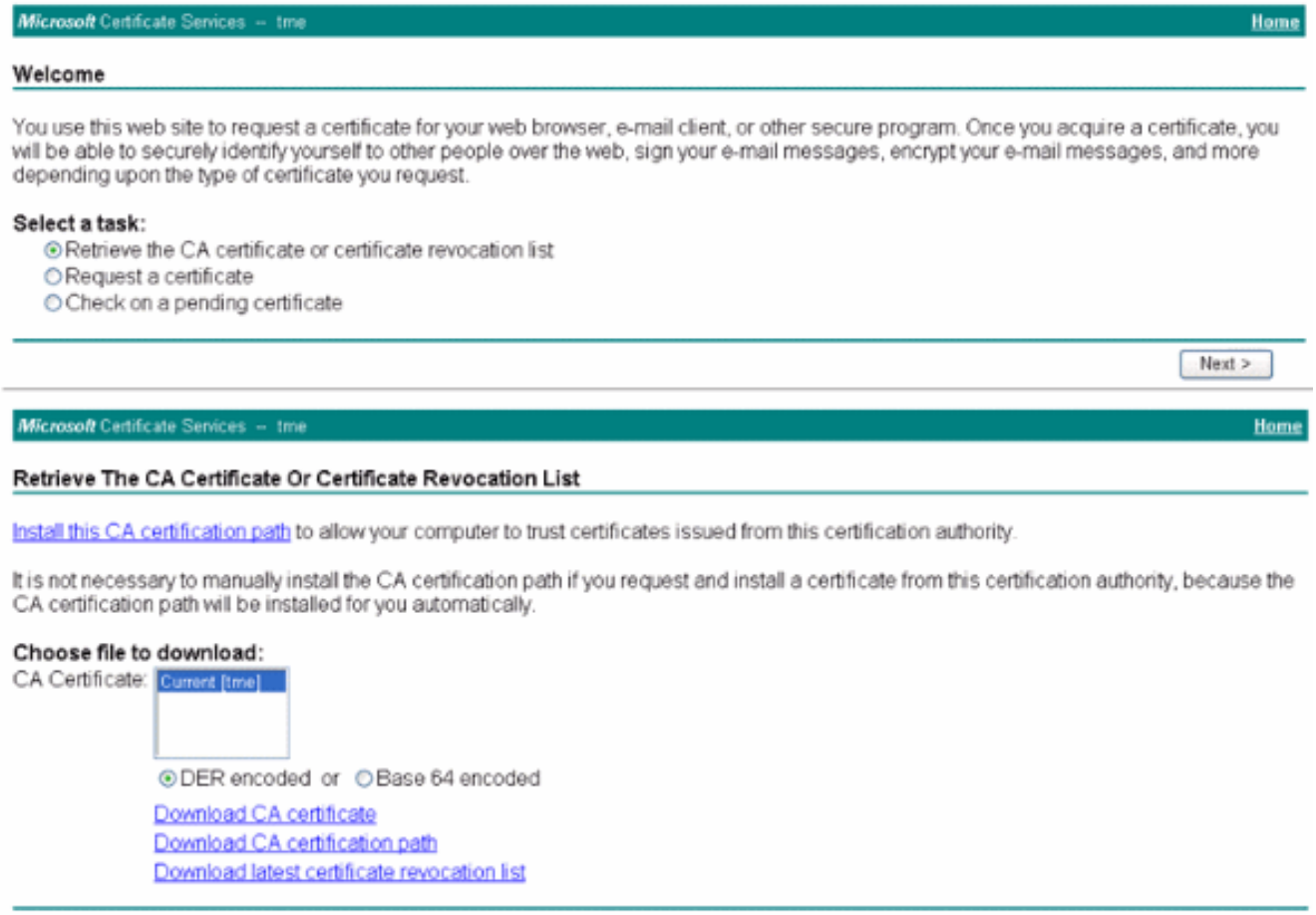
Transfira e instale um certificado CA raiz para o cliente

O cliente deve obter um certificado CA raiz de um server da autoridade de certificação. Há diversos métodos que você pode se usar para obter um certificado de cliente e para o instalar na máquina de Windows XP. A fim adquirir um certificado válido, o usuário de Windows XP tem que ser entrado usando seu usuário - identificação e deve ter uma conexão de rede.

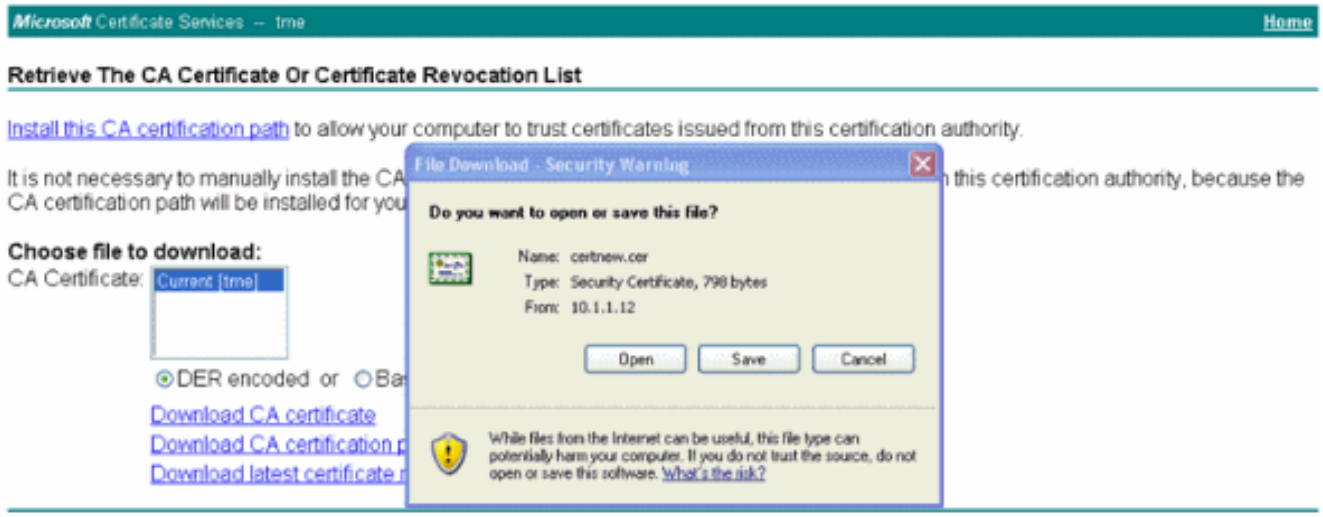
Um navegador da Web no cliente de Windows XP e uma conexão ligada com fio à rede foram usados para obter um certificado de cliente do server privado da autoridade de certificação da

raiz. Este procedimento é usado para obter o certificado de cliente de um server da autoridade de certificação de Microsoft:

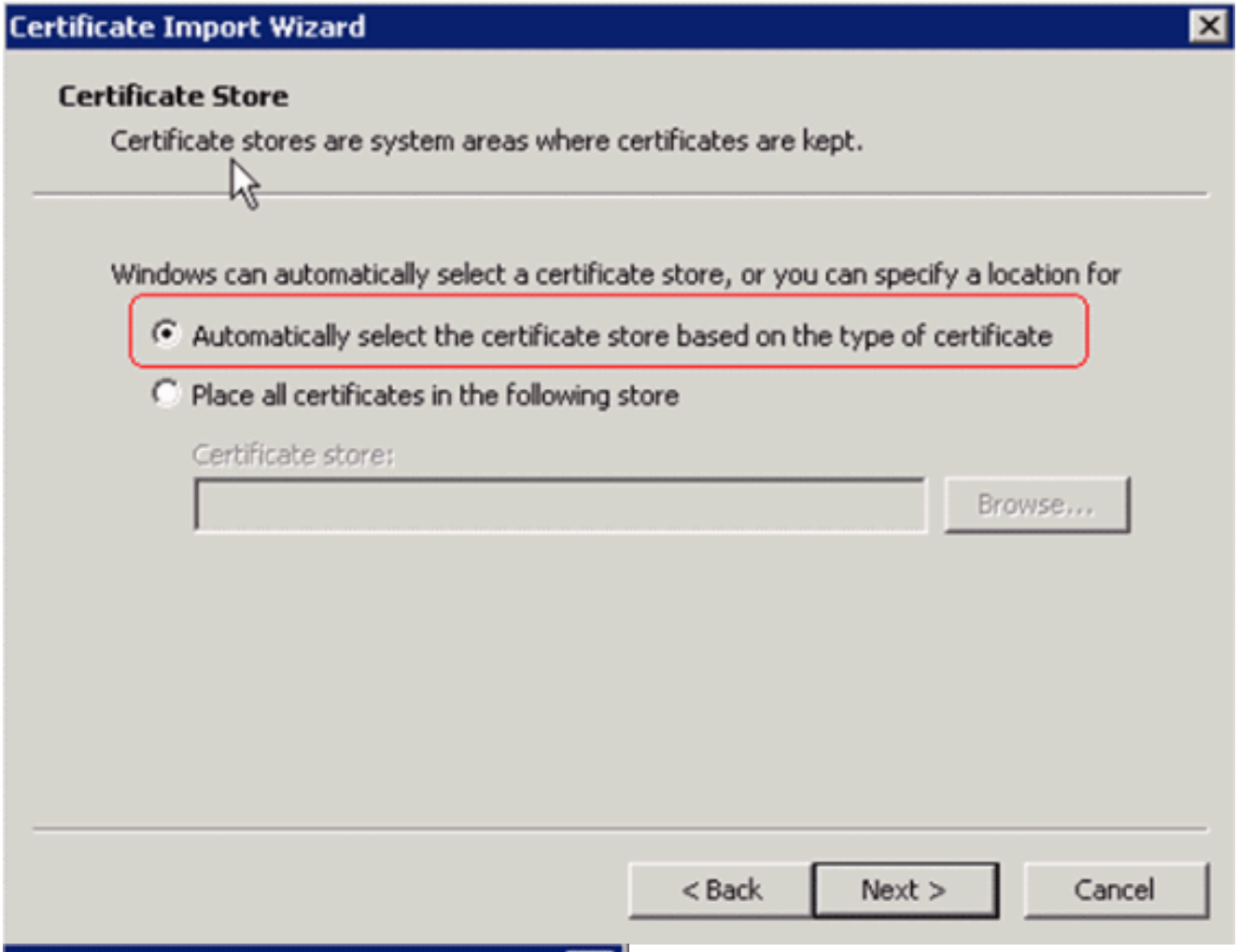
1. Use um navegador da Web no cliente e aponte o navegador ao server da autoridade de certificação. A fim fazer isto, entre em **http://IP-address-of-Root-CA/certsrv**.
2. Entre usando **Domain_Name \ user_name**. Você deve entrar usando o username do indivíduo que é usar o cliente XP.
3. No indicador bem-vindo, escolha **recuperam um certificado de CA** e clicam-no **em seguida**.
4. Selecione **Base64 que codifica** e **transfira o certificado de CA**.
5. No indicador emitido certificado, o clique **instala este certificado** e clica-o **em seguida**.
6. Escolha **automaticamente seleto a loja do certificado** e clique-a **em seguida**, para a mensagem bem sucedida da importação.
7. Conecte à autoridade de certificação para recuperar o certificado do Certificate Authority:



8. Clique o **certificado de CA da transferência**.

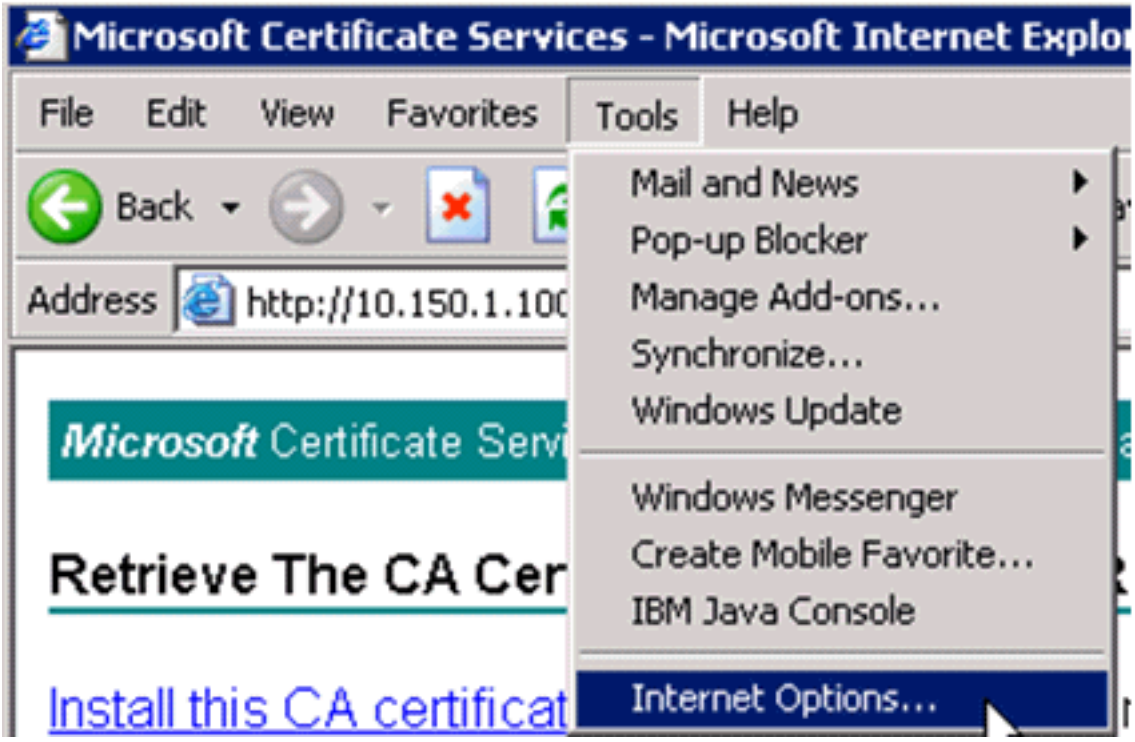

Microsoft Certificate Services -- tme
Home
Retrieve The CA Certificate Or Certificate Revocation List
Install this CA certification path to allow your computer to trust certificates issued from this certification authority.
It is not necessary to manually install the CA
this certification authority, because the
CA certification path will be installed for you
Choose file to download:
CA Certificate:
Current [tme]
DER encoded or
Download CA certificate
Download CA certification p
Download latest certificate r
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?

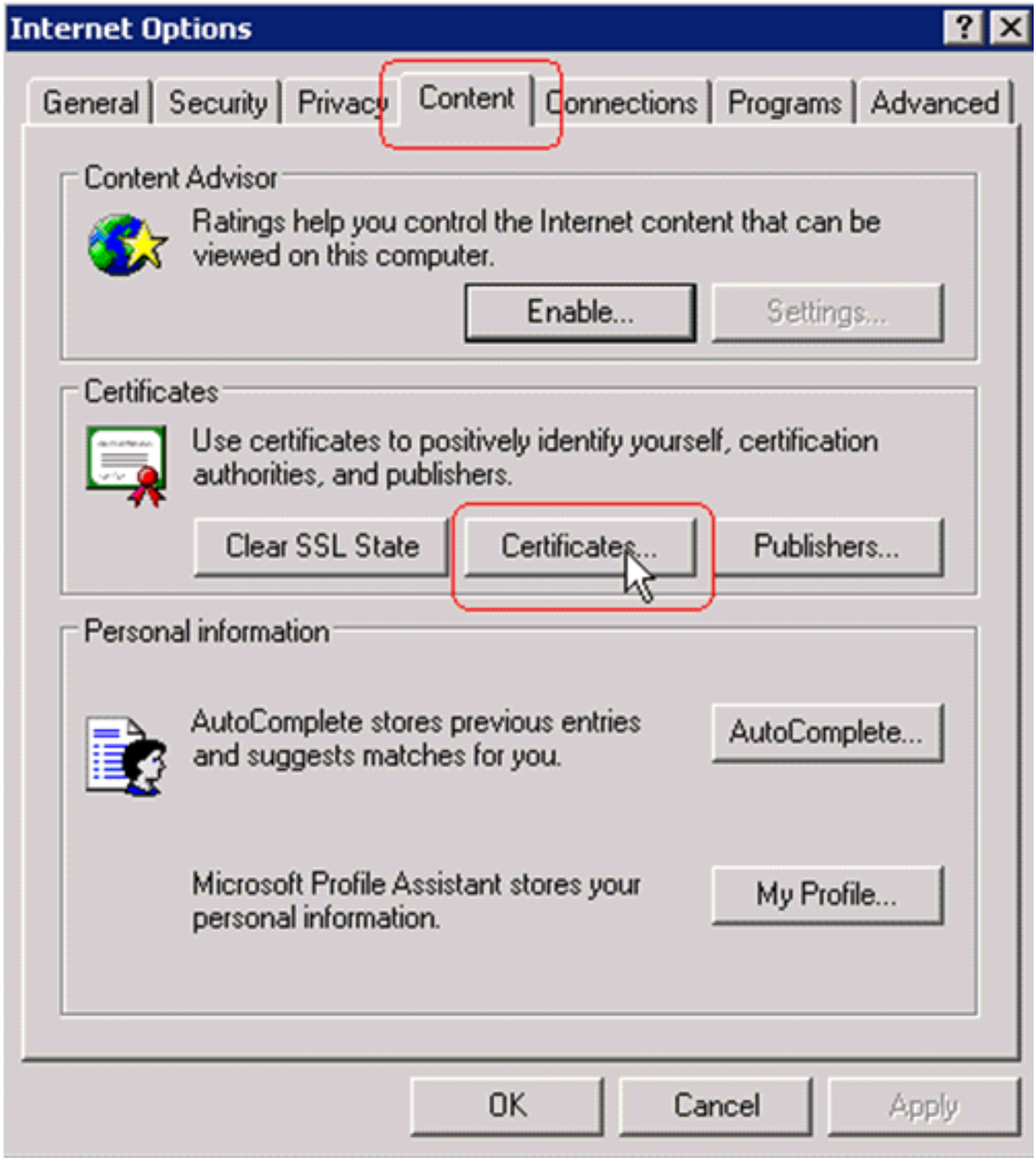

Certificate Import Wizard
Welcome to the Certificate Import Wizard
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
A certificate, which is issued by a certification authority, is a confirmation of your identity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



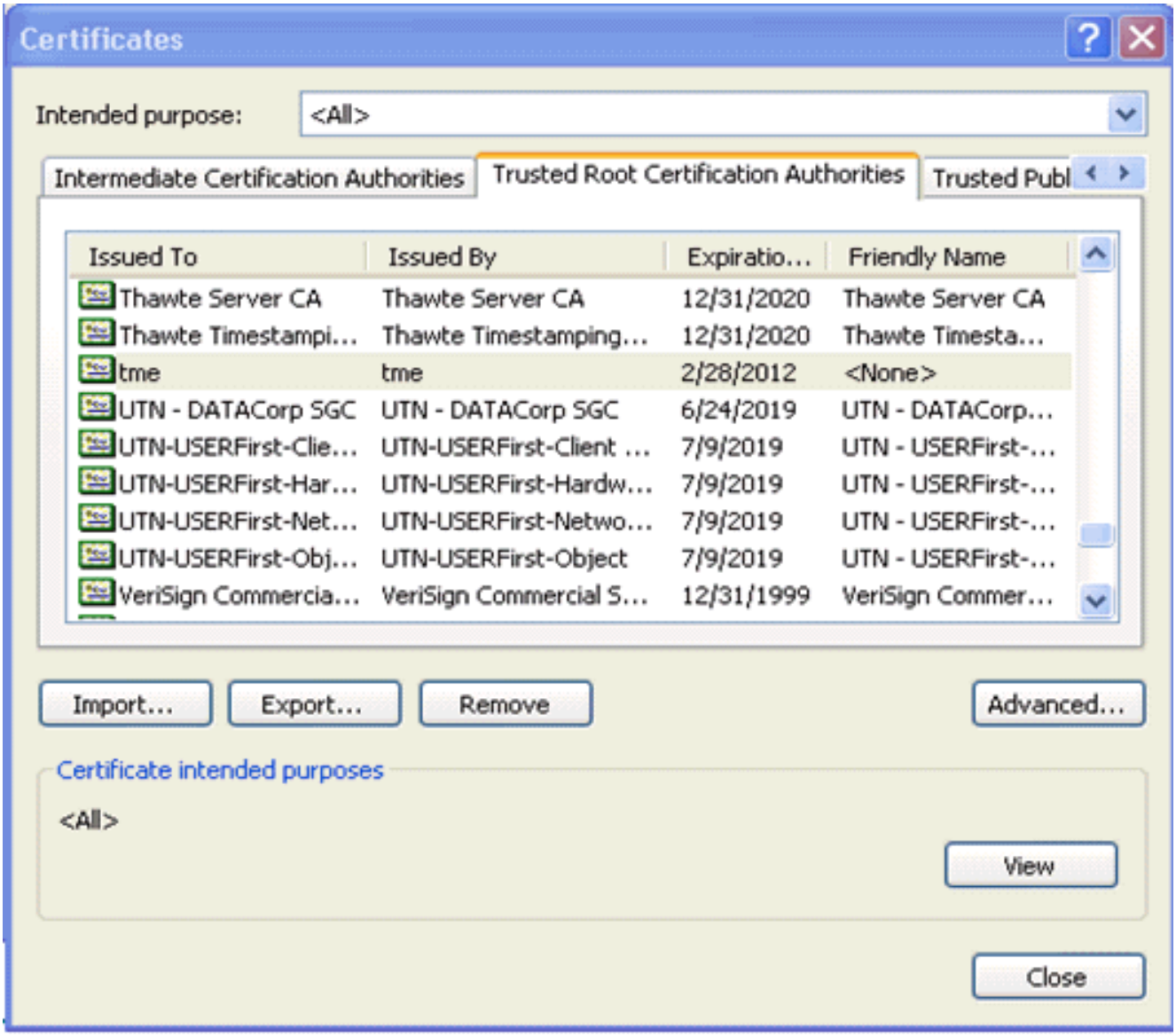
9. A fim certificar-se do certificado de autorização de certificação esteja instalado corretamente, internet explorer aberto e escolher **ferramentas > opções de internet > índice >**

Certificados.





Na Autoridade de certificação de raiz confiável, você deve ver sua autoridade de certificação recentemente
instalada:



Gerencia um certificado de cliente para um dispositivo do cliente

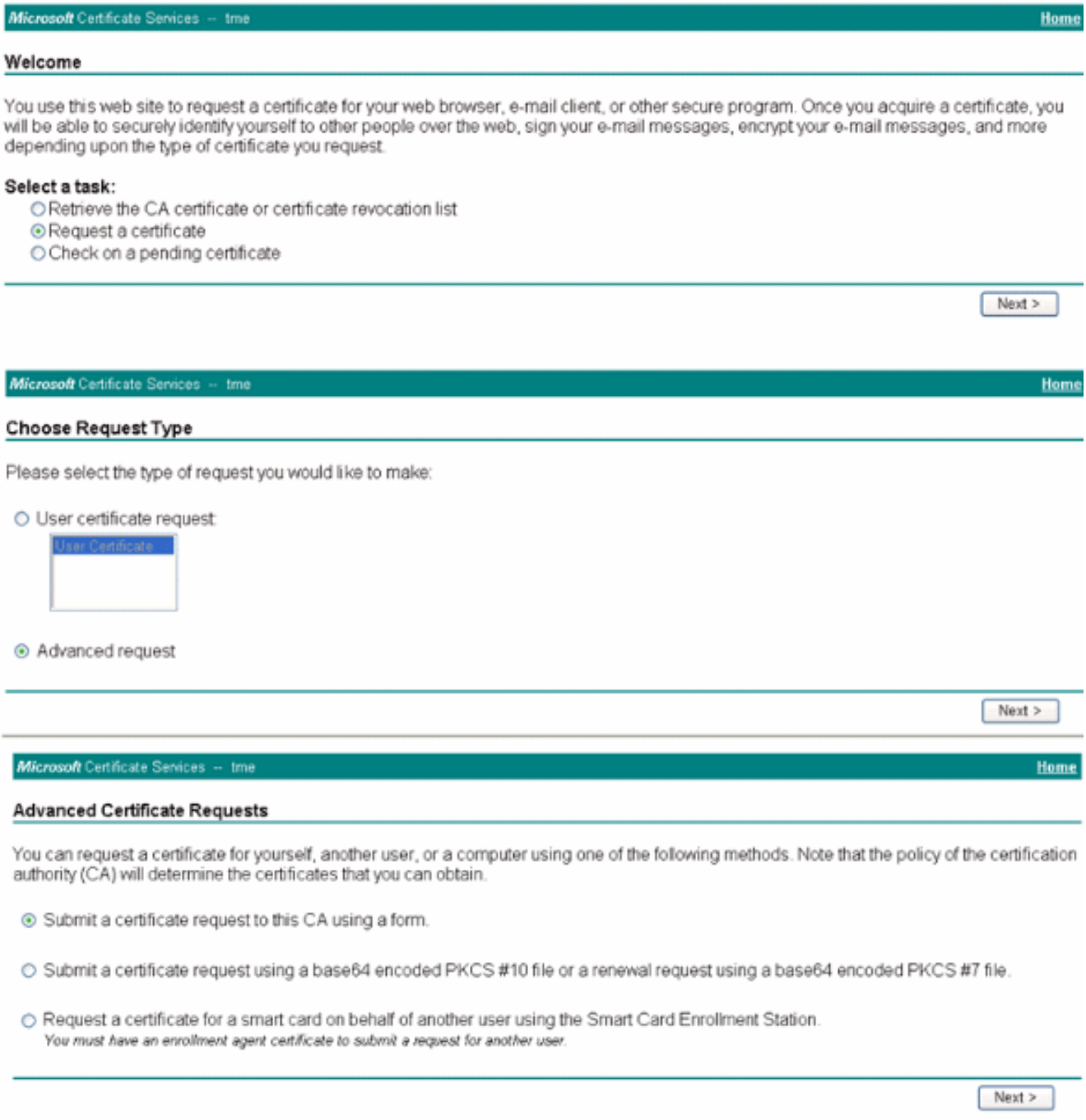
O cliente deve obter um certificado de um server da autoridade de certificação para que o WLC autentique um cliente do EAP-TLS WLAN. Há diversos métodos que você pode usar a fim obter um certificado de cliente e o instalar na máquina de Windows XP. A fim adquirir um certificado válido, o usuário de Windows XP tem que ser entrado usando seu usuário - identificação e deve ter uma conexão de rede (uma conexão ligada com fio ou uma conexão WLAN com a Segurança do 802.1x desabilitada).

Um navegador da Web no cliente de Windows XP e uma conexão ligada com fio à rede são usados para obter um certificado de cliente do server privado da autoridade de certificação da raiz. Este procedimento é usado para obter o certificado de cliente de um server da autoridade de certificação de Microsoft:

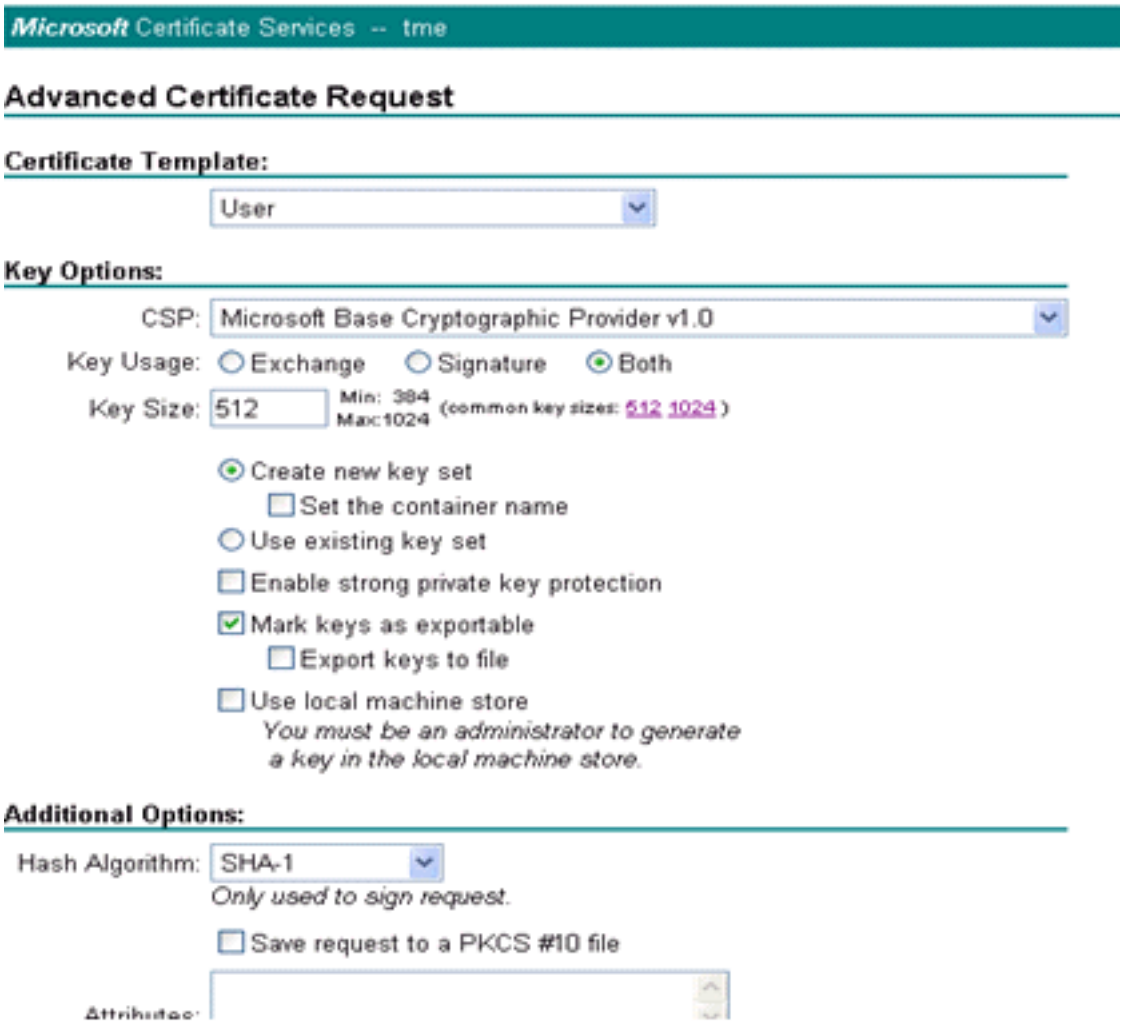
1. Use um navegador da Web no cliente e aponte o navegador ao server da autoridade de certificação. A fim fazer isto, entre em **http://IP-address-of-Root-CA/certsrv**.
2. Entre usando **Domain_Name \ user_name**. Você deve entrar usando o username do indivíduo que usa o cliente XP. (O username obtém encaixado no certificado de cliente.)
3. No indicador bem-vindo, escolha o **pedido um certificado** e clique-o **em seguida**.
4. Escolha o **pedido avançado** e clique-o **em seguida**.
5. Escolha **submetem um pedido de certificado para este CA usando um formulário** e clicam-no

em seguida.

6. No formulário de requisição de certificado avançado, escolha o molde de certificado como o **usuário**, especificam o tamanho chave como **1024** e o clique **submete-se**.
7. No indicador emitido certificado, o clique **instala este certificado**. Isto conduz à instalação bem-sucedida de um certificado de cliente no cliente de Windows XP.

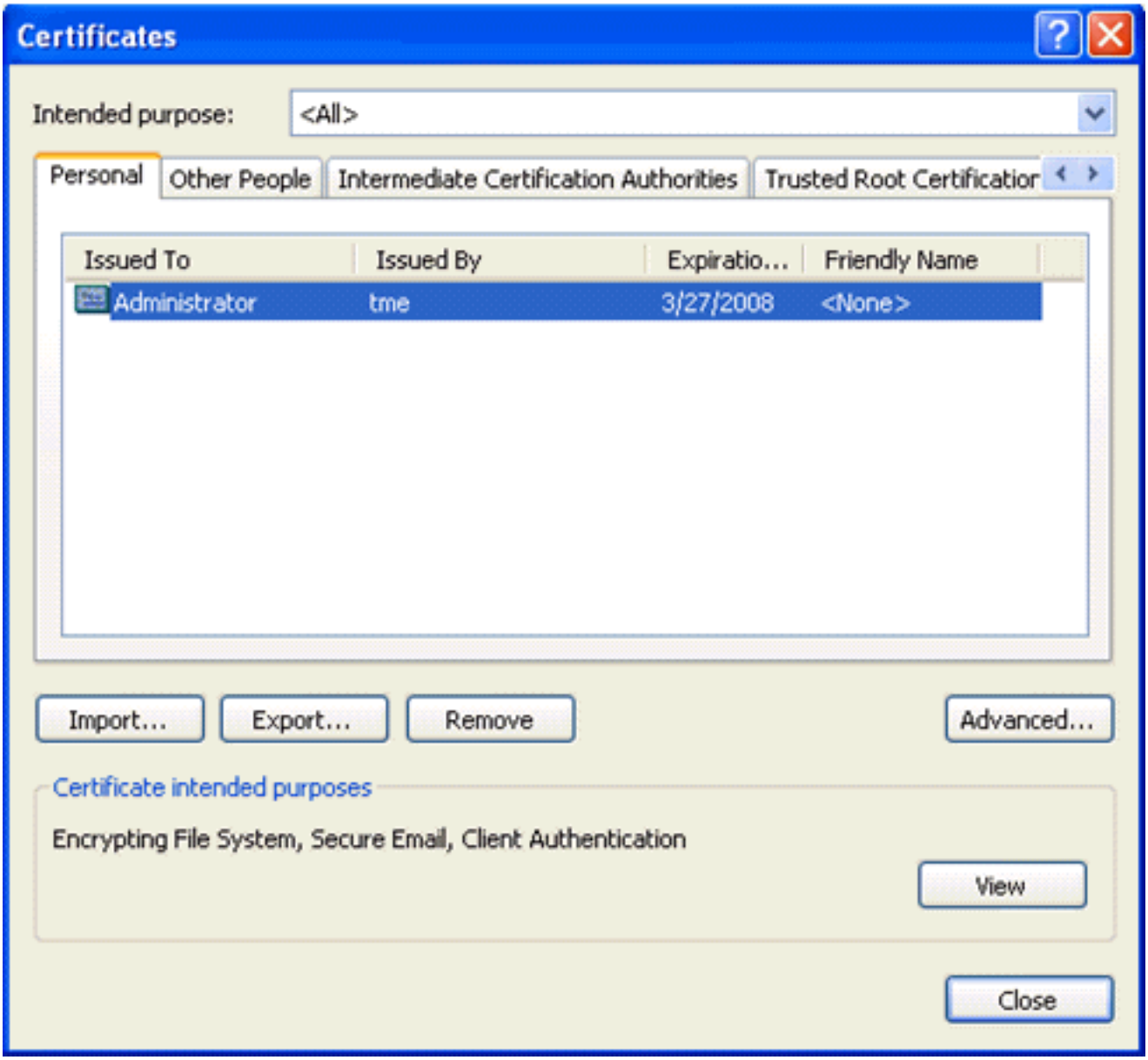


8. Selecione o **certificado de autenticação de**



cliente. O certificado de cliente é criado agora.

9. A fim certificar-se do certificado esteja instalado, vá ao internet explorer e escolha **ferramentas > opções de internet > índice > Certificados**. Na aba pessoal, você deve ver o certificado.

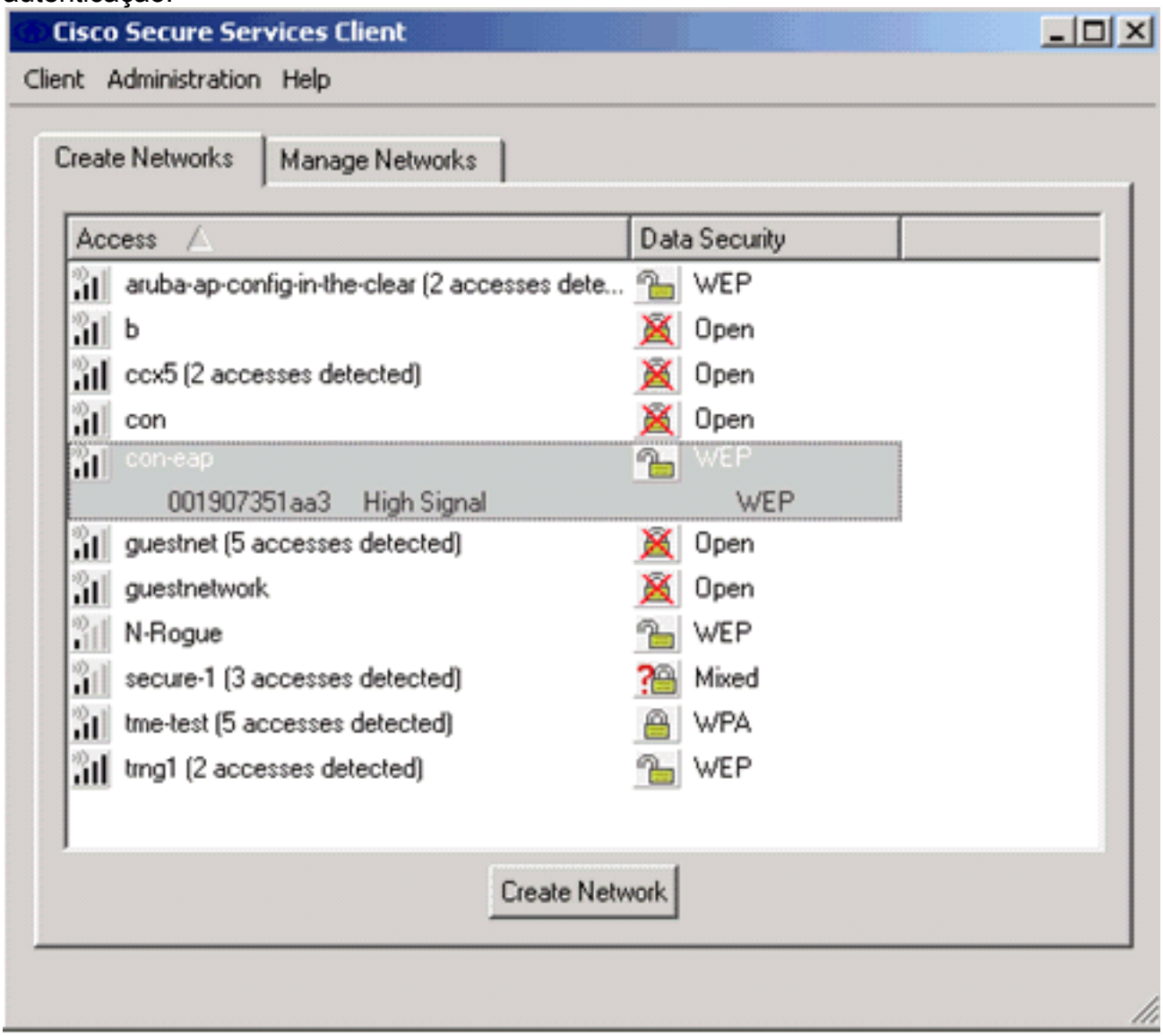


EAP-TLS com o Cisco Secure Services Client no dispositivo do cliente

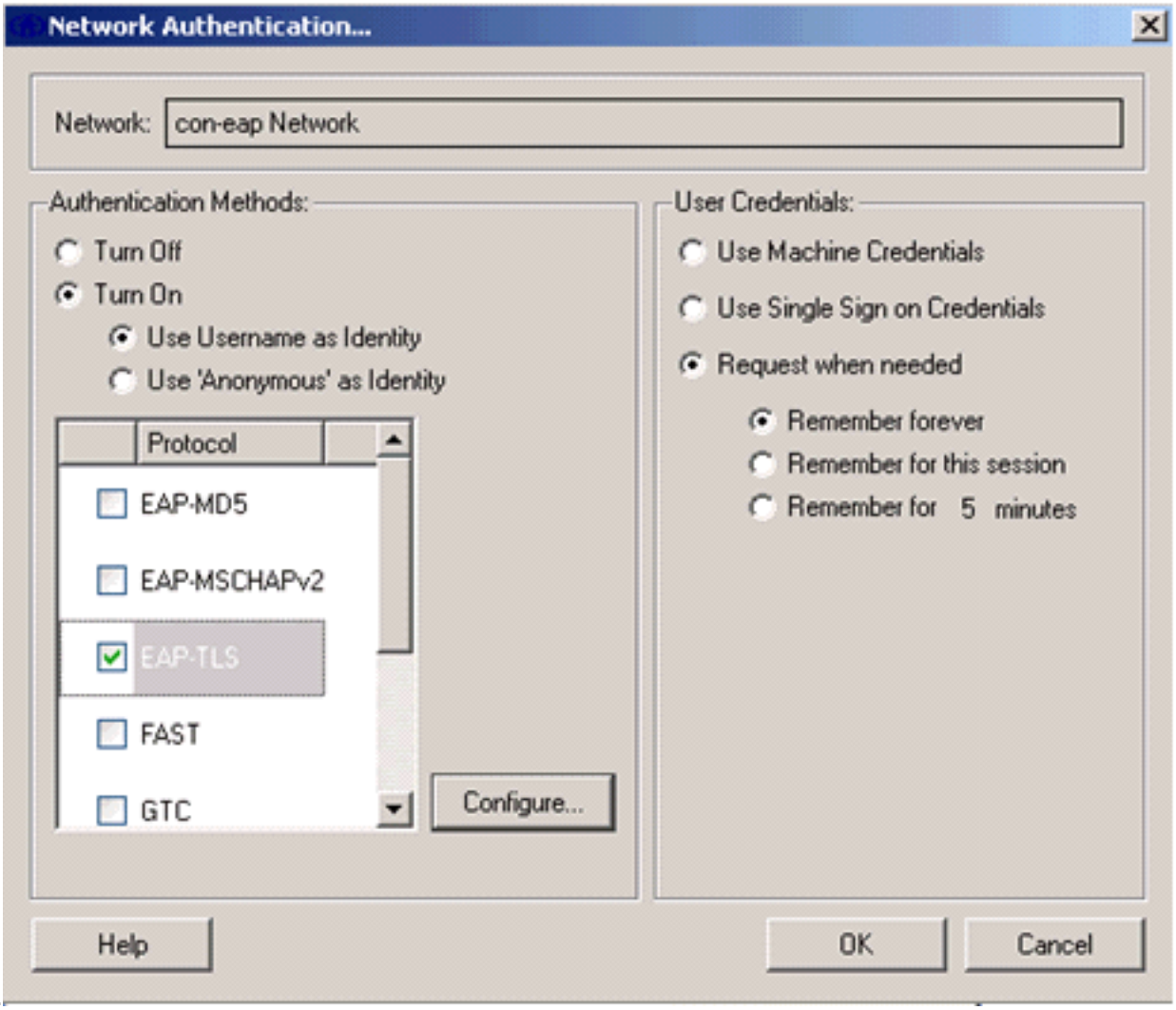
Conclua estes passos:

1. O WLC, à revelia, transmite o SSID, assim que mostra-se na lista das redes da criação de SSID feitos a varredura. A fim criar um perfil da rede, você pode clicar o SSID na lista (empresa) e o clique **cria a rede**.Se o infra-estruturo WLAN é configurado com a transmissão SSID desabilitada, você deve manualmente adicionar o SSID. A fim fazer isto, o clique **adiciona** sob dispositivos de acesso e incorpora manualmente o SSID apropriado (por exemplo, empresa). Configurar o comportamento ativo da ponta de prova para o cliente. Isto é, onde o cliente sonda ativamente para seu SSID configurado. Especifique **ativamente a busca para este dispositivo de acesso** depois que você incorpora o SSID no indicador do dispositivo de acesso adicionar.**Nota:** As configurações de porta não permitem modos de empreendimento (802.1X) se os ajustes da autenticação de EAP não são primeiros configurados para o perfil.
2. O clique **cria a rede** a fim lançar o indicador do perfil da rede, que o permite associar (ou configurado) o SSID escolhido com um mecanismo da autenticação. Atribua um nome

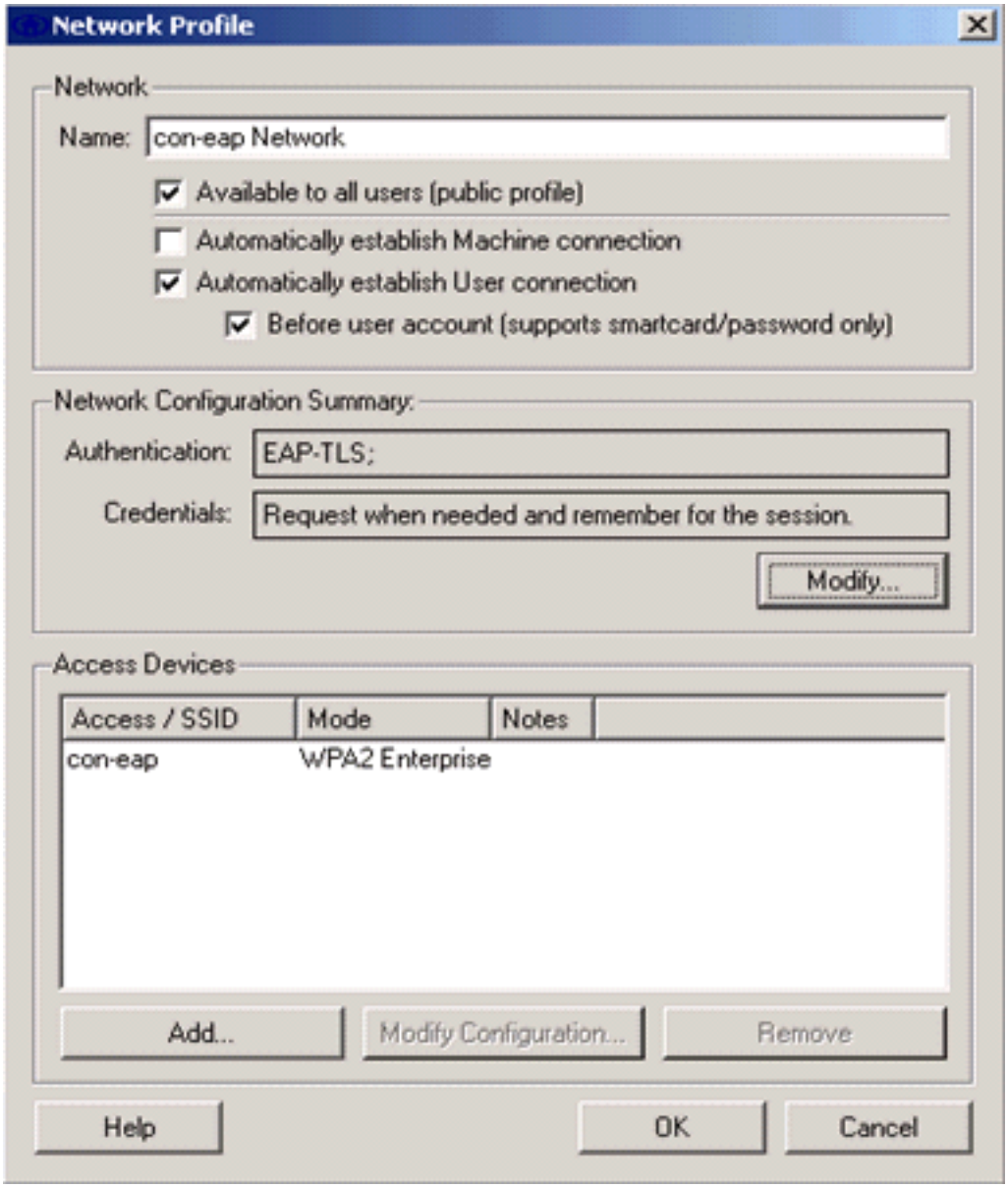
descritivo para o perfil.**Nota:** Os tipos múltiplos da Segurança de WLAN e/ou os SSID podem ser associados sob este perfil da
autenticação.



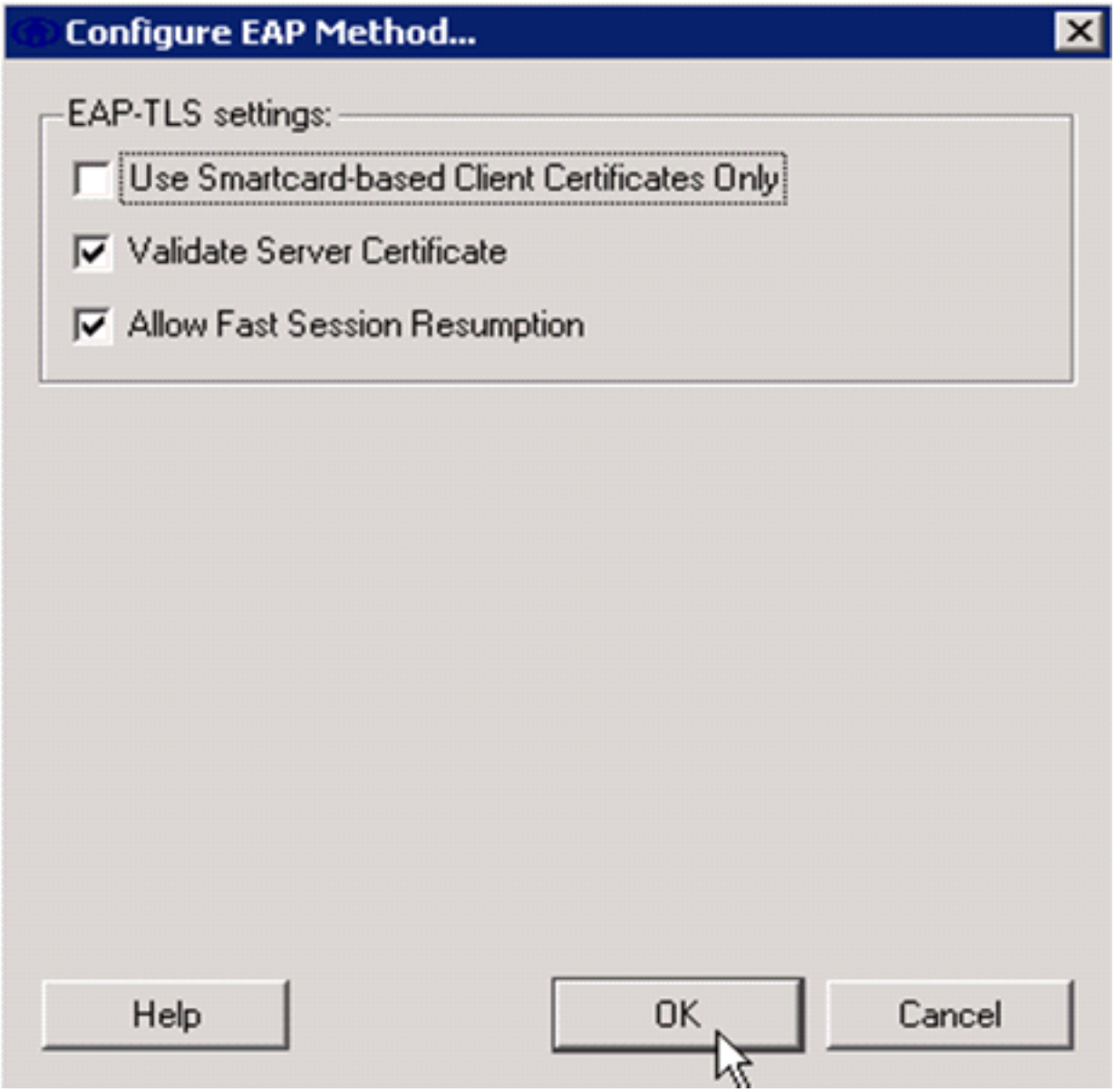
3. Gire sobre a autenticação e verifique o método do EAP-TLS. Clique então **configuram** a fim configurar propriedades do EAP-TLS.
4. Sob o sumário da configuração de rede, o clique **altera** a fim configurar o EAP/ajustes das credenciais.
5. Especifique **gerenciem sobre a autenticação**, escolhem o **EAP-TLS** sob o protocolo, e escolhem o **username** como a identidade.
6. Especifique o **único sinal do uso em credenciais** usar credenciais de logon para a autenticação de rede. O clique **configura** para estabelecer parâmetros do 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

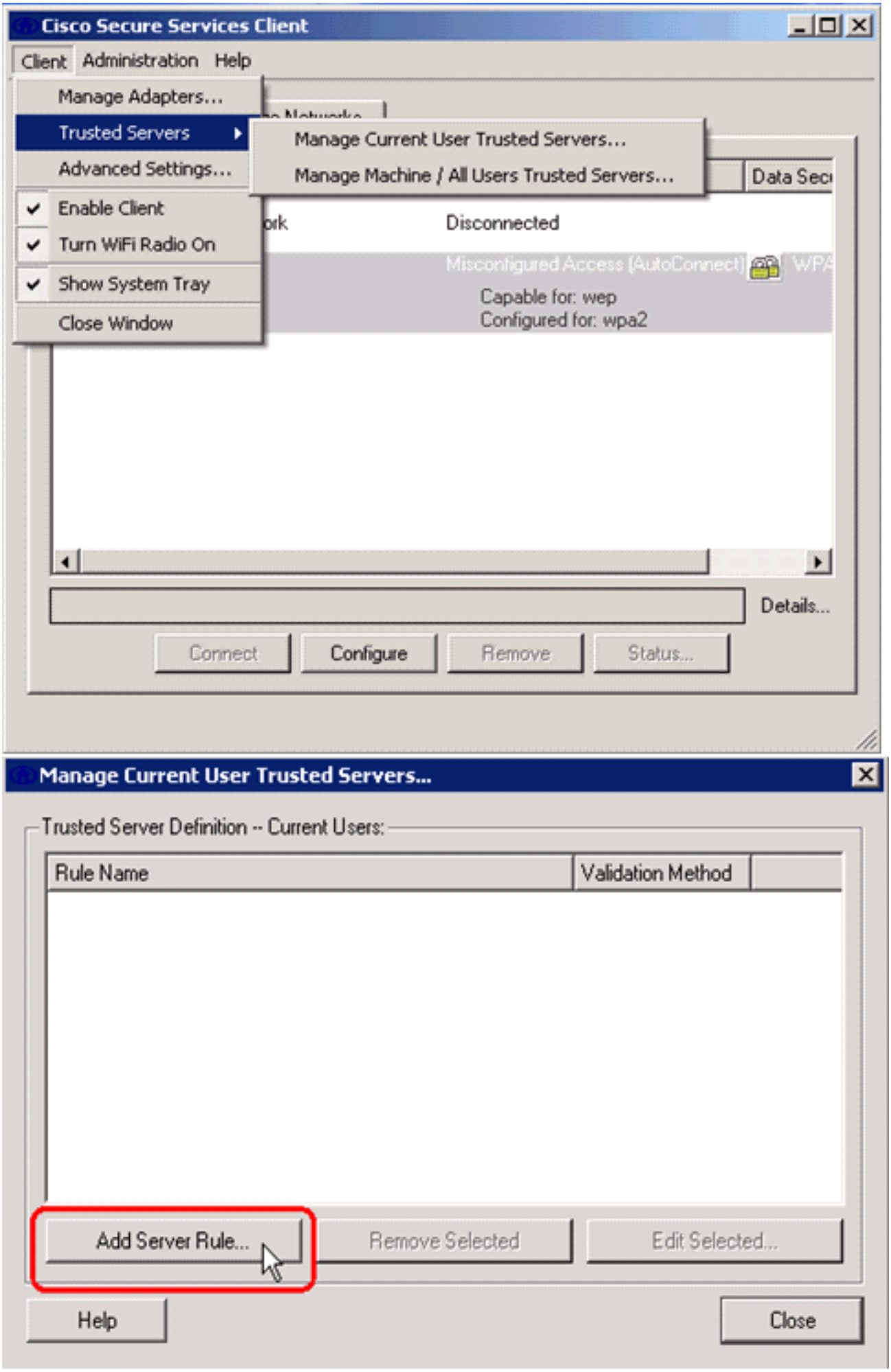
TLS.



7. A fim ter uma configuração que fixada do EAP-TLS você precisa de verificar o certificado de servidor Radius. A fim fazer isto, a verificação **valida o certificado de servidor**.

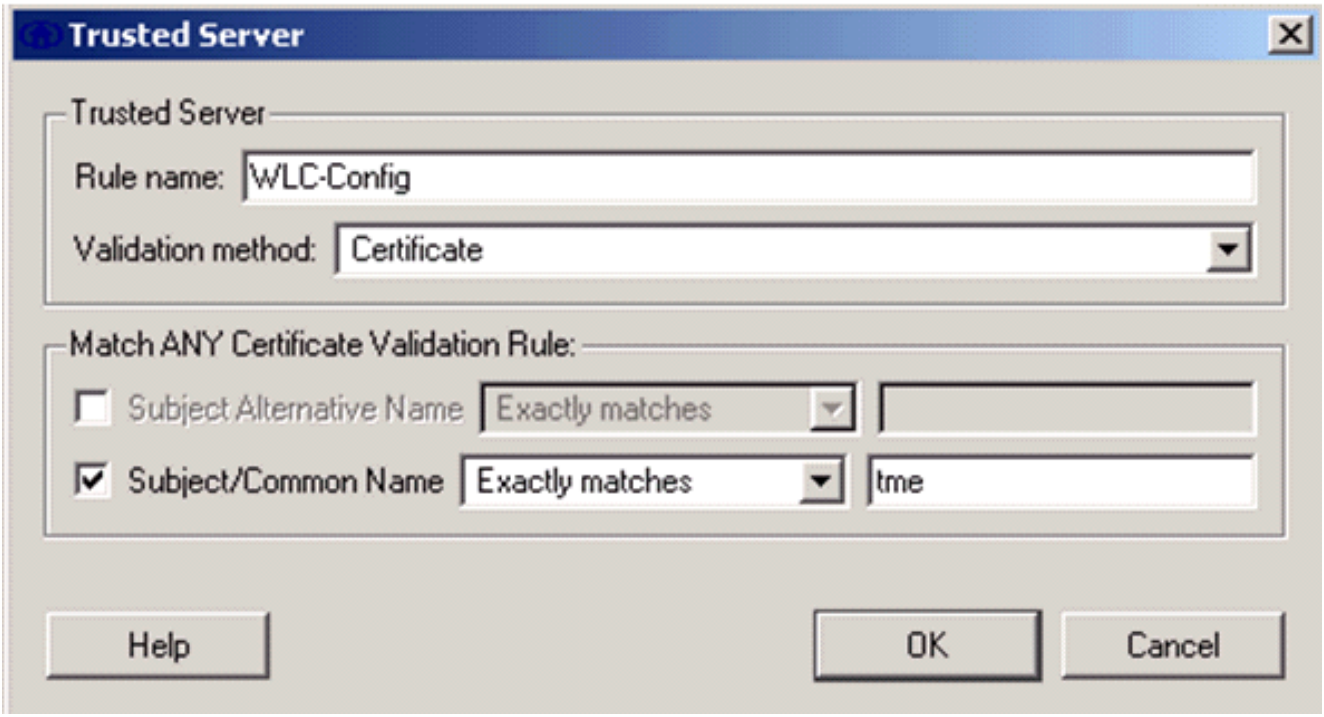


8. A fim validar o certificado de servidor Radius, você precisa de dar a informação do Cisco Secure Services Client a fim aceitar somente o certificado direito. Escolha o **cliente > confiou que os server > controlam usuário atual server confiados**.



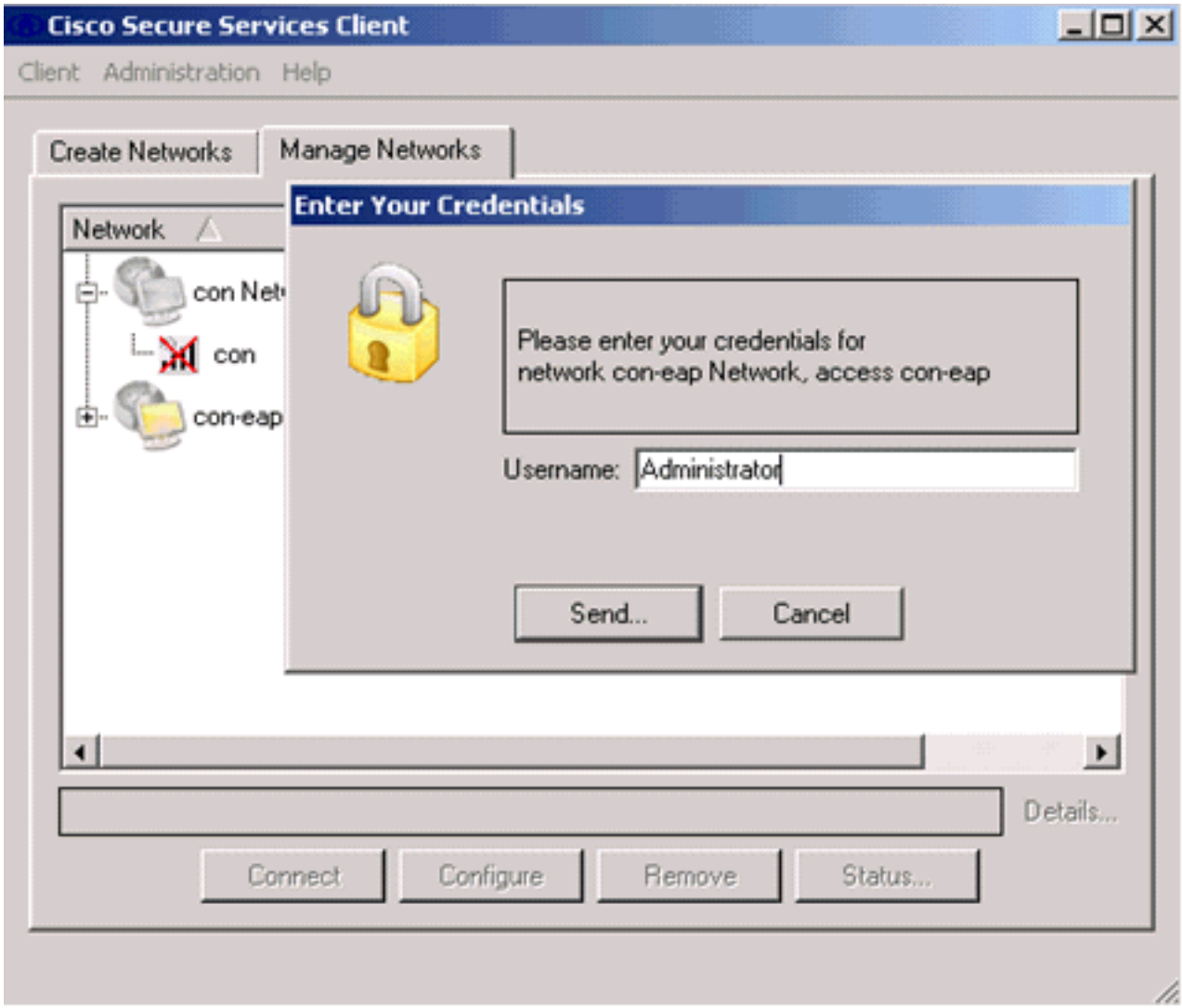
9. Dê um nome para a regra e verifique o nome do certificado de

servidor.



A configuração do EAP-TLS é terminada.

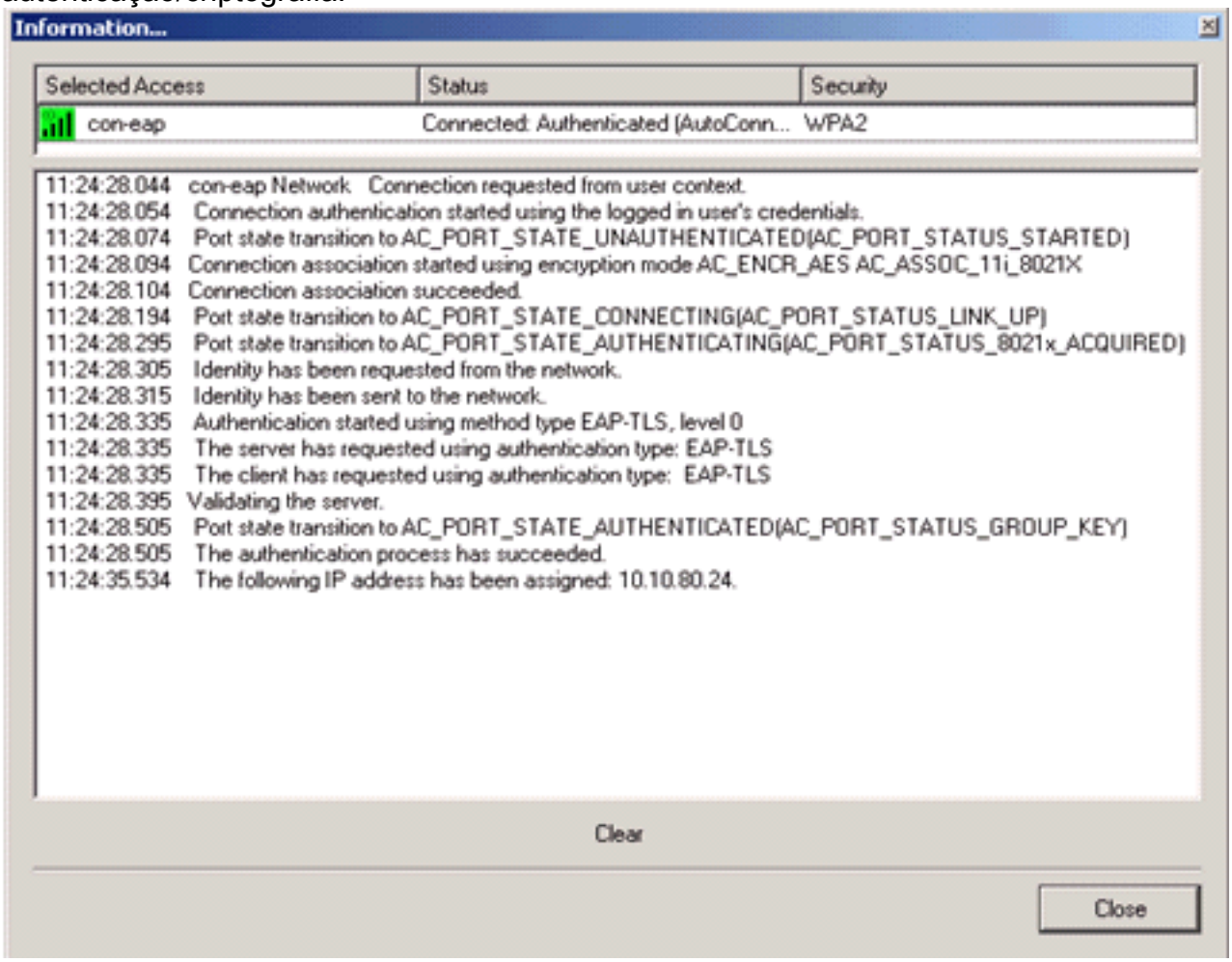
10. Conecte ao perfil da rede Wireless. O Cisco Secure Services Client pede o login de usuário:

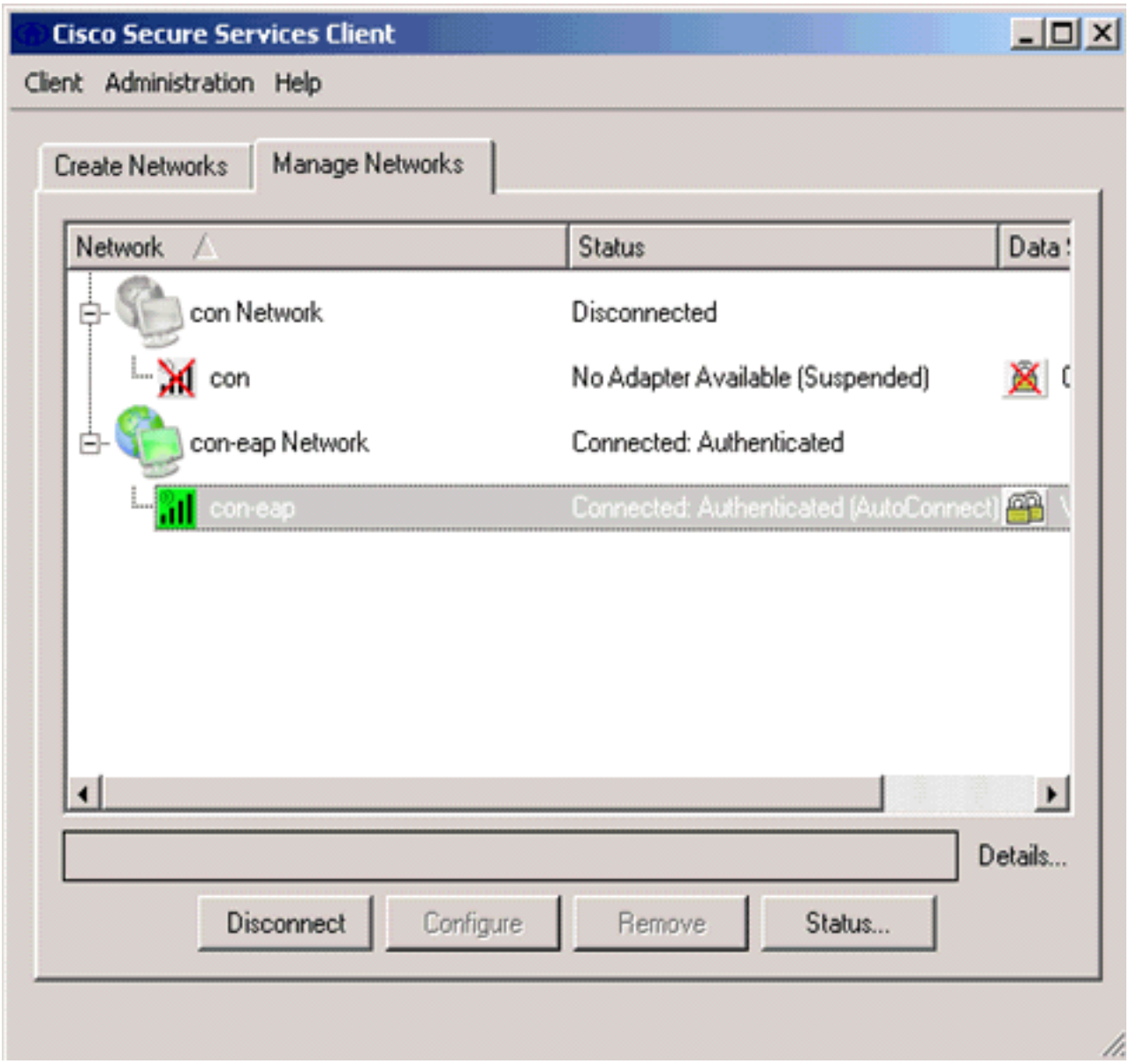


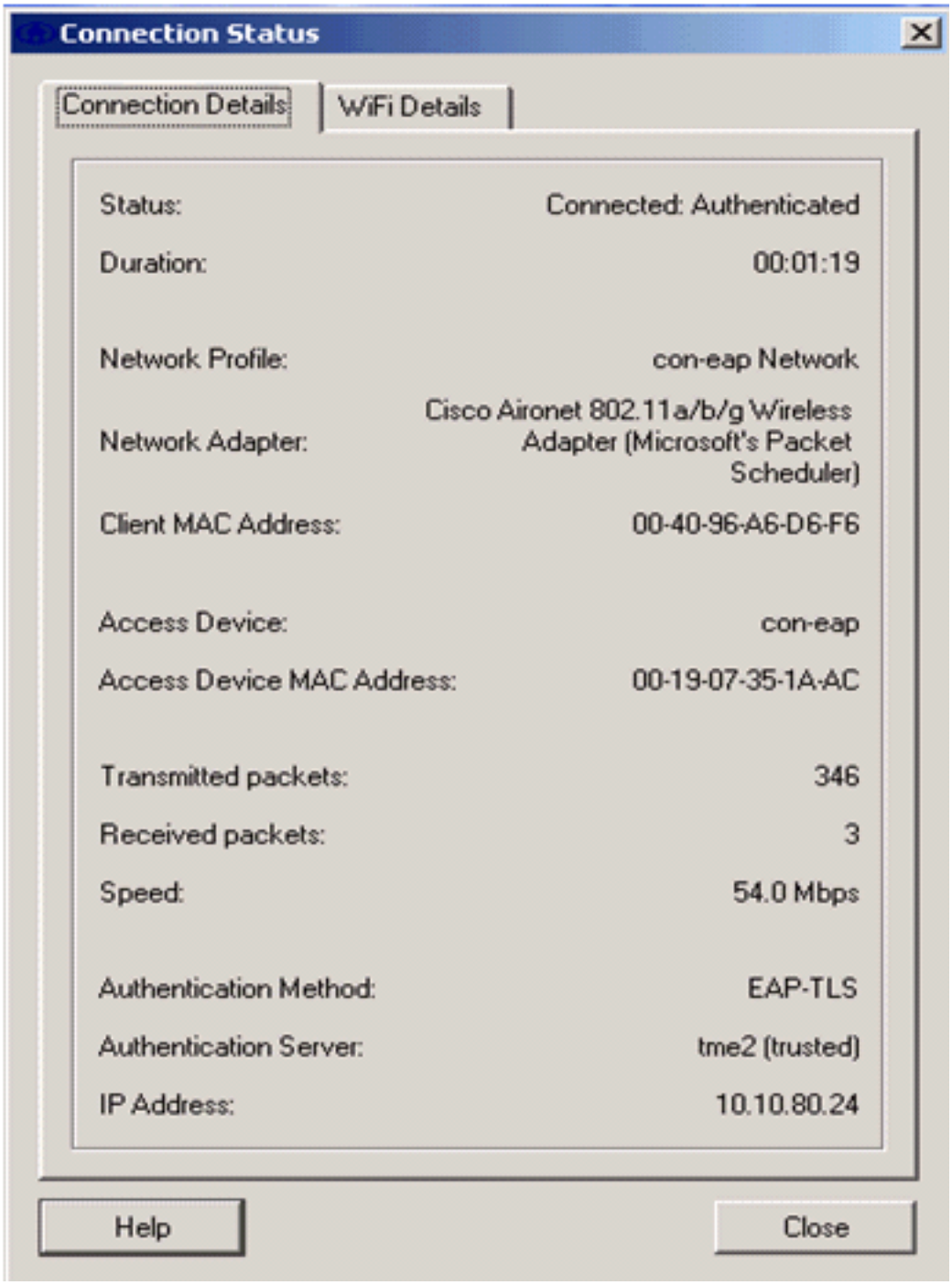
O Cisco Secure Services Client recebe o certificado de servidor e verifica-o (com a regra

configurada e a autoridade de certificação instalada). Pede então o certificado usar-se para o usuário.

11. Depois que o cliente autentica, escolha o **SSID** sob o perfil na aba das redes do controlo e clique o **estado** para perguntar detalhes da conexão.O indicador dos detalhes da conexão fornece a informação no dispositivo do cliente, o status de conexão e as estatísticas, e o método de autenticação. A aba dos detalhes de WiFi fornece detalhes no status de conexão do 802.11, que inclui o RSSI, o canal do 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 (apenas para clientes registrados) (OIT) suporta 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**.

Estes comandos debug podem ser empregados no WLC para monitorar o progresso da troca da autenticação:

- **debugar eventos aaa permitem**
- **debugar o detalhe aaa permitem**
- **debugar eventos do dot1x permitem**

- debugar estados do dot1x permitem
- debugar eventos do eap do local-AUTH aaa permitemOU
- debug aaa all enable

Informações Relacionadas

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