

Autenticação EAP Local no Controller de LAN Wireless com EAP-FAST e Exemplo de Configuração de Servidor LDAP

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Conventions](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Configurar EAP-FAST como método de autenticação EAP local no WLC](#)

[Gerar um certificado de dispositivo para a WLC](#)

[Download do certificado do dispositivo na WLC](#)

[Instalar o certificado raiz de PKI no WLC](#)

[Gerar um certificado de dispositivo para o cliente](#)

[Gerar o Certificado de CA Raiz para o Cliente](#)

[Configurar o EAP local no WLC](#)

[Configurar servidor LDAP](#)

[Criando usuários no controlador de domínio](#)

[Configurar o usuário para acesso ao LDAP](#)

[Usando o LDP para identificar os atributos do usuário](#)

[Configurar cliente sem fio](#)

[Verificar](#)

[Troubleshoot](#)

[Informações Relacionadas](#)

[Introduction](#)

Este documento explica como configurar o EAP (Extensible Authentication Protocol) - Autenticação Flexível via Autenticação EAP Local (FAST - Secure Tunneling) em uma controladora Wireless LAN (WLC). Este documento também explica como configurar o servidor de Lightweight Directory Access Protocol (LDAP) como um banco de dados de backend para EAP Local para retornar as credenciais de usuários e autenticar o usuário.

[Prerequisites](#)

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- Cisco 4400 Series WLC que executa o firmware 4.2
- Pontos de acesso Lightweight (LAP) Cisco Aironet 1232AG Series
- Servidor Microsoft Windows 2003 configurado como controlador de domínio, servidor LDAP e servidor de Autoridade de certificação.
- Adaptador do cliente do Cisco Aironet 802.11 a/b/g que executa o firmware versão 4.2
- Cisco Aironet Desktop Utility (ADU) que executa o firmware versão 4.2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Consulte as [Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.](#)

Informações de Apoio

A autenticação EAP local em controladores de LAN sem fio foi introduzida com a versão 4.1.171.0 do controlador de LAN sem fio.

O EAP local é um método de autenticação que permite que usuários e clientes sem fio sejam autenticados localmente no controlador. Ele foi projetado para uso em escritórios remotos que desejam manter a conectividade com clientes sem fio quando o sistema de 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, eliminando 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 para autenticar usuários. O EAP local oferece suporte à autenticação LEAP, EAP-FAST, EAP-TLS, P EAPv0/MSCHAPv2 e PEAPv1/GTC entre a controladora e os clientes sem fio.

O EAP local pode usar um servidor LDAP como seu banco de dados de back-end para recuperar credenciais do usuário.

Um banco de dados back-end LDAP permite que o controlador solicite as credenciais (nome de usuário e senha) de um usuário específico a um servidor LDAP. Essas credenciais são, então, usadas para autenticar o usuário.

O banco de dados back-end LDAP oferece suporte aos seguintes métodos EAP locais:

- EAP-FAST/GTC
- EAP-TLS

- PEAPv1/GTC

LEAP, EAP-FAST/MSCHAPv2 e PEAPv0/MSCHAPv2 também são suportados, **mas somente se o servidor LDAP estiver configurado para retornar uma senha de texto não criptografado**. Por exemplo, o Microsoft Active Directory não tem suporte porque não retorna uma senha de texto não criptografado. Se o servidor LDAP não puder ser configurado para retornar uma senha de texto não criptografado, LEAP, EAP-FAST/MSCHAPv2 e PEAPv0/MSCHAPv2 não serão suportados.

Observação: se algum servidor RADIUS estiver configurado no controlador, o controlador tentará autenticar os clientes sem fio usando primeiro os servidores RADIUS. Tentativa de EAP local somente se nenhum servidor RADIUS for encontrado, seja porque os servidores RADIUS atingiram o tempo limite ou porque nenhum servidor RADIUS foi configurado. Se quatro servidores RADIUS forem configurados, a controladora tentará autenticar o cliente com o primeiro servidor RADIUS, depois o segundo servidor RADIUS e, em seguida, EAP local. Se o cliente tentar reautenticar manualmente, a controladora tentará o terceiro servidor RADIUS, depois o quarto servidor RADIUS e, em seguida, o EAP local.

Este exemplo usa EAP-FAST como o método Local EAP no WLC, que por sua vez é configurado para consultar o banco de dados back-end LDAP para as credenciais do usuário de um cliente sem fio.

Configurar

Este documento usa EAP-FAST com certificados no lado do cliente e no lado do servidor. Para isso, a instalação usa o servidor **Microsoft Certificate Authority (CA)** para gerar os certificados de cliente e servidor.

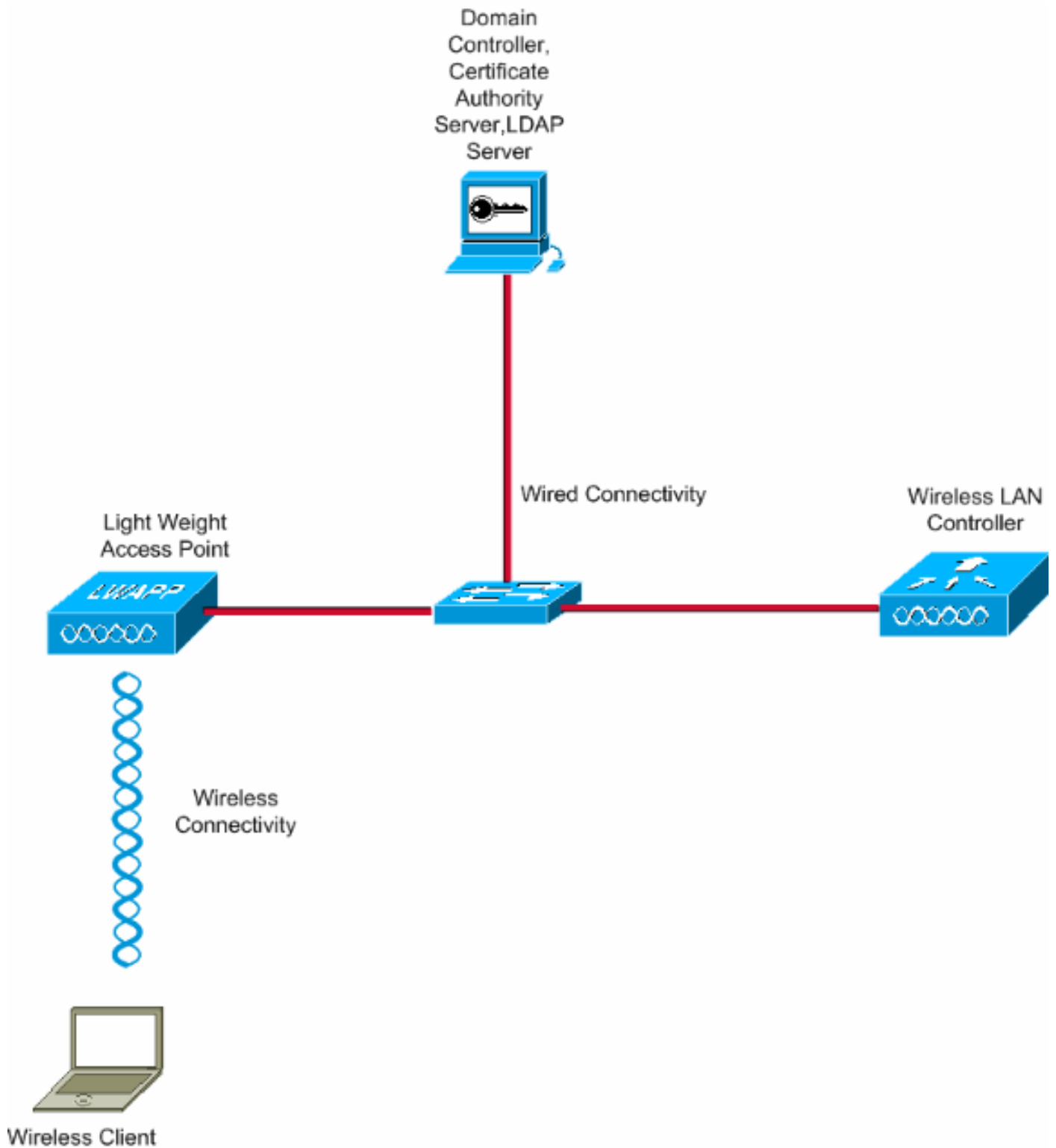
As credenciais do usuário são armazenadas no servidor LDAP de modo que, na validação de certificado bem-sucedida, o controlador consulte o servidor LDAP para recuperar as credenciais do usuário e autentique o cliente sem fio.

Este documento pressupõe que estas configurações já estão em vigor:

- Um LAP é registrado na WLC. Consulte [Registro de AP Lightweight \(LAP\) em uma controladora Wireless LAN \(WLC\)](#) para obter mais informações sobre o processo de registro.
- Um servidor DHCP é configurado para atribuir um endereço IP aos clientes sem fio.
- O servidor Microsoft Windows 2003 está configurado como controlador de domínio e como servidor de autoridade de certificação. Este exemplo usa **wireless.com** como o domínio. Consulte [Configuração do Windows 2003 como um Controlador de Domínio](#) para obter mais informações sobre como configurar um servidor Windows 2003 como um controlador de domínio. Consulte [Instalação e Configuração do Microsoft Windows 2003 Server como um Servidor de Autoridade de Certificação \(CA\)](#) para configurar o servidor Windows 2003 como servidor de Autoridade de Certificação Corporativa.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Configurações

Conclua estas etapas para implementar esta configuração:

- [Configurar EAP-FAST como método de autenticação EAP local no WLC](#)
- [Configurar servidor LDAP](#)
- [Configurar cliente sem fio](#)

Configurar EAP-FAST como método de autenticação EAP local no WLC

Como mencionado anteriormente, este documento usa EAP-FAST com certificados no lado do cliente e do servidor como o método de autenticação EAP local. A primeira etapa é baixar e instalar os seguintes certificados no servidor (WLC, neste caso) e no cliente.

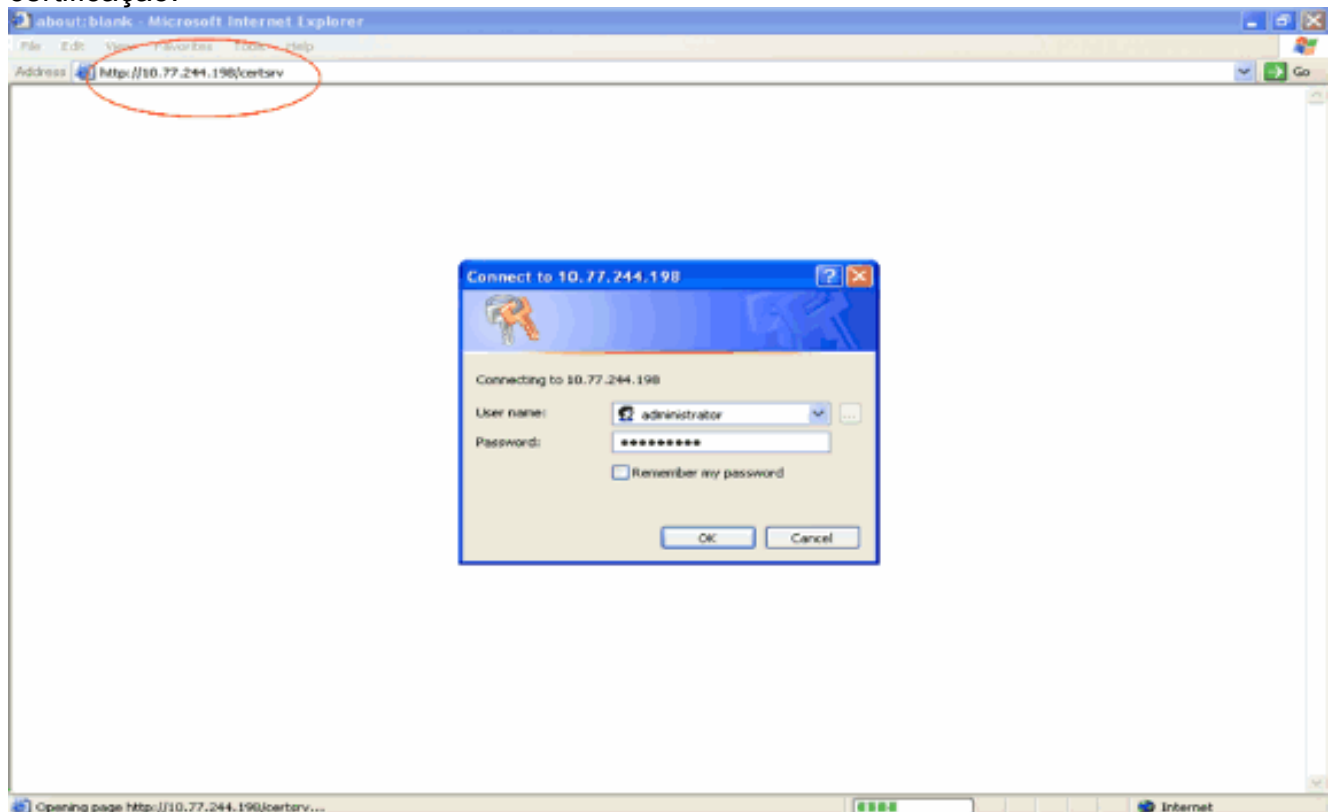
A WLC e o cliente precisam desses certificados para serem baixados do servidor de CA:

- Certificado do dispositivo (um para a WLC e outro para o cliente)
- Certificado raiz da Public Key Infrastructure (PKI) para a WLC e certificado CA para o cliente

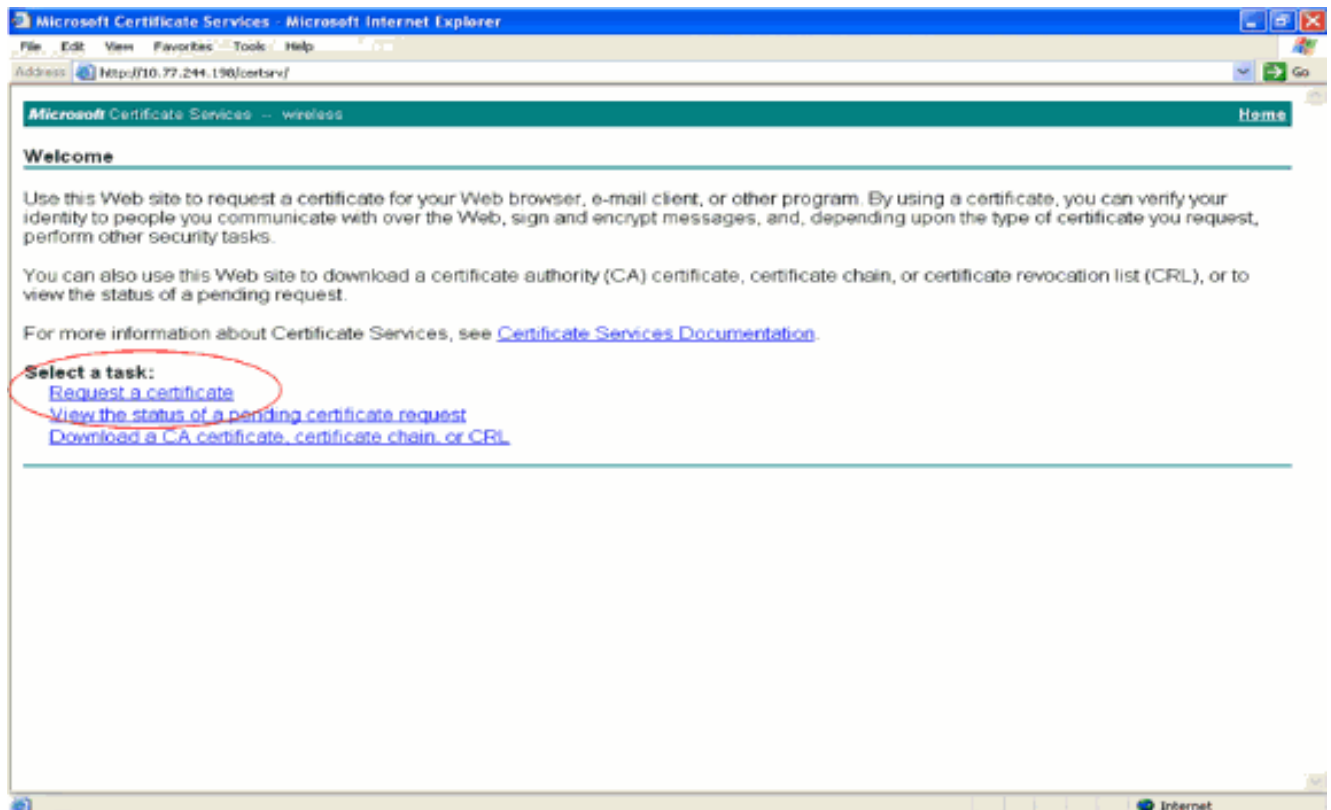
Gerar um certificado de dispositivo para a WLC

Execute estas etapas para gerar um certificado de dispositivo para o WLC do servidor CA. Este certificado de dispositivo é usado pela WLC para autenticar o cliente.

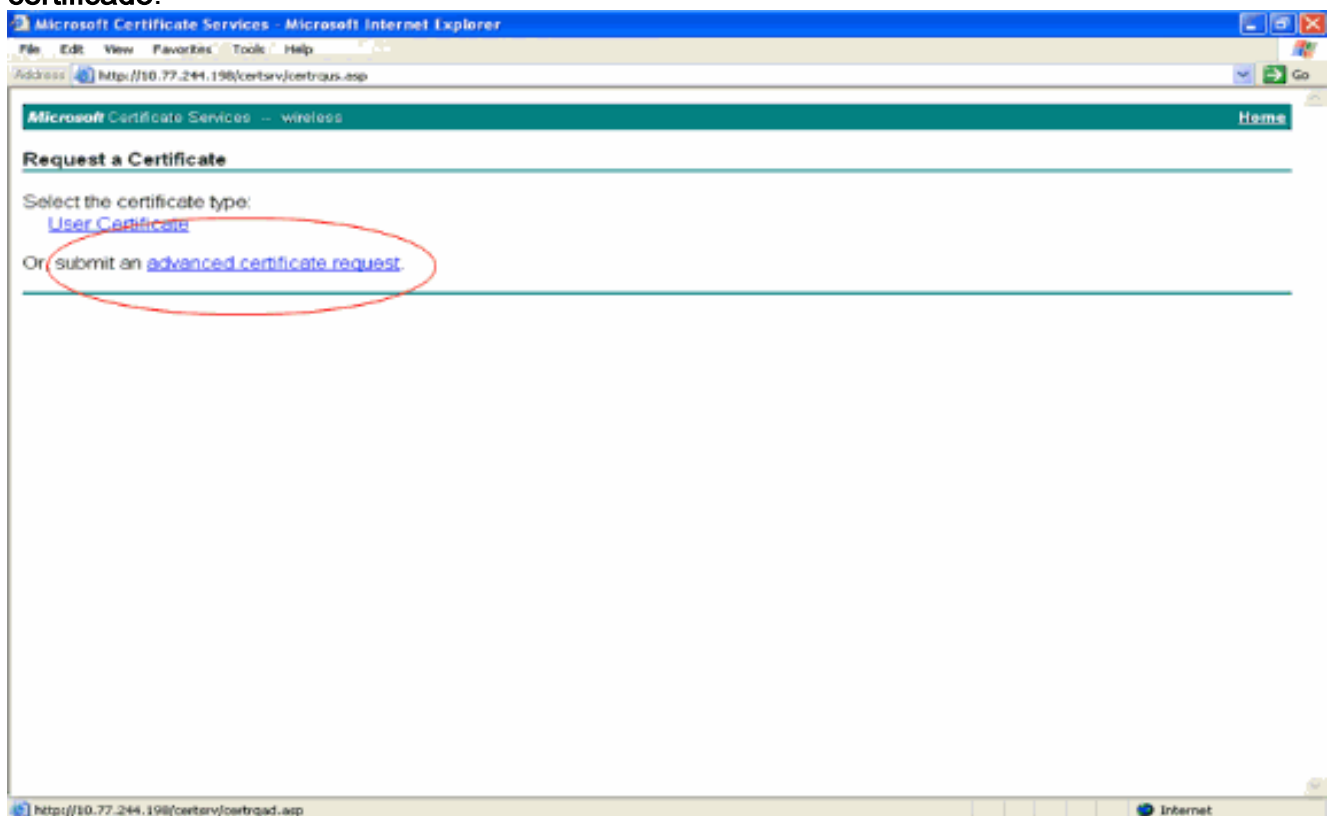
1. Acesse <http://<endereço IP do servidor de CA>/certsrv> no PC que tem uma conexão de rede com o servidor de CA. Faça login como administrador do servidor de autoridade de certificação.



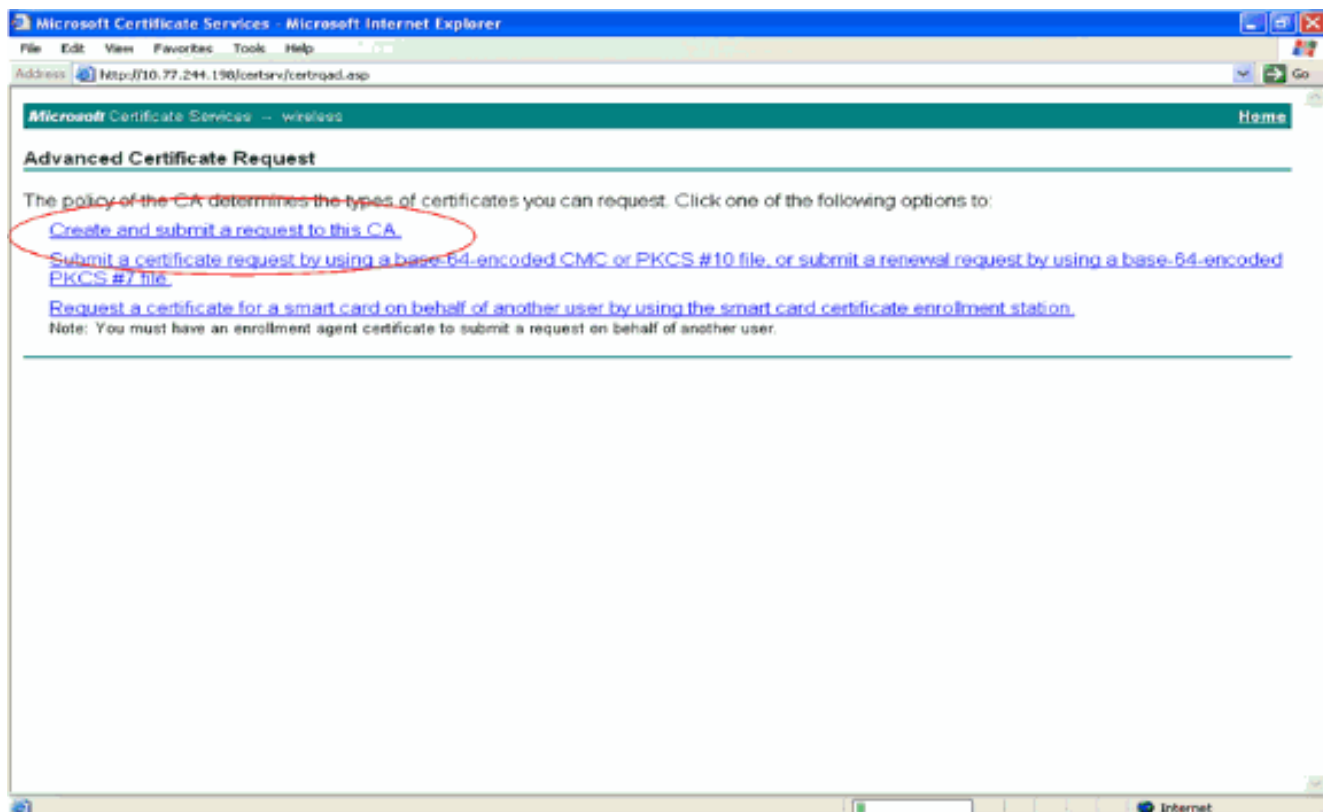
2. Selecione **Request a certificate**.



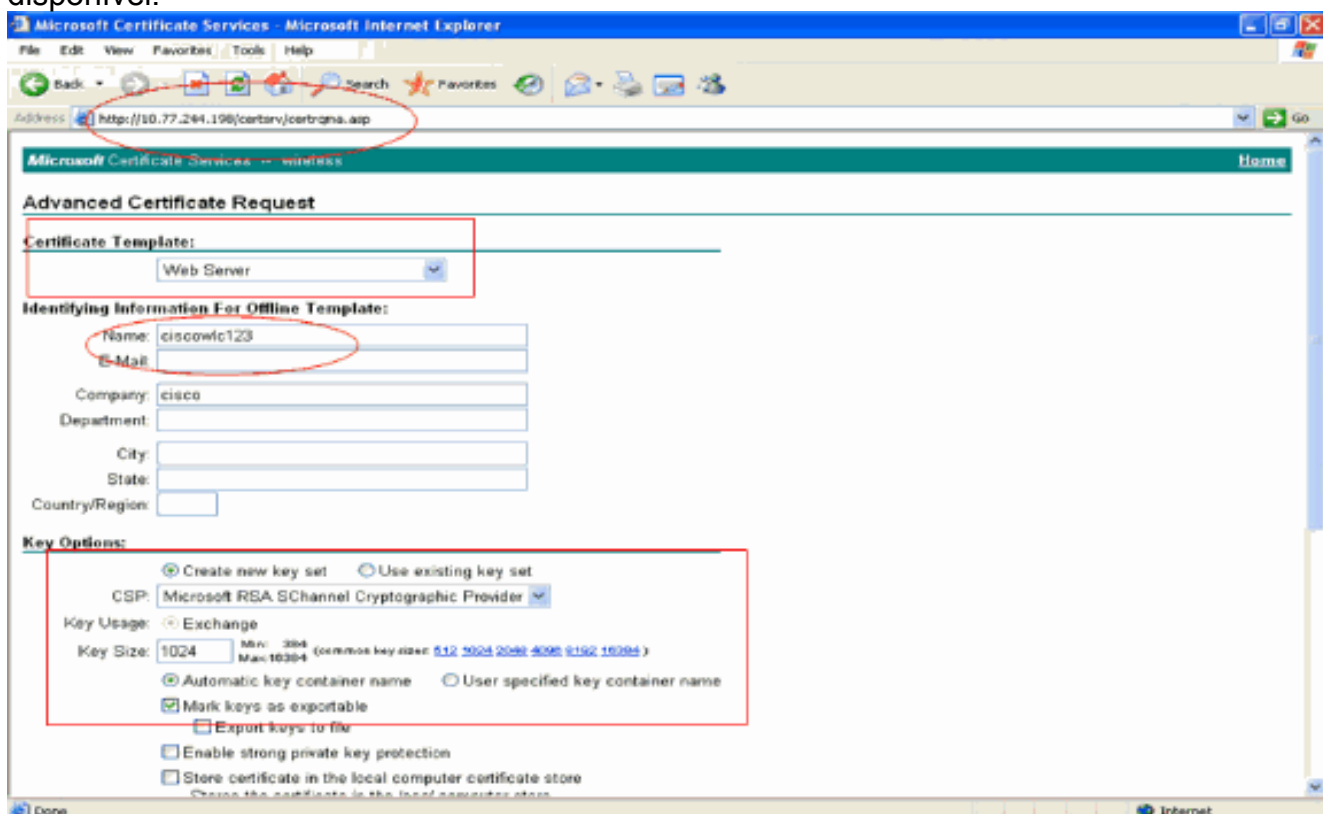
3. Na página Solicitar um certificado, clique em **solicitação avançada de certificado**.



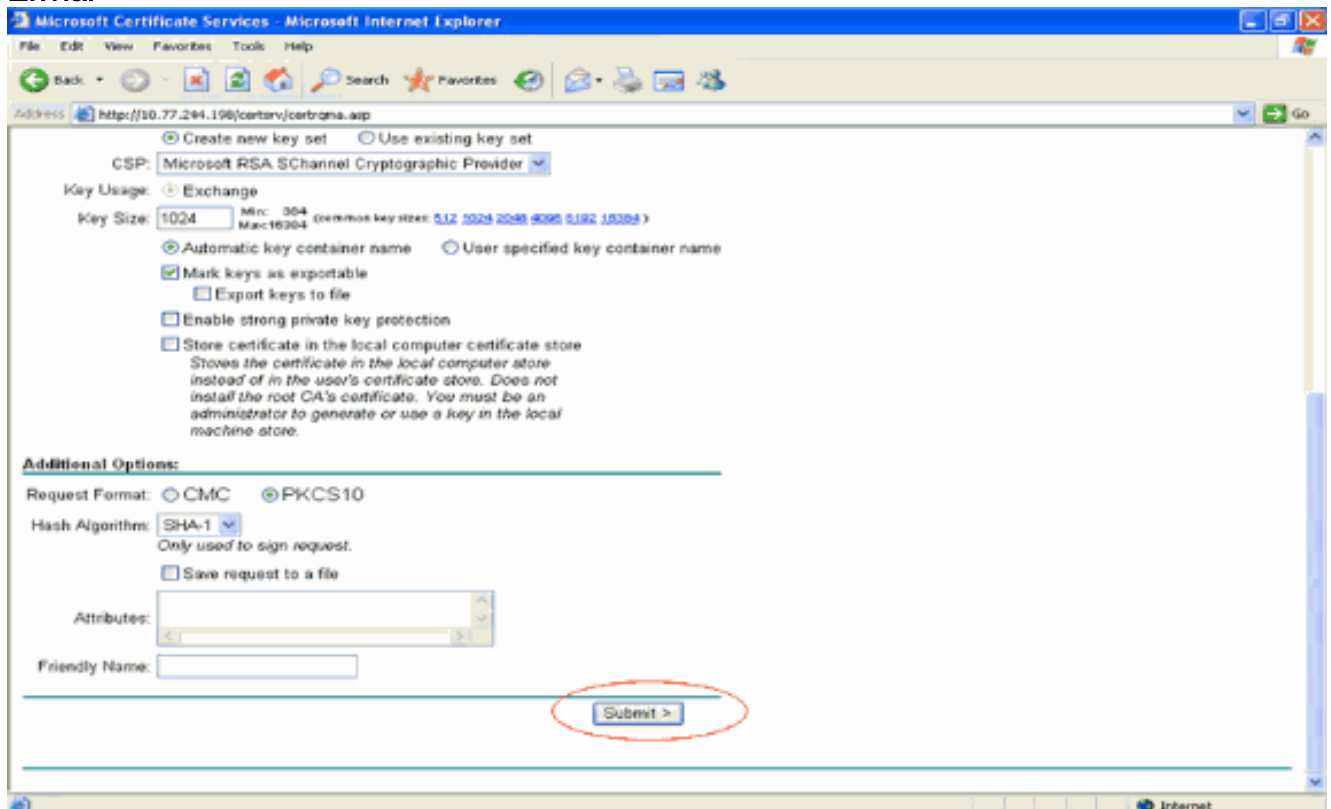
4. Na página Solicitação avançada de certificado, clique em **Criar e enviar uma solicitação a esta CA**. Isso o levará para o formulário de solicitação de certificado Avançado.



5. No formulário de solicitação de certificado avançado, escolha **Servidor Web** como o Modelo de certificado. Em seguida, especifique um nome para este certificado de dispositivo. Este exemplo usa o nome do certificado como ciscowlc123. Preencha as outras informações de identificação de acordo com sua exigência.
6. Na seção **Key Options**, selecione a opção **Mark Keys as Exportable**. Às vezes, essa opção específica ficará esmaecida e não poderá ser ativada ou desativada se você escolher um modelo de servidor Web. Nesses casos, clique em **Voltar** no menu do navegador para voltar uma página e voltar novamente a essa página. Desta vez, a opção Mark Keys as Exportable (Marcar chaves como exportáveis) deve estar disponível.



7. Configure todos os outros campos necessários e clique em **Enviar**.



The screenshot shows the Microsoft Certificate Services web interface in Microsoft Internet Explorer. The address bar displays `http://10.77.244.198/certsrv/certbma.asp`. The page contains several configuration sections:

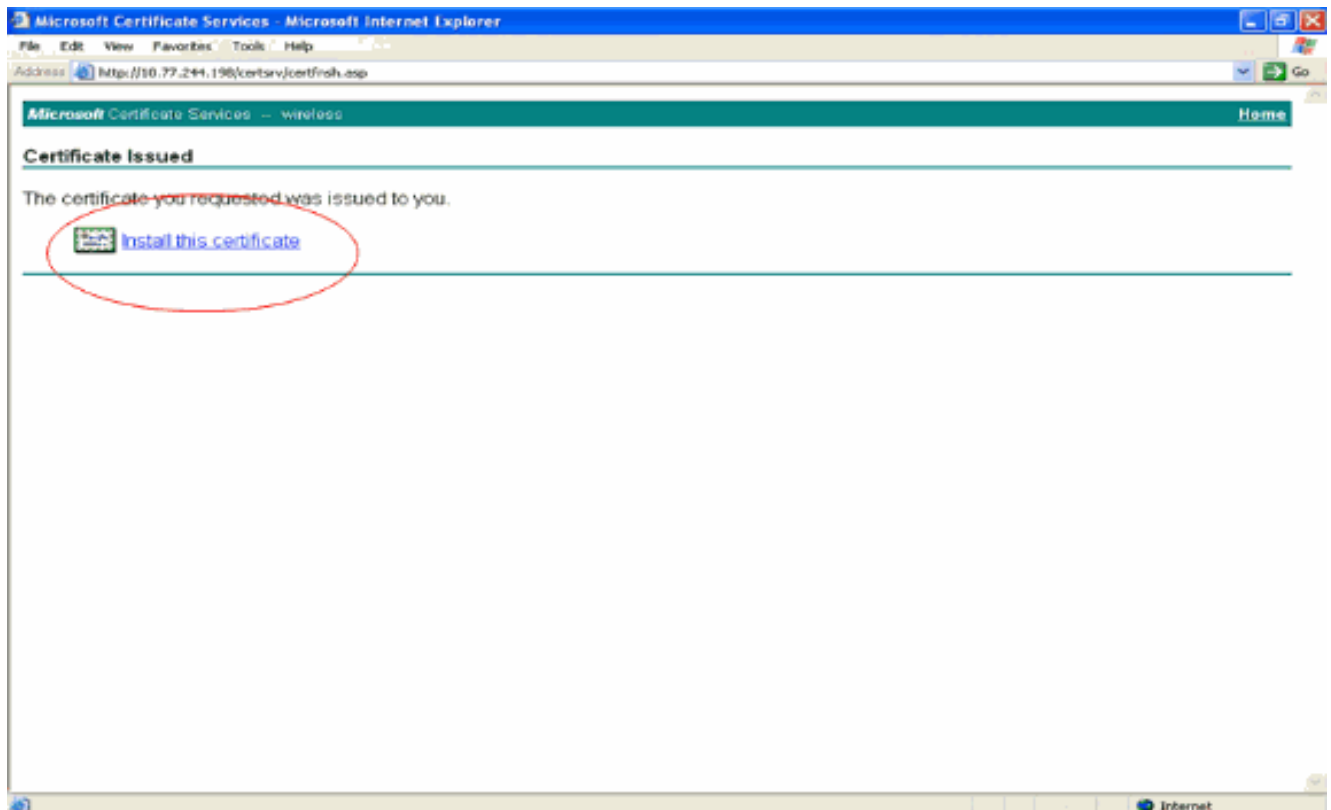
- Key Set Configuration:**
 - Radio buttons for "Create new key set" (selected) and "Use existing key set".
 - CSP: Microsoft RSA SChannel Cryptographic Provider
 - Key Usage: Exchange
 - Key Size: 1024 (with subtext: Min: 384, Max: 1024, common key sizes: 512, 1024, 2048, 4096, 5192, 10368)
 - Radio buttons for "Automatic key container name" (selected) and "User specified key container name".
 - Checked checkbox: "Mark keys as exportable".
 - Unchecked checkbox: "Export keys to file".
 - Unchecked checkbox: "Enable strong private key protection".
 - Unchecked checkbox: "Store certificate in the local computer certificate store".
 - Text below the last checkbox: "Stores the certificate in the local computer store instead of in the user's certificate store. Does not install the root CA's certificate. You must be an administrator to generate or use a key in the local machine store."
- Additional Options:**
 - Request Format: Radio buttons for "CMC" and "PKCS10" (selected).
 - Hash Algorithm: SHA-1 (dropdown menu).
 - Text below: "Only used to sign request."
 - Unchecked checkbox: "Save request to a file".
 - Attributes: A text input field with a dropdown arrow.
 - Friendly Name: A text input field.

The "Submit >" button at the bottom right is circled in red.

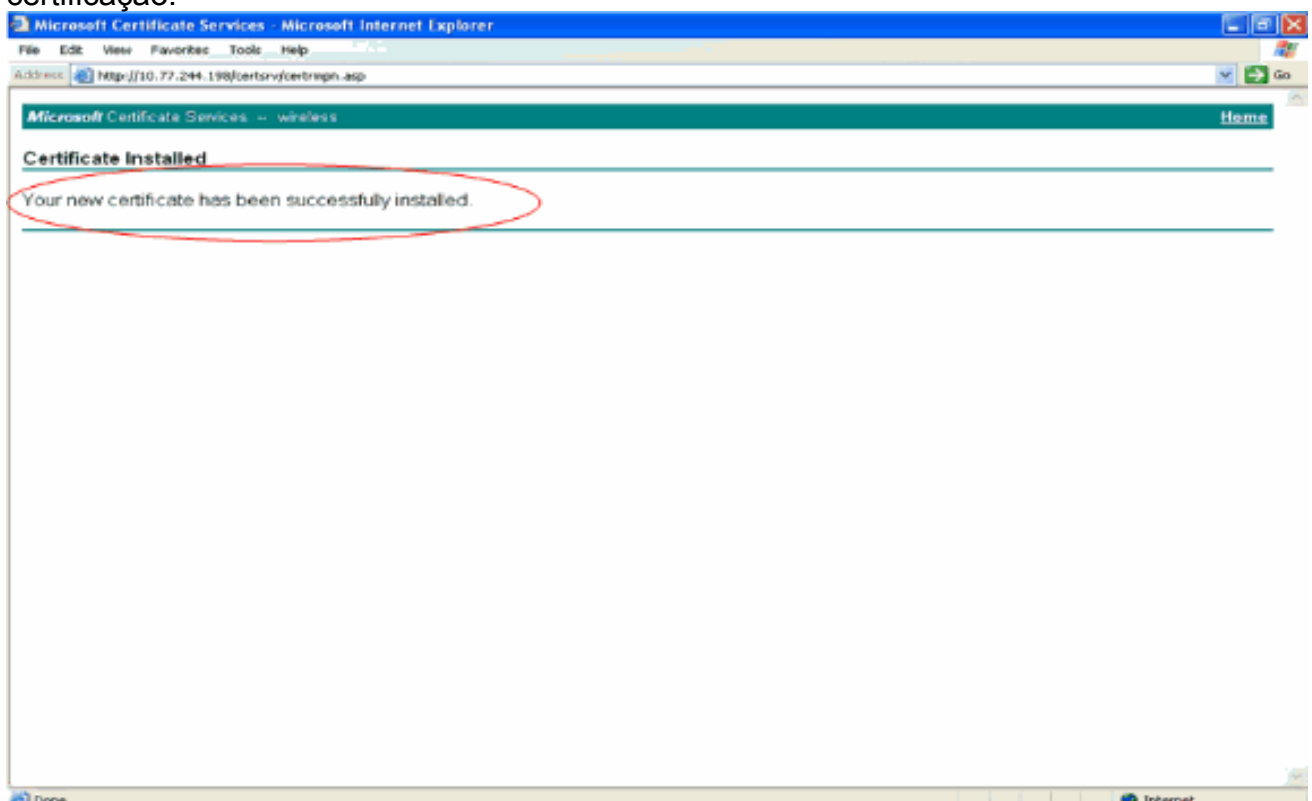
8. Clique em **Yes** na próxima janela para permitir o processo de solicitação de certificado.



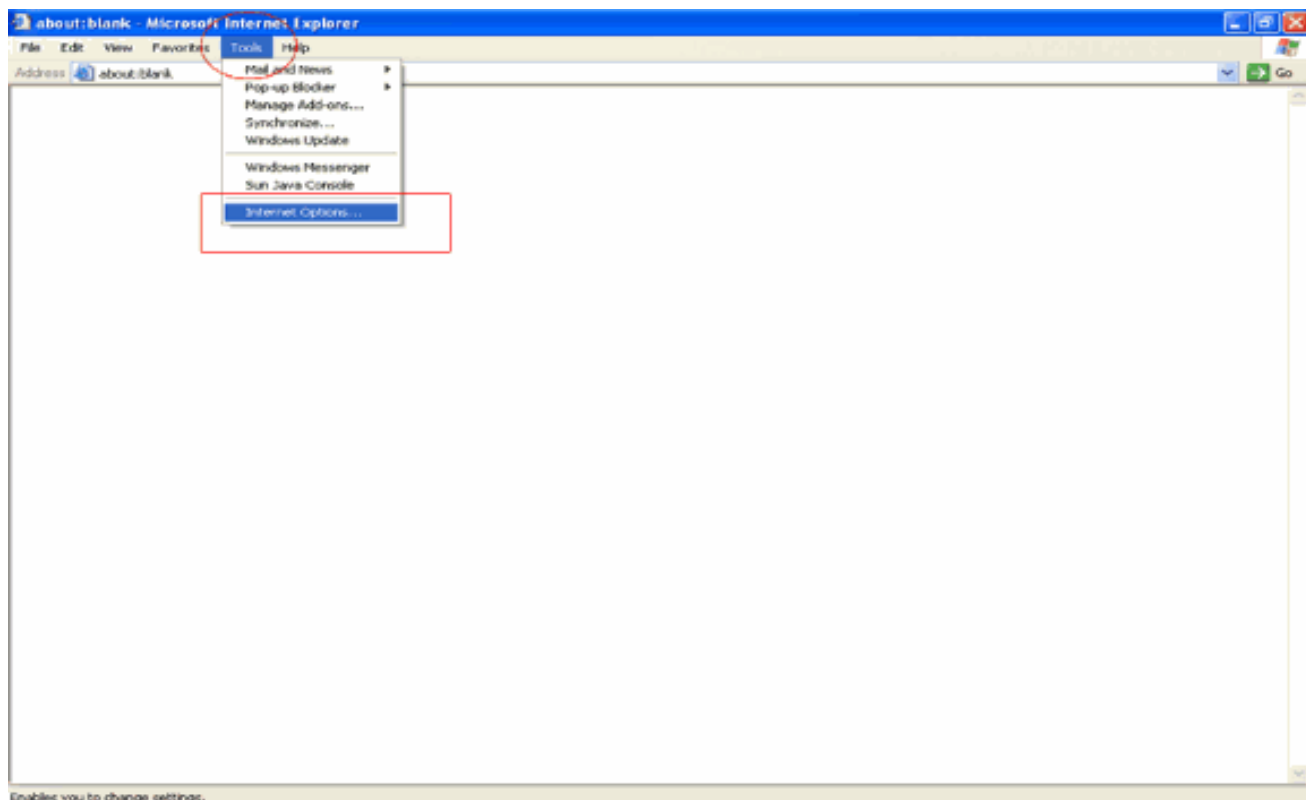
9. A janela Certificado Emitido é exibida, indicando um processo de solicitação de certificado bem-sucedido. A próxima etapa é instalar o certificado emitido no repositório de certificados deste computador. Clique em Instalar este certificado.



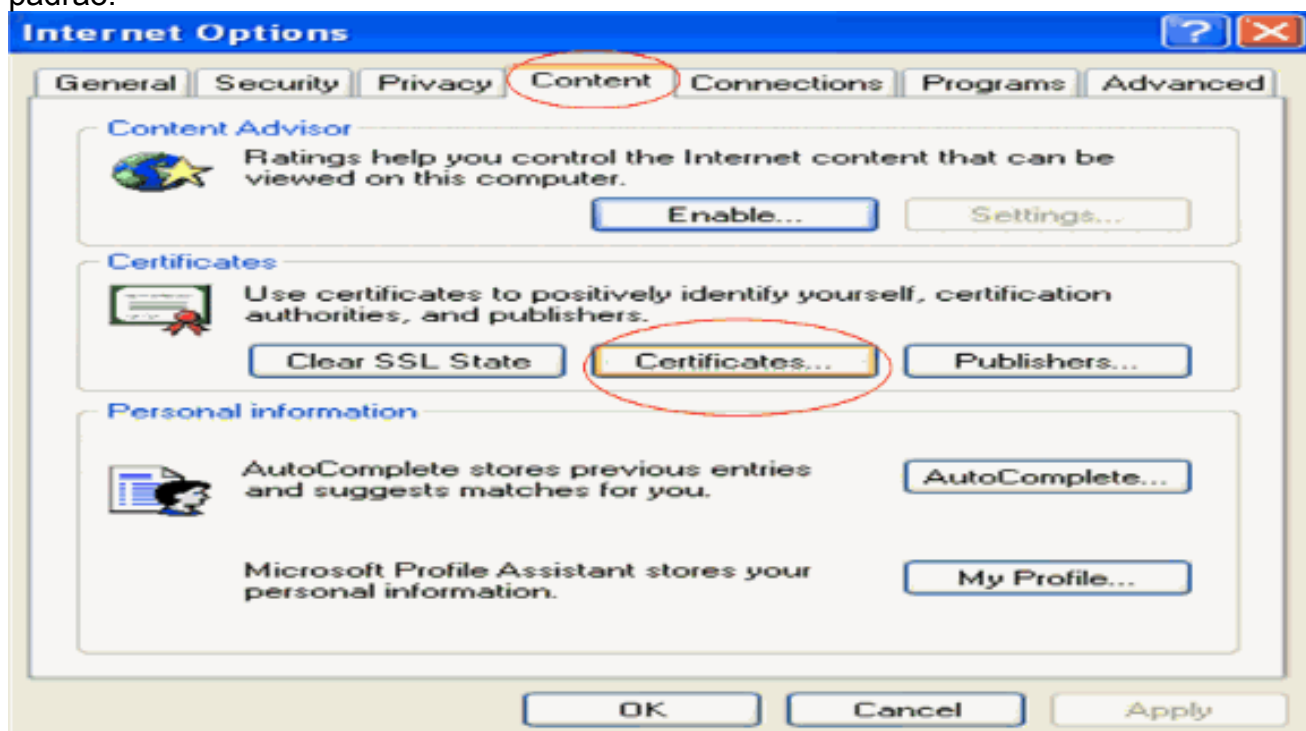
10. O novo certificado é instalado com êxito no computador de onde a solicitação é gerada para o servidor de autoridade de certificação.



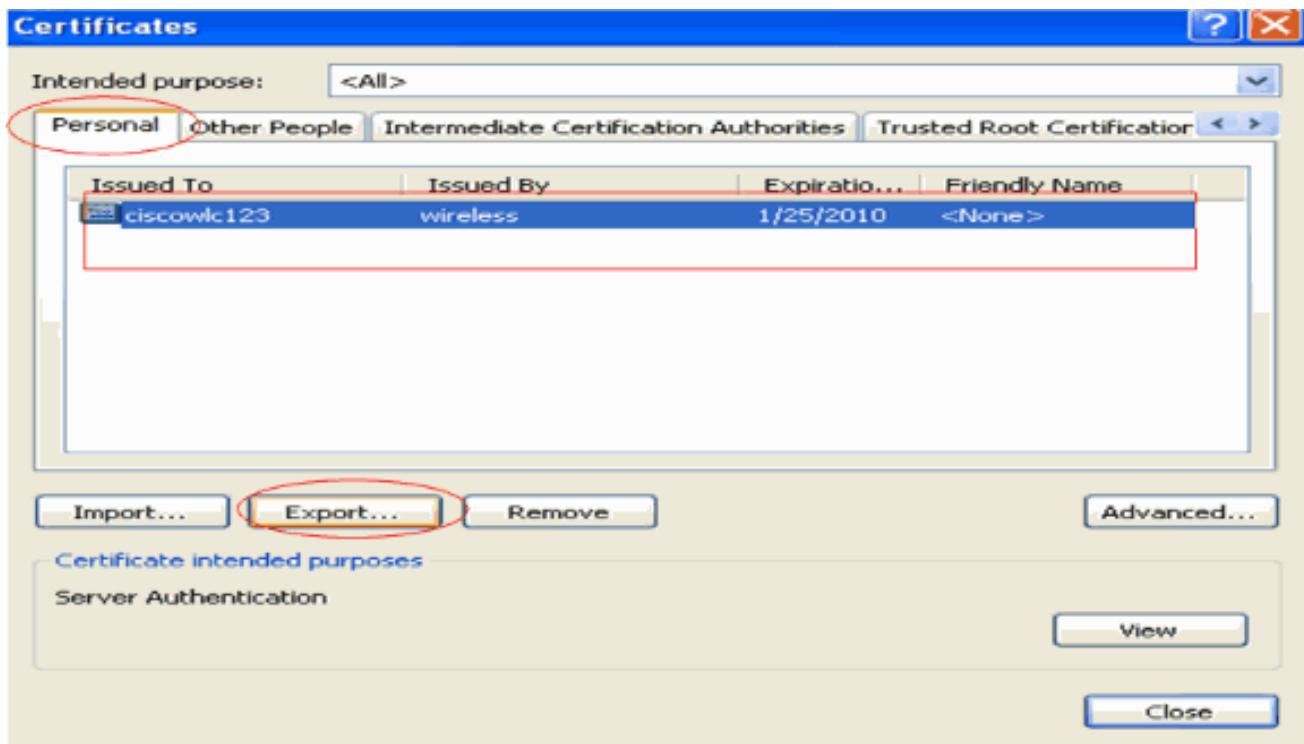
11. A próxima etapa é exportar esse certificado do armazenamento de certificados para o disco rígido como um arquivo. Este arquivo de certificado será usado posteriormente para baixar o certificado para a WLC. Para exportar o certificado do armazenamento de certificados, abra o navegador Internet Explorer e clique em **Ferramentas > Opções da Internet**.



12. Clique em **Content > Certificates** para ir para o armazenamento de certificados onde os certificados são instalados por padrão.



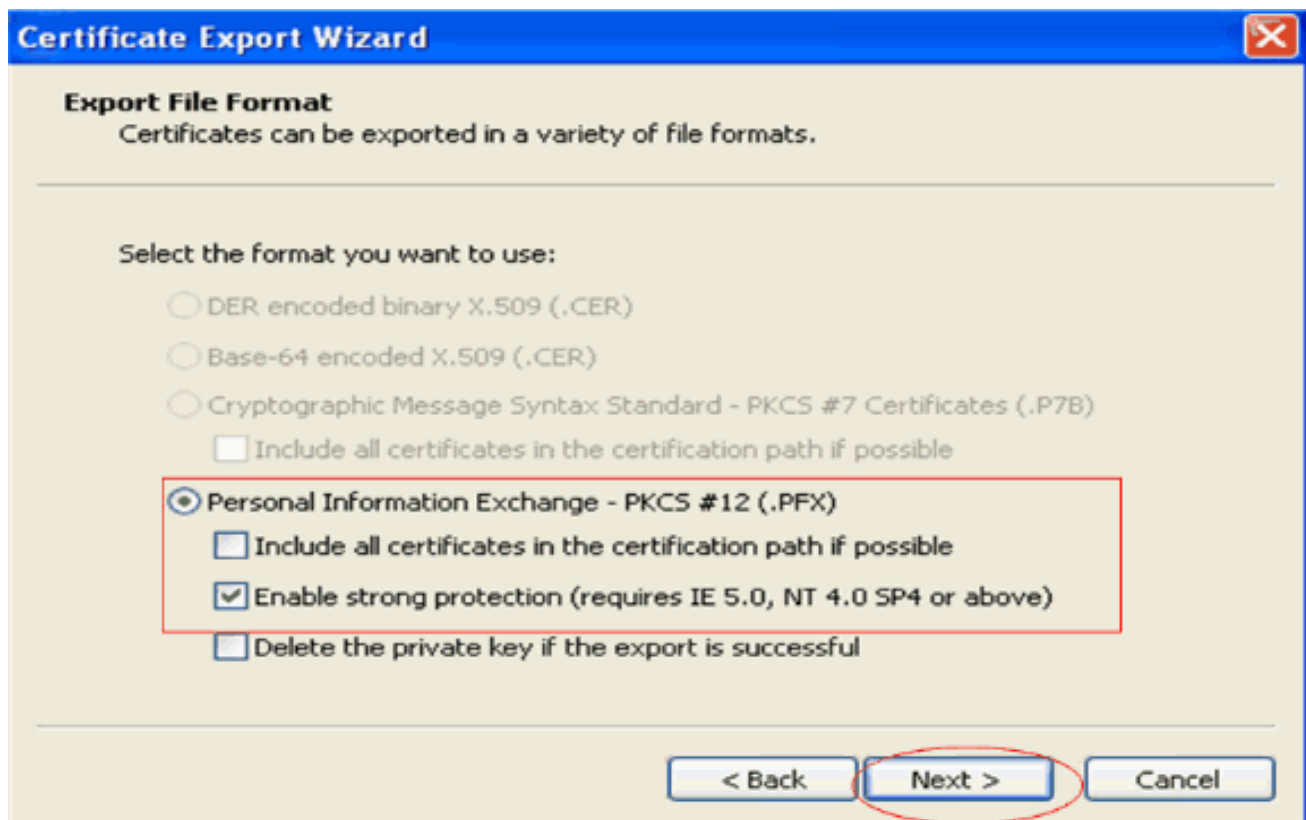
13. Os certificados do dispositivo são geralmente instalados na lista de certificados **Personal**. Aqui, você deve ver o certificado recém-instalado. Selecione o certificado e clique em **Exportar**.



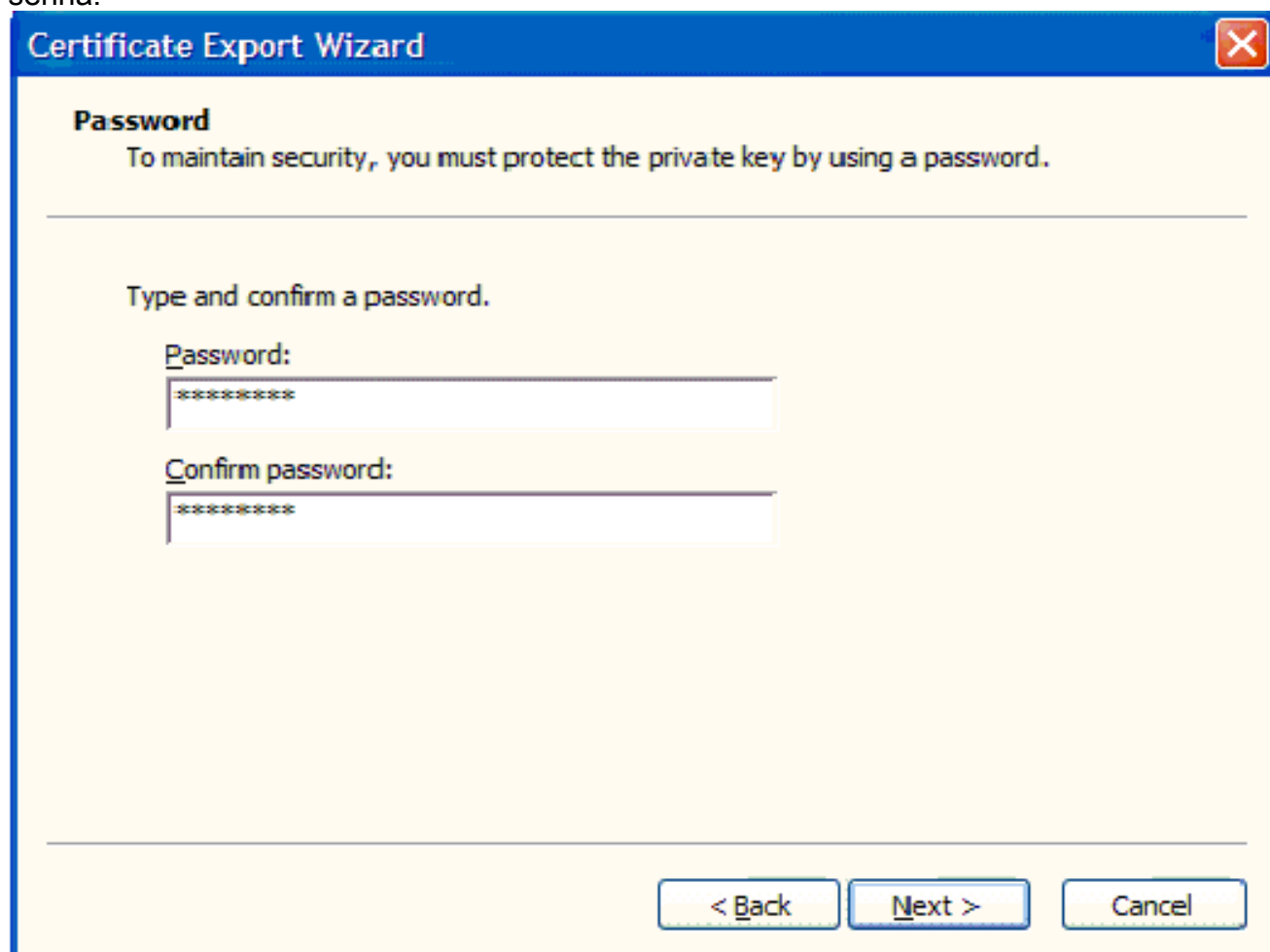
14. Clique em **Avançar** nas janelas a seguir. Escolha a opção **Sim, exportar a chave privada** na janela **Assistente de Exportação de Certificado**. Clique em **Next**.



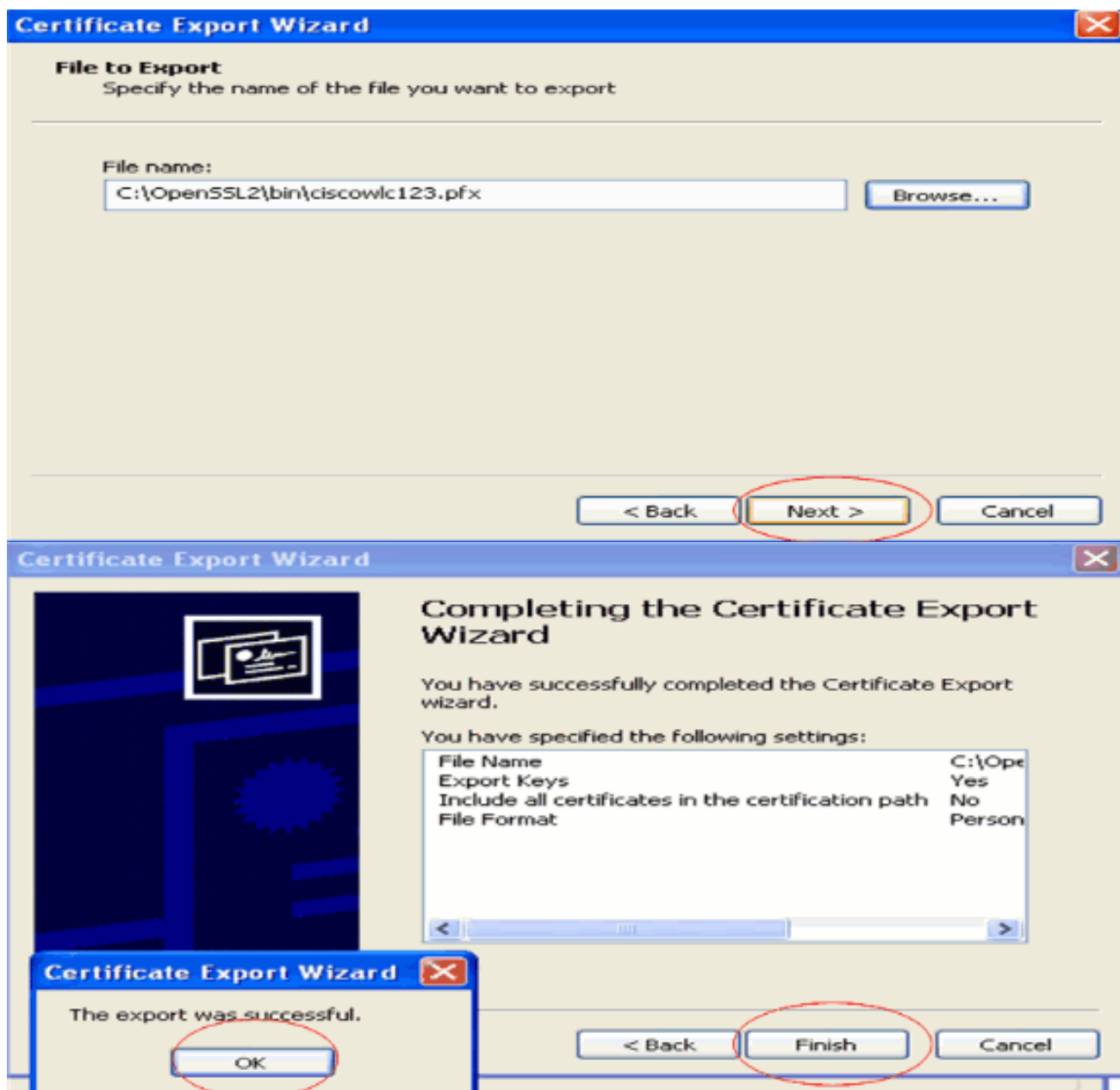
15. Escolha o formato do arquivo de exportação como **.PFX** e escolha a opção **Habilitar proteção forte**. Clique em **Next**.



16. Na janela Senha, digite uma senha. Este exemplo usa **cisco** como a senha.



17. Salve o arquivo de certificado (arquivo .PFX) no disco rígido. Clique em **Avançar** e conclua o processo de exportação com êxito.



[Download do certificado do dispositivo na WLC](#)

Agora que o certificado do dispositivo WLC está disponível como um arquivo .PFX, a próxima etapa é baixar o arquivo para o controlador. As WLCs da Cisco aceitam certificados somente no formato .PEM. Portanto, você precisa primeiro converter o arquivo de formato .PFX ou PKCS12 para um arquivo PEM usando o programa openssl.

[Converter o certificado em PFX para o formato PEM usando o programa openssl](#)

Você pode copiar o certificado para qualquer PC em que tenha o openssl instalado para convertê-lo para o formato PEM. Digite estes comandos no arquivo Openssl.exe na pasta bin do programa openssl:

Observação: você pode fazer download do openssl no [site do OpenSSL](#) .

```
openssl>pkcs12 -in ciscowlc123.pfx -out ciscowlc123.pem
!--- ciscowlc123 is the name used in this example for the exported file. !--- You can specify
any name to your certificate file. Enter Import Password : cisco
```

```
!--- This is the same password that is mentioned in step 16 of the previous section. MAC
verified Ok Enter PEM Pass phrase : cisco
!--- Specify any passphrase here. This example uses the PEM passphrase as cisco. Verifying - PEM
pass phrase : cisco
```

O arquivo de certificado é convertido no formato PEM. A próxima etapa é fazer o download do certificado do dispositivo no formato PEM para o WLC.

Observação: antes disso, você precisa de um software de servidor TFTP em seu PC de onde o arquivo PEM será baixado. Este PC deve ter conectividade com a WLC. O servidor TFTP deve ter seu diretório atual e o diretório base especificados com o local onde o arquivo PEM está armazenado.

[Faça o download do certificado do dispositivo de formato PEM convertido para o WLC](#)

Este exemplo explica o processo de download através do CLI do WLC.

1. Faça login na CLI da controladora.
2. Insira o comando **transfer download datatype eapdevcert**.
3. Insira o comando **transfer download serverip 10.77.244.196**. 10.77.244.196 é o endereço IP do servidor TFTP.
4. Insira o comando **transfer download filename ciscowlc.pem**. ciscowlc123.pem é o nome de arquivo usado neste exemplo.
5. Insira o comando **transfer download certpassword** para definir a senha do certificado.
6. Insira o comando **transfer download start** para exibir as configurações atualizadas. Em seguida, responda **y** quando for solicitado que confirme as configurações atuais e inicie o processo de download. Este exemplo mostra a saída do comando download:

```
(Cisco Controller) >transfer download start

Mode..... TFTP
Data Type..... Vendor Dev Cert
TFTP Server IP..... 10.77.244.196
TFTP Packet Timeout..... 6
TFTP Max Retries..... 10
TFTP Path.....
TFTP Filename..... ciscowlc.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 the new certificate.
Enter the reset system command to reboot the controller.
The controller is now loaded with the device certificate.
```

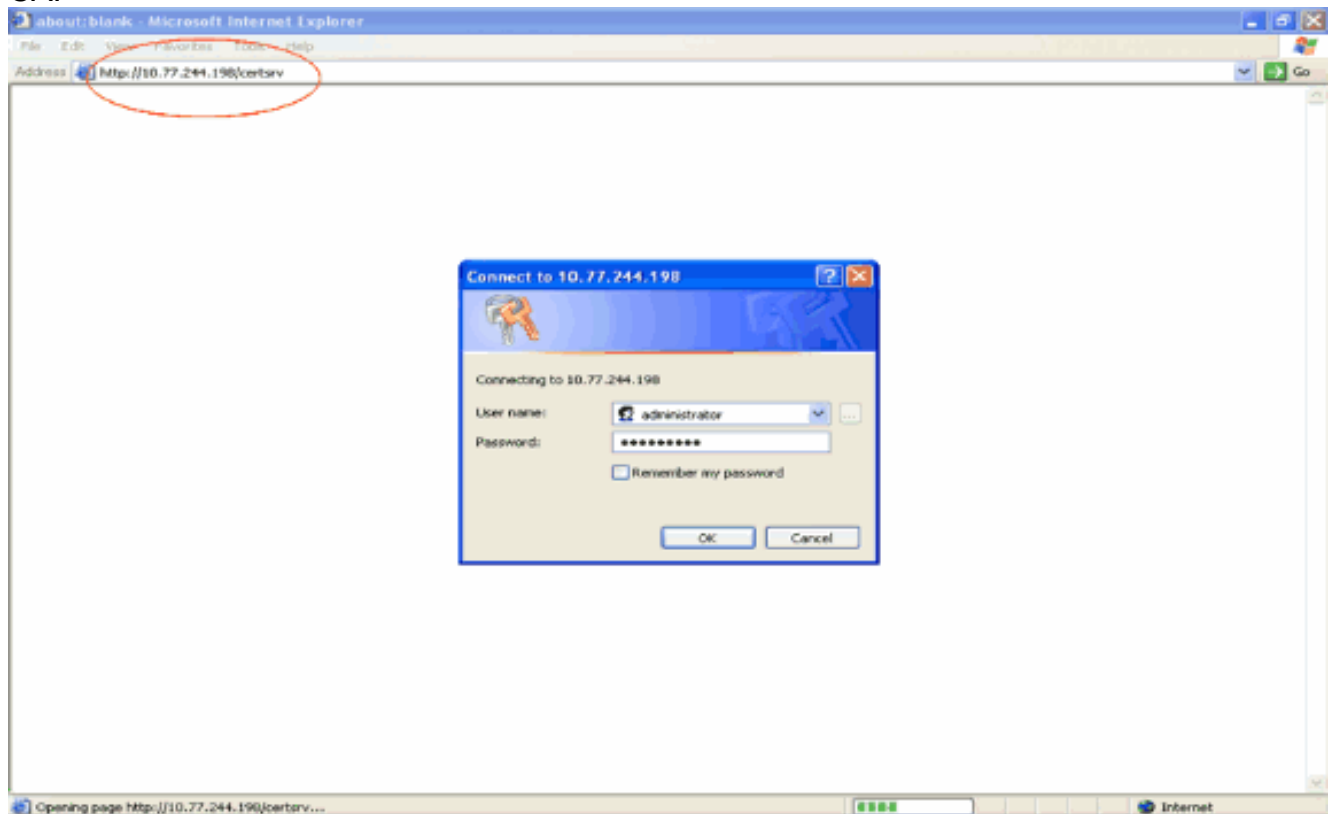
7. Digite o comando **reset system** para reinicializar a controladora. O controlador agora está carregado com o certificado do dispositivo.

[Instalar o certificado raiz de PKI no WLC](#)

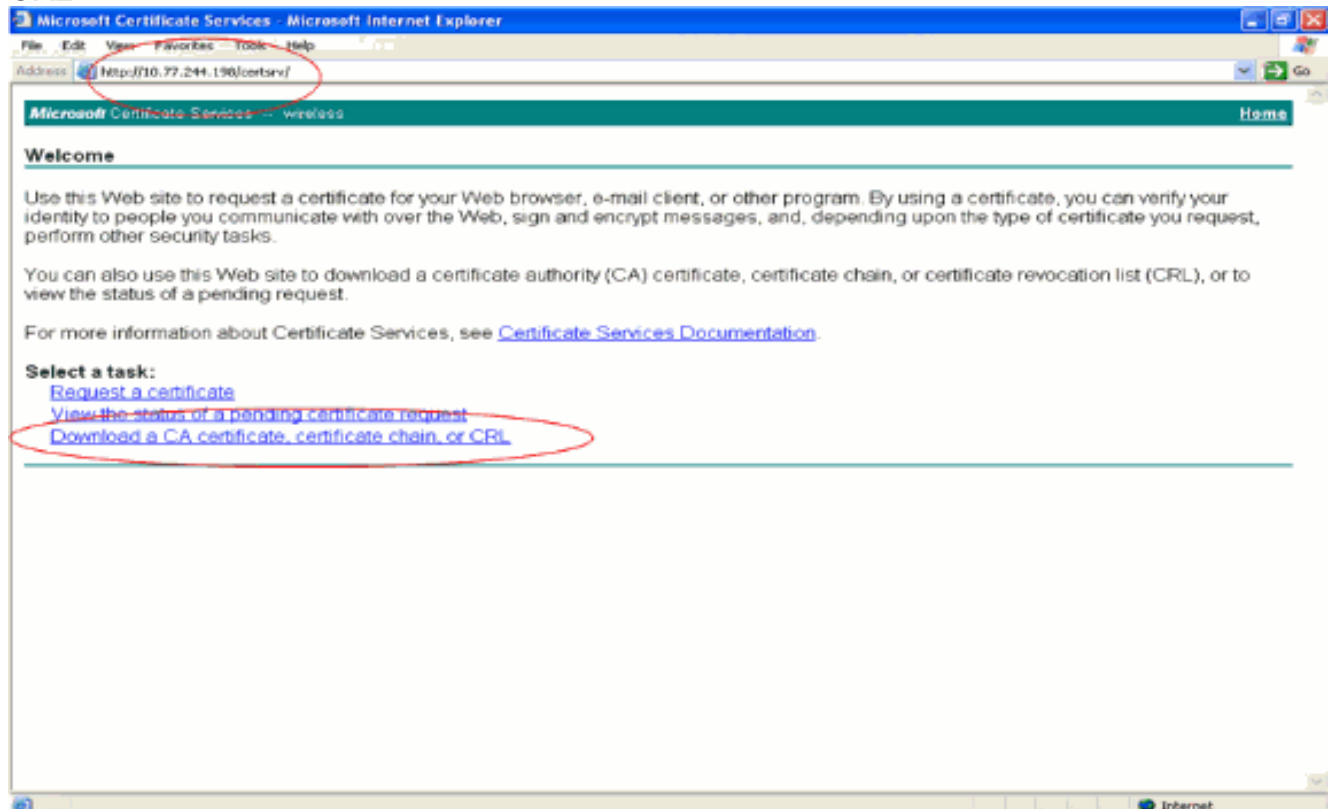
Agora que o certificado do dispositivo está instalado na WLC, a próxima etapa é instalar o certificado raiz da PKI na WLC a partir do servidor da CA. Execute estas etapas:

1. Acesse **http://<endereço IP do servidor de CA>/certsrv** no PC que tem uma conexão de rede com o servidor de CA. Efetue login como administrador do servidor de

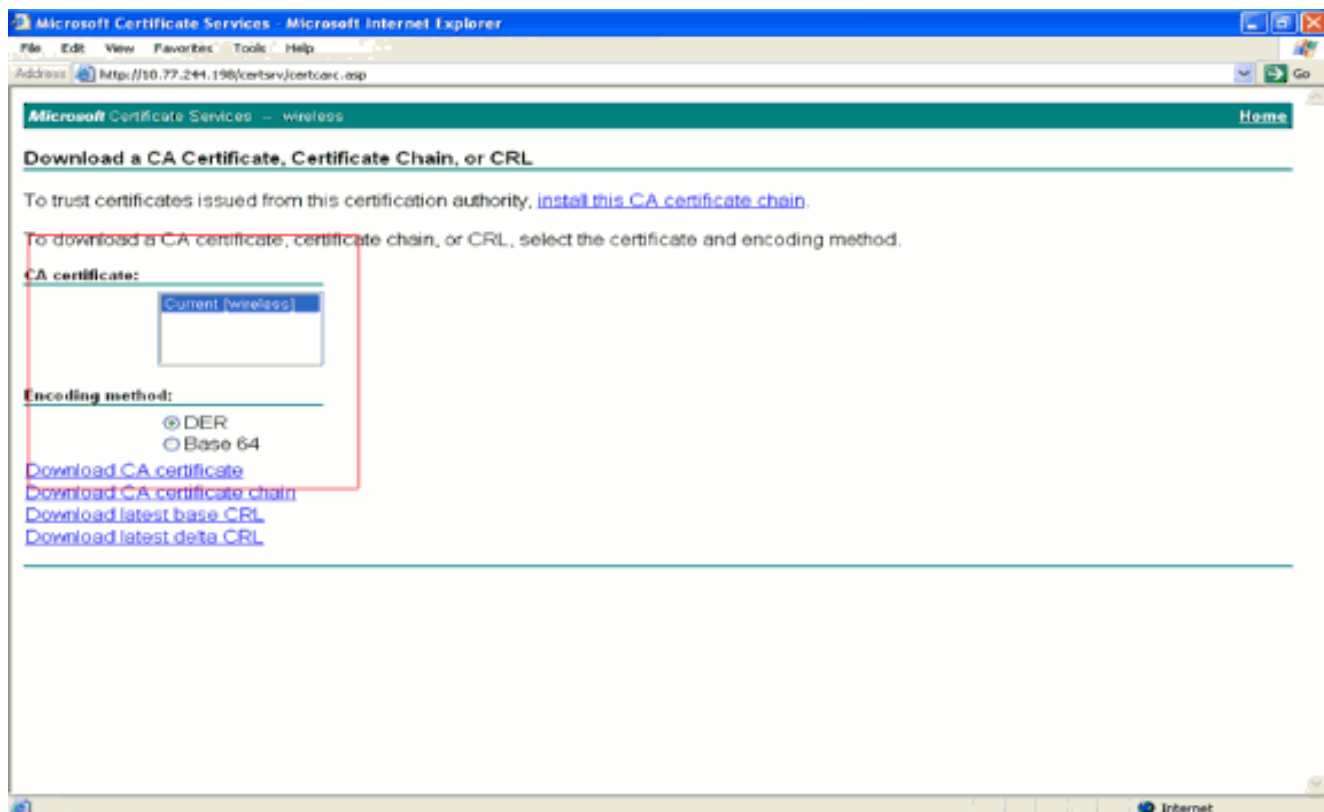
CA.



2. Clique em **Baixar um certificado de CA, uma cadeia de certificados ou um CRL.**



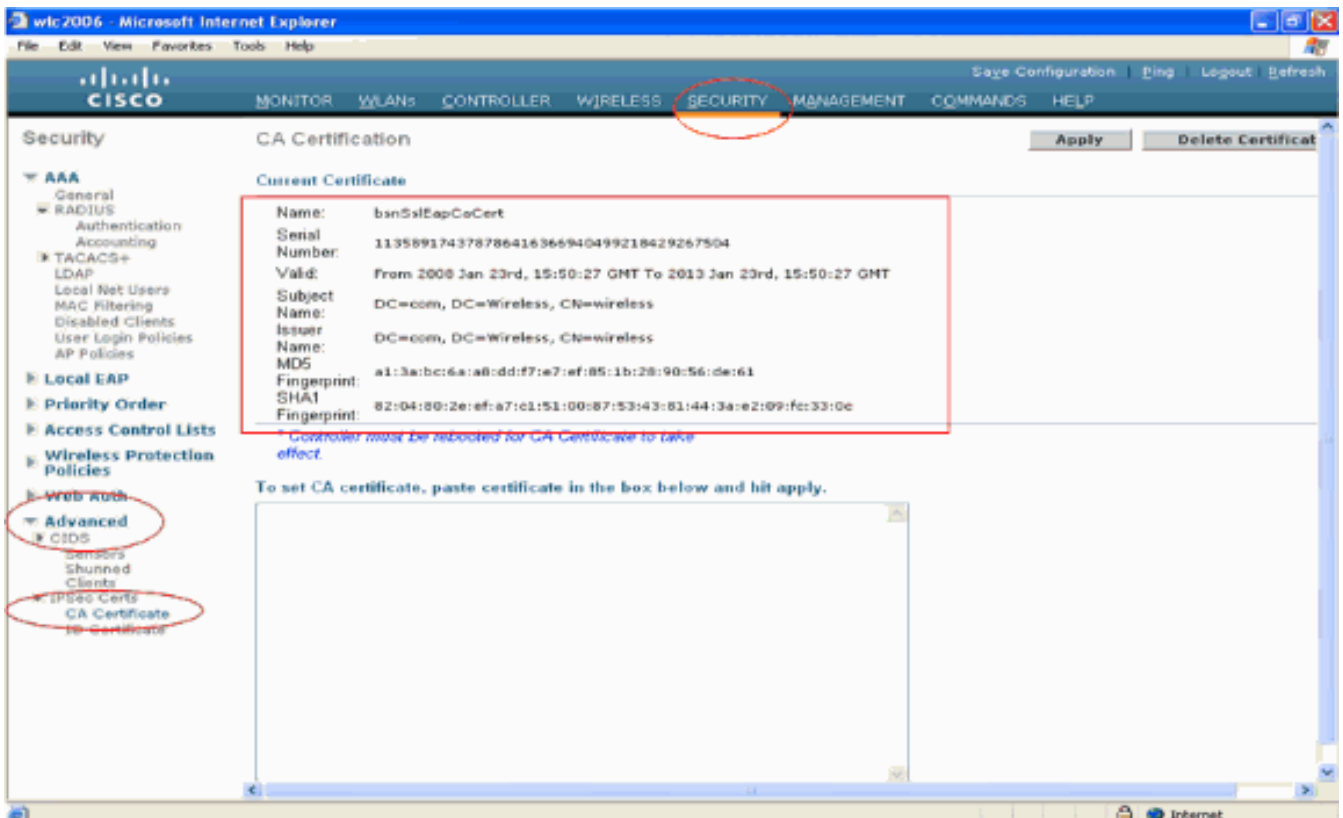
3. Na página resultante, você pode ver os certificados CA atuais disponíveis no servidor CA na caixa **CA certificate**. Escolha **DER** como o método de codificação e clique em **Download CA certificate**.



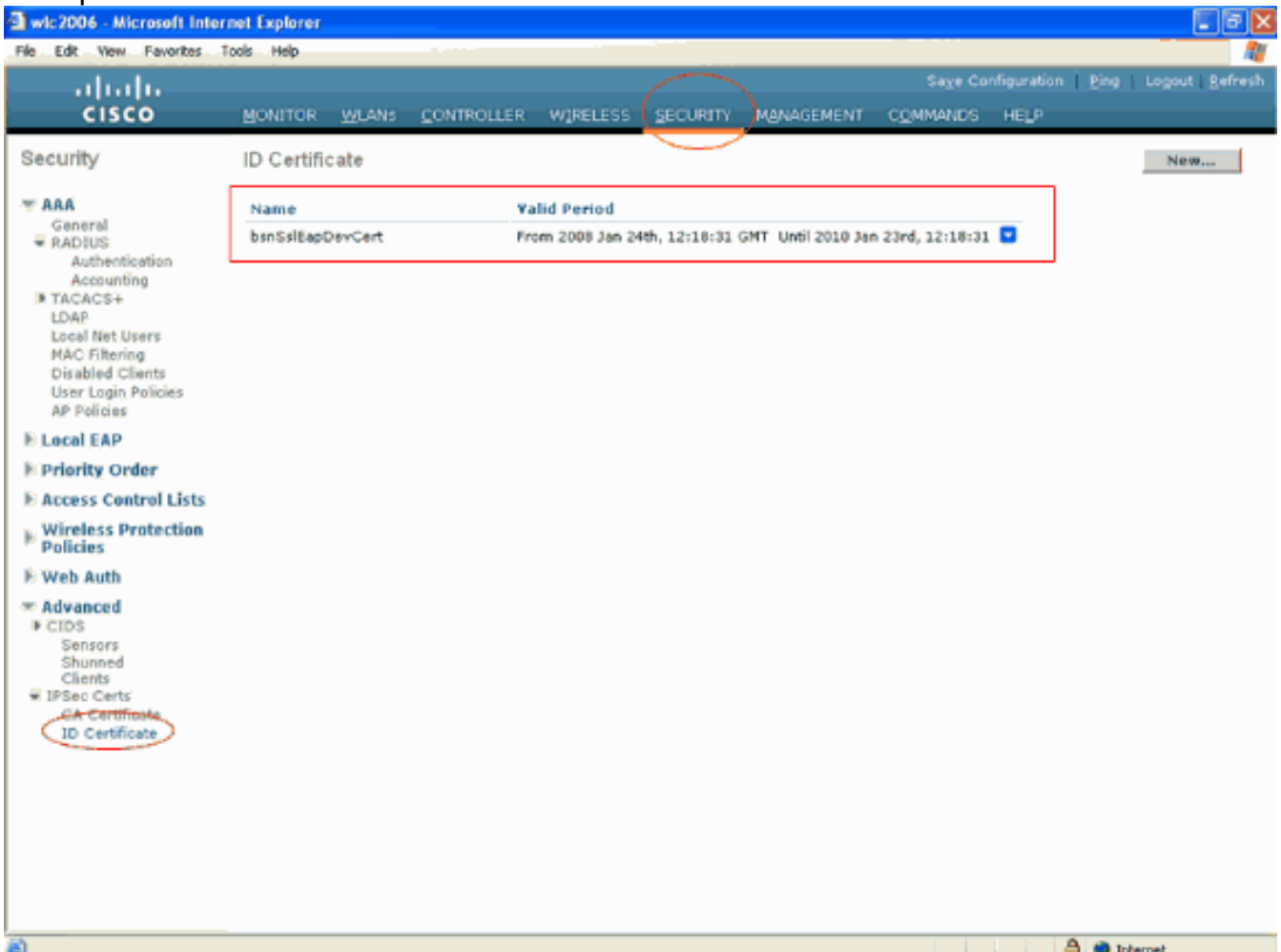
4. Salve o certificado como um arquivo **.cer**. Este exemplo usa **certnew.cer** como o nome do arquivo.
5. O próximo passo é converter o arquivo **.cer** para o formato PEM e baixá-lo para a controladora. Para executar essas etapas, repita o mesmo procedimento explicado na seção [Download do certificado do dispositivo para a WLC](#) com estas alterações: Os arquivos openssl "-in" e "-out" são **certnew.cer** e **certnew.pem**. Além disso, nenhuma senha PEM ou senha de importação é necessária nesse processo. Além disso, o comando openssl para converter o arquivo **.cer** para o arquivo **.pem** é: **x509 -in certnew.cer -inform DER -out certnew.pem -outform PEM** Na etapa 2 da seção [Download the Converted PEM Format Device Certificate to the WLC](#), o comando para baixar o certificado para a WLC é: (Cisco Controller) > **transferir download tipo de dados eapcacer** O arquivo a ser baixado para a WLC é **certnew.pem**.

Você pode verificar se os certificados estão instalados na WLC a partir da GUI da controladora, da seguinte maneira:

- Na GUI da WLC, clique em **Security**. Na página Security, clique em **Advanced > IPsec Certs** nas tarefas que aparecem à esquerda. Clique em **CA Certificate** para exibir o certificado de CA instalado. Aqui está o exemplo:



- Para verificar se o certificado do dispositivo está instalado na WLC, na GUI da WLC, clique em **Security**. Na página Security, clique em **Advanced > IPSec Certs** nas tarefas que aparecem à esquerda. Clique em **ID Certificate** para exibir o certificado do dispositivo instalado. Aqui está o exemplo:

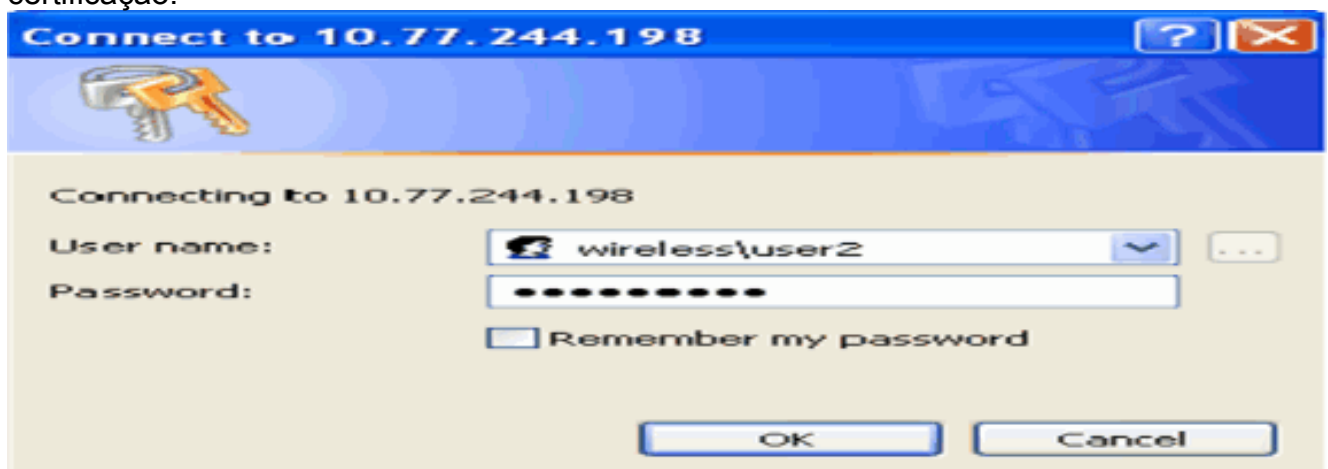


Gerar um certificado de dispositivo para o cliente

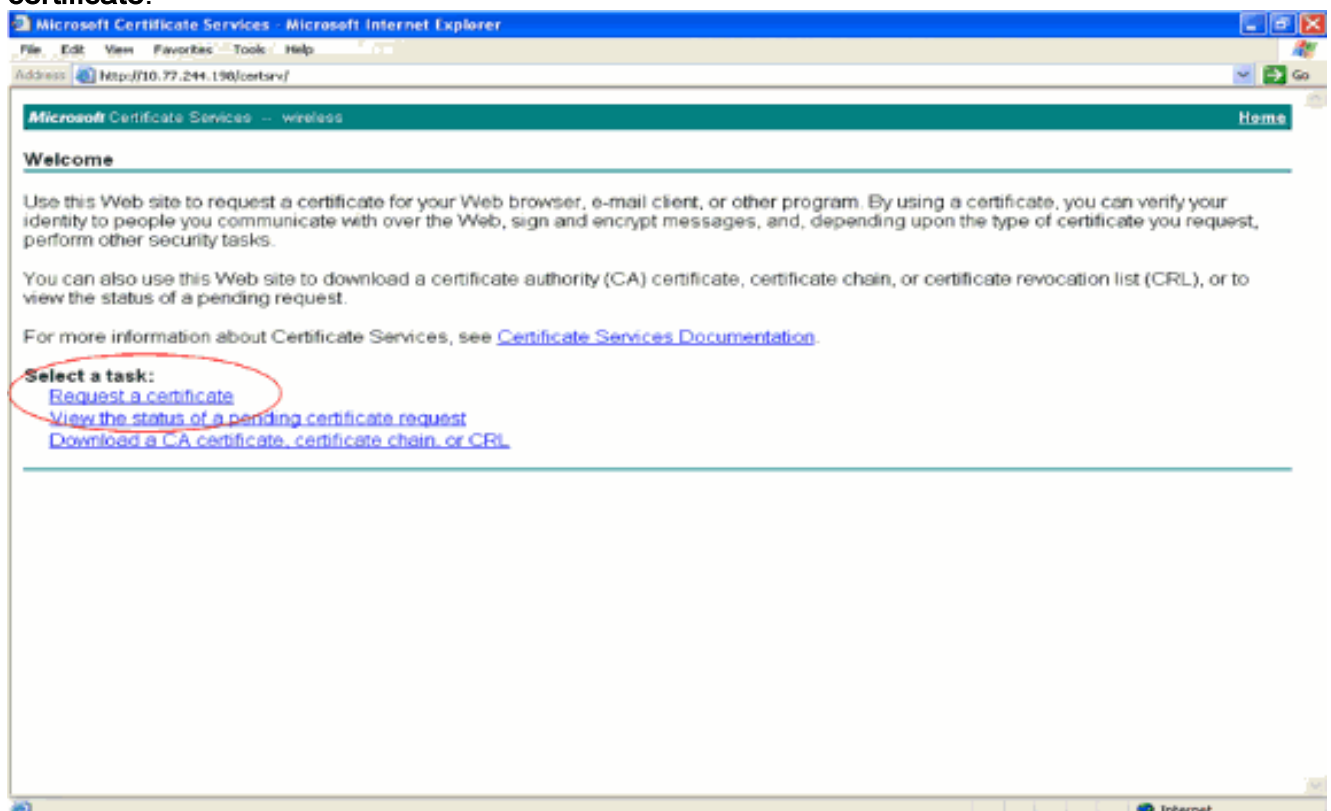
Agora que o certificado do dispositivo e o certificado da CA estão instalados na WLC, a próxima etapa é gerar esses certificados para o cliente.

Execute estas etapas para gerar o certificado do dispositivo para o cliente. Esse certificado será usado pelo cliente para autenticar na WLC. Este documento explica as etapas envolvidas na geração de certificados para o cliente profissional Windows XP.

1. Vá para <http://<endereço IP do servidor de autoridade de certificação>/certsrv> do cliente que requer que o certificado seja instalado. Efetue login como nome de domínio\nome de usuário no servidor de CA. O nome de usuário deve ser o nome do usuário que está usando esta máquina com o XP e o usuário já deve estar configurado como parte do mesmo domínio que o servidor da autoridade de certificação.

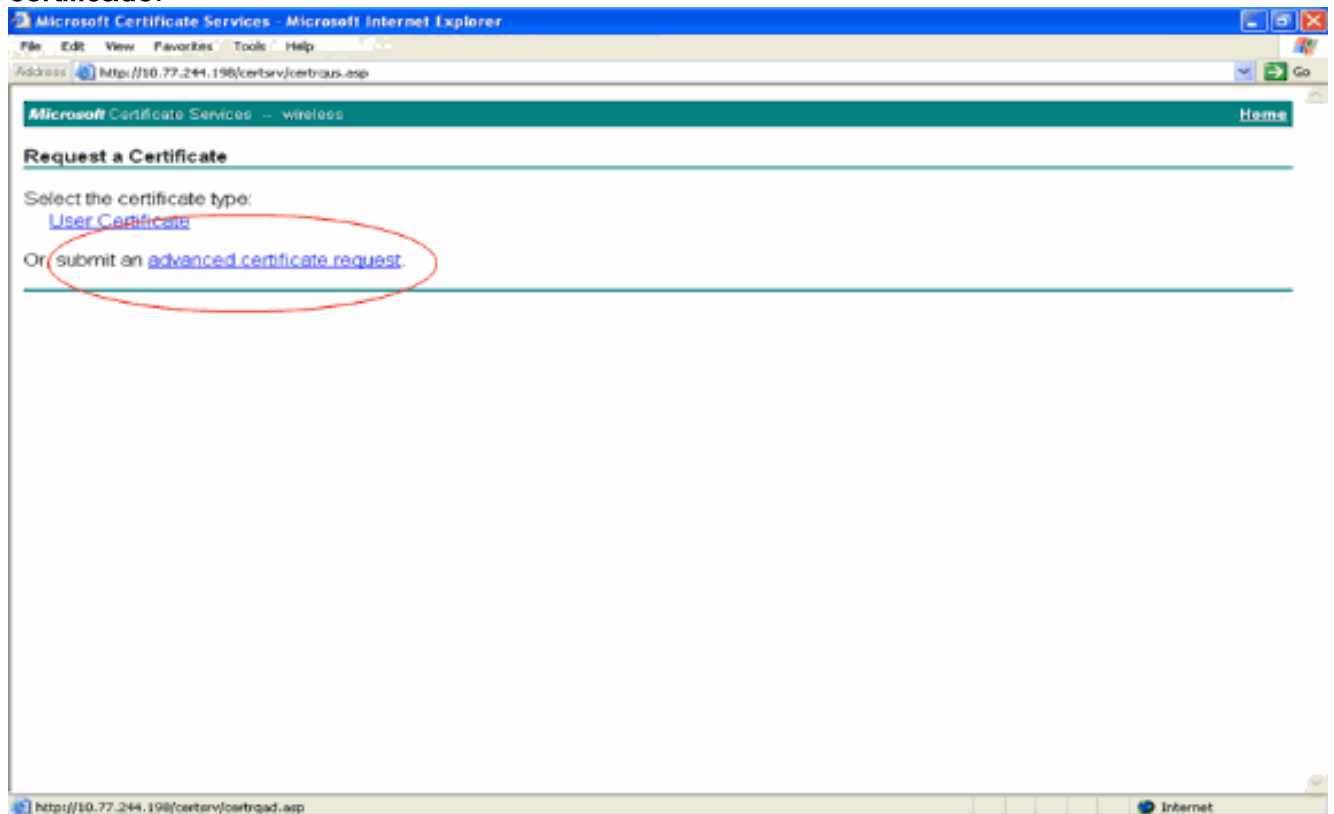


2. Selecione **Request a certificate**.

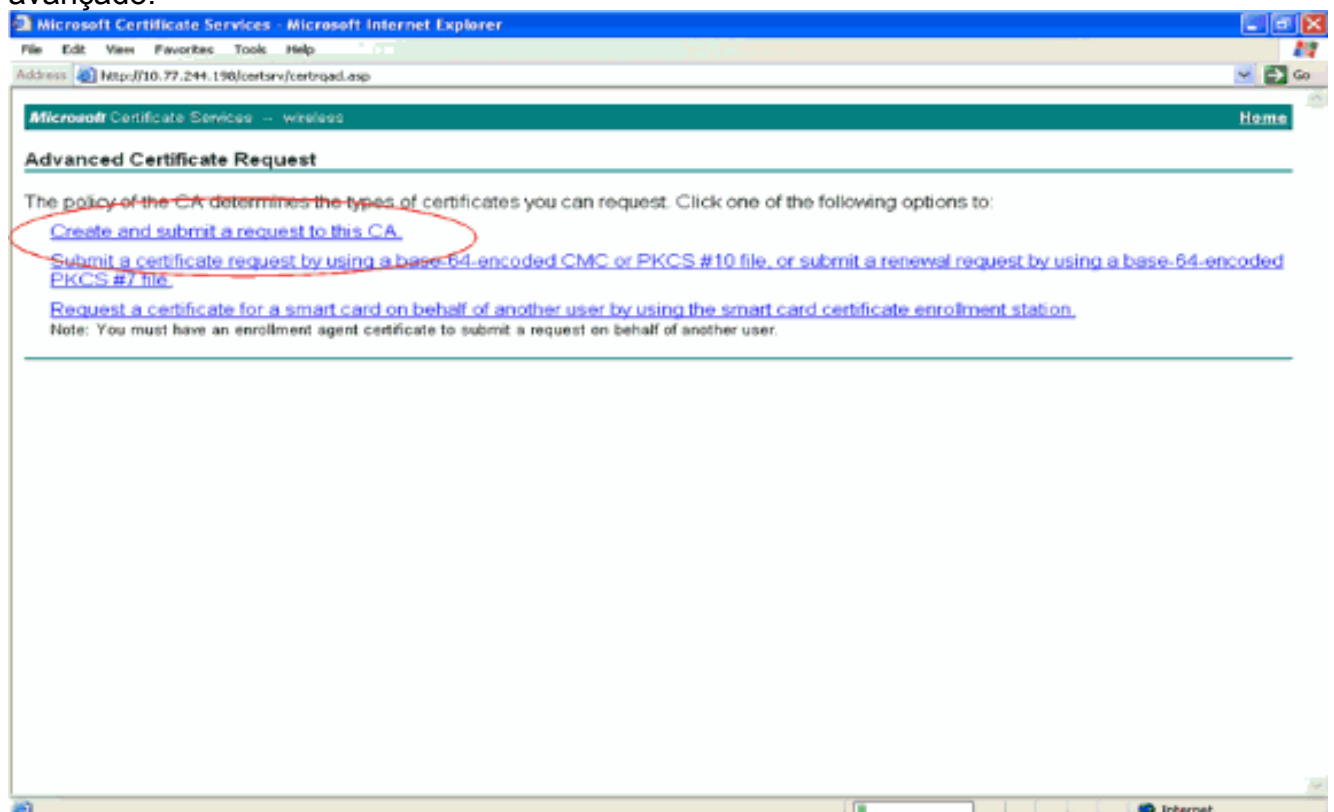


3. Na página Solicitar um certificado, clique em **solicitação avançada de**

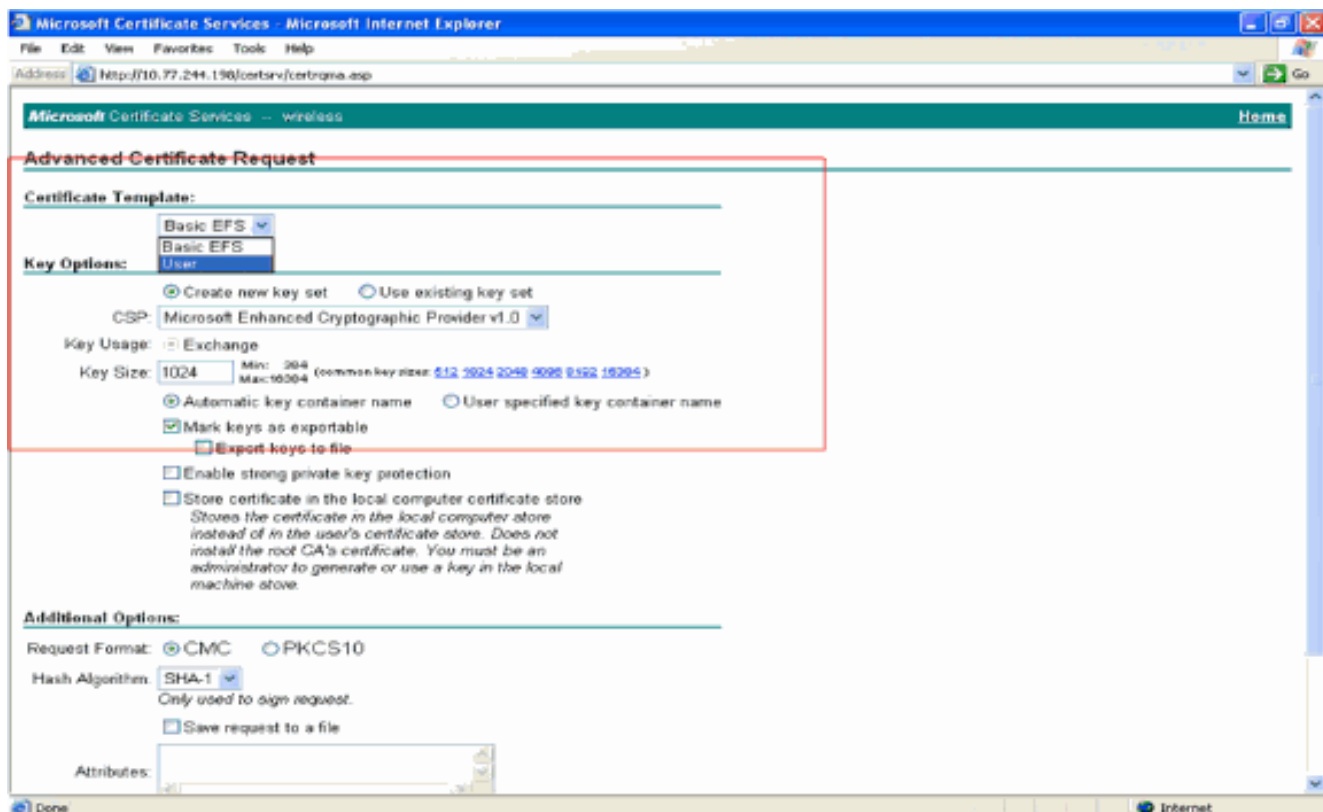
certificado.



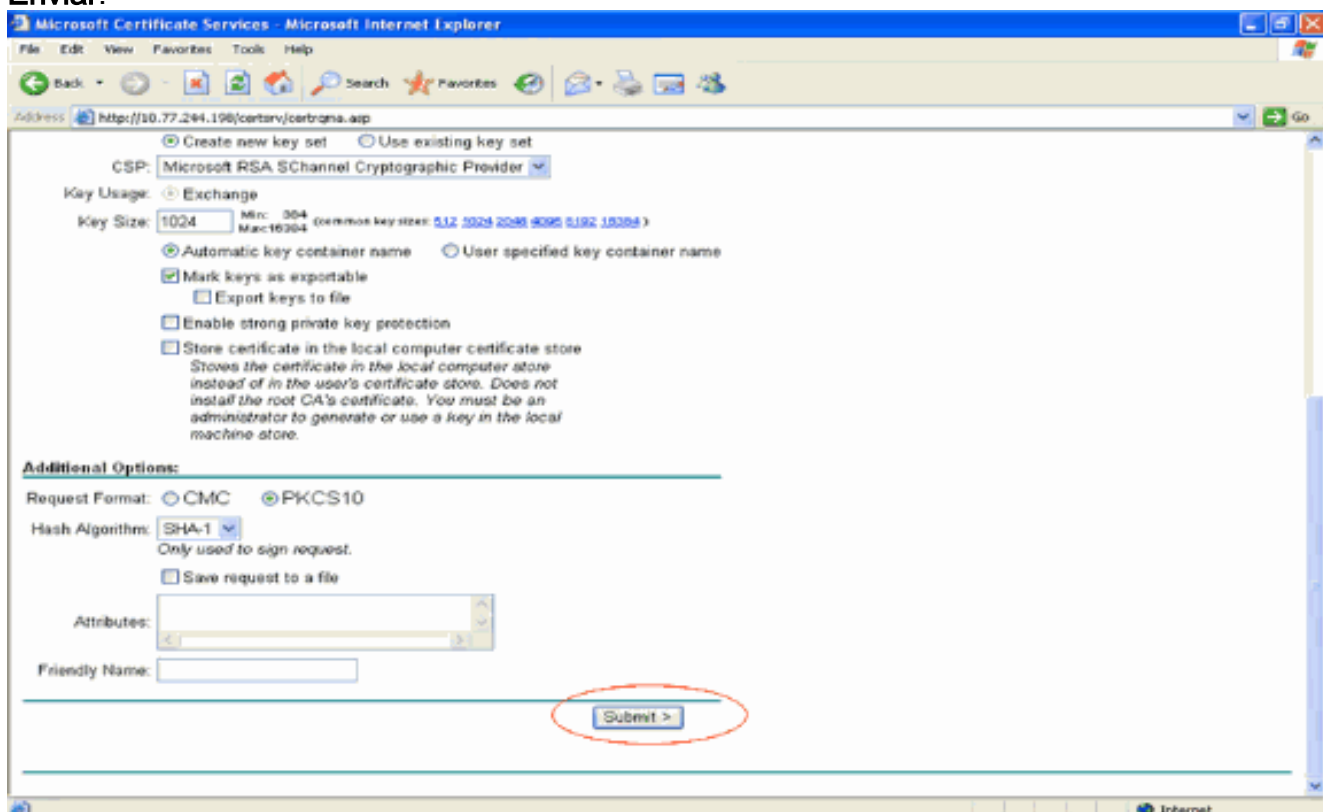
4. Na página Solicitação avançada de certificado, clique em **Criar e enviar uma solicitação a esta CA**. Isso o levará para o formulário de solicitação de certificado avançado.



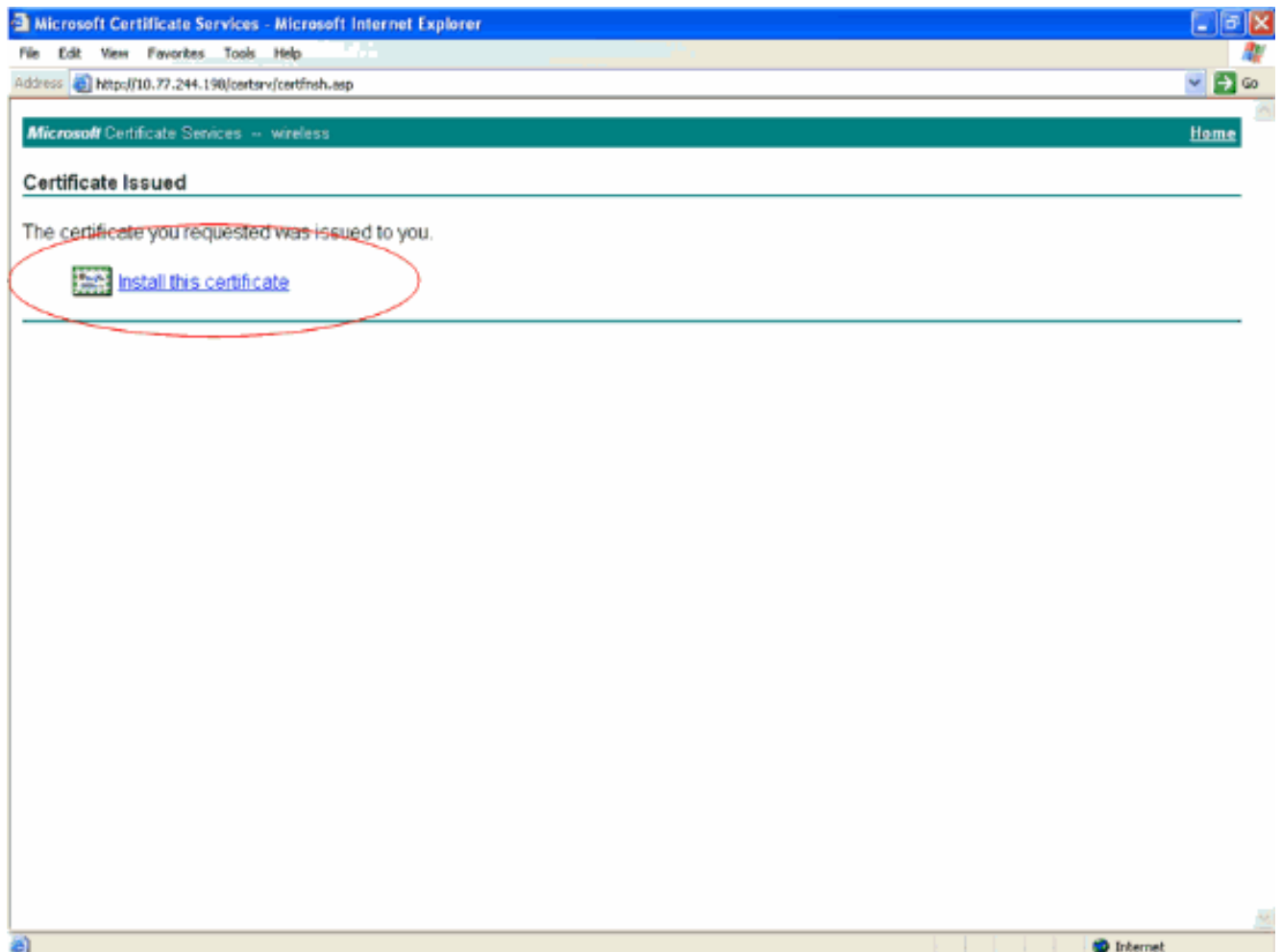
5. No formulário de solicitação de certificado avançado, escolha **Usuário** no menu suspenso Modelo de certificado. Na seção Opções-chave, escolha estes parâmetros: Digite o tamanho da chave no campo Tamanho da chave. Este exemplo usa 1024. Marque a opção **Mark Keys as Exportable**.



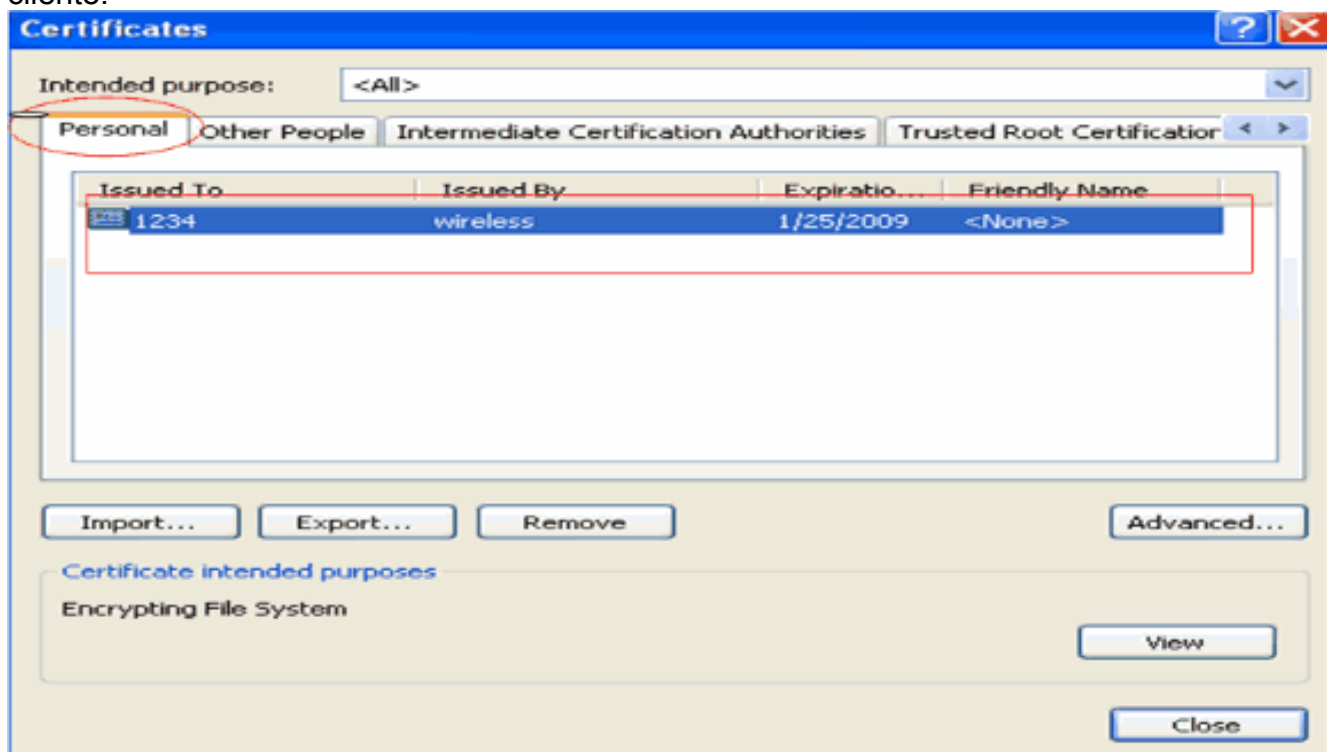
6. Configure todos os outros campos necessários e clique em **Enviar**.



7. O certificado do dispositivo do cliente agora é gerado de acordo com a solicitação. Clique em **Instalar o certificado** para instalar o certificado no armazenamento de certificados.



8. Você deve conseguir localizar o certificado do dispositivo do cliente instalado na Lista de certificados pessoais em Ferramentas > Opções da Internet > Conteúdo > Certificados no navegador IE do cliente.

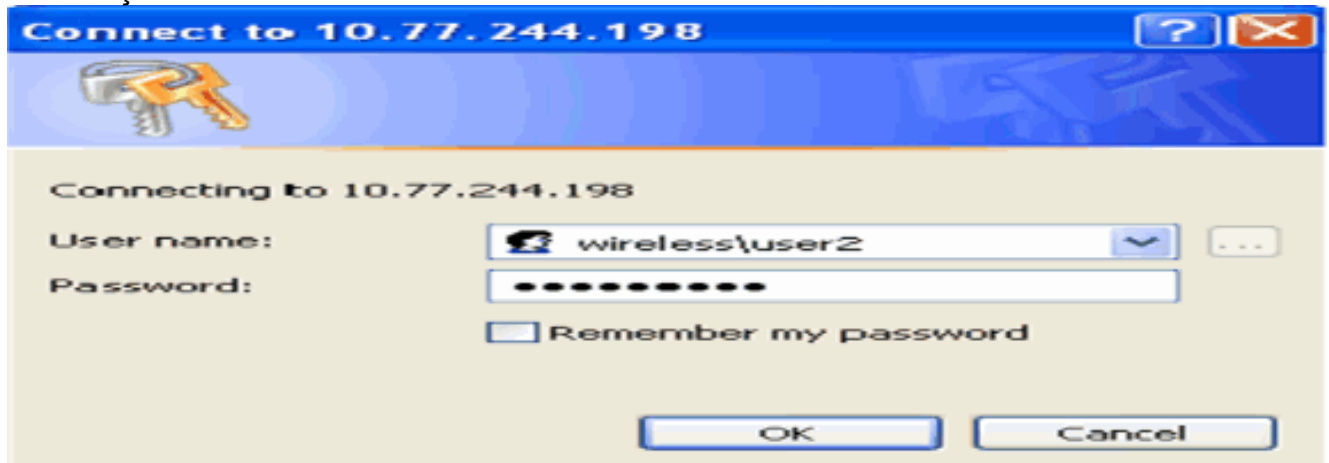


O certificado do dispositivo para o cliente está instalado no cliente.

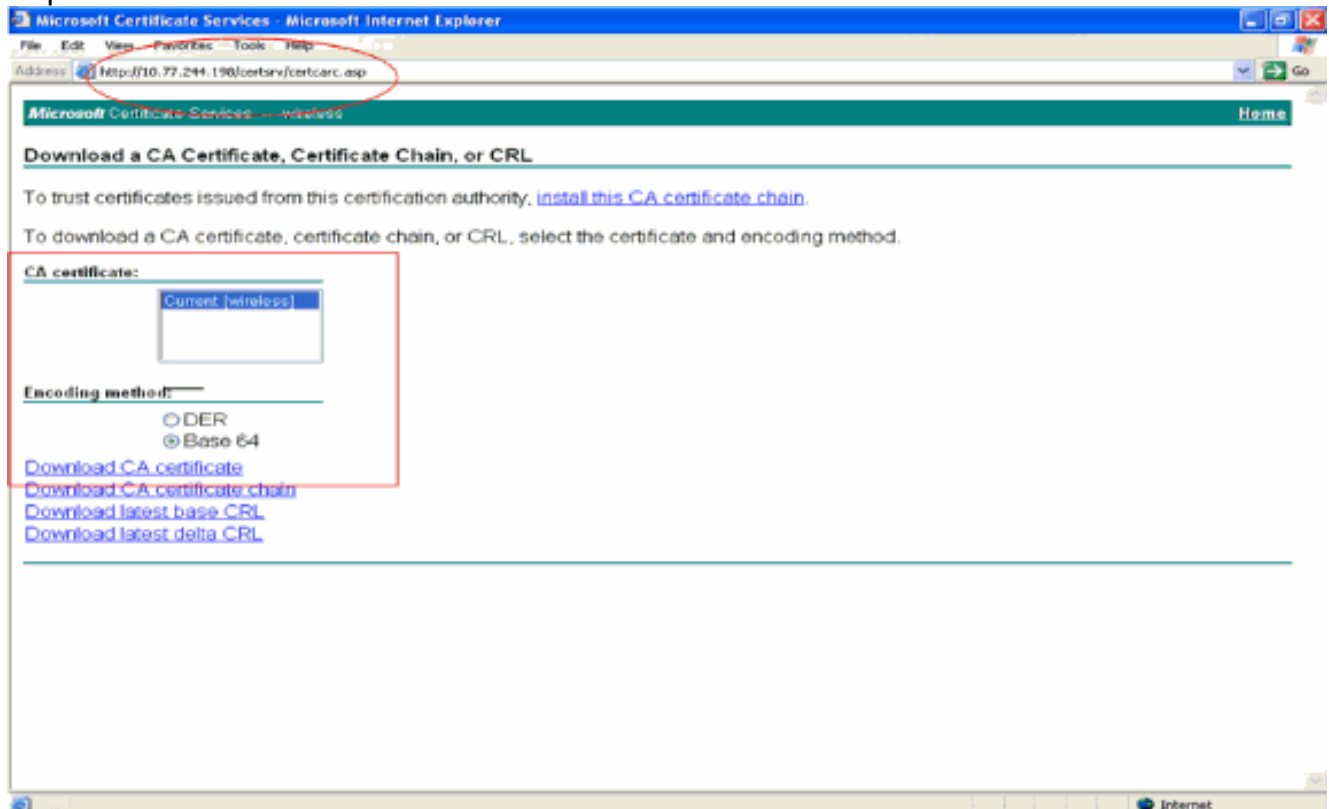
[Gerar o Certificado de CA Raiz para o Cliente](#)

A próxima etapa é gerar o certificado CA para o cliente. Conclua estas etapas a partir do PC cliente:

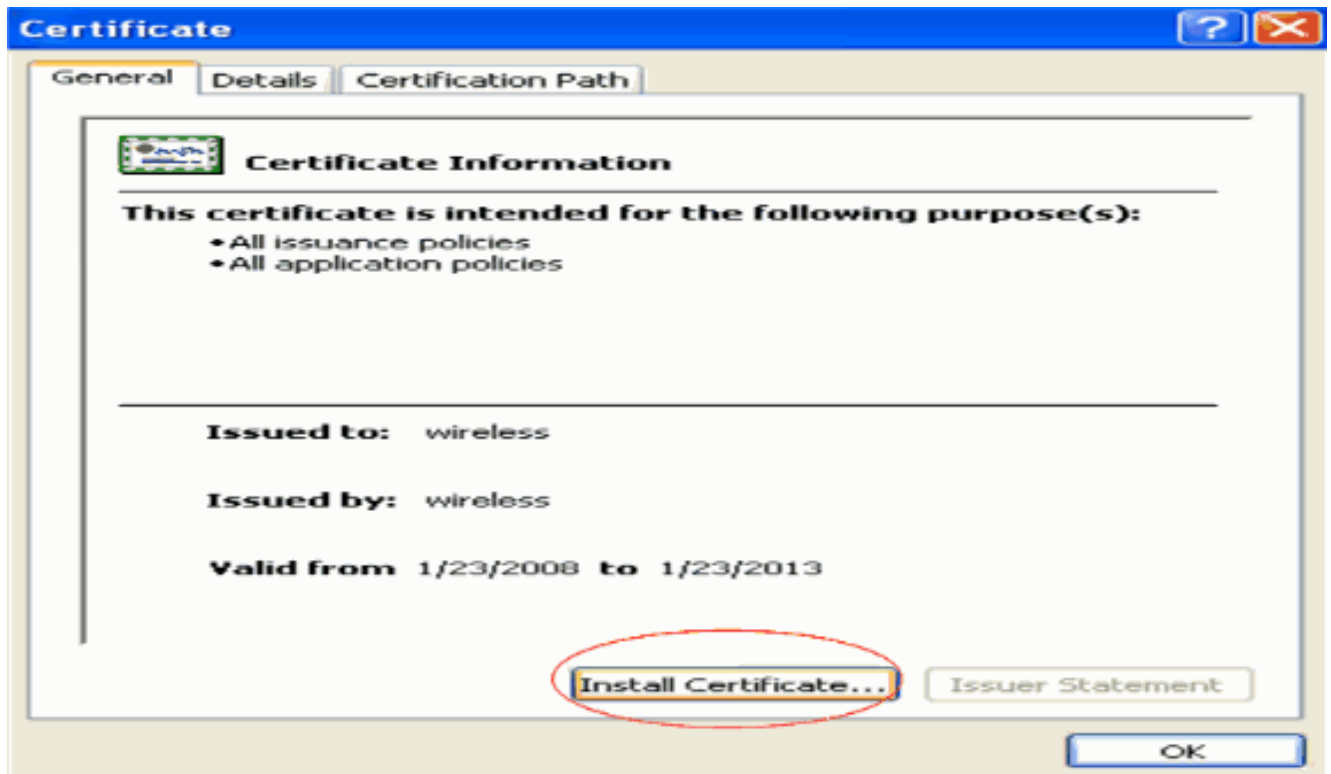
1. Vá para <http://<endereço IP do servidor de autoridade de certificação>/certsrv> do cliente que requer que o certificado seja instalado. Efetue login como nome de domínio\nome de usuário no servidor de CA. O nome de usuário deve ser o nome do usuário que está usando esta máquina com o XP e o usuário já deve estar configurado como parte do mesmo domínio que o servidor da autoridade de certificação.



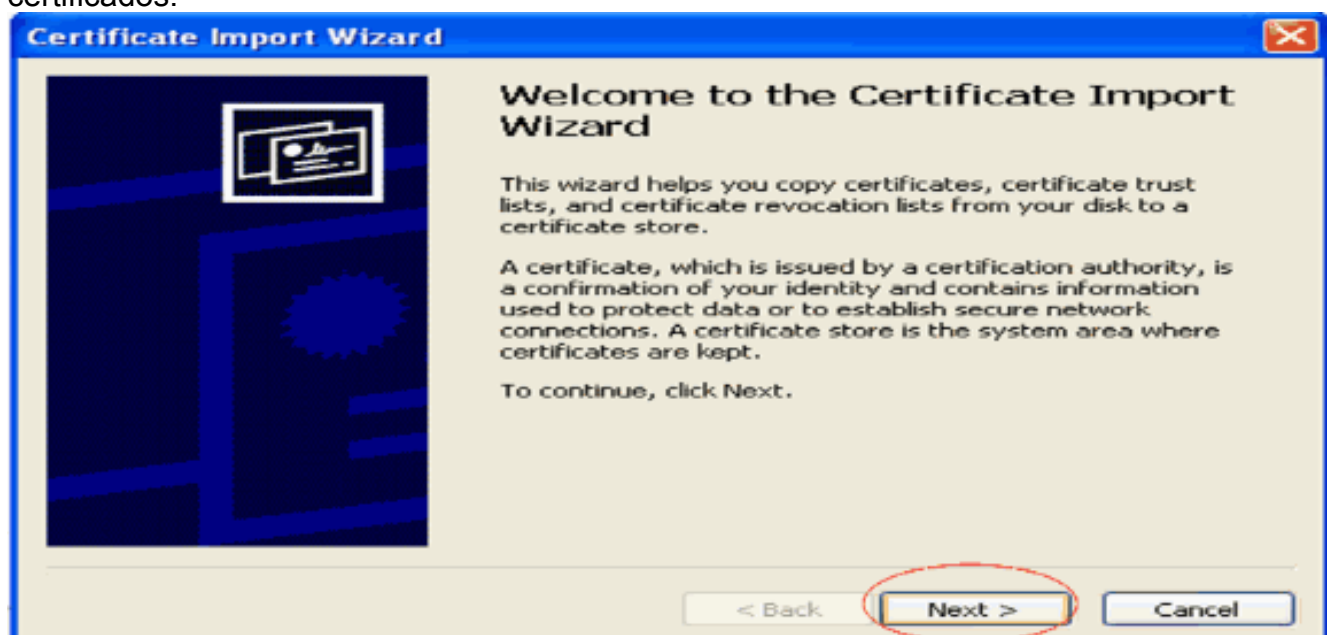
2. Na página resultante, você pode ver os certificados CA atuais disponíveis no servidor CA na caixa **CA certificate**. Escolha **Base 64** como o método de codificação. Em seguida, clique em **Download CA certificate** e salve o arquivo no PC do cliente como um arquivo **.cer**. Este exemplo usa **rootca.cer** como o nome do arquivo.



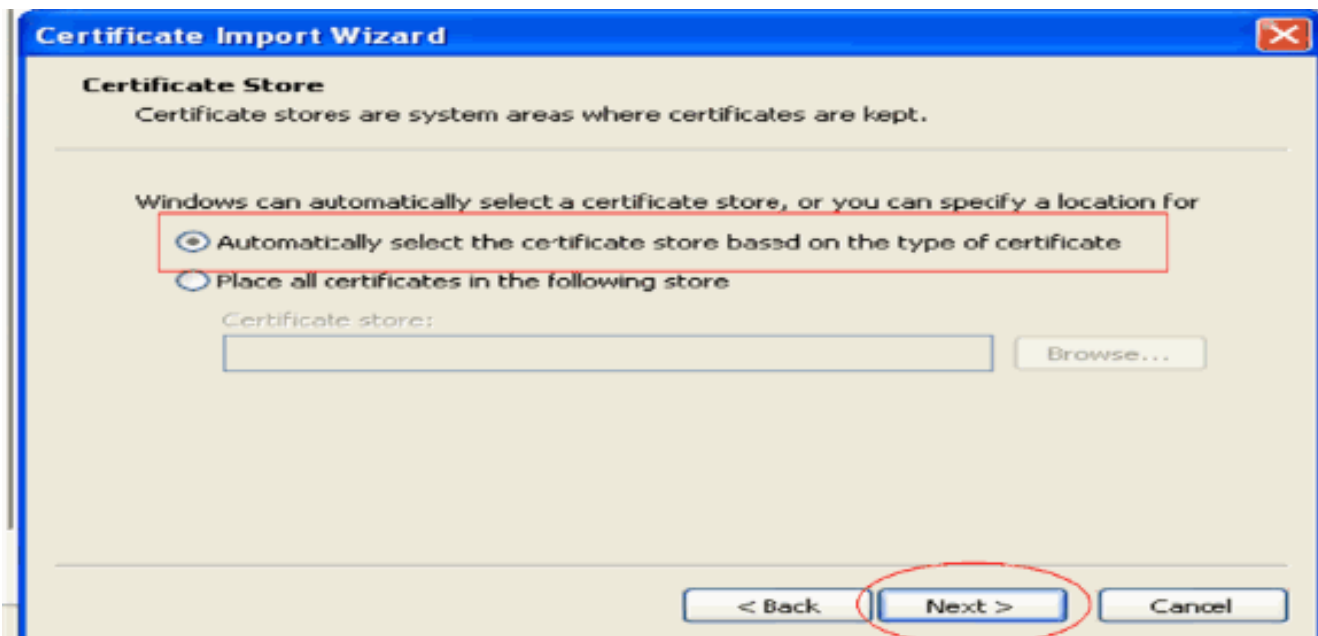
3. Em seguida, instale o certificado CA salvo no formato **.cer** no armazenamento de certificados do cliente. Clique duas vezes no arquivo **rootca.cer** e clique em **Instalar certificado**.



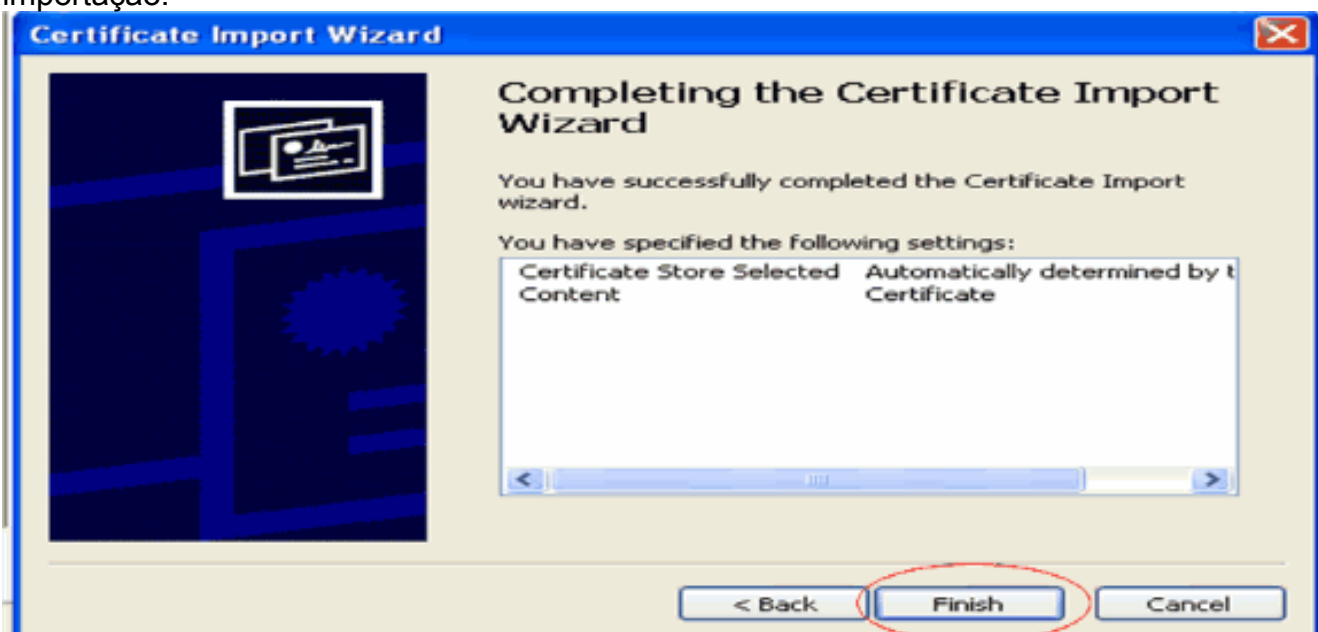
4. Clique em **Avançar** para importar o certificado do disco rígido do cliente para o armazenamento de certificados.



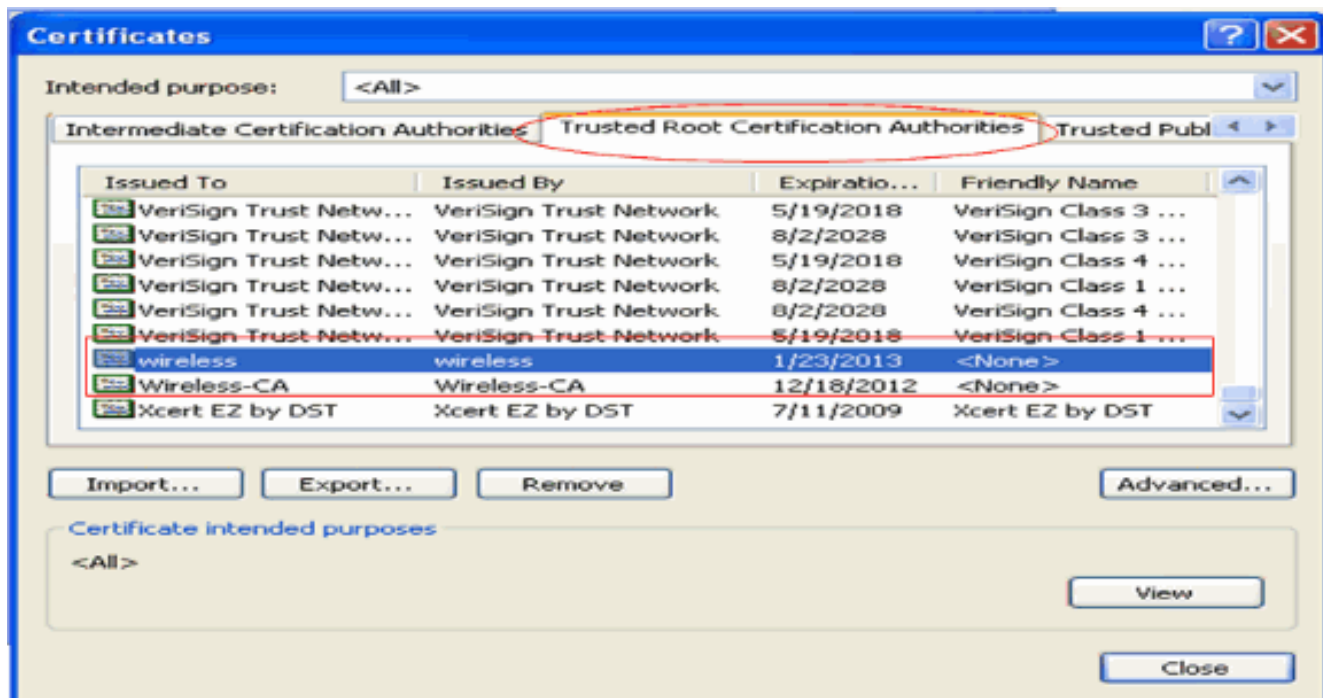
5. Selecione **Automatically select the certificate store based on the type of certificate** e clique em **Next**.



6. Clique em **Finish** para finalizar o processo de importação.



7. Por padrão, os certificados da CA são instalados na lista Autoridades de certificação raiz confiáveis no navegador IE do cliente em **Ferramentas > Opções da Internet > Conteúdo > Certificados**. Aqui está o exemplo:

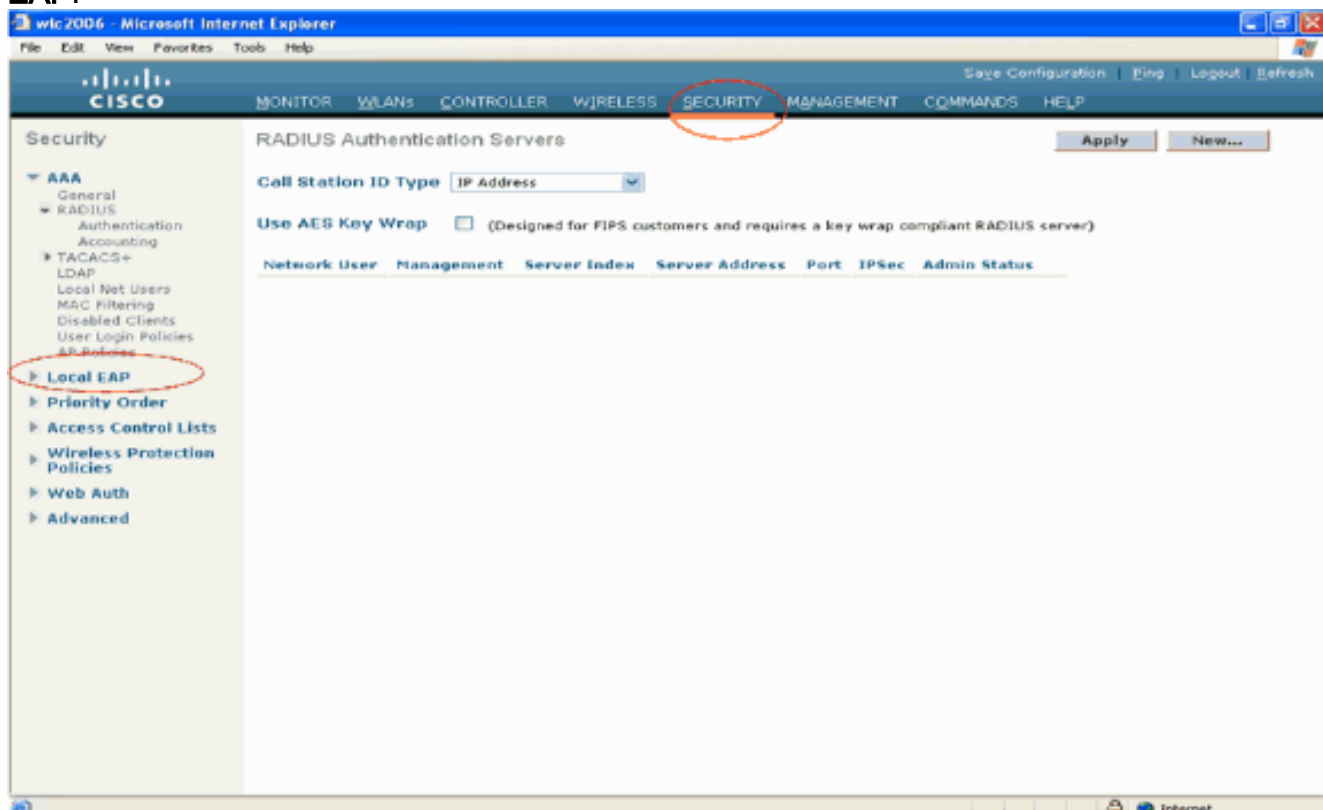


Todos os certificados necessários estão instalados na WLC, bem como no cliente para autenticação EAP-FAST Local EAP. A próxima etapa é configurar a WLC para a autenticação EAP local.

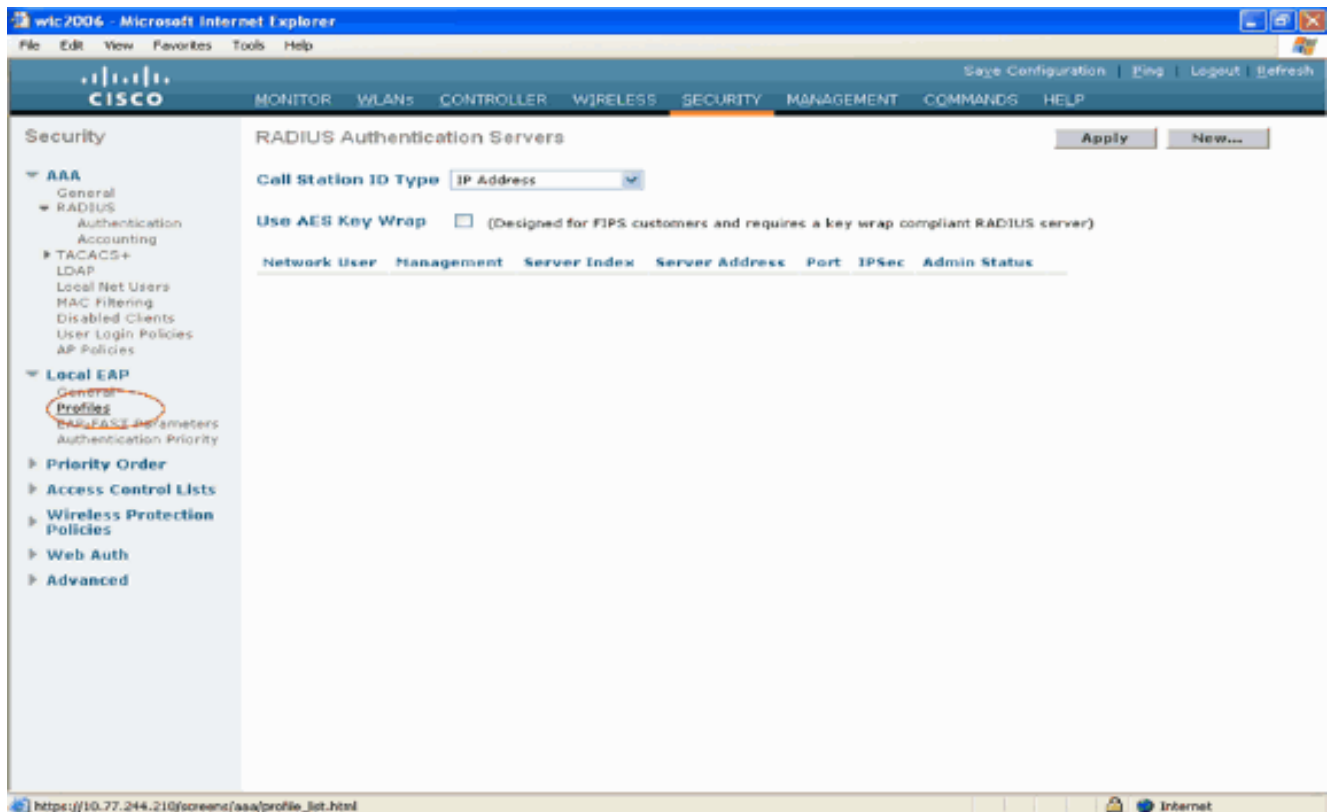
Configurar o EAP local no WLC

Conclua estes passos a partir do modo GUI da WLC para configurar a autenticação EAP Local na WLC:

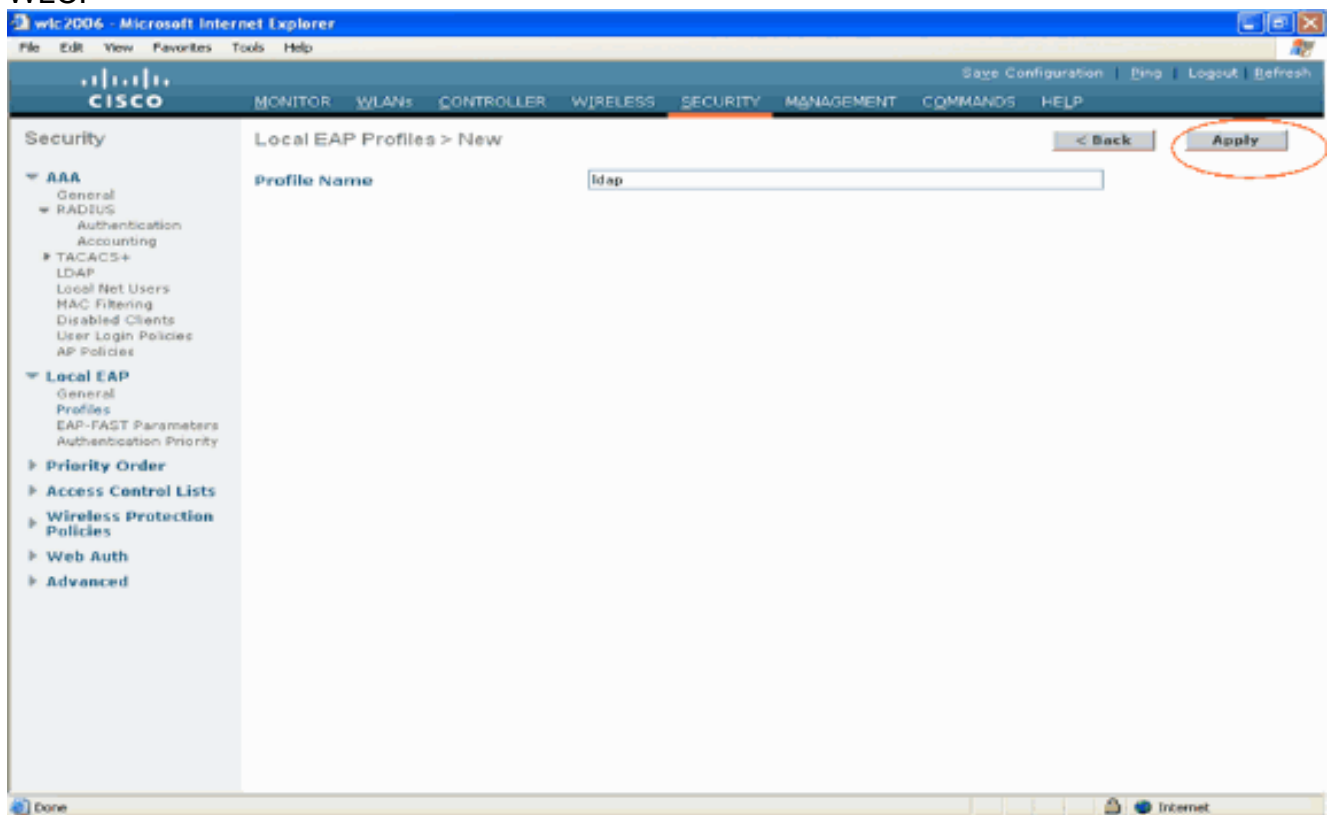
1. Clique em **Security > Local EAP**.



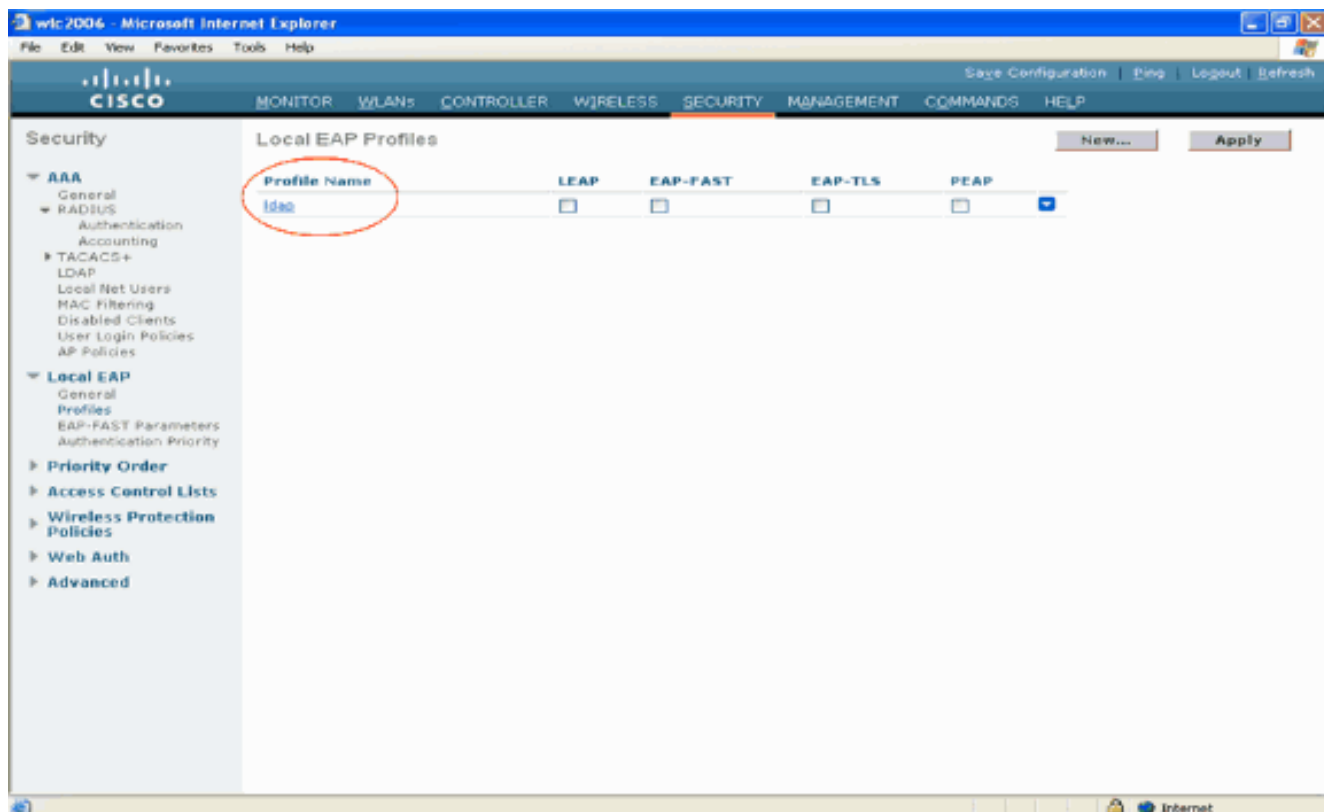
2. Em Local EAP, clique em **Profiles** para configurar o perfil Local EAP.



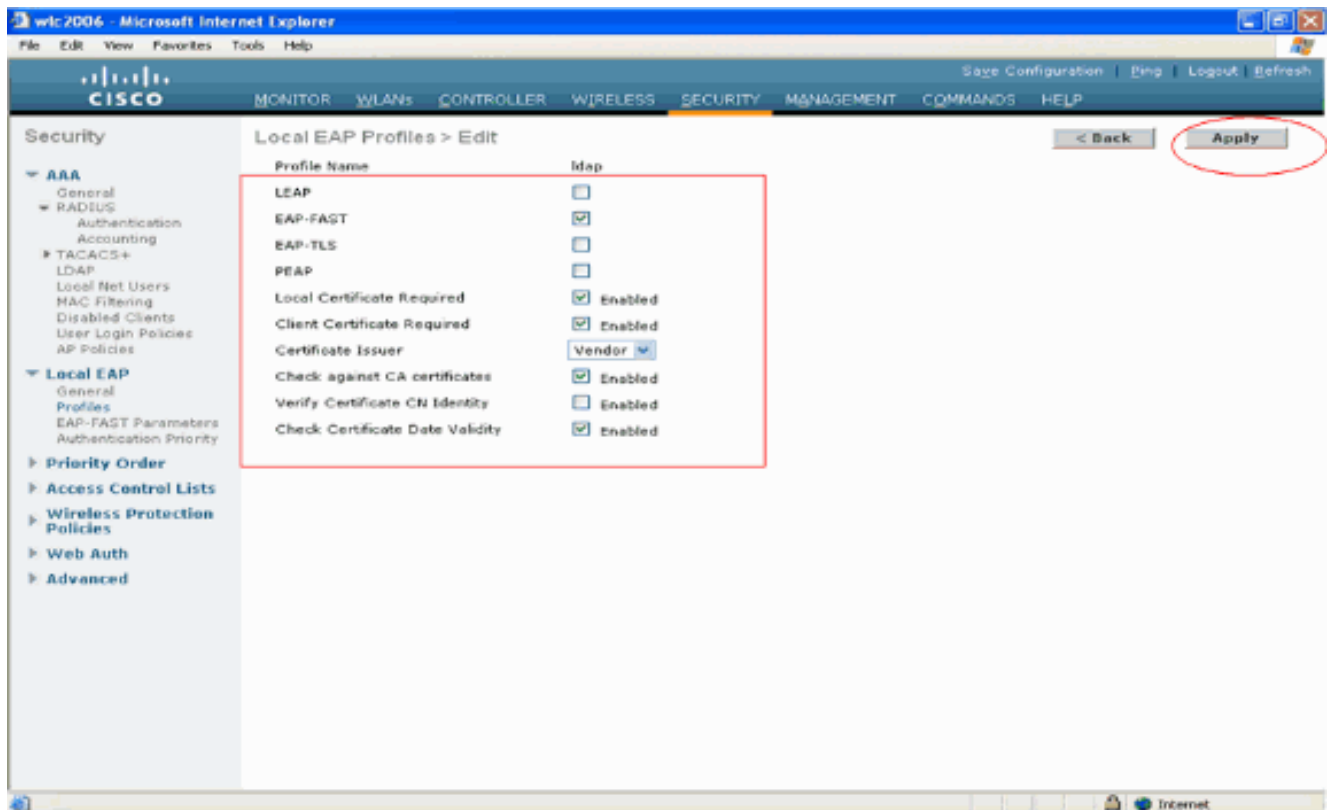
3. Clique em **New** para criar um novo perfil EAP local.
4. Configure um nome para este perfil e clique em **Apply**. Neste exemplo, o nome do perfil é **ldap**. Isso o leva aos perfis de EAP locais criados na WLC.



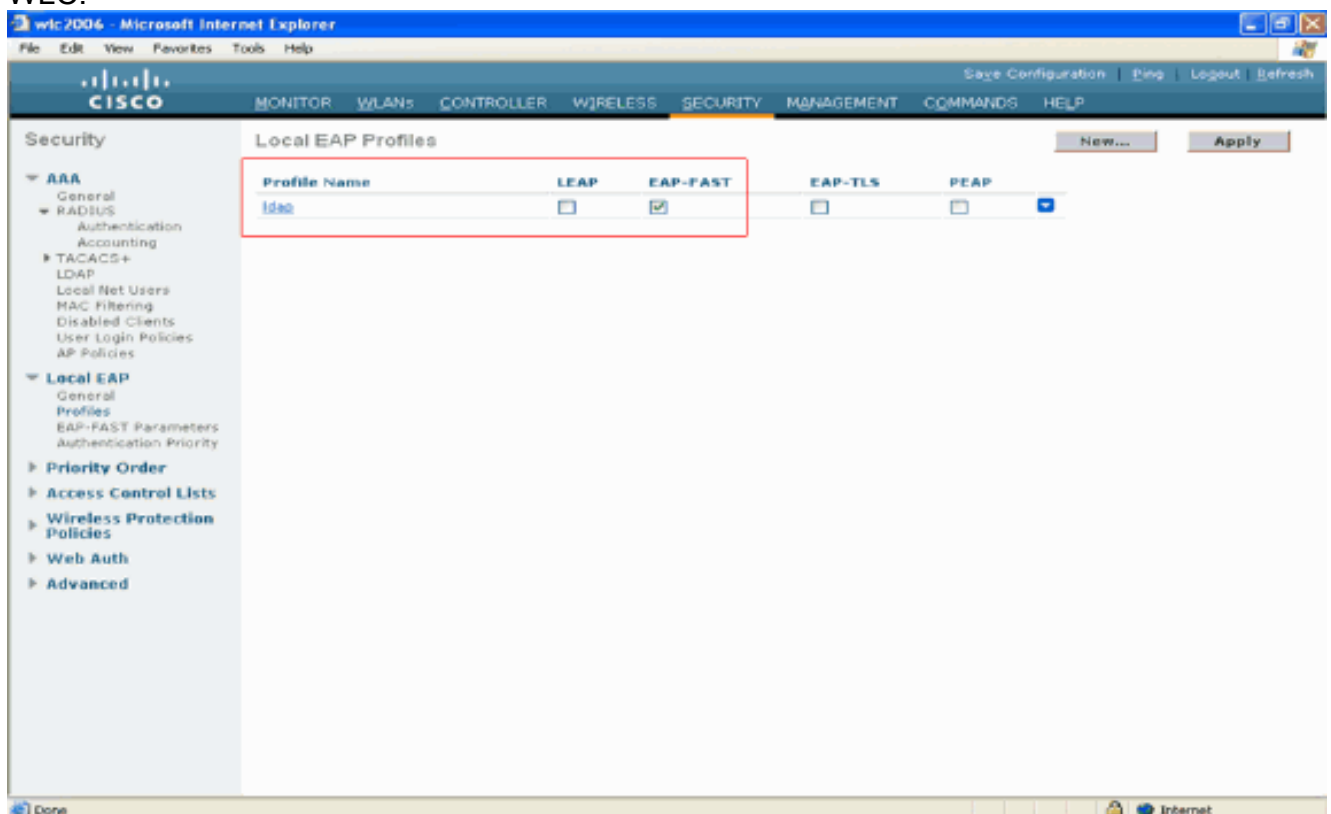
5. Clique no perfil **ldap** que acabou de ser criado, exibido no campo Nome do perfil da página Perfis EAP locais. Isso o levará para a página **Perfis EAP Locais > Editar**.



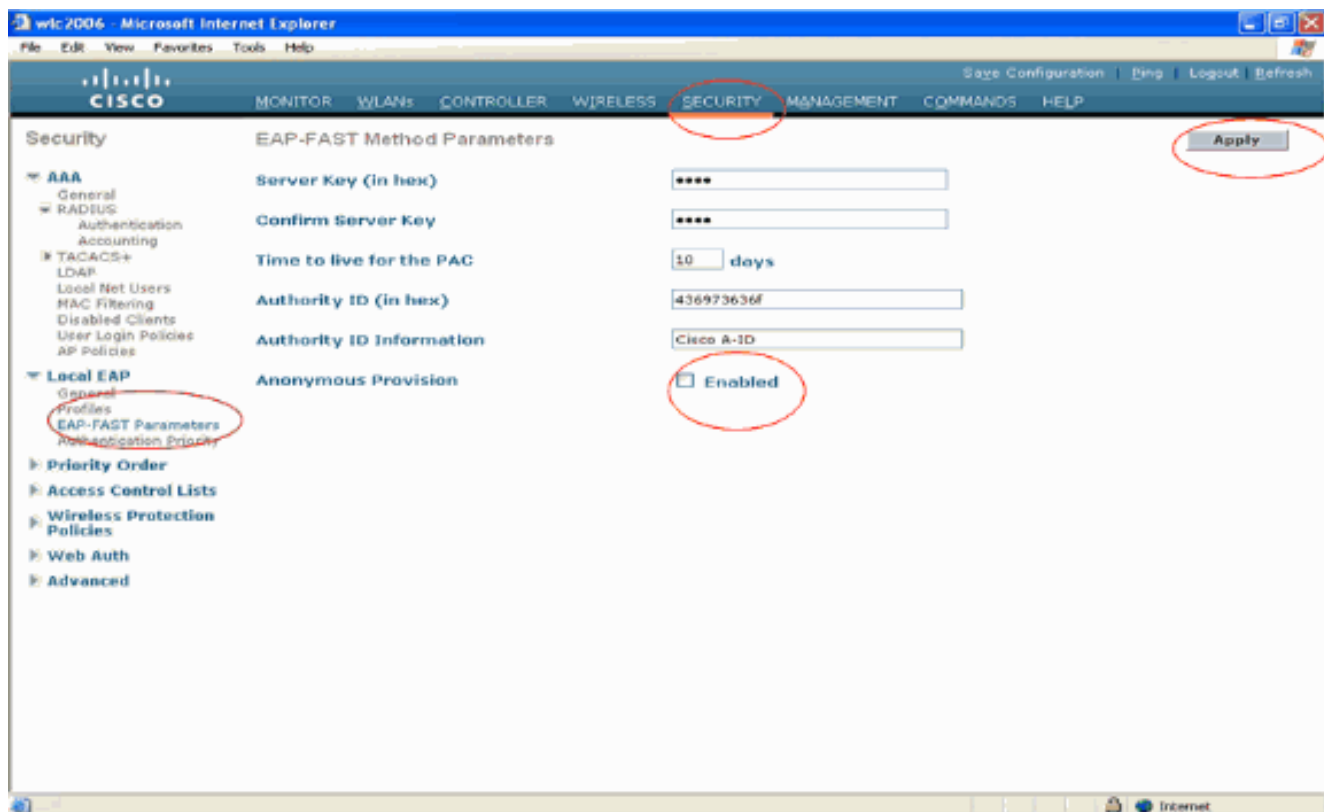
6. Configure os parâmetros específicos deste perfil na página **Perfis EAP Locais > Editar**. Escolha **EAP-FAST** como o método de autenticação EAP local. Ative as caixas de seleção ao lado de **Local Certificate Required** e **Client Certificate Required**. Escolha **Fornecedor** como Emissor do Certificado porque este documento usa um servidor de CA de terceiros. Habilite a caixa de seleção ao lado de **Verificar em relação aos certificados da autoridade de certificação** para permitir que o certificado de entrada do cliente seja validado em relação aos certificados da autoridade de certificação no controlador. Se você quiser que o nome comum (CN) no certificado de entrada seja validado em relação ao CN dos certificados de CA no controlador, marque a caixa de seleção **Verificar a identidade do CN do certificado**. A configuração padrão está desabilitada. Para permitir que o controlador verifique se o certificado do dispositivo de entrada ainda é válido e não expirou, marque a caixa de seleção **Verificar validade da data do certificado**. **Observação:** a validade da data do certificado é verificada em relação à hora UTC (GMT) atual configurada no controlador. O deslocamento de fuso horário é ignorado. Clique em **Apply**.



7. O perfil EAP Local com autenticação EAP-FAST agora é criado no WLC.



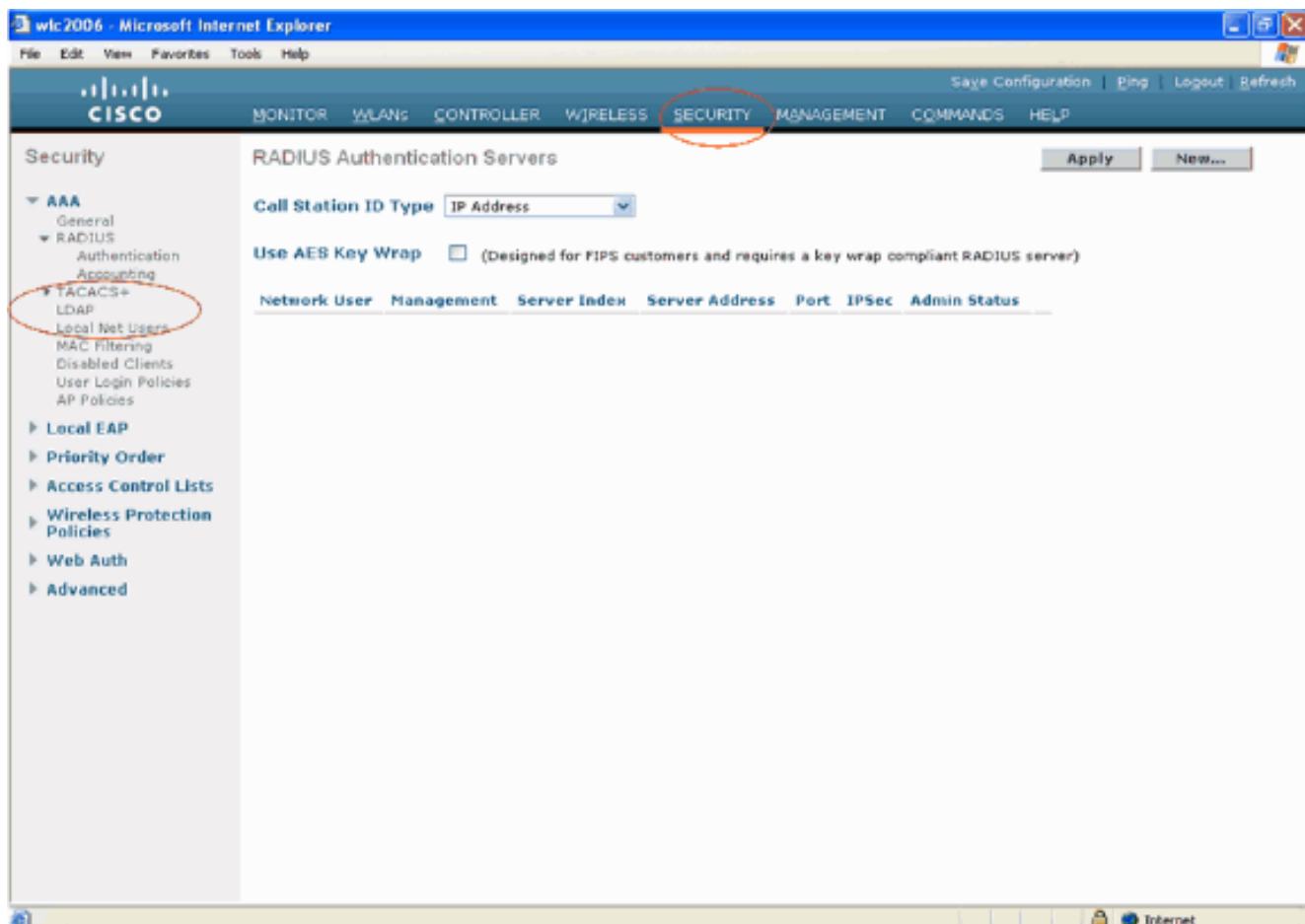
8. A próxima etapa é configurar parâmetros específicos de EAP-FAST no WLC. Na página Segurança da WLC, clique em **EAP Local > Parâmetros EAP-FAST** para ir para a página Parâmetros do método EAP-FAST. Desmarque a caixa de seleção **Provisão anônima** porque este exemplo explica EAP-FAST usando certificados. Deixe todos os outros parâmetros em seus padrões. Clique em **Apply**.



[Configurar a WLC com detalhes do servidor LDAP](#)

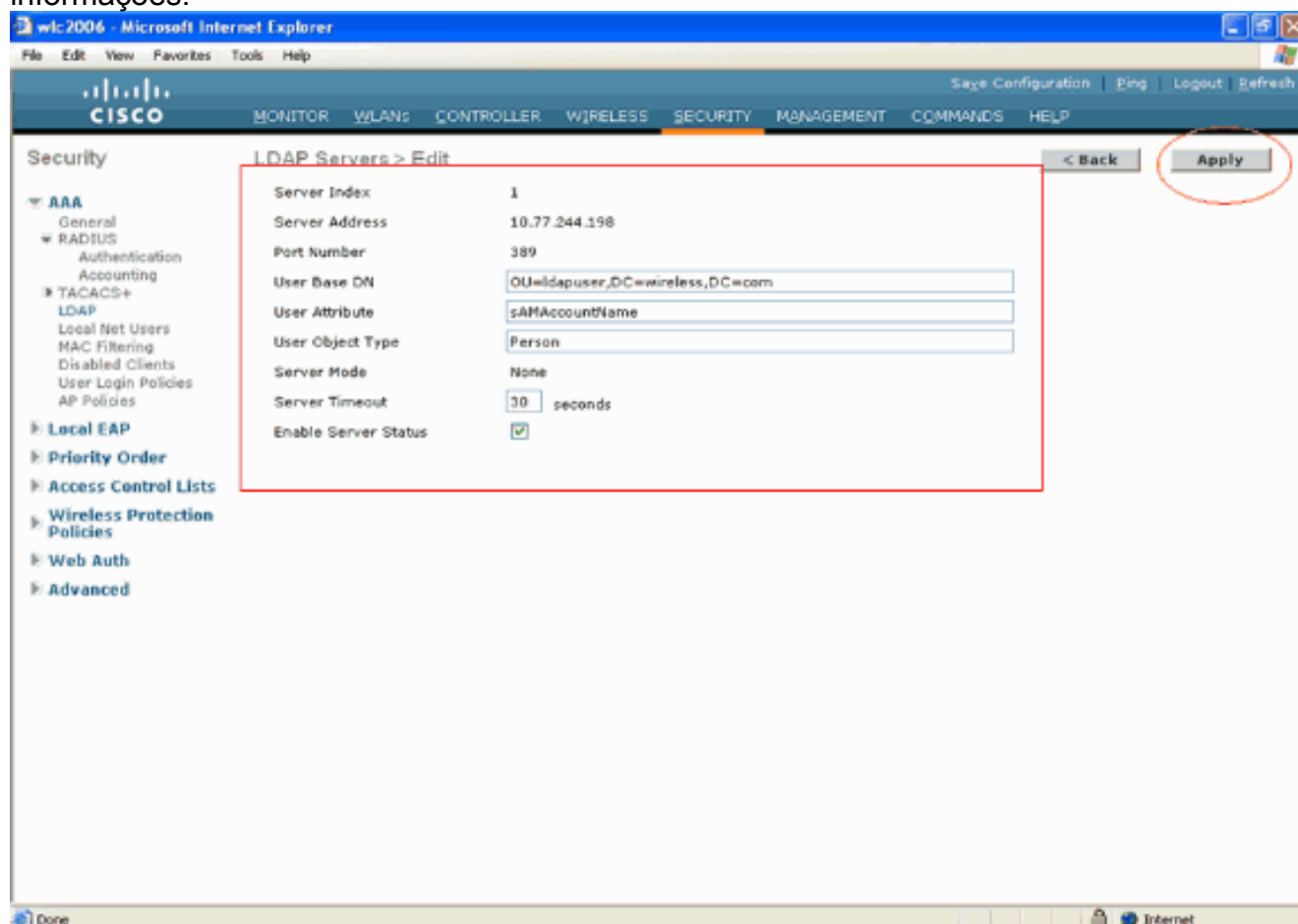
Agora que a WLC está configurada com o perfil EAP local e informações relacionadas, a próxima etapa é configurar a WLC com detalhes do servidor LDAP. Conclua estes passos no WLC:

1. Na página **Security** do WLC, selecione **AAA > LDAP** no painel de tarefas do lado esquerdo para ir para a página de configuração do servidor LDAP. Para adicionar um servidor LDAP, clique em **Novo**. A página LDAP Servers (Servidores LDAP) > New (Novo) é exibida.



2. Na página LDAP Servers Edit (Editar servidores LDAP), especifique os detalhes do servidor LDAP, como o endereço IP do servidor LDAP, o número da porta, o status Enable Server (Habilitar servidor) e assim por diante. Selecione um número na caixa suspensa Índice do servidor (prioridade) para especificar a ordem de prioridade deste servidor em relação a qualquer outro servidor LDAP configurado. É possível configurar até dezessete servidores. Se o controlador não puder acessar o primeiro servidor, ele tentará o segundo da lista e assim por diante. Digite o endereço IP do servidor LDAP no campo Endereço IP do servidor. Insira o número da porta TCP do servidor LDAP no campo **Port Number**. O intervalo válido é de 1 a 65535, e o valor padrão é 389. No campo User Base DN (Nome diferenciado da base de usuários), digite o nome diferenciado (DN) da subárvore do servidor LDAP que contém uma lista de todos os usuários. Por exemplo, ou=organizational unit, .ou=next organizational unit e o=corporation.com. Se a árvore contendo usuários for o DN base, digite o=corporation.com ou dc=corporation, dc=com. Neste exemplo, o usuário está localizado sob o **ldapuser** da Unidade Organizacional (OU) que, por sua vez, é criado como parte do domínio **Wireless.com**. O DN de base do usuário deve apontar o caminho completo onde as informações do usuário (credencial do usuário de acordo com o método de autenticação EAP-FAST) estão localizadas. Neste exemplo, o usuário está localizado sob o DN base OU=ldapuser, DC=Wireless, DC=com. Mais detalhes sobre OU, bem como a configuração do usuário, são explicados na seção [Criação de Usuários no Controlador de Domínio](#) deste documento. No campo User Attribute (Atributo de usuário), digite o nome do atributo no registro do usuário que contém o nome de usuário. No campo User Object Type (Tipo de objeto de usuário), insira o valor do atributo objectType do LDAP que identifica o registro como um usuário. Frequentemente, os registros de usuário têm diversos valores para o atributo objectType, sendo que alguns são exclusivos e outros são compartilhados com diversos tipos de objeto. **Observação:** Você pode obter o valor desses dois campos no servidor de diretório com o utilitário do navegador LDAP, que faz parte das ferramentas de

suporte do Windows 2003. Essa ferramenta do navegador LDAP da Microsoft denomina-se LDP. Com a ajuda dessa ferramenta, você pode conhecer os campos DN base do usuário, Atributo do usuário e Tipo de objeto do usuário desse usuário específico. Informações detalhadas sobre o uso do LDP para conhecer esses atributos específicos do Usuário são discutidas na seção [Uso do LDP para Identificar os Atributos do Usuário](#) deste documento. Escolha **Secure** na caixa suspensa Server Mode se quiser que todas as transações LDAP usem um túnel TLS seguro. Caso contrário, escolha **Nenhum**, que é a configuração padrão. No campo Limite de tempo do servidor, digite o número de segundos entre as retransmissões. O intervalo válido é de 2 a 30 segundos, e o valor padrão é de 2 segundos. Marque a caixa de seleção **Habilitar status do servidor** para habilitar este servidor LDAP ou desmarque-a para desabilitar. O valor padrão é desativado. Clique em **Apply (Aplicar)** para confirmar as alterações. Aqui está um exemplo já configurado com estas informações:



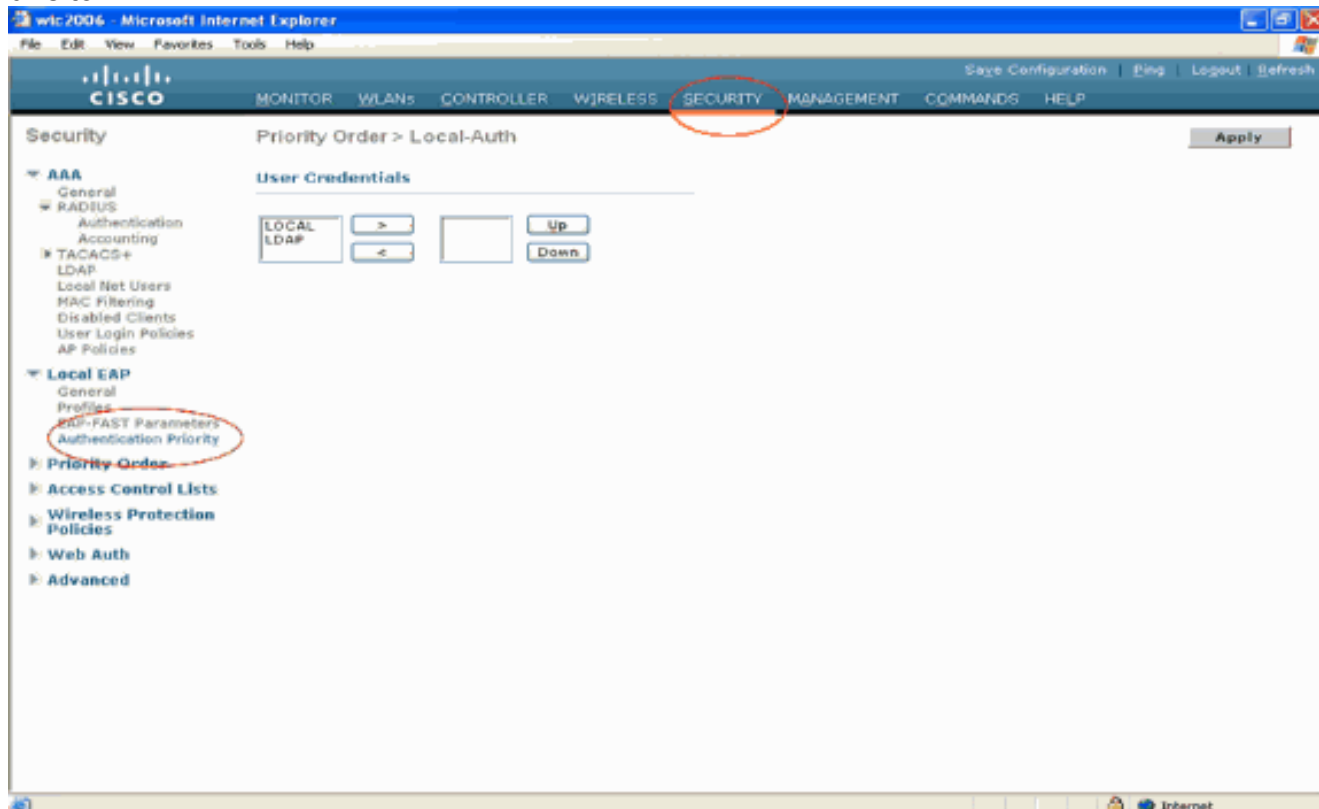
Agora que os detalhes sobre o servidor LDAP estão configurados no WLC, a próxima etapa é configurar o LDAP como o banco de dados de back-end prioritário para que o WLC primeiro procure o banco de dados LDAP para as credenciais do usuário em vez de qualquer outro banco de dados.

[Configurar LDAP como o banco de dados back-end de prioridade](#)

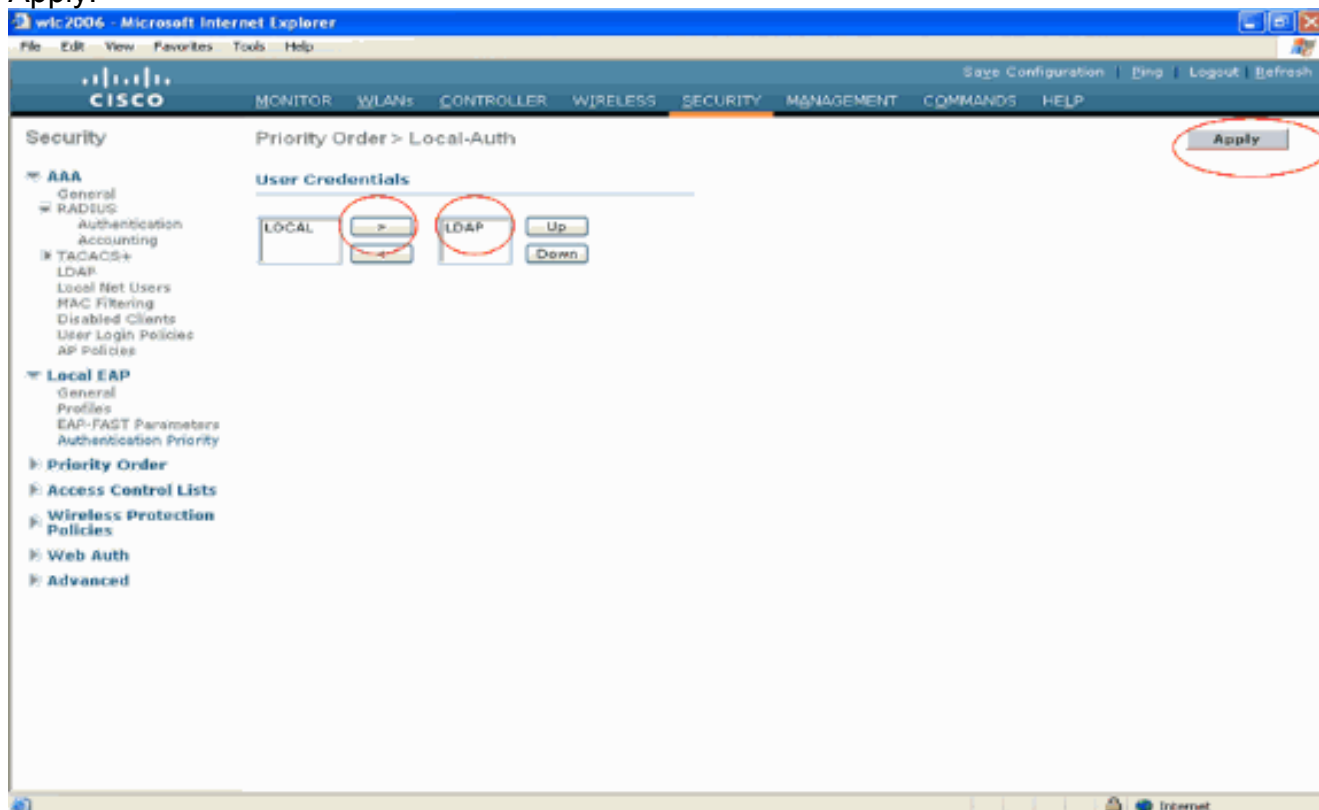
Conclua estes passos no WLC para configurar o LDAP como o banco de dados de back-end de prioridade:

1. Na página Segurança, clique em **EAP Local > Prioridade de Autenticação**. Na página Ordem de prioridade > Autenticação local, você pode encontrar dois bancos de dados (Local e LDAP) que podem armazenar as credenciais do usuário. Para tornar o LDAP o banco de

dados de prioridade, escolha **LDAP** na caixa de credenciais do usuário do lado esquerdo e clique no botão > para mover o LDAP para a caixa de ordem de prioridade no lado direito.



2. Este exemplo ilustra claramente que o LDAP é escolhido na caixa do lado esquerdo e o botão > é selecionado. Como resultado, o LDAP é movido para a caixa no lado direito que decide a prioridade. O banco de dados LDAP é escolhido como o banco de dados Authentication-priority. Clique em Apply.



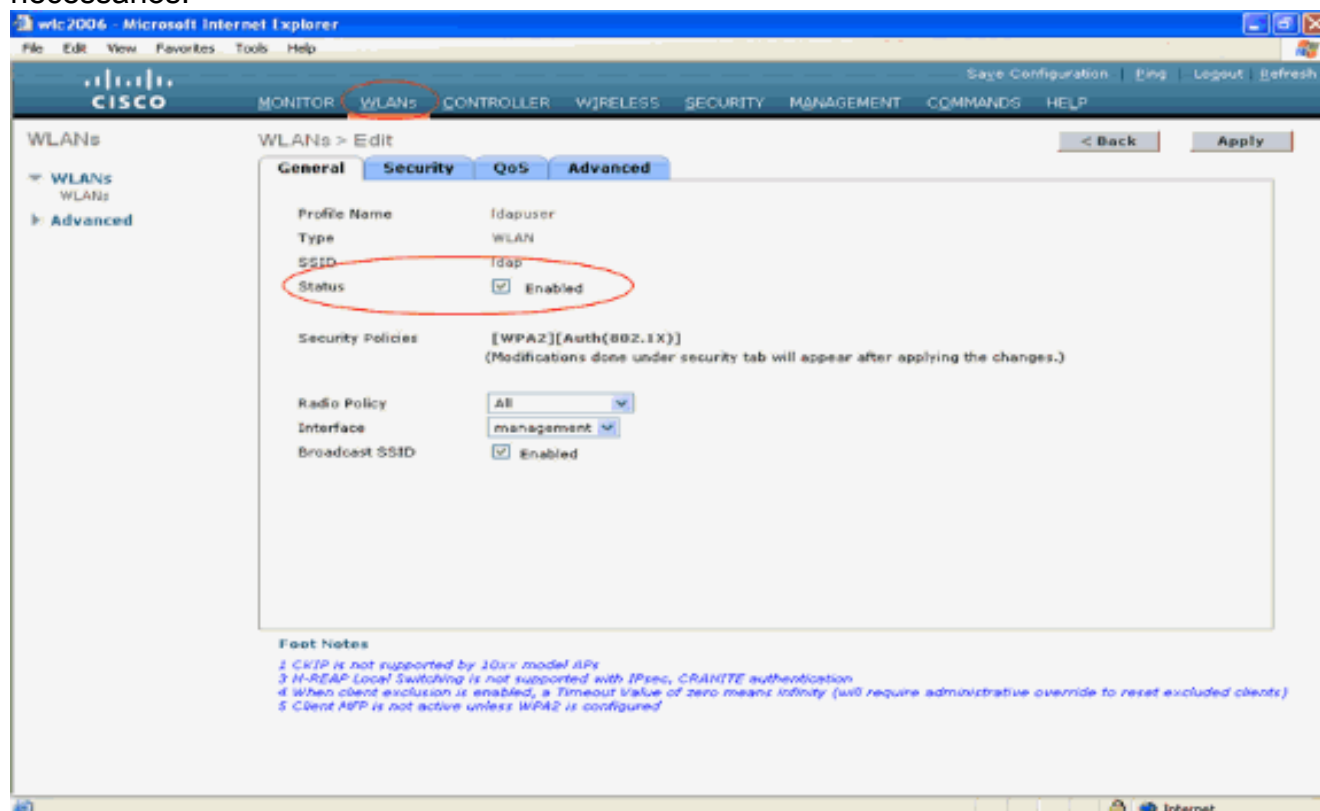
Observação: Se LDAP e LOCAL aparecerem na caixa Credenciais do Usuário à direita com

LDAP na parte superior e LOCAL na parte inferior, o EAP Local tentará autenticar clientes usando o banco de dados back-end LDAP e efetuará failover para o banco de dados do usuário local se os servidores LDAP não estiverem acessíveis. Se o usuário não for encontrado, a tentativa de autenticação será rejeitada. Se LOCAL estiver na parte superior, o EAP local tentará se autenticar usando somente o banco de dados de usuário local. Não ocorre failover para o banco de dados back-end LDAP.

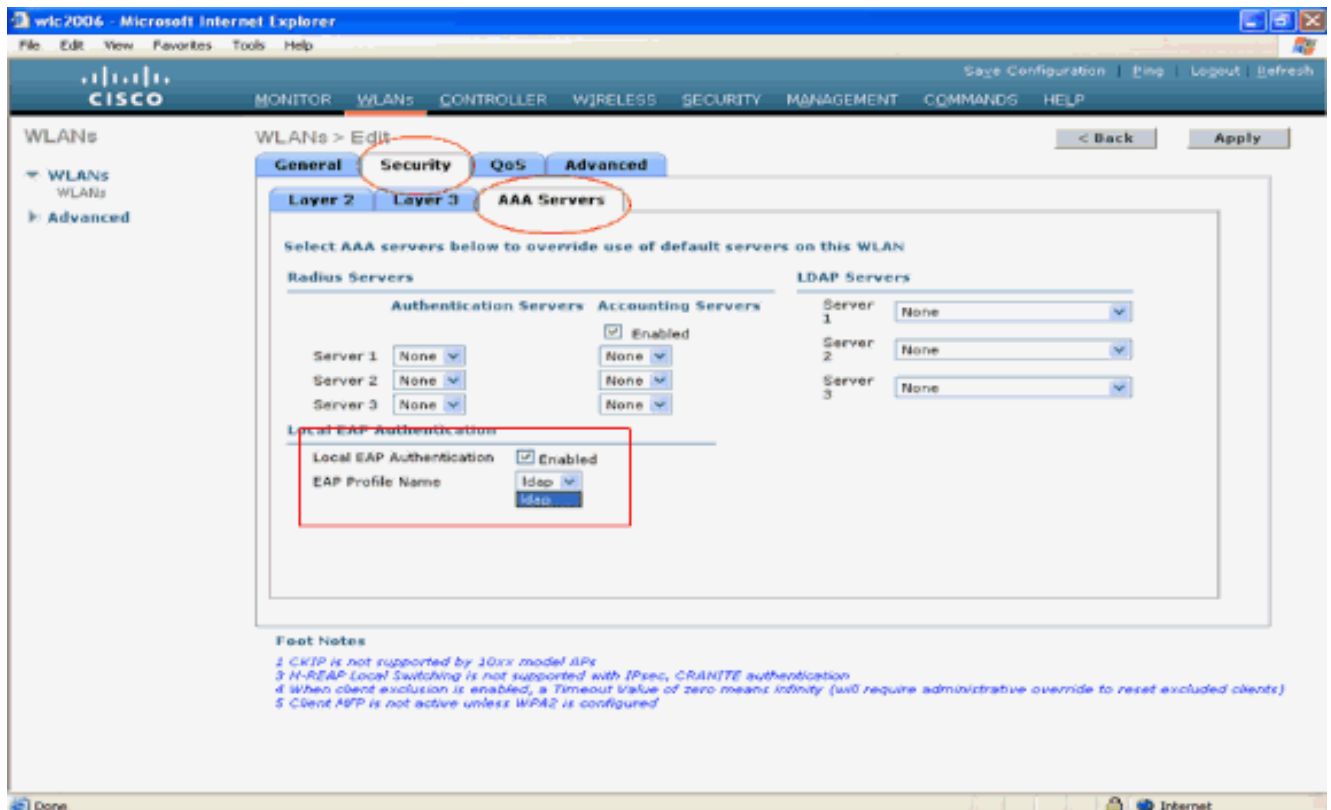
Configurar a WLAN na WLC com autenticação EAP local

A última etapa na WLC é configurar uma WLAN que usa EAP local como seu método de autenticação com LDAP como seu banco de dados de back-end. Execute estas etapas:

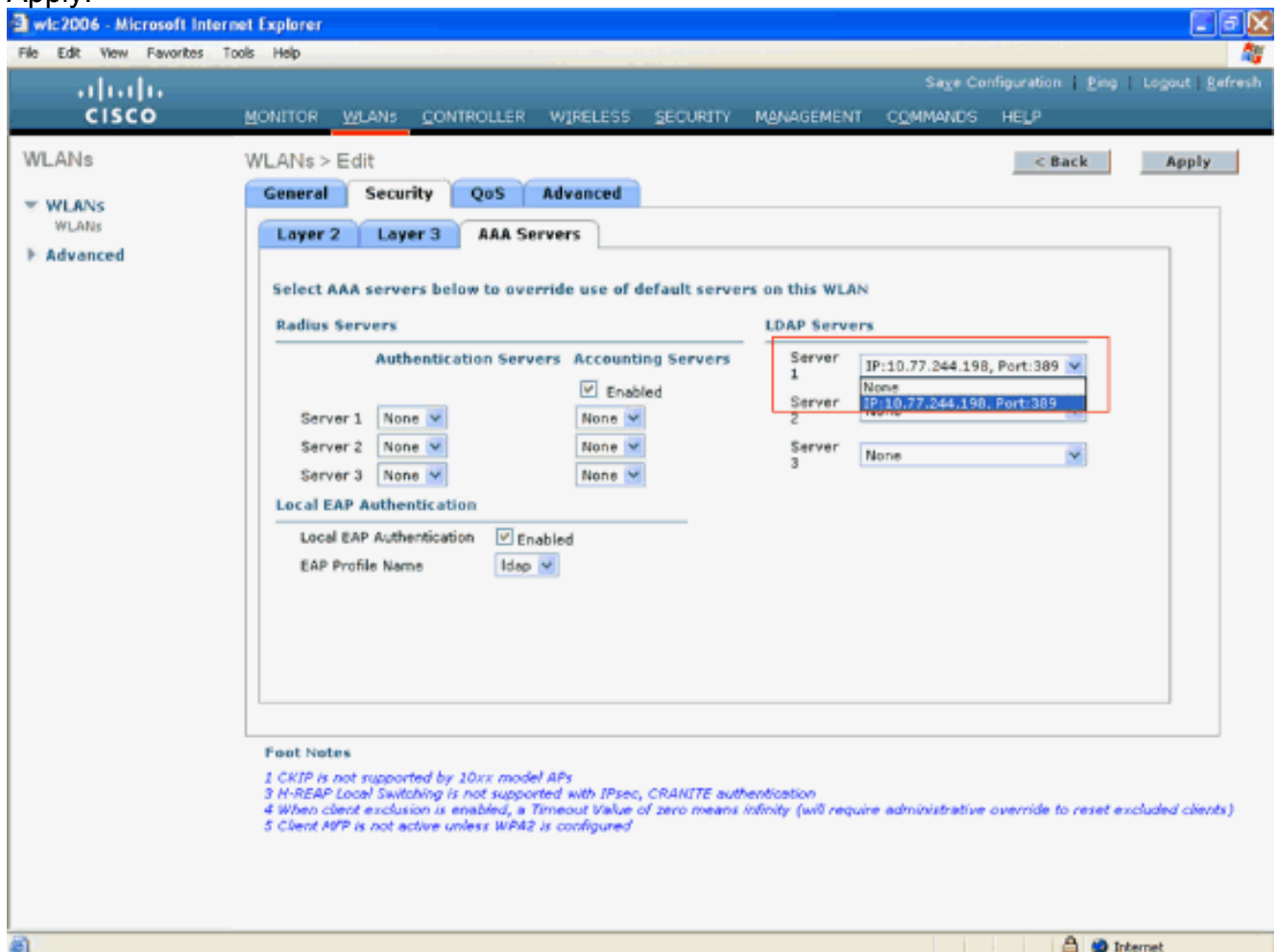
1. No menu principal da controladora, clique em **WLANs** para ir para a página de configuração de WLANs. Na página WLANs, clique em **New** para criar uma nova WLAN. Este exemplo cria um novo **ldap** de WLAN. Clique em **Apply**. A próxima etapa é configurar os parâmetros da WLAN na página WLANs > Edit .
2. Na página de edição da WLAN, habilite o status desta WLAN. Configure todos os outros parâmetros necessários.



3. Clique em **Security** para configurar os parâmetros relacionados à segurança para esta WLAN. Este exemplo usa a segurança de Camada 2 como 802.1x com WEP dinâmico de 104 bits. **Observação:** este documento usa 802.1x com WEP dinâmico como exemplo. É recomendável usar métodos de autenticação mais seguros, como WPA/ WPA2.
4. Na página de configuração WLAN Security, clique na guia **AAA servers**. Na página de servidores AAA, ative o método Local EAP Authentication e escolha **ldap** na caixa suspensa que corresponde ao parâmetro EAP Profile Name. Este é o perfil EAP Local criado neste exemplo.

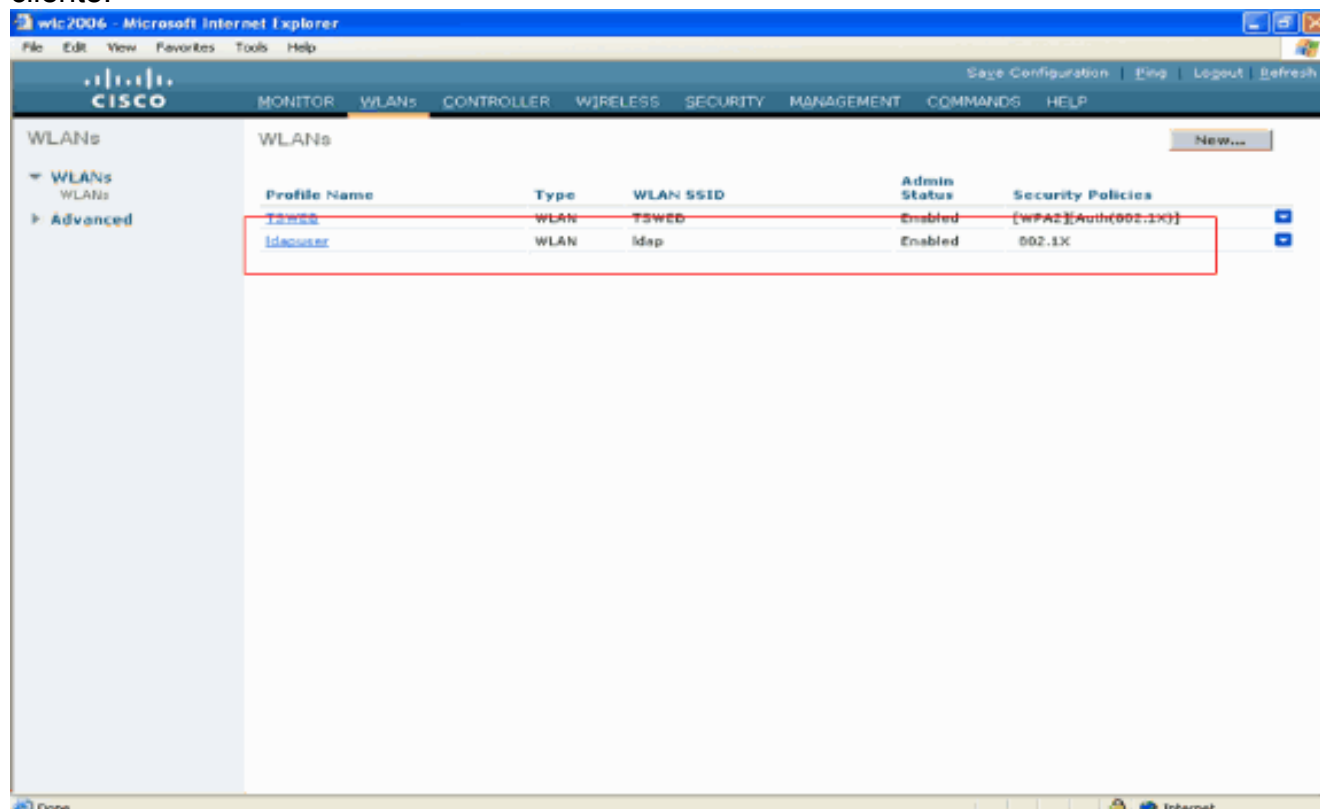


5. Escolha o servidor LDAP (que foi configurado anteriormente na WLC) na caixa suspensa. Certifique-se de que o servidor LDAP seja alcançável a partir do WLC. Clique em Apply.



6. O novo Idapde WLAN foi configurado no WLC. Esta WLAN autentica clientes com Autenticação EAP Local (EAP-FAST neste caso) e consulta um banco de dados back-end

LDAP para validação de credenciais de cliente.



[Configurar servidor LDAP](#)

Agora que o EAP local está configurado na WLC, a próxima etapa é configurar o servidor LDAP, que serve como um banco de dados de back-end para autenticar os clientes sem fio após a validação bem-sucedida do certificado.

A primeira etapa na configuração do servidor LDAP é criar um banco de dados de usuário no servidor LDAP para que o WLC possa consultar esse banco de dados para autenticar o usuário.

[Criando usuários no controlador de domínio](#)

Neste exemplo, um novo **ldapuser** da OU é criado e o usuário **user2** é criado nessa OU. Ao configurar esse usuário para acesso LDAP, a WLC pode consultar esse banco de dados LDAP para autenticação de usuário.

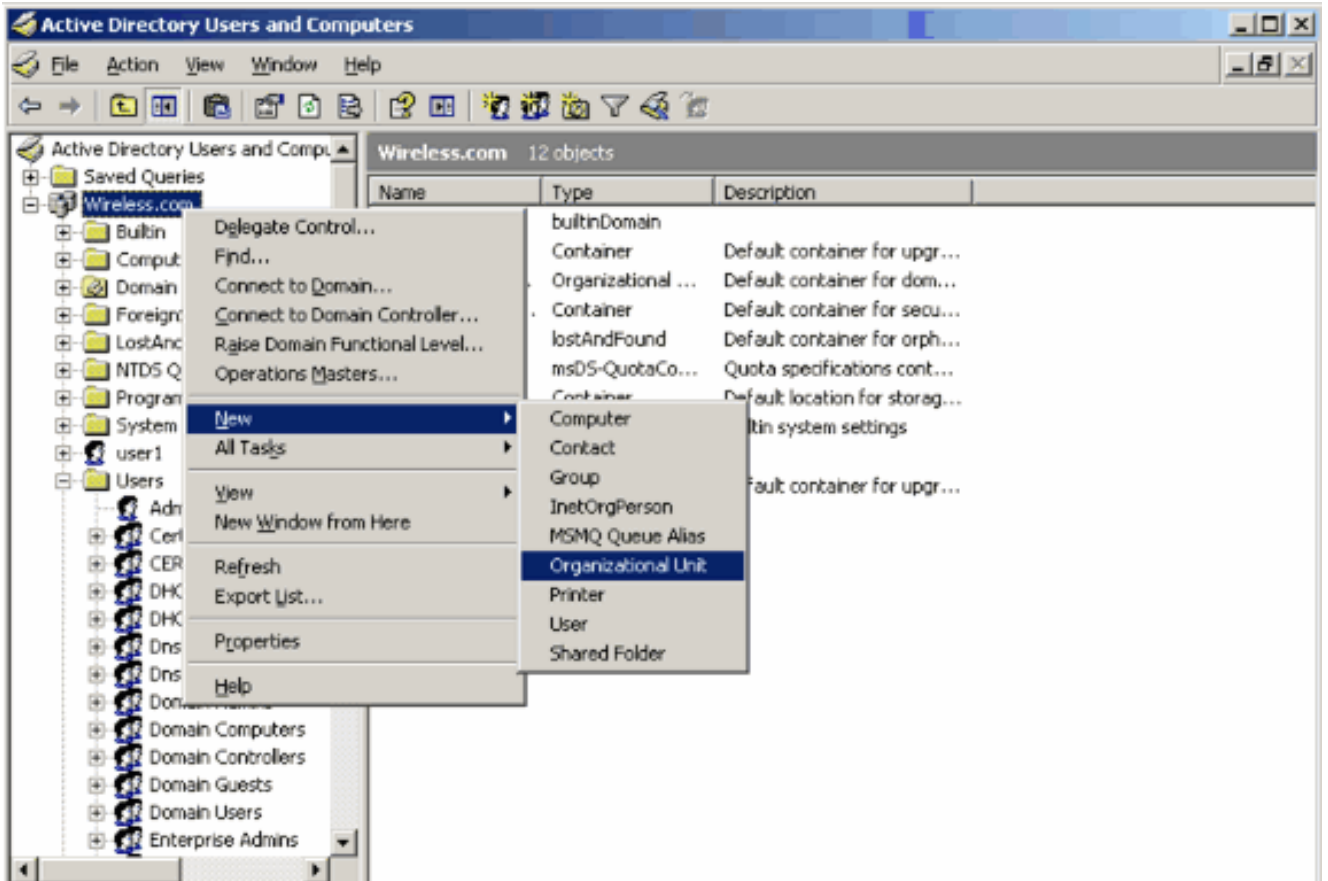
O domínio usado neste exemplo é **wireless.com**.

[Criar um banco de dados de usuário em uma UO](#)

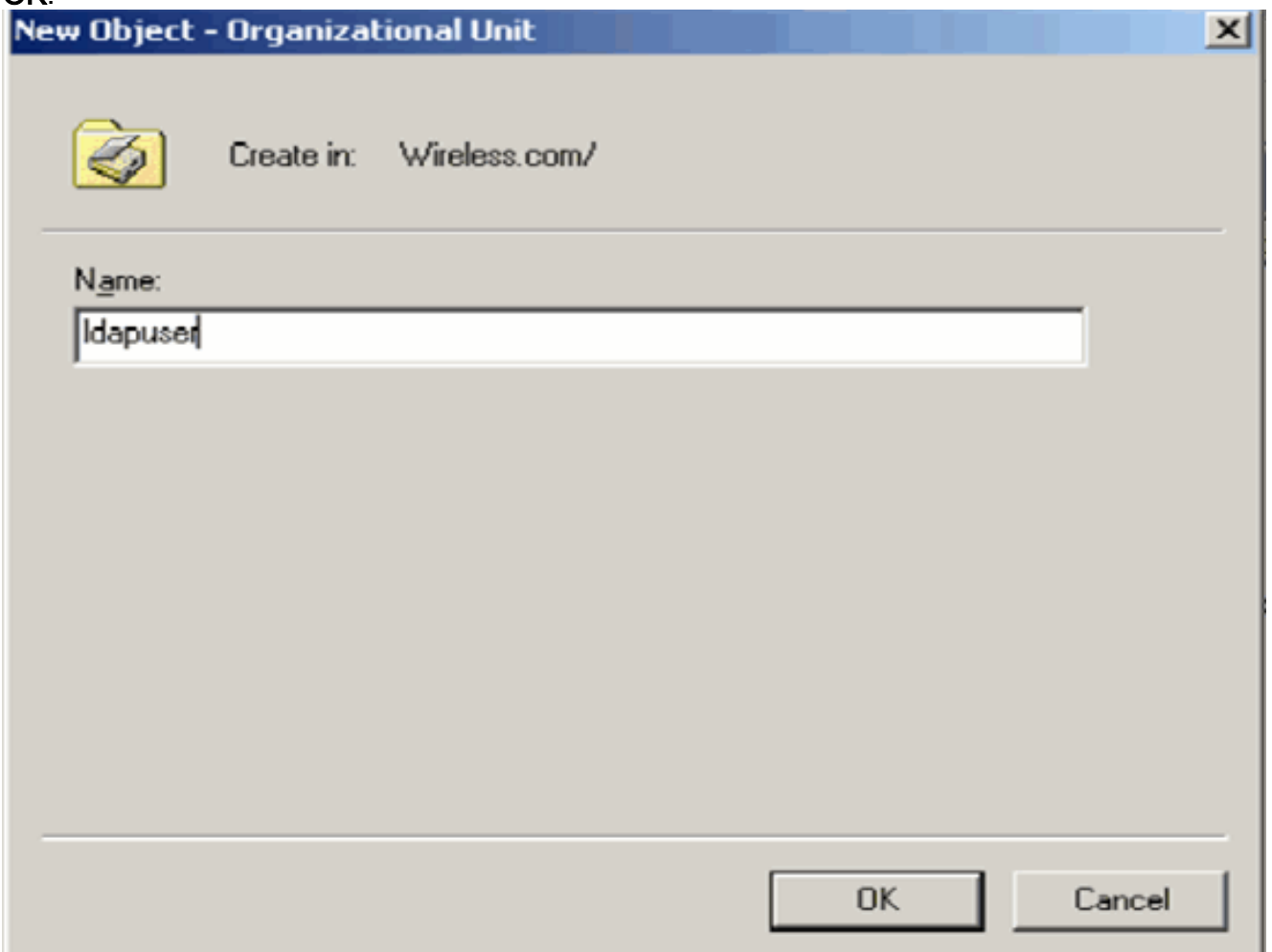
Esta seção explica como criar uma nova UO no domínio e criar um novo usuário nessa UO.

1. No controlador de domínio, clique em **Iniciar > Programas > Ferramentas Administrativas > Usuários e Computadores do Ative Directory** para iniciar o console de gerenciamento **Usuários e Computadores do Ative Directory**.
2. Clique com o botão direito do mouse no nome de domínio (**wireless.com**, neste exemplo) e selecione **New > Organizational Unit** no menu de contexto para criar uma nova

OU.

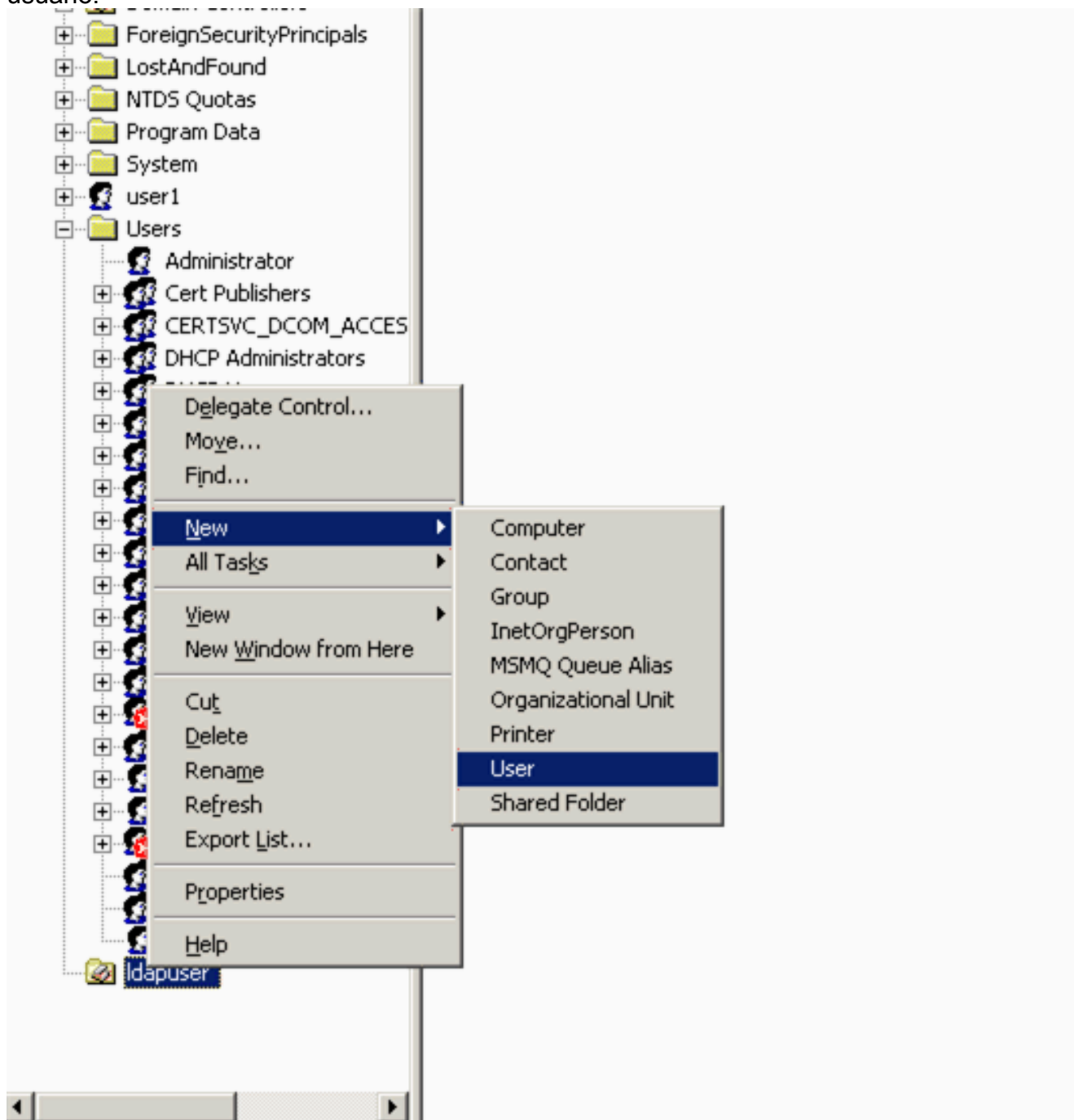


3. Atribua um nome a esta OU e clique em OK.



Agora que o novo usuário **ldapuser** da OU é criado no servidor LDAP, a próxima etapa é criar o usuário **user2** nessa OU. Para isso, siga estas etapas:

1. Clique com o botão direito do mouse na nova OU criada. Selecione **New > User** nos menus de contexto resultantes para criar um novo usuário.



2. Na página Configuração do usuário, preencha os campos obrigatórios conforme mostrado neste exemplo. Este exemplo tem **user2** como o nome de logon do usuário. Este é o nome de usuário que será verificado no banco de dados LDAP para autenticação do cliente. Este exemplo usa **abcd** como o nome e o sobrenome. Clique em Next.

New Object - User

Create in: Wireless.com/ldapuser

First name: abcd Initials: []

Last name: []

Full name: abcd

User logon name: user2 @Wireless.com

User logon name (pre-Windows 2000): WIRELESS\user2

< Back Next > Cancel

3. Digite uma senha e confirme-a. Selecione a opção **A senha nunca expira** e clique em **Avançar**.

New Object - User

Create in: Wireless.com/ldapuser

Password: []

Confirm password: []

User must change password at next logon

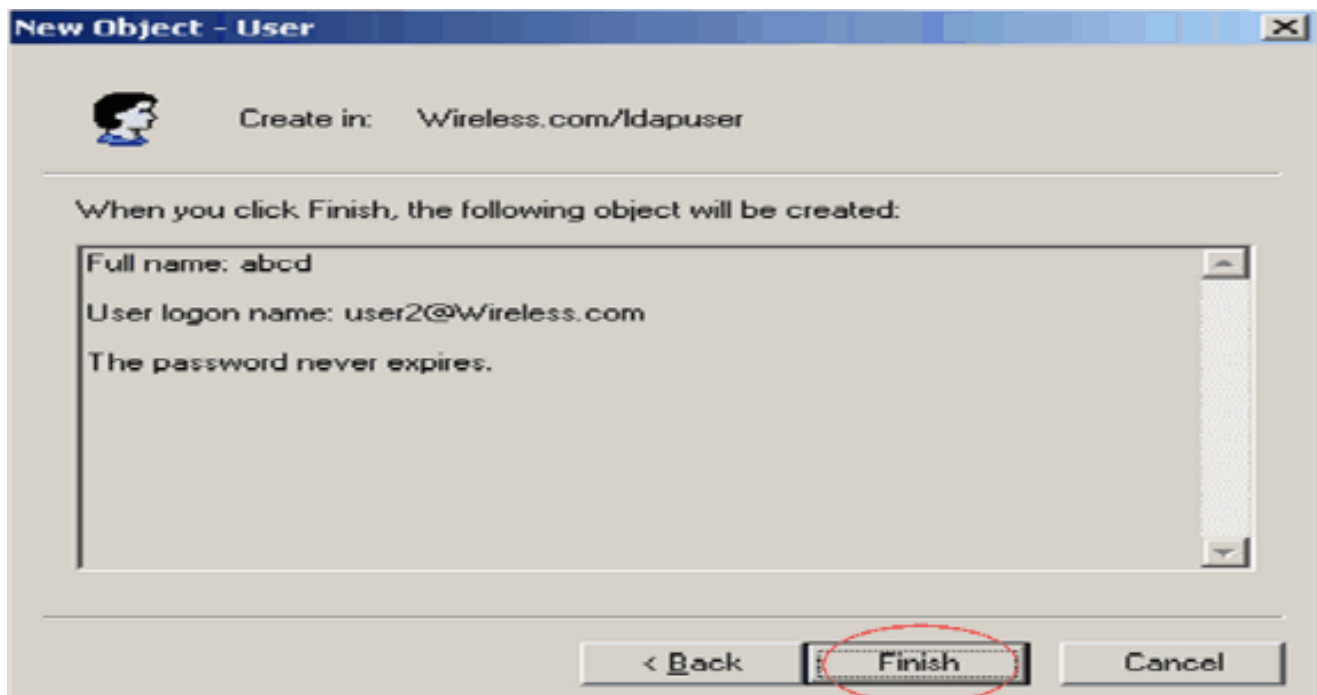
User cannot change password

Password never expires

Account is disabled

< Back Next > Cancel

4. Clique em Finish. Um novo usuário **user2** é criado sob o OU **ldapuser**. As credenciais do usuário são: nome de usuário: **user2** senha: **Laptop123**



Agora que o usuário em uma OU é criado, a próxima etapa é configurar esse usuário para acesso LDAP.

[Configurar o usuário para acesso ao LDAP](#)

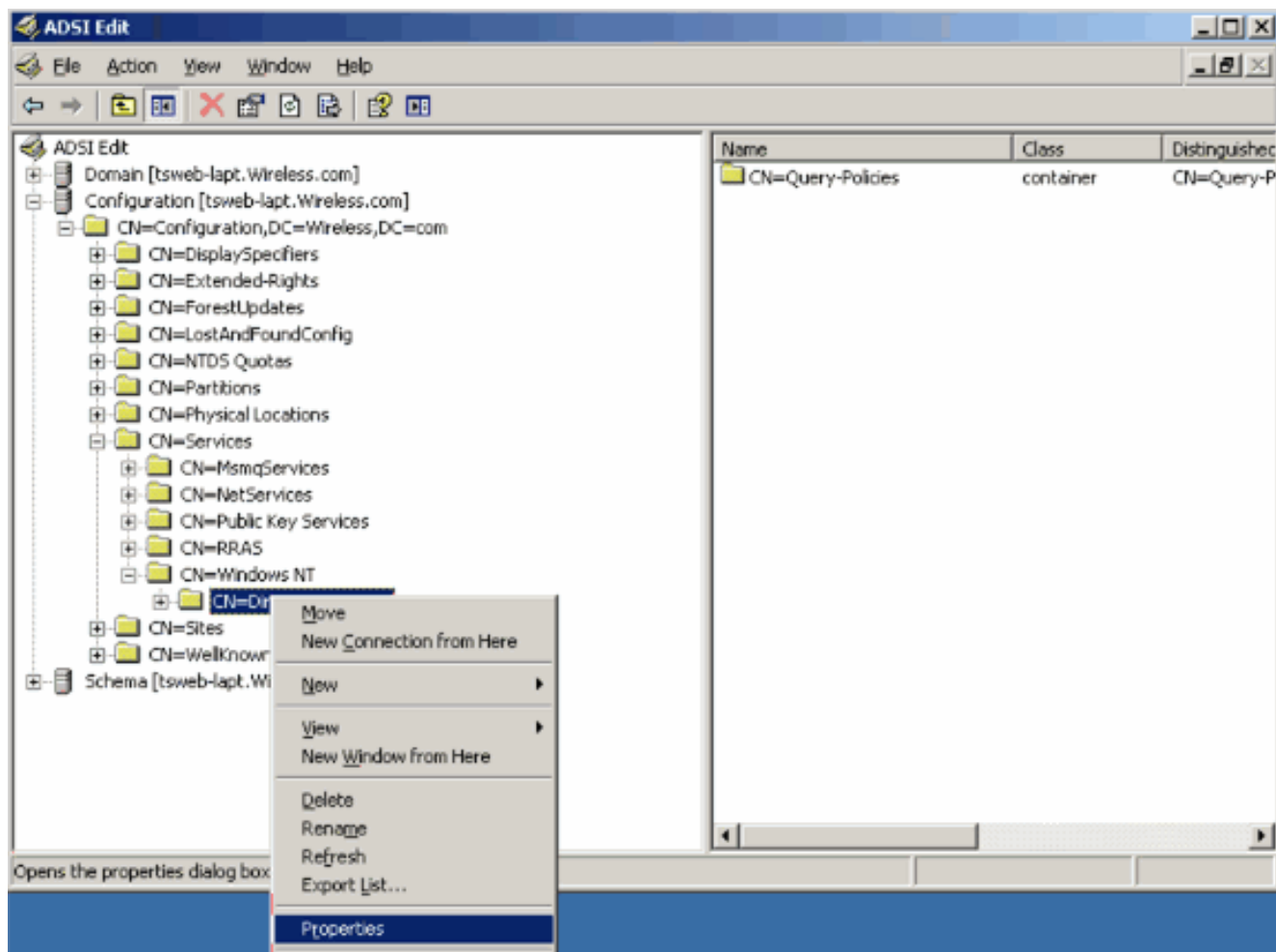
Execute as etapas nesta seção para configurar um usuário para acesso LDAP.

[Habilitar Recurso de Associação Anônima no Windows 2003 Server](#)

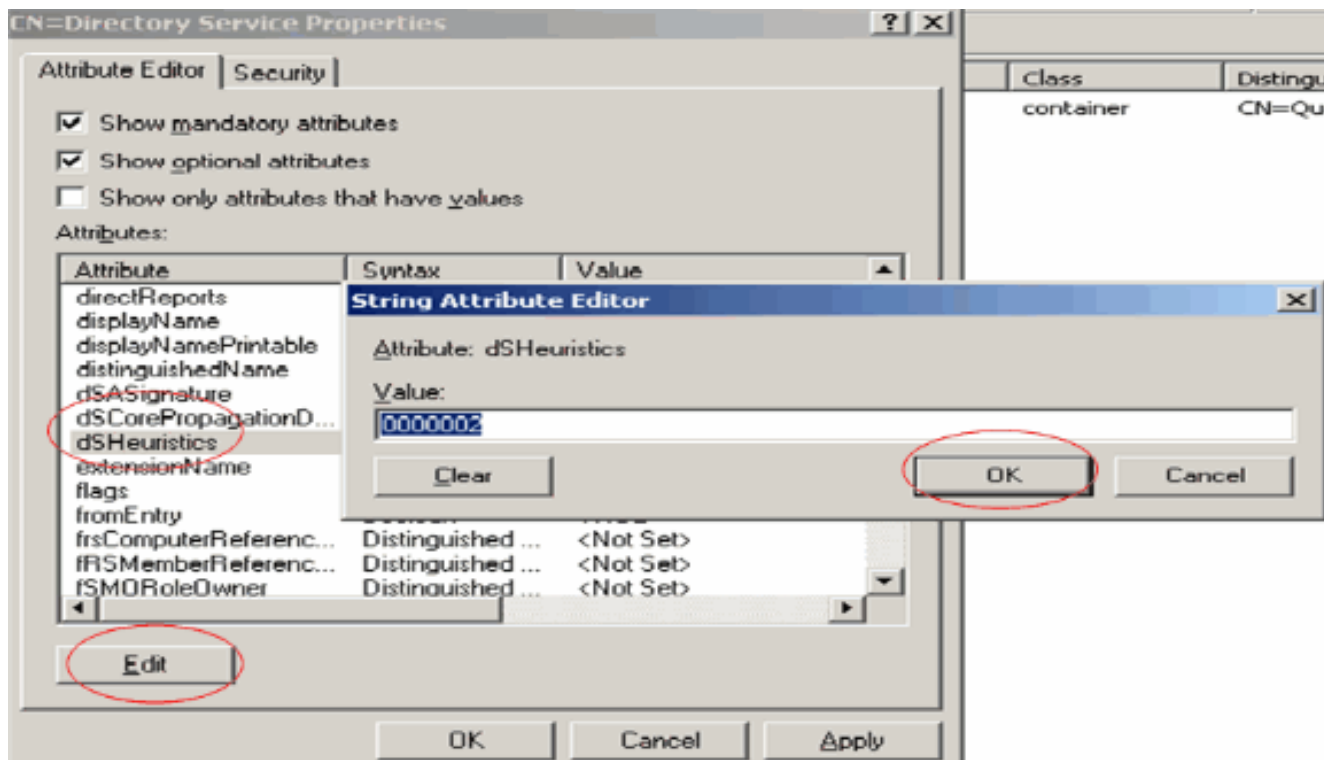
Para que aplicativos de terceiros acessem o Windows 2003 AD no LDAP, o recurso de Associação Anônima deve ser habilitado no Windows 2003. Por padrão, operações anônimas LDAP não são permitidas nos controladores de domínio do Windows 2003.

Execute estas etapas para habilitar o recurso de Associação Anônima:

1. Inicie a ferramenta **ADSI Edit** no local Start > Run > Type: **ADSI Edit.msc**. Esta ferramenta faz parte das ferramentas de suporte do Windows 2003.
2. Na janela ADSI Edit, expanda o domínio Raiz (Configuração [tsweb-lapt.Wireless.com]). Expanda **CN=Services > CN=Windows NT > CN=Directory Service**. Clique com o botão direito do mouse no contêiner **CN=Directory Service** e selecione **properties** no menu de contexto.



3. Na janela **CN=Directory Service Properties**, clique no atributo **dsHeuristics** no campo **Attribute** e escolha **Edit**. Na janela **Editor de atributos de string** deste atributo, digite o valor **0000002** e clique em **Aplicar** e **OK**. O recurso Associação Anônima está habilitado no servidor Windows 2003. **Observação:** o último (sétimo) caractere é aquele que controla a maneira como você pode se vincular ao serviço LDAP. "0" ou nenhum sétimo caractere significa que as operações LDAP anônimas estão desativadas. **A definição do sétimo caractere como "2" habilita o recurso de Associação Anônima.**

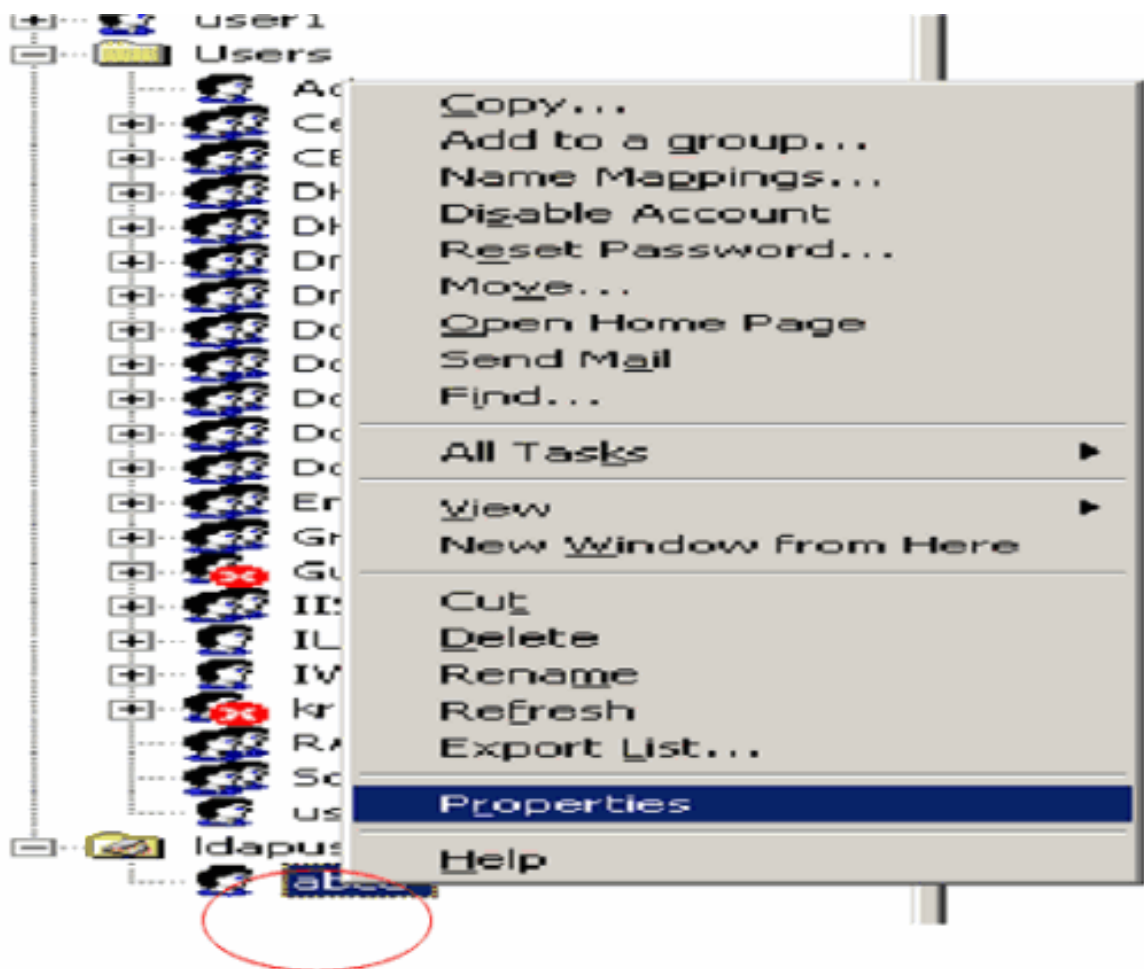


Observação: Se este atributo já contiver um valor, certifique-se de alterar somente o sétimo caractere da esquerda. Este é o único caractere que precisa ser alterado para habilitar associações anônimas. Por exemplo, se o valor atual for "0010000", você precisará alterá-lo para "0010002". Se o valor atual for menor que sete caracteres, você precisará colocar zeros nos locais não usados: "001" se tornará "0010002".

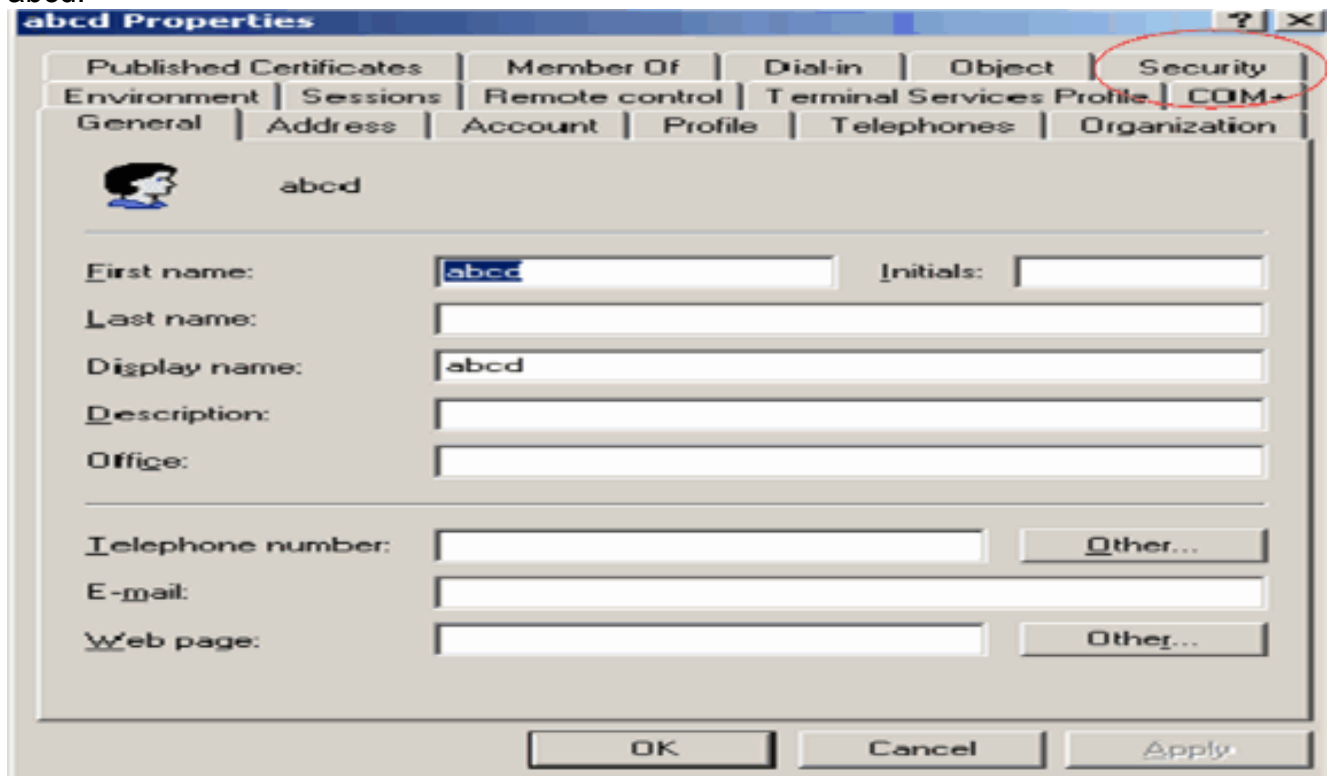
Concedendo Acesso a LOGON ANÔNIMO ao Usuário "user2"

A próxima etapa é conceder **LOGON ANÔNIMO** ao usuário **user2**. Siga estas etapas para realizar essa ação:

1. Abra **Usuários e computadores do Active Directory**.
2. Verifique se **View Advanced Features** está marcado.
3. Navegue até o usuário **user2** e clique com o botão direito do mouse nele. Selecione **Properties** no menu de contexto. Esse usuário é identificado com o nome "abcd".

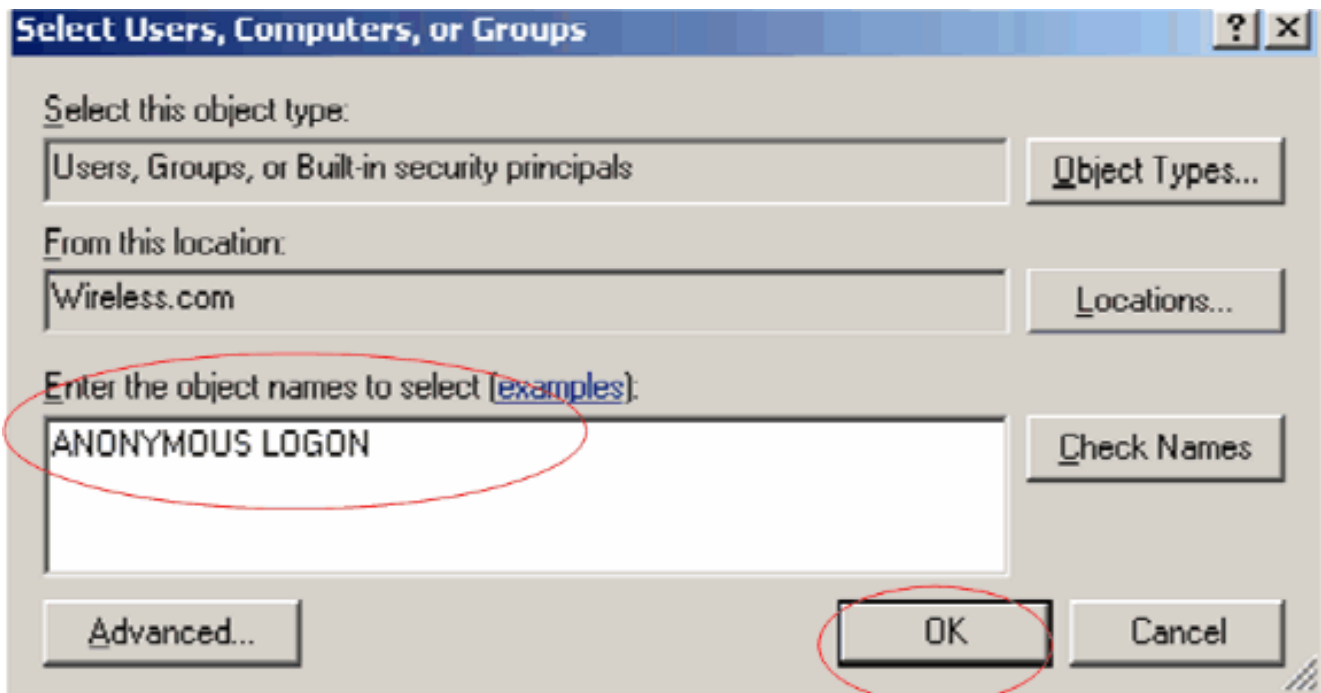


4. Vá para **Segurança** na janela Propriedades abcd.

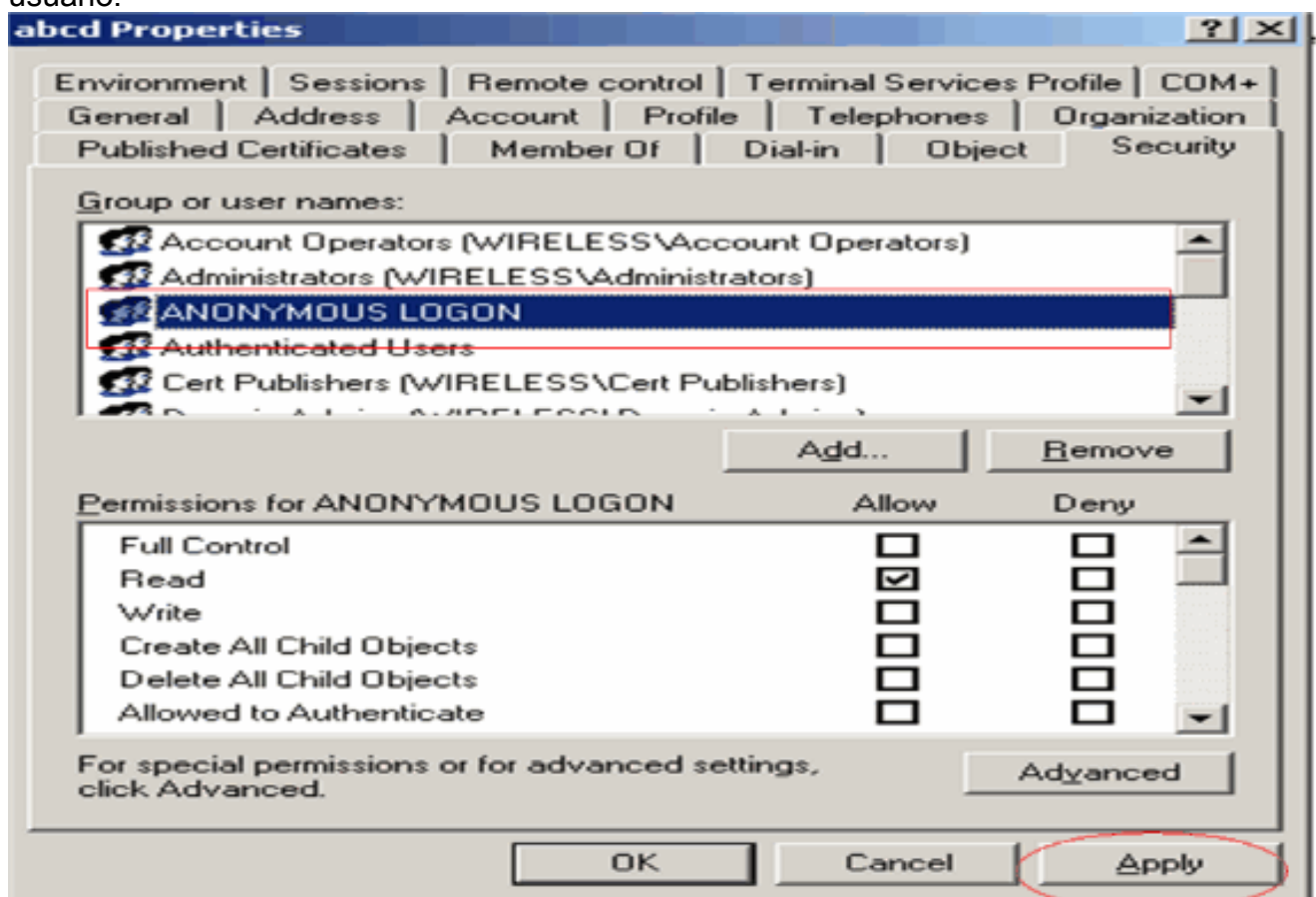


5. Clique em **Adicionar** na janela resultante.

6. Insira **ANONYMOUS LOGON** na caixa **Enter the object names to select** e confirme a caixa de diálogo.



7. Na ACL, você observará que o **LOGON ANÔNIMO** tem acesso a alguns conjuntos de propriedades do usuário. Click **OK**. O acesso ao LOGON ANÔNIMO é concedido a este usuário.

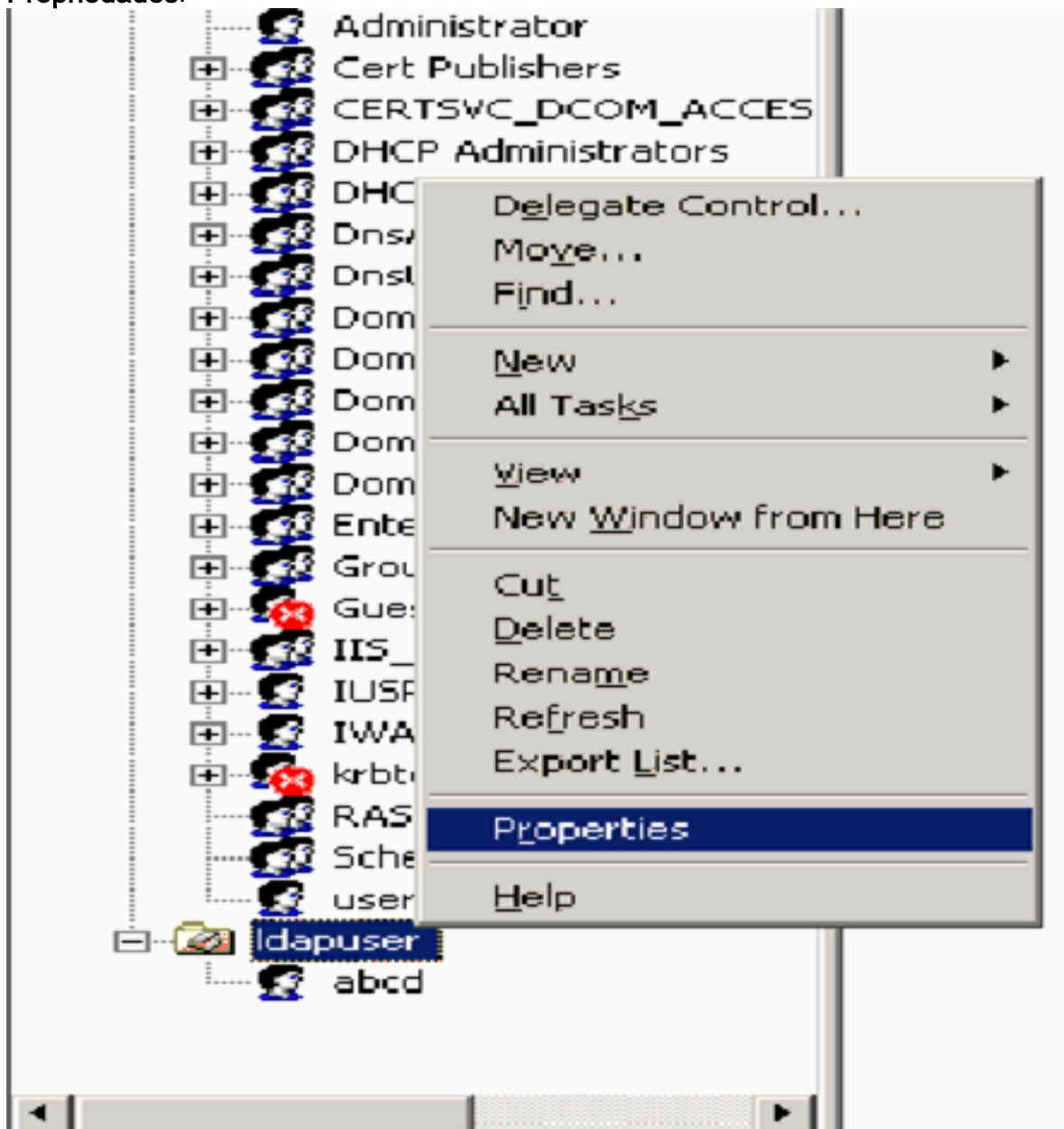


[Concedendo Permissão de Conteúdo da Lista na OU](#)

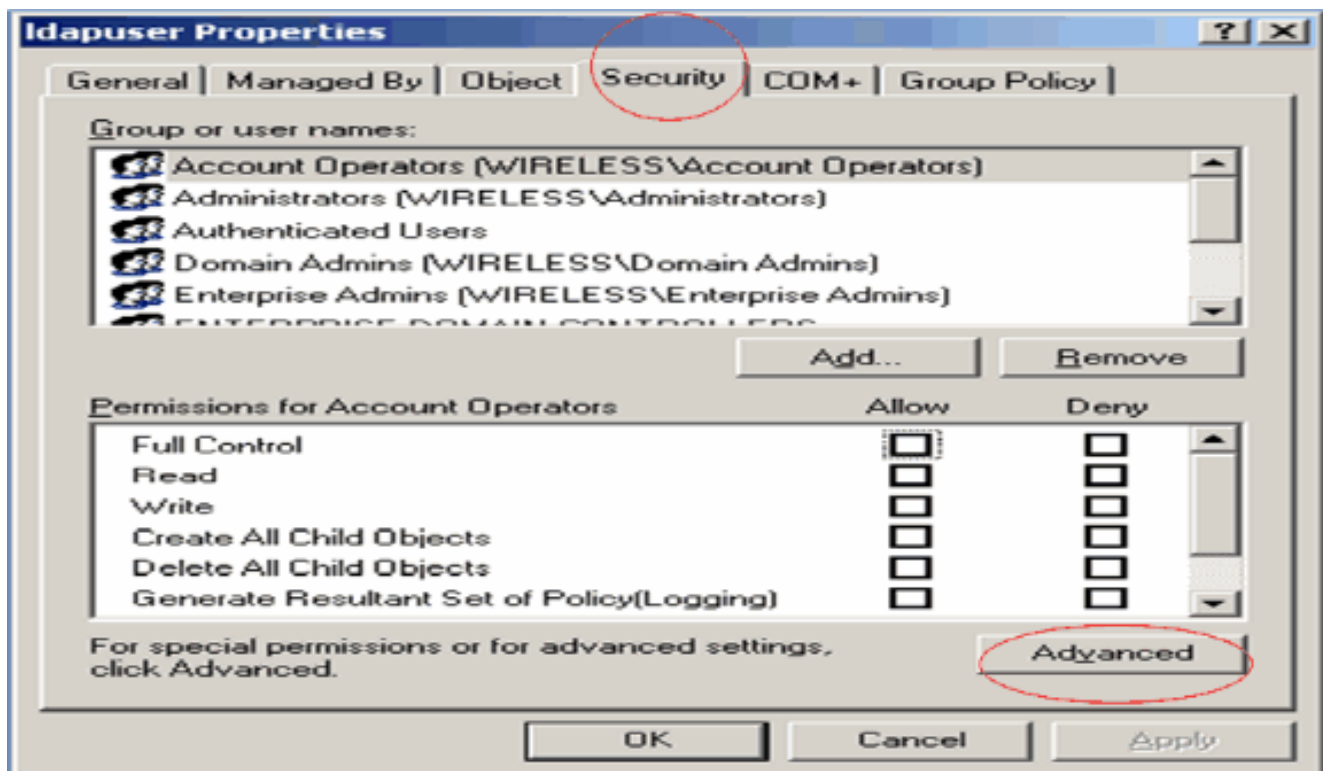
A próxima etapa é conceder pelo menos a permissão **Listar Conteúdo** ao **LOGON ANÔNIMO** na OU em que o usuário está localizado. Neste exemplo, "user2" está localizado na OU "ldapuser". Siga estas etapas para realizar essa ação:

1. Em Usuários e Computadores do Active Directory, clique com o botão direito do mouse em OU

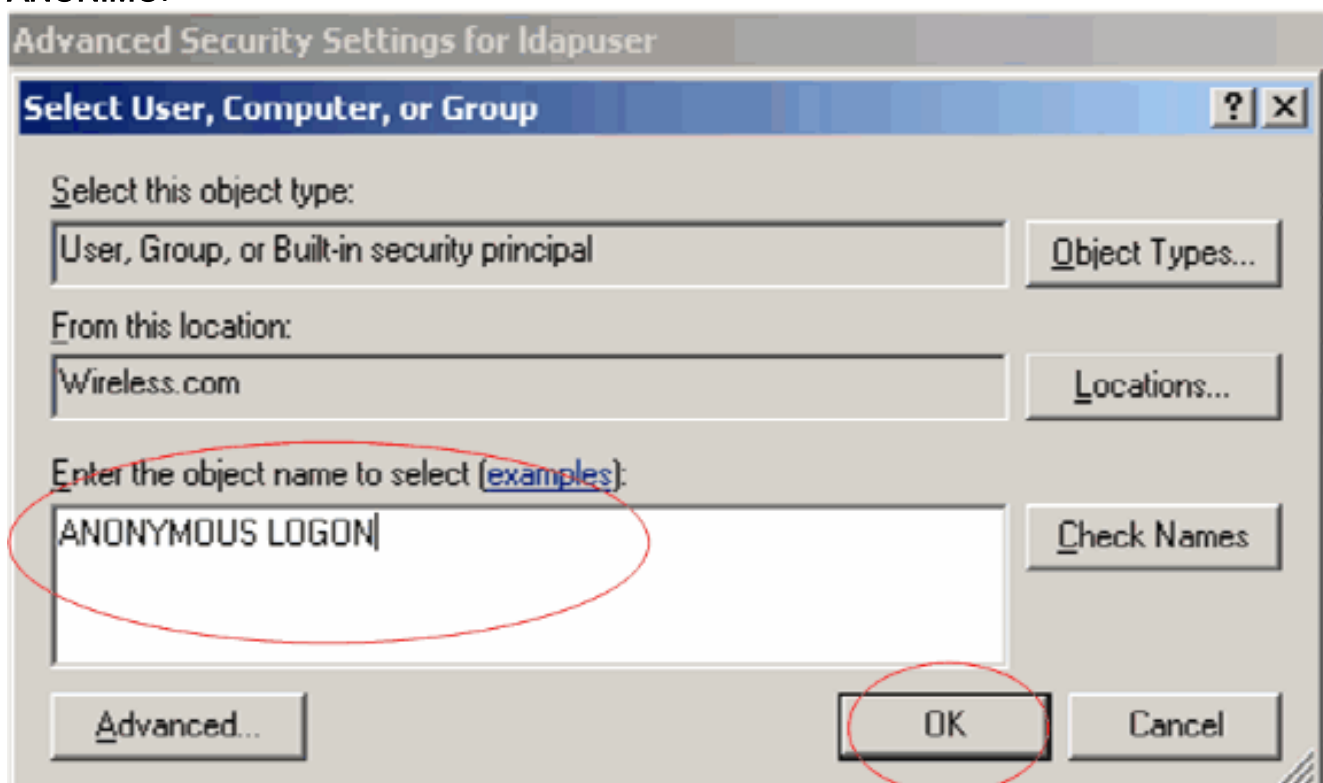
Idapuser e escolha
Propriedades.



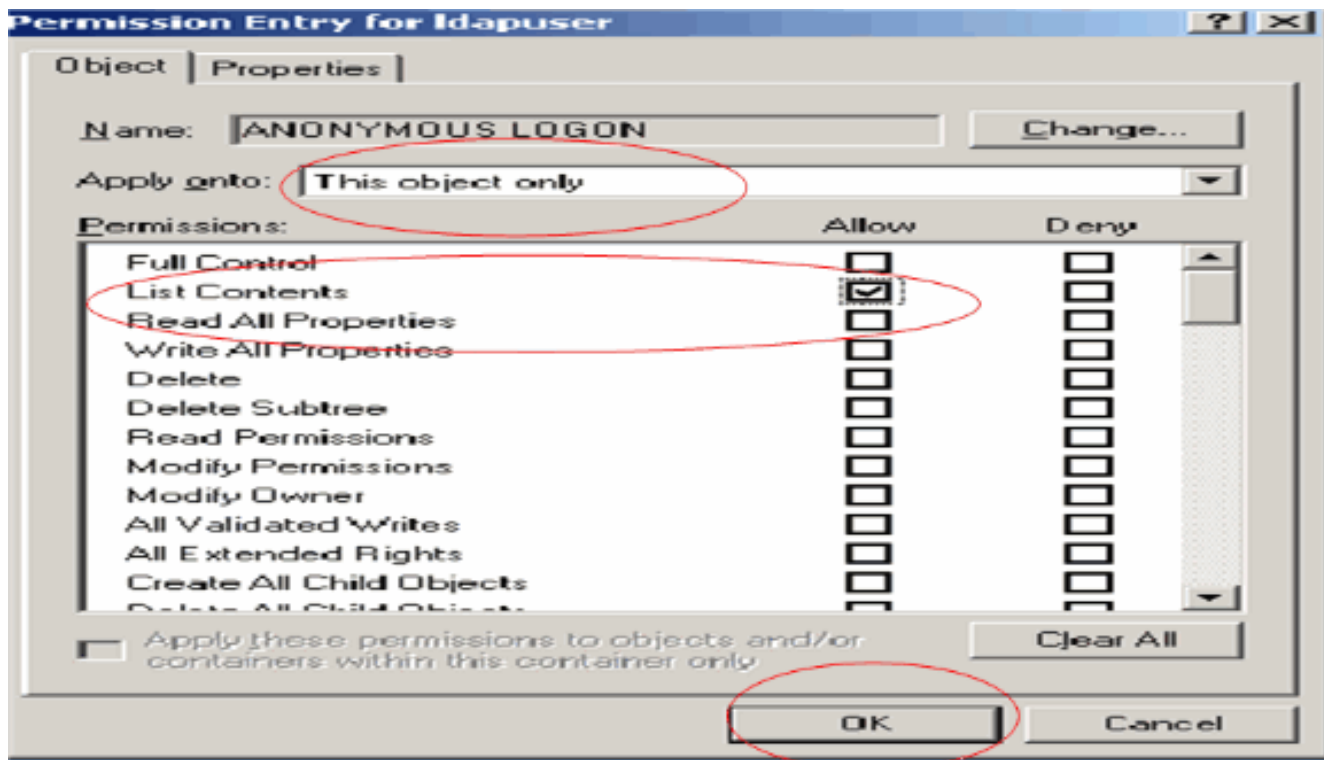
2. Clique em **Segurança** e em
Avançado.



3. Clique em Add. Na caixa de diálogo que é aberta, insira **LOGON ANÔNIMO**.



4. Reconheça o diálogo. Isso abre uma nova janela de diálogo.
5. Na caixa suspensa **Aplicar em**, escolha **Somente este objeto** e ative a caixa de seleção **Listar Conteúdo**.

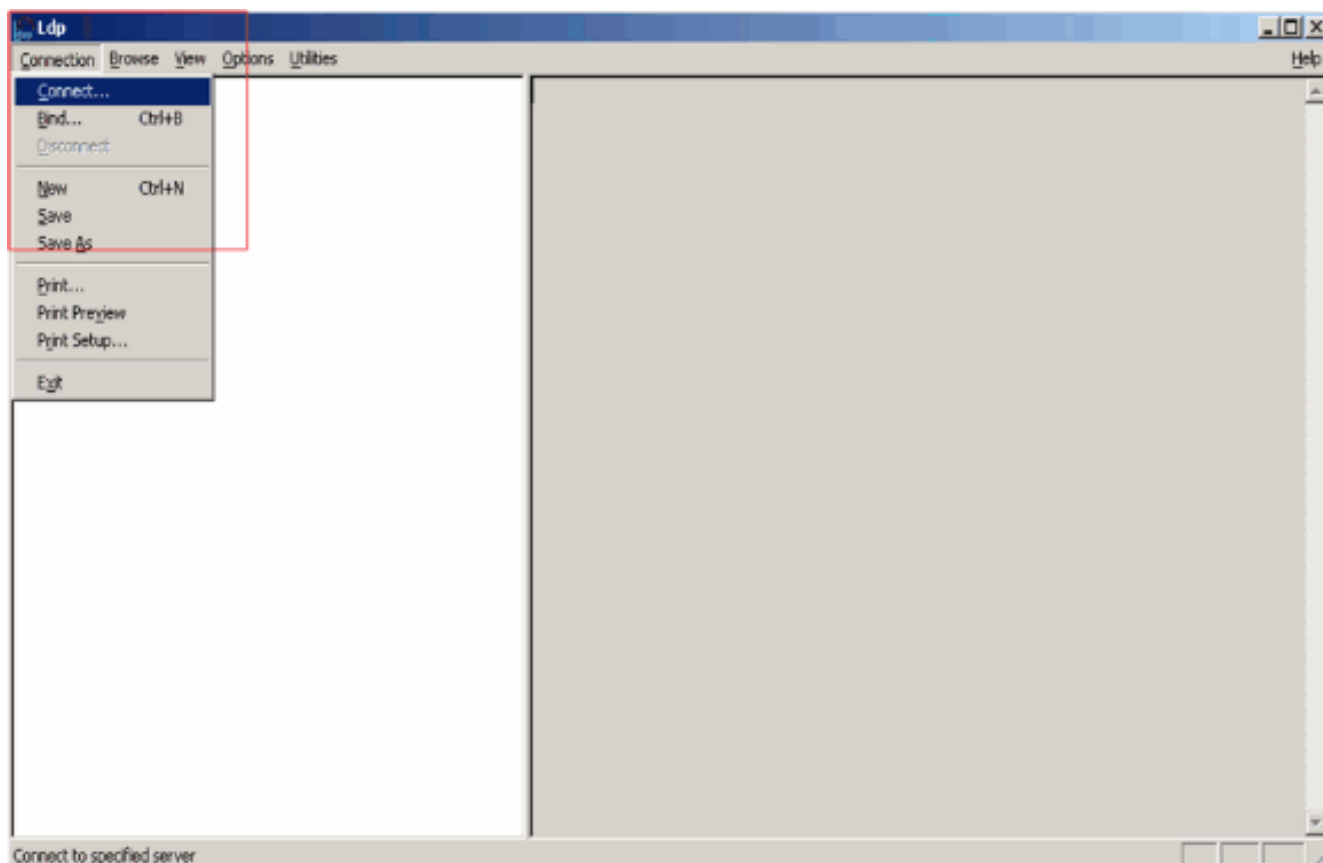


Usando o LDP para identificar os atributos do usuário

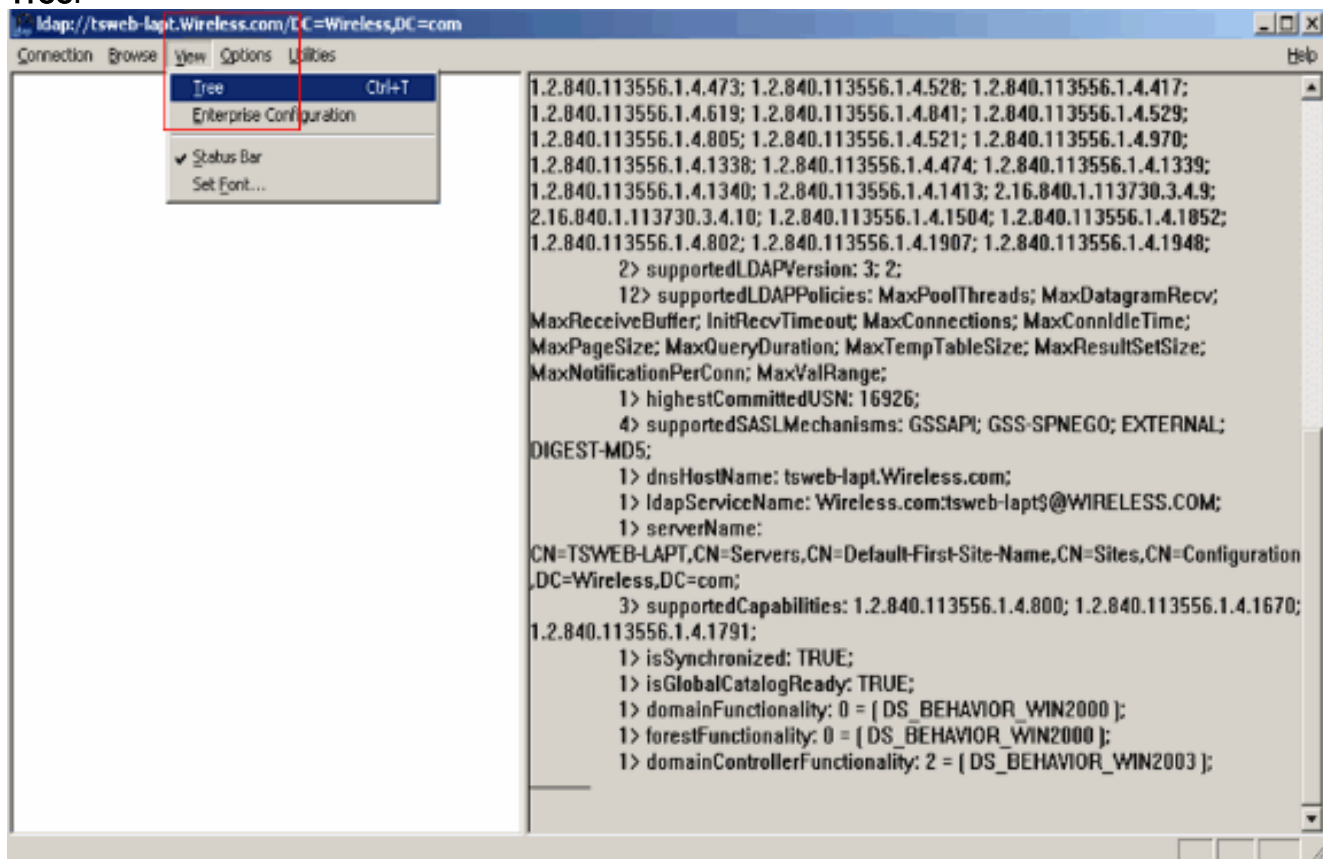
Essa ferramenta de GUI é um cliente LDAP que permite que os usuários executem operações (como conectar, vincular, pesquisar, modificar, adicionar, excluir) em qualquer diretório compatível com LDAP, como o Active Directory. O LDP é usado para visualizar objetos armazenados no Active Directory junto com seus metadados, como descritores de segurança e metadados de replicação.

A ferramenta GUI do LDP é incluída quando você instala as Ferramentas de suporte do Windows Server 2003 a partir do CD do produto. Esta seção explica o uso do utilitário LDP para identificar os atributos específicos associados ao usuário **user2**. Alguns desses atributos são usados para preencher os parâmetros de configuração do servidor LDAP no WLC, como tipo de atributo de usuário e tipo de objeto de usuário.

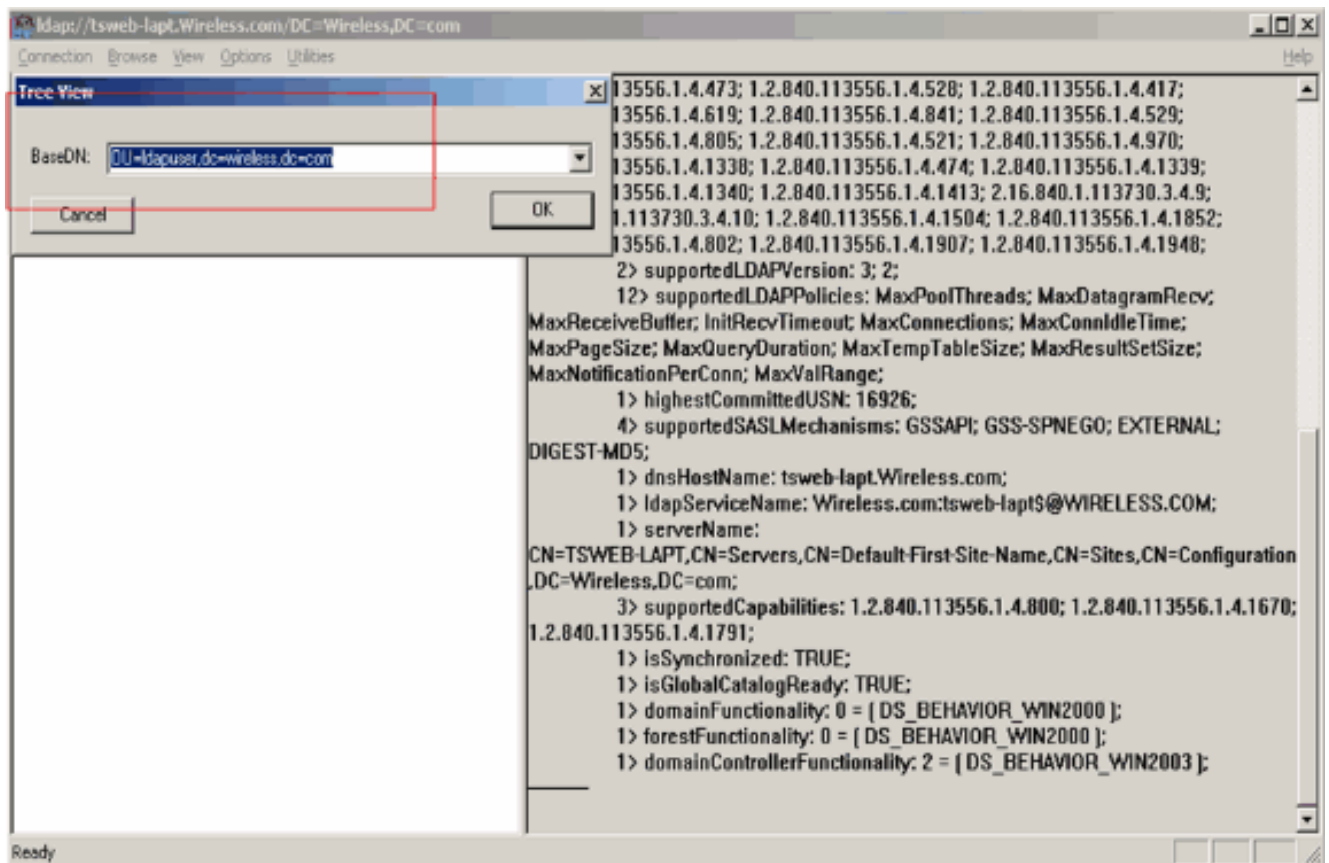
1. No servidor Windows 2003 (mesmo no mesmo servidor LDAP), clique em **Start > Run** e insira **LDP** para acessar o navegador LDP.
2. Na janela principal do LDP, clique em **Connection > Connect** e conecte-se ao servidor LDAP inserindo o endereço IP do servidor LDAP.



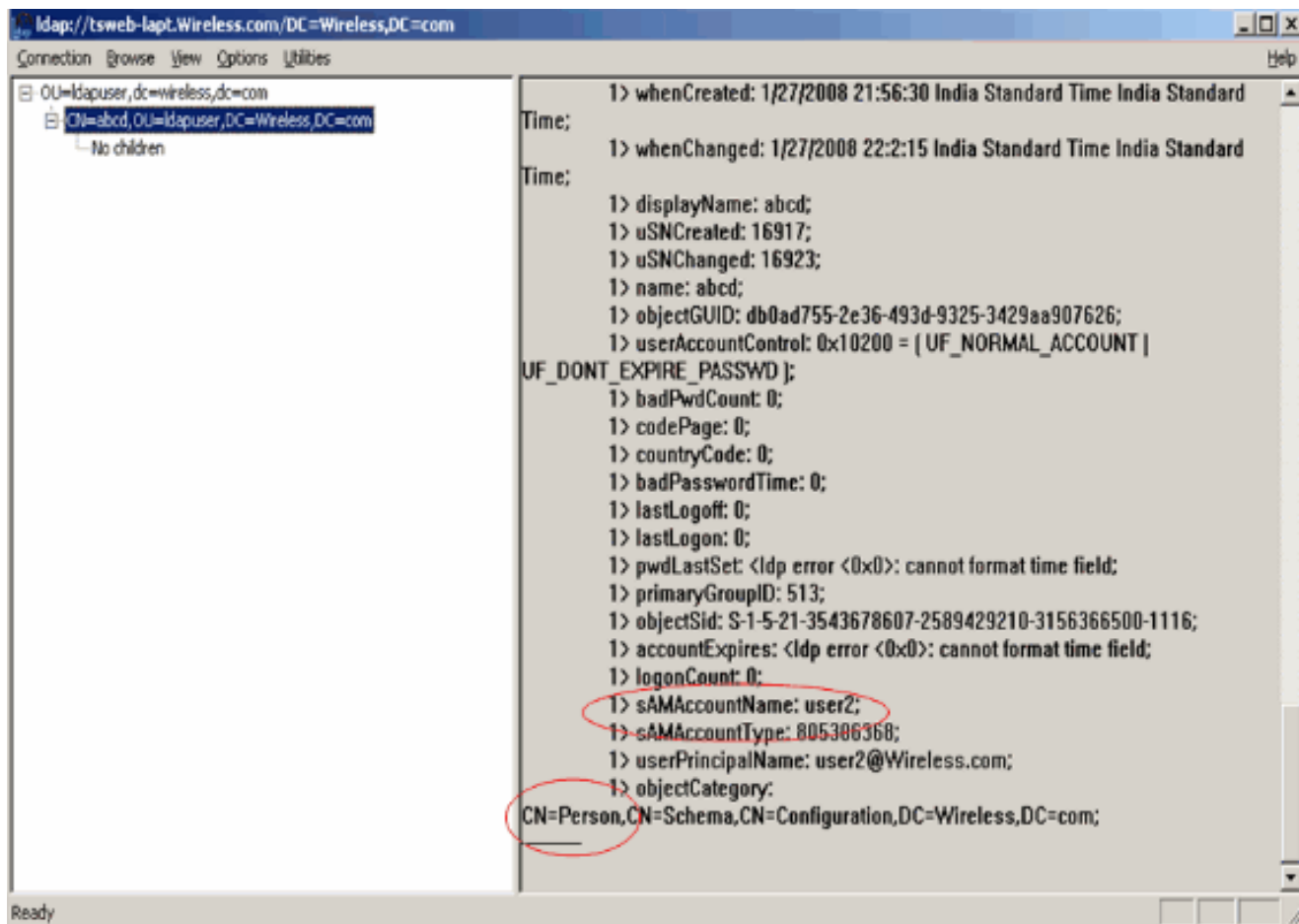
3. Depois de conectado ao servidor LDAP, selecione **View** no menu principal e clique em **Tree**.



4. Na janela resultante Visualização em árvore, insira o BaseDN do usuário. Neste exemplo, **user2** está localizado na OU "ldapuser" no domínio Wireless.com. Portanto, o BaseDN para o usuário **user2** é **OU=ldapuser, dc=wireless, dc=com**. Click **OK**.



5. O lado esquerdo do navegador LDP exibe a árvore inteira que aparece sob o BaseDN especificado (**OU=ldapuser, dc=wireless, dc=com**). Expanda a árvore para localizar o usuário **user2**. Esse usuário pode ser identificado com o valor de CN que representa o nome do usuário. Neste exemplo, é **CN=abcd**. Clique duas vezes em **CN=abcd**. No painel do lado direito do navegador LDP, o LDP exibirá todos os atributos associados ao usuário2. Este exemplo explica esta etapa:



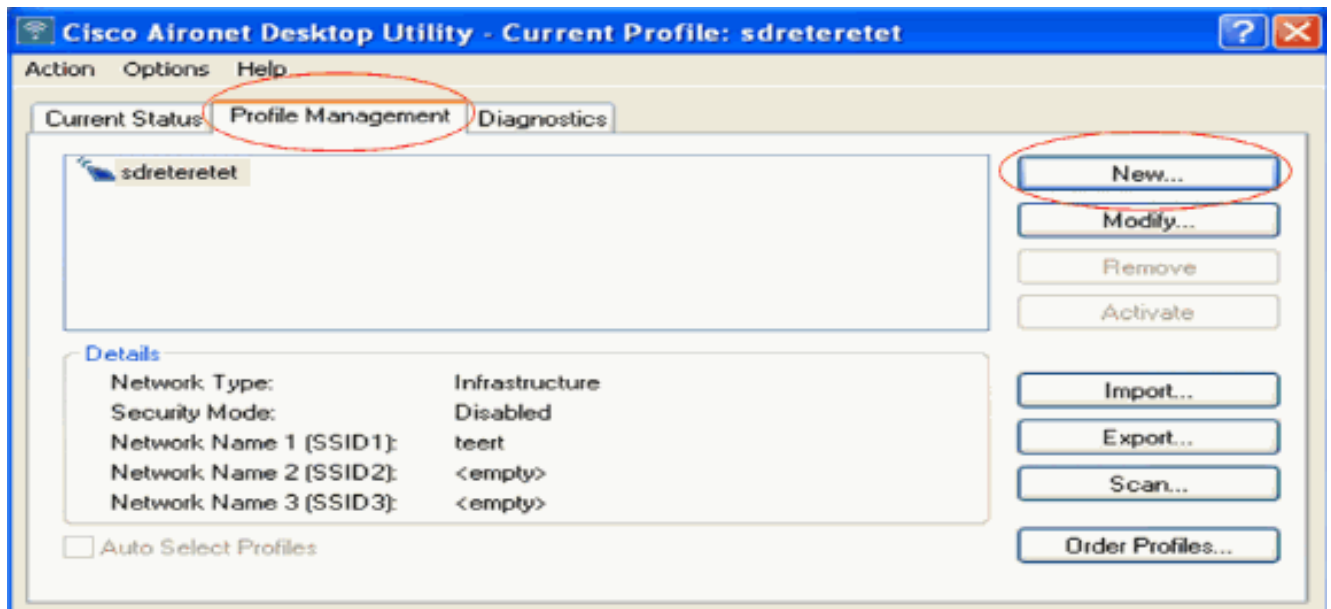
Neste exemplo, observe os campos circulados à direita.

6. Conforme mencionado na seção [Configurar WLC com Detalhes do Servidor LDAP](#) deste documento, no campo **Atributo do Usuário**, insira o nome do atributo no registro do usuário que contém o nome do usuário. Nessa saída do LDP, você pode ver que **sAMAccountName** é um atributo que contém o nome de usuário "user2". Portanto, insira o atributo **sAMAccountName** que corresponde ao campo **User Attribute** no WLC.
7. No campo **User Object Type** (Tipo de objeto de usuário), insira o valor do atributo **objectType** do LDAP que identifica o registro como um usuário. Frequentemente, os registros de usuário têm diversos valores para o atributo **objectType**, sendo que alguns são exclusivos e outros são compartilhados com diversos tipos de objeto. Na saída LDP, **CN=Person** é um valor que identifica o registro como um usuário. Portanto, especifique **Person** como o atributo **User Object Type** no WLC.

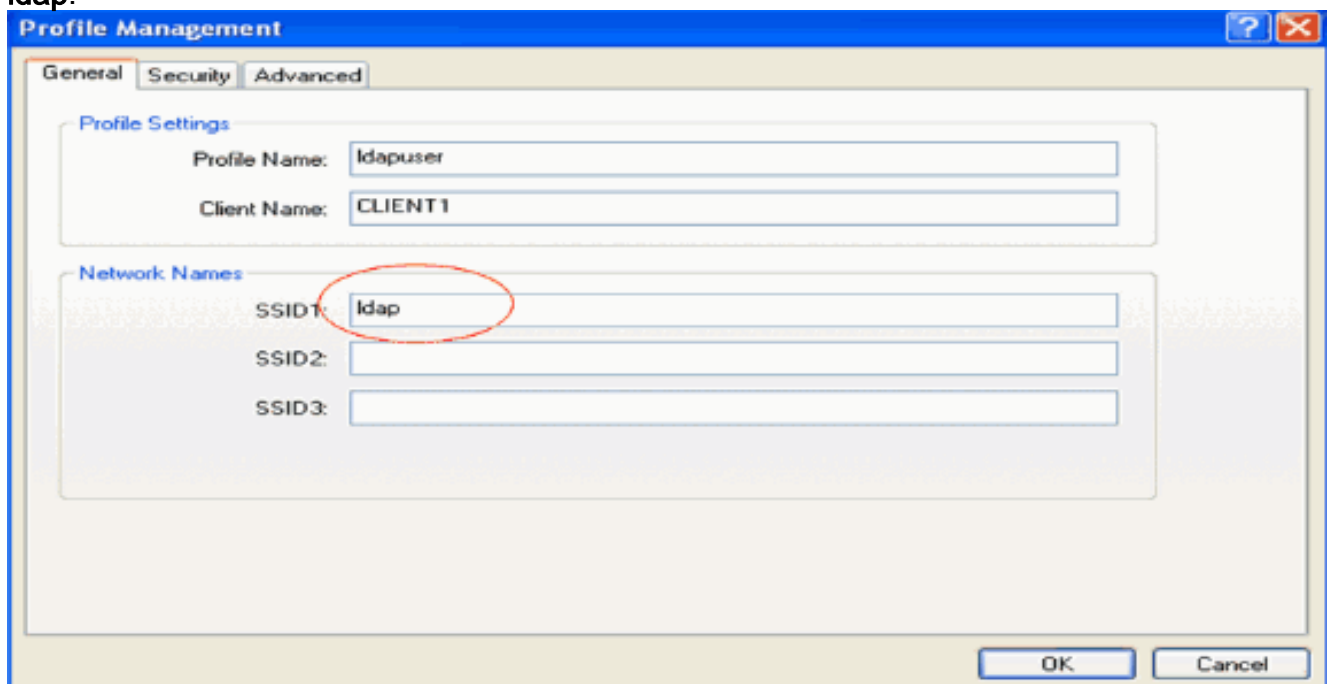
[Configurar cliente sem fio](#)

A última etapa é configurar o cliente sem fio para autenticação EAP-FAST com certificados de cliente e servidor. Siga estas etapas para realizar essa ação:

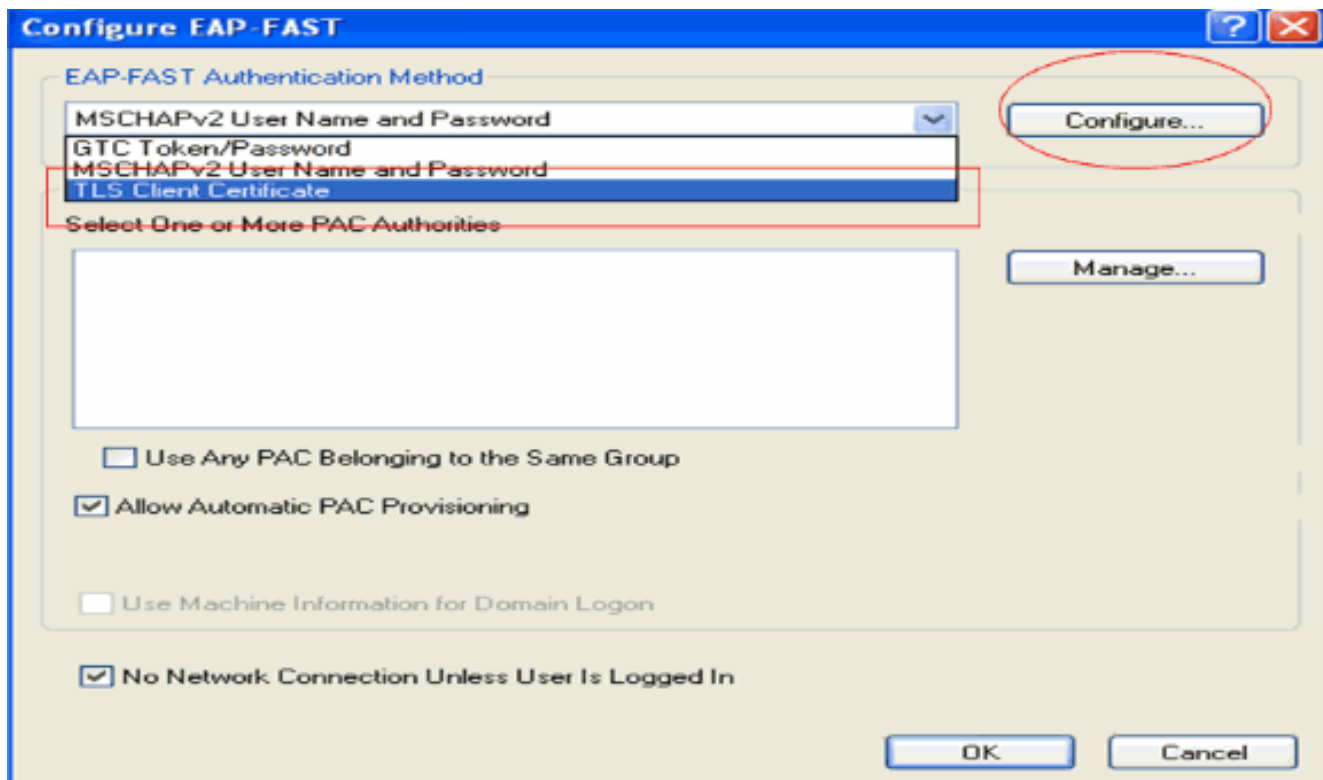
1. Inicie o **Cisco Aironet Desktop Utility (ADU)**. Na janela principal do ADU, clique em **Profile Management > New** para criar um novo perfil de cliente sem fio.



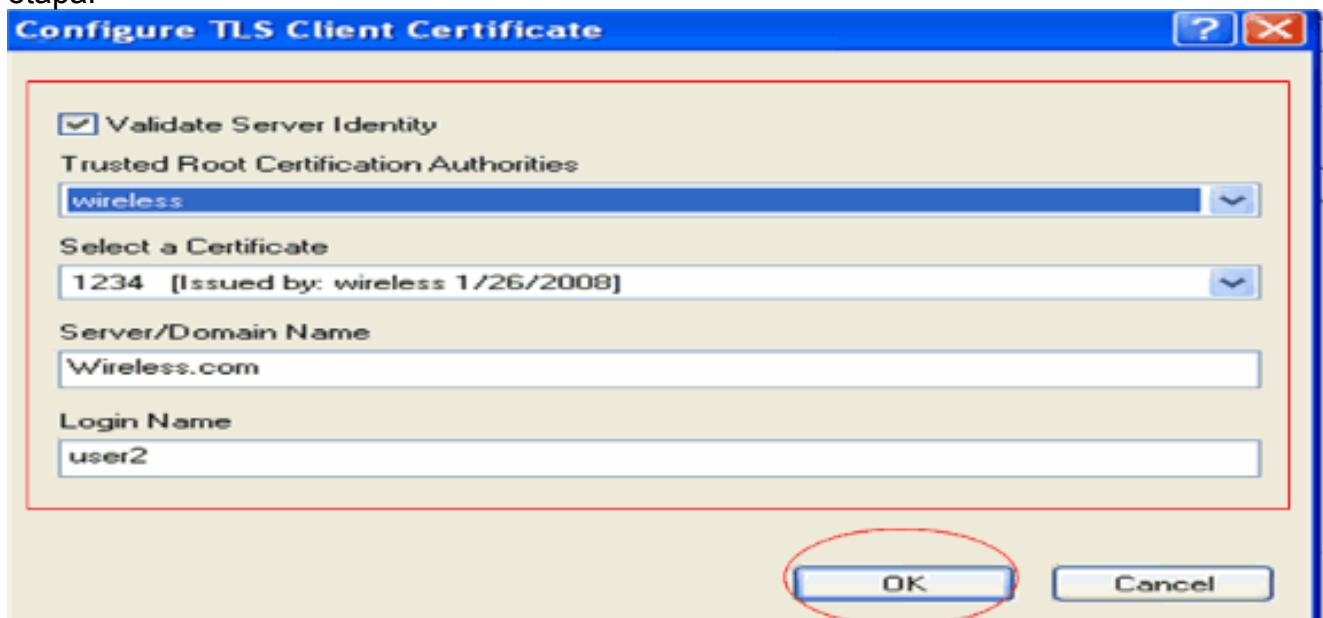
2. Especifique um nome de perfil e atribua um nome SSID a esse perfil. Esse nome SSID deve ser o mesmo configurado na WLC. Neste exemplo, o nome SSID é **ldap**.



3. Clique na guia **Security** e escolha **802.1x/EAP** como a segurança da camada 2. Escolha **EAP-FAST** como o método EAP e clique em **Configure**.
4. Na página de configuração EAP-FAST, escolha **Certificado de cliente TLS** na caixa suspensa Método de autenticação EAP-FAST e clique em **Configurar**.



5. Na janela de configuração do certificado de Cliente TLS:Habilite a caixa de seleção **Validar identidade do servidor** e selecione o certificado CA instalado no cliente (explicado na seção [Gerar o certificado CA raiz para o cliente](#) deste documento) como a autoridade de certificação raiz confiável.Selecione o certificado de dispositivo instalado no cliente (explicado na seção [Gerar um certificado de dispositivo para o cliente](#) deste documento) como o certificado de cliente.Click **OK**.Este exemplo explica esta etapa:



O perfil do cliente sem fio é criado.

Verificar

Execute estas etapas para verificar se sua configuração funciona corretamente.

1. Ative o SSID **ldap** no ADU.
2. Clique em **Sim** ou em **OK** conforme necessário nas próximas janelas. Você deve ser capaz

de ver todas as etapas de autenticação de cliente, bem como a associação para ser bem-sucedido no ADU.

Use esta seção para confirmar se a sua configuração funciona corretamente. Use o modo CLI da WLC.

- Para verificar se a WLC pode se comunicar com o servidor LDAP e localizar o usuário, especifique o comando **debug aaa ldap enable** da CLI da WLC. Este exemplo explica um processo LDAP de comunicação bem-sucedido: **Observação:** parte da saída nesta seção foi movida para as segundas linhas devido à consideração de espaço. (Cisco Controller) **>debug aaa ldap enable**

```
Sun Jan 27 09:23:46 2008: AuthenticationRequest: 0xba96514
Sun Jan 27 09:23:46 2008:      Callback.....0x8
344900
Sun Jan 27 09:23:46 2008:      protocolType.....0x0
0100002
Sun Jan 27 09:23:46 2008:      proxyState.....00:
40:96:AC:E6:57-00:00
Sun Jan 27 09:23:46 2008:      Packet contains 2 AVPs (not shown)
Sun Jan 27 09:23:46 2008: ldapTask [1] received msg 'REQUEST' (2) in state 'IDLE' (1)
Sun Jan 27 09:23:46 2008: LDAP server 1 changed state to INIT
Sun Jan 27 09:23:46 2008: ldapInitAndBind [1] called lcapi_init (rc = 0 - Success)
Sun Jan 27 09:23:46 2008: ldapInitAndBind [1] called lcapi_bind (rc = 0 - Success)
Sun Jan 27 09:23:46 2008: LDAP server 1 changed state to CONNECTED
Sun Jan 27 09:23:46 2008: LDAP server 1 now active
Sun Jan 27 09:23:46 2008: LDAP_CLIENT: UID Search (base=OU=ldapuser,DC=wireless,
DC=com, pattern=(&(objectclass=Person)(sAMAccountName=user2)))
Sun Jan 27 09:23:46 2008: LDAP_CLIENT: Returned msg type 0x64
Sun Jan 27 09:23:46 2008: ldapAuthRequest [1] called lcapi_query base="OU=ldapus
er,DC=wireless,DC=com" type="Person" attr="sAMAccountName" user="user2" (rc = 0
- Success)
Sun Jan 27 09:23:46 2008: LDAP ATTR> dn = CN=abcd,OU=ldapuser,DC=Wireless,DC=com
(size 38)
Sun Jan 27 09:23:46 2008: Handling LDAP response Success
```

A partir das informações destacadas nesta saída de depuração, fica claro que o servidor LDAP é consultado pela WLC com os Atributos do usuário especificados na WLC e que o processo LDAP é bem-sucedido.

- Para verificar se a autenticação EAP local foi bem-sucedida, especifique o comando **debug aaa local-auth eap method events enable** na CLI da WLC. Aqui está um exemplo: (Cisco Controller) **>debug aaa local-auth eap method events enable**

```
Sun Jan 27 09:38:28 2008: eap_fast.c-EVENT: New context
(EAP handle = 0x1B000009)

Sun Jan 27 09:38:28 2008: eap_fast.c-EVENT: Allocated new EAP-FAST context
(handle = 0x22000009)

Sun Jan 27 09:38:28 2008: eap_fast_auth.c-AUTH-EVENT: Process Response
(EAP handle = 0x1B000009)

Sun Jan 27 09:38:28 2008: eap_fast_auth.c-AUTH-EVENT: Received Identity

Sun Jan 27 09:38:28 2008: eap_fast_tlv.c-AUTH-EVENT: Adding PAC A-ID TLV
(436973636f0000000000000000000000)

Sun Jan 27 09:38:28 2008: eap_fast_auth.c-AUTH-EVENT: Sending Start

Sun Jan 27 09:38:29 2008: eap_fast.c-AUTH-EVENT: Process Response, type: 0x2b
```

Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT: Process Response
(EAP handle = 0x1B000009)

**Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT:
Received TLS record type: Handshake in state: Start**

Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT: Local certificate found

Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT: Reading Client Hello handshake

Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT:
TLS_DHE_RSA_AES_128_CBC_SHA proposed...

Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: Proposed ciphersuite(s):

Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: TLS_DHE_RSA_WITH_AES_128_CBC_SHA

Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: TLS_RSA_WITH_AES_128_CBC_SHA

Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: TLS_RSA_WITH_RC4_128_SHA

Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: Selected ciphersuite:

Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: TLS_DHE_RSA_WITH_AES_128_CBC_SHA

Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT: Building Provisioning Server Hello

**Sun Jan 27 09:38:29 2008: eap_fast_crypto.c-EVENT:
Starting Diffie Hellman phase 1 ...**

**Sun Jan 27 09:38:30 2008: eap_fast_crypto.c-EVENT:
Diffie Hellman phase 1 complete**

Sun Jan 27 09:38:30 2008: eap_fast_auth.c-AUTH-EVENT: DH signature length = 128

Sun Jan 27 09:38:30 2008: eap_fast_auth.c-AUTH-EVENT: Sending Provisioning Serving Hello

Sun Jan 27 09:38:30 2008: eap_fast.c-EVENT: Tx packet fragmentation required

Sun Jan 27 09:38:30 2008: eap_fast.c-AUTH-EVENT: eap_fast_rx_packet():
EAP Fast NoData (0x2b)

Sun Jan 27 09:38:30 2008: eap_fast.c-AUTH-EVENT: eap_fast_rx_packet():
EAP Fast NoData (0x2b)

Sun Jan 27 09:38:30 2008: eap_fast.c-AUTH-EVENT: eap_fast_rx_packet():
EAP Fast NoData (0x2b)

Sun Jan 27 09:38:32 2008: eap_fast.c-AUTH-EVENT: Process Response, type: 0x2b

Sun Jan 27 09:38:32 2008: eap_fast.c-EVENT: Reassembling TLS record

Sun Jan 27 09:38:32 2008: eap_fast.c-EVENT: Sending EAP-FAST Ack

.....
.....
.....

**Sun Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT:
Received TLS record type: Handshake in state: Sent provisioning Server Hello**

Sun Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT:

Reading Client Certificate handshake

Sun Jan 27 09:38:32 2008: eap_fast.c-EVENT: Added certificate 1 to chain

Sun Jan 27 09:38:32 2008: eap_fast.c-EVENT: Added certificate 2 to chain

Sun Jan 27 09:38:32 2008: eap_fast.c-EVENT: Successfully validated received certificate

Sun Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT: Rx'd I-ID:
"EAP-FAST I-ID" from Peer Cert

Sun Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT:
Reading Client Key Exchange handshake

Sun Jan 27 09:38:32 2008: eap_fast_crypto.c-EVENT:
Starting Diffie Hellman phase 2 ...

Sun Jan 27 09:38:32 2008: eap_fast_crypto.c-EVENT:
Diffie Hellman phase 2 complete.

Sun Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT:
Reading Client Certificate Verify handshake

Sun Jan 27 09:38:32 2008: eap_fast_crypto.c-EVENT:
Sign certificate verify succeeded (compare)

.....
.....
.....
.....
.....

• O comando **debug aaa local-auth db enable** também é muito útil. Aqui está um exemplo:(Cisco Controller) **>debug aaa local-auth db enable**

Sun Jan 27 09:35:32 2008: LOCAL_AUTH: EAP: Received an auth request

Sun Jan 27 09:35:32 2008: LOCAL_AUTH: Creating new context

Sun Jan 27 09:35:32 2008: LOCAL_AUTH: Local auth profile name for context 'ldapuser'

Sun Jan 27 09:35:32 2008: LOCAL_AUTH: Created new context eap session handle fb000007

Sun Jan 27 09:35:32 2008: LOCAL_AUTH: (EAP:8) Sending the Rxd EAP packet
(id 2) to EAP subsystem

Sun Jan 27 09:35:32 2008: LOCAL_AUTH: Found matching context for id - 8

Sun Jan 27 09:35:32 2008: LOCAL_AUTH: (EAP) Sending user credential
request username 'user2' to LDAP

Sun Jan 27 09:35:32 2008: LOCAL_AUTH: Found context matching MAC address - 8

.....
.....
.....
.....

```
Sun Jan 27 09:35:36 2008: LOCAL_AUTH: (EAP:8) Sending the Rxd EAP packet
(id 12) to EAP subsystem

Sun Jan 27 09:35:36 2008: LOCAL_AUTH: Found matching context for id - 8

Sun Jan 27 09:35:36 2008: LOCAL_AUTH: (EAP:8) ---> [KEY AVAIL] send_len 64, recv_len 0

Sun Jan 27 09:35:36 2008: LOCAL_AUTH: (EAP:8) received keys waiting for success

Sun Jan 27 09:35:36 2008: LOCAL_AUTH: Found matching context for id - 8

Sun Jan 27 09:35:36 2008: LOCAL_AUTH: (EAP:8) Received success event

Sun Jan 27 09:35:36 2008: LOCAL_AUTH: (EAP:8) Processing keys success
```

- Para visualizar os certificados instalados na WLC a serem usados para autenticação local, execute o comando **show local-auth certificates** na CLI da WLC. Aqui está um exemplo:(Controlador Cisco) **>show local-auth certificates**

Certificates available for Local EAP authentication:

Certificate issuer vendor

CA certificate:

Subject: DC=com, DC=Wireless, CN=wireless

Issuer: DC=com, DC=Wireless, CN=wireless

Valid: 2008 Jan 23rd, 15:50:27 GMT to 2013 Jan 23rd, 15:50:27 GMT

Device certificate:

Subject: O=cisco, CN=ciscowlc123

Issuer: DC=com, DC=Wireless, CN=wireless

Valid: 2008 Jan 24th, 12:18:31 GMT to 2010 Jan 23rd, 12:18:31 GMT

Certificate issuer cisco

CA certificate:

Subject: O=Cisco Systems, CN=Cisco Manufacturing CA

Issuer: O=Cisco Systems, CN=Cisco Root CA 2048

Valid: 2005 Jun 10th, 22:16:01 GMT to 2029 May 14th, 20:25:42 GMT

Device certificate:

Not installed.

- Para visualizar a configuração de autenticação local na WLC a partir do modo CLI, execute o comando **show local-auth config**. Aqui está um exemplo:(Controlador Cisco) **>show local-auth config**

User credentials database search order:

Primary LDAP

Timer:

Active timeout 300

Configured EAP profiles:

Name ldapuser

Certificate issuer vendor

Peer verification options:

Check against CA certificates Enabled

Verify certificate CN identity Disabled

Check certificate date validity Disabled

EAP-FAST configuration:

Local certificate required Yes

Client certificate required Yes

Enabled methods fast

Configured on WLANs 2

EAP Method configuration:

EAP-FAST:

--More-- or (q)uit

Server key <hidden>

TTL for the PAC 10

Anonymous provision allowed No

.....

.....

Authority Information Cisco A-ID

Troubleshoot

Você pode usar estes comandos para solucionar problemas de configuração:

- **debug aaa local-auth eap method events enable**
- **debug aaa all enable**
- **debug dot1x packet enable**

Informações Relacionadas

- [Exemplo de Autenticação EAP-FAST com Controladoras Wireless LAN e Servidor RADIUS Externo](#)
- [PEAP sob redes sem fio unificadas com o Internet Authentication Service da Microsoft \(IAS\)](#)
- [Exemplo de configuração de atribuição de VLAN dinâmica com WLCs baseadas em ACS para mapeamento de grupo do Active Directory](#)
- [Guia de configuração do Cisco Wireless LAN Controller - Configurando soluções de segurança](#)
- [Guia de configuração do Cisco Wireless LAN Controller - Gerenciamento do software e das configurações do controlador](#)
- [Exemplo de Configuração de Autenticação EAP com WLAN Controllers \(WLC\)](#)
- [Perguntas frequentes sobre o design e os recursos do controlador de LAN sem fio \(WLC\)](#)
- [Cisco Secure Services Client com autenticação EAP-FAST](#)
- [Perguntas frequentes sobre a controladora Wireless LAN \(WLC\)](#)
- [Perguntas frequentes sobre mensagens de sistema e erros da controladora Wireless LAN \(WLC\) das controladoras](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.