

EAP-TLS em Redes Wireless Unificadas com o ACS 4.0 e o Windows 2003

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Diagrama de Rede](#)

[Conventions](#)

[Instalação do Windows Enterprise 2003 com IIS, Certificate Authority, DNS, DHCP \(DC CA\) DC CA \(wireless-essdemoca\)](#)

[Configuração do Windows Standard 2003 com Cisco Secure ACS 4.0](#)

[Instalação e configuração básicas](#)

[Instalação do Cisco Secure ACS 4.0](#)

[Configuração do controlador Cisco LWAPP](#)

[Crie a configuração necessária para WPA2/WPA](#)

[Autenticação EAP-TLS](#)

[Instalar o Snap-in Modelos de Certificado](#)

[Crie o Modelo de Certificado para o Servidor Web ACS](#)

[Ativar o novo modelo de certificado do servidor Web ACS](#)

[Configuração do certificado ACS 4.0](#)

[Configurar certificado exportável para ACS](#)

[Instale o certificado no software ACS 4.0](#)

[Configuração do CLIENTE para EAP-TLS usando Windows Zero Touch](#)

[Executar uma instalação e configuração básicas](#)

[Configure a conexão de rede sem fio](#)

[Informações Relacionadas](#)

Introduction

Este documento descreve como configurar o acesso sem fio seguro usando Wireless LAN Controllers (WLCs), o software Microsoft Windows 2003 e o Cisco Secure Access Control Server (ACS) 4.0 via Extensible Authentication Protocol-Transport Layer Security (EAP-TLS).

Observação: para obter mais informações sobre a implantação de conexões sem fio seguras, consulte o [site da Microsoft Wi-Fi na Web](#) e o [Cisco SAFE Wireless Blueprint](#).

Prerequisites

Requirements

Há uma suposição de que o instalador tem conhecimento da instalação básica do Windows 2003 e da instalação do controlador Cisco, pois este documento abrange apenas as configurações específicas para facilitar os testes.

Para obter informações sobre instalação e configuração iniciais dos Cisco 4400 Series Controllers, consulte o [Guia de início rápido: Cisco 4400 Series Wireless LAN Controllers](#). Para obter informações sobre instalação e configuração iniciais dos Cisco 2000 Series Controllers, consulte o [Guia de início rápido: Cisco 2000 Series Wireless LAN Controllers](#).

Antes de começar, instale o sistema operacional Windows Server 2003 com Service Pack (SP)1 em cada um dos servidores do laboratório de teste e atualize todos os Service Packs. Instale os controladores e os APs e verifique se as atualizações de software mais recentes estão configuradas.

Importante: No momento em que este documento foi gravado, o SP1 é a atualização mais recente do Windows Server 2003 e o SP2 com patches de atualização é o software mais recente do Windows XP Professional.

O Windows Server 2003 com SP1, Enterprise Edition é usado para que a inscrição automática de certificados de usuário e estação de trabalho para autenticação EAP-TLS possa ser configurada. Isso é descrito na seção [Autenticação EAP-TLS](#) deste documento. A inscrição automática de certificados e a renovação automática facilitam a implantação de certificados e melhoram a segurança ao expirar e renovar certificados automaticamente.

Componentes Utilizados

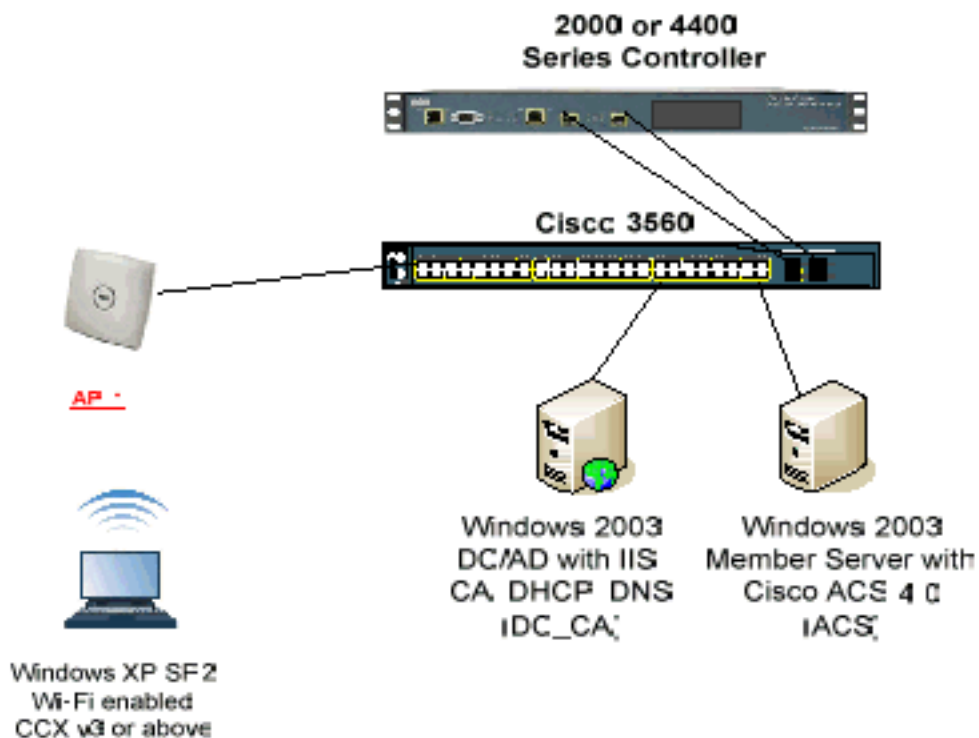
As informações neste documento são baseadas nestas versões de software e hardware:

- Controlador Cisco 2006 ou 4400 Series que executa 3.2.116.21
- Access Point Protocol (LWAPP) Cisco 1131
- Windows 2003 Enterprise com Internet Information Server (IIS), Certificate Authority (CA), DHCP e Domain Name System (DNS) instalados
- Windows 2003 Standard com Access Control Server (ACS) 4.0
- Windows XP Professional com SP (e Service Packs atualizados) e placa de interface de rede sem fio (NIC) (com suporte para CCX v3) ou solicitante de terceiros.
- Switch Cisco 3560

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:

Topologia de laboratório sem fio segura da Cisco



O objetivo principal deste documento é fornecer a você o procedimento passo a passo para implementar o EAP-TLS em Unified Wireless Networks com ACS 4.0 e o servidor Windows 2003 Enterprise. A ênfase principal é na inscrição automática do cliente para que ele se inscreva automaticamente e obtenha o certificado do servidor.

Observação: para adicionar o WPA (Wi-Fi Protected Access)/WPA2 com TKIP (Temporal Key Integrity Protocol)/AES (Advanced Encryption Standard) ao Windows XP Professional com SP, consulte a [atualização WPA2/Wireless Provisioning Services Information Element \(WPS IE\) para Windows XP com SP2](#).

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](#).

Instalação do Windows Enterprise 2003 com IIS, Certificate Authority, DNS, DHCP (DC_CA)

DC_CA (wireless-essdemoca)

DC_CA é um computador que executa o Windows Server 2003 com SP1, Enterprise Edition e executa estas funções:

- Um controlador de domínio para o domínio wireless demo.local que executa o IIS
- Um servidor DNS para o domínio DNS local de demonstração sem fio
- Um servidor DHCP
- AC raiz corporativa para o domínio de demo.local sem fio

Conclua estes passos para configurar DC_CA para estes serviços:

1. [Execute uma instalação e configuração básicas.](#)
2. [Configure o computador como um controlador de domínio.](#)
3. [Aumente o nível funcional do domínio.](#)
4. [Instalar e configurar o DHCP.](#)
5. [Instalar serviços de certificado.](#)
6. [Verifique as permissões de Administrador para certificados.](#)
7. [Adicione computadores ao domínio.](#)
8. [Permitir acesso sem fios a computadores.](#)
9. [Adicione usuários ao domínio.](#)
10. [Permitir acesso sem fio aos usuários.](#)
11. [Adicione grupos ao domínio.](#)
12. [Adicione usuários ao grupo WirelessUsers.](#)
13. [Adicione computadores clientes ao grupo WirelessUsers.](#)

[Passo 1: Executar instalação e configuração básicas](#)

Conclua estes passos:

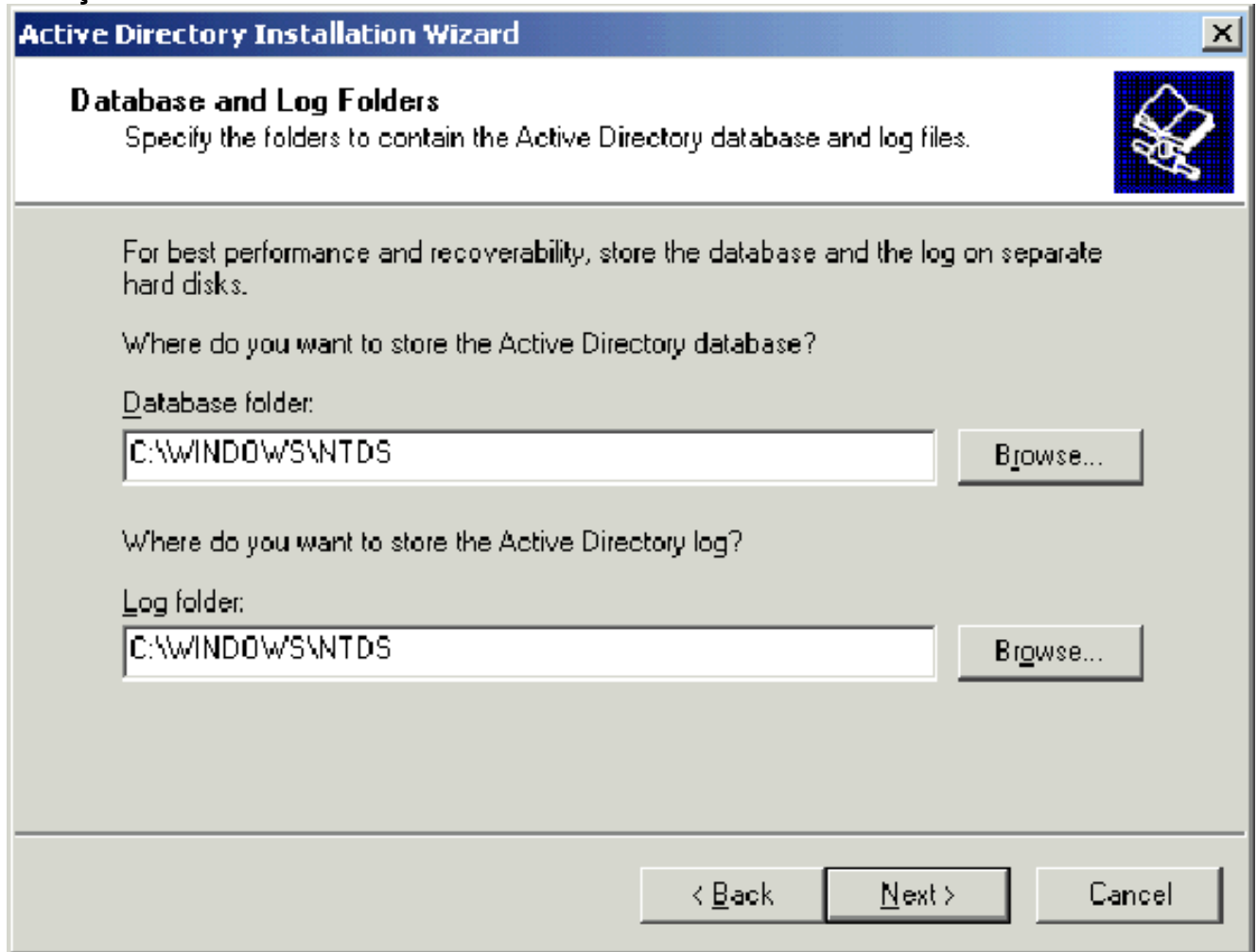
1. Instale o Windows Server 2003 com SP1, Enterprise Edition, como um servidor autônomo.
2. Configure o protocolo TCP/IP com o endereço IP 172.16.100.26 e a máscara de sub-rede 255.255.255.0.

[Passo 2: Configurar o computador como um controlador de domínio](#)

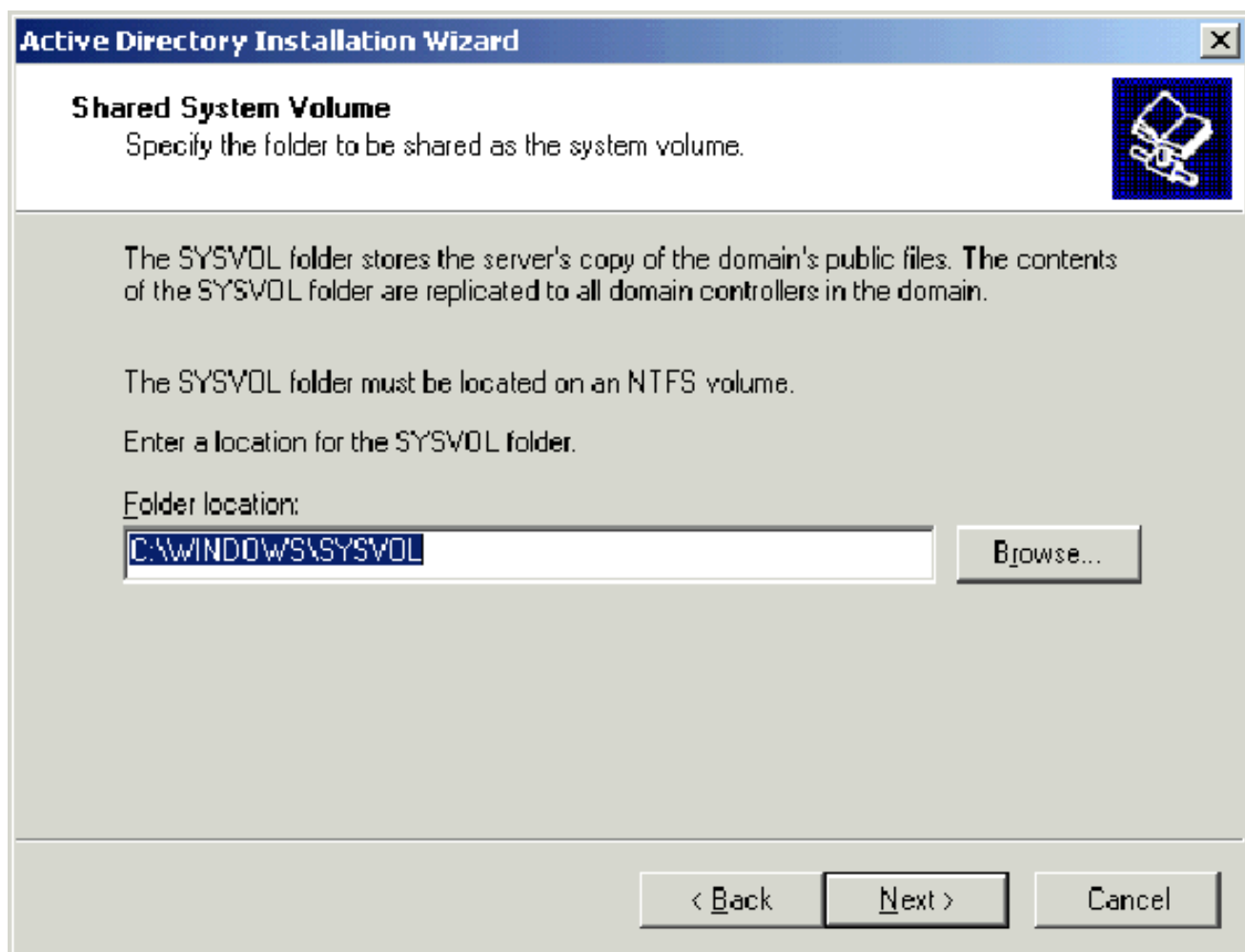
Conclua estes passos:

1. Para iniciar o Assistente de Instalação do Active Directory, escolha **Iniciar > Executar**, digite **dcpromo.exe** e clique em **OK**.
2. Na página Bem-vindo ao Assistente de Instalação do Active Directory, clique em **Avançar**.
3. Na página Compatibilidade do sistema operacional, clique em **Avançar**.
4. Na página Tipo de controlador de domínio, selecione **Controlador de domínio para um novo domínio** e clique em **Avançar**.
5. Na página Criar novo domínio, selecione **Domínio em uma nova floresta** e clique em **Avançar**.
6. Na página Instalar ou Configurar DNS, selecione **Não, apenas instalar e configurar DNS neste computador** e clique em **Avançar**.
7. Na página Novo nome de domínio, digite **wireless demo.local** e clique em **Avançar**.
8. Na página Nome de domínio NetBIOS, digite o nome do NetBIOS de domínio como **demo sem fio** e clique em **Avançar**.

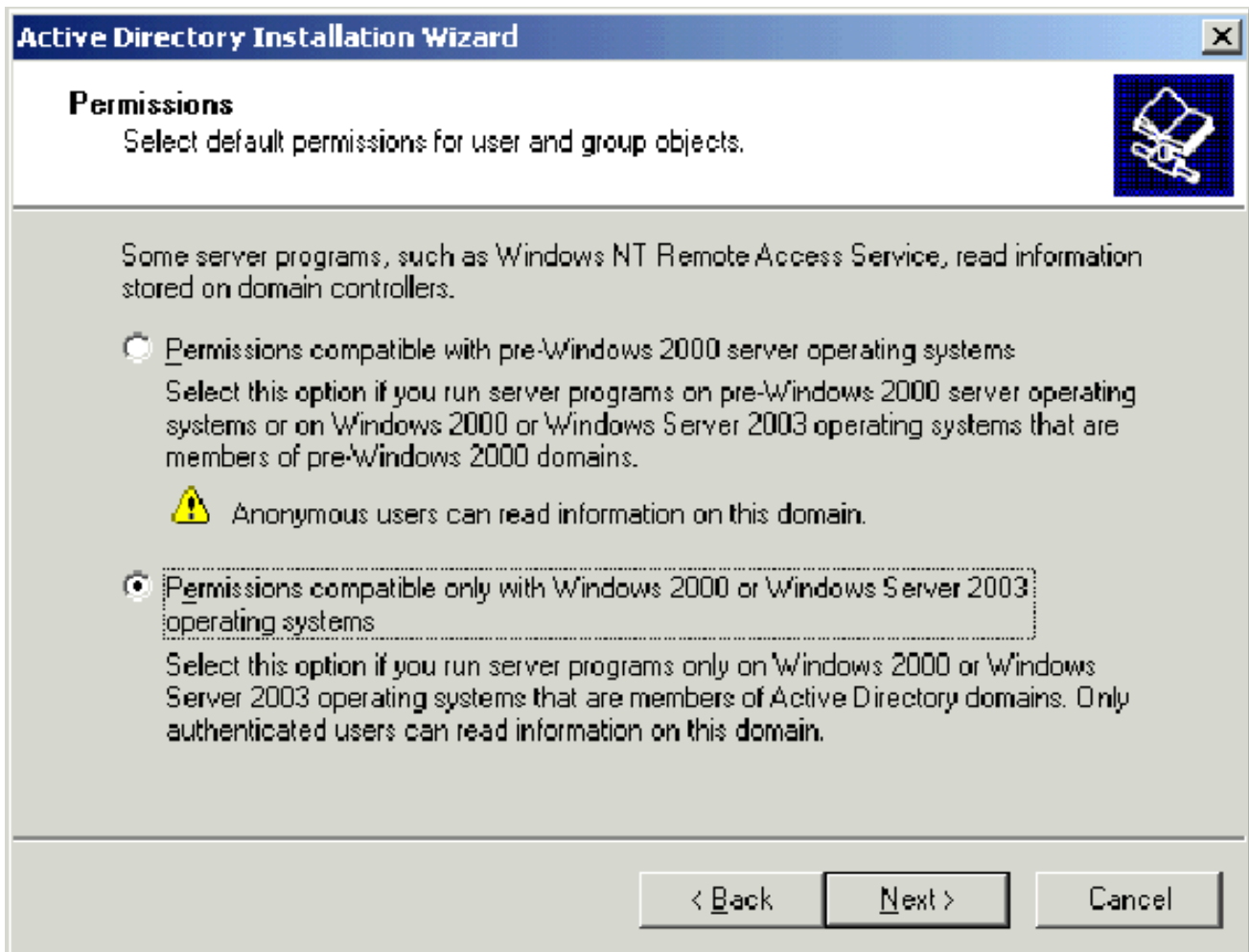
9. Na página Local de Pastas de Banco de Dados e Log, aceite os diretórios Pastas de Banco de Dados e Log padrão e clique em **Avançar**.



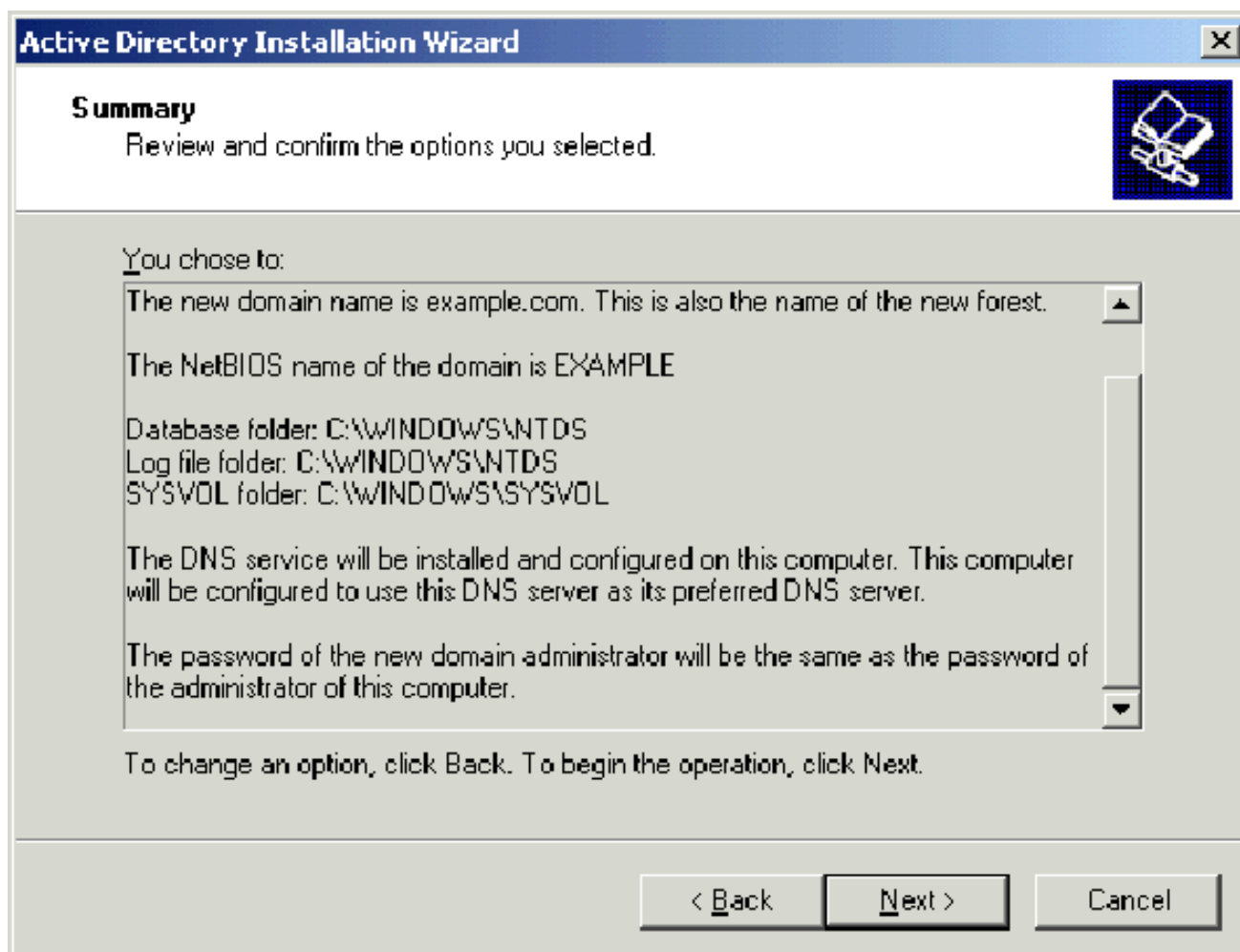
10. Na caixa de diálogo Volume do sistema compartilhado, verifique se o local da pasta padrão está correto e clique em **Avançar**.



11. Na página Permissões, verifique se **Permissões compatíveis somente com os sistemas operacionais Windows 2000 ou Windows Server 2003** estão selecionadas e clique em **Avançar**.



12. Na página Senha de administração do modo de restauração dos serviços de diretório, deixe as caixas de senha em branco e clique em **Avançar**.
13. Revise as informações na página Resumo e clique em **Avançar**.

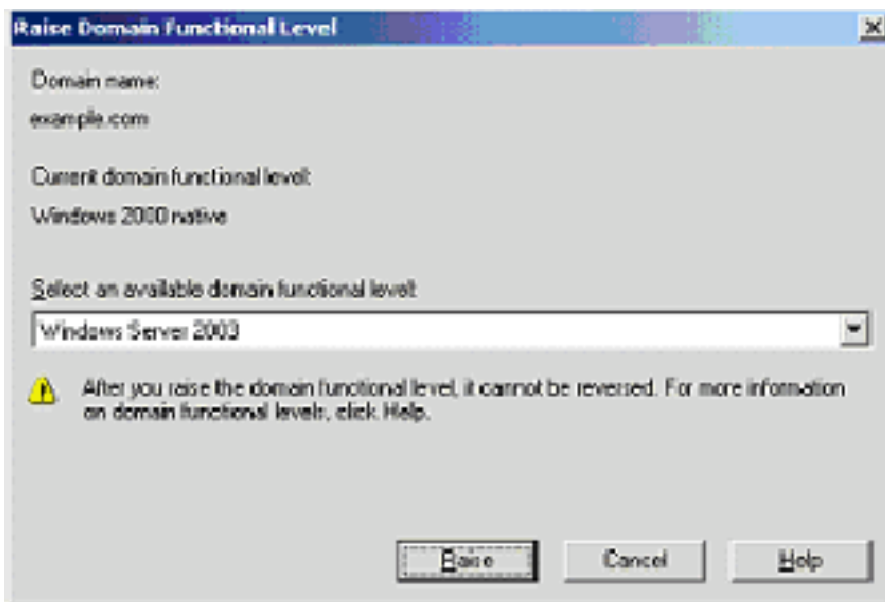


14. Na página Concluindo o Assistente de Instalação do Active Directory, clique em **Concluir**.
15. Quando solicitado a reiniciar o computador, clique em **Reiniciar agora**.

[Passo 3: Aumente o nível funcional do domínio](#)

Conclua estes passos:

1. Abra o snap-in Domínios e Confianças do Active Directory na pasta **Ferramentas Administrativas**(Iniciar > Ferramentas Administrativas > Domínios e Confianças do Active Directory) e clique com o botão direito do mouse no computador de domínio **DC_CA.wireless demo.local**.
2. Clique em **Aumentar o nível funcional do domínio** e selecione **Windows Server 2003** na página Aumentar o nível funcional do



domínio.

3. Clique em **Aumentar**, clique em **OK** e, em seguida, clique em **OK** novamente.

[Passo 4: Instalar e configurar o DHCP](#)

Conclua estes passos:

1. Instale o DHCP (Dynamic Host Configuration Protocol) como um componente do Serviço de Rede usando **Adicionar ou Remover Programas** no Painel de Controle.
2. Abra o snap-in DHCP na pasta Ferramentas Administrativas (**Iniciar > Programas > Ferramentas Administrativas > DHCP**) e realce o servidor DHCP, **DC_CA.wirelessdemo.local**.
3. Clique em **Ação** e, em seguida, clique em **Autorizar** para autorizar o serviço DHCP.
4. Na árvore do console, clique com o botão direito do mouse em **DC_CA.wirelessdemo.local** e clique em **Novo escopo**.
5. Na página Bem-vindo do assistente Novo escopo, clique em **Avançar**.
6. Na página Nome do escopo, digite **CorpNet** no campo Nome.

New Scope Wizard

Scope Name

You have to provide an identifying scope name. You also have the option of providing a description.



Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.

Name:

Description:

7. Clique em **Avançar** e preencha estes parâmetros: Endereço IP inicial—172.16.100.1 Endereço IP final—172.16.100.254 Comprimento—24 Máscara de sub-rede—255.255.255.0

New Scope Wizard

IP Address Range

You define the scope address range by identifying a set of consecutive IP addresses.



Enter the range of addresses that the scope distributes.

Start IP address:

End IP address:

A subnet mask defines how many bits of an IP address to use for the network/subnet IDs and how many bits to use for the host ID. You can specify the subnet mask by length or as an IP address.

Length:

Subnet mask:

< Back

Next >

Cancel

8. Clique em **Next** e digite **172.16.100.1** para o endereço IP inicial e **172.16.100.100** para o endereço IP final ser excluído. Em seguida, clique em Avançar. Isso reserva os endereços IP no intervalo de 172.16.100.1 a 172.16.100.100. Esses endereços IP reservados não são alocados pelo servidor DHCP.

New Scope Wizard

Add Exclusions

Exclusions are addresses or a range of addresses that are not distributed by the server.



Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.

Start IP address:

End IP address:

Excluded address range:

9. Na página Duração da concessão, clique em **Avançar**.

10. Na página Configurar opções de DHCP, escolha **Sim, desejo configurar essas opções agora** e clique em **Avançar**.

New Scope Wizard

Configure DHCP Options

You have to configure the most common DHCP options before clients can use the scope.



When clients obtain an address, they are given DHCP options such as the IP addresses of routers (default gateways), DNS servers, and WINS settings for that scope.

The settings you select here are for this scope and override settings configured in the Server Options folder for this server.

Do you want to configure the DHCP options for this scope now?

- Yes, I want to configure these options now
- No, I will configure these options later

< Back

Next >

Cancel

11. Na página Router (Default Gateway) (Roteador (Gateway padrão)), adicione o endereço padrão do roteador **172.16.100.1** e clique em **Next (Avançar)**.

Router (Default Gateway)

You can specify the routers, or default gateways, to be distributed by this scope.



To add an IP address for a router used by clients, enter the address below.

IP address:

Add

172.16.100.1

Remove

Up

Down

< Back

Next >

Cancel

12. Na página Nome de domínio e Servidores DNS, digite **wireless demo.local** no campo Domínio pai, digite **172.16.100.26** no campo Endereço IP e clique em **Adicionar** e em **Avançar**.

New Scope Wizard

Domain Name and DNS Servers

The Domain Name System (DNS) maps and translates domain names used by clients on your network.



You can specify the parent domain you want the client computers on your network to use for DNS name resolution.

Parent domain:

To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.

Server name:

Resolve

IP address:

172.16.100.26

Add

Remove

Up

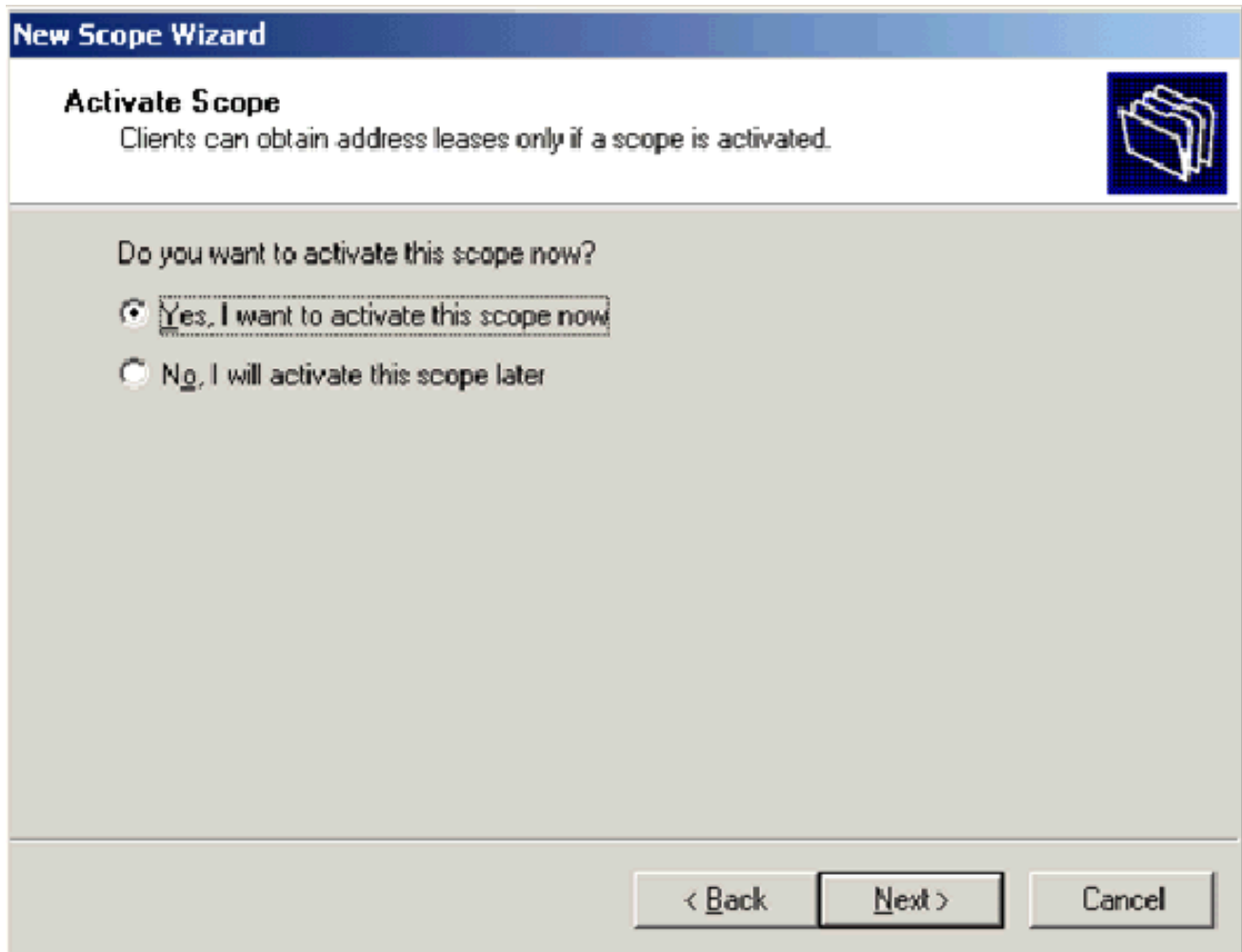
Down

< Back

Next >

Cancel

13. Na página Servidores WINS, clique em **Avançar**.
14. Na página Ativar escopo, escolha **Sim, desejo ativar esse escopo agora** e clique em **Avançar**.



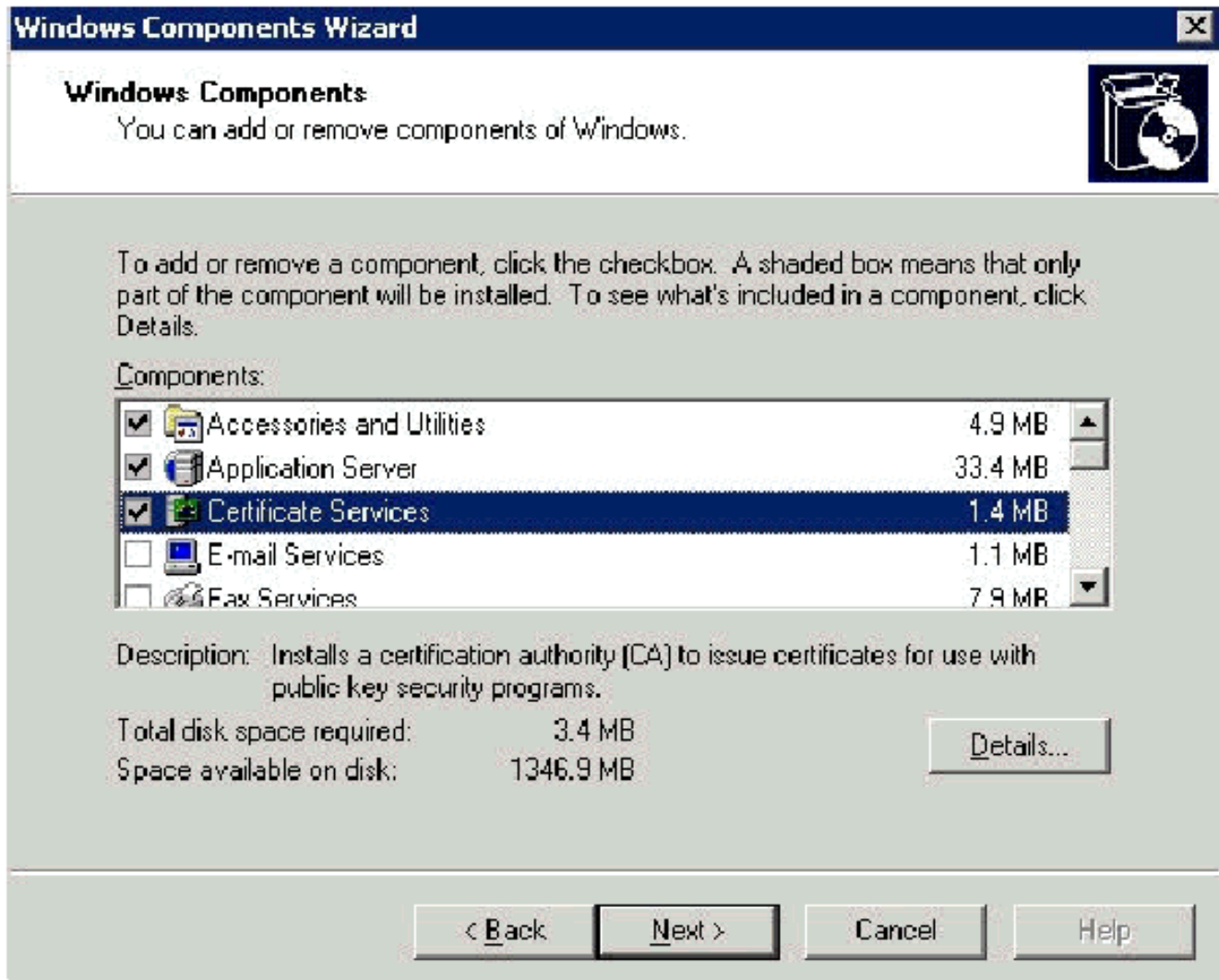
15. Na página Completing the New Scope Wizard, clique em **Finish**.

[Passo 5: Instalar serviços de certificado](#)

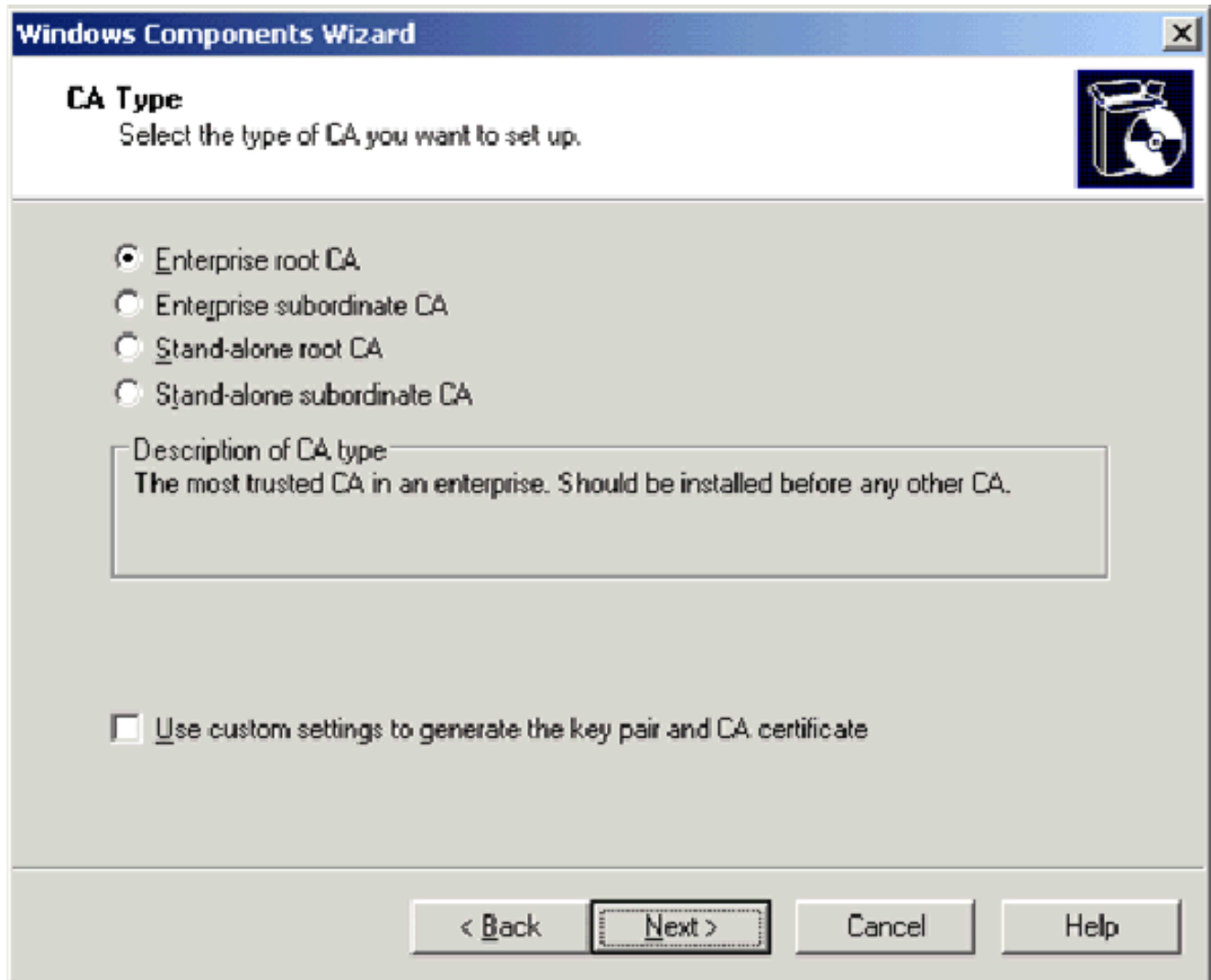
Conclua estes passos:

Observação: o IIS deve ser instalado antes da instalação dos Serviços de Certificado e o usuário deve fazer parte da OU do Administrador Corporativo.

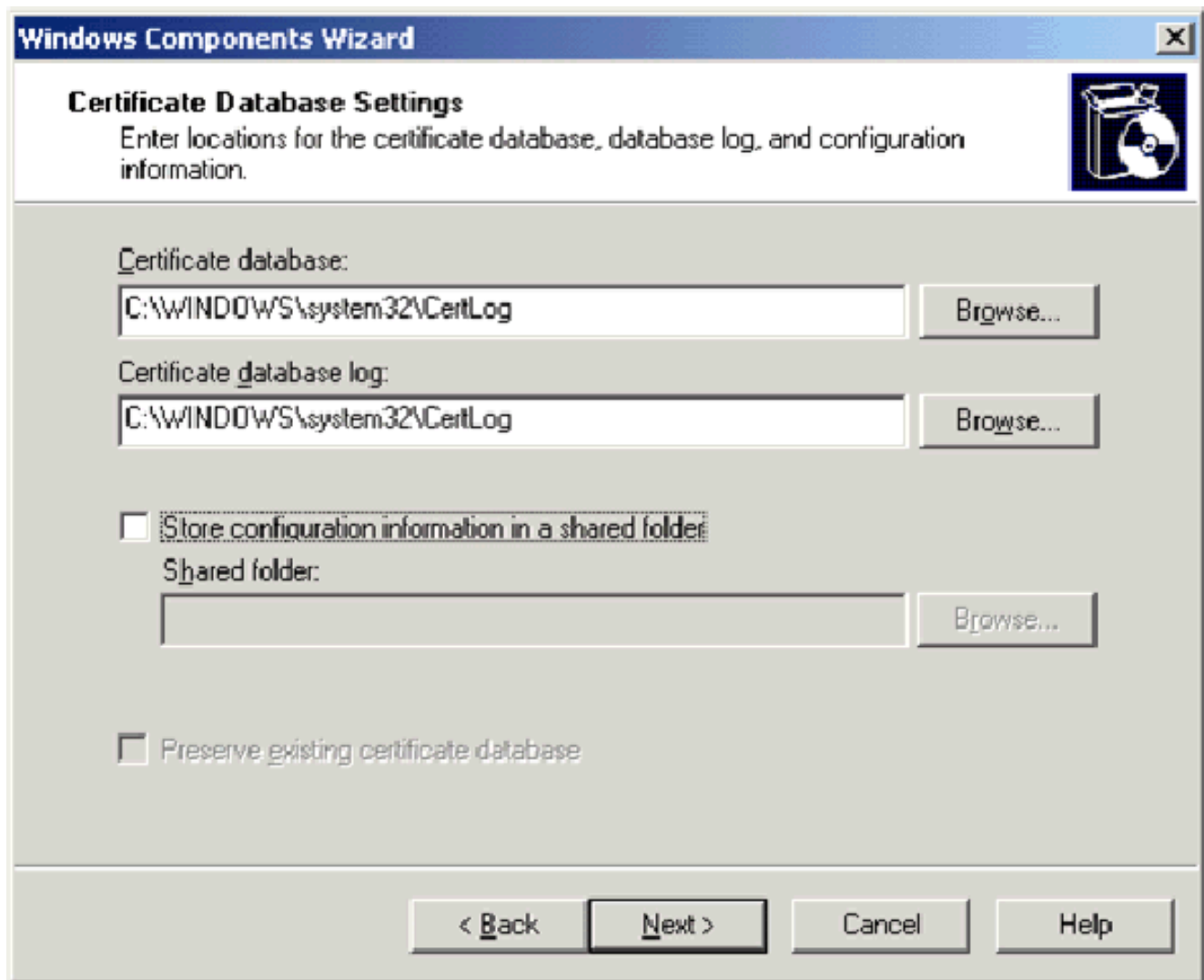
1. No Painel de controle, abra **Adicionar ou remover programas** e clique em **Adicionar/remover componentes do Windows**.
2. Na página Assistente de componentes do Windows, escolha **Serviços de certificado** e clique em **Avançar**.



3. Na página Tipo de CA, escolha **AC raiz Enterprise** e clique em **Avançar**.



4. Na página CA Identifying information (Informações de identificação da CA), digite **wireless democa** no Common name (Nome comum desta CA). Você pode inserir os outros detalhes opcionais e clicar em **Avançar**. Aceite os padrões na página Configurações do banco de dados de certificado.

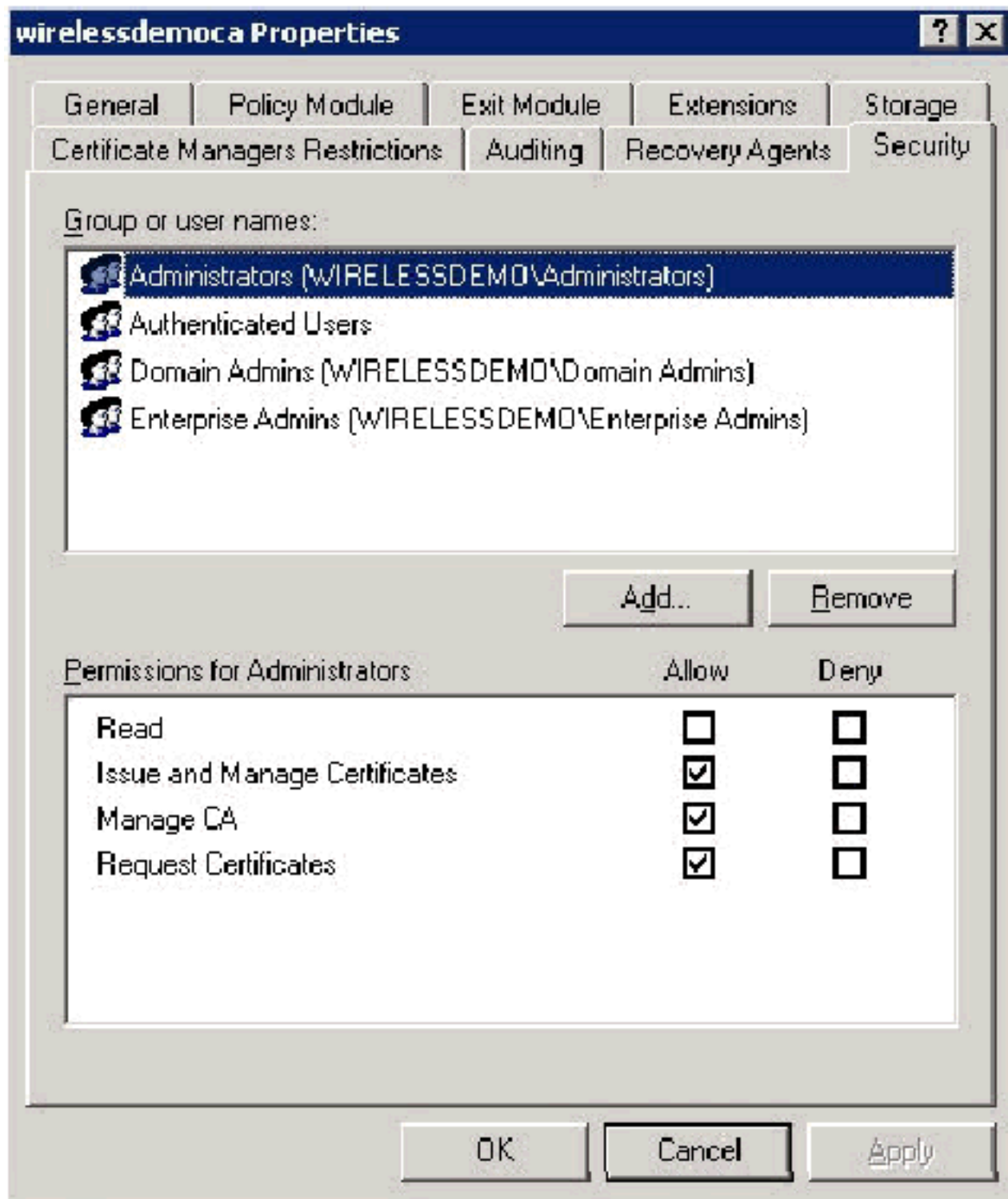


5. Clique em Next. Após concluir a instalação, clique em **Concluir**.
6. Clique em **OK** depois de ler o aviso sobre a instalação do IIS.

[Passo 6: Verificar permissões de administrador para certificados](#)

Conclua estes passos:

1. Escolha **Iniciar > Ferramentas Administrativas > Autoridade de Certificação**.
2. Clique com o botão direito do mouse em **wireless democa CA** e clique em **Propriedades**.
3. Na guia **Segurança**, clique em **Administradores** na lista Nomes de grupo ou usuário.
4. Na lista **Permissões** ou **Administradores**, verifique se estas opções estão definidas como **Permitir**: Emitir e gerenciar certificados Gerenciar CASolicitar certificados Se qualquer um deles estiver definido como **Negar** ou não estiver selecionado, defina a permissão como **Permitir**.



5. Clique em **OK** para fechar a caixa de diálogo Propriedades da CA sem fio e feche a Autoridade de Certificação.

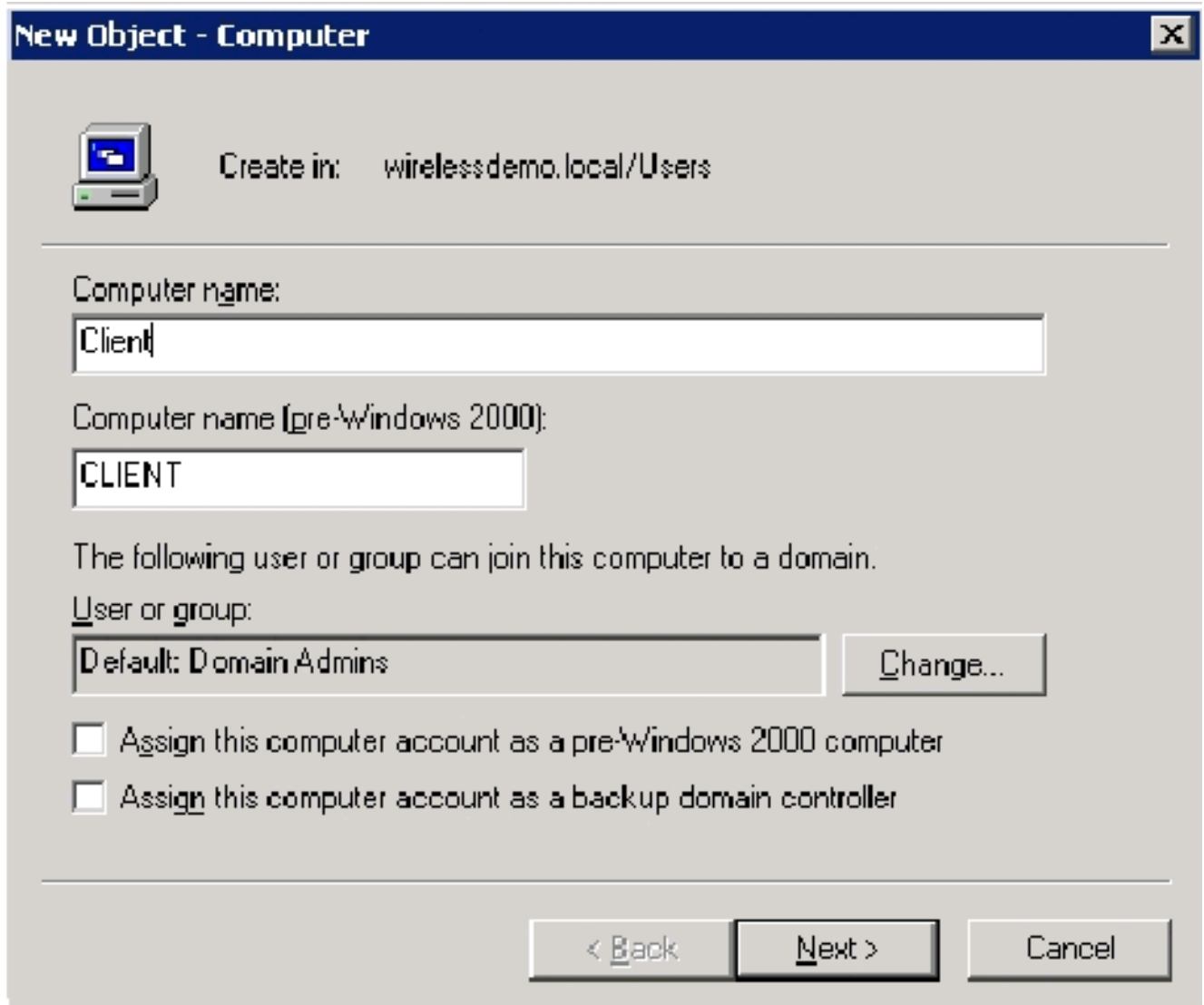
[Passo 7: Adicionar computadores ao domínio](#)

Conclua estes passos:

Observação: se o computador já estiver adicionado ao domínio, vá para [Adicionar usuários ao domínio](#).

1. Abra o snap-in Utilizadores e Computadores do Active Directory.
2. Na árvore do console, expanda **wireless demo.local**.
3. Clique com o botão direito do mouse em **Usuários**, clique em **Novo** e clique em **Computador**.

4. Na caixa de diálogo Novo objeto - computador, digite o nome do computador no campo Nome do computador e clique em **Avançar**. Este exemplo usa o nome do computador **Cliente**.



5. Na caixa de diálogo Gerenciado, clique em **Avançar**.
6. Na caixa de diálogo Novo objeto-computador, clique em **Concluir**.
7. Repita as etapas de 3 a 6 para criar contas de computador adicionais.

[Passo 8: Permitir acesso sem fio a computadores](#)

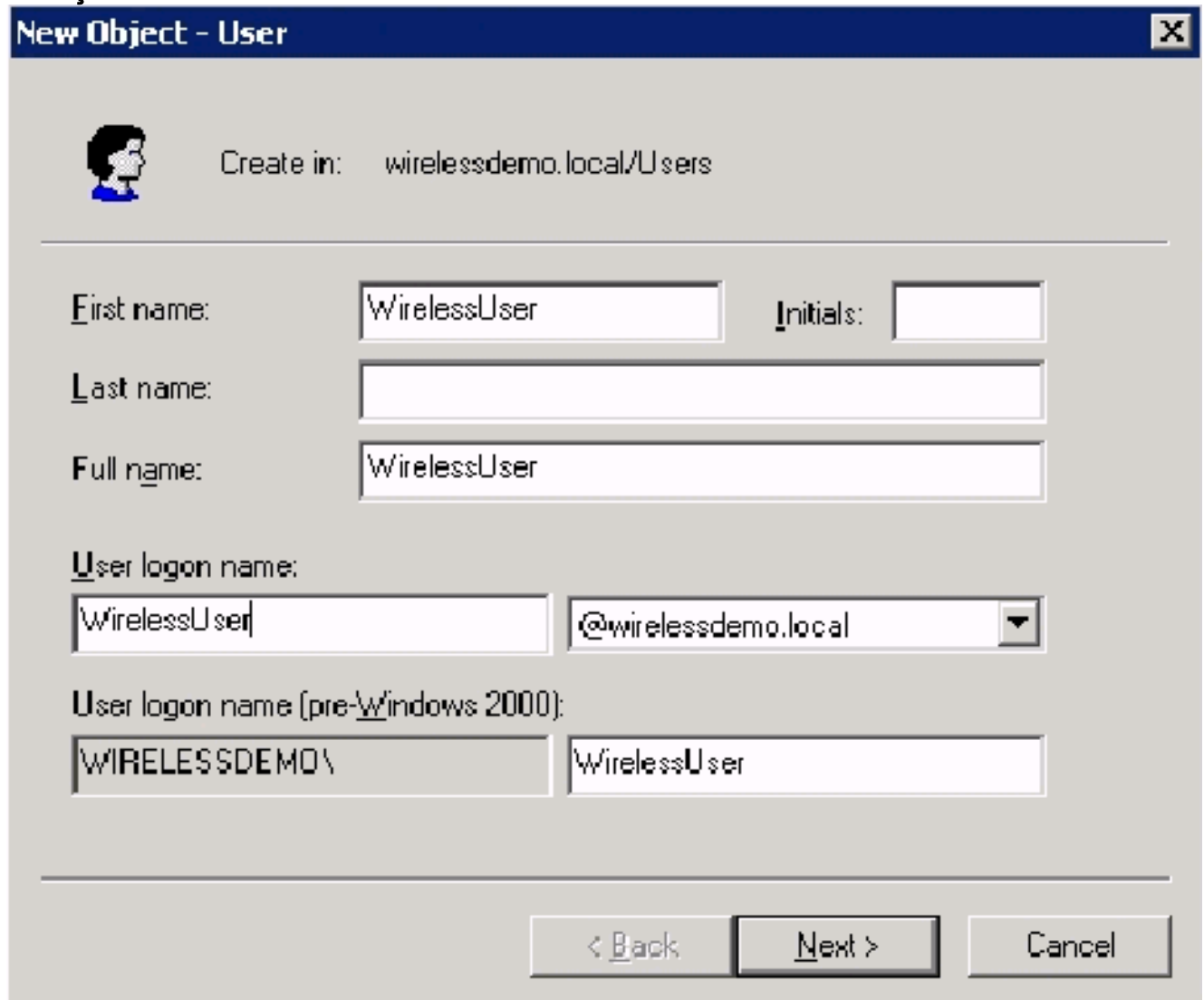
Conclua estes passos:

1. Na árvore de console Usuários e Computadores do Active Directory, clique na pasta **Computadores** e clique com o botão direito do mouse no computador para o qual deseja atribuir acesso sem fio. Este exemplo mostra o procedimento com o computador **CLIENTE** que você adicionou na etapa 7.
2. Clique em **Propriedades** e vá para a guia Discar.
3. Escolha **Permitir acesso** e clique em **OK**.

[Etapa 9: Adicionar usuários ao domínio](#)

Conclua estes passos:

1. Na árvore de console Usuários e Computadores do Ative Directory, clique com o botão direito do mouse em **Usuários**, clique em **Novo** e, em seguida, clique em **Usuário**.
2. Na caixa de diálogo Novo objeto - usuário, digite **WirelessUser** no campo Nome e digite **WirelessUser** no campo Nome de logon do usuário e clique em **Avançar**.



New Object - User

Create in: wirelessdemo.local/Users

First name: Initials:

Last name:

Full name:

User logon name:

User logon name (pre-Windows 2000):

< Back Next > Cancel

3. Na caixa de diálogo Novo objeto - usuário, digite uma senha de sua escolha nos campos Senha e Confirmar senha. Desmarque a caixa de seleção **Usuário deve alterar a senha no próximo logon** e clique em **Avançar**.

New Object - User

Create in: wirelessdemo.local/Users

Password: [.....]

Confirm password: [.....]

User must change password at next logon

User cannot change password

Password never expires

Account is disabled

< Back Next > Cancel

4. Na caixa de diálogo Novo objeto - usuário, clique em **Concluir**.
5. Repita as etapas de 2 a 4 para criar contas de usuário adicionais.

[Etapa 10: Permitir acesso sem fio aos usuários](#)

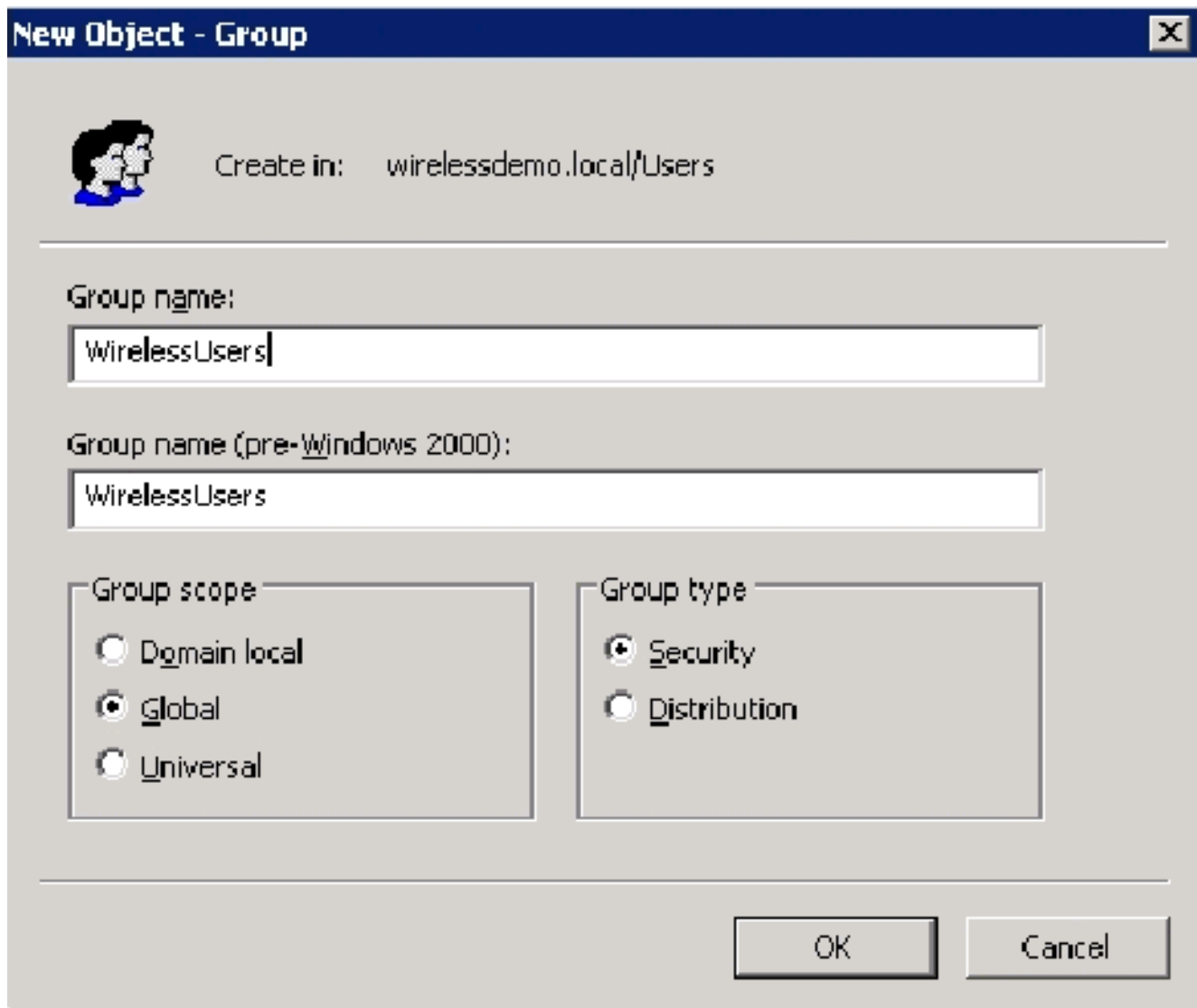
Conclua estes passos:

1. Na árvore de console Usuários e Computadores do Ative Directory, clique na pasta **Usuários**, clique com o botão direito do mouse em **WirelessUser**, clique em **Propriedades** e vá para a guia **Discar**.
2. Escolha **Permitir acesso** e clique em **OK**.

[Etapa 11: Adicionar grupos ao domínio](#)

Conclua estes passos:

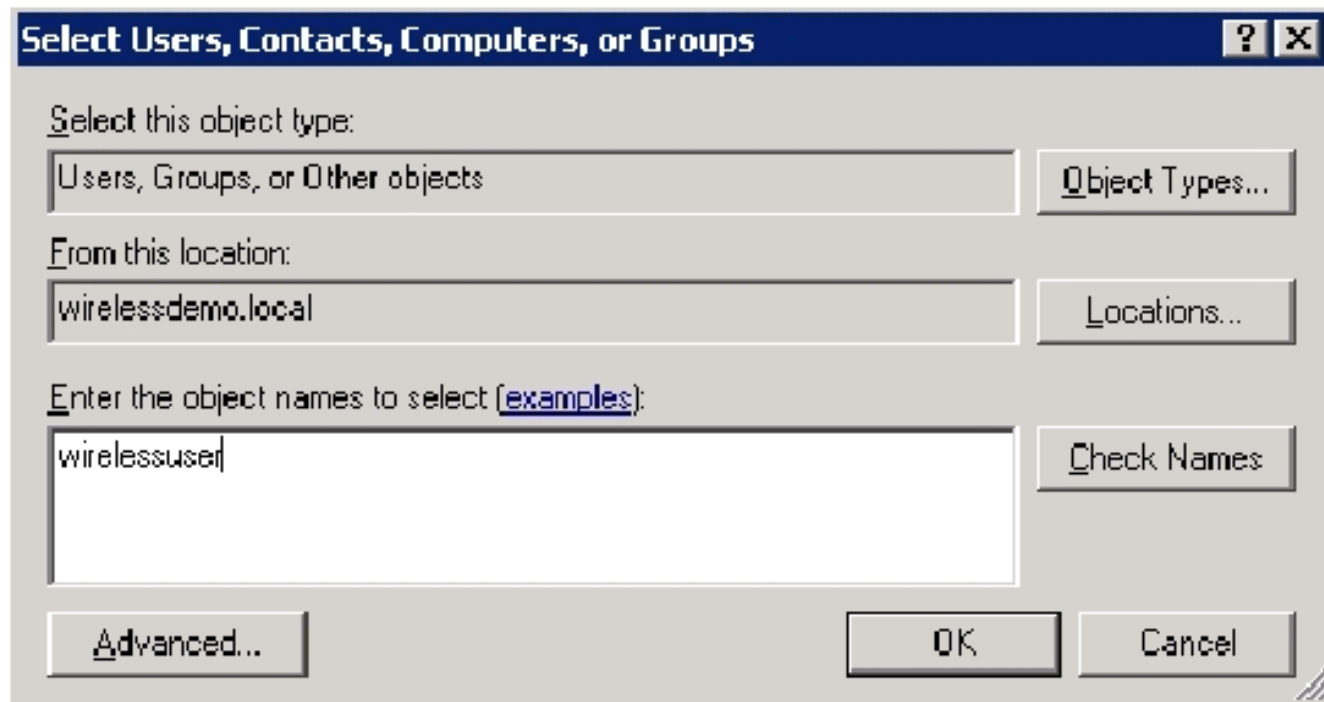
1. Na árvore de console Usuários e Computadores do Ative Directory, clique com o botão direito do mouse em **Usuários**, clique em **Novo** e em **Grupo**.
2. Na caixa de diálogo Novo objeto - grupo, digite o nome do grupo no campo Nome do grupo e clique em **OK**. Este documento usa o nome de grupo **WirelessUsers**.



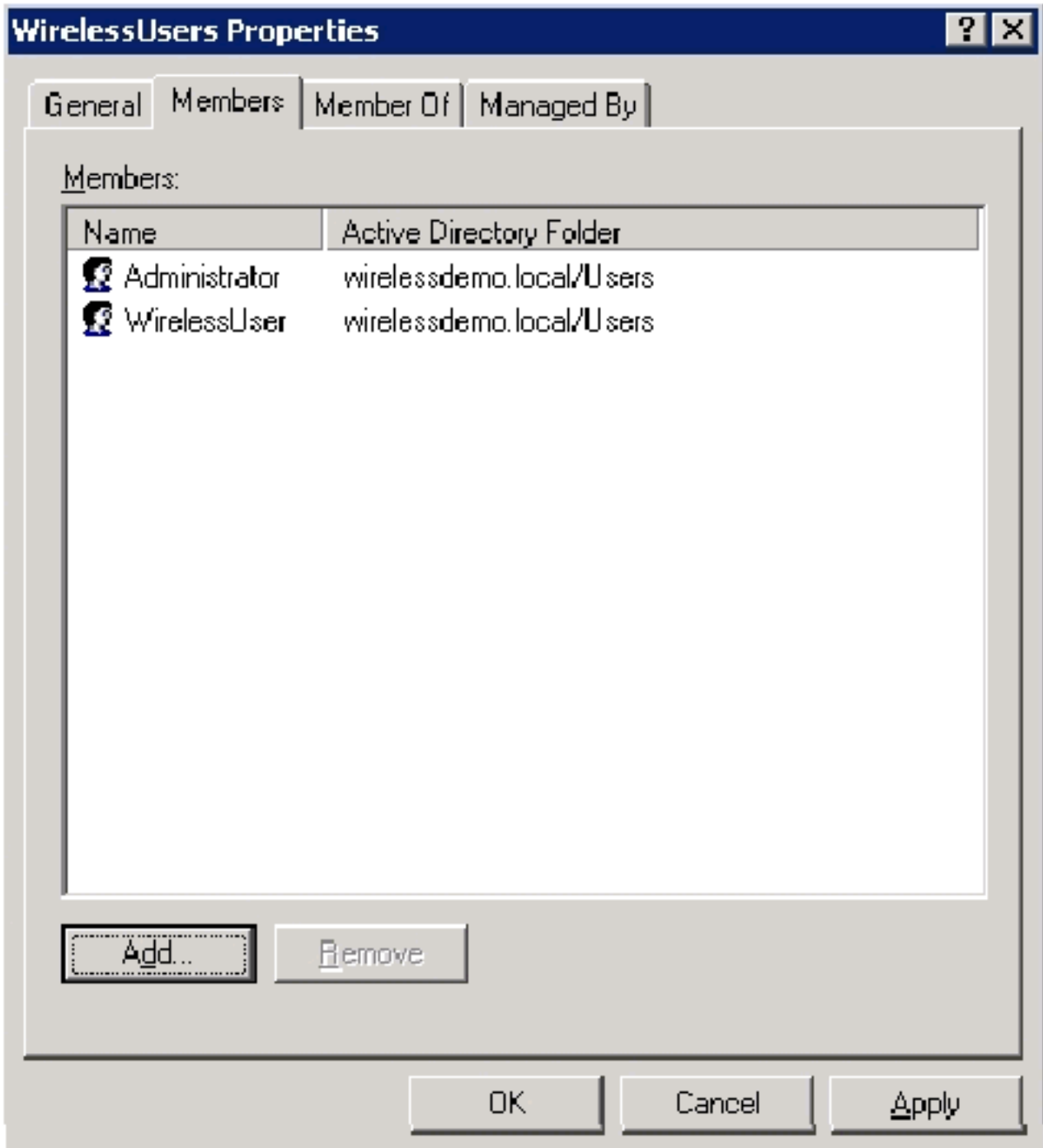
[Etapa 12: Adicionar usuários ao grupo WirelessUsers](#)

Conclua estes passos:

1. No painel de detalhes de Usuários e Computadores do Active Directory, clique duas vezes em Grupo **Usuários Sem Fio**.
2. Vá até a guia Membros e clique em **Adicionar**.
3. Na caixa de diálogo Selecionar usuários, contatos, computadores ou grupos, digite o nome dos usuários que deseja adicionar ao grupo. Este exemplo mostra como adicionar o usuário **wireless** ao grupo. Click **OK**.



4. Na caixa de diálogo Vários nomes encontrados, clique em **OK**. A conta de usuário WirelessUser é adicionada ao grupo WirelessUsers.

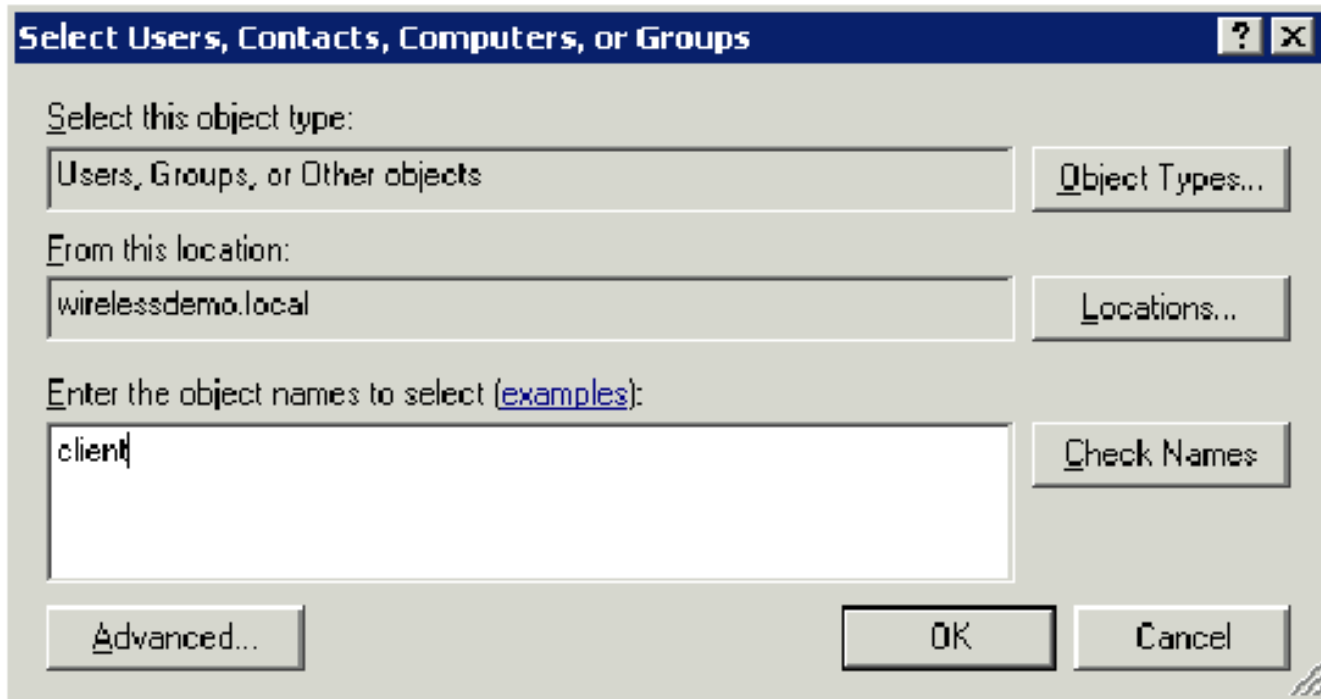


5. Clique em **OK** para salvar as alterações no grupo WirelessUsers.
6. Repita esse procedimento para adicionar mais usuários ao grupo.

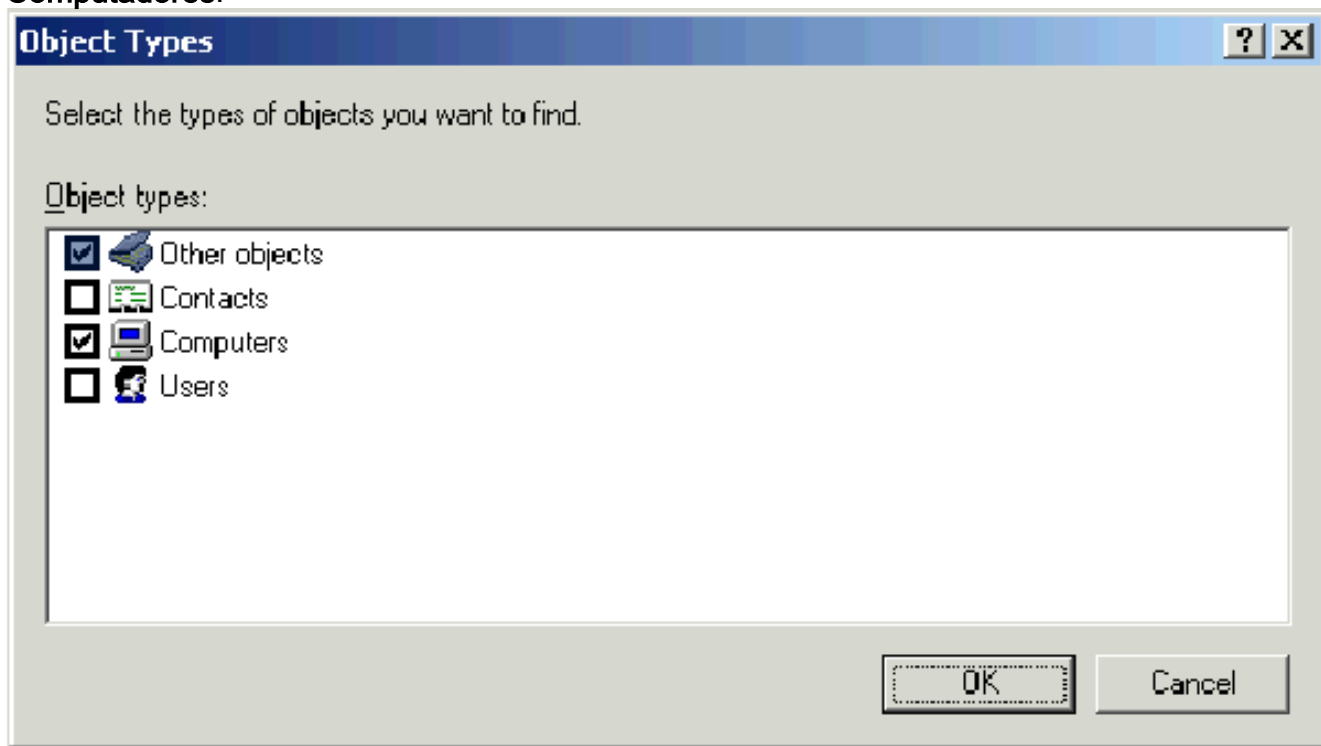
[Passo 13: Adicionar computadores clientes ao grupo WirelessUsers](#)

Conclua estes passos:

1. Repita as etapas 1 e 2 na seção [Adicionar usuários ao grupo de usuários sem fio](#) deste documento
2. Na caixa de diálogo Selecionar usuários, contatos ou computadores, digite o nome do computador que deseja adicionar ao grupo. Este exemplo mostra como adicionar o computador chamado **cliente** ao grupo.



3. Clique em **Tipos de objeto**, desmarque a caixa de seleção **Usuários** e marque **Computadores**.



4. Clique em **OK** duas vezes. A conta do computador CLIENT é adicionada ao grupo WirelessUsers.
5. Repita o procedimento para adicionar mais computadores ao grupo.

[Configuração do Windows Standard 2003 com Cisco Secure ACS 4.0](#)

O Cisco Secure ACS é um computador que executa o Windows Server 2003 com SP1, Standard Edition, que fornece autenticação e autorização RADIUS para o controlador. Conclua os procedimentos nesta seção para configurar o ACS como um servidor RADIUS:

Instalação e configuração básicas

Conclua estes passos:

1. Instale o Windows Server 2003 com SP1, Standard Edition, como um **servidor membro** chamado **ACS** no domínio **wireless demo.local**. **Observação:** o nome do servidor ACS é exibido como **cisco_w2003** nas configurações restantes. Substitua o ACS ou o **cisco_w2003** na configuração restante do laboratório.
2. Para a conexão de área local, configure o protocolo TCP/IP com o endereço IP de **172.16.100.26**, a máscara de sub-rede de **255.255.255.0** e o endereço IP do servidor DNS de **127.0.0.1**.

Instalação do Cisco Secure ACS 4.0

Observação: consulte o [Guia de Instalação do Cisco Secure ACS 4.0 para Windows](#) para obter mais informações sobre como configurar o Cisco Secure ACS 4.0 para Windows.

Conclua estes passos:

1. Usando uma conta de administrador de domínio, faça login no computador chamado ACS para Cisco Secure ACS. **Observação:** somente as instalações executadas no computador onde você instala o Cisco Secure ACS são suportadas. As instalações remotas executadas com o Windows Terminal Services ou produtos como Virtual Network Computing (VNC), não são testadas e não são suportadas.
2. Insira o CD Cisco Secure ACS em uma unidade de CD-ROM no computador.
3. Se a unidade de CD-ROM suportar o recurso de execução automática do Windows, a caixa de diálogo Cisco Secure ACS for Windows Server será exibida. **Observação:** se o computador não tiver um service pack necessário instalado, uma caixa de diálogo será exibida. Os service packs do Windows podem ser aplicados antes ou depois da instalação do Cisco Secure ACS. Você pode continuar com a instalação, mas o service pack necessário deve ser aplicado depois que a instalação for concluída. Caso contrário, o Cisco Secure ACS pode não funcionar de forma confiável.
4. Execute uma destas tarefas: Se a caixa de diálogo Cisco Secure ACS para Windows Server for exibida, clique em **Instalar**. Se a caixa de diálogo Cisco Secure ACS for Windows Server não for exibida, execute **setup.exe**, localizado no diretório raiz do CD Cisco Secure ACS.
5. A caixa de diálogo Cisco Secure ACS Setup (Configuração do Cisco Secure ACS) exibe o contrato de licença de software.
6. Leia o contrato de licença de software. Se aceitar o contrato de licença de software, clique em **Aceitar**. A caixa de diálogo Bem-vindo exibe informações básicas sobre o programa de configuração.
7. Depois de ler as informações na caixa de diálogo Bem-vindo, clique em **Avançar**.
8. A caixa de diálogo Antes de começar lista os itens que você deve concluir antes de continuar com a instalação. Se tiver concluído todos os itens listados na caixa de diálogo Antes de começar, marque a caixa correspondente para cada item e clique em **Avançar**. **Observação:** se você não tiver concluído todos os itens listados na caixa Antes de começar, clique em **Cancelar** e em **Sair da configuração**. Depois de concluir todos os itens listados na caixa de diálogo Antes de começar, reinicie a instalação.
9. A caixa de diálogo Escolher local de destino é exibida. Em Pasta de destino, o local de

instalação é exibido. Esta é a unidade e o caminho onde o programa de configuração instala o Cisco Secure ACS.

10. Para alterar o local de instalação, faça o seguinte:Clique em **Procurar**. A caixa de diálogo Escolher pasta é exibida. A caixa Caminho contém o local de instalação.Alterar o local de instalação. Você pode digitar o novo local na caixa Caminho ou usar as listas Unidades e Diretórios para selecionar um novo drive e diretório. O local de instalação deve estar em uma unidade local do computador.**Observação:** não especifique um caminho que contenha um caractere percentual, "%". Se você fizer isso, a instalação pode parecer continuar corretamente, mas falha antes de ser concluída.Click **OK**.**Observação:** se você especificou uma pasta que não existe, o programa de configuração exibe uma caixa de diálogo para confirmar a criação da pasta. Para continuar, clique em **Sim**.
11. Na caixa de diálogo Escolher local de destino, o novo local de instalação aparece em Pasta de destino.
12. Clique em Next.
13. A caixa de diálogo Authentication Database Configuration lista opções para autenticar usuários. Você pode autenticar somente com o banco de dados de usuários do Cisco Secure ou também com um banco de dados de usuários do Windows.**Observação:** depois de instalar o Cisco Secure ACS, você pode configurar o suporte de autenticação para todos os tipos de banco de dados de usuário externo além dos bancos de dados de usuário do Windows.
14. Para autenticar usuários somente com o banco de dados de usuários do Cisco Secure, escolha a opção **Verificar somente o banco de dados do Cisco Secure ACS**.
15. Se você quiser autenticar usuários com um banco de dados de usuário do Windows Security Access Manager (SAM) ou um banco de dados de usuário do Active Directory, além do banco de dados de usuário do Cisco Secure, faça o seguinte:Escolha a opção **Também verificar Banco de Dados de Usuário do Windows**.A caixa de seleção **Sim, consulte a opção "Conceder permissão de discagem ao usuário"** se torna disponível.**Observação:** a caixa de seleção "Conceder permissão de discagem ao usuário" se aplica a todas as formas de acesso controladas pelo Cisco Secure ACS, não apenas ao acesso de discagem. Por exemplo, um usuário que acessa a rede através de um túnel VPN não está discando para um servidor de acesso à rede. No entanto, se a caixa **Sim, consulte "Conceder permissão de discagem ao usuário"** estiver marcada, o Cisco Secure ACS aplicará as permissões de discagem de usuário do Windows para determinar se o usuário deve conceder acesso à rede.Se quiser permitir acesso a usuários autenticados por um banco de dados de usuários de domínio do Windows somente quando eles tiverem permissão de discagem em sua conta do Windows, marque a caixa **Sim, consulte "Conceder permissão de discagem ao usuário"**.
16. Clique em Next.
17. O programa de configuração instala o Cisco Secure ACS e atualiza o registro do Windows.
18. A caixa de diálogo Opções avançadas lista vários recursos do Cisco Secure ACS que não estão habilitados por padrão. Para obter mais informações sobre esses recursos, consulte o [Guia do usuário do Cisco Secure ACS for Windows Server, versão 4.0](#).**Observação:** os recursos listados aparecem na interface HTML do Cisco Secure ACS somente se você os habilitar. Após a instalação, você pode ativá-las ou desativá-las na página Opções avançadas na seção Configuração da interface.
19. Para cada recurso que deseja habilitar, marque a caixa correspondente.
20. Clique em Next.
21. A caixa de diálogo Monitoramento de serviço ativo é exibida.**Observação:** após a

instalação, você pode configurar os recursos de monitoramento de serviço ativo na página Gerenciamento de serviço ativo na seção Configuração do sistema.

22. Se você deseja que o Cisco Secure ACS monitore os serviços de autenticação de usuário, marque a caixa **Enable Login Monitoring**. Na lista Script a executar, escolha a opção que deseja aplicar em caso de falha de serviço de autenticação: **Nenhuma ação corretiva** — O Cisco Secure ACS não executa um script. **Observação:** essa opção é útil se você habilitar notificações por email de eventos. **Reinicialização** — O Cisco Secure ACS executa um script que reinicializa o computador que executa o Cisco Secure ACS. **Reiniciar tudo** — O Cisco Secure ACS reinicia todos os serviços do Cisco Secure ACS. **Reiniciar RADIUS/TACACS+** — O Cisco Secure ACS reinicia somente os serviços RADIUS e TACACS+.
23. Se quiser que o Cisco Secure ACS envie uma mensagem de e-mail quando o monitoramento de serviço detectar um evento, marque a caixa **Notificação por e-mail**.
24. Clique em Next.
25. A caixa de diálogo Senha de criptografia do banco de dados é exibida. **Observação:** a senha de criptografia de banco de dados é criptografada e armazenada no registro ACS. Você pode precisar reutilizar essa senha quando surgirem problemas críticos e o banco de dados precisar ser acessado manualmente. Mantenha essa senha em mãos para que o Suporte Técnico possa obter acesso ao banco de dados. A senha pode ser alterada a cada período de expiração.
26. Insira uma senha para criptografia do banco de dados. A senha precisa ter pelo menos oito caracteres e deve conter caracteres e dígitos. Não há caracteres inválidos. Clique em Next.
27. O programa de configuração é concluído e a caixa de diálogo Cisco Secure ACS Service Initiation é exibida.
28. Para cada opção Cisco Secure ACS Services Initiation desejada, marque a caixa correspondente. As ações associadas às opções ocorrem depois que o programa de configuração é concluído. **Sim, desejo iniciar o Cisco Secure ACS Service agora** — Inicia os serviços do Windows que compõem o Cisco Secure ACS. Se você não selecionar essa opção, a interface HTML do Cisco Secure ACS não estará disponível a menos que você reinicialize o computador ou inicie o serviço CSAdmin. **Sim, desejo que a Instalação inicie o Cisco Secure ACS Administrator do meu navegador após a instalação** — Abre a interface HTML do Cisco Secure ACS no navegador da Web padrão para a conta de usuário atual do Windows. **Sim, desejo ver o arquivo Readme** — Abre o arquivo README.TXT no Bloco de Notas do Windows.
29. Clique em Next.
30. Se você selecionou uma opção, os serviços do Cisco Secure ACS são iniciados. A caixa de diálogo Setup Complete (Instalação concluída) exibe informações sobre a interface HTML do Cisco Secure ACS.
31. Clique em Finish. **Observação:** o restante da configuração é documentado na seção para o tipo de EAP configurado.

[Configuração do controlador Cisco LWAPP](#)

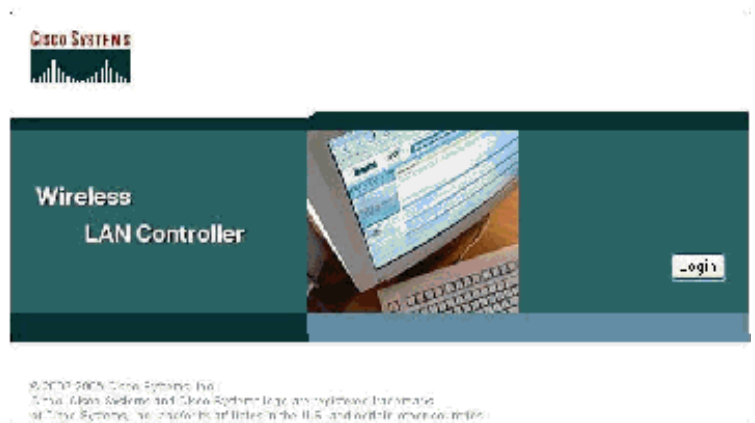
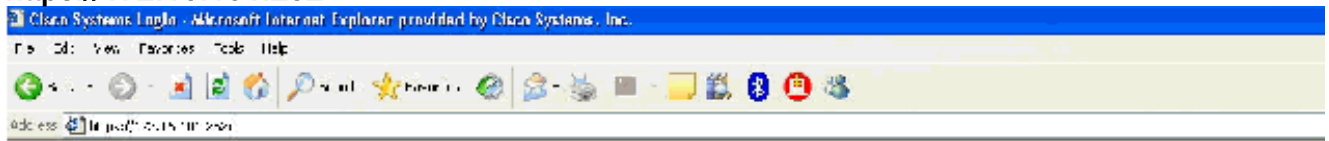
[Crie a configuração necessária para WPA2/WPA](#)

Conclua estes passos:

Observação: a suposição é que o controlador tem conectividade básica com a rede e a

alcançabilidade de IP com a interface de gerenciamento é bem-sucedida.

1. Faça login no controlador navegando até <https://172.16.101.252>.



2. Clique em login.
3. Faça login com o usuário padrão **admin** e a senha padrão **admin**.
4. Crie o mapeamento da VLAN da interface no menu Controller.
5. Clique em **Interfaces**.
6. Clique em **New**.
7. No campo Nome da interface, digite **Funcionário**. (Esse campo pode ser qualquer valor que você desejar.)
8. No campo ID da VLAN, digite **20**. (Esse campo pode ser qualquer VLAN transportada na rede.)
9. Clique em Apply.
10. Configure as informações conforme mostrado nesta janela Interfaces > Edit.

Address: https://172.16.101.252/screens/frameset.html

CISCO SYSTEMS

MONITOR | WLANs | CONTROLLER | WIRELESS | SECURITY

Controller

General

Inventory

Interfaces

Internal DHCP Server

Mobility Management

Mobility Groups

Mobility Statistics

Ports

Master Controller Mode

Network Time Protocol

QoS Profiles

Interfaces > Edit

General Information

Interface Name: employee

Interface Address

VLAN Identifier: 20

IP Address: 172.16.100.1

Netmask: 255.255.255.0

Gateway: 172.16.100.1

Physical Information

Port Number: 1

DHCP Information

Primary DHCP Server: 172.16.100.25

Secondary DHCP Server: 0.0.0.0

Access Control List

ACL Name: none

Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients.

11. Clique em Apply.
12. Clique em **WLAN**.
13. Clique em **New**.
14. No campo WLAN SSID, digite **Employee**.
15. Clique em Apply.
16. Configure as informações conforme mostrado nesta janela WLANs > Editar. **Observação:** WPA2 é o método de criptografia de Camada 2 escolhido para este laboratório. Para permitir que clientes WPA com TKIP-MIC se associem a este SSID, você também pode marcar as caixas **modo de compatibilidade WPA** e **Permitir clientes TKIP WPA2** ou os clientes que não suportam o método de criptografia AES 802.11i.

WLAN6 > Edit

WLAN ID	1
WLAN SSID	Employee

General Policies

Radius Policy	All
Admin Status	<input checked="" type="checkbox"/> Enabled
Session Timeout (secs)	1800
Quality of Services (QoS)	Silver (best effort)
WMM Policy	Disabled
7920 Pkts Support	<input type="checkbox"/> Client CAC Limit <input type="checkbox"/> AP CAC Limit
Broadcast SSID	<input checked="" type="checkbox"/> Enabled
Allow PPP Override	<input type="checkbox"/> Enabled
Client Exclusion	<input checked="" type="checkbox"/> Enabled ** 60 Timeout Value (secs)
DHCP Server	<input type="checkbox"/> Override
DHCP Addr. Assignment	<input checked="" type="checkbox"/> Required
Interface Name	employee

Security Policies

Layer 2 Security	WPA2
	<input type="checkbox"/> MAC Filtering
Layer 3 Security	None
	<input type="checkbox"/> Web Policy **

* Web Policy cannot be used in combination with IPsec and L2TP.

** When client exclusion is enabled, a timeout value of zero means infinity (will require administrative override to reset excluded clients)

Radius Servers

	Authentication Servers	Accounting Servers
Server 1	IP:172.16.100.25, Port:1812	none
Server 2	none	none
Server 3	none	none

WPA2 Parameters

WPA Compatibility Mode	<input checked="" type="checkbox"/> Enable
Allow WPA2 TKIP Clients	<input checked="" type="checkbox"/> Enable
Pre-Shared Key	<input type="checkbox"/> Enabled (WPA2 passphrase has been set)

17. Clique em **Apply**.
18. Clique no menu **Segurança** e adicione o servidor RADIUS.
19. Clique em **New**.
20. Adicione o endereço IP do servidor RADIUS (172.16.100.25) que é o servidor ACS configurado anteriormente.
21. Verifique se a chave compartilhada corresponde ao cliente AAA configurado no servidor ACS.
22. Clique em **Apply**.



Security

AAA

- General
- RADIUS Authentication
- RADIUS Accounting
- Local Net Users
- MAC Filtering
- Disabled Clients
- User Login Policies
- AP Policies

Access Control Lists

Web Auth Certificate

Wireless Protection Policies

- Trusted AP Policies
- Rogue Policies
- Standard Signatures
- Custom Signatures
- Client Exclusion Policies
- AP Authentication

RADIUS Authentication Servers > New

Server Index (Priority)	1 <input type="button" value="v"/>
Server IP Address	<input type="text" value="172.16.100.25"/>
Keys Format	ASCII <input type="button" value="v"/>
Shared Secret	<input type="password" value="••••••"/>
Confirm Shared Secret	<input type="password" value="••••••"/>
Key Wrap	<input type="checkbox"/>
Port Number	<input type="text" value="1812"/>
Server Status	Enabled <input type="button" value="v"/>
Support for RFC 3576	Enabled <input type="button" value="v"/>
Retransmit Timeout	<input type="text" value="2"/> seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input type="checkbox"/> Enable

23. A configuração básica agora está completa e você pode começar a testar o EAP-TLS.

[Autenticação EAP-TLS](#)

A autenticação EAP-TLS requer certificados de computador e de utilizador no cliente sem fios, a adição de EAP-TLS como um tipo de EAP à política de acesso remoto para acesso sem fios e uma reconfiguração da ligação de rede sem fios.

Para configurar DC_CA para fornecer inscrição automática para certificados de computador e usuário, faça os procedimentos nesta seção.

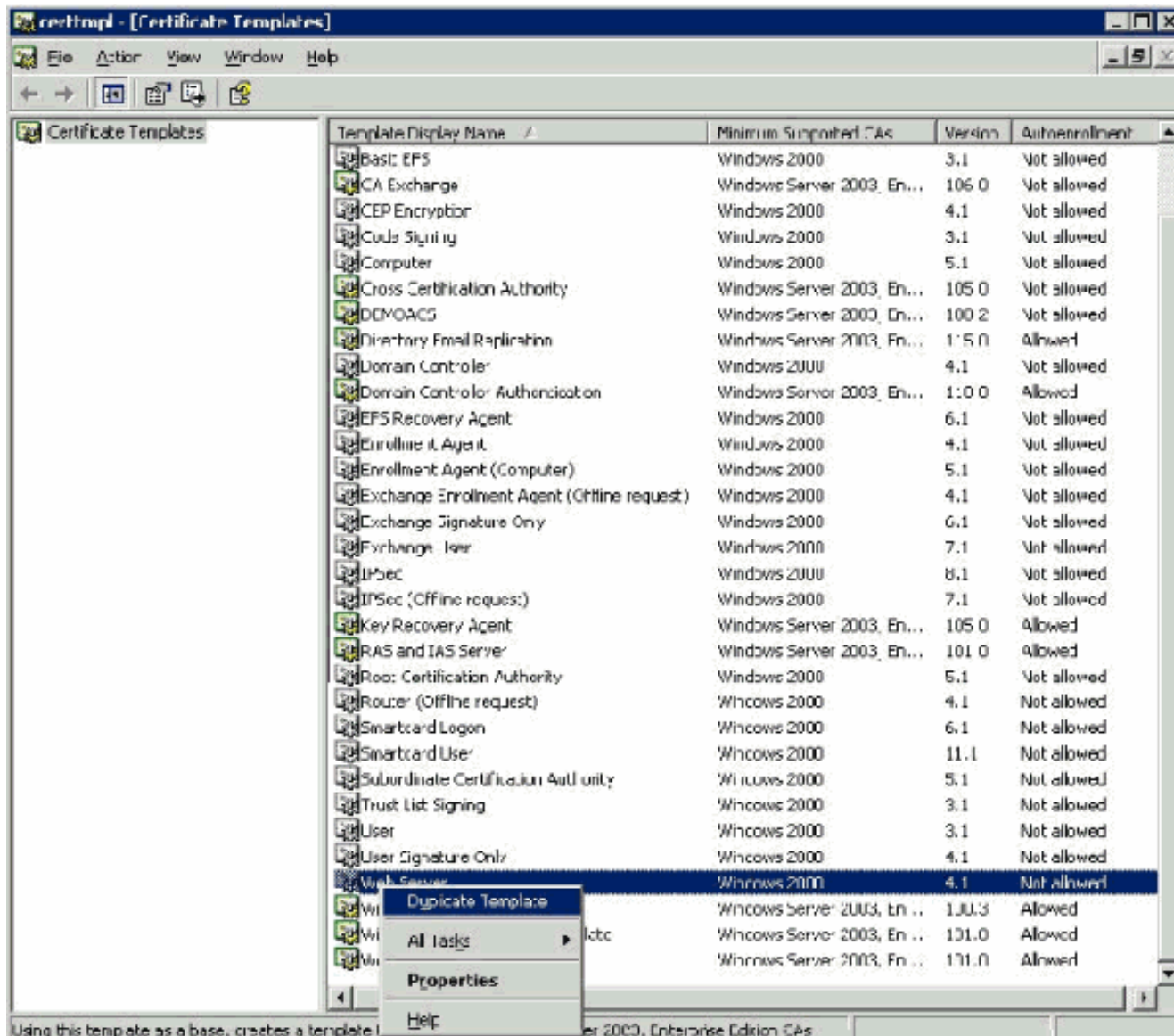
Observação: a Microsoft alterou o modelo do Servidor Web com a versão da CA do Windows 2003 Enterprise para que as chaves não sejam mais exportáveis e a opção fique acinzentada. Não há outros modelos de certificado fornecidos com serviços de certificado para autenticação de servidor e que permitem marcar chaves como exportáveis disponíveis na lista suspensa para que você tenha que criar um novo modelo que faça isso.

Observação: o Windows 2000 permite chaves exportáveis e esses procedimentos não precisam ser seguidos se você usar o Windows 2000.

[Instalar o Snap-in Modelos de Certificado](#)

Conclua estes passos:

1. Escolha **Iniciar > Executar**, digite **mmc** e clique em **OK**.
2. No menu **Arquivo**, clique em **Adicionar/remover snap-in** e, em seguida, clique em **Adicionar**.
3. Em **Snap-in**, clique duas vezes em **Modelos de certificado**, clique em **Fechar** e em **OK**.
4. Na árvore do console, clique em **Modelos de certificado**. Todos os modelos de certificado aparecem no painel **Detalhes**.
5. Para ignorar as etapas de 2 a 4, digite **certtmpl.msc**, que abre o snap-in **Modelos de certificado**.



[Crie o Modelo de Certificado para o Servidor Web ACS](#)

Conclua estes passos:

1. No painel **Detalhes** do snap-in **Modelos de certificado**, clique no modelo do **servidor Web**.
2. No menu **Ação**, clique em **Duplicar**

Properties of New Template [?] [X]

Issuance Requirements | Superseded Templates | Extensions | Security

General | Request Handling | Subject Name

Template display name:
Copy of Web Server

Minimum Supported CAs: Windows Server 2003, Enterprise Edition

After you apply changes to this tab, you can no longer change the template name.

Template name:
Copy of Web Server

Validity period: 2 years
Renewal period: 6 weeks

Publish certificate in Active Directory
 Do not automatically reenroll if a duplicate certificate exists in Active Directory

OK Cancel Apply

modelo.

3. No campo Nome de exibição do modelo, digite

Properties of New Template [?] [X]

Issuance Requirements | Superseded Templates | Extensions | Security

General | Request Handling | Subject Name

Template display name:
ACS

Minimum Supported CAs: Windows Server 2003, Enterprise Edition

After you apply changes to this tab, you can no longer change the template name.

Template name:
ACS

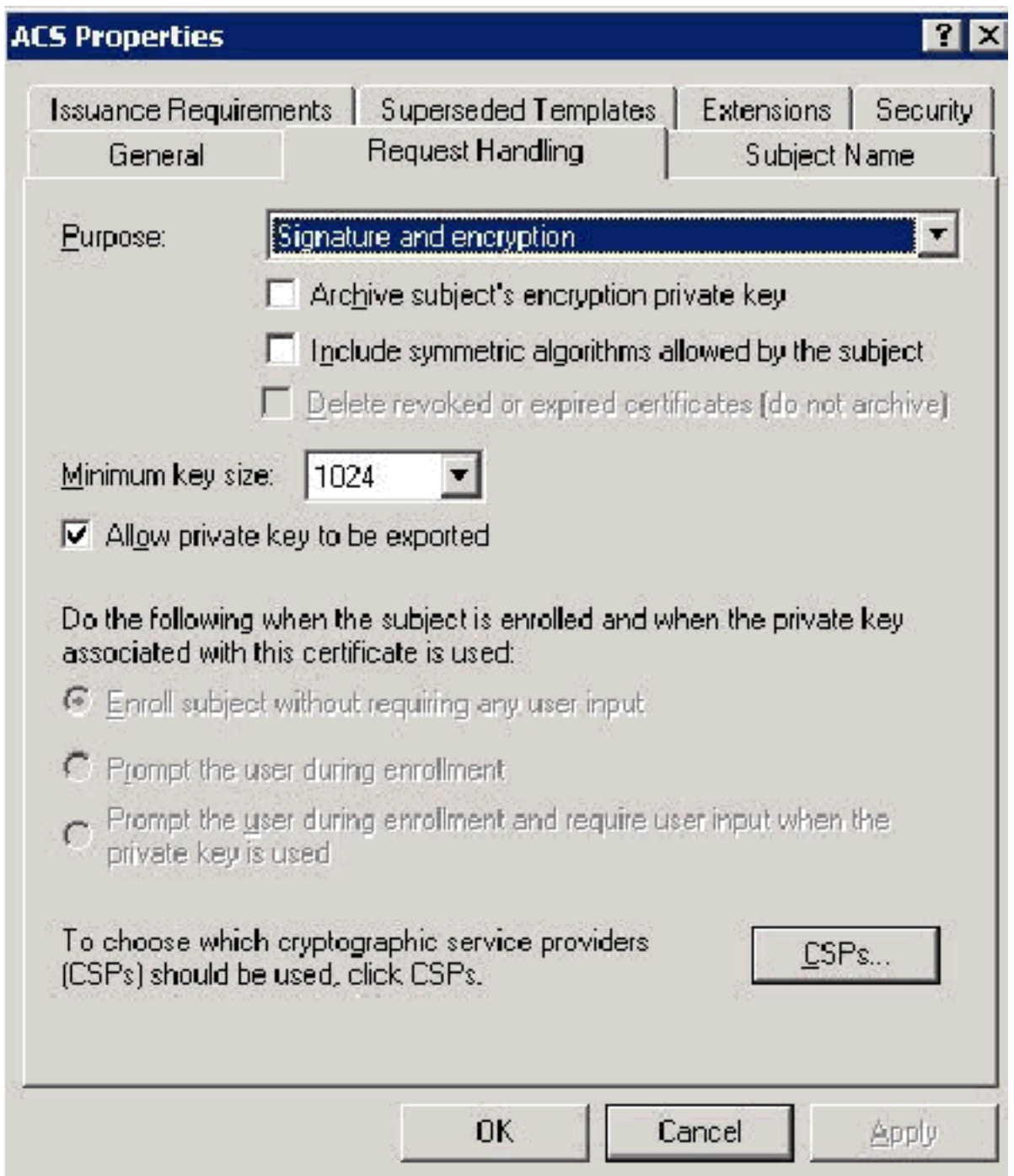
Validity period: 2 years
Renewal period: 6 weeks

Publish certificate in Active Directory
 Do not automatically reenroll if a duplicate certificate exists in Active Directory

OK Cancel Apply

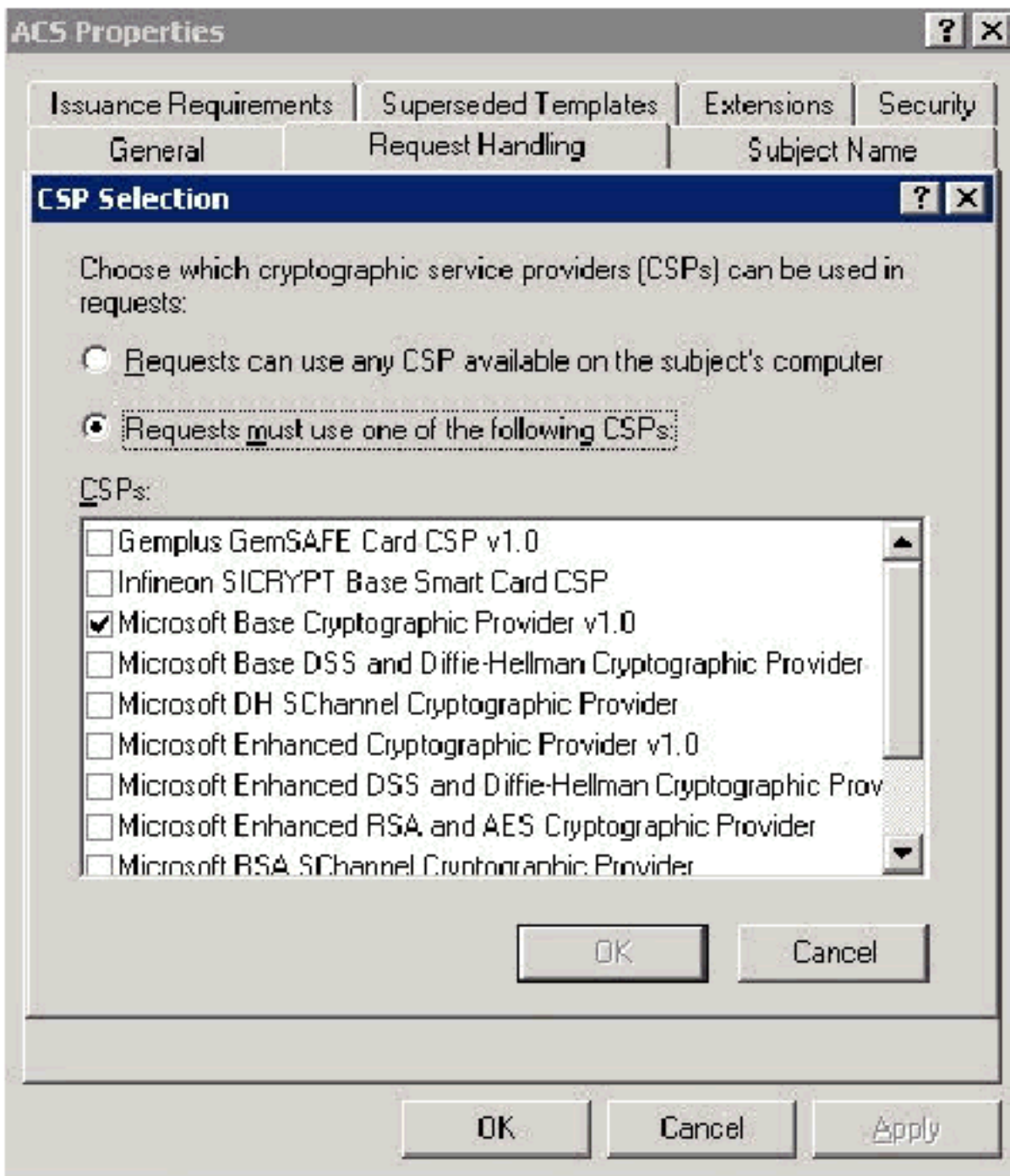
ACS.

4. Vá até a guia Solicitar tratamento e marque **Permitir exportação de chave**



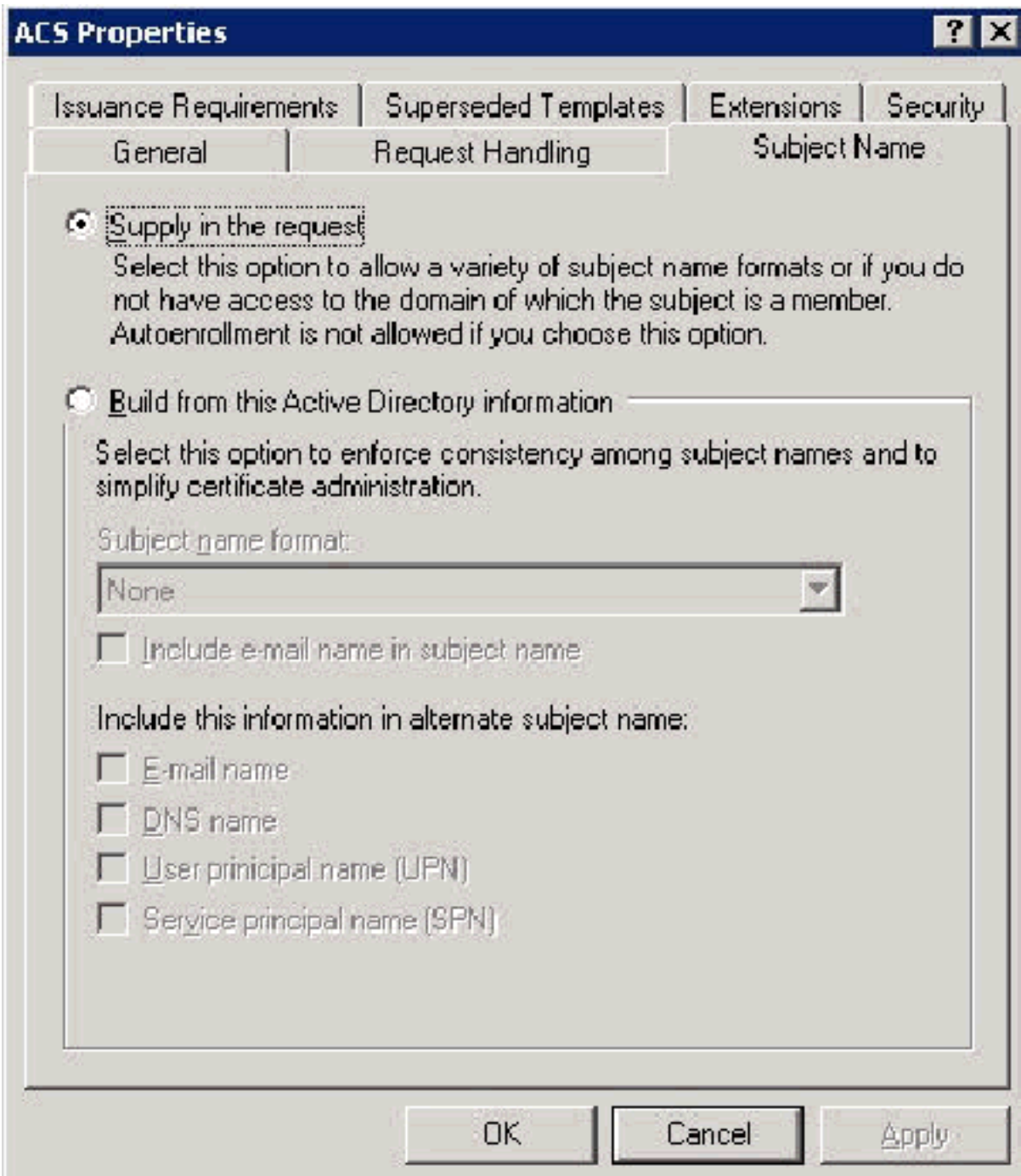
privada.

5. Escolha Solicitações que devem usar um dos CSPs a seguir e marque Microsoft Base Cryptographic Provider v1.0. Desmarque todos os outros CSPs marcados e clique em



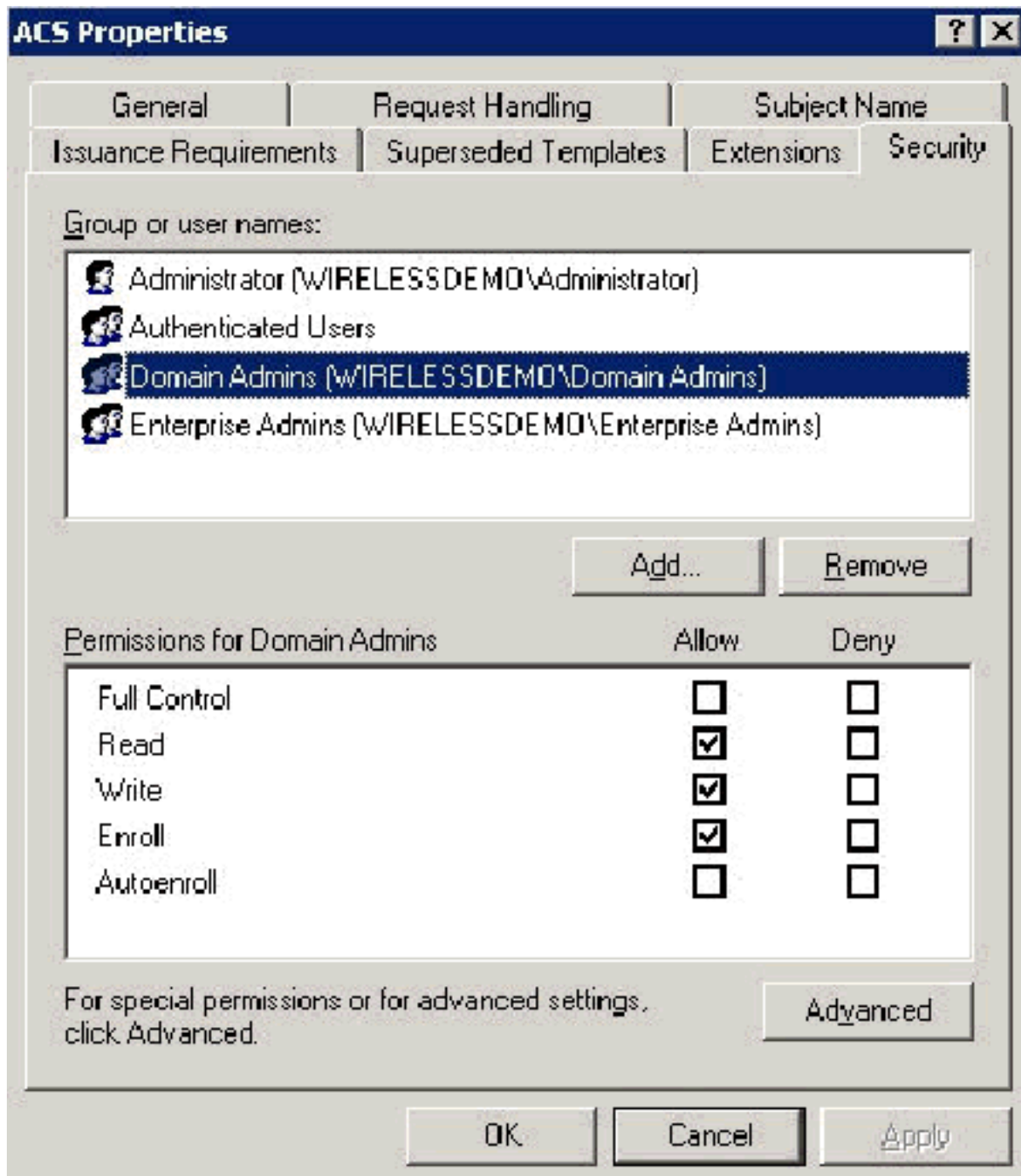
OK.

6. Vá para a guia Nome do assunto, escolha **Suprimento na solicitação** e clique em

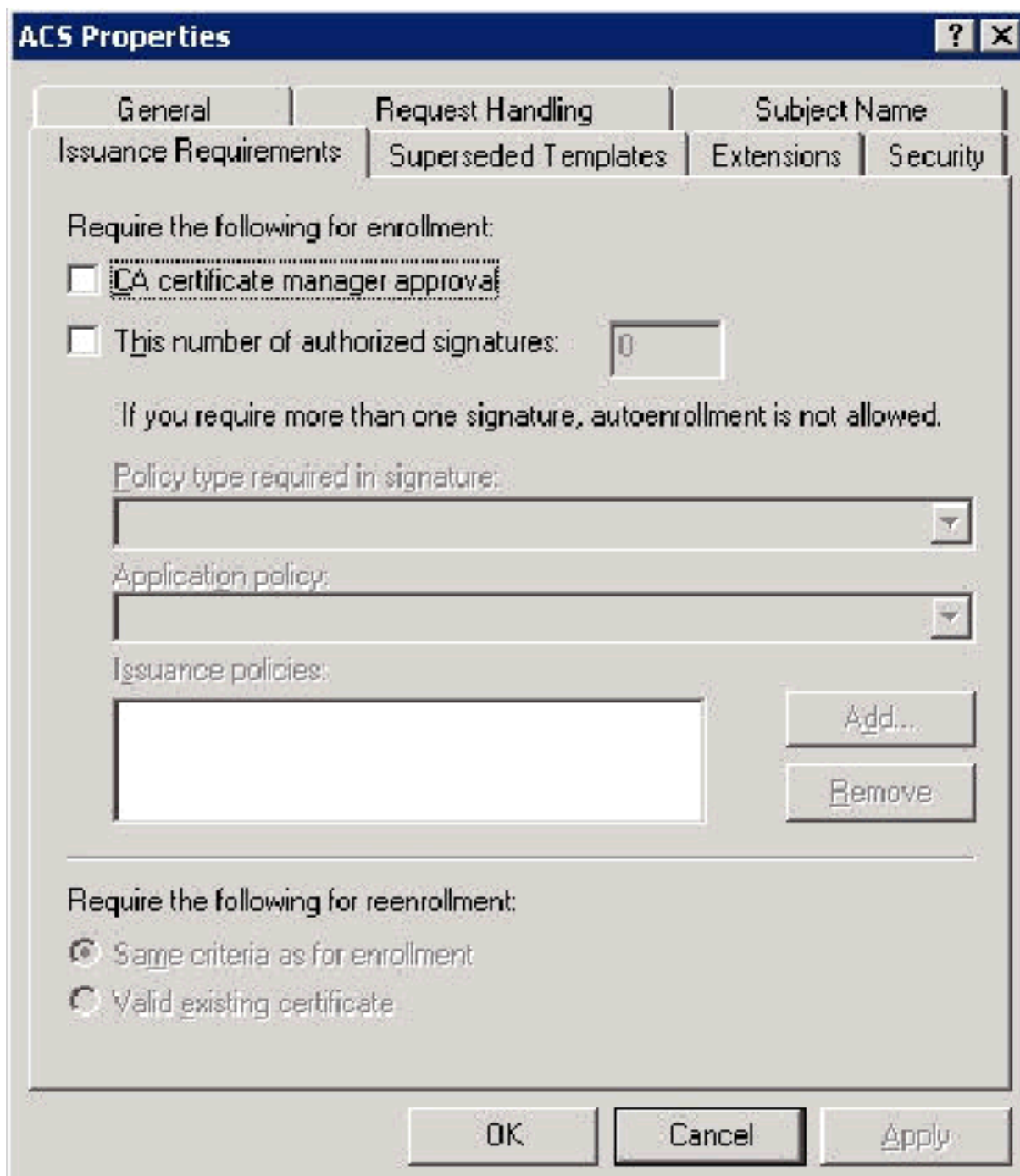


OK.

- Vá até a guia Segurança, realce o **Grupo de administradores de domínio** e verifique se a opção **Inscriver** está marcada em Permitido. **Importante:** Se optar por criar apenas a partir destas informações do Ative Directory, selecione **UPN (User principal name)** e desmarque **Incluir nome de correio eletrônico** no nome do assunto e nome de correio eletrônico porque não foi introduzido um nome de correio eletrônico para a conta WirelessUser no snap-in Utilizadores e Computadores do Ative Directory. Se você não desabilitar essas duas opções, a inscrição automática tentará usar o e-mail, o que resulta em um erro de inscrição automática.



8. Se necessário, existem medidas de segurança adicionais para evitar que os certificados sejam automaticamente enviados. Eles podem ser encontrados na guia Requisitos de Emissão. Isso não é discutido mais neste documento.

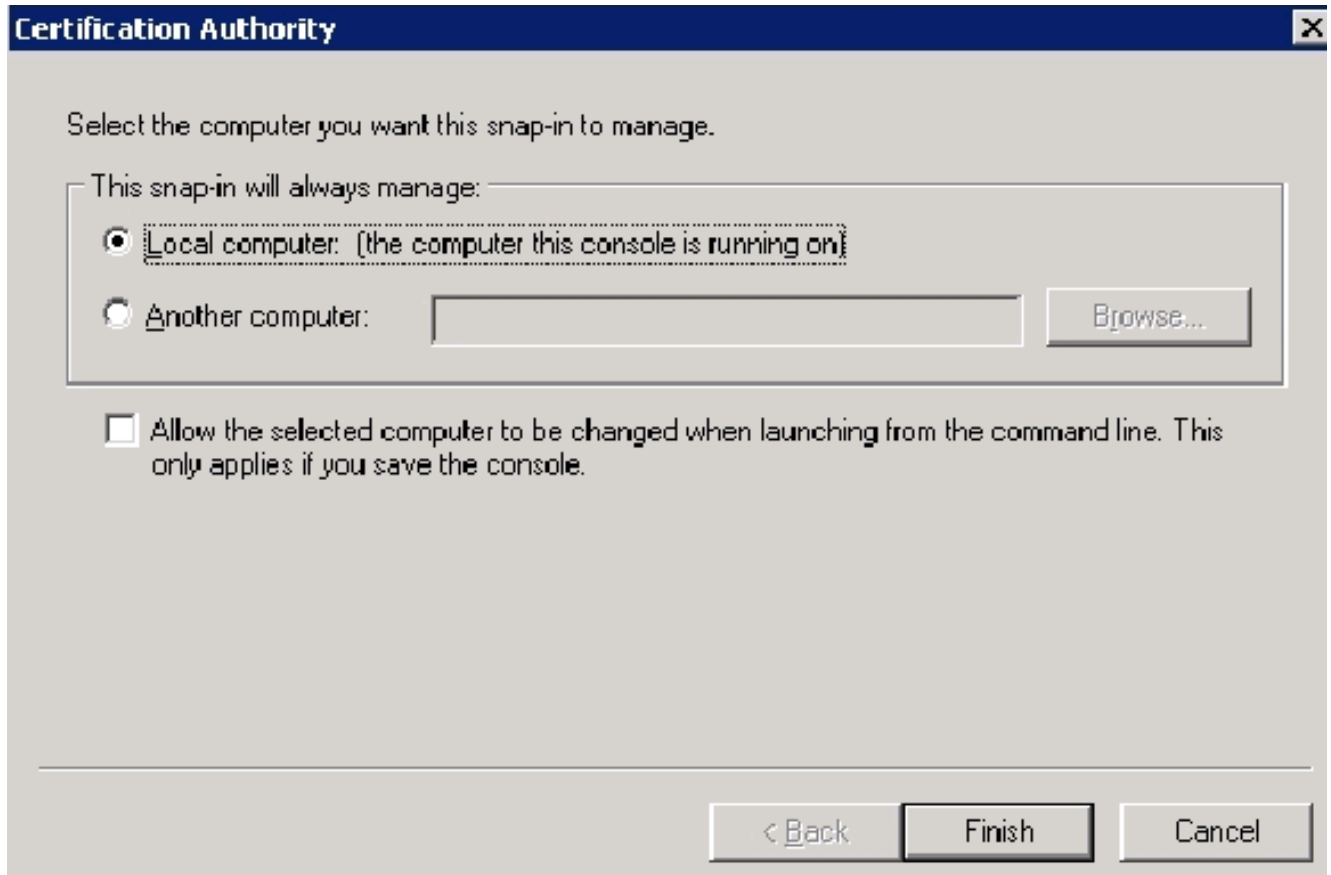


9. Clique em **OK** para salvar o modelo e passar para a emissão desse modelo a partir do snap-in Autoridade de certificação.

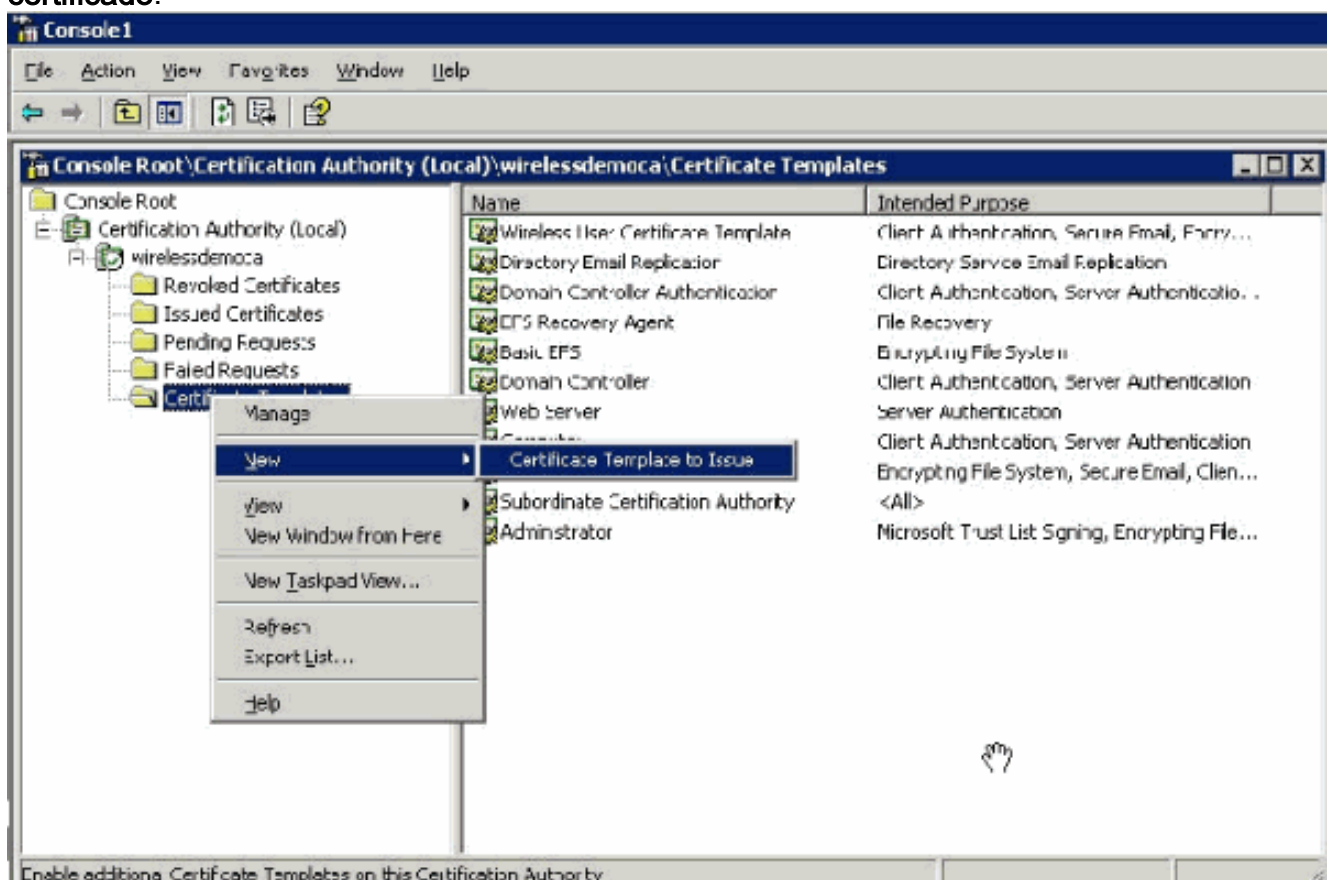
[Ativar o novo modelo de certificado do servidor Web ACS](#)

Conclua estes passos:

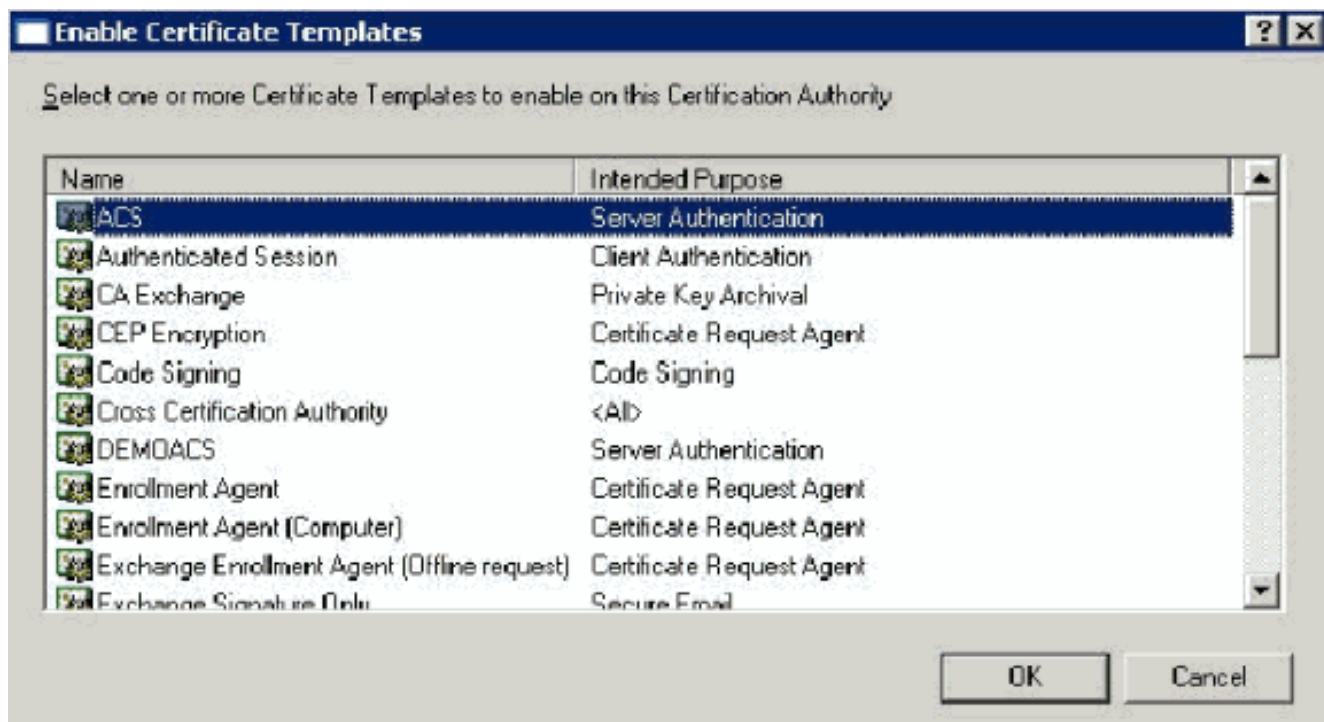
1. Abra o snap-in **Autoridade de Certificação**. Siga as etapas de 1 a 3 na seção [Create the Certificate Template for the ACS Web Server](#), escolha a opção **Certificate Authority**, escolha **Local Computer** e clique em **Finish**.



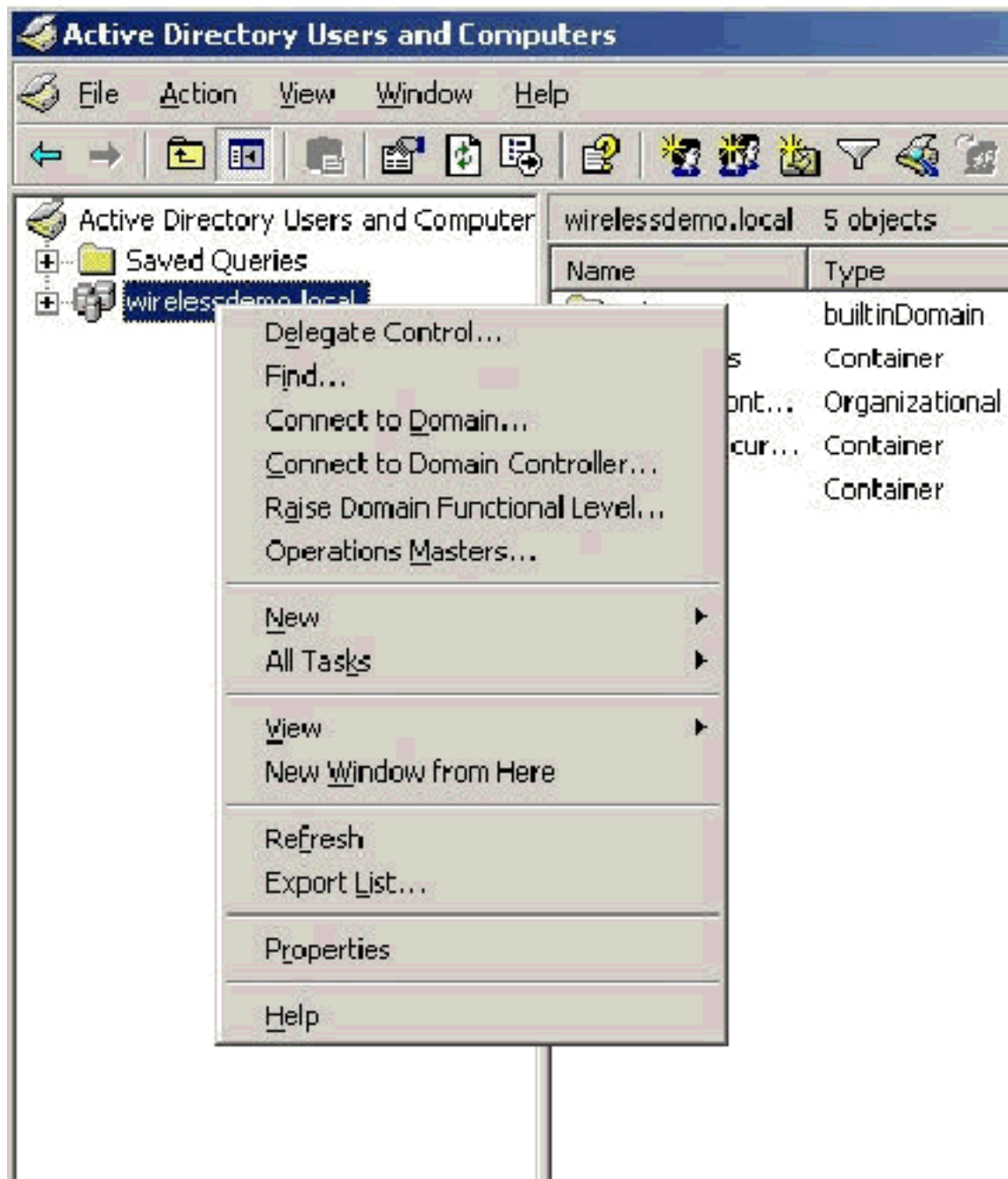
2. Na árvore do console, expanda **wireless democa** e clique com o botão direito do mouse em **Modelos de certificado**.



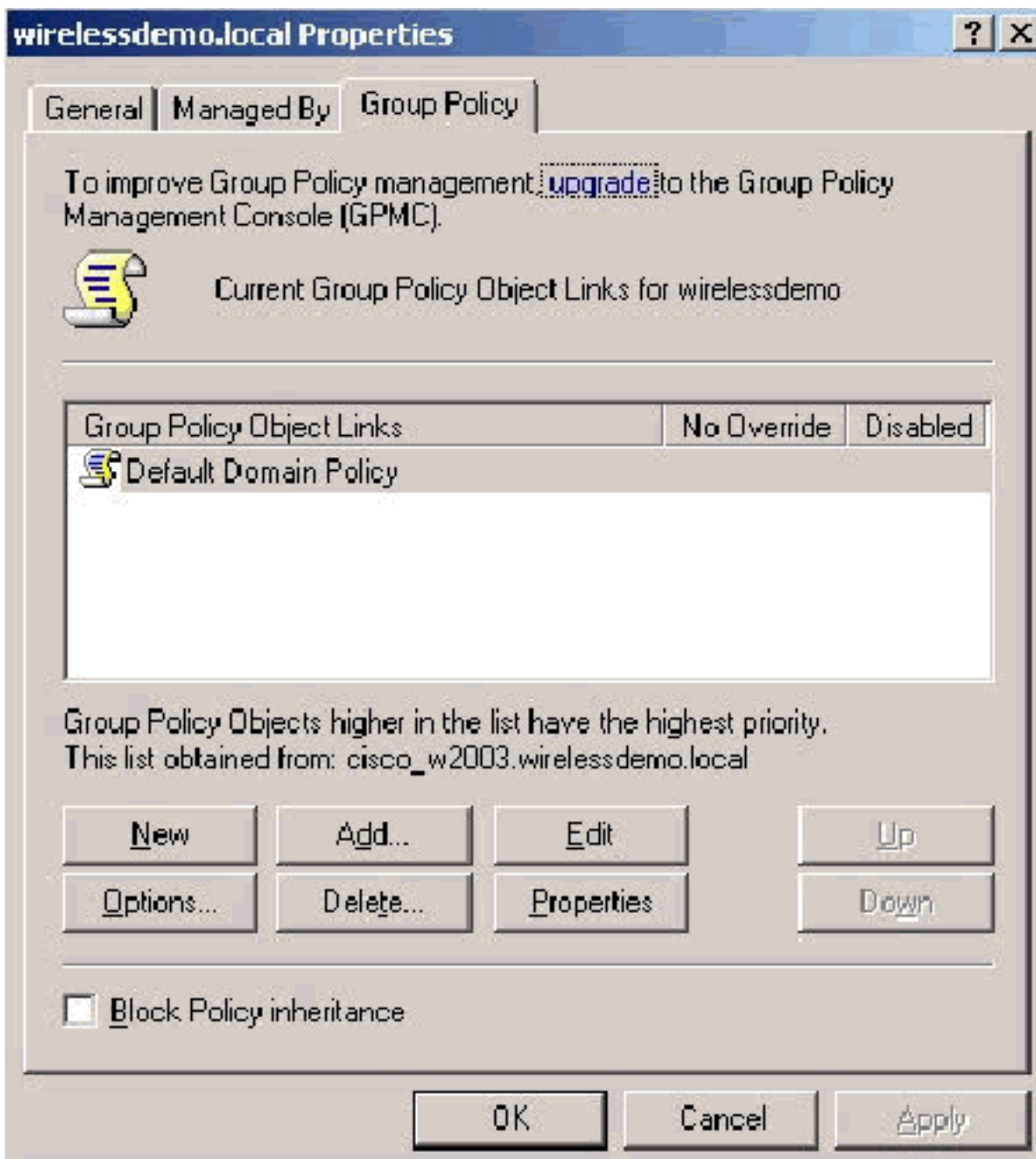
3. Escolha **Novo > Modelo de certificado a ser emitido**.
4. Clique no Modelo de certificado **ACS**.



5. Clique em **OK** e abra o **snap-in Usuários e Computadores do Ative Directory**.
6. Na árvore do console, clique duas vezes em **Usuários e Computadores do Ative Directory**, clique com o botão direito do mouse no **domínio wireless demo.local** e clique em **Propriedades**.

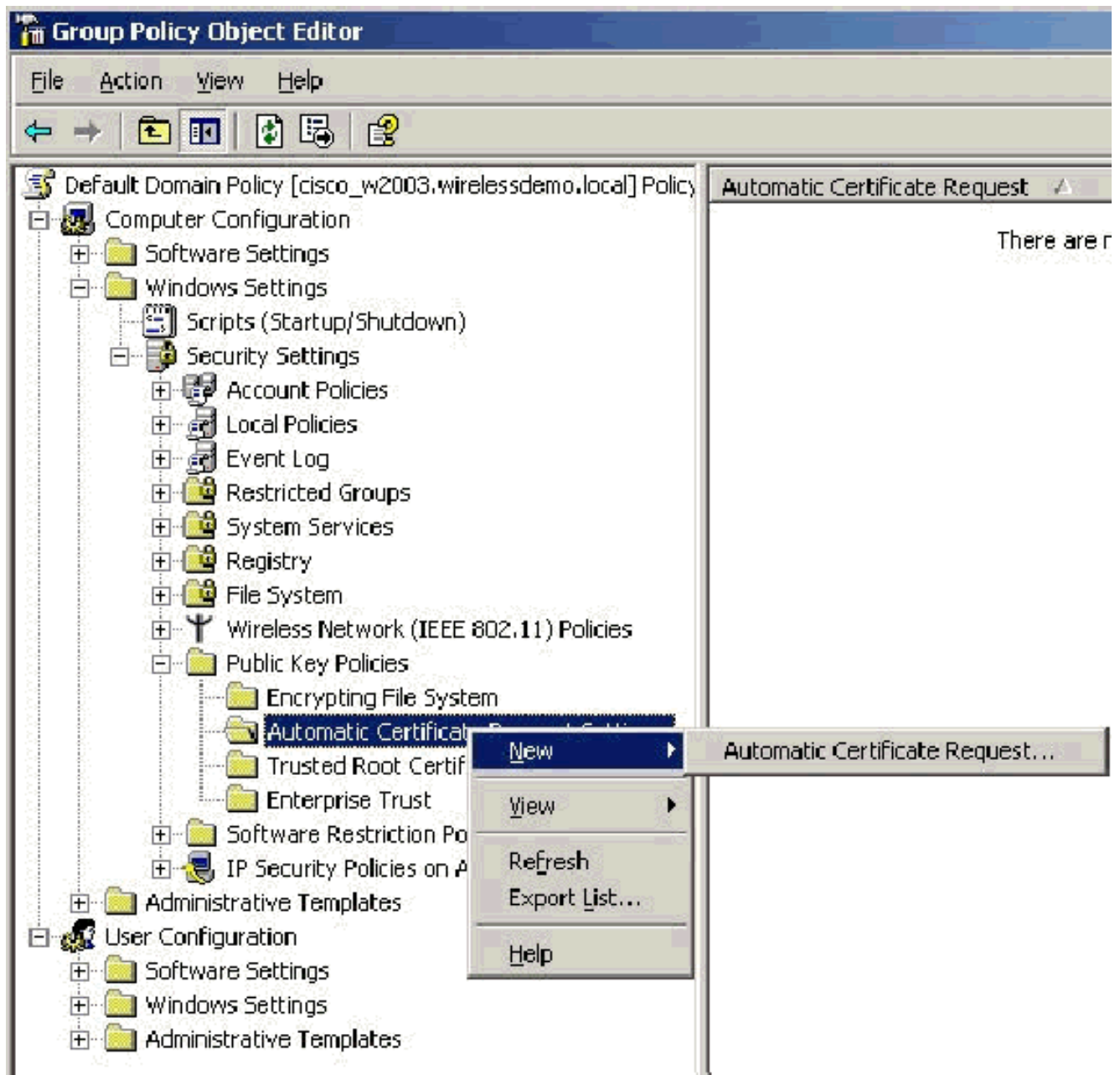


7. Na guia Diretiva de grupo, clique em **Política de domínio padrão** e clique em **Editar**. Isso abre o snap-in Editor de objetos de política de

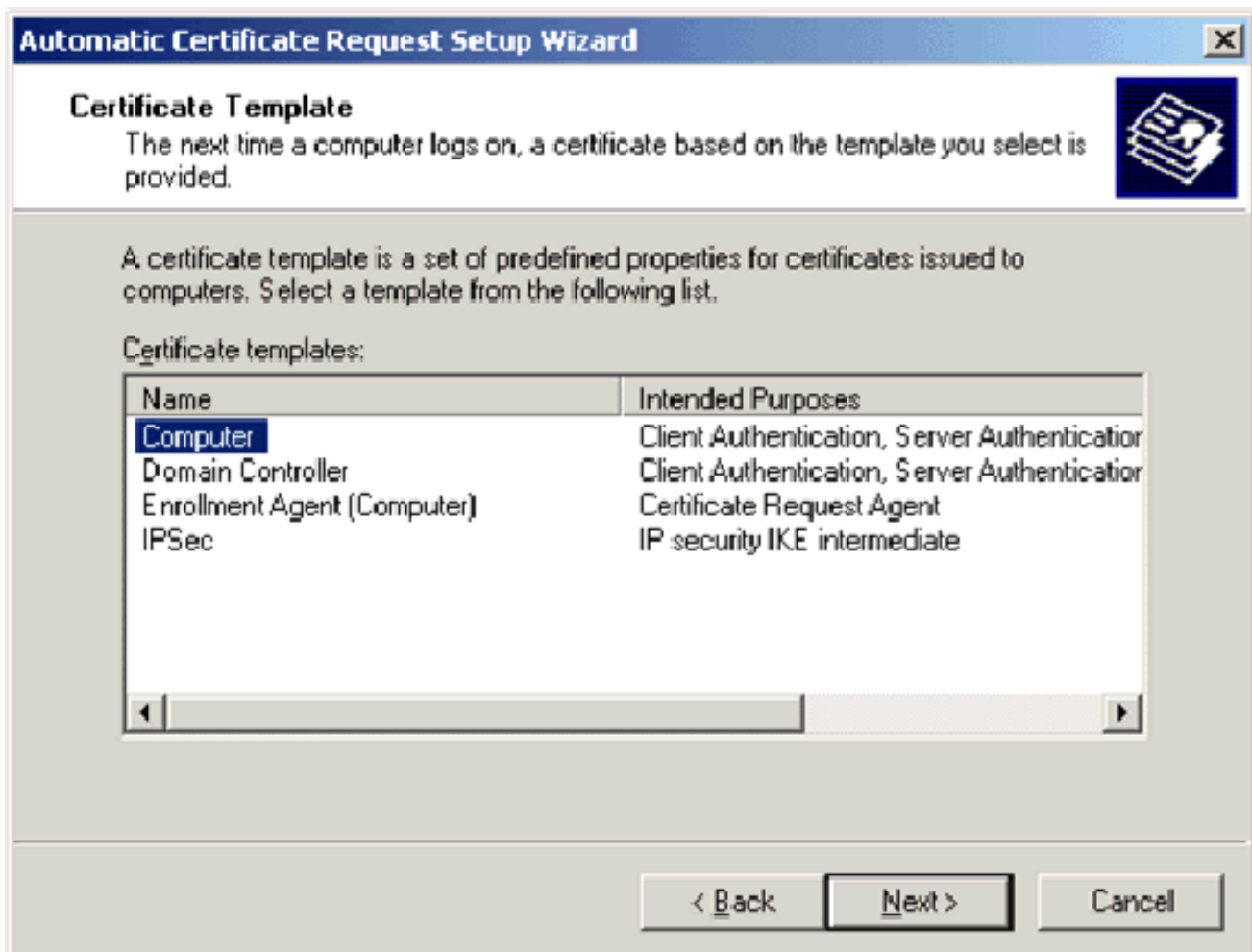


grupo.

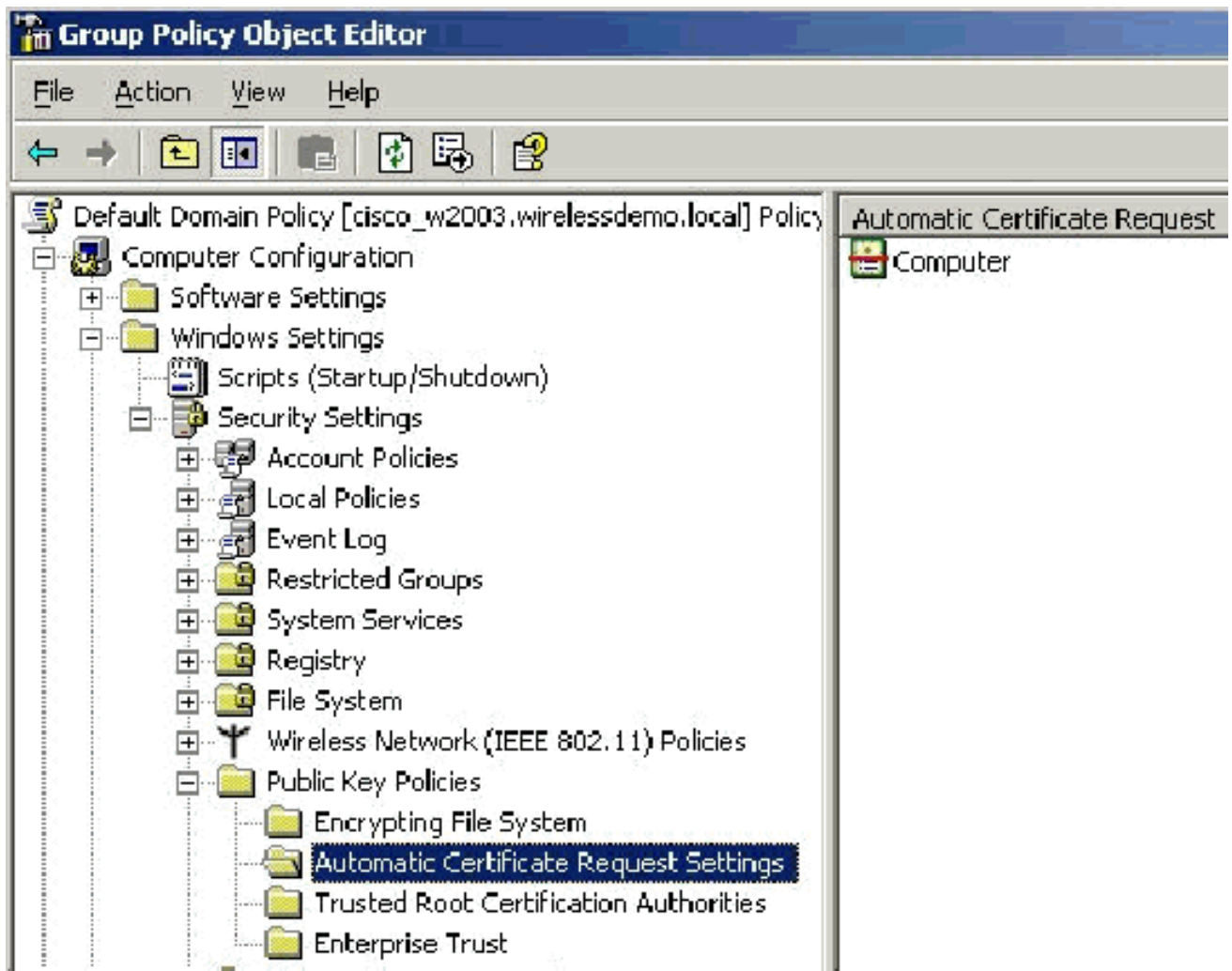
8. Na árvore do console, expanda **Configuração do computador > Configurações do Windows > Configurações de segurança > Políticas de chave pública** e selecione **Configurações automáticas de solicitação de certificado**.



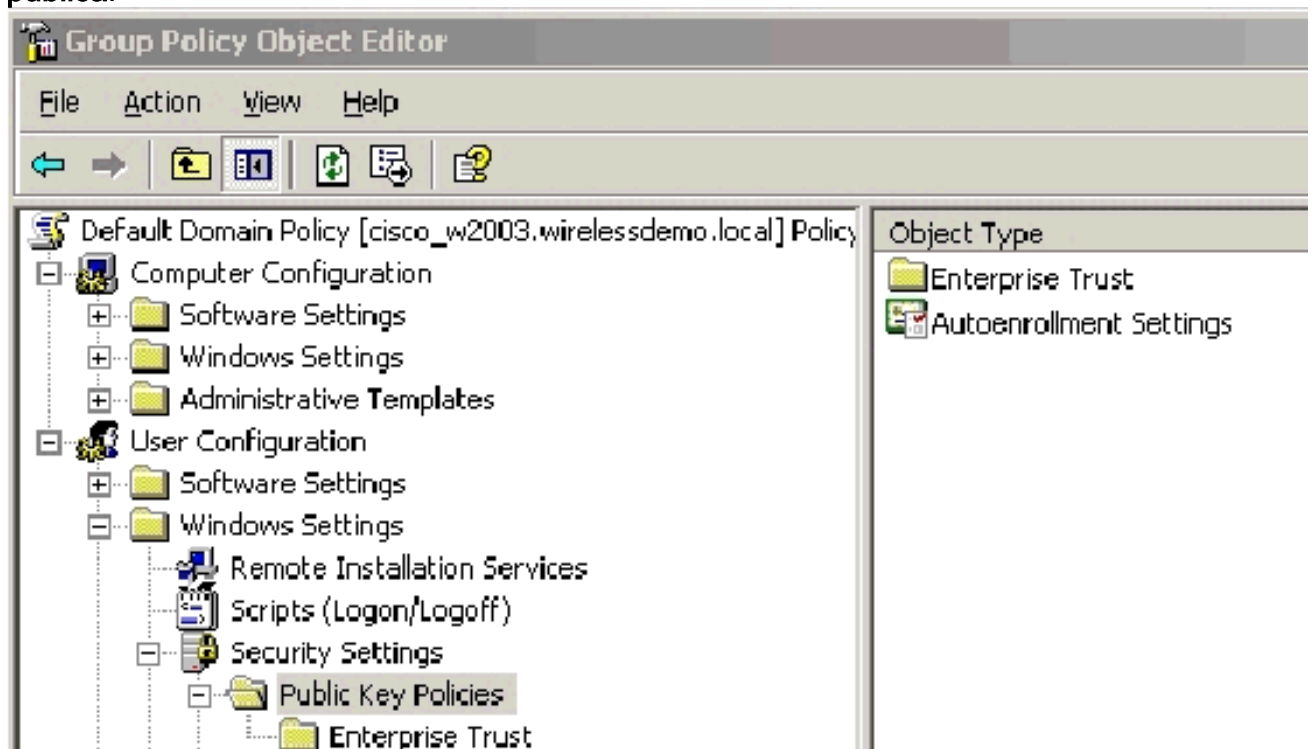
9. Clique com o botão direito do mouse em **Configurações automáticas de solicitação de certificado** e escolha **Novo > Solicitação automática de certificado**.
10. Na página Bem-vindo ao Assistente de configuração de solicitação automática de certificado, clique em **Avançar**.
11. Na página Modelo de certificado, clique em **Computador** e clique em **Avançar**.



12. Na página Completing the Automatic Certificate Request Setup Wizard (Concluindo o Assistente de configuração de solicitação de certificado automático), clique em **Finish (Concluir)**. O tipo de certificado Computador agora é exibido no painel de detalhes do snap-in Editor de objetos de política de grupo.

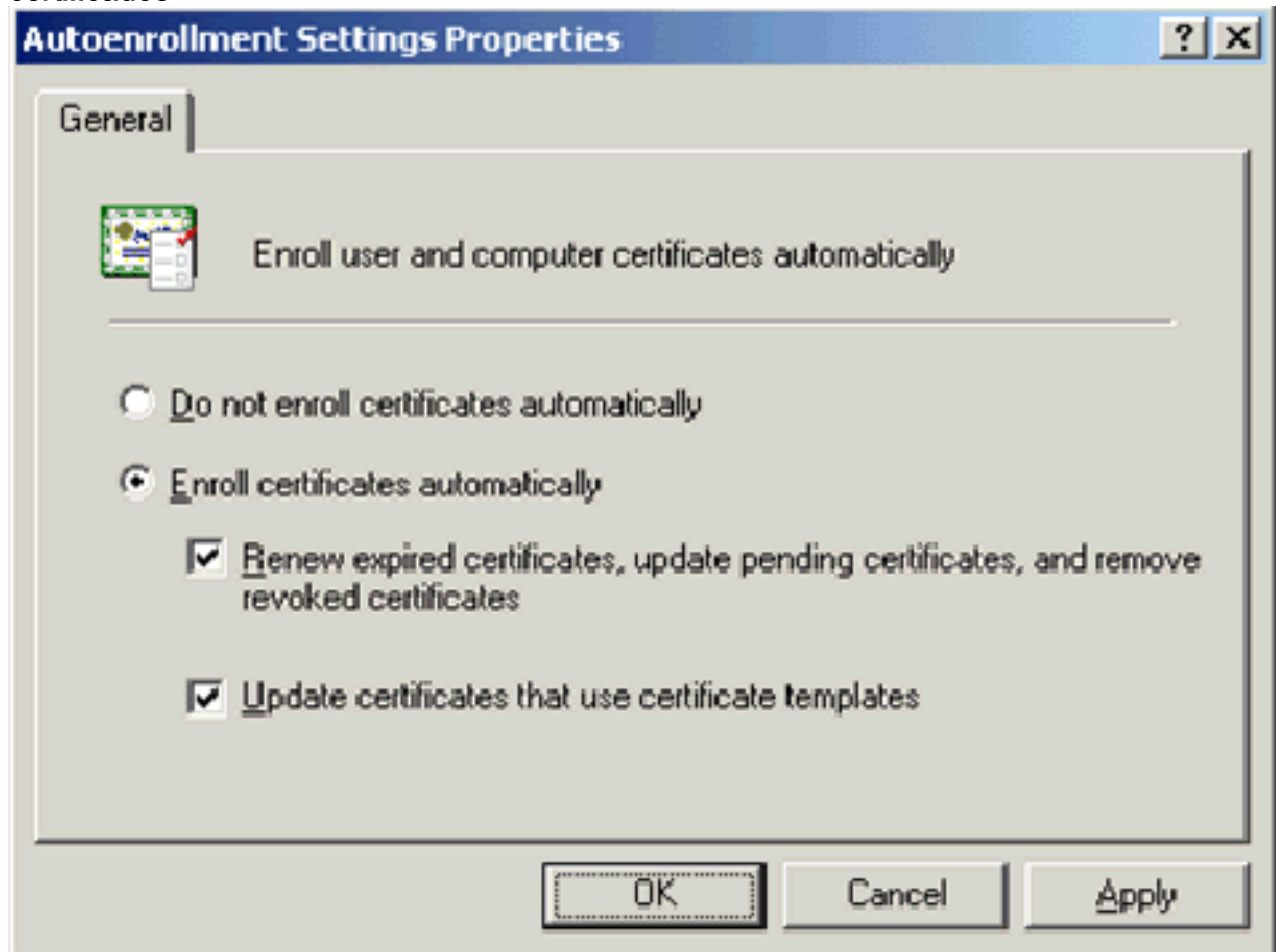


13. Na árvore do console, expanda **Configuração do usuário > Configurações do Windows > Configurações de segurança > Políticas de chave pública**.



14. No painel de detalhes, clique duas vezes em **Configurações de inscrição automática**.
 15. Escolha **Inscrever certificados automaticamente** e marque **Renovar certificados expirados**,

atualizar certificados pendentes e remover certificados revogados e Atualizar certificados que utilizem modelos de certificados.



16. Click OK.

[Configuração do certificado ACS 4.0](#)

[Configurar certificado exportável para ACS](#)

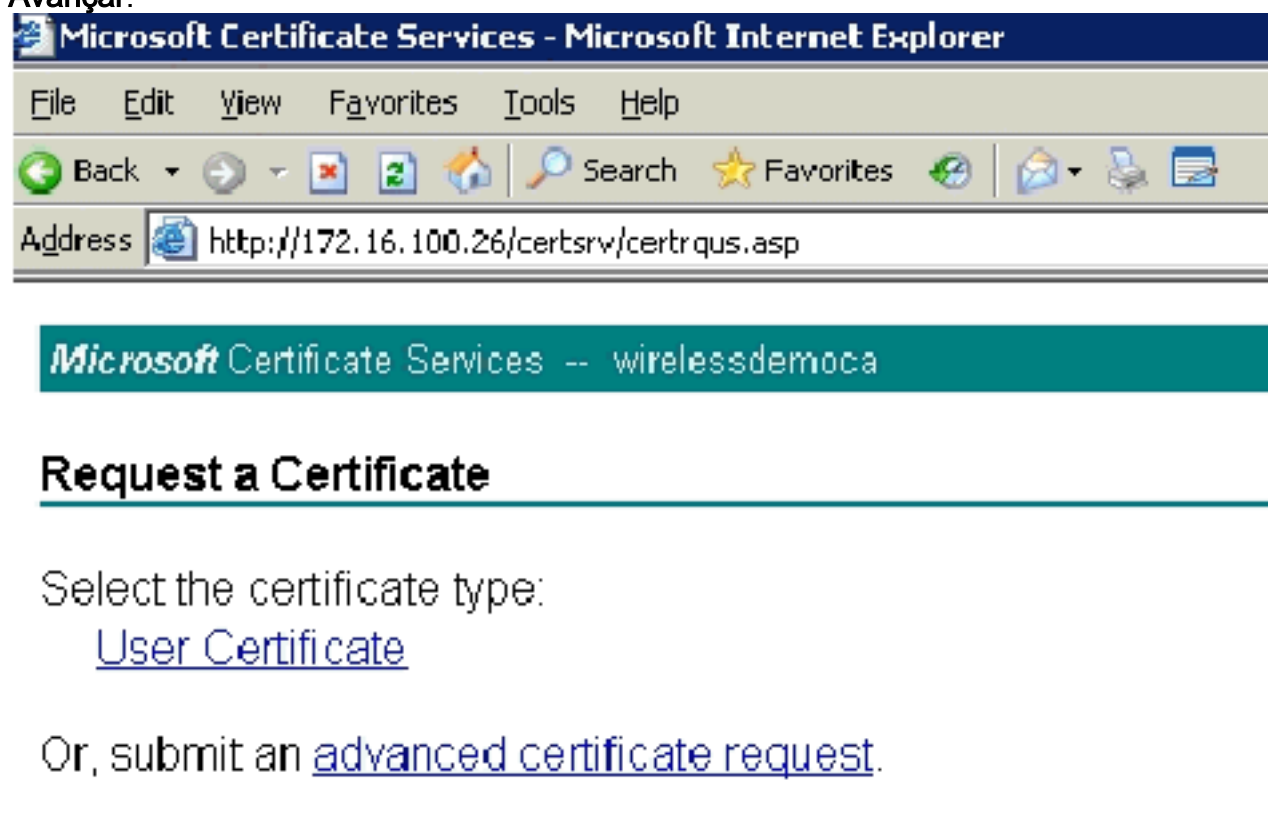
Importante: O servidor ACS deve obter um certificado de servidor do servidor de CA raiz Enterprise para autenticar um cliente WLAN EAP-TLS.

Importante: Verifique se o Gerenciador do IIS não está aberto durante o processo de configuração do certificado, pois ele causa problemas com informações em cache.

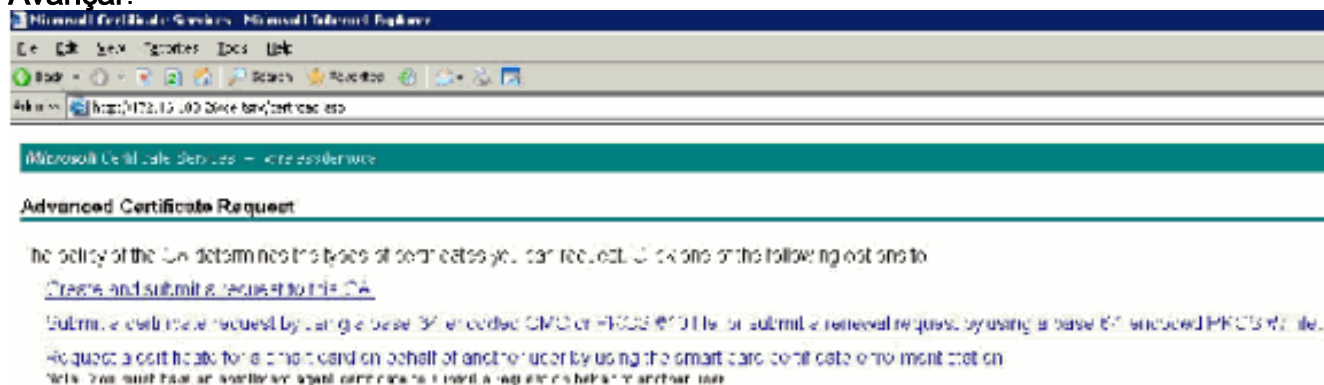
1. Efetue login no servidor ACS com uma conta que tenha direitos de Administrador Corporativo.
2. Na máquina ACS local, aponte o navegador para o servidor da autoridade de certificação da Microsoft em <http://IP-address-of-Root-CA/certsrv>. Nesse caso, o endereço IP é **172.16.100.26**.
3. Efetue login como Administrador.



4. Escolha **Solicitar um certificado** e clique em **Avançar**.



5. Escolha **Solicitação avançada** e clique em **Avançar**.



6. Escolha **Criar e enviar uma solicitação para esta CA** e clique em **Avançar**. **Importante:** O motivo para esta etapa é o fato do Windows 2003 não permitir chaves exportáveis e você precisa gerar uma solicitação de certificado com base no certificado ACS que você criou anteriormente e que

permite.

Microsoft Certificate Services - wirelessdemo.local

Advanced Certificate Request

Certificate Template:

Administrator

Key Options:

Administrator
Basic EFS
EFS Recovery Agent
User
CSP: Wireless User Certificate Template
Key Usage: S.Ordinary Certification Authority
Key Store: Web Server
Max: 15384
1024 2048 4096 8192 16384

Automatic key container name User specified key container name

Mark keys as exportable
 Export keys to file

Enable strong private key protection

Store certificate in the local computer certificate store
Saves 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: CMC PKCS10

Hash Algorithm: SHA-1
Only used to sign request.

Save request to file

Attributes:

Friendly Name:

7. Nos Modelos de certificado, selecione o modelo de certificado criado anteriormente chamado **ACS**. As opções são alteradas após a seleção do modelo.
8. Configure o nome para ser o nome de domínio totalmente qualificado do servidor ACS. Nesse caso, o nome do servidor ACS é `cisco_w2003.wirelessdemo.local`. Certifique-se de que o certificado de armazenamento no arquivo de certificados do computador local está marcado e clique em

Microsoft Certificate Services - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites

Address: http://172.16.100.26/certsrv/certreqs.asp

Certificate Template:

ACS

Identifying Information For Offline Template:

Name: cisco_w2003_wirelessdemo.local

E-Mail:

Company:

Department:

City:

State:

Country/Region:

Key Options:

Create new key set Use existing key set

CSP: Microsoft Base Cryptographic Provider v1.0

Key Usage: Exchange

Key Size: 1024 Min:1024 Max:1024 (common key sizes: 3072)

Automatic key container name User specified key container name

Mark keys as exportable

Export keys to file

Store certificate in the local computer certificate store
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: CMC PKCS10

Hash Algorithm: SHA-1
Only used to sign request.

Save request to a file

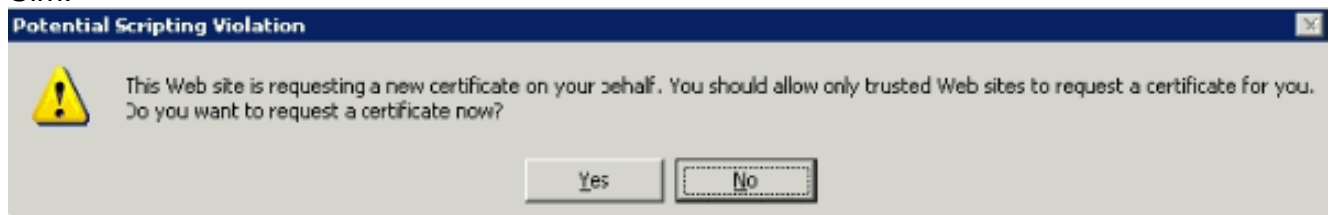
Attributes:

Friendly Name:

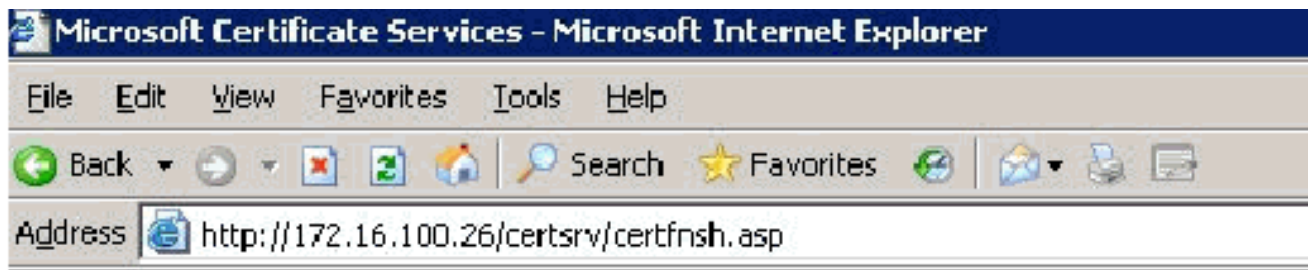
Submit >

Enviar.

9. Uma janela pop-up é exibida e avisa sobre uma possível violação de script. Clique em Sim.



10. Clique em Instalar este certificado.



Microsoft Certificate Services -- wirelessdemoca

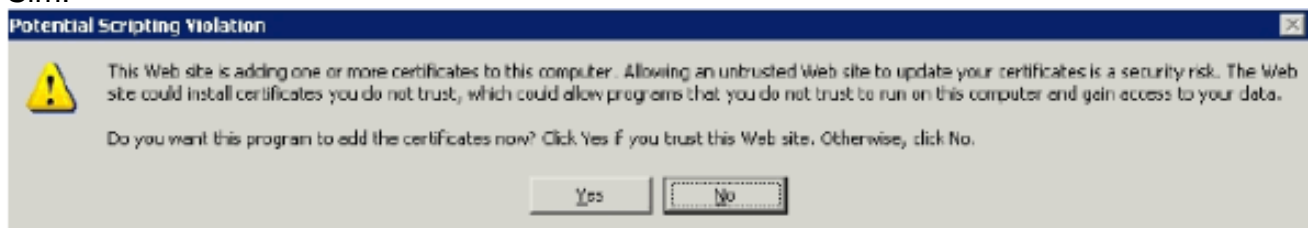
Certificate Issued

The certificate you requested was issued to you.

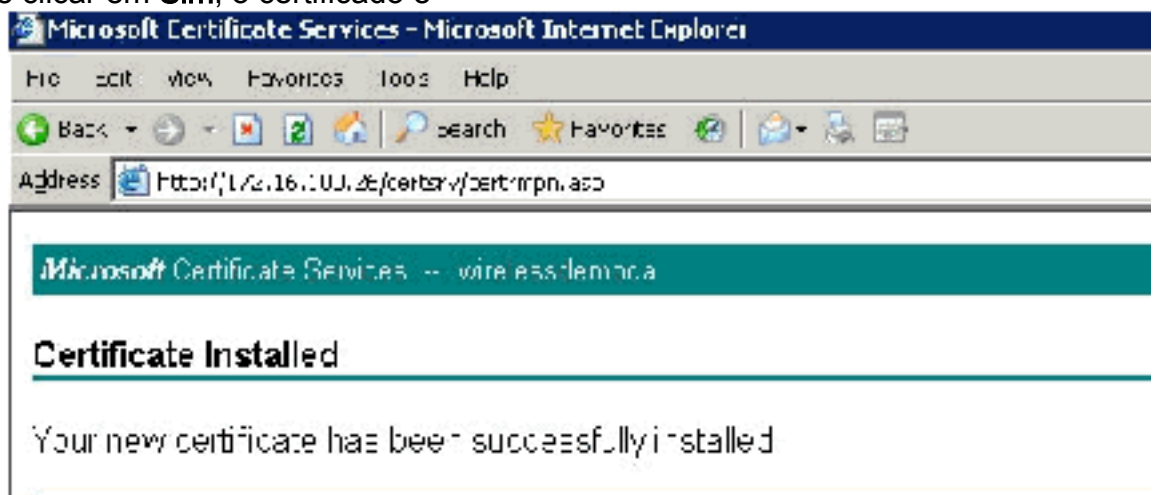


[Install this certificate](#)

11. Uma janela pop-up é exibida novamente e avisa sobre uma possível violação de script. Clique em **Sim**.

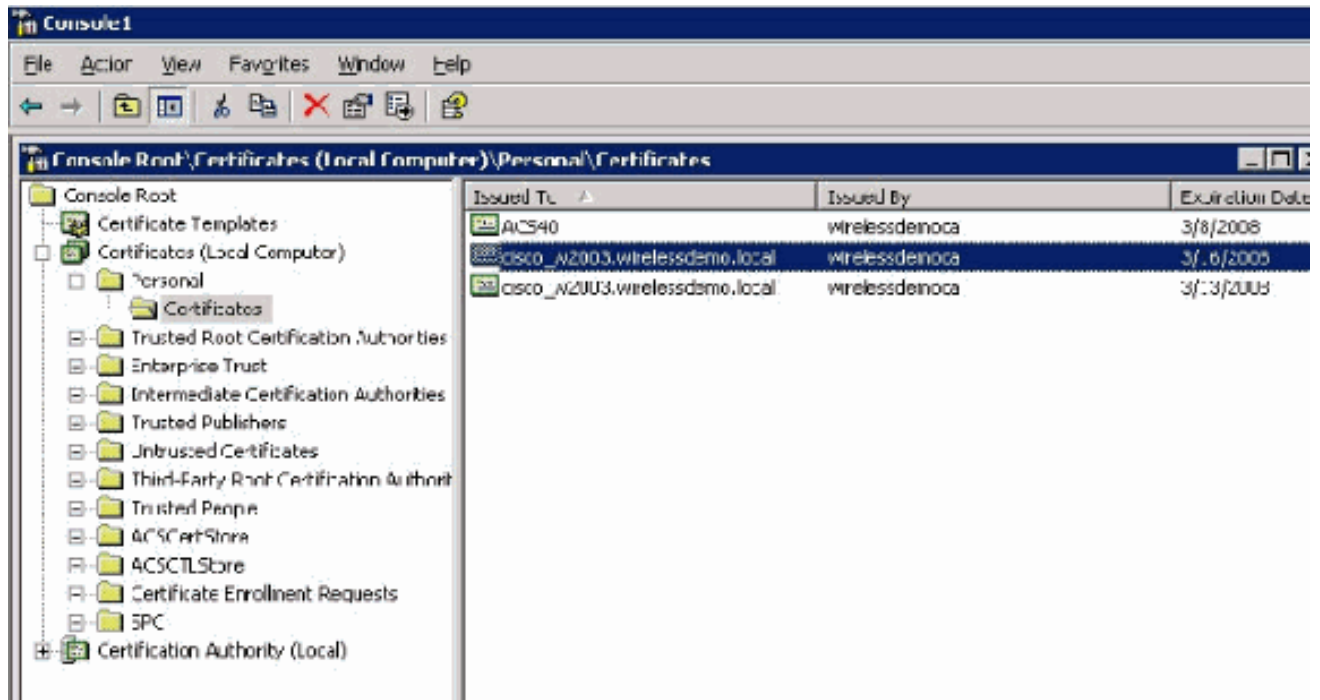


12. Depois de clicar em **Sim**, o certificado é



instalado.

13. Neste ponto, o certificado é instalado na pasta Certificados. Para acessar esta pasta, escolha **Iniciar > Executar**, digite **mmc**, pressione **Enter** e escolha **Pessoal > Certificados**.



14. Agora que o certificado está instalado no computador local (ACS ou cisco_w2003 neste exemplo), você precisa gerar um arquivo de certificado (.cer) para a configuração do arquivo de certificado ACS 4.0.
15. No servidor ACS (cisco_w2003 neste exemplo), aponte o navegador no servidor da Autoridade de Certificação da Microsoft para [http://172.16.100.26 /certsrv](http://172.16.100.26/certsrv).

[Instale o certificado no software ACS 4.0](#)

Conclua estes passos:

1. No servidor ACS (cisco_w2003 neste exemplo), aponte o navegador no servidor Microsoft CA para <http://172.16.100.26 /certsrv>.
2. Na opção Seleccionar uma tarefa, escolha **Baixar um certificado CA, uma cadeia de certificados ou uma CRL**.
3. Escolha o método de codificação de rádio **Base 64** e clique em **Download CA Certificate**.

Microsoft Certificate Services - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites

Address http://172.16.100.26/certs/v/certbase.asp

Microsoft Certificate Services -- wirelessdemora

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority [install this CA certificate chain](#).

To download a CA certificate, certificate chain, or CRL, select the certificate encoding method:

CA certificate:

Current (wirelessdemora)

Encoding method:

DER

Base 64

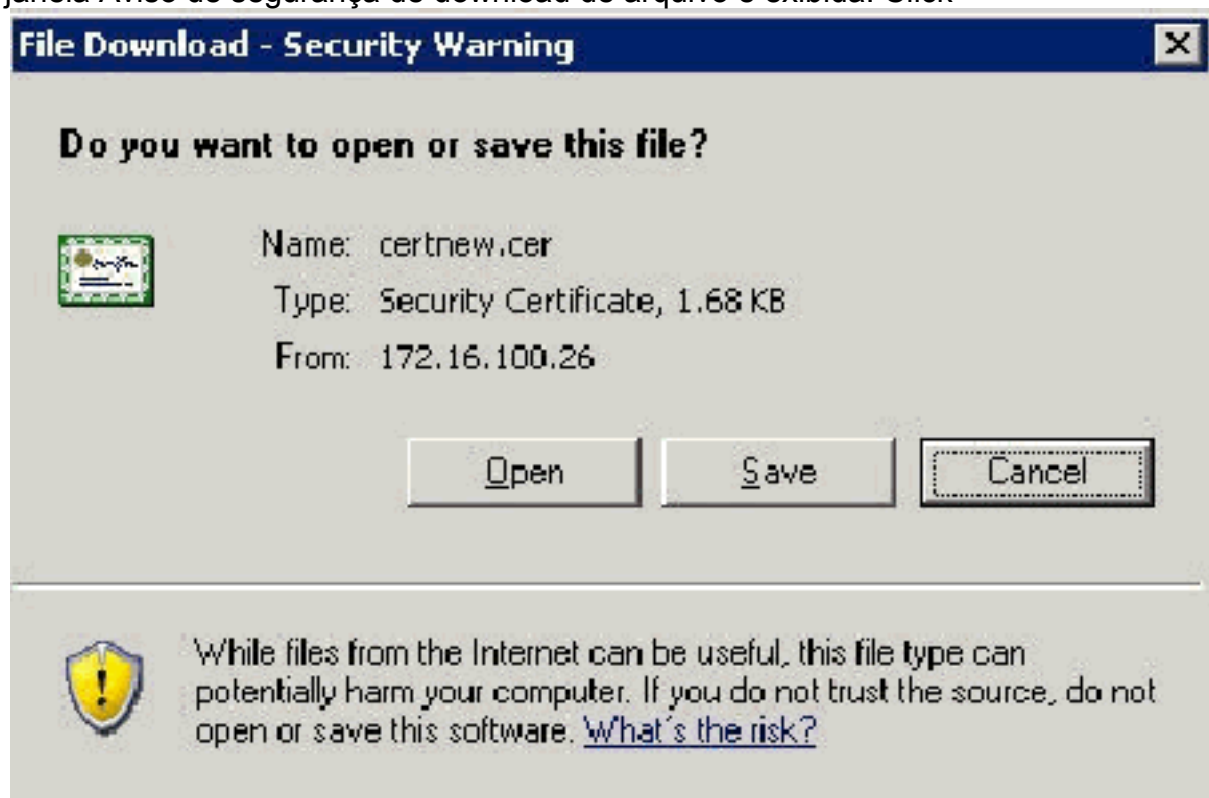
[Download CA certificate](#)

[Download CA certificate chain](#)

[Download latest base CRL](#)

[Download latest delta CRL](#)

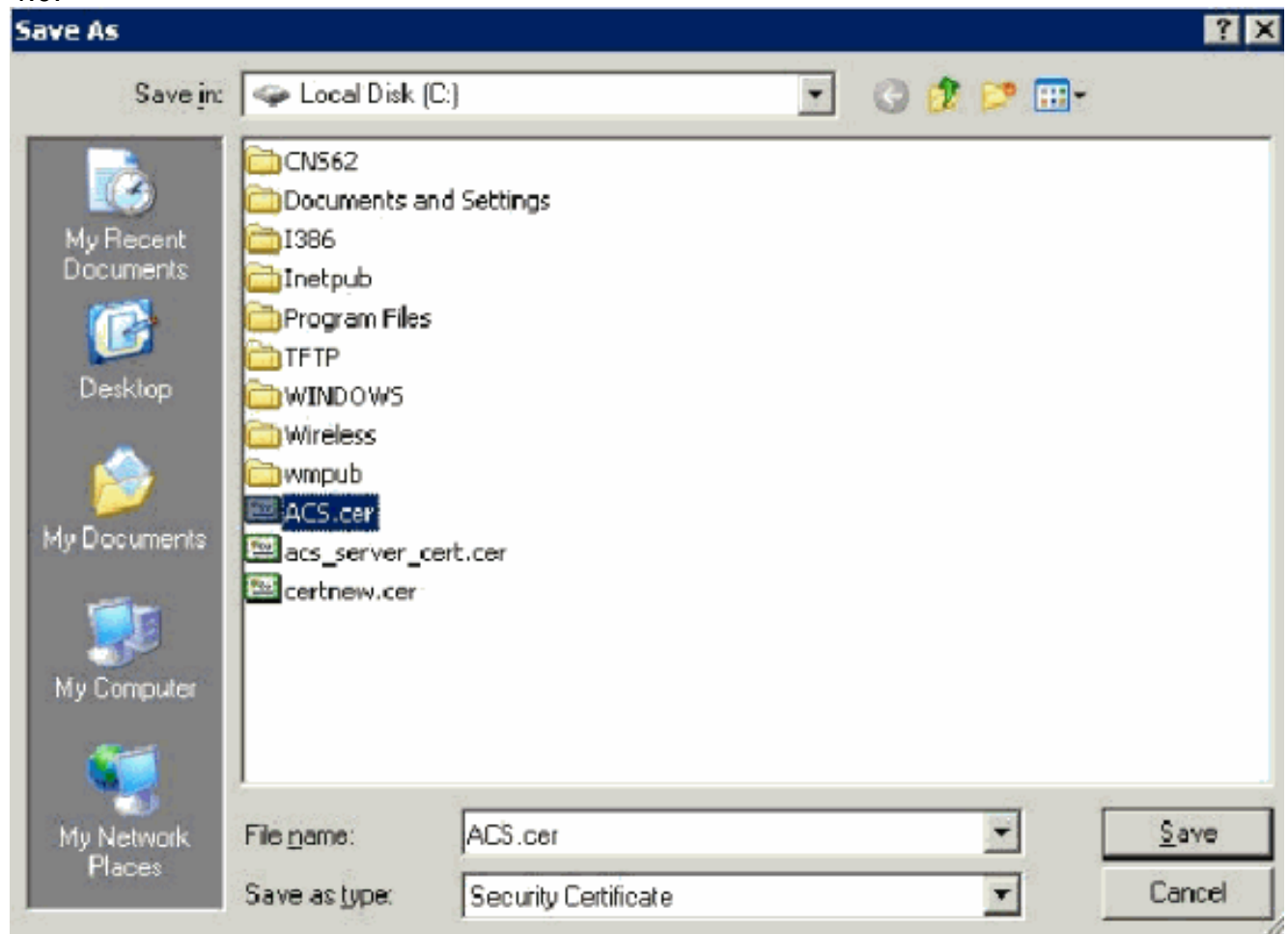
4. Uma janela Aviso de segurança de download de arquivo é exibida. Click



Save.

5. Salve o arquivo com um nome como ACS.cer ou qualquer nome que desejar. Lembre-se desse nome, pois ele é usado durante a configuração da autoridade de certificação ACS no ACS

4.0.



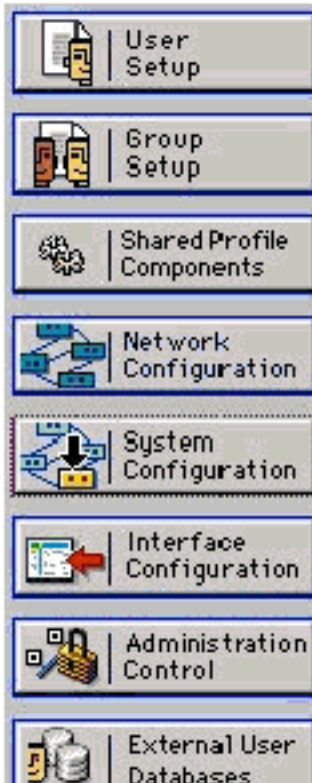
6. Abra o **ACS Admin** do atalho da área de trabalho criado durante a instalação.

7. Clique em **Configuração do**



System Configuration

Select



- [Service Control](#)
- [Logging](#)
- [Date Format Control](#)
- [Local Password Management](#)
- [ACS Internal Database Replication](#)
- [ACS Backup](#)
- [ACS Restore](#)
- [ACS Service Management](#)
- [VoIP Accounting Configuration](#)
- [ACS Certificate Setup](#)
- [Global Authentication Setup](#)

sistema.

8. Clique em ACS Certificate Setup (Configuração do certificado ACS).

System Configuration

Select

ACS Certificate Setup

-  [Install ACS Certificate](#)
-  [ACS Certification Authority Setup](#)
-  [Edit Certificate Trust List](#)
-  [Certificate Revocation Lists](#)
-  [Generate Certificate Signing Request](#)
-  [Generate Self-Signed Certificate](#)

Cancel

9. Clique em Install ACS Certificate (Instalar certificado ACS).

System Configuration

Edit

Install ACS Certificate

Install new certificate 	
<input type="radio"/> Read certificate from file	
Certificate file	<input type="text"/>
<input checked="" type="radio"/> Use certificate from storage	
Certificate CN	<input type="text"/>
Private key file	<input type="text"/>
Private key password	<input type="text"/>

10. Escolha **Usar certificado do armazenamento** e digite o nome de domínio totalmente qualificado de `cisco_w2003.wirelessdemo.local` (ou `ACS.wirelessdemo.local` se você usou o ACS como o

nome).

System Configuration

Edit

Install ACS Certificate

Install new certificate 

Read certificate from file

Certificate file

Use certificate from storage

Certificate CN

Private key file


Private key password

11. Clique em Submit.

System Configuration

Edit

Install ACS Certificate

Installed Certificate Information 

Issued to:	cisco_w2003.wirelessdemo.local
Issued by:	wirelessdemoca
Valid from:	March 17 2006 at 08:33:25
Valid to:	March 16 2008 at 08:33:25
Validity:	OK


The current configuration has been changed. Restart ACS in "System Configuration:Service Control" to adopt the new settings for EAP-TLS or PEAP support only.

12. Clique em Configuração do sistema.


13. Clique em **Controle de serviço** e em **Reiniciar**.

System Configuration

Select

CiscoSecure ACS on cisco_w2003 

Is Currently Running

Services Log File Configuration 

Level of detail

None

Low

Full

Generate New File

Every day

Every week


Every month

When size is greater than KB

Manage Directory

Keep only the last files

Delete files older than days

 [Back to Help](#)

14. Clique em **Configuração do sistema**.
15. Clique em **Configuração de autenticação global**.
16. Marque **Permitir EAP-TLS** e todas as caixas abaixo dele.

System Configuration

Global Authentication Setup

EAP Configuration

PEAP

Allow EAP-MSCHAPv2

Allow EAP-GTC

Allow Posture Validation

Cisco client initial message:

PEAP session timeout (minutes):

Enable Fast Reconnect:

EAP-FAST

[EAP-FAST Configuration](#)

EAP-TLS

Allow EAP-TLS

Select one or more of the following options:

- Certificate SAN comparison
- Certificate CN comparison
- Certificate Binary comparison

EAP-TLS session timeout (minutes):

17. Clique em **Enviar + Reiniciar**.
18. Clique em **Configuração do sistema**.
19. Clique em **ACS Certification Authority Setup**.
20. Na janela ACS Certification Authority Setup, digite o nome e o local do arquivo *.cer criado anteriormente. Neste exemplo, o arquivo *.cer criado é **ACS.cer** no diretório raiz c:\.
21. Digite **c:\acs.cer** no campo de arquivo de certificado CA e clique em **Enviar**.

System Configuration

ACS Certification Authority Setup

CA Operations

Add new CA certificate to local certificate storage

CA certificate file

System Configuration

ACS Certification Authority Setup

CA Operations

Add new CA certificate to local certificate storage

CA certificate file

The current configuration has been changed. Restart ACS in "System Configuration:Service Control" to adopt the new settings for EAP-TLS or PEAP support only.

New CA certificate is successfully added into the global system certificate storage.

CA certificate common name	wirelessdemo.ca
----------------------------	-----------------

22. Reinicie o serviço ACS.

[Configuração do CLIENTE para EAP-TLS usando Windows Zero Touch](#)

CLIENTE é um computador que executa o Windows XP Professional com SP2 que atua como um cliente sem fio e obtém acesso aos recursos da Intranet por meio do AP sem fio. Conclua os procedimentos nesta seção para configurar o CLIENTE como um cliente sem fio.

[Executar uma instalação e configuração básicas](#)

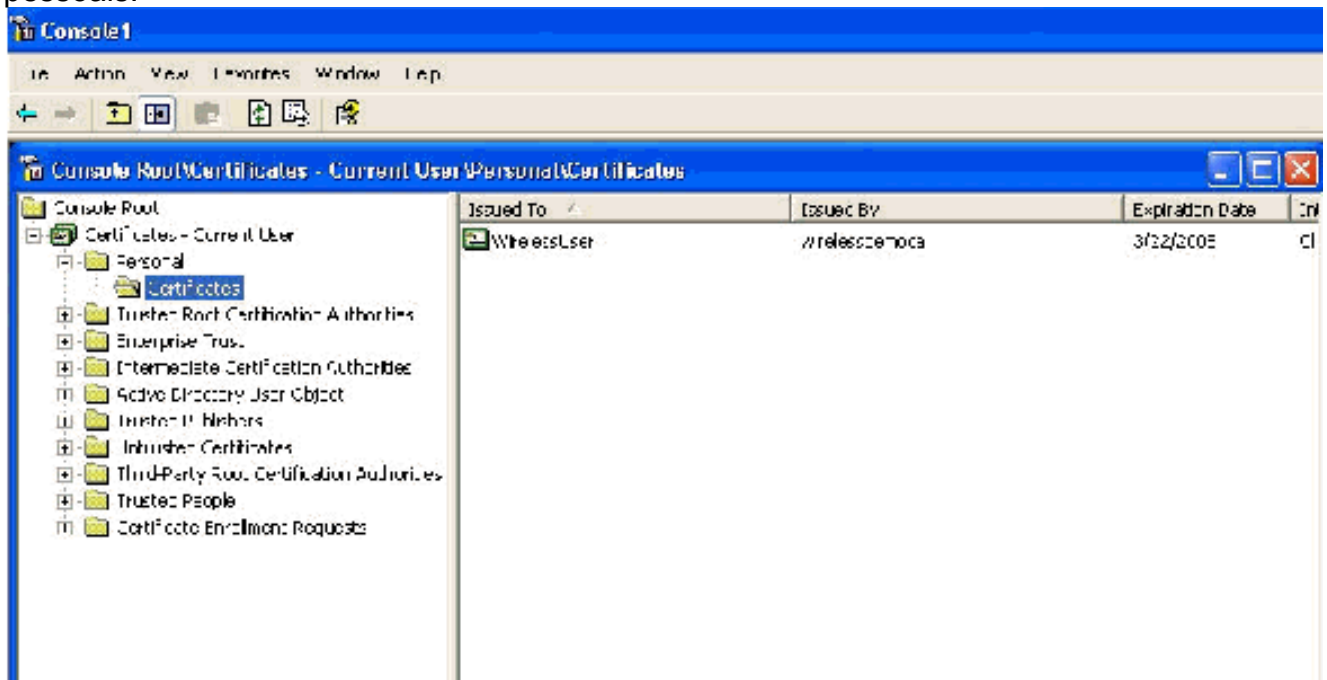
Conclua estes passos:

1. Conecte CLIENTE ao segmento de rede da Intranet usando um cabo Ethernet conectado ao switch.
2. No CLIENTE, instale o Windows XP Professional com SP2 como um computador membro chamado **CLIENT** no domínio wireless demo.local.
3. Instale o Windows XP Professional com SP2. Ele deve ser instalado para ter suporte EAP-TLS e PEAP. **Observação:** o Firewall do Windows é ativado automaticamente no Windows XP Professional com SP2. Não desligue o firewall.

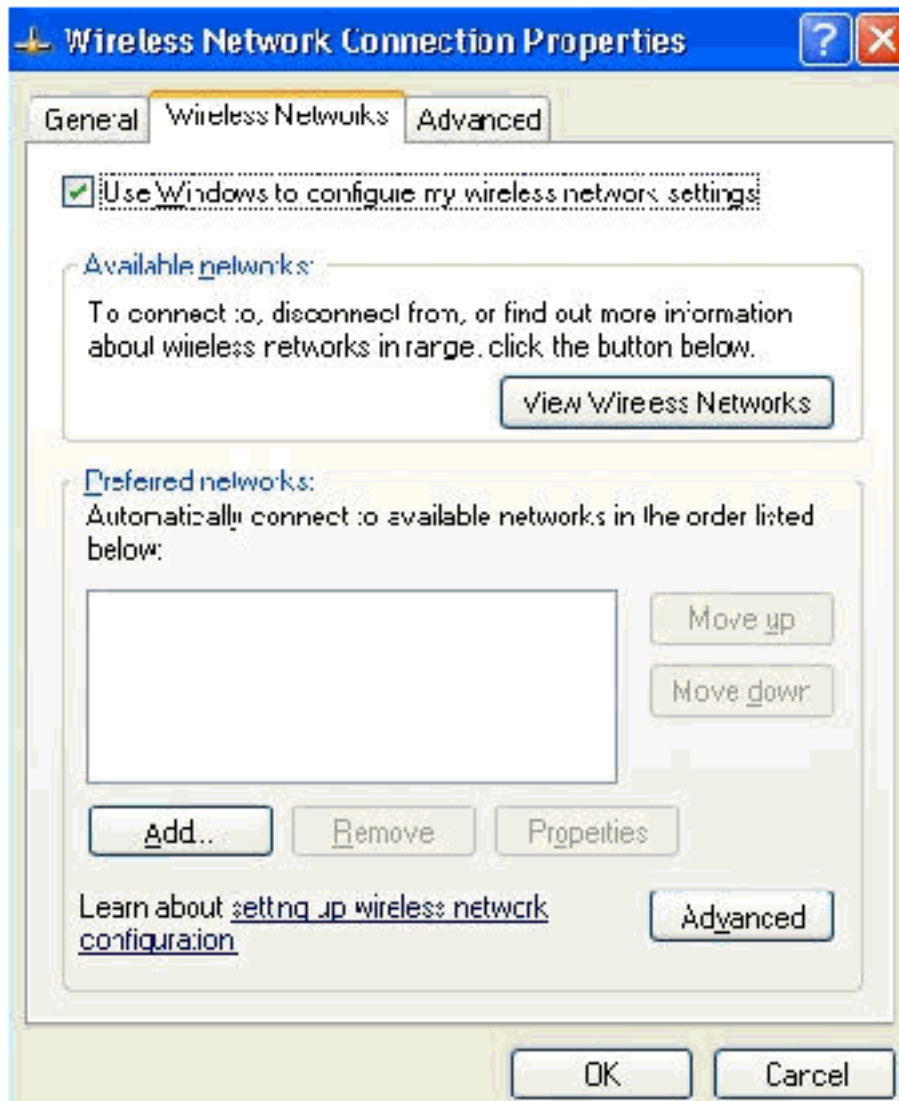
[Configure a conexão de rede sem fio](#)

Conclua estes passos:

1. Faça logoff e, em seguida, faça logon usando a conta WirelessUser no domínio wirelessdemo.local. **Observação:** atualize as configurações do computador e do grupo de configuração do usuário e obtenha um certificado de computador e usuário para o computador cliente sem fio imediatamente, digitando **gpupdate** em um prompt de comando. Caso contrário, quando você faz logoff e depois faz logon, ele executa a mesma função que **gpupdate**. Você deve estar conectado ao domínio conectando-se por meio do fio. **Observação:** para validar se o certificado está instalado automaticamente no cliente, abra o certificado MMC e valide se o certificado WirelessUser está disponível na pasta Certificados pessoais.

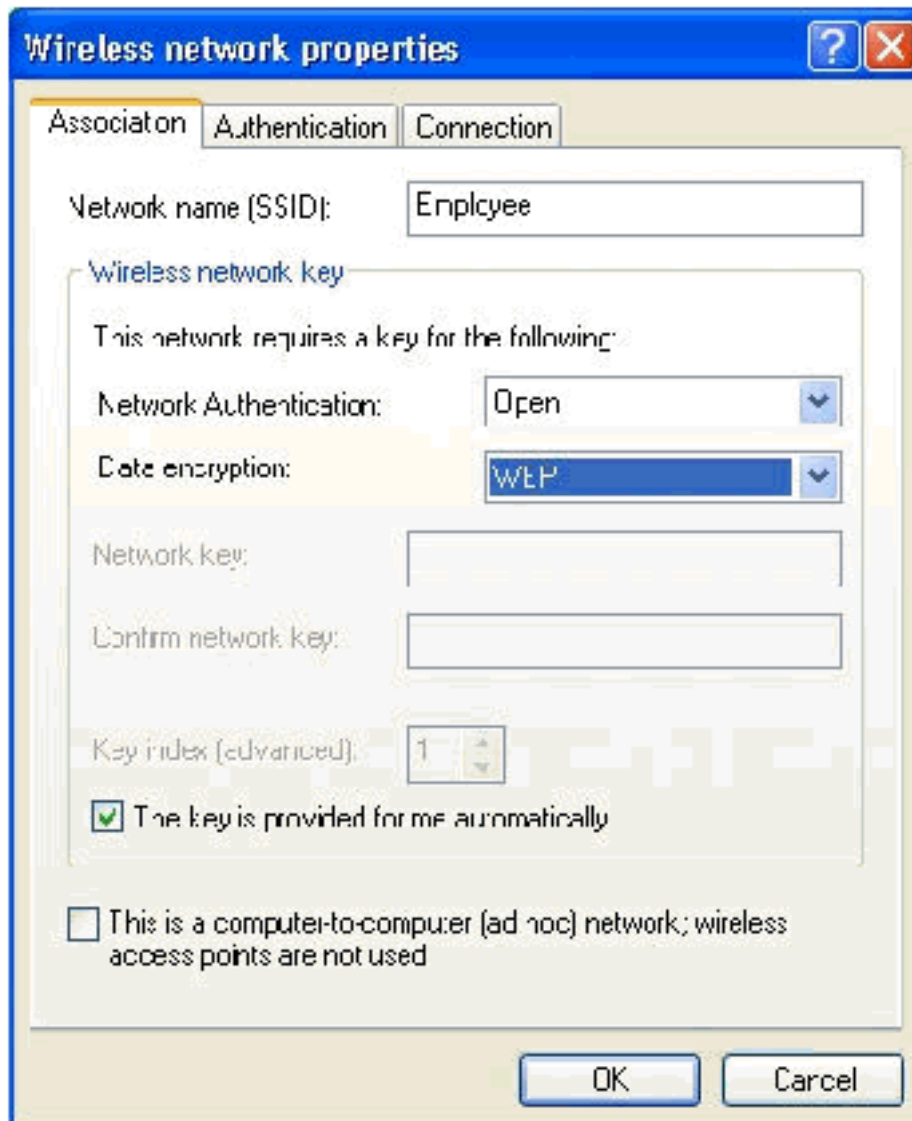


2. Escolha **Iniciar > Painel de controle**, clique duas vezes em **Conexões de rede** e clique com o botão direito do mouse em **Conexão de rede sem fio**.
3. Clique em **Propriedades**, vá para a guia **Redes sem fio** e verifique se o **Windows do usuário para configurar minhas configurações de rede sem fio** está



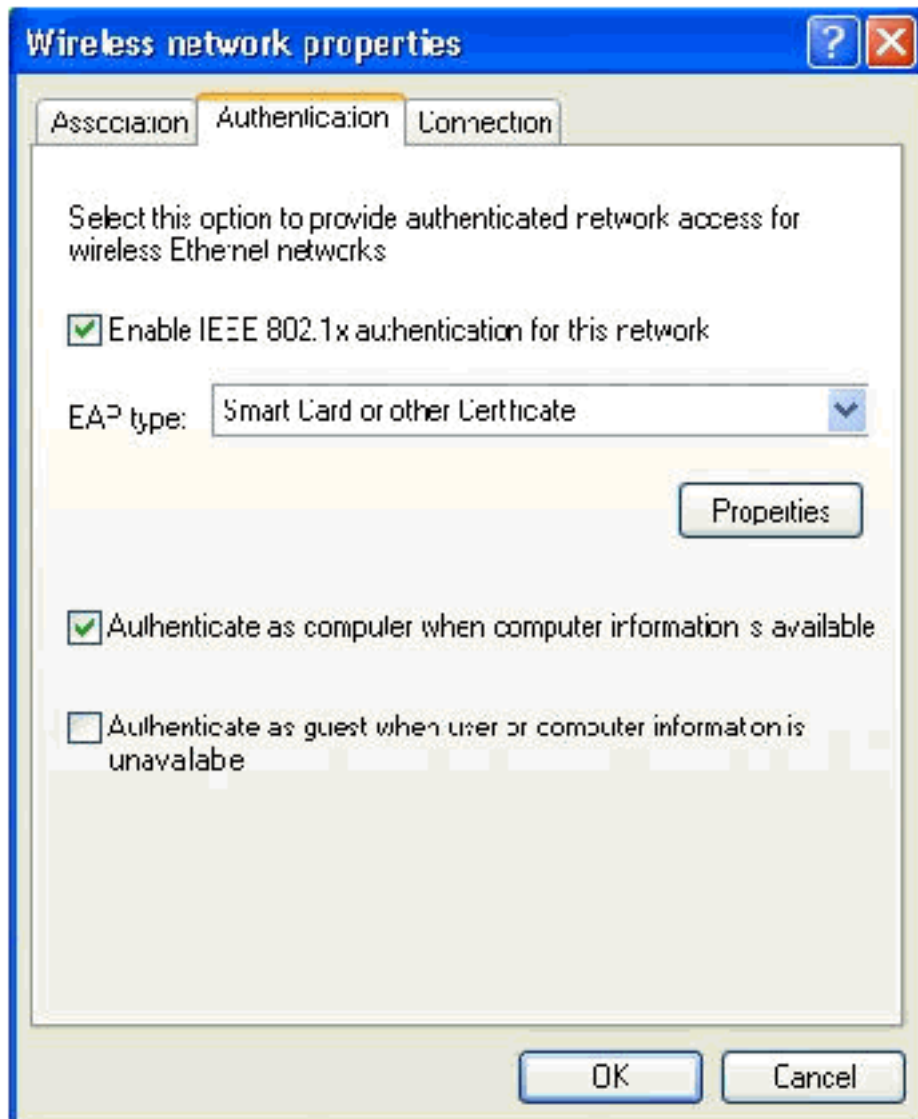
marcado.

4. Clique em Add.
5. Vá até a guia Associação e digite **Funcionário** no campo Nome da rede (SSID).
6. Verifique se Data Encryption (Criptografia de dados) está definido como **WEP** e a **chave é fornecida para mim automaticamente** está



marcada.

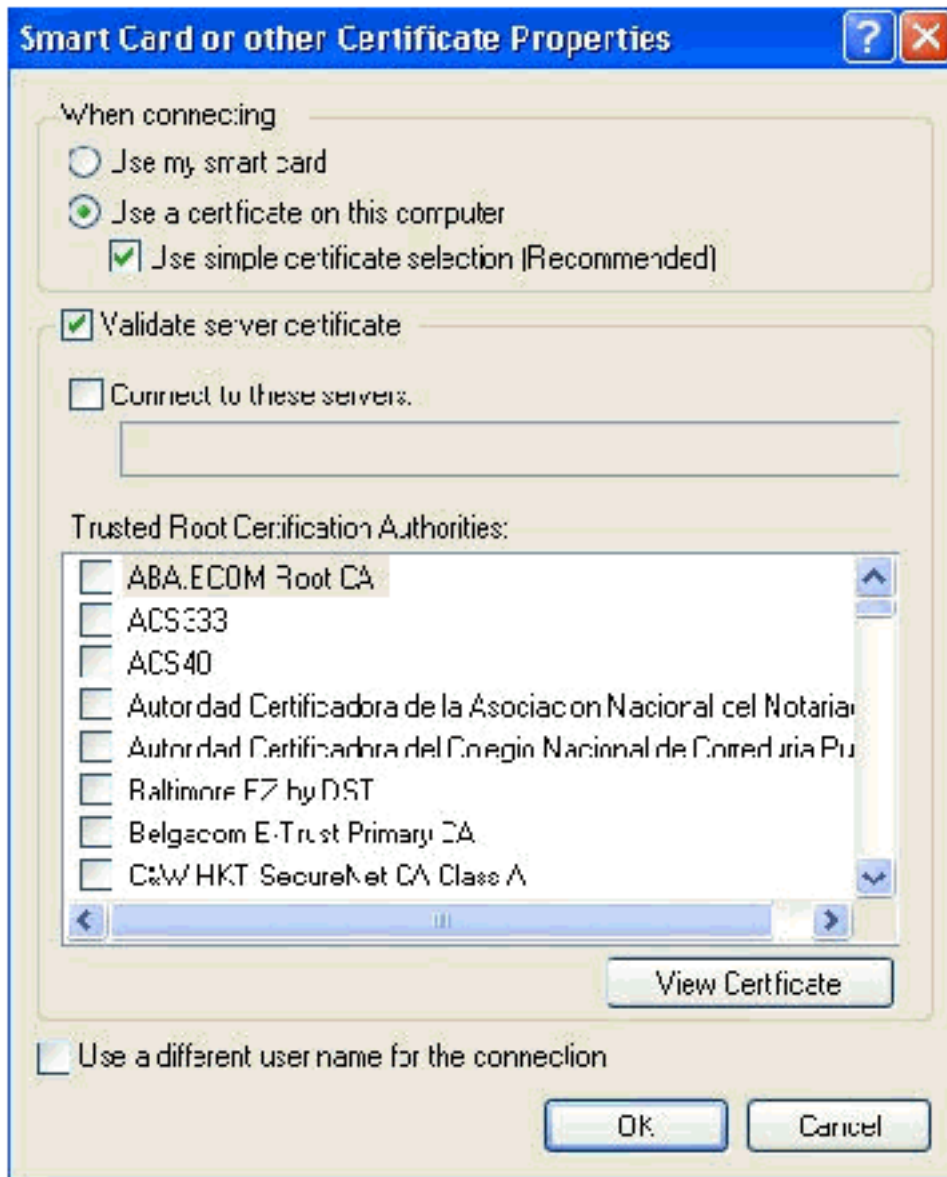
7. Vá até a guia Autenticação.
8. Confirme se o tipo de EAP está configurado para utilizar **Smart Card** ou **outro certificado**. Se não estiver, selecione-o no menu suspenso.
9. Se você quiser que a máquina seja autenticada antes do login (o que permite que scripts de login ou push de política de grupo sejam aplicados), escolha a opção **Autenticar como computador quando as informações do computador estiverem**



disponíveis.

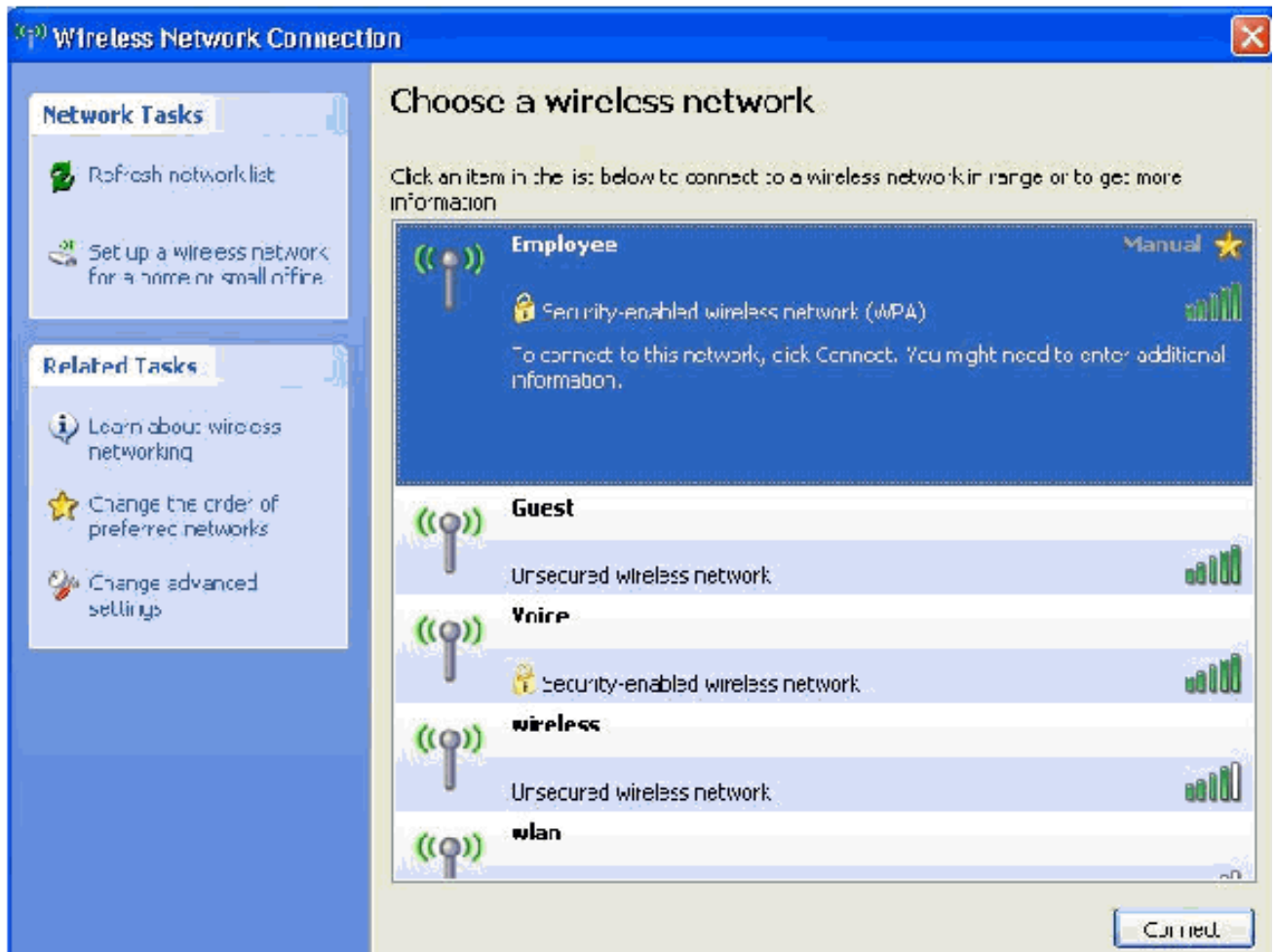
10. Clique em Propriedades.

11. Verifique se as caixas nessa janela estão

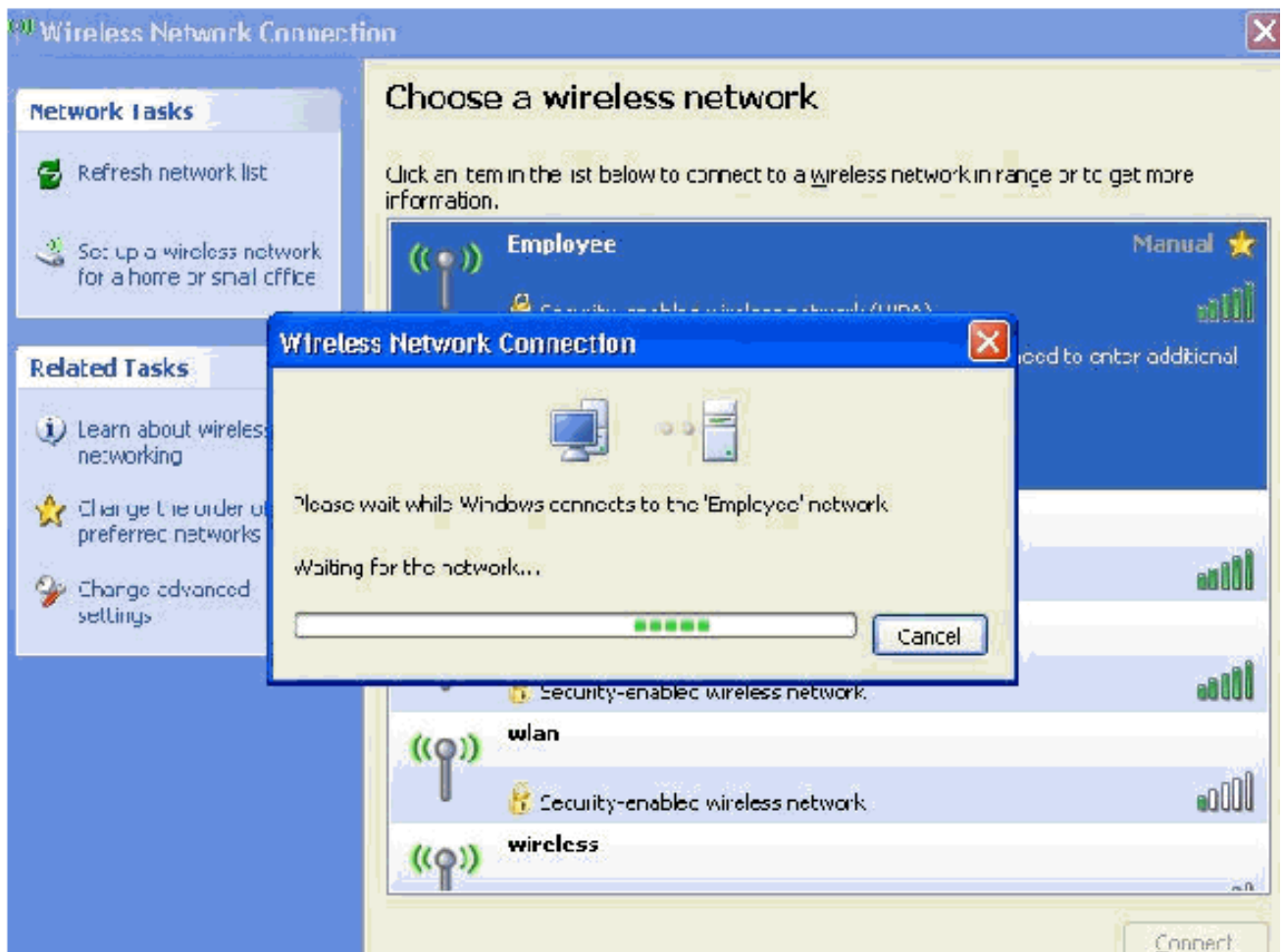


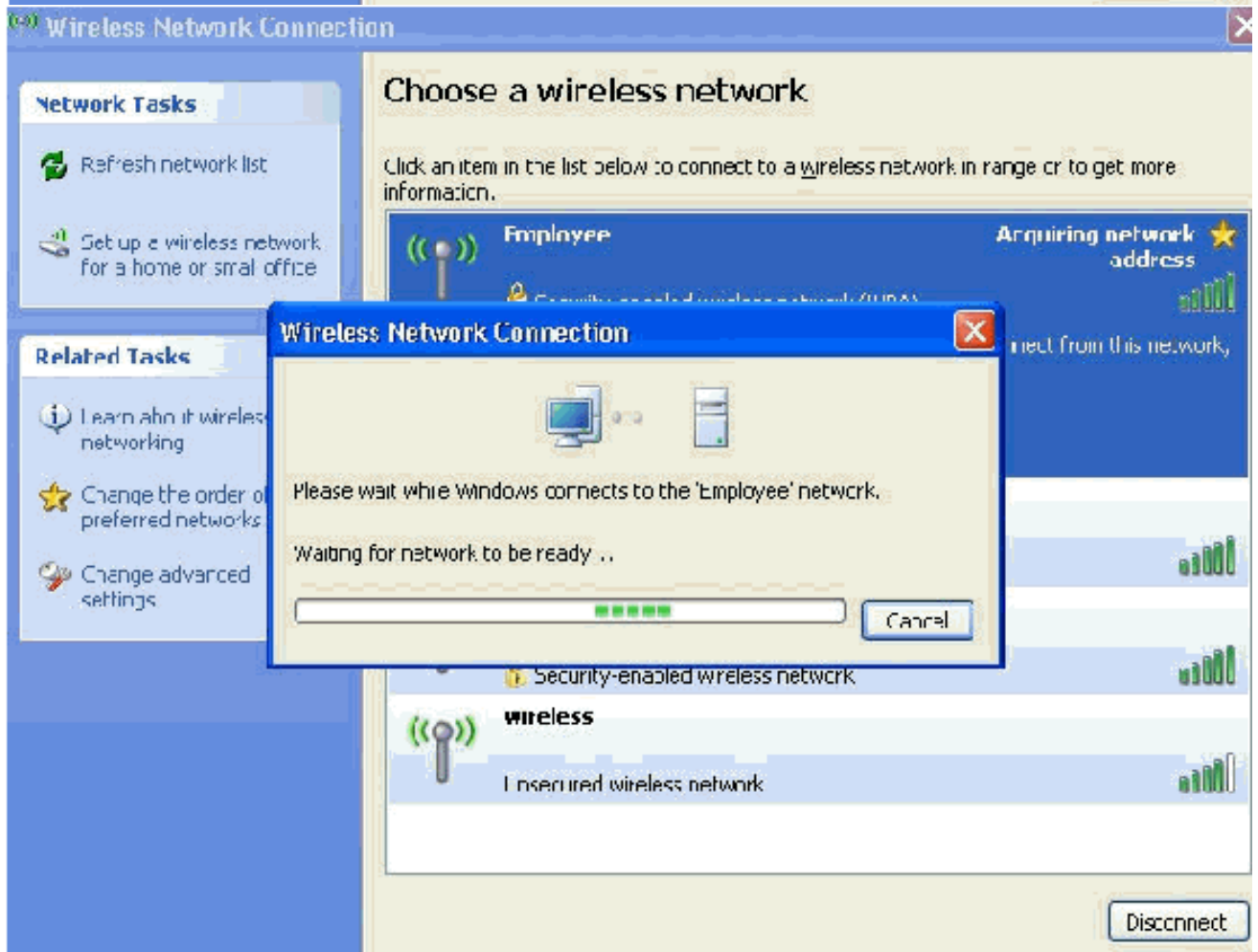
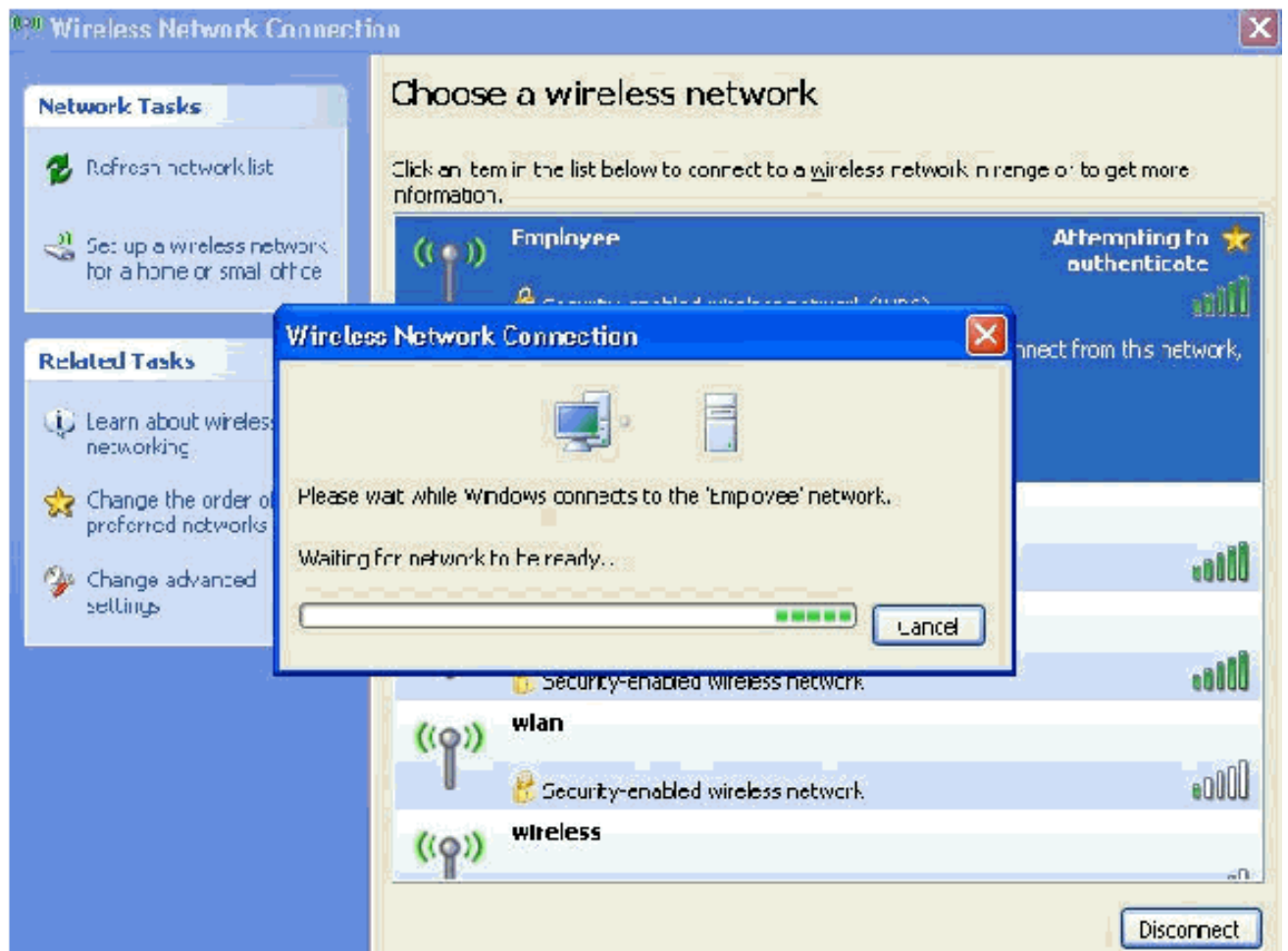
marcadas.

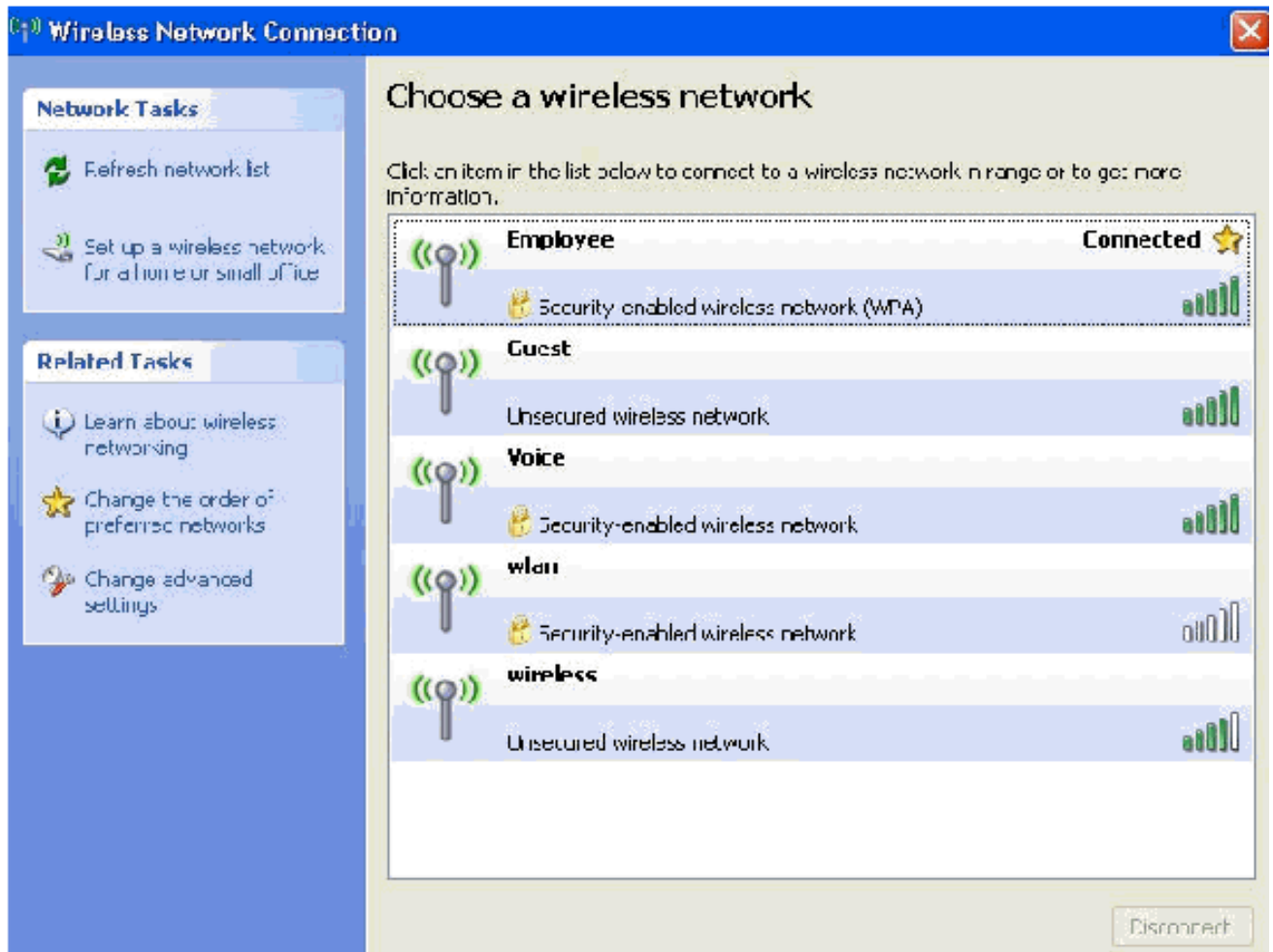
12. Clique em **OK** três vezes.
13. Clique com o botão direito do mouse no ícone de conexão de rede sem fio na bandeja do sistema e clique em **Exibir redes sem fio disponíveis**.
14. Clique na rede sem fio **do funcionário** e clique em **Conectar**.



Essas capturas de tela indicam se a conexão foi concluída com êxito.







15. Depois que a autenticação for bem-sucedida, verifique a configuração TCP/IP do adaptador sem fio usando Conexões de rede. Ele deve ter um intervalo de endereços de 172.16.100.100-172.16.100.254 do escopo DHCP ou do escopo criado para os clientes sem fio.
16. Para testar a funcionalidade, abra um navegador e navegue até <http://wirelessdemoca> (ou o endereço IP do servidor de CA empresarial).

Informações Relacionadas

- [Exemplo de Configuração de Autenticação EAP com Controladores WLAN \(WLC\)](#)
- [Guia de configuração do controlador de LAN sem fio](#)
- [Exemplo de configuração básica dos controladores LAN sem fio e do access point lightweight](#)
- [VLANs no exemplo de configuração de Wireless LAN Controllers](#)
- [Exemplo de configuração de VLANs de grupo de AP com controladores de LAN sem fio](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)