PEAP em UWNs com ACS 5.1 e Windows 2003 Server

Contents

Introduction

Este documento descreve como configurar o acesso wireless seguro usando controladores de

LAN Wireless, o software Microsoft Windows 2003 e o Cisco Secure Access Control Server (ACS) 5.1 via Protected Extensible Authentication Protocol (PEAP) com a versão 2 do Microsoft Challenge Handshake Authentication Protocol (MS-CHAP).

Observação: para obter informações sobre a implantação de redes sem fio seguras, consulte o site Microsoft Wi-Fi e o Cisco SAFE Wireless Blueprint.

Prerequisites

Requirements

Presume-se que o instalador tenha conhecimento da instalação básica do Windows 2003 e da instalação do Cisco Wireless LAN Controller, pois este documento abrange apenas as configurações específicas para facilitar os testes.

Para obter informações sobre a instalação e a configuração iniciais dos Cisco 5508 Series Controllers, consulte o Guia de Instalação do Cisco 5500 Series Wireless Controller. Para obter informações sobre a instalação e a configuração iniciais dos Cisco 2100 Series Controllers, consulte o Guia de Início Rápido: Cisco 2100 Series Wireless LAN Controller.

Os guias de instalação e configuração do Microsoft Windows 2003 podem ser encontrados em Instalando o Windows Server 2003 R2 .

Antes de começar, instale o sistema operacional Microsoft Windows Server 2003 com SP1 em cada um dos servidores no laboratório de teste e atualize todos os Service Packs. Instale as controladoras e os pontos de acesso lightweight (LAPs) e verifique se as atualizações de software mais recentes estão configuradas.

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 PEAP possa ser configurada. A inscrição automática e a renovação automática de certificados 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 2106 ou 5508 Series com 7.0.98.0
- AP Cisco 1142 Lightweight Access Point Protocol (LWAPP)
- Windows 2003 Enterprise com Internet Information Server (IIS), Certificate Authority (CA), DHCP e Domain Name System (DNS) instalados
- Cisco 1121 Secure Access Control System Appliance (ACS) 5.1
- Windows XP Professional com SP (e Service Packs atualizados) e placa de interface de rede sem fio (NIC) (com suporte ao CCX v3) ou solicitante de terceiros.
- Switch Cisco 3750

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.

Configurar

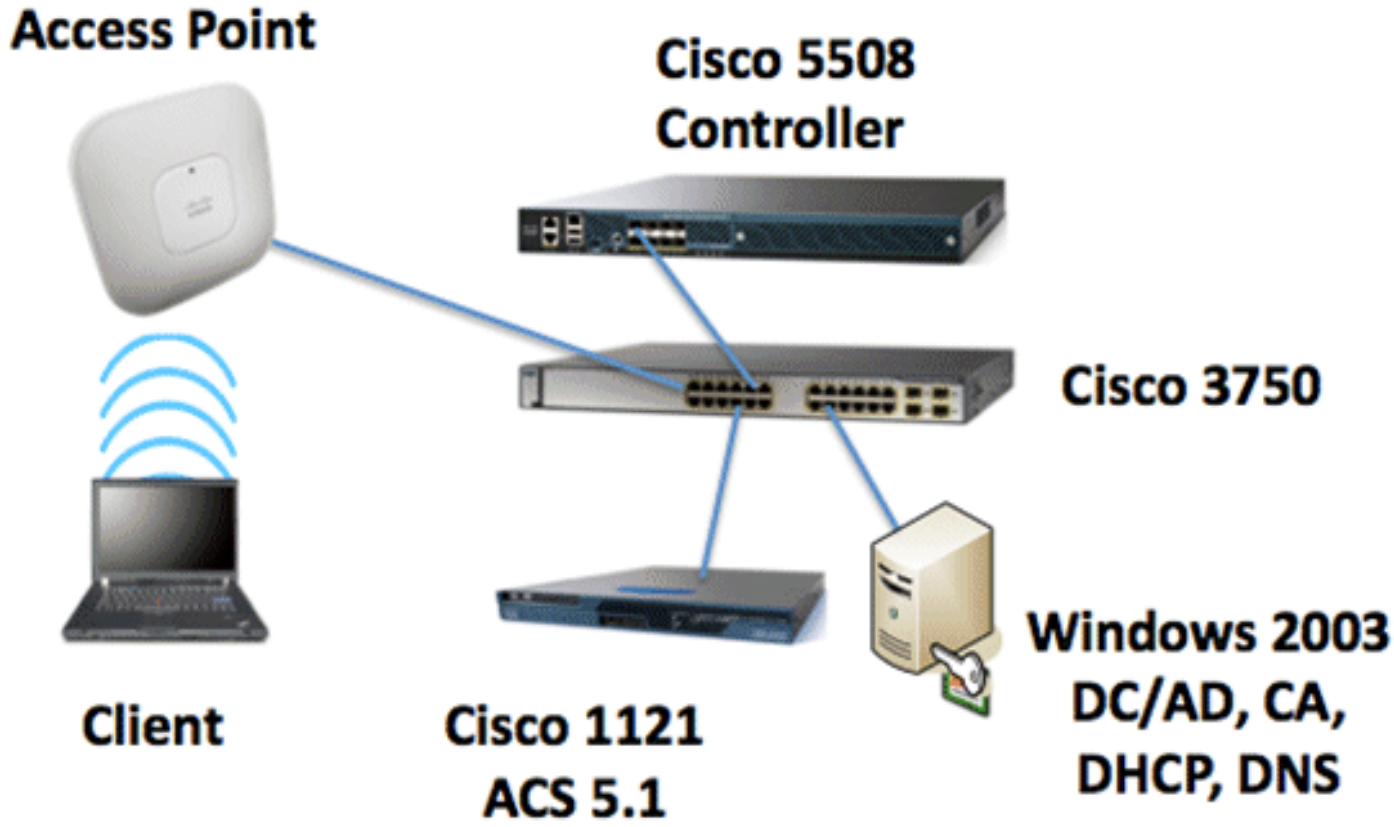
Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

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 o procedimento passo a passo para implementar o PEAP em Unified Wireless Networks com ACS 5.1 e o Windows 2003 Enterprise Server. A ênfase principal está no registro automático do cliente, de modo que o cliente faça o registro automático e obtenha o certificado do servidor.

Observação: para adicionar WPA/WPA2 (Wi-Fi Protected Access) com TKIP/AES (Temporal Key Integrity Protocol) ao Windows XP Professional com SP, consulte a atualização WPA2/Wireless Provisioning Services Information Element (WPS IE) para Windows XP com Service Pack 2 .

Instalação do Windows Enterprise 2003 com IIS, Autoridade de Certificação, DNS, DHCP (CA)

CA (democracia)

CA é um computador que executa o Windows Server 2003 com SP2, Enterprise Edition e executa estas funções:

- Um controlador de domínio para o domínio **demo.local** que executa o IIS
- Um servidor DNS para o domínio DNS **demo.local**
- Um servidor DHCP
- CA raiz corporativa para o domínio **demo.local**

Execute estas etapas para configurar o CA para estes serviços:

1. Execute uma instalação e configuração básicas.
2. Configure o computador como um controlador de domínio.
3. Elevar 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 fio a computadores.
9. Adicione usuários ao domínio.
10. Permitir acesso sem fio a usuários.
11. Adicionar grupos ao domínio.
12. Adicione usuários ao grupo usuários sem fio.
13. Adicione computadores cliente ao grupo de usuários sem fio.

Executar Instalação e Configuração Básicas

Execute estas etapas:

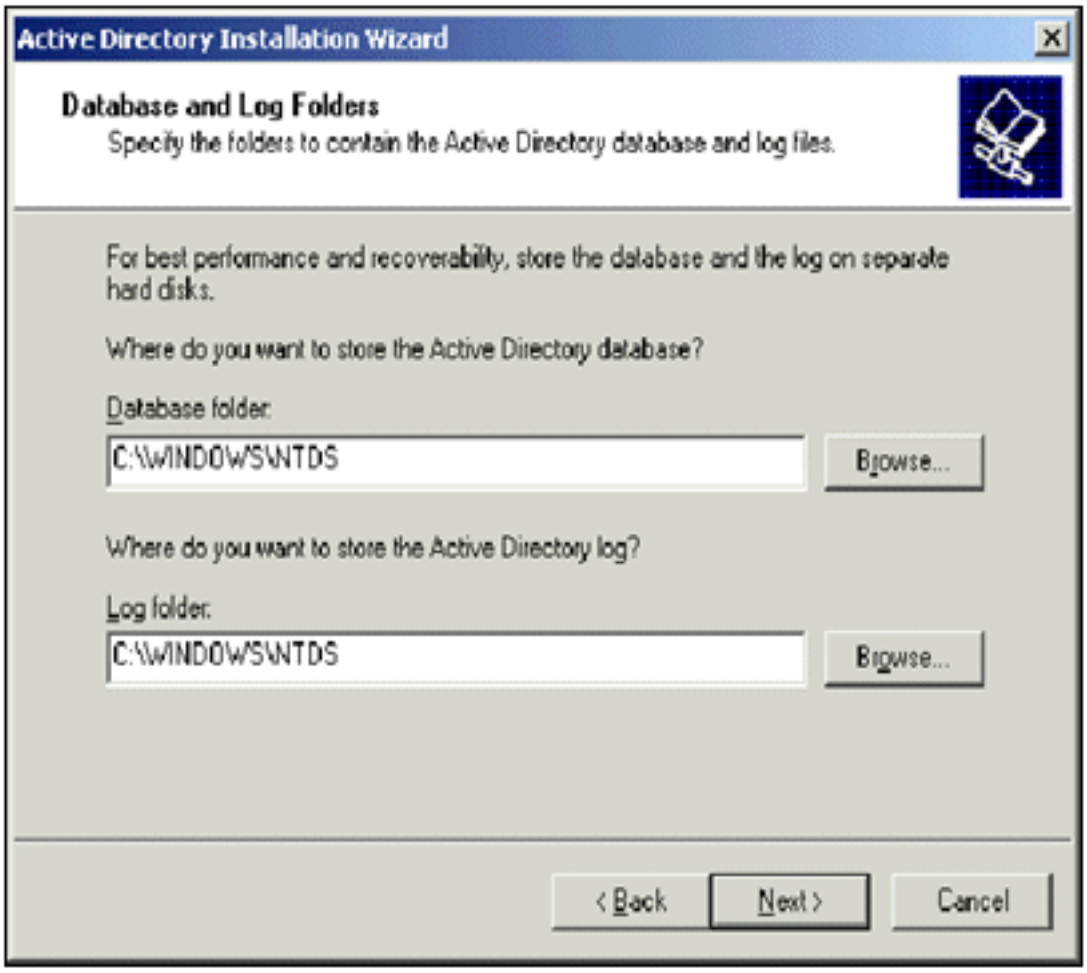
1. Instale o Windows Server 2003 com SP2, Enterprise Edition, como um servidor autônomo.
2. Configure o protocolo TCP/IP com o endereço IP de *10.0.10.10* e a máscara de sub-rede de *255.255.255.0*.

Configurar o computador como um controlador de domínio

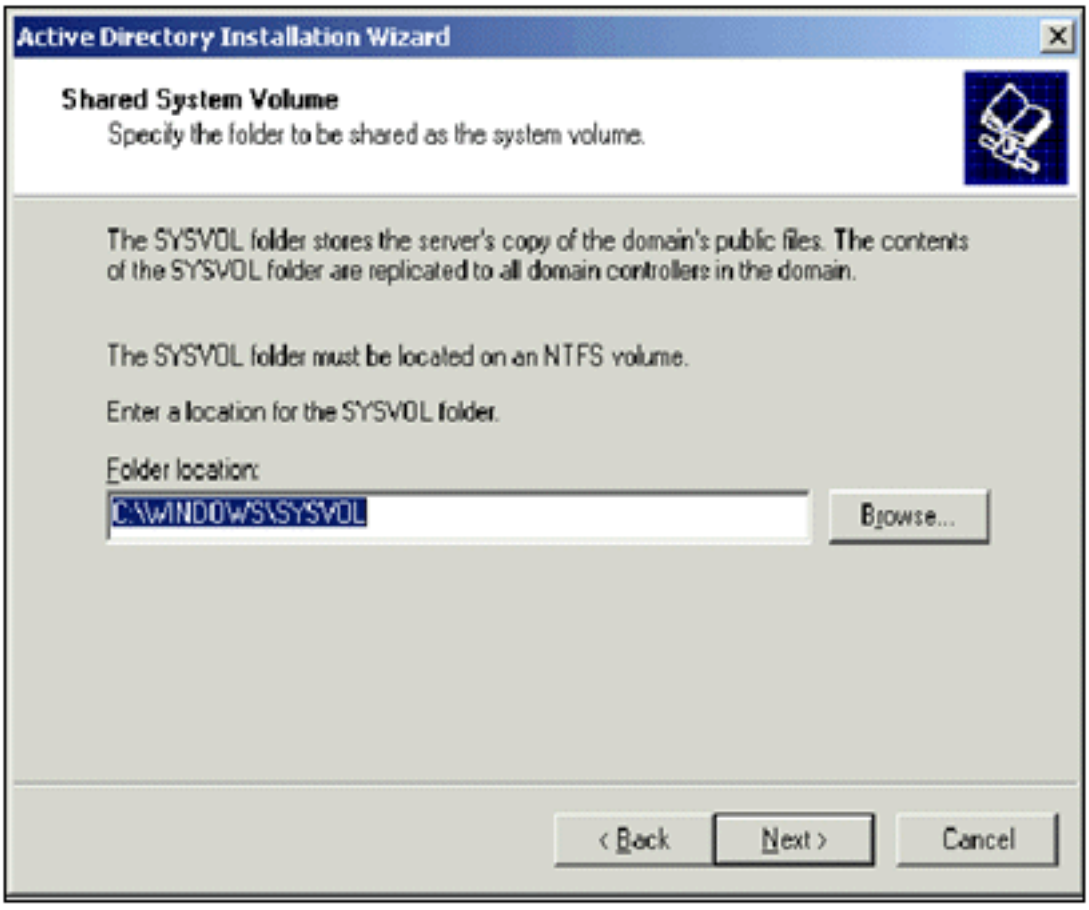
Execute estas etapas:

1. Para iniciar o Assistente de instalação do Ative Diretory, escolha **Iniciar** > **Executar**, **digite dcpromo.exe** e clique em **OK**.
2. Na página Bem-vindo ao Assistente de instalação do Ative Diretory, 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 **Próximo**.
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 **demo.local** e clique em **Avançar**.

8. Na página Nome do domínio NetBIOS, digite o nome NetBIOS do domínio como **demo** e clique em **Avançar**.
9. Na página Localizações de Pastas de Log e Banco de Dados, aceite os diretórios padrão de Pastas de Log e Banco de Dados e clique em

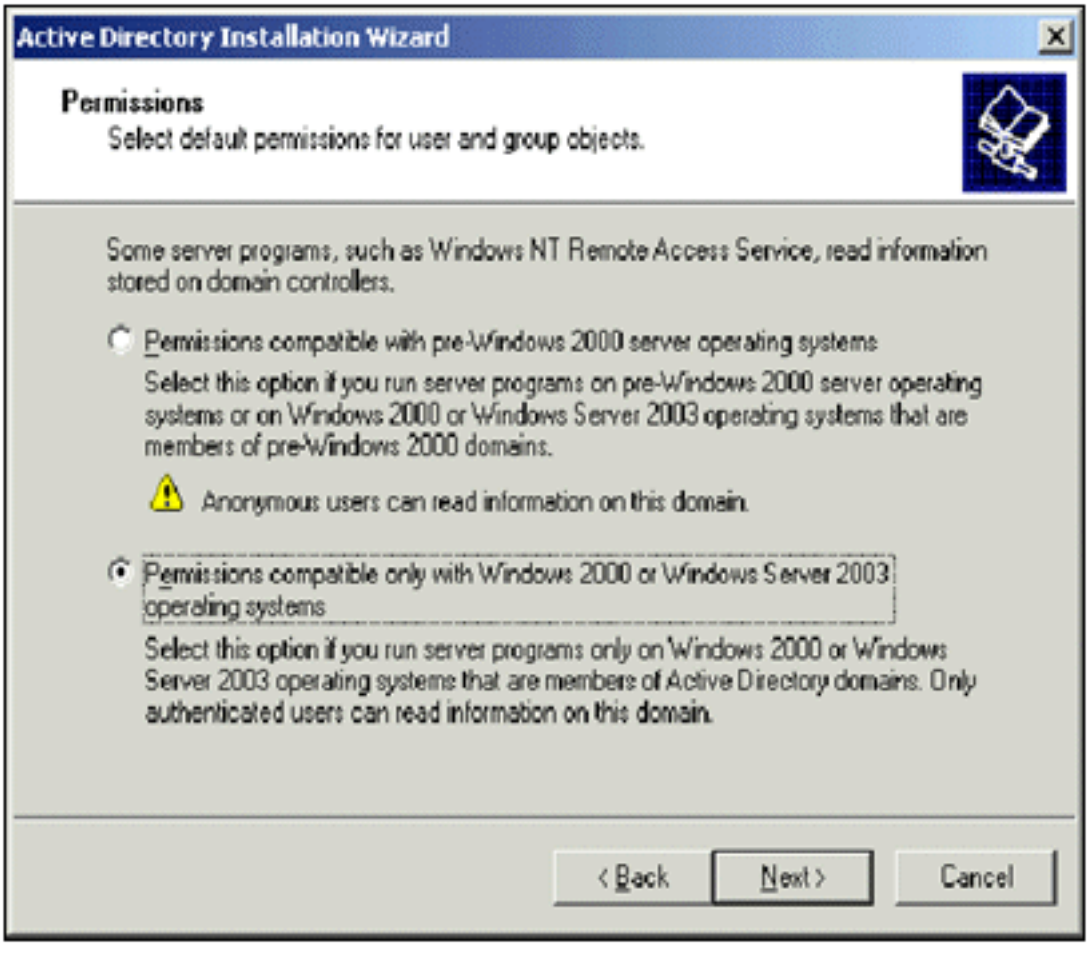


Próximo.
10. Na página Volume de sistema compartilhado, verifique se o local da pasta padrão está correto e clique em



Avançar.

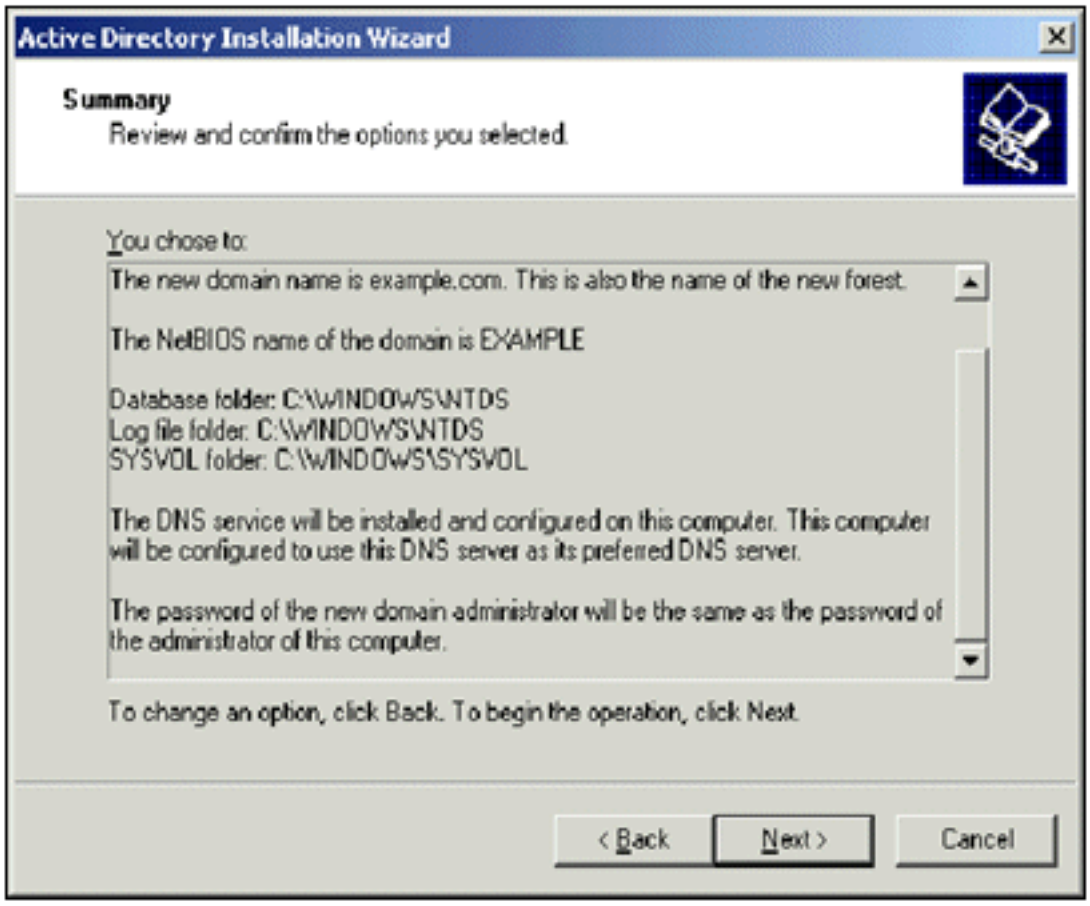
11. Na página Permissões, verifique se **Permissões compatíveis apenas com os sistemas operacionais Windows 2000 ou Windows Server 2003** estão selecionadas e clique em



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 **Próximo**.

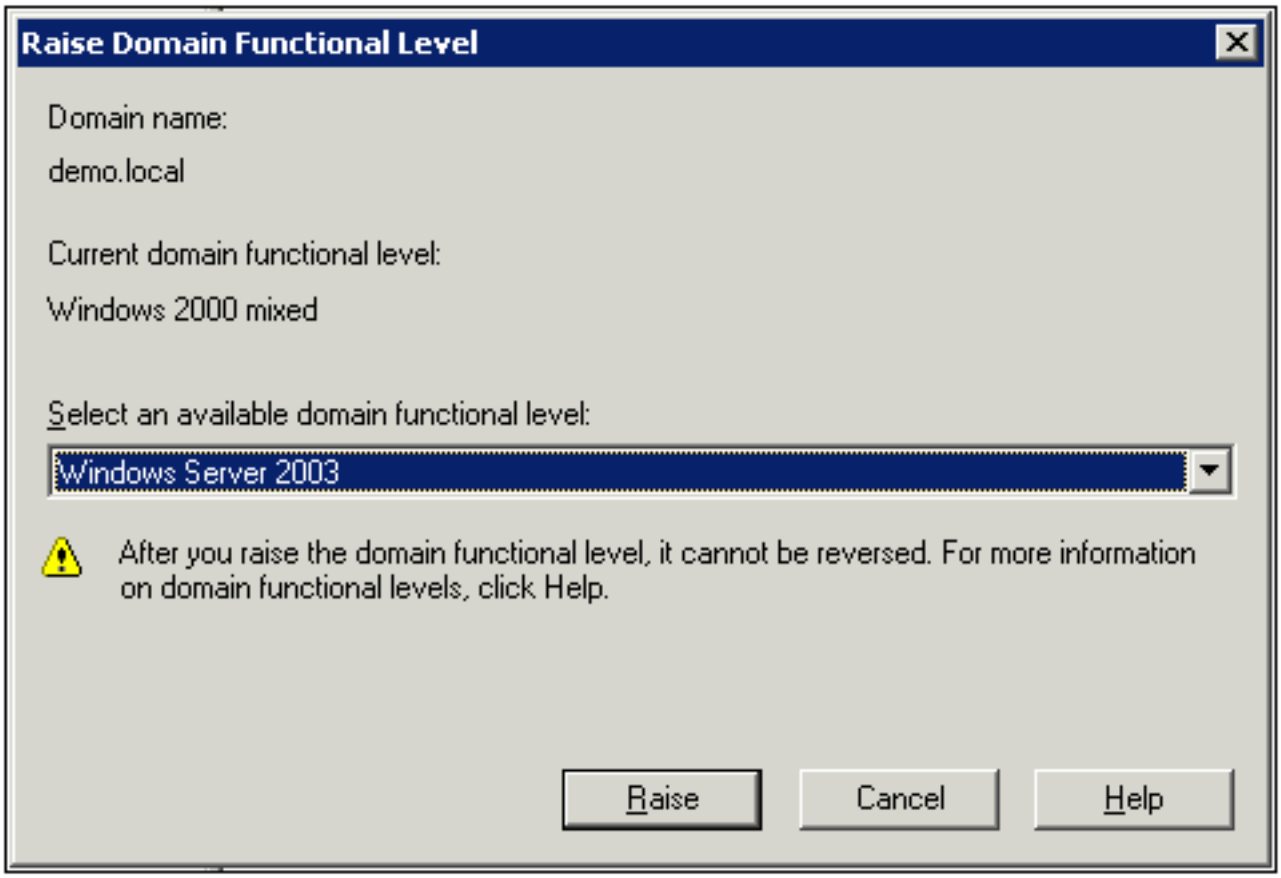


14. Ao concluir a instalação do Ative Diretory, clique em **Concluir**.
15. Quando solicitado a reiniciar o computador, clique em **Reiniciar agora**.

Elevar o nível funcional do domínio

Execute estas etapas:

1. Abra o snap-in Domínios e Relações de Confiança do Ative Diretory na pasta Ferramentas Administrativas (Iniciar > Programas > Ferramentas Administrativas > Domínios e Relações de Confiança do Ative Diretory) e clique com o botão direito do mouse no computador do domínio CA.demo.local.
2. Clique em **Aumentar nível funcional do domínio** e selecione **Windows Server 2003** na página Aumentar nível funcional do
domínio.

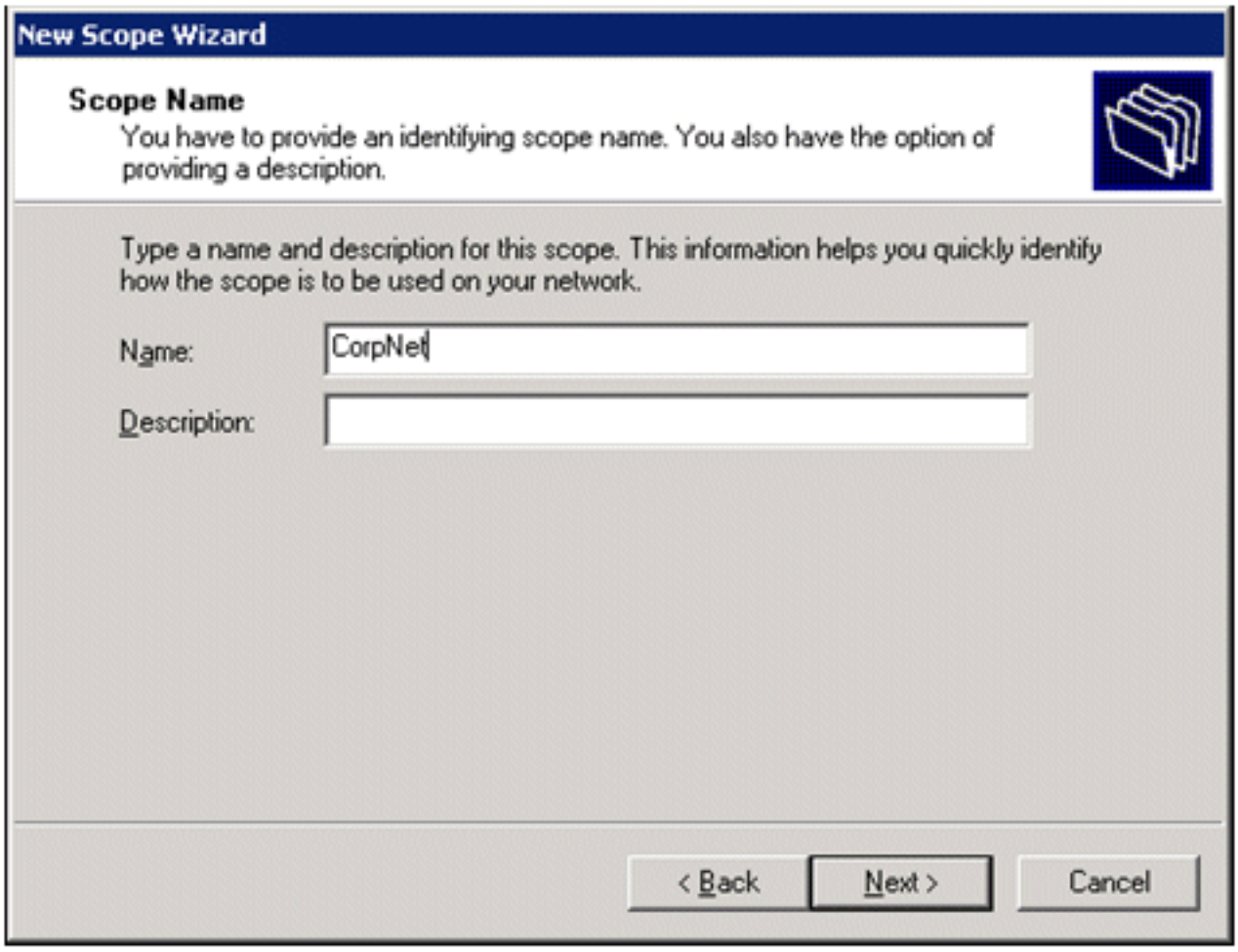


3. Clique em **Raise**, clique em **OK** e em **OK** novamente.

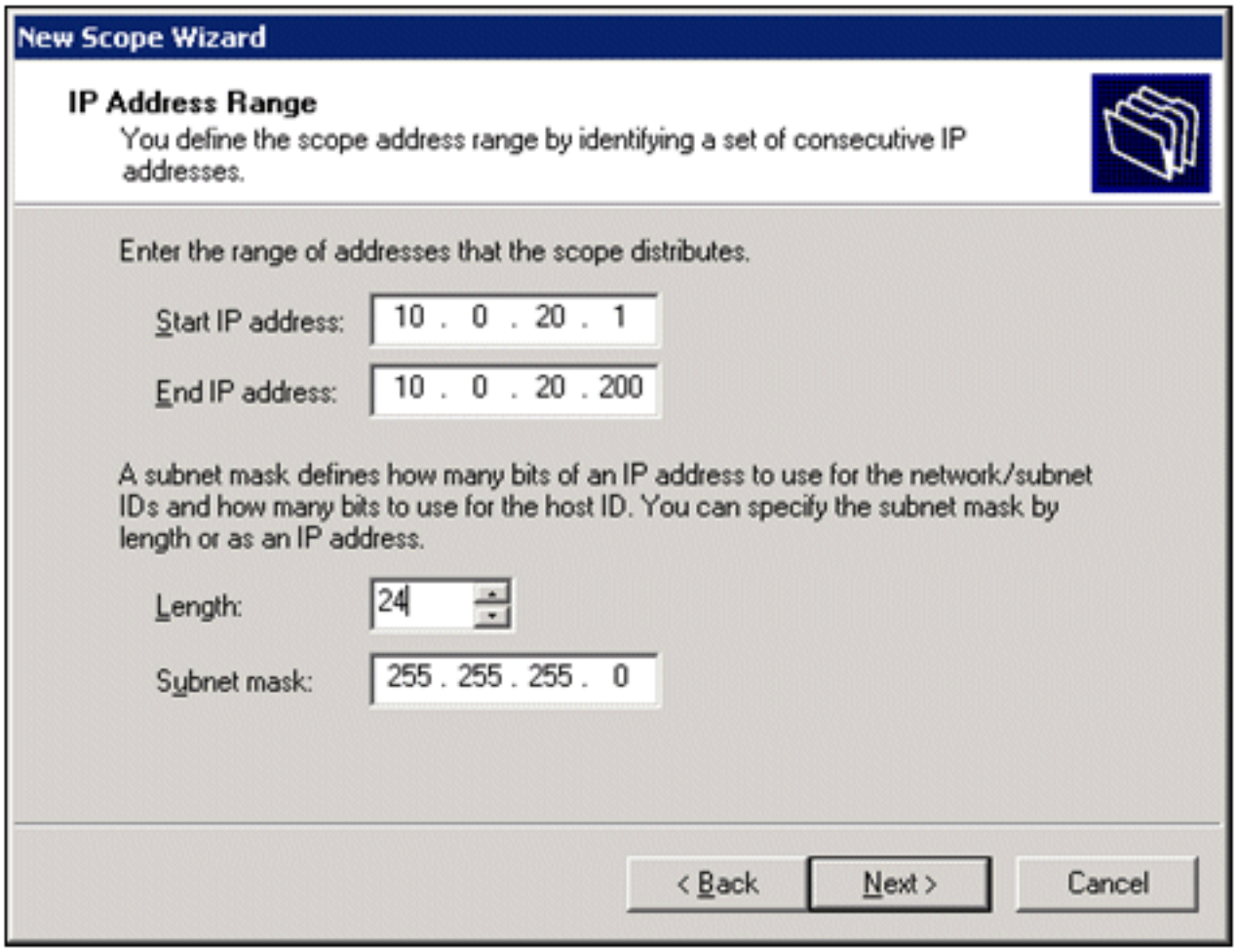
Instalar e configurar o DHCP

Execute estas etapas:

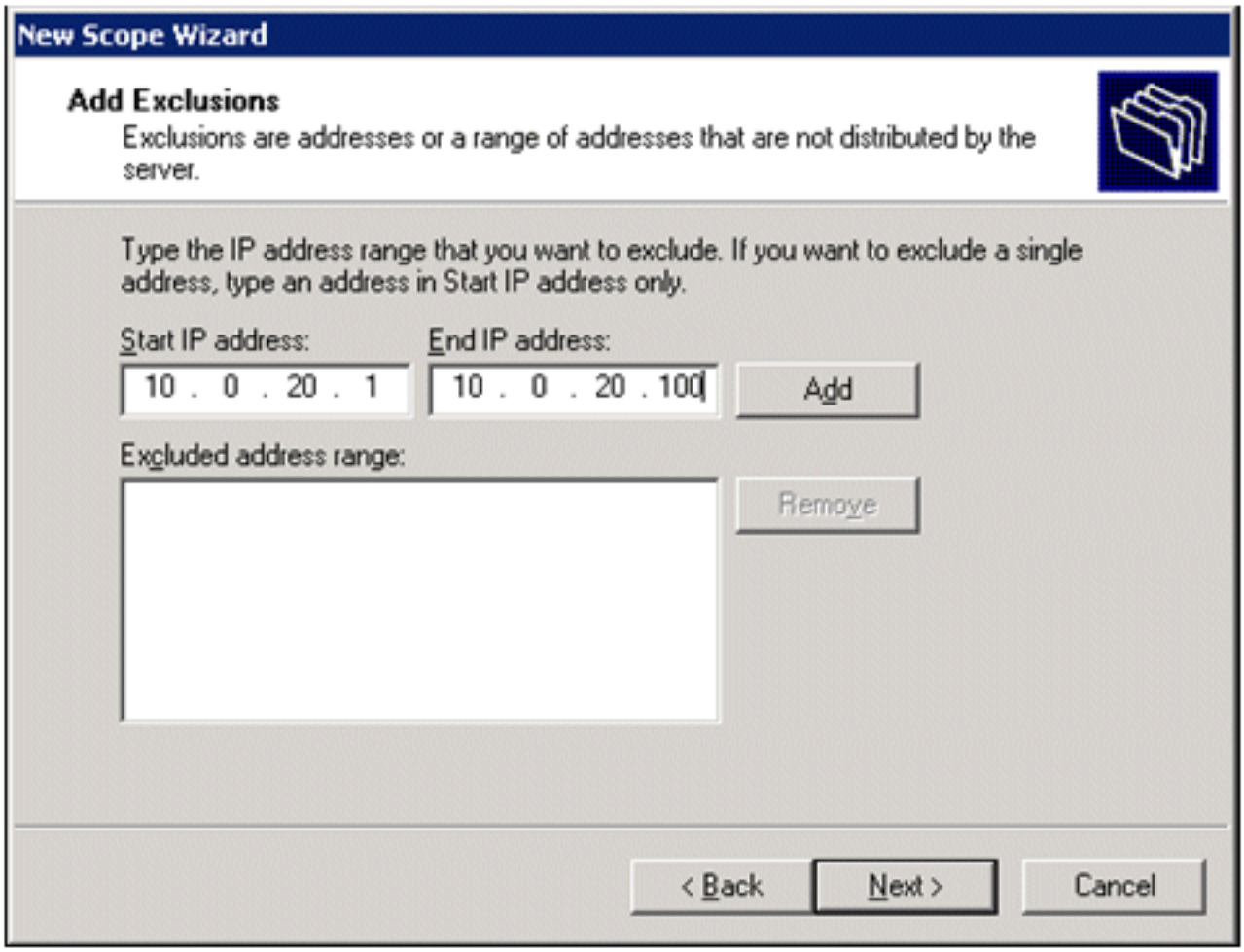
1. Instale o **Dynamic Host Configuration Protocol (DHCP)** como um componente do **Networking Service** usando **Adicionar ou Remover Programas** no Painel de Controle.
2. Abra o snap-in DHCP na pasta Administrative Tools (Iniciar > Programas > Administrative Tools > DHCP) e realce o servidor DHCP, CA.demo.local.
3. Clique em **Action** e, em seguida, clique em **Authorize** para autorizar o serviço DHCP.
4. Na árvore do console, clique com o botão direito do mouse em **CA.demo.local** e clique em **Novo escopo**.
5. Na página Bem-vindo do assistente para Novo escopo, clique em **Próximo**.
6. Na página Nome do escopo, digite **CorpNet** no campo Nome.



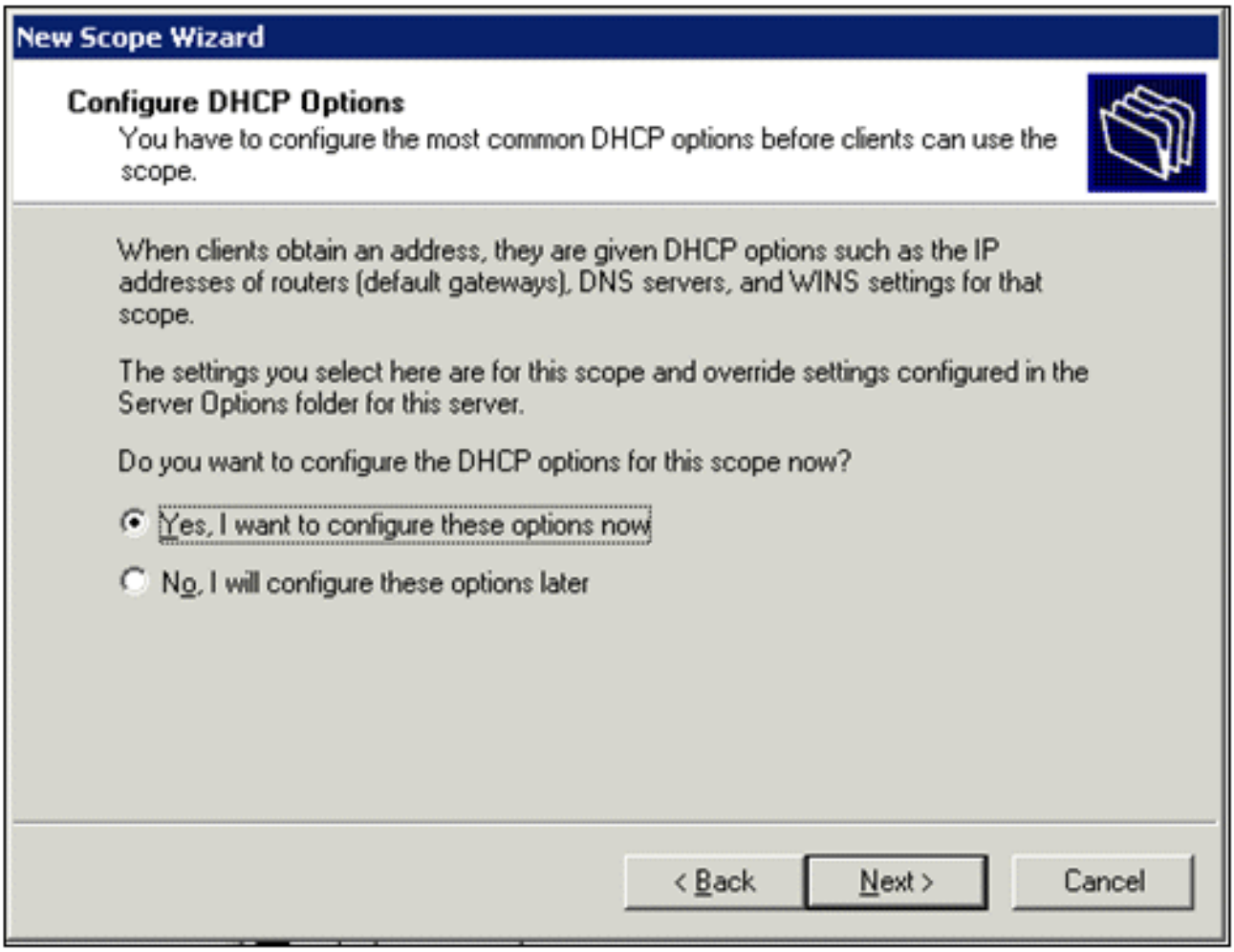
7. Clique em **Avançar** e preencha estes parâmetros:Endereço IP inicial - **10.0.20.1**Endereço IP final - **10.0.20.200**Comprimento - **24**Máscara de sub-rede - **255.255.255.0**



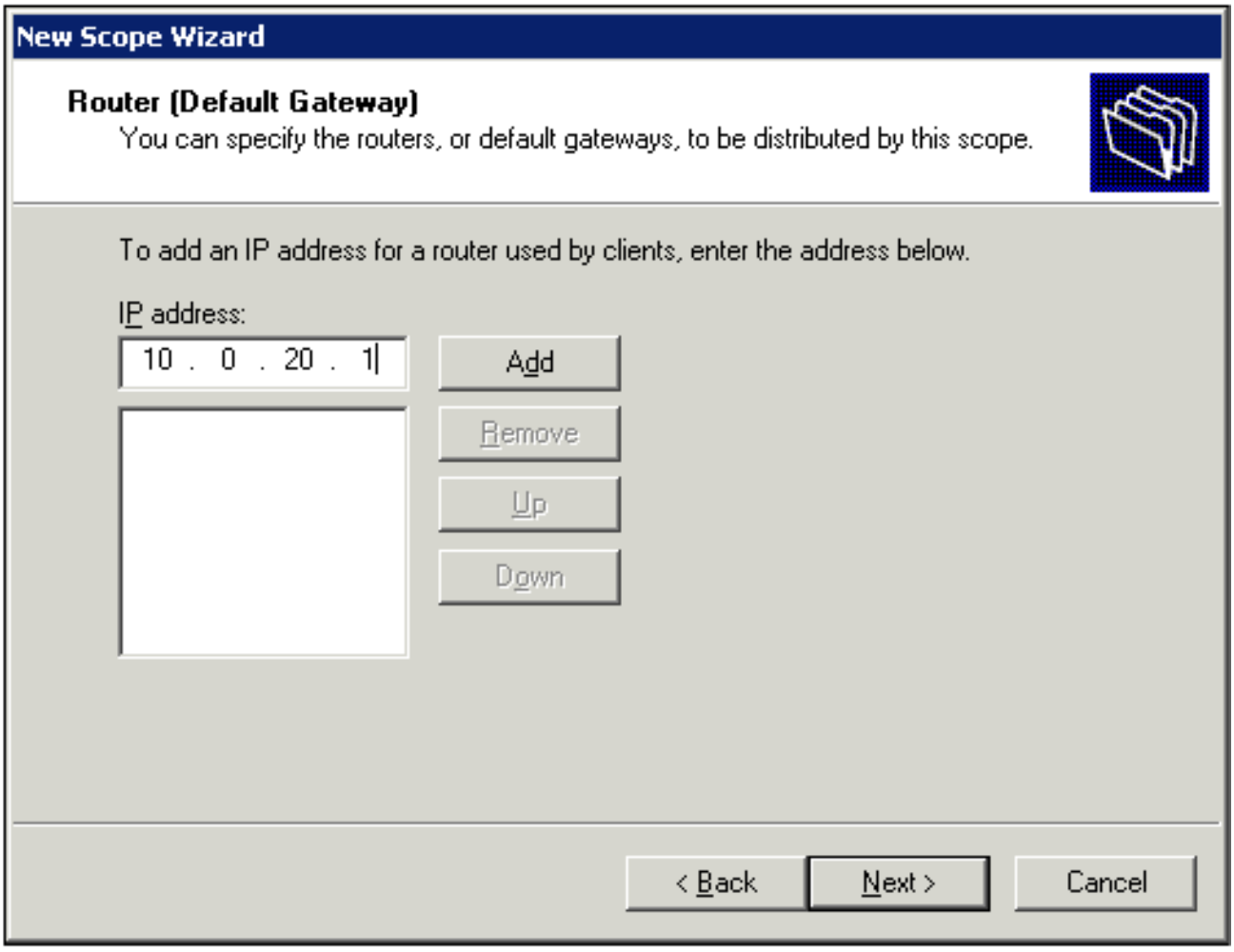
8. Clique em **Next** e insira *10.0.20.1* para o endereço IP inicial e *10.0.20.100* para o endereço IP final a ser excluído. Em seguida, clique em Avançar. Isso reserva os endereços IP no intervalo de 10.0.20.1 a 10.0.20.100. Esses endereços IP de reserva não são alocados pelo servidor
DHCP.



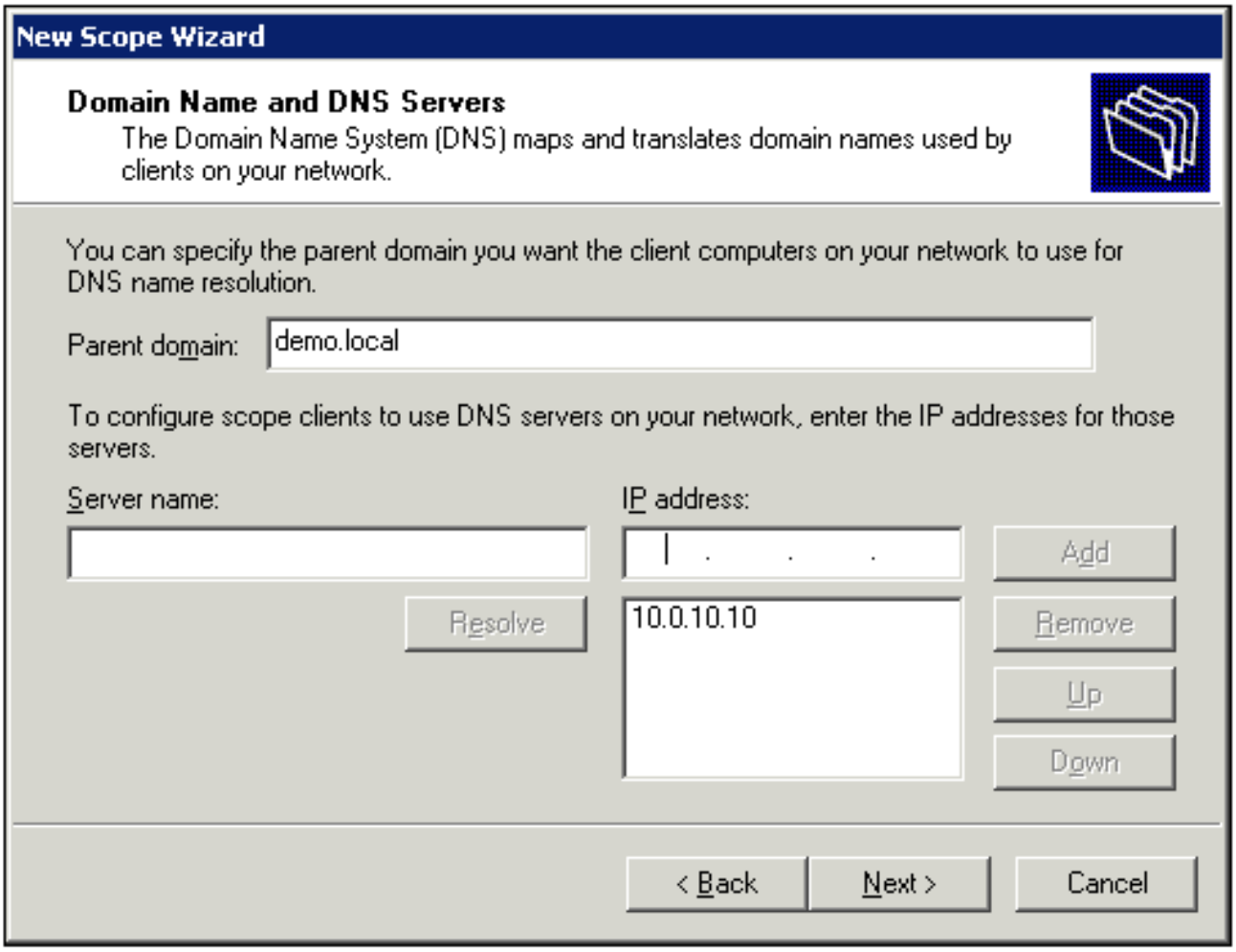
9. Na página Lease Duration, clique em **Next**.
10. Na página Configure DHCP Options (Configurar opções de DHCP), escolha **Yes, I want to configure these options now** e clique em **Next**.



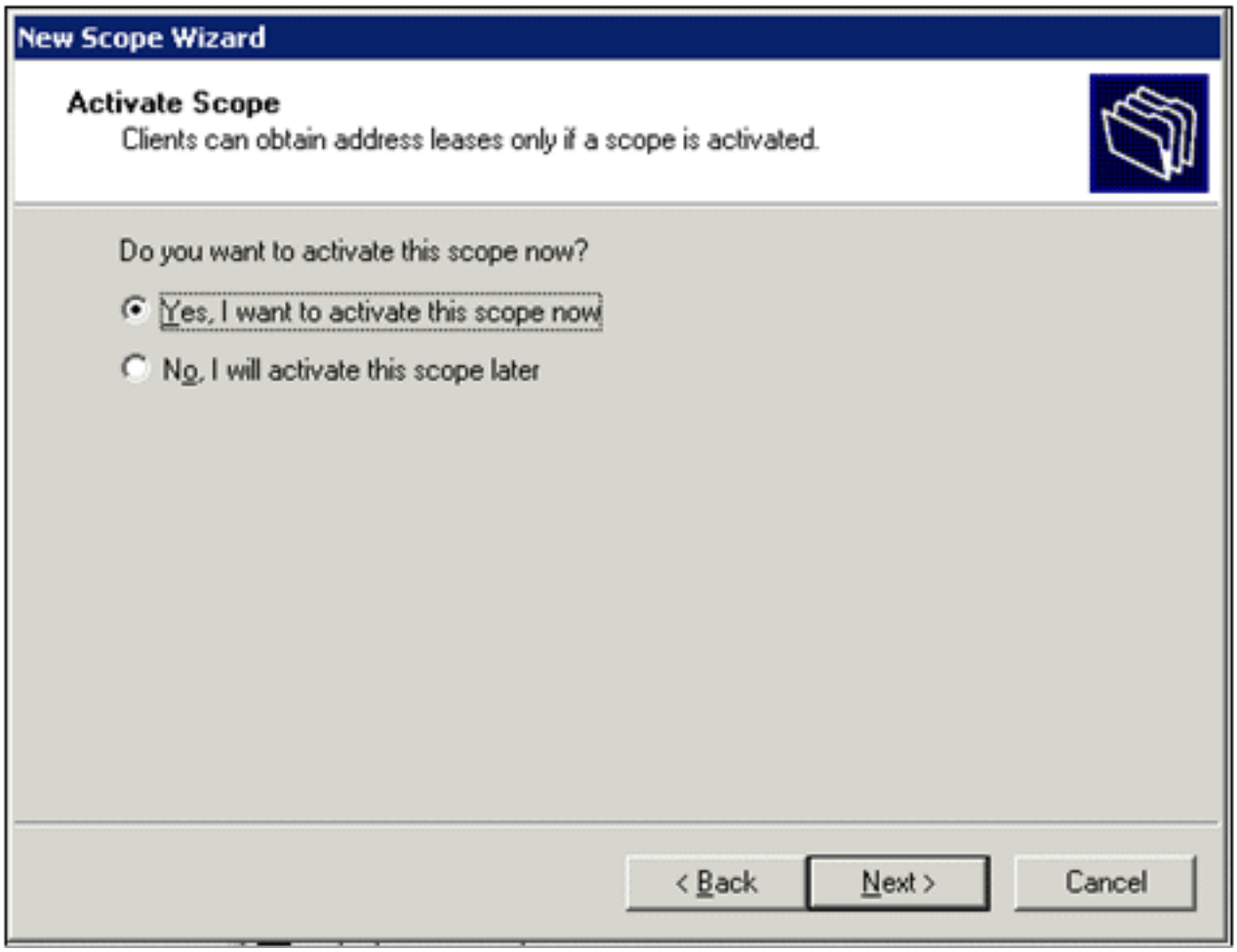
11. Na página Router (Default Gateway), adicione o endereço de roteador padrão *10.0.20.1* e clique em
Next.



12. Na página Nome do domínio e servidores DNS, digite *demo.local* no campo Domínio pai, digite *10.0.10.10* no campo Endereço IP, clique em *Adicionar* e clique em *Avançar*.



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. Quando terminar com a página Assistente de Novo Escopo, clique em **Finalizar**.

Instalar Serviços de Certificado

Execute estas etapas:

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

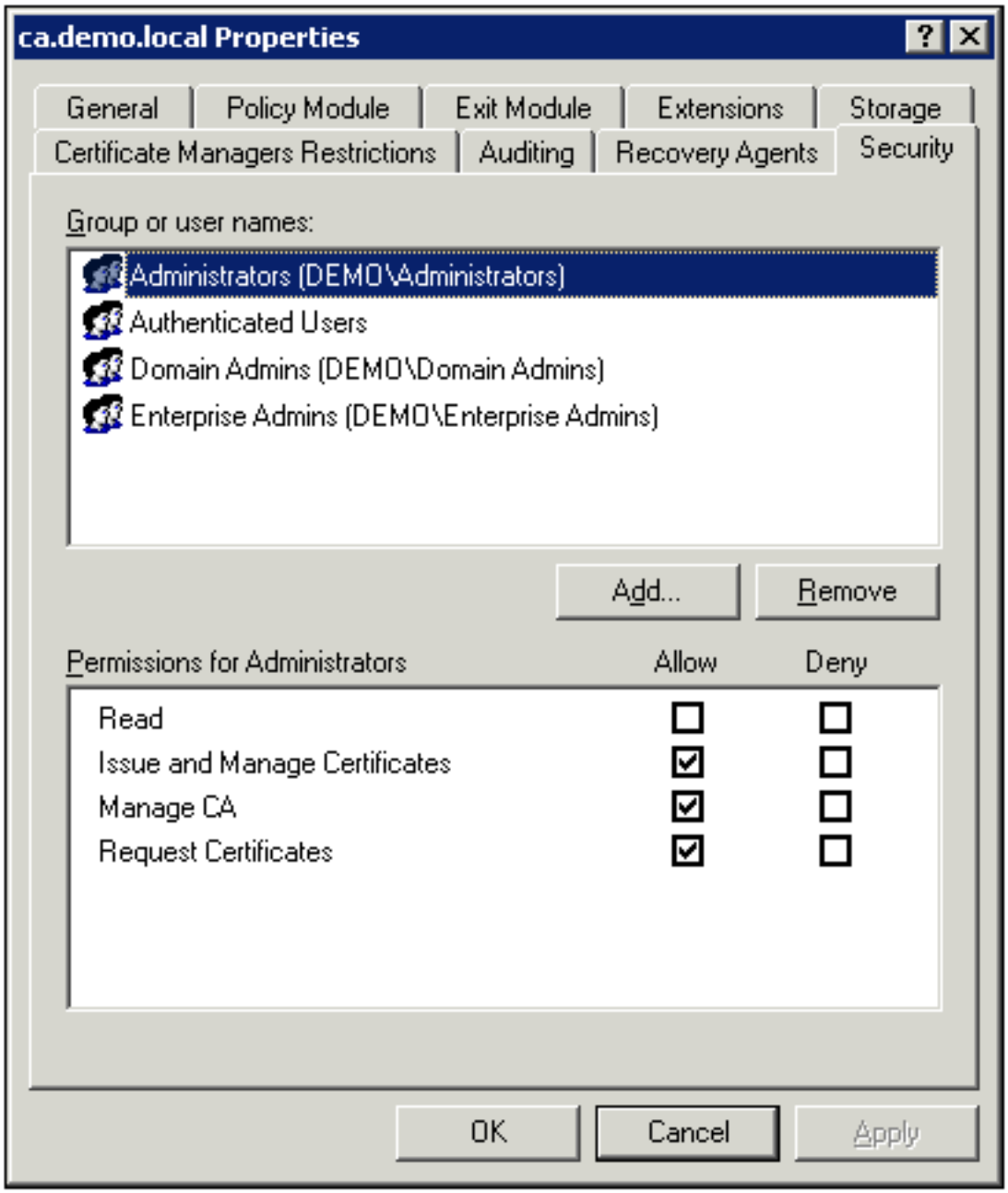
1. No Painel de Controle, abra **Adicionar ou Remover Programas** e clique em **Adicionar/Remover Componentes do Windows**.
2. Na página do Assistente de Componentes do Windows, escolha Serviços de Certificados e clique em Avançar.
3. Na página Tipo de CA, escolha CA raiz Corporativa e clique em Avançar.
4. Na página Informações de identificação da CA, digite *democa* na caixa Nome comum para esta CA. Você também pode inserir os outros detalhes opcionais. Em seguida, clique em **Avançar** e aceite os padrões na página Configurações do banco de dados de certificados.
5. Clique em Next. Ao concluir a instalação, clique em **Concluir**.
6. Clique em **OK** depois de ler a mensagem de aviso sobre a instalação do IIS.

Verificar permissões de administrador para certificados

Execute estas etapas:

1. Escolha **Start** > **Administrative Tools** > **Certification Authority**.

2. Clique com o botão direito do mouse em **democa CA** e, em seguida, clique em **Propriedades**.
3. Na guia Segurança, clique em **Administradores** na lista Nomes de grupo ou de usuário.
4. Na lista Permissões para administradores, verifique se estas opções estão definidas como **Permitir**:Emitir e gerenciar certificadosGerenciar CASolicitar certificadosSe qualquer uma dessas opções estiver definida como Negar ou não estiver selecionada, defina as permissões como



Permitir.

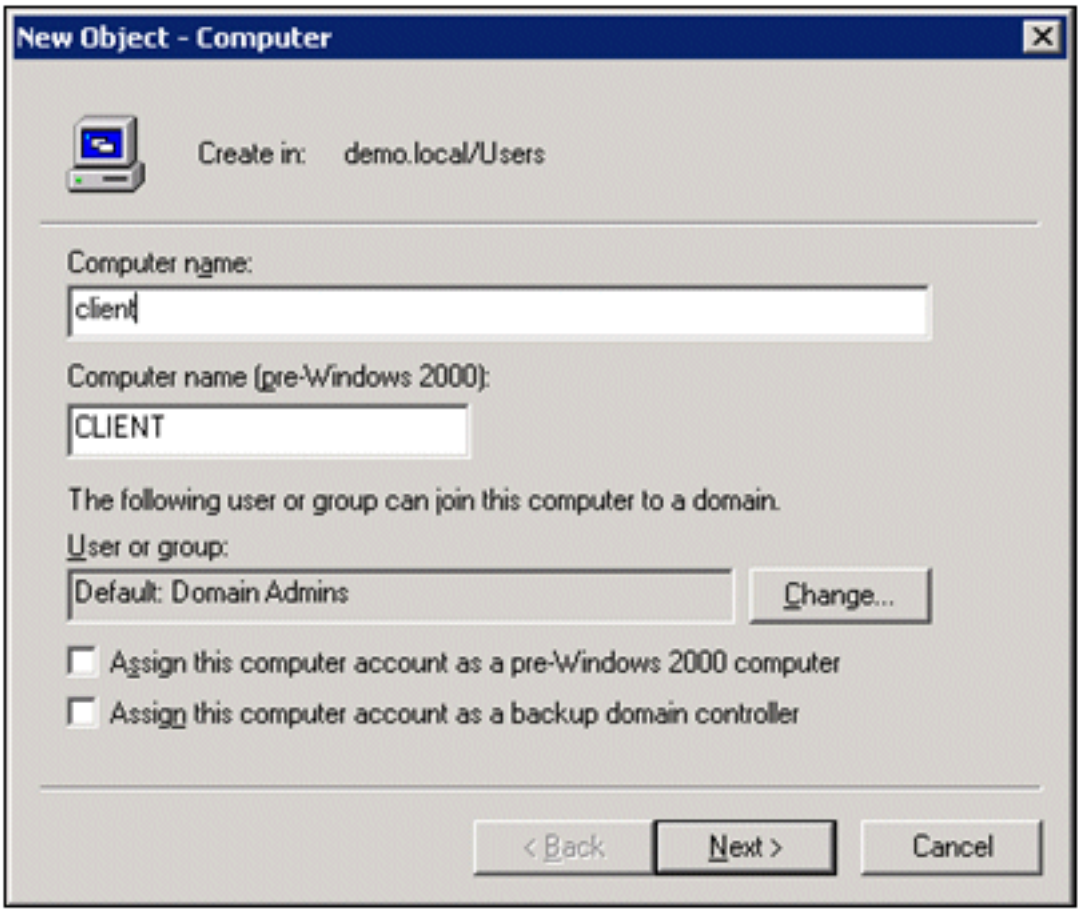
5. Clique em **OK** para fechar a caixa de diálogo Propriedades da CA democrática e feche a Autoridade de Certificação.

Adicionar computadores ao domínio

Execute estas etapas:

Observação: se o computador já tiver sido adicionado ao domínio, prossiga para Adicionar usuários ao domínio.

1. Abra o snap-in **Usuários e Computadores do Ative Diretory**.
2. Na árvore do console, expanda **demo.local**.
3. Clique com o botão direito do mouse em **Computers**, clique em **New** e em **Computer**.
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 *Client*.

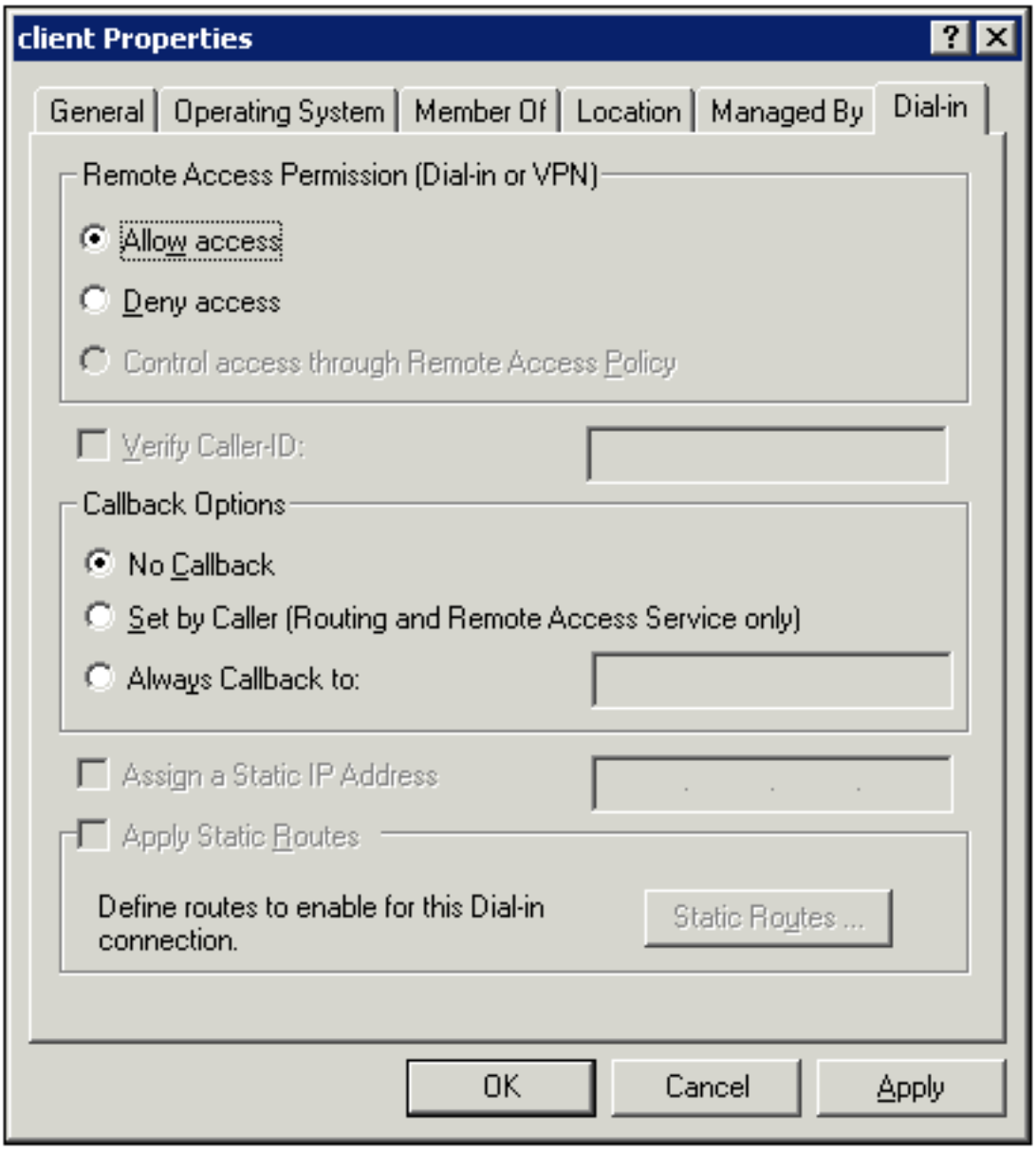


5. Na caixa de diálogo Gerenciado, clique em **Avançar**.
6. Na caixa de diálogo Novo objeto - Computador, clique em **Concluir**.
7. Repita as etapas 3 a 6 para criar contas de computador adicionais.

Permitir acesso sem fio a computadores

Execute estas etapas:

1. Na árvore do console Ative Diretory Users and Computers (Usuários e computadores do Ative Diretory), clique na pasta **Computers (Computadores)** e clique com o botão direito do mouse no computador ao qual deseja atribuir acesso sem fio. Este exemplo mostra o procedimento com o computador **Cliente** que você adicionou na etapa 7. Clique em **Properties** e vá para a guia **Dial-in**.
2. Na Permissão de acesso remoto, escolha **Permitir acesso** e clique em

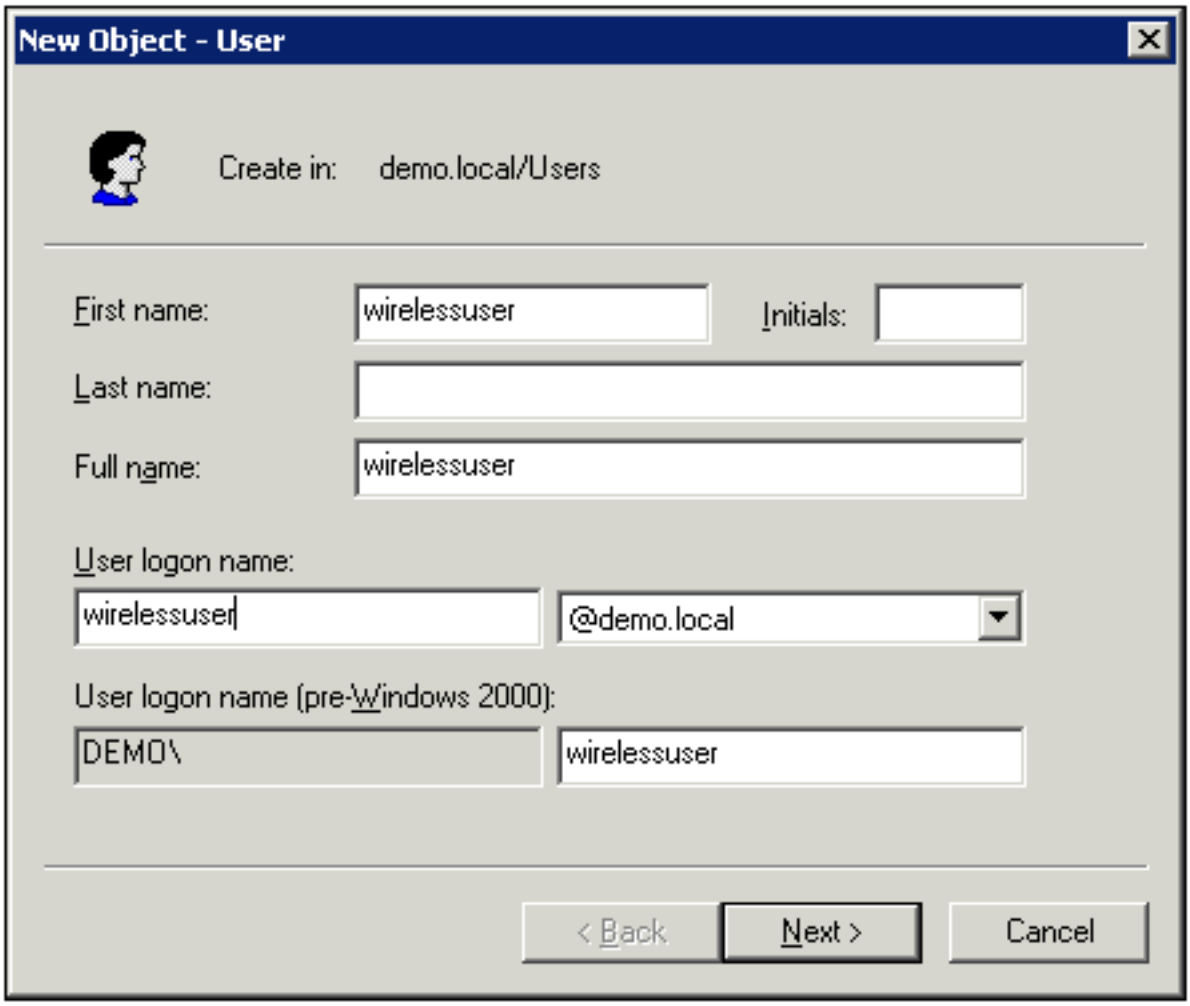


OK.

[Adicionar usuários ao domínio]

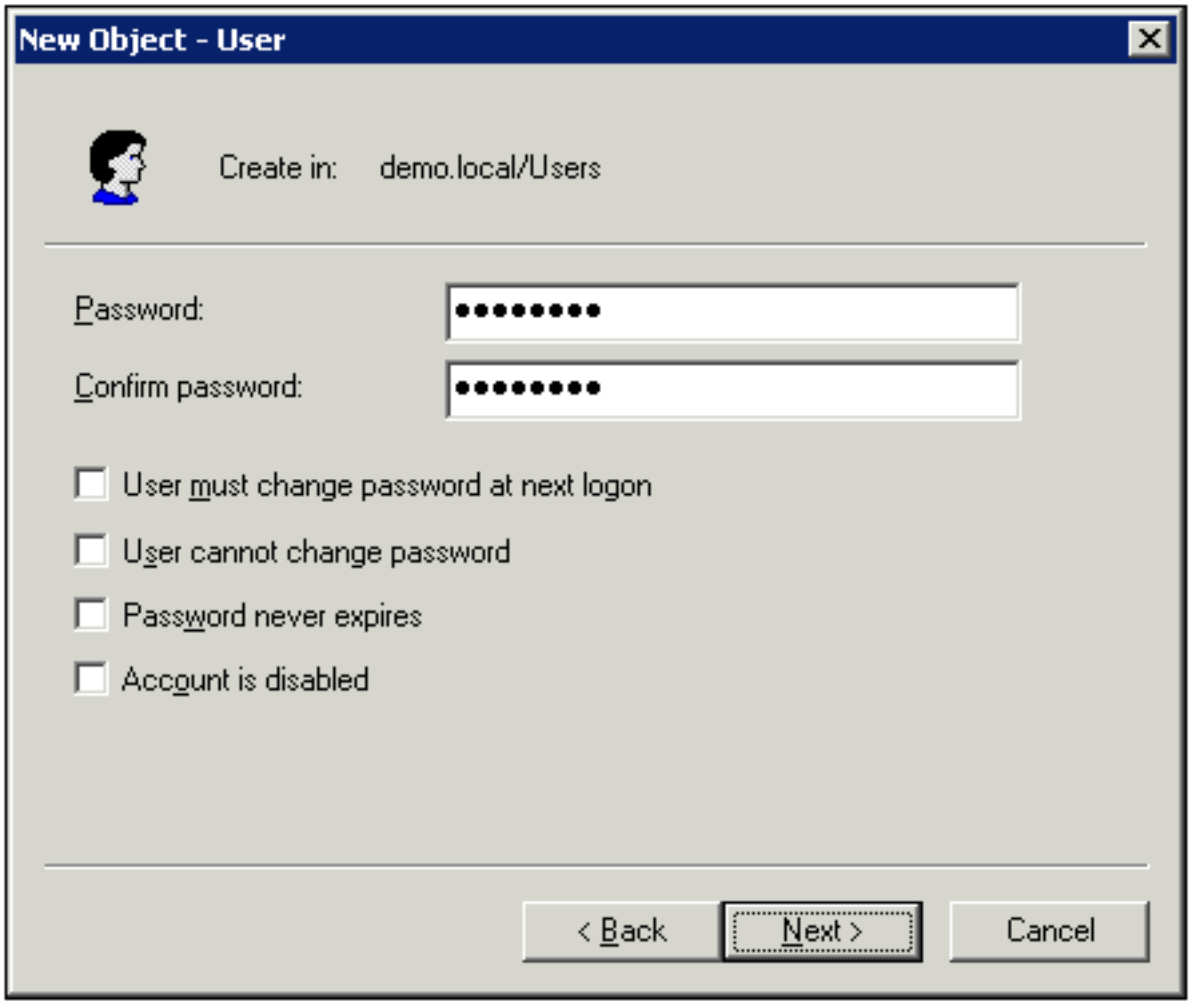
Execute estas etapas:

1. Na árvore do console Ative Diretory Users and Computers, clique com o botão direito do mouse em **Users**, clique em **New** e clique em **User**.
2. Na caixa de diálogo New Object - User (Novo objeto - Usuário), digite o nome do usuário sem fio. Este exemplo usa o nome *wirelesuser* no campo Nome e *wirelesser* no campo Nome de logon do usuário. Clique em



Next.

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 **O usuário deve alterar a senha no próximo logon** e clique em **Avançar**.



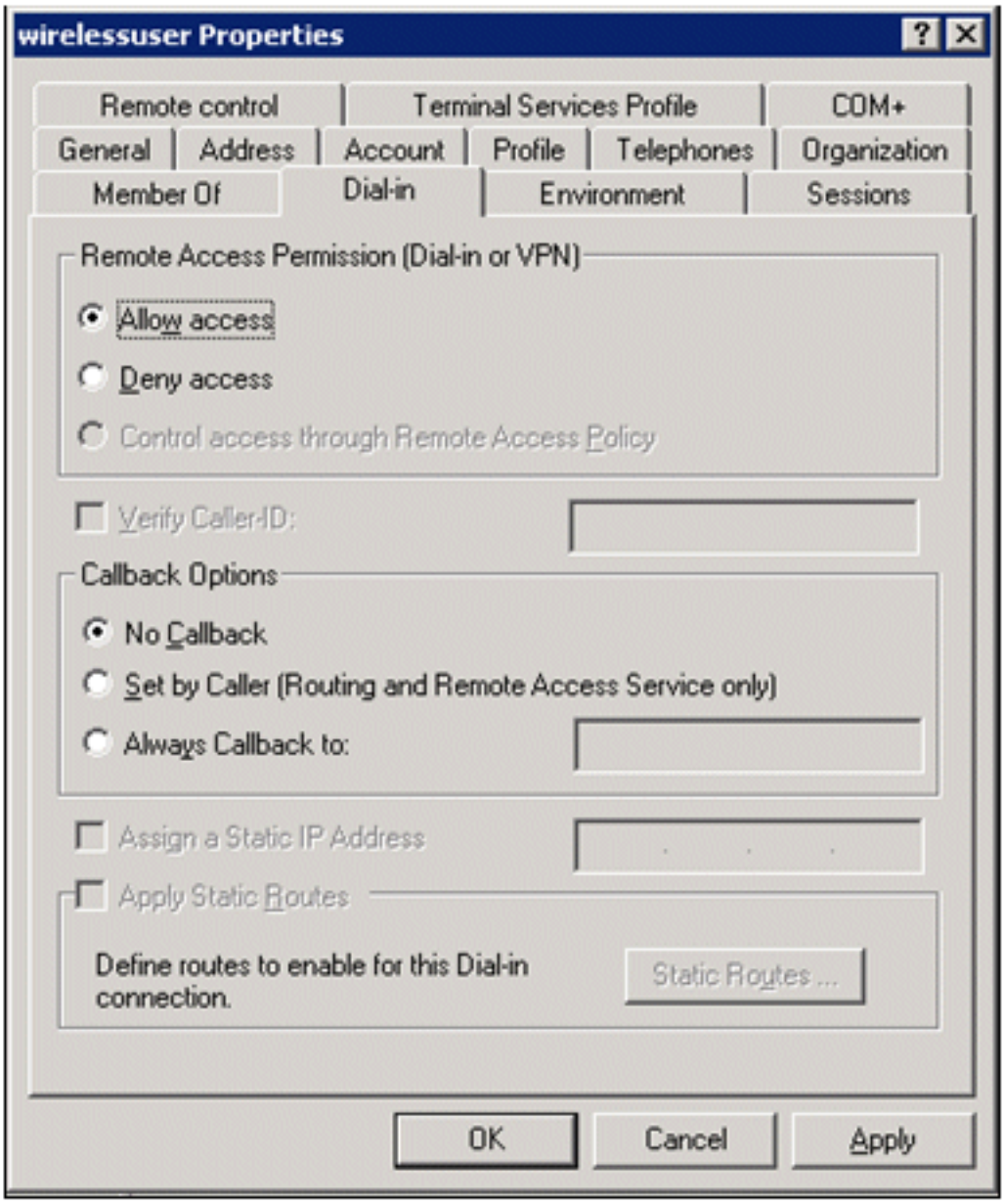
4. Na caixa de diálogo Novo objeto - usuário, clique em **Concluir**.
5. Repita as etapas de 2 a 4 para criar contas de usuário adicionais.

Permitir acesso sem fio aos usuários

Execute estas etapas:

1. Na árvore do console Ative Diretory Users and Computers, clique na pasta **Users**, clique com o botão direito do mouse em **wireluserser**, clique em **Properties** e vá para a guia **Dial-in**.
2. Na Permissão de acesso remoto, escolha **Permitir acesso** e clique em

OK.

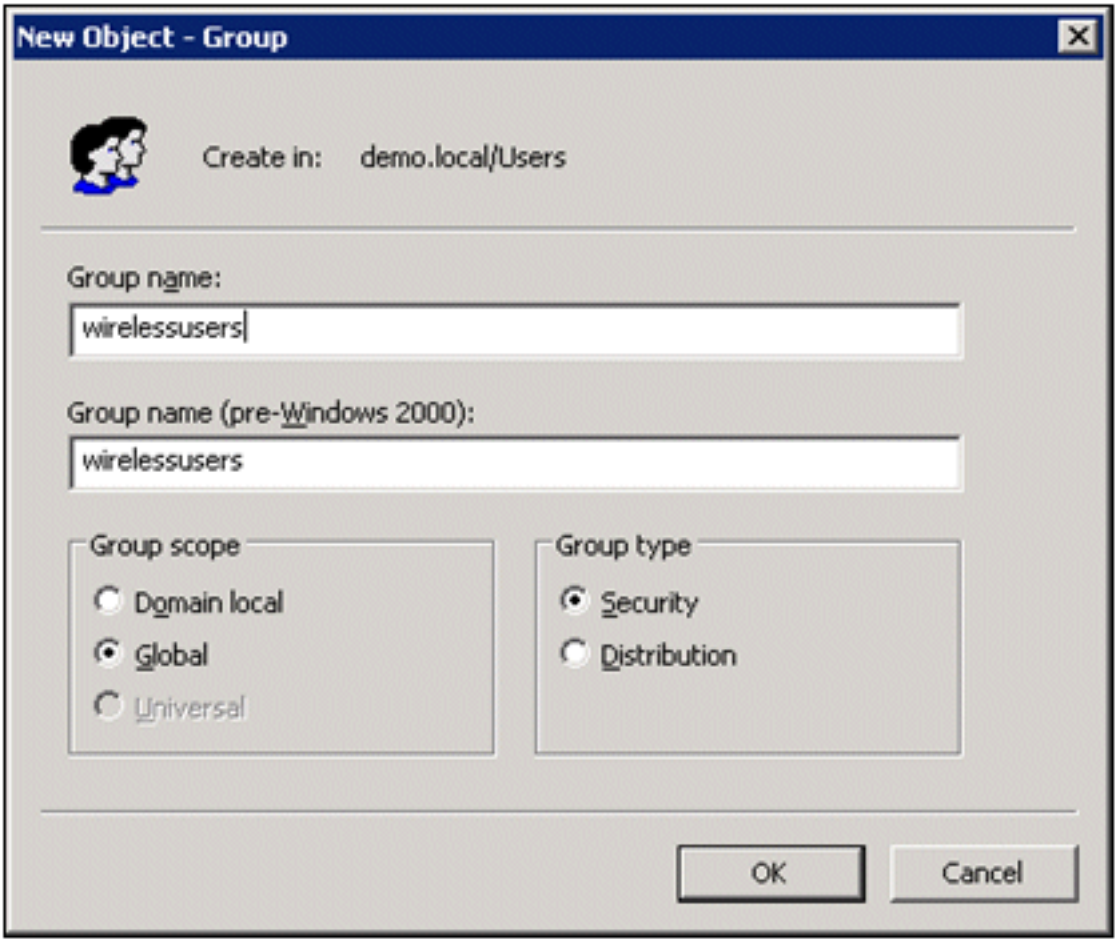


[Adicionar grupos ao domínio]

Execute estas etapas:

1. Na árvore do console Ative Diretory Users and Computers, clique com o botão direito do mouse em **Users**, clique em **New** e clique em **Group**.
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

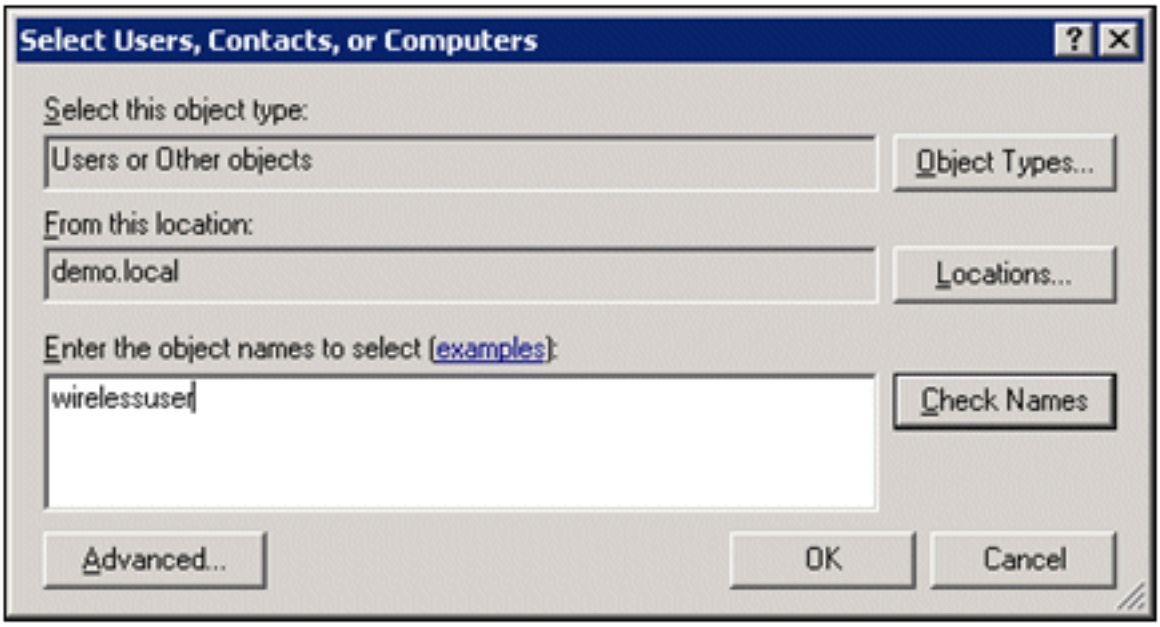
wirelesusers.



Adicionar usuários ao grupo usuários sem fio

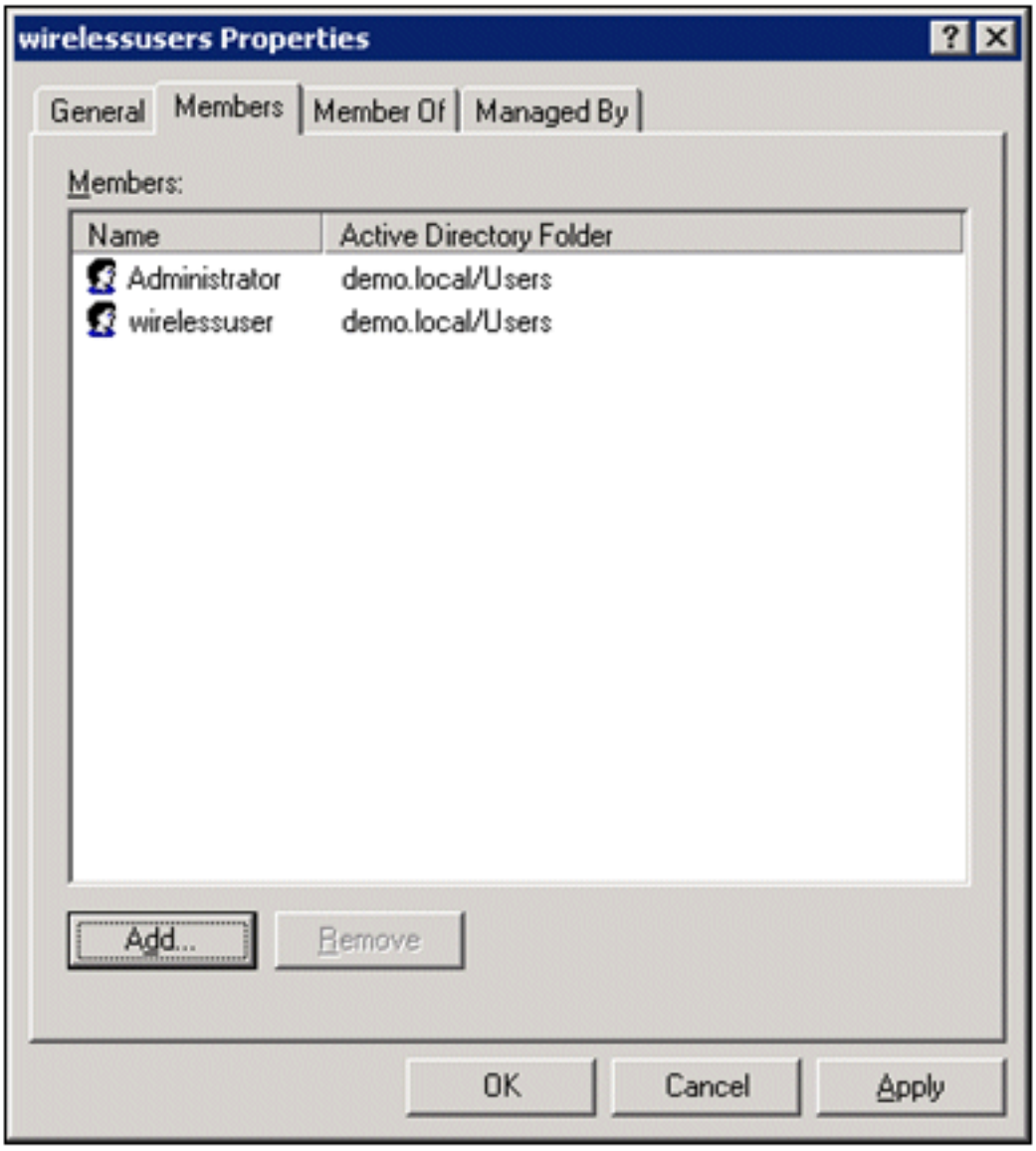
Execute estas etapas:

1. No painel de detalhes de Usuários e computadores do Ative Diretory, clique duas vezes no 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 sem fio é adicionada ao grupo de usuários sem



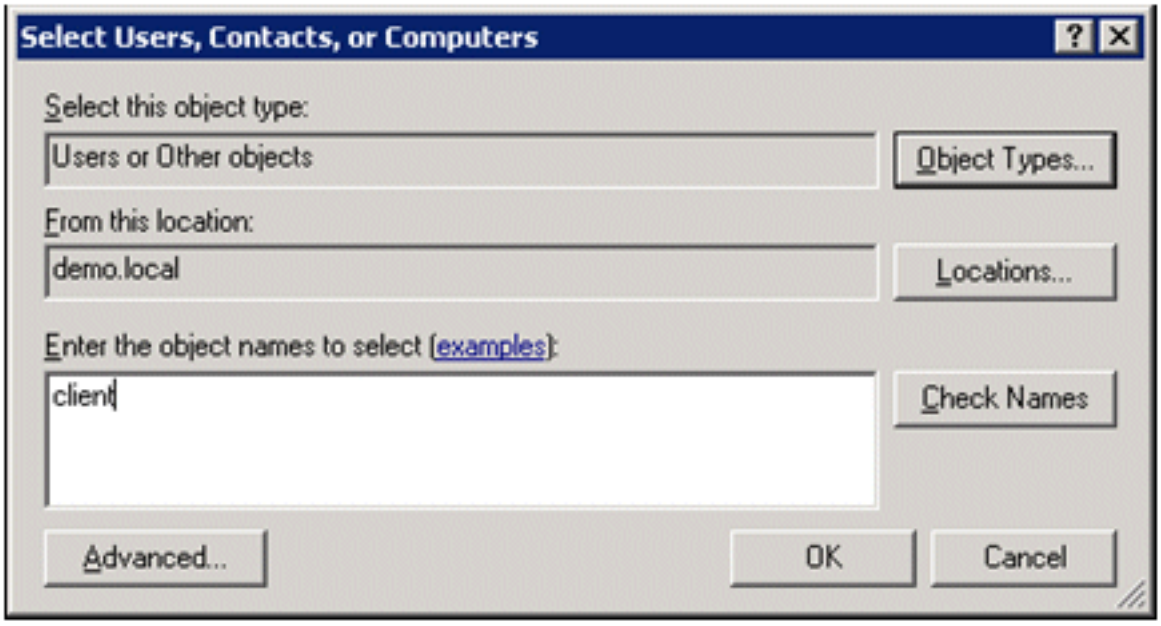
fio.

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

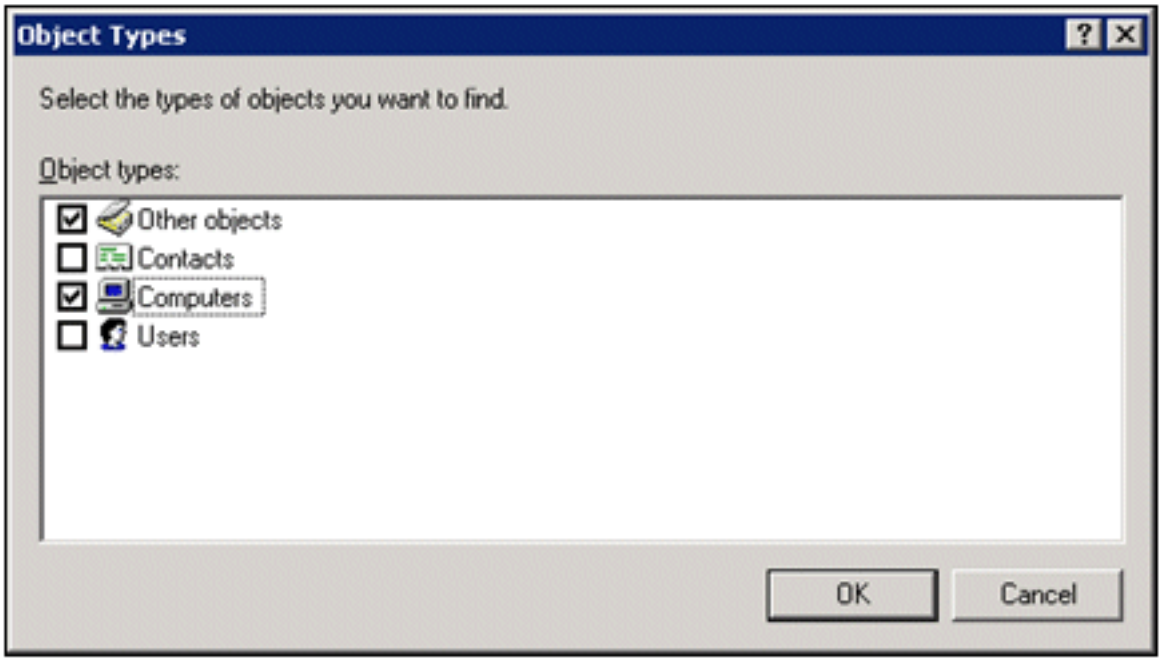
Adicionar computadores cliente ao grupo usuários sem fio

Execute estas etapas:

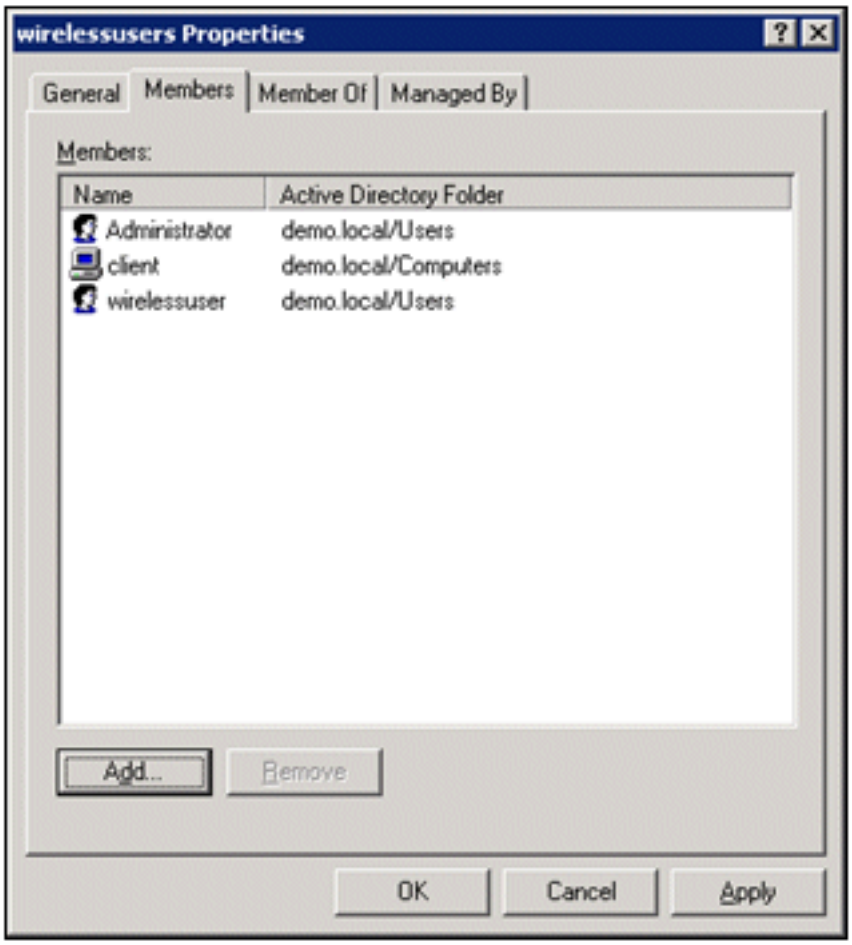
1. Repita as etapas 1 e 2 na seção Adicionar usuários ao grupo de usuários sem fio deste documento.
2. Na caixa de diálogo Selecionar usuários, contatos ou computadores, digite o nome do computador que deseja adicionar ao grupo. Este exemplo mostra como adicionar o computador chamado *cliente* ao grupo.



3. Clique em **Object Types**, desmarque a caixa de seleção **Users** e, em seguida, marque **Computers**.



4. Clique duas vezes em **OK**. A conta do computador CLIENTE é adicionada ao grupo de



usuários sem fio.

5. Repita o procedimento para adicionar mais computadores ao grupo.

Cisco 1121 Secure ACS 5.1

Instalação usando o dispositivo CSACS-1121 Series

O dispositivo CSACS-1121 é pré-instalado com o software ACS 5.1. Esta seção fornece uma visão geral do processo de instalação e das tarefas que você deve executar antes de instalar o ACS.

1. Conecte o CSACS-1121 ao console da rede e do equipamento. Consulte o Capítulo 4, "Conexão de cabos".
2. Ligue o dispositivo CSACS-1121. Consulte o Capítulo 4, "Ligando o dispositivo CSACS-1121 Series".
3. Execute o comando **setup** no prompt da CLI para definir as configurações iniciais do servidor ACS. Consulte Executando o programa de configuração.

Instalar o servidor ACS

Esta seção descreve o processo de instalação para o servidor ACS no dispositivo CSACS-1121 Series.

- Execute o programa de configuração
- Verificar o processo de instalação
- Tarefas de pós-instalação

Para obter informações detalhadas sobre a instalação do Cisco Secure ACS Server, consulte o Guia de Instalação e Atualização do Cisco Secure Access Control System 5.1.

Configuração do controlador Cisco WLC5508

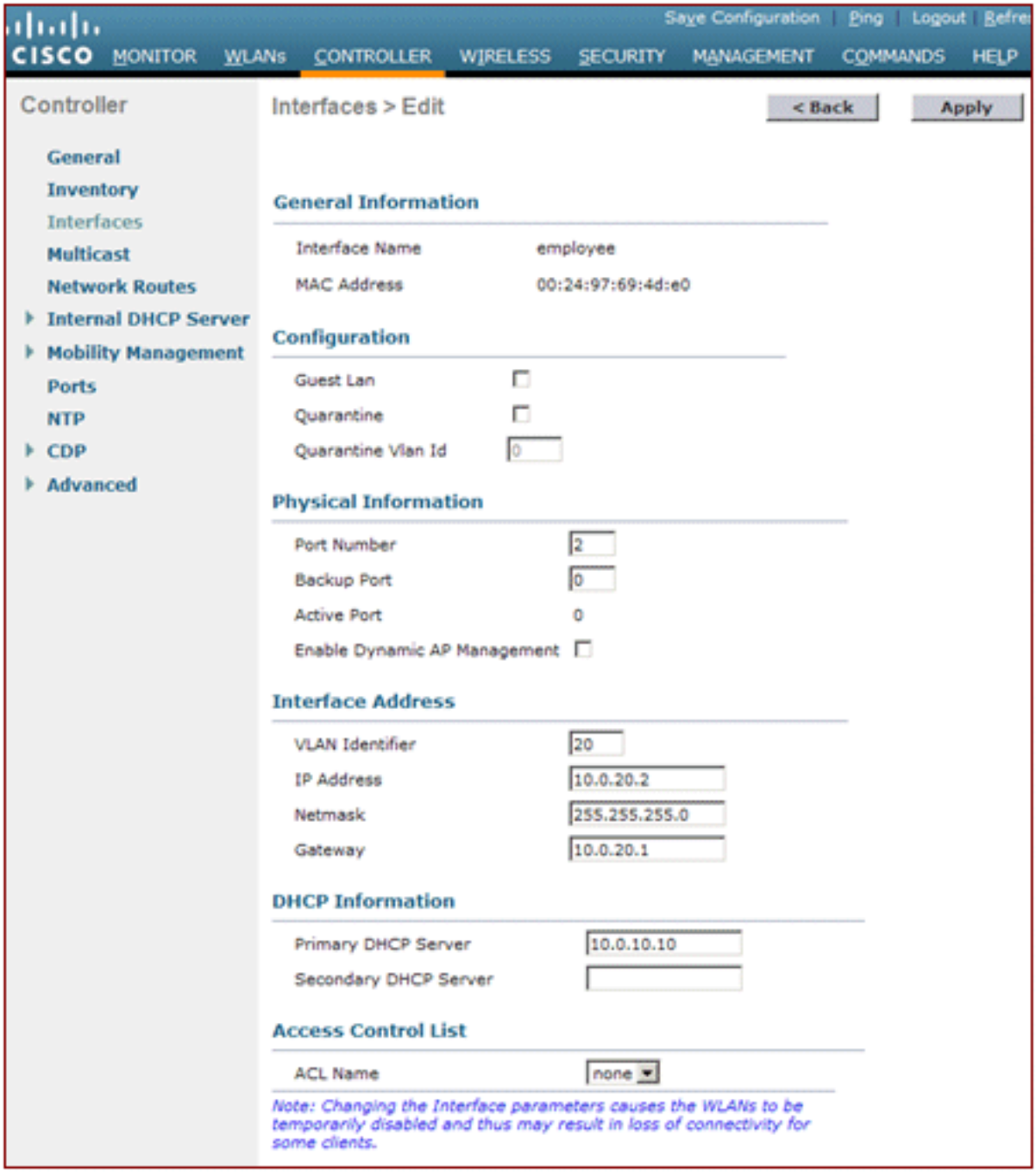
Crie a configuração necessária para WPAv2/WPA

Execute estas etapas:

Observação: presume-se que o controlador tenha conectividade básica com a rede e alcance IP à interface de gerenciamento seja bem-sucedido.

1. Navegue até **https://10.0.1.10** para fazer login no controlador.

2. Clique em login.
3. Faça login com o usuário padrão *admin* e a senha padrão *admin*.
4. Crie uma nova Interface para mapeamento VLAN no menu **Controller**.
5. Clique em **Interfaces**.
6. Clique em **New**.
7. No campo Nome da interface, informe *Funcionário*. (Esse campo pode ter 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 na janela Interfaces > Edit:Endereço IP da interface - **10.0.20.2**Máscara de rede - **255.255.255.0**Gateway - **10.0.10.1**DHCP primário - **10.0.10.10**

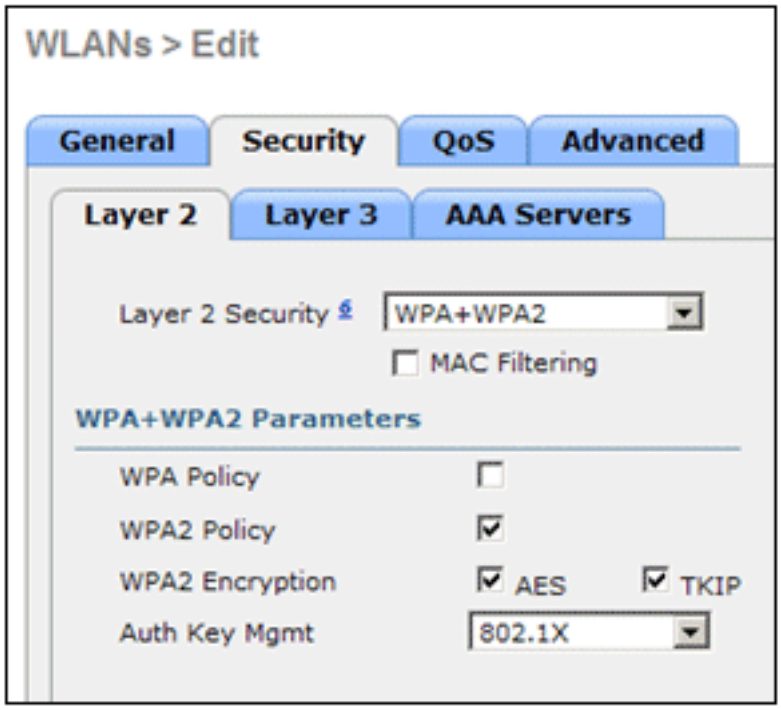


11. Clique em Apply.
12. Clique na guia **WLANs**.
13. Escolha **Criar Novo** e clique em **Ir**.
14. Insira um Nome de perfil e, no campo SSID da WLAN, insira *Employee*.

15. Escolha um ID para a WLAN e clique em **Apply**.

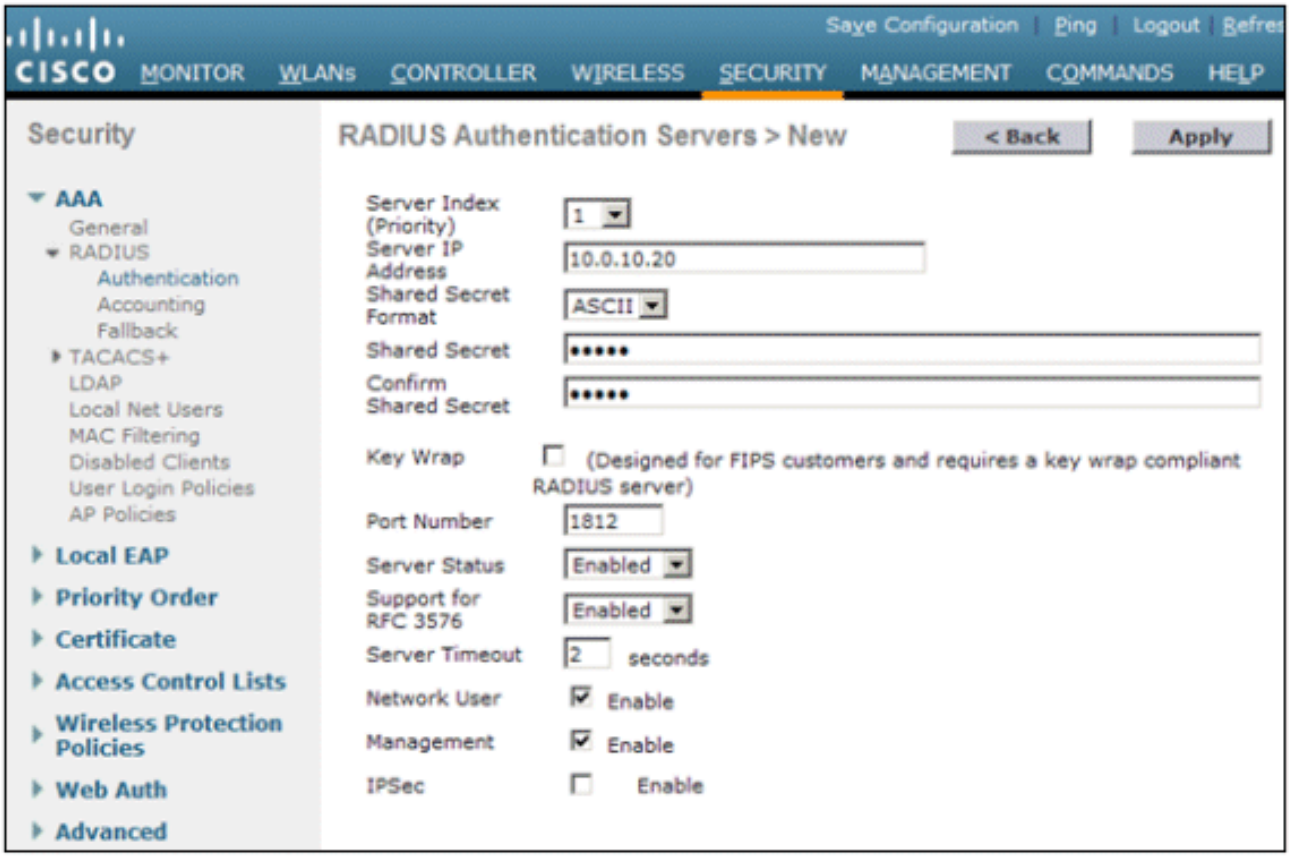
16. Configure as informações para esta WLAN quando a janela WLANs > Edit for exibida.**Observação: o** WPAv2 é o método de criptografia da camada 2 escolhido para este laboratório. Para permitir que WPA com clientes TKIP-MIC se associem a este SSID, você também pode marcar as caixas **Modo de compatibilidade WPA** e **Permitir clientes TKIP WPA2** ou os clientes que não suportam o método de criptografia AES 802.11i.
17. Na tela WLANs > Edit, clique na guia **General**.
18. Certifique-se de que a caixa Status esteja marcada para **Enabled** e que a **Interface** apropriada (funcionário) esteja selecionada. Além disso, certifique-se de marcar a caixa de seleção **Enabled** para Broadcast
    SSID.

19. Clique na guia Security.
20. No submenu Layer 2, marque **WPA + WPA2** para Layer 2 Security. Para a criptografia WPA2, marque **AES + TKIP** para permitir clientes TKIP.
21. Escolha **802.1x** como o método de



autenticação.

22. Ignore o submenu Layer 3, pois ele não é obrigatório. Depois que o servidor RADIUS estiver configurado, o servidor apropriado poderá ser escolhido no menu Authentication (Autenticação).
23. As guias **QoS** e **Advanced** podem ser deixadas como padrão, a menos que sejam necessárias configurações especiais.
24. Clique no menu **Security** para adicionar o servidor RADIUS.
25. No submenu RADIUS, clique em **Authentication**. Em seguida, clique em **New**.
26. Adicione o endereço IP do servidor RADIUS (10.0.10.20) que é o servidor ACS configurado anteriormente.
27. Verifique se a chave compartilhada corresponde ao cliente AAA configurado no servidor ACS. Verifique se a caixa **Network User** está marcada e clique em **Apply**.



28. A configuração básica está concluída e você pode começar a testar o PEAP.

Autenticação PEAP

O PEAP com MS-CHAP versão 2 requer certificados nos servidores ACS, mas não nos clientes sem fio. O registro automático de certificados de computador para os servidores ACS pode ser usado para simplificar uma implantação.

Para configurar o servidor de autoridade de certificação para fornecer registro automático para certificados de computador e usuário, conclua os procedimentos nesta seção.

Observação: a Microsoft alterou o modelo de servidor da Web com a versão da autoridade de certificação empresarial do Windows 2003 para que as chaves não possam mais ser exportadas e a opção fique acinzentada. Não há nenhum outro modelo de certificado fornecido com os serviços de certificado que são para autenticação de servidor e dão a capacidade de marcar chaves como exportáveis que estão disponíveis na lista suspensa, portanto você tem que criar um novo modelo que faça isso.

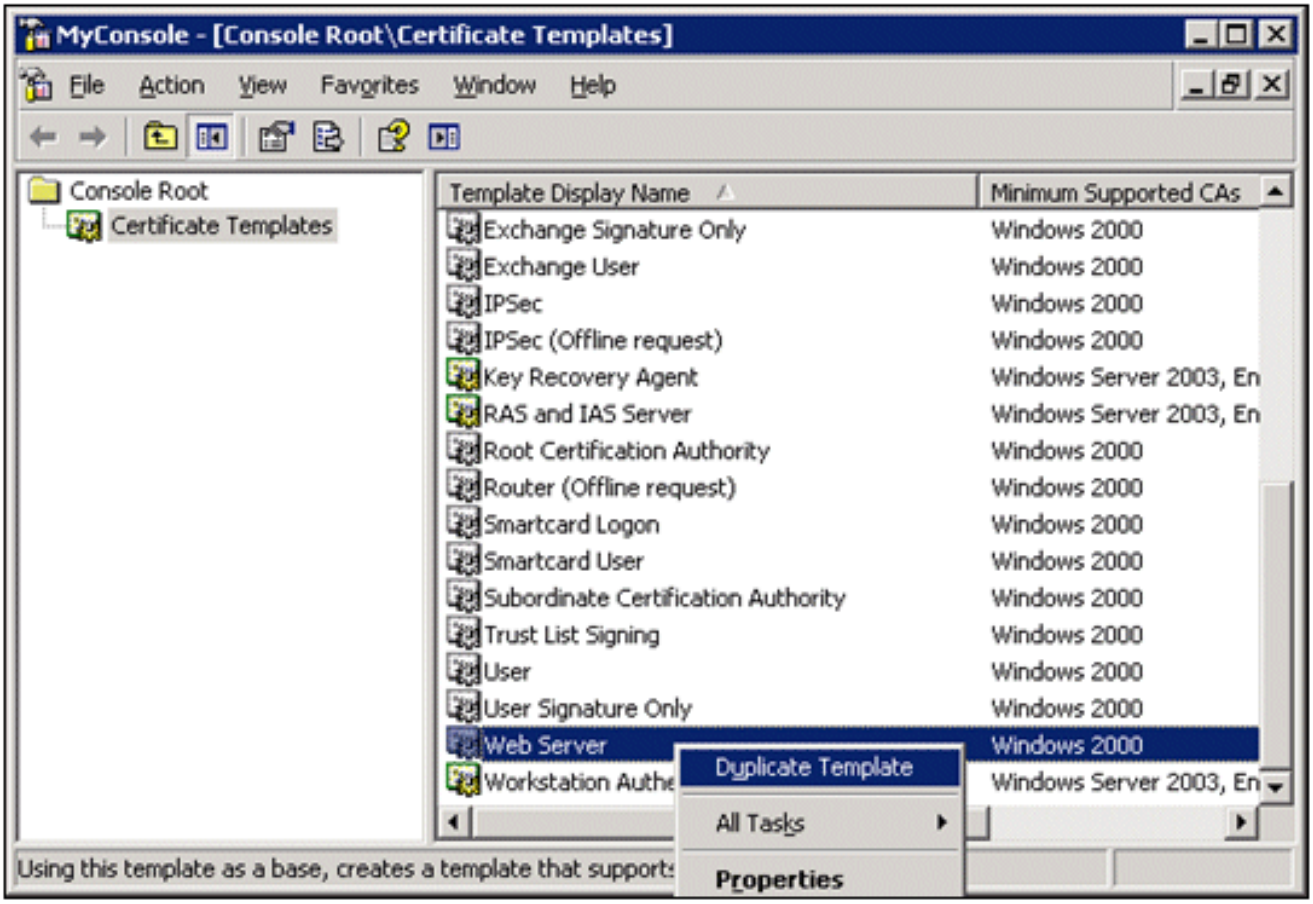
Observação: o Windows 2000 permite chaves exportáveis e esses procedimentos não precisam ser seguidos se você usar o Windows 2000.

Instalar o Snap-in de Modelos de Certificado

Execute estas etapas:

1. Escolha **Start > Run**, digite **mmc** e clique em **OK**.
2. No menu Arquivo, clique em **Adicionar/remover snap-in** e em **Adicionar**.
3. Em Snap-in, clique duas vezes em **Modelos de certificado**, clique em **Fechar** e em **OK**.

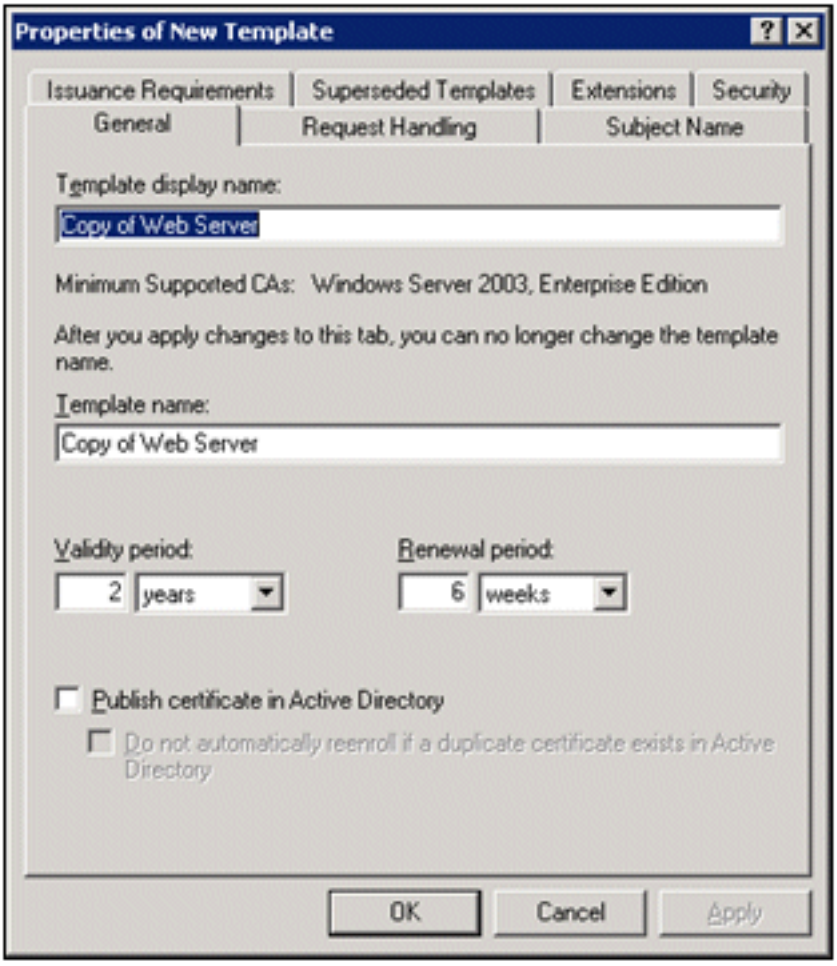
4. Na árvore do console, clique em **Modelos de certificado**. Todos os modelos de certificado são exibidos no painel Detalhes.
5. Para ignorar as etapas 2 a 4, insira *certtmpl.msc*, que abrirá o snap-in de modelos de certificado.



Criar o Modelo de Certificado para o Servidor Web ACS

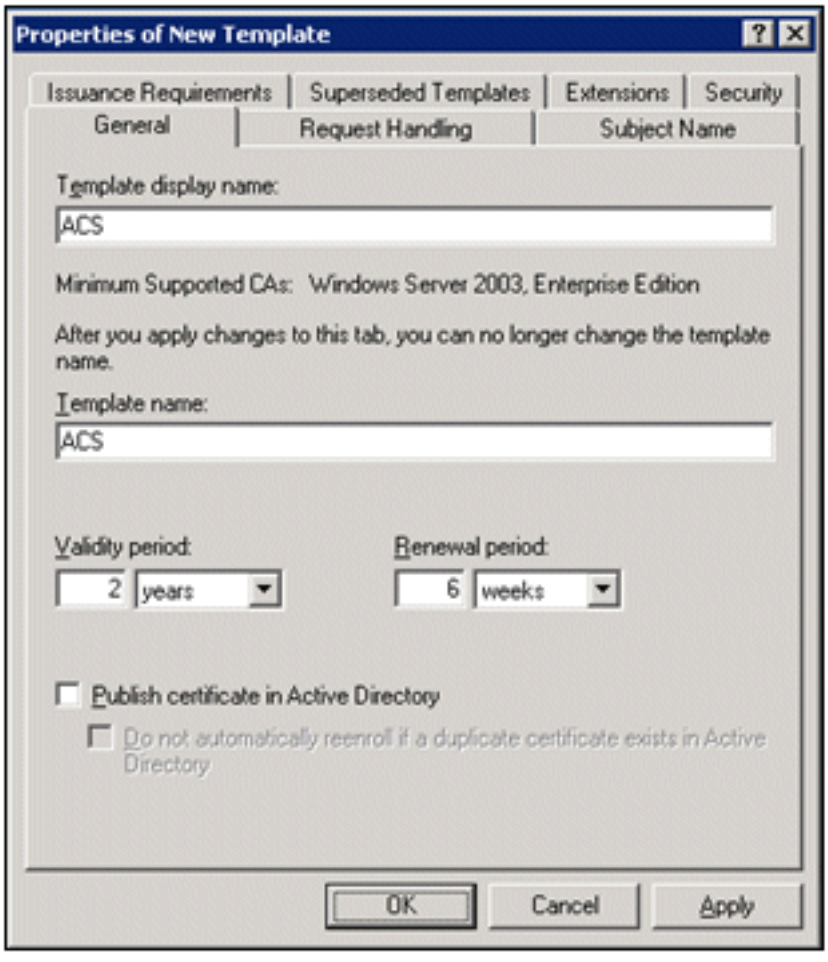
Execute estas etapas:

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



modelo.

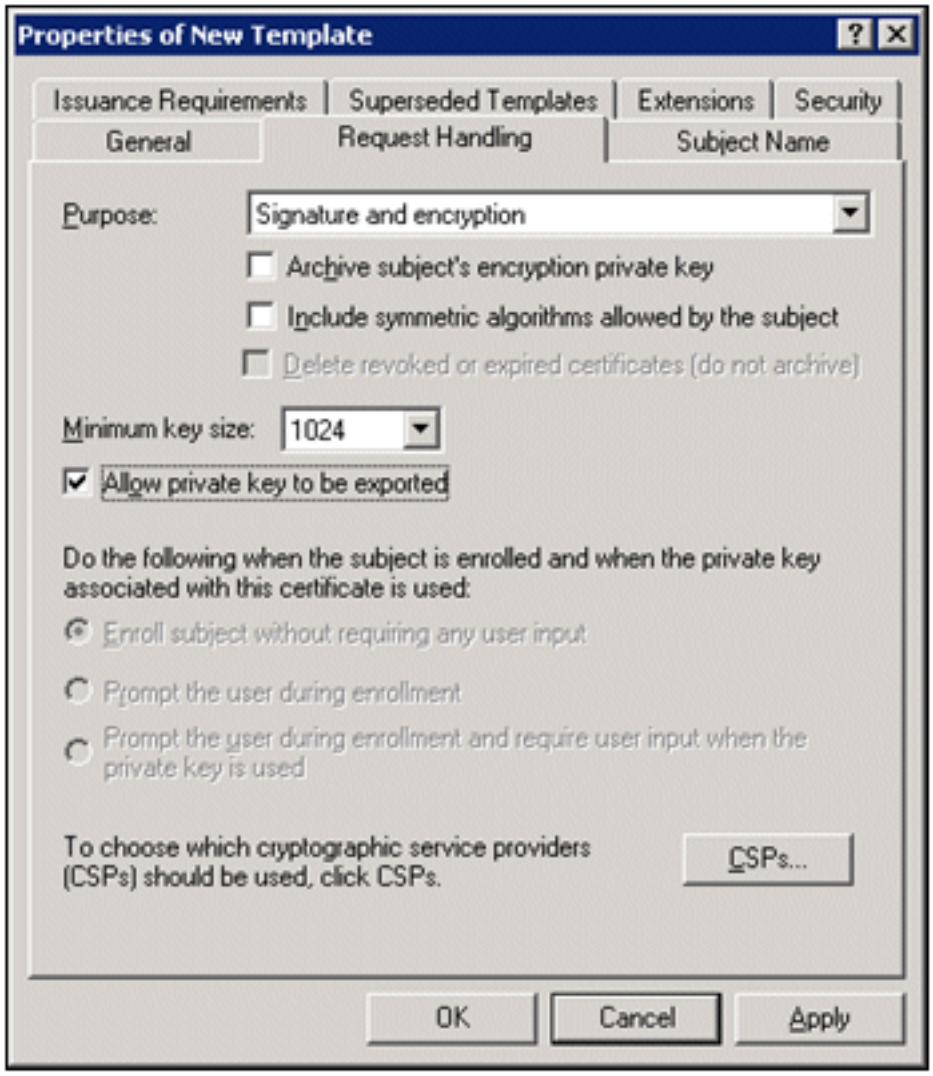
3. No campo Nome de exibição do modelo, insira



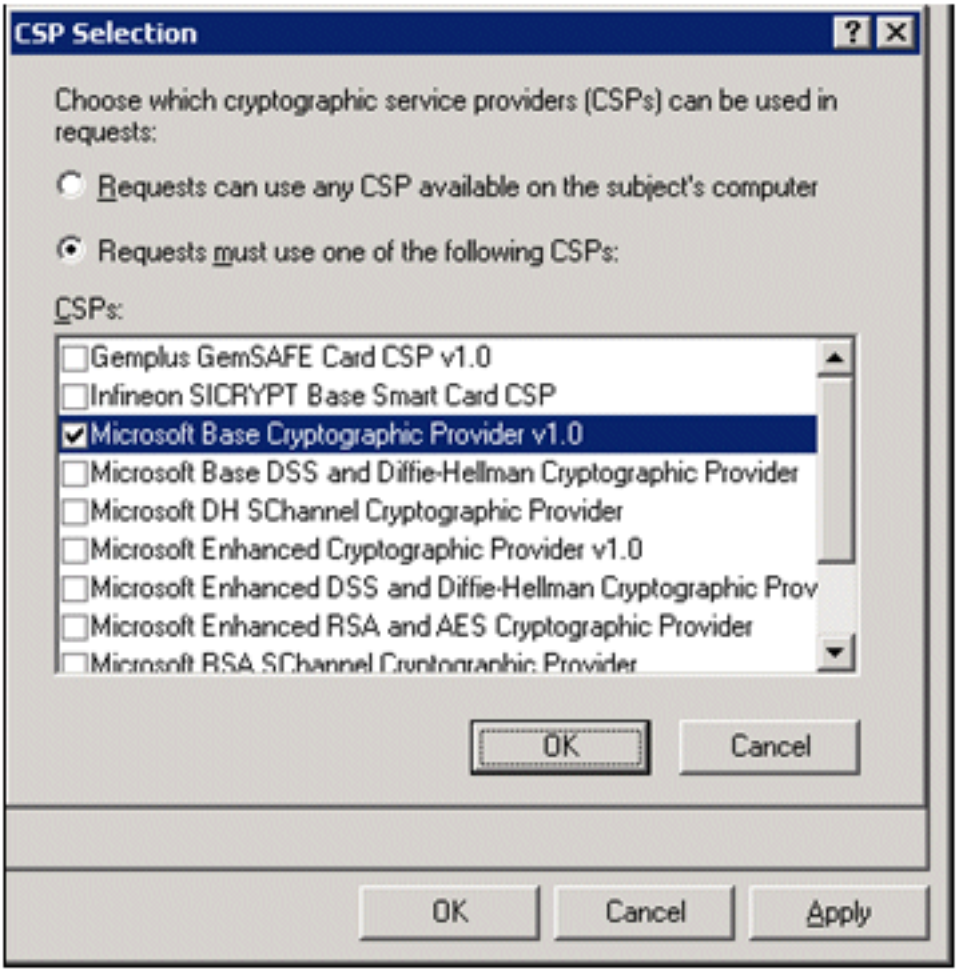
ACS.

4. Vá até a guia **Tratamento de solicitações** e marque **Permitir que a chave privada seja**

exportada. Verifique também se **Signature and Encryption** está selecionado no menu suspenso Purpose.

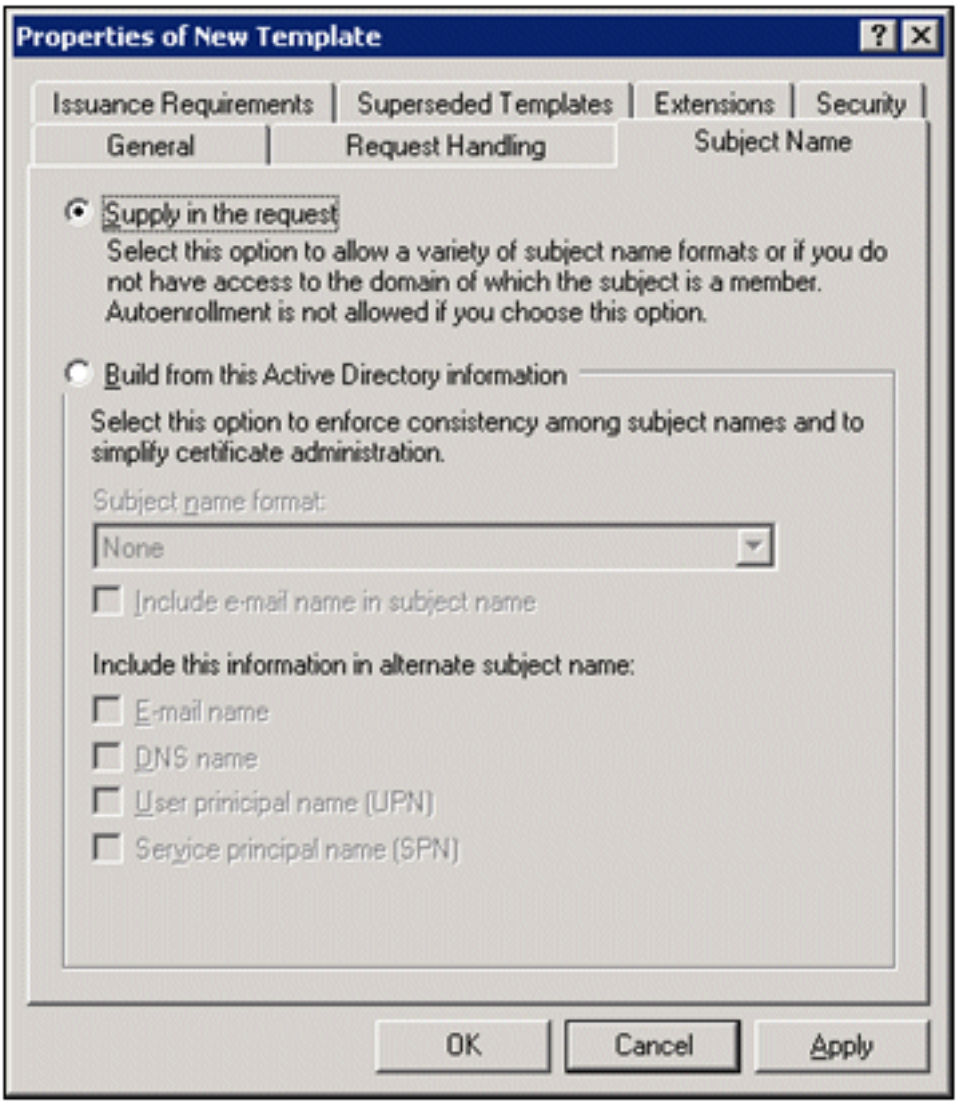


5. Choose **Requests deve usar um dos seguintes CSPs** e verificar **Microsoft Base Cryptographic Provider v1.0**. Desmarque todos os outros CSPs marcados e clique em



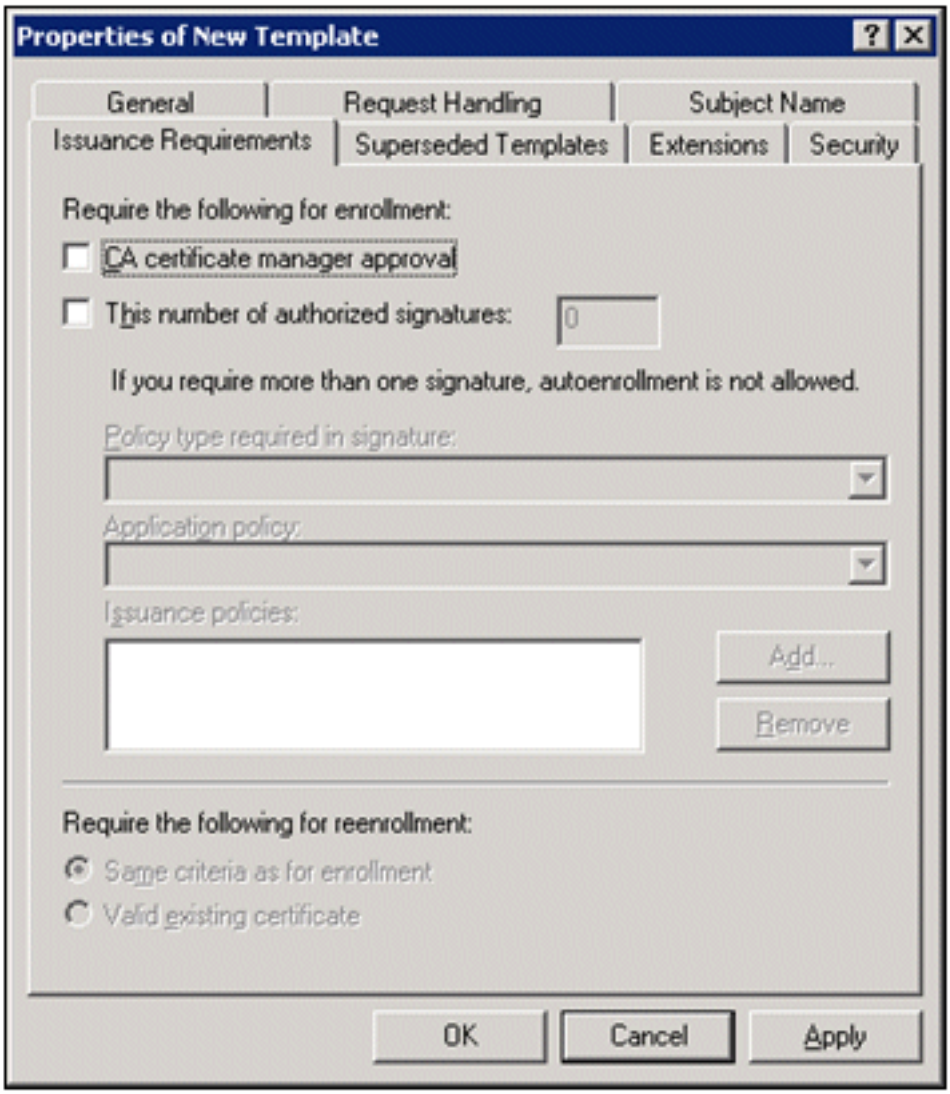
OK.

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



OK.

7. Vá até a guia **Security**, realce o **Domain Admins Group** e verifique se a opção **Enroll** está marcada em Allowed.**Observação:** se você optar por criar a partir dessas informações do Ative Diretory, marque apenas o **Nome UPN** e desmarque a opção **Incluir nome do email** no nome do assunto e no nome do email, pois um nome de email não foi inserido para a conta de Usuário Sem Fio no snap-in Usuários e Computadores do Ative Diretory. Se você não desativar essas duas opções, o registro automático tentará usar o e-mail, o que resultará em um erro de registro automático.
8. Há medidas de segurança adicionais, se necessário, para impedir que os certificados sejam removidos automaticamente. Eles podem ser encontrados na guia Issuance Requirements (Requisitos de emissão). Isso não é discutido mais neste



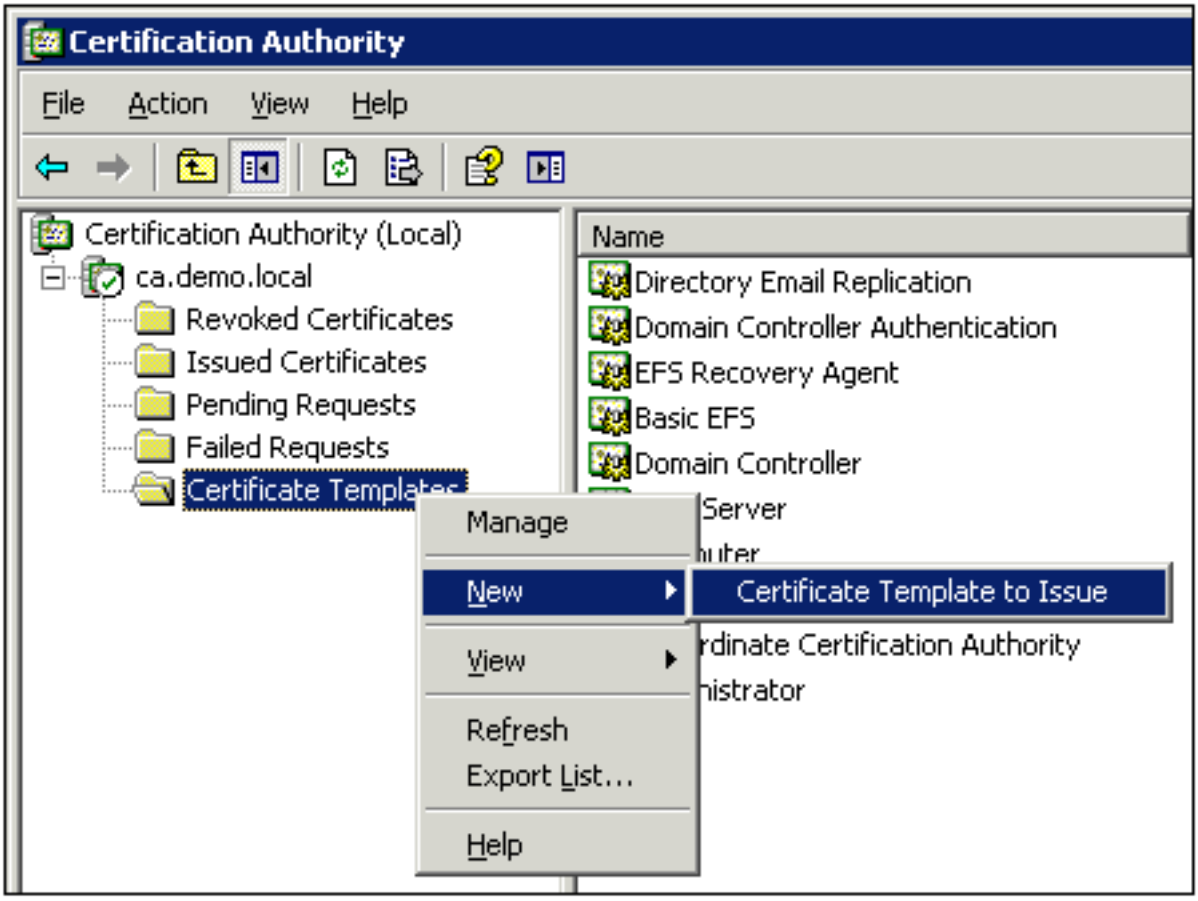
documento.

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

Habilitar o novo modelo de certificado de servidor Web ACS

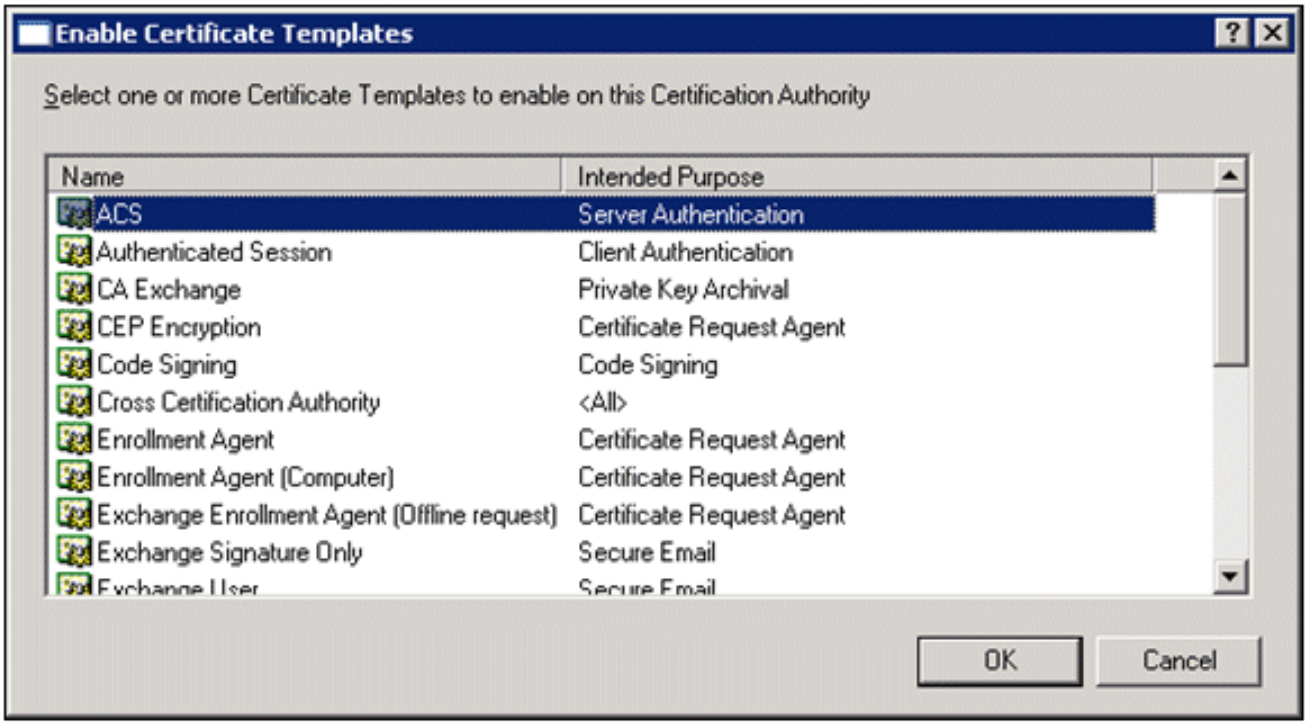
Execute estas etapas:

1. Abra o snap-in Autoridade de Certificação. Execute as etapas de 1 a 3 na seção Criar o modelo de certificado para o servidor Web ACS, escolha a opção **Autoridade de certificação**, escolha **Computador local** e clique em **Concluir**.
2. Na árvore de console da Autoridade de certificação, expanda **ca.demo.local** e clique com o botão direito do mouse em **Modelos de certificado**.
3. Vá para **New > Certificate Template to**

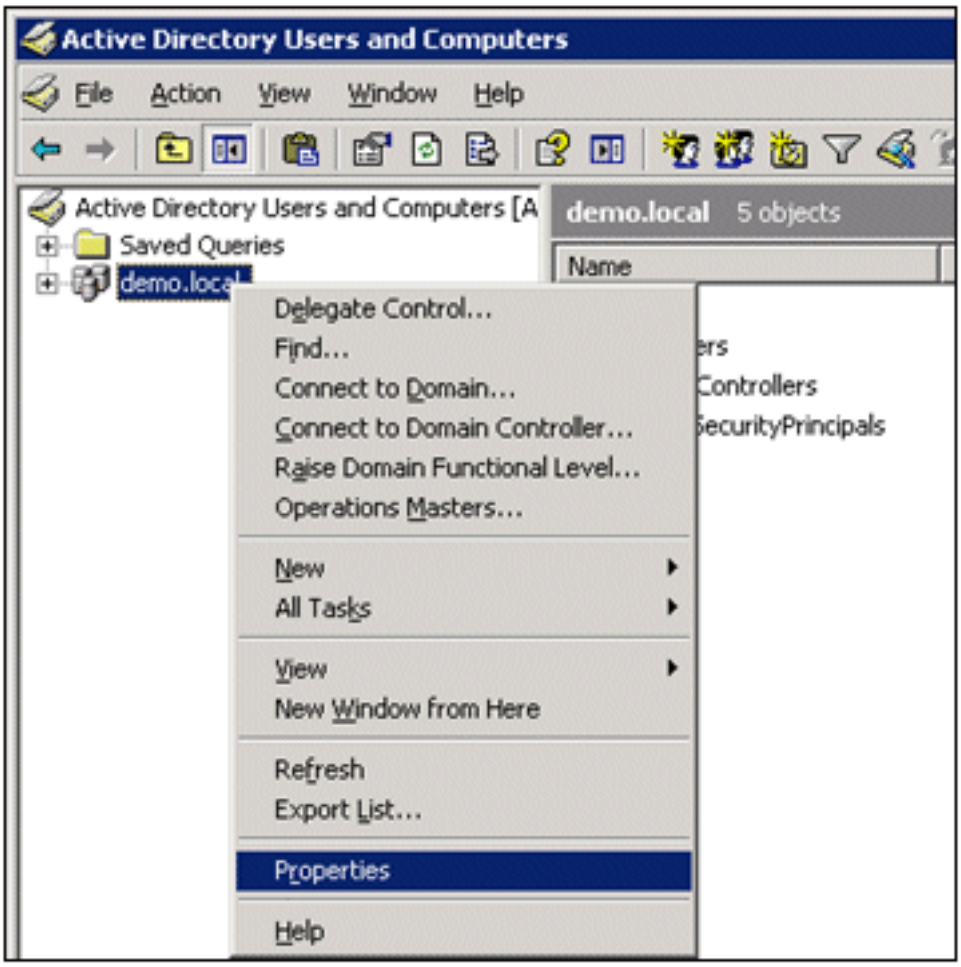


Issue.

4. Clique no **Modelo de certificado ACS**.

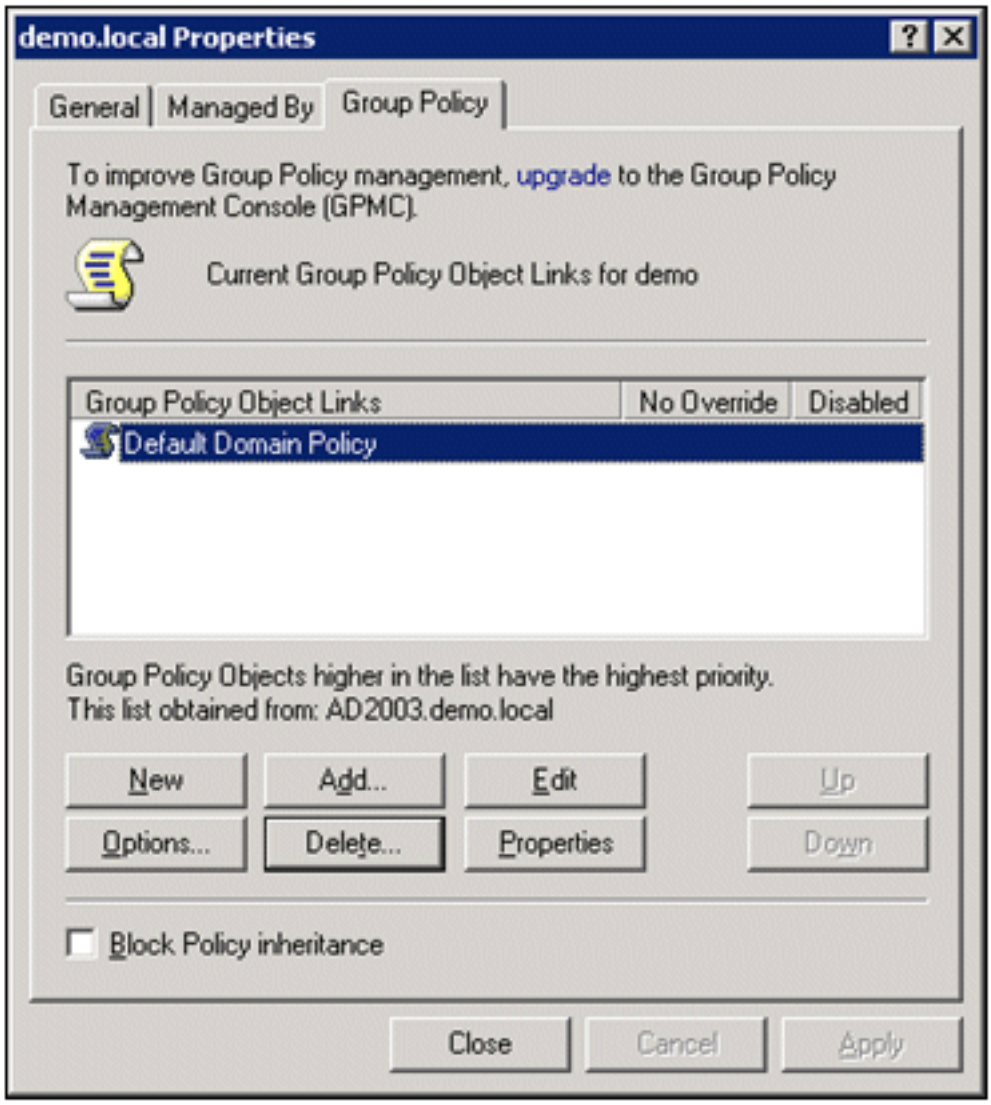


5. Clique em **OK** e abra o **snap-in Usuários e computadores do Ative Diretory**.
6. Na árvore do console, clique duas vezes em **Usuários e computadores do Ative Diretory**, clique com o botão direito do mouse em **demo.local** e clique em



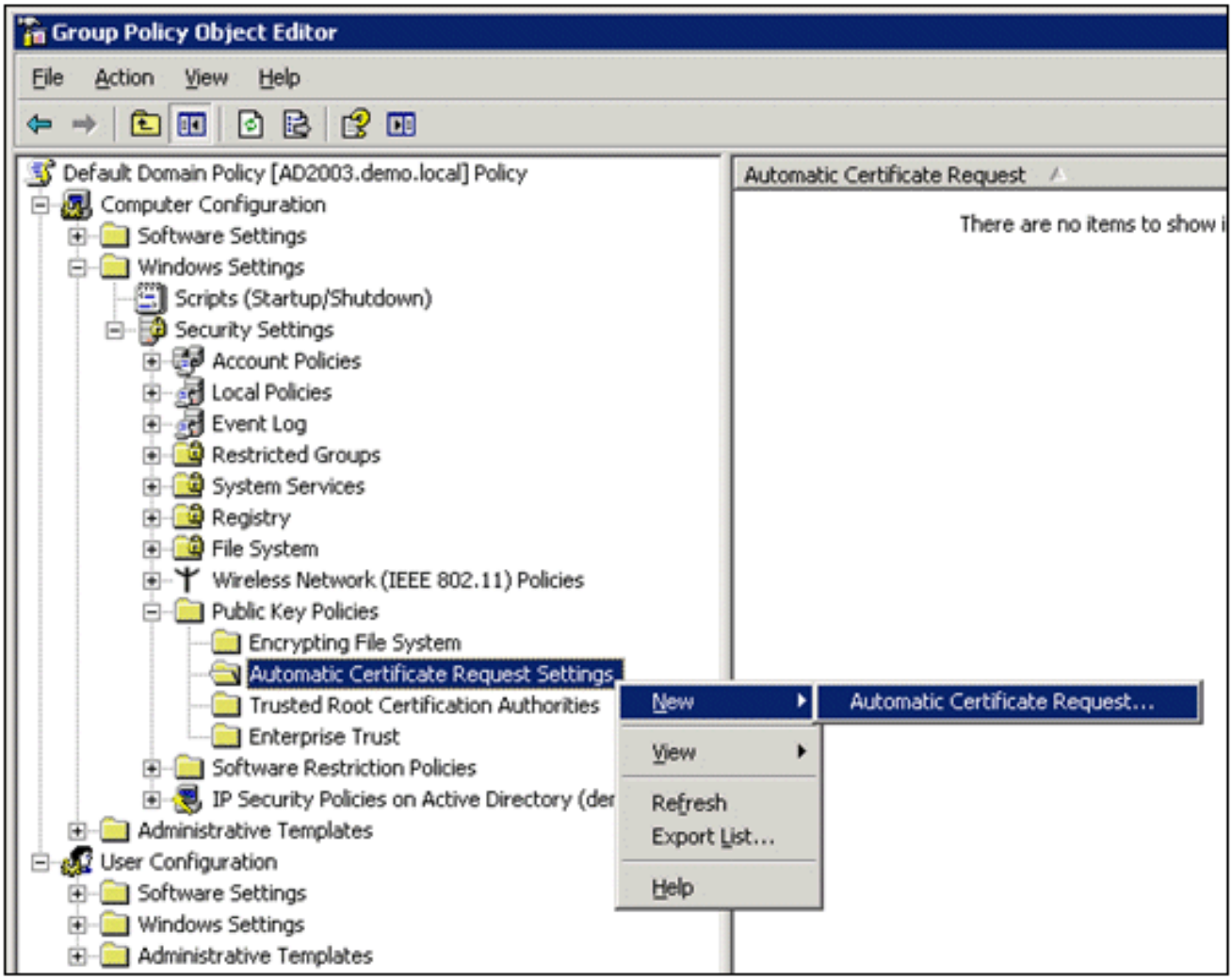
Propriedades.

7. Na guia Diretiva de Grupo, clique em **Diretiva de Domínio Padrão** e em **Editar**. Isso abre o snap-in Editor de Objeto de Diretiva de



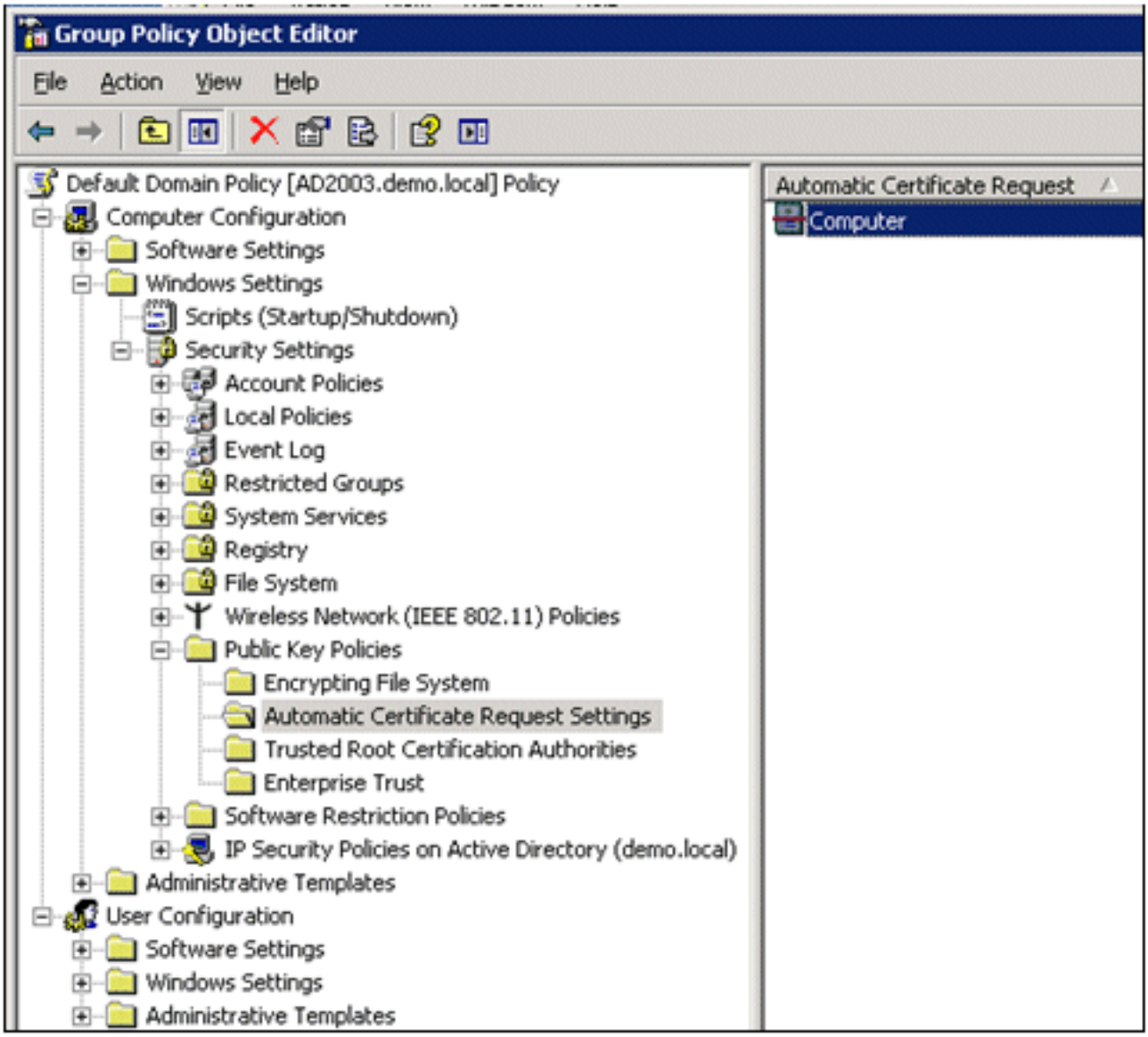
Grupo.

8. Na árvore do console, expanda Configuração do Computador > **Configurações do Windows** > Configurações de Segurança > Políticas de Chave Pública e escolha Configurações Automáticas de Solicitação de
Certificado.

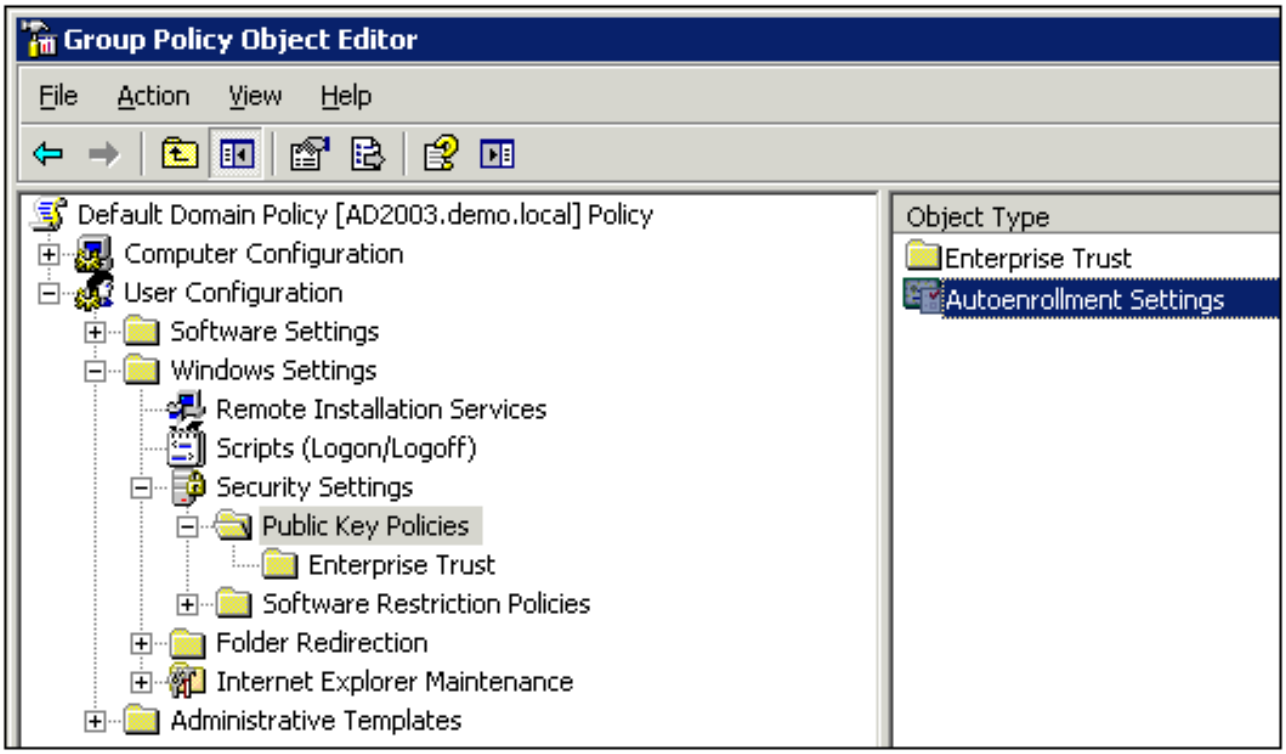


9. Clique com o botão direito do mouse em **Automatic Certificate Request Settings** e escolha **New > Automatic Certificate Request**.
10. Na página Bem-vindo ao Assistente para configuração de solicitação automática de certificado, clique em **Avançar**.
11. Na página Modelo de certificado, clique em **Computador** e em **Avançar**.

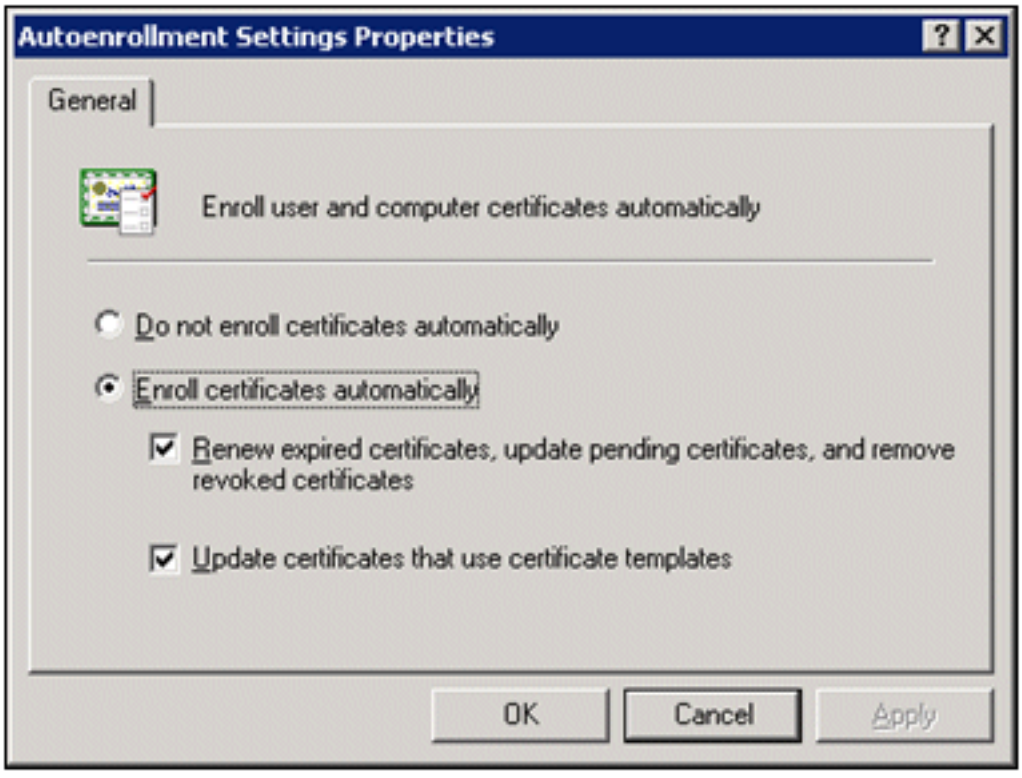
12. Quando concluir a página do Assistente para configuração de solicitação automática de certificado, clique em **Concluir**. O tipo de certificado Computador agora aparece no painel de detalhes do snap-in Editor de Objeto de Diretiva de Grupo.



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 registro automático**.



15. Escolha **Registrar certificados automaticamente** e marque **Renovar certificados expirados, atualizar certificados pendentes e remover certificados revogados** e **Atualizar certificados que usam modelos de**



certificado.

16. Click **OK**.

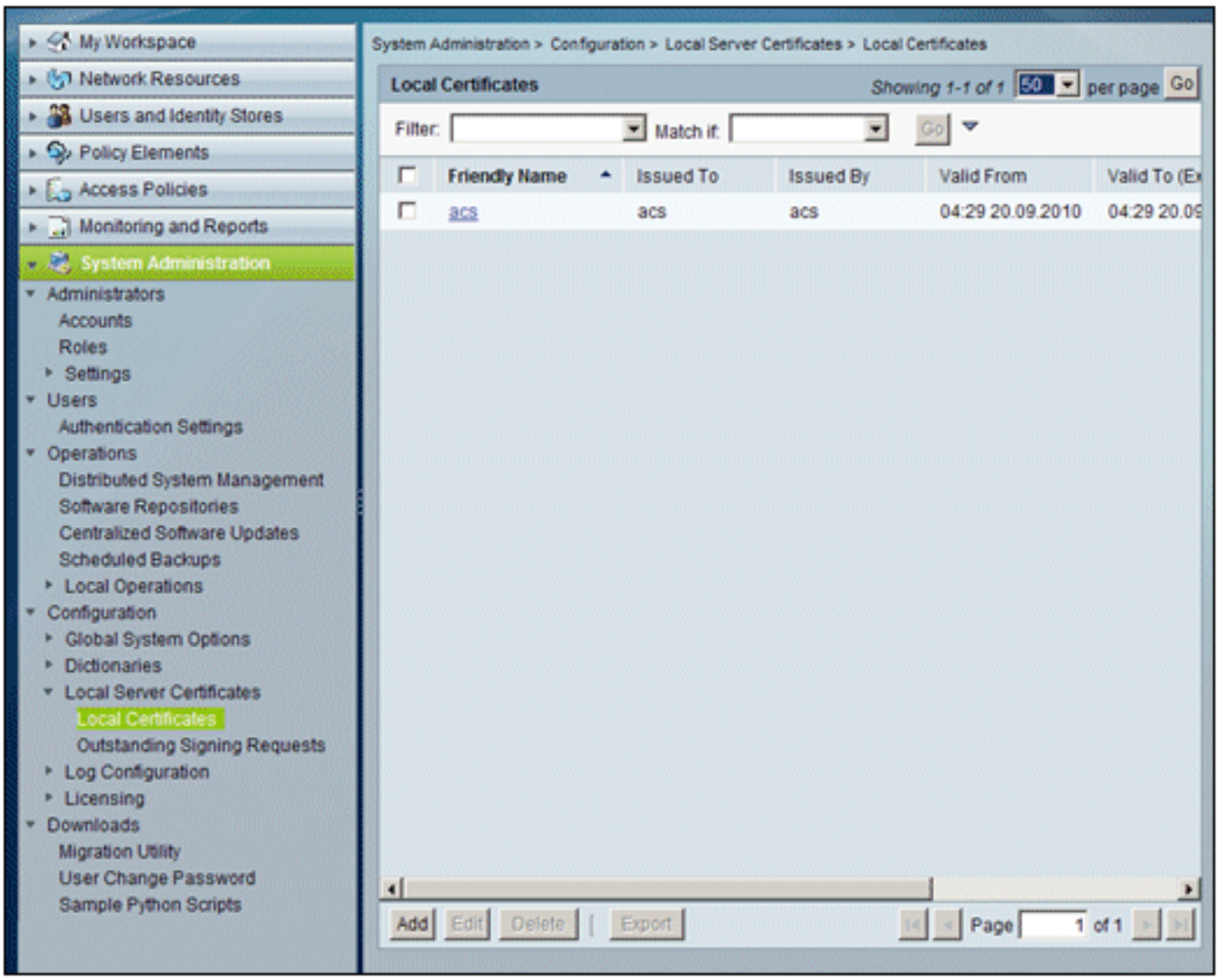
Configuração do certificado ACS 5.1

Configurar certificado exportável para ACS

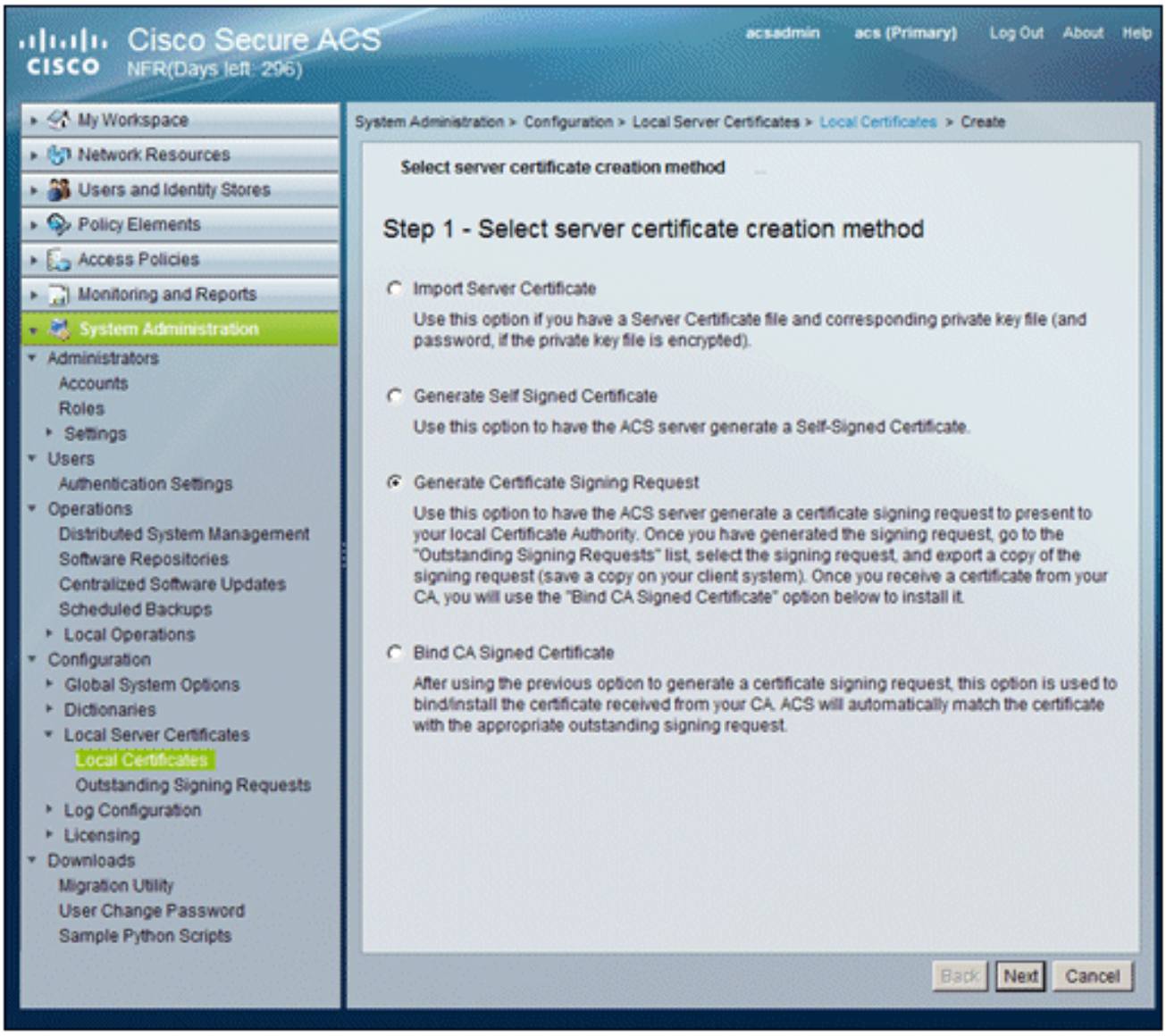
Observação: o servidor ACS deve obter um certificado de servidor do servidor de CA raiz da empresa para autenticar um cliente PEAP WLAN.

Observação: verifique se o Gerenciador do IIS não está aberto durante o processo de configuração de certificado, pois isso causa problemas com as informações armazenadas em cache.

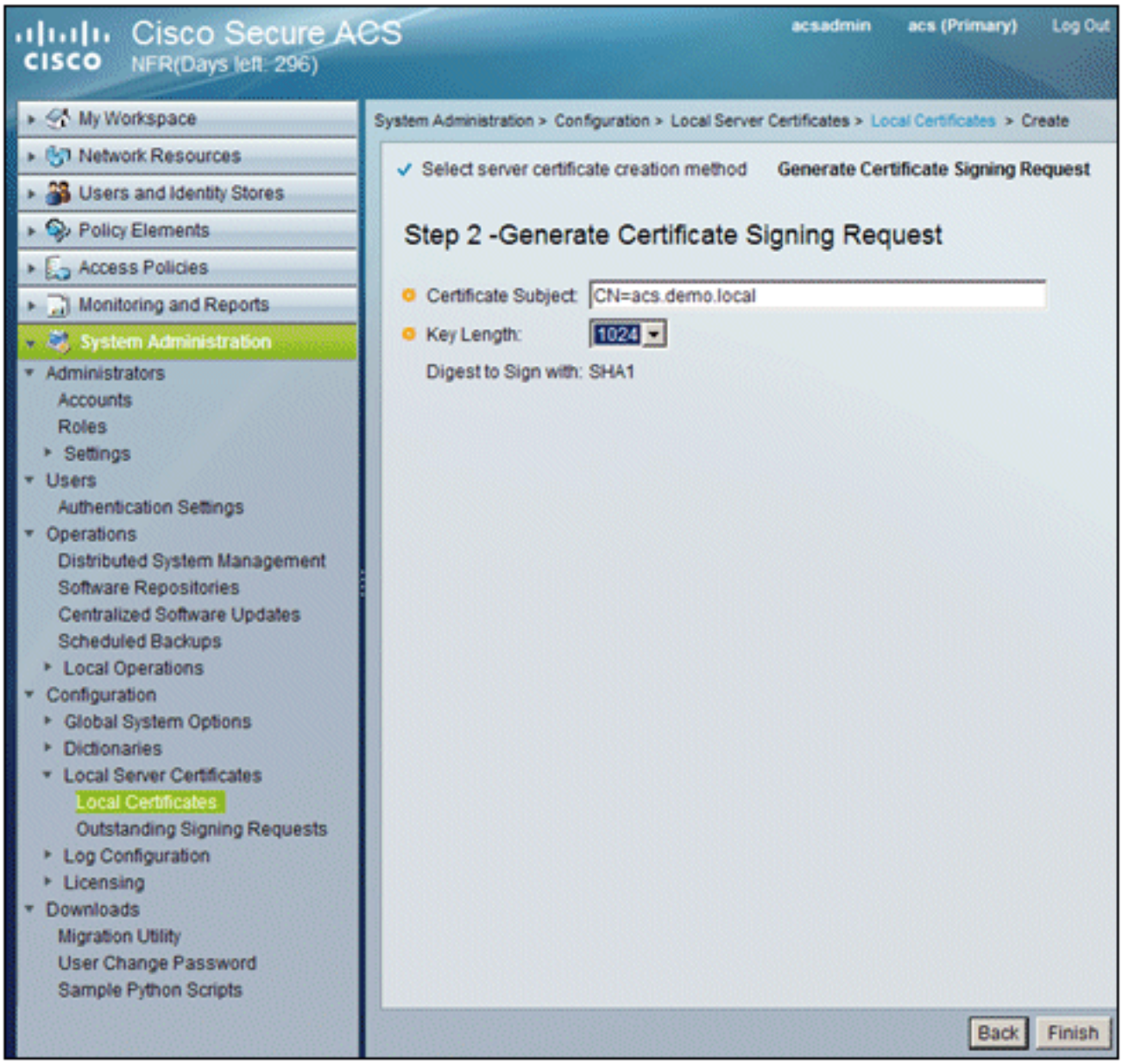
1. Efetue login no servidor ACS com uma conta de direitos de administrador.
2. Vá para **Administração do sistema > Configuração > Certificados do servidor local**. Clique em
   Add.



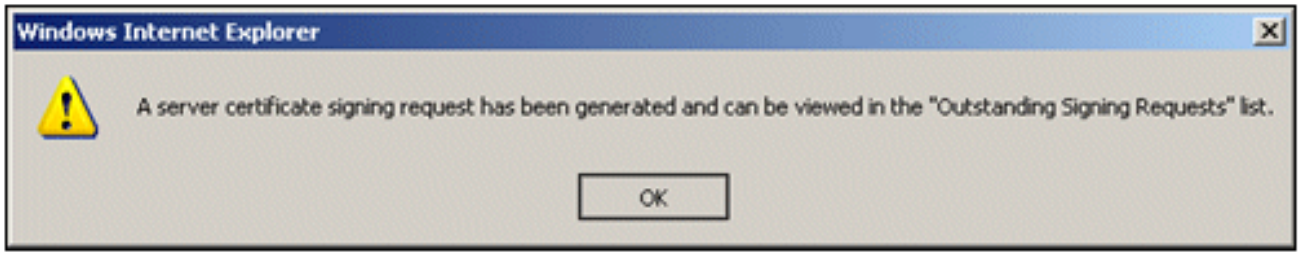
3. Ao escolher um método de criação de certificado de servidor, escolha **Gerar Solicitação de Assinatura de Certificado**. Clique em
   Next.



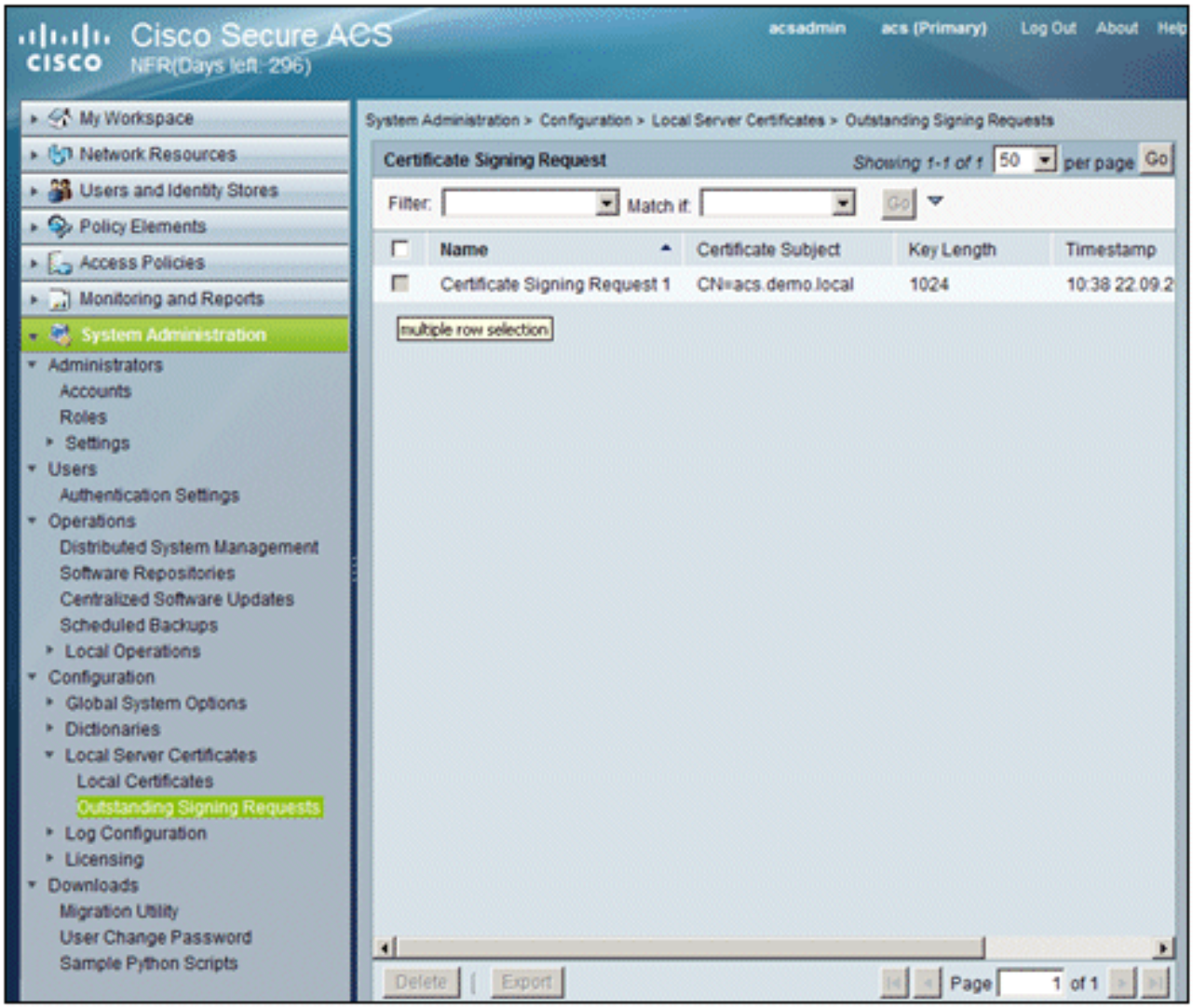
4. Insira o assunto e o comprimento da chave do certificado como exemplo e clique em **Finish**:Assunto do certificado - **CN=acs.demo.local**Comprimento da chave - **1024**



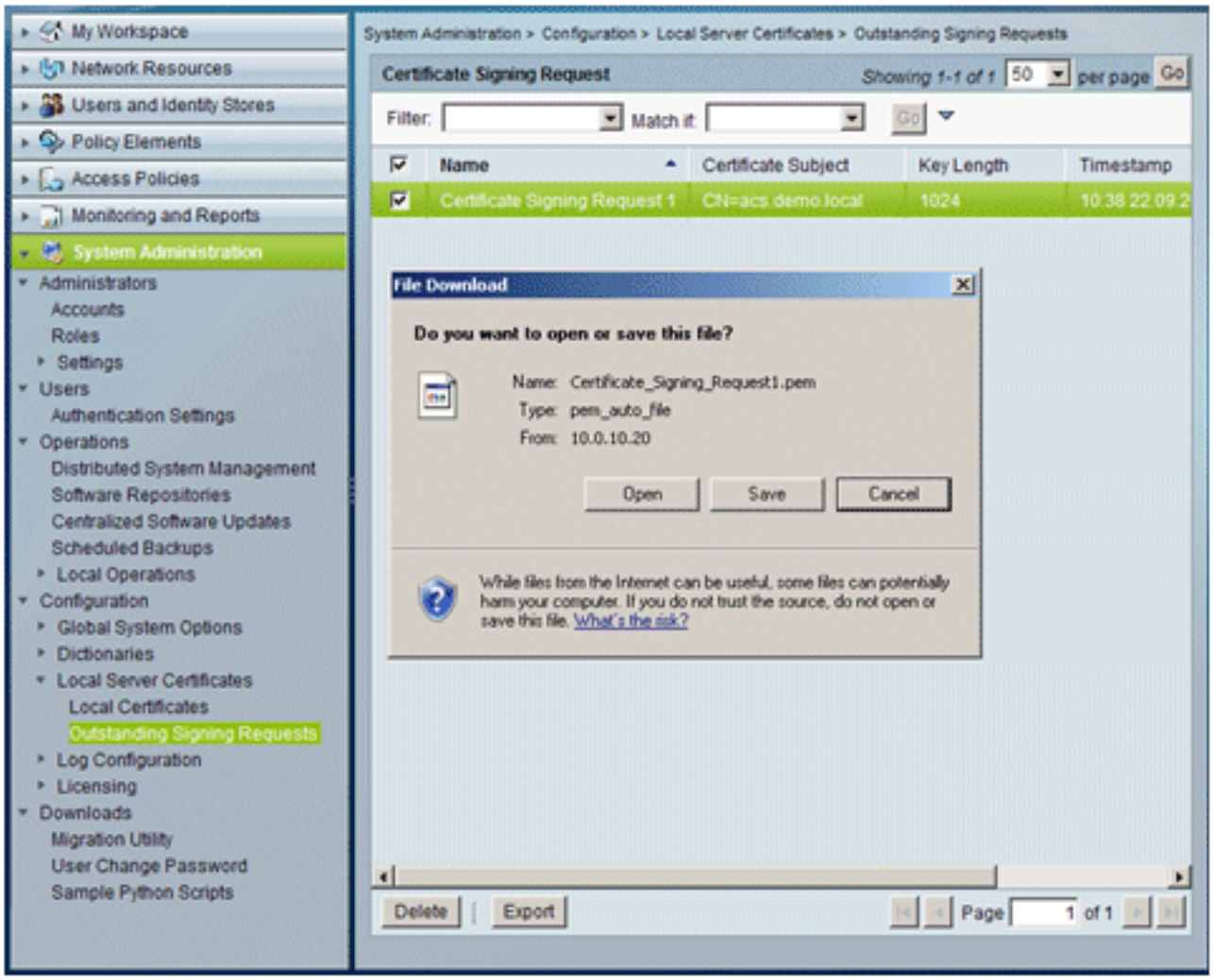
5. O ACS solicitará que uma solicitação de assinatura de certificado tenha sido gerada. Click **OK**.



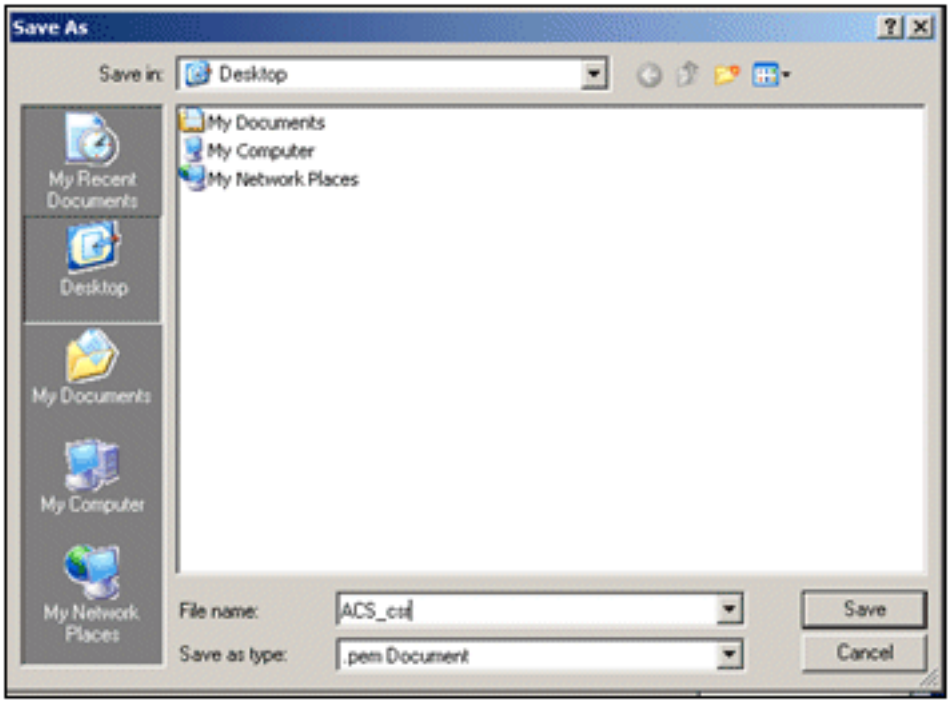
6. Em Administração do sistema, vá para **Configuração > Certificados do servidor local > Solicitações de assinatura pendentes**.**Observação:** o motivo para essa etapa é que o Windows 2003 não permite chaves exportáveis e você precisa gerar uma solicitação de certificado com base no Certificado ACS criado anteriormente.



7. Escolha a entrada **Certificate Signing Request** e clique em **Export**.



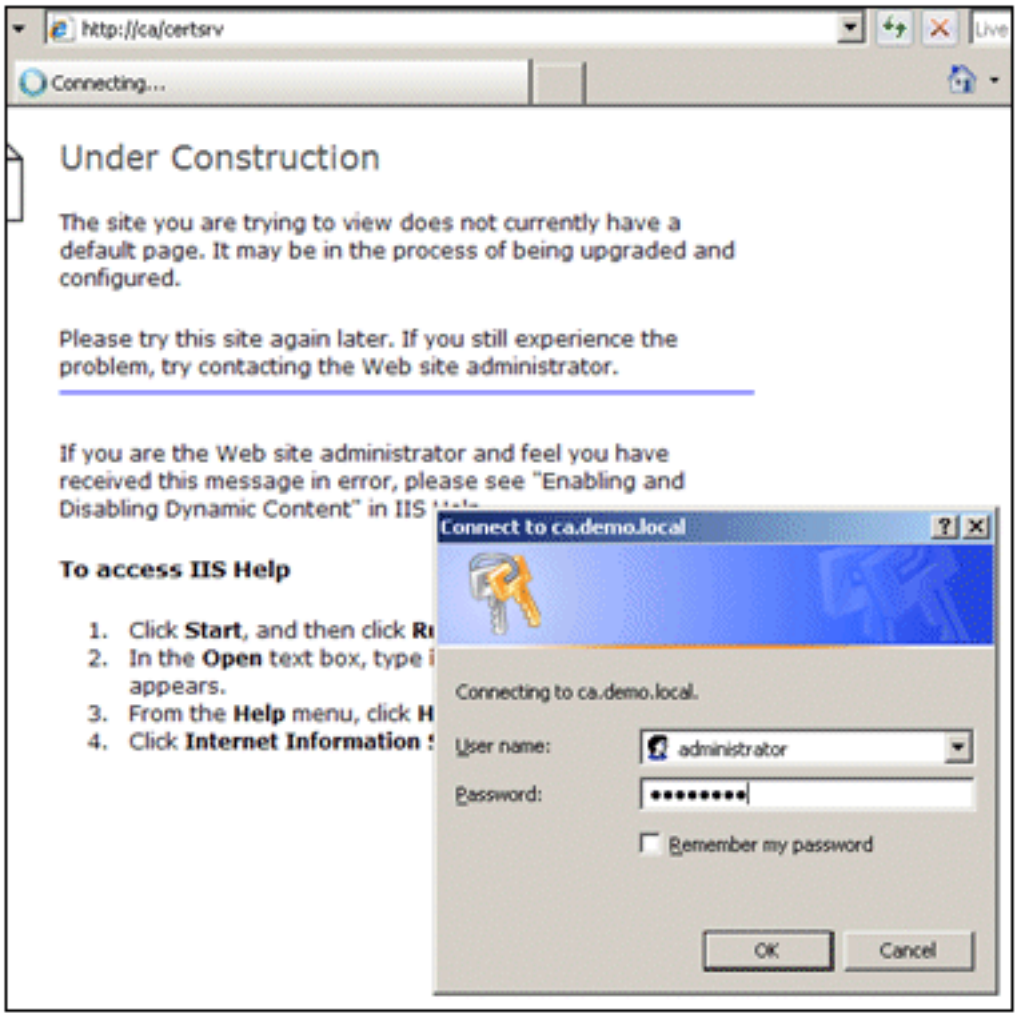
8. Salve o arquivo **.pem** do certificado ACS no desktop.



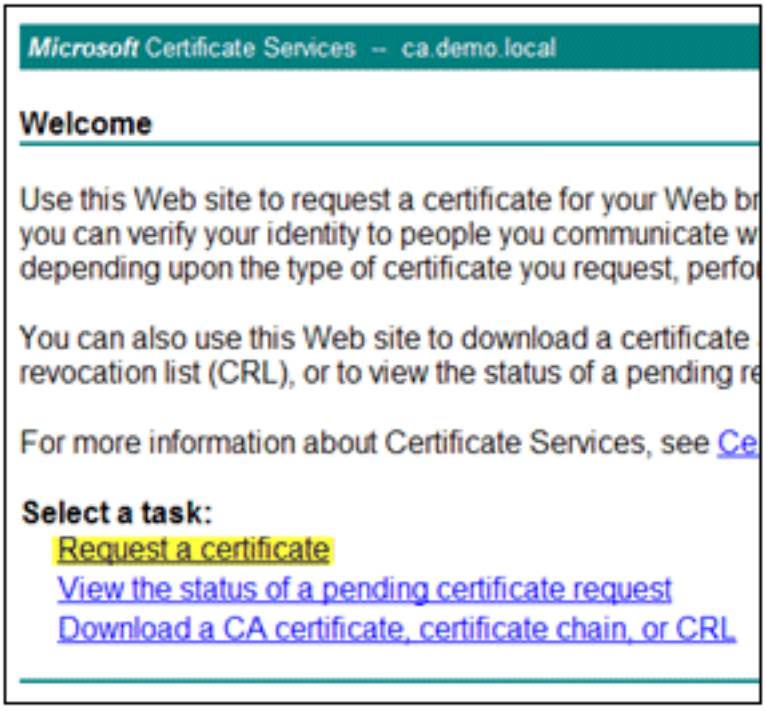
Instale o certificado no software ACS 5.1

Execute estas etapas:

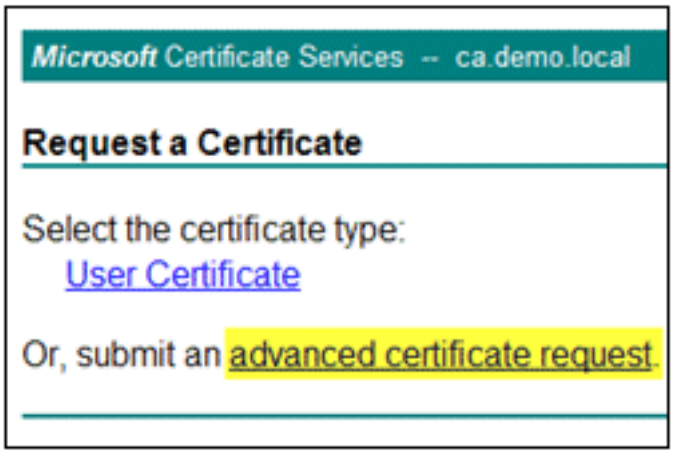
1. Abra um navegador e conecte-se à URL do servidor de CA **http://10.0.10.10/certsrv**.



2. A janela Serviços de Certificados da Microsoft é exibida. Escolha **Solicitar um certificado**.

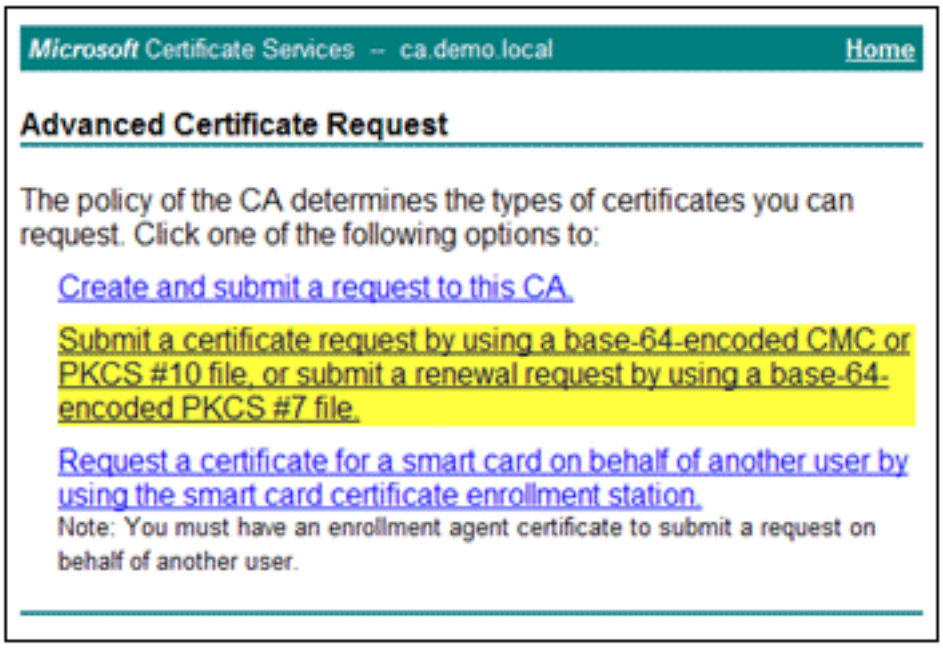


3. Clique em para enviar uma **solicitação de certificado**



avançada.

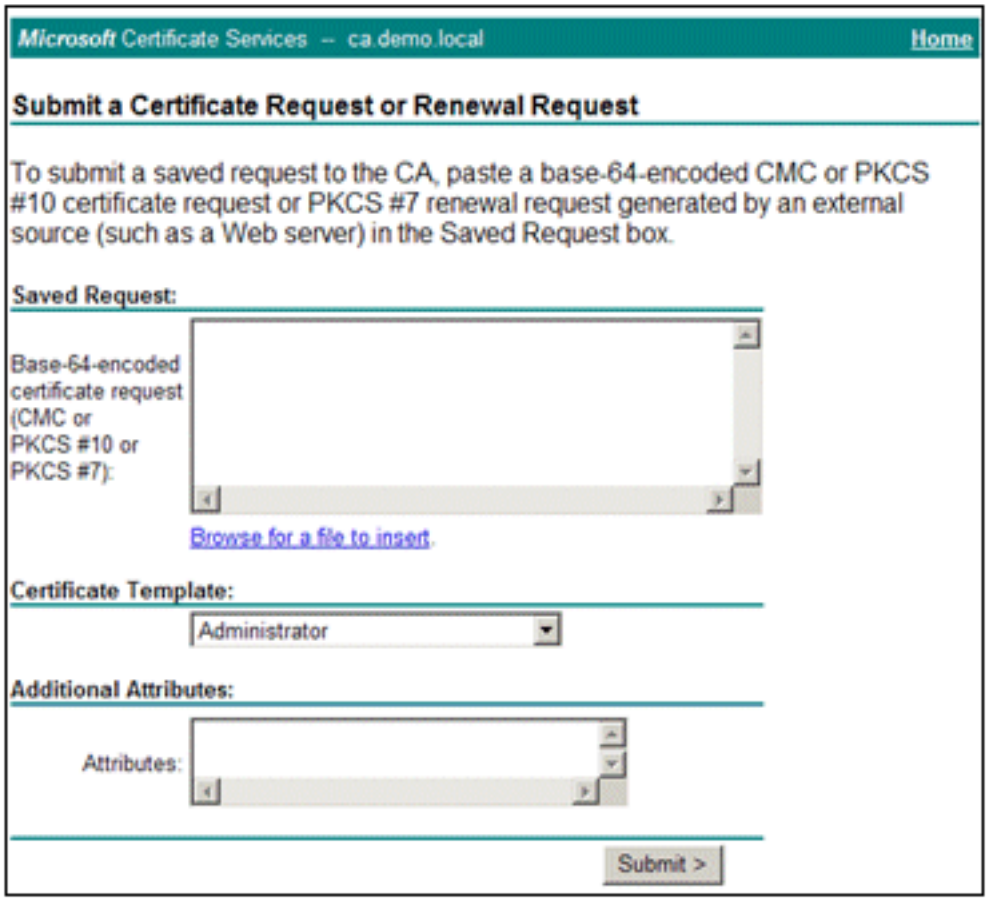
4. Na solicitação avançada, clique em **Enviar uma solicitação de certificado usando um código**



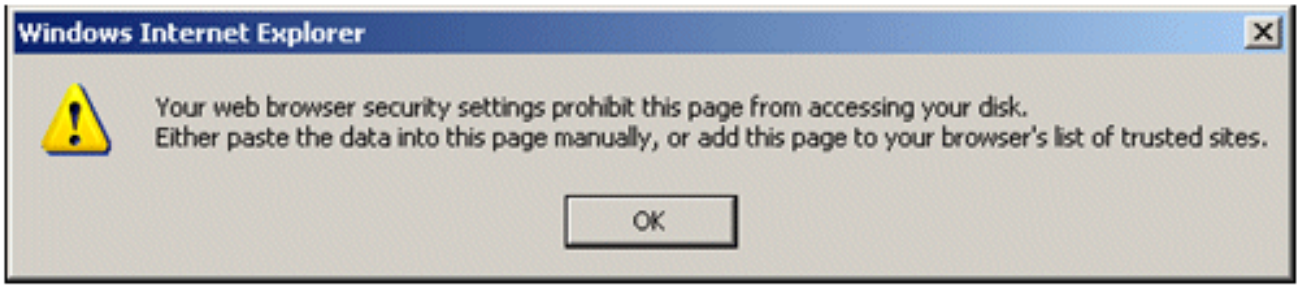
de base 64...

5. No campo Solicitação salva, se a segurança do navegador permitir, navegue até o arquivo de solicitação de certificado ACS anterior e insira-

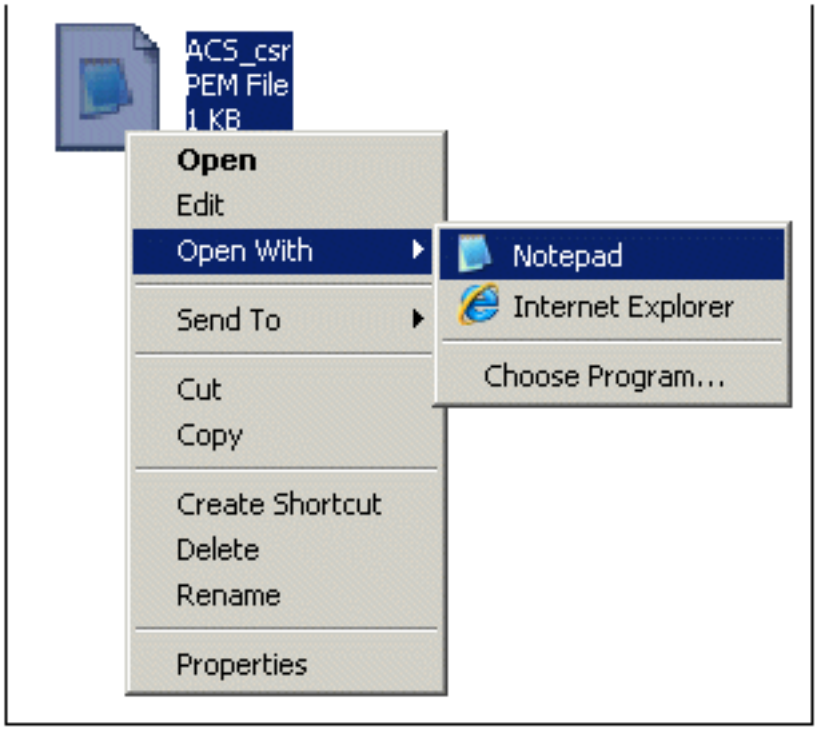
o.



6. As configurações de segurança do navegador talvez não permitam acessar o arquivo em um disco. Em caso afirmativo, clique em **OK** para executar uma colagem manual.

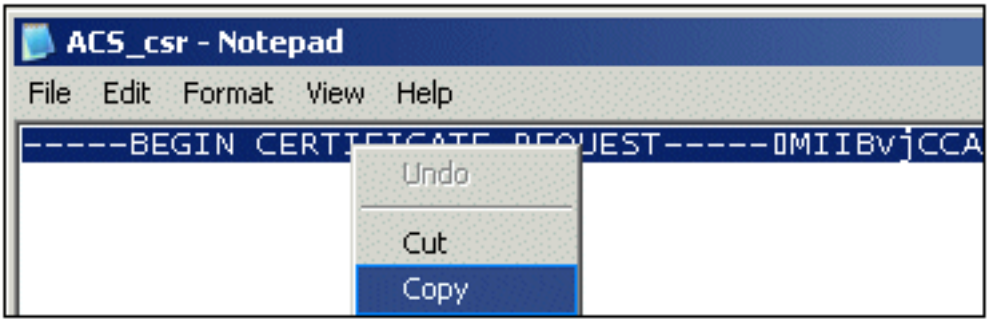


7. Localize o arquivo ACS *.pem da exportação do ACS anterior. Abra o arquivo usando um editor de texto (por exemplo, o Bloco de



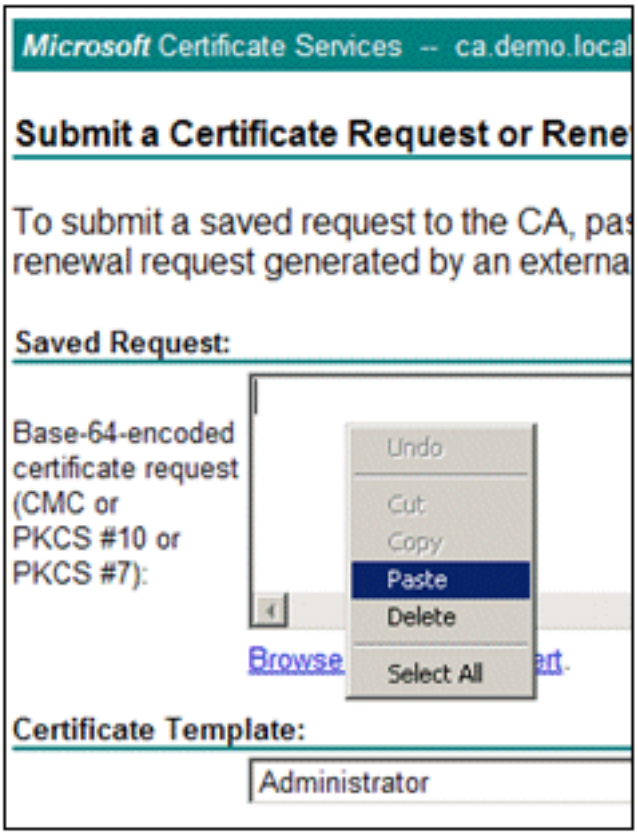
Notas).

8. Realce todo o conteúdo do arquivo e clique em



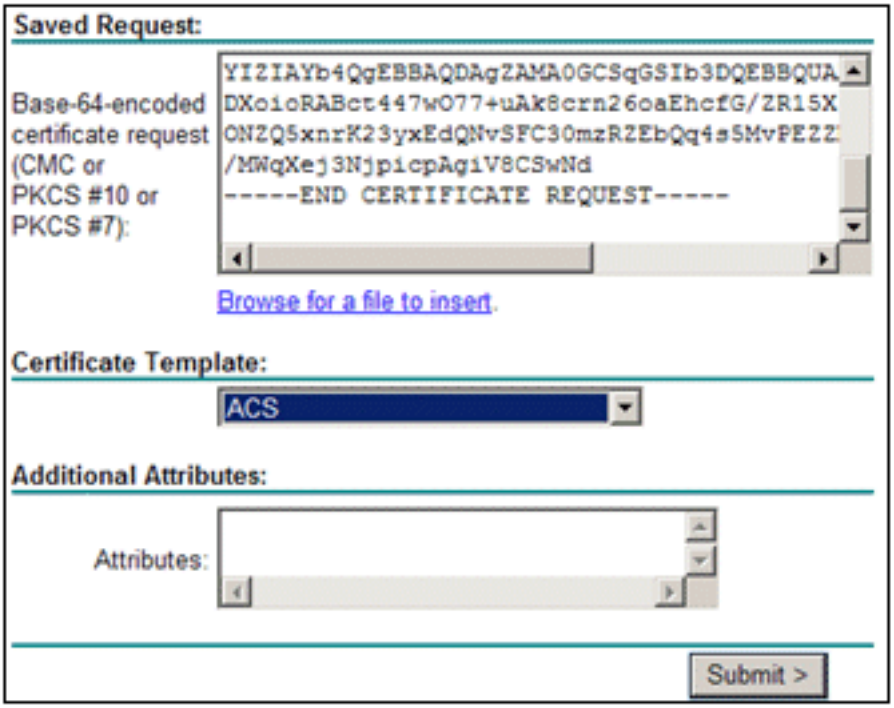
Copiar.

9. Retorne à janela de solicitação de certificado da Microsoft. **Cole** o conteúdo copiado no

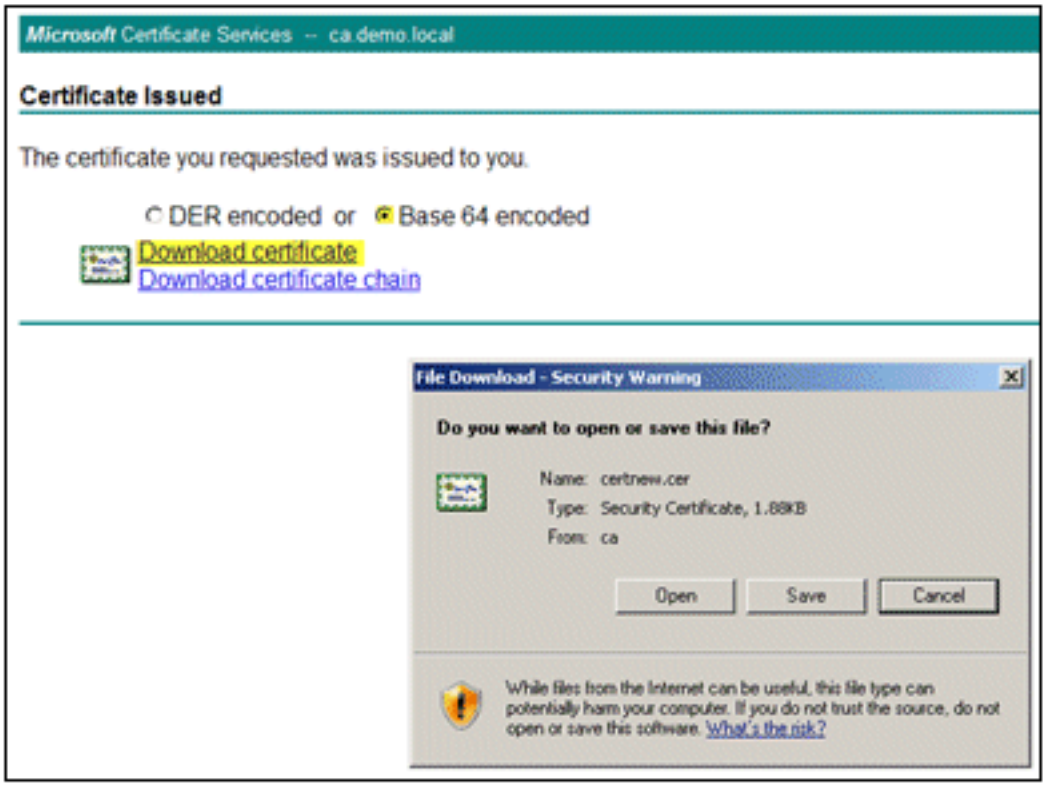


campo Solicitação salva.

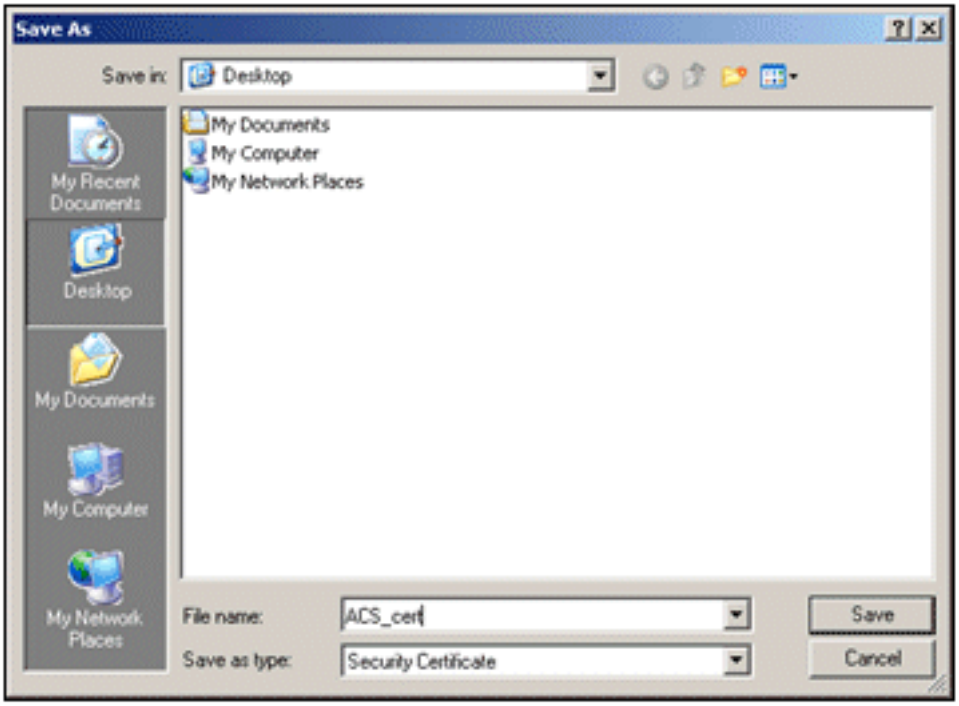
10. Escolha **ACS** como o Modelo de certificado e clique em **Enviar**.



11. Depois que o certificado for emitido, escolha **Base 64 encoded** e clique em **Download certificate**.

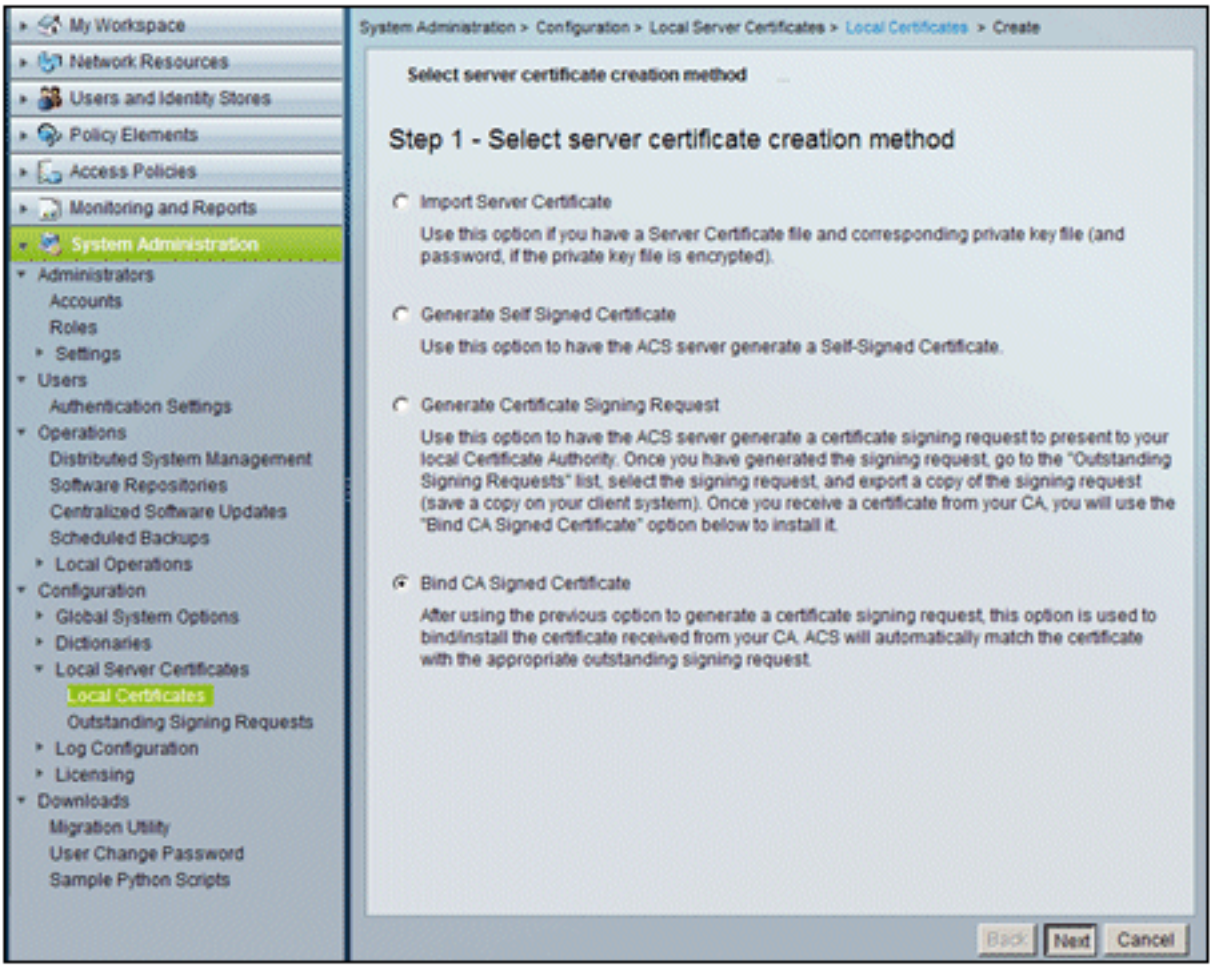


12. Clique em **Save** para salvar o certificado na área de



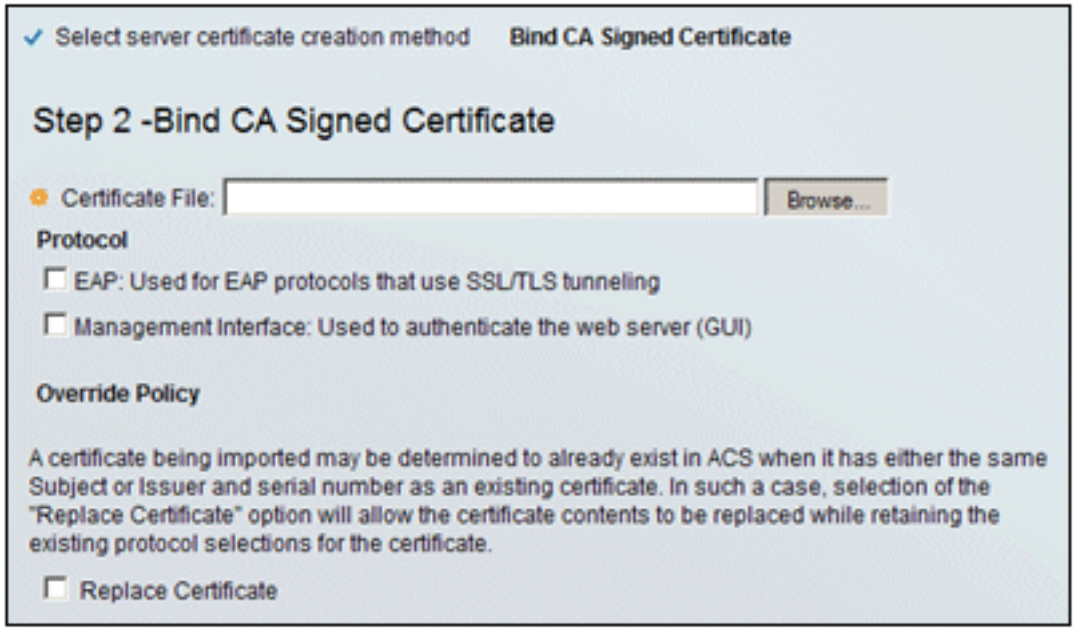
trabalho.

13. Vá para **ACS > Administração do sistema > Configuração > Certificados de servidor local**. Escolha **Bind CA Signed Certificate** e clique em



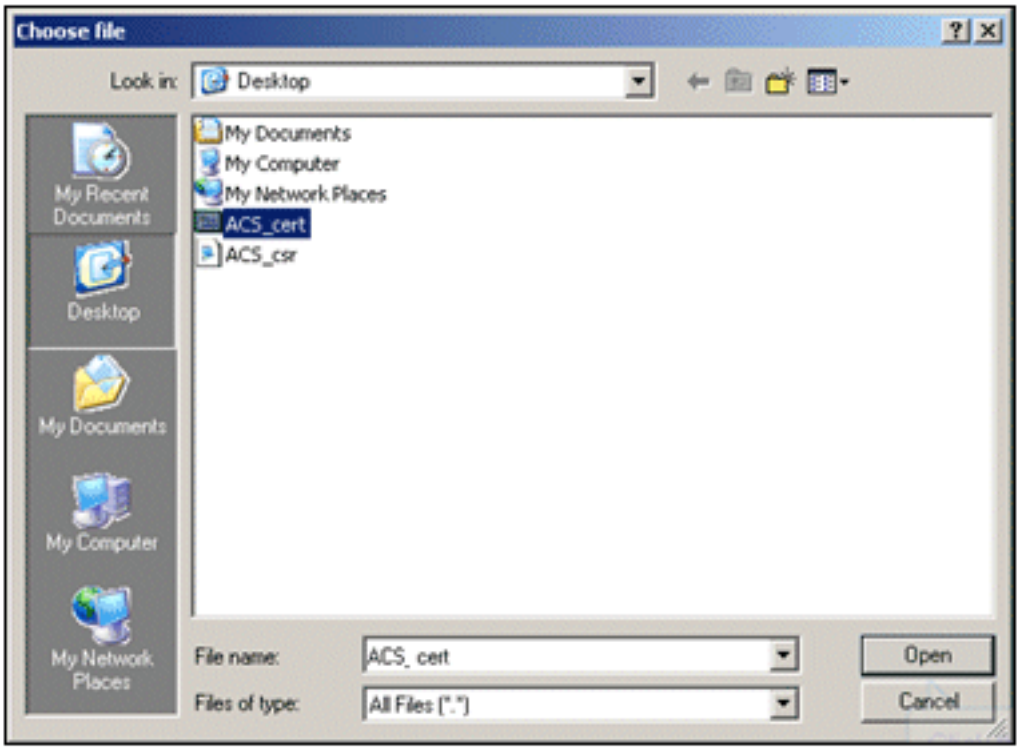
Next.

14. Clique em **Browse** e localize o certificado



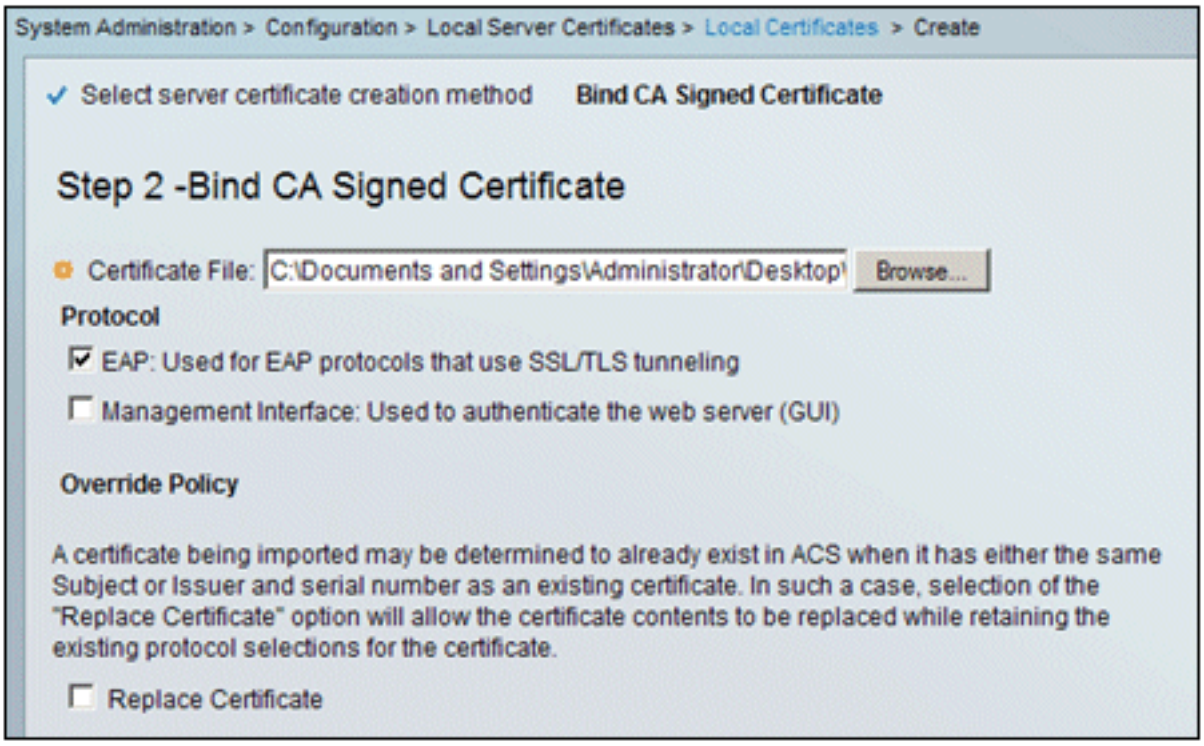
salvo.

15. Escolha o certificado ACS que foi emitido pelo servidor CA e clique em

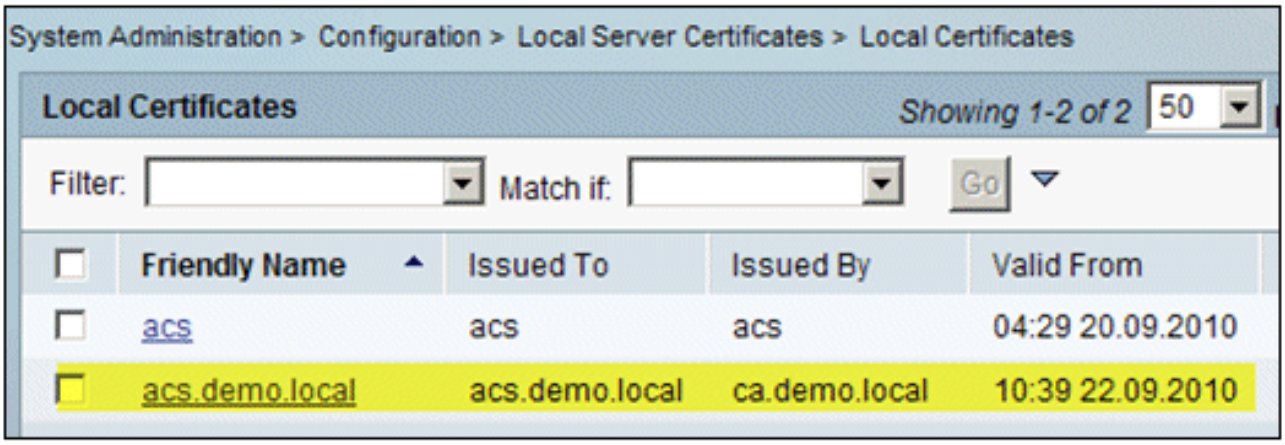


Abrir.

16. Além disso, marque a caixa Protocol (Protocolo) para **EAP** e clique em **Finish**.



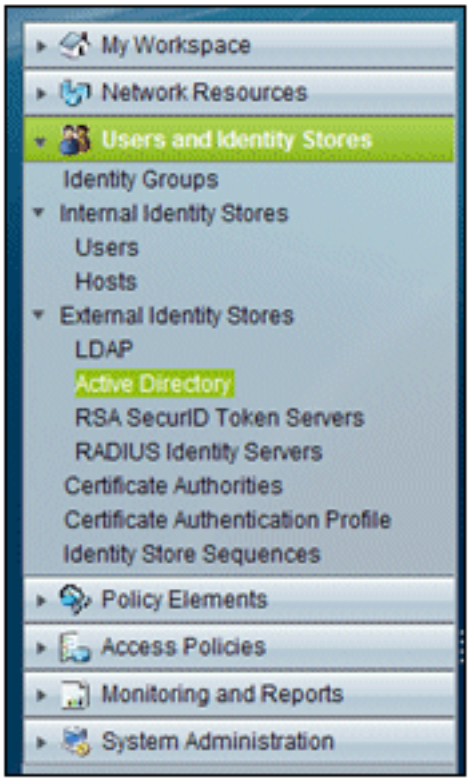
17. O certificado ACS emitido pela CA aparecerá no certificado local ACS.



Configurar o Repositório de Identidades do ACS para o Ative Diretory

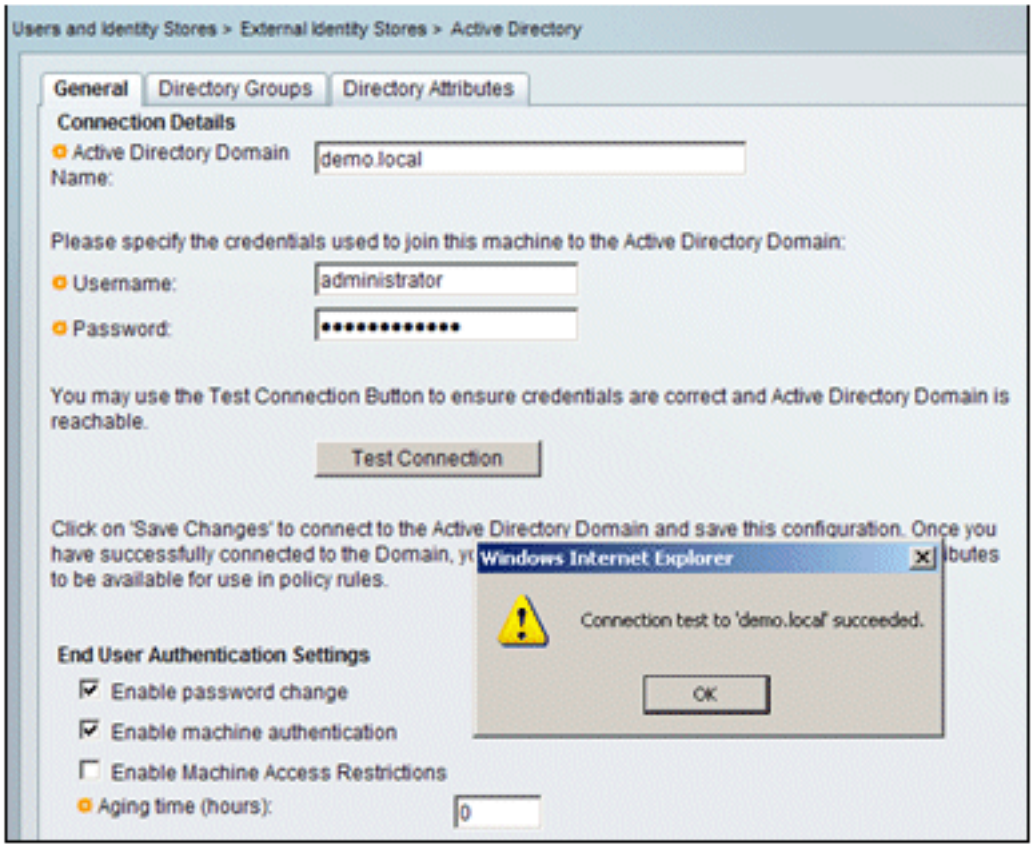
Execute estas etapas:

1. Conecte-se ao ACS e faça login com a conta de administrador.
2. Vá para **Users and Identity Stores > External Identity Stores > Ative**



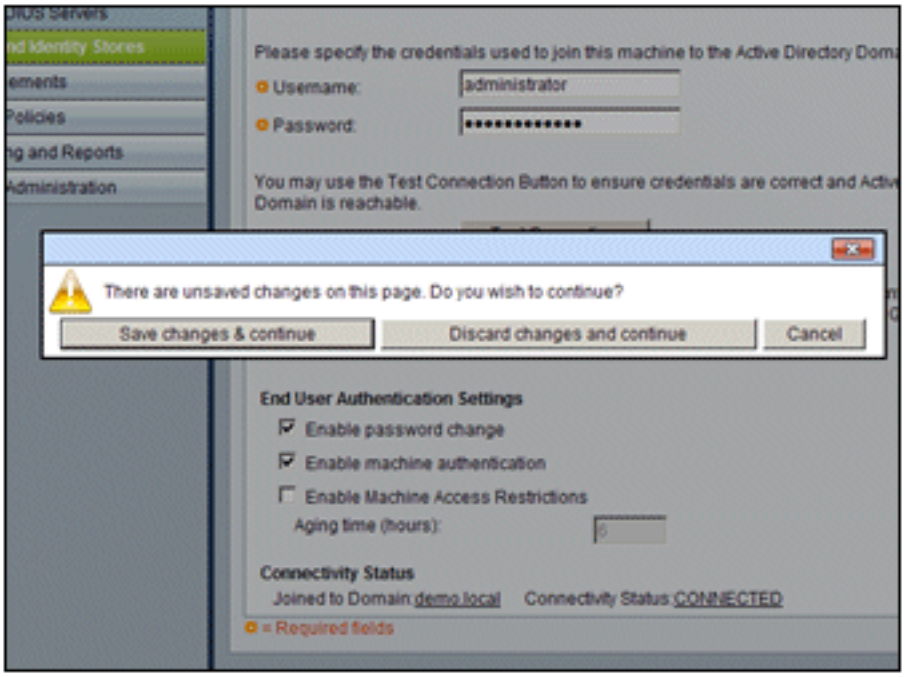
Diretory.

3. Insira o *demo* do domínio do Ative Diretory.*local*, insira a senha do servidor e clique em **Testar conexão**. Clique em **OK** para



continuar.

4. Clique em **Save**

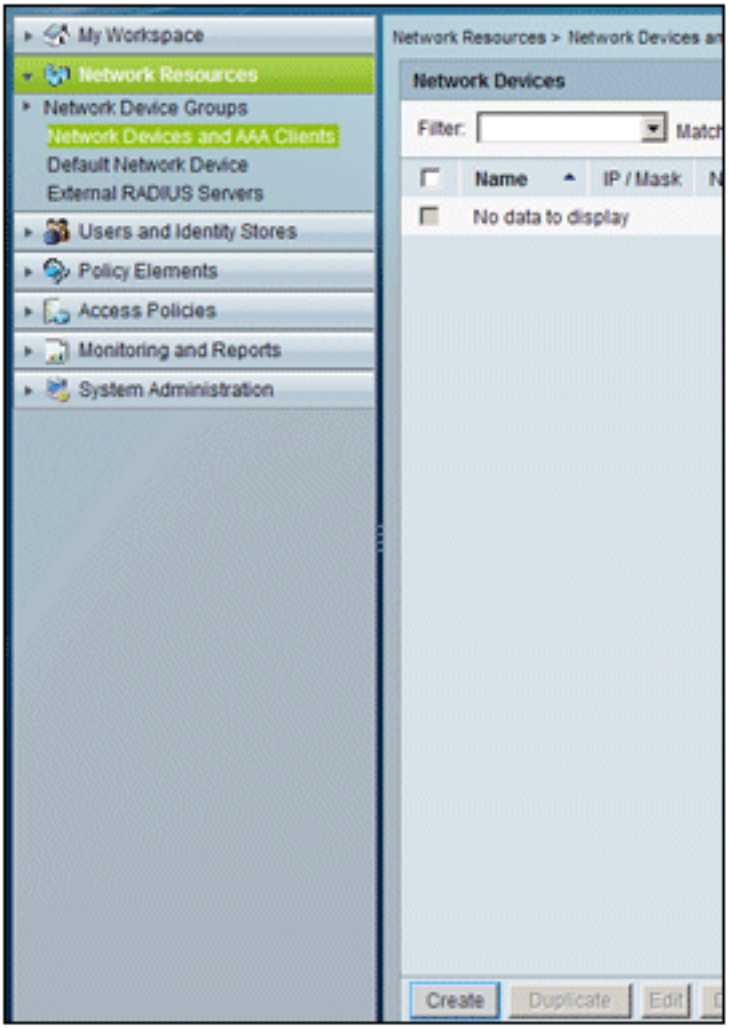


Changes. **Observação:** para obter mais informações sobre o procedimento de integração do ACS 5.x, consulte [ACS 5.x e posterior: Exemplo de Configuração de Integração com o Microsoft Ative Diretory](#).

Adicionar um controlador ao ACS como um cliente AAA

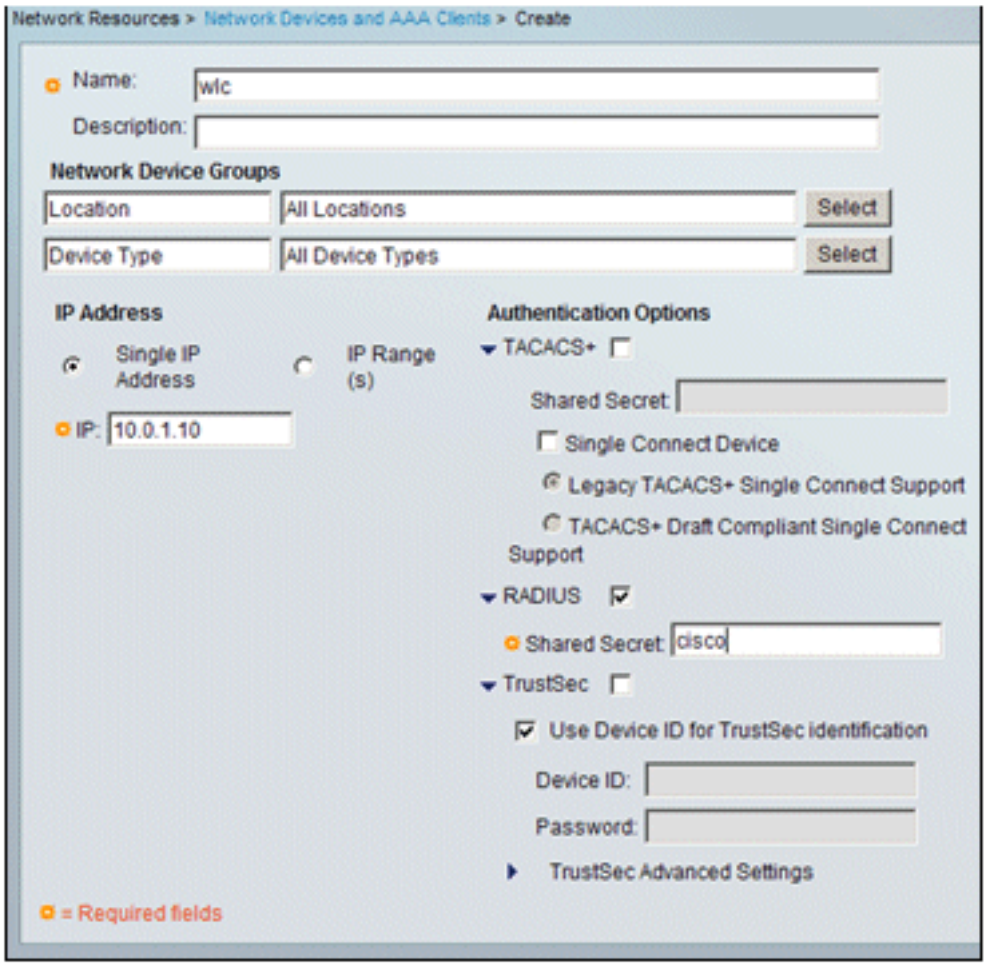
Execute estas etapas:

1. Conecte-se ao ACS e vá para **Network Resources > Network Devices and AAA Clients**.



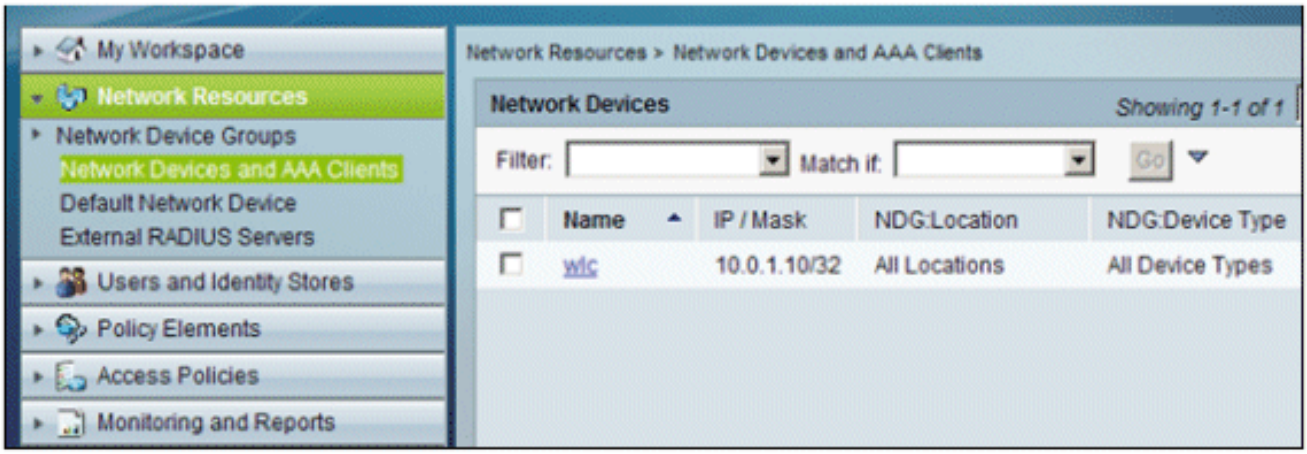
Clique em **Criar**.

2. Insira nestes campos:Nome - **wlc**IP - **10.0.1.10**Caixa de seleção RADIUS - **Marcada**Segredo



compartilhado - **cisco**

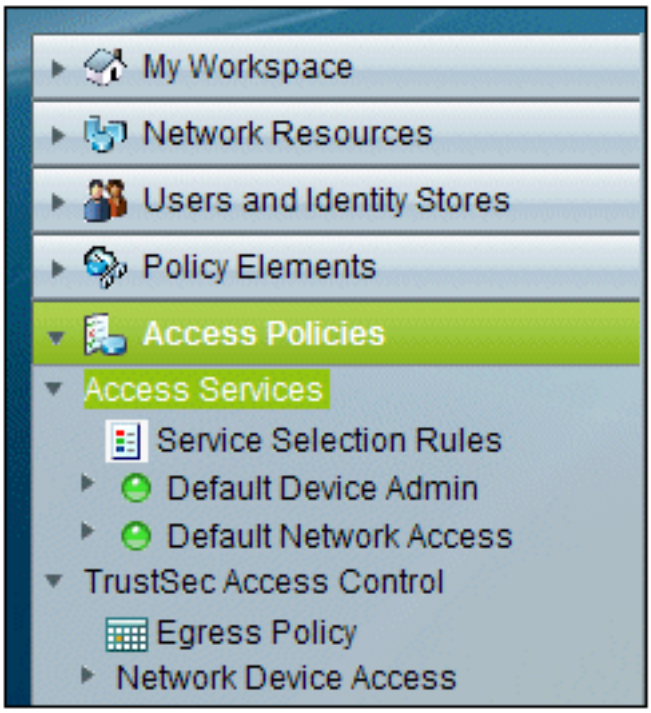
3. Clique em **Enviar** quando terminar. A controladora aparecerá como uma entrada na lista de dispositivos de rede
ACS.



Configurar políticas de acesso ACS para rede sem fio

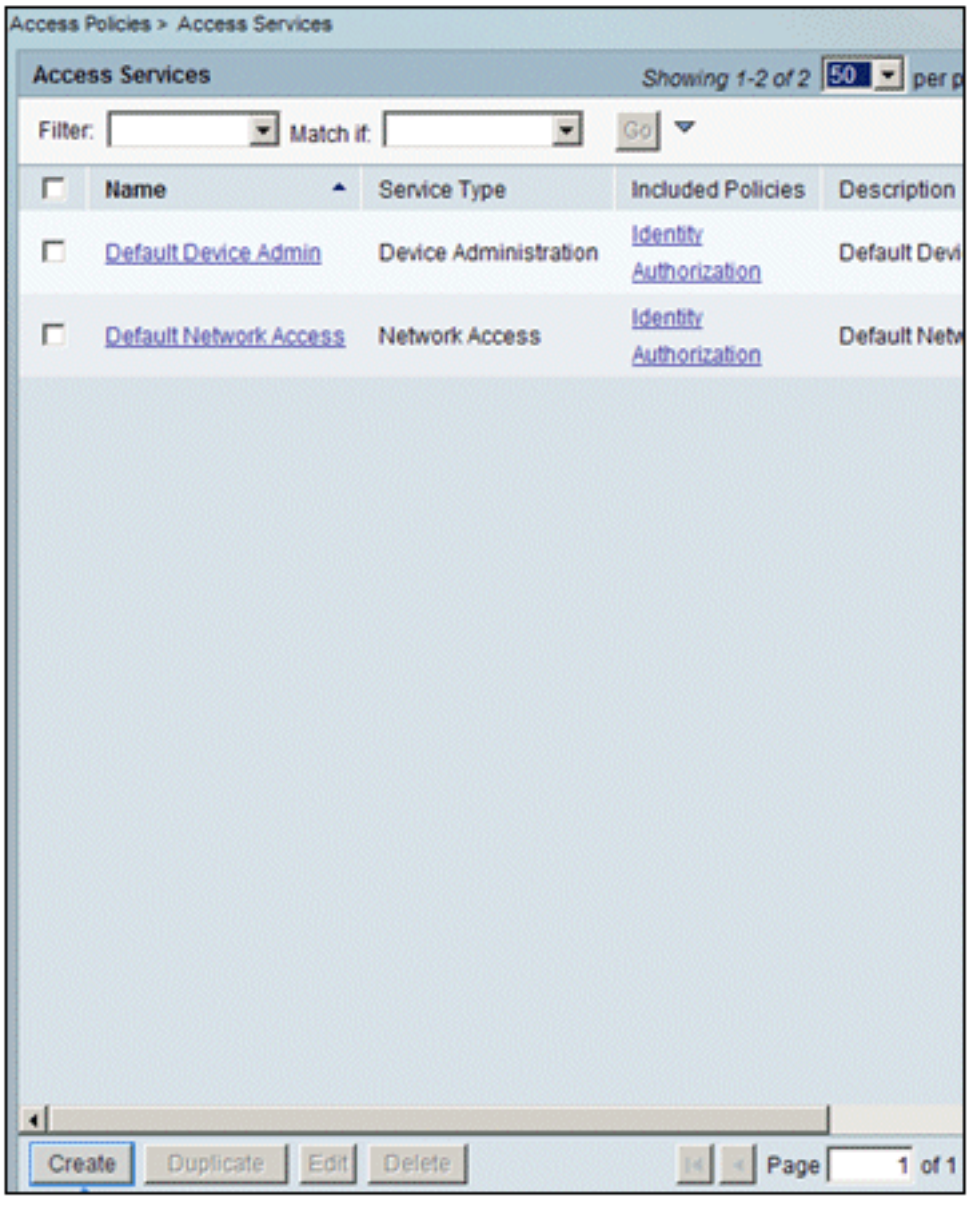
Execute estas etapas:

1. No ACS, vá para **Access Policies > Access**



Services.

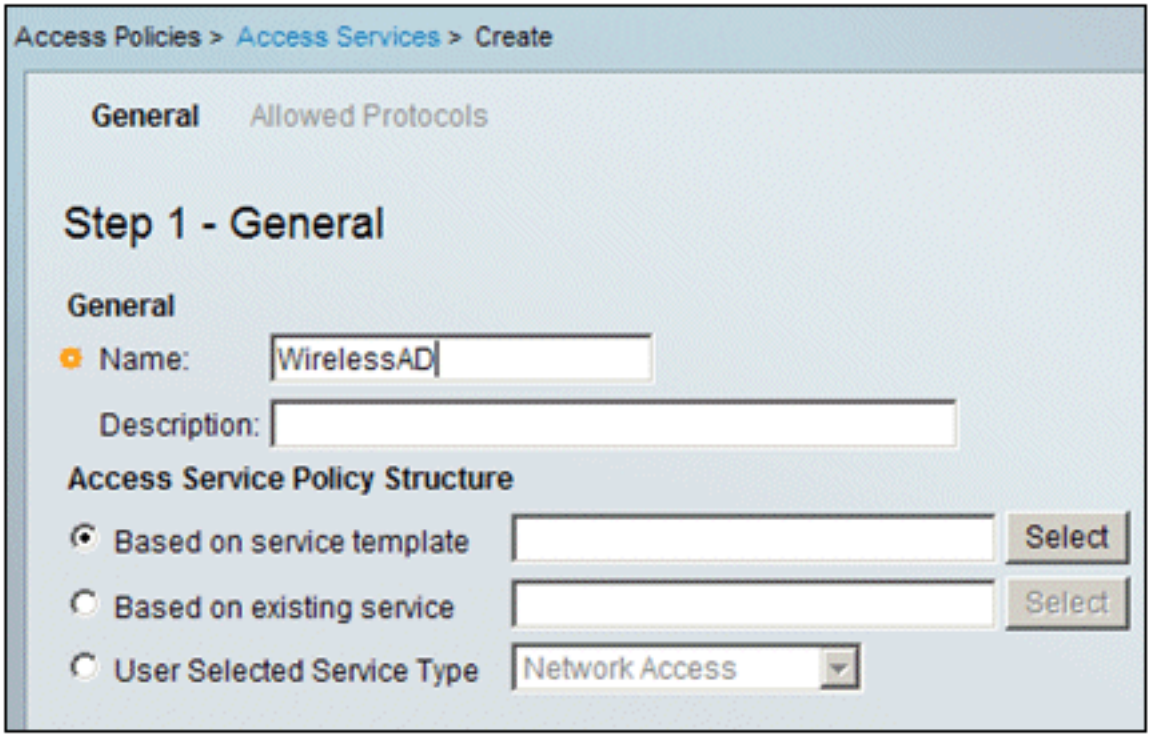
2. Na janela Serviços do Access, clique em



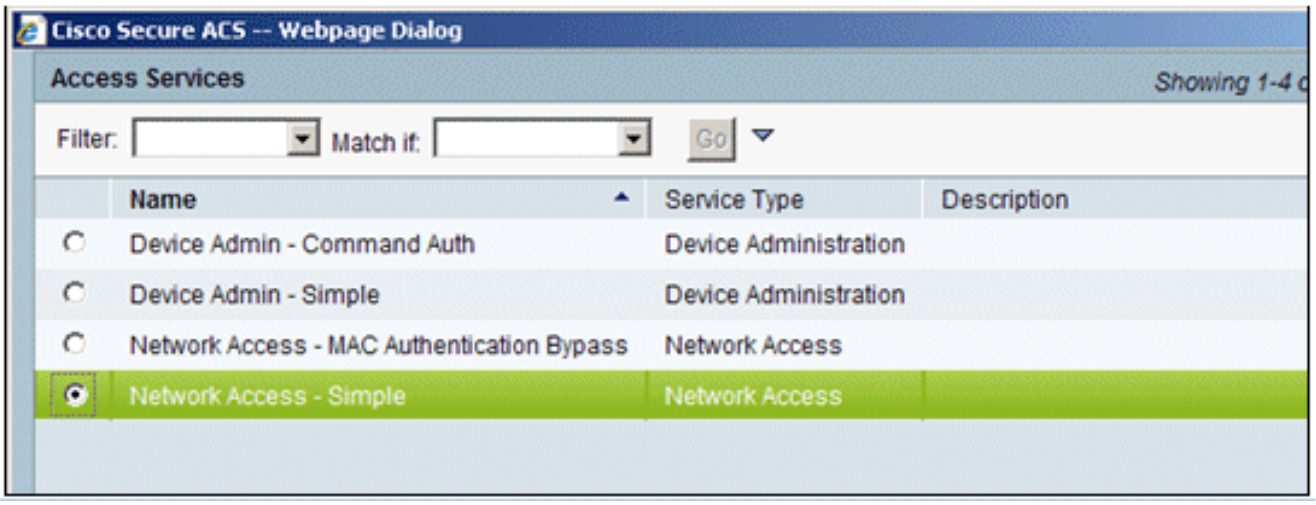
Criar.

3. Crie um serviço de acesso e insira um nome (por exemplo, WirelessAD). Escolha **Baseado**

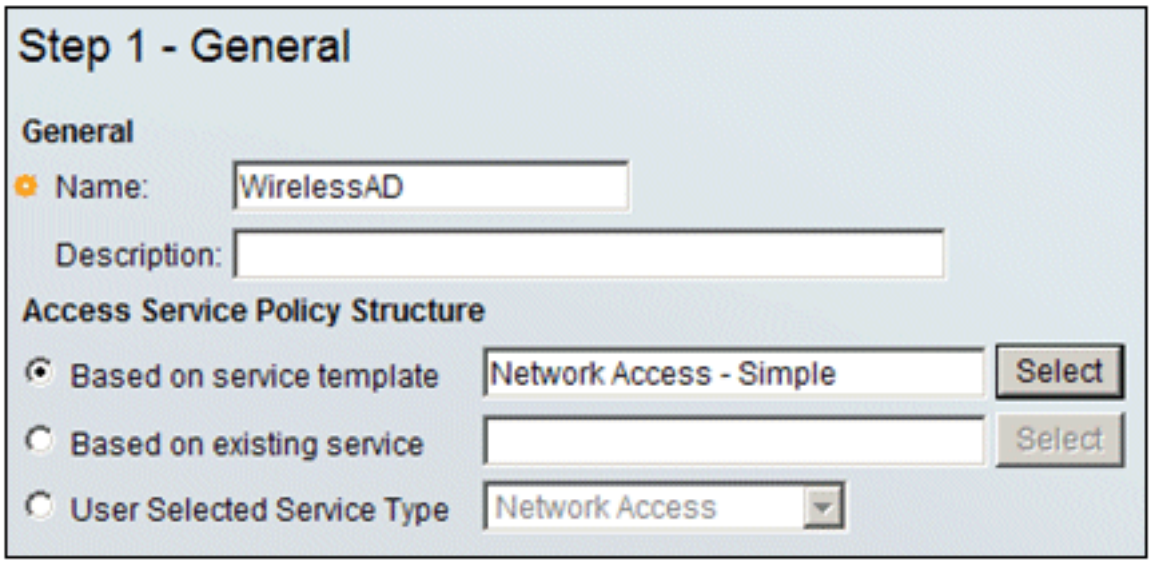
no modelo de serviço e clique em **Selecionar**.



4. Na caixa de diálogo da página da Web, escolha **Acesso à rede - Simples**. Click **OK**.

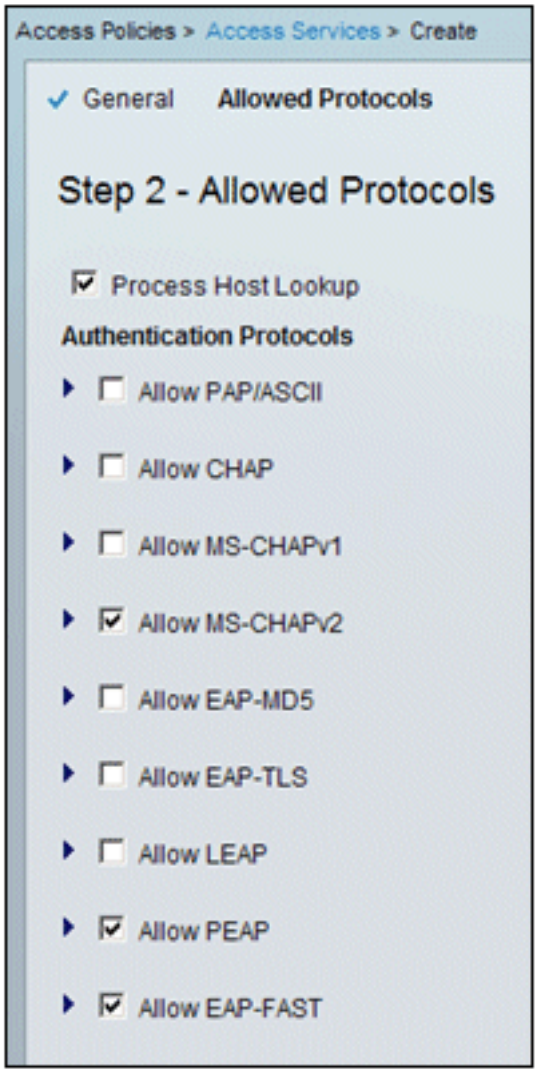


5. Na caixa de diálogo da página da Web, escolha **Acesso à rede - Simples**. Click **OK**. Depois que o modelo for selecionado, clique em

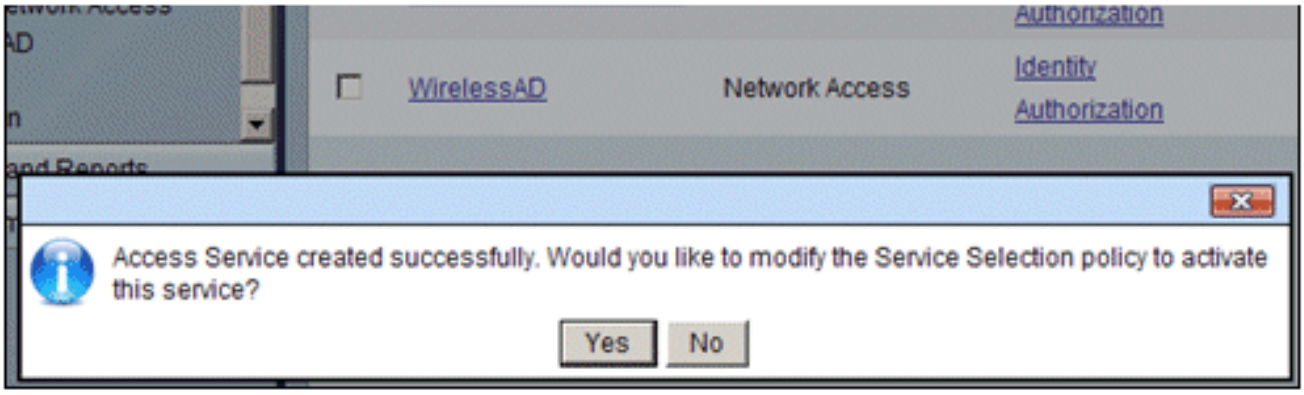


Avançar.

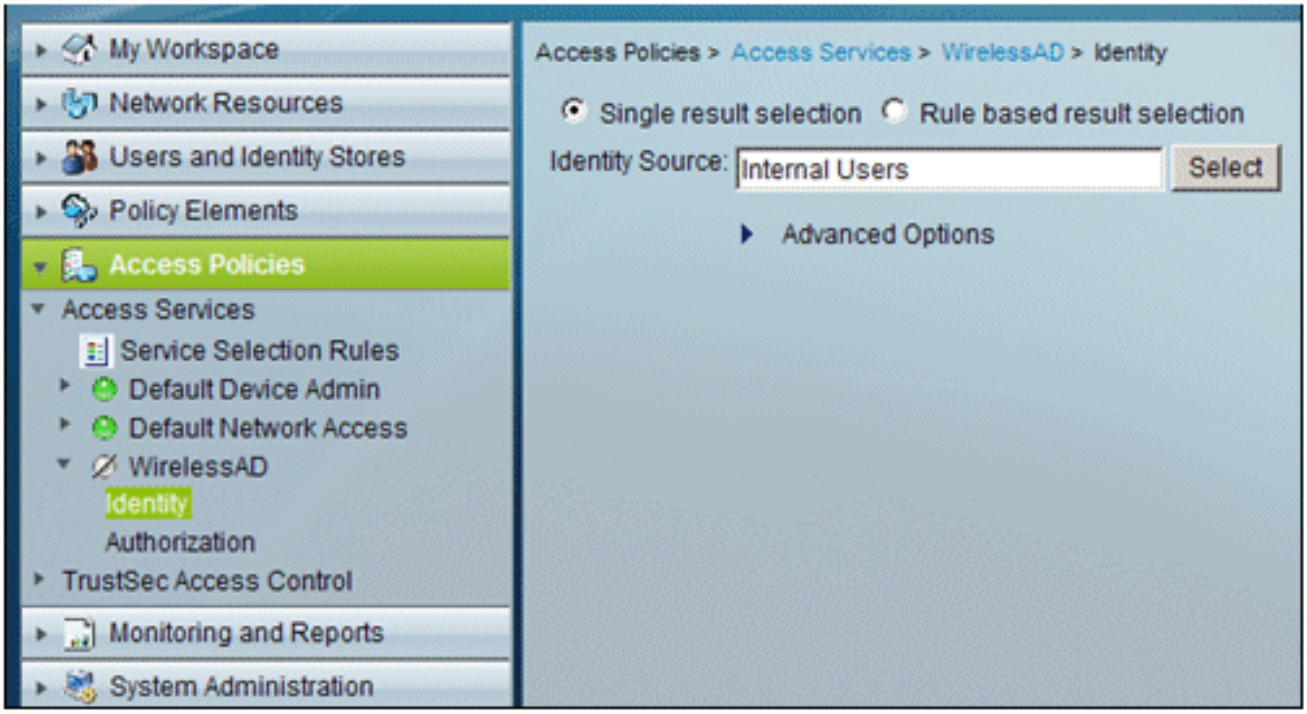
6. Em Allowed Protocols, marque as caixas **Allow MS-CHAPv2** e **Allow PEAP**. Clique em Finish.



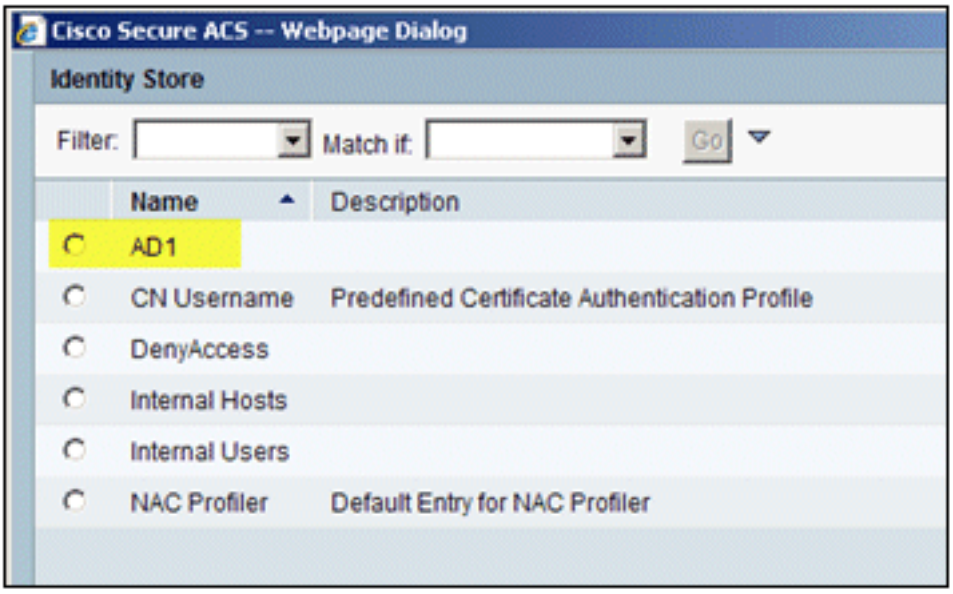
7. Quando o ACS solicitar que você ative o novo serviço, clique em **Sim**.



8. No novo serviço de acesso que acabou de ser criado/ativado, expanda e escolha **Identidade**. Para a Origem da identidade, clique em **Selecionar**.

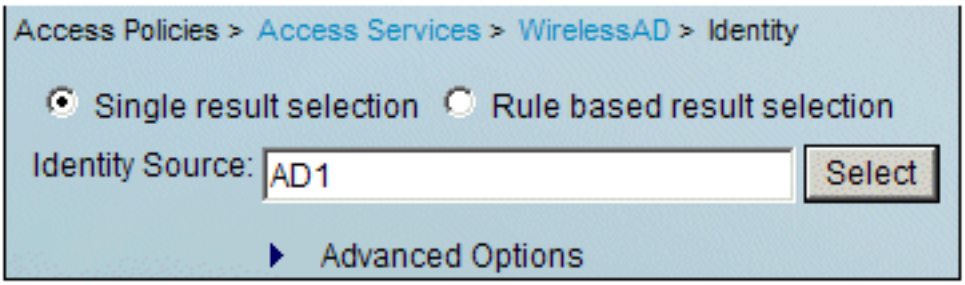


9. Escolha **AD1** para o Ative Diretory que foi configurado no ACS e clique em **OK**.



10. Confirme se a fonte de identidade é AD1 e clique em **Save**

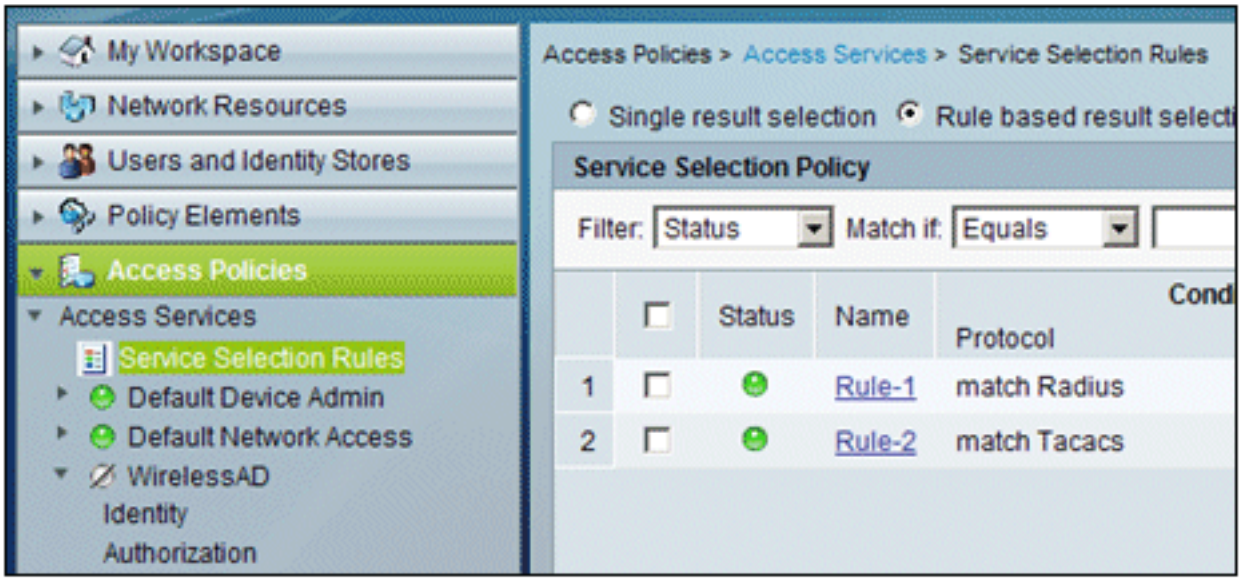
Changes.



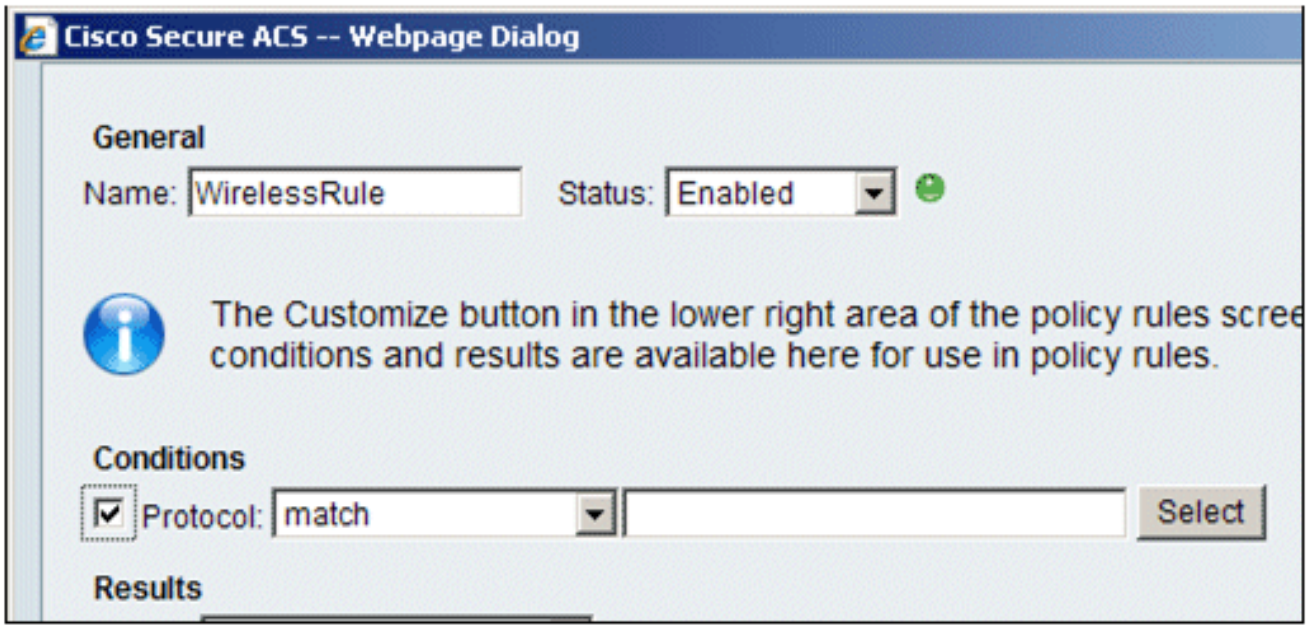
Criar política de acesso e regra de serviço ACS

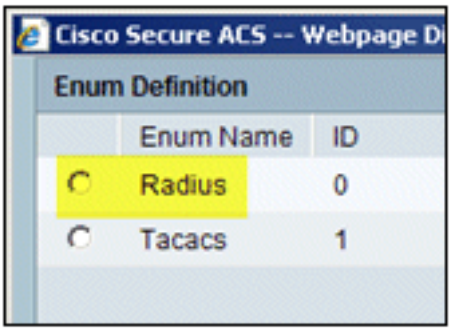
Execute estas etapas:

1. Vá para **Access Policies > Service Selection Rules**.

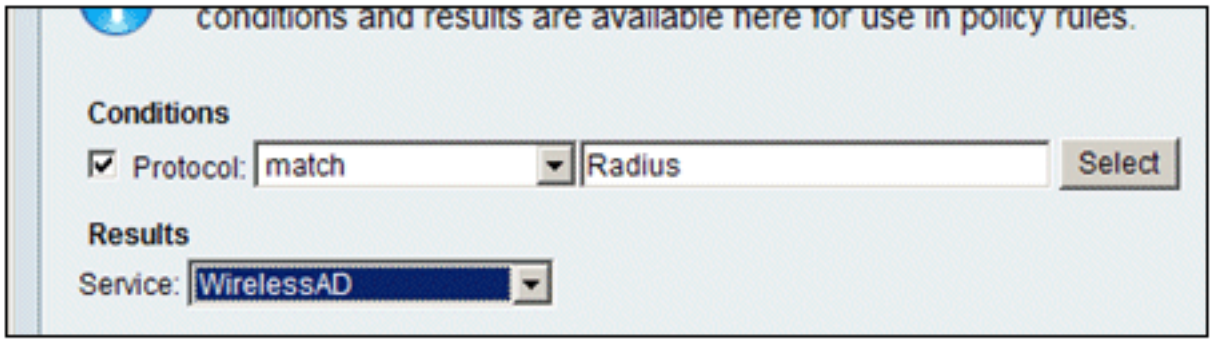


2. Clique em **Criar** na janela Política de seleção de serviço. Dê um nome à nova regra (por exemplo, *WirelessRule*). Marque a caixa de seleção para **Protocol** para corresponder a **Radius**.

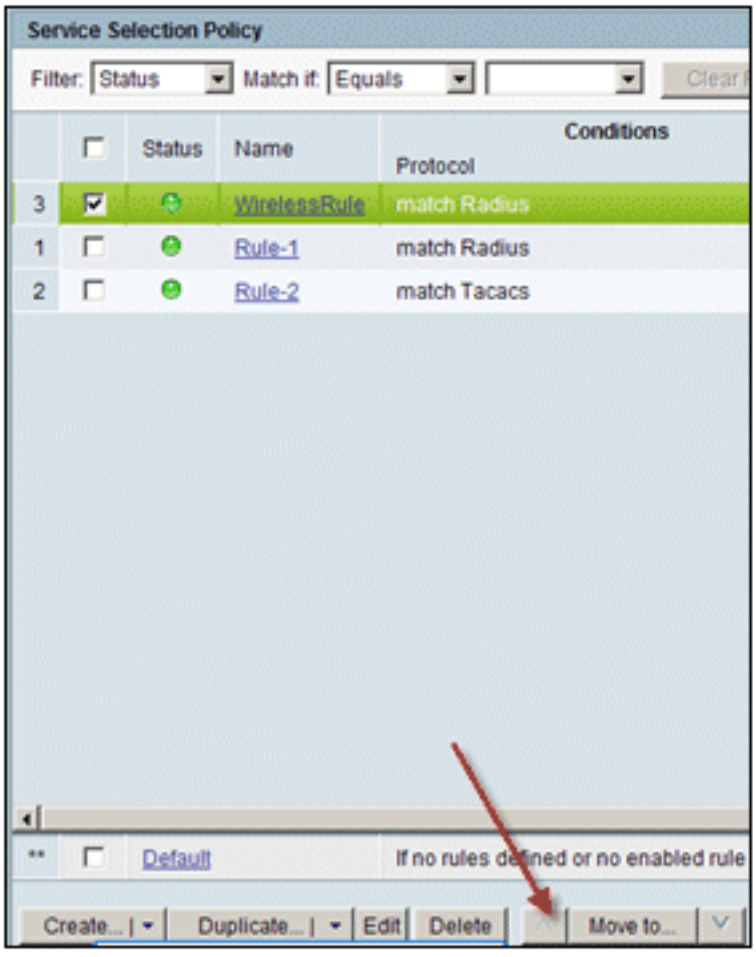




3. Selecione **Radius** e clique em **OK**.
4. Em Resultados, escolha **WirelessAD** para Serviço (criado na etapa anterior).



5. Quando a nova regra sem fio for criada, escolha e **Mova** essa regra para o topo, que será a primeira regra a identificar a autenticação radius sem fio usando o Ative Diretory.



Configuração do CLIENTE para PEAP usando Windows Zero Touch

Em nosso exemplo, CLIENT é um computador que executa o Windows XP Professional com SP que atua como um cliente sem fio e obtém acesso aos recursos da Intranet por meio do AP sem fio. Conclua os procedimentos desta seção para configurar o CLIENT como um cliente sem fio.

Executar uma Instalação e Configuração Básicas

Execute estas etapas:

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

Instale o adaptador de rede wireless

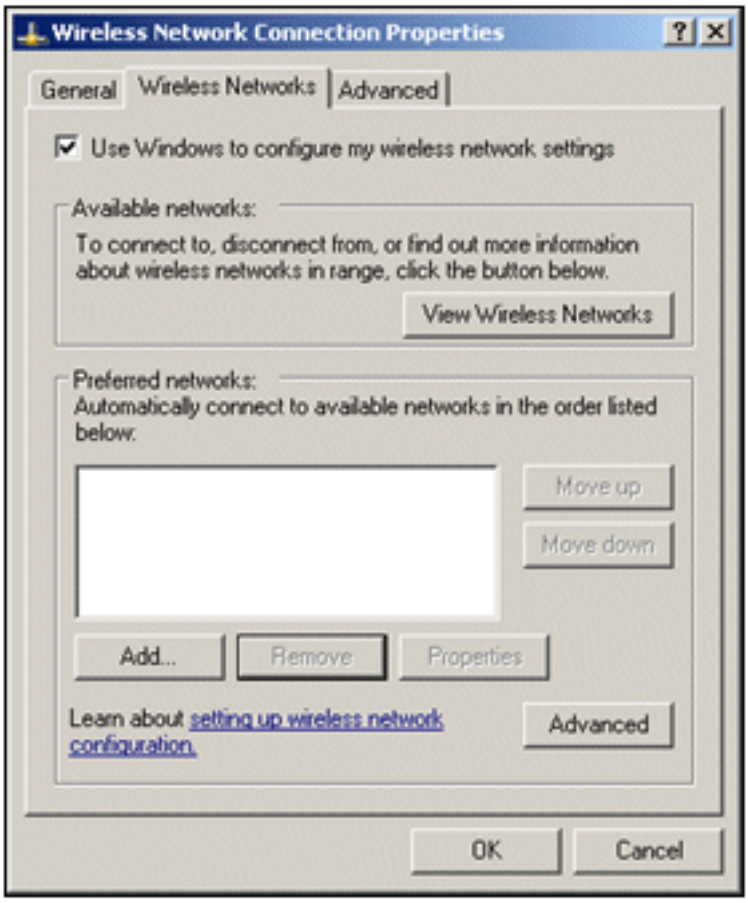
Execute estas etapas:

1. Desligue o computador CLIENTE.
2. Desconecte o computador CLIENTE do segmento de rede da Intranet.
3. Reinicie o computador CLIENTE e faça logon usando a conta de administrador local.
4. Instale o adaptador de rede sem fio.**Nota:** Não instale o software de configuração do fabricante para o adaptador sem fio. Instale os drivers do adaptador de rede sem fio usando o Assistente para Adicionar Hardware. Além disso, quando solicitado, forneça o CD fornecido pelo fabricante ou um disco com drivers atualizados para uso com o Windows XP Professional com SP2.

Configurar a conexão de rede sem fio

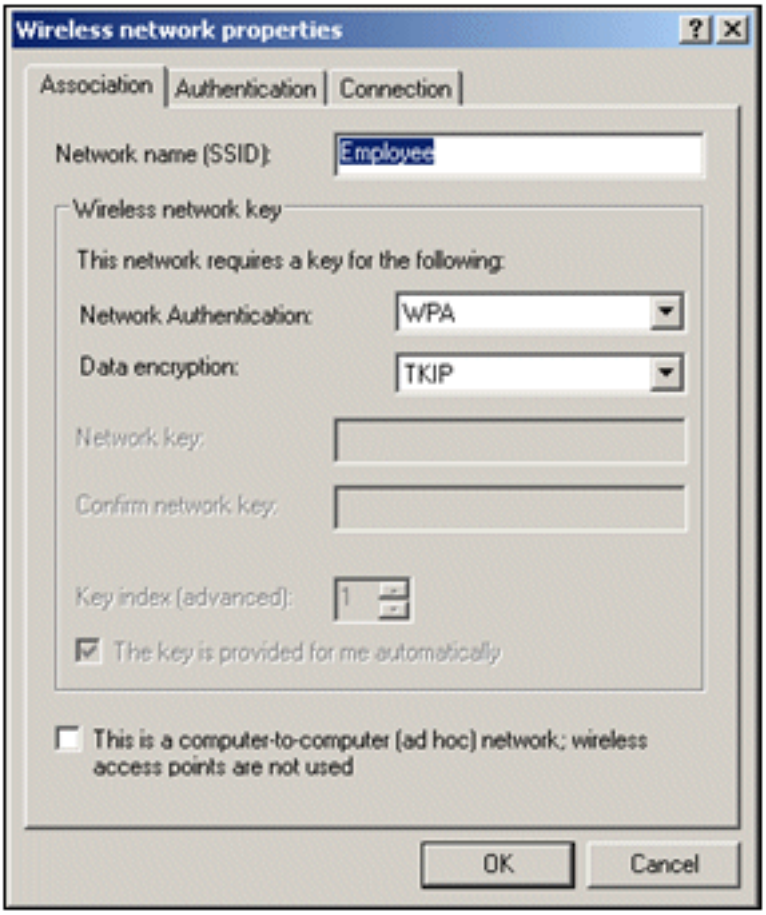
Execute estas etapas:

1. Faça logoff e depois faça logon usando a conta **WirelessUser** no domínio **demo.local**.
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 **Properties**, vá para a guia **Wireless Networks** e verifique se a opção **Use Windows to configure my wireless network settings** está



marcada.

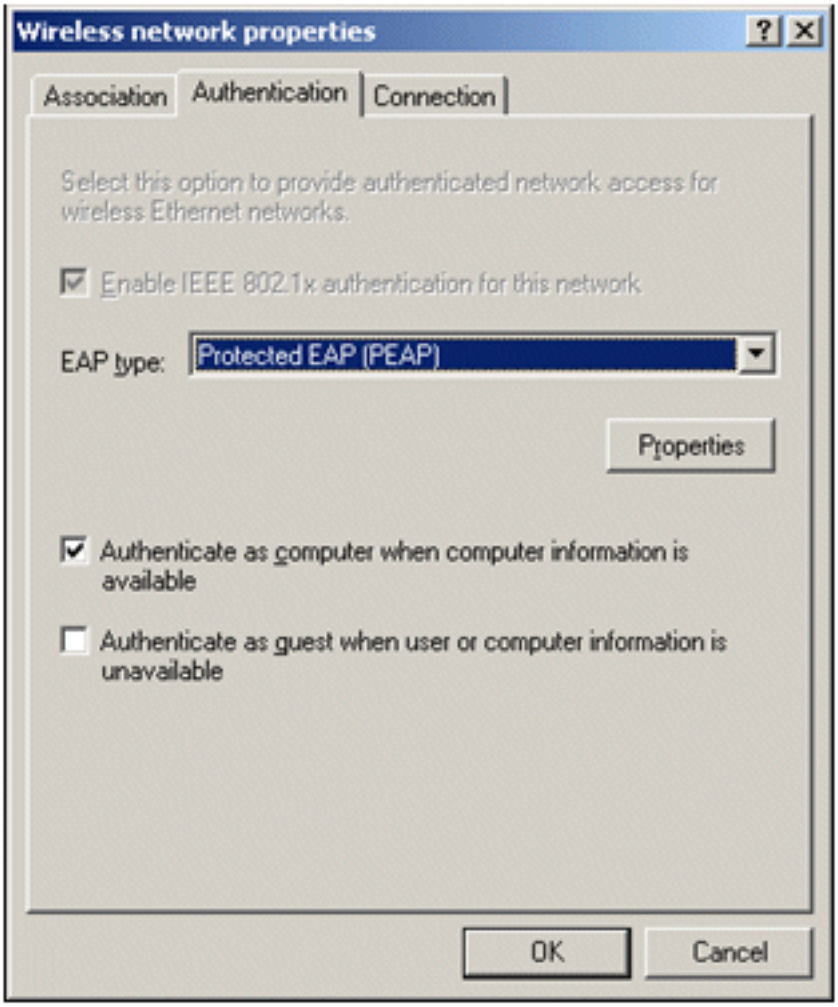
4. Clique em Add.
5. Na guia Associação, insira *Funcionário* no campo Nome da rede (SSID).
6. Escolha **WPA** para a autenticação de rede e verifique se a criptografia de dados está



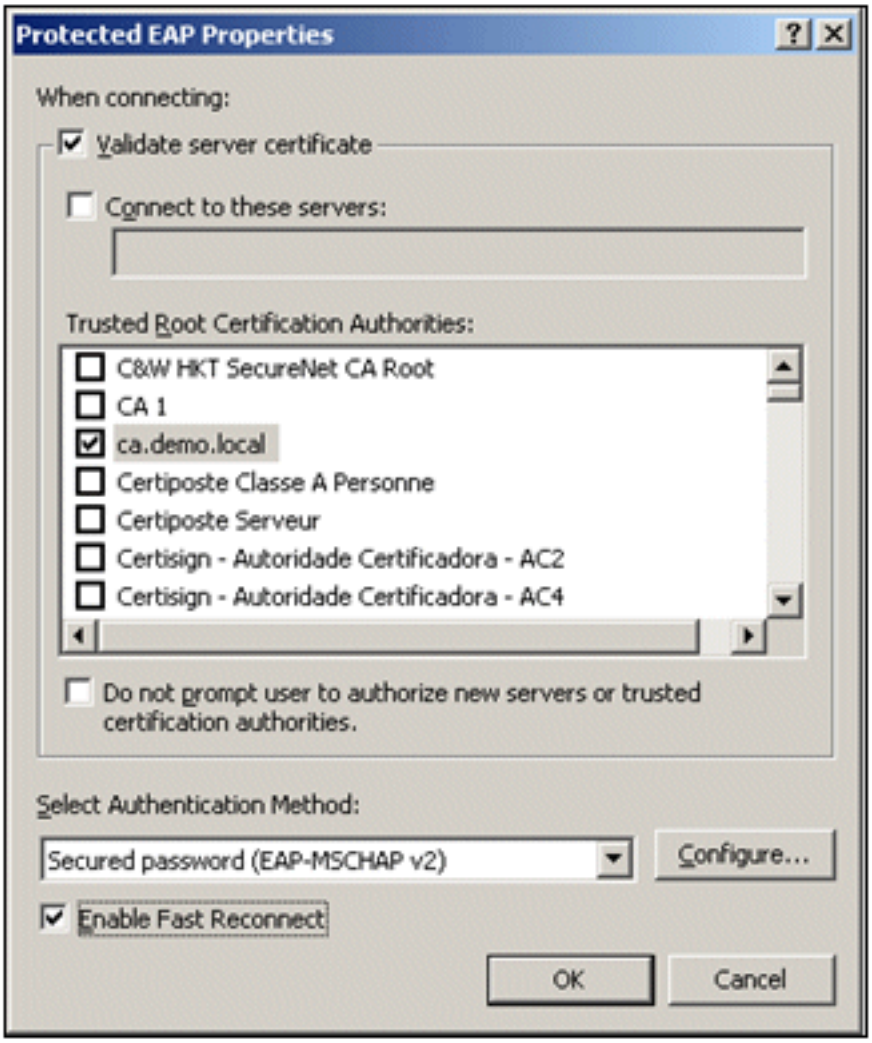
definida como **TKIP**.

7. Clique na guia **Authentication**.

8. Valide se o tipo de EAP está configurado para usar **EAP Protegido (PEAP)**. Se não estiver, escolha-o no menu suspenso.
9. Se desejar que a máquina seja autenticada antes do logon (o que permite que scripts de logon ou envios por push de diretiva de grupo sejam aplicados), marque **Autenticar como computador quando as informações do computador estiverem**



disponíveis.
10. Clique em Propriedades.
11. Como o PEAP envolve a autenticação do servidor pelo cliente, verifique se a opção **Validar certificado do servidor** está marcada. Além disso, verifique se a CA que emitiu o certificado ACS está marcada no menu Trusted Root Certification Authorities.
12. Escolha **Secured password (EAP-MSCHAP v2)** em Authentication Method, pois ela é usada para autenticação



interna.

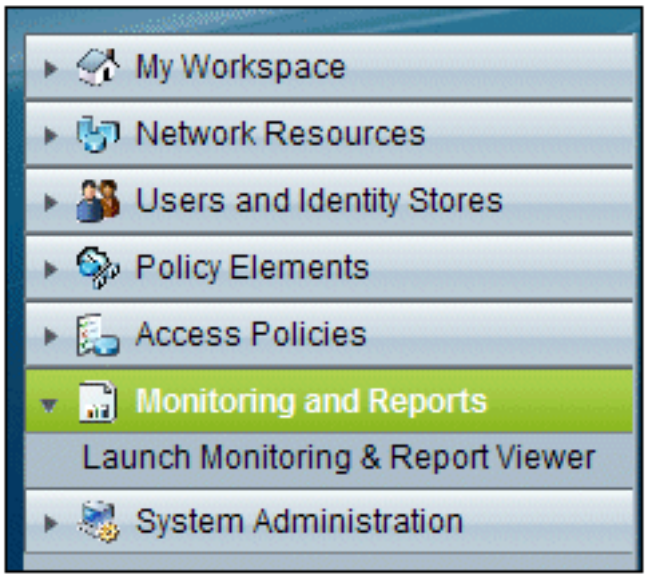
13. Certifique-se de que a caixa de seleção **Enable Fast Reconnect** esteja marcada. Em seguida, clique em **OK** três vezes.
14. Clique com o botão direito do mouse no ícone de conexão de rede sem fio na bandeja do sistema e clique em **Exibir redes sem fio disponíveis**.
15. Clique na rede sem fio Employee e, em seguida, clique em **Connect**. O cliente sem fio mostrará **Connected** se a conexão for bem-sucedida.

16. 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 endereço de 10.0.20.100-10.0.20.200 do escopo do DHCP ou do escopo criado para os clientes sem fio CorpNet.
17. Para testar a funcionalidade, abra um navegador e vá até **http://10.0.10.10** (ou o endereço IP do servidor CA).

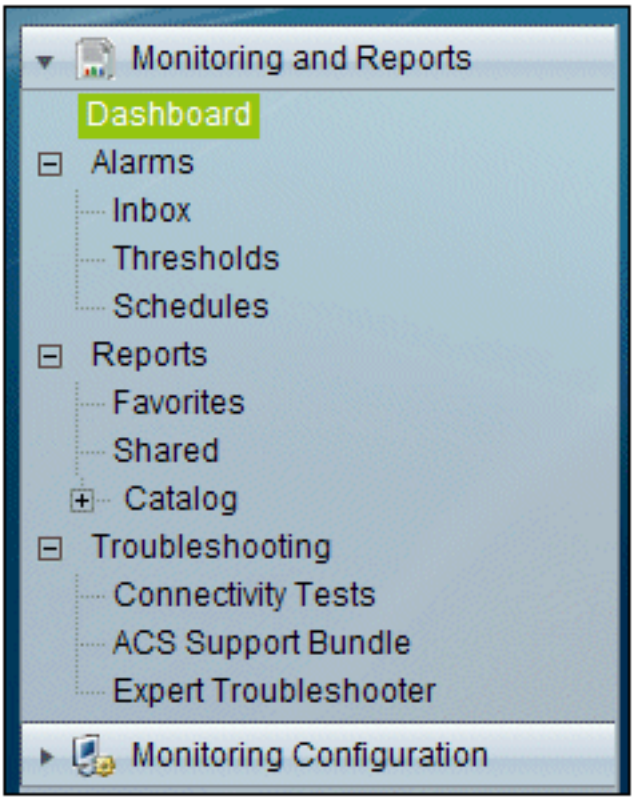
Solucionar problemas de autenticação sem fio com ACS

Execute estas etapas:

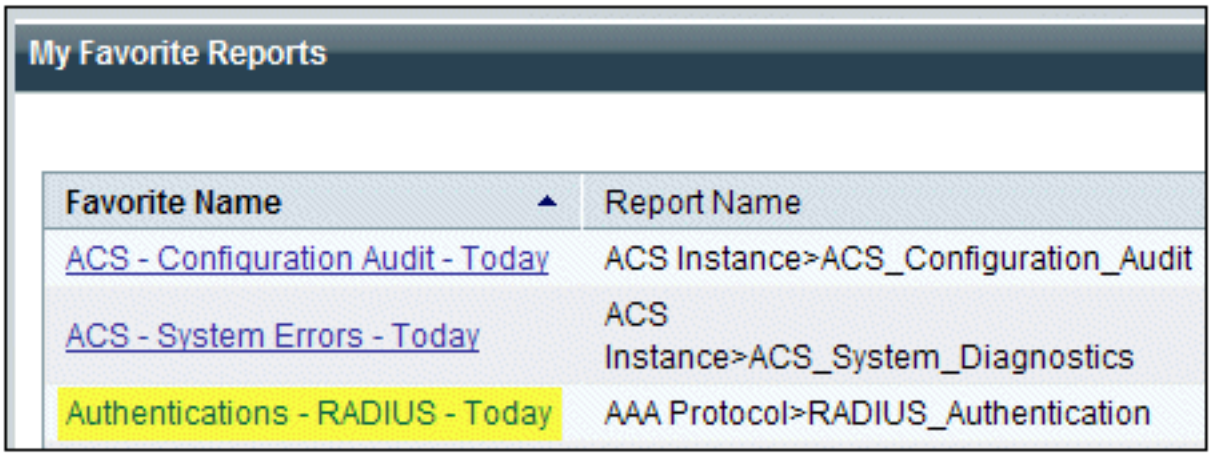
1. Vá para **ACS > Monitoramento e relatórios** e clique em **Iniciar o Monitoramento e o Visualizador de relatórios**.



2. Uma janela ACS separada será aberta. Clique em **Painel**.



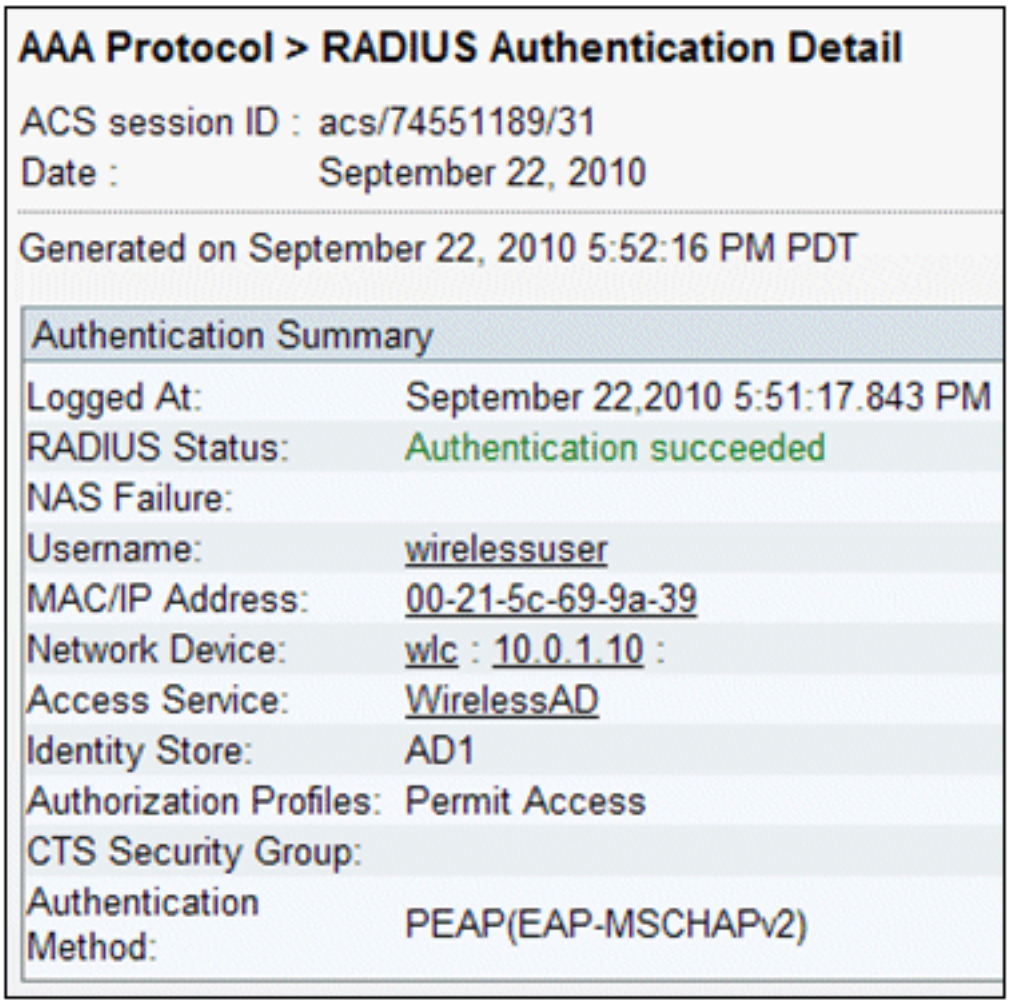
3. Na seção Meus relatórios favoritos, clique em **Autenticações - RADIUS -**



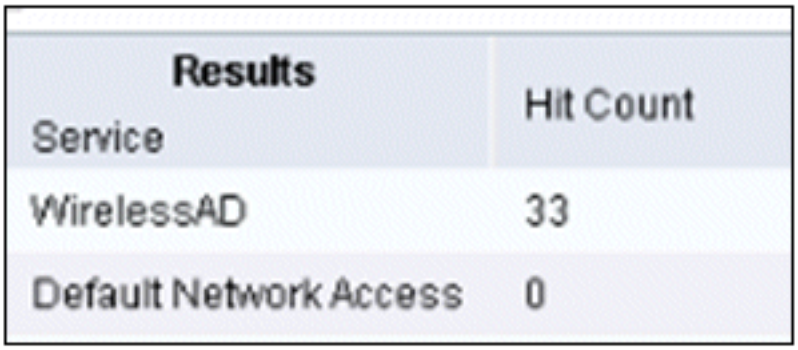
Hoje.

4. Um log mostrará todas as autenticações RADIUS como Pass ou Fail. Em uma entrada registrada, clique no **ícone de lupa** na coluna Detalhes.

5. O RADIUS Authentication Detail fornecerá muitas informações sobre as tentativas registradas.



6. A contagem de ocorrências do serviço ACS pode fornecer uma visão geral das tentativas que correspondem às regras criadas no ACS. Vá para **ACS > Access Policies > Access Services** e clique em **Service Selection Rules**.



Results Service	Hit Count
WirelessAD	33
Default Network Access	0

A autenticação PEAP falha com o servidor ACS

Quando o cliente falhar na autenticação PEAP com um servidor ACS, verifique se você encontrou a mensagem de erro `NAS dupliated authentication attempts` na opção **Failed attempts** no menu **Report and Activity** do ACS.

Você poderá receber esta mensagem de erro quando o Microsoft Windows XP SP2 estiver instalado no computador cliente e o Windows XP SP2 for autenticado em um servidor de terceiros que não seja o Microsoft IAS. Em particular, o servidor Cisco RADIUS (ACS) usa um método diferente para calcular a ID do tipo de protocolo de autenticação extensível:comprimento:valor (EAP-TLV) do que o método usado pelo Windows XP. A Microsoft identificou isso como um defeito no suplicante do XP SP2.

Para obter uma Correção, entre em contato com a Microsoft e consulte o artigo PEAP authentication is not successful when you connect to a third-party RADIUS server . O problema subjacente é que, no lado do cliente, com o utilitário Windows, a opção de reconexão rápida está desativada para PEAP por padrão. No entanto, essa opção é habilitada por padrão no lado do servidor (ACS). Para resolver esse problema, desmarque a opção Reconexão rápida no servidor ACS (em Opções globais do sistema). Como alternativa, você pode habilitar a opção Reconexão rápida no lado do cliente para resolver o problema.

Execute estas etapas para habilitar a reconexão rápida no cliente que executa o Windows XP usando o utilitário Windows:

1. Vá para **Iniciar > Configurações > Painel de controle**.
2. Clique duas vezes no ícone **Conexões de rede**.
3. Clique com o botão direito do mouse no ícone **Conexão de rede sem fio** e clique em **Propriedades**.
4. Clique na guia **Redes sem fio**.
5. Escolha a opção **Usar o Windows para definir as configurações da minha rede sem fio** para permitir que o Windows configure o adaptador cliente.
6. Se você já tiver configurado um SSID, escolha o SSID e clique em **Propriedades**. Caso contrário, clique em **New** para adicionar uma nova WLAN.
7. Insira o SSID na guia Association (Associação). Verifique se a Autenticação de rede está **aberta** e se a Criptografia de dados está definida como **WEP**.
8. Clique em **Authentication**.
9. Escolha a opção **Enable IEEE 802.1x authentication for this network**.

10. Escolha **PEAP** como o Tipo de EAP e clique em **Propriedades**.
11. Escolha a opção **Enable Fast Reconnect** na parte inferior da página.

Informações Relacionadas

- PEAP em redes sem fio unificadas com ACS 4.0 e Windows 2003
- Exemplo de Configuração da Controladora Cisco Wireless LAN (WLC) e Cisco ACS 5.x (TACACS+) para Autenticação da Web
- Guia de Instalação e Atualização do Cisco Secure Access Control System 5.1
- 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.