

# PEAP sob redes sem fio unificadas com o Internet Authentication Service da Microsoft (IAS)

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Conventions](#)

[Visão geral do PEAP](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Configurar o Microsoft Windows 2003 Server](#)

[Configurar o Microsoft Windows 2003 Server](#)

[Instalar e configurar os serviços DHCP no Microsoft Windows 2003 Server](#)

[Instalar e Configurar o Microsoft Windows 2003 Server como um Servidor de Autoridade de Certificação \(CA\)](#)

[Conectar clientes ao domínio](#)

[Instale o Internet Authentication Service no Microsoft Windows 2003 Server e Solicite um Certificado](#)

[Configurar o serviço de autenticação da Internet para a autenticação PEAP-MS-CHAP v2](#)

[Adicionar usuários ao Active Directory](#)

[Permitir acesso sem fio aos usuários](#)

[Configurar a controladora Wireless LAN e APs leves](#)

[Configurar a WLC para autenticação RADIUS através do servidor RADIUS MS IAS](#)

[Configurar uma WLAN para os clientes](#)

[Configurar os clientes sem fio](#)

[Configurar os clientes sem fio para a autenticação PEAP-MS CHAPv2](#)

[Verificar e solucionar problemas](#)

[Informações Relacionadas](#)

## Introduction

Este original fornece um exemplo de configuração para configurar o Protected Extensible Authentication Protocol (PEAP) com a autenticação Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) versão 2 em uma rede Cisco Unified Wireless com o Microsoft Internet Authentication Service (IAS) como um servidor RADIUS.

# Prerequisites

## Requirements

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

**Observação:** este documento tem como objetivo dar aos leitores um exemplo da configuração necessária no servidor MS para a autenticação PEAP - MS CHAP. A configuração do servidor Microsoft apresentada nesta seção foi testada no laboratório e descobriu-se que estava funcionando conforme esperado. Se você tiver problemas para configurar o servidor Microsoft, entre em contato com a Microsoft para obter ajuda. O Cisco TAC não suporta a configuração do servidor Microsoft Windows.

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

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.

## Componentes Utilizados

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

- Controlador Cisco 4400 Series com firmware versão 4.0
- AP do protocolo LWAPP (Lightweight Access Point Protocol) do Cisco 1131
- Windows 2003 Enterprise Server (SP1) com serviços de Internet Authentication Service (IAS), Certificate Authority (CA), DHCP e Domain Name System (DNS) instalados
- Windows XP Professional com SP 2 (e Service Packs atualizados) e placa de interface de rede sem fio (NIC) Cisco Aironet 802.11a/b/g
- Aironet Desktop Utility Versão 4.0
- Switch Cisco 3560

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](#).

## Visão geral do PEAP

O PEAP usa o Transport Level Security (TLS) para criar um canal criptografado entre um cliente PEAP de autenticação, como um laptop Wireless, e um autenticador PEAP, como o Microsoft Internet Authentication Service (IAS) ou qualquer servidor RADIUS. O PEAP não especifica um método de autenticação, mas fornece segurança adicional para outros protocolos de autenticação EAP, como EAP-MSCHAPv2, que podem operar através do canal criptografado TLS fornecido pelo PEAP. O processo de autenticação PEAP consiste em duas fases principais:

### **Fase um do PEAP: canal criptografado TLS**

O cliente Wireless se associa ao AP. Uma associação baseada em IEEE 802.11 fornece uma autenticação de Sistema Aberto ou Chave Compartilhada antes de uma associação segura ser criada entre o cliente e o Ponto de Acesso (LAP). Depois que a associação baseada em IEEE 802.11 é estabelecida com êxito entre o cliente e o Ponto de acesso, a sessão TLS é negociada com o AP. Após a conclusão bem-sucedida da autenticação entre o cliente Wireless e o servidor IAS, a sessão TLS é negociada entre eles. A chave derivada nessa negociação é usada para criptografar todas as comunicações subsequentes.

### **Fase dois do PEAP: comunicação autenticada por EAP**

A comunicação EAP, que inclui a negociação EAP, ocorre dentro do canal TLS criado pelo PEAP na primeira etapa do processo de autenticação PEAP. O servidor IAS autentica o cliente Wireless com EAP-MS-CHAP v2. O LAP e a controladora apenas encaminham mensagens entre o cliente Wireless e o servidor RADIUS. A WLC e o LAP não podem descriptografar essas mensagens porque não é o ponto final de TLS.

Depois que ocorre a etapa um do PEAP e o canal TLS é criado entre o servidor IAS e o cliente Wireless 802.1X, para uma tentativa de autenticação bem-sucedida em que o usuário forneceu credenciais válidas baseadas em senha com PEAP-MS-CHAP v2, a sequência de mensagens RADIUS é esta:

1. O servidor IAS envia uma mensagem de solicitação de identidade ao cliente: EAP-Solicitação/Identidade.
2. O cliente responde com uma mensagem de resposta de identidade: EAP-Resposta/Identidade.
3. O servidor IAS envia uma mensagem de desafio MS-CHAP v2: EAP-Request/EAP-Type=EAP MS-CHAP-V2 (Challenge).
4. O cliente responde com um desafio e uma resposta MS-CHAP v2: EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (Response).
5. O servidor IAS envia de volta um pacote de sucesso MS-CHAP v2 quando o servidor autentica com êxito o cliente: EAP-Request/EAP-Type=EAP-MS-CHAP-V2 (Sucesso).
6. O cliente responde com um pacote de sucesso MS-CHAP v2 quando o cliente autentica com êxito o servidor: EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (Êxito).
7. O servidor IAS envia um EAP-TLV que indica uma autenticação bem-sucedida.
8. O cliente responde com uma mensagem de status de êxito EAP-TLV.
9. O servidor conclui a autenticação e envia uma mensagem EAP-Success usando texto simples. Se as VLANs forem implantadas para isolamento do cliente, os atributos da VLAN serão incluídos nesta mensagem.

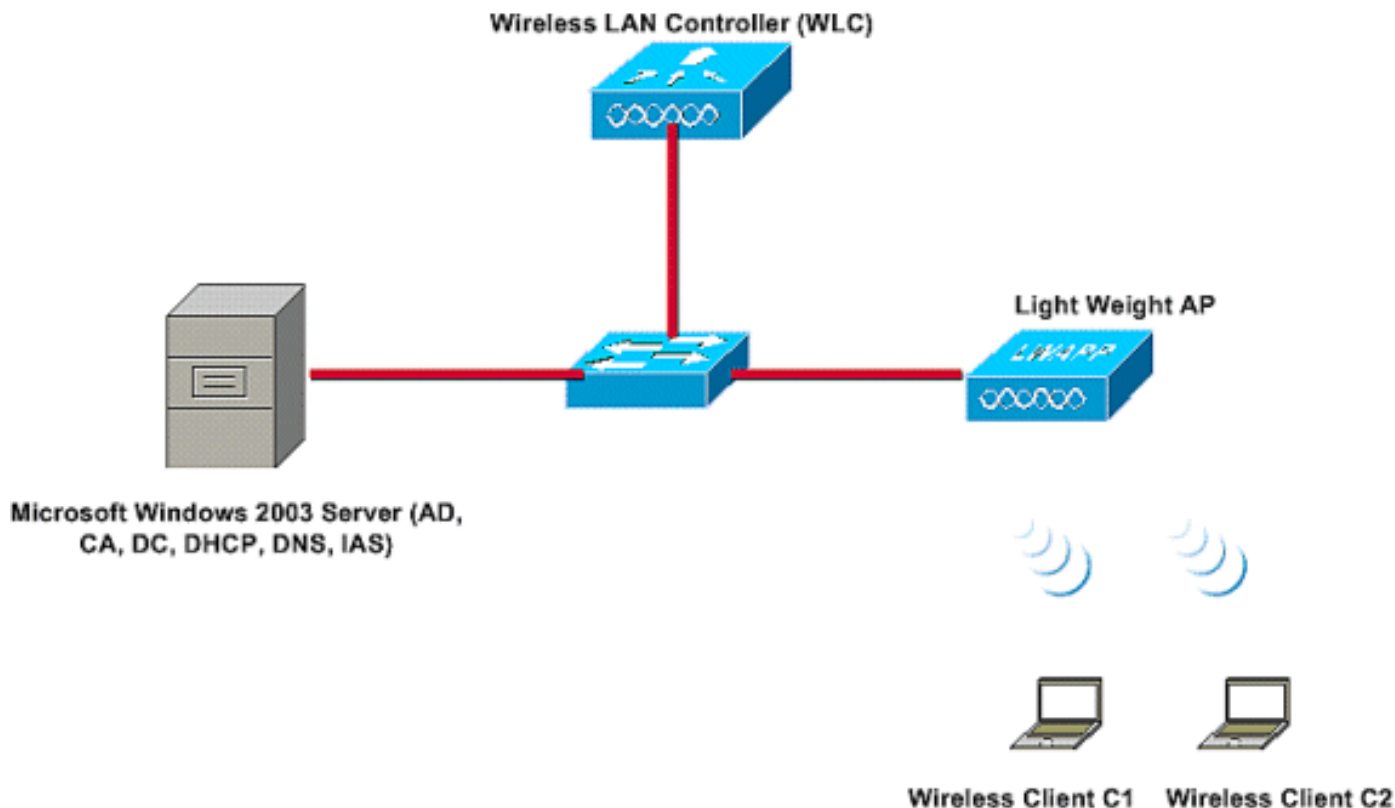
## **Configurar**

Este documento fornece um exemplo para a configuração do PEAP MS-CHAP v2.

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:



Nesta configuração, um servidor Microsoft Windows 2003 executa estas funções:

- Controlador de domínio para o domínio **Wireless.com**
- servidor DHCP/DNS
- Servidor de Autoridade de Certificação (CA)
- Active Directory - para manter o banco de dados do usuário
- Internet Authentication Service (IAS) - para autenticar os usuários sem fio

Esse servidor se conecta à rede com fio por meio de um switch de Camada 2, como mostrado.

A controladora Wireless LAN (WLC) e o LAP registrado também se conectam à rede através do switch de Camada 2.

Os clientes sem fio C1 e C2 usarão a autenticação WPA2 (Wi-Fi Protected Access 2) - PEAP MSCHAP v2 para se conectar à rede sem fio.

O objetivo é configurar o servidor Microsoft 2003, o Wireless LAN Controller e o Light Weight AP para autenticar os clientes Wireless com a autenticação PEAP MSCHAP v2.

A próxima seção explica como configurar os dispositivos para essa configuração.

## Configurações

Esta seção examina a configuração necessária para configurar a Autenticação PEAP MS-CHAP v2 nesta WLAN:

- Configurar o Microsoft Windows 2003 Server
- Configurar a controladora Wireless LAN (WLC) e os APs leves
- Configurar os clientes sem fio

Comece com a configuração do servidor Microsoft Windows 2003.

## Configurar o Microsoft Windows 2003 Server

### Configurar o Microsoft Windows 2003 Server

Como mencionado na seção Configuração de rede, use o servidor Microsoft Windows 2003 na rede para executar essas funções.

- **Controlador de domínio** - para o domínio **Wireless**
- **servidor DHCP/DNS**
- **Servidor de Autoridade de Certificação (CA)**
- **Internet Authentication Service (IAS)** - para autenticar os usuários sem fio
- **Active Directory** - para manter o banco de dados do usuário

Configure o servidor Microsoft Windows 2003 para esses serviços. Comece com a configuração do servidor Microsoft Windows 2003 como um controlador de domínio.

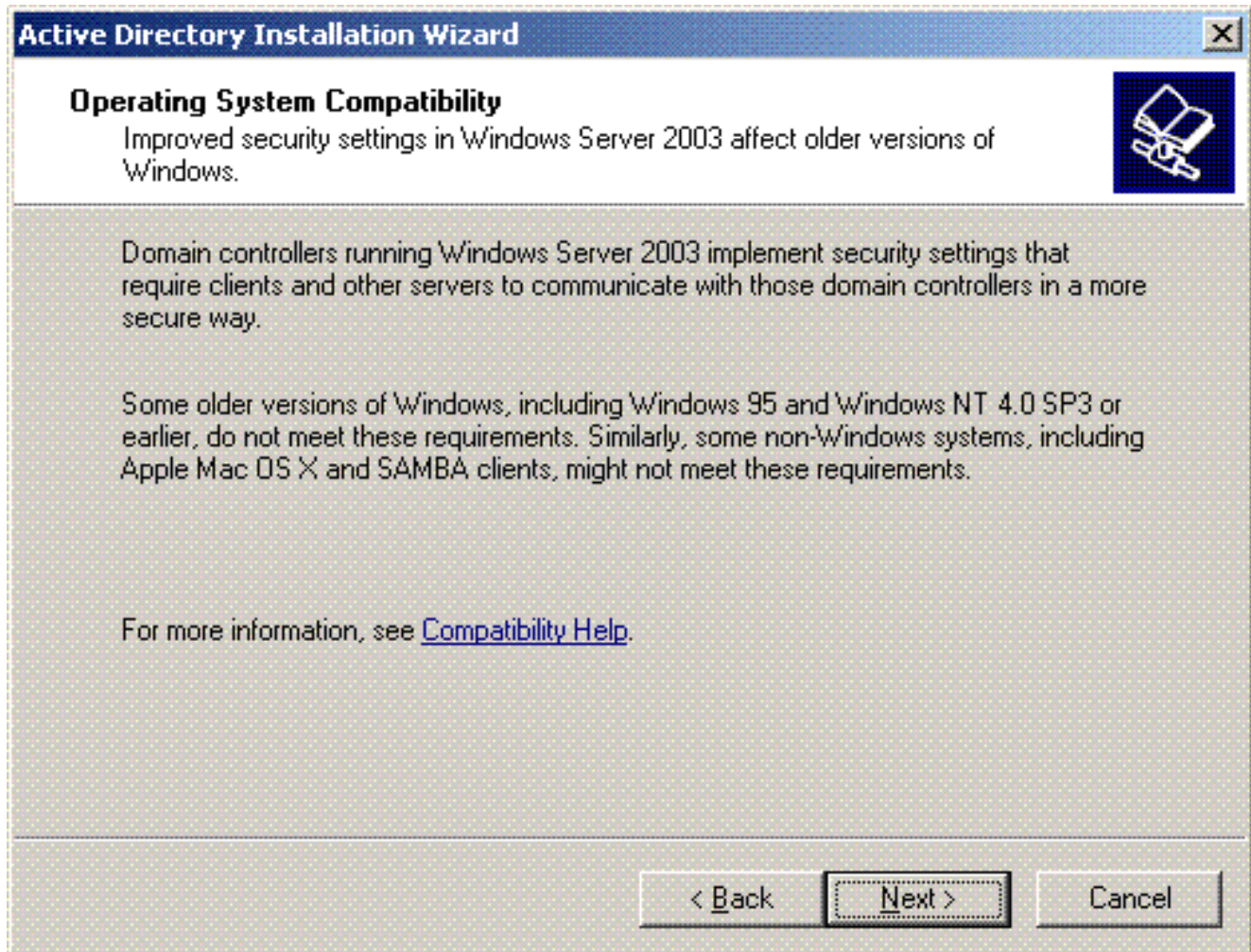
### **Configurar o servidor Microsoft Windows 2003 como um controlador de domínio**

Para configurar o servidor Microsoft Windows 2003 como um controlador de domínio, siga estas etapas:

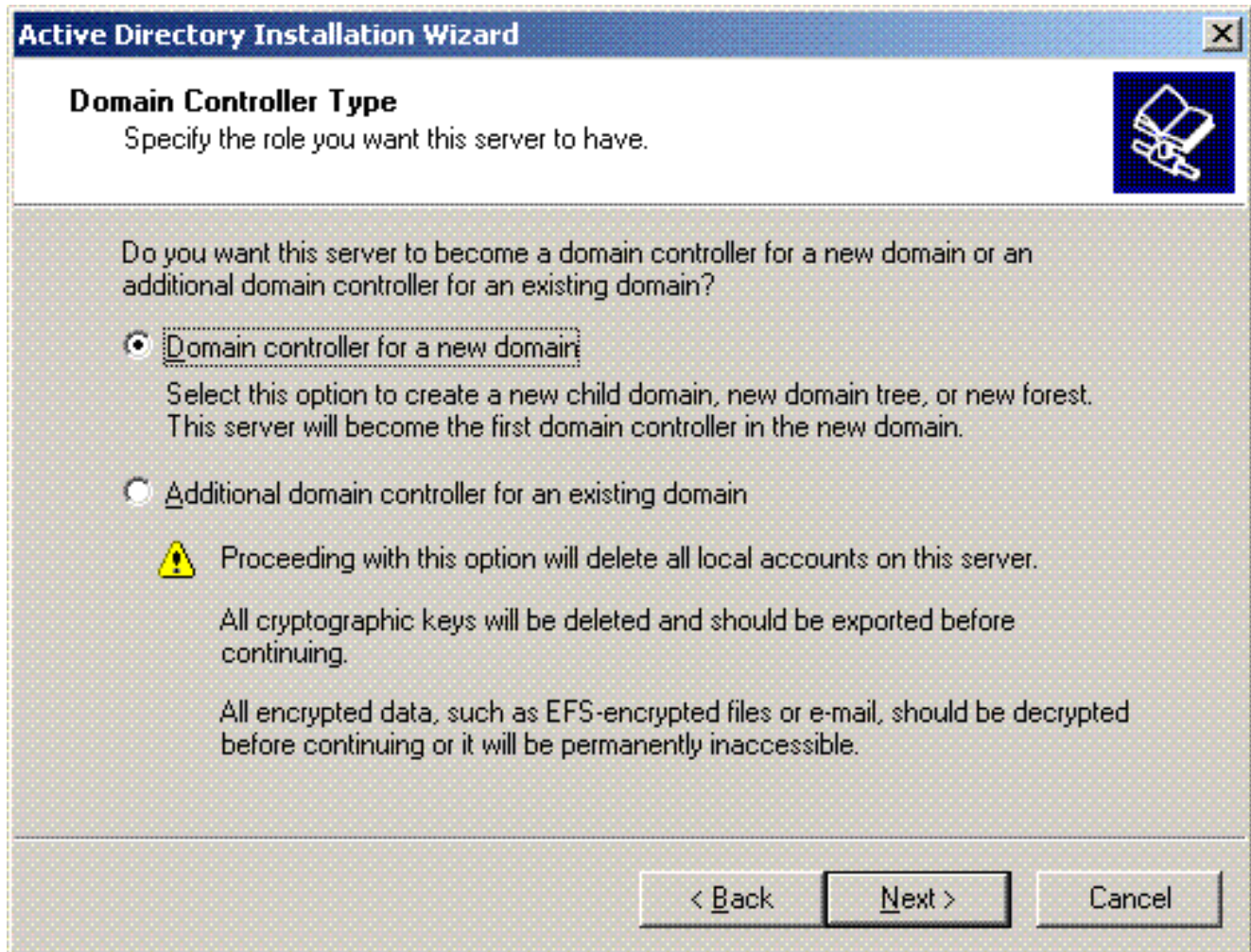
1. Clique em **Iniciar**, clique em **Executar**, digite **dcpromo.exe** e clique em **OK** para iniciar o Assistente de instalação do Active Directory.



2. Clique em **Avançar** para executar o Assistente de Instalação do Active Directory.

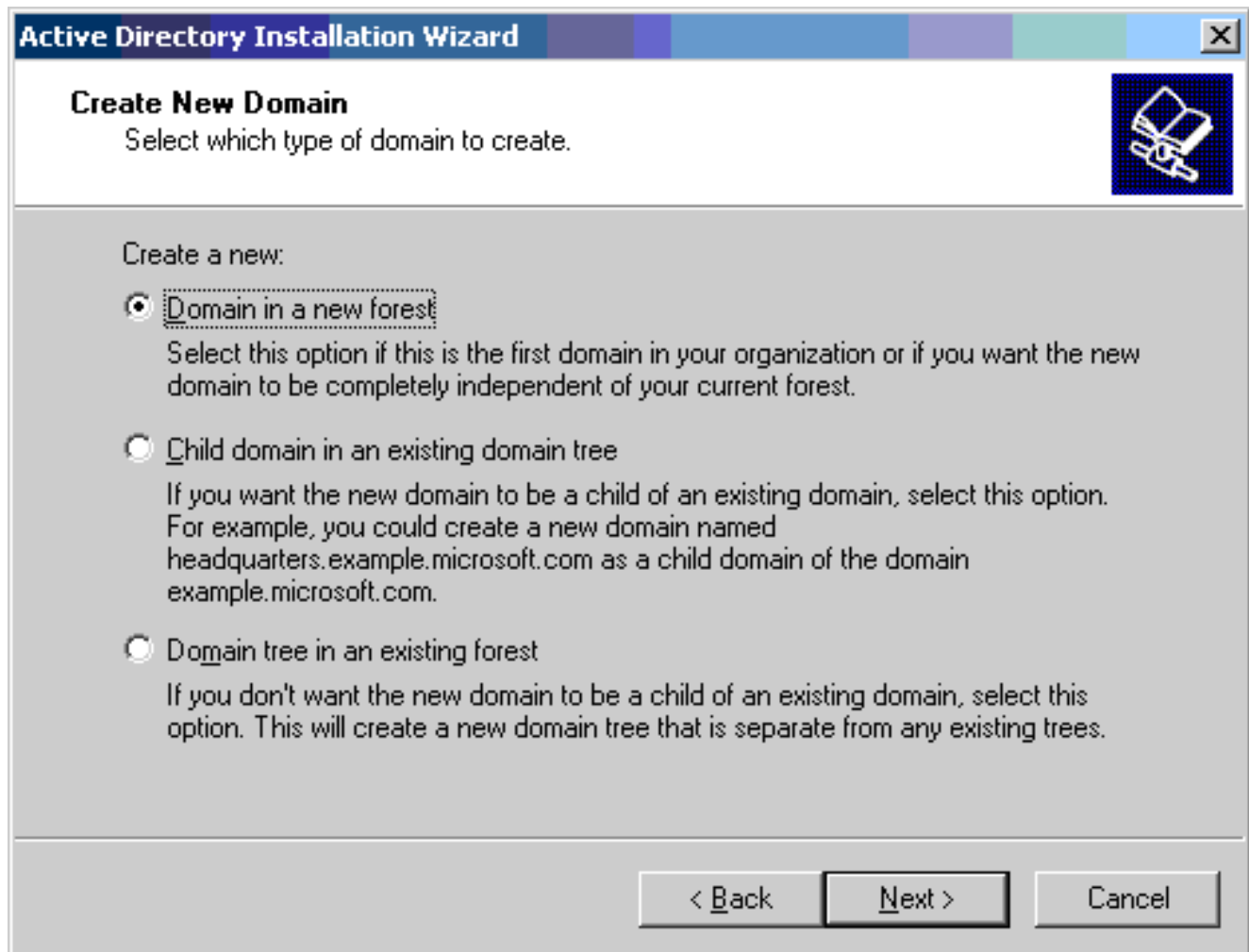


3. Para criar um novo domínio, escolha a opção **Domain Controller** para um novo domínio.

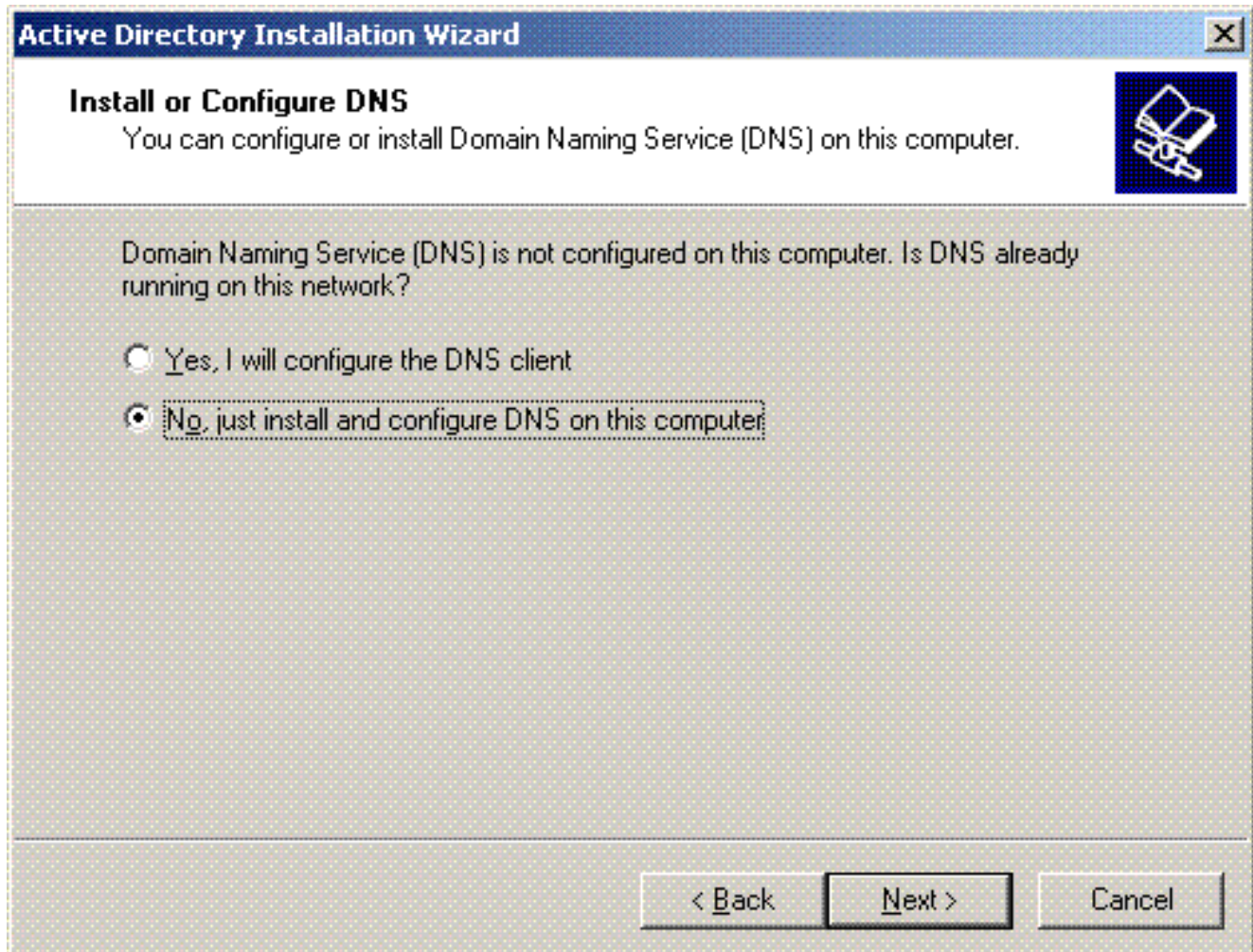


4. Clique em **Avançar** para criar uma nova floresta de árvores de domínio.

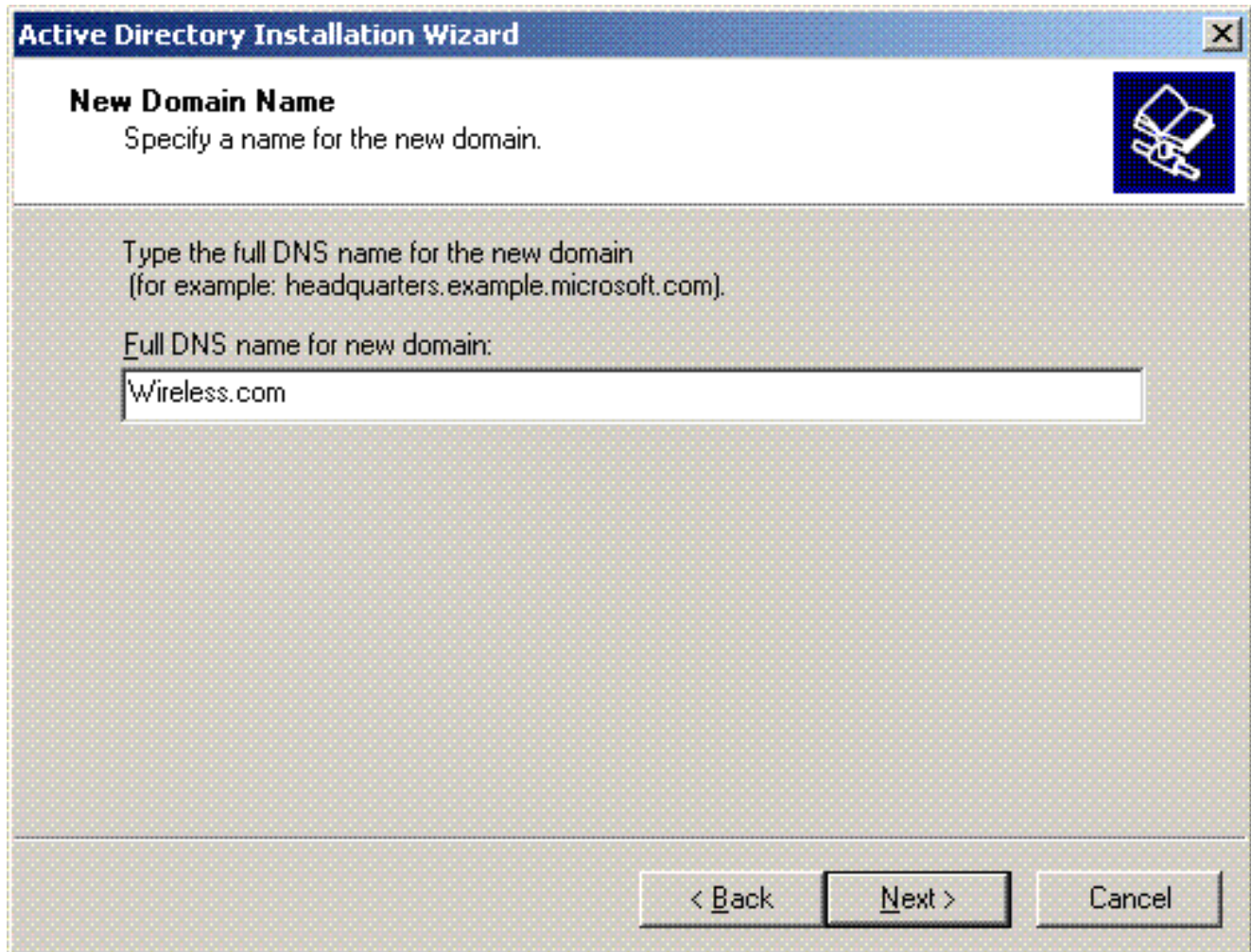




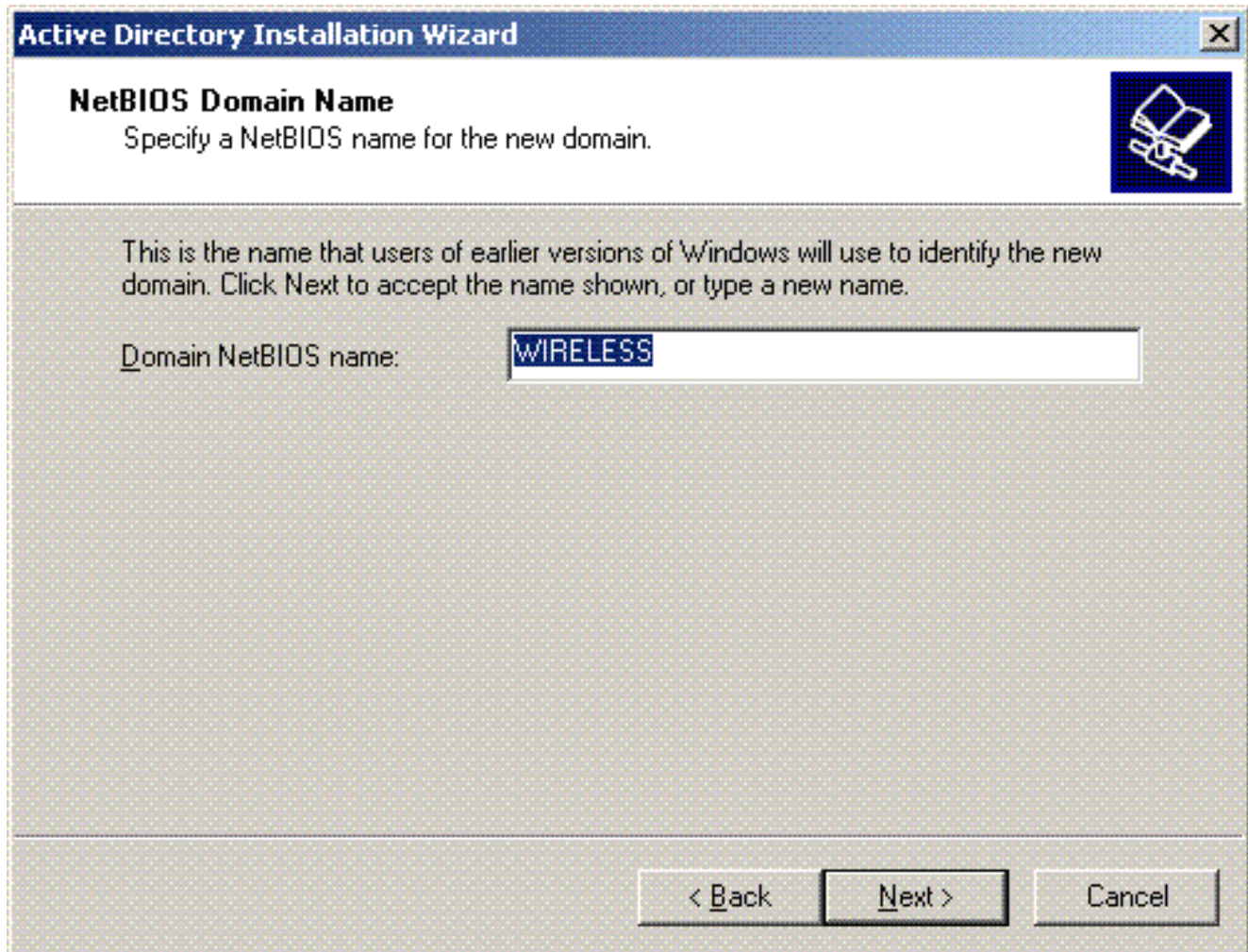
5. Se o DNS não estiver instalado no sistema, o assistente fornecerá opções com as quais configurar o DNS. Escolha **Não, Apenas Instalar e Configurar DNS** neste computador. Clique em Next.



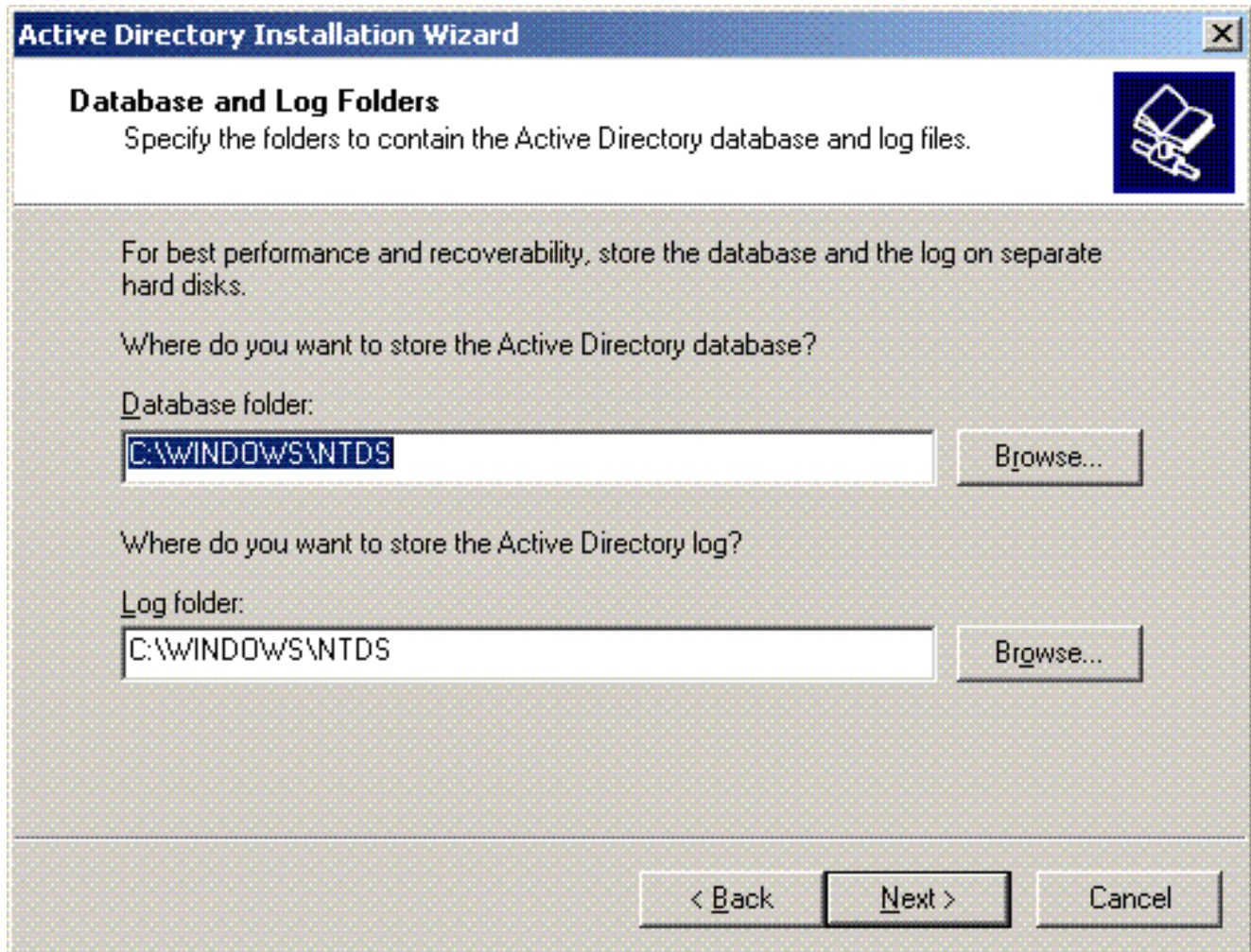
6. Digite o nome DNS completo do novo domínio. Neste exemplo, **Wireless.com** é usado e clique em **Avançar**.



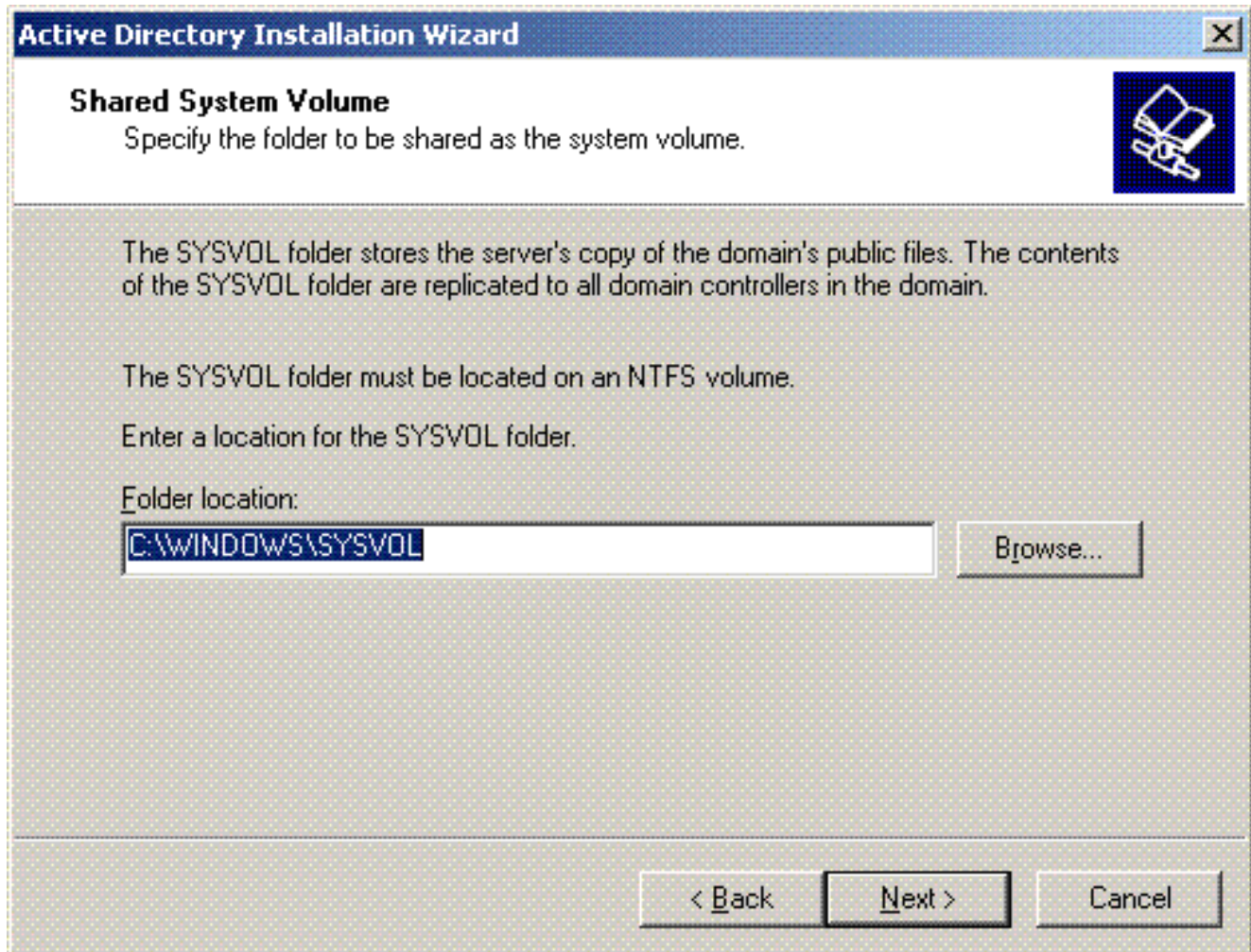
7. Insira o nome NETBIOS para o domínio e clique em **Avançar**. Este exemplo usa **WIRELESS**.



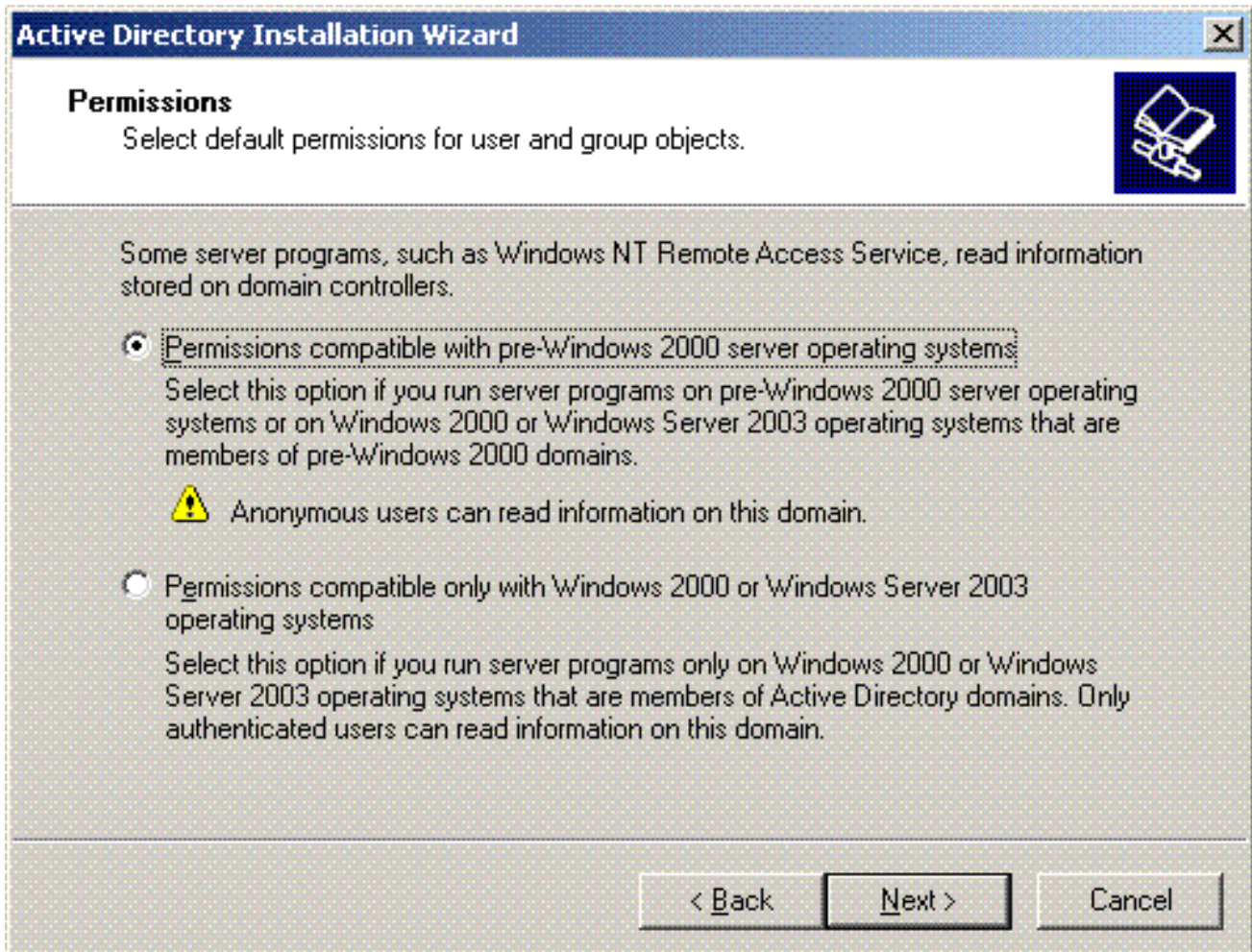
8. Escolha o banco de dados e os locais de log para o domínio. Clique em Next.



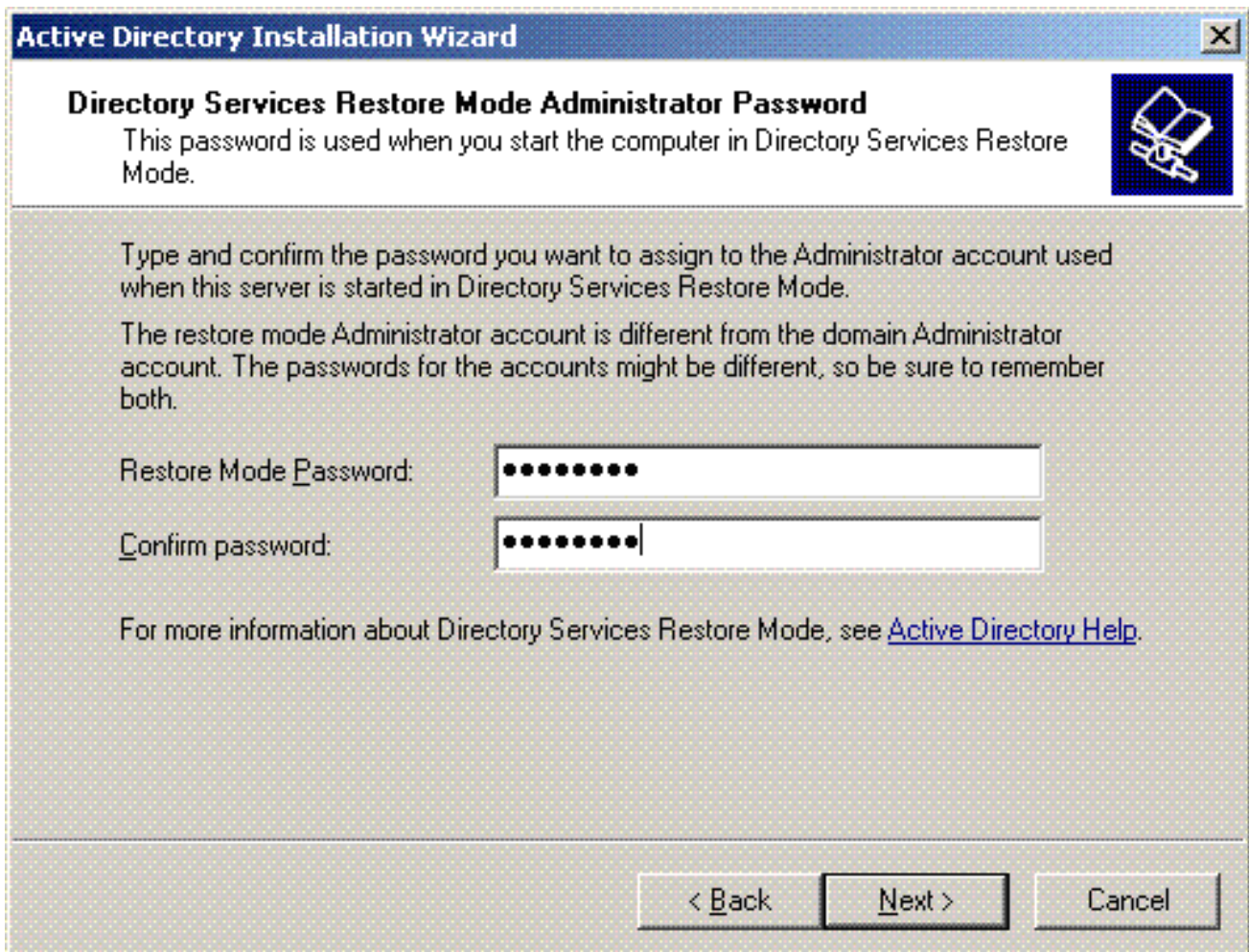
9. Escolha um local para a pasta Sysvol. Clique em Next.



10. Escolha as permissões padrão para os usuários e grupos. Clique em Next.

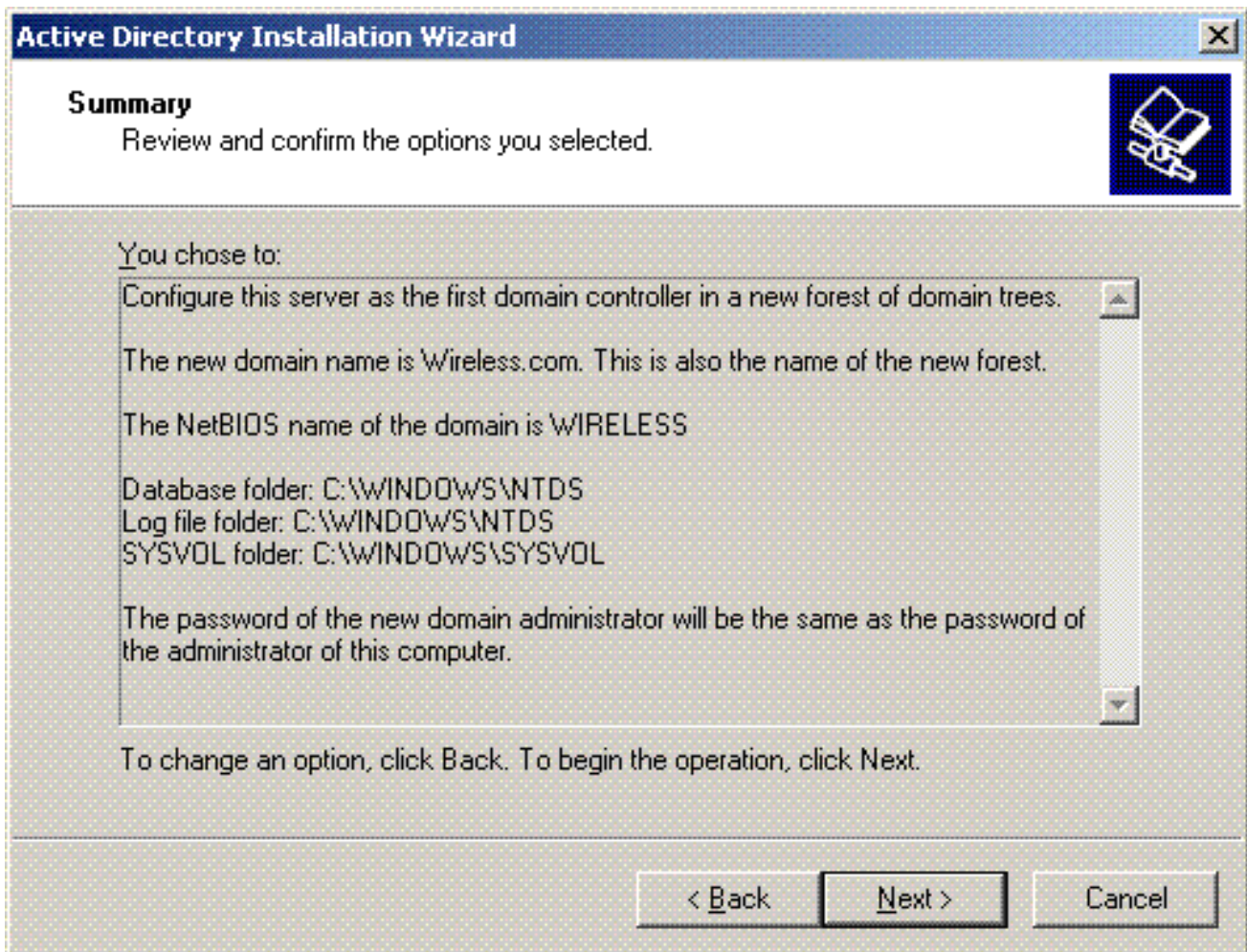


11. Defina a Senha do administrador e clique em **Avançar**.

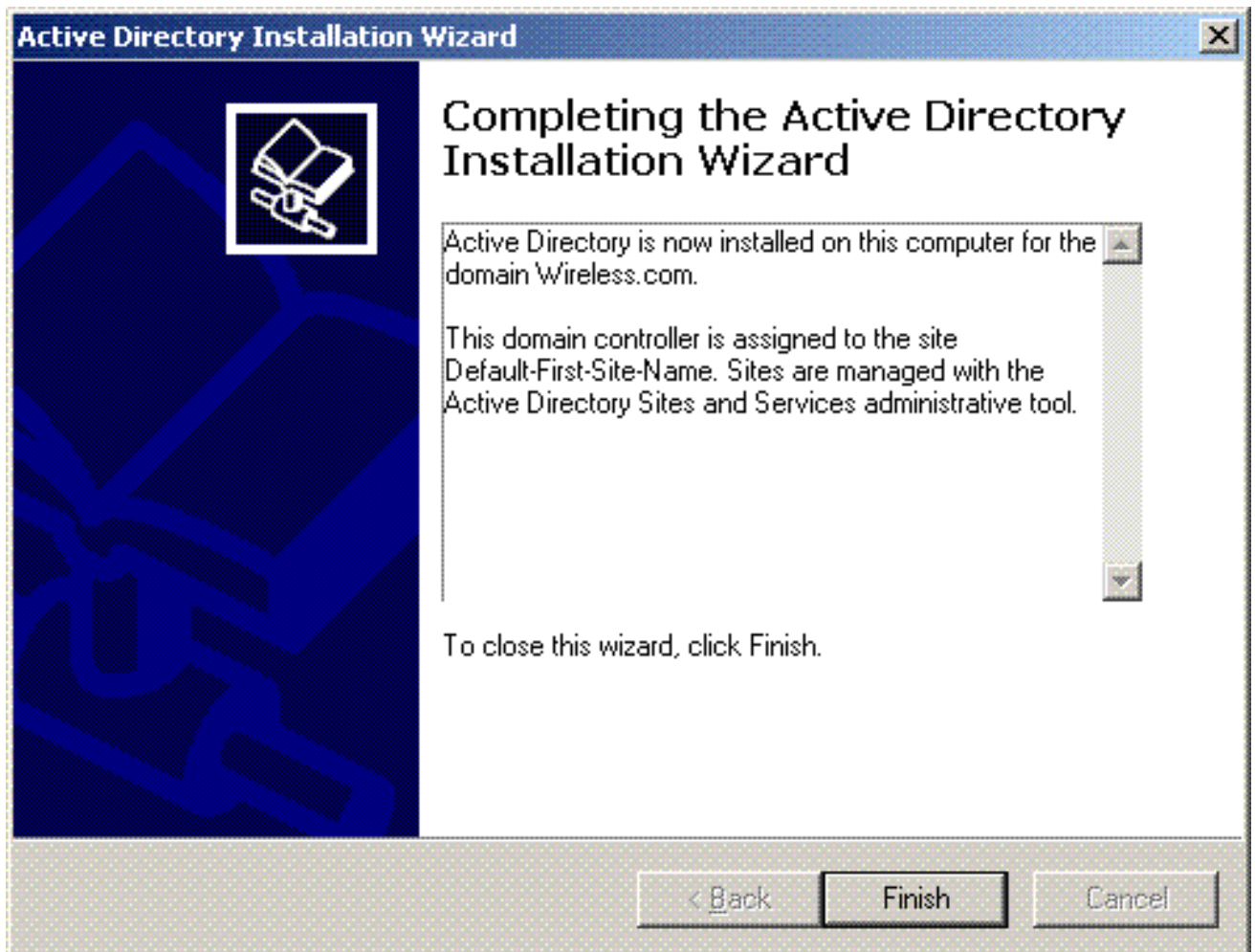


12. Clique em **Avançar** para aceitar as opções de domínio definidas anteriormente.

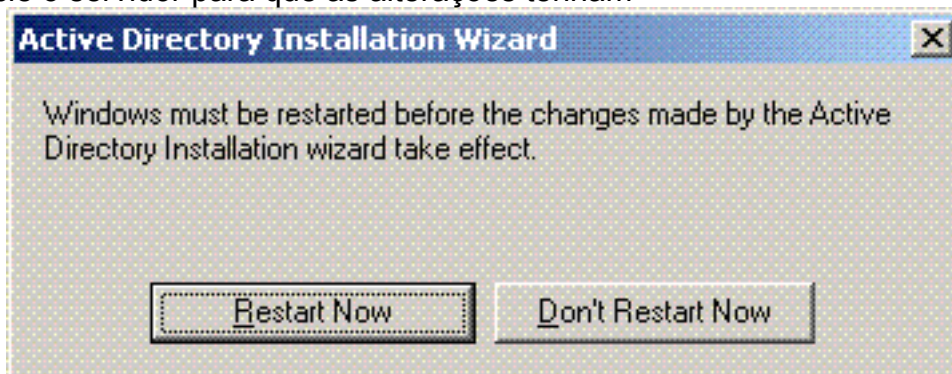




13. Clique em **Concluir** para fechar o Assistente de Instalação do Ative Directory.



14. Reinicie o servidor para que as alterações tenham



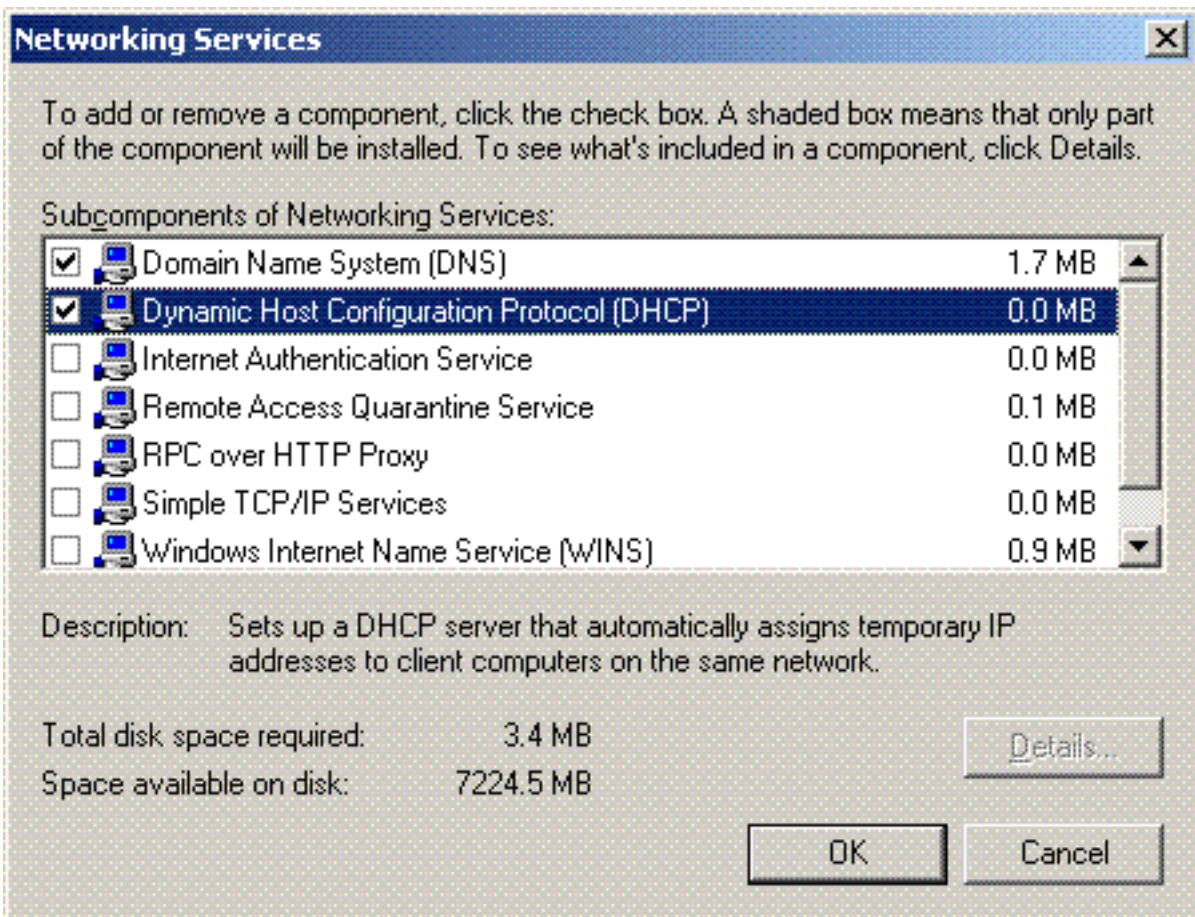
efeito.

Com esta etapa, você configurou o servidor Microsoft Windows 2003 como um controlador de domínio e criou um novo domínio **Wireless.com**. Em seguida, configure os serviços DHCP no servidor.

### [Instalar e configurar os serviços DHCP no Microsoft Windows 2003 Server](#)

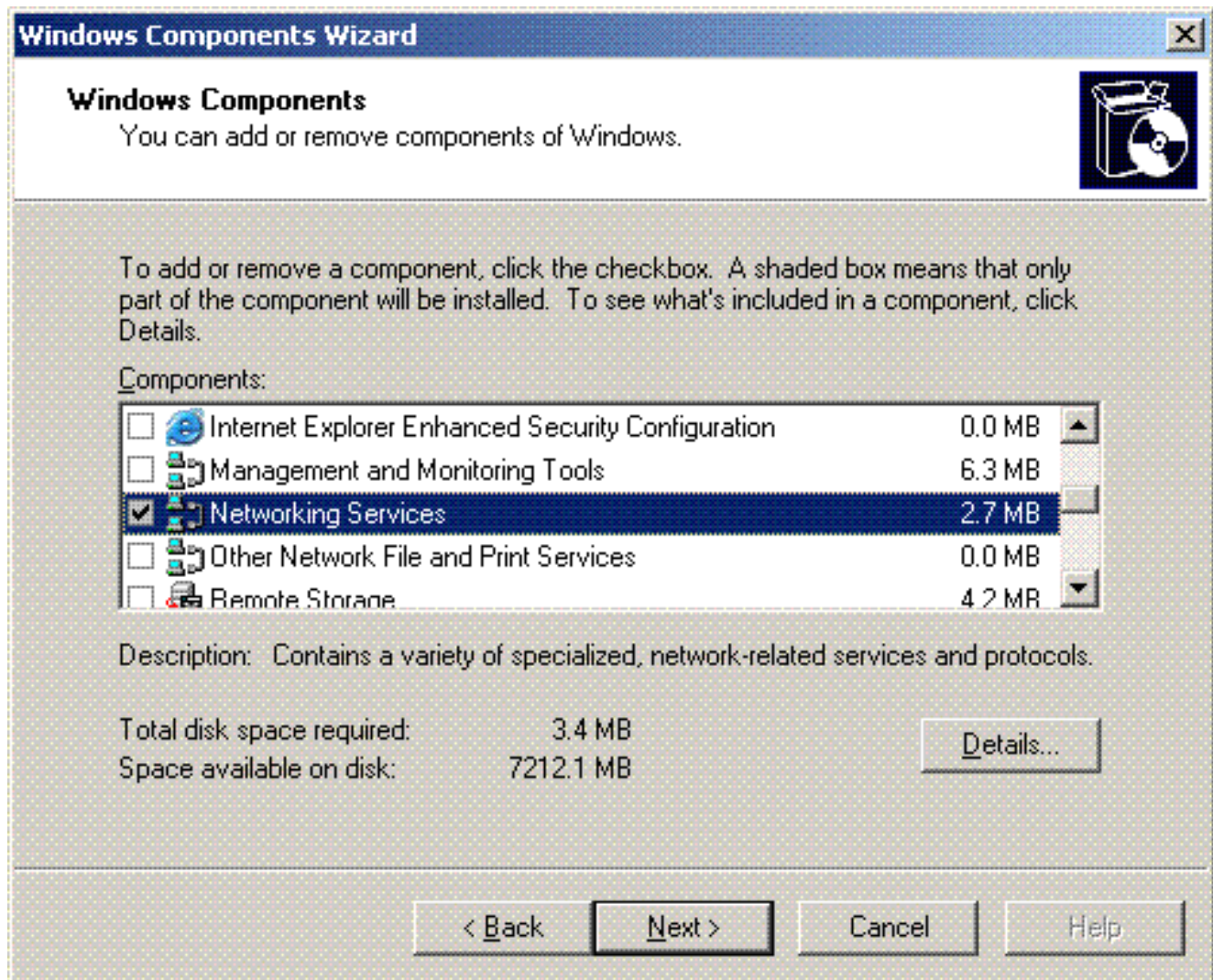
O serviço DHCP no servidor Microsoft 2003 é usado para fornecer endereços IP aos clientes Wireless. Para instalar e configurar os serviços DHCP neste servidor, siga estas etapas:

1. Clique em **Adicionar ou remover programas** no Painel de controle.
2. Clique em **Adicionar/remover componentes do Windows**.
3. Escolha **Networking Services** e clique em **Details**.
4. Escolha **Dynamic Host Configuration Protocol (DHCP)** e clique em



OK.

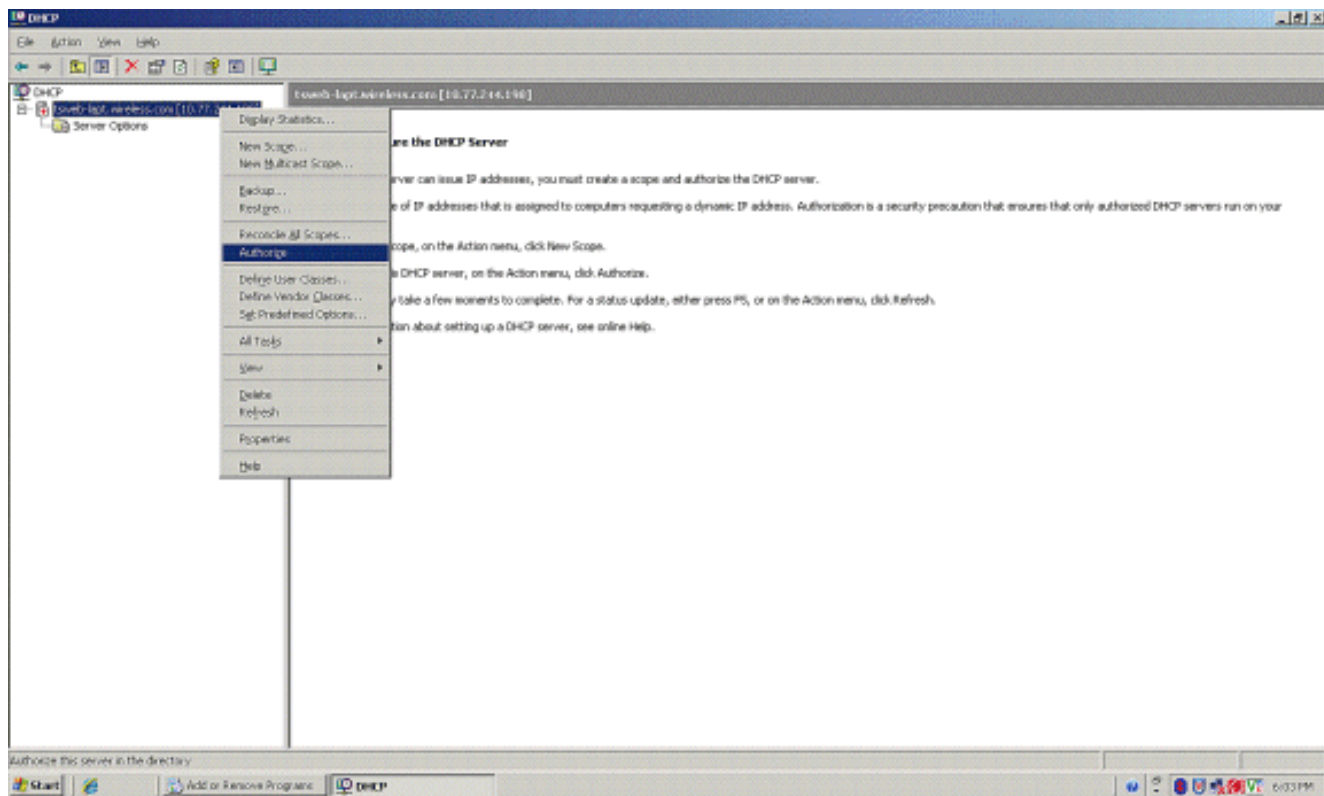
5. Clique em **Avançar** para instalar o serviço DHCP.



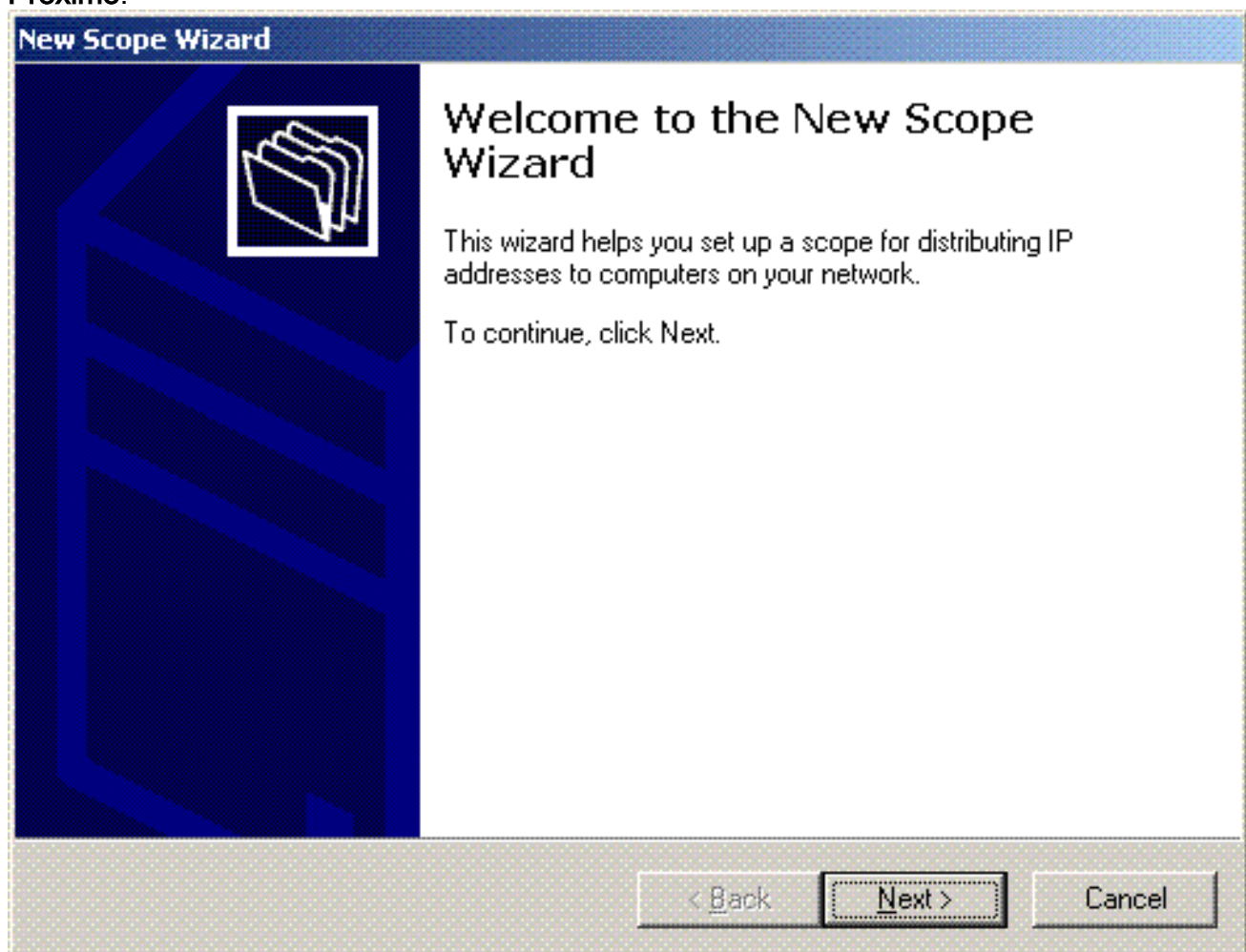
6. Clique em **Concluir** para concluir a instalação.



7. Para configurar os serviços DHCP, clique em **Start > Programs > Administrative tools** e clique no snap-in **DHCP**.
8. Escolha o servidor DHCP - **tsweb-lapt.wireless.com** (neste exemplo).
9. Clique em **Action** e, em seguida, clique em **Authorize** para autorizar o serviço DHCP.



10. Na árvore Console, clique com o botão direito do mouse em **tsweb-lapt.wireless.com** e, em seguida, clique em **Novo escopo** para definir um intervalo de endereços IP para os clientes Wireless.
11. Na página Bem-vindo ao Assistente de Novo Escopo do Assistente de Novo Escopo, clique em **Próximo**.



12. Na página Nome do escopo, digite o nome do escopo DHCP. Neste exemplo, use **DHCP-Clients** como o nome do escopo. Clique em **Next**.

**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:

< Back    Next >    Cancel

13. Na página Intervalo de endereços IP, insira os endereços IP inicial e final do escopo e clique em **Avançar**.

## 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: 10 . 77 . 244 . 218

End IP address: 10 . 77 . 244 . 219

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: 8

Subnet mask: 255 . 0 . 0 . 0

< Back

Next >

Cancel

14. Na página Adicionar exclusões, mencione o endereço IP que você gostaria de reservar/excluir do escopo do DHCP. Clique em Next.



## 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:

Add

Excluded address range:

Remove

< Back

Next >

Cancel

15. Mencione a duração da concessão na página Lease Duration e clique em **Next**.

## New Scope Wizard

### Lease Duration

The lease duration specifies how long a client can use an IP address from this scope.



Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate.

Set the duration for scope leases when distributed by this server.

Limited to:

Days:	Hours:	Minutes:
<input type="text" value="8"/>	<input type="text" value="0"/>	<input type="text" value="0"/>

< Back

Next >

Cancel

16. Na página Configure DHCP options (Configurar opções de DHCP), escolha **Yes, I want to configure DHCP Option now (Sim, desejo configurar a opção de DHCP agora)** e clique em **Next (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

17. Se houver um roteador de gateway padrão, mencione o endereço IP do roteador de gateway na página Roteador (gateway padrão) e clique em **Avançar**.

## New Scope Wizard

### 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

Remove

Up

Down

< Back

Next >

Cancel

18. Na página Nome do domínio e servidores DNS, digite o nome do domínio que foi configurado anteriormente. No exemplo, use **Wireless.com**. Insira o endereço IP do servidor. Clique em Add.

## 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:

IP address:

Add

Resolve

Remove

Up

Down

< Back

Next >

Cancel

19. Clique em Next.

20. Na página Servidor WINS, clique em **Avançar**.

21. Na página Ativar escopo, escolha **Sim, desejo ativar o escopo agora** e clique em **Avançar**.

## New Scope Wizard

### Activate Scope

Clients can obtain address leases only if a scope is activated.



Do you want to activate this scope now?

- Yes, I want to activate this scope now
- No, I will activate this scope later

< Back

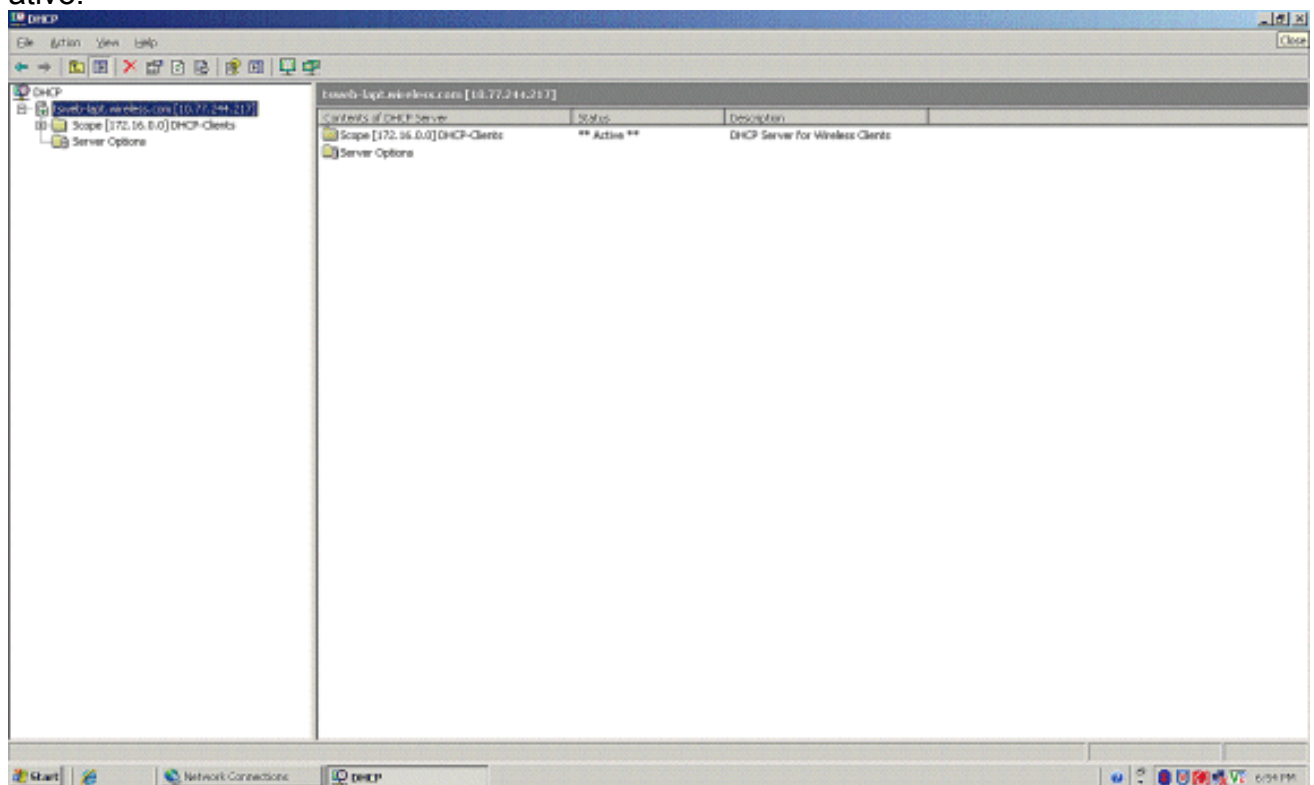
Next >

Cancel

22. Ao concluir o Assistente de Novo Escopo, clique em **Concluir**.



23. Na janela Snap-in DHCP, verifique se o escopo DHCP que foi criado está ativo.



Agora que o DHCP/ DNS está habilitado no servidor, configure o servidor como um servidor de Autoridade de Certificação (CA) empresarial.

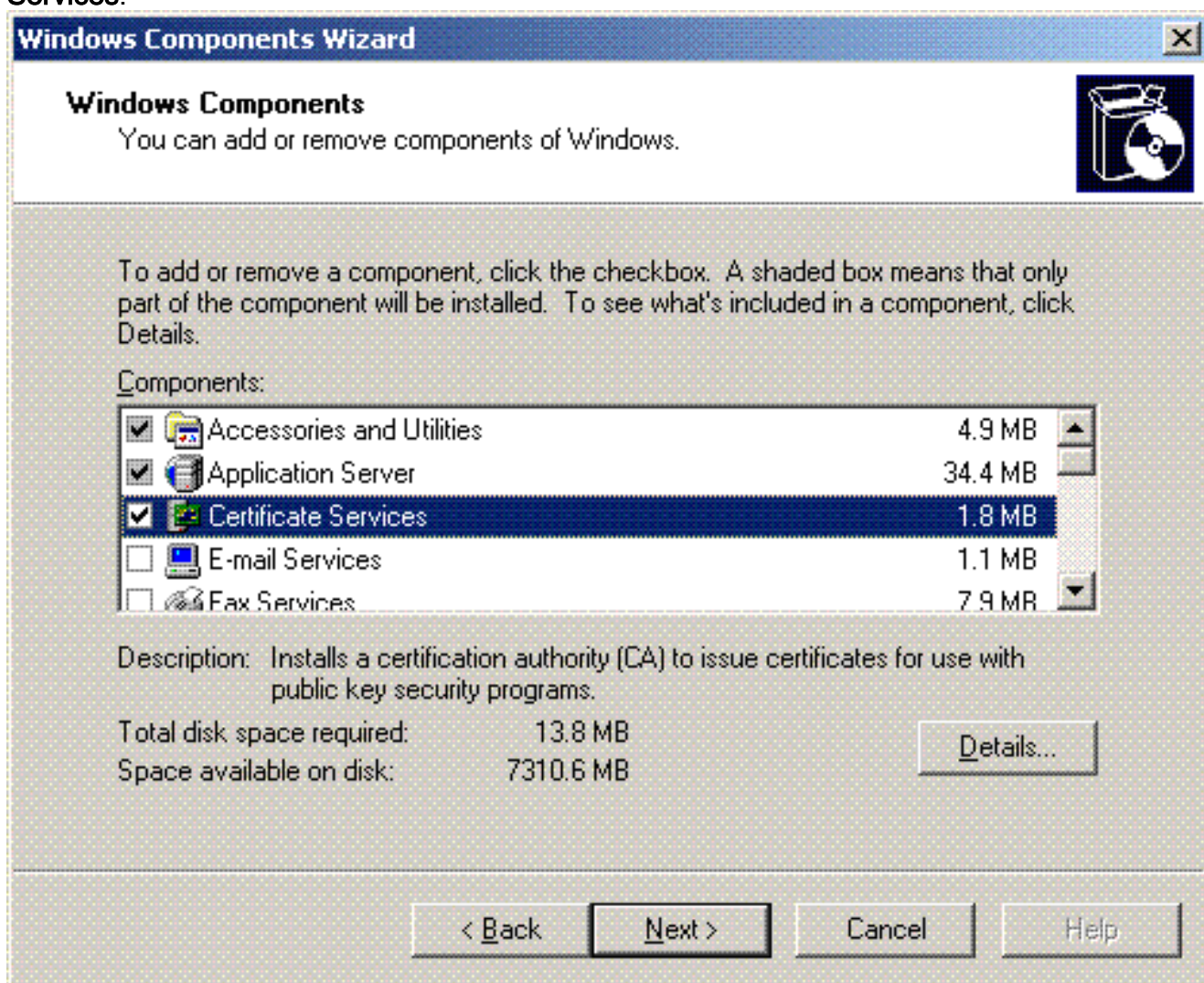
[Instalar e Configurar o Microsoft Windows 2003 Server como um Servidor de](#)

## Autoridade de Certificação (CA)

O PEAP com EAP-MS-CHAPv2 valida o servidor RADIUS com base no certificado presente no servidor. Além disso, o certificado do servidor deve ser emitido por uma autoridade de certificação pública que seja confiável para o computador cliente (ou seja, o certificado público da autoridade de certificação pública já existe na pasta Autoridade de Certificação Raiz Confiável no repositório de certificados do computador cliente). Neste exemplo, configure o servidor Microsoft Windows 2003 como uma Autoridade de Certificação (CA) que emite o certificado para o Serviço de Autenticação da Internet (IAS).

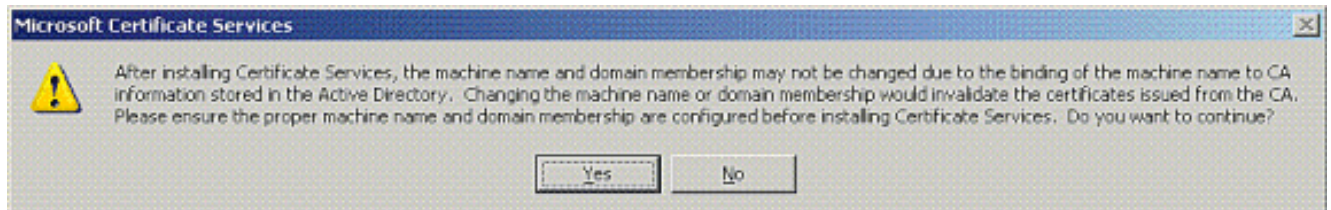
Para instalar e configurar os serviços de certificado no servidor, siga estas etapas:

1. Clique em **Adicionar ou remover programas** no **Painel de controle**.
2. Clique em **Adicionar/Remover componentes do Windows**.
3. Clique em **Certificate Services**.

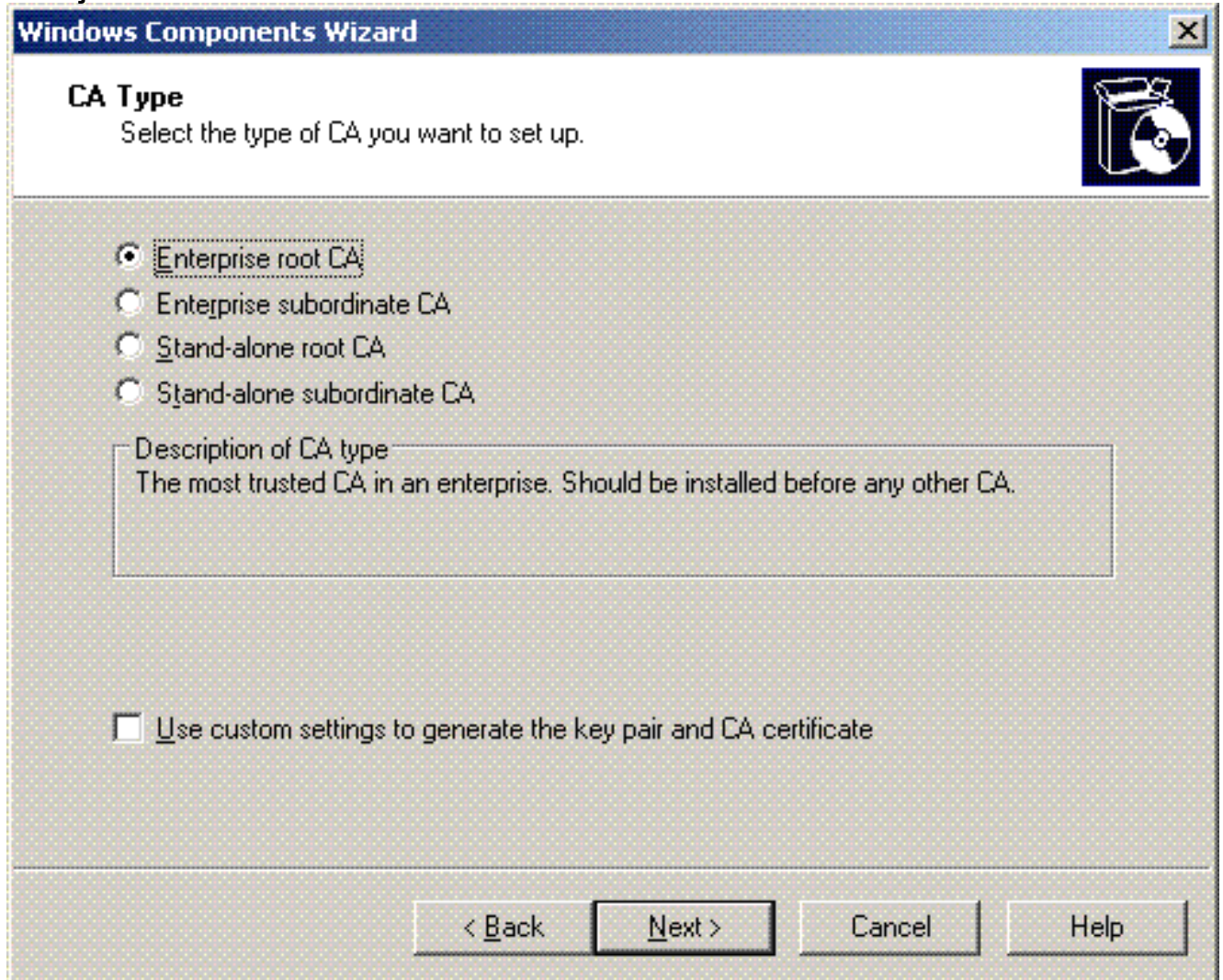


4. Clique em **Sim** para a mensagem de aviso, **Depois de instalar os serviços de certificado, o computador não poderá ser renomeado e não poderá ingressar nem ser removido de um domínio. Deseja continuar?**






5. Em Tipo de autoridade de certificação, escolha **CA raiz empresarial** e clique em **Avançar**.



6. Insira um nome para identificar a autoridade de certificação. Este exemplo usa **Wireless-CA**. Clique em **Next**.

**Windows Components Wizard** X

**CA Identifying Information**   
Enter information to identify this CA.

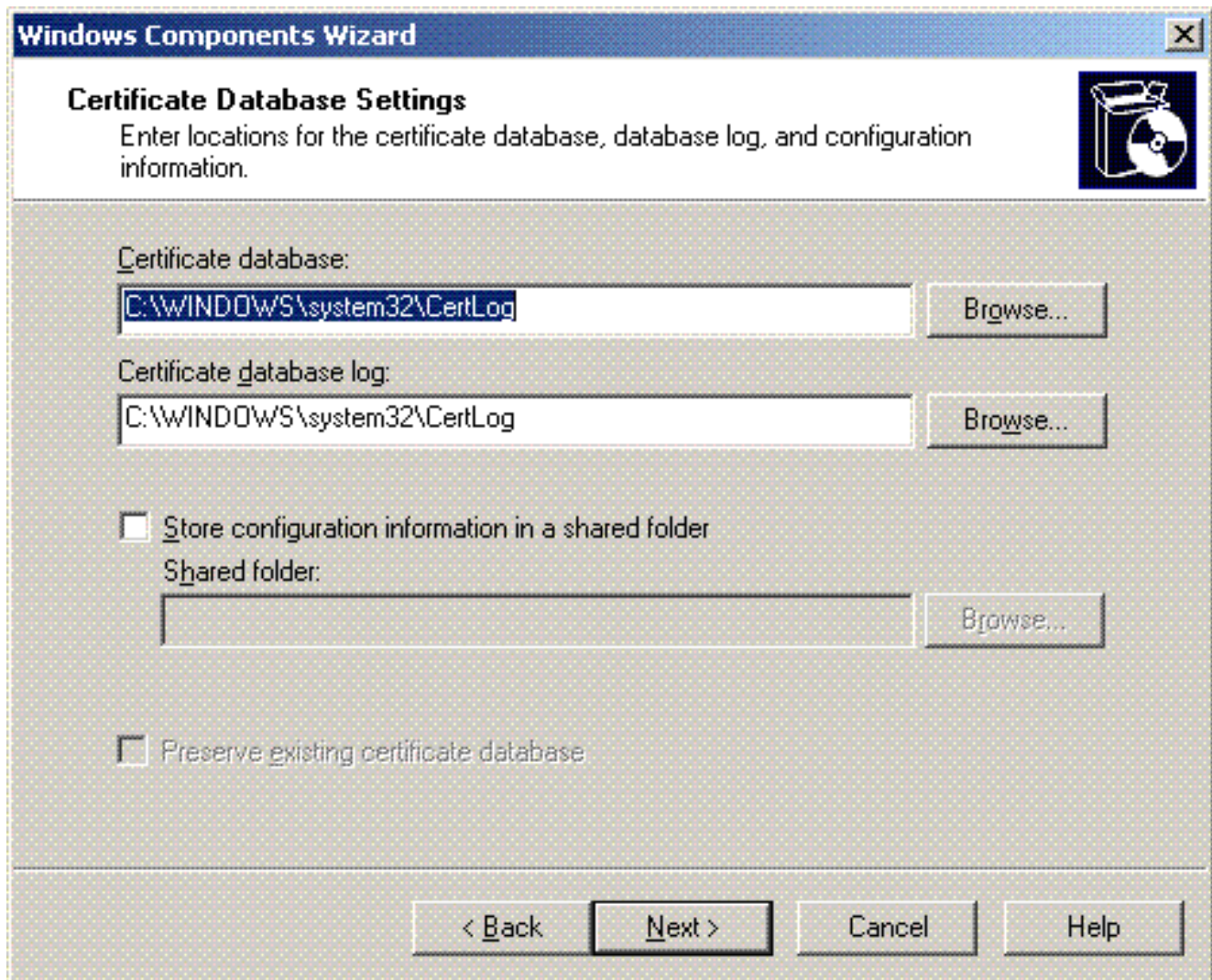
Common name for this CA:

Distinguished name suffix:

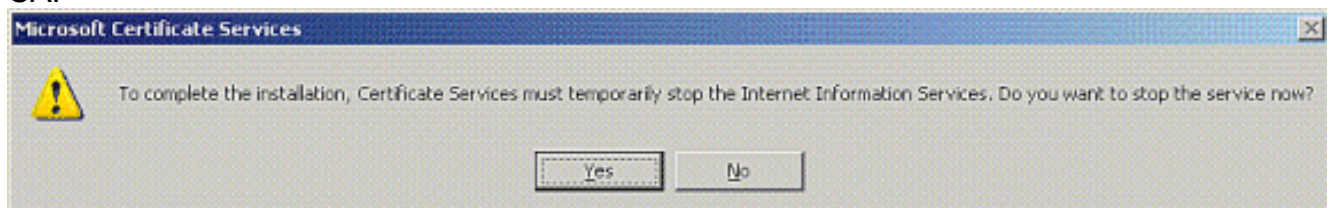
Preview of distinguished name:

Validity period:     
Expiration date: 12/12/2012 7:01 PM

- Um diretório de "Log de Certificados" é criado para o armazenamento do banco de dados de certificados. Clique em Next.



8. Se o IIS estiver habilitado, ele deverá ser interrompido antes que você continue. Clique em **OK** para exibir a mensagem de aviso de que o IIS deve ser interrompido. Ele é reiniciado automaticamente após a instalação do CA.



9. Clique em **Concluir** para concluir a instalação dos serviços da Autoridade de certificação (CA).

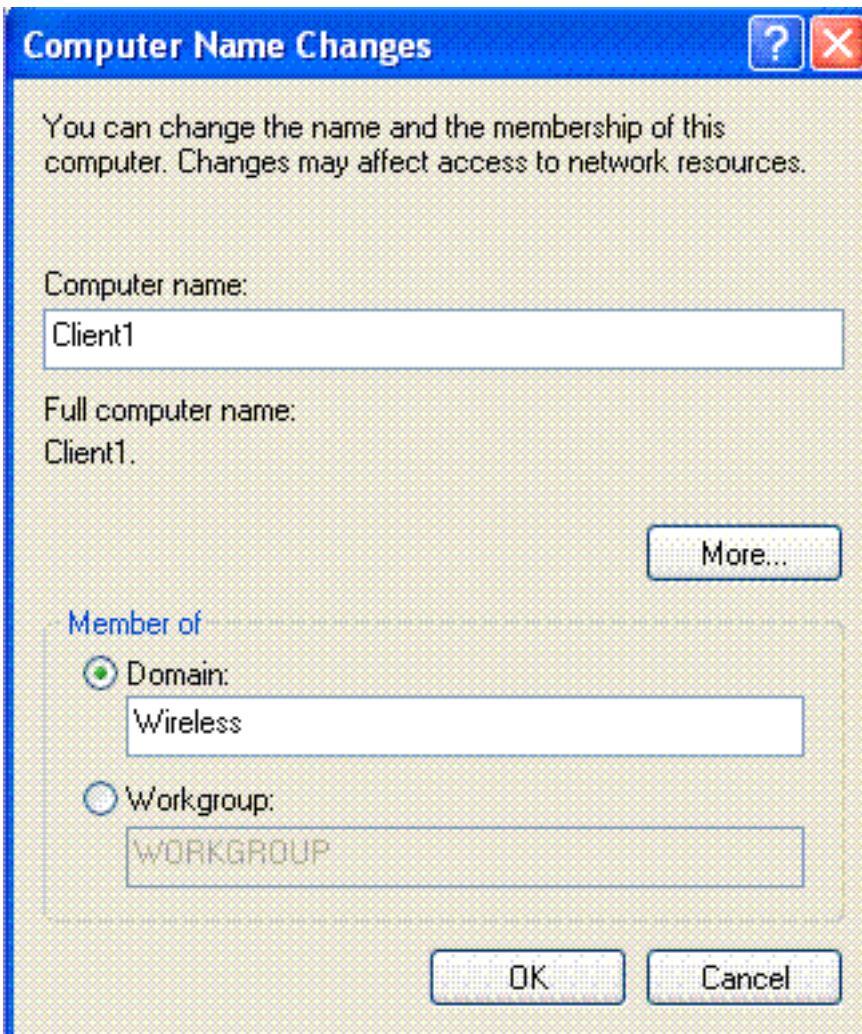


A próxima etapa é instalar e configurar o Internet Authentication Service no servidor Microsoft Windows 2003.

### [Conectar clientes ao domínio](#)

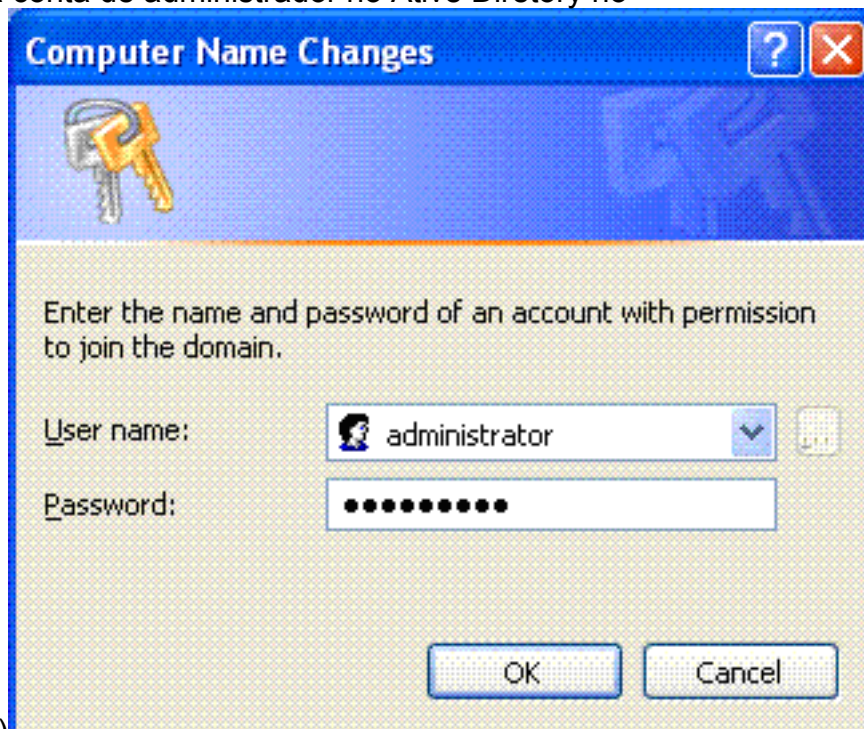
A próxima etapa é conectar os clientes à rede com fio e baixar as informações específicas do domínio do novo domínio. Em outras palavras, conecte os clientes ao domínio. Para isso, conclua essas etapas:

1. Conecte os clientes à rede com fio com um cabo Ethernet direto.
2. Inicialize o cliente e faça login com o nome de usuário/senha do cliente.
3. Clique em **Iniciar**; clique em **Executar**; digite **cmd**; e clique em **OK**.
4. No prompt de comando, digite **ipconfig** e clique em **Enter** para verificar se o DHCP funciona corretamente e se o cliente recebeu um endereço IP do servidor DHCP.
5. Para unir o cliente ao domínio, clique com o botão direito do mouse em **Meu computador** e escolha **Propriedades**.
6. Clique na guia **Nome do computador**.
7. Clique em **Alterar**.
8. Clique em **Domain**; digite **wireless.com**; e clique em



OK.

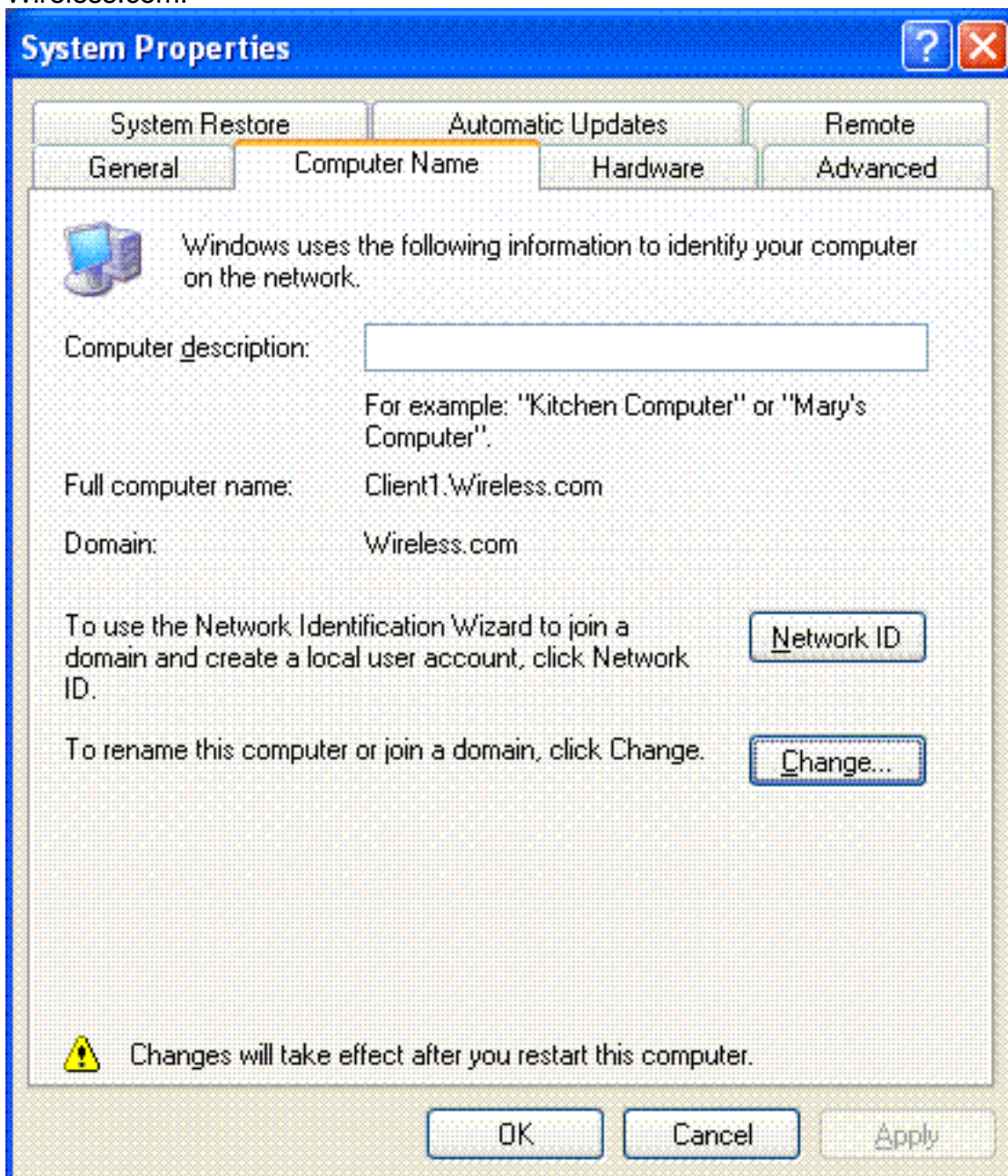
9. Digite **Username Administrator** e a senha específica do domínio ao qual o cliente ingressa. (Esta é a conta de administrador no Active Directory no



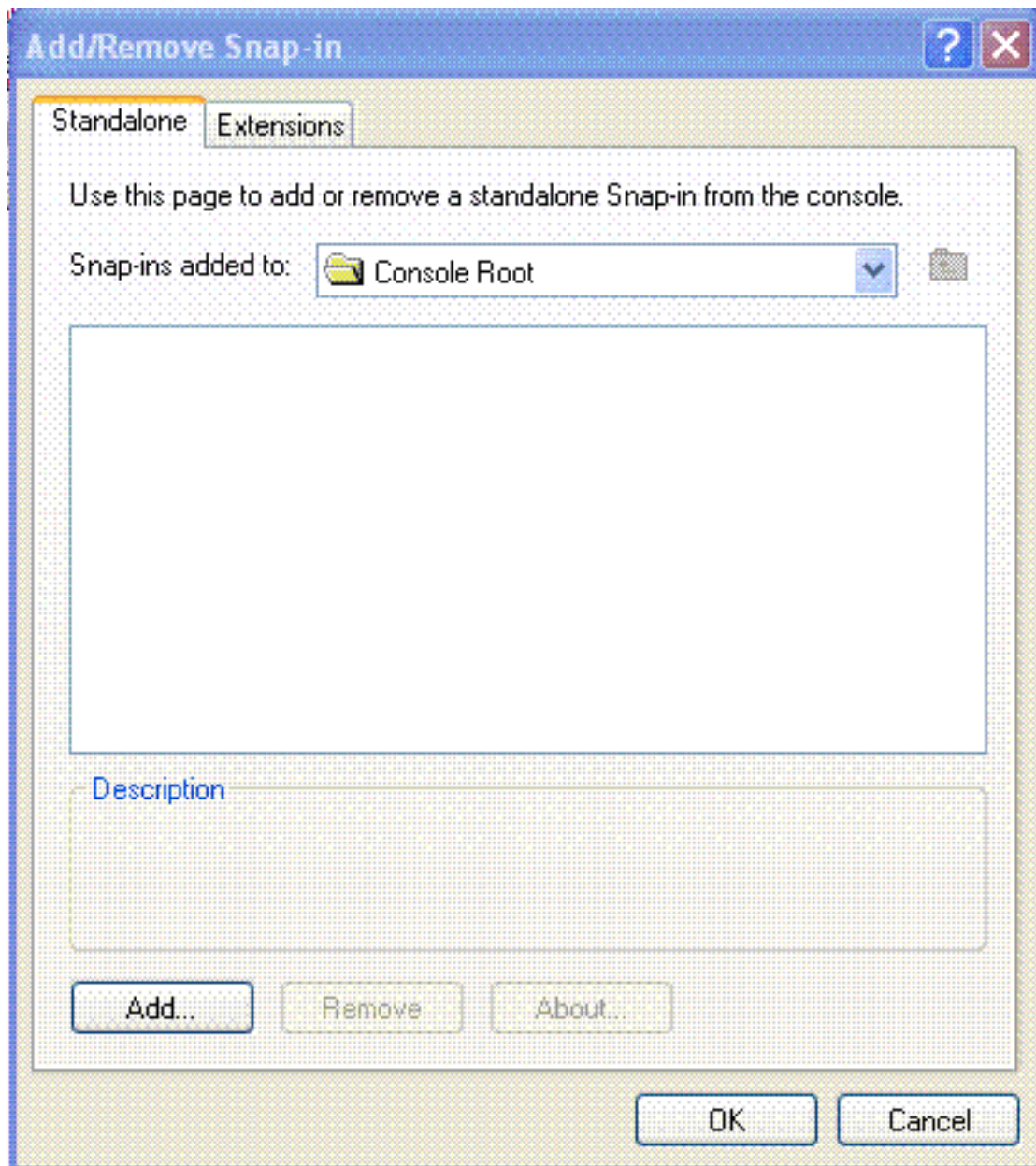
servidor.)



10. Click **OK**.
11. Clique em **Sim** para reiniciar o computador.
12. Quando o computador for reiniciado, faça login com estas informações: Nome de usuário = **Administrador**; Senha = <senha do domínio>; Domínio = **Sem fio**.
13. Clique com o botão direito do mouse em **Meu computador** e clique em **Propriedades**.
14. Clique na guia **Nome do computador** para verificar se você está no domínio Wireless.com.



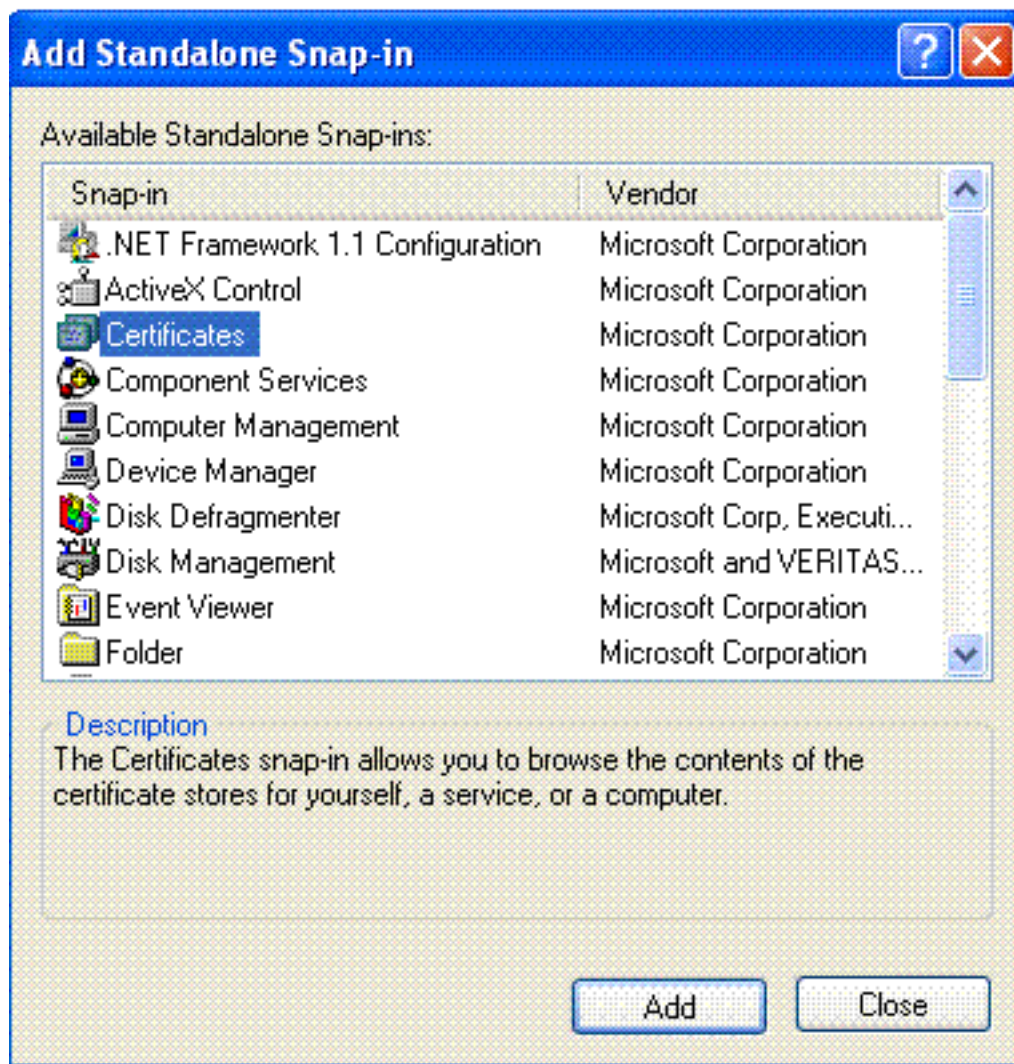
15. A próxima etapa é verificar se o cliente recebeu o certificado CA (confiança) do servidor.
16. Clique em **Iniciar**; clique em **Executar**; digite **mmc** e clique em **OK**.
17. Clique em **File** e clique em **Add/Remove snap-**



in.

18. Clique em Add.

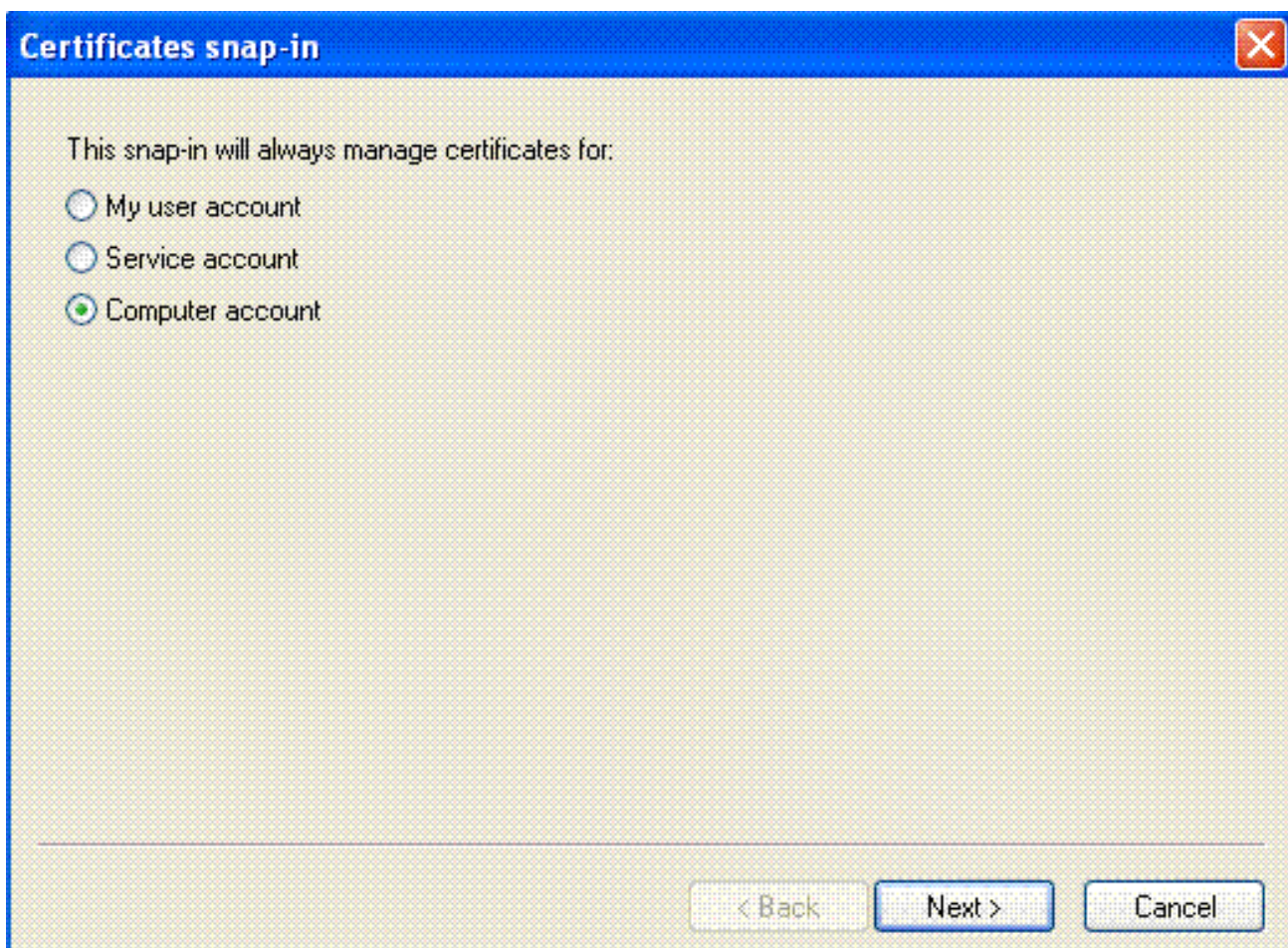
19. Escolha **Certificate** e clique em



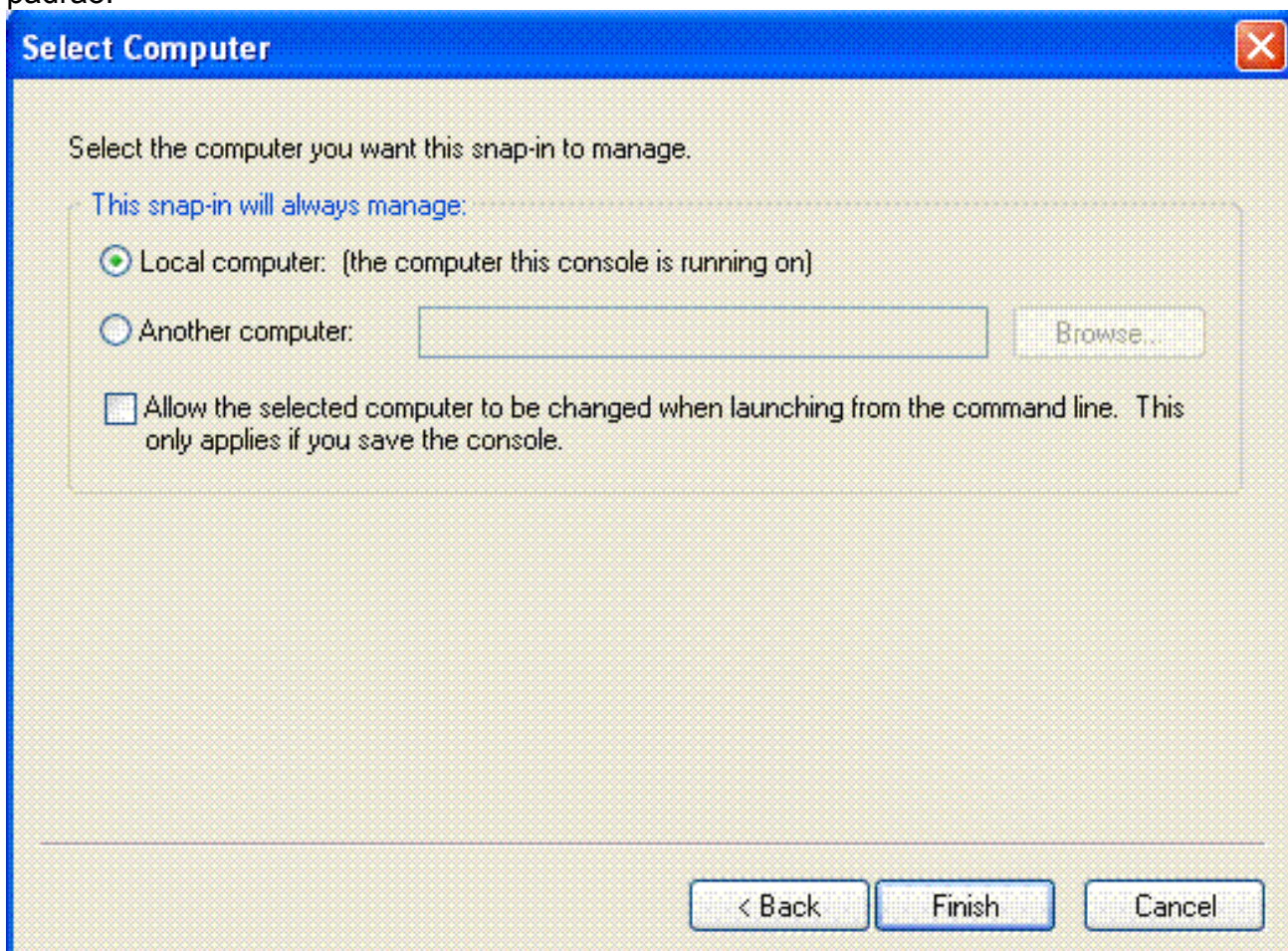
Add.

20. Escolha **Computer Account** e clique em **Next**.



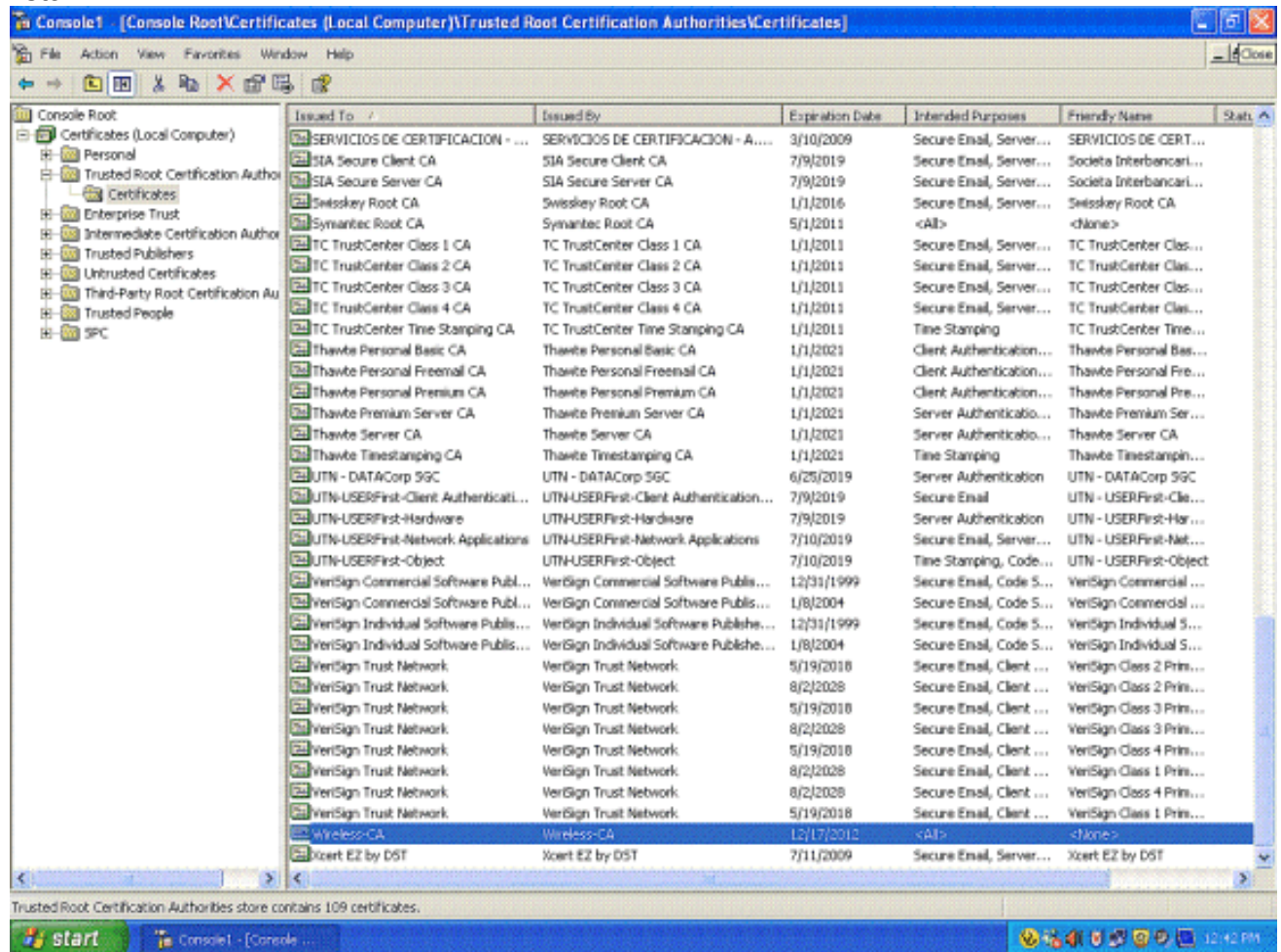


21. Clique em **Concluir** para aceitar o computador local padrão.



22. Clique em **Fechar** e em **OK**.

23. Expanda **Certificados (Computador Local)**; expanda **Autoridades de Certificação Raiz Confiáveis**; e clique em **Certificados**. Localize **Wireless** na lista.



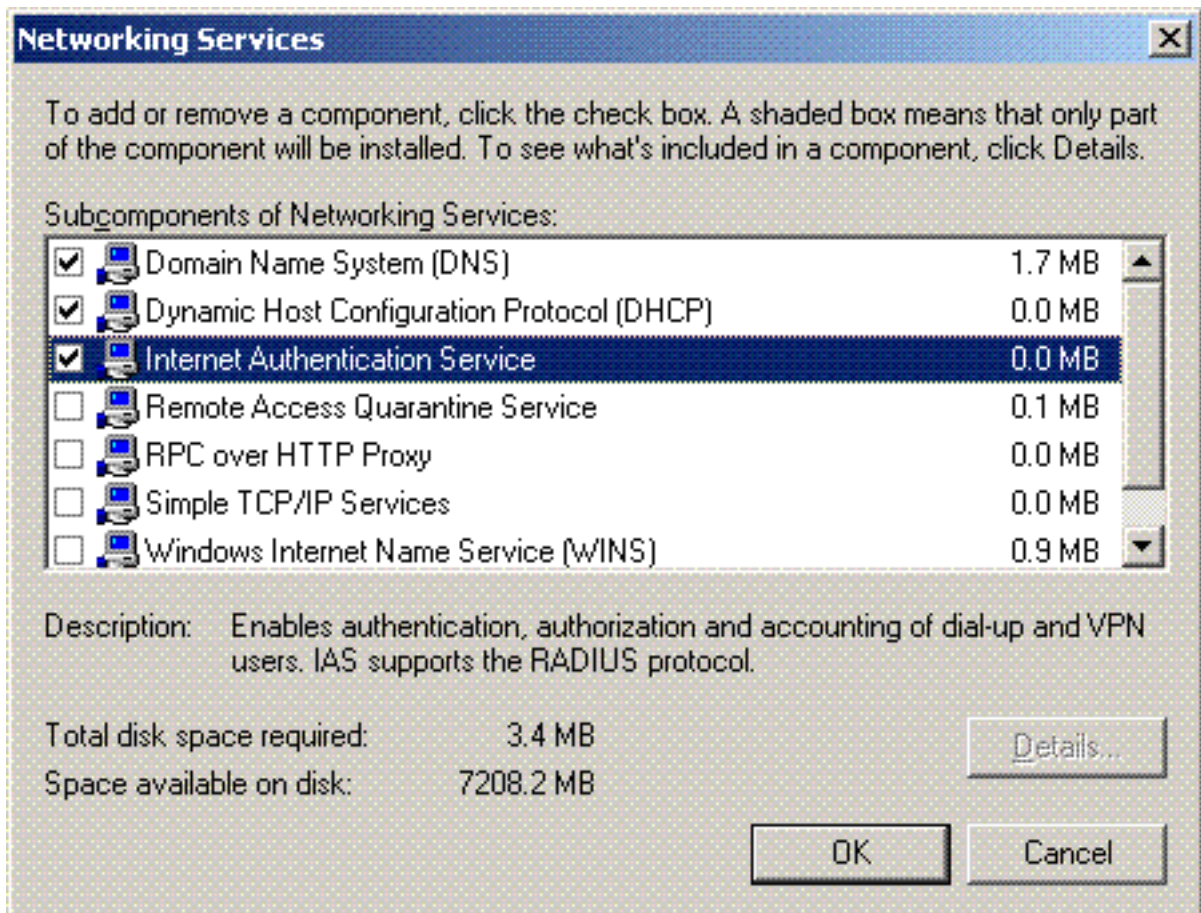
24. Repita este procedimento para adicionar mais clientes ao domínio.

## [Instale o Internet Authentication Service no Microsoft Windows 2003 Server e Solicite um Certificado](#)

Nesta configuração, o IAS (Internet Authentication Service) é usado como um servidor RADIUS para autenticar clientes Wireless com autenticação PEAP.

Conclua estas etapas para instalar e configurar o IAS no servidor.

1. Clique em **Adicionar ou remover programas** no Painel de controle.
2. Clique em **Adicionar/remover componentes do Windows**.
3. Escolha **Networking Services** e clique em **Details**.
4. Selecione **Internet Authentication Service**; clique em **OK**; e clique em

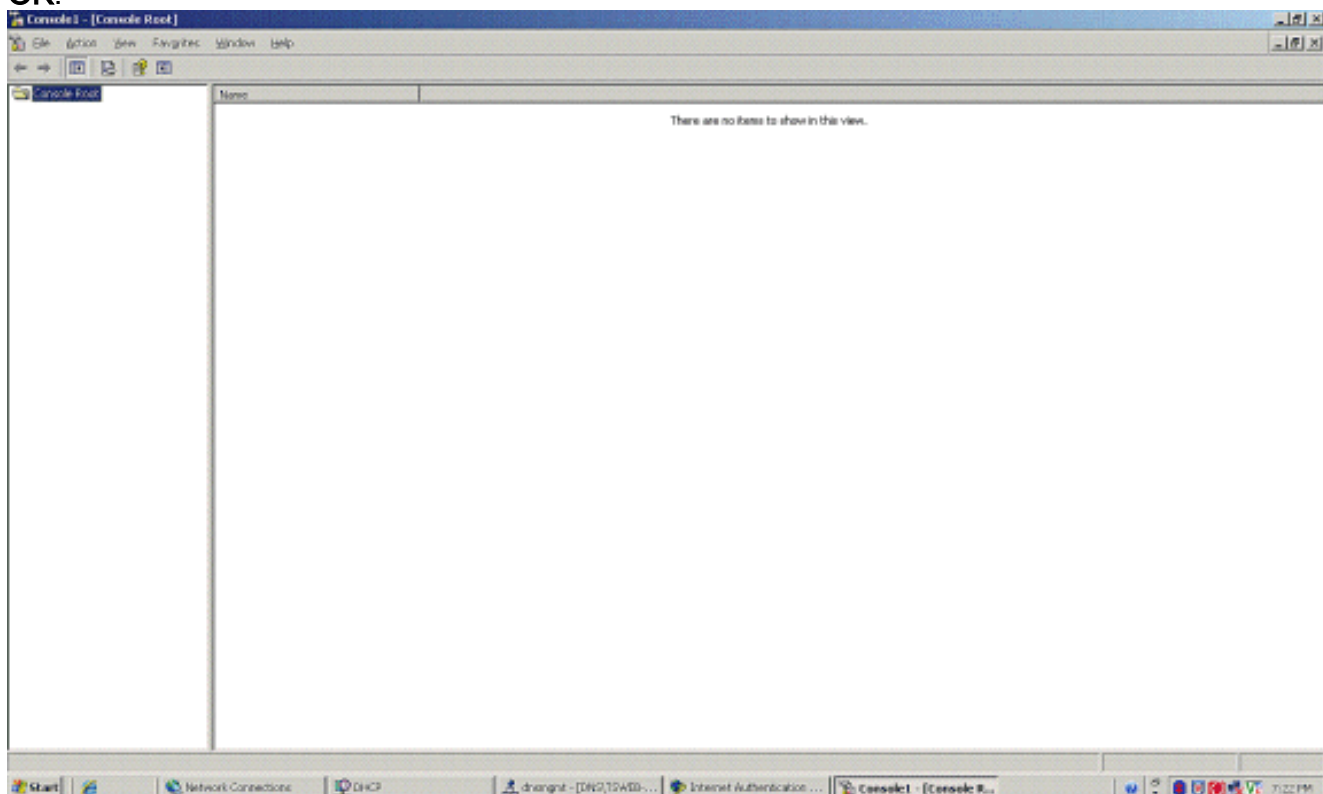


**Next.**

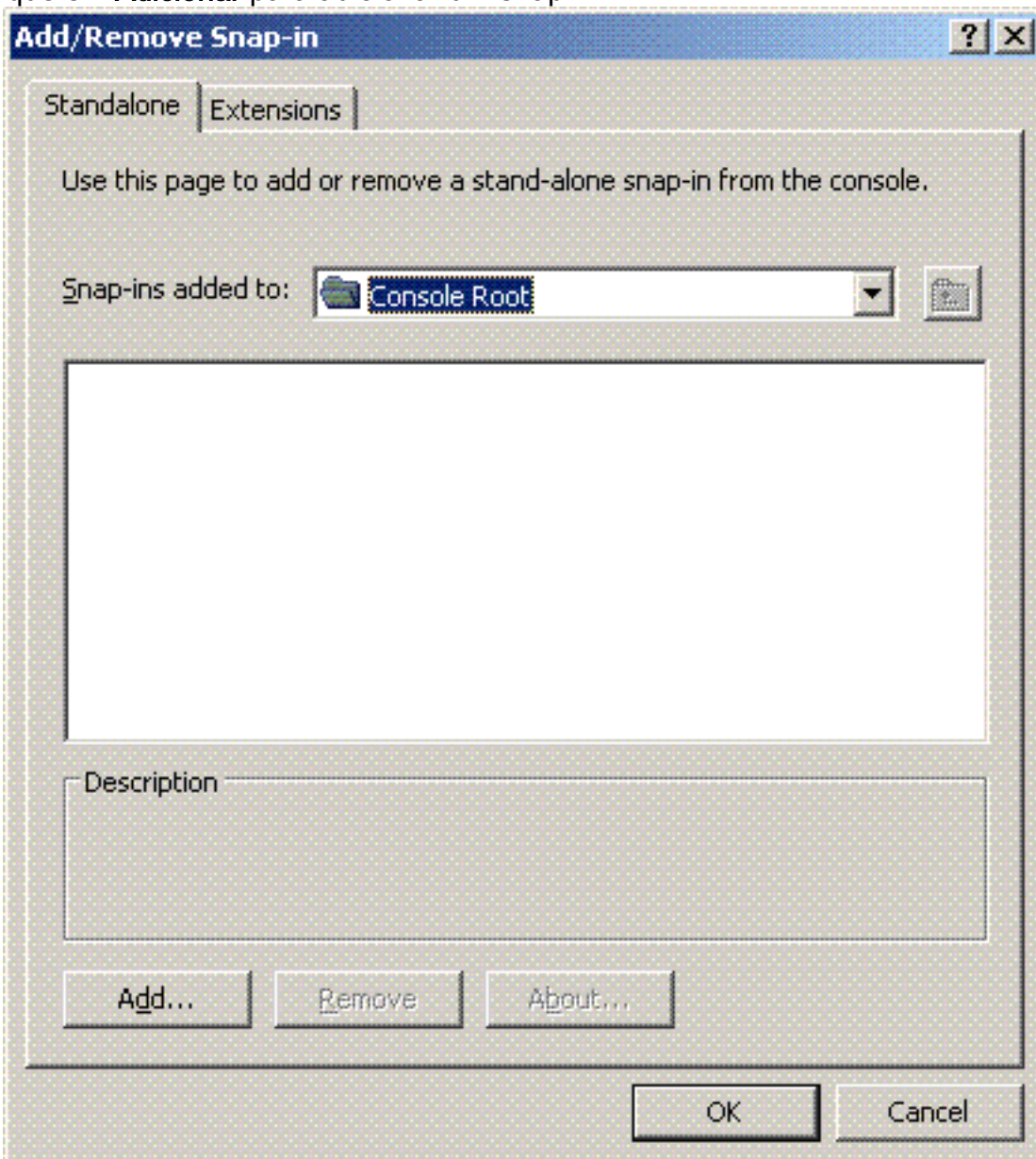
5. Clique em **Concluir** para concluir a instalação do IAS.



6. A próxima etapa é instalar o certificado do computador para o IAS (Internet Authentication Service).
7. Clique em **Iniciar**; clique em **Executar**; digite **mmc**; e clique em **OK**.

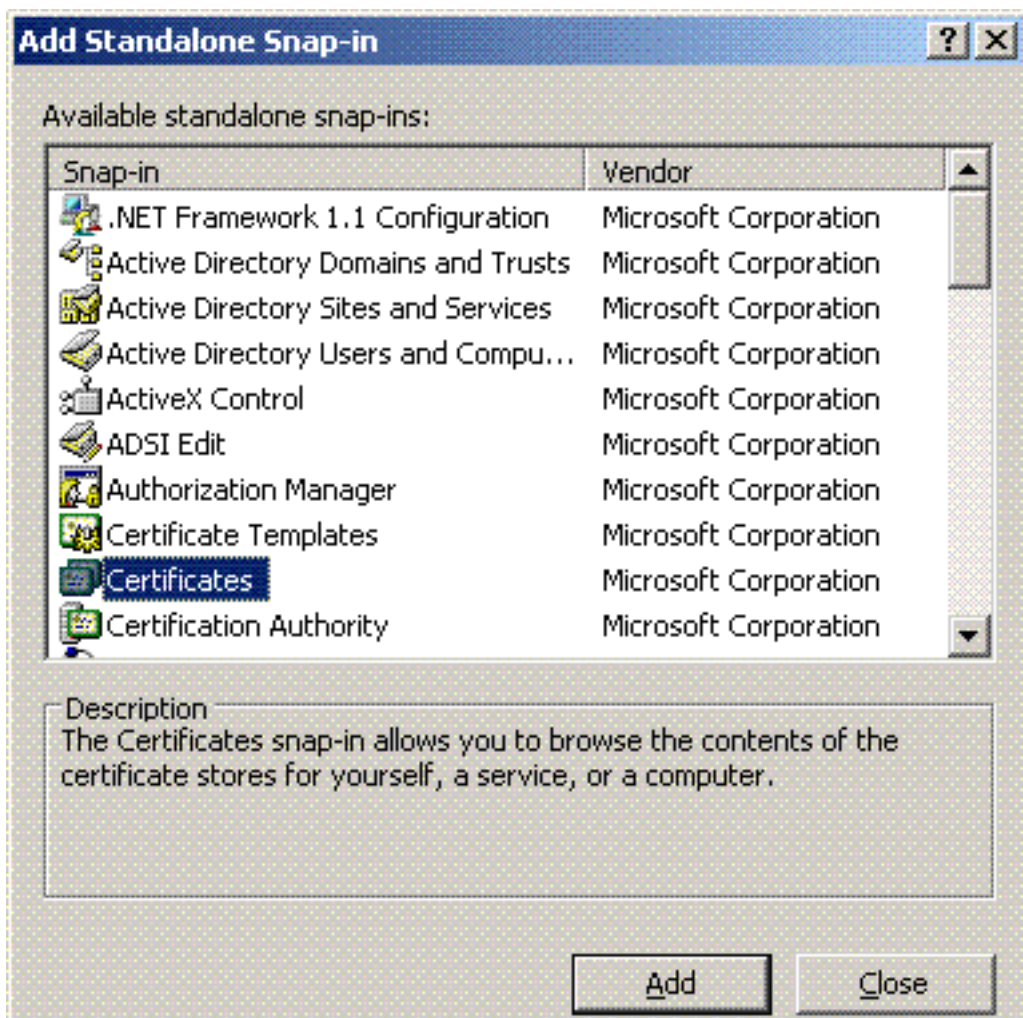


8. Clique em **Console** no menu Arquivo e escolha o snap-in **Adicionar/Remover**.
9. Clique em **Adicionar** para adicionar um snap-



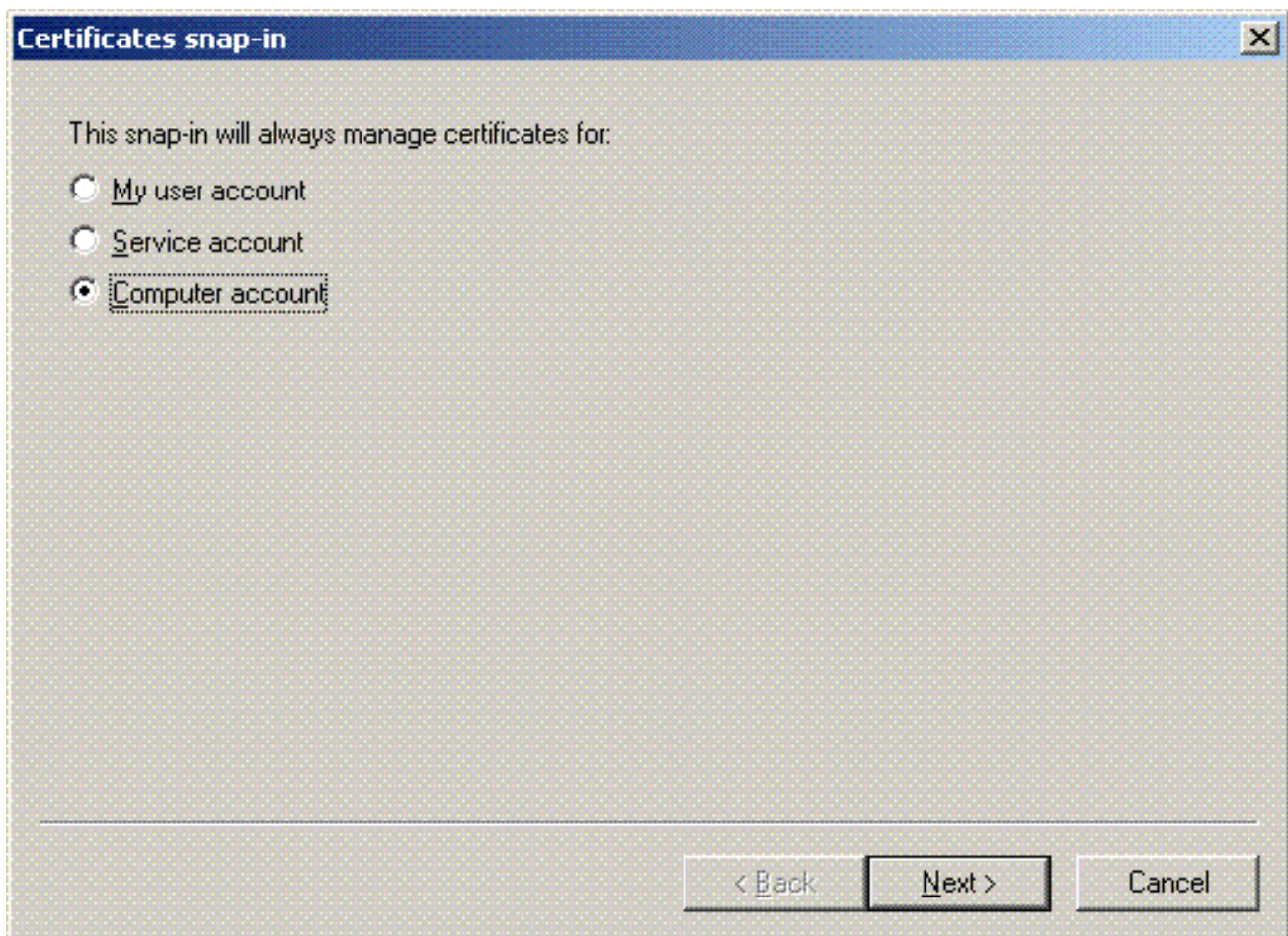
in.

10. Escolha **Certificados** na lista de snap-ins e clique em

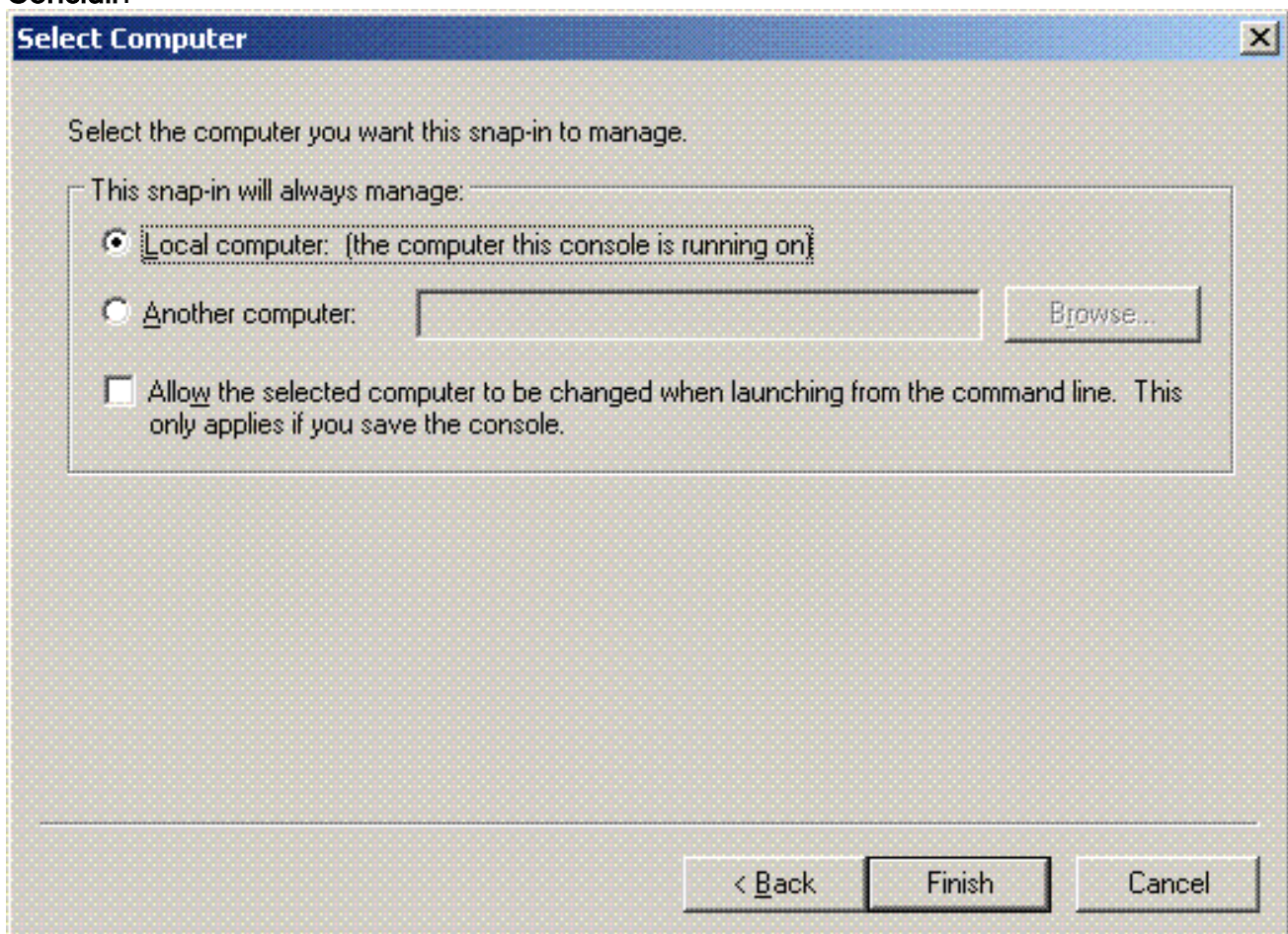


**Adicionar.**

11. Escolha **Conta do computador** e clique em **Avançar**.

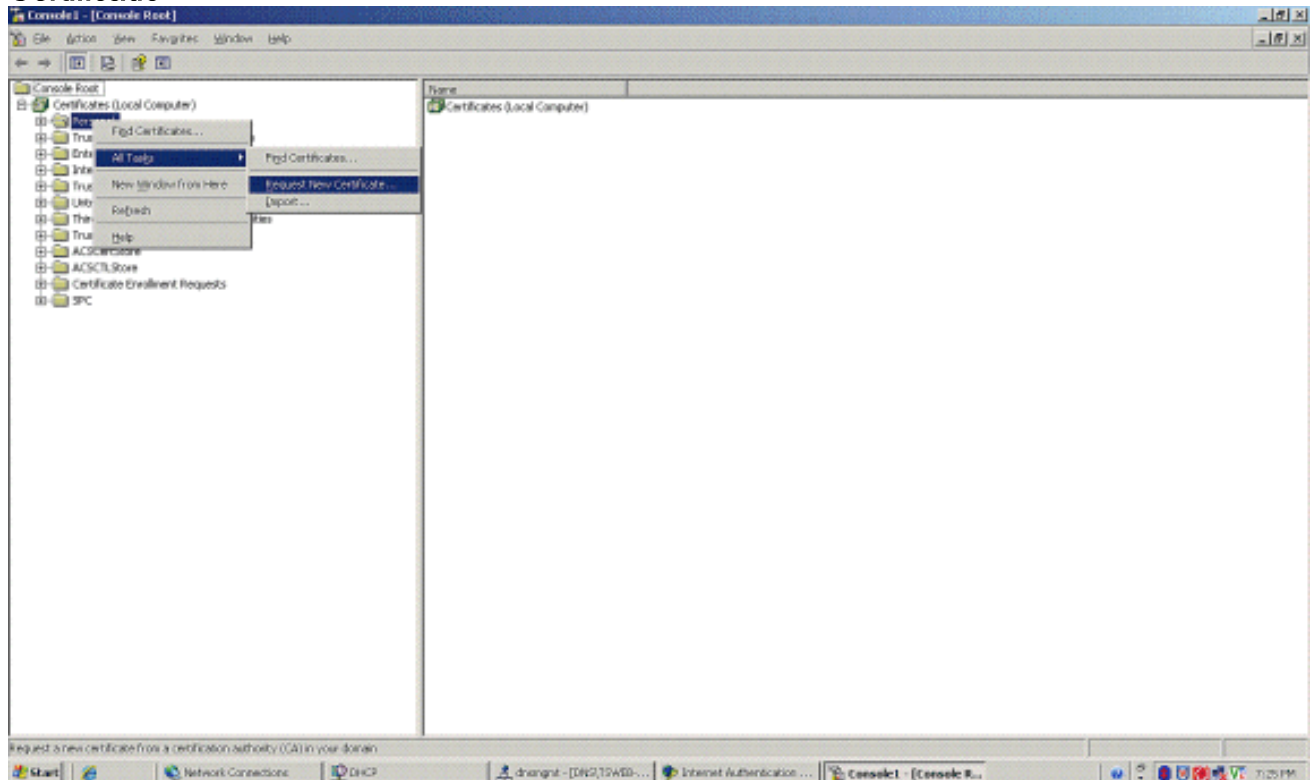


12. Escolha **Computador local** e clique em **Concluir**.



13. Clique em **Fechar** e em **OK**.

14. Expanda **Certificados (Computador Local)**; clique com o botão direito do mouse em **Pasta Pessoal**; escolha **Todas as tarefas** e, em seguida, **Solicitar Novo Certificado**.



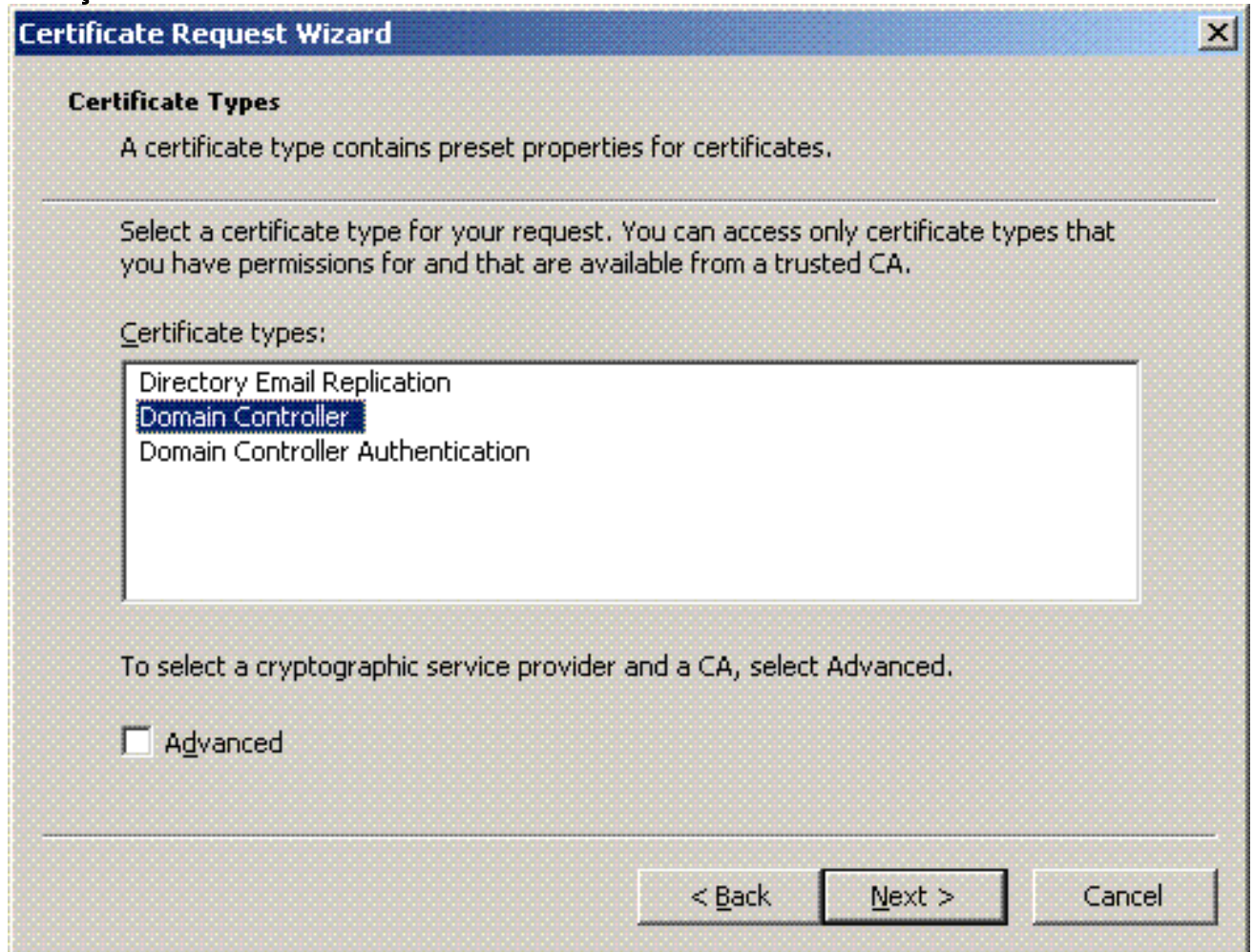
15. Clique em **Avançar** em **Bem-vindo ao Assistente de Solicitação de Certificado**.



16. Escolha o modelo de certificado do **Controlador de Domínio** (se você solicitar um certificado



de computador em um servidor que não seja o DC, escolha um modelo de certificado do Computador) e clique em Avançar.



17. Digite um nome e uma descrição para o certificado.

**Certificate Request Wizard** [X]

**Certificate Friendly Name and Description**

You can provide a name and description that help you quickly identify a specific certificate.

---

Type a friendly name and description for the new certificate.

Friendly name:

Description:

---

< Back   Next >   Cancel

18. Clique em **Concluir** para concluir o assistente de solicitação de certificação.

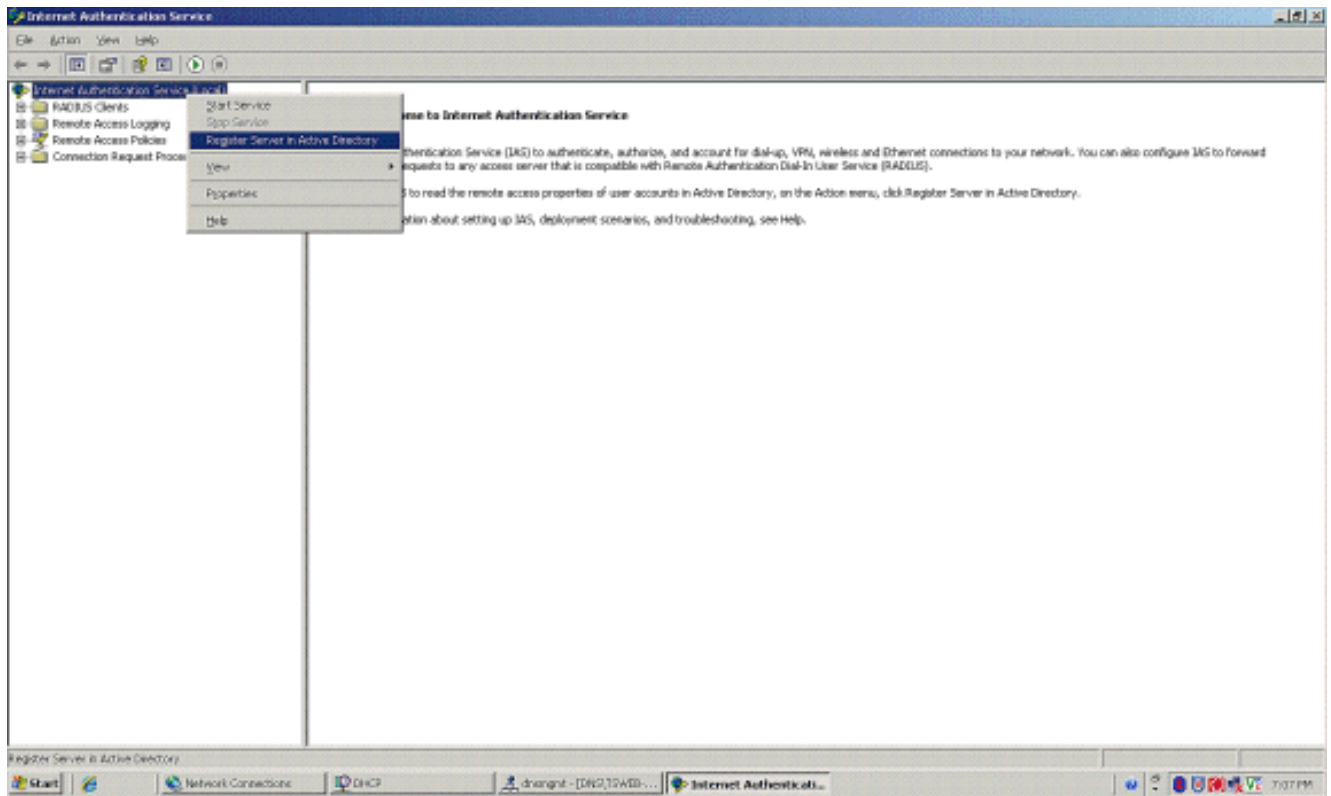


## [Configurar o serviço de autenticação da Internet para a autenticação PEAP-MS-CHAP v2](#)

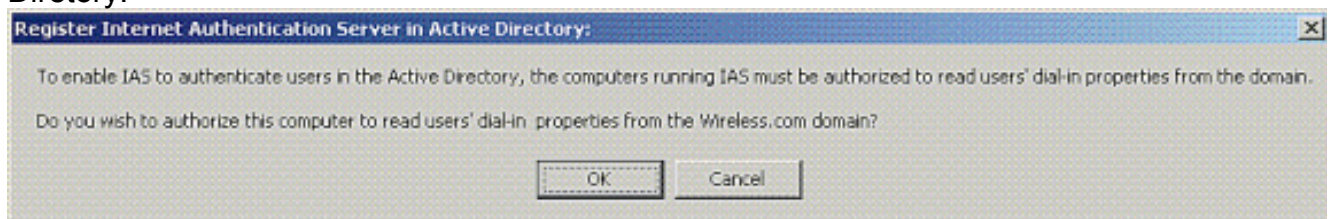
Agora que você instalou e solicitou um certificado para o IAS, configure o IAS para autenticação.

Conclua estes passos:

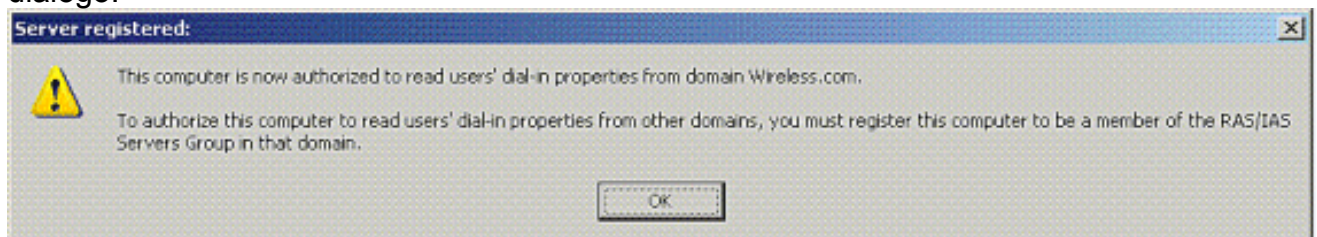
1. Clique em **Iniciar > Programas > Ferramentas Administrativas** e clique em **Internet Authentication Service** snap-in.
2. Clique com o botão direito do mouse em **Internet Authentication Service (IAS)** e clique em **Register Service in Active Directory**.



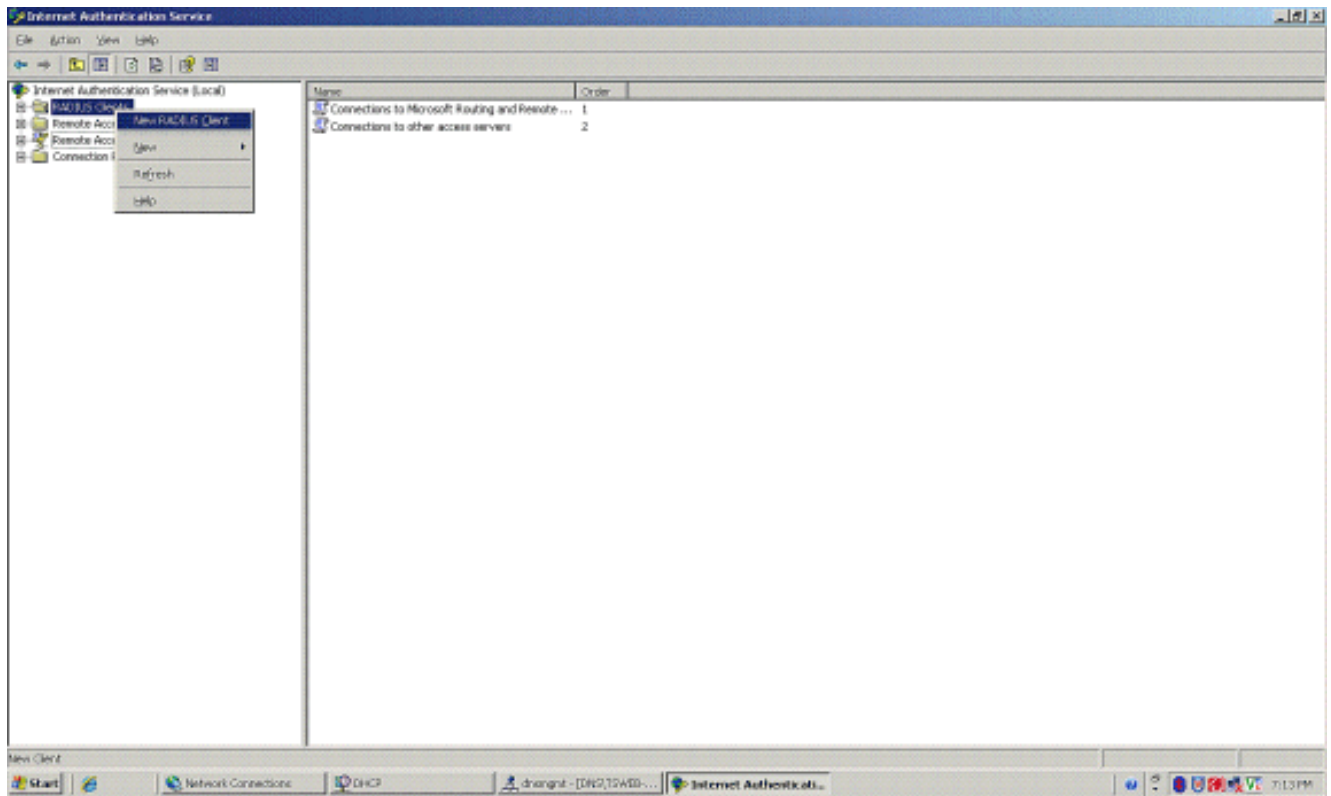
3. A caixa de diálogo Registrar Internet Authentication Service no Ative Directory é exibida; clique em OK. Isso permite que o IAS autentique usuários no Ative Directory.



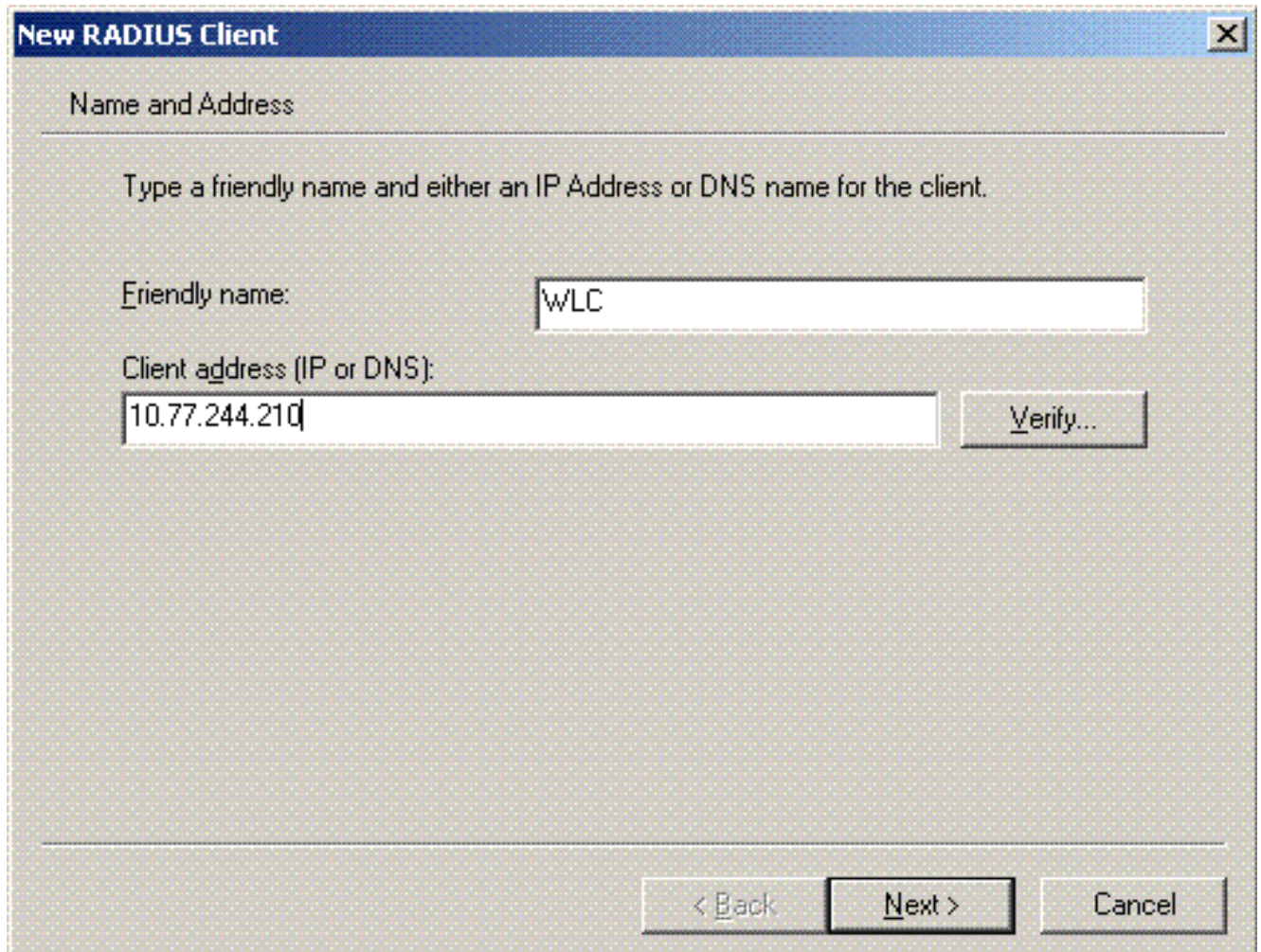
4. Clique em OK na próxima caixa de diálogo.



5. Adicione o Wireless LAN Controller como um cliente AAA no servidor MS IAS.
6. Clique com o botão direito do mouse em RADIUS Clients e escolha New RADIUS Client.

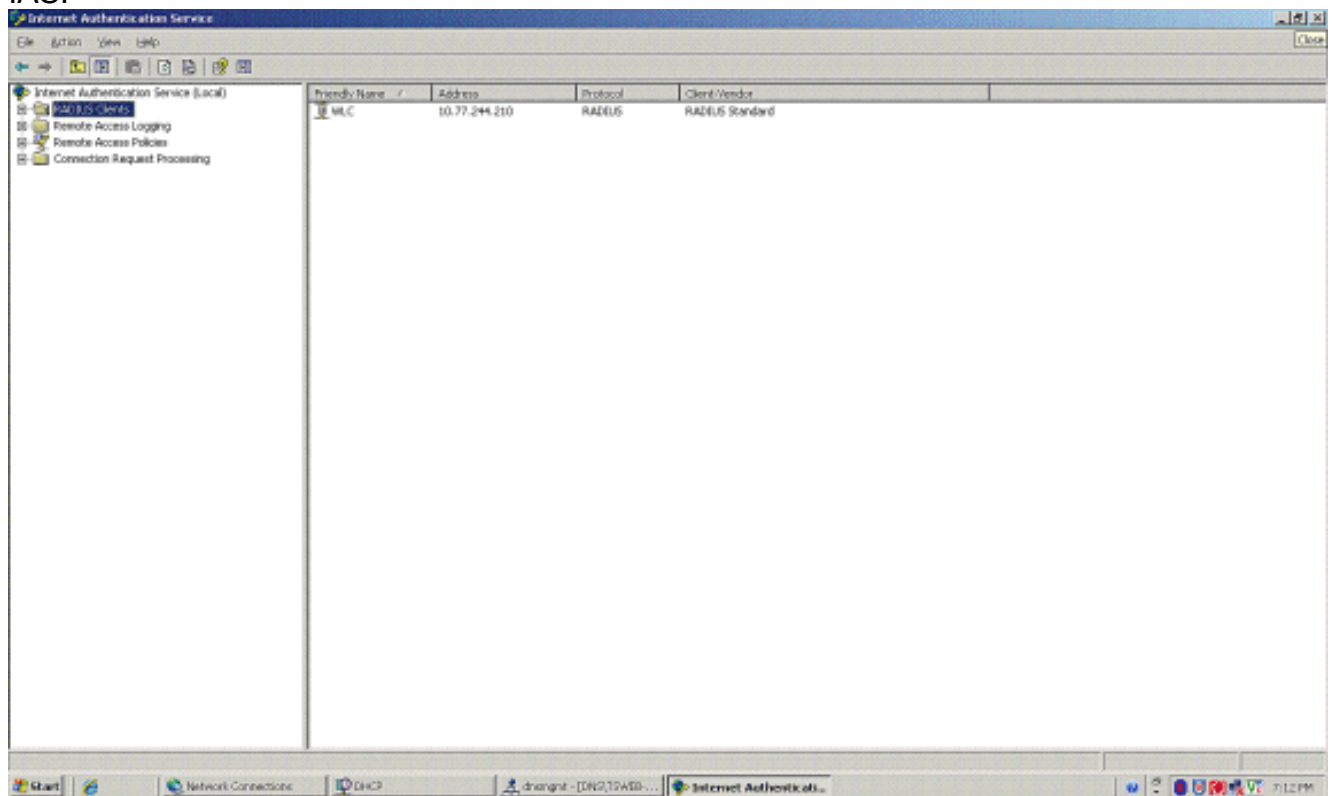


7. Digite o nome do cliente (WLC nesse caso) e insira o endereço IP da WLC. Clique em Next.

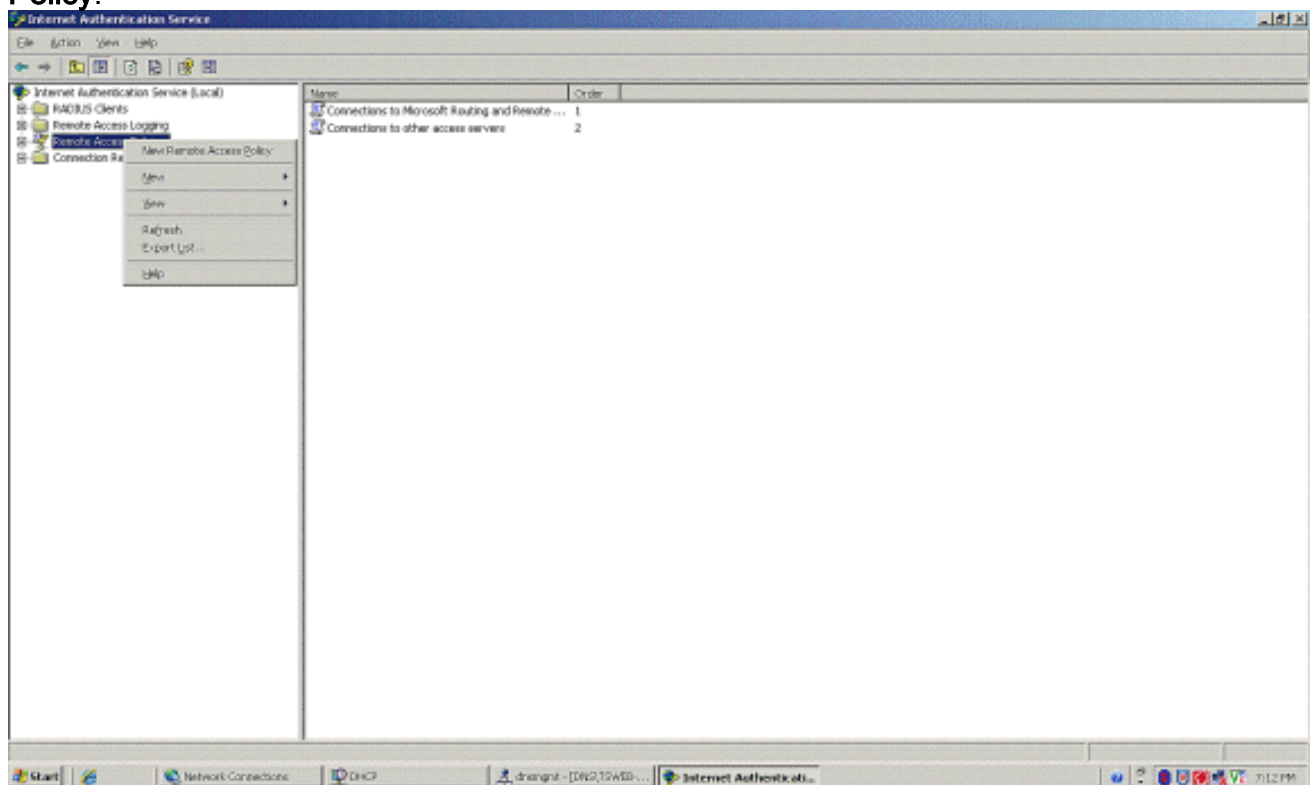


8. Na próxima página, em Client-Vendor, escolha **RADIUS Standard**; insira o segredo compartilhado e clique em **Finish**.
9. Observe que a WLC é adicionada como um cliente AAA no

# IAS.



10. Crie uma política de acesso remoto para os clientes.
11. Para fazer isso, clique com o botão direito do mouse em **Remote Access Policies** e escolha **New Remote Access Policy**.




12. Digite um nome para a política de acesso remoto. Neste exemplo, use o nome **PEAP**. Em seguida, clique em **Avançar**.

**New Remote Access Policy Wizard** [X]

**Policy Configuration Method**

The wizard can create a typical policy, or you can create a custom policy.



How do you want to set up this policy?

Use the wizard to set up a typical policy for a common scenario

Set up a custom policy

Type a name that describes this policy.

Policy name:


Example: Authenticate all VPN connections.

< Back    Next >    Cancel

13. Escolha os atributos da política com base em seus requisitos. Neste exemplo, escolha **Wireless**.

**New Remote Access Policy Wizard** [X]

**Access Method**  
Policy conditions are based on the method used to gain access to the network.



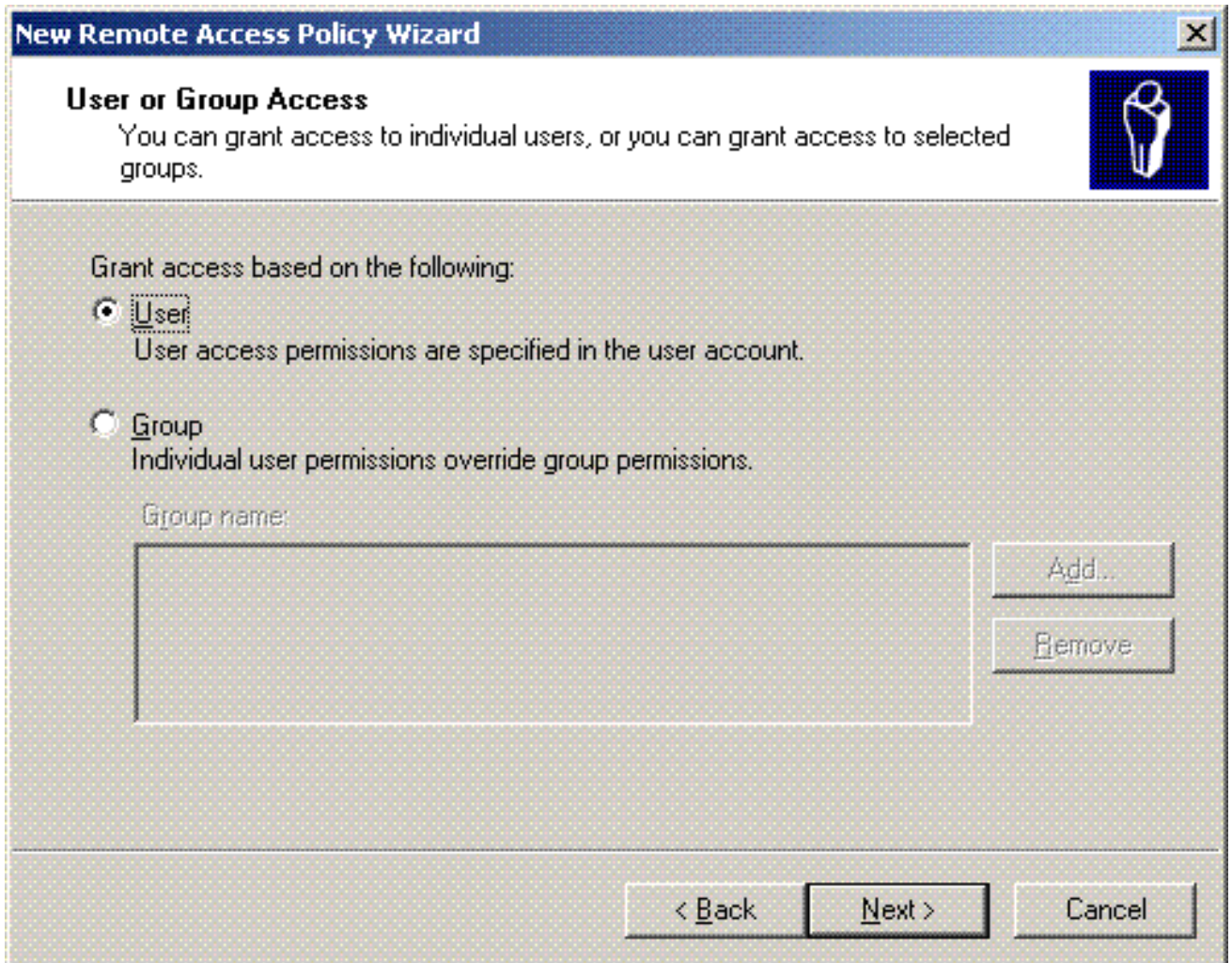
Select the method of access for which you want to create a policy.

- V**PN  
Use for all VPN connections. To create a policy for a specific VPN type, go back to the previous page, and select Set up a custom policy.
- D**ial-up  
Use for dial-up connections that use a traditional phone line or an Integrated Services Digital Network (ISDN) line.
- W**ireless  
Use for wireless LAN connections only.
- E**thernet  
Use for Ethernet connections, such as connections that use a switch.

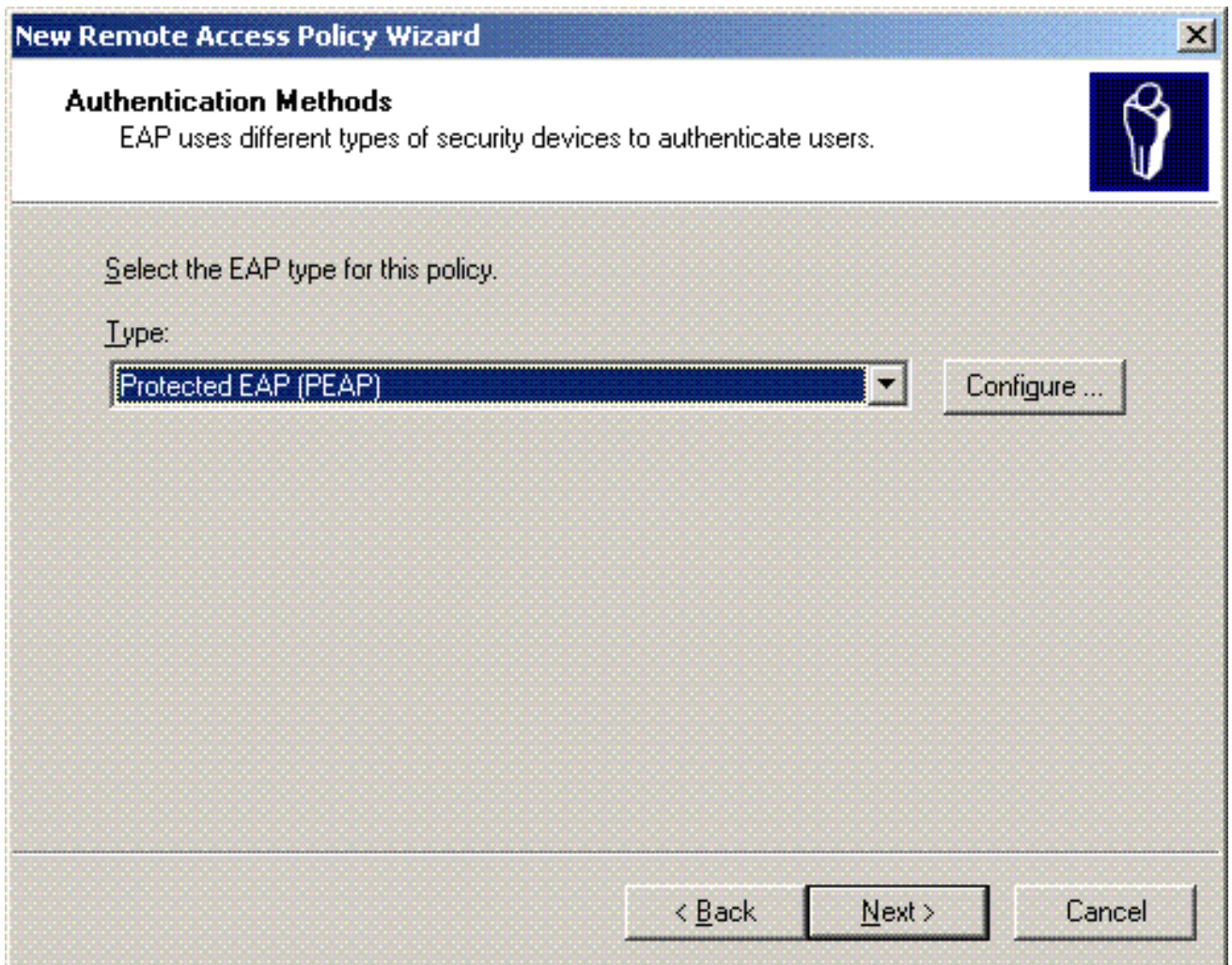
< **B**ack   **N**ext >   Cancel

14. Na próxima página, escolha **Usuário** para aplicar esta política de acesso remoto à lista de usuários.

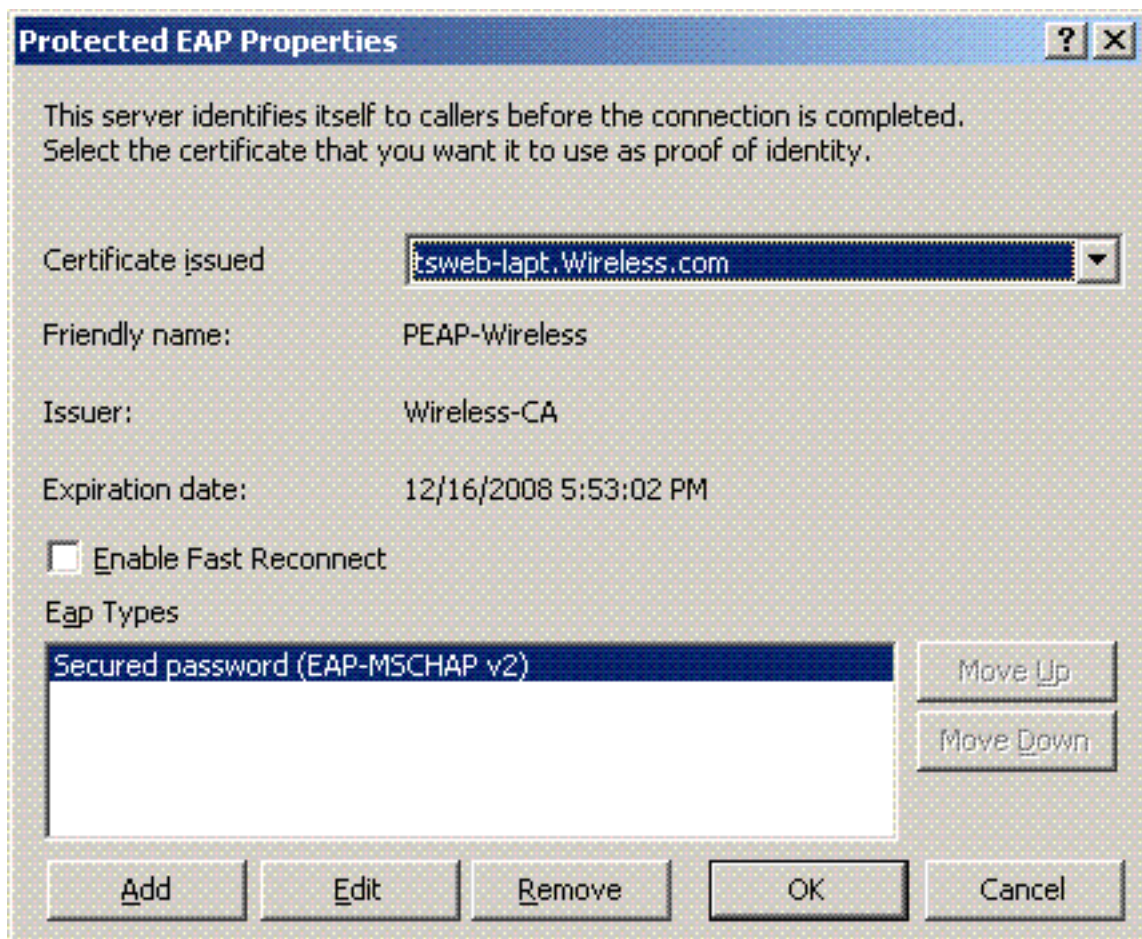




15. Em Authentication Methods, escolha **Protected EAP (PEAP)** e clique em **Configure**.

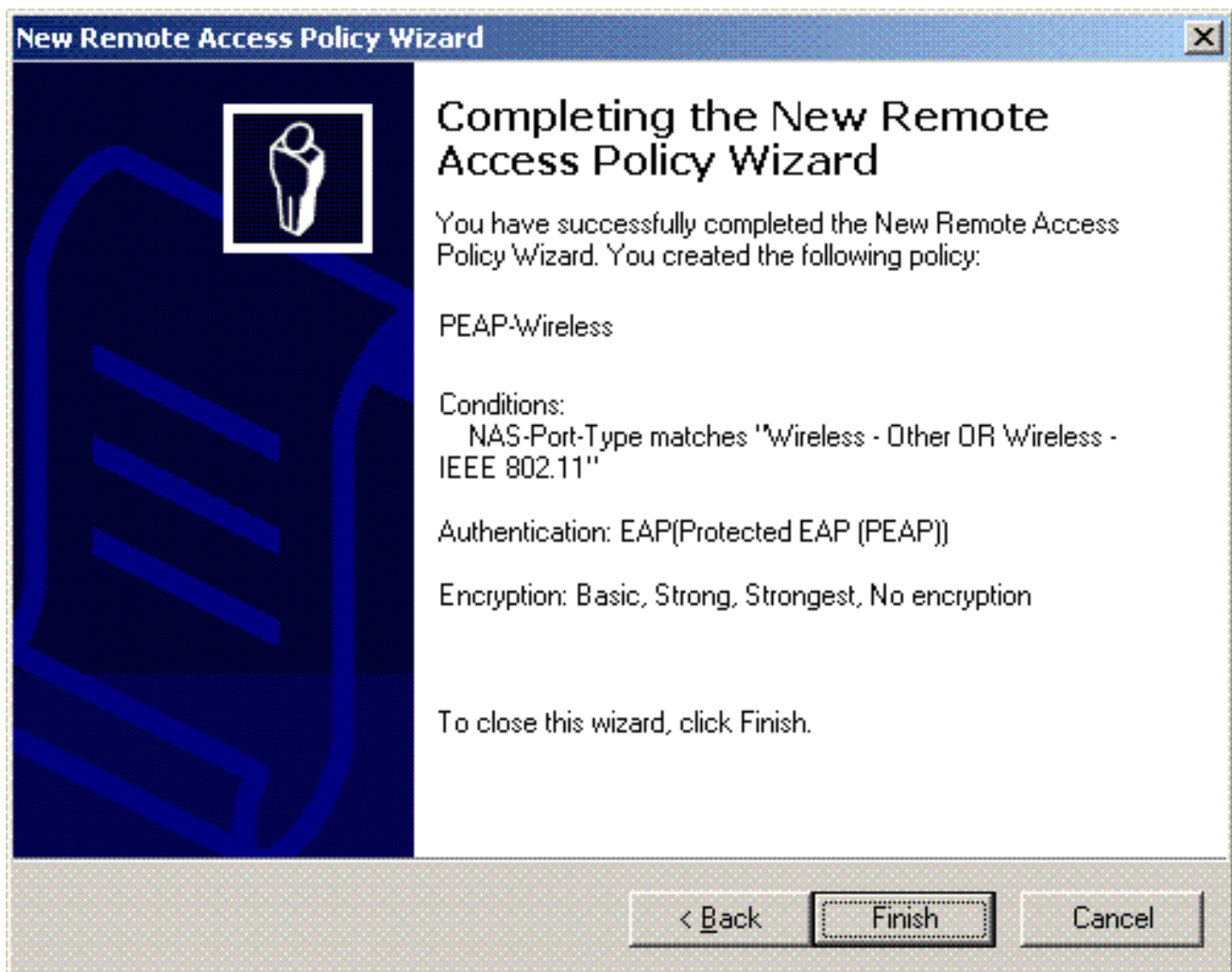


16. Na página **Protected EAP Properties**, escolha o certificado apropriado no menu suspenso Certificate Issued e clique em

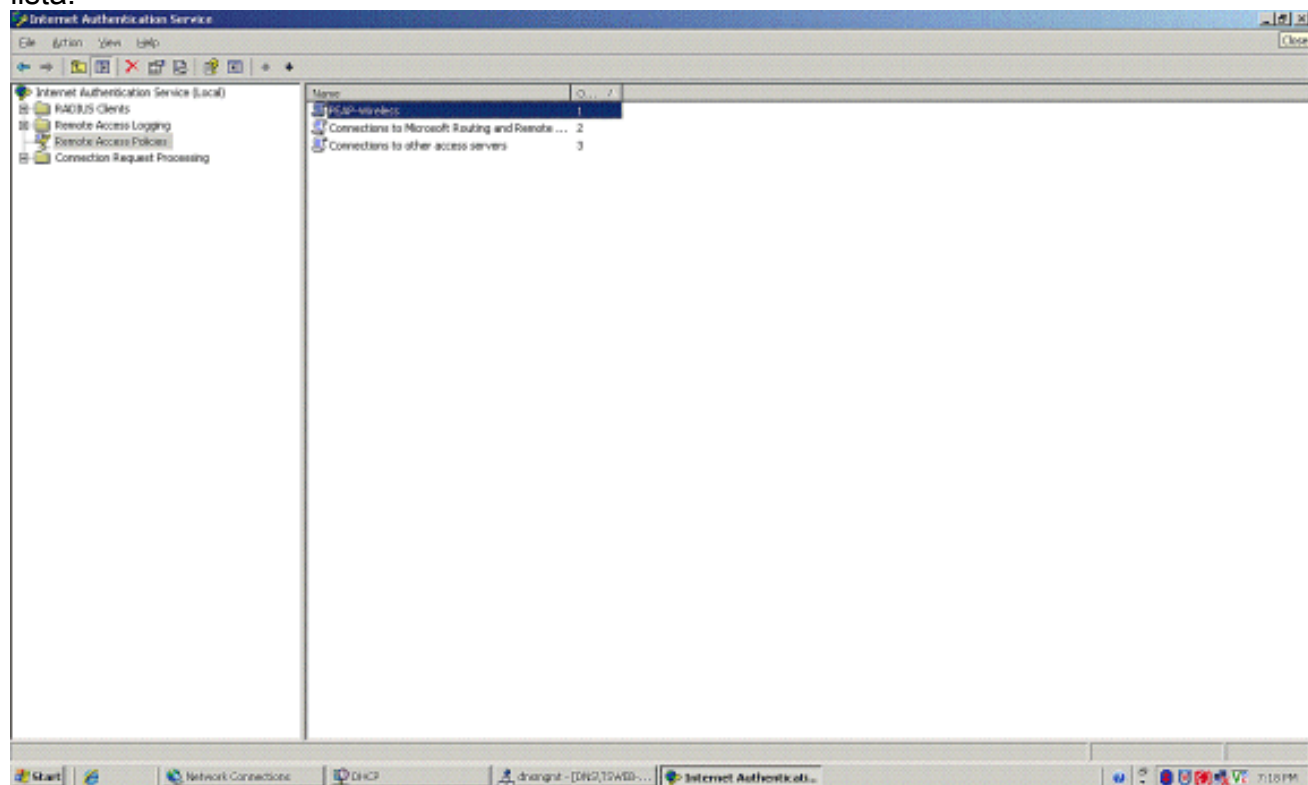


OK.

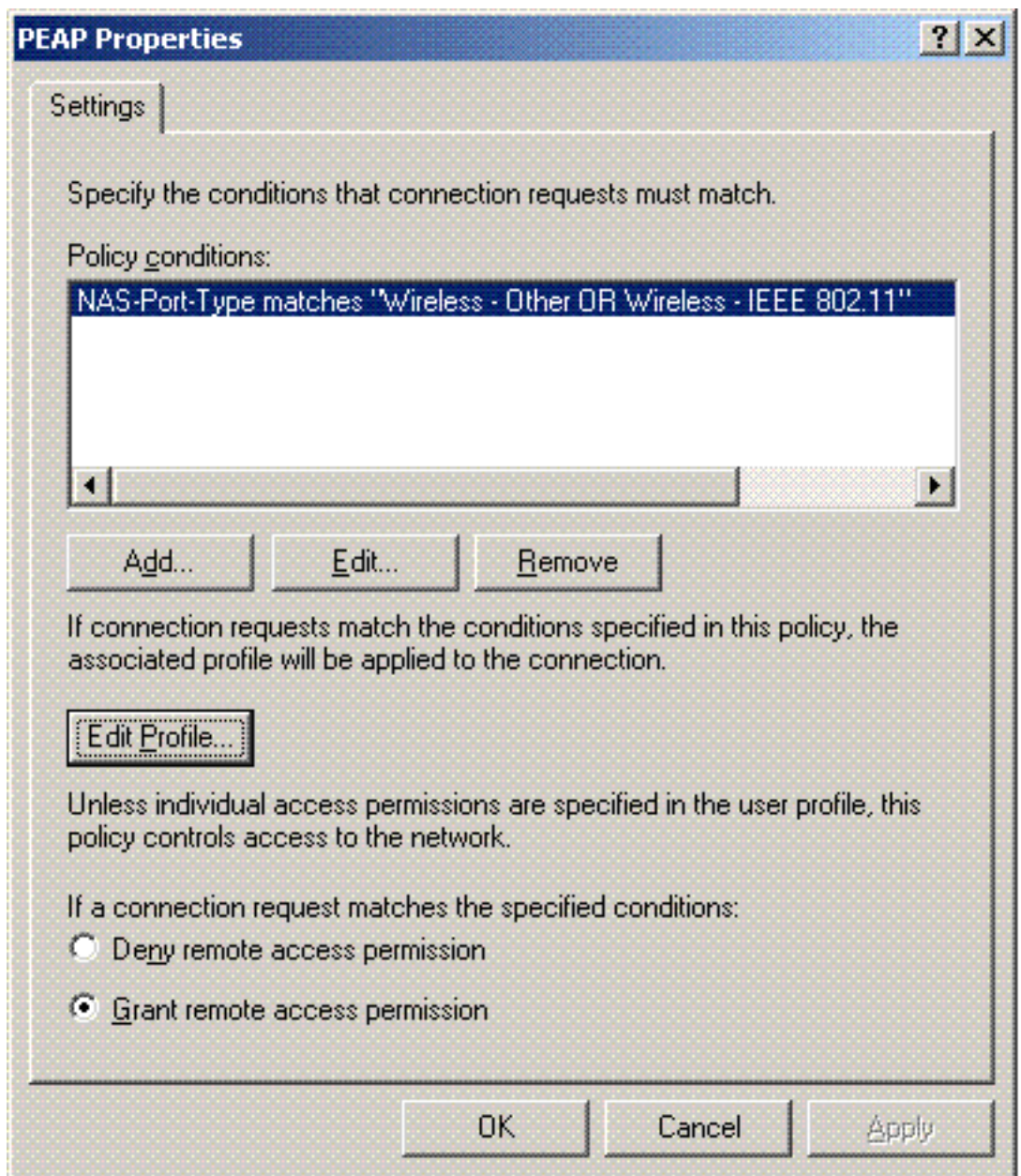
17. Verifique os detalhes da política de acesso remoto e clique em **Finish**.



18. A política de acesso remoto foi adicionada à lista.



19. Clique com o botão direito do mouse na diretiva e clique em **Propriedades**. Escolha "Conceder permissão de acesso remoto" em "Se uma solicitação de conexão corresponder às condições"



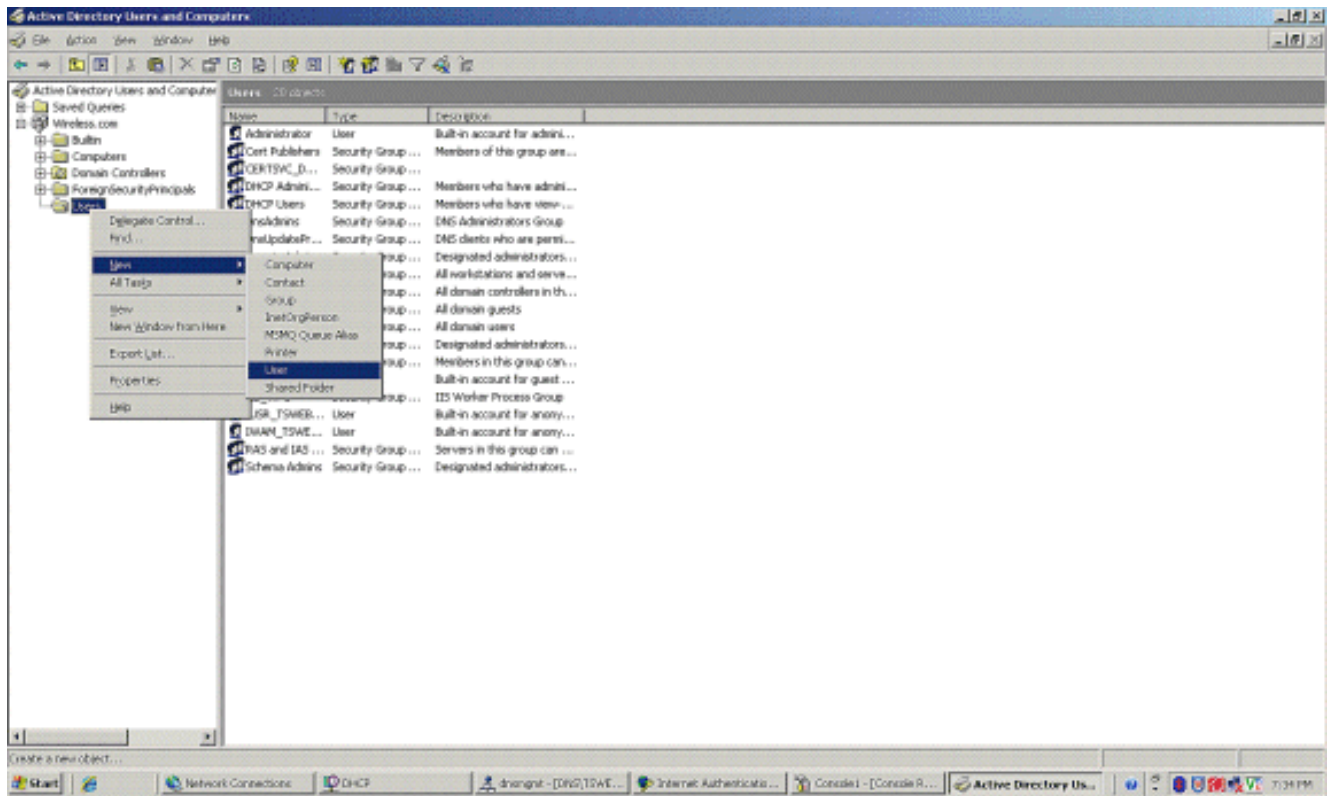
especificadas".

## [Adicionar usuários ao Ative Directory](#)

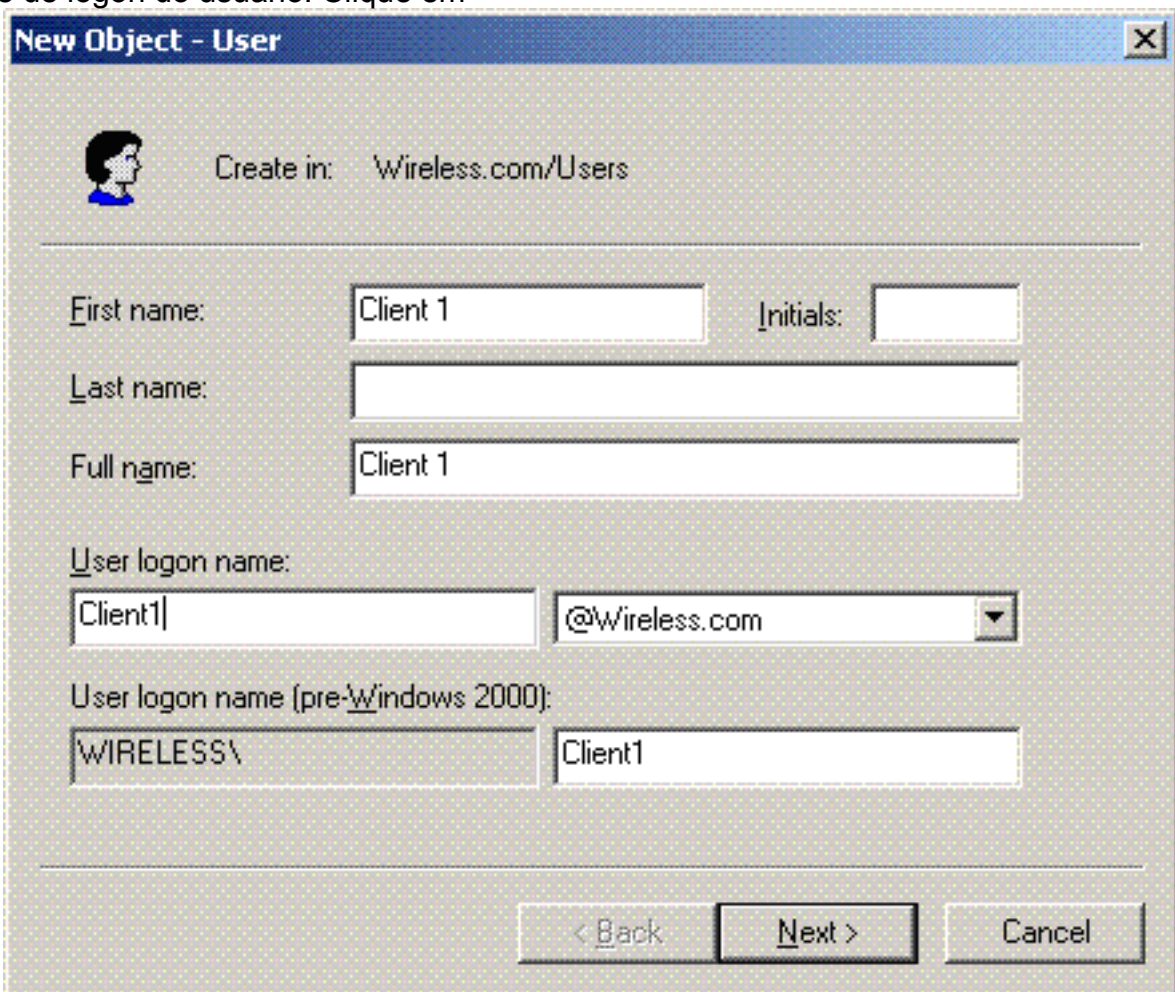
Nessa configuração, o banco de dados do usuário é mantido no Ative Directory.

Para adicionar usuários ao banco de dados do Ative Directory, siga estas etapas:

1. Na árvore do console Ative Directory 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 **WirelessUser** no campo Nome e **WirelessUser** 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

**New Object - User** [X]

 Create in: Wireless.com/Users

---

Password: [.....]

Confirm password: [.....]

User must change password at next logon

User cannot change password

Password never expires

Account is disabled


---

< Back   Next >   Cancel

Avançar.

4. Na caixa de diálogo Novo objeto - usuário, clique em

**New Object - User** [X]

 Create in: Wireless.com/Users

---

When you click Finish, the following object will be created:

Full name: Client 1

User logon name: Client1@Wireless.com

---

< Back   Finish   Cancel

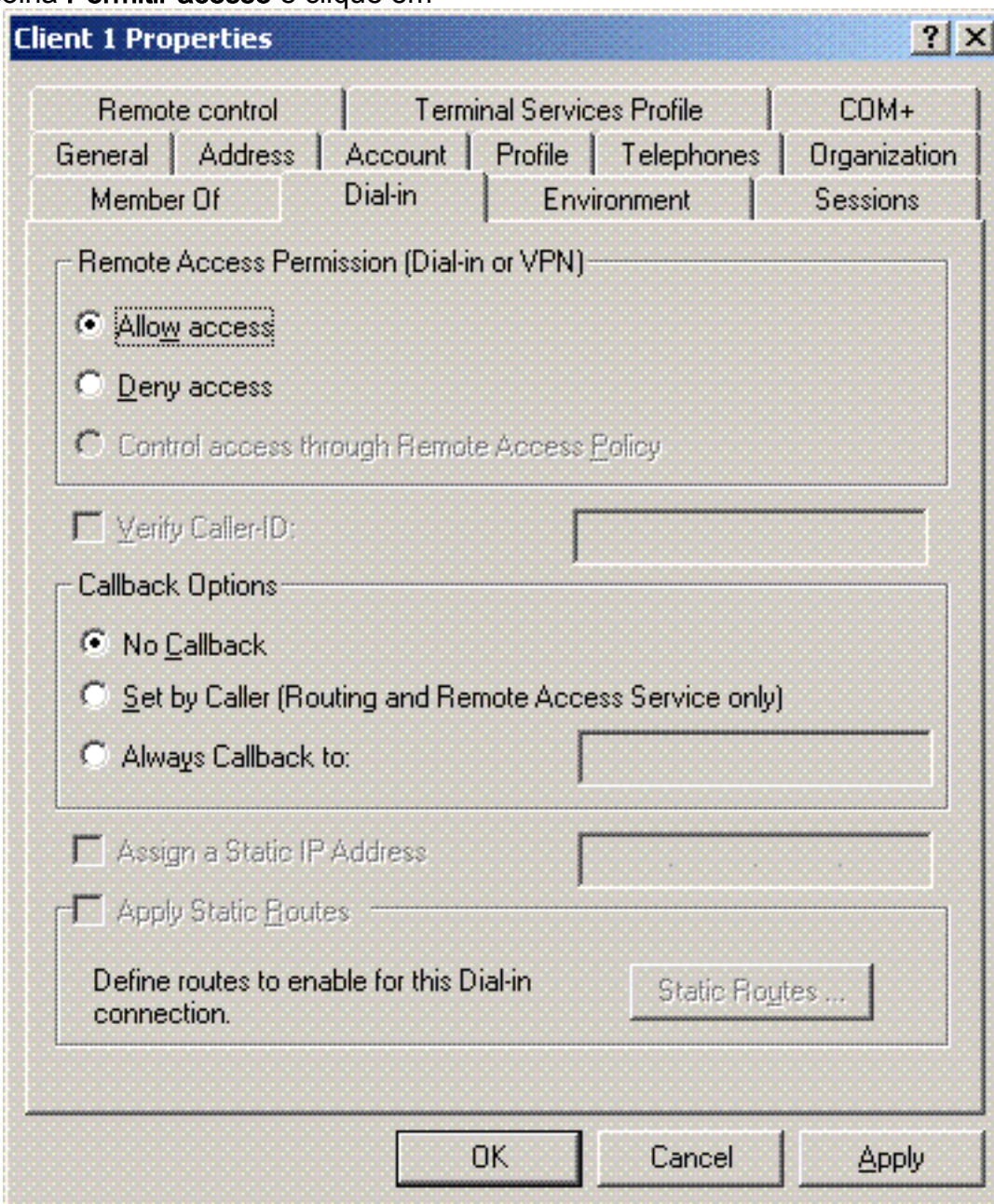
Concluir.

5. Repita as etapas de 2 a 4 para criar contas de usuário adicionais.

## Permitir acesso sem fio aos usuários

Conclua estes passos:

1. Na árvore do console Usuários e computadores do Active 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.

## Configurar a controladora Wireless LAN e APs leves

Agora, configure os dispositivos Wireless para essa configuração. Isso inclui a configuração de controladores de LAN sem fio, APs leves e clientes sem fio.

## Configurar a WLC para autenticação RADIUS através do servidor RADIUS MS IAS



Primeiro configure o WLC para usar o MS IAS como o servidor de autenticação. A WLC precisa ser configurada para encaminhar as credenciais do usuário a um servidor RADIUS externo. O servidor RADIUS externo valida as credenciais do usuário e fornece acesso aos clientes Wireless. Para fazer isso, adicione o servidor MS IAS como um servidor RADIUS na página **Segurança > Autenticação RADIUS**.

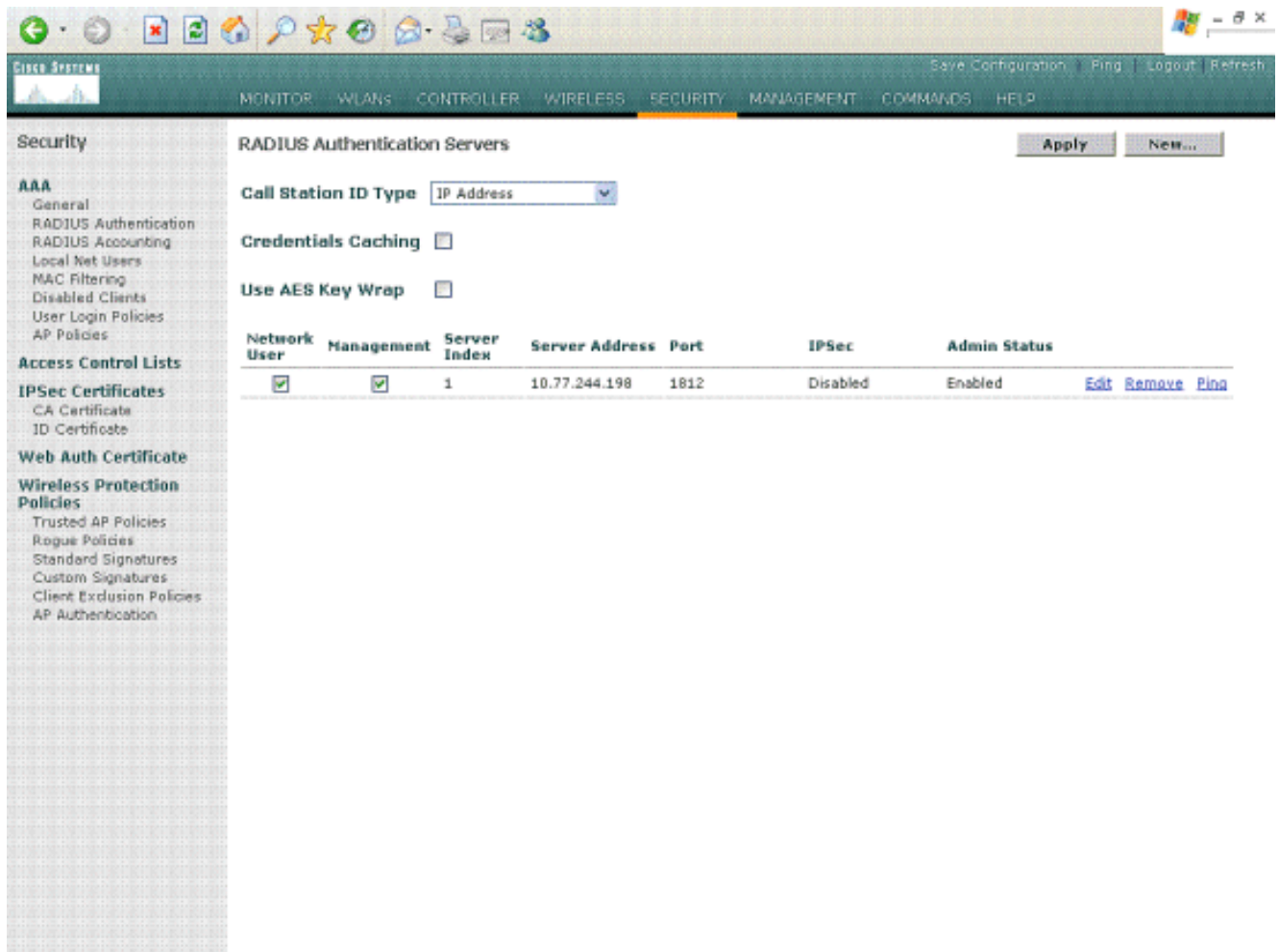
Conclua estes passos:

1. Escolha **Security** e **RADIUS Authentication** na GUI da controladora para exibir a página RADIUS Authentication Servers. Em seguida, clique em **New** para definir um servidor RADIUS.

The screenshot shows the Cisco Systems GUI for configuring a new RADIUS Authentication Server. The page is titled "RADIUS Authentication Servers > New" and includes the following fields and options:

- Server Index (Priority):** 1
- Server IP Address:** 10.77.244.198
- Shared Secret Format:** ASCII
- Shared Secret:** [Redacted]
- Confirm Shared Secret:** [Redacted]
- Key Wrap:**
- Port Number:** 1812
- Server Status:** Enabled
- Support for RFC 3576:** Enabled
- Retransmit Timeout:** 2 seconds
- Network User:**  Enable
- Management:**  Enable
- IPsec:**  Enable

2. Defina os parâmetros do servidor RADIUS na página **Servidores de autenticação RADIUS > Novo**. Esses parâmetros incluem o endereço IP do servidor RADIUS, o segredo compartilhado, o número da porta e o status do servidor. As caixas de seleção Network User and Management determinam se a autenticação baseada em RADIUS se aplica a usuários de gerenciamento e de rede. Este exemplo usa o MS IAS como o servidor RADIUS com o endereço IP 10.77.244.198.



3. Clique em Apply.
4. O servidor MS IAS foi adicionado à WLC como um servidor Radius e pode ser usado para autenticar clientes Wireless.

## [Configurar uma WLAN para os clientes](#)

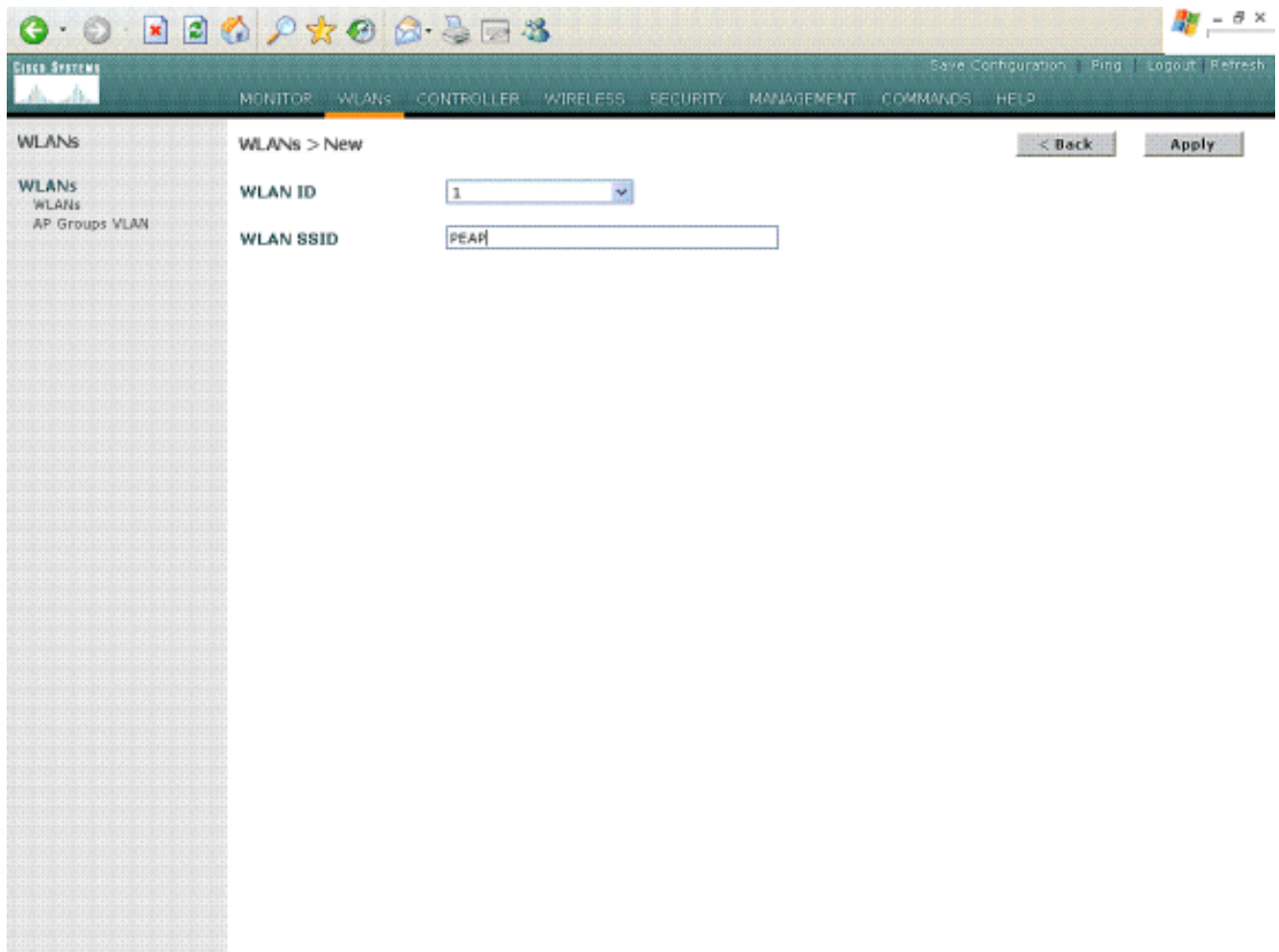
Configure o SSID (WLAN) ao qual os clientes Wireless se conectam. Neste exemplo, crie o SSID e nomeie-o como **PEAP**.

Defina a Autenticação da Camada 2 como WPA2 para que os clientes executem a autenticação baseada em EAP (PEAP-MSCHAPv2 neste caso) e usem AES como o mecanismo de criptografia. Deixe todos os outros valores em seus padrões.

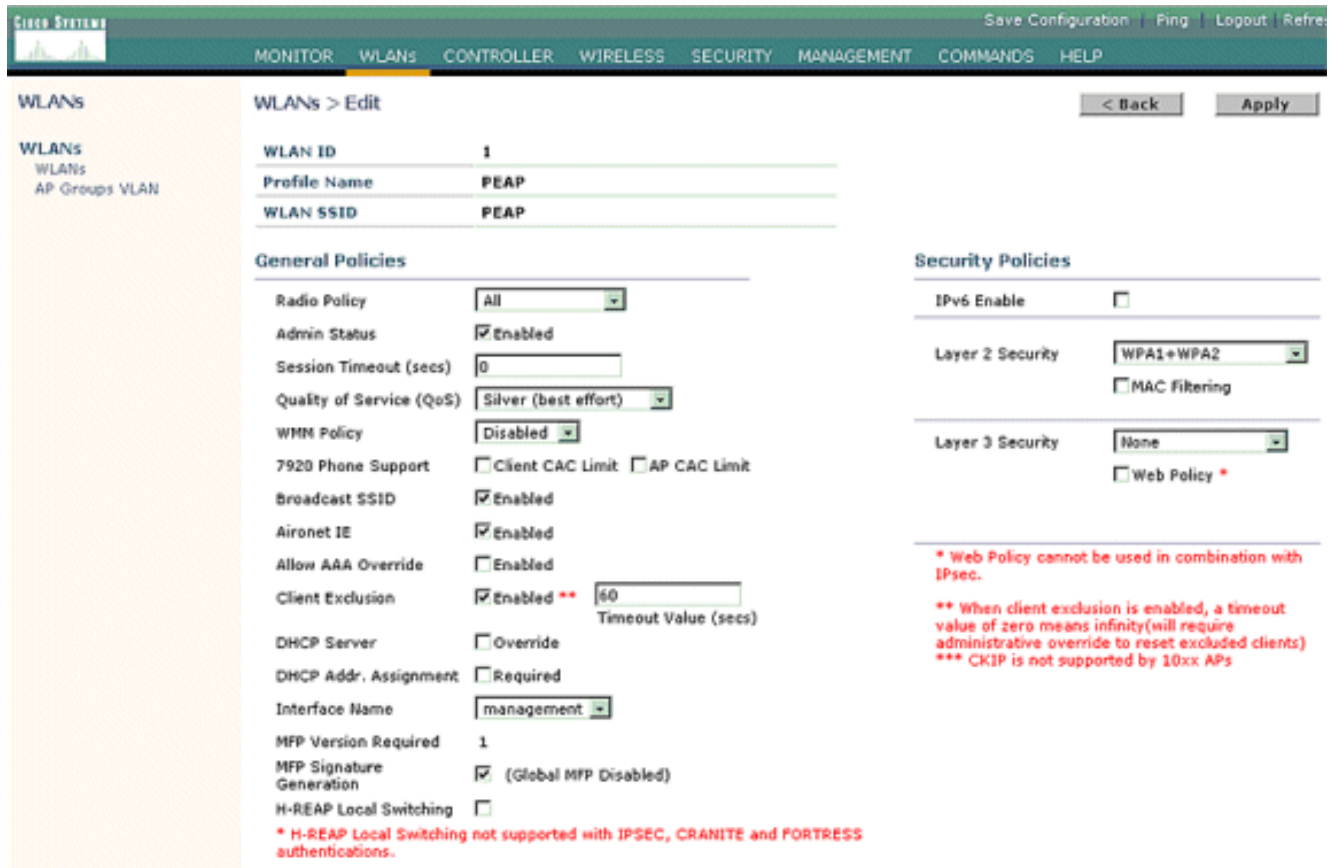
**Observação:** este documento vincula a WLAN às interfaces de gerenciamento. Quando há várias VLANs na rede, você pode criar uma VLAN separada e vinculá-la ao SSID. Para obter informações sobre como configurar VLANs em WLCs, consulte [Exemplo de Configuração de VLANs em Wireless LAN Controllers](#).

Para configurar uma WLAN na WLC, siga estes passos:

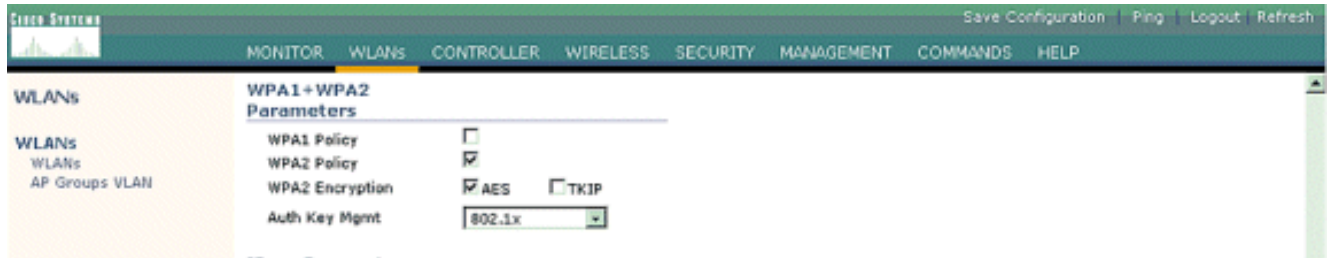
1. Clique em **WLANs** na GUI do controlador para exibir a página WLANs. Esta página lista as WLANs que existem na controladora.
2. Escolha **New** para criar uma nova WLAN. Insira o ID da WLAN e o SSID da WLAN para a WLAN e clique em **Apply**.



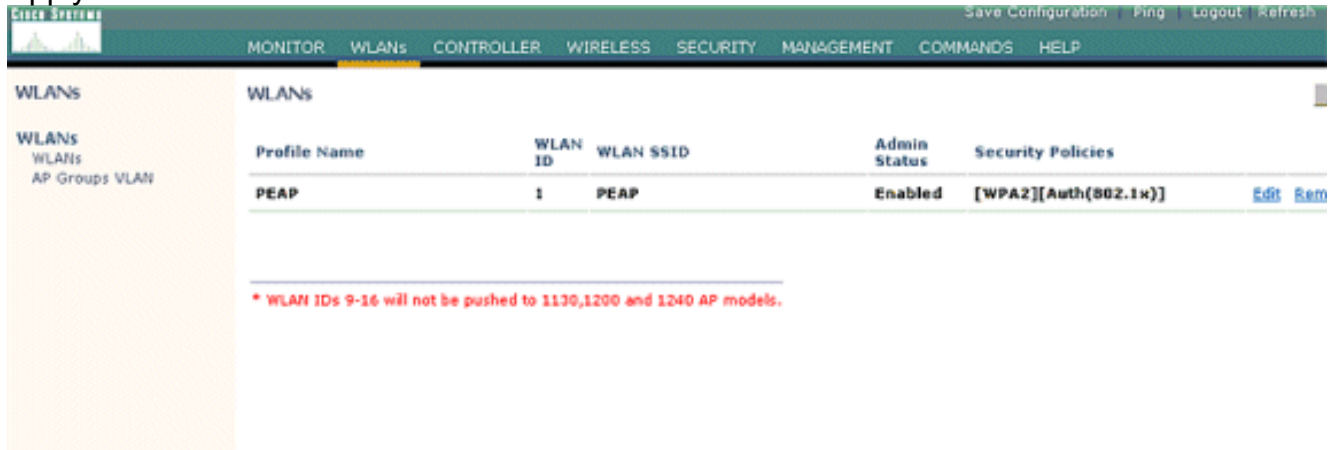
3. Quando você criar uma nova WLAN, a página **WLAN > Edit** da nova WLAN será exibida. Nesta página você pode definir vários parâmetros específicos para esta WLAN que incluem Políticas Gerais, Servidores RADIUS, Políticas de Segurança e Parâmetros 802.1x.



4. Verifique **Admin Status** em General Policies para habilitar a WLAN. Se você quiser que o AP transmita o SSID em seus quadros beacon, marque **Broadcast SSID**.
5. Em Layer 2 Security, selecione **WPA1+WPA2**. Isso ativa a WPA na WLAN. Role para baixo na página e escolha a política WPA. Este exemplo usa a criptografia WPA2 e AES. Escolha o servidor RADIUS apropriado no menu suspenso em Servidores RADIUS. Neste exemplo, use **10.77.244.198** (endereço IP do servidor MS IAS). Os outros parâmetros podem ser modificados com base no requisito da rede WLAN.



6. Clique em **Apply**.



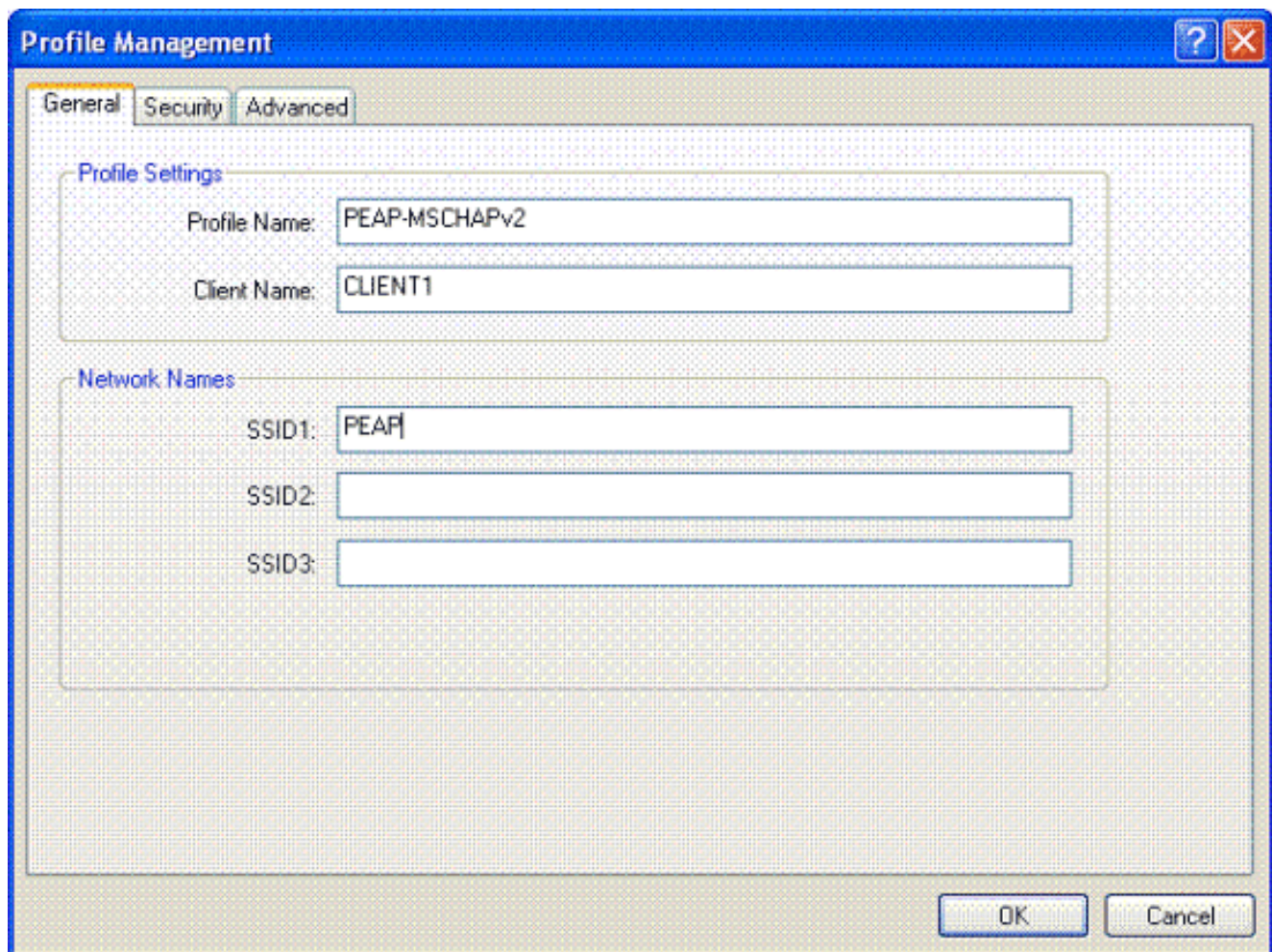
## [Configurar os clientes sem fio](#)

### [Configurar os clientes sem fio para a autenticação PEAP-MS CHAPv2](#)

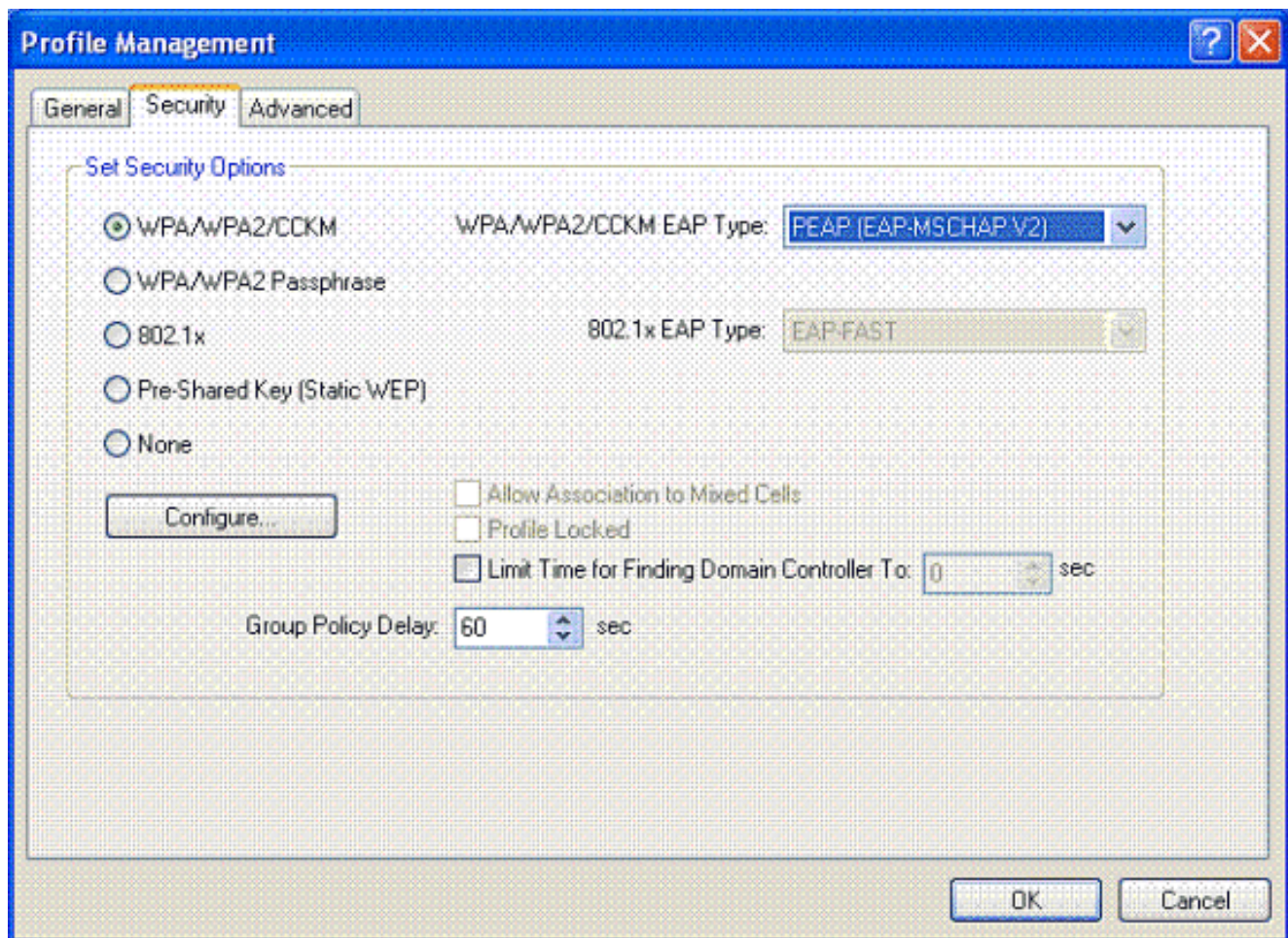
Este exemplo fornece informações sobre como configurar o cliente Wireless com o Cisco Aironet Desktop Utility. Antes de configurar o adaptador cliente, certifique-se de que a versão mais recente do firmware e do utilitário seja usada. Encontre a versão mais recente do firmware e dos utilitários na página Wireless downloads (Downloads sem fio) em Cisco.com.

Para configurar o adaptador cliente Wireless Cisco Aironet 802.11 a/b/g com o ADU, siga estas etapas:

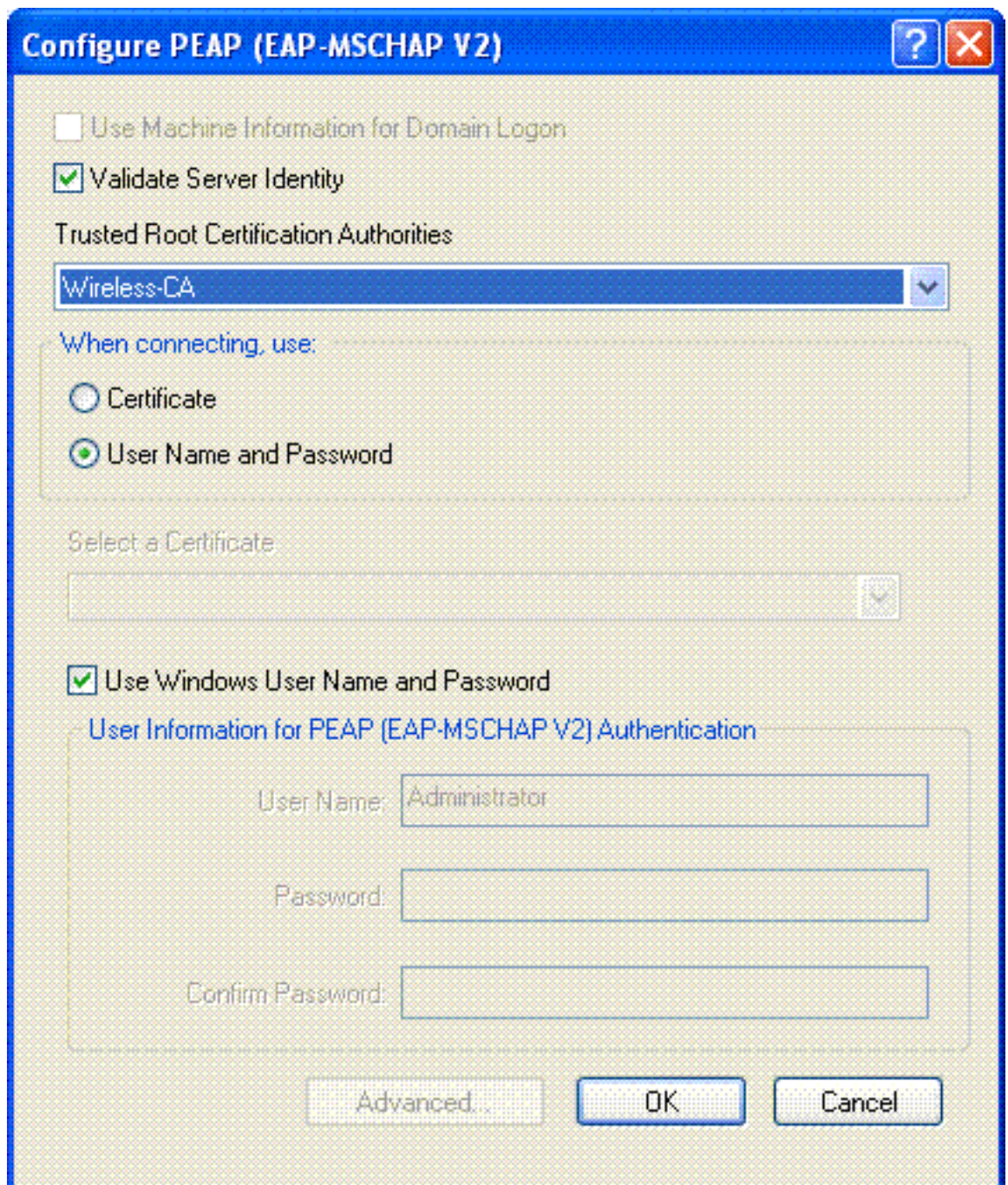
1. Abra o Aironet Desktop Utility.
2. Clique em **Gerenciamento de perfil** e clique em **Novo** para definir um perfil.
3. Na guia General (Geral), insira o Profile name (Nome do perfil) e o SSID (SSID). Neste exemplo, use o SSID que você configurou no WLC (PEAP).



4. Escolha a guia Security; escolha **WPA/WPA2/CCKM**; em WPA/WPA2/CCKM EAP, digite **PEAP [EAP-MSCHAPv2]** e clique em **Configure**.



5. Escolha **Validate Server Certificate** e **Wireless-CA** no menu suspenso Trusted Root Certificate

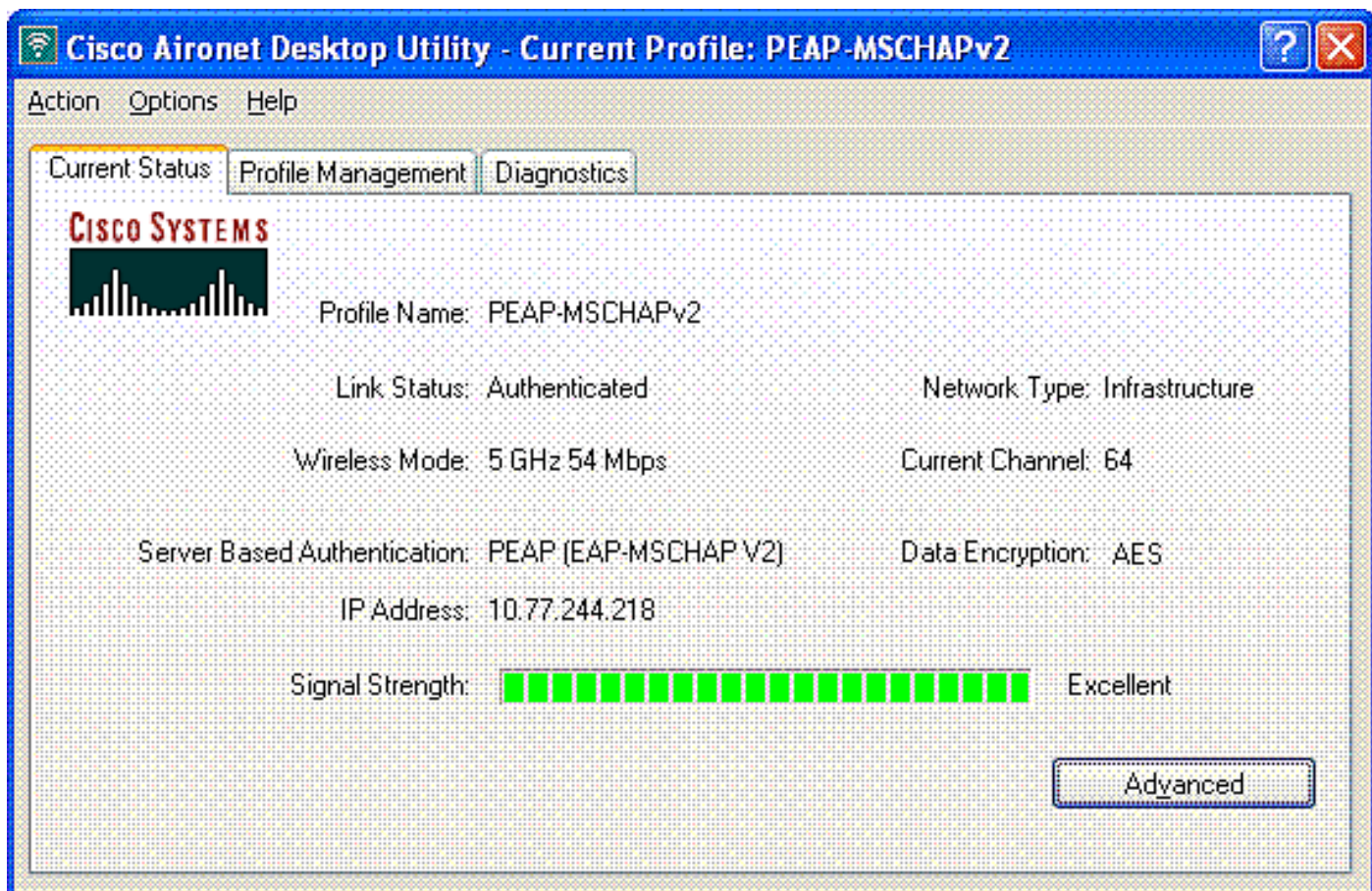


Authorities.

6. Clique em **OK** e ative o perfil. **Observação:** quando você usa o EAP Protegido-Microsoft Challenge Handshake Authentication Protocol Versão 2 (PEAP-MSCHAPv2) com o Microsoft XP SP2 e a placa Wireless é gerenciada pelo Microsoft Wireless Zero Configuration (WZC), você deve aplicar o hotfix KB885453 da Microsoft. Isso evita vários problemas de autenticação relacionados ao PEAP Fast Resume.

## [Verificar e solucionar problemas](#)

Para verificar se a configuração funciona como esperado, ative o perfil PEAP-MSCHAPv2 no Wireless client Client1.



Quando o perfil PEAP-MSCHAPv2 é ativado no ADU, o cliente executa a autenticação aberta 802.11 e, em seguida, executa a autenticação PEAP-MSCHAPv2. Este é um exemplo de autenticação PEAP-MSCHAPv2 bem-sucedida.

Use os comandos debug para entender a sequência de eventos que ocorrem.

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

Esses comandos debug no Controller de LAN Wireless são úteis.

- **debug dot1x events enable** — Para configurar a depuração de eventos 802.1x
- **debug aaa events enable** — Para configurar a depuração de eventos AAA
- **debug mac addr <mac address>** — Para configurar a depuração MAC, use o comando debug mac
- **debug dhcp message enable** — Para configurar a depuração de mensagens de erro DHCP

Estas são as saídas de exemplo dos comandos **debug dot1x events enable** e **debug client <mac address>**.

**debug dot1x events enable:**

```
Tue Dec 18 06:58:45 2007: 00:40:96:ac:e6:57 Received EAPOL START from
mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:45 2007: 00:40:96:ac:e6:57 Sending EAP-Request/Identity to
mobile 00:40:96:ac:e6:57 (EAP Id 2)
Tue Dec 18 06:58:45 2007: 00:40:96:ac:e6:57 Received Identity Response (count=2) from
mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for
```





**mobile 00:40:96:ac:e6:57 (EAP Id 13)**  
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 **Sending default RC4 key to**  
**mobile 00:40:96:ac:e6:57**  
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 **Sending Key-Mapping RC4 key to**  
**mobile 00:40:96:ac:e6:57**  
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 **Received Auth Success while in**  
**Authenticating state for mobile 00:40:96:ac:e6:57**

## **debug mac addr <MAC Address>:**

Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Association received from**  
**mobile 00:40:96:ac:e6:57 on AP 00:0b:85:51:5a:e0**  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 STA: 00:40:96:ac:e6:57 -  
rates (8): 12 18 24 36 48 72 96 108 0 0 0 0 0 0  
Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 RUN (20)**  
**Change state to START (0)**  
Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 START (0)**  
**Initializing policy**  
Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 START (0)**  
**Change state to AUTHCHECK (2)**  
Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 AUTHCHECK (2)**  
**Change state to 8021X\_REQD (3)**  
Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 8021X\_REQD (3)**  
Plumbed mobile LWAPP rule on AP 00:0b:85:51:5a:e0  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Changing state for**  
**mobile 00:40:96:ac:e6:57 on AP 00:0b:85:51:5a:e0 from Associated to Associated**  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Stopping deletion of  
Mobile Station: 00:40:96:ac:e6:57 (callerId: 48)  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Sending Assoc Response to  
station 00:40:96:ac:e6:57 on BSSID 00:0b:85:51:5a:e0 (status 0)  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Changing state for  
mobile 00:40:96:ac:e6:57 on AP 00:0b:85:51:5a:e0 from Associated to Associated  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 10.77.244.218 Removed NPU entry.  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 dot1x - moving  
mobile 00:40:96:ac:e6:57 into Connecting state  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Sending EAP-**  
**Request/Identity to mobile 00:40:96:ac:e6:57 (EAP Id 1)**  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Received EAPOL START from**  
**mobile 00:40:96:ac:e6:57**  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **EAP State update from**  
**Connecting to Authenticating for mobile 00:40:96:ac:e6:57**  
Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 dot1x -**  
**moving mobile 00:40:96:ac:e6:57 into Authenticating state**  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57  
Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57  
Processing Access-Challenge for mobile 00:40:96:ac:e6:57  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57  
Entering Backend Auth Req state (id=3) for mobile 00:40:96:ac:e6:57  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57  
**Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 3)**  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57  
**Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 3, EAP Type 25)**  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57  
Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57  
Processing Access-Challenge for mobile 00:40:96:ac:e6:57  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57  
Entering Backend Auth Req state (id=4) for mobile 00:40:96:ac:e6:57  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57  
Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 4)  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57

Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 4, EAP Type 25)  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57  
Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57  
Processing Access-Challenge for mobile 00:40:96:ac:e6:57  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57  
Entering Backend Auth Req state (id=5) for mobile 00:40:96:ac:e6:57  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57  
Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 5)  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57  
Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 5, EAP Type 25)  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57  
Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57  
Processing Access-Challenge for mobile 00:40:96:ac:e6:57  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57  
Entering Backend Auth Req state (id=6) for mobile 00:40:96:ac:e6:57  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57  
Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 6)  
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57  
Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 9, EAP Type 25)  
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57  
Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57  
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57  
Processing Access-Challenge for mobile 00:40:96:ac:e6:57  
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57  
Entering Backend Auth Req state (id=10) for mobile 00:40:96:ac:e6:57  
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57  
Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 10)  
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57  
Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 10, EAP Type 25)  
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57  
Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57  
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57  
Processing Access-Challenge for mobile 00:40:96:ac:e6:57  
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57  
Entering Backend Auth Req state (id=11) for mobile 00:40:96:ac:e6:57  
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57  
**Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 11)**  
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57  
**Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 11, EAP Type 25)**  
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57  
Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57  
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57  
**Processing Access-Accept for mobile 00:40:96:ac:e6:57**  
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57  
**Creating a new PMK Cache Entry for station 00:40:96:ac:e6:57 (RSN 0)**  
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57  
**Sending EAP-Success to mobile 00:40:96:ac:e6:57 (EAP Id 12)**  
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57  
**Sending default RC4 key to mobile 00:40:96:ac:e6:57**  
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57  
**Sending Key-Mapping RC4 key to mobile 00:40:96:ac:e6:57**  
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218  
8021X\_REQD (3) **Change state to L2AUTHCOMPLETE (4)**  
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218  
L2AUTHCOMPLETE (4) Plumbed mobile LWAPP rule on AP 00:0b:85:51:5a:e0  
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218  
L2AUTHCOMPLETE (4) Change state to RUN (20)  
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN  
(20) Reached PLUMBFASPATH: from line 4041  
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN  
(20) Replacing Fast Path rule  
type = Airespace AP Client

```
on AP 00:0b:85:51:5a:e0, slot 0, interface = 2
ACL Id = 255, Jumbo Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 5006
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN (20)
Card = 0 (slot 0), InHandle = 0x00000000,
OutHandle = 0x00000000, npuCryptoFlag = 0x0000
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN
(20) Successfully plumbed mobile rule (ACL ID 255)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN
(20) Reached RETURN: from line 4041
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 Entering Backend
Auth Success state (id=12) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 Received Auth Success
while in Authenticating state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 dot1x -
moving mobile 00:40:96:ac:e6:57 into Authenticated state
```

**Observação:** se você usar o Microsoft Supplicant para autenticar com um Cisco Secure ACS para autenticação PEAP, o cliente possivelmente não será autenticado com êxito. Às vezes, a conexão inicial pode ser autenticada com êxito, mas as tentativas subsequentes de autenticação de conexão rápida não se conectam com êxito. Esse é um problema conhecido. Os detalhes desse problema e a correção para o mesmo estão disponíveis [aqui](#) .

## [Informações Relacionadas](#)

- [PEAP em redes sem fio unificadas com ACS 4.0 e Windows 2003](#)
- [Exemplo de Configuração de Autenticação EAP com WLAN Controllers \(WLC\)](#)
- [Atualização do software da controladora Wireless LAN \(WLC\) para as versões 3.2, 4.0 e 4.1](#)
- [Guias de configuração de Cisco 4400 Series Wireless LAN Controllers](#)
- [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.