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

# Contents

Introduction **Prerequisites** Requirements Componentes Utilizados Diagrama de Rede **Conventions** Instalação do Windows Enterprise 2003 com IIS, Certificate Authority, DNS, DHCP (DC\_CA) DC CA (wireless-essdemoca) Configuração do Windows Standard 2003 com Cisco Secure ACS 4.0 Instalação e configuração básicas Instalação do Cisco Secure ACS 4.0 Configuração do controlador Cisco LWAPP Crie a configuração necessária para WPA2/WPA Autenticação EAP-TLS Instalar o Snap-in Modelos de Certificado Crie o Modelo de Certificado para o Servidor Web ACS Ativar o novo modelo de certificado do servidor Web ACS Configuração do certificado ACS 4.0 Configurar certificado exportável para ACS Instale o certificado no software ACS 4.0 Configuração do CLIENTE para EAP-TLS usando Windows Zero Touch Executar uma instalação e configuração básicas Configure a conexão de rede sem fio Informações Relacionadas

# **Introduction**

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

**Observação:** para obter mais informações sobre a implantação de conexões sem fio seguras, consulte o <u>site da Microsoft Wi-Fi na Web e o Cisco SAFE Wireless Blueprint</u>.

# **Prerequisites**

# **Requirements**

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

Para obter informações sobre instalação e configuração iniciais dos Cisco 4400 Series Controllers, consulte o <u>Guia de início rápido: Cisco 4400 Series Wireless LAN Controllers.</u> Para obter informações sobre instalação e configuração iniciais dos Cisco 2000 Series Controllers, consulte o <u>Guia de início rápido: Cisco 2000 Series Wireless LAN Controllers.</u>

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

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

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

# **Componentes Utilizados**

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

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

# Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:

Topologia de laboratório sem fio segura da Cisco



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

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

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 <u>Convenções de Dicas Técnicas da Cisco para obter mais informações sobre</u> <u>convenções de documentos.</u>

Instalação do Windows Enterprise 2003 com IIS, Certificate Authority, DNS, DHCP (DC\_CA)

DC\_CA (wireless-essdemoca)

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

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

Conclua estes passos para configurar DC\_CA para estes serviços:

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

## Passo 1: Executar instalação e configuração básicas

Conclua estes passos:

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

Passo 2: Configurar o computador como um controlador de domínio

- 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 **Avançar**.
- 6. Na página Instalar ou Configurar DNS, selecione Não, apenas instalar e configurar DNS neste computador e clique em Avançar.
- 7. Na página Novo nome de domínio, digite wireless demo.local e clique em Avançar.
- 8. Na página Nome de domínio NetBIOS, digite o nome do NetBIOS de domínio como **demo sem fio** e clique em **Avançar**.

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

#### Avançar.

Active Directory Installation Wizard	×
<b>Database and Log Folders</b> Specify the folders to contain the Active Directory database and log i	files.
For best performance and recoverability, store the database and the hard disks.	log on separate
Where do you want to store the Active Directory database?	
Database folder:	
C:\WINDOWS\NTDS	B <u>r</u> owse
Where do you want to store the Active Directory log? Log folder:	
C:\WINDOWS\NTDS	Br <u>o</u> wse
< <u>B</u> ack <u>N</u> ex	(t) Cancel

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

Active Directory Installation Wizard
Specify the folder to be shared as the system volume.
The SYSVOL folder stores the server's copy of the domain's public files. The contents of the SYSVOL folder are replicated to all domain controllers in the domain.
The SYSVOL folder must be located on an NTFS volume.
Enter a location for the SYSVOL folder.
Eolder location:
C:\WINDOWS\SYSVOL B_owse
<u> </u>

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

Active Directory Installation Wizard		
Permissions Select default permissions for user and group objects.		
Some server programs, such as Windows NT Remote Access Service, read information stored on domain controllers.		
Permissions compatible with pre-Windows 2000 server operating systems Select this option if you run server programs on pre-Windows 2000 server operating systems or on Windows 2000 or Windows Server 2003 operating systems that are members of pre-Windows 2000 domains.		
<ul> <li>Anonymous users can read information on this domain.</li> <li>Permissions compatible only with Windows 2000 or Windows Server 2003 operating systems</li> </ul>		
Select this option if you run server programs only on Windows 2000 or Windows Server 2003 operating systems that are members of Active Directory domains. Only authenticated users can read information on this domain.		
< <u>B</u> ack <u>N</u> ext> Cancel		

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

<b>ummary</b> Reviewiand	confirm the options	you selecte	ed.		Ś
You chose I	0:				
The new do	main name is examp	ole.com. Thi	s is also the nar	ne of the new fore	est. 🔺
The NetBIC	S name of the doma	ain is EXAMI	PLE		_
Database fo	lder: C:\WINDOWS	SANTDS			
Log file fold	er: C:\WINDOWS\	ITDS			
SYSVUL to	der: C:\WINDUWS	SYSVUL			
The DNS s will be confi	ervice will be installe gured to use this DN	d and config IS server as	gured on this co its preferred D1	mputer. This com NS server.	iputer
The passwo	and of the new doma	in administra	ator will be the s	ame as the passv	vord of
the administ	rator of this compute	er.			-
To change	an option, click Bac	k. To beain	the operation, o	lick Next	
	• • • • •				
			< <u>B</u> ack	<u>N</u> ext⇒	Cance

- 14. Na página Concluindo o Assistente de Instalação do Ative Diretory, clique em Concluir.
- 15. Quando solicitado a reiniciar o computador, clique em Reiniciar agora.

#### Passo 3: Aumente o nível funcional do domínio

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

aise Dom	in Functional Lev	vel 📕		×
Domain nar	ne:			
example.co	m			
Currenit don	nain functional level			
Windows 2	000 mative			
Callant an a		the set has set		
Windows 3	Server 2003	Decinical Romot.		1
After an de	rou raise the domain main functional leve	i functional level, it canno Is, click Help.	( De reversed. For more in	nronnation
		Base	Cancel	Help

domínio.\_\_\_\_

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

## Passo 4: Instalar e configurar o DHCP

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

New Scope Wizard	
Scope Name You have to provide an identifying scope name. You also have the option of providing a description.	(J)
Type a name and description for this scope. This information helps you quickly identi how the scope is to be used on your network.	ify
Name: CorpNet	
Description:	
<u>≺Back</u> <u>Next&gt;</u> 0	Cancel

 Clique em Avançar e preencha estes parâmetros:Endereço IP inicial—172.16.100.1Endereço IP final—172.16.100.254Comprimento—24Máscara de subrede—255.255.255.0

New Scope Wizard
IP Address Range You define the scope address range by identifying a set of consecutive IP addresses.
Enter the range of addresses that the scope distributes. <u>Start IP address:</u> 172 . 16 . 100 . 1 <u>End IP address:</u> 172 . 16 . 100 . 254
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: 24 📑 Subnet mask: 255 . 255 . 0
< <u>B</u> ack <u>N</u> ext ≻ Cancel

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

# New Scope Wizard

#### Add Exclusions

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



Type the IP address rang address, type an address	e that you want to exclude. in Start IP address only.	If you want to exc	clude a single
<u>S</u> tart IP address: 172 . 16 . 100 . 1	End IP address:	A <u>d</u> d	
Excluded address range:			
		Remo <u>v</u> e	
	<u> </u>	ack <u>N</u> ext	> Cancel

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

Avançar.

New Scope Wizard
Configure DHCP Options You have to configure the most common DHCP options before clients can use the scope.
When clients obtain an address, they are given DHCP options such as the IP addresses of routers (default gateways), DNS servers, and WINS settings for that scope. The settings you select here are for this scope and override settings configured in the Server Options folder for this server.
Do you want to configure the DHCP options for this scope now?
Yes, I want to configure these options now
No, I will configure these options later
< <u>B</u> ack <u>N</u> ext> Cancel

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

#### Router (Default Gateway)

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



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

	New	Scope	Wizar	ď
--	-----	-------	-------	---

#### **Domain Name and DNS Servers**

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



arent do <u>m</u> ain: wirelessdem	io.local	
o configure scope clients to	use DNS servers on your network, enter th	ne IP addresses for tho:
erver name:	I <u>P</u> address:	
		Add
	Resolve 172.16.100.26	Bemove
		Up
		D <u>a</u> wn

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

New Scope Wizard	
Activate Scope Clients can obtain address leases only if a s	cope 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	
	< <u>B</u> ack <u>N</u> ext> Cancel

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

Passo 5: Instalar serviços de certificado

Conclua estes passos:

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

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

Avançar.

You can add or remove components of W	indows.
To add or remove a component, click the part of the component will be installed. To Details.	checkbox. A shaded box means that only see what's included in a component, click
<u>Components:</u>	
🗹 📻 Accessories and Utilities	4.9 MB 🔺
Application Server	33.4 MB 💻
🔽 😫 Certificate Services	1.4 MB
🔲 💻 E-mail Services	1.1 MB
🗖 🚳 Fax Services	7.9 MB 💻
Description: Installs a certification authorit public key security programs.	ty (CA) to issue certificates for use with
Total disk space required: 3.4	MB Details
Space available on disk: 1346.9	MB

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

Windows Components Wizard	×
CA Type Select the type of CA you want to set up.	Ĩ
<ul> <li>Enterprise root CA</li> <li>Enterprise subordinate CA</li> <li>Stand-alone root CA</li> <li>Stand-alone subordinate CA</li> <li>Description of CA type</li> <li>The most trusted CA in an enterprise. Should be installed before any other CA.</li> </ul>	
< <u>B</u> ack <u>N</u> ext> Cancel He	lp

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

ndows Components Wizard	
Certificate Database Settings Enter locations for the certificate database, database log, and config information.	guration
<u>C</u> ertificate database:	
C:\WINDOWS\system32\CertLog	Browse
Certificate database log:	
C:\WINDOWS\system32\CertLog	Bro <u>w</u> se
Store configuration information in a shared folder Shared folder:	
	Blowse
Preserve existing certificate database	
< <u>B</u> ack <u>N</u> ext > Car	ncel Help

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

#### Passo 6: Verificar permissões de administrador para certificados

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

elessdemoca Properties		?
General   Policy Module   Exit Mo Certificate Managers Restrictions   Audi	odule   Extension ting   Recovery Ag	ns   Storage gents Security
Group or user names:		
Administrators (WIRELESSDEMO)	Administrators)	The second s
🕵 Authenticated Users		
🛛 💯 Domain Admins (WIRELESSDEM)	0\Domain Admins)	
🛛 🕵 Enterprise Admins (WIRELESSDEI	MONEnterprise Admi	ins)
1081.0547 17 181		
2		
	A <u>d</u> d	<u>R</u> emove
Permissions for Administrators	Allow	Deny
Read		
Issue and Manage Certificates		
Manage CA		ō
Manage CA Request Certificates	N	
Manage CA Request Certificates	N N	
Manage CA Request Certificates		

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

Passo 7: Adicionar computadores ao domínio

Conclua estes passos:

**Observação:** se o computador já estiver adicionado ao domínio, vá para <u>Adicionar usuários ao</u> <u>domínio</u>.

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

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

ew Object - Computer	X
Create in: wirelessdemo.local/Users	
Computer name:	
Client	
Computer name (pre-Windows 2000):	
CLIENT	
The following user or group can join this computer to a domain	
User or aroup:	
Default: Domain Admins <u>C</u> hange	
Assign this computer account as a pre-Windows 2000 computer	
Assign this computer account as a backup domain controller	
< <u>B</u> ack <u>N</u> ext >	Cancel

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

Passo 8: Permitir acesso sem fio a computadores

Conclua estes passos:

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

Etapa 9: Adicionar usuários ao domínio

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

w Object - User		
😴 Creat	e in: wirelessdemo.local/Users	
Eirst name:	WirelessUser <u>I</u> nitials:	
Last name:		
Full name:	WirelessUser	
<u>U</u> ser logon name	<	
WirelessUser	@wirelessdemo.local	-
User logon name	: (pre- <u>W</u> indows 2000):	
WIRELESSDEN	10 \ WirelessUser	
	< Black Next >	Cancel

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

ew object - oser		
Create in: wirele	essdemo.local/Users	
<u>P</u> assword:	••••	
<u>C</u> onfirm password:	••••	
User <u>m</u> ust change passw	ord at next logon	
User cannot change pass	word	
Pass <u>w</u> ord never expires		
Account is disabled		
	< <u>B</u> ack <u>N</u> ext >	Cancel

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

Etapa 10: Permitir acesso sem fio aos usuários

Conclua estes passos:

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

# Etapa 11: Adicionar grupos ao domínio

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

New Object -	Group
--------------	-------

Create in: wireles	sdemo.local/Users
Group n <u>a</u> me: WirelessUsers	
Group name (pre- <u>W</u> indows 200 WirelessUsers	0):
Group scope O D <u>o</u> main local	Group type
<ul> <li>Global</li> <li>○ Universal</li> </ul>	© <u>D</u> istribution
	OK Cancel

#### Etapa 12: Adicionar usuários ao grupo WirelessUsers

- 1. No painel de detalhes de Usuários e Computadores do Ative Diretory, clique duas vezes em Grupo **Usuários Sem Fio**.
- 2. Vá até a guia Membros e clique em Adicionar.
- 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.

? X
<u>O</u> bject Types
Locations
<u>C</u> heck Names
_
Cancel

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

WirelessUsers Proper	ties	? ×
General Members	Member Of Managed By	
		1
<u>M</u> embers:		
Name Administrator	Active Directory Folder	
Wireless Iser	wirelessdemo. local/U sers	
	<u>h</u> emove	
	OK Cancel	Apply (

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

# Passo 13: Adicionar computadores clientes ao grupo WirelessUsers

- 1. Repita as etapas 1 e 2 na seção <u>Adicionar usuários ao grupo de usuários sem fio</u> deste documento
- 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.

Select Users, Contacts, Computers, or Groups		? ×
<u>S</u> elect this object type:		
Users, Groups, or Other objects		<u>O</u> bject Types
<u>F</u> rom this location:		
wirelessdemo.local		Locations
Enter the object names to select ( <u>examples</u> ):		
client		<u>C</u> heck Names
<u>A</u> dvanced	0K	Cancel

££5

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

Object Types	<u>? X</u>
Select the types of objects you want to find.	
Object types:	
🗹 🐗 Other objects	
🗖 📺 Contacts	
🔽 🔜 Computers	
🗖 🗖 🕵 Users	
	OK Cancel

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

# Configuração do Windows Standard 2003 com Cisco Secure ACS 4.0

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

# Instalação e configuração básicas

Conclua estes passos:

- Instale o Windows Server 2003 com SP1, Standard Edition, como um servidor membro chamado ACS no domínio wireless demo.local.Observação: o nome do servidor ACS é exibido como cisco\_w2003 nas configurações restantes. Substitua o ACS ou o cisco\_w2003 na configuração restante do laboratório.
- Para a conexão de área local, configure o protocolo TCP/IP com o endereço IP de 172.16.100.26, a máscara de sub-rede de 255.255.255.0 e o endereço IP do servidor DNS de 127.0.0.1.

# Instalação do Cisco Secure ACS 4.0

**Observação:** consulte o <u>Guia de Instalação do Cisco Secure ACS 4.0 para Windows</u> para obter mais informações sobre como configurar o Cisco Secure ACS 4.0 para Windows.

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

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

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

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

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

# Configuração do controlador Cisco LWAPP

## Crie a configuração necessária para WPA2/WPA

Conclua estes passos:

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

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

1. Faça login no controlador navegando até





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

CIRCO SYSTEMS					
allo, allo,	MONITOR WUNNS CONTR	OLLER WIRELESS SECURITY			
Controller	Interfaces > Edit				
General Inventory	General Information				
Interfaces	Interface Name employee				
Internal DHCP Server	Interface todace				
Mobility Management Mobility Groups Mobility Statistics Ports Master Controller Mode Network Time Protocol QoS Profiles	VLAN Icentifier IP Address Netmask Gateway Physical Information Port Number DHCP Information	20 172.16.100.4 255.255.255.0 172.16.100.1			
	Primary DHCP Server Secondary DHCP Server Access Control List ACL Name	172.16.100.25 0.0.0.0			

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

 $\mathsf{WLANs} > \mathsf{Edit}$ 

WLAN ID	1		
WLAN 5510	Employee		
Ceneral Policies		Security Policies	
Radio Policy			wate a
Admin Status	✓ Enabled	LUYOF 2 SCOUNTY	W AL
Session Timeout (secs)	1830		
Quality of Scrvics (QoB)	Silver (best offart)	Layer 3 Security	Nоге 💌
WMM Policy	Disabled 🛩		🔲 Web Policy "
7920 P ione Support	🔲 Client CAC Limit 🔄 🗛 CAC Limit		
Broaccast SSID	💌 Enabled		
Allow AAA Override	🕅 Enabled	* Web Policy cannot be and L2TP.	e used in combination with IPsec
Client Exclusion	Enabled ** 60 Timeout Value (secs)	** When plient exclusions are means until the plant of the second	on is enabled, a timpout value of I require acministrative override t
DHCP Server	Override 📃	reset excluded clients)	
DI CP Addr. Assignment	💌 Required		
Interface Name	empləyee 🖌		
Radius Servers			
	Authentication Servers Accounting Servers		
Server 1	TP:172.16.100.25, Port:1812 💙 none 💙		
Server 2	rone 💙 none 🏏		
Server 3	rone 🕑 none 🧹		
WPA2 Parameters			
WPA Compatibility Mode	🕑 Enable		
Allow WPA2 TKIF Clients	🗹 Enable		
Pre-Shared Key	📄 Enabled (WPA2 passphrase has been set)		

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

Apply.

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

CISCO SYSTEMS				
adha adha	MONITOR WLANS (	CONTROLLER	WIRELESS	SECURITY
Security	RADIUS Authentication	on Servers >!	New	
AAA General	Server Index (Priorit	ty) 1	1	
RADIUS Authentication RADIUS Accounting Local Net Users	Server IPAddress	172.1	16.100.25	
MAC Filtering Disabled Clients	Keys Format	ASC	II <b>v</b>	
AP Policies	Shared Secret	••••	••	
Access Control Lists Web Auth Certificate	Confirm Shared Secret	••••	••	
Wireless Protection Policies	Key Wrap			
Rogue Policies Standard Signatures	Port Number	1812		
Custom Signatures Client Exclusion Policies AP Authentication	Server Status	Enab	led 💙	
	Support for RFC 357	6 Enab	led ⊻	
	Retransmit Timeout	2	seconds	
	Network User	<b>I</b> E	inable	
	Management	E 6	nable	



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

# Autenticação EAP-TLS

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

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

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

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

# Instalar o Snap-in Modelos de Certificado

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

5	. Para ignorar as etapas de 2 a	a 4, digite	certtmpl.msc,	que abre o	snap-in Modelos de	
	certificado.					

Certificate Templates	Template Display Name /	Minimum Supported CAs	Version	Autoenrolinent
	Basic EFS	Windows 2000	3.1	Not allowed
	CA Exchange	Windows Server 2003, En	106.0	Vot allowed
	CEP Encryption	Windows 2000	4.1	Vot allowed
	Code Signing	Winduws 2000	3.1	Not allowed
	Computer	Windows 2000	5.1	Vot allowed
	Cross Certification Authority	Windows Server 2003, En	105 0	Vot allowed
	DEMOACS	Windows Server 2000, En	100 2	Vot allowed
	Directory Email Replication	Windows Server 2003, Fn	1:50	Allowed
	Dorran Controler	Windows 2000	4.1	Vot allowed
	Dorrain Controlor Authencication	Windows Server 2003 En	1:00	Allowed
	EPS Recovery Acent	Windows 2000	Simported TAs         Version         Autoenrollnent           2000         3.1         Vot allowed           Server 2003, En         106 0         Vot allowed           2000         4.1         Vot allowed           2000         3.1         Vot allowed           2000         3.1         Vot allowed           2000         5.1         Vot allowed           2000         5.1         Vot allowed           Server 2003, En         105 0         Vot allowed           Server 2003, En         105 0         Allowed           2000         5.1         Vot allowed           2000         6.1         Vot allowed           2000         5.1         Vot allowed           2000         6.1         Vot allowed           2000         6.1         Vot allowed           2000         6.1         Vot allowed           2000         6.1         Vot allowed           2000         7.1         Vot allowed           2000         7.1         Vot allowed           2000         5.1         Vot allowed           2000         5.1         Vot allowed           2000         5.1         Vot allow	
	Enrolline it Agent	Windows 2000		
	Enrollment Agent (Computer)	Windows 2000	5.1	Vot allowed
	Exchange Enrolment Agent (Offline request)	Windows 2000	4.1	Vot allowed
	Exchange Signature Only	Windows 2000	6.1	Not allowed
	Exchange liser	Windows 2000	7.1	Not allowed
	Relieved	Windows 2000	8.1	Not allowed
	IPSec (Offine request)	Windows 2000	7.1	Not allowed
	Key Recovery Acent	Windows Server 2003, En	105.0	Allowed
	RAS and IAS Server	Windows Server 2003 En	101 0	Allowed
	Roo: Certification Authority	Windows 2000	5.1	Not allowed
	Router (Offline request)	Wincows 2000	4.1	Not allowed
	Smartcard Logon	Wincows 2000	6,1	Not allowed
	Smartcard User	Wincows 2000	11.1	Not allowed
	Suburdinate Certification Authority	Wilcows 2000	5.1	Not allowed
	Trust List Signing	Wincows 2000	3.1	Not allowed
	GitUser	Wincows 2000	3.1	Not allowed
	User Signature Only	Wincows 2000	4.1	Not allowed
	Wigh Server	Wincows 2000	4.1	Not allowed
	Dypicate Templa:e	Wincows Server 2003, En	1.0.3	Alowed
	Wi al tasks Late	Wincows Server 2003, En	101.0	Alowed
		Wincows Server 2003, En	101:0	Allowed

# Crie o Modelo de Certificado para o Servidor Web ACS

- 1. No painel Detalhes do snap-in Modelos de certificado, clique no modelo do servidor Web.
- 2. No menu Ação, clique em Duplicar
| -  | Inplace  | 2                 |           |
|--|--|-------------------|-----------|
| Issuance Requireme   | nts Superseded Templates   | Extensions        | Security  |
| General  | Request Handling   | Subject I         | Name      |
| T <u>e</u> mplate display na   | me:  |                   |           |
| Copy of Web Serve  | er   |                   |           |
| Minimum Supported  | CAs: Windows Server 2003, E  | nterprise Editic  | n         |
| After you apply char<br>name.  | nges to this tab, you can no long  | ier change the    | template  |
| <u>T</u> emplate name:   |  |                   |           |
| Copy of Web Serve  | 3r ::  |                   |           |
| Validitu period:   | Benewal period   |                   |           |
| Validity period:<br>2 years<br>□ Publish certificat<br>□ Do not autor          | Renewal period:<br>6 weeks<br>te in Active Directory<br>natically reenroll if a duplicate ca | •rtificate exists | in Active |
| Validity period:<br>2 years<br>Eublish certificat<br>Do not autor<br>Directory | Enewal period<br>6 weeks<br>te in Active Directory<br>natically reenroll if a duplicate ce   | Tificate exists   | in Activ  |

3. No campo Nome de exibição do modelo, digite

	mplace	
Issuance Requiremen	ts   Superseded Templates   E	ktensions 📔 Secur
General	Request Handling	Subject Name
Template display par		
	iic.	
JACOJ		
Minimum Supported 0	CAs: Windows Server 2003, Enter	prise Edition
initianity of apportogic		prise maniari
After you apply chang	ges to this tab, you can no longer o	hange the templati
name.		
Template name:		
Template name.		
ACS		
Validity period:	<u>R</u> enewal period: ■ 6 weeks	-
Validity period: 2 years	<u> <u> R</u>enewal period: <u> 6</u> weeks </u>	•
⊻alidity period: 2 years	<u> <u> R</u>enewal period: 6   weeks </u>	•
Validity period: 2 years	<u>Renewal period:</u> 6       6       e in Active Directory	•
Validity period: 2 years	<u>R</u> enewal period: 6 weeks	•
Validity period: 2 years Publish certificate Do not autom	Renewal period: 6 weeks I for the second	• ate exists in Active
Validity period: 2 years Publish certificate Do not autom Directory	Enewal period: 6 weeks e in Active Directory atically reenroll if a duplicate certific	•ate exists in Activ
Validity period: 2 years Publish certificate Do not autom Directory	Enewal period: 6 weeks e in Active Directory atically reenroll if a duplicate certific	• ate exists in Active
Validity period: 2 years Publish certificate Do not autom Directory	Enewal period: 6 weeks e in Active Directory atically reenroll if a duplicate certific	<b>T</b> sate exists in Active
Validity period: 2 years Publish certificate Do not autom Directory	Enewal period: 6 weeks e in Active Directory atically reenroll if a duplicate certific	Tate exists in Active
Validity period: 2 years Publish certificate Do not autom Directory	Enewal period: 6 weeks e in Active Directory atically reenroll if a duplicate certific OK Cane	el Apoly

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

Subject Name         Signature and encryption         Archive subject's encryption private key         Include symmetric algorithms allowed by the subject         Delete revoked or expired certificates (do not archive)
<ul> <li>Signature and encryption</li> <li>Archive subject's encryption private key</li> <li>Include symmetric algorithms allowed by the subject</li> <li>Delete revoked or expired certificates (do not archive)</li> </ul>
<ul> <li>Archive subject's encryption private key</li> <li>Include symmetric algorithms allowed by the subject</li> <li>Delete revoked or expired certificates (do not archive)</li> </ul>
<ul> <li>Include symmetric algorithms allowed by the subject</li> <li>Delete revoked or expired certificates (do not archive)</li> </ul>
Delete revoked or expired certificates (do not archive)
size: 1024 💌
ate key to be exported
ing when the subject is enrolled and when the private key ith this certificate is used:
ject without requiring any user input
e user during enrollment
e user during enrollment and require user input when the y is used
hich cryptographic service providers <u>C</u> SPs

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

	uest Handling	Subject Name
SP Selection		?
Choose which cryptographic requests:	service providers (CS	Ps) can be used in
C <u>R</u> equests can use any C	SP available on the su	ubject's computer
Requests <u>m</u> ust use one of	of the following CSPs:	
<u>C</u> SPs:		
Microsoft Base Cryptogra Microsoft Base DSS and Microsoft DH SChannel C Microsoft Enhanced Cryp Microsoft Enhanced DSS Microsoft Enhanced RSA	onial Cara Con ohic Provider v1.0 Diffie Hellman Cryptog ryptographic Provider tographic Provider v1. and Diffie Hellman Cr and AES Cryptograph	praphic Provider 0 yptographic Prov nic Provider
Microsoft BSA SChannel	Cruptopraphic Provide	

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

	ance Requirements   Superseded Templates   Extensions   Securi General   Request Handling Subject Name
с С	Supply in the request Select this option to allow a variety of subject name formats or if you do not have access to the domain of which the subject is a member. Autoenrollment is not allowed if you choose this option. Build from this Active Directory information
11 Section 1	Select this option to enforce consistency among subject names and to simplify certificate administration.
1.55	Subject name format:
	None
10	🗖 Include e-mail name in subject name
111	Include this information in alternate subject name:
194	E-mail name
Control of	<u>D</u> NS name
100	User prinicipal name (UPN)
1	Service principal name (SPN)

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

General Request H	landling S	ubject Name
Issuance Requirements   Supersed	led Templates   Exter	nsions Security
<u>G</u> roup or user names:		
🛿 🖉 Administrator (WIRELESSDEM	10\Administrator)	
🕼 🕼 Authenticated Users		
🕵 Domain Admins (WIRELESSDI	EMO\Domain Admins)	
🛛 💯 Enterprise Admins (WIRELESS	DEMO\Enterprise Adn	nins)
Press Strate Propriet Approximation Front Strategy and		
		1
	Add	<u>R</u> emove
Permissions for Domain Admins	A <u>d</u> d	<u>R</u> emove
Permissions for Domain Admins	A <u>d</u> d Allow	<u>R</u> emove Deny
Permissions for Domain Admins	A <u>d</u> d Allow	<u>R</u> emove Deny
Permissions for Domain Admins Full Control Read Write	A <u>d</u> d Allow III IIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	Remove Deny
Permissions for Domain Admins Full Control Read Write Enroll	Add Allow I I I I I I I I I I I I I I I I I I I	Remove Deny
Permissions for Domain Admins Full Control Read Write Enroll Autoenroll	Add Allow Q	Remove Deny
Permissions for Domain Admins Full Control Read Write Enroll Autoenroll	Add Allow V V	Remove Deny
Permissions for Domain Admins Full Control Read Write Enroll Autoenroll	Add Allow ☑ ☑ ☑ ☑	Remove Deny
Permissions for Domain Admins Full Control Read Write Enroll Autoenroll For special permissions or for advanced	Add Allow V V Ced settings.	Remove Deny

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

	-	
General	Request Handling	Subject Name
Issuance Requirements	Superseded Templates	Extensions   Security
Require the following f	or enrollment:	
CA certificate man	ager approval	
This number of aut	horized signatures:	<u> </u>
-	·	
If you require more	e than one signature, autoer	roliment is not allowed.
Policy type require	d in signature:	
l		<u> </u>
Application policy:		
l.		<u>M</u> .
Issuance policies.		-
		<u>R</u> emove
		-
Require the following f	or reenrollment:	
C Same criteria as fo	r enrollment	
C Valid existing certif	icate	

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

### Ativar o novo modelo de certificado do servidor Web ACS

Conclua estes passos:

 Abra o snap-in Autoridade de Certificação. Siga as etapas de 1 a 3 na seção <u>Create the</u> <u>Certificate Template for the ACS Web Server</u>, escolha a opção Certificate Authority, escolha Local Computer e clique em Finish.

Certification Authority		×
Select the computer you This snap-in will always © Local computer: ( © Another computer:	want this snap-in to manage. s manage: the computer this console is running on) :	e
Allow the selected only applies if you	d computer to be changed when launching from the command line. I save the console.	This
	< <u>B</u> ack Finish	Cancel

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

🗭 🖃 🛅 🛄 🔛 🗠 🛯	(Local)\wirelessdemoca\Certificate Tem	plates 🔳
Console Root Certification Authority (Local) Wirelessdemoca Revoked Certificates Sector Pending Requests Faied Requests Value Vew Window from He Vew Taskpad View Refresh Export List Telp	Name Wireless Like: Certificare Template Diractory Email Replication Domain Controller Authentication DrS Recovery Agent Basic EFS Domain Controller Web Server Certificate Template to Issue Subordinate Certification Authority ere Administrator	Intended Purpose         Client A thentration, Service Email, Encry,         Directory Service Email Replication         Client Authentication, Server Authentication.         File Recovery         Bioryphing File System         Client Authentication, Server Authentication         Server Authentication         Client Authentication, Server Authentication         Server Authentication, Server Authentication         Client Authentication, Server Authentication         Encrypting File System, Secure Email, Clien <all>         Nicrosoft Trust List Signing, Encrypting File</all>

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

#### Enable Certificate Templates

Select one or more Certificate Templates to enable on this Certification Authority

Name	Intended Purpose	-
ACS	Server Authentication	-
Authenticated Session	Client Authentication	
🙀 CA Exchange	Private Key Archival	
CEP Encryption	Certificate Request Agent	
🙀 Code Signing	Code Signing	
Cross Certification Authority	KAID	
DEMOACS	Server Authentication	
🐺 Enrolment Agent	Certificate Request Agent	
Enrolment Agent (Computer)	Certificate Request Agent	
Exchange Enrollment Agent (Offline request)	Certificate Request Agent	
Exchange Signature Only	Secure Email	

- 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 no **domínio wireless demo.local** e clique em **Propriedades**.

? X



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

To improve Grou	p Policy manage	ment upgrade	to the Group P	olicy
	nsole (GFMC). ent Group Policy	Object Links fo	r wirelessdemo	)
Group Policy O	bject Links		No Override	Disabled
	nain Folicy			
Group Policy Obj This list obtained	ects higher in the from: cisco_w20	e list have the h 003.wirelessdem	ighest priority. io.local	
Group Policy Obj This list obtained <u>N</u> ew	ects higher in the from: cisco_w20 A <u>d</u> d	e list have the h )03.wirelessdem <u>E</u> dit	ighest priority. io.local	Цр
Group Policy Obj This list obtained <u>N</u> ew Options	ects higher in the from: cisco_w20 A <u>d</u> d Dele <u>t</u> e	e list have the h 103.wirelessdem <u>E</u> dit <u>P</u> roperties	ighest priority. io.local	<u>U</u> p Do <u>w</u> n
Group Policy Obj This list obtained <u>N</u> ew Options	ects higher in the from: cisco_w20 A <u>d</u> d Dele <u>t</u> e	e list have the h )03.wirelessdem <u>E</u> dit <u>P</u> roperties	ighest priority. io.local	<u>U</u> p Do <u>w</u> n

grupo.

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

🚡 Group Policy Object Editor	ti ti		
File Action <u>V</u> iew <u>H</u> elp			
🗢 🔶 💽 💽 🛃 😫			
<ul> <li>Default Domain Policy [cisco_w2003.wirel</li> <li>Computer Configuration</li> <li>Software Settings</li> <li>Windows Settings</li> <li>Scripts (Startup/Shutdown)</li> <li>Security Settings</li> <li>Security Settings</li> <li>Computer Policies</li> <li>Event Log</li> <li>System Services</li> <li>System</li> <li>Site System</li> <li>Wireless Network (IEEE 8</li> <li>Public Key Policies</li> </ul>	essdemo.local] ( 02.11) Policies	Policy	Automatic Certificate Request A There are r
Automatic Certificat	New	•	Automatic Certificate Request
Enterprise Trust	⊻iew	•	
<ul> <li>⊕</li></ul>	Refresh Export List		
<ul> <li>User Configuration</li> <li>Software Settings</li> <li>Windows Settings</li> <li>Administrative Templates</li> </ul>	Help		

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

ti <b>ficate Template</b> The nextitime a computer logs on, a c provided.	ertificate based on the template you select is
A certificate template is a set of prede computers. Select a template from the	ined properties for certificates issued to following list.
C <u>e</u> rtificate templates:	
Name	Intended Purposes
Computer Domain Controller Enrollment Agent (Computer) IPSec	Client Authentication, Server Authenticatio Client Authentication, Server Authenticatio Certificate Request Agent IP security IKE intermediate
•	•

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

Group Policy Object Editor	
<u>File Action View Help</u>	
<ul> <li>Default Domain Policy [cisco_w2003.wirelessdemo.local] Policy</li> <li>Computer Configuration</li> <li>Software Settings</li> <li>Windows Settings</li> <li>Scripts (Startup/Shutdown)</li> <li>Security Settings</li> <li>Scolar Policies</li> <li>Event Log</li> <li>Restricted Groups</li> <li>System Services</li> <li>System Services</li> <li>System Services</li> <li>Signature Setting</li> <li>System Services</li> <li>Signature Setting</li> <li>System Services</li> <li>System Services</li> <li>Subject Policies</li> <li>System Services</li> <li>System Services</li> <li>Subject Policies</li> <li>System Services</li> <li>Subject Policies</li> </ul>	Automatic Certificate Request
i Encrypting File System Automatic Certificate Request Settings I Trusted Root Certification Authorities I Enterprise Trust	

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



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

atualizar certificados pendentes e remover certificados revogados  ${\rm e}$  Atualizar certificados que utilizem modelos de

#### certificados.

Autoenrollment Settings Properties
General
Enroll user and computer certificates automatically
<ul> <li><u>D</u>o not enroll certificates automatically</li> <li><u>E</u>nroll certificates automatically</li> </ul>
Benew expired certificates, update pending certificates, and remove revoked certificates
Update certificates that use certificate templates
OK Cancel Apply

16. Click OK.

# Configuração do certificado ACS 4.0

### Configurar certificado exportável para ACS

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

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

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



4. Escolha Solicitar um certificado e clique em



Microsoft Certificate Services -- wirelessdemocal

### **Request a Certificate**

Select the certificate type: User Certificate

Or, submit an advanced certificate request.

5. Escolha Solicitação avançada e clique em



Wels, You suid have an exercise on equal commons to confil a regret on behavior another care

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

nite. ork	a) 🔊 🐟 🔎 Sector i 😓 -ovaeros d	a 🔉 🕹 🗖
less 💽 http://11	22.16.100.25)Certsry/certruma.asp	C/ [27: 00: 000
- Per Inder La		
icrosofi Certifi	cate Services — wire essdemena	
dvanced Ce	rtificate Request	
ertificate Lenu	late:	
	Admini shalor	<u> </u>
e Ontione:	Desir EEB	
opdons.	End Recovery Agen.	1. And an end of the second se
	Uper	my kay sel
CSP:	Wireless User Carificate Template	Nierry1 🗋 💌
Кеу Озасы.	S. Lucine of Sodifice time As thereity	
No. Com	Wer Sever	
1407 N 10.	Max 15884	2 1024 2048 40V2 8102 10284 )
	Automatic key container name	OUser specified key container name
	🖻 Märk keys as expendible	
	🗖 Export keys to file	
	□ =nahtri un uricate kex nurie :	116
	Device control process	
	Screening and the second secon	l ner hen licare is hre /
	instead of is the user's contribute	n strute Doos not
	instell the root CA's centilicate 🕚	/cu muat ke an
	administrator to generate or use	a hay in the local
	machine store.	
ditional Optic	)IIS:	
accest Format.	© CIVIC   C PKCS10	
ni Na katalar ( da da se katalar	21.6.1	
iae Accimin.		
	Comp daeo to agin requeat	
	🗖 Save request to a lite	
		*
Atticutes:		T
Friendly Mame:		
		Submit >
		- donne -

- 7. Nos Modelos de certificado, selecione o modelo de certificado criado anteriormente chamado **ACS**. As opções são alteradas após a seleção do modelo.
- 8. Configure o nome para ser o nome de domínio totalmente qualificado do servidor ACS. Nesse caso, o nome do servidor ACS é cisco\_w2003.wirelessdemo.local. Certifique-se de que o certificado de armazenamento no arquivo de certificados do computador local está marcado e clique em

🖹 Microsoft Certific	ate Services - Microsoft Internet Diplorer
Elle <u>E</u> dik <u>M</u> ew P	agvarites Icols Help
🕽 Deck 💌 🕤 🗠 🖪	) 😰 🐔 🖓 Search 🤹 Pavoritas 🕘 🝰 🗟
lddreec 🔊 http://17	2.16.100.35(tertsrv/certrgna.asp
Certificate Temp	date:
	ACS
Line of the second	nation For Alline Template
roentilying intoin	nation For Unine Template:
Name:	[cisco_w2003.wneessdemb.iddei
C-Mail:	
Company:	
Department:	
City:	
State:	
Country/Region:	
Key Ontions:	
rey opness	Construent low and College quiction low and
COD-	Missesset Pase Constantanta kis Braidery 1 0
Key Hoone:	Exchange
Kay Siza:	1024 Min:1024 Mar:1024 (common key size: 3029.)
	Automatic key container name     O User specified key container name
	🗹 Mark keys as exportable
	Export keys to file
	Store cartificate in the local computer certificate store Stores the certificate in the local computer store instead of in the user's certificate store. Does not install the root CA's certificate. You must be an administrator to generate or use a key in the local mechine store.
Additional Optio	ns:
Request Format:	CMC CPKCS10
Hash Algorithm:	SHA-1  Coly used to sign request.
	□ Save request to a file
Attributes:	A V A
Friendly Name:	
	Submit >

#### Enviar.

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

	Onn.		
	Potential	Scripting Violation	I,
	1	This Web site is requesting a new certificate on your behalf. You should allow only trusted Web sites to request a certificate for you. Do you want to request a certificate now?	
		Yes No	
n	) Clique	em Instalar este	

10. Clique em Instalar este certificado.

Eile	Edit	⊻iew	F <u>a</u> vorites	Tools	Help			
🗿 Ba	ack 💌	0 -	2 2 💰		5earch	📌 Favorites	😸 🝰 •	3 🖬

Microsoft Certificate Services -- wirelessdemoca

### Certificate Issued

The certificate you requested was issued to you.



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

Sim.	
Potential	Scripting Violation
⚠	This Web site is adding one or more certificates to this computer. Allowing an unbrusted Web site to update your certificates is a security risk. The Web site could install certificates you do not trust, which could allow programs that you do not trust to run on this computer and gain access to your data. Do you want this program to add the certificates now? Click Yes if you trust this Web site. Otherwise, click No.
	<u> </u>

12. Depois de clicar em Sim, o certificado é

<ul> <li>How How House House House</li> <li>Image: A second seco</li></ul>	👷 Havorites 🛛 🕢 🖓 • 🐍 🗟 mpn. aso ess tiem tht a
- 💽 👔 🐔 🔎 search x/(172,16,100,25/certsrv/certm artificiate Services — wire e	👷 Havorites - 🧐 📄 - 🚴 🔤 Iriph, aso ess: tempicia
ertificate Services wire e	mph, aso essideminicia
ertificate Services vire e	ess tempca
artificate Services — wire e	essileminda
SUDLARS DEVERS - WIRE	REPORT OF A
Installed	
And the second	servers at address to a still
ertificate has been suc	cessfully installed
ertificate	has been suc

instalado.

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



- 14. Agora que o certificado está instalado no computador local (ACS ou cisco\_w2003 neste exemplo), você precisa gerar um arquivo de certificado (.cer) para a configuração do arquivo de certificado ACS 4.0.
- 15. No servidor ACS (cisco\_w2003 neste exemplo), aponte o navegador no servidor da Autoridade de Certificação da Microsoft para http://172.16.100.26 /certsrv.

### Instale o certificado no software ACS 4.0

Conclua estes passos:

- 1. No servidor ACS (cisco\_w2003 neste exemplo), aponte o navegador no servidor Microsoft CA para http://172.16.100.26 /certsrv.
- 2. Na opção Selecionar uma tarefa, escolha **Baixar um certificado CA, uma cadeia de certificados ou uma CRL**.
- 3. Escolha o método de codificação de rádio **Base 64** e clique em **Download CA Certificate**.

🚔 Miur	usult Certificate Services - Microsoft Toternet I	se planeer
De	Edt gien Favorites Ipols Lielo	
🔇 Bac	k 🔹 🔿 👻 😰 👔 🐔 🔑 Search 🛚 👷 =avorte	s 🐵 🙆 s 😓 🚍
Addres:	🗑 📵 =ttp://172.10.100.26/certs/v/certcard ast	

Microsoff Cepting Geroces -- wrelessdemonal

#### Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from the certification authority install this CA certificate chain.

To down date a CA cost ficate, certificate chain, or CRL isolate the certificate and encoding method.

CA certificate:

C urrent	wielessdemocal

Lacoding method:

⊂ D\_R ©Ecso 64

<u>Down dad CA certificate</u> <u>Down dad CA certificate chain</u> Down dad latest base CRL Down dad latest delta CRL

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

•	Name: Tune:	certnew.cer Security Certific	ate 1.68 KB	
80° 30° 40° 408	From:	172.16.100.26		
		<u>O</u> pen	<u>S</u> ave	Cance

 Salve o arquivo com um nome como ACS.cer ou qualquer nome que desejar. Lembre-se desse nome, pois ele é usado durante a configuração da autoridade de certificação ACS no ACS 4.0. Save As ? X 💽 🕝 😰 📂 🖽-Save in: 🧼 Local Disk (C:) CNS62 Documents and Settings My Recent Documents DI386 Inetpub Program Files TFTP Desktop ) WINDOWS Wireless ) wmpub ACS.cer My Documents 🕮 acs\_server\_cert.cer 🔛 certnew.cer My Computer Save ACS.cer • My Network File name: Places Security Certificate -Cancel Save as type:

- 6. Abra o ACS Admin do atalho da área de trabalho criado durante a instalação.
- 7. Clique em Configuração do



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

# System Configuration



### ACS). System Configuration

Edit
Install ACS Certificate
Install new certificate
© Read certificate from file
Certificate file
Our Second Se
Certificate CN
Private key file
Private key password

 Escolha Usar certificado do armazenamento e digite o nome de domínio totalmente qualificado de cisco\_w2003.wirelessdemo.local (ou ACS.wirelessdemo.local se você usou o ACS como o nome). System Configuration

Install ACS Certificate	
Install new certificate	?
O Read certificate from file	
Certificate file	
Ose certificate from storage	
Certificate CN cisco_w2003.wirelessde	
Private key file	
Private key password	

11. Clique em

Submit.

# System Configuration

Edit

### Install ACS Certificate

?

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

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

12. Clique em **Configuração do sistema**.

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

# System Configuration

Select

CiscoSecure ACS on cisco\_w2003

# **Is Currently Running**

?

Services Log File Configuration
Level of detail
O None
O Full
Generate New File
• Every day
C Every week
O Every month
○ When size is greater than 2048 KB
Manage Directory
C Keep only the last 7 files
Delete files older than 7 days
Back to Helm

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

# System Configuration

### **Global Authentication Setup**

EAP Configuratio	n 🤶
PEAP	
Allow EAP-MSCHAPV2	
□ Allow EAP-GTC	
Allow Posture Validation	
Cisco client initial message:	
PEAP session timeout (minutes):	120
Enable Fast Reconnect:	
EAP-FAST	
EAP-FAST Configuration	
Coloct and or more of the following entires:	
Select one or more of the following options:	
I√ Certificate SAN comparison	
🗹 Certificate CN comparison	
🗹 Certificate Binary comparison	
EAP-TLS session timeout (minutes):	120

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

## System Configuration

dit				
ACS Certification Au	uthority Set	up		
CA Operation	IS		?	
Add new CA certificate to local certificate	storage			
CA certificate file	acs.cer			
stem Configuration				
stem Configuration				
stem Configuration ACS Certification Authority Setup	New CA certificate is succe	essully added into the	global sy	ystem certificat
stem Configuration ACS Certification Authority Setup CA Operations	New CA certificate is succ CA certificate common m	essully added into the storage. ame	global sy wirel	ystem certificat

22. Reinicie o serviço ACS.

## Configuração do CLIENTE para EAP-TLS usando Windows Zero Touch

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

#### Executar uma instalação e configuração básicas

Conclua estes passos:

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

#### Configure a conexão de rede sem fio

Conclua estes passos:

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

pessoais.				
The Console 1				
Le Action Yew Levontes Window Le	р			
수 🔁 📧 💼 😫 🞼				
🚡 Consule RootWertificates - Corrent U	ser Personal Certificates			×
📴 Cansole Root	Issued To	Essued By	Expiration Date	In
Certificates - Current User 	₩¥e essLser	Wrelesscemoca	3/22/2008	c

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

eneral Wireless Networks /	Advanced
Use <u>W</u> indows to configure	rry wireless network settings
Available <u>n</u> elworks:	
To connect :o, disconnect fr about witeless retworks in ra	om, or find out more information arge.click the button below.
	View Wireless Networks
Prefeired nelworks: Automatically connect to availabelow:	ailable networks in the order listed
Prefeired nelworks: Automatically connect to available	ailable networks in the order listed Move <u>up</u> Move <u>dowr</u>
Prefeired networks: Automatically connect to availabelow: Add	ailable networks in the order listed Move yp Move dowr

marcado.

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

Association	Authentication	Connection	
Network na	me (SSID): network kev	Enplcyee	
This betw	ork requires a ke	y for the following:	
Network	Authentication:	Open	
Date enc	ryption:	WEP	
Network I	keji:		
Contirm n	etwork key:		
Key index	(edvanced),		
🔽 The k	ey is provided fo	rme auromatically	
The k	ey is provided fo computei-to-cor points are not us	rme auromatically npu:er (ad hoc) network; w ed	ireless

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

1	Vireless ne	twork proper	ties		? 🗙
	Association	Authenlica:ion	Connection		
	Select this wireless Eth	option to provide nemel networks	authenticated retwor	k access for	
	🗹 Enable	EEE 802.1x au:ł	nentication for this net	work	
	EA <sup>o</sup> type:	Smart Card or o	ther Certhicate		~
	Aulhent	icate as compule icate as guest wh abe	er when computer infor	Propeitie	ilable
is			OK	Car	ncel

- 10. Clique em Propriedades.
- 11. Verifique se as caixas nessa janela estão

mart Card or other Certificate Properties 🛛 🛛 🛜 🔯
When connecting
Series my smart pard
Subset a certificate on this computer
Jse simple certificate selection (Recommended)
Validate server certificate
Connect to these servers.
Trusted Root Certification Authorities:
ABA.ECOM Root CA
ACS333
ACS40
Autor dad Certificadora de la Asociación Nacional cel Notaria
Autor dad Lertificadora del Loegio Nacional de Lorreduria Pu
Relasson F.Tr. et Primeru CA
C:WHKT SecureNet CA Class A
View Certificate
Use a different user name for the connection
OK. Cancel

marcadas.

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



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







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

### Informações Relacionadas

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