# PEAP em UWNs com ACS 5.1 e Windows 2003 Server

## Contents

Introduction **Prerequisites** Requirements Componentes Utilizados **Conventions** Configurar Diagrama de Rede Instalação do Windows Enterprise 2003 com IIS, Autoridade de Certificação, DNS, DHCP (CA) CA (democracia) Cisco 1121 Secure ACS 5.1 Instalação usando o dispositivo CSACS-1121 Series Instalar o servidor ACS Configuração do controlador Cisco WLC5508 Crie a configuração necessária para WPAv2/WPA Autenticação PEAP Instalar o Snap-in de Modelos de Certificado Criar o Modelo de Certificado para o Servidor Web ACS Habilitar o novo modelo de certificado de servidor Web ACS Configuração do certificado ACS 5.1 Configurar certificado exportável para ACS Instale o certificado no software ACS 5.1 Configurar o Repositório de Identidades do ACS para o Ative Diretory Adicionar um controlador ao ACS como um cliente AAA Configurar políticas de acesso ACS para rede sem fio Criar política de acesso e regra de servico ACS Configuração do CLIENTE para PEAP usando Windows Zero Touch Executar uma Instalação e Configuração Básicas Instale o adaptador de rede wireless Configurar a conexão de rede sem fio Solucionar problemas de autenticação sem fio com ACS A autenticação PEAP falha com o servidor ACS Informações Relacionadas

## **Introduction**

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

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

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

## **Prerequisites**

### **Requirements**

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

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

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

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

O Windows Server 2003 com SP1, Enterprise Edition, é usado para que a inscrição automática de certificados de usuário e estação de trabalho para autenticação PEAP possa ser configurada. A inscrição automática e a renovação automática de certificados facilitam a implantação de certificados e melhoram a segurança ao expirar e renovar certificados automáticamente.

#### **Componentes Utilizados**

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

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

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

## **Conventions**

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

## **Configurar**

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

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

### Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:

Topologia de laboratório sem fio segura da Cisco



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

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

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

## CA (democracia)

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

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

Execute estas etapas para configurar o CA para estes serviços:

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

#### Executar Instalação e Configuração Básicas

Execute estas etapas:

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

#### Configurar o computador como um controlador de domínio

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

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

Active Directory Installation Wizard		
Database and Log Folders Specify the folders to contain the Active Directory database and log files.		
For best performance and recoverability, store the database and the log on separate hard disks.		
Where do you want to store the Active Directory database?		
Database folder:		
C:\WINDOWSWTDS Bjowse		
Where do you want to store the Active Directory log?		
C:\WINDOWSWTDS Browse		
< <u>B</u> ack <u>N</u> ext> Cancel		

## Próximo. 🗕

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

Active Directory Installation Wizard	×
Shared System Volume Specify the folder to be shared as the system volume.	Se la constante da constante constante da co
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>B</u> ack <u>N</u> ext> Ca	ncel

#### Avançar. 🗕

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

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.
C 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.
Anonymous users can read information on this domain.
<ul> <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

#### Avançar.

12. Na página Senha de Administração do Modo de Restauração dos Serviços de Diretório, deixe as caixas de senha em branco e clique em **Avançar**.

13. Revise as informações na página Resumo e clique em

umma Re	ry view and confirm the options you selected.
You	i chose to:
The	e new domain name is example.com. This is also the name of the new forest.
The	NetBIOS name of the domain is EXAMPLE
Da Log SY	abase folder: C:\WINDOWS\NTDS file folder: C:\WINDOWS\NTDS SVDL folder: C:\WINDOWS\SYSVDL
The will	DNS service will be installed and configured on this computer. This computer be configured to use this DNS server as its preferred DNS server.
The	e password of the new domain administrator will be the same as the password of administrator of this computer.
To	change an option, click Back. To begin the operation, click Next.

Próximo. 🖵

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

#### Elevar o nível funcional do domínio

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



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

#### Instalar e configurar o DHCP

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

New Scope Wizard			
Scope Name You have to p providing a de	rovide an identifying scope name. You also have the option of scription.		
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:	CorpNet		
Description:			
	< <u>B</u> ack <u>N</u> ext > Cancel		

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

New Scope Wizard
IP Address Range You define the scope address range by identifying a set of consecutive IP addresses.
Enter the range of addresses that the scope distributes.
Start IP address: 10 . 0 . 20 . 1
End IP address: 10 . 0 . 20 . 200
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
Sybnet mask: 255 . 255 . 0
< <u>B</u> ack <u>N</u> ext> Cancel

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

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:           10.0.20.1         10.0.20.100
Excluded address range:
Remove
< <u>B</u> ack <u>N</u> ext > Cancel

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

New Scope Wizard		
Configure DHCP Options You have to configure the most common DHCP options before clients can use the scope.	þ	
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		
C No, I will configure these options later		
< <u>B</u> ack <u>N</u> ext > Cancel		

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

New Scope Wizard	
Router (Default Gateway) You can specify the routers, or default gateways, to be distributed by this scope.	Ð
To add an IP address for a router used by clients, enter the address below.	
IP address:       10 . 0 . 20 . 1       Add         Image: Image state stat	
D <u>o</u> wn	
< <u>B</u> ack <u>N</u> ext > Cancel	

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

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 do <u>m</u> ain: demo.local			
To configure scope clients to use DNS servers servers.	s on your network, enter the IP ad	dresses for those	
<u>S</u> erver name:	I <u>P</u> address:		
		A <u>d</u> d	
Resolve	10.0.10.10	<u>R</u> emove	
		<u>Ц</u> р	
		Down	
	,		
	< <u>B</u> ack <u>N</u> ext >	Cancel	

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

New Scope Wizard			
Activate Scope Clients can obtain address leases only if a s	cope is activated.		(C)
Do you want to activate this scope now?			
Yes, I want to activate this scope now			
C No, I will activate this scope later			
	< <u>B</u> ack	<u>N</u> ext >	Cancel

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

#### Instalar Serviços de Certificado

Execute estas etapas:

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

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

Verificar permissões de administrador para certificados

Execute estas etapas:

1. Escolha Start > Administrative Tools > Certification Authority.

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

ca.demo.local Properties	? ×
General   Policy Module   Exit Mod Certificate Managers Restrictions   Auditin	ule Extensions Storage g Recovery Agents Security
<u>G</u> roup or user names: Administrators (DEMO\Administrators Authenticated Users Domain Admins (DEMO\Domain Adm Enterprise Admins (DEMO\Enterprise	) nins) : Admins)
Permissions for Administrators Read Issue and Manage Certificates Manage CA Request Certificates	A <u>d</u> d <u>R</u> emove Allow Deny □ □ □ ■ □ ■ □ ■ □ ■ □ ■ □
, ОК	Cancel Apply

#### Permitir.

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

#### Adicionar computadores ao domínio

Execute estas etapas:

**Observação:** se o computador já tiver sido adicionado ao domínio, prossiga para <u>Adicionar</u> <u>usuários ao domínio</u>.

- 1. Abra o snap-in Usuários e Computadores do Ative Diretory.
- 2. Na árvore do console, expanda demo.local.
- 3. Clique com o botão direito do mouse em Computers, clique em New e em Computer.
- 4. Na caixa de diálogo Novo objeto Computador, digite o nome do computador no campo Nome do computador e clique em **Avançar**. Este exemplo usa o nome do computador

w Object - Compute	r I
Create in:	demo.local/Users
Computer name:	
client	
Computer name (pre-W	/indows 2000):
CLIENT	
1	
The following user or g	roup can join this computer to a domain.
The following user or g User or group: Default: Domain Admi	roup can join this computer to a domain.
The following user or g User or group: Default: Domain Admi	roup can join this computer to a domain. ns
The following user or g User or group: Default: Domain Admi	roup can join this computer to a domain.  ns
The following user or g User or group: Default: Domain Admi	roup can join this computer to a domain.  ns
The following user or g User or group: Default: Domain Admi	roup can join this computer to a domain.  ns  Change  er account as a pre-Windows 2000 computer er account as a backup domain controller  < Back Next > Cancel

Client.

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

#### Permitir acesso sem fio a computadores

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

General   Uperating System   Member Uf   Location	Managed By Dial-in
Remote Access Permission (Dial-in or VPN)	
Allow access	
○ <u>D</u> eny access	
C Control access through Remote Access Policy	
Callback Options	
• No <u>C</u> allback	
Set by Caller (Routing and Remote Access Servi	ce only)
C Always Callback to:	
Assign a Static IP Address	
Apply Static <u>R</u> outes	
Define routes to enable for this Dial-in	atic Ro <u>u</u> tes
OK Car	ncel <u>A</u> pply

#### Adicionar usuários ao domínio

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

ew Object - User				
Create in	: demo.local/L	lsers		
<u>F</u> irst name:	wirelessuser		Initials:	
Last name:				
Full n <u>a</u> me:	wirelessuser			
User logon name:				
wirelessuser		@demo.loca	al	<b>•</b>
User logon name (pr	e- <u>W</u> indows 2000	):		
DEMO\		wirelessuser		
		< Back	Next >	Cano
		- Error	<u></u>	

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

New Object - User	×
Create in: demo.local/Users	
Password:	
Confirm password:	
User must change password at next logon	
User cannot change password	
Pass <u>w</u> ord never expires	
Account is disabled	
< <u>B</u> ack Next> Ca	ancel

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

#### Permitir acesso sem fio aos usuários

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

Rem	ote control	Term	inal Service	es Profile	COM+
General Memi	Address er Of	Account Dial-in	Profile Envir	Telephones onment	Organization Sessions
Remo	e Access Pe	ermission (Dial-i	n or VPN)-		
• Alk	w access				
С <u>D</u> е	ny access				
C Co	ntrol access	through Remot	e Access <u>F</u>	Policy	
<b>□</b> Ve	ify Caller-ID:		Г		
Callba	k Options-		1		
• No	Callback				
© <u>S</u> e	t by Caller (F	Routing and Re	mote Acce:	ss Service only	)
C Ak	vays Callbac	ik to:	Г		
Γ As	ion a Static	IP Address	Г		
	olu Static Bo	utes	L		
		wahla (as this D	tal in		
Defin	e routes to e	enable for this L	hai-in	Static Ro	utes

Adicionar grupos ao domínio

- 1. Na árvore do console Ative Diretory Users and Computers, clique com o botão direito do mouse em **Users**, clique em **New** e clique em **Group**.
- 2. Na caixa de diálogo Novo objeto Grupo, digite o nome do grupo no campo Nome do grupo e clique em **OK**. Este documento usa o nome de grupo

-	234		
	Group name:		_
	wirelessusers		
	Group name (pre- <u>W</u> indows 2	2000):	
	wirelessusers		
	Group scope	Group type	
	C Domain local		
	Global	C Distribution	
	Citiciument		
	Universal		

#### Adicionar usuários ao grupo usuários sem fio

- 1. No painel de detalhes de Usuários e computadores do Ative Diretory, clique duas vezes no grupo *Usuários sem fio*.
- 2. Vá até a guia Membros e clique em Adicionar.
- 3. Na caixa de diálogo Selecionar usuários, contatos, computadores ou grupos, digite o nome dos usuários que deseja adicionar ao grupo. Este exemplo mostra como adicionar o usuário *wireless* ao grupo. Click

elect Users, Contacts, or Computers		
Select this object type:		
Users or Other objects		Object Type
From this location:		
demo local		Landiana
demonoca		
Enter the object names to select ( <u>examples</u> ):		
Enter the object names to select ( <u>examples</u> ): wirelessuser		Check Nam
Enter the object names to select ( <u>examples</u> ): wirelessuser		Check Nam
Enter the object names to select ( <u>examples</u> ): wirelessuser		<u>Check Narr</u>
Enter the object names to select ( <u>examples</u> ): wirelessuser	OK	Cancer

4. Na caixa de diálogo Vários Nomes Encontrados, clique em **OK**. A conta de usuário sem fio é adicionada ao grupo de usuários sem

irelessusers Propei	rties	?
General Members	Member Of Managed By	
Members:		
Name	Active Directory Folder	
🖸 Administrator	demo.local/Users	
😰 wirelessuser	demo.local/Users	
Add	Bemove	
Add	<u>R</u> emove	
Add	<u>R</u> emove	
Add	Bemove OK Cancel	Apply

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

#### Adicionar computadores cliente ao grupo usuários sem fio

Execute estas etapas:

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

elect Users, Contacts, or Computers	?
Select this object type:	
Users or Other objects	Object Types
Erom this location:	
demo.local	Locations
Enter the object names to select (examples):	
client	

grupo. 🖣

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

Object Types	1	2 ×
Select the types of objects you want to find.		
Object types:		_
Contacts		
Computers		
		_
	OK Cancel	

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

wirelessusers Prope	erties	? ×
General Members	Member Of Managed By	
Members:		
Name	Active Directory Folder	
Administrator	demo.local/Users demo.local/Computers	
🖸 wirelessuser	demo.local/Users	
Add	Bemove	
	OK Carcel	Annik
		0000

usuários sem fio.

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

## Cisco 1121 Secure ACS 5.1

### Instalação usando o dispositivo CSACS-1121 Series

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

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

### Instalar o servidor ACS

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

- Execute o programa de configuração
- Verificar o processo de instalação
- <u>Tarefas de pós-instalação</u>

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

## Configuração do controlador Cisco WLC5508

### Crie a configuração necessária para WPAv2/WPA

Execute estas etapas:

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

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



controlador.

- 2. Clique em login.
- 3. Faça login com o usuário padrão admin e a senha padrão admin.
- 4. Crie uma nova Interface para mapeamento VLAN no menu Controller.
- 5. Clique em Interfaces.
- 6. Clique em New.
- 7. No campo Nome da interface, informe *Funcionário*. (Esse campo pode ter qualquer valor que você desejar.)
- 8. No campo ID da VLAN, digite *20*. (Esse campo pode ser qualquer VLAN transportada na rede.)
- 9. Clique em Apply.
- Configure as informações conforme mostrado na janela Interfaces > Edit:Endereço IP da interface - 10.0.20.2Máscara de rede - 255.255.255.0Gateway - 10.0.10.1DHCP primário -10.0.10.10

միսիս			s	a <u>v</u> e Configuration	Ping   Logo	ut   <u>B</u> efrei
CISCO MONITOR WI	ANS CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP
Controller	Interfaces > Edit			< 84	ack /	pply
General Inventory Interfaces	General Informat	ion				
Multicast	Interface Name	em; 00:	ployee 24:97:69:4d:e	0		
Internal DHCP Server	Configuration					
<ul> <li>Mobility Management Ports</li> </ul>	Guest Lan					
NTP b CDP	Quarantine					
Advanced	Physical Informat	tion				
	Port Number		2			
	Backup Port		0			
	Enable Dynamic AF	Management				
	Interface Addres	s				
	VLAN Identifier		20			
	IP Address Netmask		255.255.255	0		
	Gateway		10.0.20.1			
	DHCP Information	n				
	Primary DHCP Ser	ver ierver	10.0.10.10			
	Access Control Li	st				
	ACL Name		none 💌		_	
	Note: Changing the In temporarily disabled a some clients.	terface param and thus may r	eters causes t esult in loss of	he WLANs to be f connectivity for		

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

սիսիս				S	ave Configuration	Ping   I	Logout <u>R</u> efree
CISCO MONITOR	WLANS		WIRELESS	SECURITY	MANAGEMENT	COMMAN	NDS HELP
WLANs	W	LANs > New			< Ba	sck	Apply
WLANS		Туре	E	WLAN 💌			
Advanced		Profile Name	E	Employee			
		SSID	E	Employee			
		ID		1			

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

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

IIIIII CISCO MONITOR	<u>w</u> lans <u>c</u> ontro	DLLER WIRELESS	Sa <u>S</u> ECURITY	ve Configuration	<u>Ping</u> Logout <u>R</u> efre
WLANs	WLANs > E	Edit		< Ba	ack Apply
WLANs	General	Security Q	S Advance	ed	
Advanced	Profile Name	Employee			
	Туре	WLAN			
	SSID	Employee			
	Status	Enabled			
	Security Policies	[WPA2][Aut] (Modifications of changes.)	a(802.1X)] done under secur	ity tab will appear	r after applying the
	Radio Po Interface Broadca SSID	alicy All e employee st IC Enabled	×		

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

WLANs > E	dit		
General	Security	QoS	Advanced
Layer 2	Layer 3	AAA Se	ervers
Layer 2 WPA+WPA	Security 🗐 🔽 Г 2 Parameter	VPA+WPA2 MAC Filte	ering
WPA Po	licy		
WPA2 P	olicy	2	
WPA2 E	ncryption	M AE	S 🗹 TKIP
Auth Ke	y Mgmt	802.1	1X 💌

autenticação. L

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

սիսիս		Save Configuration   Ping   Logout Befree
CISCO MONITOR WL	ANS <u>C</u> ONTROLLER	WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Security	RADIUS Auther	ntication Servers > New < Back Apply
<ul> <li>AAA         General         <ul> <li>RADIUS</li> <li>Authentication</li> <li>Accounting</li> <li>Fallback</li> </ul> </li> <li>TACACS+         <ul> <li>LDAP</li> <li>Local Net Users</li> <li>MAC Filtering</li> <li>Disabled Clients</li> <li>User Login Policies</li> <li>AP Policies</li> </ul> </li> </ul>	Server Index (Priority) Server IP Address Shared Secret Format Shared Secret Confirm Shared Secret Key Wrap	
Local EAP	Server Status	Enabled 💌
Priority Order	Support for	Enabled 💌
▶ Certificate	Server Timeout	2 seconds
Access Control Lists	Network User	Enable
<ul> <li>Wireless Protection Policies</li> </ul>	Management	Enable
Web Auth	IPSec	Enable
Advanced		

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

## Autenticação PEAP

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

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

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

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

#### Instalar o Snap-in de Modelos de Certificado

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

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

🌇 MyConsole - [Console Root\Ce	rtificate Templates]	
🚡 Elle Action View Favorites	<u>W</u> indow <u>H</u> elp	_8×
Console Root	Template Direlau Name /	Minimum Supported CAc.
Certificate Templates	Recharge Signature Only	Windows 2000
Contracto remplaces	Searchinge Signature Only	Windows 2000
	Light Exchange User	Windows 2000
	GegIPSec	Windows 2000
	LiggIPSec (Offline request)	Windows 2000
	Key Recovery Agent	Windows Server 2003, En
	RAS and IAS Server	Windows Server 2003, En
	Root Certification Authority	Windows 2000
	Router (Offline request)	Windows 2000
	Smartcard Logon	Windows 2000
	30 Smartcard Liser	Windows 2000
	29 Subordinate Certification Authority	Windows 2000
	Truck Lick Circling	Windows 2000
	Ligg Trust List Signing	Windows 2000
	GggUser	Windows 2000
	द्धि User Signature Only	Windows 2000
	Web Server	Windows 2000
	Workstation Authe Duplicate Template	Windows Server 2003, En 🖵
	All Tasks	
Using this template as a base, creates a	a template that supports Properties	

### Criar o Modelo de Certificado para o Servidor Web ACS

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

Properties of New Template
Issuance Requirements   Superseded Templates   Extensions   Security General   Request Handling   Subject Name
Template display name:
Copy of Web Server
Minimum Supported CAs: Windows Server 2003, Enterprise Edition
After you apply changes to this tab, you can no longer change the template name.
Iemplate name:
Copy of Web Server
Validity period: Renewal period:
2 years V 6 weeks V
Publish certificate in Active Directory
Do not automatically reenrol if a duplicate certificate exists in Active Directory
OK Cancel Apply

#### modelo. I

3. No campo Nome de exibição do modelo, insira

operties of New	Template	?
Issuance Require	ments   Superseded Templates   E	xtensions   Securi
General	Request Handling	Subject Name
Template display	name:	
ACS		
Minimum Support	ted CAs: Windows Server 2003, Ente	rprise Edition
After you apply c	hanges to this tab, you can no longer	change the template
name.		
Iemplate name:		
ACS		
⊻alidity period:	Benewal period:	
2 uears	F B weeks	-
I a l'icais		_
Publish certifi	icate in Active Directory	
E Constant	densities to second if the destruction and if	and a solute in A stine
Directory	tomatically reenrol in a duplicate certir	cate exists in Active
a narototy		
		on laroh

ACS.

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

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

Properties of N	ew Template 🧣	×
Issuance Requ General	uirements   Superseded Templates   Extensions   Secur Request Handling   Subject Name	w
Purpose:	Signature and encryption    Signature and encryption    Archive subject's encryption private key	]
Minimum key Minimum key Allow prive Allow prive Do the followi associated wi	size: 1024 ate key to be exported ng when the subject is enrolled and when the private key th this certificate is used:	
C Prompt the Prompt the private ke	ject without requiring any user input e user during enrollment e user during enrollment and require user input when the y is used	
To choose wh (CSPs) should	hich cryptographic service providers <u>C</u> SPs	
	OK Cancel Apply	

suspenso Purpose.

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

5P Selection		? >
Choose which cryptograph requests:	nic service providers (CSPs) ca	an be used in
C Requests can use any	CSP available on the subject	s computer
• Requests must use on	e of the following CSPs:	
<u>C</u> SPs:		
Gemplus GemSAFE Ca	rd CSP v1.0 e Smart Card CSP	-
Microsoft Base Cryptog     Microsoft Base DSS an     Microsoft DH SChanne     Microsoft Enhanced Cr     Microsoft Enhanced DS     Microsoft Enhanced RS     Microsoft Enhanced RS     Microsoft RSA SChanne	raphic Provider v1.0 nd Diffie-Hellman Cryptographic I Cryptographic Provider yptographic Provider v1.0 SS and Diffie-Hellman Cryptogr SA and AES Cryptographic Provider	aphic Prov
	OK	Cancel
	OK Cancel	

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

operties of New T	emplate						1
Issuance Requireme	ents Su	perseded	Template	25	Extensio	ons	Security
General	Rec	quest Han	dling		Sub	ject Na	ame
<ul> <li>Supply in the re Select this option not have acces Autoenrollment</li> <li>Build from this A</li> </ul>	quest on to allow ss to the di is not allow Active Dire	a variety omain of v wed if you ctory infor	of subjec which the choose t mation =	t na subj his d	me forma ject is a n option.	ts or if nembe	you do r.
Select this option simplify certificate Subject name for	n to enforc e administr rmat:	e consiste ation.	ency amor	ngs	ubject na	imes ai	nd to
None						Ŧ	
[Include e-ma	sil name in	subject na	ame				
Include this infor	mation in a	alternate s	ubject na	me:			
E-mail name							
DNS name							
□ User prinicip	al name (U	IPN)					
E Sergice print	cipal name	(SPN)					
	ſ	OK		Ca	ancel		Apply

OK. 🛏

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

Properties of New Template
General Request Handling Subject Name Issuance Requirements Superseded Templates Extensions Security
Require the following for enrollment:
This number of authorized signatures:
If you require more than one signature, autoenrollment is not allowed.
Bolicy type required in signature:
Application policy:
Issuance policies:
Add
Bemove
Require the following for reenrollment: Same criteria as for enrollment Valid existing certificate
OK Cancel Apply

documento.

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

### Habilitar o novo modelo de certificado de servidor Web ACS

- 1. Abra o snap-in Autoridade de Certificação. Execute as etapas de 1 a 3 na seção <u>Criar o</u> modelo de certificado para o servidor Web ACS, escolha a opção Autoridade de certificação, escolha Computador local e clique em Concluir.
- 2. Na árvore de console da Autoridade de certificação, expanda **ca.demo.local** e clique com o botão direito do mouse em **Modelos de certificado**.
- 3. Vá para New > Certificate Template to
| 🔯 Certification Authority     |          |                   |                                 |  |
|-------------------------------|----------|-------------------|---------------------------------|--|
| <u>File Action View H</u> elp |          |                   |                                 |  |
|                               | 😫 💵      |                   |                                 |  |
| Certification Authority (Lo   | cal)     | Name              |                                 |  |
| 📄 😰 ca.demo.local             |          | Dire              | ctory Email Replication         |  |
| Revoked Certificat            | es       | Dom 😥             | ain Controller Authentication   |  |
| Issued Certificates           | 5        | EFS               | Recovery Agent                  |  |
| Pending Requests              |          | Basic EFS         |                                 |  |
| Certificate Templa            | tec      | Domain Controller |                                 |  |
|                               | Manage   |                   | Server                          |  |
|                               |          |                   | huter                           |  |
|                               | New      | •                 | Certificate Template to Issue   |  |
|                               | View     |                   | rdinate Certification Authority |  |
|                               | <u></u>  |                   | histrator                       |  |
|                               | Refresh  |                   |                                 |  |
|                               | Export L | _ist              |                                 |  |
|                               | Help     |                   |                                 |  |
|                               | Tob      | -                 | 1                               |  |

Issue.

4. Clique no Modelo de certificado

#### ACS.

Enable Certificate Templates		?
elect one or more Certificate Templates to enable	e 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	<alb< td=""><td></td></alb<>	
🐹 Enrollment Agent	Certificate Request Agent	
🐹 Enrollment Agent (Computer)	Certificate Request Agent	
Exchange Enrollment Agent (Offline request)	Certificate Request Agent	
🐹 Exchange Signature Only	Secure Email	
Evohanne User	Secure Email	<u> </u>
		OK Cancel

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

lange Active Direct	ory Users and Computers
Sele Action	<u>Y</u> iew <u>W</u> indow <u>H</u> elp
(= >   🗈 🛙	0 🖻 🖻 🗟 😢 💷  🖉 🖢 🖓 🚳
Active Directo	ry Users and Computers [A eries Additional Sobjects Name All Tasks Yew New Window from Here
	Export List
	P <u>r</u> operties
	Help

## Propriedades.

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

demo.local Properties		? ×
General Managed By Group Policy		
To improve Group Policy management, upgrade Management Console (GPMC). Current Group Policy Object Links for	to the Group Po r demo	licy
Group Policy Object Links	No Override	Disabled
Group Policy Objects higher in the list have the h This list obtained from: AD2003.demo.local	ighest priority.	
New         Add         Edit           Options         Delete         Properties		Up Down
Block Policy inheritance		
Close	Cancel	Apply

Grupo.

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



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

Automatic Certificate Request Setup	Wizard 🗙
Certificate Template The next time a computer logs on, a provided.	certificate based on the template you select is
A certificate template is a set of pred computers. Select a template from th Certificate templates:	efined properties for certificates issued to e following list.
Name	Intended Purposes
Computer Domain Controller Enrollment Agent (Computer) IPSec	Client Authentication, Server Authenticatior Client Authentication, Server Authenticatior Certificate Request Agent IP security IKE intermediate
•	<b>&gt;</b>
	< <u>B</u> ack <u>N</u> ext > Cancel

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

🚡 Group Policy Object Editor			
Eile Action View Help			
S Default Domain Policy [AD2003.demo.local] Policy	Automatic Certificate Request		
E-B Computer Configuration	Computer		
Software Settings			
- Windows Settings			
— Scripts (Startup/Shutdown)			
E-B Security Settings			
Account Policies			
Local Policies			
Event Log			
Restricted Groups			
System Services			
Registry			
🕢 过 File System			
😑 🚞 Public Key Policies			
Encrypting File System			
Enterprise Trust			
Software Restriction Policies			
IP Security Policies on Active Directory (demo.local)			
Administrative Templates			
E 💭 User Configuration			
Software Settings			
⊕ —      Windows Settings			
Administrative Templates			

- 13. Na árvore do console, expanda **Configuração do usuário > Configurações do Windows > Configurações de segurança > Políticas de chave pública**.
- 14. No painel de detalhes, clique duas vezes em **Configurações de registro automático**.



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

rollme	ent Settings Prop	erties		? ×
ral				
7	Enroll user and cor	nputer certificates	automatically	
Don	ot enroll certificates	automatically		
V	Renew expired cert revoked certificates	ficates, update p	ending certificates, an	id remove
2	Update certificates	hat use certificat	e templates	
		OK	Cancel	Apply
	ral	ral         Enroll user and con         Do not enroll certificates         Enroll certificates automa         Enroll certificates automa         Image: Enroll certificates         Enroll certificates         Image: Enroll certificates </td <td>ral         Enroll user and computer certificates         Do not enroll certificates automatically         Enroll certificates automatically         Enroll certificates automatically         Image: Renew expired certificates, update prevoked certificates         Image: Update certificates that use certificates         OK</td> <td>ral         Image: Enroll user and computer certificates automatically         Do not enroll certificates automatically         Enroll certificates automatically         Image: Enroll certificates automaticertificates automatically</td>	ral         Enroll user and computer certificates         Do not enroll certificates automatically         Enroll certificates automatically         Enroll certificates automatically         Image: Renew expired certificates, update prevoked certificates         Image: Update certificates that use certificates         OK	ral         Image: Enroll user and computer certificates automatically         Do not enroll certificates automatically         Enroll certificates automatically         Image: Enroll certificates automaticertificates automatically

16. Click **OK**.

# Configuração do certificado ACS 5.1

Configurar certificado exportável para ACS

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

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

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

Add.					
► 🛠 My Workspace	System Administration > Config	juration > Local Server	Certificates > Local	Certificates	
► 🔄 Network Resources	Local Certificates		Sho	wing 1-1 of 1 50 💌	er page Go
Users and Identity Stores	Filler				
Policy Elements	rmar. [	Match II.		00	
► 🛵 Access Policies	Friendly Name	<ul> <li>Issued To</li> </ul>	Issued By	Valid From	Valid To (Ex
Monitoring and Reports	acs	acs	acs	04:29 20.09.2010	04:29 20.09
🔹 🍭 System Administration					
<ul> <li>Administrators         Accounts         Roles         Settings</li> <li>Users         Authentication Settings</li> <li>Operations         Distributed System Management         Software Repositories         Centralized Software Updates         Scheduled Backups         Local Operations</li> <li>Configuration         Solobal System Options         Dictionaries         Local Server Certificates         Local Server Certificates         Local Gentricates         Local Gentricates</li></ul>					
Migration Utility					
Sample Python Scripts	Add Edit Delete	Export		Page 1	of 1 🗾

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



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



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



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



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



8. Salve o arquivo .pem do certificado ACS no

Save As					?×
Save in:	Desktop		. 00	1 🗗 🖽 -	
My Recent Documents Desktop My Documents My Computer	My Documents My Computer	aces			
My Network	File name:	ACS_ctal		•	Save
Places	Save as type:	.pem Document		•	Cancel
					11.

## Instale o certificado no software ACS 5.1

Execute estas etapas:

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



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



#### certificado.

3. Clique em para enviar uma solicitação de certificado



#### avançada.

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

Microsoft Certificate Services - ca.demo.local	<u>Home</u>
Advanced Certificate Request	
The policy of the CA determines the types of certificates you can request. Click one of the following options to:	n
Create and submit a request to this CA.	
Submit a certificate request by using a base-64-encoded CM PKCS #10 file, or submit a renewal request by using a base- encoded PKCS #7 file.	<u>AC or</u> -64-
Request a certificate for a smart card on behalf of another us using the smart card certificate enrollment station. Note: You must have an enrollment agent certificate to submit a request behalf of another user.	er by on
benan or another oser.	

#### de base 64...

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

Submit a Certi	icate Request of Renewal Request
To submit a sav #10 certificate r source (such as	ed request to the CA, paste a base-64-encoded CMC or PKCS equest or PKCS #7 renewal request generated by an external a Web server) in the Saved Request box.
Saved Request:	
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	≍ ▼ Browse for a file to insert.
Certificate Templ	ate:
	Administrator 🔹
Additional Attribu	tes:
Attributes:	x x

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

Windows	Internet Explorer
♪	Your web browser security settings prohibit this page from accessing your disk. Either paste the data into this page manually, or add this page to your browser's list of trusted sites.
	ОК

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

ACS_csr PEM File 1 KB	
Open Edit	
Open With	🝺 Notepad
Send To 🕨	🏉 Internet Explorer
Cut Copy	Choose Program
Create Shortcut Delete Rename	
Properties	

Notas).

8. Realce todo o conteúdo do arquivo e clique em

📕 ACS_csr - Notep	ad	
File Edit Format	/iew Help	
BEGIN CER	Undo	ESTOMIIBVjCCA
	Cut	
	Сору	

Copiar.

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

Submit a Cert	ificate F	Request o	r Ren
oubline a cert	incuto r	lequest o	
To submit a sav	ved reau	lest to the	CA. D
renewal reques	t genera	ated by an	exterr
		-	
Saved Request:			
Base-64-encoded		Undo	
(CMC or		Cut	
PKCS #10 or		Сору	
PKCS #7):	7	Paste	
	Browne	Delete	-
		C-1- + + #	311
	Diowse	Select All	

campo Solicitação salva.

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

Saved Request:	
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	YIZIAYb4QgEBBAQDAgZAMA0GCSqGSIb3DQEBBQUA DXoioRABct447w077+uAk8crn26oaEhcfG/ZR15X ONZQ5xnrK23yxEdQNvSFC30mzRZEbQq4s5MvPEZZ /MWqXej3NjpicpAgiV8CSwNd END CERTIFICATE REQUEST
Certificate Templ	Browse for a file to insert. ate: ACS
Additional Attribu	nes.
Attributes:	X X X
	Submit >

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

s issued to you.
Base 64 encoded
chain
File Download - Security Warning
Do you want to open or save this file?
Name: certnew.cer
Type: Security Certificate, 1.88KB From: ca
UpenSaveCano
where test from the internet can be useful, this file type can potentially harm your computer. If you do not trust the source.

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



trabalho.

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



14. Clique em Browse e localize o certificado

<ul> <li>Select server certificate creation method</li> <li>Bind CA Signed Certificate</li> </ul>	
Step 2 -Bind CA Signed Certificate	
Certificate File:     Brows	æ
Protocol	
EAP: Used for EAP protocols that use SSL/TLS tunneling	
Management Interface: Used to authenticate the web server (GUI)	
Override Policy	
A certificate being imported may be determined to already exist in ACS when it Subject or Issuer and serial number as an existing certificate. In such a case, a "Replace Certificate" option will allow the certificate contents to be replaced whe existing protocol selections for the certificate.	has either the same selection of the ile retaining the
Replace Certificate	

salvo. <sup>L</sup>

Abrir.

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

Choose file						<u>?</u> ×
Look in:	Desktop		•	+ 8 0	* 🔳 •	
My Recent Documents Desktop My Documents My Computer	My Documents My Computer My Network Pla ACS_cert ACS_csr	ces				
My Network Places	File name: Files of type:	ACS, cert All Files (".")		1		Open Cancel

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



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

Λ	റ	C	
	U.	J	

system Administration > Configuration > Local Server Certificates > Local Certificates								
Local Certificates Showing 1-2 of 2 50 💌								
Filter: Match if: Go 🔽								
	Friendly Name	•	Issued To	Issued By	Valid From			
	acs		acs	acs	04:29 20.09.2010			
	acs.demo.local		acs.demo.local	ca.demo.local	10:39 22.09.2010			

## Configurar o Repositório de Identidades do ACS para o Ative Diretory

Execute estas etapas:

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



#### Diretory.

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

General	Directory Groups	Directory Attributes	
Connecti	on Details		
Active D Name:	irectory Domain	demo.local	
Please sp	ecify the credential	Is used to join this machin	te to the Active Directory Domain:
0 Userna	me:	administrator	
Passw	ord		-
You may u reachable	use the Test Conne	ection Button to ensure cre Test Connection	edentials are correct and Active Directory Doma
rou may u reachable	use the Test Conne	ection Button to ensure cre Test Connection	edentials are correct and Active Directory Doma
You may t reachable Click on 'S	use the Test Conne Save Changes' to c sessfully connected	Test Connection	ory Domain and save this configuration. Once y
You may u reachable Click on 'S have succ o be avail	use the Test Conne Save Changes' to c sessfully connected lable for use in poli	Test Connection Test Connection onnect to the Active Direct to the Domain, yt Window icy rules.	ory Domain and save this configuration. Once y
You may u reachable Click on 'S have succ to be avail	use the Test Conne Save Changes' to c ressfully connected lable for use in poli	Test Connection Test Connection onnect to the Active Direct to the Domain, yt Window icy rules.	ory Domain and save this configuration. Once y s Internet Explorer
You may t reachable Click on % have succ to be avail End User	ase the Test Conne Save Changes' to c ressfully connected lable for use in poli	Test Connection Test Connection onnect to the Active Direct to the Domain, yt Window icy rules.	ony Domain and save this configuration. Once y s Internet Explorer
You may o reachable Click on S have succ o be avail End User I En En:	ase the Test Conne Save Changes' to c essfully connected lable for use in poli <b>Authentication Se</b> able password cha	Test Connection Test Connection onnect to the Active Direct to the Domain, yr Window icy rules.	ory Domain and save this configuration. Once y s Internet Explorer Connection test to 'demo.local' succeeded.
Click on 'S have succ be avail End User F En: F En:	use the Test Conne Save Changes' to c ressfully connected lable for use in poli <b>Authentication Se</b> able password cha	ection Button to ensure cre Test Connection onnect to the Active Direct to the Domain, yt Window icy rules.	ory Domain and save this configuration. Once y sa Internet Explorer Connection test to 'demo.local' succeeded.

continuar.

4. Clique em Save



Observação:

para obter mais informações sobre o procedimento de integração do ACS 5.x, consulte <u>ACS</u> 5.x e posterior: Exemplo de Configuração de Integração com o Microsoft Ative Diretory.

## Adicionar um controlador ao ACS como um cliente AAA

Execute estas etapas:

Changes.

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



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

Description:			
Location	All Locations		Select
Device Type	All Device Types		Select
IP Address Single IP Address IP: 10.0.1.10	C IP Range (s)	Authentication Options TACACS+ Shared Secret Shared Secret Single Connect Device C Legacy TACACS+ Sing TACACS+ Draft Comple Support RADIUS Support Shared Secret: Shared	le Connect Supp iant Single Conr ec identification

compartilhado - cisco

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

► 🛠 My Workspace	Network	Resources	s > Ne	twork Devices an	d AAA Clients		
Network Resources	Network Devices Showing						Showing 1-1 of 1
Network Device Groups     Network Devices and AAA Clients	Filte	r. 🗌		Match	it.	٠	Go 🔻
Default Network Device External RADIUS Servers		Name	•	IP / Mask	NDG:Location		NDG:Device Type
Busers and Identity Stores     Store		wic		10.0.1.10/32	All Locations		All Device Types
Policy Elements							
Access Policies							
Monitoring and Reports							

## Configurar políticas de acesso ACS para rede sem fio

Execute estas etapas:

1. No ACS, vá para Access Policies > Access



#### Services.

2. Na janela Serviços do Access, clique em

Acces	s Services			Showing 1-2 of 2	50 💌 p
Filter:		Match if	t	Go 🔻	
	Name	•	Service Type	Included Policies	Descript
	Default Devic	e Admin	Device Administration	Identity Authorization	Default
	Default Netw	ork Access	Network Access	Identity Authorization	Default

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

no modelo de serviço e clique em Selecionar.

Access Policies > Access Services > Create	
General Allowed Protocols	
Step 1 - General	
General	
Name: WirelessAD	
Description:	
Access Service Policy Structure	
Based on service template	Select
C Based on existing service	Select
C User Selected Service Type Network Access	

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

Acce	ss Services		Showing 1-4
Filter	Match if:	Go 🔻	
	Name 🔺	Service Type	Description
0	Device Admin - Command Auth	Device Administration	
0	Device Admin - Simple	Device Administration	
0	Network Access - MAC Authentication Bypass	Network Access	
•	Network Access - Simple	Network Access	

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

Step 1 - General	
General	
Name: WirelessAD	
Description:	
Access Service Policy Structur	re
Based on service template	Network Access - Simple Select
C Based on existing service	Select
C User Selected Service Type	Network Access
ar.	

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



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



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



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

🗿 Cisco S	Secure ACS We	bpage Dialog							
Identit	Identity Store								
Filter:		Match if: Go 🗢							
	Name 🔺	Description							
C	AD1								
0	CN Username	Predefined Certificate Authentication Profile							
0	DenyAccess								
0	Internal Hosts								
0	Internal Users								
0	NAC Profiler	Default Entry for NAC Profiler							

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

OK.

	Access Policies > Access Services > WirelessAD > Identity	
	Single result selection C Rule based result se	lection
	Identity Source: AD1	Select
Changes	Advanced Options	

## Criar política de acesso e regra de serviço ACS

Execute estas etapas:

1. Vá para Access Policies > Service Selection Rules.



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

C	Cisco Secure ACS Webpage Dialog
	General Name: WirelessRule Status: Enabled 💌 😂
	The Customize button in the lower right area of the policy rules scree conditions and results are available here for use in policy rules.
	Conditions  Protocol: match Select
	Results

C	Cisco	Secure ACS -	- Webpage Di
	Enun	n Definition	
		Enum Name	e ID
	C	Radius	0
	С	Tacacs	1

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

Conditions			
Protoco	I: match	<ul> <li>Radius</li> </ul>	Sele

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

	Ser	vice Se	election P	olicy			
	Filt	er: Sta	itus 💽	Match if: Equa	uls 💌	• C	lear P
			Status	Name	Protocol	Conditions	
	3		•	WirelessRule	match Radius		200
	1		0	Rule-1	match Radius		
	2		Θ	Rule-2	match Tacacs		
	<b>1</b>		Default		If no rules detro	ed or no enabled	Irule
Diretory.	C	reate	•  Di	uplicate   · E	dit Delete	Move to	V

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

## Executar uma Instalação e Configuração Básicas

Execute estas etapas:

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

## Instale o adaptador de rede wireless

Execute estas etapas:

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

## Configurar a conexão de rede sem fio

Execute estas etapas:

- 1. Faça logoff e depois faça logon usando a conta **WirelessUser** no domínio **demo.local**.
- 2. Escolha **Iniciar > Painel de controle**, clique duas vezes em **Conexões de rede** e clique com o botão direito do mouse em **Conexão de rede sem fio**.
- 3. Clique em **Properties**, vá para a guia **Wireless Networks** e verifique se a opção **Use Windows to configure my wireless network settings** está

👃 Wireless Network Connection P	roperties	<u>? ×</u>			
General Wireless Networks Advan	ced				
Use Windows to configure my wi	eless network settings				
Available networks:					
To connect to, disconnect from, or find out more information about wireless networks in range, click the button below.					
	View Wireless Networks				
below:	Move up	, 			
Add Remove	Properties				
configuration.	Advanced				
	OK Car	ncel			

marcada.

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

Wireless network properties		?)
Association Authentication 0	Connection	
Network name (SSID):	mployee	
Wireless network key		
This network requires a key	for the following:	
Network Authentication:	WPA	-
Data encryption:	TKIP	•
Network key:		
Confirm network key.		
Key index (advanced):		
The key is provided for r	ne automatically	
This is a computer-to-comp access points are not used	outer (ad hoc) network; v I	vireless
	OK	Cancel

definida como TKIP.

7. Clique na guia Authentication.

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

Wireless net	work properties	? ×
Association	Authentication Connection	
Select this wireless Et	option to provide authenticated network access for hemet networks.	
₽ <u>E</u> nable	IEEE 802.1x authentication for this network	
EAP type:	Protected EAP (PEAP)	•
	Propertie	s
Authen availab	ticate as <u>c</u> omputer when computer information is le ticate as guest when user or computer information is lable	
	OK Car	ncel

#### disponíveis.

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

Protected EAP Properties	1			
When connecting:				
Validate server certificate				
Connect to these servers:				
Trusted Root Certification Authorities:				
C&W HKT SecureNet CA Root				
CA 1				
✓ ca.demo.local				
Certiposte Classe A Personne				
Certiposte Serveur				
Certisign - Autoridade Certificadora - AC2				
Certisign - Autoridade Certificadora - AC4				
Do not grompt user to authorize new servers or trusted certification authorities.				
Select Authentication Method:				
Secured password (EAP-MSCHAP v2)				
Finable Fast Reconnect				
OK Cancel				

interna.

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



- 16. Depois que a autenticação for bem-sucedida, verifique a configuração TCP/IP do adaptador sem fio usando Conexões de rede. Ele deve ter um intervalo de endereço de 10.0.20.100-10.0.20.200 do escopo do DHCP ou do escopo criado para os clientes sem fio CorpNet.
- 17. Para testar a funcionalidade, abra um navegador e vá até http://10.0.10.10 (ou o endereço IP do servidor CA).

# Solucionar problemas de autenticação sem fio com ACS

Execute estas etapas:

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



Visualizador de relatórios.

2. Uma janela ACS separada será aberta. Clique em



#### Painel.

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

ly Favorite Reports					
Report Name					
ACS Instance>ACS_Configuration_Audi					
ACS Instance>ACS_System_Diagnostics					
AAA Protocol>RADIUS_Authentication					

Hoje. 느

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

AAA Protocol > RADI	US Authenti	cation				
Authentication Status : Date :	Pass or Fail September 22, 2010 ( <u>Last 30 Minutes</u>   <u>Last Hour</u>   <u>Last 12 Hours</u>   Today   <u>Yesterday</u>   <u>Last 7 Days</u>   <u>Last 30 Days</u> )					
Generated on September	22, 2010 5:51	34 PM PDT				
Logged At	RADIUS Status	NAS Failure Details	Username	MAC/IP Address	Access Service	Authentication Method
Sep 22,10 5:51:17.843 F	PM 🖌	٩,	wirelessuser	00-21-5c-69-9a-39	WirelessAD	PEAP (EAP-MSCHAPv2)

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

AAA Protocol > RADIUS Authentication Detail					
ACS session ID : acs/74551189/31 Date : September 22, 2010					
Generated on September 22, 2010 5:52:16 PM PDT					
Authentication Summary					
Logged At:	September 22,2010 5:51:17.843 PI				
RADIUS Status:	Authentication succeeded				
NAS Failure:					
Username:	wirelessuser				
MAC/IP Address:	00-21-5c-69-9a-39				
Network Device:	wlc : 10.0.1.10 :				
Access Service:	WirelessAD				
Identity Store:	AD1				
Authorization Profiles:	Permit Access				
CTS Security Group:					
Authentication Method:	PEAP(EAP-MSCHAPv2)				
6. A contagem de ocorrências do serviço ACS pode fornecer uma visão geral das tentativas que correspondem às regras criadas no ACS. Vá para ACS > Access Policies > Access Services e clique em Service Selection

Results Service	Hit Count
WirelessAD	33
Default Network Access	0

## A autenticação PEAP falha com o servidor ACS

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

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

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

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

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

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

## Informações Relacionadas

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

## 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.