Autenticação EAP Local no Controller de LAN Wireless com EAP-FAST e Exemplo de Configuração de Servidor LDAP

Contents

Introduction **Prerequisites** Requirements **Componentes Utilizados Conventions** Informações de Apoio Configurar Diagrama de Rede Configurações Configurar EAP-FAST como método de autenticação EAP local no WLC Gerar um certificado de dispositivo para a WLC Download do certificado do dispositivo na WLC Instalar o certificado raiz de PKI no WLC Gerar um certificado de dispositivo para o cliente Gerar o Certificado de CA Raiz para o Cliente Configurar o EAP local no WLC Configurar servidor LDAP Criando usuários no controlador de domínio Configurar o usuário para acesso ao LDAP Usando o LDP para identificar os atributos do usuário Configurar cliente sem fio Verificar Troubleshoot Informações Relacionadas

Introduction

Este documento explica como configurar o EAP (Extensible Authentication Protocol) -Autenticação Flexível via Autenticação EAP Local (FAST - Secure Tunneling) em uma controladora Wireless LAN (WLC). Este documento também explica como configurar o servidor de Lightweight Directory Access Protocol (LDAP) como um banco de dados de backend para EAP Local para retornar as credenciais de usuários e autenticar o usuário.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- Cisco 4400 Series WLC que executa o firmware 4.2
- Pontos de acesso Lightweight (LAP) Cisco Aironet 1232AG Series
- Servidor Microsoft Windows 2003 configurado como controlador de domínio, servidor LDAP e servidor de Autoridade de certificação.
- Adaptador do cliente do Cisco Aironet 802.11 a/b/g que executa o firmware versão 4.2
- Cisco Aironet Desktop Utility (ADU) que executa o firmware versão 4.2

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>

Informações de Apoio

A autenticação EAP local em controladores de LAN sem fio foi introduzida com a versão 4.1.171.0 do controlador de LAN sem fio.

O EAP local é um método de autenticação que permite que usuários e clientes sem fio sejam autenticados localmente no controlador. Ele foi projetado para uso em escritórios remotos que desejam manter a conectividade com clientes sem fio quando o sistema de back-end for interrompido ou o servidor de autenticação externo for desativado. Quando você habilita o EAP local, o controlador serve como o servidor de autenticação e o banco de dados de usuário local, eliminando a dependência de um servidor de autenticação externo. O EAP local recupera as credenciais do usuário do banco de dados de usuário local ou do banco de dados back-end LDAP para autenticar usuários. O EAP local oferece suporte à autenticação LEAP, EAP-FAST, EAP-TLS, P EAPv0/MSCHAPv2 e PEAPv1/GTC entre a controladora e os clientes sem fio.

O EAP local pode usar um servidor LDAP como seu banco de dados de back-end para recuperar credenciais do usuário.

Um banco de dados back-end LDAP permite que o controlador solicite as credenciais (nome de usuário e senha) de um usuário específico a um servidor LDAP. Essas credenciais são, então, usadas para autenticar o usuário.

O banco de dados back-end LDAP oferece suporte aos seguintes métodos EAP locais:

- EAP-FAST/GTC
- EAP-TLS

• PEAPv1/GTC

LEAP, EAP-FAST/MSCHAPv2 e PEAPv0/MSCHAPv2 também são suportados, **mas somente se o servidor LDAP estiver configurado para retornar uma senha de texto não criptografado**. Por exemplo, o Microsoft Ative Diretory não tem suporte porque não retorna uma senha de texto não criptografado. Se o servidor LDAP não puder ser configurado para retornar uma senha de texto não criptografado, LEAP, EAP-FAST/MSCHAPv2 e PEAPv0/MSCHAPv2 não serão suportados.

Observação: se algum servidor RADIUS estiver configurado no controlador, o controlador tentará autenticar os clientes sem fio usando primeiro os servidores RADIUS. Tentativa de EAP local somente se nenhum servidor RADIUS for encontrado, seja porque os servidores RADIUS atingiram o tempo limite ou porque nenhum servidor RADIUS foi configurado. Se quatro servidores RADIUS forem configurados, a controladora tentará autenticar o cliente com o primeiro servidor RADIUS, depois o segundo servidor RADIUS e, em seguida, EAP local. Se o cliente tentar reautenticar manualmente, a controladora tentará o terceiro servidor RADIUS, depois o quarto servidor RADIUS e, em seguida, EAP local. Se o cliente tentar reautenticar manualmente, o EAP local.

Este exemplo usa EAP-FAST como o método Local EAP no WLC, que por sua vez é configurado para consultar o banco de dados back-end LDAP para as credenciais do usuário de um cliente sem fio.

Configurar

Este documento usa EAP-FAST com certificados no lado do cliente e no lado do servidor. Para isso, a instalação usa o servidor **Microsoft Certificate Authority (CA)** para gerar os certificados de cliente e servidor.

As credenciais do usuário são armazenadas no servidor LDAP de modo que, na validação de certificado bem-sucedida, o controlador consulte o servidor LDAP para recuperar as credenciais do usuário e autentique o cliente sem fio.

Este documento pressupõe que estas configurações já estão em vigor:

- Um LAP é registrado na WLC. Consulte <u>Registro de AP Lightweight (LAP) em uma</u> <u>controladora Wireless LAN (WLC)</u> para obter mais informações sobre o processo de registro.
- Um servidor DHCP é configurado para atribuir um endereço IP aos clientes sem fio.
- O servidor Microsoft Windows 2003 está configurado como controlador de domínio e como servidor de autoridade de certificação. Este exemplo usa wireless.com como o domínio.Consulte <u>Configuração do Windows 2003 como um Controlador de Domínio</u> para obter mais informações sobre como configurar um servidor Windows 2003 como um controlador de domínio.Consulte <u>Instalação e Configuração do Microsoft Windows 2003</u> <u>Server como um Servidor de Autoridade de Certificação (CA)</u> para configurar o servidor Windows 2003 como servidor de Autoridade de Certificação Corporativa.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Configurações

Conclua estas etapas para implementar esta configuração:

- Configurar EAP-FAST como método de autenticação EAP local no WLC
- <u>Configurar servidor LDAP</u>
- <u>Configurar cliente sem fio</u>

Configurar EAP-FAST como método de autenticação EAP local no WLC

Como mencionado anteriormente, este documento usa EAP-FAST com certificados no lado do cliente e do servidor como o método de autenticação EAP local. A primeira etapa é baixar e instalar os seguintes certificados no servidor (WLC, neste caso) e no cliente.

A WLC e o cliente precisam desses certificados para serem baixados do servidor de CA:

- Certificado do dispositivo (um para a WLC e outro para o cliente)
- Certificado raiz da Public Key Infrastructure (PKI) para a WLC e certificado CA para o cliente

Gerar um certificado de dispositivo para a WLC

Execute estas etapas para gerar um certificado de dispositivo para o WLC do servidor CA. Este certificado de dispositivo é usado pela WLC para autenticar o cliente.

 Acesse http://<endereço IP do servidor de CA>/certsrv no PC que tem uma conexão de rede com o servidor de CA. Faça logon como administrador do servidor de autoridade de certificação.



2. Selecione Request a certificate.

Microsoft Certificate Services - Microsoft Internet Explorer	
File Edit View Favorites Tools Help	
1d3/H33 🕘 http://10.77.244.198/certary/	🚽 🔁 👄
Microsoft Certificate Services wireless	Home
Welcome	
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using identity to people you communicate with over the Web, sign and encrypt messages, and, depending upo perform other security tasks.	a certificate, you can verify your in the type of certificate you request,
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or ce view the status of a pending request.	rtificate revocation list (CRL), or to
For more information about Certificate Services, see Certificate Services Documentation.	
Select a task: Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL	
	Internet

3. Na página Solicitar um certificado, clique em solicitação avançada de

certificado.	
Microsoft Certificate Services - Microsoft Internet Explorer	
File Edit Wew Favorities' Tools Help	A Y
Address 🕘 http://10.77.244.198/certsrv/certraps.asp	🛁 🛃 Go
Microsoft Cartificate Services wireless	Home
Request a Certificate	
Select the certificate type: User Catheren Or (submit an advanced certificate request.	
	<u></u>
http://10.77.244.198/centerv/centrgad.asp	 Internet

 Na página Solicitação avançada de certificado, clique em Criar e enviar uma solicitação a esta CA. Isso o levará para o formulário de solicitação de certificado Avançado.

Microsoft Certificate Services - Microsoft Internet Explorer	
Nie Edz View Pavorites Tools Help	
iddress 🕘 http://10.77.244.198/certsrv/certrgad.asp	🗹 🛃 Go
Microsoft Certificate Services wireless	Heme
Advanced Certificate Request	
The policy of the CA determines the types of certificates you can request. Click one of the follo	ving options to:
Create and submit a request to this CA	and channels.
Submit a certificate request by using a base Muencoded CMC or RKCS #10 file, or submit	a ranewal remeat by using a base. B4-ancoded
PKCS #7 file	a reneral respect of sample state of streams
Request a certificate for a smart card on behalf of another user by using the smart card cert	icate enrolment station.
Note: You must have an enrollment agent certificate to submit a request on behalf of another user.	
	Internet

- 5. No formulário de solicitação de certificado avançado, escolha Servidor Web como o Modelo de certificado. Em seguida, especifique um nome para este certificado de dispositivo. Este exemplo usa o nome do certificado como ciscowlc123. Preencha as outras informações de identificação de acordo com sua exigência.
- 6. Na seção Key Options, selecione a opção Mark Keys as Exportable. Às vezes, essa opção específica ficará esmaecida e não poderá ser ativada ou desativada se você escolher um modelo de servidor Web. Nesses casos, clique em Voltar no menu do navegador para voltar uma página e voltar novamente a essa página. Desta vez, a opção Mark Keys as Exportable (Marcar chaves como exportáveis) deve estar

disponível.	
Microsoft Certificate Services - Microsoft Internet Explorer	T 6 🗙
File Edt View Pavorites Tools Help	A
Gast · D - B & Pearth frances @ B · D - 3	
Address at http://10.77.244.198/cartsrv/certsrgna.asp	💌 🛃 GO
ANCRUSOF CHIRCHE Semices miletess	neme
Advanced Certificate Request	
Certificate Template:	
Web Server	
Identifying Intermation For Offline Template:	
Tiame: ciscowic123	
6-421	
Company: eisco	
Department:	
City	
State:	
Country/Region	
Key Options:	
Create new key set Ouse existing key set	
CSP: Microsoft RSA SChannel Cryptographic Provider V	
Key Usage: @ Exchange	
Key Size: 1024 Max: 10304 (common key size:: 512 1024 2048 4098 9192 10294)	
Automatic key container name Ouser specified key container name	
Mark keys as exportable	
Export keys to file	
E Enable strong private key protection	
Store certricate in the local computer certificate store	
Done	Internet

7. Configure todos os outros campos necessários e clique em **Enviar**.

Alicrosoft Certificate Services - Microsoft Internet Explorer	
File Edit View Pavorites Tools Help	At
🔇 Sad. • 🕥 - 🖹 📓 🐔 🔎 Search 👷 Pavortes 🤣 😥 🖓 🖼 🖄	
Address and http://10.77.244.198/centerv/centrgna.asp	💌 🛃 😡 .
Create new key set Use existing key set	
CSP: Microsoft RSA SChannel Cryptographic Previder 🛩	
Key Usage. 🛞 Exchange	
Key Size: 1024 Mir: 004 (cemmon keysizer: 512 3029 2089 4085 5192 35385)	
Automatic key container name	
Mark keys as exportable	
Export keys to file	
Enable strong private key protection	
Stores the certificate in the local computer centricate store Stores the certificate in the local computer atore instead of in the user's certificate store. Does not install the root CA's certificate. You must be an administrator to generate or use a key in the local machine store.	
Additional Options:	
Request Format: O CMC	
Hash Algorithm: SHA-1 V	
Only used to sign request.	
Save request to a file	
Attributes:	
Friendly Name:	
Submit >	
LA.	

8. Clique em **Yes** na próxima janela para permitir o processo de solicitação de certificado.

Potentia	al Scripting Violation
♪	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

 A janela Certificado Emitido é exibida, indicando um processo de solicitação de certificado bem-sucedido. A próxima etapa é instalar o certificado emitido no repositório de certificados deste computador. Clique em Instalar este certificado.

Alicrosoft Certificate Services - Microsoft Internet Explorer	
File Edit View Favorities' Tools Help	
Address 💩 http://10.77.244.198/certsrv/certfirsh-asp	🛩 🛃 Go
Manual Carl Carl Carlson Station	
ABCASSOR Certificate Services - witeross	Home
Certificate Issued	
The certificate you requested was issued to you.	
Install this certificate	
	8
a)	Internet

10. O novo certificado é instalado com êxito no computador de onde a solicitação é gerada para o servidor de autoridade de

🛩 🔁
Home
Internet
ficados para

11. A próxima etapa é exportar esse certificado do armazenamento de certificados para o disco rígido como um arquivo. Este arquivo de certificado será usado posteriormente para baixar o certificado para a WLC.Para exportar o certificado do armazenamento de certificados, abra o navegador Internet Explorer e clique em Ferramentas > Opções da Internet.

Pla Edit View Eavortes Tools Hills	-
The same term into the same term into the	100
Address and advantiblevik	
Enables you to change settings.	-

12. Clique em **Content > Certificates** para ir para o armazenamento de certificados onde os certificados são instalados por

 Os certificados do dispositivo são geralmente instalados na lista de certificados Personal. Aqui, você deve ver o certificado recém-instalado. Selecione o certificado e clique em Exportar.

Certificates			? 🔀
Intended purpose:	<all></all>		~
Personal Other Peop	le Intermediate Certificatio	n Authorities Trusted Root Certif	icatior 🔹 >
Issued To	Issued By	Expiratio Friendly Name	<u> </u>
🕅 ciscowlc123	wireless	1/25/2010 <none></none>	
Import Exp	ort Remove		dvanced
Certificate intended p	rposes		
Server Authentication			
			A Marca Andrea State Sta
			View

14. Clique em Avançar nas janelas a seguir. Escolha a opção Sim, exportar a chave privada na janela Assistente de Exportação de Certificado. Clique em

Next.	
Certificate Export Wizard	
Export Private Key You can choose to export the private key with the certificate.	
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.	¢
Do you want to export the private key with the certificate?	
Yes, export the private key	
No, do not export the private key	
< Back Next > Car	ncel

 Escolha o formato do arquivo de exportação como .PFX e escolha a opção Habilitar proteção forte. Clique em Next.

ate Export Wizard
rt File Format Certificates can be exported in a variety of file formats.
elect the format you want to use:
O DER encoded binary X.509 (.CER)
Base-64 encoded X.509 (.CER)
O Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
Include all certificates in the certification path if possible
Personal Information Exchange - PKCS #12 (.PFX)
Include all certificates in the certification path if possible
Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)

16. Na janela Senha, digite uma senha. Este exemplo usa **cisco** como a senha.

Certificate Export Wizard	×
Password To maintain security, you must protect the private key by using a password.	
Type and confirm a password.	
Password:	

Confirm password:	

< <u>B</u> ack <u>N</u> ext > Cance	

 Salve o arquivo de certificado (arquivo .PFX) no disco rígido. Clique em Avançar e conclua o processo de exportação com êxito.



Download do certificado do dispositivo na WLC

Agora que o certificado do dispositivo WLC está disponível como um arquivo .PFX, a próxima etapa é baixar o arquivo para o controlador. As WLCs da Cisco aceitam certificados somente no formato .PEM. Portanto, você precisa primeiro converter o arquivo de formato .PFX ou PKCS12 para um arquivo PEM usando o programa openSSL.

Converter o certificado em PFX para o formato PEM usando o programa openSSL

Você pode copiar o certificado para qualquer PC em que tenha o openSSL instalado para convertê-lo para o formato PEM. Digite estes comandos no arquivo Openssl.exe na pasta bin do programa openSSL:

Observação: você pode fazer download do openSSL no site do OpenSSL .

!--- This is the same password that is mentioned in step 16 of the previous section. MAC
verified Ok Enter PEM Pass phrase : cisco
!--- Specify any passphrase here. This example uses the PEM passphrase as cisco. Verifying - PEM
pass phrase : cisco

O arquivo de certificado é convertido no formato PEM. A próxima etapa é fazer o download do certificado do dispositivo no formato PEM para o WLC.

Observação: antes disso, você precisa de um software de servidor TFTP em seu PC de onde o arquivo PEM será baixado. Este PC deve ter conectividade com a WLC. O servidor TFTP deve ter seu diretório atual e o diretório base especificados com o local onde o arquivo PEM está armazenado.

Faça o download do certificado do dispositivo de formato PEM convertido para o WLC

Este exemplo explica o processo de download através do CLI do WLC.

- 1. Faça login na CLI da controladora.
- 2. Insira o comando transfer download datatype eapdevcert.
- 3. Insira o comando **transfer download serverip** *10.77.244.196*.10.77.244.196 é o endereço IP do servidor TFTP.
- 4. Insira o comando **transfer download filename** *ciscowlc.pem*.ciscowlc123.pem é o nome de arquivo usado neste exemplo.
- 5. Insira o comando transfer download certpassword para definir a senha do certificado.
- 6. Insira o comando transfer download start para exibir as configurações atualizadas.Em seguida, responda y quando for solicitado que confirme as configurações atuais e inicie o processo de download.Este exemplo mostra a saída do comando download: (Cisco Controller) >transfer download start

7. Digite o comando **reset system** para reinicializar a controladora. O controlador agora está carregado com o certificado do dispositivo.

Instalar o certificado raiz de PKI no WLC

Agora que o certificado do dispositivo está instalado na WLC, a próxima etapa é instalar o certificado raiz da PKI na WLC a partir do servidor da CA. Execute estas etapas:

1. Acesse http://<endereço IP do servidor de CA>/certsrv no PC que tem uma conexão de rede com o servidor de CA. Efetue login como administrador do servidor de



2. Clique em Baixar um certificado de CA, uma cadeia de certificados ou um CRL.

🗟 Microsoft Certificate Services - Microsoft Internet Explorer 🗧 🖬 🔀
Plan Edit Vern Filteritas Tooks teep
Address 🍯 http://10.77.244.198/certsrv/
Microsoft Certificate Services ···· wireless Herme
Welcome
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.
For more information about Certificate Services, see Certificate Services Documentation.
Select a task: Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL
internet

3. Na página resultante, você pode ver os certificados CA atuais disponíveis no servidor CA na caixa CA certificate. Escolha DER como o método de codificação e clique em Download CA certificate.

🗿 Microsoft Certificate Services - Microsoft Internet Explorer	
File Edit View Favorities' Tools Help	
Address 🕘 http://10.77.244.198/certsrv/certcarc.asp	🛩 💽
Microsoft Certificate Services - wireless	Home
Download a CA Certificate, Certificate Chain, or CRL	
To trust certificates issued from this certification authority, install this CA certificate chain.	
To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.	
CA centificate:	
Current (wireless)	
Encoding method:	
ODER	
O Base 64 Download CA certificate	
Download CA certificate chain	
Download latest base CRL Download latest delta CRL	
2	
概2	- Internet

- 4. Salve o certificado como um arquivo **.cer**. Este exemplo usa **certnew.cer** como o nome do arquivo.
- 5. O próximo passo é converter o arquivo .cer para o formato PEM e baixá-lo para a controladora. Para executar essas etapas, repita o mesmo procedimento explicado na seção Download do certificado do dispositivo para a WLC com estas alterações:Os arquivos openSSL "-in" e "-out" são certnew.cer e certnew.pem.Além disso, nenhuma senha PEM ou senha de importação é necessária nesse processo.Além disso, o comando openSSL para converter o arquivo .cer para o arquivo .pem é:x509 -in certnew.cer -inform DER -out certnew.pem -outform PEMNa etapa 2 da seção Download the Converted PEM Format Device Certificate to the WLC, o comando para baixar o certificado para a WLC é:(Cisco Controller)>transferir download tipo de dados eapcacertO arquivo a ser baixado para a WLC é certnew.pem.

Você pode verificar se os certificados estão instalados na WLC a partir da GUI da controladora, da seguinte maneira:

 Na GUI da WLC, clique em Security. Na página Security, clique em Advanced > IPSec Certs nas tarefas que aparecem à esquerda. Clique em CA Certificate para exibir o certificado de CA instalado. Aqui está o exemplo:



 Para verificar se o certificado do dispositivo está instalado na WLC, na GUI da WLC, clique em Security. Na página Security, clique em Advanced > IPSec Certs nas tarefas que aparecem à esquerda. Clique em ID Certificate para exibir o certificado do dispositivo instalado. Aqui está o

exemplo:									
awic2006 - Microsoft Inter	rnet Explorer								
File Edit View Favorites	Tools Help								
սիսիս									n <u>P</u> ing Logout <u>R</u> efresh
CISCO	MONITOR	WLANS	CONTROLLER	W1RELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
Security	ID Certific	ate			\bigcirc				New
- ARA	Name		Ya	lid Period					
General RADIUS Authentication	bsnSslEapD	levCert	Fire	m 2008 Jan 24	th, 12:18:31 (GMT Until 2010 Jac	n 23rd, 12:18:31		
Accounting									
Local Net Users MAC Filtering									
Disabled Clients User Login Policies AP Policies									
E Local EAP									
Priority Order									
E Access Control Lists									
Wireless Protection Policies									
N Web Auth									
ID Certificate									
									A Diterret

Gerar um certificado de dispositivo para o cliente

Agora que o certificado do dispositivo e o certificado da CA estão instalados na WLC, a próxima etapa é gerar esses certificados para o cliente.

Execute estas etapas para gerar o certificado do dispositivo para o cliente. Esse certificado será usado pelo cliente para autenticar na WLC. Este documento explica as etapas envolvidas na geração de certificados para o cliente profissional Windows XP.

 Vá para http://<endereço IP do servidor de autoridade de certificação>/certsrv do cliente que requer que o certificado seja instalado. Efetue login como nome de domínio\nome de usuário no servidor de CA. O nome de usuário deve ser o nome do usuário que está usando esta máquina com o XP e o usuário já deve estar configurado como parte do mesmo domínio que o servidor da autoridade de

certificação.		
Connect to 10.77.	244.198	
		1955
Connecting to 10.77.2	244.198	
User name:	🛃 wireless\user2	~
Password:		
	Remember my pass	word
	Connecting to 10.77.2 Connecting to 10.77.2 User name: Password:	Connect to 10.77.244.198 Connecting to 10.77.244.198 User name: Password: Remember my pass

2. Selecione Request a

certificate.

IN LOR VIEW PAVOLENS TOON HED	
S2ms2 4 Http://10.77.244.190/centsrv/	×
Microsoft Certificate Services wireless	Her
Nelcome	
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate for your Web, sign and encrypt messages, and, depending upon the ty beform other security tasks.	ficate, you can verify your pe of certificate you request,
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate view the status of a pending request.	revocation list (CRL), or to
For more information about Certificate Services, see Certificate Services Documentation.	

certificado.

Microsoft Certificate Services - Microsoft Internet Explorer	
Pée Edit Wew Favorities Tools Help	A
Address di http://10.77.244.198/certsrv/certraps.asp	🛁 🛃 Go
Managah Casilianta Casicaa - Madaaa	Element 🖉
Ancrosoff Certificate Services wireless	Home
Request a Certificate	
Select the certificate type:	
User Cadificate	
Or submit as advanced cartificate request	
Of Submit an <u>auxaliced certificate request.</u>	
http://10.77.244.199/centerv/centrgad.acp	Internet

4. Na página Solicitação avançada de certificado, clique em **Criar e enviar uma solicitação a esta CA**. Isso o levará para o formulário de solicitação de certificado

vançado.	
Microsoft Certificate Services - Microsoft Internet Explorer	
Edit View Pavorites Tools Help	1
2003 🕘 Mtp://10.77.244.190/cettary/cettogad.asp	💌 🔁 🛛
Nicrosoff Certificate Services wireless	Home
Advanced Certificate Request	
he policy of the CA determines the types of certificates you can request. Click one of the following options to:	
Create and submit a request to this CA.	
Submit a certificate request by using a base 64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-e PKCS #7 file	ncoded
Request a certificate for a smart card on behalf of another user by using the smart card certificate enrolment station. Note: You must have an enrollment agent certificate to submit a request on behalf of another user.	

5. No formulário de solicitação de certificado avançado, escolha Usuário no menu suspenso Modelo de certificado.Na seção Opções-chave, escolha estes parâmetros:Digite o tamanho da chave no campo Tamanho da chave. Este exemplo usa 1024.Marque a opção Mark Keys as Exportable.

Wiccosoft Certi	ficate Services - Microsoft Internet Explorer	
File Edit View	Pavorites Tools Help	
Address 🔕 http://10	.77.244.198/certsrv/certrgma.asp	a 🔁 👻
Microsoff Centre	ate Seveces wreless	Home
Advanced Ce	rtificate Request	1
Certificate Temp	date:	
	Basic EFS 💌	
K. Orden	Basic EFS	
Key Options:	Oxer	
000	Create new key set Use existing key set	
Key Usage:	Exchange	
Key Size	1024 Min: 294 (common key sizer \$12,1024,2040,4098,0102,16004.)	
ray orce.	Astematic key container name Ollar ynactified key container name	
	Mark keys as exportable	
	Export keys to file	
	Enable strong private key protection	
	Store certificate in the local computer certificate store Stores the certificate in the local computer store instead of in the user's certificate store. Does not install the root CA's certificate. You must be an administrator to generate or use a key in the local machinetone.	
	maconne ocore.	
Additional Optio	ns:	
Request Format:	© CMC O PKCS10	
Hash Algorithm.	SHA-1 V	
	City data to sign regulate.	
	La care request to a file	
Attributes:		
Ocea	let at a	Internet

6. Configure todos os outros campos necessários e clique em

Enviar.		
Microsoft Certi	Ificate Services - Microsoft Internet Explorer	E 6 🔀
File Edit View	Pavorites Tools Help	
G tak • 🕥	🗉 🖻 🐔 🔎 Search 🤺 Pavortes 🤣 🍙 🖓 🖼 🦓	
Address 🙋 http://10	0.77.244.198/certary/certrana.eep	💙 🔂 😡 .
	O Use existing key set O Use existing key set O	-
CSP:	Microsoft RSA SChannel Cryptographic Provider	
Key Usage:	Exchange	
Key Size:	1024 Min: 304 (common key sizes: 512 2028 2088 6392 10208) Marc 10204	
	Automatic key container name O User specified key container name	
	Mark keys as exportable	
	Export keys to file	
	Enable strong private key protection	
Additional Option	Store centrate in the scal computer centrate store Stores the centrificate in the local computer store instead of in the user's certificate store. Does not install the root CA's certificate. You must be an administrator to generate or use a key in the local machine store.	
Request Format:	© CMC	
Hash Algorithm:	SHA-1 V Only used to sign request.	
	Save request to a file	
Attributes:		
Friendly Name:		
	Submit >	
ei		🕥 Internet

 O certificado do dispositivo do cliente agora é gerado de acordo com a solicitação. Clique em Instalar o certificado para instalar o certificado no armazenamento de certificados.

Microsoft Certificate Services - Microsoft Internet Explorer	
File Edit View Favorites Tools Help	At
Address 🕘 http://10.77.244.190/certSrv/certfinsh.asp	🗹 🄁 ຜ
	<u>a</u>
Microsoff Certificate Services wireless	Home
Certificate Issued	
The certificate you requested was issued to you.	
Install this certificate	
a)	😰 Internet

 Você deve conseguir localizar o certificado do dispositivo do cliente instalado na Lista de certificados pessoais em Ferramentas > Opções da Internet > Conteúdo > Certificados no navegador IE do cliente

Silonto.				
Certificates				<u>?</u>
Intended purpose: </th <th>\ ></th> <th></th> <th></th> <th>~</th>	\ >			~
Personal Other People	Intermediate Certification	Authorities Trusted R	oot Certification	< >
Issued To	Issued By	Expiratio Frier	odly Name	<u> </u>
E 1234	wireless	1/25/2009 <nor< td=""><td>18></td><td></td></nor<>	18>	
Import Export	Remove		Advanc	ed
Certificate intended purp	oses			
Encrypting File System			View	
			Clos	e

O certificado do dispositivo para o cliente está instalado no cliente.

Gerar o Certificado de CA Raiz para o Cliente

A próxima etapa é gerar o certificado CA para o cliente. Conclua estas etapas a partir do PC cliente:

 Vá para http://<endereço IP do servidor de autoridade de certificação>/certsrv do cliente que requer que o certificado seja instalado. Efetue login como nome de domínio\nome de usuário no servidor de CA. O nome de usuário deve ser o nome do usuário que está usando esta máquina com o XP e o usuário já deve estar configurado como parte do mesmo domínio que o servidor da autoridade de certificação.

Connect to 10.	77.244.198	2 🔀
		1 mar
Connecting to 10.	77.244.198	
User name:	🖸 wireless\user2	~
Password:		
	Remember my password	
	ОК	Cancel

 Na página resultante, você pode ver os certificados CA atuais disponíveis no servidor CA na caixa CA certificate. Escolha Base 64 como o método de codificação. Em seguida, clique em Download CA certificate e salve o arquivo no PC do cliente como um arquivo .cer. Este exemplo usa rootca.cer como o nome do

arquivo.	
Microsoft Certificate Services - Microsoft Internet Explorer	
File Edit View Paviorities Tools Help	
Address White//10.77.244.198/certsrv/certcarc.asp	🛩 🔁 😡
Microsoft Conference Services - Inferiors	Heme
Download a CA Certificate, Certificate Chain, or CRL	
To trust certificates issued from this certification authority, instal this CA certificate chain.	
To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.	
CA certificate:	
Encoding method: O DER O Base 64 Download CA certificate Download CA certificate chain Download latest base CRL Download latest delta CRL	
	Internet

3. Em seguida, instale o certificado CA salvo no formato .cer no armazenamento de certificados do cliente. Clique duas vezes no arquivo rootca.cer e clique em **Instalar certificado**.

General Details Certification Path
Certificate Information
All issuance policies All application policies
Issued to: wireless
Issued by: wireless
Valid from 1/23/2008 to 1/23/2013
Install Certificate Issuer Statement

 Clique em Avançar para importar o certificado do disco rígido do cliente para o armazenamento de certificados

Certificate Import Wizard		
	Welcome to the Certificate Import Wizard This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store. A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept. To continue, click Next. < Back	

5. Selecione Automatically select the certificate store based on the type of certificate e clique em

Next.

tificate Store Certificate stores are s	ystem areas where certificates are kept.
Windows can automatio	cally select a certificate store, or you can specify a location f
 Automatically set 	ect the certificate store based on the type of certificate
O Place all certifica	tes in the following store
Certificate store	:
	Browse

6. Clique em Finish para finalizar o processo de

Completing the C Wizard You have successfully complexizard. You have specified the follow Certificate Store Selected Content	Certificate Import eted the Certificate Import wing settings: Automatically determined by t Certificate
< Back	Finish Cancel
	Completing the C Wizard You have successfully complexized. You have specified the follow Certificate Store Selected Content

7. Por padrão, os certificados da CA são instalados na lista Autoridades de certificação raiz confiáveis no navegador IE do cliente em Ferramentas > Opções da Internet > Conteúdo > Certificados. Aqui está o exemplo:

tificates				?
tended purpose: <a>All>	•			
Intermediate Certification A	uthorities Trusted Root C	ertification Aut	horities Trusted Put	× 1
Issued To	Issued By	Expiratio	Friendly Name	-
VeriSign Trust Netw	VeriSign Trust Network	5/19/2018	VeriSign Class 3	
VeriSign Trust Netw	VeriSign Trust Network	8/2/2028	VeriSign Class 3	
VeriSign Trust Netw	VeriSign Trust Network	5/19/2018	VeriSign Class 4	
VeriSign Trust Netw	VeriSign Trust Network	8/2/2028	VeriSign Class 1	
VeriSign Trust Netw	VeriSign Trust Network	8/2/2028	VeriSign Class 4	
VeriSign Trust Netw	VeriSign Trust-Network	5/19/2018	VeriSign Class 1	
is wireless	wireless	1/23/2013	<none></none>	
Wireless-CA	Wireless-CA	12/18/2012	<none></none>	
Xcert EZ by DST	Xcert EZ by DST	7/11/2009	Xcert EZ by DST	~
Import Export	Remove		Advan	ced
<all></all>			View	
				se

Todos os certificados necessários estão instalados na WLC, bem como no cliente para autenticação EAP-FAST Local EAP. A próxima etapa é configurar a WLC para a autenticação EAP local.

Configurar o EAP local no WLC

Conclua estes passos a partir do **modo GUI da WLC** para configurar a autenticação EAP Local na WLC:

1. Clique em **Security > Local**

Ref Edit Year Provides Toda Sage Centifiguration End Legout Before CISCO MONITOR WLANS CONTROLLER VIRELESS SECURITY MANAGEMENT COMMANDS HELP Security RADIUS Authentication Servers Apply New * AAA General Call Station ID Type IP Address V * RADIUS Authentication Accounting (Designed for FIPS outcomers and requires a key wrap compliant RADIUS server) New Access Control Lists Network User Nanagement Server Index Server Address Port IPSec Admin Status > Local EAP > Local EAP Norters Protection Network User > Moreless Protections Norters Protection Norters Protection Norters Protection > Worb Auth Advanced Advanced Norters Protection Norters Protection	AC . wic2006 - Microsoft Inter	rnet Explorer
Security Concernation Conservation Conservation <th>Pile Edit View Privorkes 1 </th> <th>Toob Help Sage Configuration Ping Lagout Be MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP</th>	Pile Edit View Privorkes 1 	Toob Help Sage Configuration Ping Lagout Be MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
> Web Auth > Advanced	Security * AAA General * RADIUS Authentication Accounting * TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies * Delicies * Local EAP * Priority Order * Access Control Lists * Wireless Protection Policies	RADIUS Authentication Servers Apply New Call Station 1D Type IP Address Image: Call Station 1D Type Image: Call S
	Web Auth Advanced	

2. Em Local EAP, clique em **Profiles** para configurar o perfil Local EAP.



- 3. Clique em New para criar um novo perfil EAP local.
- 4. Configure um nome para este perfil e clique em **Apply**. Neste exemplo, o nome do perfil é **Idap**. Isso o leva aos perfis de EAP locais criados na

WLC.									
wic2006 - Microsoft Inter	net Explorer								C 🖬 🗙
File Edit View Pavorites T	ools Help								
ahaha								nfiguration <u>P</u> ir	ng Logout Befresh
CISCO	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
Security	Local EA	P Profile	s > New					< Back	Apply
 AAA General RADIUS Authentication Accounting TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Cocal EAP General PAP-FAST Parameters Authentication Priority 	Profile No	me		Idap					
▶ Priority Order									
▶ Access Control Lists									
Wireless Protection Policies									
▶ Web Auth									
▶ Advanced									
() Done								A 4	Internet
	_								

 Clique no perfil Idap que acabou de ser criado, exibido no campo Nome do perfil da página Perfis EAP locais. Isso o levará para a página Perfis EAP Locais > Editar.

🗿 wic2006 - Microsoft Inter	net Explorer								
File Edit View Pavorites	Tools Help	_							
ahaha								nfiguration <u>P</u> ing	Logout Refresh
CISCO	MONITOR	<u>W</u> LAN5	CONTROLLER	W]RELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	
Security	Local EA	P Profile:	9		_			New	Apply
- AAA	Profile Na	me		LEAP I	CAP-PAST	EAP-TLS	PEAP		
General RADBUS Authentication Accounting TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies	Idao				3				
 Local EAP General Profiles EAP-FAST Parameters Authentication Priority 									
▶ Priority Order									
▶ Access Control Lists									
Wireless Protection Policies									
▶ Web Auth									
Advanced									

6. Configure os parâmetros específicos deste perfil na página Perfis EAP Locais > Editar.Escolha EAP-FAST como o método de autenticação EAP local.Ative as caixas de seleção ao lado de Local Certificate Required e Client Certificate Required.Escolha Fornecedor como Emissor do Certificado porque este documento usa um servidor de CA de terceiros.Habilite a caixa de seleção ao lado de Verificar em relação aos certificados da autoridade de certificação para permitir que o certificação no controlador.Se você quiser que o nome comum (CN) no certificado de entrada seja validado em relação ao CN dos certificados de CA no controlador, marque a caixa de seleção Verificar a identidade do CN do certificado. A configuração padrão está desabilitada. Para permitir que o controlador verifique se o certificado do dispositivo de entrada ainda é válido e não expirou, marque a caixa de seleção Verificar validade da data do certificado.Observação: a validade da data do certificado é verificada em relação à hora UTC (GMT) atual configurada no controlador. O deslocamento de fuso horário é ignorado.Clique em Apply.



7. O perfil EAP Local com autenticação EAP-FAST agora é criado no

Wic2006 - Microsoft Intern	et Explorer							
File Edit View Fevorites To	ols Help							
ahaha						Saye Co	miguration ping	Logout Befresh
CISCO	MONITOR WEARS	CONTROLLER	WIRELESS	SECORTA	MANAGEMENT	COMMANDS	HEDP	
Security	Local EAP Profile:	0					New	Apply
- AAA	Profile Name		LEAP EA	P-PAST	EAP-TLS	PEAP		
- RADIUS	Ideo							
Authentication Accounting								
TACACS+ LDAP								
Local Net Users NAC Filtering								
Disabled Clients								
AP Policies								
T Local EAP								
Profiles EAR-EAST Parameters								
Authentication Priority								
▶ Priority Order								
Access Control Lists								
Policies								
▶ Web Auth								
Advanced								
Cone Cone							🙆 🥥 In	ternet

8. A próxima etapa é configurar parâmetros específicos de EAP-FAST no WLC. Na página Segurança da WLC, clique em EAP Local > Parâmetros EAP-FAST para ir para a página Parâmetros do método EAP-FAST.Desmarque a caixa de seleção Provisão anônima porque este exemplo explica EAP-FAST usando certificados. Deixe todos os outros parâmetros em seus padrões. Clique em Apply.

Wic2006 - Microsoft Intern File Edit View Pavorites Ti	net Explorer sols Help			
uluilu cisco	MONITOR WLANS CONTROLLER WIRELESS	SECURITY MANAGEMENT	Saye Confi COMMANDS	guration <u>P</u> ing Logout <u>B</u> efre HELP
Security	EAP-FAST Method Parameters	\bigcirc		Apply
T AAA General	Server Key (in hex)	••••		
RADIUS Authentication	Confirm Server Key	••••		
IN TACACS+	Time to live for the PAC	10 days		
Local Net Users MAC Filtering Disabled Clients	Authority ID (in hex)	436973636f		
User Login Policies AP Policies	Authority ID Information	Citco A-ID		
Local EAP General Profiles EAP-FAST Parameters Distantication Priority	Anonymous Provision	Enabled		
Priority Order				
Access Control Lists Wireless Protection Policies				
6 Web Auth				
E Advanced				
				🎒 🚭 Internet

Configurar a WLC com detalhes do servidor LDAP

Agora que a WLC está configurada com o perfil EAP local e informações relacionadas, a próxima etapa é configurar a WLC com detalhes do servidor LDAP. Conclua estes passos no WLC:

 Na página Security do WLC, selecione AAA > LDAP no painel de tarefas do lado esquerdo para ir para a página de configuração do servidor LDAP. Para adicionar um servidor LDAP, clique em Novo. A página LDAP Servers (Servidores LDAP) > New (Novo) é exibida.



2. Na página LDAP Servers Edit (Editar servidores LDAP), especifique os detalhes do servidor LDAP, como o endereço IP do servidor LDAP, o número da porta, o status Enable Server (Habilitar servidor) e assim por diante. Selecione um número na caixa suspensa Índice do servidor (prioridade) para especificar a ordem de prioridade deste servidor em relação a qualquer outro servidor LDAP configurado. É possível configurar até dezessete servidores. Se o controlador não puder acessar o primeiro servidor, ele tentará o segundo da lista e assim por diante. Digite o endereço IP do servidor LDAP no campo Endereço IP do servidor.Insira o número da porta TCP do servidor LDAP no campo Port Number. O intervalo válido é de 1 a 65535, e o valor padrão é 389.No campo User Base DN (Nome diferenciado da base de usuários), digite o nome diferenciado (DN) da subárvore do servidor LDAP que contém uma lista de todos os usuários. Por exemplo, ou=organizational unit, .ou=next organizational unit e o=corporation.com. Se a árvore contendo usuários for o DN base, digite o=corporation.com ou dc=corporation, dc=com.Neste exemplo, o usuário está localizado sob o Idapuser da Unidade Organizacional (OU) que, por sua vez, é criado como parte do domínio Wireless.com.O DN de base do usuário deve apontar o caminho completo onde as informações do usuário (credencial do usuário de acordo com o método de autenticação EAP-FAST) estão localizadas. Neste exemplo, o usuário está localizado sob o DN base OU=Idapuser, DC=Wireless, DC=com.Mais detalhes sobre OU, bem como a configuração do usuário, são explicados na seção Criação de Usuários no Controlador de Domínio deste documento.No campo User Attribute (Atributo de usuário), digite o nome do atributo no registro do usuário que contém o nome de usuário.No campo User Object Type (Tipo de objeto de usuário), insira o valor do atributo objectType do LDAP que identifica o registro como um usuário. Frequentemente, os registros de usuário têm diversos valores para o atributo objectType, sendo que alguns são exclusivos e outros são compartilhados com diversos tipos de objeto. Observação: Você pode obter o valor desses dois campos no servidor de diretório com o utilitário do navegador LDAP, que faz parte das ferramentas de

suporte do Windows 2003. Essa ferramenta do navegador LDAP da Microsoft denomina-se LDP. Com a ajuda dessa ferramenta, você pode conhecer os campos DN base do usuário, Atributo do usuário e Tipo de objeto do usuário desse usuário específico. Informações detalhadas sobre o uso do LDP para conhecer esses atributos específicos do Usuário são discutidas na seção <u>Uso do LDP para Identificar os Atributos do Usuário</u> deste documento.Escolha Secure na caixa suspensa Server Mode se quiser que todas as transações LDAP usem um túnel TLS seguro. Caso contrário, escolha Nenhum, que é a configuração padrão.No campo Limite de tempo do servidor, digite o número de segundos entre as retransmissões. O intervalo válido é de 2 a 30 segundos, e o valor padrão é de 2 segundos.Marque a caixa de seleção Habilitar status do servidor para habilitar este servidor LDAP ou desmarque-a para desabilitar. O valor padrão é desativado.Clique em Apply (Aplicar) para confirmar as alterações.Aqui está um exemplo já configurado com estas informações:

Mic2006 - Microsoft Internet Explorer	
He Edit View Pavorites Tools Help	
allalla Sage Con	figuration Eing Logout Refresh
CISCO MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS	неця
Security LDAP Servers > Edit Conoral General PADDUS Server Index Authenication Accounting DACCOP Deal Net Users Local Net Users Machenication Accounting User Base DN Diser Login Policies AP Policies AP Policies Server Mode Policies None Policies Server Timeout Policies Server Status Wireless Protection Server Status Web Auth Advanced	< Back Apply
0 Done	📋 🥥 Internet

Agora que os detalhes sobre o servidor LDAP estão configurados no WLC, a próxima etapa é configurar o LDAP como o banco de dados de back-end prioritário para que o WLC primeiro procure o banco de dados LDAP para as credenciais do usuário em vez de qualquer outro banco de dados.

Configurar LDAP como o banco de dados back-end de prioridade

Conclua estes passos no WLC para configurar o LDAP como o banco de dados de back-end de prioridade:

 Na página Segurança, clique em EAP Local > Prioridade de Autenticação. Na página Ordem de prioridade > Autenticação local, você pode encontrar dois bancos de dados (Local e LDAP) que podem armazenar as credenciais do usuário.Para tornar o LDAP o banco de dados de prioridade, escolha **LDAP** na caixa de credenciais do usuário do lado esquerdo e clique no botão > para mover o LDAP para a caixa de ordem de prioridade no lado

direito.

🕲 wic2006 - Microsoft Intern	set Explorer									🗙
File Edit View Pavorites To	ools Help									<i></i>
սիսիս								nfiguration	Eing Logeut	<u>R</u> efresh
cisco	MONITOR	<u>WLAN5</u>	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP		
Security	Priority 0	rder > Lo	ocal-Auth		\bigcirc				Appl	Y .
 AAA General General RADIUS Autheotication Accounting TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Local EAP General Profile Di-FAST Parameters Autheotication Priority Priority Ordez Access Control Lists Wireless Protection Policies Web Auth Advanced 	LOCAL LOCAL LDAP			p Mn					App	×
1									🔮 Internet	

 Este exemplo ilustra claramente que o LDAP é escolhido na caixa do lado esquerdo e o botão > é selecionado. Como resultado, o LDAP é movido para a caixa no lado direito que decide a prioridade. O banco de dados LDAP é escolhido como o banco de dados Authentication-priority.Clique em



Observação: Se LDAP e LOCAL aparecerem na caixa Credenciais do Usuário à direita com

LDAP na parte superior e LOCAL na parte inferior, o EAP Local tentará autenticar clientes usando o banco de dados back-end LDAP e efetuará failover para o banco de dados do usuário local se os servidores LDAP não estiverem acessíveis. Se o usuário não for encontrado, a tentativa de autenticação será rejeitada. Se LOCAL estiver na parte superior, o EAP local tentará se autenticar usando somente o banco de dados de usuário local. Não ocorre failover para o banco de dados back-end LDAP.

Configurar a WLAN na WLC com autenticação EAP local

A última etapa na WLC é configurar uma WLAN que usa EAP local como seu método de autenticação com LDAP como seu banco de dados de back-end. Execute estas etapas:

- No menu principal da controladora, clique em WLANs para ir para a página de configuração de WLANs. Na página WLANs, clique em New para criar uma nova WLAN. Este exemplo cria um novo Idap de WLAN.Clique em Apply A próxima etapa é configurar os parâmetros da WLAN na página WLANs > Edit.
- 2. Na página de edição da WLAN, habilite o status desta WLAN. Configure todos os outros parâmetros



- 3. Clique em Security para configurar os parâmetros relacionados à segurança para esta WLAN. Este exemplo usa a segurança de Camada 2 como 802.1x com WEP dinâmico de 104 bits.Observação: este documento usa 802.1x com WEP dinâmico como exemplo. É recomendável usar métodos de autenticação mais seguros, como WPA/ WPA2.
- 4. Na página de configuração WLAN Security, clique na guia AAA servers. Na página de servidores AAA, ative o método Local EAP Authentication e escolha Idap na caixa suspensa que corresponde ao parâmetro EAP Profile Name. Este é o perfil EAP Local criado neste exemplo.

5. Escolha o servidor LDAP (que foi configurado anteriormente na WLC) na caixa suspensa . Certifique-se de que o servidor LDAP seja alcançável a partir do WLC.Clique em Apply.

wic2006 - Microsoft In	Internet Explorer	X
File Edit View Favorites	es Tools Help	
cisco	Sage Configuration Bing L MONITOR <u>W</u> LANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP	ogout I <u>R</u> efresh
WLANS WLANS MLANS Advonced	Super Security QS Advanced Layer 2 Layer 3 Add Servers Security QS Add Servers Security Layer 3 Add Servers Security Caser 4 Server 1 Server 3 Server 1 None Server 4 Server 7 Server 7 Server 2 None Server 7 Server 7 Server 7 Local EAP Authentication Case 6 Server 7 Server 7 Server 7 Server 7 Local EAP Authentication Case 6 Server 7 Server 7	Apply
81 	🚔 🥥 Interr	et

6. O novo Idapde WLAN foi configurado no WLC. Esta WLAN autentica clientes com Autenticação EAP Local (EAP-FAST neste caso) e consulta um banco de dados back-end

LDAP para validação de credenciais de

cliente.

wic2006 - Microsoft Inter	net Explorer						
File Edit View Flavorites T	tools Help				Sa	ve Configuration Pina Lo	cout Refres
CISCO	MONITOR WLANS	CONTROLLER WIR	ELESS SECURITY	MANAGEMENT	COMMA	NDS HELP	
WLANs	WLANs					N	0.w
WLANS WLANS	Profile Name	Туре	WLAN SSID	Ad	imin atus	Security Policies	
Advanced	Tawee	WEAN	TSWED	En	sbled	[WPA2][Auth(002.1X)]	
	Idepuser	WLAN	ldep	En	abled	002.1X	
Done						🛆 🔮 Interne	t

Configurar servidor LDAP

Agora que o EAP local está configurado na WLC, a próxima etapa é configurar o servidor LDAP, que serve como um banco de dados de back-end para autenticar os clientes sem fio após a validação bem-sucedida do certificado.

A primeira etapa na configuração do servidor LDAP é criar um banco de dados de usuário no servidor LDAP para que o WLC possa consultar esse banco de dados para autenticar o usuário.

Criando usuários no controlador de domínio

Neste exemplo, um novo **Idapuser** da OU é criado e o usuário **user2** é criado nessa OU. Ao configurar esse usuário para acesso LDAP, a WLC pode consultar esse banco de dados LDAP para autenticação de usuário.

O domínio usado neste exemplo é wireless.com.

Criar um banco de dados de usuário em uma UO

Esta seção explica como criar uma nova UO no domínio e criar um novo usuário nessa UO.

- No controlador de domínio, clique em Iniciar > Programas > Ferramentas Administrativas > Usuários e Computadores do Ative Diretory para iniciar o console de gerenciamento Usuários e Computadores do Ative Diretory.
- Clique com o botão direito do mouse no nome de domínio (wireless.com, neste exemplo) e selecione New > Organizational Unit no menu de contexto para criar uma nova

OU.

dctive Directory Users and Computers			
G Ele Action View Window Help			_8×
	n 🔊 🖉 🖓		
Active Directory Users and Compt Wireless.com Wireless.com	12 objects		
D-00 Wreless.com	Туре	Description	
Builtin Dglegate Control	builtinDomain		
E-Comput Find	Container	Default container for upgr	
Domain Connect to Domain	. Organizational	Default container for dom	
⊡ Foreign: <u>Connect to Domain Controller</u>	. Container	Default container for secu	
LostAnc Raise Domain Functional Level	lostAndFound	Default container for orph	
⊡ NTD5 Q Operations Masters	msDS-QuotaCo	Quota specifications cont	
Program	Container	Default location for storag	
All Tasks	Contact	Itin system settings	
	Group		
C Ada	InetOrdPerson	rault container for upgr	
New Window from Here	MSMO Queue Alias		
+ C2 CER Refresh	Organizational Unit		
OHK Export List	Printer		
I DHK	User		
Dns Properties	Shared Folder		
🕀 🕵 Dns 🛛 Help			
Don.	1		
Domain Computers			
Domain Controllers			
Domain Guescs			
Enterprise Admins			

3. Atribua um nome a esta OU e clique em

OK.	w Object ·	Organizal	tional Unit			X
	Ø	Create in:	Wireless.com/			
	N <u>a</u> me:					_
	Idapuser					
-						_
				OK	Cancel	

Agora que o novo usuário **Idapuser** da OU é criado no servidor LDAP, a próxima etapa é criar o usuário **user2** nessa OU. Para isso, siga estas etapas:

 Clique com o botão direito do mouse na nova OU criada. Selecione New > User nos menus de contexto resultantes para criar um novo



2. Na página Configuração do usuário, preencha os campos obrigatórios conforme mostrado neste exemplo. Este exemplo tem user2 como o nome de logon do usuário.Este é o nome de usuário que será verificado no banco de dados LDAP para autenticação do cliente. Este exemplo usa abcd como o nome e o sobrenome. Clique em Next.

New Object - User	×
Create in: Wireless.com/Idapuser	
Eirst name: abcd Initials:	
Last name:	
Full ngme: abcd	
User logon name:	
user2 @Wireless.com	
User logon riame (pre- <u>W</u> indows 2000):	
WIRELESS\ user2	
< Back Next > Cancel	

3. Digite uma senha e confirme-a. Selecione a opção **A senha nunca expira e clique em Avancar**.

ew Object - User	
Create in:	Wireless.com/Idapuser
Password:	
<u>C</u> onfirm password:	•••••
🔲 User <u>m</u> ust change p	assword at next logon
🔲 U <u>s</u> er cannot change	e password
Password never exp	pires
Account is disabled	
	< <u>B</u> ack <u>N</u> ext > Cancel

 Clique em Finish.Um novo usuário user2 é criado sob o OU Idapuser. As credenciais do usuário são:nome de usuário: user2senha: Laptop123



Agora que o usuário em uma OU é criado, a próxima etapa é configurar esse usuário para acesso LDAP.

Configurar o usuário para acesso ao LDAP

Execute as etapas nesta seção para configurar um usuário para acesso LDAP.

Habilitar Recurso de Associação Anônima no Windows 2003 Server

Para que aplicativos de terceiros acessem o Windows 2003 AD no LDAP, o recurso de Associação Anônima deve ser habilitado no Windows 2003. Por padrão, operações anônimas LDAP não são permitidas nos controladores de domínio do Windows 2003.

Execute estas etapas para habilitar o recurso de Associação Anônima:

- 1. Inicie a ferramenta **ADSI Edit** no local Start > Run > Type: **ADSI Edit.msc**. Esta ferramenta faz parte das ferramentas de suporte do Windows 2003.
- Na janela ADSI Edit, expanda o domínio Raiz (Configuração [tsweblapt.Wireless.com]).Expanda CN=Services > CN=Windows NT > CN=Diretory Service. Clique com o botão direito do mouse no contêiner CN=Diretory Service e selecione properties no menu de contexto.



3. Na janela CN=Diretory Service Properties, clique no atributo dsHeuristics no campo Attribute e escolha Edit. Na janela Editor de atributos de string deste atributo, digite o valor 0000002 e clique em Aplicar e OK. O recurso Associação Anônima está habilitado no servidor Windows 2003.Observação: o último (sétimo) caractere é aquele que controla a maneira como você pode se vincular ao serviço LDAP. "0" ou nenhum sétimo caractere significa que as operações LDAP anônimas estão desativadas. A definição do sétimo caractere como "2" habilita o recurso de Associação Anônima.

EN=Directory Service Pr	operties		? X		
Attribute Editor Security	1			Class	Distingu
Show mandatory attri	ibutes			container	CN=Qu
Show optional attribu	tes				
Show only attributes	that have <u>v</u> alues				
Attributes:					
Attribute	Syntax	Value	▲		
directReports	String Attribu	ite Editor			×
displayNamePrintable	Attribute: dSH	leuristics			
distinguishedName	Value				
dSCorePropagationD					
dSHeuristics	Junior		6		
flags	Clear		(ок	Cancel
fromEntry					
frsComputerReferenc	Distinguished	<not set=""></not>			
fSM0RoleOwner	Distinguished	<not set=""></not>	<u> </u>		
Edit					
	OK	Cancel	Apply		

Observação: Se este atributo já contiver um valor, certifique-se de alterar somente o sétimo caractere da esquerda. Este é o único caractere que precisa ser alterado para habilitar associações anônimas. Por exemplo, se o valor atual for "0010000", você precisará alterá-lo para "0010002". Se o valor atual for menor que sete caracteres, você precisará colocar zeros nos locais não usados: "001" se tornará "0010002".

Concedendo Acesso a LOGON ANÔNIMO ao Usuário "user2"

A próxima etapa é conceder **LOGON ANÔNIMO** ao usuário **user2**. Siga estas etapas para realizar essa ação:

- 1. Abra Usuários e computadores do Active Directory.
- 2. Verifique se View Advanced Features está marcado.
- Navegue até o usuário user2 e clique com o botão direito do mouse nele. Selecione Properties no menu de contexto. Esse usuário é identificado com o nome "abcd".

哇 🗠 🌄 useri		
🖃 🛄 Users		
	⊆opy Add to a group Name Mappings Di <u>s</u> able Account	
	<u>Neset Password</u> Mo <u>v</u> e Open Home Page	
	Find	
	All Tasks	-
	Vjew New <u>W</u> indow from Here	•
	Cu <u>t</u> Delete	
E Kr	Rena <u>m</u> e Refresh	
R/	Export List	
💽 us 🗖	Properties	
i 🕵 alas	Help	
(

4. Vá para Segurança na janela Propriedades

Published Certificates	L Member Of L Dia		-
nvironment Session	Bemote control Ter	minal Services Profile	CO
General Address	Account Profile	Telephones Organ	izati
-			
abcd			
<u>F</u> irst name:	abed	Initials:	
Last name:			
Display name:	abcd		
Digplay Hame.	1		
Description:	1		
Offi <u>c</u> e:			
<u>T</u> elephone number:		<u>O</u> ther	
E-mail:			
hideb energy		Other	
web page:		Other	
		course II to	

- 5. Clique em Adicionar na janela resultante.
- 6. Insira ANONYMOUS LOGON na caixa Enter the object names to select e confirme a caixa de

diálogo.

<u>? ×</u>
Object Types
Locations
Check Names
K Cancel

7. Na ACL, você observará que o **LOGON ANÔNIMO** tem acesso a alguns conjuntos de propriedades do usuário. Click **OK**. O acesso ao LOGON ANÔNIMO é concedido a este usuário.

abcd Properties	<u>? ×</u>
Environment Sessions Remote control Terminal Service General Address Account Profile Telephones Published Certificates Member Of Dial-in Object	s Profile COM+ Organization ct Security
<u>G</u> roup or user names:	
Account Operators (WIRELESS Account Operators)	<u> </u>
ANONYMOUS LOGON	
Cert Publishers (WIRELESS\Cert Publishers)	-
Add Permissions for ANONYMOUS LOGON Allow	<u>Remove</u> Deny
Full Control Image: Control Read Read Image: Control Read Write Image: Control Read Create All Child Objects Image: Control Read Delete All Child Objects Image: Control Read Allowed to Authenticate Image: Control Read	
For special permissions or for advanced settings, click Advanced.	Advanced
OK Cancel	

Concedendo Permissão de Conteúdo da Lista na OU

A próxima etapa é conceder pelo menos a permissão **Listar Conteúdo** ao **LOGON ANÔNIMO** na OU em que o usuário está localizado. Neste exemplo, "user2" está localizado na OU "Idapuser". Siga estas etapas para realizar essa ação:

1. Em Usuários e Computadores do Ative Diretory, clique com o botão direito do mouse em OU

Idapuser e escolha Propriedades.

	Administrator Cert Publishers CERTSVC_DCOM_ACCES DHCP Administrators DHC	
	Dnsv Mo <u>v</u> e Dnsl Find Dom	_
	Dom <u>N</u> ew Dom All Tas <u>k</u> s Dom	*
	Dom <u>View</u> Ente New <u>W</u> indow from Here Grou	-
÷	Gue: <u>D</u> elete IIS_ <u>D</u> elete IUSF Rena <u>m</u> e Refresh	
	RAS Properties	_
	Sche user <u>H</u> elp	
	abcd	

2. Clique em **Segurança** e em **Avançado**.

apuser Properties			? ×
General Managed By Object Security CC	JM+ Group F	Policy	
Group or user names:			
Account Operators (WIRELESS \Account	t Operators)	1	-
Administrators (WIRELESS Administrator	s)		
🛃 Authenticated Users			
🛛 🖅 Domain Admins (WIRELESS\Domain Ad	lmins)		
Enterprise Admins (WIRELESS\Enterpris	e Admins)		-1
	^		<u> </u>
	Add	<u>Remove</u>	
Permissions for Account Operators	Allow	Deny	_
Full Control			•
Read			
Write			
Create All Child Objects			
Delete All Child Objects			
Generate Resultant Set of Policy(Logging)			-
For special permissions or for advanced setting click Advanced.	as.	Advanced	\geq
	I	1	

3. Clique em Add. Na caixa de diálogo que é aberta, insira LOGON ANÔNIMO.

Advanced Security Settings for Idapuser	
Select User, Computer, or Group	<u>? ×</u>
Select this object type:	
User, Group, or Built-in security principal	Object Types
From this location:	
Wireless.com	Locations
Enter the object name to select (examples):	
ANONYMOUS LOGON	<u>C</u> heck Names
Advanced OK	Cancel

- 4. Reconheça o diálogo. Isso abre uma nova janela de diálogo.
- 5. Na caixa suspensa **Aplicar em**, escolha **Somente este objeto** e ative a caixa de seleção **Listar**

Conteúdo.

Permission Entry for Idapuser			? ×
Object Properties			
Name: ANONYMOUS LOGON		<u>C</u> hange	
Apply onto: This object only		1	-
Permissions:	Allow	Deny	
Full Control List Contents Read All Properties Write All Properties Delete Delete Subtree Read Permissions Modify Permissions Modify Owner All Validated Writes All Extended Rights Create All Child Objects Delete All Child Objects Delete All Child Objects			
	οκ	Cane	el

Usando o LDP para identificar os atributos do usuário

Essa ferramenta de GUI é um cliente LDAP que permite que os usuários executem operações (como conectar, vincular, pesquisar, modificar, adicionar, excluir) em qualquer diretório compatível com LDAP, como o Ative Diretory. O LDP é usado para visualizar objetos armazenados no Ative Diretory junto com seus metadados, como descritores de segurança e metadados de replicação.

A ferramenta GUI do LDP é incluída quando você instala as Ferramentas de suporte do Windows Server 2003 a partir do CD do produto. Esta seção explica o uso do utilitário LDP para identificar os atributos específicos associados ao usuário **user2**. Alguns desses atributos são usados para preencher os parâmetros de configuração do servidor LDAP no WLC, como tipo de atributo de usuário e tipo de objeto de usuário.

- 1. No servidor Windows 2003 (mesmo no mesmo servidor LDAP), clique em **Start > Run** e insira **LDP** para acessar o navegador LDP.
- Na janela principal do LDP, clique em Connection > Connect e conecte-se ao servidor LDAP inserindo o endereço IP do servidor LDAP.

Here Loop	. O ×
Connection Browse View Options Utilities	Help
Connect Bind Optionnect	*
Save As	
Print Pregiew Print Sebup	
Egt	
	×
CONNECT OD SPECIFIED SERVER	

3. Depois de conectado ao servidor LDAP, selecione **View** no menu principal e clique em **Tree**.

ldap://tsweb-lapt.Wireless.com/EC=Wireless,DC=com	
onnection Browse Yew Options Utilities	B
Tree Ctrl+T Enterprise Configuration ✓ Status Bar Set Font	<pre>1.2.840.113556.1.4.473; 1.2.840.113556.1.4.528; 1.2.840.113556.1.4.417; 1.2.840.113556.1.4.619; 1.2.840.113556.1.4.841; 1.2.840.113556.1.4.529; 1.2.840.113556.1.4.805; 1.2.840.113556.1.4.521; 1.2.840.113556.1.4.970; 1.2.840.113556.1.4.1338; 1.2.840.113556.1.4.474; 1.2.840.113556.1.4.1339; 1.2.840.113556.1.4.1340; 1.2.840.113556.1.4.1413; 2.16.840.1.113730.3.4.9; 2.16.840.1.113730.3.4.10; 1.2.840.113556.1.4.1504; 1.2.840.113556.1.4.1952; 1.2.840.113556.1.4.802; 1.2.840.113556.1.4.1907; 1.2.840.113556.1.4.1952; 1.2.840.113556.1.4.802; 1.2.840.113556.1.4.1907; 1.2.840.113556.1.4.1948; 2.> supportedLDAPVersion: 3; 2: 12.> supportedLDAPVersion: 3; 2: 13.> highestCommittedUSN: 16926; 4.> supportedSASLMechanisms: GSSAPI; GSS-SPNEGO; EXTERNAL; DIGEST-MD5; 1.> dnsHostName: tsweb-lapt.Wireless.com; 1.> ldapServiceName: Wireless.com; 1.> ldapServiceName: Wireless.com; 3.> supportedCapabilities: 1.2.840.113556.1.4.800; 1.2.840.113556.1.4.1670; 1.2.840.113556.1.4.1791; 1.> isGlobalCatalogReady: TRUE; 1.> isGlobalCatalogReady: TRUE; 1.> isGlobalCatalogReady: TRUE; 1.> domainFunctionality: 0 = [DS_BEHAVIOR_WIN2000]; 1.> domainControllerFunctionality: 2 = [DS_BEHAVIOR_WIN2003];</pre>

4. Na janela resultante Visualização em árvore, insira o BaseDN do usuário. Neste exemplo, user2 está localizado na OU "Idapuser" no domínio Wireless.com. Portanto, o BaseDN para o usuário user2 é OU=Idapuser, dc=wireless, dc=com. Click OK.

5. O lado esquerdo do navegador LDP exibe a árvore inteira que aparece sob o BaseDN especificado (OU=Idapuser, dc=wireless, dc=com). Expanda a árvore para localizar o usuário user2. Esse usuário pode ser identificado com o valor de CN que representa o nome do usuário. Neste exemplo, é CN=abcd. Clique duas vezes em CN=abcd. No painel do lado direito do navegador LDP, o LDP exibirá todos os atributos associados ao usuário2. Este exemplo explica esta etapa:



Neste exemplo, observe os campos circulados à direita.

- 6. Conforme mencionado na seção <u>Configurar WLC com Detalhes do Servidor LDAP</u> deste documento, no campo Atributo do Usuário, insira o nome do atributo no registro do usuário que contém o nome do usuário.Nessa saída do LDP, você pode ver que sAMAccountName é um atributo que contém o nome de usuário "user2". Portanto, insira o atributo sAMAccountName que corresponde ao campo User Attribute no WLC.
- 7. No campo User Object Type (Tipo de objeto de usuário), insira o valor do atributo objectType do LDAP que identifica o registro como um usuário. Frequentemente, os registros de usuário têm diversos valores para o atributo objectType, sendo que alguns são exclusivos e outros são compartilhados com diversos tipos de objeto.Na saída LDP, CN=Person é um valor que identifica o registro como um usuário. Portanto, especifique Person como o atributo User Object Type no WLC.

Configurar cliente sem fio

A última etapa é configurar o cliente sem fio para autenticação EAP-FAST com certificados de cliente e servidor. Siga estas etapas para realizar essa ação:

 Inicie o Cisco Aironet Desktop Utility (ADU). Na janela principal do ADU, clique em Profile Management > New para criar um novo perfil de cliente sem fio.

🕾 Cisco Aironet Desktop UI	ility - Current Profile: sdreteretet	? 🛛
Action Options Help		
Current Status Profile Managem	Diagnostics	
Sdreteretet		New
		Modify
		Remove
		Activate
∠ Details		
Network Type:	Infrastructure	Import
Security Mode:	Disabled	
Network Name 1 (SSID1):	teert	Export
Network Name 2 (SSID2):	<empty></empty>	Scan
Network Name 3 (SSID3):	<empty></empty>	Scart
Auto Select Profiles		Order Profiles

2. Especifique um nome de perfil e atribua um nome SSID a esse perfil. Esse nome SSID deve ser o mesmo configurado na WLC. Neste exemplo, o nome SSID é

Client Name: CLIENT1 Network Names SSID1 Idap SSID2 SSID3	Client Name: CLIENT1	
Network Names SSID1 Map SSID2: SSID3:		
SSID2 SSID3:	Network Names	
SSID3:	SSID2	
	SSID3:	

- 3. Clique na guia **Security** e escolha **802.1x/EAP** como a segurança da camada 2. Escolha **EAP-FAST** como o método EAP e clique em **Configure**.
- 4. Na página de configuração EAP-FAST, escolha **Certificado de cliente TLS** na caixa suspensa Método de autenticação EAP-FAST e clique em **Configurar**.

Configure EAP-FAST	? 🔀
EAP-FAST Authentication Method	
MSCHAPv2 User Name and Password	Configure
GTC Token/Password	
TLS Client Certificate	
Select One or More PAC Authorities	
	Manage
Use Any PAC Belonging to the Same Group	
Allow Automatic PAC Provisioning	
Use Machine Information for Domain Logon	
No Network Connection Unless User Is Logged In	
	K Cancel

5. Na janela de configuração do certificado de Cliente TLS:Habilite a caixa de seleção Validar identidade do servidor e selecione o certificado CA instalado no cliente (explicado na seção Gerar o certificado CA raiz para o cliente deste documento) como a autoridade de certificação raiz confiável.Selecione o certificado de dispositivo instalado no cliente (explicado na seção Gerar um certificado de dispositivo para o cliente deste documento) como o certificado de cliente.Click OK.Este exemplo explica esta etana:

onfigure TLS Client Certificate	? D
Validate Server Identity	
Trusted Root Certification Authorities	
wireless	~
Select a Certificate	
1234 [Issued by: wireless 1/26/2008]	✓
Server/Domain Name	
Wireless.com	
Login Name	
user2	
	OK Cancel

O perfil do cliente sem fio é criado.

Verificar

Execute estas etapas para verificar se sua configuração funciona corretamente.

- 1. Ative o SSID Idap no ADU.
- 2. Clique em Sim ou em OK conforme necessário nas próximas janelas. Você deve ser capaz

de ver todas as etapas de autenticação de cliente, bem como a associação para ser bemsucedido no ADU.

Use esta seção para confirmar se a sua configuração funciona corretamente. Use o modo CLI da WLC.

 Para verificar se a WLC pode se comunicar com o servidor LDAP e localizar o usuário, especifique o comando debug aaa Idap enable da CLI da WLC. Este exemplo explica um processo LDAP de comunicação bem-sucedido:Observação: parte da saída nesta seção foi movida para as segundas linhas devido à consideração de espaço.(Cisco Controller) >debug aaa Idap enable

```
Sun Jan 27 09:23:46 2008: AuthenticationRequest: 0xba96514
Sun Jan 27 09:23:46 2008: Callback.....0x8
344900
Sun Jan 27 09:23:46 2008:
                           protocolType.....0x0
0100002
Sun Jan 27 09:23:46 2008: proxyState.....00:
40:96:AC:E6:57-00:00
Sun Jan 27 09:23:46 2008:
                         Packet contains 2 AVPs (not shown)
Sun Jan 27 09:23:46 2008: ldapTask [1] received msg 'REQUEST' (2) in state 'IDLE' (1)
Sun Jan 27 09:23:46 2008: LDAP server 1 changed state to INIT
Sun Jan 27 09:23:46 2008: ldapInitAndBind [1] called lcapi_init (rc = 0 - Success)
Sun Jan 27 09:23:46 2008: ldapInitAndBind [1] called lcapi_bind (rc = 0 - Success)
Sun Jan 27 09:23:46 2008: LDAP server 1 changed state to CONNECTED
Sun Jan 27 09:23:46 2008: LDAP server 1 now active
Sun Jan 27 09:23:46 2008: LDAP_CLIENT: UID Search (base=OU=ldapuser, DC=wireless,
DC=com, pattern=(&(objectclass=Person)(sAMAccountName=user2)))
Sun Jan 27 09:23:46 2008: LDAP_CLIENT: Returned msg type 0x64
Sun Jan 27 09:23:46 2008: ldapAuthRequest [1] called lcapi_query base="OU=ldapus
er,DC=wireless,DC=com" type="Person" attr="sAMAccountName" user="user2" (rc = 0
- Success)
Sun Jan 27 09:23:46 2008: LDAP ATTR> dn = CN=abcd,OU=ldapuser,DC=Wireless,DC=com
 (size 38)
Sun Jan 27 09:23:46 2008: Handling LDAP response Success
```

A partir das informações destacadas nesta saída de depuração, fica claro que o servidor LDAP é consultado pela WLC com os Atributos do usuário especificados na WLC e que o processo LDAP é bem-sucedido.

 Para verificar se a autenticação EAP local foi bem-sucedida, especifique o comando debug aaa local-auth eap method events enable na CLI da WLC. Aqui está um exemplo:(Cisco Controller) >debug aaa local-auth eap method events enable

 Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT: Process Response (EAP handle = 0x1B000009)Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT: Received TLS record type: Handshake in state: Start Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT: Local certificate found Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT: Reading Client Hello handshake Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT: TLS_DHE_RSA_AES_128_CBC_SHA proposed... Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: Proposed ciphersuite(s): Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: TLS_DHE_RSA_WITH_AES_128_CBC_SHA Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: TLS_RSA_WITH_AES_128_CBC_SHA Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: TLS_RSA_WITH_RC4_128_SHA Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: Selected ciphersuite: Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: TLS_DHE_RSA_WITH_AES_128_CBC_SHA Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT: Building Provisioning Server Hello Sun Jan 27 09:38:29 2008: eap_fast_crypto.c-EVENT: Starting Diffie Hellman phase 1 ... Sun Jan 27 09:38:30 2008: eap_fast_crypto.c-EVENT: Diffie Hellman phase 1 complete Sun Jan 27 09:38:30 2008: eap_fast_auth.c-AUTH-EVENT: DH signature length = 128 Sun Jan 27 09:38:30 2008: eap_fast_auth.c-AUTH-EVENT: Sending Provisioning Serving Hello Sun Jan 27 09:38:30 2008: eap_fast.c-EVENT: Tx packet fragmentation required Sun Jan 27 09:38:30 2008: eap_fast.c-AUTH-EVENT: eap_fast_rx_packet(): EAP Fast NoData (0x2b) Sun Jan 27 09:38:30 2008: eap_fast.c-AUTH-EVENT: eap_fast_rx_packet(): EAP Fast NoData (0x2b) Sun Jan 27 09:38:30 2008: eap_fast.c-AUTH-EVENT: eap_fast_rx_packet(): EAP Fast NoData (0x2b) Sun Jan 27 09:38:32 2008: eap_fast.c-AUTH-EVENT: Process Response, type: 0x2b Sun Jan 27 09:38:32 2008: eap_fast.c-EVENT: Reassembling TLS record Sun Jan 27 09:38:32 2008: eap_fast.c-EVENT: Sending EAP-FAST Ack Sun Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT: Received TLS record type: Handshake in state: Sent provisioning Server Hello

Sun Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT:

Read	ling	Cli	lent Cert:	ificate	e handshake		
Sun	Jan	27	09:38:32	2008:	eap_fast.c-H	event :	Added certificate 1 to chain
Sun	Jan	27	09:38:32	2008:	eap_fast.c-H	event :	Added certificate 2 to chain
Sun	Jan	27	09:38:32	2008:	eap_fast.c-H	event :	Successfully validated received certificate
Sun "EAl	Jan P-FAS	27 ST 1	09:38:32 I-ID" from	2008: m Peer	eap_fast_aut Cert	ch.c-AU	JTH-EVENT: Rx'd I-ID:
Sun Read	Jan ding	27 Cli	09:38:32 Lent Key 1	2008: Exchang	eap_fast_aut ge handshake	ch.c-AU	JTH-EVENT:
Sun Sta:	Jan rting	27 g Di	09:38:32	2008: lman pl	eap_fast_cry hase 2	/pto.c	EVENT:
Sun Dif:	Jan Eie I	27 Hell	09:38:32 Lman phase	2008: e 2 con	eap_fast_cry mplete.	/pto.c	EVENT:
Sun Rea o	Jan ling	27 Cli	09:38:32 Lent Cert:	2008: ificate	eap_fast_aut e Verify hand	th.c-AU	JTH-EVENT:
Sun Sign	Jan 1 cei	27 rtif	09:38:32 Eicate ve	2008: rify su	eap_fast_cry ucceeded (com	/pto.c- mpare)	EVENT:
	••••	• • • •		••••		••••	
• • •	••••	• • • •		••••		•••••	
• • •	••••	• • • •		••••		•••••	
	••••	• • • •		••••		•••••	
Оc	oma	and	o debug a	aaa loo	cal-auth db e	enable	também é muito útil. Aqui está um
exe Sun	mpl Jan	0:((27	09:35:32	ntroller 2008:	<pre>c) >debug aa LOCAL_AUTH:</pre>	a loca	l-auth db enable Received an auth request
Sun	Jan	27	09:35:32	2008:	LOCAL_AUTH:	Creat	ng new context
Sun	Jan	27	09:35:32	2008:	LOCAL_AUTH:	Local	auth profile name for context 'ldapuser'
Sun	Jan	27	09:35:32	2008:	LOCAL_AUTH:	Create	ed new context eap session handle fb000007
Sun (id	Jan 2) t	27 to B	09:35:32 EAP subsys	2008: s	LOCAL_AUTH:	(EAP:8	3) Sending the Rxd EAP packet
Sun	Jan	27	09:35:32	2008:	LOCAL_AUTH:	Found	matching context for id - 8
Sun requ	Jan 1est	27 use	09:35:32 ername 'us	2008: ser2' 1	LOCAL_AUTH: to LDAP	(EAP)	Sending user credential
Sun	Jan	27	09:35:32	2008:	LOCAL_AUTH:	Found	context matching MAC address - 8
	••••					•••••	
• • •	••••	• • • •		••••		•••••	
•••	••••	• • • •		••••		•••••	
	••••					••••	

Sun Jan 27 09:35:36 2008: LOCAL_AUTH: (EAP:8) Sending the Rxd EAP packet (id 12) to EAP subsys
Sun Jan 27 09:35:36 2008: LOCAL_AUTH: Found matching context for id - 8
Sun Jan 27 09:35:36 2008: LOCAL_AUTH: (EAP:8) ---> [KEY AVAIL] send_len 64, recv_len 0
Sun Jan 27 09:35:36 2008: LOCAL_AUTH: (EAP:8) received keys waiting for success
Sun Jan 27 09:35:36 2008: LOCAL_AUTH: Found matching context for id - 8
Sun Jan 27 09:35:36 2008: LOCAL_AUTH: (EAP:8) Received success event
Sun Jan 27 09:35:36 2008: LOCAL_AUTH: (EAP:8) Received success event

 Para visualizar os certificados instalados na WLC a serem usados para autenticação local, execute o comando show local-auth certificates na CLI da WLC. Aqui está um exemplo:(Controlador Cisco) >show local-auth certificates
 Certificates available for Local EAP authentication:

Certificate issuer vendor

CA certificate:

Subject: DC=com, DC=Wireless, CN=wireless

Issuer: DC=com, DC=Wireless, CN=wireless

Valid: 2008 Jan 23rd, 15:50:27 GMT to 2013 Jan 23rd, 15:50:27 GMT

Device certificate:

Subject: O=cisco, CN=ciscowlc123

Issuer: DC=com, DC=Wireless, CN=wireless

Valid: 2008 Jan 24th, 12:18:31 GMT to 2010 Jan 23rd, 12:18:31 GMT

Certificate issuer cisco

CA certificate:

Subject: O=Cisco Systems, CN=Cisco Manufacturing CA

Issuer: O=Cisco Systems, CN=Cisco Root CA 2048

Valid: 2005 Jun 10th, 22:16:01 GMT to 2029 May 14th, 20:25:42 GMT

Device certificate:

Not installed.

 Para visualizar a configuração de autenticação local na WLC a partir do modo CLI, execute o comando show local-auth config. Aqui está um exemplo:(Controlador Cisco) >show local-auth config

User credentials database search order:

Timer:									
Active timeout	300								
Configured EAP profiles:									
Name	ldapuser								
Certificate issuer	vendor								
Peer verification options:									
Check against CA certificates	Enabled								
Verify certificate CN identity	Disabled								
Check certificate date validity	Disabled								
EAP-FAST configuration:									
Local certificate required	Yes								
Client certificate required	Yes								
Enabled methods	fast								
Configured on WLANs	2								
EAP Method configuration:									
EAP-FAST:									
More or (q)uit									
Server key	<hidden></hidden>								
TTL for the PAC	10								
Anonymous provision allowed	No								
Authority Information	Cisco A-ID								

Troubleshoot

Você pode usar estes comandos para solucionar problemas de configuração:

- debug aaa local-auth eap method events enable
- debug aaa all enable
- debug dot1x packet enable

Informações Relacionadas

- Exemplo de Autenticação EAP-FAST com Controladoras Wireless LAN e Servidor RADIUS
 <u>Externo</u>
- PEAP sob redes sem fio unificadas com o Internet Authentication Service da Microsoft (IAS)
- Exemplo de configuração de atribuição de VLAN dinâmica com WLCs baseadas em ACS para mapeamento de grupo do Ative Diretory
- <u>Guia de configuração do Cisco Wireless LAN Controller Configurando soluções de</u> segurança
- <u>Guia de configuração do Cisco Wireless LAN Controller Gerenciamento do software e das</u> <u>configurações do controlador</u>
- Exemplo de Configuração de Autenticação EAP com WLAN Controllers (WLC)
- Perguntas frequentes sobre o design e os recursos do controlador de LAN sem fio (WLC)
- <u>Cisco Secure Services Client com autenticação EAP-FAST</u>
- Perguntas frequentes sobre a controladora Wireless LAN (WLC)
- <u>Perguntas frequentes sobre mensagens de sistema e erros da controladora Wireless LAN</u>
 <u>(WLC) das controladoras</u>
- Suporte Técnico e Documentação Cisco Systems

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.