# WPA (Wi-Fi Protected Access) em um Exemplo de Configuração de Rede Wireless Unificada da Cisco

# Contents

Introduction Prerequisites Requirements Componentes Utilizados Conventions Suporte a WPA e WPA2 Instalação de rede Configurar os dispositivos para o modo empresarial WPA2 Configurar a WLC para autenticação RADIUS através de um servidor RADIUS externo Configurar a WLAN para o Modo de Operação WPA2 Enterprise Configurar o servidor RADIUS para a autenticação do modo empresarial WPA2 (EAP-FAST) Configurar o cliente sem fio para o modo de operação WPA2 Enterprise Configurar o cliente sem fio para o modo de operação WPA2 Enterprise Configure os dispositivos para o modo WPA2-Personal Troubleshoot Informações Relacionadas

# **Introduction**

Este documento descreve como configurar o WPA (Wi-Fi Protected Access) em uma Cisco Unified Wireless Network.

# **Prerequisites**

### **Requirements**

Verifique se você tem o conhecimento básico desses tópicos antes de experimentar esta configuração:

- WPA
- Soluções de segurança para LAN sem fio (WLAN)Observação: consulte <u>Visão Geral do Cisco</u> <u>Wireless LAN Security</u> para obter informações sobre as soluções de segurança WLAN da Cisco.

### **Componentes Utilizados**

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

- Pontos de acesso Lightweight (LAP) Cisco 1000 Series
- Controladora de LAN sem fio (WLC) Cisco 4404 com firmware 4.2.61.0
- Adaptador cliente Cisco 802.11a/b/g com firmware 4.1
- Aironet Desktop Utility (ADU) que executa o firmware versão 4.1
- Servidor Cisco Secure ACS versão 4.1

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>

# Suporte a WPA e WPA2

O Cisco Unified Wireless Network inclui suporte para as certificações WPA e WPA2 da Wi-Fi Alliance. A WPA foi introduzida pela Wi-Fi Alliance em 2003. A WPA2 foi introduzida pela Wi-Fi Alliance em 2004. Todos os produtos com certificação Wi-Fi para WPA2 precisam ser interoperáveis com os produtos com certificação Wi-Fi para WPA.

A WPA e a WPA2 oferecem um alto nível de garantia para usuários finais e administradores de rede de que seus dados permanecerão privados e de que o acesso a suas redes será restrito a usuários autorizados. Ambos têm modos de operação pessoais e corporativos que atendem às necessidades distintas dos dois segmentos de mercado. O Modo Empresarial de cada um usa IEEE 802.1X e EAP para autenticação. O modo pessoal de cada um usa a chave pré-compartilhada (PSK) para a autenticação. A Cisco não recomenda o Modo Pessoal para implantações empresariais ou governamentais porque ele usa uma PSK para autenticação de usuário. A PSK não é segura para ambientes corporativos.

A WPA aborda todas as vulnerabilidades WEP conhecidas na implementação de segurança IEEE 802.11 original, trazendo uma solução de segurança imediata para as WLANs em ambientes corporativos e de pequenos escritórios/escritórios residenciais (SOHO). A WPA usa TKIP para criptografia.

A WPA2 é a próxima geração de segurança Wi-Fi. É a implementação interoperável da Wi-Fi Alliance do padrão IEEE 802.11i ratificado. Ele implementa o algoritmo de criptografia AES recomendado pelo National Institute of Standards and Technology (NIST) usando o Counter Mode com o Cipher Block Chaining Message Authentication Code Protocol (CCMP). O WPA2 facilita a conformidade com FIPS 140-2 do governo.

#### Comparação dos tipos de modo WPA e WPA2

	WPA	WPA2
	<ul> <li>Autentica</li> </ul>	Autentica
Modo corporativo	ção: IEEE	ção:
(empresanal, governamental	802.1X/E	IEEE
educacional)	AP	802.1X/E
oddolonaly	<ul> <li>Criptograf</li> </ul>	AP

	ia: TKIP/MIC	<ul> <li>Criptograf</li> <li>ia: AES-</li> <li>CCMP</li> </ul>
Modo pessoal (SOHO, Início/Pessoal)	<ul> <li>Autentica ção: PSK</li> <li>Criptograf ia: TKIP/MIC</li> </ul>	<ul> <li>Autentica ção: PSK</li> <li>Criptograf ia: AES- CCMP</li> </ul>

No modo de operação empresarial, a WPA e a WPA2 usam 802.1X/EAP para autenticação. O 802.1X fornece às WLANs uma autenticação forte e mútua entre um cliente e um servidor de autenticação. Além disso, o 802.1X fornece chaves de criptografia dinâmicas por usuário e por sessão, eliminando a carga administrativa e os problemas de segurança relacionados às chaves de criptografia estáticas.

Com o 802.1X, as credenciais usadas para autenticação, como senhas de logon, nunca são transmitidas sem criptografia, ou sem criptografia, pelo meio sem fio. Embora os tipos de autenticação 802.1X forneçam autenticação forte para LANs sem fio, o TKIP ou o AES são necessários para criptografia, além do 802.1X, já que a criptografia WEP 802.11 padrão é vulnerável a ataques de rede.

Existem vários tipos de autenticação 802.1X, cada um fornecendo uma abordagem diferente para a autenticação, contando com a mesma estrutura e EAP para comunicação entre um cliente e um ponto de acesso. Os produtos Cisco Aironet suportam mais tipos de autenticação EAP 802.1X do que qualquer outro produto WLAN. Os tipos suportados incluem:

- <u>Cisco LEAP</u>
- Autenticação EAP flexível via encapsulamento seguro (EAP-FAST)
- EAP-Transport Layer Security (EAP-TLS)
- Protocolo de autenticação extensível protegido (PEAP)
- TLS em túnel EAP (EAP-TTLS)
- EAP-Módulo de identidade do assinante (EAP-SIM)

Outro benefício da autenticação 802.1X é o gerenciamento centralizado para grupos de usuários de WLAN, incluindo rotação de chaves baseada em políticas, atribuição de chaves dinâmicas, atribuição de VLAN dinâmica e restrição de SSID. Esses recursos alternam as chaves de criptografia.

No modo Pessoal de operação, uma chave pré-compartilhada (senha) é usada para autenticação. O modo pessoal requer apenas um ponto de acesso e um dispositivo cliente, enquanto o modo empresarial normalmente requer um RADIUS ou outro servidor de autenticação na rede.

Este documento fornece exemplos para a configuração de WPA2 (modo Empresarial) e WPA2-PSK (modo Pessoal) em uma rede Cisco Unified Wireless.

#### Instalação de rede

Nesta configuração, uma WLC Cisco 4404 e um LAP Cisco 1000 Series são conectados através de um Switch de Camada 2. Um servidor RADIUS externo (Cisco Secure ACS) também está conectado ao mesmo switch. Todos os dispositivos estão na mesma sub-rede. O ponto de acesso (LAP) é registrado inicialmente na controladora. É necessário criar duas LANs sem fio, uma para

o modo WPA2 Enterprise e outra para o modo WPA2 Personal.

A WLAN do modo WPA2-Enterprise (SSID: WPA2-Enterprise) usará EAP-FAST para autenticar os clientes Wireless e o AES para criptografia. O servidor Cisco Secure ACS será usado como o servidor RADIUS externo para autenticar os clientes sem fio.

A WLAN do modo WPA2-Personal (SSID: WPA2-PSK) usará a WPA2-PSK para autenticação com a chave pré-compartilhada "abcdefghijk".

Você precisa configurar os dispositivos para esta configuração:



### Configurar os dispositivos para o modo empresarial WPA2

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

Execute estas etapas para configurar os dispositivos para o modo de operação WPA2 Enterprise:

- 1. Configurar a WLC para autenticação RADIUS através de um servidor RADIUS externo
- 2. Configurar a WLAN para a Autenticação do Modo Empresarial WPA2 (EAP-FAST)
- 3. Configurar o cliente sem fio para o modo WPA2-Enterprise

<u>Configurar a WLC para autenticação RADIUS através de um servidor RADIUS</u> <u>externo</u> A WLC precisa ser configurada para encaminhar as credenciais do usuário a um servidor RADIUS externo. O servidor RADIUS externo valida as credenciais do usuário usando EAP-FAST e fornece acesso aos clientes sem fio.

Conclua estes passos para configurar o WLC para um servidor RADIUS externo:

- Escolha Security e RADIUS Authentication na GUI da controladora para exibir a página RADIUS Authentication Servers. Em seguida, clique em New para definir um servidor RADIUS.
- Defina os parâmetros do servidor RADIUS na página Servidores de autenticação RADIUS > Novo. Esses parâmetros incluem:Endereço IP do servidor RADIUSshared secretnúmero da portaStatus do servidorEste documento usa o servidor ACS com um endereço IP 10.77.244.196.

				Sa <u>v</u> e Co	nfiguration <u>P</u> ing	Logout   Befresh
cisco	MONITOR WLANS CONTRO	LLER WIRELESS SECURITY	MANAGEMENT C	QMMANDS	нецр	
Security	RADIUS Authentication S	ervers > New			< Back	Apply
General	Server Index (Priority)	1 .				
RADIUS     Authentication     Accounting	Server IPAddress	10.77.244.196				
TACACS+ LDAP	Shared Secret Format	ASCII ×				
Local Net Users MAC Filtering	Shared Secret	•••••				
User Login Policies AP Policies	Confirm Shared Secret	****				
Local EAP	Key Wrap	(Designed for FIPS customers)	and requires a key w	rap compliant	RADIUS server)	
Priority Order	Port Number	1812				
▶ Access Control Lists	Port Number	1012				
Wireless Protection     Policies	Server Status	Enabled 💌				
Web Auth	Support for RFC 3576	Enabled 💌				
Advanced	Server Timeout	2 seconds				
	Network User	🕅 Enable				
	Management	Enable				
	IPSec	Enable				

3. Clique em Apply.

### Configurar a WLAN para o Modo de Operação WPA2 Enterprise

Em seguida, configure a WLAN que os clientes usarão para se conectar à rede sem fio. O SSID da WLAN para o modo WPA2-Empresa será WPA2-Empresa. Este exemplo atribui esta WLAN à interface de gerenciamento.

Conclua estes passos para configurar a WLAN e seus parâmetros relacionados:

- 1. Clique em **WLANs** na GUI do controlador para exibir a página WLANs.Esta página lista as WLANs que existem na controladora.
- 2. Clique em New para criar uma nova WLAN.
- Insira o nome SSID da WLAN e o nome do perfil na página WLANs > New. Em seguida, clique em Apply.Este exemplo usa WPA2-Enterprise como o SSID.

		_					Sa <u>v</u> e Co	nfiguration <u>Ping</u>	Logout Befr
CISCO	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
WLANs	WLANs > N	New						< Back	Apply
WLANS	Туре		WLAN						
▶ Advanced	Profile Nam	ne	WPA2-Ent	erprise					
	WLAN SSID	,	WPA2-Ent	erprise					

- 4. Quando você criar uma nova WLAN, a página WLAN > Edit da nova WLAN será exibida. Nesta página, você pode definir vários parâmetros específicos para esta WLAN. Isso inclui políticas gerais, políticas de segurança, políticas de QOS e parâmetros avançados.
- 5. Em General Policies (Regras gerais), marque a caixa de seleção **Status** para habilitar a WLAN.

- alulu-					Sage Co	nfiguration   Bing	Logout <u>R</u> efresh
CISCO	MONITOR WLANS COM	ITROLLER WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
WLANs	WLANs > Edit					< Back	Apply
	General Security	QoS Advanced					
✓ WLANS WLANS							
Advanced	Profile Name	WPA2-Enterprise					
	Туре	WLAN					
	SSID	WPA2-Enterprise					
	Status	Enabled					
	Security Policies	[WPA2][Auth(802.1X	)]				
		(Modifications done unde	r security tab	will appear after ap	plying the chang	pes.)	
	Radio Policy	AI X					
	Interface	management 💌					
	Broadcast SSID	Enabled					
	For the block of						
	Foot Notes	they model diff					
	2 Web Policy cannot be use	ed in combination with IPse	ec.				
	4 When client exclusion is	enabled, a Timeout Value	of zero means	infinity (will require	e administrative	override to reset excl	uded clients)
	S Client MFP is not active u	nless WPA2 is configured					

- 6. Se você quiser que o AP transmita o SSID em seus quadros beacon, marque a caixa de seleção SSID de broadcast.
- Clique na guia Security. Em Layer 2 Security, selecione WPA+WPA2. Isso ativa a autenticação WPA para a WLAN.

cisco	Sage Configuration Bing Logout Befresh MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANS	WLANs > Edit < Back Apply General Security QoS Advanced
WLANs Advanced	Layer 2 Layer 3 AAA Servers Layer 2 Security WPA+WPA2 MAC Filtering Static WEP Parameters
	802.11 Data Encryption     Current Key:     104 bits WEP Static Key (Key Index = 0)       Type     Key Size     Key Index     Encryption Key       WEP     not set     1     ASCII
	CKIP Parameters &           802.11 Data Encryption         Current Key:         0 bits CKIP Key (Key Index= 0)           Key Size         Key Index         Encryption Key         Key Format
	Foot Notes
	1 CKIP is not supported by 10xx model APs 2 Web Policy cannot be used in combination with IPsec 3 H-REAP Local Switching is not supported with IPsec, CRANITE authentication 4 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients) 5 Client MIP is not active unless WPA2 is configured

8. Role a página para baixo para modificar os **parâmetros WPA+WPA2**.Neste exemplo, a política WPA2 e a criptografia AES estão selecionadas

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMM	Sa <u>v</u> e Configuration : Eing   Logout   <u>R</u> efresh MANDS   HELP
VLANS VLANS VLANS Advanced	MONITOR       WLANS       CONTROLLER       WIRELESS       SECURITY       MANAGEMENT       COMM         WLANS > Edit	Key Format
	2 Web Policy cannot be used in combination with IPsec 3 H-REAP Local Switching is not supported with IPsec, CRANITE authentication 4 When client exclusion is enabled, a Timeout Value of zero means infinity (will require admin 5 Client MPP is not active unless WPA2 is configured	istrative override to reset excluded clients)

- 9. Em Auth Key Mgmt, selecione **802.1x**.Isso habilita a WPA2 usando a autenticação 802.1x/EAP e a criptografia AES para a WLAN.
- 10. Clique na guia **Servidores AAA.** Em Authentication Servers, escolha o endereço IP do servidor apropriado.Neste exemplo, 10.77.244.196 é usado como o servidor

ADIUS.		
	Sa <u>v</u> e Configurat	ion   <u>P</u> ing   Logout   <u>R</u> efr
CISCO	MONITOR MUANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP	
LANs	WLANs > Edit	< Back Apply
UT AND	General Security QoS Advanced	
WLANs	Laver 2 Laver 3 AAA Servers	
Advanced		
	Select AAA servers below to override use of default servers on this WLAN	
	Radius Servers LDAP Servers	
	Authentication Servers Accounting Servers Server 1 None -	
	Enabled Server 2 None	
	Server 1P:10.77.244.196, Port:1812 • None • Server 3 None •	
	Server None None .	
	Server None	
	3 [Note 22]	
	Local EAP Authentication	
	Local EAP Authentication I_Enabled	
	Foot Notes	
	1 CKIP is not supported by 10xx model APs 2 Web Policy cannot be used in combination with IPsec	
	3 H-REAP Local Switching is not supported with IPsec, CRANITE authentication 4 When client accurate application of Transport Value of page means inforty (will require administrative quertid	a to secat evolutied clients)
	5 Client MP is not active unless WPA2 is configured	roureset excluded chemas

11. Clique em Apply. Observação: essa é a única configuração EAP que precisa ser configurada na controladora para autenticação EAP. Todas as outras configurações específicas do EAP-FAST precisam ser feitas no servidor RADIUS e nos clientes que precisam ser autenticados.

### <u>Configurar o servidor RADIUS para a autenticação do modo empresarial WPA2</u> (EAP-FAST)

Neste exemplo, o Cisco Secure ACS é usado como o servidor RADIUS externo. Execute estas etapas para configurar o servidor RADIUS para autenticação EAP-FAST:

- 1. Crie um banco de dados de usuário para autenticar clientes
- 2. Adicione a WLC como AAA Client ao servidor RADIUS

. . . . . . .

3. <u>Configurar a autenticação EAP-FAST no servidor RADIUS com o provisionamento de PAC anônimo em banda</u>Observação: o EAP-FAST pode ser configurado com o Provisionamento de PAC In-band anônimo ou Provisionamento de PAC In-band autenticado. Este exemplo usa o Provisionamento PAC Anônimo In-band. Para obter informações detalhadas e exemplos sobre como configurar o EAP FAST com Provisionamento PAC In-band Anônimo e Provisionamento In-band Autenticado, consulte <u>Autenticação EAP-FAST com</u> <u>Controladoras Wireless LAN e Exemplo de Configuração de Servidor RADIUS Externo</u>.

#### Crie um banco de dados de usuário para autenticar clientes EAP-FAST

Conclua estas etapas para criar um banco de dados de usuário para clientes EAP-FAST no ACS. Este exemplo configura o nome de usuário e a senha do cliente EAP-FAST como User1 e User1, respectivamente. 1. Na GUI do ACS na barra de navegação, selecione **User Setup**. Crie um novo usuário sem fio e clique em **Add/Edit** para ir para a página Edit deste



 Na página User Setup Edit, configure Real Name e Description, bem como as configurações de Password, conforme mostrado neste exemplo.Este documento usa o banco de dados interno do ACS para autenticação de senha.

kess http://127.0	.0.1:1065/	- 61
Cisco Svorems	User Setup	
alb alb	Edit	Help
User Setup Setup Setup	User: User1 (New User)	Account Disabled     Oxisting & Oremann     Supplementary User Info     Password Avdientication     Group to which the user is assigned
Network Configuration System Configuration	Supplementary User Info       Real Name       Description	Callback Client 3D Advanced SetSings Advanced SetSings Network Access Restrictions Nan Seasions Usage Operan Access to hable Overvised able Covervised able
Administration Centrol Control Control Posture Posture Validation Network Access Profiles	User Setup ? Password Authentication: ACS Internal Database CiscoSecure PAP (Also used for CHAP/MS- CHAP/ARAP, if the Separate field is not	Advanced TACACS+ Settings     TACACS+ Enable Parsword     TACACS+ Enable Parsword     TACACS+ Dutheand Parsword     TACACS+ Shell Command Authorization     Command Authorization for Network Device Nanagement Applications     TACACS+ Unknown Services     TACACS+ Unknown Services     RADIUS Attributes     RADIUS Yeador-Specific Attributes
Reports and Activity	Checked.) Password Confirm Password Separate (CHAP/MS-CHAP/ARAP) Password	Account Disabled Status Select the Account Disabled check box to disable this account: clear the check box to enable the account. [Back to Top]
	Confirm Password Submit Cancel	Deleting a Username The Delete button appears only when you are editing an existing user account, not when you are adding a new user account. To delete the connect user account from the database, click <b>Delete</b> . When asked to confirm your action, click <b>OK</b> .

- 3. Escolha ACS Internal Database na caixa suspensa Password Authentication.
- 4. Configure todos os outros parâmetros necessários e clique em Enviar.

#### Adicione a WLC como AAA Client ao servidor RADIUS

Conclua estas etapas para definir o controlador como um cliente AAA no servidor ACS:

- Clique em Network Configuration na GUI do ACS. Na seção Add AAA client da página Network Configuration, clique em Add Entry para adicionar a WLC como o cliente AAA ao servidor RADIUS.
- Na página AAA Client, defina o nome da WLC, o endereço IP, o segredo compartilhado e o método de autenticação (RADIUS/Cisco Airespace). Consulte a documentação do fabricante para outros servidores de autenticação não ACS.

CiscoSecure ACS - Mic	rosoft Internet Explorer	د روب این بیدر
Address http://127.0.0	71:1002\ xxxx Toos Gieb	uns " 🙀
Cinco Svorems	Network Configuration	×
-dbs-dbs-	Edit	E Help
User Setup Setup Setup Setup SharedProfile Components Network Configuration System Configuration	Add AAA Client AAA Client Hostname WLC AAA Client IP Address 10.77.244.204 Shared Secret cisco	AAA Client Hostname     AAA Client IP Address     Shared Secret     Network Device Group     BADUS Key Yane     Authenticate Using     Single Connect TACACS - AAA Client     Lea Bodate Withdee Packets from this     AAA Client     Lea RADIUS Transiting Packets from this     AAA Client     Replace RADIUS Part info with Username     from this AAA Client     Nath Client
Administration Central User Databases	RADIUS Key Wrap Key Encryption Key Message Authenticator Code Key	AAA Client Hortname
Network Access	Authenticate Lision RADIUS (Cisco Airesnace)	The AAA Client Hostname is the name assigned to the AAA client.
Activity Online Decementation	Single Connect TACACS+ AAA Client (Record stop in accounting on failure)	AAA Client IP Address
- I service and	Log Update/Watchdog Packets from this AAA Client     Log RADIUS Tunneling Packets from this AAA Client	The AAA Client IP Address is the IP address assigned to the AAA client.
	Replace RADIUS Port info with Username from this AAA Client     Match Framed-IP-Address with user IP address for accounting packets from     this AAA Client	If you want to designate more than one AAA client with a single AAA client entry in ACS, you can specify the D address for each AAA client to be represented by this AAA client actors. To
Done		internet

**Observação:** a chave secreta compartilhada que você configura no WLC e no servidor ACS deve corresponder. O segredo compartilhado diferencia maiúsculas de minúsculas.

3. Clique em Enviar e aplicar.

# Configurar a autenticação EAP-FAST no servidor RADIUS com o provisionamento de PAC anônimo em banda

#### Provisionamento anônimo em banda

Este é um dos dois métodos de provisionamento em banda em que o ACS estabelece uma conexão segura com o cliente usuário final com a finalidade de fornecer ao cliente uma nova PAC. Essa opção permite um handshake TLS anônimo entre o cliente do usuário final e o ACS.

Este método opera dentro de um túnel do protocolo de acordo Diffie-HellmanKey (ADHP) autenticado antes que o peer autentique o servidor ACS.

Em seguida, o ACS requer a autenticação EAP-MS-CHAPv2 do usuário. Na autenticação de usuário bem-sucedida, o ACS estabelece um túnel Diffie-Hellman com o cliente de usuário final. O ACS gera uma PAC para o usuário e a envia ao cliente usuário final nesse túnel, juntamente com informações sobre esse ACS. Esse método de provisionamento usa EAP-MSCHAPv2 como o método de autenticação na fase zero e EAP-GTC na fase dois.

Como um servidor não autenticado é provisionado, não é possível usar uma senha de texto simples. Portanto, somente as credenciais MS-CHAP podem ser usadas dentro do túnel. O MS-CHAPv2 é usado para provar a identidade do par e receber uma PAC para outras sessões de autenticação (EAP-MS-CHAP será usado apenas como método interno).

Conclua estas etapas para configurar a autenticação EAP-FAST no servidor RADIUS para provisionamento anônimo em banda:

1. Clique em **System Configuration** na GUI do servidor RADIUS. Na página System Configuration, escolha **Global Authentication** 



 Na página de configuração Autenticação global, clique em Configuração EAP-FAST para ir para a página de configurações EAP-FAST.

state 181 and distri	.0.0.1:1065/		1 <b>2</b> 0
Cisco Systems	System Configuration		×
Diller 1	EAP Configuration	?	Help
Group Setup	PEAP  Allow EAP-MSCHAPv2  Allow EAP-GTC		Use this page to specify settings for various authentication protocols.
Shared Profile Components	Allow Posture Validation		• PEAP • EAP-FAST • EAP-FAST • EAP-FAST • EAP-FAST
Sustem Configuration	Callow EAP-TLS Select one or more of the following options: Certificate SAN comparison Certificate CN comparison		EAP-MDS     AP-EAP-Request Timesut     MS-CHAP-Configuration
Administration Control	EAP-TLS session timeout (minutes): 120		EAP Configuration
Validation	Cisco client initial message: PEAP session timeout (minutes): 120		authentic stool information (UTV, 2.204), EAP 18 separed on top of another protocols such as UDV, 902.1n or RADEUS and supports multiple "authentication" types. [Back to Tisp]
Reports and	Enable Fast Reconnect:	_	реар
Activity	EAP-FAST EAP-FAST Configuration		PEAP is the outer layer protocol for the secure tunnel.
	EAP-TLS	-	Note: HEAP is a contribute-based authentication protocol. HEAP authentication can occur only after you have completed the required steps on the <b>ACS Certificate Setup page.</b>
	Select one or more of the following options:	-	<ul> <li>Allow EAP-MSCHAPv2 — Use to enable EAP-MSCHAPv2 within MS PEAP authentication. Enable this protocol for any repository that supports MS- CHAPv2, such as Microsoft AD, and the ACS Internal Database.</li> </ul>
	Submit Submit + Restart Cancel		

3. Na página Configurações de EAP-FAST, marque a caixa de seleção **Permitir EAP-FAST** para ativar o EAP-FAST no servidor RADIUS.

ElscoSecure ACS - M	Scrosoft Internet Explorer	LIDIX
Ele Edt Yew Far	roniters Iools Help	Links 🍟 🦧
Address a http://127.0	0.0.1:1065/	💌 🛃 Go
Cisco Systems	System Configuration	×
	EAP-FAST Configuration	A Help A
User Setup	EAD EAD Rothings	EAP-FAST Configuration Page
Setup	EAP-FAST Settings	Use this page to configure EAP-FAST authentication settings.
Shareditrofile Components Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration	Allow EAP-FAST Active master key TTL Retired master key TTL Imonths  Tunnel PAC TTL Imonths  Client initial message: Authority ID Info: Reduebacs Authority ID Info: Allow anonymous in-band PAC provisioning Allow authenticated in-band PAC provisioning Require client on authenticated provisioning Require client certificate for provisioning	EAP-FAST Settings     Cleant initial measures     Antherity ID Infe     Allow anthentics the and PAC provisioning     Allow anthentic attain     Allow anthentic attain     Allow anthentic method     EAP-FAST settings     EAP-FAST settings     EAP-FAST Settings     Actual EAP-FAST—To enable EAP-FAST authentication, select this check box.
Reports and Counter and Count	Allow Machine Authentication Machine PAC TTL 1 weeks Allow Stateless session resume Authorization PAC TTL 1 hours Allowed inner methods EAP-GTC EAP-GTC EAP-TLS Submit Submit + Restart Cancel	<ul> <li>Active Master Key TIL - Enter a value for the amount of time that a master key is used to generate new Protected Access Credentials (PACs). When the time to live (TTL) defined for the Master Key expires, the master key is considered retired and a new master key is generated.</li> <li>Retired master key TIL - Enter a value for the amount of time that PACs generated using a retired master key are acceptable for EAP-FAST authentication. When an end-user client gains network access using a PAC based on a retired master key, ACS sends a new PAC to the end-user client.</li> <li>Tennel PAC TIL - Enter a value for the amount of time that a PAC is used before it expires and must be replaced. If the master key used to generate the Tunnel PAC has not expired, new PAC creation and assignment is automatic. If the master key used to generate the Tunnel PAC has net expired, new PAC creation and assignment is automatic. If the master key used to generate the tonnel PAC empired, automatic or manual growinsoning must be used to provide the end-user client with a new PAC.</li> </ul>
		internet
start 🕜 🥭	CiscoSecure ACS - Mic	9 7:58 PM

- 4. Configure os valores TTL (Time-to-Live) da chave mestra ativa/desativada conforme desejado ou defina-a com o valor padrão conforme mostrado neste exemplo.Consulte Chaves mestre para obter informações sobre chaves mestre ativas e desativadas. Além disso, consulte Chaves mestras e TTLs PAC para obter mais informações.O campo Authority ID Info (Informações de ID da autoridade) representa a identidade textual desse servidor ACS, que um usuário final pode usar para determinar em qual servidor ACS será autenticado. O preenchimento deste campo é obrigatório.O campo Mensagem de exibição inicial do cliente especifica uma mensagem a ser enviada aos usuários que se autenticam em um cliente EAP-FAST. O comprimento máximo é de 40 caracteres. Um usuário verá a mensagem inicial apenas se o cliente do usuário final suportar a exibição.
- 5. Se desejar que o ACS execute o fornecimento de PAC anônimo dentro da banda, marque a caixa de seleção **Permitir fornecimento de PAC anônimo dentro da banda**.
- 6. Métodos internos permitidos Essa opção determina quais métodos EAP internos podem ser executados dentro do túnel EAP-FAST TLS. Para provisionamento anônimo em banda, você deve habilitar EAP-GTC e EAP-MS-CHAP para compatibilidade com versões anteriores. Se você selecionar Permitir fornecimento de PAC anônimo em banda, deverá selecionar EAP-MS-CHAP (fase zero) e EAP-GTC (fase dois).

### Configurar o cliente sem fio para o modo de operação WPA2 Enterprise

A próxima etapa é configurar o cliente sem fio para o modo de operação WPA2 Enterprise.

Conclua estas etapas para configurar o cliente sem fio para o modo WPA2 Enterprise.

1. Na janela Aironet Desktop Utility, clique em Profile Management > New para criar um perfil

para o usuário WPA2-Enterprise WLAN.Como mencionado anteriormente, este documento usa o nome WLAN/SSID como **WPA2-Enterprise** para o cliente sem fio.

 Na janela Gerenciamento de perfil, clique na guia Geral e configure o Nome do perfil, o Nome do cliente e o nome SSID como mostrado neste exemplo. Clique em OK

ofile M	anageme	ent		? 🛛
General	Security	Advance	b	
Profile	Settings			
	Profile	e Name:	WPA2-Enterprise	
	Clien	it Name:	Wireless-Client1	
Netwo	ork Names			
		SSID1:	WPA2-Enterprise	
		SSID2:		
		SSID3:		
L.		ananan aragitar		
			OK	Cancel

 Clique na guia Security e escolha WPA/WPA2/CCKM para habilitar o modo de operação WPA2. Em WPA/WPA2/CCKM EAP Type, selecione EAP-FAST. Clique em Configure para definir a configuração EAP-FAST.

Profile Management		? 🗙
General Security Advanced		
- Set Security Options	)	
⊙ WPA/WPA2/CCKM	WPA/WPA2/CCKM EAP Type: EAP-FAST	
○ WPA/WPA2 Passphrase		
○ 802.1x	802.1x EAP Type: LEAP	
O Pre-Shared Key (Static WEP)		
○ None		
Configure	Allow Association to Mixed Cells	
	Limit Time for Finding Domain Controller To: 0 0 sec	
Group Policy Delay:	60 🗢 sec	
	ОК	Cancel

4. Na janela Configurar EAP-FAST, marque a caixa de seleção Permitir Provisionamento Automático de PAC. Se você quiser configurar o fornecimento de PAC anônimo, EAP-MS-CHAP será usado como o único método interno na fase zero.

Configure EAP-FAST	? 🔀
EAP-FAST Authentication Method	
MSCHAPv2 User Name and Password	Configure
Protected Access Credentials (PAC)	
Select One or More PAC Authorities	
	Manage
<	<b>&gt;</b>
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	
	OK Cancel

- 5. Escolha Nome de usuário e Senha MSCHAPv2 como o método de autenticação na caixa suspensa Método de autenticação EAP-FAST. Clique em Configurar.
- 6. Na janela Configure MSCHAPv2 User Name and Password (Configurar nome de usuário e senha MSCHAPv2), escolha as configurações apropriadas de nome de usuário e senha.Este exemplo escolhe Solicitar automaticamente o nome do usuário e a senha.

	- M 201	
ny>		
er Name and Password S	Settings	
💿 Use Temporary Use	ar Name and Password	
O Use Windows I	User Name and Password	
Automatically F	Prompt for User Name and Password	
O Use Saved User Nar	me and Password	
User Name:	Administrator	
Password:		
Confirm Password:		
Confirm Password: Domain:		

mesmo nome de usuário e senha devem ser registrados no ACS. Como mencionado anteriormente, este exemplo usa User1 e User1 respectivamente como nome de usuário e senha. Além disso, observe que esse é um provisionamento anônimo dentro da banda. Portanto, o cliente não pode validar o certificado do servidor. É necessário verificar se a caixa de seleção Validar identidade do servidor está desmarcada.

7. Click OK.

#### Verificar o Modo de Operação do WPA2 Enterprise

Conclua estas etapas para verificar se a configuração do modo WPA2 Enterprise está funcionando corretamente:

- 1. Na janela do Aironet Desktop Utility, selecione o perfil **WPA2-Enterprise** e clique em **Ativate** para ativar o perfil do cliente sem fio.
- 2. Se você tiver habilitado o MS-CHAP ver2 como sua autenticação, o cliente solicitará o nome

		,			
dD.	1101	ıar	'IO	Δ	а
uc	usu	iui	IU.	C	u

Please enter your E network	AP-FAST username and password to log on to the wirele:
User Name :	User1
Password :	•••••
Log on to :	
Card Name :	Cisco Aironet 802.11a/b/g Wireless Adapter

 Durante o processamento EAP-FAST do usuário, o cliente solicitará uma PAC ao servidor RADIUS. Quando você clica em Sim, o fornecimento de PAC é iniciado.

EAP-FAST Authentica	tion		×
You do not have a valid l automatic provisioning?	PAC from the authentication se	rver. Do you want to proceed and request	
	Yes	No	

4. Após o fornecimento bem-sucedido da PAC na fase zero, as fases um e dois são seguidas e ocorre um procedimento de autenticação bem-sucedido.Após a autenticação bem-sucedida, o cliente sem fio é associado à WLAN WPA2-Enterprise. Aqui está a captura de tela:

😤 Cisco Aironet Desktop Utility	y - Current Profile: WPA2-E	nterprise 🛛 🛛 🔀
Action Options Help		
Current Status Profile Management	Diagnostics	
CISCO SYSTEMS		
Profile Name:	WPA2-Enterprise	
Link Status:	Authenticated	Network Type: Infrastructure
Wireless Mode:	5 GHz 54 Mbps	Current Channel: 149
Server Based Authentication:	EAP-FAST	Data Encryption: AES
IP Address:	10.77.244.221	
Signal Strength:		Good
		Advanced

Você também pode verificar se o servidor RADIUS recebe e valida a solicitação de autenticação do cliente sem fio. Verifique os relatórios Passed Authentications e Failed Attempts no servidor ACS para fazer isso. Esses relatórios estão disponíveis em Relatórios e atividades no servidor ACS.

# Configure os dispositivos para o modo WPA2-Personal

Execute estas etapas para configurar os dispositivos para o modo de operação WPA2-Personal:

- 1. Configurar a WLAN para a Autenticação do Modo WPA2-Personal
- 2. Configurar o cliente sem fio para o modo WPA2-Personal

#### Configurar a WLAN para o Modo de Operação Pessoal WPA2

Você precisa configurar a WLAN que os clientes usarão para se conectar à rede sem fio. O SSID da WLAN para o modo WPA2-Personal será WPA2-Personal. Este exemplo atribui esta WLAN à interface de gerenciamento.

Conclua estes passos para configurar a WLAN e seus parâmetros relacionados:

- 1. Clique em **WLANs** na GUI do controlador para exibir a página WLANs.Esta página lista as WLANs que existem na controladora.
- 2. Clique em New para criar uma nova WLAN.
- Insira o nome SSID da WLAN, o nome do perfil e a ID da WLAN na página WLANs > New (WLANs > Novo). Em seguida, clique em Apply.Este exemplo usa WPA2-Personal como SSID.

						Sa <u>x</u> e Co	infiguration <u>P</u> ing	Logout   <u>R</u> efresh
CISCO	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	нецр	
WLANs	WLANs > New						< Back	Apply
WLANS	Туре	WLAN						
Advanced	Profile Name	WPA2-Per	sonal					
	WLAN SSID	WPA2-Per	sonal					

- 4. Quando você criar uma nova WLAN, a página WLAN > Edit da nova WLAN será exibida. Nesta página, você pode definir vários parâmetros específicos para esta WLAN. Isso inclui políticas gerais, políticas de segurança, políticas de QOS e parâmetros avançados.
- 5. Em General Policies (Regras gerais), marque a caixa de seleção **Status** para habilitar a WLAN.
- 6. Se você quiser que o AP transmita o SSID em seus quadros beacon, marque a caixa de seleção **SSID de broadcast**.
- 7. Clique na guia Security. Em Layer Security, escolha WPA+WPA2. Isso ativa a autenticação WPA para a

WLAN.

- ahaha					Sa <u>v</u> e Co	onfiguration 👔 Bing	Logout Befresh
cisco	MONITOR WLANS CONTR	OLLER WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
WLANs	WLANs > Edit					< Back	Apply
W HILANIA	General Security	QoS Advanced					
WLANS	Layer 2 Layer 3	AAA Servers					
Advanced							-
	Layer 2 Security WPA4	WPA2					
	□ MAC	; Filtering					
	Static WEP Parameters						
	802.11 Data Encryption	Current Key:	104 bits WE	P Static Key (Key I	ndex = 0)		
		Type Key Size	Key Index	Encryption Key	ć.	Key Format	
		WEP not set 💌	1 💌			ASCII .	
	Allow Shared Key Authentication	Enabled					_
	CKIP Parameters #						
	802.11 Data Encryption	Current Key: 0 8	its CKIP Key	(Key Index= 0)			
		Key Size Key	Index Encr	ption Key	ĸ	ey Format	
		not set 💌 1				ASCII .	
		<b></b>					<u> </u>
	<u> </u>						1 1
	Foot Notes						
	I CKIP is not supported by 10 2 Web Policy cannot be used i 3 H.REAR Local Switching in the	har model APs in combination with IPse of supported with IPse	CRANTE and	hantination			
	4 When client exclusion is end 5 Client MFP is not active unle	abled, a Timeout Value of ss WPA2 is configured	of zero means	infinity (will require	e administrative	override to reset exc	cluded clients)

- 8. Role a página para baixo para modificar os **parâmetros WPA+WPA2**.Neste exemplo, a política WPA2 e a criptografia AES estão selecionadas.
- 9. Em Auth Key Mgmt, selecione **PSK** para habilitar WPA2-PSK.
- 10. Insira a chave pré-compartilhada no campo apropriado, conforme mostrado.

ululu cisco ≝on	NITOR WLANS CONT	ROLLER WIRELESS SECURITY	Sage Co MANAGEMENT COMMANDS	HELP	Logout   <u>R</u> efresh
CISCO MON WLANS WL/ WLANS Advanced	ANS > Edit ieneral Security Layer 2 Layer 3 MMH Mode Key Permutation 802.11 Data Encryption 802.11 Data Encryption WPA+WPA2 Parameters WPA Policy WPA2 Policy WPA2 Policy WPA2 Encryption Auth Key Mgmt PSK Format CKIP is not supported by 1 When client exclusion is en	ROLLER       WIPELESS       SECURITY         QoS       Advanced         AAA Servers	Nentication	HELP < Back ey Format ASCII = override to reset excl	Apply

**Observação:** a chave pré-compartilhada usada no WLC deve corresponder à configurada nos clientes sem fio.

11. Clique em Apply.

#### Configurar o cliente sem fio para o modo WPA2-Personal

A próxima etapa é configurar o cliente sem fio para o modo de operação WPA2-Personal.

Conclua estas etapas para configurar o cliente sem fio para o modo WPA2-Personal:

- 1. Na janela Aironet Desktop Utility, clique em **Profile Management > New** para criar um perfil para o usuário WPA2-PSK WLAN.
- 2. Na janela Gerenciamento de perfil, clique na guia **Geral** e configure o Nome do perfil, o Nome do cliente e o nome SSID como mostrado neste exemplo. Em seguida, clique em **OK**.

Profile Management	? 🔀
General Security Advanc	ed
Profile Settings	
Profile Name:	WPA2-Personal
Client Name:	Wireless-Client2
Network Names	
SSID1:	WPA2-Personal
SSID2:	
SSID3:	
	OK. Cancel

3. Clique na guia **Security** e escolha **WPA/WPA2 Passphrase** para habilitar o modo de operação WPA2-PSK. Clique em **Configure** para configurar a chave pré-compartilhada WPA-

PSK.

Profile Management			? 🔀
General Security Advanced			
- Set Security Options			
○ WPA/WPA2/CCKM	WPA/WPA2/CCKM EAP Type:	LEAP	
WPA/WPA2 Passphrase			
○ 802.1x	802.1x EAP Type:	LEAP	
O Pre-Shared Key (Static WEP)			
◯ None			
Configure	Allow Association to Mixed Co Profile Locked	ella	
	Limit Time for Finding Domain	Controller To: 0	tec sec
Group Policy Delay:	60 😂 sec		
		<u> Service and a</u>	
			OK Cancel

4. Insira a chave pré-compartilhada e clique em

Configure WPA/WPA2 Passphrase	? 🔀
Enter a WPA/WPA2 passphrase (8 to 63 A	SCII or 64 hexadecimal characters)
abcdefghijkl	
	OK Cancel

#### Verificar o modo de operação WPA2-Personal

Conclua estas etapas para verificar se a configuração do modo WPA2-Enterprise está funcionando corretamente:

- 1. Na janela do Aironet Desktop Utility, selecione o perfil **WPA2-Personal** e clique em **Ativate** para ativar o perfil do cliente sem fio.
- Quando o perfil é ativado, o cliente sem fio se associa à WLAN após a autenticação bemsucedida.Aqui está a captura de tela:

🖻 Cisco Aironet Desktop Utility - Current Profile: WPA2-Personal 🛛 🔹 👔				
Action Options Help				
Current Status Profile Management	Diagnostics			
CISCO SYSTEMS				
Profile Name:	WPA2-Personal			
Link Status:	Authenticated	Network Type: Infrastructure		
Wireless Mode:	5 GHz 54 Mbps	Current Channel: 149		
Server Based Authentication:	None	Data Encryption: AES		
IP Address:	10.77.244.221			
Signal Strength:		Good		
		Advanced		

### **Troubleshoot**

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Estes comandos debug serão úteis para solucionar problemas de configuração:

Nota:Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos debug.

 debug dot1x events enable — Ativa a depuração de todos os eventos dot1x. Aqui está um exemplo de saída de depuração com base na autenticação bem-sucedida: Observação: algumas das linhas desta saída foram movidas para duas linhas devido a limitações de espaço.

```
(Cisco Controller)>debug dot1x events enable
Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Sending EAP -Request/Identity
to mobile 00:40:96:af:3e:93 (EAP Id 1)
Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Received EAPOL START from
mobile 00:40:96:af:3e:93
Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity
to mobile 00:40:96:af:3e:93 (EAP Id 2)
Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Received EAP Response packet with
mismatching id (currentid=2, eapid=1) from mobile 00:40:96:af:3e:93
Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Received Identity Response
(count=2) from mobile 00:40:96:af:3e:93
Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Processing Access-Challenge
for mobile 00:40:96:af:3e:93
.....
```

Wed Feb 20 14:20:00 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 19, EAP Type 43) Wed Feb 20 14:20:00 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:00 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 20) Wed Feb 20 14:20:01 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 20, EAP Type 43) Wed Feb 20 14:20:29 2007: Creating dot1x interface with key 00:0b:85:91:c3:c0 -0 Wed Feb 20 14:20:29 2007: Resetting the group key timer for 3689 seconds on AP 00:0b:85:91:c3:c0 Wed Feb 20 14:20:29 2007: Creating dot1x interface with key 00:0b:85:91:c3:c0 -1 Wed Feb 20 14:20:29 2007: Resetting the group key timer for 3696 seconds on AP 00:0b:85:91:c3:c0 Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received EAPOL START from mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to mobile 00:40:96:af:3e:93 (EAP Id 22) Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received Identity Response (count=3) from mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 WARNING: updated EAP-Identifer 22 ===> 19 for STA 00:40:96:af:3e:93 Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 19) Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 19, EAP Type 3) Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 20) Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 20, EAP Type 43) Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 21) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 21, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 22) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 22, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 23) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 23, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 24) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 24, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 25) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from

mobile 00:40:96:af:3e:93 (EAP Id 25, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 26) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 26, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 27) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 27, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Reject for mobile00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Failure to mobile 00:4096:af:3e:93 (EAP Id 27) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Setting quiet timer for 5 seconds for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to mobile 00:40:96:af:3e:93 (EAP Id 1) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to mobile 00:40:96:af:3e:93 (EAP Id 1) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAPOL START from mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to mobile 00:40:96:af:3e:93 (EAP Id 2) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received Identity Response (count=2) from mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 WARNING: updated EAP-Identifer 2 ===> 20 for STA 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 20) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 20, EAP Type 3) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 21) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 21, EAP Type 43) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 22) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 22, EAP Type 43) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 WARNING: updated EAP-Identifer 22 ===> 24 for STA 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 24) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 24, EAP Type 43) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 25) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 25, EAP Type 43) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Accept for

mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Creating a new PMK Cache Entry for
tation 00:40:96:af:3e:93 (RSN 0)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP-Success to
mobile 00:40:96:af:3e:93 (EAP Id 25)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending default RC4 key to
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending Key-Mapping RC4 key to
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received Auth Success while in
Authenticating state for mobile 00:40:96:af:3e:93

- debug dot1x packet enable Habilita a depuração de mensagens de pacote 802.1x.
- debug aaa events enable Ativa a saída de depuração de todos os eventos aaa.

## Informações Relacionadas

- <u>WPA2 Wi-Fi Protected Access 2</u>
- Exemplo de Autenticação EAP-FAST com Controladoras Wireless LAN e Servidor RADIUS
   Externo
- Exemplo de Configuração de Autenticação EAP com WLAN Controllers (WLC)
- <u>Visão Geral da Configuração do WPA</u>
- <u>Suporte de produtos Wireless</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.