Configurar 802.1x - PEAP com FreeRadius e WLC 8.3

Contents

Introduction **Prerequisites** Requirements **Componentes Utilizados** Configurar Diagrama de Rede Instalar o servidor httpd e o MariaDB Instalar o PHP 7 no CentOS 7 Instalar FreeRADIUS **FreeRADIUS** WLC como Cliente de Autenticação, Autorização e Contabilidade (AAA - Authentication, Authorization, and Accounting) em FreeRADIUS FreeRADIUS como servidor RADIUS na WLC **WLAN** Adicionar usuários ao banco de dados RADIUS gratuito Certificados em freeRADIUS Configuração do dispositivo final Importar certificado RADIUS gratuito Criar perfil de WLAN Verificar Processo de autenticação em WLC Troubleshoot

Introduction

Este documento descreve como configurar uma rede local sem fio (WLAN) com segurança 802.1x e PEAP (Protected Extensible Authentication Protocol) como EAP (Extensible Authentication Protocol). FreeRADIUS é usado como o servidor RADIUS (Remote Authentication Dial-In User Service) externo.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento básico sobre estes tópicos:

- Linux
- editor de Vim
- Controladores LAN sem fio (WLCs) AireOS

Observação: este documento tem como objetivo dar aos leitores um exemplo de configuração necessária em um servidor RADIUS gratuito para autenticação PEAP-MS-CHAPv2. A configuração do servidor freeRADIUS apresentada neste documento foi testada no laboratório e foi encontrada para funcionar como esperado. O Cisco Technical Assistance Center (TAC) não oferece suporte à configuração de servidor RADIUS gratuito.

Componentes Utilizados

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

- CentOS7 ou Red Hat Enterprise Linux 7 (RHEL7) (recomendado 1 GB de RAM e pelo menos 20 GB de HDD)
- WLC 5508 v8.3
- MariaDB (MySQL)
- FreeRADIUS
- PHP 7

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.

Configurar

Diagrama de Rede



Instalar o servidor httpd e o MariaDB

Etapa 1. Execute estes comandos para instalar o servidor httpd e o MariaDB.

[root@tac-mxwireless ~]# yum -y update [root@tac-mxwireless ~]# yum -y groupinstall "Development Tools" [root@tac-mxwireless ~]# yum -y install httpd httpd-devel mariadb-server mariadb Etapa 2. Inicie e habilite o httpd (Apache) e o servidor MariaDB.

[root@tac-mxwireless ~]# systemctl enable httpd [root@tac-mxwireless ~]# systemctl start httpd [root@tac-mxwireless ~]# systemctl start mariadb [root@tac-mxwireless ~]# systemctl enable mariadb

Etapa 3. Defina as configurações iniciais de MariaDB para protegê-la.

[root@tac-mxwireless ~] #mysql_secure_installation

Note: Executar todas as partes deste script. É recomendado para todos os servidores MariaDB em uso de produção. Leia cada etapa cuidadosamente.

In order to log into MariaDB to secure it, we'll need the current password for the root user. If you've just installed MariaDB, and you haven't set the root password yet, the password will be blank, so you should just press enter here.

Enter current password for root (enter for none): OK, successfully used password, moving on...

Setting the root password ensures that nobody can log into the MariaDB root user without the proper authorisation.

Set root password? [Y/n] Y New password: Re-enter new password: Password updated successfully! Reloading privilege tables.. ... Success! By default, a MariaDB installation has an anonymous user, allowing anyone to log into MariaDB without having to have a user account created for them. This is intended only for testing, and to make the installation go a bit smoother. You should remove them before moving into a production environment. Remove anonymous users? [Y/n] y ... Success! Normally, root should only be allowed to connect from 'localhost'. This ensures that someone cannot guess at the root password from the network. Disallow root login remotely? [Y/n] y ... Success! By default, MariaDB comes with a database named 'test' that anyone can access. This is also intended only for testing, and should be removed before moving into a production environment. Remove test database and access to it? [Y/n] y - Dropping test database... ... Success! - Removing privileges on test database... ... Success! Reloading the privilege tables will ensure that all changes made so far will take effect immediately. Reload privilege tables now? [Y/n] y ... Success! Cleaning up... All done! If you've completed all of the above steps, your MariaDB installation should now be secure. Thanks for using MariaDB! Etapa 4. Configure o banco de dados para freeRADIUS (use a mesma senha configurada na Etapa 3).

[root@tac-mxwireless ~]# mysql -u root -p -e "CREATE DATABASE radius" [root@tac-mxwireless ~]# mysql -u root -p -e "show databases" [root@tac-mxwireless ~]# mysql -u root -p MariaDB [(none)]> GRANT ALL ON radius.* TO radius@localhost IDENTIFIED BY "radiuspassword"; MariaDB [(none)]> FLUSH PRIVILEGES; MariaDB [(none)]> \q Bye

Instalar o PHP 7 no CentOS 7

Etapa 1. Execute estes comandos para instalar o PHP 7 em CentOS7.

```
[root@tac-mxwireless ~]# cd ~
[root@tac-mxwireless ~]# curl 'https://setup.ius.io/' -o setup-ius.sh
[root@tac-mxwireless ~]# sudo bash setup-ius.sh
[root@tac-mxwireless ~]# sudo yum remove php-cli mod_php php-common
[root@tac-mxwireless ~]# sudo yum -y install mod_php70u php70u-cli php70u-mysqlnd php70u-devel
php70u-gd php70u-mcrypt php70u-mbstring php70u-xml php70u-pear
[root@tac-mxwireless ~]# sudo apachectl restart
```

Instalar FreeRADIUS

Etapa 1. Execute este comando para instalar o FreeRADIUS.

[root@tac-mxwireless ~]# yum -y install freeradius freeradius-utils freeradius-mysql freeradiussqlite

Etapa 2. Faça o radius.service começar após mariadb.service.

Execute este comando:

[root@tac-mxwireless ~]# vim /etc/systemd/system/multi-user.target.wants/radiusd.service
Adicione uma linha na seção [unidade]:

After=mariadb.service

A seção [Unidade] deve ser semelhante a esta:

[Unit] Description=FreeRADIUS high performance RADIUS server. After=syslog.target network.target After=mariadb.service

Etapa 3. Inicie e ative o freeradius para iniciar na inicialização.

[root@tac-mxwireless ~]# systemctl start radiusd.service [root@tac-mxwireless ~]# systemctl enable radiusd.service

Etapa 4. Habilite firewalld para segurança.

```
[root@tac-mxwireless ~]# systemctl enable firewalld
[root@tac-mxwireless ~]# systemctl start firewalld
[root@tac-mxwireless ~]# systemctl status firewalld
```

Etapa 5. Adicione regras permanentes à zona padrão para permitir serviços http, https e radius.

[root@tac-mxwireless ~]# firewall-cmd --get-services | egrep 'http|https|radius'
[root@tac-mxwireless ~]# firewall-cmd --add-service={http,https,radius} --permanent success
Etapa 6. Recarregue o firewall para que as alterações entrem em vigor.

[root@tac-mxwireless ~]# firewall-cmd --reload

FreeRADIUS

Para configurar o FreeRADIUS para usar MariaDB, siga estas etapas.

Etapa 1. Importe o esquema de banco de dados RADIUS para preencher o banco de dados

RADIUS.

```
[root@tac-mxwireless ~]# mysql -u root -p radius < /etc/raddb/mods-
config/sql/main/mysql/schema.sql
Etapa 2. Crie um soft link para Structured Query Language (SQL) em /etc/raddb/mods ativado.
```

```
[root@tac-mxwireless ~]# ln -s /etc/raddb/mods-available/sql /etc/raddb/mods-enabled/
Etapa 3. Configure o módulo SQL /raddb/mods-available/sql e altere os parâmetros de conexão
do banco de dados para direcionar seu ambiente.
```

[root@tac-mxwireless ~]# vim /etc/raddb/mods-available/sql
A seção SQL deve ser semelhante a esta.

```
sql {
    driver = "rlm_sql_mysql"
    dialect = "mysql"
    # Connection info:
    server = "localhost"
    port = 3306
    login = "radius"
    password = "radpass" # Database table configuration for everything except Oracle radius_db =
    "radius" } # Set to `yes' to read radius clients from the database (`nas' table) # Clients will
    ONLY be read on server startup. read_clients = yes # Table to keep radius client info
    client_table = "nas"
```

Etapa 4. Altere o direito do grupo de /etc/raddb/mods-enabled/sql para radiusd.

[root@tac-mxwireless ~]# chgrp -h radiusd /etc/raddb/mods-enabled/sql

WLC como cliente de Autenticação, Autorização e Contabilidade (AAA) no FreeRADIUS

Etapa 1. Edite /etc/raddb/clients.conf para definir a chave compartilhada para WLC.

[root@tac-mxwireless ~]# vim /etc/raddb/clients.conf Etapa 2. Na parte inferior, adicione o endereço ip do controlador e a chave compartilhada.

client{ secret = shortname = }

FreeRADIUS como servidor RADIUS na WLC

GUI:

Etapa 1. Abra a GUI do WLC e navegue até SECURITY > RADIUS > Authentication > New

(SEGURANÇA > RADIUS > Autenticação > Novo) como mostrado na imagem.



Etapa 2. Preencha as informações do servidor RADIUS conforme mostrado na imagem.

RADIUS Authentication Servers > New								
Server Index (Priority)	2 ~	_						
Server IP Address(Ipv4/Ipv6)	a.b.c.d							
Shared Secret Format	ASCII 🗸							
Shared Secret	•••••							
Confirm Shared Secret	•••••							
Key Wrap	□ (Designed fo	r FIPS customers and requires a key wrap compliant RADIUS server)						
Port Number	1812							
Server Status	Enabled \sim							
Support for CoA	Disabled \vee							
Server Timeout	10 seconds							
Network User	🗹 Enable							
Management	🗹 Enable							
Management Retransmit Timeout	2 seconds							
IPSec	Enable							

CLI:

> config radius auth add <index> <radius-ip-address> 1812 ascii <shared-key>
> config radius auth disable <index>
> config radius auth retransmit-timeout <index> <timeout-seconds>
> config radius auth enable <index>
WLAN

GUI:

Etapa 1. Abra a GUI do WLC e navegue até WLANs > Create New > Goas mostradas na imagem.

ıı ııı ı، cısco	<u>M</u> ONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	W <u>I</u> RELESS	<u>s</u> ecurity	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HE <u>L</u> P	<u>F</u> EEDBACK	
WLANs	WLANs									
 ₩LANS WLANS Advanced 	Current Filt	be r: Nor	ne [<u>Cha</u>	<u>nge Filter] [Cl</u>	<u>ear Filter]</u>		[Create Ne	ew 🗸	Go

Etapa 2. Escolha um nome para o SSID (Service Set Identifier) e o perfil e clique em Aplicar como

mostrado na imagem.

WLANs > New		< Back	Apply
Туре	WLAN \vee		
Profile Name	profile-name		
SSID	SSID-name		
ID	2 ~		

CLI:

> config wlan create <id> <profile-name> <ssid-name>

Etapa 3. Atribua o servidor RADIUS à WLAN.

CLI:

> config wlan radius_server auth add <wlan-id> <radius-index> $\ensuremath{\mathsf{GUI}}$:

Navegue até **Security > AAA Servers** e escolha o servidor RADIUS desejado; em seguida, clique em **Apply** como mostrado na imagem.

WLANs > Edit 'ise-prof'	< Back	Apply
General Security QoS Policy-Mapping Advanced		
Layer 2 Layer 3 AAA Servers		
		^
Select AAA servers below to override use of default servers on this WLAN		
RADIUS Servers		
RADIUS Server Overwrite interface Enabled		
Authentication Servers Accounting Servers EAP Parameters		
🗹 Enabled Enable 🗌		
Server 1 IP:172.16.15.8, Port:1812 V None V		
Server 2 None V None V		
Server 3 None V None V		
Server 4 None V None V		
Server 5 None V None V		
Server 6 None V None V		
RADIUS Server Accounting		
Interim Update 🗹 Interim Interval 0 Seconds		~
<)	•

Etapa 4. Como opção, aumente o tempo de sessão.

> config wlan session-timeout <wlan-id> <session-timeout-seconds> $\ensuremath{\mathsf{GUI}}$:

Navegue até Advanced > Enable Session Timeout > clique em Apply, como mostrado na imagem.

WL	ANs > Edit	'ise-pro	of'						< Back	Apply	
G	eneral	Security	QoS	Policy-Mapping	Adva	nced					
	Allow AAA (Override	Enabled	1		DHCP				Â	
	Coverage H Detection	Hole	🗹 Enabled	1		рнс	P Server	Ov	erride		
	Enable Ses Timeout	sion	⊠ 2880 Ses	o sion Timeou (secs)		DHC Assi	P Addr. gnment	🗌 Re	quired		
	Aironet IE		Enabled			OEAP					
	Diagnostic <u>18</u>	Channel	Enabled			Spli	t Tunnel	🗌 Enal	bled		
	Override Ir ACL	nterface	IPv4 None		Pv6 None ∨	Manage	ment Frame Prot	ection (M	IFP)		
	Layer2 Ad		None 🖂								
	URL ACL		None 🗸			MFP	Client Protection 5	d Option	nal 🗸		
	P2P Blockir	ng Action	Disabled	~		DTIM P	eriod (in beacon ir	ntervals)			
	Client Exclu	usion ³	☑ Enabled 60 Tir	meout Value (secs)		802.	11a/n (1 - 255)	1			
	Maximum . Clients <mark>ª</mark>	Allowed	0			802. NAC	11b/g/n (1 - 255)) 1			
<	Static IP Tu	unneling	-			NAC	State None	$\overline{}$		>	

Etapa 5. Ativar a WLAN.

CLI:

>	config	wlan	enable	<wlan-id></wlan-id>
G	UI:			

Navegue até General > Status > Tick Enabled > Clique em Apply como mostrado na imagem.

ANs > Edit 'ssid-	name'	< Back
ieneral Security	QoS Policy-Mapping Advanced	
Profile Name	ssid-name	
Туре	WLAN	
SSID	ssid-name	
Status	Enabled	

Adicionar usuários ao banco de dados RADIUS gratuito

Por padrão, os clientes usam protocolos PEAP, no entanto, o freeRadius suporta outros métodos (não abordados neste guia).

Etapa 1. Edite o arquivo /etc/raddb/users.

[root@tac-mxwireless ~]# nano /etc/raddb/users

Etapa 2. Na parte inferior do arquivo, anexe as informações do usuário. Neste exemplo, **user1** é o nome de usuário e **Cisco123** a senha.

user1 Cleartext-Password := <Cisco123>

Etapa 3. Reinicie o FreeRadius.

[root@tac-mxwireless ~]# systemctl restart radiusd.service

Certificados em freeRADIUS

O FreeRADIUS vem com um certificado padrão de autoridade de certificação (CA) e um certificado de dispositivo que estão armazenados no caminho /etc/raddb/certs. O nome desses certificados é ca.pem e server.pem. server.pem é o certificado que os clientes recebem enquanto passam pelo processo de autenticação. Se precisar atribuir um certificado diferente para autenticação EAP, basta excluí-los e salvar os novos no mesmo caminho com exatamente o mesmo nome.

Configuração do dispositivo final

Configure uma máquina Windows de laptop para se conectar a um SSID com autenticação 802.1x e PEAP/MS-CHAP (versão Microsoft do Challenge-Handshake Authentication Protocol) versão 2.

Para criar o perfil da WLAN na máquina Windows, há duas opções:

- 1. Instale o certificado autoassinado na máquina para validar e confiar no servidor RADIUS livre para concluir a autenticação
- Ignore a validação do servidor RADIUS e confie em qualquer servidor RADIUS usado para executar a autenticação (não recomendado, pois pode se tornar um problema de segurança). A configuração dessas opções é explicada na configuração do dispositivo final -Criar o perfil de WLAN.

Importar certificado RADIUS gratuito

Se você usar os certificados padrão instalados em freeRADIUS, siga estas etapas para importar o certificado EAP do servidor freeRADIUS para o dispositivo final.

Etapa 1. Obtenha o certificado do FreeRadius:

```
----BEGIN CERTIFICATE----
MIIE4TCCA8mgAwIBAgIJAKLmHn4eZLjBMA0GCSqGSIb3DQEBBQUAMIGTMQswCQYD
VQQGEwJGUjEPMA0GA1UECBMGUmFkaXVzMRIwEAYDVQQHEwlTb21ld2hlcmUxFTAT
BgNVBAoTDEV4YW1wbGUgSW5jLjEgMB4GCSqGSIb3DQEJARYRYWRtaW5AZXhhbXBs
ZS5jb20xJjAkBgNVBAMTHUV4YW1wbGUgQ2VydG1maWNhdGUgQXV0aG9yaXR5MB4X
{\tt DTE3MDMzMTExMTIxNloXDTE3MDUzMDExMTIxNlowgZMxCzAJBgNVBAYTAkZSMQ8w}
DQYDVQQIEwZSYWRpdXMxEjAQBqNVBAcTCVNvbWV3aGVyZTEVMBMGA1UEChMMRXhh
bXBsZSBJbmMuMSAwHqYJKoZIhvcNAQkBFhFhZG1pbkBleGFtcGxlLmNvbTEmMCQG
A1UEAxMdRXhhbXBsZSBDZXJ0aWZpY2F0ZSBBdXRob3JpdHkwqqEiMA0GCSqGSIb3
DQEBAQUAA4IBDwAwggEKAoIBAQC0vJ53NN7J9vhpKhcB3B00XLpeQFWjqolQOB9F
/8Lh2Hax2rzb9wxOi1MOyXR+kN22H7RNwUHET8VdyGUsA4OdZWuyzI8sKi5H42GU
Eu6GDw1YJvhHn4rVC360ZU/Nbaxj0eR8ZG0JGse4ftQKLfckkvCOS5QGn4X1elRS
oFe27HRF+pTDHd+nzbaDvhYWvFoe6iA27Od7AY/sDuo/tiIJWGdm9ocPz3+0IiFC
ay6dtG55YQOHxKaswH7/HJkLsKWhS4YmXLgJXCeeJqooqr+TEwyCDEaFaiX835Jp
gwNNZ7X5US0Fcjuu0tpJJ3hfQ8K6uXjEWP0kDE0DAnqp4/n9AgMBAAGjggE0MIIB
MDAdBgNVHQ4EFgQUysFNRZKpAlcFCEgwdOPVGV0waLEwgcgGA1UdIwSBwDCBvYAU
ysFNRZKpAlcFCEgwdOPVGV0waLGhgZmkgZYwgZMxCzAJBgNVBAYTAkZSMQ8wDQYD
VQQIEwZSYWRpdXMxEjAQBqNVBAcTCVNvbWV3aGVyZTEVMBMGA1UEChMMRXhhbXBs
ZSBJbmMuMSAwHqYJKoZIhvcNAQkBFhFhZG1pbkBleGFtcGx1LmNvbTEmMCQGA1UE
AxMdRXhhbXBsZSBDZXJ0aWZpY2F0ZSBBdXRob3JpdHmCCQCi5h5+HmS4wTAMBgNV
HRMEBTADAQH/MDYGA1UdHwQvMC0wK6ApoCeGJWh0dHA6Ly93d3cuZXhhbXBsZS5j
b20vZXhhbXBsZV9jYS5jcmwwDQYJKoZIhvcNAQEFBQADggEBACsPR2jiOFXnTsK4
1wnrrMy1ZZb12gDuqK+zKELox2mz1DMMK83tBsL8yjkv70KeZn821IzfTrTfvhzV
mjX6HgaWfYyMjYYYSw/iEu2JsAtQdpvC3di10nGwVPHlzbozPdov8cZtCb21ynfY
Z6cNjx8+aYQIcsRIyqA11XMOBwIXo141TOmoODdgfX951poLwgktRLkv17Y7owsz
ChYDO++H7Iewsxx5pQfm56dA2cNrlTwWtMvViKyX7GlpwlbB0xgkLiFJ5+GFbfLh
a0HBHZWhTKvffbr62mkbfjCUfJU4T3xgY9zFwiwT+BetCJgAGy8CT/qmnO+NJERO
RUvDhfE=
```

----END CERTIFICATE-----

Etapa 2. Copie e cole a saída da etapa anterior em um arquivo de texto e altere a extensão para .crt

Etapa 3. Clique duas vezes no arquivo e selecione **Instalar certificado...** conforme mostrado na imagem.

Certificate 🔀
General Details Certification Path
Certificate Information
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.
Issued to: Example Certificate Authority
Issued by: Example Certificate Authority
Valid from 3/ 31/ 2017 to 5/ 30/ 2017
Install Certificate Issuer Statement
ОК

Etapa 4. Instale o certificado no repositório das Autoridades de Certificação Raiz Confiáveis conforme mostrado na imagem.

Certificate Import Wizard	8
Certificate Store Certificate stores are system areas where certific	ates are kept.
Windows can automatically select a certificate sto the certificate.	are, or you can specify a location for ased on the type of certificate
Place all certificates in the following store	
Certificate store:	Browse
Select Certificate Store	
Select the certificate store you want to use.	
Personal Trusted Root Certification Authorities Enterprise Trust Intermediate Certification Authorities Trusted Publishers Untrusted Certificates Show physical stores	Back Next > Cancel
OK Cancel	ок

Criar perfil de WLAN

Etapa 1. Clique com o botão direito do mouse no ícone Iniciar e selecione **Painel de controle** conforme mostrado na imagem.

Programs and Features
Mobility Center
Power Options
Event Viewer
System
Device Manager
Network Connections
Disk Management
Computer Management
Command Prompt
Command Prompt (Admin)
Task Manager
Control Panel
File Explorer
Search
Run
Shut down or sign out
Desktop
👔 אין

Etapa 2. Navegue até **Rede e Internet > Central de Rede e Compartilhamento > clique em Configurar uma nova conexão ou rede** conforme mostrado na imagem.



Etapa 3. Selecione Conectar manualmente a uma rede sem fio e clique em Nextas na imagem.

	-		×
🔶 👙 Set Up a Connection or Network			
Choose a connection option			
Connect to the Internet Set up a broadband or dial-up connection to the Internet.			
Set up a new network Set up a new router or access point.			
Manually connect to a wireless network Connect to a hidden network or create a new wireless profile.			
Set up a dial-up or VPN connection to your workplace.			
	Next	Car	vcel
L	THEMA	Car	

Etapa 4. Insira as informações com o nome do SSID e o tipo de segurança WPA2-Enterprise e clique em **Avançar** conforme mostrado na imagem.

←	Se Manually connect to	a wireless network	-		×
	Enter information	or the wireless network you want to add			
	Network name:	SSID-name			
	Security type:	WPA2-Enterprise ~			
	Encryption type:	AES			
	Security Key:	Hide characte	HTS.		
	Start this connecti	on automatically			
	Connect even if th Warning: If you se	e network is not broadcasting lect this option, your computer's privacy might be at ris	k.		
			Vext	Can	cel

Etapa 5. Selecione **Alterar configurações de conexão** para personalizar a configuração do perfil da WLAN como mostrado na imagem.

	-		\times
 Manually connect to a wireless network 			
Successfully added ise-ssid			
→ Change connection settings			
Open the connection properties so that I can change the settings.			
		Ck	ose

Etapa 6. Navegue até a guia **Segurança** e clique em **Configurações** conforme mostrado na imagem.

ise-ssid Wireless Network Properties		×		
Connection Security				
Security type:	WPA2-Enterprise		\sim	
Encryption type:	AES		\sim	
Choose a network aut	hentication method:	_	_	
Microsoft: Protected I	EAP (PEAP)	Settin	igs	
Remember my cre time I'm logged or	dentials for this conne n	ction each		
Advanced settings				
		ОК	Car	ncel

Passo 7. Escolha se o servidor RADIUS é validado ou não.

Em caso afirmativo, ative Verify the server's identity by validation the certificate and from Trusted Root Certification Authority: selecione o certificado autoassinado de freeRADIUS.

Depois disso, selecione **Configurar** e desativar **Usar automaticamente meu nome de logon e senha do Windows...** e clique em **OK** como mostrado nas imagens.

Protected EAP Properties	×
When connecting:	
Verify the server's identity by validating the certificate	
Connect to these servers (examples:srv1;srv2;.*\.srv3\.com):	
Trusted Root Certification Authorities:	
Equility & Oethol Index and Equility of State Associated and Index and Equility of State Associated and Index and Equility of the state of the s	^
Example Certification Authority	
 I an alternal Laternalistic Soft that (2000) E. J. S. Son of Contents of Soft Soft Soft Soft Soft Soft Soft S	~
< >	
Notifications before connecting: Tell user if the server name or root certificate isn't specified	~
Select Authentication Method:	
Secured password (EAP-MSCHAP v2) Configur	re
Enable Fast Reconnect	_
Disconnect if server does not present cryptobinding TLV	
Enable Identity Privacy	
OK Cano	el
EAP MSCHAPv2 Properties X	
,	
When connecting:	
Automatically use my Windows logon name and password (and domain if any).	

Etapa 8. Configure as credenciais do usuário.

Cancel

ΟK

Depois de voltar à guia Segurança, selecione **Configurações avançadas**, especifique o modo de autenticação como **autenticação do usuário** e salve as credenciais configuradas em freeRADIUS para autenticar o usuário, como mostrado nas imagens.

ise-ssid Wireless Ne	twork Propertie	s	×
Connection Security			
Security type:	WPA2-Enterprise		~
Encryption type:	AES		\sim
Choose a network au	thentication method:		
Microsoft: Protected	EAP (PEAP)	Settin	gs
Remember my cro	edentials for this con	nection each	
une in ogged o			
Advanced settings	•		
		OK	Cancel

Advanced settings		×
802.1X settings 802.11 settings		
Specify authentication mode:		
User authentication	V Save c	rodontiak
Delete credentials for all use	ers	
Enable single sign on for this ne	twork	
Perform immediately before	user logon	
O Perform immediately after u	iser logon	
Maximum delay (seconds):	10	*
Allow additional dialogs to b sign on	e displayed during	single
This network uses separate and user authentication	virtual LANs for m	achine
	ОК	Cancel
Windows Security		
Save credentials		
Saving your gradentials allow		uter to connect to the notice
when you're not logged on	(for example,	to download updates).

.1 1.1 1. cisco	user1	

 \times

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Processo de autenticação em WLC

Execute os próximos comandos para monitorar o processo de autenticação de um usuário específico:

```
> debug client <mac-add-client>
> debug dot1x event enable
> debug dot1x aaa enable
```

Para uma maneira fácil de ler as saídas do debug client, use a ferramenta Wireless debug analyzer:

Analisador de depuração sem fio

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.