Configure 802.1x - PEAP con FreeRadius y WLC 8.3

Contenido

Introducción **Prerequisites** Requirements **Componentes Utilizados** Configurar Diagrama de la red Instalar el servidor httpd y MariaDB Instalación de PHP 7 en CentOS 7 Instalar FreeRADIUS **FreeRADIUS** WLC como cliente de autenticación, autorización y contabilidad (AAA) en FreeRADIUS FreeRADIUS como servidor RADIUS en WLC **WLAN** Agregar usuarios a base de datos de RADIUS libre Certificados en freeRADIUS Configuración del dispositivo final Importar certificado FreeRADIUS **Crear perfil WLAN** Verificación Proceso de autenticación en WLC **Troubleshoot**

Introducción

Este documento describe cómo configurar una red de área local inalámbrica (WLAN) con seguridad 802.1x y protocolo de autenticación extensible protegido (PEAP) como protocolo de autenticación extensible (EAP). FreeRADIUS se utiliza como servidor RADIUS (servicio de usuario de acceso telefónico de autenticación remota externa).

Prerequisites

Requirements

Cisco recomienda que tenga conocimientos básicos sobre estos temas:

- Linux
- editor Vim
- Controladores LAN inalámbricos (WLC) AireOS

Nota: Este documento está diseñado para dar a los lectores un ejemplo sobre la configuración requerida en un servidor FreeRADIUS para la autenticación PEAP-MS-CHAPv2. La configuración del servidor freeRADIUS que se presenta en este documento se ha probado en el laboratorio y se ha encontrado que funciona según lo esperado. El centro de asistencia técnica Cisco Technical Assistance Center (TAC) no admite la configuración del servidor RADIUS libre.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- CentOS7 o Red Hat Enterprise Linux 7 (RHEL7) (RAM recomendada de 1 GB y HDD de al menos 20 GB)
- 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 la red



Paso 1. Ejecute estos comandos para instalar el servidor httpd y 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
Paso 2. Inicie y active httpd (Apache) y el 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
Paso 3. Configure la configuración inicial de MariaDB para protegerla.

[root@tac-mxwireless ~]#mysql_secure_installation

Nota: Ejecute todas las partes de este script. Se recomienda para todos los servidores MariaDB en uso de producción. Lea atentamente cada paso.

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! Paso 4. Configure la base de datos para freeRADIUS (utilice la misma contraseña configurada en el paso 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

Instalación de PHP 7 en CentOS 7

[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

Paso 1. Ejecute este comando para instalar FreeRADIUS.

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

Paso 2. Haga que radius.service comience después de mariadb.service.

Ejecute este comando:

[root@tac-mxwireless ~]# vim /etc/systemd/system/multi-user.target.wants/radiusd.service
Agregue una línea en la sección [unidad]:

After=mariadb.service

La sección [Unit] debe tener el siguiente aspecto:

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

Paso 3. Inicie y active freeradius para que se inicie al arrancar.

[root@tac-mxwireless ~]# systemctl start radiusd.service [root@tac-mxwireless ~]# systemctl enable radiusd.service Paso 4. Habilite el firewall para la seguridad.

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

Paso 5. Agregue reglas permanentes a la zona predeterminada para permitir los servicios http, https y radius.

[root@tac-mxwireless ~]# firewall-cmd --get-services | egrep 'http|https|radius'
[root@tac-mxwireless ~]# firewall-cmd --add-service={http,https,radius} --permanent success
Paso 6. Recarga el firewall para que los cambios surtan efecto.

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

FreeRADIUS

Para configurar FreeRADIUS para utilizar MariaDB, siga estos pasos.

Paso 1. Importe el esquema de base de datos RADIUS para rellenar la base de datos RADIUS.

```
[root@tac-mxwireless ~]# mysql -u root -p radius < /etc/raddb/mods-
config/sql/main/mysql/schema.sql
Paso 2. Cree un enlace programable para lenguaje de consulta estructurado (SQL) en
/etc/raddb/mods-enabled.
```

```
[root@tac-mxwireless ~]# ln -s /etc/raddb/mods-available/sql /etc/raddb/mods-enabled/
Paso 3. Configure el módulo SQL /raddb/mods-available/sql y cambie los parámetros de conexión
de la base de datos para ajustar su entorno.
```

[root@tac-mxwireless ~]# vim /etc/raddb/mods-available/sql La sección SQL debe tener un aspecto similar a este.

 $sql {$

```
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"
```

Paso 4. Cambie el derecho de grupo de /etc/raddb/mods-enabled/sql a radiusd.

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

WLC como Cliente de Autenticación, Autorización y Contabilización (AAA) en FreeRADIUS

Paso 1. Edite /etc/raddb/clients.conf para establecer la clave compartida para el WLC.

[root@tac-mxwireless ~]# vim /etc/raddb/clients.conf
Paso 2. En la parte inferior, agregue la dirección ip del controlador y la clave compartida.

client{ secret = shortname = }

FreeRADIUS como servidor RADIUS en WLC

GUI:

Paso 1. Abra la GUI del WLC y navegue hasta **SECURITY > RADIUS > Authentication > New** como se muestra en la imagen.

սիսիս		Saye Configuration <u>P</u> ing Logout <u>R</u> efresh
cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK	<mark>∩</mark> <u>H</u> ome
Security	RADIUS Authentication Servers	Apply New
▼ AAA General	Auth Called Station ID Type 🛛 🗛 MAC Address:SSID 🚽	
 RADIUS Authentication 	Use AES Key Wrap 🗌 (Designed for FIPS customers and requires a key wrap compliant RADIUS server)	
Accounting Fallback	MAC Delimiter Hyphen \vee	
DNS	Framed MTU 1300	

Paso 2. Complete la información del servidor RADIUS como se muestra en la imagen.

RADIUS Authentication Serv	vers > New	
Server Index (Priority)	2 ~	
Server IP Address(Ipv4/Ipv6)	a.b.c.d	
Shared Secret Format	ASCII 🗸	1
Shared Secret	•••••	
Confirm Shared Secret	•••••	
Key Wrap	(Designed for	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:

Paso 1. Abra la GUI del WLC y navegue hasta **WLANs > Create New >** Goas mostradas en la imagen.

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs	WLANS
 WLANS WLANS Advanced 	Current Filter: None [Change Filter] [Clear Filter] Create New Create New

Paso 2. Elija un nombre para el identificador de conjunto de servicios (SSID) y el perfil y, a continuación, haga clic en Aplicaciones mostradas en la imagen.

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

CLI:

> config wlan create <id> <profile-name> <ssid-name>
Paso 3. Asigne el servidor RADIUS a la WLAN.

CLI:

Navegue hasta **Seguridad > Servidores AAA** y elija el servidor RADIUS deseado, luego haga clic en **Aplicar** como se muestra en la imagen.

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		
Authoptication Service: Accounting Service: FAD Department		
Finabled Penabled Finabled		
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		
Server 5 None V None V		
Server 6 None V None V		
RADIUS Server Accounting		
Interim Update 🔽 Interim Interval 0 Seconds		~
<	2	>

Paso 4. Opcionalmente, aumente el tiempo de sesión.

CLI:

>	config	wlan	session-	-timeout	<wlan-id></wlan-id>	<session-timeout-seconds></session-timeout-seconds>
G	SUI:					

Navegue hasta **Avanzado > Activar Tiempo de Espera de Sesión >** haga clic en **Aplicar** como se muestra en la imagen.

WL	ANs > Edit	t 'ise-pro	of'						< Back	Apply
-	General	Security	QoS	Policy-Mapping	Adva	inced				
	Allow AAA (Override	Enabled	ł		DHCP				
	Coverage I Detection	Hole	🗹 Enabled	ł		DHC	P Server	0	verride	
	Enable Ses Timeout	ssion	⊠ 2880 Ses:	o sion Timeou (secs)		DHC Assi	P Addr. gnment	R	equired	
	Aironet IE		Enabled			OEAP				
	Diagnostic <u>18</u>	Channel	Enabled			Spli	t Tunnel	🗌 En i	abled	
	Override II ACL	nterface	IPv4 None		IPv6 None ∨	Manage	ement Frame P	Protection (MFP)	
	Layer2 Ad		None 🖂							
	URL ACL		None 🗸			MFP	Client Protectio	on 🛃 🛛 Optic	onal 🗸	
	P2P Blocki	ng Action	Disabled	~		DTIM P	eriod (in beaco	on intervals)	
	Client Excl	usion ²	⊡ Enabled Tir	meout Value (secs)]	802.	11a/n (1 - 255	5) 1		
	Maximum Clients <mark>8</mark>	Allowed	0			802. NAC	11b/g/n (1 - 2	:55) 1		
<	Static IP To	unneling	m			NAC	State None	\sim		> ×

Paso 5. Habilite la WLAN.

CLI:

```
> config wlan enable <wlan-id>
GUI:
```

Vaya a General > Status > Tick Enabled > Click Apply como se muestra en la imagen.

								< Back
QoS Policy-Mapping A	Advanced							
	_							
ssid-name								
WLAN								
ssid-name								
Enabled								
	QoS Policy-Mapping ssid-name WLAN ssid-name @ Enabled	QoS Policy-Mapping Advanced ssid-name WLAN ssid-name Image: Constraint of the state of	QoS Policy-Mapping Advanced ssid-name WLAN ssid-name Image: Constraint of the state of	QoS Policy-Mapping Advanced ssid-name WLAN ssid-name Image: Contract of the second sec	QoS Policy-Mapping Advanced ssid-name WLAN ssid-name @ Enabled	QoS Policy-Mapping Advanced ssid-name WLAN ssid-name Imabled	QoS Policy-Mapping Advanced ssid-name WLAN ssid-name Imabled	QoS Policy-Mapping Advanced ssid-name

Agregar usuarios a base de datos de RADIUS libre

De forma predeterminada, los clientes utilizan protocolos PEAP, sin embargo freeRadius admite otros métodos (no incluidos en esta guía).

Paso 1. Edite el archivo /etc/raddb/users.

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

Paso 2. En la parte inferior del archivo, añada la información de los usuarios. En este ejemplo, **user1** es el nombre de usuario y **Cisco123** la contraseña.

user1 Cleartext-Password := <Cisco123> Paso 3. Reinicie FreeRadius.

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

Certificados en freeRADIUS

FreeRADIUS incluye un certificado predeterminado de la Autoridad de certificación (CA) y un certificado de dispositivo que se almacenan en la ruta /etc/raddb/certs. El nombre de estos certificados es ca.pem y server.pem. server.pem es el certificado que los clientes reciben mientras pasan por el proceso de autenticación. Si necesita asignar un certificado diferente para la autenticación EAP, simplemente puede eliminarlos y guardar los nuevos en la misma ruta con el mismo nombre exacto.

Configuración del dispositivo final

Configure un equipo portátil Windows para conectarse a un SSID con autenticación 802.1x y PEAP/MS-CHAP (versión de Microsoft del Protocolo de autenticación por desafío mutuo) versión 2.

Para crear el perfil WLAN en el equipo de Windows hay dos opciones:

- 1. Instale el certificado autofirmado en el equipo para validar y confiar en el servidor freeRADIUS para completar la autenticación
- 2. Omita la validación del servidor RADIUS y confíe en cualquier servidor RADIUS utilizado para realizar la autenticación (no recomendado, ya que puede convertirse en un problema de seguridad). La configuración de estas opciones se explica en End device configuration Create the WLAN Profile (Configuración del dispositivo final Crear el perfil WLAN).

Importar certificado FreeRADIUS

Si utiliza los certificados predeterminados instalados en freeRADIUS, siga estos pasos para importar el certificado EAP del servidor freeRADIUS al dispositivo final.

Paso 1. Obtenga el certificado de FreeRadius:

[root@tac-mxwireless ~]# cat /etc/raddb/certs/ca.pem

⁻⁻⁻⁻BEGIN CERTIFICATE-----

MIIE4TCCA8mgAwIBAgIJAKLmHn4eZLjBMA0GCSqGSIb3DQEBBQUAMIGTMQswCQYD VQQGEwJGUjEPMA0GA1UECBMGUmFkaXVzMRIwEAYDVQQHEw1Tb21ld2hlcmUxFTAT BgNVBAoTDEV4YW1wbGUgSW5jLjEgMB4GCSqGSIb3DQEJARYRYWRtaW5AZXhhbXBs ZS5jb20xJjAkBgNVBAMTHUV4YW1wbGUgQ2VydGlmaWNhdGUgQXV0aG9yaXR5MB4X DTE3MDMzMTExMTIxN1oXDTE3MDUzMDExMTIxN1owgZMxCzAJBgNVBAYTAkZSMQ8w DQYDVQQIEwZSYWRpdXMxEjAQBgNVBACTCVNvbWV3aGVyZTEVMBMGA1UEChMMRXhh bXBsZSBJbmMuMSAwHgYJKoZIhvcNAQkBFhFhZG1pbkB1eGFtcGxlLmNvbTEmMCQG A1UEAxMdRXhhbXBsZSBDZXJ0aWZpY2F0ZSBBdXRob3JpdHkwggEiMA0GCSqGSIb3 DQEBAQUAA4IBDwAwggEKAoIBAQC0vJ53NN7J9vhpKhcB3B00XLpeQFWjqolQOB9F /8Lh2Hax2rzb9wx0i1M0yXR+kN22H7RNwUHET8VdyGUsA40dZWuyzI8sKi5H42GU

${\tt Eu6GDw1YJvhHn4rVC360ZU/Nbaxj0eR8ZG0JGse4ftQKLfckkvC0S5QGn4X1elRS}$
oFe27HRF+pTDHd+nzbaDvhYWvFoe6iA27Od7AY/sDuo/tilJWGdm9ocPz3+0IiFC
$ay \texttt{6dtG55YQOHxKaswH7/HJkLsKWhS4YmXLgJXCeeJqooqr+TEwyCDEaFaiX\texttt{835Jp}}{}$
$gw \texttt{NNZ7X5US0FcjuuOtpJJ3hfQ8K6uXjEWPOkDE0DAnqp4/n9Ag \texttt{MBAAGjggE0MIIB}{MBAAGjggE0MIIB}$
${\tt MDAdBgNVHQ4EFgQUysFNRZKpAlcFCEgwdOPVGV0waLEwgcgGA1UdIwSBwDCBvYAU}$
ys FNRZKpAlcFCEgwdOPVGV0 wa LGhgZmkgZYwgZMxCzAJBgNVBAYTAkZSMQ8wDQYD wa SNRZKpAlcFCEgwdOPVGV0 wa LGhgZmkgZYwgZMxCzAJBgNVBAYTAkZSMQ8wDQYD wa SNRZKpAlcFCEgwdOPVGV0 wa LGhgZmkgZYwgZMxCzAJBgNVBAYTAkZSMQ8wDQYD wa SNRZKpAlcFCEgwdOPVGV0 wa
$\verb"VQQIEwZSYWRpdXMxEjAQBgNVBAcTCVNvbWV3aGVyZTEVMBMGA1UEChMMRXhhbXBs"$
${\tt ZSBJbmMuMSAwHgYJKoZIhvcNAQkBFhFhZG1pbkBleGFtcGxlLmNvbTEmMCQGA1UE}$
${\tt AxMdRXhhbXBsZSBDZXJ0aWZpY2F0ZSBBdXRob3JpdHmCCQCi5h5+HmS4wTAMBgNV}$
${\tt HRMEBTADAQH/MDYGA1UdHwQvMC0wK6ApoCeGJWh0dHA6Ly93d3cuZXhhbXBsZS5j}$
$b \verb+20vZXhhbXBsZV9jYS5jcmwwDQYJKoZIhvcNAQEFBQADggEBACsPR2jiOFXnTsK4$
lwnrrMylZZb12gDuqK+zKELox2mzlDMMK83tBsL8yjkv70KeZn821IzfTrTfvhzV
mjX6HgaWfYyMjYYYSw/iEu2JsAtQdpvC3di10nGwVPHlzbozPdov8cZtCb21ynfY
Z6cNjx8+aYQIcsRIyqA1IXMOBwIXo141TOmoODdgfX951poLwgktRLkv17Y7owsz
$\texttt{ChYDO++H7} Iews xx5pQfm56dA2cNrlTwWtMvViKyX7GlpwlbBOxgkLiFJ5+GFbfLh}$
a 0 HBHZWhTKvffbr62 mkbfjCUfJU4T3xgY9zFwiwT+BetCJgAGy8CT/qmnO+NJERO
RUvDhfE=

----END CERTIFICATE-----

Paso 2. Copie y pegue el resultado del paso anterior en un archivo de texto y cambie la extensión a .crt

Paso 3. Haga doble clic en el archivo y seleccione **Instalar certificado...** como se muestra en la imagen.



Paso 4. Instale el certificado en el almacén Autoridades de certificación raíz de confianza como se muestra en la imagen.

Certificate Import Wizard	×
Certificate Store Certificate stores are system areas where certificates are	kept.
Windows can automatically select a certificate store, or yo the certificate.	u can specify a location for
Place all certificates in the following store	le type of cel uncate
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

Crear perfil WLAN

Paso 1. Haga clic con el botón derecho del ratón en el icono Inicio y seleccione **Panel de control** como se muestra en la imagen.

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

Paso 2. Navegue hasta **Red e Internet > Centro de redes y recursos compartidos> haga clic en Configurar una nueva conexión o red** como se muestra en la imagen.



Paso 3. Seleccione **Conexión manual a una red inalámbrica** y haga clic en Nextas que se muestra en la imagen.

	-		×
🔶 🛬 Set Up a Connection or Network			
Chapter a connection option			
choose a connection option			
Connect to the Internet			
Set up a broadband or dial-up connection to the Internet.			
Set up a new network			
Manually connect to a viralers network			
Connect to a hidden network or create a new wireless profile.			
Connect to a workplace			
Set up a dial-up or VPN connection to your workplace.			
	Next	Can	cel

Paso 4. Introduzca la información con el nombre del SSID y el tipo de seguridad WPA2-Enterprise y haga clic en **Next** como se muestra en la imagen.

←	Se Manually connect to a	wireless network	-		×
	Enter information f	or the wireless network you want to add			
	Network name:	SSID-name			
	Security type:	W9A2-Enterprise ~			
	Encryption type:	AES			
	Security Key:	Hide character	5		
	Start this connection	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 risk			
		N	ext	Can	cel

Paso 5. Seleccione **Cambiar configuración de conexión** para personalizar la configuración del perfil WLAN como se muestra en la imagen.

		-		×
 Search State Stat				
Successfully added ise-ssid				
→ Change connection settings				
Open the connection properties so that I can change the	settings.			
			Close	e

Paso 6. Vaya a la ficha **Seguridad** y haga clic en **Configuración** como se muestra en la imagen.

ise-ssid Wireless Ne	twork 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

Paso 7. Elija si el servidor RADIUS está validado o no.

En caso afirmativo, habilite Verificar la identidad del servidor validando el certificado y de Autoridades de certificación raíz de confianza: list (lista) seleccione el certificado autofirmado de freeRADIUS.

Después de seleccionar **Configure** y disable **Use automáticamente mi nombre de inicio de sesión** y contraseña de Windows..., luego haga clic en OK como se muestra en las imágenes.

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:	_
Diggline & Olefred Linder dat Diggline & Olefred Linder dat Diggline & State Association of States dat	^
Example Certification Authority	
La debande Cationadera a Metteria (CECC) La Cation de Catione Serviciones Serviciones	~
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).	

Paso 8.	Configure las credenciales del usuario.

Cancel

ОK

Una vez de nuevo a la ficha Security , seleccione **Advanced settings**, especifique el modo de autenticación como **User authentication** y guarde las credenciales configuradas en freeRADIUS para autenticar al usuario, como se muestra en las imágenes.

ise-ssid Wireless Ne	twork Propertie	<u>s</u>	×
Connection Security			
Security type:	WPA2-Enterprise		~
Encryption type:	AES		~
Choose a network aut	thentication method	:	
Microsoft: Protected	EAP (PEAP)	✓ Settin	igs
Remember my cre time I'm logged o	edentials for this con	nection each	
Advanced settings			
Advanced settings			
		ОК	Cancel

02.1X settings 802.11 settings			Ì	
Specify authentication mode:				
User authentication	Save c	redentials		
Delete credentials for all users	s			
Enable single sign on for this net	work			
Perform immediately before up	user logon			
 Perform immediately after use 	er logon			
Maximum delay (seconds):	10	*		
Allow additional dialogs to be sign on	displayed during	single		
This network uses separate vi	irtual LANs for ma	achine		
and user authentication				
and user authentication				
and user authentication	ОК	Cancel		
Vindows Security	ОК	Cancel		
Vindows Security Save credentials	OK	Cancel		
Vindows Security Save credentials Saving your credentials allows when you're not logged on (f	ок s your compe for example, t	Cancel uter to cont to downloa	nect to the net ad updates).	tw
Vindows Security Save credentials Saving your credentials allows when you're not logged on (f	ок s your compt for example, t	Cancel uter to cont to downloa	nect to the ner ad updates).	tw

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

OK

 \times

Cancel

Proceso de autenticación en WLC

Ejecute los siguientes comandos para monitorear el proceso de autenticación para un usuario específico:

> debug client <mac-add-client>
 > debug dot1x event enable
 > debug dot1x aaa enable
 Para leer fácilmente los resultados de debug client, utilice la herramienta Wireless debug

Analizador de depuración inalámbrica

Troubleshoot

analyzer:

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.