# Configure 802.1x - PEAP with FreeRadius and WLC 8.3

## Contents

Introduction **Prerequisites** Requirements **Components Used** Configure **Network Diagram** Install httpd Server and MariaDB Install PHP 7 on CentOS 7 Install FreeRADIUS **FreeRADIUS** WLC as Authentication, Authorization, and Accounting (AAA) Client on FreeRADIUS FreeRADIUS as RADIUS Server on WLC **WLAN** Add Users to freeRADIUS Database Certificates on freeRADIUS **End Device Configuration** Import FreeRADIUS Certificate Create WLAN Profile Verify Authentication Process on WLC **Troubleshoot** 

# Introduction

This documents describes how to set up a Wireless Local Area Network (WLAN) with 802.1x security and Protected Extensible Authentication Protocol (PEAP) as Extensible Authentication Protocol (EAP). FreeRADIUS is used as the external Remote Authentication Dial-In User Service (RADIUS) server.

# Prerequisites

#### Requirements

Cisco recommends that you have basic knowledge of these topics:

- Linux
- Vim editor
- AireOS Wireless LAN Controllers (WLCs)

**Note**: This document is intended to give the readers an example on the configuration required on a freeRADIUS server for PEAP-MS-CHAPv2 authentication. The freeRADIUS server configuration presented in this document has been tested in the lab and found to work as expected. The Cisco Technical Assistance Center (TAC) does not support freeRADIUS server configuration.

#### **Components Used**

The information in this document is based on these software and hardware versions:

- CentOS7 or Red Hat Enterprise Linux 7 (RHEL7) (Recommended 1 GB RAM and at least 20 GB 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.

# Configure

#### **Network Diagram**



#### Install httpd Server and MariaDB

Step 1. Run these commands to install httpd server and 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
Step 2. Start and enable httpd (Apache) and MariaDB server.
```

[root@tac-mxwireless ~]# systemctl enable httpd [root@tac-mxwireless ~]# systemctl start httpd [root@tac-mxwireless ~]# systemctl start mariadb [root@tac-mxwireless ~]# systemctl enable mariadb
Step 3. Configure initial MariaDB settings to secure it.

[root@tac-mxwireless ~] #mysql\_secure\_installation

**Note**: Run all parts of this script. It is recommended for All MariaDB Servers in production use. Read each step carefully.

[root@tac-mxwireless ~] #mysql\_secure\_installation

Step 4. Configure Database for freeRADIUS (use same password configured in Step 3).

[root@tac-mxwireless ~] #mysql\_secure\_installation

#### Install PHP 7 on CentOS 7

Step 1. Run these commands to install PHP 7 on CentOS7.

[root@tac-mxwireless ~] #mysql\_secure\_installation

#### Install FreeRADIUS

Step 1. Run this command to install FreeRADIUS.

[root@tac-mxwireless ~]#mysql\_secure\_installation
Step 2. Make radius.service start after mariadb.service.

Run this command:

[root@tac-mxwireless ~]#mysql\_secure\_installation
Add a line in [Unit] section:

[root@tac-mxwireless ~] #mysql\_secure\_installation
[Unit] section must look like this:

[root@tac-mxwireless ~]#mysql\_secure\_installation
Step 3. Start and enable freeradius to start at boot up.

[root@tac-mxwireless ~] #mysql\_secure\_installation
Step 4. Enable firewalld for security.

[root@tac-mxwireless ~]#mysql\_secure\_installation Step 5. Add permanent rules to default zone to allow http, https and radius services.

[root@tac-mxwireless ~] #mysql\_secure\_installation
Step 6. Reload firewalld for changes to take effect.

[root@tac-mxwireless ~] #mysql\_secure\_installation

#### **FreeRADIUS**

In order to configure FreeRADIUS to use MariaDB, follow these steps.

Step 1. Import the RADIUS database scheme to populate RADIUS database.

[root@tac-mxwireless ~]#mysql\_secure\_installation Step 2. Create a soft link for Structured Query Language (SQL) under /etc/raddb/mods-enabled.

[root@tac-mxwireless ~]#mysql\_secure\_installation Step 3. Configure SQL module /raddb/mods-available/sql and change the database connection parameters to suite your environment.

[root@tac-mxwireless ~] #mysql\_secure\_installation
SQL section must look similar to this.

[root@tac-mxwireless ~]#mysql\_secure\_installation
Step 4. Change group right of /etc/raddb/mods-enabled/sql to radiusd.

[root@tac-mxwireless ~] #mysql\_secure\_installation

# WLC as Authentication, Authorization, and Accounting (AAA) Client on FreeRADIUS

Step 1. Edit /etc/raddb/clients.conf in order to set shared key for WLC.

[root@tac-mxwireless ~] #mysql\_secure\_installation
Step 2. At the bottom, add your controller ip address and the shared key.

#### FreeRADIUS as RADIUS Server on WLC

GUI:

Step 1. Open the GUI of the WLC and navigate to **SECURITY > RADIUS > Authentication > New** as shown in the image.

uluili. cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK	Saye Configuration   <u>P</u> ing   Logout   <u>R</u> efresh <mark>1</mark> <u>H</u> ome
Security	RADIUS Authentication Servers	Apply New
▼ AAA General	Auth Called Station ID Type $\square$ AP MAC Address:SSID $\checkmark$	
<ul> <li>RADIUS Authentication</li> </ul>	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	

Step 2. Fill the RADIUS server information as shown in the image.

RADIUS Authentication Serv	vers > 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 for	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:

[root@tac-mxwireless ~] #mysql\_secure\_installation

#### WLAN

GUI:

Step 1. Open the GUI of the WLC and navigate to **WLANs > Create New > Go**as shown in the image.



Step 2. Choose a name for the Service Set Identifier (SSID) and profile, then click **Apply**as shown in the image.

WLANs > New			< Back	Apply
Туре	WLAN V			
Profile Name	profile-name			
SSID	SSID-name			
ID	2 ~	1		

CLI:

[root@tac-mxwireless ~] #mysql\_secure\_installation
Step 3. Assign the RADIUS server to the WLAN.

CLI:

 $\label{eq:good_secure_installation} \end{tabulk} GUI:$ 

Navigate to **Security > AAA Servers** and choose the desired RADIUS server, then click **Apply** as shown in the image.

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	>

Step 4. Optionally increase the session time.

CLI:

 $\label{eq:secure_installation} $$ GUI: $$ OUT $$ Contended on the secure_installation of the secure of the secur$ 

Navigate to **Advanced > Enable Session Timeout >** click **Apply** as shown in the image.

WL	ANs≻Edit 'ise-p	rof				< Back	Apply
G	eneral Security	y QoS Policy-Mapping	J Adv	anced			
	Allow AAA Override	Enabled		DHCP		_	
	Coverage Hole Detection	🗹 Enabled		DHC	P Server	Override	
	Enable Session Timeout	28800 Session Timeou (secs	)	DHCI Assiç	P Addr. 9nment	Required	
	Aironet IE	Enabled		OEAP			
	Diagnostic Channel <u>18</u>	Enabled		Split	: Tunnel	Enabled	
	Override Interface ACL	IPv4 None 🗡	IPv6 None ∨	Manage	ment Frame I	Protection (MFP)	
	Layer2 Ad	None 🗸					
	URL ACL	None 🗸		MFP	Client Protecti	ion 🛃 Optional 🗸	
	P2P Blocking Action	Disabled $\vee$		DTIM Pe	eriod (in beaco	on intervals)	
	Client Exclusion ²	Enabled Timeout Value (secs)		802.	11a/n (1 - 25	5) 1	
	Maximum Allowed Clients <sup>g</sup>	0		802. N <b>ac</b>	11b/g/n (1 - 2	255) 1	
<	Static IP Tunneling	□		NAC	State None	$\overline{\mathbf{v}}$	>

#### Step 5. Enable the WLAN.

#### CLI:

 $\label{eq:good_secure_installation} \end{tabulk} GUI:$ 

#### Navigate to General > Status > Tick Enabled > Click Apply as shown in the image.

Ns > Edit 'ssid-r	ame'	< Back
eneral Security	QoS Policy-Mapping Advanced	
Profile Name	ssid-name	
Туре	WLAN	
SSID	ssid-name	
Status	Enabled	

#### Add Users to freeRADIUS Database

By default clients use PEAP protocols, however freeRadius support other methods (not covered in this guide).

Step 1. Edit the file /etc/raddb/users.

[root@tac-mxwireless ~] #mysql\_secure\_installation

Step 2. At the bottom of the file append the users information. In this example, **user1** is the username and **Cisco123** the password.

[root@tac-mxwireless ~] #mysql\_secure\_installation

#### **Certificates on freeRADIUS**

FreeRADIUS comes with a default Certification Authoritiy (CA) certificate and a device certificate which are stored in the path /etc/raddb/certs. The name of these certificates are ca.pem and server.pem. server.pem is the certificate that clients receive while they go through the authentication process. If you need to assign a different certificate for EAP authentication you can simply delete them and save the new ones in the same path with that exact same name.

#### **End Device Configuration**

Configure a laptop Windows machine to connect to an SSID with 802.1x Authentication and PEAP/MS-CHAP (Microsoft version of the Challenge-Handshake Authentication Protocol) version 2.

In order to create the WLAN profile on the windows machine there are two options:

- 1. Install the self-signed certificate on the machine to validate and trust freeRADIUS server in order to complete the authentication
- 2. Bypass the validation of the RADIUS server and trust any RADIUS server used to perform the authentication (not recommended, as it can become a security issue). The configuration for these options are explained on End device configuration Create the WLAN Profile.

#### Import FreeRADIUS Certificate

If you use the default certificates installed on freeRADIUS, follow these steps in order to import the EAP certificate from the freeRADIUS server into the end device.

Step 1. Get the cert from FreeRadius:

[root@tac-mxwireless ~] #mysql\_secure\_installation

Step 2. Copy and paste the output of the previous step into a text file and change extension to .crt

Step 3. Double click the file and select **Install Certificate...** as shown in the image.

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

Step 4. Install the certificate into the **Trusted Root Certification Authorities** store as shown in the image.

Certificate Import Wizard	83
Certificate Store	
Certificate stores are system areas where certificates are kept.	
Windows can automatically select a certificate store, or you can specify a location for the certificate.	
Automatically select the certificate store based on the type of certificate	
Place all certificates in the following store	
Certificate store:	
Select Certificate Store	
Select the certificate store you want to use.	
Personal Trusted Root Certification Authorities Enterprise Trust Intermediate Certification Authorities Trusted Publishers Intrusted Certificates	
Show obveiral stores Back Next > Cance	el 🛛
OK Cancel OK	

#### **Create WLAN Profile**

Step 1. Right click on Start icon and select Control panel as shown in the image.

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 אין א 👔 🛄 אין אין אין אין 🙀 Netw	or 👷

Step 2. Navigate to **Network and Internet > Network and Sharing Center> click Set up a new connection or network** as shown in the image.

💐 Network and Sharing Center					
🔶 🚽 🕆 🛧 🕹 Control F	Panel > Network and Internet > Network a	and Sharing Center			
Control Panel Home View your basic network information and set up connections					
Change adapter settings	View your active networks Change adapter settings				
Change advanced sharing settings	<b>cisco.com</b> Domain network	Access type: Internet Connections: <i>Iternet</i>			
	Change your networking settings Set up a new connection or net Set up a broadband, dial-up, or Troubleshoot problems Diagnose and repair network p	twork r VPN connection; or set up a router or access point. roblems, or get troubleshooting information.			

Step 3. Select Manually connect to a wireless network and click Nextas shown in the image.

	-		×
🔶 👙 Set Up a Connection or Network			
Choose a connection option			
			-
Connect to the Internet			
<ul> <li>Set up a broadband or dial-up connection to the internet.</li> </ul>			
with the second			
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.			
Connect to a workplace			
Set up a dial-up or VPN connection to your workplace.			
	Next	Car	ral
	Next	Car	icei

Step 4. Enter the information with the name of the SSID and security type WPA2-Enterprise and click **Next** as shown in the image.

÷	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	characters			
	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 b	ve at risk.			
			Nex	t	Can	cel

Step 5. Select **Change connection settings** in order to customize the configuration of the WLAN profile as shown in the image.

	-		$\times$
<ul> <li>Second Second Sec</li></ul>			
Successfully added ise-ssid			
→ Change connection settings Open the connection properties so that I can change the settings			
open die connection properces so diec r can change die securitys.			
		Clo	se

Step 6. Navigate to **Security** tab and click **Settings** as shown in the image.

ise-ssid Wireless Network Properties 🛛 🗙				
Connection Security				
Security type:	WPA2-Enterprise		$\sim$	
Encryption type:	AES		$\sim$	
Choose a network aut	hentication method:		_	
Microsoft: Protected E	EAP (PEAP) 🗸 🗸	Settin	gs	
Remember my credentials for this connection each time I'm logged on				
Advanced settings				
		ОК	Can	cel

Step 7. Choose if RADIUS server is validated or not.

If yes, enable Verify the server's identity by validating the certificate and from Trusted Root Certification Authorities: list select the self-signed certificate of freeRADIUS.

After that select **Configure** and disable **Automatically use my Windows logon name and password...**, then click **OK** as shown in the images.

Protected EAP Properties	×
When connecting:	_
Connect to these servers (examples:srv1;srv2;.*\.srv3\.com):	
Trusted Root Certification Authorities:	
Digglite & Cleffed Lands and     Digglite & Cleffed Lands and     Digglite & Cleffed Lands and     Digglite & Cleffed Lands and Lands and     Digglite & Cleffed Lands	^
Example Certification Authority	~
Notifications before connecting: Tell user if the server name or root certificate isn't specified	~
Select Authentication Method: Secured password (EAP-MSCHAP v2) Configur	e
Enable Fast Reconnect     Disconnect if server does not present cryptobinding TLV     Enable Identity Privacy	
OK Cance	el
EAP MSCHAPv2 Properties X	
When connecting:	

Step 8. Configure the user credentials.

OK

Automatically use my Windows logon name and password (and domain if any).

Cancel

Once back to Security tab, select **Advanced settings**, specify authentication mode as **User authentication** and save the credentials that were configured on freeRADIUS in order to authenticate the user, as shown in the images.

ise-ssid Wireless Ne	twork Properti	es	×	
Connection Security				
Security type:	WPA2-Enterprise		~	
Encryption type:	AES		~	
Choose a network aut	thentication method	l:		
Microsoft: Protected	EAP (PEAP)	✓ Settin	igs	
Remember my cre time I'm logged o	Remember my credentials for this connection each			
Advanced settings				
Parances seconds				
		OK	Cancel	

User authentication Save creden	_
User authentication Save creden	
	ntials
Delete credentials for all users	
Enable single sign on for this network	
Perform immediately before user logon	
O Perform immediately after user logon	_
Maximum delay (seconds): 10	*
Allow additional dialogs to be displayed during single sign on	e
This network uses separate virtual LANs for machine and user authentication	e
ОК	Cancel
ows Security	
e credentials	

Saving your cro when you're n	edentials allows your cor ot logged on (for examp	nputer to connect to the network le, to download updates).
 cisco	user1	
		OK Cancel

Х

# Verify

Use this section in order to confirm that your configuration works properly.

#### **Authentication Process on WLC**

Run the next commands in order to monitor the authentication process for a specific user:

[root@tac-mxwireless ~]#mysql\_secure\_installation
For an easy way to read debug client outputs, use the Wireless debug analyzer tool:

Wireless Debug Analyzer

## Troubleshoot

There is currently no specific troubleshooting information available for this configuration.