# 配置802.1x — 使用FreeRadius和WLC 8.3的 PEAP

## 目錄

簡介 必要條件 需求 採用元件 設定 網路圖表 安裝httpd伺服器和MariaDB 在CentOS 7上安裝PHP 7 安裝FreeRADIUS **FreeRADIUS** WLC作為FreeRADIUS上的驗證、授權和計量(AAA)使用者端 在WLC上將FreeRADIUS作為RADIUS伺服器 **WLAN** 將使用者新增到freeRADIUS資料庫 freeRADIUS上的憑證 終端裝置配置 匯入FreeRADIUS證書 建立WLAN設定檔 驗證 WLC上的驗證程式 疑難排解

## 簡介

本檔案介紹如何將具有802.1x安全性和受保護的可擴充驗證通訊協定(PEAP)的無線區域網路 (WLAN)設定為可擴充驗證通訊協定(EAP)。 FreeRADIUS用作外部遠端驗證撥入使用者服務 (RADIUS)伺服器。

## 必要條件

### 需求

思科建議您瞭解以下主題的基本知識:

- Linux
- Vim編輯器
- AireOS無線LAN控制器(WLC)

註:本文檔旨在為讀者提供有關freeRADIUS伺服器上進行PEAP-MS-CHAPv2身份驗證所需

的配置的示例。本文中介紹的freeRADIUS伺服器配置已在實驗室中經過測試,發現可按預期 工作。思科技術援助中心(TAC)不支援freeRADIUS伺服器配置。

### 採用元件

本文中的資訊係根據以下軟體和硬體版本:

- CentOS7或Red Hat Enterprise Linux 7(RHEL7)(建議使用1 GB記憶體和至少20 GB硬碟)
- WLC 5508 v8.3
- MariaDB(MySQL)
- FreeRADIUS
- •7菲律賓比索

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

## 設定

#### 網路圖表

#### freeRADIUS



### 安裝httpd伺服器和MariaDB

步驟1.運行這些命令以安裝httpd伺服器和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
步驟2.啟動並啟用httpd(Apache)和MariaDB伺服器。

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

步驟3.配置初始MariaDB設定以保護它。

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

**附註**:運行此指令碼的所有部分。建議在生產中使用所有MariaDB伺服器。仔細閱讀每一步。

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!

步驟4.為freeRADIUS配置資料庫(使用步驟3中配置的相同密碼)。

[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

#### 在CentOS 7上安裝PHP 7

步驟1.運行這些命令以在CentOS7上安裝PHP 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

### 安裝FreeRADIUS

步驟1.運行此命令以安裝FreeRADIUS。

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

步驟2.使radius.service 在mariadb.service之後啟動。

運行此命令:

[root@tac-mxwireless ~]# vim /etc/systemd/system/multi-user.target.wants/radiusd.service 在[unit]一行:

After=mariadb.service [**Unit]部分必須如下所示**:

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

#### 步驟3.啟動並啟用freeradius以在啟動時啟動。

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

#### 步驟4.啟用firewalld以確保安全。

[root@tac-mxwireless ~]# systemctl enable firewalld [root@tac-mxwireless ~]# systemctl start firewalld [root@tac-mxwireless ~]# systemctl status firewalld 步驟5.將永久規則新增到預設區域以允許http、https和radius服務。

[root@tac-mxwireless ~]# firewall-cmd --get-services | egrep 'http|https|radius'
[root@tac-mxwireless ~]# firewall-cmd --add-service={http,https,radius} --permanent success
步驟6.重新載入防火牆以使更改生效。

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

#### **FreeRADIUS**

若要將FreeRADIUS設定為使用MariaDB,請執行以下步驟。

#### 步驟1.匯入RADIUS資料庫方案以填充RADIUS資料庫。

[root@tac-mxwireless ~]# mysql -u root -p radius < /etc/raddb/modsconfig/sql/main/mysql/schema.sql

步驟2.在/etc/raddb/mods-enabled下為結構化查詢語言(SQL)建立軟連結。

[root@tac-mxwireless ~]# ln -s /etc/raddb/mods-available/sql /etc/raddb/mods-enabled/ 步驟3.配置SQL模組/raddb/mods-available/sql並更改資料庫連線引數以套件環境。

[root@tac-mxwireless ~]# vim /etc/raddb/mods-available/sql SQL節必須與以下內容類似。

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"
步驟4.將/etc/raddb/mods-enabled/sql的組許可權更改為radiusd。

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

#### WLC在FreeRADIUS上作為驗證、授權和記帳(AAA)使用者端

步驟1。編輯/etc/raddb/clients.conf,設定WLC的共用金鑰。

[root@tac-mxwireless ~]# vim /etc/raddb/clients.conf 步驟2.在底部,新增控制器IP地址和共用金鑰。

client{ secret = shortname = }

### 在WLC上將FreeRADIUS作為RADIUS伺服器

GUI:

0

步驟1。開啟WLC的GUI,然後導覽至SECURITY > RADIUS > Authentication > New,如下圖所示

սիսիս		Sa <u>v</u> e Configuration   <u>P</u> ing   Logout   <u>R</u> efresh
CISCO	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK	n <u>H</u> ome
Security	RADIUS Authentication Servers	Apply New
▼ AAA General	Auth Called Station ID Type AP MAC Address:SSID	
<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 🗸	
DNS	Framed MTU 1300	

步驟2.填寫RADIUS伺服器資訊,如圖所示。

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 $$	
Server Timeout	10 second	5
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:

步驟1。開啟WLC的GUI,然後導覽至WLANs > Create New > Goas,如下圖所示。

cisco	<u>M</u> ONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	WIRELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK	
WLANs	WLANs									
<ul> <li>₩LANS</li> <li>WLANS</li> <li>Advanced</li> </ul>	Current Filt	er: No	ne [ <u>Cha</u>	nge Filter] [Cl	<u>ear Filter]</u>			Create N	ew	Go

#### 步驟2.選擇服務集標識符(SSID)和配置文件的名稱,然後按一下Applyas(如圖所示)。

W	/LANs > New			< Back	Apply
	Туре	WLAN V	_		
	Profile Name	profile-name			
	SSID	SSID-name			
	ID	2 ~			

CLI:

> config wlan create <id> <profile-name> <ssid-name>
步驟3.將RADIUS伺服器分配給WLAN。

CLI:

o

> config wlan radius\_server auth add <wlan-id> <radius-index>
GUI:

導覽至**Security > AAA Servers**,然後選擇所需的RADIUS伺服器,然後按一下**Apply**,如下圖所示

_ANs > Edit 'ise-pro	f	< Back A	pply
General Security	QoS Policy-Mapping Advanced		
Layer 2 Layer 3	AAA Servers		_
		^	
Select AAA servers belo	w to override use of default servers on this WLAN		
RADIUS Servers			
RADIUS Server Overw	rite interface Enabled		
8	Kan Garage State		
Server 1 IP:172.16.	15.8. Port:1812 V None V		1
Server 2 None	V None V		
Server 3 None			
Server 4 None	V None V		
Server 5 None	V None V		
Server 6 None			
RADIUS Server Account	ing		
Interim Undate	L/I Interior Intervallo Concente		

#### 步驟4.(可選)增加會話時間。

CLI:

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

導覽至Advanced > Enable Session Timeout >按一下Apply,如下圖所示。

WL	ANs > Edit 'is	e-pro	f						< Back	Apply	
6	ieneral Secu	ırity	QoS	Policy-Mapping	g Ad	vanced					
	Allow AAA Overri	ide	🗌 Enabled	d		DHCP				Î	
	Coverage Hole Detection		🗹 Enabled	d		DHC	P Server		verride		
	Enable Session Timeout		⊠ 2880 Ses	)0 sion Timeou (secs	)	DHC Assi	P Addr. gnment		equired		
	Aironet IE		Enabled			OEAP					
	Diagnostic Chan <u>18</u>	nel	Enabled			Spli	t Tunnel	🗌 En a	abled		
	Override Interfa ACL	ice	IPv4 None	2 1	IPv6 None	🗹 Manage	ement Frame	Protection (	MFP)		
	Layer2 Ad		None 🗸								
	URL ACL		None 🗸			MFP	Client Proted	tion 🛃 🛛 Optio	onal 🗸		
	P2P Blocking Act	tion	Disabled	~		DTIM P	eriod (in beac	con intervals)	)		
	Client Exclusion	3	⊠ Enabled Ti	) meout Value (secs)		802	11a/n (1 - 25	55) 1			
	Maximum Allowe Clients <u>ª</u>	ed	0			802 NAC	11b/g/n (1 -	255) 1			
<	Static IP Tunneli	ing	□			NAC	State None	· · · · · ·		>	

#### 步驟5.啟用WLAN。

#### CLI:

> config wlan enable <wlan-id>
GUI:

#### 導覽至General > Status > Tick Enabled > Click Apply,如下圖所示。

WLANs > Edit 'ssid-r	name'	< Back
General Security	QoS Policy-Mapping Advanced	
Profile Name	ssid-name	
Type	WLAN	
SSID	ssid-name	
Status	C Enabled	

### 將使用者新增到freeRADIUS資料庫

預設情況下,客戶端使用PEAP協定,但freeRadius支援其他方法(本指南未涉及)。

步驟1.編輯文**件/etc/raddb/users**。

user1 Cleartext-Password := <Cisco123>

#### 步驟3.重新啟動FreeRadius。

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

#### freeRADIUS上的憑證

FreeRADIUS附帶預設證書頒發機構(CA)證書和裝置證書,這些證書儲存在路徑/etc/raddb/certs中 。這些證書的名稱為ca.pem和server.pem。server.pem是使用者端進行驗證過程中收到的憑證。如 果您需要為EAP身份驗證分配不同的證書,只需刪除這些證書並將新證書儲存在同一路徑中,並且 使用完全相同的名稱。

#### 終端裝置配置

配置筆記型電腦Windows電腦,以使用802.1x身份驗證和PEAP/MS-CHAP(Microsoft版本的質詢 — 握手身份驗證協定)版本2連線到SSID。

要在Windows電腦上建立WLAN配置檔案,有兩種選擇:

- 1. 在電腦上安裝自簽名證書以驗證和信任freeRADIUS伺服器以完成身份驗證
- 2. 繞過RADIUS伺服器的驗證,並信任任何用於執行驗證的RADIUS伺服器(不建議,因為這可 能成為安全問題)。這些選項的配置將在終端裝置配置 — 建立WLAN配置檔案中說明。

#### 匯入FreeRADIUS證書

如果您使用安裝在freeRADIUS上的預設證書,請按照以下步驟操作,將EAP證書從freeRADIUS伺 服器匯入到終端裝置。

步驟1.從FreeRadius取得憑證:

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

----BEGIN CERTIFICATE----

MIIE4TCCA8mgAwIBAgIJAKLmHn4eZLjBMA0GCSqGSIb3DQEBBQUAMIGTMQswCQYD VQQGEwJGUjEPMA0GA1UECBMGUmFkaXVzMRIwEAYDVQQHEwlTb21ld2hlcmUxFTAT BgNVBAoTDEV4YW1wbGUgSW5jLjEgMB4GCSqGSIb3DQEJARYRYWRtaW5AZXhhbXBs ZS5jb20xJjAkBgNVBAMTHUV4YW1wbGUgQ2VydG1maWNhdGUgQXV0aG9yaXR5MB4X DTE3MDMzMTExMTIxNloXDTE3MDUzMDExMTIxNlowgZMxCzAJBgNVBAYTAkZSMQ8w DQYDVQQIEwZSYWRpdXMxEjAQBgNVBAcTCVNvbWV3aGVyZTEVMBMGA1UEChMMRXhh A1UEAxMdRXhhbXBsZSBDZXJ0aWZpY2F0ZSBBdXRob3JpdHkwggEiMA0GCSqGSIb3 DQEBAQUAA4IBDwAwggEKAoIBAQC0vJ53NN7J9vhpKhcB3B00XLpeQFWjqolQOB9F /8Lh2Hax2rzb9wxOi1MOyXR+kN22H7RNwUHET8VdyGUsA4OdZWuyz18sKi5H42GU Eu6GDw1YJvhHn4rVC360ZU/Nbaxj0eR8ZG0JGse4ftQKLfckkvCOS5QGn4X1elRS oFe27HRF+pTDHd+nzbaDvhYWvFoe6iA27Od7AY/sDuo/tiIJWGdm9ocPz3+0IiFC ay6dtG55YQOHxKaswH7/HJkLsKWhS4YmXLgJXCeeJqooqr+TEwyCDEaFaiX835Jp gwNNZ7X5US0FcjuuOtpJJ3hfQ8K6uXjEWPOkDE0DAnqp4/n9AgMBAAGjggE0MIIB MDAdBgNVHQ4EFgQUysFNRZKpAlcFCEgwdOPVGV0waLEwgcgGA1UdIwSBwDCBvYAU ys FNRZKpAlcFCEgwdOPVGV0 wa LGhgZmkgZYwgZMxCzAJBgNVBAYTAkZSMQ8wDQYD wa SNRZKpAlcFCEgwdOPVGV0 wa LGhgZmkgZYwgZMxCzAJBgNVBAYTAkZSMQ8wDQYD wa SNRZKpAlcFCEgwdOPVGV0 wa LGhgZmkgZYwgZMxCzAJBgNVBAYTAkZSMQ8wDQYD wa SNRZKpAlcFCEgwdOPVGV0 waVQQIEwZSYWRpdXMxEjAQBgNVBAcTCVNvbWV3aGVyZTEVMBMGA1UEChMMRXhhbXBs ZSBJbmMuMSAwHgYJKoZIhvcNAQkBFhFhZG1pbkBleGFtcGxlLmNvbTEmMCQGA1UE AxMdRXhhbXBsZSBDZXJ0aWZpY2F0ZSBBdXRob3JpdHmCCQCi5h5+HmS4wTAMBqNV HRMEBTADAQH/MDYGA1UdHwQvMC0wK6ApoCeGJWh0dHA6Ly93d3cuZXhhbXBsZS5j

b20vZXhhbXBsZV9jYS5jcmwwDQYJKoZIhvcNAQEFBQADggEBACsPR2jiOFXnTsK4 lwnrrMylZZbl2gDuqK+zKELox2mzlDMMK83tBsL8yjkv70KeZn821IzfTrTfvhzV mjX6HgaWfYyMjYYYSw/iEu2JsAtQdpvC3di10nGwVPHlzbozPdov8cZtCb21ynfY Z6cNjx8+aYQIcsRIyqA1IXMOBwIXo141TOmoODdgfX95lpoLwgktRLkv17Y7owsz ChYDO++H7Iewsxx5pQfm56dA2cNrlTwWtMvViKyX7GlpwlbBOxgkLiFJ5+GFbfLh a0HBHZWhTKvffbr62mkbfjCUfJU4T3xgY9zFwiwT+BetCJgAGy8CT/qmnO+NJERO RUvDhfE=

----END CERTIFICATE----

步驟2.將上一步的輸出複製並貼上到文本檔案中,並將副檔名更改為.crt

步驟3.按兩下該檔案並選擇Install Certificate... 如下圖所示。

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

步驟4.將憑證安裝到**受信任的根憑證授權單位**儲存區,如下圖所示。

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. Automatically select the certificate store ba	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

### 建立WLAN設定檔

步驟1。按一下右鍵「Start(開始)」圖示並選擇「Control panel」,如下圖所示。

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
🚹 א א א א א א א א א א א א א א א א א א א

步驟2.導覽至**Network and Internet > Network and Sharing Center**>按一下Set up a new connection or network,如下圖所示。



步驟3.選擇手動連線到無線網路,然後單擊Nextas(如圖所示)。

	-		×
🔶 👙 Set Up a Connection or Network			
Choose a connection option			
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	Can	cel

步驟4.輸入SSID名稱和安全型別WPA2-Enterprise的資訊,然後按一下**Next**(如圖所示)。

←	Se Manually connect to	a wireless network	-		×
	Enter information	for the wireless network you want to add	ł		
	Network name:	SSID-name			
	Security type:	WPA2-Enterprise ~			
	Encryption type:	AES			
	Security Key.	Hide chara	cters		
	Start this connect	ion automatically			
	Connect even if the Warning: If you se	e network is not broadcasting elect this option, your computer's privacy might be at	risk.		
			Next	Can	cel

步驟5.選擇Change connection settings以自訂WLAN設定檔的組態,如下圖所示。

	-		$\times$
<ul> <li>Manually connect to a wireless network</li> </ul>			
Successfully added ise-ssid			
Change connection settings			
Open the connection properties so that I can change the settings.			
		0	
		Clo	se

步驟6.導覽至Security索引標籤,然後按一下Settings,如下圖所示。

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 credentials for this connection each time I'm logged on				
une in logged of				
	_			
Advanced settings				
		ОК	Can	cel

步驟7.選擇是否已驗證RADIUS伺服器。

如果是,請啟用**通過驗證證書和從受信任的根證書頒發機構**驗證服**務器的標識:**清單選擇 freeRADIUS的自簽名證書。

選擇Configure並禁用Automatically use my Windows logon name and password...後,按一下 OK,如下圖所示。

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:	
Bagolio & Olefrei Issue das     Bagolio & Olefrei Issue das	^
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) Configu Enable Fast Reconnect Disconnect if server does not present cryptobinding TLV Enable Identity Privacy	re
OK Canc	el
EAP MSCHAPv2 Properties ×	

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

步驟8.配置使用者憑據。

回到「安全」頁籤後,選擇**Advanced settings**,將身份驗證模式指定為**User authentication**,並儲 存在freeRADIUS上配置的憑據以驗證使用者,如下圖所示。

ise-ssid Wireless Ne	twork Properties		×
Connection Security			
Security type:	WPA2-Enterprise		~
Encryption type:	AES		~
Choose a network aut	thentication method:		
Microsoft: Protected	EAP (PEAP)	Settin	igs
Remember my cre	edentials for this conne	ction each	
une in ogged o			
Advanced settings			
		ОК	Cancel

Specify authentication mode:		
User authentication	Save cre	edentials
Delete credentials for all users		
Enable single sign on for this netw	ork	
Perform immediately before us	ser logon	
<ul> <li>Perform immediately after use</li> </ul>	r logon	
Maximum delay (seconds):	10	*
Allow additional dialogs to be a sign on	displayed during s	ingle
This network uses separate vir and user authentication	tual LANs for mag	chine

Windows Secur	ity		×
Save creder Saving your cre when you're no	tials dentials allows your com t logged on (for example	puter to connect to the network e, to download updates).	
 cisco	user1		
		OK Cancel	

## 驗證

使用本節內容,確認您的組態是否正常運作。

## WLC上的驗證程式

運行以下命令以監控特定使用者的身份驗證過程:

> debug client <mac-add-client>

- > debug dot1x event enable
- > debug dot1x aaa enable

若要輕鬆讀取偵錯使用者端輸出,請使用無線偵錯分析器工具:

無線偵錯分析器

## 疑難排解

目前尚無適用於此組態的具體疑難排解資訊。