# 802.1x 구성 - FreeRadius 및 WLC 8.3을 사용하 는 PEAP

# 목차

소개 사전 요구 사항 요구 사항 사용되는 구성 요소 구성 네트워크 다이어그램 httpd 서버 및 MariaDB 설치 CentOS 7에 PHP 7 설치 FreeRADIUS 설치 자유 RADIUS FreeRADIUS의 AAA(Authentication, Authorization, and Accounting) 클라이언트로 WLC WLC의 RADIUS 서버로 FreeRADIUS **WLAN** freeRADIUS 데이터베이스에 사용자 추가 freeRADIUS의 인증서 최종 디바이스 컨피그레이션 FreeRADIUS 인증서 가져오기 WLAN 프로파일 생성 다음을 확인합니다. WLC의 인증 프로세스 문제 해결

# 소개

이 문서에서는 802.1x 보안 및 PEAP(Protected Extensible Authentication Protocol)를 EAP(Extensible Authentication Protocol)로 무선 WLAN(Local Area Network)을 설정하는 방법에 대 해 설명합니다. FreeRADIUS는 외부 RADIUS(Remote Authentication Dial-In User Service) 서버로 사용됩니다.

# 사전 요구 사항

## 요구 사항

Cisco에서는 이러한 주제에 대한 기본적인 지식을 얻을 것을 권장합니다.

- 리눅스
- 비디오 편집기
- AireOS WLC(Wireless LAN Controller)

**참고**: 이 문서는 PEAP-MS-CHAPv2 인증을 위해 freeRADIUS 서버에 필요한 구성에 대한 예 를 독자에게 제공하기 위한 것입니다.이 문서에 제시된 freeRADIUS 서버 컨피그레이션은 Lab에서 테스트되었으며 예상대로 작동하는 것으로 확인되었습니다.Cisco TAC(Technical Assistance Center)는 freeRADIUS 서버 컨피그레이션을 지원하지 않습니다.

#### 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

• CentOS7 또는 Red Hat Enterprise Linux 7(RHEL7)(권장 1GB RAM 및 20GB HDD)

- WLC 5508 v8.3
- MariaDB(MySQL)
- 자유 RADIUS
- PHP 7

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바 이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

# 구성

네트워크 다이어그램



#### httpd 서버 및 MariaDB 설치

1단계. 이러한 명령을 실행하여 httpd 서버 및 MariaDB를 설치합니다.

[root@tac-mxwireless ~]# yum -y groupinstall "Development Tools" [root@tac-mxwireless ~]# yum -y install httpd httpd-devel mariadb-server mariadb 2단계. httpd(Apache) 및 MariaDB 서버를 시작하고 활성화합니다.

[root@tac-mxwireless ~]# systemctl enable httpd [root@tac-mxwireless ~]# systemctl start httpd [root@tac-mxwireless ~]# systemctl start mariadb [root@tac-mxwireless ~]# systemctl enable mariadb 3단계. 초기 MariaDB 설정을 구성하여 보호합니다.

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

**참고:**이 스크립트의 모든 부분을 실행합니다.프로덕션 환경에서 모든 MariaDB 서버에 사용하는 것이 좋습니다.각 단계를 주의 깊게 읽으십시오.

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! 4단계. freeRADIUS를 위해 데이터베이스를 구성합니다(3단계에서 구성한 것과 동일한 비밀번호 사용).

[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

#### CentOS 7에 PHP 7 설치

1단계. 이러한 명령을 실행하여 CentOS7에 PHP 7을 설치합니다.

[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

#### FreeRADIUS 설치

1단계, 이 명령을 실행하여 FreeRADIUS를 설치합니다.

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

2단계. radius.service를 mariadb.service 이후 시작합니다.

#### 다음 명령을 실행합니다.

[root@tac-mxwireless ~]# vim /etc/systemd/system/multi-user.target.wants/radiusd.service [Unit] 섹션에 라인 추가:

After=mariadb.service [Unit] 섹션은 다음과 같아야 합니다.

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

5단계. http, https 및 radius 서비스를 허용하기 위해 기본 영역에 영구 규칙을 추가합니다.

[root@tac-mxwireless ~]# firewall-cmd --add-service={http,https,radius} --permanent success

[root@tac-mxwireless ~]# firewall-cmd --get-services | egrep 'http|https|radius'

MariaDB를 사용하도록 FreeRADIUS를 구성하려면 다음 단계를 수행합니다.

1단계, RADIUS 데이터베이스 구성표를 가져와 RADIUS 데이터베이스를 채웁니다.

#### 3단계, 부팅 시 freeradius를 시작 및 활성화합니다.

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

[root@tac-mxwireless ~]# systemctl enable radiusd.service 4단계, 보안을 위해 방화벽을 활성화합니다.

6단계, 변경 사항을 적용하려면 방화벽을 다시 로드합니다.

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

자유 RADIUS

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

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

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

```
2단계. /etc/radb/mods가 활성화된 SQL(Structured Query Language)에 대한 소프트 링크를 생성합
니다.
```

[root@tac-mxwireless ~]# ln -s /etc/raddb/mods-available/sql /etc/raddb/mods-enabled/ 3단계. SQL 모듈 /radb/mods-available/sql을 구성하고 데이터베이스 연결 매개 변수를 사용자 환경 에 맞게 변경합니다.

[root@tac-mxwireless ~]# vim /etc/raddb/mods-available/sql SQL 섹션은 이와 유사해야 합니다.

```
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" 4단계. 그룹 권한의 /etc/radb/mods-enabled/sgl을 radiusd로 변경합니다.

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

# FreeRADIUS에서 AAA(Authentication, Authorization, and Accounting) 클라이언트로 WLC

1단계. WLC의 공유 키를 설정하려면 /etc/raddb/clients.conf를 편집합니다.

[root@tac-mxwireless ~]# vim /etc/raddb/clients.conf 2단계. 하단에서 컨트롤러 IP 주소와 공유 키를 추가합니다.

client{ secret = shortname = }

#### WLC의 RADIUS 서버로 FreeRADIUS

GUI:

1단계. WLC의 GUI를 열고 이미지에 표시된 대로 SECURITY > RADIUS > Authentication > New로 이동합니다.



#### 2단계. 이미지에 표시된 대로 RADIUS 서버 정보를 채웁니다.

ADIUS Authentication Serv	/ers > 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	$\Box$ (Designed fo	r FIPS customers and requires a key wrap compliant RADIUS server)
Port Number	1812	
Server Status	Enabled $\sim$	
Support for CoA	Disabled $ \sim $	
Server Timeout	10 second	:
Network User	🗹 Enable	
Management	🗹 Enable	
Management Retransmit Timeout	2 seconds	
TDC	E Enable	

#### CLI:

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

#### WLAN

#### GUI:

#### 1단계. WLC의 GUI를 열고 이미지에 표시된 WLANs > Create New > Goas로 이동합니다.

،، ،،، ،، 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	HELP	<u>F</u> EEDBACK
WLANs	WLANs								
WLANS     WLANS     Advanced	Current Filt	er: No	ne [ <u>Cha</u>	nge Filter] [Cl	<u>ear Filter]</u>			Create N	lew 🗸 Go

2단계. SSID(Service Set Identifier) 및 프로파일의 이름을 선택한 다음 이미지에 표시된 대로 Applyas를 클릭합니다.

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> 3단계. WLAN에 RADIUS 서버를 할당합니다.

CLI:

Security(**보안) > AAA Servers(AAA 서버**)로 이동하고 원하는 RADIUS 서버를 선택한 다음 이미지 에 표시된 대로 **Apply(적용**)를 클릭합니다.

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		
Authentication Servers Accounting Servers EAP Parameters		
🗹 Enabled 🔤 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		~
<	>	,

4단계. 선택적으로 세션 시간을 늘립니다.

#### Advanced(**고급) > Enable Session Timeout(세션 시간 제한 활성화)으로 이동하고** 이미지에 표시된 대로 **Apply(적용**)를 클릭합니다.

WL	ANs > Ec	lit 'ise-pro	of'					< Back	Apply
G	eneral	Security	QoS	Policy-Mapping	Adva	nced			
	Allow AA/	A Override	Enabled	1		DHCP		_	^
	Coverage Detection	e Hole N	🗹 Enabled	ł		DHC	P Server	Override	
	Enable S Timeout	ession	⊠ <mark>2880</mark> Sest	o sion Timeou (secs)		DHC Assi	P Addr. gnment	Required	
	Aironet I	E	Enabled			OEAP			
	Diagnost <u>18</u>	ic Channel	Enabled			Spli	t Tunnel	Enabled	
	Override ACL	Interface	IPv4 None	· ~	IPv6 None 🗸	Manage	ement Frame Prote	ection (MFP)	
	Layer2 A URL ACL	cl	None ~			MFP	Client Protection 4	Optional 🗸	
	P2P Bloc	king Action	Disabled	~		DTIM P	eriod (in beacon in	tervals)	
	Client Ex	dusion ²	Enabled 60	meout Value (secs)	]	802.	11a/n (1 - 255)	1	
	Maximur Clients <mark>4</mark>	n Allowed	0			802. NAC	11b/g/n (1 - 255)	1	
<	Static IP	Tunneling	□- ·· ·			NAC	State None	$\overline{\mathbf{v}}$	>

#### 5단계. WLAN을 활성화합니다.

CLI:

> config wlan enable <wlan-id>
GUI:

이미지에 표시된 대로 General(일반) > Status(상태) > Tick Enabled(틱 활성화) > Apply(적용)를 클 릭합니다.

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

### freeRADIUS 데이터베이스에 사용자 추가

기본적으로 클라이언트는 PEAP 프로토콜을 사용하지만 freeRadius는 다른 방법을 지원합니다(이 설명서에서 다루지 않음). [root@tac-mxwireless ~]# nano /etc/raddb/users 2단계. 파일 하단에서 사용자 정보를 추가합니다.이 예에서 user1은 사용자 이름이고 Cisco123은 비밀번호입니다.

user1 Cleartext-Password := <Cisco123> 3단계. FreeRadius를 다시 시작합니다.

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

#### freeRADIUS의 인증서

FreeRADIUS에는 기본 CA(Certification Authority) 인증서 및 /etc/radb/certs 경로에 저장되는 디바 이스 인증서가 함께 제공됩니다. 이러한 인증서의 이름은 ca.pem 및 server.pem입니다 .server.pem은 클라이언트가 인증 프로세스를 진행하는 동안 수신하는 인증서입니다.EAP 인증을 위해 다른 인증서를 할당해야 하는 경우, 인증서를 삭제하고 동일한 이름으로 동일한 경로에 새 인 증서를 저장할 수 있습니다.

#### 최종 디바이스 컨피그레이션

802.1x 인증 및 PEAP/MS-CHAP(Challenge-Handshake Authentication Protocol의 Microsoft 버전) 버전 2를 사용하여 SSID에 연결하도록 랩톱 Windows 시스템을 구성합니다.

Windows 시스템에서 WLAN 프로파일을 생성하려면 다음 두 가지 옵션이 있습니다.

- 1. 인증을 완료하기 위해 freeRADIUS 서버를 검증하고 신뢰하도록 시스템에 자체 서명 인증서 를 설치합니다.
- 2. RADIUS 서버의 검증을 건너뛰고 인증을 수행하는 데 사용되는 모든 RADIUS 서버를 신뢰합니다(보안 문제가 될 수 있으므로 권장하지 않음). 이러한 옵션에 대한 컨피그레이션은 엔드디바이스 컨피그레이션 WLAN 프로파일 생성에서 설명합니다.

#### FreeRADIUS 인증서 가져오기

freeRADIUS에 설치된 기본 인증서를 사용하는 경우 freeRADIUS 서버에서 최종 디바이스로 EAP 인증서를 가져오려면 다음 단계를 수행합니다.

1단계. FreeRadius에서 인증서를 가져옵니다.

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

----BEGIN CERTIFICATE----

MIIE4TCCA8mgAwIBAgIJAKLmHn4eZLjBMA0GCSqGSIb3DQEBBQUAMIGTMQswCQYD VQQGEwJGUjEPMA0GA1UECBMGUmFkaXVzMRIwEAYDVQQHEwlTb21ld2hlcmUxFTAT BgNVBAoTDEV4YW1wbGUgSW5jLjEgMB4GCSqGSIb3DQEJARYRYWRtaW5AZXhhbXBs

ZS5jb20xJjAkBqNVBAMTHUV4YW1wbGUqQ2VydG1maWNhdGUqQXV0aG9yaXR5MB4X  ${\tt DTE3MDMzMTExMTIxNloXDTE3MDUzMDExMTIxNlowgZMxCzAJBgNVBAYTAkZSMQ8w}$ DQYDVQQIEwZSYWRpdXMxEjAQBgNVBAcTCVNvbWV3aGVyZTEVMBMGA1UEChMMRXhh b XBs ZSBJ bm MuMSAwHg YJKo ZIhvc NAQkBFhFh ZG1 pbk BlegFtc GxlLmNvbTEmMCQG and the second statement of the second statementA1UEAxMdRXhhbXBsZSBDZXJ0aWZpY2F0ZSBBdXRob3JpdHkwggEiMA0GCSqGSIb3 DQEBAQUAA4IBDwAwggEKAoIBAQC0vJ53NN7J9vhpKhcB3B00XLpeQFWjqolQOB9F /8Lh2Hax2rzb9wxOi1MOyXR+kN22H7RNwUHET8VdyGUsA4OdZWuyz18sKi5H42GU Eu6GDwlYJvhHn4rVC36OZU/Nbaxj0eR8ZG0JGse4ftQKLfckkvCOS5QGn4X1elRS oFe27HRF+pTDHd+nzbaDvhYWvFoe6iA27Od7AY/sDuo/tilJWGdm9ocPz3+0IiFC ay6dtG55YQOHxKaswH7/HJkLsKWhS4YmXLgJXCeeJqooqr+TEwyCDEaFaiX835Jp gwNNZ7X5US0FcjuuOtpJJ3hfQ8K6uXjEWPOkDE0DAnqp4/n9AgMBAAGjggE0MIIB MDAdBqNVHQ4EFqQUysFNRZKpAlcFCEqwdOPVGV0waLEwqcqGA1UdIwSBwDCBvYAU ys FNRZKpAlcFCEgwdOPVGV0 wa LGhgZmkgZYwgZMxCzAJBgNVBAYTAkZSMQ8wDQYDVQQIEwZSYWRpdXMxEjAQBgNVBAcTCVNvbWV3aGVyZTEVMBMGA1UEChMMRXhhbXBs ZSBJbmMuMSAwHgYJKoZIhvcNAQkBFhFhZG1pbkBleGFtcGxlLmNvbTEmMCQGA1UE AxMdRXhhbXBsZSBDZXJ0aWZpY2F0ZSBBdXRob3JpdHmCCQCi5h5+HmS4wTAMBqNV HRMEBTADAQH/MDYGA1UdHwQvMC0wK6ApoCeGJWh0dHA6Ly93d3cuZXhhbXBsZS5j b20vZXhhbXBsZV9jYS5jcmwwDQYJKoZIhvcNAQEFBQADqqEBACsPR2jiOFXnTsK4 1wnrrMy1ZZb12qDuqK+zKELox2mz1DMMK83tBsL8yjkv70KeZn821IzfTrTfvhzV mjX6HgaWfYyMjYYYSw/iEu2JsAtQdpvC3di10nGwVPHlzbozPdov8cZtCb21ynfY Z6cNjx8+aYQIcsRIyqA11XMOBwIXo141TOmoODdgfX951poLwgktRLkv17Y7owsz ChYDO++H7Iewsxx5pQfm56dA2cNrlTwWtMvViKyX7GlpwlbBOxgkLiFJ5+GFbfLh a0HBHZWhTKvffbr62mkbfjCUfJU4T3xgY9zFwiwT+BetCJgAGy8CT/qmnO+NJERO RUvDhfE =

----END CERTIFICATE----

2단계. 이전 단계의 출력을 복사하여 텍스트 파일에 붙여넣고 확장명을 .crt로 변경합니다.

#### 3단계. 파일을 두 번 클릭하고 인증서 설치...를 선택합니다. 이미지에 표시된 것처럼

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

4단계. 이미지에 표시된 대로 신뢰할 수 있는 루트 인증 기관 저장소에 인증서를 설치합니다.

Certificate Import Wizard	8
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.	
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 Back Next > Cancellance Back Next > Cancell	el
OK Cancel OK	

#### WLAN 프로파일 생성

1단계. 시작 아이콘을 마우스 오른쪽 버튼으로 클릭하고 이미지에 표시된 대로 **제어판**을 선택합니 다.

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 🛄 🕨 Downl 👽 Networ 👽	1

2단계. Network and Internet(네트워크 및 인터넷) > Network and Sharing Center(네트워크 및 공유 센터)> 이미지에 표시된 대로 Set up a new connection or network(새 연결 또는 네트워크 설정)를 클릭합니다.

💐 Network and Sharing Cente	r	
🔶 🚽 🗸 🛧 💆 🔸 Control F	anel > Network and Internet > Network	and Sharing Center
Control Panel Home	View your basic network inforr	mation and set up connections
Change adapter settings	View your active networks	
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 ne Set up a broadband, dial-up, o Troubleshoot problems Diagnose and repair network p	etwork or VPN connection; or set up a router or access point. problems, or get troubleshooting information.

3단계. 무선 네트워크에 수동으로 연결을 선택하고 이미지에 표시된 다음을 클릭합니다.

	-	• 0	- ×
🛬 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.			
Connect to a workplace			
Set up a dial-up or VPN connection to your workplace.			
		_	
	Next		Cancel

4단계. SSID 및 보안 유형 WPA2-Enterprise의 이름으로 정보를 입력하고 이미지에 표시된 **다음**을 클릭합니다.

<i>←</i>	Se Manually connect to	a wireless network	-		×
	Enter information	for the wireless network you want to add			
	Network name:	SSID-name			
	Security type:	WPA2-Enterprise ~			
	Encryption type:	AES			
	Security Key:	Hide characte	15		
	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 risk			
		N	ext	Can	cel

5단계. 이미지에 표시된 대로 WLAN 프로파일의 컨피그레이션을 사용자 지정하려면 **연결 설정 변** 경을 선택합니다.

	-		$\times$
<ul> <li>Search State Stat</li></ul>			
Successfully added ise-ssid			
→ Change connection settings			
Open the connection properties so that I can change the settings.			
		-	
		Clo	se

6단계. **보안** 탭으로 이동하고 이미지에 표시된 대로 **설정**을 클릭합니다.

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

7단계. RADIUS 서버가 유효한지 여부를 선택합니다.

대답이 "예"인 경우 **인증서**와 **신뢰할 수 있는 루트 인증 기관**에서 **인증서를 검증하여 서버 ID 확인 을 활성화합니다.**list 는 freeRADIUS의 자체 서명 인증서를 선택합니다.

그런 다음 **Configure** and disable **Automatically use my Windows logon name and password...를** 선택하고 이미지에 표시된 대로 OK(확인)를 클릭합니다.

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:	- 1
Eacht & Clefest to seal	^
Let 11 1996 Assaults of face by	
E Constantino de Const	
List som to be	
Example Certification Authority	
Contract Contraction for the	
to an alternate better water in a solar trap ( 1999)	
Equilation of Control Control States	~
< >	
Notifications before connecting:	_
Tall uses if the sense name or root cartificate isn't specified	
Tell user if the server name or root certificate isn't specified	~
Select Authentication Method:	
Secured password (EAP-MSCHAP v2) Configur	P
conngu	
Enable Fast Reconnect	
Disconnect if server does not present cryptobinding TLV	
Enable Identity Privacy	
OK Cance	el
EAP MSCHAPv2 Properties ×	
14 from compositions	

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

8단계. 사용자 자격 증명을 구성합니다.

Security(보안) 탭으로 다시 돌아와서 Advanced(고급) 설정을 선택하고 인증 모드를 User authentication(사용자 인증)으로 지정하고 이미지에 표시된 대로 사용자를 인증하기 위해 freeRADIUS에 구성된 자격 증명을 저장합니다.

ise-ssid Wireless Network Properties $\times$				
Connection Security				
Security type:	WPA2-Enterprise	1	~	
Encryption type:	AES		~	1
Choose a network aut	thentication metho	d:		
Microsoft: Protected	EAP (PEAP)	Y	Settings	
Remember my credentials for this connection each time I'm logged on				
Advanced settings				
Planatices security				
		OK		Cancel

User authentication	Save c	redentials
Delete credentials for all users		
Enable single sign on for this netw	vork	
Perform immediately before u	iser logon	
<ul> <li>Perform immediately after use</li> </ul>	er logon	
Maximum delay (seconds):	10	*
Allow additional dialogs to be sign on	displayed during	single
This network uses separate vi and user authentication	rtual LANs for ma	achine
		Consul.
	OK	Cancel

### Save credentials

Saving your credentials allows your computer to connect to the network when you're not logged on (for example, to download updates).

×

սիսիս	user1	
cisco	•••••••	
		OK Cancel

# 다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

#### WLC의 인증 프로세스

특정 사용자에 대한 인증 프로세스를 모니터링하려면 다음 명령을 실행합니다.

> debug client <mac-add-client>

> debug dot1x event enable

> debug dot1x aaa enable

디버그 클라이언트 출력을 쉽게 읽을 수 있도록 무선 디버그 분석기 도구를 사용합니다.

<u>무선 디버그 분석기</u>

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.