802.1x 구성 - FreeRadius 및 WLC 8.3을 사용하는 PEAP

목차

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 대해 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 예를 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

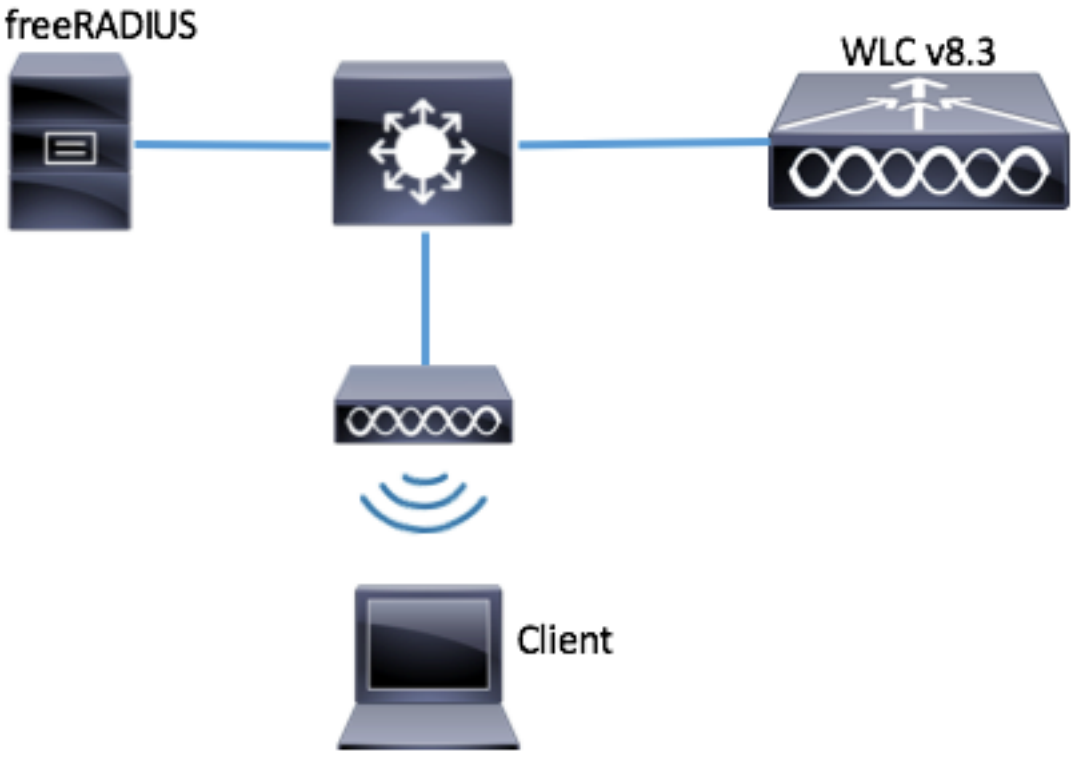
이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 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 디바이스는 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 update
```

```
[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 ~]# 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
```

FreeRADIUS 설치

1단계. 이 명령을 실행하여 FreeRADIUS를 설치합니다.

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

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
```

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.

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

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

```
[root@tac-mxwireless ~]# firewall-cmd --get-services | egrep 'http|https|radius'
[root@tac-mxwireless ~]# firewall-cmd --add-service={http,https,radius} --permanent success
```

6단계. 변경 사항을 적용하려면 방화벽을 다시 로드합니다.

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

자유 RADIUS

MariaDB를 사용하도록 FreeRADIUS를 구성하려면 다음 단계를 수행합니다.

1단계. RADIUS 데이터베이스 구성표를 가져와 RADIUS 데이터베이스를 채웁니다.

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

2단계. **/etc/**radb**/mods**가 활성화된 SQL(Structured Query Language)에 대한 소프트 링크**를 생성합니다**.

```
[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 환경에 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/sql을 radiusd**로 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.conf**를 편집합니다.

```
[root@tac-mxwireless ~]# vim /etc/raddb/clients.conf
```

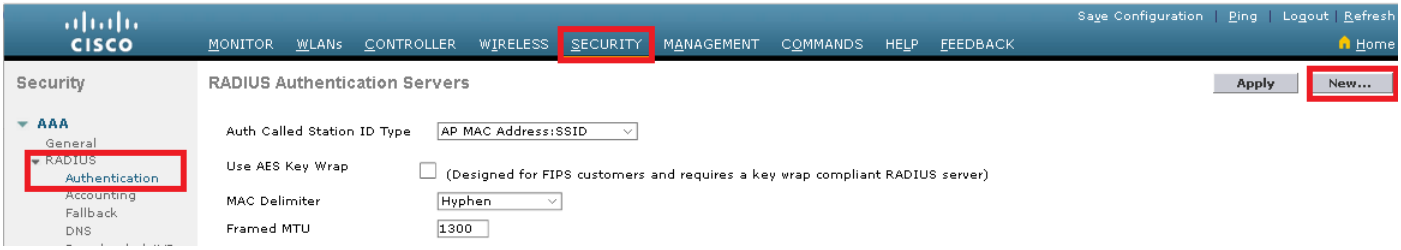
2단계. 하단에서 컨트롤러 IP 주소와 공유 키를 추가합니다.

```
client{ secret = shortname = }
```

WLC의 RADIUS 서버로 FreeRADIUS

GUI:

1단계. WLC의 GUI를 열고 이미지에 표시된 대로 **SECURITY > RADIUS > Authentication > New**로 이동합니다.



2단계. 이미지에 표시된 대로 RADIUS 서버 정보를 채웁니다.

CLI:

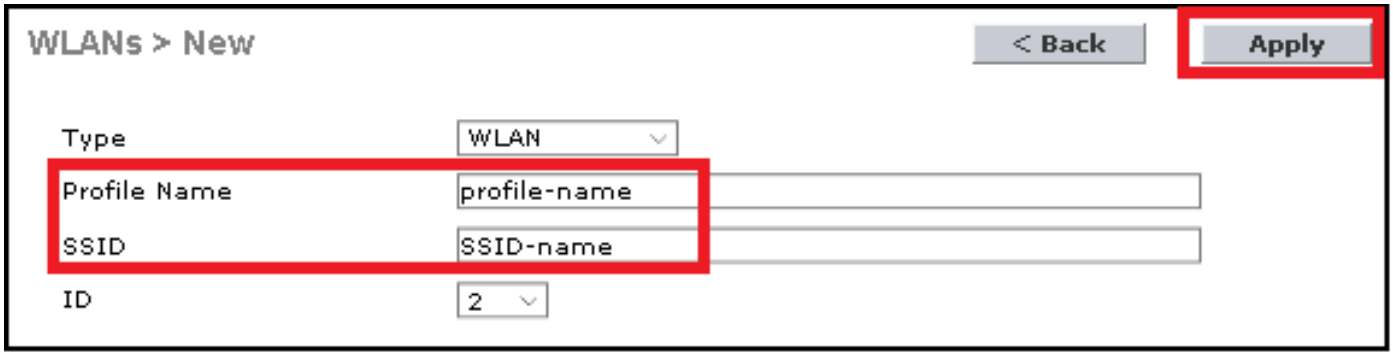
```
> config radius auth add <index> <radius-ip-address> 1812 ascii <shared-key>
> config radius auth disable <index>
> config radius auth retransmit-timeout <index> <timeout-seconds>
> config radius auth enable <index>
```

WLAN

GUI:

1단계. WLC의 GUI를 열고 이미지에 표시된 **WLANs > Create New > Goas**로 이동합니다.

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



CLI:

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

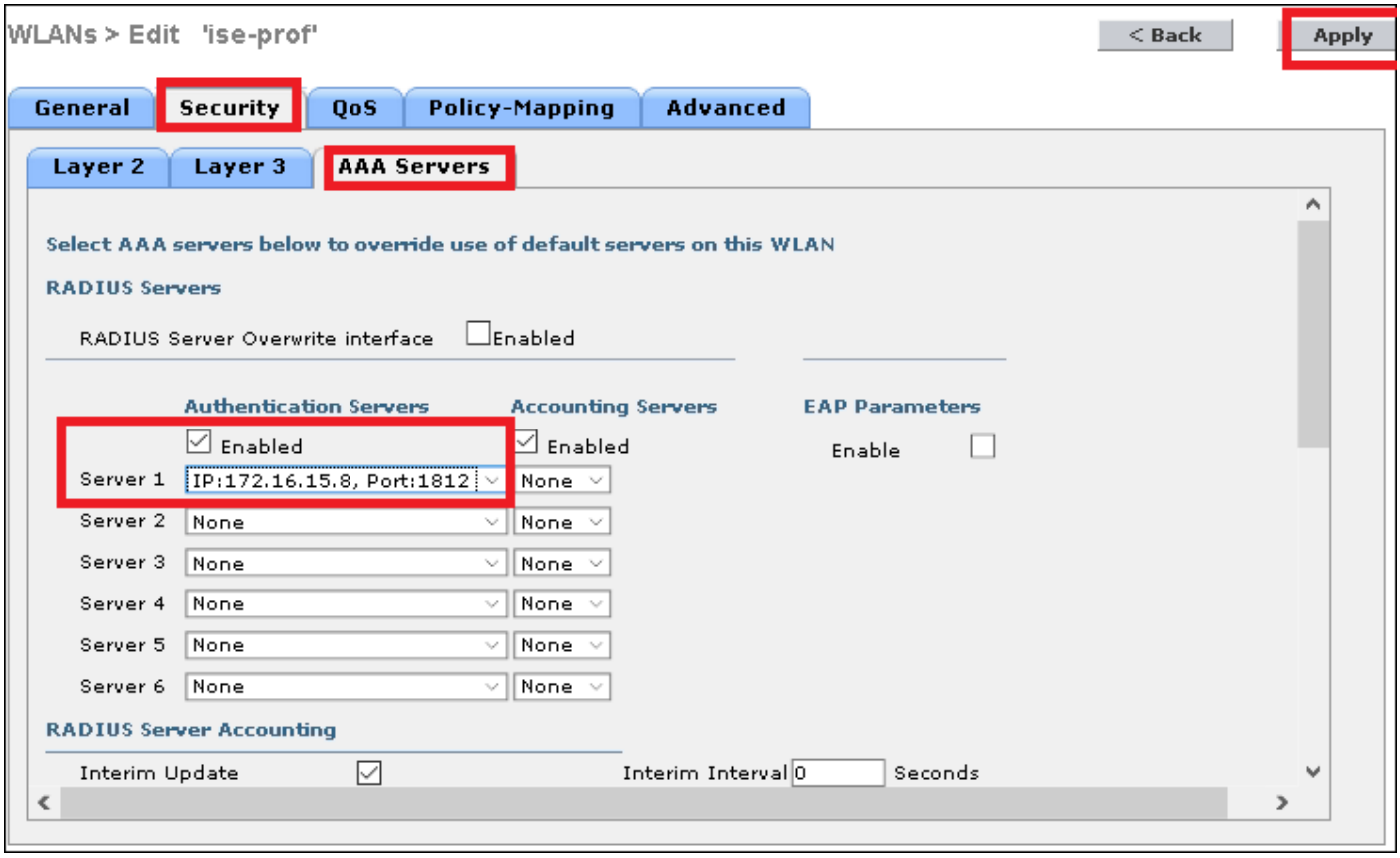
3단계. WLAN에 RADIUS 서버를 할당합니다.

CLI:

```
> config wlan radius_server auth add <wlan-id> <radius-index>
```

GUI:

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



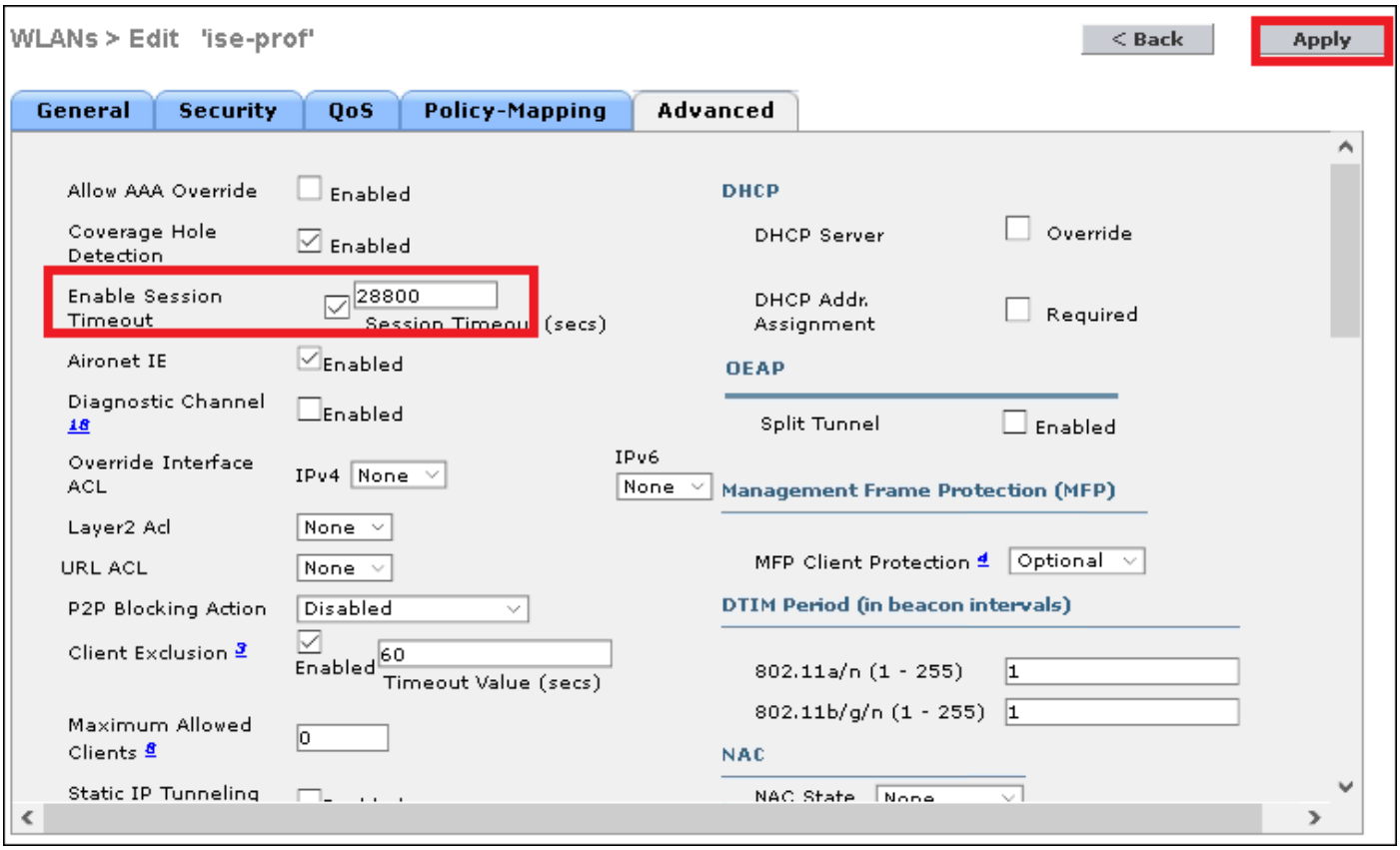
4단계. 선택적으로 세션 시간을 늘립니다.

CLI:

```
> config wlan session-timeout <wlan-id> <session-timeout-seconds>
```

GUI:

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



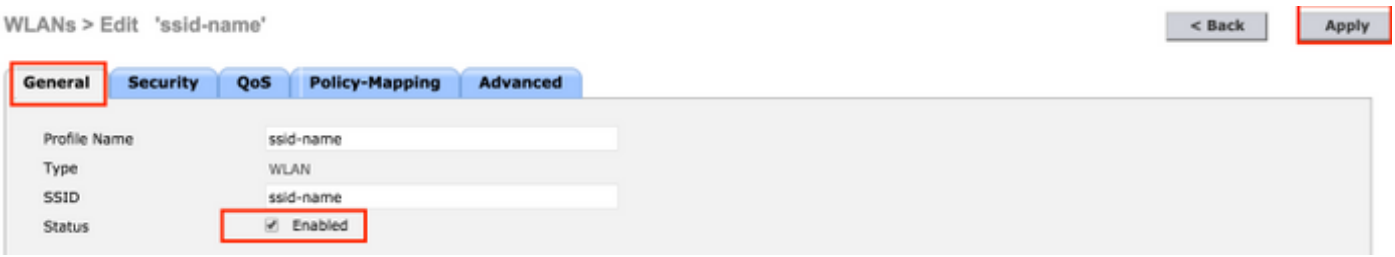
5단계. WLAN을 활성화합니다.

CLI:

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

GUI:

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



freeRADIUS 데이터베이스에 사용자 추가

기본적으로 클라이언트는 PEAP 프로토콜을 사용하지만 freeRadius는 다른 방법을 지원합니다(이 설명서에서 다루지 않음).

1단계. 파일 **/etc/radb/users를 편집합니다**.

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

2단계. 파일 하단에서 사용자 정보를 추가합니다.이 예에서 **user1**은 사용자 이름이고 **Cisco123**은 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 디바이스 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 인증서를 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 인증서를 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 엔드 디바이스 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.

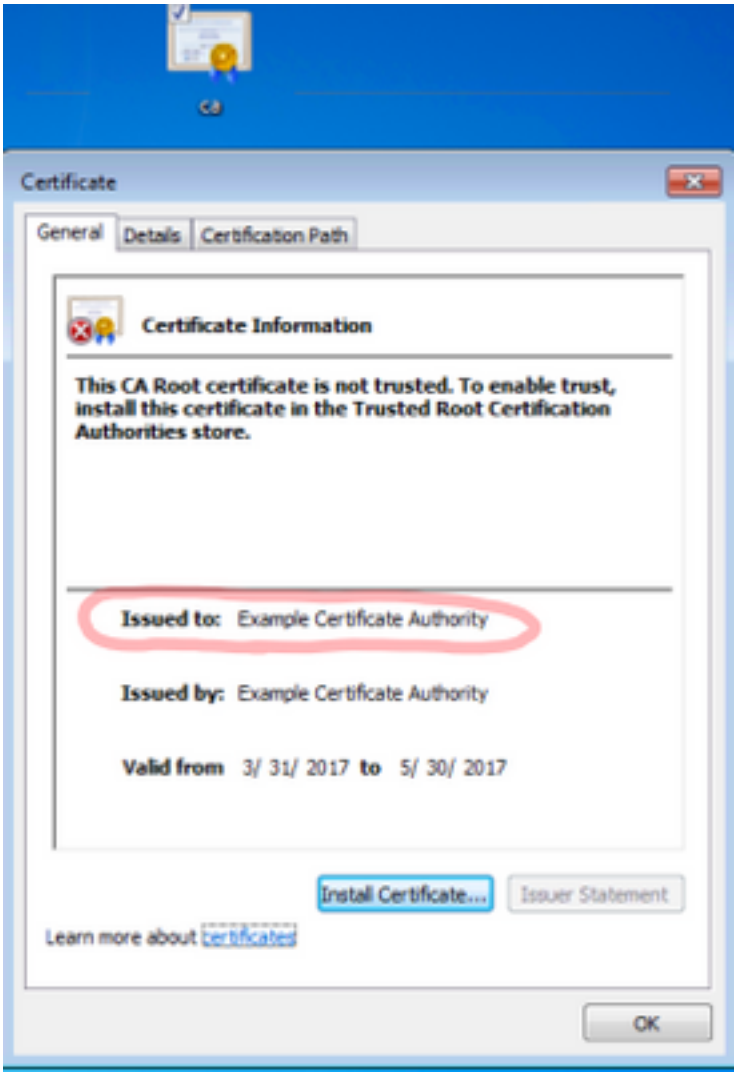
```
[root@tac-mxwireless ~]# cat /etc/raddb/certs/ca.pem

-----BEGIN CERTIFICATE-----
MIIE4TCCA8mgAwIBAgIJAKLmHn4eZLjBMA0GCSqGSIb3DQEBBQUAMIGTMQswCQYD
VQQGEwJGUjEPMA0GA1UECBMGUmFkaXVzMRIwEAYDVQQHEwlTb21ld2hlcmUxFTAT
BgNVBAoTDEV4YW1wbGUgSW5jLjEgMB4GCSqGSIb3DQEJARYRYWRtaW5AZXhhbXBs
```

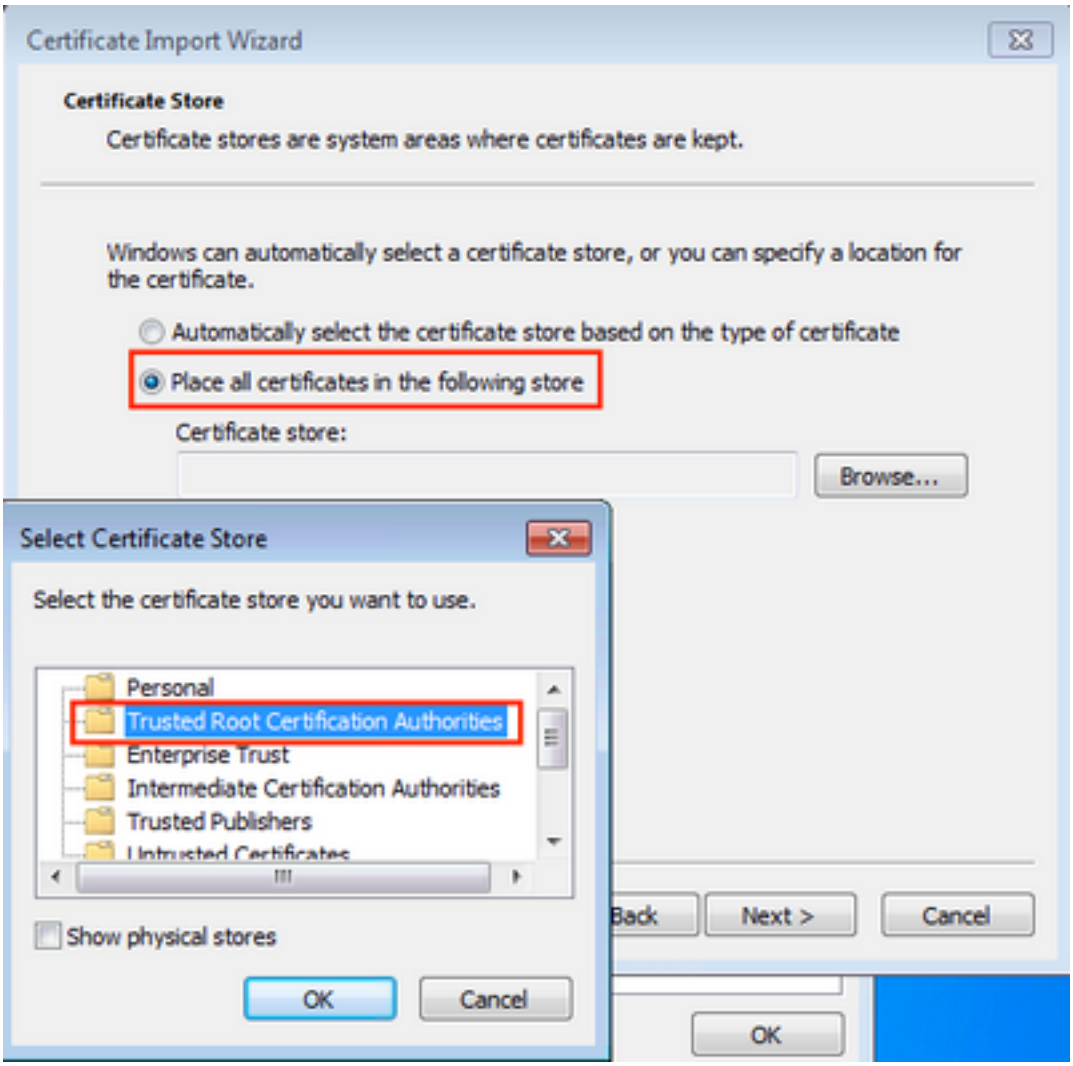
```
ZS5jb20xJjAkBgNVBAMTHUV4YW1wbGUgQ2VydGlmaWNhdGUgQXV0aG9yaXR5MB4X
DTE3MDMzMTExMTIxNloXDTE3MDUzMDExMTIxNlowgZMxCzAJBgNVBAYTAkZSMQ8w
DQYDVQQIEwZSYWRpdXMxEjAQBgNVBAcTCVNvbWV3aGVyZTEVMBMGA1UEChMMRXhh
bXBsZSBJbmMuMSAwHgYJKoZIhvcNAQkBFhFhZG1pbkBleGFtcGxlLmNvbTEmMCQG
A1UEAxMdRXhhbXBsZSBDZXJ0aWZpY2F0ZSBBdXRob3JpdHkwggEiMA0GCSqGSIb3
DQEBAQUAA4IBDwAwggEKAoIBAQC0vJ53NN7J9vhpKhcB3B0OXLpeQFWjqolQOB9F
/8Lh2Hax2rzb9wxOi1MOyXR+kN22H7RNwUHET8VdyGUsA4OdZWuyzI8sKi5H42GU
Eu6GDw1YJvhHn4rVC36OZU/Nbaxj0eR8ZG0JGse4ftQKLfckkvCOS5QGn4X1elRS
oFe27HRF+pTDHd+nzbaDvhYWvFoe6iA27Od7AY/sDuo/tiIJWGdm9ocPz3+0IiFC
ay6dtG55YQOHxKaswH7/HJkLsKWhS4YmXLgJXCeeJqooqr+TEwyCDEaFaiX835Jp
gwNNZ7X5US0FcjuuOtpJJ3hfQ8K6uXjEWPOkDE0DAnqp4/n9AgMBAAGjggE0MIIB
MDAdBgNVHQ4EFgQUysFNRZKpAlcFCEgwdOPVGV0waLEwgcgGA1UdIwSBwDCBvYAU
ysFNRZKpAlcFCEgwdOPVGV0waLGhgZmkgZYwgZMxCzAJBgNVBAYTAkZSMQ8wDQYD
VQQIEwZSYWRpdXMxEjAQBgNVBAcTCVNvbWV3aGVyZTEVMBMGA1UEChMMRXhhbXBs
ZSBJbmMuMSAwHgYJKoZIhvcNAQkBFhFhZG1pbkBleGFtcGxlLmNvbTEmMCQGA1UE
AxMdRXhhbXBsZSBDZXJ0aWZpY2F0ZSBBdXRob3JpdHmCCQCi5h5+HmS4wTAMBgNV
HRMEBTADAQH/MDYGA1UdHwQvMC0wK6ApoCeGJWh0dHA6Ly93d3cuZXhhbXBsZS5j
b20vZXhhbXBsZV9jYS5jcmwwDQYJKoZIhvcNAQEFBQADggEBACsPR2jiOFXnTsK4
1wnrrMylZZb12gDuqK+zKELox2mzlDMMK83tBsL8yjkv70KeZn821IzfTrTfvhzV
mjX6HgaWfYyMjYYYSw/iEu2JsAtQdpvC3di10nGwVPHlzbozPdov8cZtCb21ynfY
Z6cNjx8+aYQIcsRIyqA1IXMOBwIXo141TOmoODdgfX95lpoLwgktRLkvl7Y7owsz
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

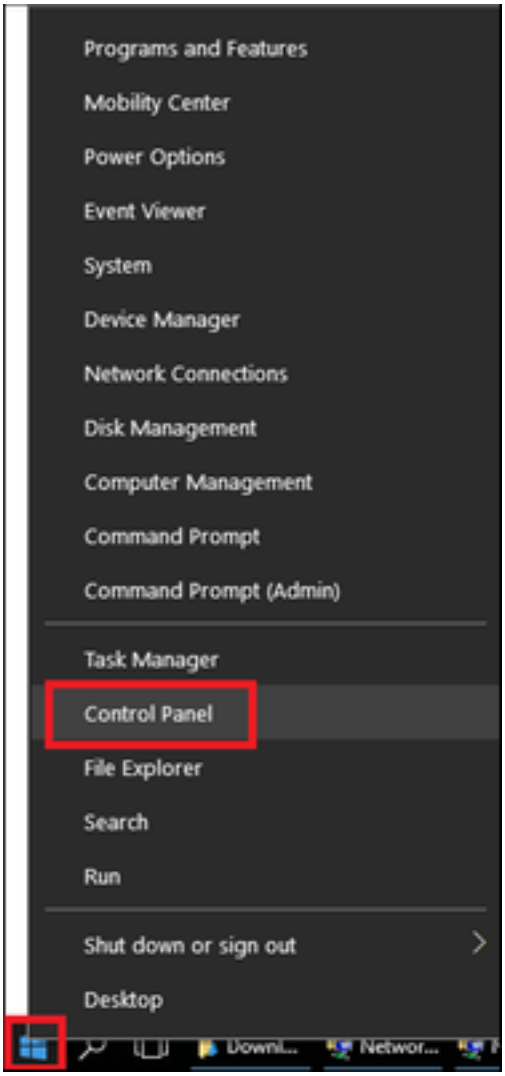


4단계. 이미지에 표시된 대로 신뢰할 수 있는 **루트 인증 기관** 저장소에 인증서를 설치합니다.

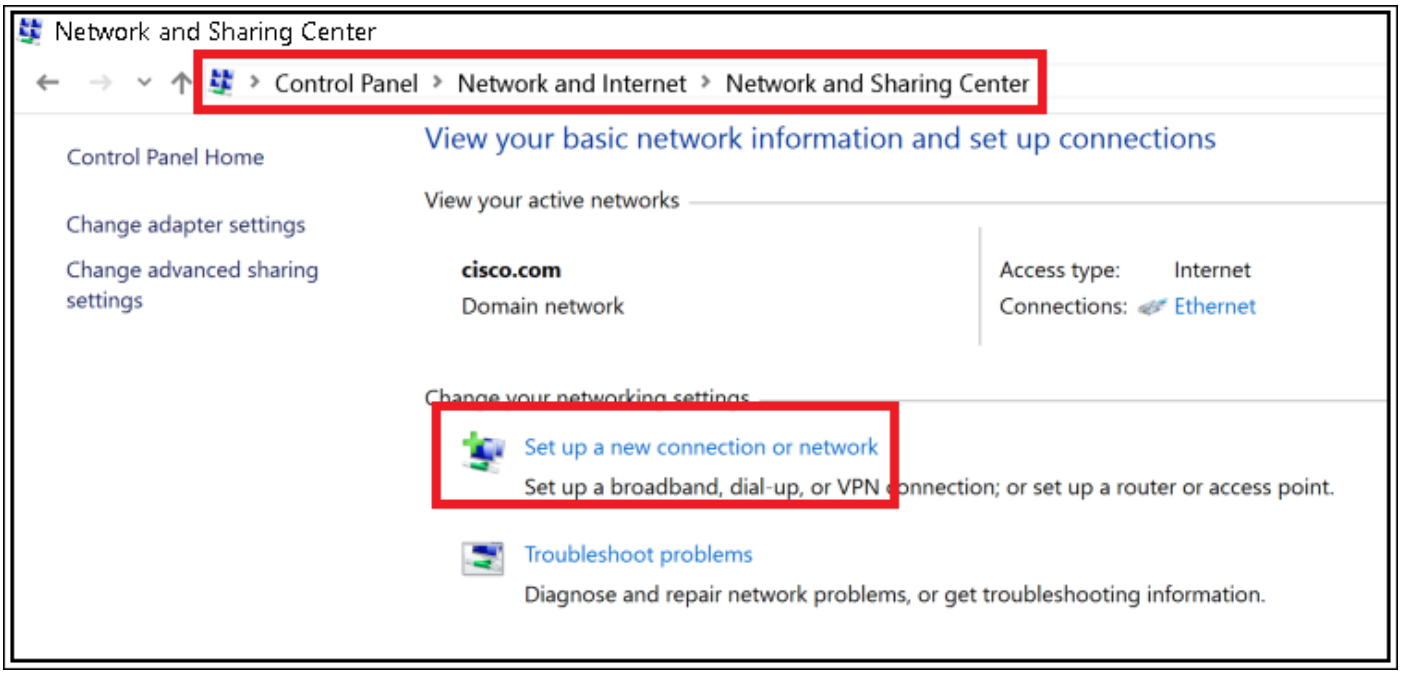


WLAN 프로파일 생성

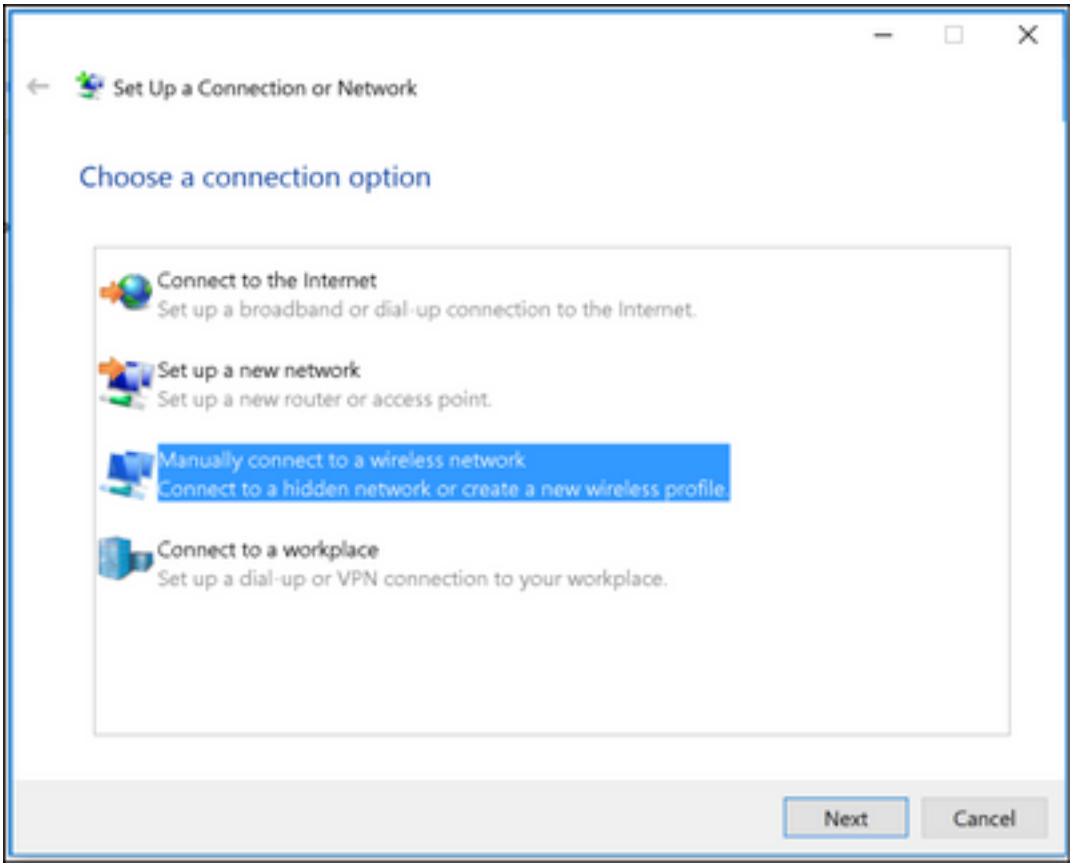
1단계. 시작 아이콘을 마우스 오른쪽 버튼으로 클릭하고 이미지에 표시된 대로 **제어판**을 선택합니다.



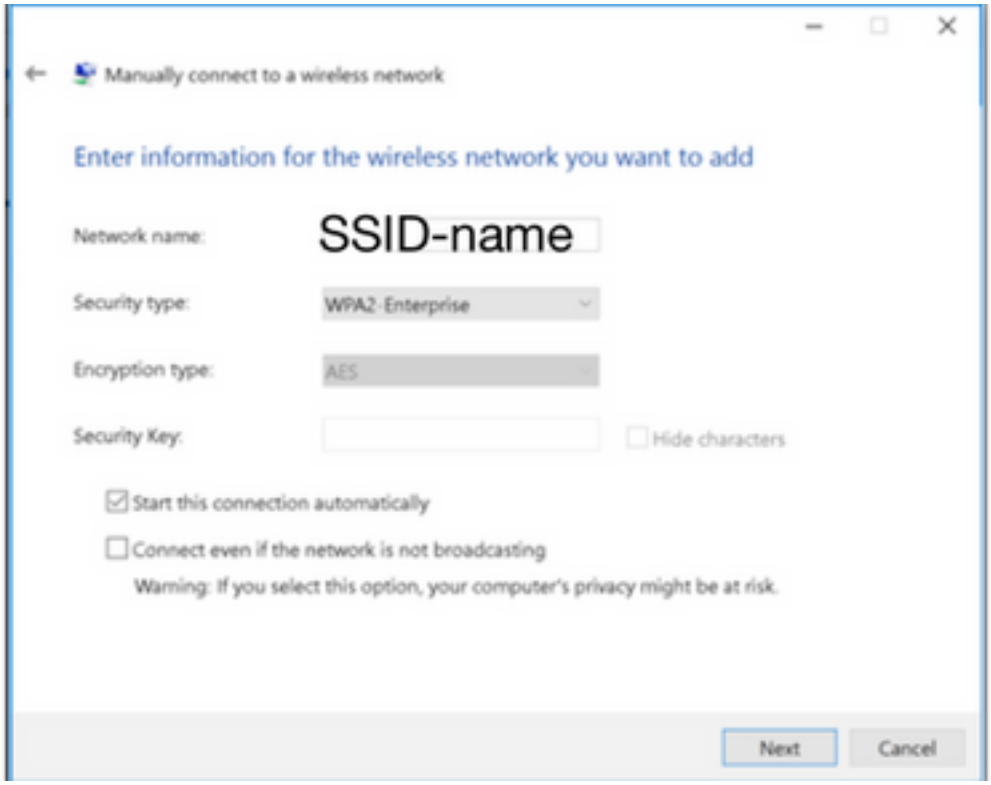
2단계. Network **and Internet(네트워크 및 인터넷) > Network and Sharing Center(네트워크 및 공유 센터)>** 이미지에 표시된 대로 **Set up a new connection or network(새 연결 또는 네트워크 설정)를 클릭합니다**.



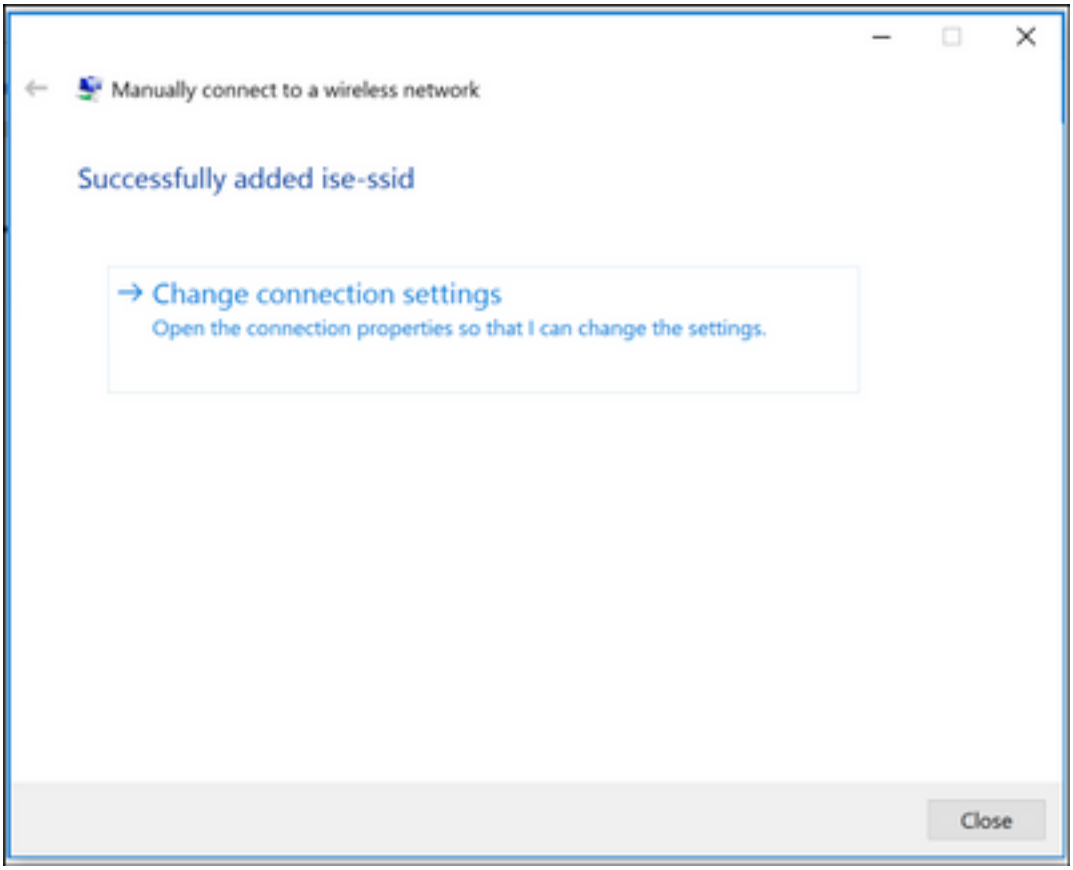
3단계. **무선 네트워크에 수동으로 연결**을 선택하고 이미지에 표시된 다음**을** 클릭합니다.



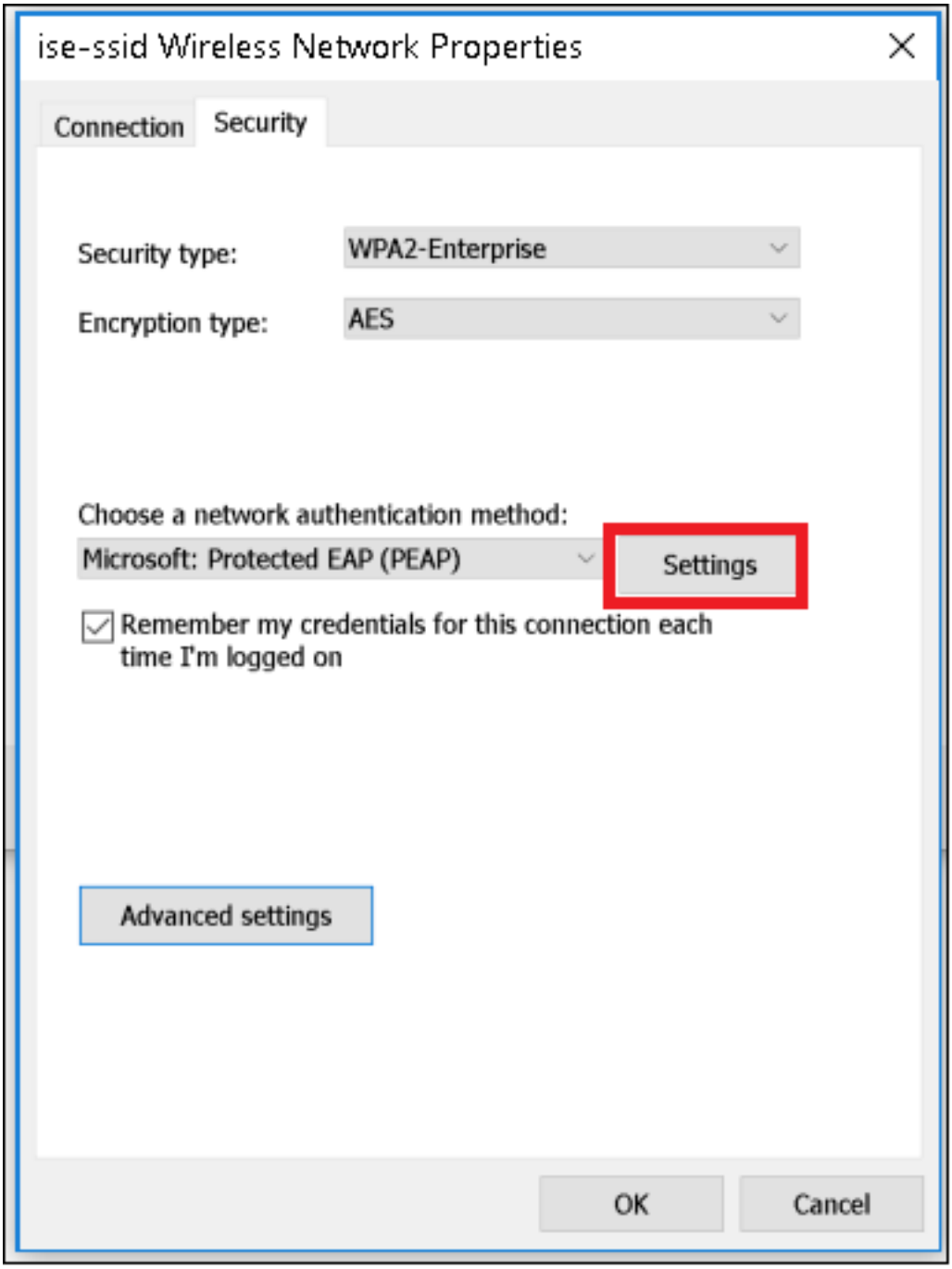
4단계. SSID 및 보안 유형 WPA2-Enterprise의 이름으로 정보를 입력하고 이미지에 표시된 **다음**을 클릭합니다.



5단계. 이미지에 표시된 대로 WLAN 프로파일의 컨피그레이션을 사용자 지정하려면 **연결 설정 변경**을 선택합니다.



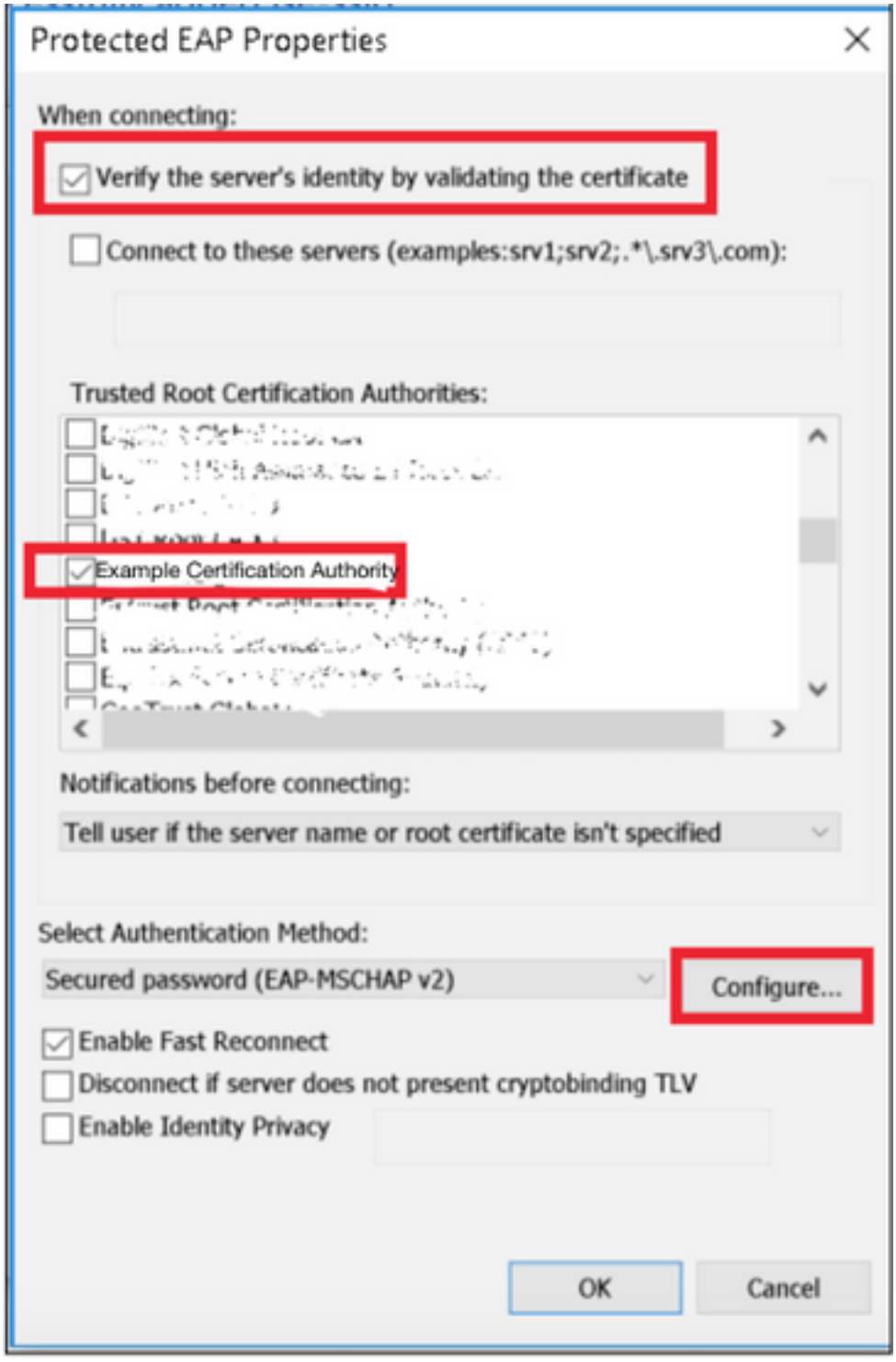
6단계. **보안** 탭으로 이동하고 이미지에 표시된 대로 **설정**을 클릭합니다.

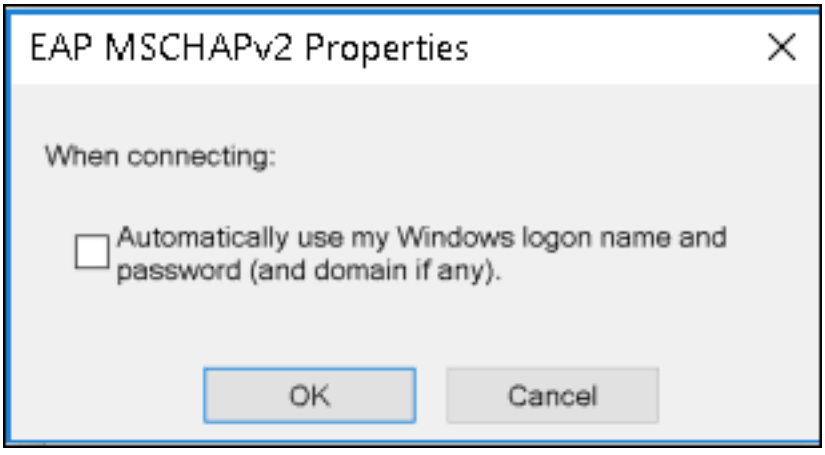


7단계. RADIUS 서버가 유효한지 여부를 선택합니다.

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

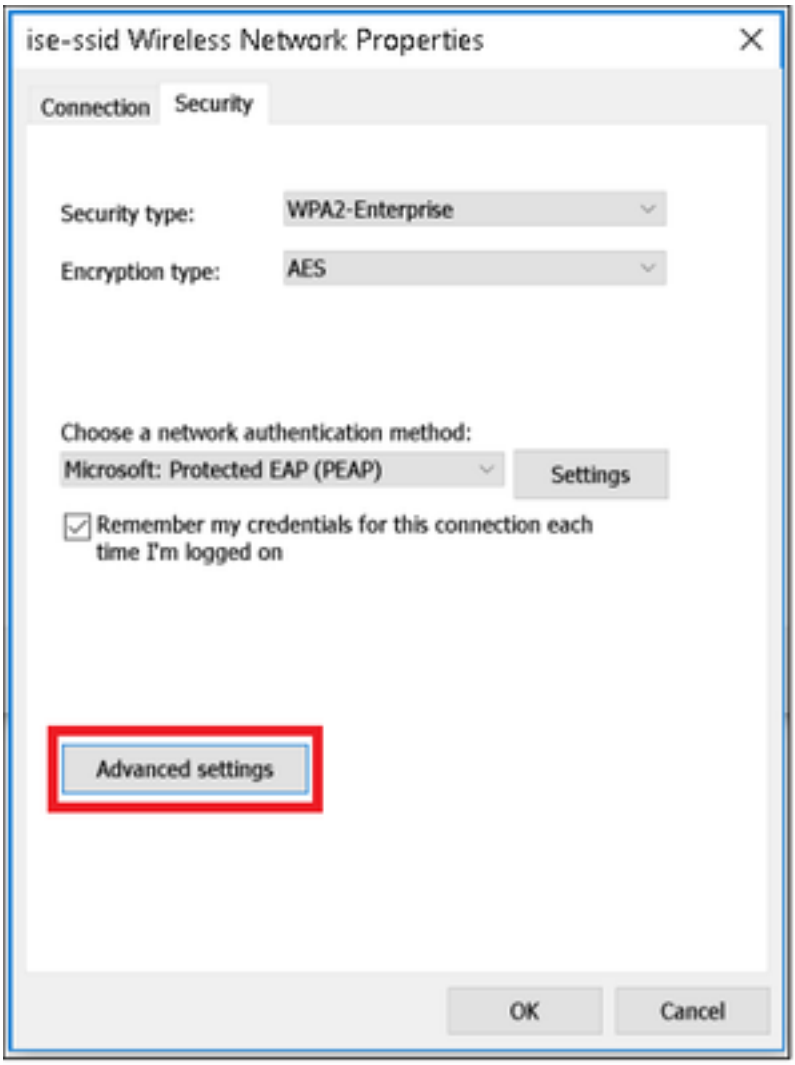
그런 다음 **Configure** and disable **Automatically use my Windows logon name and password...**를 선택하고 이미지에 표시된 대로 OK(확인)를 클릭합니다.

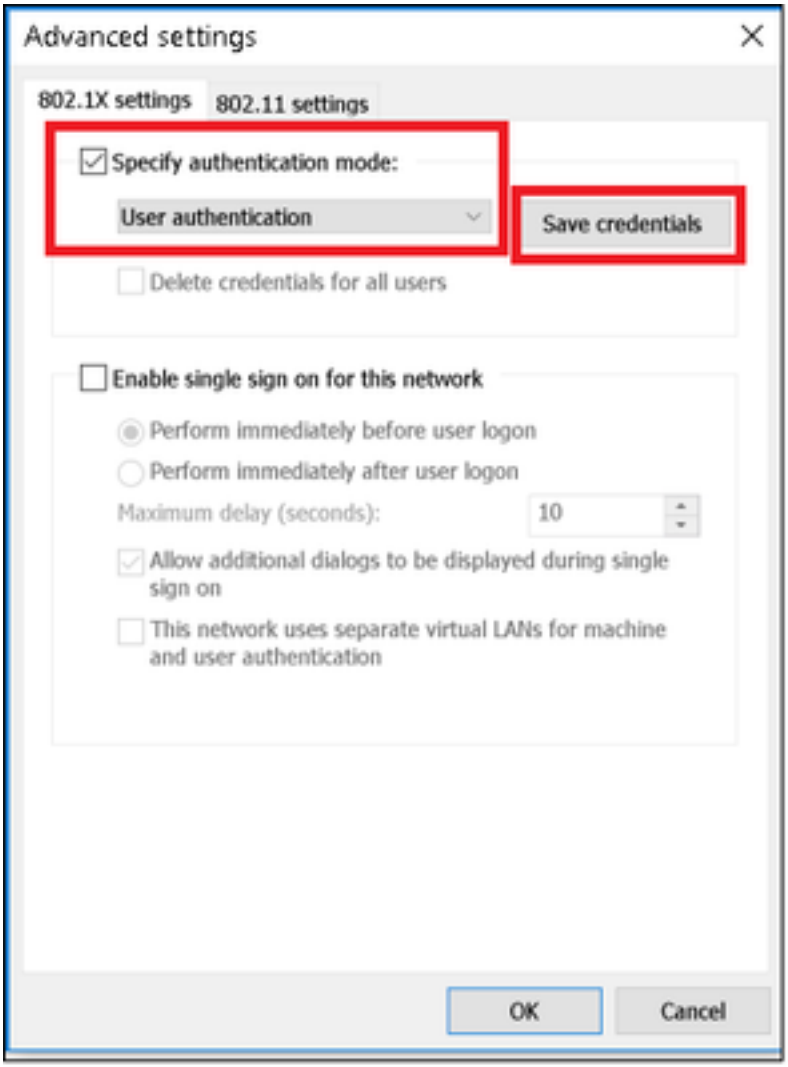


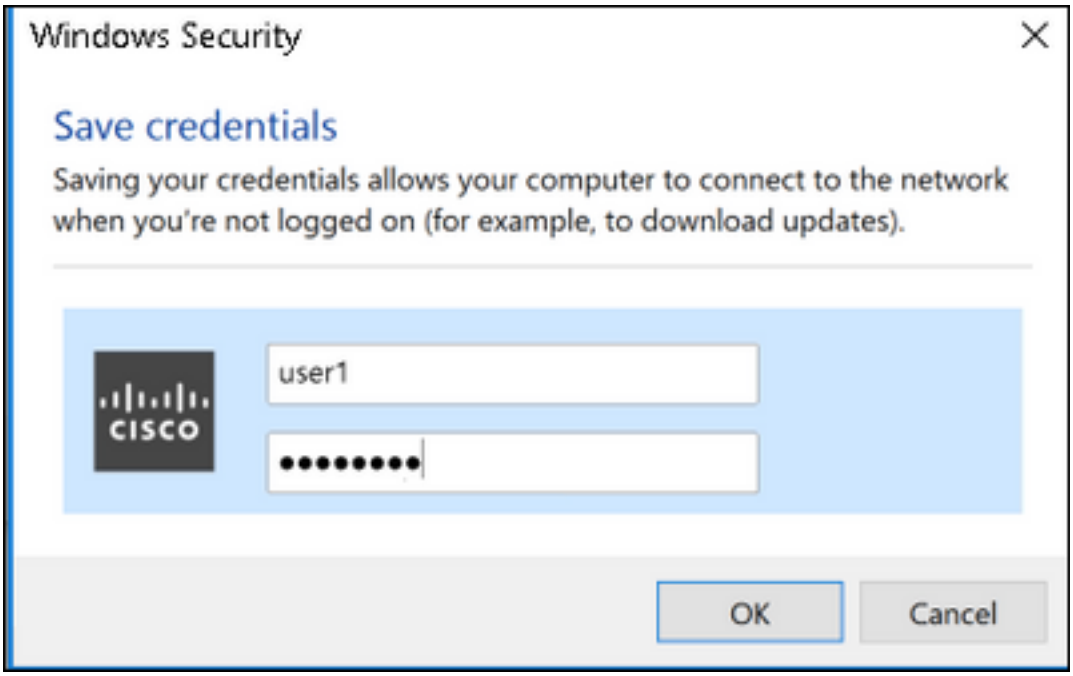


8단계. 사용자 자격 증명을 구성합니다.

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







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.

무선 디버그 분석기

문제 해결

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