802.1x WLAN + VLAN 재정의(Mobility Express(ME) 8.2 및 ISE 2.1)

목차

소개
사전 요구 사항
요구 사항
사용되는 구성 요소
구성
네트워크 다이어그램
구성
ME의 구성
ISE에서 ME 선언
ISE에서 새 사용자 생성
인증 규칙 생성
권한 부여 규칙 생성
엔드 디바이스 구성
다음을 확인합니다.
ME의 인증 프로세스
ISE의 인증 프로세스

소개

이 문서에서는 Mobility Express 컨트롤러 및 외부 원격 RADIUS(Remote Authentication Dial-In User Service) 서버를 사용하여 Wi-Fi Protected Access 2(WPA2) 엔터프라이즈 보안을 사용하여 WLAN(Wireless Local Area Network)을 설정하는 방법에 대해 설명합니다.ISE(Identity Service Engine)는 외부 RADIUS 서버의 예로 사용됩니다.

이 가이드에서 사용되는 EAP(Extensible Authentication Protocol)는 PEAP(Protected Extensible Authentication Protocol)입니다. 클라이언트가 특정 VLAN에 할당된다는 것 외에도(WLAN에 지정된 VLAN이 아닌).

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 802.1x
- PEAP
- 인증 기관(CA)
- 인증서

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

ME v8.2

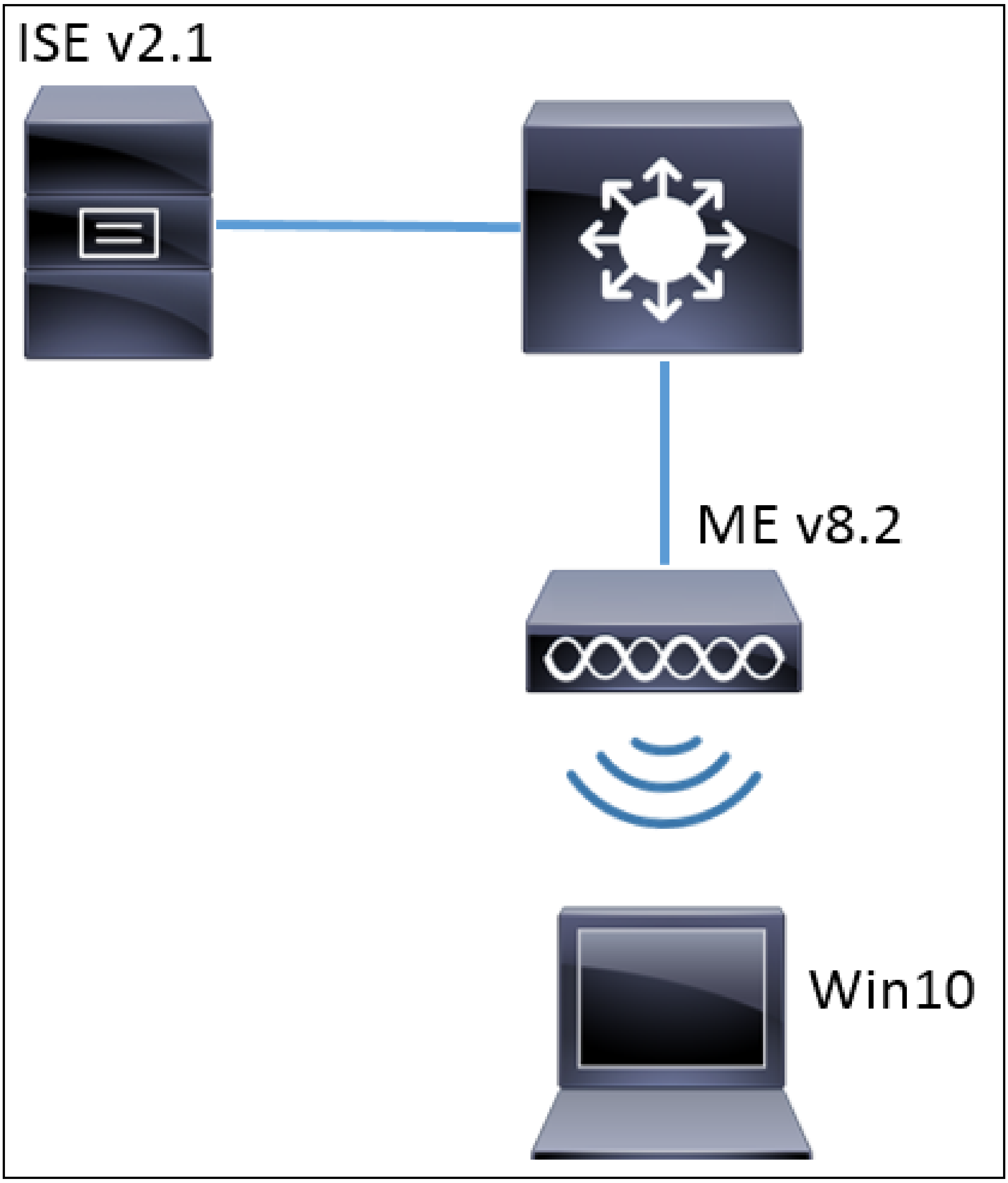
ISE v2.1

Windows 10 랩톱

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



구성

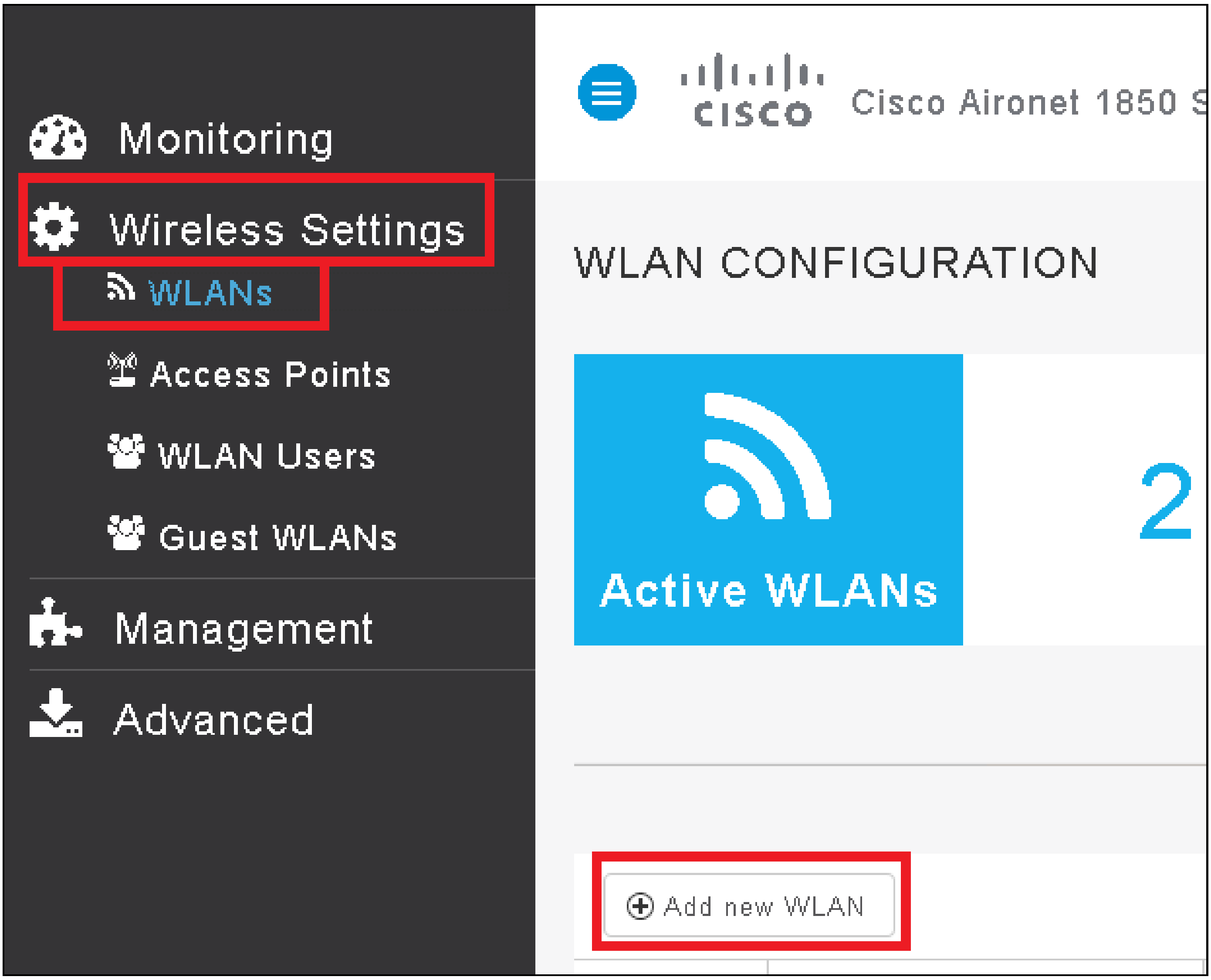
일반적인 단계는 다음과 같습니다.

1. ME에서 SSID(Service Set Identifier)를 생성하고 ME에서 RADIUS 서버(이 예에서는 ISE)를 선언합니다.
2. RADIUS 서버(ISE)에서 ME 선언
3. ISE에서 인증 규칙 생성
4. ISE에서 권한 부여 규칙 생성
5. 엔드포인트 구성

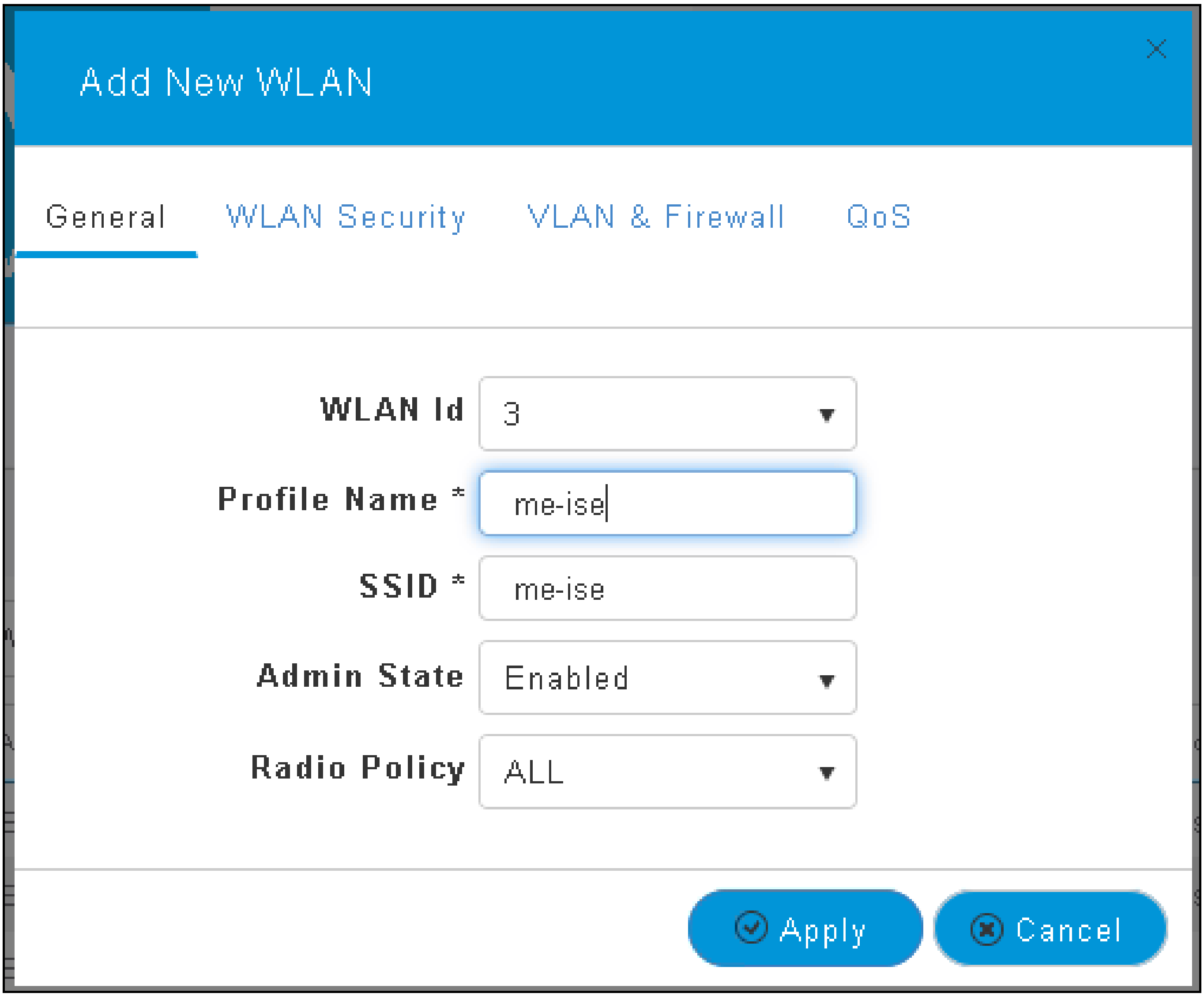
ME의 구성

RADIUS 서버와 ME 간의 통신을 허용하려면 ME에서 RADIUS 서버를 등록하고 그 반대의 경우 RADIUS 서버를 등록해야 합니다.이 단계에서는 RADIUS 서버를 ME에 등록하는 방법을 보여줍니다.

1단계. ME의 GUI를 열고 **Wireless Settings(무선 설정) > WLANs(WLAN) > Add new WLAN(새 WLAN 추가).**



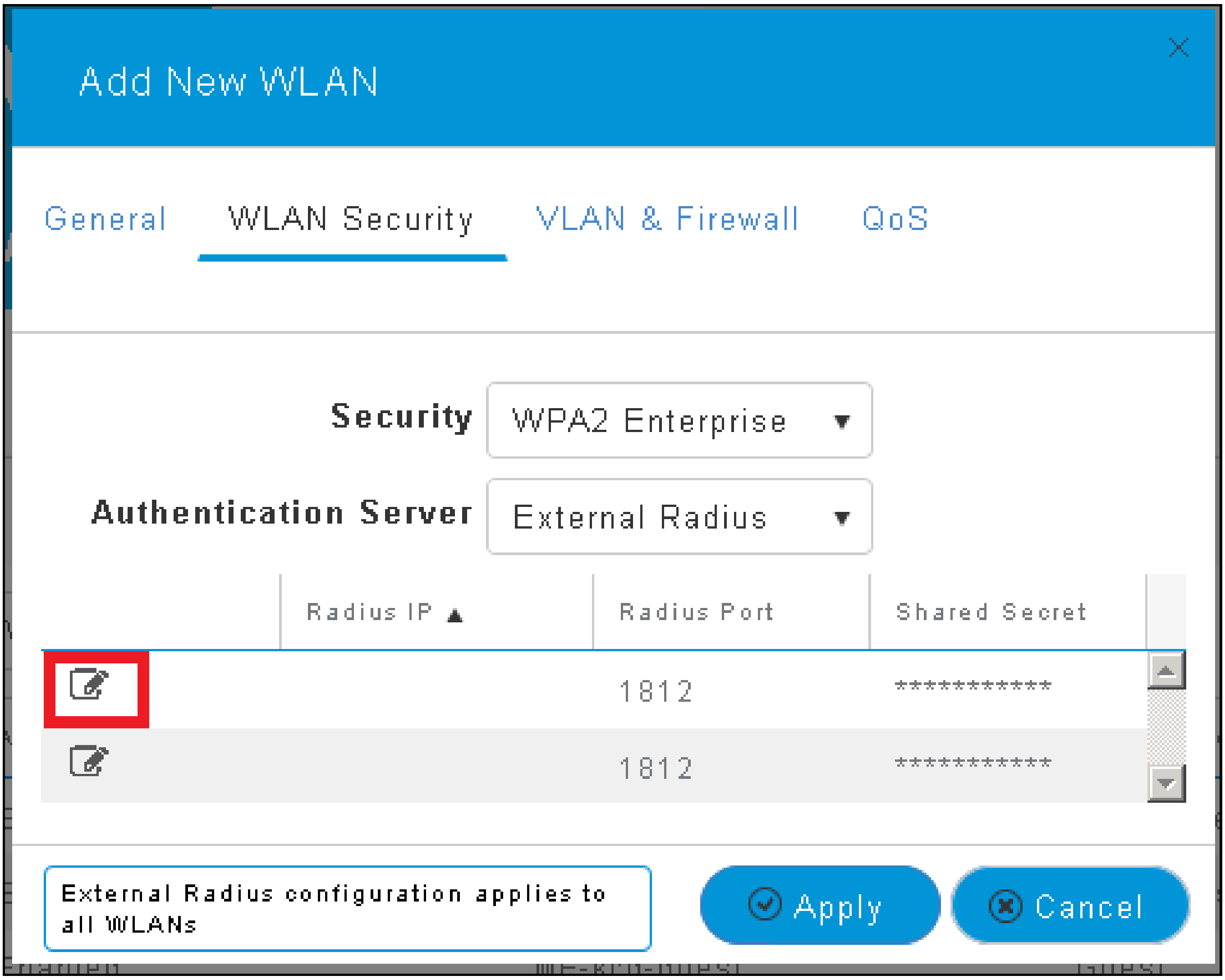
2단계. WLAN의 이름을 선택합니다.



WLAN Id: 3 ▾
Profile Name *: me-ise
SSID *: me-ise
Admin State: Enabled ▾
Radio Policy: ALL ▾

3단계. **WLAN Security(WLAN 보안**) 탭 아래에서 Security configuration(보안 컨피그레이션)을 지정합니다.

WPA2 **Enterprise를** 선택합니다. 인증 서버에서는 **외부 RADIUS를** 선택합니다.수정 옵션을 클릭하여 RADIUS의 IP 주소를 추가하고 **공유 암호** 키를 선택합니다.

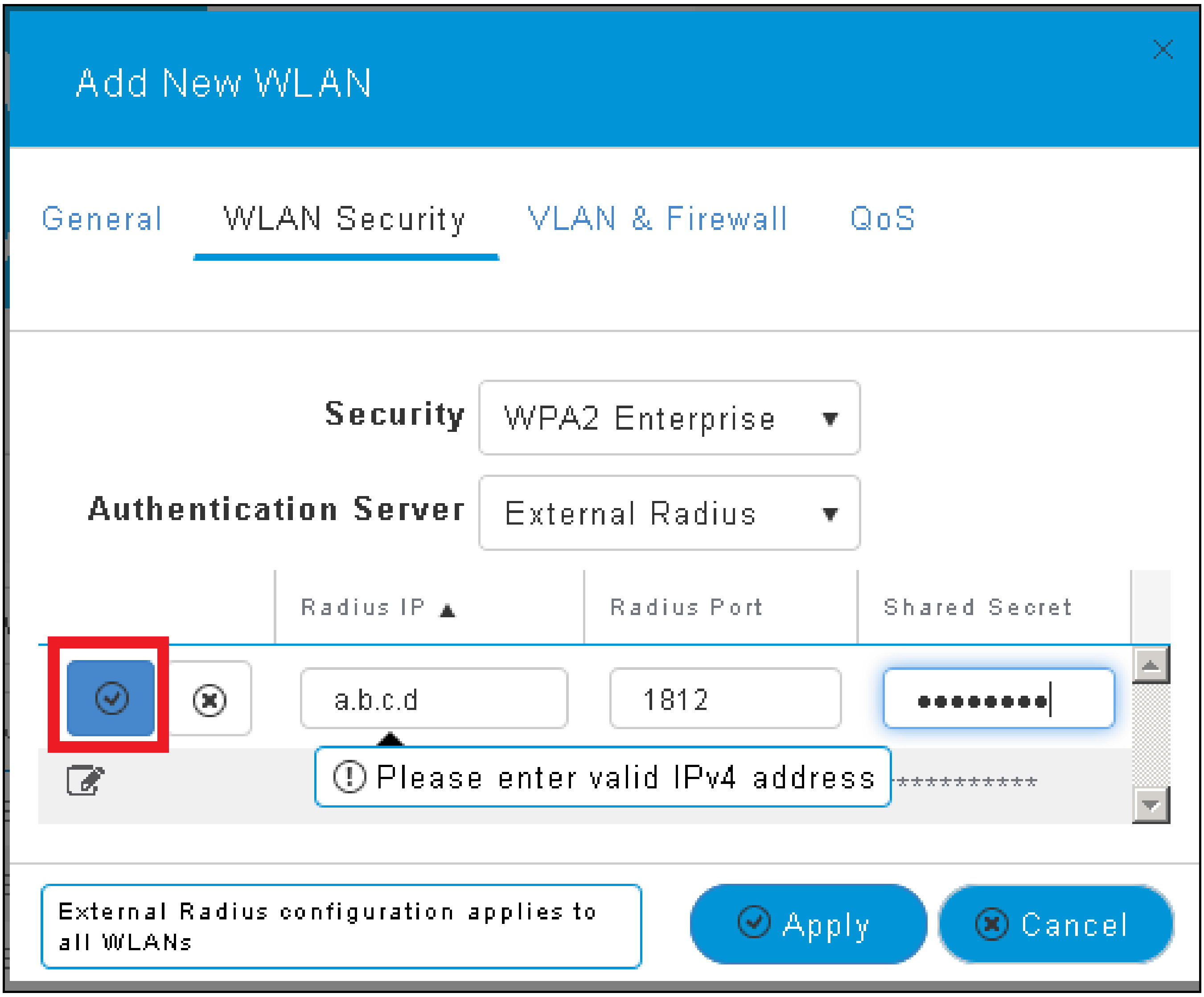


Security WPA2 Enterprise

Authentication Server External Radius

	Radius IP ▲	Radius Port	Shared Secret
✎		1812	************
✎		1812	************

External Radius configuration applies to all WLANs



Security: WPA2 Enterprise

Authentication Server: External Radius

Radius IP ▲	Radius Port	Shared Secret
a.b.c.d	1812	●●●●●●●●●

Please enter valid IPv4 address

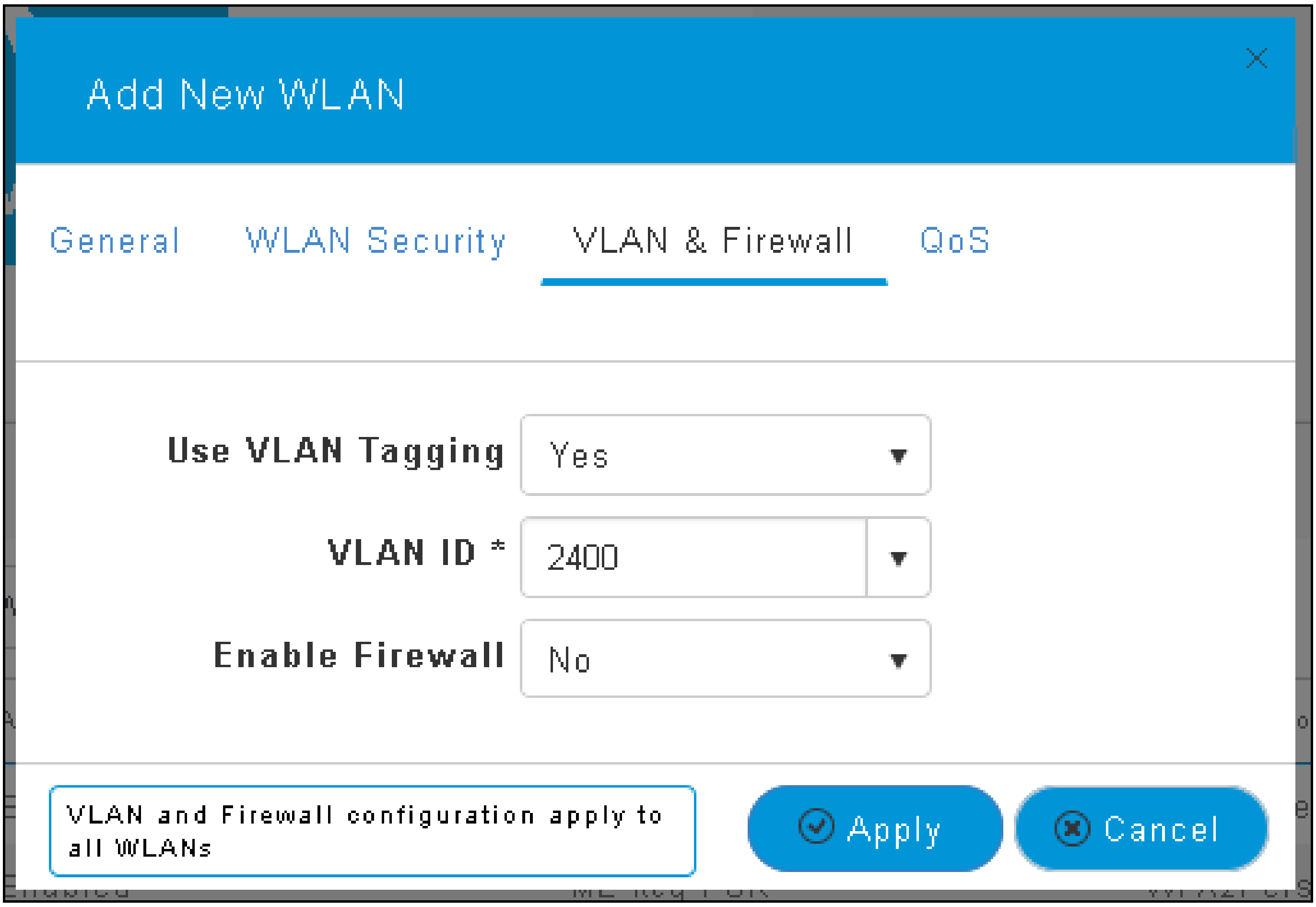
External Radius configuration applies to all WLANs

<a.b.c.d>는 RADIUS 서버에 해당합니다.

4단계. SSID에 VLAN을 할당합니다.

AP의 VLAN에 SSID를 할당해야 하는 경우 이 단계를 건너뛸 수 있습니다.

이 SSID에 대한 사용자를 특정 VLAN(AP의 VLAN 제외)에 할당하려면 **Use VLAN Tagging(VLAN 태깅 사용)**을 활성화하고 원하는 **VLAN ID를 할당합니다**.



Add New WLAN

Use VLAN Tagging: Yes

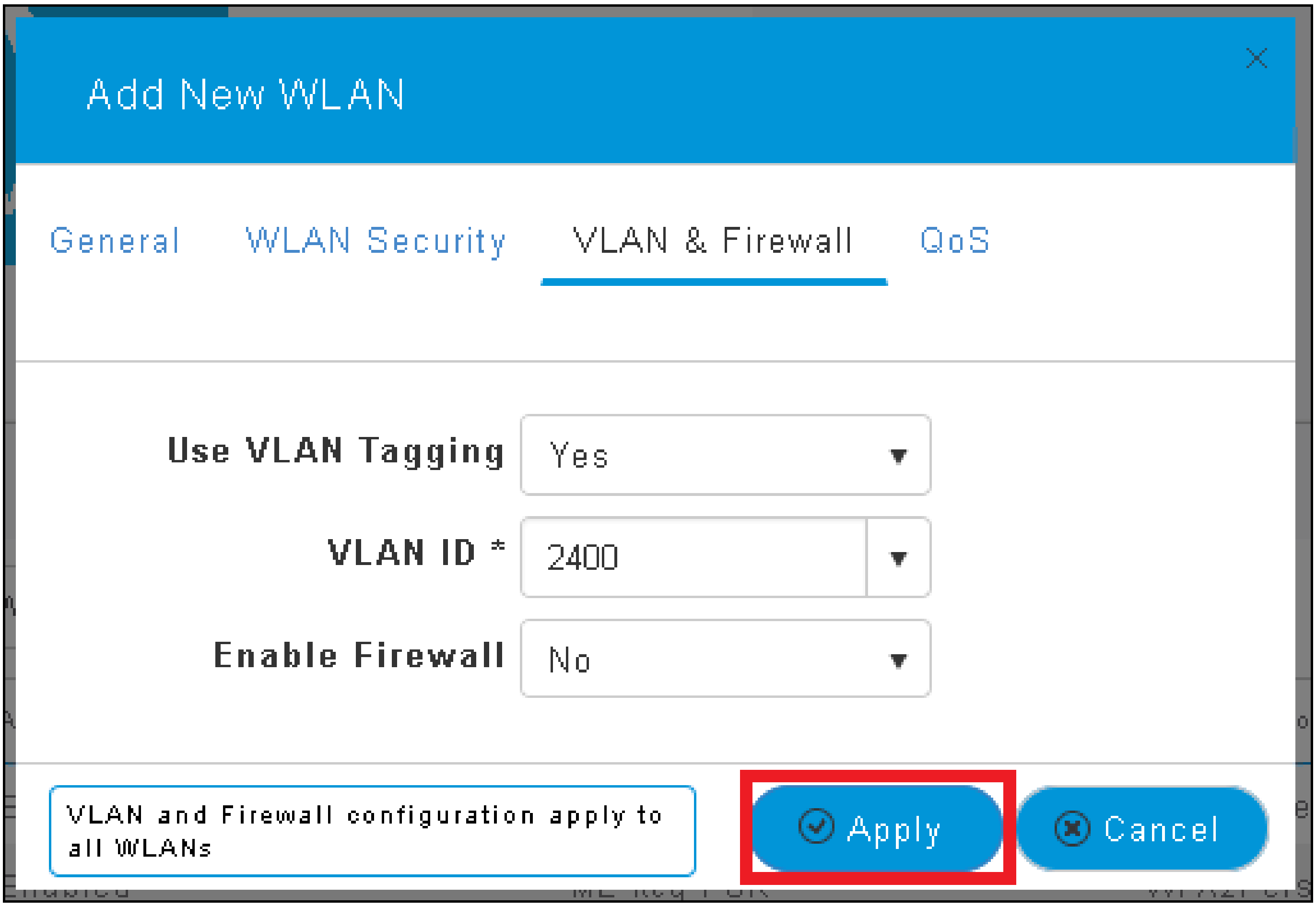
VLAN ID *: 2400

Enable Firewall: No

VLAN and Firewall configuration apply to all WLANs

참고:VLAN Tagging을 사용하는 경우 액세스 포인트가 연결된 스위치 포트가 트렁크 포트로 구성되고 AP VLAN이 기본으로 구성되었는지 확인합니다.

5단계. Apply(**적용**)를 클릭하여 컨피그레이션을 완료합니다.



Use VLAN Tagging: Yes

VLAN ID *: 2400

Enable Firewall: No

VLAN and Firewall configuration apply to all WLANs

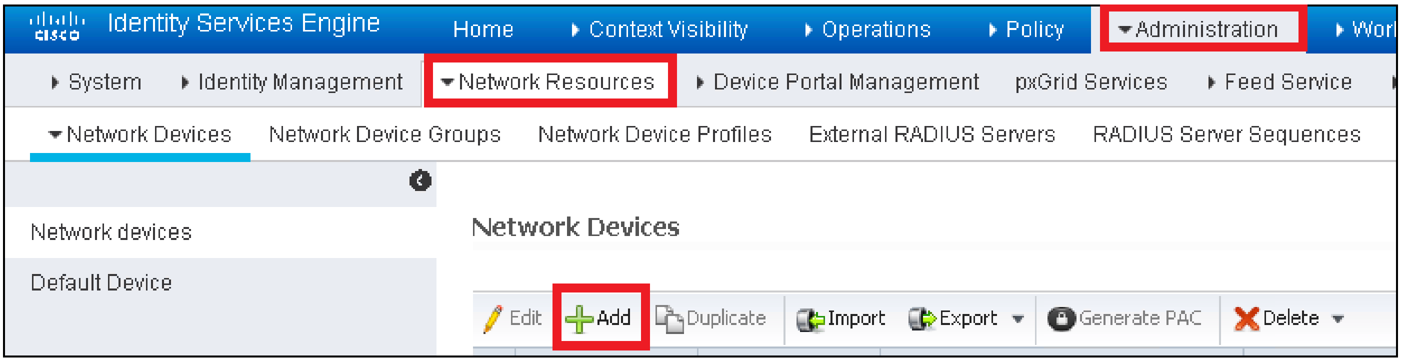
6단계. 선택 사항, VLAN 재지정을 허용하도록 WLAN을 구성합니다.

WLAN에서 AAA 재지정을 활성화하고 필요한 VLAN을 추가합니다.이렇게 하려면 ME 관리 인터페이스에 대한 CLI 세션을 열고 다음 명령을 실행해야 합니다.

```
>config wlan disable <wlan-id>
>config wlan aaa-override enable <wlan-id>
>config wlan enable <wlan-id>
>config flexconnect group default-flexgroup vlan add <vlan-id>
```

ISE에서 ME 선언

1단계. ISE 콘솔을 열고 Administration(관리) **> Network Resources(네트워크 리소스) > Network Devices(네트워크 디바이스) > Add(추가)로 이동합니다.**

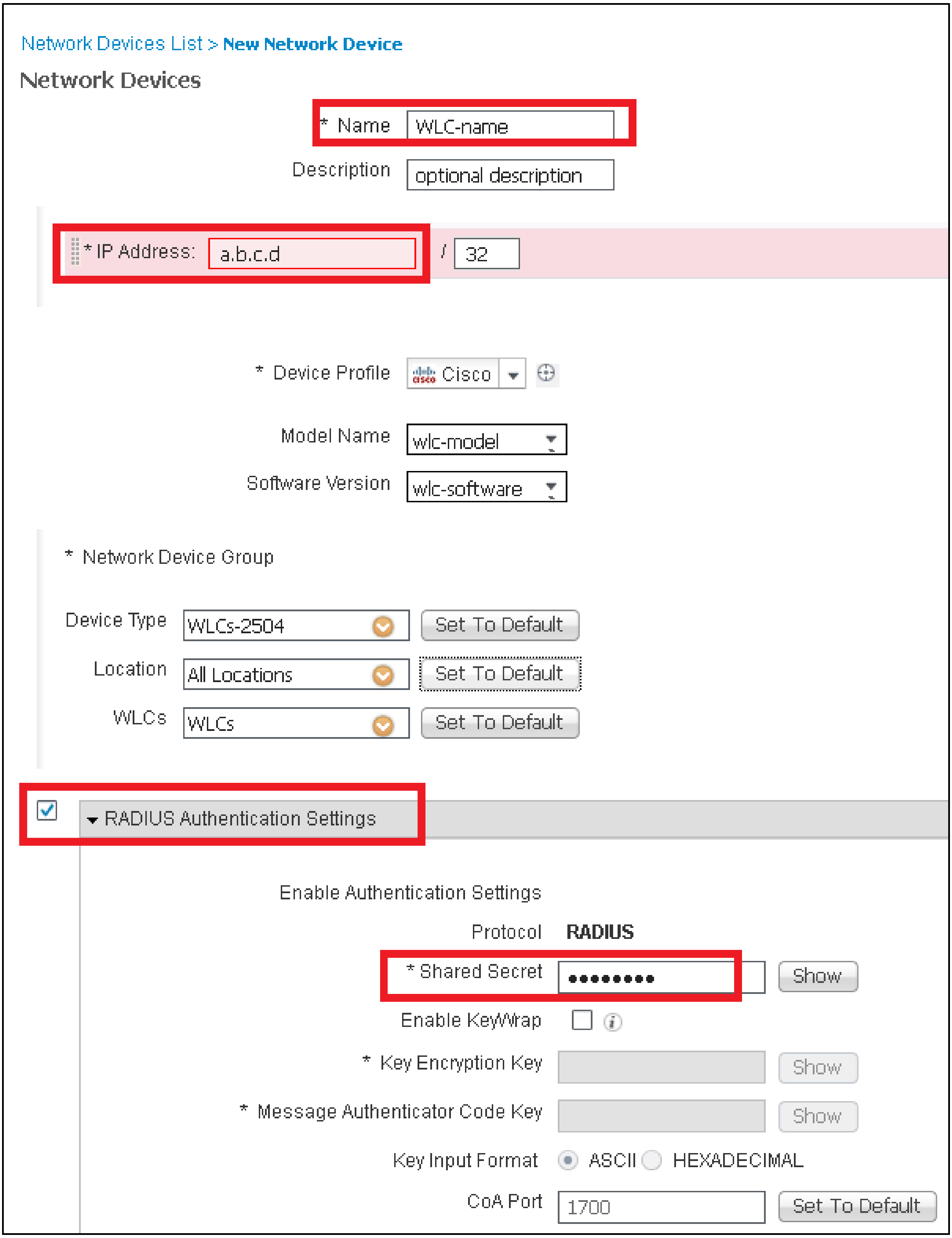


2단계. 정보를 입력합니다.

선택적으로, 모델 이름, 소프트웨어 버전, 설명을 지정하고 디바이스 유형, 위치 또는 WLC에 따라

네트워크 디바이스 그룹을 할당할 수 있습니다.

a.b.c.d는 ME의 IP 주소에 해당합니다.



Network Devices List > **New Network Device**

Network Devices

* Name: WLC-name

Description: optional description

* IP Address: a.b.c.d / 32

* Device Profile: Cisco

Model Name: wlc-model

Software Version: wlc-software

* Network Device Group

Device Type: WLCs-2504 | Set To Default

Location: All Locations | Set To Default

WLCs: WLCs | Set To Default

☑ RADIUS Authentication Settings

Enable Authentication Settings

Protocol: **RADIUS**

* Shared Secret: ●●●●●●●●● | Show

Enable KeyWrap: □

* Key Encryption Key: | Show

* Message Authenticator Code Key: | Show

Key Input Format: ● ASCII ○ HEXADECIMAL

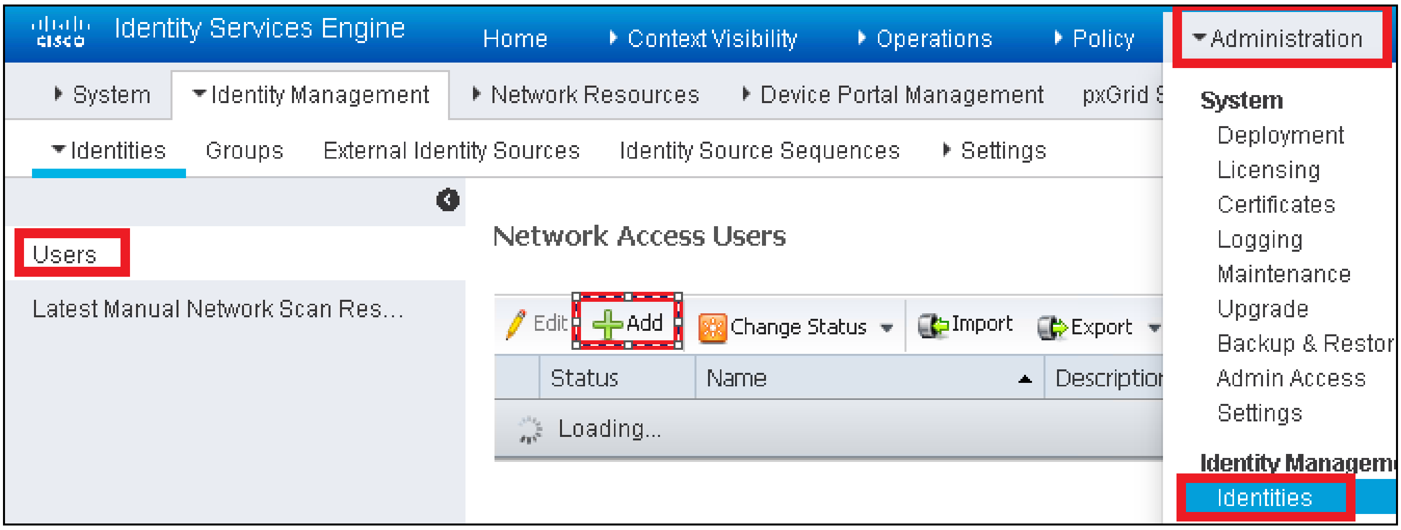
CoA Port: 1700 | Set To Default

네트워크 디바이스 그룹에 대한 자세한 내용은 다음 링크를 참조하십시오.

ISE - 네트워크 디바이스 그룹

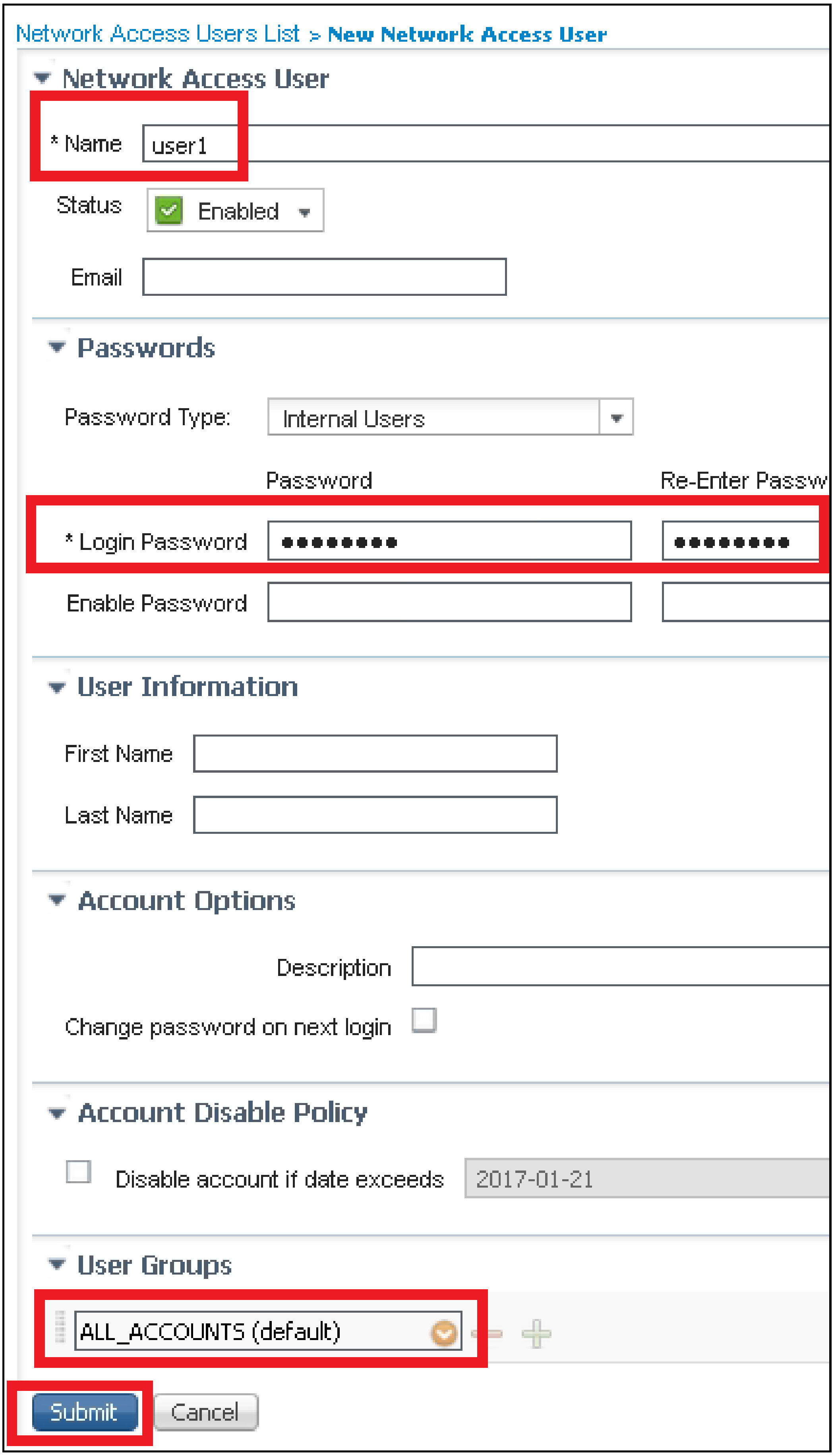
ISE에서 새 사용자 생성

1단계. 다음으로 이동합니다. **관리 > 신원 관리 > ID > 사용자 > 추가.**



2단계. 정보를 입력합니다.

이 예에서는 이 사용자가 ALL_ACCOUNTS라는 그룹에 속하지만 필요에 따라 조정할 수 있습니다.



Network Access Users List > New Network Access User

Network Access User

* Name user1

Status ☑ Enabled

Email

Passwords

Password Type: Internal Users

	Password	Re-Enter Passw
* Login Password	•••••••••	•••••••••
Enable Password		

User Information

First Name

Last Name

Account Options

Description

Change password on next login □

Account Disable Policy

□ Disable account if date exceeds 2017-01-21

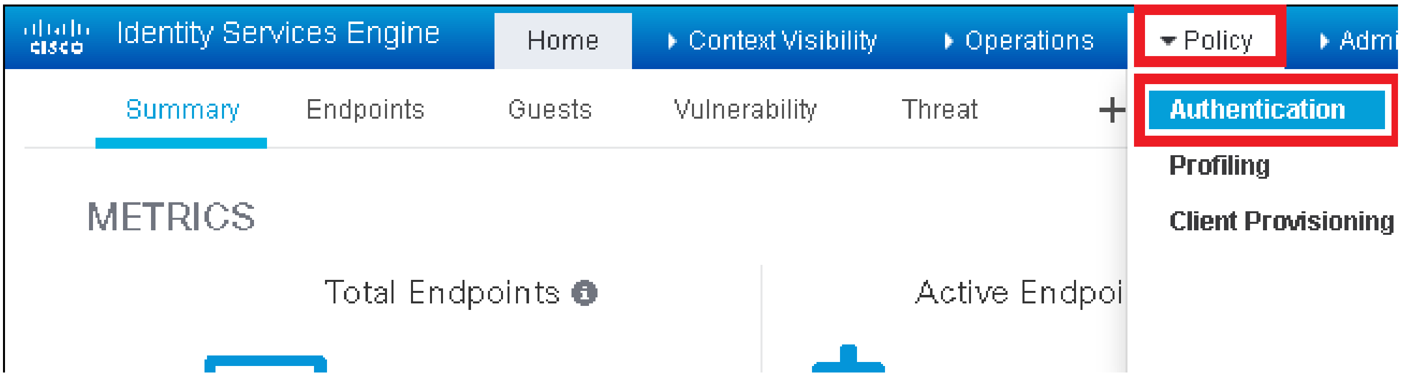
User Groups

ALL_ACCOUNTS (default)

인증 규칙 생성

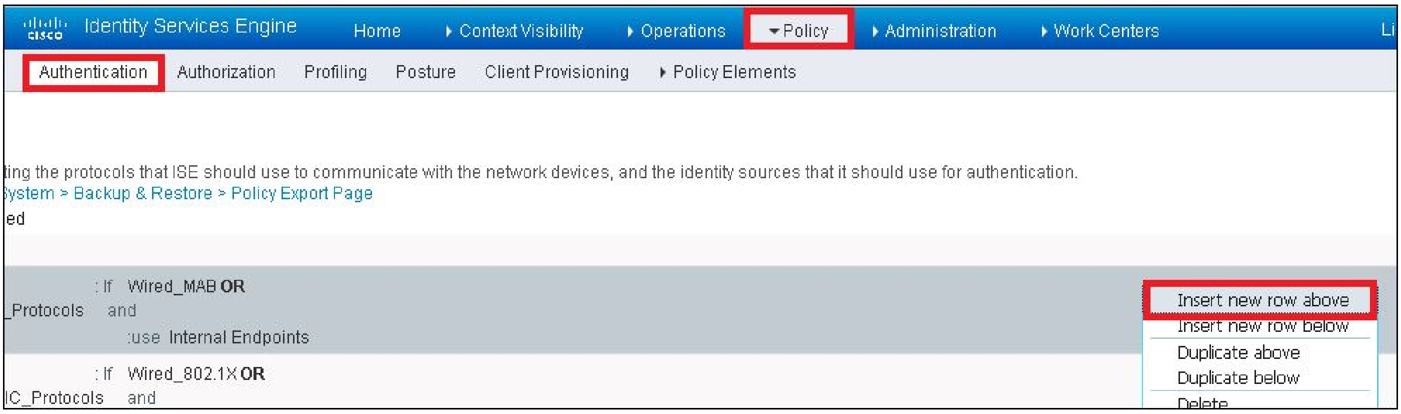
인증 규칙은 사용자의 자격 증명이 올바른지 확인(사용자가 실제 사용자인지 확인)하고 사용자가 사용할 수 있는 인증 방법을 제한하는 데 사용됩니다.

1단계. 탐색 Policy(**정책) > Authentication(인증)으로 이동합니다**.



2단계. 새 인증 규칙을 삽입합니다.

이렇게 하려면 **Policy(정책) > Authentication(인증) > Insert new row above/below(위/아래에 새 행 삽입)로 이동합니다.**

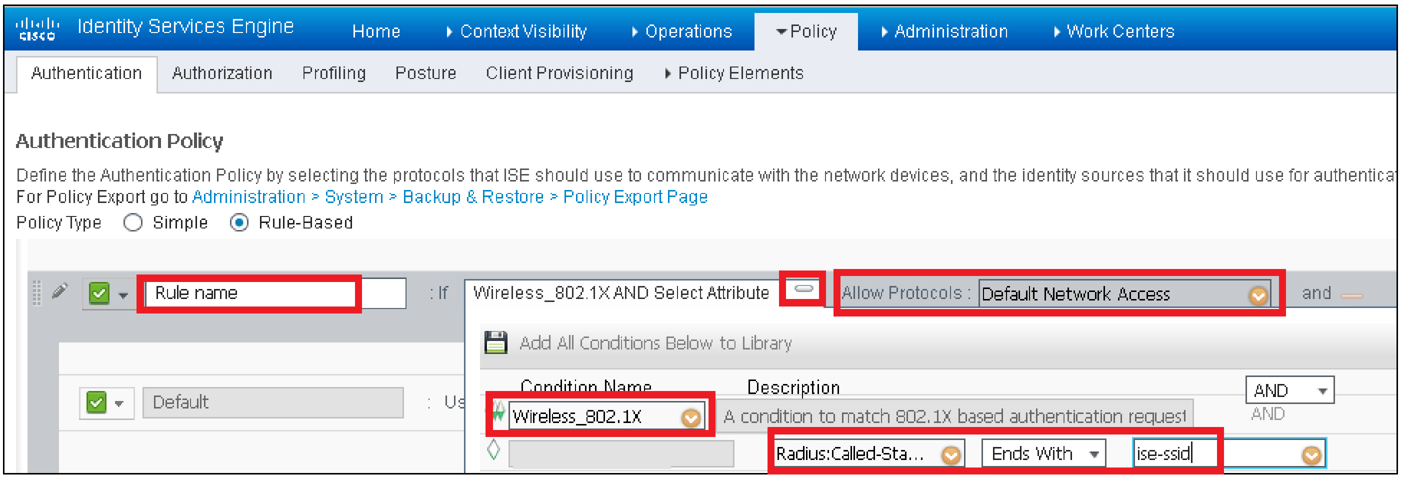


ting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication.
ystem > Backup & Restore > Policy Export Page
ed

: If Wired_MAB OR
_Protocols and
:use Internal Endpoints
: If Wired_802.1X OR
IC_Protocols and

3단계. 필요한 정보를 입력합니다.

이 인증 규칙 예는 **Default Network Access(기본 네트워크 액세스**) 목록 아래에 나열된 모든 프로토콜을 허용합니다. 이는 Wireless 802.1x 클라이언트 및 Called-Station-ID의 인증 요청에 적용되며 *ise-ssid*로 끝납니다.



Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentica
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page
Policy Type ○ Simple ● Rule-Based

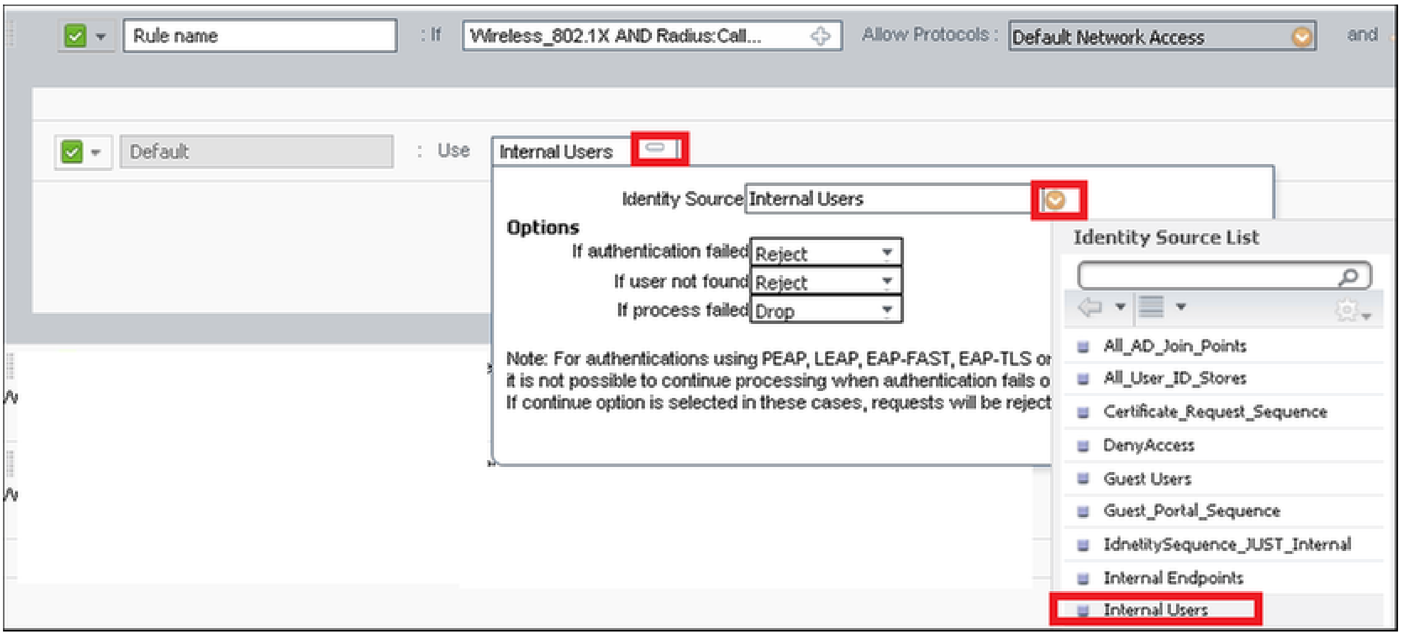
☑ Rule name : If Wireless_802.1X AND Select Attribute Allow Protocols : Default Network Access and

Add All Conditions Below to Library

Condition Name	Description	
Wireless_802.1X	A condition to match 802.1X based authentication request	AND
Radius:Called-Sta...	Ends With	ise-ssid

☑ Default : Us

또한 이 인증 규칙과 일치하는 클라이언트의 ID 소스를 선택합니다(이 예에서는 *내부 사용자*가 사용됨).



Identity Source Internal Users

Options

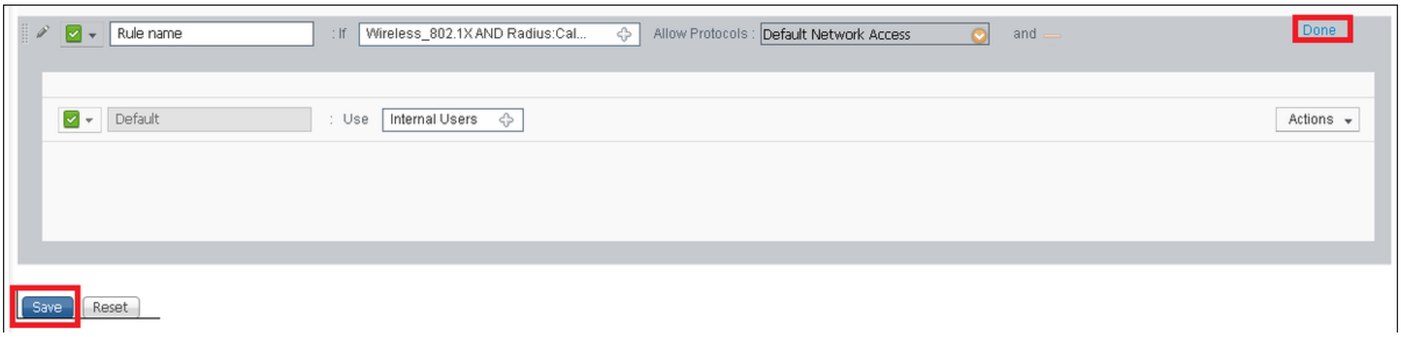
If authentication failed Reject

If user not found Reject

If process failed Drop

Note: For authentications using PEAP, LEAP, EAP-FAST, EAP-TLS or
it is not possible to continue processing when authentication fails o
If continue option is selected in these cases, requests will be reject

완료되면 Done(완료) 및 **Save(저장)**를 **클릭합니다.**


Rule name
: If
Wireless_802.1X AND Radius:Cal...
Allow Protocols : Default Network Access
and
Done
Default
: Use
Internal Users
Actions
Save
Reset

Allow Protocols Policies(프로토콜 정책 허용)에 대한 자세한 내용은 다음 링크를 참조하십시오.

허용되는 프로토콜 서비스

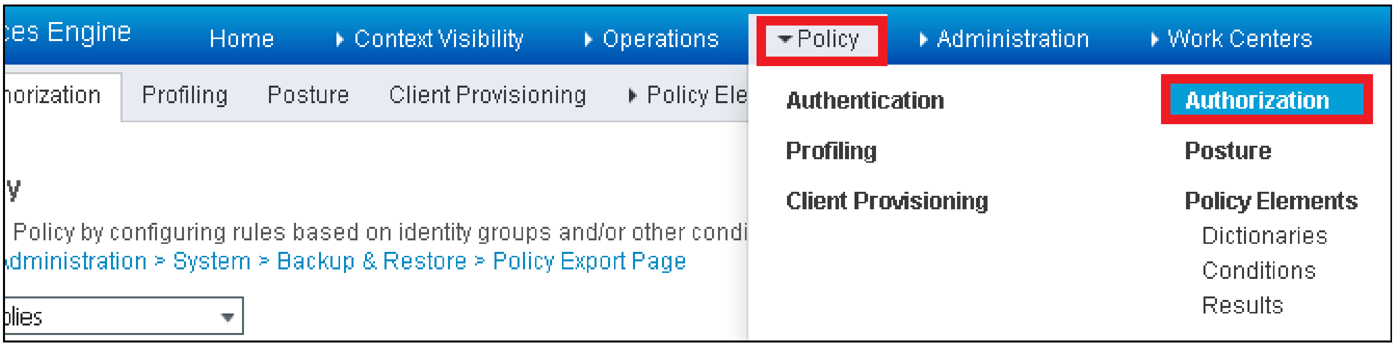
ID 소스에 대한 자세한 내용은 다음 링크를 참조하십시오.

사용자 ID 그룹 생성

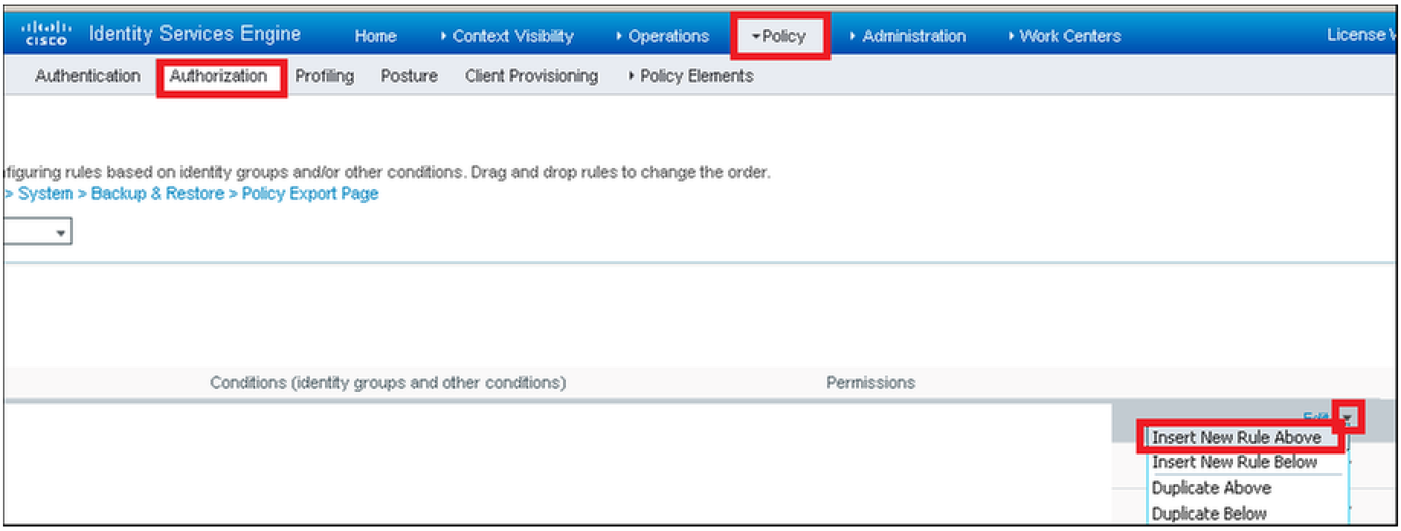
권한 부여 규칙 생성

권한 부여 규칙은 클라이언트가 네트워크에 가입할 수 있는지 여부를 결정하는 담당자입니다

1단계. Policy(정책) **> Authorization(권한 부여)으로 이동합니다.**

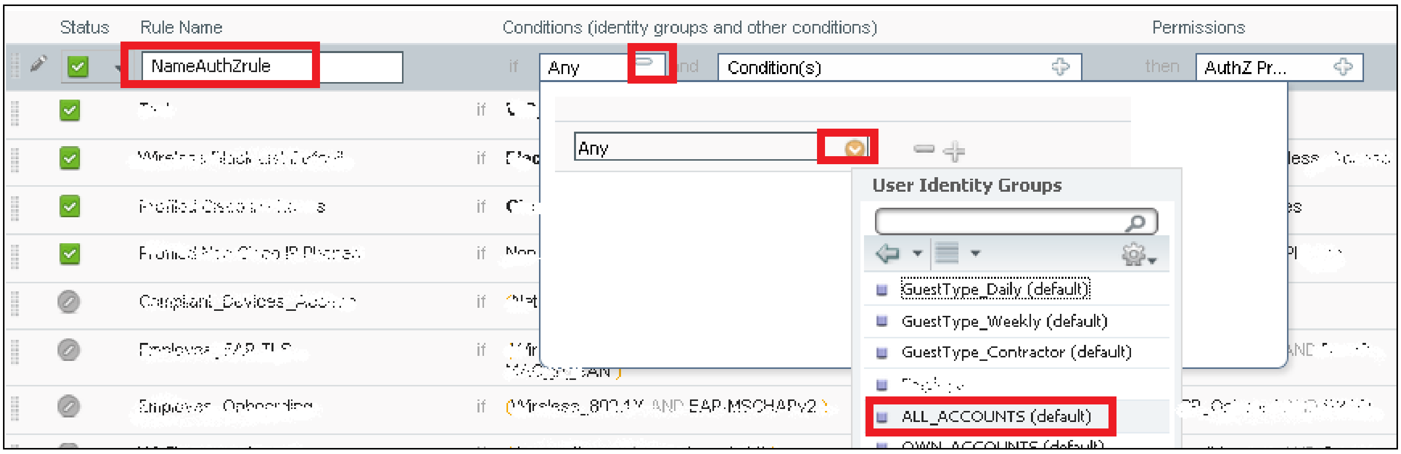


2단계. 새 규칙을 삽입합니다.Policy(**정책) > Authorization(권한 부여) > Insert New Rule Above/Below(위에/아래에 새 규칙 삽입)로 이동합니다.**



3단계. 정보를 입력합니다.

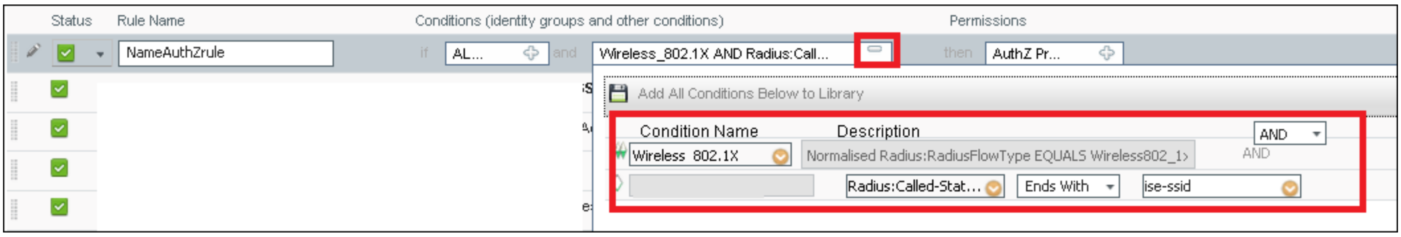
먼저 규칙 이름과 사용자가 저장되는 ID 그룹을 선택합니다.이 예에서는 사용자가 그룹 ALL_*ACCOUNTS*에 *저장됩니다.*


Status
Rule Name
Conditions (identity groups and other conditions)
Permissions
if
and
then
User Identity Groups
GuestType_Daily (default)
GuestType_Weekly (default)
GuestType_Contractor (default)
ALL_ACCOUNTS (default)
OWN_ACCOUNTS (default)

Rule Name: NameAuthZrule | Any | Condition(s) | AuthZ Pr...

Any

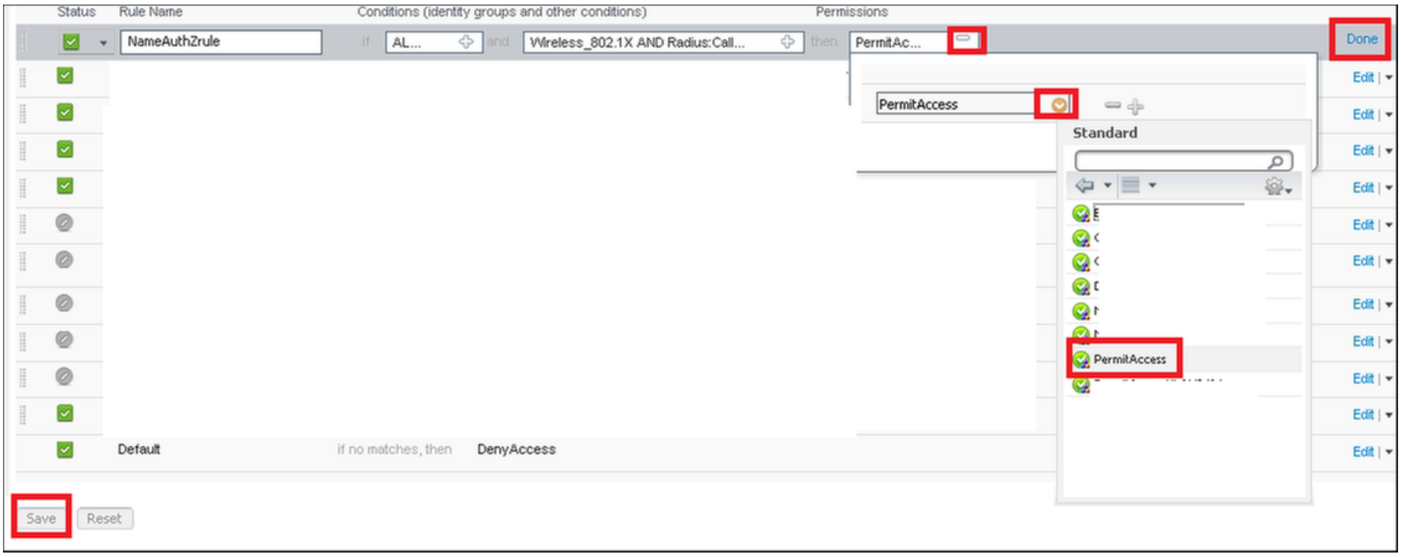
그런 다음 권한 부여 프로세스가 이 규칙에 속하도록 하는 다른 조건을 선택합니다.이 예에서 권한 부여 프로세스는 802.1x Wireless를 사용하고 스테이션 ID라고 하는 경우 이 규칙에 *적용됩니다. ise-ssid*로 *끝납니다.*


Status
Rule Name
Conditions (identity groups and other conditions)
Permissions
if
and
then
Add All Conditions Below to Library
Condition Name
Description

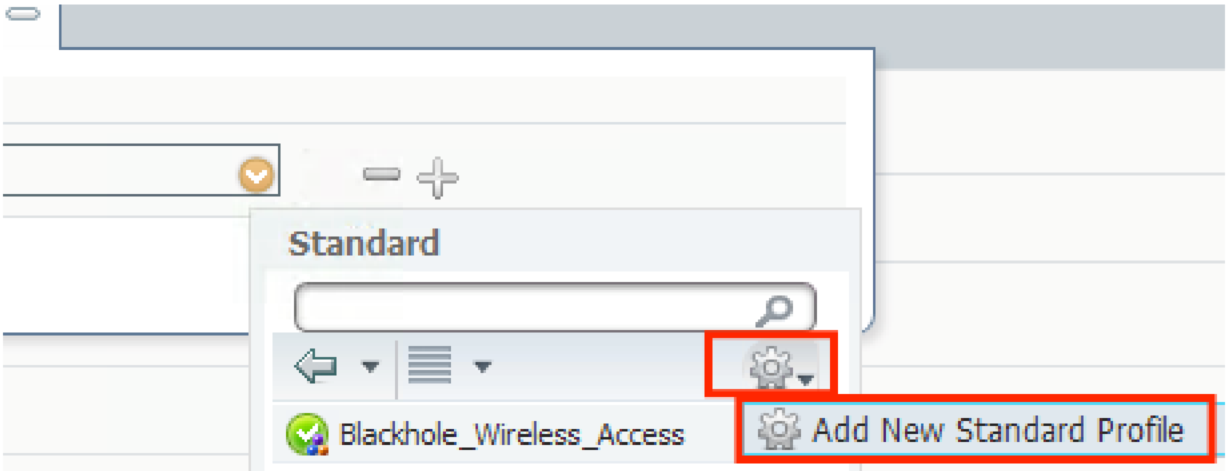
NameAuthZrule | AL... | Wireless_802.1X AND Radius:Call... | AuthZ Pr...

Condition Name	Description	
Wireless_802.1X	Normalised Radius:RadiusFlowType EQUALS Wireless802_1x	AND
	Radius:Called-Stat... Ends With ise-ssid	

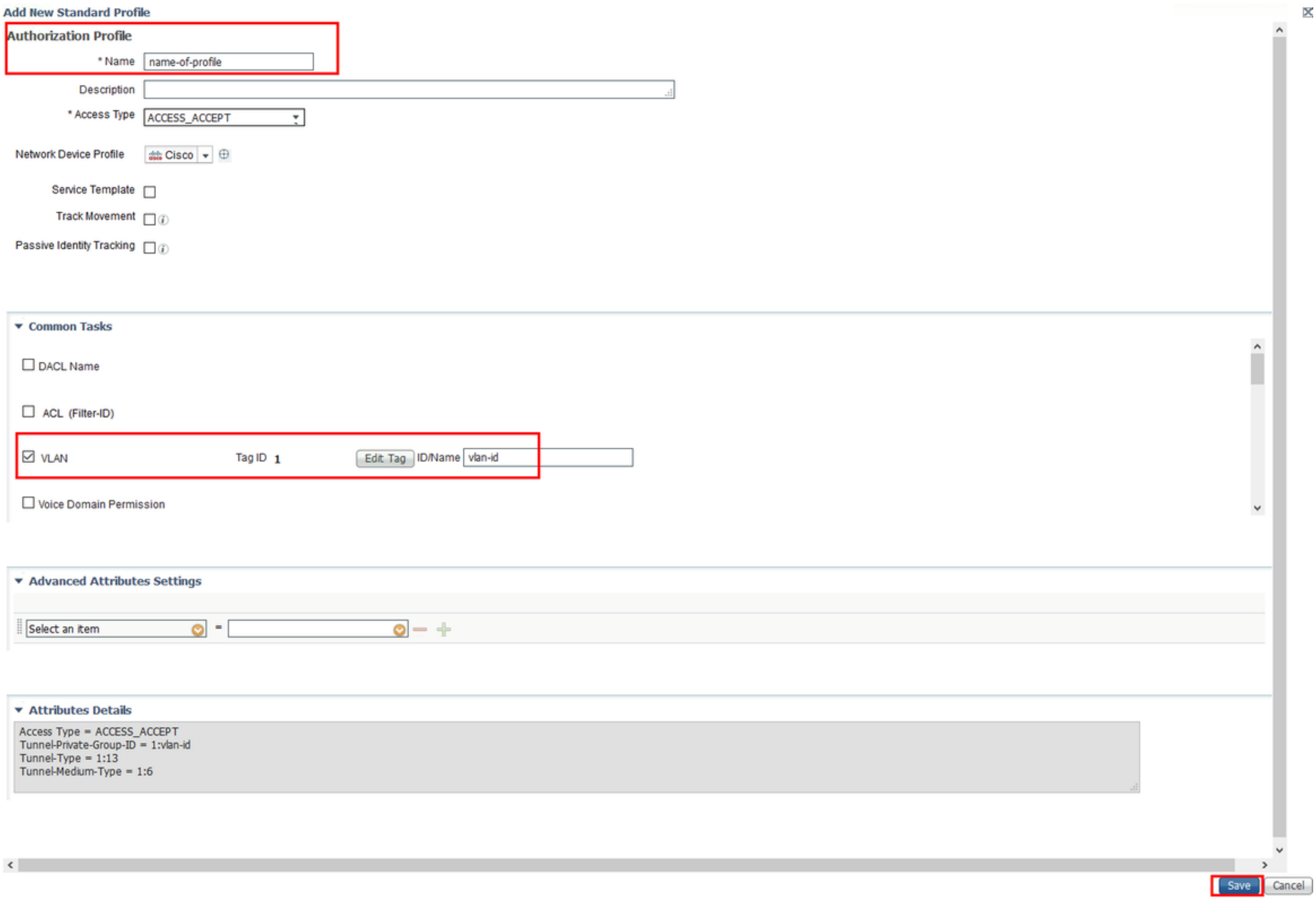
마지막으로 클라이언트가 네트워크에 연결할 수 있는 권한 부여 프로파일을 선택하고 **Done** and **Save**를 클릭합니다.



선택적으로, 무선 클라이언트를 다른 VLAN에 할당할 새 권한 부여 프로파일을 생성합니다.



정보를 입력합니다.



Authorization Profile

* Name: name-of-profile

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template □

Track Movement □

Passive Identity Tracking □

Common Tasks

□ DACL Name

□ ACL (Filter-ID)

☑ VLAN Tag ID 1 Edit Tag ID/Name vlan-id

□ Voice Domain Permission

Advanced Attributes Settings

Select an item =

Attributes Details

```
Access Type = ACCESS_ACCEPT
Tunnel-Private-Group-ID = 1:vlan-id
Tunnel-Type = 1:13
Tunnel-Medium-Type = 1:6
```

엔드 디바이스 구성

PEAP/MS-CHAPv2(Challenge-Handshake Authentication Protocol 버전 2의 Microsoft 버전)를 사용하여 802.1x 인증을 사용하여 SSID에 연결하도록 Windows 10 랩톱을 구성합니다.

이 컨피그레이션 예에서는 ISE가 자체 서명 인증서를 사용하여 인증을 수행합니다.

Windows 시스템에서 WLAN 프로파일을 생성하려면 다음 두 가지 옵션이 있습니다.

1. 인증을 완료하기 위해 ISE 서버를 검증하고 신뢰하기 위해 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).

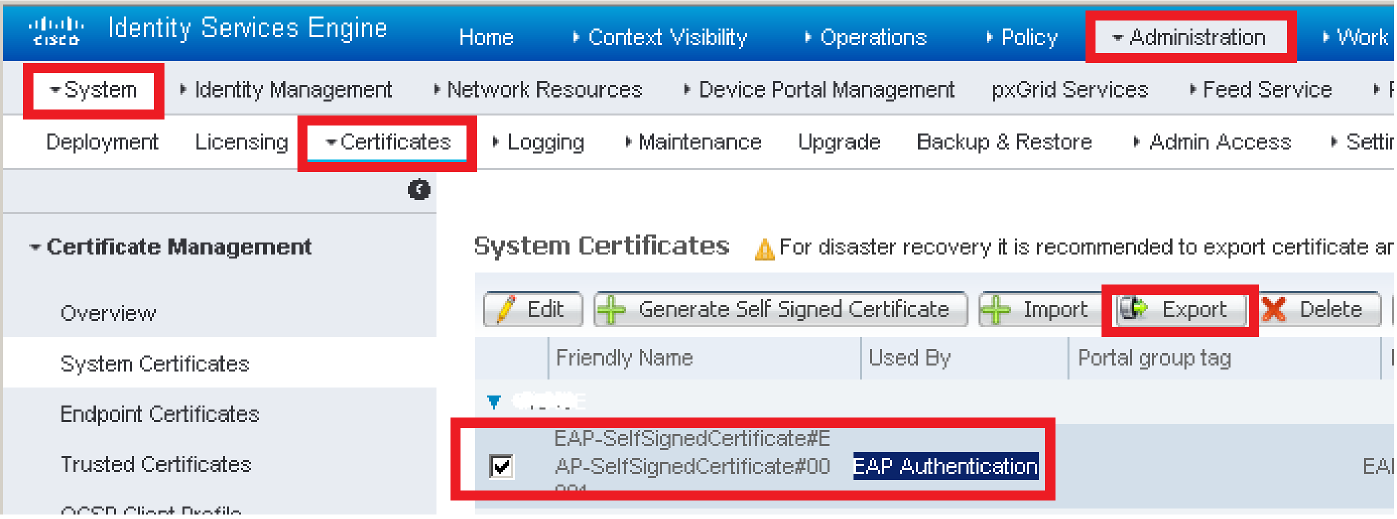
이러한 옵션에 대한 컨피그레이션은 엔드 디바이스 컨피그레이션 - Create the WLAN Profile - 7단계에서 설명합니다.

장치 구성 종료 - ISE 자체 서명 인증서 설치

1단계. ISE에서 자체 서명 인증서를 내보냅니다.

ISE에 로그인하고 Administration(관리) **> System(시스템) > Certificates(인증서) > System Certificates(시스템 인증서)로 이동합니다**.

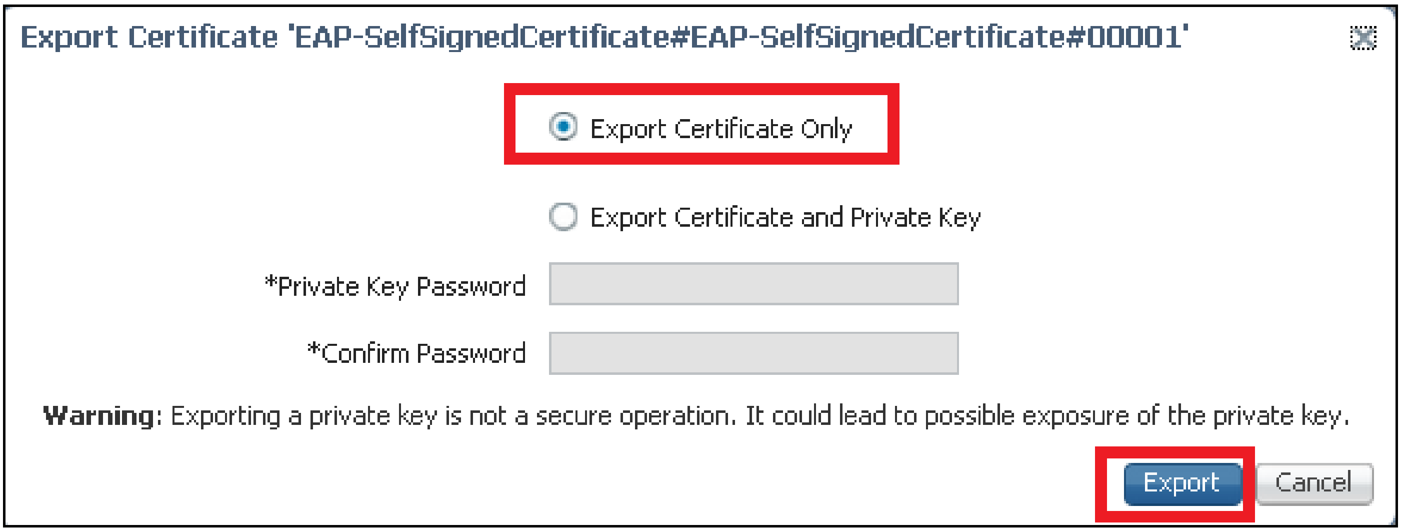
그런 다음 EAP 인증에 사용되는 인증서를 선택하고 Export(내보내기)를 **클릭합니다.**



System Certificates ⚠ For disaster recovery it is recommended to export certificate ar

	Friendly Name	Used By	Portal group tag	
▼ [redacted]				
☑	EAP-SelfSignedCertificate#EAP-SelfSignedCertificate#00001	EAP Authentication		EAI

필요한 위치에 인증서를 저장합니다.이 인증서는 Windows 시스템에 설치되어 있습니다.


Export Certificate 'EAP-SelfSignedCertificate#EAP-SelfSignedCertificate#00001'

● Export Certificate Only

○ Export Certificate and Private Key

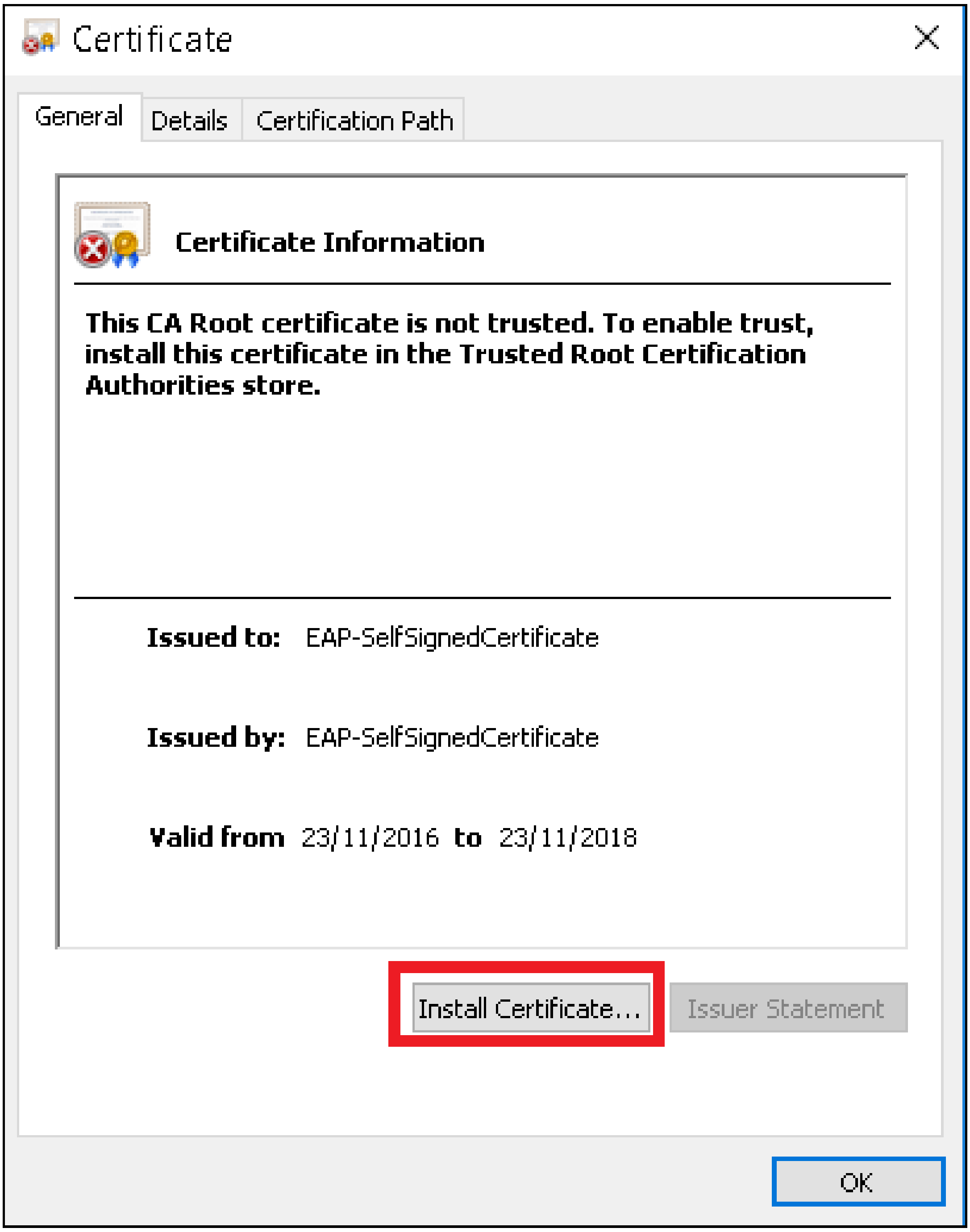
*Private Key Password

*Confirm Password

Warning: Exporting a private key is not a secure operation. It could lead to possible exposure of the private key.

2단계. Windows 시스템에 인증서를 설치합니다.

Windows 시스템으로 내보내기 전에 내보낸 인증서를 복사하고, 파일 확장명을 .pem에서 .crt로 변경한 다음 두 번 클릭한 다음 **Install Certificate...**를 선택합니다..



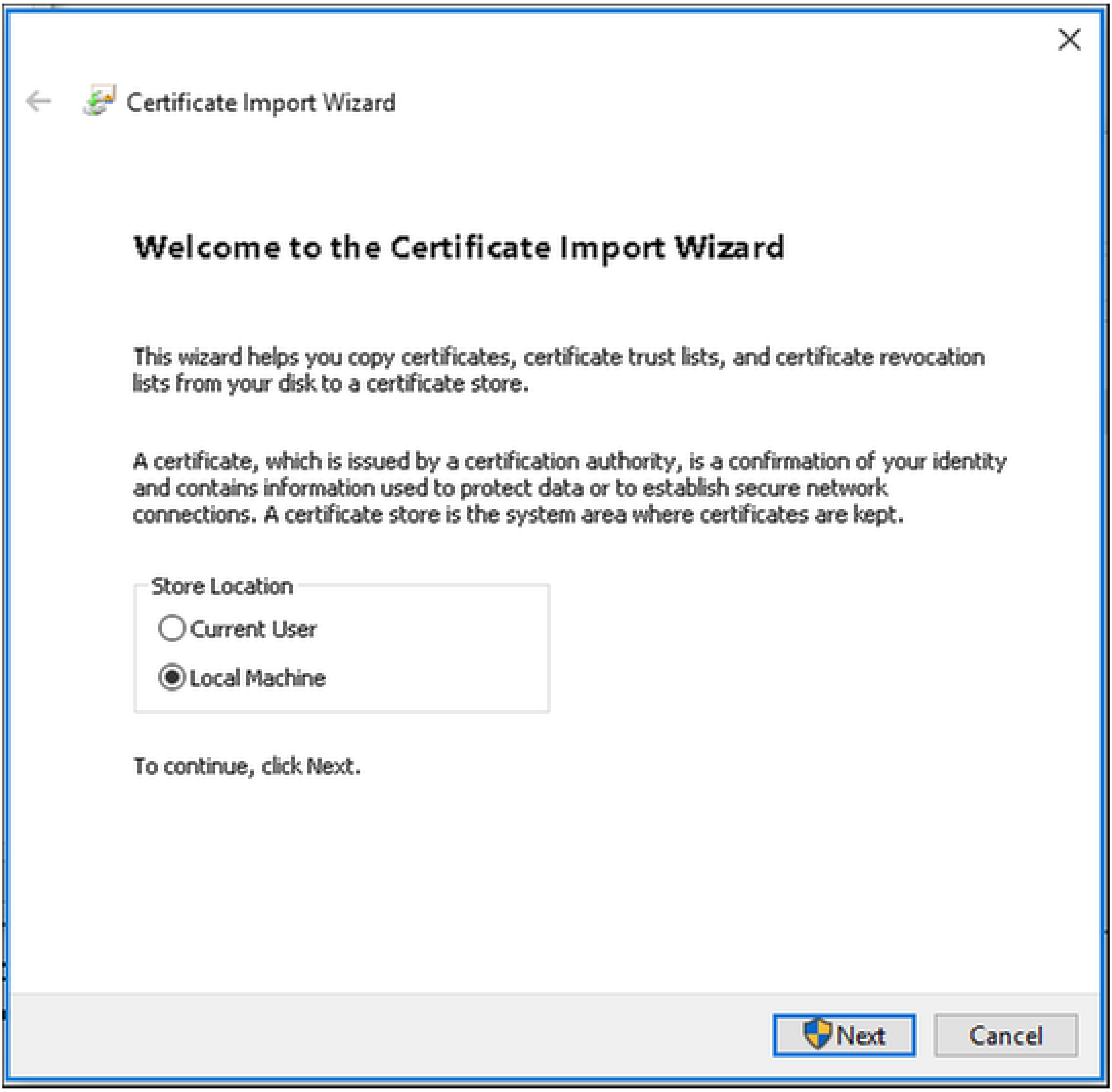
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: EAP-SelfSignedCertificate

Issued by: EAP-SelfSignedCertificate

Valid from 23/11/2016 to 23/11/2018

Local Machine(**로컬 머신**)에 설치하도록 선택한 다음 **Next(다음)**를 클릭합니다.



Certificate Import Wizard

Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

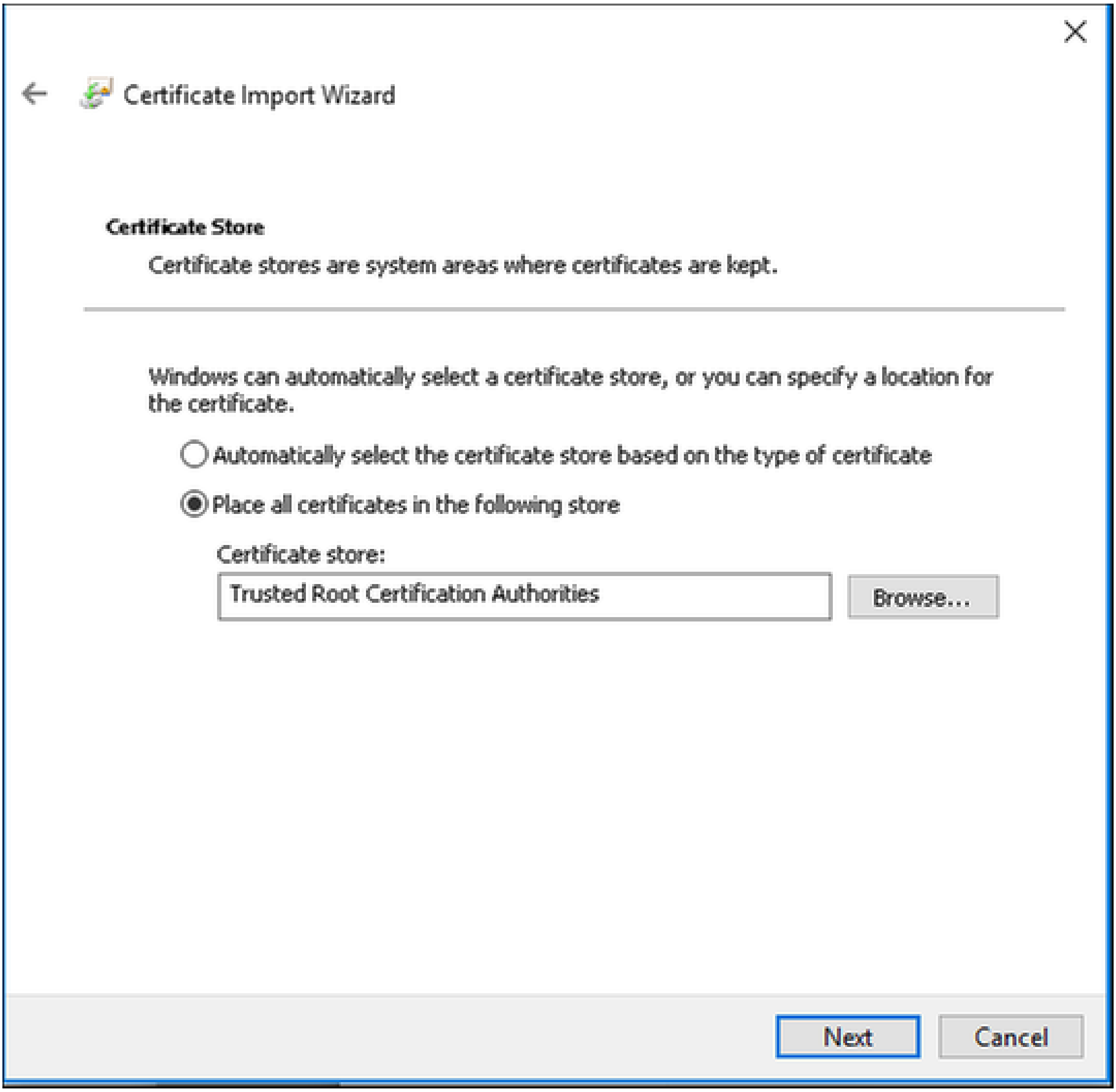
Store Location

○ Current User

● Local Machine

To continue, click Next.

Place **all certificates in the following store(다음 저장소에 모든 인증서 배치)**를 선택한 다음 Trusted Root Certification Authorities(신뢰할 수 있는 루트 인증 기관**)**를 찾아 선택합니다.그런 다음 **Next(다음**)를 클릭합니다.



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.

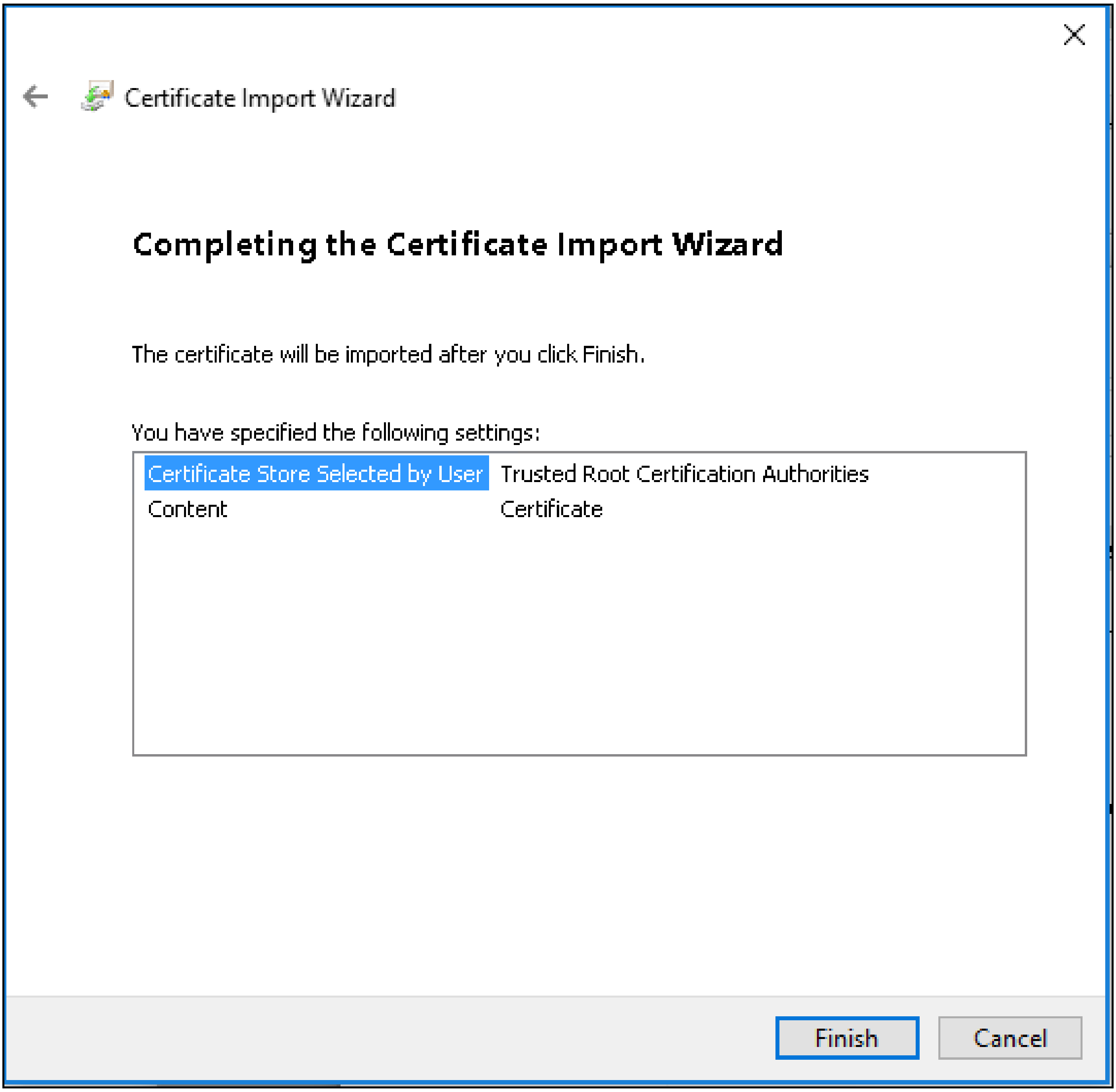
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

Trusted Root Certification Authorities

그런 다음 Finish(**마침)를 클릭합니다.**



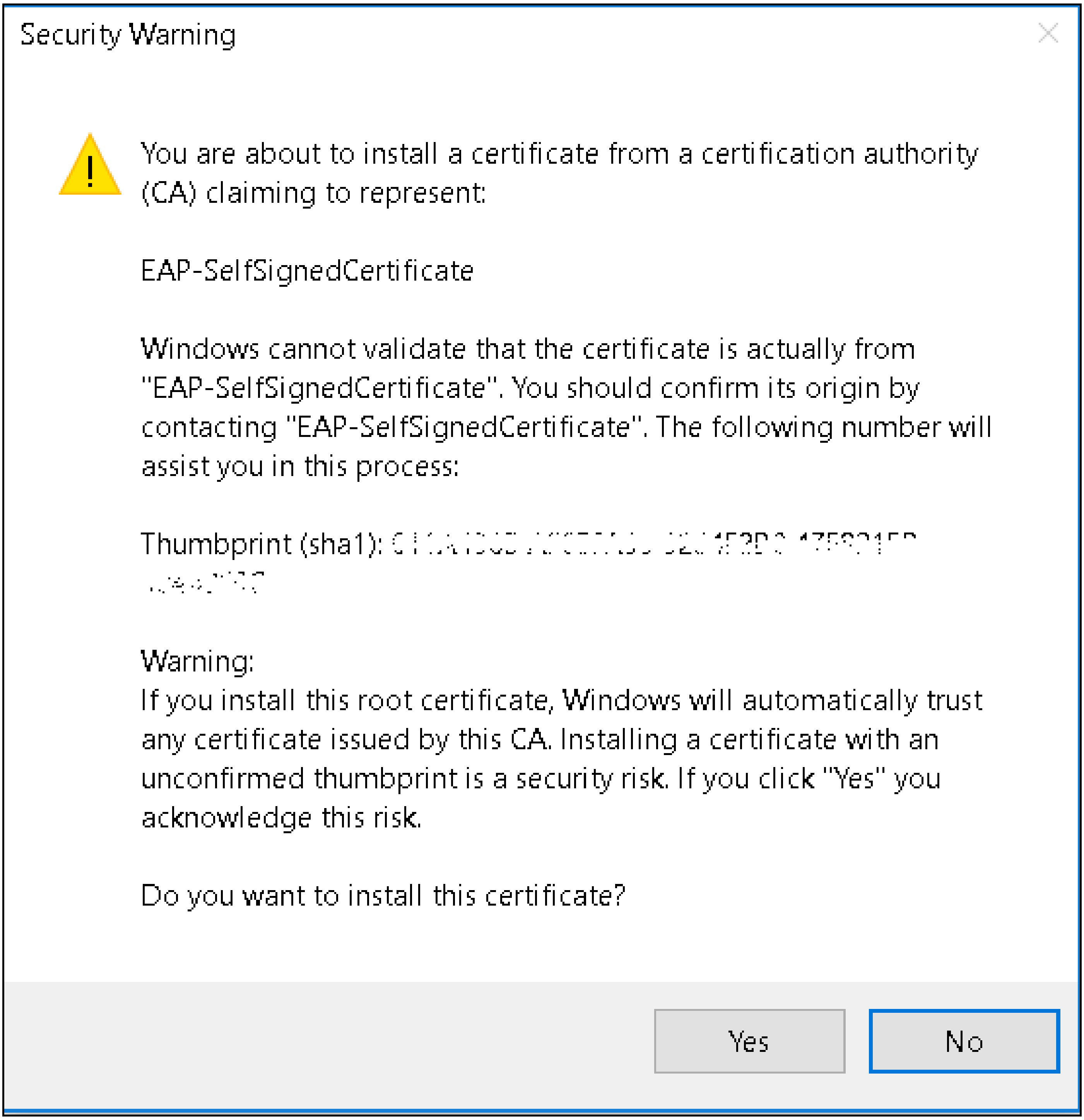
Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certification Authorities
Content	Certificate

끝에서 **예**를 클릭하여 인증서 설치를 확인합니다.



Security Warning

You are about to install a certificate from a certification authority (CA) claiming to represent:

EAP-SelfSignedCertificate

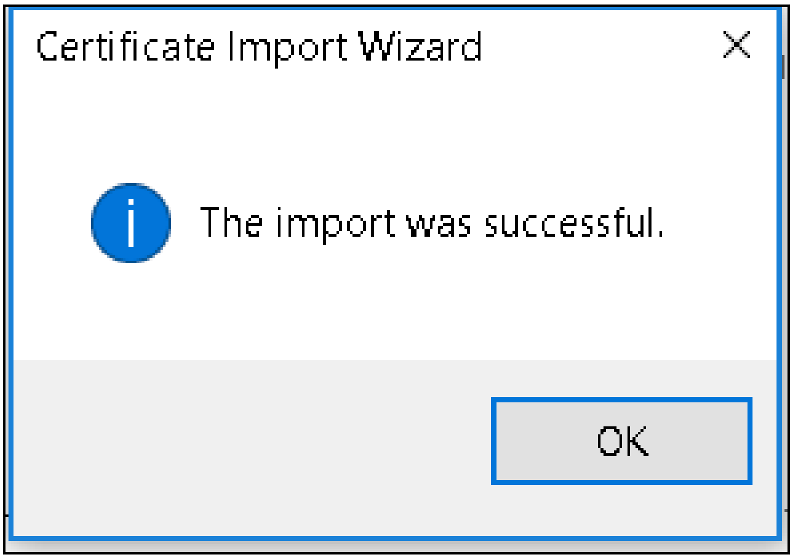
Windows cannot validate that the certificate is actually from "EAP-SelfSignedCertificate". You should confirm its origin by contacting "EAP-SelfSignedCertificate". The following number will assist you in this process:

Thumbprint (sha1): [redacted]

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

마지막으로 **확인**을 클릭합니다.

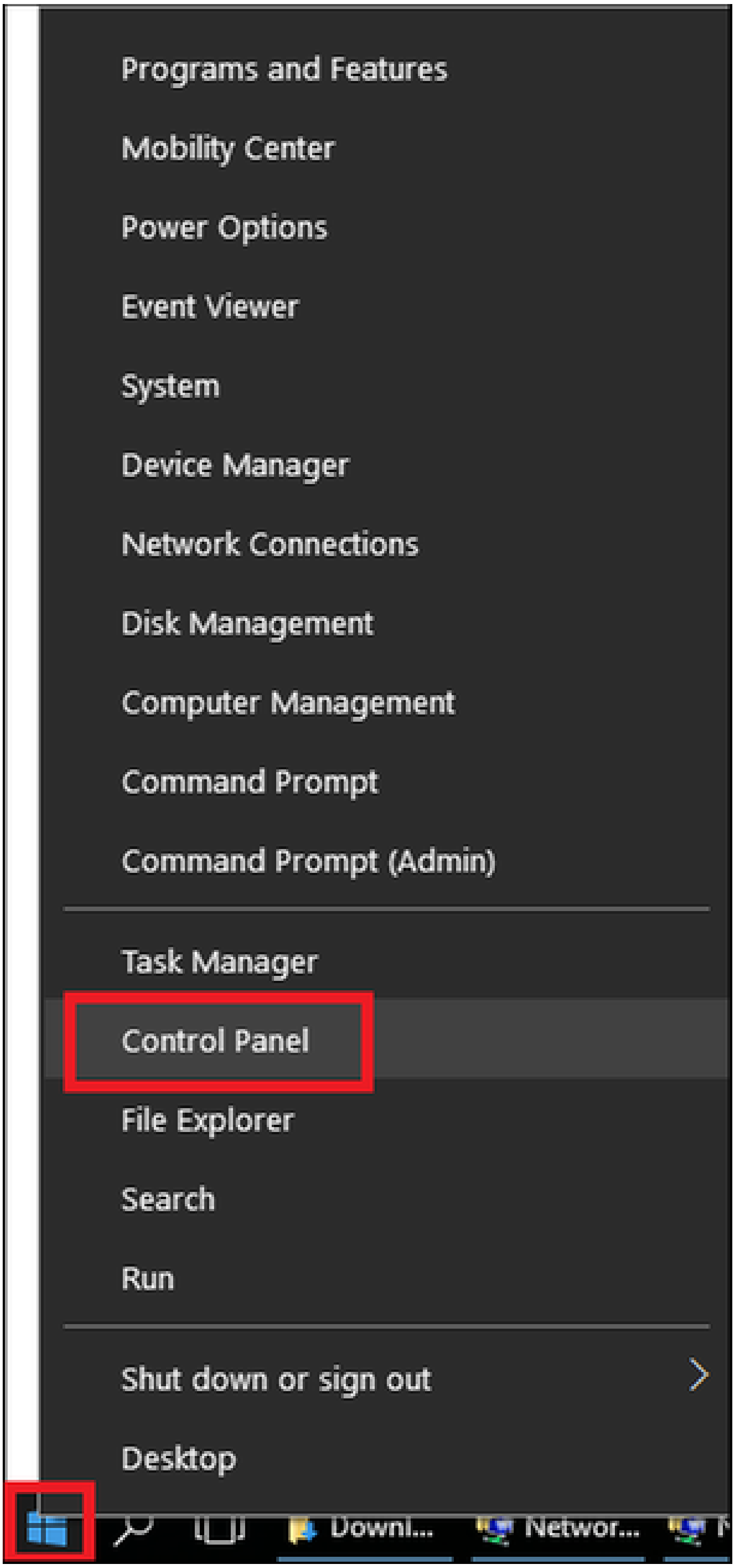


Certificate Import Wizard

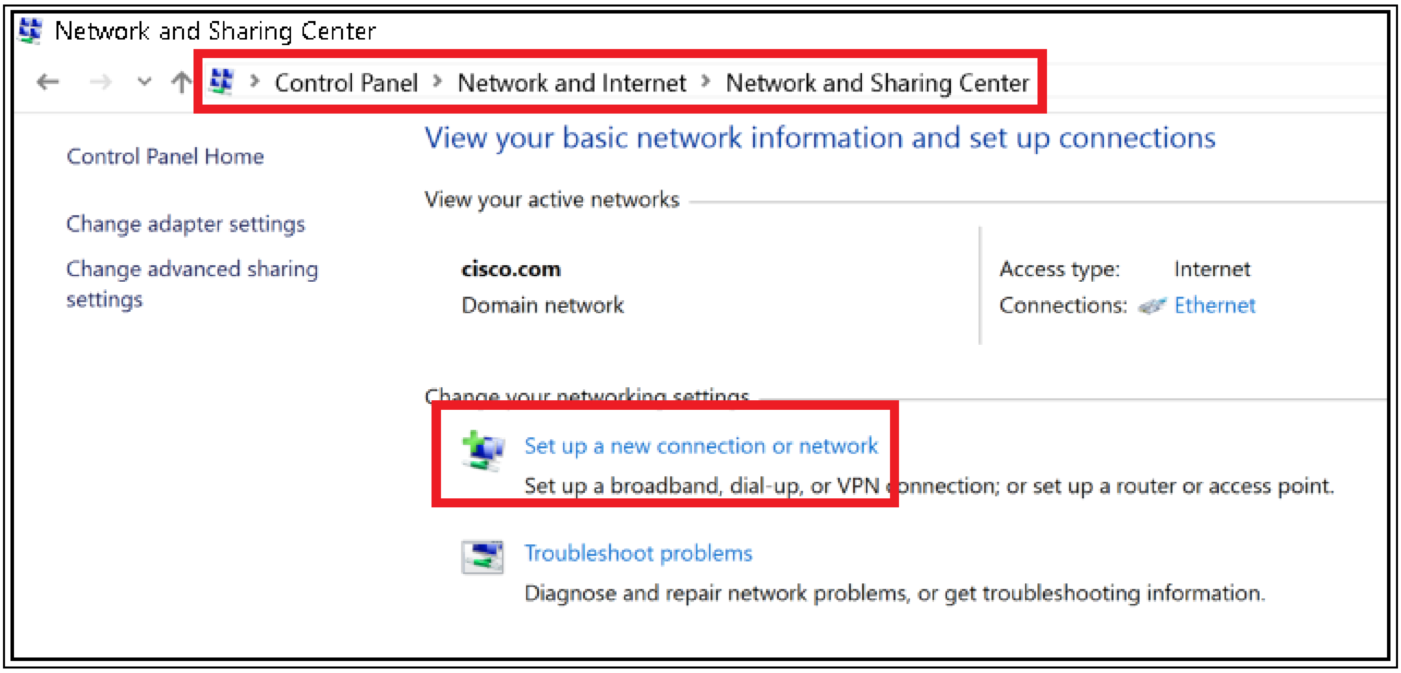
The import was successful.

장치 구성 종료 - WLAN 프로파일 만들기

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



2단계. **네트워크 및 인터넷**으로 이동한 다음 **네트워크 및 공유 센터**로 이동하여 **새 연결 또는 네트워크 설정을 클릭합니다.**



Network and Sharing Center

Control Panel › Network and Internet › Network and Sharing Center

Control Panel Home

Change adapter settings

Change advanced sharing settings

View your basic network information and set up connections

View your active networks

cisco.com
Domain network

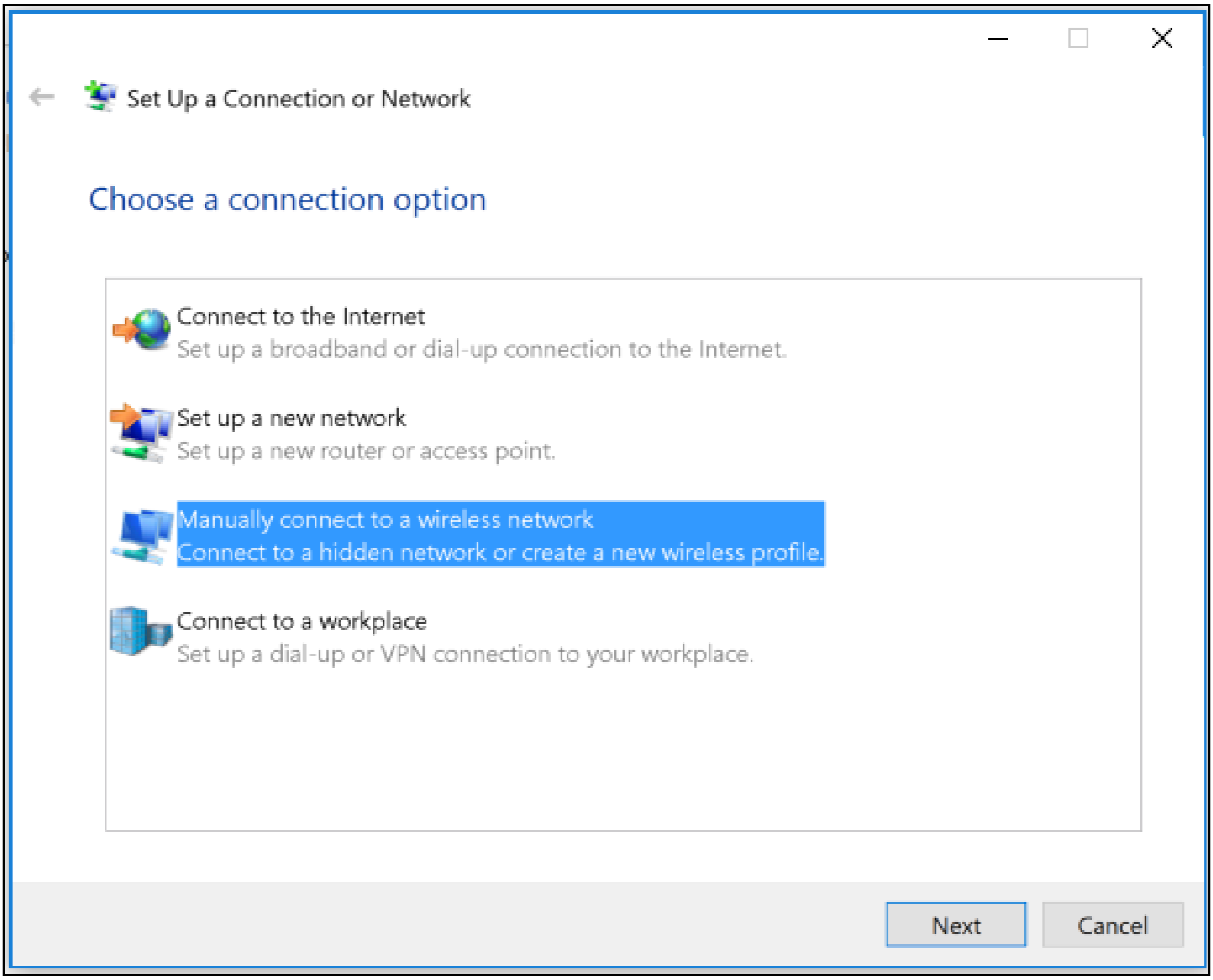
Access type: Internet
Connections: Ethernet

Change your networking settings

Set up a new connection or network
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

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



Set Up a Connection or Network

Choose a connection option

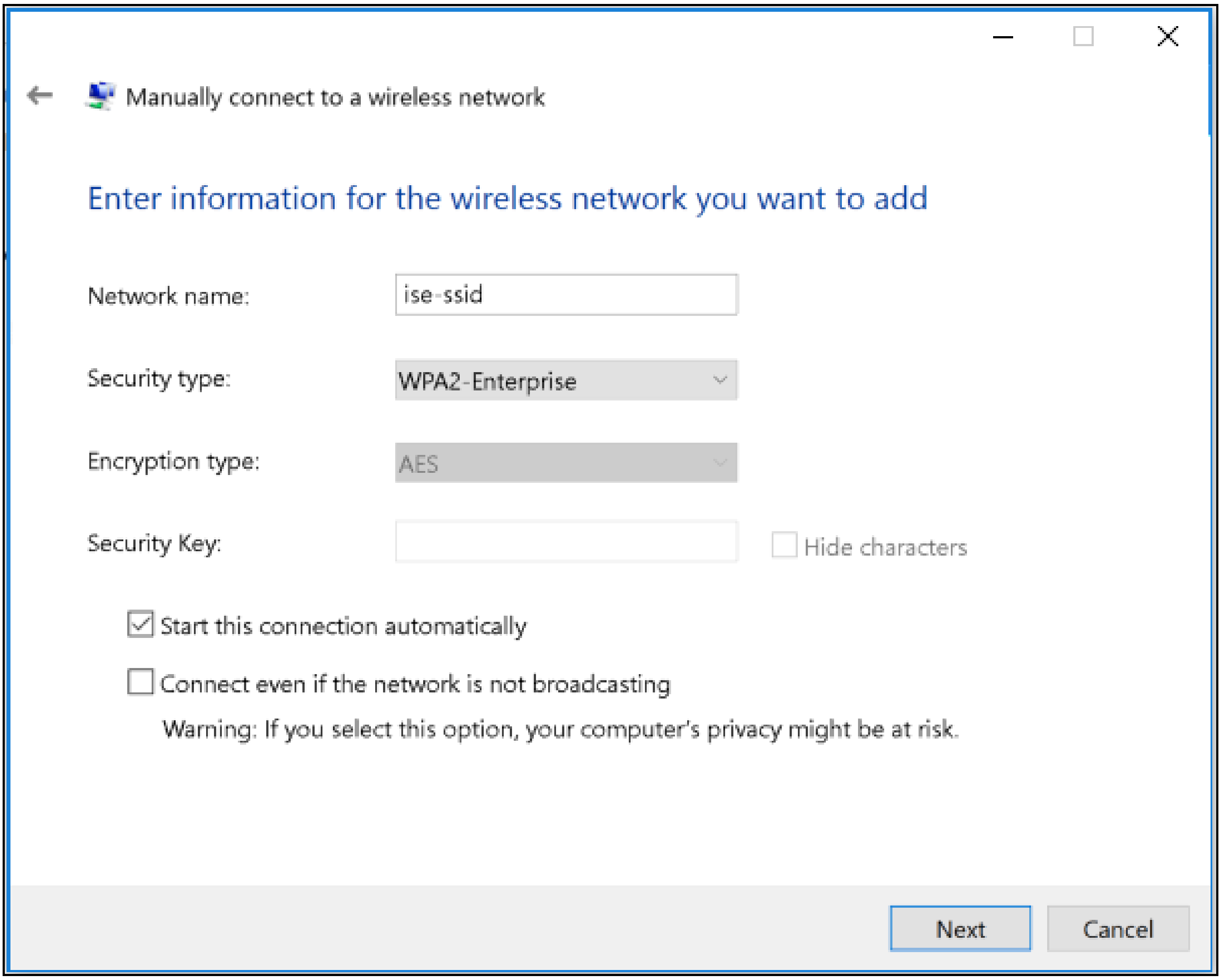
Connect to the Internet
Set up a broadband or dial-up connection to the Internet.

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.

4단계. SSID 및 보안 유형 WPA2-Enterprise의 이름으로 정보를 입력하고 **Next**를 클릭합니다.



Manually connect to a wireless network

Enter information for the wireless network you want to add

Network name: ise-ssid

Security type: WPA2-Enterprise

Encryption type: AES

Security Key:

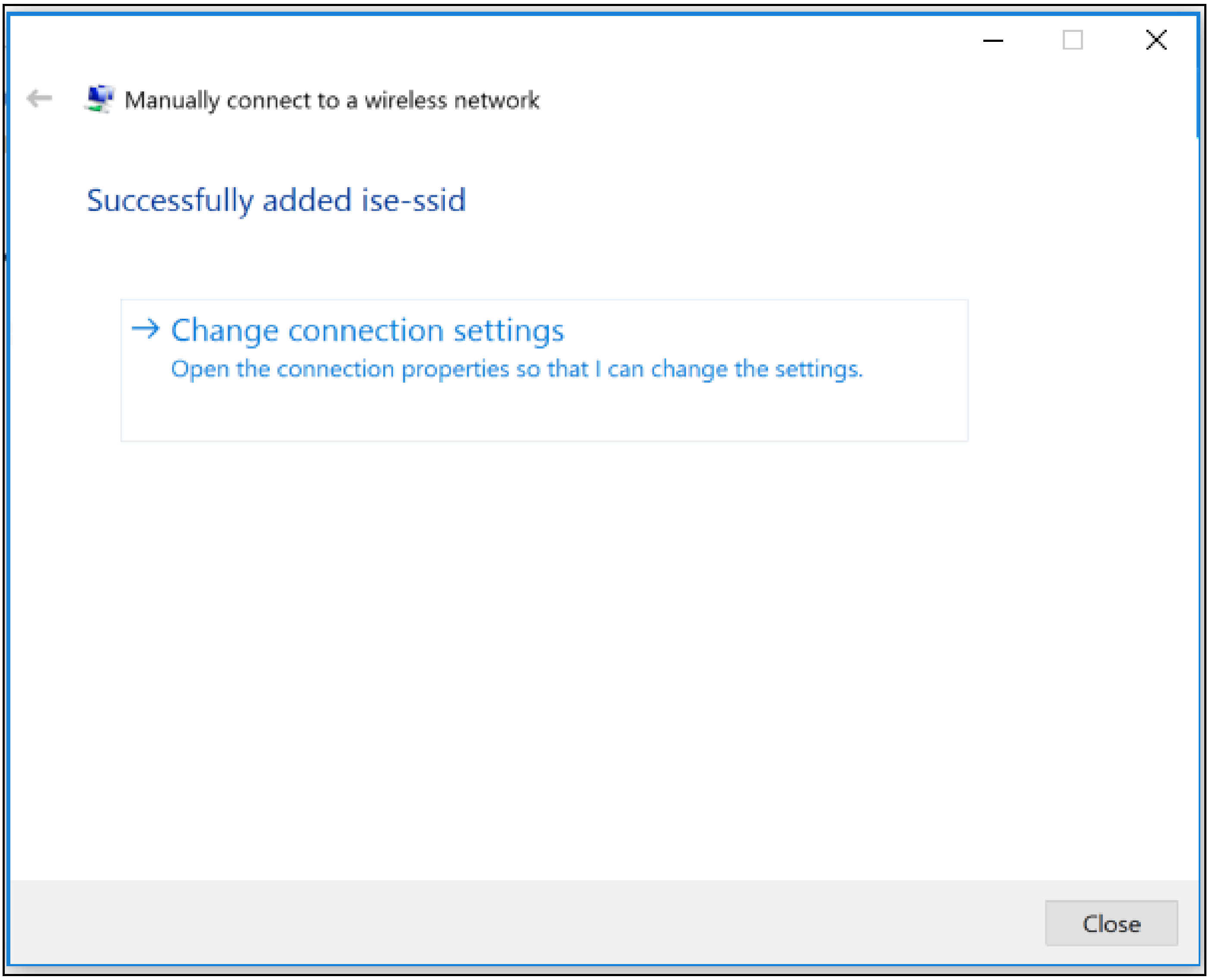
□ Hide characters

☑ Start this connection automatically

□ Connect even if the network is not broadcasting

Warning: If you select this option, your computer's privacy might be at risk.

5단계. **연결 설정 변경**을 선택하여 WLAN 프로파일의 컨피그레이션을 사용자 지정합니다.

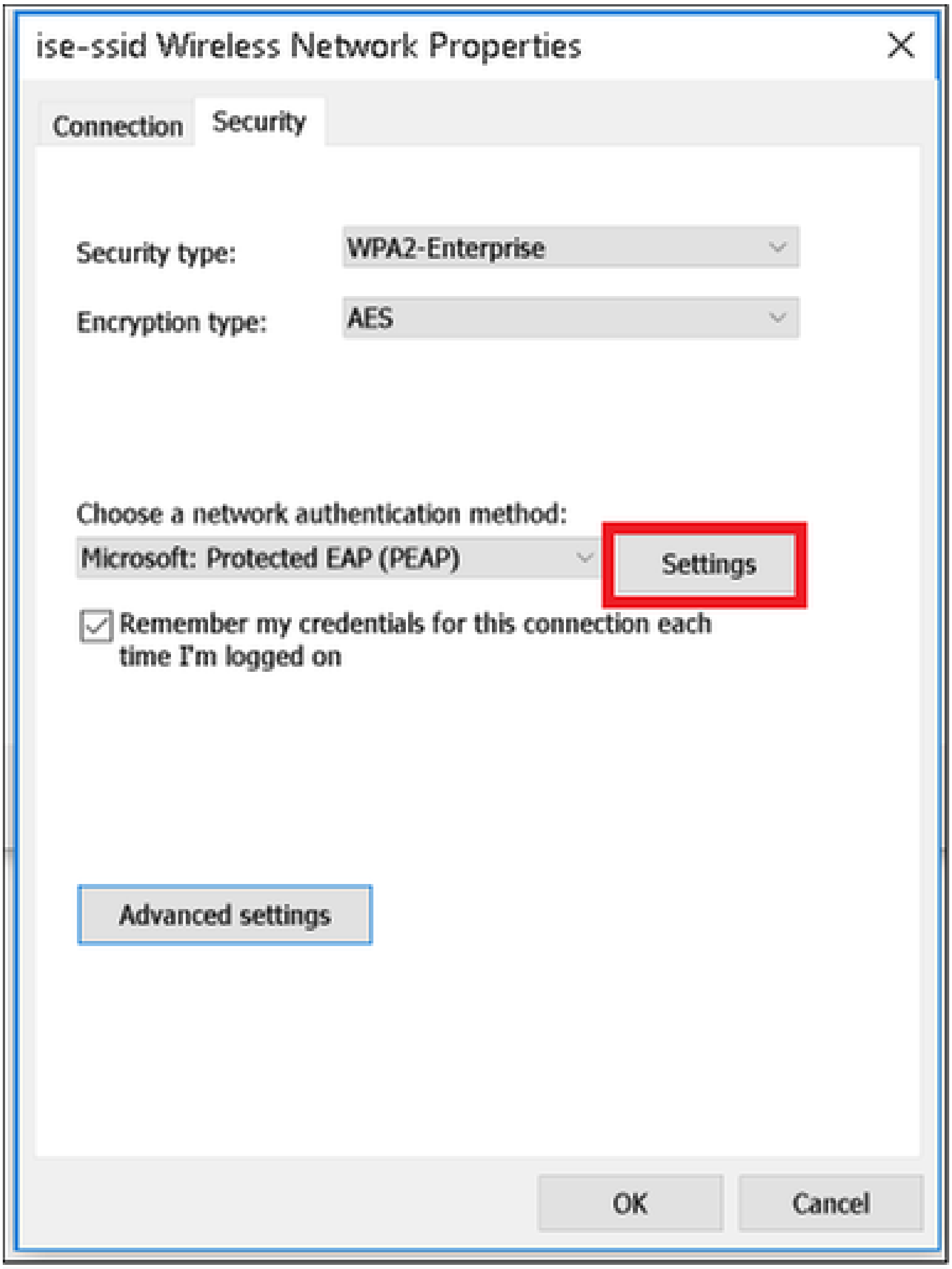


Manually connect to a wireless network

Successfully added ise-ssid

→ Change connection settings
Open the connection properties so that I can change the settings.

6단계. **보안** 탭으로 이동하고 **설정**을 클릭합니다.



ise-ssid Wireless Network Properties

Security type: WPA2-Enterprise

Encryption type: AES

Choose a network authentication method:

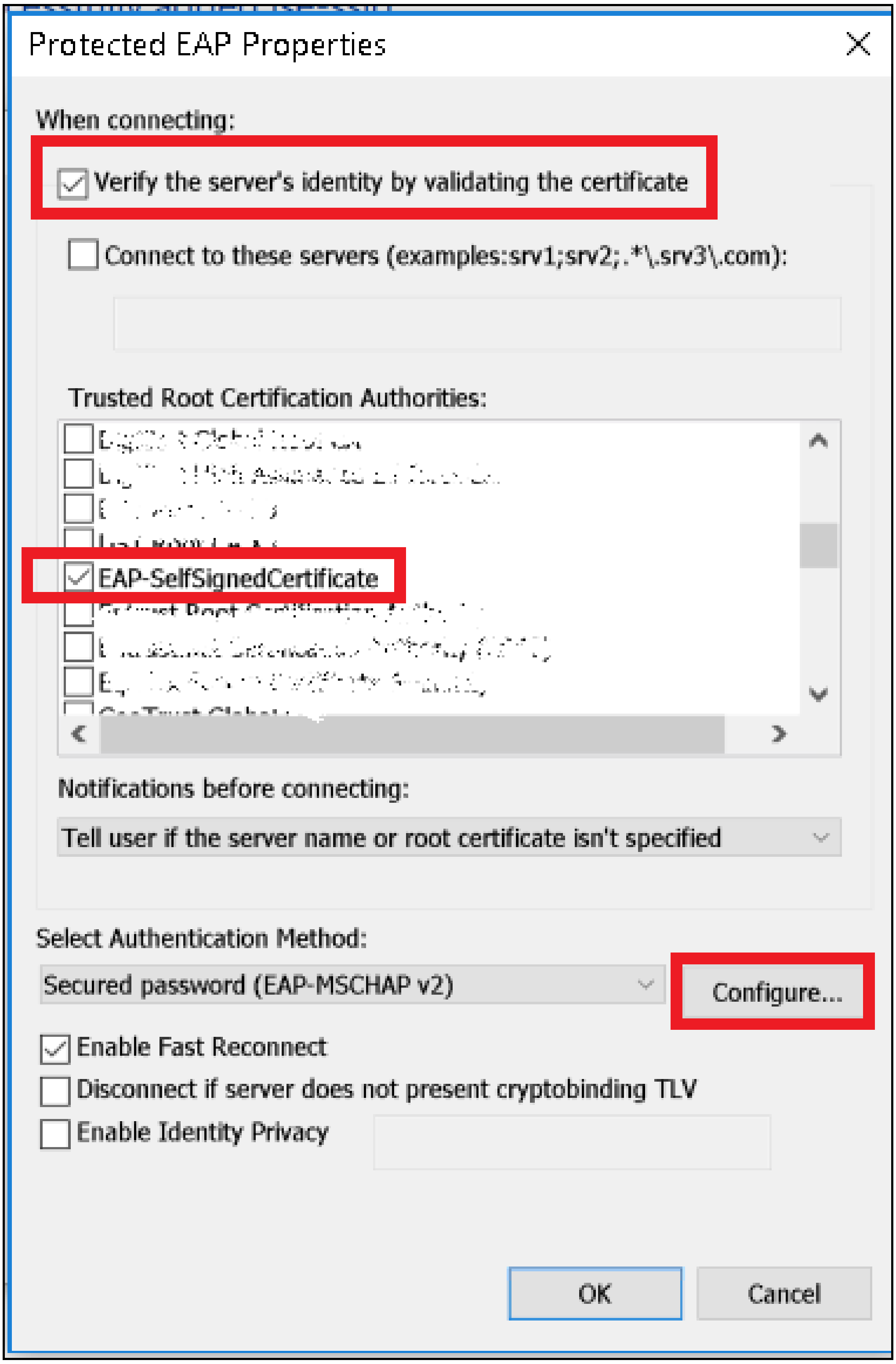
Microsoft: Protected EAP (PEAP)

☑ Remember my credentials for this connection each time I'm logged on

7단계. RADIUS 서버가 유효한지 여부를 선택합니다.

대답이 "예"인 경우 **Verify the server's identity by validating the certificate** and from Trusted **Root Certification Authorities:** list(신뢰할 수 있는 루트 인증 기관: 목록)에서 ISE의 자체 서명 인증서를 선택합니다.

그런 다음 **Configure** and disable **Automatically use my Windows logon name and password...를** 선택하고 **확인**을 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:

□ [illegible]
□ [illegible]
□ [illegible]
□ [illegible]
☑ EAP-SelfSignedCertificate
□ Entrust Root Certification Autho[illegible]
□ [illegible]
□ [illegible]
□ GeoTrust Global [illegible]

Notifications before connecting:

Tell user if the server name or root certificate isn't specified

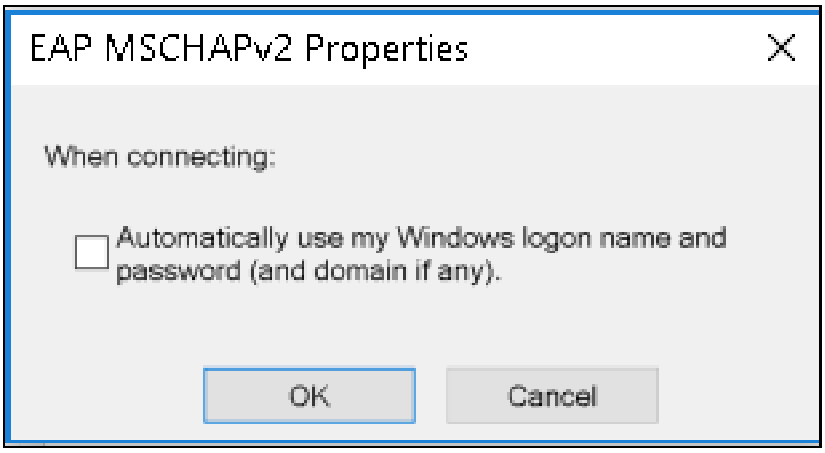
Select Authentication Method:

Secured password (EAP-MSCHAP v2)

☑ Enable Fast Reconnect

□ Disconnect if server does not present cryptobinding TLV

□ Enable Identity Privacy



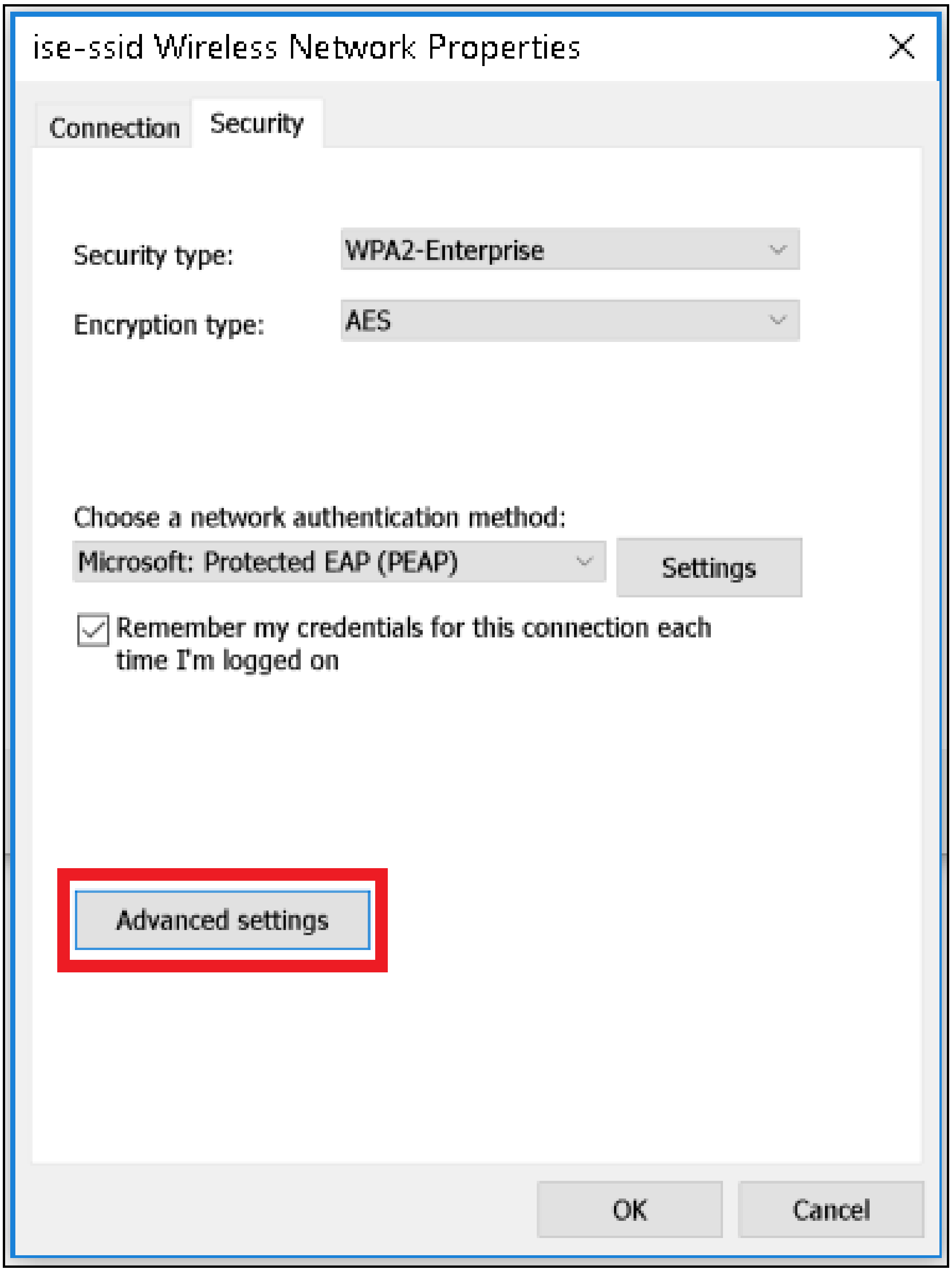
EAP MSCHAPv2 Properties

When connecting:

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

8단계. 사용자 자격 증명을 구성합니다.

다시 **보안** 탭으로 돌아가서 **고급 설정**을 선택하고 인증 모드를 **사용자 인증**으로 지정하고 ISE에서 사용자를 인증하도록 구성된 자격 증명을 저장합니다.



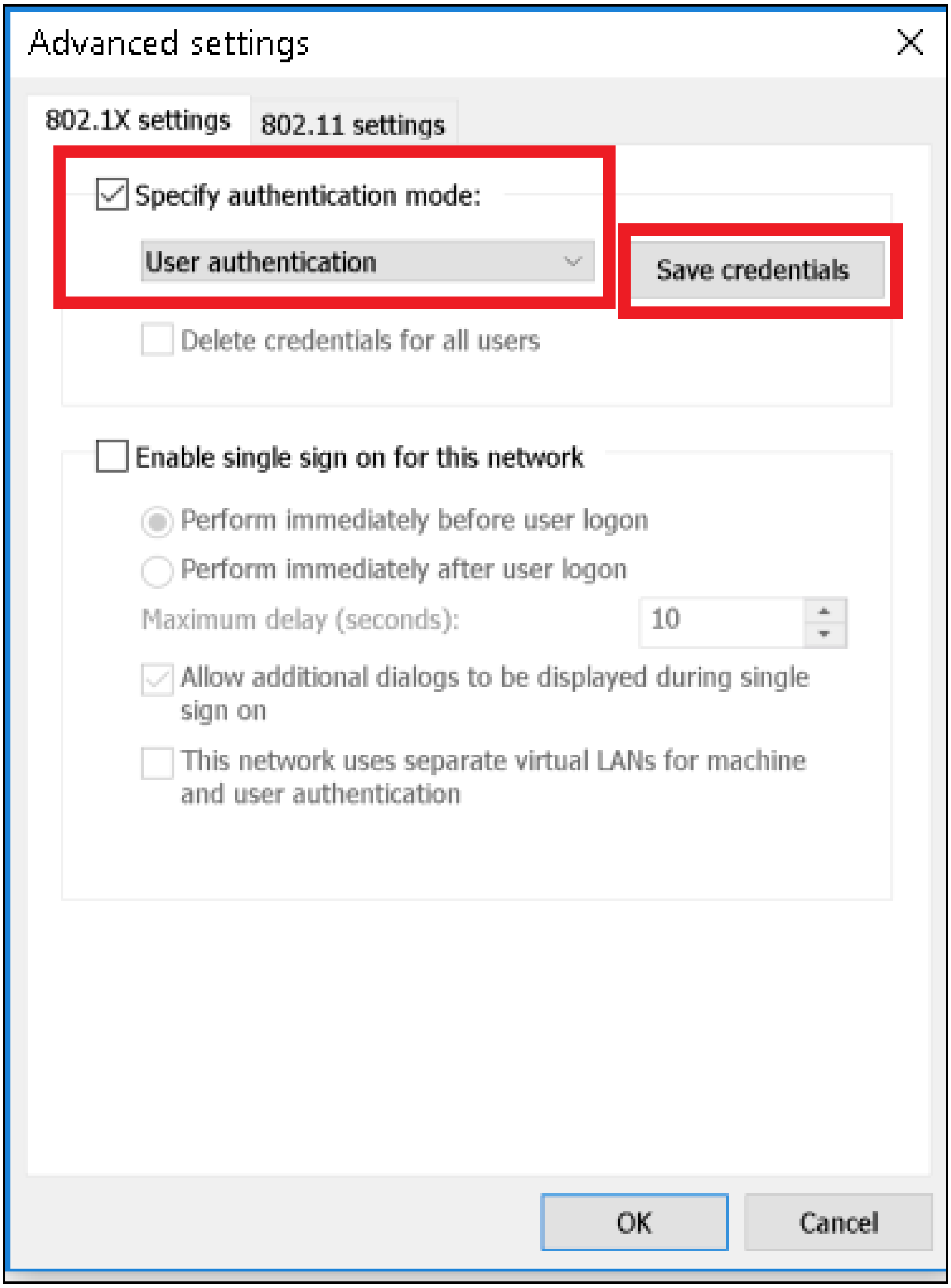
ise-ssid Wireless Network Properties

Security type: WPA2-Enterprise

Encryption type: AES

Choose a network authentication method: Microsoft: Protected EAP (PEAP)

☑ Remember my credentials for this connection each time I'm logged on



Advanced settings

802.1X settings | 802.11 settings

☑ Specify authentication mode:

User authentication

□ Delete credentials for all users

□ Enable single sign on for this network

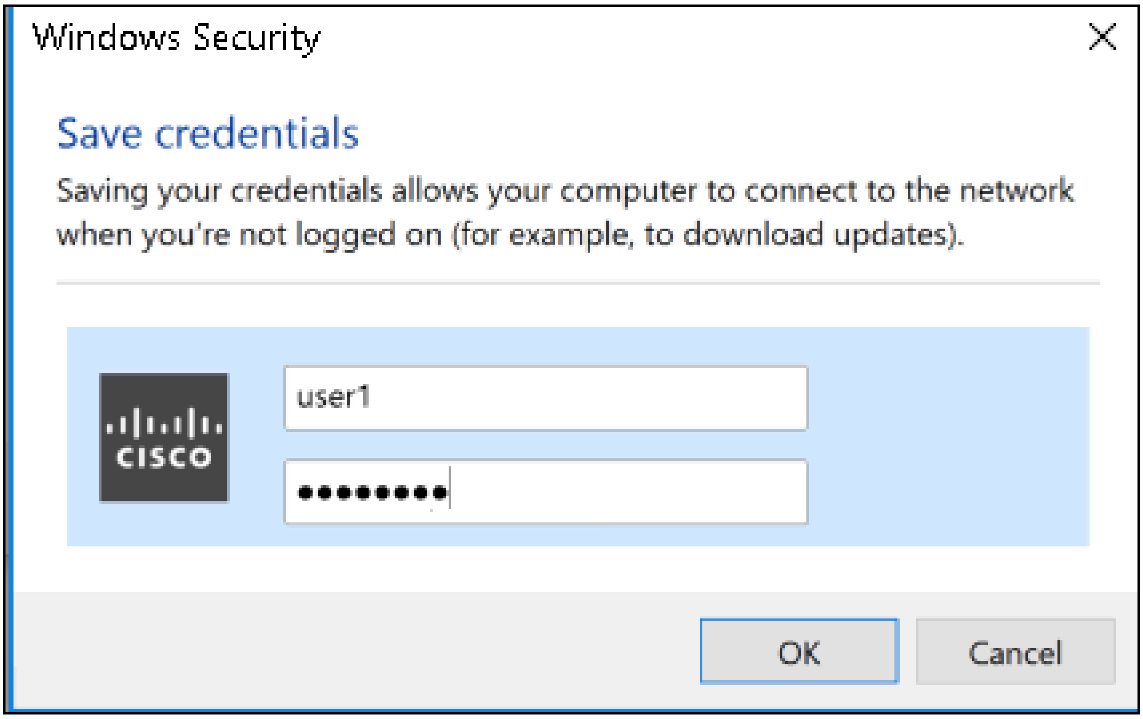
● Perform immediately before user logon

○ Perform immediately after user logon

Maximum delay (seconds): 10

☑ Allow additional dialogs to be displayed during single sign on

□ This network uses separate virtual LANs for machine and user authentication


Windows Security

Save credentials

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

user1

●●●●●●●●●

다음을 확인합니다.

인증 흐름은 WLC 또는 ISE 관점에서 확인할 수 있습니다.

ME의 인증 프로세스

특정 사용자에 대한 인증 프로세스를 모니터링하려면 다음 명령을 실행합니다.

```
> debug client <mac-add-client>
```

성공적인 인증의 예(일부 출력이 생략됨):

```
*apfMsConnTask_0: Nov 25 16:36:24.333: 08:74:02:77:13:45 Processing assoc-req
station:08:74:02:77:13:45 AP:38:ed:18:c6:7b:40-01 thread:669ba80
*apfMsConnTask_0: Nov 25 16:36:24.333: 08:74:02:77:13:45 Association received from mobile on
BSSID 38:ed:18:c6:7b:4d AP 1852-4
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 Applying site-specific Local Bridging
override for station 08:74:02:77:13:45 - vapId 3, site 'FlexGroup', interface 'management'
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 Applying Local Bridging Interface
Policy for station 08:74:02:77:13:45 - vlan 0, interface id 0, interface 'management'
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 Set Clinet Non AP specific
apfMsAccessVlan = 2400
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 This apfMsAccessVlan may be changed
later from AAA after L2 Auth
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 Received 802.11i 802.1X key management
suite, enabling dot1x Authentication
*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 0.0.0.0 START (0) Change state to
AUTHCHECK (2) last state START (0)
*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 0.0.0.0 AUTHCHECK (2) Change state to
8021X_REQD (3) last state AUTHCHECK (2)
*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 0.0.0.0 8021X_REQD (3) DHCP required on
```

```
AP 38:ed:18:c6:7b:40 vapId 3 apVapId 3for this client
*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 apfPemAddUser2:session timeout
forstation 08:74:02:77:13:45 - Session Tout 0, apfMsTimeOut '0' and sessionTimerRunning flag is
0
*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 Stopping deletion of Mobile Station:
(callerId: 48)
*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 Func: apfPemAddUser2, Ms Timeout = 0,
Session Timeout = 0
*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 Sending assoc-resp with status 0
station:08:74:02:77:13:45 AP:38:ed:18:c6:7b:40-01 on apVapId 3
*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 Sending Assoc Response to station on
BSSID 38:ed:18:c6:7b:4d (status 0) ApVapId 3 Slot 1
*spamApTask0: Nov 25 16:36:24.341: 08:74:02:77:13:45 Sent dot1x auth initiate message for mobile
08:74:02:77:13:45
*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 reauth_sm state transition 0 ---> 1
for mobile 08:74:02:77:13:45 at 1x_reauth_sm.c:47
*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 EAP-PARAM Debug - eap-params for
Wlan-Id :3 is disabled - applying Global eap timers and retries
*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 Disable re-auth, use PMK lifetime.
*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 Station 08:74:02:77:13:45 setting
dot1x reauth timeout = 1800
*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 dot1x - moving mobile
08:74:02:77:13:45 into Connecting state
*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 Sending EAP-Request/Identity to
mobile 08:74:02:77:13:45 (EAP Id 1)
*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.401: 08:74:02:77:13:45 Received EAPOL EAPPKT from mobile
08:74:02:77:13:45
*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.401: 08:74:02:77:13:45 Received Identity Response (count=1)
from mobile 08:74:02:77:13:45
.
.
.
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.978: 08:74:02:77:13:45 Processing Access-Accept for mobile
08:74:02:77:13:45
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.978: 08:74:02:77:13:45 Username entry (user1) created in
mscb for mobile, length = 253
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.978: 08:74:02:77:13:45 Station 08:74:02:77:13:45 setting
dot1x reauth timeout = 1800
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.978: 08:74:02:77:13:45 Creating a PKC PMKID Cache entry for
station 08:74:02:77:13:45 (RSN 2)
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Adding BSSID 38:ed:18:c6:7b:4d to
PMKID cache at index 0 for station 08:74:02:77:13:45
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: New PMKID: (16)
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: [0000] 80 3a 20 8c 8f c2 4c 18 7d 4c 28 e7 7f 10 11 03
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Adding Audit session ID payload in
Mobility handoff
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 0 PMK-update groupcast messages sent
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 PMK sent to mobility group
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Disabling re-auth since PMK lifetime
can take care of same.
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Sending EAP-Success to mobile
08:74:02:77:13:45 (EAP Id 70)
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Freeing AAACB from Dot1xCB as AAA
auth is done for mobile 08:74:02:77:13:45
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Found an cache entry for BSSID
38:ed:18:c6:7b:4d in PMKID cache at index 0 of station 08:74:02:77:13:45
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Found an cache entry for BSSID
38:ed:18:c6:7b:4d in PMKID cache at index 0 of station 08:74:02:77:13:45
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: Including PMKID in M1 (16)
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: [0000] 80 3a 20 8c 8f c2 4c 18 7d 4c 28 e7 7f 10 11 03
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: M1 - Key Data: (22)
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: [0000] dd 14 00 0f ac 04 80 3a 20 8c 8f c2 4c 18 7d 4c
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: [0016] 28 e7 7f 10 11 03
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Starting key exchange to mobile
```

```
08:74:02:77:13:45, data packets will be dropped
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 Sending EAPOL-Key Message to mobile
08:74:02:77:13:45
state INITPMK (message 1), replay counter 00.00.00.00.00.00.00.00
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 Reusing allocated memory for EAP Pkt
for retransmission to mobile 08:74:02:77:13:45
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 Entering Backend Auth Success state
(id=70) for mobile 08:74:02:77:13:45
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 Received Auth Success while in
Authenticating state for mobile 08:74:02:77:13:45
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 dot1x - moving mobile
08:74:02:77:13:45 into Authenticated state
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.983: 08:74:02:77:13:45 Received EAPOL-Key from mobile
08:74:02:77:13:45
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.983: 08:74:02:77:13:45 Received EAPOL-key in PTK_START
state (message 2) from mobile 08:74:02:77:13:45
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.983: 08:74:02:77:13:45 Successfully computed PTK from
PMK!!!
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.983: 08:74:02:77:13:45 Received valid MIC in EAPOL Key
Message M2!!!!!
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 00000000: 30 14 01 00 00 0f ac 04 01 00 00 0f ac 04 01
00 0..............
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 00000010: 00 0f ac 01 0c 00 ......
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 00000000: 01 00 00 0f ac 04 01 00 00 0f ac 04 01 00 00
0f ...............
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 00000010: ac 01 0c 00 ....
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 08:74:02:77:13:45 PMK: Sending cache add
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 08:74:02:77:13:45 Stopping retransmission timer for
mobile 08:74:02:77:13:45
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 08:74:02:77:13:45 Sending EAPOL-Key Message to mobile
08:74:02:77:13:45
 state PTKINITNEGOTIATING (message 3), replay counter 00.00.00.00.00.00.00.01
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 08:74:02:77:13:45 Reusing allocated memory for EAP Pkt
for retransmission to mobile 08:74:02:77:13:45
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Received EAPOL-key in
PTKINITNEGOTIATING state (message 4) from mobile 08:74:02:77:13:45
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Stopping retransmission timer for
mobile 08:74:02:77:13:45
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 8021X_REQD (3) Change state
to L2AUTHCOMPLETE (4) last state 8021X_REQD (3)
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Mobility query, PEM State:
L2AUTHCOMPLETE
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Building Mobile Announce :
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Building Client Payload:
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Client Ip: 0.0.0.0
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Client Vlan Ip: 172.16.0.136, Vlan
mask : 255.255.255.224
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Client Vap Security: 16384
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Virtual Ip: 192.0.2.1
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 ssid: ise-ssid
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Building VlanIpPayload.
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 L2AUTHCOMPLETE (4) DHCP
required on AP 38:ed:18:c6:7b:40 vapId 3 apVapId 3for this client
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Not Using WMM Compliance code qosCap
00
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 L2AUTHCOMPLETE (4) Plumbed
mobile LWAPP rule on AP 38:ed:18:c6:7b:40 vapId 3 apVapId 3 flex-acl-name:
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 L2AUTHCOMPLETE (4) Change
state to DHCP_REQD (7) last state L2AUTHCOMPLETE (4)
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7)
pemAdvanceState2 6623, Adding TMP rule
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) Adding Fast
Path rule
type = Airespace AP - Learn IP address
```

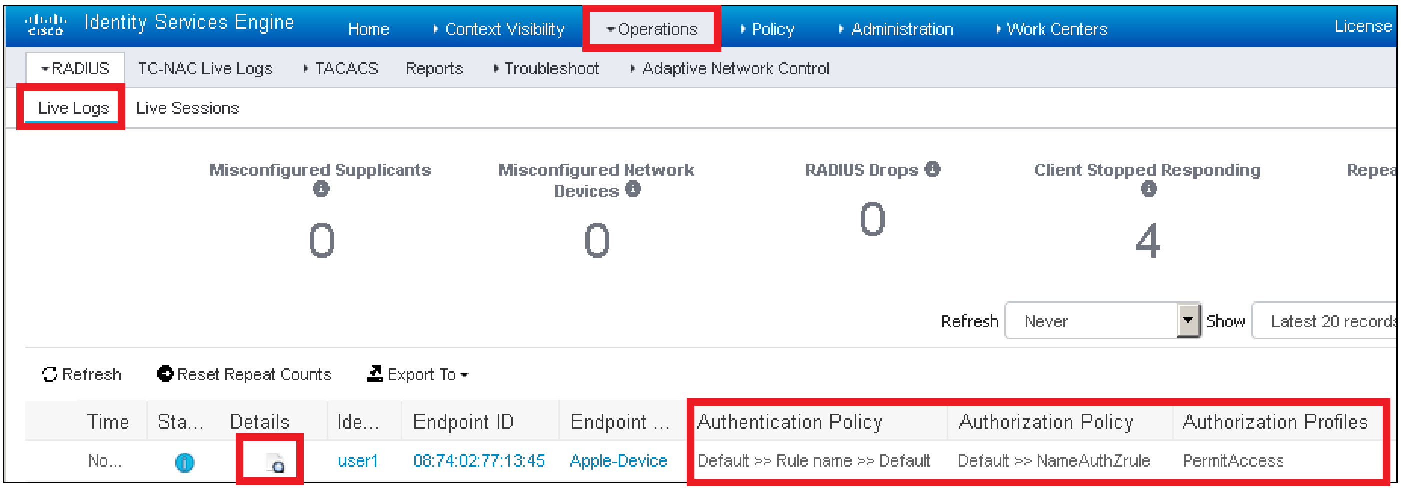
```
on AP 38:ed:18:c6:7b:40, slot 1, interface = 1, QOS = 0
IPv4 ACL ID = 255, IPv
*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) mobility role
update request from Unassociated to Local
Peer = 0.0.0.0, Old Anchor = 0.0.0.0, New Anchor = 172.16.0.136
*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) State Update from
Mobility-Incomplete to Mobility-Complete, mobility role=Local, client
state=APF_MS_STATE_ASSOCIATED
*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) pemAdvanceState2
6261, Adding TMP rule
*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) Replacing Fast
Path rule
type = Airespace AP - Learn IP address
on AP 38:ed:18:c6:7b:40, slot 1, interface = 1, QOS = 0
IPv4 ACL ID = 255,
*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) Successfully
plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255)
*pemReceiveTask: Nov 25 16:36:25.990: 08:74:02:77:13:45 0.0.0.0 Added NPU entry of type 9,
dtlFlags 0x0
*pemReceiveTask: Nov 25 16:36:25.990: 08:74:02:77:13:45 0.0.0.0 Added NPU entry of type 9,
dtlFlags 0x0
*apfReceiveTask: Nov 25 16:36:27.835: 08:74:02:77:13:45 WcdbClientUpdate: IP Binding from WCDB
ip_learn_type 1, add_or_delete 1
*apfReceiveTask: Nov 25 16:36:27.835: 08:74:02:77:13:45 IPv4 Addr: 0:0:0:0
*apfReceiveTask: Nov 25 16:36:27.835: 08:74:02:77:13:45 In apfRegisterIpAddrOnMscb_debug:
regType=1 Invalid src IP address, 0.0.0.0 is part of reserved ip address range (caller
apf_ms.c:3593)
*apfReceiveTask: Nov 25 16:36:27.835: 08:74:02:77:13:45 IPv4 Addr: 0:0:0:0
*apfReceiveTask: Nov 25 16:36:27.840: 08:74:02:77:13:45 WcdbClientUpdate: IP Binding from WCDB
ip_learn_type 1, add_or_delete 1
*apfReceiveTask: Nov 25 16:36:27.841: 08:74:02:77:13:45 172.16.0.16 DHCP_REQD (7) Change state
to RUN (20) last state DHCP_REQD (7)
```

디버그 클라이언트 출력을 쉽게 읽을 수 있도록 *무선 디버그 분석기* 도구를 사용하십시오.

무선 디버그 분석기

ISE의 인증 프로세스

Operations(작업) > RADIUS > Live Logs(라이브 로그)로 이동하여 사용자에게 할당된 인증 정책, 권한 부여 정책 및 권한 부여 프로파일을 확인합니다.



Time	Sta...	Details	Ide...	Endpoint ID	Endpoint ...	Authentication Policy	Authorization Policy	Authorization Profiles
No...			user1	08:74:02:77:13:45	Apple-Device	Default >> Rule name >> Default	Default >> NameAuthZrule	PermitAccess

자세한 내용을 보려면 **Details(세부 정보)**를 클릭하여 더 자세한 인증 프로세스를 확인하십시오.