

# PEAP, ISE 2.1 및 WLC 8.3으로 802.1X 인증 구성

## 목차

---

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[구성](#)

[네트워크 다이어그램](#)

[설정](#)

[WLC에서 RADIUS 서버 선언](#)

[SSID 생성](#)

[ISE에서 WLC 선언](#)

[ISE에서 새 사용자 생성](#)

[인증 구조 생성](#)

[권한 부여 프로파일 생성](#)

[권한 부여 규칙 생성](#)

[엔드 디바이스 컨피그레이션](#)

[최종 디바이스 컨피그레이션 - ISE 자체 서명 인증서 설치](#)

[End Device Configuration\(엔드 디바이스 컨피그레이션\) - WLAN Profile\(WLAN 프로필 생성\)](#)

[다음을 확인합니다.](#)

[WLC의 인증 프로세스](#)

[ISE의 인증 프로세스](#)

[문제 해결](#)

---

## 소개

이 문서에서는 802.1x 보안 및 VLAN(Virtual Local Area Network) 재정의로 WLAN(Wireless Local Area Network)을 설정하는 방법에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 802.1x
- PEAP(Protected Extensible Authentication Protocol)
- CA(인증 기관)
- 인증서

## 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- WLC v8.3.102.0
- ISE(Identity Service Engine) v2.1
- Windows 10 랩톱

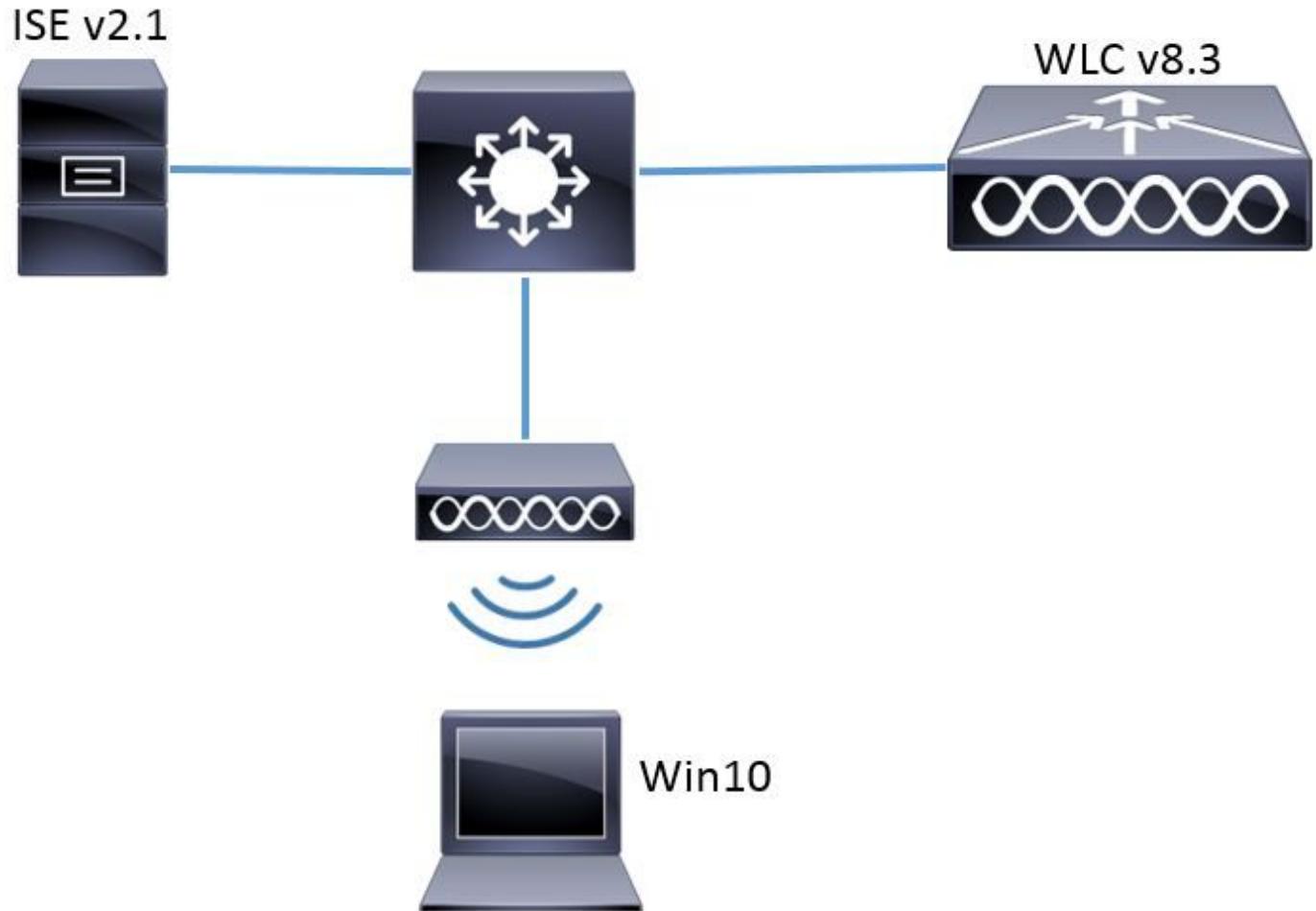
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

## 배경 정보

802.1x 보안 및 VLAN을 사용하여 WLAN을 설정할 경우 EAP(Extensible Authentication Protocol as Extensible Authentication Protocol)로 보호되는 EAP로 재정의할 수 있습니다.

## 구성

### 네트워크 다이어그램



## 설정

일반적인 단계는 다음과 같습니다.

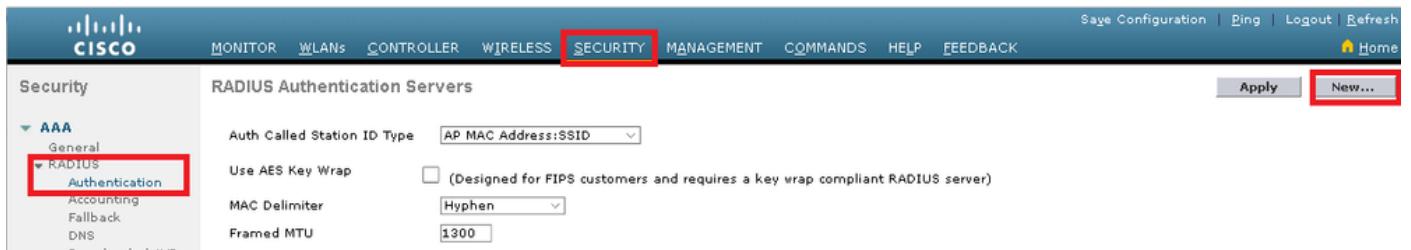
1. WLC에서 RADIUS 서버를 선언하거나 그 반대로 선언하여 서로 통신을 허용합니다.
2. WLC에서 SSID(Service Set Identifier)를 생성합니다.
3. ISE에서 인증 규칙을 생성합니다.
4. ISE에서 권한 부여 프로파일을 생성합니다.
5. ISE에서 권한 부여 규칙을 생성합니다.
6. 앤드포인트를 구성합니다.

### WLC에서 RADIUS 서버 선언

RADIUS 서버와 WLC 간의 통신을 허용하려면 WLC에 RADIUS 서버를 등록해야 하며 그 반대의 경우도 마찬가지입니다.

GUI:

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



2단계. 이미지에 표시된 대로 RADIUS 서버 정보를 입력합니다.

RADIUS Authentication Servers > 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 <input type="checkbox"/> (Designed for FIPS customers and requires a key wrap compliant RADIUS server)	
Port Number	1812
Server Status	Enabled
Support for CoA	Disabled
Server Timeout	10 seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input checked="" type="checkbox"/> Enable
Management Retransmit Timeout	2 seconds
IPSec	<input type="checkbox"/> Enable

CLI:

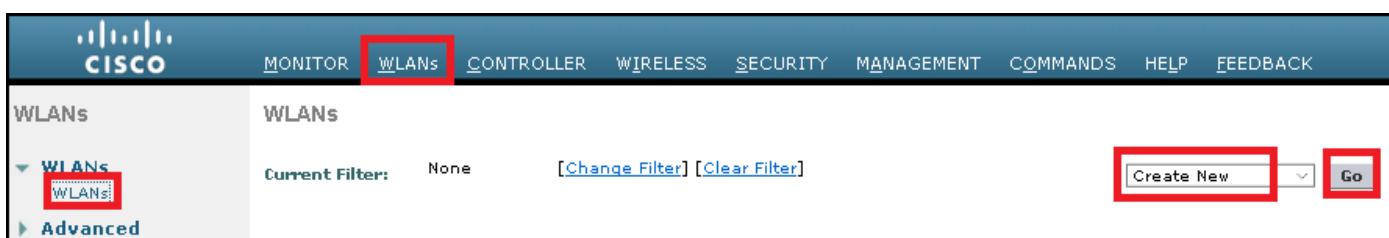
```
> config radius auth add <index> <a.b.c.d> 1812 ascii <shared-key>
> config radius auth disable <index>
> config radius auth retransmit-timeout <index> <timeout-seconds>
> config radius auth enable <index>
```

<a.b.c.d>는 RADIUS 서버에 해당합니다.

SSID 생성

GUI:

1단계. 이미지에 표시된 대로 WLC의 GUI를 열고 WLANs(WLAN) > Create New(새로 만들기) > Go(이동)로 이동합니다.



2단계. SSID 및 프로필의 이름을 선택한 다음 이미지에 표시된 대로 Apply(적용)를 클릭합니다.

WLANs > New

< Back **Apply**

Type	WLAN
Profile Name	profile-name
SSID	SSID-name
ID	2

CLI:

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

3단계. RADIUS 서버를 WLAN에 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 누릅니다.

WLANs > Edit 'ise-prof'

**General** **Security** **QoS** **Policy-Mapping** **Advanced**

**Layer 2** **Layer 3** **AAA Servers**

Select AAA servers below to override use of default servers on this WLAN

**RADIUS Servers**

RADIUS Server Overwrite interface  Enabled

Authentication Servers	Accounting Servers	EAP Parameters
<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	Enable <input type="checkbox"/>
Server 1 IP:172.16.15.8, Port:1812	None	None
Server 2 None	None	None
Server 3 None	None	None
Server 4 None	None	None
Server 5 None	None	None
Server 6 None	None	None

**RADIUS Server Accounting**

Interim Update  Interim Interval  Seconds

4단계. Allow AAA Override(AAA 재정의 허용)를 활성화하고 선택적으로 세션 시간 제한을 늘립니다.

CLI:

```
> config wlan aaa-override enable <wlan-id>
> config wlan session-timeout <wlan-id> <session-timeout-seconds>
```

GUI:

WLANs(WLAN) > WLAN ID > Advanced(고급)로 이동하고 Allow AAA Override(AAA 재정의 허용)를 활성화합니다. 선택적으로 이미지에 표시된 대로 Session Timeout을 지정합니다.

General		Security		QoS		Policy-Mapping		Advanced	
Allow AAA Override <input checked="" type="checkbox"/> Enabled		Coverage Hole Detection <input checked="" type="checkbox"/> Enabled		Enable Session Timeout <input checked="" type="checkbox"/> 28800 <small>Session Timeout (secs)</small>		DHCP			
						DHCP Server <input type="checkbox"/> Override			
						DHCP Addr. Assignment <input type="checkbox"/> Required			
Aironet IE <input checked="" type="checkbox"/> Enabled		Diagnostic Channel <a href="#">18</a> <input type="checkbox"/> Enabled		Override Interface ACL IPv4 <input type="checkbox"/> None		IPv6 <input type="checkbox"/> None		802.11a/n (1 - 255) <input type="checkbox"/> 1	
Layer2 Adc <input type="checkbox"/> None		URL Adc <input type="checkbox"/> None		P2P Blocking Action <input type="checkbox"/> Disabled		Client Exclusion <a href="#">2</a> <input checked="" type="checkbox"/> Enabled 60 <small>Timeout Value (secs)</small>		802.11b/g/n (1 - 255) <input type="checkbox"/> 1	
Maximum Allowed Clients <a href="#">3</a> <input type="checkbox"/> 0		Static IP Tunneling <input type="checkbox"/> . . .		NAC State <input type="checkbox"/> None		Management Frame Protection (MFP)			
						MFP Client Protection <a href="#">4</a> <input type="checkbox"/> Optional			
						DTIM Period (in beacon intervals)			
						NAC			

5단계. WLAN을 활성화합니다.

CLI:

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

GUI:

이미지에 표시된 대로 WLANS(WLAN) > WLAN ID > General(일반)로 이동하여 SSID를 활성화합니다.

WLANS > Edit 'ise-prof'

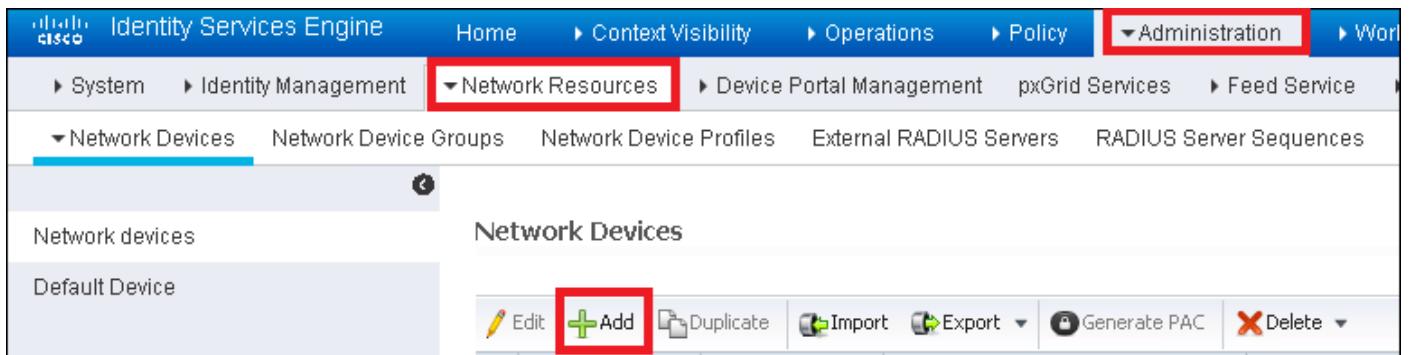
[Back](#) [Apply](#)

**General** **Security** **QoS** **Policy-Mapping** **Advanced**

Profile Name	ise-prof
Type	WLAN
SSID	ise-ssid
Status	<input checked="" type="checkbox"/> Enabled
Security Policies [WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)	
Radio Policy	All
Interface/Interface Group(G)	management
Multicast Vlan Feature	<input type="checkbox"/> Enabled
Broadcast SSID	<input checked="" type="checkbox"/> Enabled
NAS-ID	none

## ISE에서 WLC 선언

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



## 2단계. 값을 입력합니다.

선택적으로, 지정된 모델 이름, 소프트웨어 버전, 설명이 될 수 있으며 디바이스 유형, 위치 또는 WLC에 따라 네트워크 디바이스 그룹을 할당할 수 있습니다.

a.b.c.d는 요청된 인증을 전송하는 WLC 인터페이스에 해당합니다. 기본적으로 이미지에 표시된 대로 관리 인터페이스입니다.

Network Devices List > New Network Device

Network Devices

\* Name

Description

\* IP Address:  /

\* Device Profile  Cisco

Model Name

Software Version

\* Network Device Group

Device Type

Location

WLCs



▼ RADIUS Authentication Settings

Enable Authentication Settings

Protocol **RADIUS**

\* Shared Secret

Enable KeyWrap  

\* Key Encryption Key

\* Message Authenticator Code Key

Key Input Format  ASCII  HEXADECIMAL

CoA Port

네트워크 디바이스 그룹에 대한 자세한 내용은 다음을 참조하십시오.

[ISE - 네트워크 디바이스 그룹](#)

## ISE에서 새 사용자 생성

1단계. 이미지에 표시된 대로 Administration > Identity Management > Identities > Users > Add로 이동합니다.

The screenshot shows the ISE web interface with the following navigation path: Home > Context Visibility > Operations > Policy > Administration > Identity Management > Identities > Users. The 'Users' tab is selected. On the right, a sidebar titled 'System' lists various management options like Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Backup & Restore, Admin Access, and Settings. Below the sidebar, another 'Identity Management' section has a 'Identities' tab highlighted with a red box. The main content area displays a table titled 'Network Access Users' with columns for Status, Name, and Description. A message 'Loading...' is visible. At the top of the table, there are buttons for Edit, Add (highlighted with a red box), Change Status, Import, and Export.

2단계. 정보를 입력합니다.

이 예에서 이 사용자는 ALL\_ACCOUNTS라는 그룹에 속하지만, 이미지에 표시된 대로 필요에 따라 조정할 수 있습니다.

## Network Access Users List > New Network Access User

### Network Access User

\* Name

Status  Enabled

Email

### Passwords

Password Type: Internal Users

\* Login Password

Re-Enter Password

Enable Password

### User Information

First Name

Last Name

### Account Options

Description

Change password on next login

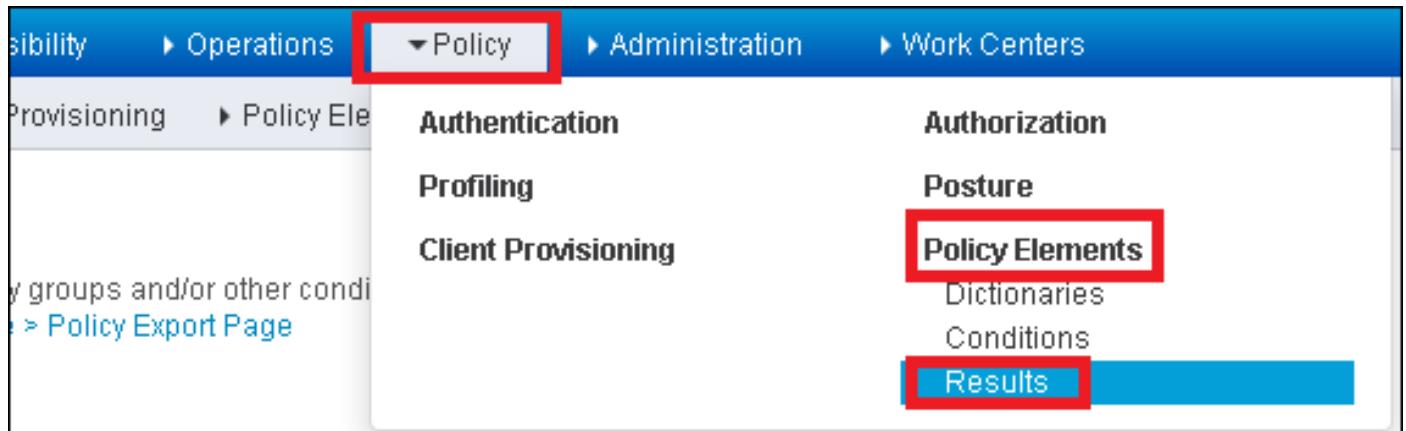
### Account Disable Policy

Disable account if date exceeds

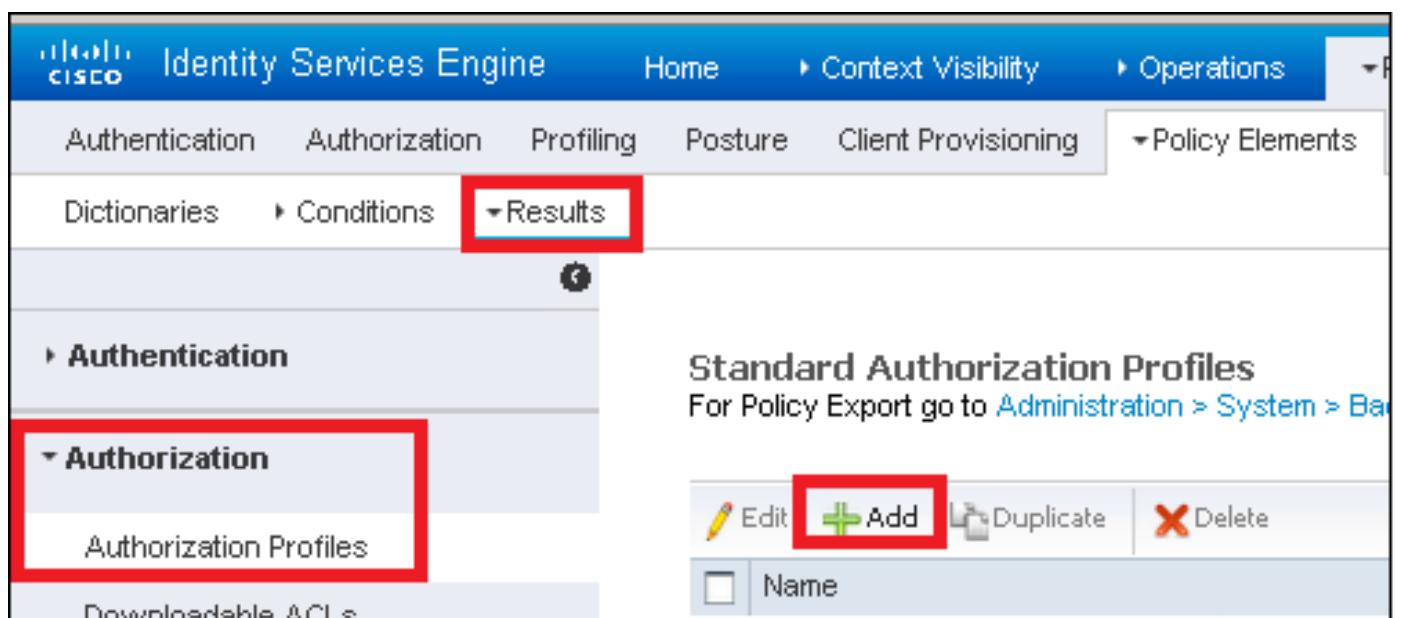
### User Groups

재정의 또는 기타 매개변수. 이 예에 표시된 권한 부여 프로파일은 액세스 승인을 사용자에게 전송하고 VLAN 2404를 할당합니다.

1단계. 이미지에 표시된 대로 Policy > Policy Elements > Results로 이동합니다.



2단계. 새 권한 부여 프로파일을 추가합니다. 이미지에 표시된 대로 Authorization Profiles > Add로 이동합니다.



3단계. 이미지에 표시된 대로 값을 입력합니다.

## Authorization Profiles > New Authorization Profile

### Authorization Profile

* Name	PermitAccessVLAN2404	
Description		
* Access Type	ACCESS_ACCEPT	▼
Network Device Profile	Cisco	▼
Service Template	<input type="checkbox"/>	
Track Movement	<input type="checkbox"/>	
Passive Identity Tracking	<input type="checkbox"/>	

### Common Tasks

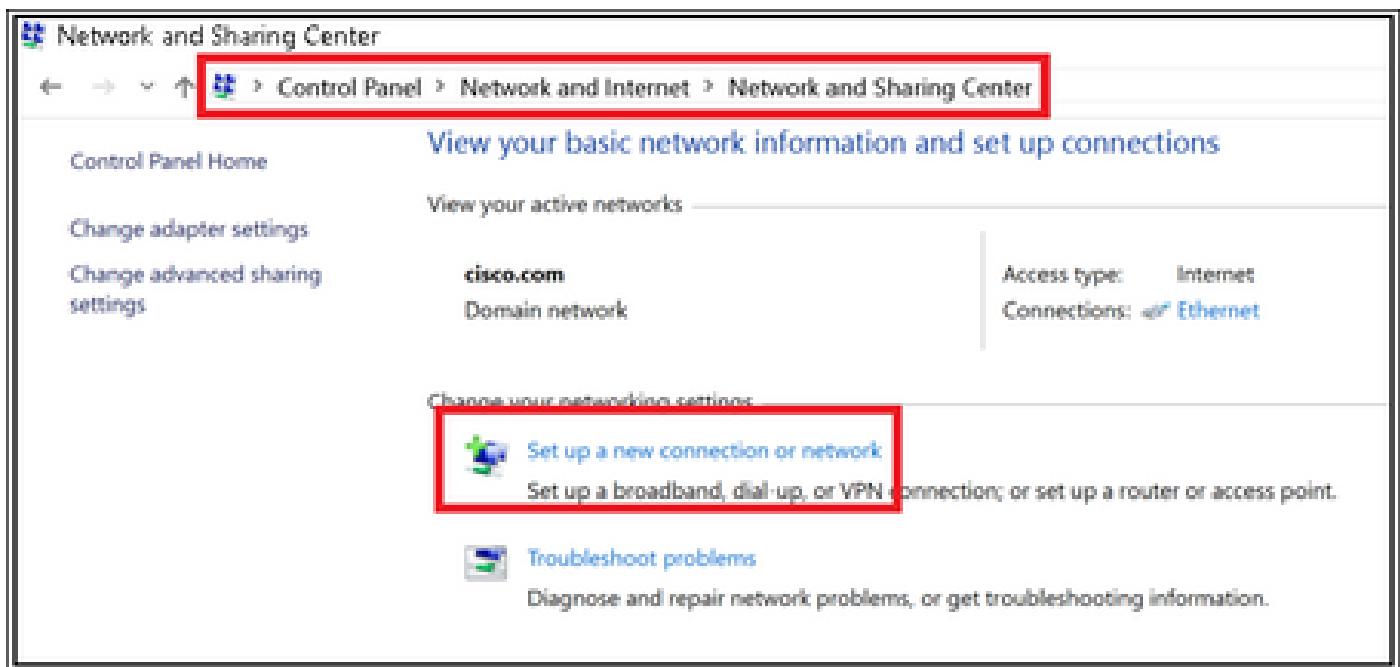
<input type="checkbox"/> ACL (Filter-ID)	
<input checked="" type="checkbox"/> VLAN	Tag ID <input type="text" value="0"/> Edit Tag
<input type="checkbox"/> Voice Domain Permission	ID/Name <input type="text" value="2404"/>
<input type="checkbox"/> Web Redirection (CNAME MDM NCD PDD)	

### Advanced Attributes Settings

Select an item	=	<input type="text"/>
----------------	---	----------------------

### Attributes Details

Access Type = ACCESS\_ACCEPT  
Tunnel-Private-Group-ID = NaN:2404  
Tunnel-Type = NaN:13  
Tunnel-Medium-Type = NaN:6



3단계. 이미지에 표시된 대로 Manually connect to a wireless network(무선 네트워크에 수동으로 연결)를 선택하고 Next(다음)를 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.

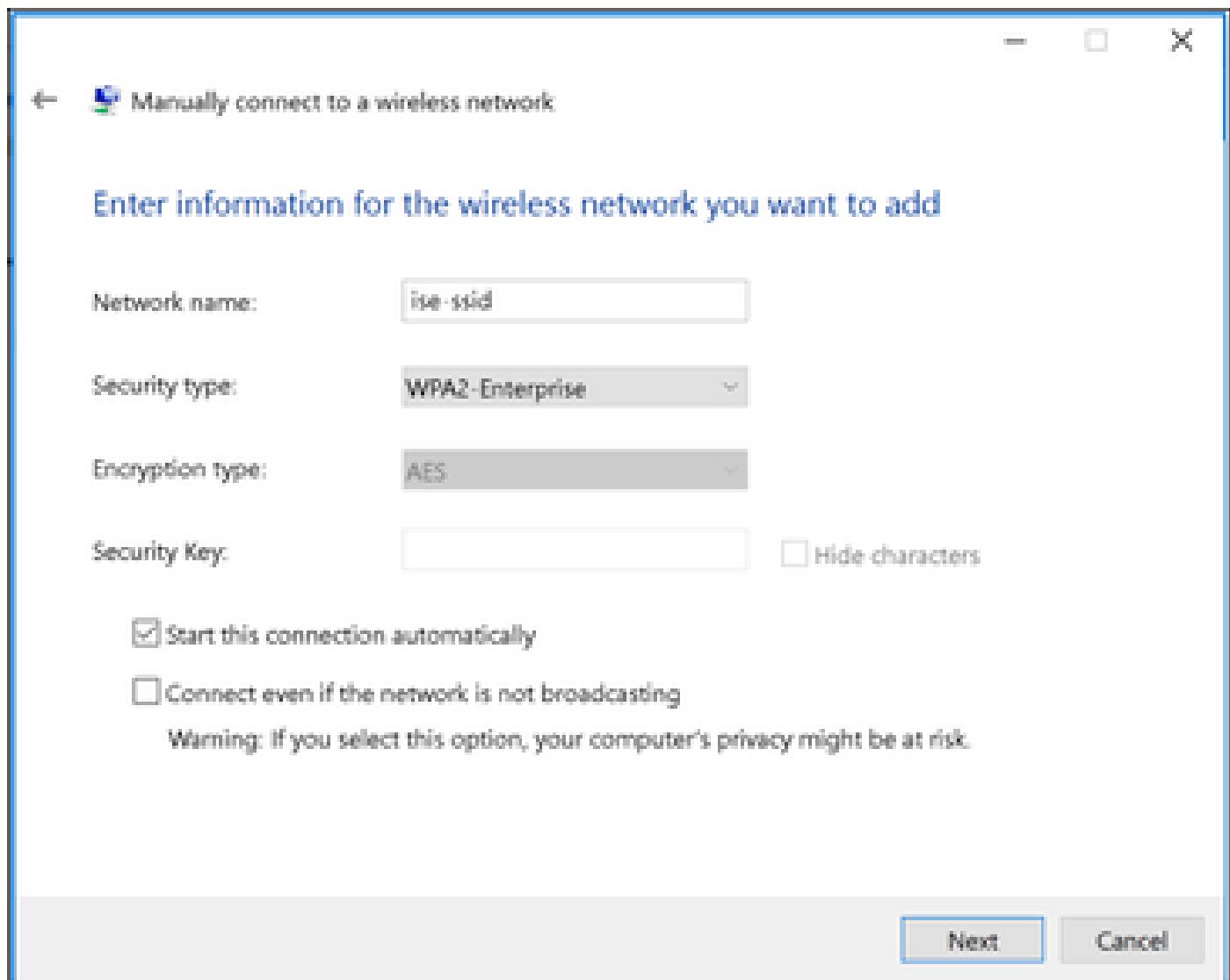
 Connect to a workplace

Set up a dial-up or VPN connection to your workplace.

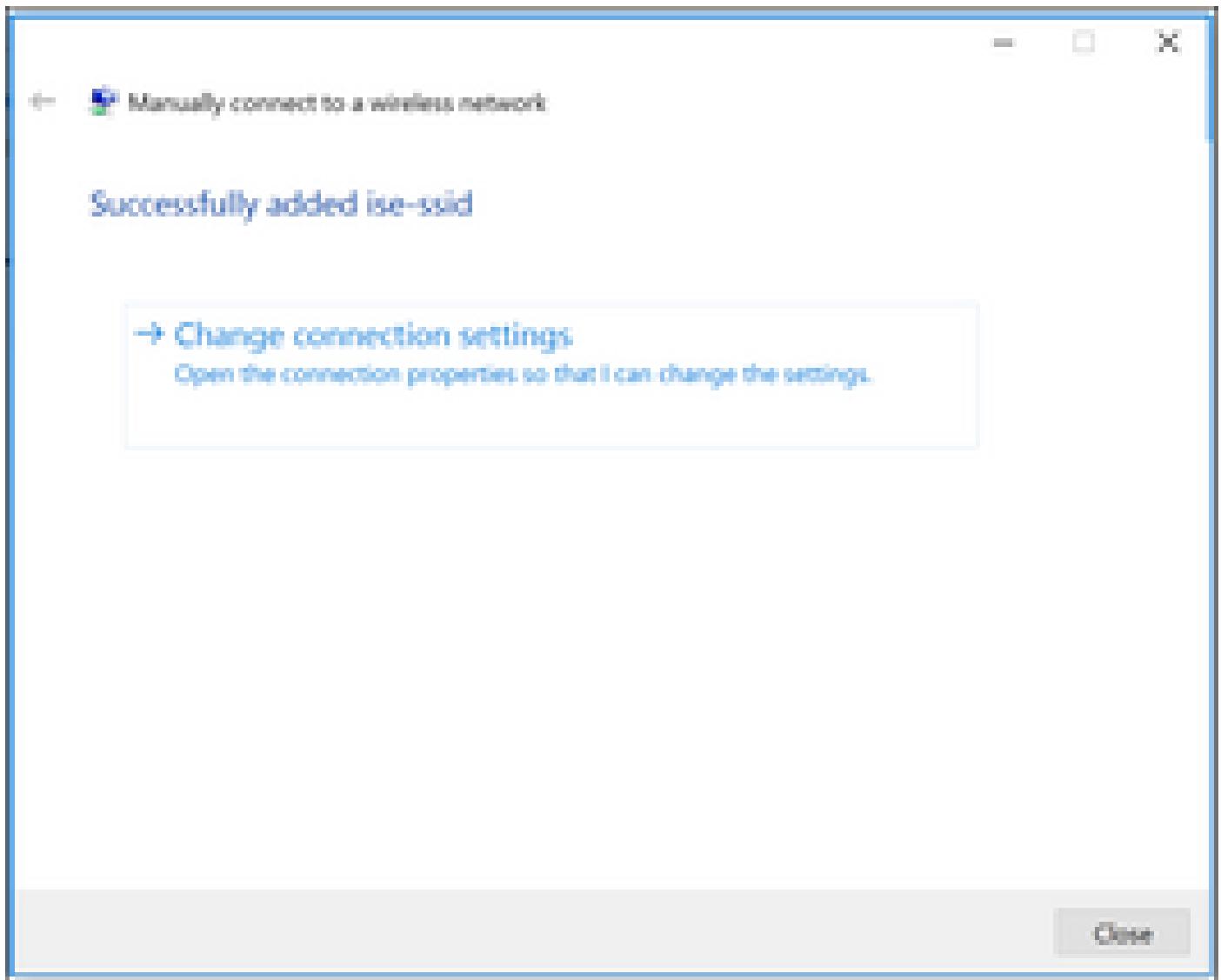
Next

Cancel

4단계. 이미지에 표시된 대로 SSID 이름 및 보안 유형 WPA2-Enterprise의 정보를 입력하고 Next(다음)를 클릭합니다.



5단계. 이미지에 표시된 대로 WLAN 프로파일의 컨피그레이션을 사용자 지정하려면 연결 설정 변경을 선택합니다.



6단계. 이미지에 표시된 대로 Security(보안) 탭으로 이동하고 Settings(설정)를 클릭합니다.

## ise-ssid Wireless Network Properties

X

Connection Security

Security type: WPA2-Enterprise

Encryption type: AES

Choose a network authentication method:

Microsoft: Protected EAP (PEAP)

Settings

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

Advanced settings

OK

Cancel

7단계. RADIUS 서버가 유효한지 여부를 선택합니다.

대답이 "예"인 경우 Verify server identity by validating the certificate(인증서를 검증하여 서버 ID 확인)를 활성화하고 Trusted Root Certification Authorities(신뢰할 수 있는 루트 인증 기관) 목록에서 ISE의 자체 서명 인증서를 선택합니다.

그런 다음 구성 및 사용 안 함 내 Windows 로그온 이름 및 암호 자동 사용...을 선택한 다음 이미지에 표시된 대로 확인을 클릭합니다.

## Protected EAP Properties

X

When connecting:

Verify the server's identity by validating the certificate

Connect to these servers (examples: srv1;srv2; \*.srv3.com):

Trusted Root Certification Authorities:

Local Computer Certificate Store  
 Local Computer Personal Certificate Store  
 Enterprise Certificate Store  
 Trusted Publishers

EAP-SelfSignedCertificate

Microsoft Default Certificate Store  
 Trusted Root Certification Authorities Certificate Store  
 Enterprise Root Certificate Store  
 Current User Certificate Store

Notifications before connecting:

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



Select Authentication Method:

Secured password (EAP-MSCHAP v2)

Configure...

Enable Fast Reconnect

Disconnect if server does not present cryptobinding TLV

Enable Identity Privacy

OK

Cancel

Security(보안) 탭으로 돌아가면 Advanced(고급) 설정을 선택하고, 인증 모드를 User authentication(사용자 인증)으로 지정한 다음 ISE에서 구성한 자격 증명을 저장하여 이미지에 표시된 대로 사용자를 인증합니다.

## ise-ssid Wireless Network Properties



Connection Security

Security type: WPA2-Enterprise

Encryption type: AES

Choose a network authentication method:

Microsoft: Protected EAP (PEAP)

Settings

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

Advanced settings

OK

Cancel

## 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

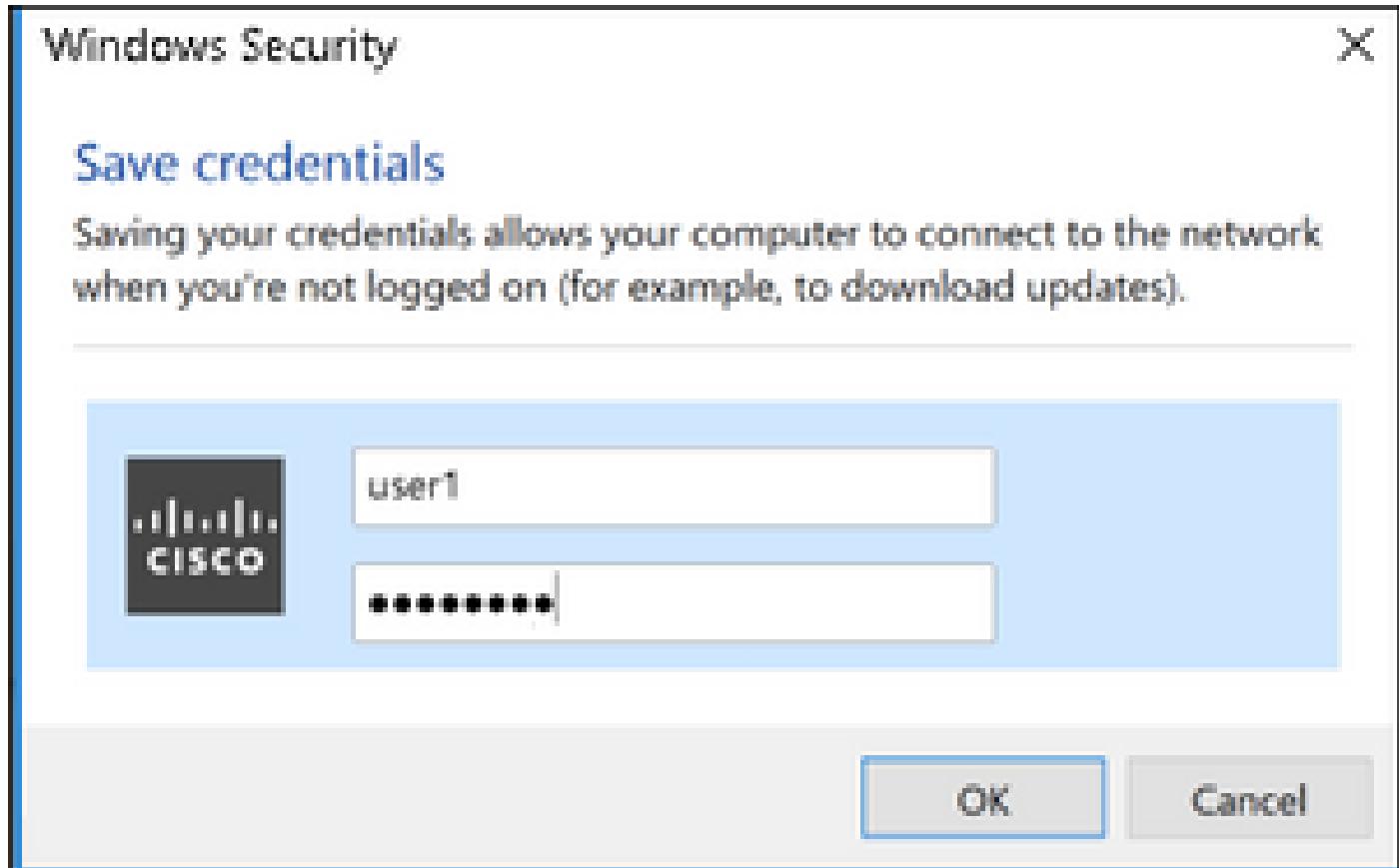
Maximum delay (seconds):

10



Allow additional dialogs to be displayed during single sign-on

This network uses separate virtual LANs for machine and user authentication



다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

인증 흐름은 WLC 또는 ISE 관점에서 확인 할 수 있습니다.

### 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
```

성공적인 인증의 예(일부 출력이 생략됨):

```
<#root>
```

```
*apfMsConnTask_1: Nov 24 04:30:44.317:
```

```
e4:b3:18:7c:30:58 Processing assoc-req station:e4:b3:18:7c:30:58 AP:00:c8:8b:26:2c:d0-00
```

```
thread:1a5cc288
```

```
*apfMsConnTask_1: Nov 24 04:30:44.317: e4:b3:18:7c:30:58 Reassociation received from mobile on BSSID 00
```

```
*apfMsConnTask_1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 Applying Interface(management) policy on Mobil
```

```
*apfMsConnTask_1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 Applying site-specific Local Bridging override
*apfMsConnTask_1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 Applying Local Bridging Interface Policy for s
*apfMsConnTask_1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 RSN Capabilities: 60
*apfMsConnTask_1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 Marking Mobile as non-
e4:b3:18:7c:30:58 Received 802.11i 802.1X key management suite, enabling dot1x Authentication
11w Capable
*apfMsConnTask_1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 Received RSN IE with 1 PMKIDs from mobile e4:b
*apfMsConnTask_1: Nov 24 04:30:44.319: Received PMKID: (16)
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 Searching for PMKID in MSCB PMKID cache for mo
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 No valid PMKID found in the MSCB PMKID cache f
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 0.0.0.0 START (0) Initializing policy
*apfMsConnTask_1: Nov 24 04:30:44.319:

e4:b3:18:7c:30:58 0.0.0.0 START (0) Change state to AUTHCHECK (2) last state START (0)

*apfMsConnTask_1: Nov 24 04:30:44.319:

e4:b3:18:7c:30:58 0.0.0.0 AUTHCHECK (2) Change state to 8021X_REQD (3) last state AUTHCHECK (2)

*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 0.0.0.0 8021X_REQD (3) Plumbed mobile LWAPP ru
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 apfMsAssoStateInc
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 apfPemAddUser2 (apf_policy.c:437) Changing sta
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 apfPemAddUser2:session timeout for station e4:b
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 Stopping deletion of Mobile Station: (callerId
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 Func: apfPemAddUser2, Ms Timeout = 0, Session
*apfMsConnTask_1: Nov 24 04:30:44.320: e4:b3:18:7c:30:58 Sending Assoc Response to station on BSSID 00:
*spamApTask2: Nov 24 04:30:44.323: e4:b3:18:7c:30:58 Successful transmission of LWAPP Add-Mobile to AP
*spamApTask2: Nov 24 04:30:44.325: e4:b3:18:7c:30:58 Received ADD_MOBILE ack - Initiating 1x to STA e4:
*spamApTask2: Nov 24 04:30:44.325: e4:b3:18:7c:30:58

Sent dot1x auth initiate message for mobile e4:b3:18:7c:30:58

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 reauth_sm state transition 0 ---> 1 for mob
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 EAP-PARAM Debug - eap-params for Wlan-Id :2
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 Disable re-auth, use PMK lifetime.
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 Station e4:b3:18:7c:30:58 setting dot1x rea
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 Stopping reauth timeout for e4:b3:18:7c:30:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 dot1x - moving mobile e4:b3:18:7c:30:58 int
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326:

e4:b3:18:7c:30:58 Sending EAP-Request/Identity to mobile e4:b3:18:7c:30:58 (EAP Id 1)

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 Received EAPOL EAPPKT from mobile e4:b3:18:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 Received Identity Response (count=1) from mo
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 Resetting reauth count 1 to 0 for mobile e4:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 EAP State update from Connecting to Authenti
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 dot1x - moving mobile e4:b3:18:7c:30:58 into
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 Entering Backend Auth Response state for mo
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 Created Acct-Session-ID (58366cf4/e4:b3:18:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.386: e4:b3:18:7c:30:58 Processing Access-Challenge for mobile e4:b
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.387: e4:b3:18:7c:30:58 Entering Backend Auth Req state (id=215) for m
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.387: e4:b3:18:7c:30:58 WARNING: updated EAP-Identifier 1 ===> 215
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.387: e4:b3:18:7c:30:58 Sending EAP Request from AAA to mobile e4:b
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.387: e4:b3:18:7c:30:58 Allocating EAP Pkt for retransmission to mo
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.390: e4:b3:18:7c:30:58 Received EAPOL EAPPKT from mobile e4:b3:18:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.390: e4:b3:18:7c:30:58 Received EAP Response from mobile e4:b3:18:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.390: e4:b3:18:7c:30:58 Resetting reauth count 0 to 0 for mobile e4:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.390: e4:b3:18:7c:30:58 Entering Backend Auth Response state for mo
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.393: e4:b3:18:7c:30:58 Processing Access-Challenge for mobile e4:b
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.393: e4:b3:18:7c:30:58 Entering Backend Auth Req state (id=216) for m
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.393: e4:b3:18:7c:30:58 Sending EAP Request from AAA to mobile e4:b
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.393: e4:b3:18:7c:30:58 Reusing allocated memory for EAP Pkt for re
```

\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.530:

e4:b3:18:7c:30:58 Processing Access-Accept for mobile e4:b3:18:7c:30:58

\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.530: e4:b3:18:7c:30:58 Resetting web IPv4 acl from 255 to 255  
\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.530: e4:b3:18:7c:30:58 Resetting web IPv4 Flex acl from 65535 to 6  
\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.530:

e4:b3:18:7c:30:58 Username entry (user1) created for mobile, length = 253

\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.530:

e4:b3:18:7c:30:58 Found an interface name:'vlan2404' corresponds to interface name received: vlan2404

\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.530: e4:b3:18:7c:30:58 override for default ap group, marking intg  
\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.530: e4:b3:18:7c:30:58 Applying Interface(management) policy on Mo  
\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.530: e4:b3:18:7c:30:58 Re-applying interface policy for client  
\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 apfApplyWlanPolicy: Apply WLAN Policy over  
\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.531:

e4:b3:18:7c:30:58 Inserting AAA Override struct for mobile

MAC: e4:b3:18:7c:30:58, source 4

\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Applying override policy from source Overrid  
\*Dot1x\_NW\_MsgTask\_0: Nov 24

04:30:44.531: e4:b3:18:7c:30:58 Found an interface name:'vlan2404' corresponds to interface name received

\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Applying Interface(vlan2404) policy on Mobi  
\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Re-applying interface policy for client  
\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Setting re-auth timeout to 0 seconds, got f  
\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Station e4:b3:18:7c:30:58 setting dot1x read  
\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Stopping reauth timeout for e4:b3:18:7c:30:  
\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Creating a PKC PMKID Cache entry for station  
\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Resetting MSCB PMK Cache Entry 0 for station  
\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Adding BSSID 00:c8:8b:26:c1 to PMKID cache  
\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.531: New PMKID: (16)  
\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.531: [0000] cc 3a 3d 26 80 17 8b f1 2d c5 cd fd a0 8a c4 39  
\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 unsetting PmkIdValidatedByAp  
\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Updating AAA Overrides from local for static  
\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Adding Audit session ID payload in Mobility  
\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 0 PMK-update groupcast messages sent  
\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 PMK sent to mobility group  
\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Disabling re-auth since PMK lifetime can ta  
\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Sending EAP-Success to mobile e4:b3:18:7c:30:  
\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 Freeing AACB from Dot1xCB as AAA auth is do  
\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 key Desc Version FT - 0  
\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 Found an cache entry for BSSID 00:c8:8b:26:  
\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.532: Including PMKID in M1 (16)  
\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.532: [0000] cc 3a 3d 26 80 17 8b f1 2d c5 cd fd a0 8a c4 39  
\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.532: M1 - Key Data: (22)  
\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.532: [0000] dd 14 00 0f ac 04 cc 3a 3d 26 80 17 8b f1 2d c5  
\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.532: [0016] cd fd a0 8a c4 39  
\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.532:

e4:b3:18:7c:30:58 Starting key exchange to mobile e4:b3:18:7c:30:58, data packets will be dropped

\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.532:

e4:b3:18:7c:30:58 Sending EAPOL-Key Message to mobile e4:b3:18:7c:30:58

state INITPMK (message 1), replay counter 00.00.00.00.00.00.00.00

\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 Reusing allocated memory for EAP Pkt for r  
\*Dot1x\_NW\_MsgTask\_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 Entering Backend Auth Success state (id=223)

```

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 Received Auth Success while in Authentication
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 dot1x - moving mobile e4:b3:18:7c:30:58 into
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.547: e4:b3:18:7c:30:58 Received EAPOL-Key from mobile e4:b3:18:7c:30:58
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.547: e4:b3:18:7c:30:58 Ignoring invalid EAPOL version (1) in EAPOL
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.547: e4:b3:18:7c:30:58 key Desc Version FT - 0
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.547:

e4:b3:18:7c:30:58 Received EAPOL-key in PTK_START state (message 2) from mobile

e4:b3:18:7c:30:58
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Successfully computed PTK from PMK!!!
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Received valid MIC in EAPOL Key Message M2!
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Not Flex client. Do not distribute PMK Key
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Stopping retransmission timer for mobile e4:b3:18:7c:30:58
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 key Desc Version FT - 0
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Sending EAPOL-Key Message to mobile e4:b3:18:7c:30:58
state PTKINITNEGOTIATING (message 3), replay counter 00.00.00.00.00.00.00.01
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Reusing allocated memory for EAP Pkt for retransmit
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Received EAPOL-Key from mobile e4:b3:18:7c:30:58
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Ignoring invalid EAPOL version (1) in EAPOL
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 key Desc Version FT - 0
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555:

e4:b3:18:7c:30:58 Received EAPOL-key in PTKINITNEGOTIATING state (message 4)

from mobile e4:b3:18:7c:30:58
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Stopping retransmission timer for mobile e4:b3:18:7c:30:58
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Freeing EAP Retransmit Buffer for mobile e4:b3:18:7c:30:58
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 apfMs1xStateInc
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 apfMsPeapSimReqCntInc
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 apfMsPeapSimReqSuccessCntInc
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555:

e4:b3:18:7c:30:58 0.0.0.0 8021X_REQD (3) Change state to L2AUTHCOMPLETE (4) last state 8021X_REQD (3)

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Mobility query, PEM State: L2AUTHCOMPLETE
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Building Mobile Announce :
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 Building Client Payload:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 Client IP: 0.0.0.0
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 Client Vlan IP: 172.16.0.134, Vlan mask: 0.0.0.255
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 Client Vap Security: 16384
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 Virtual IP: 10.10.10.10
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 ssid: ise-ssid
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 Building VlanIpPayload.
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 Not Using WMM Compliance code qosCap 00
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 L2AUTHCOMPLETE (4) Plumbed mobile L2
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556:

e4:b3:18:7c:30:58 0.0.0.0 L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7) last state L2AUTHCOMPLETE (4)

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) pemAdvanceState2 6677
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Adding Fast Path rule
  type = Airespace AP - Learn IP address
  on AP 00:c8:8b:26:2c:d0, slot 0, interface = 1, QoS = 0
  IPv4 ACL ID = 255, IPv6
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Fast Path rule (contd)
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Fast Path rule (contd)
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Successfully plumbed
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 Successfully Plumbed PTK session Keysfor mobile
*spamApTask2: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 Successful transmission of LWAPP Add-Mobile to AP
*pemReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 Added NPU entry of type 9, dtlFlags 0x00000000
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) mobility role update request
  Peer = 0.0.0.0, Old Anchor = 0.0.0.0, New Anchor = 172.16.0.3
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) State Update from Mobility

```

```

*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) pemAdvanceState2 6315, Ad
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Replacing Fast Path rule
    IPv4 ACL ID = 255,
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Fast Path rule (contd...)
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Fast Path rule (contd...)
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Successfully plumbed mobi
*pemReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 Sent an XID frame
*dtlArpTask: Nov 24 04:30:47.932: e4:b3:18:7c:30:58 Static IP client associated to interface wlan2404 w
*dtlArpTask: Nov 24 04:30:47.933: e4:b3:18:7c:30:58 apfMsRunStateInc
*dtlArpTask: Nov 24 04:30:47.933:

e4:b3:18:7c:30:58 172.16.0.151 DHCP_REQD (7) Change state to RUN (20)

last state DHCP_REQD (7)

```

디버그 클라이언트 출력을 쉽게 읽을 수 있는 방법은 무선 디버그 분석기 도구를 사용합니다.

### [Wireless Debug Analyzer](#)

### ISE의 인증 프로세스

사용자에게 할당된 인증 정책, 권한 부여 정책 및 권한 부여 프로파일을 확인하기 위해 Operations(운영) > RADIUS > Live Logs(라이브 로그)로 이동합니다.

자세한 내용을 보려면 Details를 클릭하여 그림과 같이 보다 자세한 인증 프로세스를 확인합니다.

Time	Sta...	Details	Endp...	Endpoint ...	Authentication Policy	Authorization Policy	Authorization Profiles	
No...	1		user1	08:47:02:77:13:45	Apple-Device	Default >> Rule name >> Default	Default >> NameAuthZrule	PermitAccessVLAN2404

### 문제 해결

현재 이 구성의 문제를 해결하는 데 사용할 수 있는 특정 정보가 없습니다.

## 이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서([링크 제공됨](#))를 참조할 것을 권장합니다.