

ISE 내부 CA를 사용하여 9800 WLC에서 EAP-TLS 구성

목차

[소개](#)

[사전 요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[EAP-TLS 인증 흐름](#)

[EAP-TLS 흐름의 단계](#)

[구성](#)

[네트워크 다이어그램](#)

[설정](#)

[ISE 구성](#)

[네트워크 디바이스 추가](#)

[내부 CA 확인](#)

[인증 방법 추가](#)

[인증서 템플릿 지정](#)

[인증서 포털 생성](#)

[내부 사용자 추가](#)

[ISE 인증서 프로비저닝 포털 및 RADIUS 정책 구성](#)

[9800 WLC 컨피그레이션](#)

[9800 WLC에 ISE 서버 추가](#)

[9800 WLC에 서버 그룹 추가](#)

[9800 WLC에서 AAA 방법 목록 구성](#)

[9800 WLC에서 Authorization Method\(권한 부여 방법\) 목록 구성](#)

[9800 WLC에서 정책 프로파일 생성](#)

[9800 WLC에서 WLAN 생성](#)

[9800 WLC에서 정책 프로파일을 사용하여 WLAN 매핑](#)

[9800 WLC의 액세스 포인트에 정책 태그 매핑](#)

[설정 완료 후 WLC 구성 실행](#)

[사용자에 대한 인증서 생성 및 다운로드](#)

[Windows 10 시스템에 인증서 설치](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[참조](#)

소개

이 문서에서는 ISE(Identity Services Engine)의 인증 기관을 사용하여 사용자를 인증하는 EAP-TLS

인증에 대해 설명합니다.

사전 요구 사항

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 무선 컨트롤러: 17.09.04a를 실행하는 C9800-40-K9
- Cisco ISE: 버전 3 패치 4 실행
- AP 모델: C9130AXI-D
- 스위치: 9200-L-24P

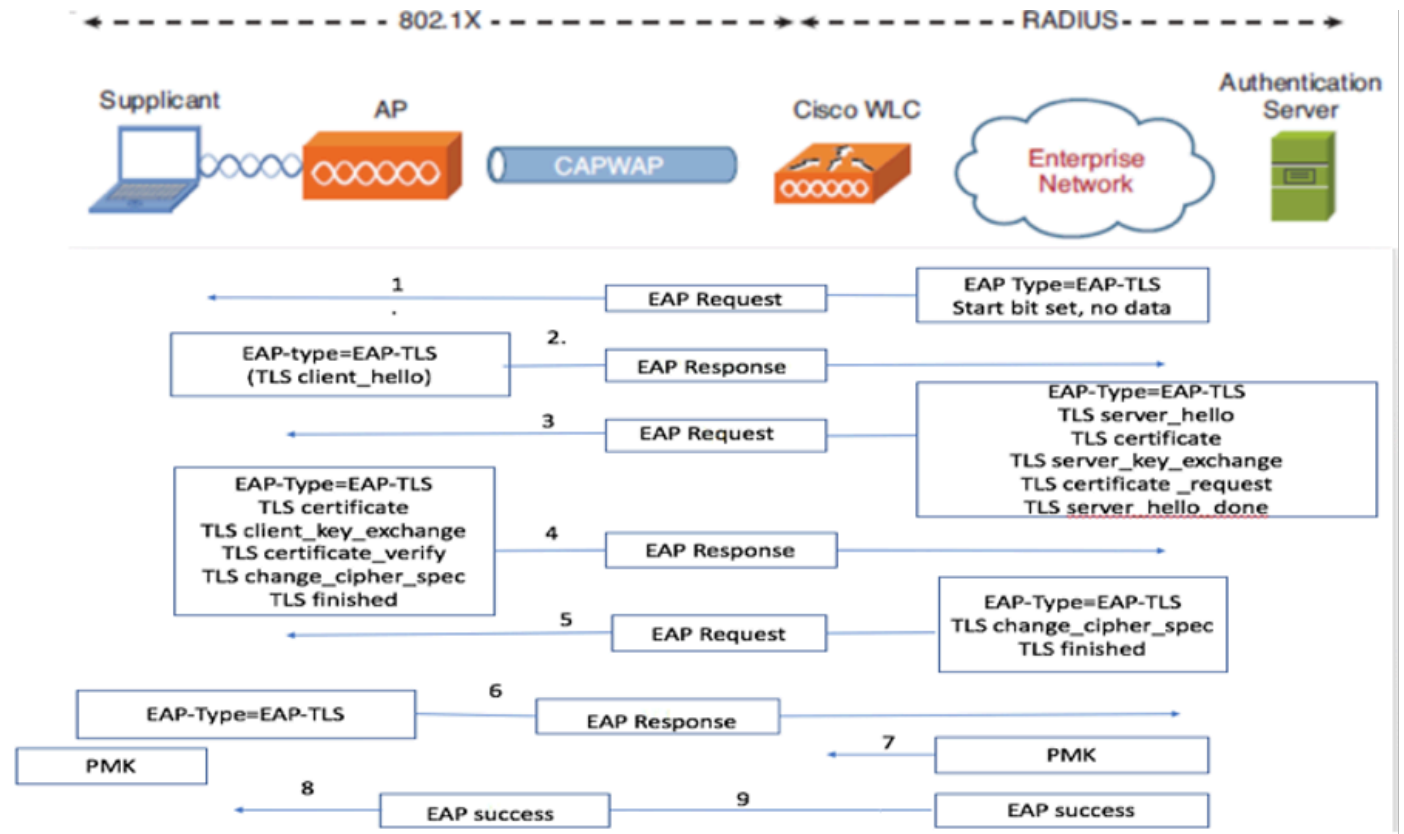
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

대부분의 조직에는 EAP-TLS 인증을 위해 최종 사용자에게 인증서를 발급하는 자체 CA가 있습니다. ISE에는 EAP-TLS 인증에 사용할 사용자에 대한 인증서를 생성하는 데 사용할 수 있는 내장형 인증 기관이 포함되어 있습니다. 본격적인 CA를 사용할 수 없는 시나리오에서는 사용자 인증을 위해 ISE CA를 사용하는 것이 유리합니다.

이 문서에서는 ISE CA를 효과적으로 사용하여 무선 사용자를 인증하는 데 필요한 컨피그레이션 단계를 간략하게 설명합니다. EAP-TLS 인증 흐름

EAP-TLS 인증 흐름



EAP-TLS 인증 흐름

EAP-TLS 흐름의 단계

1. 무선 클라이언트가 액세스 포인트(AP)와 연결됩니다.
2. 이 단계에서 AP는 데이터 전송을 허용하지 않고 인증 요청을 전송한다.
3. 서플리컨트 역할을 하는 클라이언트는 EAP 응답 ID로 응답 합니다.
4. WLC(Wireless LAN Controller)는 사용자 ID 정보를 인증 서버에 전달합니다.
5. RADIUS 서버는 EAP-TLS 시작 패킷으로 클라이언트에 응답합니다.
6. 이 시점부터 EAP-TLS 대화가 시작됩니다.
7. 클라이언트는 암호가 NULL로 설정된 client_hello 핸드셰이크 메시지를 포함하여 EAP-응답을 인증 서버로 다시 전송합니다.
8. 인증 서버는 다음을 포함하는 Access-Challenge 패킷으로 응답합니다.

TLS server_hello
Handshake message
Certificate
Server_key_exchange
Certificate request
Server_hello_done

9. 클라이언트가 다음을 포함하는 EAP 응답 메시지로 응답합니다.

Certificate (for server validation)
Client_key_exchange

Certificate_verify (to verify server trust)
Change_cipher_spec
TLS finished

10. 클라이언트 인증에 성공하면 RADIUS 서버는 다음을 포함하는 액세스 챌린지를 보냅니다.

Change_cipher_spec
Handshake finished message

11. 클라이언트가 RADIUS 서버를 인증하기 위해 해시를 확인합니다.

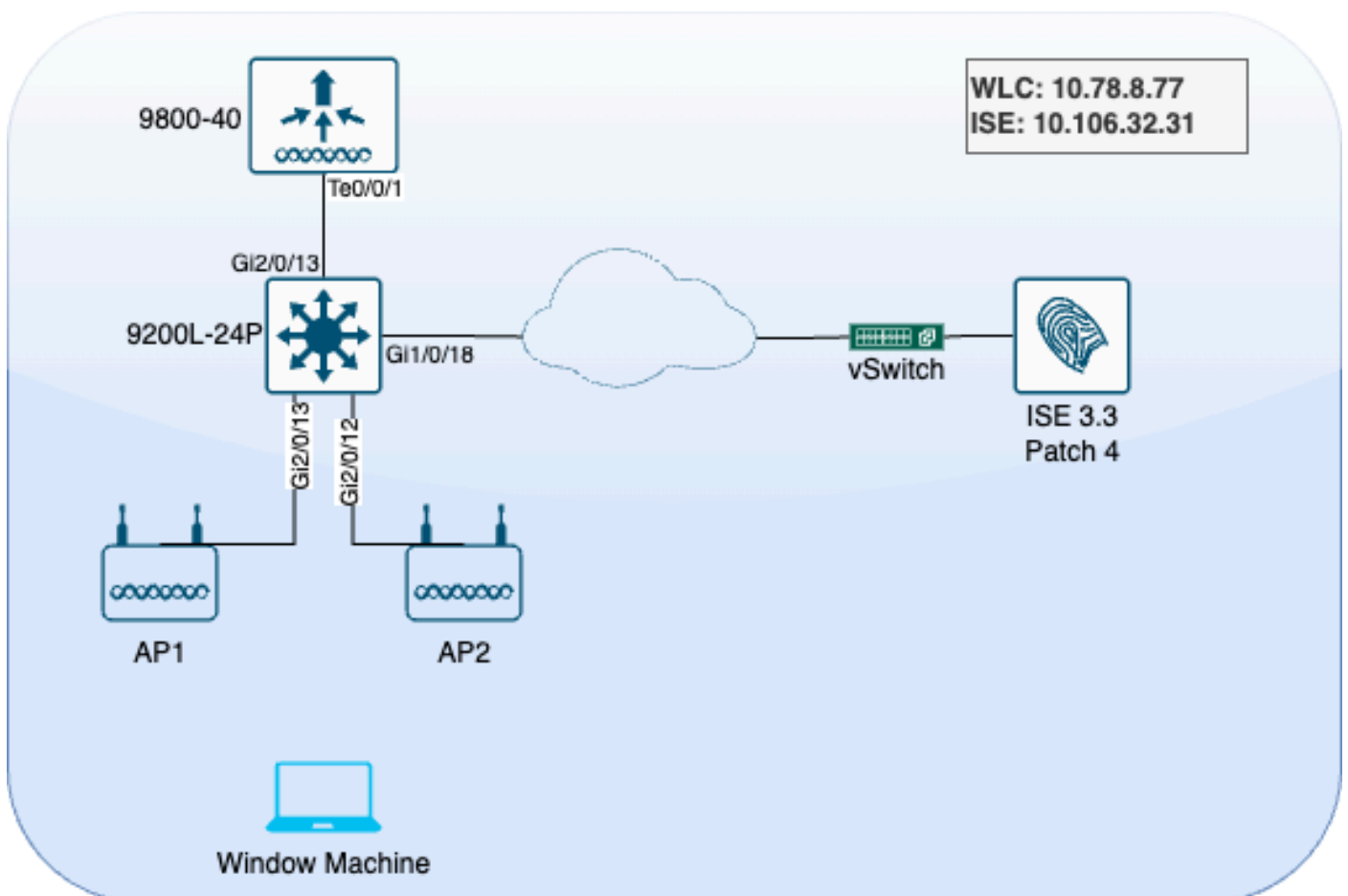
12. 새 암호화 키는 TLS 핸드셰이크 중 비밀에서 동적으로 파생됩니다.

13. EAP 성공 메시지가 서버에서 인증자에게 전송된 다음 신청자에게 전송됩니다.

14. 이제 EAP-TLS가 활성화된 무선 클라이언트가 무선 네트워크에 액세스할 수 있습니다.

구성

네트워크 다이어그램

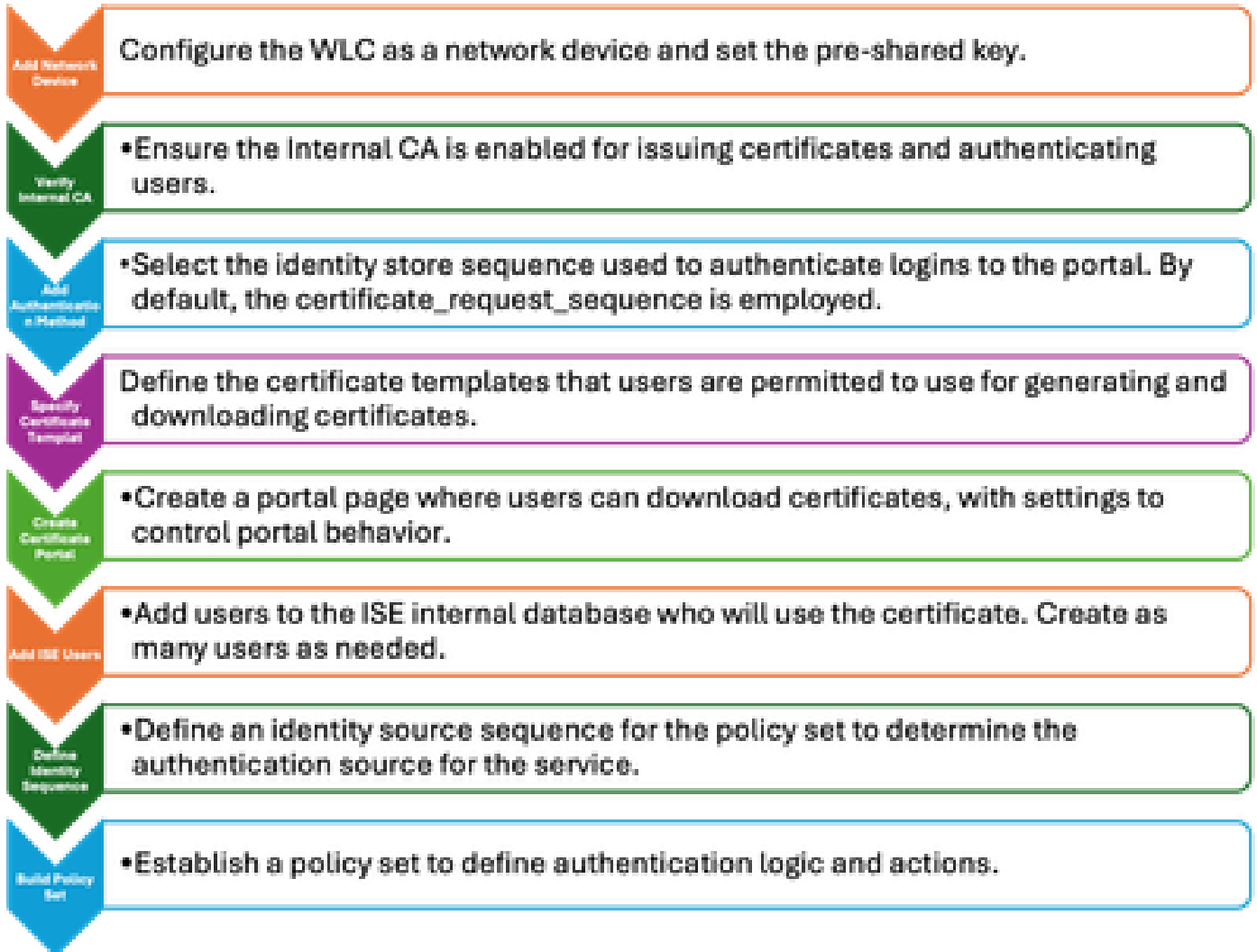


설정

이 섹션에서는 두 가지 구성 요소를 구성합니다. ISE 및 9800 WLC.

ISE 구성

다음은 ISE 서버의 구성 단계입니다. 각 단계에는 시각적 지침을 제공하기 위한 스크린샷이 함께 제공됩니다.

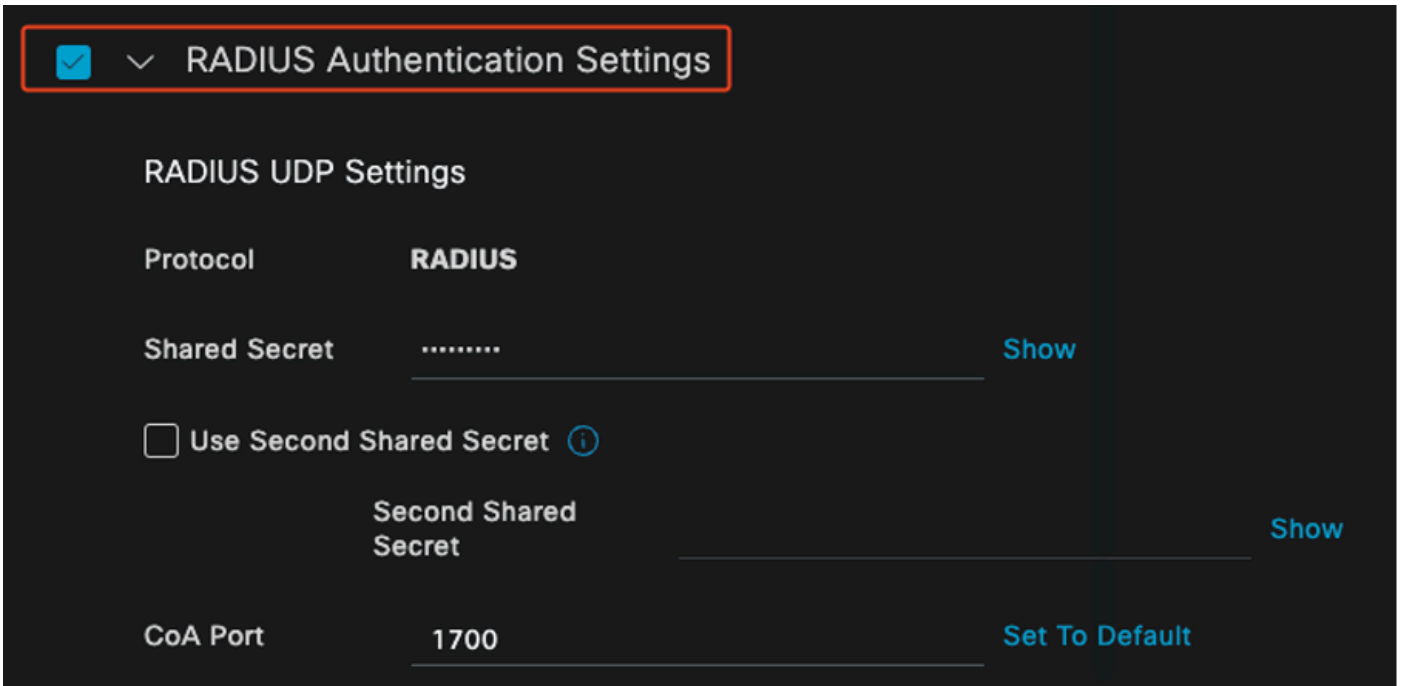


ISE 서버 컨피그레이션 단계

네트워크 디바이스 추가

WLC(Wireless LAN Controller)를 네트워크 디바이스로 추가하려면 다음 지침을 따르십시오.

1. Administration(관리) > Network Resources(네트워크 리소스) > Network Devices(네트워크 디바이스)로 이동합니다.
2. WLC 추가 프로세스를 시작하려면+Add 아이콘을 클릭합니다.
3. 사전 공유 키가 WLC 및 ISE 서버와 일치하는지 확인하여 적절한 통신을 활성화합니다.
4. 모든 세부 정보를 올바르게 입력했으면 왼쪽 하단 모서리에서 Submit(제출)을 클릭하여 컨피그레이션을 저장합니다

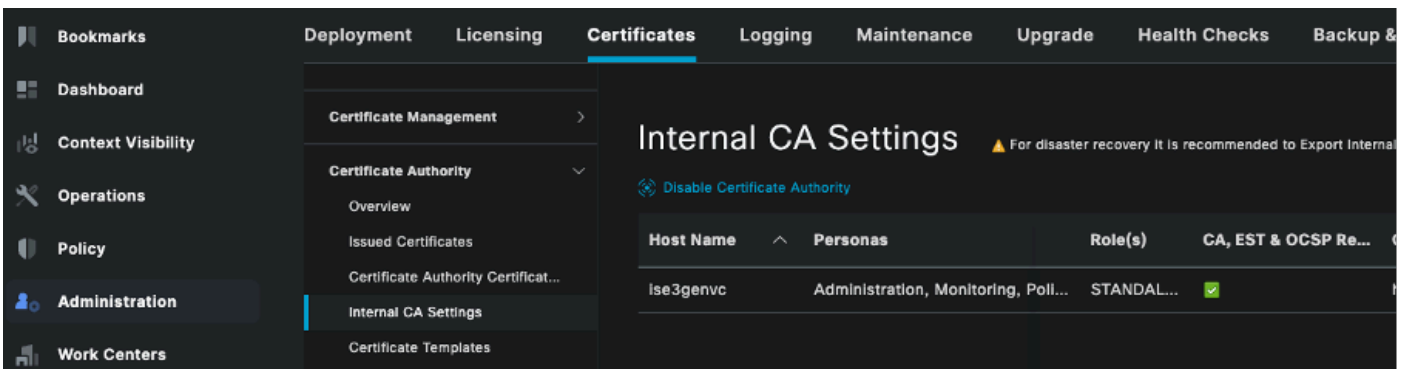


네트워크 디바이스 추가

내부 CA 확인

내부 CA(Certificate Authority) 설정을 확인하려면 다음 단계를 수행하십시오.

1. Administration(관리) > System(시스템) > Certificates(인증서) > Certificate Authority(인증 기관) > Internal CA Settings(내부 CA 설정)로 이동합니다.
2. CA 열이 활성화되어 내부 CA가 활성화되었는지 확인합니다.



내부 CA 확인

인증 방법 추가

Administration(관리) > Identity Management(ID 관리) > Identity Source Sequences(ID 소스 시퀀스)로 이동합니다. 포털 로그인 소스를 제어하려면 사용자 지정 ID 시퀀스를 추가합니다.

Identities Groups External Identity Sources **Identity Source Sequences** Settings

Identity Source Sequences List > Allow_EMP_Cert

Identity Source Sequence

Identity Source Sequence

* Name

Description

Certificate Based Authentication

Select Certificate Authentication Profile

Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available	Selected
Internal Endpoints	<input checked="" type="checkbox"/> Internal Users
Guest Users	<input type="checkbox"/>
All_AD_Join_Points	<input type="checkbox"/>

인증 방법

인증서 템플릿 지정

인증서 템플릿을 지정하려면 다음 단계를 수행합니다.

1단계. Administration(관리) > System(시스템) > Certificates(인증서) > Certificate Authority(인증 기관) > Certificate Templates(인증서 템플릿)로 이동합니다.

2단계. 새 인증서 템플릿을 생성하려면 +Add 아이콘을 클릭합니다.

2.1 템플릿에 대해 ISE 서버에 로컬인 고유한 이름을 제공합니다.

2.2 CN(Common Name)이 \$UserName\$로 설정되어 있는지 확인합니다.

2.3 SAN(주체 대체 이름)이 MAC 주소에 매핑되었는지 확인합니다.

2.4 SCEP RA 프로필을 ISE 내부 CA로 설정합니다.

2.5 extended key usage(확장 키 사용) 섹션에서 클라이언트 인증을 활성화합니다.

Field	Value
* Name	EAP_Authentication_Certificate_Template
Description	This template will be used to issue certificates for EAP Authentication
Subject	\$UserName\$
Common Name (CN)	\$UserName\$
Organizational Unit (OU)	Example unit
Organization (O)	Company name
City (L)	City
State (ST)	State
Country (C)	US
Subject Alternative Name (SAN)	MAC Address
Key Type	RSA
Key Size	2048
* SCEP RA Profile	ISE Internal CA
Valid Period	730 Day(s) (Valid Range 1 - 3652)
Extended Key Usage	<input checked="" type="checkbox"/> Client Authentication <input type="checkbox"/> Server Authentication

인증서 템플릿

인증서 포털 생성

클라이언트 인증서 생성을 위한 인증서 포털을 생성하려면 다음 단계를 수행합니다.

1단계. Administration(관리) > Device Portal Management(디바이스 포털 관리) > Certificate Provisioning(인증서 프로비저닝)으로 이동합니다.

2단계. Create(생성)를 클릭하여 새 포털 페이지를 설정합니다.

3단계. 포털을 쉽게 식별할 수 있도록 포털의 고유한 이름을 제공합니다.

3.1. 포털에 대한 포트 번호를 선택합니다. 8443으로 설정합니다.

3.2. ISE가 이 포털을 수신 대기할 인터페이스를 지정합니다.

3.3. 인증서 그룹 태그를 기본 포털 인증서 그룹으로 선택합니다.

3.4. 이 포털에 대한 로그인을 인증하는 데 사용되는 ID 저장소 시퀀스를 나타내는 인증 방법을 선택합니다.

3.5. 구성원이 포털에 액세스할 수 있는 권한 있는 그룹을 포함합니다. 예를 들어, 사용자가 이 그룹에 속하는 경우 Employee 사용자 그룹을 선택합니다.

3.6. 인증서 프로비저닝 설정에서 허용되는 인증서 템플릿을 정의합니다.

The screenshot displays the Cisco ISE Administration console interface. The top navigation bar includes 'Blocked List', 'BYOD', 'Certificate Provisioning' (highlighted), and 'Client Provisioning'. The left sidebar contains navigation options: 'Bookmarks', 'Dashboard', 'Context Visibility', 'Operations', 'Policy', 'Administration' (selected), 'Work Centers', and 'Interactive Features'. The main content area is titled 'Portals Settings and Customization'. It features a form for configuring a portal with the following fields:

- Portal Name:** EMP CERTIFICATE PORTAL
- Description:** (empty)
- Language File:** (dropdown menu)
- Portal test URL:** (text field)

At the bottom of the main content area, there are two sub-sections: 'Portal Behavior and Flow Settings' (highlighted) and 'Portal Page Customization'.

Portal & Page Settings

Portal Settings

HTTPS port:*

1

8443

(8000 - 8999)

Allowed Interfaces:*

2

For PSNs Using Physical Interfaces

- Gigabit Ethernet 0
- Gigabit Ethernet 1
- Gigabit Ethernet 2
- Gigabit Ethernet 3
- Gigabit Ethernet 4
- Gigabit Ethernet 5

For PSNs with Bonded Interfaces Configured

- Bond 0
Uses Gigabit Ethernet 0 as primary interface, Gigabit Ethernet 1 as backup
- Bond 1
Uses Gigabit Ethernet 2 as primary interface, Gigabit Ethernet 3 as backup
- Bond 2
Uses Gigabit Ethernet 4 as primary interface, Gigabit Ethernet 5 as backup

Certificate group tag: *

3

Default Portal Certificate Group

Configure certificates at:

[Administration > System > Certificates > System Certificates](#)

Authentication method: *

4

Certificate_Request_Sequence

Configure authentication methods at:

[Administration > Identity Management > Identity Source Sequences](#)

Configure authorized groups

User account with Super admin privilege or ERS admin privilege will have access to the portal

Available

Q

- ALL_ACCOUNTS (default)
- GROUP_ACCOUNTS (default)
- OWN_ACCOUNTS (default)

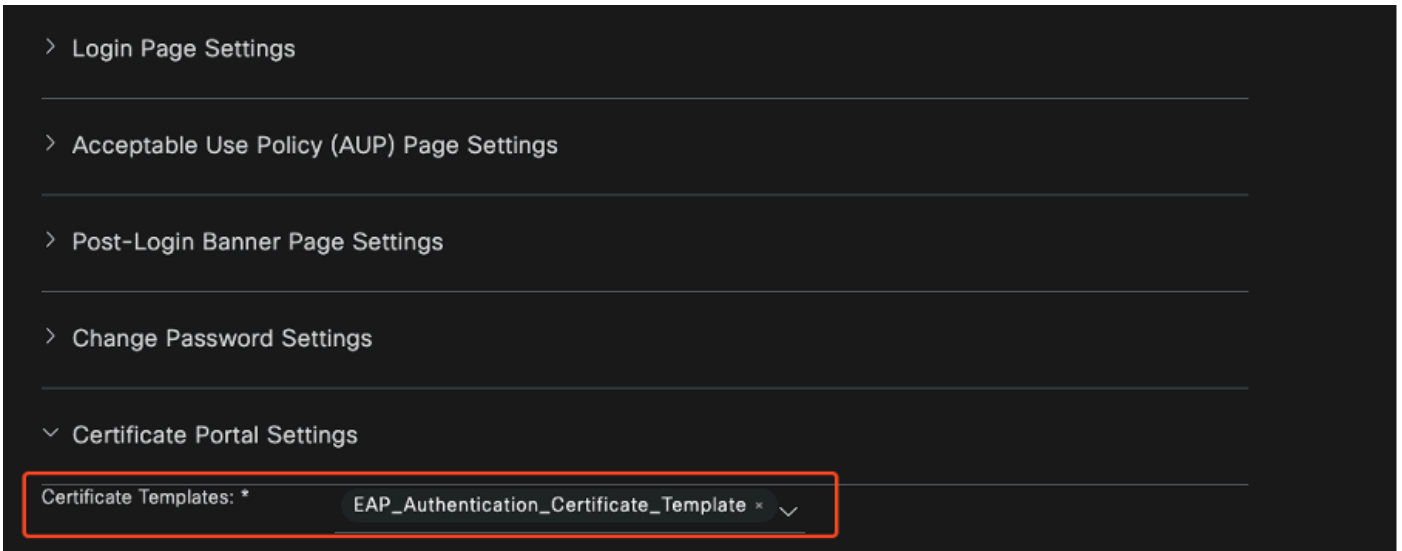
Chosen

Employee

Choose all

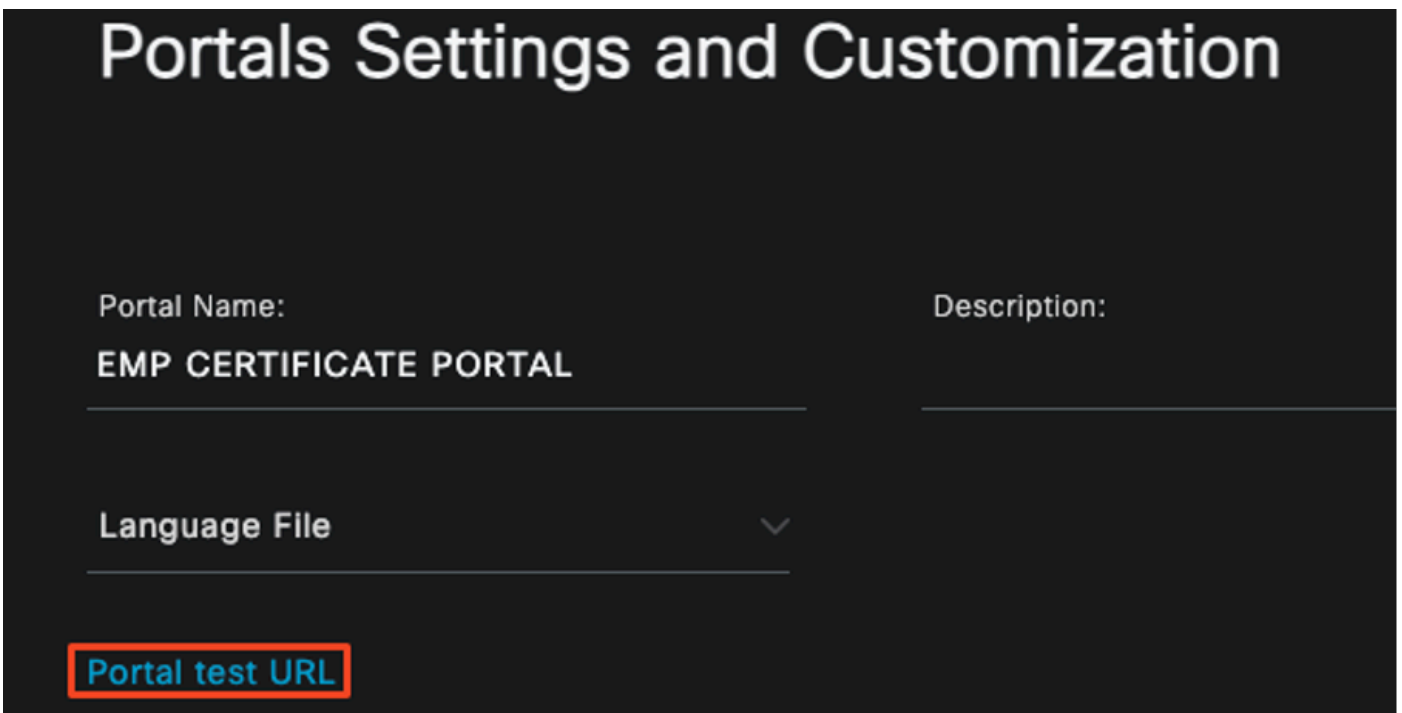
Clear all

Fully qualified domain name (FQDN):

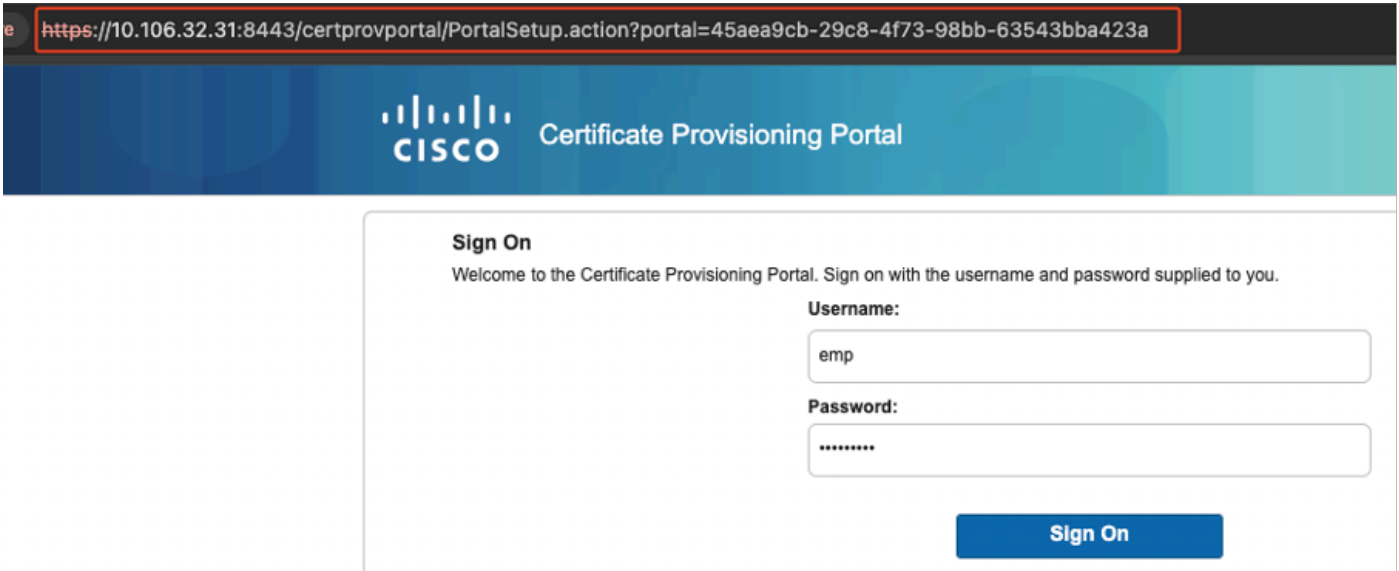


인증서 포털 컨피그레이션

이 설정이 완료되면 Portal Test URL(포털 테스트 URL)을 클릭하여 포털을 테스트할 수 있습니다. 이 작업을 수행하면 포털 페이지가 열립니다.



테스트 포털 페이지 URL

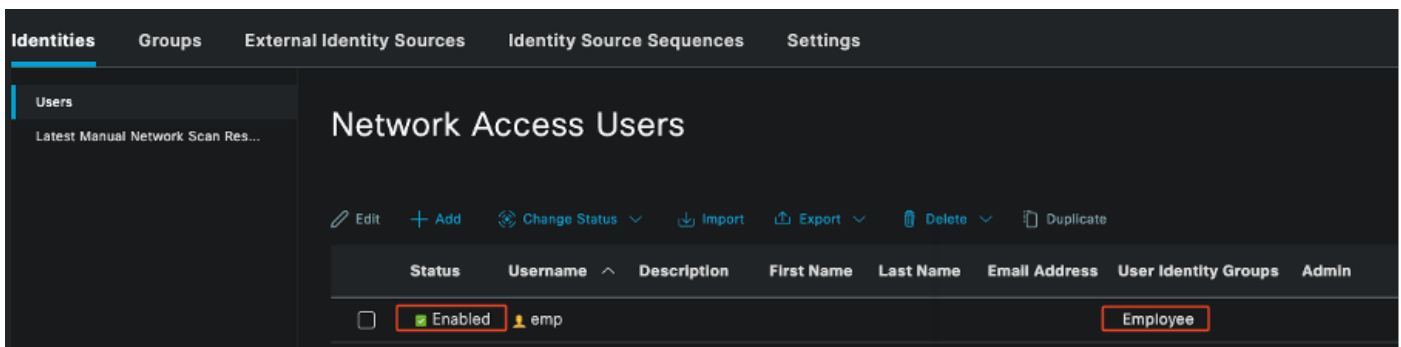


포털 페이지

내부 사용자 추가

인증서 포털을 통해 인증할 사용자를 생성하려면 다음 단계를 수행합니다.

1. Administration(관리) > Identity Management(ID 관리) > Identities(ID) > Users(사용자)로 이동합니다.
2. 시스템에 사용자를 추가하려면 옵션을 클릭합니다.
3. 사용자가 속한 사용자 ID 그룹을 선택합니다. 이 예에서는 사용자를 Employee 그룹에 할당합니다.



내부 사용자 추가

ISE 인증서 프로비저닝 포털 및 RADIUS 정책 구성

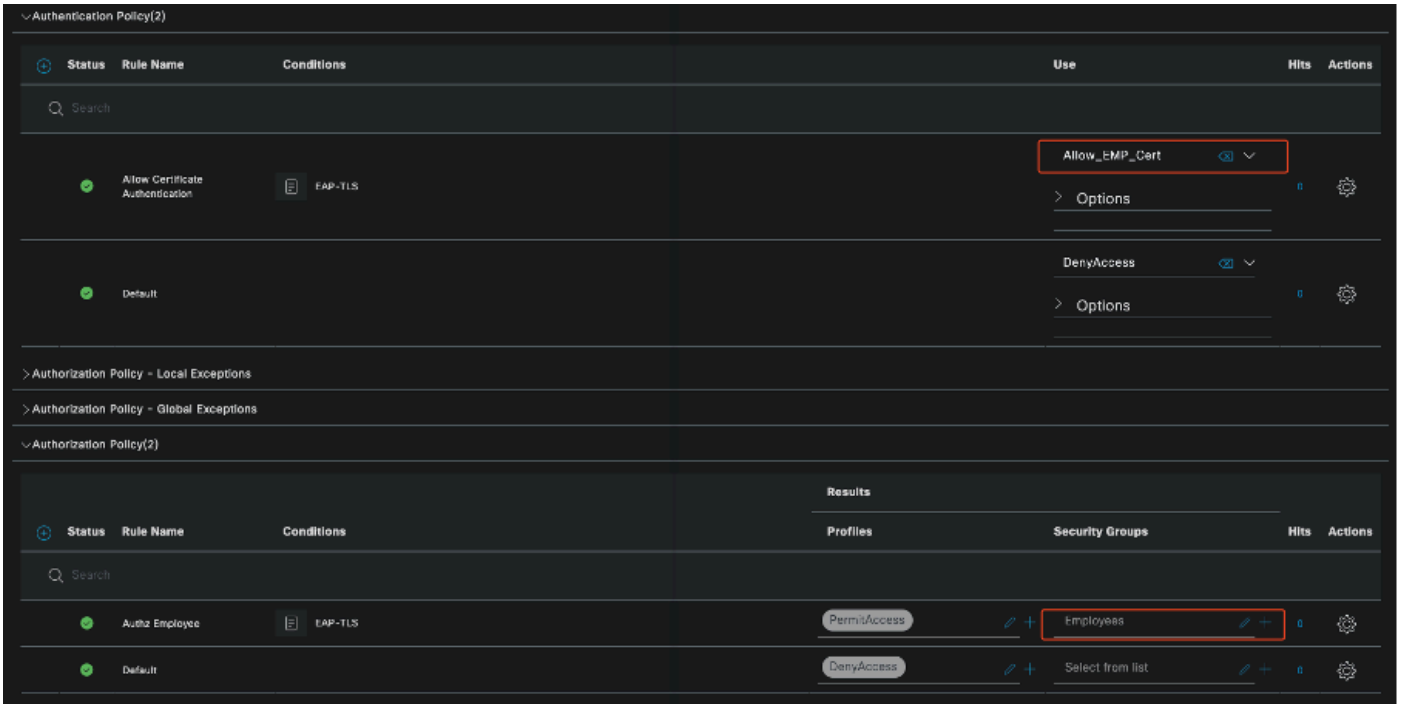
이전 섹션에서는 ISE 인증서 프로비저닝 포털의 설정에 대해 다뤘습니다. 이제 사용자 인증을 허용하도록 ISE RADIUS 정책 집합을 구성합니다.

1. ISE RADIUS 정책 집합 구성
2. Policy(정책) > Policy Sets(정책 집합)로 이동합니다.
3. 새 정책 집합을 생성하려면 더하기 기호(+)를 클릭합니다.

이 예에서는 인증서를 사용하여 사용자를 인증하도록 설계된 간단한 정책 집합을 설정합니다.



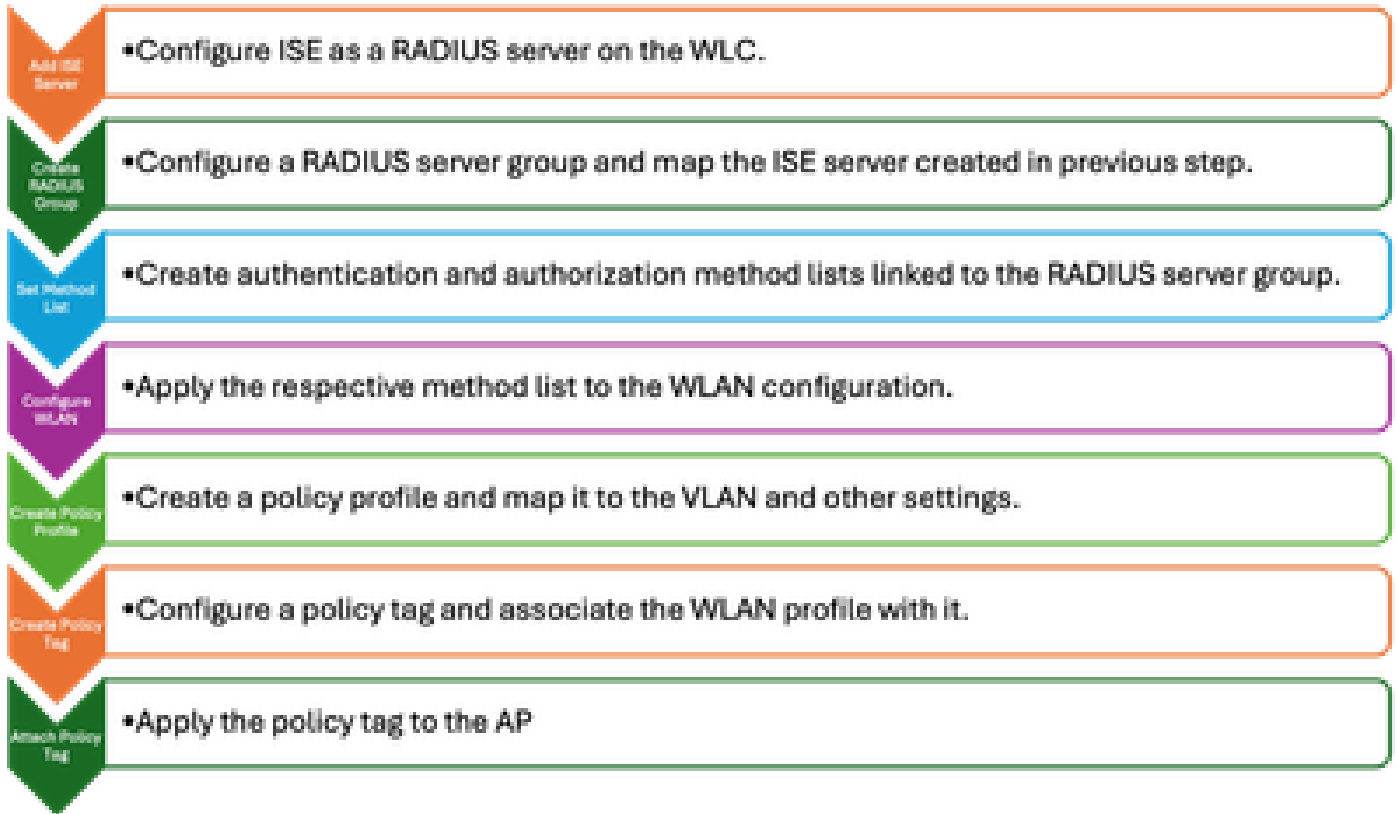
정책 설정



인증 및 권한 부여 정책을 표시하는 정책 집합

9800 WLC 컨피그레이션

9800 WLC의 컨피그레이션 단계는 다음과 같습니다. 각 단계는 이 섹션의 스크린샷과 함께 시각적 안내를 제공합니다.



WLC 컨피그레이션 단계

9800 WLC에 ISE 서버 추가

1. ISE 서버를 9800 WLC(Wireless LAN Controller)와 통합하려면 다음 단계를 수행하십시오.
2. Configuration(컨피그레이션) > Security(보안) > AAA로 이동합니다.
3. Add(추가) 버튼을 클릭하여 WLC 컨피그레이션에 ISE 서버를 포함합니다.

Configuration > Security > AAA Show Me How

+ AAA Wizard

Servers / Groups AAA Method List AAA Advanced

+ Add Delete

RADIUS

TACACS+

LDAP

Create AAA Radius Server

Name* ISE3

Server Address* 10.106.32.31

PAC Key

Key Type Clear Text

Key*

Confirm Key*

Auth Port 1812

Acct Port 1813

Server Timeout (seconds) 1-1000

Retry Count 0-100

Support for CoA ENABLED

CoA Server Key Type Clear Text

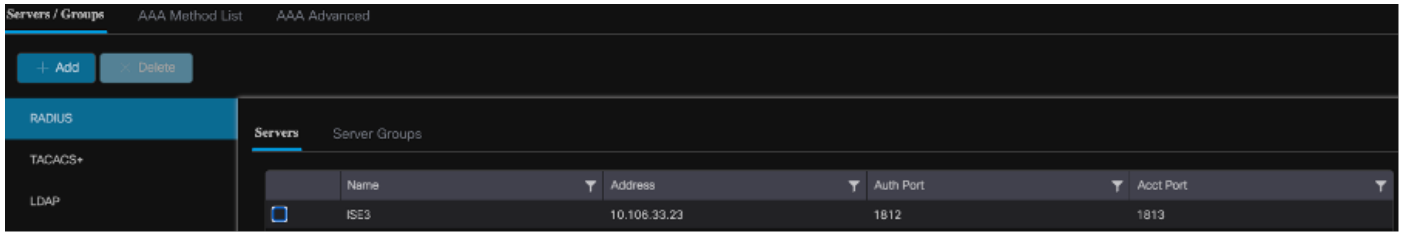
CoA Server Key

Confirm CoA Server Key

Automate Tester

WLC에 ISE 서버 추가

서버가 추가되면 서버 목록에 나타납니다.

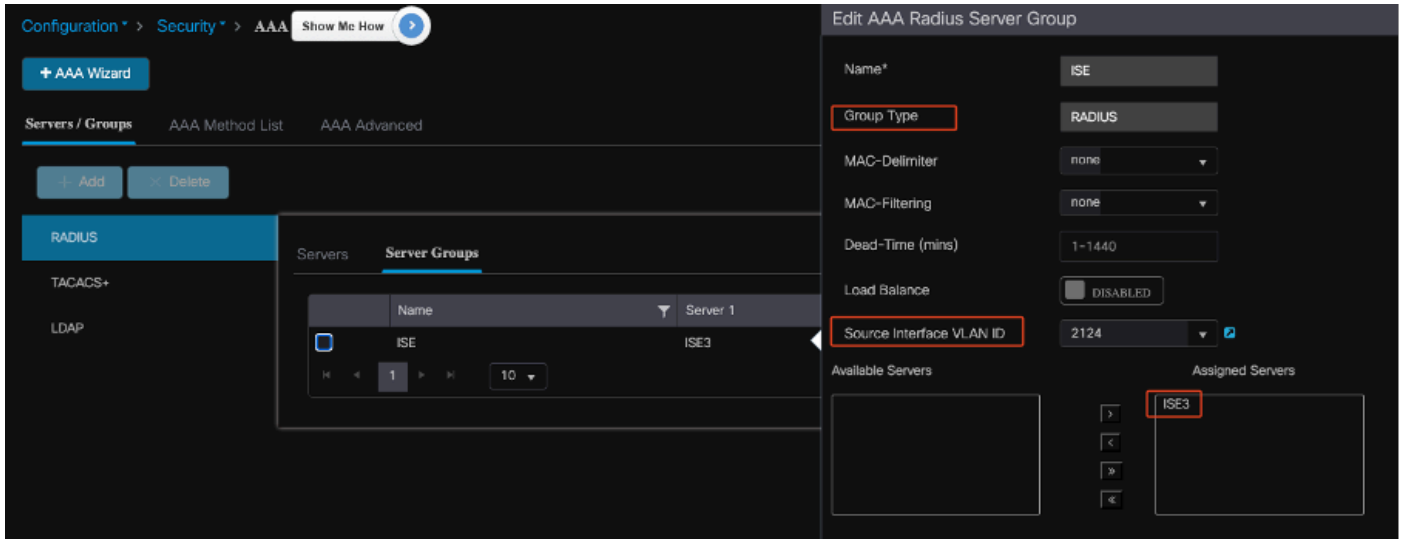


Radius 서버 표시

9800 WLC에 서버 그룹 추가

9800 Wireless LAN Controller에서 서버 그룹을 추가하는 절차는 다음과 같습니다.

1. Configuration(컨피그레이션) > Security(보안) > AAA로 이동합니다.
2. Server Group(서버 그룹) 탭을 클릭한 다음 Add(추가)를 클릭하여 새 서버 그룹을 만듭니다.

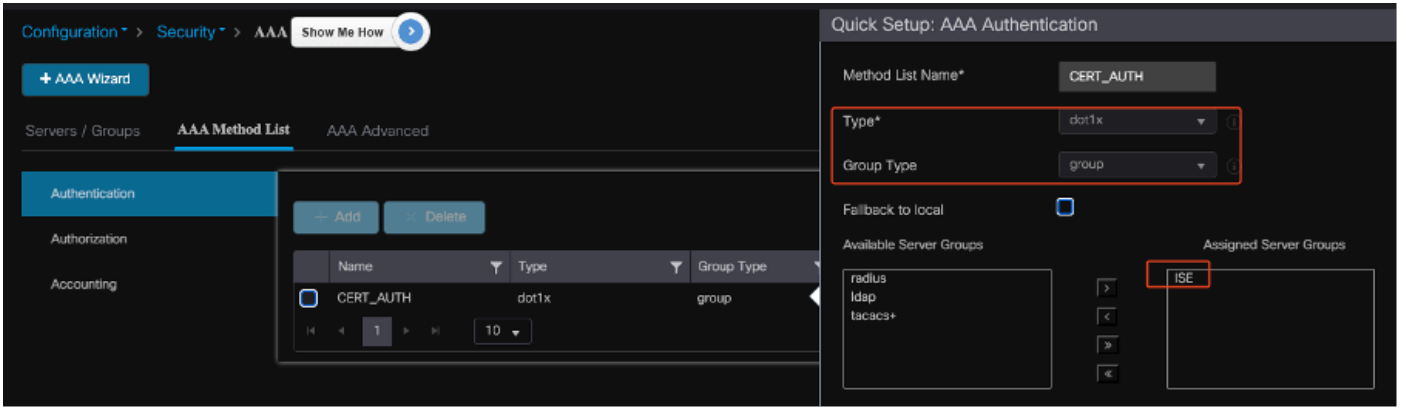


ISE 서버를 Radius 서버 그룹에 매핑

9800 WLC에서 AAA 방법 목록 구성

서버 그룹을 생성한 후 다음 단계를 사용하여 인증 방법 목록을 구성합니다.

1. Configuration(컨피그레이션) > Security(보안) > AAA > AAA Method List(AAA 메서드 목록)로 이동합니다.
2. Authentication(인증) 탭에서 새 인증 방법 목록을 추가합니다.
3. 유형을 dot1x로 설정합니다.
4. 그룹 유형으로 그룹을 선택합니다.
5. 이전에 서버 그룹으로 생성한 ISE 서버 그룹을 포함합니다.

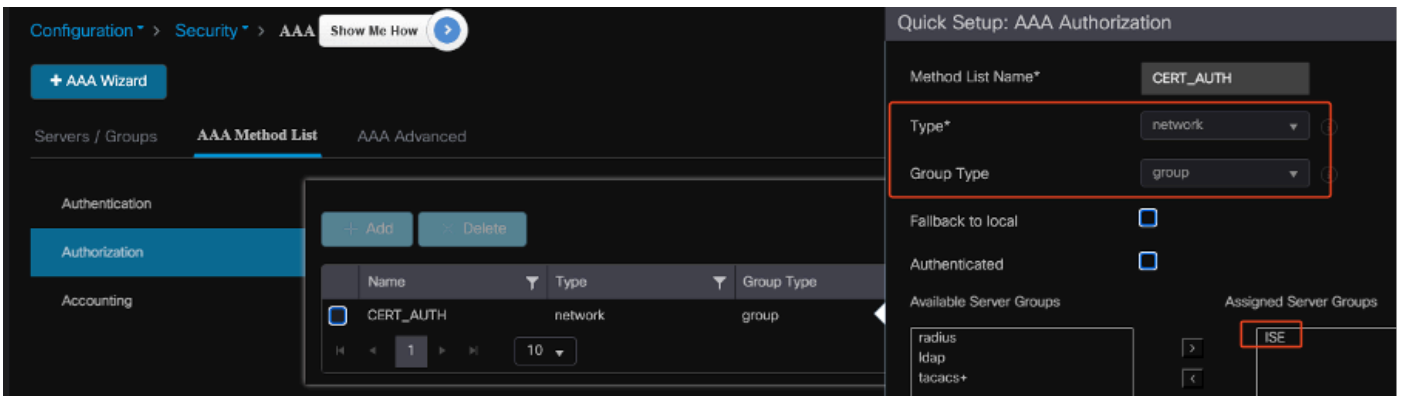


인증 방법 목록 생성

9800 WLC에서 Authorization Method(권한 부여 방법) 목록 구성

권한 부여 방법 목록을 설정하려면 다음 단계를 수행합니다.

1. AAA Method List(AAA 메서드 목록) 섹션 내의 Authorization(권한 부여) 탭으로 이동합니다.
2. Add(추가)를 클릭하여 새 권한 부여 방법 목록을 만듭니다.
3. 유형으로 network를 선택합니다.
4. 그룹 유형으로 그룹을 선택합니다.
5. ISE 서버 그룹을 서버 그룹으로 포함합니다.

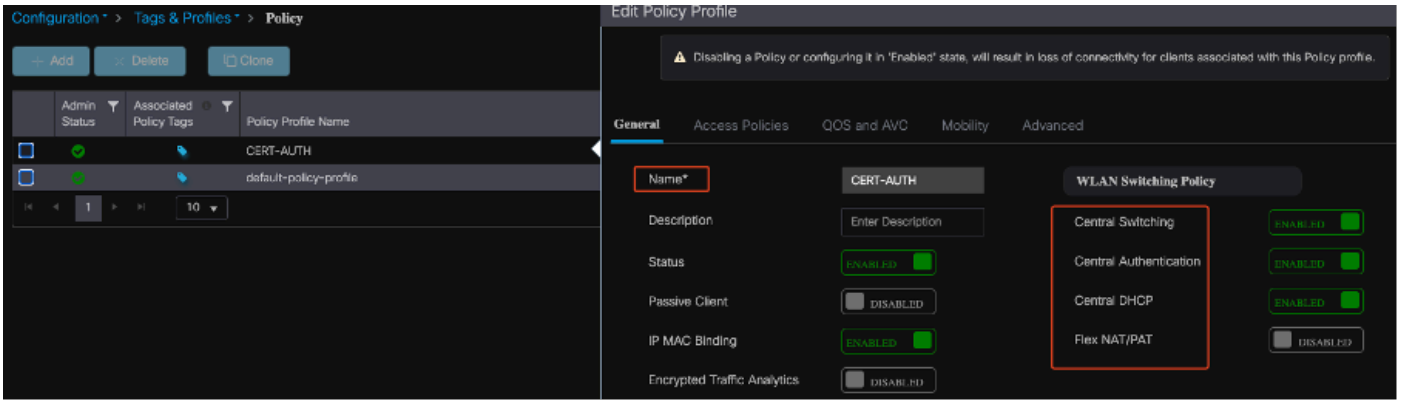


인증 방법 목록 추가

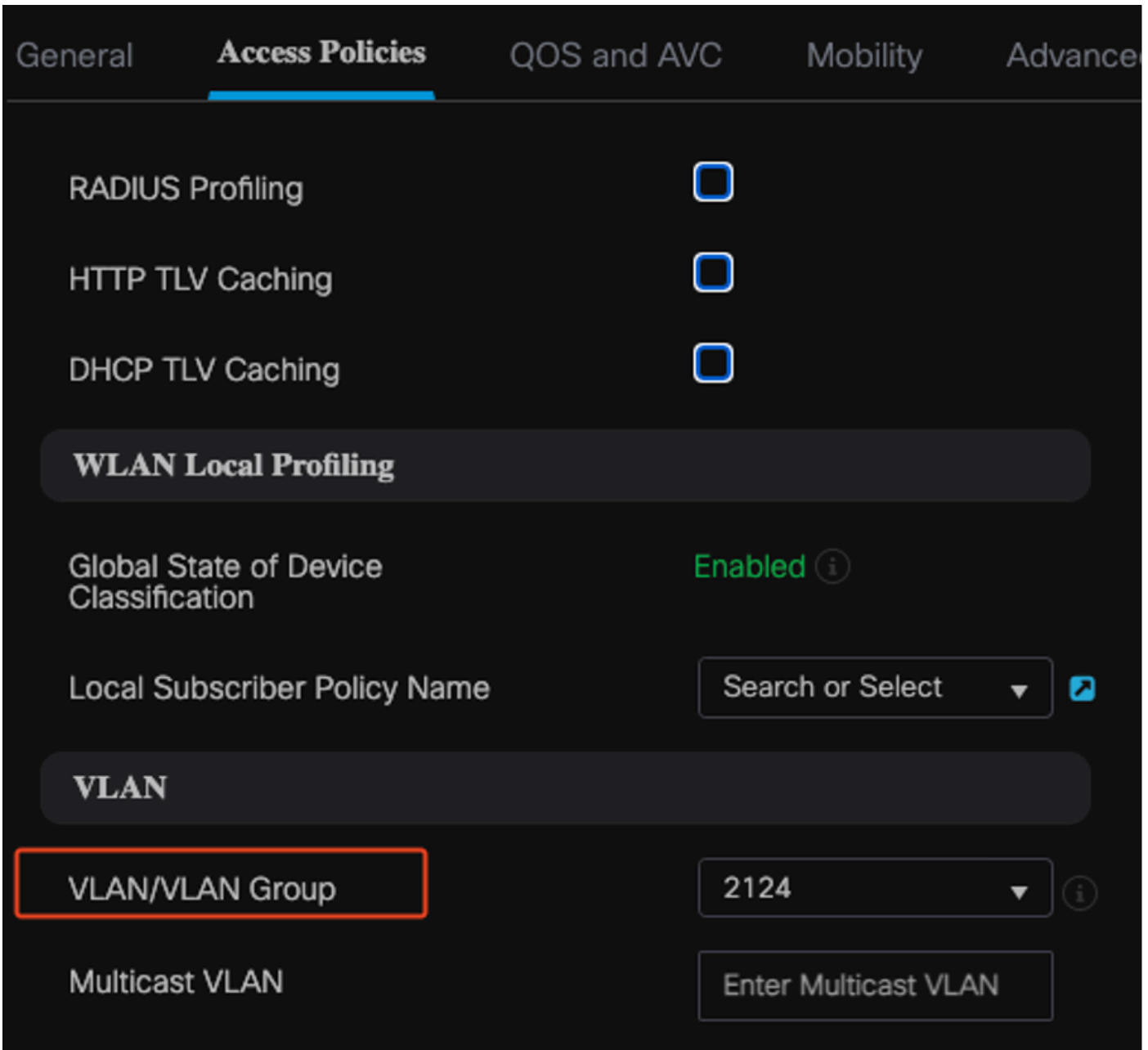
9800 WLC에서 정책 프로파일 생성

RADIUS 그룹 컨피그레이션이 완료되면 정책 프로필을 생성합니다.

1. Configuration > Tags & Profiles > Policy로 이동합니다.
2. Add(추가)를 클릭하여 새 정책 프로필을 생성합니다.
3. 정책 프로필에 대한 적절한 매개변수를 선택합니다. 이 예에서는 모든 것이 중앙이며 LAB VLAN이 클라이언트 VLAN으로 사용됩니다.



정책 프로필 구성



VLAN과 정책 간의 매핑

RADIUS 권한 부여를 구성할 때 정책 프로파일 설정의 고급 탭에서 AAA Override 옵션이 활성화되어 있는지 확인합니다. 이 설정을 사용하면 Wireless LAN Controller가 RADIUS 기반 권한 부여 정

책을 사용자 및 디바이스에 적용할 수 있습니다.

General Access Policies QOS and AVC Mobility **Advanced**

WLAN Timeout

Session Timeout (sec) 1800 ⓘ

Idle Timeout (sec) 300

Idle Threshold (bytes) 0

Client Exclusion Timeout (sec) 60

Guest LAN Session Timeout

DHCP

IPv4 DHCP Required

DHCP Server IP Address

Show more >>>

AAA Policy

Allow AAA Override

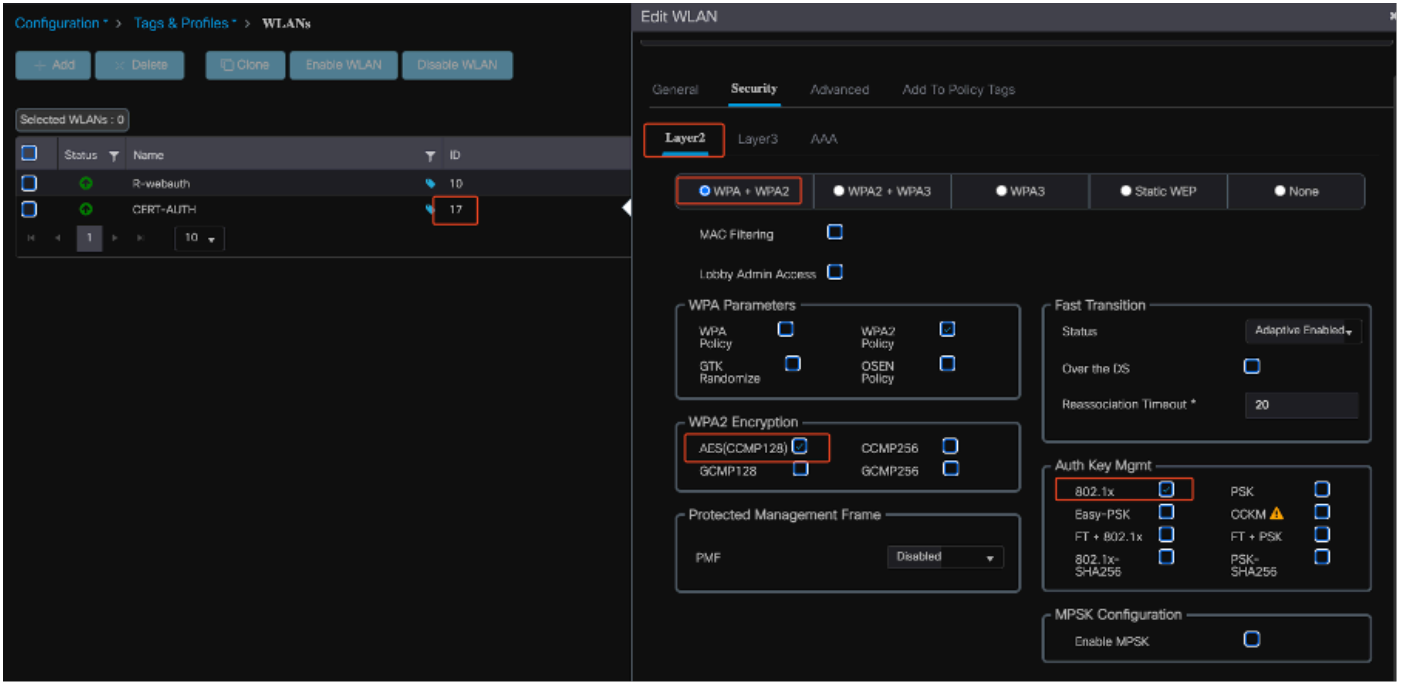
AAA 재정의

9800 WLC에서 WLAN 생성

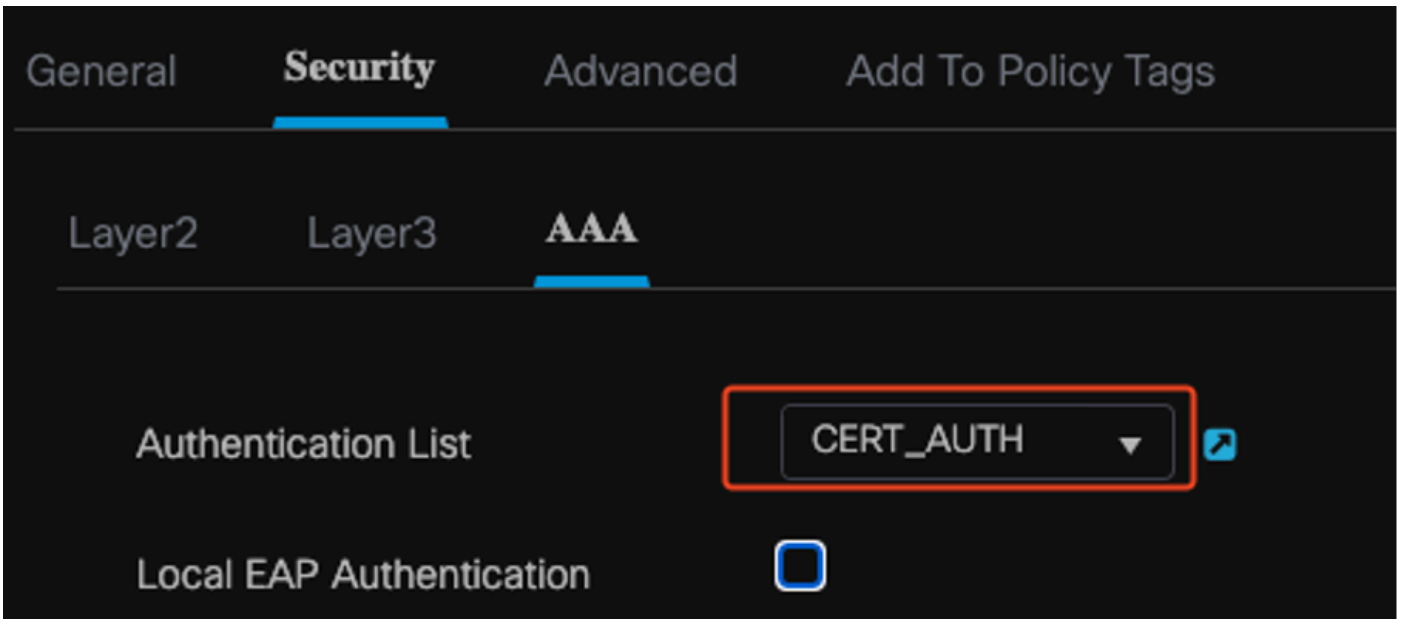
802.1x 인증을 사용하여 새 WLAN을 설정하려면 다음 단계를 수행합니다.

1. Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로필) > WLANs(WLAN)로 이동합니다.
2. Add(추가)를 클릭하여 새 WLAN을 생성합니다.

3. 레이어 2 인증 설정을 선택하고 802.1x 인증을 활성화합니다.



WLAN 프로파일 컨피그레이션

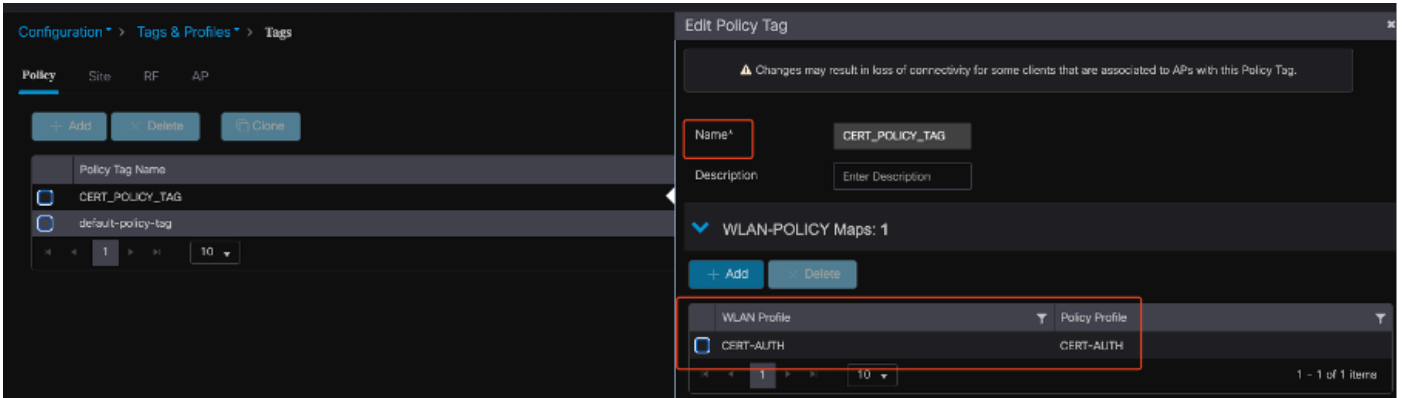


WLAN 프로파일과 방법 목록 맵

9800 WLC에서 정책 프로필을 사용하여 WLAN 매핑

WLAN을 정책 프로파일과 연결하려면 다음 단계를 수행하십시오.

1. Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로파일) > Tags(태그)로 이동합니다
2. 새 태그를 추가하려면 Add를 클릭합니다.
3. WLAN-POLICY 섹션에서 새로 생성된 WLAN을 적절한 정책 프로파일에 매핑합니다.

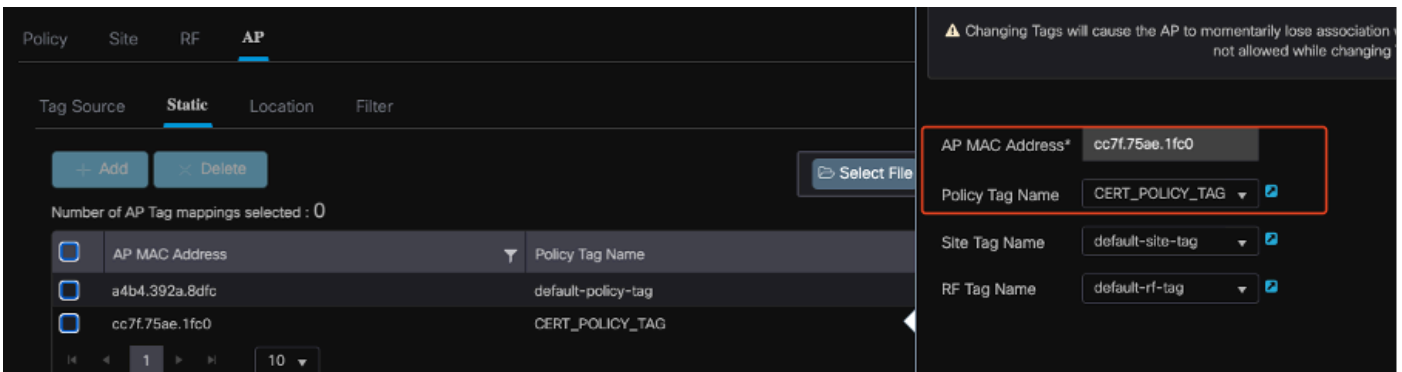


정책 태그 구성

9800 WLC의 액세스 포인트에 정책 태그 매핑

액세스 포인트(AP)에 정책 태그를 할당하는 절차는 다음과 같습니다.

1. Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로파일) > Tags(태그) > AP로 이동합니다.
2. AP 컨피그레이션 내의 Static(정적) 섹션으로 이동합니다.
3. 구성할 특정 AP를 클릭합니다.
4. 생성한 정책 태그를 선택한 AP에 할당합니다.



AP 태그 할당

설정 완료 후 WLC 구성 실행

```

aaa group server radius ISE
  server name ISE3
  ip radius source-interface Vlan2124
aaa authentication dot1x CERT_AUTH group ISE
aaa authorization network CERT_AUTH group ISE
aaa server radius dynamic-author
  client 10.106.32.31 server-key Cisco!123
!

```

```

wireless profile policy CERT-AUTH
aaa-override
ipv4 dhcp required
vlan 2124
no shutdown

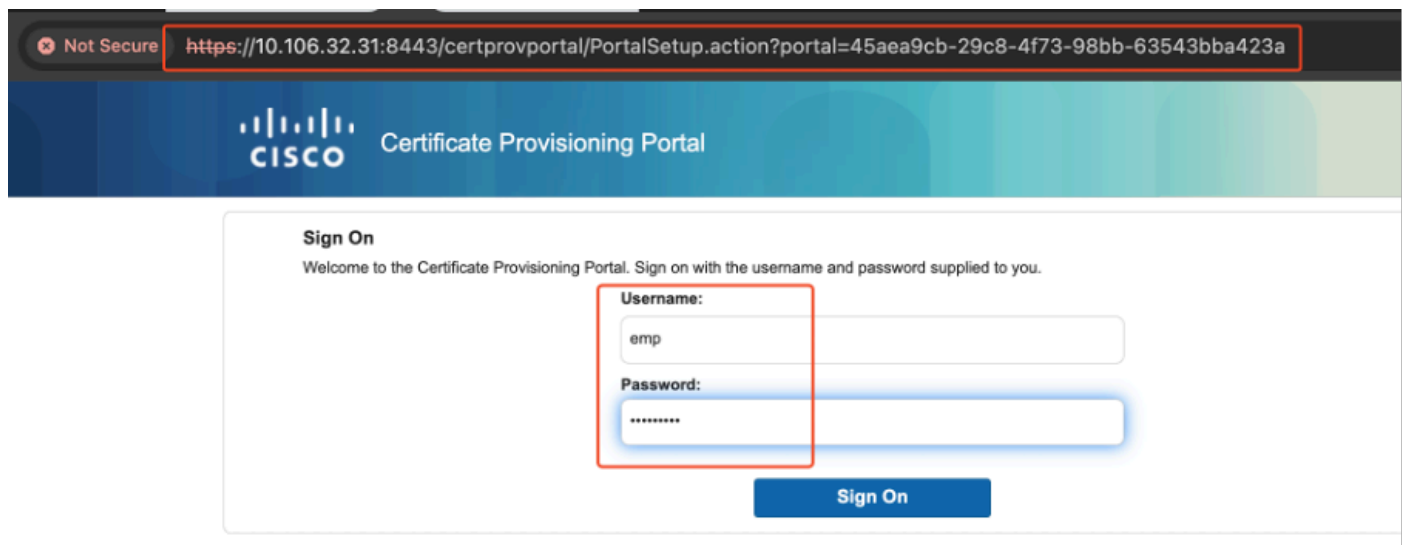
```

```
wlan CERT-AUTH policy CERT-AUTH
wlan CERT-AUTH 17 CERT-AUTH
security dot1x authentication-list CERT_AUTH
no shutdown
!
wireless tag policy CERT_POLICY_TAG
wlan CERT-AUTH policy CERT-AUTH
```

사용자에 대한 인증서 생성 및 다운로드

사용자에 대한 인증서를 만들고 다운로드하려면 다음 단계를 수행합니다.

1. 사용자가 이전에 설정한 인증서 포털에 로그인하도록 합니다.



인증서 포털 액세스

2. AUP(Acceptable Use Policy)에 동의합니다. 그러면 ISE에서 인증서 생성을 위한 페이지를 표시합니다.

3. 단일 인증서 생성을 선택합니다(인증서 서명 요청 없음).

Certificate Provisioning

I want to: *

Generate a single certificate (without a certificate...) 1

Common Name (CN): *

emp 2

MAC Address: *

242f.d0da.a563 3

Choose Certificate Template: *

EAP_Authentication_Certificate_Template 4

Description:

Certificate Download Format: *

PKCS12 format, including certificate chain (...) 5

Certificate Password: *

Enter password to download and view/install the certificate

Confirm Password: *

Generate

Reset

인증서 생성

Certificate Provisioning Portal(인증서 프로비저닝 포털)을 통해 인증서를 생성하려면 다음 필수 필드가 완료되어야 합니다.

- CN: 인증 서버는 클라이언트 인증서의 Common Name 필드에 있는 값을 사용하여 사용자를 인증합니다. Common Name(공통 이름) 필드에 사용자 이름(인증서 프로비저닝 포털에 로그인하는 데 사용됨)을 입력합니다.
- MAC 주소: SAN(주체 대체 이름)은 다양한 값을 보안 인증서와 연결할 수 있는 X.509 확장입니다. Cisco ISE, 릴리스 2.0은 MAC 주소만 지원합니다. 따라서 SAN/MAC 주소 필드에 입력합니다.
 - 인증서 템플릿: 인증서 템플릿은 CA가 요청을 검증하고 인증서를 발급할 때 사용하는 필드 집합을 정의합니다. CN(Common Name)과 같은 필드는 요청의 유효성을 검사하는 데 사용됩니다(CN은 사용자 이름과 일치해야 함). 다른 필드는 인증서를 발급하는 동

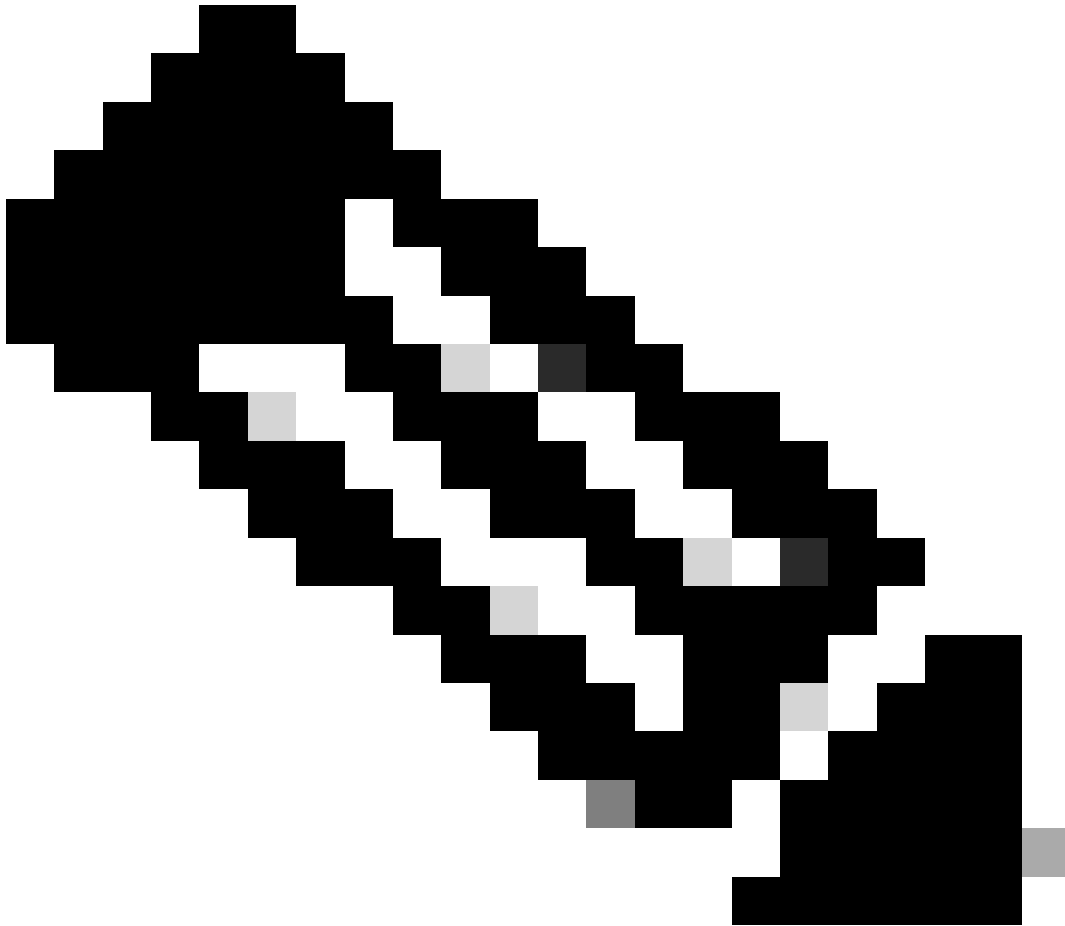
안 CA에서 사용됩니다.

- 인증서 암호: 인증서를 보호하려면 인증서 비밀번호가 필요합니다. 인증서의 내용을 보고 디바이스에서 인증서를 가져오려면 인증서 비밀번호를 제공해야 합니다.
- 암호는 다음 규칙을 준수해야 합니다.
- 암호는 대문자, 소문자 및 숫자를 각각 하나 이상 포함해야 합니다.
 - 암호는 8자에서 15자 사이여야 합니다.
 - 허용되는 문자에는 A-Z, a-z, 0-9, _, # 등이 있습니다.

모든 필드가 채워지면 Generate를 선택하여 인증서를 만들고 다운로드합니다.

Windows 10 시스템에 인증서 설치

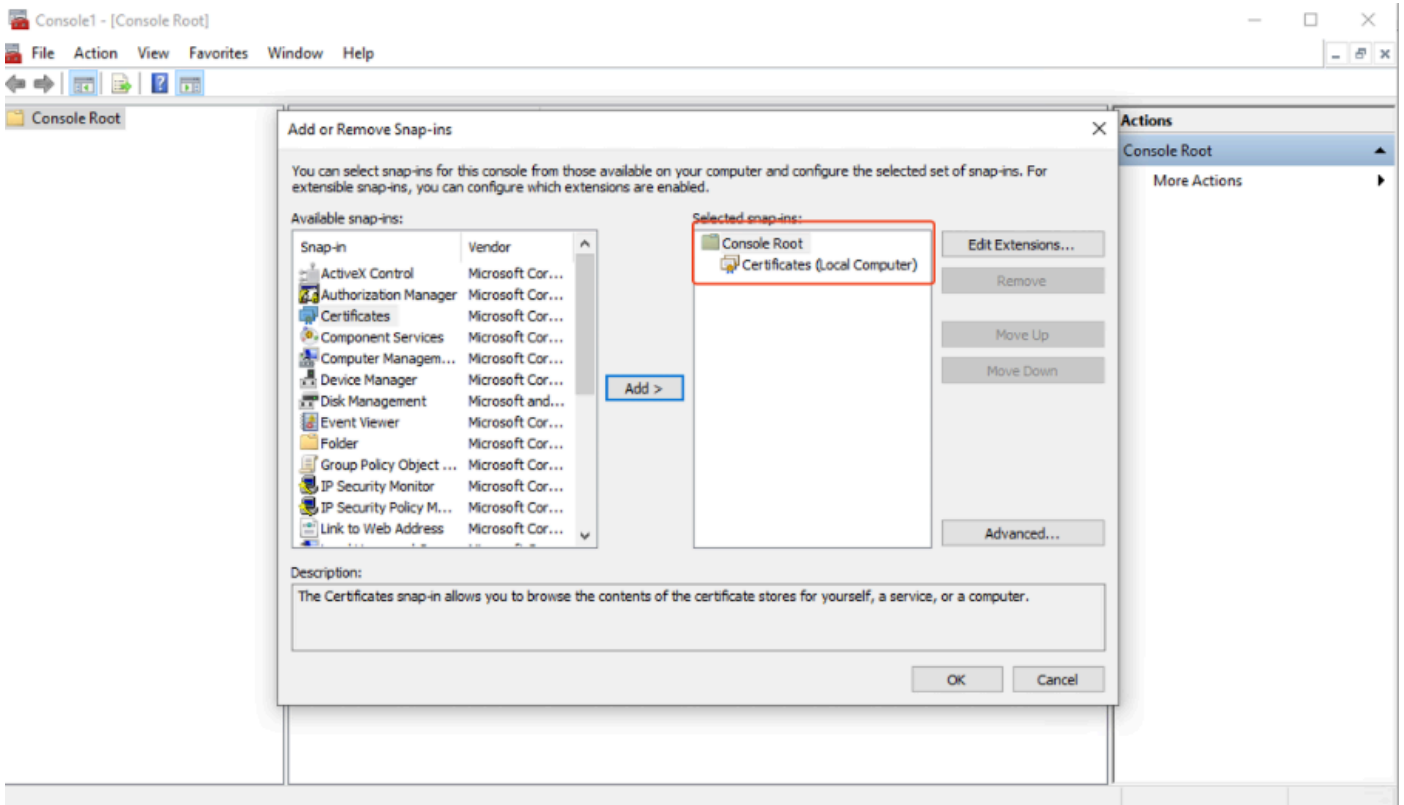
Windows 10 시스템에 인증서를 설치하려면 다음 단계를 사용하여 MMC(Microsoft Management Console)를 엽니다.



참고: 이러한 지침은 Windows 설정에 따라 다를 수 있으므로 Microsoft 설명서에서 자세한 내용을 참고하는 것이 좋습니다.

1. 시작과 실행을 차례로 클릭합니다.
2. 실행 상자에 mmc를 입력하고 Enter 키를 누릅니다. Microsoft Management Console이 열립니다.
3. 인증서 스냅인 추가:
4. 파일 > 스냅인 추가/제거 로 이동합니다.
5. Add(추가)를 선택한 다음 Certificates(인증서)를 선택하고 Add(추가)를 클릭합니다.
6. Computer Account(컴퓨터 계정), Local Computer(로컬 컴퓨터)를 선택하고 Finish(마침)를 클릭합니다.

이 단계를 통해 로컬 컴퓨터에서 인증서를 관리할 수 있습니다.



Windows MMC 콘솔

1단계. 인증서 가져오기:

- 1.1. 메뉴에서 Action을 클릭합니다.
- 1.2. 모든 작업으로 이동한 다음 가져오기를 선택합니다.
- 1.3. 프롬프트를 진행하여 시스템에 저장된 인증서 파일을 찾아 선택합니다.



← Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

C:\Users\admin\Desktop\emp-2025-01-06_08-30-59\emp_C4-E9-0

Browse...

Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX, .P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

Next

Cancel

인증서 가져오기

인증서 가져오기 프로세스 중에 포털에서 인증서를 생성할 때 생성한 비밀번호를 입력하라는 메시지가 표시됩니다. 이 비밀번호를 정확하게 입력하여 컴퓨터에 인증서를 성공적으로 가져오고 설치하십시오.

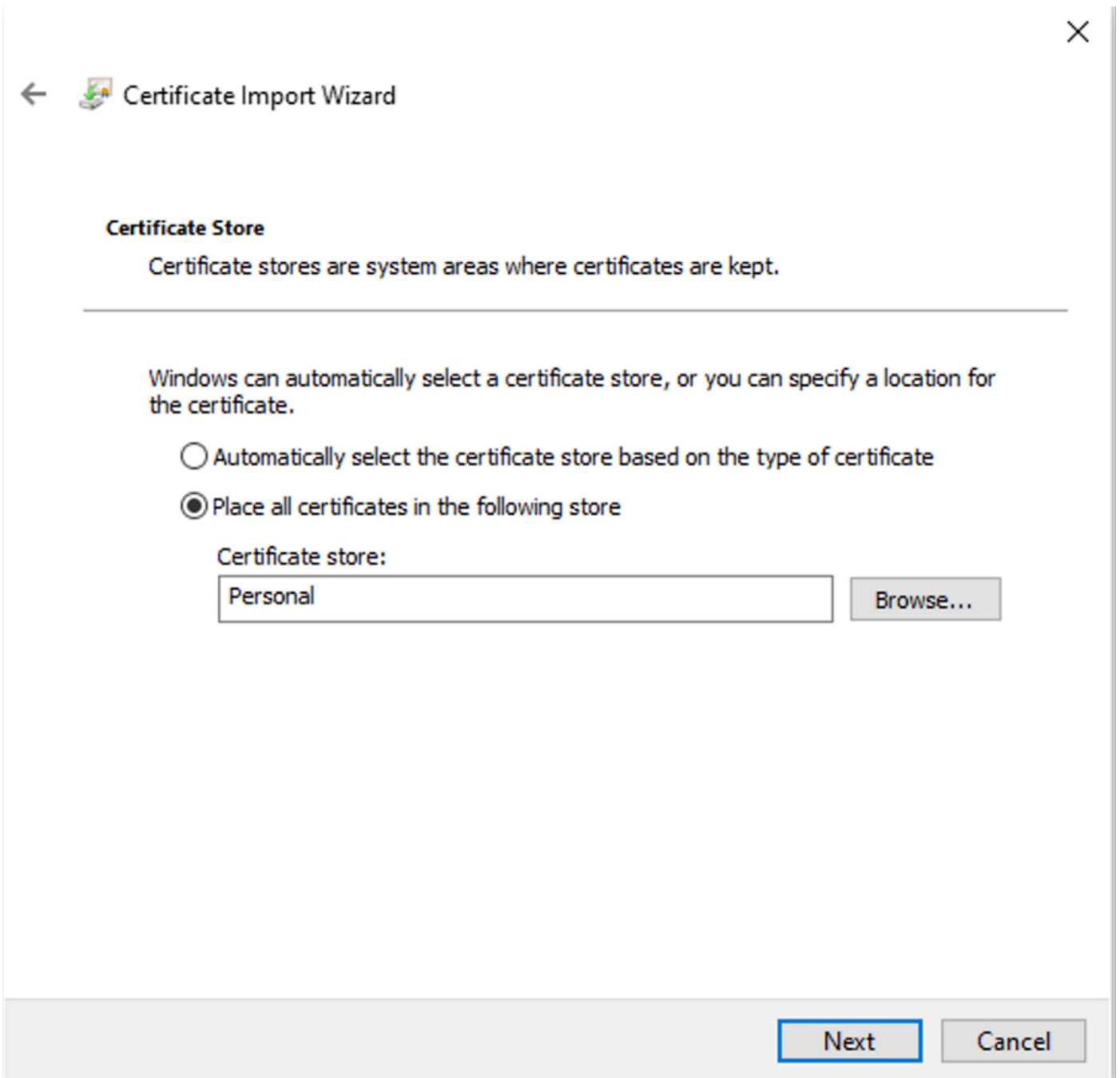
The image shows a Windows dialog box titled "Certificate Import Wizard". It has a back arrow on the left and a close button (X) on the top right. The main content is under the heading "Private key protection" and includes the text "To maintain security, the private key was protected with a password." Below this, it says "Type the password for the private key." There is a "Password:" label followed by a text input field containing ten black dots and a cursor. Below the input field is a checkbox labeled "Display Password". Underneath is the "Import options:" section with four checkboxes: "Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option." (unchecked), "Mark this key as exportable. This will allow you to back up or transport your keys at a later time." (unchecked), "Protect private key using virtualized-based security(Non-exportable)" (unchecked), and "Include all extended properties." (checked). At the bottom right, there are two buttons: "Next" (highlighted with a blue border) and "Cancel".

인증서 비밀번호 입력

2단계. 인증서를 적절한 폴더로 이동합니다.

- 2.1. Microsoft Management Console(MMC)을 열고 Certificates(로컬 컴퓨터) > Personal 폴더로 이동합니다.
- 2.2. 인증서를 검토하고 해당 유형(예: 루트 CA, 중간 CA 또는 개인)을 결정합니다.
- 2.3. 각 인증서를 적절한 저장소로 이동:
- 2.4. 루트 CA 인증서: 신뢰할 수 있는 루트 인증 기관으로 이동합니다.
- 2.5. 중간 CA 인증서 중간 인증 기관으로 이동합니다.

2.6. 개인증명서 개인 폴더에 둡니다.



개인 폴더에 인증서 저장

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status
Certificate Services Endpoint Sub CA - ise3gencv	Certificate Services Node CA - ise3gencv	1/3/2035	<All>	EndpointSubCA	
Certificate Services Node CA - ise3gencv	Certificate Services Root CA - ise3gencv	1/3/2035	<All>	certificate_nodeCA	
Certificate Services Root CA - ise3gencv	Certificate Services Root CA - ise3gencv	1/3/2035	<All>	certificate	
emp	Certificate Services Endpoint Sub CA - ise3gencv	1/6/2027	Client Authentication	emp_C4-E9-0A-00-...	
ise3gencvlab.local	ise3gencvlab.local	1/3/2027	Server Authentication, Client Authentication	Self-Signed	

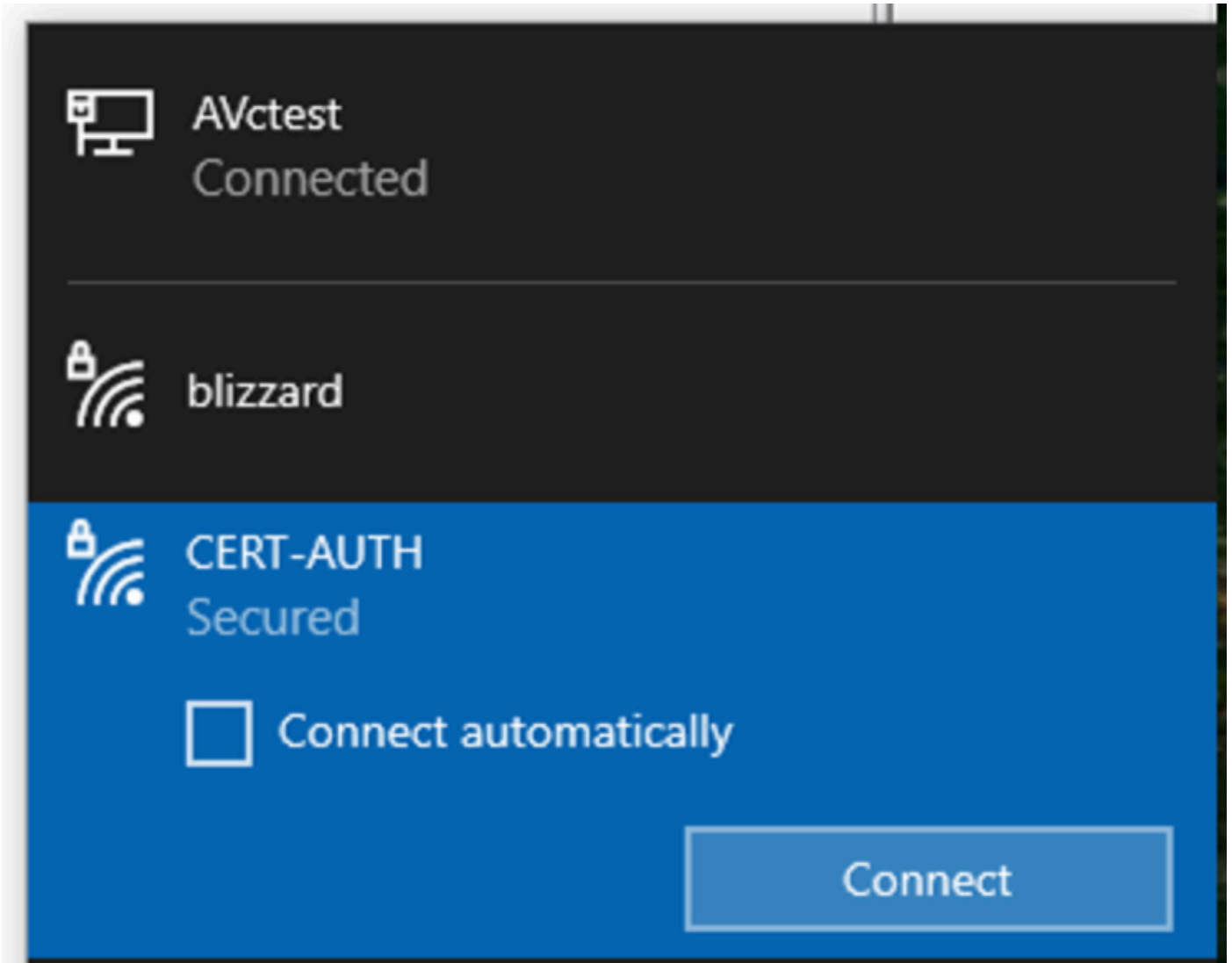
스토어에서 인증서 이동

Windows 컴퓨터 연결

인증서가 올바른 저장소로 이동되면 다음 단계를 사용하여 WLAN에 연결합니다.

1. 사용 가능한 무선 네트워크를 보려면 시스템 트레이에서 네트워크 아이콘을 클릭합니다.

2. 연결하려는 WLAN의 이름을 찾아 클릭합니다.
3. Connect(연결)를 클릭하고 추가 프롬프트를 계속 진행하여 인증을 위해 인증서를 사용하여 연결 프로세스를 완료합니다.



무선 네트워크에 연결

WLAN에 연결하는 동안 프롬프트가 표시되면 인증서를 사용하여 연결하는 옵션을 선택합니다.



CERT-AUTH

Secured

Enter your user name and password

Connect using a certificate

OK

Cancel

인증서를 자격 증명으로 사용

이렇게 하면 인증서를 사용하여 무선 네트워크에 성공적으로 연결할 수 있습니다.

```
C:\>netsh wlan show interface
```

```
There is 1 interface on the system:
```

```
Name : Wi-Fi 3
Description : TP-Link Wireless USB Adapter
GUID : ee5d1c47-43cc-4873-9ae6-99e2e43c39ea
Physical address : 24:2f:d0:da:a5:63
State : connected
SSID : CERT-AUTH
BSSID : a4:88:73:9e:8d:af
Network type : Infrastructure
Radio type : 802.11ac
Authentication : WPA2-Enterprise
Cipher : CCMP
Connection mode : Profile
Channel : 36
Receive rate (Mbps) : 360
Transmit rate (Mbps) : 360
Signal : 100%
Profile : CERT-AUTH

Hosted network status : Not available
```

```
C:\>netsh wlan show profiles CERT-AUTH | find "Smart"
```

```
EAP type : Microsoft: Smart Card or other certificate
```

무선 프로파일 확인

다음을 확인합니다.

WLAN이 WLC에 의해 브로드캐스트되고 있는지 확인합니다.

```
<#root>
```

```
POD6_9800#show wlan summ
```

```
Number of WLANs: 2
```

```
ID Profile Name SSID Status Security
```

```
-----
```

```
17
```

```
CERT-AUTH
```

```
CERT-AUTH
```

```
UP [WPA2][802.1x][AES]
```

AP가 WLC에 켜져 있는지 확인합니다.

```
POD6_9800#show ap summ
Number of APs: 1
CC = Country Code
RD = Regulatory Domain
AP Name Slots AP Model Ethernet MAC Radio MAC CC RD IP Address State Location
-----
AP1 3 C9130AXI-D cc7f.75ae.1fc0 a488.739e.8da0 IN -D 10.78.8.78 Registered default location
```

AP가 WLAN을 브로드캐스트하는지 확인합니다.

<#root>

```
POD6_9800#show ap name AP1 wlan dot11 24ghz
Slot id : 0
WLAN ID BSSID
-----
17 a488.739e.8da0
```

```
POD6_9800#show ap name AP1 wlan dot11 5ghz
Slot id : 1
WLAN ID BSSID
-----
17
a488.739e.8daf
```

EAP-TLS를 사용하여 연결된 클라이언트:

<#root>

```
POD6_9800#show wire cli summ
Number of Clients: 1
MAC Address AP Name Type ID State Protocol Method Role
-----
242f.d0da.a563 AP1 WLAN

17
IP Learn 11ac

Dot1x
Local

POD6_9800#sho wireless client mac-address 242f.d0da.a563 detail | in username|SSID|EAP|AAA|VLAN
Wireless LAN Network Name (SSID): CERT-AUTH

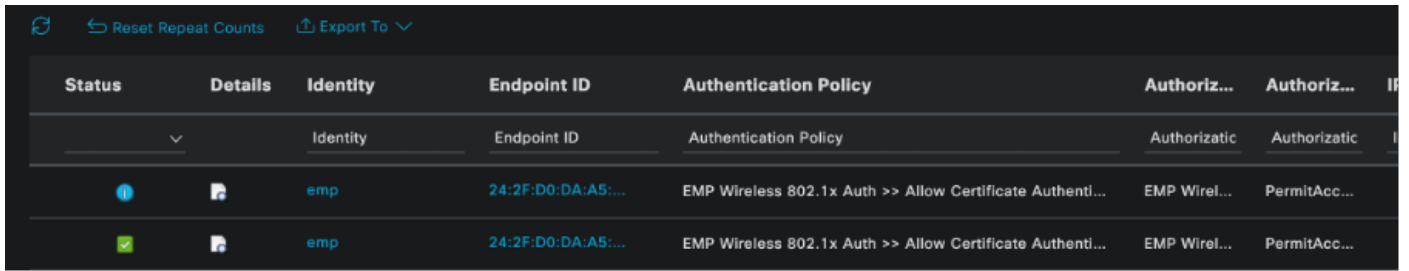
BSSID : a488.739e.8daf

EAP Type : EAP-TLS

VLAN : 2124
Multicast VLAN : 0
```

VLAN : 2124

Cisco Radius ISE 라이브 로그:



Status	Details	Identity	Endpoint ID	Authentication Policy	Authoriz...	Authoriz...	IP
	▼	Identity	Endpoint ID	Authentication Policy	Authorizatic	Authorizatic	I
ⓘ	📄	emp	24:2F:D0:DA:A5:...	EMP Wireless 802.1x Auth >> Allow Certificate Authenti...	EMP Wirel...	PermitAcc...	
✅	📄	emp	24:2F:D0:DA:A5:...	EMP Wireless 802.1x Auth >> Allow Certificate Authenti...	EMP Wirel...	PermitAcc...	

ISE Radius 라이브 로그

자세한 인증 유형:

Authentication Details

Source Timestamp	2025-01-08 11:58:21.055
Received Timestamp	2025-01-08 11:58:21.055
Policy Server	ise3genvc
Event	5200 Authentication succeeded
Username	emp
Endpoint Id	24:2F:D0:DA:A5:63
Calling Station Id	24-2f-d0-da-a5-63
Endpoint Profile	TP-LINK-Device
Identity Group	User Identity Groups:Employee,Profiled
Audit Session Id	4D084E0A0000007E46F0C6F7
Authentication Method	dot1x
Authentication Protocol	EAP-TLS
Service Type	Framed
Network Device	lab-9800
Device Type	All Device Types
Location	All Locations
NAS IPv4 Address	10.78.8.77
NAS Port Type	Wireless - IEEE 802.11
Authorization Profile	PermitAccess
Security Group	Employees

ISE 세부 로그

EAP-TLS 패킷을 표시하는 WLC EPC 캡처:

No.	Time	Source	Destination	Protocol	Length	Info
65	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	95	Request, Identity
68	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	95	Request, Identity
69	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, Identity
70	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, Identity
73	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	96	Request, TLS EAP (EAP-TLS)
74	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	TLsv1.2	304	Client Hello
78	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	182	Request, TLS EAP (EAP-TLS)
79	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, TLS EAP (EAP-TLS)
83	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	178	Request, TLS EAP (EAP-TLS)
84	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, TLS EAP (EAP-TLS)
87	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	TLsv1.2	248	Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done
95	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	640	Response, TLS EAP (EAP-TLS)
100	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	96	Request, TLS EAP (EAP-TLS)
102	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	640	Response, TLS EAP (EAP-TLS)
107	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	96	Request, TLS EAP (EAP-TLS)
109	17:36:59	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	640	Response, TLS EAP (EAP-TLS)
114	17:36:59	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	96	Request, TLS EAP (EAP-TLS)
115	17:36:59	TpLinkPte_da:a5:63	Cisco_9e:8d:af	TLsv1.2	347	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
118	17:36:59	Cisco_9e:8d:af	TpLinkPte_da:a5:63	TLsv1.2	147	Change Cipher Spec, Encrypted Handshake Message
119	17:36:59	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, TLS EAP (EAP-TLS)
126	17:36:59	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	94	Success

EAP 트랜잭션을 보여주는 WLC 캡처

- 패킷 번호 87은 문서 시작 부분에 설명된 EAP-TLS 흐름의 8단계에 해당합니다.
- 패킷 번호 115는 문서 시작 부분에 설명된 EAP-TLS 흐름의 9단계에 해당합니다.
- 패킷 번호 118은 문서의 시작 부분에 설명된 EAP-TLS 흐름의 10단계에 해당합니다.

클라이언트 연결을 보여 주는 RA(무선 활성) 추적: 이 RA 추적은 인증 트랜잭션의 관련 라인 일부를 표시하도록 필터링됩니다.

2025/01/08 11 58 20.816875191 {wncd_x_R0-2}{1} [ewlc-capwapmsg-ses] [15655] (디버그) 암호화된 DTLS 메시지 전송. 대상 IP 10.78.8.78[5256], 길이 499

2025/01/08 11 58 20.851392112 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS 10.106.33.23 1812 id 0/25, len 390으로 액세스 요청 전송

2025/01/08 11 58 20.871842938 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS id 1812/25 10.106.33.23 0, Access-Challenge, len 123에서 수신됨

2025/01/08 11 58 20.872246323 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] EAPOL 패킷 전송 - 버전 3,EAPOL 유형 EAP, 페이로드 길이 6, EAP-유형 = EAP-TLS

2025/01/08 11 58 20.881960763 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] EAPOL 패킷 수신 - 버전 1,EAPOL 유형 EAP, 페이로드 길이 204, EAP-유형 = EAP-TLS

2025/01/08 11 58 20.882292551 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS 10.106.33.23 1812 id 0/26, len 663으로 액세스 요청 전송

2025/01/08 11 58 20.926204990 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS id 1812/26 10.106.33.23 0, Access-Challenge, len 1135에서 수신됨

2025/01/08 11 58 20.927390754 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] EAPOL 패킷 전송 - 버전 3,EAPOL 유형 EAP, 페이로드 길이 1012, EAP 유형 = EAP-TLS

2025/01/08 11 58 20.935081108 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] EAPOL 패킷 수신 - 버전 1,EAPOL 유형 EAP, 페이로드 길이 6, EAP-유형 = EAP-TLS

2025/01/08 11 58 20.935405770 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS 10.106.33.23 1812 id 0/27, len 465로 액세스 요청 전송

2025/01/08 11 58 20.938485635 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS id 1812/27 10.106.33.23 0, Access-Challenge, len 1131에서 수신됨

2025/01/08 11 58 20.939630108 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] EAPOL 패킷 전송 - 버전 3,EAPOL 유형 EAP, 페이로드 길이 1008, EAP-유형

= EAP-TLS

2025/01/08 11 58 20.947417061 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] EAPOL 패킷 수신 - 버전 1,EAPOL 유형 EAP, 페이로드 길이 6, EAP-유형 = EAP-TLS

2025/01/08 11 58 20.947722851 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS 10.106.33.23 1812 id 0/28, len 465로 액세스 요청 전송

2025/01/08 11 58 20.949913199 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS id 1812/28 10.106.33.23 0, Access-Challenge, len 275에서 수신됨

2025/01/08 11 58 20.950432303 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] EAPOL 패킷 전송 - 버전 3,EAPOL 유형 EAP, 페이로드 길이 158, EAP-유형 = EAP-TLS

2025/01/08 11 58 20.966862562 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] EAPOL 패킷 수신 - 버전 1,EAPOL 유형 EAP, 페이로드 길이 1492, EAP-유형 = EAP-TLS

2025/01/08 11 58 20.967209224 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS 10.106.33.23 1812 id 0/29, len 1961로 액세스 요청 전송

2025/01/08 11 58 20.971337739 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS id 1812/29 10.106.33.23 0, Access-Challenge, len 123에서 수신

2025/01/08 11 58 20.971708100 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] EAPOL 패킷 전송 - 버전 3,EAPOL 유형 EAP, 페이로드 길이 6, EAP-유형 = EAP-TLS

2025/01/08 11 58 20.978742828 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] EAPOL 패킷 수신 - 버전 1,EAPOL 유형 EAP, 페이로드 길이 1492, EAP-유형 = EAP-TLS

2025/01/08 11 58 20.979081544 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS 10.106.33.23 1812 id 0/30, len 1961로 액세스 요청 전송

2025/01/08 11 58 20.982535977 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS id 1812/30 10.106.33.23 0, Access-Challenge, len 123에서 수신됨

2025/01/08 11 58 20.982907200 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] EAPOL 패킷 전송 - 버전 3,EAPOL 유형 EAP, 페이로드 길이 6, EAP-유형 = EAP-TLS

2025/01/08 11 58 20.990141062 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] EAPOL 패킷 수신 - 버전 1,EAPOL 유형 EAP, 페이로드 길이 1492, EAP-유형 = EAP-TLS

2025/01/08 11 58 20.990472026 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS 10.106.33.23 1812 id 0/31, len 1961로 액세스 요청 전송

2025/01/08 11 58 20.994358525 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS id 1812/31 10.106.33.23 0, Access-Challenge, len 123에서 수신됨

2025/01/08 11 58 20.994722151 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] EAPOL 패킷 전송 - 버전 3,EAPOL 유형 EAP, 페이로드 길이 6, EAP-유형 = EAP-TLS

2025/01/08 11 58 21.001735553 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] EAPOL 패킷 수신 - 버전 1,EAPOL 유형 EAP, 페이로드 길이 247, EAP-유형 = EAP-TLS

2025/01/08 11 58 21.002076369 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS 10.106.33.23 1812 id 0/32, len 706으로 액세스 요청 보내기

2025/01/08 11 58 21.013571608 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS id 1812/32 10.106.33.23 0, Access-Challenge, len 174에서 수신됨
2025/01/08 11 58 21.013987785 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] EAPOL 패킷 전송 - 버전 3,EAPOL 유형 EAP, 페이로드 길이 57, EAP-유형 = EAP-TLS
2025/01/08 11 58 21.024429150 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] EAPOL 패킷 수신 - 버전 1,EAPOL 유형 EAP, 페이로드 길이 6, EAP-유형 = EAP-TLS
2025/01/08 11 58 21.024737996 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS 10.106.33.23 1812 id 0/33, len 465로 Access-Request 전송
2025/01/08 11 58 21.057794929 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS id 1812/33 10.106.33.23 0, Access-Accept, len 324에서 수신됨
2025/01/08 11 58 21.058149893 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] eap 방법 EAP-TLS에 대한 ID 업데이트 이벤트가 발생했습니다.

문제 해결

일반적인 Wireless 802.1x 문제 해결 절차 외에는 이 문제에 대한 구체적인 문제 해결 단계가 없습니다.

1. 클라이언트 RA 추적 디버그를 수행하여 인증 프로세스를 확인합니다.
2. WLC EPC 캡처를 수행하여 클라이언트, WLC 및 RADIUS 서버 간의 패킷을 검토합니다.
3. ISE 라이브 로그를 확인하여 요청이 올바른 정책과 일치하는지 확인합니다.
4. Windows 엔드포인트에서 인증서가 올바르게 설치되어 있고 전체 신뢰 체인이 있는지 확인합니다.

참조

- [인증서 프로비저닝 포털 FAQ, 릴리스 3.2](#)
- [ISE 내부 인증 기관 서비스 이해](#)
- [WLC 및 ISE를 사용하여 EAP-TLS 이해 및 구성](#)

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.