WLC 및 ISE를 사용하여 EAP-TLS 이해 및 구성

목차

소개

이 문서에서는 802.1X 및 EAP-TLS를 사용하여 WLAN(Wireless Local Area Network)을 설정하는 방법에 대해 설명합니다

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 802.1X 인증 프로세스
- 인증서

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

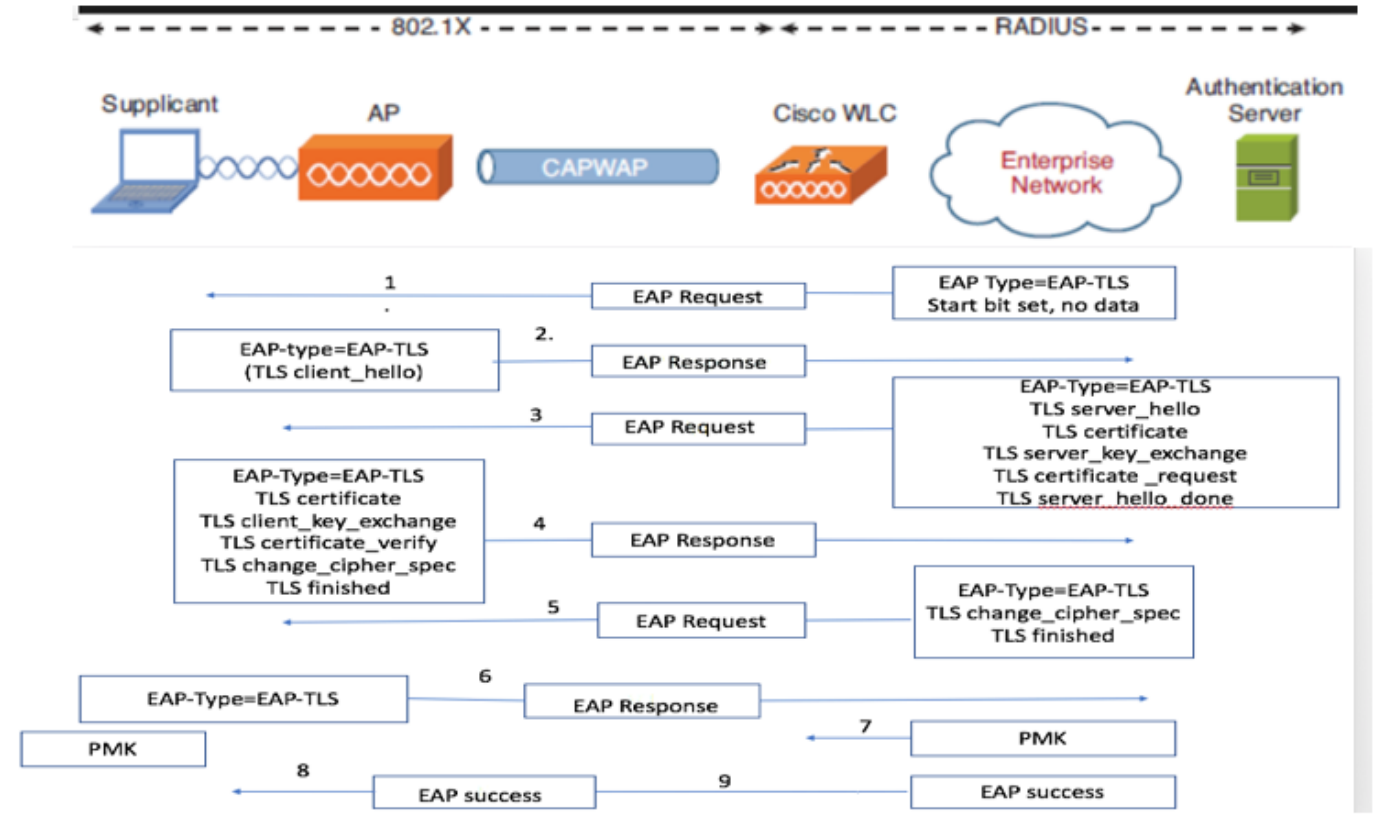
- WLC 3504 버전 8.10

- ISE(Identity Services Engine) 버전 2.7

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

배경 정보

EAP-TLS 흐름



EAP-TLS 흐름의 단계

1. 무선 클라이언트가 액세스 포인트(AP)에 연결됩니다. AP는 클라이언트가 이 시점에서 데이터를 전송하도록 허용하지 않으며 인증 요청을 보냅니다. 그러면 신청자가 EAP-Response ID로 응답합니다. 그런 다음 WLC는 사용자 ID 정보를 인증 서버에 전달합니다. RADIUS 서버는 EAP-TLS 시작 패킷으로 클라이언트에 응답합니다. EAP-TLS 대화가 이 시점에서 시작됩니다 .
2. 피어는 NULL로 설정된 암호인 "client_hello" 핸드셰이크 메시지가 포함된 인증 서버로 EAP-Response를 다시 보냅니다
3. 인증 서버는 다음을 포함하는 Access-challenge 패킷으로 응답합니다.

```
TLS server_hello
handshake message
certificate
server_key_exchange
certificate request
server_hello_done.
```

4. 클라이언트는 다음 항목을 포함하는 EAP 응답 메시지로 응답합니다.

```
Certificate ¬ Server can validate to verify that it is trusted.

client_key_exchange

certificate_verify ¬ Verifies the server is trusted

change_cipher_spec

TLS finished
```

5.클라이언트가 성공적으로 인증되면 RADIUS 서버는 "change_cipher_spec" 및 핸드셰이크 완료 메시지를 포함하는 Access-challenge로 응답합니다.

6.이를 수신하면 클라이언트는 radius 서버를 인증하기 위해 해시를 확인합니다.

7. 새 암호화 키는 TLS 핸드셰이크 중에 암호에서 동적으로 파생됩니다

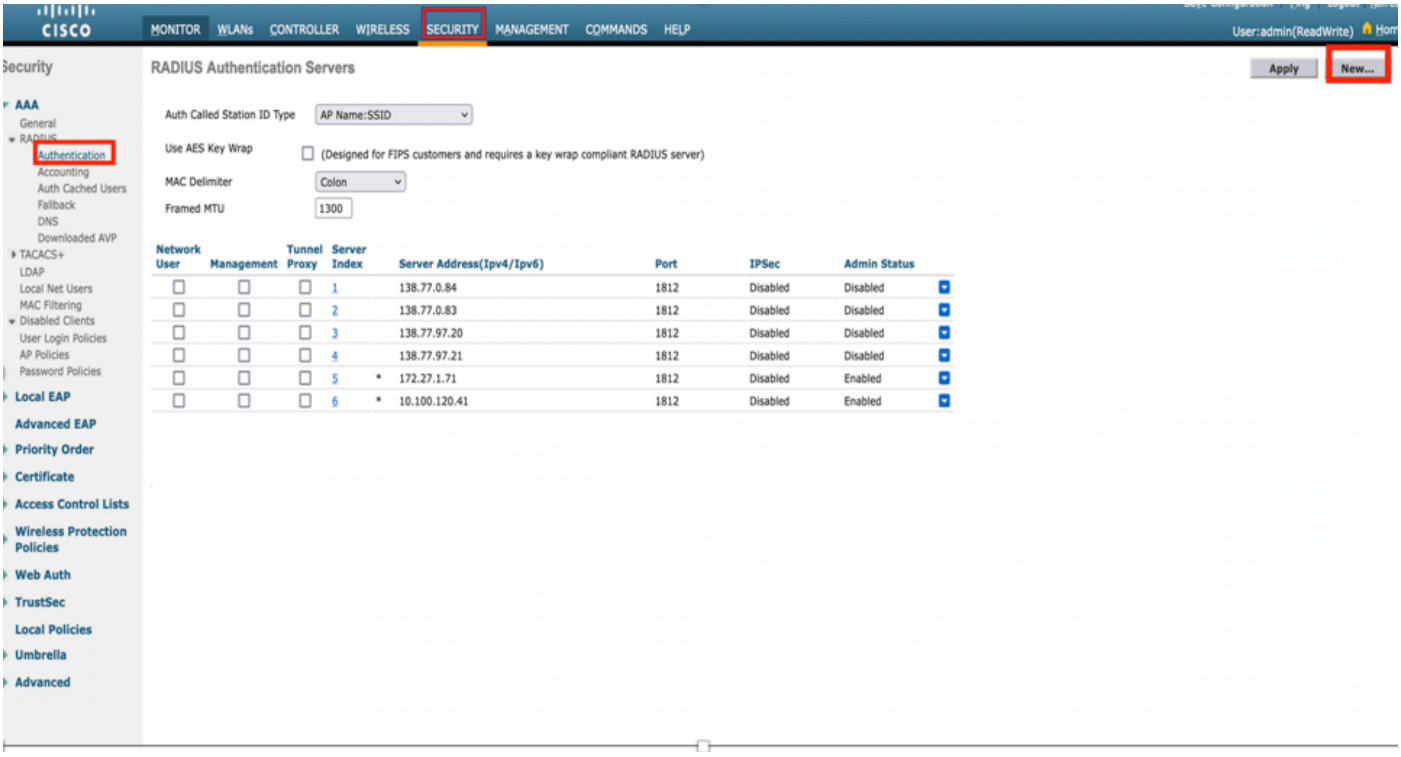
8/9.EAP-Success가 서버에서 인증자로 최종 전송되면 신청자에게 전달됩니다.

이때 EAP-TLS가 활성화된 무선 클라이언트는 무선 네트워크에 액세스할 수 있습니다.

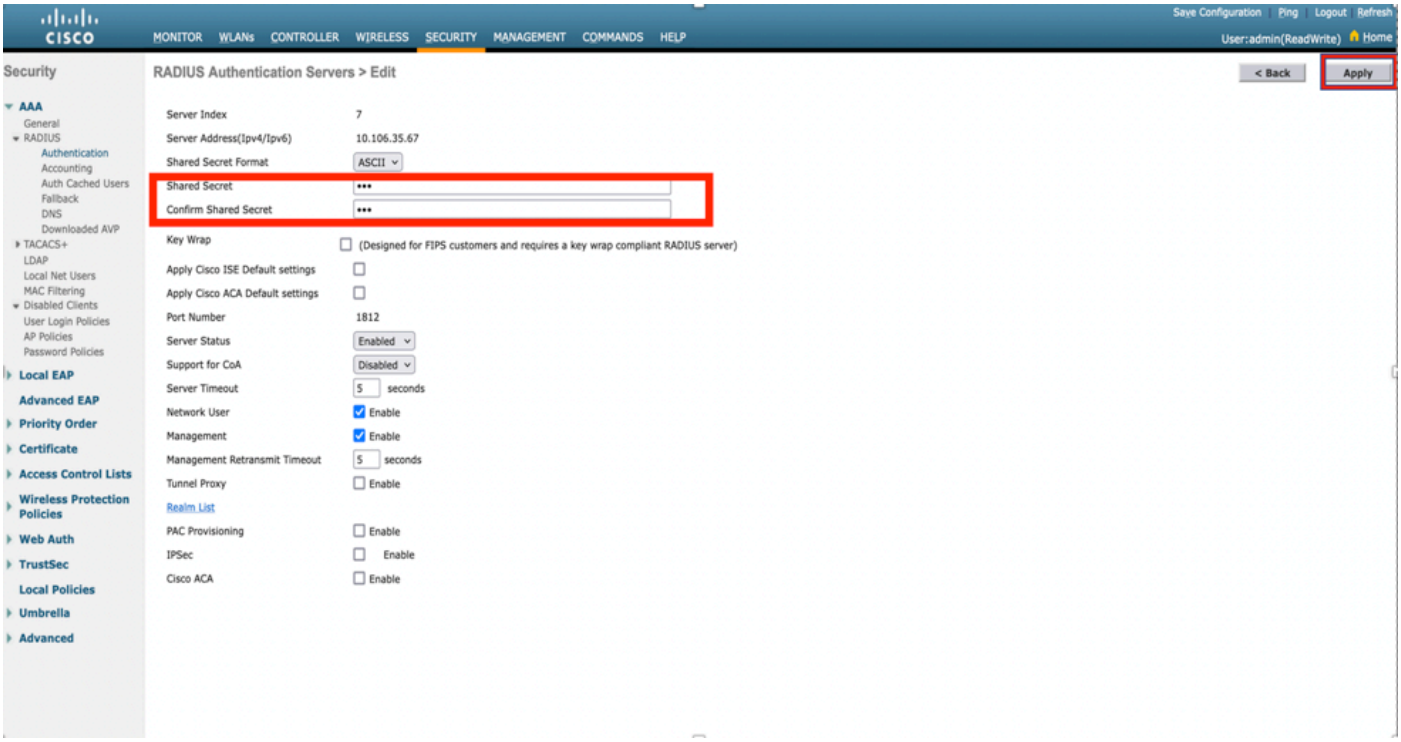
구성

Cisco Wireless LAN Controller

1단계. 첫 번째 단계는 Cisco WLC에서 RADIUS 서버를 구성하는 것입니다. RADIUS 서버를 추가하려면 Security(보안) > RADIUS **> Authentication(인증)으로 이동합니다**. 이미지에 표시된 대로 **New**(새로 만들기)를 클릭합니다.



2단계. 여기서 ISE의 WLC를 검증하기 위해 사용되는 IP 주소와 공유 암호 <password>를 입력해야 합니다. 이미지**에** 표시된 대로 계속하려면 Apply를 클릭합니다.

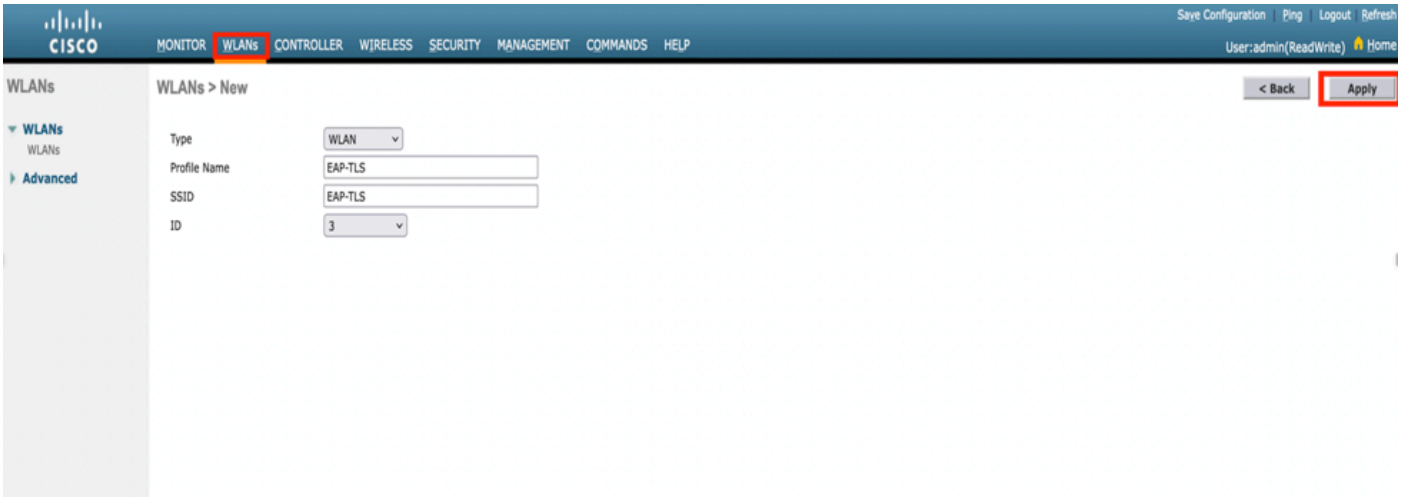


3단계. RADIUS 인증을 위한 WLAN을 생성합니다.

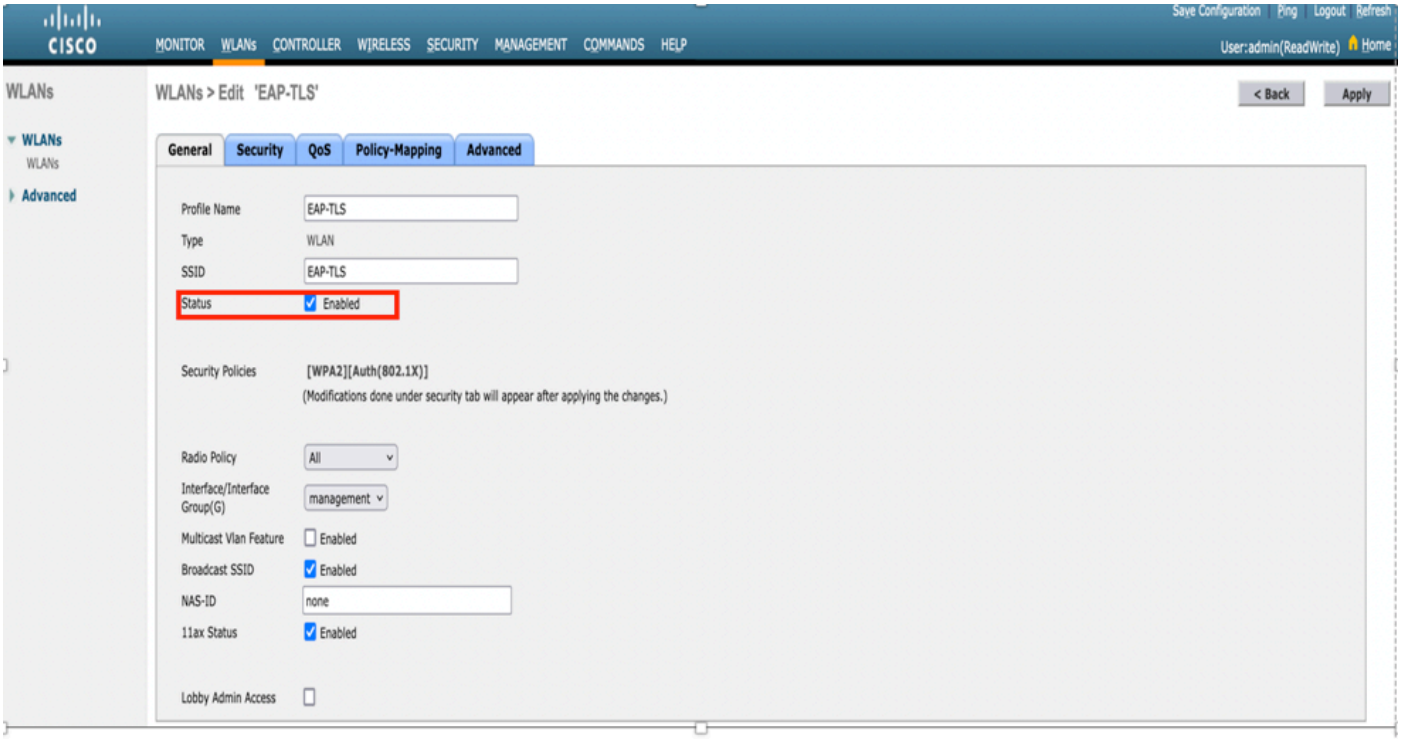
이제 새 WLAN을 생성하고 WPA-엔터프라이즈 모드를 사용하도록 구성하여 인증에 RADIUS를 사용할 수 있습니다.

4단계. 주 메뉴에서 **WLANs**를 선택하고 Create **New(새로 만들기)**를 선택한 후 **Go(이동)**를 클릭합니다.

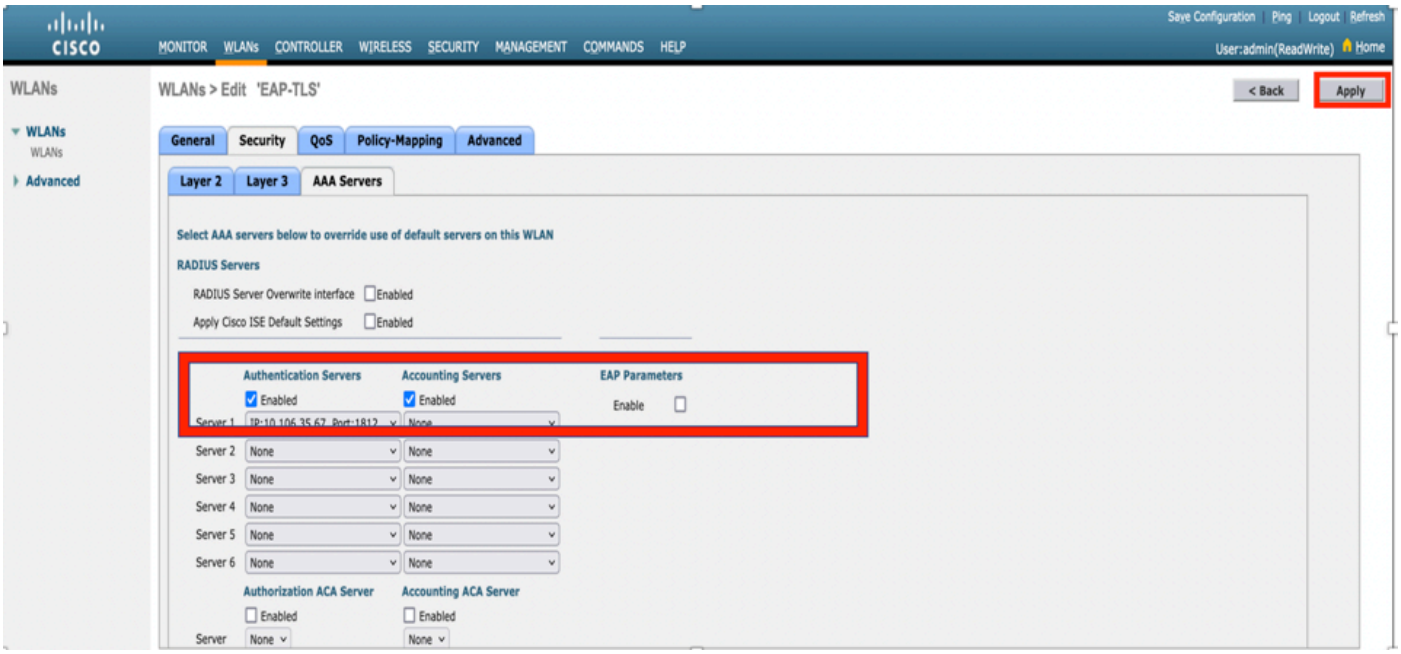
5단계. 새 WLAN EAP-TLS의 **이름을 지정합니다**. 이미지**에** 표시된 대로 계속하려면 Apply를 클릭합니다.



6단계. **General(일반)**을 클릭하고 Status(상태)가 Enabled(활성화됨)**인지 확인합니다**. 기본 보안 정책은 이미지에 표시된 802.1X 인증 및 WPA2입니다.



7단계. 이제 **Security(보안) > AAA Servers(AAA 서버)** 탭으로 이동하여 이미지에 표시된 대로 방금 구성한 RADIUS 서버를 선택합니다.



참고: 계속하기 전에 WLC에서 RADIUS 서버에 연결할 수 있는지 확인하는 것이 좋습니다. RADIUS는 (인증을 위해) UDP 포트 1812를 사용하므로 이 트래픽이 네트워크의 어느 곳에서도 차단되지 않도록 해야 합니다.

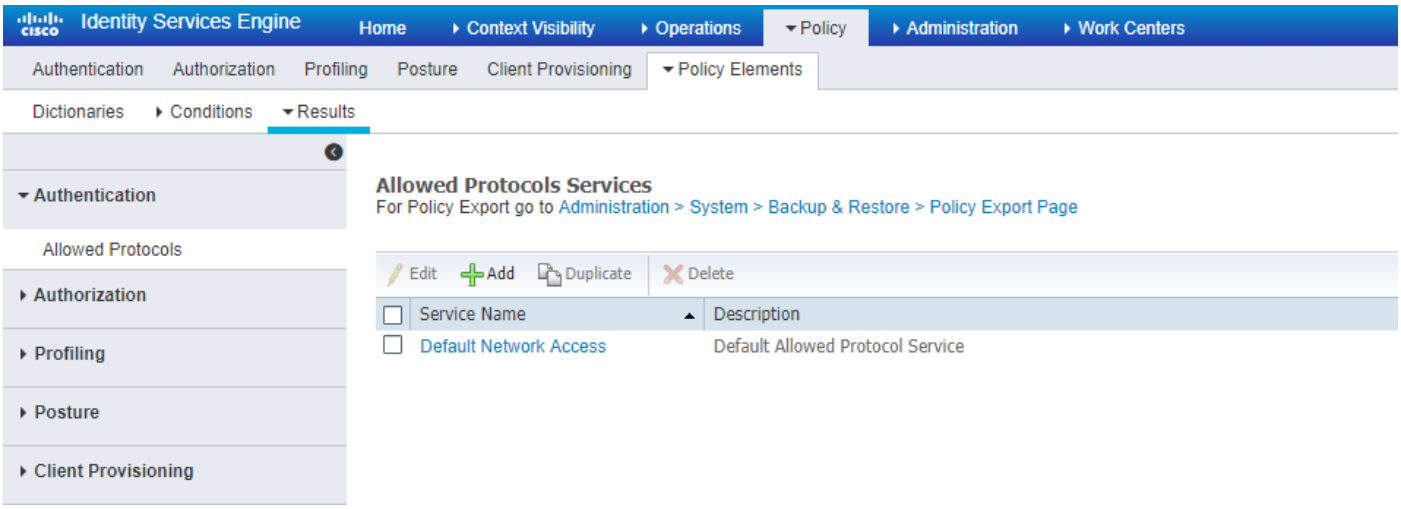
Cisco WLC를 사용하는 ISE

EAP-TLS 설정

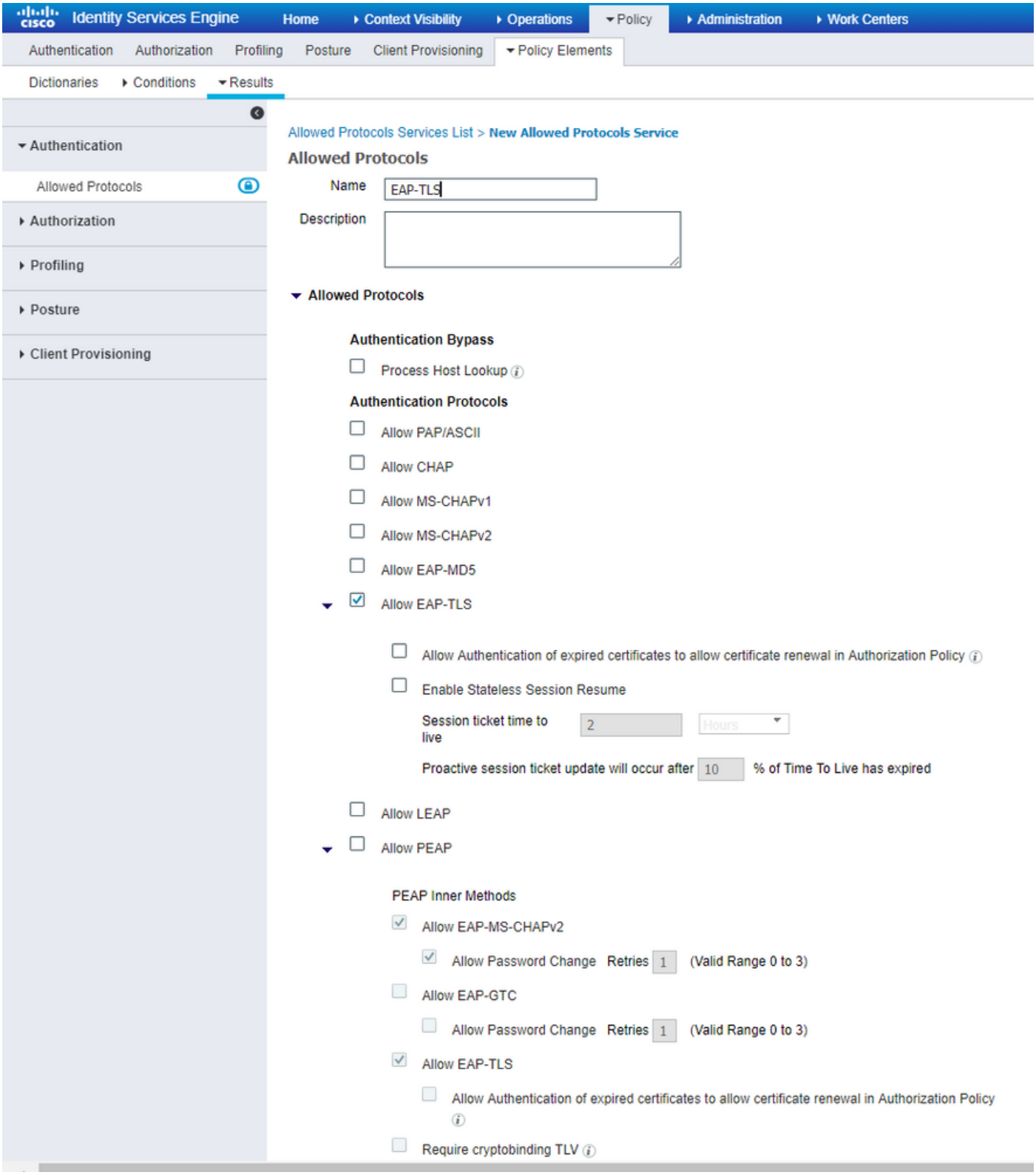
정책을 빌드하려면 정책에서 사용할 수 있는 프로토콜 목록을 만들어야 합니다. dot1x 정책이 작성되었으므로 정책 구성 방법에 따라 허용되는 EAP 유형을 지정합니다.

기본값을 사용하는 경우, 특정 EAP 유형에 대한 액세스를 잠가야 하는 경우 선호되지 않는 인증에 대부분의 EAP 유형을 허용합니다.

1단계. 이미지에 표시된 대로 **Policy(정책) > Policy Elements(정책 요소) > Results(결과) > Authentication(인증) > Allowed Protocols(허용된** 프로토콜)로 **이동하고** Add(추가)를 클릭합니다.

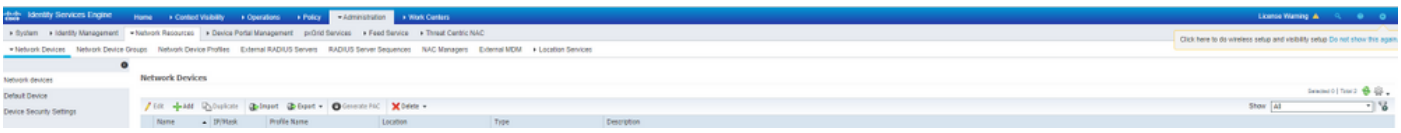


2단계. 이 Allowed Protocol(허용된 프로토콜) 목록에서 목록의 이름을 입력할 수 있습니다. 이 경우 이미지에 표시된 대로 **Allow EAP-**TLS(EAP-TLS 허용) 상자가 선택되고 다른 상자가 선택되지 않습니다.

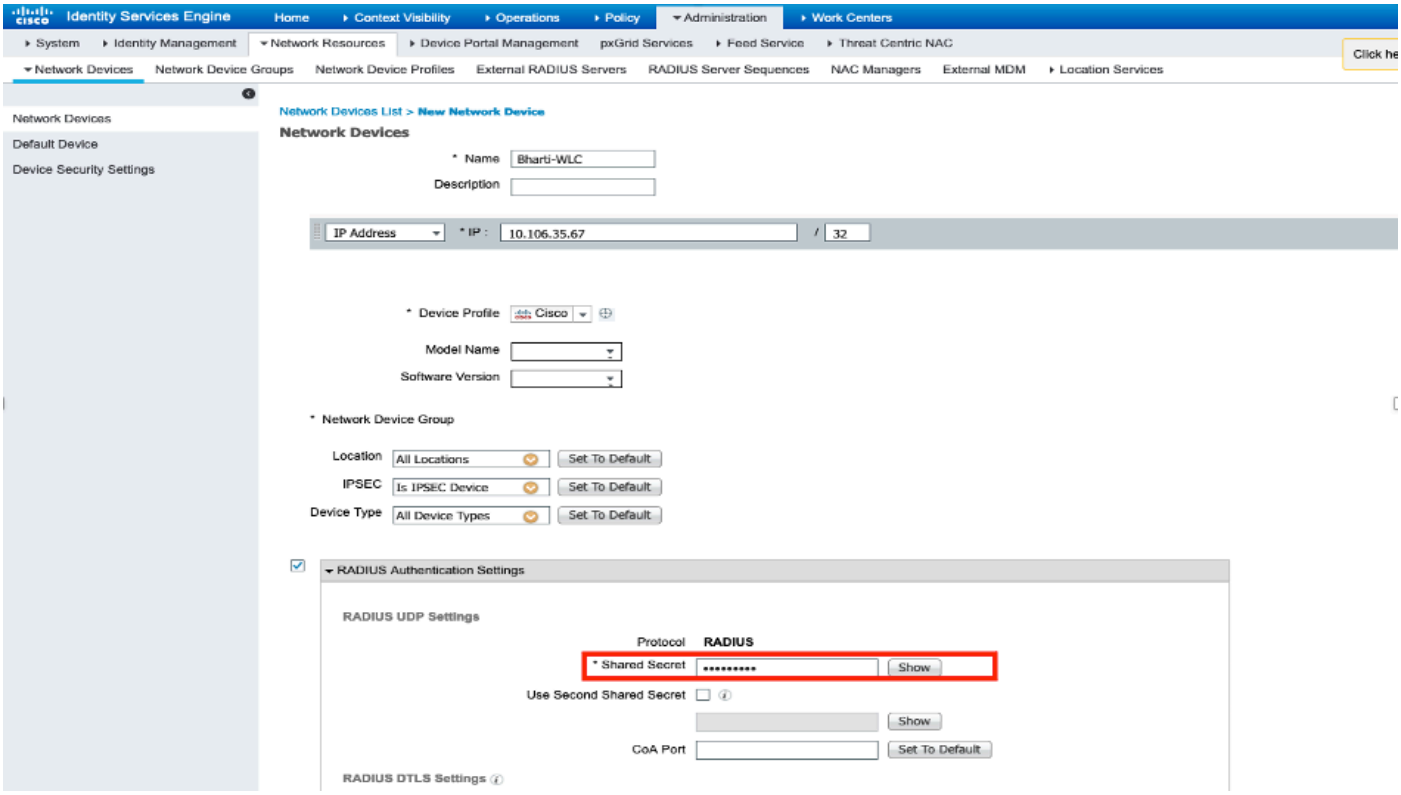


ISE의 WLC 설정

1단계. ISE 콘솔을 열고 이미지에 표시된 대로 **Administration > Network Resources > Network Devices > Add**로 이동합니다.

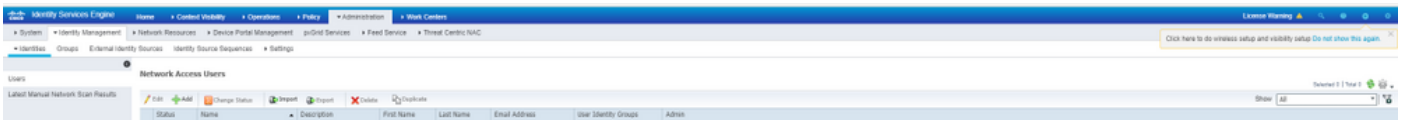


2단계. 이미지에 표시된 대로 값을 입력합니다.

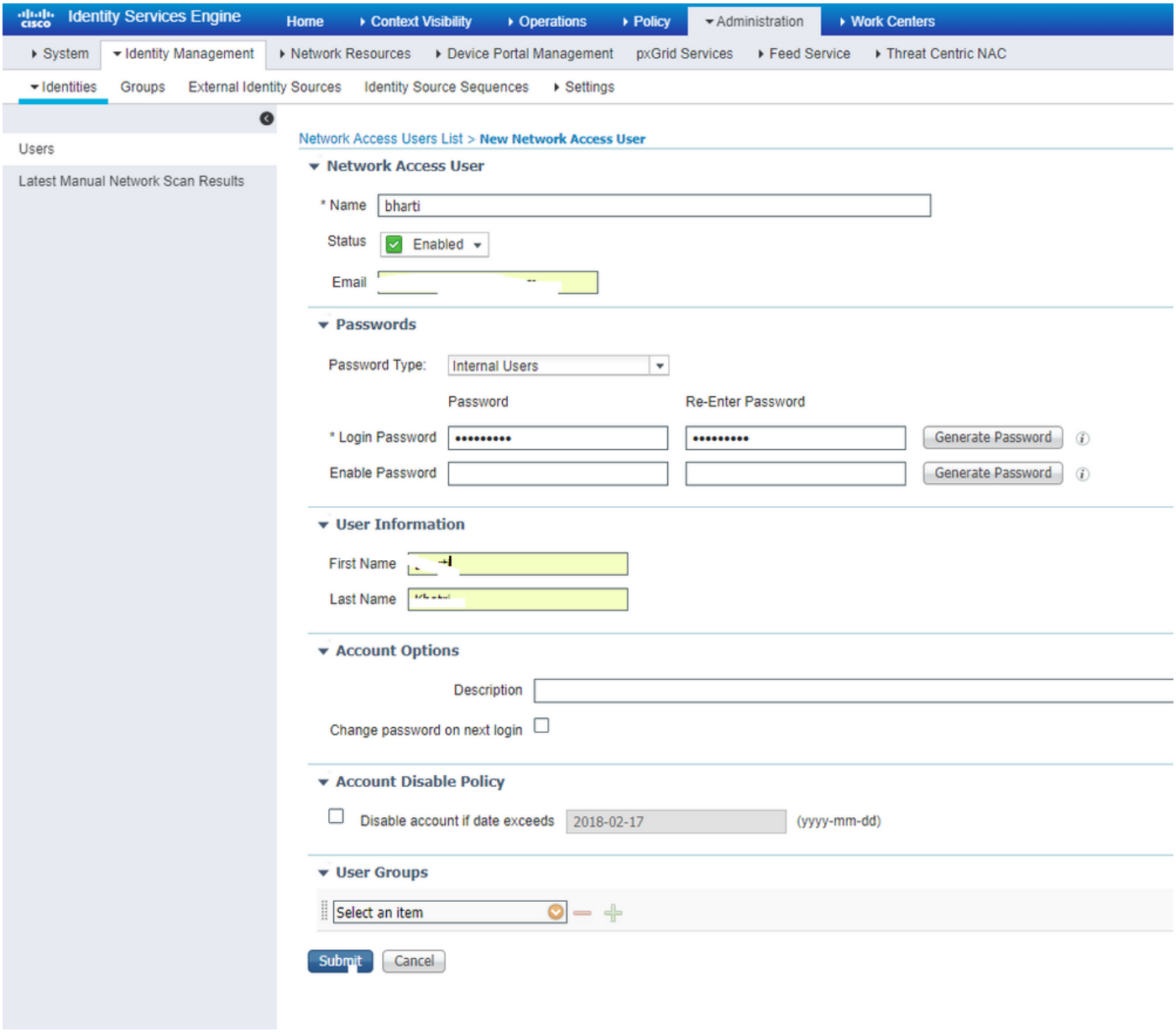


ISE에서 새 사용자 생성

1단계. 이미지에 표시된 것과 같이 Administration(관리) > Identity Management(ID 관리) > ID > Users(사용자) > Add(추가)로 이동합니다.



2단계. 이미지에 표시된 정보를 입력합니다.

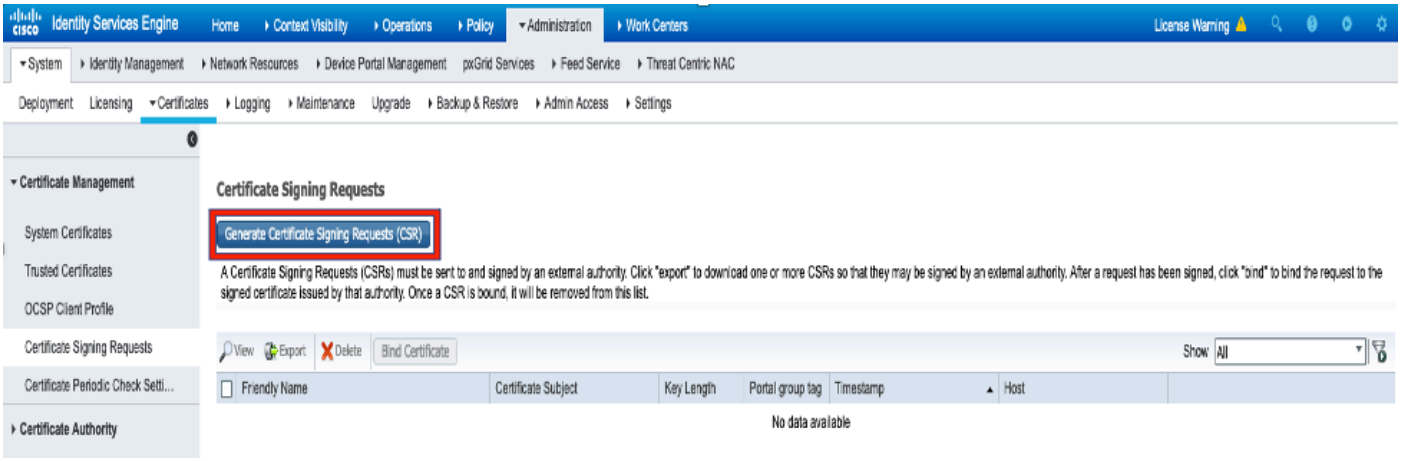


ISE의 인증서 신뢰

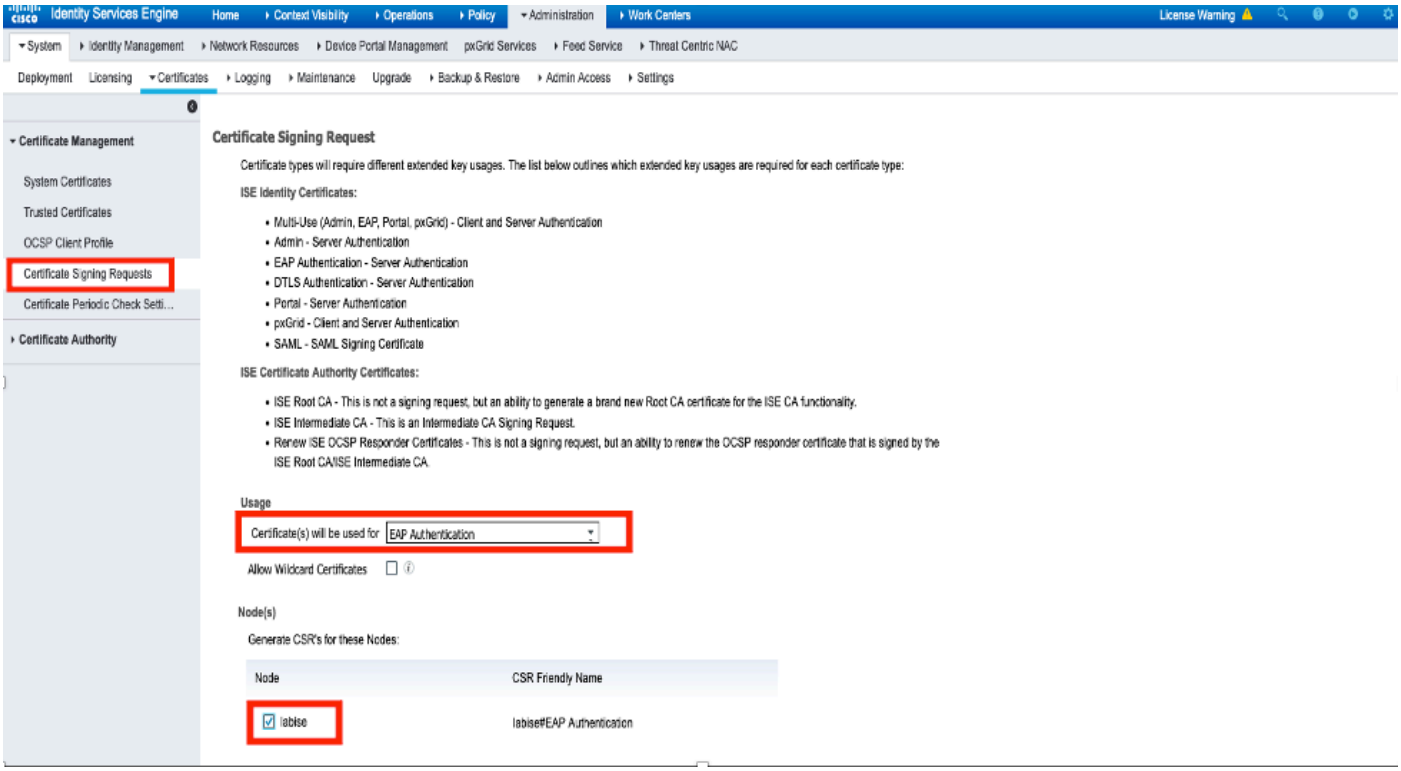
1단계. Administration(관리) > **System(시스템) > Certificates(인증서) > Certificate Management(인증서 관리) > Trusted certificates(신뢰할 수 있는 인증서)로 이동합니다**.

인증서를 ISE로 가져오려면 Import(가져오기)를 클릭합니다. ISE에서 WLC를 추가하고 사용자를 생성하면 EAP-TLS에서 가장 중요한 부분인 ISE의 인증서를 신뢰해야 합니다. 이를 위해 CSR을 생성해야 합니다.

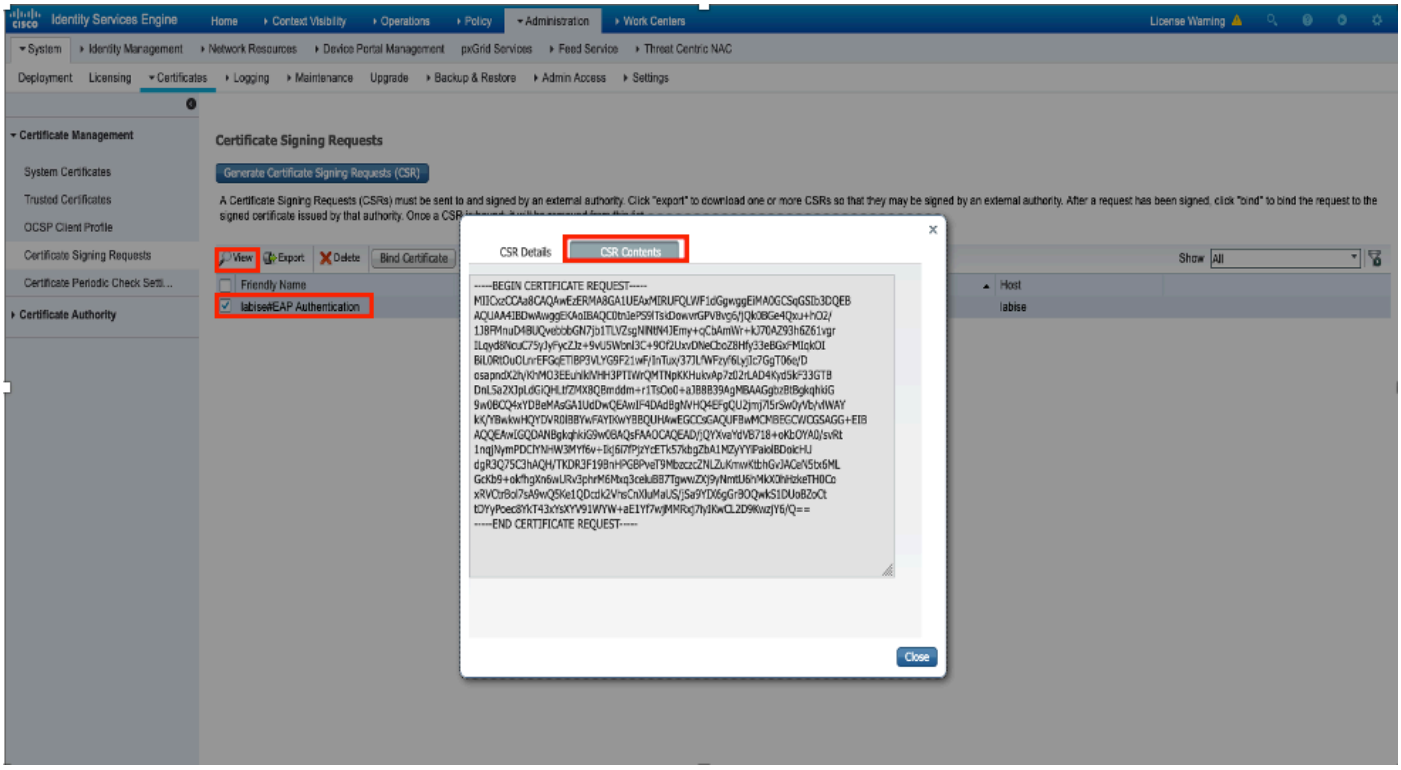
2단계. 이미지에 표시된 대로 **Administration(관리) > Certificates(인증서) > Certificate Signing Requests(인증서 서명 요청) > Generate Certificate Signing Requests (CSR)(CSR(인증서 서명 요청 생성)**로 이동합니다.



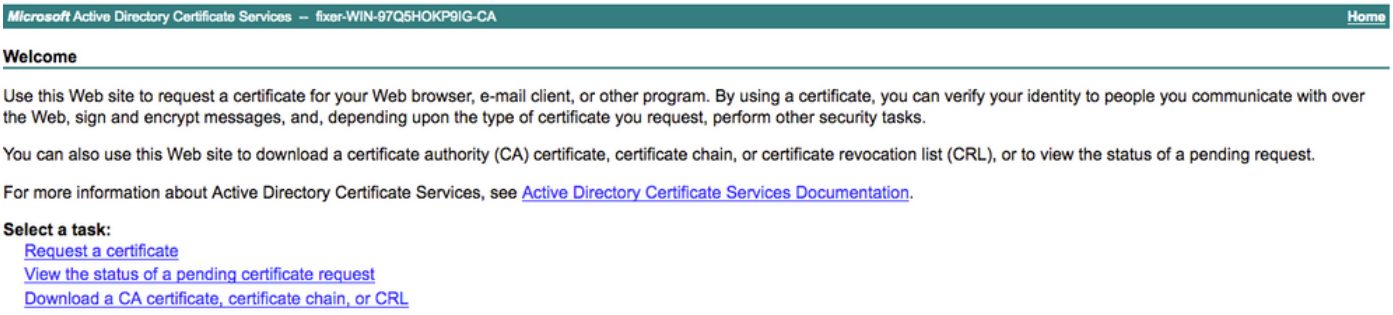
3단계. CSR을 생성하려면 Usage(**사용**)로 이동하고 **Certificate(s) is used for** drop(인증서**(s) is used for** 드롭다운 옵션**에서 이미지**에 표시된 대로 EAP Authentication(EAP **인증**)**을** 선택합니다.



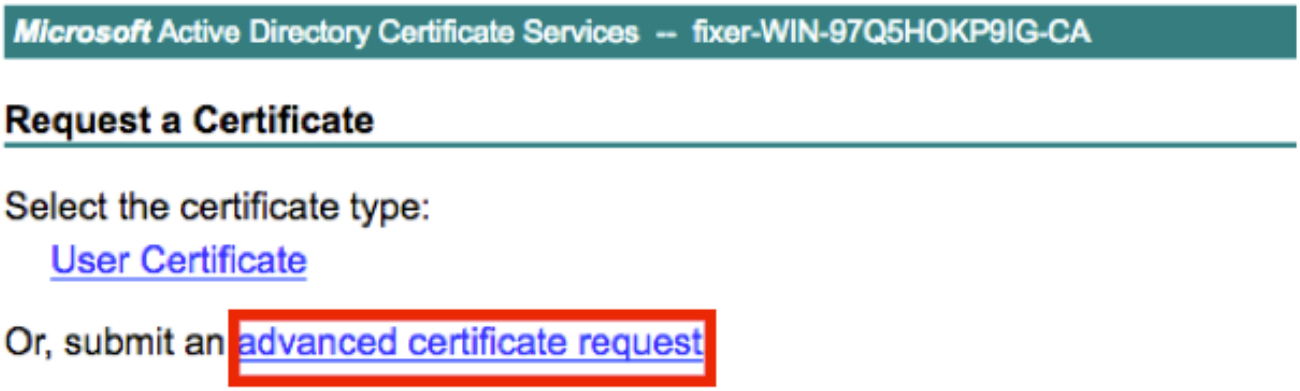
4단계. ISE에서 생성된 CSR을 볼 수 있습니다. 이미지에 표시된 대로 **View**(보기)를 클릭합니다.



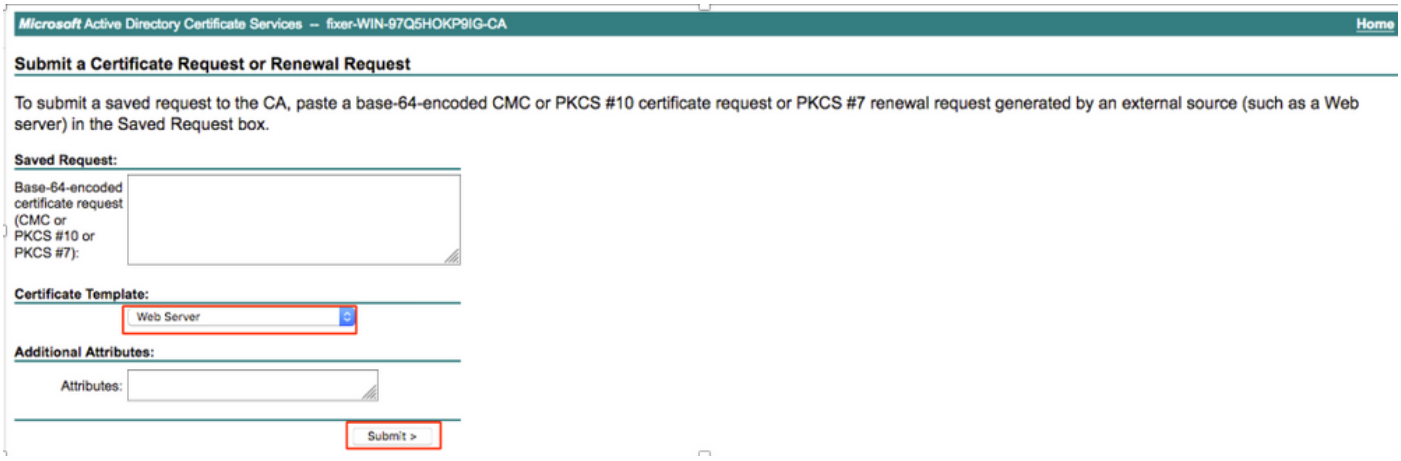
5단계. CSR이 생성되면 이미지에 표시된 대로 CA 서버를 찾아 **Request a certificate(인증서 요청)**를 클릭합니다.



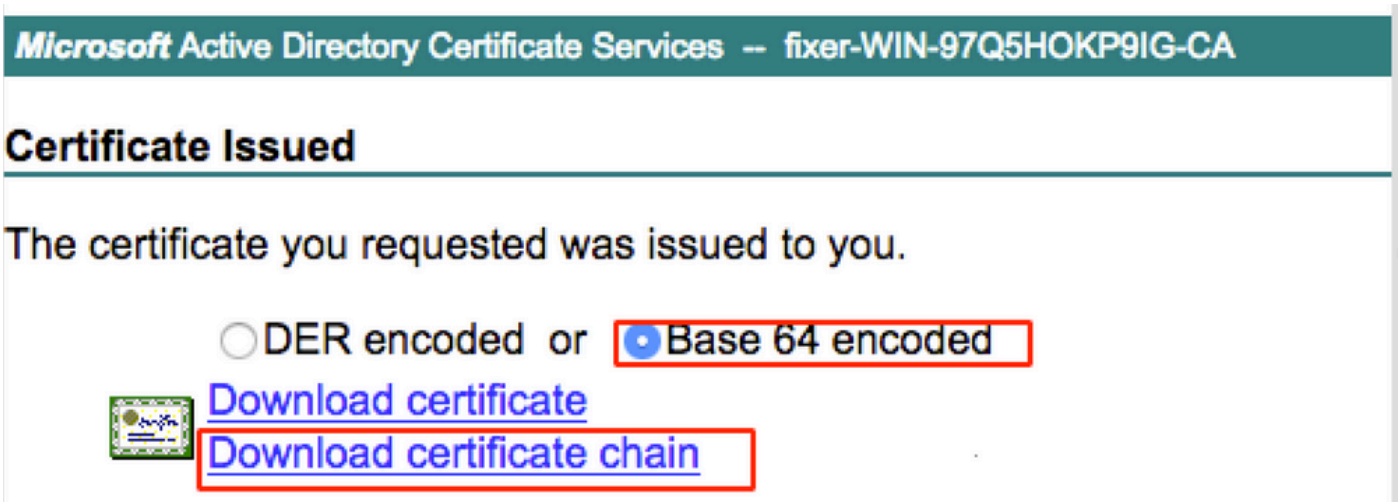
6단계. 인증서를 요청하면 이미지에 표시된 대로 **사용자 인증서** 및 **고급 인증서 요청**에 대한 옵션을 얻고 **고급 인증서 요청**을 클릭합니다.



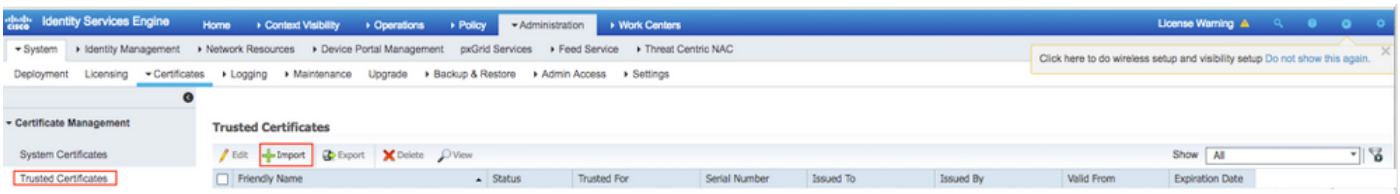
7단계. **Base-64 인코딩 인증서 요청**에서 생성된 **CSR을 붙여넣습니다**. **인증서** 템플릿에서 드롭다운 옵션에서 **웹** 서버를 선택하고 이미지에 표시된 대로 **Submit**(제출)을 클릭합니다.

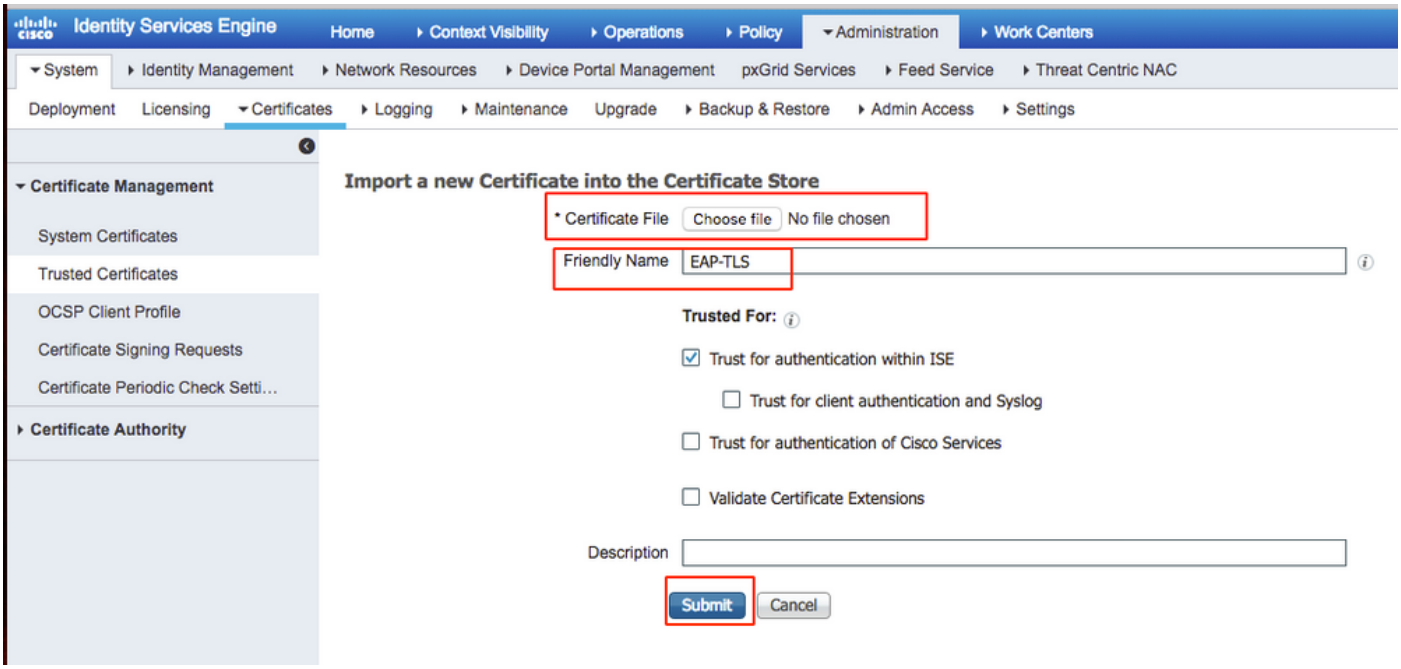


8단계. Submit(제출)을 클릭하면 인증서 유형을 선택하고 **Base-64 encoded(Base-64 인코딩)**를 선택한 다음 그림과 같이 **Download certificate chain(인증서 체인 다운로드)**을 클릭하는 옵션이 제공됩니다.

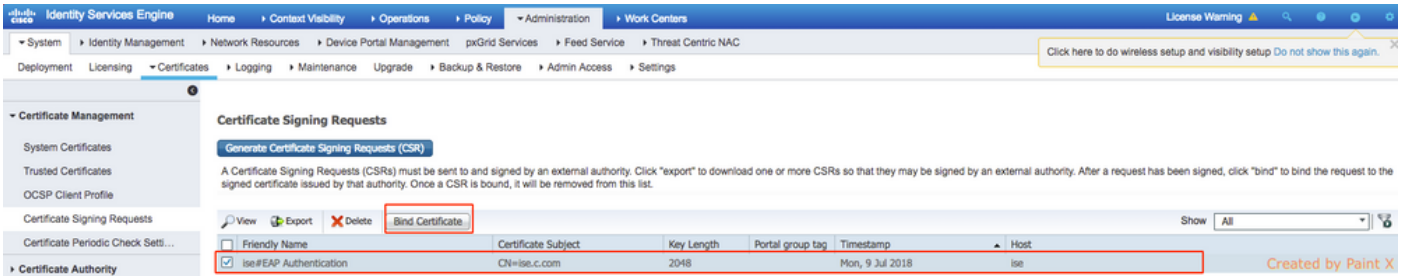


9단계. ISE 서버에 대한 인증서 다운로드가 완료되었습니다. 인증서를 추출할 수 있으며, 인증서에는 두 개의 인증서, 하나의 루트 인증서 및 다른 중간 인증서가 포함됩니다. 이미지에 표시된 대로 Administration(관리) > Certificates(인증서) **> Trusted certificates(신뢰할 수 있는 인증서) > Import(가져오기)**에서 루트 인증서를 가져올 수 있습니다.

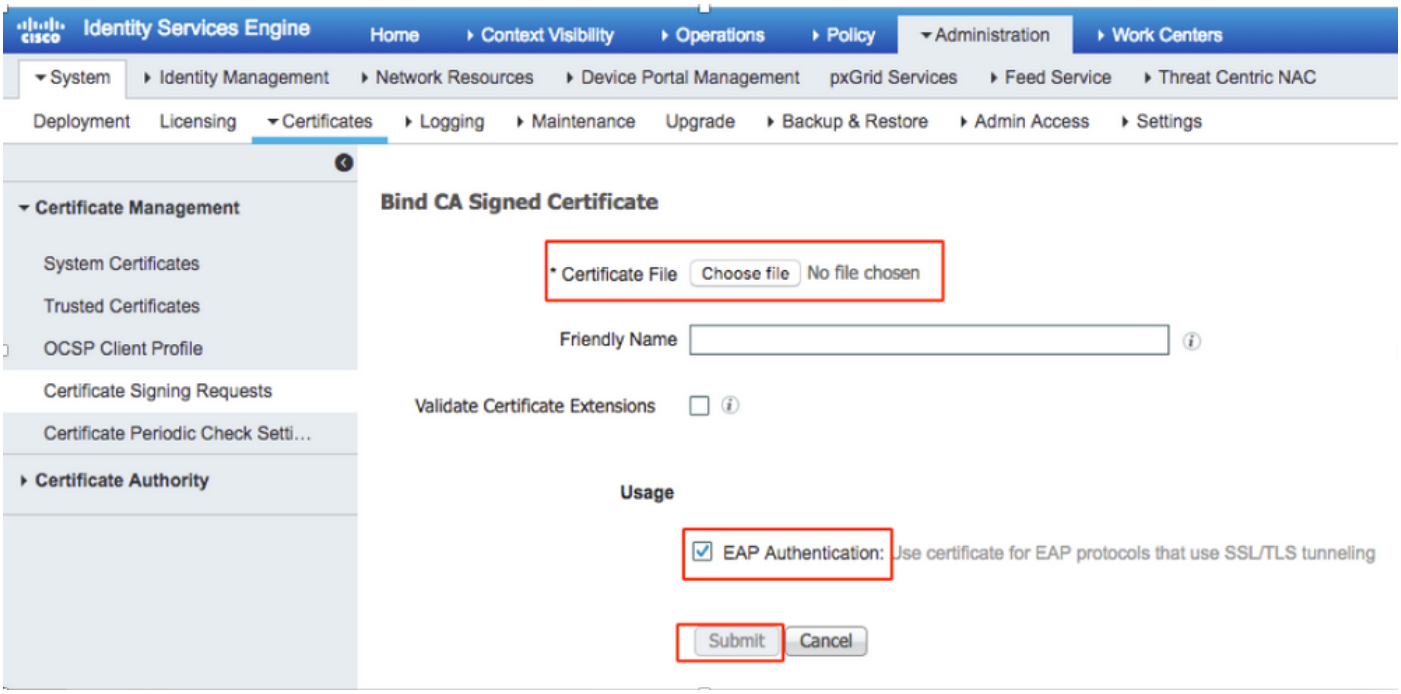




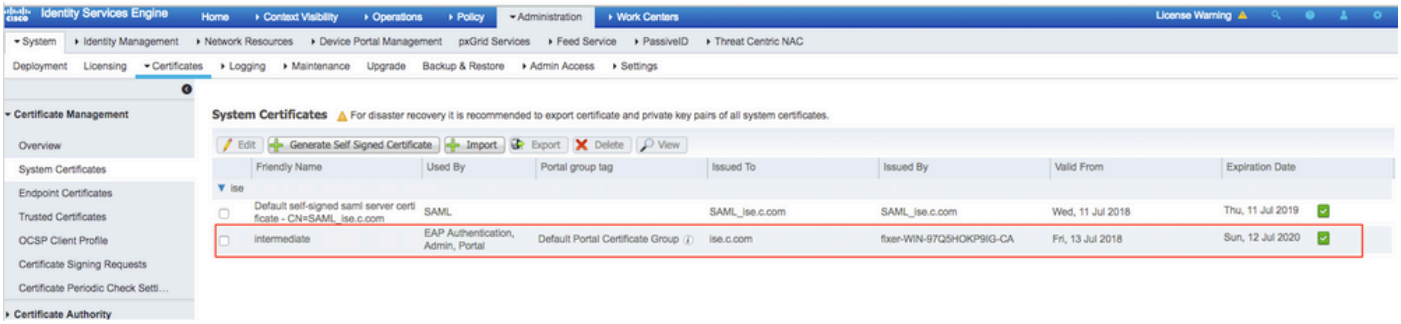
10단계. Submit(제출)을 클릭하면 인증서가 신뢰할 수 있는 인증서 목록에 추가됩니다. 또한 중간 인증서가 필요한 이유는 그림과 같이 CSR과 바인딩하기 위해서입니다.



11단계. Bind certificate(**인증서 바인딩**)를 클릭하면 데스크톱에 저장된 인증서 파일을 선택할 수 있습니다. 중간 인증서를 찾아 이미지에 표시된 대로 **Submit**(제출)을 클릭합니다.



12단계. 인증서를 보려면 이미지에 표시된 대로 **Administration > Certificates > System** Certificates로 이동합니다.



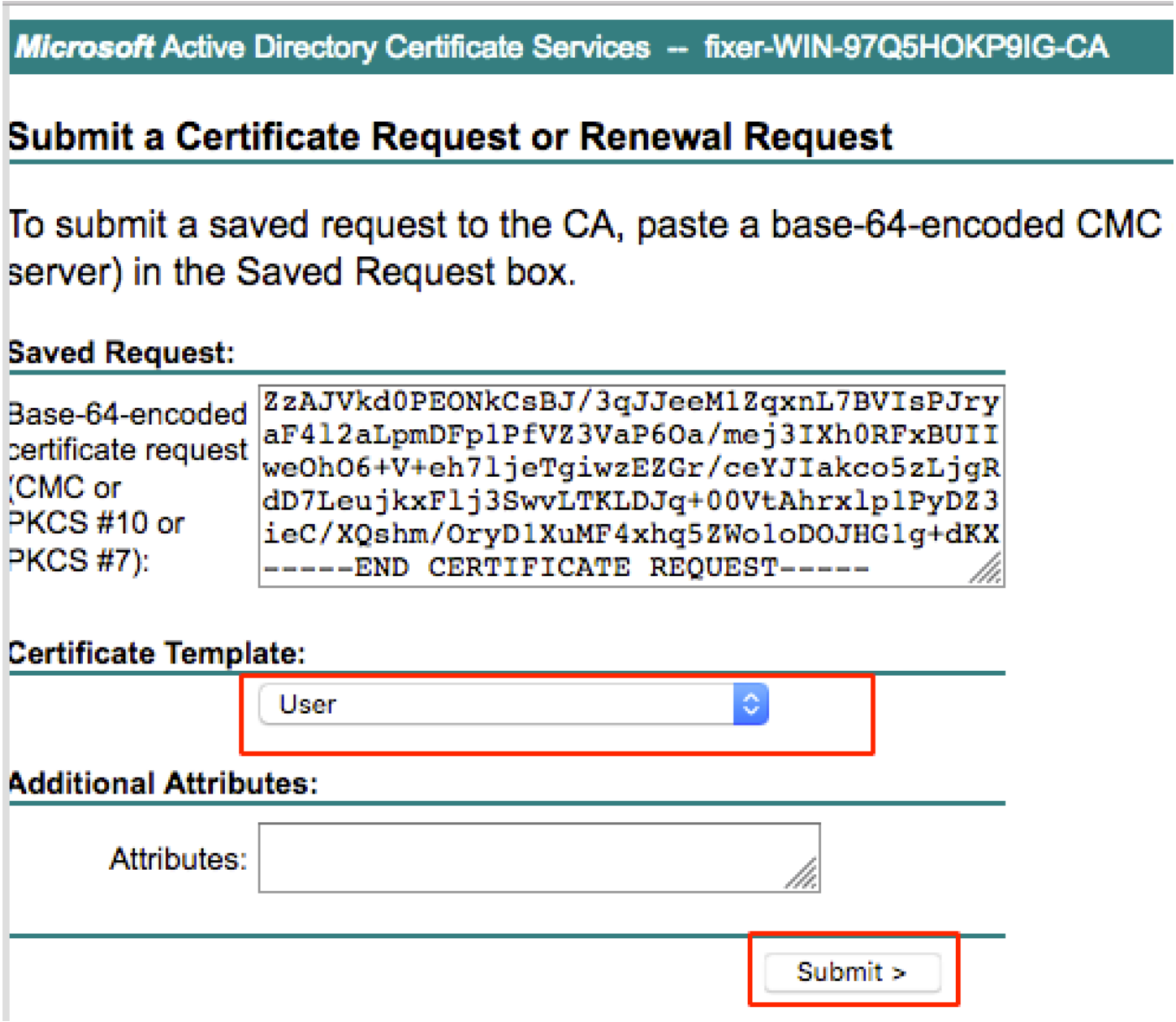
EAP-TLS용 클라이언트

클라이언트 컴퓨터에 사용자 인증서 다운로드(Windows 데스크톱)

1단계. EAP-TLS를 통해 무선 사용자를 인증하려면 클라이언트 인증서를 생성해야 합니다. 서버에 액세스할 수 있도록 Windows 컴퓨터를 네트워크에 연결합니다. 웹 브라우저를 열고 다음 주소를 입력합니다. https://sever ip addr/certsrv—

2단계. CA는 ISE에 대해 인증서를 다운로드한 것과 동일해야 합니다.

이 경우 서버용 인증서를 다운로드하는 데 사용한 것과 동일한 CA 서버를 찾아야 합니다. 동일한 CA에서 이전에 수행한 것처럼 **Request a certificate(인증서 요청)**를 클릭합니다. 그러나 이번에는 이미지에 표시된 것처럼 Certificate Template(인증서 템플릿)으로 **User(사용자)**를 선택해야 합니다
.



3단계. 그런 다음 서버에 대해 이전에 수행한 **인증서 체인** 다운로드를 클릭합니다.

인증서를 가져오면 다음 단계에 따라 Windows 노트북 컴퓨터에서 인증서를 가져옵니다.

4단계. 인증서를 가져오려면 MMC(Microsoft Management Console)에서 액세스해야 합니다.

1. MMC를 열려면 **시작 > 실행 > MMC로 이동합니다**.
2. File(파일) **> Add/Remove Snap In(스냅인 추가/제거)으로 이동합니다.**
3. Certificates(**인증서**)를 두 **번 클릭합니다**.
4. **컴퓨터 계정을 선택합니다**.
5. 로컬 **컴퓨터 > 마침** 선택
6. 스냅인 **창**을 종료하려면 확인을 클릭합니다.
7. **Certificates(인증서) > Personal(개인) > Certificates(인증서)** 옆에 있는 **[+]를** 클릭합니다.
8. Certificates(**인증서**)를 마우스 오른쪽 버튼으로 클릭하고 **All Tasks(모든 작업) >** Import(가져오기)**를** 선택합니다.
9. **Next(다음)**를 클릭합니다.
10. Browse(찾아보기)**를 클릭합니다**.
11. 가져올 **.cer, .crt 또는** .pfx를 선택합니다.
12. 열기를 **클릭합니다**.

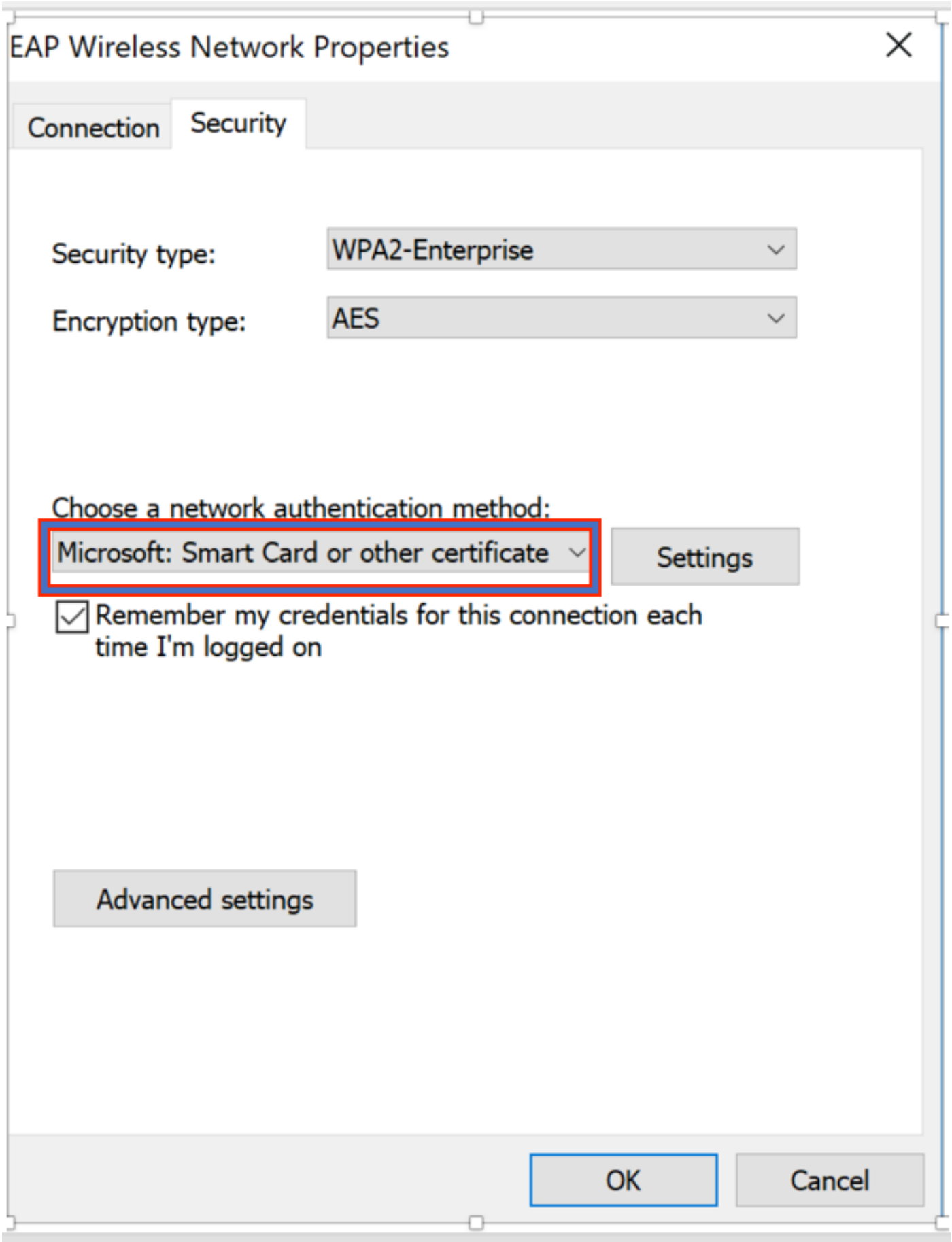
13. **Next(다음)**를 클릭합니다.
14. 인증서**의 유형에 따라 자동으로 인증서 저장소를 선택합니다**.
15. Finish(**마침) 및 OK(확인)를 클릭합니다.**

인증서 가져오기가 완료되면 EAP-TLS에 대한 무선 클라이언트(이 예에서는 windows 데스크톱)를 구성해야 합니다.

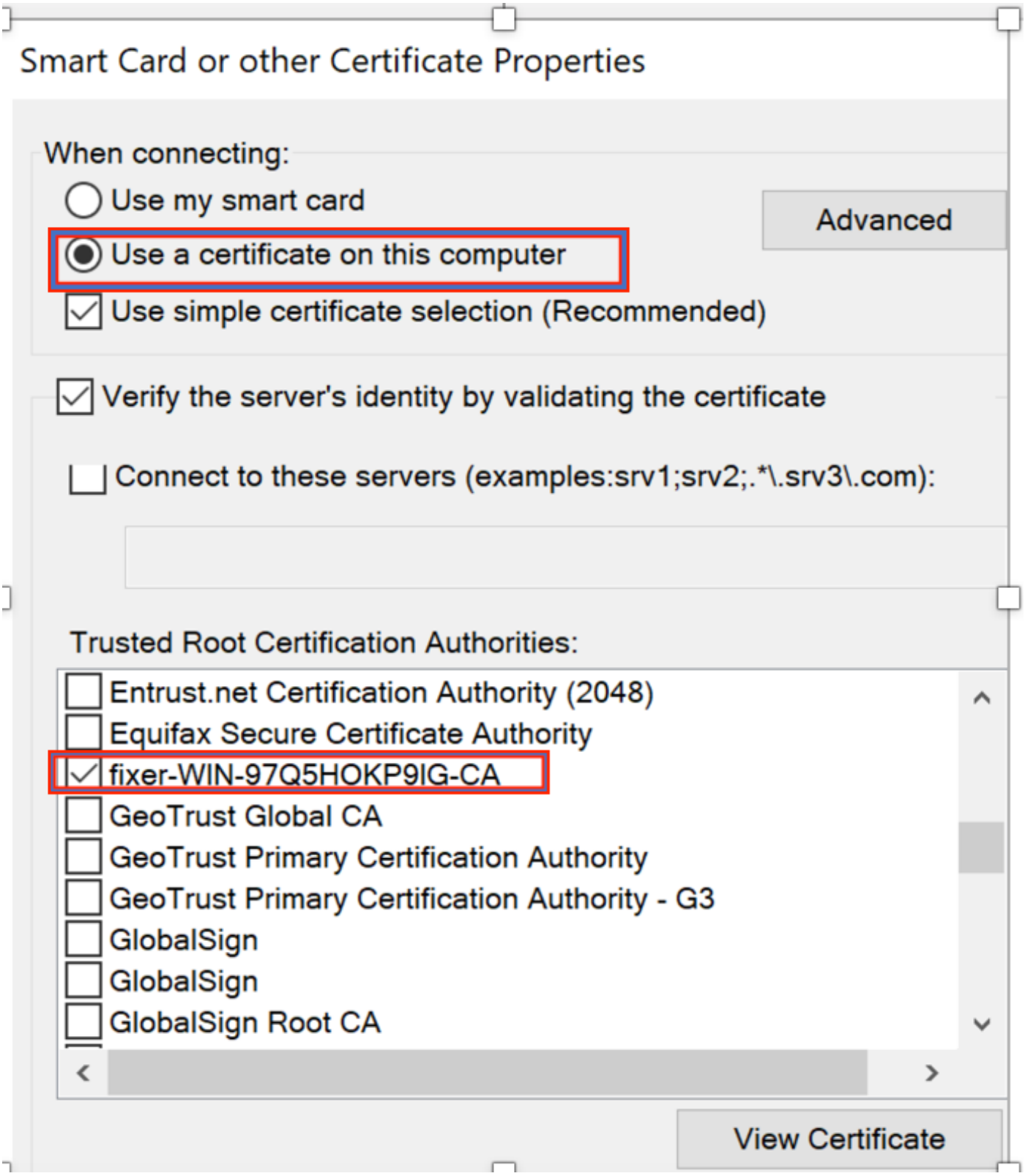
EAP-TLS용 무선 프로파일

1단계. 이전에 PEAP(Protected Extensible Authentication Protocol)에 대해 생성한 무선 프로파일을 변경하여 EAP-TLS를 대신 사용합니다. EAP **무선 프로파일을 클릭합니다**.

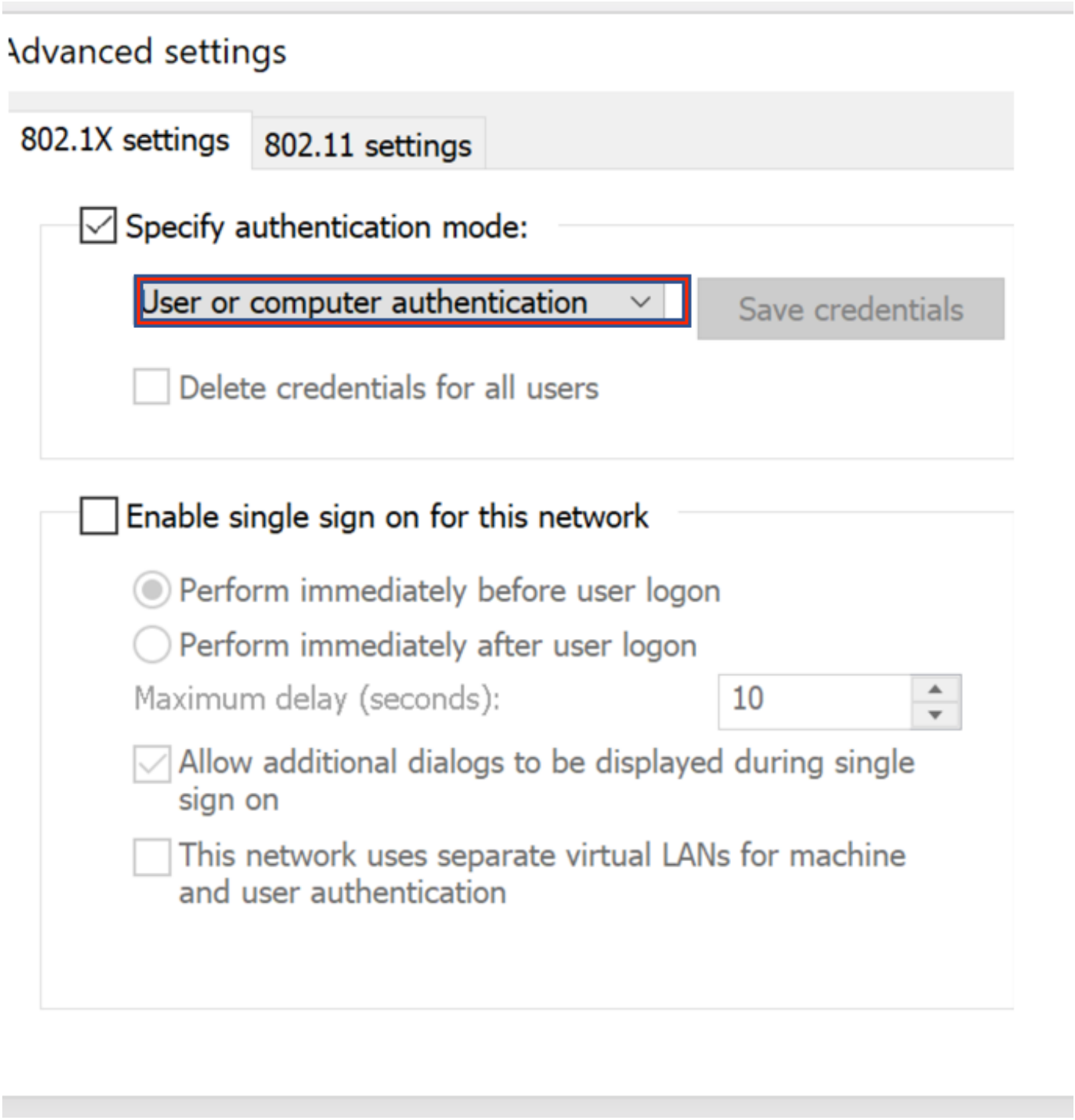
2단계. **Microsoft 선택: 스마트 카드 또는 기타 인증서**를 선택하고 이미지에 표시된 **OK**(확인)를 클릭합니다.



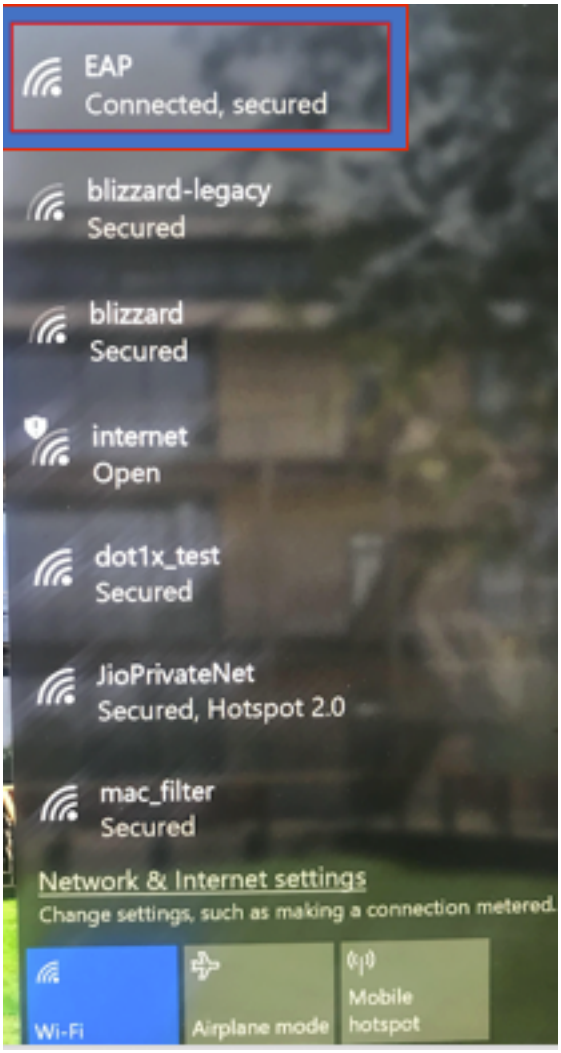
3단계. **설정**을 클릭하고 이미지에 표시된 대로 CA 서버에서 발급된 루트 인증서를 선택합니다.



4단계. **Advanced Settings(고급 설정)**를 클릭하고 이미지에 표시된 802.1x 설정 탭에서 **User or computer authentication(사용자 또는 컴퓨터 인증)**을 선택합니다.



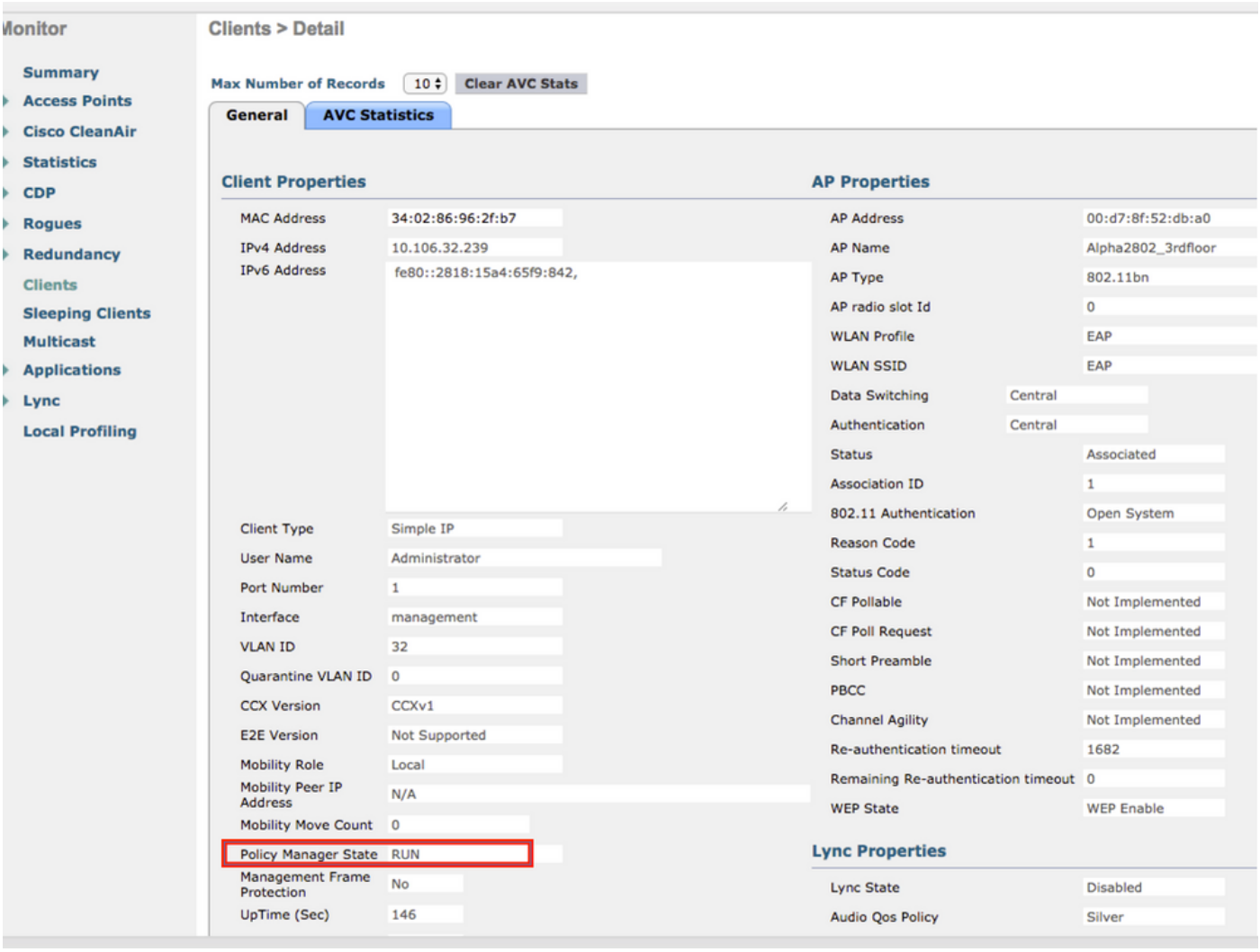
5단계. 이제 무선 네트워크에 다시 연결해 보십시오. 올바른 프로파일(이 예에서는 EAP)을 선택하고 **연결합니다**. 이미지에 표시된 대로 무선 네트워크에 연결됩니다.



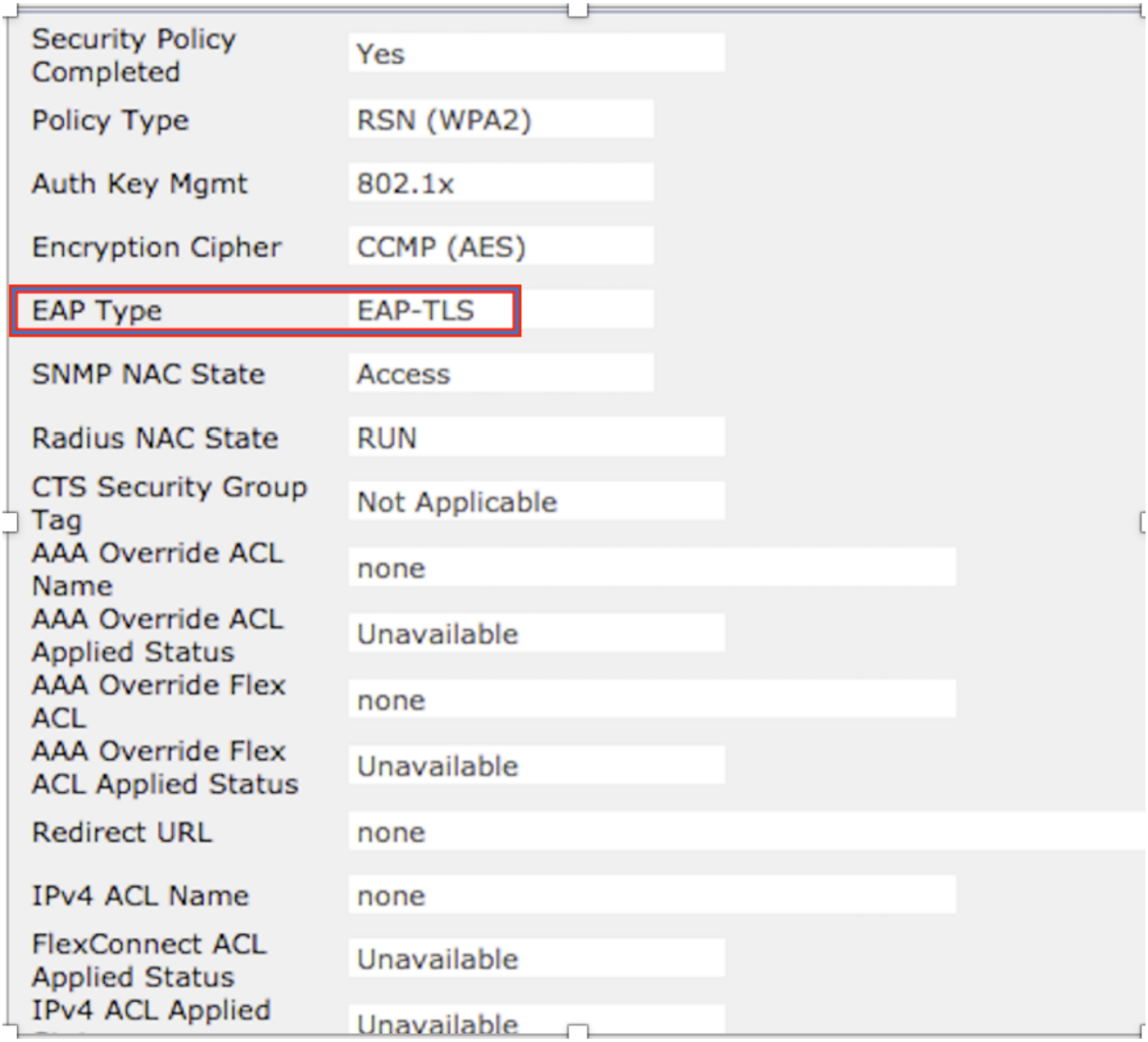
다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

1단계. 클라이언트 정책 관리자 상태는 RUN으로 **표시되어야 합니다**. 이는 클라이언트가 인증을 완료하고 IP 주소를 얻었으며 이미지에 표시된 트래픽을 전달할 준비가 되었음을 의미합니다.



2단계. 또한 이미지에 표시된 대로 클라이언트 세부사항 페이지에서 WLC의 올바른 EAP 방법을 확인합니다.

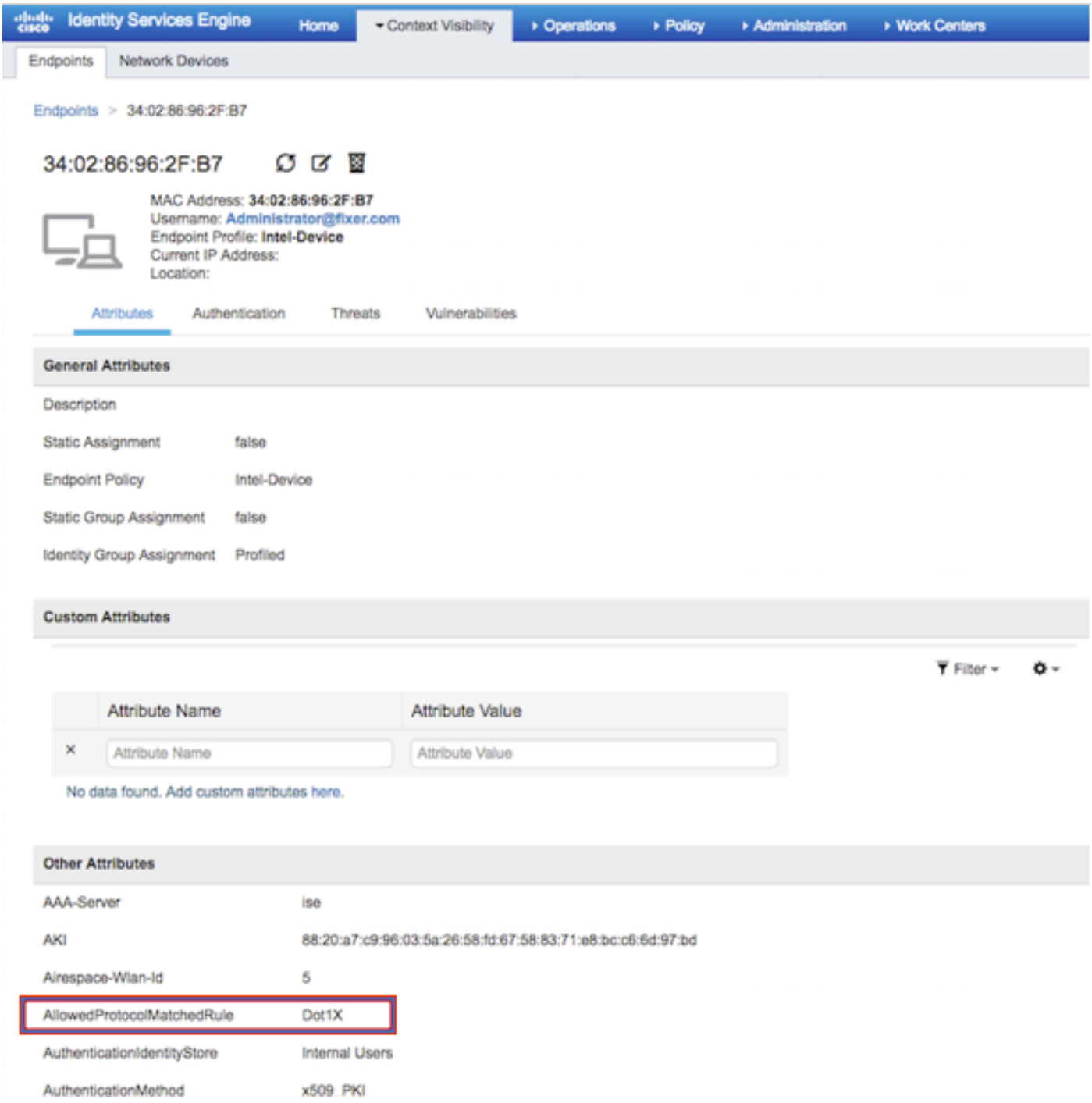


3단계. 다음은 컨트롤러의 CLI에서 클라이언트 세부사항입니다(출력 잘림).

```
(Cisco Controller-Standby) >show client detail 34:02:86:96:2f:b7
Client MAC Address.............................. 34:02:86:96:2f:b7
Client Username ................................ Administrator
AP MAC Address.................................. 00:d7:8f:52:db:a0
AP Name......................................... Alpha2802_3rdfloor
AP radio slot Id................................ 0
Client State.................................... Associated
Wireless LAN Id................................. 5
Wireless LAN Network Name (SSID)................ EAP
Wireless LAN Profile Name....................... EAP
Hotspot (802.11u)............................... Not Supported
BSSID........................................... 00:d7:8f:52:db:a4
Connected For .................................. 48 secs
Channel......................................... 1
IP Address...................................... 10.106.32.239
Gateway Address................................. 10.106.32.1
Netmask......................................... 255.255.255.0
Policy Manager State............................ RUN
Policy Type..................................... WPA2
Authentication Key Management................... 802.1x
```

```
Encryption Cipher.............................. CCMP-128 (AES)
Protected Management Frame ..................... No
Management Frame Protection..................... No
EAP Type....................................... EAP-TLS
```

4단계. ISE에서 이미지에 표시된 대로 **Context Visibility(컨텍스트 가시성) > End Points(엔드포인트) > Attributes(특성)**로 이동합니다.



BYODRegistration	Unknown
Called-Station-ID	00-d7-8f-52-db-a0:EAP
Calling-Station-ID	34-02-86-96-2f-b7
Days to Expiry	363
DestinationIPAddress	10.106.32.31
DestinationPort	1812
DetailedInfo	Invalid username or password specified
Device IP Address	10.106.32.223
Device Port	32775
Device Type	Device Type#All Device Types
DeviceRegistrationStatus	NotRegistered
ElapsedDays	7
EnableFlag	Enabled
EndPointMACAddress	34-02-86-96-2F-B7
EndPointPolicy	Intel-Device
EndPointProfilerServer	ise.c.com
EndPointSource	RADIUS Probe
Extended Key Usage - Name	130, 132, 138
Extended Key Usage - OID	1.3.6.1.5.5.7.3.2, 1.3.6.1.5.5.7.3.4, 1.3.6.1.4.1.311.1
FailureReason	-
IdentityGroup	Profiled
InactiveDays	5
IsThirdPartyDeviceFlow	false
Issuer	CN=fixer-WIN-97Q5HOKP9IG-CA\,DC=fixer\,DC=c
Issuer - Common Name	fixer-WIN-97Q5HOKP9IG-CA
Issuer - Domain Component	fixer, com

Location	Location#All Locations
MACAddress	34:02:86:96:2F:B7
MatchedPolicy	Intel-Device
MessageCode	5200
NAS-IP-Address	10.106.32.223
NAS-Identifier	HA_Pri
NAS-Port	1
NAS-Port-Type	Wireless - IEEE 802.11
Network Device Profile	Cisco
NetworkDeviceGroups	Location#All Locations, Device Type#All Device Types
NetworkDeviceName	HA_Pri
NetworkDeviceProfileId	403ea8fc-7a27-41c3-80bb-27964031a08d
NetworkDeviceProfileName	Cisco
OUI	Intel Corporate
OpenSSLErrorMessage	SSL alert: code=0x230=560 \; source=local \; type=fatal \; message="Unknown CA - error unable to get issuer certificate locally"
OpenSSLErrorStack	140160653813504:error:140890B2:SSL routines:SSL3_GET_CLIENT_CERTIFICATE:no certificate returned:s3_srvr.c:3370:
PolicyVersion	0
PostureApplicable	Yes
PostureAssessmentStatus	NotApplicable
RadiusFlowType	Wireless802_1x
RadiusPacketType	AccessRequest
SSID	00-d7-8f-52-db-a0:EAP
SelectedAccessService	Default Network Access
SelectedAuthenticationIdentityStores	EAPTLS
SelectedAuthorizationProfiles	PermitAccess
Serial Number	10 29 41 78 00 00 00 00 00 11

문제 해결

현재 이 구성에 대한 문제 해결에 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.