

ISE를 사용하여 EAP-TLS 인증 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[구성](#)

[서버 및 클라이언트 인증서 가져오기](#)

[1단계. ISE에서 CSR\(Certificate Signing Request\) 생성](#)

[2단계. CA 인증서를 ISE로 가져오기](#)

[3단계. 엔드포인트용 클라이언트 인증서 가져오기](#)

[네트워크 디바이스](#)

[4단계. ISE에서 네트워크 액세스 디바이스 추가](#)

[정책 요소](#)

[5단계. 외부 ID 소스 사용](#)

[6단계. 인증서 인증 프로파일 생성](#)

[7단계. ID 소스 시퀀스에 추가](#)

[8단계. 허용되는 프로토콜 서비스 정의](#)

[9단계. 권한 부여 프로파일 생성](#)

[보안 정책](#)

[10단계. 정책 집합 생성](#)

[11단계. 인증 정책 생성](#)

[12단계. 권한 부여 정책 생성](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[일반적인 문제 및 트러블슈팅 기법](#)

[관련 정보](#)

소개

이 문서에서는 Cisco ISE의 확장 가능 한 인증 프로토콜 전송 계층 보안 인증을 도입 하기 위한 초기 구성에 대해 설명 합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- EAP 및 RADIUS 통신 흐름에 대한 기본 이해.
- 통신 흐름의 관점에서 인증서 기반 인증 방법을 사용한 기본 RADIUS 인증 지식

- Dot1x와 MAB(MAC Authentication Bypass) 간의 차이점 이해
- PKI(Public Key Infrastructure)에 대한 기본 이해
- CA(Certificate Authority)에서 서명된 인증서를 가져오고 엔드포인트에서 인증서를 관리하는 방법에 대한 숙지입니다.
- 네트워크 장치(유선 또는 무선)에서 RADIUS(Authentication, Authorization, and Accounting) 관련 설정의 구성
- RADIUS/802.1x와 함께 사용할 신청자(엔드포인트)의 컨피그레이션

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- ISE(Identity Services Engine) 릴리스 3.x
- CA - 인증서를 발급합니다(Enterprise CA, 서드파티/공용 CA 또는 [Certificate Provisioning Portal](#) 사용).
- Active Directory(외부 ID 소스) - Windows Server, 여기서 [ISE와 호환됩니다](#).
- NAD(Network Access Device) - 스위치(유선) 또는 802.1x/AAA용으로 구성된 WLC([무선 LAN 컨트롤러](#))일 수 있습니다.
- 엔드포인트 - RADIUS/802.1x를 통해 네트워크 액세스를 위해 인증될 수 있는 (사용자) ID 및 신청자 컨피그레이션에 발급된 인증서: 사용자 인증. 머신 인증서를 가져올 수 있지만 이 예에서는 사용되지 않습니다.

 참고: 이 가이드에서는 ISE 릴리스 3.1을 사용하므로 모든 문서 참조는 이 버전을 기반으로 합니다. 그러나 Cisco ISE의 이전 릴리스에서 동일/유사 컨피그레이션이 가능하고 완벽하게 지원됩니다.

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

주요 초점은 유선 또는 무선을 통해 연결된 IP-Phone/엔드포인트와의 인증(이에 제한되지 않음)과 같은 여러 시나리오에 적용할 수 있는 ISE 컨피그레이션에 있습니다.

이 가이드의 범위에서는 ISE(RADIUS) 인증 흐름의 다음 단계를 이해하는 것이 중요합니다.

- 인증 - 네트워크 액세스를 요청하는 최종 ID(머신, 사용자 등)를 식별하고 검증합니다.
- Authorization(권한 부여) - 네트워크에서 최종 ID에 부여할 수 있는 권한/액세스를 결정합니다.
- 계정 관리 - 네트워크 액세스가 달성된 후 최종 ID의 네트워크 활동을 보고하고 추적합니다.

구성

서버 및 클라이언트 인증서 가져오기

1단계. ISE에서 CSR(Certificate Signing Request) 생성

첫 번째 단계는 ISE에서 CSR(Certificate Signing Request)을 생성하여 CA(서버)에 제출하여 ISE에 발급된 서명된 인증서를 시스템 인증서로 취득하는 것입니다. 이 인증서는 EAP-TLS(Extensible Authentication Protocol-Transport Layer Security Authentication) 인증 중에 ISE에서 서버 인증서로 표시할 수 있습니다. 이는 ISE UI에서 수행됩니다. 탐색 Administration > System: Certificates > Certificate Management > Certificate Signing Requests. 아래 Certificate Signing Requests, 클릭 Generate Certificate Signing Requests (CSR) 이 그림에 표시된 것과 같습니다.

Certificate Signing Requests



인증서 유형에는 서로 다른 확장 키 사용이 필요합니다. 이 목록에는 각 인증서 유형에 필요한 확장 키 사용이 요약되어 있습니다.

ISE ID 인증서

- 다중 사용(관리자, EAP, 포털, pxGrid) - 클라이언트 및 서버 인증
- 관리자 - 서버 인증
- EAP 인증 - 서버 인증
- DTLS(Datagram Transport Layer Security) 인증 - 서버 인증
- 포털 - 서버 인증
- pxGrid - 클라이언트 및 서버 인증
- SAML(Security Assertion Markup Language) - SAML 서명 인증서
- ISE 메시징 서비스 - 서명 인증서 생성 또는 새로운 메시징 인증서 생성

기본적으로 ISE 메시징 서비스 시스템 인증서는 구축, 노드 등록 및 기타 노드 간 통신에서 각 ISE 노드 간의 데이터 복제를 위한 것이며 ISE 내부 CA(Certificate Authority) 서버(ISE의 내부)에 의해 표시되고 발급됩니다. 이 인증서로 완료할 작업은 필요하지 않습니다.

관리 시스템 인증서는 관리 UI(관리)에 연결된 API가 사용되는 경우 및 일부 노드 간 통신과 같은 각 ISE 노드를 식별하는 데 사용됩니다. 처음으로 ISE를 설정하려면 관리 시스템 인증서를 배치합니다. 이 작업은 이 컨피그레이션 가이드와 직접적인 관련이 없습니다.

EAP-TLS(인증서 기반 인증)를 통해 IEEE 802.1x를 수행하려면 EAP 인증 시스템 인증서에 대한 작업을 수행합니다. EAP-TLS 흐름 중에 엔드포인트/클라이언트에 제공되는 서버 인증서로 사용됩니다. 그 결과 TLS 터널 내부에서 보호됩니다. 시작하려면 CSR을 만들어 EAP 인증 시스템 인증서를 만든 다음 서명을 위해 조직의 CA 서버(또는 공용 CA 제공자)를 관리하는 직원에게 제공합니다. 최종 결과는 CSR에 바인딩하고 이 단계를 통해 ISE에 연결하는 CA 서명 인증서입니다.

CSR(Certificate Signing Request) 양식에서 다음 옵션을 선택하여 CSR을 완료하고 내용을 가져옵니다

니다.

- Certificate Usage(인증서 사용) - 이 컨피그레이션 예에서는 다음을 선택합니다. **EAP Authentication**.
- 인증서에서 와일드카드 문을 사용 하려는 경우 *.example.com 그런 다음 **Allow Wildcard Certificate** 확인란. 가장 좋은 위치는 환경에 존재할 수 있는 다양한 유형의 엔드포인트 운영 체제 간에 모든 사용과 호환성을 위해 SAN(주체 대체 이름) 인증서 필드입니다.
- 인증서에 와일드카드 문을 배치하도록 선택하지 않은 경우 CA 서명 인증서를 (서명 후) 연결할 ISE 노드를 선택합니다.

 참고: 와일드카드 명령문을 포함하는 CA 서명 인증서를 CSR 내의 여러 노드에 바인딩하면 인증서가 ISE 구축의 각 ISE 노드(또는 선택한 노드)에 배포되고 서비스가 다시 시작될 수 있습니다. 그러나 서비스 재시작은 한 번에 하나의 노드로 자동으로 제한됩니다. 이를 통해 서비스 재시작 모니터링 `show application status ise` ISE CLI 명령입니다.

다음으로, Subject(제목)를 정의하려면 양식을 작성해야 합니다. 여기에는 CN(Common Name), OU(Organizational Unit), O(Organization), L(City), ST(State) 및 C(Country) 인증서 필드가 포함됩니다. \$FQDN\$ 변수는 각 ISE 노드와 연결된 관리 정규화된 도메인 이름(호스트 이름 + 도메인 이름)을 나타내는 값입니다.

- 이 Subject Alternative Name (SAN) 또한 필수 및 원하는 정보를 포함하여 신뢰를 설정하기 위해 필드를 작성해야 합니다. 인증서가 서명된 후, 이 인증서와 연결된 ISE 노드의 FQDN을 가리키는 DNS 엔트리를 정의해야 합니다.
- 마지막으로, CA 서버의 기능 및 적절한 보안 사례를 염두에 두고 적절한 Key Type(키 유형), Key Length(키 길이) 및 Digest to Sign With(서명할 다이제스트)를 정의해야 합니다. 기본값은 각각 RSA, 4096비트 및 SHA-384입니다. 사용 가능한 선택 사항 및 호환성이 ISE Admin UI 내의 이 페이지에 표시됩니다.

와일드카드 문을 사용하지 않고 완료된 CSR 양식의 예입니다. 환경에 특정한 실제 값을 사용해야 합니다.

Usage

Certificate(s) will be used for **EAP Authentication** 

Allow Wildcard Certificates 

Node(s)

Generate CSR's for these Nodes:

Node	CSR Friendly Name
<input checked="" type="checkbox"/> ise	ise#EAP Authentication
<input checked="" type="checkbox"/> ise2	ise2#EAP Authentication
<input checked="" type="checkbox"/> ise3	ise3#EAP Authentication

Subject

Common Name (CN)
\$FQDN\$ 

Organizational Unit (OU)



Organization (O)
Example Company 

City (L)
San Jose

State (ST)
California

Country (C)
US

3. 전체 CA 체인의 일부로서 모든 인증서를 ISE의 신뢰할 수 있는 인증서 저장소로 가져오면 ISE GUI로 돌아가서 **Administration > System: Certificates > Certificate Management: Certificate Signing Requests**. 서명된 인증서에 해당하는 Friendly Name(친숙한 이름) 아래에서 CSR 항목을 찾고 인증서의 확인란을 클릭한 다음 **Bind Certificate**.

Certificate Signing Requests

Generate Certificate Signing Requests (CSR)

A Certificate Signing Requests (CSRs) must be sent to and signed by an external authority. Click "export" to download one or more CSRs so that they may be signed by an external authority. After a request has been signed, click "bind" to bind the request to the signed certificate issued by that authority. Once a CSR is bound, it will be removed from this list.

2)

1)

<input type="checkbox"/>	Friendly Name	Certificate Subject	Key Length	Portal gro...	Timestamp	Host
<input checked="" type="checkbox"/>	ise#EAP Authentication	CN=ise.example.com ,O=E...	4096		Tue, 10 May 2022	ise
<input type="checkbox"/>	ise2#EAP Authentication	CN=ise2.example.com ,O=...	4096		Tue, 10 May 2022	ise2
<input type="checkbox"/>	ise3#EAP Authentication	CN=ise3.example.com ,O=...	4096		Tue, 10 May 2022	ise3

CSR에 인증서 바인딩

 **참고:** 단일 CA 서명 인증서를 한 번에 하나씩 각 CSR에 바인딩해야 합니다. 구축의 다른 ISE 노드에 대해 생성된 나머지 CSR에 대해 반복합니다.

다음 페이지에서 **Browse** 서명된 인증서 파일을 선택하고 원하는 식별 이름을 정의한 다음 **Certificate Usage(s)**를 선택합니다. 변경 사항을 저장하려면 **Submit(제출)**을 클릭합니다.

Bind CA Signed Certificate

* Certificate File EXAMPLE_ISE.cer

Friendly Name ⓘ

Validate Certificate Extensions ⓘ

Usage

EAP Authentication: Use certificate for EAP protocols that use SSL/TLS tunneling

CSR에 바인딩할 인증서 선택

4. 이때 서명된 인증서가 ISE GUI로 이동됩니다. 탐색 **Administration > System: Certificates > Certificate Management: System Certificates** CSR이 생성된 동일한 노드에 할당합니다. 다른 노드 및/또는 다른 인증서 사용에 대해 동일한 프로세스를 반복합니다.

3단계. 엔드포인트용 클라이언트 인증서 가져오기

EAP-TLS와 함께 사용할 클라이언트 인증서를 생성하려면 엔드포인트에서 유사한 프로세스를 탐색해야 합니다. 이 예에서는 ISE에서 사용자 인증을 수행하려면 사용자 계정에 서명되고 발급된 클라이언트 인증서가 필요합니다. Active Directory 환경에서 엔드포인트에 대한 클라이언트 인증서를

얻는 방법의 예는 Understand and configure EAP-TLS using WLC and ISE(WLC 및 ISE를 사용하여 EAP-TLS 이해 및 구성) > Configure(구성) > [Client for EAP-TLS에서 찾을 수 있습니다.](#)

여러 유형의 엔드포인트 및 운영 체제로 인해 프로세스가 다소 다를 수 있으므로 추가 예가 제공되지 않습니다. 그러나 전반적인 프로세스는 개념상 동일합니다. 인증서에 포함할 모든 관련 정보가 있고 CA가 서명한 CSR을 생성합니다. 이는 환경의 내부 서버든, 이러한 유형의 서비스를 제공하는 공용/서드파티 기업이든 상관없습니다.

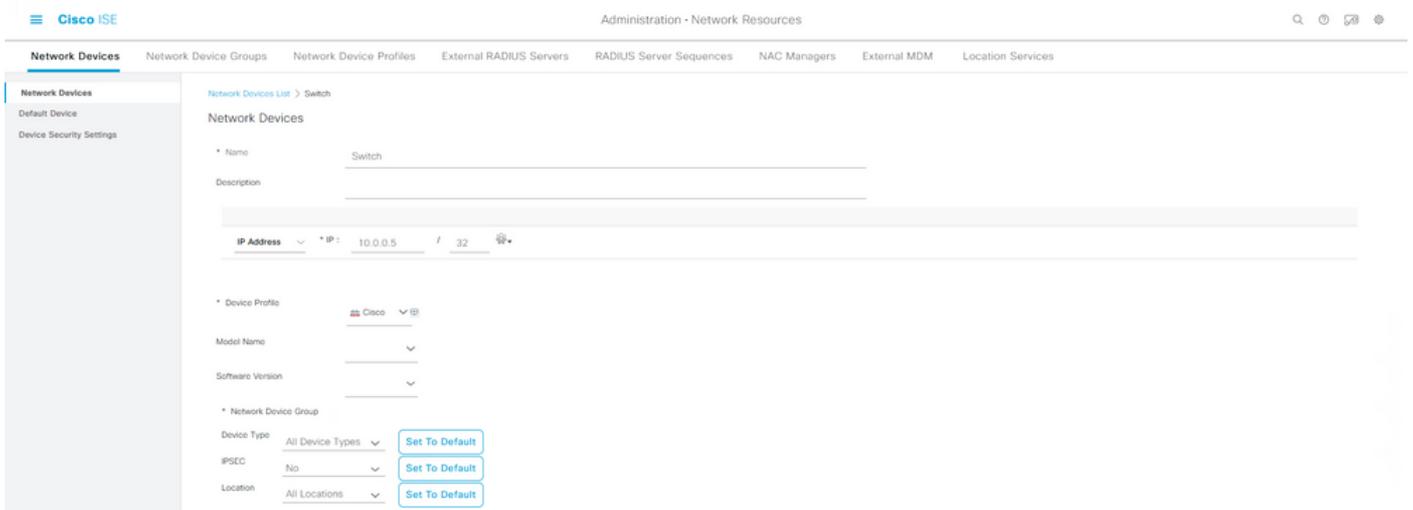
또한 CN(Common Name) 및 SAN(Subject Alternative Name) 인증서 필드에는 인증 흐름 동안 사용할 ID가 포함되어 있습니다. 또한 ID의 관점에서 서플리컨트가 EAP-TLS에 대해 구성되는 방법을 결정합니다. 시스템 및/또는 사용자 인증, 시스템 인증 또는 사용자 인증. 이 예에서는 이 문서의 나머지 부분에서는 사용자 인증만 사용합니다.

네트워크 디바이스

4단계. ISE에서 네트워크 액세스 디바이스 추가

엔드포인트가 연결된 NAD(Network Access Device)도 RADIUS/TACACS+(Device Admin) 통신이 발생할 수 있도록 ISE에서 구성됩니다. NAD와 ISE 사이에는 공유 비밀/비밀번호가 신뢰 목적으로 사용됩니다.

ISE GUI를 통해 NAD를 추가하려면 **Administration > Network Resources: Network Devices > Network Devices** 을 클릭하고 **Add**이 그림에 나와 있습니다.



네트워크 디바이스 컨피그레이션 예

ISE 프로파일링과 함께 사용할 경우, ISE PSN(Policy Service Node)이 ISE에 대한 엔드포인트 인증과 관련된 SNMP 쿼리를 통해 NAD에 연결할 수 있도록 SNMPv2c 또는 SNMPv3(더 보안)를 구성하여 사용되는 엔드포인트 유형에 대한 정확한 결정을 내리기 위해 특성을 수집합니다. 다음 예에서는 이전 예와 동일한 페이지에서 SNMP(v2c)를 설정하는 방법을 보여 줍니다.



SNMP Settings

* SNMP Version

* SNMP RO Community

SNMP Username

Security Level

Auth Protocol

Auth Password

Privacy Protocol

Privacy Password

* Polling Interval seconds (Valid Range 600 to 86400 or zero)

Link Trap Query

MAC Trap Query

* Originating Policy Services Node

SNMPv2c 컨피그레이션 예

자세한 내용은 Cisco Identity Services Engine 관리자 가이드, 릴리스 3.1 > 장: 보안 액세스 > [Cisco ISE에서 네트워크 장치 정의](#)에서 찾을 수 있습니다.

이 때 아직 하지 않은 경우 Cisco ISE를 식별 하고 인증 하려면 NAD에서 모든 AAA 관련 설정을 구성 해야 합니다.

정책 요소

이러한 설정은 인증 정책 또는 권한 부여 정책에 바인딩되는 구성 요소입니다. 이 가이드에서는 주로 각 정책 요소를 구축한 다음 인증 정책 또는 권한 부여 정책에 매핑합니다. 인증/권한 부여 정책에 대한 바인딩이 성공적으로 완료될 때까지 정책이 적용되지 않음을 이해하는 것이 중요합니다.

5단계. 외부 ID 소스 사용

외부 ID 소스는 단순히 ISE 인증 단계 중에 사용되는 최종 ID(머신 또는 사용자) 계정이 있는 소스입니다. Active Directory는 일반적으로 Active Directory에서 컴퓨터 계정에 대한 머신 인증 및/또는 최종 사용자 계정에 대한 사용자 인증을 지원하는 데 사용됩니다. 내부 엔드포인트(내부) 소스가 컴퓨터 계정/호스트 이름을 저장하지 않으므로 머신 인증과 함께 사용할 수 없습니다.

다음은 각 ID 소스에 사용할 수 있는 ISE 및 프로토콜(인증 유형)과 함께 지원되는 ID 소스입니다.

Protocol (Authentication Type)	Internal Database	Active Directory	LDAP	RADIUS Token Server or RSA
EAP-GTC, PAP (plain text password)	Yes	Yes	Yes	Yes
MS-CHAP password hash: MSCHAPv1/v2 EAP-MSCHAPv2 (as inner method of PEAP, EAP-FAST, or EAP-TTLS) LEAP	Yes	Yes	No	No
EAP-MD5 CHAP	Yes	No	No	No
EAP-TLS PEAP-TLS (certificate retrieval) Note For TLS authentications (EAP-TLS and PEAP-TLS), identity sources are not required but can optionally be added for authorization policy conditions.	No	Yes	Yes	No

ID 저장소 기능

정책 요소에 대한 자세한 내용은 Cisco Identity Services Engine Administrator Guide, Release 3.1 > Chapter: Segmentation > Policy Sets를 [참조하십시오](#).

ISE에 Active Directory 보안 그룹 추가

ISE 정책에서 Active Directory 보안 그룹을 사용하려면 먼저 Active Directory 가입 포인트에 그룹을 추가해야 합니다. ISE GUI에서 Administration > Identity Management: Active Directory > {select AD instance name / join point} > tab: Groups > Add > Select Groups From Directory.

ISE 3.x를 Active Directory와 통합하는 데 필요한 자세한 내용과 요구 사항을 보려면 이 [문서](#)를 모두

검토하십시오. [Active Directory Integration with Cisco ISE 2.x](#).

 참고: LDAP 인스턴스에 보안 그룹을 추가하는 경우에도 동일한 작업을 수행할 수 있습니다. ISE GUI에서 **Administration > Identity Management: External Identity Sources > LDAP > LDAP instance name > tab: Groups > Add > Select Groups From Directory**.

6단계. 인증서 인증 프로파일 생성

인증서 인증 프로파일의 목적은 EAP-TLS 중에 (또한 다른 인증서 기반 인증 방법 중에) ISE에 제출된 클라이언트 인증서 (엔드 ID 인증서)에서 ID (시스템 또는 사용자) 를 찾을 수 있는 인증서 필드를 ISE에 알려 주기 위한 것입니다. 이러한 설정은 ID를 인증하기 위해 인증 정책에 바인딩됩니다. ISE GUI에서 **Administration > Identity Management: External Identity Sources > Certificate Authentication Profile** 을 클릭하고 **Add**.

Use Identity From(ID에서 사용)은 ID를 찾을 수 있는 특정 필드의 인증서 특성을 선택하는 데 사용됩니다. 선택 사항은 다음과 같습니다.

Subject - Common Name

Subject Alternative Name

Subject - Serial Number

Subject

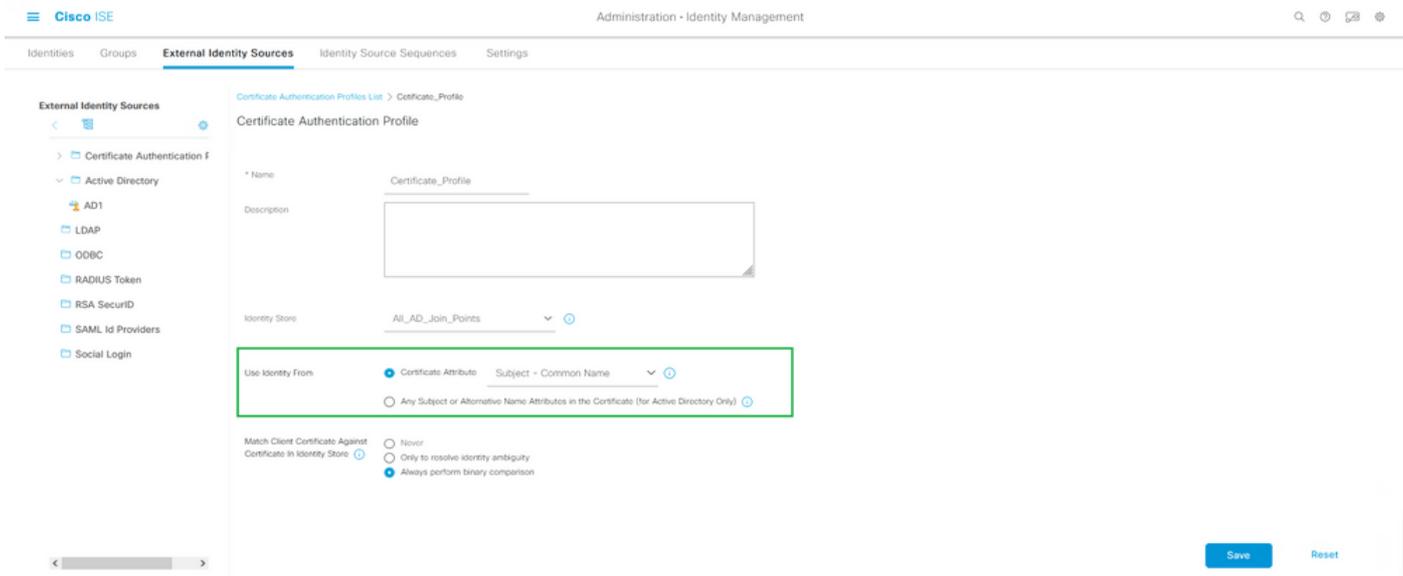
Subject Alternative Name - Other Name

Subject Alternative Name - EMail

Subject Alternative Name - DNS

ID 저장소가 Active Directory 또는 LDAP(외부 ID 소스)를 가리킬 경우, [Binary Comparison](#)이라는 기능을 사용할 수 있습니다. 이진 비교는 ISE 인증 단계에서 발생하는 Use Identity From(ID에서 사용) 선택에서 클라이언트 인증서에서 얻은 Active Directory의 ID를 조회합니다. 이진 비교 없이 ID는 클라이언트 인증서에서 간단하게 가져오며, Active Directory 외부 그룹이 조건으로 사용되거나 ISE에 대해 외부에서 수행해야 하는 다른 조건이 있을 경우 ISE 권한 부여 단계가 시작될 때까지 Active Directory에서 조회되지 않습니다. 이진 비교를 사용하려면 ID 저장소에서 최종 ID 계정을 찾을 수 있는 외부 ID 소스(Active Directory 또는 LDAP)를 선택합니다.

다음은 ID가 클라이언트 인증서의 CN(Common Name) 필드에 있고 이진 비교가 활성화된 경우(선택 사항) 컨피그레이션 예입니다.



인증서 인증 프로파일

자세한 내용은 Cisco Identity Services Engine 관리자 가이드, 릴리스 3.1 > 장: 기본 설정 > Cisco ISE CA 서비스 > 개인 장치 인증을 위해 인증서를 사용 하도록 Cisco ISE 구성 > TLS [기반 인증을 위한 인증서 인증 프로파일 만들기를](#) 참조 하십시오.

7단계. ID 소스 시퀀스에 추가

ID 소스 시퀀스는 ISE GUI에서 생성할 수 있습니다. 탐색 **Administration > Identity Management**. 아래 **Identity Source Sequences** , 클릭 **Add**.

다음 단계는 여러 Active Directory 가입 포인트를 포함하거나 내부/외부 ID 소스 조합을 원하는 대로 함께 그룹화할 수 있는 권한을 부여하는 ID 소스 시퀀스에 인증서 인증 프로파일을 추가하는 것이며, 그런 다음 아래의 인증 정책에 바인딩됩니다. Use 열.

여기에 표시된 예에서는 먼저 Active Directory에 대해 조회를 수행할 수 있도록 허용한 다음, 사용자를 찾을 수 없는 경우 다음 LDAP 서버를 조회합니다. 여러 ID 소스에 대해 항상 **Treat as if the user was not found and proceed to the next store in the sequence** 확인란이 선택되어 있습니다. 따라서 인증 요청 중에 각 ID 소스/서버를 확인합니다.

Cisco ISE Administration - Identity Management

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

Identity Source Sequences List > Identity_Sequence

Identity Source Sequence

Identity Source Sequence

* Name Identity_Sequence

Description

Certificate Based Authentication

Select Certificate Authentication Profile Certificate_Profile

Authentication Search List

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

Available	Selected
Internal Endpoints	All_AD_Join_Points
Internal Users	LDAP_Server
Guest Users	
AD1	

Advanced Search List Settings

If a selected identity store cannot be accessed for authentication

Do not access other stores in the sequence and set the "AuthenticationStatus" attribute to "ProcessError"

Treat as if the user was not found and proceed to the next store in the sequence

Save Reset

ID 소스 시퀀스

그렇지 않으면 인증서 인증 프로파일만 인증 정책에 바인딩할 수도 있습니다.

8단계. 허용되는 프로토콜 서비스 정의

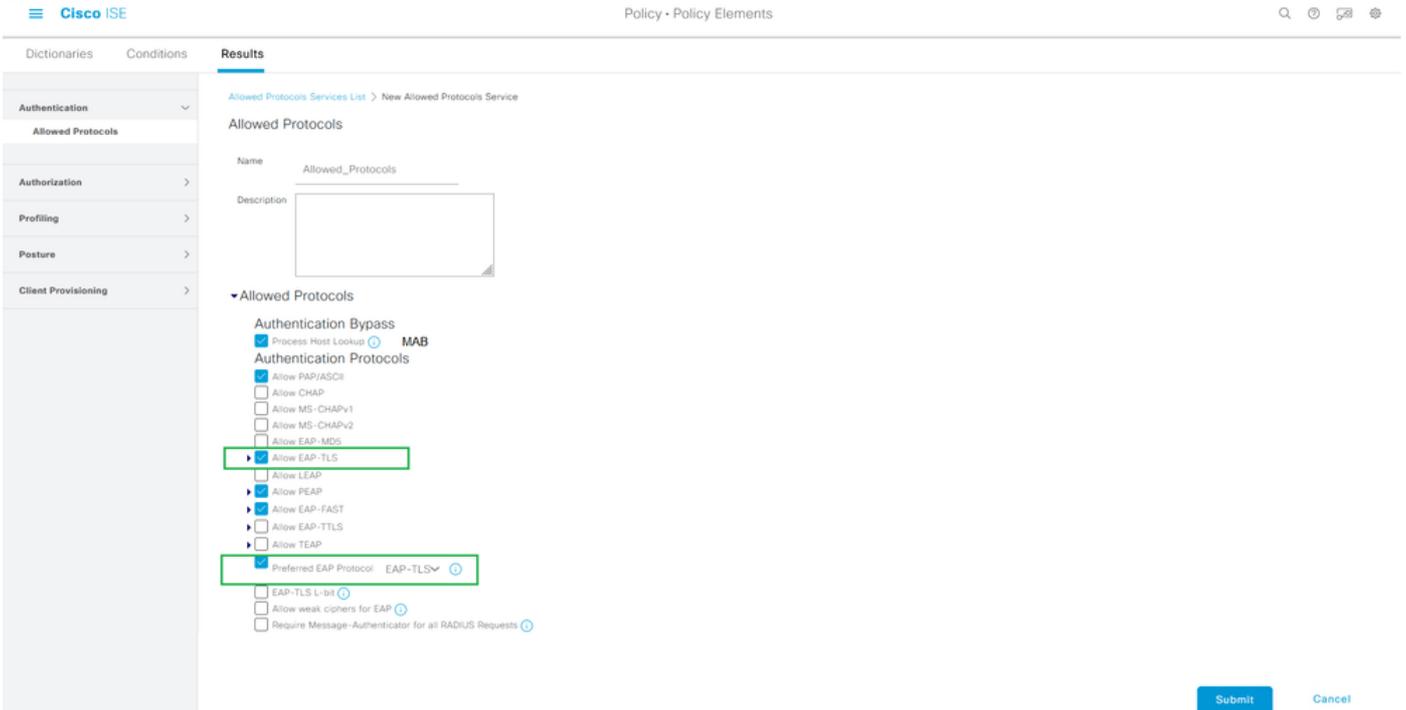
Allowed Protocols Service(허용된 프로토콜 서비스)는 RADIUS 인증 중에 ISE가 지원하는 인증 방법/프로토콜만 활성화합니다. ISE GUI에서 구성하려면 Policy(정책) > Policy Elements(정책 요소): Results(결과) > Authentication(인증) > Allowed Protocols(허용되는 프로토콜)로 이동한 다음 인증 정책에 요소로 바인딩합니다.

 참고: Authentication Bypass(인증 우회) > Process Host Lookup(프로세스 호스트 조회)은 ISE에서 활성화된 MAB와 관련이 있습니다.

이러한 설정은 (엔드포인트의) 신청자에서 지원 및 구성된 설정과 동일해야 합니다. 그렇지 않으면 인증 프로토콜이 예상대로 협상되지 않으며 RADIUS 통신이 실패할 수 있습니다. 실제 ISE 컨피그레이션에서는 ISE와 신청자가 예상대로 협상하고 인증할 수 있도록 환경에서 사용되는 모든 인증 프로토콜을 활성화하는 것이 좋습니다.

허용되는 프로토콜의 새로운 서비스 인스턴스가 생성될 때의 기본값(축소됨)입니다.

 참고: 이 컨피그레이션 예에서는 ISE와 신청자가 EAP-TLS를 통해 인증하므로 최소한 EAP-TLS를 활성화해야 합니다.



ISE가 엔드포인트 신청자에 대한 인증 요청 중에 사용할 수 있도록 허용하는 프로토콜

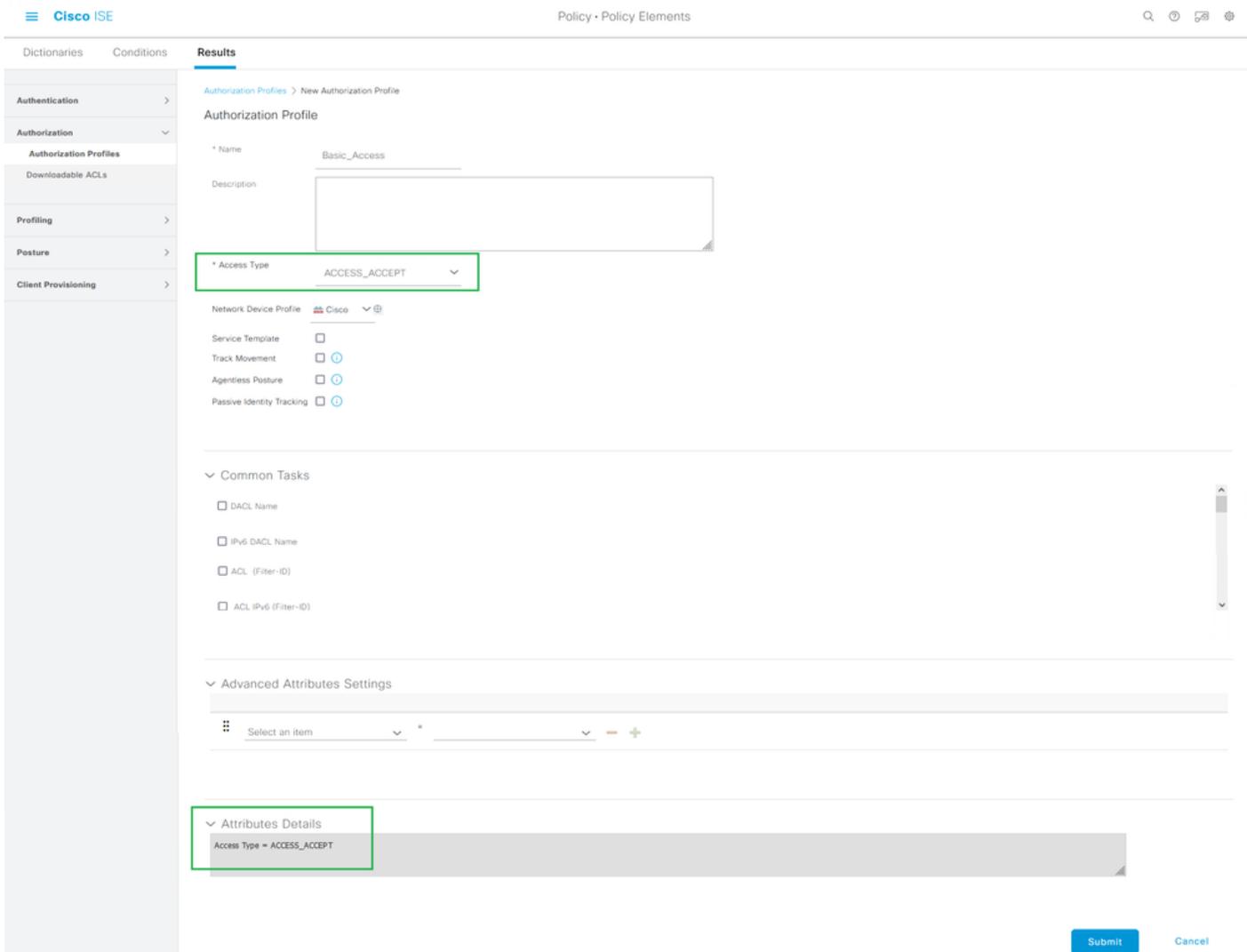
 참고: EAP-TLS 값으로 설정된 기본 EAP 프로토콜을 사용하면 ISE가 엔드포인트 IEEE 802.1x 신청자에게 제공되는 첫 번째 프로토콜로서 EAP-TLS 프로토콜을 요청합니다. 이 설정은 ISE를 통해 인증되는 대부분의 엔드포인트에서 EAP-TLS를 통해 인증하려는 경우 유용합니다.

9단계. 권한 부여 프로파일 생성

구축에 필요한 마지막 정책 요소는 권한 부여 프로파일이며, 이는 권한 부여 정책에 바인딩되고 원하는 액세스 수준을 제공합니다. 권한 부여 프로파일은 권한 부여 정책에 바인딩됩니다. ISE GUI에서 구성하려면 **Policy > Policy Elements: Results > Authorization > Authorization Profiles** 을 클릭하고 **Add**.

권한 부여 프로파일은 ISE에서 지정된 RADIUS 세션에 대해 NAD로 전달되는 특성을 가져오는 컨피그레이션을 포함하며, 이 특성은 원하는 수준의 네트워크 액세스를 달성하는 데 사용됩니다.

여기에 표시된 대로 RADIUS Access-Accept를 액세스 유형으로 전달하지만, 초기 인증 시 추가 항목을 사용할 수 있습니다. 맨 아래의 Attribute Details(특성 세부사항)를 확인합니다. 여기에는 ISE가 지정된 권한 부여 프로파일과 일치할 때 NAD에 보내는 특성의 요약이 포함됩니다.



권한 부여 프로파일 - 정책 요소

ISE 권한 부여 프로파일 및 정책에 대한 자세한 내용은 Cisco Identity Services Engine 관리자 가이드, 릴리스 3.1 > 장: 세분화 > 권한 부여 정책을 [참조 하십시오](#).

보안 정책

인증 및 권한 부여 정책은 ISE GUI에서 생성되며 **Policy > Policy Sets**. ISE 3.x에서는 기본적으로 활성화되어 있습니다. ISE를 설치할 때 항상 기본 정책 집합인 하나의 정책 집합이 정의됩니다. 기본 정책 집합은 미리 정의된 기본 인증, 권한 부여 및 예외 정책 규칙을 포함합니다.

정책 집합은 ISE 관리자가 목적과 관련하여 유사한 정책을 인증 요청 내에서 사용할 다른 집합으로 그룹화할 수 있도록 계층적으로 구성됩니다. 사용자 지정 및 그룹화 정책은 사실상 제한이 없습니다. 이와 같이, 하나의 정책 세트는 네트워크 액세스를 위한 무선 엔드포인트 인증에 사용될 수 있고, 또 다른 정책 세트는 네트워크 액세스를 위한 유선 엔드포인트 인증에 사용될 수 있으며, 또는 정책을 관리하는 다른 독특하고 차별화된 방법에 사용될 수 있습니다.

Cisco ISE는 정책 집합을 평가할 수 있으며, 내부 정책은 하향식 접근 방식을 사용하므로, 해당 집합의 모든 조건이 True로 평가할 때 먼저 지정된 정책 집합을 일치시킬 수 있습니다. ISE는 다음과 같이 정책 집합과 일치하는 내에서 인증 정책 및 권한 부여 정책을 추가 평가합니다.

1. 정책 집합 및 정책 집합 조건 평가
2. 일치하는 정책 집합 내의 인증 정책
3. 권한 부여 정책 - 로컬 예외
4. 권한 부여 정책 - 전역 예외
5. 권한 부여 정책

정책 예외는 모든 정책 집합에 대해 전역적으로 또는 특정 정책 집합 내에 로컬로 존재합니다. 이러한 정책 예외는 권한 부여 정책의 일부로 처리되는데, 이는 지정된 임시 시나리오에서 네트워크 액세스에 대해 어떤 권한 또는 결과가 제공되는지를 다루기 때문입니다.

다음 섹션에서는 ISE 인증 및 권한 부여 정책에 바인딩하여 EAP-TLS를 통해 엔드포인트를 인증하는 방법에 대해 설명합니다.

10단계. 정책 집합 생성

정책 집합은 네트워크 액세스에 허용되는 프로토콜 또는 서버 시퀀스를 나타내는 단일 사용자 정의 규칙, 인증 및 권한 부여 정책 및 정책 예외로 구성된 계층적 컨테이너이며, 모두 사용자 정의 조건 기반 규칙으로 구성됩니다.

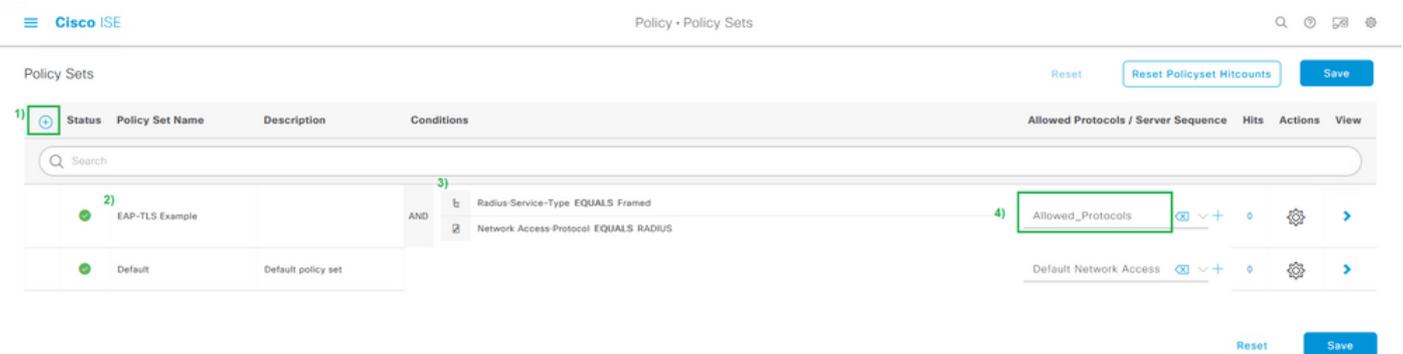
ISE GUI에서 정책 집합을 생성하려면 **Policy > Policy Set** 그런 다음 이 이미지에 표시된 것처럼 왼쪽 위 모서리에 있는 더하기(+) 아이콘을 클릭합니다.



새 정책 집합 추가

정책 집합은 이전에 구성된 이 정책 요소를 바인딩/결합할 수 있으며, 지정된 RADIUS 인증 요청(액세스 요청)에서 어떤 정책 집합을 일치시킬지를 결정하는 데 사용됩니다.

- 바인딩: 허용되는 프로토콜 서비스



정책 설정 조건 및 허용 되는 프로토콜 목록 정의

이 예에서는 RADIUS 프로토콜을 다시 시행하기 위해 중복될 수 있지만 IEEE 802.1x(framed attribute)를 시행하기 위해 RADIUS 세션에 나타나는 특정 특성 및 값을 사용합니다. 최상의 결과를

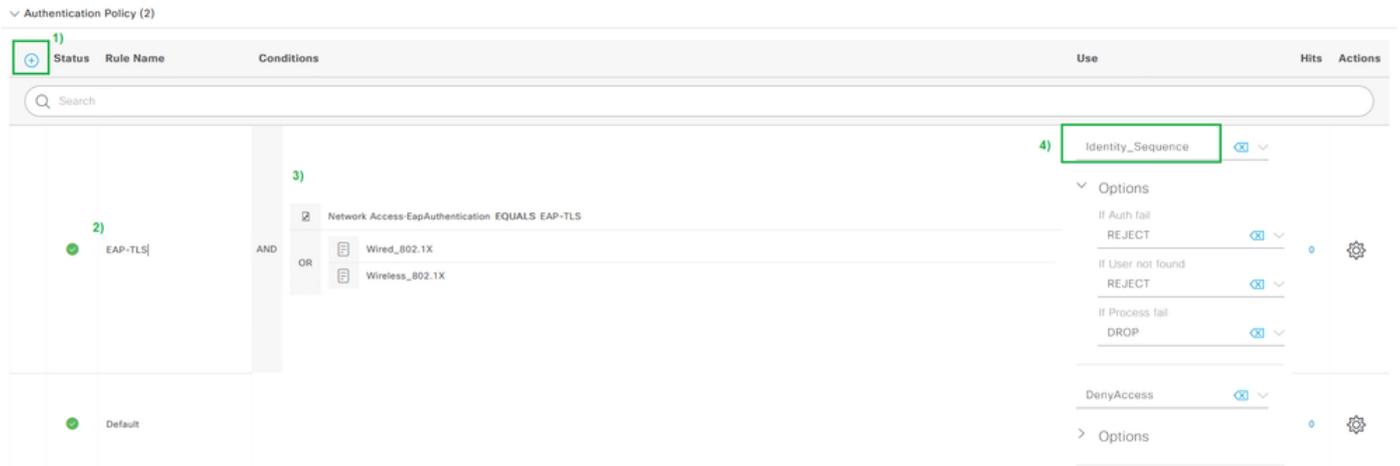
얻으려면 네트워크 장치 그룹 또는 유선 802.1x, 무선 802.1x, 또는 유선 802.1x 및 무선 802.1x 모두에 해당하는 것과 같이 원하는 의도에 적용할 수 있는 고유한 RADIUS 세션 특성만 사용하십시오

ISE의 정책 집합에 대한 자세한 내용은 Cisco Identity Services Engine 관리자 가이드, 릴리스 3.1 > 장: 세분화 > [정책 집합](#), [인증 정책](#) 및 [권한 부여 정책](#) 섹션에서 찾을 수 있습니다.

11단계. 인증 정책 생성

정책 집합 내에서 인증 정책은 인증 규칙을 일치시킬 시기를 결정하기 위해 조건과 함께 사용하도록 이전에 구성된 이러한 정책 요소를 바인딩/결합합니다.

- Bind(바인딩): 인증서 인증 프로파일 또는 ID 소스 시퀀스

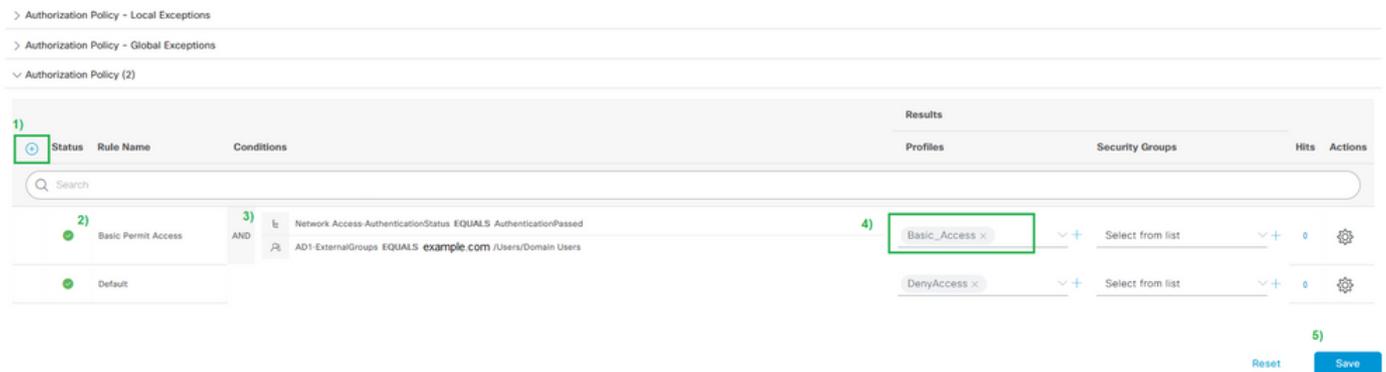


인증 정책 규칙 예

12단계. 권한 부여 정책 생성

정책 집합 내에서 권한 부여 정책은 권한 부여 규칙을 일치시킬 시기를 결정하기 위해 조건과 함께 사용하도록 이전에 구성된 이러한 정책 요소를 바인딩/결합합니다. 다음은 사용자 인증의 예입니다. 조건이 Active Directory의 도메인 사용자 보안 그룹을 가리키기 때문입니다.

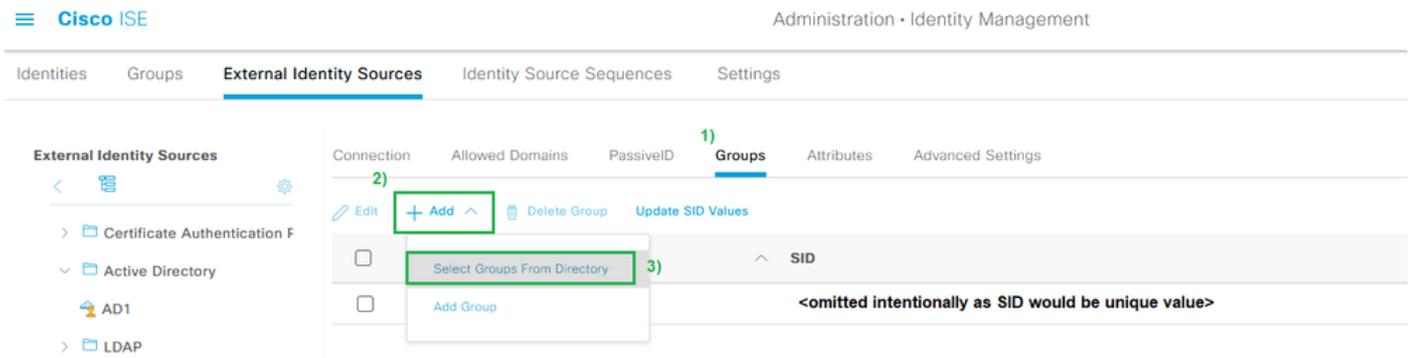
- Bind(바인딩): 권한 부여 프로파일



권한 부여 정책 규칙 예

외부 그룹(예: Active Directory 또는 LDAP)을 추가하려면 외부 서버 인스턴스에서 그룹을 추가해야

합니다. 이 예에서는 ISE UI에서 가져옵니다. Administration > Identity Management: External Identity Sources > Active Directory {AD Join Point Name} > Groups. 그룹 탭에서 다음을 선택합니다 Add > Select Groups from Directory Name(이름) 필터를 사용하여 모든 그룹(*) 또는 특정 그룹(예: Domain Users(*domain users*))을 검색하여 그룹을 검색할 수 있습니다.



ISE 정책에서 외부 그룹을 사용하려면 디렉토리에서 그룹을 추가해야 합니다

Select Directory Groups

This dialog is used to select groups from the Directory.

Domain

Name SID

Filter Filter

Type

1 Groups Retrieved.

<input type="checkbox"/>	Name	Group SID	Group Type
<input checked="" type="checkbox"/>	example.com /Users/Domain Users	<omitted SID intentionally>	GLOBAL

외부 디렉토리 내 검색 - Active Directory 예

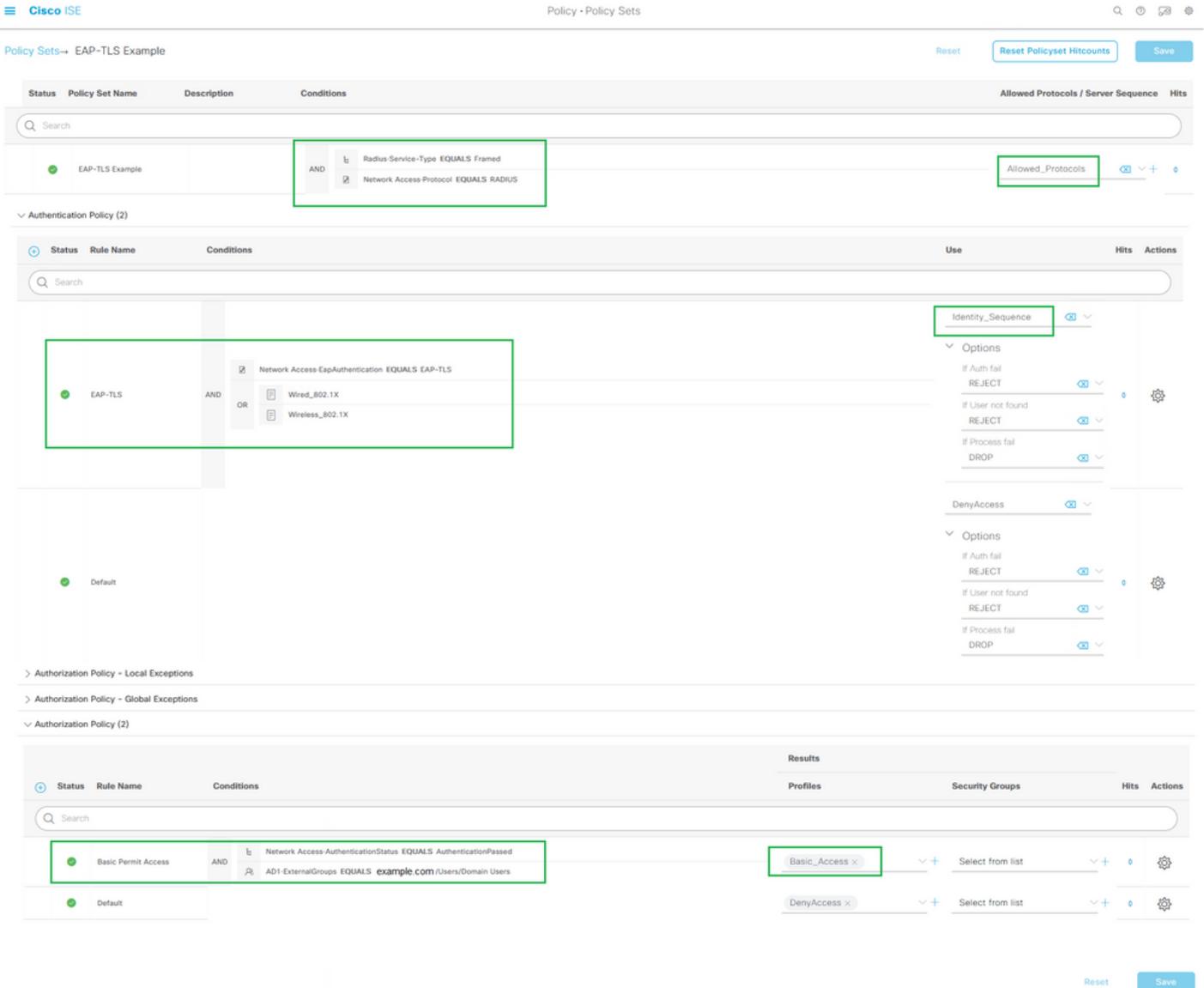
각 그룹 옆의 확인란을 선택한 후에는 ISE 내의 Policies(정책)에서 를 활용합니다. 변경 사항을 저장하기 위해 확인 및/또는 저장을 클릭하는 것을 잊지 마십시오.

다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

모든 전역 컨피그레이션 및 정책 요소가 정책 집합을 바인딩하면 컨피그레이션은 EAP-TLS를 통한

사용자 인증에 대해 이 이미지와 비슷하게 표시됩니다.



문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

컨피그레이션이 완료되면 엔드포인트를 연결하여 인증을 테스트합니다. 결과는 ISE GUI에서 확인할 수 있습니다. 선택 **Operations > Radius > Live Logs**이 그림에 나와 있는 것처럼.

인식을 위해 RADIUS 및 TACACS+(Device Admin)용 라이브 로그를 최대 지난 24시간 동안의 인증 시도/활동 및 지난 100개 레코드에 사용할 수 있습니다. 이 기간 이후에 이러한 유형의 보고 데이터를 보려면 보고서를 특히 사용해야 합니다. **ISE UI: Operations > Reports > Reports: Endpoints and Users > RADIUS Authentications**.

Radius > Live Logs의 출력 예

ISE의 RADIUS 라이브 로그에서 세션 특성을 포함하는 RADIUS 세션에 대한 정보 및 인증 흐름 동안 관찰된 동작을 진단하는 데 유용한 기타 정보를 찾을 수 있습니다. 다음을 클릭합니다. details 이 인증 시도와 관련된 세션 특성 및 관련 정보를 보려면 세션의 세부 보기를 엽니다.

문제를 해결하려면 올바른 정책이 일치하는지 확인하는 것이 중요합니다. 이 컨피그레이션 예에서는 이미지에 표시된 대로 원하는 인증 및 권한 부여 정책이 일치합니다.

Authentication Policy	EAP-TLS Example >> EAP-TLS
Authorization Policy	EAP-TLS Example >> Basic Permit Access
Authorization Result	Basic_Access

세부 보기에서 이러한 특성은 이 컨피그레이션 예의 일부로서 설계에 따라 인증이 예상대로 동작하는지 확인하기 위해 검사됩니다.

- 이벤트
 - 여기에는 인증 성공 여부가 포함됩니다.
 - 작업 시나리오에서 값은 5200 Authentication succeeded입니다.
- 사용자 이름
 - 여기에는 ISE에 제공된 클라이언트 인증서에서 가져온 최종 ID가 포함됩니다.
 - 작업 시나리오에서는 엔드포인트에 로그인한 사용자의 사용자 이름(즉, 이전 이미지의 employee1)입니다.
- 엔드포인트 ID
 - 유/무선의 경우 이 값은 엔드포인트의 NIC(네트워크 인터페이스 카드)에 대한 MAC 주소입니다.
 - 작업 시나리오에서는 연결이 VPN을 통하지 않는 한 엔드포인트의 MAC 주소가 됩니다. 이 경우 엔드포인트의 IP 주소가 될 수 있습니다.
- 인증 정책
 - 정책 조건과 일치하는 세션 특성을 기반으로 지정된 세션에 대해 일치하는 인증 정책을 표시합니다.

- 작업 시나리오에서 이는 구성된 대로 예상되는 인증 정책입니다.
 - 다른 정책이 보이면 해당 정책의 조건과 비교할 때 기대했던 정책이 참으로 평가되지 않았다는 것을 의미한다. 이 경우 세션 특성을 검토하고 각 정책에 대해 서로 다르지만 고유한 조건을 포함해야 합니다.
- 권한 부여 정책
 - 정책 조건과 일치하는 세션 특성을 기반으로 지정된 세션에 대해 일치하는 권한 부여 정책을 표시합니다.
 - 작업 시나리오에서, 이는 구성된 대로 예상되는 권한 부여 정책입니다.
 - 다른 정책을 보면 정책의 조건과 비교할 때 기대했던 정책이 참으로 평가되지 않은 것을 의미한다. 이 경우, 세션 특성을 검토하고 각 정책에 다른 고유한 조건이 포함되어 있는지 확인합니다.
- 권한 부여 결과
 - 일치하는 권한 부여 정책에 따라 지정된 세션에서 사용된 권한 부여 프로파일을 표시합니다.
 - 작업 시나리오에서 이 값은 정책에 구성된 값과 동일합니다. 감사 목적으로 검토하고 올바른 권한 부여 프로파일이 구성되었는지 확인하는 것이 좋습니다.
- 정책 서버
 - 여기에는 인증 시도와 관련된 ISE PSN(Policy Service Node)의 호스트 이름이 포함됩니다.
 - 작업 시나리오에서는 PSN이 작동하지 않거나 예상보다 높은 대기 시간 또는 인증 시간 초과로 인해 장애 조치가 발생한 경우를 제외하고 NAD(에지 디바이스라고도 함)에 구성된 대로 첫 번째 PSN 노드로 이동하는 인증만 볼 수 있습니다.
- 인증 방법
 - 지정된 세션에서 사용된 인증 방법을 표시합니다. 이 예제에서는 값을 dot1x로 표시합니다.
 - 작업 시나리오에서는 이 컨피그레이션 예에 따라 값이 dot1x로 표시됩니다. 다른 값이 표시되면 dot1x가 실패했거나 시도되지 않았다는 의미일 수 있습니다.
- 인증 프로토콜
 - 지정된 세션에서 사용된 인증 방법을 표시합니다. 이 예에서는 값이 EAP-TLS로 표시됩니다.
 - 작업 시나리오에서는 이 컨피그레이션 예에 따라 항상 값이 EAP-TLS로 표시됩니다. 다른 값이 표시되면 신청자와 ISE가 EAP-TLS를 성공적으로 협상하지 않은 것입니다.
- 네트워크 장치
 - 엔드포인트와 ISE 간의 인증 시도와 관련된 NAD(에지 디바이스라고도 함)에 대한 네트워크 디바이스 이름을 ISE에서 구성한 대로 표시합니다.
 - 작업 시나리오에서 이 이름은 항상 ISE UI에 지정됩니다. Administration > System: Network Devices. 이 컨피그레이션을 기반으로 NAD(에지 디바이스라고도 함)의 IP 주소를 사용하여 NAS IPv4 Address 세션 특성에 포함된 인증 네트워크 디바이스를 결정합니다.

이는 트러블슈팅이나 기타 가시성을 위해 검토할 수 있는 모든 세션 속성의 전체 목록이 아닙니다.

확인할 수 있는 다른 유용한 속성이 있기 때문입니다. 모든 정보에 익숙해지도록 모든 세션 특성을 검토하는 것이 좋습니다. ISE에서 수행하는 작업 또는 동작을 보여 주는 Steps(단계) 섹션에 오른쪽을 포함할 수 있습니다.

일반적인 문제 및 트러블슈팅 기법

이 목록에는 몇 가지 일반적인 문제와 문제 해결 조언이 포함되어 있으며, 결코 완전한 목록이 될 수 없습니다. 대신 이 방법을 지침으로 사용하고 ISE와 관련된 문제를 해결할 수 있는 고유한 기술을 개발하십시오.

문제: 인증 실패(5400 인증 실패) 또는 기타 인증 시도가 성공하지 못했습니다.

- 인증 실패가 발생하면 세부 정보 아이콘을 클릭하여 인증이 실패한 이유와 수행한 단계에 대한 정보를 제공합니다. 여기에는 실패 사유와 가능한 근본 원인이 포함됩니다.
- ISE는 인증 결과에 대한 결정을 내리기 때문에 ISE는 인증 시도가 성공하지 못한 이유를 이해할 수 있는 정보를 제공합니다.

문제점: 인증이 성공적으로 완료되지 않았으며 실패 이유는 "5440 엔드포인트가 EAP 세션을 취소했으며 새로 시작됨" 또는 "5411 신청자가 ISE에 응답하지 않음"으로 표시됩니다.

- 이 실패 이유는 시간 초과 전에 RADIUS 통신이 완료되지 않았음을 나타냅니다. EAP는 엔드포인트와 NAD 간에 있으므로 NAD에서 사용되는 시간 제한을 확인하고 최소 5초 동안 설정되었는지 확인해야 합니다.
- 5초로도 이 문제를 해결할 수 없는 경우에는 이 기술을 통해 이 문제가 해결되는지 확인하기 위해 몇 번 5초 정도 늘린 후 다시 테스트하는 것이 좋습니다.
- 이전 단계에서 문제가 해결되지 않을 경우, 동일한 올바른 ISE PSN 노드에서 인증이 처리되고 전반적인 동작이 비정상 동작을 나타내지 않는 것(예: NAD와 ISE PSN 노드 간의 정상 레이턴시보다 높음)을 확인하는 것이 좋습니다.
- 또한 ISE가 클라이언트 인증서를 수신하지 않는 경우 엔드포인트가 패킷 캡처를 통해 클라이언트 인증서를 전송하는지 확인하는 것이 좋습니다. 그러면 엔드포인트(사용자 인증서)가 ISE EAP 인증 인증서를 신뢰할 수 없습니다. true이면 올바른 인증서 저장소에서 CA 체인을 가져옵니다(루트 CA = 신뢰할 수 있는 루트 CA). | Intermediate CA = Trusted Intermediate CA).

문제점: 인증에 성공했지만 올바른 인증 및/또는 권한 부여 정책과 일치하지 않습니다.

- 성공했지만 올바른 인증 및/또는 권한 부여 규칙과 일치하지 않는 인증 요청이 발생하는 경우, 사용된 조건이 정확하고 RADIUS 세션에 있는지 확인하기 위해 세션 특성을 검토하는 것이 좋습니다.
- ISE는 하향식 접근 방식으로 이러한 정책을 평가합니다(포스터 정책 제외). 매칭된 정책이 매칭할 원하는 정책의 위 또는 아래에 있는지 먼저 확인해야 합니다. 인증 정책은 먼저 권한 부여 정책과 독립적으로 평가됩니다. 인증 정책이 올바르게 매칭될 경우 Steps(단계)라는 오른쪽

쪽 섹션 아래의 Authentication Details(인증 세부사항)에서 Authentication Passed(인증 전달)가 22037.

- 원하는 정책이 일치하는 정책 위에 있는 경우 이는 원하는 정책의 조건 합계가 참으로 평가되지 않았음을 의미합니다. 조건 및 세션의 모든 속성과 값을 검토하여 해당 속성이 존재하고 맞춤법 오류가 없는지 확인합니다.
- 원하는 정책이 일치하는 정책 아래에 있는 경우 원하는 정책 대신 다른 정책(위)이 일치했음을 의미합니다. 이는 조건 값이 충분히 구체적이지 않거나, 조건이 다른 정책에서 중복되거나, 정책의 순서가 잘못되었음을 의미할 수 있습니다. 문제 해결이 더 어려워지는 반면, 원하는 정책이 일치하지 않은 이유를 확인하기 위해 정책 검토를 시작하는 것이 좋습니다. 이를 통해 다음에 수행할 작업을 파악할 수 있습니다.

문제점: 인증 중에 사용된 ID 또는 사용자 이름이 예상한 값이 아닙니다.

- 이 경우 엔드포인트가 클라이언트 인증서를 전송하면 ISE가 Certificate Authentication Template(인증서 인증 템플릿)에서 올바른 인증서 필드를 사용하지 않을 가능성이 높습니다. 이 필드는 인증 단계 중에 평가됩니다.
- 클라이언트 인증서를 검토하여 원하는 ID/사용자 이름이 있는 정확한 필드를 찾고 동일한 필드가 다음에서 선택되었는지 확인합니다. ISE UI: Administration > Identity Management: External Identity Sources > Certificate Authentication Profile > (certificate authentication profile used in the Authentication Policy).

문제점: 클라이언트 인증서 체인의 알 수 없는 CA 때문 12514 EAP-TLS가 SSL/TLS 핸드셰이크에 실패한 이유를 사용하여 인증에 실패했습니다.

- 클라이언트 인증서에 ISE UI에서 신뢰할 수 없는 CA 체인의 인증서가 있는 경우 이 문제가 발생할 수 있습니다. Administration > System: Certificates > Trusted Certificates.
- 이는 일반적으로 클라이언트 인증서(엔드포인트)에 EAP 인증을 위해 ISE에 서명된 인증서 CA 체인과 다른 CA 체인이 있을 때 발생할 수 있습니다.
- 확인을 위해 클라이언트 인증서 CA 체인이 ISE에서 신뢰되는지, ISE EAP 인증 서버 인증서 CA 체인이 엔드포인트에서 신뢰되는지 확인합니다.
 - Windows OS 및 Chrome의 경우 Start > Run MMC > Add/Remove Snap-In > Certificates > User Certificates.
 - Firefox의 경우: 웹 서버에 대해 신뢰할 수 있는 CA 체인(최종 ID 인증서가 아님)을 가져옵니다.

관련 정보

- Cisco Identity Services Engine > [설치 및 업그레이드 가이드](#)
- Cisco Identity Services Engine > [컨피그레이션 가이드](#)
- Cisco Identity Services Engine > [호환성 정보](#)
- Cisco Identity Services Engine 관리자 가이드, 릴리스 3.1 > 장: 보안 액세스 > [Cisco ISE에서 네트워크 장치 정의](#)

- Cisco Identity Services Engine 관리자 가이드, 릴리스 3.1 > 장: 세분화 > [정책 집합](#)
- Cisco Identity Services Engine 관리자 가이드, 릴리스 3.1 > 장: 세분화 > [인증 정책](#)
- Cisco Identity Services Engine 관리자 가이드, 릴리스 3.1 > 장: 세분화 > [권한 부여 정책](#)
- Cisco Identity Services Engine > 구성 가이드 > [Active Directory Integration with Cisco ISE 2.x](#)
- Cisco Identity Services Engine 관리자 가이드, 릴리스 3.1 > 장: 세분화 > 네트워크 액세스 서비스 > 사용자를 [위한 네트워크 액세스](#)
- Cisco Identity Services Engine 관리자 가이드, 릴리스 3.1 > 장: 기본 설정 > [Cisco ISE의 인증서 관리](#)
- Cisco Identity Services Engine 관리자 가이드, 릴리스 3.1 > 장: 기본 설정 > Cisco ISE CA 서비스 > 개인 장치 인증에 인증서를 사용 하기 위해 Cisco ISE 구성 > TLS [기반 인증을 위한 인증서 인증 프로파일 생성](#)
- Cisco Identity Services Engine > Configuration Examples and TechNotes > [Configure ISE 2.0 Certificate Provisioning Portal\(ISE 2.0 인증서 프로비저닝 포털 구성\)](#)
- Cisco Identity Services Engine > Configuration Examples and TechNotes > [ISE에 서드파티 CA 서명 인증서 설치](#)
- Wireless LAN (WLAN)(무선 LAN(WLAN)) > Configuration Examples and TechNotes(컨피그레이션 예 및 TechNotes) > Understand [and configure EAP-TLS using WLC and ISE\(WLC 및 ISE를 사용하여 EAP-TLS 이해 및 구성\)](#)
- [기술 지원 및 문서 - Cisco Systems](#)

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.