ISE에 타사 CA 서명 인증서 설치

목차

소개

이 문서에서는 Cisco ISE(Identity Services Engine)에서 서드파티 CA 서명 인증서 설치에 대해 설명합니다. 이 프로세스는 최종 인증서 역할(EAP 인증, 포털, 관리 및 pxGrid)과 상관없이 동일합니다.

사전 요구 사항

요구 사항

Cisco에서는 기본 공개 키 인프라에 대한 지식을 보유하고 있는 것이 좋습니다.

사용되는 구성 요소

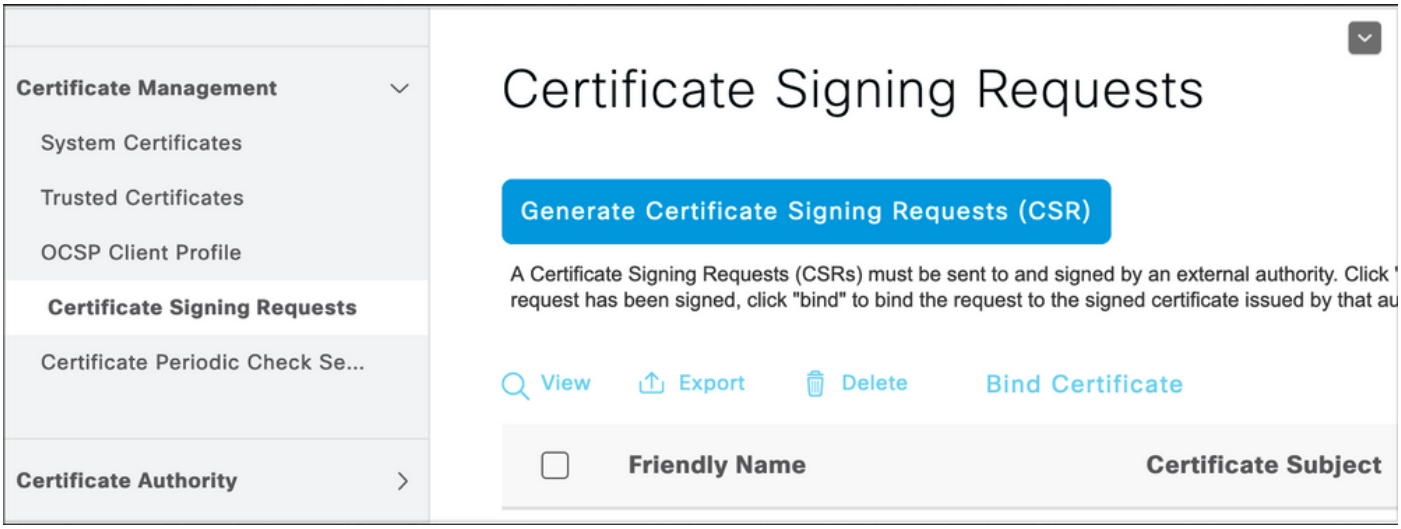
이 문서의 정보는 Cisco ISE(Identity Services Engine) 릴리스 3.0을 기반으로 합니다. 릴리스 2.X에도 동일한 구성이 적용됩니다.

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

구성

1단계. CSR(Certificate Signing Request)을 생성합니다.

CSR을 생성하려면 Administration(관리) > **Certificates(인증서) > Certificate Signing Requests(인증서 서명 요청)**로 이동하고 **Generate Certificate Signing Requests** (CSR)(CSR(**Generate Certificate Signing Requests**)를 클릭합니다.



1. Usage 섹션의 드롭다운 메뉴에서 사용할 역할을 선택합니다.인증서가 여러 역할에 사용되는 경우 다중 사용을 선택할 수 있습니다.인증서가 생성되면 필요한 경우 역할을 변경할 수 있습니다.

2. 인증서를 생성할 노드를 선택합니다.

3. 필요에 따라 정보를 입력합니다(조직 단위, 조직, 도시, 주 및 국가).

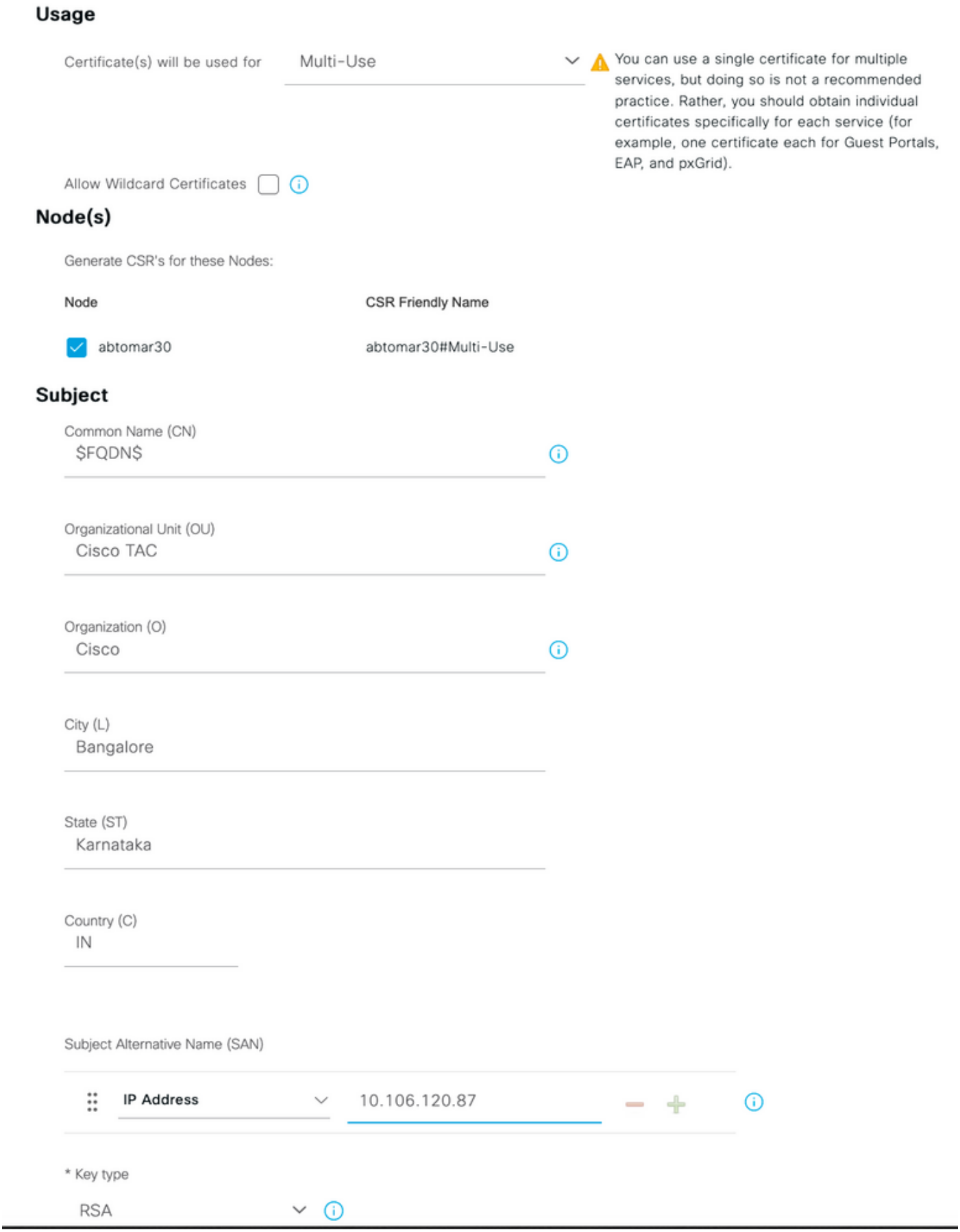
   참고:CN(Common Name) 필드 아래에서 ISE는 노드의 FQDN(Fully Qualified Domain Name)을 자동으로 채웁니다.

와일드카드:

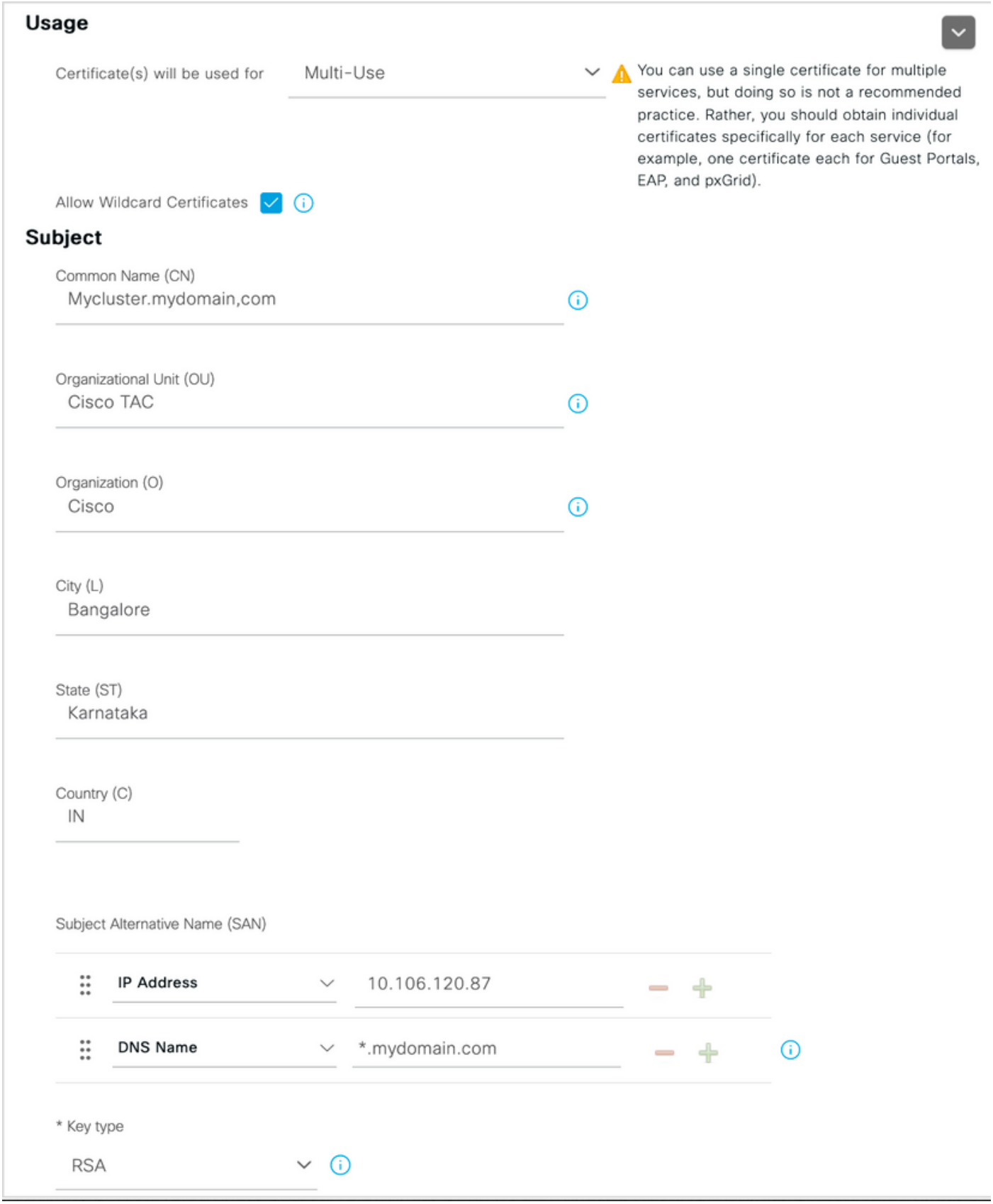
- 와일드카드 인증서를 생성하려는 경우 Allow Wildcard **Certificates** 상자**를** 선택합니다.
- 인증서가 EAP 인증에 사용되는 경우 Windows 신청자가 서버 인증서를 거부하므로 * 기호가 Subject CN 필드에 없어야 합니다.
- 서 플리 컨 트에서 **Validate Server Identity(서버 ID 검증)**가 비활성화된 경우에도 ***가** CN 필드에 있는 경우 SSL 핸드셰이크가 실패할 수 있습니다.
- 대신 CN 필드에서 일반 FQDN을 사용할 수 있으며, 그런 다음 ***.domain.com을** SAN(Subject Alternative Name) DNS Name 필드에 사용할 수 있습니다.

  참고:일부 CA(Certificate Authorities)는 CSR에 없는 경우에도 인증서의 CN에 와일드카드(*)를 자동으로 추가할 수 있습니다.이 시나리오에서는 이 작업을 방지하기 위해 특별한 요청을 제기해야 합니다.

개별 서버 인증서 CSR 예:

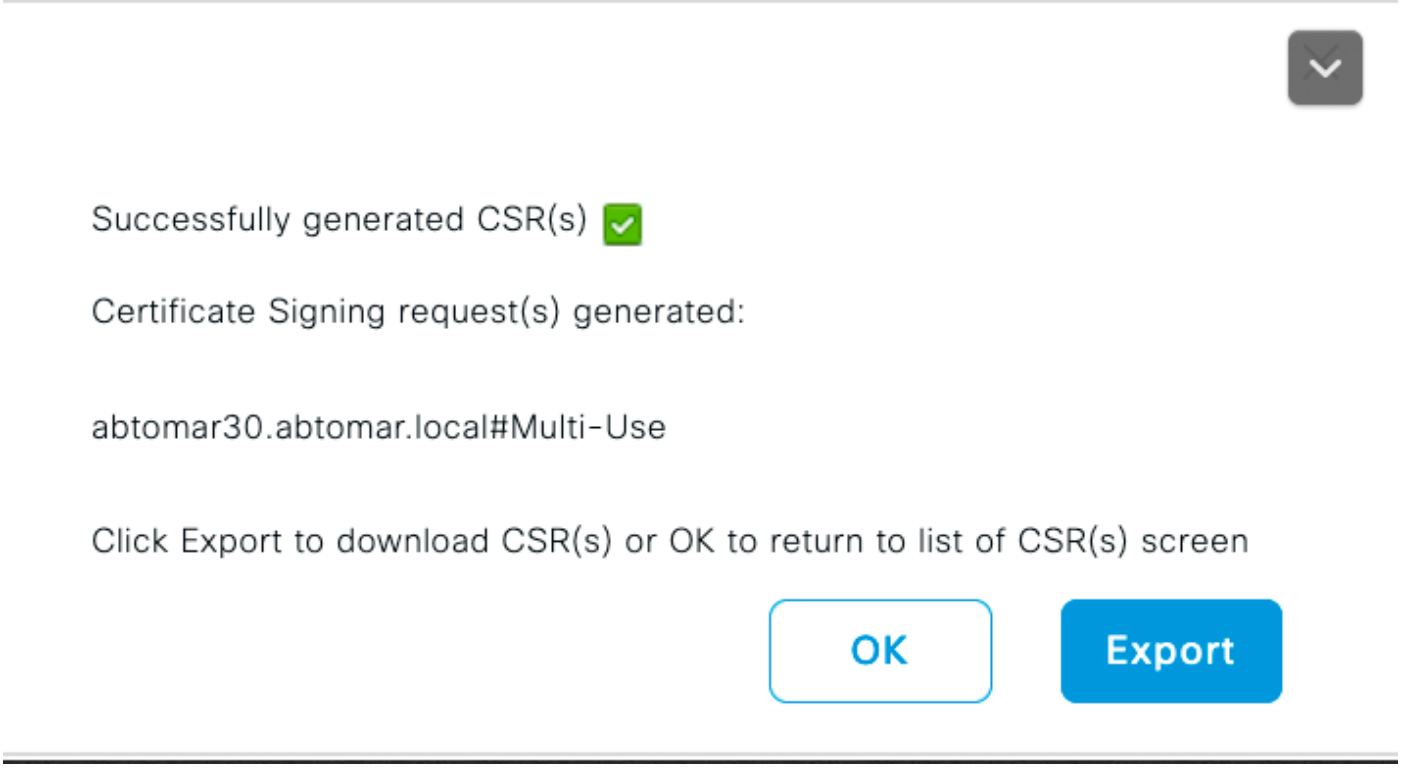

Usage
Certificate(s) will be used for
Multi-Use
You can use a single certificate for multiple services, but doing so is not a recommended practice. Rather, you should obtain individual certificates specifically for each service (for example, one certificate each for Guest Portals, EAP, and pxGrid).
Allow Wildcard Certificates
Node(s)
Generate CSR's for these Nodes:
Node
CSR Friendly Name
abtomar30
abtomar30#Multi-Use
Subject
Common Name (CN)
$FQDN$
Organizational Unit (OU)
Cisco TAC
Organization (O)
Cisco
City (L)
Bangalore
State (ST)
Karnataka
Country (C)
IN
Subject Alternative Name (SAN)
IP Address
10.106.120.87
* Key type
RSA

와일드카드 CSR 예:



참고:IP 주소를 통해 서버에 액세스할 때 인증서 경고를 피하기 위해 각 구축 노드의 IP 주소를 SAN 필드에 추가할 수 있습니다.

CSR이 생성되면 ISE는 내보내기 옵션이 있는 팝업 창을 표시합니다. 내보낸 후에는 서명을 위해 이 파일을 CA로 전송해야 합니다.



2단계. 새 인증서 체인을 가져옵니다.

인증 기관은 전체 인증서 체인(루트/중간)과 함께 서명된 서버 인증서를 반환합니다. 수신되면 다음 단계에 따라 ISE 서버로 인증서를 가져옵니다.

1. CA에서 제공하는 루트 및 중간 인증서를 가져오려면 Administration(관리) > Certificates(인증서) **> Trusted Certificates(신뢰할 수 있는 인증서)로 이동합니다**.

2. Import(**가져오기**)를 클릭한 다음 Root(루트) 및/또는 Intermediate(중간) 인증서를 선택하고 제출할 관련 확인란을 선택합니다.
3. 서버 인증서를 가져오려면 Administration(관리) **> Certificates(인증서) > Certificate Signing Requests(인증서 서명 요청)로 이동합니다**.

4. 이전에 생성한 CSR을 선택하고 Bind Certificate(인증서 **바인딩**)를 클릭합니다.

5. 새 인증서 위치를 선택하고 ISE는 데이터베이스에 생성 및 저장 된 개인 키에 인증서를 바인딩합니다.

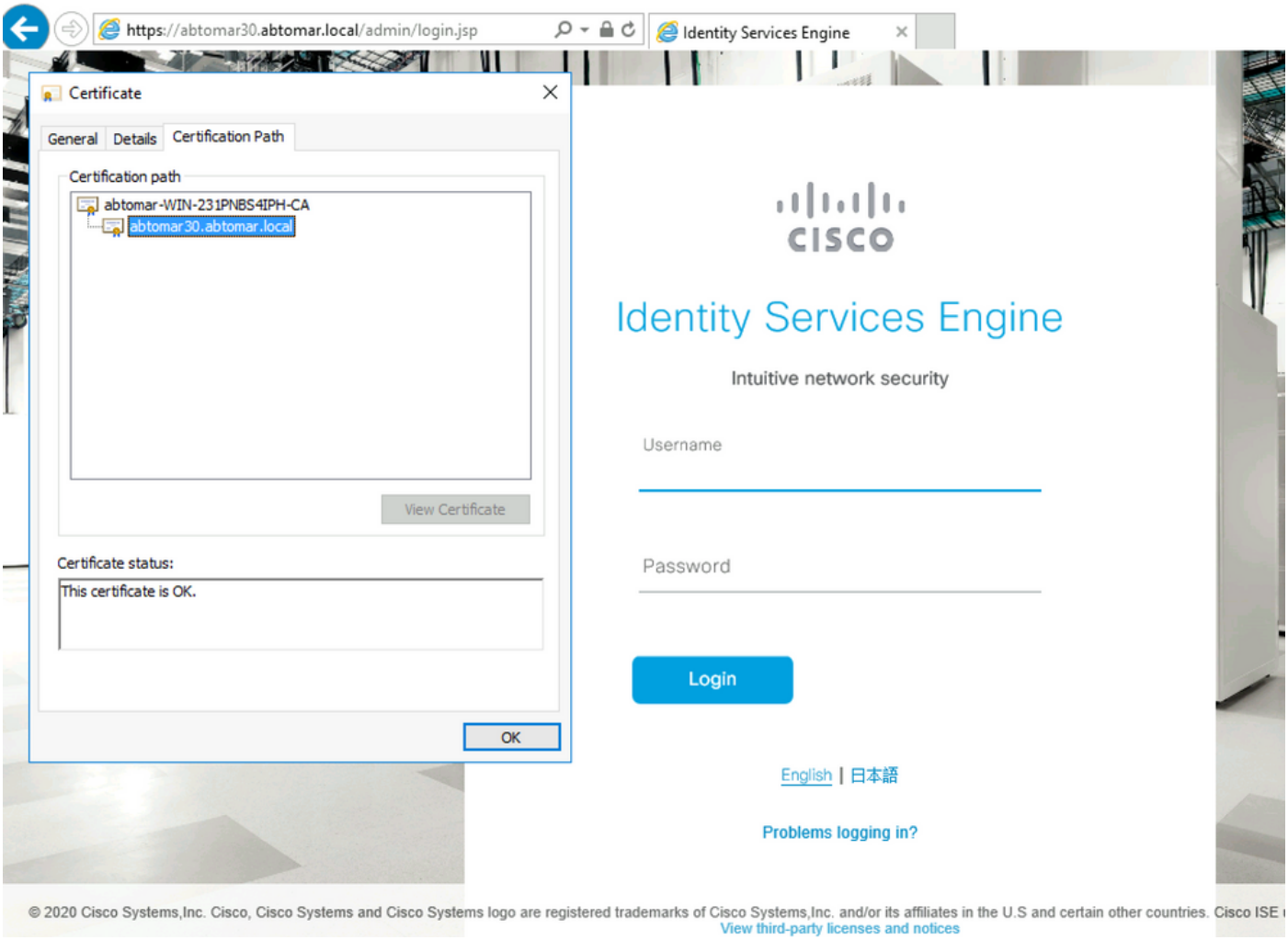
   참고:이 인증서에 대해 Admin Role(관리 역할)을 선택한 경우 특정 ISE 서버 서비스가 다시 시작됩니다.

   주의:가져온 인증서가 구축의 기본 관리 노드에 대한 것이며 관리 역할이 선택된 경우 모든 노드의 서비스는 차례로 재시작됩니다.이 작업은 예상되며 이 작업을 수행하려면 다운타임이 권장됩니다.

다음을 확인합니다.

인증서 가져오기 중에 관리 역할을 선택한 경우 브라우저에서 관리 페이지를 로드하여 새 인증서가

제자리에 있는지 확인할 수 있습니다. 체인이 올바르게 빌드되고 브라우저에서 인증서 체인을 신뢰할 수 있는 경우 브라우저는 새 관리자 인증서를 신뢰해야 합니다.



추가 확인을 위해 브라우저에서 잠금 기호를 선택하고 인증서 경로 아래에서 컴퓨터에서 전체 체인이 존재하고 신뢰할 수 있는지 확인합니다.이는 전체 체인이 서버에 의해 올바르게 전달되었음을 나타내는 직접적인 표시기가 아니라 로컬 트러스트 저장소를 기반으로 서버 인증서를 신뢰할 수 있는 브라우저의 표시기입니다.

문제 해결

dot1x 인증 중에 신청자가 ISE 로컬 서버 인증서를 신뢰하지 않음

SSL 핸드셰이크 프로세스 중에 ISE가 전체 인증서 체인을 전달하는지 확인합니다.

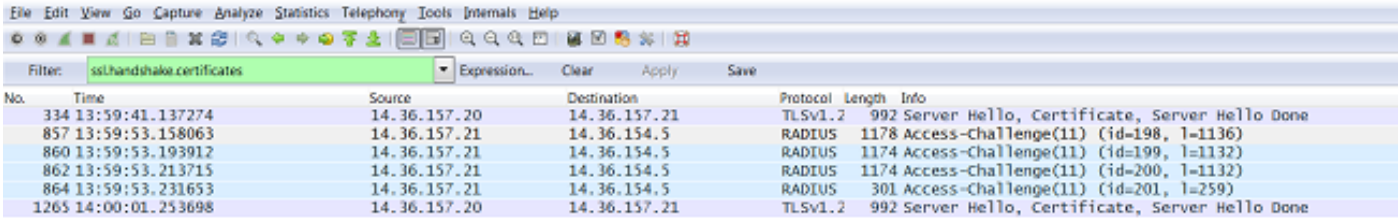
서버 인증서(예: PEAP)가 필요한 EAP 방법 및 **서버 ID 확인**이 선택된 경우 신청자는 인증 프로세스의 일부로 로컬 신뢰 저장소에 있는 인증서를 사용하여 인증서 체인을 검증합니다.SSL 핸드셰이크 프로세스의 일부로 ISE는 해당 인증서 및 체인에 있는 루트 및 중간 인증서를 나타냅니다.체인이 불완전한 경우 신청자가 서버 ID를 검증할 수 없습니다.인증서 체인이 클라이언트로 다시 전달되었는지 확인하려면 다음 단계를 수행할 수 있습니다.

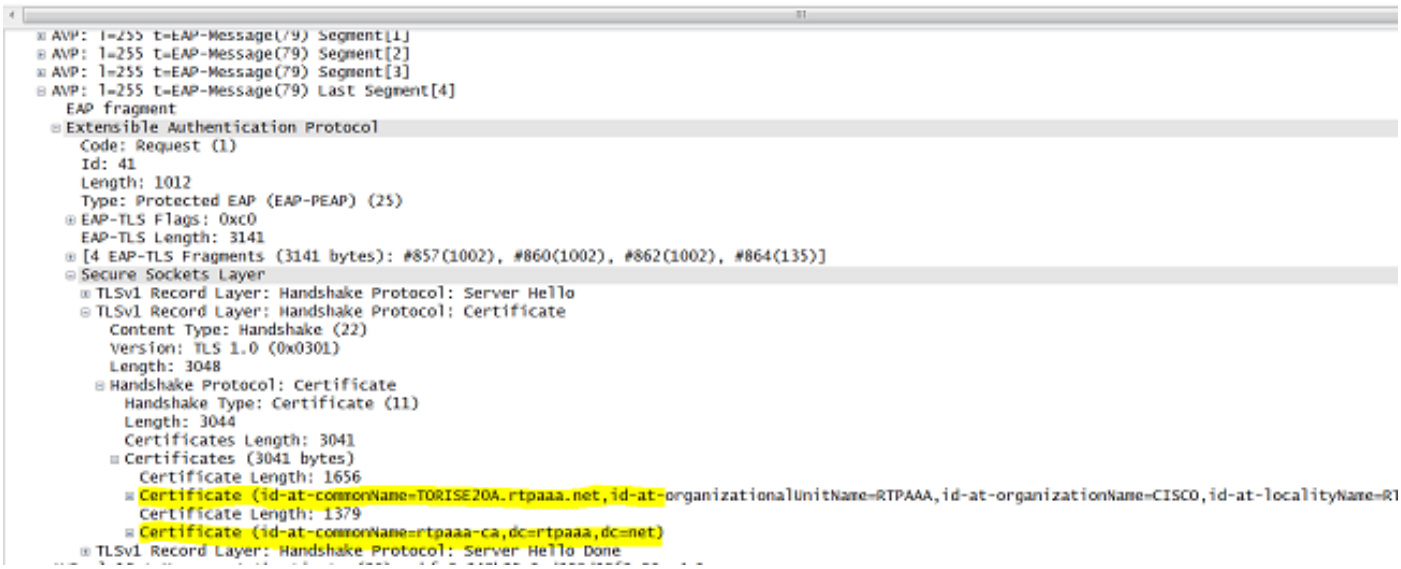
1. 인증 중에 ISE(TCPDump)에서 캡처를 가져오려면 Operations(작업) > Diagnostic Tools(진단 **툴) > General Tools(일반 툴) > TCP Dump(TCP 덤프)로 이동합니다**.

2. 캡처를 다운로드/열고 Wireshark에서 **ssl.handshake.certificates** 필터를 적용하고 액세스 챌린지를 찾습니다.

3. Expand Radius Protocol(**RADIUS 프로토콜) > Attribute Value Pairs(특성 값 쌍) > EAP-Message Last segment(EAP-메시지 마지막 세그먼트) > Extensible Authentication Protocol(확장 가능한 인증 프로토콜) > Secure Sockets Layer(SSL 소켓 레이어) > Certificate(인증서) > Certificates(인증서)로 이동합니다**.

캡처에서 인증서 체인.

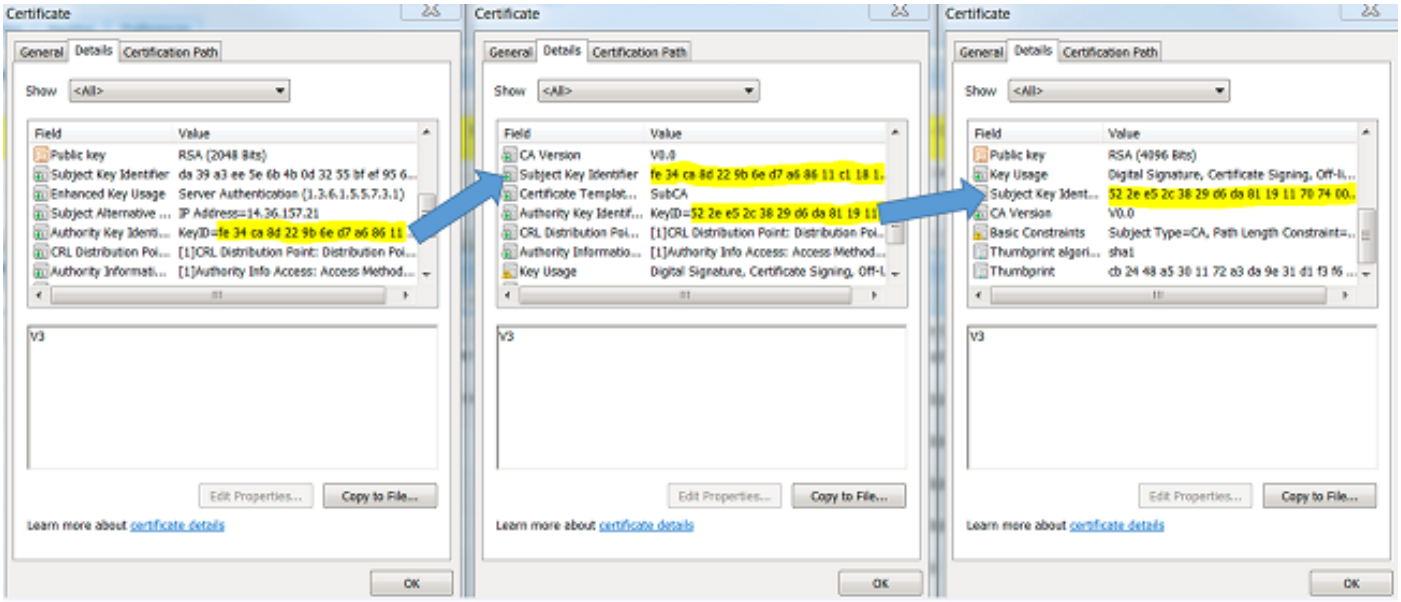




체인이 불완전한 경우 ISE **Administration(ISE 관리) > Certificates(인증서) > Trusted Certificates(신뢰할 수 있는 인증서)로 이동하고** 루트 및 (또는) Intermediate 인증서가 있는지 확인합니다.인증서 체인이 성공적으로 전달된 경우 여기에 설명된 방법을 사용하여 체인 자체를 유효한 것으로 확인해야 합니다.

각 인증서(서버, 중간 및 루트)를 열고 각 인증서의 SKI(Subject Key Identifier)를 체인의 다음 인증서의 AKI(Authority Key Identifier)에 매칭하여 신뢰 체인을 확인합니다.

인증서 체인의 예.

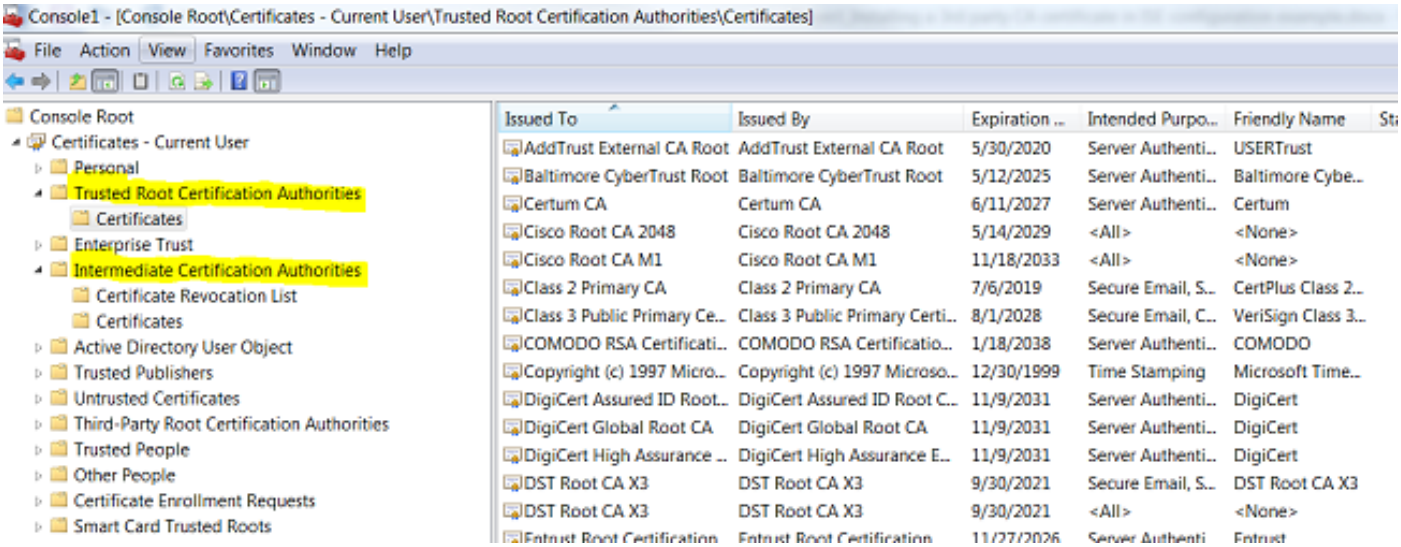


ISE 인증서 체인이 올바르지만 엔드포인트가 인증 중에 ISE의 서버 인증서를 거부함

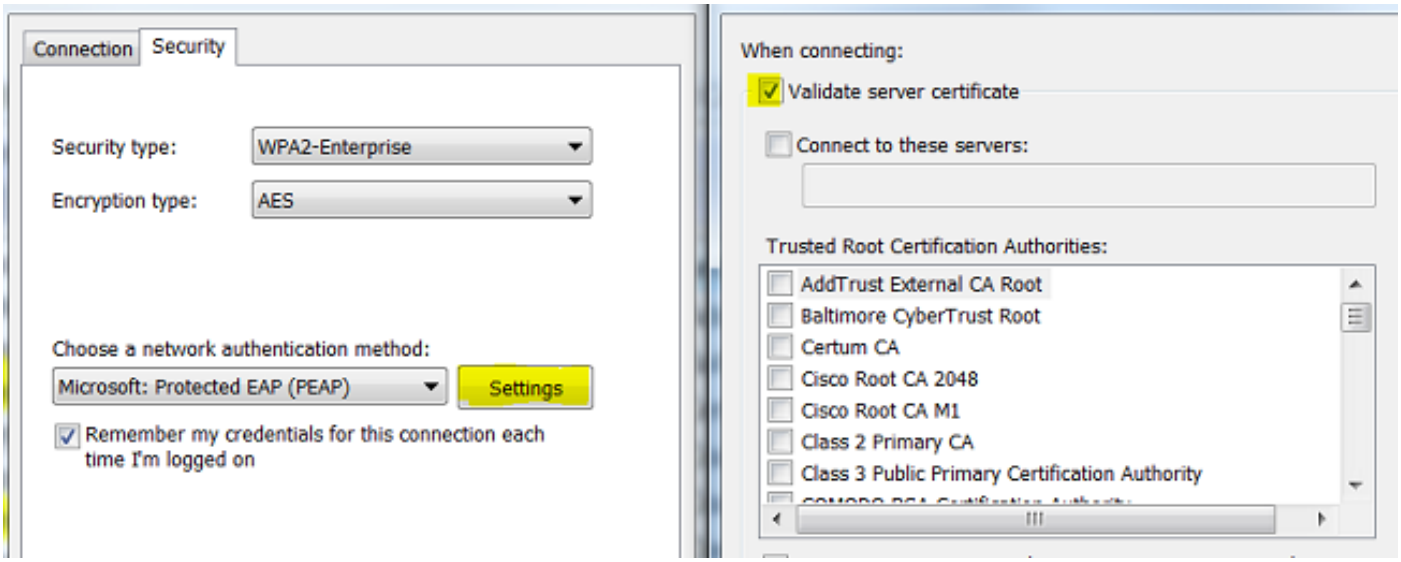
SSL 핸드셰이크 중에 ISE가 전체 인증서 체인을 제공하고 서 플리 컨 트가 여전히 인증서 체인을 거부 중인 경우다음 단계는 루트 및 중간 인증서가 클라이언트 로컬 트러스트 저장소에 있는지 확인하는 것입니다.

Windows 장치에서 이를 확인하려면 mmc.**exe** 파일 **> 스냅인 추가-제거 로 이동합니다**.사용 가능한 스냅인 열에서 **인증서**를 선택하고 **추가**를 클릭합니다.사용 중인 인증 유형(사용자 또는 시스템)에 따라 **내 사용자 계정** 또는 **컴퓨터 계정**을 선택한 다음 **확인**을 클릭합니다.

콘솔 보기에서 **Trusted Root Certification Authorities** 및 **Intermediate Certification Authorities**를 선택하여 로컬 트러스트 저장소에 루트 및 중간 인증서가 있는지 확인합니다.



서버 ID 확인 문제인지 쉽게 확인할 수 있는 방법은 서 플리 컨 트 프로필 컨피그레이션 아래 **Validate Server Certificate(서버 인증서 검증)**를 선택 취소하고 다시 테스트하십시오.



관련 정보

- [Cisco Identity Services Engine 관리자 가이드, 릴리스 3.0]
- [기술 지원 및 문서 – Cisco Systems]