ISE 관리를 위한 인증서 또는 스마트 카드 기반 인증 구성

목차

[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[사용되는 구성 요소](#)
[구성](#)
[네트워크 다이어그램](#)
[Active Directory에 ISE 가입](#)
[디렉터리 그룹 선택](#)
[관리 액세스에 Active Directory 암호 기반 인증 사용](#)
[외부 ID 그룹을 관리 그룹에 매핑](#)
[신뢰할 수 있는 인증서 가져오기](#)
[인증서 인증 프로파일 구성](#)
[클라이언트 인증서 기반 인증 활성화](#)
[다음을 확인합니다.](#)
[문제 해결](#)

소개

이 문서에서는 ISE(Identity Services Engine) 관리 액세스를 위한 클라이언트 인증서 기반 인증을 구성하는 방법에 대해 설명합니다.이 예에서는 ISE 관리자가 사용자 인증서를 인증하여 Cisco ISE(Identity Services Engine) 관리 GUI에 대한 관리자 액세스 권한을 얻습니다.

사전 요구 사항

요구 사항

Cisco는 다음 주제에 대해 알고 있는 것을 권장합니다.

- 비밀번호 및 인증서 인증을 위한 ISE 컨피그레이션.
- Microsoft AD(Active Directory)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ISE(Identity Services Engine) 버전 2.6
- Windows AD(Active Directory) Server 2008 릴리스 2
- 인증서

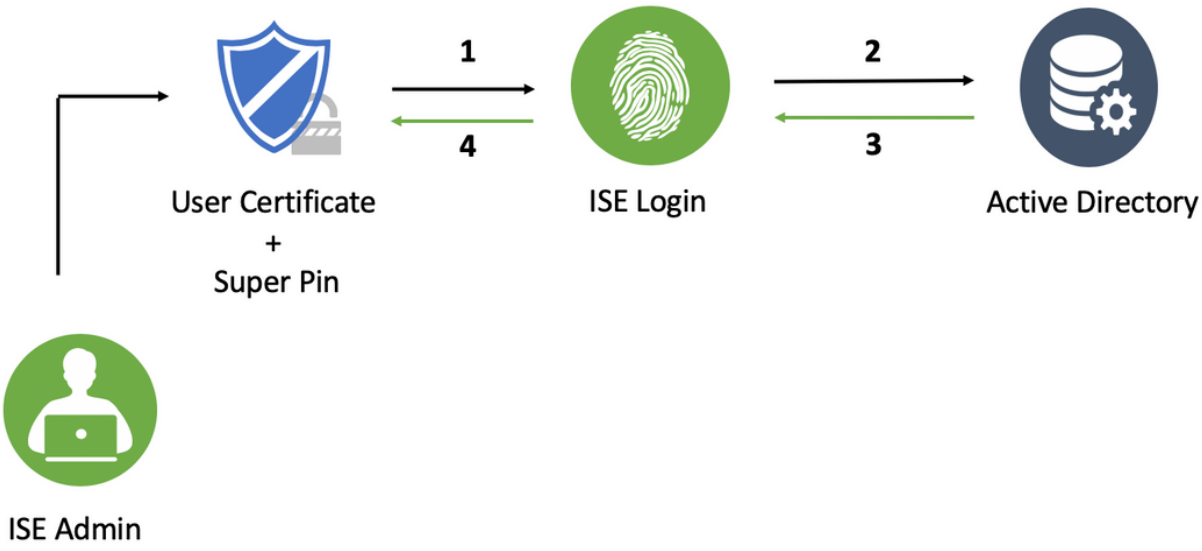
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바

이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.네트워크가 작동 중인 경우 모든 컨피그레이션의 잠재적인 영향을 이해해야 합니다.

구성

이 섹션에서는 Cisco ISE 관리 GUI에 대한 관리 액세스를 위해 클라이언트 인증서 또는 스마트 카드를 외부 ID로 구성할 수 있습니다.

네트워크 다이어그램

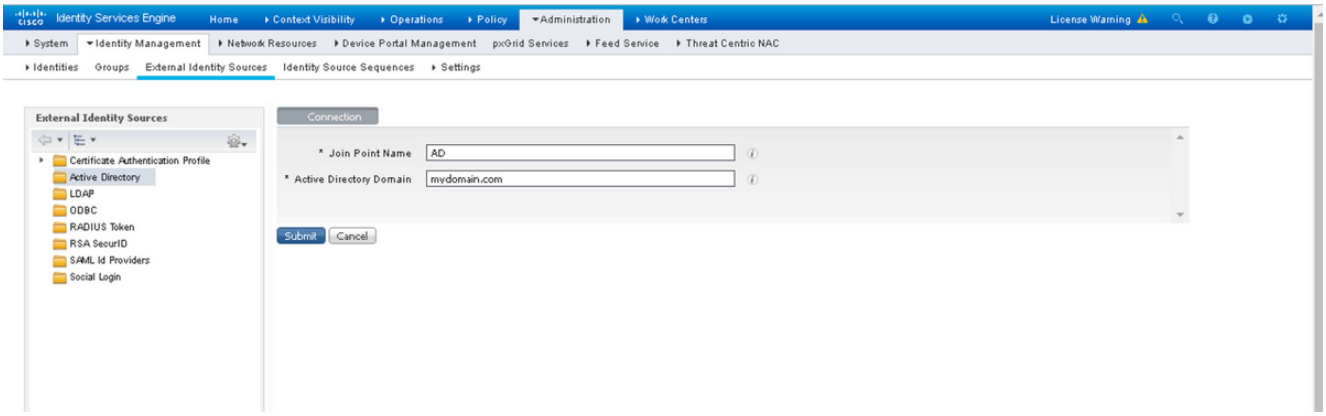


Active Directory에 ISE 가입

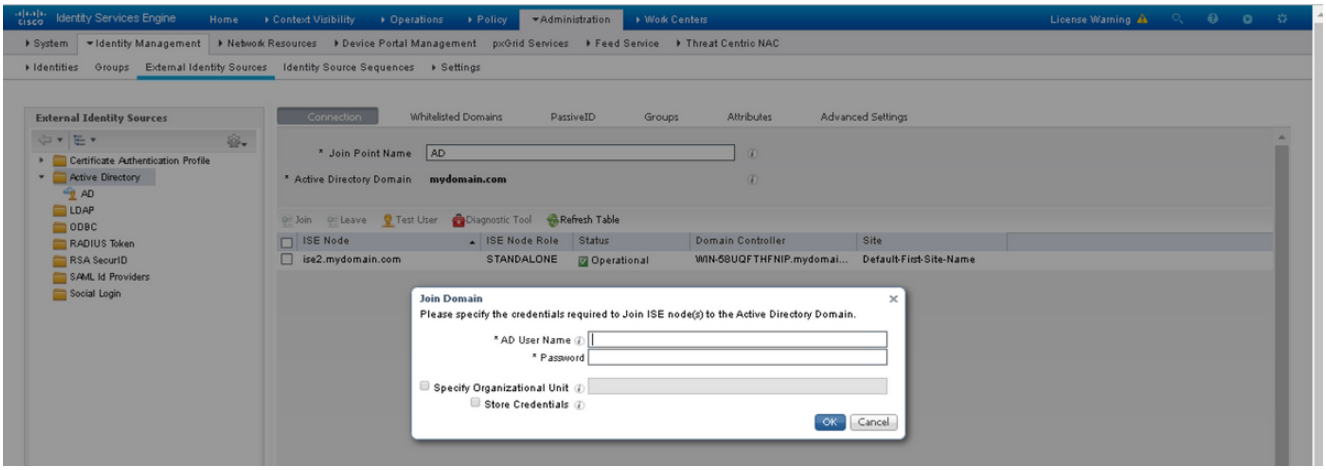
1. 관리 **선택 > ID 관리 > 외부 ID 소스 > Active Directory.**

2. Cisco ISE에서 **Join Point 이름** 및 **AD 도메인**을 사용하여 Active Directory 인스턴스를 생성합니다.

3. Submit(제출)**을 클릭합니다**.



4. 프롬프트에서 적절한 **사용자 이름** 및 **비밀번호**를 사용하여 모든 노드를 조인합니다.



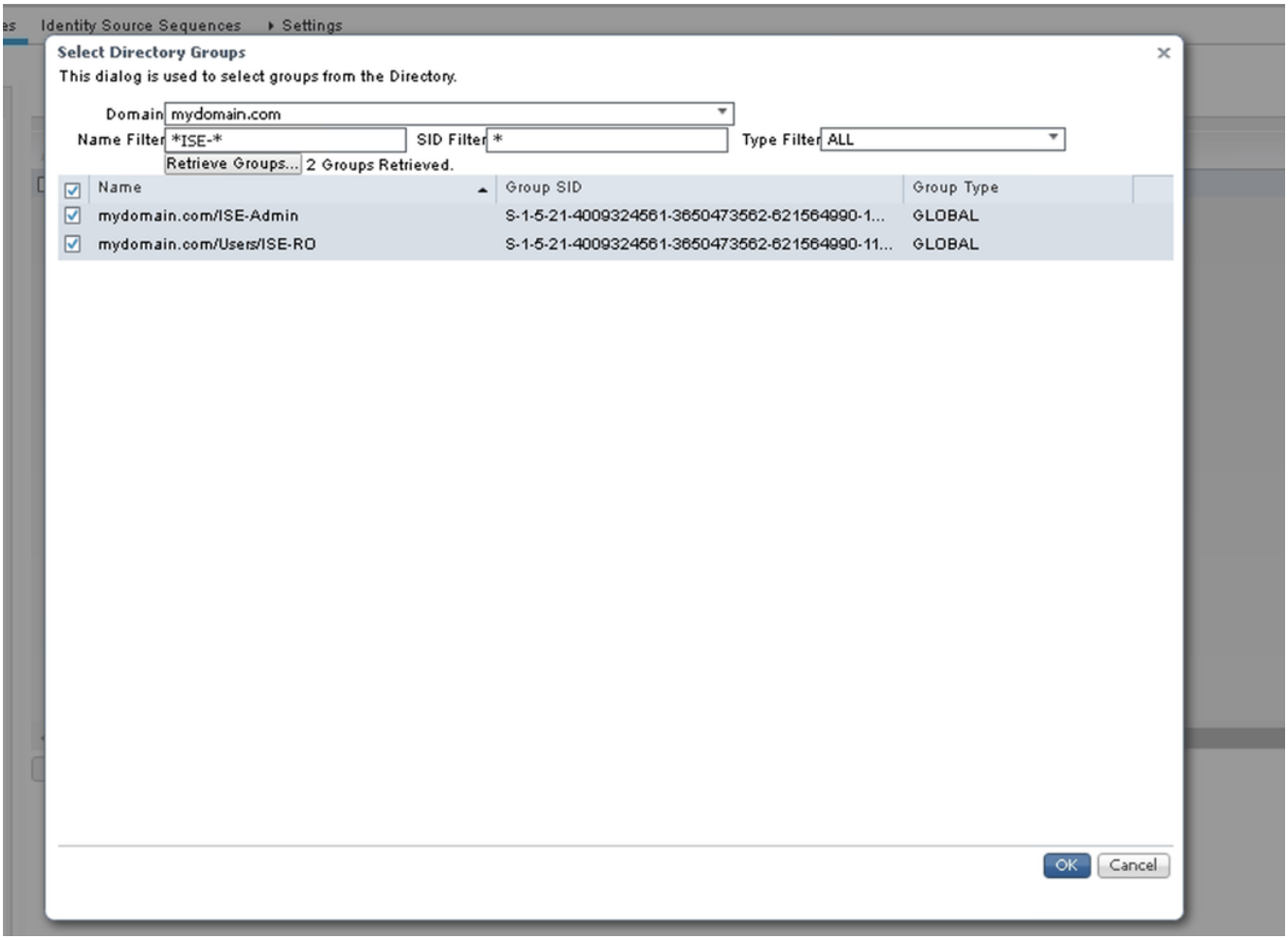
5. 저장을 **클릭합니다**.

디렉터리 그룹 선택

1. 외부 관리자 그룹을 만들고 Active Directory 그룹에 매핑합니다.

2. 관리 **> 선택ID 관리 > 외부 ID 소스 > Active Directory > 그룹 > 디렉터리에서 그룹 선택.**

3. 관리자가 속한 AD 그룹을 하나 이상 검색합니다.

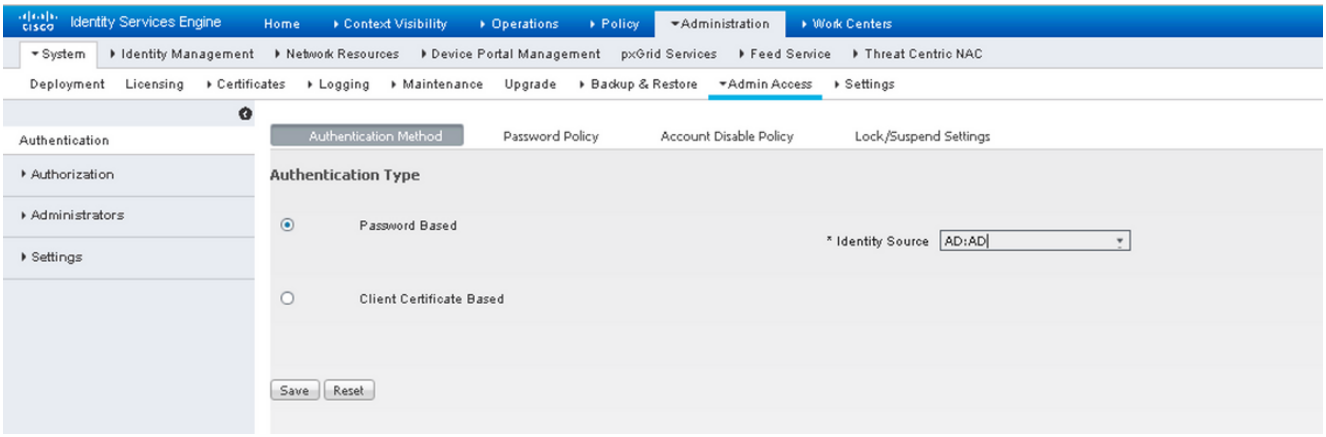


4. 저장을 **클릭합니다**.

관리 액세스에 Active Directory 암호 기반 인증 사용

1. Active Directory 인스턴스를 이전에 ISE에 가입된 비밀번호 기반 인증 방법으로 활성화합니다 .

2. 이미지에 표시된 대로 **Administration > System > Admin access > Authentication**을 선택합니다.



3. 저장을 **클릭합니다**.

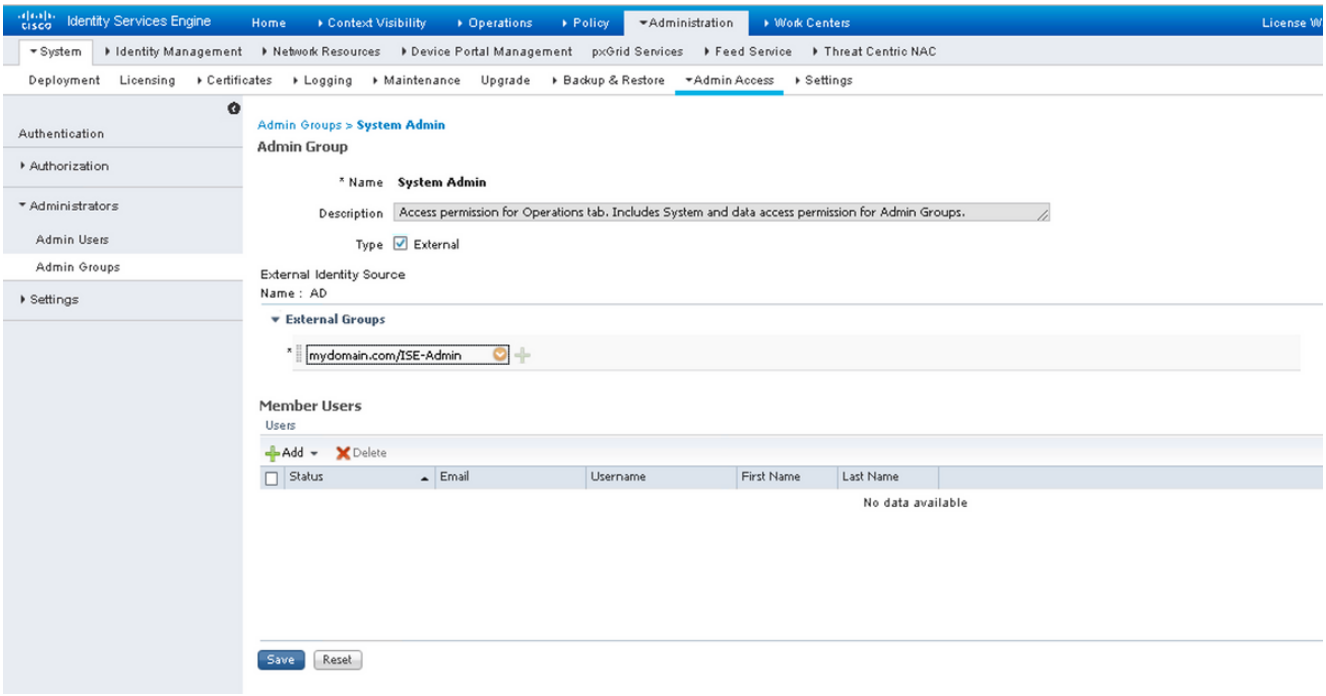
   참고:인증서 기반 인증을 활성화하려면 비밀번호 기반 인증 컨피그레이션이 필요합니다.인증서 기반 인증을 성공적으로 구성한 후 이 컨피그레이션을 되돌려야 합니다.

외부 ID 그룹을 관리 그룹에 매핑

이 예에서는 외부 AD 그룹이 기본 관리 그룹에 매핑됩니다.

1. Administration(**관리**) **>System(시스템) > Admin Access(관리 액세스) > Administrators(관리자)를 선택합니다.Admin Groups(관리자 그룹) > Super admin(수퍼 관리자)입니다.**

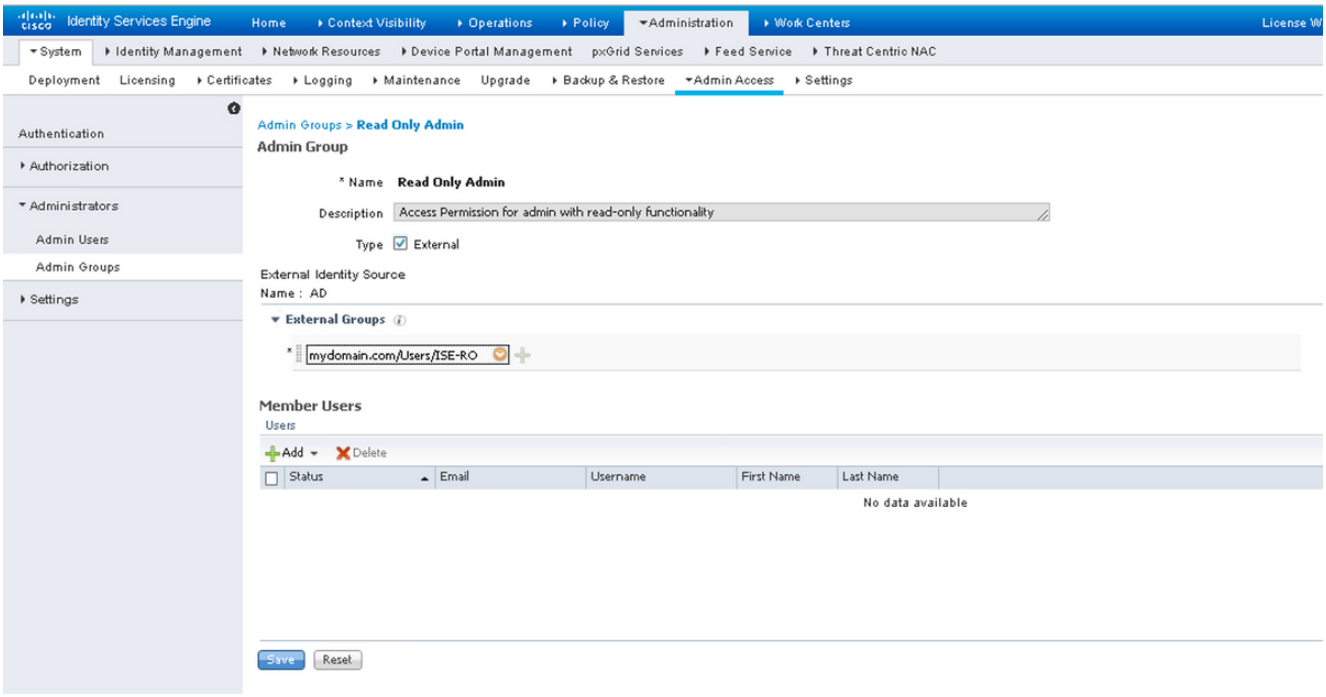
2. Type as External(**외부**으로 유형)을 선택하고 External groups(**외부 그룹**)에서 AD 그룹을 선택합니다.



3. 저장을 **클릭합니다**.

4. Administration(**관리**) > **System(시스템)** > **Admin Access(관리 액세스)** > **Administrators(관리자)** > **Admin Groups(관리 그룹)** > **Read Only Admin(읽기 전용 관리자)**을 **선택합니다**.

5. Type as External(**외부**으로 유형)을 선택하고 이미지에 표시된 대로 **External groups(외부 그룹)** 아래에서 AD 그룹을 선택합니다.



6. 저장을 **클릭합니다**.

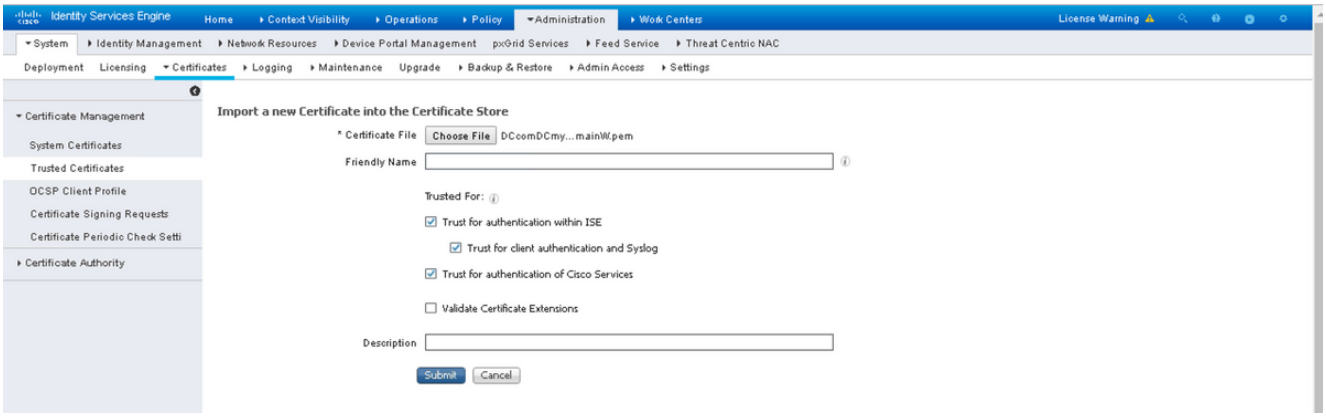
신뢰할 수 있는 인증서 가져오기

1. 클라이언트 인증서를 서명하는 CA(Certificate Authority) 인증서를 가져옵니다.

2. 선택 **Administrator > System > Certificates > Trusted Certificate > Import를 선택합니다.**

3. browse(찾아보기)를 클릭하고 CA 인증서를 선택합니다.

4. 이미지에 표시된 대로 **Trust for client authentication and Syslog 확인란**을 선택합니다.



5. 제출을 **클릭합니다.**

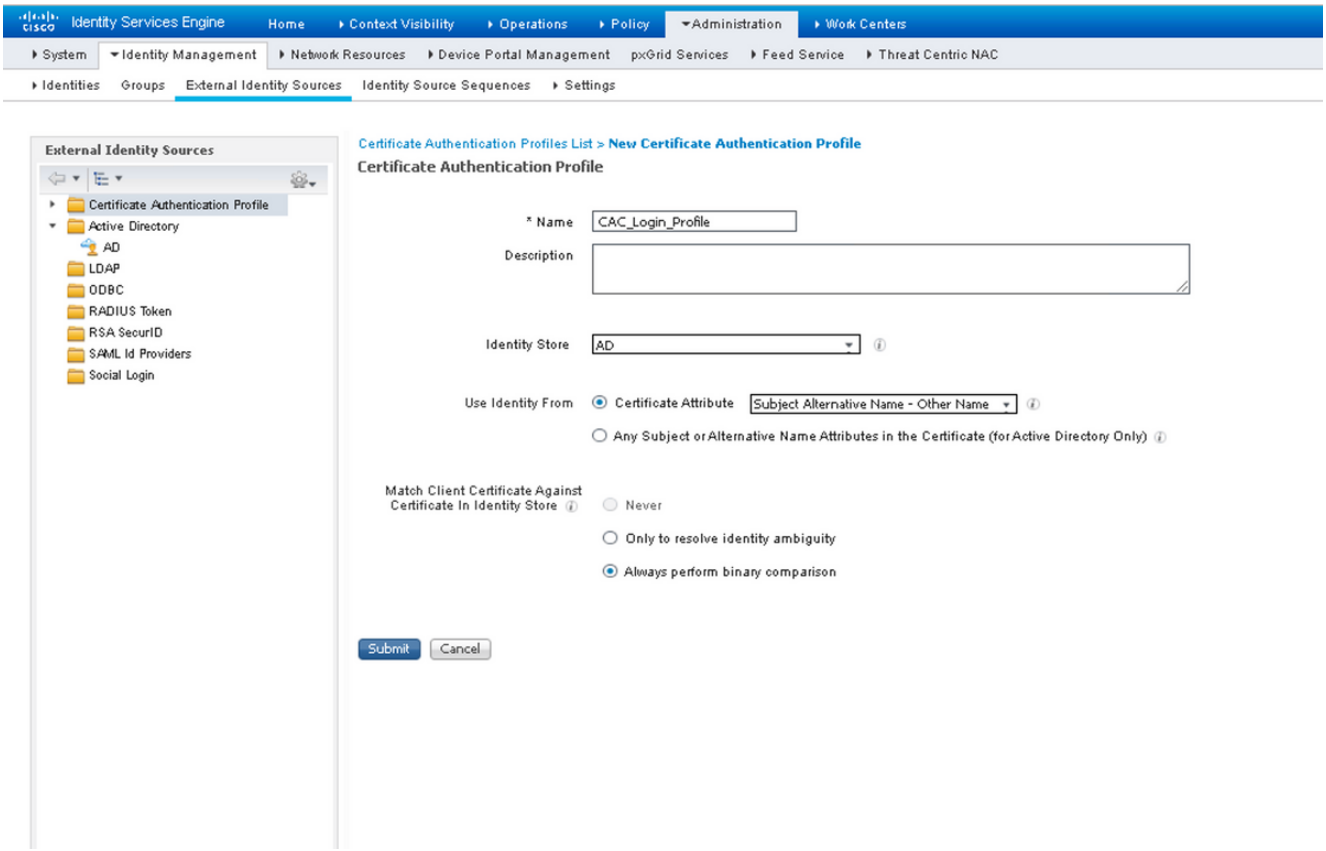
인증서 인증 프로파일 구성

1. 클라이언트 인증서 기반 인증을 위한 인증서 인증 프로파일을 생성하려면 Administration(관리) **>ID 관리 > 외부 ID 소스 > 인증서 인증 프로파일 > 추가.**

2. 프로필 이름을 추가합니다.

3. 인증서 속성에서 관리자 사용자 이름을 포함하는 적절한 특성을 선택합니다.

4. 사용자의 AD 레코드에 사용자의 인증서가 포함되어 있고 브라우저에서 받은 인증서를 AD의 인증서와 비교하려면 **항상 이진 비교** 수행 확인란을 선택하고 이전에 지정된 Active Directory 인스턴스 이름을 선택합니다.

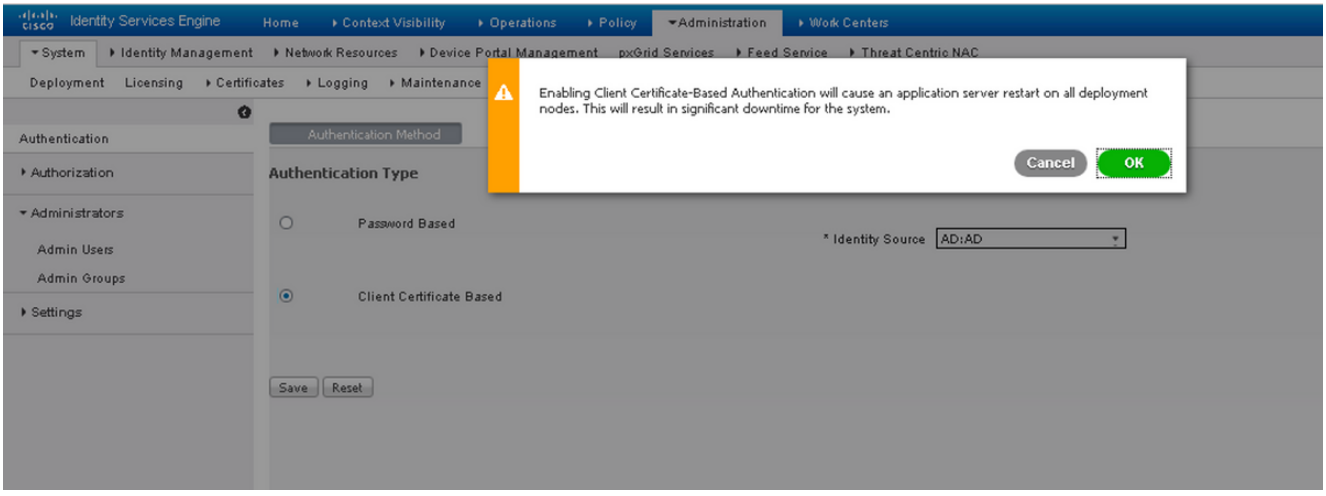


5. 제출을 **클릭합니다.**

참고:엔드포인트 ID 기반 인증에도 동일한 인증서 인증 프로파일을 사용할 수 있습니다.

클라이언트 인증서 기반 인증 활성화

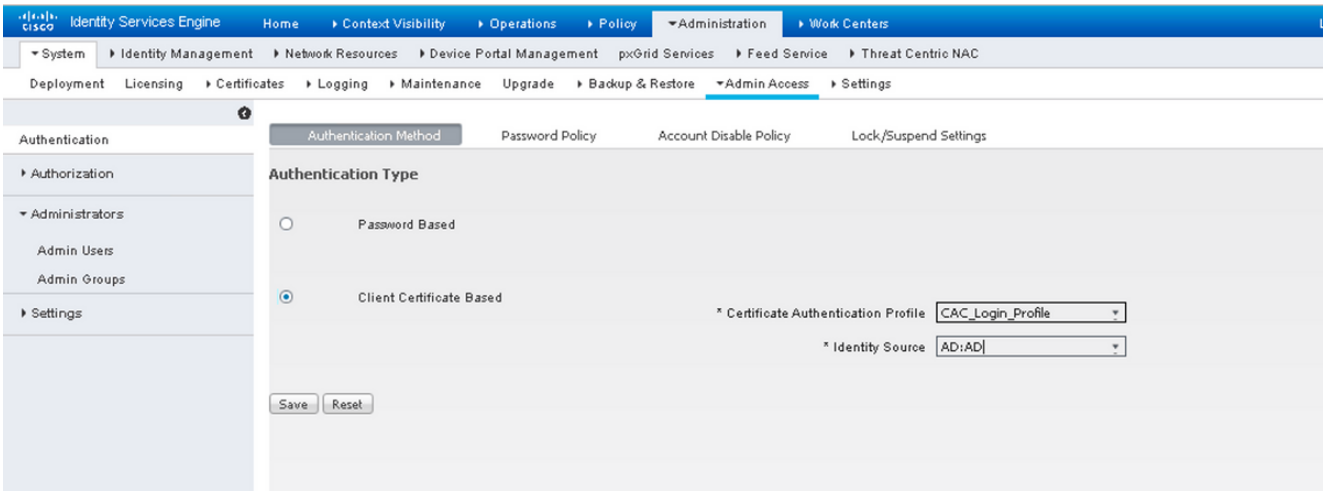
1. 선택 **관리 > 시스템 > 관리 액세스 > 인증 > 인증 방법 클라이언트 인증서 기반.**



2. **확인**을 **클릭합니다.**

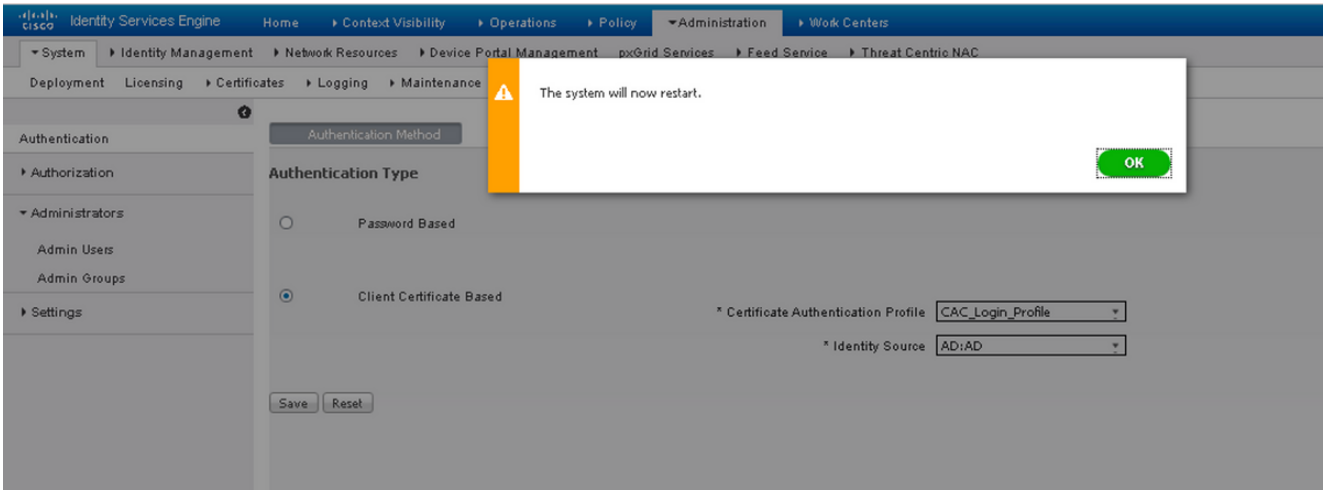
3. 이전에 구성된 **인증서 인증 프로파일**을 선택합니다.

4. Active Directory 인스턴스 이름을 선택합니다.



5. 저장을 **클릭합니다**.

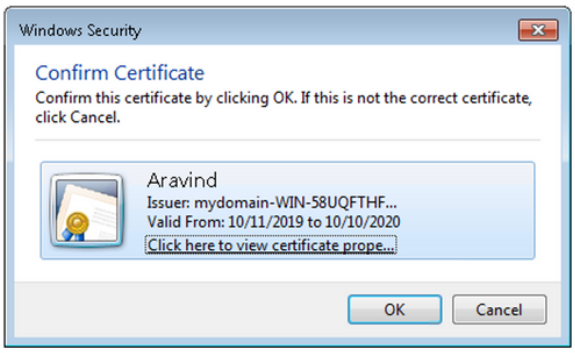
6. 구축의 모든 노드에서 ISE 서비스가 다시 시작됩니다.

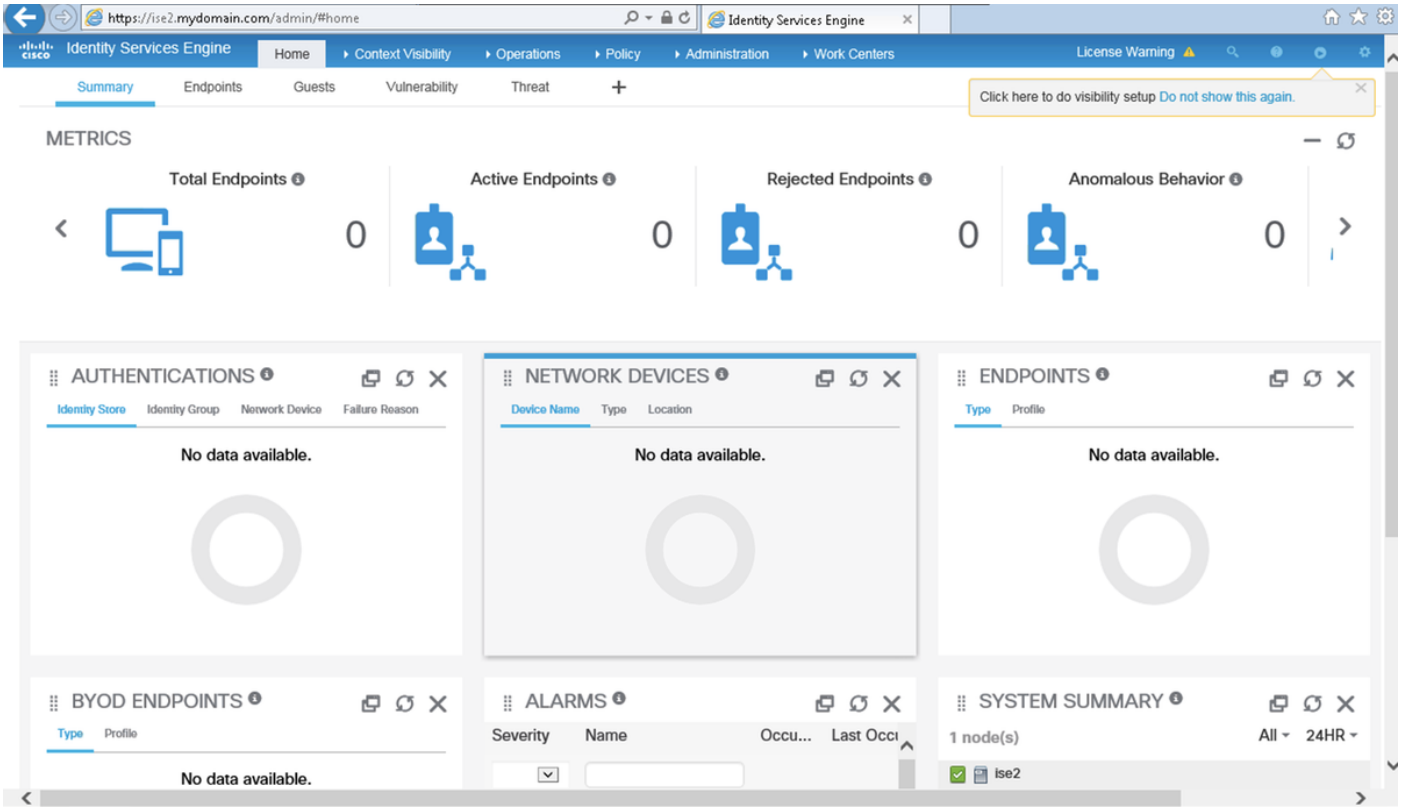


다음을 확인합니다.

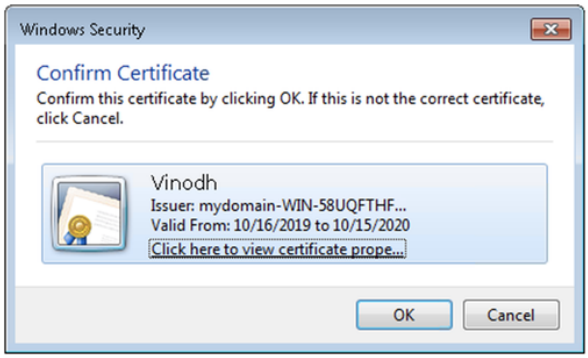
Application Server 서비스 상태가 **실행**으로 변경된 후 ISE GUI에 대한 액세스를 **확인합니다.**

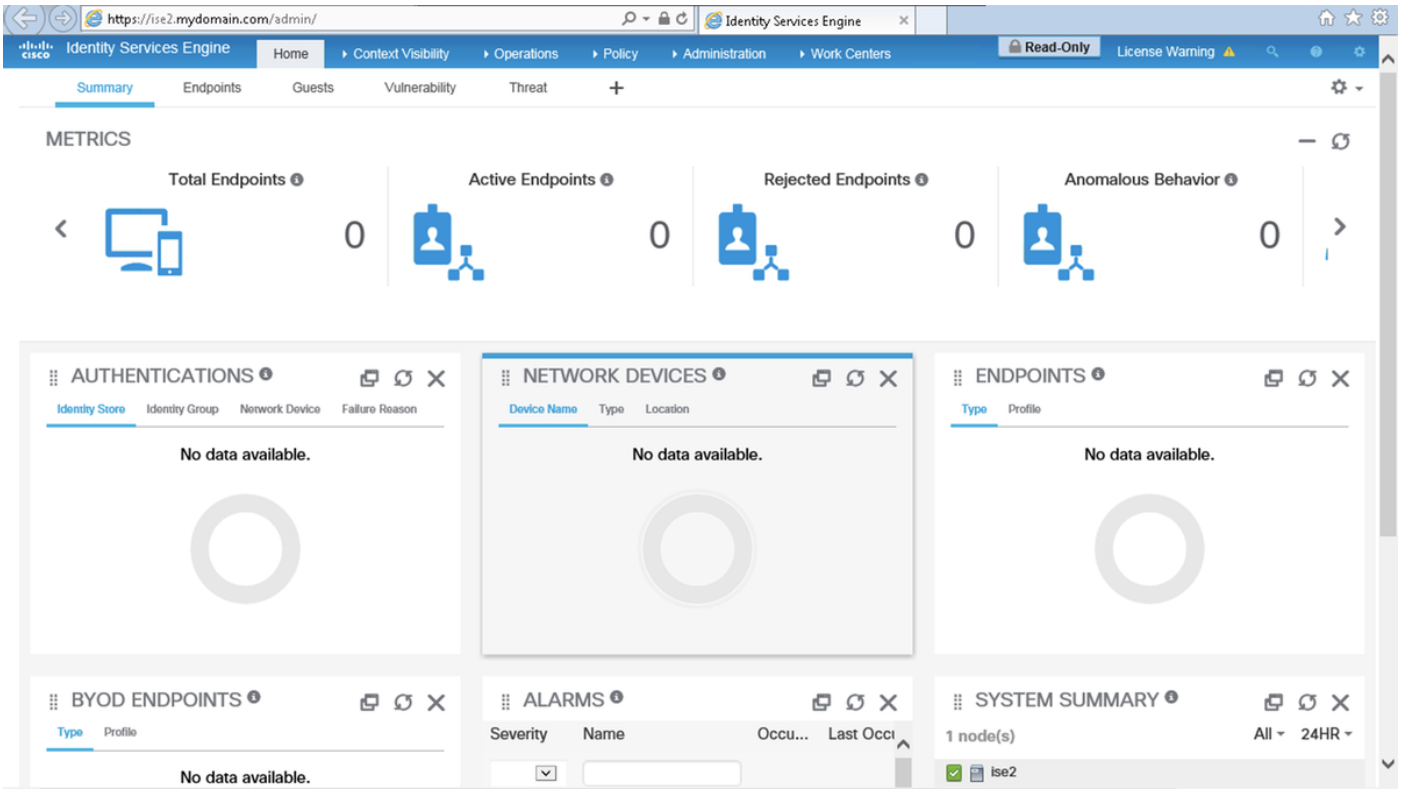
수퍼 관리자 사용자: ISE GUI에 로그인할 인증서를 선택하라는 메시지가 표시되고 인증서가 수퍼 관리자 외부 ID 그룹의 사용자 일부인 경우 수퍼 관리자 권한이 사용자에게 제공되는지 확인합니다 .





읽기 전용 관리자 사용자: ISE GUI에 로그인할 인증서를 선택하라는 메시지가 사용자에게 표시되고 인증서가 읽기 전용 관리자 외부 ID 그룹의 사용자 일부인 경우 읽기 전용 관리자 권한이 사용자에게 제공되는지 확인합니다.





참고:CAC(Common Access Card)가 사용 중인 경우, 사용자가 유효한 PIN을 입력한 후 스마트 카드는 ISE에 사용자 인증서를 제공합니다.

문제 해결

1. **application start ise safe** 명령을 사용하여 관리 포털에 대한 액세스 제어를 일시적으로 비활성화하고 컨피그레이션을 수정하고 명령 **애플리케이션 중지 ise**와 **애플리케이션 시작 ise**를 사용하여 ISE의 서비스를 다시 시작할 수 있는 안전 모드에서 Cisco ISE를 시작합니다..
2. 안전 옵션은 관리자가 실수로 모든 사용자에 대한 Cisco ISE 관리 포털에 대한 액세스를 잠근

경우 복구 방법을 제공합니다.이 이벤트는 관리자가 **Administration(관리) > Admin Access(관리 액세스) > Settings(설정) > Access(액세스) 페이지**에서 잘못된 **IP Access(IP 액세스**) 목록**을** 구성한 경우 발생할 수 있습니다.또한 **안전** 옵션**은 인증서 기반 인증을 우회하고** Cisco ISE 관리 포털에 로그인하기 위한 기본 사용자 이름 및 비밀번호 인증으로 돌아갑니다.