ISE에서 인증서 갱신 구성

목차

소개

이 문서에서는 Cisco ISE(Identity Services Engine)에서 인증서 갱신에 대한 모범 사례 및 사전 절차를 설명합니다. 또한 알람 및 알림을 설정하는 방법도 검토하여 인증서 만료와 같은 임박한 이벤트에 대해 관리자에게 경고합니다.

> **참고:** 이 문서는 인증서에 대한 진단 설명서가 아닙니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- X509 인증서
- 인증서를 사용하여 Cisco ISE 설정

사용되는 구성 요소

"이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 가동 중인 경우 모든 명령의

잠재적인 영향을 이해해야 합니다."

- Cisco ISE 릴리스 3.0.0.458
- 어플라이언스 또는 VMware

배경 정보

ISE 관리자는 결국 ISE 인증서가 만료된다는 사실을 알게 됩니다. ISE 서버에 만료된 인증서가 있는 경우 만료된 인증서를 유효한 새 인증서로 바꾸지 않으면 심각한 문제가 발생할 수 있습니다.

> **참고:** EAP(Extensible Authentication Protocol)에 사용되는 인증서가 만료되면 클라이언트에서 더 이상 ISE 인증서를 신뢰하지 않기 때문에 모든 인증이 실패할 수 있습니다. ISE 관리 인증서가 만료되면 위험은 더욱 커집니다. 관리자는 더 이상 ISE에 로그인할 수 없으며, 분산된 구축은 더 이상 작동하지 않고 복제할 수 있습니다.

ISE 관리자는 기존 인증서가 만료되기 전에 ISE에 유효한 새 인증서를 설치해야 합니다. 이러한 사전 대응 방식은 다운타임을 방지하거나 최소화하며 최종 사용자에게 미치는 영향을 방지합니다. 새로 설치된 인증서의 기간이 시작되면 새 인증서에서 EAP/Admin 또는 기타 역할을 활성화할 수 있습니다.

ISE가 알람을 생성하고 기존 인증서가 만료되기 전에 새 인증서를 설치하도록 관리자에게 알리기 위해 ISE를 구성할 수 있습니다.

> **참고:** 이 문서에서는 인증서 갱신의 영향을 입증하기 위해 자체 서명 인증서로 ISE 관리 인증서를 사용하지만, 프로덕션 시스템에는 이 접근 방식을 사용하지 않는 것이 좋습니다. EAP 및 관리자 역할 모두에 CA 인증서를 사용하는 것이 좋습니다.

구성

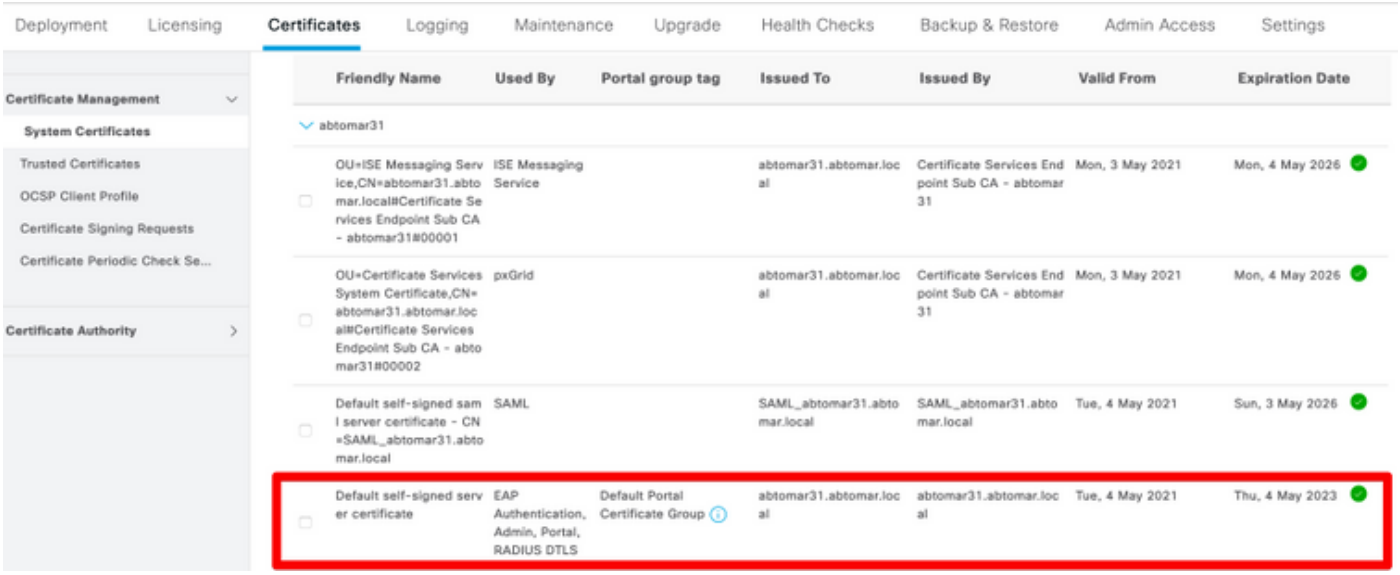
ISE 자체 서명 인증서 보기

ISE가 설치되면 자체 서명 인증서를 생성합니다. 자체 서명 인증서는 관리 액세스 및 분산형 구축(HTTPS) 내 통신은 물론 사용자 인증(EAP)에 사용됩니다. 라이브 시스템에서는 자체 서명 인증서 대신 CA 인증서를 사용합니다.

> **팁:** 자세한 내용은 Cisco Identity Services Engine 하드웨어 설치 가이드, 릴리스 3.0의 Cisco ISE의 인증서 관리 섹션을 참조하십시오.

ISE 인증서에 대한 형식은 PEM(Privacy Enhanced Mail) 또는 DER(Distinguished Encoding Rules) 형식이어야 합니다.

최초 자체 서명 인증서를 보려면 ISE GUI에서 **Administration(관리) > System(시스템) > Certificates(인증서) > System Certificates(시스템 인증서)**로 이동합니다.



CSR(인증서 서명 요청)을 통해 ISE에 서버 인증서를 설치하고 관리자 또는 EAP 프로토콜에 대한 인증서를 변경하는 경우, 자체 서명된 서버 인증서는 여전히 존재하지만 사용 중이 아닙니다.

> **주의:** 관리 프로토콜 변경의 경우 ISE 서비스를 다시 시작해야 하므로 몇 분 동안 다운타임이 발생합니다. EAP 프로토콜 변경으로 인해 ISE 서비스가 다시 시작되지 않으며 다운타임이 발생하지 않습니다.

인증서 변경 시기 결정

설치된 인증서가 곧 만료된다고 가정합니다. 인증서를 갱신하기 전에 만료하도록 두는 것과 만료 전에 인증서를 변경하는 것 중에 무엇이 더 낫습니까? 인증서 교환을 계획하고 교환으로 인한 다운타임을 관리할 시간을 가질 수 있도록 만료 전에 인증서를 변경해야 합니다.

언제 인증서를 변경해야 합니까? 시작 날짜가 이전 인증서 만료일 이전인 새 인증서를 가져옵니다. 이 두 날짜 사이의 기간은 변경 기간입니다.

> **주의:** 관리자를 활성화하면 ISE 서버에서 서비스가 재시작되고 몇 분 동안의 다운타임이 발생합니다.

이 이미지는 곧 만료되는 인증서에 대한 정보를 보여줍니다.

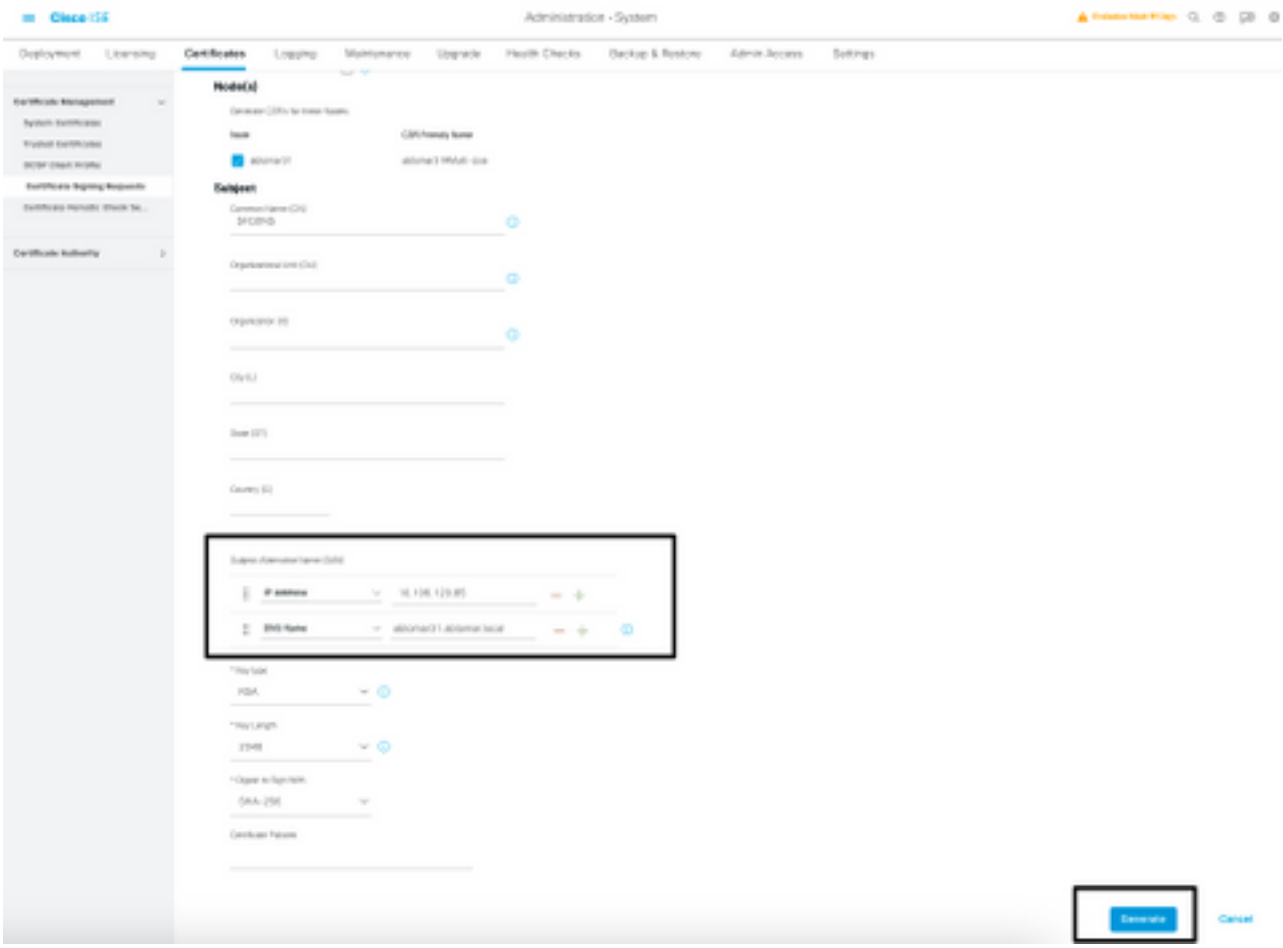
인증서 서명 요청 생성

이 절차에서는 CSR을 통해 인증서를 갱신하는 방법을 설명합니다.

1. ISE 콘솔에서 **Administration(관리) > System(시스템) > Certificates(인증서) > Certificates Signing Requests(인증서 서명 요청)**로 이동하고 **Generate Certificate Signing Request:(인증서 서명 요청 생성:)를 클릭합니다.**

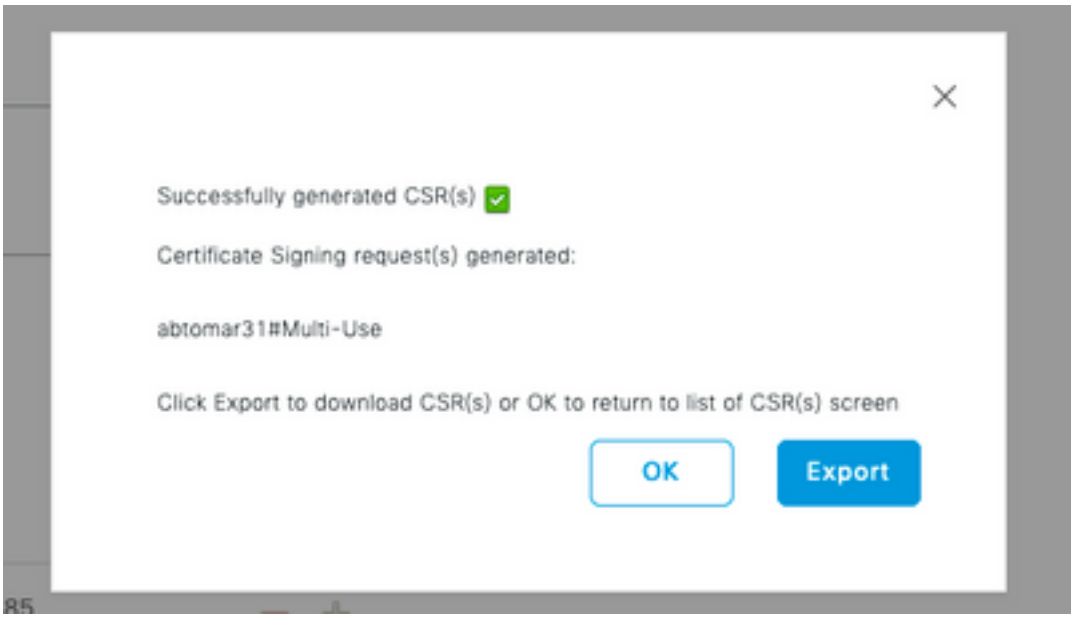
2. **인증서 주체** 텍스트 필드에 입력해야 하는 최소 정보는 CN=*ISEfqdn*입니다. 여기서 *ISEfqdn*은

ISE의 FQDN(Fully Qualified Domain Name)입니다. 쉼표를 사용하여 인증서 주체에 O(Organization), OU(Organizational Unit) 또는 C(Country)와 같은 추가 필드를 추가합니다.



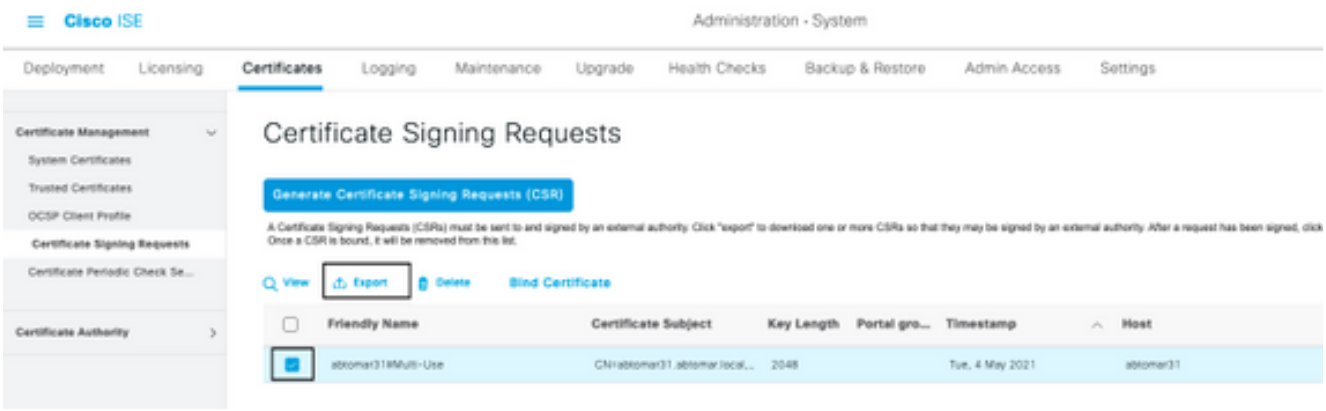
3. **SAN(Subject Alternative Name)** 텍스트 필드 행 중 하나가 ISE FQDN을 반복해야 합니다. 대체 이름 또는 와일드카드 인증서를 사용하려는 경우 두 번째 SAN 필드를 추가할 수 있습니다.

4. **Generate(생성)**를 클릭하면 CSR 필드가 올바르게 완료되었는지 여부를 나타내는 팝업 창이 표시됩니다.



5. CSR을 내보내려면 왼쪽 패널에서 **Certificate Signing Requests(인증서 서명 요청)**를 클릭하

고 CSR을 선택한 다음 **Export(내보내기)**를 클릭합니다.

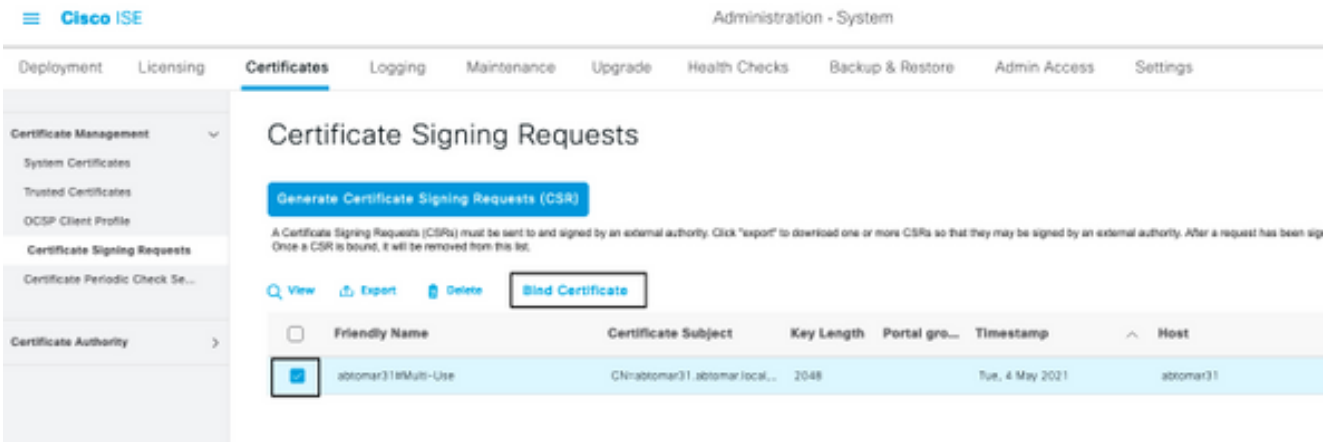


6. CSR은 컴퓨터에 저장됩니다. 서명을 위해 CA에 제출합니다.

인증서 설치

CA에서 최종 인증서를 받으면 ISE에 인증서를 추가해야 합니다.

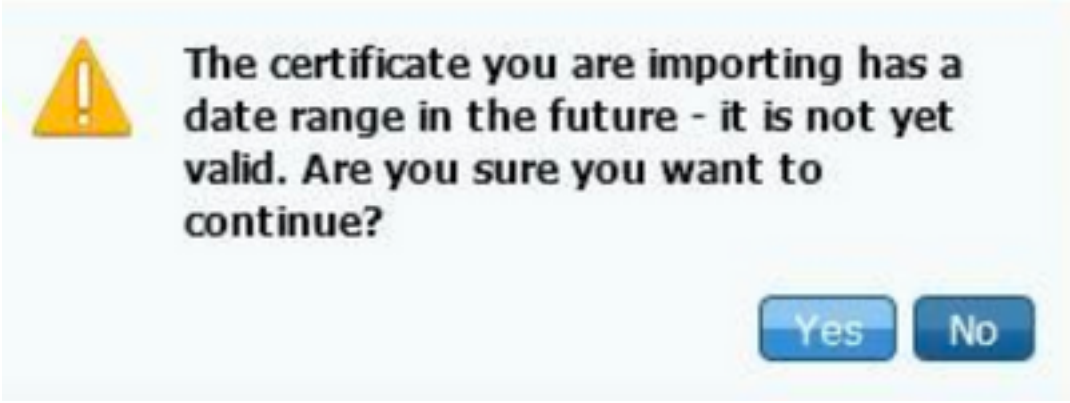
1. ISE 콘솔에서 **Administration(관리) > System(시스템) > Certificates(인증서) > Certificate Signing Requests(인증서 서명 요청)**로 이동한 다음 CRS의 확인란을 선택하고 **Bind Certificate(인증서 바인딩)**를 클릭합니다.



2. **Friendly Name(식별 이름)** 텍스트 필드에 인증서에 대한 간단하고 명확한 설명을 입력하고 제출을 누릅니다.

   참고: 지금은 EAP 또는 관리 프로토콜을 활성화하지 마십시오.
3. 시스템 인증서 아래에 다음과 같이 사용되지 않은 새 인증서가 있습니다.

4. 기존 인증서가 만료되기 전에 새 인증서가 설치되었으므로 미래의 날짜 범위를 보고하는 오류가 표시됩니다.



5. 계속하려면 **Yes(예)**를 클릭합니다. 이제 녹색으로 강조 표시된 것과 같이 인증서가 설치되었지만 사용되지 않습니다.

참고: 분산형 구축에서 자체 서명 인증서를 사용하는 경우 기본 자체 서명 인증서를 보조 ISE 서버의 신뢰할 수 있는 인증서 저장소에 설치해야 합니다. 마찬가지로 보조 자체 서명 인증서는 기본 ISE 서버의 신뢰할 수 있는 인증서 저장소에 설치해야 합니다. 이를 통해 ISE 서버가 상호 인증할 수 있습니다. 이 기능이 없으면 구축이 중단될 수 있습니다. 서드파티 CA에서 인증서를 갱신하는 경우 루트 인증서 체인이 변경되었는지 확인하고 ISE에서 신뢰할 수 있는 인증서 저장소를 적절하게 업데이트합니다. 두 시나리오 모두 ISE 노드, 엔드포인트 제어 시스템 및 신청자가 루트 인증서 체인을 확인할 수 있는지 확인합니다.

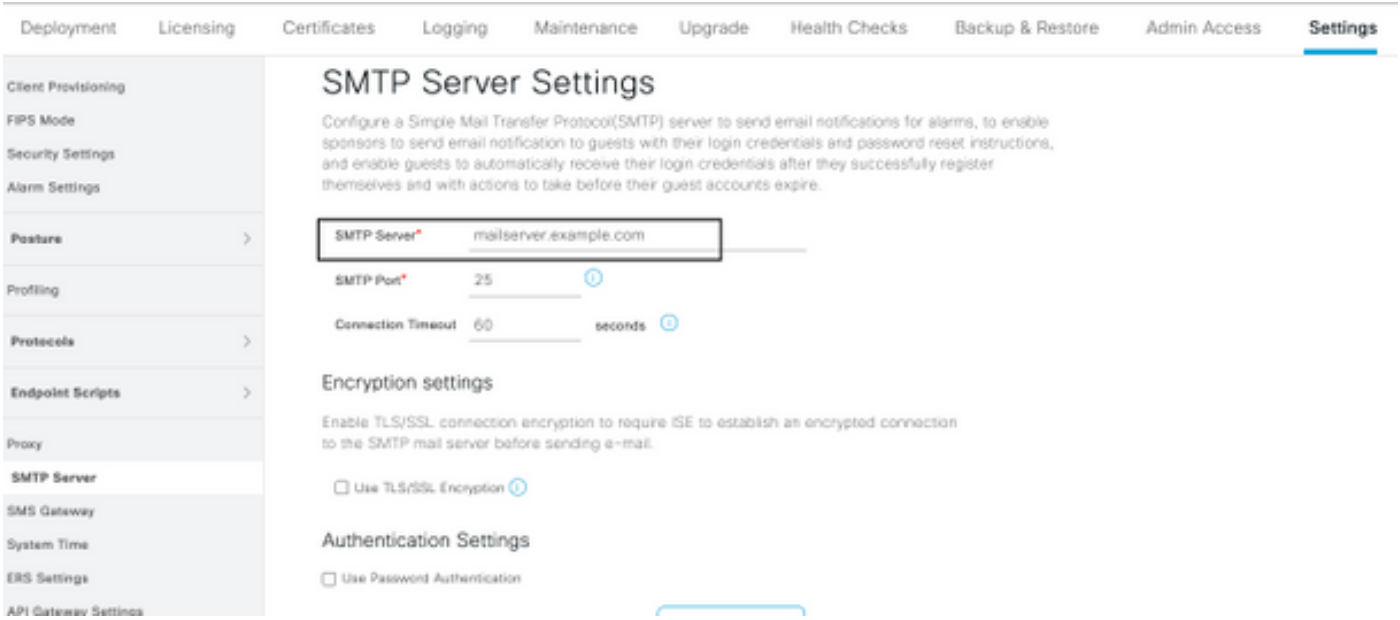
알림 시스템 구성

Cisco ISE에서는 로컬 인증서의 만료 날짜가 90일 미만일 때 알림을 보냅니다. 이러한 사전 알림을 통해 인증서 만료를 방지하고 인증서 변경을 계획하며 다운타임을 방지하거나 최소화할 수 있습니다.

알림은 다음과 같은 여러 가지 방법으로 표시됩니다.

- Local Certificates(로컬 인증서) 페이지에 색상이 지정된 만료 상태 아이콘이 나타납니다.
- Cisco ISE 시스템 진단 보고서에 만료 메시지가 나타납니다.
- 만료 전 90일과 60일, 그리고 마지막 30일 동안에는 매일 만료 알람이 생성됩니다.

만료 알람의 이메일 알림을 위해 ISE를 구성합니다. ISE 콘솔에서 **Administration(관리) > System(시스템) > Settings(설정) > SMTP Server(SMTP 서버)**로 이동하여 SMTP(Simple Mail Transfer Protocol) 서버를 식별하고, 알람에 대한 이메일 알림이 전송되도록 다른 서버 설정을 정의합니다.

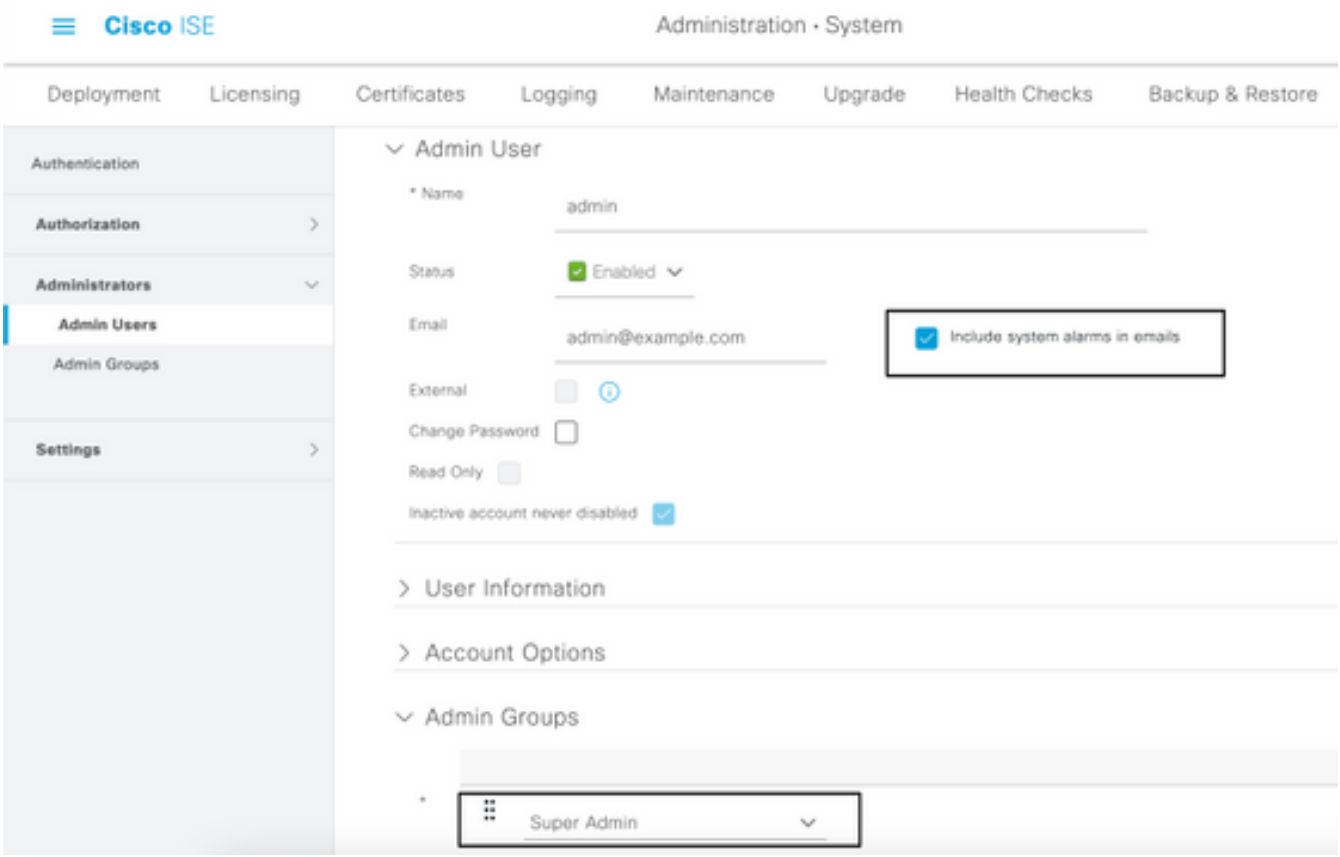


알림을 설정할 수 있는 두 가지 방법이 있습니다.

- 관리자에게 알림을 보내기 위해 관리자 액세스 사용:

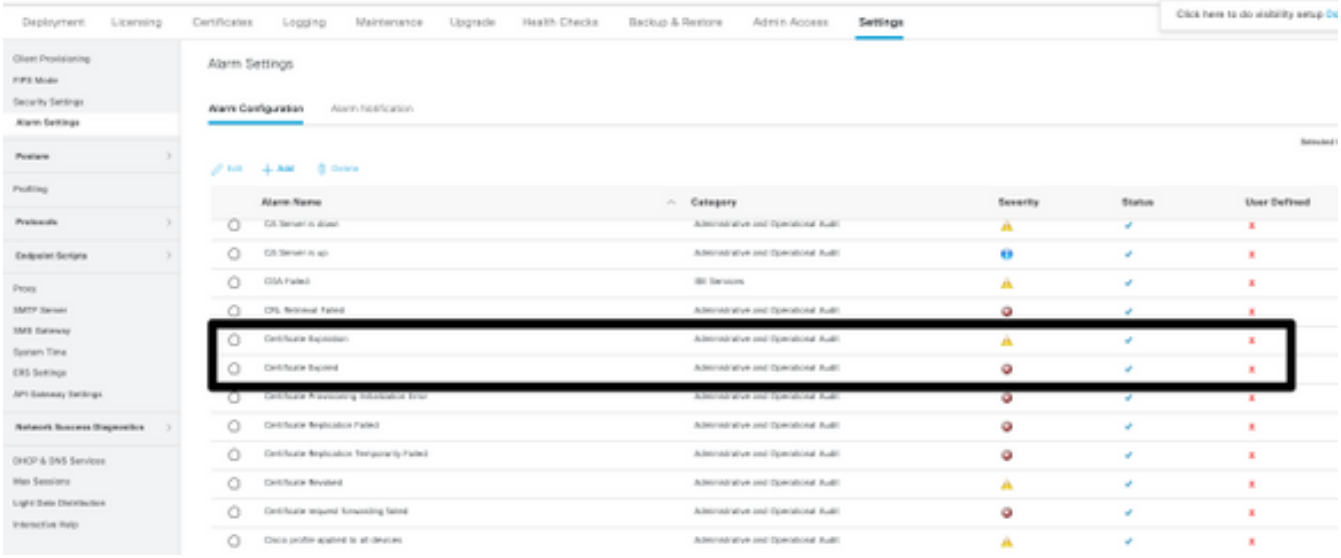
  Administration(관리) > System(시스템) > Admin Access(관리자 액세스) > Administrators(관리자) > (Admin Users)관리자 사용자로 이동합니다.

  알람 알림을 수신해야 하는 관리자 사용자에 대해 **이메일에 시스템 알람 포함** 확인란을 선택합니다. 알람 알림을 보낸 사람의 이메일 주소는 ise@*호스트 이름*으로 하드 코드됩니다.

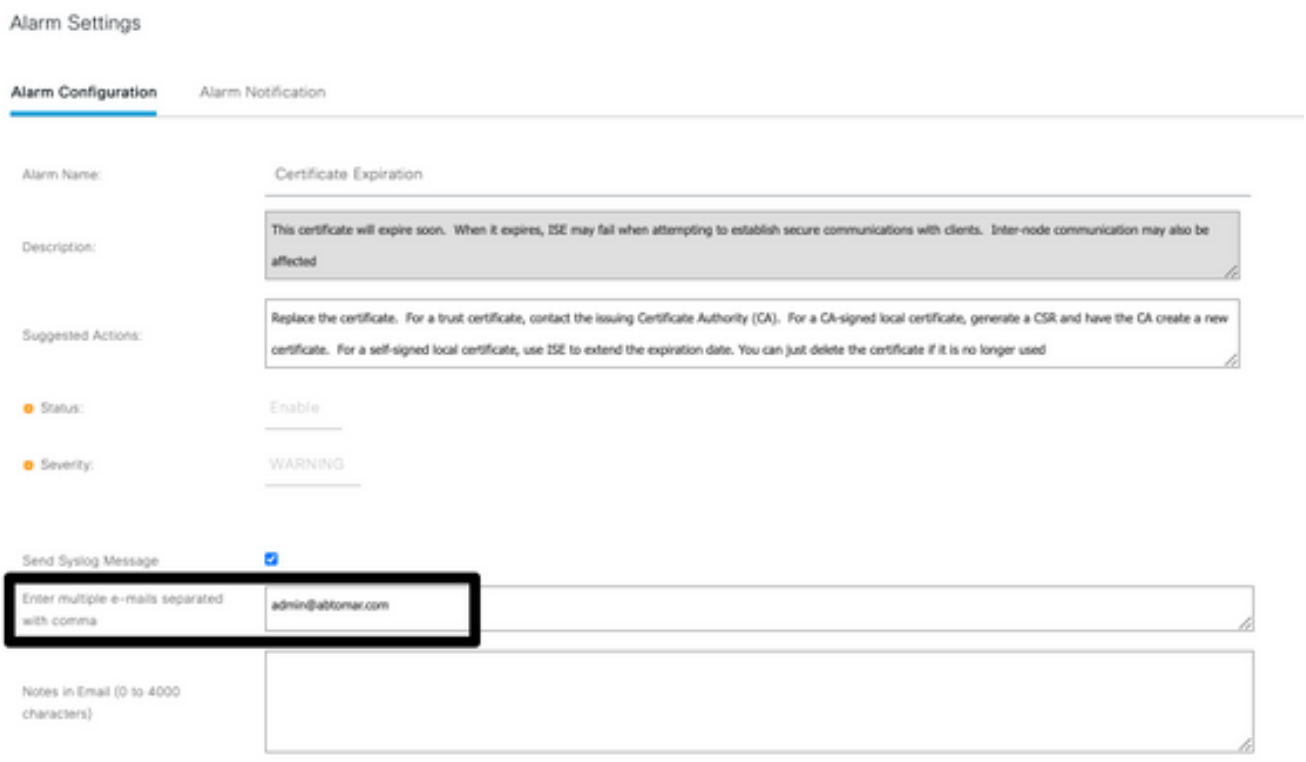


- 사용자에게 알림을 보내기 위해 ISE 경보 설정 구성:

이 이미지에 표시된 것과 같이 **Administration(관리) > System(시스템) > Settings(설정) > Alarm Settings(알람 설정) > Alarm Configuration(알람 구성)**으로 이동합니다.



참고: 해당 카테고리의 알람을 방지하려면 카테고리에 대한 Status (상태)를 비활성화합니다 .인증서 만료를 선택한 다음 **Alarm Notification(알람 알림)**을 클릭하고, 알림을 받을 사용자의 이메일 주소를 입력하고 구성 변경 사항을 저장합니다. 변경 사항은 활성화되기 전에 최대 15분이 소요될 수 있습니다.

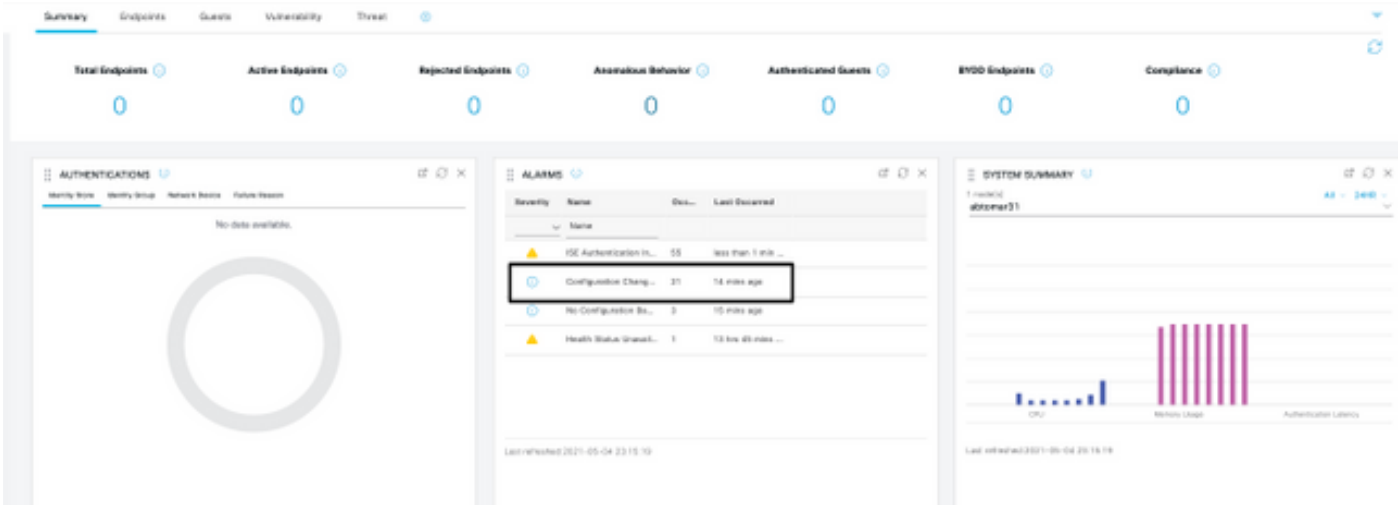


다음을 확인합니다.

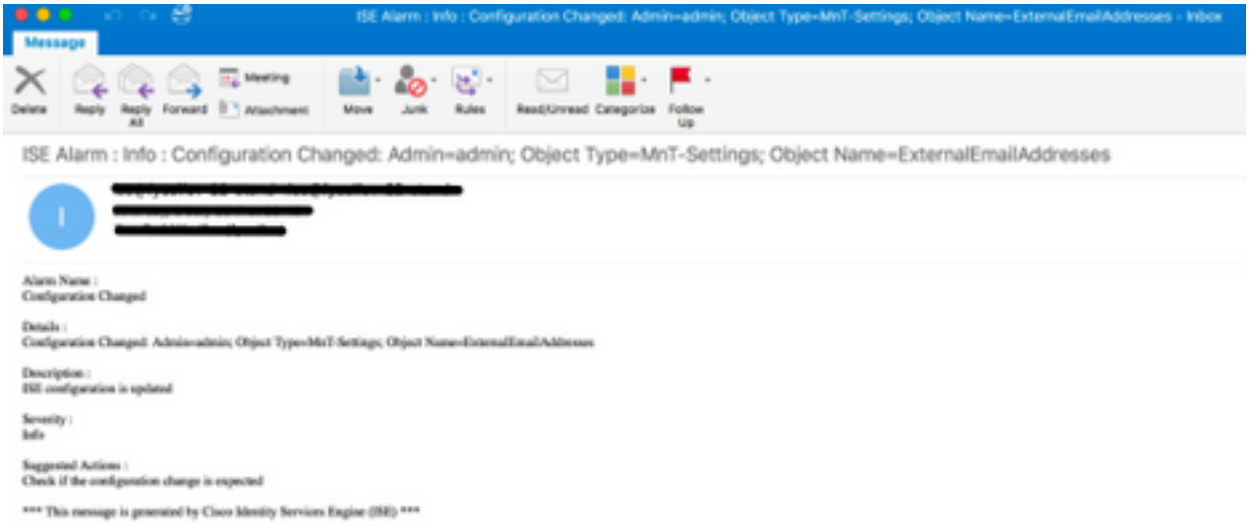
구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

알림 시스템 확인

알림 시스템이 올바르게 작동하는지 확인합니다. 이 예에서 구성을 변경하면 심각도 정보로 알림이 생성됩니다. (정보 알람은 심각도가 가장 낮은 반면 인증서 만료 시에는 심각도가 더 높은 경고가 생성됩니다.)



다음은 ISE에서 보내는 이메일 알람의 예입니다.

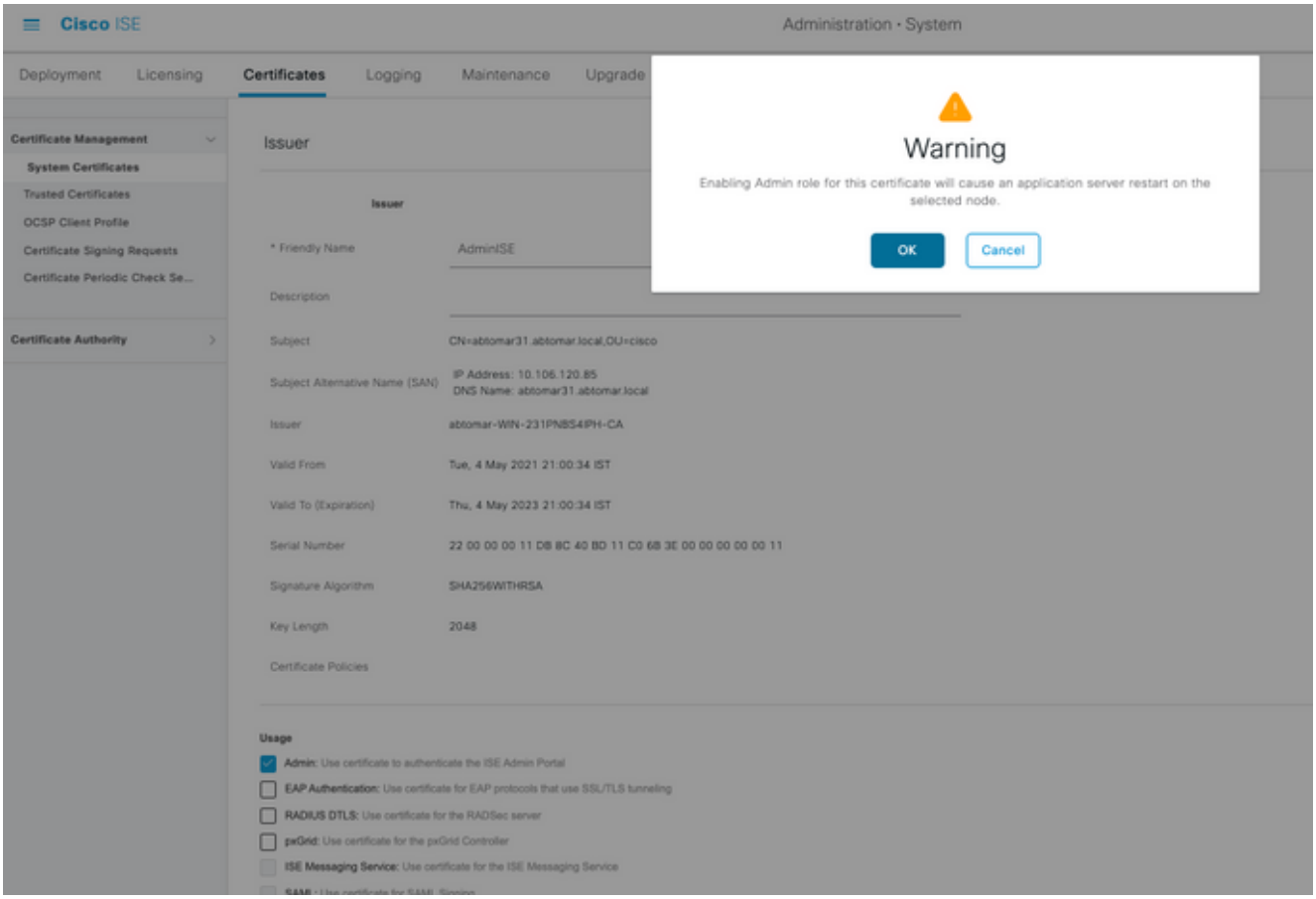


인증서 변경 확인

이 절차에서는 인증서가 올바르게 설치되었는지 확인하는 방법과 EAP 및/또는 관리자 역할을 변경하는 방법에 대해 설명합니다.

1. ISE 콘솔에서 **Administration(관리) > Certificates(인증서) > System Certificates(시스템 인증서)**로 이동하고 새 인증서를 선택하여 세부 정보를 확인합니다.

   주의: 관리자 사용을 활성화하면 ISE 서비스가 다시 시작되어 서버 다운타임이 발생합니다.



2. ISE 서버에서 인증서 상태를 확인하려면 CLI에 다음 명령을 입력합니다.

```
CLI:> show application status ise
```

3. 모든 서비스가 활성 상태가 되면 관리자로 로그인을 시도합니다.

4. 분산형 구축 시나리오의 경우 **Administration > System > Deployment로 이동합니다.** 노드에 녹색 아이콘이 있는지 확인합니다. 아이콘 위에 커서를 놓으면 범례에 "연결됨"이 표시되는지 확인합니다.

5. 최종 사용자 인증이 성공적인지 확인합니다. 이렇게 하려면 작업 > RADIUS **> 라이벨로그로 이동합니다.** 특정 인증 시도를 찾아 해당 시도가 성공적으로 인증되었는지 확인할 수 있습니다.

인증서 확인

인증서를 외부에서 확인하려는 경우 내장된 Microsoft Windows 툴 또는 OpenSSL 툴킷을 사용할 수 있습니다.

OpenSSL은 SSL(Secure Sockets Layer) 프로토콜의 오픈 소스 구현입니다. 인증서에서 자체 개인 CA를 사용하는 경우 루트 CA 인증서를 로컬 시스템에 배치하고 OpenSSL 옵션 *-CApath*를 사용해야 합니다. 중간 CA가 있는 경우 동일한 디렉토리에 배치해야 합니다.

인증서에 대한 일반 정보를 가져오고 이를 확인하려면 다음을 사용합니다.

```
openssl x509 -in certificate.pem -noout -text
openssl verify certificate.pem
```

OpenSSL 툴킷으로 인증서를 변환하는 것도 유용할 수 있습니다.

```
openssl x509 -in certificate.der -inform DER -outform PEM -out certificate.pem
```

문제 해결

현재 이 구성에 사용할 수 있는 특정 진단 정보가 없습니다.

결론

활성 상태가 되기 전에 ISE에 새 인증서를 설치할 수 있으므로 기존 인증서가 만료되기 전에 새 인증서를 설치하는 것이 좋습니다. 기존 인증서 만료일과 새 인증서 시작일 사이의 이 중복 기간은 인증서를 갱신하고 다운타임이 거의 또는 전혀 발생하지 않는 상태로 설치를 계획하는 시간을 제공합니다. 새 인증서가 유효한 날짜 범위에 들어가면 EAP 및/또는 관리자를 활성화합니다. 관리자 사용을 활성화하는 경우 서비스가 다시 시작됩니다.

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.