ISE에서 만료된 내부 OCSP 응답자 인증서 제거

목차

소개

이 문서에서는 Cisco ISE(Identity Service Engine)에서 만료된 OCSP Responder 인증서를 삭제하거나 만료 예정인 방법을 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ISE(Identity Service Engine)에 대한 기본 지식
- 인증서에 대한 기본 지식
- 온라인 인증서 상태 프로토콜(OCSP)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Identity Service Engine 3.x

이 문서의 정보는 특정 랩 환경의 장치에서 만들어졌습니다.이 문서에 사용된 모든 장치는 지워진 (기본) 구성으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

Cisco ISE(Identity Services Engine)를 사용하는 고객이 흔히 겪는 문제는 인증서가 만료되었음을 나타내는 경보를 수신하는 것입니다. 특히 OCSP responder 인증서가 만료되었거나 만료될 예정이고 인증서를 찾을 수 없는 경우 이러한 경보가 표시됩니다. 이러한 상황으로 인해 고객은 지원을 받기 위해 TAC 케이스를 열기도 합니다. 이 가이드의 목적은 고객이 만료되었거나 곧 만료될 OCSP responder 인증서를 직접 찾아 삭제할 수 있도록 지원함으로써 TAC 케이스를 제기할 필요가 없도록 하는 것입니다.

OCSP(Online Certificate Status Protocol)는 x.509 디지털 인증서의 상태를 확인하는 데 사용되는 프로토콜입니다. 이 프로토콜은 CRL(Certificate Revocation List)의 대안이며 CRL 처리로 인해 발생하는 문제를 해결합니다. Cisco ISE는 인증에서 인증서의 상태를 확인 하기 위해 HTTP를 통해 OCSP 서버와 통신 할 수 있습니다. OCSP 컨피그레이션은 Cisco ISE에 구성된 CA(Certificate Authority) 인증서에서 참조할 수 있는 재사용 가능한 컨피그레이션 객체로 구성됩니다.

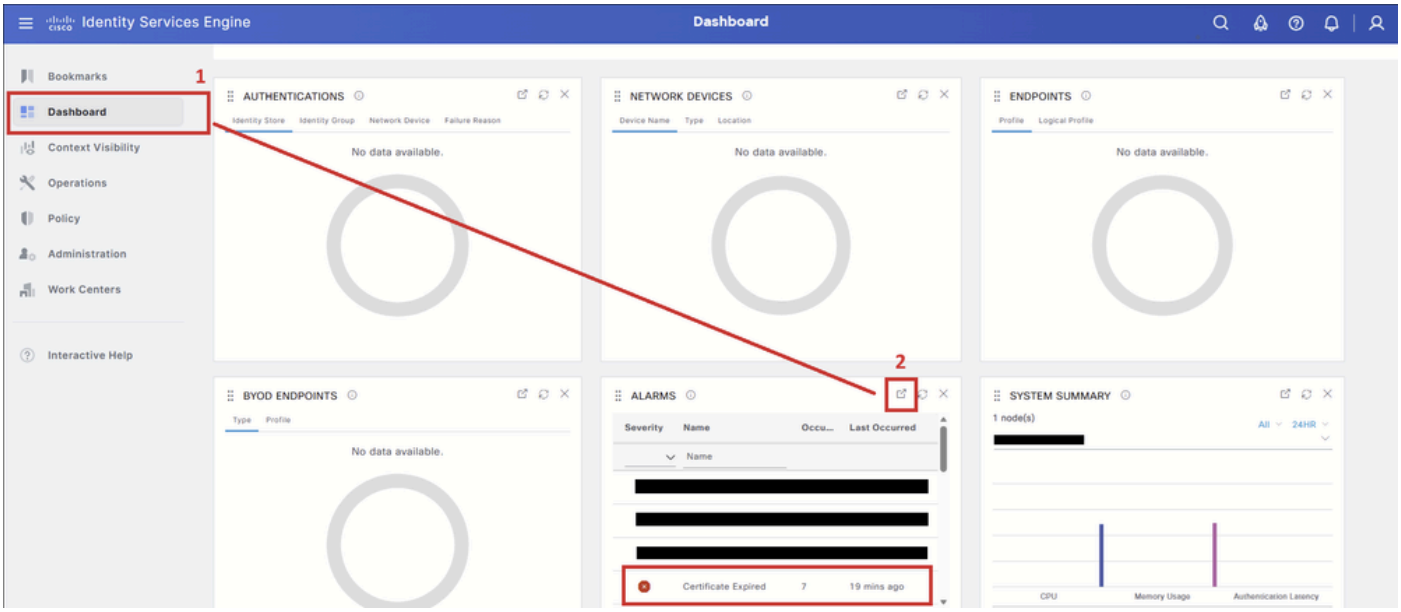
모든 Cisco ISE 구축에서 OCSP(Online Certificate Status Protocol) 응답자 인증서는 기본적으로 내부 CA(Certificate Authority) 인프라의 일부로 존재합니다. 이러한 인증서는 PAN(Primary Policy Administration Node)에서 Cisco ISE 내부 CA에 의해 발급되며 PAN 및 모든 PSN(Policy Service Node)을 포함하여 구축의 각 노드에 대해 자동으로 생성됩니다.

만료된 인증서 또는 만료 예정인 인증서는 Cisco ISE 대시보드에서 Certificate Expired(인증서 만료) 경보를 트리거할 수 있으므로 이러한 OCSP Responder 인증서를 관리하는 것이 중요합니다. Cisco ISE는 새 OCSP Responder 인증서를 자동으로 다시 생성하지만 만료된 항목은 수동으로 제거될 때까지 신뢰할 수 있는 인증서 저장소에 남아 있습니다.

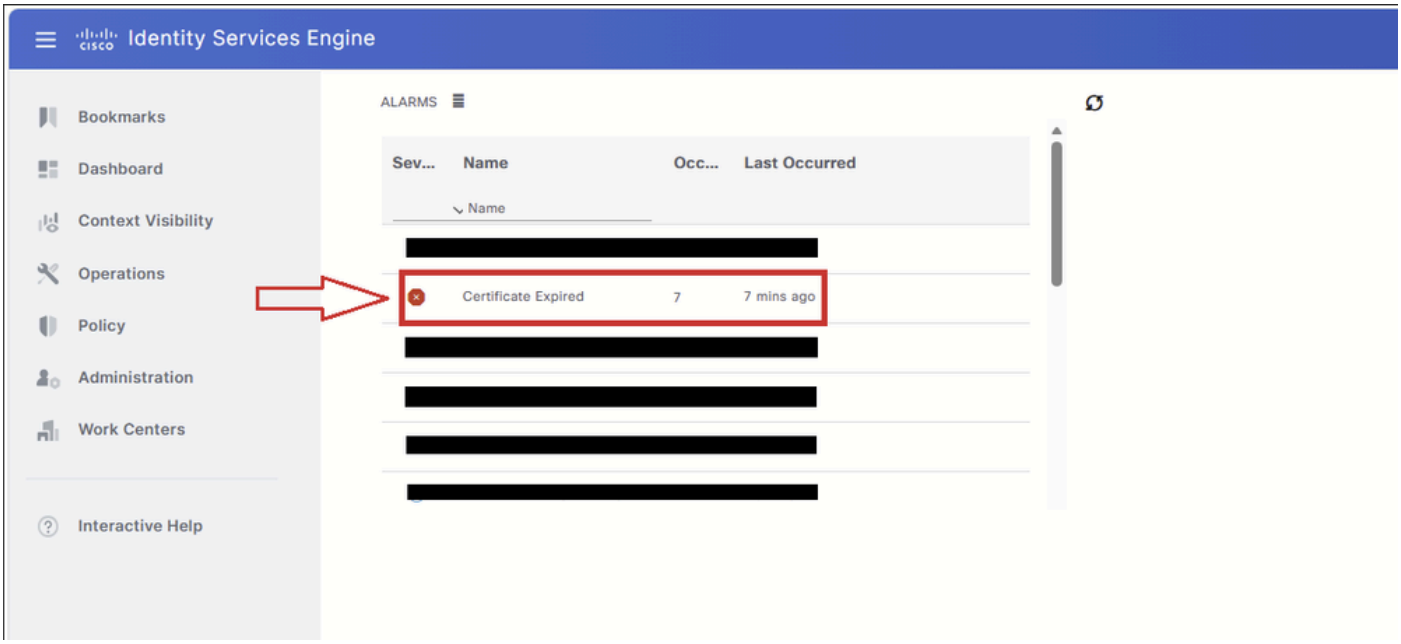
설정

1단계 - 만료된 OCSP 인증서 확인

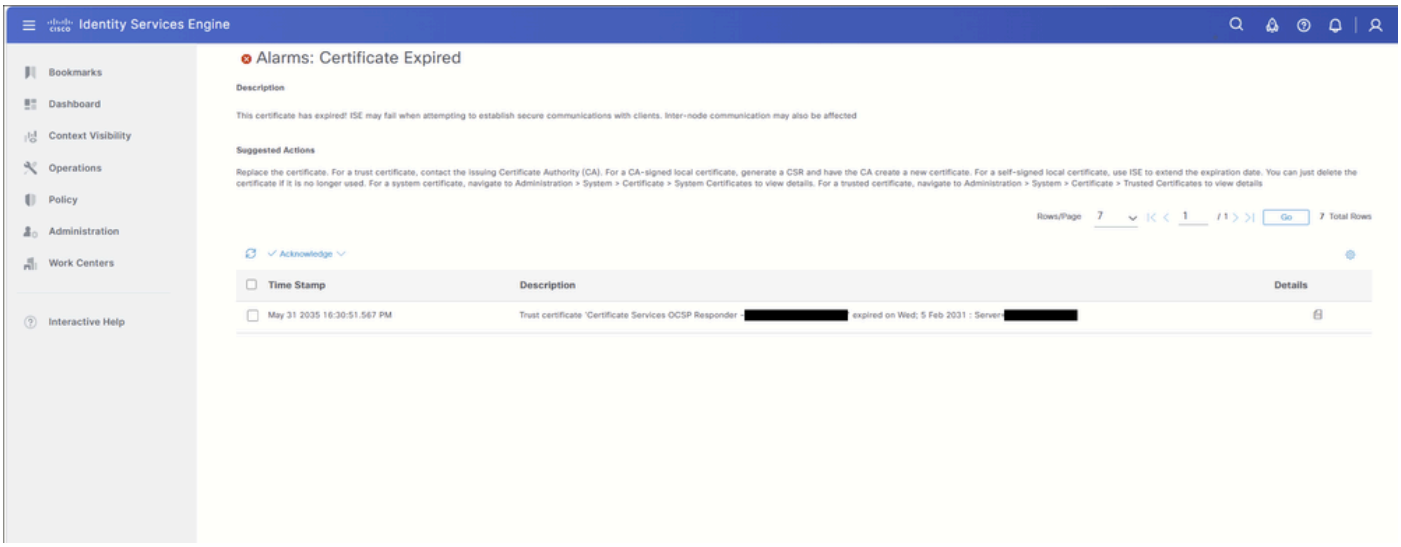
PPAN(Primary Policy Administration Node) GUI에서 Dashboard(대시보드) 탭(1)으로 이동합니다. 경보 dashlet에서 Detach(분리) 버튼(2)을 클릭하여 경보 테이블을 확장합니다.



Certificate Expired(인증서 만료) 경보를 클릭하여 테이블을 확장하고 경보와 연결된 인증서 항목을 표시합니다.



Certificate Expired(인증서 만료) 경보를 트리거한 모든 인증서가 이 테이블에 표시됩니다. 이 설명서는 OCSP Responder 인증서에만 중점을 둡니다. EAP, SAML, Admin 또는 기타 시스템 인증서와 같이 만료된 다른 인증서 유형이 테이블에 포함된 경우 해당 인증서 유형에 대한 지침은 관련 Cisco 설명서 및 Cisco ISE 관리자 설명서를 참조하십시오.



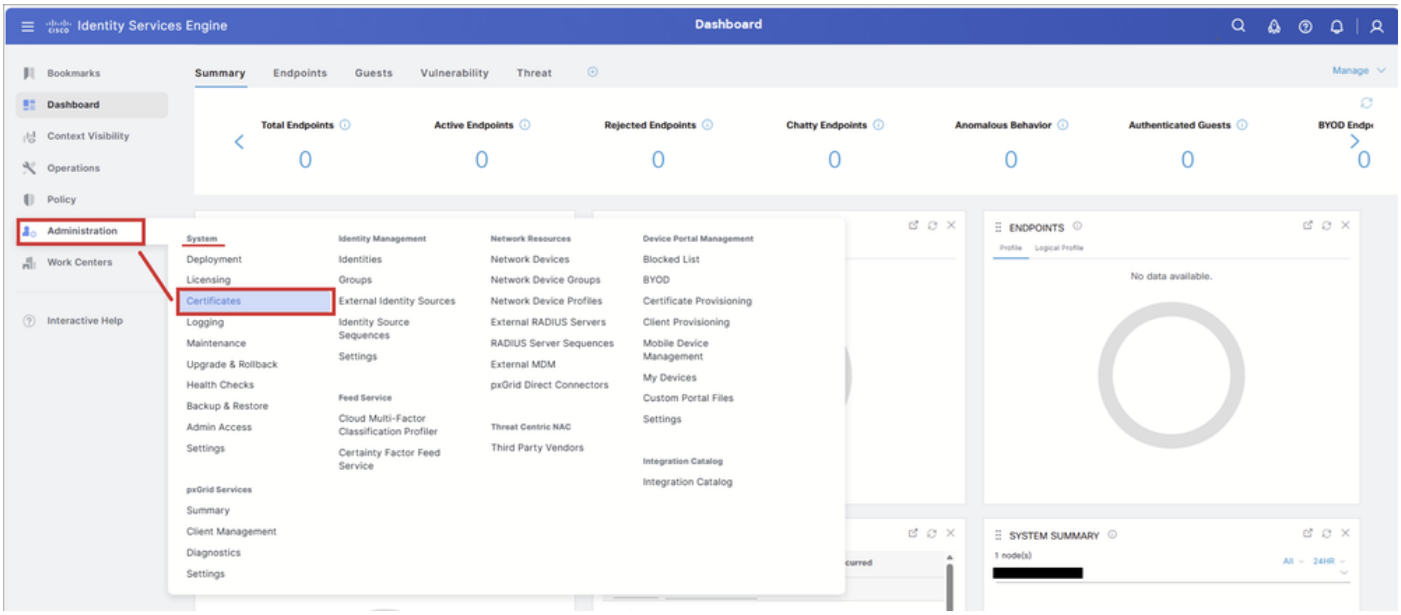
만료 된 인증서를 식별 하려면 경보 설명을 검토 하거나, 일부 시나리오에서, 만료 될 예정 입니다.

이 예에서 만료된 인증서는 다음과 같습니다. 인증서 서비스 OCSP 응답자 - <node-name>#00004.

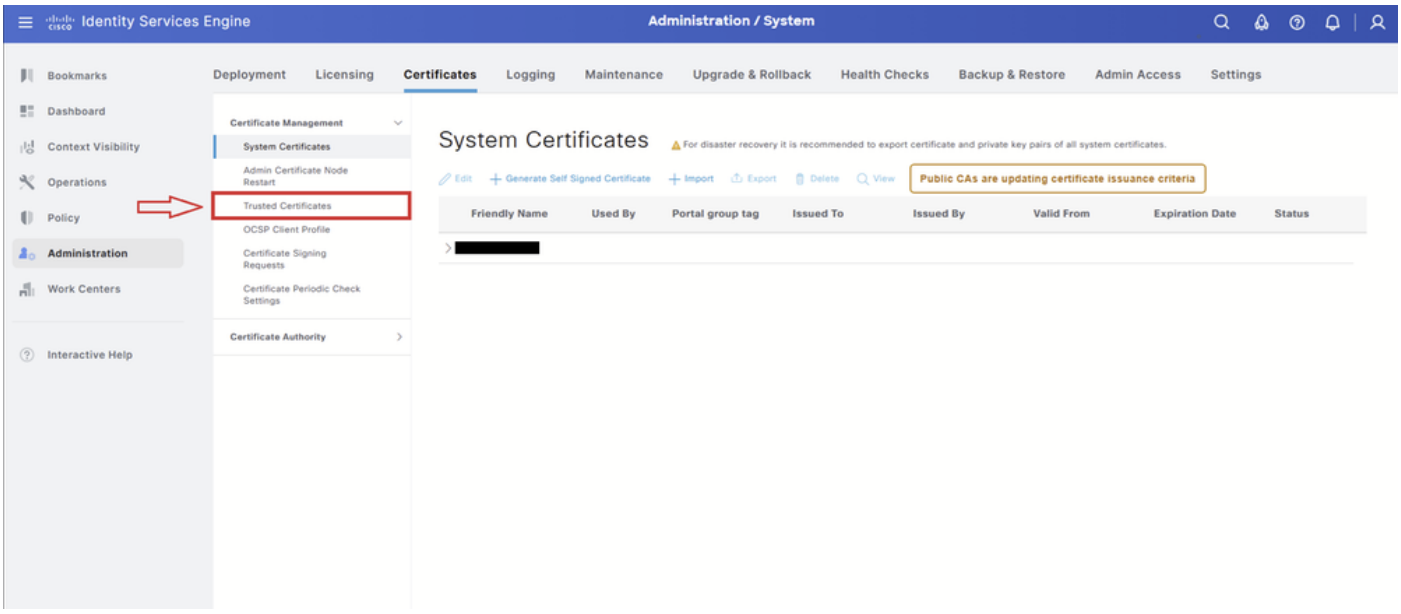
인증서 이름을 기록해 둡니다. 이 이름은 다음 단계에서 신뢰할 수 있는 인증서 저장소에서 인증서를 찾아 삭제하는 데 사용됩니다.

2단계 - 만료된 OCSP 인증서 찾기 및 삭제

다음으로 이동합니다. Administration(관리) > System(시스템) > Certificates(인증서):



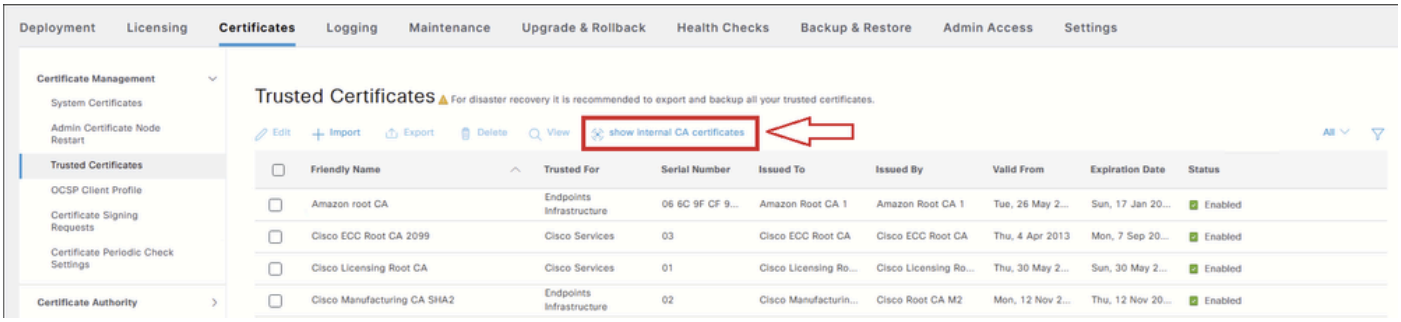
Trusted Certificates 탭을 선택합니다.



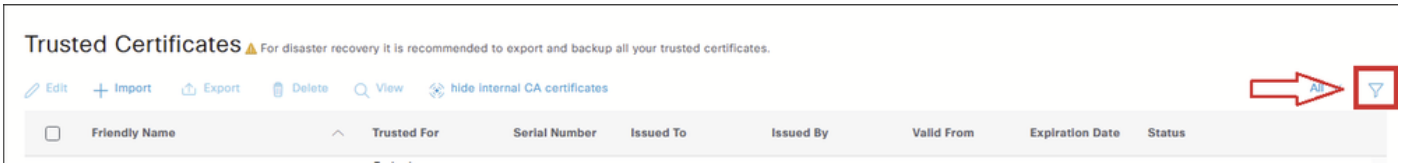
Trusted Certificates 페이지에서 show internal CA certificates를 선택합니다. 기본적으로 숨겨진 OCSP Responder 인증서를 포함하여 Cisco ISE 내부 CA(Certificate Authority) 인증서가 표시됩니다.

선택하면 버튼이 내부 CA 인증서를 숨기도록 변경됩니다.

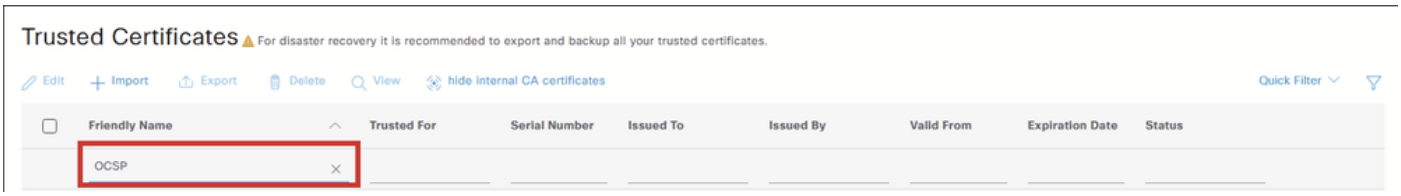
경고: 이 단계는 필수입니다. show internal CA certificates를 선택하지 않으면 OCSP Responder 인증서가 Trusted Certificate Store 테이블에 나타나지 않습니다.



Trusted Certificate Store 테이블에서 Filter 아이콘을 선택하여 삭제해야 하는 인증서를 검색합니다.

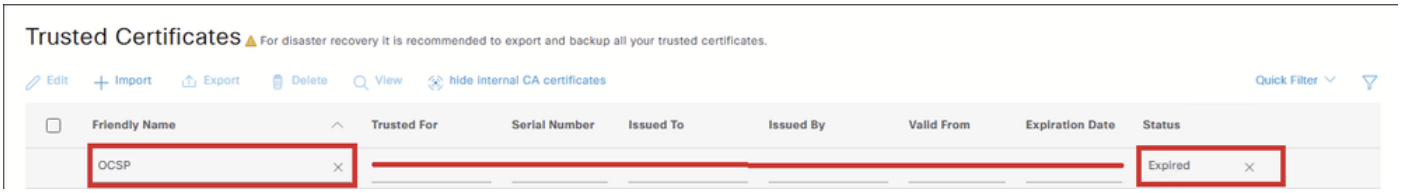


OCSP Responder 인증서가 만료될 예정이면 OCSP를 기준으로 Friendly Name(친숙한 이름)으로만 필터링합니다. OCSP Responder 인증서가 이미 만료된 경우 다음 작업을 계속 진행합니다.



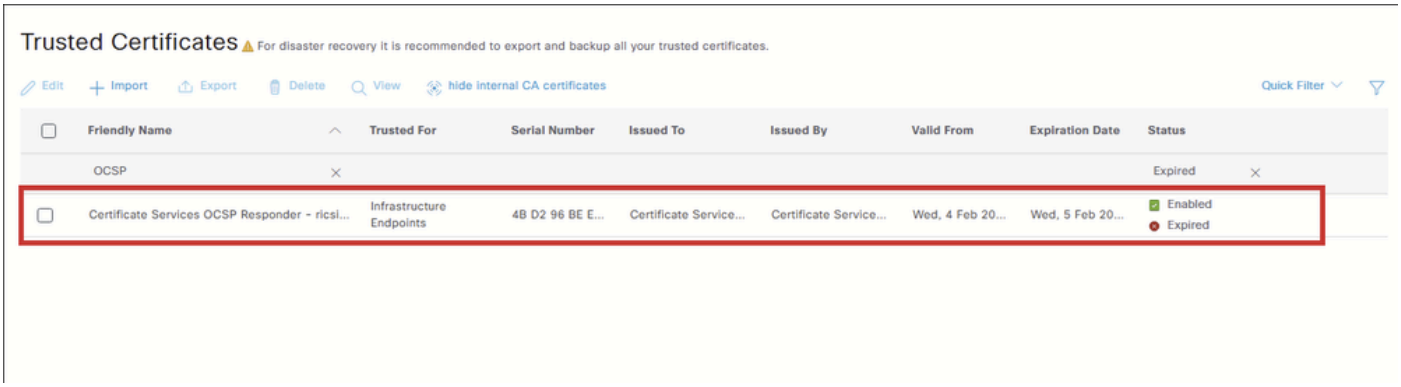
만료된 OCSP Responder 인증서를 찾으려면 다음 필터를 입력합니다.

- 이름: OCSP
- 상태: Expired(만료됨)

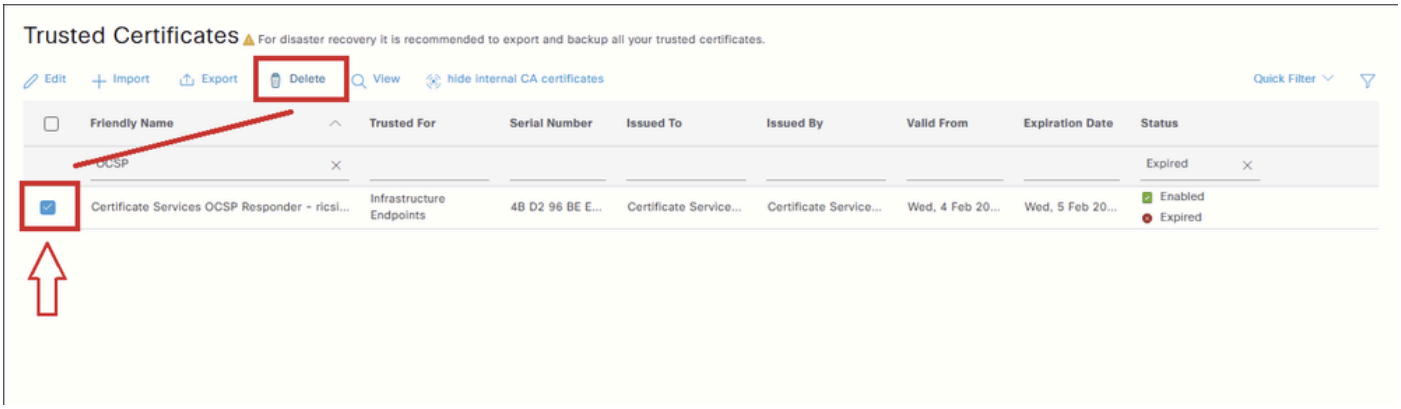


이 표에는 만료된 OCSP Responder 인증서가 표시됩니다.

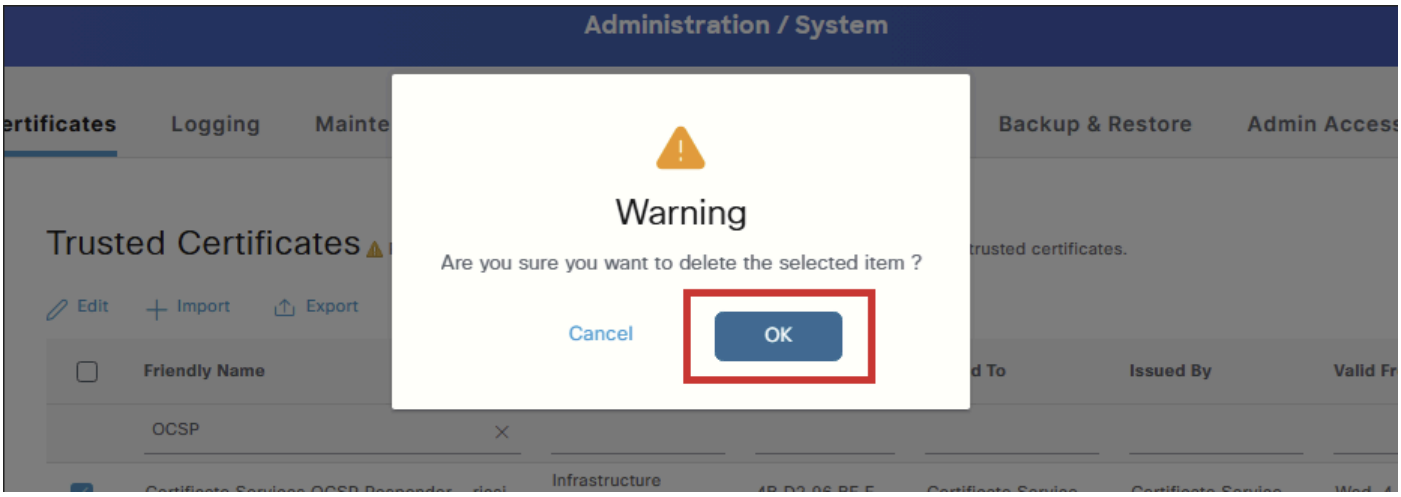
팁: 만료가 임박한 OCSP Responder 인증서를 검색하는 경우, 특히 여러 Cisco ISE 노드가 있는 구축에서 여러 인증서를 표시할 수 있습니다. 올바른 인증서를 식별하려면 OCSP로만 필터링하지 마십시오. 대신 1단계에서 경보 세부사항에 표시된 전체 인증서 이름으로 필터링합니다.



제거해야 하는 OCSP Responder 인증서 옆의 확인란을 선택하고 Delete(삭제)를 클릭합니다.



확인 경고에서 OK(확인)를 선택하여 인증서 삭제를 계속합니다.



인증서를 삭제하기 전에 OCSP Responder 인증서가 ISE 내부 CA 인프라의 일부임을 알아야 합니다.

삭제 중에 나타나는 경고는 일반적이며 모든 내부 CA 관련 인증서에 적용됩니다. 이러한 인증서 중 일부는 BYOD, pxGrid 등의 서비스에 사용되는 엔드포인트 인증서 또는 ISE 내부 CA에서 발급한 인증서를 사용하는 기타 기능에 서명하므로 내부 CA 계층 내에서 인증서를 삭제하지 않도록 주의해야 합니다.

만료된 OCSP Responder 인증서는 ISE 내부 CA에서 발급한 인증서에도 영향을 미칠 수 있습니다. 클라이언트 또는 서비스가 해당 CA에서 발급한 인증서의 상태를 쿼리하면 OCSP Responder 인증서가 만료되었기 때문에 OCSP 서비스가 오류를 반환하며, 이로 인해 인증서 상태 검증이 실패할 수 있습니다.

삭제를 선택하면 다음과 같은 두 가지 옵션이 표시됩니다.

- 인증서 삭제: 이 옵션은 신뢰할 수 있는 인증서 저장소에서 Cisco ISE 내부 CA 인증서를 삭제합니다. 내부 CA 인증서가 삭제되면 해당 CA에서 서명한 모든 엔드포인트 인증서가 유효하지 않게 되며 영향을 받는 엔드포인트가 네트워크에 액세스할 수 없습니다. 이 작업은 되돌릴 수 있습니다. 동일한 내부 CA 인증서를 신뢰할 수 있는 인증서 저장소로 다시 가져옴으로써 네트워크 액세스를 복원할 수 있습니다.
- 인증서 삭제 및 취소: 이 옵션은 Cisco ISE 내부 CA 인증서를 삭제 하고 폐기 합니다. Delete(삭제) 옵션과 마찬가지로 내부 CA에서 서명한 모든 엔드포인트 인증서가 유효하지 않게 되며, 영향을 받는 엔드포인트는 네트워크 액세스 권한을 잃게 됩니다. 그러나 이 작업은 취소할 수 없습니다. 폐기 후 기능을 복원하려면 구축에 대한 전체 Cisco ISE 루트 인증서 체인을 교체해야 합니다.

만료된 OCSP 응답자 인증서에 대해 선택할 수 있는 옵션은 무엇입니까?

설명된 영향은 엔드포인트 인증서에 능동적으로 서명하는 내부 CA 인증서에 적용됩니다. OCSP 응답자 인증서는 엔드포인트 인증서를 서명하지 않으며, OCSP 통신에 사용됩니다. 만료된 OCSP Responder 인증서로 인해 내부 CA에서 발급한 인증서에 대한 인증서 상태 검증이 실패할 수 있지만 인증서가 이미 만료되어 더 이상 유효한 OCSP 응답을 제공하지 않습니다. 이를 삭제해도 추가적인 영향은 발생하지 않습니다.

이 시나리오의 OCSP Responder 인증서가 이미 만료되었으므로 더 이상 유효하지 않습니다. 이 경우 취소할 수 있는 유효한 항목이 없으므로 삭제 및 삭제/취소는 모두 동일한 결과를 생성합니다.

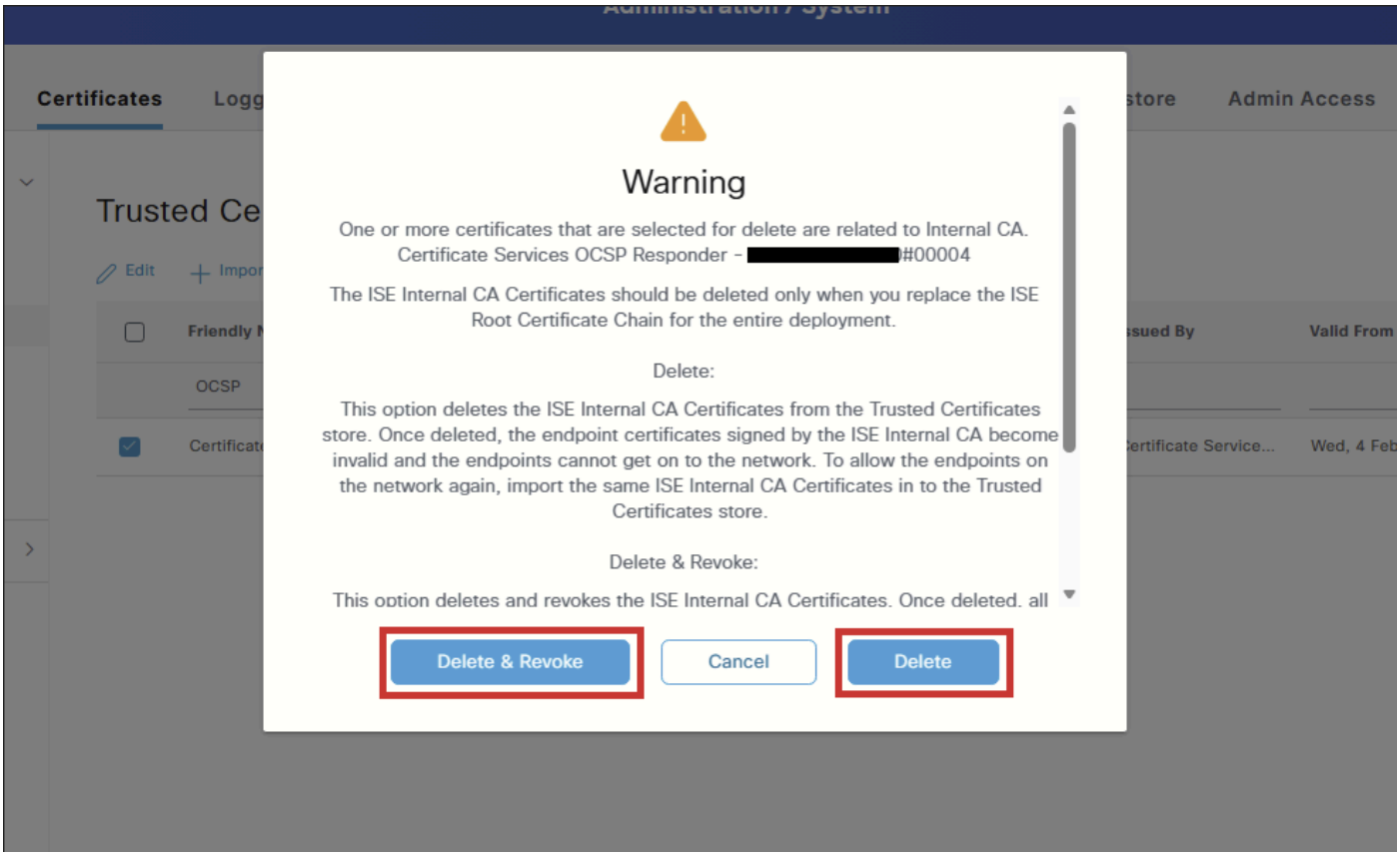
이러한 이유로 삭제 옵션은 권장되는 옵션입니다. 삭제 옵션은 간단한 작업이며 불필요한 폐기 항목을 생성하지 않기 때문입니다.

참고: OCSP 응답자 인증서는 정상 작동 중에 다시 생성되지 않습니다. 패치가 설치된 경우에만 다시 생성됩니다.
- 다중 노드 구축에서 패치가 GUI를 통해 설치되면 인증서가 재생성됩니다.
- 독립형 구축에서는 GUI 또는 CLI를 통해 패치를 설치할 때 인증서가 재생성됩니다.

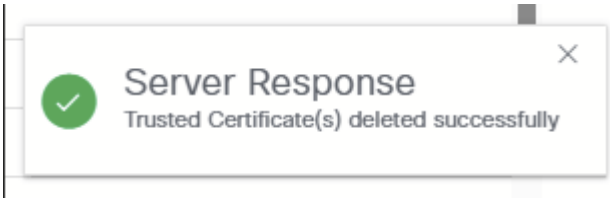
새 OCSP Responder 인증서는 다음 패치 설치 시에만 생성됩니다.

주의: 영향을 받는 노드에 신뢰할 수 있는 인증서 저장소에 유효한 OCSP Responder 인증서가 있는지 확인합니다. 유효한 인증서가 없고 OCSP를 사용하여 ISE 내부 CA에서 서명한 인증서를 검증하는 경우, 새 OCSP 응답자 인증서가 생성될 때까지 검증이 실패합니다.

유효한 OCSP Responder 인증서가 없으면 다음 설명에 따라 PPAN(Primary Policy Administration Node)에서 OCSP Responder 인증서를 갱신합니다.
1. ISE PAN GUI에 액세스합니다.
2. 관리 > 시스템 > 인증서로 이동합니다.
3. 왼쪽에서 Certificate Signing Requests(인증서 서명 요청)를 선택합니다.
4. CSR 생성을 클릭합니다. Usage(사용)의 경우 Renew ISE OCSP Responder(ISE OCSP 응답자 갱신)를 선택합니다.
5. Renew ISE OCSP Responder Certificates(ISE OCSP Responder 인증서 갱신)를 클릭하여 프로세스를 완료합니다.



인증서가 삭제되면 신뢰할 수 있는 인증서가 성공적으로 삭제되었음을 나타내는 서버 응답 알림이 나타납니다.



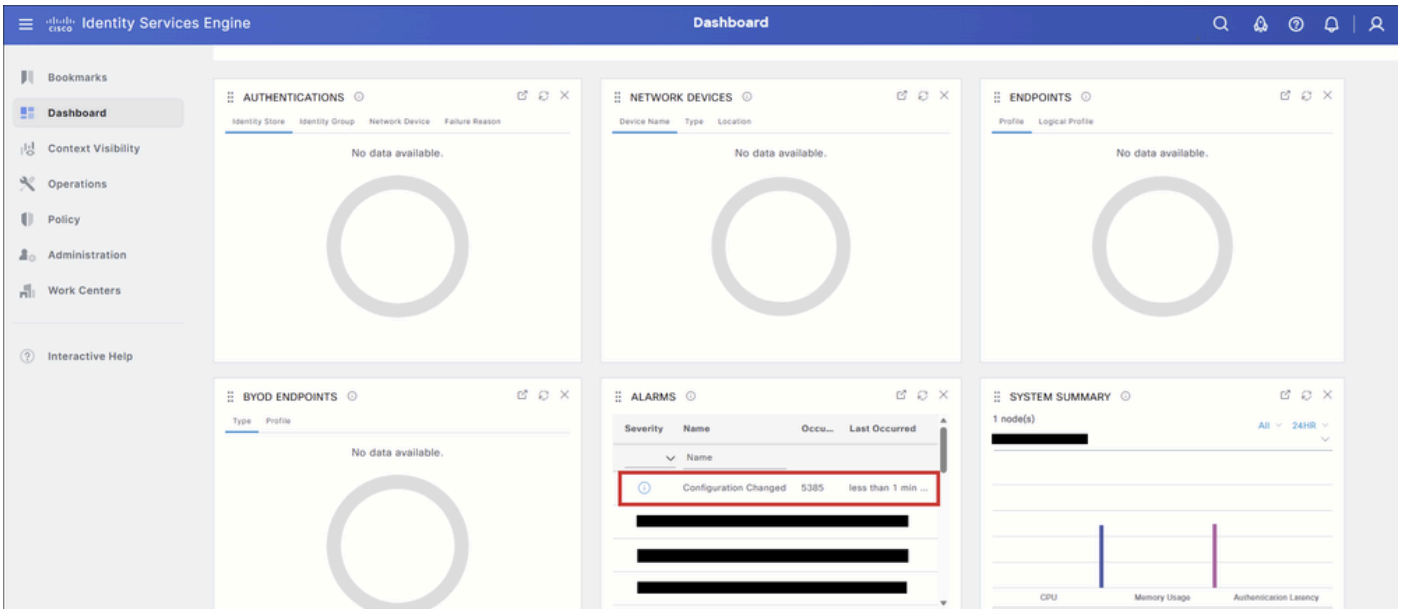
다음을 확인합니다.

인증서가 삭제 된 후, 하나 또는 두 방법 모두를 사용 하여 작업이 성공 했는지 확인 할 수 있습니다.

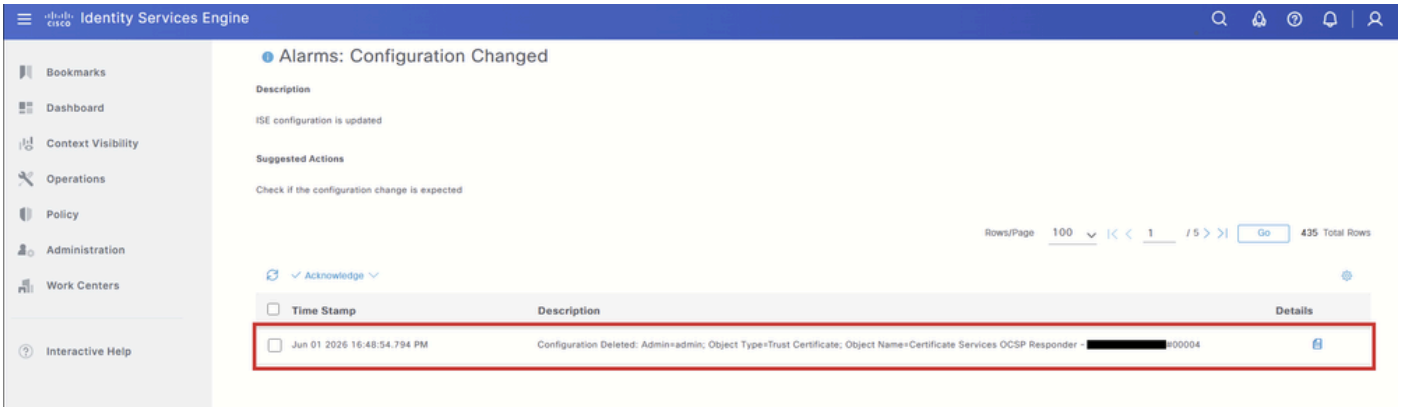
옵션 1 - Dashboard Alarms(대시보드 알람)에서 확인

Dashboard(대시보드) 페이지로 이동합니다.

Alarms dashlet(경보 dashlet)에서 Configuration Changed(컨피그레이션 변경) 경보를 찾습니다. 세부 정보를 표시하려면 알람을 선택합니다.



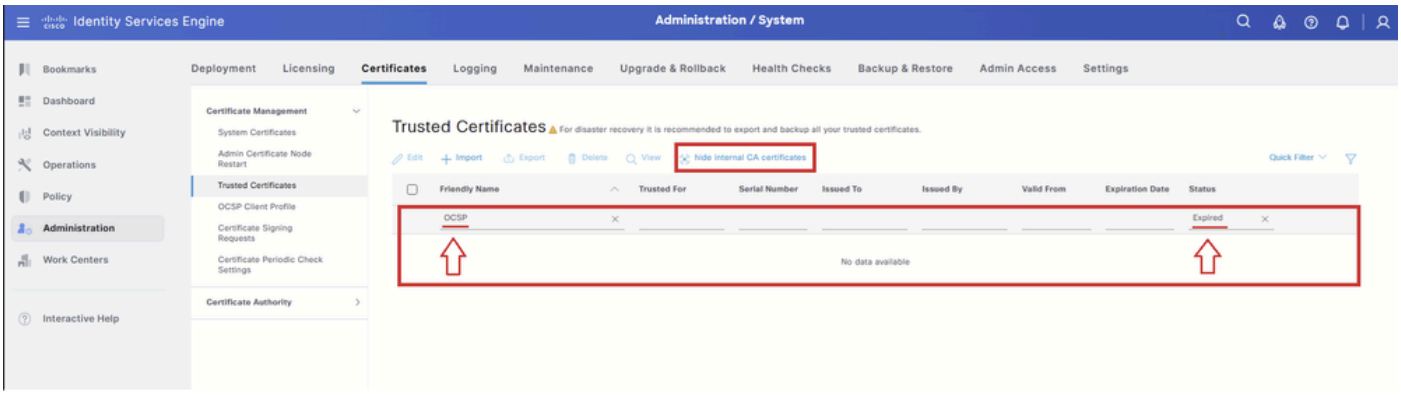
컨피그레이션 객체가 삭제되었음을 나타내는 항목이 표시되어야 합니다. 개체 이름은 제거된 OCSP 응답자 인증서와 일치해야 합니다.



옵션 2 - 신뢰할 수 있는 인증서 저장소에서 확인

추가 단계로 Trusted Certificate Store(신뢰할 수 있는 인증서 저장소) 테이블로 다시 이동하고 OCSP Responder 인증서에 대해 필터링합니다. 인증서가 삭제되었으므로 테이블에 No data available(사용 가능한 데이터 없음)이 표시되어야 합니다.

참고: show internal CA certificates를 선택해야 합니다.


Identity Services Engine
Administration / System
Bookmarks
Dashboard
Context Visibility
Operations
Policy
Administration
Work Centers
Interactive Help
Deployment
Licensing
Certificates
Logging
Maintenance
Upgrade & Rollback
Health Checks
Backup & Restore
Admin Access
Settings
Certificate Management
System Certificates
Admin Certificate Node Restart
Trusted Certificates
OCSP Client Profile
Certificate Signing Requests
Certificate Periodic Check Settings
Certificate Authority
Trusted Certificates
For disaster recovery it is recommended to export and backup all your trusted certificates.
Edit
Import
Export
Delete
View
Hide Internal CA certificates
Quick Filter
Friendly Name
Trusted For
Serial Number
Issued To
Issued By
Valid From
Expiration Date
Status
OCSP
Expired
No data available

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.