Verlopen interne OCSP-respondercertificaten verwijderen in ISE

Inhoud

Inleiding

Voorwaarden

- Vereisten
- Gebruikte componenten

Achtergrondinformatie

Configuratie

- Stap 1 - Controleer het verlopen OCSP-certificaat
- Stap 2 - Het verlopen OCSP-certificaat zoeken en verwijderen
  - Welke optie om te selecteren voor een verlopen OCSP Responder Certificate?

Verifiëren

- Optie 1 - Verifiëren via het dashboardalarm
- Optie 2 - Verifiëren in het vertrouwde certificaatarchief

Inleiding

In dit document wordt beschreven hoe verlopen OCSP-respondercertificaten in Cisco Identity Service Engine (ISE) kunnen worden verwijderd en/of hoe deze kunnen worden verlopen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van de Identity Service Engine (ISE).
- Basiskennis van certificaten.
- Online Certificate Status Protocol (OCSP)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Identity Service Engine 3.x

De informatie in dit document is gemaakt op basis van de apparaten in een specifieke laboratoriumomgeving.Alle apparaten die in dit document worden gebruikt, zijn gestart met een uitgeklaarde (standaard) configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Een veelvoorkomend probleem waarmee klanten die gebruikmaken van Cisco Identity Services Engine (ISE) worden geconfronteerd, is het ontvangen van alarmen die aangeven dat een certificaat is verlopen, met name wanneer het OCSP-antwoordcertificaat is verlopen of op het punt staat te vervallen en het certificaat niet kan worden gevonden. Deze situatie leidt er vaak toe dat klanten TAC-zaken openen voor hulp. Het doel van deze gids is om klanten in staat te stellen deze verlopen of binnenkort verlopen OCSP-respondercertificaten zelf te vinden en te verwijderen, waardoor de noodzaak om een TAC-geval te verhogen wordt vermeden.

Het Online Certificate Status Protocol (OCSP) is een protocol dat wordt gebruikt voor het controleren van de status van x.509 digitale certificaten. Dit protocol is een alternatief voor de Certificate Revocation List (CRL) en behandelt problemen die leiden tot de verwerking van CRL's. Cisco ISE heeft de mogelijkheid om via HTTP te communiceren met OCSP-servers om de status van certificaten in authenticaties te valideren. De OCSP-configuratie is geconfigureerd in een herbruikbaar configuratieobject waarnaar kan worden verwezen vanaf elk certificaat van de certificeringsinstantie (CA) dat is geconfigureerd in Cisco ISE.

In elke Cisco ISE-implementatie zijn OCSP (Online Certificate Status Protocol)-respondercertificaten standaard aanwezig als onderdeel van de interne CA (Certificate Authority)-infrastructuur. Deze certificaten worden uitgegeven door de Cisco ISE Internal CA op de PPAN (Primary Policy Administration Node) en worden automatisch gegenereerd voor elke node in de implementatie, inclusief de PAN en alle PSN's (Policy Service Nodes).

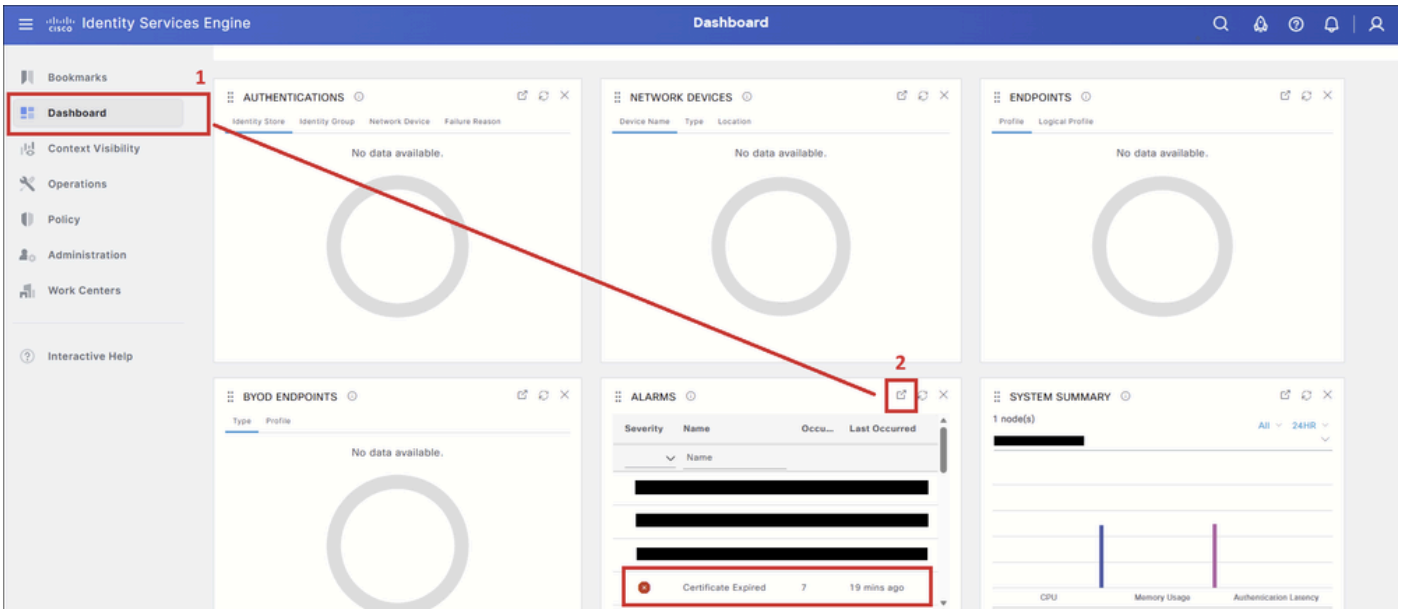
Het beheren van deze OCSP Responder-certificaten is belangrijk omdat verlopen of bijna verlopen certificaten verlopen certificaatalarmen in het Cisco ISE-dashboard kunnen activeren.

Hoewel Cisco ISE automatisch nieuwe OCSP Responder-certificaten regenereert, blijven de verlopen vermeldingen in de Trusted Certificate Store totdat ze handmatig worden verwijderd.

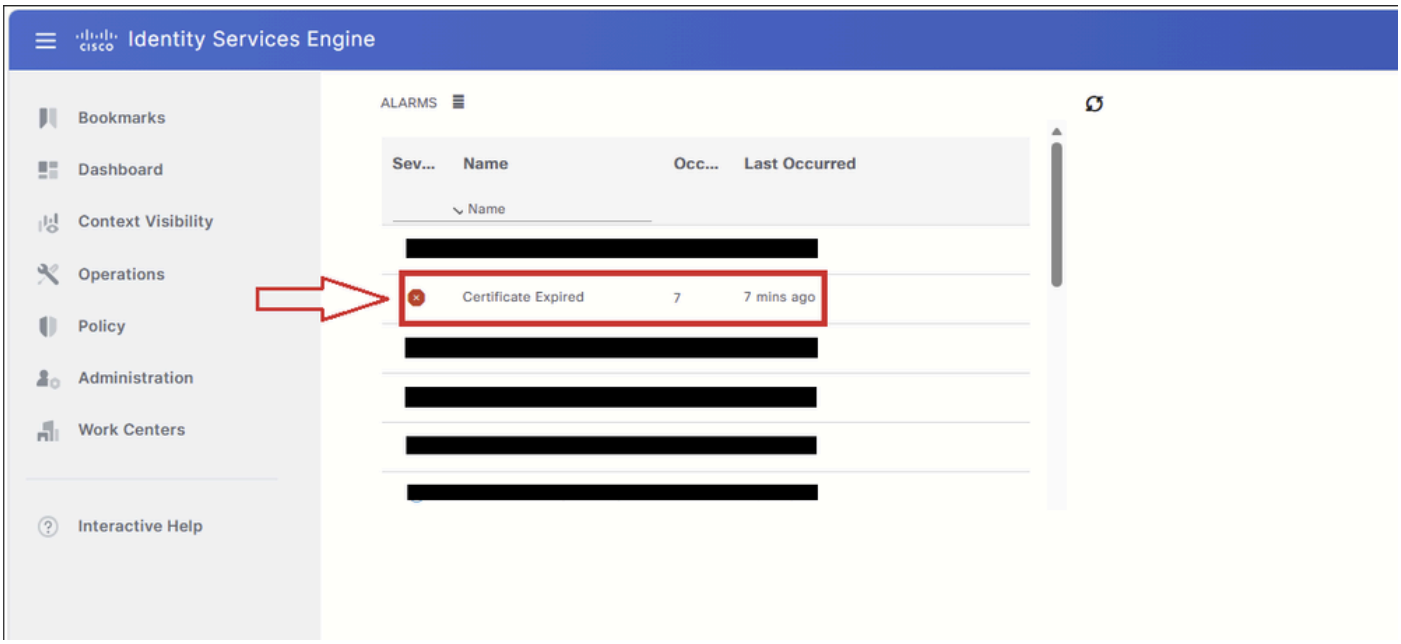
Configuratie

Stap 1 - Controleer het verlopen OCSP-certificaat

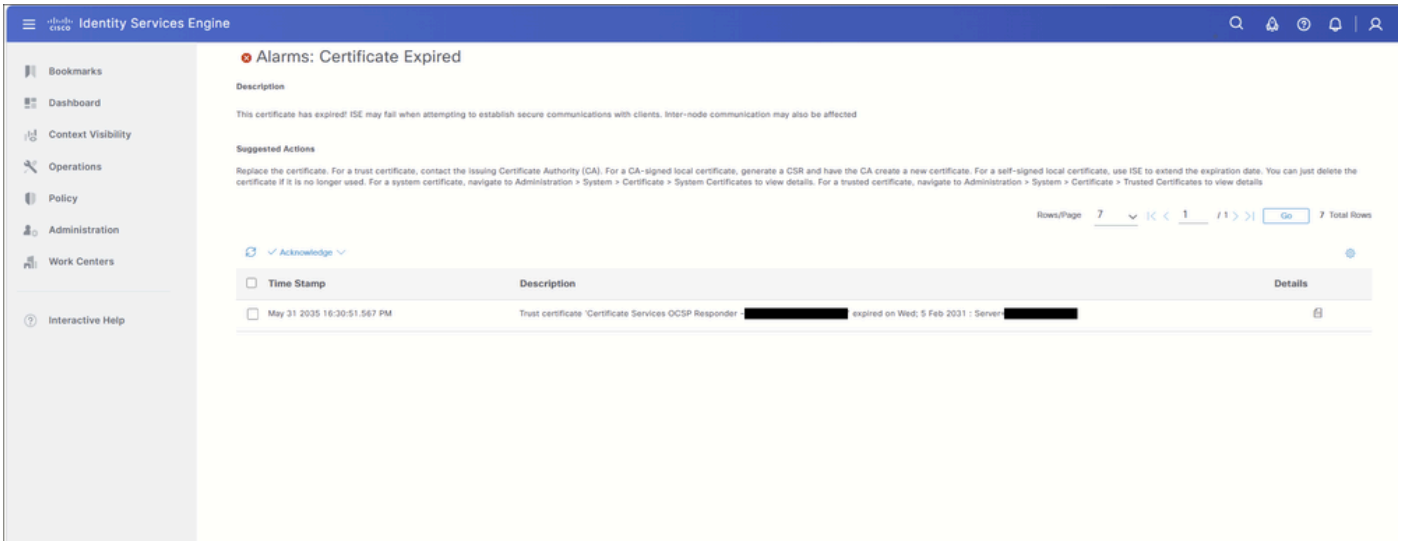
Navigeer in de PPAN (Primary Policy Administration Node) GUI naar het tabblad Dashboard (1). Klik in het dashlet Alarmen op de knop Loskoppelen (2) om de alarmtabel uit te vouwen.



Klik op het alarm Certificaat verlopen om de tabel uit te vouwen en de certificaatvermeldingen weer te geven die aan het alarm zijn gekoppeld.



Alle certificaten die het alarm Certificaat verlopen hebben geactiveerd, worden weergegeven in deze tabel. Deze gids richt zich alleen op OCSP Responder-certificaten. Als de tabel andere verlopen certificaattypen bevat, zoals EAP-, SAML-, Admin- of andere systeemcertificaten, raadpleegt u de relevante Cisco-documentatie en de Cisco ISE-beheerdershandleiding voor richtlijnen voor die certificaattypen.



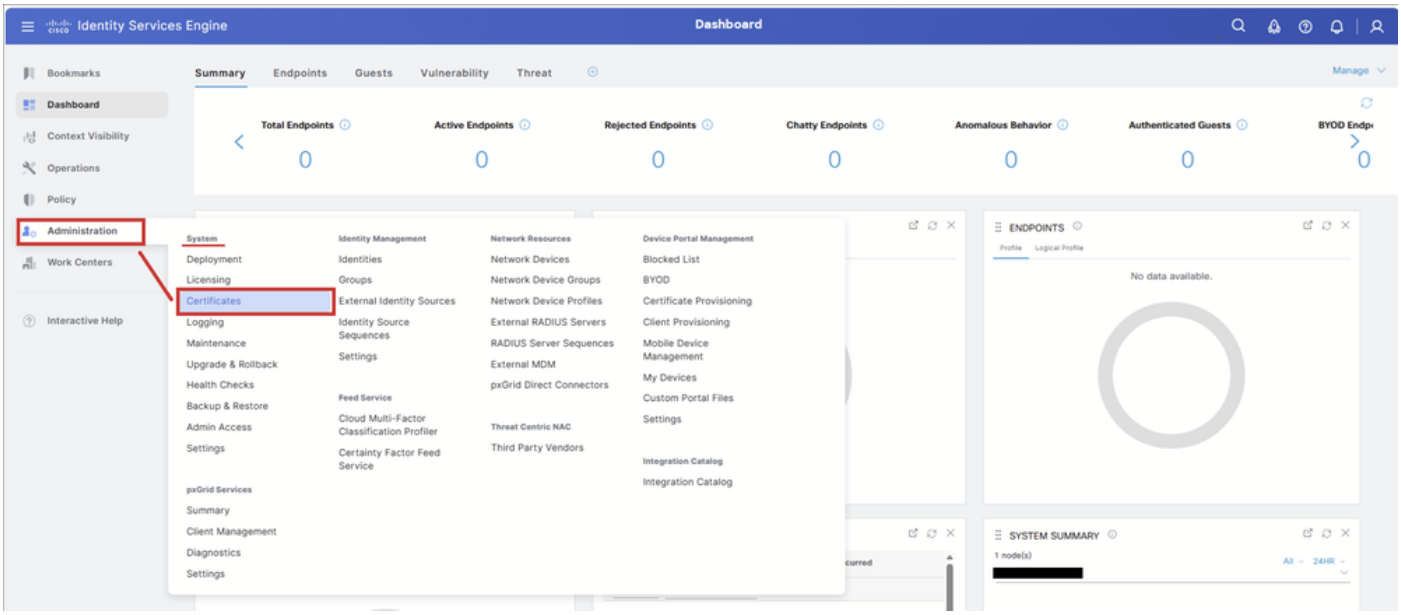
Controleer de alarmbeschrijving om het certificaat te identificeren dat is verlopen of, in sommige scenario's, op het punt staat te vervallen.

In dit voorbeeld is het verlopen certificaat: Certificate Services OCSP Responder - <node-name>#00004.

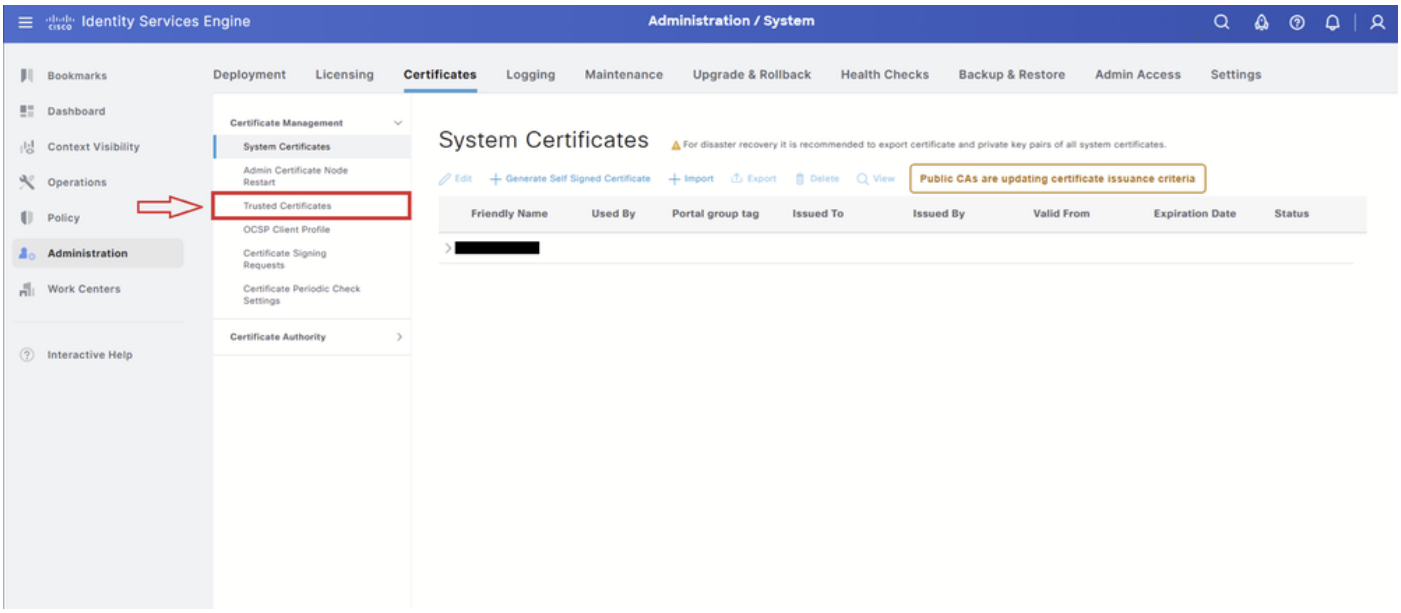
Let op de naam van het certificaat. Deze naam wordt in de volgende stappen gebruikt om het certificaat te zoeken en te verwijderen uit het vertrouwde certificaatarchief.

Stap 2 - Het verlopen OCSP-certificaat zoeken en verwijderen

Navigeer naar: Beheer > Systeem > Certificaten:



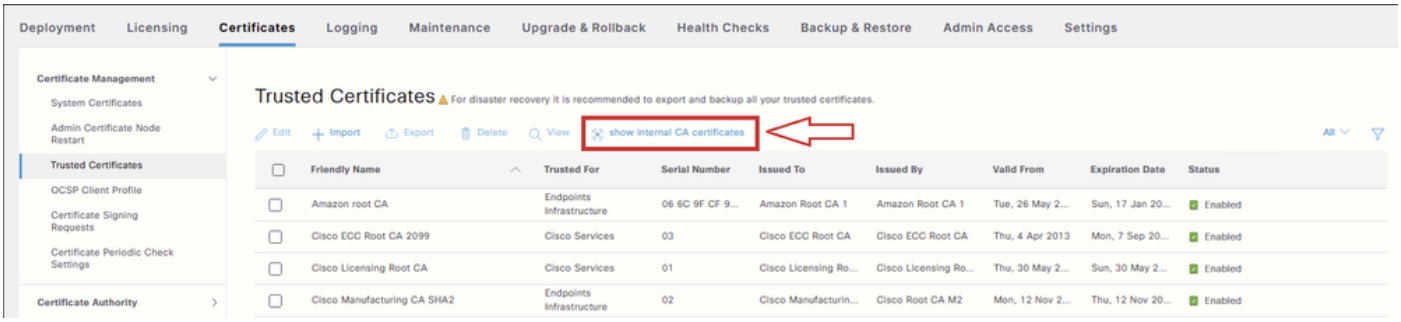
Selecteer het tabblad Vertrouwde certificaten.



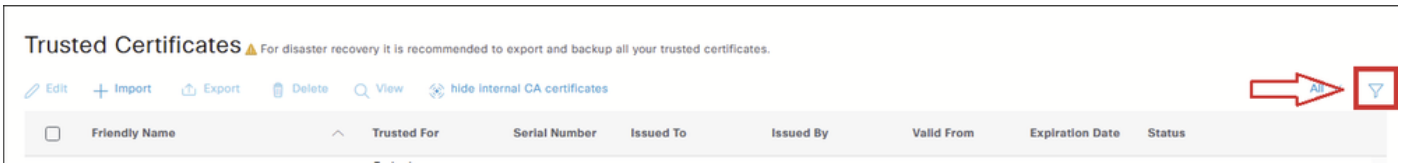
Selecteer op de pagina Vertrouwde certificaten de optie Interne CA-certificaten tonen. Hiermee worden de Cisco ISE Internal CA (Certificate Authority)-certificaten weergegeven, inclusief de OCSP Responder-certificaten die standaard zijn verborgen.

Als deze optie is geselecteerd, verandert de knop om interne CA-certificaten te verbergen.

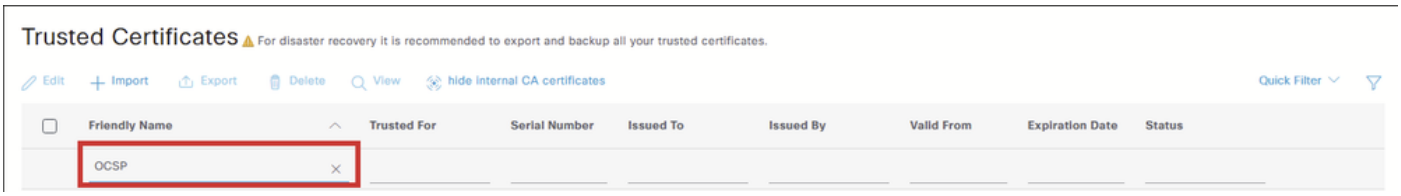
Waarschuwing: deze stap is vereist. Als Toon interne CA-certificaten niet is geselecteerd, wordt het OCSP Responder-certificaat niet weergegeven in de tabel Vertrouwd certificaatarchief.



Selecteer in de tabel Vertrouwd certificaatarchief het pictogram Filter om te zoeken naar het certificaat dat moet worden verwijderd.

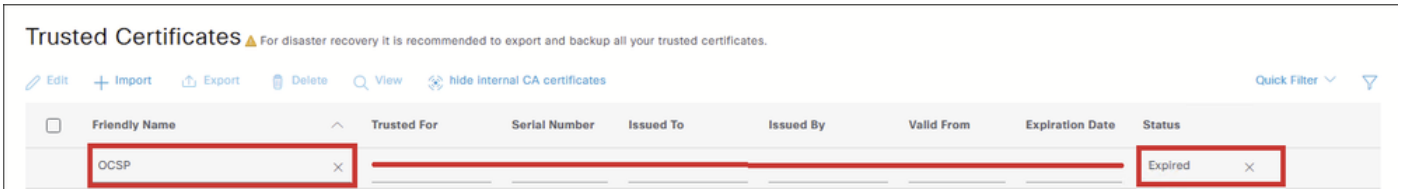


Als het OCSP Responder-certificaat bijna verloopt, filtert u alleen op OCSP onder de naam Vriendschappelijk. Als het OCSP Responder-certificaat al is verlopen, gaat u verder met de volgende actie.



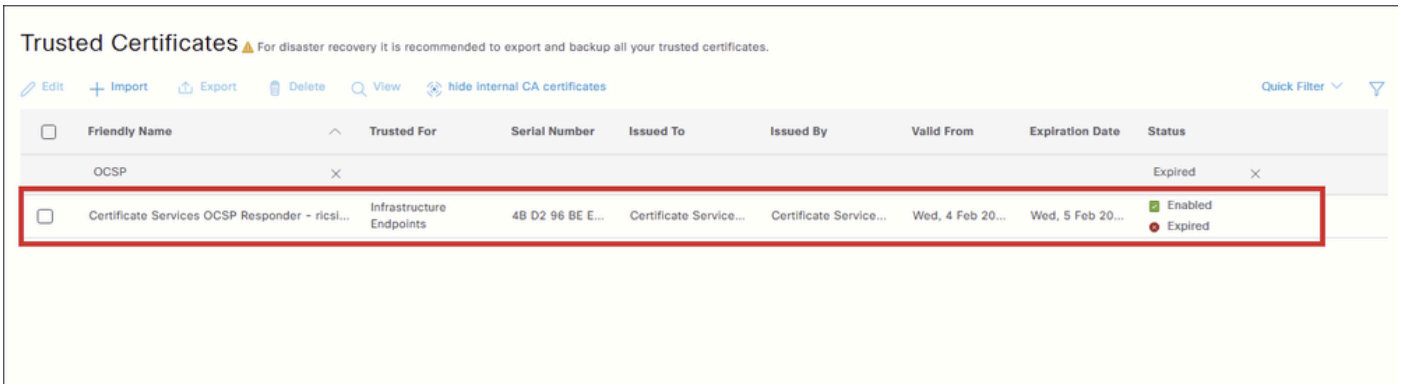
Voer de volgende filters in om een verlopen OCSP Responder-certificaat te zoeken:

- Vriendelijke naam: OCSP
- Status: verlopen

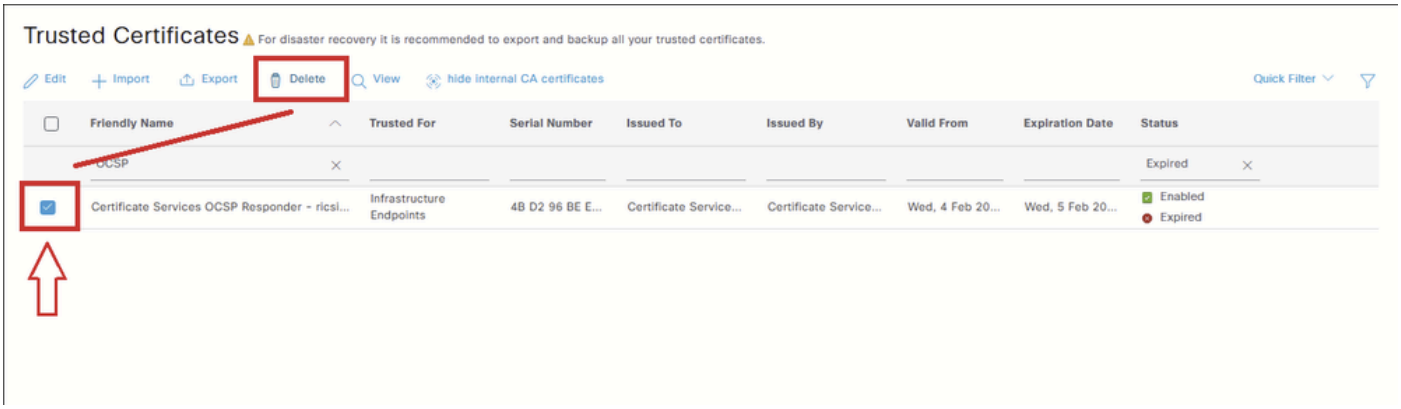


In de tabel worden de verlopen OCSP Responder-certificaten weergegeven.

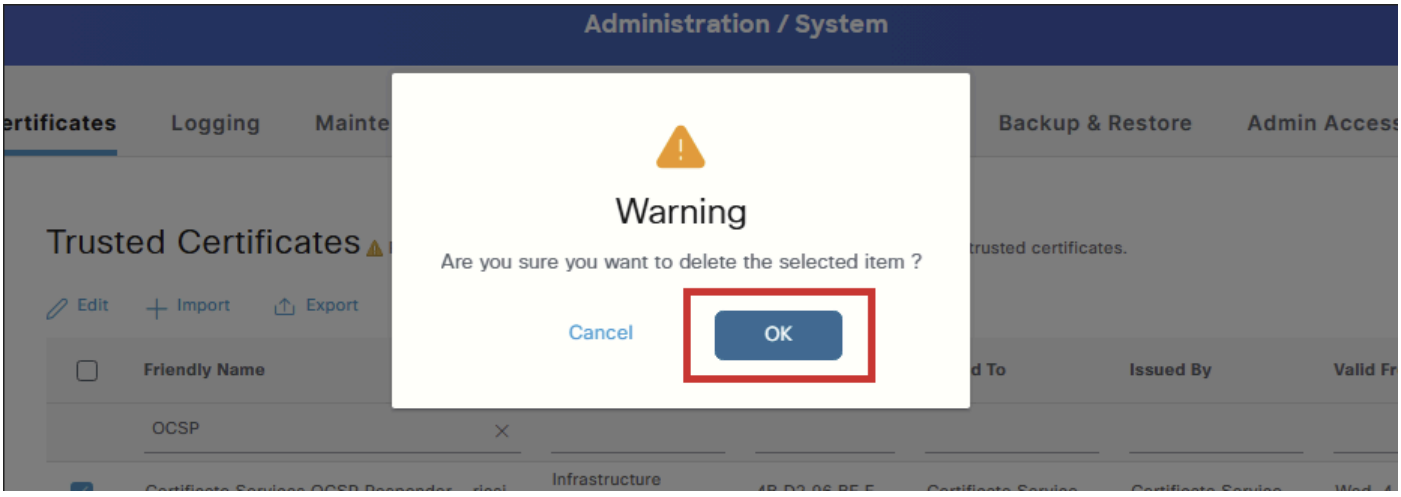
Tip: als u op zoek bent naar een OCSP Responder-certificaat dat bijna verloopt, kunnen meerdere certificaten worden weergegeven, vooral in implementaties met meerdere Cisco ISE-knooppunten. Om het juiste certificaat te identificeren, moet u niet alleen filteren op OCSP. Filter in plaats daarvan op de volledige certificaatnaam die werd weergegeven in de alarmgegevens in stap 1.



Schakel het selectievakje in naast het OCSP Responder-certificaat dat moet worden verwijderd en klik op Verwijderen.



Selecteer OK op de bevestigingswaarschuwing om door te gaan met het verwijderen van het certificaat.



Voordat u het certificaat verwijdert, is het belangrijk om te begrijpen dat het OCSP Responder-

certificaat deel uitmaakt van de ISE Internal CA-infrastructuur.

De waarschuwing die verschijnt tijdens het verwijderen is generiek en geldt voor alle interne CA-gerelateerde certificaten. Het doel is om te voorkomen dat certificaten worden verwijderd binnen de Interne CA-hiërarchie, omdat sommige van deze certificaten eindpuntcertificaten ondertekenen die worden gebruikt voor services zoals BYOD, pxGrid of andere functies die afhankelijk zijn van certificaten die zijn uitgegeven door de ISE Interne CA.

Een verlopen OCSP Responder-certificaat kan ook van invloed zijn op certificaten die zijn uitgegeven door de ISE Internal CA. Wanneer een client of service de status opvraagt van een certificaat dat is uitgegeven door die CA, retourneert de OCSP-service een fout omdat het OCSP-respondercertificaat is verlopen, waardoor de validatie van de certificaatstatus kan mislukken.

Wanneer u Verwijderen selecteert, worden twee opties weergegeven:

- Certificaat verwijderen: met deze optie wordt het Cisco ISE Internal CA-certificaat verwijderd uit het archief voor vertrouwde certificaten. Wanneer het interne CA-certificaat wordt verwijderd, worden alle eindpuntcertificaten die door die CA zijn ondertekend ongeldig en kunnen de getroffen eindpunten geen toegang krijgen tot het netwerk. Deze actie is omkeerbaar: u kunt de netwerktoegang herstellen door hetzelfde interne CA-certificaat terug te importeren in het archief voor vertrouwde certificaten.
- Certificaat verwijderen en intrekken: met deze optie wordt het Cisco ISE Internal CA-certificaat verwijderd en ingetrokken. Net als bij de optie Verwijderen worden alle eindpuntcertificaten die zijn ondertekend door de interne CA ongeldig en verliezen de getroffen eindpunten de netwerktoegang. Deze operatie is echter onomkeerbaar. Na de intrekking moet u de volledige Cisco ISE-hoofdcertificaatketen vervangen om de functionaliteit voor de implementatie te herstellen.

Welke optie om te selecteren voor een verlopen OCSP Responder Certificate?

De beschreven impact is van toepassing op interne CA-certificaten die eindpuntcertificaten actief ondertekenen. Het OCSP Responder certificaat ondertekent geen endpoint certificaten, het wordt gebruikt voor OCSP communicatie. Hoewel een verlopen OCSP Responder-certificaat ertoe kan leiden dat de certificaatstatusvalidatie mislukt voor certificaten die zijn uitgegeven door de interne certificeringsinstantie, is het certificaat al verlopen en biedt het daarom geen geldige OCSP-antwoorden meer. Het schrappen ervan heeft geen extra effect.

Omdat het OCSP Responder-certificaat in dit scenario al is verlopen, is het niet langer geldig. In dit geval produceren zowel Verwijderen als Verwijderen en Intrekken hetzelfde resultaat, omdat er niets meer geldig is om in te trekken.

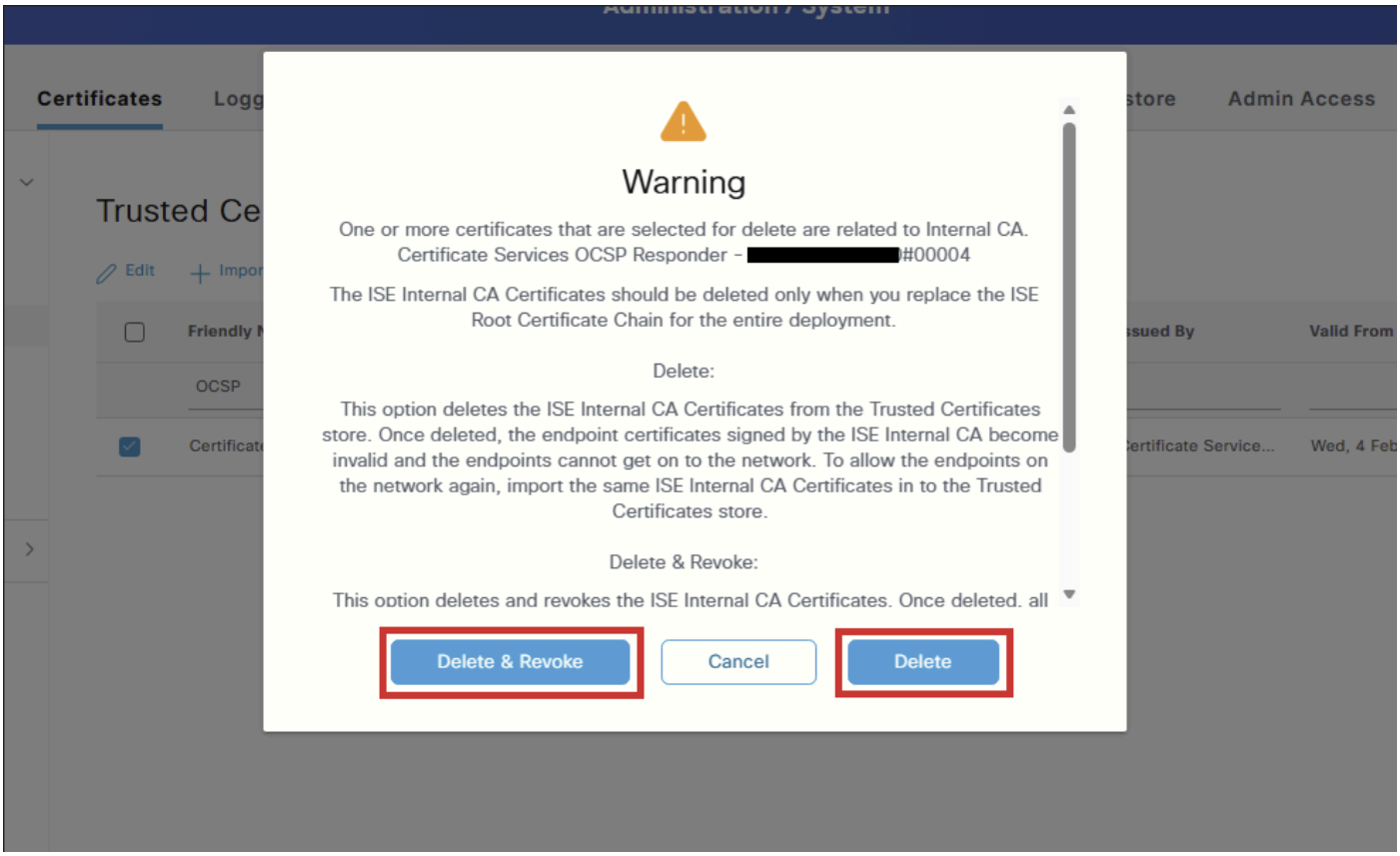
Om deze redenen is Verwijderen de aanbevolen optie, omdat het de eenvoudigere actie is en voorkomt dat een onnodige intrekkingsvermelding wordt gegenereerd.

Opmerking: OCSP Responder-certificaten worden niet geregenereerd tijdens normaal gebruik. Ze worden alleen opnieuw gegenereerd wanneer een patch is geïnstalleerd:
- In een implementatie met meerdere knooppunten worden de certificaten opnieuw gegenereerd wanneer de patch via de GUI wordt geïnstalleerd.
- In een standalone implementatie worden de certificaten opnieuw gegenereerd wanneer de patch via de GUI of de CLI is geïnstalleerd.

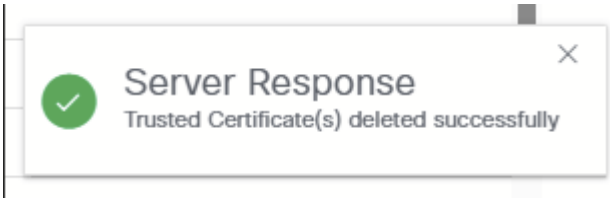
Een nieuw OCSP Responder-certificaat wordt alleen gegenereerd bij de volgende patchinstallatie.

Let op: Zorg ervoor dat de betreffende node een actief, geldig OCSP Responder-certificaat heeft in de Trusted Certificate Store. Als er geen geldig certificaat aanwezig is en OCSP wordt gebruikt om certificaten te valideren die zijn ondertekend door ISE Internal CA, mislukt die validatie totdat een nieuw OCSP Responder-certificaat is gegenereerd.

Als er geen geldig OCSP Responder-certificaat aanwezig is, verlengt u de OCSP Responder-certificaten van het PPAN (Primary Policy Administration Node), zoals hier wordt beschreven:
1. Toegang tot de ISE PPAN GUI.
2. Ga naar Beheer > Systeem > Certificaten.
3. Selecteer aan de linkerkant Certificaatondertekeningsverzoeken.
4. Klik op MVO genereren. Selecteer voor gebruik ISE OCSP-responder vernieuwen.
5. Klik op ISE OCSP Responder Certificates vernieuwen om het proces te voltooien.



Nadat het certificaat is verwijderd, wordt een melding voor de serverrespons weergegeven die aangeeft dat het vertrouwde certificaat met succes is verwijderd:



Verifiëren

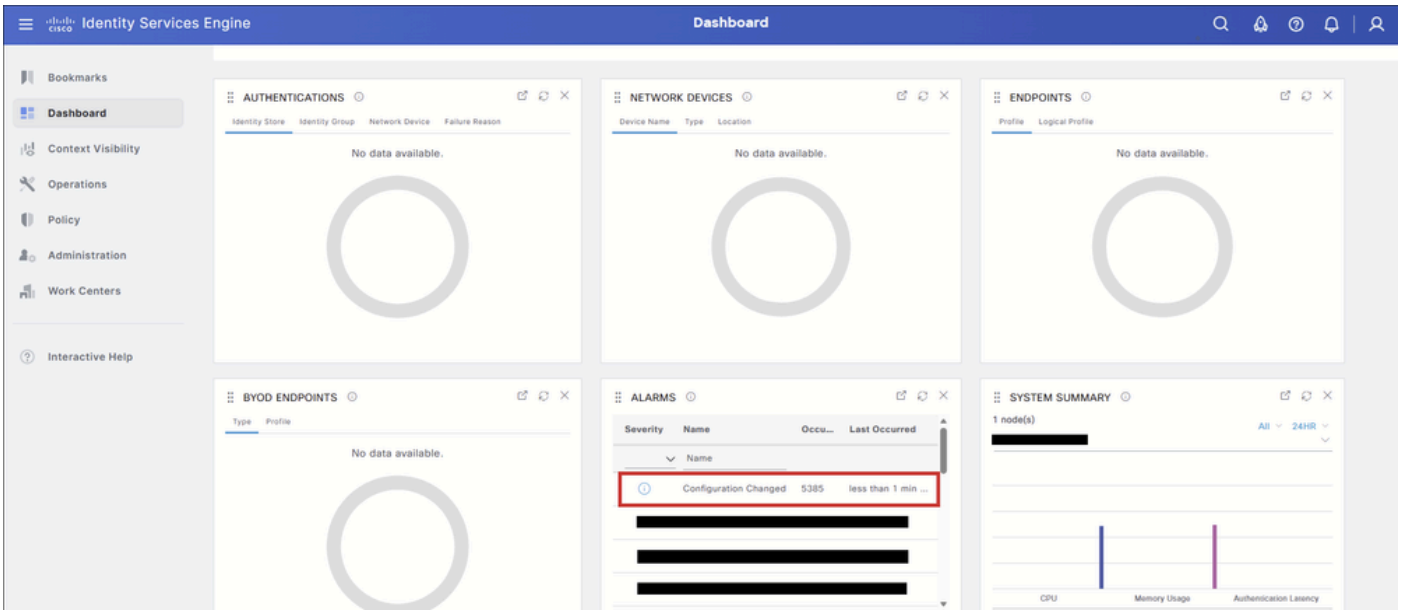
Nadat het certificaat is verwijderd, kunt u een of beide van deze methoden gebruiken om te controleren of de bewerking is geslaagd.

Optie 1 - Verifiëren via het dashboardalarm

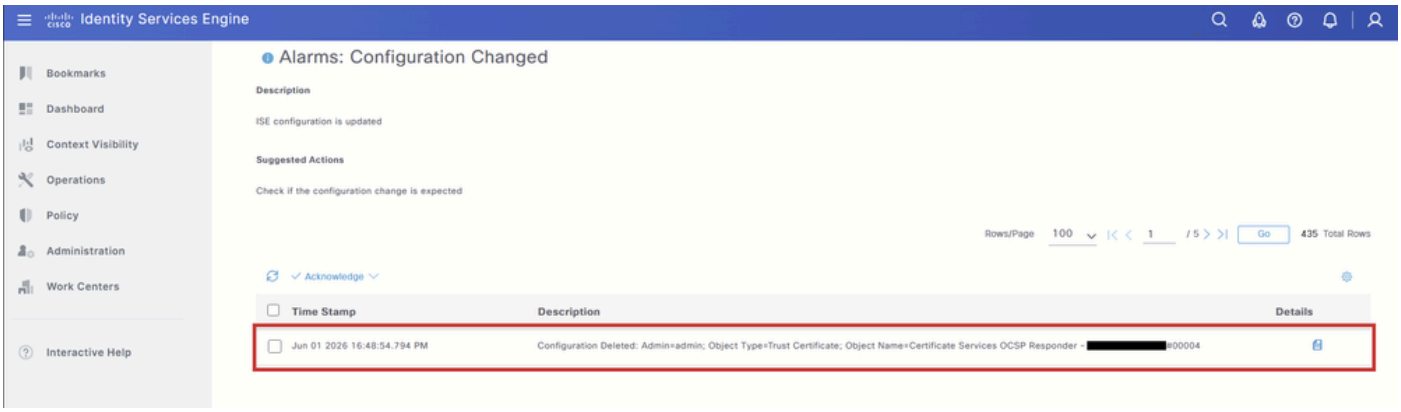
Navigeer naar de Dashboard pagina.

Zoek in het dashlet Alarms het alarm Configuration Changed (Configuratie gewijzigd). Selecteer

het alarm om de details weer te geven.



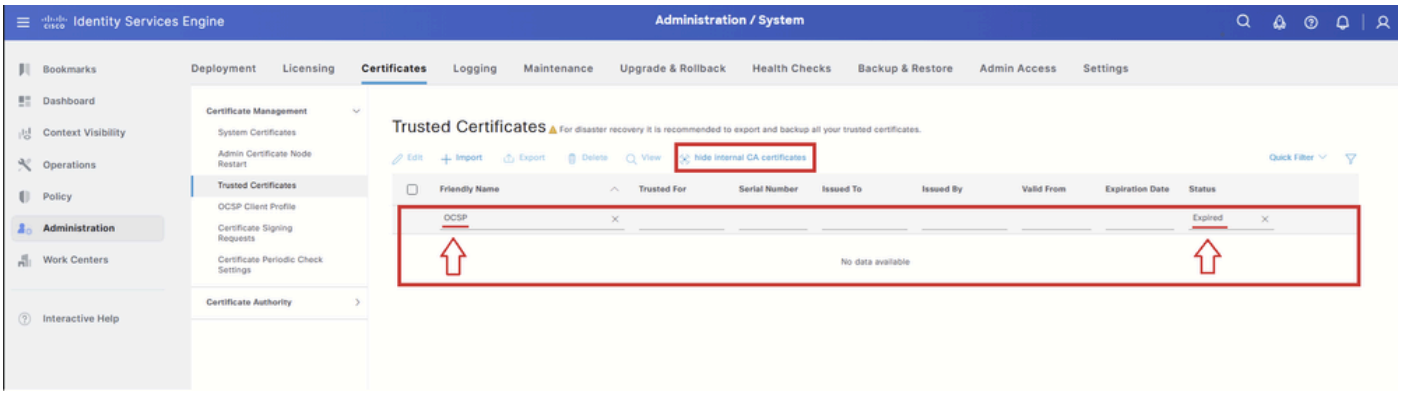
Er moet een vermelding worden weergegeven die aangeeft dat een configuratieobject is verwijderd. De objectnaam moet overeenkomen met het OCSP Responder-certificaat dat is verwijderd.



Optie 2 - Verifiëren in het vertrouwde certificaatarchief

Als extra stap navigeert u terug naar de tabel voor vertrouwde certificaatopslag en filtert u voor het OCSP-respondercertificaat. Aangezien het certificaat is verwijderd, moet in de tabel Geen gegevens beschikbaar worden weergegeven.

Opmerking: selecteer Interne CA-certificaten tonen.


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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.