Entfernen Sie abgelaufene interne OCSP-Responder-Zertifikate in der ISE.

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie abgelaufene und/oder bald ablaufende OCSP Responder-Zertifikate in der Cisco Identity Service Engine (ISE) gelöscht werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Grundkenntnisse der Identity Service Engine (ISE)
- Grundkenntnisse der Zertifikate.
- Online Certificate Status Protocol (OCSP)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Identity Service Engine 3.x

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt.Alle in diesem Dokument verwendeten Geräte begannen mit einer gelöschten (Standard-)Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Kunden, die die Cisco Identity Services Engine (ISE) verwenden, erhalten häufig Alarme, die darauf hinweisen, dass ein Zertifikat abgelaufen ist, insbesondere wenn das OCSP-Responder-Zertifikat abgelaufen ist oder bald abläuft und das Zertifikat nicht gefunden werden kann. Diese Situation führt häufig dazu, dass Kunden TAC-Tickets für Unterstützung öffnen. Der Leitfaden soll Kunden dabei helfen, abgelaufene oder bald ablaufende OCSP-Responder-Zertifikate zu lokalisieren und zu löschen. Auf diese Weise wird vermieden, dass ein TAC-Ticket erstellt werden muss.

Das Online Certificate Status Protocol (OCSP) ist ein Protokoll, das zur Statusüberprüfung von digitalen x.509-Zertifikaten verwendet wird. Dieses Protokoll ist eine Alternative zur Zertifikatsperrliste (Certificate Revocation List, CRL) und behandelt Probleme, die zur Behandlung von Zertifikatsperrlisten führen. Die Cisco ISE kann über HTTP mit OCSP-Servern kommunizieren, um den Status von Zertifikaten bei Authentifizierungen zu validieren. Die OCSP-Konfiguration wird in einem wiederverwendbaren Konfigurationsobjekt konfiguriert, auf das von jedem CA-Zertifikat (Certificate Authority) verwiesen werden kann, das in der Cisco ISE konfiguriert wurde.

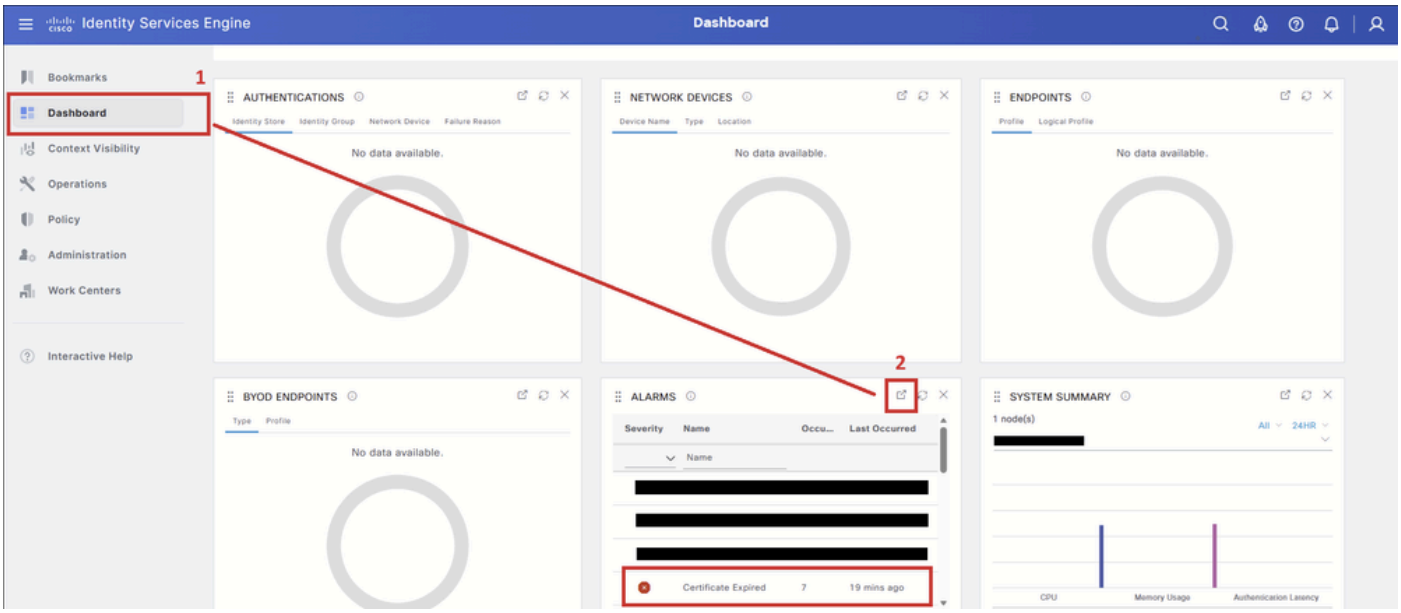
In jeder Cisco ISE-Bereitstellung sind OCSP-Responder-Zertifikate (Online Certificate Status Protocol) standardmäßig als Teil der Infrastruktur der internen Zertifizierungsstelle (Certificate Authority) vorhanden. Diese Zertifikate werden von der internen Cisco ISE-Zertifizierungsstelle auf dem PPAN (Primary Policy Administration Node) ausgestellt und automatisch für jeden Knoten in der Bereitstellung generiert, einschließlich des PAN und aller PSNs (Policy Service Nodes).

Die Verwaltung dieser OCSP Responder-Zertifikate ist wichtig, da abgelaufene oder bald ablaufende Zertifikate im Cisco ISE Dashboard abgelaufene Zertifikate auslösen können. Obwohl die Cisco ISE automatisch neue OCSP Responder-Zertifikate erstellt, bleiben die abgelaufenen Einträge im vertrauenswürdigen Zertifikatspeicher, bis sie manuell entfernt werden.

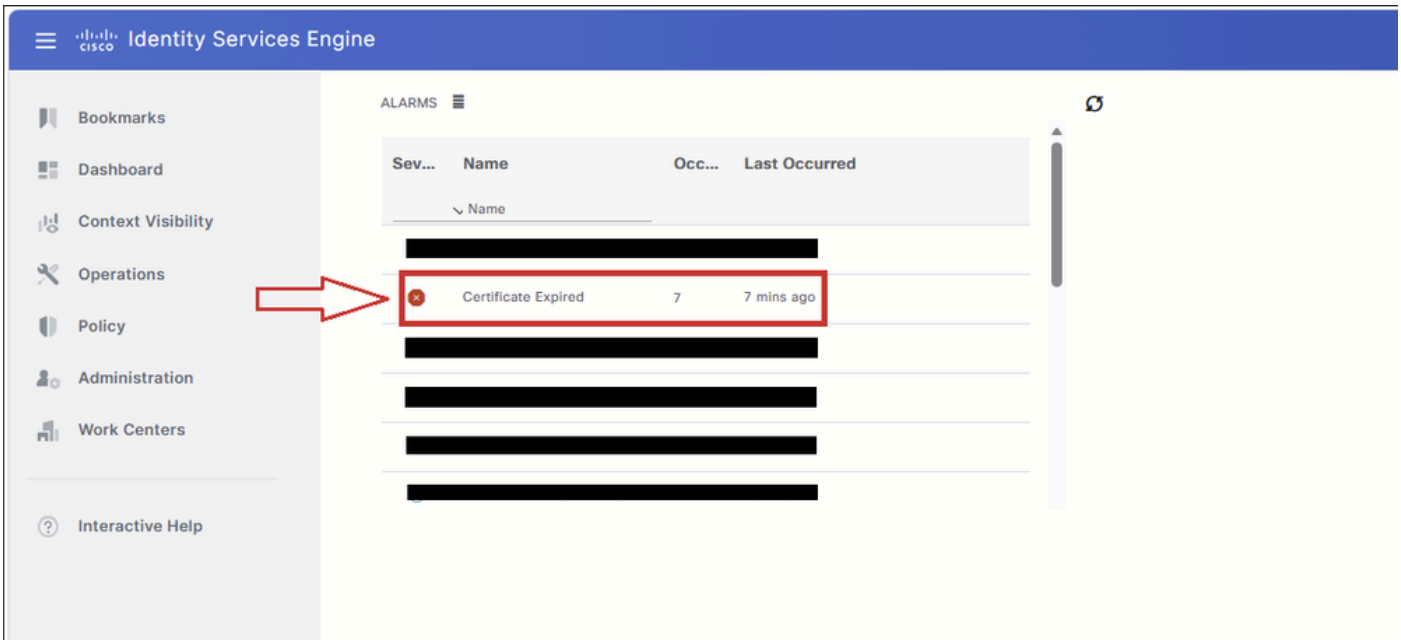
Konfiguration

Schritt 1: Überprüfen des abgelaufenen OCSP-Zertifikats

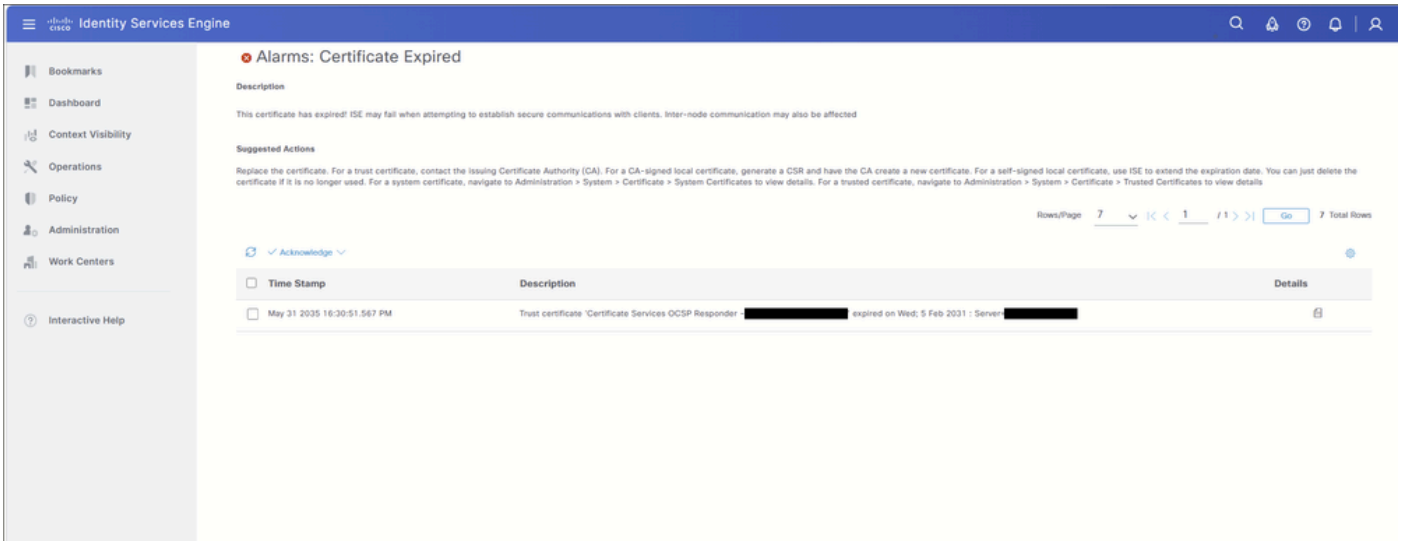
Navigieren Sie in der GUI von PPAN (Primary Policy Administration Node) zur Registerkarte Dashboard (1). Klicken Sie im Dashlet Alarme auf die Schaltfläche Trennen (2), um die Alarmtabelle zu erweitern.



Klicken Sie auf den Alarm Certificate Expired (Zertifikat abgelaufen), um die Tabelle zu erweitern und die Zertifikatseinträge anzuzeigen, die dem Alarm zugeordnet sind.



In dieser Tabelle werden alle Zertifikate angezeigt, die den Alarm "Zertifikat abgelaufen" ausgelöst haben. Dieses Handbuch behandelt nur OCSP-Responder-Zertifikate. Wenn die Tabelle andere abgelaufene Zertifikatstypen enthält, z. B. EAP, SAML, Admin oder andere Systemzertifikate, finden Sie in der entsprechenden Cisco Dokumentation und im Cisco ISE-Administratorhandbuch Hinweise zu diesen Zertifikatstypen.



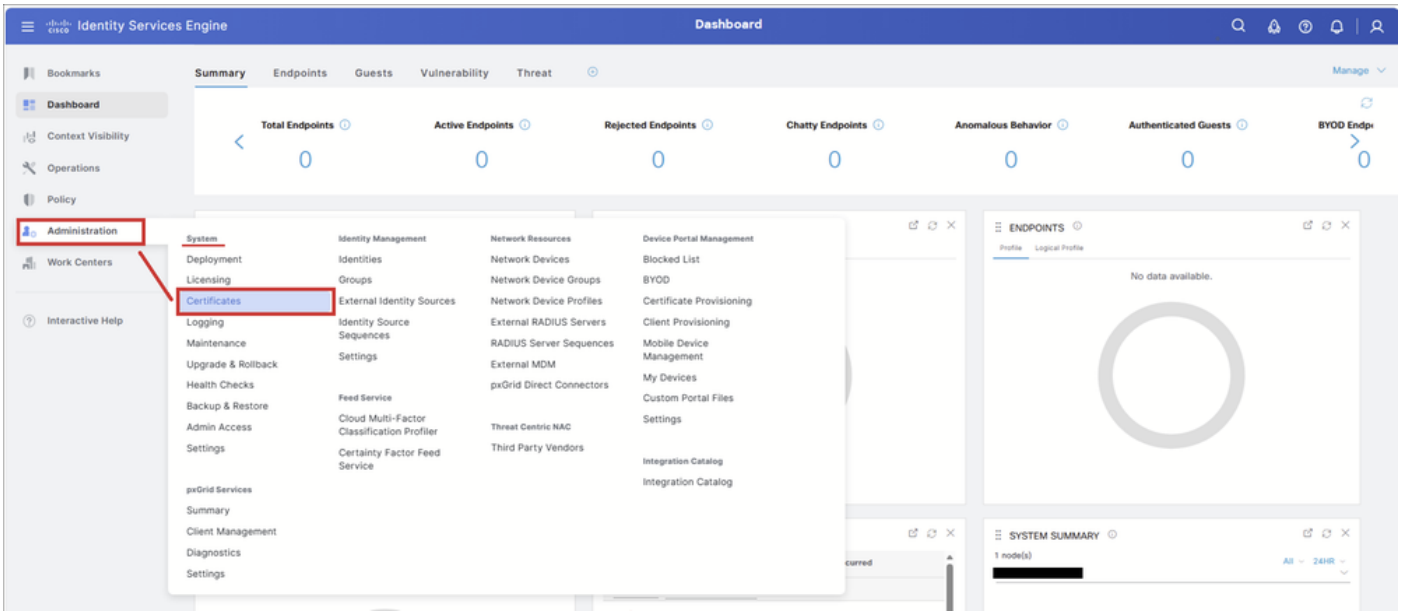
Überprüfen Sie die Alarmbeschreibung, um das abgelaufene oder in einigen Fällen bald ablaufende Zertifikat zu identifizieren.

In diesem Beispiel ist das abgelaufene Zertifikat: Certificate Services OCSP Responder - <Knotenname>#00004.

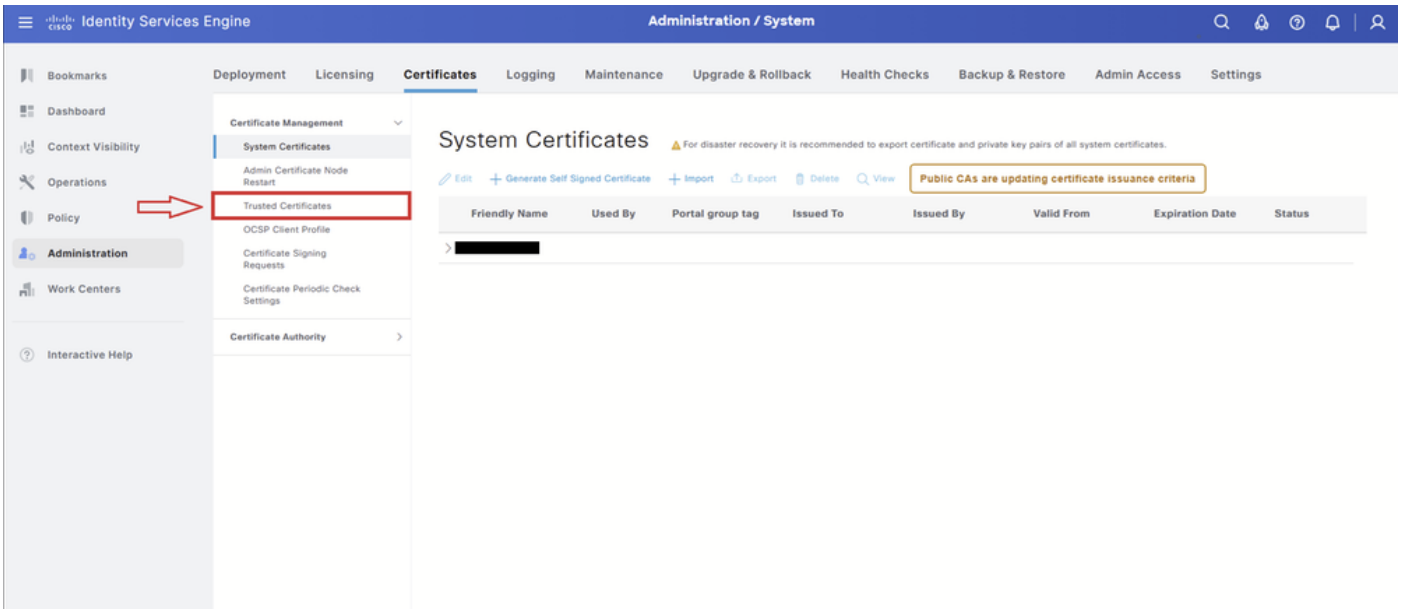
Notieren Sie sich den Namen des Zertifikats. Dieser Name wird in den nächsten Schritten verwendet, um das Zertifikat im vertrauenswürdigen Zertifikatspeicher zu suchen und zu löschen.

Schritt 2 - Suchen und Löschen des abgelaufenen OCSP-Zertifikats

Navigieren Sie zu: Administration > System > Zertifikate:



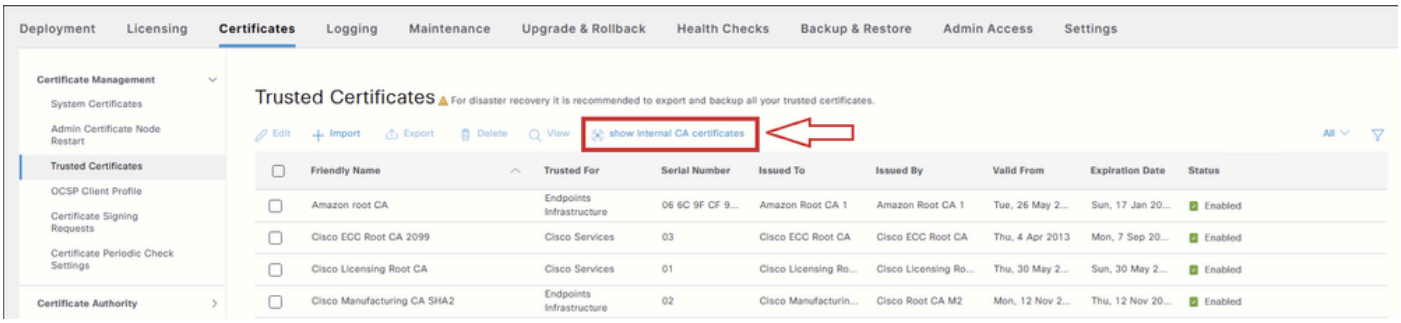
Wählen Sie die Registerkarte Vertrauenswürdige Zertifikate aus.



Wählen Sie auf der Seite Vertrauenswürdige Zertifikate die Option Interne Zertifizierungsstellenzertifikate anzeigen aus. Es werden die Cisco ISE Internal CA-Zertifikate (Certificate Authority) angezeigt, einschließlich der standardmäßig ausgeblendeten OCSP-Responder-Zertifikate.

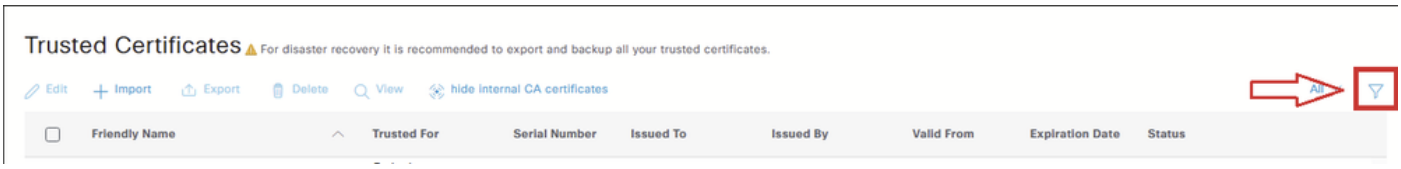
Nach der Auswahl wird die Schaltfläche so geändert, dass interne Zertifizierungsstellenzertifikate ausgeblendet werden.

Warnung: Dieser Schritt ist erforderlich. Wenn die Option zum Anzeigen interner Zertifizierungsstellenzertifikate nicht ausgewählt ist, wird das OCSP-Responder-Zertifikat nicht in der Tabelle für den vertrauenswürdigen Zertifikatspeicher angezeigt.

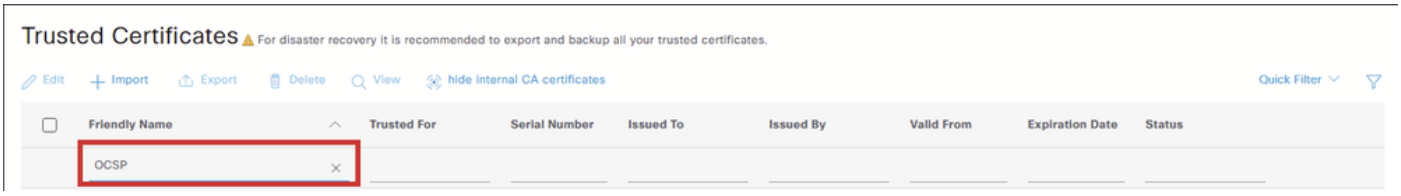


Wählen Sie in der Tabelle Vertrauenswürdiger Zertifikatspeicher das Symbol Filter (Filter) aus, um

nach dem zu löschenden Zertifikat zu suchen.

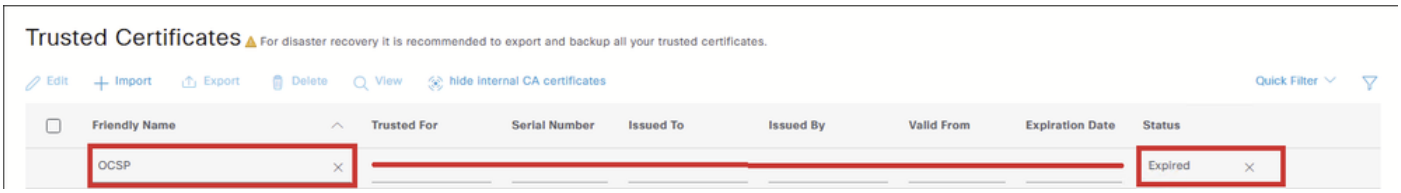


Wenn das OCSP-Responder-Zertifikat bald abläuft, filtern Sie unter "Freundlicher Name" nur nach OCSP. Wenn das OCSP Responder-Zertifikat bereits abgelaufen ist, fahren Sie mit der nächsten Aktion fort.



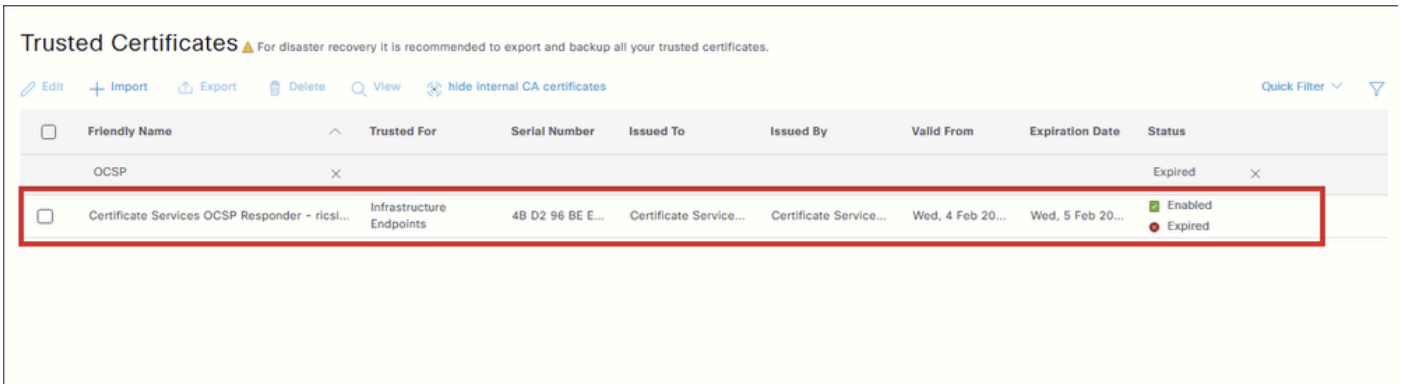
Um ein abgelaufenes OCSP Responder-Zertifikat zu finden, geben Sie folgende Filter ein:

- Anzeigename: OCSP
- Status: Abgelaufen

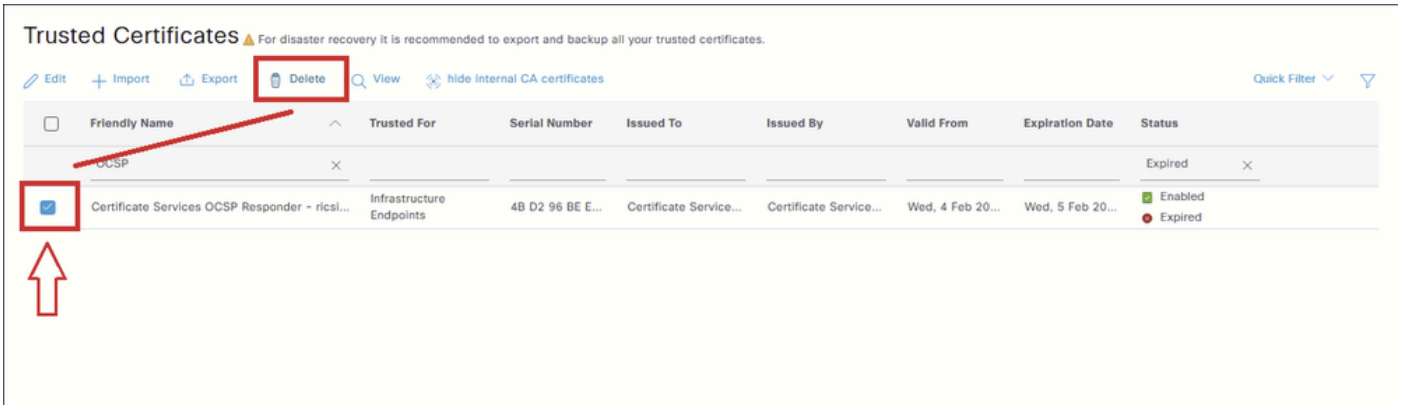


In der Tabelle werden die abgelaufenen OCSP-Responder-Zertifikate angezeigt.

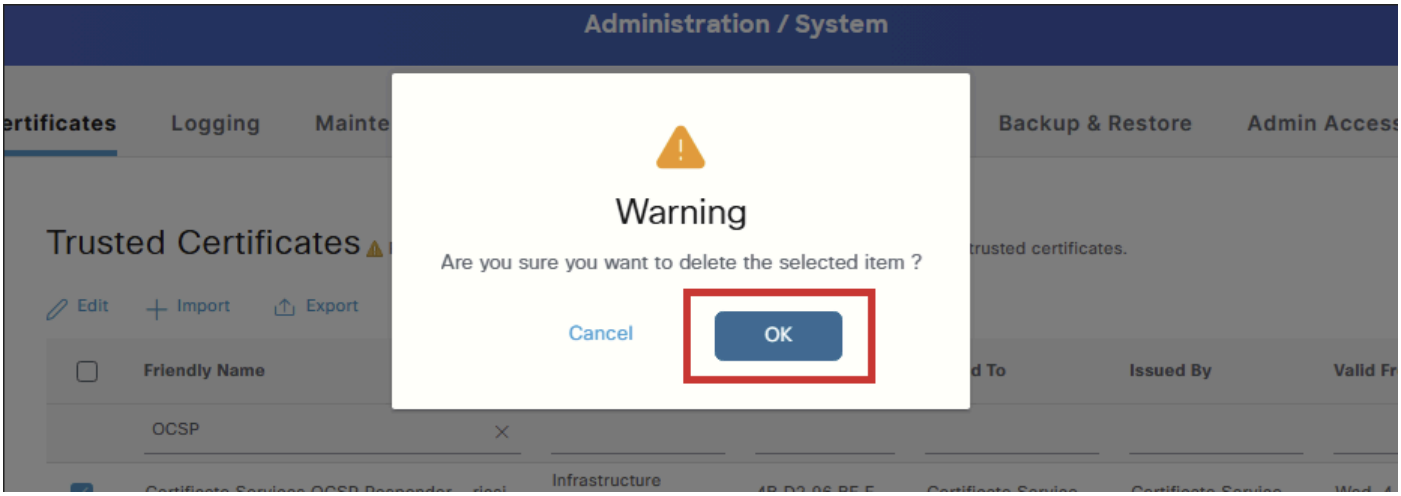
Tipp: Wenn Sie nach einem OCSP Responder-Zertifikat suchen, das bald abläuft, können mehrere Zertifikate angezeigt werden, insbesondere in Bereitstellungen mit mehreren Cisco ISE-Knoten. Um das richtige Zertifikat zu identifizieren, filtern Sie nicht nur nach OCSP. Filtern Sie stattdessen nach dem vollständigen Zertifikatsnamen, der in den Alarmdetails in Schritt 1 angezeigt wurde.



Aktivieren Sie das Kontrollkästchen neben dem zu entfernenden OCSP-Responder-Zertifikat, und klicken Sie auf Löschen.



Klicken Sie in der Bestätigungswarnung auf OK, um mit dem Löschen des Zertifikats fortzufahren.



Bevor Sie das Zertifikat löschen, ist es wichtig zu wissen, dass das OCSP-Responder-Zertifikat Teil der internen ISE-Zertifizierungsstelleninfrastruktur ist.

Die Warnung, die beim Löschen angezeigt wird, ist allgemein gehalten und gilt für alle internen CA-bezogenen Zertifikate. Sie dient dazu, vor dem Löschen von Zertifikaten in der internen Zertifizierungsstellenhierarchie zu warnen, da einige dieser Zertifikate Endpunktzertifikate signieren, die für Dienste wie BYOD, pxGrid oder andere Funktionen verwendet werden, die auf von der internen ISE-Zertifizierungsstelle ausgestellten Zertifikaten basieren.

Ein abgelaufenes OCSP-Responder-Zertifikat kann sich auch auf Zertifikate auswirken, die von der internen ISE-Zertifizierungsstelle ausgestellt wurden. Wenn ein Client oder Dienst den Status eines von dieser Zertifizierungsstelle ausgestellten Zertifikats abfragt, gibt der OCSP-Dienst einen Fehler zurück, da das OCSP-Responder-Zertifikat abgelaufen ist. Dies kann dazu führen, dass die Überprüfung des Zertifikatsstatus fehlschlägt.

Wenn Sie Löschen auswählen, werden zwei Optionen angezeigt:

- Zertifikat löschen: Mit dieser Option wird das interne Cisco ISE-Zertifizierungsstellenzertifikat aus dem Speicher für vertrauenswürdige Zertifikate gelöscht. Wenn das Zertifikat der internen Zertifizierungsstelle gelöscht wird, werden alle von dieser Zertifizierungsstelle signierten Endpunktzertifikate ungültig, und die betroffenen Endpunkte können nicht auf das Netzwerk zugreifen. Diese Aktion kann rückgängig gemacht werden: Sie können den Netzwerkzugriff wiederherstellen, indem Sie das gleiche interne Zertifizierungsstellenzertifikat zurück in den Speicher für vertrauenswürdige Zertifikate importieren.
- Zertifikat löschen und widerrufen: Diese Option löscht und widerruft das interne Zertifikat der Cisco ISE-Zertifizierungsstelle. Wie bei der Option "Löschen" werden alle von der internen Zertifizierungsstelle signierten Endpunktzertifikate ungültig, und die betroffenen Endpunkte verlieren den Netzwerkzugriff. Dieser Vorgang ist jedoch irreversibel. Nach dem Widerruf müssen Sie die gesamte Cisco ISE-Stammzertifikatkette für die Bereitstellung ersetzen, um die Funktionalität wiederherzustellen.

Welche Option kann für ein abgelaufenes OCSP-Responder-Zertifikat ausgewählt werden?

Die beschriebenen Auswirkungen gelten für interne Zertifizierungsstellenzertifikate, die Endpunktzertifikate aktiv signieren. Das OCSP-Responder-Zertifikat signiert keine Endpunktzertifikate. Es wird für die OCSP-Kommunikation verwendet. Während ein abgelaufenes OCSP-Responder-Zertifikat dazu führen kann, dass die Überprüfung des Zertifikatsstatus für von der internen Zertifizierungsstelle ausgestellte Zertifikate fehlschlägt, ist das Zertifikat bereits abgelaufen und stellt daher keine gültigen OCSP-Antworten mehr bereit. Das Löschen hat keine

zusätzlichen Auswirkungen.

Da das OCSP-Responder-Zertifikat in diesem Szenario bereits abgelaufen ist, ist es nicht mehr gültig. In diesem Fall führen sowohl Delete als auch Delete & Revoke zum gleichen Ergebnis, da nichts mehr zu widerrufen ist.

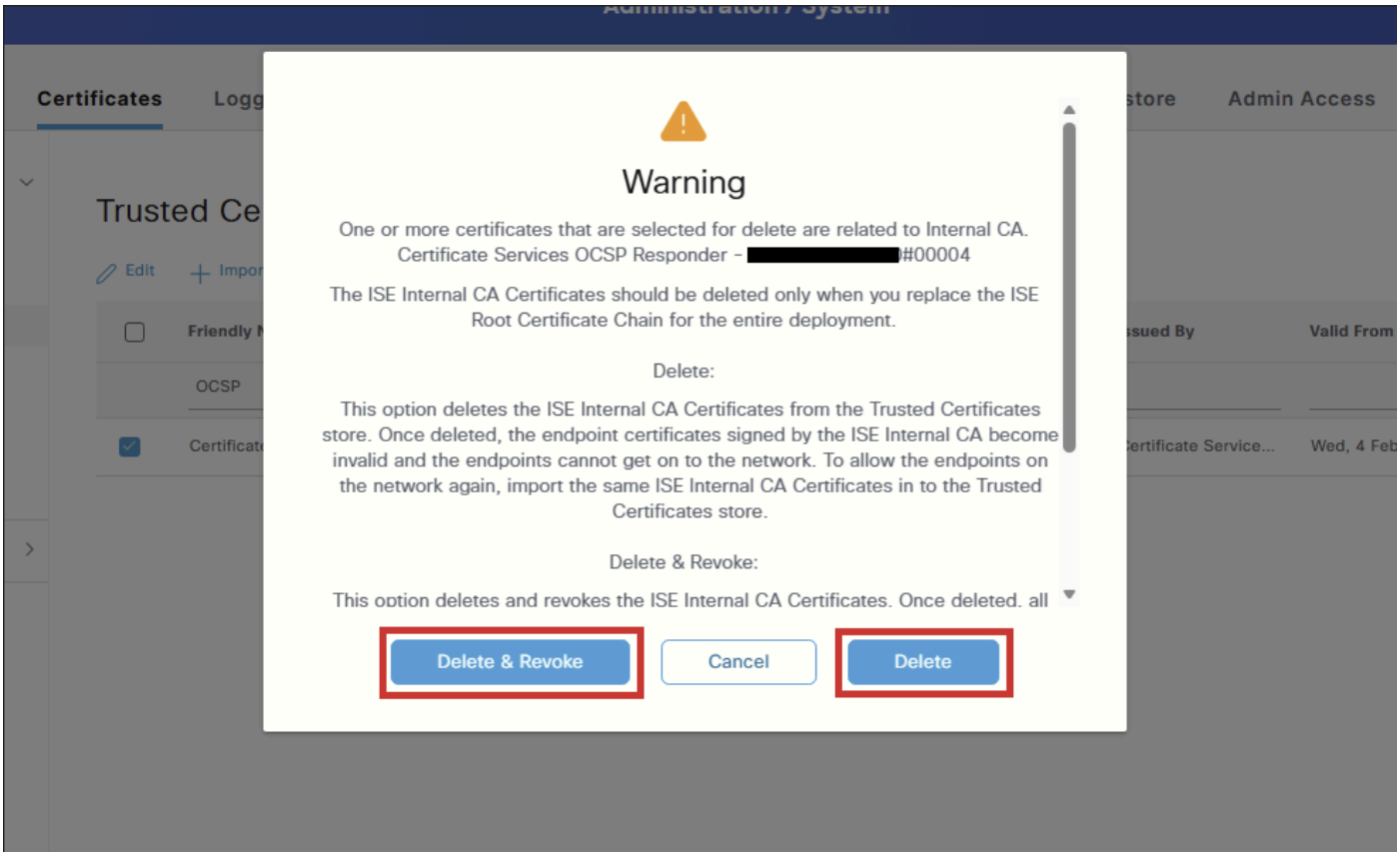
Aus diesen Gründen ist Löschen die empfohlene Option, da es sich um die einfachere Aktion handelt und keine unnötige Sperrung erzeugt werden muss.

Anmerkung: OCSP-Responder-Zertifikate werden im Normalbetrieb nicht neu generiert. Sie werden nur dann regeneriert, wenn ein Patch installiert wird:
- In einer Bereitstellung mit mehreren Knoten werden die Zertifikate neu generiert, wenn der Patch über die GUI installiert wird.
- In einer Standalone-Bereitstellung werden die Zertifikate neu generiert, wenn der Patch über die GUI oder die CLI installiert wird.

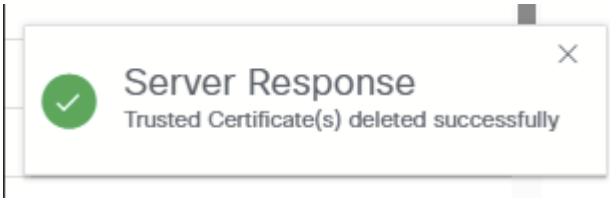
Ein neues OCSP Responder-Zertifikat wird erst bei der nächsten Patch-Installation generiert.

Vorsicht: Stellen Sie sicher, dass der betroffene Knoten über ein aktives, gültiges OCSP-Responder-Zertifikat im vertrauenswürdigen Zertifikatspeicher verfügt. Wenn kein gültiges Zertifikat vorhanden ist und OCSP zum Validieren von Zertifikaten verwendet wird, die von der internen ISE-Zertifizierungsstelle signiert wurden, schlägt die Validierung fehl, bis ein neues OCSP-Responder-Zertifikat generiert wird.

Wenn kein gültiges OCSP-Responder-Zertifikat vorhanden ist, erneuern Sie die OCSP-Responder-Zertifikate vom PPAN (Primary Policy Administration Node) wie hier beschrieben:
1. Zugriff auf die ISE PPAN-GUI
2. Gehen Sie zu Administration > System > Certificates.
3. Wählen Sie links Zertifikatsignierungsanforderungen aus.
4. Klicken Sie auf CSR erstellen. Wählen Sie zur Verwendung die Option Renew ISE OCSP Responder (ISE OCSP-Responder verlängern).
5. Klicken Sie auf Renew ISE OCSP Responder Certificates (ISE OCSP-Responder-Zertifikate verlängern), um den Prozess abzuschließen.



Nachdem das Zertifikat gelöscht wurde, wird eine Serverantwort-Benachrichtigung angezeigt, die angibt, dass das vertrauenswürdige Zertifikat erfolgreich gelöscht wurde:



Überprüfung

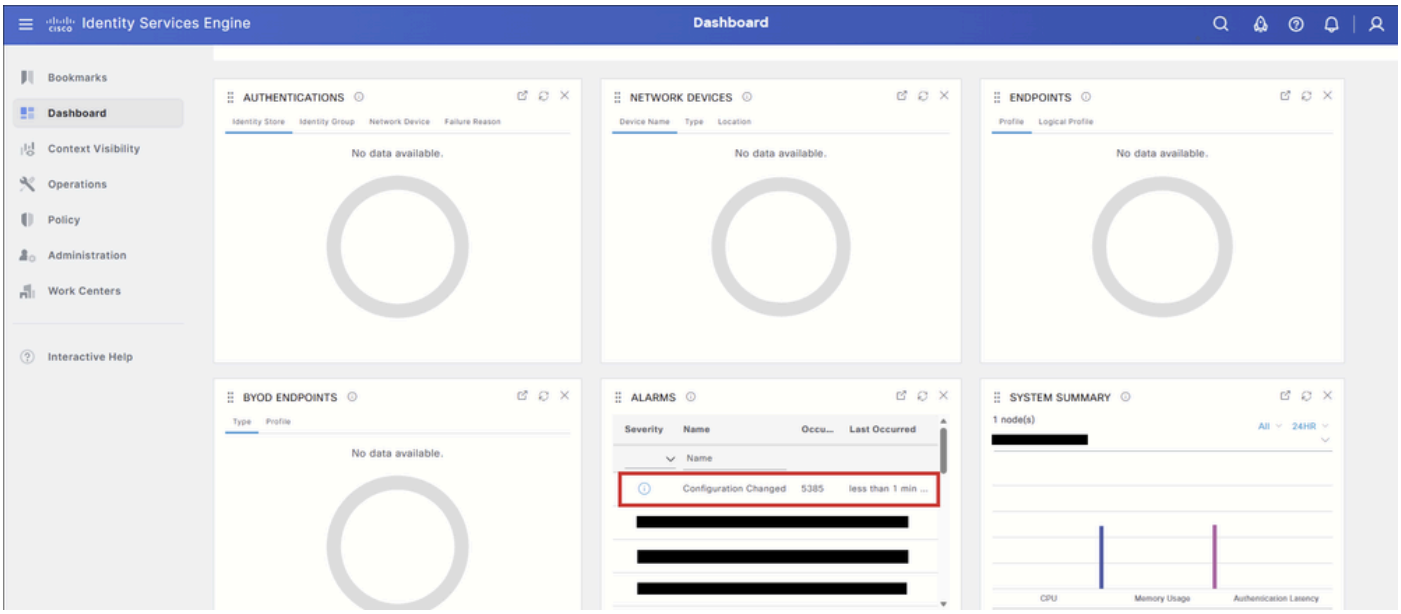
Nachdem das Zertifikat gelöscht wurde, können Sie mit einer oder beiden Methoden überprüfen, ob der Vorgang erfolgreich war.

Option 1 - Überprüfung anhand von Dashboard-Warnmeldungen

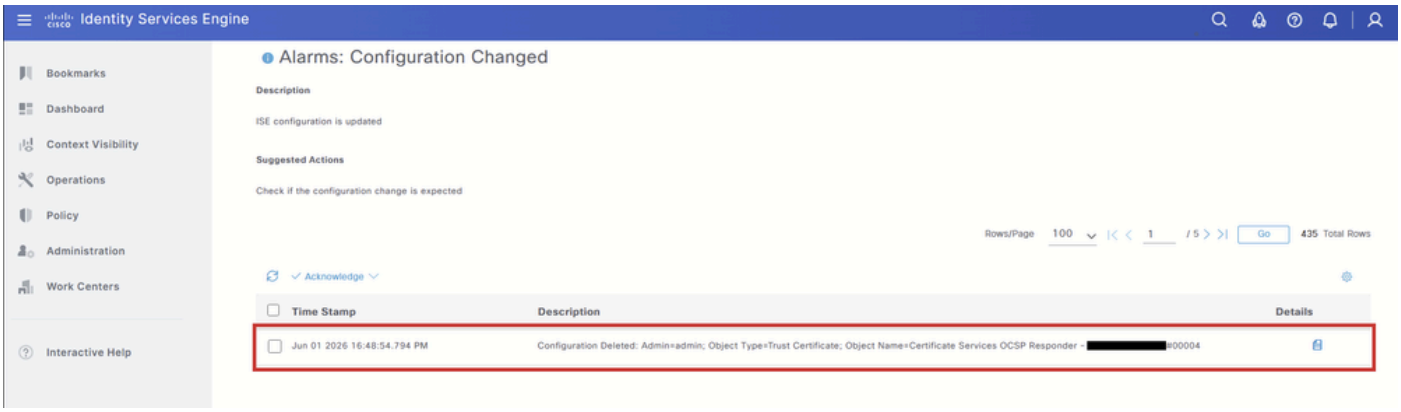
Navigieren Sie zur Seite Dashboard.

Suchen Sie im Dashlet "Alarme" den Alarm "Configuration Changed". Wählen Sie den Alarm aus,

um die Details anzuzeigen.



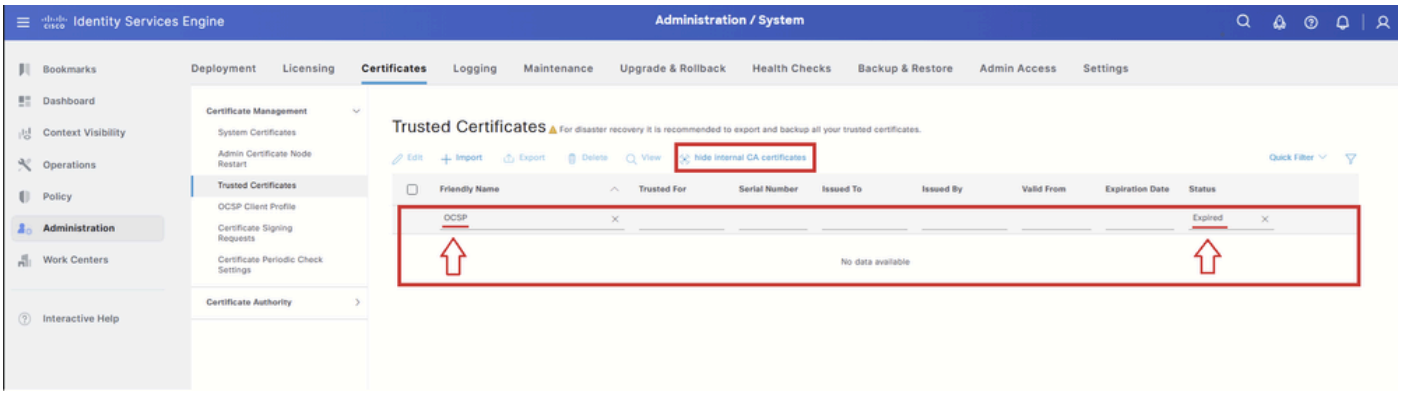
Es muss ein Eintrag angezeigt werden, der angibt, dass ein Konfigurationsobjekt gelöscht wurde. Der Objektname muss mit dem entfernten OCSP-Responder-Zertifikat übereinstimmen.



Option 2 - Überprüfung im Speicher für vertrauenswürdige Zertifikate

Navigieren Sie als zusätzlichen Schritt zurück zur Tabelle für den vertrauenswürdigen Zertifikatsspeicher, und filtern Sie nach dem OCSP-Responder-Zertifikat. Da das Zertifikat gelöscht wurde, muss die Tabelle "Keine Daten verfügbar" anzeigen.

Anmerkung: Denken Sie daran, interne Zertifizierungsstellenzertifikate anzeigen auszuwählen.


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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.