刪除ISE中的過期內部OCSP響應方證書

目錄

簡介

本文檔介紹如何在思科身份服務引擎(ISE)中刪除過期和/或即將過期OCSP響應方證書。

必要條件

需求

思科建議您瞭解以下主題：

- 身份服務引擎(ISE)的基本知識。
- 憑證的基本知識。
- 線上憑證狀態通訊協定(OCSP)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科身分識別服務引擎3.x

本文中的資訊是根據特定實驗室環境內的裝置所建立。本檔案中使用的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

使用Cisco Identity Services Engine(ISE)的客戶面臨的常見問題是收到警報，指示證書已過期，特別是在OCSP響應方證書過期或即將過期且找不到證書時。這種情況通常會導致客戶開啟TAC案例以尋求協助。本指南的目標是使客戶能夠找到並刪除這些已過期或即將過期的OCSP響應者證書，從而避擴音出TAC案例的需要。

線上證書狀態協定(OCSP)是用於檢查x.509數位證書狀態的協定。此通訊協定是憑證撤銷清單(CRL)的替代通訊協定，並處理導致處理CRL的問題。思科ISE能夠通過HTTP與OCSP伺服器通訊，以驗證身份驗證中的證書狀態。OCSP配置配置在一個可重用的配置對象中，該對象可以從思科ISE中配置的任何證書頒發機構(CA)證書引用。

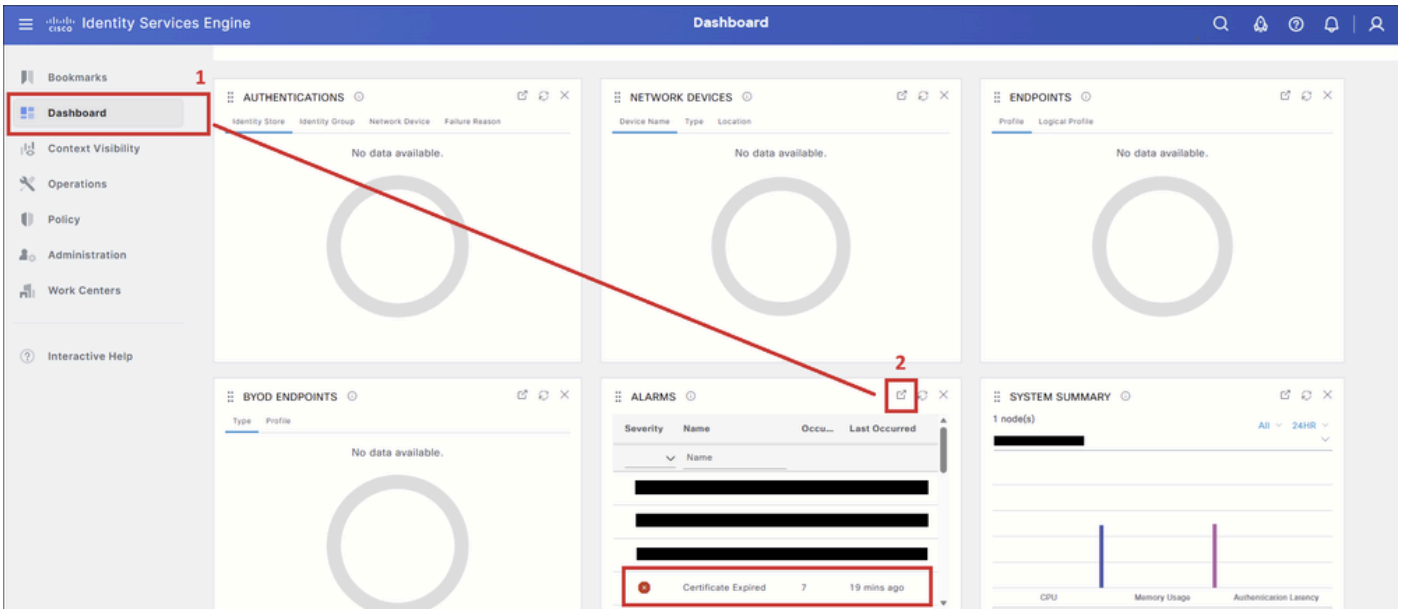
在每個思科ISE部署中，OCSP（線上證書狀態協定）響應方證書預設作為內部CA（證書頒發機構）基礎設施的一部分存在。這些證書由思科ISE內部CA在PPAN（主策略管理節點）上頒發，並為部署中的每個節點(包括PAN和所有PSN（策略服務節點）)自動生成。

管理這些OCSP響應方證書非常重要，因為過期或即將過期的證書可能會在思科ISE控制面板中觸發證書過期警報。儘管Cisco ISE會自動重新生成新的OCSP響應方證書，但過期的條目仍保留在受信任的證書儲存中，直到手動刪除它們。

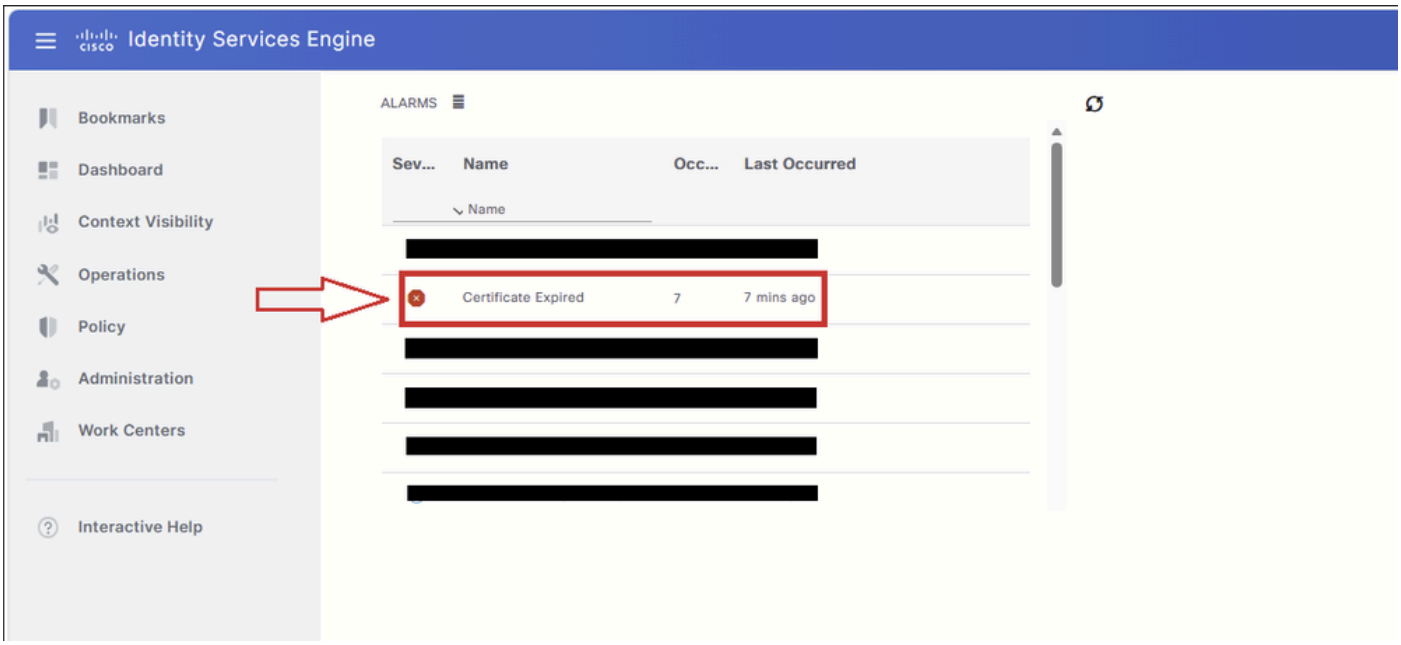
組態

第1步 — 驗證過期的OCSP證書

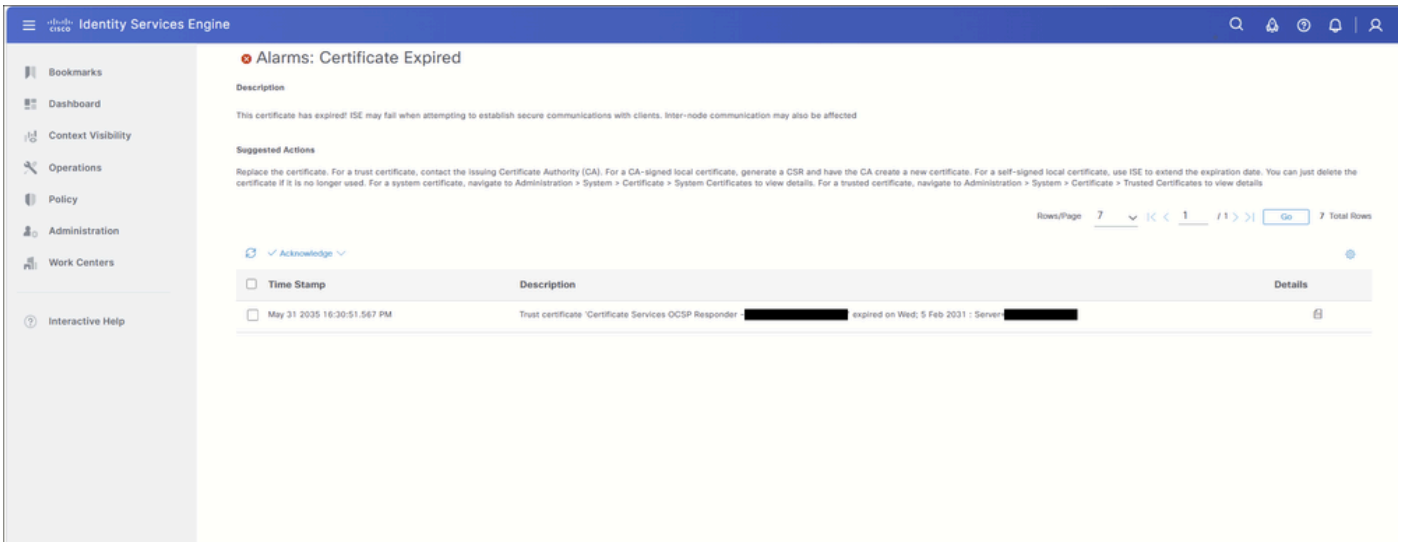
在PPAN(主策略管理節點)GUI中，導航到Dashboard（控制面板）頁籤(1)。 在Alarms dashlet中，按一下Detach按鈕(2)以展開警報表。



按一下Certificate Expired警報以展開表並顯示與警報相關聯的證書條目。



所有觸發「證書已過期」警報的證書都顯示在此表中。本指南僅重點介紹OCSP響應程式證書。如果表格包含其他過期證書型別，例如EAP、SAML、Admin或其他系統證書，請參閱相關思科文檔和Cisco ISE管理員指南獲取有關這些證書型別的指南。



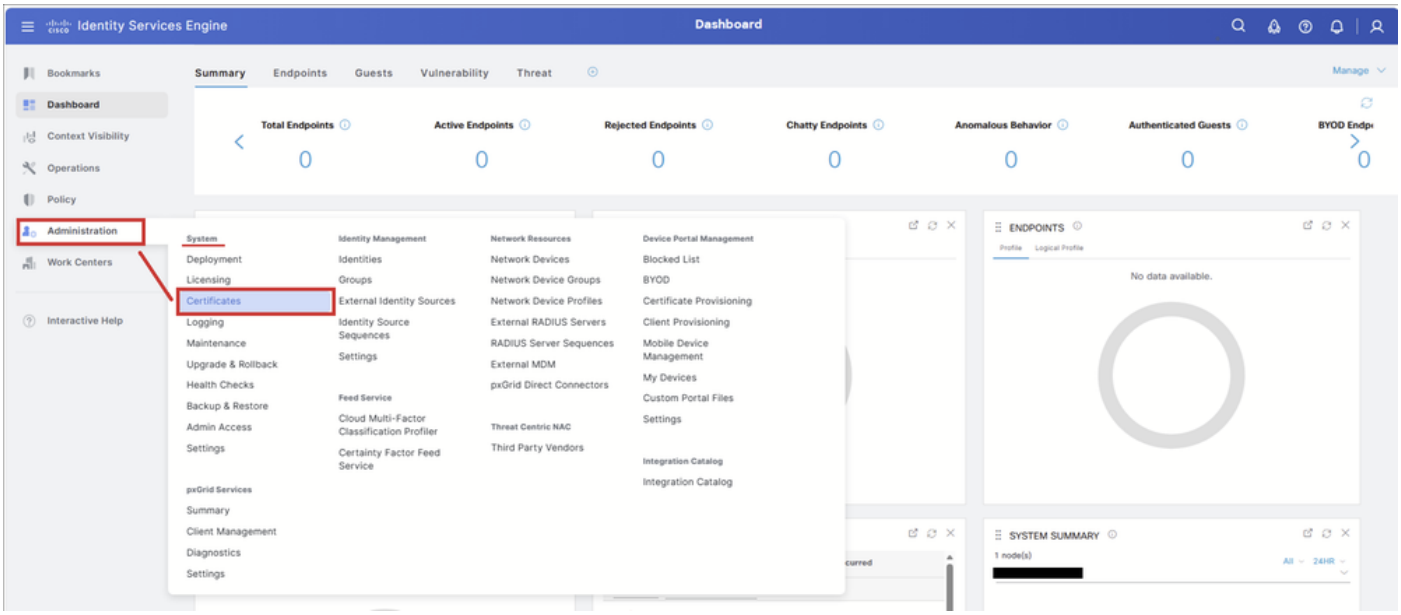
檢視警報描述，以確定已到期或在某些情況下即將到期的證書。

在本範例中，到期憑證為：證書服務OCSP響應器 — <node-name>#00004。

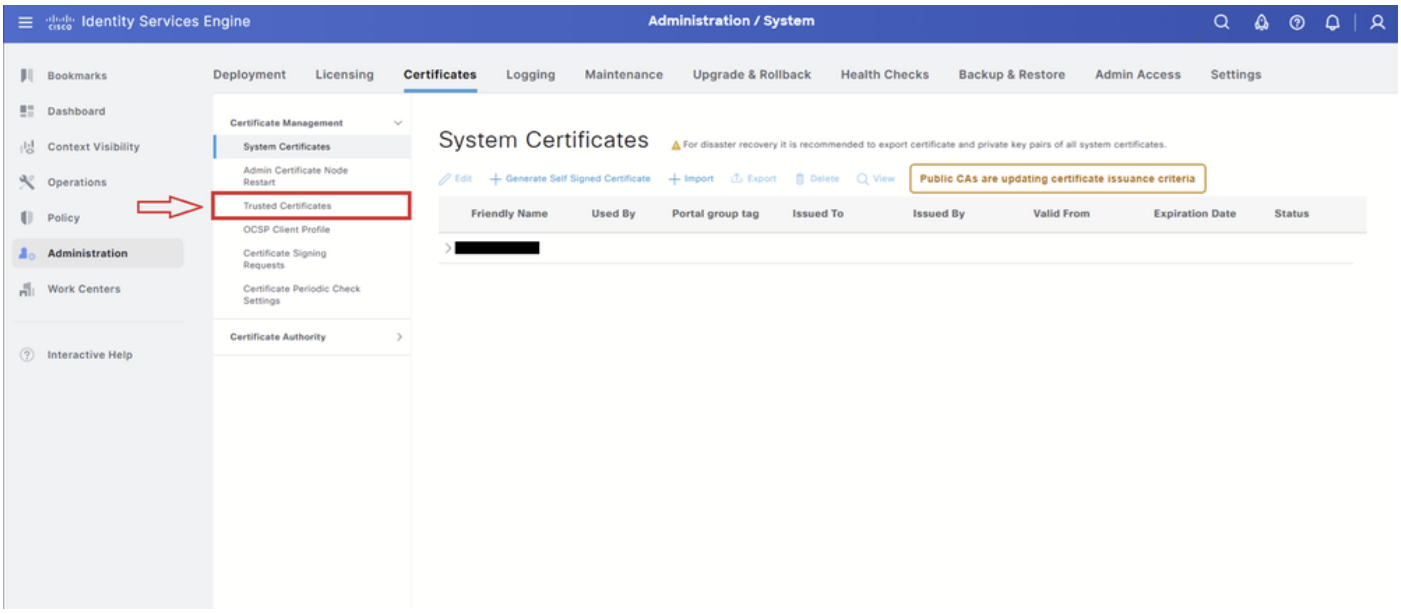
請注意證書名稱。此名稱用於後續步驟，以從受信任的證書儲存區查詢和刪除證書。

第2步 — 查詢並刪除過期的OCSP證書

導覽至：管理>系統>證書:



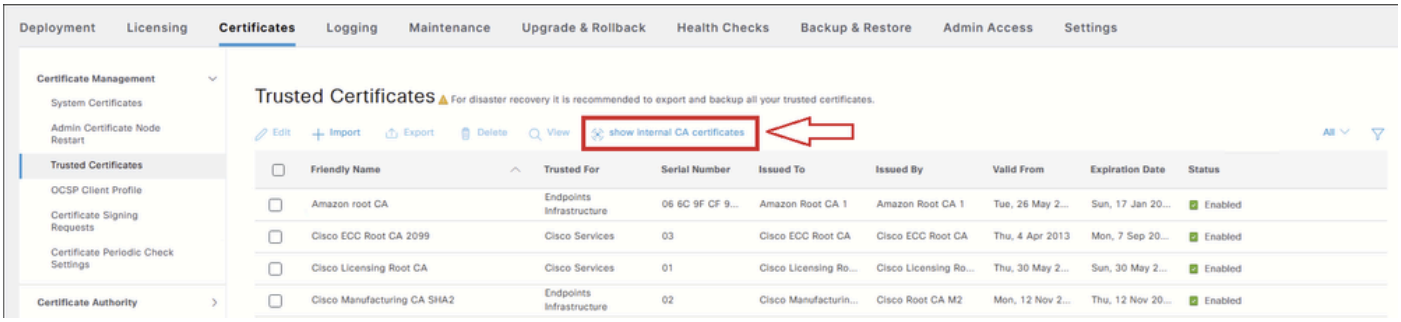
選擇Trusted Certificates頁籤。



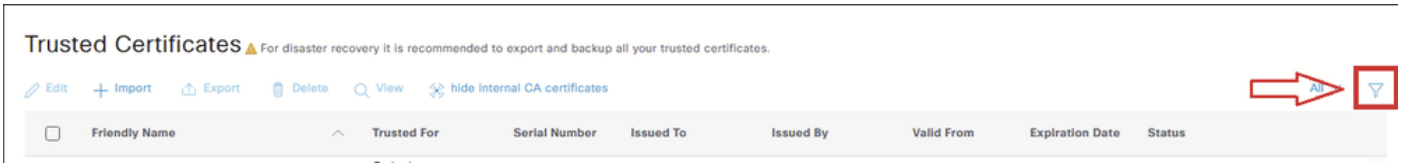
在Trusted Certificates頁面上，選擇show internal CA certificates。這將顯示Cisco ISE內部CA（證書頒發機構）證書，包括預設隱藏的OCSP響應方證書。

選擇後，該按鈕將更改為隱藏內部CA證書。

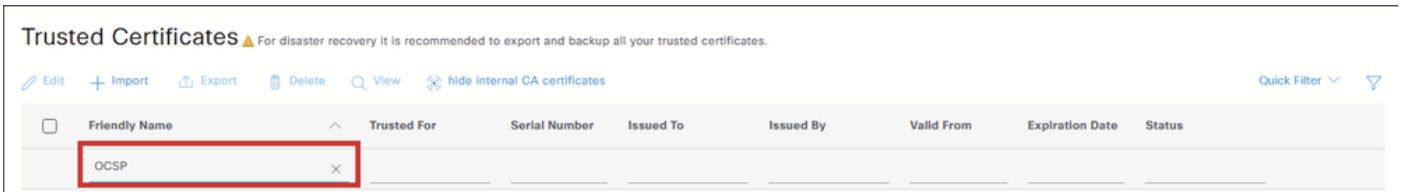
警告：此步驟是必需的。如果未選擇show internal CA certificates，則OCSP Responder證書不會顯示在Trusted Certificate Store表中。



在Trusted Certificate Store表中，選擇Filter圖示以搜尋必須刪除的證書。

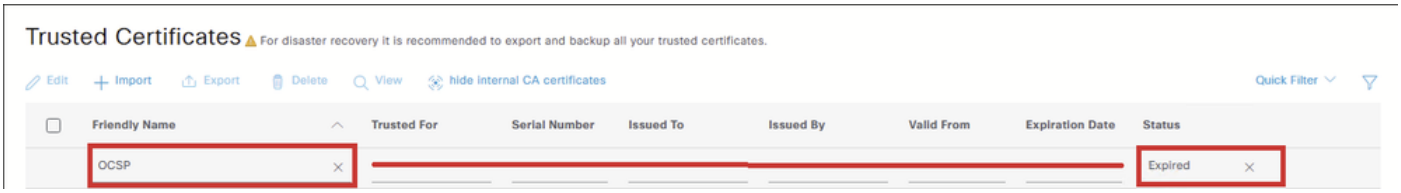


如果OCSP響應方證書即將過期，則僅按「友好名稱」下的OCSP進行過濾。如果OCSP響應程式證書已過期，請繼續執行下一步操作。



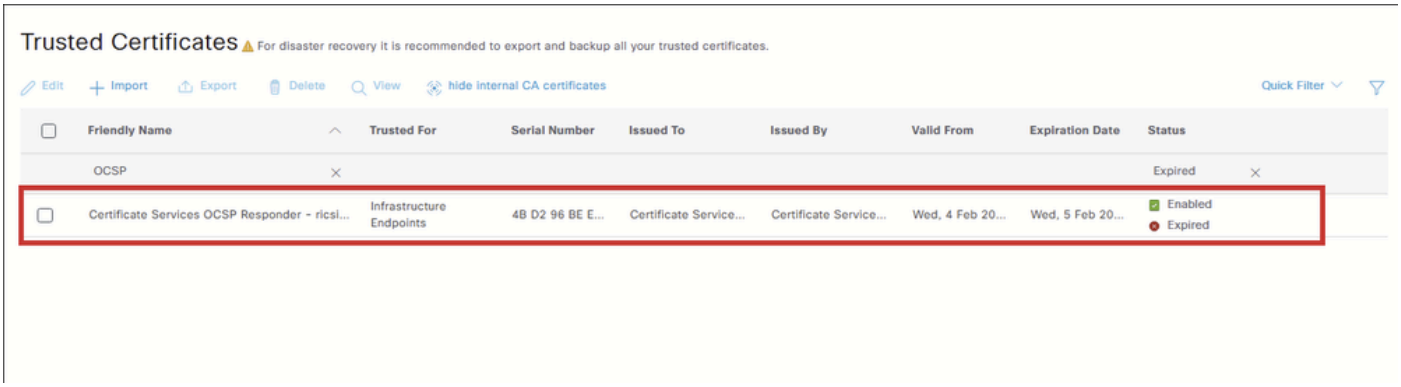
要查詢已過期的OCSP響應方證書，請輸入以下篩選器：

- 友好名稱:OCSP
- 狀態:已到期

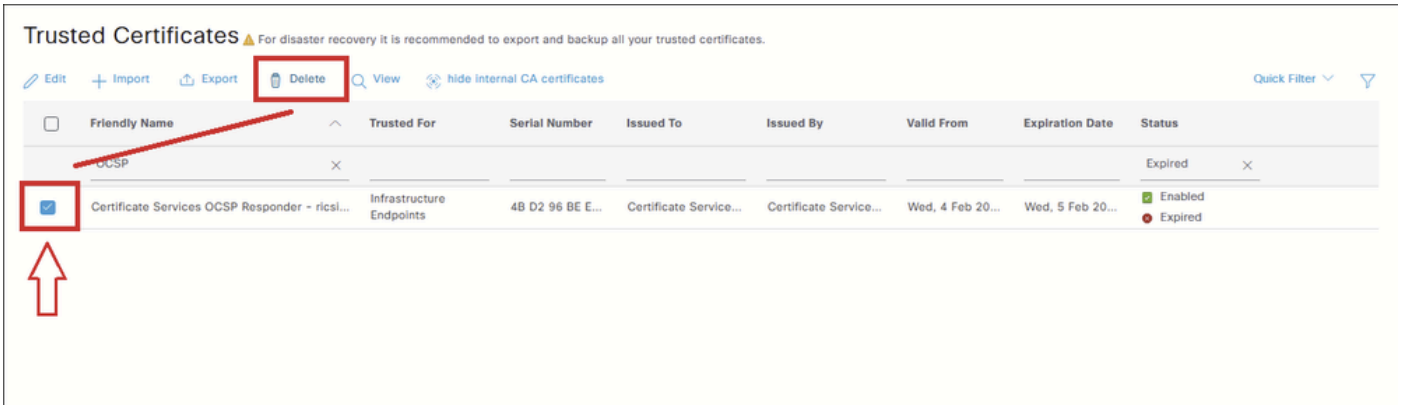


該表顯示過期的OCSP響應方證書。

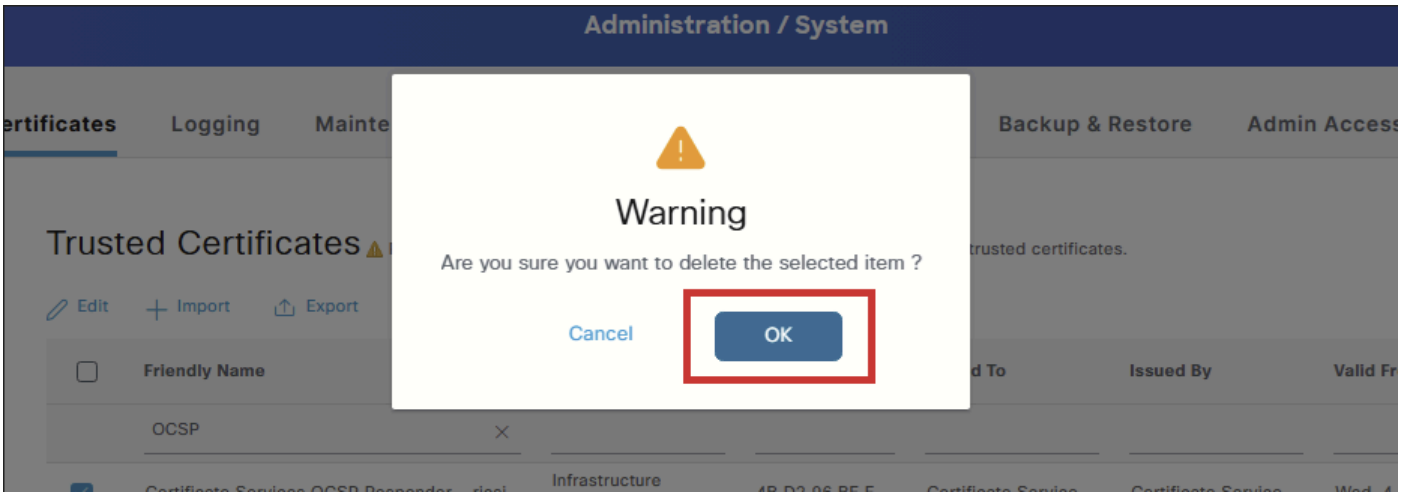
提示：如果您正在搜尋即將到期的OCSP響應方證書，則可以顯示多個證書，尤其是在具有多個思科ISE節點的部署中。要識別正確的證書，請不要僅按OCSP進行過濾。相反，請按照步驟1中警報詳細資訊中顯示的完整證書名稱進行過濾。



選中必須刪除的OCSP Responder證書旁邊的覈取方塊，然後按一下Delete。



在確認警告上選擇OK以繼續刪除證書。



刪除證書之前，必須瞭解OCSP響應方證書是ISE內部CA基礎設施的一部分。

刪除期間出現的警告是通用的，適用於所有內部CA相關證書。其目的是警告不要刪除內部CA層次結構中的證書，因為其中某些證書簽署用於服務（例如BYOD、pxGrid）或其他依賴於ISE內部CA頒發的證書的功能的終端證書。

過期的OCSP響應方證書也會影響ISE內部CA頒發的證書。當客戶端或服務查詢該CA頒發的證書的狀態時，OCSP服務將返回一個錯誤，因為OCSP響應方證書已過期，這可能導致證書狀態驗證失敗。

選擇Delete時，將顯示兩個選項：

- 刪除證書：此選項從受信任證書儲存中刪除Cisco ISE內部CA證書。刪除內部CA證書時，該CA簽署的所有端點證書將失效，受影響的端點無法訪問網路。此操作是可逆的：通過將同一內部CA證書匯入回受信任證書儲存區，可以恢復網路訪問。
- 刪除和撤銷證書：此選項刪除和撤銷思科ISE內部CA證書。與刪除選項一樣，由內部CA簽名的所有端點證書都變為無效，受影響的端點將失去網路訪問許可權。但是，此操作是不可逆的。撤銷後，您必須替換整個思科ISE根證書鏈，以便部署恢復功能。

對於已過期的OCSP響應程式證書，應選擇哪個選項？

描述的影響適用於主動簽署終端證書的內部CA證書。OCSP響應方證書不對終端證書簽名，它用於OCSP通訊。雖然過期的OCSP響應程式證書可能導致內部CA頒發的證書的證書狀態驗證失敗，但該證書已過期，因此不再提供有效的OCSP響應。刪除它不會帶來任何額外影響。

由於此方案中的OCSP響應方證書已過期，因此它不再有效。在這種情況下，「刪除」和「刪除和撤消」都會產生相同的結果，因為沒有任何有效的內容可以撤消。

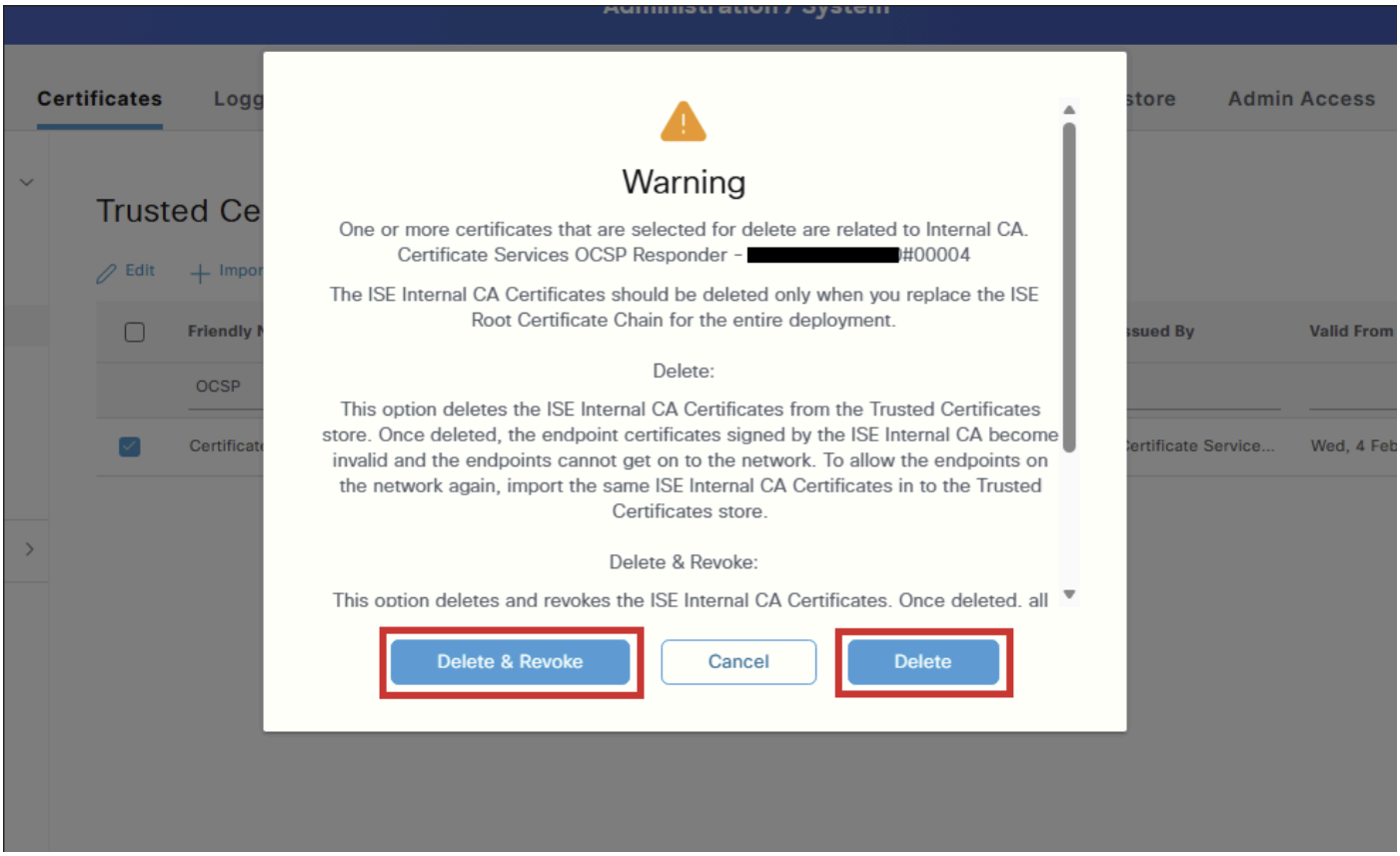
由於這些原因，建議使用Delete選項，因為它是更簡單的操作，並且避免了生成不必要的撤銷條目。

附註：在正常操作期間，不會重新生成OCSP響應方證書。僅當安裝了修補程式時才重新生成它們：
— 在多節點部署中，通過GUI安裝補丁時會重新生成證書。
— 在獨立部署中，當通過GUI或CLI安裝修補程式時，將重新生成證書。

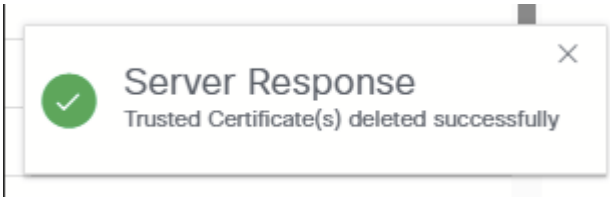
只有在下次安裝修補程式時，才會生成新的OCSP響應程式證書。

注意：請確保受影響的節點在受信任的證書儲存區中具有有效的活動OCSP響應方證書。如果有效的證書不存在，並且使用OCSP來驗證ISE內部CA簽名的證書，則驗證會失敗，直到生成新的OCSP響應方證書。

如果沒有有效的OCSP響應方證書，請從PPAN（主策略管理節點）續訂OCSP響應方證書，如下所述：
1.訪問ISE PPAN GUI。
2.轉到管理>系統>證書。
3.選擇左側的Certificate Signing Requests。
4.按一下「產生CSR」。對於Usage，選擇Renew ISE OCSP Responder。
5.按一下Renew ISE OCSP Responder Certificates完成此過程。



刪除證書後，將出現伺服器響應通知，指示已成功刪除受信任的證書：



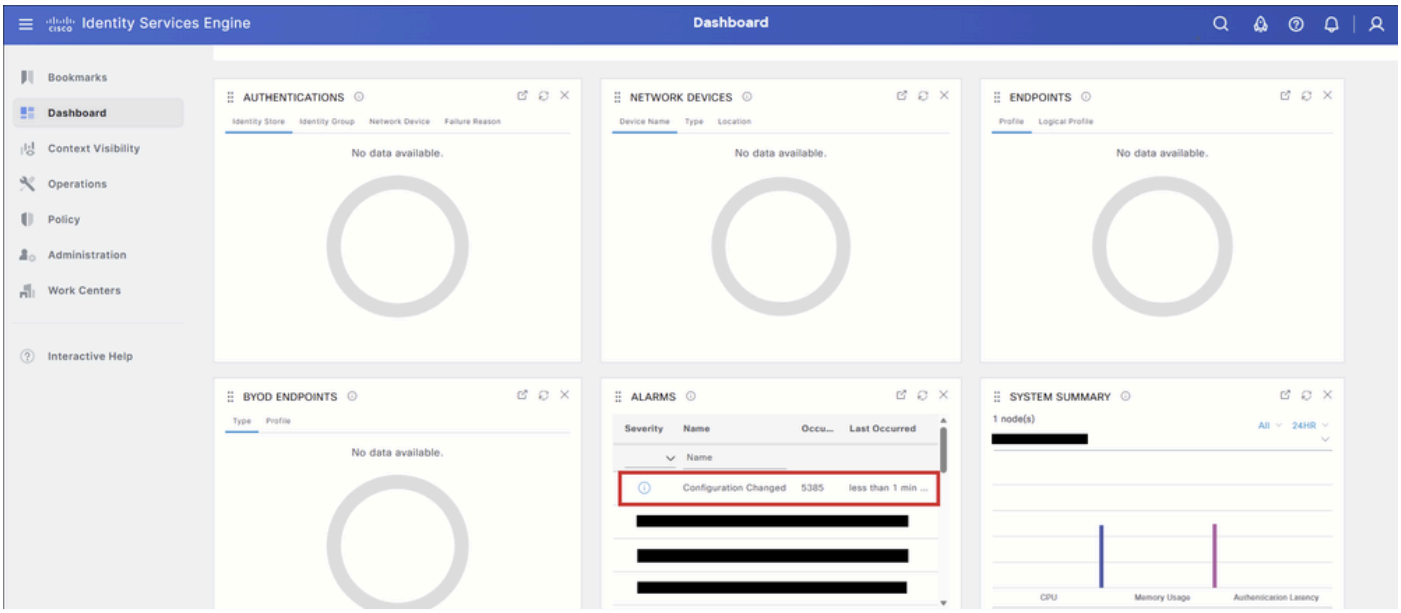
驗證

刪除證書後，可以使用其中一種方法或兩種方法驗證操作是否成功。

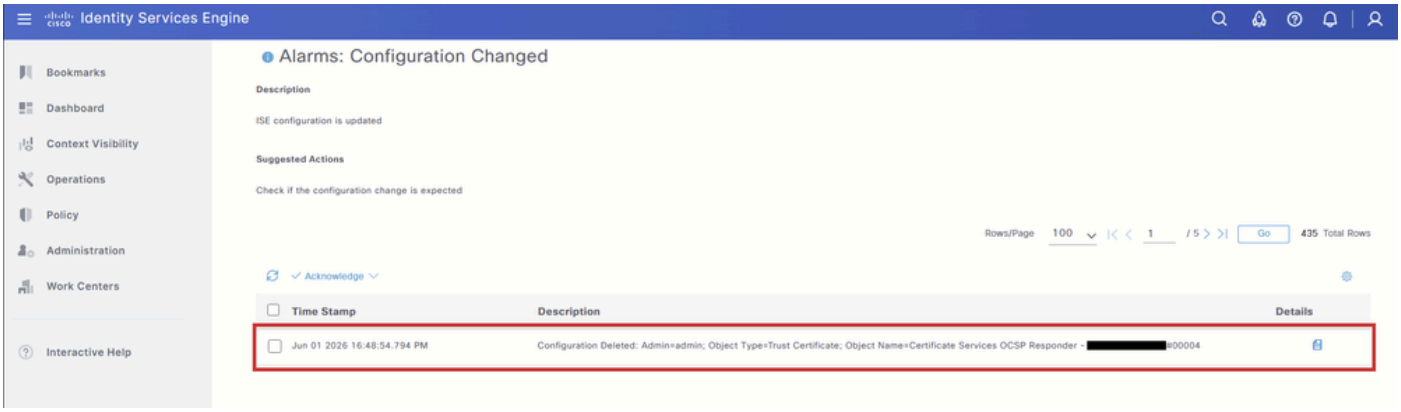
選項1 — 從儀表板警報中驗證

導航到「儀表板」頁。

在Alarms Dashlet中，找到Configuration Changed警報。選擇警報以顯示詳細資訊。



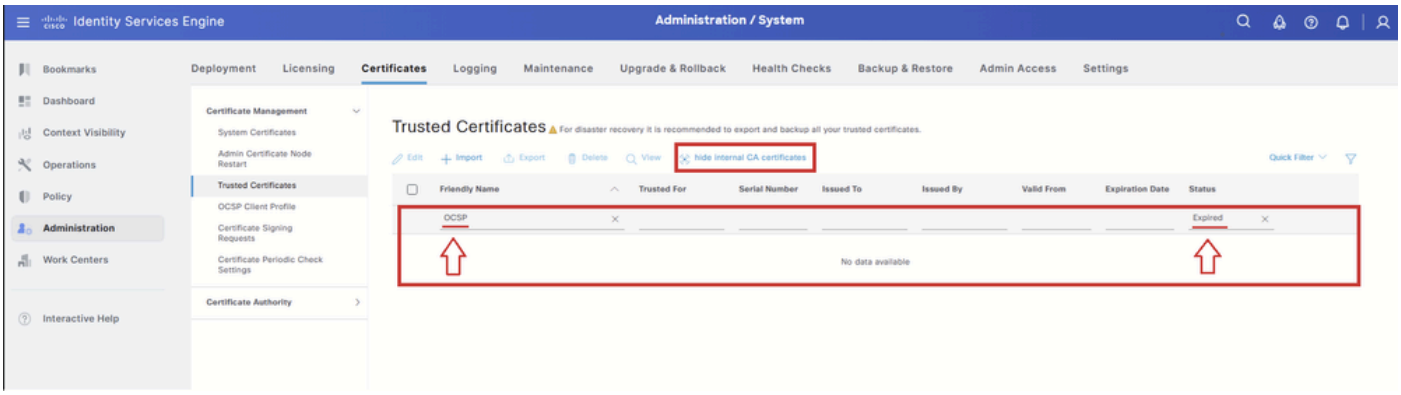
必須出現一個條目，指示配置對象已被刪除。對象名稱必須與已刪除的OCSP響應方證書匹配。



選項2 — 從受信任的證書儲存區進行驗證

作為附加步驟，導航回到Trusted Certificate Store表並過濾OCSP響應方證書。由於證書已被刪除，該表必須顯示「無可用資料」。

附註：請記得選擇show internal CA certificates。


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

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。