

# ISEでの期限切れの内部OCSPレスポнда証明書の削除

## 内容

---

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[バックグラウンド情報](#)

[コンフィギュレーション](#)

[ステップ1: 期限切れのOCSP証明書の確認](#)

[ステップ2: 期限切れのOCSP証明書の検索と削除](#)

[期限切れのOCSPレスポнда証明書に対して選択するオプションはどれか?](#)

[確認](#)

[オプション1: ダッシュボードアラームからの確認](#)

[オプション2- 信頼できる証明書ストアからの確認](#)

---

## はじめに

このドキュメントでは、Cisco Identity Service Engine(ISE)で期限切れOCSPレスポнда証明書または期限切れ間近のOCSPレスポнда証明書を削除する方法について説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- Identity Service Engine(ISE)に関する基礎知識
- 証明書の基礎知識
- オンライン証明書ステータスプロトコル(OCSP)

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Identity Service Engine(ISE)3.x

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## バックグラウンド情報

Cisco Identity Services Engine(ISE)を使用しているお客様が直面する一般的な問題として、証明書の有効期限が切れたことを示すアラームが発生することがあります。特に、OCSPレスポンド証明書書の有効期限が切れるか、間もなく期限切れになり、証明書が見つからない場合です。この状況では、お客様がTACサービスリクエストをオープンしてサポートを受けることがよくあります。このガイドの目的は、有効期限が切れた、または間もなく期限切れになるOCSPレスポンド証明書をカスタマー自身が見つけて削除できるようにすることで、TACケースを作成する必要をなくすことです。

Online Certificate Status Protocol(OCSP)は、x.509デジタル証明書の状態を確認するために使用されるプロトコルです。このプロトコルは、証明書失効リスト(CRL)の代わりとなるもので、CRLの処理を引き起こす問題に対処します。Cisco ISEには、HTTP経由でOCSPサーバと通信し、認証時の証明書のステータスを検証する機能があります。OCSP設定は、Cisco ISEで設定された任意の認証局(CA)証明書から参照できる、再利用可能な設定オブジェクトで設定されます。

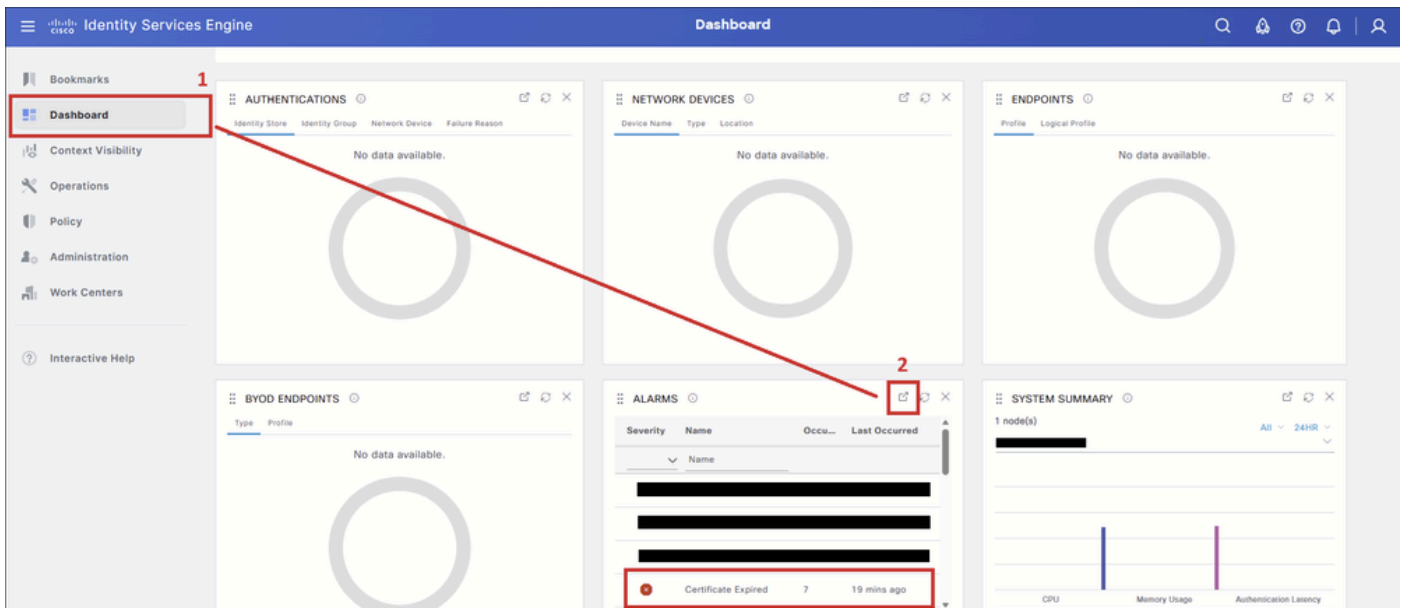
すべてのCisco ISE導入では、OCSP(Online Certificate Status Protocol)レスポンド証明書はデフォルトで内部CA(認証局)インフラストラクチャの一部として存在します。これらの証明書は、PPAN(プライマリポリシー管理ノード)上のCisco ISE内部CAによって発行され、PANおよびすべてのPSN(ポリシーサービスノード)を含む導入環境内の各ノードに対して自動的に生成されます。

期限切れの証明書または期限切れ間近の証明書は、Cisco ISEダッシュボードで証明書期限切れアラームをトリガーする可能性があるため、これらのOCSPレスポンド証明書の管理は重要です。Cisco ISEは新しいOCSPレスポンド証明書を自動的に再生成しますが、期限切れのエントリは手動で削除されるまで信頼された証明書ストアに残ります。

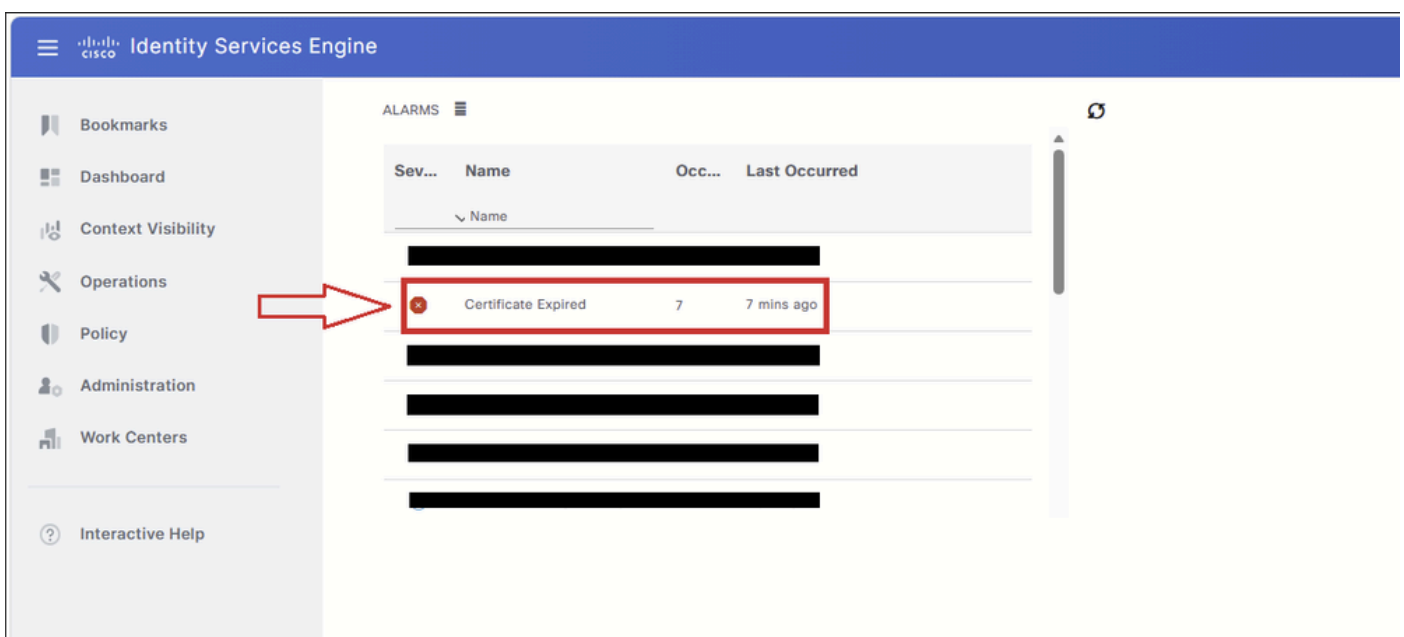
# コンフィギュレーション

## ステップ1：期限切れのOCSP証明書の確認

PPAN(Primary Policy Administration Node) GUIで、ダッシュボードタブ(1)に移動します。Alarmsダッシュレットで、Detachボタン(2)をクリックしてアラームテーブルを展開します。



Certificate Expiredアラームをクリックしてテーブルを展開し、アラームに関連付けられている証明書エントリを表示します。



Certificate Expiredアラームをトリガーしたすべての証明書がこのテーブルに表示されます。このガイドでは、OCSPレスポンド証明書のみを対象としています。EAP、SAML、Admin、その他のシステム証明書など、その他の期限切れ証明書タイプがテーブルに含まれる場合、これらの証明書タイプのガイダンスについては、関連するシスコのドキュメントおよび『Cisco ISE管理者ガイド』を参照してください。

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The main content area is titled "Alarms: Certificate Expired". It includes a description: "This certificate has expired! ISE may fail when attempting to establish secure communications with clients. Inter-node communication may also be affected." Below the description are "Suggested Actions" and a table with the following data:

Time Stamp	Description	Details
May 31 2025 16:30:51.567 PM	Trust certificate 'Certificate Services OCSP Responder - [redacted]' expired on Wed: 5 Feb 2031 : Server: [redacted]	[redacted]

アラームの説明を確認して、有効期限が切れている証明書、または一部のシナリオでは有効期限が間もなく切れる証明書を特定します。

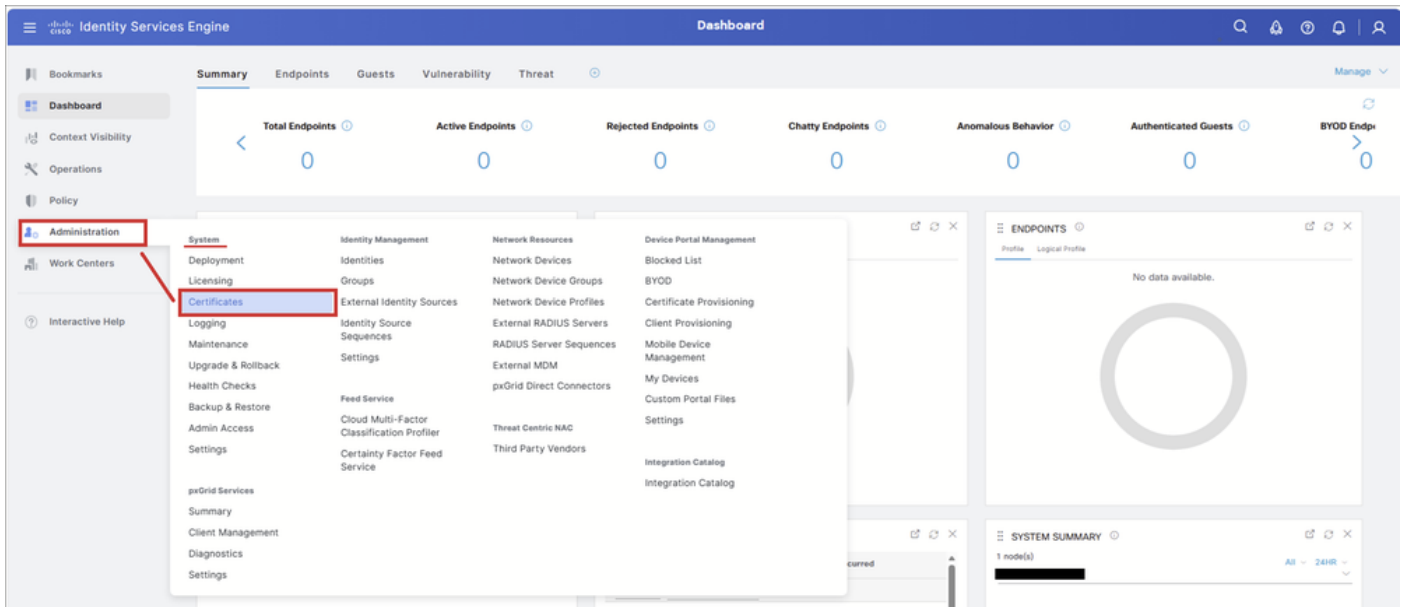
この例では、期限切れの証明書はCertificate Services OCSP Responder - <node-name>#00004です。

証明書名を書き留めます。この名前は、次の手順で信頼できる証明書ストアから証明書を見つけて削除するために使用されます。

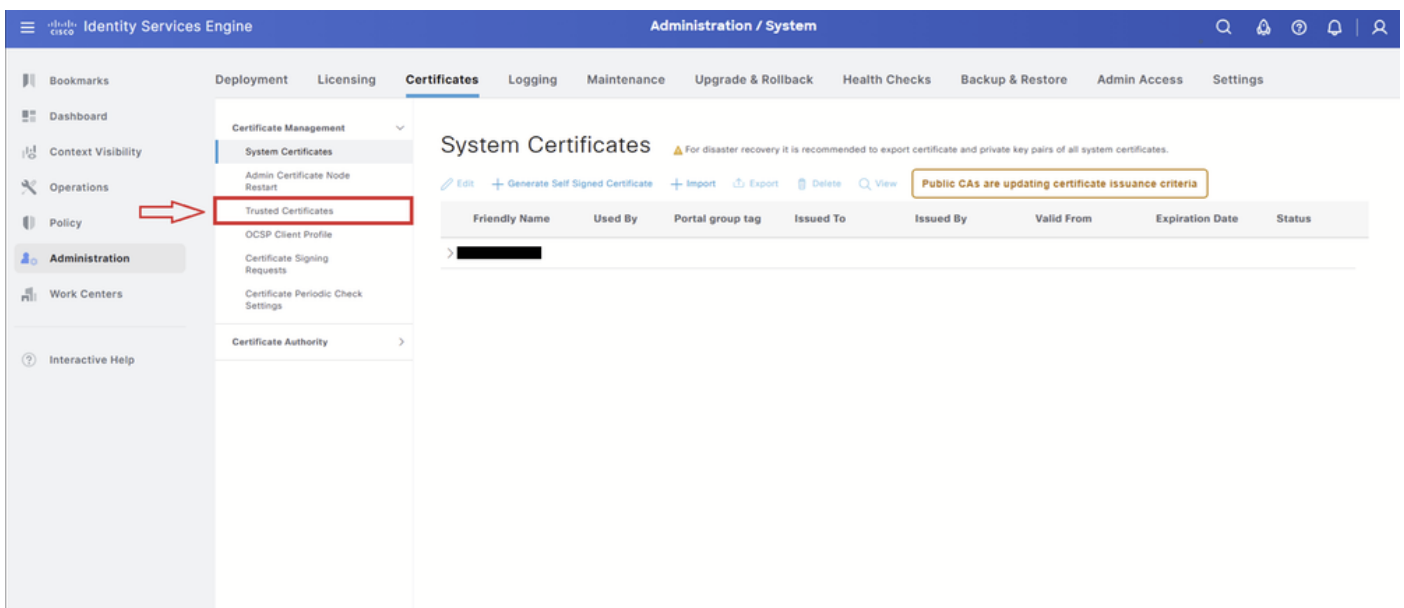
This is a close-up view of the table row from the previous screenshot. A red box highlights the description text: "Trust certificate 'Certificate Services OCSP Responder - [redacted]'#00004' expired on Wed: 5 Feb 2031 : Server: [redacted]".

## ステップ2：期限切れのOCSP証明書の検索と削除

Administration > System > Certificatesの順に選択します。



Trusted Certificatesタブを選択します。



Trusted Certificatesページで、show internal CA certificatesを選択します。これにより、デフォルトで非表示になっているOCSPレスポンス証明書を含む、Cisco ISE内部CA ( 認証局 ) 証明書が表示されます。

選択すると、ボタンが変更され、内部CA証明書が非表示になります。



**警告：**このステップは必須です。「内部CA証明書を表示」を選択しない場合、OCSPレスポンス証明書は「信頼された証明書ストア」テーブルに表示されません。



次の表に、期限切れのOCSPレスポンス証明書を示します。



ヒント：期限切れになるOCSPレスポンス証明書を検索する場合、特に複数のCisco ISEノードを使用する展開では、複数の証明書が表示される可能性があります。正しい証明書を特定するには、OCSPだけでフィルタリングしないでください。その代わりに、ステップ1のアラームの詳細に示された完全な証明書名でフィルタリングします。

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 ▼

<input type="checkbox"/>	Friendly Name	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	Status
<input type="checkbox"/>	OCSP	×						Expired <span>×</span>
<input type="checkbox"/>	Certificate Services OCSP Responder - ricl...	Infrastructure Endpoints	4B D2 96 BE E...	Certificate Service...	Certificate Service...	Wed, 4 Feb 20...	Wed, 5 Feb 20...	<input checked="" type="checkbox"/> Enabled <input checked="" type="checkbox"/> Expired

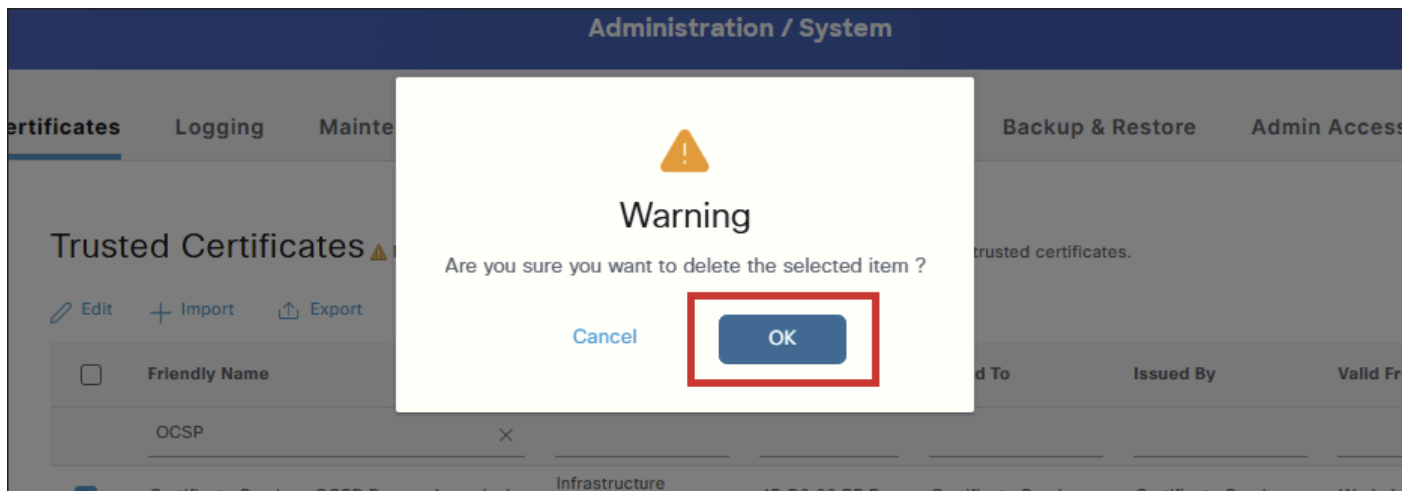
削除する必要があるOCSPレスポンス証明書の横にあるチェックボックスをオンにして、Deleteをクリックします。

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 ▼

<input type="checkbox"/>	Friendly Name	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	Status
<input type="checkbox"/>	OCSP	×						Expired <span>×</span>
<input checked="" type="checkbox"/>	Certificate Services OCSP Responder - ricl...	Infrastructure Endpoints	4B D2 96 BE E...	Certificate Service...	Certificate Service...	Wed, 4 Feb 20...	Wed, 5 Feb 20...	<input checked="" type="checkbox"/> Enabled <input checked="" type="checkbox"/> Expired

確認の警告が表示されたらOKを選択し、証明書の削除を続行します。



証明書を削除する前に、OCSPレスポンド証明書がISE内部CAインフラストラクチャの一部であることを理解することが重要です。

削除中に表示される警告は一般的なもので、すべての内部CA関連の証明書に適用されます。この目的は、内部CA階層内の証明書の削除に注意することです。これらの証明書の一部は、BYOD、pxGrid、またはISE内部CAによって発行された証明書に依存するその他の機能などのサービスに使用されるエンドポイント証明書に署名するためです。

期限切れのOCSPレスポンド証明書も、ISE内部CAによって発行された証明書に影響を与える可能性があります。クライアントまたはサービスがそのCAによって発行された証明書の状態を照会すると、OCSPレスポンド証明書の有効期限が切れているために証明書の状態の検証が失敗するため、OCSPサービスからエラーが返されます。

Deleteを選択すると、次の2つのオプションが表示されます。

- 証明書の削除：このオプションは、信頼できる証明書ストアからCisco ISE内部CA証明書を削除します。内部CA証明書が削除されると、そのCAによって署名されたすべてのエンドポイント証明書が無効になり、影響を受けるエンドポイントはネットワークにアクセスできなくなります。この操作は元に戻すことができます。つまり、同じ内部CA証明書を信頼できる証明書ストアにインポートし直すことで、ネットワークアクセスを復元できます。
- Delete & Revoke certificate：このオプションは、Cisco ISE内部CA証明書を削除および失効させます。削除オプションと同様に、内部CAによって署名されたすべてのエンドポイント証明書は無効になり、影響を受けるエンドポイントはネットワークアクセスを失います。ただし、この操作は元に戻せません。失効後、機能を復元するために、Cisco ISEルート証明書チェーン全体を置き換える必要があります。

期限切れのOCSPレスポンド証明書に対して選択するオプションはどれか？

この影響は、エンドポイント証明書にアクティブに署名する内部CA証明書に適用されます。OCSPレスポンド証明書はエンドポイント証明書に署名せず、OCSP通信に使用されます。期限切れのOCSPレスポンド証明書により、内部CAによって発行された証明書の証明書状態の検証が失敗する可能性があります。証明書はすでに期限切れになっているため、有効なOCSP応答を提供していません。削除しても何の影響もありません。

このシナリオのOCSPレスポンド証明書は既に期限切れになっているため、有効ではありません。この場合、取り消す有効な残りがいないため、削除と削除および取り消しの両方で同じ結果が生成されます。

これらの理由から、より簡単なアクションであり、不要な失効エントリの生成を回避するため、削除が推奨されるオプションです。



注:OCSPレスポンド証明書は、通常の動作中には再生成されません。パッチがインストールされている場合にのみ再生成されます。

- マルチノード展開では、パッチがGUIを介してインストールされるときに証明書が再生成されます。
- スタンドアロン展開では、GUIまたはCLIを使用してパッチをインストールするときに証明書が再生成されます。

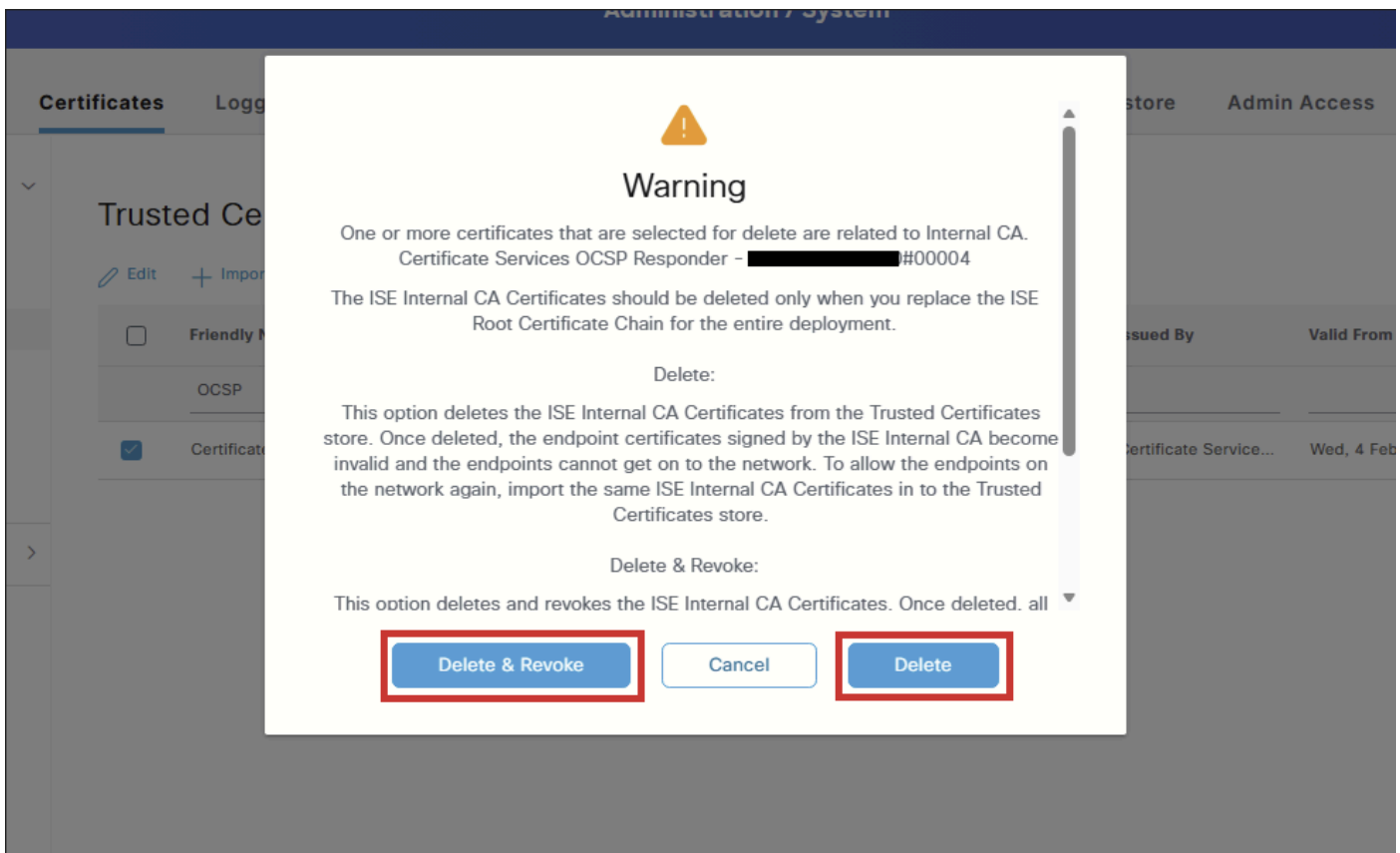
新しいOCSPレスポンド証明書は、次のパッチインストール時にのみ生成されます。



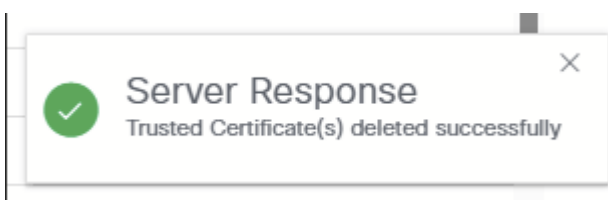
注意：影響を受けるノードの信頼できる証明書ストアに、アクティブで有効なOCSPレスポンド証明書があることを確認してください。有効な証明書が存在せず、ISE内部CAによって署名された証明書の検証にOCSPが使用される場合、新しいOCSPレスポンド証明書が生成されるまでその検証は失敗します。

有効なOCSPレスポンド証明書が存在しない場合は、次の説明に従ってPPAN (プライマリポリシー管理ノード) からOCSPレスポンド証明書を更新します。

1. ISE PPAN GUIにアクセスします。
2. Administration > System > Certificatesの順に選択します。
3. 左側でCertificate Signing Requestsを選択します。
4. 「CSRの生成」をクリックします。使用法については、ISE OCSPレスポンドの更新を選択します。
5. ISE OCSPレスポンド証明書の更新をクリックしてプロセスを完了します。



証明書が削除されると、信頼できる証明書が正常に削除されたことを示すサーバ応答通知が表示されます。



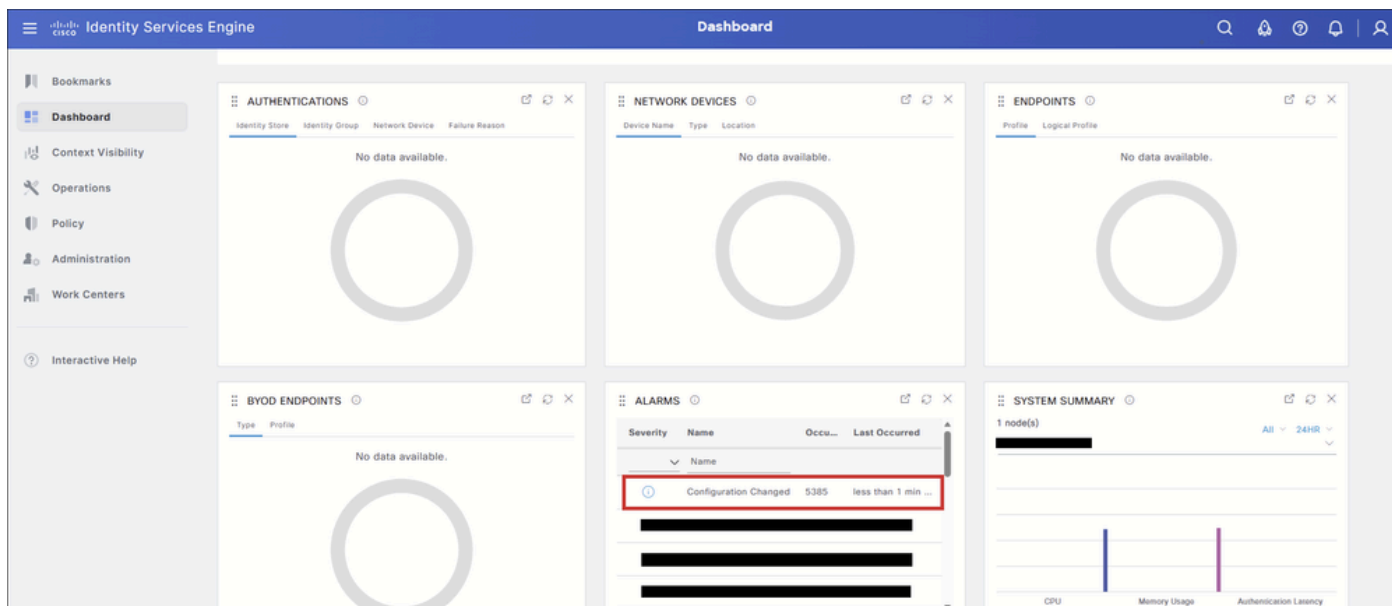
## 確認

証明書を削除した後、次のいずれか、または両方の方法を使用して、操作が正常に行われたことを確認できます。

オプション1：ダッシュボードアラームからの確認

「ダッシュボード」ページにナビゲートします。

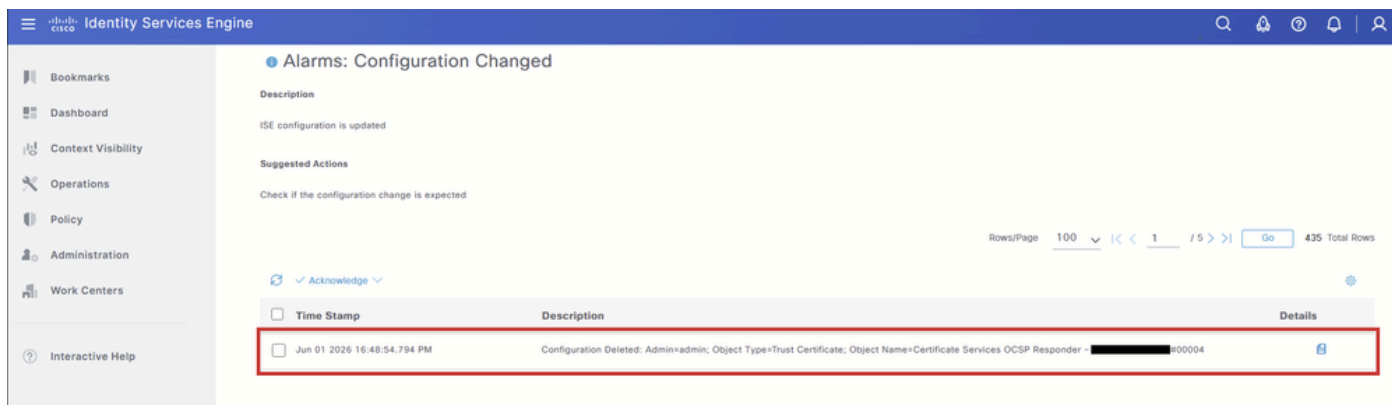
Alarmsダッシュレットで、Configuration Changedアラームを見つけます。詳細を表示するアラームを選択します。



The screenshot shows the Identity Services Engine Dashboard. The Alarms section is active, displaying a table with the following data:

Severity	Name	Occu...	Last Occurred
5385	Configuration Changed	5385	less than 1 min ...

設定オブジェクトが削除されたことを示すエントリが表示される必要があります。オブジェクト名は、削除されたOCSPレスポンド証明書と一致する必要があります。



The screenshot shows the detail page for the 'Alarms: Configuration Changed' event. The table below displays the configuration deletion event:

Time Stamp	Description	Details
Jun 01 2026 16:48:54.794 PM	Configuration Deleted: Admin=admin; Object Type=Trust Certificate; Object Name=Certificate Services OCSP Responder - [redacted]	00004

## オプション2 – 信頼できる証明書ストアからの確認

追加の手順として、信頼できる証明書ストアの表に戻り、OCSPレスポンド証明書をフィルタリングします。証明書が削除されているため、テーブルには「使用可能なデータがありません」と表示されている必要があります。



注:show internal CA certificatesを選択することを忘れないでください。

The screenshot displays the Cisco Identity Services Engine Administration / System interface. The main content area is titled "Trusted Certificates" and includes a warning: "For disaster recovery it is recommended to export and backup all your trusted certificates." Below this, there are action buttons: "Edit", "+ Import", "Export", "Delete", "View", and "hide internal CA certificates" (which is checked and highlighted with a red box). A table lists the trusted certificates with columns: Friendly Name, Trusted For, Serial Number, Issued To, Issued By, Valid From, Expiration Date, and Status. A single entry is shown with "OCSP" in the Friendly Name column and "Expired" in the Status column, both highlighted with red boxes and red arrows pointing to them. Below the table, the text "No data available" is displayed.

Friendly Name	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	Status
OCSP	X						Expired X

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。