Remover Certificados de Respondente OCSP Interno Expirados no ISE

Contents

Introdução

Este documento descreve como excluir certificados de respondente OCSP expirados e/ou prestes a expirar no Cisco Identity Service Engine (ISE).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento básico do Identity Service Engine (ISE).
- Conhecimento básico de certificados.
- Protocolo de Status de Certificados Online (OCSP)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Identity Service Engine 3.x

As informações neste documento foram criadas a partir dos dispositivos em um ambiente de laboratório específico.Todos os dispositivos usados neste documento começaram com uma configuração limpa (padrão). Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Um problema comum enfrentado pelos clientes que usam o Cisco Identity Services Engine (ISE) é receber alarmes indicando que um certificado expirou, especificamente quando o certificado do respondente OCSP expirou ou está prestes a expirar e o certificado não pode ser encontrado. Essa situação geralmente leva os clientes a abrir casos de TAC para assistência. O objetivo deste guia é capacitar os clientes a localizar e excluir eles mesmos esses certificados de respondente OCSP expirados ou prestes a expirar, evitando assim a necessidade de levantar um caso de TAC.

O OCSP (Online Certificate Status Protocol) é um protocolo usado para verificar o status de certificados digitais x.509. Esse protocolo é uma alternativa para a Lista de Certificados Revogados (CRL) e trata de problemas que resultam no tratamento de CRLs. O Cisco ISE tem a capacidade de se comunicar com servidores OCSP por HTTP para validar o status de certificados em autenticações. A configuração do OCSP é configurada em um objeto de configuração reutilizável que pode ser referenciado de qualquer certificado de autoridade de certificação (CA) configurado no Cisco ISE.

Em cada implantação do Cisco ISE, os certificados do Respondente OCSP (Online Certificate Status Protocol) estão presentes por padrão como parte da infraestrutura interna da CA (Certificate Authority). Esses certificados são emitidos pela CA interna do Cisco ISE no PPAN (Primary Policy Administration Node) e são gerados automaticamente para cada nó na implantação, incluindo o PAN e todos os PSNs (Policy Service Nodes).

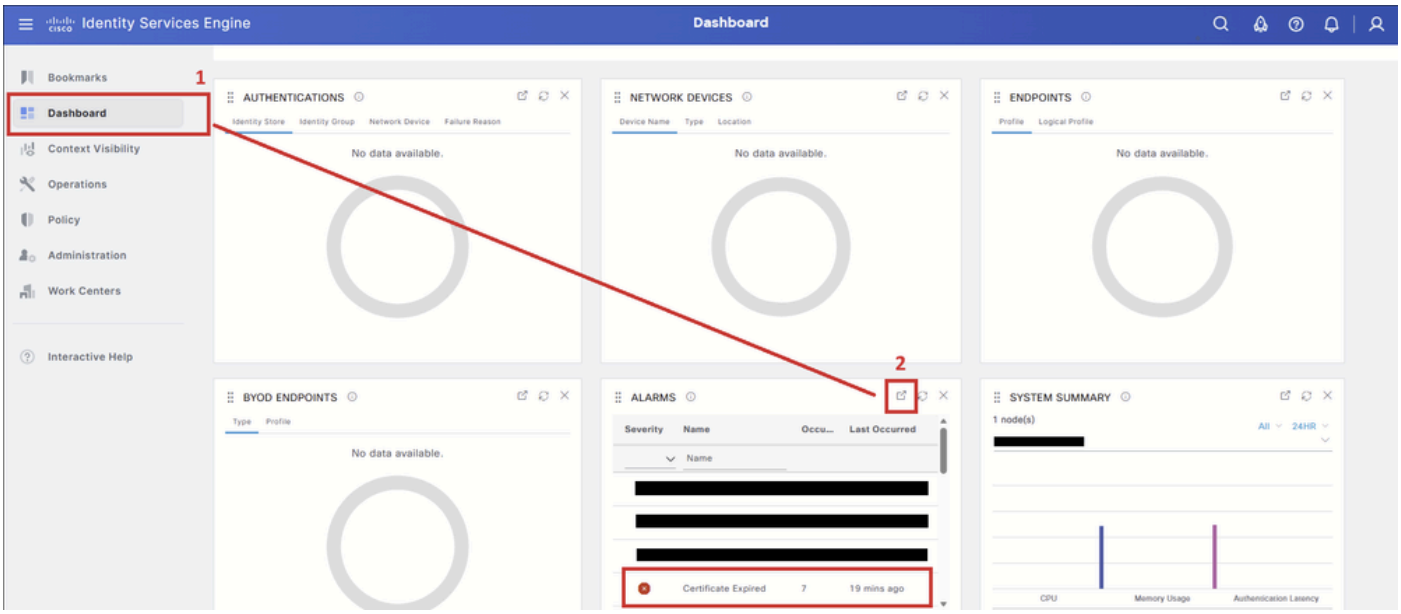
Gerenciar esses certificados de Respondente OCSP é importante porque certificados expirados ou prestes a expirar podem disparar alarmes de Certificado expirado no painel do Cisco ISE.

Embora o Cisco ISE gere automaticamente novos certificados de Respondente OCSP, as entradas expiradas permanecem no Repositório de Certificados Confiáveis até que sejam removidas manualmente.

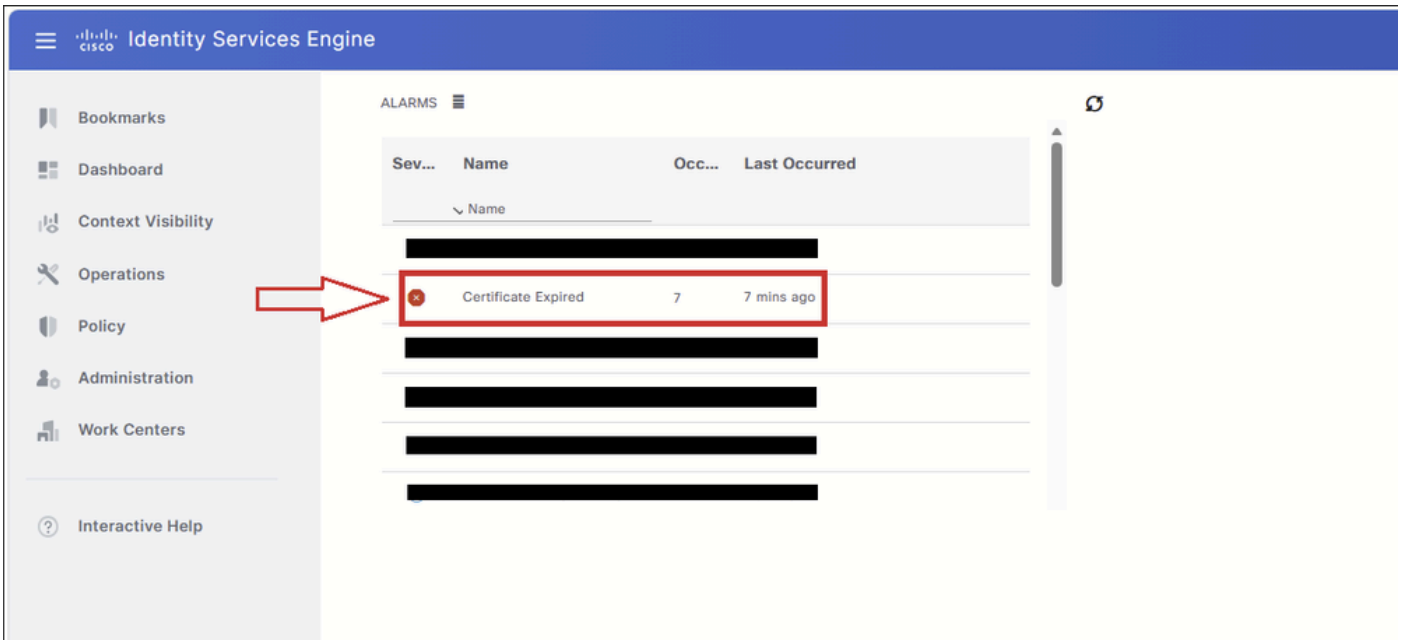
Configuração

Etapa 1 - Verificar o certificado OCSP expirado

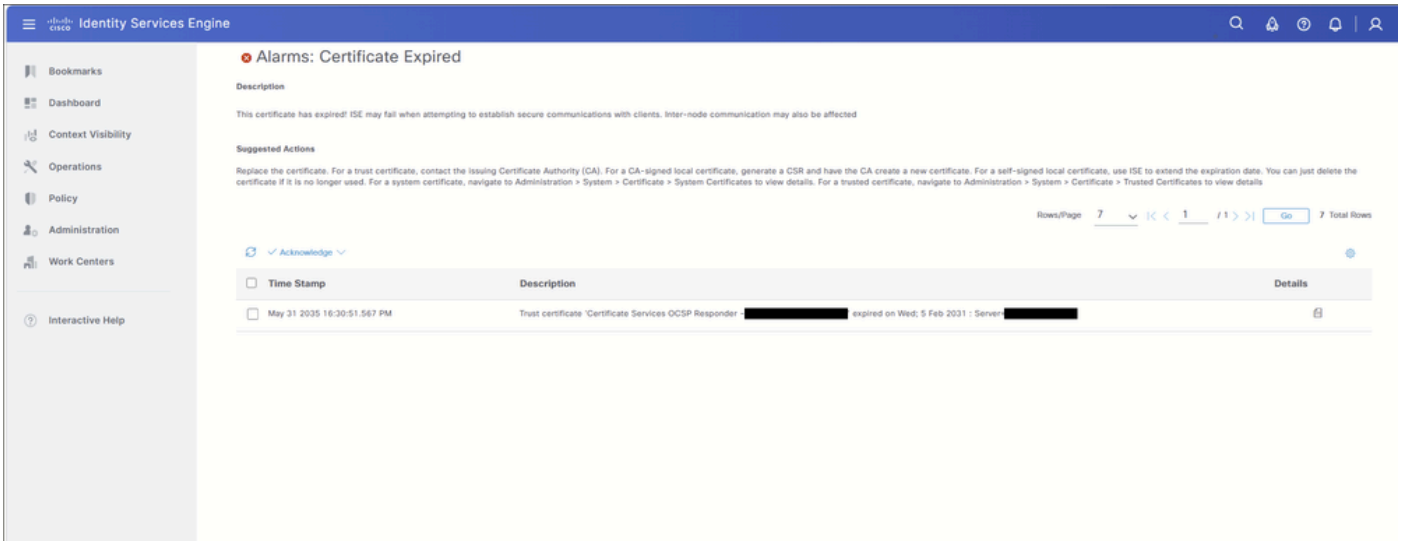
Na GUI do PPAN (Primary Policy Administration Node), navegue até a guia Dashboard (1). No dashlet Alarms, clique no botão Detach (2) para expandir a tabela de alarmes.



Clique no alarme Certificado Expirado para expandir a tabela e exibir as entradas de certificado associadas ao alarme.



Todos os certificados que dispararam o alarme Certificado Expirado são exibidos nesta tabela. Este guia se concentra apenas nos certificados do Respondente OCSP. Se a tabela incluir outros tipos de certificados expirados, como EAP, SAML, Admin ou outros certificados do sistema, consulte a documentação relevante da Cisco e o Guia do Administrador do Cisco ISE para obter orientação sobre esses tipos de certificados.



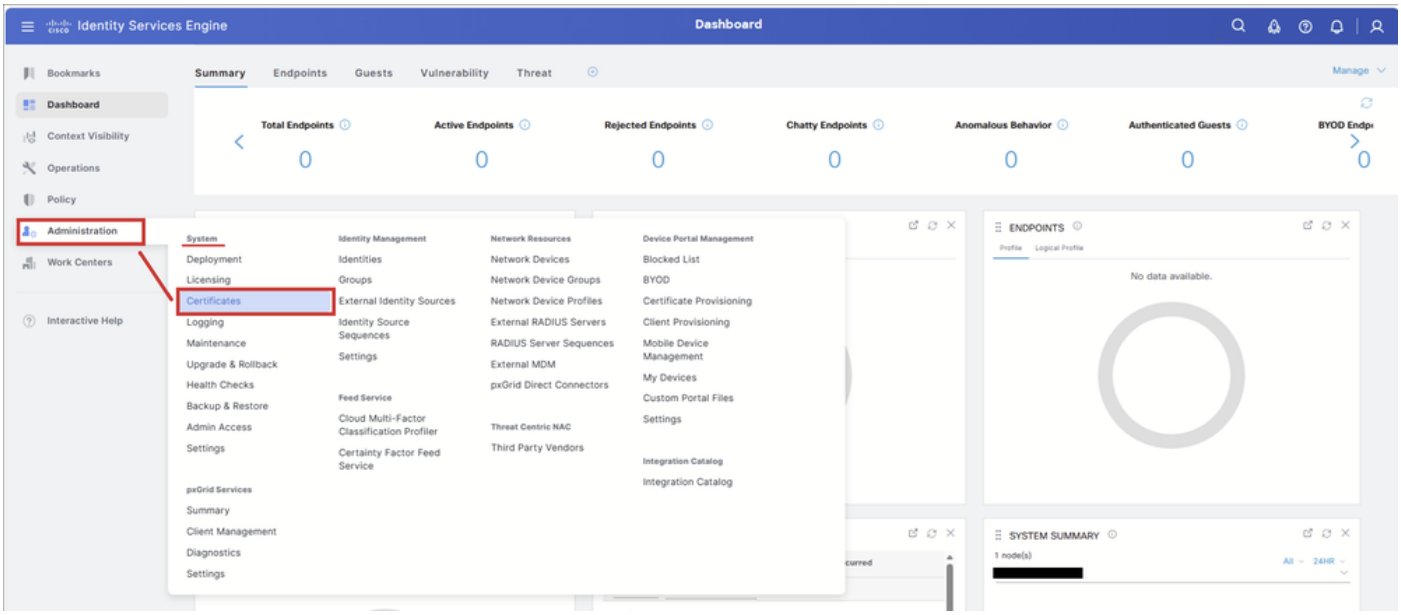
Revise a descrição do alarme para identificar o certificado que está expirado ou, em alguns cenários, prestes a expirar.

Neste exemplo, o certificado expirado é: Certificate Services OCSP Responder - <node-name>#0004.

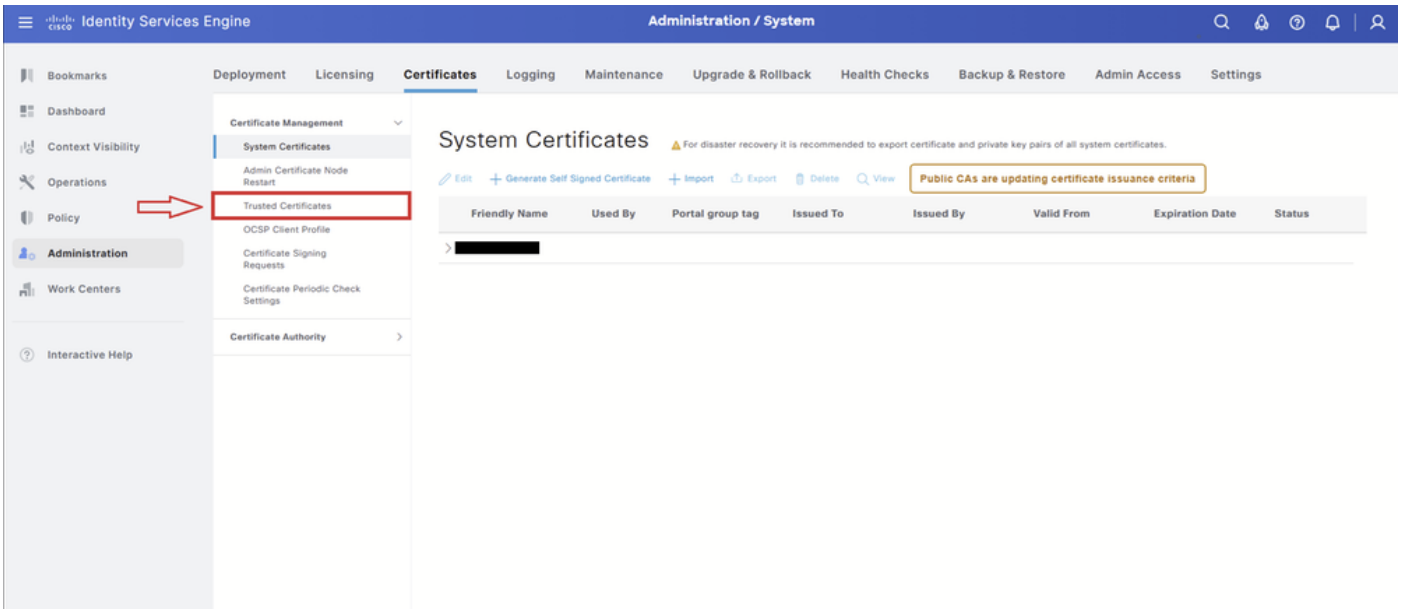
Anote o nome do certificado. Este nome é usado nas próximas etapas para localizar e excluir o certificado do Repositório de Certificados Confiáveis.

Etapa 2 - Localizar e excluir o certificado OCSP expirado

Navegue até: Administração > Sistema > Certificados:



Selecione a guia Certificados de Confiabilidade.

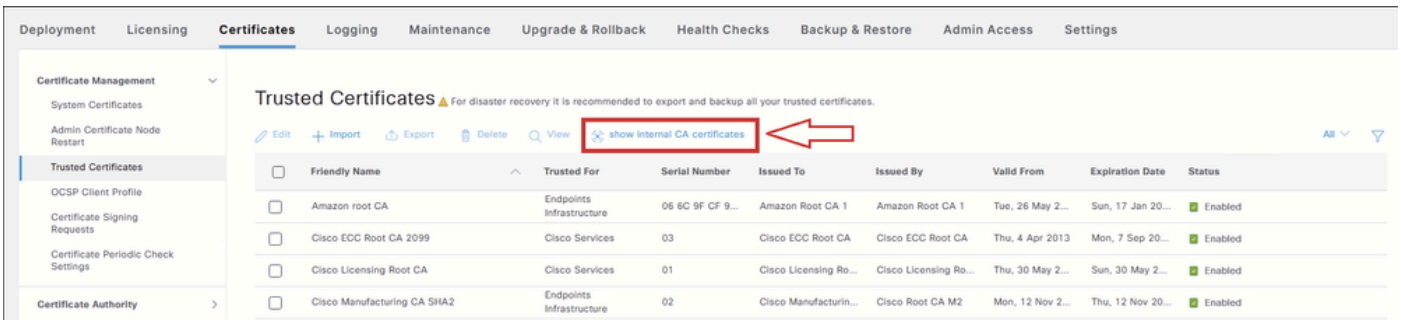


Na página Certificados de Confiabilidade, selecione show internal CA certificates. Exibe os certificados da CA interna (Autoridade de certificação) do Cisco ISE, incluindo os certificados do Respondente OCSP que estão ocultos por padrão.

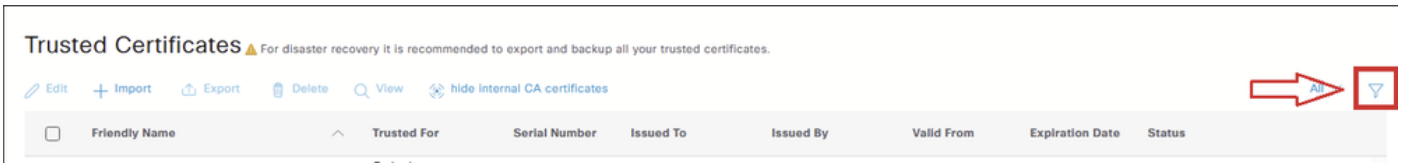
Depois de selecionado, o botão é alterado para ocultar os certificados internos da CA.

---

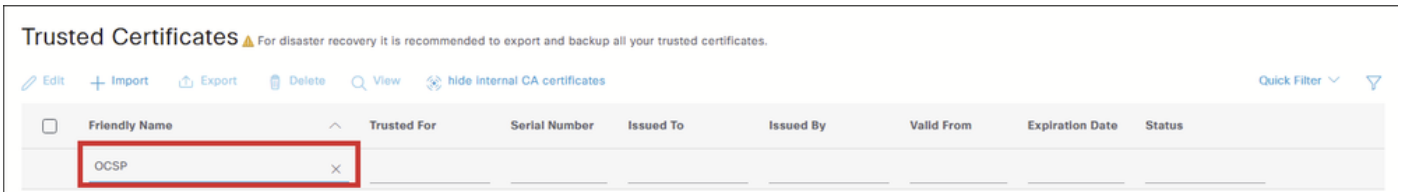
aviso: Esta etapa é obrigatória. Se mostrar certificados internos da autoridade de certificação não estiver selecionado, o certificado do Respondente OCSP não aparecerá na tabela Repositório de Certificados Confiáveis.



Na tabela Repositório de Certificados Confiáveis, selecione o ícone Filtro para procurar o certificado que deve ser excluído.

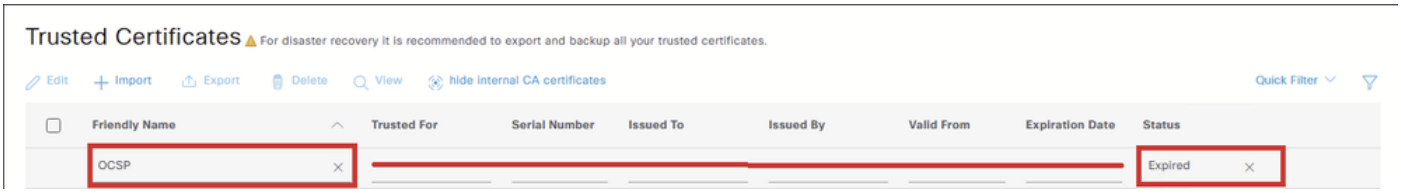


Se o certificado do Respondente OCSP estiver prestes a expirar, filtre somente por OCSP em Nome Amigável. Se o certificado do Respondente OCSP já tiver expirado, continue com a próxima ação.



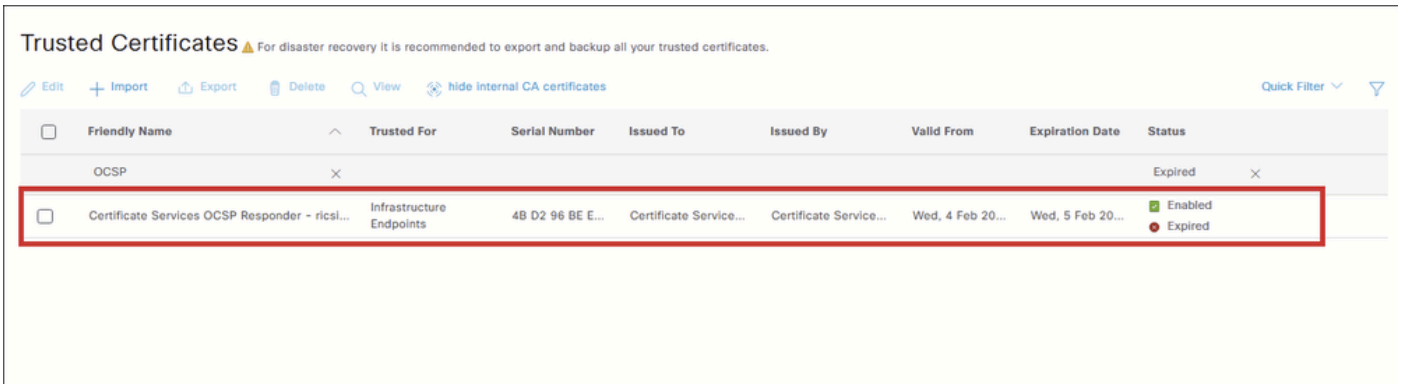
Para localizar um certificado de Respondente OCSP expirado, insira estes filtros:

- Nome amigável: OCSP
- Status: Expirado

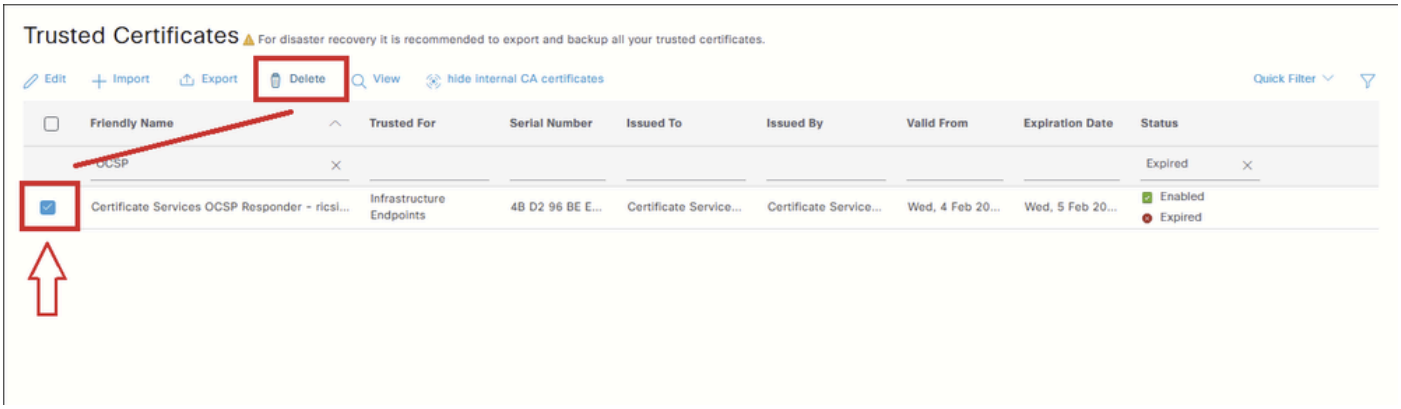


A tabela exibe os certificados do Respondente OCSP expirados.

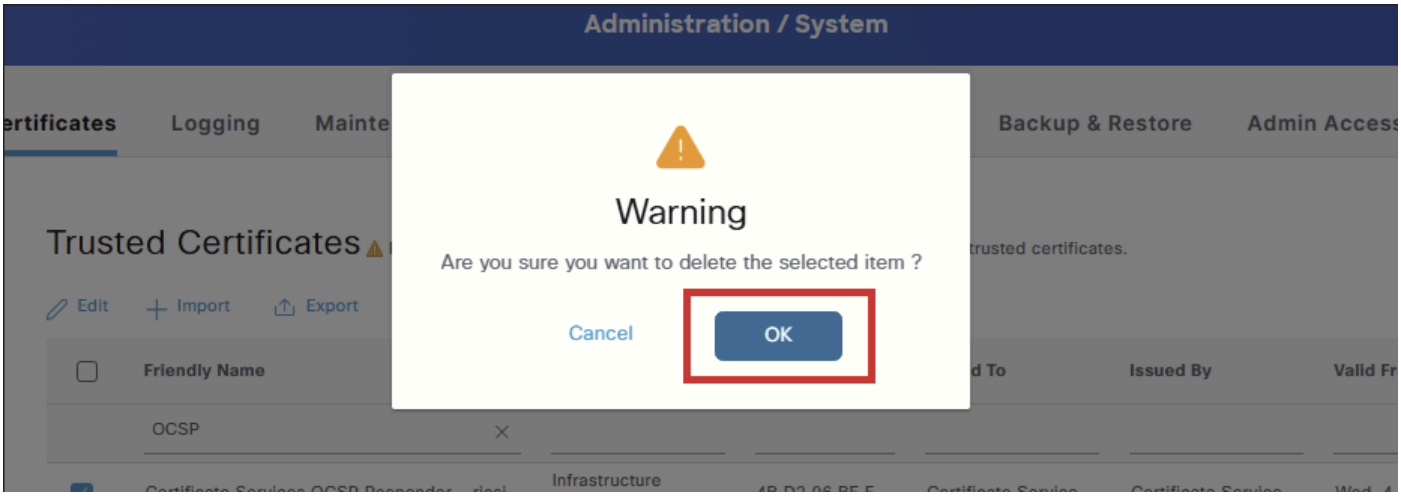
Tip: Se você estiver procurando um certificado de Respondente OCSP que está prestes a expirar, vários certificados poderão ser exibidos, especialmente em implantações com vários nós do Cisco ISE. Para identificar o certificado correto, não filtre somente pelo OCSP. Em vez disso, filtre pelo nome completo do certificado mostrado nos detalhes do alarme na Etapa 1.



Marque a caixa de seleção ao lado do certificado do Respondente OCSP que deve ser removido e clique em Excluir.



Selecione OK no aviso de confirmação para continuar a excluir o certificado.



Antes de excluir o certificado, é importante entender que o certificado do Respondente OCSP faz parte da infraestrutura interna de CA do ISE.

O aviso que aparece durante a exclusão é genérico e se aplica a todos os certificados internos relacionados a CA. Seu objetivo é prevenir contra a exclusão de certificados dentro da hierarquia de CA interna, já que alguns desses certificados assinam certificados de ponto de extremidade usados para serviços como BYOD, pxGrid ou outras funções que dependem de certificados emitidos pela CA interna do ISE.

Um certificado de Respondente OCSP expirado também pode afetar certificados emitidos pela CA interna do ISE. Quando um cliente ou serviço consulta o status de um certificado emitido por essa CA, o serviço OCSP retorna um erro porque o certificado do Respondente OCSP expirou, o que pode causar falha na validação do status do certificado.

Quando você seleciona Excluir, duas opções são apresentadas:

- Excluir certificado: Esta opção exclui o certificado de CA interno do Cisco ISE do armazenamento de certificados confiáveis. Quando o certificado interno da autoridade de certificação é excluído, todos os certificados de ponto de extremidade assinados por essa autoridade de certificação se tornam inválidos e os pontos de extremidade afetados não podem acessar a rede. Esta ação é reversível: você pode restaurar o acesso à rede importando o mesmo certificado interno CA de volta para o armazenamento Certificados de Confiabilidade.
- Excluir e revogar certificado: Essa opção exclui e revoga o certificado de CA interno do Cisco ISE. Como ocorre com a opção Excluir, todos os certificados de ponto de extremidade assinados pela CA interna se tornam inválidos e os pontos de extremidade afetados perdem o acesso à rede. No entanto, esta operação é irreversível. Após a revogação, você deve substituir toda a cadeia de certificados raiz do Cisco ISE para que a implantação restaure a funcionalidade.

Qual opção selecionar para um certificado de respondente OCSP expirado?

O impacto descrito aplica-se a certificados internos de CA que assinam ativamente certificados de ponto de extremidade. O certificado do Respondente OCSP não assina certificados de ponto de extremidade; ele é usado para comunicação OCSP. Embora um certificado do Respondente OCSP expirado possa causar falha na validação do status do certificado para certificados emitidos pela CA interna, o certificado já expirou e, portanto, não está mais fornecendo respostas OCSP válidas. Excluí-lo não traz nenhum impacto adicional.

Como o certificado do Respondente OCSP nesse cenário já expirou, ele não é mais válido. Nesse caso, Excluir e Excluir e Revogar produzem o mesmo resultado, já que não há mais nada válido a ser revogado.

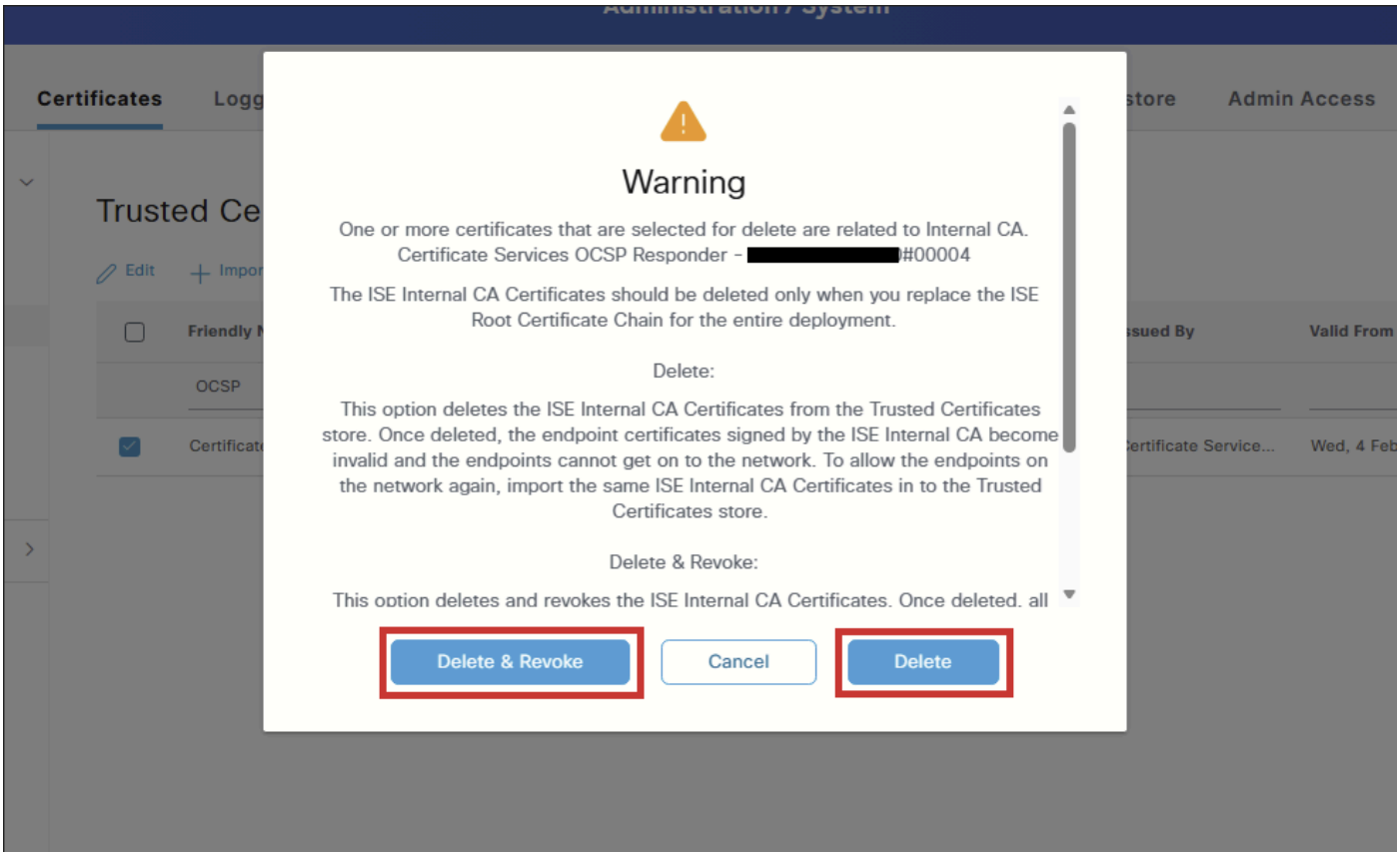
Por esses motivos, Excluir é a opção recomendada, pois é a ação mais simples e evita gerar uma entrada de revogação desnecessária.

Note: Os certificados do Respondente OCSP não são regenerados durante a operação normal. Eles são regenerados apenas quando um patch é instalado:
- Em uma implantação de vários nós, os certificados são gerados novamente quando o patch é instalado por meio da GUI.
- Em uma implantação autônoma, os certificados são regenerados quando o patch é instalado por meio da GUI ou da CLI.

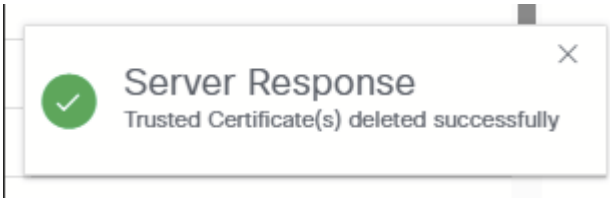
Um novo certificado de Respondente OCSP é gerado somente na próxima instalação de patch.

Caution: Verifique se o nó afetado tem um certificado de Respondente OCSP válido e ativo no Repositório de Certificados Confiáveis. Se um certificado válido não estiver presente e o OCSP for usado para validar certificados assinados pela CA interna do ISE, essa validação falhará até que um novo certificado do Respondente OCSP seja gerado.

Se um certificado válido do Respondente OCSP não estiver presente, renove os certificados do Respondente OCSP no PPAN (Nó de Administração de Política Primária) conforme descrito aqui:
1. Acesse a GUI do ISE PPAN.
2. Vá para Administração > Sistema > Certificados.
3. Selecione Certificate Signing Requests (Solicitações de assinatura de certificado) à esquerda.
4. Clique em Gerar CSR. Para Uso, selecione Renew ISE OCSP Responder.
5. Clique em Renovar Certificados de Respondente OCSP do ISE para concluir o processo.



Depois que o certificado for excluído, uma notificação de Resposta do servidor será exibida indicando que o certificado confiável foi excluído com êxito:



Verificar

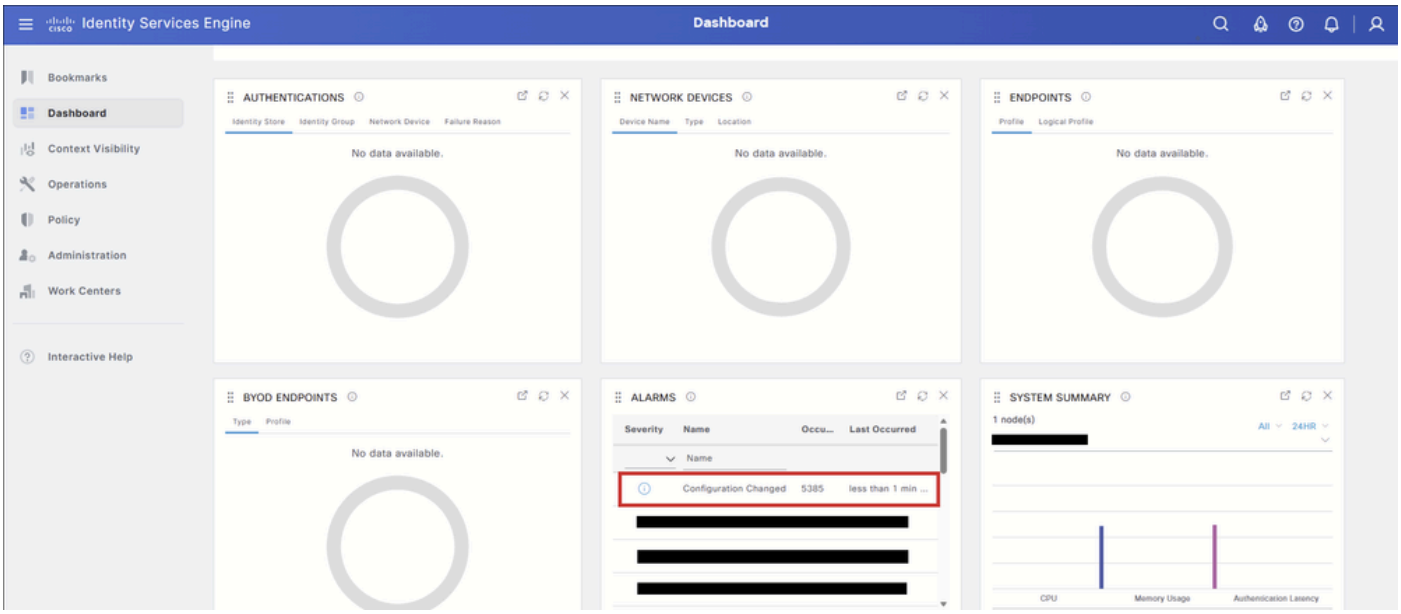
Depois que o certificado for excluído, você poderá usar um ou ambos os métodos para verificar se a operação foi bem-sucedida.

Opção 1 - Verificar a partir dos alarmes do painel

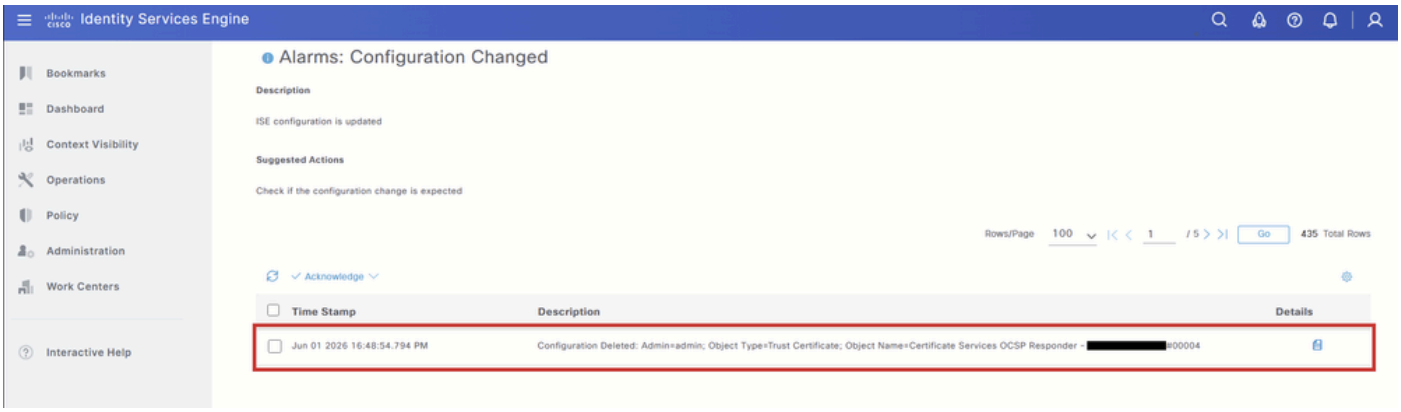
Navegue até a página Painel.

No dashlet Alarms, localize o alarme Configuration Changed. Selecione o alarme para exibir os

detalhes. @ info: whatsthis



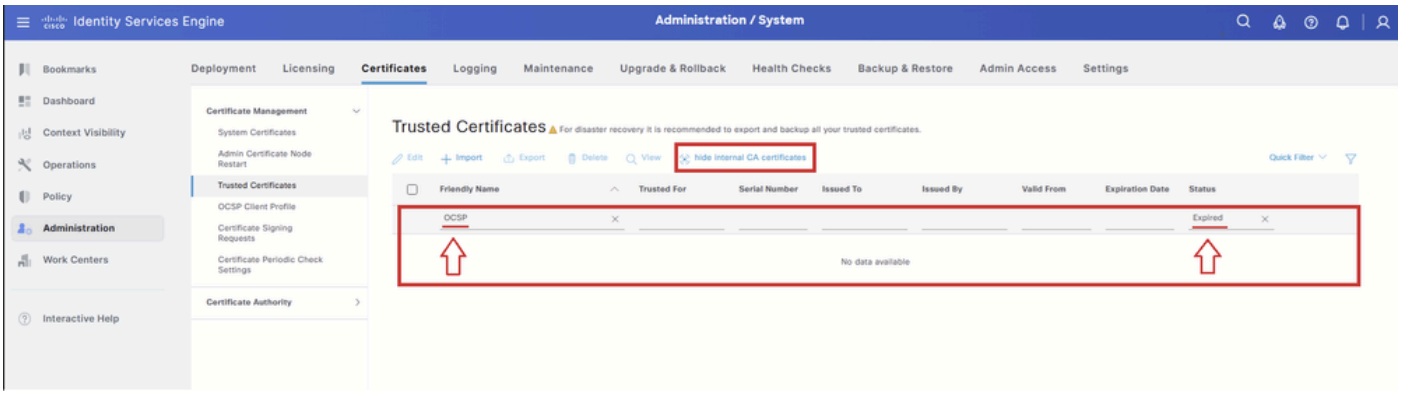
Deve aparecer uma entrada indicando que um objeto de configuração foi excluído. O nome do objeto deve corresponder ao certificado do Respondente OCSP que foi removido.



Opção 2 - Verificar a partir do Repositório de Certificados Confiáveis

Como etapa adicional, navegue de volta para a tabela Repositório de Certificados Confiáveis e filtre o certificado do Respondente OCSP. Como o certificado foi excluído, a tabela deve exibir Nenhum dado disponível.

Note: Lembre-se de selecionar 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

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.