Eliminar certificados de respondedor OCSP interno caducado en ISE

Contenido

Introducción

Este documento describe cómo eliminar los certificados de Respondedor OCSP caducados o a punto de caducar en Cisco Identity Service Engine (ISE).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimientos básicos de Identity Service Engine (ISE).
- Conocimiento básico de Certificados.
- Online Certificate Status Protocol (OCSP)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Identity Service Engine 3.x

La información de este documento se creó a partir de los dispositivos en un entorno de laboratorio específico.Todos los dispositivos utilizados en este documento se iniciaron con una configuración (predeterminada) desactivada. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Un problema habitual al que se enfrentan los clientes que utilizan Cisco Identity Services Engine (ISE) es la recepción de alarmas que indican que un certificado ha caducado, concretamente cuando el certificado del respondedor de OCSP ha caducado o está a punto de hacerlo y no se puede encontrar el certificado. Esta situación a menudo lleva a los clientes a abrir casos de TAC para obtener asistencia. El objetivo de esta guía es permitir a los clientes localizar y eliminar ellos mismos estos certificados de respuesta de OCSP caducados o que van a caducar próximamente, con lo que se evita la necesidad de plantear un caso de TAC.

El Protocolo de estado de certificados en línea (OCSP) es un protocolo que se utiliza para comprobar el estado de los certificados digitales x.509. Este protocolo es una alternativa a la Lista de revocación de certificados (CRL) y aborda los problemas que dan lugar a la gestión de CRL. Cisco ISE tiene la capacidad de comunicarse con los servidores OCSP a través de HTTP para validar el estado de los certificados en las autenticaciones. La configuración de OCSP se configura en un objeto de configuración reutilizable al que se puede hacer referencia desde cualquier certificado de autoridad de certificación (CA) configurado en Cisco ISE.

En cada implementación de Cisco ISE, los certificados de Respondedor OCSP (Online Certificate Status Protocol) están presentes de forma predeterminada como parte de la infraestructura interna de CA (Certificate Authority). Estos certificados los emite la CA interna de Cisco ISE en el PPAN (nodo de administración de políticas principal) y se generan automáticamente para cada nodo de la implementación, incluidos el PAN y todos los PSN (nodos de servicios de políticas).

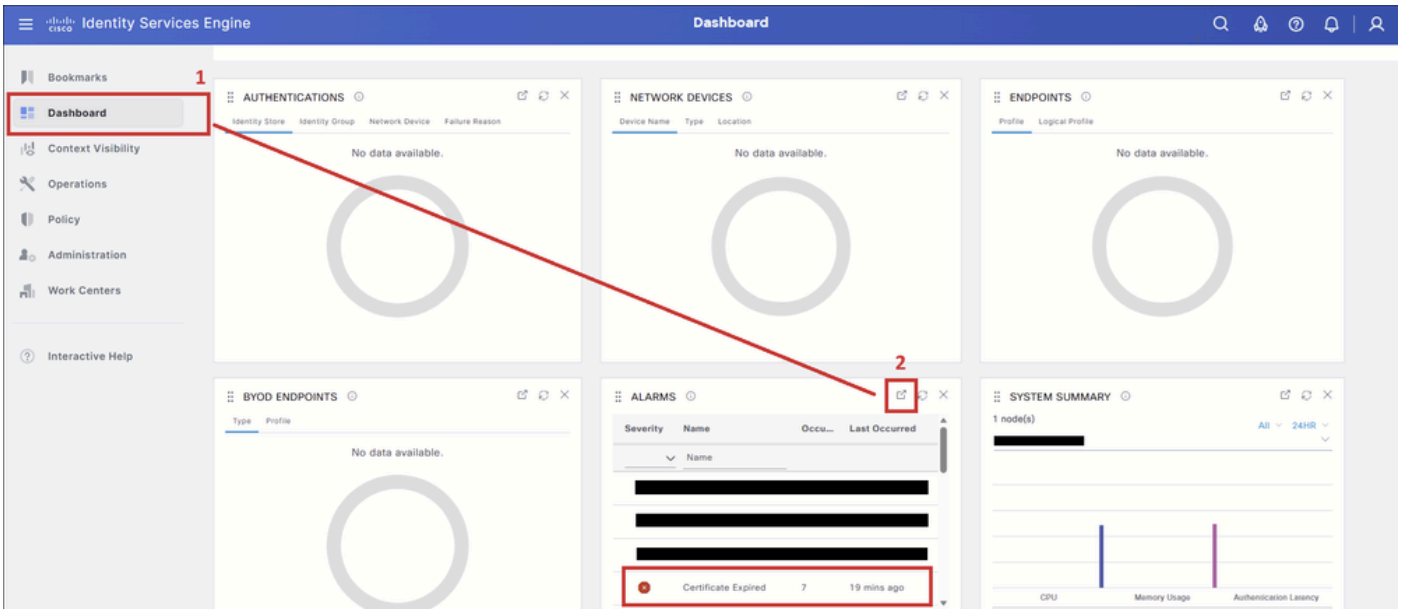
La administración de estos certificados de Respondedor de OCSP es importante porque los

certificados caducados o a punto de caducar pueden activar alarmas de certificados caducados en el panel de Cisco ISE. Aunque Cisco ISE regenera automáticamente nuevos certificados de Respondedor de OCSP, las entradas caducadas permanecen en el almacén de certificados de confianza hasta que se quitan manualmente.

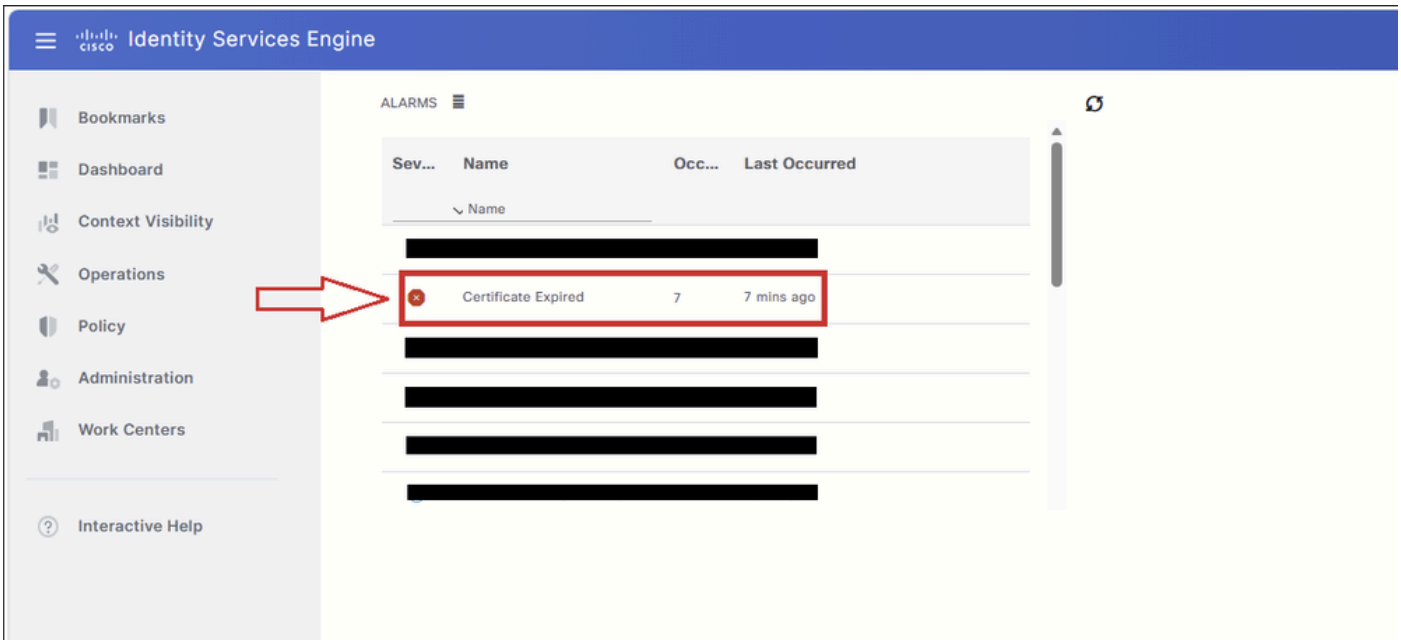
Configuración

Paso 1: Verificación del certificado OCSP caducado

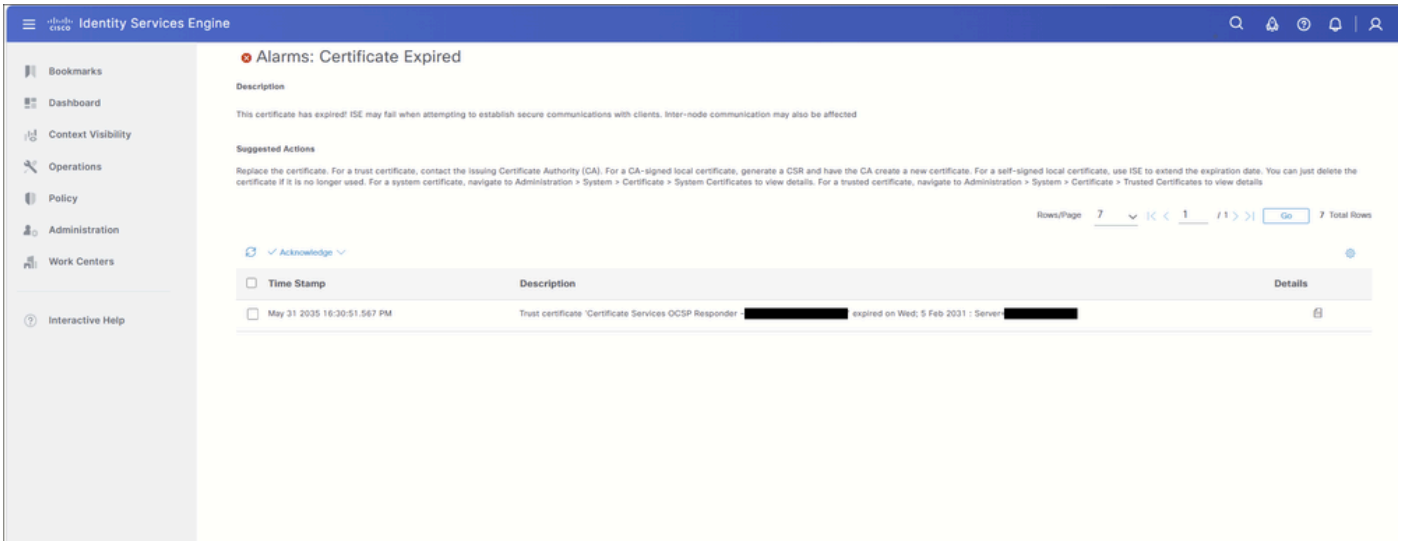
En la GUI de PPAN (Primary Policy Administration Node), vaya a la pestaña Panel (1). En el dashlet Alarmas, haga clic en el botón Separar (2) para expandir la tabla de alarmas.



Haga clic en la alarma Certificate Expired para expandir la tabla y mostrar las entradas de certificado asociadas con la alarma.



En esta tabla se muestran todos los certificados que activaron la alarma Certificate Expired . Esta guía se centra únicamente en los certificados de Respondedor de OCSP. Si la tabla incluye otros tipos de certificados caducados, como EAP, SAML, Admin u otros certificados del sistema, consulte la documentación pertinente de Cisco y la Guía del administrador de Cisco ISE para obtener orientación sobre dichos tipos de certificados.



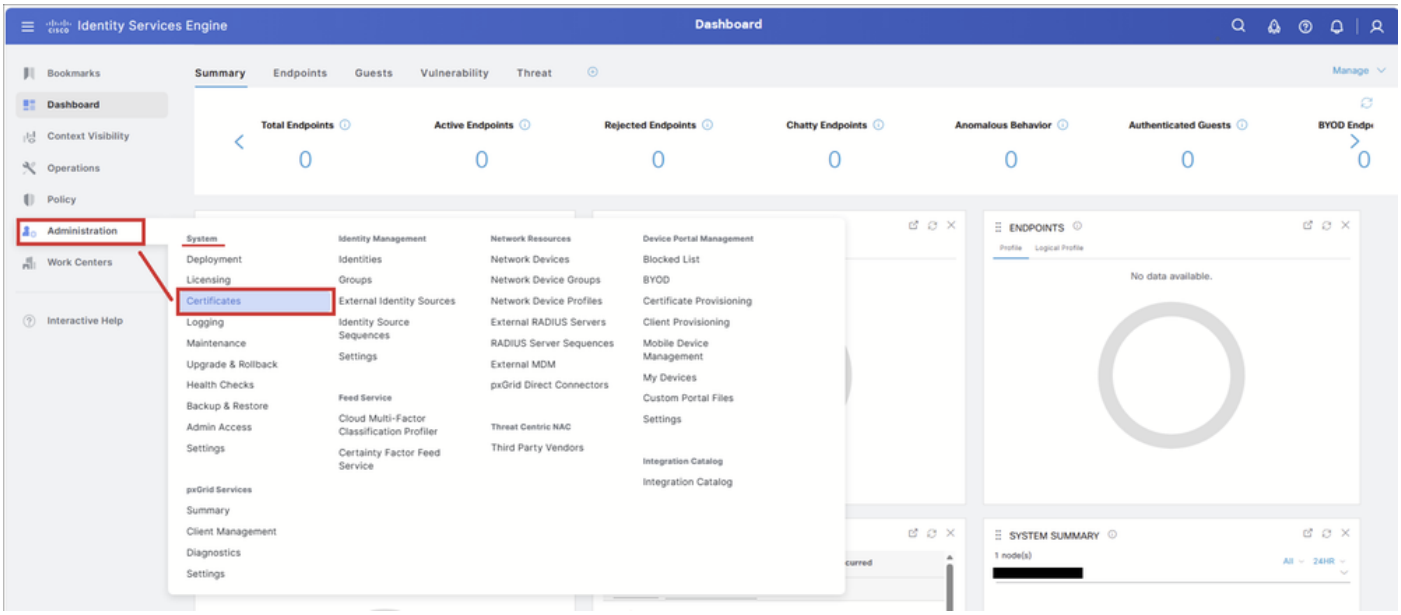
Revise la descripción de la alarma para identificar el certificado que ha caducado o, en algunos casos, que está a punto de hacerlo.

En este ejemplo, el certificado caducado es: Respondedor de OCSP de Servicios de Certificate Server: <node-name>#00004.

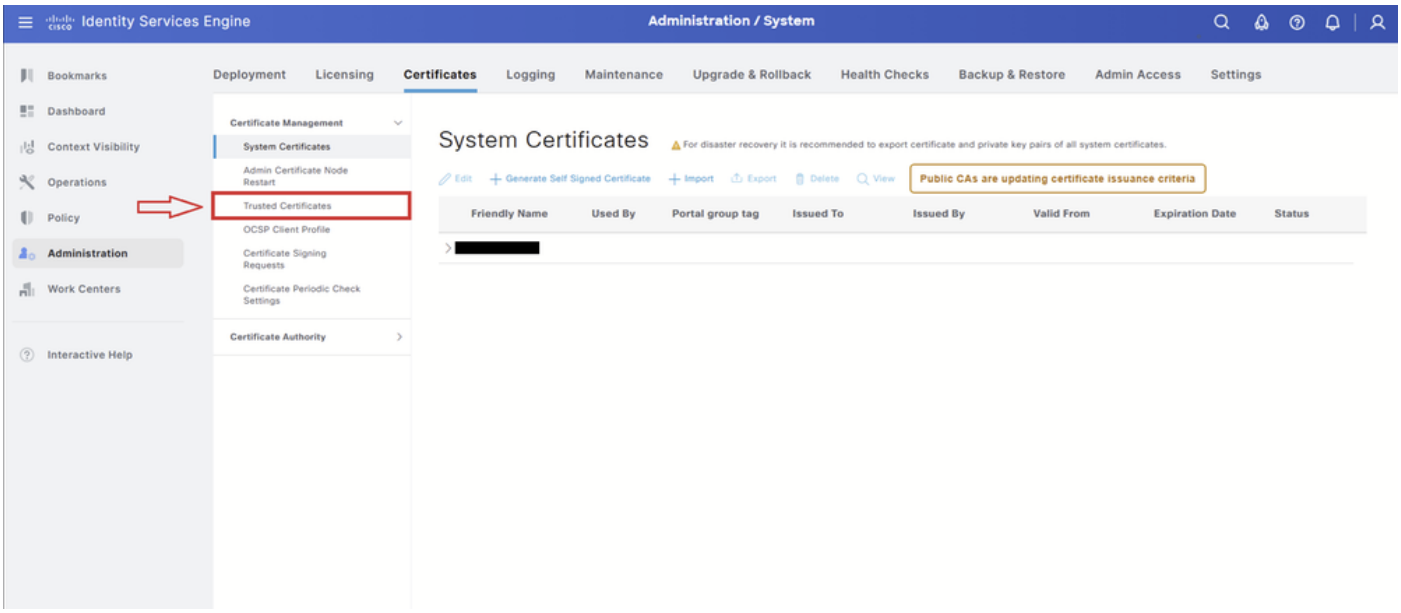
Tome nota del nombre del certificado. Este nombre se utiliza en los pasos siguientes para buscar y eliminar el certificado del almacén de certificados de confianza.

Paso 2: Buscar y eliminar el certificado OCSP caducado

Navegue hasta: Administration > System > Certificates:



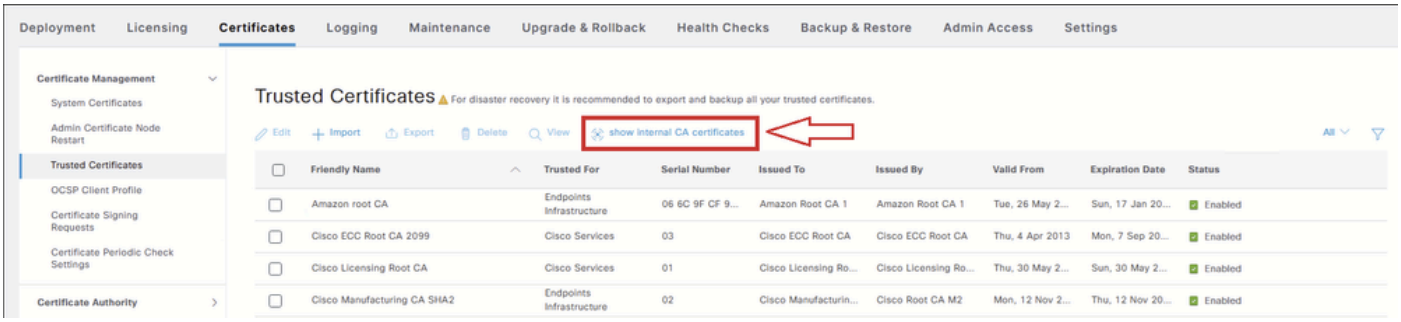
Seleccione la pestaña Certificados de confianza.



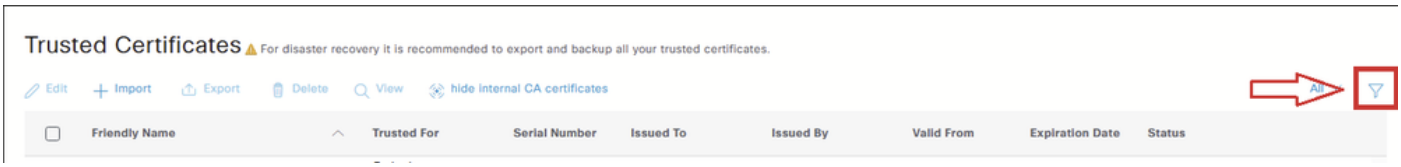
En la página Certificados de confianza, seleccione show internal CA certificates. Muestra los certificados de CA interna (autoridad de certificación) de Cisco ISE, incluidos los certificados de OCSP Responder que están ocultos de forma predeterminada.

Una vez seleccionado, el botón cambia para ocultar los certificados de CA internos.

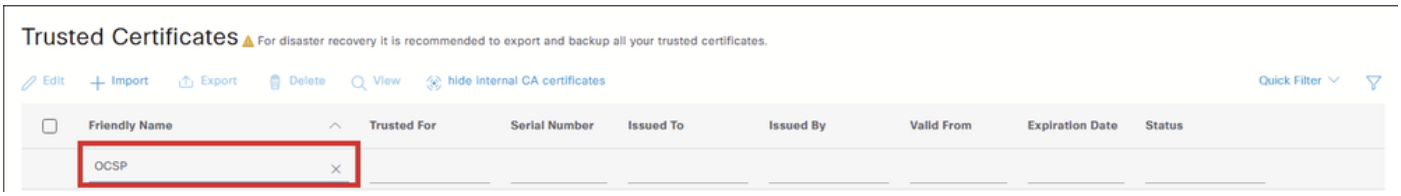
Advertencia: Este paso es obligatorio. Si no se selecciona show internal CA certificates, el certificado de Respondedor de OCSP no aparece en la tabla Almacén de certificados de confianza.



En la tabla Almacén de certificados de confianza, seleccione el icono Filtro para buscar el certificado que se debe eliminar.

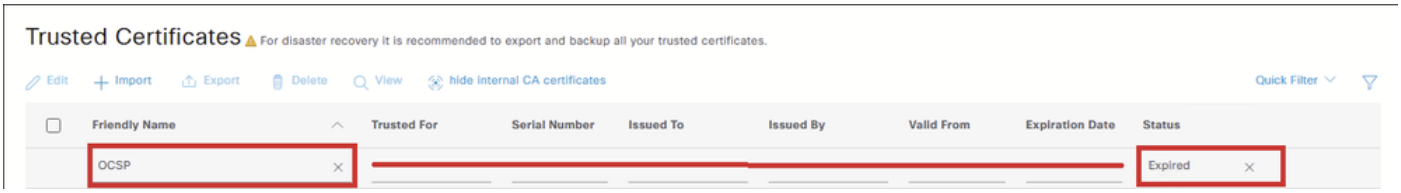


Si el certificado del Respondedor de OCSP está a punto de caducar, filtre sólo por OCSP en Nombre descriptivo. Si el certificado del Respondedor de OCSP ya ha caducado, continúe con la siguiente acción.



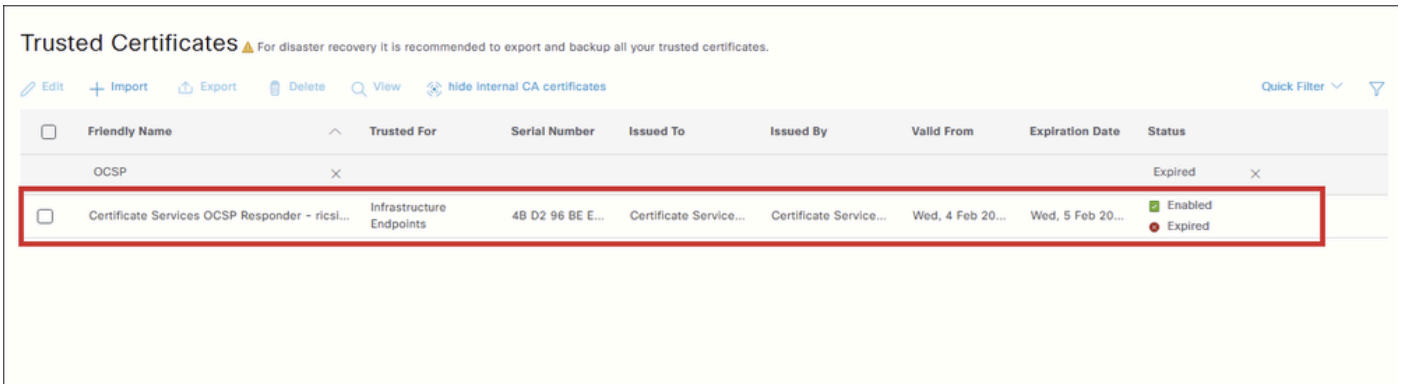
Para buscar un certificado de Respondedor de OCSP caducado, introduzca estos filtros:

- Nombre descriptivo: OCSP
- Estado: Vencido

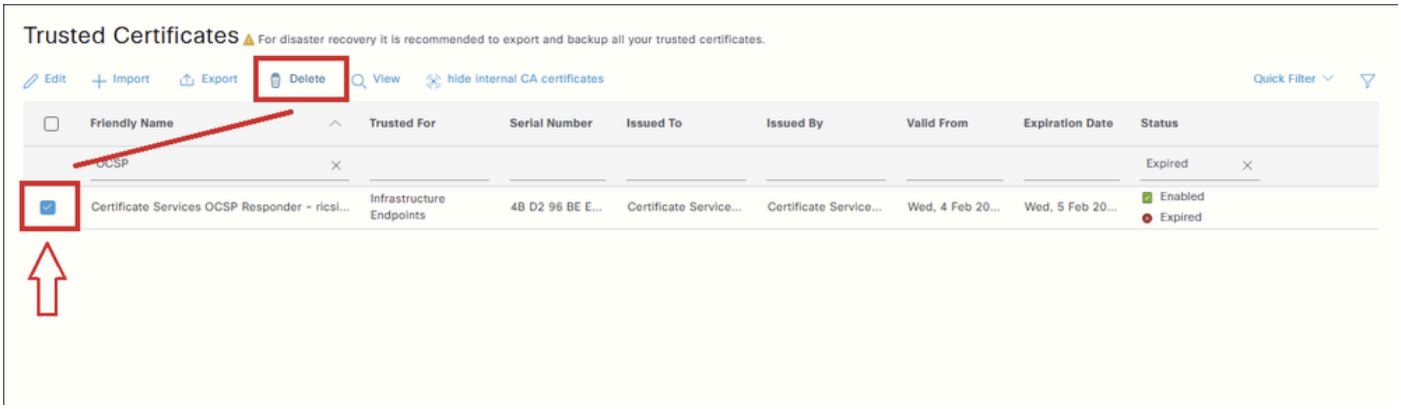


La tabla muestra los certificados de Respondedor de OCSP caducados.

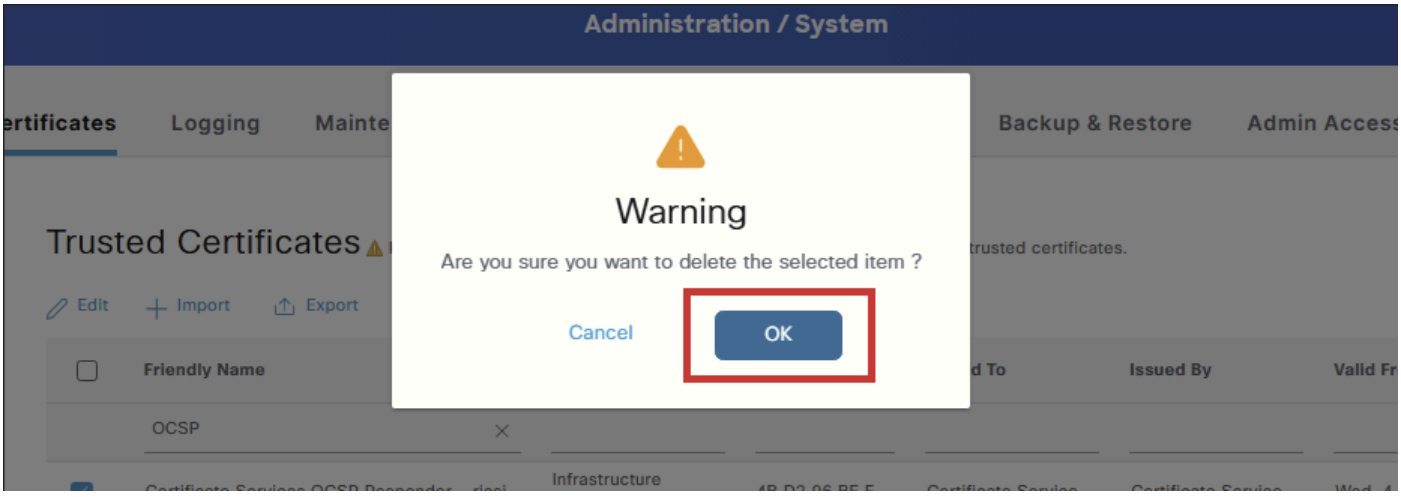
Consejo: Si busca un certificado de Respondedor de OCSP que está a punto de caducar, se pueden mostrar varios certificados, especialmente en implementaciones con varios nodos de Cisco ISE. Para identificar el certificado correcto, no filtre sólo por OCSP. En su lugar, filtre por el nombre completo del certificado que se mostró en los detalles de la alarma en el paso 1.



Seleccione la casilla de verificación junto al certificado de Respondedor de OCSP que debe quitarse y haga clic en Eliminar.



Seleccione Aceptar en la advertencia de confirmación para continuar con la eliminación del certificado.



Antes de eliminar el certificado, es importante comprender que el certificado de Respondedor de

OCSP forma parte de la infraestructura de CA interna de ISE.

La advertencia que aparece durante la eliminación es genérica y se aplica a todos los certificados internos relacionados con la CA. Su objetivo es evitar la eliminación de certificados dentro de la jerarquía de CA interna, ya que algunos de estos certificados firman certificados de terminales utilizados para servicios como BYOD, pxGrid u otras funciones que se basan en certificados emitidos por la CA interna de ISE.

Un certificado de Respondedor de OCSP caducado también puede afectar a los certificados emitidos por la CA interna de ISE. Cuando un cliente o servicio consulta el estado de un certificado emitido por esa CA, el servicio OCSP devuelve un error porque el certificado de Respondedor OCSP ha caducado, lo que puede hacer que falle la validación del estado del certificado.

Al seleccionar Delete, se presentan dos opciones:

- Eliminar certificado: Esta opción elimina el certificado de CA interna de Cisco ISE del almacén de certificados de confianza. Cuando se elimina el certificado de CA interna, todos los certificados de extremo firmados por esa CA dejan de ser válidos y los extremos afectados no pueden tener acceso a la red. Esta acción es reversible: puede restaurar el acceso a la red importando el mismo certificado de CA interna al almacén de certificados de confianza.
- Eliminar y revocar certificado: Esta opción elimina y revoca el certificado de CA interna de Cisco ISE. Al igual que ocurre con la opción Eliminar, todos los certificados de extremo firmados por la CA interna dejan de ser válidos y los extremos afectados pierden el acceso a la red. Sin embargo, esta operación es irreversible. Después de la revocación, debe reemplazar toda la cadena de certificados raíz de Cisco ISE para que la implementación restaure la funcionalidad.

¿Qué opción se debe seleccionar para un certificado de respondedor OCSP caducado?

El impacto descrito se aplica a los certificados de CA interna que firman activamente certificados de extremos. El certificado de Respondedor de OCSP no firma certificados de extremo, se utiliza para la comunicación de OCSP. Aunque un certificado de Respondedor de OCSP caducado puede hacer que falle la validación del estado del certificado para los certificados emitidos por la CA interna, el certificado ya ha caducado y, por tanto, ya no proporciona respuestas de OCSP válidas. Su eliminación no conlleva ningún impacto adicional.

Debido a que el certificado del Respondedor de OCSP en este escenario ya ha expirado, ya no es válido. En este caso, tanto Delete como Delete & Revoke producen el mismo resultado, ya que no queda nada válido para revocar.

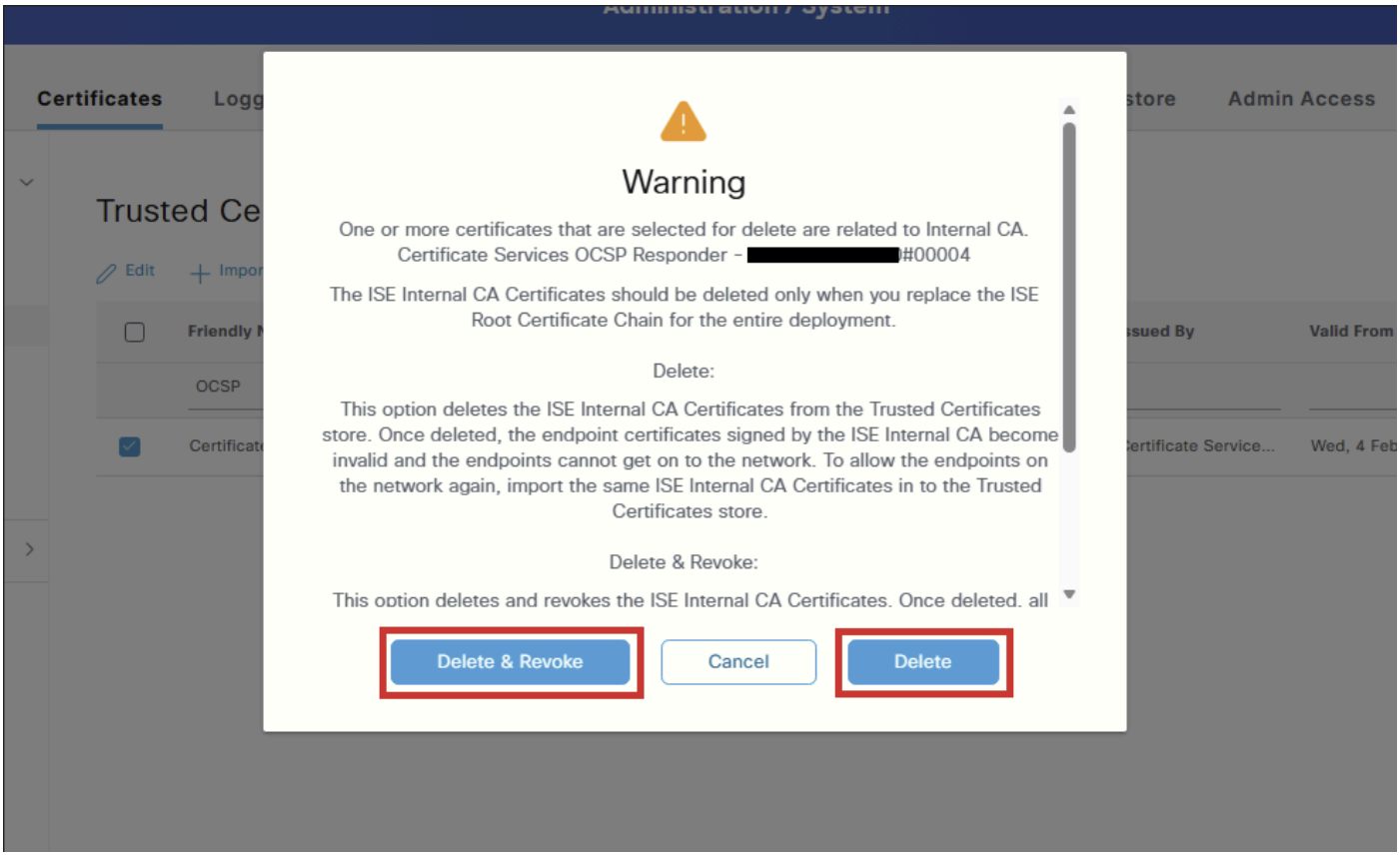
Por estas razones, Delete es la opción recomendada, ya que es la acción más simple y evita generar una entrada de revocación innecesaria.

Nota: Los certificados de Respondedor de OCSP no se vuelven a generar durante el funcionamiento normal. Sólo se regeneran cuando se instala un parche:
- En una implementación de varios nodos, los certificados se vuelven a generar cuando el parche se instala a través de la GUI.
- En una implementación independiente, los certificados se vuelven a generar cuando el parche se instala mediante la GUI o la CLI.

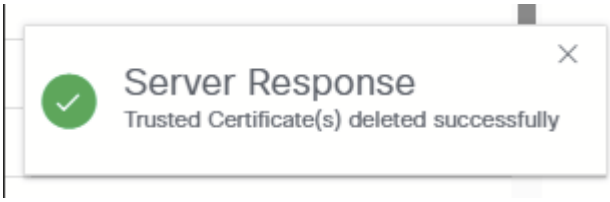
Sólo se genera un nuevo certificado de Respondedor de OCSP en la siguiente instalación de parches.

Precaución: Asegúrese de que el nodo afectado tenga un certificado de Respondedor de OCSP válido y activo en el almacén de certificados de confianza. Si no hay ningún certificado válido y se utiliza OCSP para validar los certificados firmados por la CA interna de ISE, la validación no se realizará hasta que se genere un nuevo certificado de Respondedor de OCSP.

Si no hay un certificado de Respondedor de OCSP válido, renueve los certificados de Respondedor de OCSP del PPAN (nodo de administración de directiva principal) como se describe a continuación:
1. Acceder a la GUI de ISE PAN.
2. Vaya a Administration > System > Certificates.
3. Seleccione Solicitudes de Firma de Certificados a la izquierda.
4. Pulse Generar CSR. Para Uso, seleccione Renovar Respondedor OCSP de ISE.
5. Haga clic en Renovar certificados de Respondedor de ISE OCSP para completar el proceso.



Después de eliminar el certificado, aparece una notificación de respuesta del servidor que indica que el certificado de confianza se eliminó correctamente:



Verificación

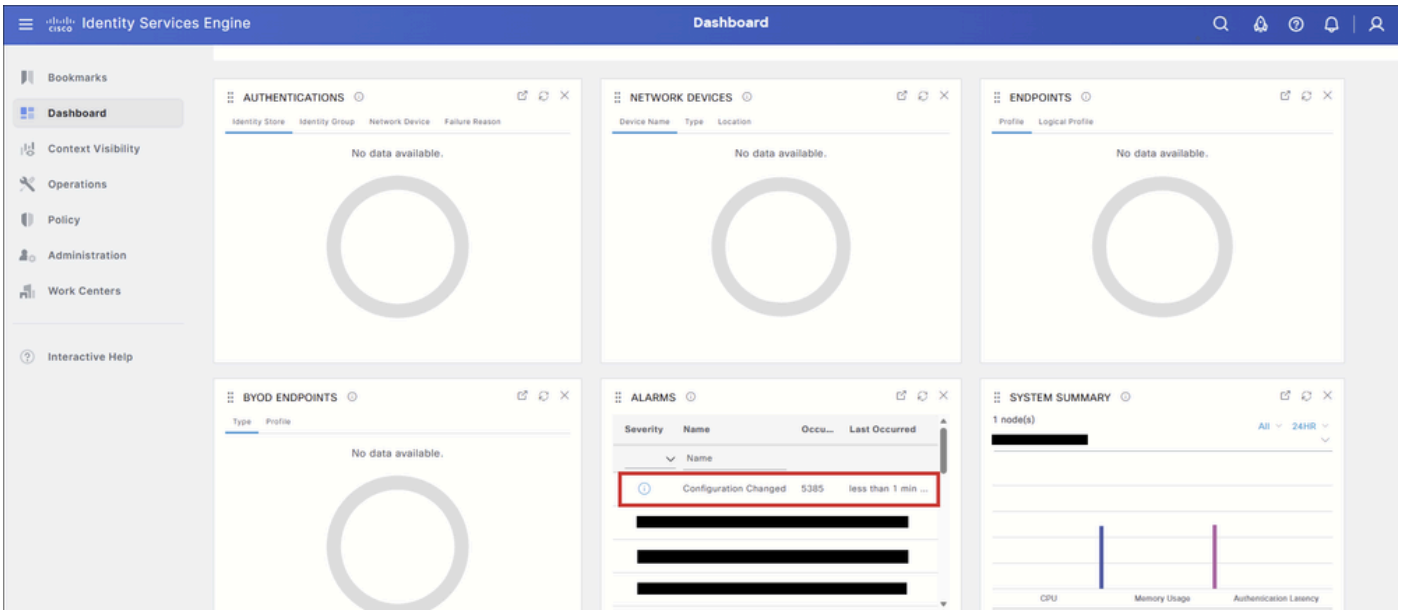
Después de eliminar el certificado, puede utilizar uno o ambos métodos para comprobar que la operación se ha realizado correctamente.

Opción 1: Verificar desde las alarmas del panel

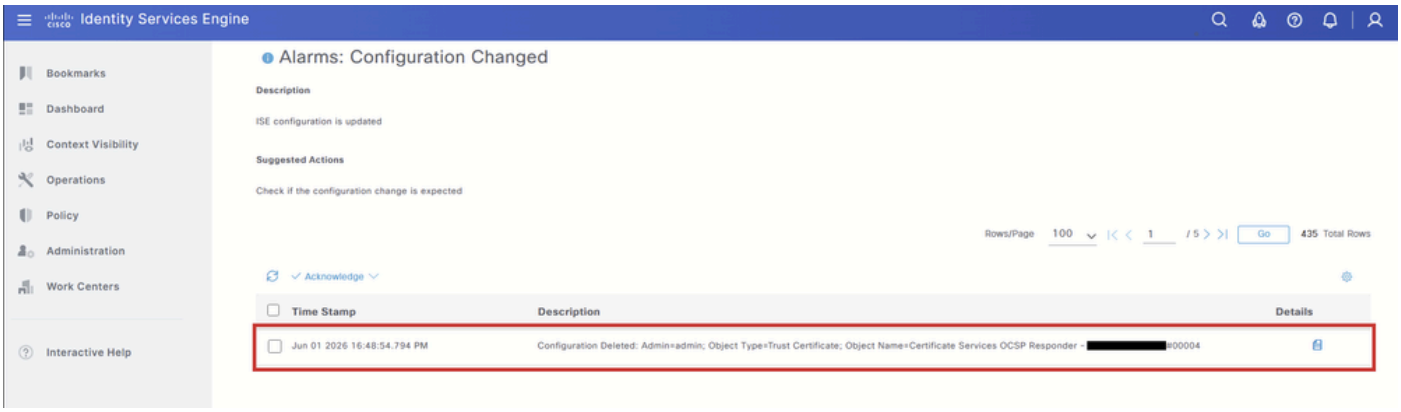
Acceda a la página Panel.

En el dashlet Alarmas, localice la alarma Configuration Changed . Seleccione la alarma para

mostrar los detalles.



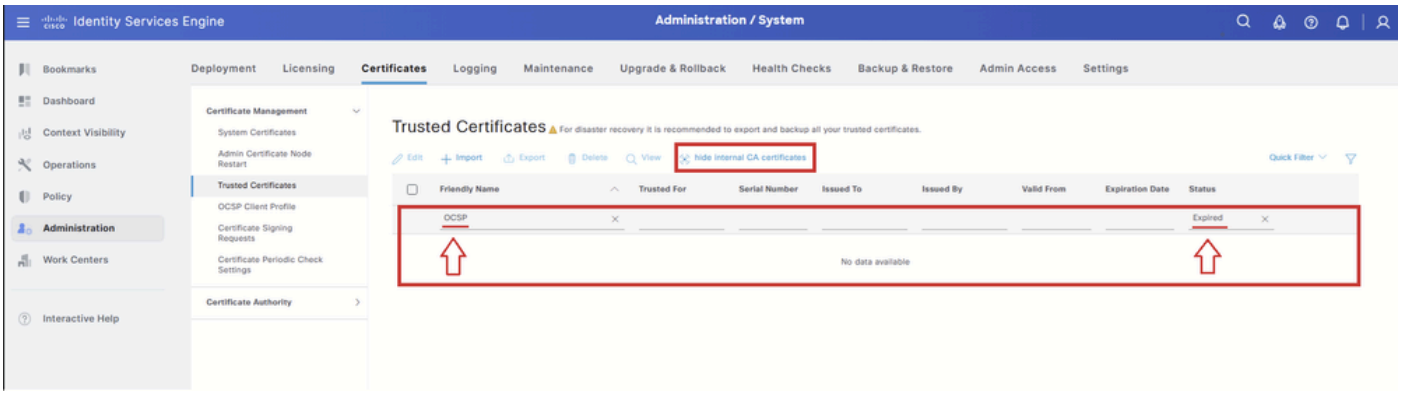
Debe aparecer una entrada que indique que se ha eliminado un objeto de configuración. El nombre de objeto debe coincidir con el certificado del Respondedor de OCSP que se quitó.



Opción 2: verificar desde el almacén de certificados de confianza

Como paso adicional, vuelva a la tabla Almacén de certificados de confianza y filtre el certificado de Respondedor de OCSP. Puesto que se ha eliminado el certificado, la tabla debe mostrar No hay datos disponibles.

Nota: Recuerde seleccionar 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

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).