

Expiración y eliminación del certificado CER

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Generar un certificado nuevo](#)

[Eliminar certificados vencidos](#)

Introducción

Este documento describe un problema con Cisco Emergency Responder (CER) donde recibe la **CertExpiryEmergency**: Mensaje de alarma de vencimiento de certificado **EMERGENCY_ALARM** de la CLI y ofrece una solución al problema.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento de las versiones 2.x a 9.x de CER.

Además, esta configuración requiere que el sistema:

- No contiene configuración de servidor de nombres de dominio (DNS)
- Tiene instalado un servidor CER y certificaciones que están a punto de caducar

Nota: La dirección IP del sistema no importa si ingresa los comandos **Generate New** o **Regenerate** después de haber cambiado el nombre de host o la dirección IP.

Componentes Utilizados

La información de este documento se basa en la versión 9.x de CER.

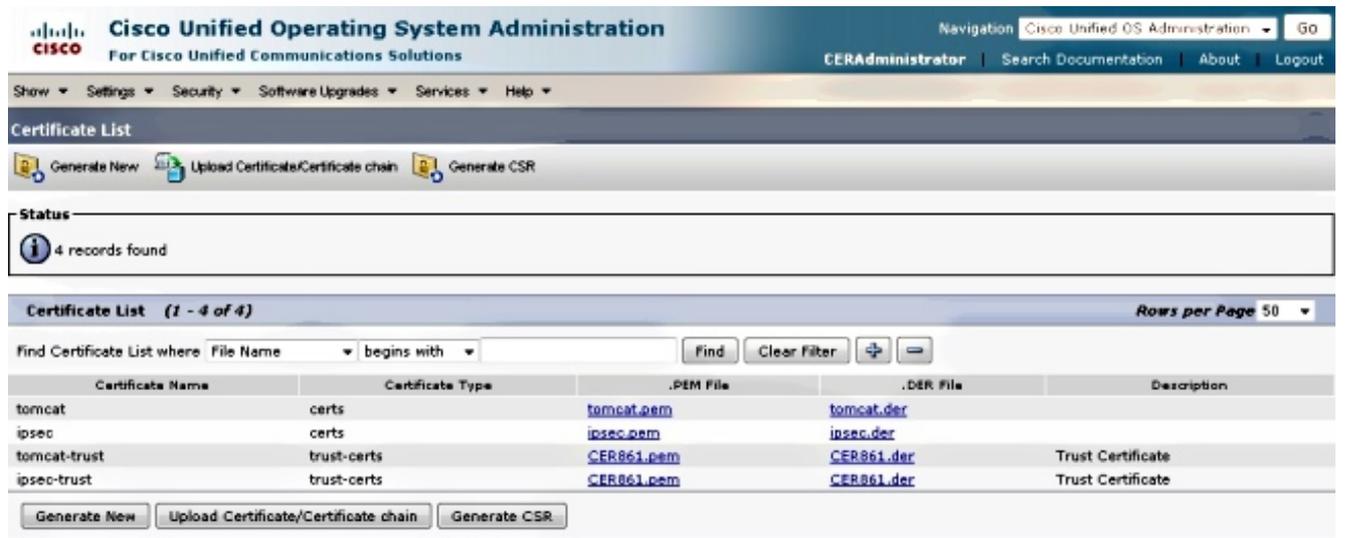
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Generar un certificado nuevo

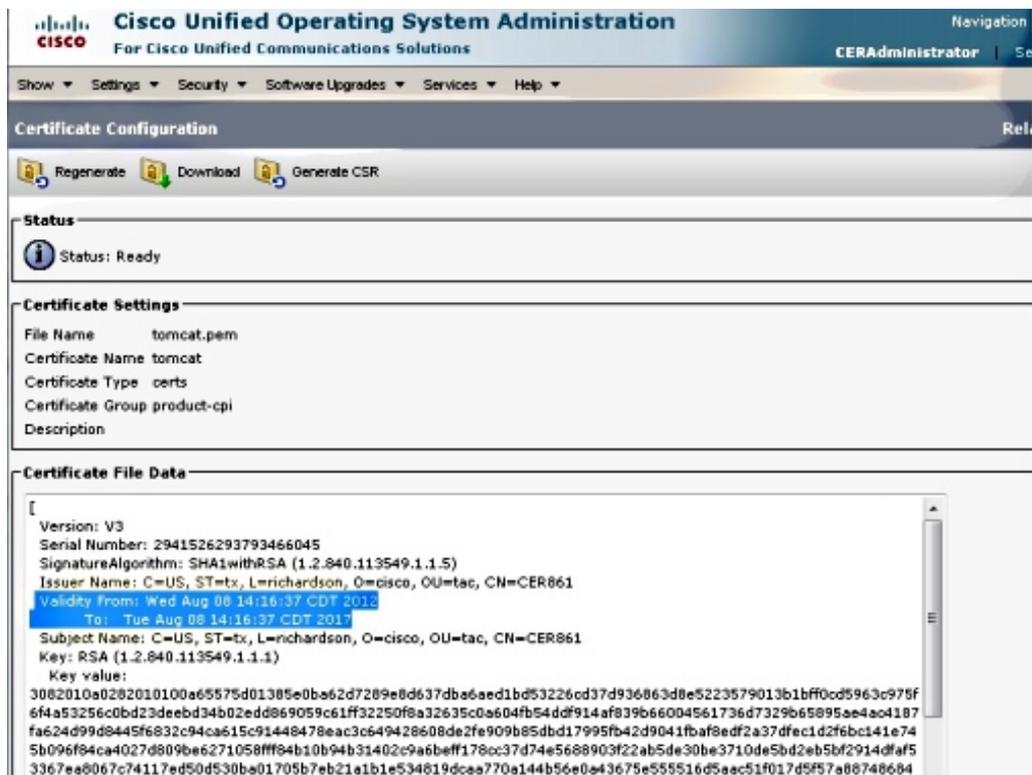
1. Vaya a la GUI en la página de administración del sistema operativo (OS) y seleccione la página **Seguridad > Administración de certificados**.



2. Para mostrar la lista de certificados, haga clic en el botón **Buscar**.



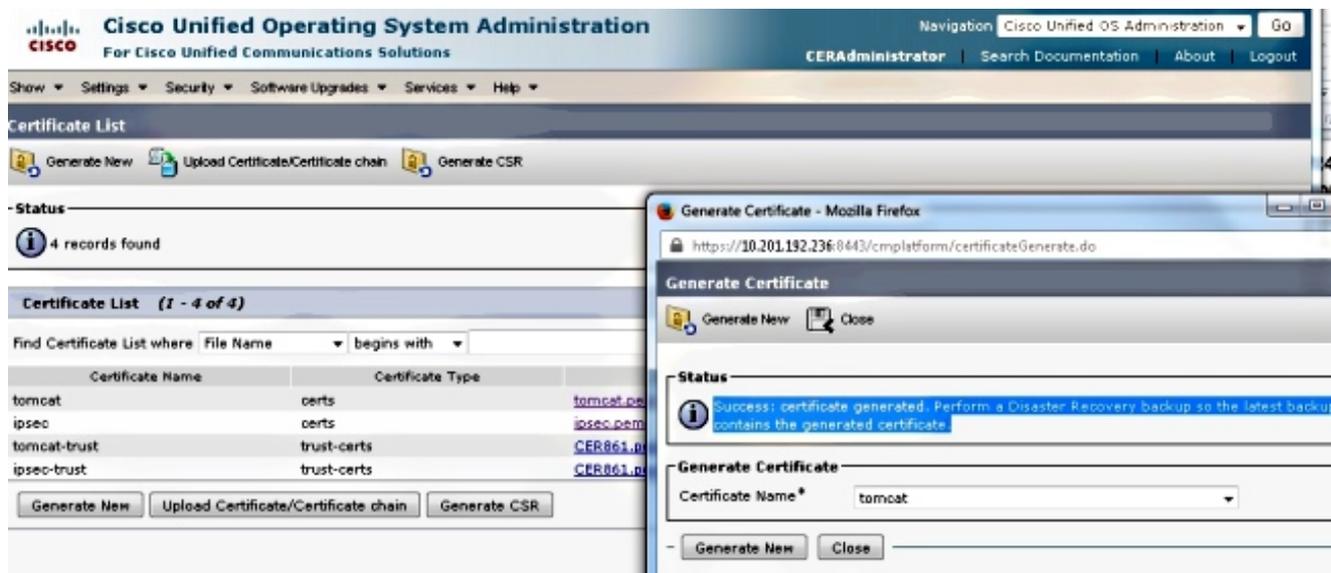
Esta captura de pantalla muestra el certificado **tomcat.pem** y la fecha de **validez** está resaltada. Si el certificado está a punto de caducar, realice los siguientes pasos.



3. Desplácese a la página anterior y haga clic en el icono **Generar nuevo**. Aparece esta pantalla:



4. Para regenerar el certificado, haga clic en **Generar nuevo** en la ventana emergente. Se muestra un mensaje de confirmación para anunciar que el certificado se ha regenerado.



5. Debe reiniciar Tomcat o el servicio de seguridad de protocolo de Internet (IPSec) (si regeneró certificados IPSec). Para reiniciar Tomcat, abra una CLI al nodo e ingrese el comando **utils service restart Cisco Tomcat**. La página web solicita una descarga del nuevo certificado una vez que la página vuelva a estar en línea.

Eliminar certificados vencidos

Notas importantes sobre la eliminación del certificado:

- Asegúrese de que los certificados que se han definido para su eliminación ya no están en uso o han caducado.
- Siempre verifique toda la información del certificado, porque no se puede guardar después de eliminarlo.

Revise todos los certificados con la extensión **.pem** y verifique que estén todos dentro de un rango de tiempo válido. Si no lo son, se pueden eliminar.

Si hay varios servidores en el clúster, debe ir a la dirección IP de cada uno de los servidores. A continuación, en la página OS Admin (Administración del sistema operativo), puede completar los pasos enumerados en la sección Configure (Configurar).