

Vencimiento y cancelación del certificado CER



ID del Documento: 117566

Actualizado: De marcha el 05 de 2014

Contribuido por Guillermo Ryan Bennett, ingeniero de Cisco TAC.



[Descarga PDF](#)



[Imprimir](#)

[Feedback](#)

Productos Relacionados

- [Certificados](#)

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Genere un nuevo certificado](#)

[Borre los certificados vencidos](#)

[Discusiones relacionadas de la comunidad del soporte de Cisco](#)

Introducción

Este documento describe un problema con el Cisco Emergency Responder (CER) donde usted recibe el **CertExpiryEmergency: Certifique el** mensaje de alarma del **vencimiento EMERGENCY_ALARM** del CLI y ofrece una solución al problema.

Prerrequisites

Requisitos

Cisco recomienda que usted tiene conocimiento de las versiones 2.x CER con 9.x.

Además, esta configuración requiere que su sistema:

- No contiene ninguna configuración del Domain Name Server (DNS)
- Tiene un servidor CER instalado y certificados que estén a punto de expirar

Note: El IP Address del sistema no importa si usted ingresa los **nuevos** o **regenerados** comandos de la **generación** después de que usted haya cambiado el nombre de host o el IP Address.

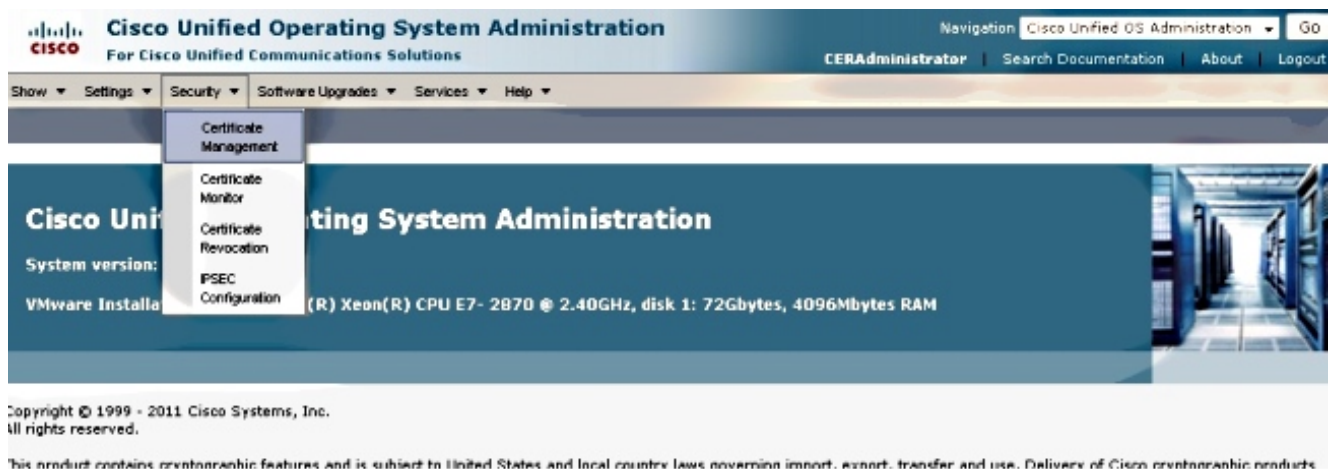
Componentes Utilizados

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Genere un nuevo certificado

1. Vaya al GUI en la página de administración del operating system (OS) y seleccione la página del **Certificate Management (Administración de certificados)** de la Seguridad.



2. Para visualizar la lista de Certificados, haga clic el **botón Find Button**.

Cisco Unified Operating System Administration
For Cisco Unified Communications Solutions

Navigation Cisco Unified OS Administration Go
CERAdministrator | Search Documentation | About | Logout

Show Settings Security Software Upgrades Services Help

Certificate List

Generate New Upload Certificate/Certificate chain Generate CSR

Status
4 records found

Certificate List (1 - 4 of 4) Rows per Page 50

Find Certificate List where File Name begins with Find Clear Filter

Certificate Name	Certificate Type	.PEM File	.DER File	Description
tomcat	certs	tomcat.pem	tomcat.der	
ipsec	certs	ipsec.pem	ipsec.der	
tomcat-trust	trust-certs	CER861.pem	CER861.der	Trust Certificate
ipsec-trust	trust-certs	CER861.pem	CER861.der	Trust Certificate

Generate New Upload Certificate/Certificate chain Generate CSR

Esta captura de pantalla muestra el certificado **tomcat.pem**, y se resalta el Validitydate. Si el certificado está a punto de expirar, complete los pasos próximos.

Cisco Unified Operating System Administration
For Cisco Unified Communications Solutions

Navigation CERAdministrator

Show Settings Security Software Upgrades Services Help

Certificate Configuration

Regenerate Download Generate CSR

Status
Status: Ready

Certificate Settings

File Name tomcat.pem
Certificate Name tomcat
Certificate Type certs
Certificate Group product-cpi
Description

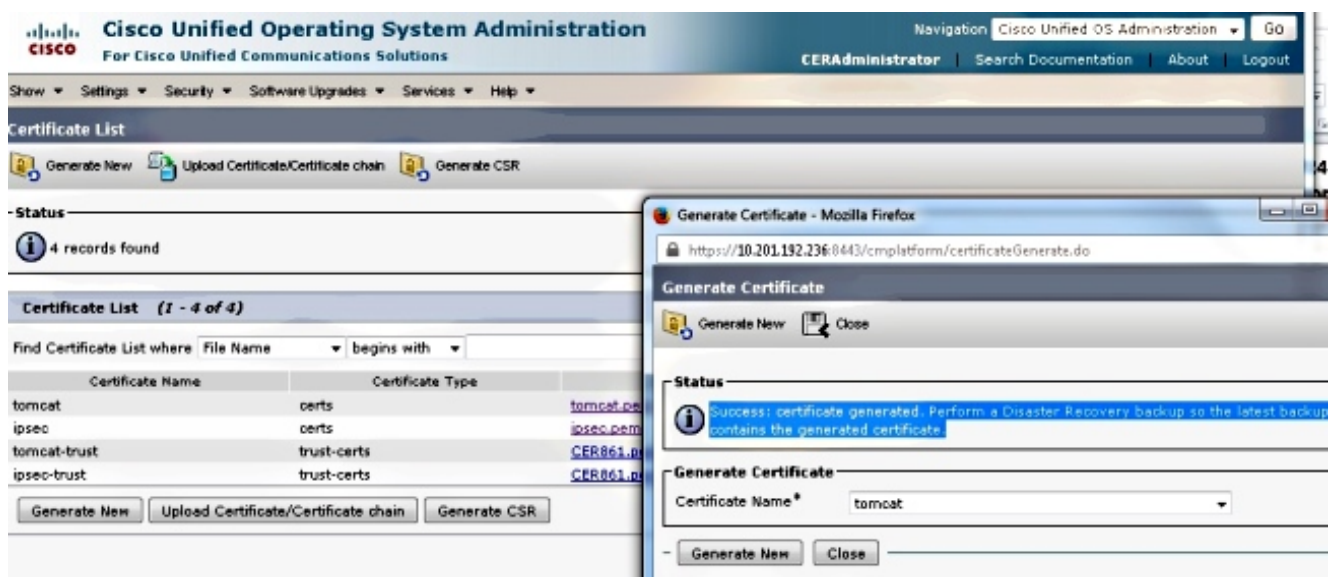
Certificate File Data

```
[
Version: V3
Serial Number: 2941526293793466045
SignatureAlgorithm: SHA1withRSA (1.2.840.113549.1.1.5)
Issuer Name: C=US, ST=tx, L=richardson, O=cisco, OU=tac, CN=CER861
Validity From: Wed Aug 08 14:16:37 CDT 2012
To: Tue Aug 08 14:16:37 CDT 2017
Subject Name: C=US, ST=tx, L=richardson, O=cisco, OU=tac, CN=CER861
Key: RSA (1.2.840.113549.1.1.1)
Key value:
3082010a0282010100a65575d01385e0ba62d7289e8d637dba6aed1bd53226cd37d936863d0e5223579013b1bff0cd5963c975f
6f4a53256c0bd23deebd34b02edd869059c61ff32250fa32635c0a604fb54ddf914af839b66004561736d7329b65895ae4ac4187
fa624d99d8445f6832c94ca615c91448478eac3c649428608de2fe909b85dbd17995fb42d9041fbaf8edf2a37dfec1d2f6bc141e74
5b096f84ca4027d809be6271058fff94b10b94b31402c9a6beff178cc37d74e5688903f22ab5de30be3710de5bd2eb5bf2914dfaf5
3367ea8067c74117ed50d530ba01705b7eb21a1b1e534819dca5770a144b56e0a43675e5551d5aac51f017d5f57a88748684
```

3. Navegue a la página previa y haga clic el nuevo icono de la generación. Este pantallas emergentes para arriba:



4. Para regenerar el certificado, el tecleo **genera nuevo** en la ventana emergente. Visualizaciones de un Mensaje de éxito para anunciar que el certificado está regenerado.



5. Usted debe recomenzar Tomcat o el servicio de la seguridad de protocolos en Internet (IPSec) (si usted regeneró los Certificados del IPSec). Para recomenzar el tomcat, abrir un CLI en el nodo y ingresar el comando del **tomcat de Cisco del reinicio del servicio del utils**. La página web indica para una descarga del nuevo certificado una vez que la página está detrás en línea.

Certificados vencidos de la cancelación

NOTAS IMPORTANTES sobre la cancelación del certificado:

- Asegúrese de que los Certificados que se fijan para la cancelación sean no más funcionando o estén expirados realmente.
- Marque siempre toda la información en el certificado, porque no puede ser guardado después de que se borre.

Revise todos los Certificados con la extensión del **.pem** y verifíquelos que son todos dentro de un rango de tiempo válido. Si no son, después pueden ser borrados.

Si los servidores múltiples están en el cluster, usted debe ir a la dirección IP de cada uno de los servidores. Entonces, dentro de la página de administración OS, usted puede completar los pasos enumerados en la sección de la configuración.

¿Era este documento útil? [Sí ningún](#)

Gracias por su feedback.

[Abra un caso de soporte](#) (requiere un [contrato de servicios con Cisco](#).)

Discusiones relacionadas de la comunidad del soporte de Cisco

[La comunidad del soporte de Cisco](#) es un foro para que usted haga y conteste a las preguntas, las sugerencias de la parte, y colabora con sus pares.

Refiera a los [convenios de los consejos técnicos de Cisco](#) para la información sobre los convenios usados en este documento.

Actualizado: De marcha el 05 de 2014

ID del Documento: 117566