

# Expiração e supressão do certificado CER



ID do Documento: 117566

Atualizado em: março 05, 2014

Contribuído por William Ryan Bennett, engenheiro de TAC da Cisco.



[Transferência PDF](#)



[Imprimir](#)

[Feedback](#)

## Produtos Relacionados

- [Certificados](#)

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Gerencia um certificado novo](#)

[Suprima de certificados expirados](#)

[Cisco relacionado apoia discussões da comunidade](#)

## Introdução

Este documento descreve um problema com o Cisco Emergency Responder (CER) onde você recebe o **CertExpiryEmergency: Certificate o** mensagem de alarme da **expiração EMERGENCY\_ALARM** do CLI e oferece uma solução ao problema.

## Pré-requisitos

### Requisitos

Cisco recomenda que você tem o conhecimento de versões 2.x à 9.x CER.

Adicionalmente, esta configuração exige que seu sistema:

- Não contém nenhuma configuração do Domain Name Server (DNS)
- Tem um server CER instalado e os certificates que estejam a ponto de expirar

**Note:** O endereço IP de Um ou Mais Servidores Cisco ICM NT do sistema não importa se você incorpora os comandos **novos** ou **regenerados da geração** depois que você mudou o hostname ou o endereço IP de Um ou Mais Servidores Cisco ICM NT.

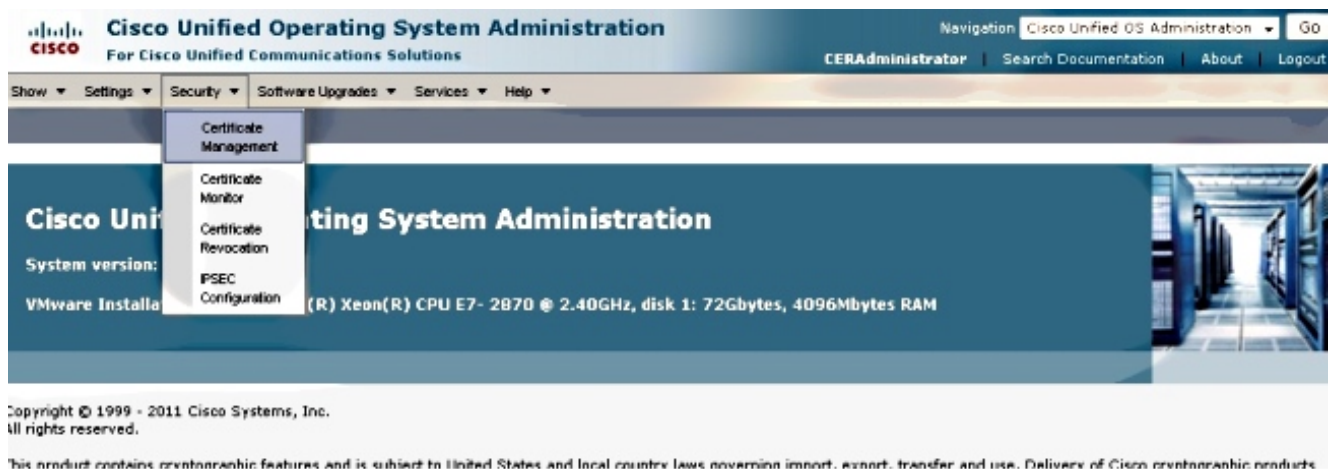
## Componentes Utilizados

A informação neste documento é baseada na versão 9.x CER.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

## Gerencia um certificado novo

1. Vá ao GUI na página de administração do operating system (OS) e selecione a página do > gerenciamento de certificado da Segurança.



2. A fim indicar a lista de Certificados, clique o **botão 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	<a href="#">tomcat.pem</a>	<a href="#">tomcat.der</a>	
ipsec	certs	<a href="#">ipsec.pem</a>	<a href="#">ipsec.der</a>	
tomcat-trust	trust-certs	<a href="#">CER861.pem</a>	<a href="#">CER861.der</a>	Trust Certificate
ipsec-trust	trust-certs	<a href="#">CER861.pem</a>	<a href="#">CER861.der</a>	Trust Certificate

Generate New Upload Certificate/Certificate chain Generate CSR

Esta captura de tela mostra o certificado **tomcat.pem**, e o Validitydate é destacado. Se o certificado está a ponto de expirar, termine as próximas etapas.

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

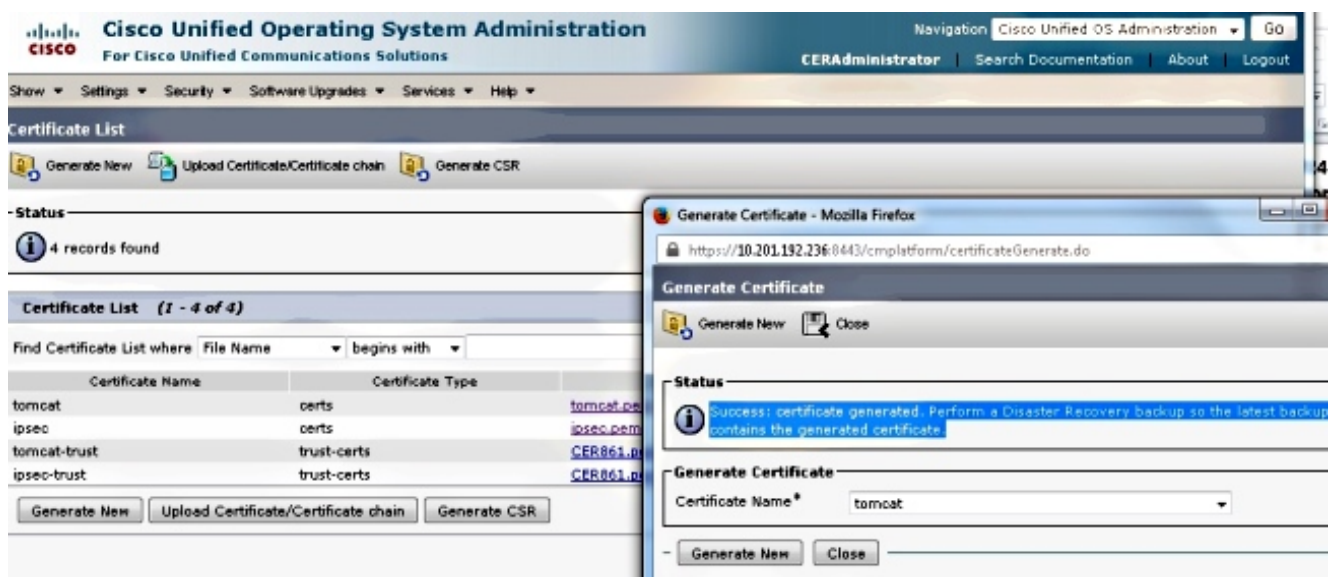
Certificate File Data

```
[
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
fa624d99d8445f6832c94ca615c91448478eac3c649428608de2fe909b85dbd17995fb42d9041fba8edf2a37dfec1d2f6bc141e74
5b096f84ca4027d809be6271058fff94b10b94b31402c9a6beff178cc37d74e5688903f22ab5de30be3710de5bd2eb5bf2914dfaf5
3367ea8067c74117ed50d530ba01705b7eb21a1b1e534819dca5770a144b56e0a43675e5551d5aac51f017d5f57a88748684
```

3. Navegue à página anterior e clique o ícone novo da geração. Este pop de tela acima:



4. A fim regenerar o certificado, o clique **gerencie novo** na janela pop-up. Indicadores de mensagem de sucesso a fim anunciar que o certificado está regenerado.



5. Você deve reiniciar Tomcat ou o serviço da segurança de protocolo do Internet (IPsec) (se você regenerou Certificados do IPsec). A fim reiniciar Tomcat, abrir um CLI ao nó e incorporar o comando de **Cisco Tomcat do reinício do serviço dos utils**. O Web page alerta para uma transferência do certificado novo uma vez que a página é para trás em linha.

## Certificados expirados da supressão

Observações importantes sobre o supressão do certificado:

- Assegure-se de que os Certificados que são ajustados para o supressão sejam já não dentro uso ou estejam expirados realmente.
- Verifique sempre toda a informação no certificado, porque não pode ser salvar depois que é.

Revisto todos os Certificados com a extensão do **.pem** e verifique que são todos dentro de uma escala de tempo válido. Se não são, a seguir podem ser suprimidos.

Se os servidores múltiplos estão no conjunto, você deve ir ao endereço IP de Um ou Mais Servidores Cisco ICM NT de cada um dos server. Então, dentro da página de admin do OS, você pode terminar as etapas alistadas na seção configurar.

Era este documento útil? [Sim nenhum](#)

Obrigado para seu feedback.

[Abra um caso de suporte](#) (exige um [contrato de serviço Cisco](#).)

## Cisco relacionado apoia discussões da comunidade

[Cisco apoia a comunidade](#) é um fórum para que você faça e responda a perguntas, sugestões da parte, e colabora com seus pares.

Refira [convenções dos dicas técnicas da Cisco](#) para obter informações sobre das convenções usadas neste documento.

Atualizado em: março 05, 2014

ID do Documento: 117566