CER Certificate Expiry and Deletion

Contents

Introduction

This document describes a problem with the Cisco Emergency Responder (CER) where you receive the **CertExpiryEmergency: Certificate Expiry EMERGENCY_ALARM** alarm message from the CLI and offers a solution to the problem.

Prerequisites

Requirements

Cisco recommends that you have knowledge of CER Versions 2.x through 9.x.

Additionally, this configuration requires that your system:

- Contains no Domain Name Server (DNS) configuration
- Has a CER server installed and certifcates that are about to expire

  Note: The IP address of the system does not matter if you enter the **Generate New** or **Regenerate** commands after you have changed the hostname or IP address.

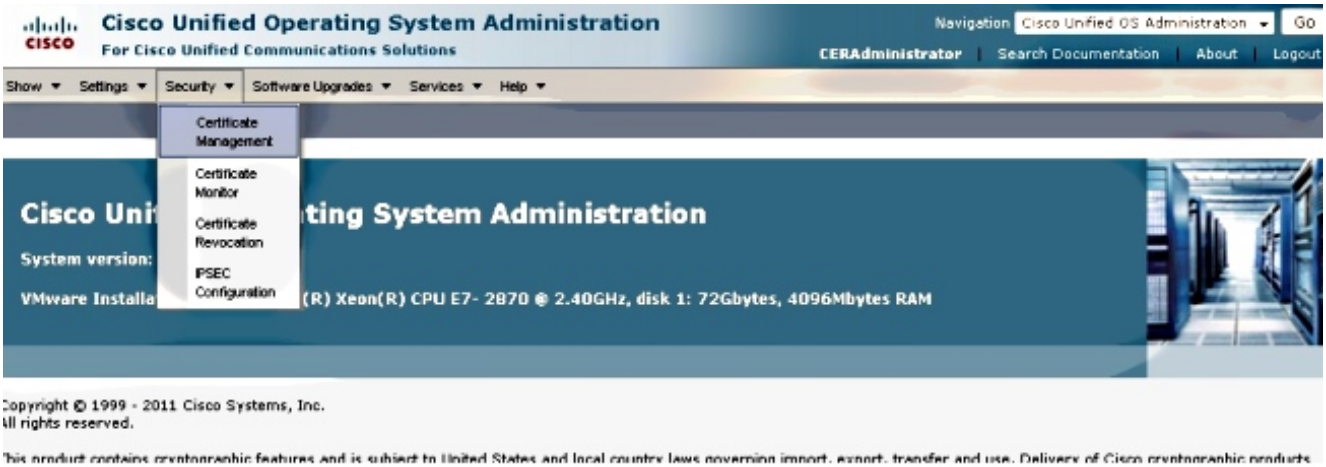
Components Used

The information in this document is based on CER Version 9.x.

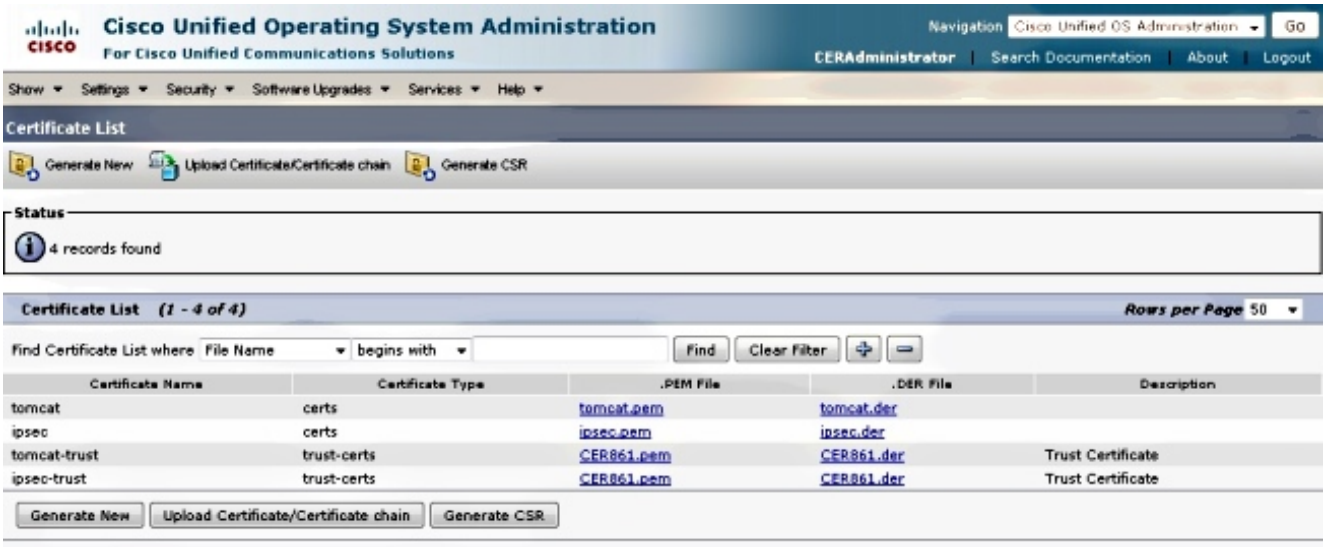
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Generate a New Certificate

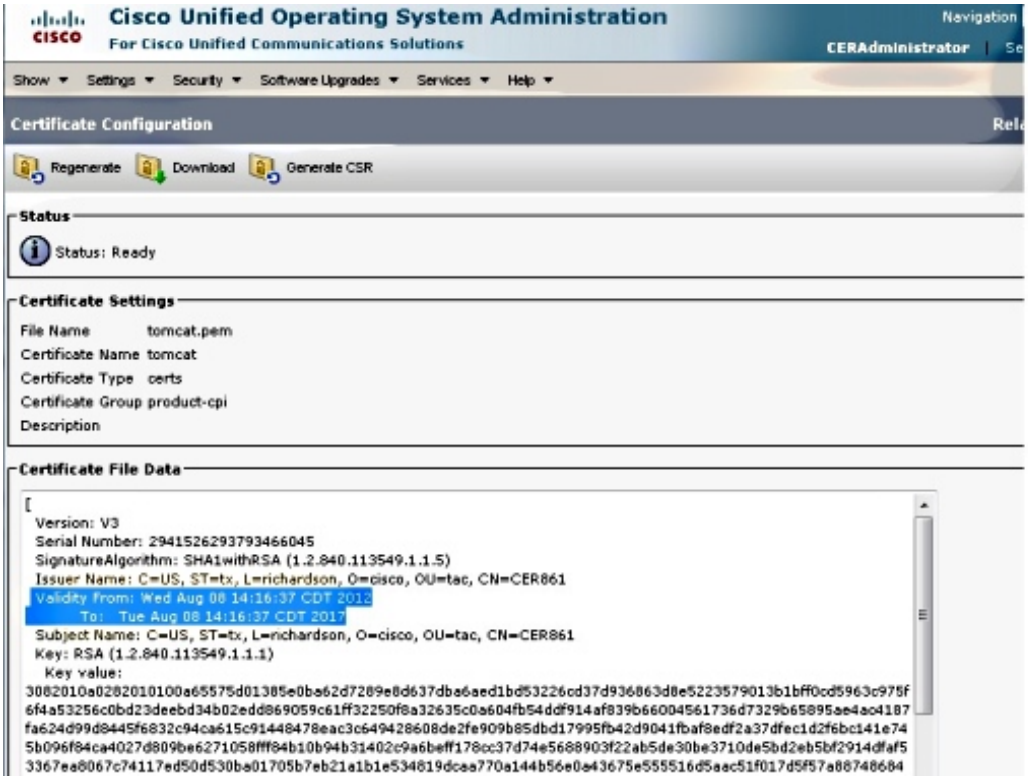
1. Go to the GUI in the operating system (OS) Administration page and select the **Security > Certificate Management** page.



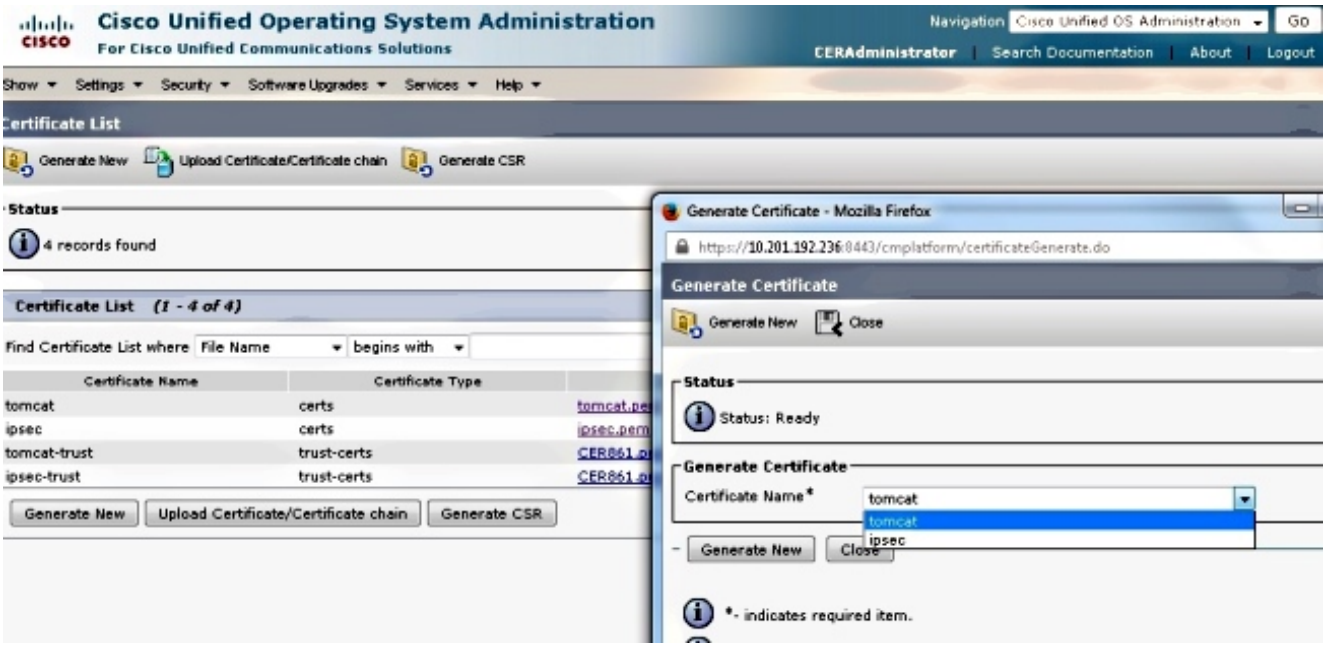
2. In order to display the list of certificates, click the **Find** button.



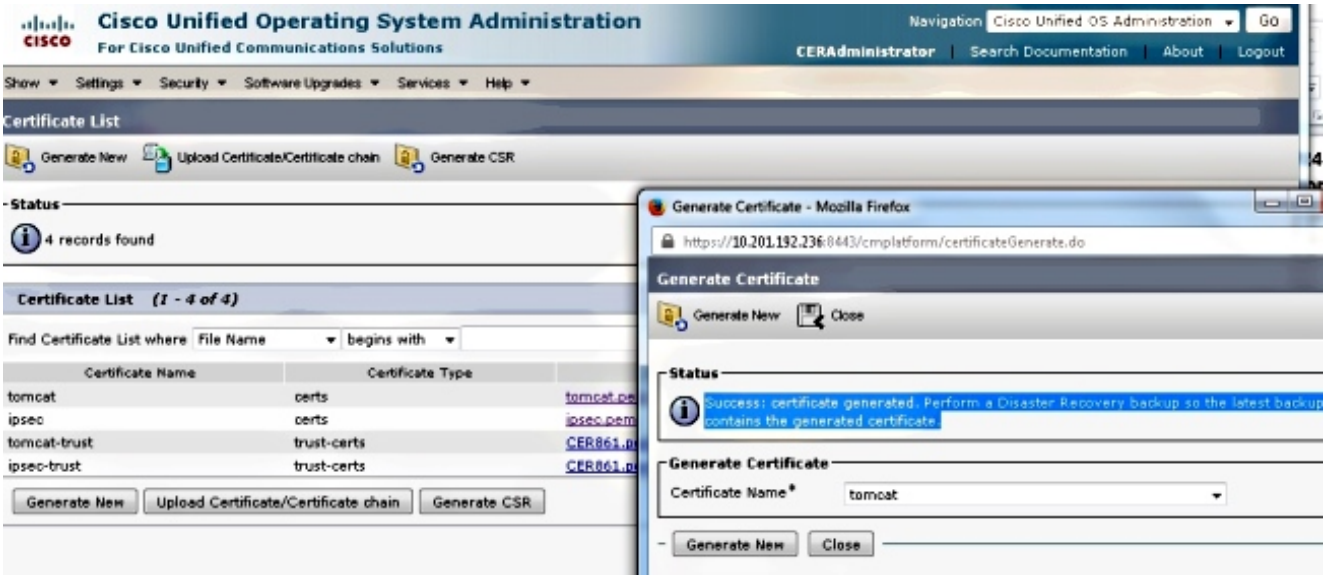
This screen capture shows the **tomcat.pem** certificate, and the **Validity** date is highlighted. If the certificate is about to expire, complete the next few steps.



3. Navigate to the previous page and click the **Generate New** icon. This screen pops up:



4. In order to regenerate the certificate, click **Generate New** in the popup window. A success message displays in order to announce that the certificate is regenerated.



5. You must restart Tomcat or the Internet Protocol Security (IPSec) service (if you regenerated IPSec certificates). In order to restart Tomcat, open a CLI to the node and enter the **utils service restart Cisco Tomcat** command. The webpage prompts for a download of the new certificate once the page is back online.

Delete Expired Certificates

Important notes about certificate deletion:

- Ensure that certificates that are set for deletion are no longer in use or are actually expired.
- Always check all of the information in the certificate, because it is not able to be saved after it is deleted.

Review all of the certificates with the **.pem** extension and verify that they are all within a valid time range. If they are not, then they can be deleted.

If multiple servers are in the cluster, you must go to the IP address of each of the servers. Then, within the OS Admin page, you can complete the steps listed in the Configure section.