Contents

Introduction

This document describes a problem with Cisco CallManager (CM) where you receive the **CertExpiryEmergency: Certificate Expiry EMERGENCY_ALARM** alarm message from the Real-Time Monitoring Tool (RTMT) client, and offers a solution to the problem.

Prerequisites

Requirements

Cisco recommends that you have knowledge of CM Versions 6.x through 9.x, and that your system:

- Does not have a Domain Name System (DNS) configuration. This is done for simplicity of the document, but many systems have it configured which is OK.
- Does have a certificate that is expired and must be regenerated, or a certificate that is scheduled to expire.

  Note: The IP address of the system does not matter if you enter the **Generate New** or **Regenerate** command after you change the host name or IP address.

Components Used

The information in this document is based on the Cisco CM server with administration pages.

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.

Problem

You receive a **CertExpiryEmergency: Certificate Expiry EMERGENCY_ALARM** alarm message from the RTMT in CM:

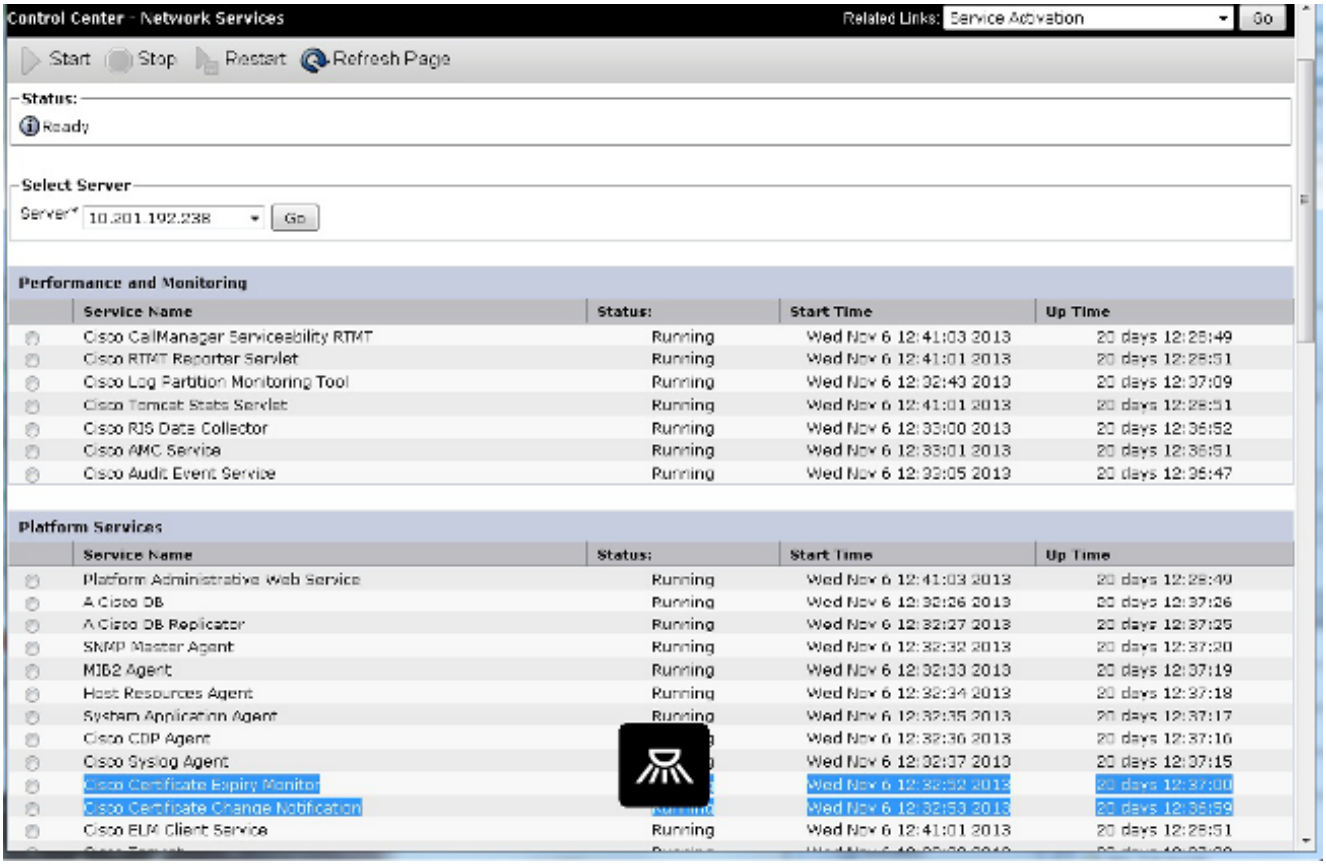
```
Message from syslogd@HOST-CM-PRI at Fri Jul 5 13:00:00 2013 ...
HOST-CM912 local7 0 : 629: Jul 30 17:00:00.352 UTC :
%CCM_UNKNOWN-CERT-0-CertExpiryEmergency: Certificate Expiry EMERGENCY_ALARM
Message:Certificate expiration Notification.
 Certificate name:CAPF Unit:CAPF Type:own-cert
Expiration:Fri Dec 28 12:14:42:000 EST 2012 / App ID:Cisco Certificate
Monitor Cluster ID:Node ID:HOST-CM-PRI

Message from syslogd@HOST-CM-PRI at Fri Jul 5 13:00:00 2013 ...
HOST-CM912 local7 0 : 630: Jul 30 17:00:00.353 UTC :
%CCM_UNKNOWN-CERT-0-CertExpiryEmergency: Certificate Expiry EMERGENCY_ALARM
Message:Certificate expiration Notification. Certificate name:CAPF-5d0a9888
Unit:CallManager-trust Type:trust-cert Expiration:Fri Dec 28 App ID:
 Cisco Certificate
Monitor Cluster ID: Node ID:HOST-CM-PRI

Message from syslogd@HOST-CM-PRI at Fri Jul 5 13:00:00 2013 ...
HOST-CM912 local7 0 : 631: Jul 30 17:00:00.354 UTC :
%CCM_UNKNOWN-CERT-0-CertExpiryEmergency: Certificate Expiry EMERGENCY_ALARM
Message:Certificate expiration Notification. Certificate name:CAPF-5d0a9888
Unit:CAPF-trust Type:trust-cert Expiration:Fri Dec 28 12:14:4 App ID:
 Cisco Certificate
Monitor Cluster ID: Node ID:HOST-CM-PRI
```

Solution

Use the information in this section in order to resolve the CM alarm message problem.

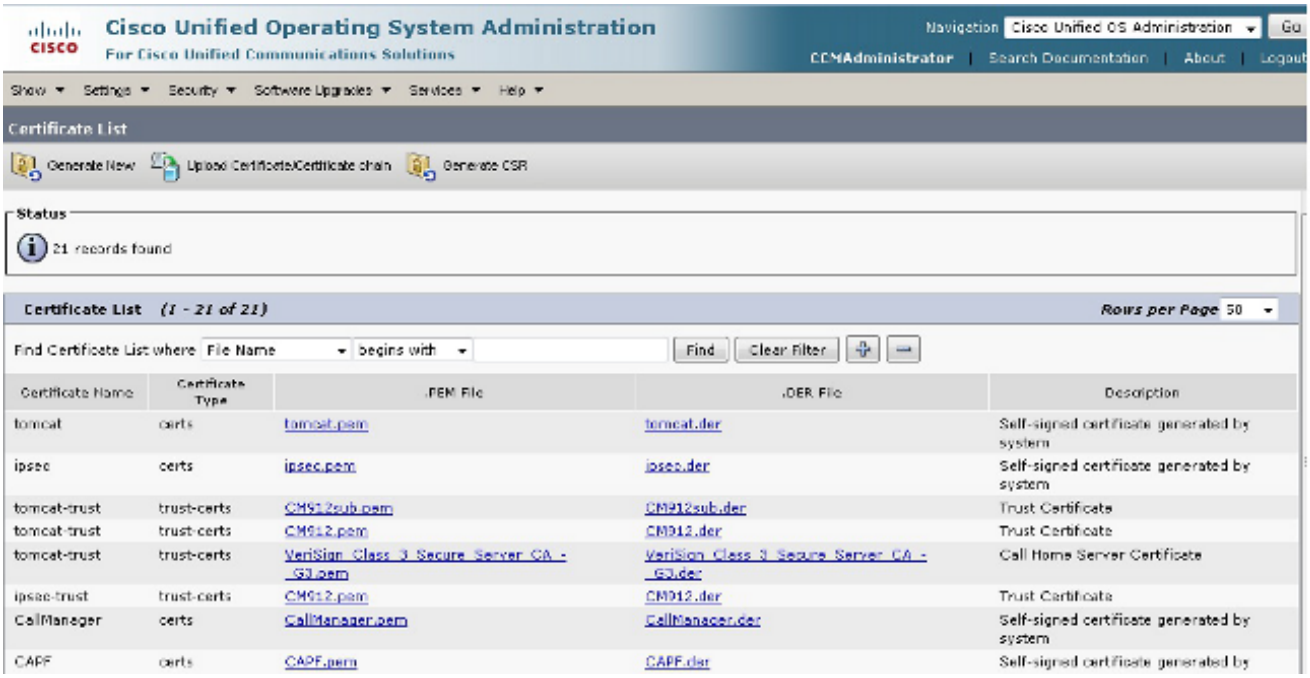
1. From the CM Unified Serviceability page GUI, navigate to **Tools > Control Center - Network Services**.

2. Stop the **Cisco Certificate Expiry Monitor** and **Cisco Certificate Change Notification** services on all of the servers in the cluster:



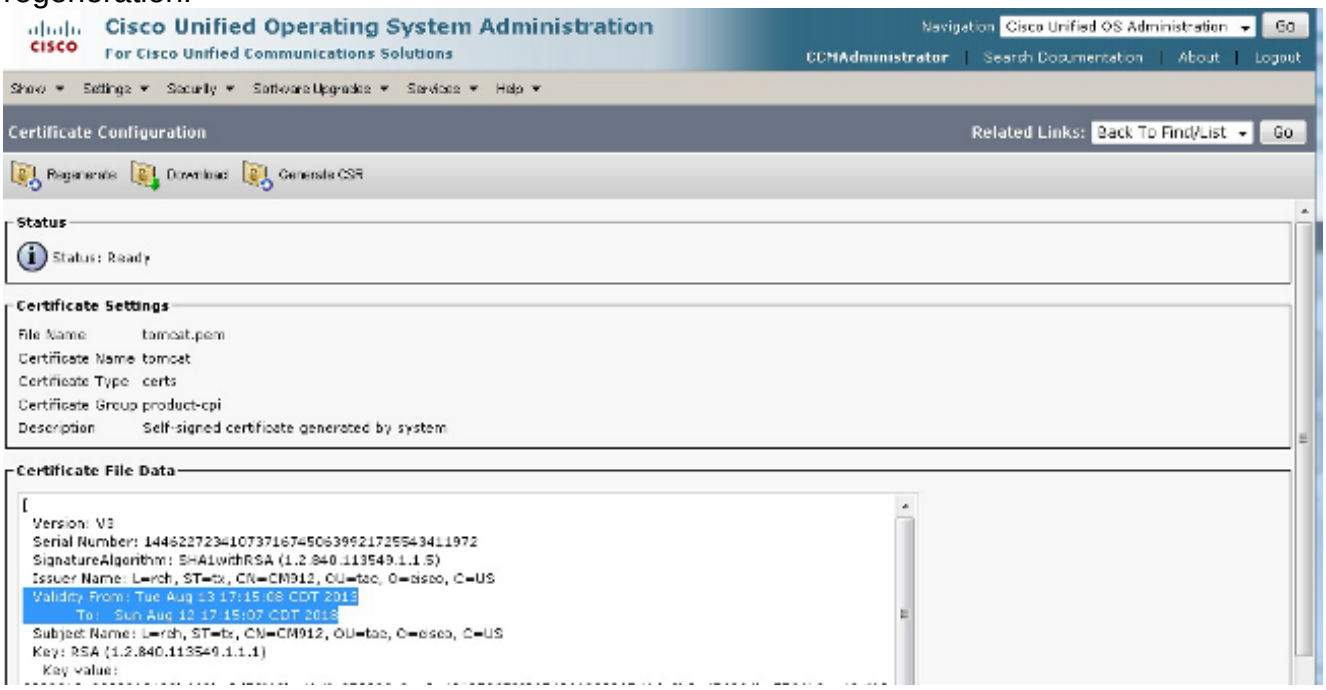
3. From the Operating System (OS) Administration GUI, navigate to **Security > Certificate Management**, and this screen displays:

4. Click **Find** in order to display all of the certificates on a particular server:

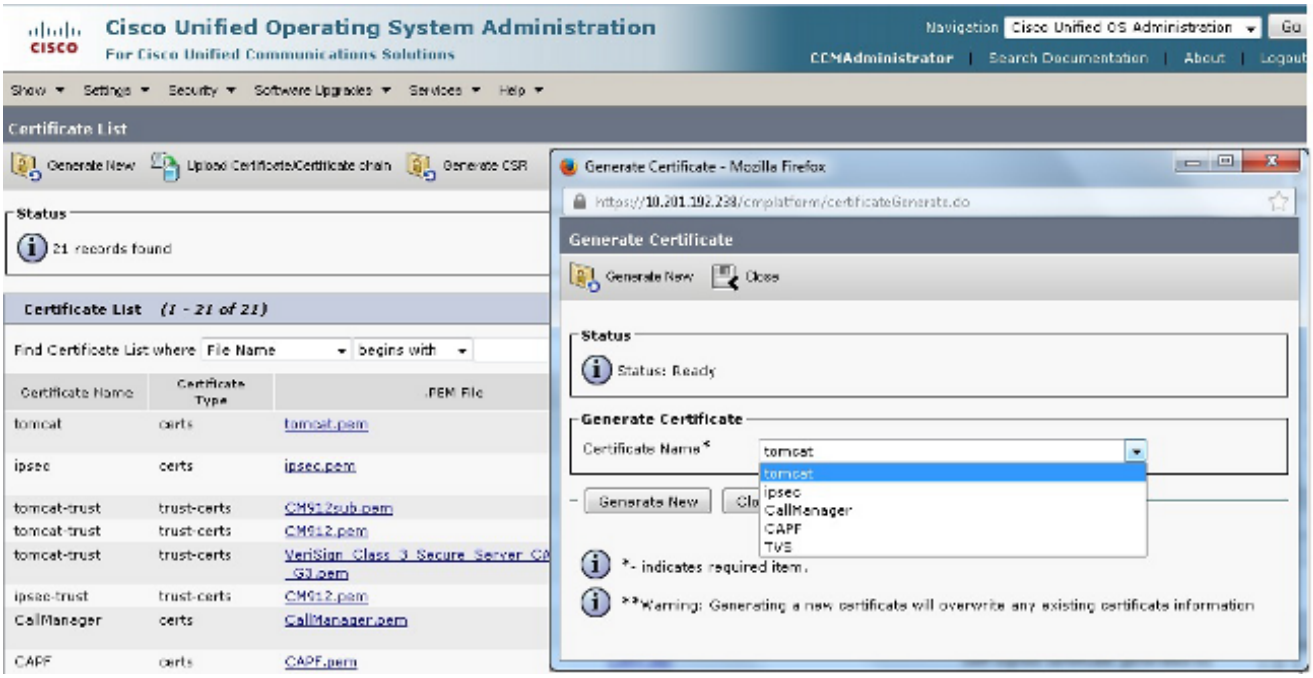


5. Click any certificate (a Tomcat certificate in this case) and view the date, as highlighted in the next image. For Tomcat certificates, verify if the server uses a third-party certificate for the **ccmadmin** page login. You can check this when you log into the page from a browser.

   Note: If it is a third-party signed certificate, reference the [CUCM Uploading CCMAdmin Web GUI Certificates] Cisco Support Community article and complete the steps after the Tomcat regeneration.

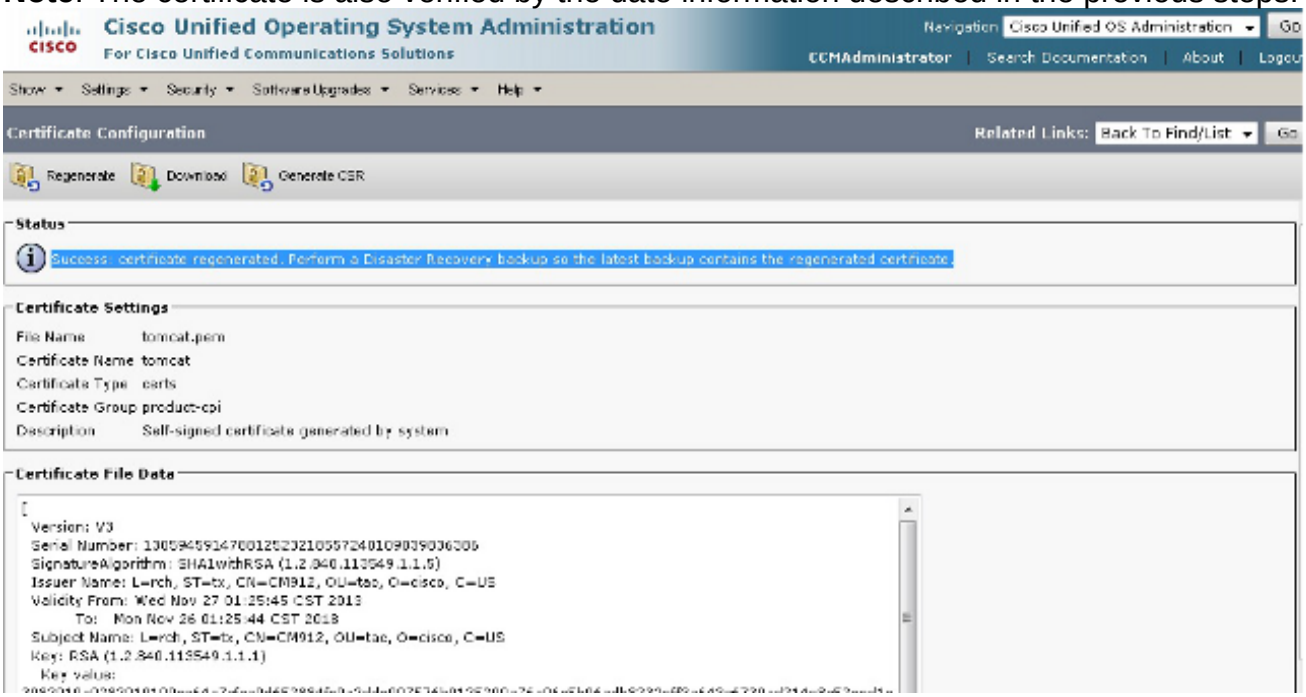


6. Navigate to the **Certificate Management** page on the Publisher. Find and click the **tomcat.pem** file, and then click **Regenerate**:



7. In order to restart Tomcat service on that node, open a CLI to the node and enter the **utils service restart Cisco Tomcat** command. Once the certificate is generated, a message pops up in order to confirm that the certificate is current.

   Note: The certificate is also verified by the date information described in the previous steps.



8. Complete this process for each of the subscribers in the cluster in order to regenerate the tomcat certificates.

Certificate Regeneration for CUCM Versions 8.x and Later

Use the information in this section in order to regenerate expired certificates for Cisco Unified Communications Manager (CUCM) Versions 8.x and later.

Note: Regenerate the certificates after normal business hours, because you must restart

services and reboot the phones in the process.

CAPF

For the Certificate Authority Proxy Function (CAPF) regeneration, ensure that the cluster is not in a secure cluster mode: navigate to **System > Enterprise Parameters** from the CM Administration web page, and search for **Cluster Secure Mode**. If the value is **0**, then the cluster is not in a secure cluster mode. If the value is any number other than zero, then the cluster is in a secure mode, and you must use the Certificate Trust List (CTL) client in order to update the CTL file.

> **Note**: Reference the IP Phone Security and CTL (Certificate Trust List) Cisco Support Community article for more information.

1. From the Publisher, navigate to the Certificate Management page.
2. Open the **CAPF.pem** file and click **Regenerate**. This renews the certificate and creates two new trust files: one is the CM-trust and the other is the CAPF-trust.
3. From the the Serviceability page, navigate to **Tools > Feature Services**.
4. If the CAPF service is activated under **Feature Services**, then restart the service. If the CAPF service is not activated, then a restart is not necessary.
5. Navigate to **Tools > Network Services** from the Serviceability page, and restart the Trust Verification Service (TVS) service.
6. Navigate to **Tools > Feature Services** from the Serviceability page, specify the node, and restart the TFTP service.
7. Once the services are restarted, reboot the phones so that they can retrieve the updated Identity Trust List (ITL) file.
8. Return to the Certificate Management page and delete the two old trust files. These are the two expired trust files that you received from the error output. The new certificates have a serial number that matches the **CAPF.pem** file.
9. Complete the previous steps for each subscriber.

IPSec

Internet Protocol Security (IPSec) certificates affect the Disaster Recovery Failure (DRF) master and local, which deals with backup and restore functions.

1. Navigate to the OS Administration page on the Publisher.
2. Navigate to **Security > Certificate Management** and click the **IPSEC.pem** file.

3. Click **Regenerate** in order to update the trust file.

4. Reboot the server that the certificate was regenerated on. This is required because every service must be restarted after any regeneration / update of any certificate. However, IPSec does not have a service restart ability other than to reboot the entire node. If other certificates need to be updated / regenerated, complete all the steps and then reboot the node after all the certificates have been processed through. This allows the server to have all the certificates updated in the truststore and read in properly.

CM

1. Navigate to the OS Administration page on the Publisher.

2. Navigate to the Certificate Management page, click **Find**, click the **CallManager.pem** file, and then click **Regenerate**.

3. Navigate to **Tools > Feature Service** on the Serviceability page, find the specified node, and restart the Cisco CM service.

4. From the Serviceability page, navigate to **Tools > Network Services**, and restart the TVS service.

5. From the Serviceability page, navigate to **Tools > Feature Services**, specify the node, and restart the CM and CTI services.

6. Reboot the phones so that they can retrieve the updated ITL file.

7. Complete the previous steps for each subscriber.

TVS

1. Navigate to the OS Administration page on the Publisher.

2. Navigate to **Security > Certificate Management**, click **Find**, click the **TVS.pem** file, and then click **Regenerate**.

3. From the Serviceability page, navigate to **Tools > Network Services**, and restart the TVS service.

4. From the Serviceability page, navigate to **Tools > Feature Services**, specify the node, and restart the TFTP service.

5. Reboot the phones so that they can retrieve the updated ITL file.

6. Complete the previous steps for each subscriber.

Delete Certificates

When you delete certificates, ensure that the previously mentioned services are stopped, and that the certificates you delete are not currently used or are actually expired.

Also, always check all of the information within the certificate, because you cannot save it after deletion.