Enhancement in Security Certificate Management CUCM 11.x

Contents

Introduction

This document describes the advancement made in certificate management for Cisco Unified Communications Manager (CUCM) implemented in version 11.x.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- CUCM

Components Used

The information in this document is based on these software versions:

- CUCM version 11.5.1.10000-6

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.

Background Information

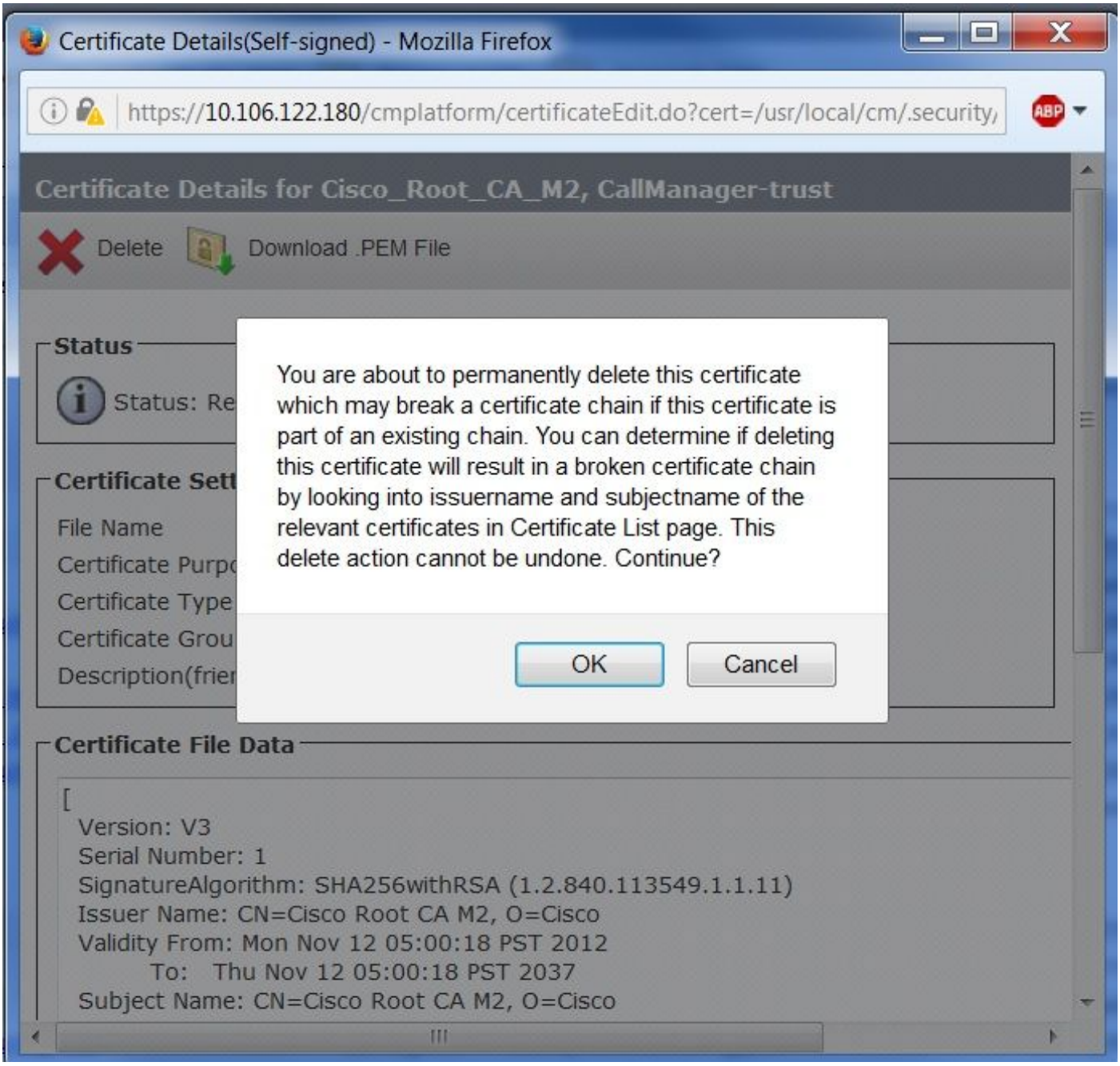
CUCM certificate management helps Unified Communications or security administrators take

advantagesmanage certificates more efficiently. Advantages of the enhancement made include a decreased time during removal of unwanted of expired certificates in CUCM and IM&Presence.

Certificate Management

Old Versions

Prior to CUCM version 11, this message appeared if a certificate is deleted.



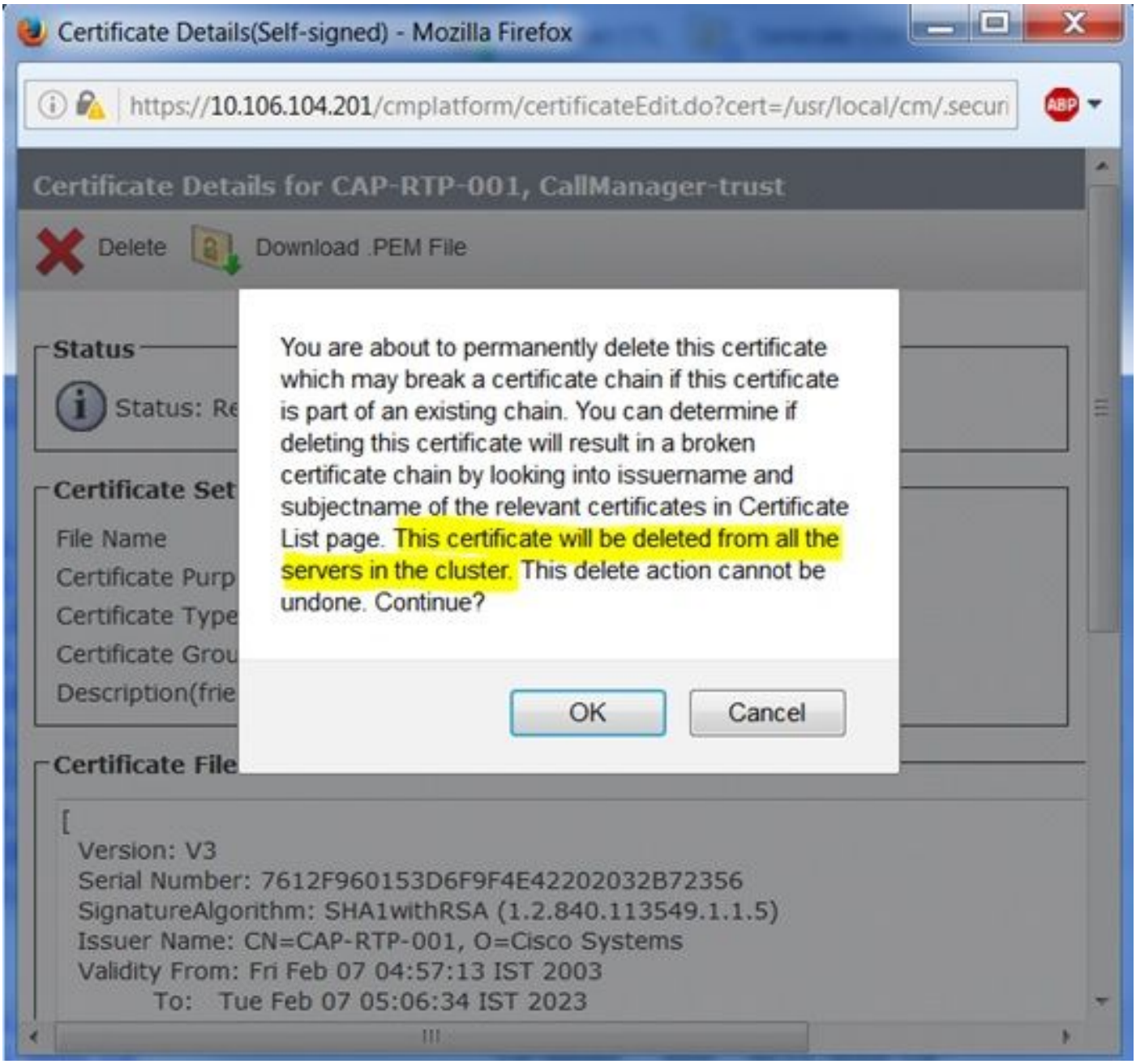
The certificate gets deleted only from the node on which the delete operation is initiated.

If the same certificate is not deleted in other nodes, the deleted certificate gets populated back in the node where it was initially deleted. This is due to the certificate monitoring service called Certificate Change Notification. As a best practice in older versions of CUCM, the Certificate Change Notification service is stopped on all the CUCM nodes before certificate deletion. Another drawback in older versions is the requirement to log in to the OS administration section of each

node in order to delete a single unwanted or expired certificate, which becomes tedious and time consuming especially for a big cluster.

New Versions

Starting at CUCM version 11.0 or higher, any unwanted or expired certificates that are deleted from the current node are also deleted from all other nodes within the cluster.



The enhancement was included to address these defects:

CSCto86463 - Deleted certificates reappear, unable to remove certificates from CUCM

CSCus28550 - Cert Management Enhancement to delete a certificate from all nodes

Frequently Asked Questions

Q. What are the type of certificates included in this enhancement?

A. For Cisco Unified Communications Manager:

- tomcat-trust
- CallManager-trust
- Phone-SAST-trust

For Cisco Unified Communications Manager IM & Presence:

- tomcat-trust

Q. What happens at the backend for this enhancement?

A. As soon as a certificate is deleted in any one of the CUCM nodes:

- Certificate is deleted from the local node
- Platform event triggers deletion of the same certificate to all other nodes.

Verifiy

Once a certificate is deleted via the OS Administration page in a node, log in to other nodes and check if the certificate is present or not. If a deleted certificate is not deleted from all the nodes, check the logs generated through the instance of certificate deletion.

- Syslogs
- IPT Platform CertMgr Logs

In a common working scenario, these are the expected logs.

Syslogs

Platform-event is seen in other nodes (other than the node where the certificate deletion was initiated). In this example, a tomcat-trust certificate named CUCMSUB1.pem was deleted from the publisher, diplaying this on the subscriber's syslog.

```
Aug  6 20:20:47 CUCMSUB1 user 6 ilog_impl: Received request for platform-event (--no-wait
platform-event-clusterwide-certificate-delete HOSTNAME=CUCM-PUB UNIT=tomcat-trust
NAME=CUCMSUB1.pem)
```

IPT Platform CertMgr Logs

In the CertMgr logs, the records confirm that the certificate is on queue for deletion from the database entries.

```
2016-08-06 21:22:06,151 INFO [main] - IN -- CertDBAction.java - deleteCertificateInDB(certInfo)
-

2016-08-06 21:22:06,151 INFO [main] -

DBParameters ...

PKID :                    null

CN :                       L=BGL,ST=Karnataka,CN=CUCMSUB1,OU=TAC,O=Cisco,C=IN

serialNo :              4d6dc0cb7bc73e70c3ded20690d15fa8
```

```
hostName :         CUCMSUB1

issuerName :      L=BGL,ST=Karnataka,CN=CUCMSUB1,OU=TAC,O=Cisco,C=IN

Certificate :         Not Printing huge Certificate String..

IPV4Address :     10.106.99.196

IPV6Address :

TimeToLive :       NULL

TkCertificateDistribution :1

UNIT :                  tomcat-trust

TYPE :                   trust-certs

ROLE :                  null

RoleMoniker :    null

RoleEnum :null

SERVICE :                           null

ServiceMoniker :               null

ServiceEnum :0

2016-08-06 21:22:06,151 INFO [main] - DB - Certifciate Store Plugin Handler is
:com.cisco.ccm.certmgmt.db.CertDBImpl

2016-08-06 21:22:06,156 INFO [main] - IN -- CertDBImpl.java - deleteCertificate(certInfo) –
```

SQL command triggered for deletion of the certificate can be seen in the CertMgr logs.

```
2016-08-06 21:22:08,980 DEBUG [main] - Delete query of CERTIFICATEPROCESSNODEMAP :DELETE FROM
CERTIFICATEPROCESSNODEMAP WHERE FKCERTIFICATE="cdd0365a-2d17-3483-4d00-1bf08f942cf5" AND
SERVERNAME = "CUCMSUB1"

2016-08-06 21:22:08,980 DEBUG [main] - execute(DELETE FROM CERTIFICATEPROCESSNODEMAP WHERE
FKCERTIFICATE="cdd0365a-2d17-3483-4d00-1bf08f942cf5" AND SERVERNAME = "CUCMSUB1")
```

From the CertMgr logs, the entries confirm that the certificate is deleted from the FILE-SYSTEM (certificate with pem or der extensions).

```
2016-08-06 21:22:09,009 DEBUG [main] - deleteDERandPEM: sCertDir =
/usr/local/platform/.security/tomcat/trust-certs --- sAlias = CUCMSUB1

2016-08-06 21:22:09,009 INFO [main] - IN -- TomcatCertMgr.java - removeFromKeyStore(..) -

2016-08-06 21:22:09,010 INFO [main] - IN -- RSACryptoEngine.java -
removeFromKeyStore(keystoreFile, keystorePass, alias) -

2016-08-06 21:22:09,010 INFO [main] - IN -- RSACryptoEngine.java - loadKeyStore(keystoreFile,
keystorePass) -

2016-08-06 21:22:09,086 INFO [main] - OUT -- RSACryptoEngine.java - loadKeyStore -

2016-08-06 21:22:09,103 DEBUG [main] - Removing certificate from keystore : CUCMSUB1
```

If certificate deletion is still not reflected to the rest of the nodes in a cluster or logs show errors, proceed to open a TAC case with the CUCM team.