Troubleshooting Certificate Expiry alert of Smart Call Home Certificate on Collaboration Products

Contents

Introduction

This document describes the solutions for Certificate Expiry alert of Verisign certificate(VeriSign_Class_3_Secure_Server_CA_-_G3.der) provided for Smart Call Home which is set to expire on Feb 2020 in the following Cisco Unified Collaboration Products that are covered in this document.

Cisco Unified Communications Manager (UCM)
Cisco Unified Communications Manager Session Management Edition
Cisco IM and Presence Service (CUPS)
Cisco Unity Connection
Cisco Finesse
Cisco SocialMiner
Cisco MediaSense
Cisco Unified Contact Center Express
Cisco Unified Intelligence Center (CUIC)
Cisco Virtualized Voice Browser
Cisco Prime License Manager

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

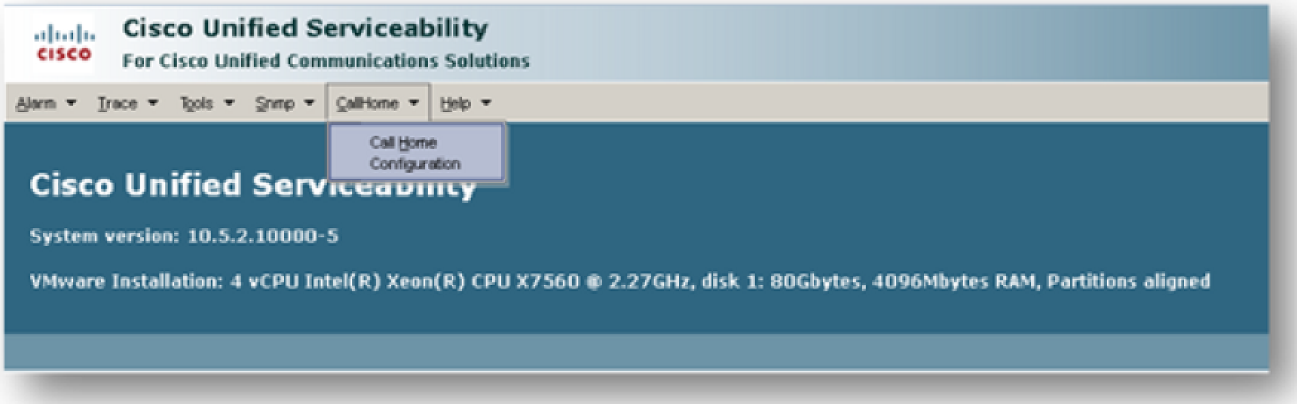
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Background Information

Smart Call Home is an automated support capability that monitors Cisco devices on your network. The Call Home feature allows you to communicate and send the diagnostic alerts, inventory, and other messages to the Smart Call Home backend server.

Use this section to verify if Smart Call Home is enabled

Step 1. From the Cisco Unified Serviceability page, choose CallHome > Configuration.

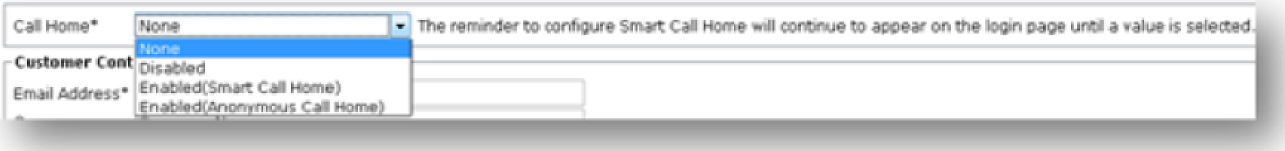

cisco
Cisco Unified Serviceability
For Cisco Unified Communications Solutions
Alarm
Trace
Tools
Snmp
CallHome
Help
Call Home
Configuration

Cisco Unified Serviceability

System version: 10.5.2.10000-5

VMware Installation: 4 vCPU Intel(R) Xeon(R) CPU X7560 @ 2.27GHz, disk 1: 80Gbytes, 4096Mbytes RAM, Partitions aligned

Step 2. Check if the Call Home field is set to Disabled or Enabled



Call Home* None

The reminder to configure Smart Call Home will continue to appear on the login page until a value is selected.

Customer Cont

Email Address*

Problem

The VeriSign certificate(VeriSign_Class_3_Secure_Server_CA_-_G3.der) provided by default as tomcat-trust certificate for Smart Call Home on Cisco Unified Collaboration Products is set to expire on Feb 2020. The following expiration alert may be seen below:

```
%UC_CERT-4-CertValidLessThanMonth: %[Message=Certificate expiration Notification.
Certificate name:VeriSign_Class_3_Secure_Server_CA_-_G3.der
Unit:tomcat-trust Type:own-cert ]
[AppID=Cisco Certificate Monitor][ClusterID=][NodeID=UCM-PUB.ciscolab.com]
```

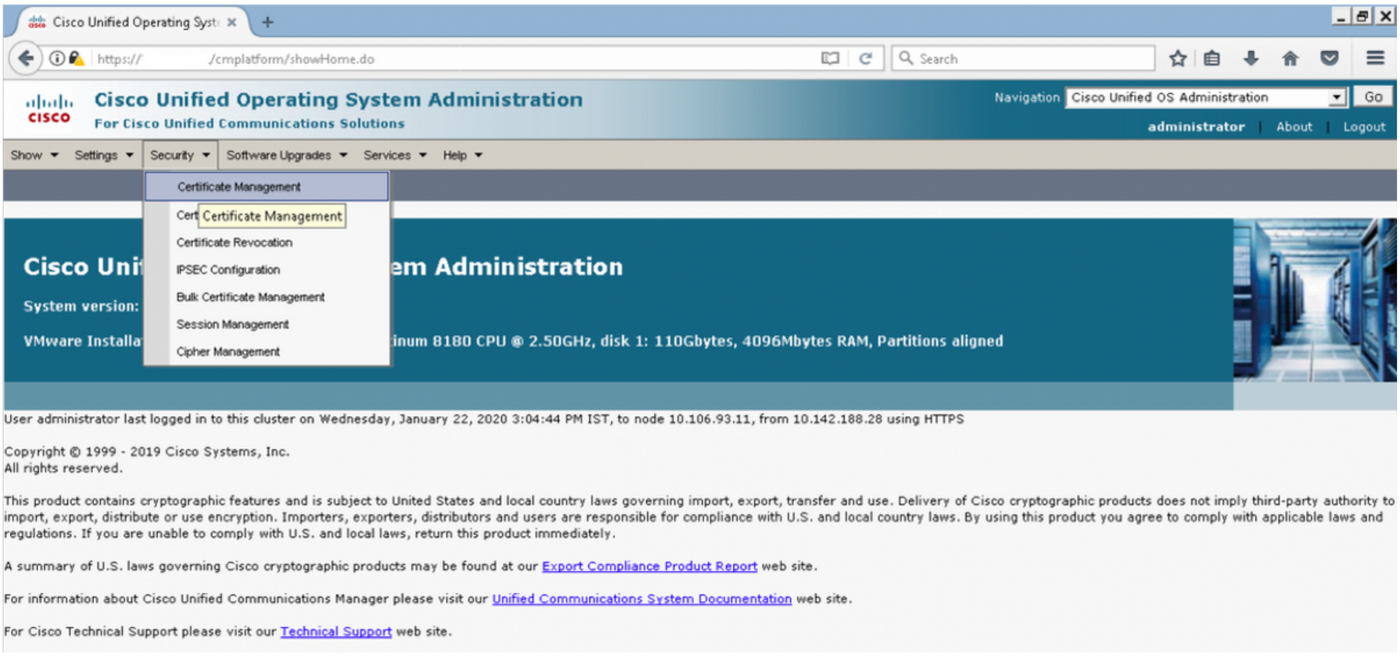
Solution

This issue is documented by Cisco bug ID CSCvs64158 .

Workaround for 11.0(1) and higher versions

We need to perform below steps to Delete the expired certificate (VeriSign_Class_3_Secure_Server_CA_-_G3.der)

Step 1. Browse to the Cisco Unified OS Administration GUI on the Publisher and Click on **Security** > **Certificate Management**


Cisco Unified Operating Syst
https:// /cmplatform/showHome.do
Search
Cisco Unified Operating System Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified OS Administration Go
administrator | About | Logout
Show Settings Security Software Upgrades Services Help
Certificate Management
Certificate Management
Certificate Revocation
IPSEC Configuration
Bulk Certificate Management
Session Management
Cipher Management
Cisco Uni em Administration
System version:
VMware Installa inum 8180 CPU @ 2.50GHz, disk 1: 110Gbytes, 4096Mbytes RAM, Partitions aligned

User administrator last logged in to this cluster on Wednesday, January 22, 2020 3:04:44 PM IST, to node 10.106.93.11, from 10.142.188.28 using HTTPS

Copyright © 1999 - 2019 Cisco Systems, Inc.
All rights reserved.

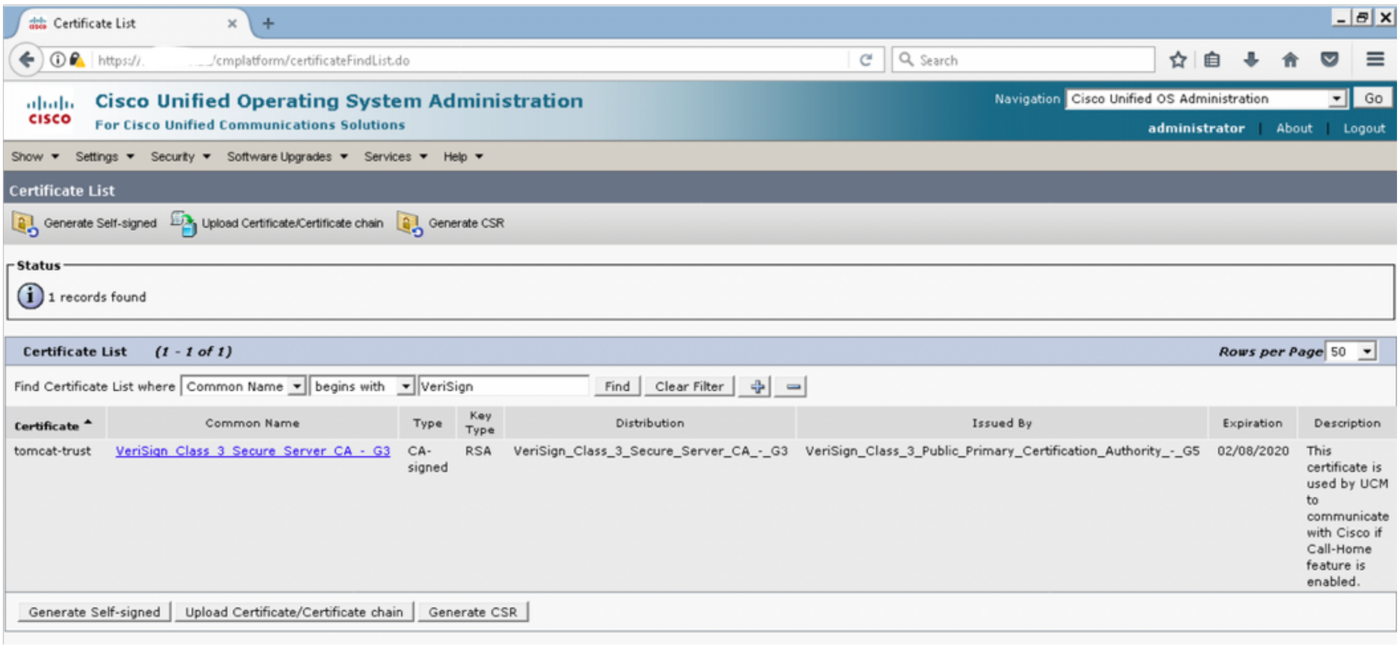
This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at our Export Compliance Product Report web site.

For information about Cisco Unified Communications Manager please visit our Unified Communications System Documentation web site.

For Cisco Technical Support please visit our Technical Support web site.

Step 2. Find Certificate List where Common Name contains VeriSign

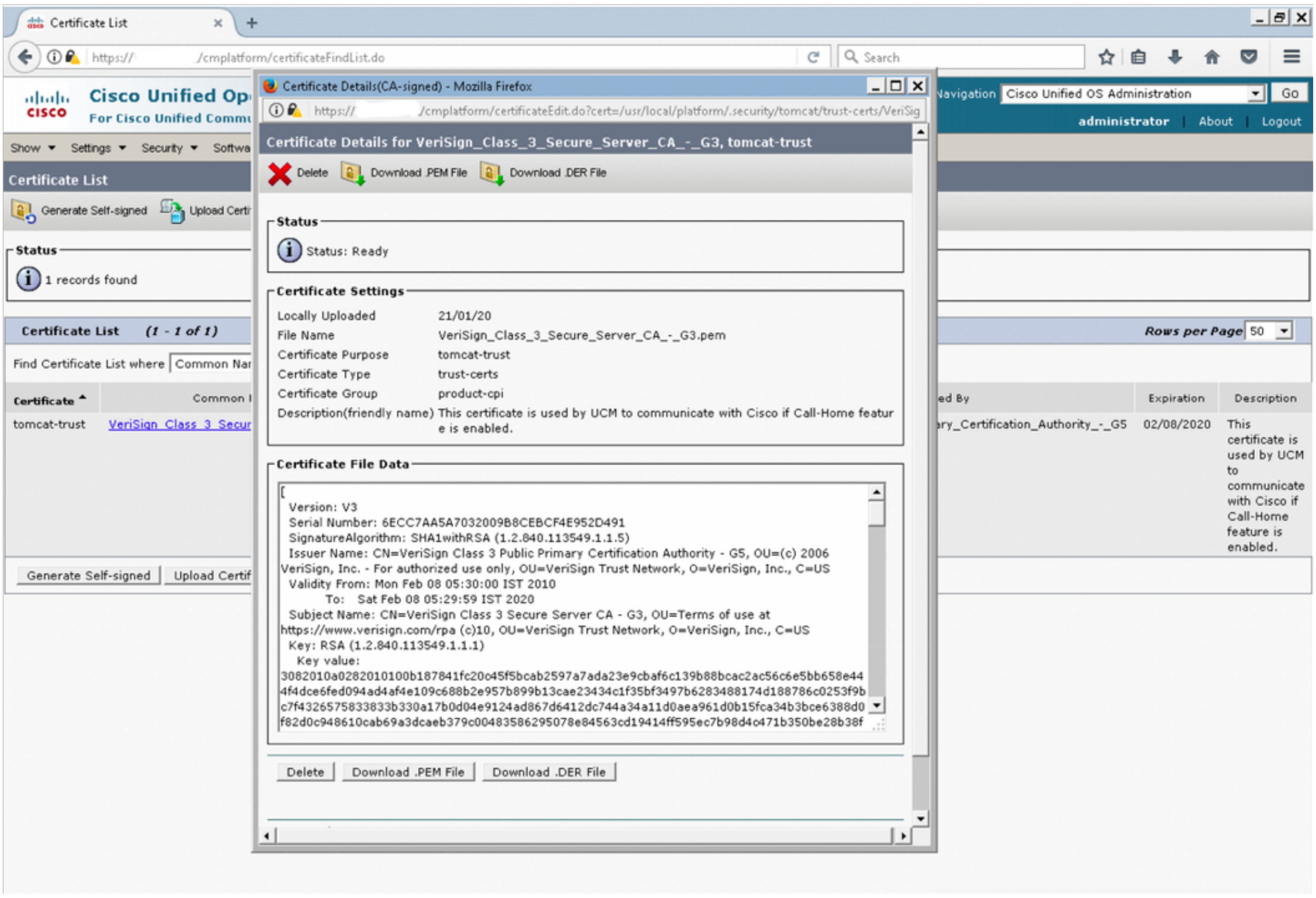

Certificate List
https:// /cmplatform/certificateFindList.do
Search
Cisco Unified Operating System Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified OS Administration Go
administrator | About | Logout
Show Settings Security Software Upgrades Services Help
Certificate List
Generate Self-signed
Upload Certificate/Certificate chain
Generate CSR
Status
Certificate List (1 - 1 of 1)
Rows per Page 50
Find
Clear Filter
Generate Self-signed
Upload Certificate/Certificate chain
Generate CSR

1 records found

Find Certificate List where Common Name begins with VeriSign

Certificate	Common Name	Type	Key Type	Distribution	Issued By	Expiration	Description
tomcat-trust	VeriSign_Class_3_Secure_Server_CA_-_G3	CA-signed	RSA	VeriSign_Class_3_Secure_Server_CA_-_G3	VeriSign_Class_3_Public_Primary_Certification_Authority_-_G5	02/08/2020	This certificate is used by UCM to communicate with Cisco if Call-Home feature is enabled.

Step 3. Click on **VeriSign_Class_3_Secure_Server_CA_-_G3** and you will see the pop-up window highlighting the details of the certificate


Certificate List
https:// /cmplatform/certificateFindList.do
Search
Cisco Unified Op
For Cisco Unified Commu
Navigation Cisco Unified OS Administration
Go
administrator | About | Logout
Show Settings Security Softwa
Certificate List
Generate Self-signed Upload Certi
Certificate Details(CA-signed) - Mozilla Firefox
https:// /cmplatform/certificateEdit.do?cert=/usr/local/platform/.security/tomcat/trust-certs/VeriSig
Delete
Download .PEM File
Download .DER File

Certificate Details for VeriSign_Class_3_Secure_Server_CA_-_G3, tomcat-trust

Status

Status: Ready

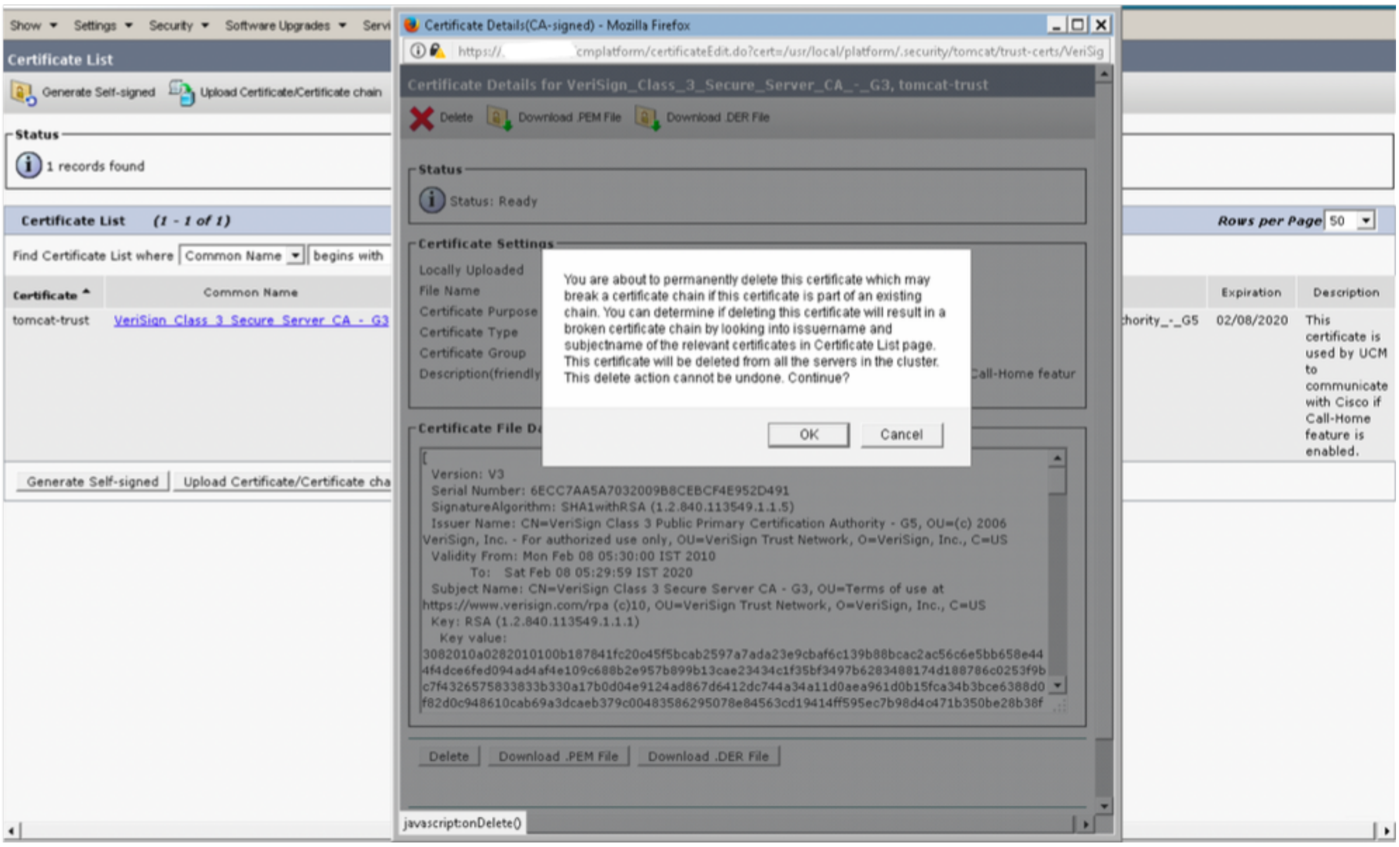
Certificate Settings

Locally Uploaded	21/01/20
File Name	VeriSign_Class_3_Secure_Server_CA_-_G3.pem
Certificate Purpose	tomcat-trust
Certificate Type	trust-certs
Certificate Group	product-cpi
Description(friendly name)	This certificate is used by UCM to communicate with Cisco if Call-Home featur e is enabled.

Certificate File Data

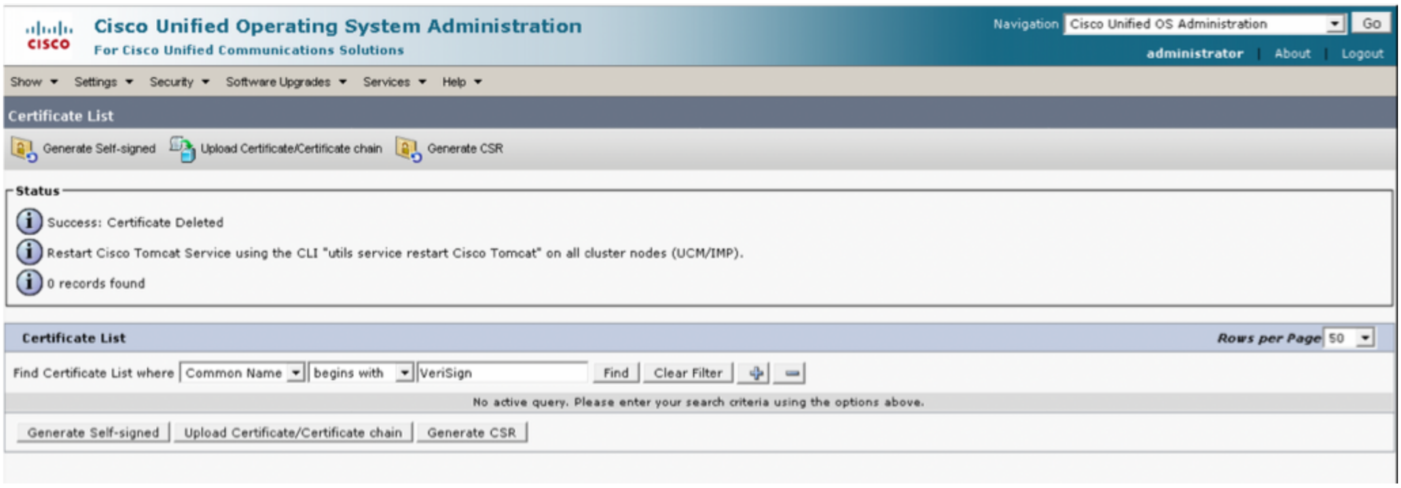
```
[
  Version: V3
  Serial Number: 6ECC7AA5A7032009B8CEBCF4E952D491
  SignatureAlgorithm: SHA1withRSA (1.2.840.113549.1.1.5)
  Issuer Name: CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU=(c) 2006
VeriSign, Inc. - For authorized use only, OU=VeriSign Trust Network, O=VeriSign, Inc., C=US
  Validity From: Mon Feb 08 05:30:00 IST 2010
           To:   Sat Feb 08 05:29:59 IST 2020
  Subject Name: CN=VeriSign Class 3 Secure Server CA - G3, OU=Terms of use at
https://www.verisign.com/rpa (c)10, OU=VeriSign Trust Network, O=VeriSign, Inc., C=US
  Key: RSA (1.2.840.113549.1.1.1)
    Key value:
3082010a0282010100b187841fc20c45f5bcab2597a7ada23e9cbaf6c139b88bcac2ac56c6e5bb658e44
4f4dce6fed094ad4af4e109c688b2e957b899b13cae23434c1f35bf3497b6283488174d188786c0253f9b
c7f4326575833833b330a17b0d04e9124ad867d6412dc744a34a11d0aea961d0b15fca34b3bce6388d0
f82d0c948610cab69a3dcaeb379c00483586295078e84563cd19414ff595ec7b98d4c471b350be28b38f
```

Step 4. Click on **Delete** button and warning prompted Click **OK**. The certificate should be deleted from all nodes in the cluster.



You are about to permanently delete this certificate which may break a certificate chain if this certificate is part of an existing chain. You can determine if deleting this certificate will result in a broken certificate chain by looking into issuername and subjectname of the relevant certificates in Certificate List page. This certificate will be deleted from all the servers in the cluster. This delete action cannot be undone. Continue?

OK
Cancel
Show Settings Security Software Upgrades Servi
Certificate List
Generate Self-signed Upload Certificate/Certificate chain
Status
1 records found
Certificate List (1 - 1 of 1)
Find Certificate List where Common Name begins with
Certificate
Common Name
tomcat-trust
VeriSign Class 3 Secure Server CA - G3
Generate Self-signed Upload Certificate/Certificate cha
Certificate Details(CA-signed) - Mozilla Firefox
https:// cmplatform/certificateEdit.do?cert=/usr/local/platform/.security/tomcat/trust-certs/VeriSig
Certificate Details for VeriSign_Class_3_Secure_Server_CA_-_G3, tomcat-trust
Delete
Download .PEM File
Download .DER File
Status: Ready
javascript:onDelete()
Rows per Page 50
Expiration
Description
thority_-_G5
02/08/2020
This certificate is used by UCM to communicate with Cisco if Call-Home feature is enabled.


Cisco Unified Operating System Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified OS Administration Go
administrator | About | Logout
Show Settings Security Software Upgrades Services Help
Certificate List
Generate Self-signed Upload Certificate/Certificate chain Generate CSR

Status

Success: Certificate Deleted

Restart Cisco Tomcat Service using the CLI "utils service restart Cisco Tomcat" on all cluster nodes (UCM/IMP).

0 records found

Certificate List — Rows per Page 50

Find Certificate List where Common Name begins with VeriSign Find Clear Filter

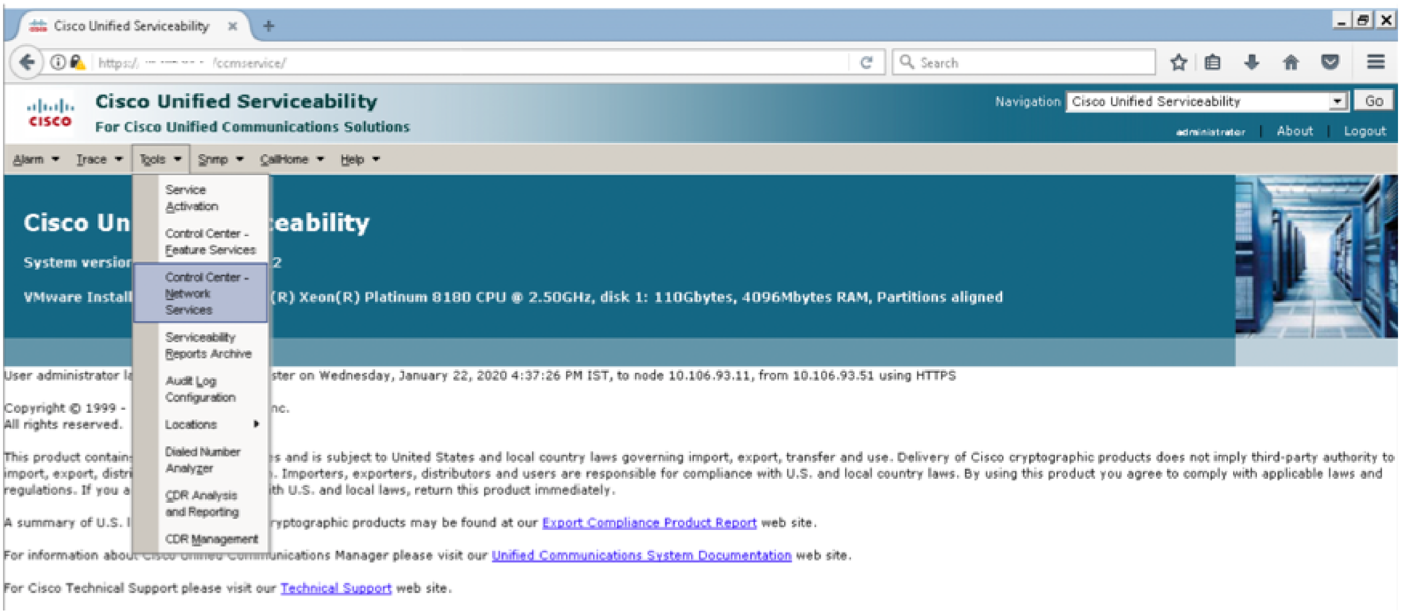
No active query. Please enter your search criteria using the options above.

Generate Self-signed | Upload Certificate/Certificate chain | Generate CSR

For all other versions

We need to perform below steps before we delete the certificate

Step 1. Navigate to **Cisco Unified Serviceability** > **Tools** > **Control Center - Network Services**


Cisco Unified Serviceability
https://. ··· ···· ··· · /ccmservice/
Search
Cisco Unified Serviceability
For Cisco Unified Communications Solutions
Navigation Cisco Unified Serviceability Go
administrator | About | Logout
Alarm Trace Tools Snmp CallHome Help
Service Activation
Control Center - Feature Services
Control Center - Network Services
Serviceability Reports Archive
Audit Log Configuration
Locations
Dialed Number Analyzer
CDR Analysis and Reporting
CDR Management
Cisco Un eability

System versio 2

VMware Install (R) Xeon(R) Platinum 8180 CPU @ 2.50GHz, disk 1: 110Gbytes, 4096Mbytes RAM, Partitions aligned

User administrator l ster on Wednesday, January 22, 2020 4:37:26 PM IST, to node 10.106.93.11, from 10.106.93.51 using HTTPS

Copyright © 1999 - nc.
All rights reserved.

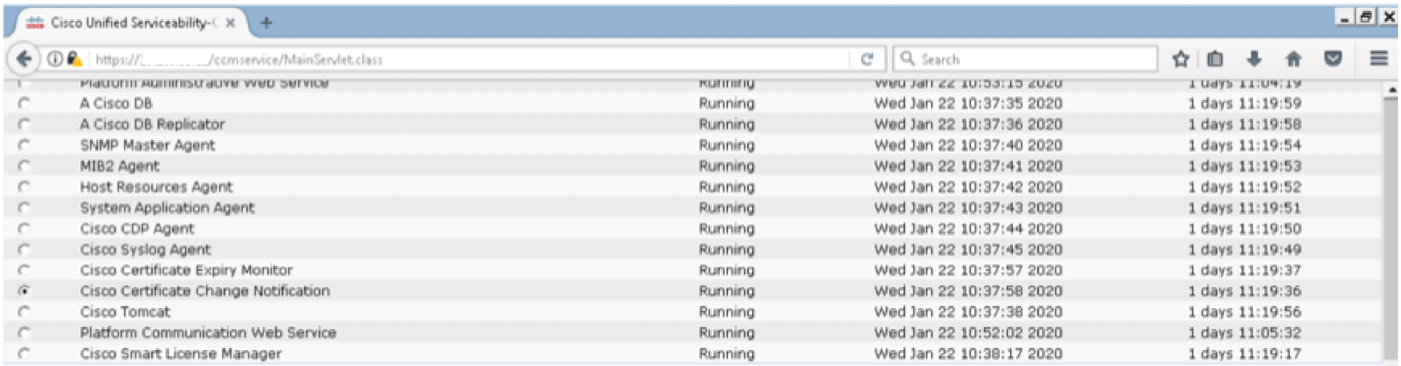
This product contain s and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distri . Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you a th U.S. and local laws, return this product immediately.

A summary of U.S. l ryptographic products may be found at our Export Compliance Product Report web site.

For information about Cisco Unified Communications Manager please visit our Unified Communications System Documentation web site.

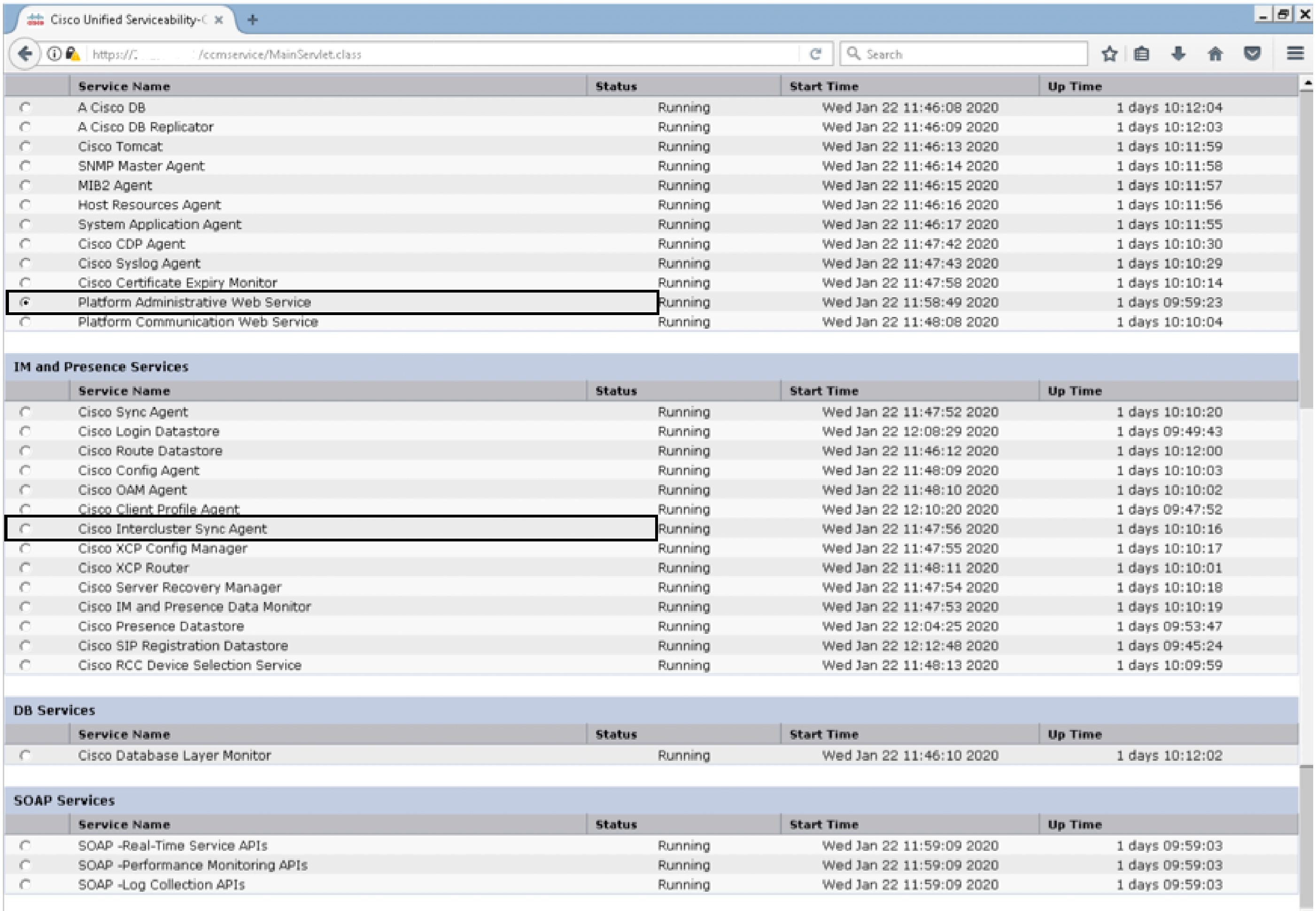
For Cisco Technical Support please visit our Technical Support web site.

Step 2. Stop **Cisco Certificate Change Notification** on all node in the cluster


Cisco Unified Serviceability-C
https://[...]/ccmservice/MainServlet.class
Search

○	Platform Administrative Web Service	Running	Wed Jan 22 10:53:15 2020	1 days 11:04:19
○	A Cisco DB	Running	Wed Jan 22 10:37:35 2020	1 days 11:19:59
○	A Cisco DB Replicator	Running	Wed Jan 22 10:37:36 2020	1 days 11:19:58
○	SNMP Master Agent	Running	Wed Jan 22 10:37:40 2020	1 days 11:19:54
○	MIB2 Agent	Running	Wed Jan 22 10:37:41 2020	1 days 11:19:53
○	Host Resources Agent	Running	Wed Jan 22 10:37:42 2020	1 days 11:19:52
○	System Application Agent	Running	Wed Jan 22 10:37:43 2020	1 days 11:19:51
○	Cisco CDP Agent	Running	Wed Jan 22 10:37:44 2020	1 days 11:19:50
○	Cisco Syslog Agent	Running	Wed Jan 22 10:37:45 2020	1 days 11:19:49
○	Cisco Certificate Expiry Monitor	Running	Wed Jan 22 10:37:57 2020	1 days 11:19:37
●	Cisco Certificate Change Notification	Running	Wed Jan 22 10:37:58 2020	1 days 11:19:36
○	Cisco Tomcat	Running	Wed Jan 22 10:37:38 2020	1 days 11:19:56
○	Platform Communication Web Service	Running	Wed Jan 22 10:52:02 2020	1 days 11:05:32
○	Cisco Smart License Manager	Running	Wed Jan 22 10:38:17 2020	1 days 11:19:17

Step 3. Incase of IM and Presence Server Stop **Platform Administration Web Services** and **Cisco Intercluster Sync Agent**



Cisco Unified Serviceability-C
https://.../ccmservice/MainServlet.class
Search

	Service Name	Status	Start Time	Up Time
○	A Cisco DB	Running	Wed Jan 22 11:46:08 2020	1 days 10:12:04
○	A Cisco DB Replicator	Running	Wed Jan 22 11:46:09 2020	1 days 10:12:03
○	Cisco Tomcat	Running	Wed Jan 22 11:46:13 2020	1 days 10:11:59
○	SNMP Master Agent	Running	Wed Jan 22 11:46:14 2020	1 days 10:11:58
○	MIB2 Agent	Running	Wed Jan 22 11:46:15 2020	1 days 10:11:57
○	Host Resources Agent	Running	Wed Jan 22 11:46:16 2020	1 days 10:11:56
○	System Application Agent	Running	Wed Jan 22 11:46:17 2020	1 days 10:11:55
○	Cisco CDP Agent	Running	Wed Jan 22 11:47:42 2020	1 days 10:10:30
○	Cisco Syslog Agent	Running	Wed Jan 22 11:47:43 2020	1 days 10:10:29
○	Cisco Certificate Expiry Monitor	Running	Wed Jan 22 11:47:58 2020	1 days 10:10:14
●	Platform Administrative Web Service	Running	Wed Jan 22 11:58:49 2020	1 days 09:59:23
○	Platform Communication Web Service	Running	Wed Jan 22 11:48:08 2020	1 days 10:10:04

IM and Presence Services

	Service Name	Status	Start Time	Up Time
○	Cisco Sync Agent	Running	Wed Jan 22 11:47:52 2020	1 days 10:10:20
○	Cisco Login Datastore	Running	Wed Jan 22 12:08:29 2020	1 days 09:49:43
○	Cisco Route Datastore	Running	Wed Jan 22 11:46:12 2020	1 days 10:12:00
○	Cisco Config Agent	Running	Wed Jan 22 11:48:09 2020	1 days 10:10:03
○	Cisco OAM Agent	Running	Wed Jan 22 11:48:10 2020	1 days 10:10:02
○	Cisco Client Profile Agent	Running	Wed Jan 22 12:10:20 2020	1 days 09:47:52
○	Cisco Intercluster Sync Agent	Running	Wed Jan 22 11:47:56 2020	1 days 10:10:16
○	Cisco XCP Config Manager	Running	Wed Jan 22 11:47:55 2020	1 days 10:10:17
○	Cisco XCP Router	Running	Wed Jan 22 11:48:11 2020	1 days 10:10:01
○	Cisco Server Recovery Manager	Running	Wed Jan 22 11:47:54 2020	1 days 10:10:18
○	Cisco IM and Presence Data Monitor	Running	Wed Jan 22 11:47:53 2020	1 days 10:10:19
○	Cisco Presence Datastore	Running	Wed Jan 22 12:04:25 2020	1 days 09:53:47
○	Cisco SIP Registration Datastore	Running	Wed Jan 22 12:12:48 2020	1 days 09:45:24
○	Cisco RCC Device Selection Service	Running	Wed Jan 22 11:48:13 2020	1 days 10:09:59

DB Services

	Service Name	Status	Start Time	Up Time
○	Cisco Database Layer Monitor	Running	Wed Jan 22 11:46:10 2020	1 days 10:12:02

SOAP Services

	Service Name	Status	Start Time	Up Time
○	SOAP -Real-Time Service APIs	Running	Wed Jan 22 11:59:09 2020	1 days 09:59:03
○	SOAP -Performance Monitoring APIs	Running	Wed Jan 22 11:59:09 2020	1 days 09:59:03
○	SOAP -Log Collection APIs	Running	Wed Jan 22 11:59:09 2020	1 days 09:59:03

Step 4. Delete the certificate on all the nodes including IM and Presence as described in Section *Workaround for 11.0(1) and higher* in this document

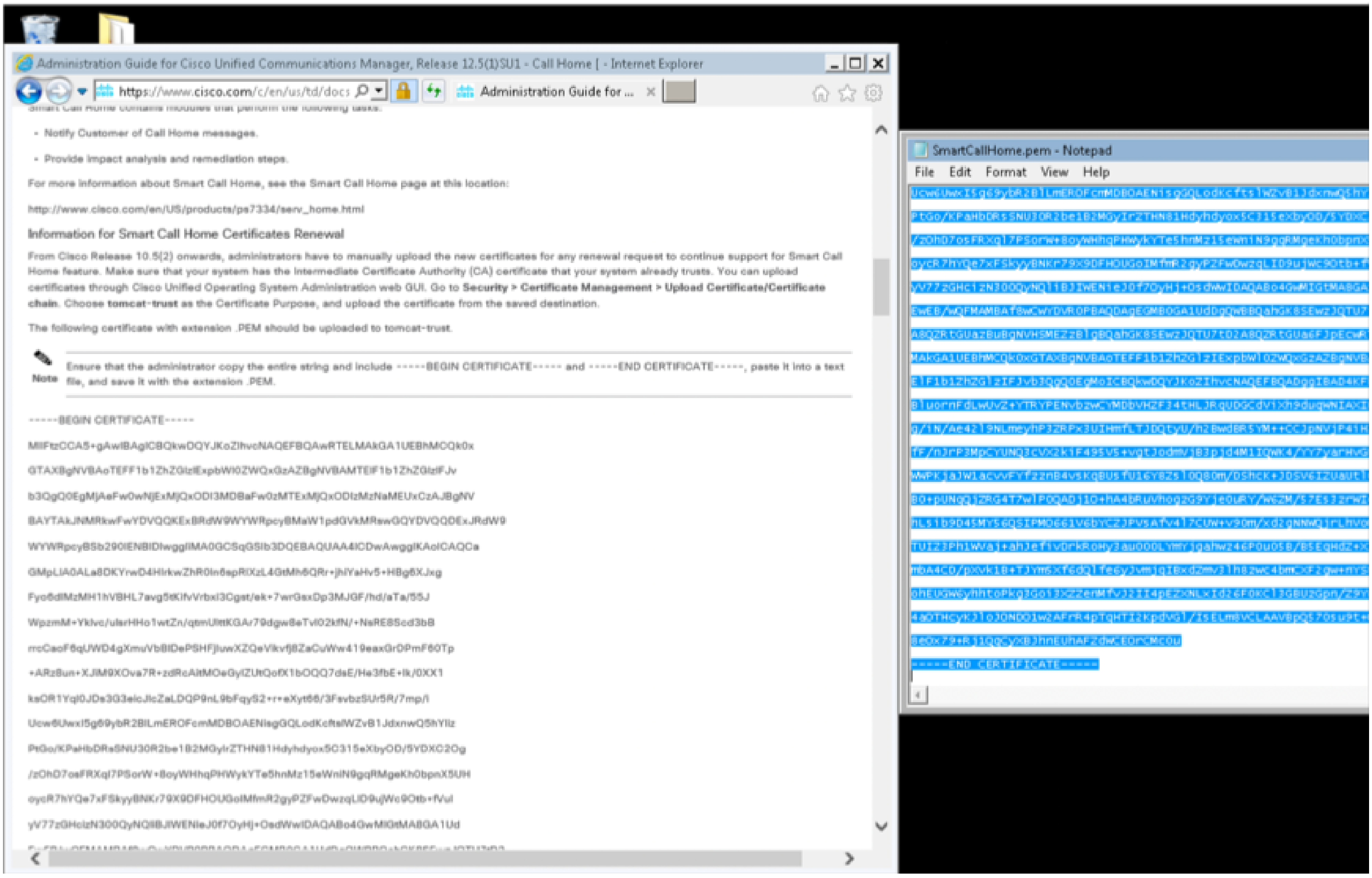
Step 5. Start the service which were stopped in Step 2. and Step 3.

> **Note**: If you delete the certificate and you do an upgrade prior to 7 Feb 2020, the certificate will reappear after the upgrade and which has to be removed again. Any upgrades after 7 Feb 2020 will not re-add the certificate

Smart Call Home Certificates Renewal Procedure

If Smart Call Home is disabled, no further action is required after deleting the certificate. If Smart Call Home is enabled, follow the steps

Step 1. Copy the certificate content from UCM Administration Guide Section *Information for Smart Call Home Certificates*



Administration Guide for Cisco Unified Communications Manager, Release 12.5(1)SU1 - Call Home [- Internet Explorer
https://www.cisco.com/c/en/us/td/docs
Administration Guide for ...
SmartCallHome.pem - Notepad
File Edit Format View Help

- Notify Customer of Call Home messages.
- Provide impact analysis and remediation steps.

For more information about Smart Call Home, see the Smart Call Home page at this location:

http://www.cisco.com/en/US/products/ps7334/serv_home.html

Information for Smart Call Home Certificates Renewal

From Cisco Release 10.5(2) onwards, administrators have to manually upload the new certificates for any renewal request to continue support for Smart Call Home feature. Make sure that your system has the Intermediate Certificate Authority (CA) certificate that your system already trusts. You can upload certificates through Cisco Unified Operating System Administration web GUI. Go to **Security > Certificate Management > Upload Certificate/Certificate chain**. Choose **tomcat-trust** as the Certificate Purpose, and upload the certificate from the saved destination.

The following certificate with extension .PEM should be uploaded to tomcat-trust.

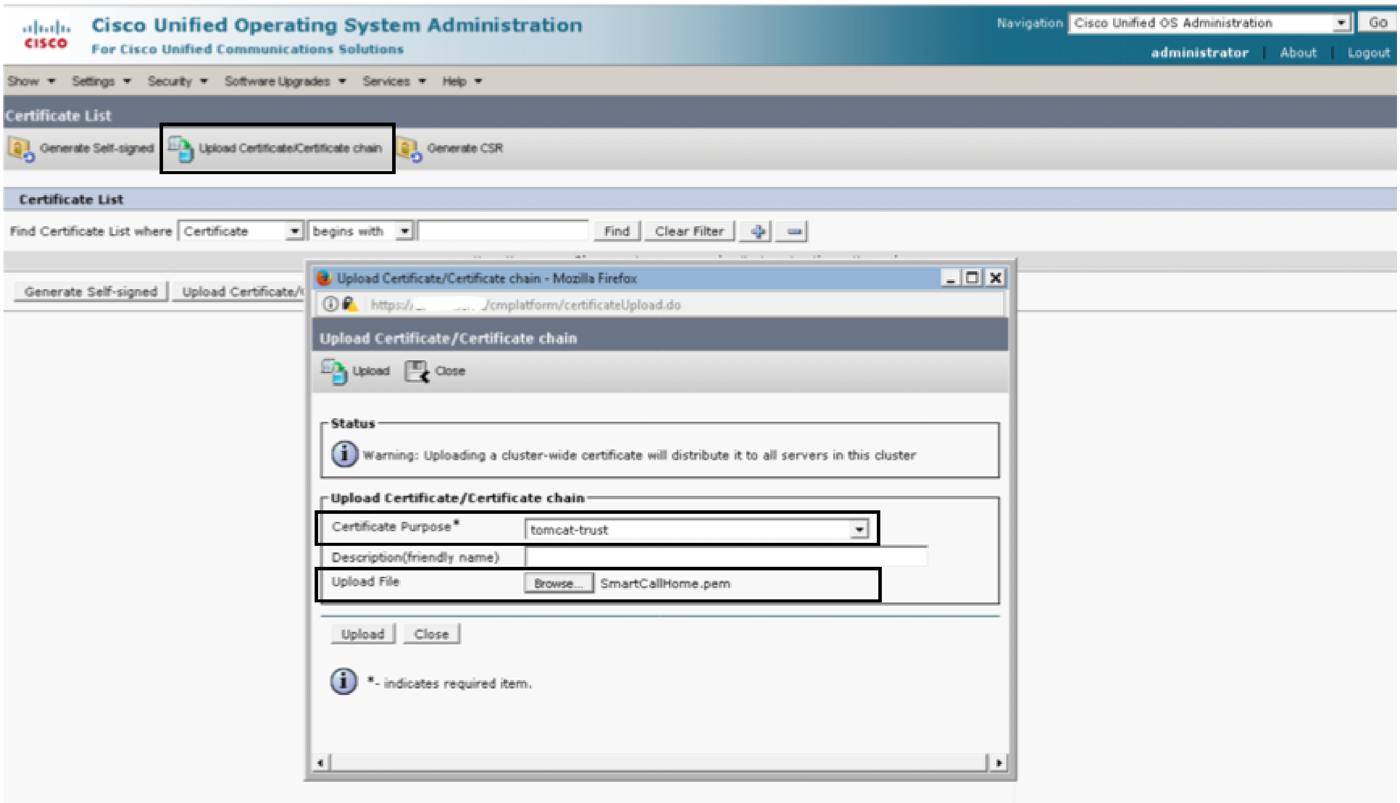
Note: Ensure that the administrator copy the entire string and include -----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----, paste it into a text file, and save it with the extension .PEM.

```
-----BEGIN CERTIFICATE-----
MIIFtzCCA5+gAwIBAgICBQkwDQYJKoZIhvcNAQEFBQAwRTELMAkGA1UEBhMCQk0x
GTAXBgNVBAoTEFF1b1ZhZGlzIExpbWl0ZWQxGzAZBgNVBAMTElF1b1ZhZGlzIFJv
b3QgQ0EgMjAeFw0wNjExMjQxODI3MDBaFw0zMTExMjQxODIzMzNaMEUxCzAJBgNV
BAYTAkJNMRkwFwYDVQQKExBRdW9WYWRpcyBMaW1pdGVkMRswGQYDVQQDExJRdW9
WYWRpcyBSb290IENBIDIwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCa
GMpLlA0ALa8DKYrwD4HIrkwZhR0In6spRIXzL4GtMh6QRr+jhiYaHv5+HBg6XJxg
Fyo6dIMzMH1hVBHL7avg5tKifvVrbxi3Cgst/ek+7wrGsxDp3MJGF/hd/aTa/55J
WpzmM+Yklvc/ulsrHHo1wtZn/qtmUIttKGAr79dgw8eTvI02kfN/+NsRE8Scd3bB
rrcCaoF6qUWD4gXmuVbBlDePSHFjIuwXZQeVikvfj8ZaCuWw419eaxGrDPmF60Tp
+ARz8un+XJiM9XOva7R+zdRcAitMOeGylZUtQofX1bOQQ7dsE/He3fbE+Ik/0XX1
ksOR1YqI0JDs3G3eicJlcZaLDQP9nL9bFqyS2+r+eXyt66/3FsvbzSUr5R/7mp/i
Ucw6UwxI5g69ybR2BlLmEROFcmMDBOAENisgGQLodKcftslWZvB1JdxnwQ5hYIiz
PtGo/KPaHbDRsSNU30R2be1B2MGyIrZTHN81Hdyhdyox5C315eXbyOD/5YDXC2Og
/zOhD7osFRXql7PSorW+8oyWHhqPHWykYTe5hnMz15eWniN9gqRMgeKh0bpnX5UH
oycR7hYQe7xFSkyyBNKr79X9DFHOUGoIMfmR2gyPZFwDwzqLID9ujWc9Otb+fVuI
yV77zGHcizN300QyNQliBJIWENieJ0f7OyHj+OsdWwIDAQABo4GwMIGtMA8GA1Ud
```

```
UcwGUwxI5g69ybR2BlLmEROFcmMDBOAENisgQQLodKcftslWZvB1JdxnwQ5hY
PtGo/KPaHbDRsSNU3OR2be1B2MGyIrZTHN81Hdyhdyox5C315eXbyOD/5YDXC
/zOhD7osFRXql7PSorW+8oyWHhqPHWykYTe5hnMz15ewn1N9ggRMgeKh0bpnX
oycR7hYQe7xFSkyyBNKr79X9DFHOUGoIMfmR2gyPZFwDwzqLID9ujWc9Otb+f
yV77zGHcizN300QyNQlIBJIWENieJ0f7OyHj+OsdWwIDAQABo4GwMIGtMA8GA
EwEB/wQFMAMBAf8wCwYDVR0PBAQDAgEGMB0GA1UdDgQWBBQahGK8SEwzJQTU7
A8QZRtGUazBuBgNVHSMEZzBlgBQahGK8SEwzJQTU7tO2A8QZRtGUa6FJpEcwR
MAkGA1UEBhMCQk0xGTAXBgNVBAoTEFF1b1ZhZGlzIExpbWl0ZWQxGzAZBgNVB
ElF1b1ZhZGlzIFJvb3QgQ0EgMoICBQkwDQYJKoZIhvcNAQEFBQADggIBAD4KF
BluornFdLwUvZ+YTRYPENvbzwCYMDbVHZF34tHLJRqUDGCdViXh9duqWNIAXI
g/iN/Ae42l9NLmeyhP3ZRPx3UIHmfLTJDQtyU/h2BwdBR5YM++CCJpNVjP4iH
fF/nJrP3MpCYUNQ3cVX2kiF495V5+vgtJodmVjB3pjd4M1IQWK4/YY7yarHvG
WwPKjaJWlacvvFYfzznB4vsKqBUsfU16Y8Zsl0Q80m/DShcK+J0SV6IZUaUtl
8O+pUNgqjzRG4T7wlP0QADj1O+hA4bRuVhogzG9Yje0uRY/W6ZM/57Es3zrWI
nLs1b9D45MY56QSIPMO661V6bYCZJPVsAfv4l7CUW+v90m/xd2gNNWQjrLhVo
TUIz3Ph1WVaj+ahJefivDrkRoHy3au000LYmYjgahwz46P0u05B/B5EQHdZ+X
mbA4CD/pXvk1B+TJYm5Xf6dQlfe6yJvmjqIBxdZmv3lh8zwc4bmCXF2gw+nYS
ohEUGW6yhhtoPkg3Go13XZzenMfvJ2lI4pEZXNLxId26F0KCl3GBUzGpn/Z9Y
4aOTHcyKJloJONDO1w2AFrR4pTqHTI2KpdVGl/IsELm8VCLAAVBpQ570su9t+
8eOx79+Rj1QqCyXBJhnEUhAFZdWCEOrCMc0u
-----END CERTIFICATE-----
```

Note: Same certificate is valid for 10.5 and higher version

Step 2. Upload the .pem file as tomcat-trust in Cisco Unified OS Administration GUI **Certificate Management** Page per the screenshot



Cisco Unified Operating System Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified OS Administration
Go
administrator
About
Logout
Show
Settings
Security
Software Upgrades
Services
Help
Certificate List
Generate Self-signed
Upload Certificate/Certificate chain
Generate CSR
Certificate List
Find
Clear Filter
Generate Self-signed
Upload Certificate/
Upload Certificate/Certificate chain - Mozilla Firefox
Upload Certificate/Certificate chain
Upload
Close
Upload
Close

Find Certificate List where Certificate begins with

https://[redacted]/cmplatform/certificateUpload.do

Status

Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster

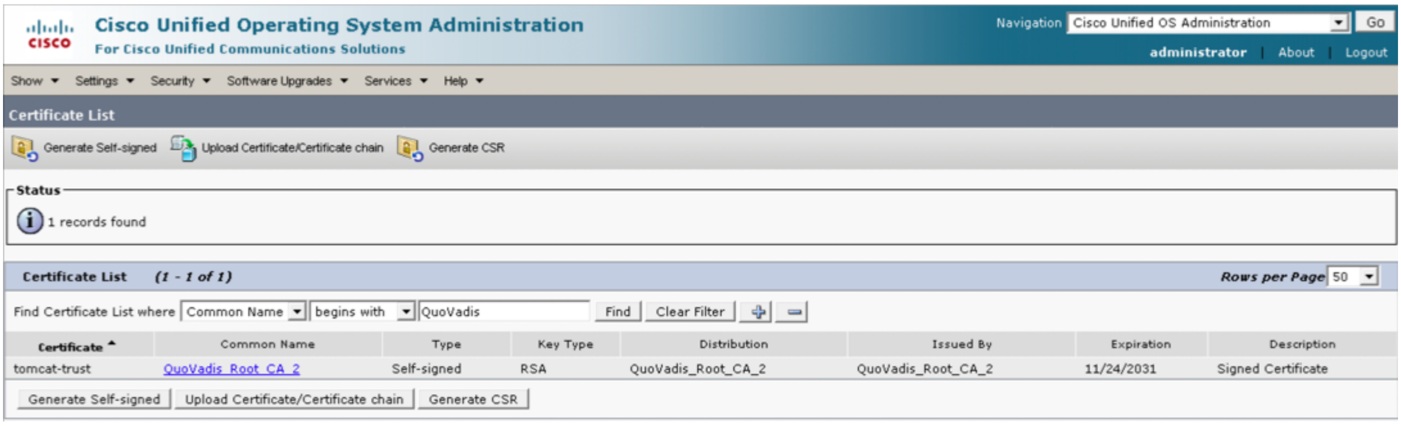
Upload Certificate/Certificate chain

Certificate Purpose*	tomcat-trust
Description(friendly name)	
Upload File	Browse... SmartCallHome.pem

*- indicates required item.

Step 3. Verify **QuoVadis_Root_CA_2** is listed as tomcat-trust by finding Certificate where

Common Name contains QuoVadis



Navigation: Cisco Unified OS Administration

Status

1 records found

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

Find Certificate List where Common Name begins with QuoVadis

Certificate	Common Name	Type	Key Type	Distribution	Issued By	Expiration	Description
tomcat-trust	QuoVadis_Root_CA_2	Self-signed	RSA	QuoVadis_Root_CA_2	QuoVadis_Root_CA_2	11/24/2031	Signed Certificate

For Cisco Prime License Manager

For Prime License Manager 10.5

The expired certificate (VeriSign_Class_3_Secure_Server_CA_-_G3) can be deleted from system by applying this COP file (ciscocm.plm-CSCvs64158_remove_sch_cert_C0050-1.k3.cop.sgn). Please review the Readme file for installation instructions.

For Prime License Manager 11.5

The expired certificate (VeriSign_Class_3_Secure_Server_CA_-_G3) can be deleted from system by applying this COP file (ciscocm.plm-CSCvs64158_remove_sch_cert_C0050-1.k3.cop.sgn). Please review the Readme file for installation instructions.