Alerte d'expiration du certificat de dépannage du certificat Smart Call Home sur les produits de collaboration

Contenu

Introduction

Ce document décrit les solutions pour l'alerte d'expiration de certificat du certificat Verisign (VeriSign_Class_3_Secure_Server_CA_-_G3.der) fournies pour Smart Call Home, qui expirera le 20 février 2020 dans les produits de collaboration unifiée Cisco suivants couverts dans ce 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)
Navigateur vocal virtualisé Cisco
Gestionnaire de licences Cisco Prime

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

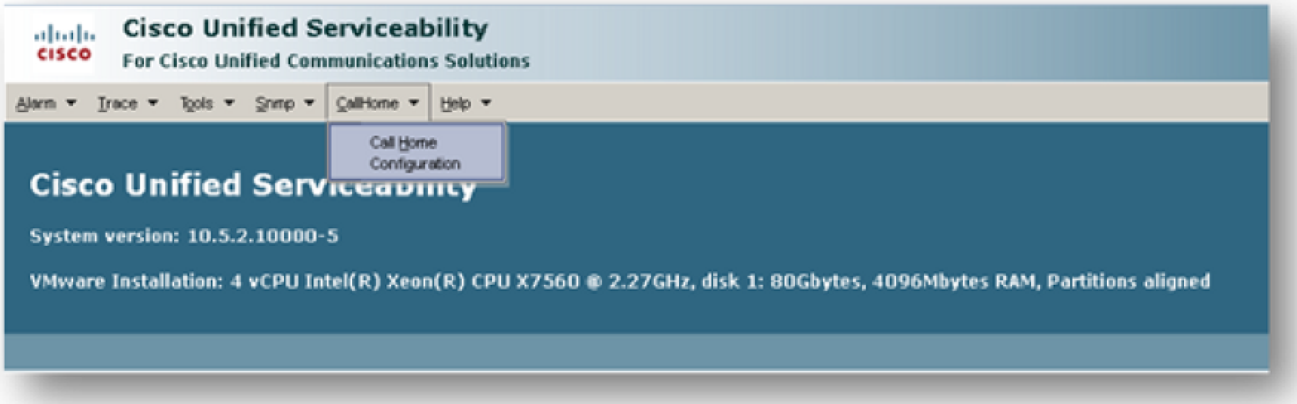
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informations générales

Smart Call Home est une fonctionnalité d'assistance automatisée qui surveille les périphériques Cisco sur votre réseau. La fonction Call Home vous permet de communiquer et d'envoyer les alertes de diagnostic, l'inventaire et d'autres messages au serveur principal Smart Call Home.

Utilisez cette section pour vérifier si Smart Call Home est activé

Étape 1. Sur la page Cisco Unified Serviceability, sélectionnez CallHome > Configuration.



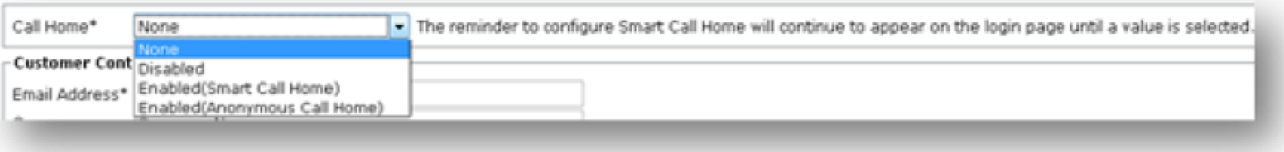
Cisco Unified Serviceability
For Cisco Unified Communications Solutions

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

Étape 2. Vérifier si le champ Call Home est défini sur Disabled ou 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*

Problème

Le certificat VeriSign (VeriSign_Class_3_Secure_Server_CA_-_G3.der) fourni par défaut en tant que certificat tomcat-trust pour Smart Call Home sur les produits Cisco Unified Collaboration expirera le 20 février 2020. L'alerte d'expiration suivante peut être vue ci-dessous :

```
%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]
```

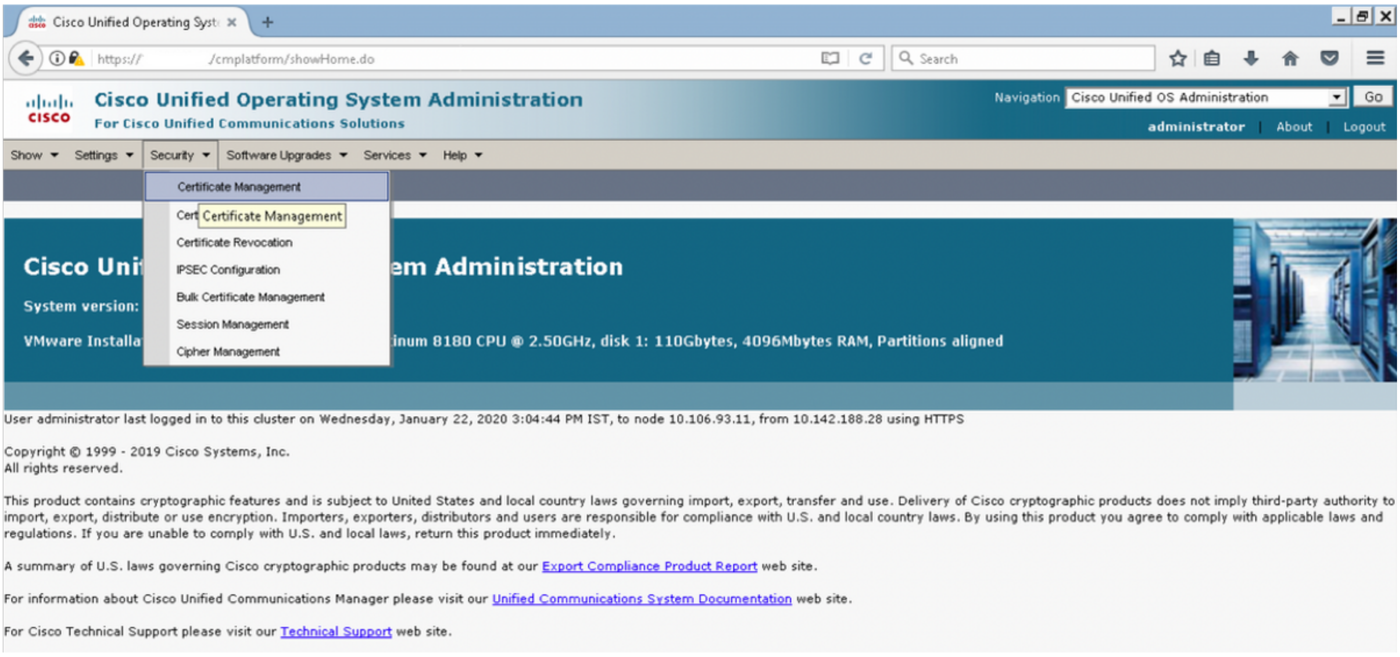
Solution

Ce problème est documenté par l'ID de bogue Cisco CSCvs64158 .

Solution pour les versions 11.0(1) et ultérieures

Nous devons effectuer les étapes suivantes pour supprimer le certificat expiré (VeriSign_Class_3_Secure_Server_CA_-_G3.der)

Étape 1. Accédez à l'interface utilisateur graphique de Cisco Unified OS Administration sur le serveur de publication et cliquez sur **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.

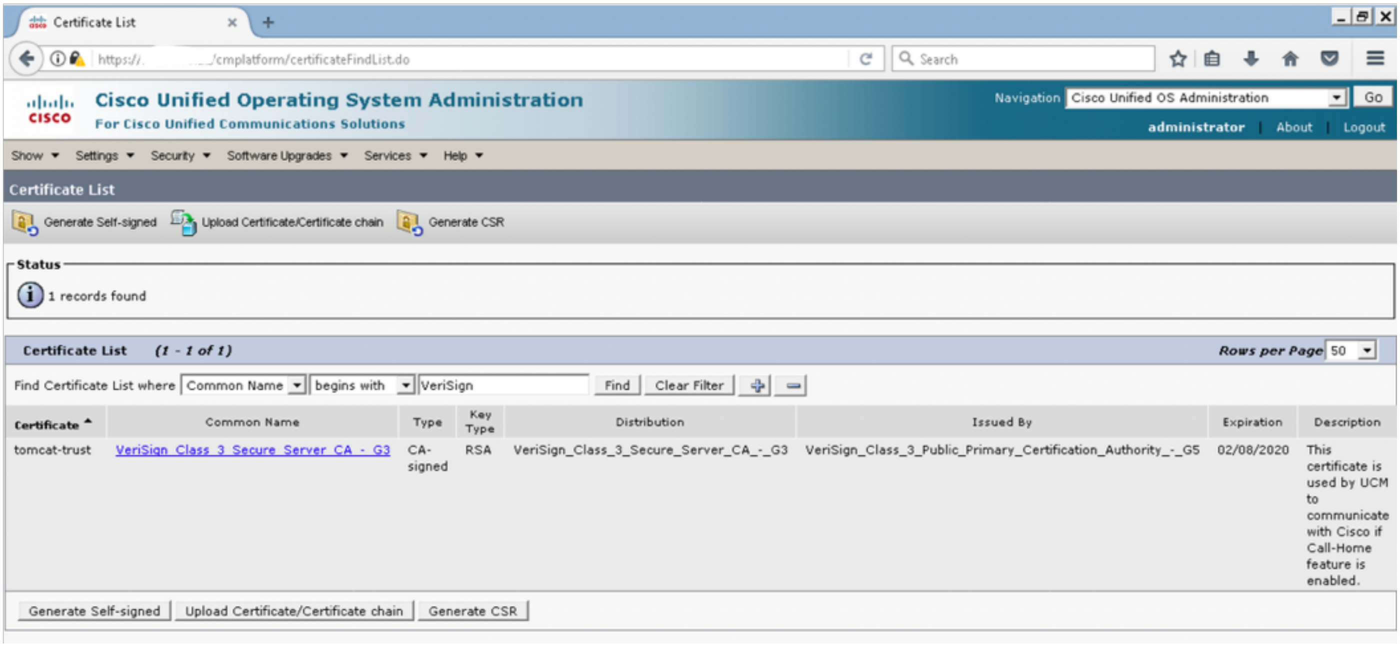
This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors 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.

Étape 2. Rechercher une liste de certificats dans laquelle le nom commun contient 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

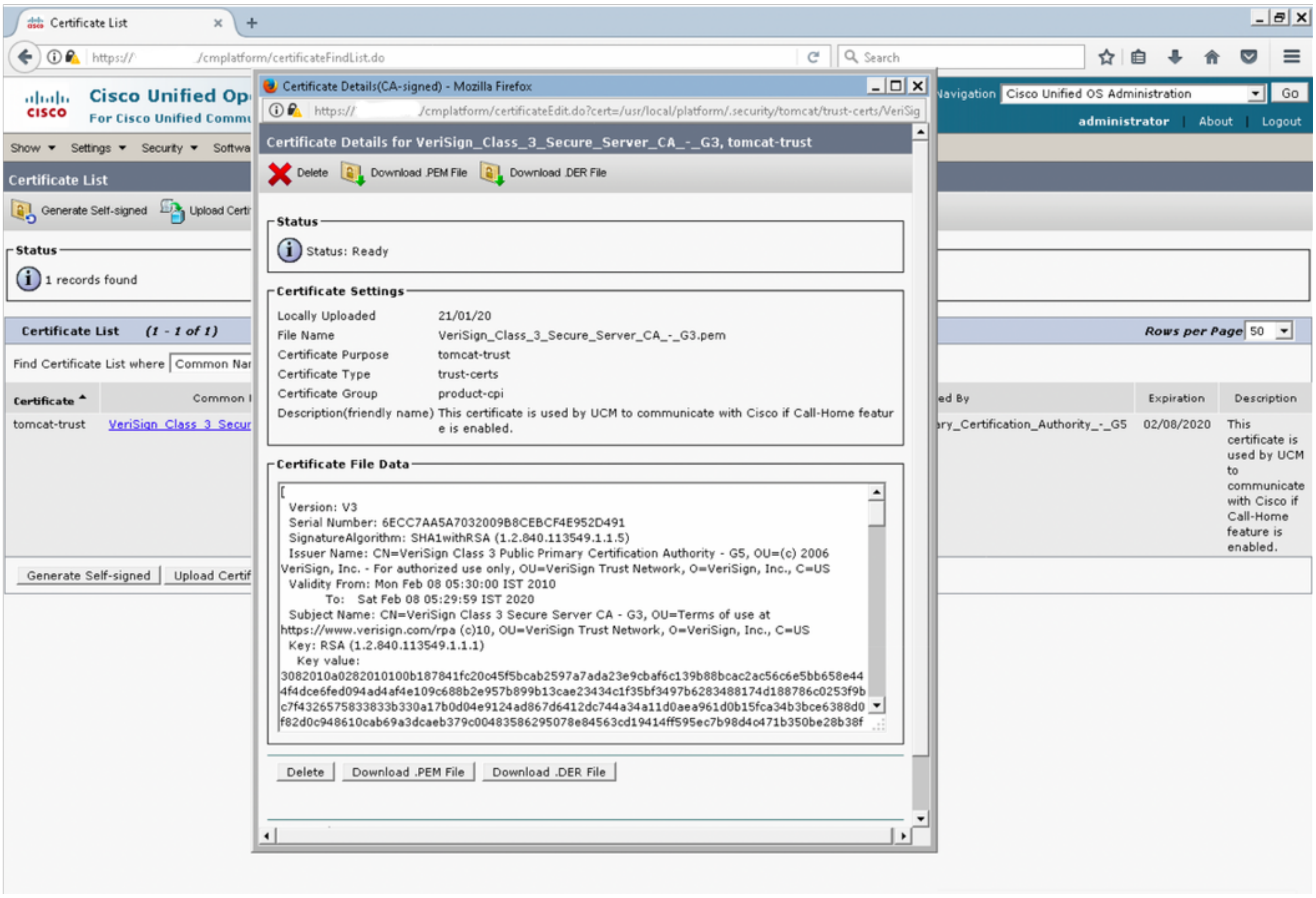
1 records found

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

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

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.

Étape 3. Cliquez sur **VeriSign_Class_3_Secure_Server_CA_-_G3** et la fenêtre contextuelle affichera les détails du certificat



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
Status
1 records found
Certificate List (1 - 1 of 1)
Rows per Page 50
Find Certificate List where Common Nar
Certificate
Common I
ed By
Expiration
Description
tomcat-trust
VeriSign_Class_3_Secur
ry_Certification_Authority_-_G5
02/08/2020
This certificate is used by UCM to communicate with Cisco if Call-Home feature is enabled.
Generate Self-signed
Upload Certif
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

Status: Ready

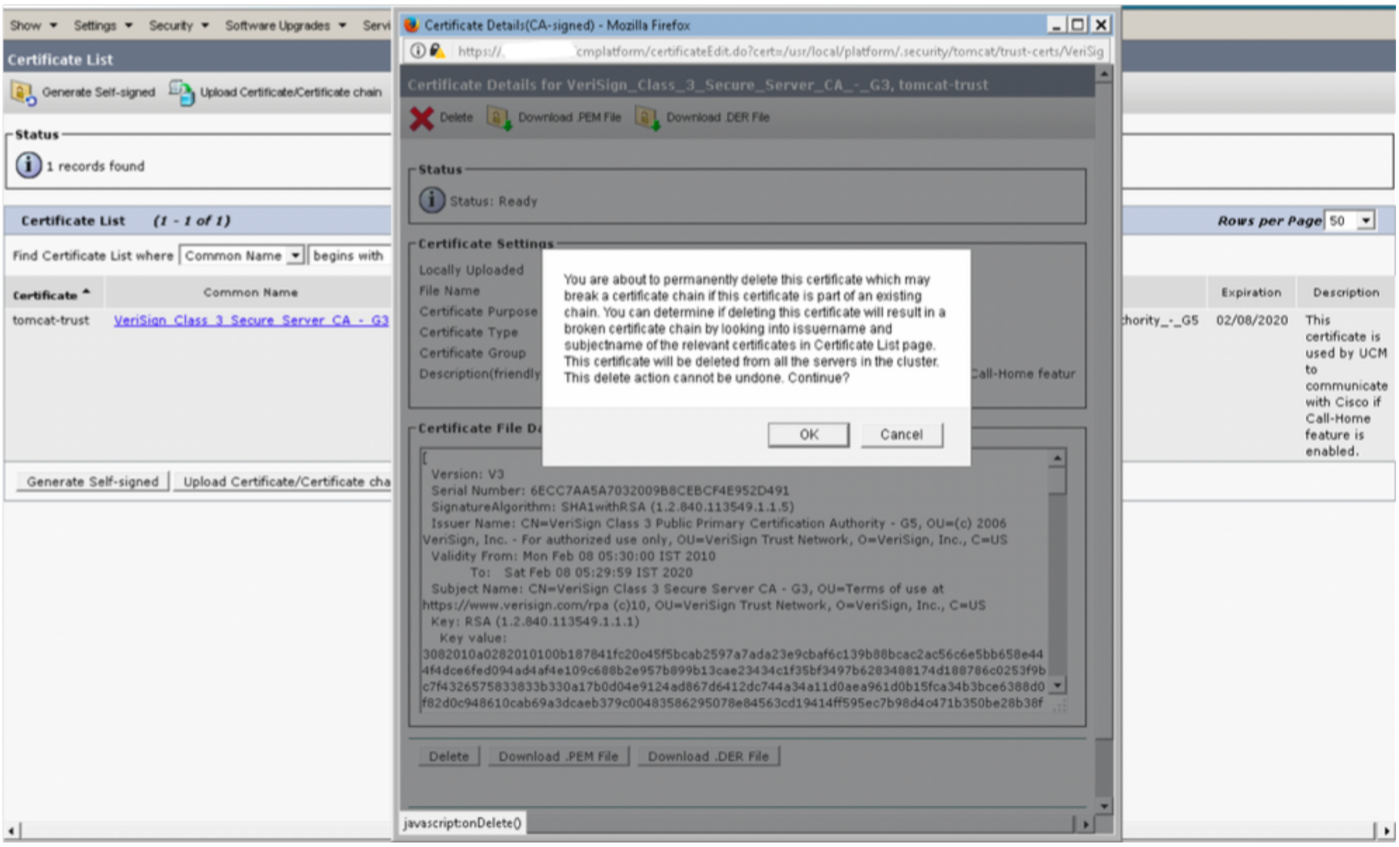
Certificate Settings

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 feature 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
```

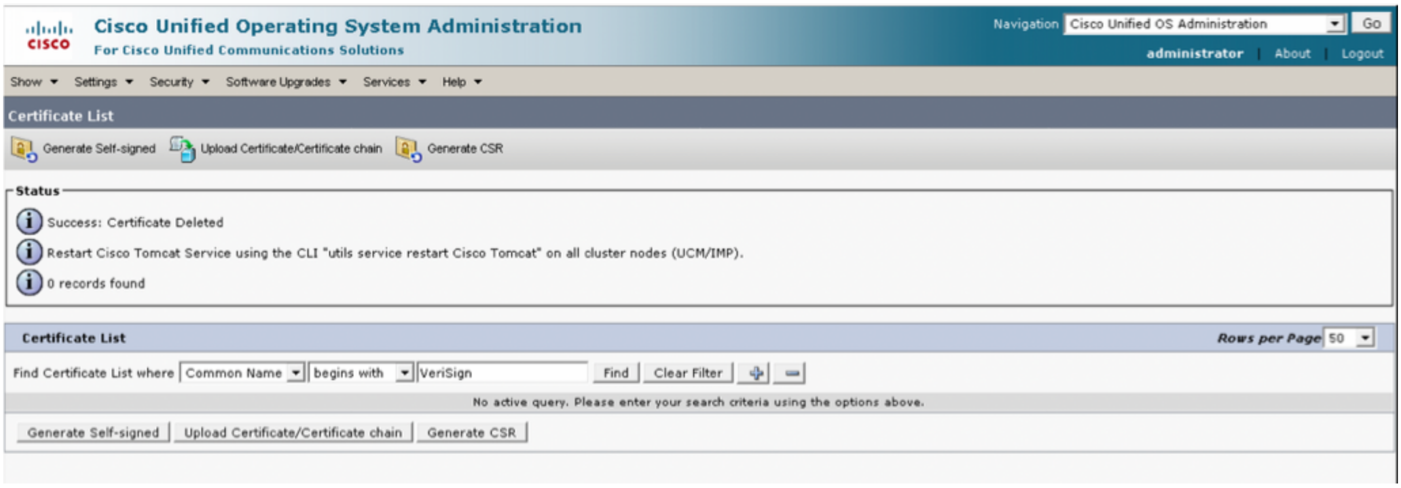
Étape 4. Cliquez sur le bouton **Supprimer** et un avertissement vous invite à cliquer sur **OK**. Le certificat doit être supprimé de tous les noeuds du cluster.



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)
Rows per Page 50
Find Certificate List where Common Name begins with
Certificate
Common Name
Expiration
Description
tomcat-trust
VeriSign_Class_3_Secure_Server_CA_-_G3
hority_-_G5
02/08/2020
This certificate is used by UCM to communicate with Cisco if Call-Home feature is enabled.
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
Status: Ready
Certificate Settings
Locally Uploaded
File Name
Certificate Purpose
Certificate Type
Certificate Group
Description(friendly
Call-Home featur
Certificate File D

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?

```
[
  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
```


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
Generate Self-signed
Upload Certificate/Certificate chain
Generate CSR

Certificate List

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

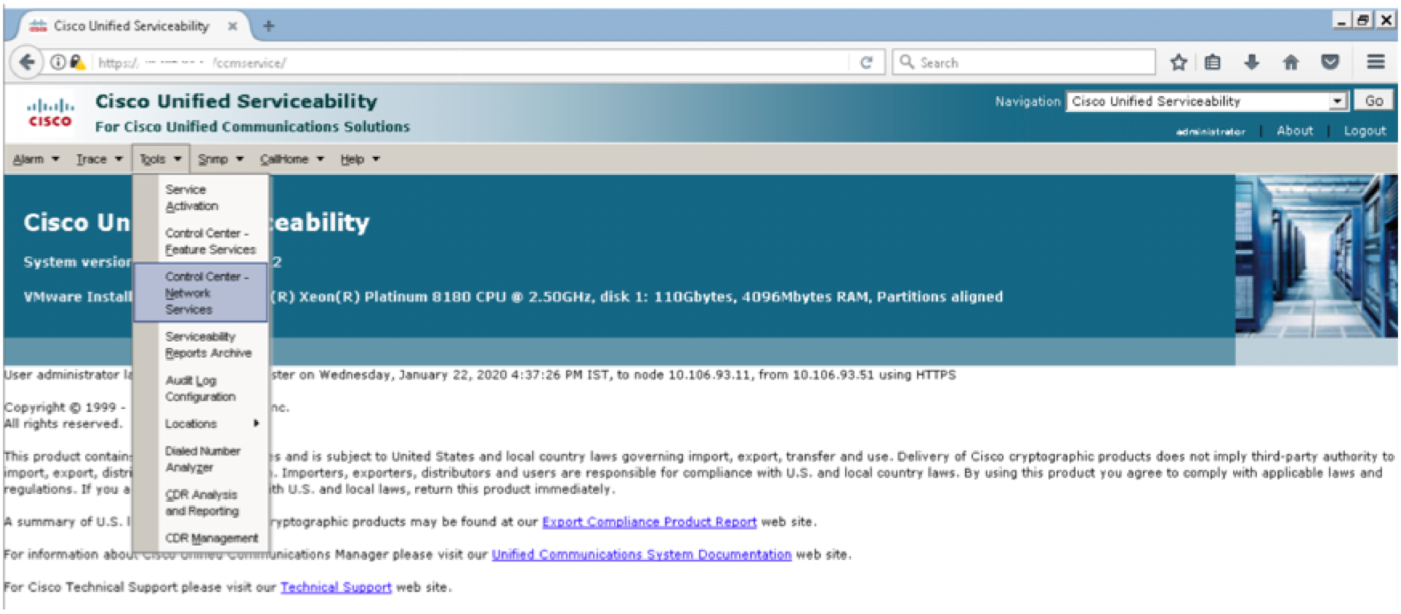
Find Certificate List where Common Name begins with VeriSign Find Clear Filter

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

Pour toutes les autres versions

Nous devons effectuer les étapes suivantes avant de supprimer le certificat

Étape 1. Accédez à **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 versior 2

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

User administrator la 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.

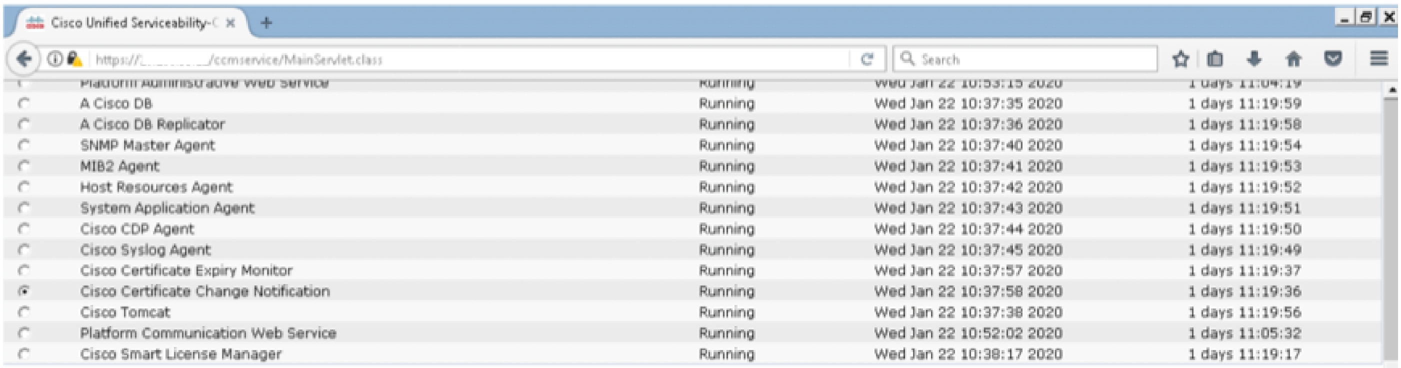
This product contain s and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distri . Importers, exporters, distributors and users are responsible for compliance 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 nunications Manager please visit our Unified Communications System Documentation web site.

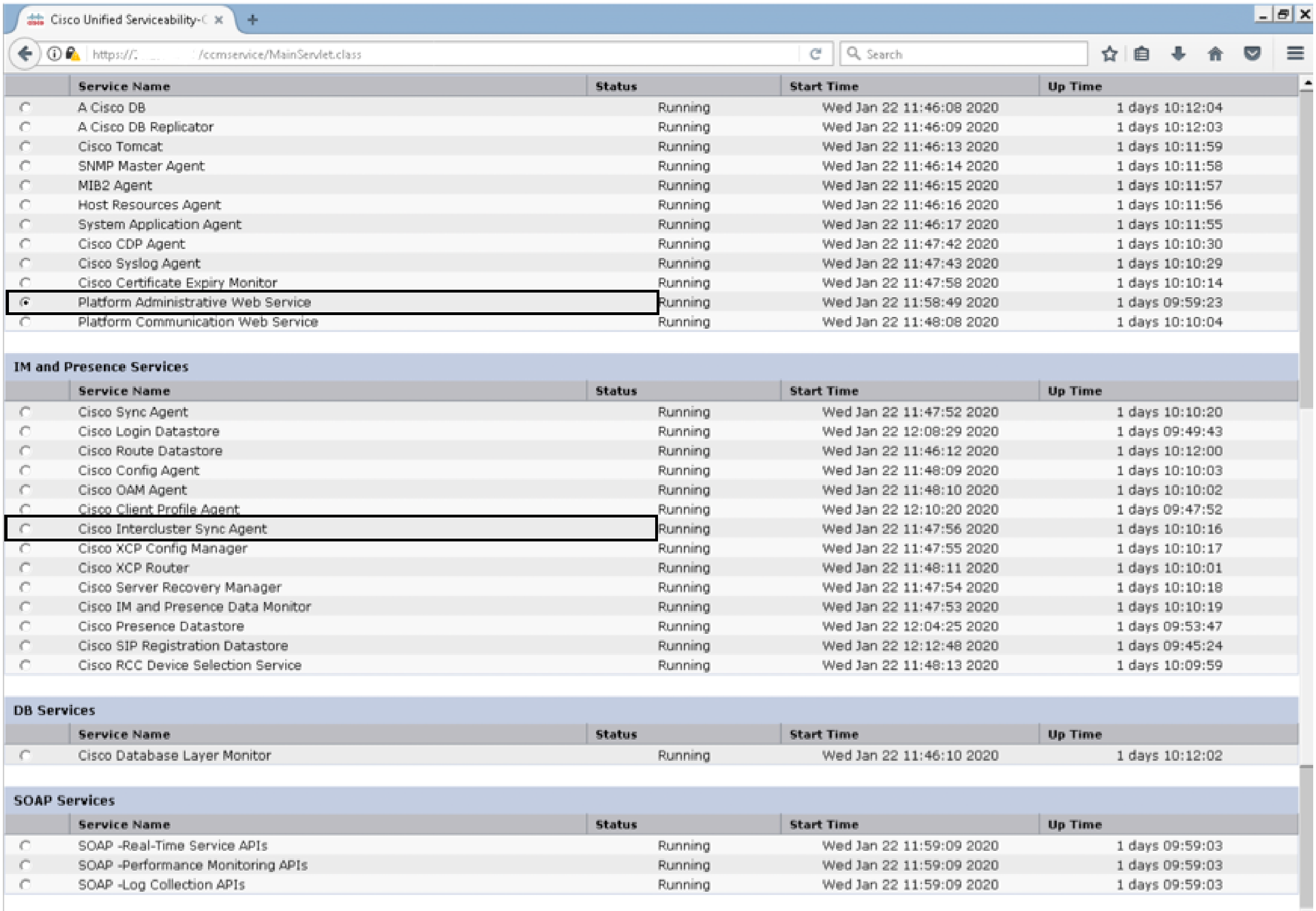
For Cisco Technical Support please visit our Technical Support web site.

Étape 2. Arrêter la **notification de modification de certificat Cisco** sur tous les noeuds du cluster


Cisco Unified Serviceability-C
https://l /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

Étape 3. En cas d'arrêt des **services Web d'administration de la plate-forme** IM and Presence Server et **Cisco Intercluster Sync Agent**



	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

Étape 4. Supprimer le certificat sur tous les noeuds, y compris la messagerie instantanée et la présence, comme décrit dans la section *Solution pour 11.0(1) et les versions ultérieures* de ce document

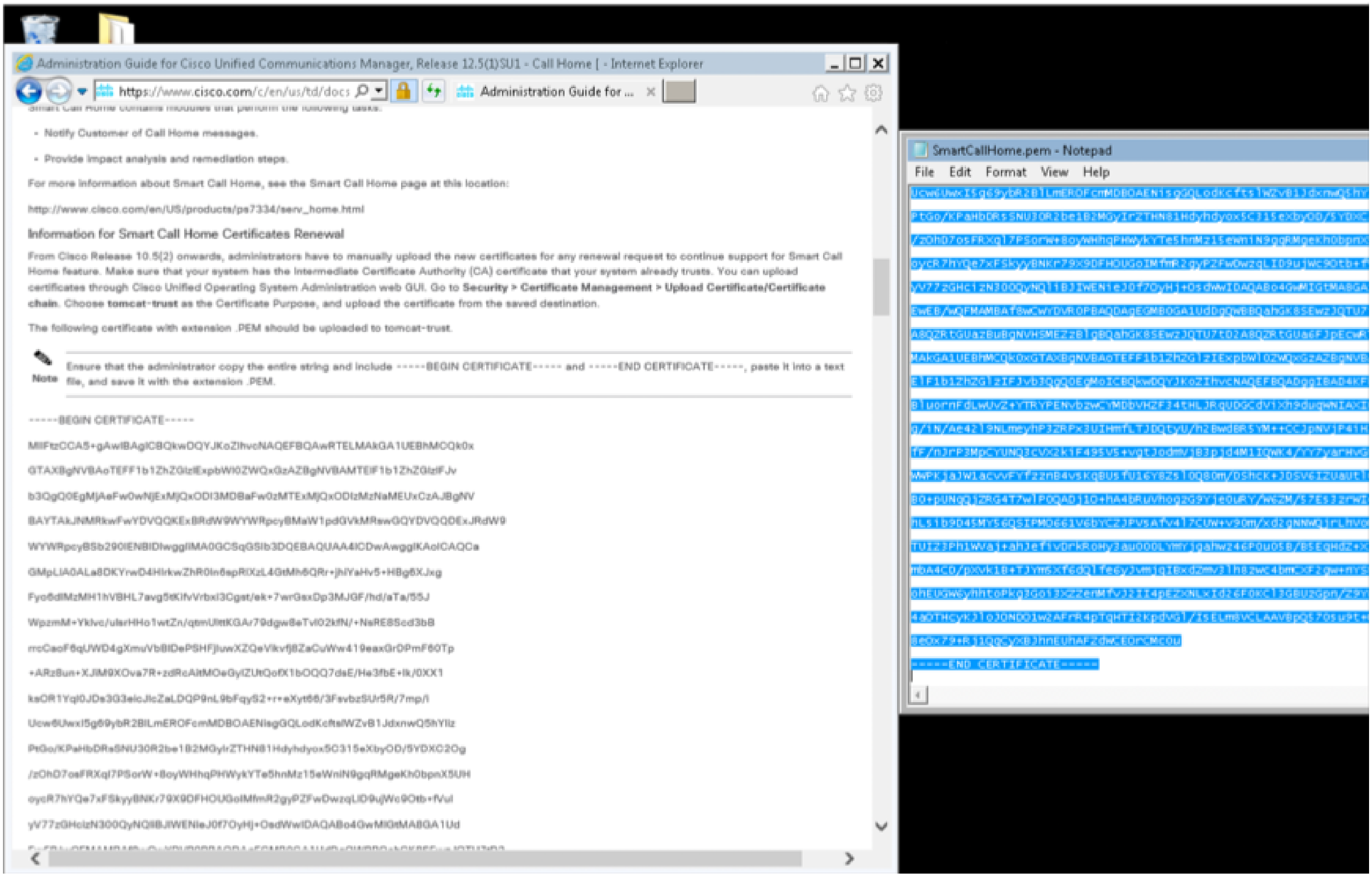
Étape 5. Démarrez le service qui a été arrêté à l'étape 2. et Étape 3.

> **Note**: Si vous supprimez le certificat et que vous effectuez une mise à niveau avant le 7 février 2020, le certificat réapparaîtra après la mise à niveau et devra être supprimé à nouveau. Aucune mise à niveau après le 7 février 2020 ne réajoutera le certificat

Procédure de renouvellement des certificats Smart Call Home

Si Smart Call Home est désactivé, aucune autre action n'est requise après la suppression du certificat. Si Smart Call Home est activé, procédez comme suit

Étape 1. Copier le contenu du certificat à partir des *informations de* la section Guide d'administration UCM *pour les certificats Smart Call Home*



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

- 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.

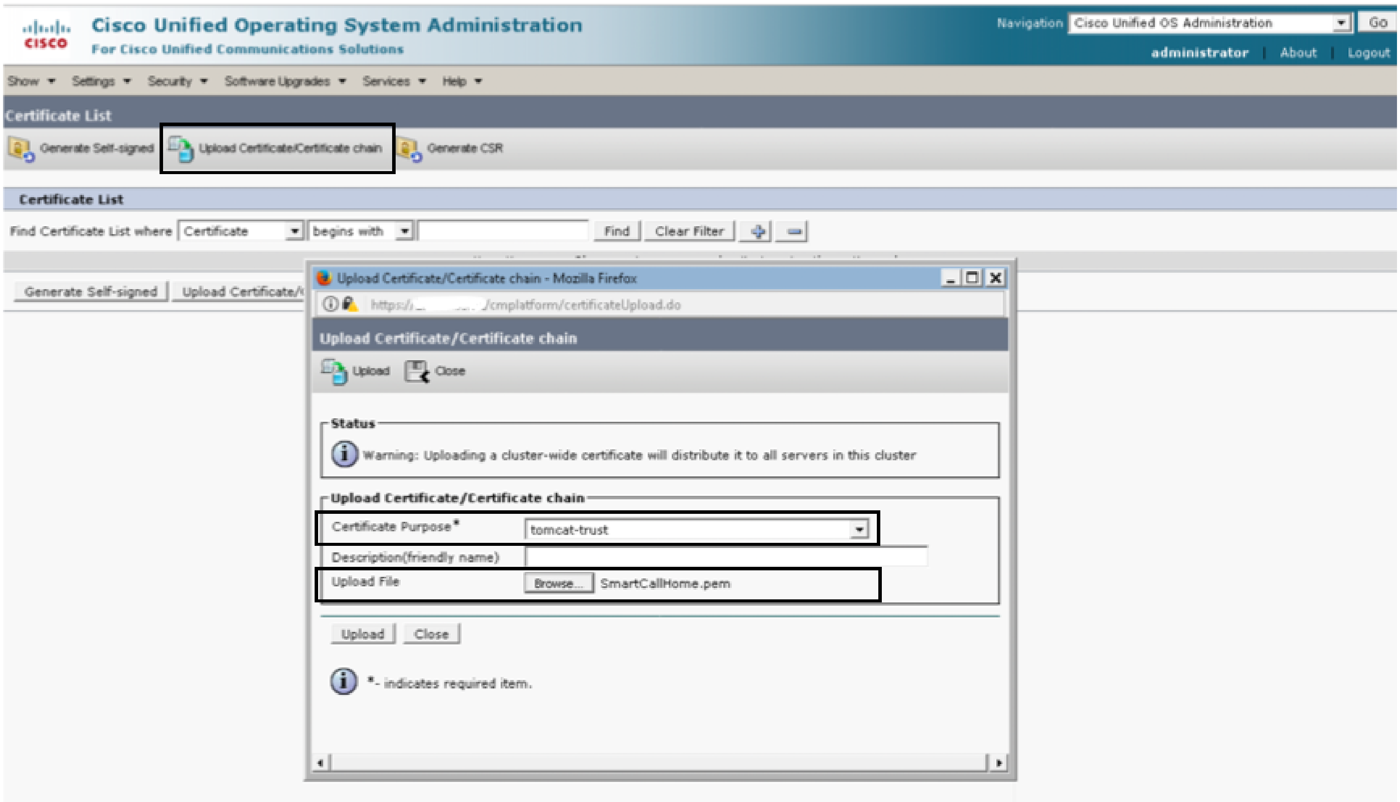
```
-----BEGIN CERTIFICATE-----
MIIFtzCCA5+gAwIBAgICBQkwDQYJKoZIhvcNAQEFBQAwRTELMAkGA1UEBhMCQk0x
GTAXBgNVBAoTEFF1b1ZhZGlzIExpbWl0ZWQxGzAZBgNVBAMTElF1b1ZhZGlzIFJv
b3QgQ0EgMjAeFw0wNjExMjQxODI3MDBaFw0zMTExMjQxODIzMzNaMEUxCzAJBgNV
BAYTAkJNMRkwFwYDVQQKExBRdW9WYWRpcyBMaW1pdGVkMRswGQYDVQQDExJRdW9W
YWRpcyBSb290IENBIDIwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCa
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
```

SmartCallHome.pem - Notepad

```
Ucw6UwxI5g69ybR2BlLmEROFcmMDBOAENisgGQLodKcftslWZvB1JdxnwQ5hY
PtGo/KPaHbDRsSNU30R2be1B2MGyIrZTHN81Hdyhdyox5C315eXbyOD/5YDXC
/zOhD7osFRXql7PSorW+8oyWHhqPHWykYTe5hnMz15eWniN9gqRMgeKh0bpnX
oycR7hYQe7xFSkyyBNKr79X9DFHOUGoIMfmR2gyPZFwDwzqLID9ujWc9Otb+f
yV77zGHcizN300QyNQliBJIWENieJ0f7OyHj+OsdWwIDAQABo4GwMIGtMA8GA
EwEB/wQFMAMBAf8wCwYDVR0PBAQDAgEGMB0GA1UdDgQWBBQahGK8SEwzJQTU7
A8QZRtGUazBuBgNVHSMEZzBlgBQahGK8SEwzJQTU7tD2A8QZRtGUaaFJpEcwR
MAkGA1UEBhMCQk0xGTAXBgNVBAoTEFF1b1ZhZGlzIExpbWl0ZWQxGzAZBgNVB
ElF1b1ZhZGlzIFJvb3QgQ0EgMoICBQkwDQYJKoZIhvcNAQEFBQADggIBAD4KF
BluornFdLwUvZ+YTRYPENvbzwCYMDbVHZF34tHLJRqUDGCdViXh9duqWNIAXI
g/iN/Ae42l9NLmeyhP3ZRPx3UIHmfLTJDQtyU/h2BwdBR5YM++CCJpNVjP4iH
fF/nJrP3MpCYUNQ3cVX2kiF495V5+vgtJodmVjB3pjd4M1IQWK4/YY7yarHvG
WWPKjaJW1acvvFYfzznB4vsKqBUsfU16Y8Zsl0Q80m/DShcK+JDSV6IZUaUtl
B0+pUNqQjZRG4T7wlP0QADj1O+hA4bRuVhogzG9Yje0uRY/W6ZM/57Es3zrWI
hLsib9D45MY56QSIPMO661V6bYCZJPVsAfv4l7CUW+v90m/xd2gNNWQjrLhVo
TUIZ3Ph1WVaj+ahJefivDrkRoHy3au000LYmYjgahwz46P0u05B/B5EqHdZ+X
mbA4CD/pXvk1B+TJYm5Xf6dQlfe6yJvmjqIBxdZmv3lh8zwc4bmCXF2gw+nYS
ohEUGW6yhhtoPkg3Goi3XZZenMfvJ2II4pEZXNLxId26F0KCl3GBUzGpn/Z9Y
4aOTHcyKJloJONDO1w2AFrR4pTqHTI2KpdVGl/IsELm8VCLAAVBpQ570su9t+
8eOx79+Rj1QqCyXBJhnEUhAFZdWCEOrCMc0u
-----END CERTIFICATE-----
```

Note: Le même certificat est valide pour la version 10.5 et supérieure

Étape 2. Téléchargez le fichier .pem en tant que tomcat-trust dans la page **Gestion des certificats** de l'interface utilisateur graphique de Cisco Unified OS Administration par capture d'écran



Cisco Unified Operating System Administration

For Cisco Unified Communications Solutions

Navigation: Cisco Unified OS Administration

administrator | About | Logout

Certificate List

Certificate List

Find Certificate List where: Certificate | begins with

Upload Certificate/Certificate chain - Mozilla Firefox

https://... /cmplatform/certificateUpload.do

Upload Certificate/Certificate chain

Status

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

Upload Certificate/Certificate chain

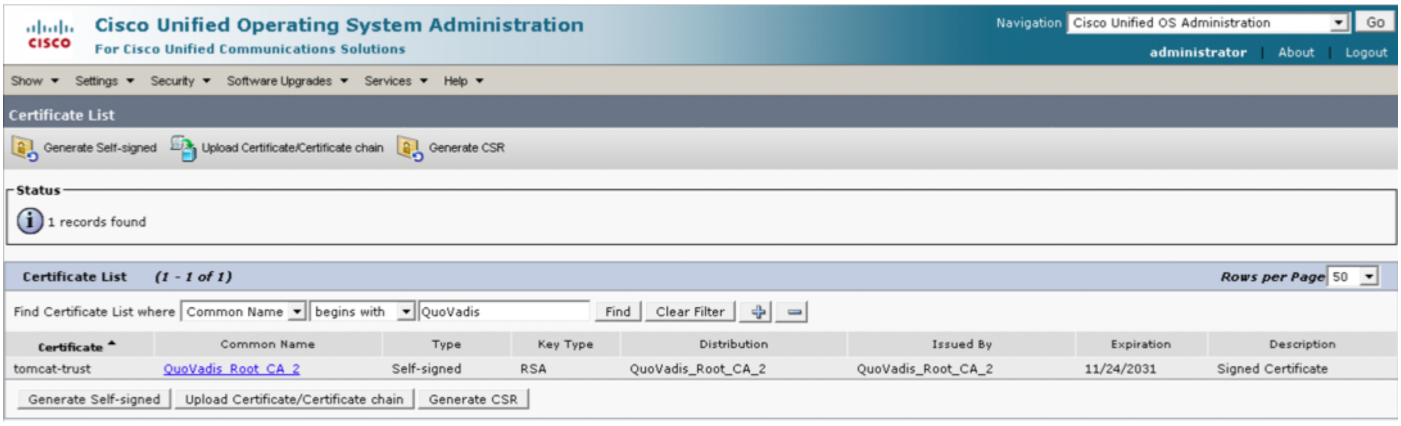
Certificate Purpose*: tomcat-trust

Description(friendly name):

Upload File: Browse... SmartCallHome.pem

*- indicates required item.

Étape 3. Vérifiez que **QuoVadis_Root_CA_2** est répertorié comme tomcat-trust en recherchant le certificat où Common Name contient QuoVadis


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 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

Pour Cisco Prime License Manager

Pour Prime License Manager 10.5

Le certificat expiré (VeriSign_Class_3_Secure_Server_CA_-_G3) peut être supprimé du système en appliquant ce fichier COP (ciscocm.plm-CSCvs64158_remove_sch_cert_C0050-1.k3.cop.sgn). Veuillez consulter le fichier Readme pour obtenir des instructions d'installation.

Pour Prime License Manager 11.5

Le certificat expiré (VeriSign_Class_3_Secure_Server_CA_-_G3) peut être supprimé du système en appliquant ce fichier COP (ciscocm.plm-CSCvs64158_remove_sch_cert_C0050-1.k3.cop.sgn). Veuillez consulter le fichier Readme pour obtenir des instructions d'installation.