

Fehlerbehebung: Warnung zum Ablauf eines Zertifikats bei Smart Call Home-Zertifikat für Collaboration-Produkte

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Problem](#)

[Lösung](#)

[Problemumgehung für Versionen ab 11.0\(1\)](#)

[Für alle anderen Versionen](#)

[Verlängerungsverfahren für Smart Call Home-Zertifikate](#)

[Für Cisco Prime License Manager](#)

[Für Prime License Manager 10.5](#)

[Für Prime License Manager 11.5](#)

Einführung

Dieses Dokument beschreibt die Lösungen für die Warnung zum Ablauf von Zertifikaten (Certificate Expiry Alert of Verisign Certificate, VeriSign_Class_3_Secure_Server_CA_G3.der) für Smart Call Home, die ab Februar 2020 in den folgenden Cisco Unified Collaboration-Produkten ablaufen soll, die in diesem Dokument behandelt werden.

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

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

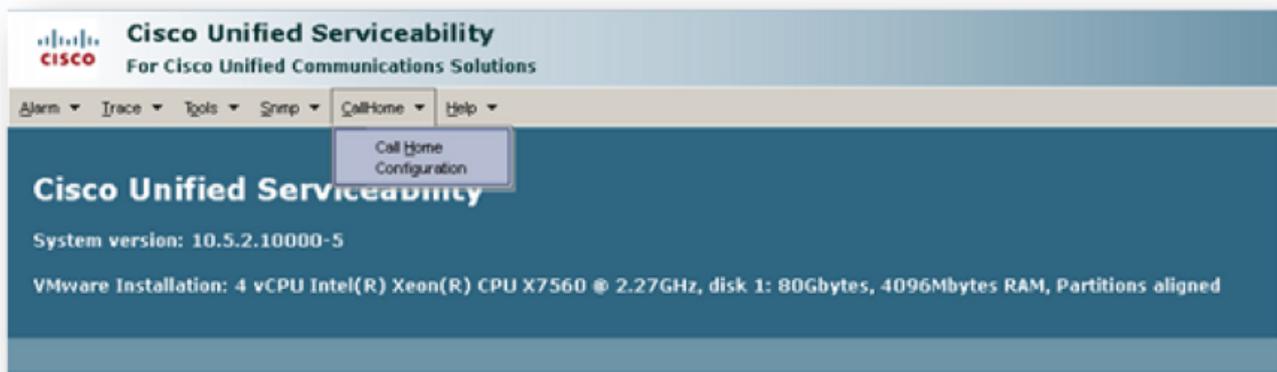
Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

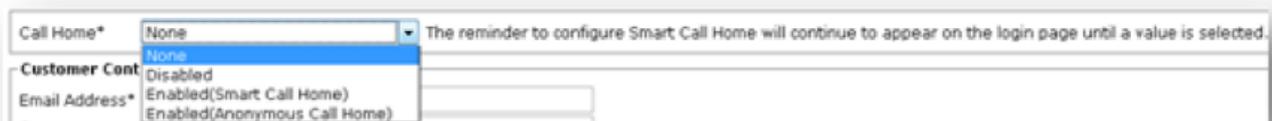
Smart Call Home ist eine automatisierte Support-Funktion, die Cisco Geräte in Ihrem Netzwerk überwacht. Mit der Call Home-Funktion können Sie Diagnosewarnungen, Inventar und andere Nachrichten an den Smart Call Home-Backend-Server kommunizieren und senden.

Überprüfen Sie in diesem Abschnitt, ob Smart Call Home aktiviert ist.

Schritt 1: Wählen Sie auf der Seite Cisco Unified Service (Cisco Unified Serviceability) CallHome > Configuration (CallHome > Konfiguration) aus.



Schritt 2: Überprüfen, ob das Feld "Call Home" auf "Disabled" (Deaktiviert) oder "Enabled" (Aktiviert) eingestellt ist



Problem

Das VeriSign-Zertifikat (VeriSign_Class_3_Secure_Server_CA_-_G3.der), das standardmäßig als "tomcat-trust"-Zertifikat für Smart Call Home auf Cisco Unified Collaboration-Produkten bereitgestellt wird, läuft ab Februar 2020 ab. Die folgende Ablaufwarnung kann unten angezeigt werden:

```
%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]

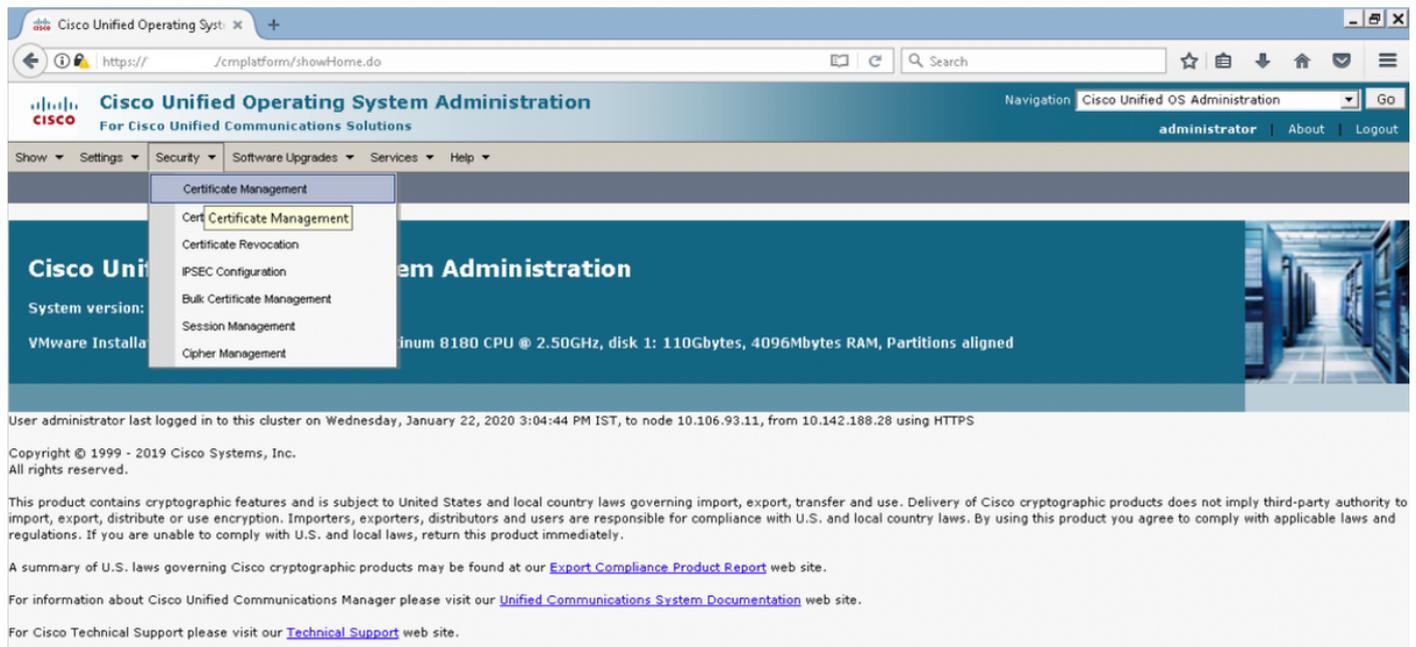
Lösung

Dieses Problem wird durch die Cisco Bug-ID [CSCvs64158](#) dokumentiert.

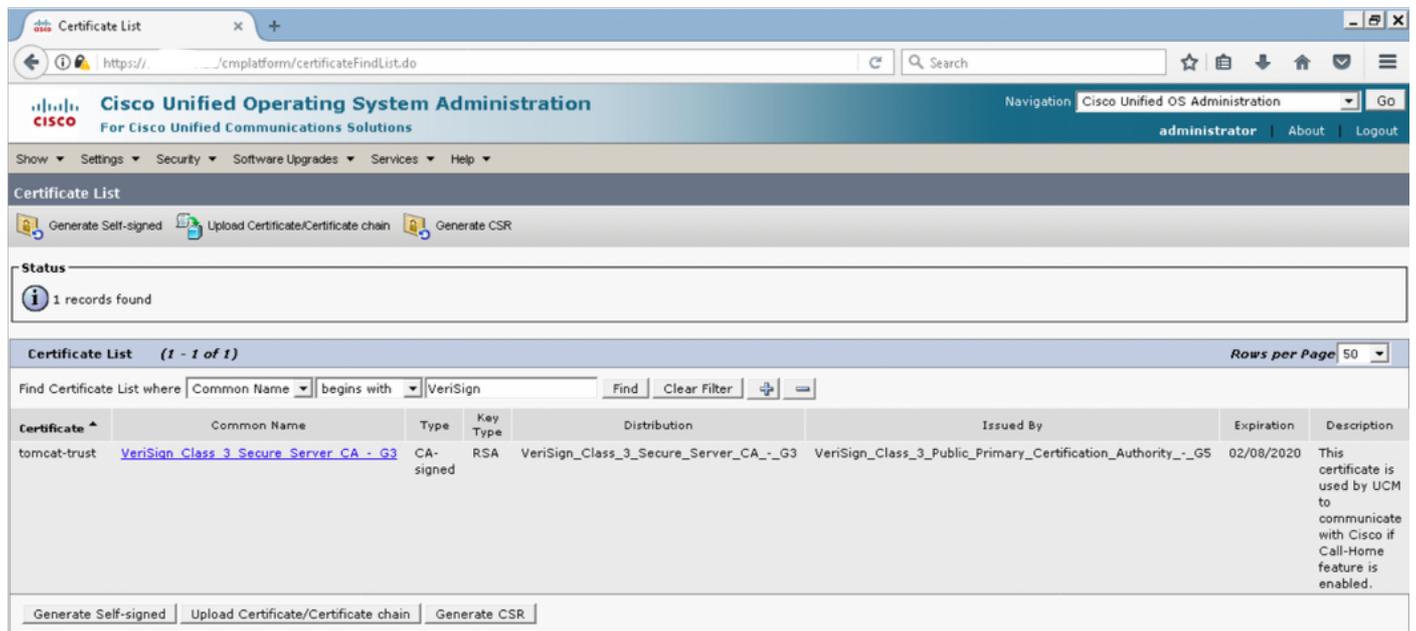
Problemumgehung für Versionen ab 11.0(1)

Führen Sie die folgenden Schritte aus, um das abgelaufene Zertifikat zu löschen (VeriSign_Class_3_Secure_Server_CA__G3.der).

Schritt 1: Rufen Sie im Publisher die Benutzeroberfläche für die Cisco Unified OS-Verwaltung auf, und klicken Sie auf **Sicherheit > Zertifikatsverwaltung**.

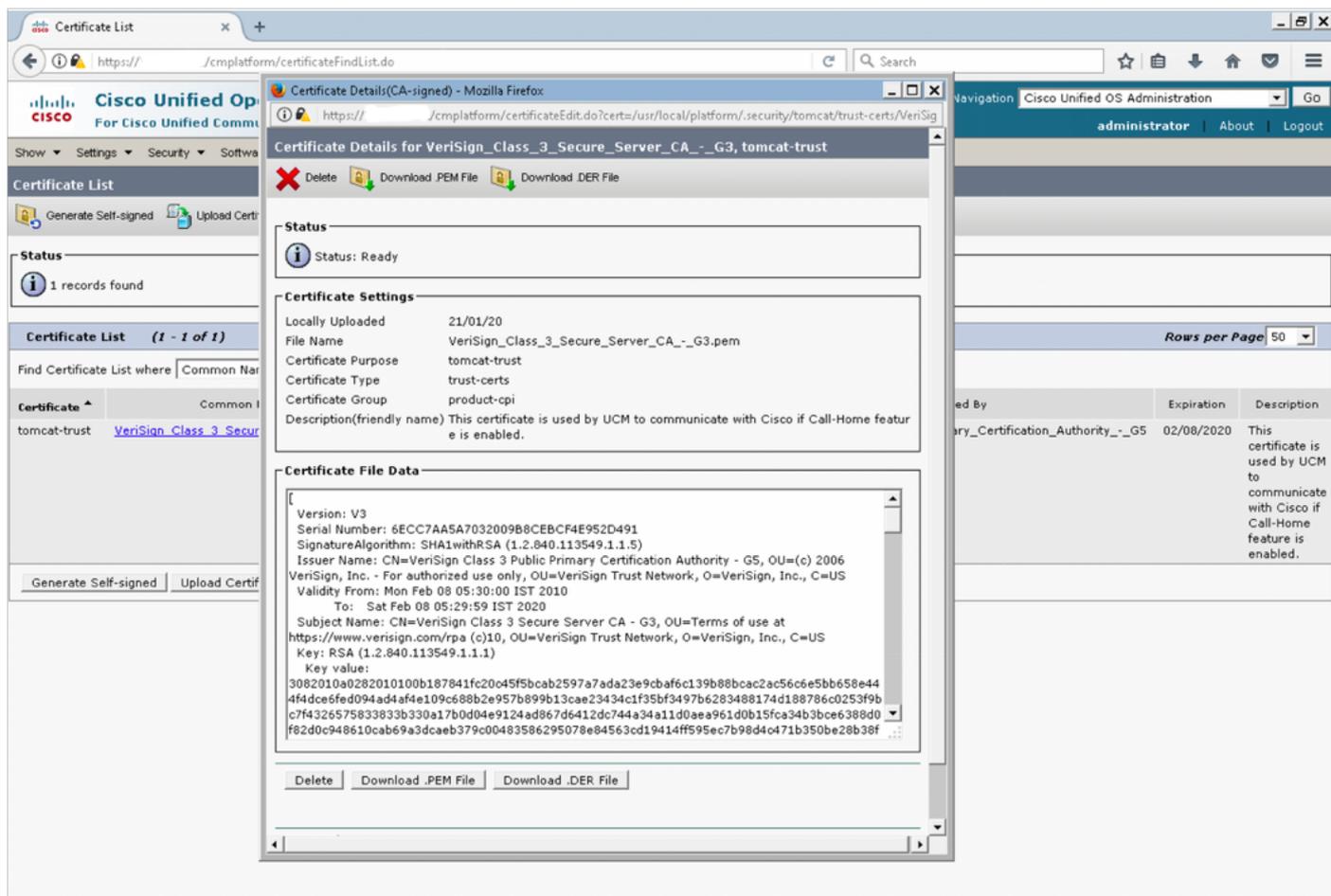


Schritt 2: Zertifikatsliste suchen, in der Common Name VeriSign enthält

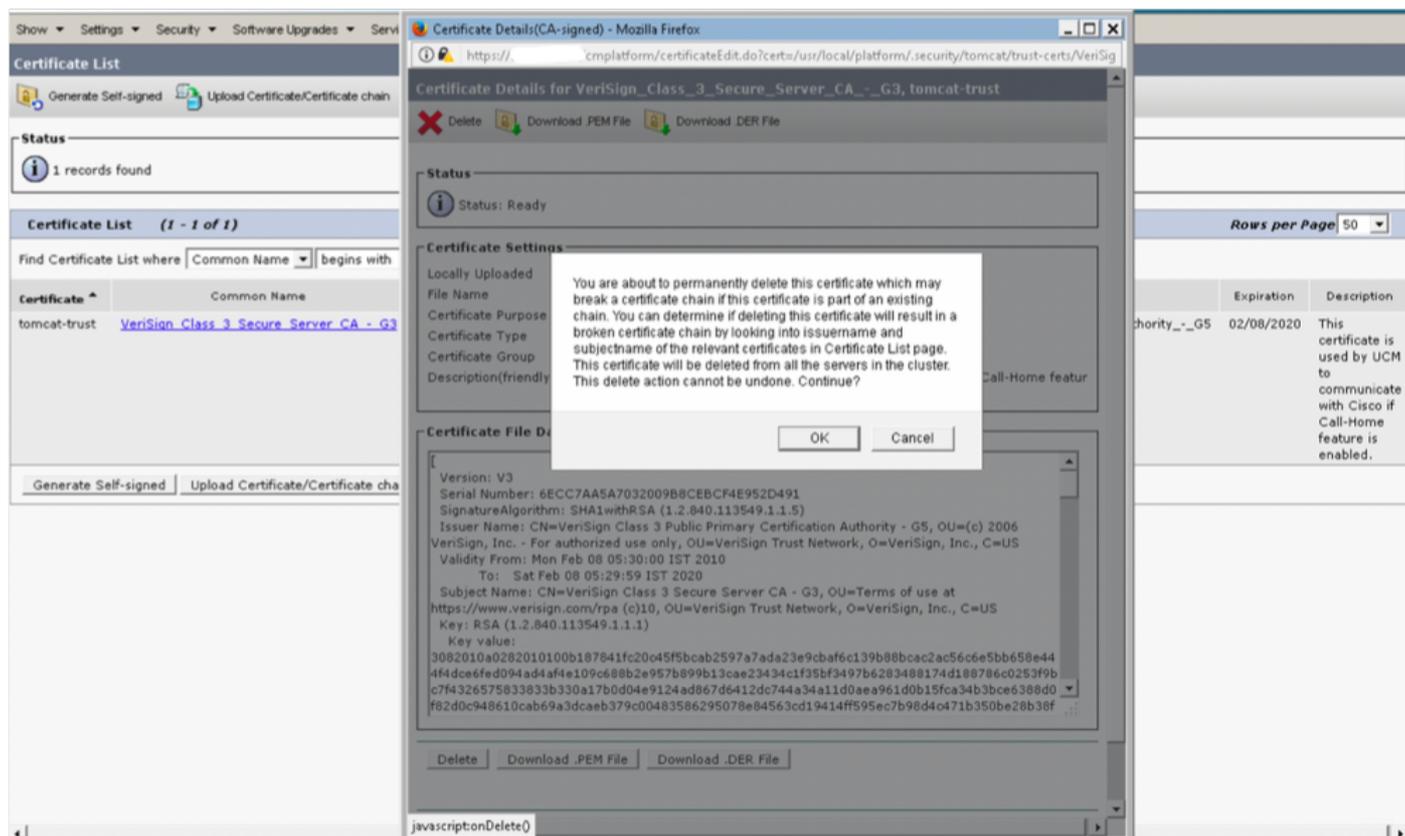


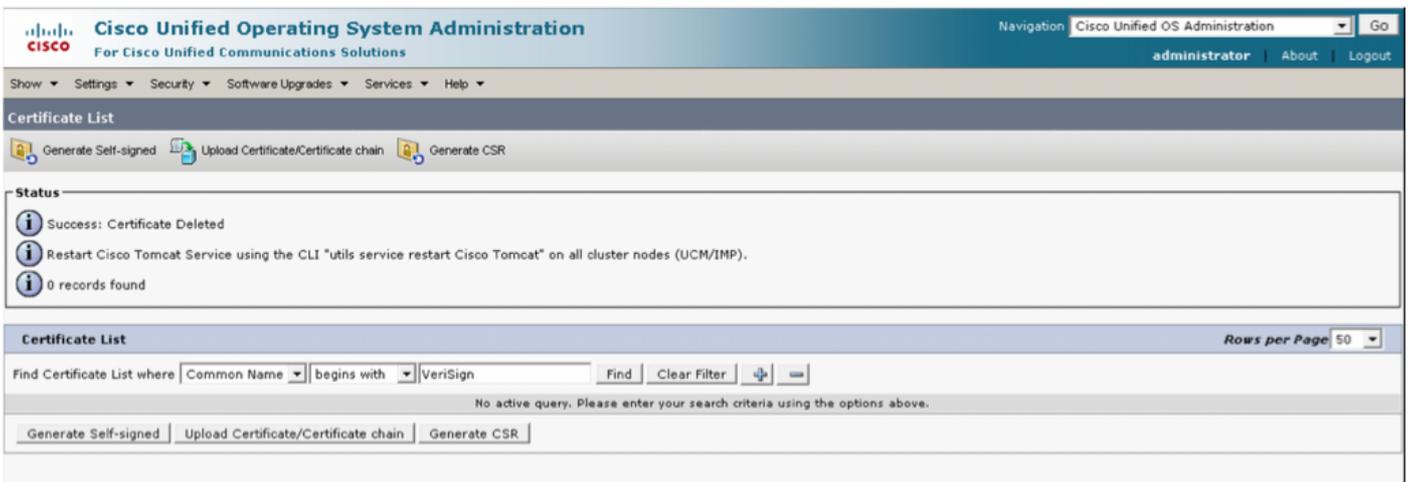
Schritt 3: Klicken Sie auf [VeriSign_Class_3_Secure_Server_CA__G3](#), und Sie sehen das Popup-

Fenster, in dem die Details des Zertifikats hervorgehoben sind.



Schritt 4: Klicken Sie auf die **Schaltfläche Löschen**, und eine Warnung wird angezeigt. Klicken Sie auf **OK**. Das Zertifikat sollte von allen Knoten im Cluster gelöscht werden.

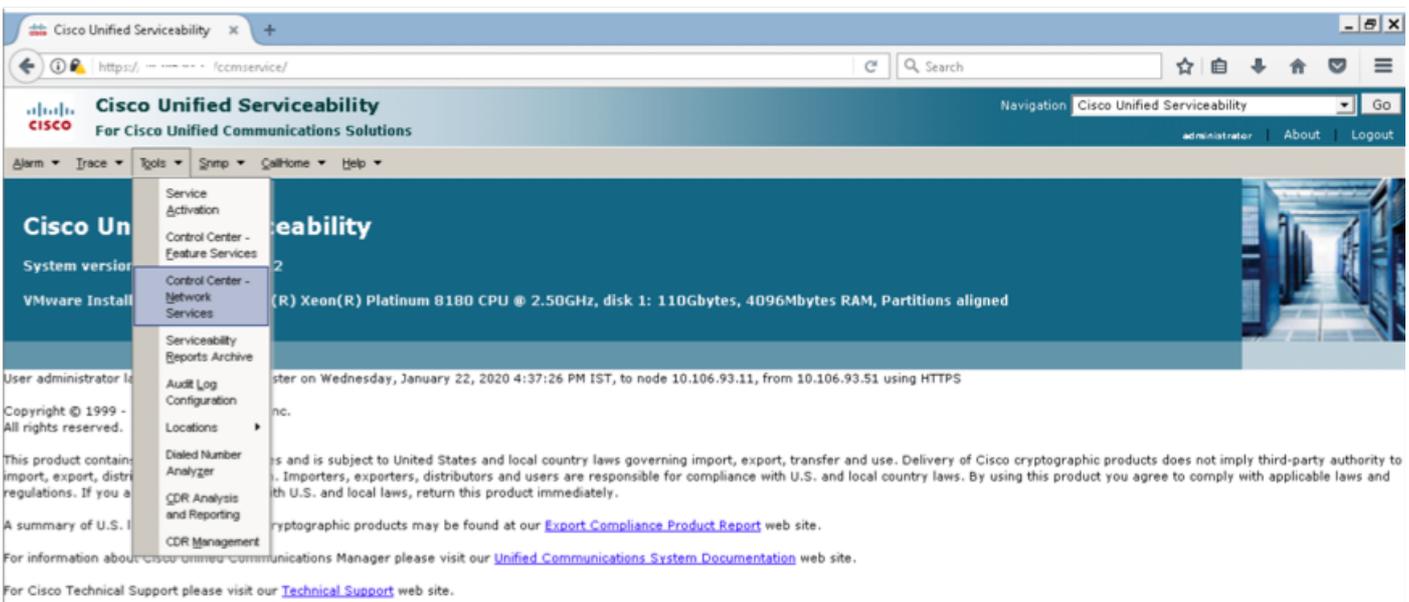




Für alle anderen Versionen

Wir müssen die folgenden Schritte ausführen, bevor wir das Zertifikat löschen.

Schritt 1: Navigieren Sie zu **Cisco Unified Serviceability > Tools > Control Center - Network Services**.



Schritt 2: Stoppen der **Benachrichtigung zur Cisco Zertifikatsänderung** auf allen Knoten im Cluster

Service Name	Status	Last Update	Age
Platform Administration Web Service	Running	Wed Jan 22 10:33:15 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

Schritt 3: Fall von IM und Presence Server Stopp **Platform Administration Web Services** und **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

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

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

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

Schritt 4: Löschen Sie das Zertifikat auf allen Knoten einschließlich IM und Presence wie in Abschnitt *Problemumgehung für 11.0(1) und höher* in diesem Dokument beschrieben.

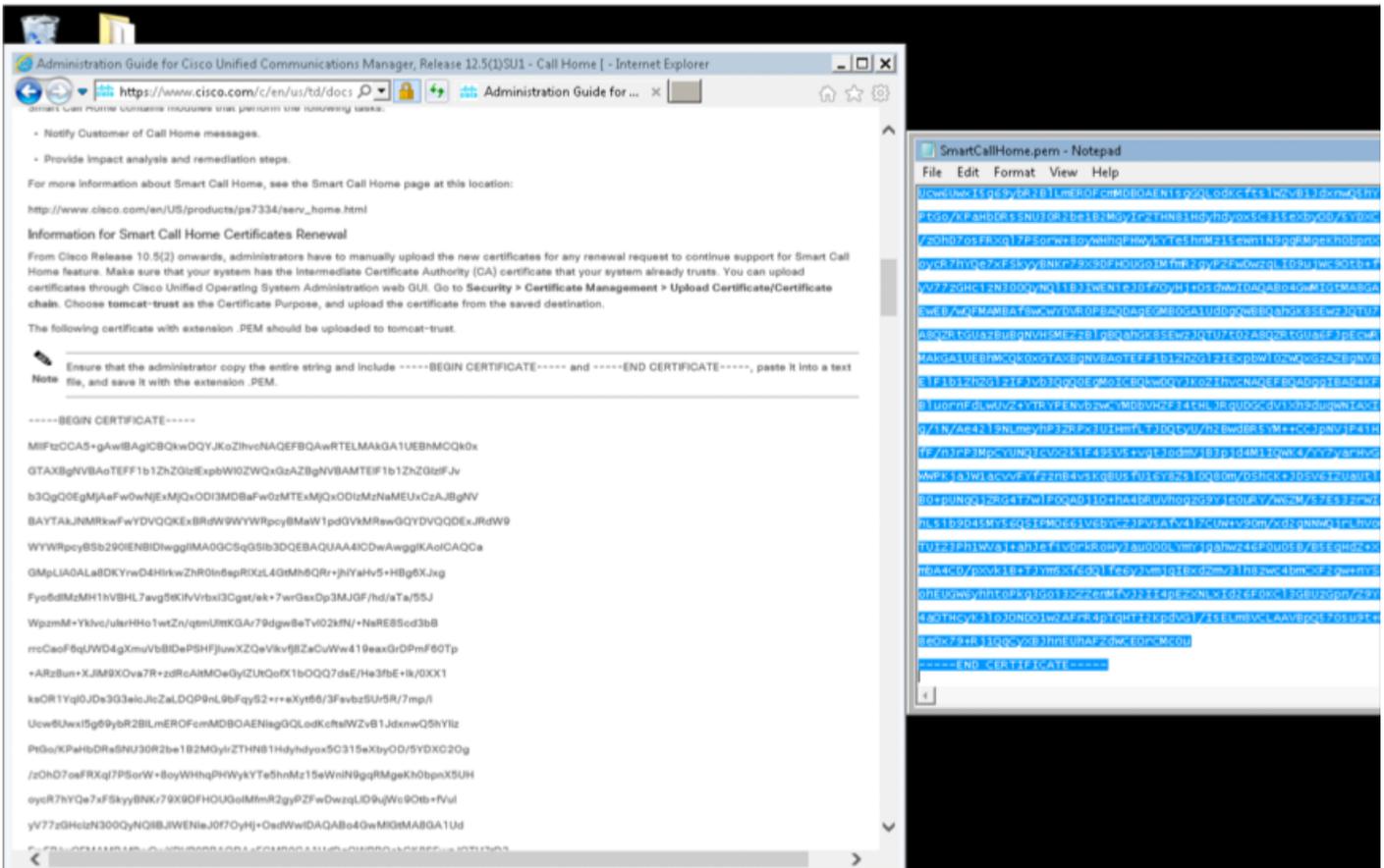
Schritt 5: Starten Sie den Dienst, der in Schritt 2 beendet wurde. und Schritt 3.

Hinweis: Wenn Sie das Zertifikat löschen und ein Upgrade vor dem 7. Februar 2020 durchführen, wird das Zertifikat nach dem Upgrade erneut angezeigt und muss erneut entfernt werden. Bei Upgrades nach dem 7. Februar 2020 wird das Zertifikat nicht erneut hinzugefügt.

Verlängerungsverfahren für Smart Call Home-Zertifikate

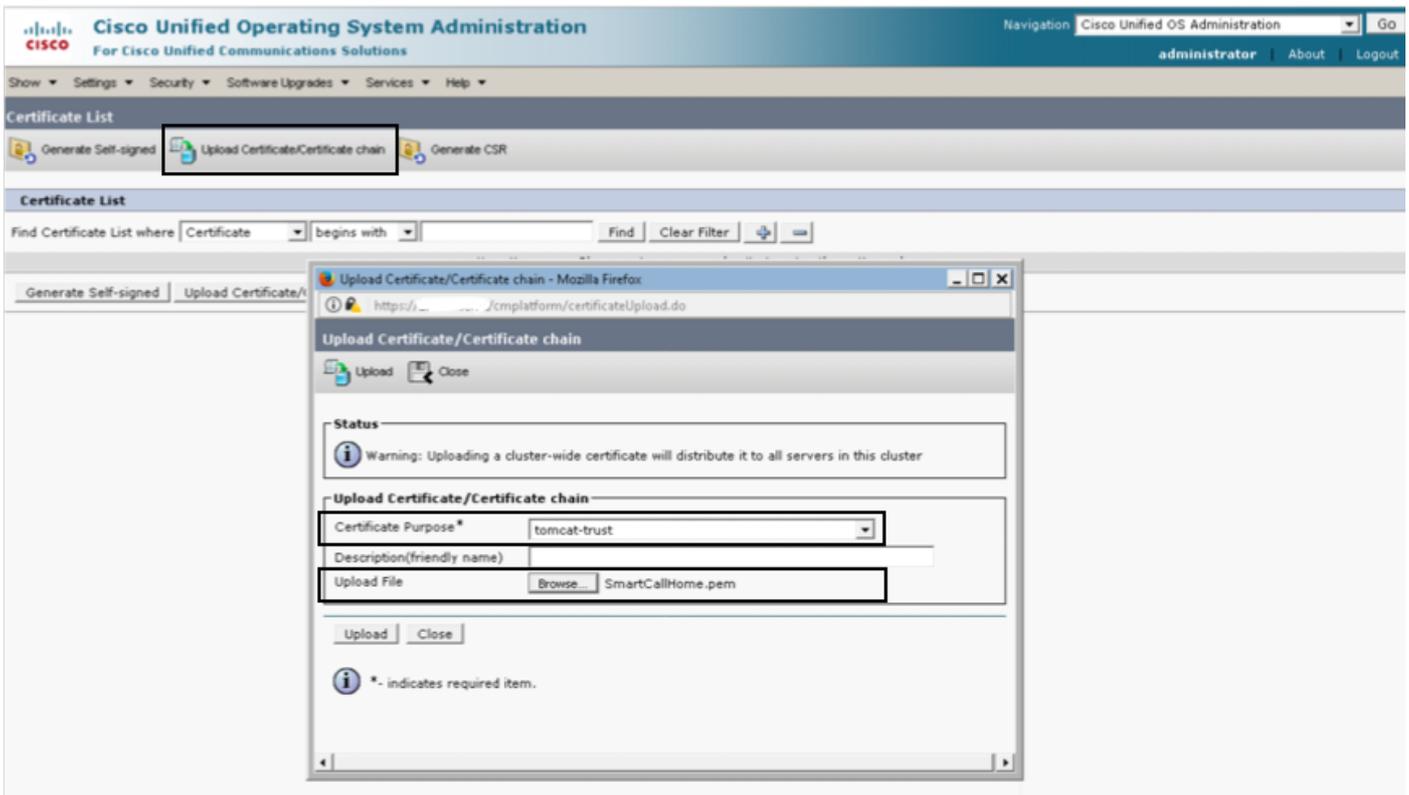
Wenn Smart Call Home deaktiviert ist, ist nach dem Löschen des Zertifikats keine weitere Aktion erforderlich. Wenn Smart Call Home aktiviert ist, gehen Sie wie folgt vor

Schritt 1: Kopieren Sie den Zertifikatsinhalt aus den *Smart Call Home-Zertifikaten* im [UCM-Administrationsleitfaden](#).



Hinweis: Das gleiche Zertifikat gilt für Version 10.5 und höher.

Schritt 2: Laden Sie die .pem-Datei pro Screenshot als tomcat trust in die GUI-Zertifikatsverwaltungsseite von Cisco Unified OS Administration hoch.



Schritt 3: Überprüfen Sie, ob QuoVadis_Root_CA_2 als tomcat-trust aufgeführt ist, indem Sie

Zertifikat finden, in dem der Common Name QuoVadis enthält.

The screenshot shows the Cisco Unified Operating System Administration interface. At the top, there is a navigation bar with the Cisco logo and the text "Cisco Unified Operating System Administration For Cisco Unified Communications Solutions". The user is logged in as "administrator". Below the navigation bar, there are several tabs: "Show", "Settings", "Security", "Software Upgrades", "Services", and "Help". The main content area is titled "Certificate List" and contains three buttons: "Generate Self-signed", "Upload Certificate/Certificate chain", and "Generate CSR". Below this, there is a "Status" section with an information icon and the text "1 records found". The main table is titled "Certificate List (1 - 1 of 1)" and has a "Rows per Page" dropdown set to 50. The table has columns for "Certificate", "Common Name", "Type", "Key Type", "Distribution", "Issued By", "Expiration", and "Description". The first row shows a certificate for "tomcat-trust" with a common name of "QuoVadis_Root_CA_2", type "Self-signed", key type "RSA", distribution "QuoVadis_Root_CA_2", issued by "QuoVadis_Root_CA_2", expiration "11/24/2031", and description "Signed Certificate". Below the table, there are three buttons: "Generate Self-signed", "Upload Certificate/Certificate chain", and "Generate CSR".

Für Cisco Prime License Manager

Für Prime License Manager 10.5

Das abgelaufene Zertifikat (VeriSign_Class_3_Secure_Server_CA_-_G3) kann durch Anwenden dieser COP-Datei aus dem System gelöscht werden ([ciscocm.plm-CSCvs64158_remove_sch_cert_C0050-1.k3.cop.sgn](#)). In der Readme-Datei finden Sie Installationsanweisungen.

Für Prime License Manager 11.5

Das abgelaufene Zertifikat (VeriSign_Class_3_Secure_Server_CA_-_G3) kann durch Anwenden dieser COP-Datei aus dem System gelöscht werden ([ciscocm.plm-CSCvs64158_remove_sch_cert_C0050-1.k3.cop.sgn](#)). In der Readme-Datei finden Sie Installationsanweisungen.