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

Inhalt

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

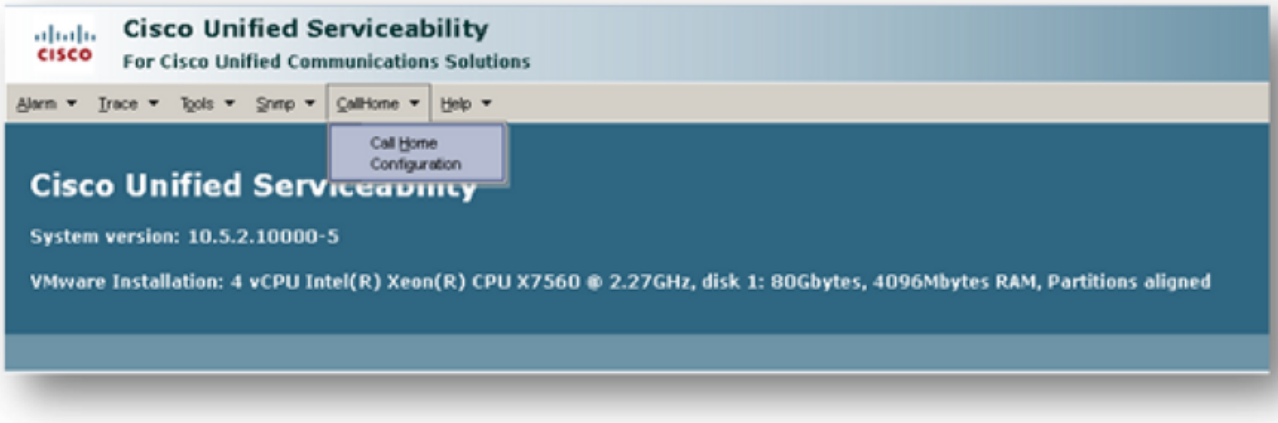
Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines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

Hintergrundinformationen

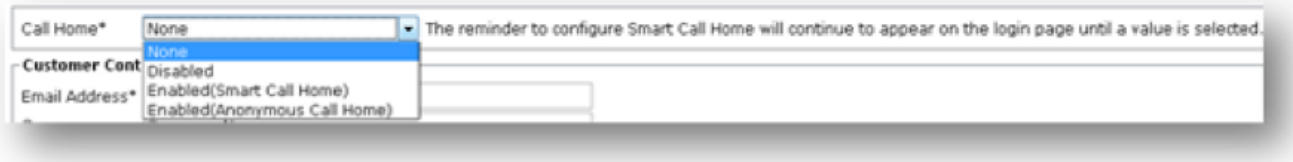
Smart Call Home ist eine automatisierte Support-Funktion, die Cisco Geräte in Ihrem Netzwerk überwacht. Mit der Call Home-Funktion können Sie Diagnosewarnungen, Inventar und andere Nachrichten an den Smart Call Home-Backend-Server kommunizieren und senden.

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]
```

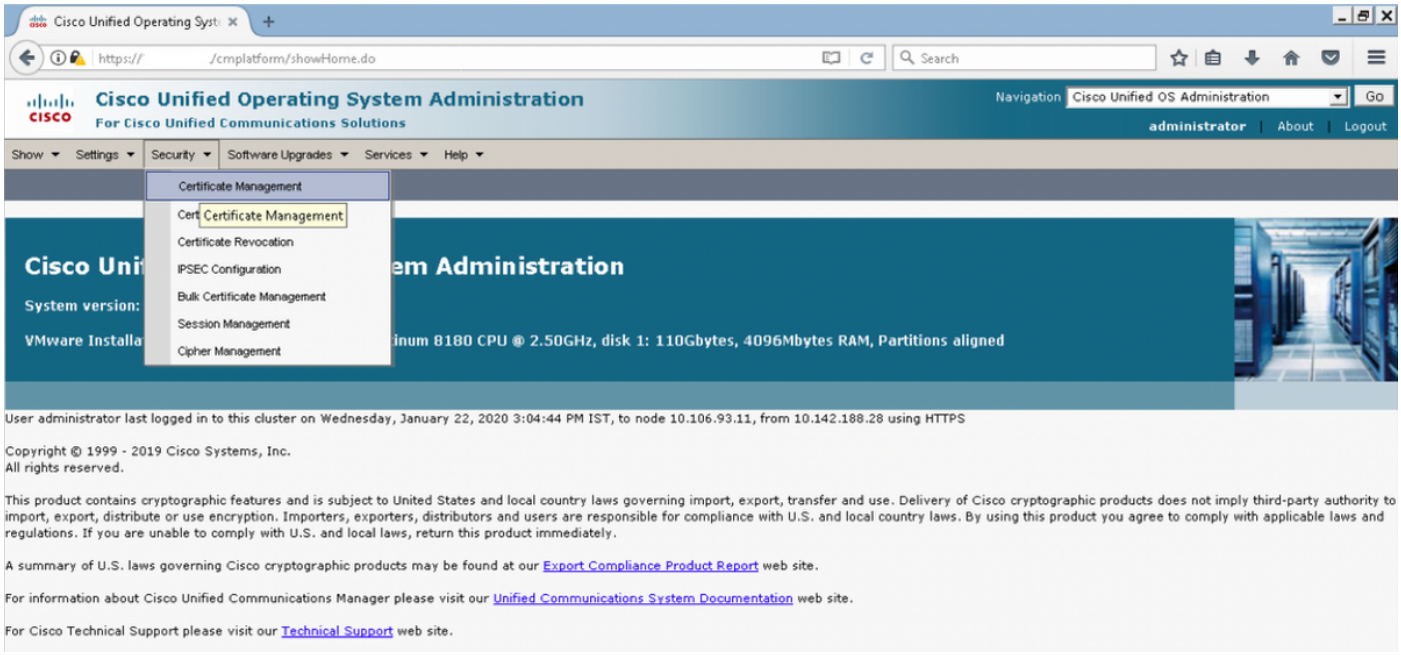
Lösung

Dieses Problem wird durch die Cisco Bug-ID CSCvs64158 dokumentiert.

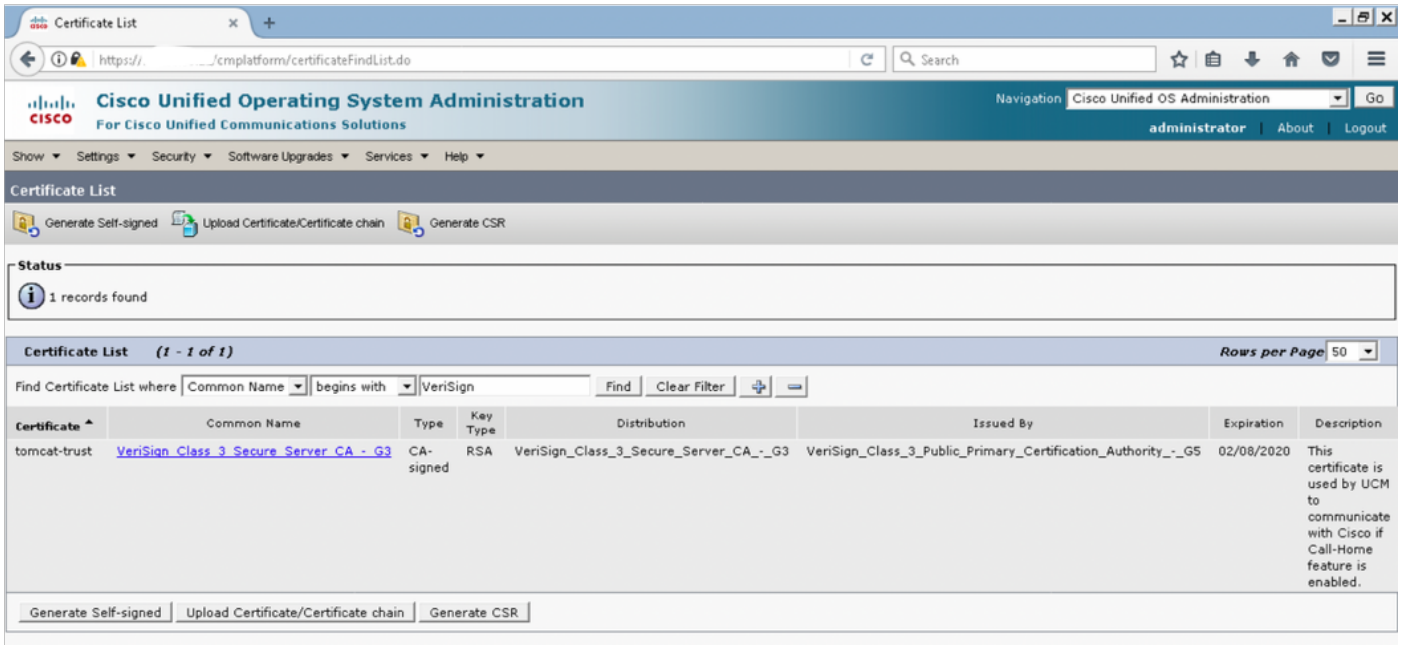
Problemumgehung für Versionen ab 11.0(1)

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.**

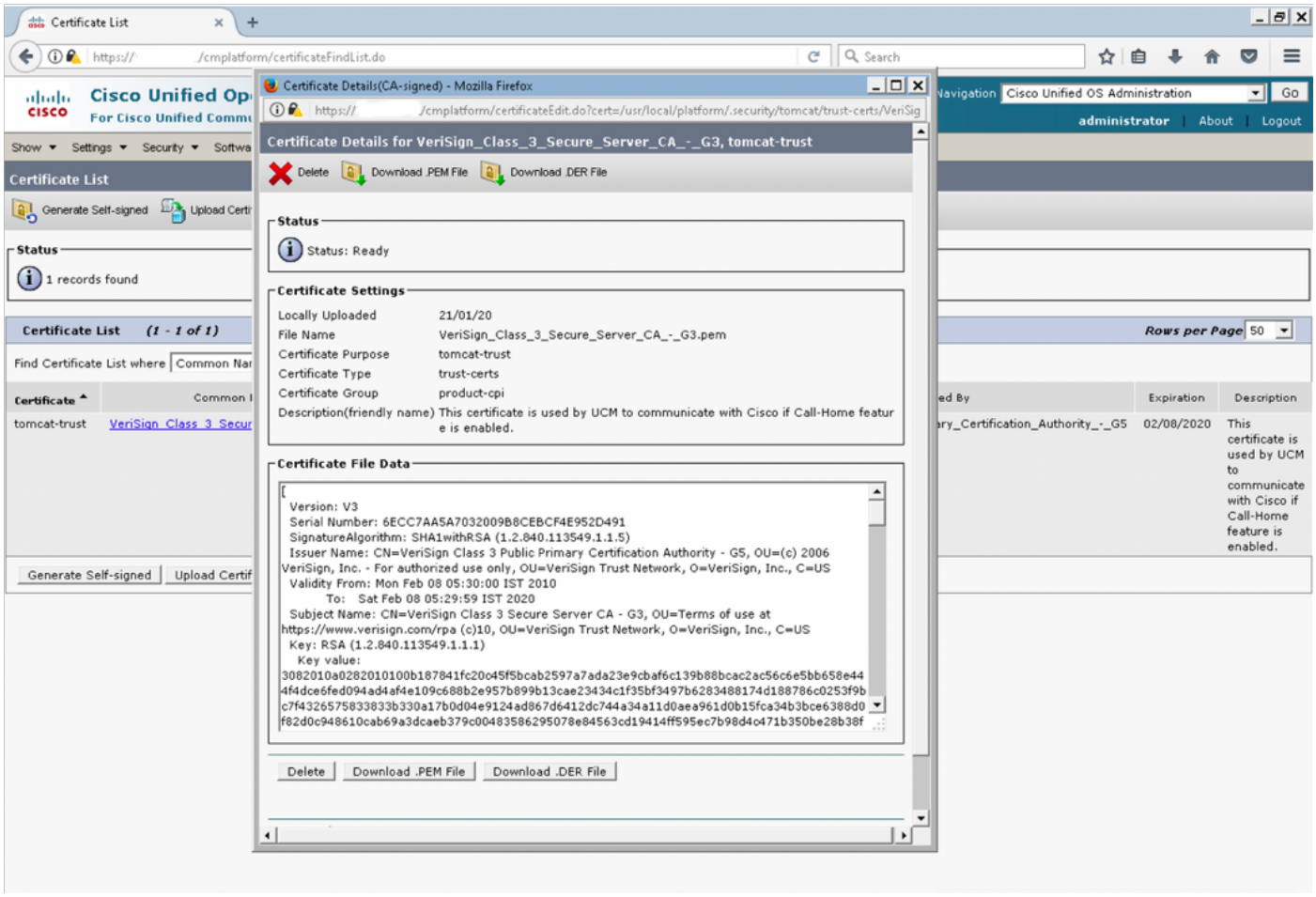


Schritt 2: Zertifikatsliste suchen, in der Common Name VeriSign enthält

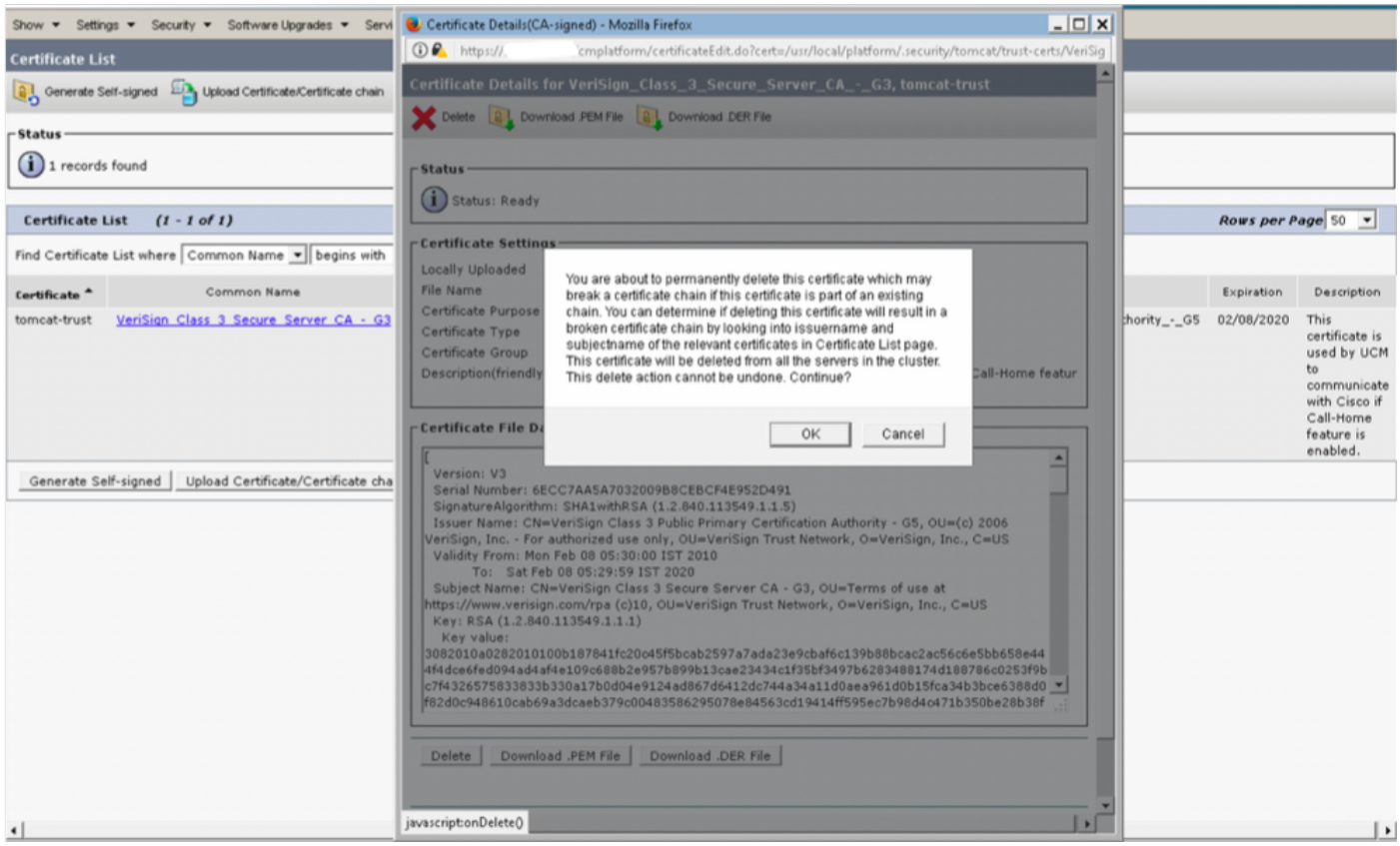


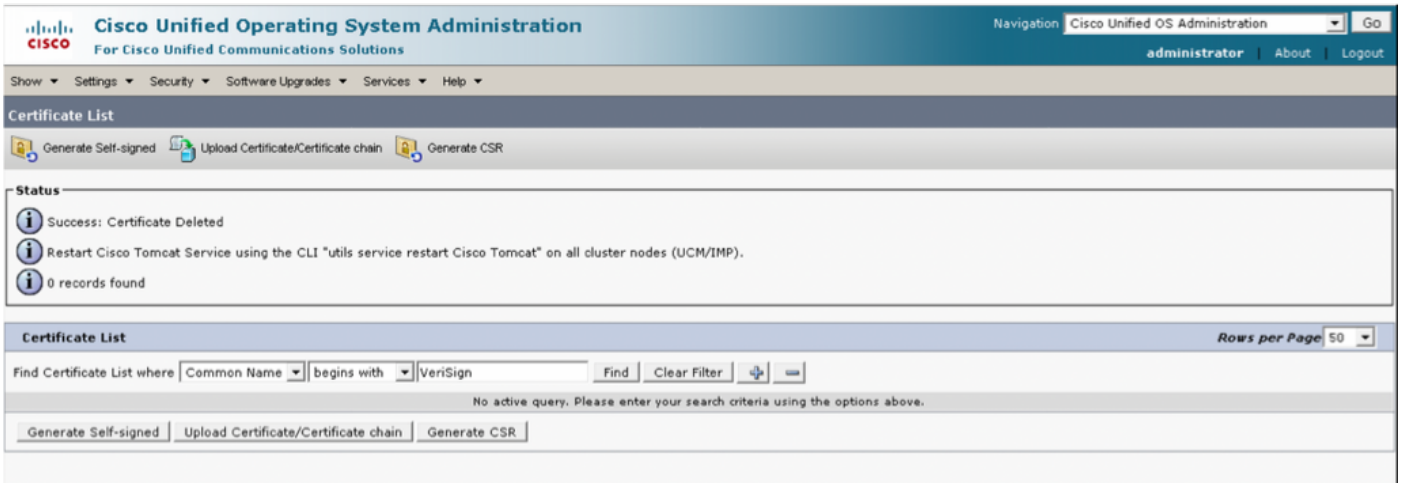
Schritt 3: Klicken Sie auf **VeriSign_Class_3_Secure_Server_CA__G3**, und Sie sehen das Popup-

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.

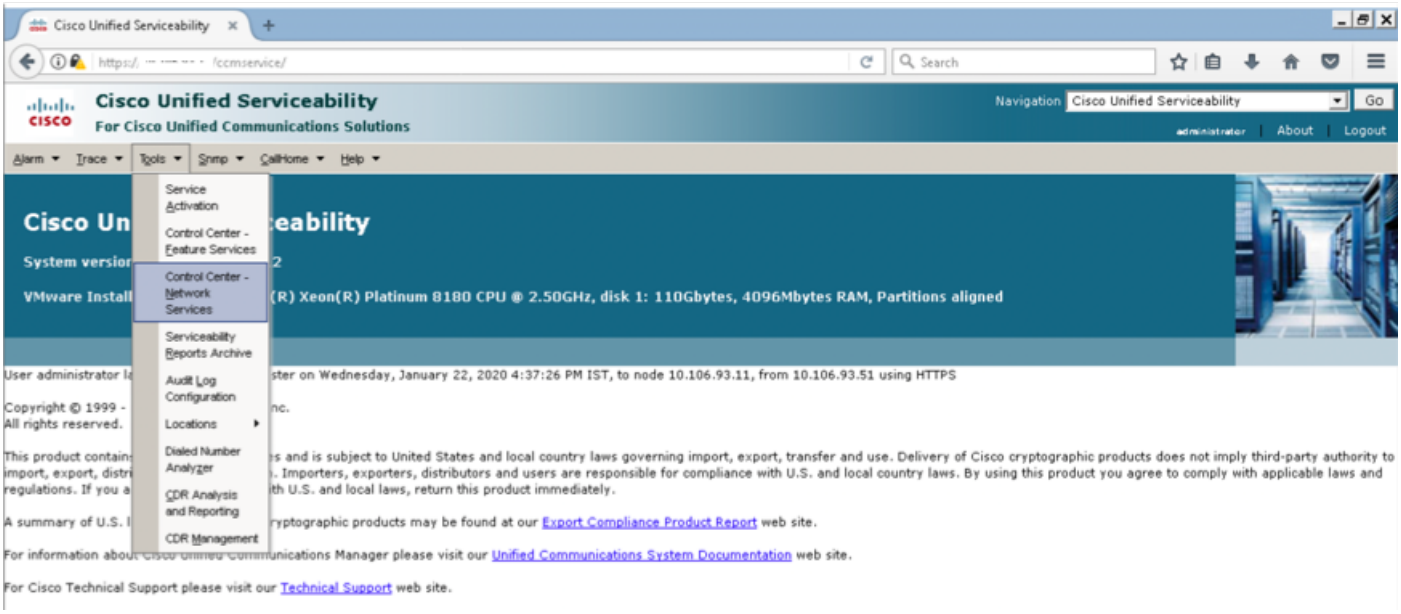




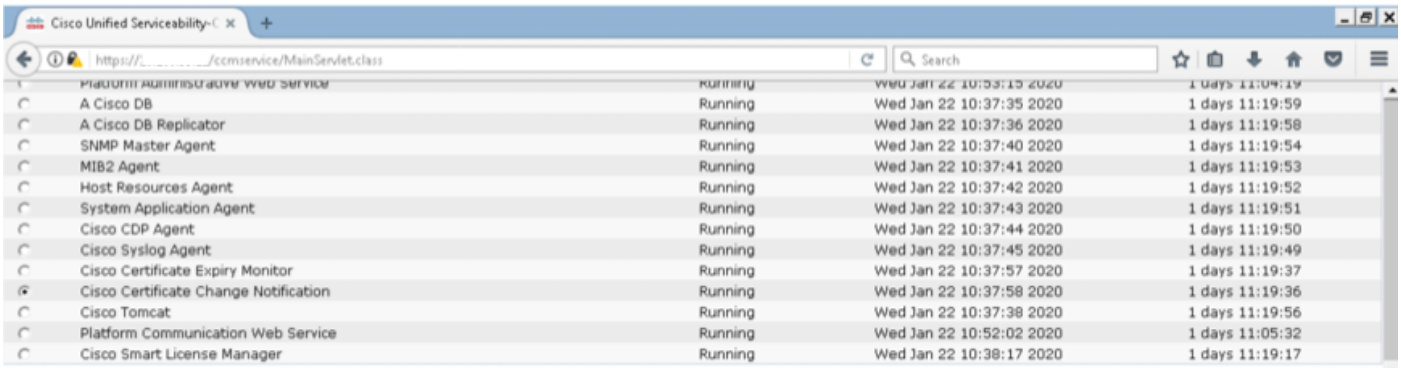
Für alle anderen Versionen

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

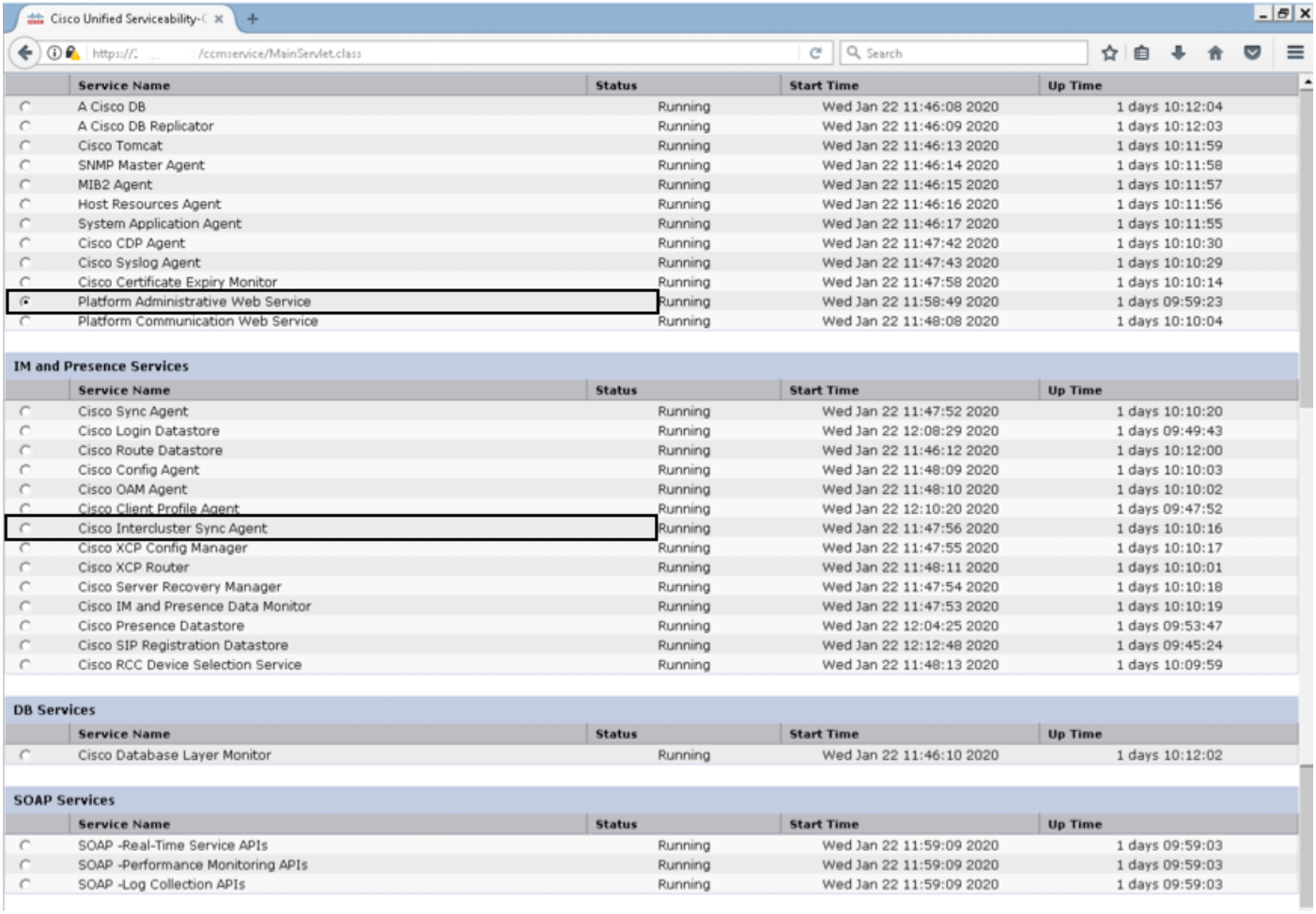
Schritt 1: Navigieren Sie zu **Cisco Unified Serviceability > Tools > Control Center - Network Services.**



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



Schritt 3: Fall von IM und Presence Server Stopp **Platform Administration Web Services** und **Cisco Intercluster Sync Agent**



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.

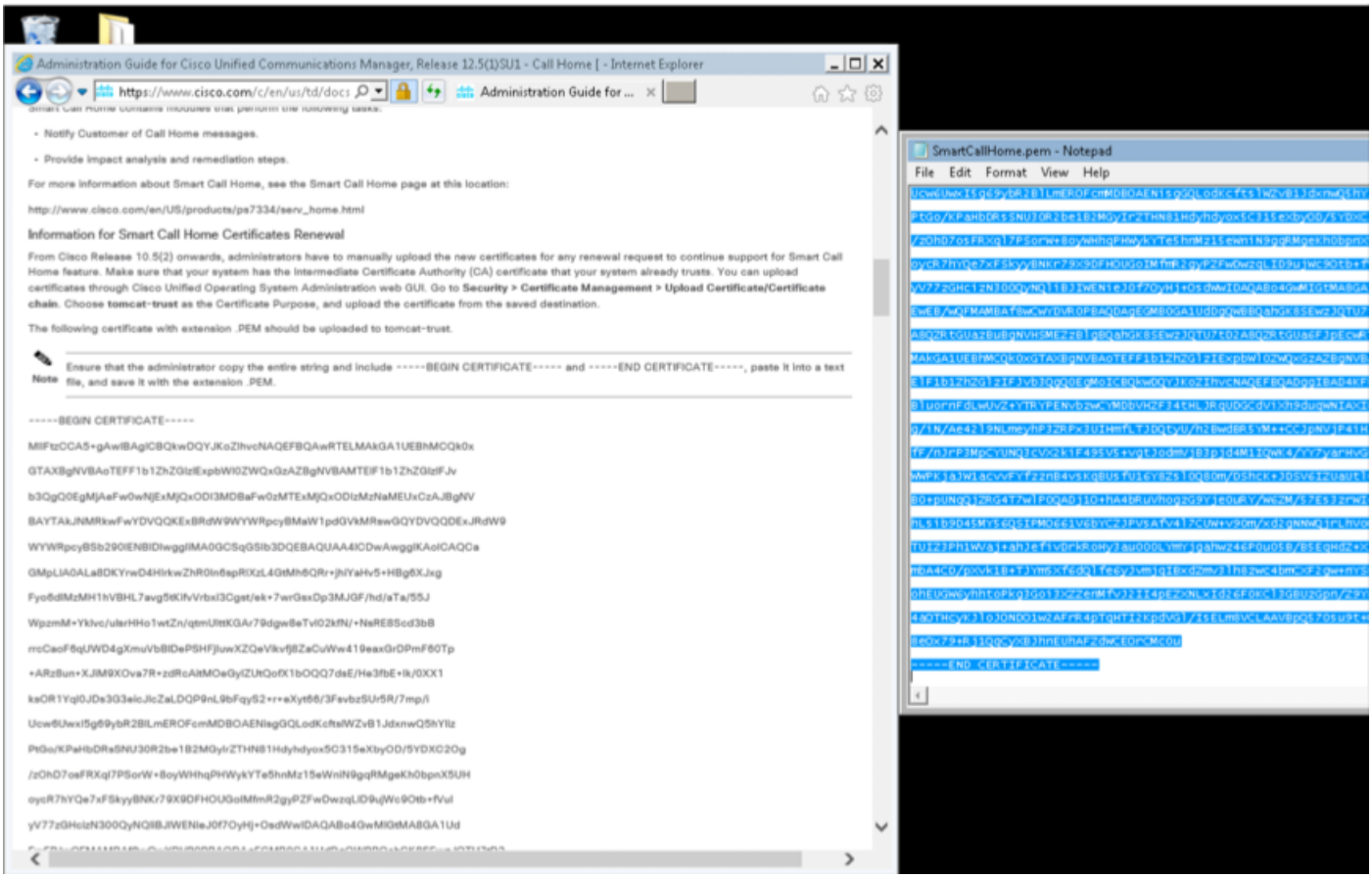
Schritt 5: Starten Sie den Dienst, der in Schritt 2 beendet wurde. und Schritt 3.

> **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

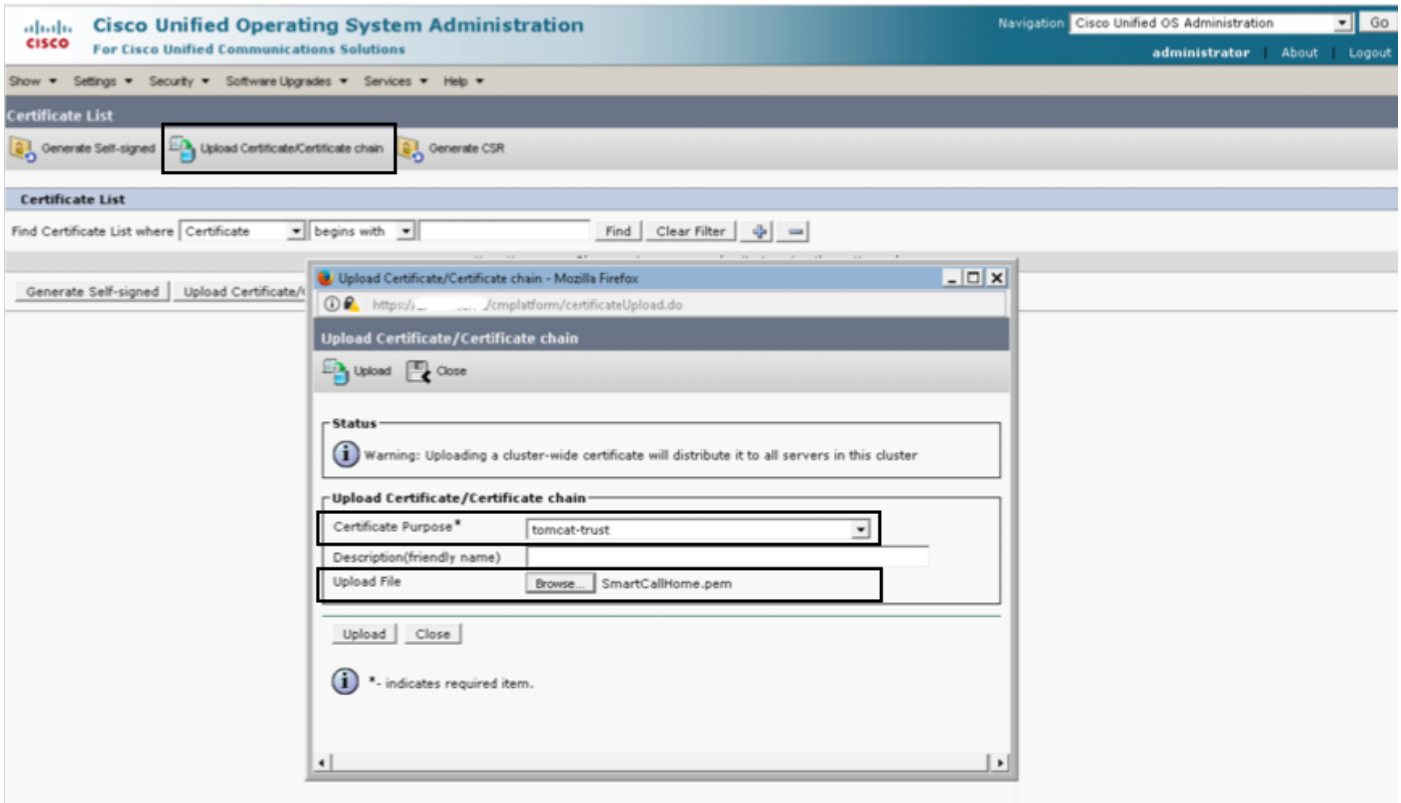
Wenn Smart Call Home deaktiviert ist, ist nach dem Löschen des Zertifikats keine weitere Aktion erforderlich. Wenn Smart Call Home aktiviert ist, gehen Sie wie folgt vor

Schritt 1: Kopieren Sie den Zertifikatsinhalt aus den *Smart Call Home-Zertifikaten im* UCM-Administrationsleitfaden.



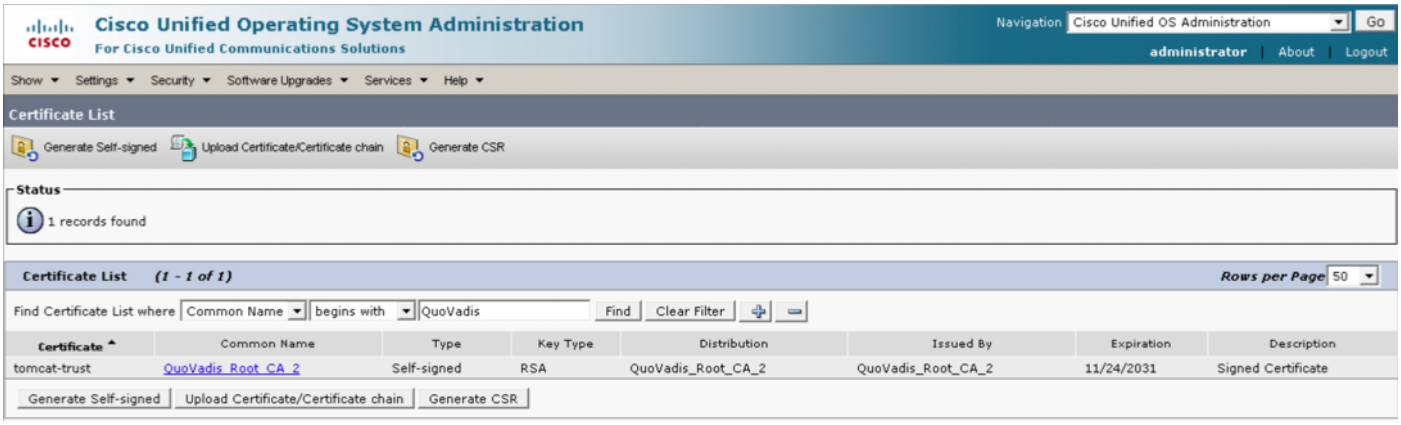
Hinweis: Das gleiche Zertifikat gilt für Version 10.5 und höher.

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.



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.