

Resolución de problemas de la alerta de vencimiento del certificado de Smart Call Home Certificate en productos de colaboración

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Problema](#)

[Solución](#)

[Solución alternativa para 11.0\(1\) y versiones posteriores](#)

[Para todas las demás versiones](#)

[Procedimiento de renovación de certificados Smart Call Home](#)

[Para Cisco Prime License Manager](#)

[Para Prime License Manager 10.5](#)

[Para Prime License Manager 11.5](#)

Introducción

Este documento describe las soluciones para la alerta de caducidad de certificados del certificado de Verisign(VeriSign_Class_3_Secure_Server_CA_-_G3.der) proporcionado para Smart Call Home que caduca en febrero de 2020 en los siguientes productos de Cisco Unified Collaboration que se tratan en este documento.

Cisco Unified Communications Manager (UCM)
Edición de administración de sesiones de Cisco Unified Communications Manager
Servicio de mensajería instantánea y presencia (CUPS) de Cisco
Cisco Unity Connection
Cisco Finesse
Cisco SocialMiner
Cisco MediaSense
Cisco Unified Contact Center Express
Cisco Unified Intelligence Center (CUIC)
Navegador de voz virtualizado de Cisco
Cisco Prime License Manager

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

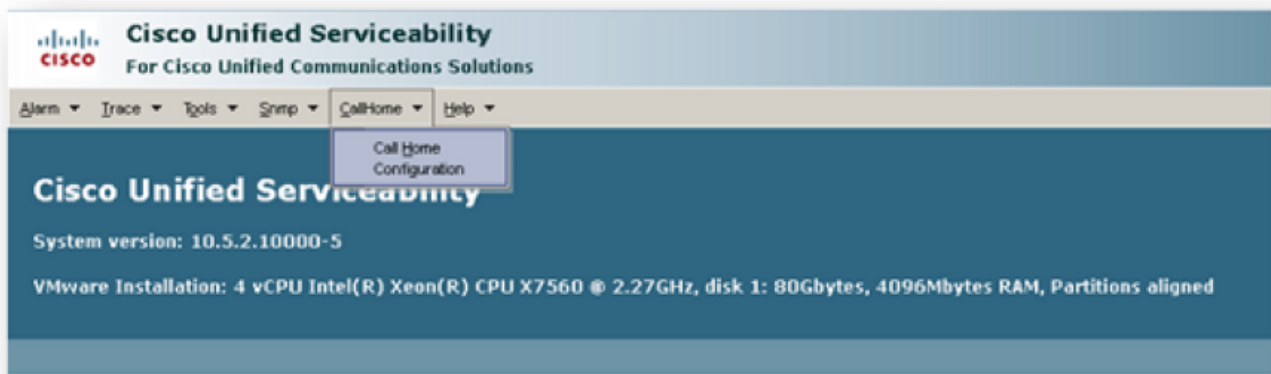
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Antecedentes

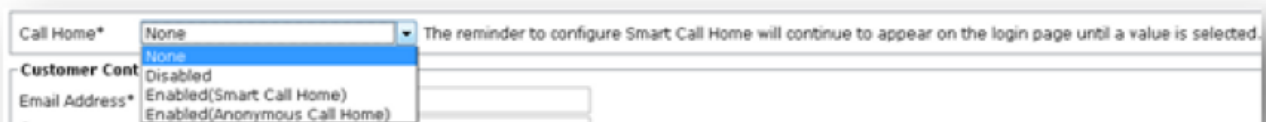
Smart Call Home es una función de soporte automatizado que supervisa los dispositivos Cisco de su red. La función Call Home permite comunicar y enviar las alertas de diagnóstico, el inventario y otros mensajes al servidor de respaldo de Smart Call Home.

Utilice esta sección para verificar si Smart Call Home está habilitado

Paso 1. En la página Serviciabilidad de Cisco Unified, elija CallHome > Configuration.



Paso 2. Compruebe si el campo Call Home está establecido en Disabled (Desactivado) o Enabled (Activado)



Problema

El certificado VeriSign(VeriSign_Class_3_Secure_Server_CA_-_G3.der) proporcionado de forma predeterminada como certificado de confianza de tomcat para Smart Call Home en Cisco Unified Collaboration Products caducará en febrero de 2020. A continuación se muestra la siguiente alerta de vencimiento:

```
%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]
```

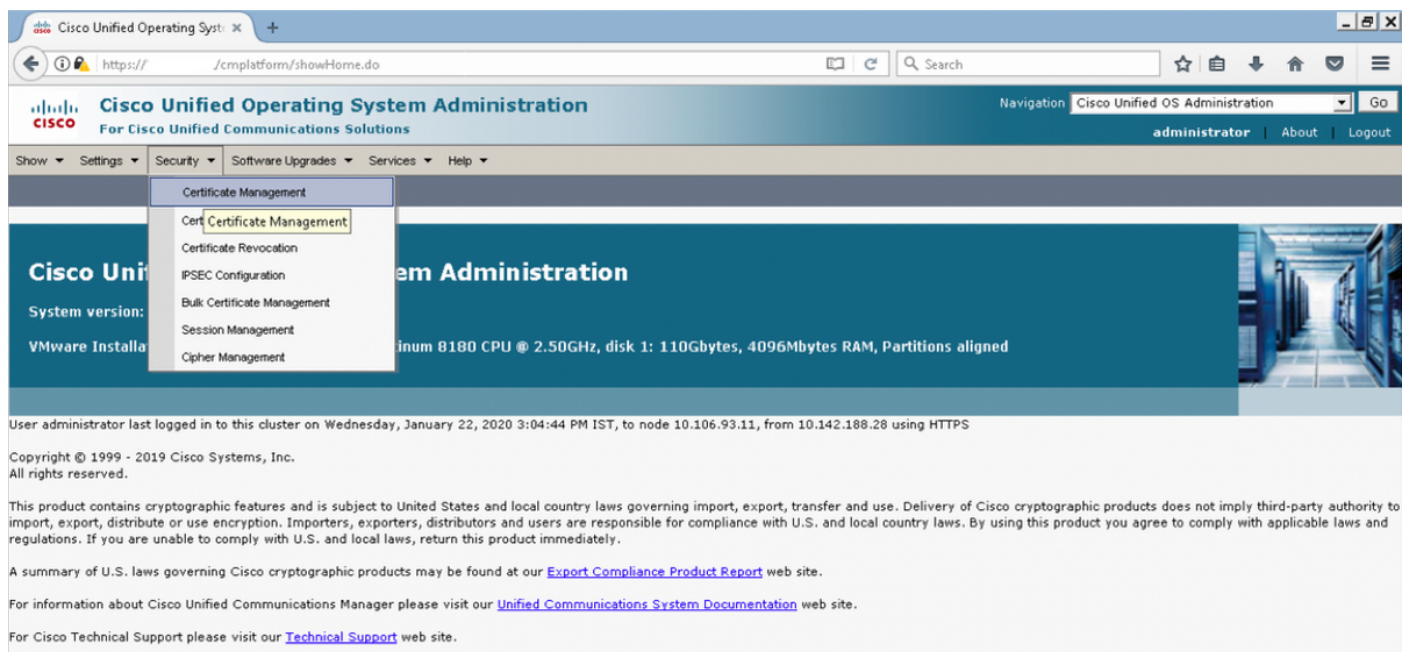
Solución

Este problema se documenta con el ID de bug de Cisco [CSCvs64158](#) .

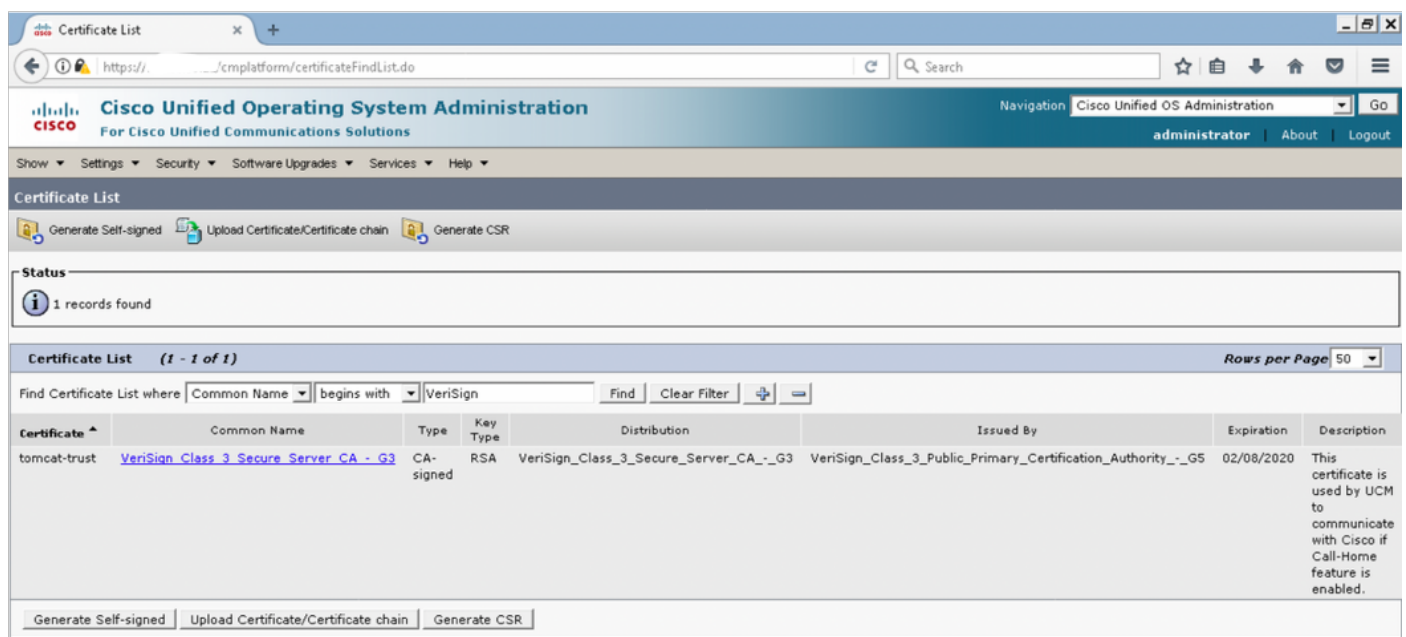
Solución alternativa para 11.0(1) y versiones posteriores

Debemos realizar los pasos siguientes para eliminar el certificado caducado (VeriSign_Class_3_Secure_Server_CA_-_G3.der)

Paso 1. Vaya a la GUI de administración de Cisco Unified OS en el editor y haga clic en **Seguridad > Administración de certificados**

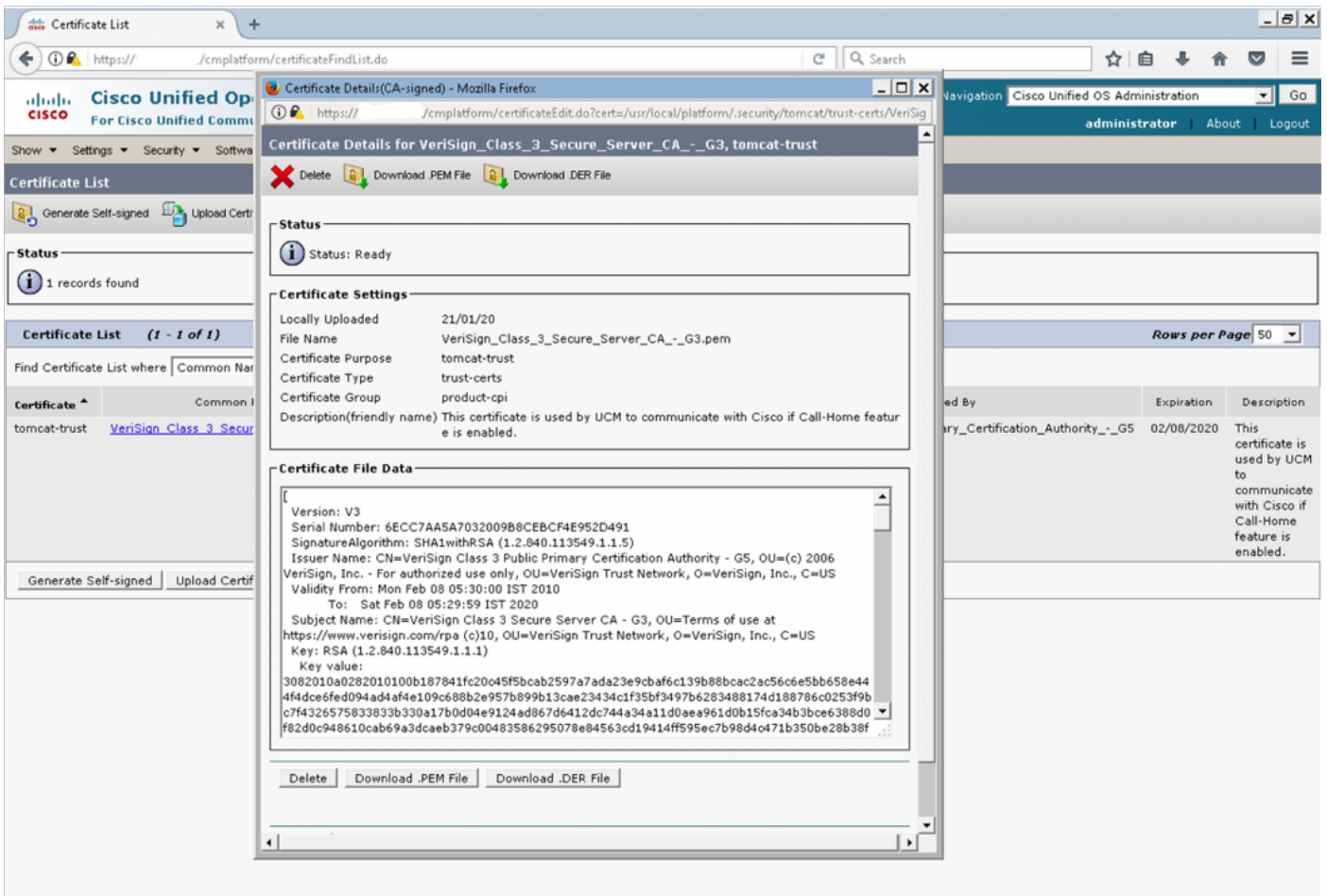


Paso 2. Buscar lista de certificados donde el nombre común contiene VeriSign

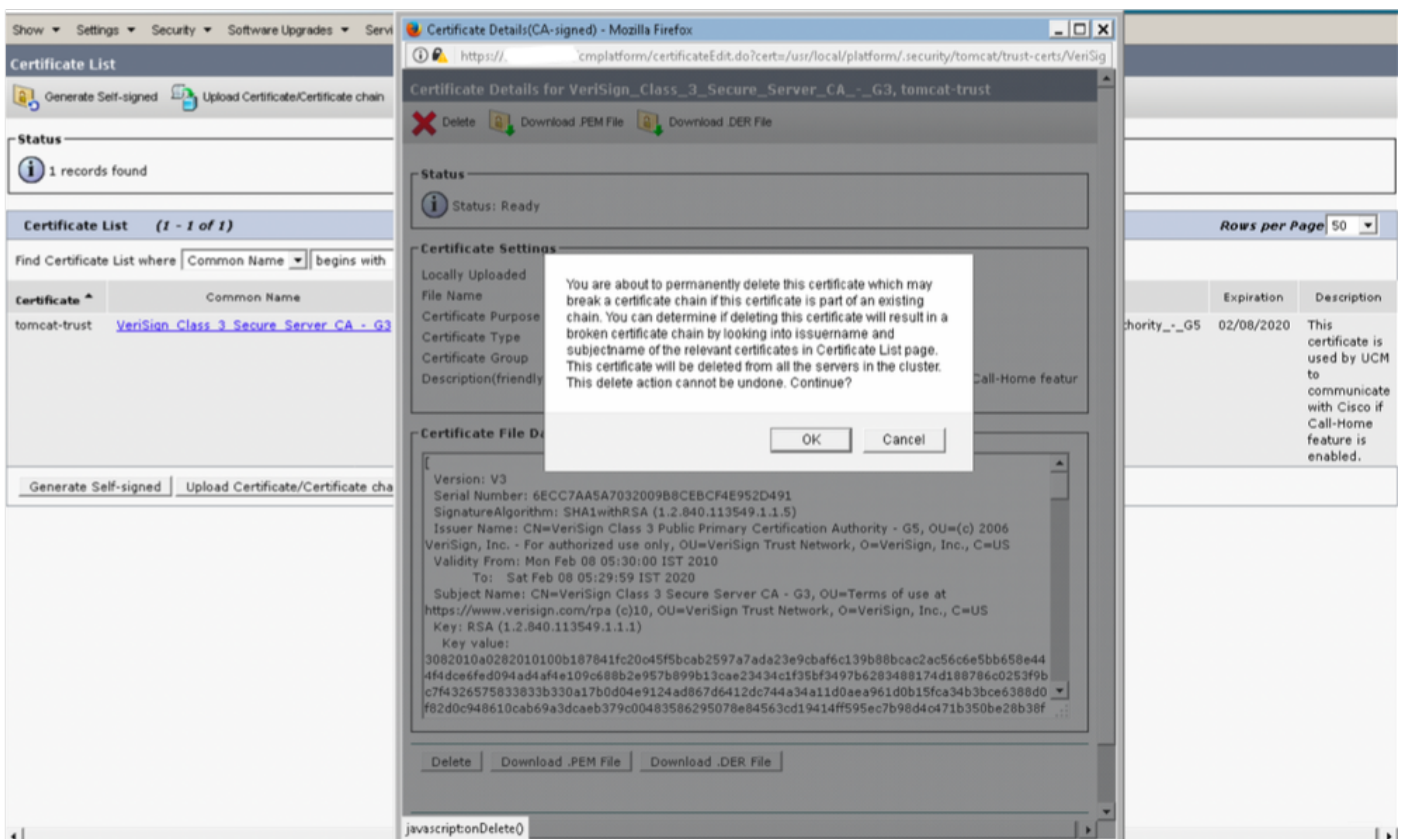


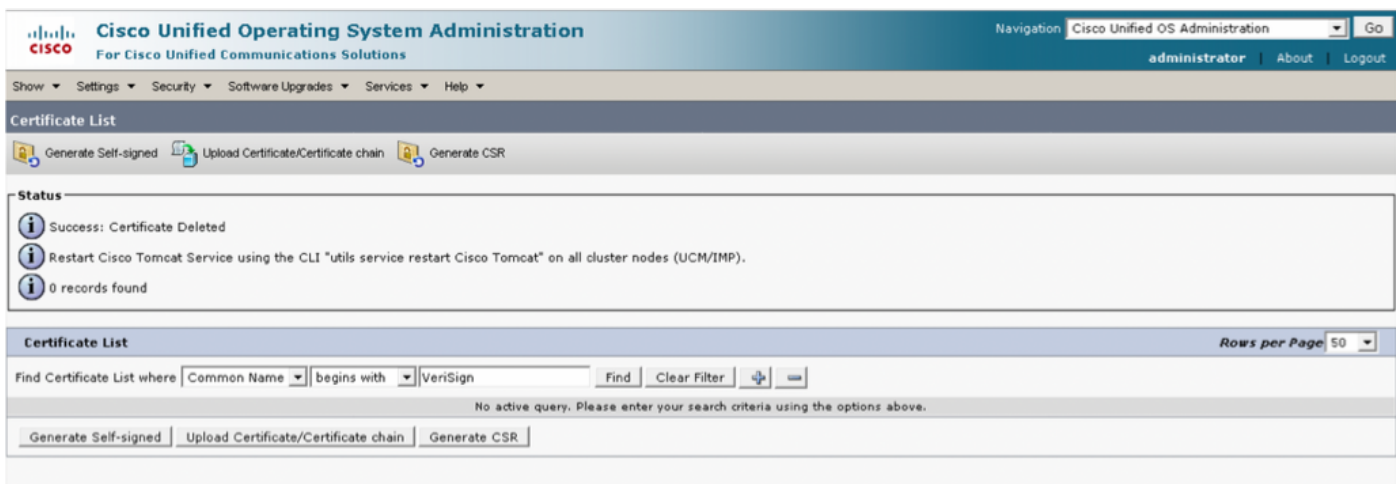
Paso 3. Haga clic en [VeriSign_Class_3_Secure_Server_CA_-_G3](#) y verá la ventana emergente

que resalta los detalles del certificado



Paso 4. Haga clic en el botón **Eliminar** y se le pedirá advertencia Haga clic en **Aceptar**. El certificado debe eliminarse de todos los nodos del clúster.





Para todas las demás versiones

Necesitamos realizar los siguientes pasos antes de eliminar el certificado

Paso 1. Vaya a **Serviciabilidad de Cisco Unified > Herramientas > Control Center - Servicios de red**



Paso 2. Detener **notificación de cambio de certificado de Cisco** en todos los nodos del clúster



Paso 3. En caso de IM and Presence Server Stop **Platform Administration Web Services** y **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

Paso 4. Elimine el certificado en todos los nodos, incluyendo IM y Presence, como se describe en Sección *Solución alternativa para 11.0(1) y superior* en este documento

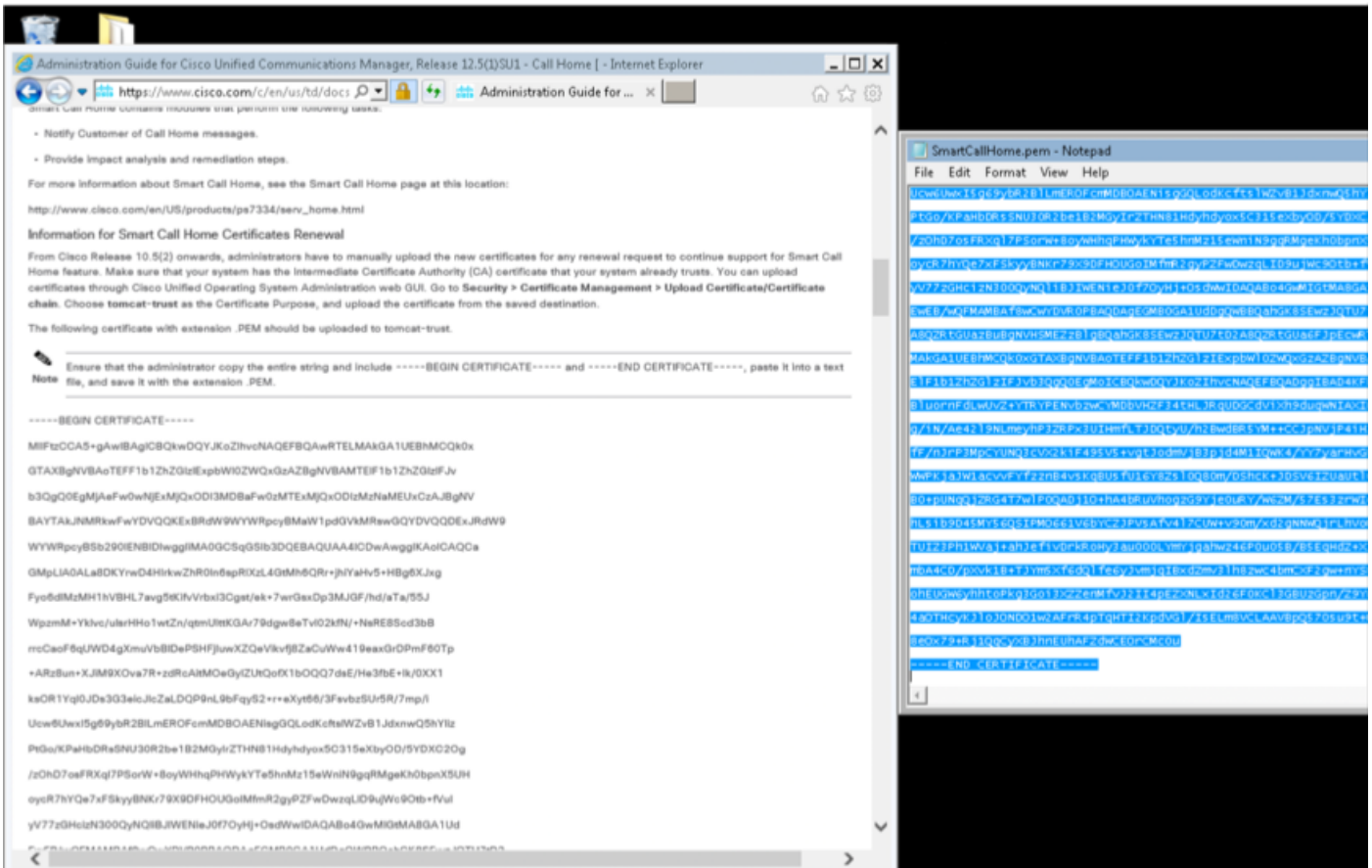
Paso 5. Inicie el servicio que se detuvo en el paso 2. y Paso 3.

Nota: Si elimina el certificado y realiza una actualización antes del 7 de febrero de 2020, el certificado volverá a aparecer después de la actualización y debe eliminarse de nuevo. Las actualizaciones posteriores al 7 de febrero de 2020 no volverán a agregar el certificado

Procedimiento de renovación de certificados Smart Call Home

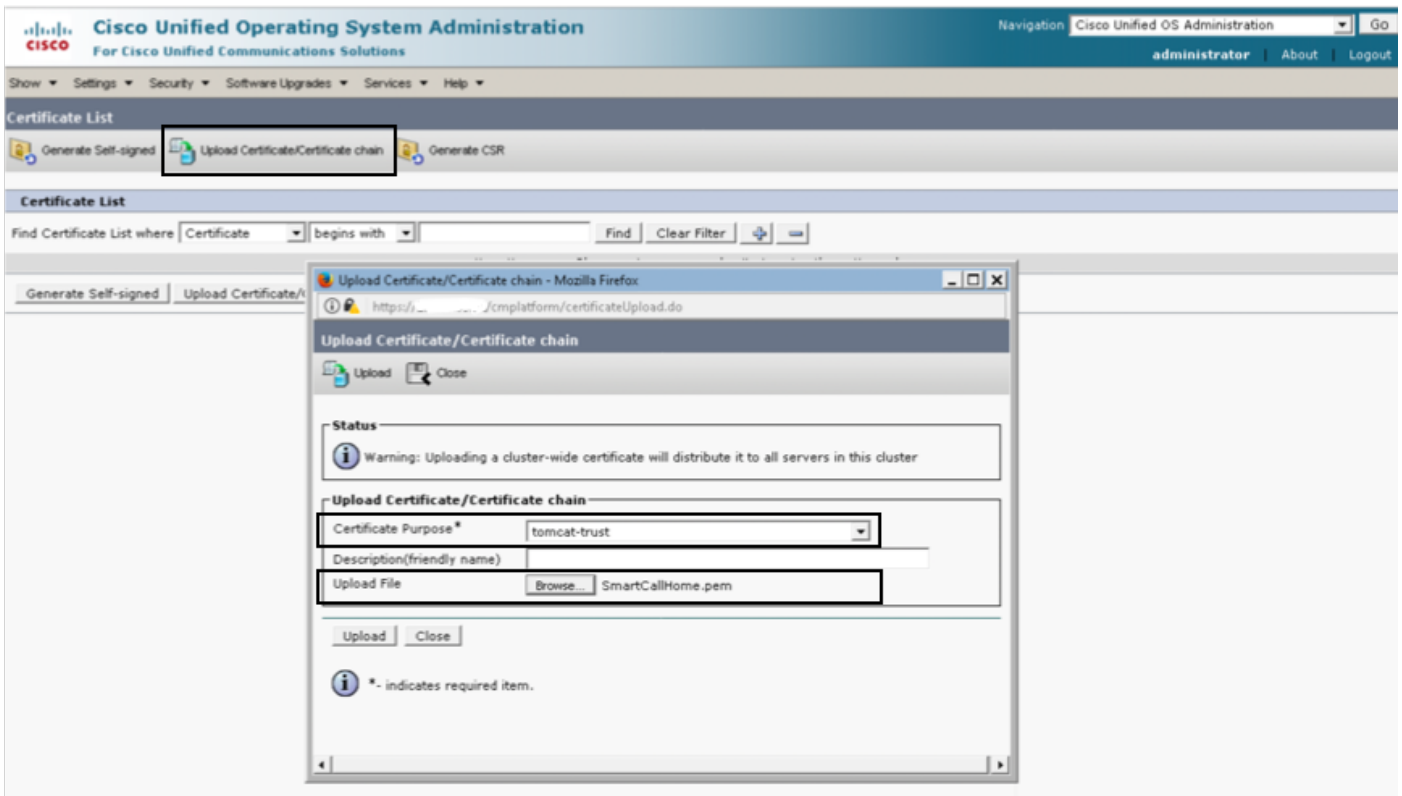
Si se desactiva Smart Call Home, no se requiere ninguna otra acción después de eliminar el certificado. Si Smart Call Home está activado, siga los pasos

Paso 1. Copie el contenido del certificado de la sección [Guía de administración de UCM Información para los certificados Smart Call Home](#)



Nota: El mismo certificado es válido para la versión 10.5 y posterior

Paso 2. Cargue el archivo .pem como tomcat-trust en la página GUI de administración de certificados de Cisco Unified OS Administration por la captura de pantalla



Paso 3. Verifique que QuoVadis_Root_CA_2 aparezca como tomcat-trust al encontrar el

certificado donde Common Name contiene QuoVadis

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 with the common name "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".

Para Cisco Prime License Manager

Para Prime License Manager 10.5

El certificado caducado (VeriSign_Class_3_Secure_Server_CA_-_G3) se puede eliminar del sistema aplicando este archivo COP (ciscocm.plm-CSCvs64158_remove_sch_cert_C0050-1.k3.cop.sgn). Revise el archivo Léame para obtener instrucciones de instalación.

Para Prime License Manager 11.5

El certificado caducado (VeriSign_Class_3_Secure_Server_CA_-_G3) se puede eliminar del sistema aplicando este archivo COP (ciscocm.plm-CSCvs64158_remove_sch_cert_C0050-1.k3.cop.sgn). Revise el archivo Léame para obtener instrucciones de instalación.