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

Contenido

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

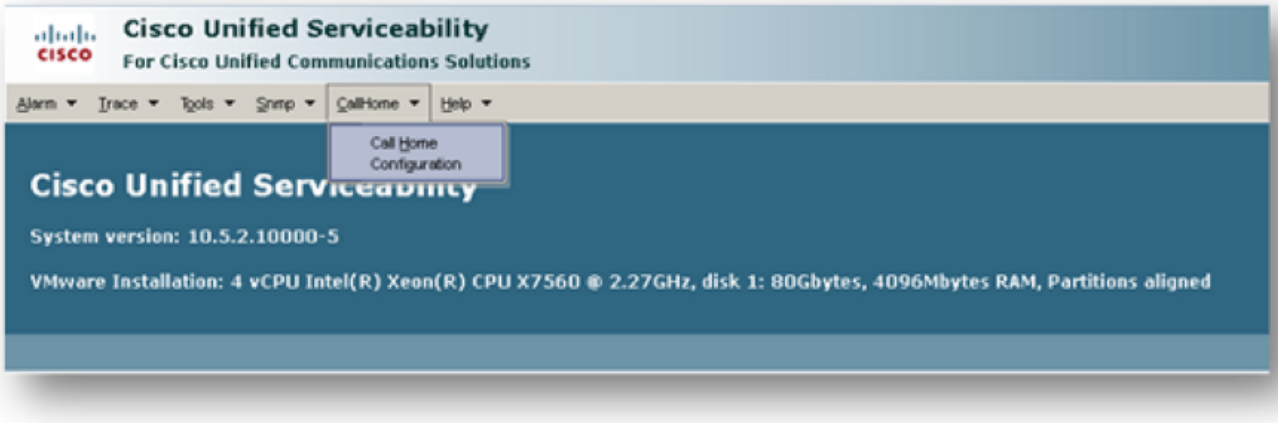
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Antecedentes

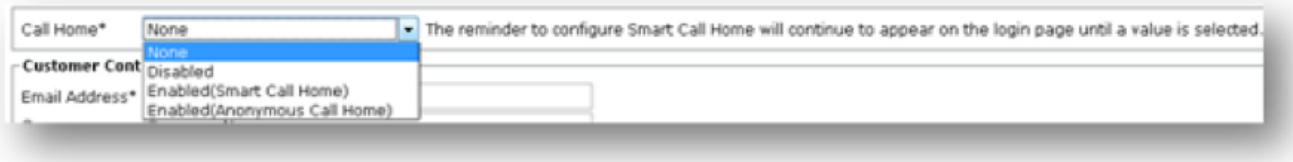
Smart Call Home es una función de soporte automatizado que supervisa los dispositivos Cisco de su red. La función Call Home permite comunicar y enviar las alertas de diagnóstico, el inventario y otros mensajes al servidor de respaldo de Smart Call Home.

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]
```

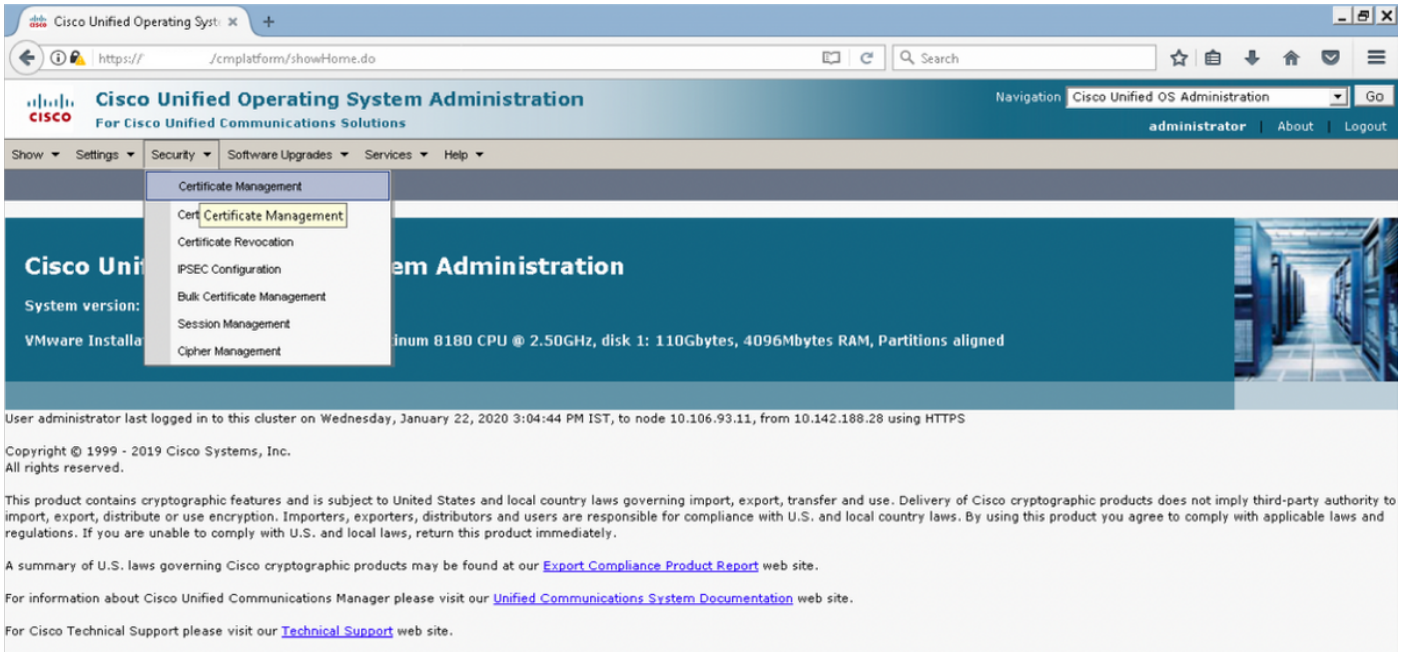
Solución

Este problema se documenta con el ID de bug de Cisco CSCvs64158 .

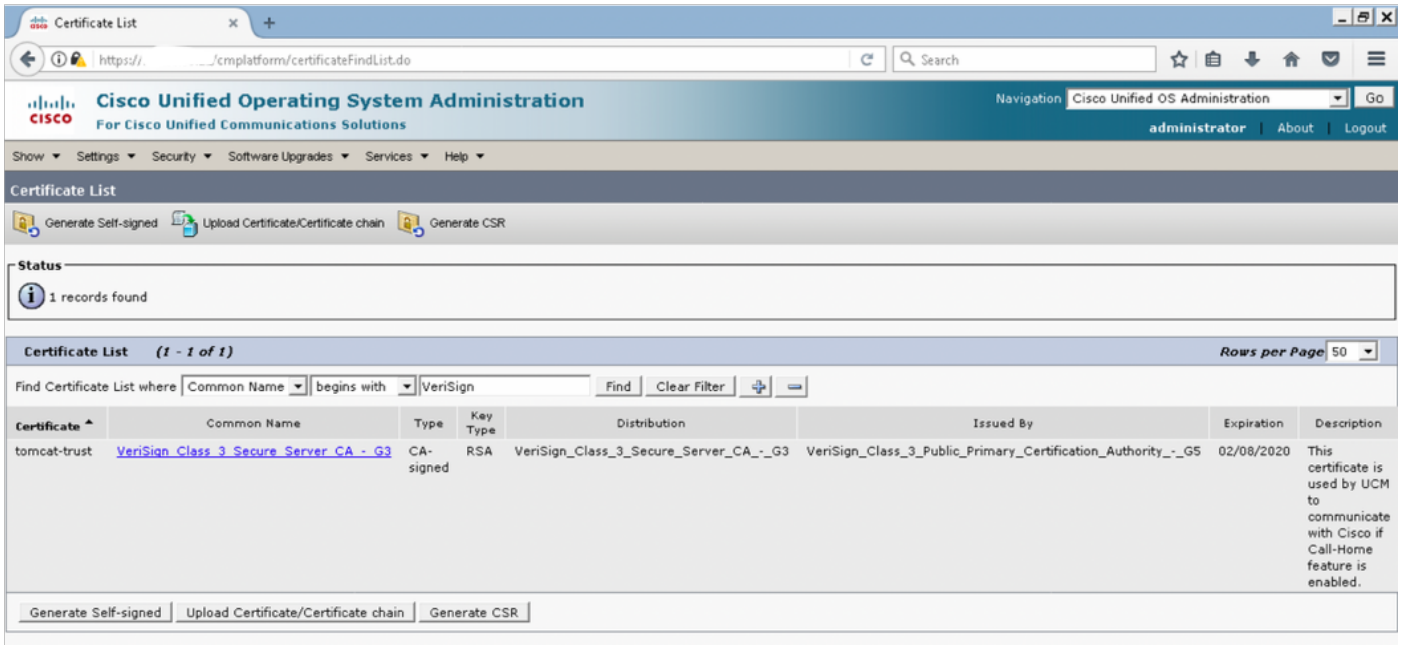
Solución alternativa para 11.0(1) y versiones posteriores

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**

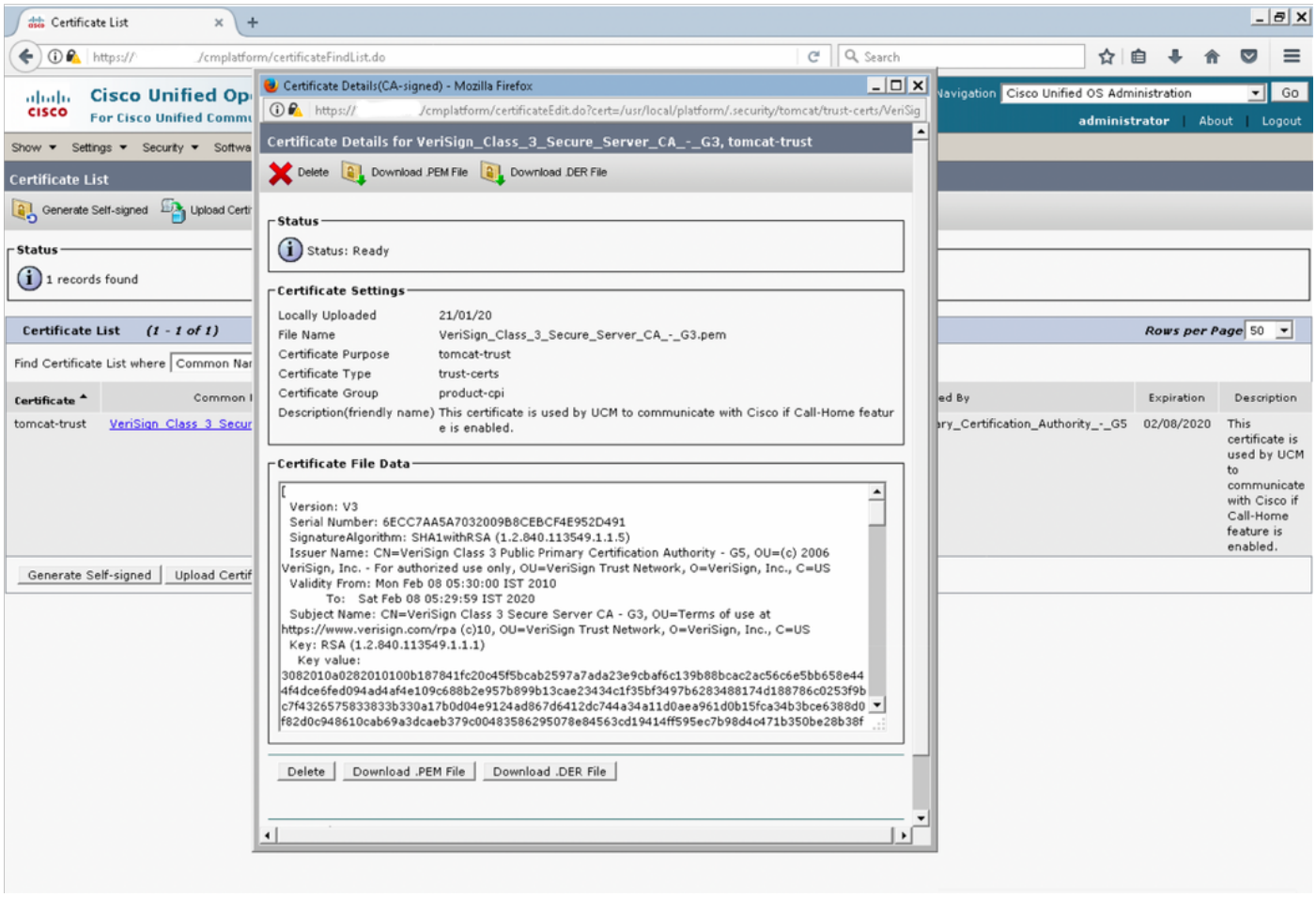


Paso 2. Buscar lista de certificados donde el nombre común contiene VeriSign

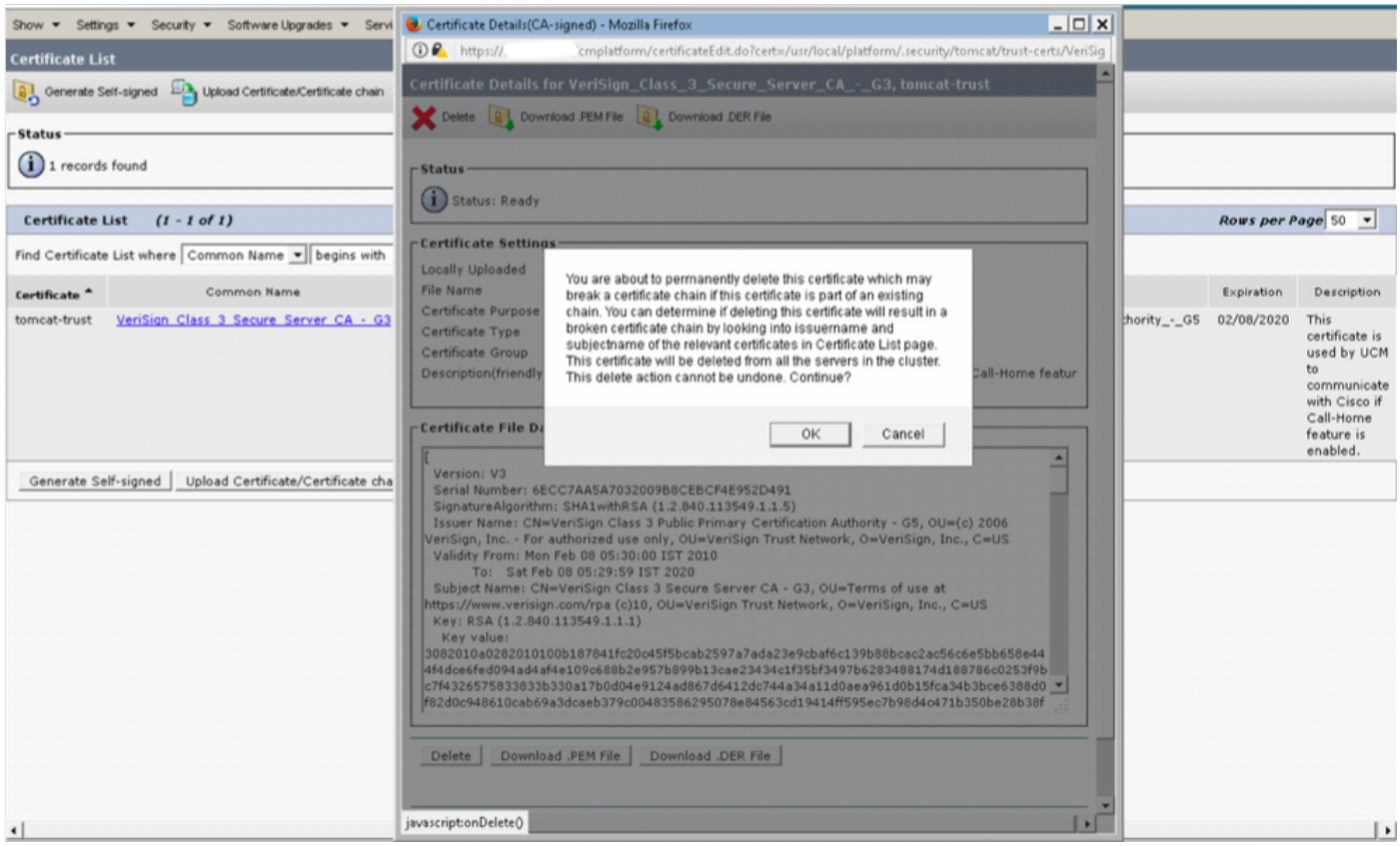


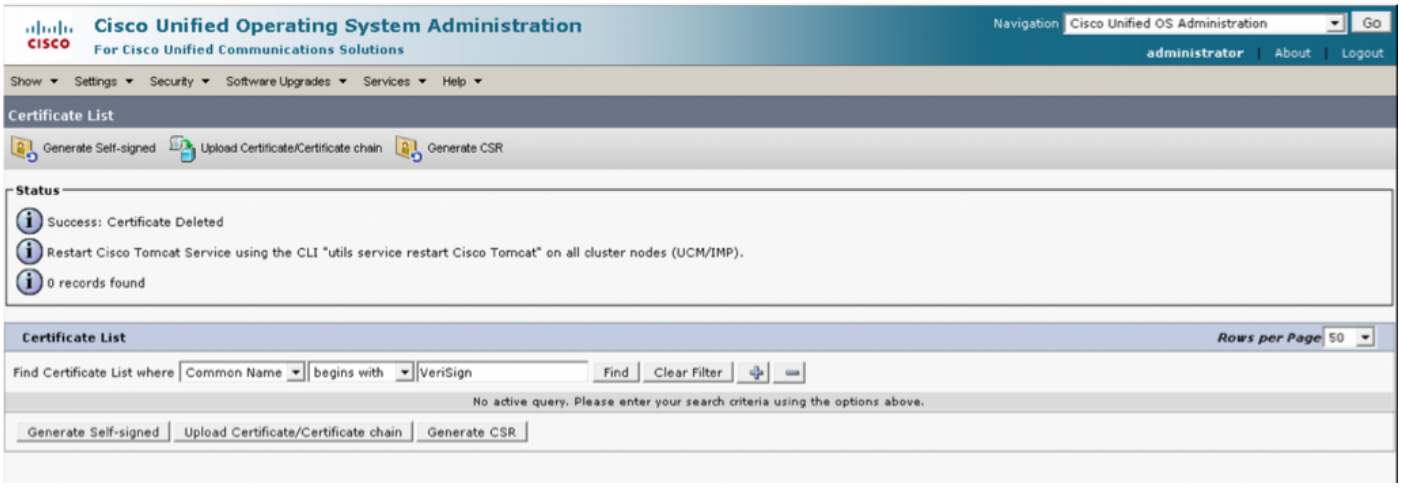
Paso 3. Haga clic en **VeriSign_Class_3_Secure_Server_CA_-_G3** y verá la ventana emergente

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.

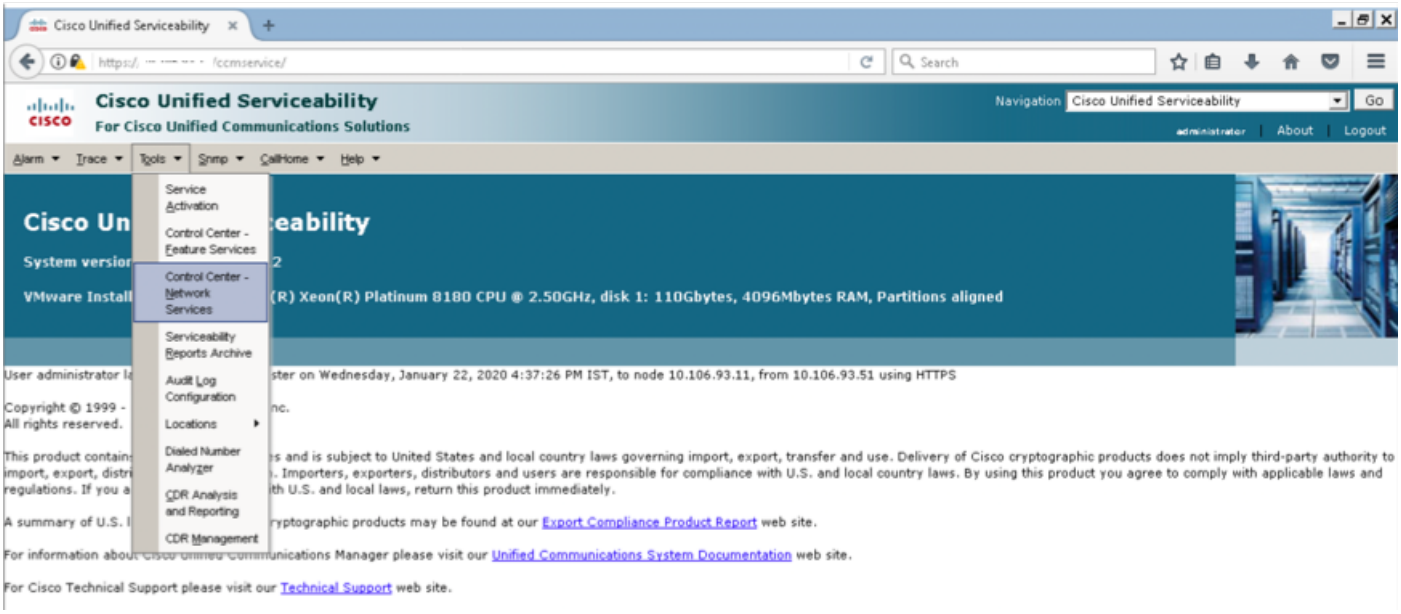




Para todas las demás versiones

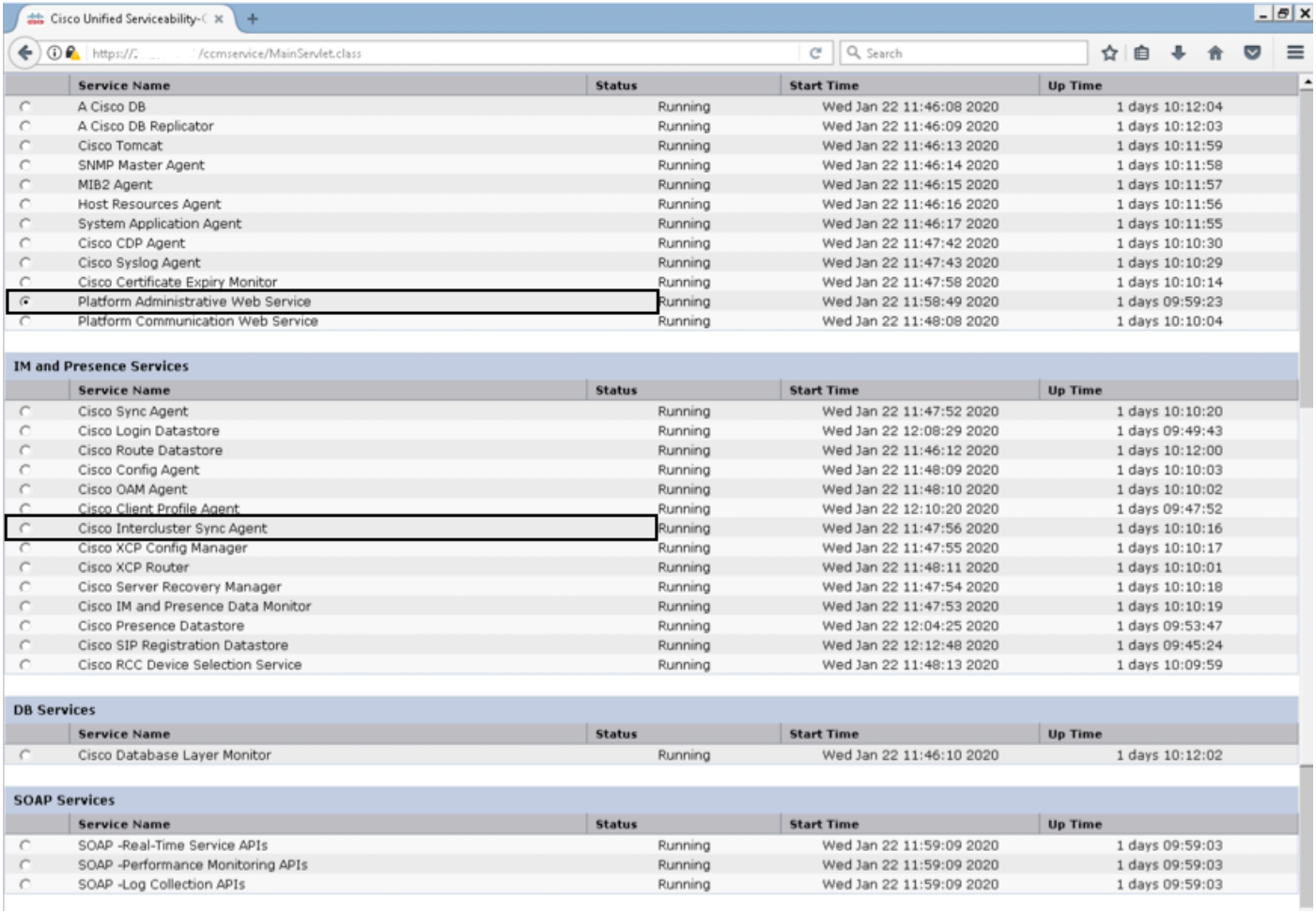
Necesitamos realizar los siguientes pasos antes de eliminar el certificado

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**



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

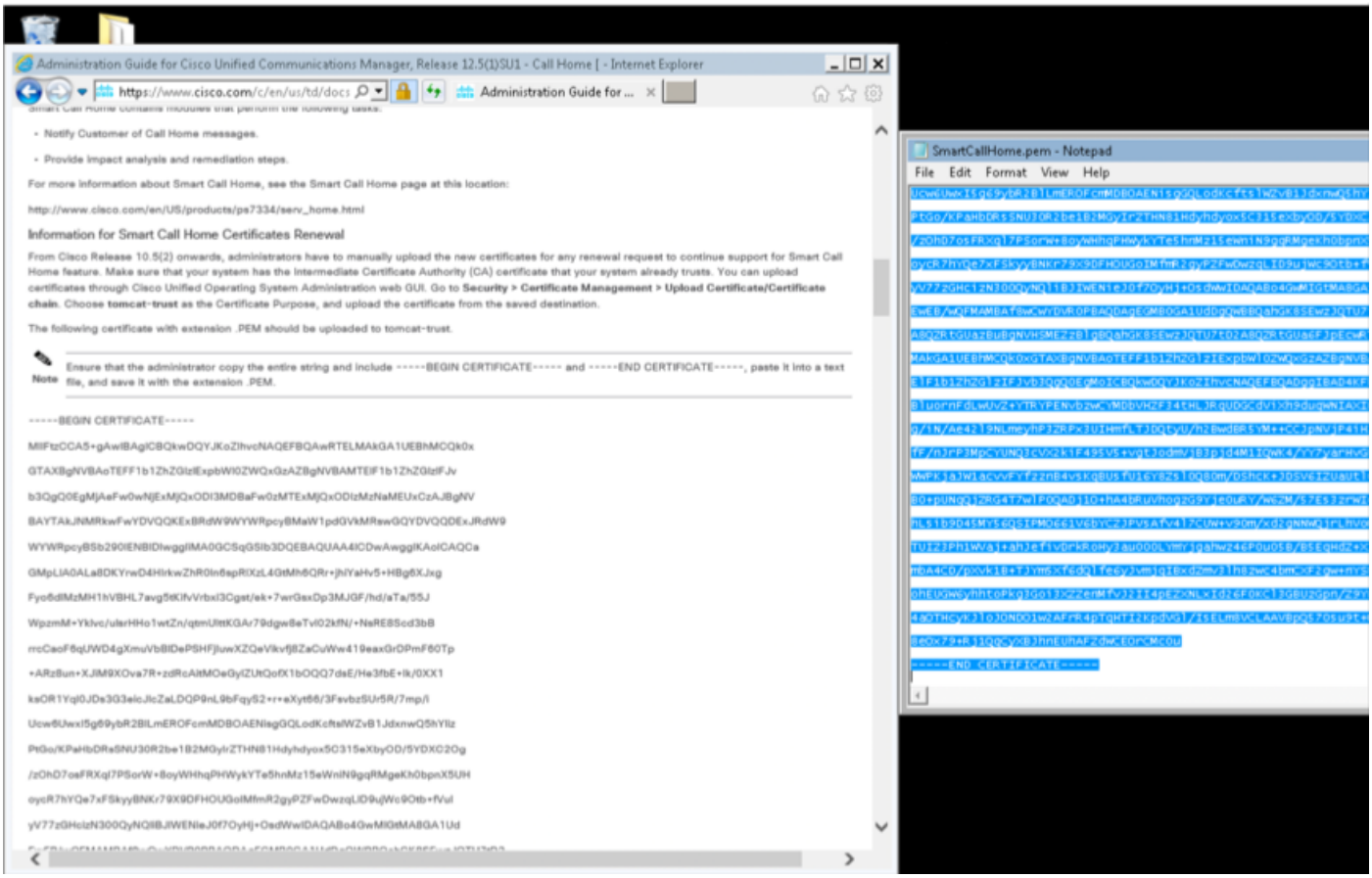
Paso 5. Inicie el servicio que se detuvo en el paso 2. y Paso 3.

> **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

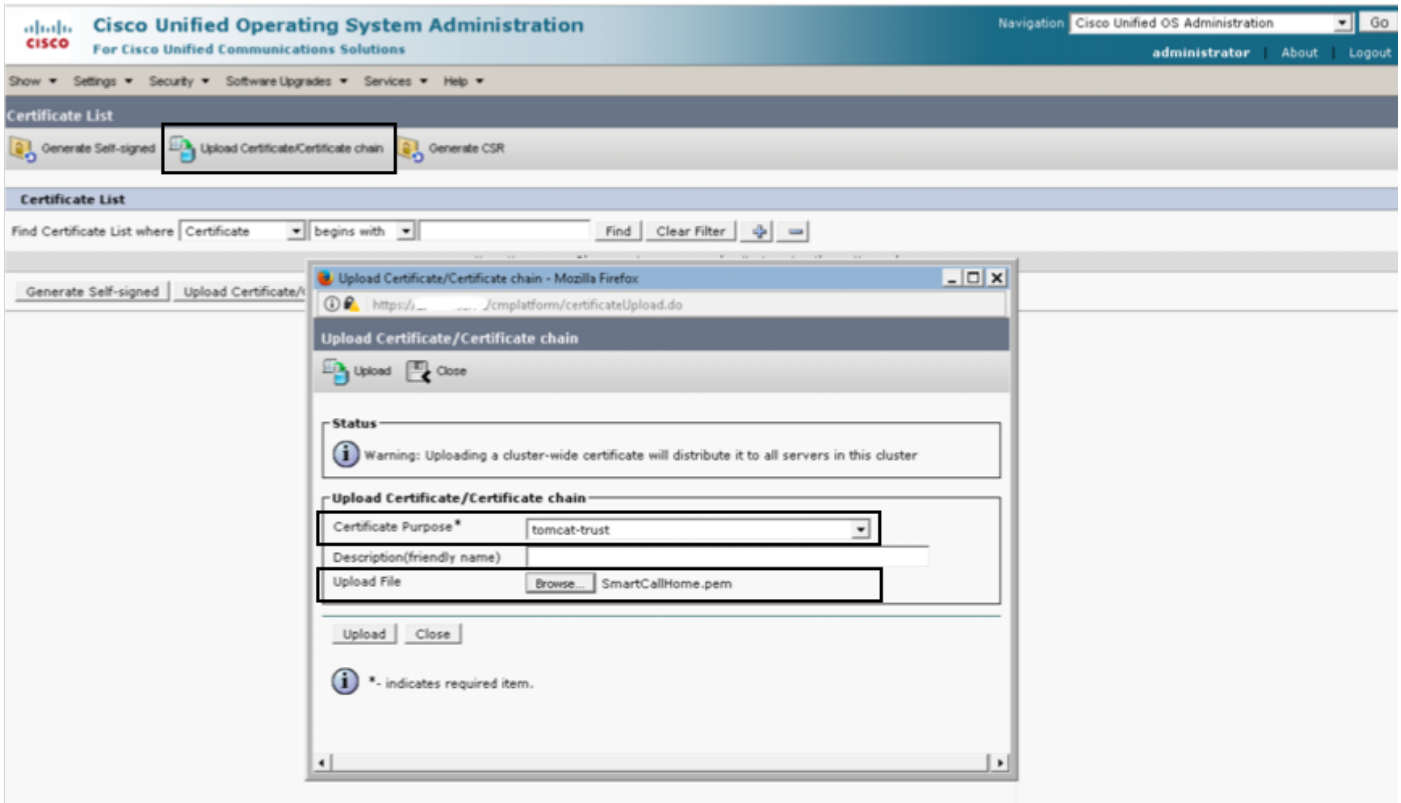
Si se desactiva Smart Call Home, no se requiere ninguna otra acción después de eliminar el certificado. Si Smart Call Home está activado, siga los pasos

Paso 1. Copie el contenido del certificado de la sección Guía de administración de UCM *Información para los certificados Smart Call Home*



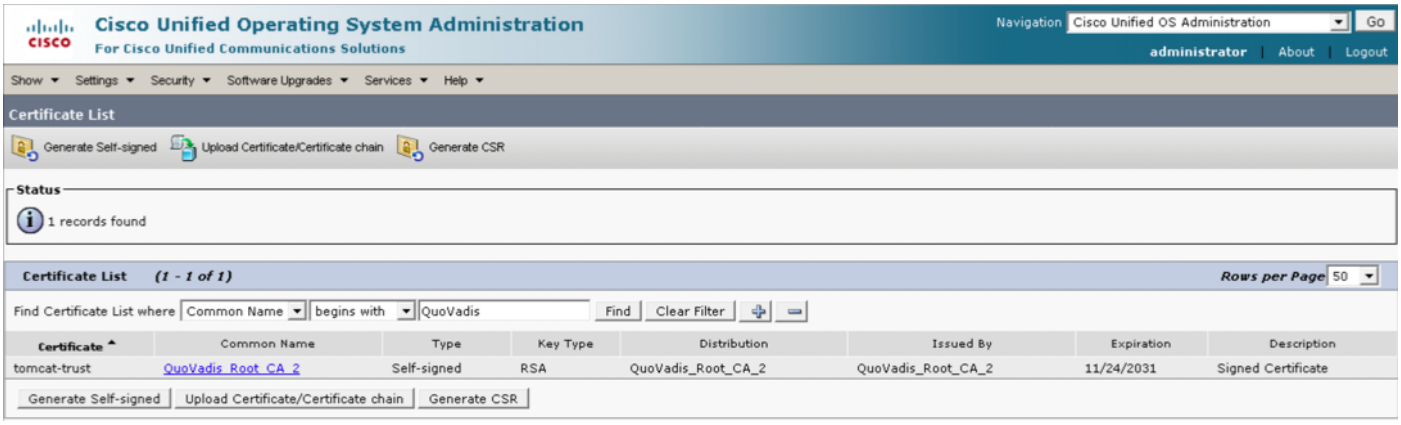
Nota: El mismo certificado es válido para la versión 10.5 y posterior

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



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.