Solução de problemas de alerta de expiração de certificado do Smart Call Home Certificate em produtos de colaboração

Contents

Introduction

Este documento descreve as soluções para alerta de expiração de certificado do certificado Verisign(VeriSign_Class_3_Secure_Server_CA_-_G3.der) fornecidas para o Smart Call Home, que expira em fevereiro de 2020 nos seguintes produtos Cisco Unified Collaboration que são abordados neste documento.

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)
Navegador de voz virtualizado da Cisco
Cisco Prime License Manager

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

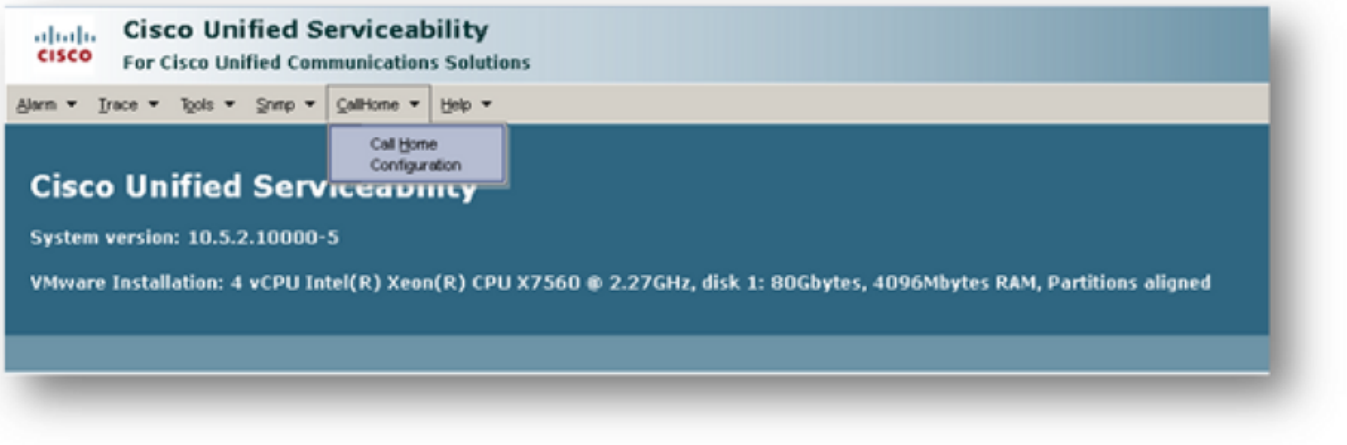
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informações de Apoio

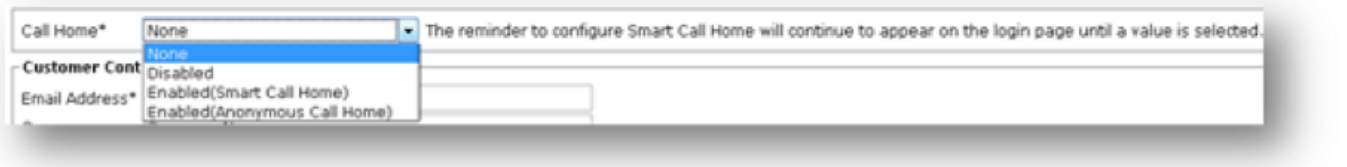
O Smart Call Home é um recurso de suporte automatizado que monitora os dispositivos da Cisco na sua rede. O recurso Call Home permite que você comunique e envie alertas de diagnóstico, inventário e outras mensagens para o servidor back-end do Smart Call Home.

Utilize esta seção para verificar se o Smart Call Home está ativado

Etapa 1. Na página Cisco Unified Serviceability, escolha CallHome > Configuration.



Etapa 2. Verifique se o campo Call Home está definido como Disabled (Desabilitado) ou Enabled (Habilitado)



Problema

O certificado VeriSign(VeriSign_Class_3_Secure_Server_CA_-_G3.der) fornecido por padrão como certificado tomcat-trust para Smart Call Home em produtos Cisco Unified Collaboration está definido para expirar em fevereiro de 2020. O seguinte alerta de expiração pode ser visto abaixo:

```
%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]
```

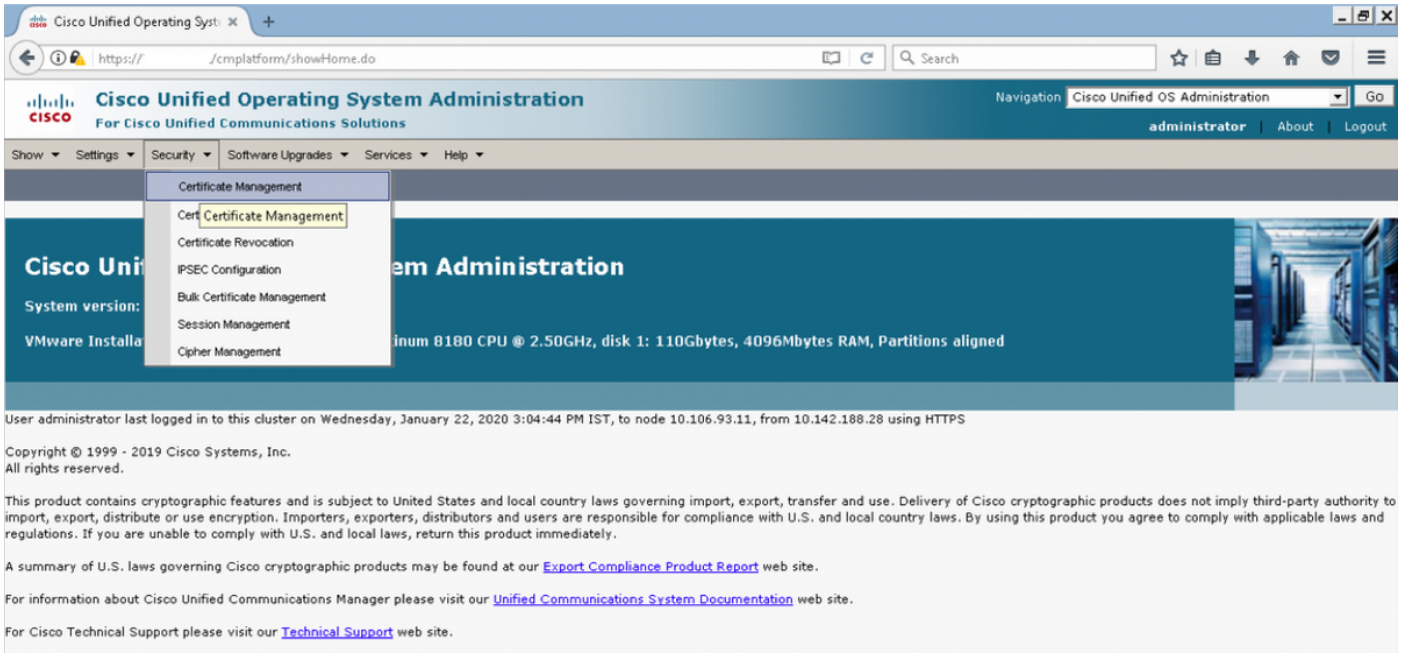
Solução

Esse problema é documentado pela ID de bug da Cisco CSCvs64158 .

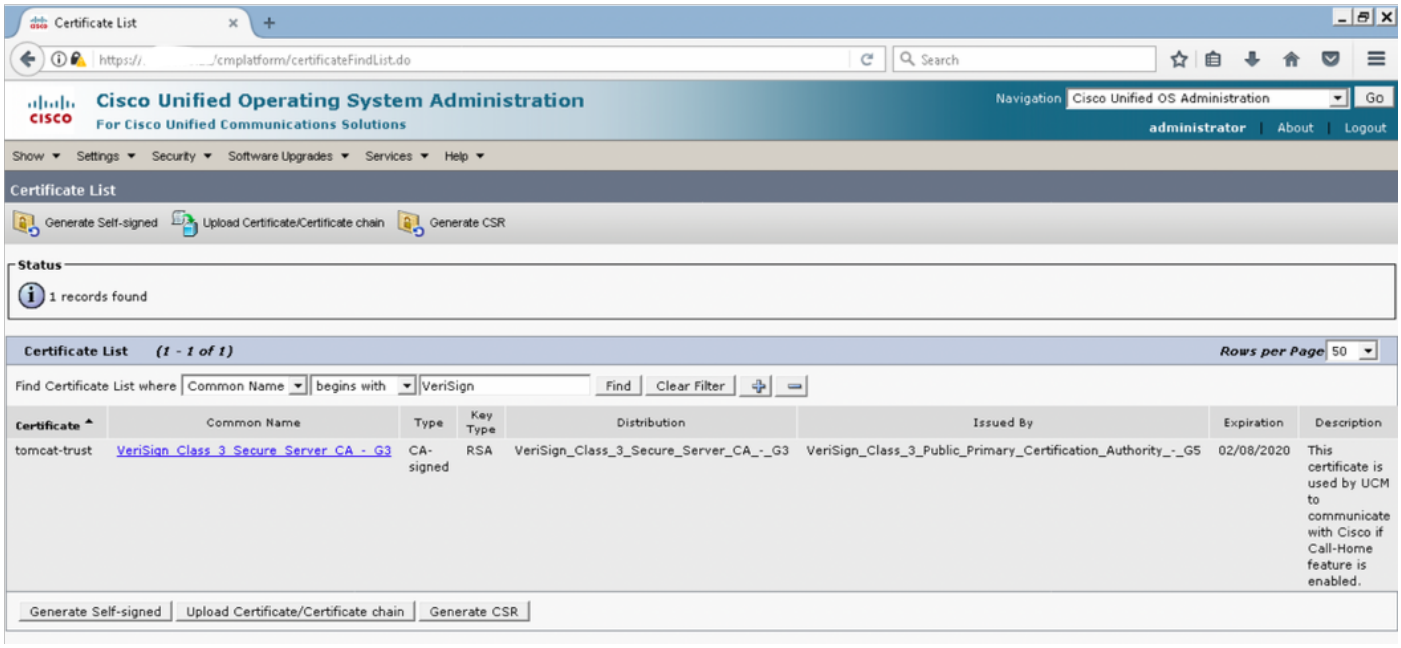
Solução alternativa para versões 11.0(1) e superiores

Precisamos executar as etapas abaixo para excluir o certificado expirado (VeriSign_Class_3_Secure_Server_CA_-_G3.der)

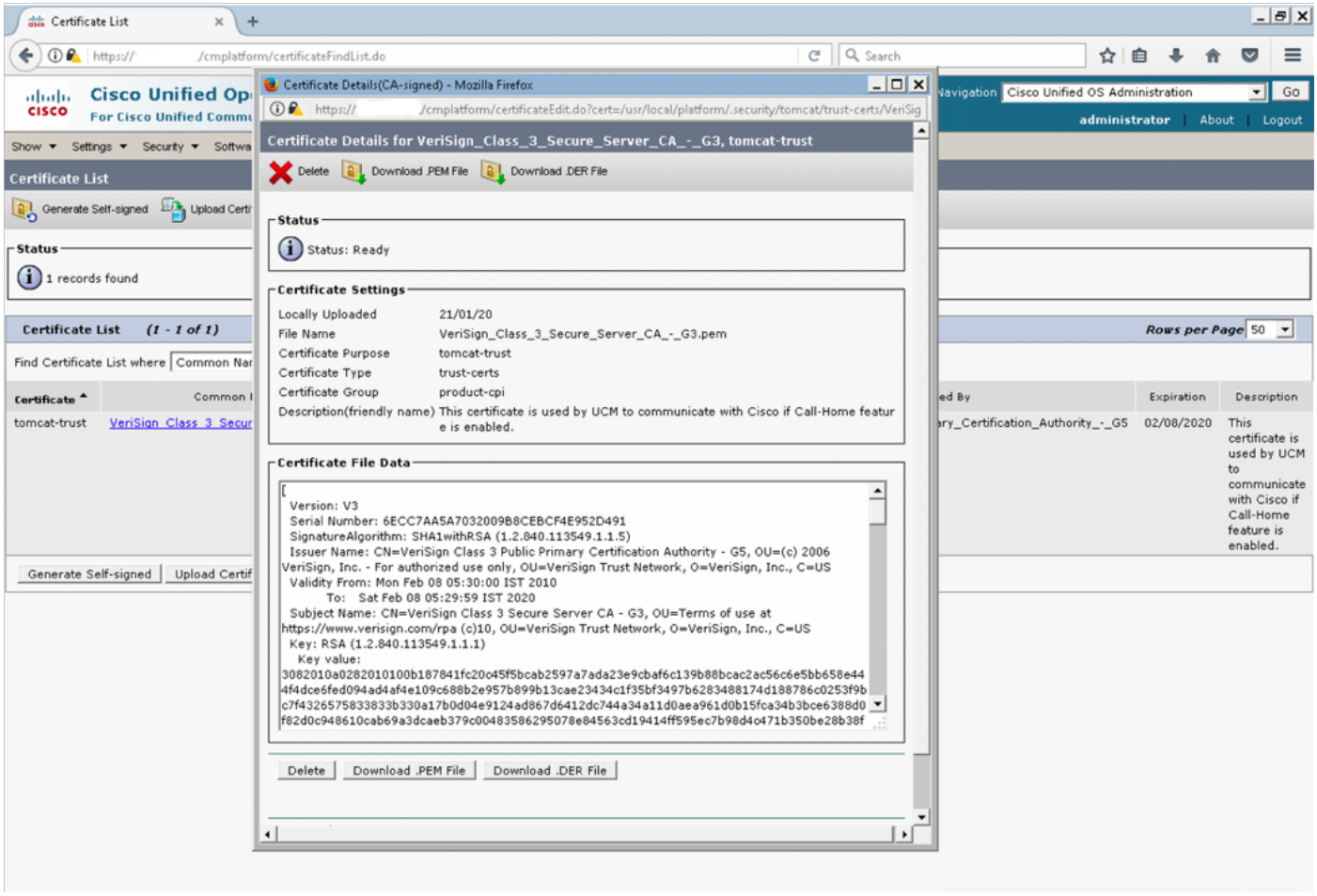
Etapa 1. Navegue até a GUI do Cisco Unified OS Administration no Publisher e clique em **Security > Certificate Management**



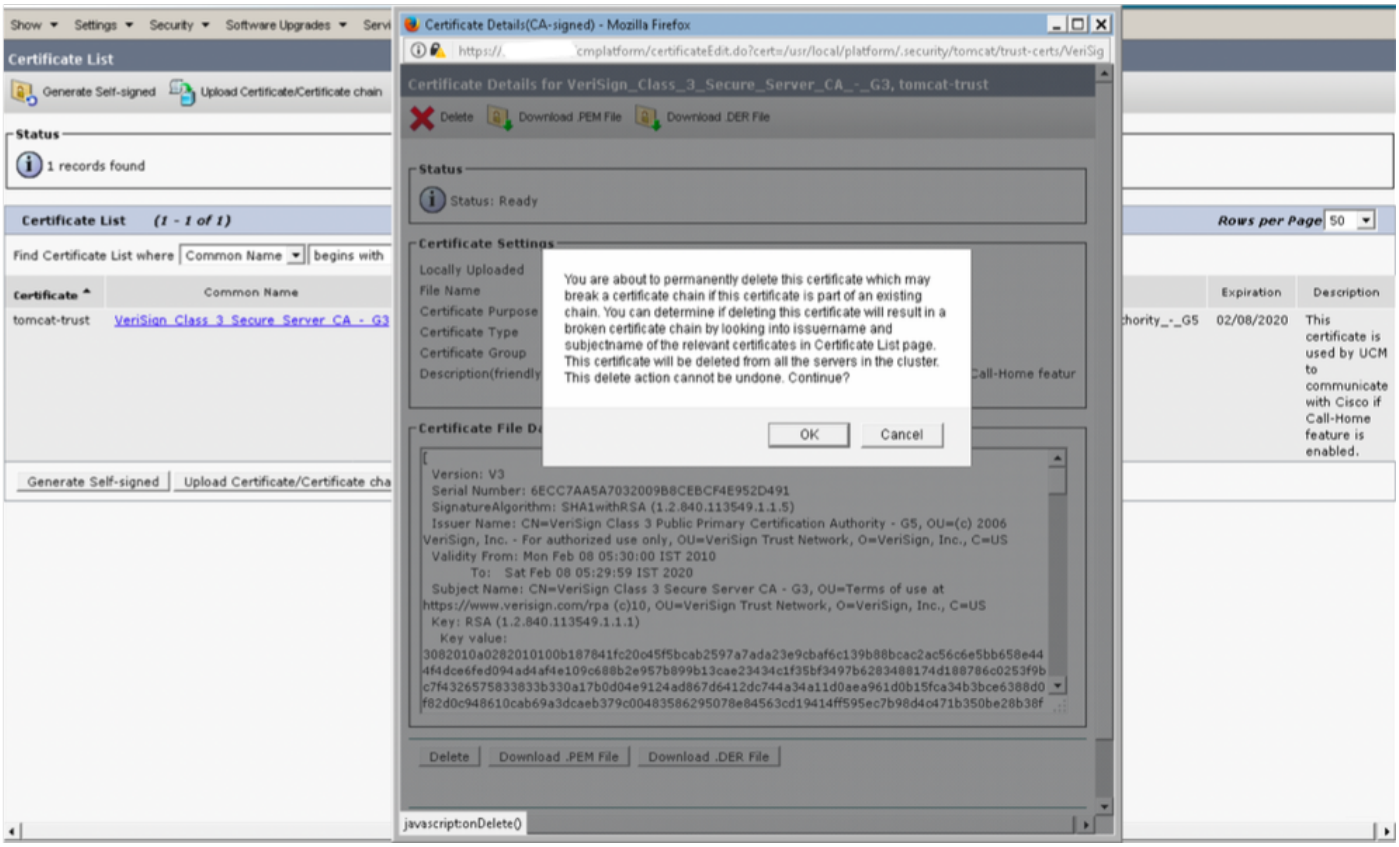
Etapa 2. Localizar lista de certificados onde o nome comum contém VeriSign

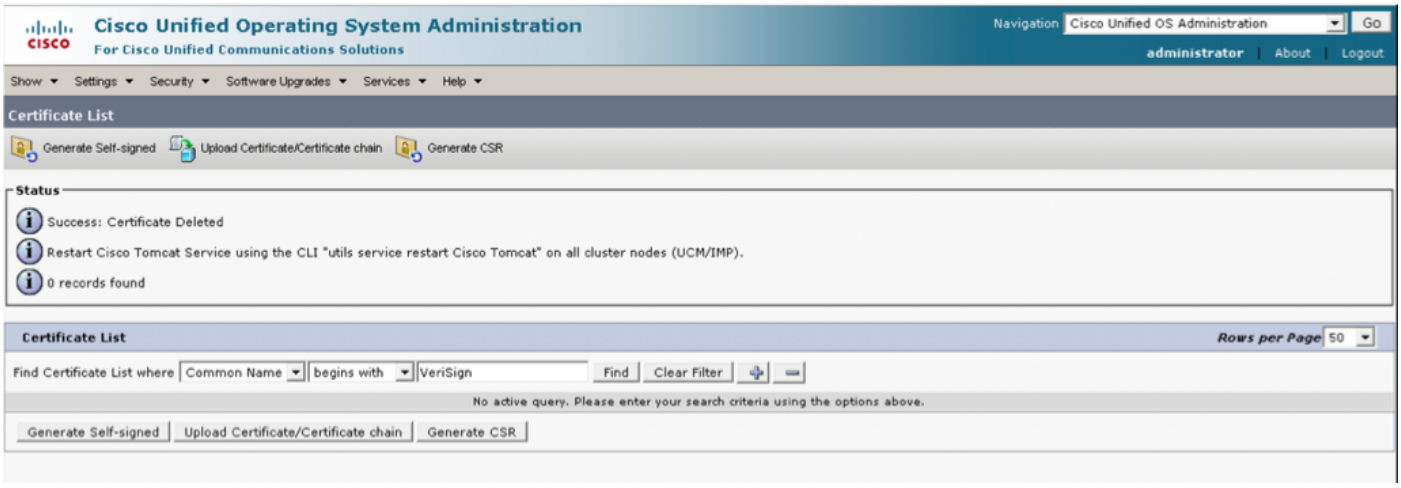


Etapa 3. Clique em **VeriSign_Class_3_Secure_Server_CA_-_G3** e você verá a janela pop-up destacando os detalhes do certificado



Etapa 4. Clique no botão **Excluir** e, em seguida, clique em **OK**. O certificado deve ser excluído de todos os nós no cluster.

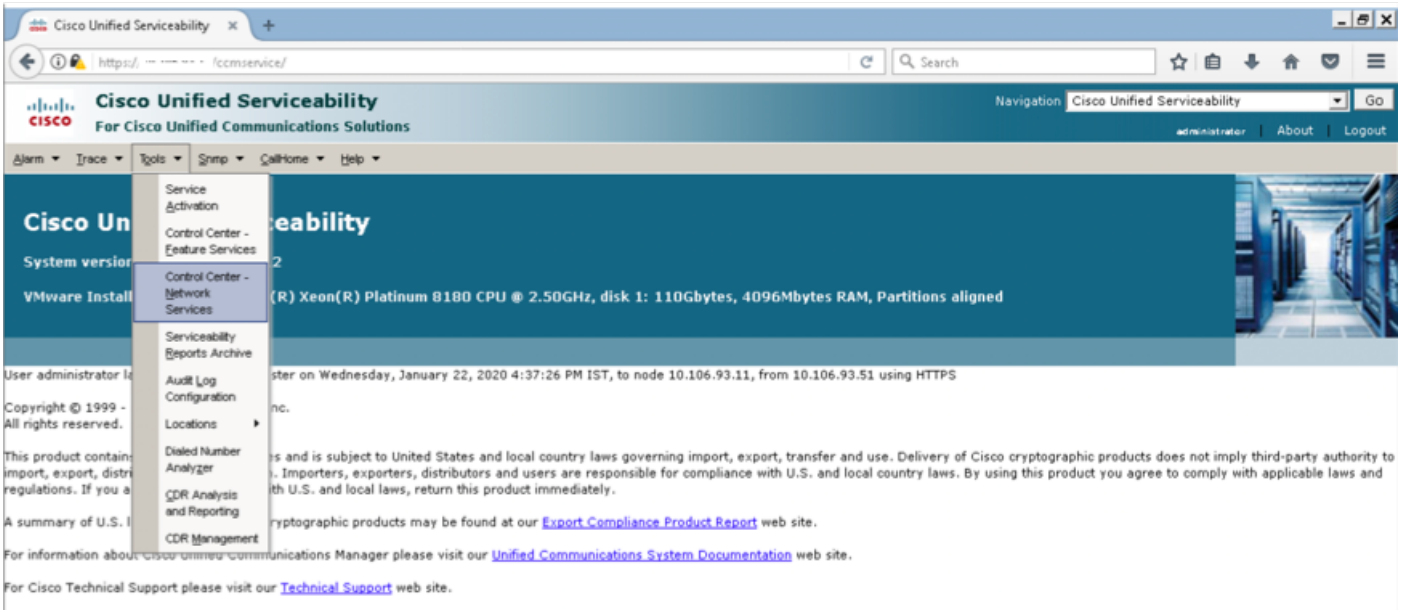




Para todas as outras versões

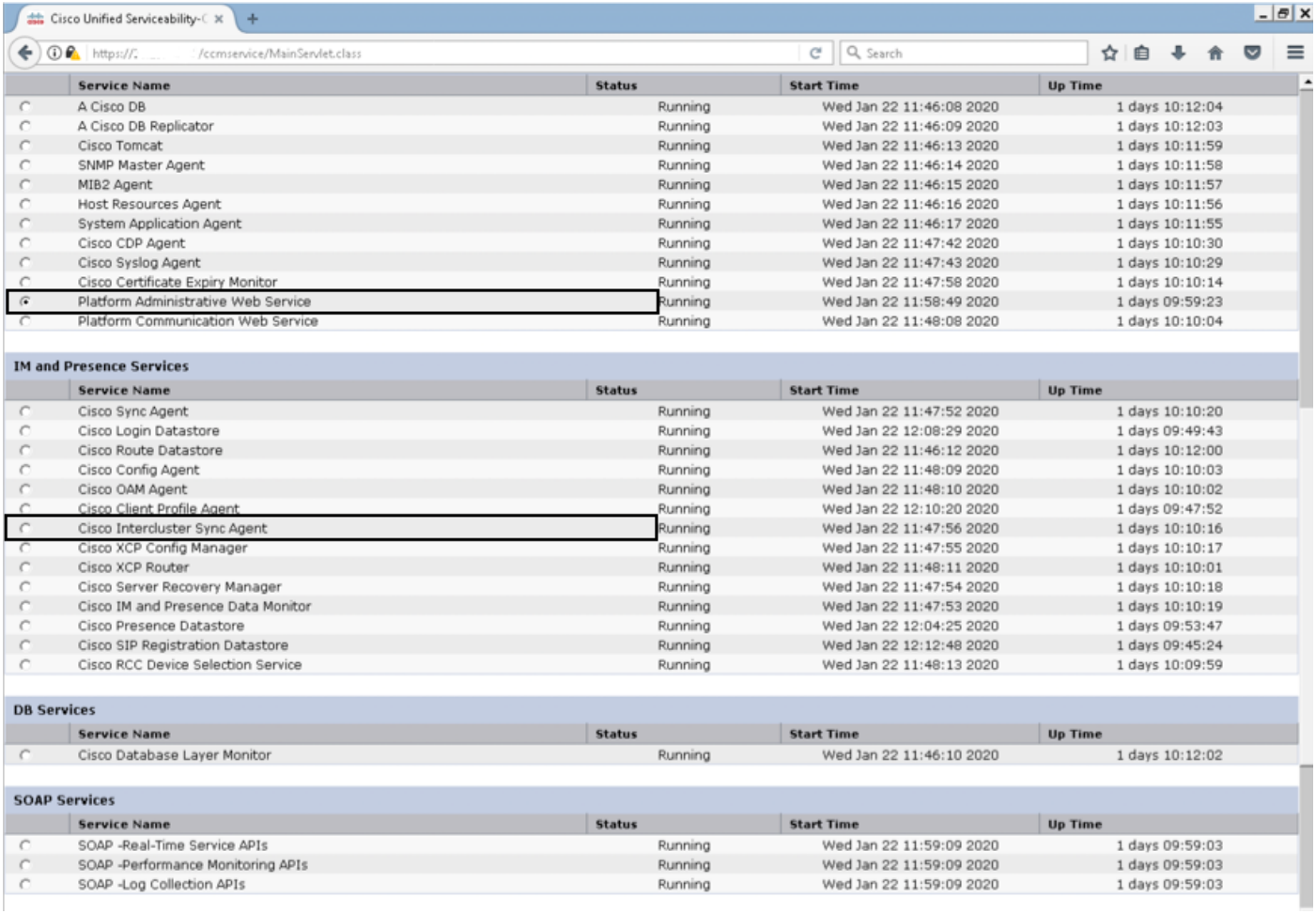
Precisamos executar as etapas abaixo antes de excluir o certificado

Etapa 1. Navegue até **Cisco Unified Serviceability > Tools > Control Center - Network Services**



Etapa 2. Parar **Notificação de Alteração de Certificado da Cisco** em todos os nós do cluster

Etapa 3. Em caso de interrupção do IM e do Presence Server **Platform Administration Web Services** e **Cisco Intercluster Sync Agent**



Etapa 4. Exclua o certificado em todos os nós, incluindo IM e Presença, conforme descrito na Seção *Alternativa para 11.0(1) e posterior* neste documento

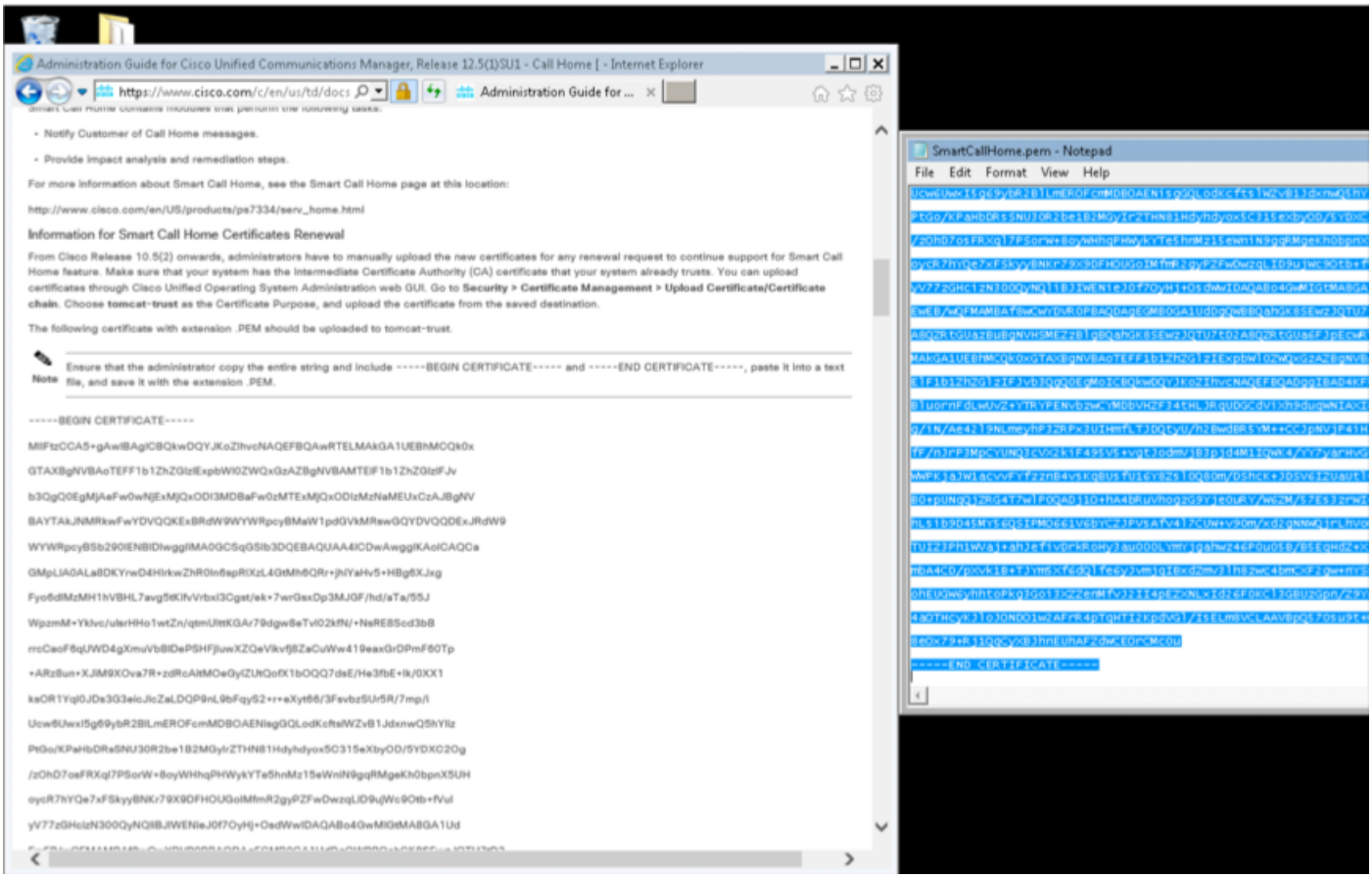
Etapa 5. Inicie o serviço que foi interrompido na Etapa 2. e Etapa 3.

> **Note**: Se você excluir o certificado e fizer uma atualização antes de 7 de fevereiro de 2020, o certificado será reexibido após a atualização e que deverá ser removido novamente. Quaisquer atualizações após 7 de fevereiro de 2020 não adicionarão novamente o certificado

Procedimento de renovação de certificados do Smart Call Home

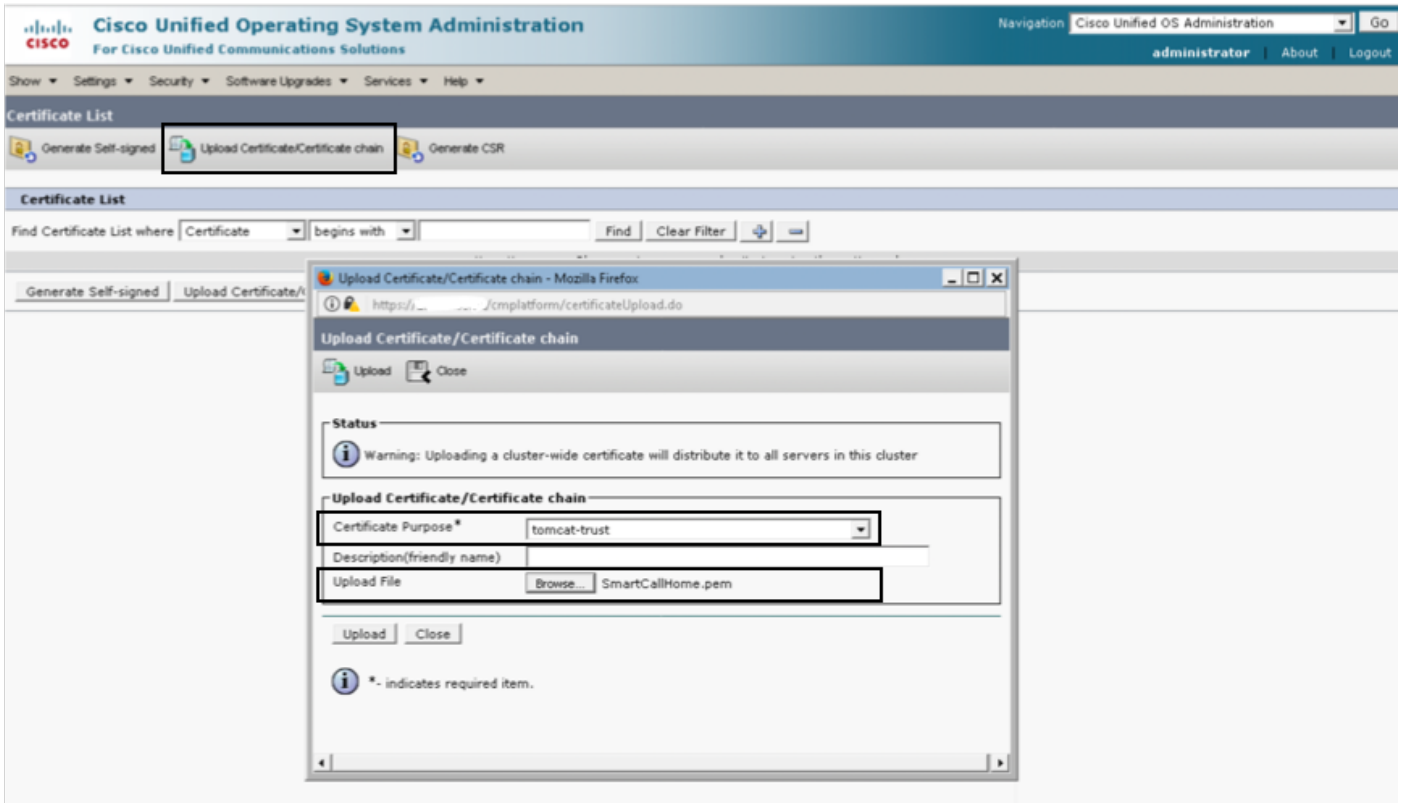
Se o Smart Call Home estiver desativado, nenhuma ação adicional será necessária após a exclusão do certificado. Se o Smart Call Home estiver ativado, siga as etapas

Etapa 1. Copie o conteúdo do certificado do Guia de administração do UCM *Informações da* seção *dos certificados do Smart Call Home*



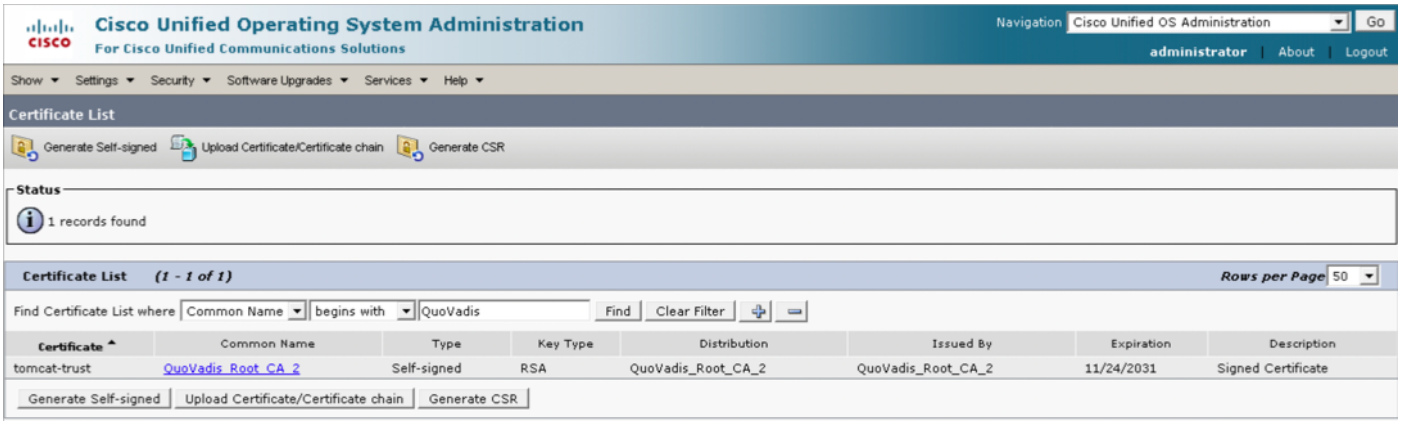
Note: O mesmo certificado é válido para 10.5 e versão superior

Etapa 2. Carregue o arquivo .pem como tomcat-trust na **página de gerenciamento de certificado** da GUI do Cisco Unified OS Administration por captura de tela



Etapa 3. Verifique se **QuoVadis_Root_CA_2** está listado como tomcat-trust ao localizar o

certificado onde o nome comum contém QuoVadis



Para o Cisco Prime License Manager

Para o Prime License Manager 10.5

O certificado expirado (VeriSign_Class_3_Secure_Server_CA_-_G3) pode ser excluído do sistema aplicando este arquivo COP (ciscocm.plm-CSCvs64158_remove_sch_cert_C0050-1.k3.cop.sgn). Leia o arquivo Leiame para ver as instruções de instalação.

Para o Prime License Manager 11.5

O certificado expirado (VeriSign_Class_3_Secure_Server_CA_-_G3) pode ser excluído do sistema aplicando este arquivo COP (ciscocm.plm-CSCvs64158_remove_sch_cert_C0050-1.k3.cop.sgn). Leia o arquivo Leiame para ver as instruções de instalação.