

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

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Problema](#)

[Solução](#)

[Solução alternativa para versões 11.0\(1\) e superiores](#)

[Para todas as outras versões](#)

[Procedimento de renovação de certificados do Smart Call Home](#)

[Para o Cisco Prime License Manager](#)

[Para o Prime License Manager 10.5](#)

[Para o Prime License Manager 11.5](#)

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

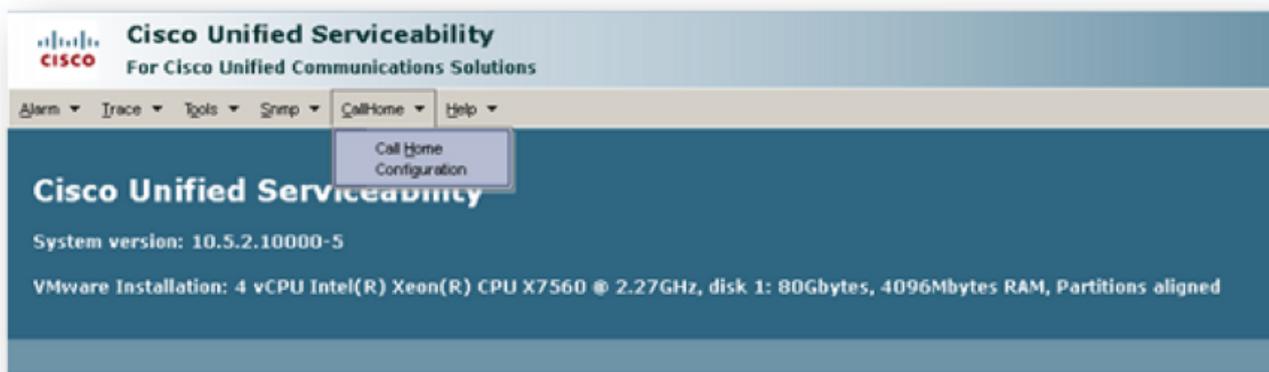
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

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]
```

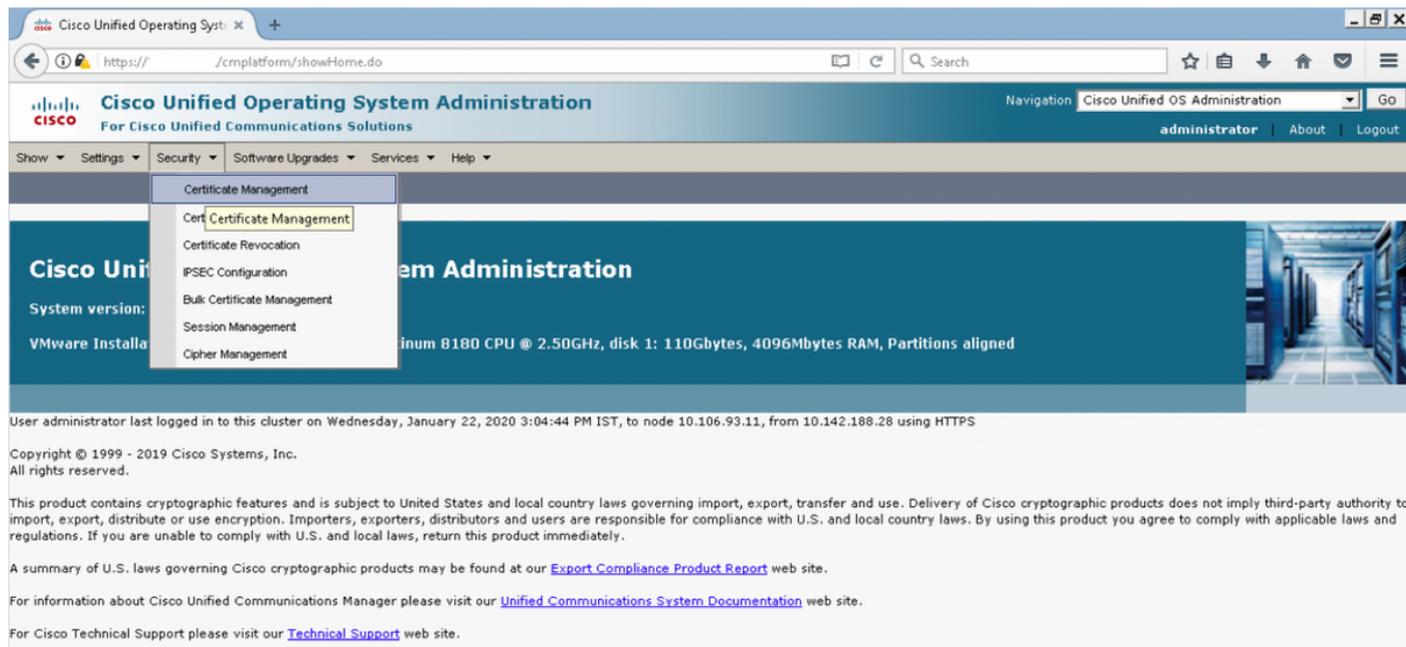
Solução

Esse problema é documentado pela ID de bug da Cisco [CSCvs64158](#).

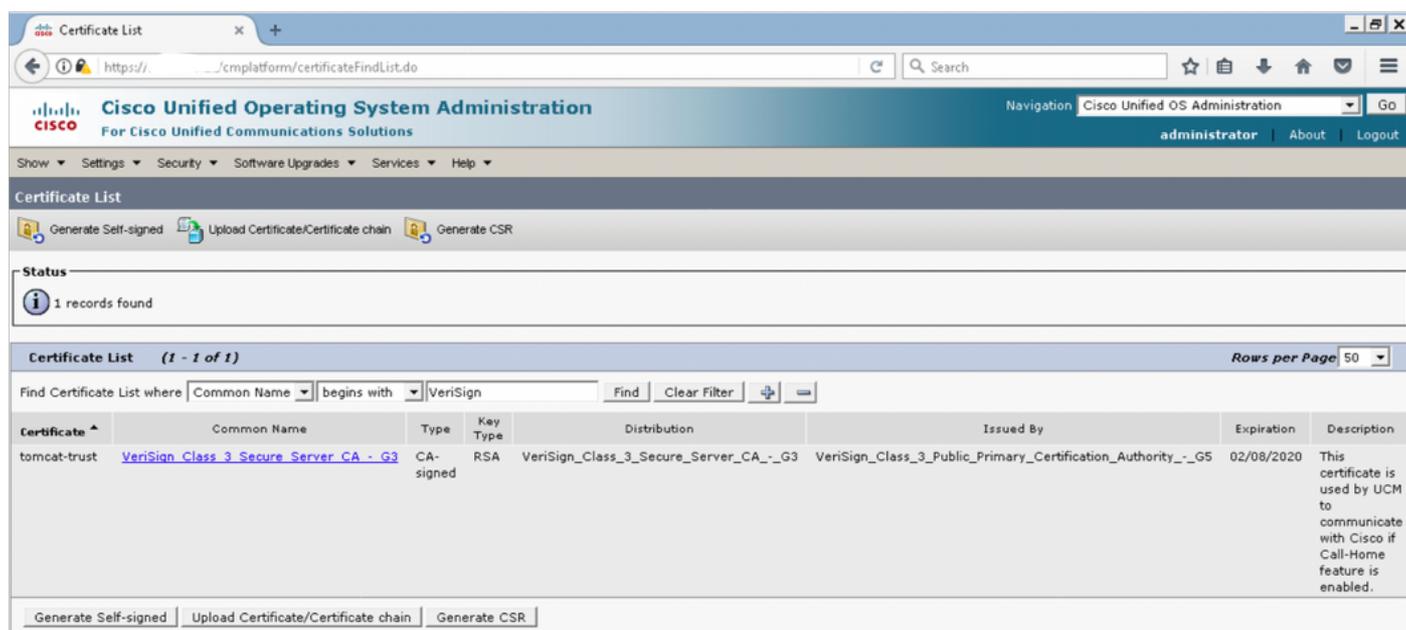
Solução alternativa para versões 11.0(1) e superiores

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

Certificate List

1 records found

Certificate List (1 - 1 of 1)

Common Name
tomcat-trust VeriSign_Class_3_Secure_Server_CA_-_G3

Certificate Details for VeriSign_Class_3_Secure_Server_CA_-_G3, tomcat-trust

Status: Ready

Certificate Settings

- Locally Uploaded: 21/01/20
- File Name: VeriSign_Class_3_Secure_Server_CA_-_G3.pem
- Certificate Purpose: tomcat-trust
- Certificate Type: trust-certs
- Certificate Group: product-cpi
- Description(friendly name): This certificate is used by UCM to communicate with Cisco if Call-Home feature is enabled.

Certificate File Data

```

[
  Version: V3
  Serial Number: 6ECC7AA5A7032009B8CEBCF4E952D491
  SignatureAlgorithm: SHA1withRSA (1.2.840.113549.1.1.5)
  Issuer Name: CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU=(c) 2006 VeriSign, Inc. - For authorized use only, OU=VeriSign Trust Network, O=VeriSign, Inc., C=US
  Validity From: Mon Feb 08 05:30:00 IST 2010
  To: Sat Feb 08 05:29:59 IST 2020
  Subject Name: CN=VeriSign Class 3 Secure Server CA - G3, OU=Terms of use at https://www.verisign.com/rpa (c)10, OU=VeriSign Trust Network, O=VeriSign, Inc., C=US
  Key: RSA (1.2.840.113549.1.1.1)
  Key value:
  3082010a0282010100b187841fc20c45f5bcab2597a7ada23e9cbaf6c139b88bcac2ac56c6e5bb658e44
  4f4dce6fed094ad4af4e109c688b2e957b899b13cae23434c1f35bf3497b6283488174d188786c0253f9b
  c7f4326575833833b330a17b0d04e9124ad867d6412dc744a34a11d0aea961d0b15fca34b3bce6388d0
  f82d0c948610cab69a3dcaeb379c00483586295078e84563cd19414ff595ec7b98d4c471b350be28b38f
]
  
```

Buttons: Delete, Download .PEM File, Download .DER File

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

Certificate List

1 records found

Certificate List (1 - 1 of 1)

Common Name
tomcat-trust VeriSign_Class_3_Secure_Server_CA_-_G3

Certificate Details for VeriSign_Class_3_Secure_Server_CA_-_G3, tomcat-trust

Status: Ready

Certificate Settings

- Locally Uploaded: 21/01/20
- File Name: VeriSign_Class_3_Secure_Server_CA_-_G3.pem
- Certificate Purpose: tomcat-trust
- Certificate Type: trust-certs
- Certificate Group: product-cpi
- Description(friendly name): This certificate is used by UCM to communicate with Cisco if Call-Home feature is enabled.

Certificate File Data

```

[
  Version: V3
  Serial Number: 6ECC7AA5A7032009B8CEBCF4E952D491
  SignatureAlgorithm: SHA1withRSA (1.2.840.113549.1.1.5)
  Issuer Name: CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU=(c) 2006 VeriSign, Inc. - For authorized use only, OU=VeriSign Trust Network, O=VeriSign, Inc., C=US
  Validity From: Mon Feb 08 05:30:00 IST 2010
  To: Sat Feb 08 05:29:59 IST 2020
  Subject Name: CN=VeriSign Class 3 Secure Server CA - G3, OU=Terms of use at https://www.verisign.com/rpa (c)10, OU=VeriSign Trust Network, O=VeriSign, Inc., C=US
  Key: RSA (1.2.840.113549.1.1.1)
  Key value:
  3082010a0282010100b187841fc20c45f5bcab2597a7ada23e9cbaf6c139b88bcac2ac56c6e5bb658e44
  4f4dce6fed094ad4af4e109c688b2e957b899b13cae23434c1f35bf3497b6283488174d188786c0253f9b
  c7f4326575833833b330a17b0d04e9124ad867d6412dc744a34a11d0aea961d0b15fca34b3bce6388d0
  f82d0c948610cab69a3dcaeb379c00483586295078e84563cd19414ff595ec7b98d4c471b350be28b38f
]
  
```

Buttons: Delete, Download .PEM File, Download .DER File

Confirmation Dialog:

You are about to permanently delete this certificate which may break a certificate chain if this certificate is part of an existing chain. You can determine if deleting this certificate will result in a broken certificate chain by looking into issuername and subjectname of the relevant certificates in Certificate List page. This certificate will be deleted from all the servers in the cluster. This delete action cannot be undone. Continue?

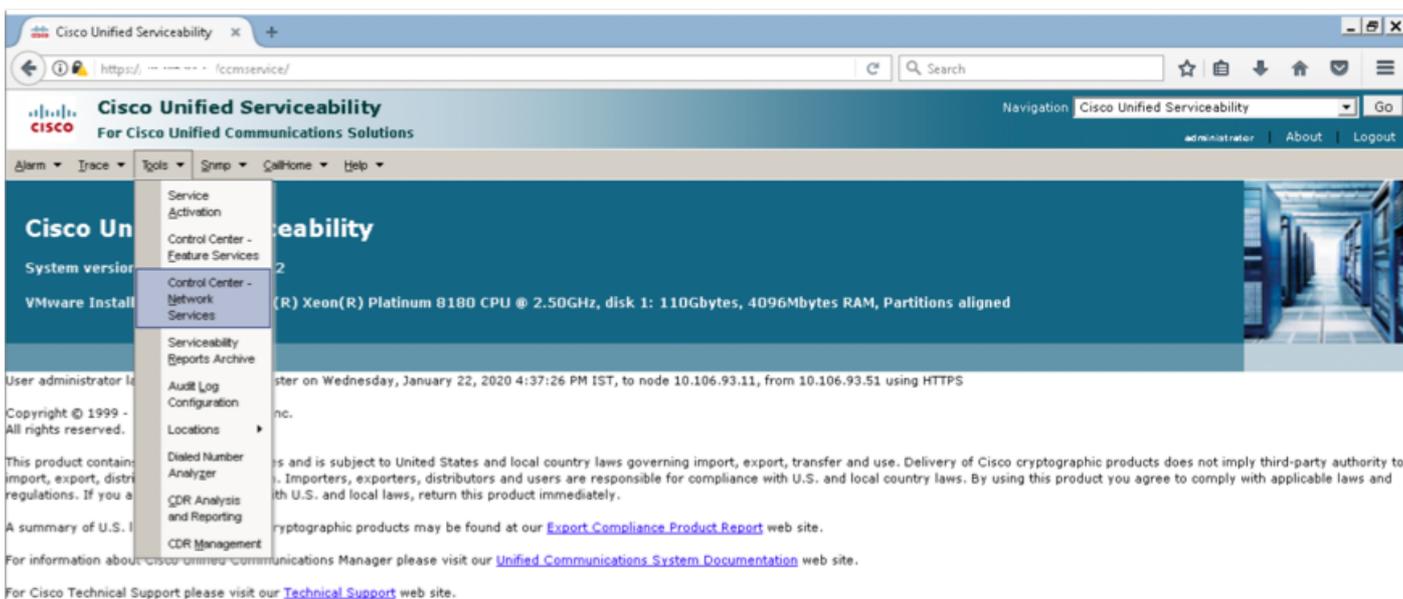
Buttons: OK, Cancel



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

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

IM and Presence Services			
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

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

SOAP Services			
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

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

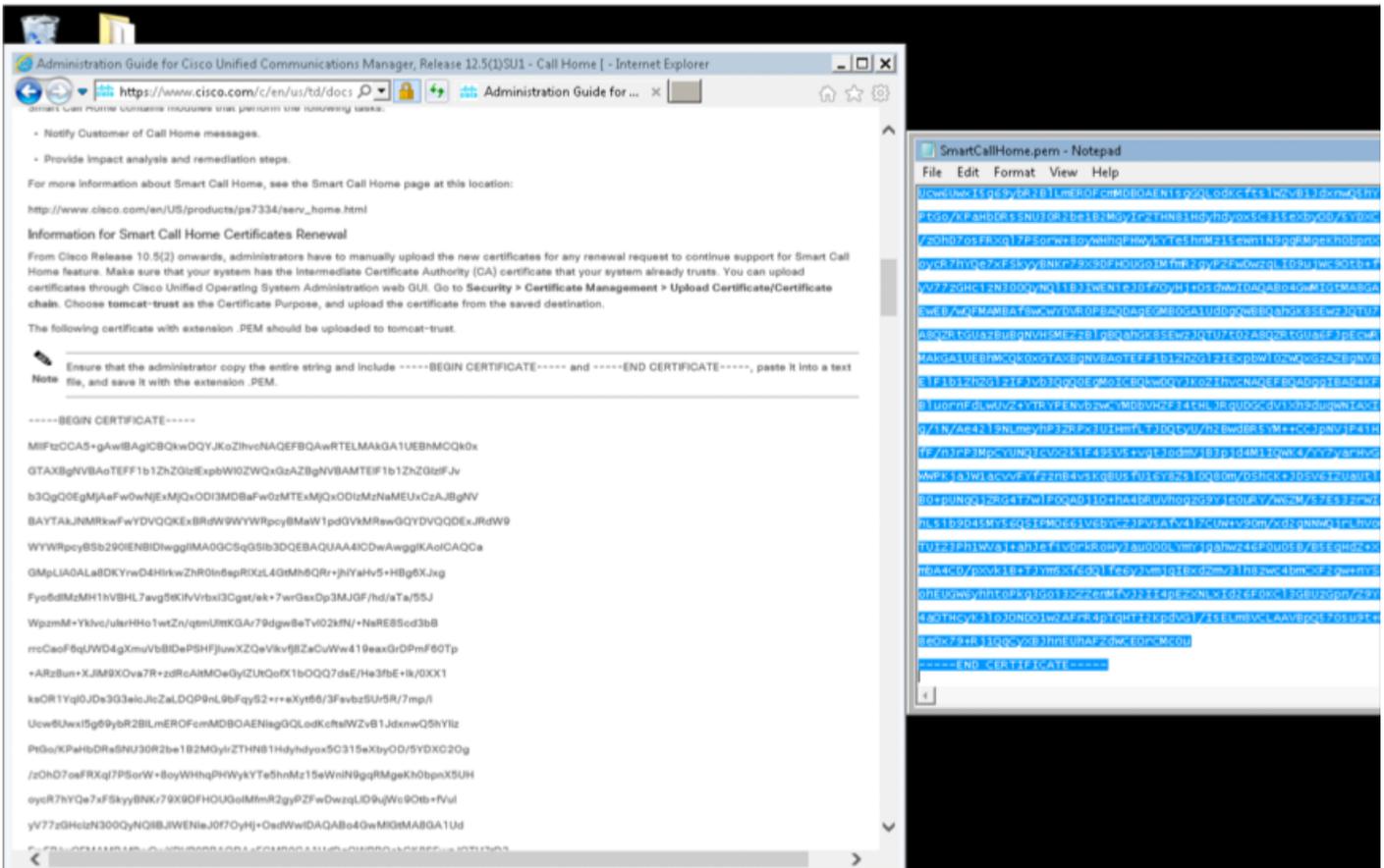
Etapa 5. Inicie o serviço que foi interrompido na Etapa 2. e Etapa 3.

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

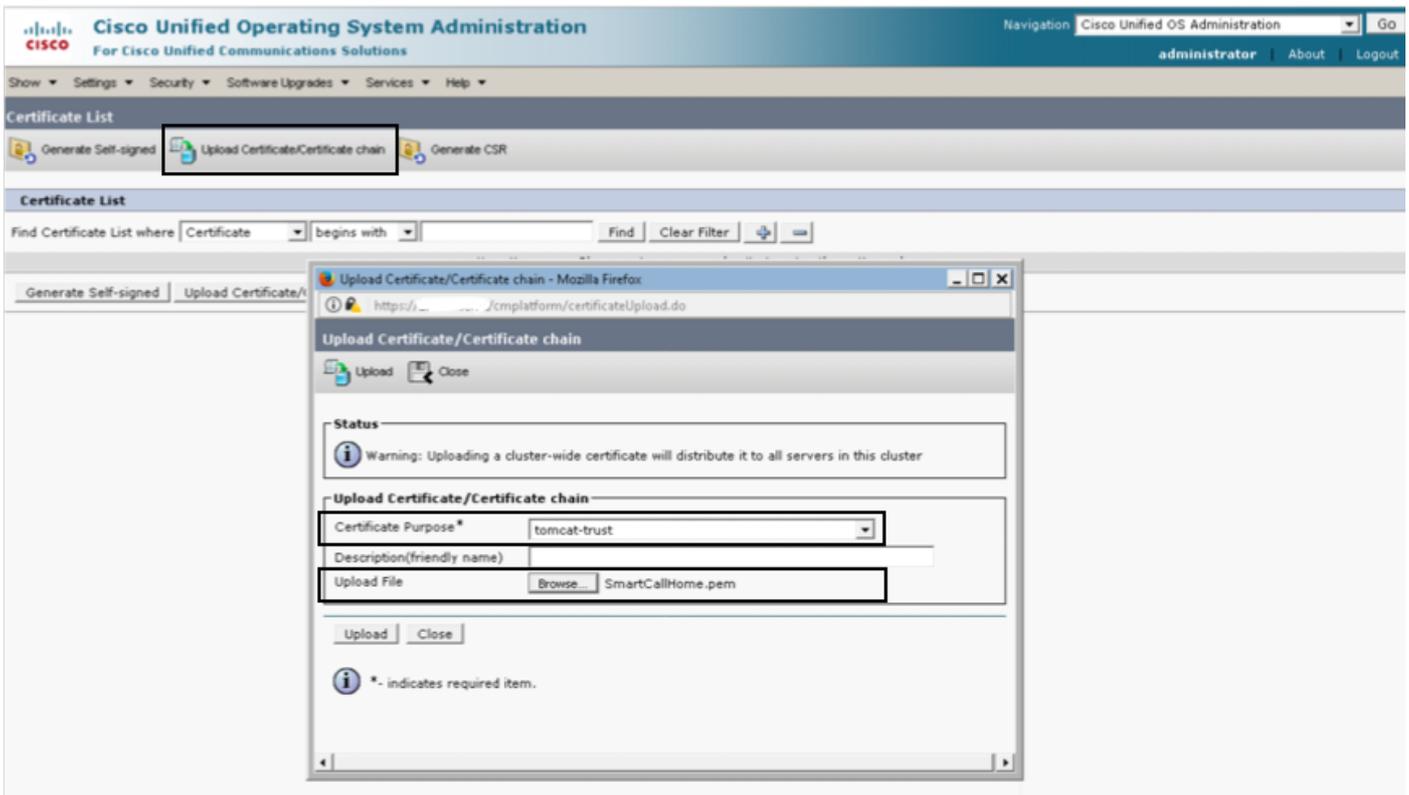
Se o Smart Call Home estiver desativado, nenhuma ação adicional será necessária após a exclusão do certificado. Se o Smart Call Home estiver ativado, siga as etapas

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

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 only record in the table is 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".

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 Leiam 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 Leiam para ver as instruções de instalação.