コラボレーション製品のSmart Call Home証明書の証明書期限切れアラートのトラブルシューティング

内容

概要

このドキュメントでは、Smart Call Homeに対して提供されるVerisign証明書(VeriSign_Class_3_Secure_Server_CA_-_G3.der)の証明書の期限切れアラートのソリューションについて説明します。このドキュメントでは、次のシスコユニファイドコラボレーション製品で期限がです。

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

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

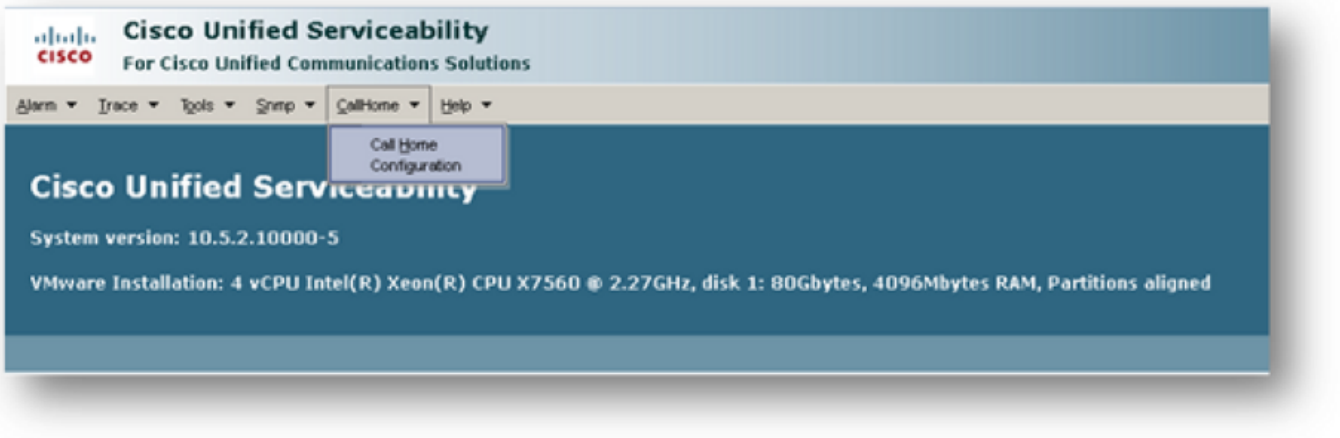
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

背景説明

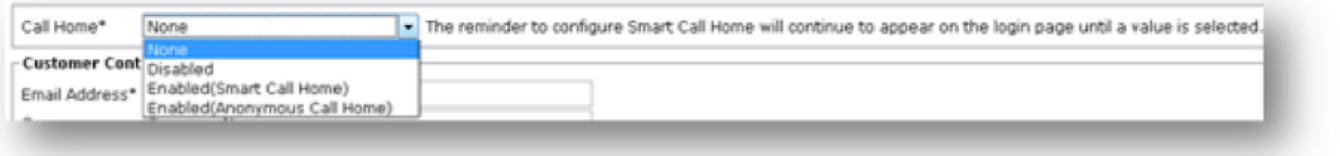
Smart Call Home は、ネットワーク上のシスコ デバイスを監視する自動サポート機能で、Call Home 機能を使用すると、Smart Call Home バックエンド サーバと通信し、診断アラート、インベントリなどのメッセージを送信できます。

このセクションでは、Smart Call Homeが有効になっているかどうかを確認します

ステップ1:[Cisco Unified Serviceability]ページで、[CallHome] > [Configuration]を選択します。



ステップ2:[Call Home]フィールドが[Disabled]または[Enabled]に設定されていることを確認します



問題

Cisco Unified Collaboration製品のSmart Call Home用のtomcat-trust証明書としてデフォルトで提供されるVeriSign証明書(VeriSign_Class_3_Secure_Server_CA_-_G3.der)は、2020年2月に期限切れになります。次の期限切れアラートが表示されます。

```
%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]
```

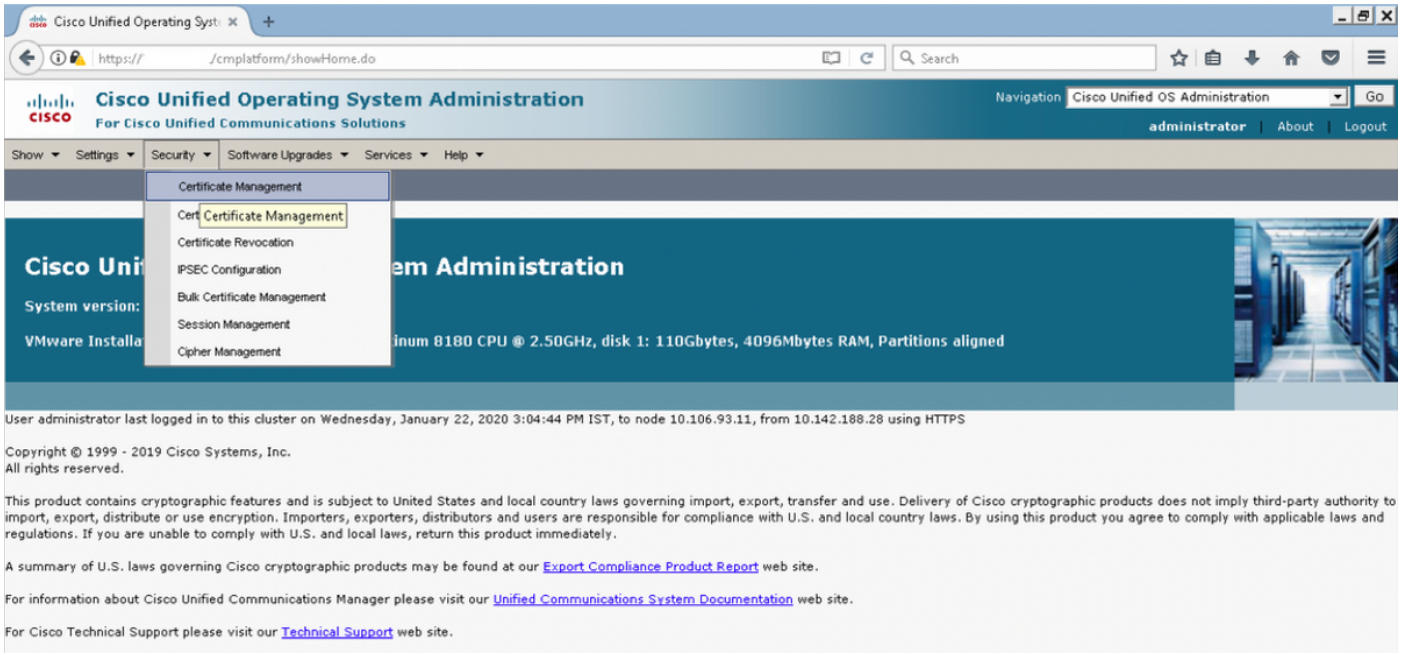
解決方法

この問題は、Cisco Bug ID CSCvs64158（登録ユーザ専用）に記載されています。

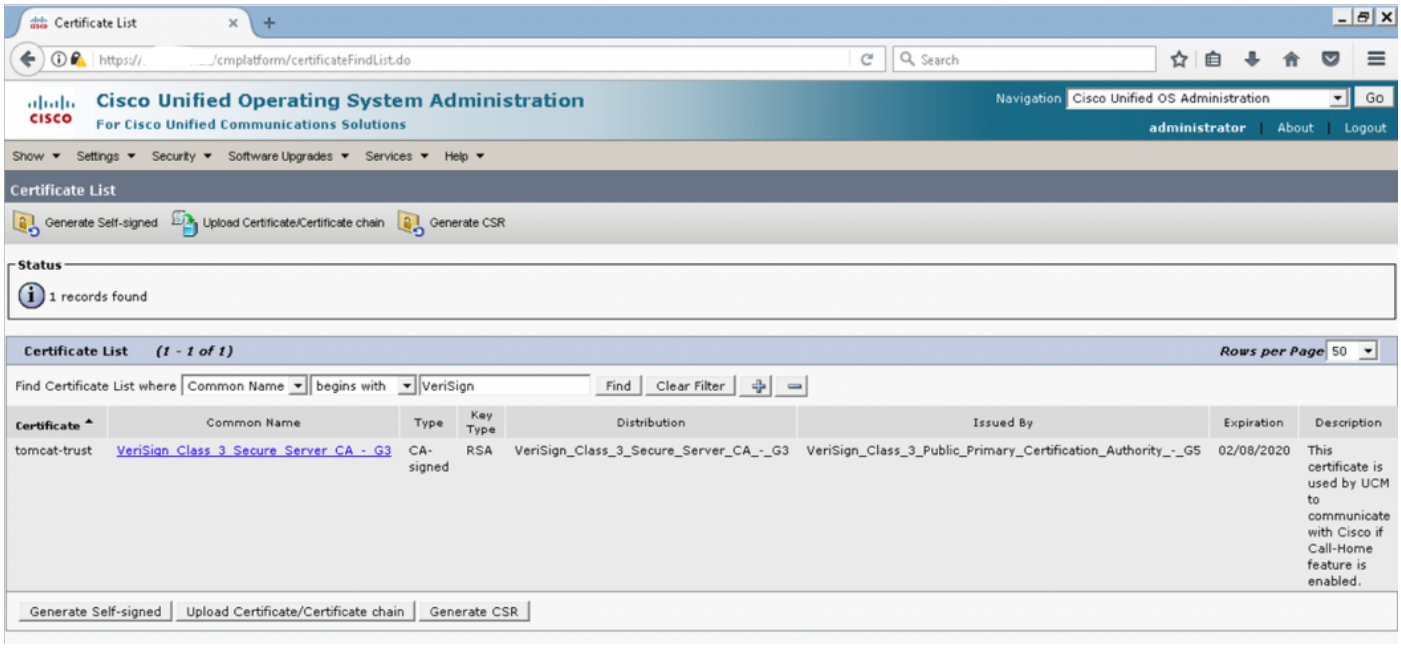
11.0(1)以降のバージョンの回避策

期限切れの証明書を削除するには、次の手順を実行する必要があります (VeriSign_Class_3_Secure_Server_CA_-_G3.der)

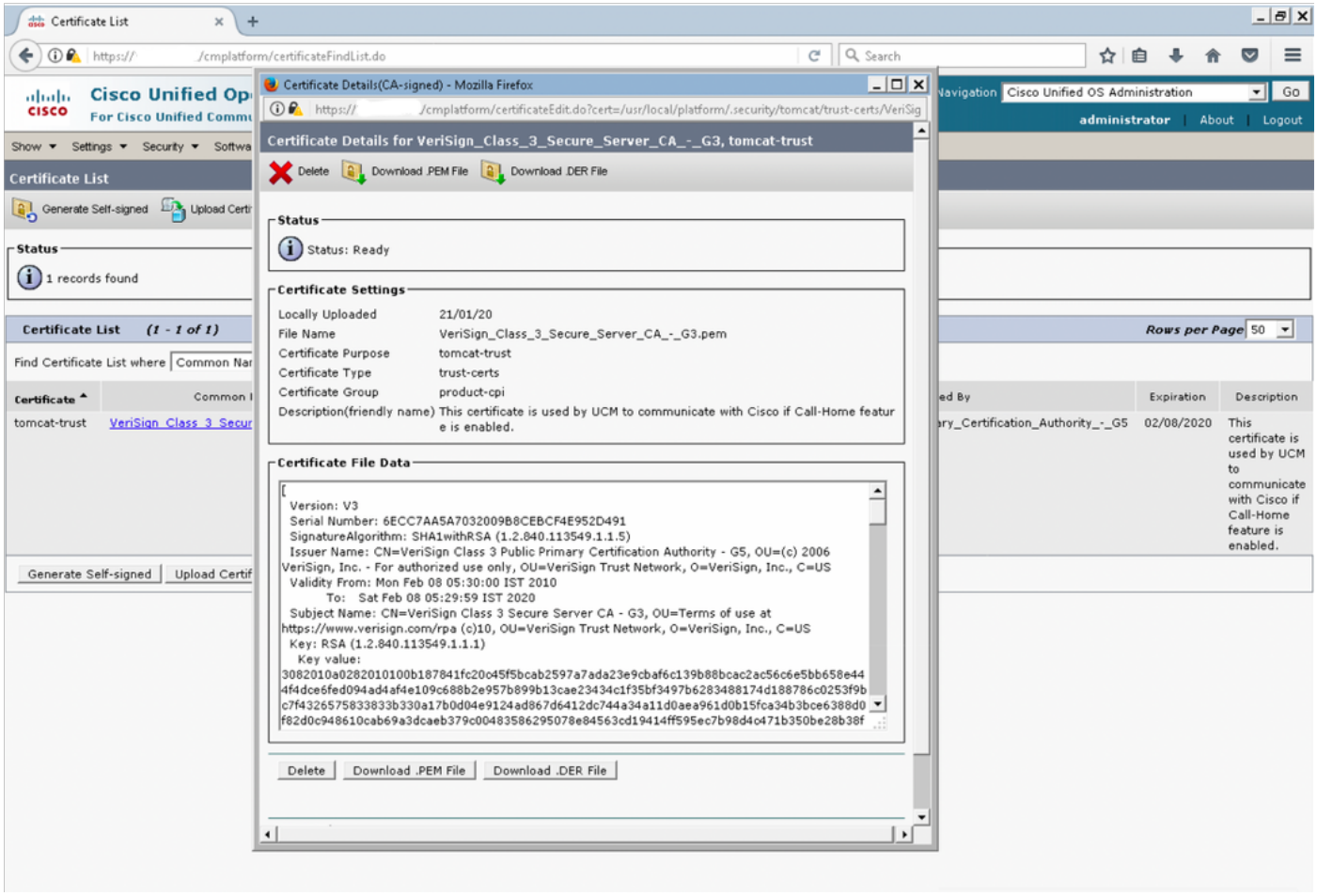
ステップ1：パブリッシャのCisco Unified OS Administration GUIを参照し、[Security] > [Certificate Management]をクリックします



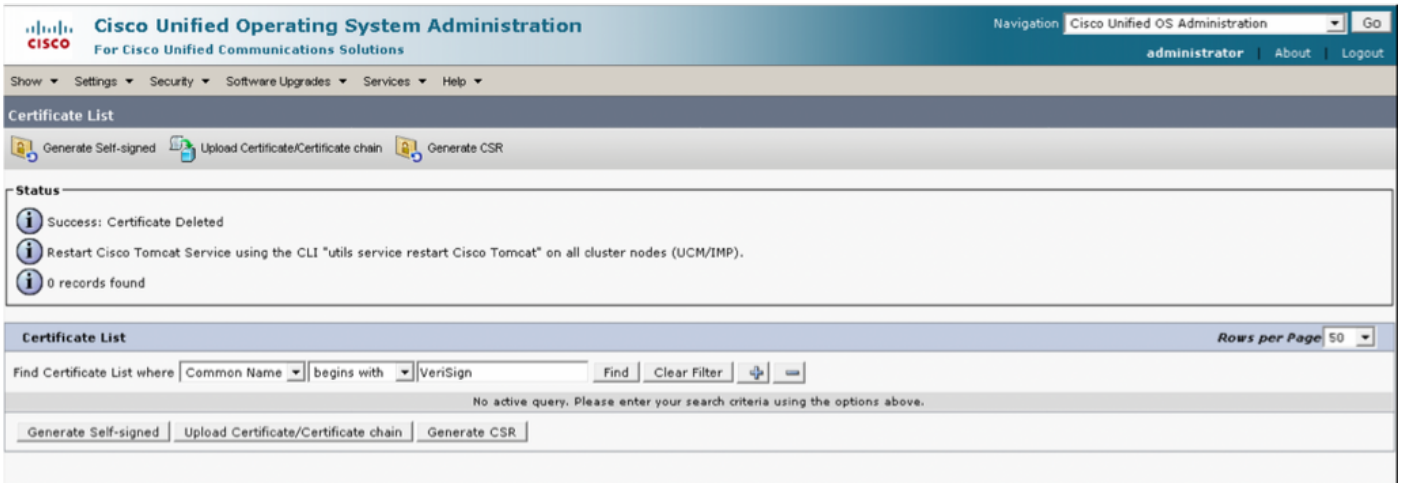
ステップ2：共通名にVeriSignが含まれる証明書リストの検索



ステップ3:[VeriSign_Class_3_Secure_Server_CA_-_G3]をクリックします。ポップアップウィンドウが開き、証明書の詳細が強調表示されます



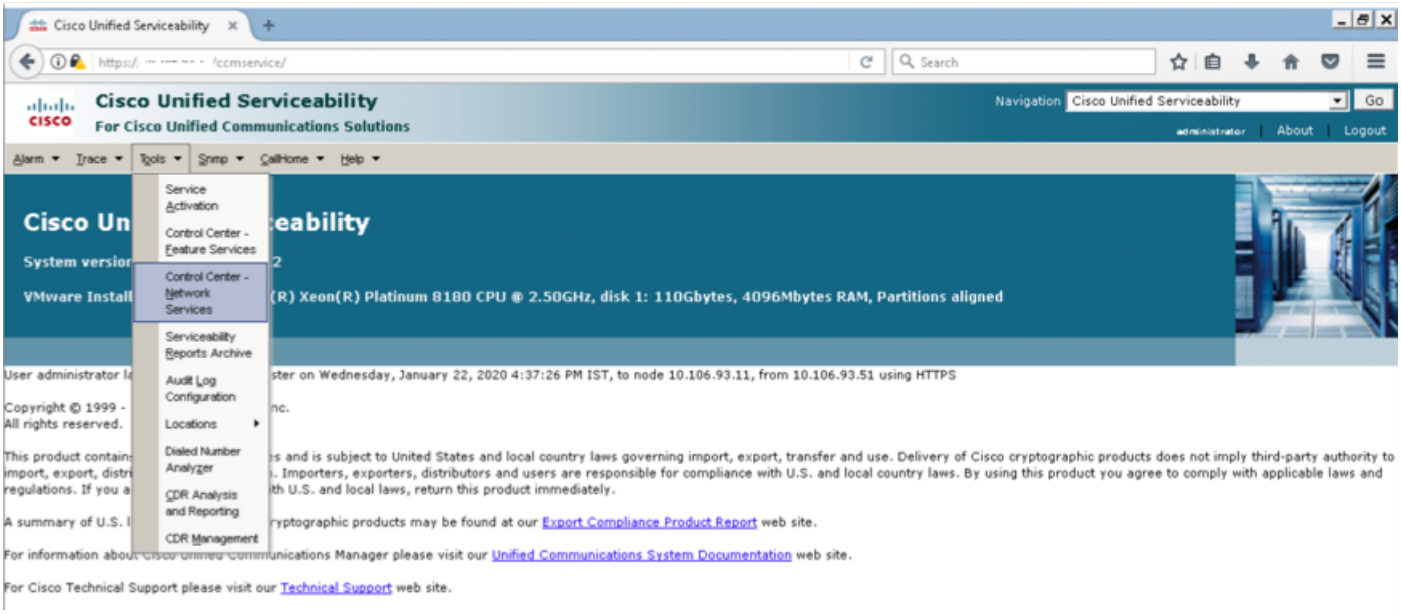
ステップ4:[Delete]ボタンをクリックし、**警告を表示**して[OK]をクリックします。証明書は、クラスタ内のすべてのノードから削除する必要があります。



他のすべてのバージョン

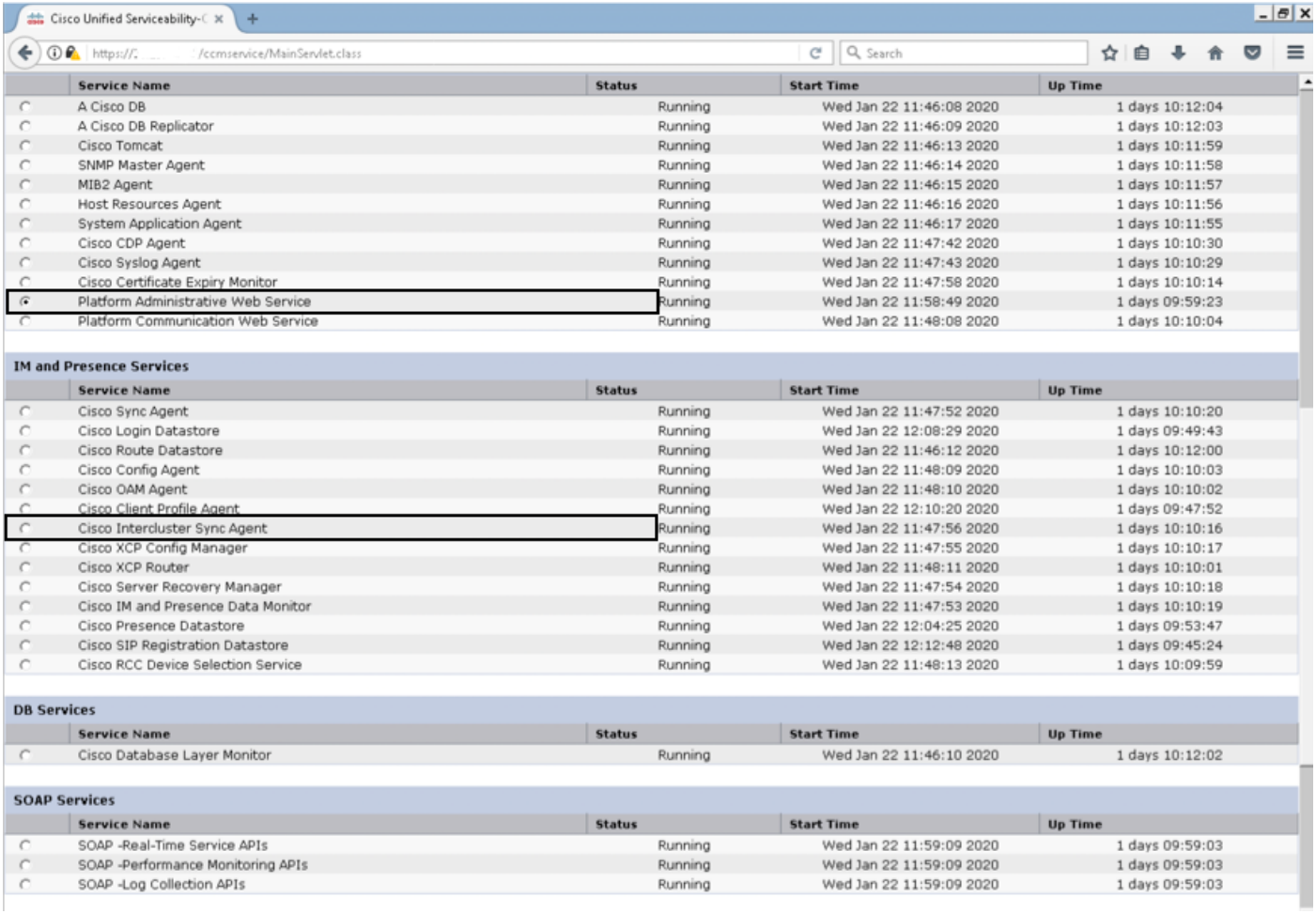
証明書を削除する前に、次の手順を実行する必要があります

ステップ1:**[Cisco Unified Serviceability] > [Tools] > [Control Center - Network Services]に移動します。**



ステップ2：クラスタ内**のすべてのノードで**Cisco証明書変更通知を停止します

ステップ3:IM and Presence Server Stop **Platform Administration Web ServicesおよびCisco Intercluster Sync Agentの場合**



ステップ4：このドキュメントの「*11.0(1)以降の回避策*」セクションで説明されているように、*IM and Presenceを含むすべてのノードの証明書を削除*します

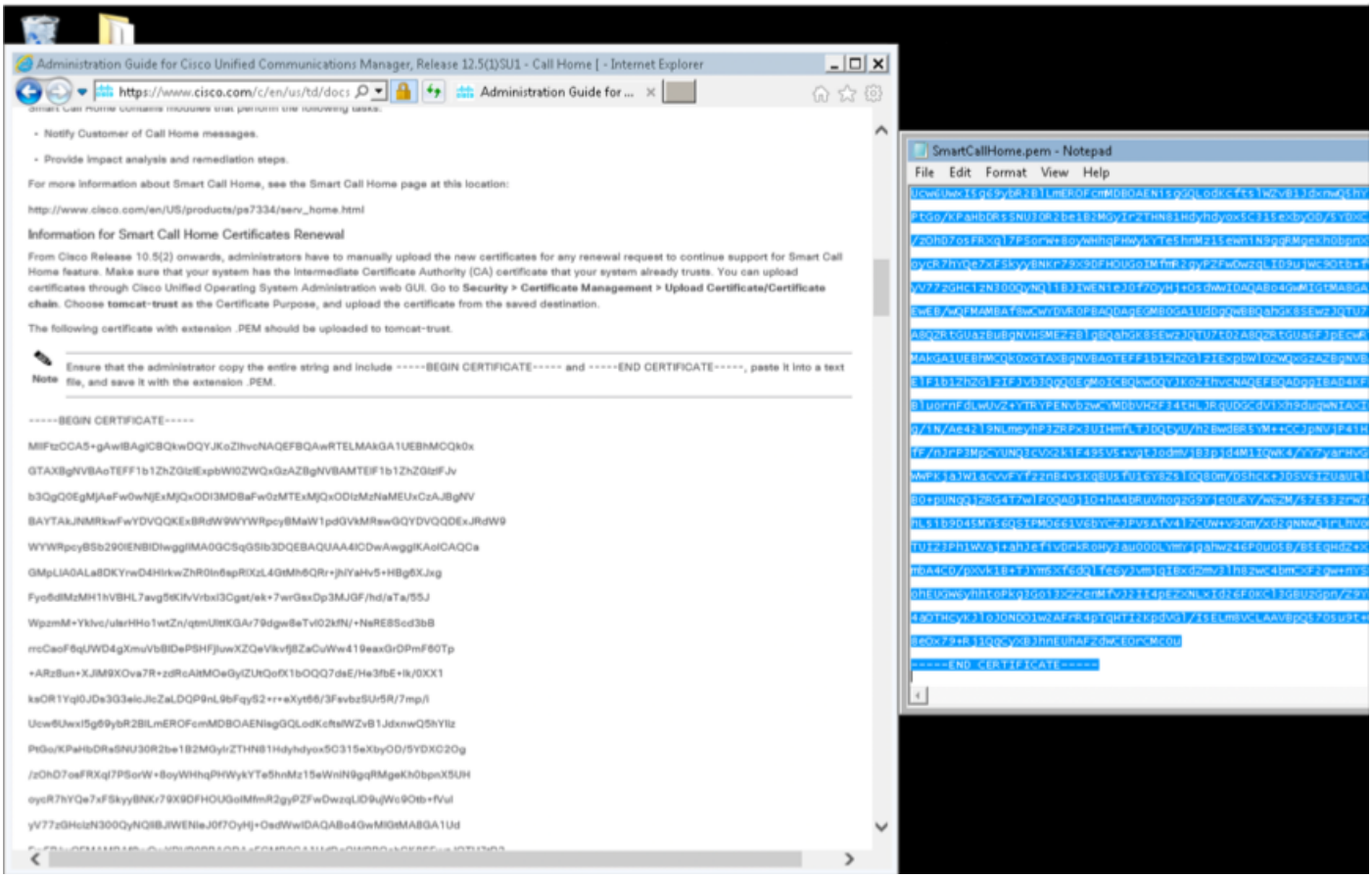
ステップ5：ステップ2とステップ3で停止したサービスを開始します。

> **注**：証明書を削除し、2020年2月7日より前にアップグレードを実行すると、アップグレード後に証明書が再度表示され、再度削除する必要があります。2020年2月7日以降のアップグレードでは、証明書は再度追加されません

Smart Call Home証明書の更新手順

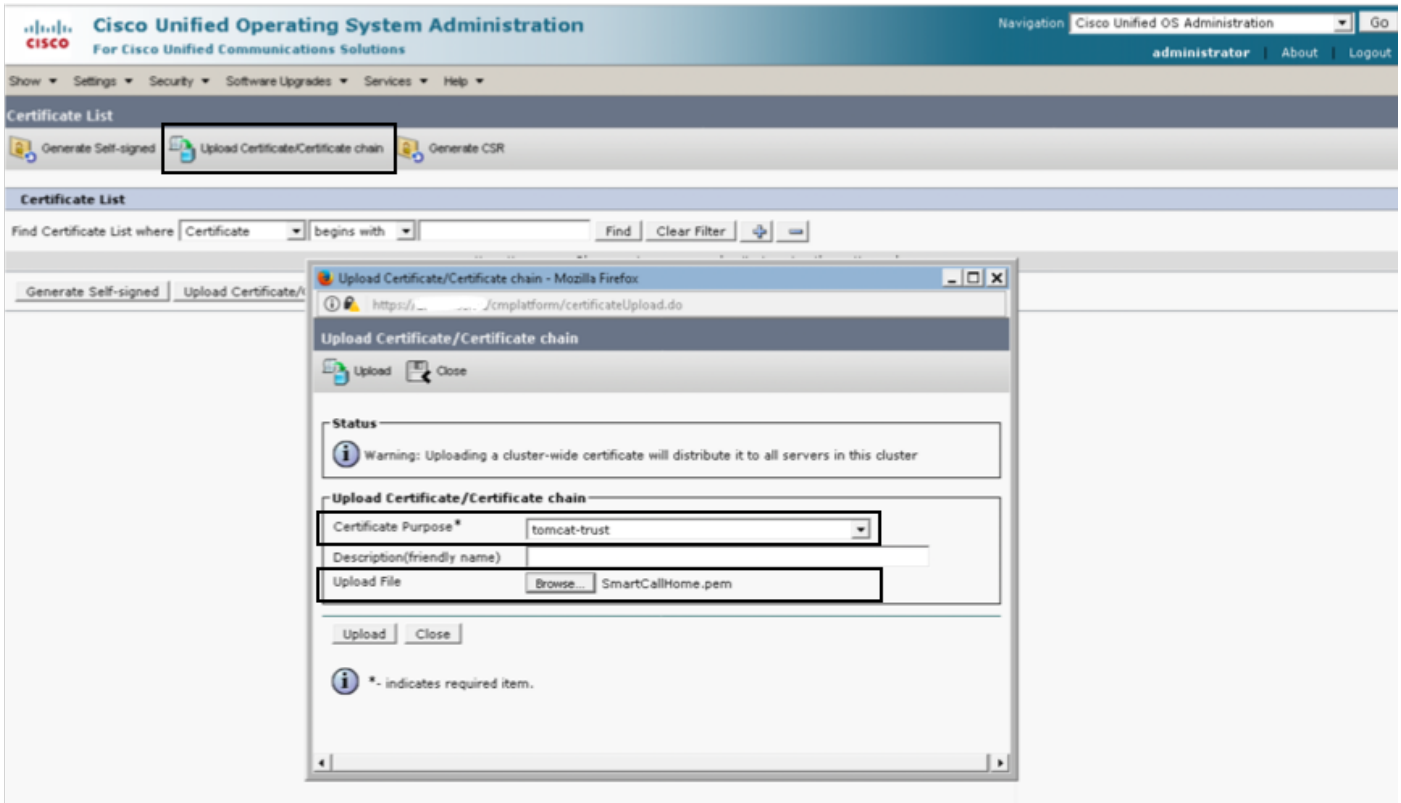
Smart Call Homeが無効になっている場合は、証明書を削除した後に追加の操作は必要ありません。Smart Call Homeが有効になっている場合は、次の手順を実行します

ステップ1:『UCMアドミニストレーションガイド』セクション「*Smart Call Home証明書の情報」から証明書の内容をコピーする*



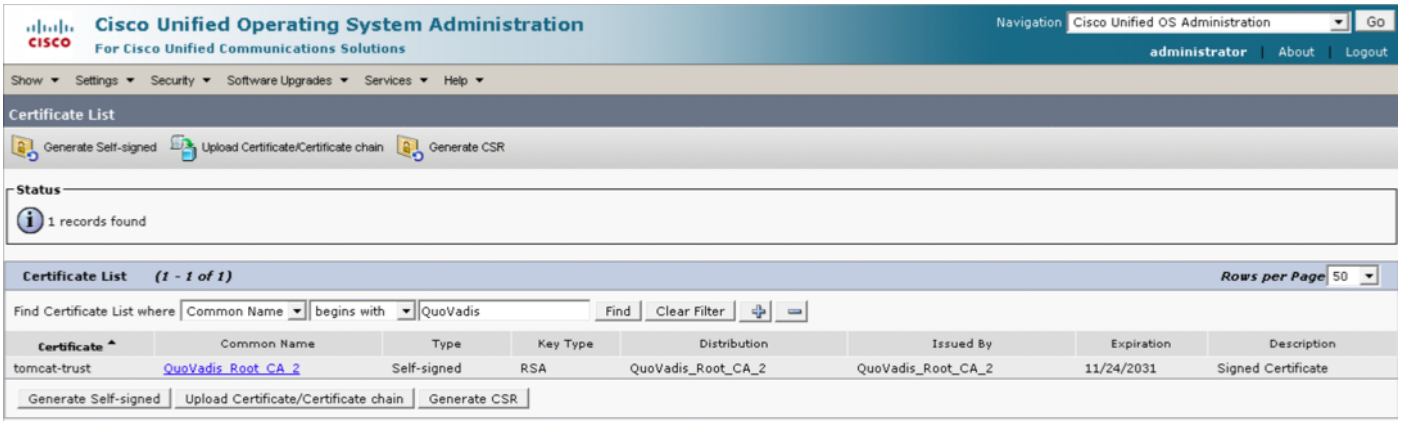
注：10.5以降のバージョンでは同じ証明書が有効です

ステップ2：スクリーンショットに従って、[Cisco Unified OS Administration]の[GUI Certificate Management]ページで.pemファイルをtomcat-trust**としてアップロードします**



ステップ3：共通名に**QuoVadisが含まれている証明書を見つけることで、**

QuoVadis_Root_CA_2がtomcat-trustとしてリストされていることを確認します



Cisco Prime License Managerの場合

Prime License Manager 10.5

期限切れの証明書(VeriSign_Class_3_Secure_Server_CA_-_G3)は、このCOPファイル(ciscocm.plm-CSCvs64158_remove_sch_cert_C0050-1.cop3.sgn)を適用することでシステムから削除できます. インストール手順については、Readmeファイルを参照してください。

Prime License Manager 11.5

期限切れの証明書(VeriSign_Class_3_Secure_Server_CA_-_G3)は、このCOPファイル(ciscocm.plm-CSCvs64158_remove_sch_cert_C0050-1.cop3.sgn)。 インストール手順については、Readmeファイルを参照してください。