Risoluzione dei problemi relativi all'avviso di scadenza del certificato di Smart Call Home sui prodotti Collaboration

Sommario

Introduzione

Questo documento descrive le soluzioni per l'avviso di scadenza del certificato di verifica (VeriSign_Class_3_Secure_Server_CA_-_G3.der) fornito per Smart Call Home che scadrà a febbraio 2020 nei seguenti prodotti Cisco Unified Collaboration descritti in questo 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)
Cisco Virtualized Voice Browser
Cisco Prime License Manager

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

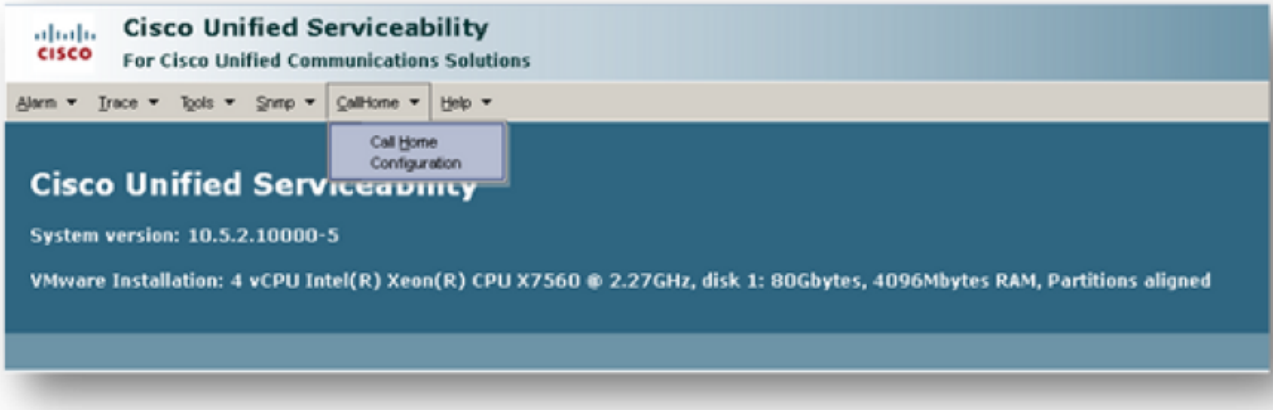
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

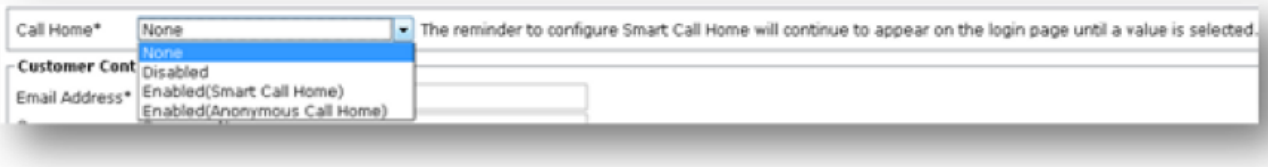
Smart Call Home è una funzionalità di supporto automatizzato per il monitoraggio dei dispositivi Cisco della rete. La funzione Call Home consente di comunicare e inviare gli avvisi di diagnostica, l'inventario e altri messaggi al server back-end Smart Call Home.

Utilizzare questa sezione per verificare se Smart Call Home è abilitato

Passaggio 1. Dalla pagina Cisco Unified Serviceability, scegliere CallHome > Configurazione.



Passaggio 2. Verificare se il campo Call Home è impostato su Disabilitato o Abilitato



Problema

Il certificato VeriSign (VeriSign_Class_3_Secure_Server_CA_-_G3.der) fornito per impostazione predefinita come certificato tomcat-trust per Smart Call Home sui prodotti Cisco Unified Collaboration scadrà a febbraio 2020. Di seguito è riportato il seguente avviso di scadenza:

```
%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]
```

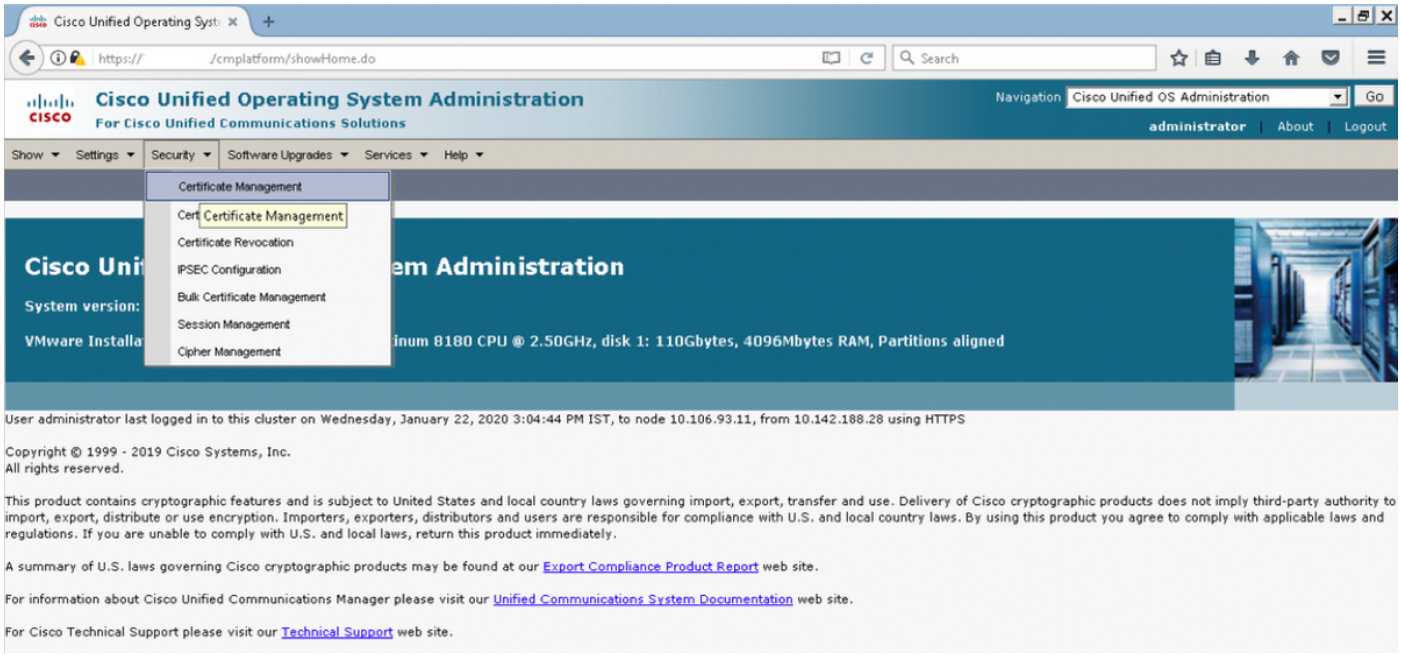
Soluzione

Questo problema è documentato dall'ID bug Cisco CSCvs64158.

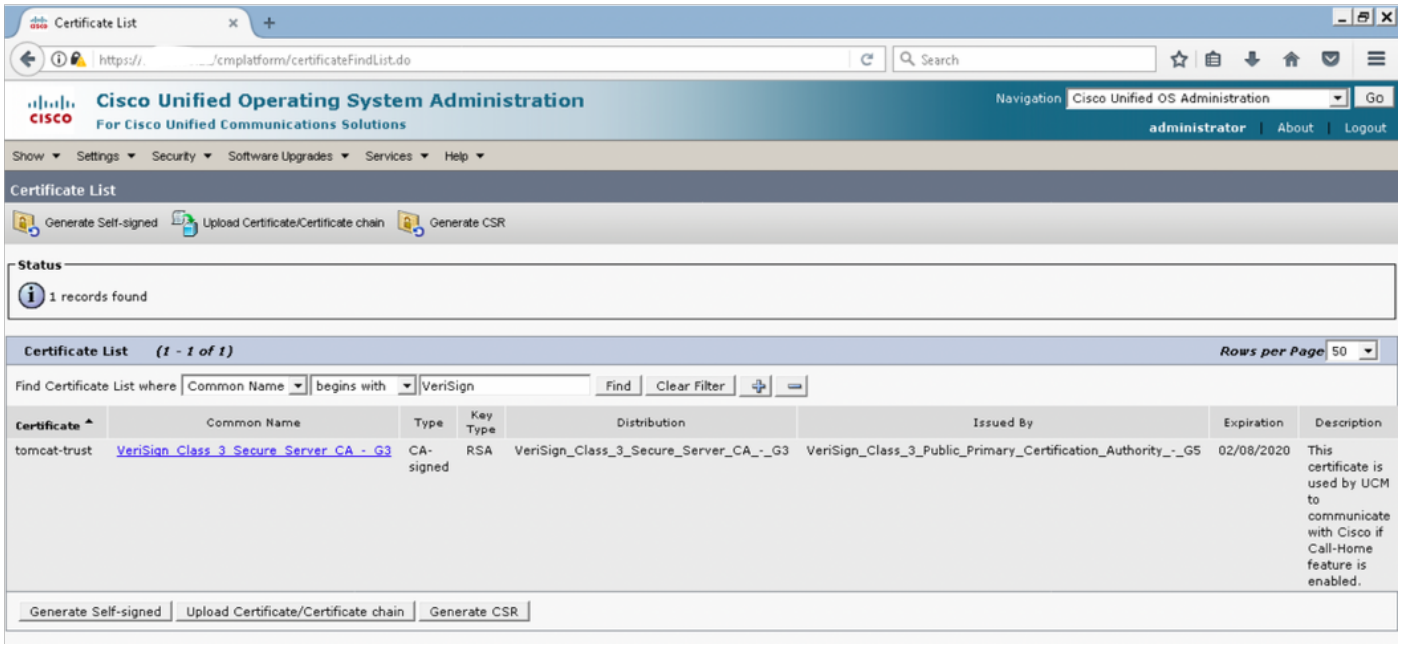
Soluzione per la versione 11.0(1) e successive

Per eliminare il certificato scaduto è necessario eseguire la procedura seguente (VeriSign_Class_3_Secure_Server_CA_-_G3.der)

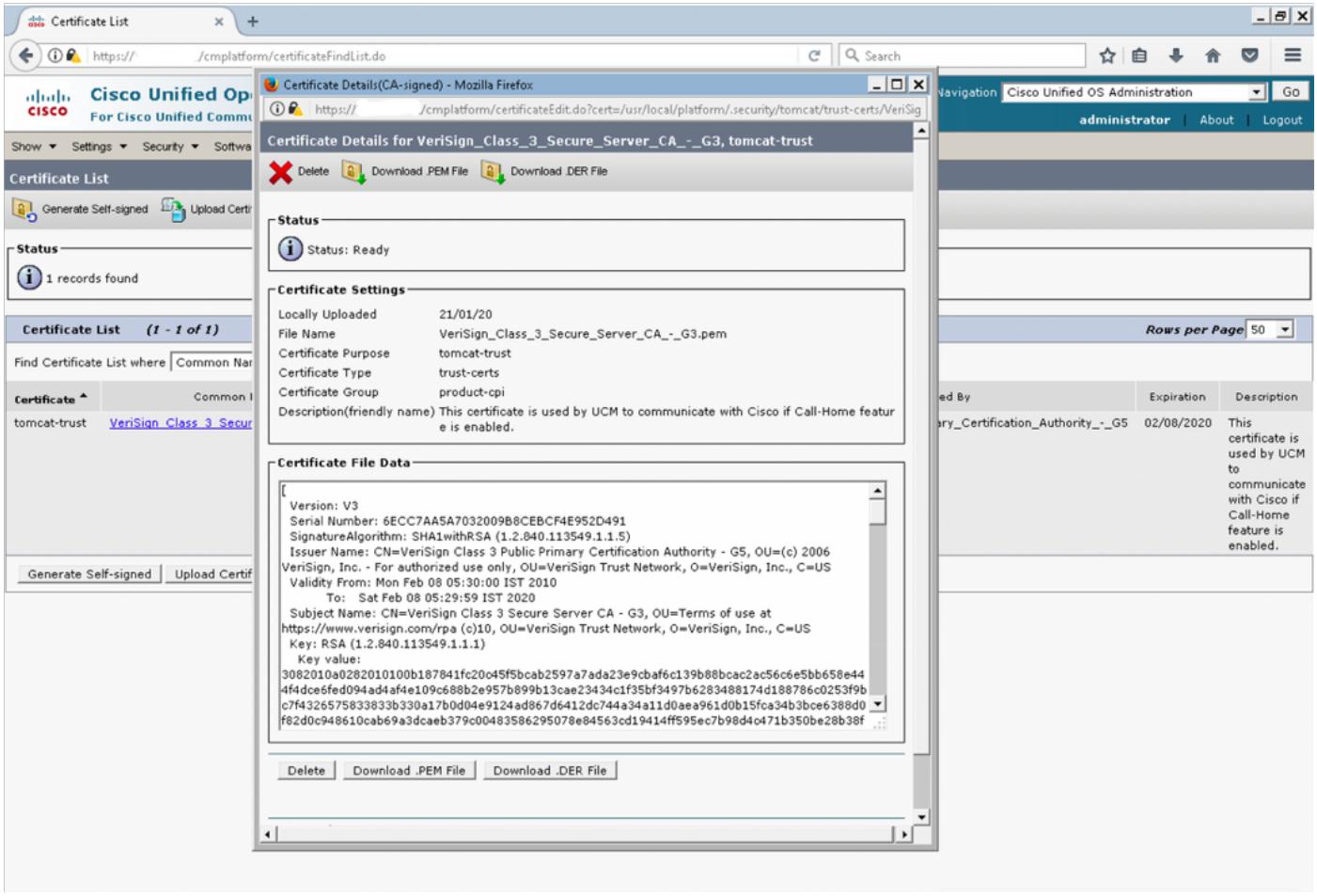
Passaggio 1. Accedere all'interfaccia utente grafica di amministrazione del sistema operativo Cisco Unified nel server di pubblicazione e fare clic su **Security > Certificate Management**



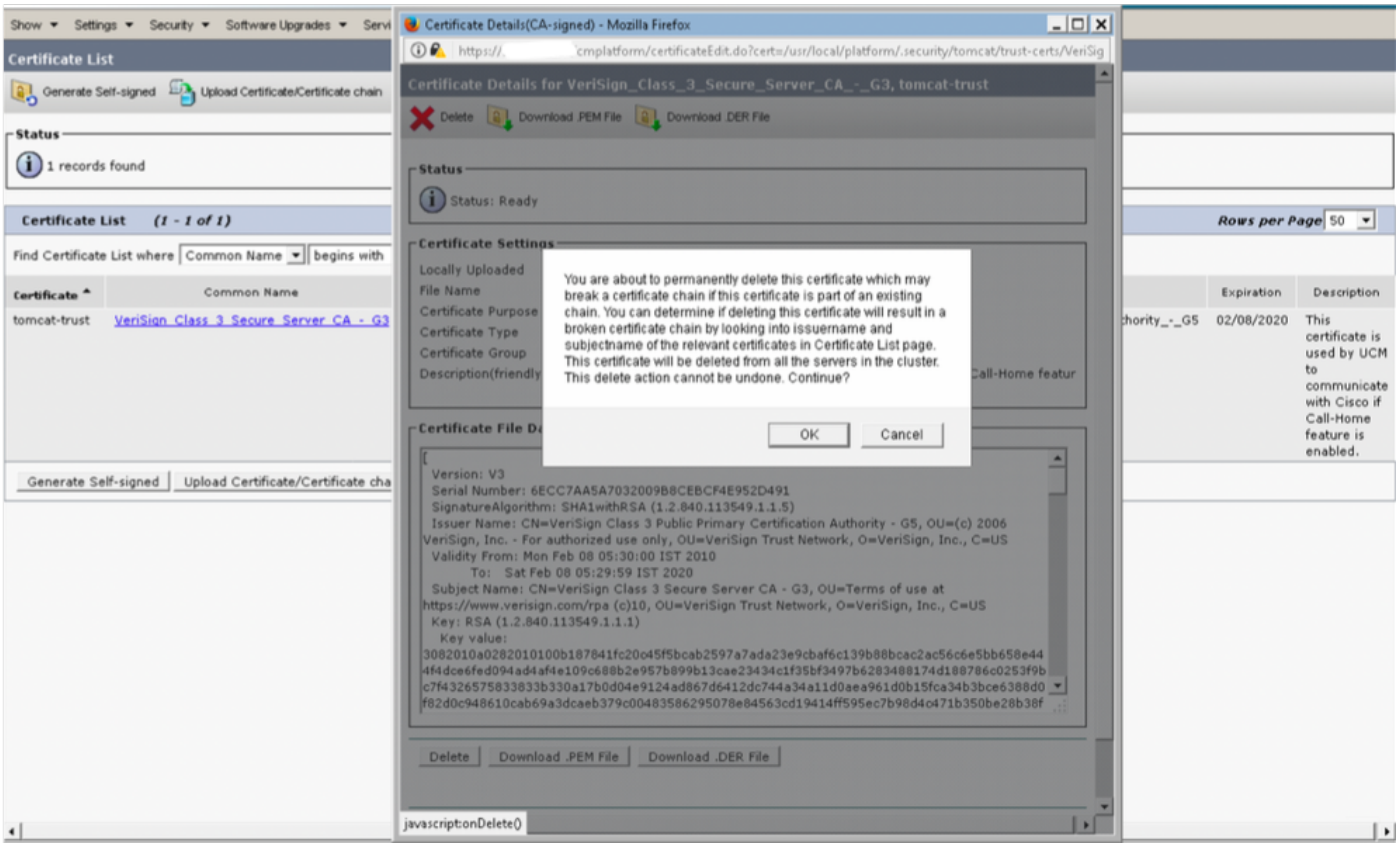
Passaggio 2. Trovare l'elenco dei certificati in cui il nome comune contiene VeriSign

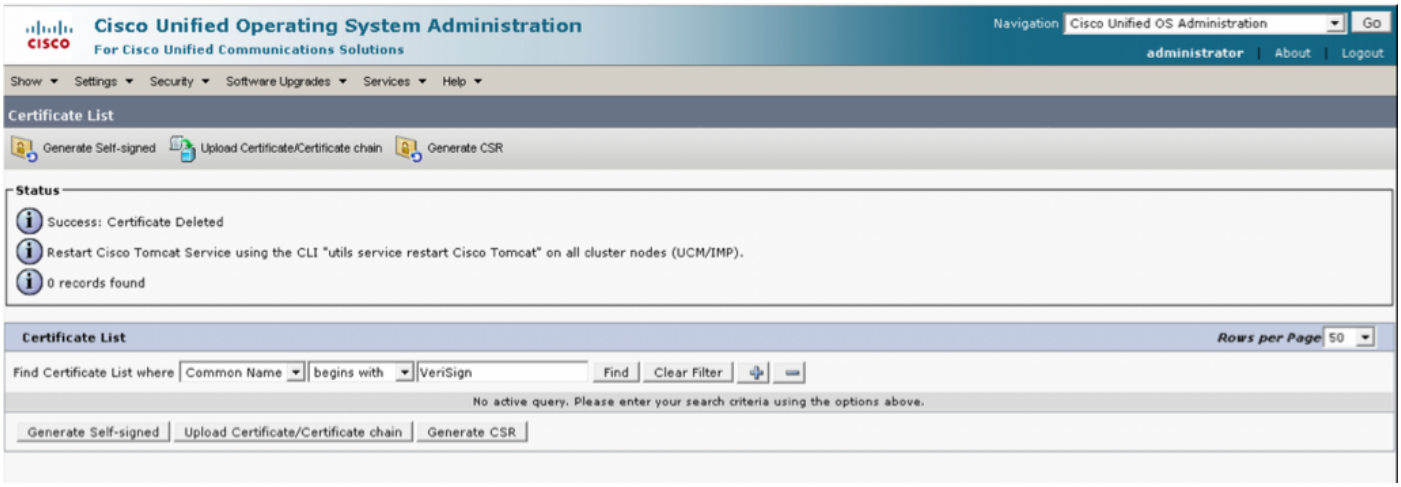


Passaggio 3. Fare clic su **VeriSign_Class_3_Secure_Server_CA_-_G3** e verrà visualizzata la finestra popup che evidenzia i dettagli del certificato



Passaggio 4. Fare clic sul pulsante **Elimina** e viene visualizzato un avviso. Fare clic su **OK**. Eliminare il certificato da tutti i nodi del cluster.

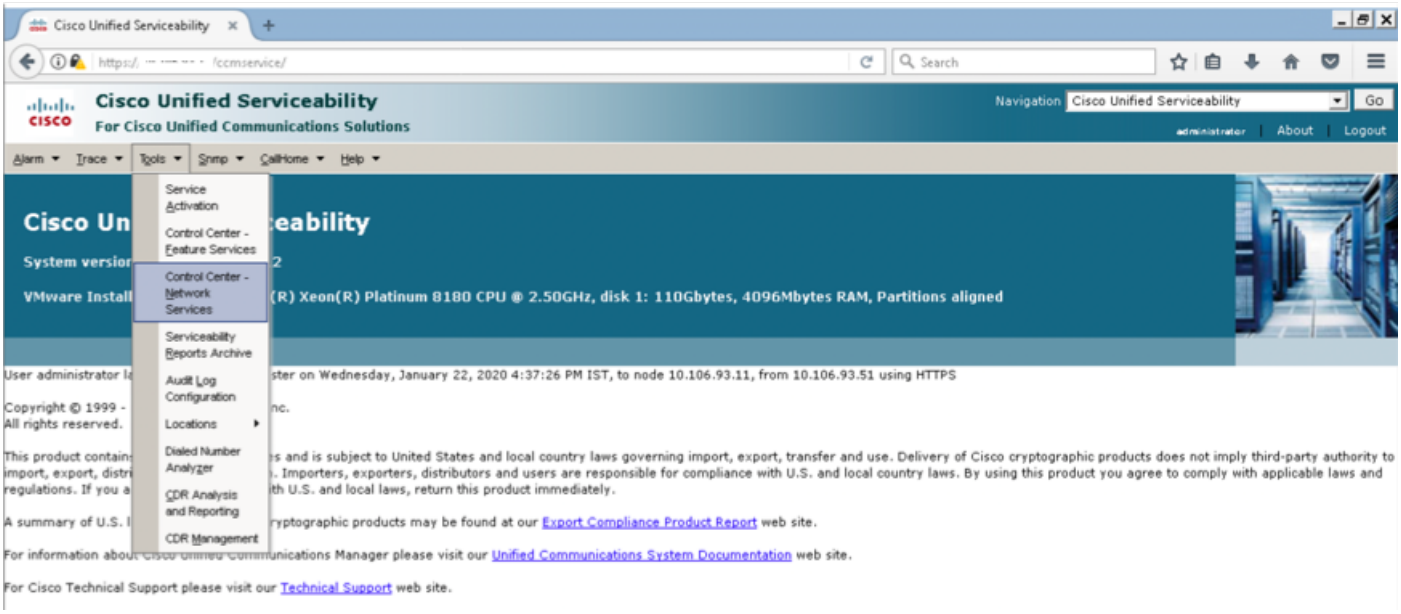




Per tutte le altre versioni

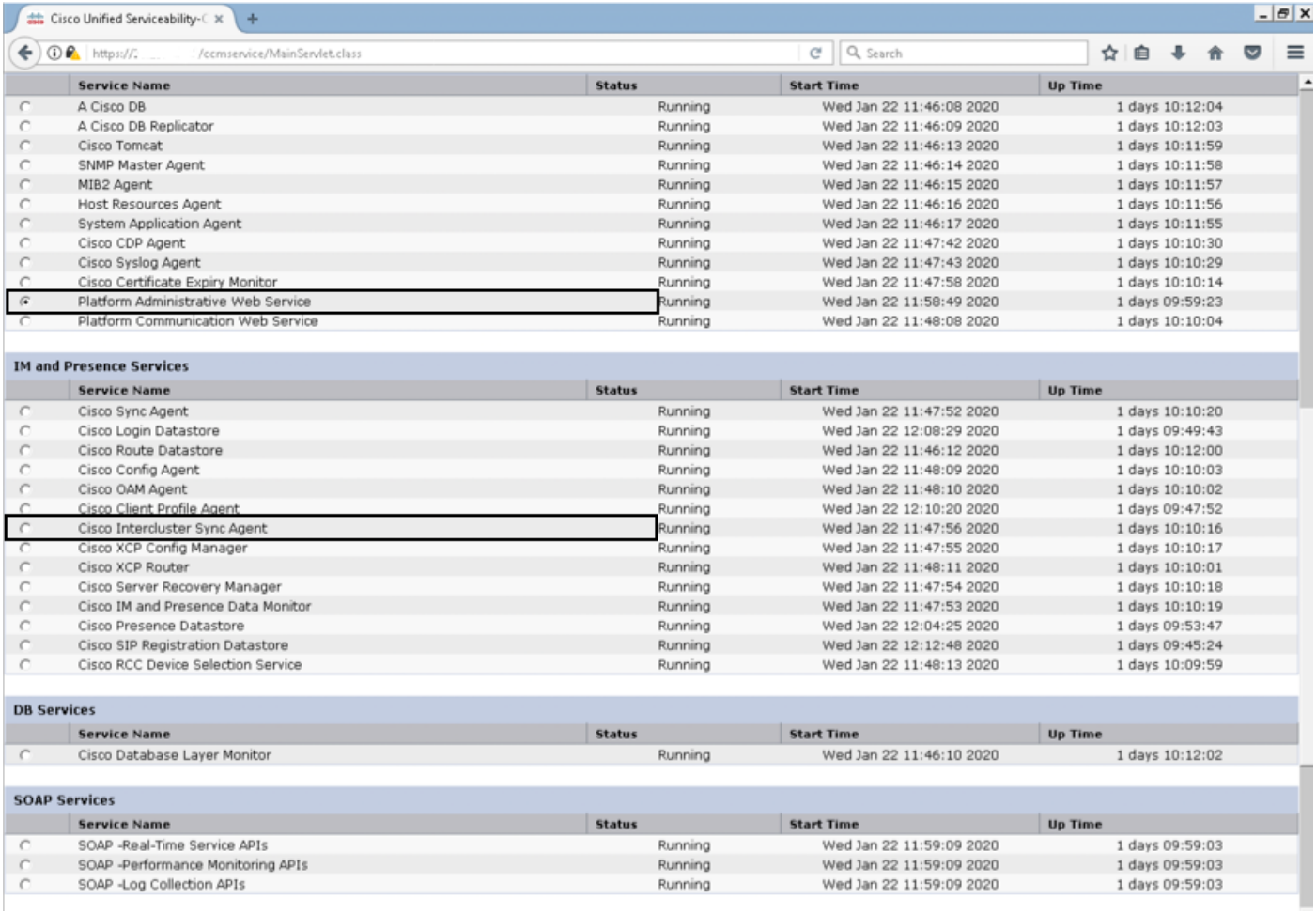
Prima di eliminare il certificato, è necessario eseguire i passaggi seguenti

Passaggio 1. Passare a **Cisco Unified Serviceability > Strumenti > Control Center - Servizi di rete**



Passaggio 2. Arrestare la **notifica di modifica del certificato Cisco** in tutti i nodi del cluster

Passaggio 3. In caso di IM e Presence Server, arrestare **Platform Administration, Web Services** e **Cisco Intercluster Sync Agent**



Passaggio 4. Eliminare il certificato su tutti i nodi, inclusi Messaggistica immediata e Presenza, come descritto nella sezione *Soluzione per la versione 11.0(1) e successive* di questo documento

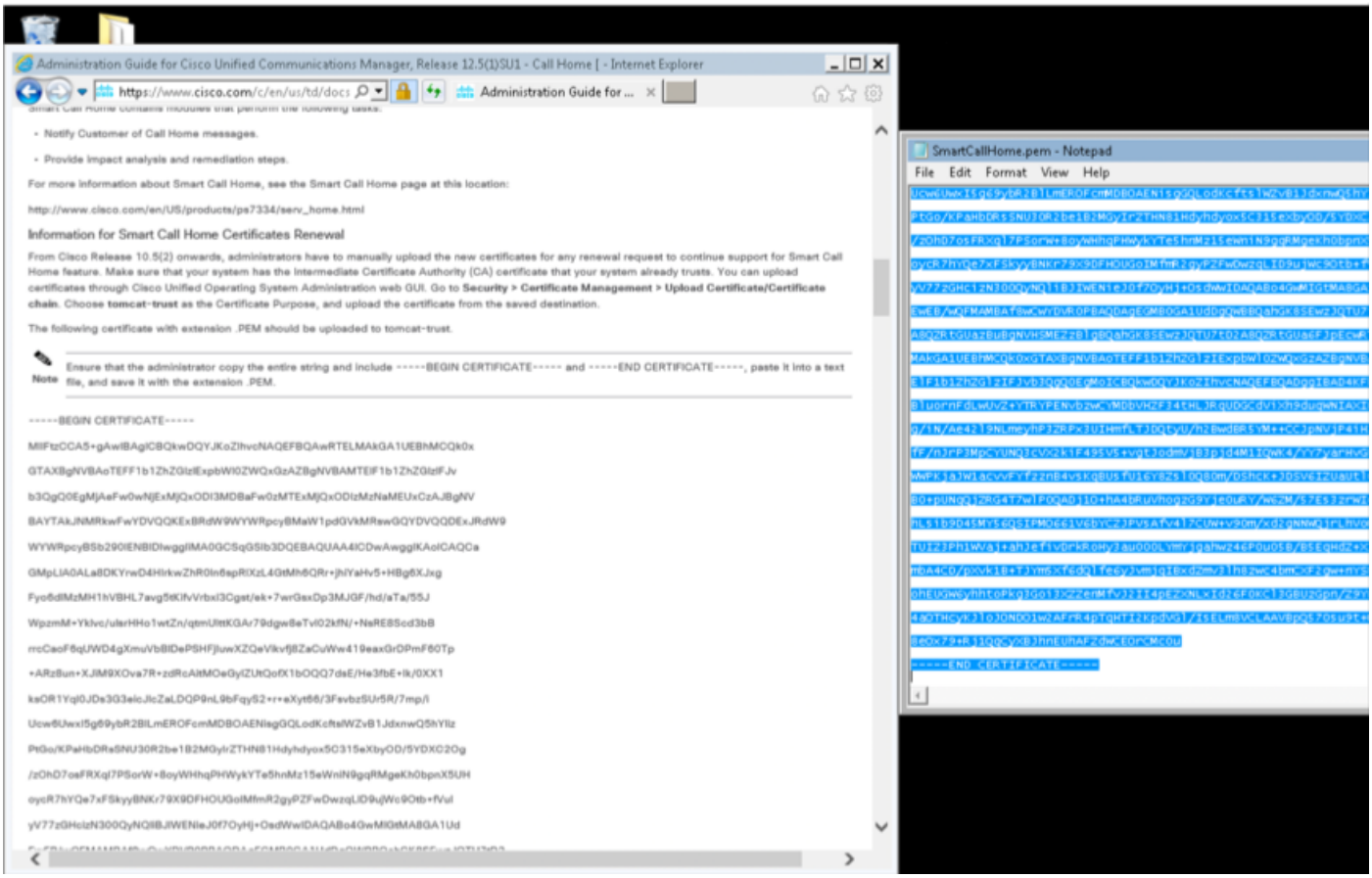
Passaggio 5. Avviare il servizio arrestato nel Passaggio 2. e nel Passaggio 3.

> **Nota:** Se si elimina il certificato e si esegue un aggiornamento prima del 7 febbraio 2020, il certificato verrà nuovamente visualizzato dopo l'aggiornamento e dovrà essere rimosso di nuovo. Gli aggiornamenti successivi al 7 febbraio 2020 non aggiungeranno nuovamente il certificato

Procedura di rinnovo dei certificati Smart Call Home

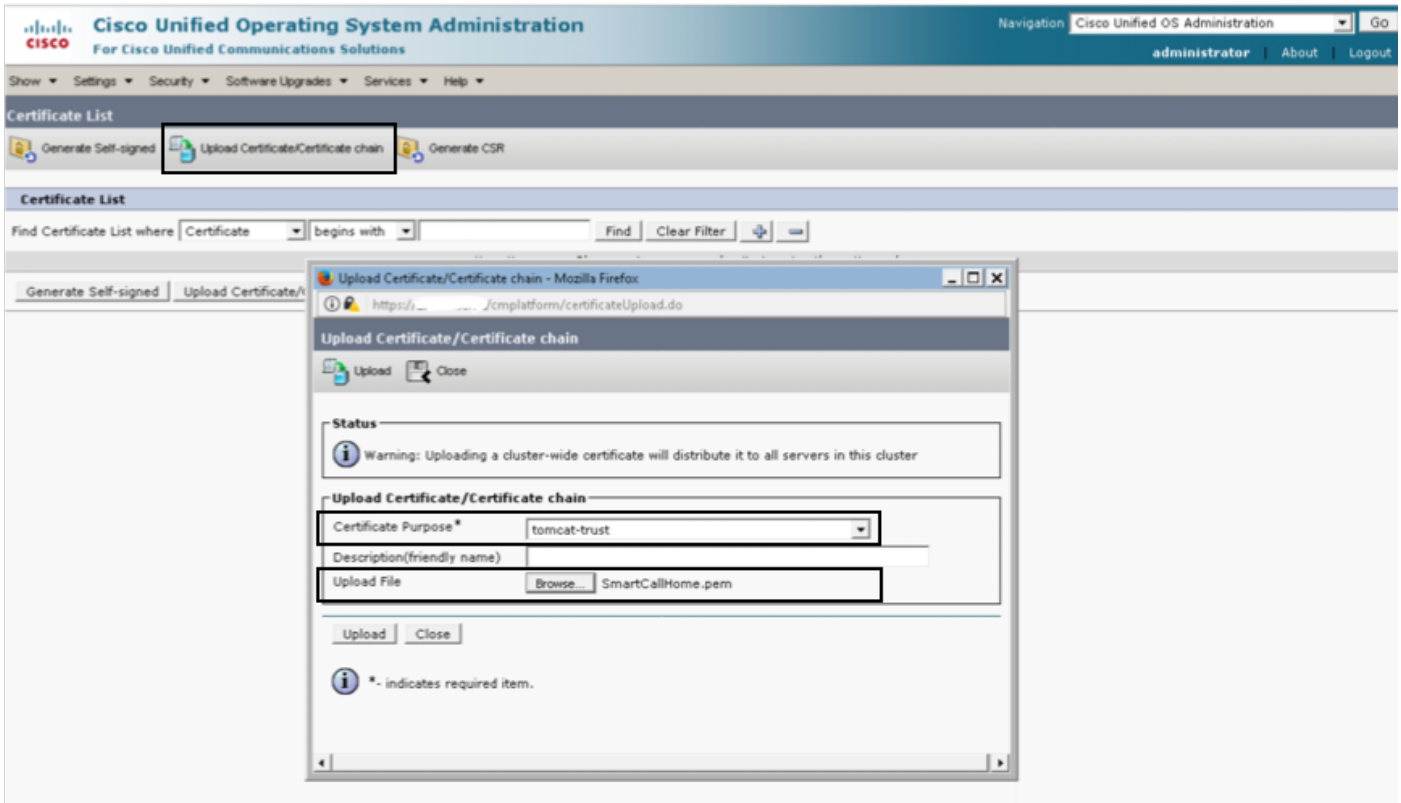
Se Smart Call Home è disabilitato, non sono necessarie ulteriori azioni dopo l'eliminazione del certificato. Se Smart Call Home è abilitato, seguire la procedura

Passaggio 1. Copiare il contenuto del certificato dalla sezione UCM Administration Guide *Information for Smart Call Home Certificates*



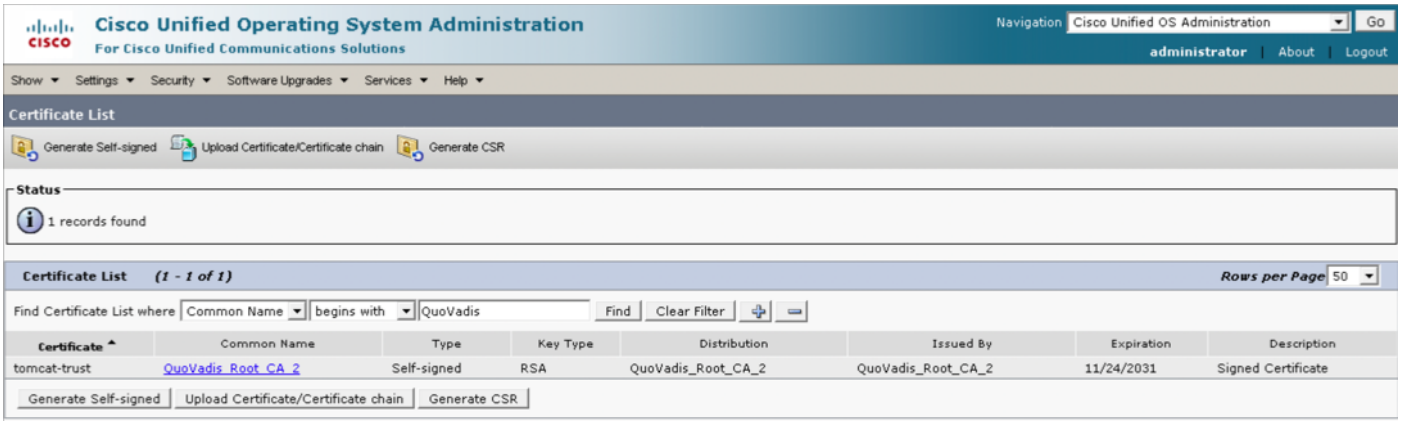
Nota: Lo stesso certificato è valido per la versione 10.5 e successive

Passaggio 2. Caricare il file .pem come tomcat-trust nella pagina Cisco Unified OS Administration GUI **Certificate Management** per lo screenshot



Passaggio 3. Verificare che **QuoVadis_Root_CA_2** sia elencato come tomcat-trust individuando il

certificato in cui il nome comune contiene QuoVadis



Per Cisco Prime License Manager

Per Prime License Manager 10.5

Il certificato scaduto (VeriSign_Class_3_Secure_Server_CA_-_G3) può essere eliminato dal sistema applicando questo file COP (ciscocm.plm-CSCvs64158_remove_sch_cert_C0050-1.k3.cop.sgn). Per istruzioni sull'installazione, consultare il file Leggimi.

Per Prime License Manager 11.5

Il certificato scaduto (VeriSign_Class_3_Secure_Server_CA_-_G3) può essere eliminato dal sistema applicando questo file COP (ciscocm.plm-CSCvs64158_remove_sch_cert_C0050-1.k3.cop.sgn). Per istruzioni sull'installazione, consultare il file Leggimi.