

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

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Problema](#)

[Soluzione](#)

[Soluzione per la versione 11.0\(1\) e successive](#)

[Per tutte le altre versioni](#)

[Procedura di rinnovo dei certificati Smart Call Home](#)

[Per Cisco Prime License Manager](#)

[Per Prime License Manager 10.5](#)

[Per Prime License Manager 11.5](#)

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

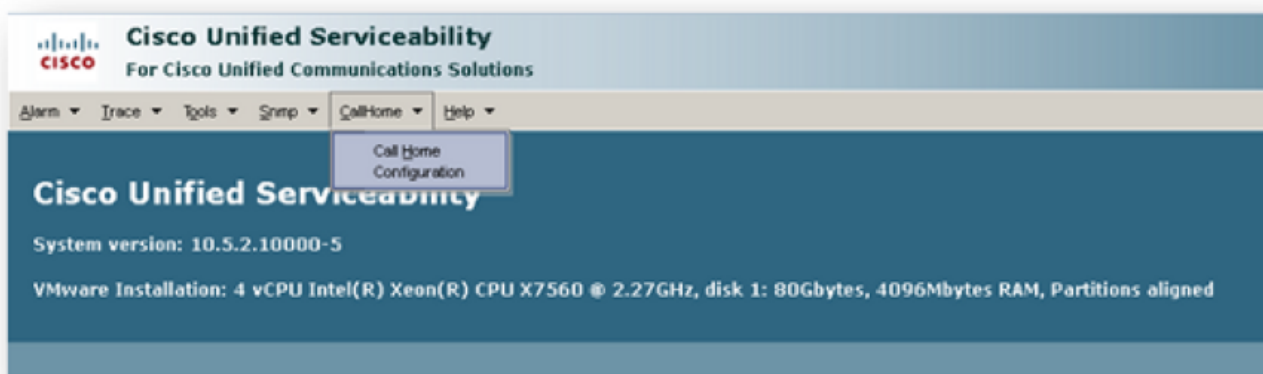
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze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

Premesse

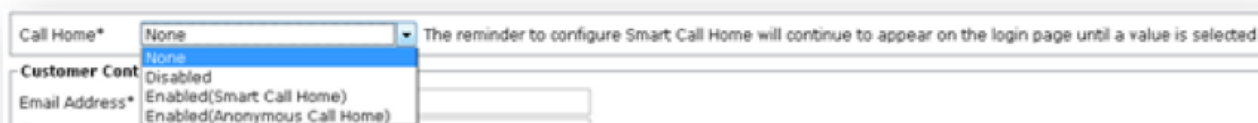
Smart Call Home è una funzionalità di supporto automatizzato per il monitoraggio dei dispositivi Cisco della rete. La funzione Call Home consente di comunicare e inviare gli avvisi di diagnostica, l'inventario e altri messaggi al server back-end Smart Call Home.

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]
```

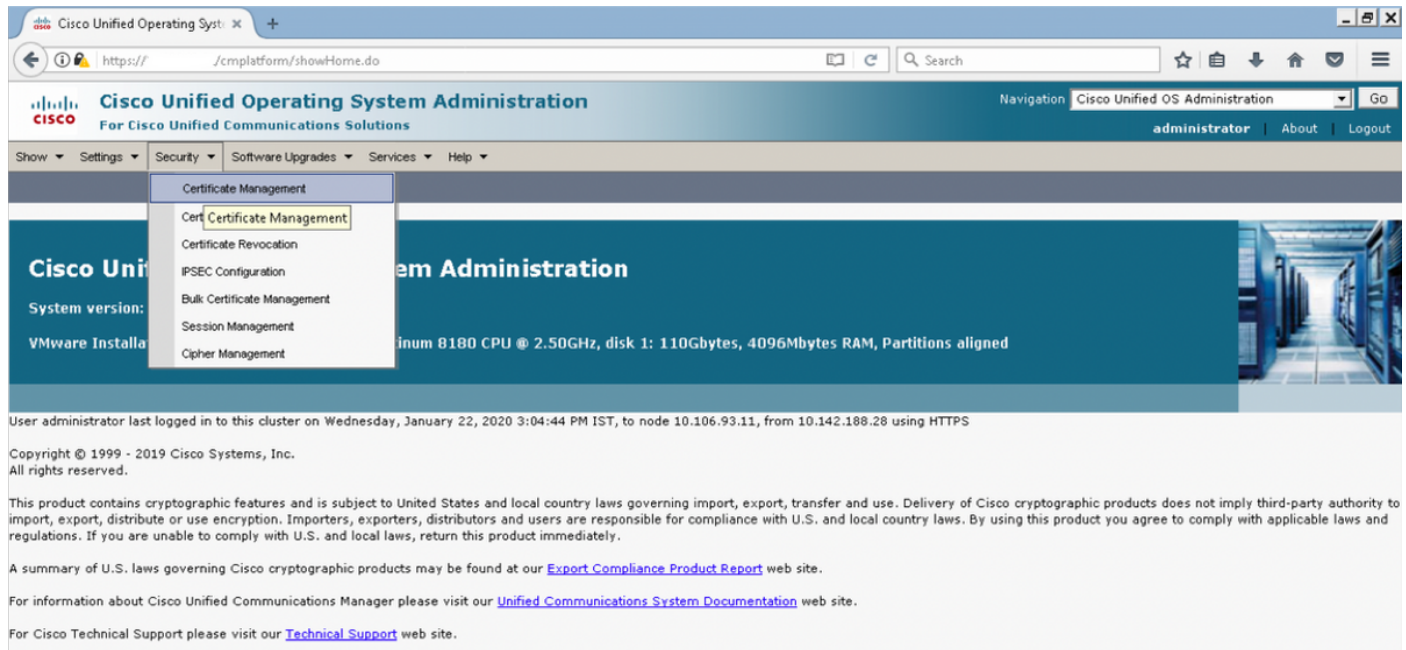
Soluzione

Questo problema è documentato dall'ID bug Cisco [CSCvs64158](#).

Soluzione per la versione 11.0(1) e successive

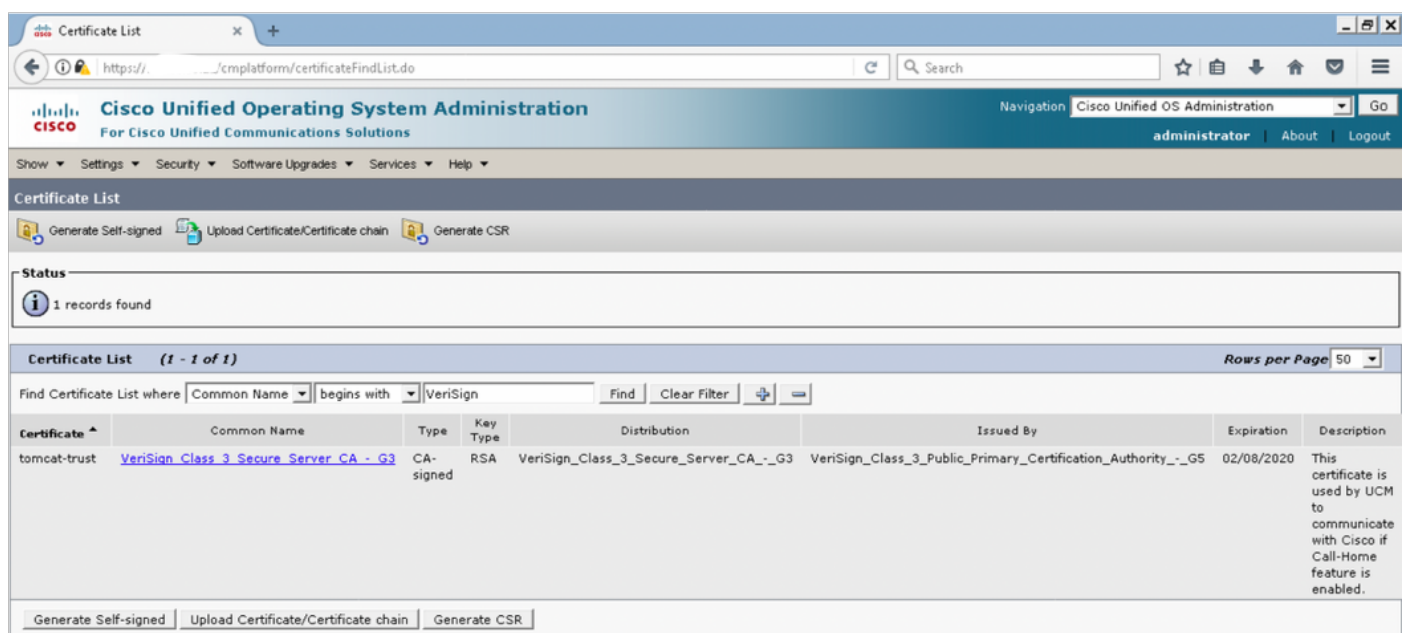
Per eliminare il certificato scaduto è necessario eseguire la procedura seguente (VeriSign_Class_3_Secure_Server_CA_-_G3.der)

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**



The screenshot shows the Cisco Unified Operating System Administration web interface. The user is logged in as 'administrator'. The 'Security' menu is expanded, and 'Certificate Management' is selected. The main content area displays system information: 'System version: VMware Install...', 'CPU: Intel Xeon 8180 CPU @ 2.50GHz', and 'disk 1: 110Gbytes, 4096Mbytes RAM, Partitions aligned'. A footer contains copyright information and legal disclaimers.

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



The screenshot shows the 'Certificate List' page in the Cisco Unified Operating System Administration interface. The search filter is set to 'VeriSign'. The table below shows the search results.

Certificate	Common Name	Type	Key Type	Distribution	Issued By	Expiration	Description
tomcat-trust	VeriSign_Class_3_Secure_Server_CA_-_G3	CA-signed	RSA	VeriSign_Class_3_Secure_Server_CA_-_G3	VeriSign_Class_3_Public_Primary_Certification_Authority_-_G5	02/08/2020	This certificate is used by UCM to communicate with Cisco if Call-Home feature is enabled.

Passaggio 3. Fare clic su [VeriSign_Class_3_Secure_Server_CA_-_G3](#) e verrà visualizzata la finestra popup che evidenzia i dettagli del certificato

Certificate List

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
  Signature Algorithm: 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
  4f4dce6fed094ad4af4e109c688b2e957b899b13cae23434cf35bf3497b6283488174d188786c0253f9b
  c7f4326575833833b330a17b0d04e9124ad867d6412dc744a34a11d0aa961d0b15fca34b3bce6388d0
  f82d0c948610cab69a3dcaeb379c00483586295078e84563cd19414ff595ec7b98d4c471b350be28b38f
]
  
```

Delete Download .PEM File Download .DER File

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.

Certificate List

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

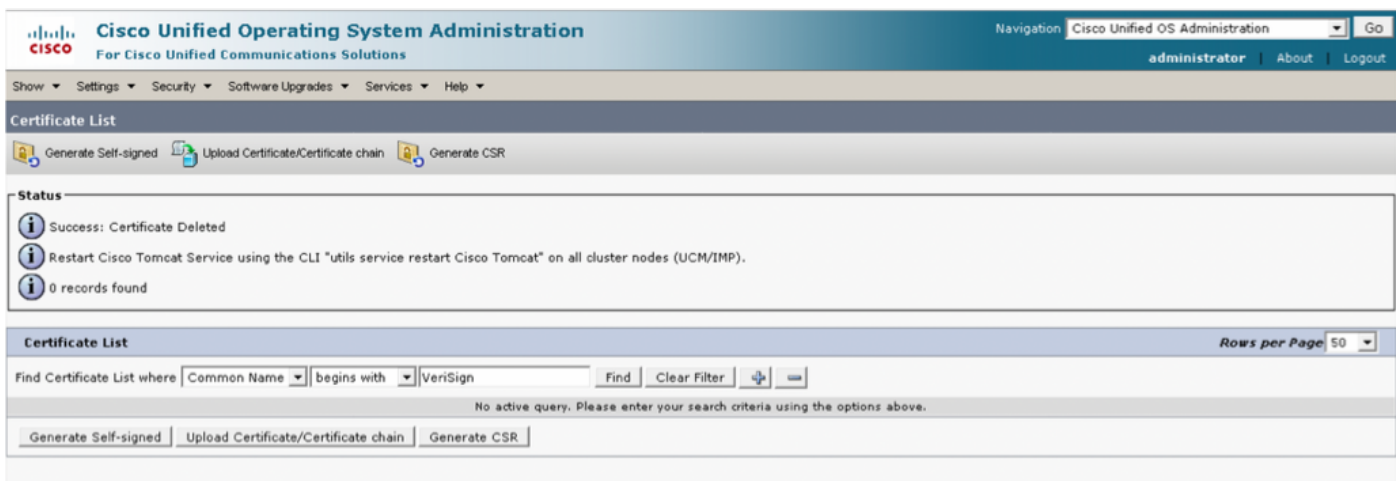
```

[
  Version: V3
  Serial Number: 6ECC7AA5A7032009B8CEBCF4E952D491
  Signature Algorithm: 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
  4f4dce6fed094ad4af4e109c688b2e957b899b13cae23434cf35bf3497b6283488174d188786c0253f9b
  c7f4326575833833b330a17b0d04e9124ad867d6412dc744a34a11d0aa961d0b15fca34b3bce6388d0
  f82d0c948610cab69a3dcaeb379c00483586295078e84563cd19414ff595ec7b98d4c471b350be28b38f
]
  
```

Delete Download .PEM File Download .DER File

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?

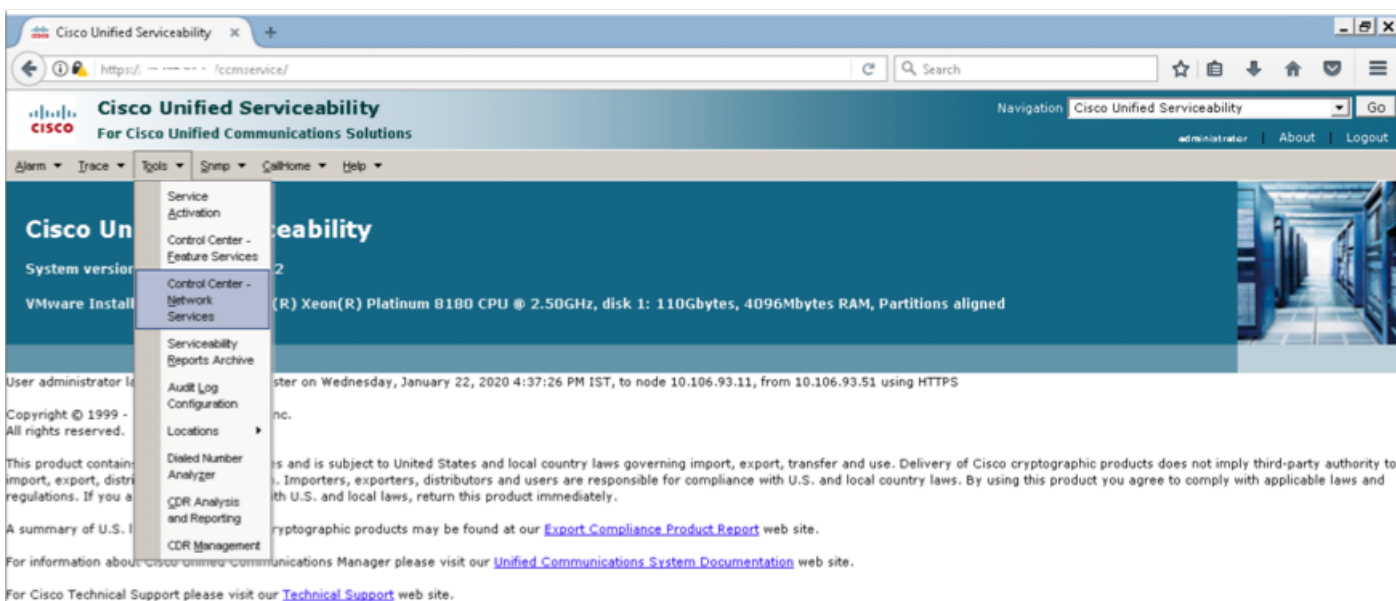
OK Cancel



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**

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

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

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

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

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](#)

certificato in cui il nome comune contiene QuoVadis

Cisco Unified Operating System Administration
For Cisco Unified Communications Solutions

Navigation Cisco Unified OS Administration Go
administrator | About | Logout

Show Settings Security Software Upgrades Services Help

Certificate List

Generate Self-signed Upload Certificate/Certificate chain Generate CSR

Status
1 records found

Certificate List (1 - 1 of 1) Rows per Page 50

Find Certificate List where Common Name begins with QuoVadis Find Clear Filter

Certificate	Common Name	Type	Key Type	Distribution	Issued By	Expiration	Description
tomcat-trust	QuoVadis_Root_CA_2	Self-signed	RSA	QuoVadis_Root_CA_2	QuoVadis_Root_CA_2	11/24/2031	Signed Certificate

Generate Self-signed Upload Certificate/Certificate chain Generate CSR

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.