Configurazione di Secure RTP in Contact Center Enterprise

Sommario

Introduzione

Questo documento descrive come proteggere il traffico SRTP (Real-time Transport Protocol) nel flusso completo delle chiamate di Contact Center Enterprise (CCE).

Prerequisiti

La generazione e l'importazione di certificati non rientrano nell'ambito del presente documento, pertanto è necessario creare e importare nei rispettivi componenti certificati per Cisco Unified Communication Manager (CUCM), Customer Voice Portal (CVP) Call Server, Cisco Virtual Voice Browser (CVB) e Cisco Unified Border Element (CUBE). Se si utilizzano certificati autofirmati, lo scambio di certificati deve essere eseguito tra componenti diversi.

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- CCE
- CVP
- CUBO
- CUCM
- CVB

Componenti usati

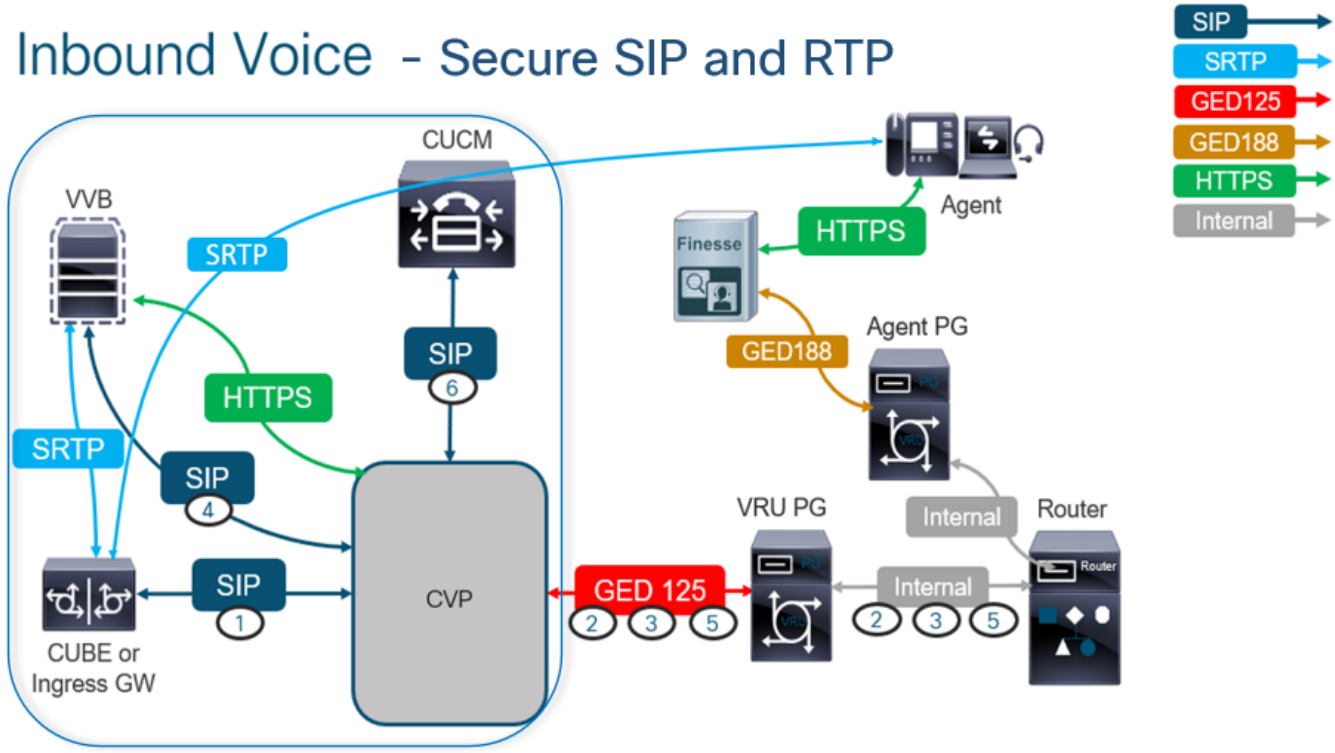
Le informazioni di questo documento si basano sulla versione 12.6 di Package Contact Center Enterprise (PCCE), CVP, CVB e CUCM, ma sono valide anche per le versioni precedenti.

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.

Configurazione

> **Nota**: nel flusso chiamate completo del contact center, per abilitare il RTP sicuro, devono essere abilitati i segnali SIP sicuri. Pertanto, le configurazioni descritte in questo documento consentono sia il SIP sicuro che l'SRTP.

Il diagramma seguente mostra i componenti coinvolti nei segnali SIP e RTP nel flusso di chiamata completo del contact center. Quando una chiamata vocale arriva al sistema, viene prima effettuata tramite il gateway in entrata o CUBE, quindi avviare le configurazioni su CUBE. Quindi, configurare CVP, CVB e CUCM.



Task 1: configurazione protetta CUBE

In questa attività, è possibile configurare CUBE per proteggere i messaggi del protocollo SIP e il protocollo RTP.

Configurazioni richieste:

- Configurare un trust point predefinito per l'interfaccia utente SIP
- Modificare i peer di composizione per l'utilizzo di TLS e SRTP

Passaggi:

1. Aprire una sessione SSH in CUBE.

2. Eseguire questi comandi per fare in modo che lo stack SIP utilizzi il certificato CA del CUBO. CUBE stabilisce la connessione SIP TLS da/a CUCM (198.18.133.3) e CVP (198.18.133.13):

Conf t Sip-ua Transport tcp tls v1.2 crypto signaling remote-addr 198.18.133.3 255.255.255.255 trustpoint ms-ca-name crypto signaling remote-addr 198.18.133.13 255.255.255.255 trustpoint ms-ca-name exit

```
CC-VCUBE(config)#sip-ua
CC-VCUBE(config-sip-ua)#transport tcp tls v1.2
CC-VCUBE(config-sip-ua)#crypto signaling remote-addr 198.18.133.3 255.255.255.255 trustpoint ms-ca-name
CC-VCUBE(config-sip-ua)#crypto signaling remote-addr 198.18.133.13 255.255.255.255 trustpoint ms-ca-name
CC-VCUBE(config-sip-ua)#exit
CC-VCUBE(config)#
```

3. Eseguire questi comandi per abilitare TLS sul dial peer in uscita verso CVP. Nell'esempio, il dial-peer tag 6000 viene usato per indirizzare le chiamate a CVP:

Conf t dial-peer voice 6000 voip session target ipv4:198.18.133.13:5061 session transport tcp tls srtp exit

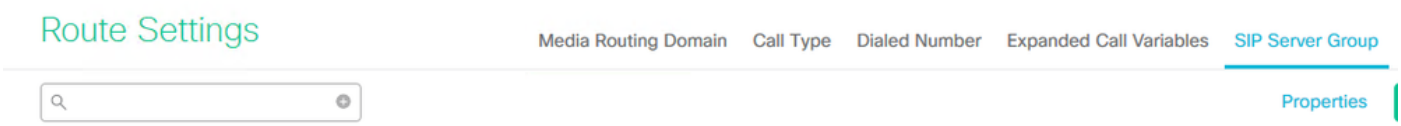
```
CC-VCUBE#
CC-VCUBE#Conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CC-VCUBE(config)#dial-peer voice 6000 voip
CC-VCUBE(config-dial-peer)#session target ipv4:198.18.133.13:5061
CC-VCUBE(config-dial-peer)#session transport tcp tls
CC-VCUBE(config-dial-peer)#SRTP
CC-VCUBE(config-dial-peer)#exit
CC-VCUBE(config)#
CC-VCUBE(config)#
```

Task 2: configurazione sicura di CVP

In questa attività, configurare il server di chiamata CVP per proteggere i messaggi del protocollo SIP (SIP TLS).

Passaggi:

1. Accedi a UCCE Web Administration.
2. Passa a Call Settings > Route Settings > SIP Server Group.

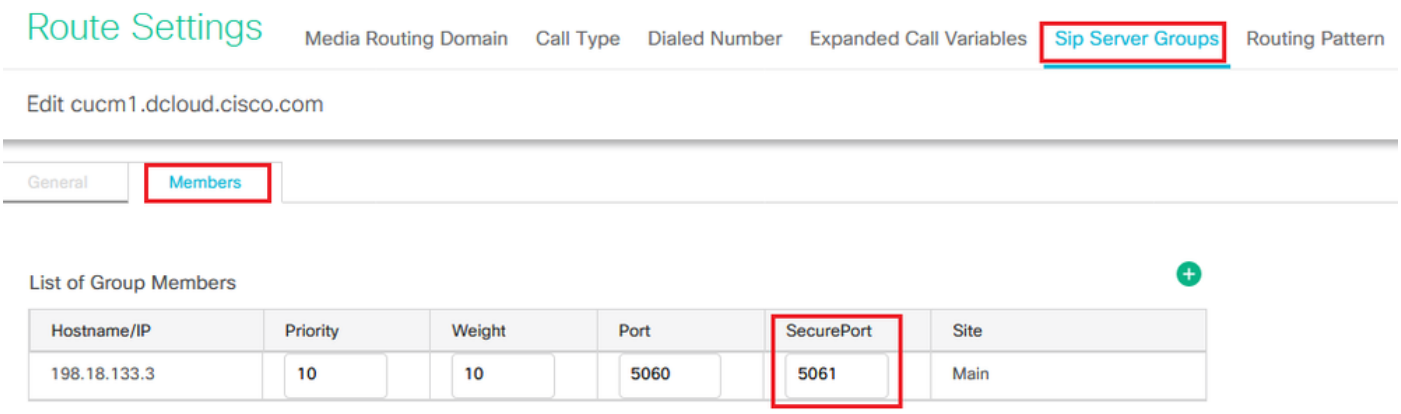


In base alle configurazioni, sono stati configurati i gruppi di server SIP per CUCM, CVB e CUBE. Per tutte le porte SIP protette, è necessario impostarle su 5061. Nell'esempio vengono utilizzati i seguenti gruppi di server SIP:

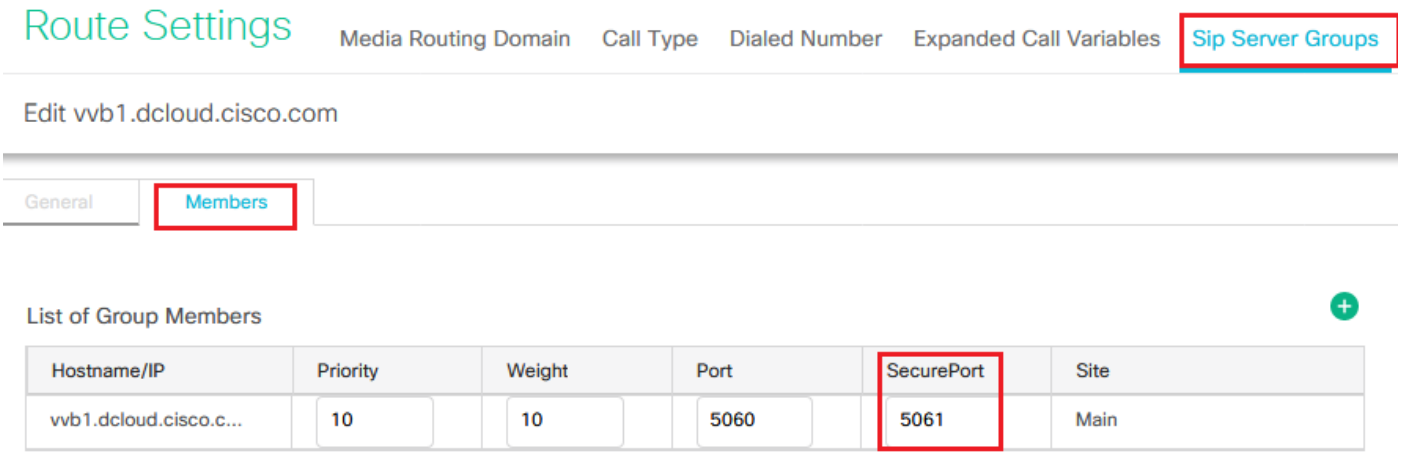
- cucm1.dcloud.cisco.com per CUCM

- vvb1.dcloud.cisco.com per CVB
- cube1.dcloud.cisco.com per CUBE

3. Clic cucm1.dcloud.cisco.come quindi nella Members che mostra i dettagli delle configurazioni dei gruppi di server SIP. Imposta SecurePort a 5061 e fare clic su Save.



4. Clic vvb1.dcloud.cisco.com e quindi nella Members , impostare la scheda **SecurePort** a 5061 e fare clic su Save.

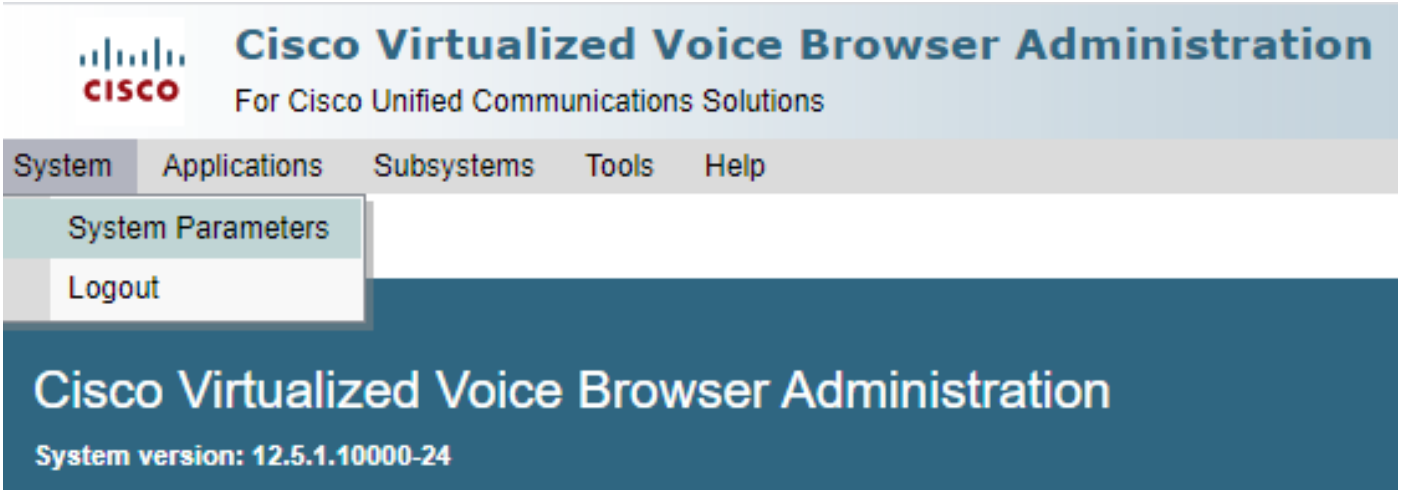


Task 3: configurazione sicura di CVB

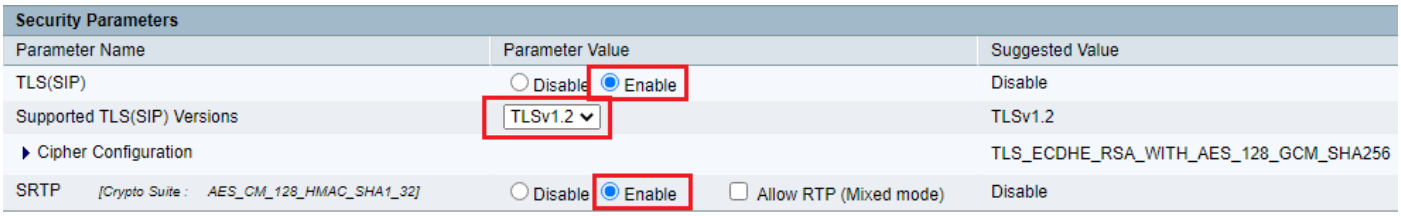
In questa attività, configurare CVB per proteggere i messaggi del protocollo SIP (SIP TLS) e SRTP.

Passaggi:

1. Aprire il Cisco VVB Admin pagina.
2. Passa a System > System Parameters.

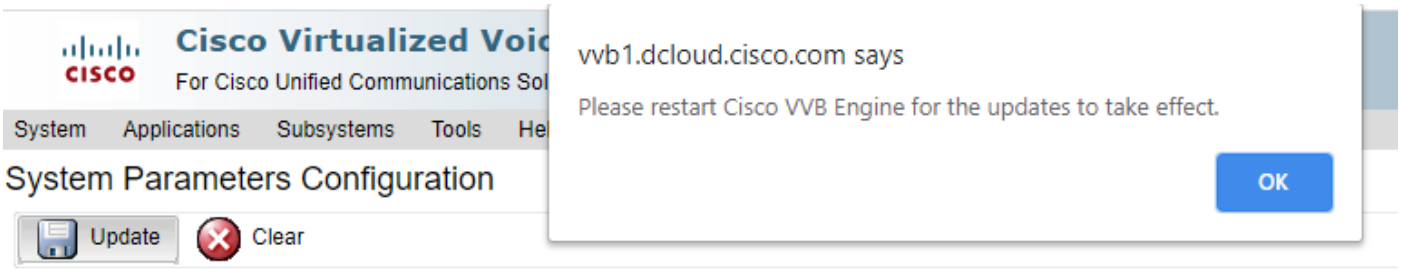


3. Nella scheda Security Parameters , scegliere Enable per TLS (SIP) . Mantieni Supported TLS(SIP) version as TLSv1.2 e scegliere Enable per SRTP.

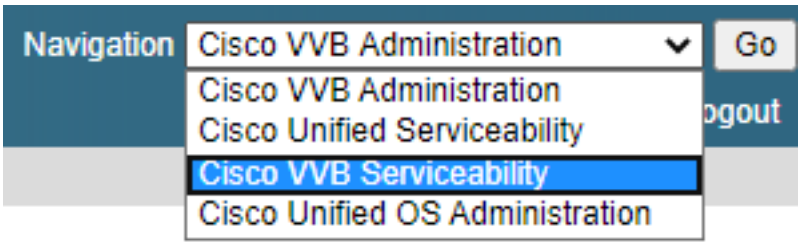


Security Parameters		
Parameter Name	Parameter Value	Suggested Value
TLS(SIP)	Disable / Enable	Disable
Supported TLS(SIP) Versions	TLSv1.2	TLSv1.2
Cipher Configuration		TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
SRTP [Crypto Suite : AES_CM_128_HMAC_SHA1_32]	Disable / Enable / Allow RTP (Mixed mode)	Disable

4. Clic **Update**. Clic Ok quando viene richiesto di riavviare il motore CVB.

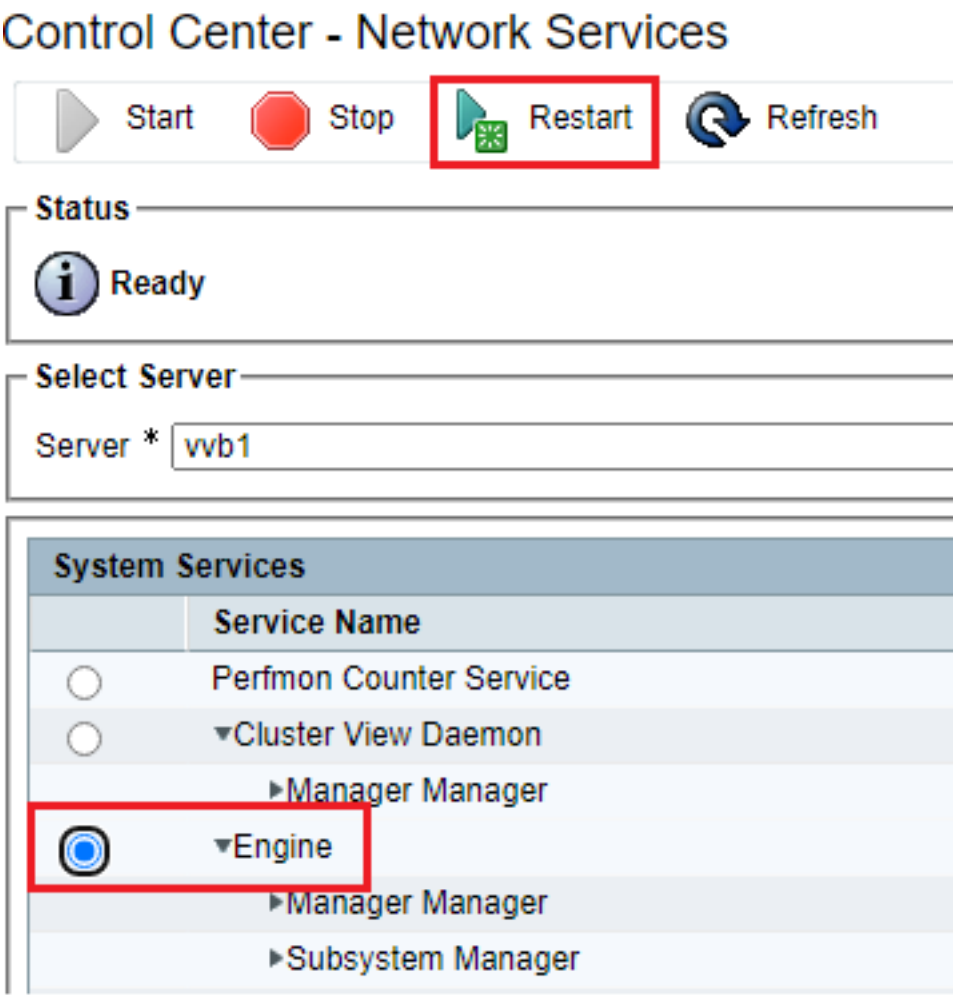


5. Queste modifiche richiedono il riavvio del motore Cisco VB. Per riavviare il motore VB, passare alla Cisco VVB Serviceability , quindi scegliere **Go**.



6. Passa a Tools > Control Center – Network Services.

7. Scegli Engine e fare clic su Restart.



Task 4: configurazione sicura di CUCM

Per proteggere i messaggi SIP e RTP su CUCM, eseguire le seguenti configurazioni:

- Impostare la modalità di protezione CUCM sulla modalità mista
- Configurare i profili di sicurezza trunk SIP per CUBE e CVP
- Associare i profili di sicurezza trunk SIP ai rispettivi trunk SIP e abilitare SRTP
- Comunicazione dei dispositivi degli agenti di sicurezza con CUCM

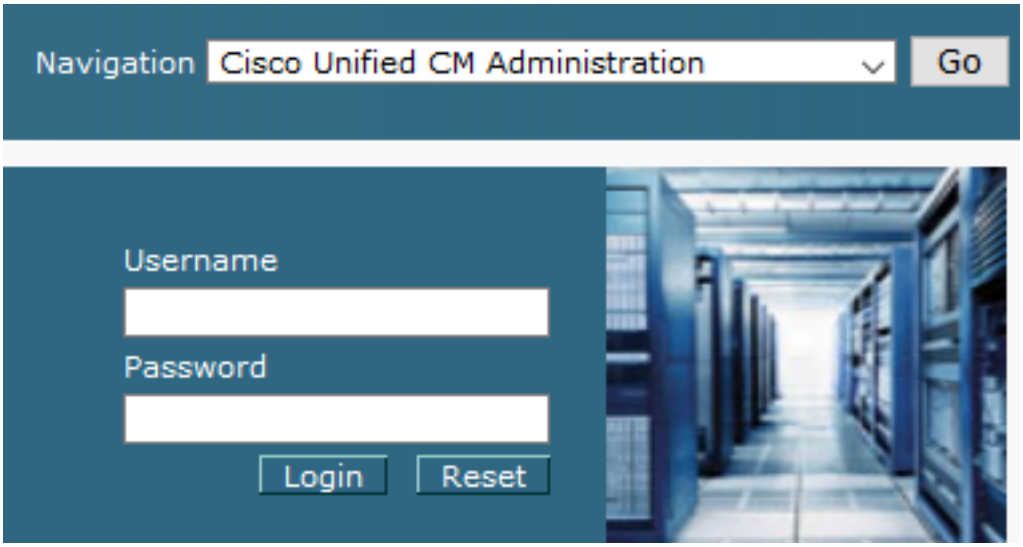
Impostare la modalità di protezione CUCM sulla modalità mista

CUCM supporta due modalità di protezione:

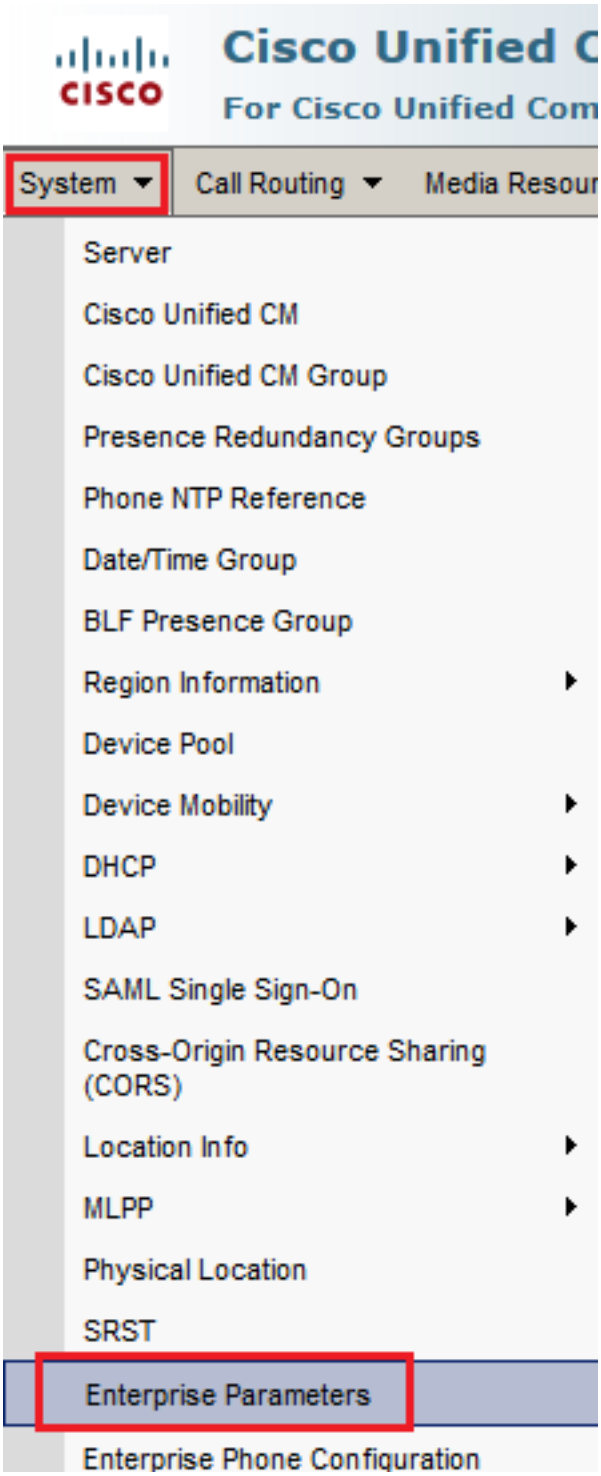
- Modalità non protetta (modalità predefinita)
- Modalità mista (modalità protetta)

Passaggi:

1. Accedere all'interfaccia di amministrazione CUCM.



2. Quando si accede a CUCM, è possibile passare a **System > Enterprise Parameters**.

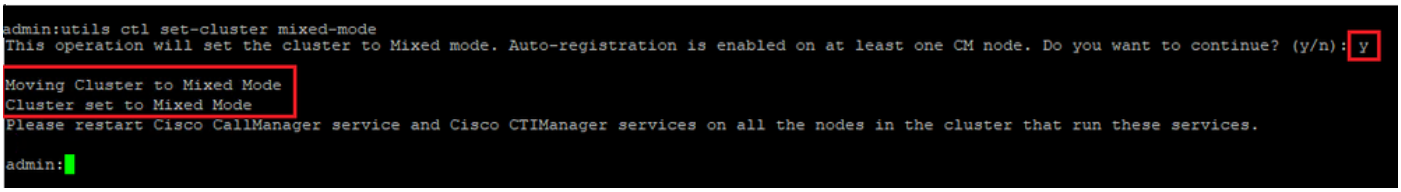


3. Nell'ambito Security Parameters , verificare se il Cluster Security Mode è impostato su 0.

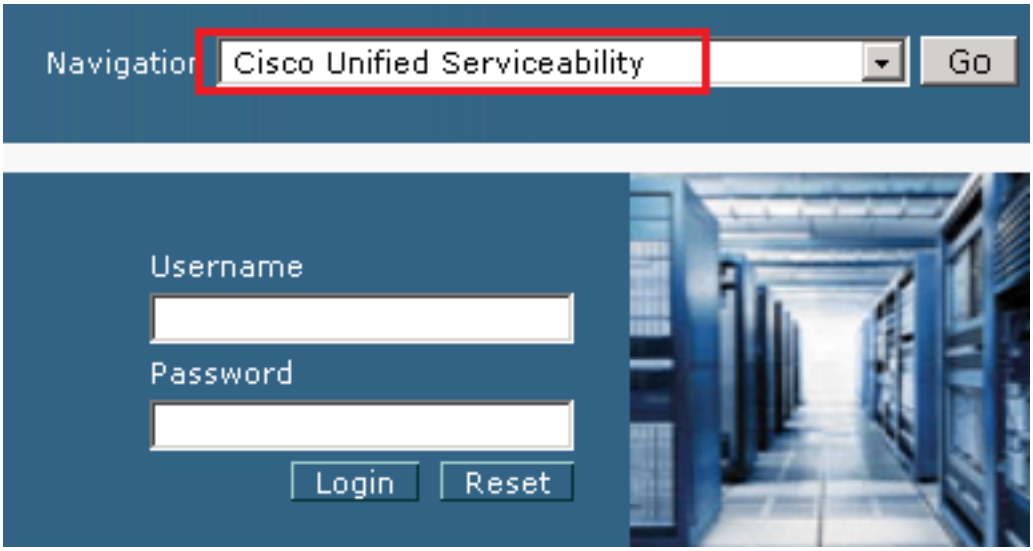
4. Se la modalità di protezione del cluster è impostata su 0, significa che la modalità di protezione del cluster è impostata su non protetta. è necessario abilitare la modalità mista dalla CLI.
5. Aprire una sessione SSH su CUCM.
6. Dopo aver eseguito correttamente l'accesso a CUCM tramite SSH, eseguire questo comando:

utils ctl set-cluster mixed-mode

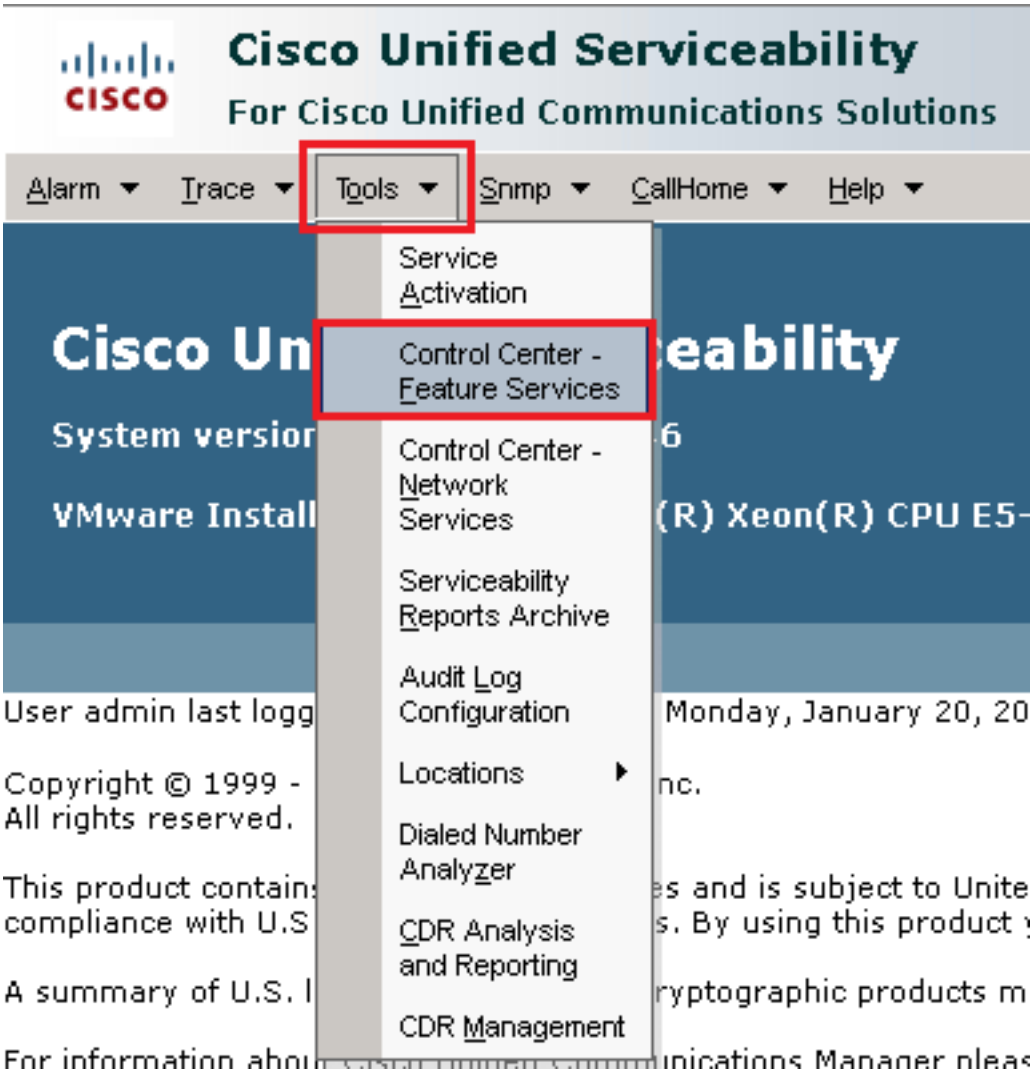
7. Tipo y e fare clic su Enter quando richiesto. Con questo comando viene impostata la modalità di protezione cluster su mista.



8. Per rendere effettive le modifiche, riavviare il Cisco CallManager e Cisco CTIManager servizi.
9. Per riavviare i servizi, spostarsi e accedere a **Cisco Unified Serviceability**.

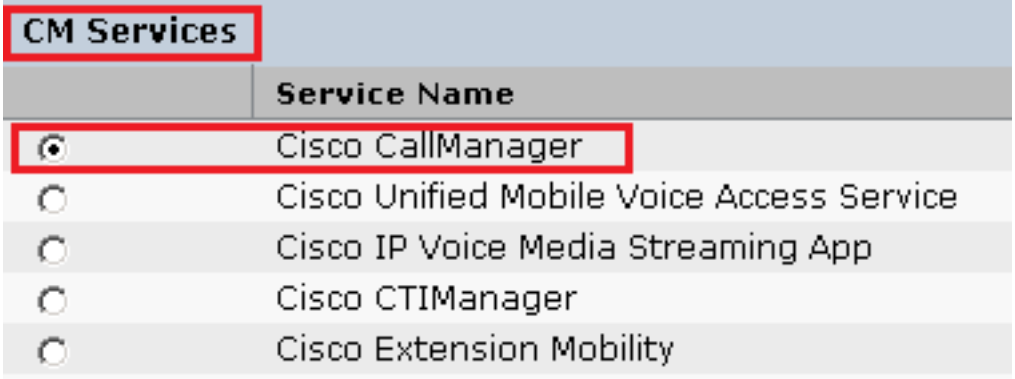


10. Dopo aver eseguito correttamente l'accesso, passare a Tools > Control Center – Feature Services.

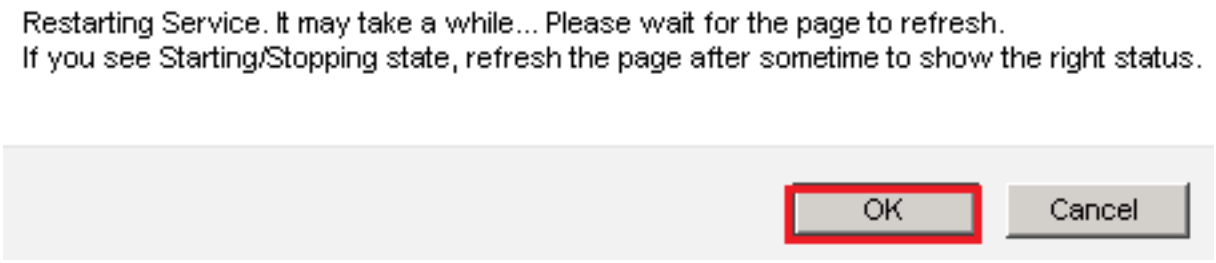


11. Scegliere il server, quindi fare clic su Go.

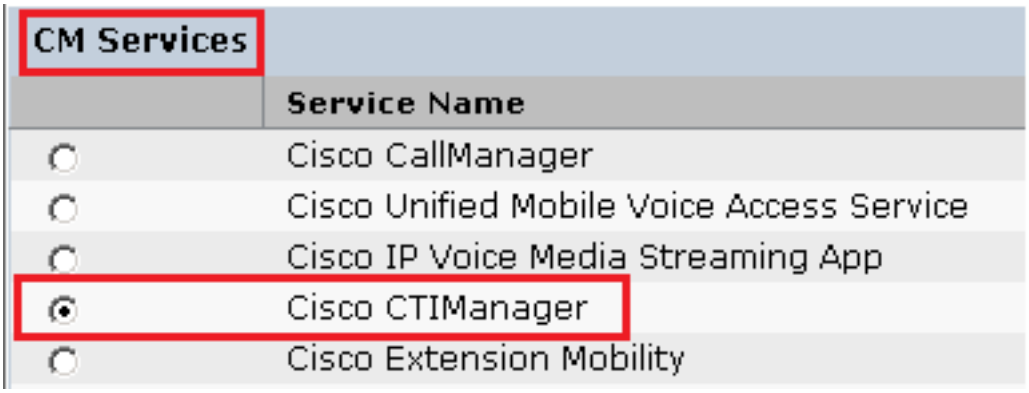
12. Sotto i servizi CM, scegliere Cisco CallManager , quindi scegliere Restart nella parte superiore della pagina.



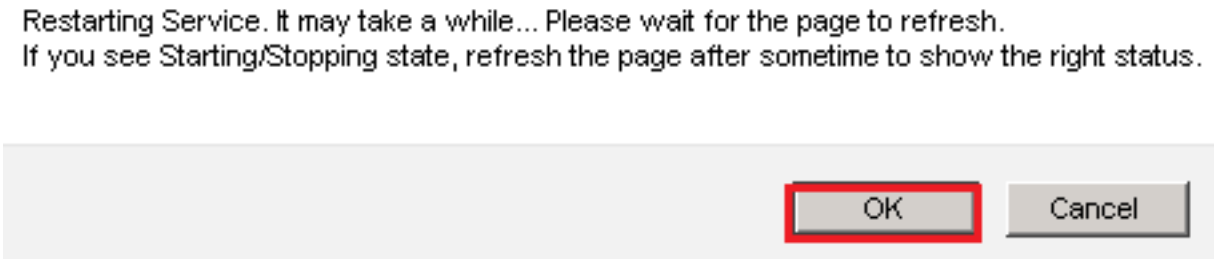
13. Confermare il messaggio e fare clic su OK. Attendere il riavvio del servizio.



14. Dopo il riavvio di Cisco CallManager, scegliere il **Cisco CTIManager** quindi fare clic su Restart pulsante per il riavvio Cisco CTIManager servizio.



15. Confermare il messaggio e fare clic su OK. Attendere il riavvio del servizio.

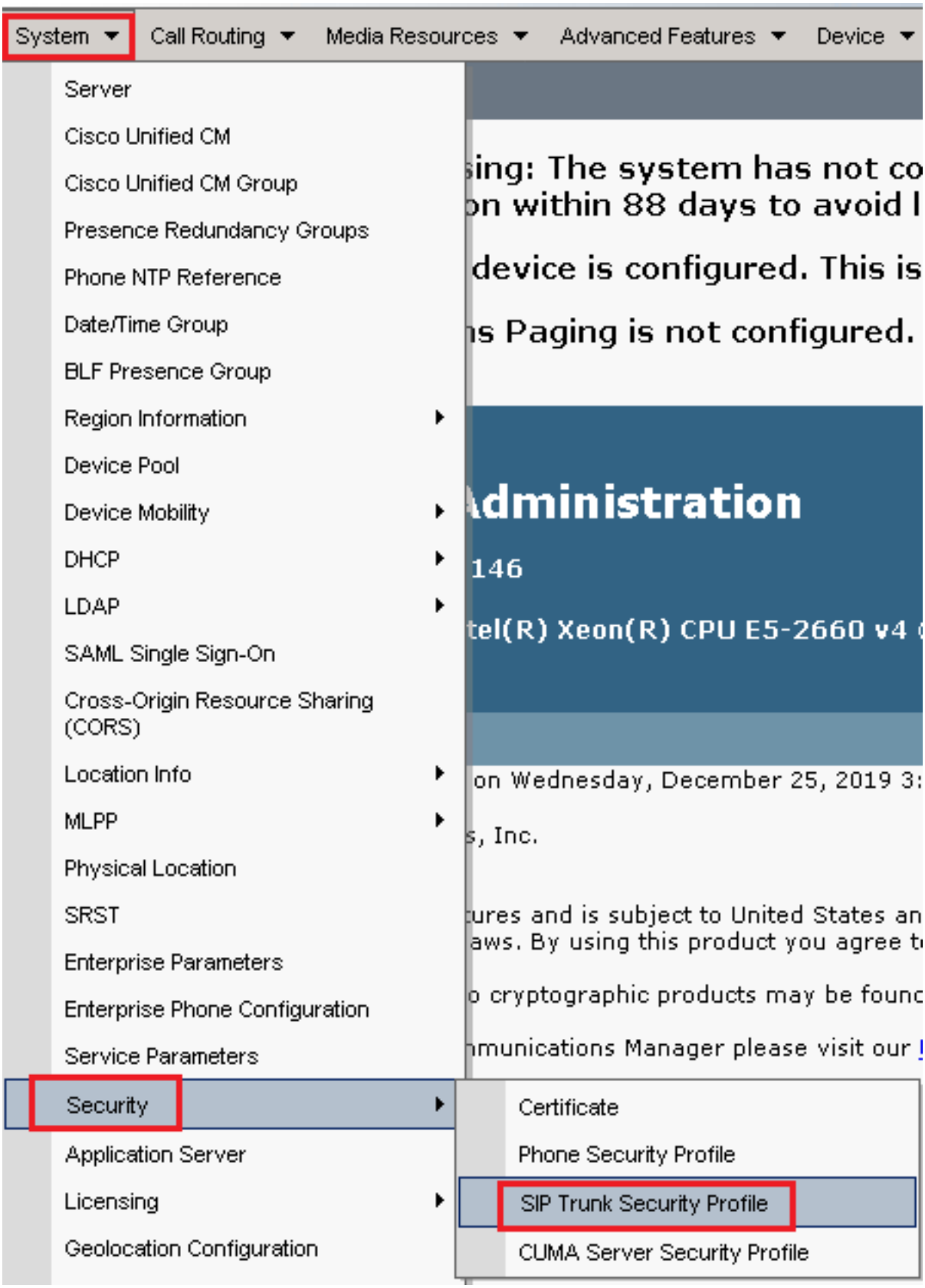


16. Dopo il riavvio corretto dei servizi, per verificare che la modalità di protezione del cluster sia impostata sulla modalità mista, passare all'amministrazione CUCM come illustrato nel passaggio 5. e quindi controllare la Cluster Security Mode. Ora deve essere impostato su 1.

Configurare i profili di sicurezza trunk SIP per CUBE e CVP

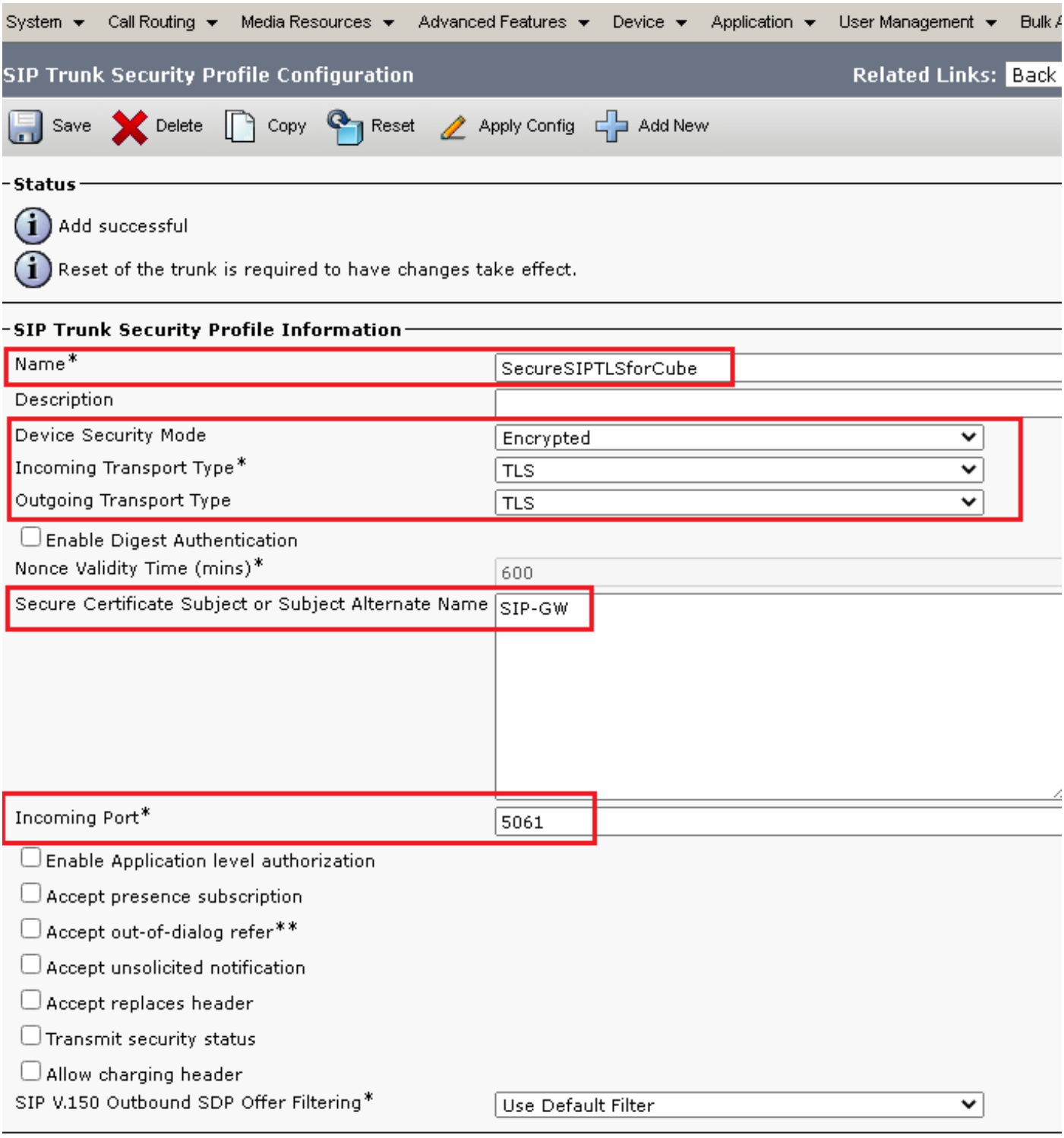
Passaggi:

1. Accedere all'interfaccia di amministrazione CUCM.
2. Dopo aver eseguito correttamente l'accesso a CUCM, passare a System > Security > SIP Trunk Security Profile per creare un profilo di sicurezza del dispositivo per CUBE.



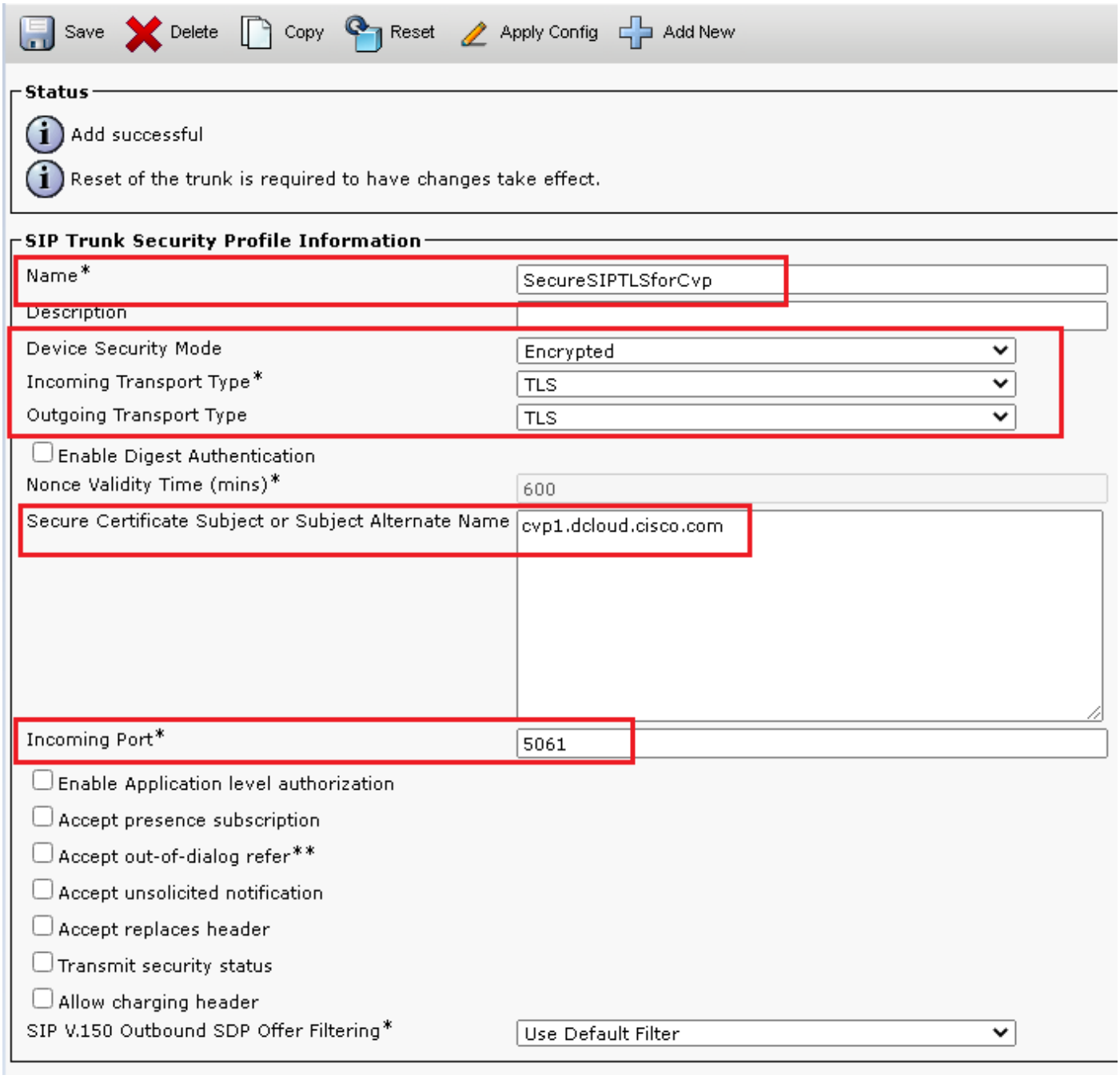
3. In alto a sinistra, fare clic su **Add New** (Aggiungi nuovo) per aggiungere un nuovo profilo.

4. Configurazione SIP Trunk Security Profile come questa immagine e fare clic su Save in basso a sinistra.



5. Assicurarsi di impostare Secure Certificate Subject or Subject Alternate Name al nome comune (CN) del certificato CUBE in quanto deve corrispondere.

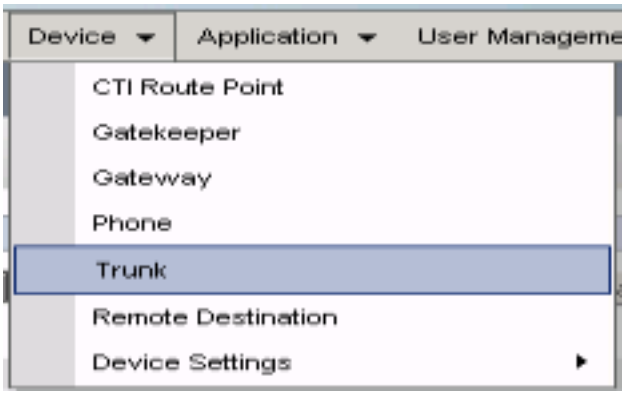
6. Fare clic su Copy e modificare il Name a SecureSipTLSforCVP. Cambia Secure Certificate Subject al CN del certificato del server di chiamata CVP come deve corrispondere. Clic Save pulsante.



Associazione dei profili di sicurezza trunk SIP ai rispettivi trunk SIP e abilitazione SRTP

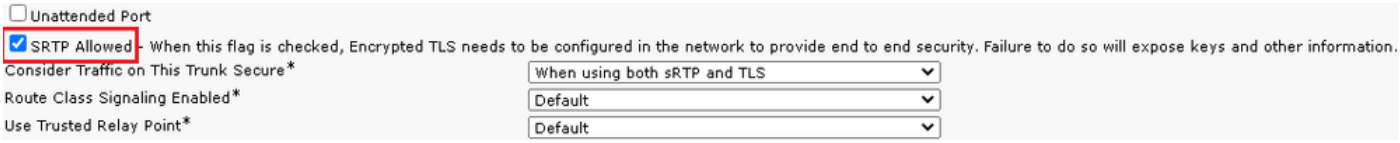
Passaggi:

1. Nella pagina Amministrazione CUCM, passare a Device > Trunk.

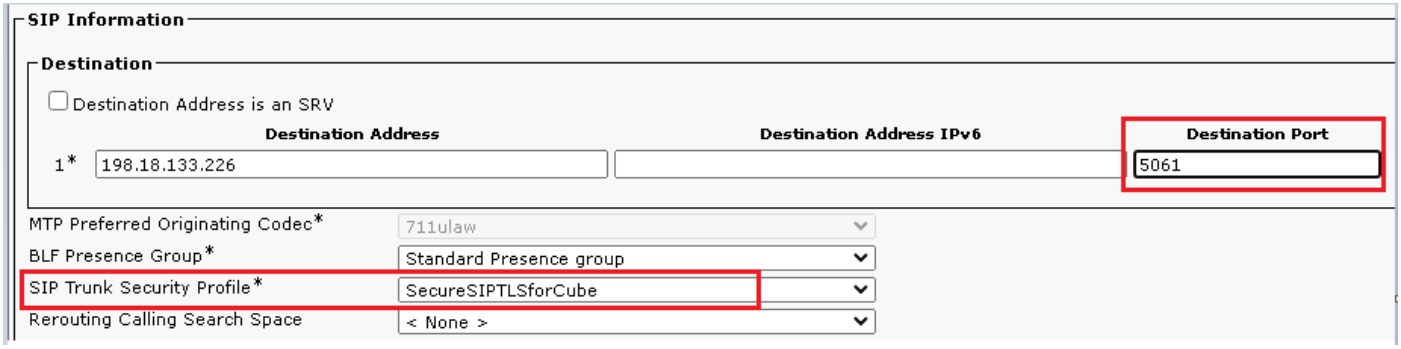


2. Cerca il trunk CUBE. In questo esempio, il nome del trunk CUBE è vCube , quindi scegliere Find.

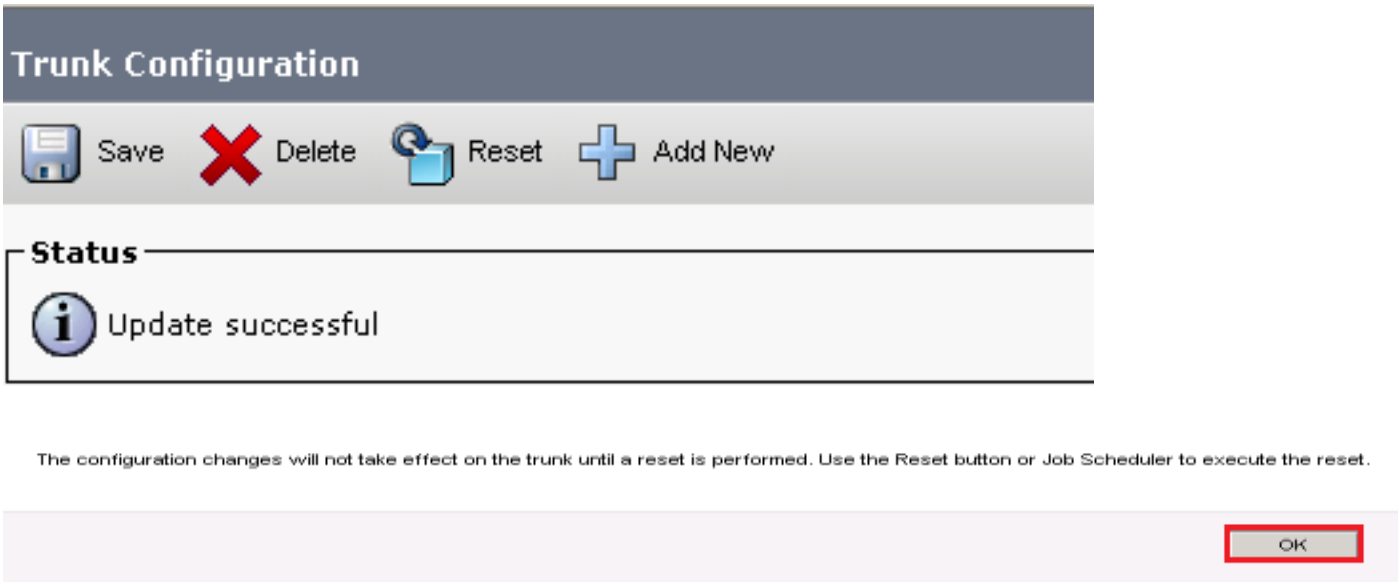
3. Clic vCUBE per aprire la pagina di configurazione del trunk vCUBE.
4. Dentro Device Information , selezionare la SRTP Allowed per abilitare SRTP.



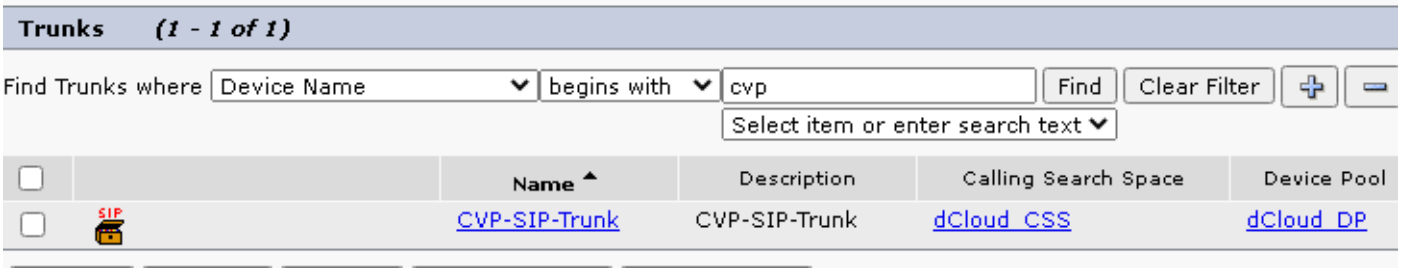
5. Scorrere fino alla SIP Information e modificare la Destination Port a 5061.
6. Cambia SIP Trunk Security Profile a SecureSIPTLSForCube.



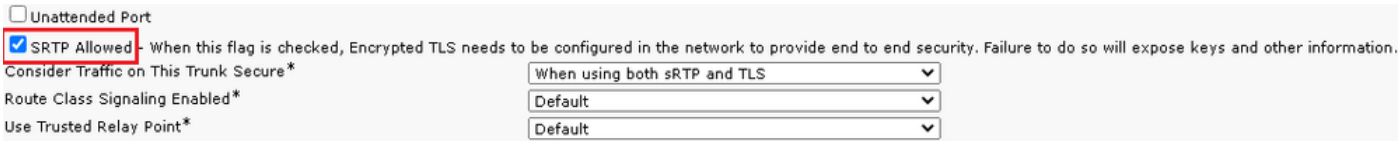
7. Clic Save quindi Rest a save e applicare le modifiche.



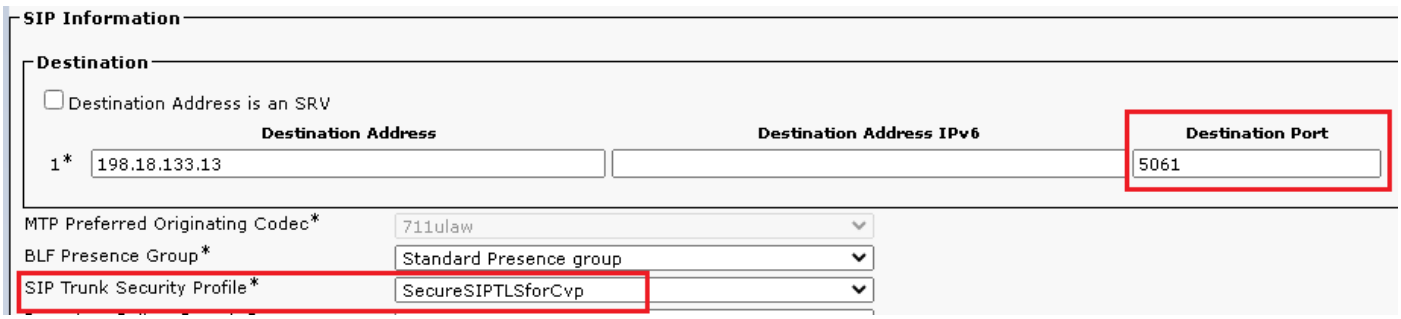
8. Passa a Device > Trunk, cercare CVP trunk, in questo esempio CVP trunk name è cvp-SIP-Trunk. Clic Find.



9. Clic CVP-SIP-Trunk per aprire la pagina di configurazione del trunk CVP.
10. Dentro Device Information sezione, controllo SRTP Allowed per abilitare SRTP.



11. Scorrere fino alla SIP Information , modificare la Destination Port a 5061.
12. Cambia SIP Trunk Security Profile a SecureSIPTLSForCvp.



13. Clic Save quindi Rest a save e applicare le modifiche.

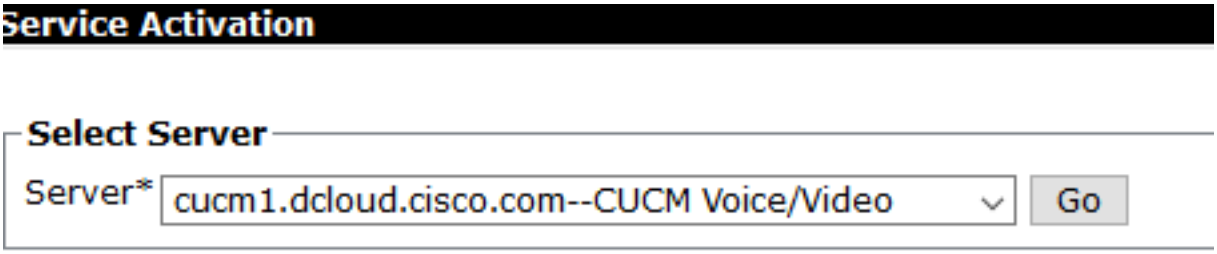
Comunicazione dei dispositivi degli agenti sicuri con CUCM

Per abilitare le funzionalità di protezione per un dispositivo, è necessario installare un certificato LSC (Locally Significant Certificate) e assegnare il profilo di protezione al dispositivo. LSC possiede la chiave pubblica per l'endpoint, firmata dalla chiave privata CAPF CUCM. Per impostazione predefinita, non è installato sui telefoni.

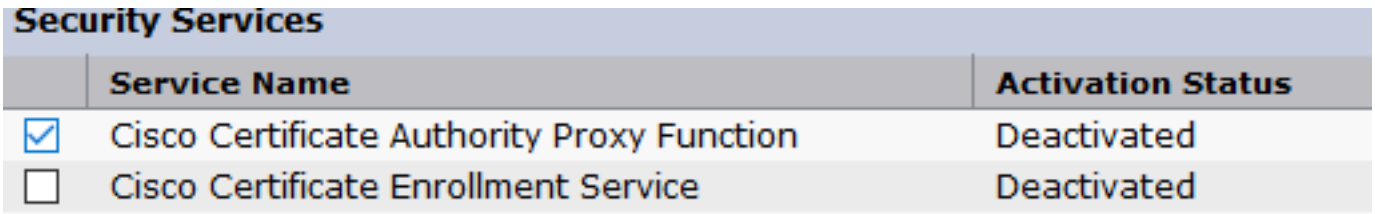
Passaggi:

1. Accedi a Cisco Unified Serviceability interfaccia.
2. Passa a Tools > Service Activation.

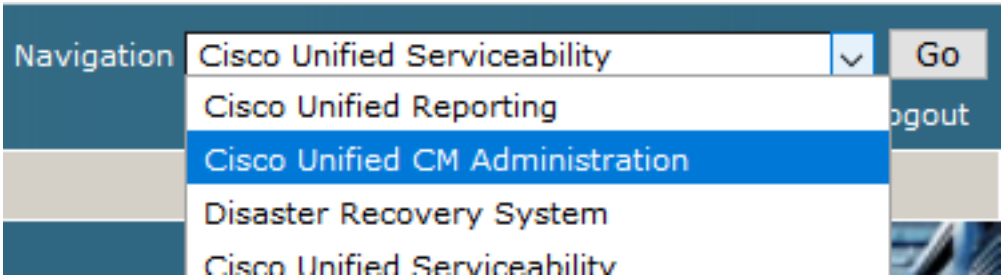
3. Scegliere il server CUCM e fare clic su Go.



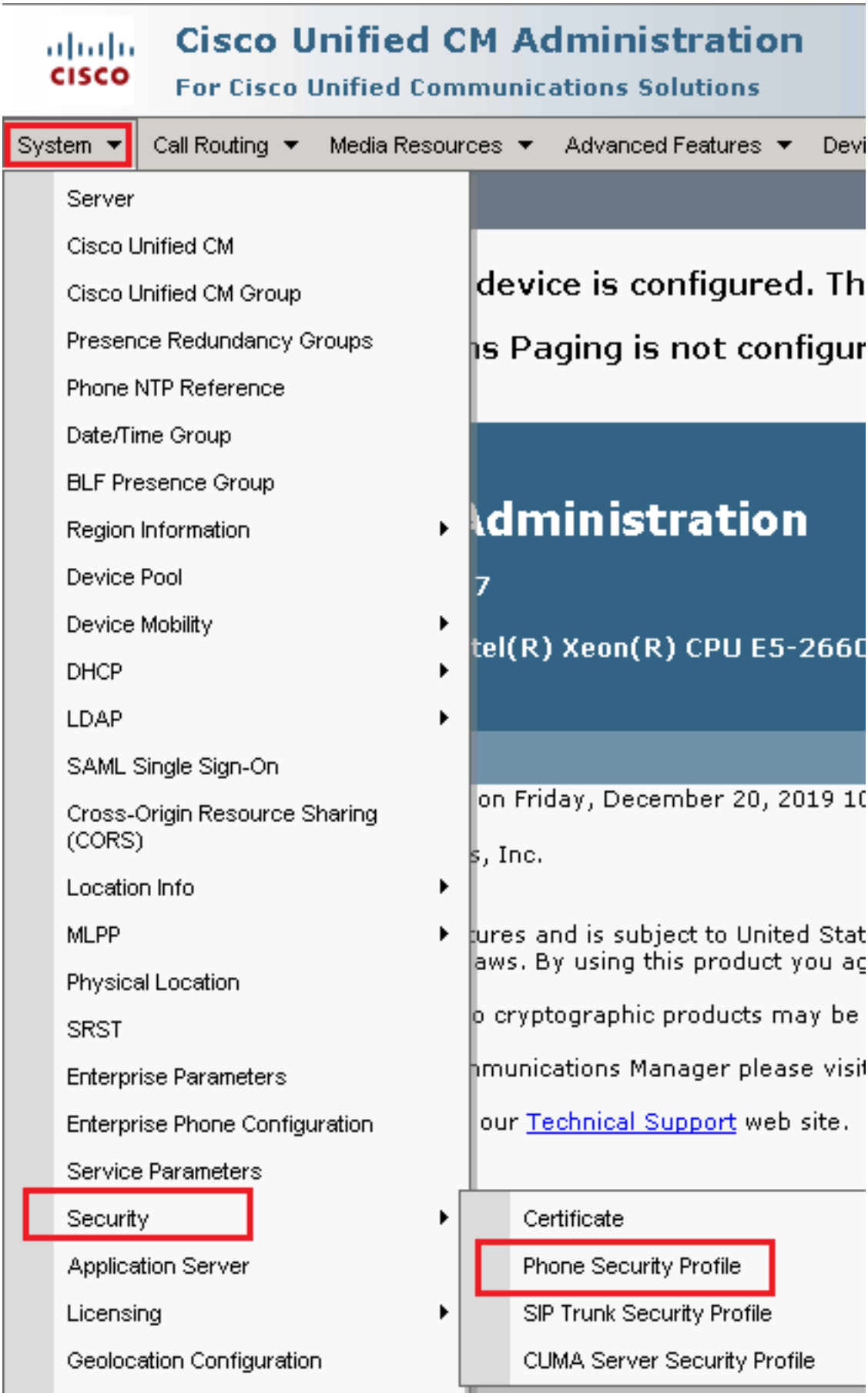
4. Assegno Cisco Certificate Authority Proxy Function e fare clic su Save per attivare il servizio. Clic Ok per confermare.



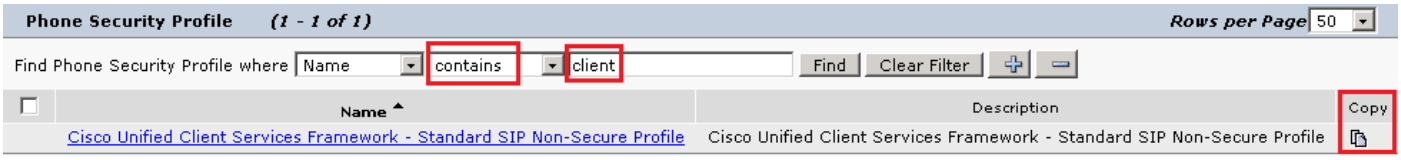
5. Assicurarsi che il servizio sia attivato, quindi passare all'amministrazione CUCM.



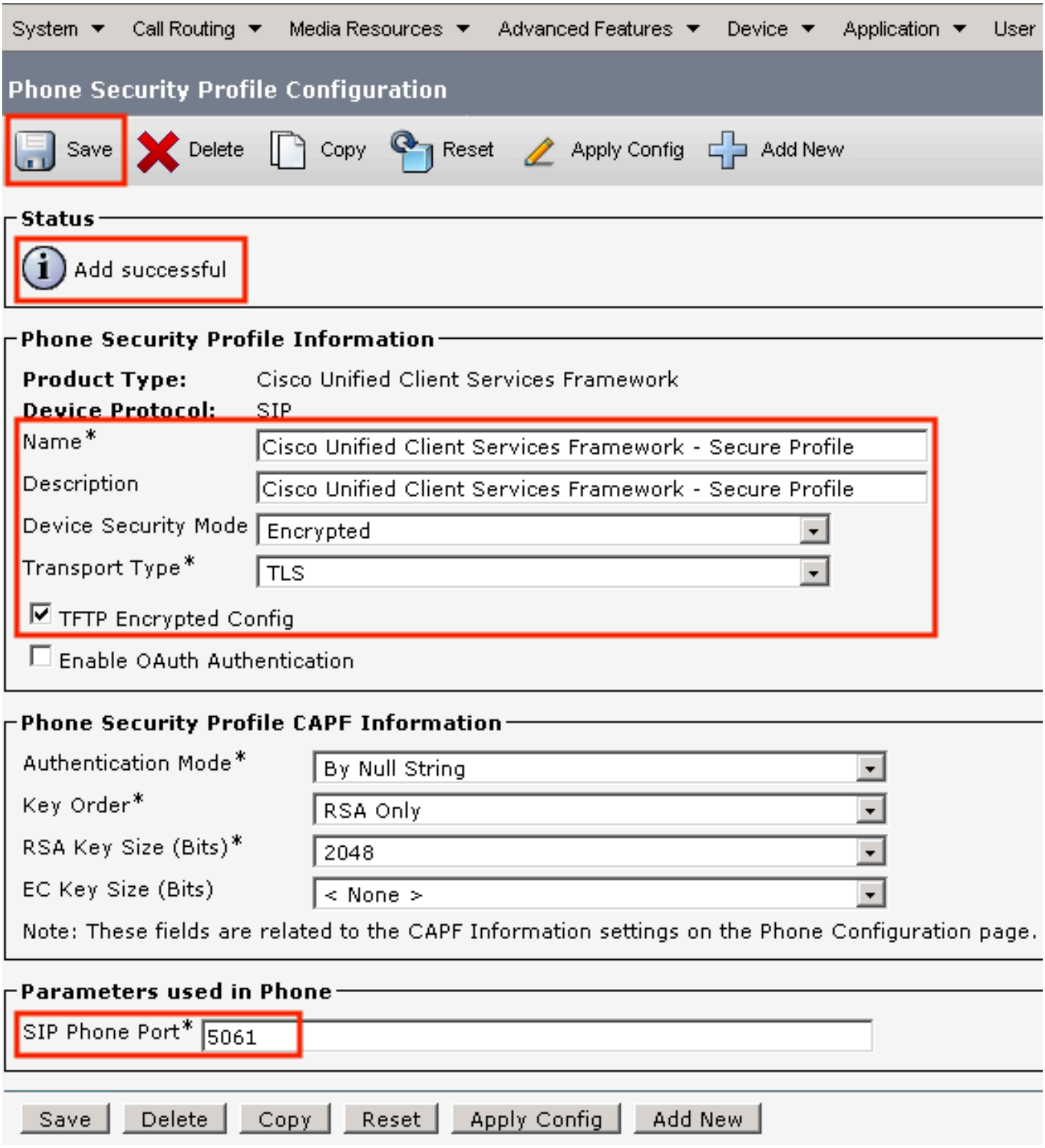
6. Dopo aver eseguito correttamente l'accesso all'amministrazione CUCM, passare a System > Security > Phone Security Profile per creare un profilo di sicurezza per il dispositivo agente.



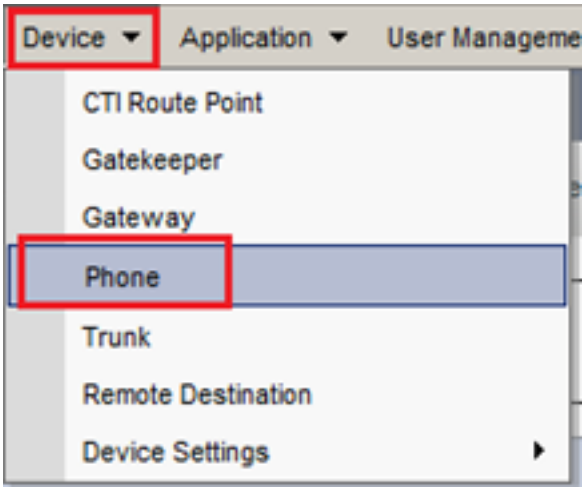
7. Individuare il profilo di sicurezza corrispondente al tipo di dispositivo dell'agente. In questo esempio, viene utilizzato un telefono fisso, quindi scegliere Cisco Unified Client Services Framework - Standard SIP Non-Secure Profile. Fare clic sull'icona Copia per copiare il profilo.



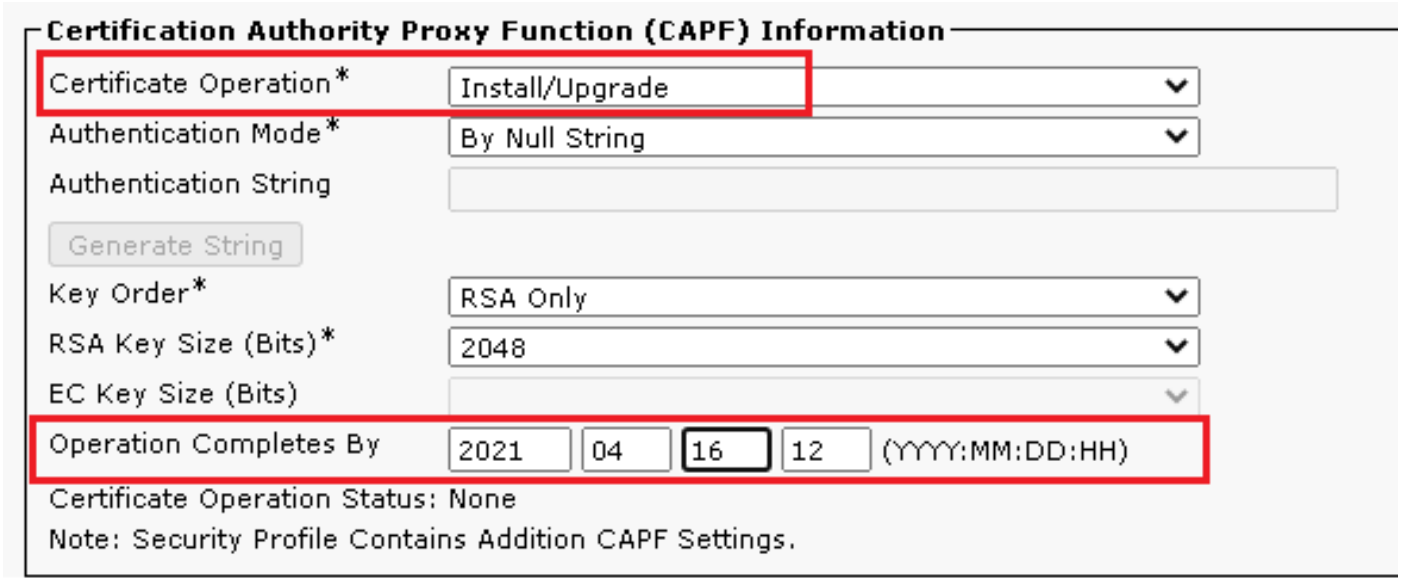
8. Rinomina il profilo in Cisco Unified Client Services Framework - Secure Profile. CModificare i parametri come in questa immagine, quindi fare clic su Save in alto a sinistra nella pagina.



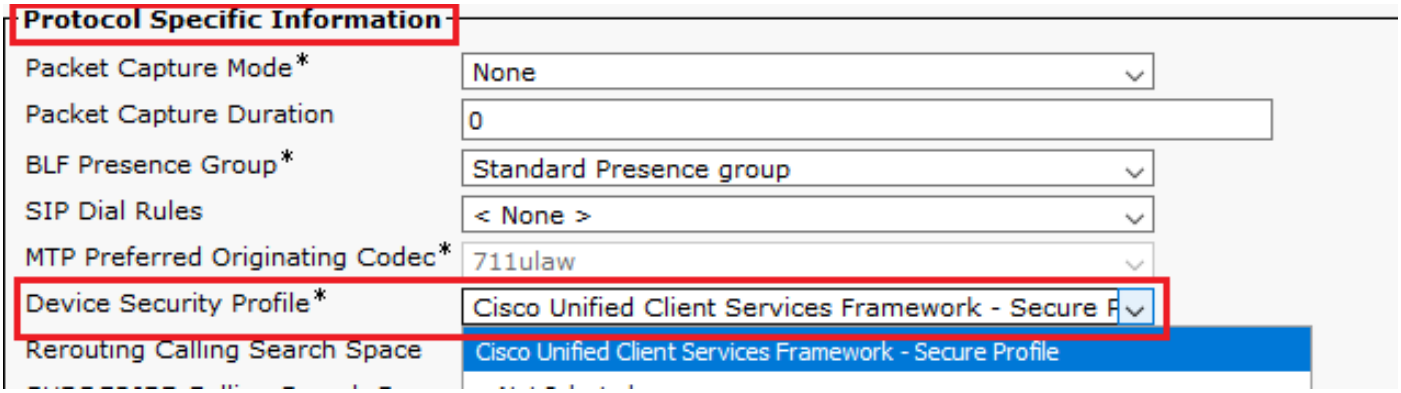
9. Dopo aver creato correttamente il profilo del dispositivo telefonico, passare a Device > Phone.



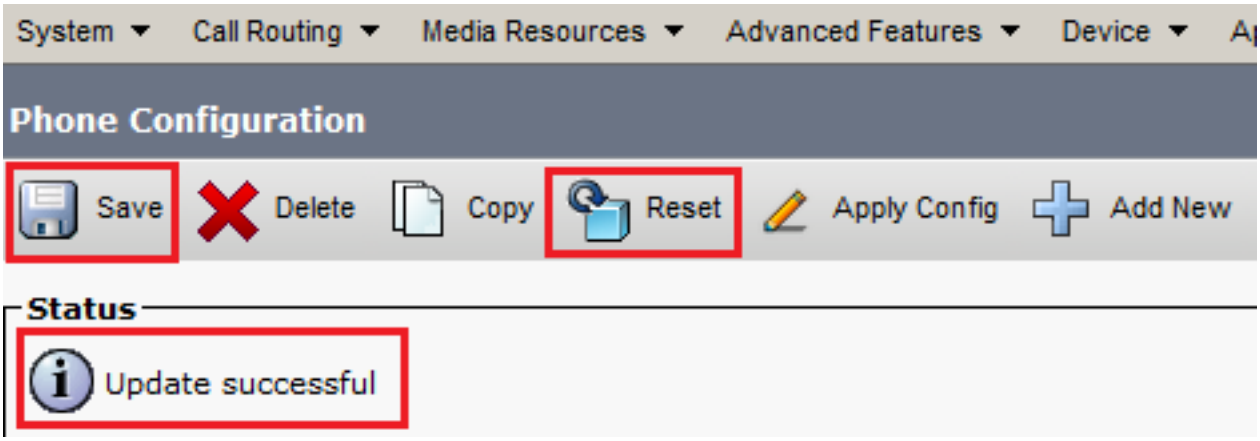
10. Clic Find per elencare tutti i telefoni disponibili, quindi fare clic su telefono agente.
11. Verrà visualizzata la pagina Configurazione telefono agente. Cerca Certification Authority Proxy Function (CAPF) Information sezione. Per installare LSC, impostare Certificate Operation a Install/Upgrade e Operation Completes by a qualsiasi data futura.



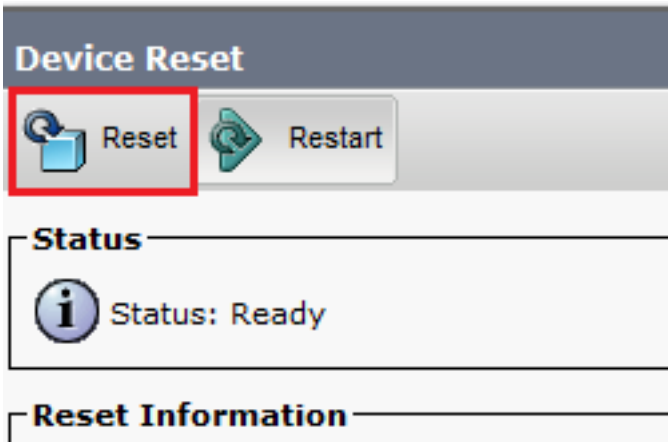
12. Cerca Protocol Specific Information e modificare la Device Security Profile a Cisco Unified Client Services Framework – Secure Profile.



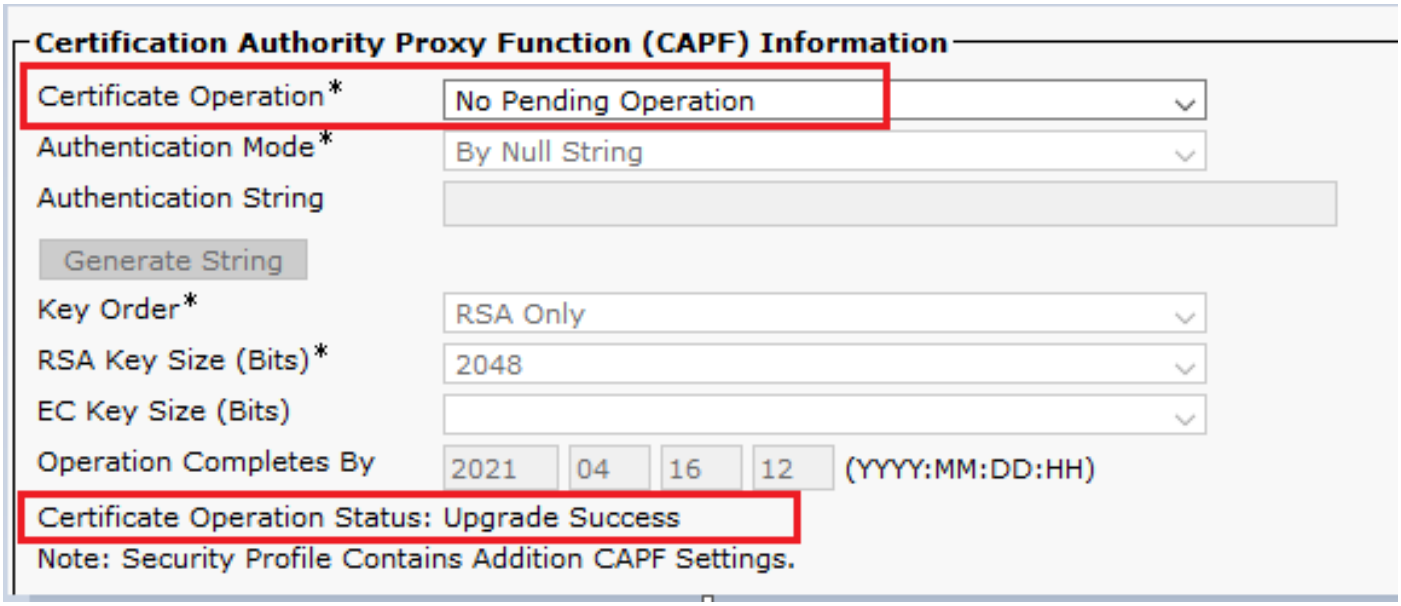
13. Clic Save in alto a sinistra nella pagina. Assicurarsi che le modifiche siano state salvate correttamente, quindi fare clic su Reset.



14. Viene visualizzata una finestra popup, fare clic su Reset per confermare l'azione.



15. Una volta che il dispositivo agente si è registrato nuovamente con CUCM, aggiornare la pagina corrente e verificare che LSC sia installato correttamente. Assegno Certification Authority Proxy Function (CAPF) Information sezione, Certificate Operation deve essere impostato su No Pending Operation e Certificate Operation Status è impostato su Upgrade Success.



16. Fare riferimento agli stessi passaggi del passaggio. 7 - 13 per proteggere i dispositivi di altri agenti che si desidera utilizzare con SIP e RTP sicuri con CUCM.

Verifica

Per verificare che il protocollo RTP sia protetto in modo appropriato, effettuare le seguenti operazioni:

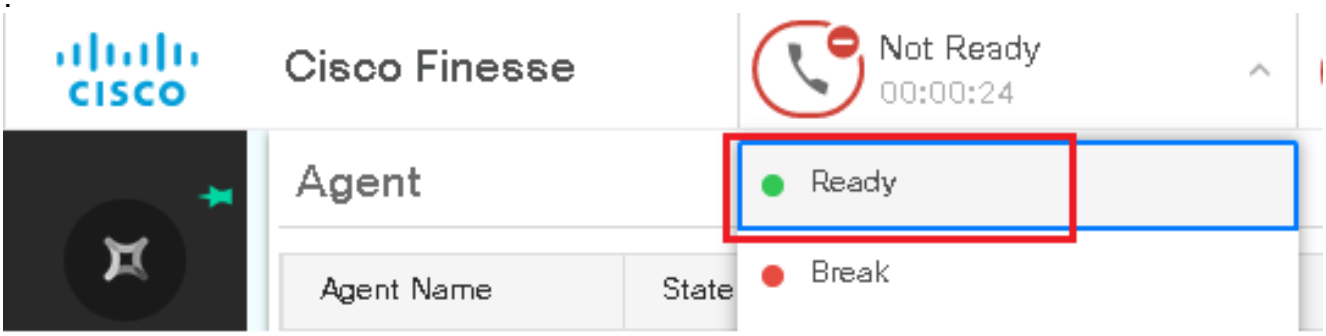
1. Effettuare una chiamata di prova al contact center e ascoltare il prompt IVR.
2. Allo stesso tempo, aprire la sessione SSH su vCUBE ed eseguire questo comando:
   show call active voice brief

```
Total call-legs: 2
1E85 : 100642 465092660ms.1 (02:55:19.809 UTC Thu Mar 25 2021) +1090 pid:6000100 Answer 3227046971 active
 dur 00:00:26 tx:0/0 rx:0/0 dscp:0 media:0 audio tos:0xB8 video tos:0x0
 IP 198.18.133.76:5062 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off Transcoded: No ICE
 media inactive detected:n media contrl rcvd:n/a timestamp:n/a
 long duration call detected:n long duration call duration:n/a timestamp:n/a
 LostPacketRate:0.00 OutOfOrderRate:0.00
 LocalUUID:4865626844c25f248e19a95a65b0ad50
 RemoteUUID:674ECD1639ED7A710000ABF910000178
 VRF:
1E85 : 100643 465093670ms.1 (02:55:20.819 UTC Thu Mar 25 2021) +70 pid:6000 Originate 6016 active
 dur 00:00:26 tx:0/0 rx:0/0 dscp:0 media:0 audio tos:0xB8 video tos:0x0
 IP 198.18.133.143:25346 SRTP: on rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off Transcoded: No IC
 media inactive detected:n media contrl rcvd:n/a timestamp:n/a
 long duration call detected:n long duration call duration:n/a timestamp:n/a
 LostPacketRate:0.00 OutOfOrderRate:0.00
 LocalUUID:674ECD1639ED7A710000ABF910000178
 RemoteUUID:4865626844c25f248e19a95a65b0ad50
 VRF:
```

Suggerimento: verificare se l'SRTP è on tra CUBE e VVB (198.18.133.143). In caso affermativo, ciò conferma che il traffico RTP tra CUBE e VB è sicuro.

3. Rendere disponibile un agente per rispondere alla chiamata.

.

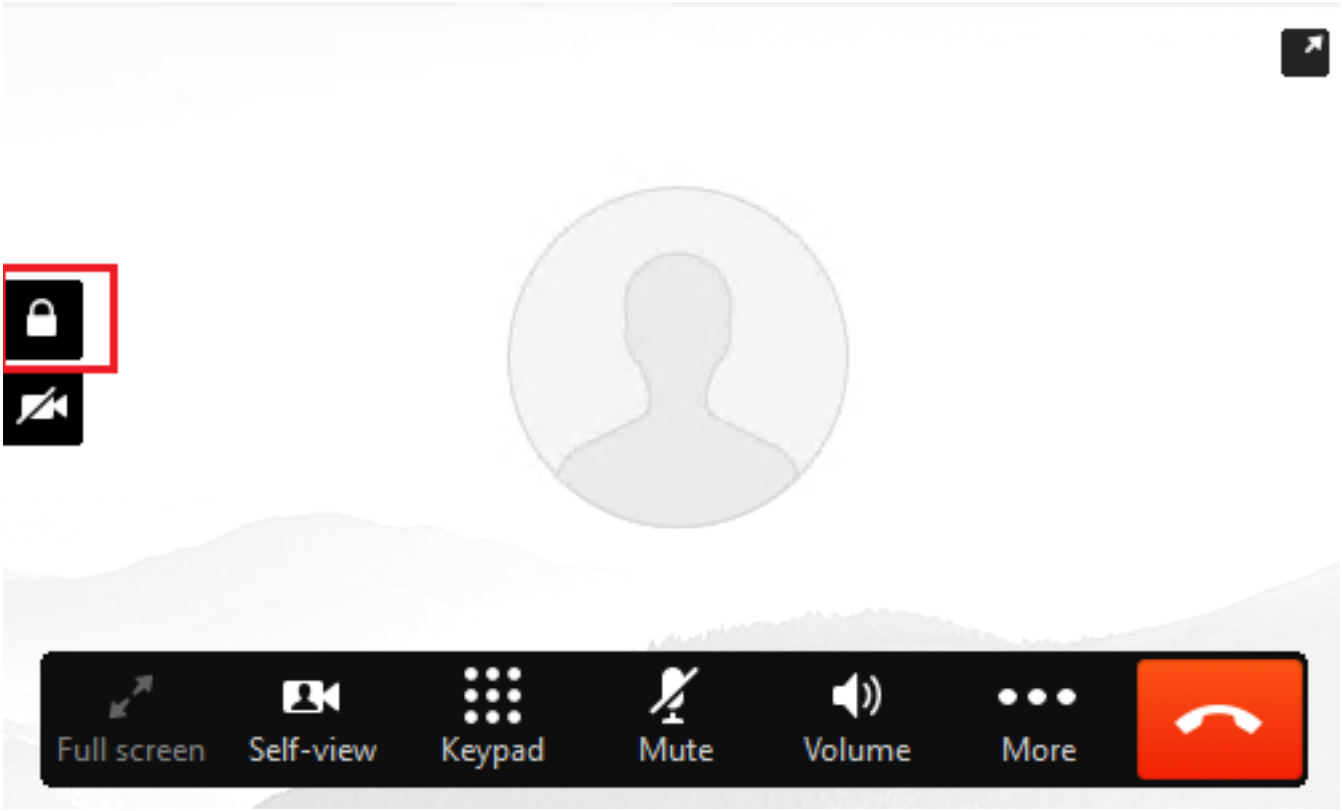


4. L'agente viene riservato e la chiamata viene instradata all'agente. Risponda alla chiamata.
5. La chiamata viene connessa all'agente. Tornare alla sessione SSH vCUBE ed eseguire questo comando:
   show call active voice brief

```
Total call-legs: 2
1E85 : 100642 465092660ms.1 (02:55:19.809 UTC Thu Mar 25 2021) +1090 pid:6000100 Answer 3227046971 connected
 dur 00:04:01 tx:0/0 rx:0/0 dscp:0 media:0 audio tos:0xB8 video tos:0x0
 IP 198.18.133.76:5062 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off Transcoded: No ICE: Off
 media inactive detected:n media contrl rcvd:n/a timestamp:n/a
 long duration call detected:n long duration call duration:n/a timestamp:n/a
 LostPacketRate:0.00 OutOfOrderRate:0.00
 LocalUUID:4865626844c25f248e19a95a65b0ad50
 RemoteUUID:00003e7000105000a000005056a06cb8
 VRF:
1E85 : 100643 465093670ms.1 (02:55:20.819 UTC Thu Mar 25 2021) +70 pid:6000 Originate 6016 connected
 dur 00:04:01 tx:0/0 rx:0/0 dscp:0 media:0 audio tos:0xB8 video tos:0x0
 IP 198.18.133.75:24648 SRTP: on rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off Transcoded: No ICE: Off
 media inactive detected:n media contrl rcvd:n/a timestamp:n/a
 long duration call detected:n long duration call duration:n/a timestamp:n/a
 LostPacketRate:0.00 OutOfOrderRate:0.00
 LocalUUID:00003e7000105000a000005056a06cb8
 RemoteUUID:4865626844c25f248e19a95a65b0ad50
 VRF:
```

Suggerimento: verificare se l'SRTP è on tra i telefoni degli agenti (198.18.133.75). In caso affermativo, viene confermato che il traffico RTP tra CUBE e l'agente è sicuro.

6. Inoltre, una volta connessa la chiamata, sul dispositivo agente viene visualizzato un blocco di sicurezza. Ciò conferma anche che il traffico RTP è sicuro.



Per verificare che i segnali SIP siano protetti correttamente, fare riferimento all'articolo Configure Secure SIP Signaling.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).