

Configurazione di Secure RTP in Contact Center Enterprise

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Task 1: configurazione protetta CUBE](#)

[Task 2: configurazione sicura di CVP](#)

[Task 3: configurazione sicura di CVB](#)

[Task 4: configurazione sicura di CUCM](#)

[Impostare la modalità di protezione CUCM sulla modalità mista](#)

[Configurare i profili di sicurezza trunk SIP per CUBE e CVP](#)

[Associazione dei profili di sicurezza trunk SIP ai rispettivi trunk SIP e abilitazione SRTP](#)

[Comunicazione dei dispositivi degli agenti sicuri con CUCM](#)

[Verifica](#)

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

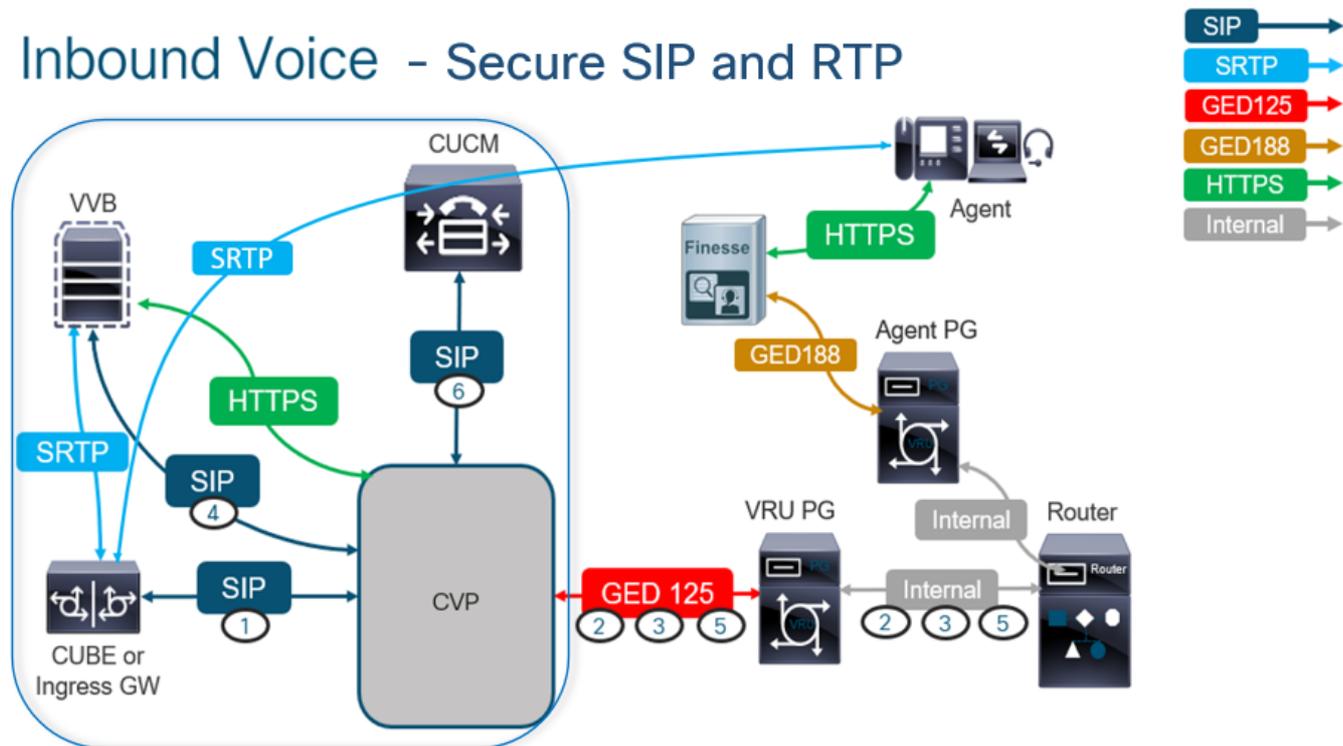
Le informazioni di questo documento si basano sulla versione 12.6 di Package Contact Center Enterprise (PCCE), CVP, CVB e CUCM, ma sono valide anche per le versioni precedenti.

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
```

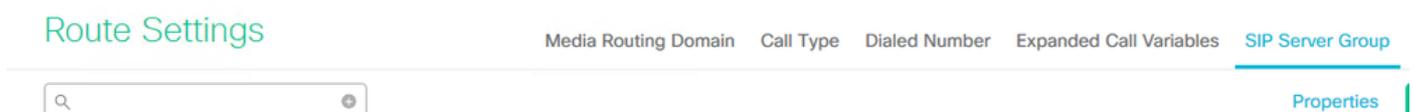
```
CC-VCUBE#
CC-VCUBE#Conf t
Enter configuration commands, one per line. End with CNTL/Z.
CC-VCUBE (config)#dial-peer voice 6000 voip
CC-VCUBE (config-dial-peer)#session target ipv4:198.18.133.13:5061
CC-VCUBE (config-dial-peer)#session transport tcp tls
CC-VCUBE (config-dial-peer)#SRTP
CC-VCUBE (config-dial-peer)#exit
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.com` quindi nella `Members` che mostra i dettagli delle configurazioni dei gruppi di server SIP. Imposta `SecurePort` a `5061` e fare clic su `Save`.

Route Settings [Media Routing Domain](#) [Call Type](#) [Dialed Number](#) [Expanded Call Variables](#) **Sip Server Groups** [Routing Pattern](#)

Edit `cucm1.dcloud.cisco.com`

General **Members**

List of Group Members +

Hostname/IP	Priority	Weight	Port	SecurePort	Site
198.18.133.3	10	10	5060	5061	Main

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

Route Settings [Media Routing Domain](#) [Call Type](#) [Dialed Number](#) [Expanded Call Variables](#) **Sip Server Groups**

Edit `vvb1.dcloud.cisco.com`

General **Members**

List of Group Members +

Hostname/IP	Priority	Weight	Port	SecurePort	Site
vvb1.dcloud.cisco.c...	10	10	5060	5061	Main

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`.



Cisco Virtualized Voice Browser Administration

For Cisco Unified Communications Solutions

System Applications Subsystems Tools Help

System Parameters

Logout

Cisco Virtualized Voice Browser Administration

System version: 12.5.1.10000-24

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

Parameter Name	Parameter Value	Suggested Value
TLS(SIP)	<input type="radio"/> Disable <input checked="" type="radio"/> Enable	Disable
Supported TLS(SIP) Versions	TLSv1.2	TLSv1.2
▶ Cipher Configuration		TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
SRTP <small>[Crypto Suite : AES_CM_128_HMAC_SHA1_32]</small>	<input type="radio"/> Disable <input checked="" type="radio"/> Enable <input type="checkbox"/> Allow RTP (Mixed mode)	Disable

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

The screenshot shows the 'System Parameters Configuration' page with an 'Update' button. A dialog box is displayed over the page, stating: 'vwb1.dcloud.cisco.com says Please restart Cisco VVB Engine for the updates to take effect.' with an 'OK' button.

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

The screenshot shows the 'Navigation' menu with the following options: Cisco VVB Administration, Cisco VVB Administration, Cisco Unified Serviceability, Cisco VVB Serviceability (highlighted), and Cisco Unified OS Administration. A 'Go' button is visible next to the first two items.

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

The screenshot shows the 'Tools' menu with the following options: Control Center - Network Services and Performance Configuration and Logging.

7. Scegli Engine e fare clic su Restart.

Control Center - Network Services

Start Stop **Restart** Refresh

Status

i Ready

Select Server

Server *

System Services	
	Service Name
<input type="radio"/>	Perfmon Counter Service
<input type="radio"/>	▼Cluster View Daemon
	▶Manager Manager
<input checked="" type="radio"/>	▼Engine
	▶Manager Manager
	▶Subsystem Manager

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

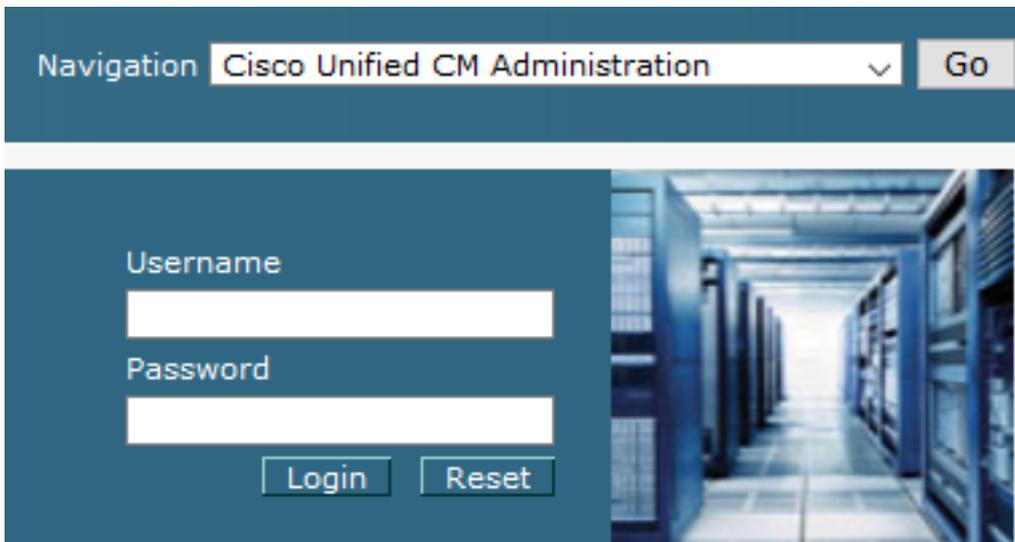
Impostare la modalità di protezione CUCM sulla modalità mista

CUCM supporta due modalità di protezione:

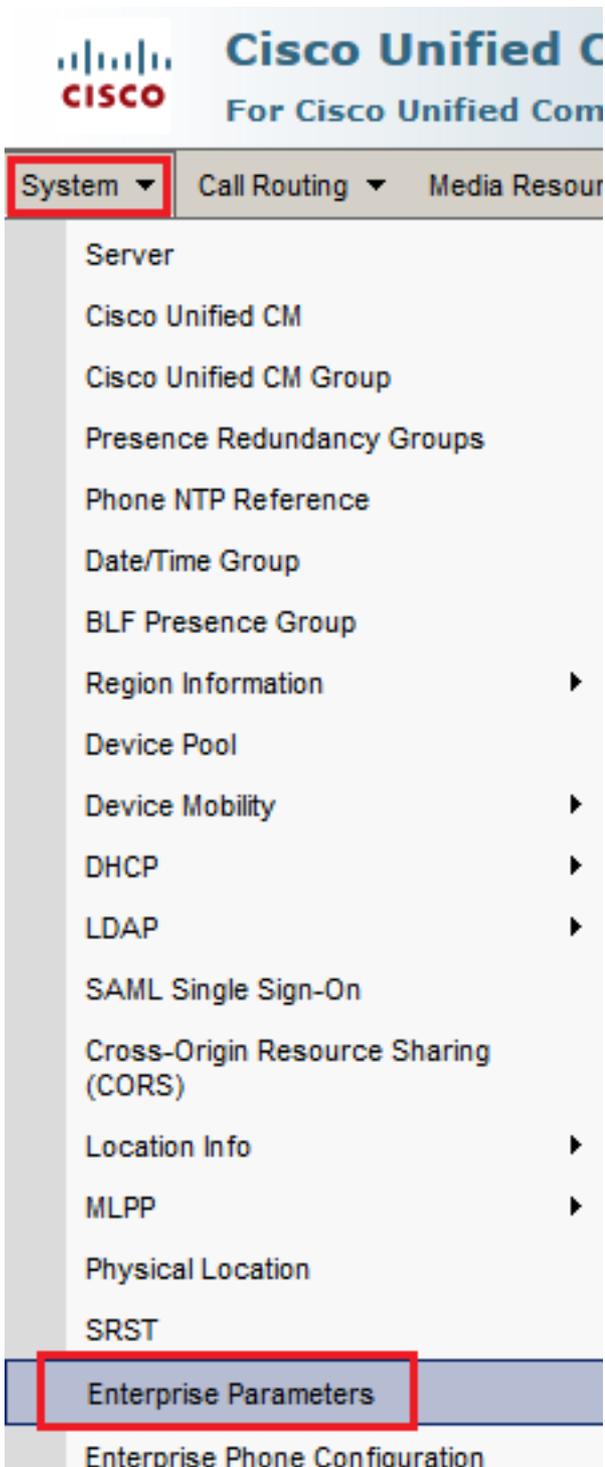
- Modalità non protetta (modalità predefinita)
- Modalità mista (modalità protetta)

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.



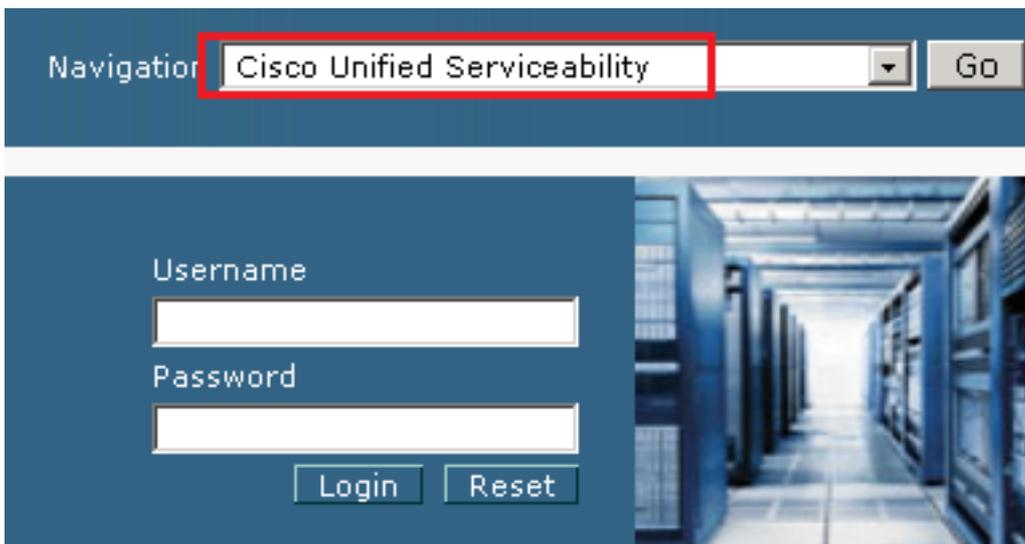
4. Se la modalità di protezione del cluster è impostata su 0, significa che la modalità di protezione del cluster è impostata su non protetta. è necessario abilitare la modalità mista dalla CLI.
5. Aprire una sessione SSH su CUCM.
6. Dopo aver eseguito correttamente l'accesso a CUCM tramite SSH, eseguire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

utils ctl set-cluster mixed-mode

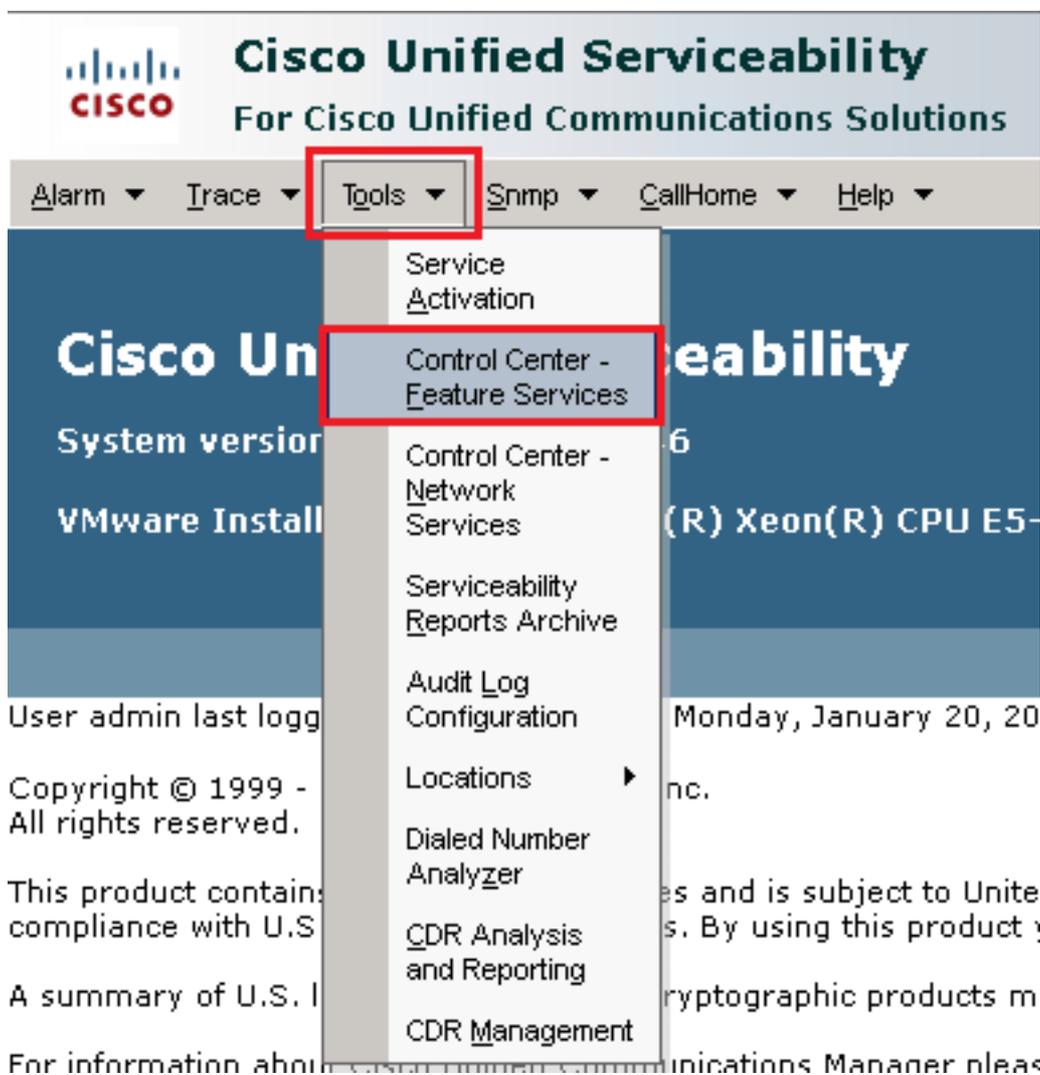
7. Tipo `y` e fare clic su `Enter` quando richiesto. Con questo comando viene impostata la modalità di protezione cluster su mista.

```
admin:utils ctl set-cluster mixed-mode
This operation will set the cluster to Mixed mode. Auto-registration is enabled on at least one CM node. Do you want to continue? (y/n): y
Moving Cluster to Mixed Mode
Cluster set to Mixed Mode
Please restart Cisco CallManager service and Cisco CTIManager services on all the nodes in the cluster that run these services.
admin:
```

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.

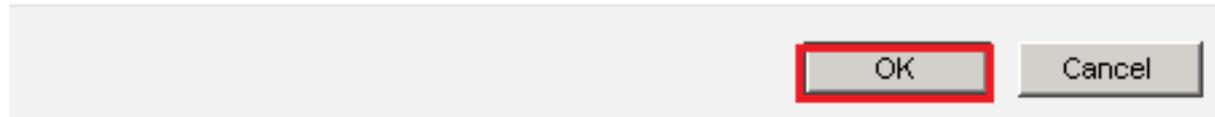


12. Sotto i servizi CM, scegliere Cisco CallManager , quindi scegliere Restart nella parte superiore della pagina.

CM Services	
	Service Name
<input checked="" type="radio"/>	Cisco CallManager
<input type="radio"/>	Cisco Unified Mobile Voice Access Service
<input type="radio"/>	Cisco IP Voice Media Streaming App
<input type="radio"/>	Cisco CTIManager
<input type="radio"/>	Cisco Extension Mobility

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

Restarting Service. It may take a while... Please wait for the page to refresh.
If you see Starting/Stopping state, refresh the page after sometime to show the right status.

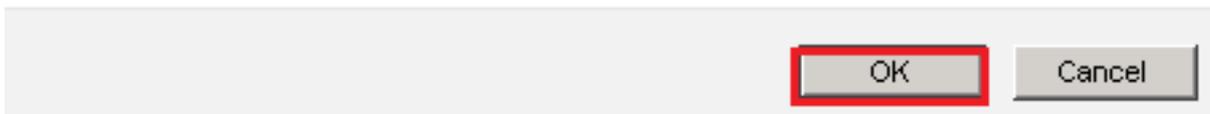


14. Dopo il riavvio di Cisco CallManager, scegliere il **Cisco CTIManager** quindi fare clic su **Restart** pulsante per il riavvio Cisco CTIManager servizio.

CM Services	
	Service Name
<input type="radio"/>	Cisco CallManager
<input type="radio"/>	Cisco Unified Mobile Voice Access Service
<input type="radio"/>	Cisco IP Voice Media Streaming App
<input checked="" type="radio"/>	Cisco CTIManager
<input type="radio"/>	Cisco Extension Mobility

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

Restarting Service. It may take a while... Please wait for the page to refresh.
If you see Starting/Stopping state, refresh the page after sometime to show the right status.



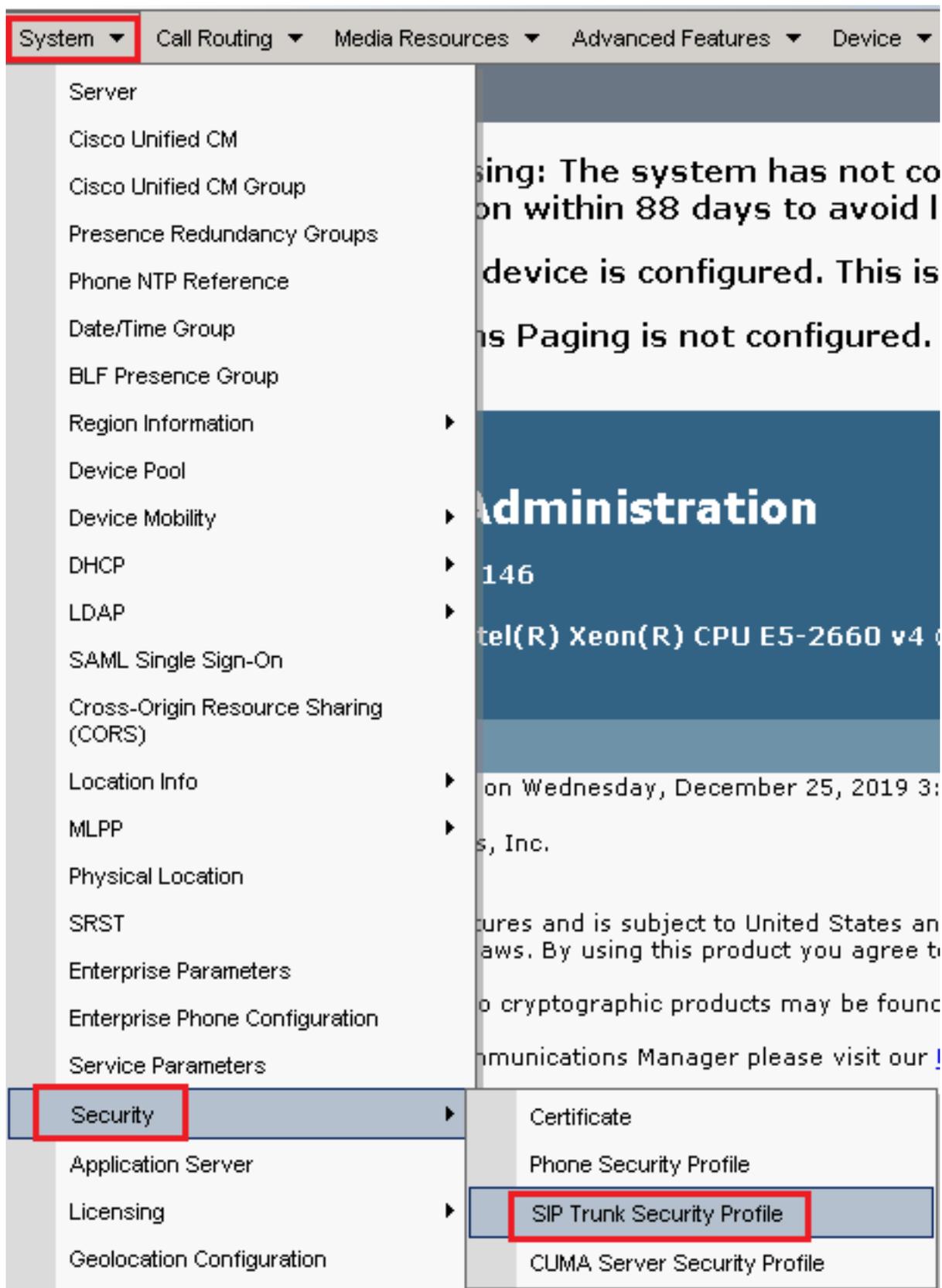
16. Dopo il riavvio corretto dei servizi, per verificare che la modalità di protezione del cluster sia impostata sulla modalità mista, passare all'amministrazione CUCM come illustrato nel passaggio 5. e quindi controllare la Cluster Security Mode. Ora deve essere impostato su 1.

Security Parameters	
Cluster Security Mode *	1
Cluster SIPOAuth Mode *	Disabled

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.

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features

Find and List SIP Trunk Security Profiles

 Add New  Select All  Clear All  Delete Selected

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

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk A

SIP Trunk Security Profile Configuration

Related Links: [Back](#)

 Save  Delete  Copy  Reset  Apply Config  Add New

- Status -

-  Add successful
-  Reset of the trunk is required to have changes take effect.

- SIP Trunk Security Profile Information -

Name*	SecureSIPTLSforCube
Description	
Device Security Mode	Encrypted ▾
Incoming Transport Type*	TLS ▾
Outgoing Transport Type	TLS ▾
<input type="checkbox"/> Enable Digest Authentication	
Nonce Validity Time (mins)*	600
Secure Certificate Subject or Subject Alternate Name	SIP-GW
Incoming Port*	5061

Enable Application level authorization
 Accept presence subscription
 Accept out-of-dialog refer**
 Accept unsolicited notification
 Accept replaces header
 Transmit security status
 Allow charging header

SIP V.150 Outbound SDP Offer Filtering* Use Default Filter ▾

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.

Status

- Add successful
- Reset of the trunk is required to have changes take effect.

SIP Trunk Security Profile Information

Name* SecureSIPTLSforCvp

Description

Device Security Mode Encrypted

Incoming Transport Type* TLS

Outgoing Transport Type TLS

Enable Digest Authentication

Nonce Validity Time (mins)* 600

Secure Certificate Subject or Subject Alternate Name cvp1.dcloud.cisco.com

Incoming Port* 5061

Enable Application level authorization

Accept presence subscription

Accept out-of-dialog refer**

Accept unsolicited notification

Accept replaces header

Transmit security status

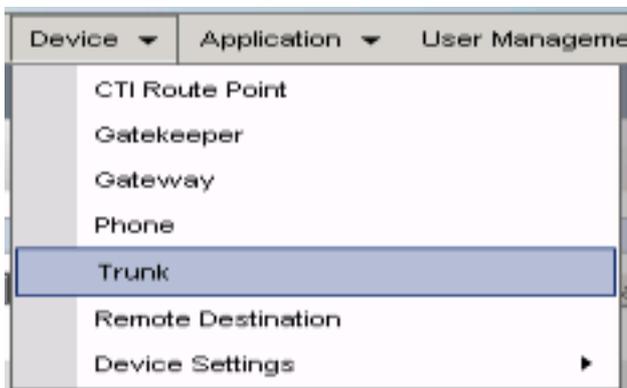
Allow charging header

SIP V.150 Outbound SDP Offer Filtering* Use Default Filter

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.

Trunks (1 - 5 of 5)						
Find Trunks where Device Name begins with vCube						
	Name	Description	Calling Search Space	Device Pool	Route Pattern	Partition
<input type="checkbox"/>	vCUBE	dCloud_CSS	dCloud_CSS	dCloud_DP	cloudcherry.sip.twilio.com	dCloud_PT
<input type="checkbox"/>	vCUBE	dCloud_CSS	dCloud_CSS	dCloud_DP	7800	PSTN_Incoming_Numbers
<input type="checkbox"/>	vCUBE	dCloud_CSS	dCloud_CSS	dCloud_DP	6016	PSTN_Incoming_Numbers
<input type="checkbox"/>	vCUBE	dCloud_CSS	dCloud_CSS	dCloud_DP	7019	PSTN_Incoming_Numbers
<input type="checkbox"/>	vCUBE	dCloud_CSS	dCloud_CSS	dCloud_DP	44413XX	Robot Agent Remote Destinations

3. Clic vCUBE per aprire la pagina di configurazione del trunk vCUBE.

4. Dentro Device Information , selezionare la SRTP Allowed per abilitare SRTP.

Unattended Port
 SRTP Allowed - When this flag is checked, Encrypted TLS needs to be configured in the network to provide end to end security. Failure to do so will expose keys and other information.
Consider Traffic on This Trunk Secure*
Route Class Signaling Enabled*
Use Trusted Relay Point*

When using both sRTP and TLS
Default
Default

5. Scorrere fino alla SIP Information e modificare la Destination Port a 5061.

6. Cambia SIP Trunk Security Profile a SecureSIPTLSForCube.

SIP Information

Destination

Destination Address is an SRV

1* Destination Address: 198.18.133.226 Destination Address IPv6: Destination Port: 5061

MTP Preferred Originating Codec*: 711ulaw
BLF Presence Group*: Standard Presence group
SIP Trunk Security Profile*: SecureSIPTLSforCube
Rerouting Calling Search Space: < None >

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

Trunk Configuration

 Save  Delete  Reset  Add New

Status

 Update successful

The configuration changes will not take effect on the trunk until a reset is performed. Use the Reset button or Job Scheduler to execute the reset.

OK

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

Trunks (1 - 1 of 1)				
Find Trunks where				
	Device Name	begins with	cvp	Find
	Clear Filter  			
	Select item or enter search text			
<input type="checkbox"/>	Name ^	Description	Calling Search Space	Device Pool
<input type="checkbox"/>	 CVP-SIP-Trunk	CVP-SIP-Trunk	dCloud_CSS	dCloud_DP

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

Unattended Port

SRTP Allowed - When this flag is checked, Encrypted TLS needs to be configured in the network to provide end to end security. Failure to do so will expose keys and other information. Consider Traffic on This Trunk Secure*

Route Class Signaling Enabled*

Use Trusted Relay Point*

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

SIP Information

Destination

Destination Address is an SRV

Destination Address	Destination Address IPv6	Destination Port
1* 198.18.133.13		5061

MTP Preferred Originating Codec*

BLF Presence Group*

SIP Trunk Security Profile*

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

The configuration changes will not take effect on the trunk until a reset is performed. Use the Reset button or Job Scheduler to execute the reset.

OK

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.

Service Activation

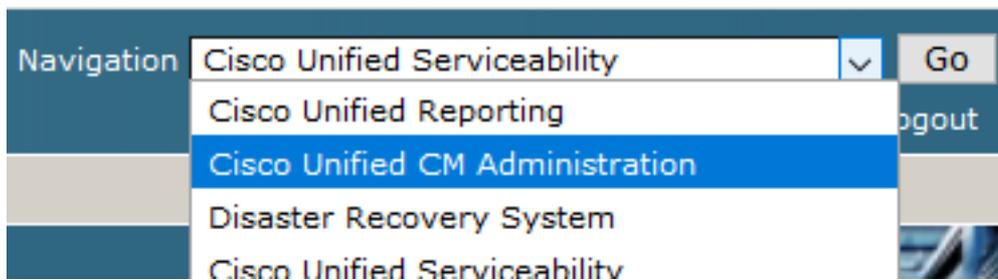
Select Server

Server*

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

Security Services		
	Service Name	Activation Status
<input checked="" type="checkbox"/>	Cisco Certificate Authority Proxy Function	Deactivated
<input type="checkbox"/>	Cisco Certificate Enrollment Service	Deactivated

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.



System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Devi

- Server
 - Cisco Unified CM
 - Cisco Unified CM Group
 - Presence Redundancy Groups
 - Phone NTP Reference
 - Date/Time Group
 - BLF Presence Group
 - Region Information ▶
 - Device Pool
 - Device Mobility ▶
 - DHCP ▶
 - LDAP ▶
 - SAML Single Sign-On
 - Cross-Origin Resource Sharing (CORS)
 - Location Info ▶
 - MLPP ▶
 - Physical Location
 - SRST
 - Enterprise Parameters
 - Enterprise Phone Configuration
 - Service Parameters
 - Security** ▶
 - Certificate
 - Phone Security Profile**
 - SIP Trunk Security Profile
 - CUMA Server Security Profile
 - Application Server
 - Licensing ▶
 - Geolocation Configuration

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.

Phone Security Profile (1 - 1 of 1) Rows per Page 50

Find Phone Security Profile where Name contains client Find Clear Filter + -

Name	Description	Copy
Cisco Unified Client Services Framework - Standard SIP Non-Secure Profile	Cisco Unified Client Services Framework - Standard SIP Non-Secure Profile	

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.

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User

Phone Security Profile Configuration

Save Delete Copy Reset Apply Config Add New

Status

Add successful

Phone Security Profile Information

Product Type: Cisco Unified Client Services Framework
Device Protocol: SIP

Name*
Description
Device Security Mode
Transport Type*
 TFTP Encrypted Config
 Enable OAuth Authentication

Phone Security Profile CAPF Information

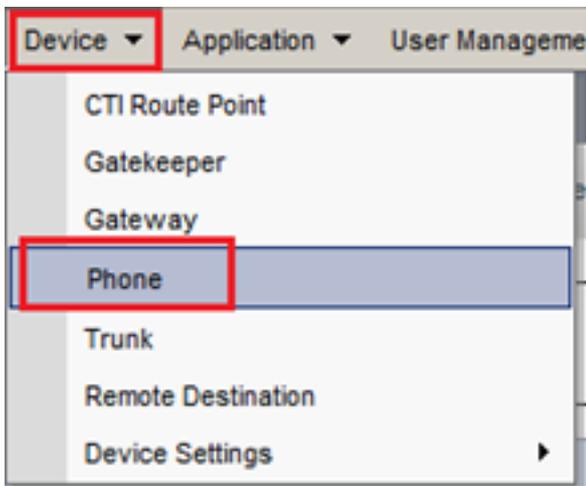
Authentication Mode*
Key Order*
RSA Key Size (Bits)*
EC Key Size (Bits)
Note: These fields are related to the CAPF Information settings on the Phone Configuration page.

Parameters used in Phone

SIP Phone Port*

Save Delete Copy Reset Apply Config Add New

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.

A screenshot of the 'Certification Authority Proxy Function (CAPF) Information' configuration page. The page contains several fields: 'Certificate Operation*' (dropdown menu set to 'Install/Upgrade'), 'Authentication Mode*' (dropdown menu set to 'By Null String'), 'Authentication String' (text input field), 'Generate String' (button), 'Key Order*' (dropdown menu set to 'RSA Only'), 'RSA Key Size (Bits)*' (dropdown menu set to '2048'), 'EC Key Size (Bits)' (dropdown menu), and 'Operation Completes By' (date and time picker set to 2021, 04, 16, 12). A red box highlights the 'Certificate Operation*' dropdown and the 'Operation Completes By' date/time fields. Below the fields, it says 'Certificate Operation Status: None' and 'Note: Security Profile Contains Addition CAPF Settings.'

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

A screenshot of the 'Protocol Specific Information' configuration page. The page contains several fields: 'Packet Capture Mode*' (dropdown menu set to 'None'), 'Packet Capture Duration' (text input field set to '0'), 'BLF Presence Group*' (dropdown menu set to 'Standard Presence group'), 'SIP Dial Rules' (dropdown menu set to '< None >'), 'MTP Preferred Originating Codec*' (dropdown menu set to '711ulaw'), 'Device Security Profile*' (dropdown menu set to 'Cisco Unified Client Services Framework - Secure F'), and 'Rerouting Calling Search Space' (dropdown menu set to 'Cisco Unified Client Services Framework - Secure Profile'). A red box highlights the 'Device Security Profile*' dropdown menu.

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

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ A

Phone Configuration

 Save
  Delete
  Copy
  Reset
  Apply Config
  Add New

Status

 Update successful

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

Device Reset

 Reset
  Restart

Status

 Status: Ready

Reset Information

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**.

Certification Authority Proxy Function (CAPF) Information

Certificate Operation* No Pending Operation ▾
Authentication Mode* ▾ By Null String ▾
 Authentication String

Key Order* ▾ RSA Only ▾
RSA Key Size (Bits)* ▾ 2048 ▾
 EC Key Size (Bits) ▾
 Operation Completes By (YYYY:MM:DD:HH)
Certificate Operation Status: Upgrade Success
 Note: Security Profile Contains Addition CAPF Settings.

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

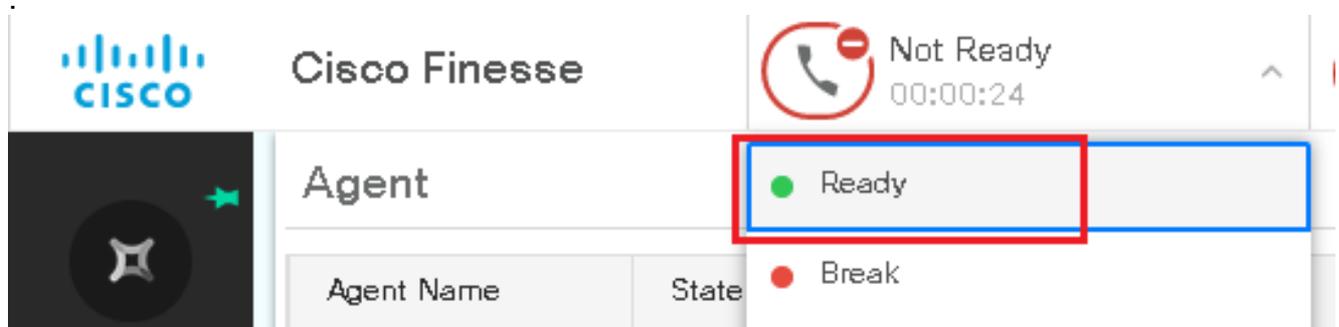
Per verificare che il protocollo RTP sia protetto in modo appropriato, effettuare le seguenti operazioni:

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
lE85 : 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 g7llulaw 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:
lE85 : 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 g7llulaw 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: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.

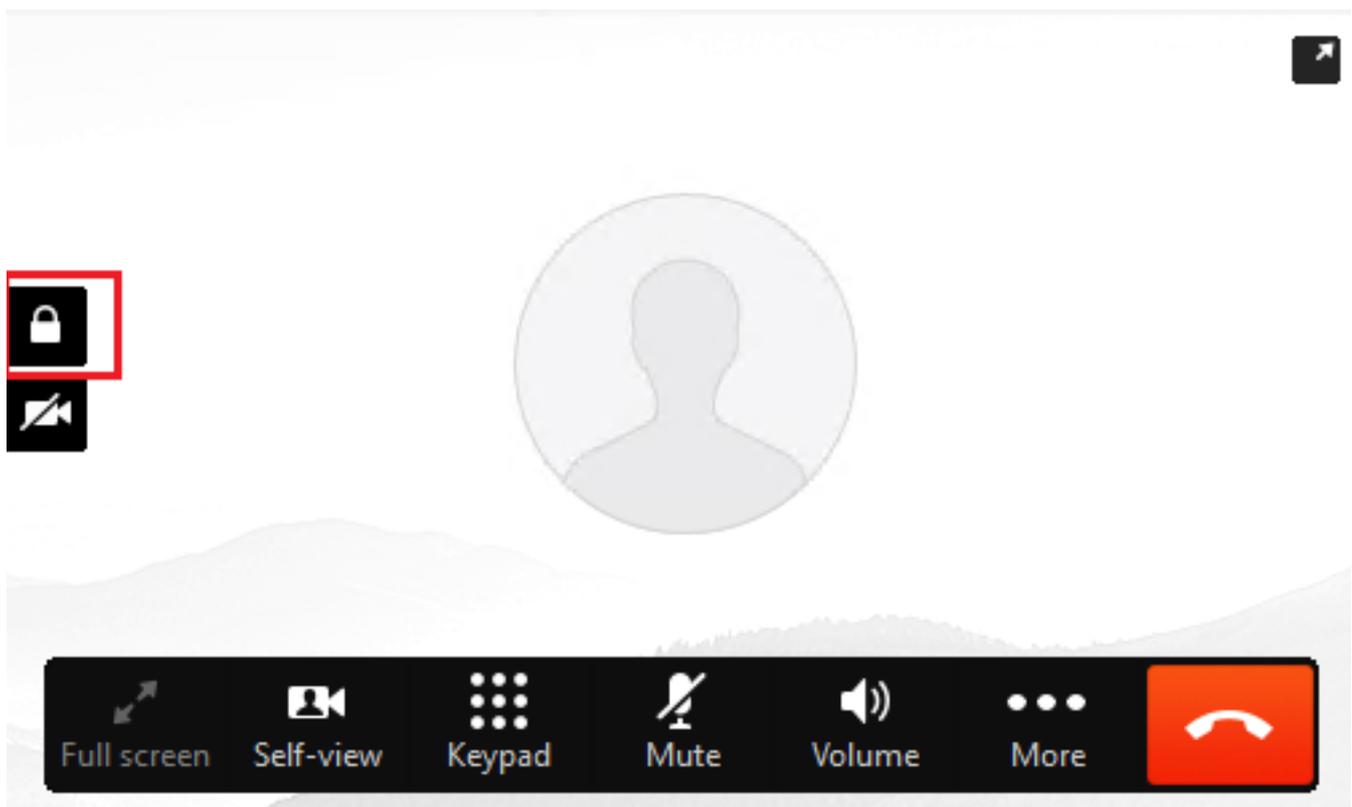


4. L'agente viene riservato e la chiamata viene instradata all'agente. Risponda alla chiamata.
5. La chiamata viene connessa all'agente. Tornare alla sessione SSH vCUBE ed eseguire questo comando:
show call active voice brief

```
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).