

# Configurazione della segnalazione SIP protetta in Contact Center Enterprise

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Attività 1. Configurazione protetta CUBE](#)

[Attività 2. Configurazione sicura CVP](#)

[Attività 3. Configurazione sicura CVB](#)

[Attività 4. Configurazione sicura CUCM](#)

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

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

[Associa profili di sicurezza trunk SIP ai rispettivi trunk SIP](#)

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

[Verifica](#)

[Risoluzione dei problemi](#)

## Introduzione

In questo documento viene descritto come proteggere la segnalazione SIP (Session Initiation Protocol) nel flusso di chiamate completo 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), server di chiamata Customer Voice Portal (CVP), 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

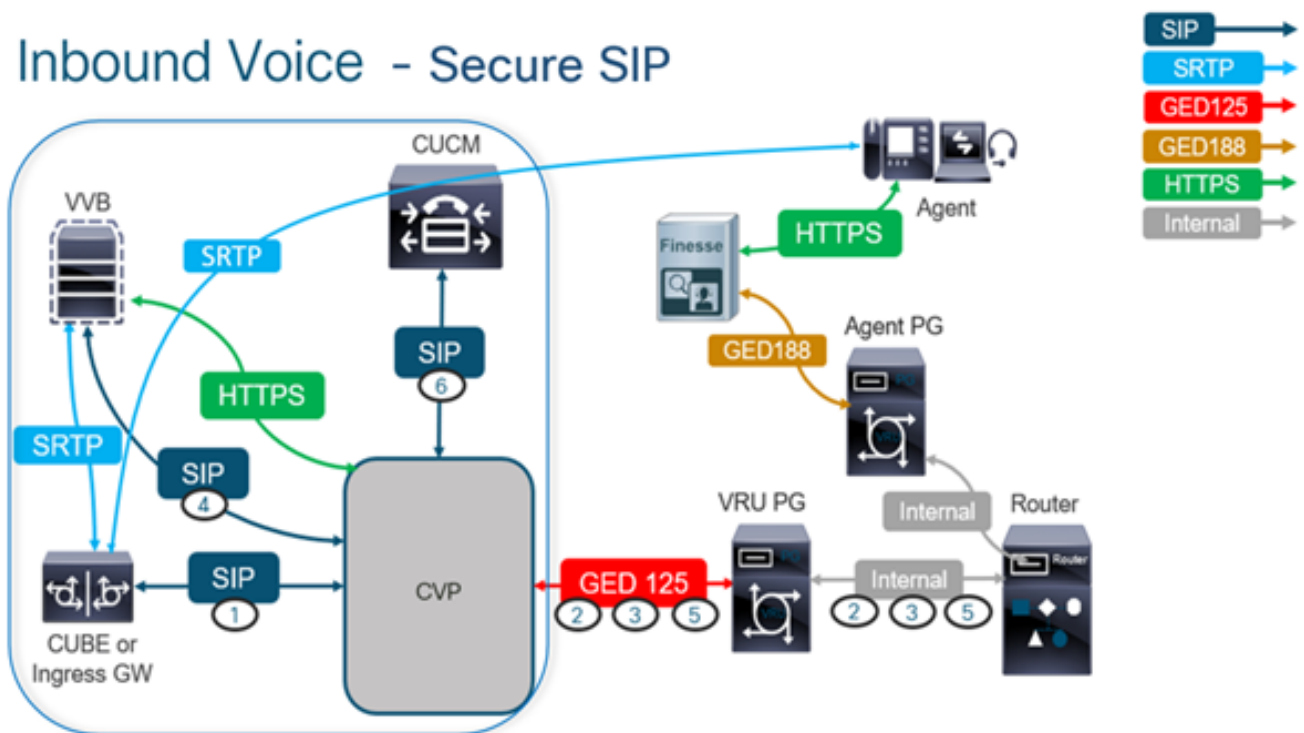
## Componenti usati

Le informazioni fornite in 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

Il diagramma successivo mostra i componenti coinvolti nella segnalazione SIP nel flusso chiamate completo del contact center. Quando una chiamata vocale arriva al sistema, prima viene tramite il gateway in entrata o CUBE, quindi avviare configurazioni SIP sicure su CUBE. Quindi, configurare CVP, CVB e CUCM.



### Attività 1. Configurazione protetta CUBE

In questa attività configurare CUBE per proteggere i messaggi del protocollo SIP.

Configurazioni richieste:

- Configurare un trust point predefinito per l'agente utente SIP
- Modificare i peer di composizione in modo che utilizzino TLS (Transport Layer Security)

Passaggi:

1. Aprire la sessione SSH (Secure Shell) in CUBE.
2. Eseguire questi comandi per fare in modo che lo stack SIP utilizzi il certificato CA

(Certification Authority) del CUBE. CUBE stabilisce una 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 utilizzato 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 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)#
CC-VCUBE(config-dial-peer)#exit
CC-VCUBE(config)#
```

## Attività 2. Configurazione sicura 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**.

### Route Settings

Media Routing Domain Call Type Dialed Number Expanded Call Variables **SIP Server Group**

Properties

In base alle configurazioni configurate, sono presenti gruppi di server SIP configurati 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** e quindi nella **Members** che mostra i dettagli della configurazione del gruppo di server SIP. Imposta **SecurePort** a 5061 e fare clic su **Save**.

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** scheda. Imposta SecurePort su 5061 e fare clic SU Save.

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

### Attività 3. Configurazione sicura CVB

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

Passaggi:

1. Accedi a **Cisco VVB Administration** 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 come TLSv1.2.

Security Parameters		
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 [Crypto Suite : AES_CM_128_HMAC_SHA1_32]	<input checked="" type="radio"/> Disable <input type="radio"/> Enable <input type="checkbox"/> Allow RTP (Mixed mode)	Disable

4. Fare clic su **Aggiorna**. Clic ok quando viene richiesto di riavviare il motore CVB.

The screenshot shows the Cisco Virtualized Voice Administration interface. A notification dialog box is displayed over the configuration page, stating: "vwb1.dcloud.cisco.com says Please restart Cisco VVB Engine for the updates to take effect." The dialog has an "OK" button. Below the dialog, the "System Parameters Configuration" page is visible, with an "Update" button highlighted.

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

The screenshot shows the navigation menu of the Cisco VVB Administration interface. The "Cisco VVB Administration" dropdown menu is open, showing the following options: "Cisco VVB Administration", "Cisco Unified Serviceability", "Cisco VVB Serviceability" (highlighted in blue), and "Cisco Unified OS Administration". A "Go" button is visible to the right of the menu.

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

The screenshot shows the "Tools" menu in the Cisco VVB Administration interface. The "Tools" menu is open, showing the following options: "Control Center - Network Services" (highlighted in blue) 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 \* vrb1

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

### Attività 4. Configurazione sicura CUCM

Per proteggere i messaggi SIP su CUCM, effettuare le seguenti configurazioni:

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

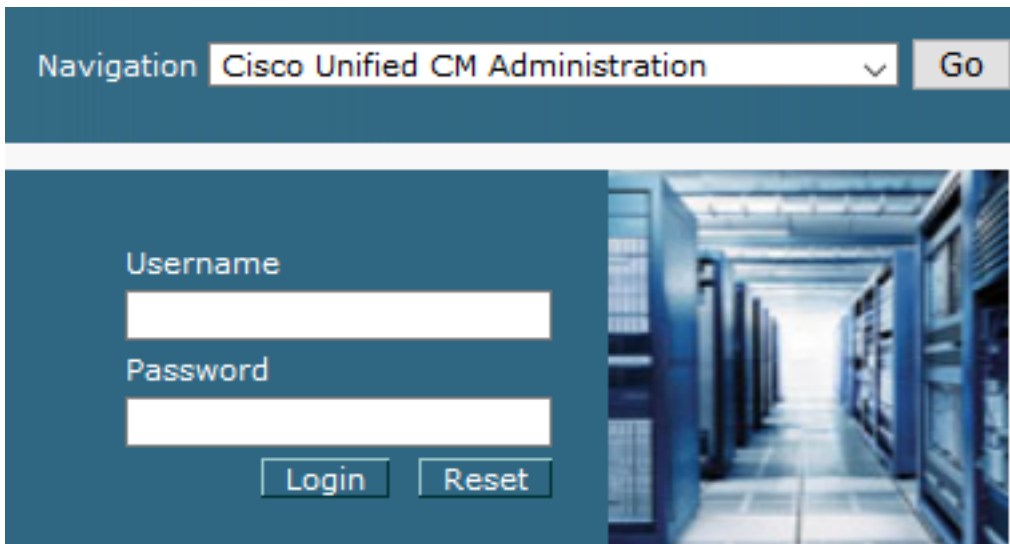
#### Impostare la modalità di protezione CUCM sulla modalità mista

CUCM supporta due modalità di protezione:

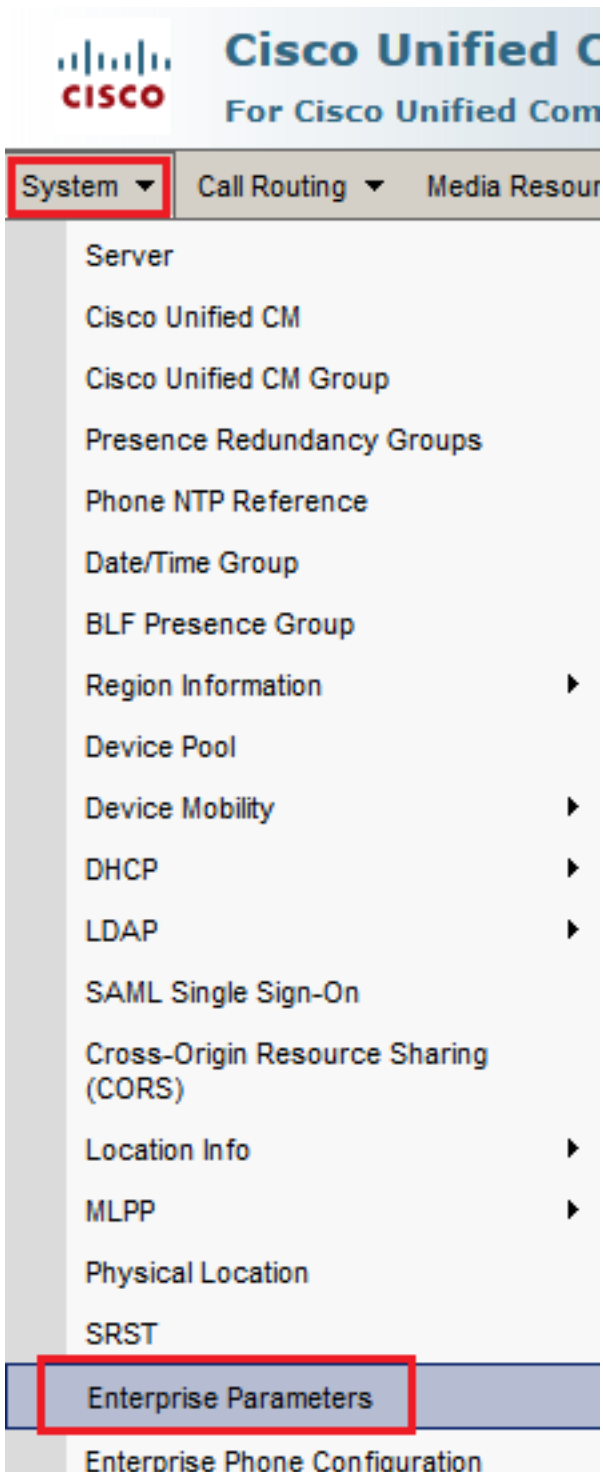
- Modalità non protetta (modalità predefinita)
- Modalità mista (modalità protetta)

Passaggi:

1. Per impostare la modalità di protezione su Modalità mista, accedere a [Cisco Unified CM Administration](#) interfaccia.



2. Dopo aver eseguito correttamente l'accesso a CUCM, passare a [System > Enterprise Parameters](#).



3. Al di sotto del Security Parameters Sezione, controlla se 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 il login a CUCM tramite SSH, eseguire questo



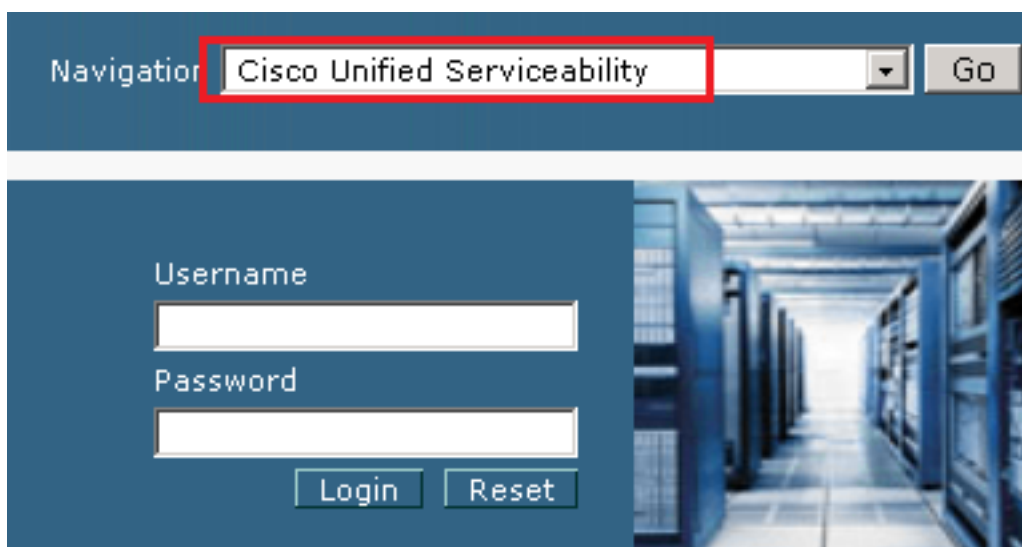
comando: `utils ctl set-cluster mixed-mode`

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

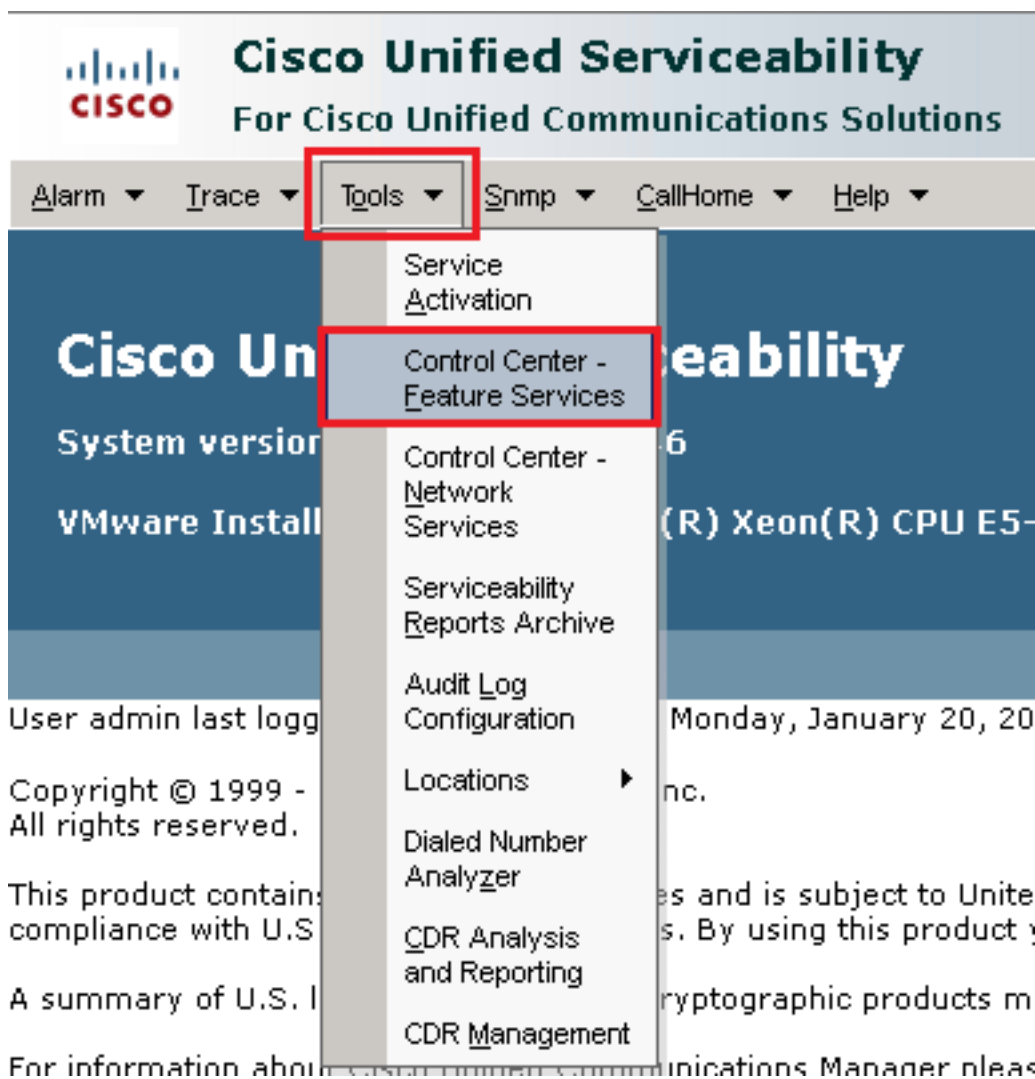
```
admin:utils ctl set-cluster mixed-mode
This operation will set the cluster to Mixed mode. Auto-registration is enabled on at least one CM node. Do you want to continue? (y/n): y
Moving Cluster to Mixed Mode
Cluster set to Mixed Mode
Please restart Cisco CallManager service and Cisco CTIManager services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

8. Per rendere effettive le modifiche, riavviare Cisco CallManager e Cisco CTIManager servizi.

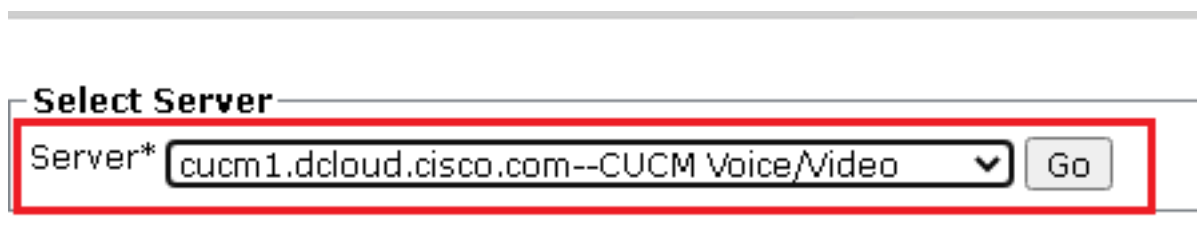
9. Per riavviare i servizi, spostarsi e accedere a Cisco Unified Serviceability.



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



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

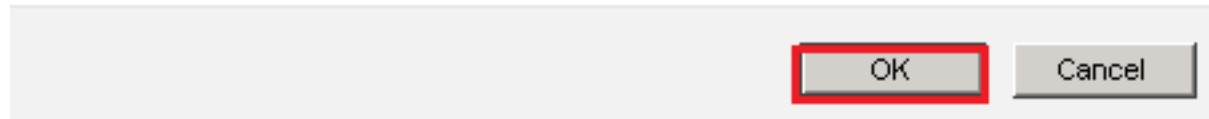


12. Sotto i servizi di CM, scegliere Cisco CallManager quindi fare clic su Restart nella parte superiore della pagina.

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.

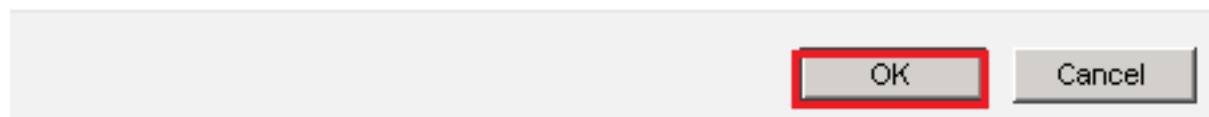


14. Dopo il corretto riavvio di Cisco CallManager, scegliere Cisco CTIManager quindi fare clic su **Restart** pulsante per il riavvio Cisco CTIManager servizio.

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.



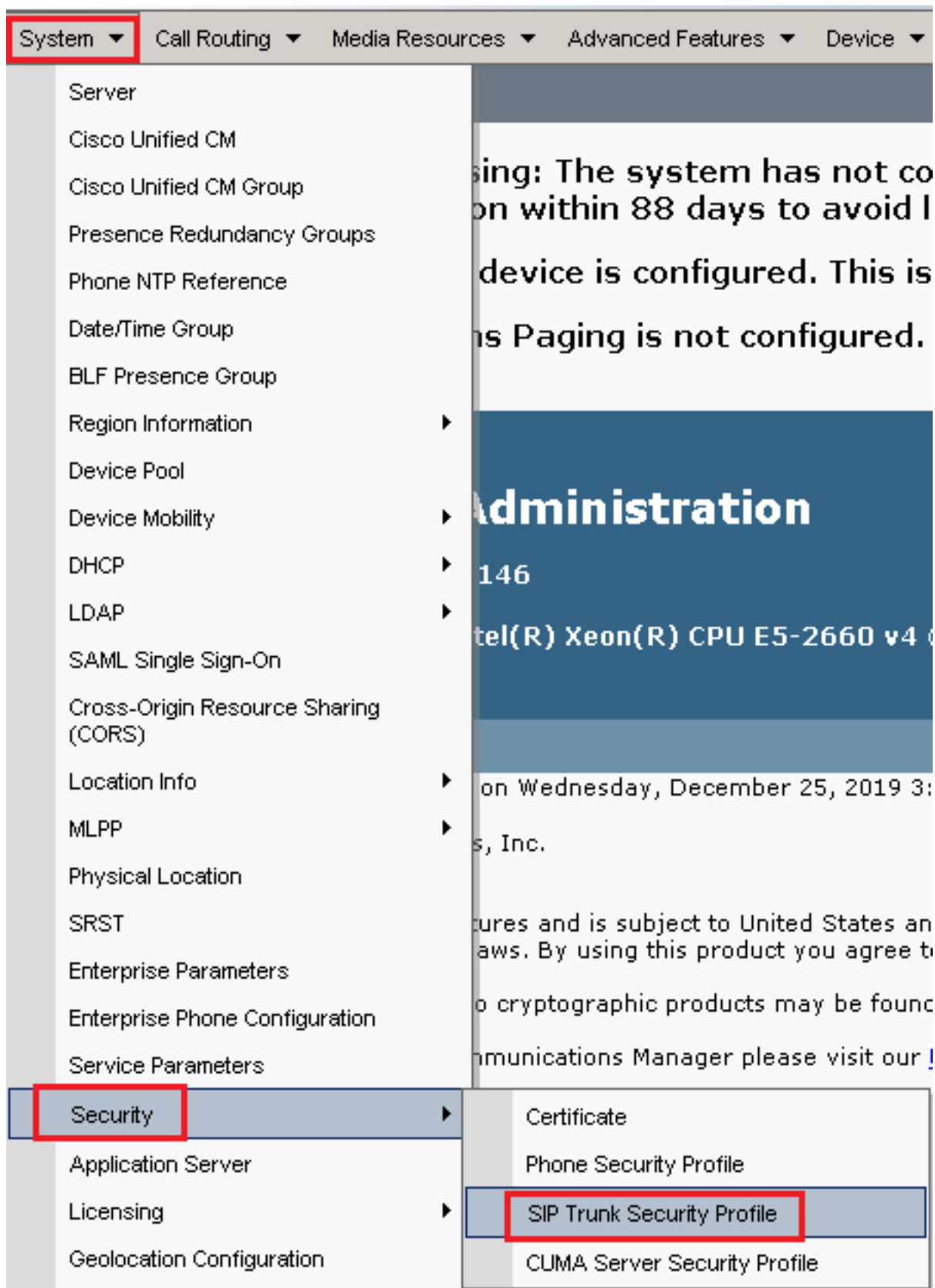
16. Dopo il riavvio corretto dei servizi, verificare che la modalità di protezione del cluster sia impostata sulla modalità mista, passare all'amministrazione CUCM come illustrato al passo 5, quindi controllare la **Cluster Security Mode**. Ora deve essere impostato su **1**.

Security Parameters	
<a href="#">Cluster Security Mode</a> *	1
<a href="#">Cluster SIPOAuth Mode</a> *	Disabled

## Configurare i profili di sicurezza trunk SIP per CUBE e CVP

Passaggi:

1. Accedi a CUCM administration interfaccia.
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** 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 mostrato nell'immagine, quindi fare clic su **Save** in basso a sinistra per **Save** e'.



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` e `Secure Certificate Subject` al CN del certificato del server di chiamata CVP come deve corrispondere. Clic `Save` pulsante.

**Status**

- i** Add successful
- i** 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

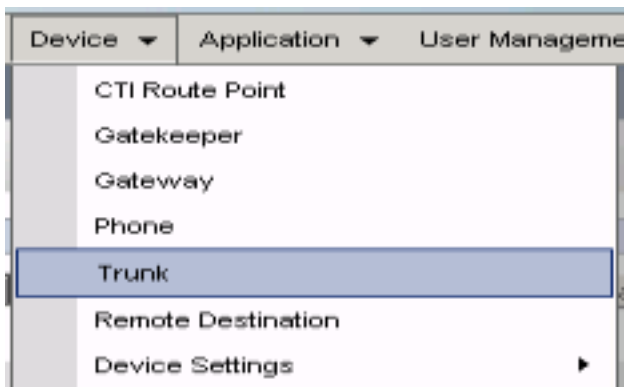
Allow charging header

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

## Associa profili di sicurezza trunk SIP ai rispettivi trunk SIP

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 . Clic Find.

Trunks (1 - 5 of 5)

Find Trunks where Device Name begins with vCube Find Clear Filter

	Name	Description	Calling Search Space	Device Pool	Route Pattern	Partition
<input type="checkbox"/>	vCUBE		dCloud_CSS	dCloud_DP	cloudcherry_sip.twilio.com	dCloud_PT
<input type="checkbox"/>	vCUBE		dCloud_CSS	dCloud_DP	7800	PSTN_Incoming_Numbers
<input type="checkbox"/>	vCUBE		dCloud_CSS	dCloud_DP	6016	PSTN_Incoming_Numbers
<input type="checkbox"/>	vCUBE		dCloud_CSS	dCloud_DP	7019	PSTN_Incoming_Numbers
<input type="checkbox"/>	vCUBE		dCloud_CSS	dCloud_DP	44413XX	Robot Agent Remote Destinations

3. Fare clic su vCUBE per aprire la pagina di configurazione del trunk vCUBE.

4. Scorri fino a SIP Information e modificare la Destination Port a 5061.

5. Cambia SIP Trunk Security Profile a SecureSIPTLSForCube.

SIP Information

Destination

Destination Address is an SRV

1*	Destination Address	Destination Address IPv6	Destination Port
	198.18.133.226		5061

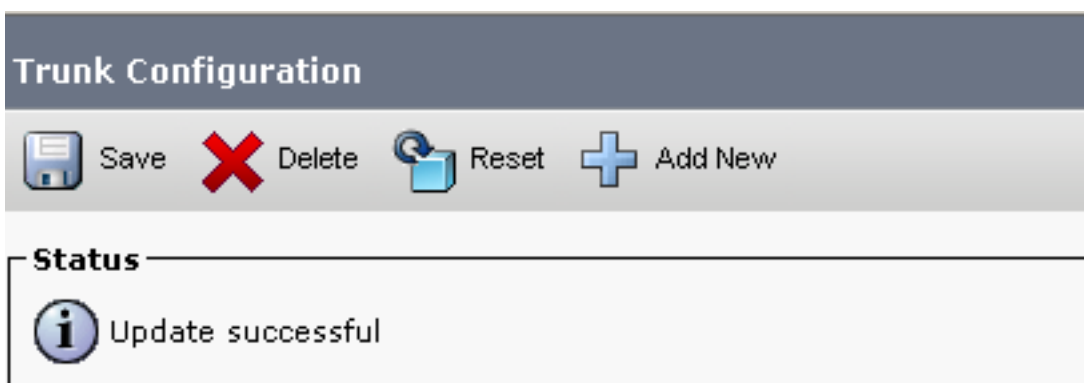
MTP Preferred Originating Codec\* 711ulaw

BLF Presence Group\* Standard Presence group

SIP Trunk Security Profile\* SecureSIPTLSforCube

Rerouting Calling Search Space < None >


6. Clic Save quindi Rest per 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






- Passa a **Device > Trunk** cercare CVP trunk. In questo esempio, il nome del trunk CVP 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				
	Name	Description	Calling Search Space	Device Pool
<input type="checkbox"/>	 <a href="#">CVP-SIP-Trunk</a>	CVP-SIP-Trunk	<a href="#">dCloud_CSS</a>	<a href="#">dCloud_DP</a>

- Clic **CVP-SIP-Trunk** per aprire la pagina di configurazione di CVP trunk.
- Scorri fino a **SIP Information** e modifica **Destination Port** a **5061** .
- Cambia **SIP Trunk Security Profile** a **SecureSIPTLSForCvp**.

SIP Information		
Destination		
<input type="checkbox"/>	Destination Address is an SRV	
	Destination Address	Destination Address IPv6
1*	198.18.133.13	
		Destination Port
		5061
MTP Preferred Originating Codec*	711ulaw	
BLF Presence Group*	Standard Presence group	
SIP Trunk Security Profile*	SecureSIPTLSforCvp	

- Clic **Save** quindi **Rest** per 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

## Comunicazione dei dispositivi degli agenti sicuri con CUCM

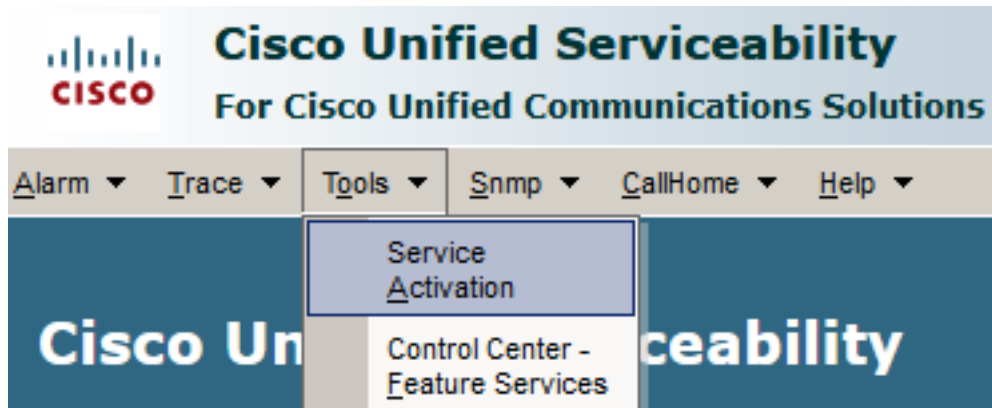
Per abilitare le funzionalità di protezione per un dispositivo, è necessario installare un certificato



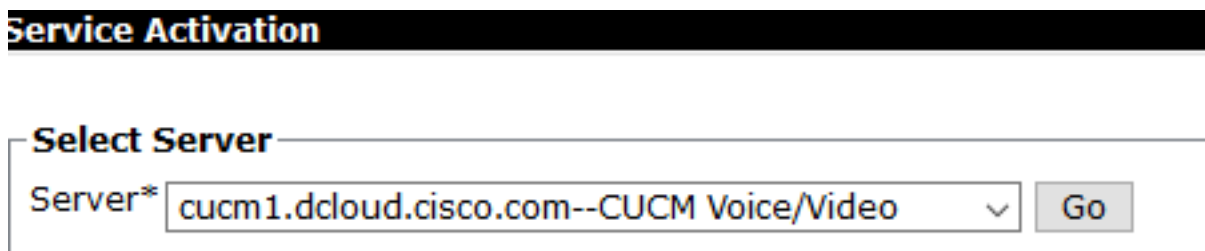
LSC (Locally Significant Certificate) e assegnare un profilo di protezione al dispositivo. Il servizio LSC possiede la chiave pubblica per l'endpoint, firmata dalla chiave privata CAPF (Certificate Authority Proxy Function). Per impostazione predefinita, non è installato sui telefoni.

Passaggi:

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



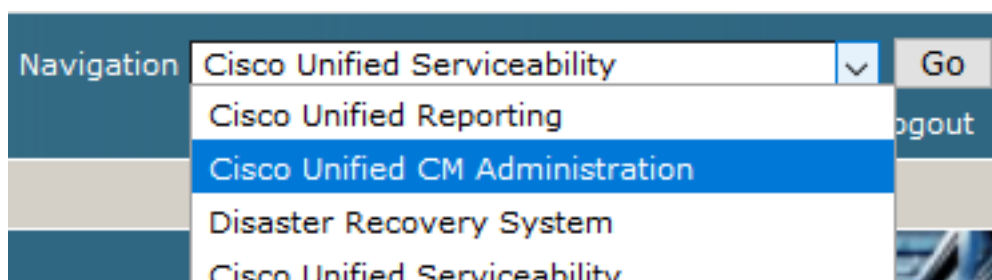
3. Scegliere il server CUCM e fare clic su **Go**.



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

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. Verificare che il servizio sia attivato, quindi passare a **Cisco Unified CM Administration**.



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.



# Cisco Unified CM Administration

For Cisco Unified Communications Solutions

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 ▶

Application Server

Licensing ▶

Geolocation Configuration

device is configured. The  
Paging is not configur

## Administration

7

tel(R) Xeon(R) CPU E5-2660

on Friday, December 20, 2019 10

s, Inc.

ures and is subject to United Stat  
aws. By using this product you ac

o cryptographic products may be

munications Manager please visit


our [Technical Support](#) web site.

Certificate

Phone Security Profile

SIP Trunk Security Profile

CUMA Server Security Profile

7. Individuare i profili di sicurezza corrispondenti al tipo di dispositivo agente. In questo esempio, viene utilizzato un telefono fisso, quindi scegliere Cisco Unified Client Services Framework - Standard SIP Non-Secure Profile . Clic Copy  per copiare il profilo.

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

Find Phone Security Profile where

<input type="checkbox"/>	Name ^	Description	Copy
<input type="checkbox"/>	<a href="#">Cisco Unified Client Services Framework - Standard SIP Non-Secure Profile</a>	Cisco Unified Client Services Framework - Standard SIP Non-Secure Profile	<input type="button" value="Copy"/>

8. Rinomina il profilo in Cisco Unified Client Services Framework - Secure Profile, modificare i parametri come mostrato nell'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

**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

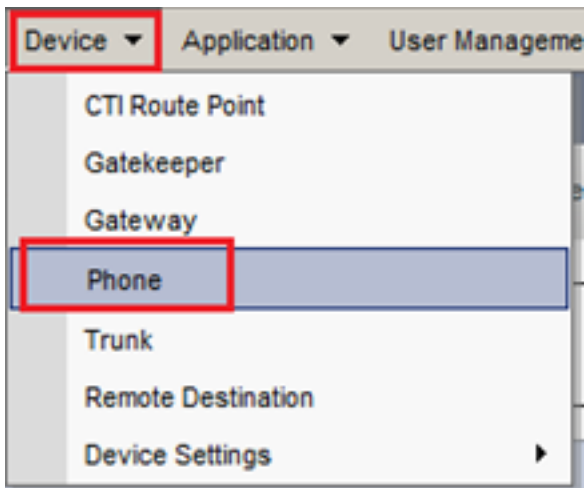
**Phone Security Profile CAPF Information**

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\*

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



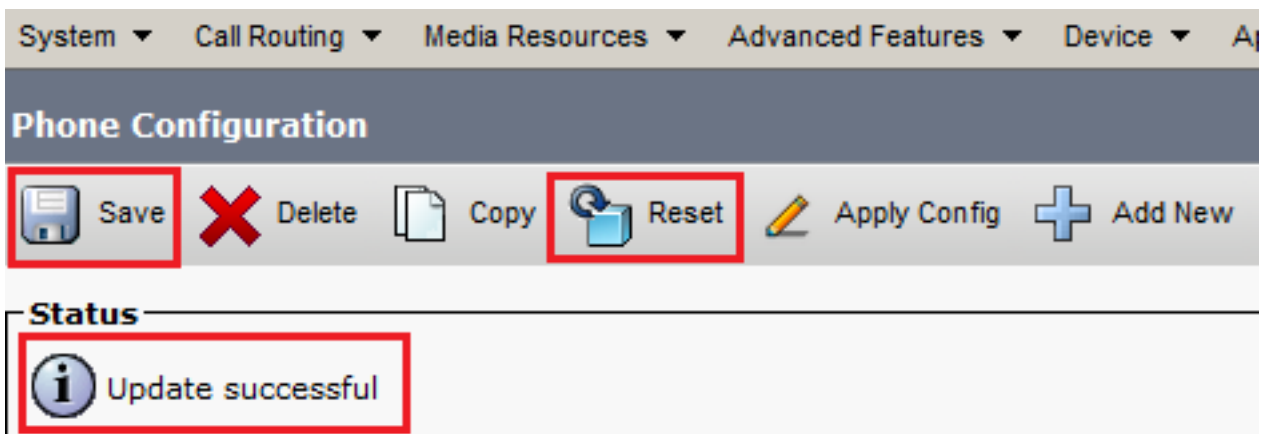
10. Clic Find per elencare tutti i telefoni disponibili, fare clic su telefono agente.
11. Verrà visualizzata la pagina Configurazione telefono agente. Cerca Certification Authority Proxy Function (CAPF) Information sezione. Per installare LSC, impostare Certificate Operation a Install/Upgrade e Operation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

A screenshot of the 'Certification Authority Proxy Function (CAPF) Information' configuration page. The page contains several fields and dropdown menus. The 'Certificate Operation\*' dropdown is set to 'Install/Upgrade' and is highlighted with a red box. The 'Authentication Mode\*' dropdown is set to 'By Null String'. The 'Authentication String' field is empty, with a 'Generate String' button below it. The 'Key Order\*' dropdown is set to 'RSA Only'. The 'RSA Key Size (Bits)\*' dropdown is set to '2048'. The 'EC Key Size (Bits)' dropdown is empty. The 'Operation Completes By' field is set to '2021 04 16 12 (YYYY:MM:DD:HH)' and is highlighted with a red box. Below the date field, the 'Certificate Operation Status' is 'None' and a note states 'Note: Security Profile Contains Addition CAPF Settings.'

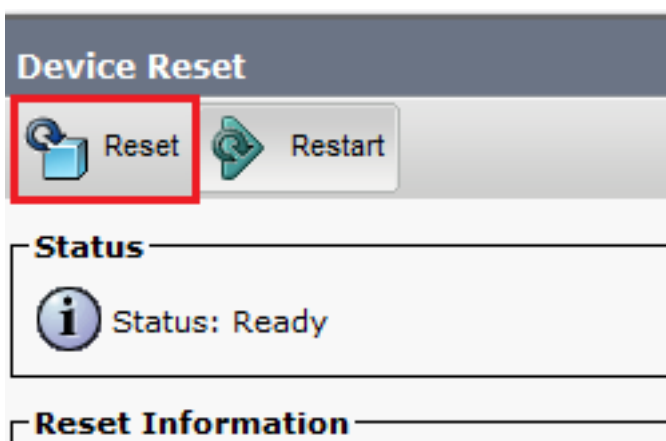
12. Cerca Protocol Specific Information sezione. Cambia Device Security Profile a Cisco Unified Client Services Framework – Secure Profile.

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

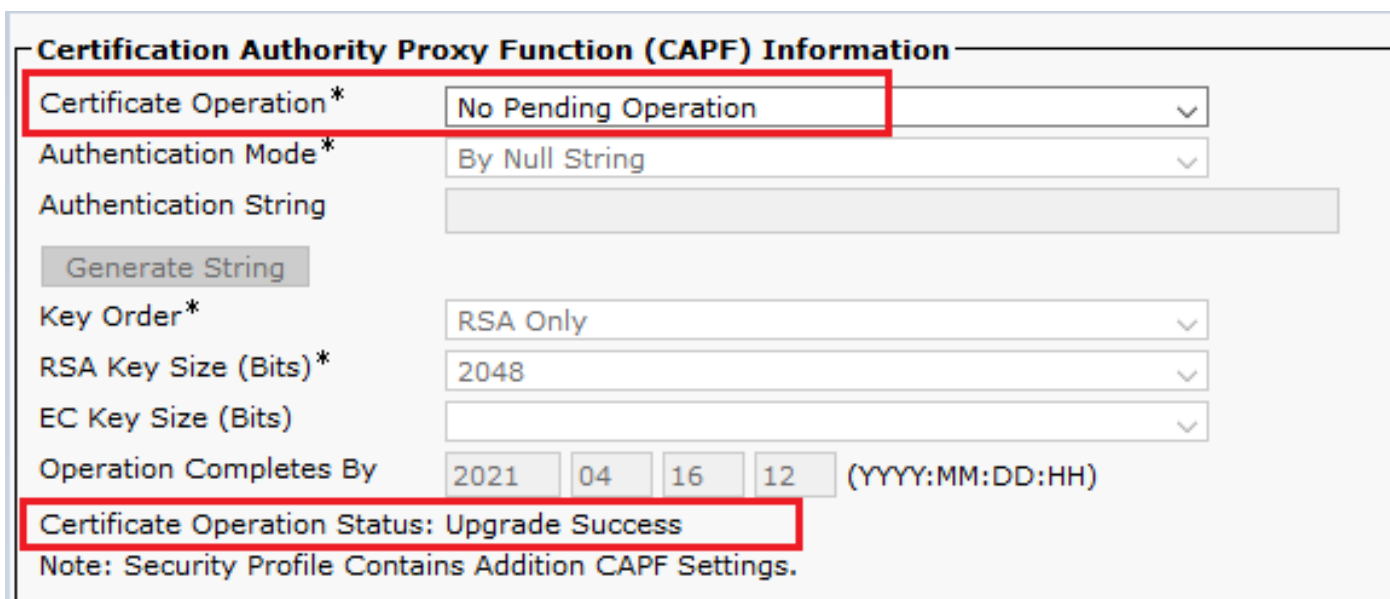
13. Clic Save in alto a sinistra nella pagina. Assicurarsi che le modifiche siano state salvate correttamente e fare clic su Reset.



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 alla sezione Passi. 7-13 per proteggere altri agenti e dispositivi che si desidera utilizzare per proteggere il SIP con CUCM.

# Verifica

Per verificare che la segnalazione SIP sia protetta correttamente, procedere come segue:

1. Aprire la sessione SSH su vCUBE, eseguire il comando `show sip-ua connections tcp tls detail` e confermare che al momento non vi è alcuna connessione TLS stabilita con CVP (198.18.133.13).

```
CC-VCUBE#show sip-ua connections tcp tls detail
Total active connections      : 1
No. of send failures         : 0
No. of remote closures       : 34
No. of conn. failures        : 0
No. of inactive conn. ageouts : 12
TLS client handshake failures : 0
TLS server handshake failures : 0

-----Printing Detailed Connection Report-----
Note:
** Tuples with no matching socket entry
- Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port>'
  to overcome this error condition
++ Tuples with mismatched address/port entry
- Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port> id <connid>'
  to overcome this error condition

Remote-Agent:198.18.133.3, Connections-Count:1
  Remote-Port Conn-Id Conn-State  WriteQ-Size Local-Address  TLS-Version
  =====
          44868      49 Established      0           -             TLSv1.2

Remote-Agent:198.18.133.13, Connections-Count:0

----- SIP Transport Layer Listen Sockets -----
Conn-Id      Local-Address
=====
0            [0.0.0.0]:5061:
```



**Nota:** al momento, solo una sessione TLS attiva con CUCM, per le opzioni SIP è abilitata su CUCM (198.18.13.3). Se non è attivata alcuna opzione SIP, non esiste alcuna connessione SIP TLS.

2. Accedere a CVP e avviare Wireshark.
3. Effettua una chiamata di prova al numero del contact center.
4. Passare alla sessione CVP; su Wireshark, eseguire questo filtro per controllare la segnalazione SIP con CUBE:  
`ip.addr == 198.18.133.226 && tls && tcp.port==5061`

No.	Time	Source	Destination	Protocol	Length	Info
2409	63.180370	198.18.133.226	198.18.133.13	TLSv1.2	173	Client Hello
2411	63.183691	198.18.133.13	198.18.133.226	TLSv1.2	1153	Server Hello, Certificate, Server Hello Done
2414	63.188871	198.18.133.226	198.18.133.13	TLSv1.2	396	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
2415	63.202820	198.18.133.13	198.18.133.226	TLSv1.2	60	Change Cipher Spec
2416	63.203063	198.18.133.13	198.18.133.226	TLSv1.2	123	Encrypted Handshake Message
2419	63.207380	198.18.133.226	198.18.133.13	TLSv1.2	614	Application Data
2421	63.255349	198.18.133.13	198.18.133.226	TLSv1.2	635	Application Data
2508	63.495508	198.18.133.13	198.18.133.226	TLSv1.2	1067	Application Data
2565	63.505008	198.18.133.226	198.18.133.13	TLSv1.2	587	Application Data

**Verifica:** la connessione SIP over TLS è stata stabilita? In caso affermativo, l'output conferma che i segnali SIP tra CVP e CUBE sono protetti.

5. Controllare la connessione SIP TLS tra CVP e CVB. Nella stessa sessione di Wireshark, eseguire questo filtro:

```
ip.addr == 198.18.133.143 && tls && tcp.port==5061
```

No.	Time	Source	Destination	Protocol	Length	Info
2490	63.358533	198.18.133.13	198.18.133.143	TLSv1.2	171	Client Hello
2494	63.360224	198.18.133.143	198.18.133.13	TLSv1.2	1205	Server Hello, Certificate, Server Hello Done
2496	63.365714	198.18.133.13	198.18.133.143	TLSv1.2	321	Client Key Exchange
2498	63.405567	198.18.133.13	198.18.133.143	TLSv1.2	129	Change Cipher Spec, Encrypted Handshake Message
2501	63.434468	198.18.133.143	198.18.133.13	TLSv1.2	129	Change Cipher Spec, Encrypted Handshake Message
2503	63.442731	198.18.133.13	198.18.133.143	TLSv1.2	631	Application Data
2505	63.446286	198.18.133.143	198.18.133.13	TLSv1.2	539	Application Data
2506	63.472083	198.18.133.143	198.18.133.13	TLSv1.2	1003	Application Data
2566	63.512809	198.18.133.13	198.18.133.143	TLSv1.2	715	Application Data

**Verifica:** la connessione SIP over TLS è stata stabilita? In caso affermativo, l'uscita conferma che i segnali SIP tra CVP e CVB sono protetti.

6. È inoltre possibile verificare la connessione SIP TLS con CVP da CUBE. Passare alla sessione SSH vCUBE ed eseguire questo comando per controllare i segnali sip sicuri:

```
show sip-ua connections tcp tls detail
```

```
CC-VCUBE#show sip-ua connections tcp tls detail
Total active connections      : 2
No. of send failures         : 0
No. of remote closures       : 0
No. of conn. failures        : 0
No. of inactive conn. ageouts : 0
TLS client handshake failures : 0
TLS server handshake failures : 0

-----Printing Detailed Connection Report-----
Note:
** Tuples with no matching socket entry
  - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port>'
    to overcome this error condition
++ Tuples with mismatched address/port entry
  - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port> id <connid>'
    to overcome this error condition

Remote-Agent:198.18.133.3, Connections-Count:1
  Remote-Port Conn-Id Conn-State WriteQ-Size Local-Address TLS-Version
  =====
      38896      2 Established      0      -      TLSv1.2

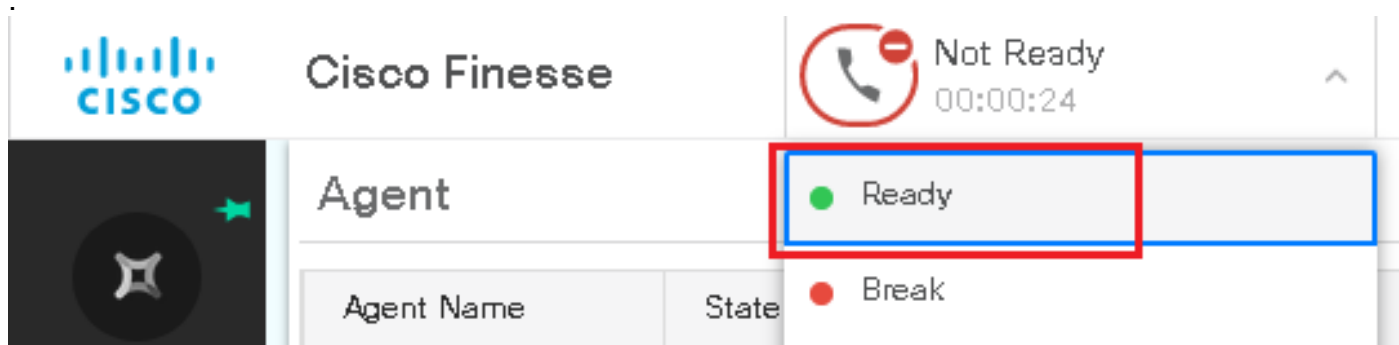
Remote-Agent:198.18.133.13, Connections-Count:1
  Remote-Port Conn-Id Conn-State WriteQ-Size Local-Address TLS-Version
  =====
      5061      3 Established      0      -      TLSv1.2

----- SIP Transport Layer Listen Sockets -----
  Conn-Id      Local-Address
  =====
      0      [0.0.0.0]:5061:
```

**Verifica:** la connessione SIP over TLS è stabilita con CVP? In caso affermativo, l'output conferma che i segnali SIP tra CVP e CUBE sono protetti.

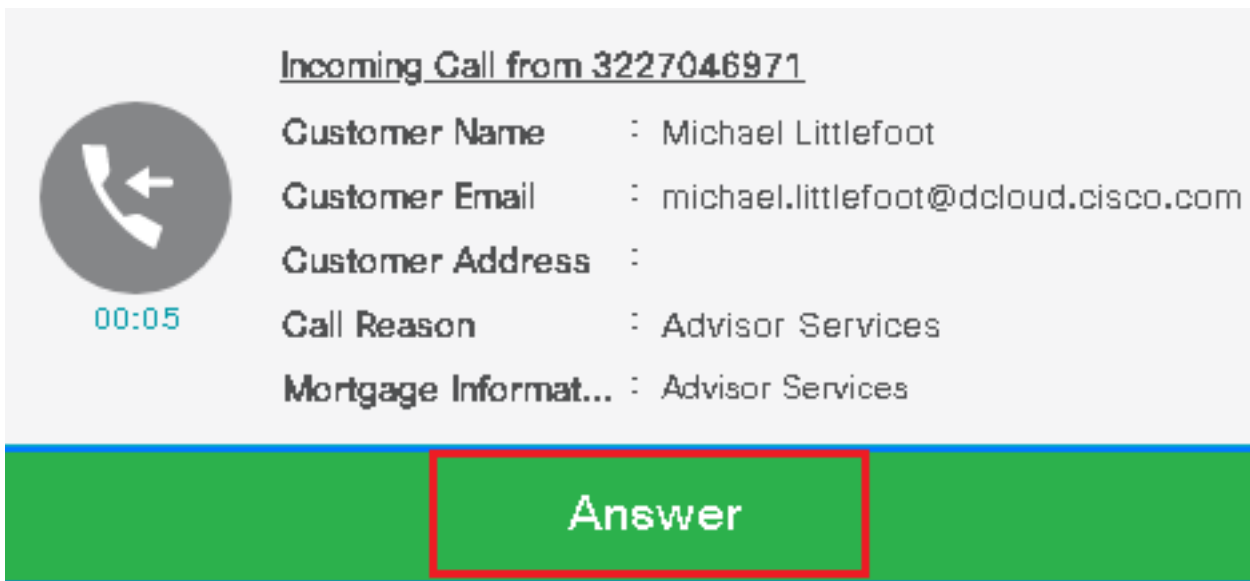
7. Al momento, la chiamata è attiva e si ascolta Music on Hold (MOH) poiché non è disponibile alcun agente per rispondere alla chiamata.

8. Rendere disponibile l'agente per rispondere alla chiamata.





9. L'agente viene riservato e la chiamata viene indirizzata a lui/lei. Clic Answer per rispondere alla chiamata.



**Incoming Call from 3227046971**

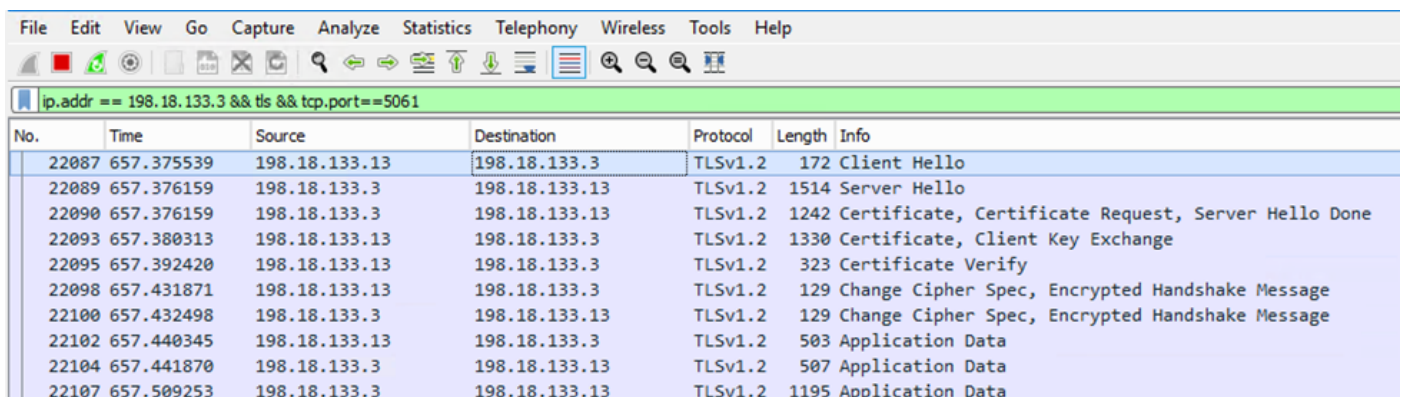
Customer Name : Michael Littlefoot  
Customer Email : michael.littlefoot@dcloud.cisco.com  
Customer Address :  
Call Reason : Advisor Services  
Mortgage Informat... : Advisor Services

**Answer**

10. La chiamata si connette all'agente.

11. Per verificare i segnali SIP tra CVP e CUCM, passare alla sessione CVP ed eseguire questo filtro in Wireshark:

```
ip.addr == 198.18.133.3 && tls && tcp.port==5061
```



No.	Time	Source	Destination	Protocol	Length	Info
22087	657.375539	198.18.133.13	198.18.133.3	TLSv1.2	172	Client Hello
22089	657.376159	198.18.133.3	198.18.133.13	TLSv1.2	1514	Server Hello
22090	657.376159	198.18.133.3	198.18.133.13	TLSv1.2	1242	Certificate, Certificate Request, Server Hello Done
22093	657.380313	198.18.133.13	198.18.133.3	TLSv1.2	1330	Certificate, Client Key Exchange
22095	657.392420	198.18.133.13	198.18.133.3	TLSv1.2	323	Certificate Verify
22098	657.431871	198.18.133.13	198.18.133.3	TLSv1.2	129	Change Cipher Spec, Encrypted Handshake Message
22100	657.432498	198.18.133.3	198.18.133.13	TLSv1.2	129	Change Cipher Spec, Encrypted Handshake Message
22102	657.440345	198.18.133.13	198.18.133.3	TLSv1.2	503	Application Data
22104	657.441870	198.18.133.3	198.18.133.13	TLSv1.2	507	Application Data
22107	657.509253	198.18.133.3	198.18.133.13	TLSv1.2	1195	Application Data

**Controllare:** tutte le comunicazioni SIP con CUCM (198.18.133.3) over TLS? In caso affermativo, l'output conferma che i segnali SIP tra CVP e CUCM sono protetti.

## Risoluzione dei problemi

Se TLS non viene stabilito, eseguire questi comandi su CUBE per abilitare il debug TLS alla risoluzione dei problemi:

- Debug ssl openssl errors
- Debug ssl openssl msg
- Debug ssl openssl states

## 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).