

# Configuración de la señalización SIP segura en Contact Center Enterprise

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Tarea 1. Configuración segura de CUBE](#)

[Tarea 2. Configuración segura de CVP](#)

[Tarea 3. Configuración segura de CVB](#)

[Tarea 4. Configuración segura de CUCM](#)

[Establecer el modo de seguridad de CUCM en modo mixto](#)

[Configuración de los perfiles de seguridad del troncal SIP para CUBE y CVP](#)

[Asociar perfiles de seguridad de línea troncal SIP a líneas troncales SIP respectivas](#)

[Comunicación de dispositivos de agentes seguros con CUCM](#)

[Verificación](#)

[Troubleshoot](#)

## Introducción

En este documento se describe cómo proteger la señalización del protocolo de inicio de sesión (SIP) en el flujo de llamadas completo de Contact Center Enterprise (CCE).

## Prerequisites

La generación y la importación de certificados no están incluidas en el ámbito de este documento, por lo que se deben crear e importar certificados para Cisco Unified Communication Manager (CUCM), el servidor de llamadas de Customer Voice Portal (CVP), Cisco Virtual Voice Browser (CVVB) y Cisco Unified Border Element (CUBE) en los componentes respectivos. Si utiliza certificados autofirmados, el intercambio de certificados debe realizarse entre los diferentes componentes.

## Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- CCE
- CVP
- CUBO
- CUCM
- CVVB

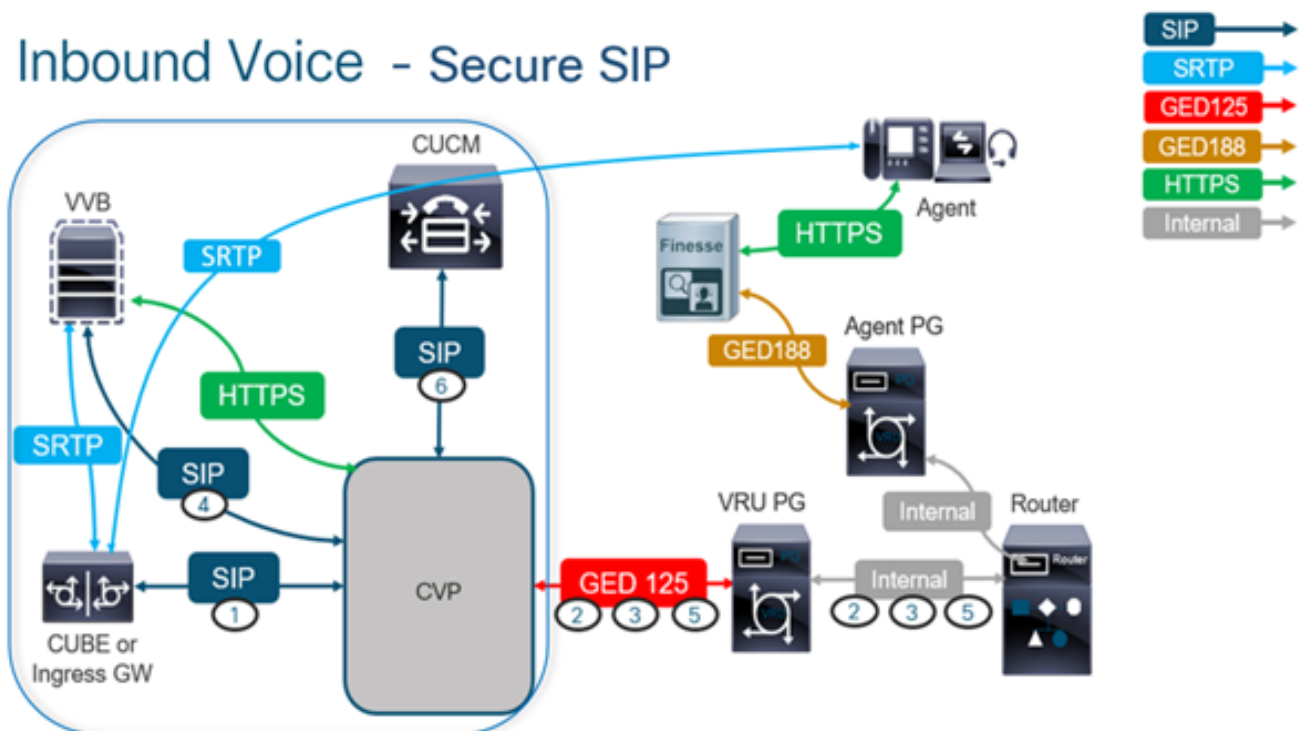
## Componentes Utilizados

La información de este documento se basa en Package Contact Center Enterprise (PCCE), CVP, CVB y CUCM versión 12.6, pero también es aplicable a las versiones anteriores.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Configurar

El siguiente diagrama muestra los componentes implicados en la señalización SIP en el flujo de llamadas completo del centro de contacto. Cuando el sistema recibe una llamada de voz, primero se realiza a través del gateway de entrada o CUBE, así que inicie configuraciones SIP seguras en CUBE. A continuación, configure CVP, CVB y CUCM.



### Tarea 1. Configuración segura de CUBE

En esta tarea, configure CUBE para proteger los mensajes del protocolo SIP.

Configuraciones necesarias:

- Configuración de un punto de confianza predeterminado para el agente de usuario SIP (UA)
- Modificar los pares de marcado para utilizar la seguridad de la capa de transporte (TLS)

Pasos:

1. Abra una sesión de Secure Shell (SSH) en CUBE.
2. Ejecute estos comandos para que la pila SIP utilice el certificado de la autoridad certificadora

(CA) del CUBE. CUBE establece una conexión SIP TLS desde/hacia CUCM (198.18.133.3) y 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. Ejecute estos comandos para habilitar TLS en el par de marcado saliente para CVP. En este ejemplo, la etiqueta dial-peer 6000 se utiliza para rutear llamadas 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)#
```

## Tarea 2. Configuración segura de CVP

En esta tarea, configure el servidor de llamadas CVP para proteger los mensajes del protocolo SIP (SIP TLS).

Pasos:

1. Inicie sesión en UCCE Web Administration.
2. Desplácese hasta **Call Settings > Route Settings > SIP Server Group**.

### Route Settings

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

Properties

Según sus configuraciones, tiene grupos de servidores SIP configurados para CUCM, CVB y CUBE. Debe establecer los puertos SIP seguros en 5061 para todos ellos. En este ejemplo, se utilizan estos grupos de servidores SIP:

- cucm1.dcloud.cisco.com para CUCM
- vvb1.dcloud.cisco.com para CVVB
- cube1.dcloud.cisco.com para CUBE

3. Haga clic en **cucm1.dcloud.cisco.com** y luego en el **Members**, que muestra los detalles de la configuración del grupo de servidores SIP. Set **SecurePort** a 5061 y haga clic en **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. Haga clic en `vvb1.dcloud.cisco.com` y luego en el **Members** ficha. Establezca SecurePort en 5061 y haga clic en **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

### Tarea 3. Configuración segura de CVB

En esta tarea, configure CVB para proteger los mensajes del protocolo SIP (SIP TLS).

Pasos:

1. Inicie sesión en **Cisco VVB Administration** página.
2. Desplácese hasta **System > System Parameters**.

The screenshot shows the Cisco Virtualized Voice Browser Administration interface. At the top, there is a navigation bar with the following items: System, Applications, Subsystems, Tools, and Help. Below this, a dropdown menu is open, showing 'System Parameters' and 'Logout'. The main header area displays the Cisco logo and the text 'Cisco Virtualized Voice Browser Administration For Cisco Unified Communications Solutions'. At the bottom, there is a dark blue banner with the text 'Cisco Virtualized Voice Browser Administration' and 'System version: 12.5.1.10000-24'.

3. En el **Security Parameters** sección, elija **Enable** para TLS(SIP) . Mantener **Supported TLS(SIP)**

version como 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
SRTSP [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. Haga clic en Update (Actualizar). Haga clic en ok cuando se le solicite reiniciar el motor CVB.

The screenshot shows the Cisco Virtualized Voice Administration interface. A notification dialog box is displayed over the 'System Parameters Configuration' page. The dialog box contains the text: 'vwb1.dcloud.cisco.com says Please restart Cisco VVB Engine for the updates to take effect.' and an 'OK' button. In the background, the 'Update' button is highlighted.

5. Estos cambios requieren que se reinicie el motor Cisco VB. Para reiniciar el motor VB, navegue hasta Cisco VVB Serviceability haga clic en 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), and 'Cisco Unified OS Administration'. A 'Go' button is visible next to the dropdown.

6. Desplácese hasta Tools > Control Center – Network Services.

The screenshot shows the 'Tools' menu in the Cisco VVB Administration interface. The 'Control Center - Network Services' option is highlighted, indicating the next step in the process.

7. Elegir Engine y haga clic en 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

### Tarea 4. Configuración segura de CUCM

Para proteger los mensajes SIP en CUCM, realice las siguientes configuraciones:

- Establecer el modo de seguridad de CUCM en modo mixto
- Configuración de los perfiles de seguridad del troncal SIP para CUBE y CVP
- Asociar perfiles de seguridad de línea troncal SIP a líneas troncales SIP respectivas
- Comunicación de dispositivos de agentes seguros con CUCM

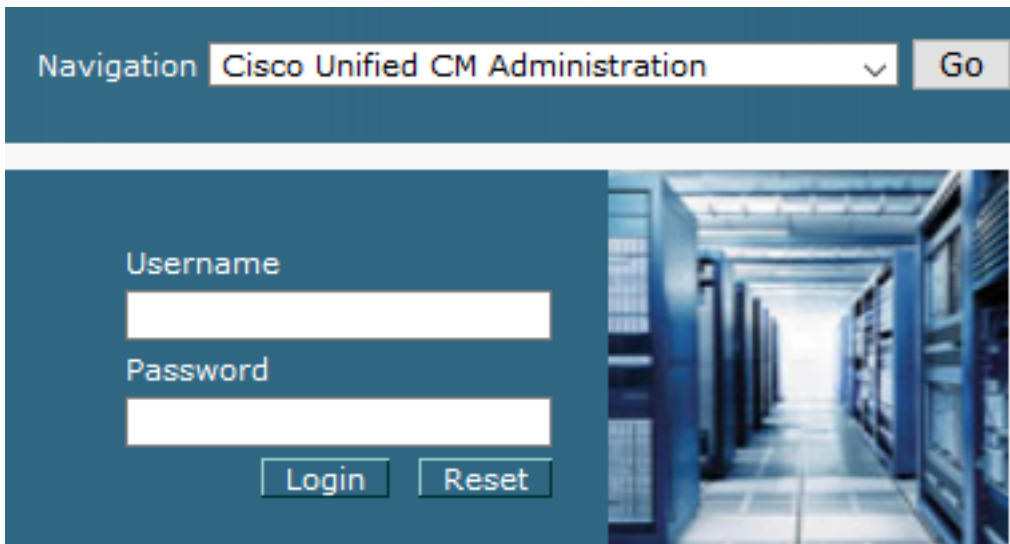
#### Establecer el modo de seguridad de CUCM en modo mixto

CUCM admite dos modos de seguridad:

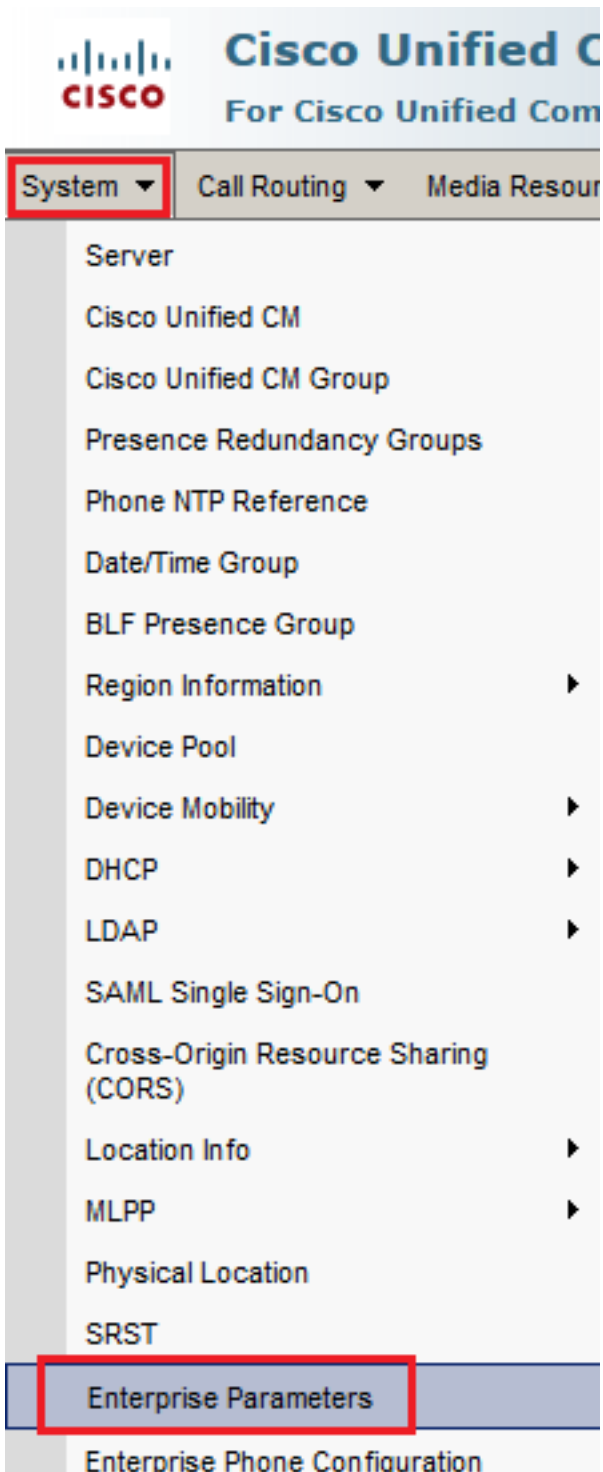
- Modo no seguro (modo predeterminado)
- Modo mixto (modo seguro)

Pasos:

1. Para establecer el modo de seguridad en Mixed Mode, inicie sesión en Cisco Unified CM Administration interfaz.



2. Después de iniciar sesión correctamente en CUCM, vaya a [System > Enterprise Parameters](#).



3. Debajo del Security Parameters Sección, comprobar si Cluster Security Mode se establece en 0.



4. Si el modo de seguridad de clúster se establece en 0, significa que el modo de seguridad de clúster se establece en no seguro. Debe habilitar el modo mixto desde CLI.
5. Abra una sesión SSH en CUCM.
6. Después de haber iniciado sesión correctamente en CUCM a través de SSH, ejecute este comando: `utils ctl set-cluster mixed-mode`

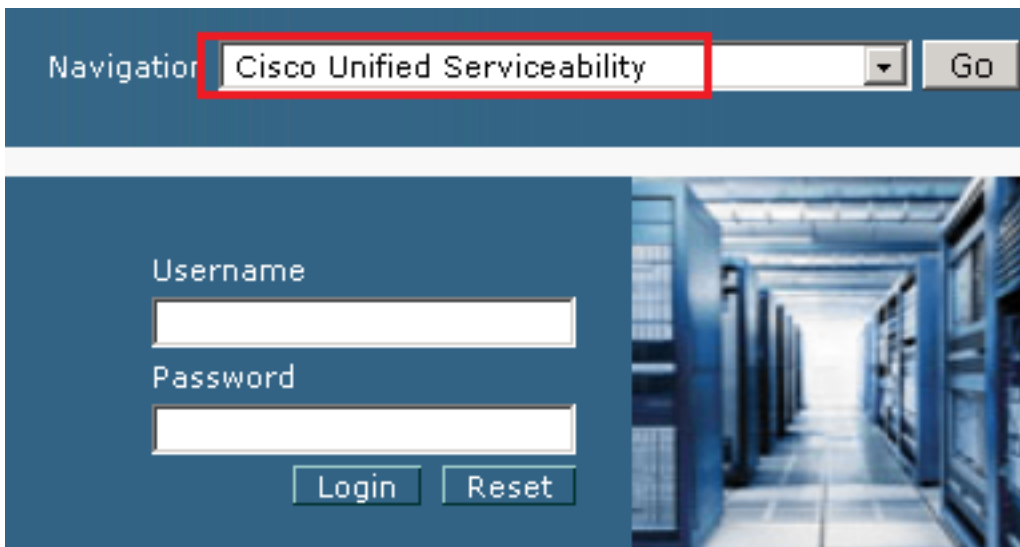


7. Tipo **y** y haga clic en **Intro** cuando se le solicite. Este comando establece el modo de seguridad del clúster en modo mixto.

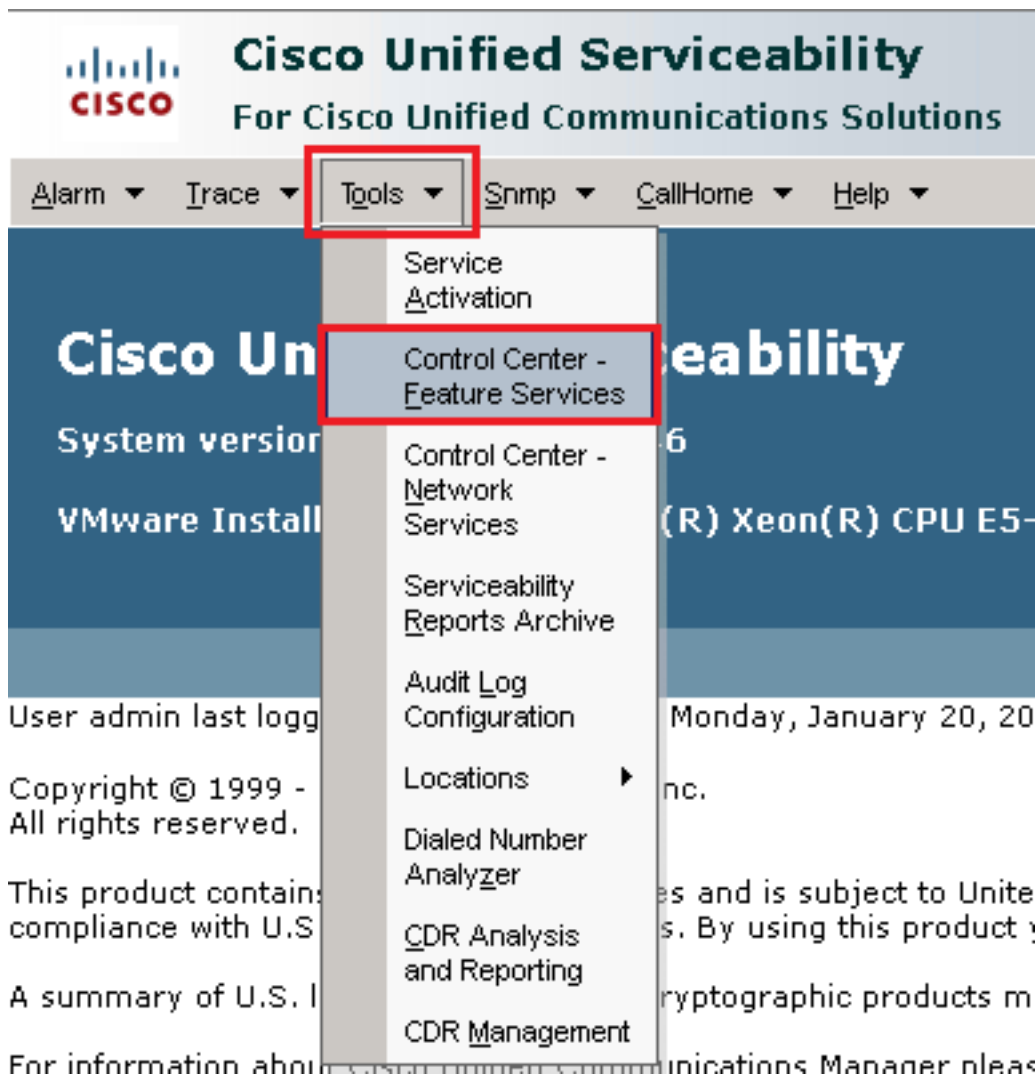
```
admin:utils ctl set-cluster mixed-mode
This operation will set the cluster to Mixed mode. Auto-registration is enabled on at least one CM node. Do you want to continue? (y/n): y
Moving Cluster to Mixed Mode
Cluster set to Mixed Mode
Please restart Cisco CallManager service and Cisco CTIManager services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

8. Para que los cambios surtan efecto, reinicie Cisco CallManager y Cisco CTIManager servicios.

9. Para reiniciar los servicios, navegue e inicie sesión en Cisco Unified Serviceability.



10. Después de iniciar sesión correctamente, vaya a **Tools > Control Center – Feature Services**.



11. Elija el servidor y haga clic en Go.



12. Debajo de los servicios CM, seleccione Cisco CallManager haga clic en Restart en la parte superior de la página.

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. Confirme el mensaje emergente y haga clic en **OK**. Espere a que el servicio se reinicie correctamente.

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. Tras un reinicio correcto de Cisco CallManager, elija Cisco CTIManager haga clic en **Restart** botón para reiniciar Cisco CTIManager servicio.

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. Confirme el mensaje emergente y haga clic en **OK**. Espere a que el servicio se reinicie correctamente.

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.



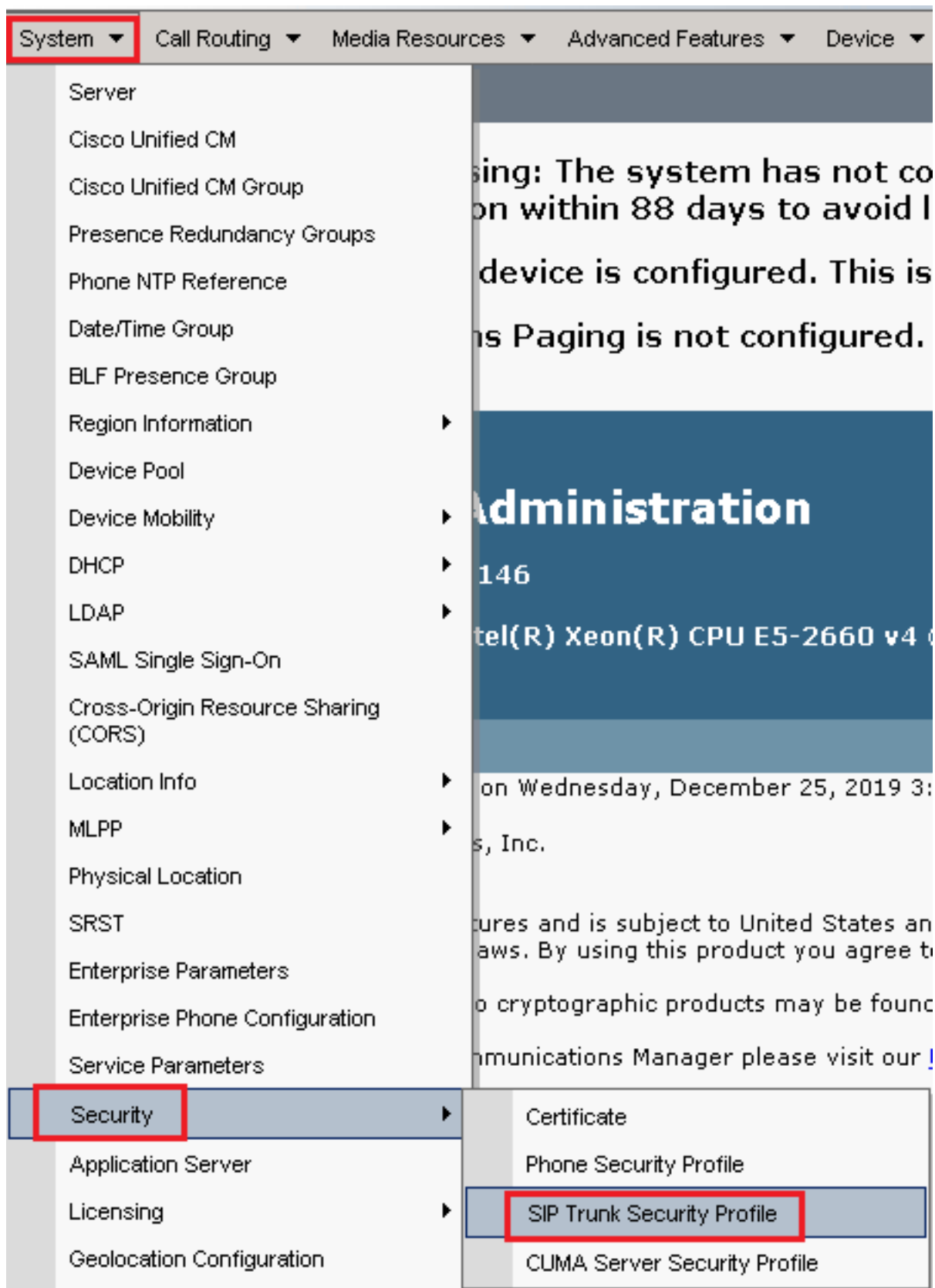
16. Después de que los servicios se reinicien correctamente, verifique que el modo de seguridad del clúster esté configurado en modo mixto, navegue hasta la administración de CUCM como se explicó en el paso 5. luego, verifique el **Cluster Security Mode**. Ahora debe configurarse en 1.

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

### Configuración de los perfiles de seguridad del troncal SIP para CUBE y CVP

Pasos:

1. Inicie sesión en CUCM administration interfaz.
2. Después de iniciar sesión correctamente en CUCM, vaya a System > Security > SIP Trunk Security Profile para crear un perfil de seguridad de dispositivo para CUBE.



3. En la parte superior izquierda, haga clic en Add New para agregar un nuevo perfil.

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features







## Find and List SIP Trunk Security Profiles

 Add New  Select All  Clear All  Delete Selected

4. Configurar SIP Trunk Security Profile como se muestra en esta imagen, haga clic en **Save** en la parte inferior izquierda de la página para **Save** de ti.



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. Asegúrese de establecer el Secure Certificate Subject or Subject Alternate Name al nombre común (CN) del certificado de CUBE, ya que debe coincidir.

6. Haga clic Copy y cambiar el Name a SecureSipTLSforCVP y el Secure Certificate Subject al CN del certificado del servidor de llamadas CVP, ya que debe coincidir. Haga clic en Save botón.

**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

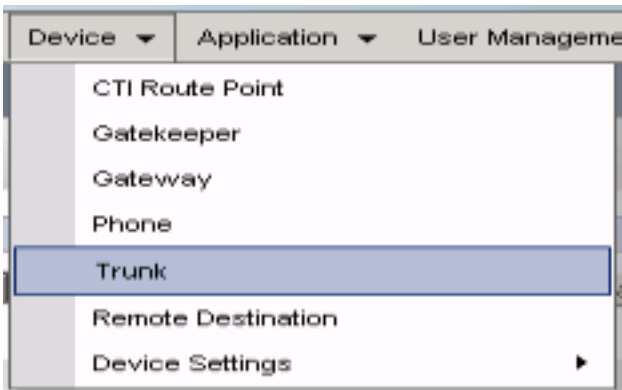
Allow charging header

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

## Asociar perfiles de seguridad de línea troncal SIP a líneas troncales SIP respectivas

Pasos:

1. En la página Administración de CUCM, desplácese hasta Device > Trunk.



2. Busque el troncal CUBE. En este ejemplo, el nombre de troncal de CUBE es vCube . Haga clic en 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. Haga clic en vCUBE para abrir la página de configuración del troncal de vCUBE.

4. Desplácese hasta SIP Information y cambiar la sección Destination Port a 5061.

5. Cambiar SIP Trunk Security Profile a SecureSIPTLSForCube.

SIP Information

Destination

Destination Address is an SRV

Destination Address: 1\* 198.18.133.226

Destination Address IPv6: [Empty]

Destination Port: 5061

MTP Preferred Originating Codec\*: 711ulaw

BLF Presence Group\*: Standard Presence group

SIP Trunk Security Profile\*: SecureSIPTLSforCube

Rerouting Calling Search Space: < None >

6. Haga clic en Save luego Rest con el fin de Save y aplicar cambios.

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

7. Desplácese hasta **Device > Trunks** busque el troncal CVP. En este ejemplo, el nombre del troncal de CVP es **cvp-SIP-Trunk** . Haga clic en **Find**.

Trunks (1 - 1 of 1)				
Find Trunks where				
<input type="checkbox"/>	Device Name	begins with	cvp	Find
Clear Filter <input type="button" value="+"/> <input type="button" value="-"/>				
Select item or enter search text				
<input type="checkbox"/>	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>






8. Haga clic en **CVP-SIP-Trunk** para abrir la página de configuración del troncal de CVP.

9. Desplácese hasta **SIP Information** sección y cambiar **Destination Port** a **5061** .

10. Cambiar **SIP Trunk Security Profile** a **SecureSIPTLSforCvp**.

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

11. Haga clic en **Save** luego **Rest** con el fin de **save** y aplicar cambios.

Trunk Configuration	
 Save	 Delete
 Reset	 Add New
<b>Status</b>	
 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

## Comunicación de dispositivos de agentes seguros con CUCM

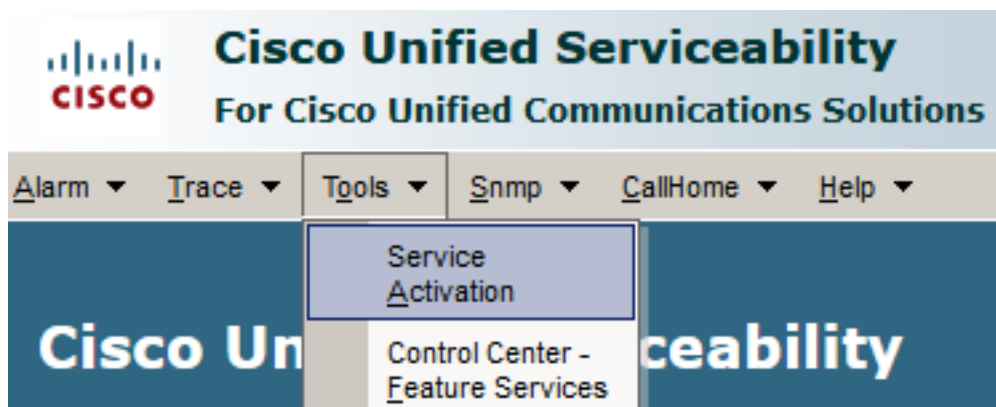
Para habilitar las funciones de seguridad para un dispositivo, debe instalar un certificado de



importancia local (LSC) y asignar un perfil de seguridad a ese dispositivo. El LSC posee la clave pública para el terminal, que está firmada por la clave privada de la función proxy de autoridad certificadora (CAPF). No está instalado en los teléfonos de forma predeterminada.

Pasos:

1. Inicie sesión en Cisco Unified Serviceability Interface.
2. Desplácese hasta **Tools > Service Activation**.



3. Elija el servidor de CUCM y haga clic en **Go**.

### Service Activation

**Select Server**

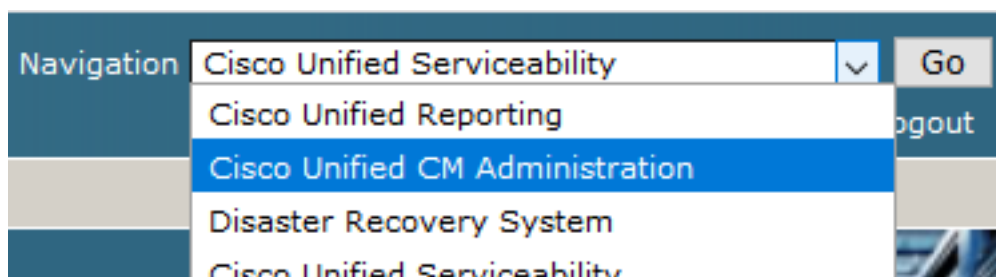
Server\*

4. Cheque **Cisco Certificate Authority Proxy Function** y haga clic en **Save** para activar el servicio. Haga clic en **Ok** para confirmar.

### 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. Asegúrese de que el servicio está activado y, a continuación, navegue hasta **Cisco Unified CM Administration**.



6. Después de iniciar sesión correctamente en la administración de CUCM, vaya a **System >**

Security > Phone Security Profile para crear un perfil de seguridad de dispositivo para el dispositivo del agente.

The screenshot shows the Cisco Unified CM Administration web interface. At the top, the Cisco logo and the text "Cisco Unified CM Administration For Cisco Unified Communications Solutions" are visible. Below the header is a navigation bar with several menu items: "System", "Call Routing", "Media Resources", "Advanced Features", and "Devices". The "System" menu is expanded, showing a list of sub-items. The "Security" item is highlighted with a red box. A secondary menu is open for "Security", showing options like "Certificate", "Phone Security Profile", "SIP Trunk Security Profile", and "CUMA Server Security Profile". The "Phone Security Profile" option is also highlighted with a red box. The background of the page shows a blurred view of a configuration page with some text like "device is configured. The", "Paging is not configur", and "Administration".

7. Busque los perfiles de seguridad correspondientes al tipo de dispositivo del agente. En este

ejemplo, se utiliza un teléfono basado en software, así que elija Cisco Unified Client Services Framework - Standard SIP Non-Secure Profile . Haga clic en Copy para copiar este perfil.

Phone Security Profile (1 - 1 of 1)		Rows per Page	
Find Phone Security Profile where	Name contains client	50	
<input type="checkbox"/>	Name	Description	Copy
	Cisco Unified Client Services Framework - Standard SIP Non-Secure Profile	Cisco Unified Client Services Framework - Standard SIP Non-Secure Profile	

8. Cambie el nombre del perfil a Cisco Unified Client Services Framework - Secure Profile, cambie los parámetros como se muestra en esta imagen y haga clic en Save en la parte superior izquierda de la página.

System Call Routing Media Resources Advanced Features Device Application User

### Phone Security Profile Configuration

Save Delete Copy Reset Apply Config Add New

**Status**

**i** Add successful

**Phone Security Profile Information**

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

Name\* Cisco Unified Client Services Framework - Secure Profile  
Description Cisco Unified Client Services Framework - Secure Profile  
Device Security Mode Encrypted  
Transport Type\* TLS

TFTP Encrypted Config  
 Enable OAuth Authentication

**Phone Security Profile CAPF Information**

Authentication Mode\* By Null String  
Key Order\* RSA Only  
RSA Key Size (Bits)\* 2048  
EC Key Size (Bits) < None >

Note: These fields are related to the CAPF Information settings on the Phone Configuration page.

**Parameters used in Phone**

SIP Phone Port\* 5061

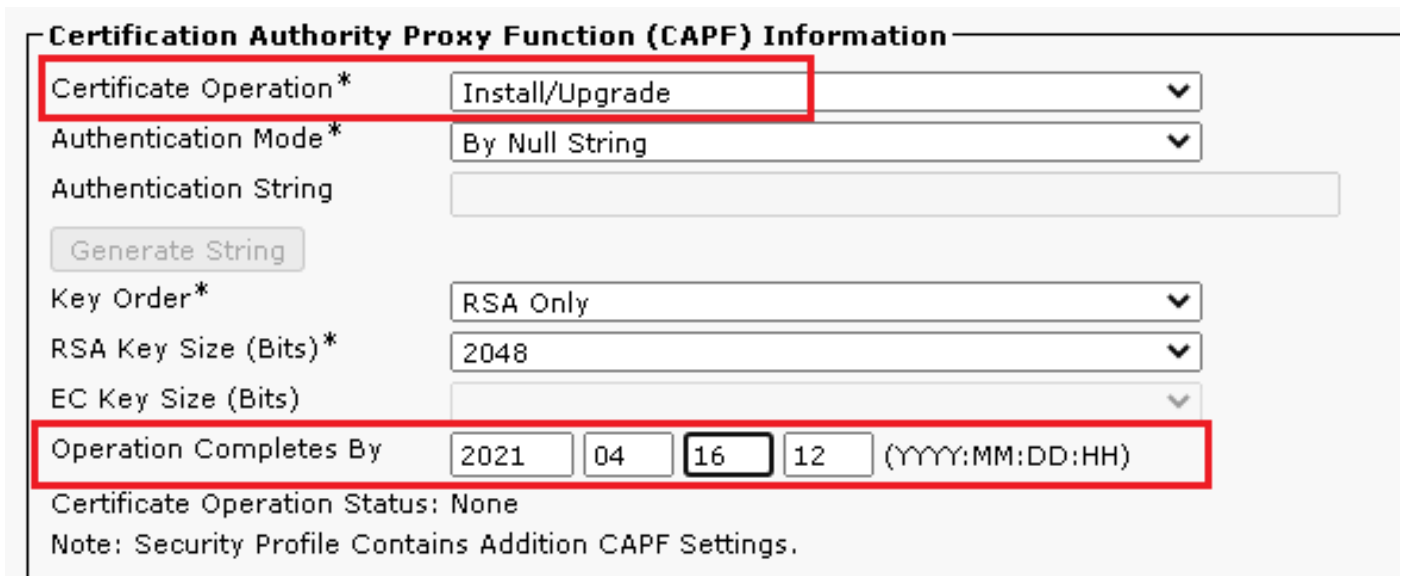
Save Delete Copy Reset Apply Config Add New

9. Después de crear correctamente el perfil de dispositivo de teléfono, vaya a Device > Phone.

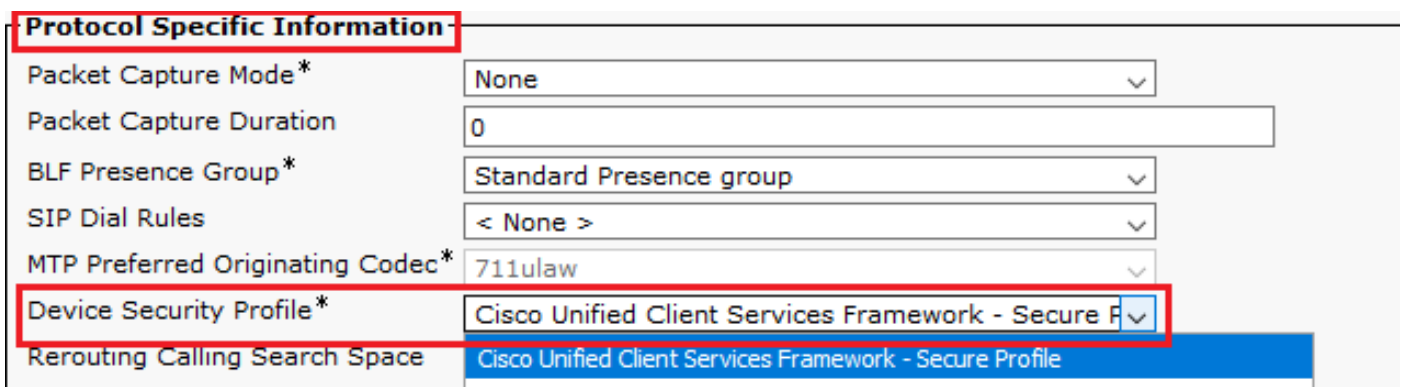


10. Haga clic en Find para enumerar todos los teléfonos disponibles, haga clic en teléfono del agente.

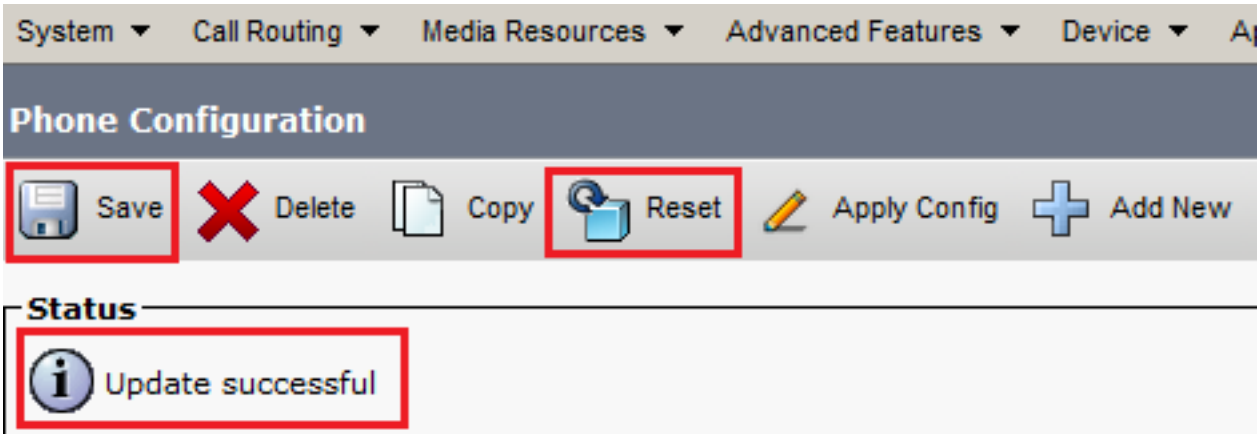
11. Se abre la página Configuración del teléfono del agente. Buscar Certification Authority Proxy Function (CAPF) Information sección. Para instalar LSC, configure Certificate Operation a Install/Upgrade y Operation Completes by en cualquier fecha futura.



12. Buscar Protocol Specific Information sección. Cambiar Device Security Profile a Cisco Unified Client Services Framework – Secure Profile.

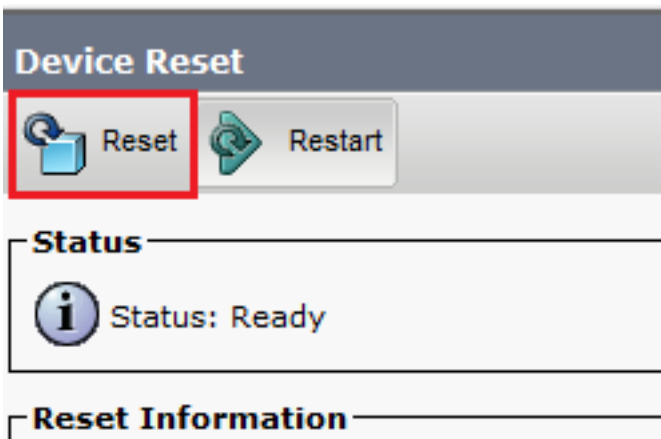


13. Haga clic en **Save** en la parte superior izquierda de la página. Asegúrese de que los cambios se han guardado correctamente y haga clic en **Reset**.



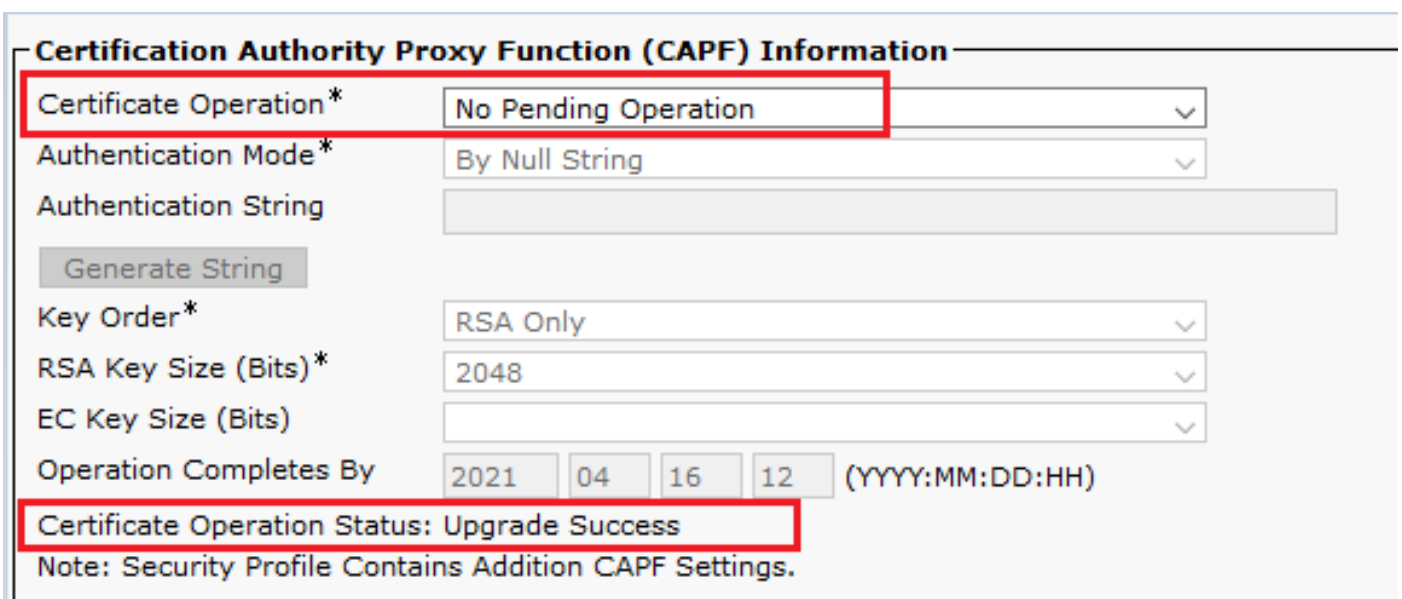
The screenshot shows the top navigation bar with tabs for System, Call Routing, Media Resources, Advanced Features, Device, and Applications. Below this is the 'Phone Configuration' section. A toolbar contains several icons: a floppy disk for 'Save', a red 'X' for 'Delete', a document for 'Copy', a circular arrow for 'Reset', a pencil for 'Apply Config', and a plus sign for 'Add New'. The 'Save' and 'Reset' buttons are highlighted with red boxes. Below the toolbar is a 'Status' section with a message icon and the text 'Update successful', which is also highlighted with a red box.

14. Se abre una ventana emergente, haga clic en **Reset** para confirmar la acción.



The screenshot shows a 'Device Reset' dialog box. It has a title bar and two buttons: 'Reset' and 'Restart'. The 'Reset' button is highlighted with a red box. Below the buttons is a 'Status' section with a message icon and the text 'Status: Ready'. At the bottom is a 'Reset Information' section.

15. Una vez que el dispositivo agente se registre de nuevo en CUCM, actualice la página actual y verifique que el LSC se haya instalado correctamente. Cheque **Certification Authority Proxy Function (CAPF) Information** sección, **Certificate Operation** se debe establecer en **No Pending Operation**, y **Certificate Operation Status** se establece en **Upgrade Success**.



The screenshot shows the 'Certification Authority Proxy Function (CAPF) Information' section. It contains several fields and dropdown menus. The 'Certificate Operation\*' field is set to 'No Pending Operation' and is highlighted with a red box. Other fields include 'Authentication Mode\*' (By Null String), 'Authentication String' (with a 'Generate String' button), 'Key Order\*' (RSA Only), 'RSA Key Size (Bits)\*' (2048), and 'EC Key Size (Bits)'. The 'Operation Completes By' field is set to '2021 04 16 12 (YYYY:MM:DD:HH)'. At the bottom, the 'Certificate Operation Status: Upgrade Success' is highlighted with a red box. A note below states: 'Note: Security Profile Contains Addition CAPF Settings.'

16. Consulte Pasos. 7-13 para proteger otros dispositivos de agentes que desee utilizar para proteger SIP con CUCM.

## Verificación

Para validar que la señalización SIP está asegurada correctamente, siga estos pasos:

1. Abra la sesión SSH en vCUBE, ejecute el comando `show sip-ua connections tcp tls detail`, y confirme que no hay ninguna conexión TLS establecida actualmente con CVP (198.18.133.13).

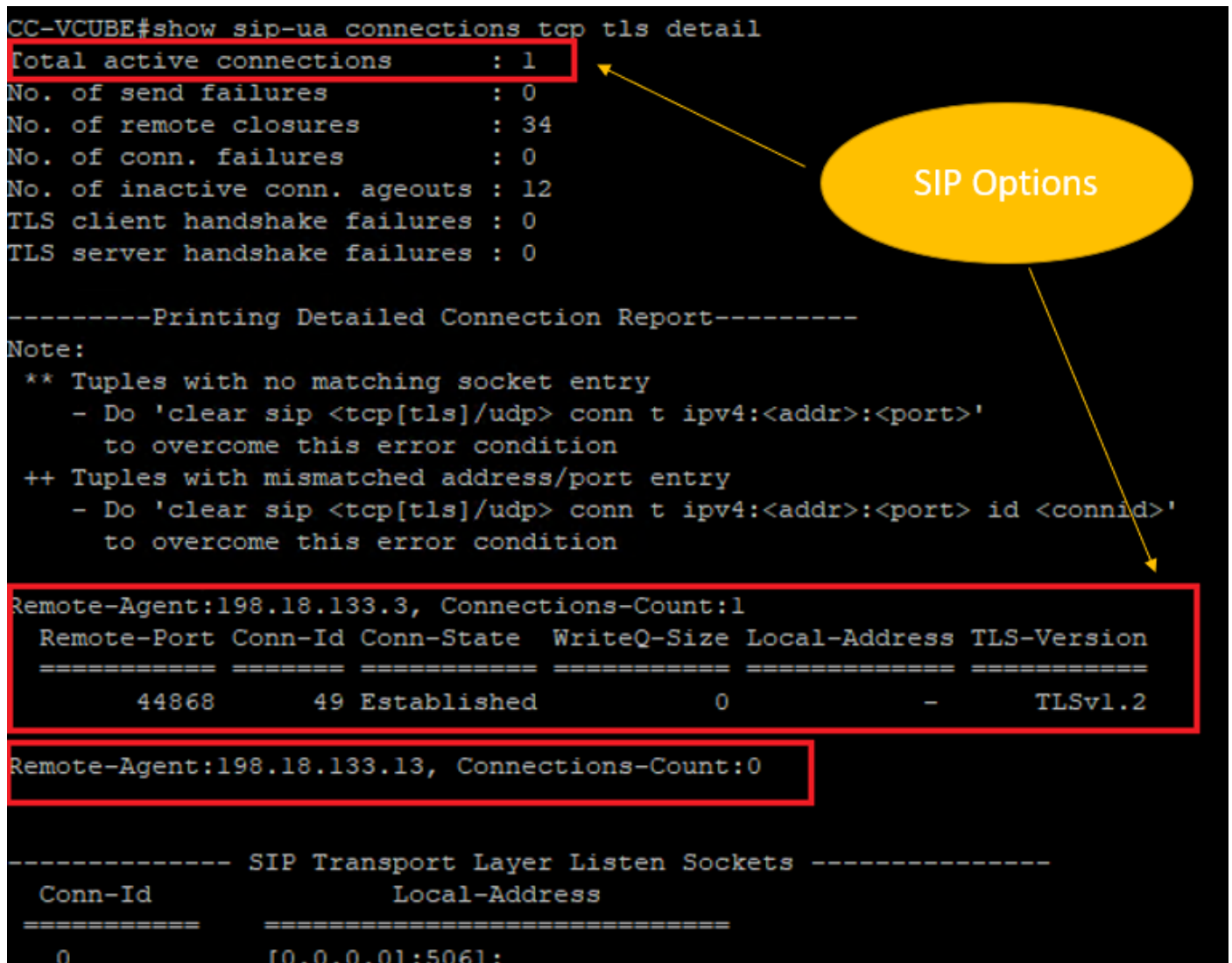
```
CC-VCUBE#show sip-ua connections tcp tls detail
Total active connections      : 1
No. of send failures         : 0
No. of remote closures       : 34
No. of conn. failures        : 0
No. of inactive conn. ageouts : 12
TLS client handshake failures : 0
TLS server handshake failures : 0

-----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:** En este momento, solo se ha activado una sesión TLS activa con CUCM para las opciones SIP en CUCM (198.18.133.3). Si no están activadas las opciones SIP, no existe ninguna conexión SIP TLS.

2. Inicie sesión en CVP e inicie Wireshark.
3. Realice una llamada de prueba al número del centro de contacto.
4. Navegue hasta la sesión de CVP; en Wireshark, ejecute este filtro para verificar la señalización 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

**Verifique:** ¿Está establecida la conexión SIP sobre TLS? Si la respuesta es sí, la salida confirma que las señales SIP entre CVP y CUBE son seguras.

5. Compruebe la conexión SIP TLS entre CVP y CVB. En la misma sesión de Wireshark, ejecute este 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

**Verifique:** ¿Está establecida la conexión SIP sobre TLS? Si la respuesta es sí, la salida confirma que las señales SIP entre CVP y CVB están aseguradas.

6. También puede verificar la conexión SIP TLS con CVP desde CUBE. Navegue hasta la sesión SSH de vCUBE y ejecute este comando para verificar las señales SIP seguras:

```
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

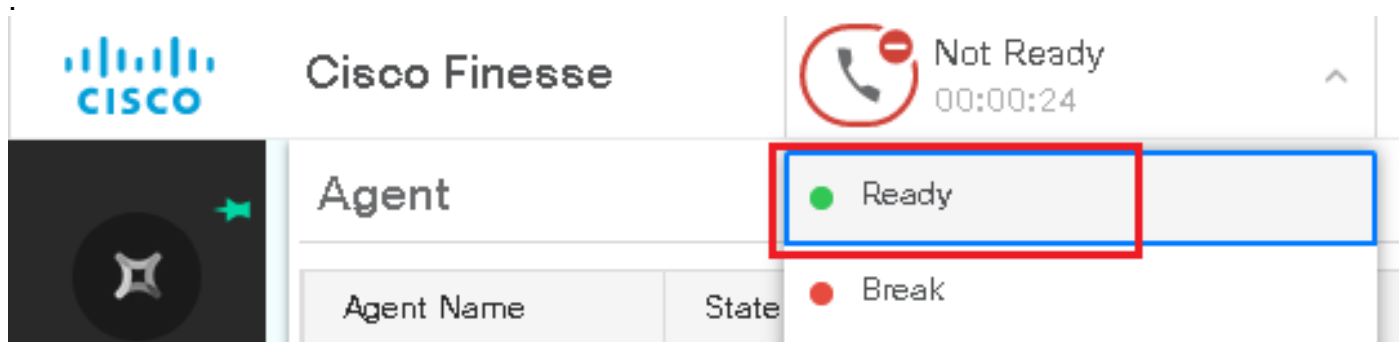
Remote-Agent:198.18.133.13, Connections-Count:1
  Remote-Port Conn-Id Conn-State WriteQ-Size Local-Address TLS-Version
  =====
      5061      3 Established      0      -      TLSv1.2

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

**Compruebe:** ¿Está establecida la conexión SIP sobre TLS con CVP? Si la respuesta es sí, la salida confirma que las señales SIP entre CVP y CUBE son seguras.

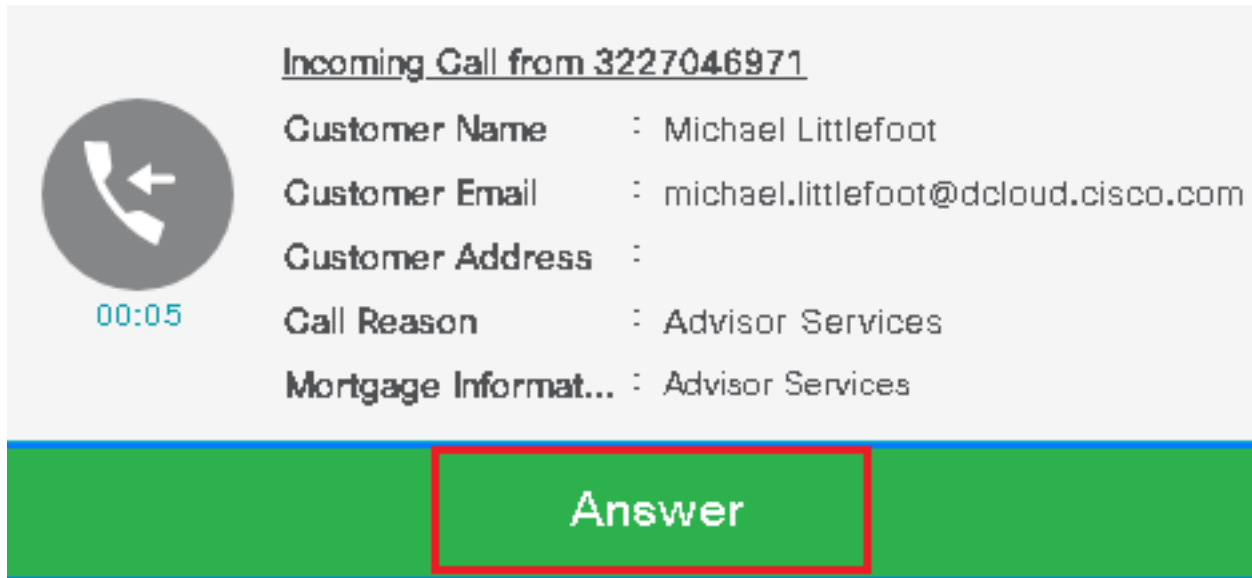
7. En este momento, la llamada está activa y se oye Música en espera (MOH), ya que no hay ningún agente disponible para contestar la llamada.

8. Haga que el agente esté disponible para contestar la llamada.





9. El agente se reserva y la llamada se dirige a él. Haga clic en Answer para contestar la llamada.



**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

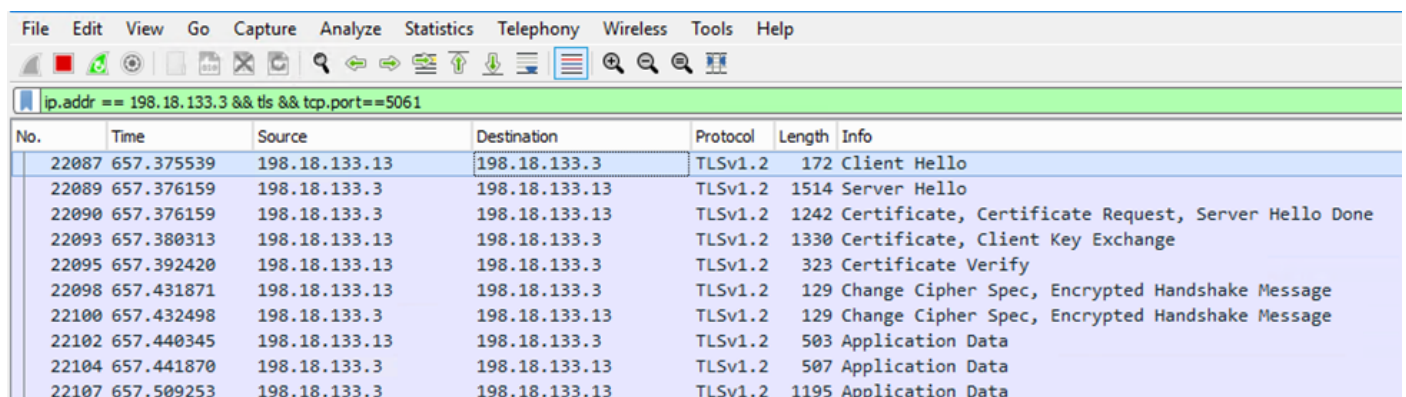
00:05

**Answer**

10. La llamada se conecta con el agente.

11. Para verificar las señales SIP entre CVP y CUCM, navegue hasta la sesión de CVP y ejecute este filtro en 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

**Comprobar:** ¿todas las comunicaciones SIP con CUCM (198.18.133.3) sobre TLS? Si la respuesta es sí, la salida confirma que las señales SIP entre CVP y CUCM son seguras.

## Troubleshoot

Si no se establece TLS, ejecute estos comandos en CUBE para habilitar debug TLS para resolver problemas:

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

## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).