

Configurar a sinalização SIP segura no Contact Center Enterprise

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Tarefa 1. Configuração segura do CUBE](#)

[Tarefa 2. Configuração segura do CVP](#)

[Tarefa 3. Configuração segura do CVB](#)

[Tarefa 4. Configuração segura do CUCM](#)

[Definir o modo de segurança do CUCM para o modo misto](#)

[Configurar perfis de segurança de tronco SIP para CUBE e CVP](#)

[Associar perfis de segurança de tronco SIP aos respectivos troncos SIP](#)

[Comunicação segura de dispositivos de agentes com o CUCM](#)

[Verificar](#)

[Troubleshoot](#)

Introduction

Este documento descreve como proteger a sinalização do Session Initiation Protocol (SIP) no fluxo de chamadas abrangente do Contact Center Enterprise (CCE).

Prerequisites

A geração e a importação de certificados estão fora do escopo deste documento, portanto, os certificados para o Cisco Unified Communication Manager (CUCM), o servidor de chamadas do Customer Voice Portal (CVP), o Cisco Virtual Voice Browser (CVB) e o Cisco Unified Border Element (CUBE) devem ser criados e importados para os respectivos componentes. Se você usar certificados autoassinados, a troca de certificados deve ser feita entre componentes diferentes.

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- CCE
- CVP
- CUBO
- CUCM
- CVB

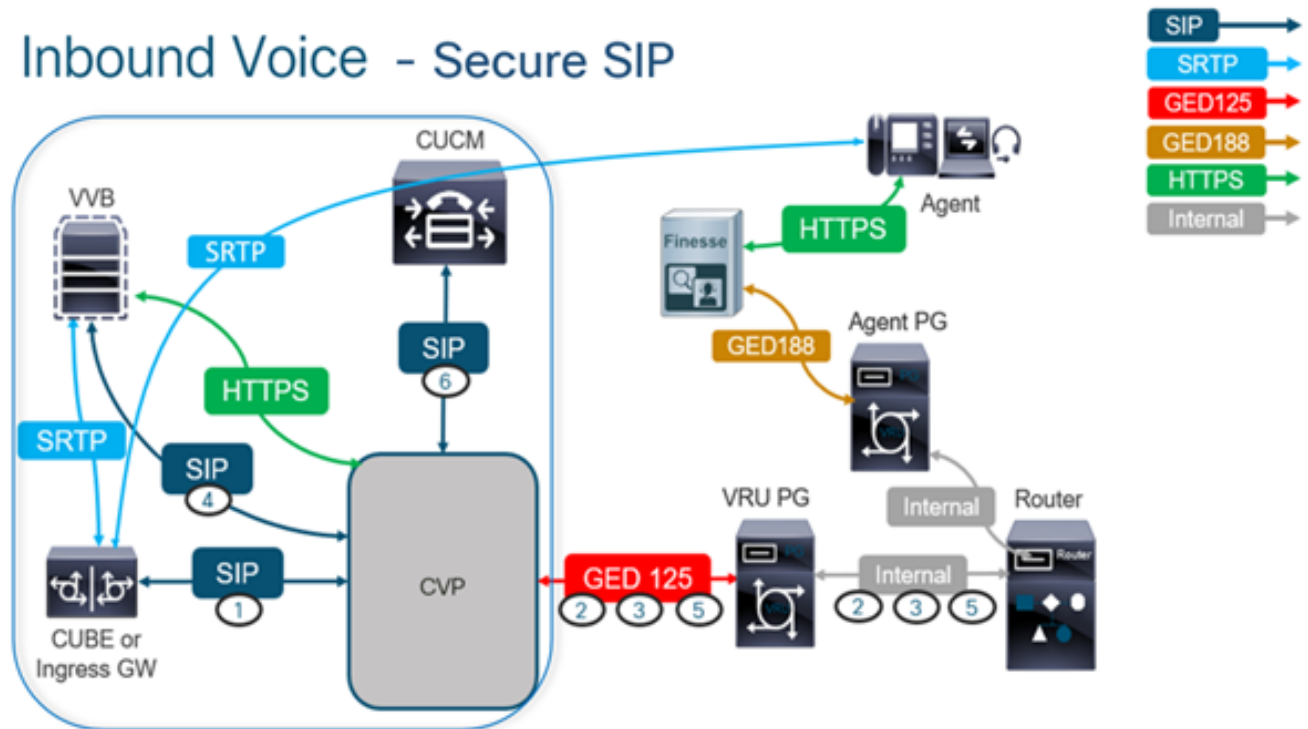
Componentes Utilizados

As informações neste documento são baseadas no Package Contact Center Enterprise (PCCE), CVP, CVB e CUCM versão 12.6, mas também se aplicam às versões anteriores.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

O próximo diagrama mostra os componentes envolvidos na sinalização SIP no fluxo de chamadas abrangente da central de contatos. Quando uma chamada de voz chega ao sistema, primeiro vem através do gateway de entrada ou CUBE, portanto, inicie configurações SIP seguras no CUBE. Em seguida, configure CVP, CVB e CUCM.



Tarefa 1. Configuração segura do CUBE

Nesta tarefa, configure o CUBE para proteger as mensagens do protocolo SIP.

Configurações necessárias:

- Configurar um ponto de confiança padrão para o agente de usuário (UA) do SIP
- Modifique os correspondentes de discagem para usar o protocolo TLS

Etapas:

1. Abra a sessão Secure Shell (SSH) para o CUBE.
2. Execute esses comandos para que a pilha SIP use o certificado de Autoridade de certificação (CA) do CUBE. O CUBE estabelece uma conexão SIP TLS de/para 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. Execute estes comandos para ativar o TLS no peer de discagem de saída para o CVP.

Neste exemplo, a tag de peer de discagem 6000 é usada para rotear chamadas para o 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)#
```

Tarefa 2. Configuração segura do CVP

Nesta tarefa, configure o servidor de chamadas CVP para proteger as mensagens de protocolo SIP (SIP TLS).

Etapas:

1. Efetue login no UCCX Web Administration.
2. Navegue até **Call Settings > Route Settings > SIP Server Group**.

Route Settings

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

Properties

Com base em suas configurações, você tem grupos de servidores SIP configurados para CUCM, CVB e CUBE. Você precisa definir portas SIP seguras como 5061 para todas elas. Neste exemplo, estes grupos de servidores SIP são usados:

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

3. Clique em **cucm1.dcloud.cisco.com** e depois no **Members**, que mostra os detalhes da Configuração do grupo de servidores SIP. Configure **SecurePort** para 5061 e clique em **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. Clique em vvb1.dcloud.cisco.com e depois no **Members** guia. Definir SecurePort como 5061 e clique em 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

Tarefa 3. Configuração segura do CVB

Nesta tarefa, configure o CVB para proteger as mensagens de protocolo SIP (SIP TLS).

Etapas:

1. Efetue login no **Cisco VVB Administration**
2. Navegue até **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. No **Security Parameters**, escolha **Enable** para TLS(SIP). Manter **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. Clique em Update. Clique em ok quando solicitado a reiniciar o mecanismo CVB.

The screenshot shows the Cisco VVB 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 visible.

5. Essas alterações exigem uma reinicialização do mecanismo Cisco VB. Para reiniciar o mecanismo VVB, navegue até Cisco VVB Serviceability em seguida, clique em Go.

The screenshot shows the 'Navigation' menu in the Cisco VVB Administration interface. The menu is open, showing a list of options: 'Cisco VVB Administration', 'Cisco VVB Administration', 'Cisco Unified Serviceability', 'Cisco VVB Serviceability', and 'Cisco Unified OS Administration'. The 'Cisco VVB Serviceability' option is highlighted in blue. A 'Go' button is visible to the right of the menu.

6. Navegue até Tools > Control Center – Network Services.

The screenshot shows the 'Tools' menu in the Cisco VVB Administration interface. The menu is open, showing a list of options: 'Control Center - Network Services' and 'Performance Configuration and Logging'. The 'Control Center - Network Services' option is highlighted in blue.

7. Escolher Engine e clique em Restart.

Control Center - Network Services



Status

 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

Tarefa 4. Configuração segura do CUCM

Para proteger as mensagens SIP no CUCM, execute as próximas configurações:

- Definir o modo de segurança do CUCM para o modo misto
- Configurar perfis de segurança de tronco SIP para CUBE e CVP
- Associar perfis de segurança de tronco SIP aos respectivos troncos SIP
- Comunicação segura de dispositivos de agentes com o CUCM

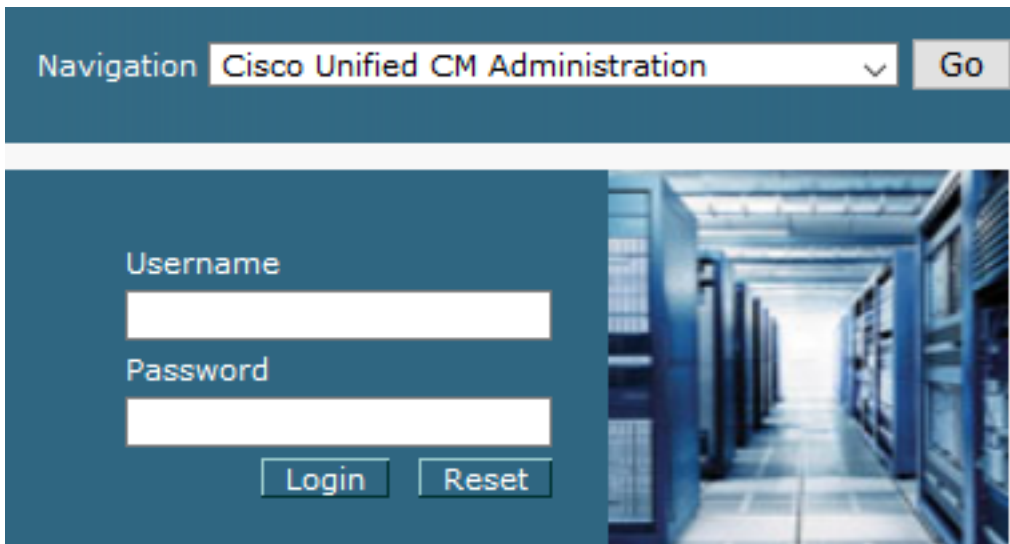
Definir o modo de segurança do CUCM para o modo misto

O CUCM suporta dois modos de segurança:

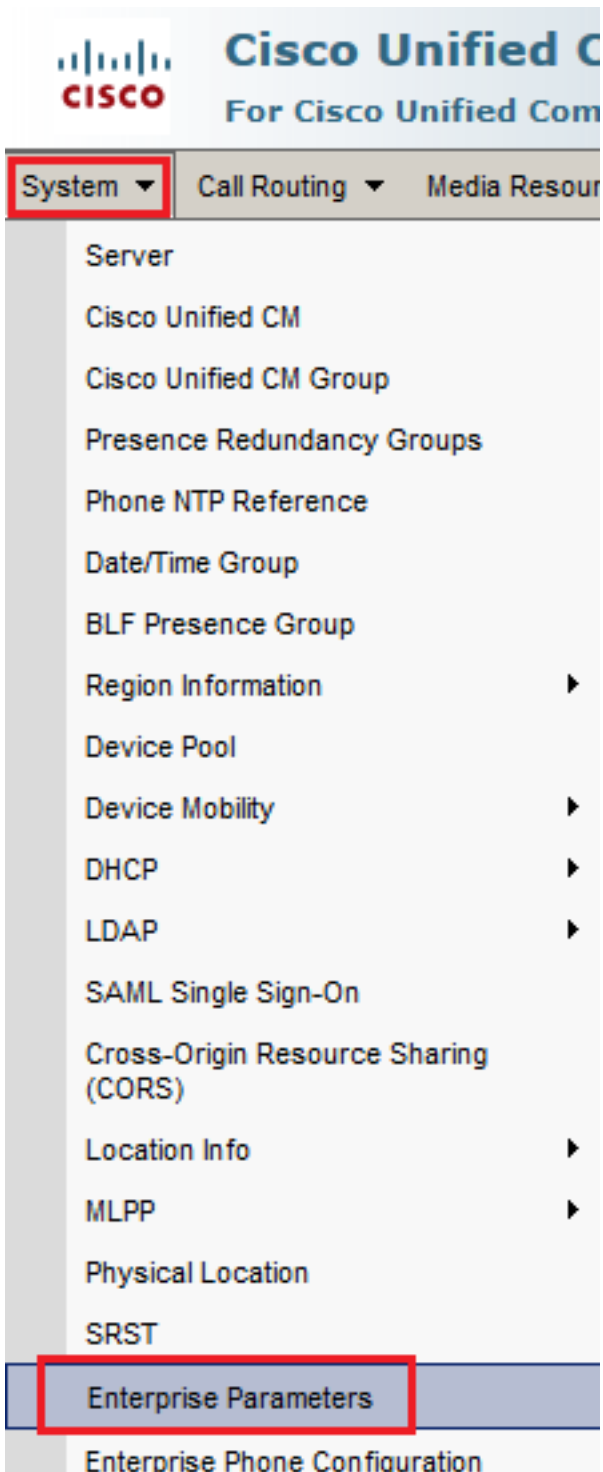
- Modo não seguro (modo padrão)
- Modo misto (modo seguro)

Etapas:

1. Para definir o modo de segurança como Mixed Mode, faça login no Cisco Unified CM Administration interface.



2. Depois de fazer login com êxito no CUCM, navegue até [System > Enterprise Parameters](#).



3. Abaixo do Security Parameters Seção, verifique se Cluster Security Mode está definido como 0.

Security Parameters	
Cluster Security Mode *	0
Cluster SIPOAuth Mode *	Disabled

4. Se o Modo de Segurança de Cluster estiver definido como 0, isso significa que o modo de segurança de cluster está definido como não seguro. Você precisa ativar o modo misto a partir do CLI.
5. Abra uma sessão SSH para o CUCM.
6. Depois de fazer login com êxito no CUCM via SSH, execute este comando: `utils ctl set-cluster`

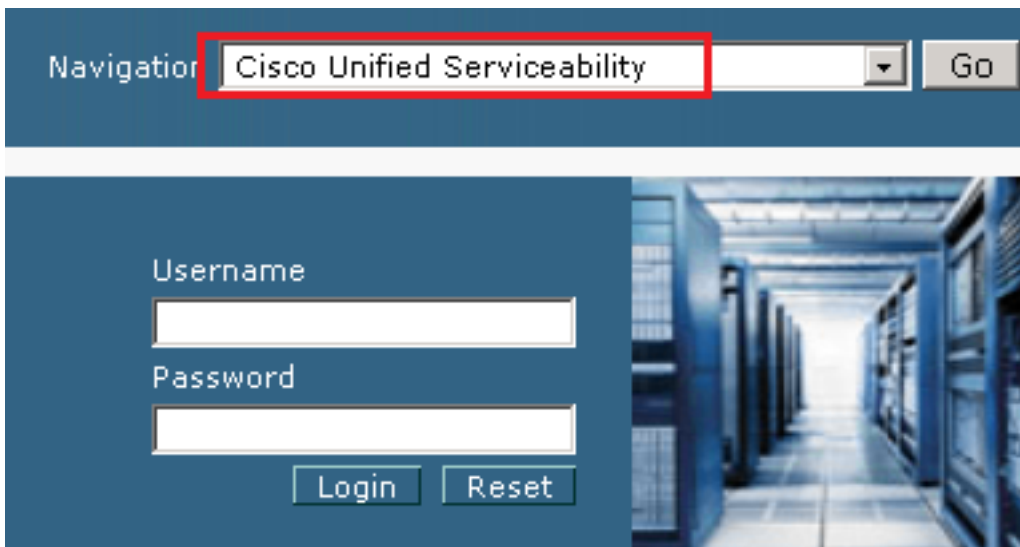
mixed-mode

7. Tipo y e clique em **Enter** quando solicitado. Este comando define o modo de segurança de cluster para o modo misto.

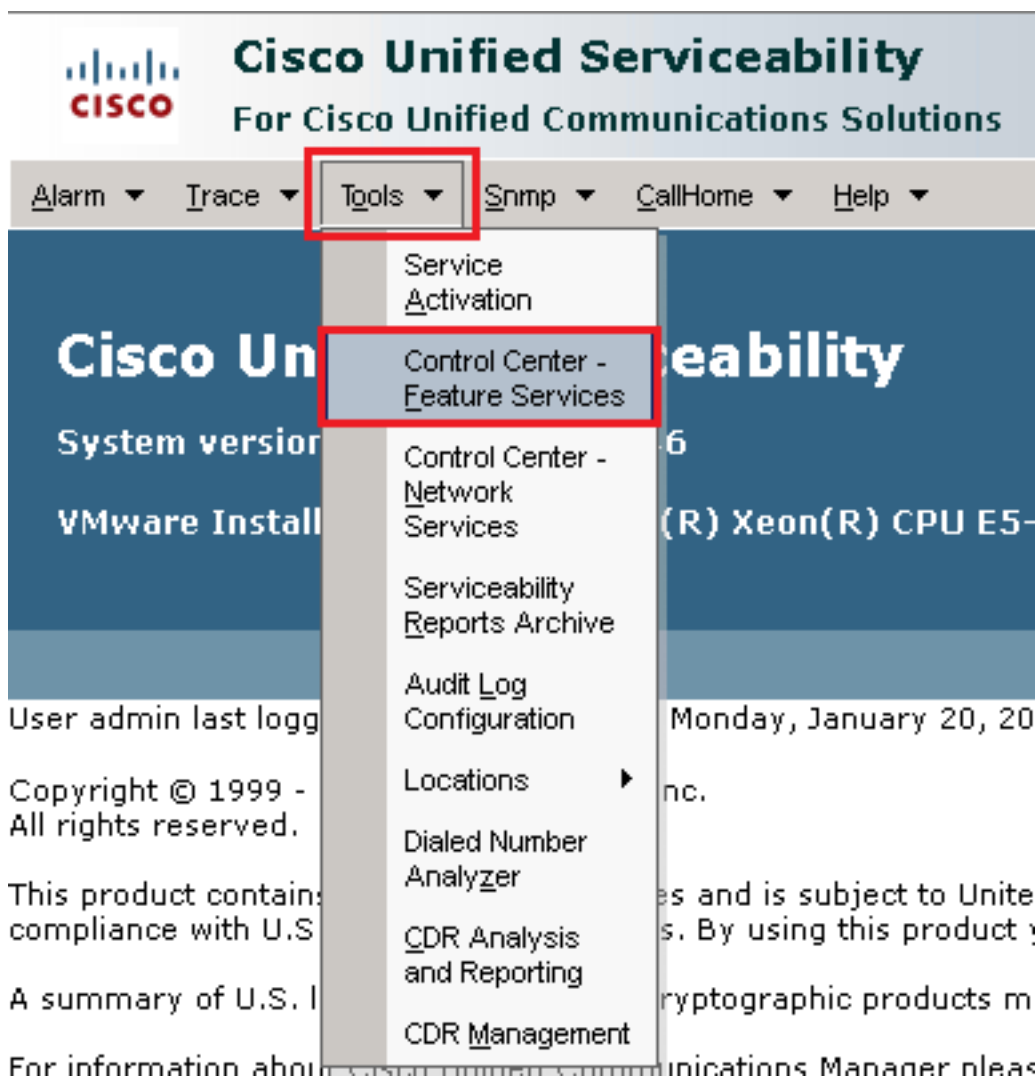
```
admin:utils ctl set-cluster mixed-mode
This operation will set the cluster to Mixed mode. Auto-registration is enabled on at least one CM node. Do you want to continue? (y/n): y
Moving Cluster to Mixed Mode
Cluster set to Mixed Mode
Please restart Cisco CallManager service and Cisco CTIManager services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

8. Para que as alterações entrem em vigor, reinicie Cisco CallManager e Cisco CTIManager serviços.

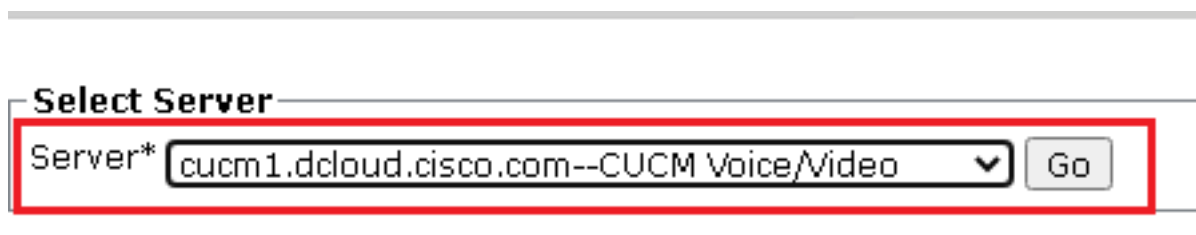
9. Para reiniciar os serviços, navegue e faça login no Cisco Unified Serviceability.



10. Depois de fazer o login com êxito, navegue até **Tools > Control Center – Feature Services**.



11. Escolha o servidor e clique em Go.



12. Abaixo dos serviços CM, escolha Cisco CallManager em seguida, clique em Restart na parte superior da 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 a mensagem pop-up e clique em **OK**. Aguarde até que o serviço seja reiniciado com êxito.

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. Após uma reinicialização bem-sucedida do Cisco CallManager, escolha Cisco CTIManager em seguida, clique em **Restart** para reiniciar Cisco CTIManager serviço.

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 a mensagem pop-up e clique em **OK**. Aguarde até que o serviço seja reiniciado com êxito.

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.



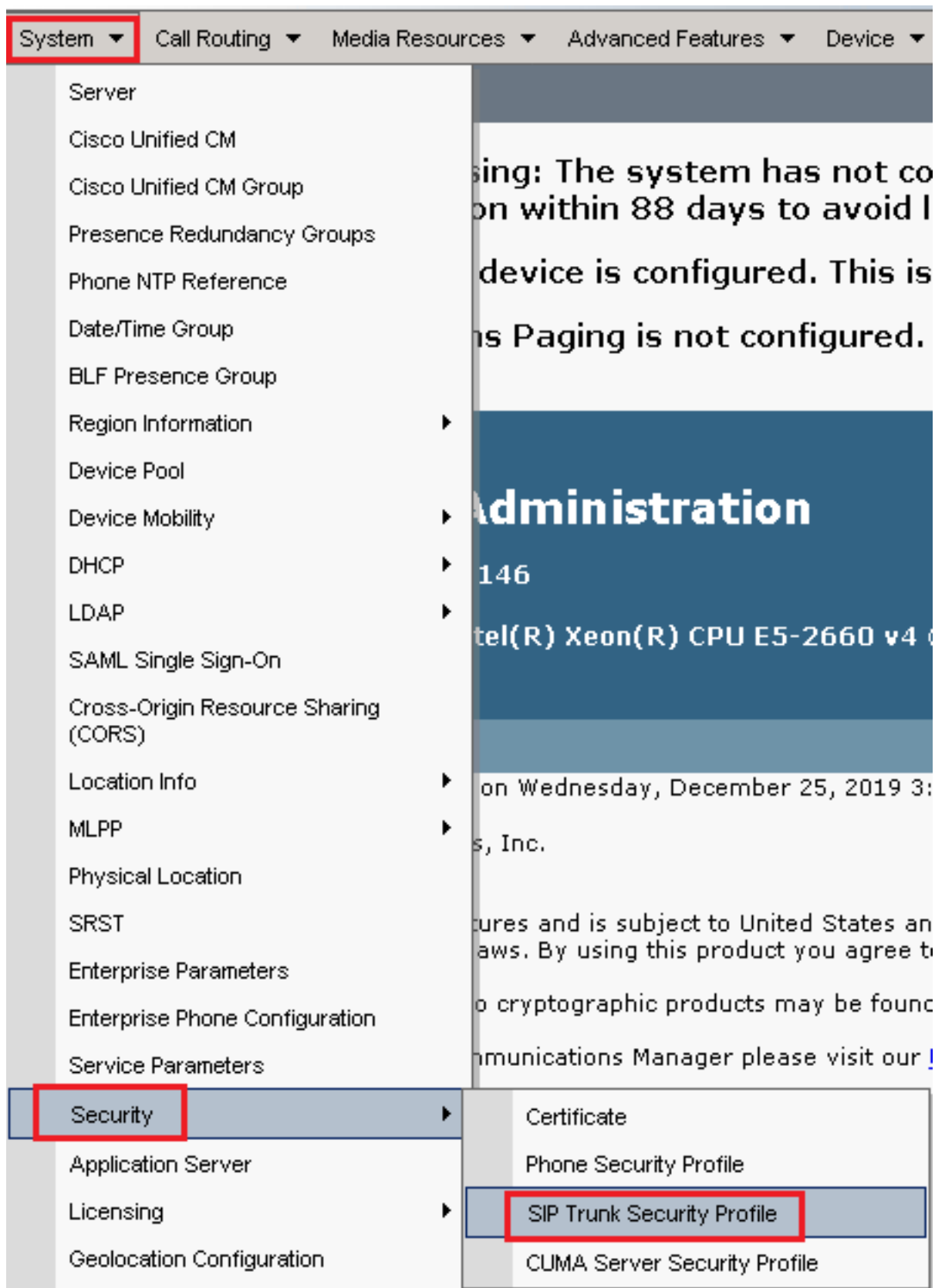
16. Depois que os serviços forem reiniciados com êxito, verifique se o modo de segurança do cluster está definido como modo misto, navegue até a administração do CUCM conforme explicado na Etapa 5. em seguida, verifique o **Cluster Security Mode**. Agora ele deve ser definido como 1.

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

Configurar perfis de segurança de tronco SIP para CUBE e CVP

Etapas:

1. Efetue login no CUCM administration interface.
2. Após o login bem-sucedido no CUCM, navegue até System > Security > SIP Trunk Security Profile para criar um perfil de segurança de dispositivo para o CUBE.



3. Na parte superior esquerda, clique em Add New para adicionar um novo perfil.

Find and List SIP Trunk Security Profiles

 Add New  Select All  Clear All  Delete Selected



4. Configurar SIP Trunk Security Profile como mostrado nesta imagem, clique em **Save** na parte inferior esquerda da página para **Save** o seu

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
<input type="checkbox"/> Enable Application level authorization	
<input type="checkbox"/> Accept presence subscription	
<input type="checkbox"/> Accept out-of-dialog refer**	
<input type="checkbox"/> Accept unsolicited notification	
<input type="checkbox"/> Accept replaces header	
<input type="checkbox"/> Transmit security status	
<input type="checkbox"/> Allow charging header	
SIP V.150 Outbound SDP Offer Filtering*	Use Default Filter

5. Certifique-se de definir o `Secure Certificate Subject` or `Subject Alternate Name` para o Nome comum (CN) do certificado CUBE, pois ele deve corresponder.

6. Clique em `Copy` e altere o Name para `SecureSipTLSforCvp` e o `Secure Certificate Subject` ao CN do certificado de servidor de chamada CVP, pois ele deve corresponder. Clique em `Save` botão.

Status

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

SIP Trunk Security Profile Information

Name*

Description

Device Security Mode

Incoming Transport Type*

Outgoing Transport Type

Enable Digest Authentication

Nonce Validity Time (mins)*

Secure Certificate Subject or Subject Alternate Name

Incoming Port*

Enable Application level authorization

Accept presence subscription

Accept out-of-dialog refer**

Accept unsolicited notification

Accept replaces header

Transmit security status

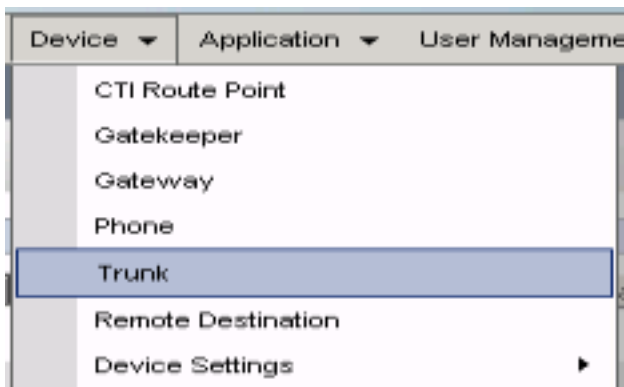
Allow charging header

SIP V.150 Outbound SDP Offer Filtering*

Associar perfis de segurança de tronco SIP aos respectivos troncos SIP

Etapas:

1. Na página Administração do CUCM, navegue até `Device > Trunk`.



2. Procure o tronco CUBE. Neste exemplo, o nome do tronco CUBE é vCube . Clique em 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. Clique em vCUBE para abrir a página de configuração do tronco vCUBE.

4. Role para baixo até SIP Information e altere a Destination Port para 5061.

5. alteram SIP Trunk Security Profile para SecureSIPTLSForCube.

SIP Information

Destination

Destination Address is an SRV

	Destination Address	Destination Address IPv6	Destination Port
1*	198.18.133.226		5061

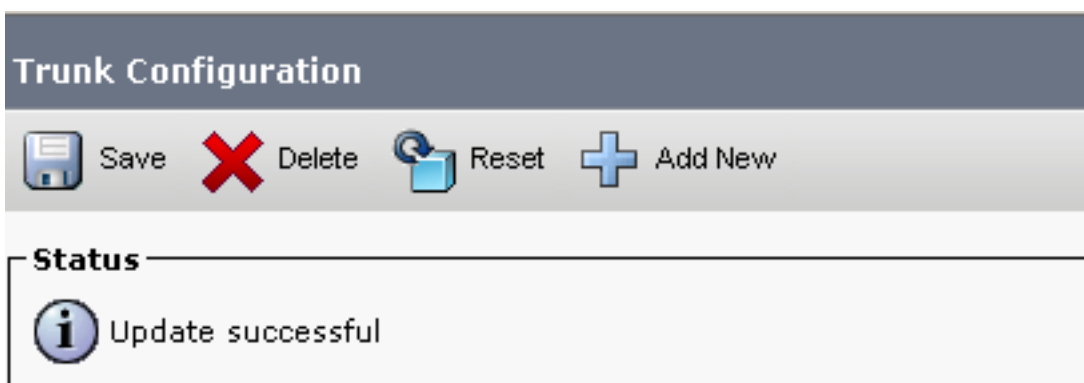
MTP Preferred Originating Codec* 711ulaw

BLF Presence Group* Standard Presence group

SIP Trunk Security Profile* SecureSIPTLSforCube

Rerouting Calling Search Space < None >




6. Clique em Save em seguida Rest para Save e aplicar alterações.



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. Navegue até **Device > Trunks** procure o tronco CVP. Neste exemplo, o nome do tronco CVP é **cvp-SIP-Trunk** . Clique em **Find**.

Trunks (1 - 1 of 1)				
Find Trunks where				
<input type="checkbox"/>	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






8. Clique em **CVP-SIP-Trunk** para abrir a página de configuração do tronco CVP.

9. Role para baixo até **SIP Information** e altere **Destination Port** para **5061** .

10. altere **SIP Trunk Security Profile** para **SecureSIPTLSForCvp**.

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

11. Clique em **Save** em seguida **Rest** para save e aplicar alterações.

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

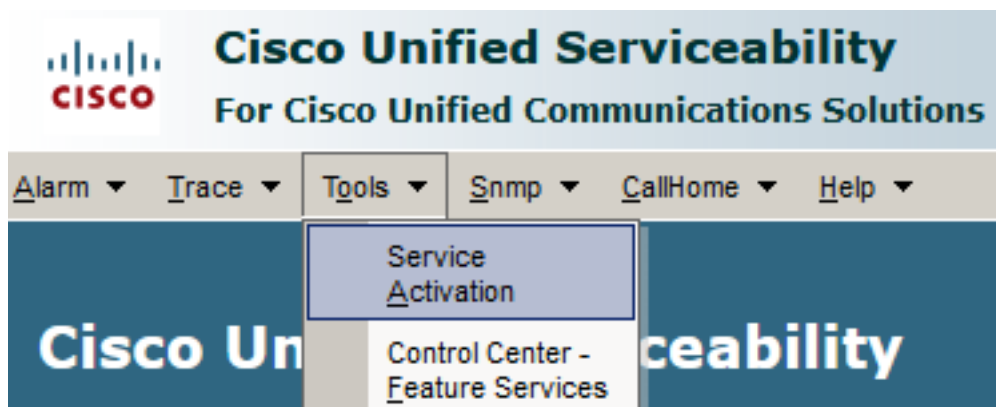
Comunicação segura de dispositivos de agentes com o CUCM

Para habilitar recursos de segurança para um dispositivo, você deve instalar um LSC (Locally

Significant Certificate) e atribuir um perfil de segurança a esse dispositivo. O LSC possui a chave pública para o ponto final, que é assinada pela chave privada CAPF (Certificate Authority Proxy Function). Por padrão, ele não é instalado nos telefones.

Etapas:

1. Efetue login no Cisco Unified Serviceability Interface.
2. Navegue até **Tools > Service Activation**.



3. Escolha o servidor CUCM e clique em **Go**.

Service Activation

Select Server

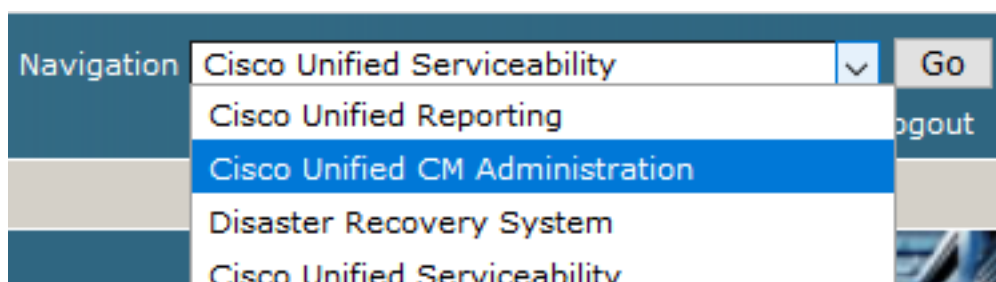
Server*

4. Verificar **Cisco Certificate Authority Proxy Function** e clique em **Save** para ativar o serviço. Clique em **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. Verifique se o serviço está ativado e navegue até **Cisco Unified CM Administration**.



6. Depois de fazer login com êxito na administração do CUCM, navegue para **System > Security > Phone Security Profile** para criar um perfil de segurança de dispositivo para o dispositivo do

agente.


The screenshot shows the Cisco Unified CM Administration web interface. At the top, the Cisco logo and the title "Cisco Unified CM Administration" are visible, along with the subtitle "For Cisco Unified Communications Solutions". Below the header is a navigation bar with several menu items: "System", "Call Routing", "Media Resources", "Advanced Features", and "Devices". The "System" menu is highlighted with a red box. A dropdown menu is open under "System", listing various configuration categories. The "Security" category is highlighted with a red box. A secondary dropdown menu is open under "Security", listing "Certificate", "Phone Security Profile", "SIP Trunk Security Profile", and "CUMA Server Security Profile". The "Phone Security Profile" option is highlighted with a red box. The main content area on the right is partially visible, showing a blue header with the word "Administration" and some text about device configuration and paging.

7. Localize os perfis de segurança de acordo com o tipo de dispositivo do seu agente. Neste exemplo, um softphone é usado, então escolha Cisco Unified Client Services Framework - Standard SIP

Non-Secure Profile . Clique em Copy  para copiar este perfil.

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. Renomear o perfil para Cisco Unified Client Services Framework - Secure Profile, altere os parâmetros conforme mostrado nesta imagem e clique em Save na parte superior esquerda da página.

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* 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 >

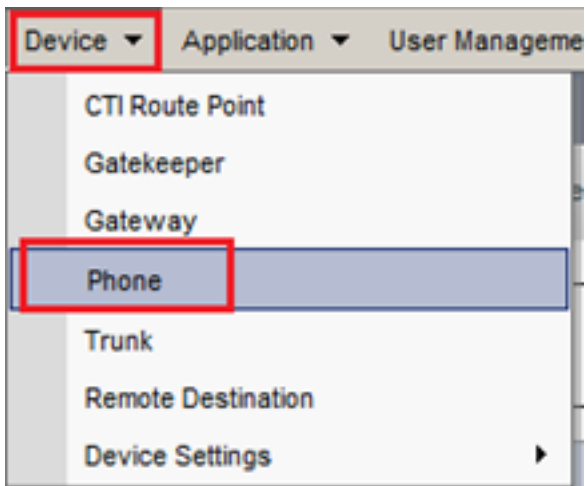
Note: These fields are related to the CAPF Information settings on the Phone Configuration page.

Parameters used in Phone

SIP Phone Port* 5061

Save Delete Copy Reset Apply Config Add New

9. Após a criação bem-sucedida do perfil do dispositivo telefônico, navegue até Device > Phone.



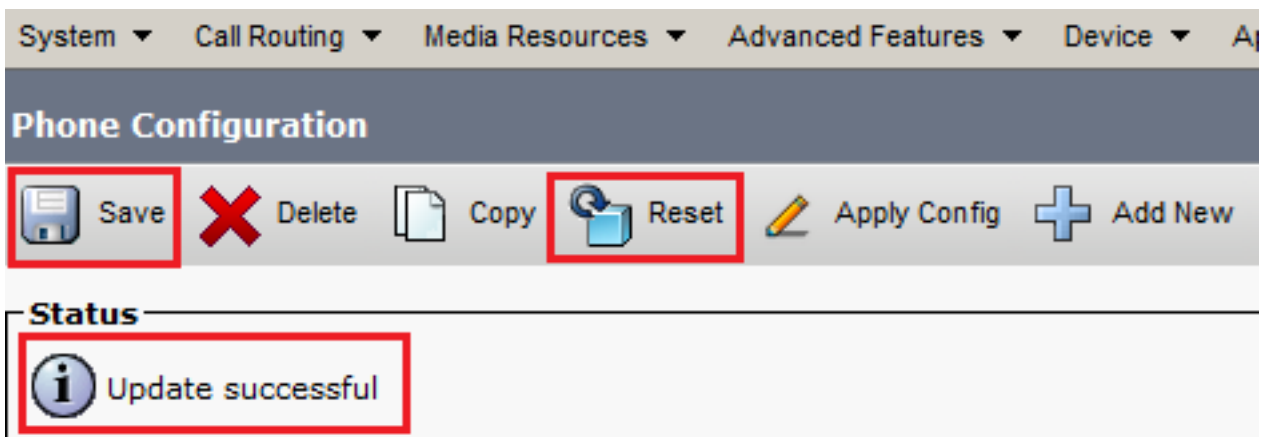
10. Clique em Find para listar todos os telefones disponíveis, clique em telefone do agente.
11. A página Configuração do telefone do agente é aberta. Localizar Certification Authority Proxy Function (CAPF) Information seção. Para instalar o LSC, configure Certificate Operation para Install/Upgrade e Operation Completes by para qualquer 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*' field is set to 'Install/Upgrade' and is highlighted with a red box. The 'Authentication Mode*' field is set to 'By Null String'. The 'Authentication String' field is empty, with a 'Generate String' button below it. The 'Key Order*' field is set to 'RSA Only'. The 'RSA Key Size (Bits)*' field is set to '2048'. The 'EC Key Size (Bits)' field 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 fields, it says 'Certificate Operation Status: None' and 'Note: Security Profile Contains Addition CAPF Settings.'

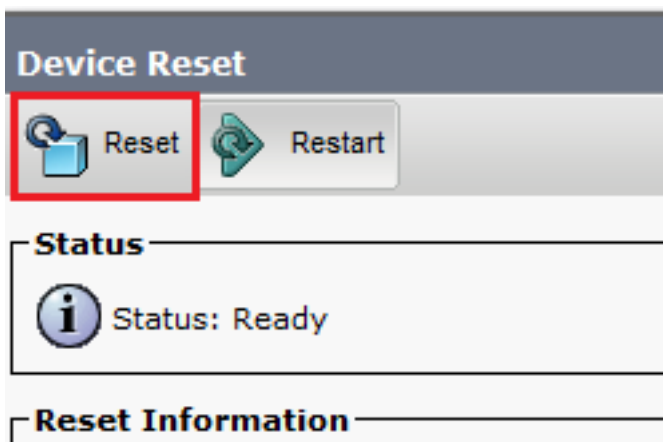
12. Localizar Protocol Specific Information seção. alteram Device Security Profile para Cisco Unified Client Services Framework – Secure Profile.

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

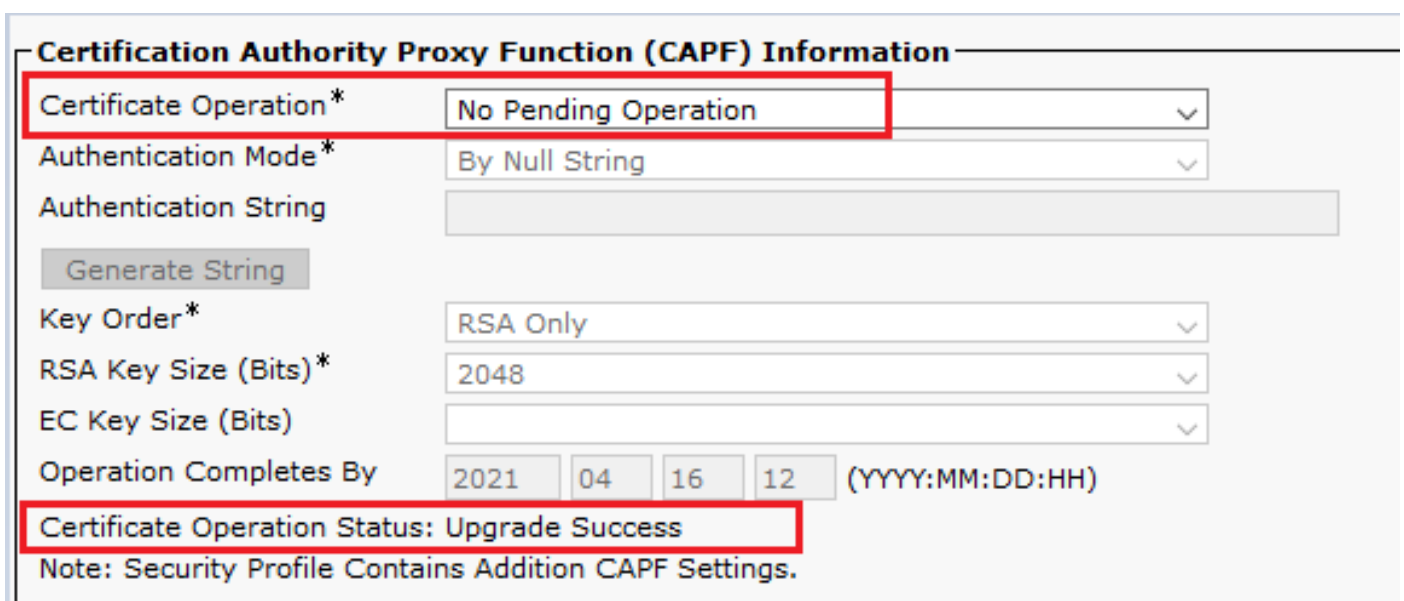
13. Clique em save na parte superior esquerda da página. Verifique se as alterações foram salvas com êxito e clique em Reset.



14. Uma janela pop-up será aberta. Clique em **Reset** para confirmar a ação.



15. Depois que o dispositivo do agente se registrar novamente no CUCM, atualize a página atual e verifique se o LSC foi instalado com êxito. Verificar **Certification Authority Proxy Function (CAPF) Information** seção, **Certificate Operation** deve ser definido como **No Pending Operation**, e **Certificate Operation Status** está definido como **Upgrade Success**.



16. Consulte as Etapas. 7-13 para proteger outros dispositivos de agentes que você deseja usar para proteger o SIP com o CUCM.

Verificar

Para validar se a sinalização SIP está protegida corretamente, execute estas etapas:

1. Abra a sessão SSH para o vCUBE, execute o comando `show sip-ua connections tcp tls detail` e confirme que não há conexão TLS estabelecida no momento com o CVP (198.18.133.13).

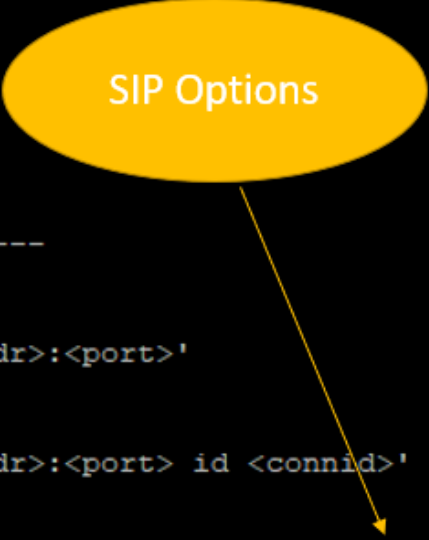
```
CC-VCUBE#show sip-ua connections tcp tls detail
Total active connections      : 1
No. of send failures         : 0
No. of remote closures       : 34
No. of conn. failures        : 0
No. of inactive conn. ageouts : 12
TLS client handshake failures : 0
TLS server handshake failures : 0

-----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:
```



Observação: neste momento, apenas uma sessão TLS ativa com CUCM, para opções SIP, está habilitada no CUCM (198.18.133.3). Se nenhuma opção SIP estiver habilitada, não haverá conexão SIP TLS.

2. Faça login no CVP e inicie o Wireshark.
3. Faça uma chamada de teste para o número da central de contatos.
4. Navegue para a sessão CVP; no Wireshark, execute este filtro para verificar a sinalização SIP com CUBE:
`ip.addr == 198.18.133.226 && tls && tcp.port==5061`

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

Verificar: Conexão SIP sobre TLS estabelecida? Se sim, a saída confirma que os sinais SIP entre o CVP e o CUBE estão protegidos.

5. Verifique a conexão SIP TLS entre o CVP e o CVB. Na mesma sessão do Wireshark, execute este filtro:

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

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

Verificar: Conexão SIP sobre TLS estabelecida? Se sim, a saída confirma que os sinais SIP entre o CVP e o CVB estão protegidos.

6. Você também pode verificar a conexão SIP TLS com o CVP a partir do CUBE. Navegue até a sessão vCUBE SSH e execute este comando para verificar os sinais sip seguros:

```
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

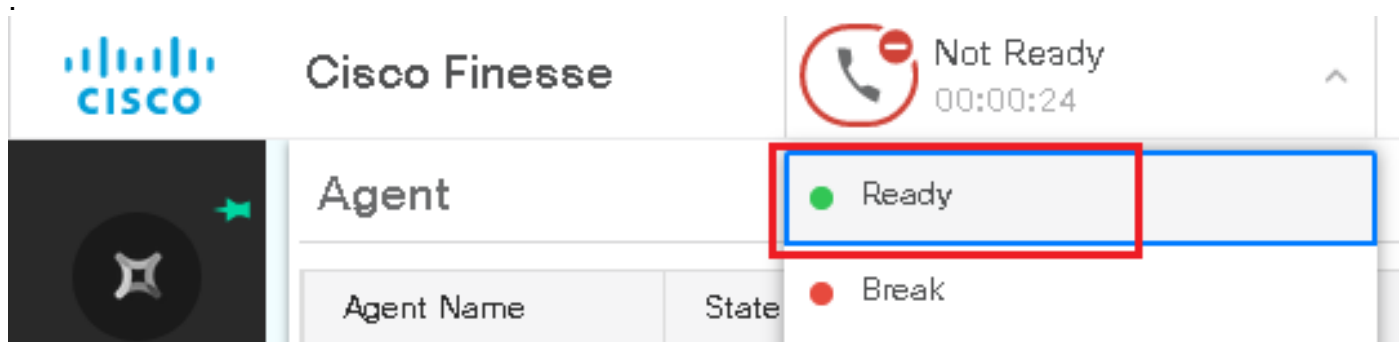
----- SIP Transport Layer Listen Sockets -----
  Conn-Id          Local-Address
  =====
      0            [0.0.0.0]:5061:

```

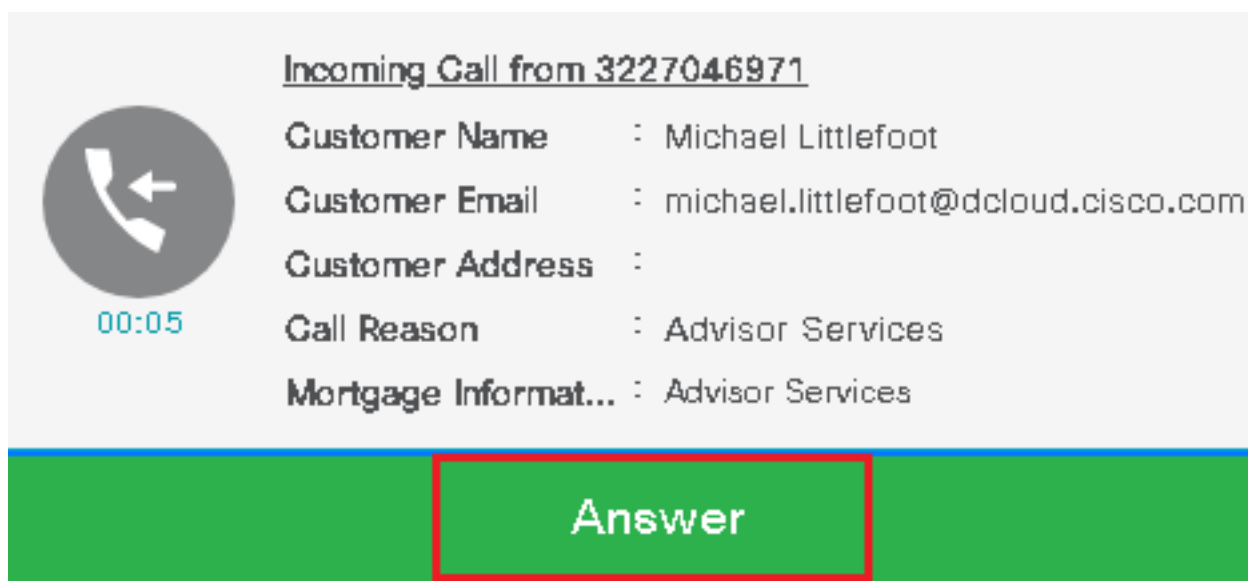
Verificar: a conexão SIP sobre TLS foi estabelecida com o CVP? Se sim, a saída confirma que os sinais SIP entre o CVP e o CUBE estão protegidos.

7. Neste momento, a chamada está ativa e você ouve o Music on Hold (MOH), pois não há agente disponível para atender a chamada.

8. Disponibilize o agente para atender a chamada.



9. O agente é reservado e a chamada é roteada para ele. Clique em **Answer** para atender a chamada.



Incoming Call from 3227046971

Customer Name : Michael Littlefoot

Customer Email : michael.littlefoot@dcloud.cisco.com

Customer Address :

Call Reason : Advisor Services

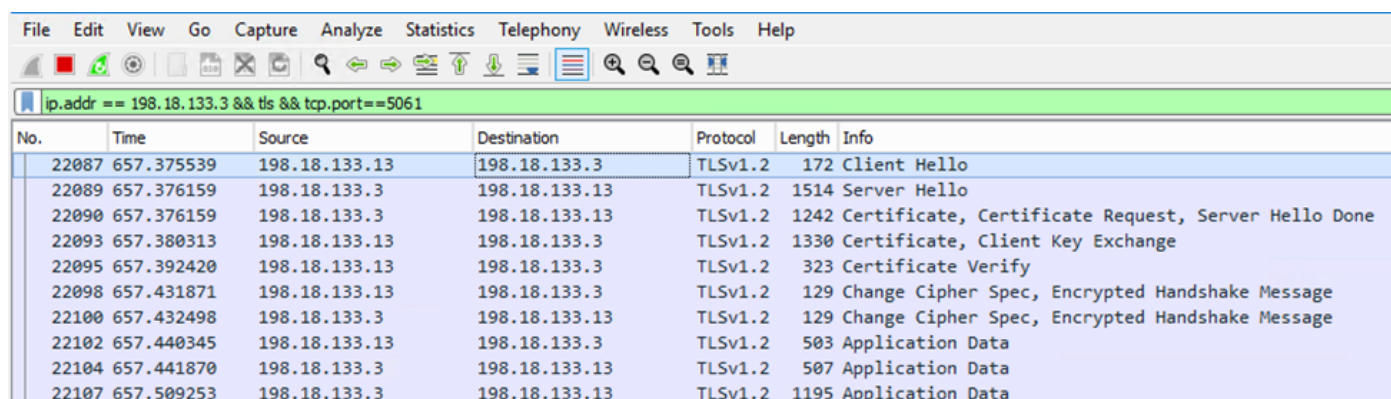
Mortgage Informat... : Advisor Services

Answer

10. A chamada se conecta ao agente.

11. Para verificar os sinais SIP entre o CVP e o CUCM, navegue para a sessão CVP e execute este filtro no 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

Verificação: Todas as comunicações SIP são feitas com CUCM (198.18.133.3) sobre TLS? Se sim, a saída confirma que os sinais SIP entre o CVP e o CUCM estão protegidos.

Troubleshoot

Se o TLS não estiver estabelecido, execute estes comandos no CUBE para permitir que o TLS de depuração solucione problemas:

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

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.