

Configurar o RTP seguro 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](#)

[Associe perfis de segurança de tronco SIP aos respectivos troncos SIP e habilite o SRTP](#)

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

[Verificar](#)

Introduction

Este documento descreve como proteger o tráfego do protocolo de transporte em tempo real (SRTP) 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 do Cisco Unified Communication Manager (CUCM), do Customer Voice Portal (CVP) Call Server, do Cisco Virtual Voice Browser (CVB) e do 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.

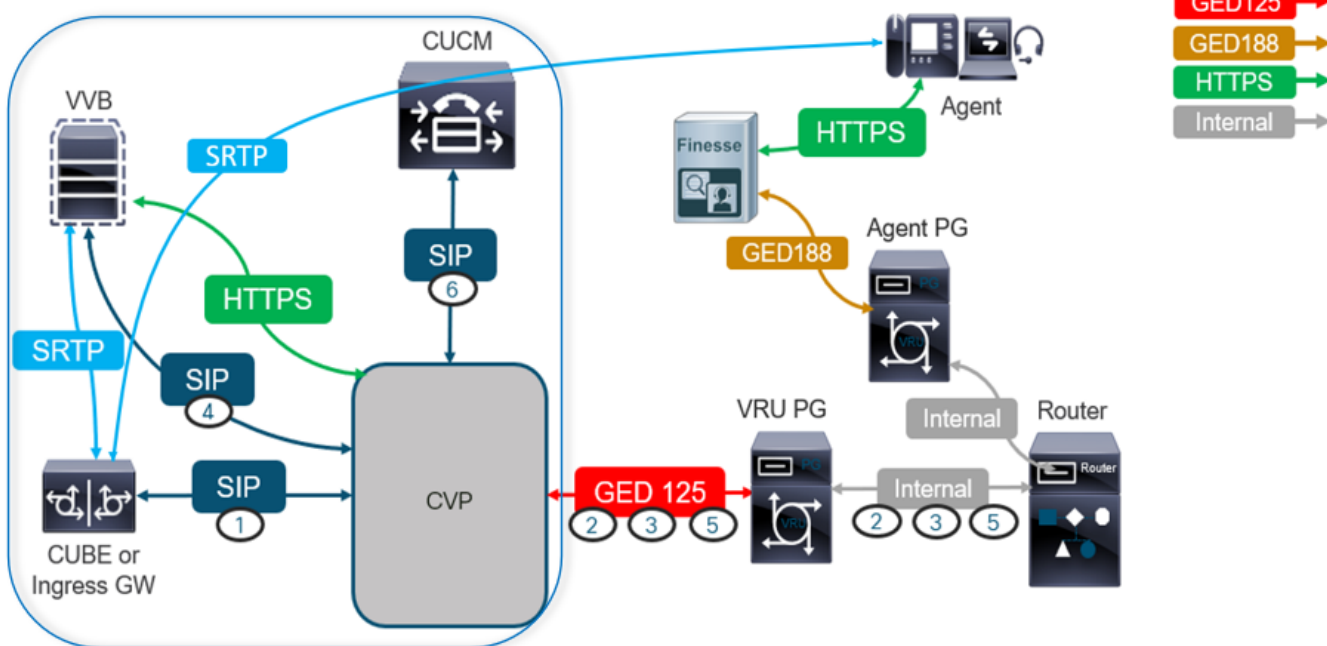
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Observação: no fluxo de chamadas abrangente da central de contatos, para habilitar o RTP seguro, sinais SIP seguros devem ser habilitados. Portanto, as configurações neste documento habilitam o SIP e o SRTP seguros.

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

Inbound Voice - Secure SIP and RTP



Tarefa 1: Configuração segura do CUBE

Nesta tarefa, você configura o CUBE para proteger mensagens de protocolo SIP e RTP.

Configurações necessárias:

- Configurar um ponto de confiança padrão para o SIP UA
- Modifique os correspondentes de discagem para usar TLS e SRTP

Etapas:

1. Abra uma sessão SSH para o CUBE.
2. Execute esses comandos para que a pilha SIP use o certificado CA do CUBE. O CUBE estabelece uma conexão SIP TLS de/para o CUCM (198.18.133.3) e o 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 srtp exit
```

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

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. Faça login no UCCE 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` depois no **Members** que mostra os detalhes das Configurações do Grupo de Servidores SIP. Configurado **SecurePort** para 5061 e clique em **Save**.

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

Edit `cucm1.dcloud.cisco.com`

General **Members**

List of Group Members +

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

4. Clique em `vvb1.dcloud.cisco.com` e depois no **Members** , defina o **SecurePort** para 5061 e clique em **Save**.

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

Edit `vvb1.dcloud.cisco.com`

General **Members**

List of Group Members +

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

Tarefa 3: Configuração segura do CVB

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

Etapas:

1. Abra o Cisco VVB Admin
2. Navegue até `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. Na guia Security Parameters , escolha Enable para TLS (SIP) . Mantenha a Supported TLS(SIP) version as TLSv1.2 e escolher Enable para SRTP.

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

4. Clique em Update. Clique em OK quando solicitado a reiniciar o mecanismo CVB.

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

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

The screenshot shows the 'Navigation' menu with the following items: 'Cisco VVB Administration', 'Cisco VVB Administration', 'Cisco Unified Serviceability', 'Cisco VVB Serviceability', and 'Cisco Unified OS Administration'. The 'Cisco VVB Serviceability' item is highlighted, and a 'Go' button is visible next to it.

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

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

7. Escolher Engine e clique em 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

Tarefa 4: Configuração segura do CUCM

Para proteger mensagens SIP e RTP no CUCM, execute estas configurações:

- Definir o modo de segurança do CUCM para o modo misto
- Configurar perfis de segurança de tronco SIP para CUBE e CVP
- Associe perfis de segurança de tronco SIP aos respectivos troncos SIP e habilite o SRTP
- Comunicação de dispositivo de Agentes Seguros com CUCM

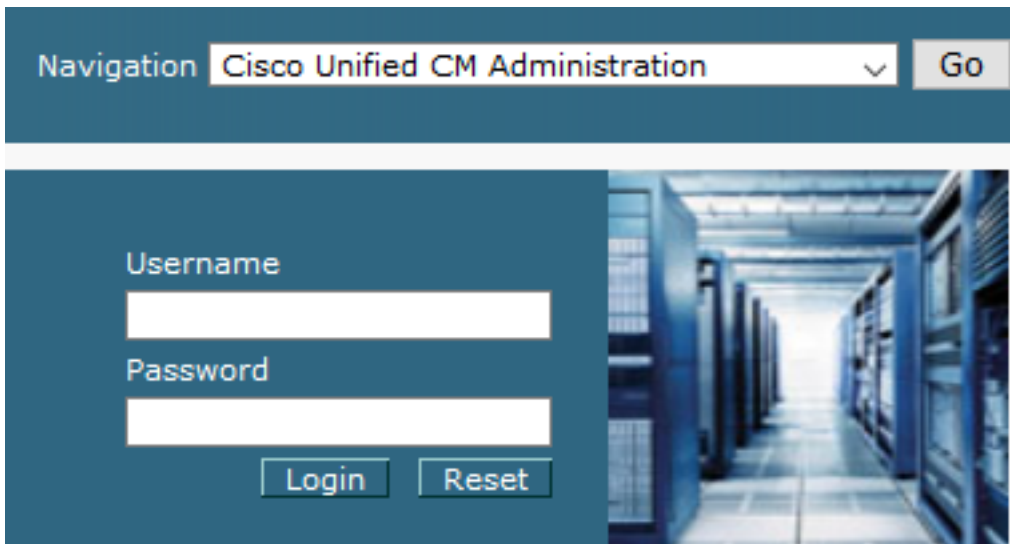
Definir o modo de segurança do CUCM para o modo misto

O CUCM suporta dois modos de segurança:

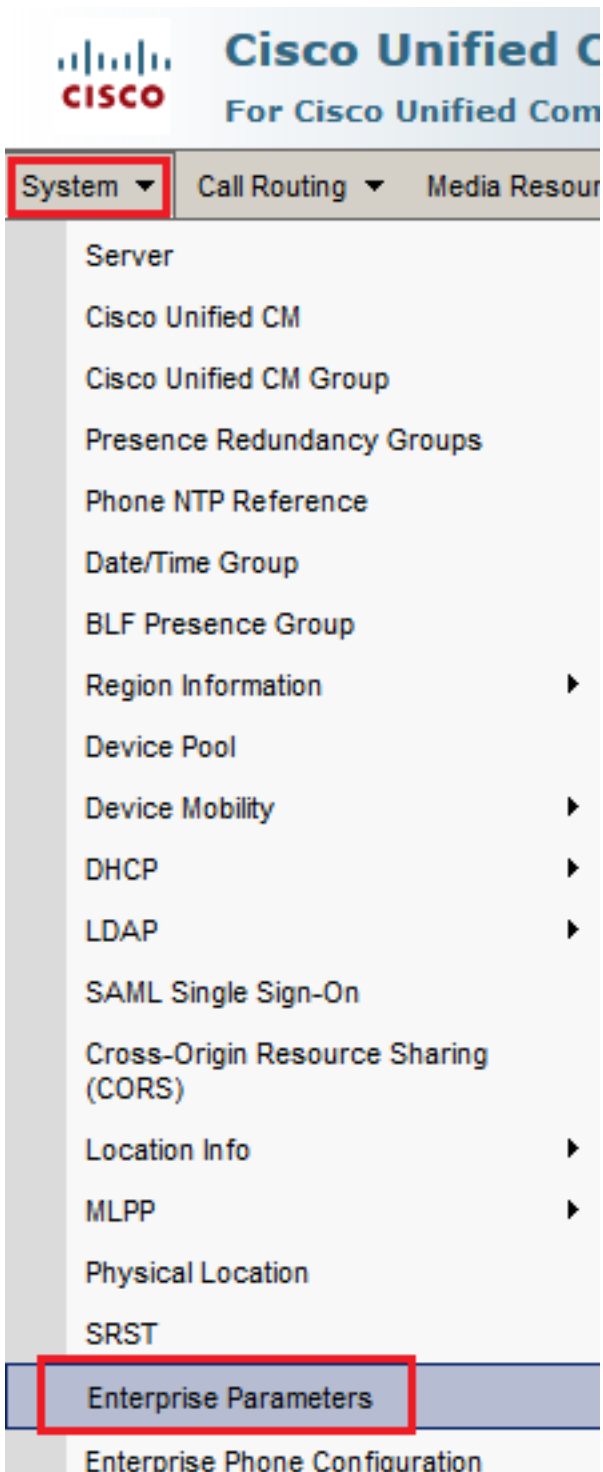
- Modo não seguro (modo padrão)
- Modo misto (modo seguro)

Etapas:

1. Faça login na interface de administração do CUCM.



2. Ao fazer login no CUCM, você pode navegar para **System > Enterprise Parameters**.



3. Sob o comando `Security Parameters` , verifique se a `Cluster Security Mode` está definido como `0`.



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. Após o login bem-sucedido no CUCM via SSH, execute este comando:

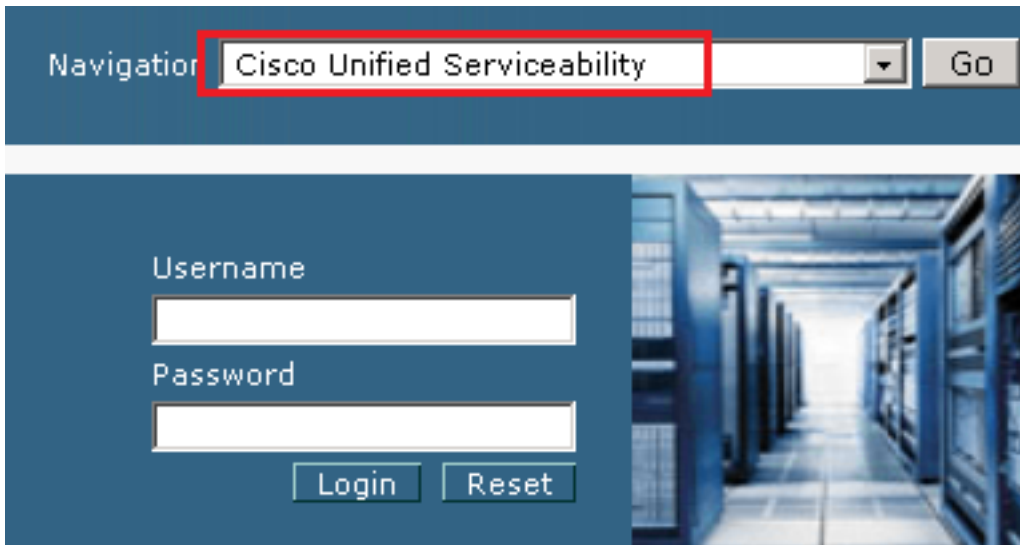
utils ctl set-cluster mixed-mode

7. Tipo `y` e clique em `Enter` no prompt. Este comando define o modo de segurança de cluster para o modo misto.

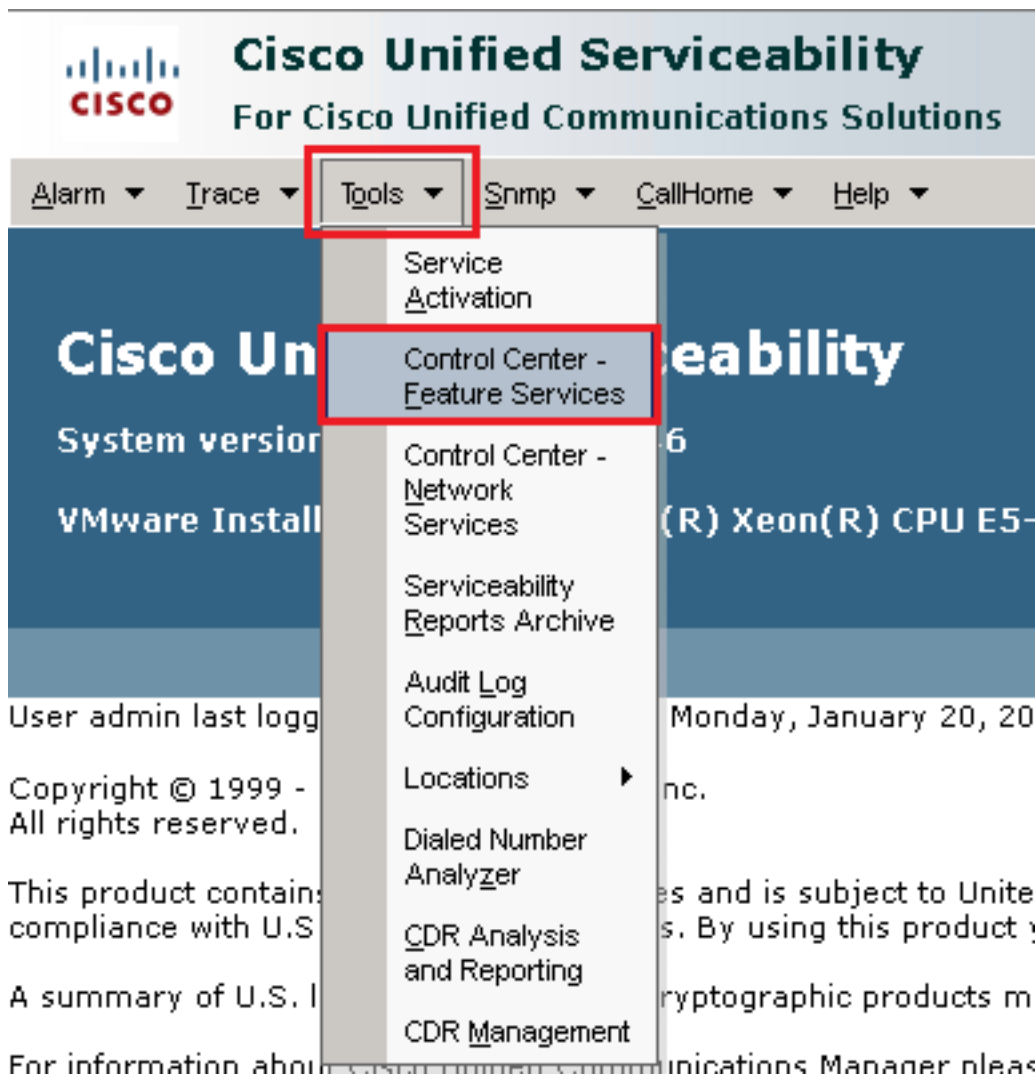
```
admin:utils ctl set-cluster mixed-mode
This operation will set the cluster to Mixed mode. Auto-registration is enabled on at least one CM node. Do you want to continue? (y/n): y
Moving Cluster to Mixed Mode
Cluster set to Mixed Mode
Please restart Cisco CallManager service and Cisco CTIManager services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

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

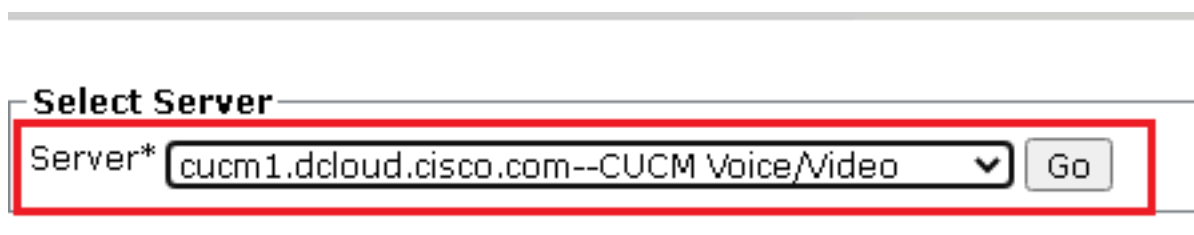
9. Para reiniciar os serviços, navegue e faça login no Cisco Unified Serviceability.



10. Após o login bem-sucedido, navegue até `Tools > Control Center – Feature Services`.



11. Escolha o servidor e clique em Go.



12. Abaixo dos serviços CM, escolha o comando Cisco CallManager e 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 a reinicialização bem-sucedida do Cisco CallManager, escolha o 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.



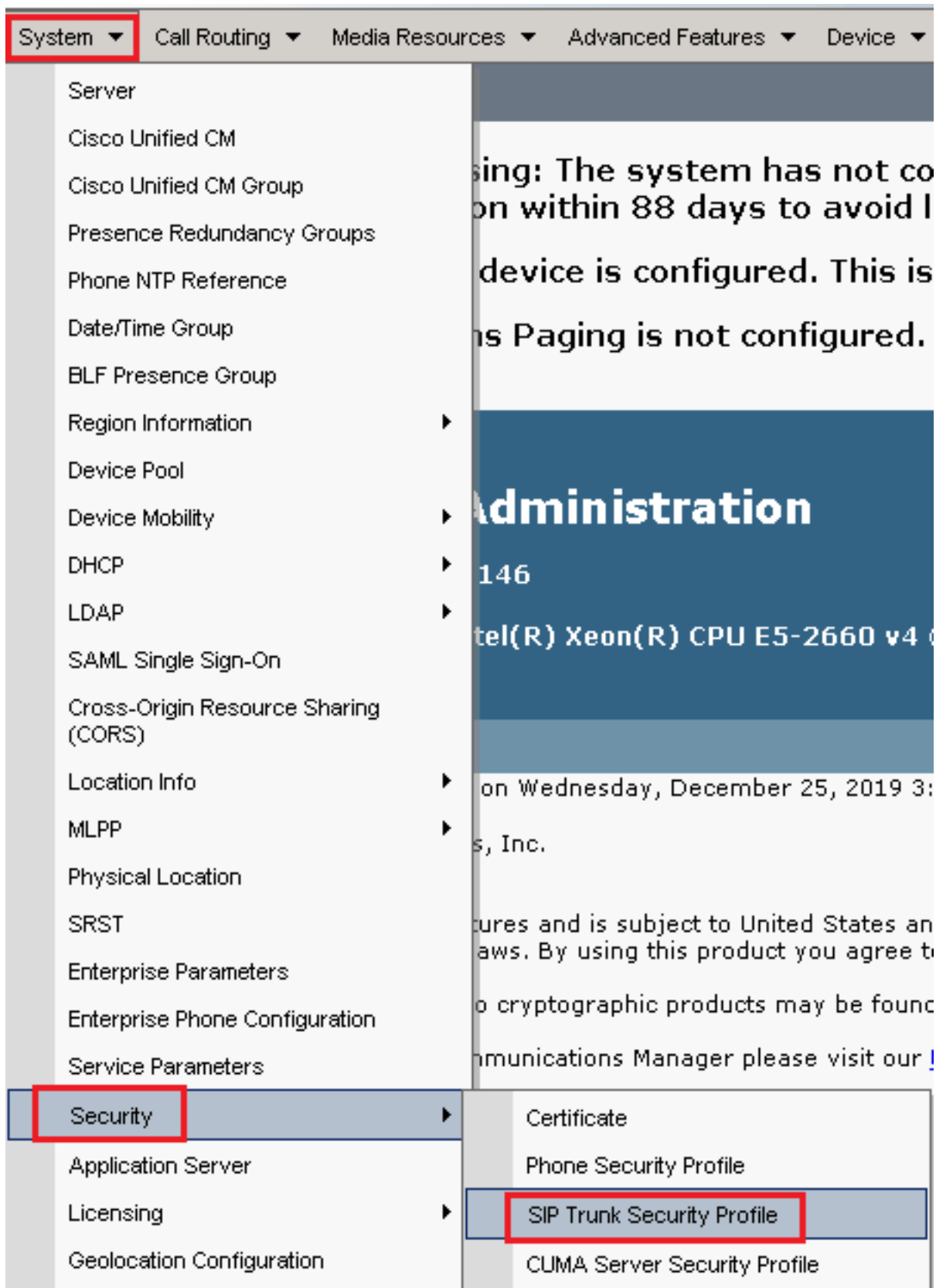
16. Após a reinicialização bem-sucedida dos serviços, para verificar se o modo de segurança do cluster está definido como modo misto, navegue até a administração do CUCM, conforme explicado na Etapa 5. e verifique a Cluster Security Mode. Agora ele deve ser definido como 1.

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

Configurar perfis de segurança de tronco SIP para CUBE e CVP

Etapas:

1. Faça login na interface de administração do CUCM.
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 esta imagem e clique em Save na parte inferior esquerda da página.

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`. alteram `Secure Certificate Subject` ao CN do certificado de servidor de chamada CVP, pois ele deve corresponder. Clique em `save` botão.

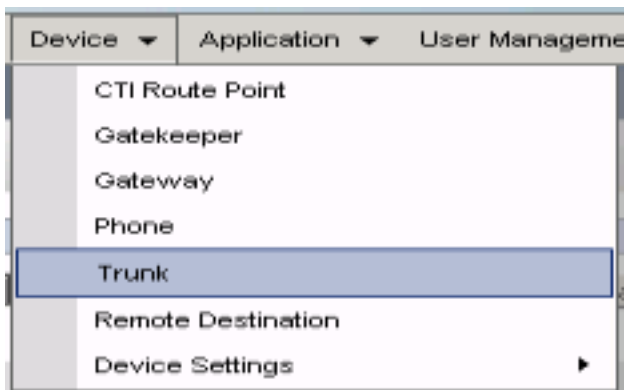
The screenshot displays the configuration page for a SIP Trunk Security Profile. At the top, there is a toolbar with icons for Save, Delete, Copy, Reset, Apply Config, and Add New. Below the toolbar, the **Status** section shows two informational messages: "Add successful" and "Reset of the trunk is required to have changes take effect." The main section is titled **SIP Trunk Security Profile Information**. It contains several configuration fields and options:

- Name***: SecureSIPTLSforCvp
- Description**: (empty)
- 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

Associe perfis de segurança de tronco SIP aos respectivos troncos SIP e habilite o SRTP

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 e 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. IN Device Information, verifique a SRTP Allowed para habilitar o SRTP.

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

When using both sRTP and TLS
Default
Default

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

6. alteram SIP Trunk Security Profile para SecureSIPTLSForCube.

SIP Information

Destination

Destination Address is an SRV

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

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

7. 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

- Navegue até **Device > Trunk**, 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 begins with

<input type="checkbox"/>	Name ^	Description	Calling Search Space	Device Pool
<input type="checkbox"/>	CVP-SIP-Trunk	CVP-SIP-Trunk	dCloud_CSS	dCloud_DP

- Clique em **CVP-SIP-Trunk** para abrir a página de configuração do tronco CVP.
- IN **Device Information**, verifique **SRTP Allowed** para habilitar o SRTP.

Unattended Port

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

Consider Traffic on This Trunk Secure*

Route Class Signaling Enabled*

Use Trusted Relay Point*

- Role para baixo até **SIP Information**, altere o **Destination Port** para **5061**.
- alteram **SIP Trunk Security Profile** para **SecureSIPTLSForCvp**.

SIP Information

Destination

Destination Address is an SRV

Destination Address

Destination Address IPv6

Destination Port

1*

MTP Preferred Originating Codec*

BLF Presence Group*

SIP Trunk Security Profile*

- 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.

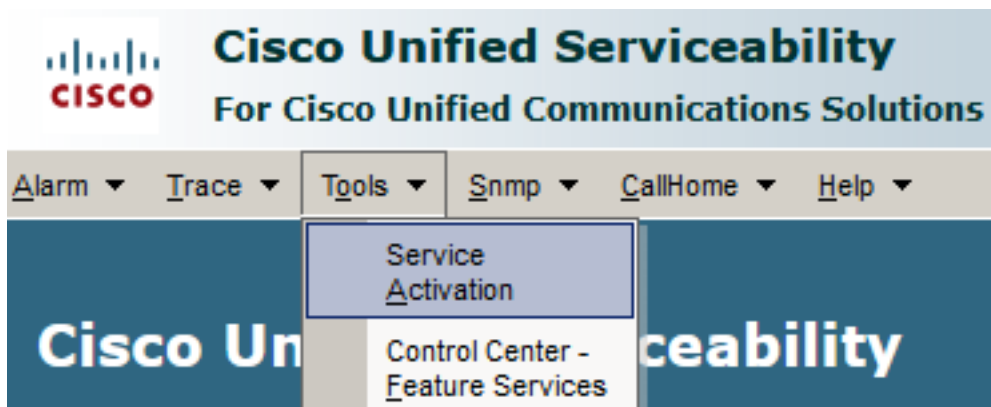
OK

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 o perfil de segurança a esse dispositivo. O LSC possui a chave pública para o endpoint, que é assinada pela chave privada CUCM CAPF. 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

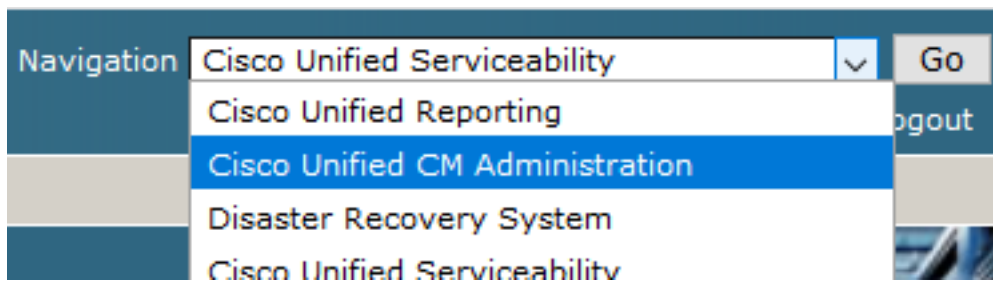
Server*

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 a administração do CUCM.



6. Após o login bem-sucedido na administração do CUCM, navegue até `System > Security > Phone Security Profile` para criar um perfil de segurança de dispositivo para o dispositivo do agente.



System ▾

Call Routing ▾

Media Resources ▾

Advanced Features ▾

Devi

Server

Cisco Unified CM

Cisco Unified CM Group

Presence Redundancy Groups

Phone NTP Reference

Date/Time Group

BLF Presence Group

Region Information ▶

Device Pool

Device Mobility ▶

DHCP ▶

LDAP ▶

SAML Single Sign-On

Cross-Origin Resource Sharing (CORS)

Location Info ▶

MLPP ▶

Physical Location

SRST

Enterprise Parameters

Enterprise Phone Configuration

Service Parameters

Security ▶

Application Server

Licensing ▶

Geolocation Configuration

device is configured. The
as 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. Localize o perfil de segurança referente ao seu tipo de dispositivo de agente. Neste exemplo, um softphone é usado, então escolha Cisco Unified Client Services Framework - Standard SIP Non-Secure Profile. Clique no ícone de cópia  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. C Altere os parâmetros como 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*
Description
Device Security Mode
Transport Type*
 TFTP Encrypted Config
 Enable OAuth Authentication

Phone Security Profile CAPF Information

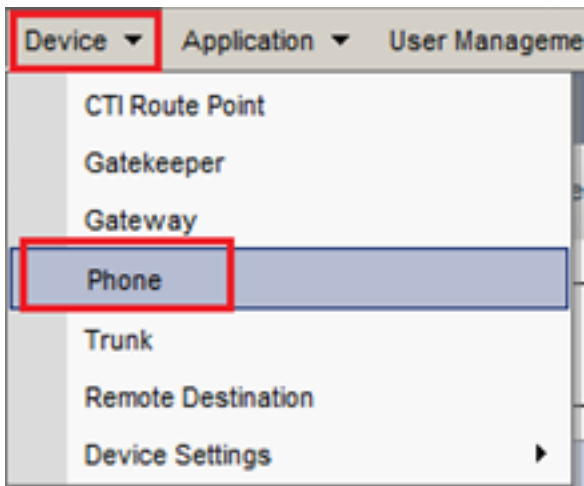
Authentication Mode*
Key Order*
RSA Key Size (Bits)*
EC Key Size (Bits)
Note: These fields are related to the CAPF Information settings on the Phone Configuration page.

Parameters used in Phone

SIP Phone Port*

Save Delete Copy Reset Apply Config Add New

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



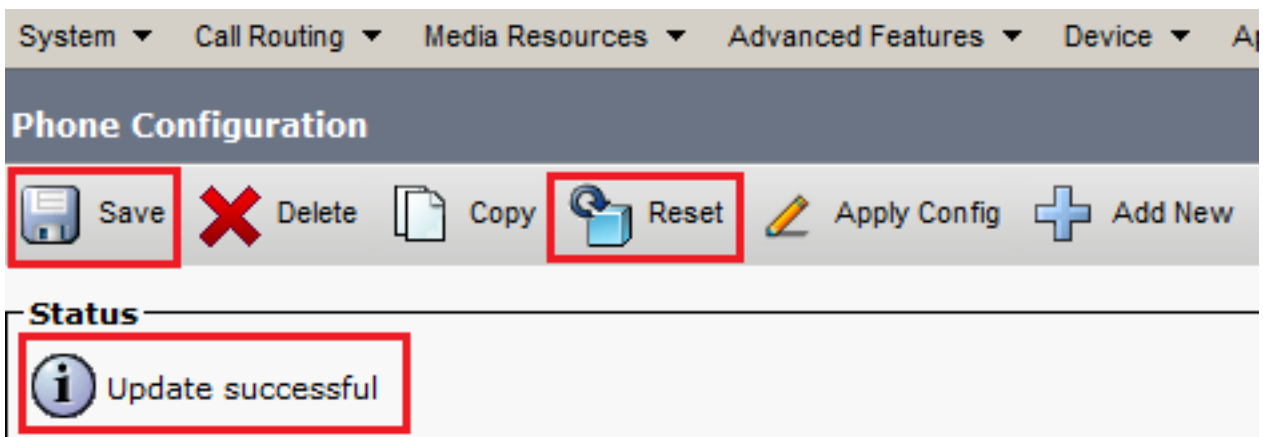
10. Clique em **Find** para listar todos os telefones disponíveis e, em seguida, clique em telefone do agente.
11. A página Configuração do telefone do agente é aberta. Localizar **Certification Authority Proxy Function (CAPF) Information** seção. Para instalar o LSC, configure **Certificate Operation** 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*' dropdown is set to 'Install/Upgrade'. The 'Authentication Mode*' dropdown is set to 'By Null String'. The 'Authentication String' field is empty. There is a 'Generate String' button. 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)'. Below the fields, it says 'Certificate Operation Status: None' and 'Note: Security Profile Contains Addition CAPF Settings.'.

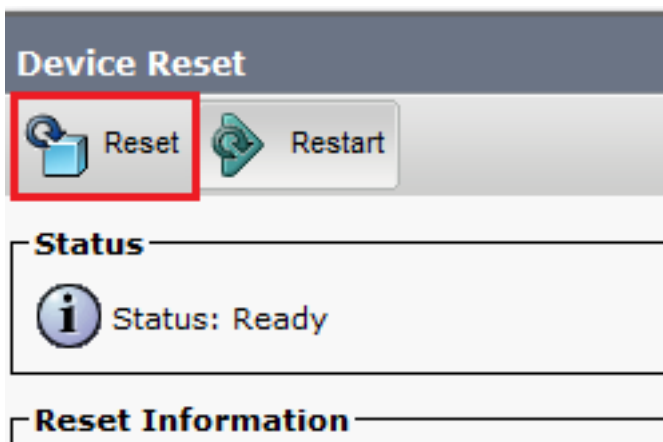
12. Localizar **Protocol Specific Information** e altere a **Device Security Profile** para **Cisco Unified Client Services Framework – Secure Profile**.

A screenshot of the 'Protocol Specific Information' configuration page. The page contains several fields and dropdown menus. The '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'. The 'Rerouting Calling Search Space' dropdown is set to 'Cisco Unified Client Services Framework - Secure Profile'.

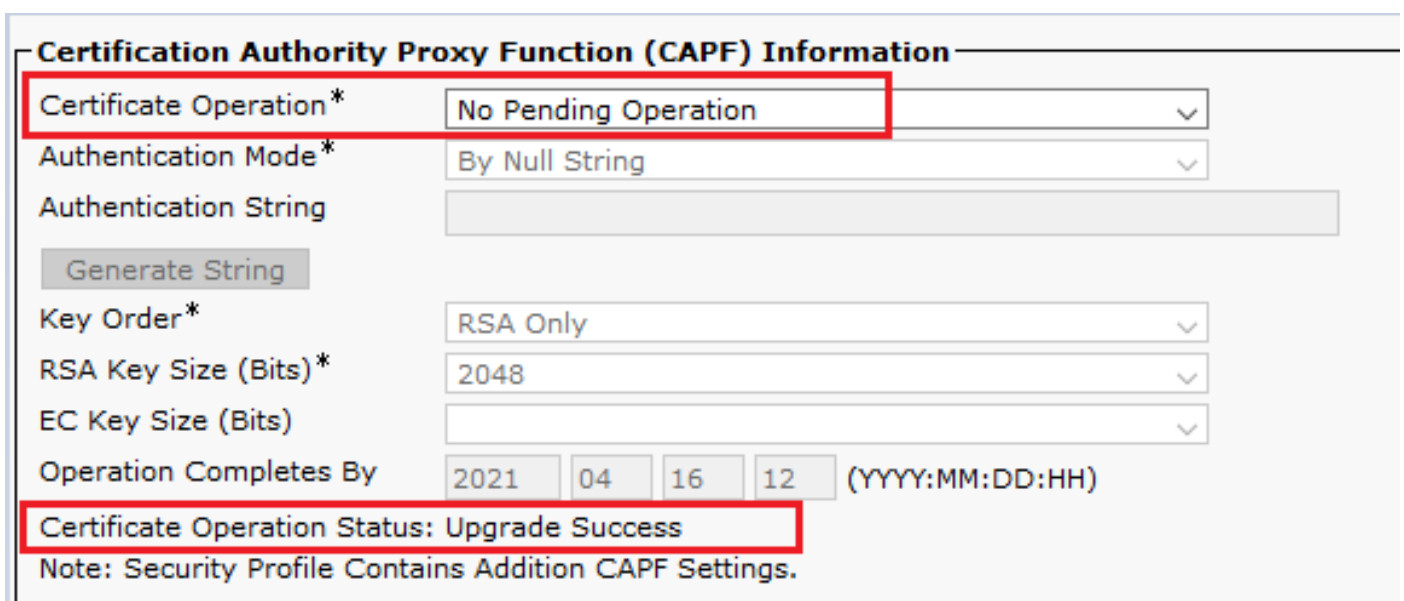
13. Clique em **save** na parte superior esquerda da página. Verifique se as alterações foram salvas com êxito e clique em **Reset**.



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 mesmas etapas da Etapa 1. 7 - 13 para proteger os dispositivos de outros agentes que você deseja usar SIP e RTP seguros com CUCM.

Verificar

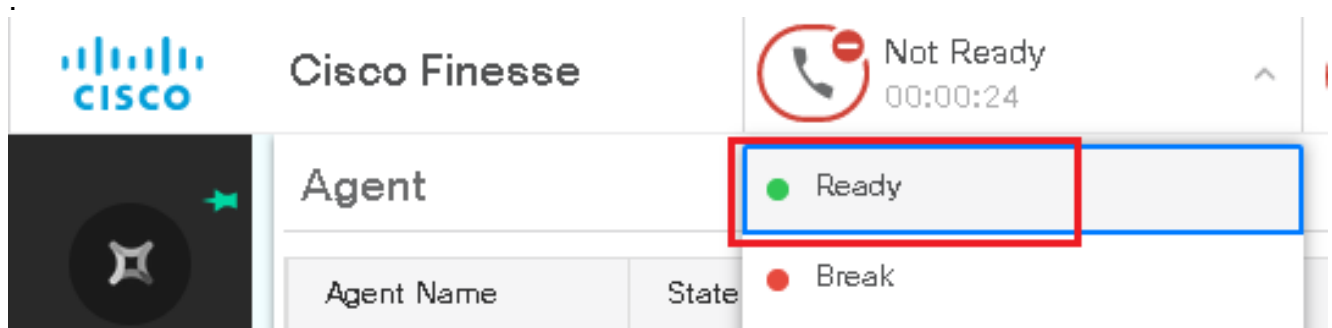
Para validar se o RTP está protegido corretamente, execute estas etapas:

1. Faça uma chamada de teste para a central de contatos e ouça o prompt IVR.
2. Ao mesmo tempo, abra a sessão SSH para o vCUBE e execute este comando:
show call active voice brief

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

Dica: verifique se o SRTP está on entre CUBE e VVB (198.18.133.143). Se sim, isso confirma que o tráfego RTP entre CUBE e VB é seguro.

3. Disponibilize um agente para atender a chamada.

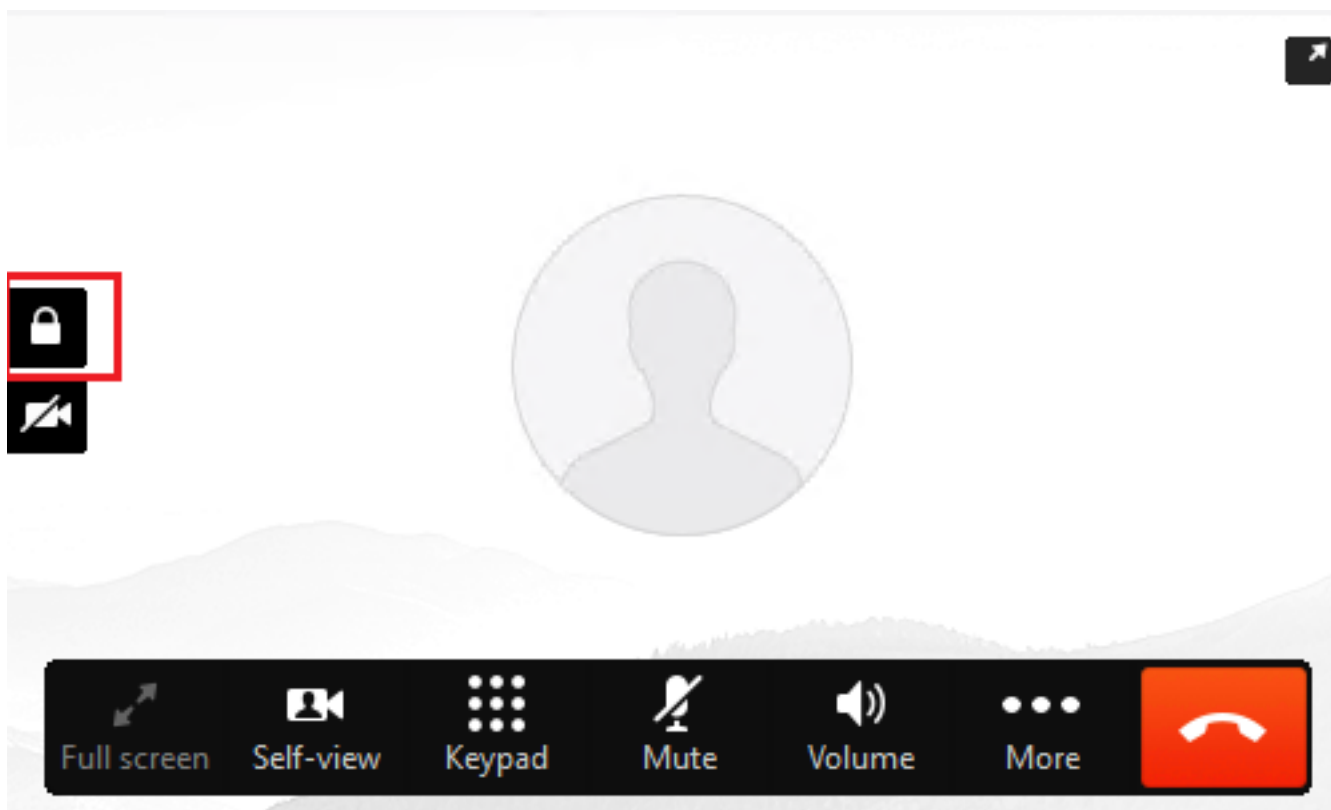


4. O agente é reservado e a chamada é roteada para o agente. Atenda a chamada.
5. A chamada é conectada ao agente. Volte para a sessão vCUBE SSH e execute este comando:
show call active voice brief

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

Dica: verifique se o SRTP está on entre o CUBE e os telefones dos agentes (198.18.133.75). Se sim, isso confirma que o tráfego RTP entre o CUBE e o agente está seguro.

6. Além disso, quando a chamada é conectada, um bloqueio de segurança é exibido no dispositivo do agente. Isso também confirma que o tráfego RTP está seguro.



Para validar se os sinais SIP estão protegidos corretamente, consulte o artigo [Configurar Sinalização SIP Segura](#).

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.