

在联系中心企业版中配置安全SIP信令

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[任务1.CUBE安全配置](#)

[任务2.CVP安全配置](#)

[任务3.CVVB安全配置](#)

[任务4.CUCM安全配置](#)

[将CUCM安全模式设置为混合模式](#)

[为CUBE和CVP配置SIP中继安全配置文件](#)

[将SIP中继安全配置文件关联到各自的SIP中继](#)

[安全代理与CUCM的设备通信](#)

[验证](#)

[故障排除](#)

简介

本文档介绍如何在联系中心企业版(CCE)综合呼叫流程中保护会话初始协议(SIP)信令。

先决条件

证书生成和导入不在本文档的讨论范围之内，因此必须创建思科统一通信管理器(CUCM)、客户语音门户(CVP)呼叫服务器、思科虚拟语音浏览器(CVVB)和思科统一边界元素(CUBE)的证书并将其导入到各自的组件中。如果使用自签名证书，则必须在不同组件之间执行证书交换。

要求

Cisco 建议您了解以下主题：

- CCE
- CVP
- CUBE
- CUCM
- CVVB

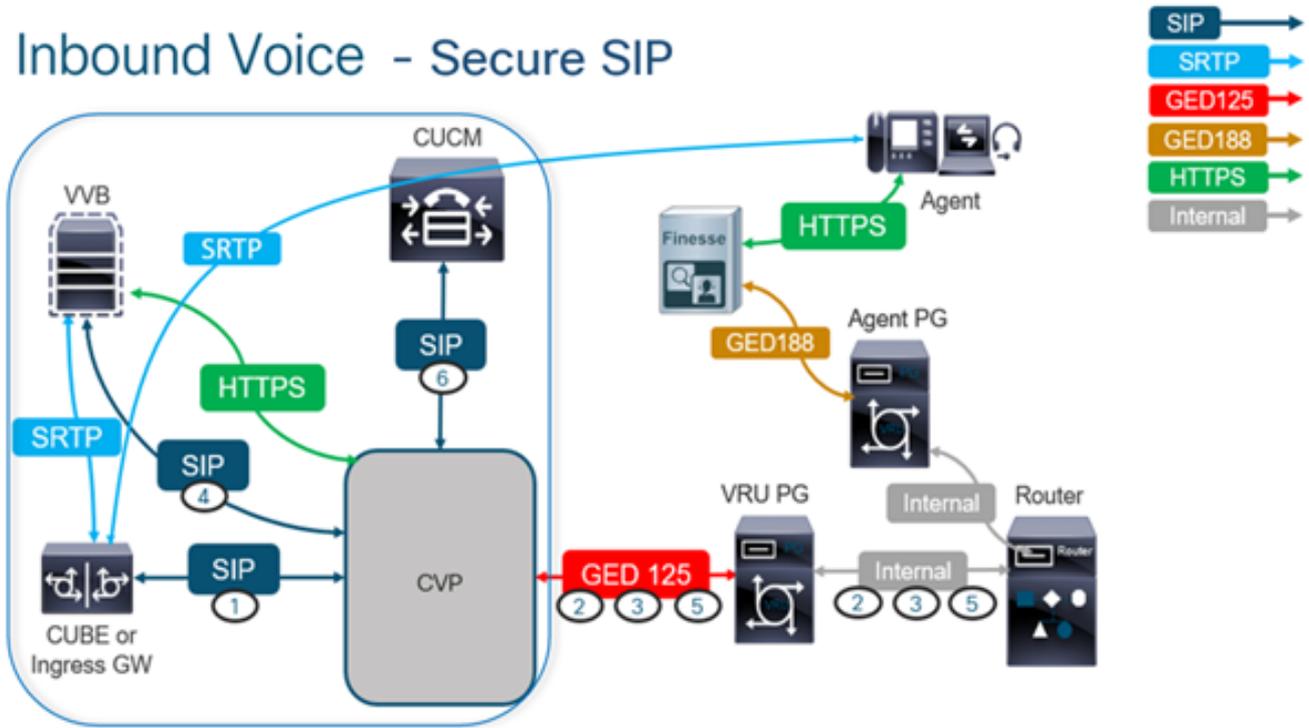
使用的组件

本文档中的信息基于Package Contact Center Enterprise(PCCE)、CVP、CVVB和CUCM版本12.6，但它也适用于早期版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

下图显示了联系中心综合呼叫流程中参与SIP信令的组件。当语音呼叫进入系统时，首先通过入口网关或CUBE，因此在CUBE上开始安全SIP配置。接下来，配置CVP、CVVB和CUCM。



任务1.CUBE安全配置

在本任务中，配置CUBE以保护SIP协议消息。

所需的配置：

- 为SIP用户代理(UA)配置默认信任点
- 修改拨号对等体以使用传输层安全(TLS)

步骤：

1. 打开与CUBE的安全外壳(SSH)会话。
2. 运行这些命令以使SIP堆栈使用CUBE的证书颁发机构(CA)证书。CUBE建立从/到CUCM(198.18.133.3)和CVP(198.18.133.13)的SIP TLS连接。

```
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. 运行这些命令以启用对CVP的传出拨号对等体上的TLS。在本示例中，拨号对等体标记6000用于将呼叫路由到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)#
```

任务2.CVP安全配置

在本任务中，配置CVP呼叫服务器以保护SIP协议消息(SIP TLS)。

步骤：

1. 登录到UCCE Web Administration.
2. 导航至 Call Settings > Route Settings > SIP Server Group.

Route Settings

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

Properties

根据您的配置，您为CUCM、CVVB和CUBE配置了SIP服务器组。您需要将所有安全SIP端口设置为5061。在本示例中，使用以下SIP服务器组：

- cucm1.dcloud.cisco.com 对于CUCM
- vvb1.dcloud.cisco.com 适用于CVVB
- cube1.dcloud.cisco.com 对于CUBE

3. 点击 cucm1.dcloud.cisco.com 然后在 Members 选项卡，其中显示了SIP服务器组配置的详细信息。设置 SecurePort 到 5061 并点击 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. 点击 vvb1.dcloud.cisco.com 然后在 Members 选项卡。将SecurePort设置为 5061 并点击 Save.

Edit vvb1.dcloud.cisco.com

General

Members

List of Group Members

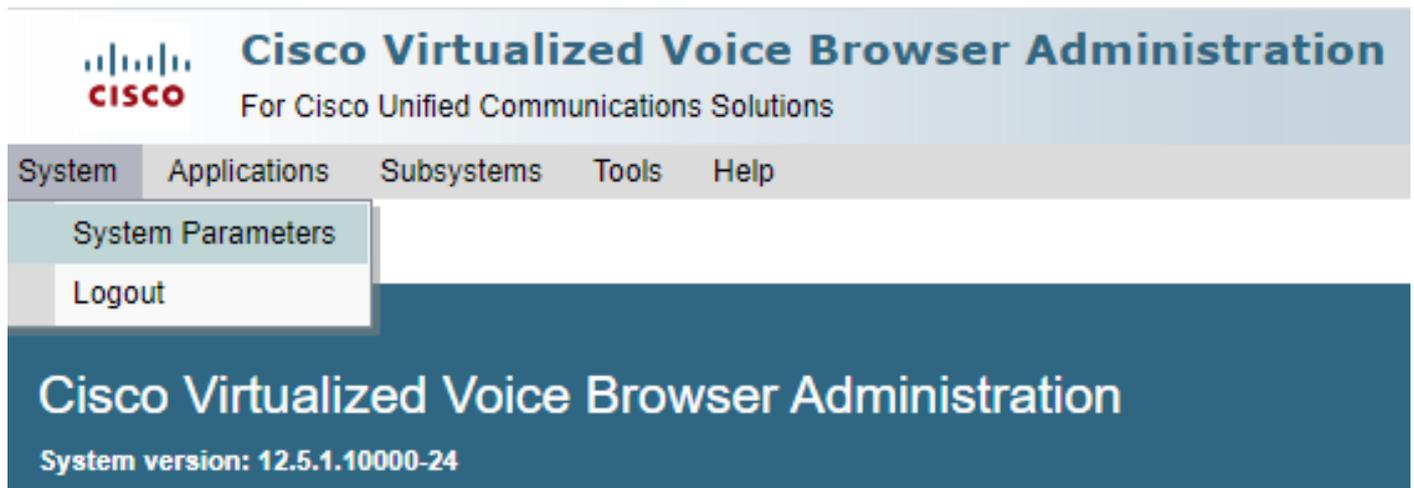
Hostname/IP	Priority	Weight	Port	SecurePort	Site
vvb1.dcloud.cisco.c...	10	10	5060	5061	Main

任务3.CVVB安全配置

在本任务中，配置CVVB以保护SIP协议消息(SIP TLS)。

步骤：

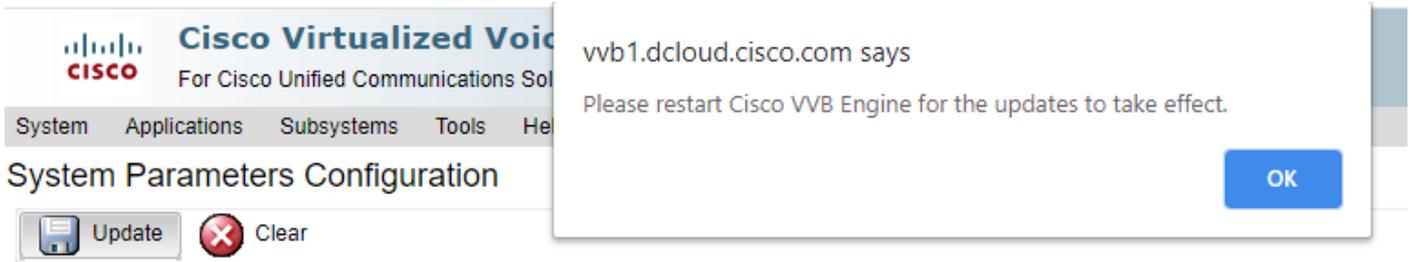
1. 登录到 **Cisco VVB Administration** 页码。
2. 导航至 **System > System Parameters**。



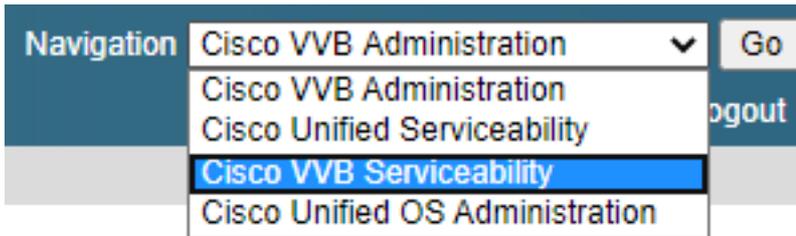
3. 如果 **Security Parameters** 部分，选择 **Enable** 对于 **TLS(SIP)**。保留 **Supported TLS(SIP) version** 作为 **TLSv1.2**。

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
	S RTP [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. 单击更新。点击 **OK** 提示重新启动CVVB引擎时。



5. 这些更改需要重新启动Cisco VVB引擎。要重新启动VVB引擎，请导航至 Cisco VVB Serviceability ?? 然后单击 Go.



6. 导航至 Tools > Control Center – Network Services.



7. 选择 Engine 并点击 Restart.

Control Center - Network Services

Start Stop **Restart** Refresh

Status

i Ready

Select Server

Server * vvb1

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

任务4.CUCM安全配置

要保护CUCM上的SIP消息，请执行以下配置：

- 将CUCM安全模式设置为混合模式
- 为CUBE和CVP配置SIP中继安全配置文件
- 将SIP中继安全配置文件关联到各自的SIP中继
- 安全代理与CUCM的设备通信

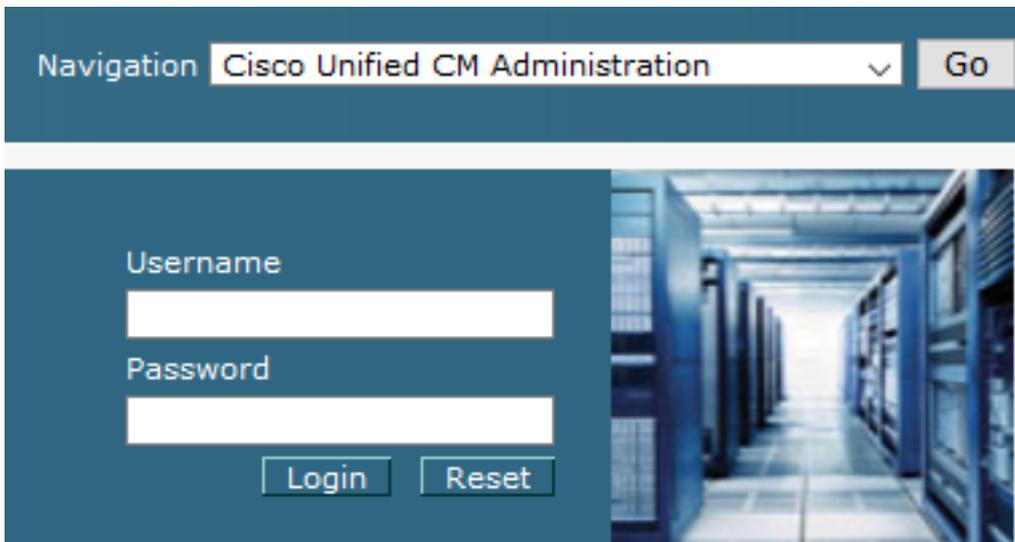
将CUCM安全模式设置为混合模式

CUCM支持两种安全模式：

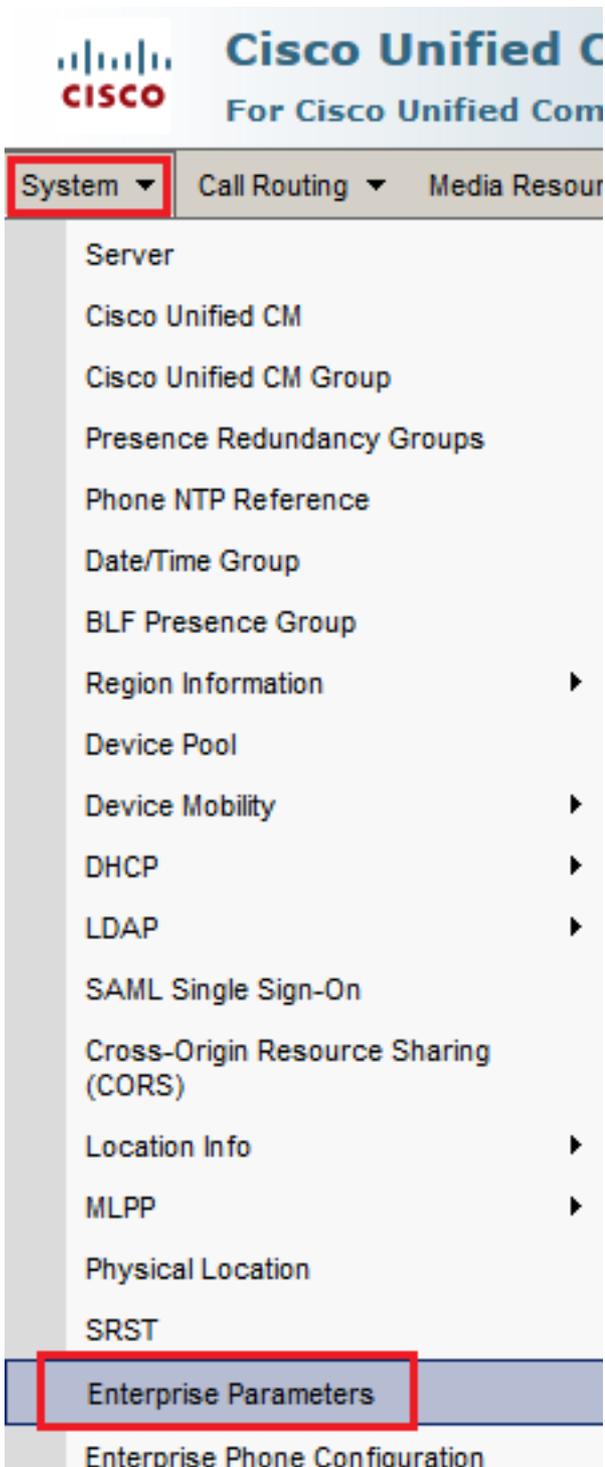
- 非安全模式 (默认模式)
- 混合模式 (安全模式)

步骤：

1. 要将安全模式设置为混合模式，请登录 Cisco Unified CM Administration 接口。



2. 成功登录CUCM后，导航至 [System > Enterprise Parameters](#).



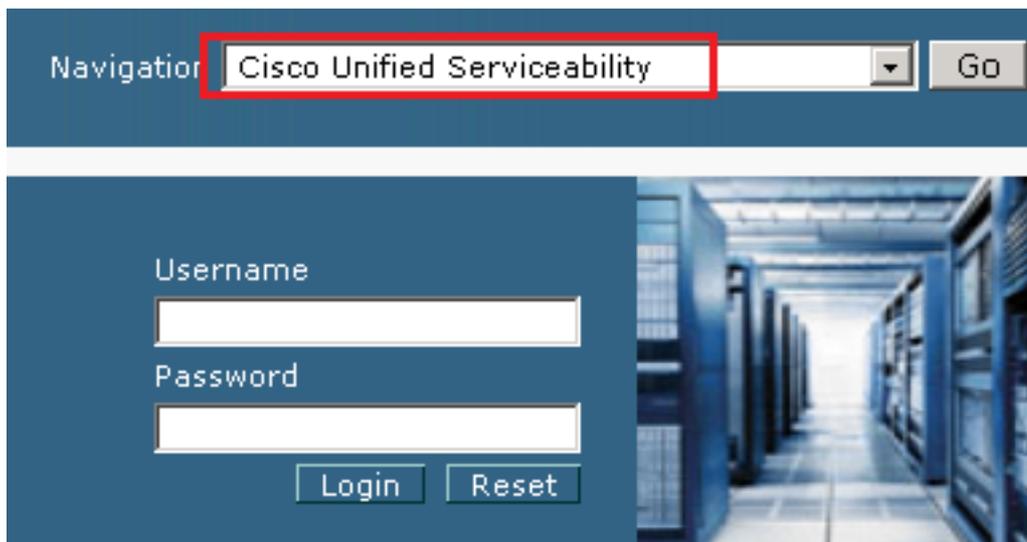
3. 在 Security Parameters 部分，检查是否 Cluster Security Mode 设置为 0。



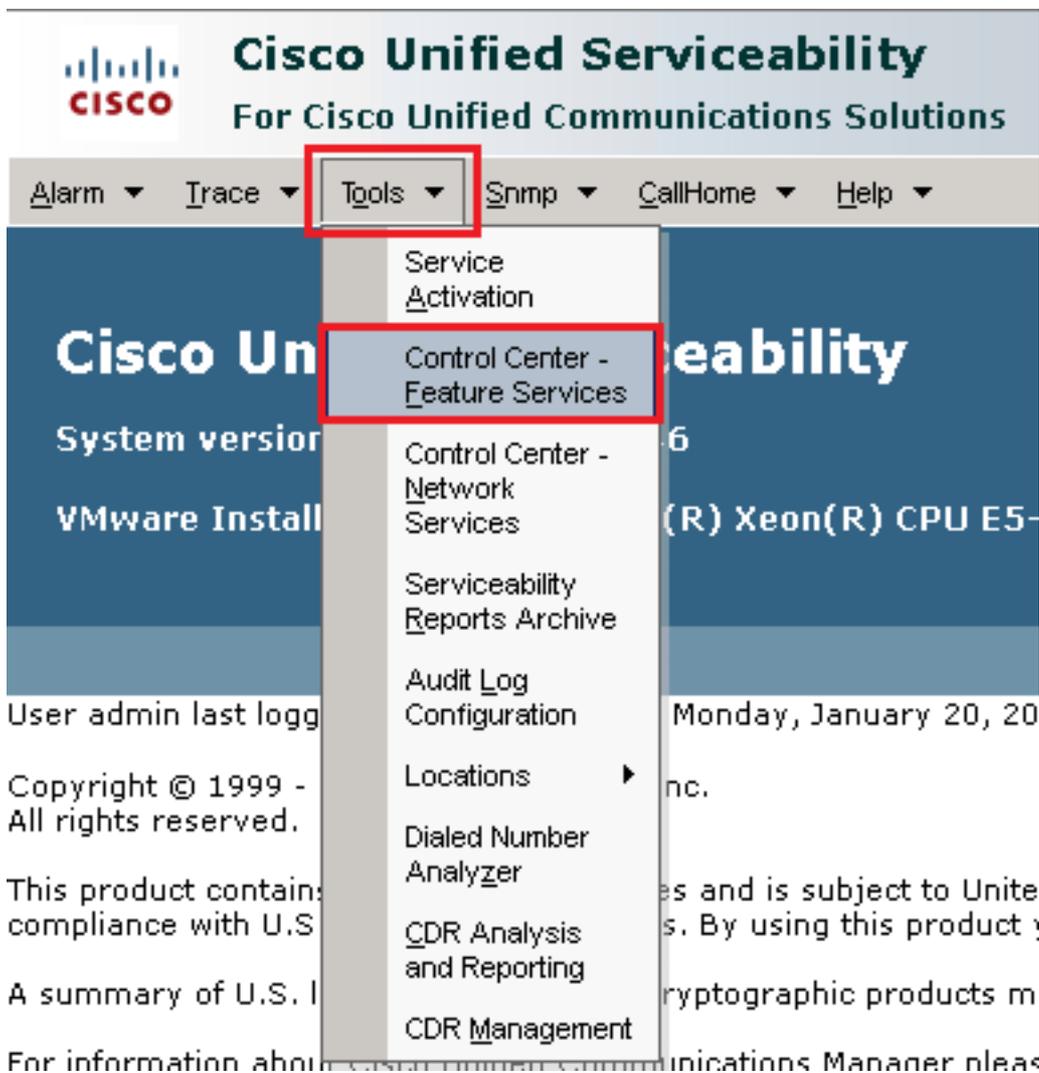
4. 如果集群安全模式设置为0，则表示集群安全模式设置为非安全。您需要从CLI启用混合模式。
5. 打开到CUCM的SSH会话。
6. 通过SSH成功登录CUCM后，请运行以下命令：`utils ctl set-cluster mixed-mode`
7. 类型 `y` 并在出现提示时单击Enter。此命令将集群安全模式设置为混合模式。

```
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. 要使更改生效，请重新启动 Cisco CallManager 和 Cisco CTIManager 服务。
9. 要重新启动服务，请导航并登录 Cisco Unified Serviceability.



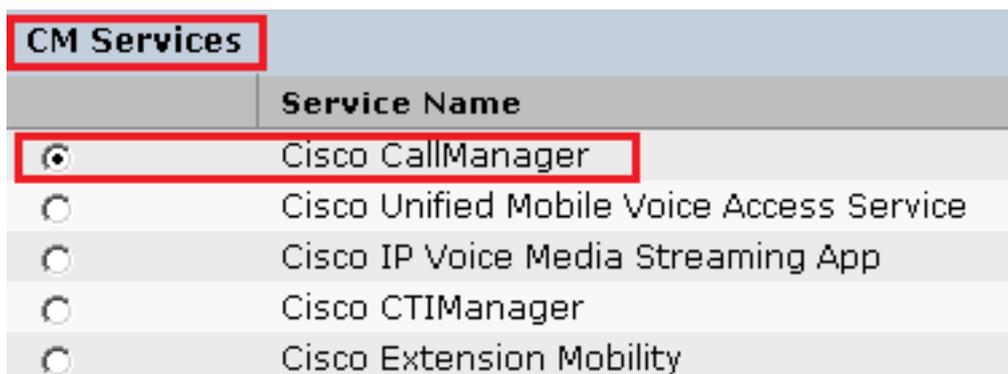
10. 成功登录后，导航至 Tools > Control Center – Feature Services.



11. 选择服务器，然后单击 Go.



12. 在CM服务下，选择 Cisco CallManager ?? 然后单击 Restart 按钮。



13. 确认弹出消息，然后单击 ok.等待服务成功重新启动。

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. 成功重新启动 Cisco CallManager，选择思科 CTIManager ?? 然后单击 Restart 按钮重启 Cisco CTIManager 服务。

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. 确认弹出消息，然后单击 OK.等待服务成功重新启动。

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.



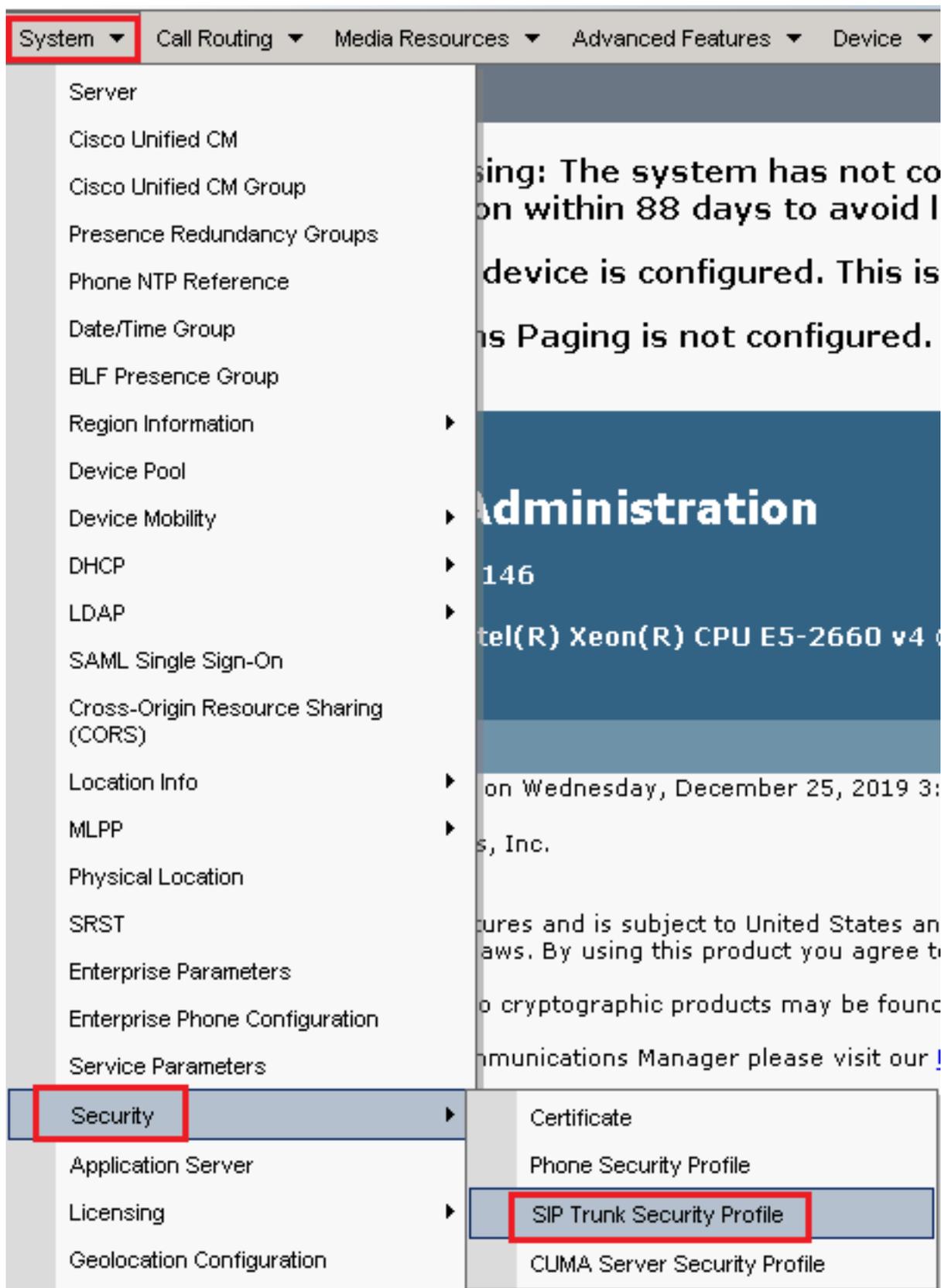
16. 服务成功重新启动后，验证集群安全模式是否设置为混合模式，然后按照步骤5中的说明导航到CUCM管理。然后检查 Cluster Security Mode.现在必须设置为 1.

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

为CUBE和CVP配置SIP中继安全配置文件

步骤：

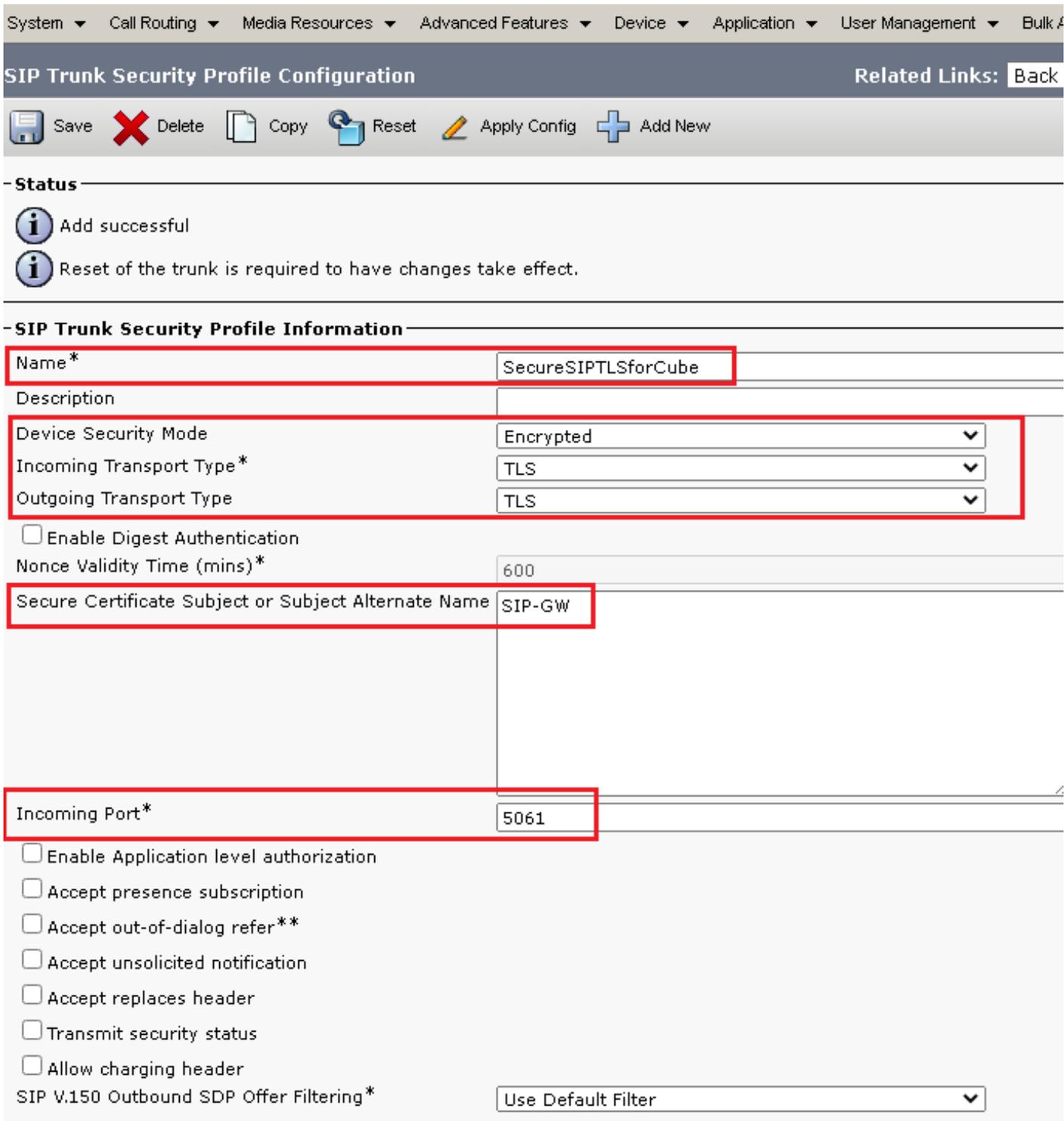
1. 登录到 CUCM administration 接口.
2. 成功登录CUCM后，导航至 System > Security > SIP Trunk Security Profile 以便为CUBE创建设备安全配置文件。



3. 在左上角，单击 **Add New** 以便添加新配置文件。



4. 配置 SIP Trunk Security Profile 如本图所示，然后单击 Save 位于页面左下角的 Save 它。



5. 确保已设置 Secure Certificate Subject or Subject Alternate Name CUBE证书的公用名(CN)，因为它必须匹配

。

6.单击 Copy 按钮并更改 Name 到 SecureSipTLSforCVP 和 Secure Certificate Subject CVP呼叫服务器证书的 CN，因为它必须匹配。点击 Save 按钮。

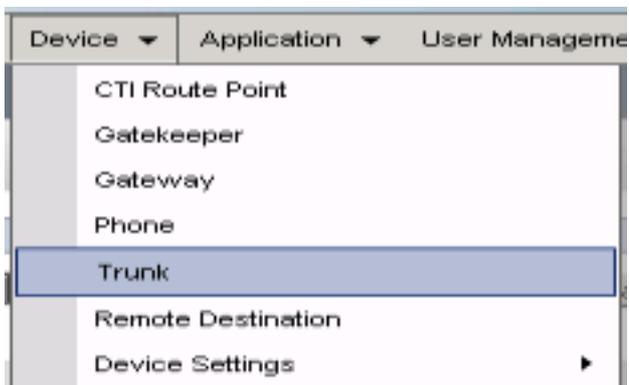
The screenshot displays the configuration interface for a SIP Trunk Security Profile. At the top, there is a toolbar with icons for Save, Delete, Copy, Reset, Apply Config, and Add New. Below the toolbar, the 'Status' section shows two informational messages: 'Add successful' and 'Reset of the trunk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

将SIP中继安全配置文件关联到各自的SIP中继

步骤：

1. 在CUCM Administration页面上，导航至 Device > Trunk.



2. 搜索CUBE中继。在本示例中，CUBE中继名称为 vCube。点击 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. 点击vCUBE以打开vCUBE中继配置页面。

4. 向下滚动到 SIP Information 部分，并更改 Destination Port 到 5061。

5. Change (更改) SIP Trunk Security Profile 到 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. 点击 Save 然后 Rest 为了 Save 并应用更改。



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. 导航至 Device > Trunk，并搜索CVP中继。在本示例中，CVP中继名称为 cvp-SIP-Trunk。点击 Find。

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

8. 点击 CVP-SIP-Trunk 以打开CVP中继配置页面。
9. 向下滚动到 SIP Information 部分，并更改 Destination Port 到 5061。
10. Change (更改) SIP Trunk Security Profile 到 SecureSIPTLSForCvp。

SIP Information

Destination

Destination Address is an SRV

1*	Destination Address	Destination Address IPv6	Destination Port
	198.18.133.13		5061

MTP Preferred Originating Codec* 711ulaw

BLF Presence Group* Standard Presence group

SIP Trunk Security Profile* SecureSIPTLSforCvp

11. 点击 Save 然后 Rest 为了 save 并应用更改。

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

安全代理与CUCM的设备通信

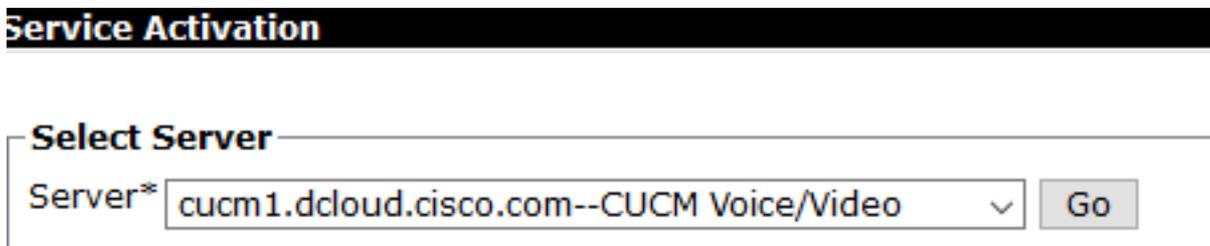
要启用设备的安全功能，必须安装本地重要证书(LSC)并为该设备分配安全配置文件。LSC拥有终端的公钥，该公钥由证书授权代理功能(CAPF)私钥签名。默认情况下，它不会安装在电话上。

步骤：

1. 登录到 Cisco Unified Serviceability Interface.
2. 导航至 Tools > Service Activation.



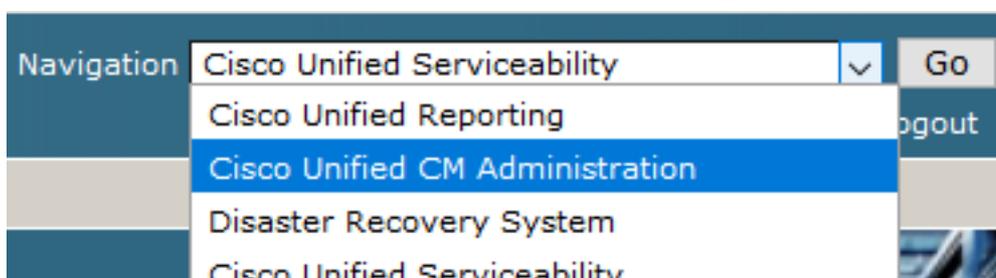
3. 选择CUCM服务器并单击 Go .



4. 检查 Cisco Certificate Authority Proxy Function 并点击 Save 激活服务。点击 Ok 确认。

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. 确保服务已激活，然后导航至 Cisco Unified CM Administration.



6. 成功登录CUCM管理后，导航至 System > Security > Phone Security Profile 为代理设备创建设备安全配置文件。



Cisco Unified CM Administration

For Cisco Unified Communications Solutions

System ▾

Call Routing ▾

Media Resources ▾

Advanced Features ▾

Devices

Server

Cisco Unified CM

Cisco Unified CM Group

Presence Redundancy Groups

Phone NTP Reference

Date/Time Group

BLF Presence Group

Region Information ▶

Device Pool

Device Mobility ▶

DHCP ▶

LDAP ▶

SAML Single Sign-On

Cross-Origin Resource Sharing (CORS)

Location Info ▶

MLPP ▶

Physical Location

SRST

Enterprise Parameters

Enterprise Phone Configuration

Service Parameters

Security ▶

Application Server

Licensing ▶

Geolocation Configuration

device is configured. The
Paging is not configur

Administration

7

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

on Friday, December 20, 2019 10

s, Inc.

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

o cryptographic products may be

munications Manager please visit

our [Technical Support](#) web site.

Certificate

Phone Security Profile

SIP Trunk Security Profile

CUMA Server Security Profile

7. 查找与您的座席设备类型对应的安全配置文件。在本示例中，使用软件电话，因此选择 Cisco Unified Client Services Framework - Standard SIP Non-Secure Profile，点击 Copy 以便复制此配置文件。

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. 将配置文件重命名为 Cisco Unified Client Services Framework - Secure Profile 更改此图中所示的参数，然后单击 Save 在页面左上角。

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 >

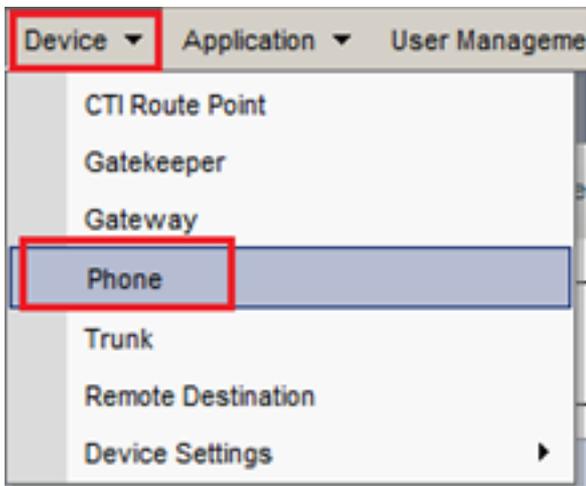
Note: These fields are related to the CAPF Information settings on the Phone Configuration page.

Parameters used in Phone

SIP Phone Port* 5061

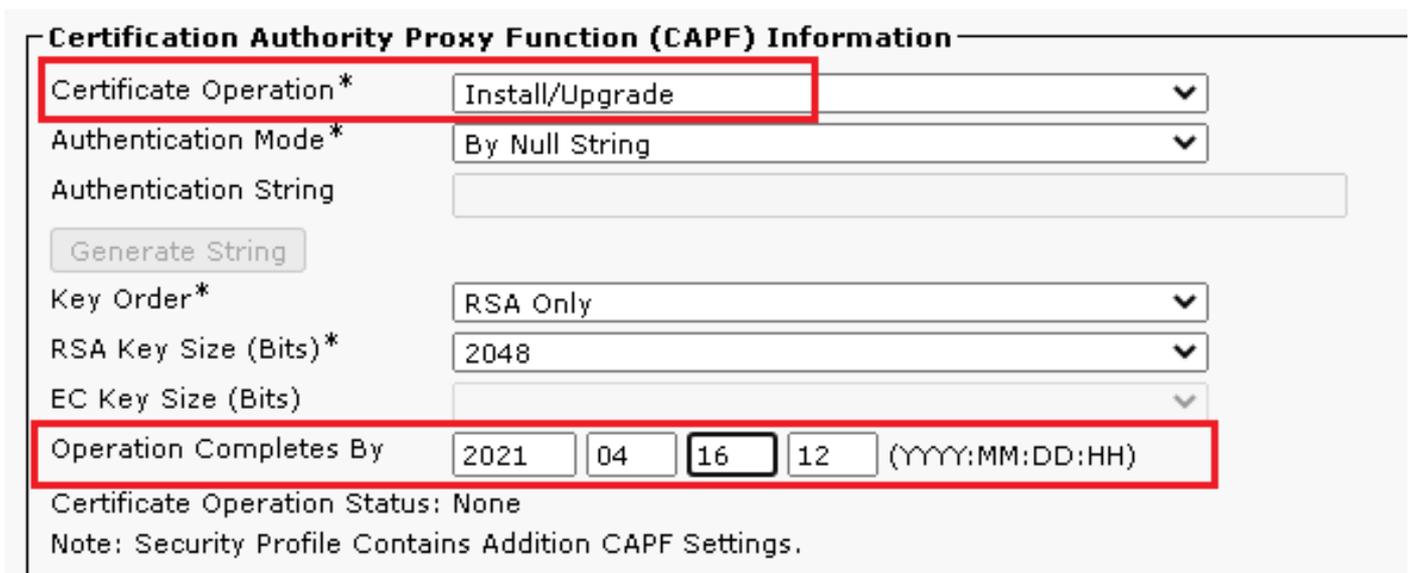
Save Delete Copy Reset Apply Config Add New

9. 成功创建电话设备配置文件后，导航至 Device > Phone.

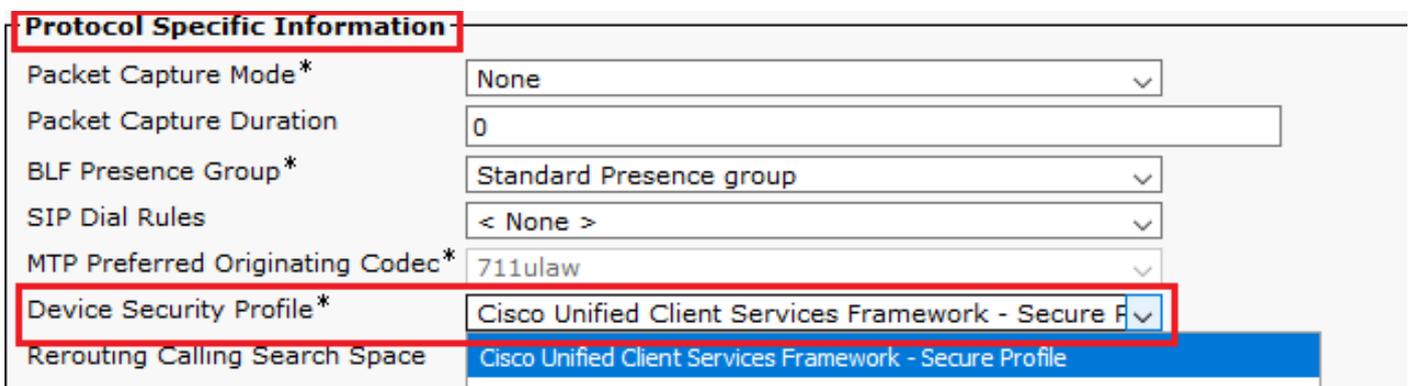


10. 点击 Find 要列出所有可用电话，请单击座席电话。

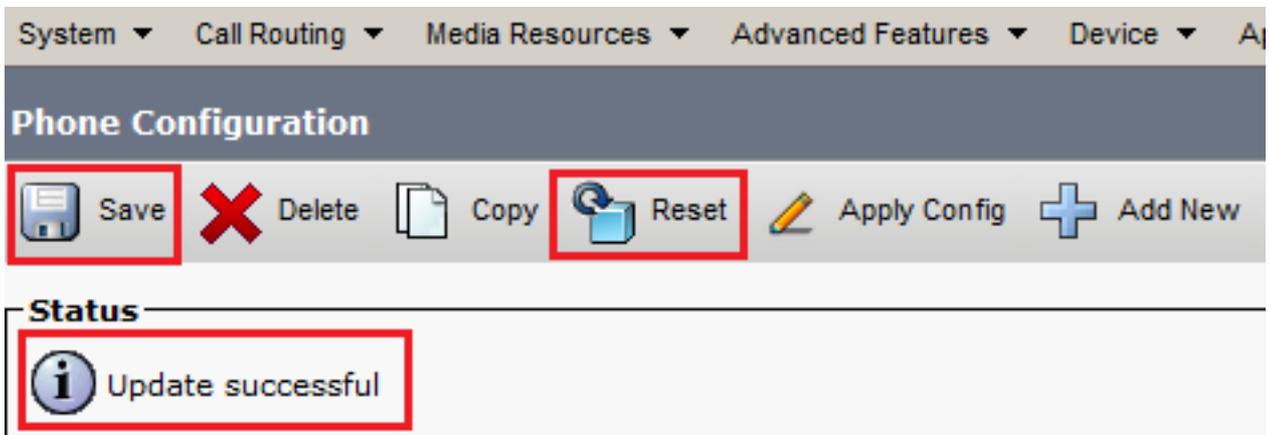
11. 座席电话配置页面打开。查找 Certification Authority Proxy Function (CAPF) Information 部分。要安装 LSC，请设置 Certificate Operation 到 Install/Upgrade 和 Operation Completes by 到任何未来日期。



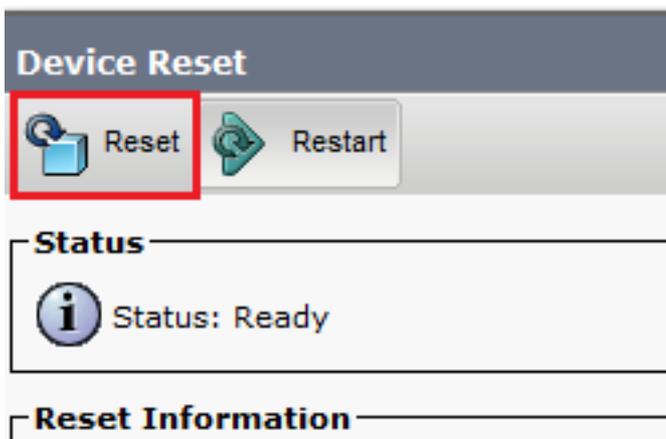
12. 查找 Protocol Specific Information 部分。Change (更改) Device Security Profile 到 Cisco Unified Client Services Framework – Secure Profile.



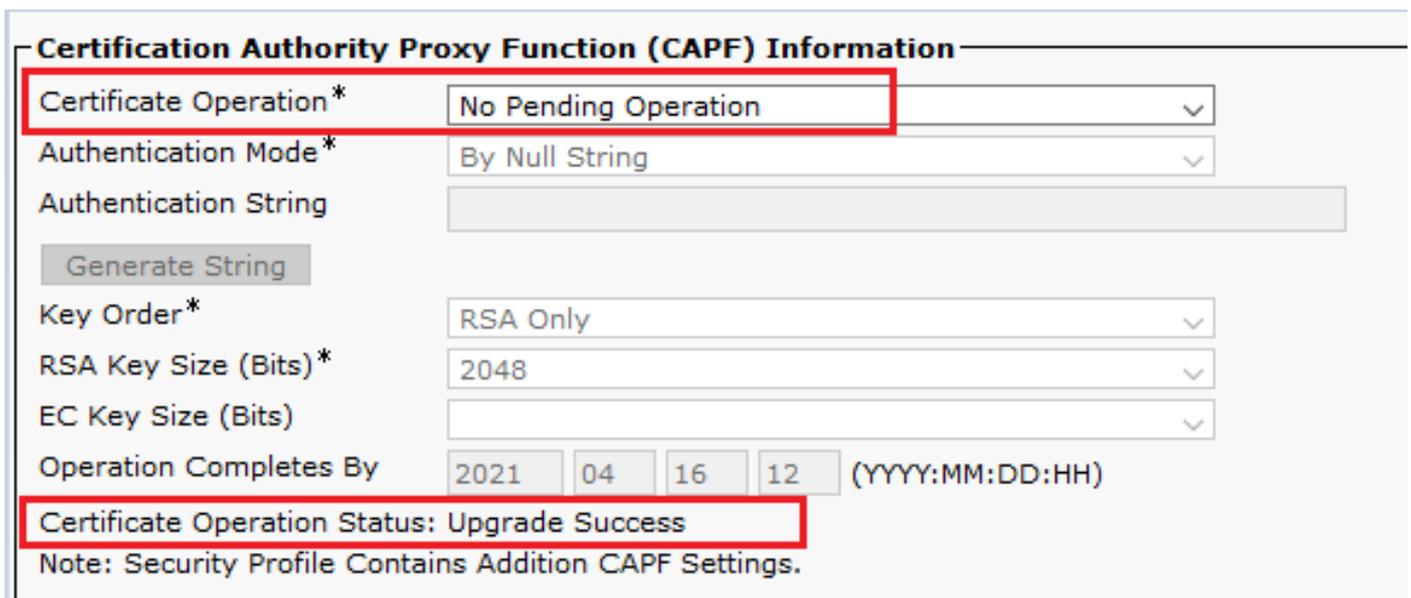
13. 点击 Save 在页面左上角。确保更改已成功保存，然后单击 Reset.



14. 系统将打开一个弹出窗口，单击 **Reset** 确认操作。



15. 代理设备再次向CUCM注册后，刷新当前页面并验证LSC是否安装成功。检查 **Certification Authority Proxy Function (CAPF) Information** 部分，**Certificate Operation** 必须设置为 **No Pending Operation**，和 **Certificate Operation Status** 设置为 **Upgrade Success**。



16. 请参阅步骤。7-13，以保护要用于保护CUCM的SIP的其他代理设备。

验证

要验证SIP信令是否受到适当保护，请执行以下步骤：

1. 打开到vCUBE的SSH会话，运行命令 `show sip-ua connections tcp tls detail`，并确认当前未与CVP(198.18.133.13)建立TLS连接。

```
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;
```



注意：此时，在CUCM(198.18.133.3)上仅启用一个与CUCM的SIP选项的活动TLS会话。如果未启用SIP选项，则不存在SIP TLS连接。

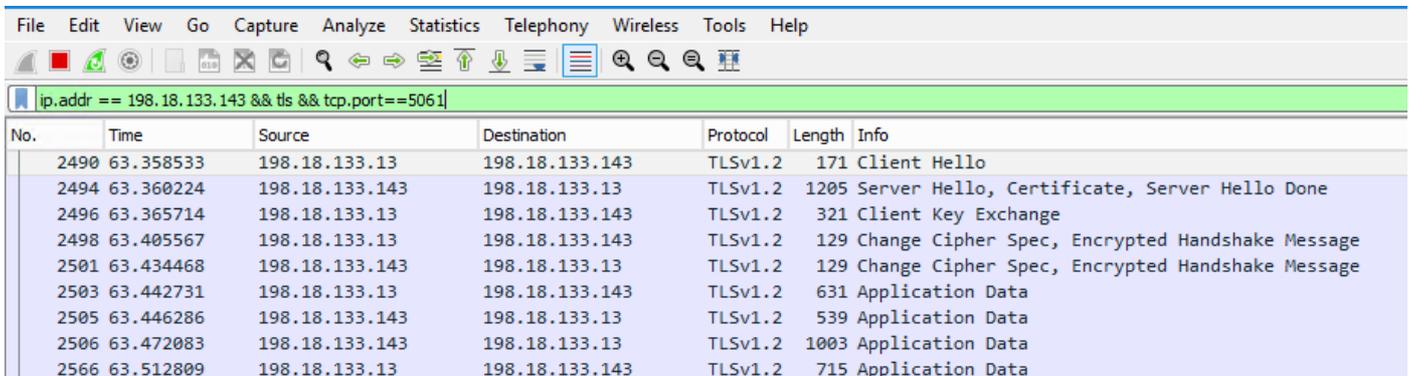
2. 登录到CVP并启动Wireshark。
3. 拨打联系中心号码。
4. 导航到CVP会话；在Wireshark上，运行此过滤器以使用CUBE检查SIP信令：
`ip.addr == 198.18.133.226 && tls && tcp.port==5061`

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

检查：是否已建立SIP over TLS连接？如果是，输出确认CVP和CUBE之间的SIP信号是安全的。

5.检查CVP和CVVB之间的SIP TLS连接。在同一Wireshark会话中，运行此过滤器：

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



The image shows a Wireshark interface with a filter applied: `ip.addr == 198.18.133.143 && tls && tcp.port==5061`. The packet list table below shows the following details:

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

检查：是否已建立SIP over TLS连接？如果是，输出确认CVP和CVVB之间的SIP信号是安全的。

6.您还可以从CUBE验证与CVP的SIP TLS连接。导航到vCUBE SSH会话，并运行此命令以检查安全SIP信号：

```
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

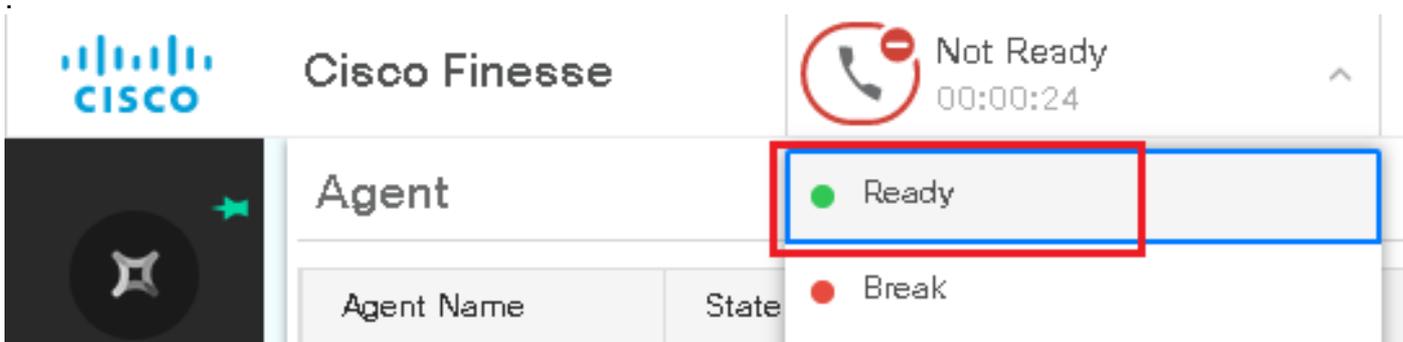
Remote-Agent:198.18.133.13, Connections-Count:1
  Remote-Port Conn-Id Conn-State WriteQ-Size Local-Address TLS-Version
  =====
      5061      3 Established      0      -      TLSv1.2

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

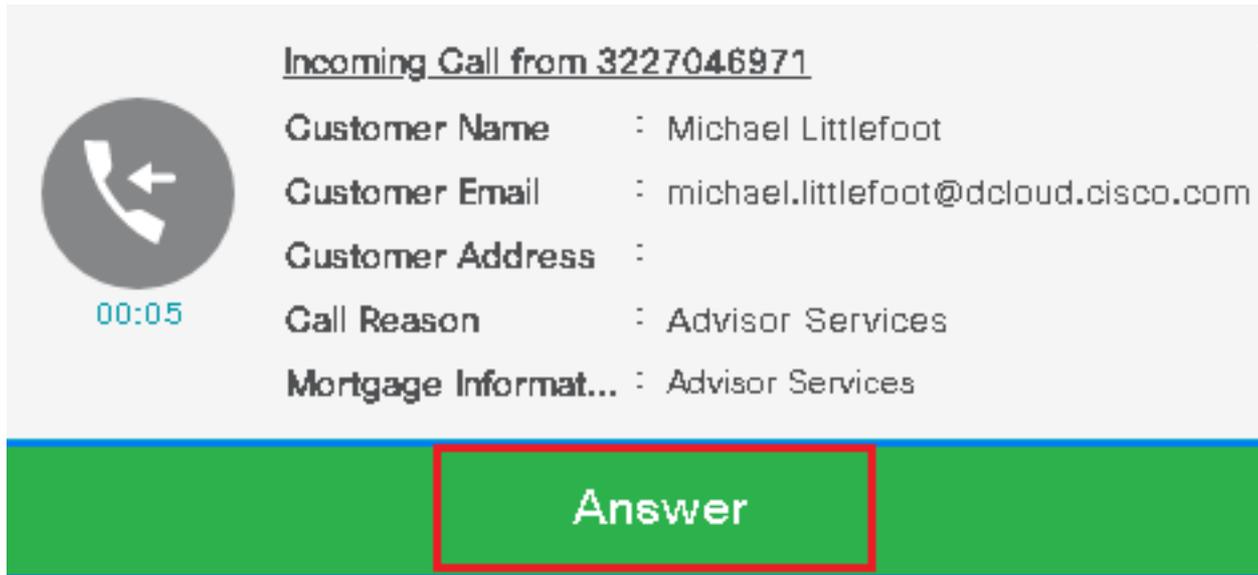
检查：是否与CVP建立了SIP over TLS连接？如果是，输出确认CVP和CUBE之间的SIP信号是安全的。

7.此时，呼叫处于活动状态，您听到保留音乐(MOH)，因为没有座席可以应答呼叫。

8.使座席能够应答呼叫。



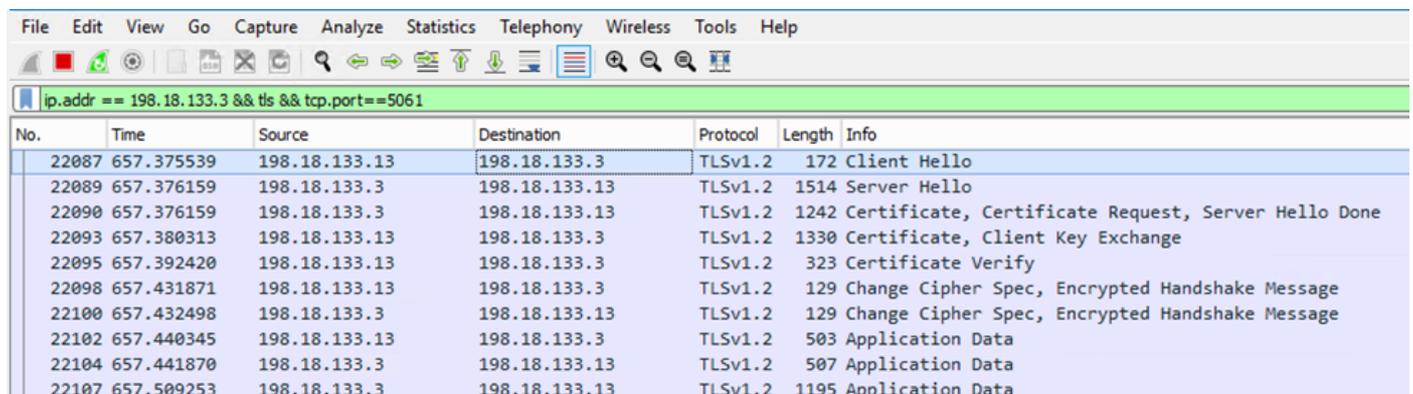
9.座席将被保留，并且呼叫被路由到他/她。点击 Answer 接听电话。



The image shows a call notification interface. On the left is a circular icon with a telephone handset and a left-pointing arrow, with a timer below it showing '00:05'. To the right of the icon, the text reads: 'Incoming Call from 3227046971', 'Customer Name : Michael Littlefoot', 'Customer Email : michael.littlefoot@dcloud.cisco.com', 'Customer Address :', 'Call Reason : Advisor Services', and 'Mortgage Informat... : Advisor Services'. At the bottom of the notification is a green bar with a red border containing the word 'Answer' in white text.

10.呼叫连接到座席。

11.为了验证CVP和CUCM之间的SIP信号，请导航到CVP会话，并在Wireshark中运行此过滤器：
ip.addr == 198.18.133.3 && tls && tcp.port==5061



The image shows a Wireshark network traffic capture. The filter bar at the top contains the filter: 'ip.addr == 198.18.133.3 && tls && tcp.port==5061'. The main pane displays a list of captured packets, all of which are TLSv1.2 messages between 198.18.133.3. The packets include Client Hello, Server Hello, Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, and Application Data.

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

检查：是否所有与CUCM(198.18.133.3)的SIP通信都通过TLS?如果是，输出确认CVP和CUCM之间的SIP信号是安全的。

故障排除

如果未建立TLS，请在CUBE上运行以下命令以启用debug TLS进行故障排除：

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

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。