在Contact Center Enterprise中配置安全RTP

目录

简介

本文档介绍如何保护联系中心企业版(CCE)综合呼叫流中的实时传输协议(SRTP)流量。

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，但它也适用于以前的版本。

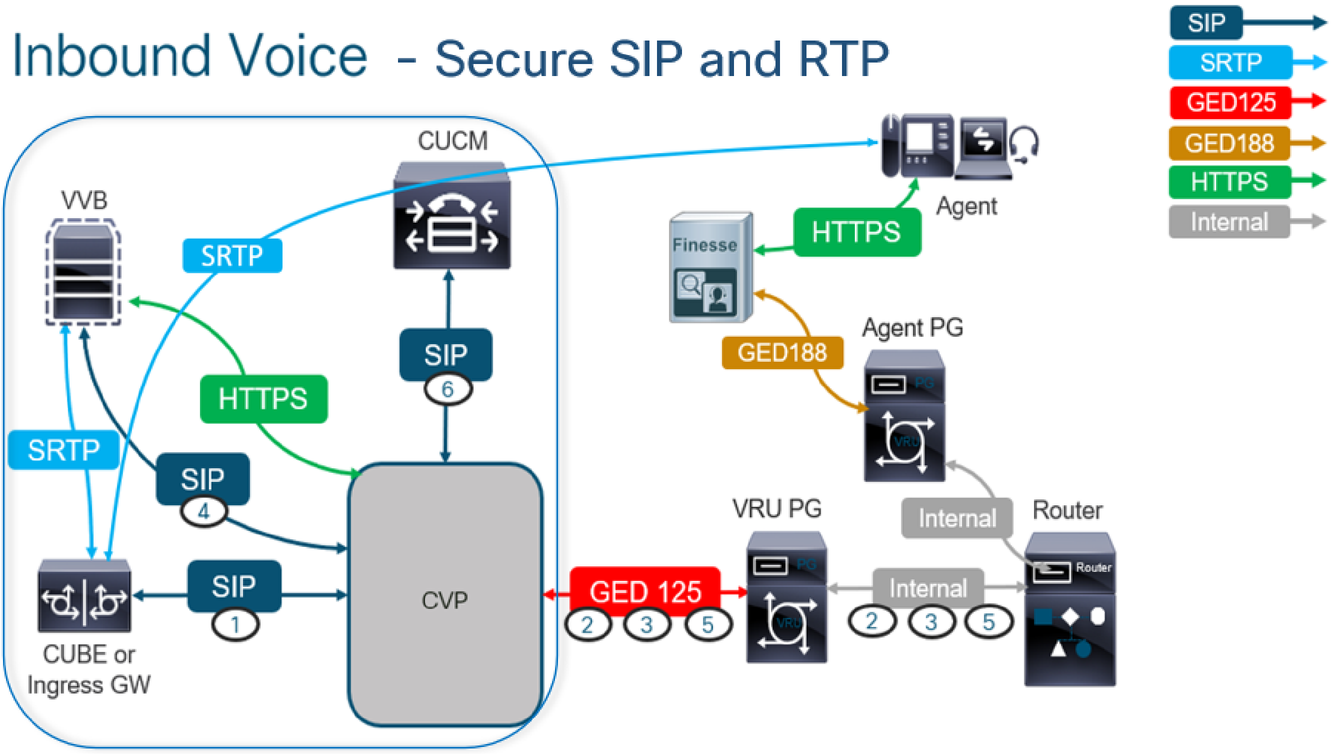
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原

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

> **注意**：在联系中心综合呼叫流程中，为了启用安全RTP，必须启用安全SIP信号。因此，本文档中的配置同时启用安全SIP和SRTP。

下图显示了联系中心综合呼叫流程中涉及SIP信号和RTP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上开始配置。接下来，配置CVP、CVVB和CUCM。



任务1:CUBE安全配置

在本任务中，您将配置CUBE以保护SIP协议消息和RTP。

所需的配置：

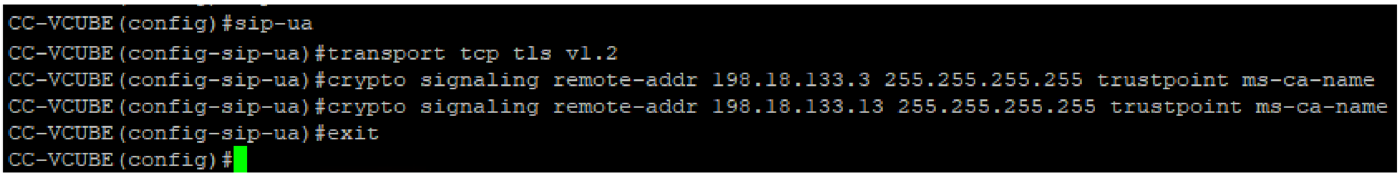
- 为SIP UA配置默认信任点
- 修改拨号对等体以使用TLS和SRTP

步骤：

1. 打开到CUBE的SSH会话。

2. 运行这些命令以使SIP堆栈使用CUBE的CA证书。CUBE建立从/到CUCM(198.18.133.3)和CVP(198.18.133.13)的SIP TLS连接：

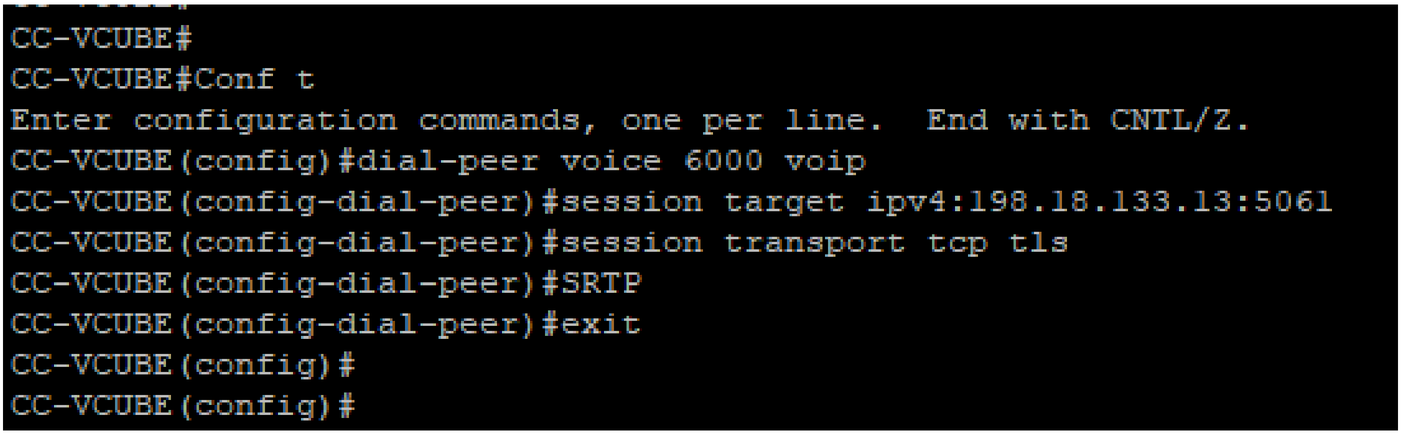
```
Conf t Sip-ua Transport tcp tls v1.2 crypto signaling remote-addr 198.18.133.3 255.255.255.255 trustpoint ms-ca-name crypto
signaling remote-addr 198.18.133.13 255.255.255.255 trustpoint ms-ca-name exit
```



```
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 srtp exit



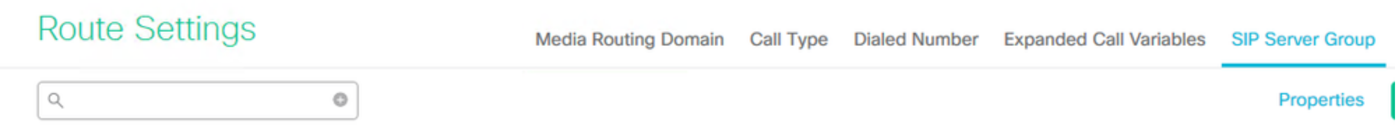
```
CC-VCUBE#
CC-VCUBE#Conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CC-VCUBE(config)#dial-peer voice 6000 voip
CC-VCUBE(config-dial-peer)#session target ipv4:198.18.133.13:5061
CC-VCUBE(config-dial-peer)#session transport tcp tls
CC-VCUBE(config-dial-peer)#SRTP
CC-VCUBE(config-dial-peer)#exit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

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：

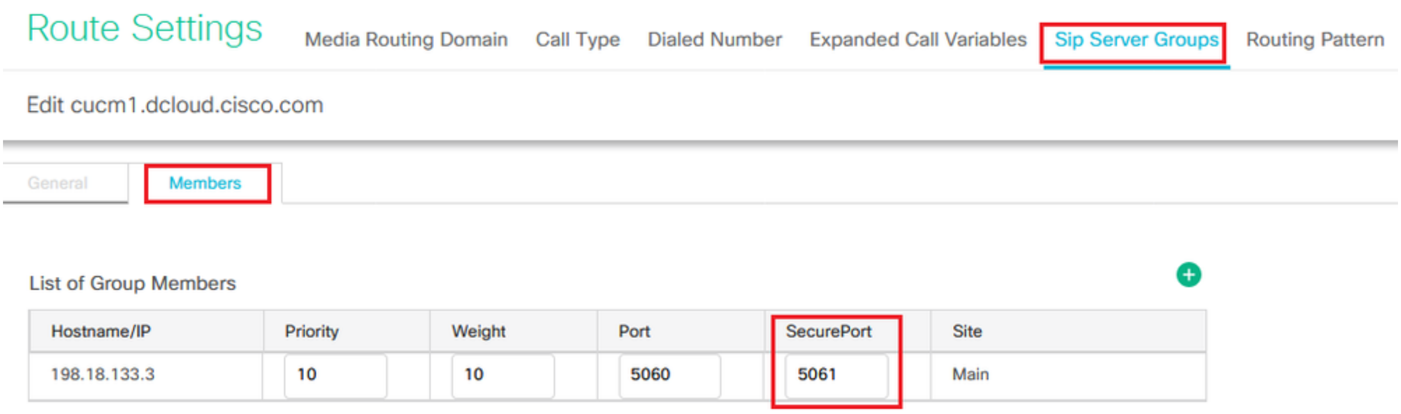
1. 登录 UCCE Web Administration.
2. 导航至 Call Settings > Route Settings > SIP Server Group.



根据您的配置，您已为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 选项卡显示SIP服务器组配置的详细信息。设置 SecurePort 到 5061 并点击 Save.

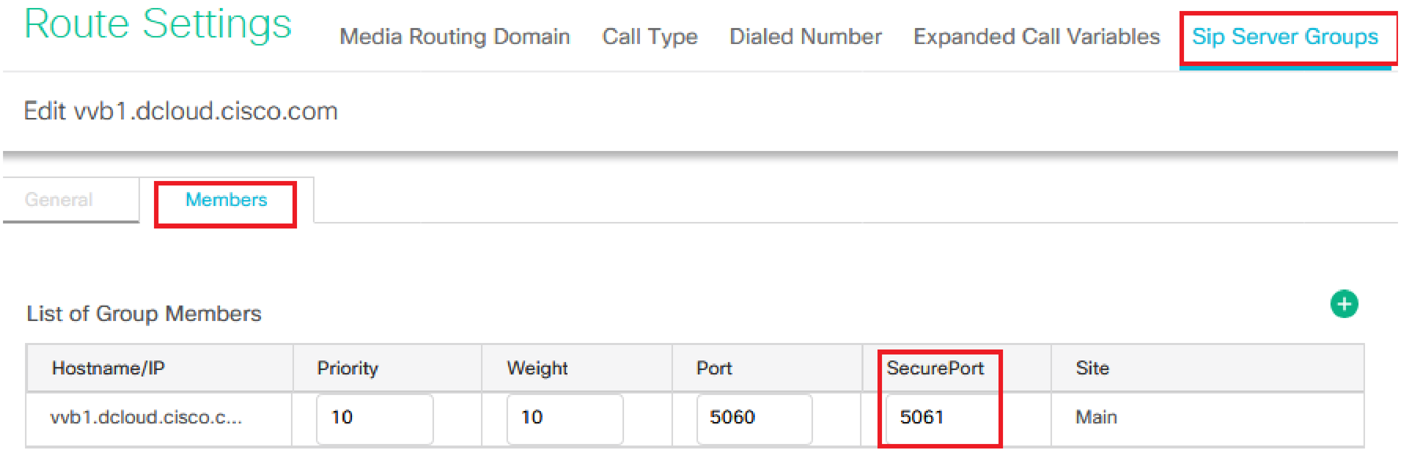


Edit cucm1.dcloud.cisco.com

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，设置 **SecurePort** 到 5061 并点击 Save.



Edit vvb1.dcloud.cisco.com

List of Group Members

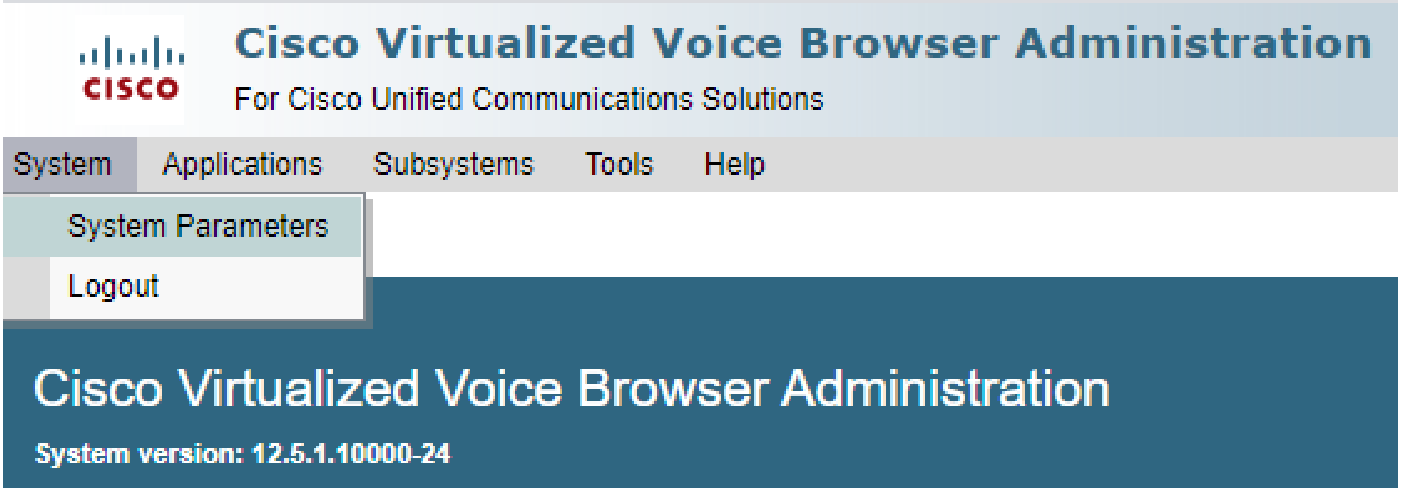
Hostname/IP	Priority	Weight	Port	SecurePort	Site
vvb1.dcloud.cisco.c...	10	10	5060	5061	Main

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)和SRTP。

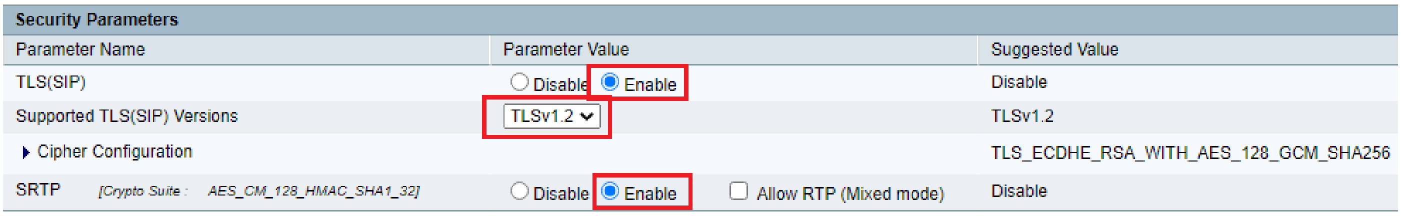
步骤：

1. 打开 Cisco VVB Admin 页码.
2. 导航至 System > System Parameters.


cisco
Cisco Virtualized Voice Browser Administration
For Cisco Unified Communications Solutions
System
Applications
Subsystems
Tools
Help
System Parameters
Logout
Cisco Virtualized Voice Browser Administration

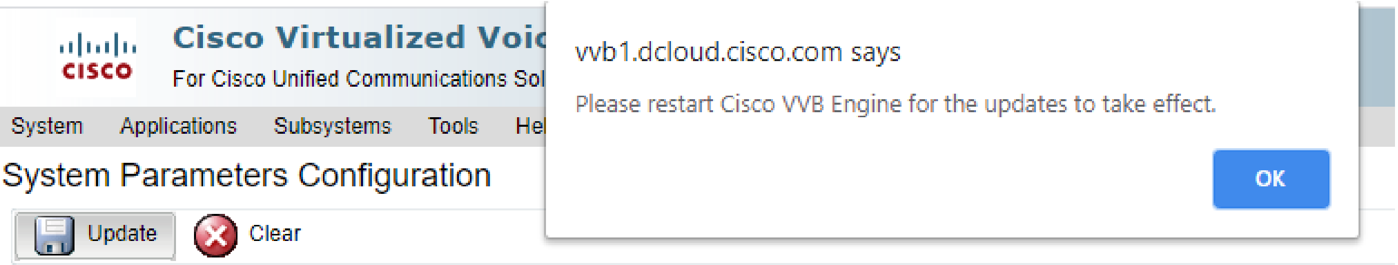
System version: 12.5.1.10000-24

3. 在 Security Parameters 部分，选择 Enable 对于 TLS (SIP) .保留 Supported TLS(SIP) version as TLSv1.2 选择 Enable 对于 SRTP.



Security Parameters		
Parameter Name	Parameter Value	Suggested Value
TLS(SIP)	○ Disable ● Enable	Disable
Supported TLS(SIP) Versions	TLSv1.2	TLSv1.2
▸ Cipher Configuration		TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
SRTP [Crypto Suite : AES_CM_128_HMAC_SHA1_32]	○ Disable ● Enable □ Allow RTP (Mixed mode)	Disable

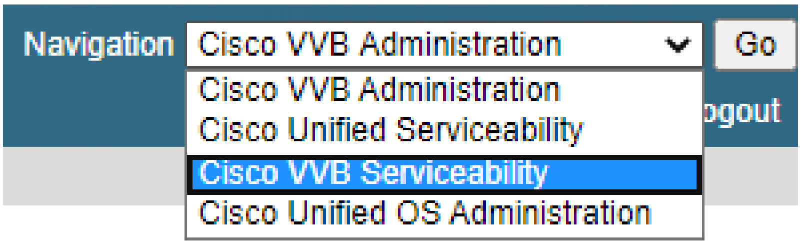
4. 点击 **Update.**点击 Ok 提示重新启动CVVB引擎时。



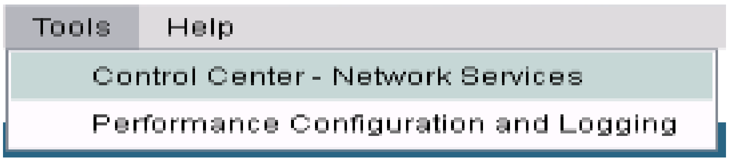
vvb1.dcloud.cisco.com says

Please restart Cisco VVB Engine for the updates to take effect.

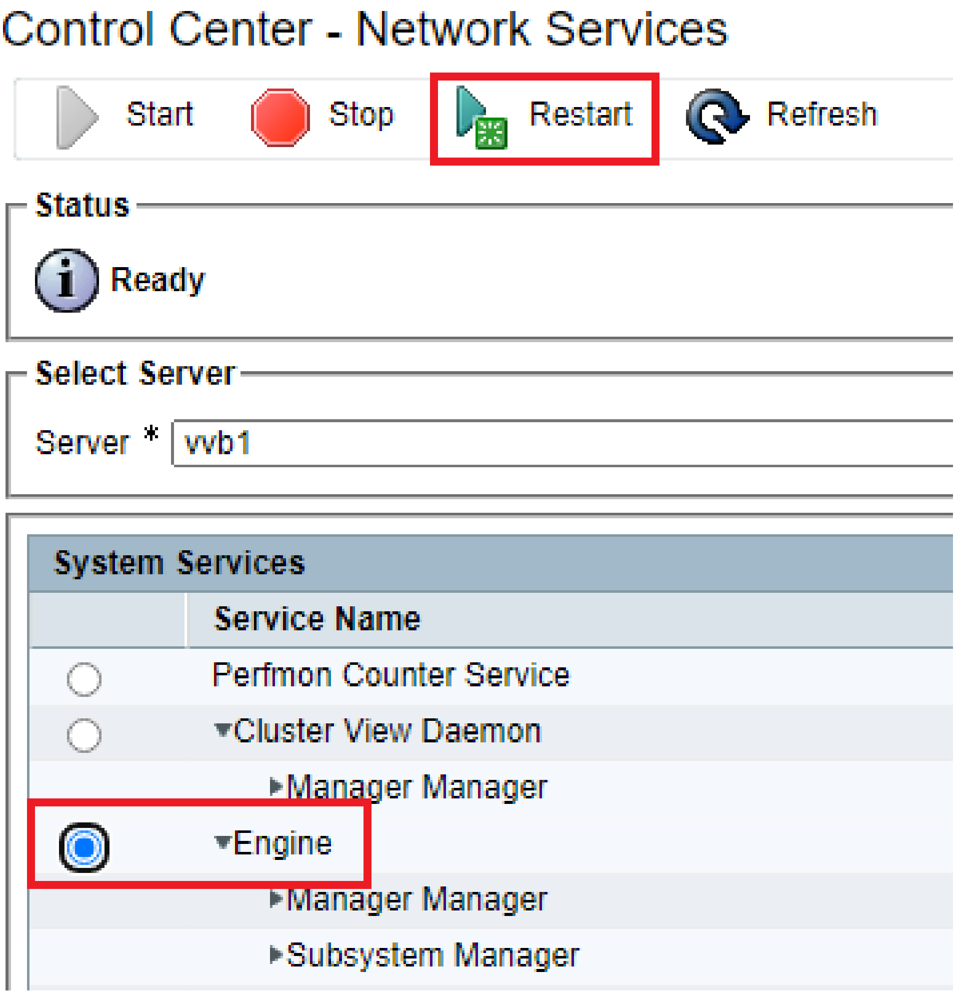
5. 这些更改需要重新启动Cisco VVB引擎。要重新启动VVB引擎，请导航至 Cisco VVB Serviceability ，然后单击 **Go.**



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


Tools
Help
Control Center - Network Services
Performance Configuration and Logging

7. 选择 Engine 并点击 Restart.



Control Center - Network Services

Status

Ready

Select Server

Server * vvb1

System Services

	Service Name
○	Perfmon Counter Service
○	▾Cluster View Daemon
	▸Manager Manager
●	▾Engine
	▸Manager Manager
	▸Subsystem Manager

任务4:CUCM安全配置

要保护CUCM上的SIP消息和RTP，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中继并启用SRTP
- 安全代理与CUCM的设备通信

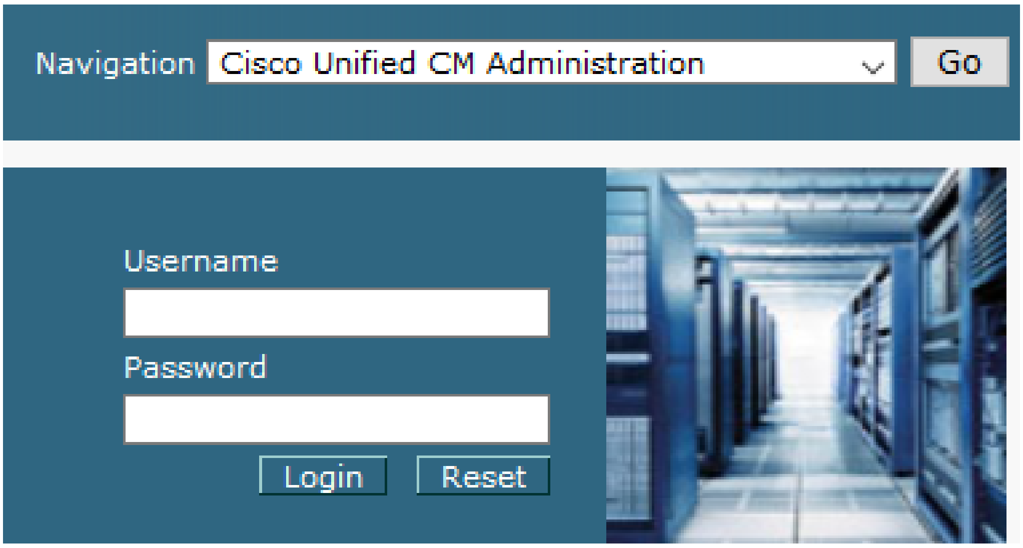
将CUCM安全模式设置为混合模式

CUCM支持两种安全模式：

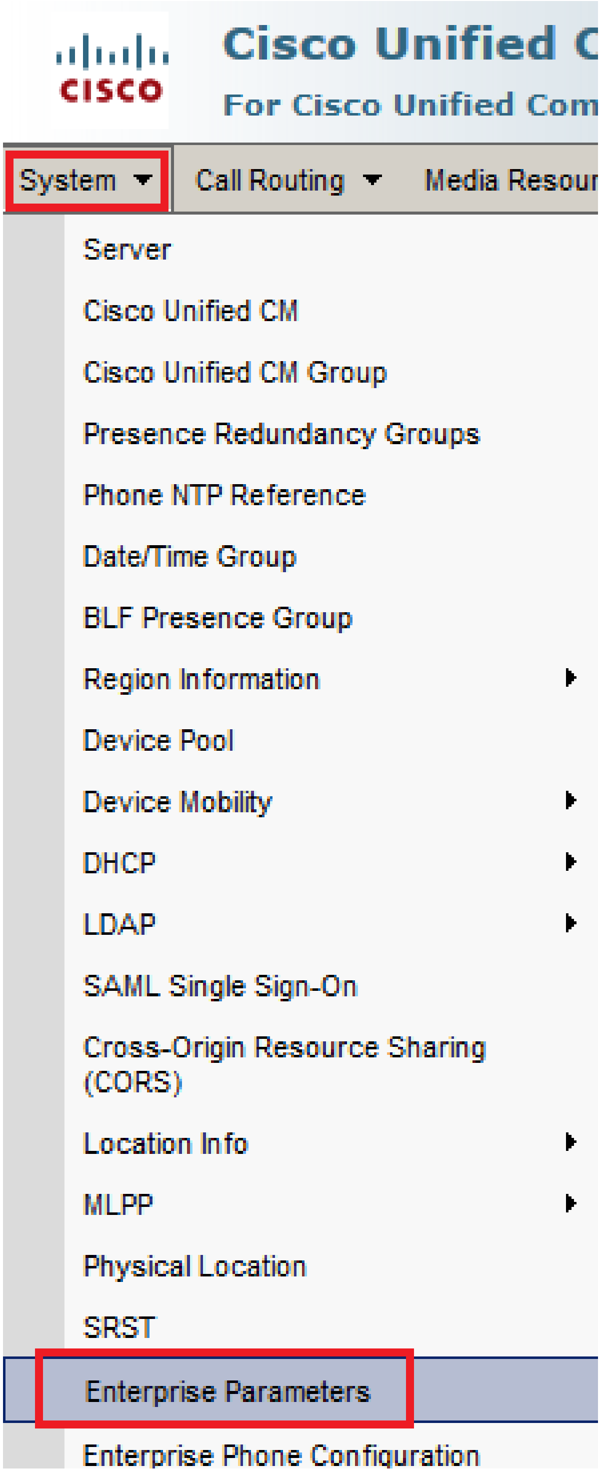
- 非安全模式（默认模式）
- 混合模式（安全模式）

步骤：

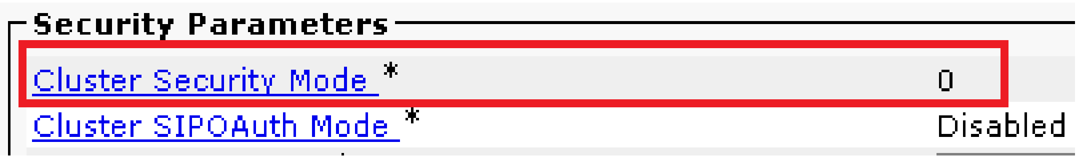
1. 登录到CUCM管理界面。



2. 登录到CUCM时，可以导航到 **System > Enterprise Parameters**.



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



Security Parameters

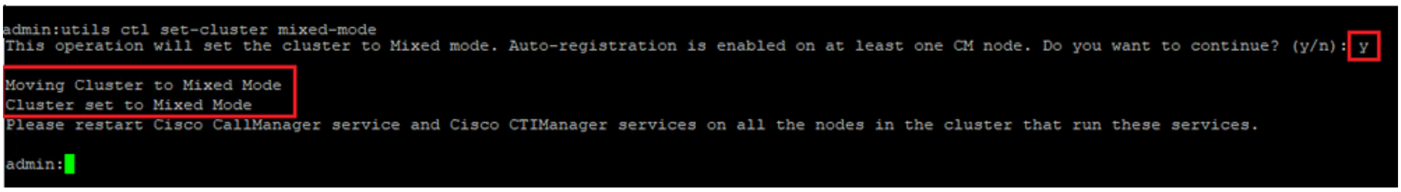
Cluster Security Mode * 0

Cluster SIPOAuth Mode * Disabled

4. 如果Cluster Security Mode设置为0，则表示集群安全模式设置为non-secure。您需要从CLI启用混合模式。
5. 打开到CUCM的SSH会话。
6. 成功通过SSH登录CUCM后，请运行以下命令：

utils ctl set-cluster mixed-mode

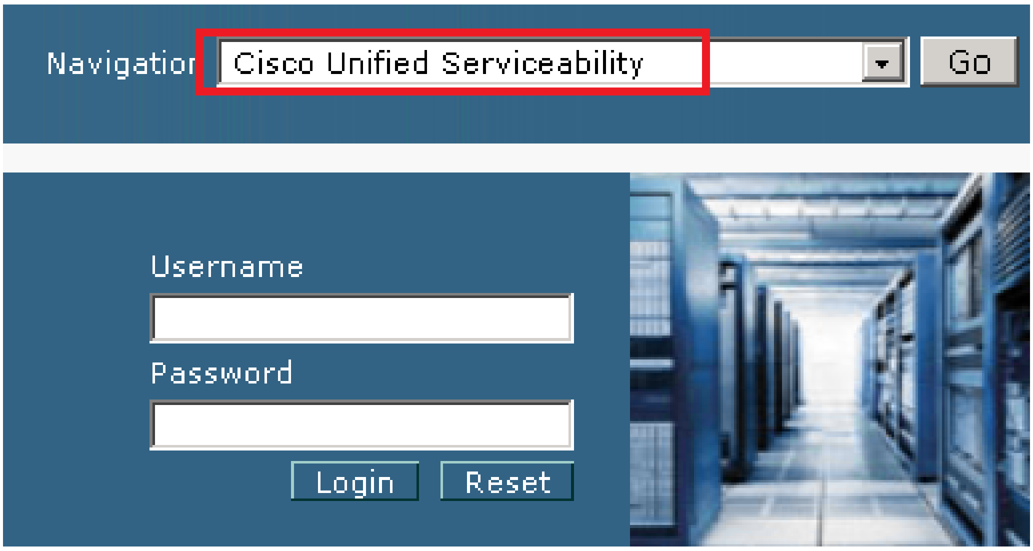
7. 类型 y 并点击 Enter 系统提示时。此命令将集群安全模式设置为混合模式。



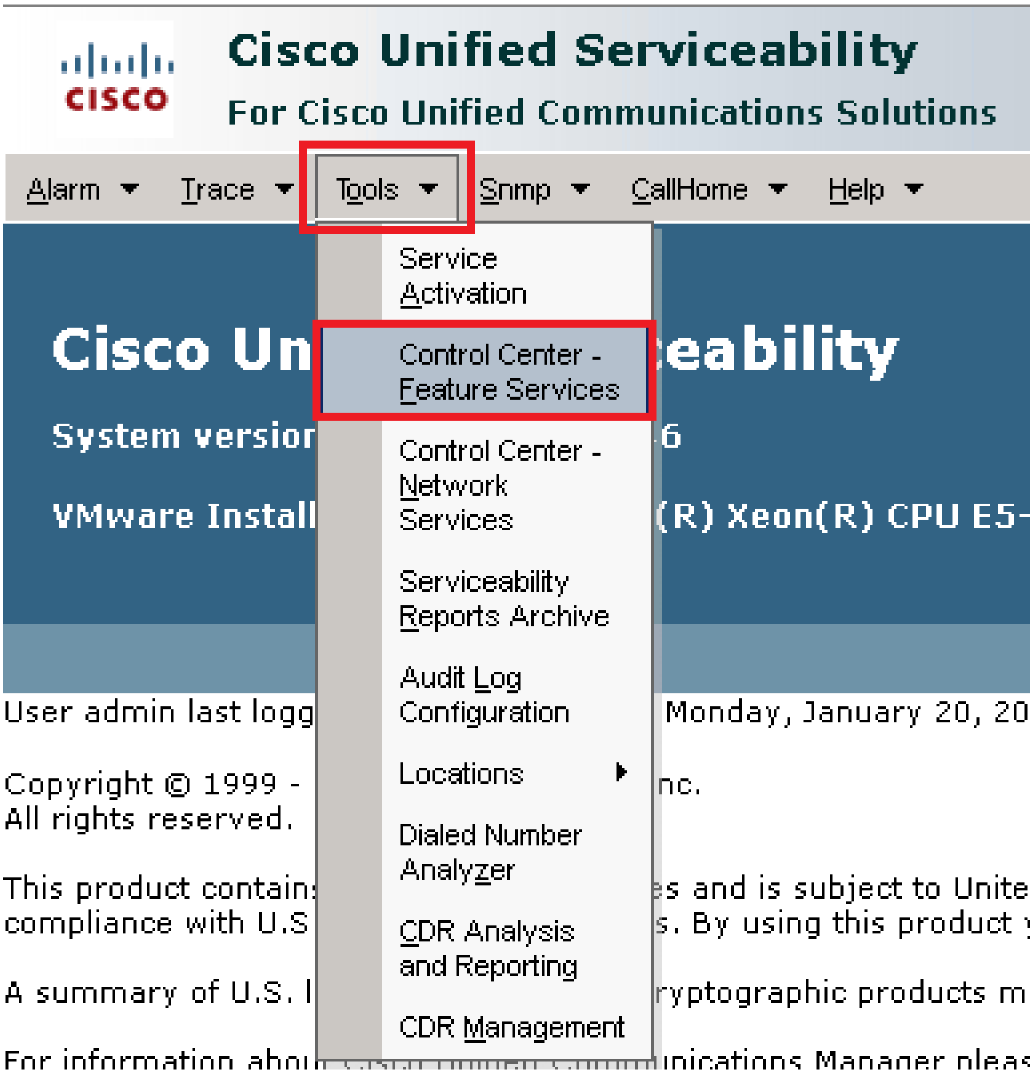
```
admin:utils ctl set-cluster mixed-mode
This operation will set the cluster to Mixed mode. Auto-registration is enabled on at least one CM node. Do you want to continue? (y/n): y

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.


Cisco Unified Serviceability
For Cisco Unified Communications Solutions
Alarm
Trace
Tools
Snmp
CallHome
Help
Service Activation
Control Center - Feature Services
Control Center - Network Services
Serviceability Reports Archive
Audit Log Configuration
Locations
Dialed Number Analyzer
CDR Analysis and Reporting
CDR Management

Cisco Un eability

System versior 6

VMware Install (R) Xeon(R) CPU E5-

User admin last logg Monday, January 20, 20

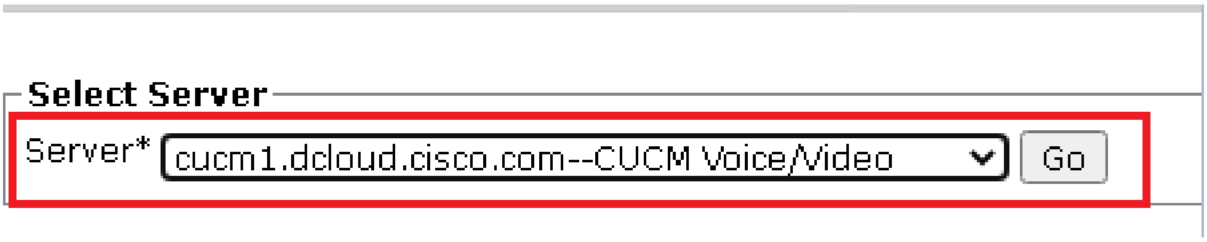
Copyright © 1999 - nc.
All rights reserved.

This product contain es and is subject to Unite
compliance with U.S s. By using this product

A summary of U.S. l ryptographic products m

For information abou nications Manager pleas

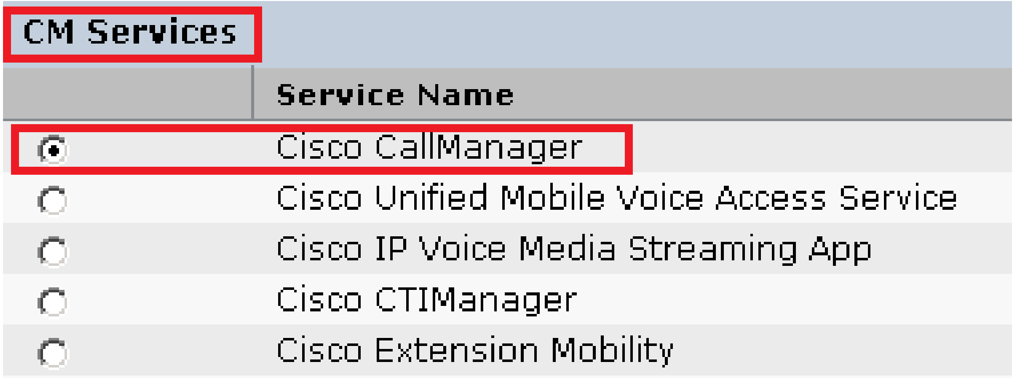
11. 选择服务器，然后单击 Go.



Select Server

Server* cucm1.dcloud.cisco.com--CUCM Voice/Video Go

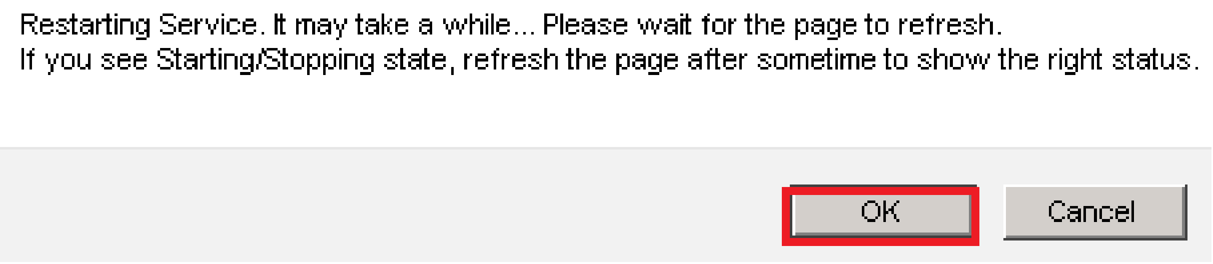
12. 在CM服务下，选择 Cisco CallManager ，然后单击 Restart 按钮。



CM Services

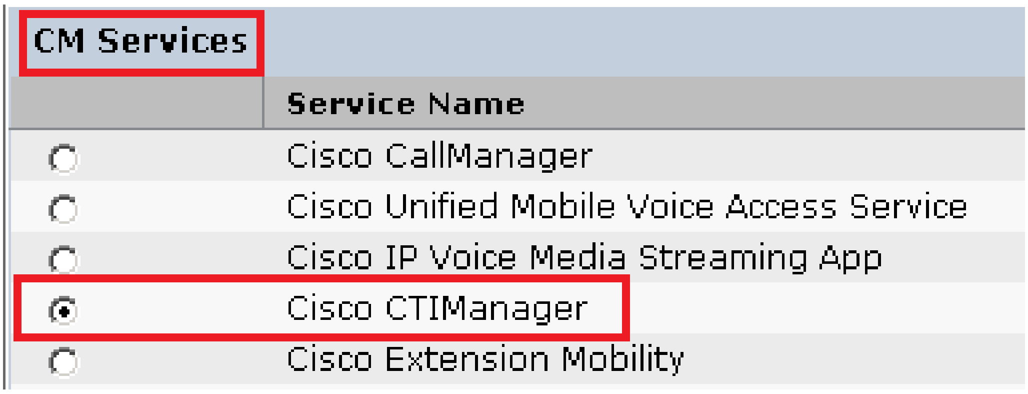
	Service Name
●	Cisco CallManager
○	Cisco Unified Mobile Voice Access Service
○	Cisco IP Voice Media Streaming App
○	Cisco CTIManager
○	Cisco Extension Mobility

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.

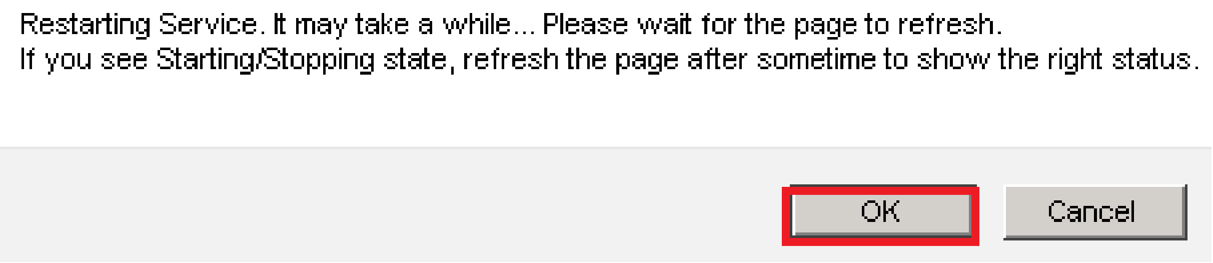
14. 在成功重新启动 Cisco CallManager，选择 **Cisco CTIManager** ？？然后单击 Restart 按钮重启 Cisco CTIManager 服务。



CM Services

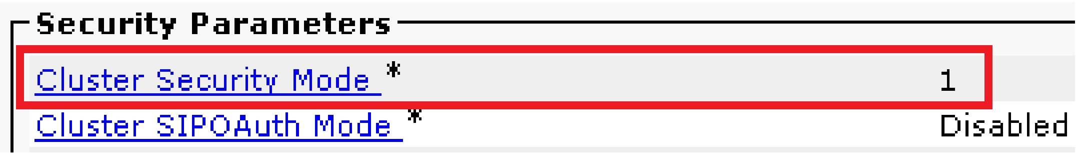
	Service Name
○	Cisco CallManager
○	Cisco Unified Mobile Voice Access Service
○	Cisco IP Voice Media Streaming App
●	Cisco CTIManager
○	Cisco Extension Mobility

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. 成功重新启动服务后，为了验证集群安全模式是否设置为混合模式，请按照步骤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.



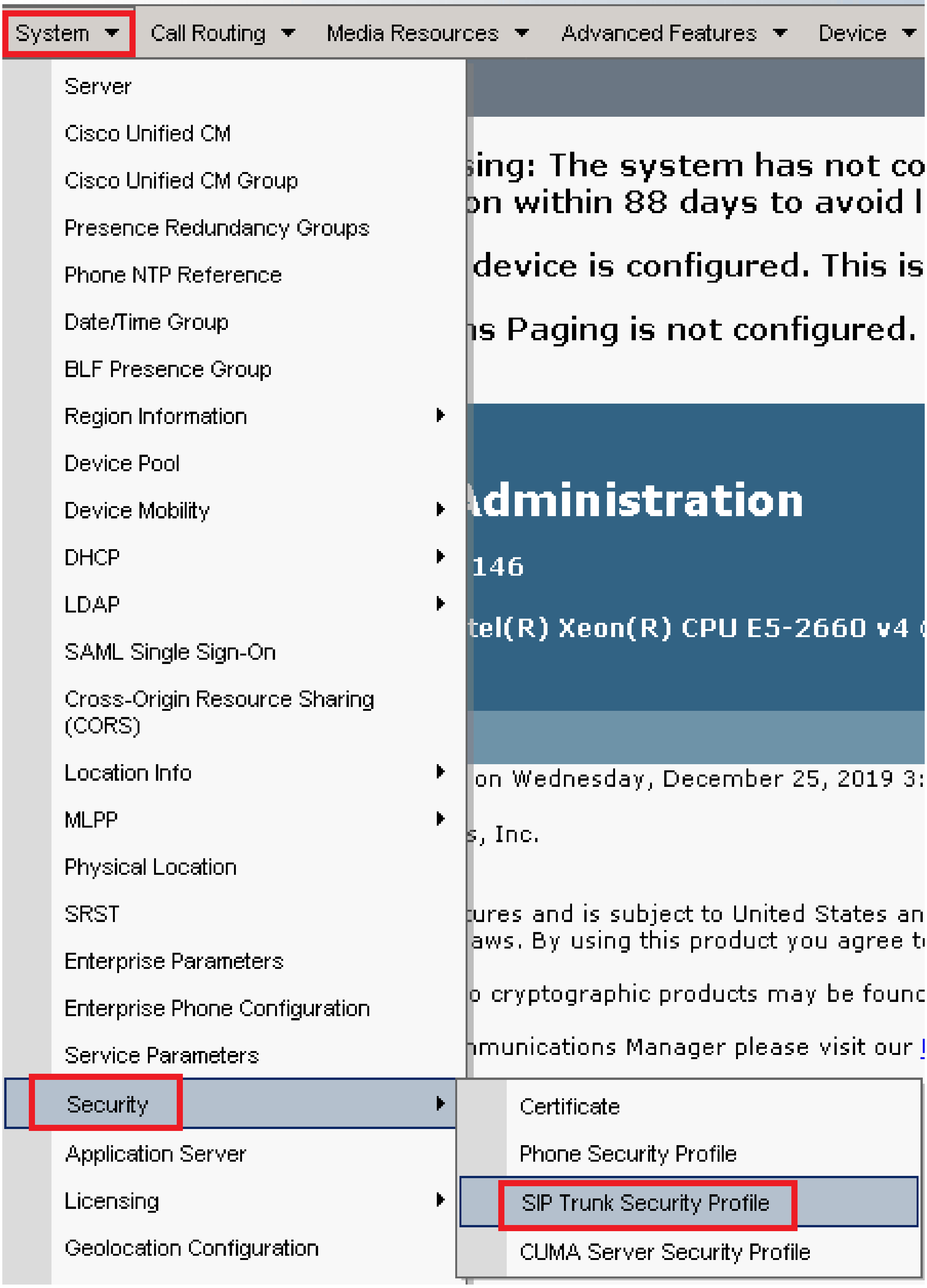
Security Parameters

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管理界面。
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。



sing: The system has not co
on within 88 days to avoid l

device is configured. This is

ns Paging is not configured.

Administration

146

tel(R) Xeon(R) CPU E5-2660 v4 (

on Wednesday, December 25, 2019 3:

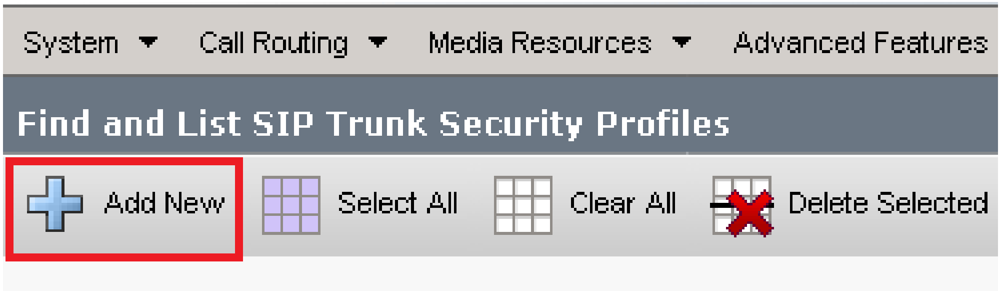
s, Inc.

tures and is subject to United States an
aws. By using this product you agree t

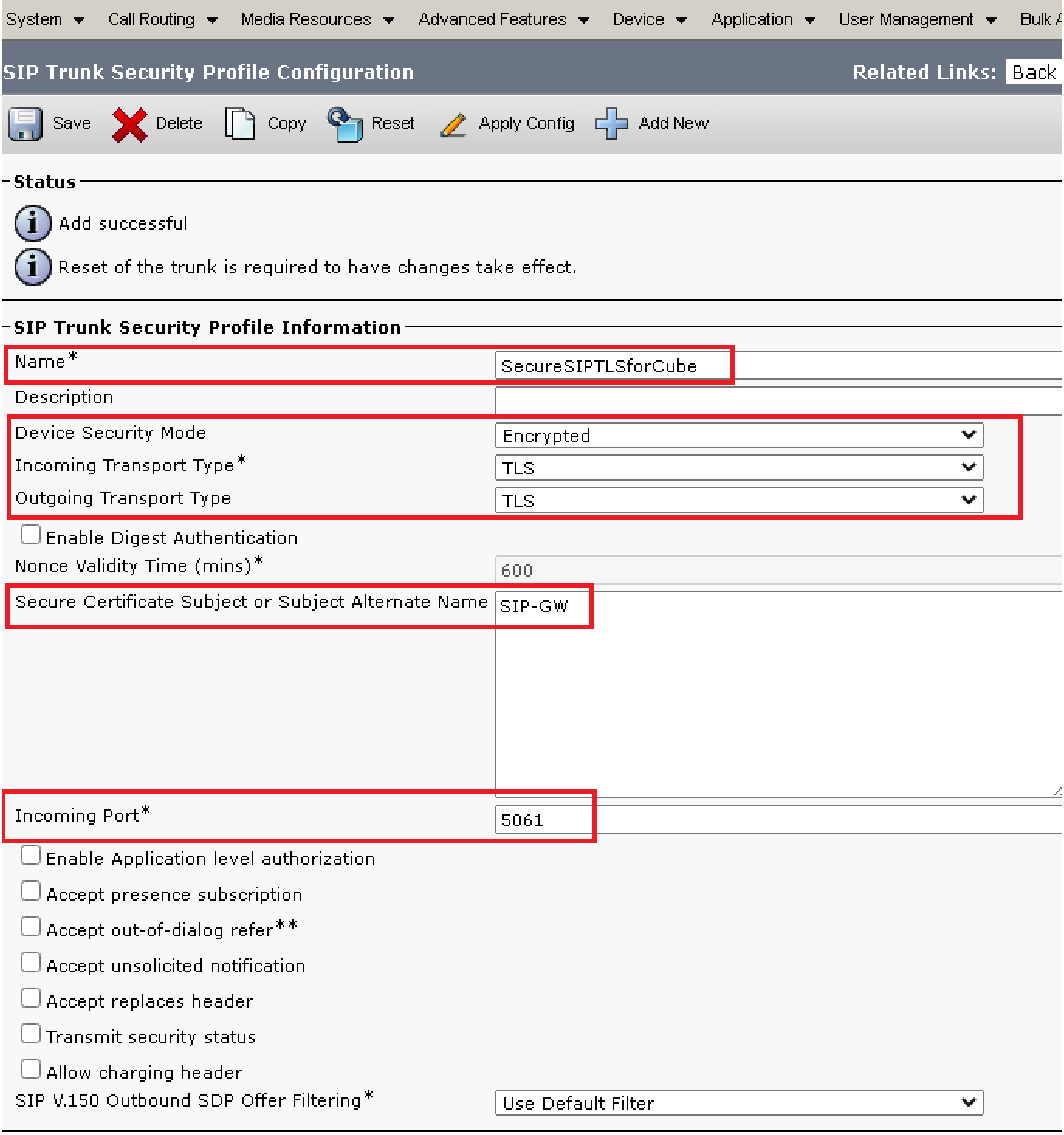
o cryptographic products may be founc

nmunications Manager please visit our

3. 在左上角，单击**Add New**添加新配置文件。



4. 配置 SIP Trunk Security Profile 作为此图像，然后单击 Save 在页面左下角。



Status

Add successful

Reset of the trunk is required to have changes take effect.

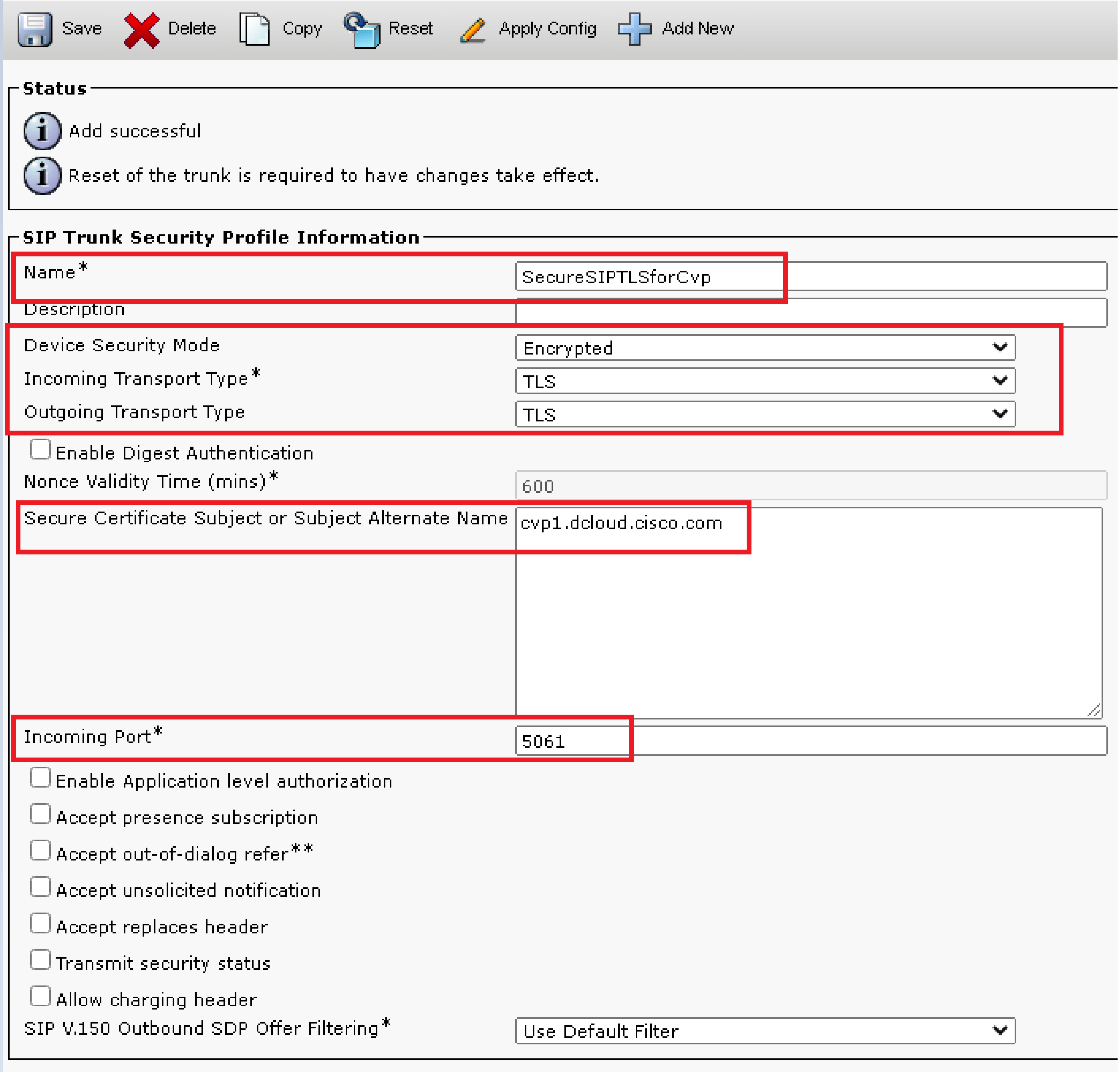
SIP Trunk Security Profile Information

Name*	SecureSIPTLSforCube
Description	
Device Security Mode	Encrypted
Incoming Transport Type*	TLS
Outgoing Transport Type	TLS
□ Enable Digest Authentication	
Nonce Validity Time (mins)*	600
Secure Certificate Subject or Subject Alternate Name	SIP-GW
Incoming Port*	5061
□ Enable Application level authorization	
□ Accept presence subscription	
□ Accept out-of-dialog refer**	
□ Accept unsolicited notification	
□ Accept replaces header	
□ Transmit security status	
□ Allow charging header	
SIP V.150 Outbound SDP Offer Filtering*	Use Default Filter

5.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.Change（更改） 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。



Status

Add successful

Reset of the trunk is required to have changes take effect.

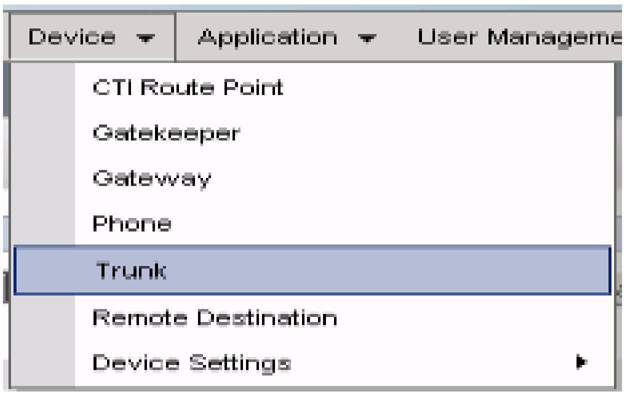
SIP Trunk Security Profile Information

Name*	SecureSIPTLSforCvp
Description	
Device Security Mode	Encrypted
Incoming Transport Type*	TLS
Outgoing Transport Type	TLS
□ Enable Digest Authentication	
Nonce Validity Time (mins)*	600
Secure Certificate Subject or Subject Alternate Name	cvp1.dcloud.cisco.com
Incoming Port*	5061
□ Enable Application level authorization	
□ Accept presence subscription	
□ Accept out-of-dialog refer**	
□ Accept unsolicited notification	
□ Accept replaces header	
□ Transmit security status	
□ Allow charging header	
SIP V.150 Outbound SDP Offer Filtering*	Use Default Filter

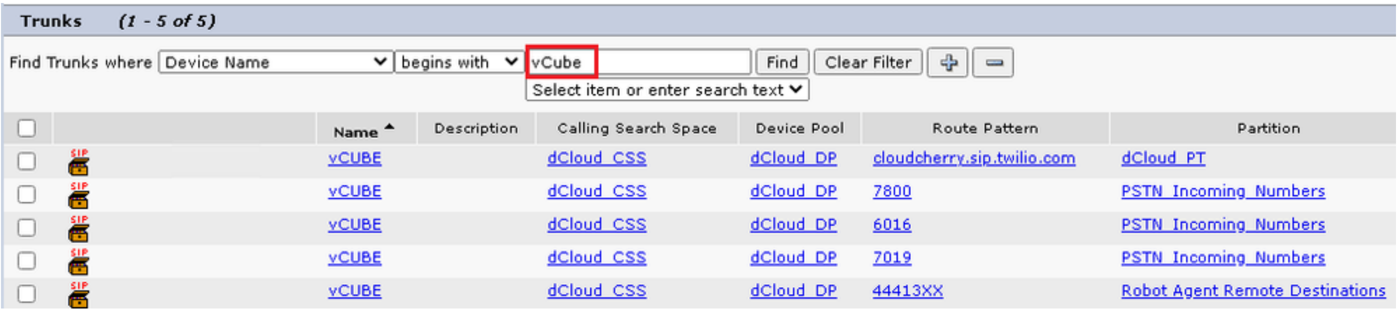
将SIP中继安全配置文件关联到各自的SIP中继并启用SRTP

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，然后单击Find.



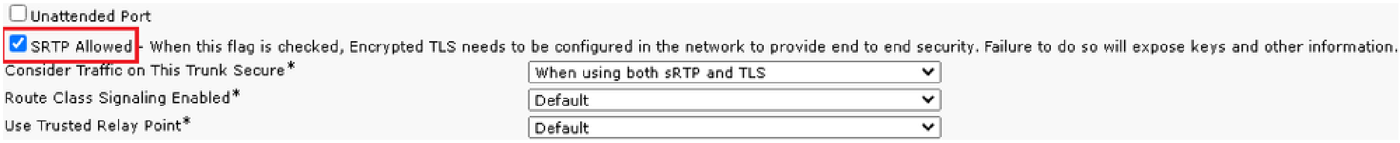
Trunks (1 - 5 of 5)

Find Trunks where Device Name begins with vCube [Find] [Clear Filter]
Select item or enter search text

□		Name	Description	Calling Search Space	Device Pool	Route Pattern	Partition
□	SIP	vCUBE		dCloud_CSS	dCloud_DP	cloudcherry.sip.twilio.com	dCloud_PT
□	SIP	vCUBE		dCloud_CSS	dCloud_DP	7800	PSTN_Incoming_Numbers
□	SIP	vCUBE		dCloud_CSS	dCloud_DP	6016	PSTN_Incoming_Numbers
□	SIP	vCUBE		dCloud_CSS	dCloud_DP	7019	PSTN_Incoming_Numbers
□	SIP	vCUBE		dCloud_CSS	dCloud_DP	44413XX	Robot Agent Remote Destinations

3. 点击vCUBE 打开vCUBE中继配置页面。

4. 在Device Information 部分，请检查SRTP Allowed 复选框以启用SRTP。



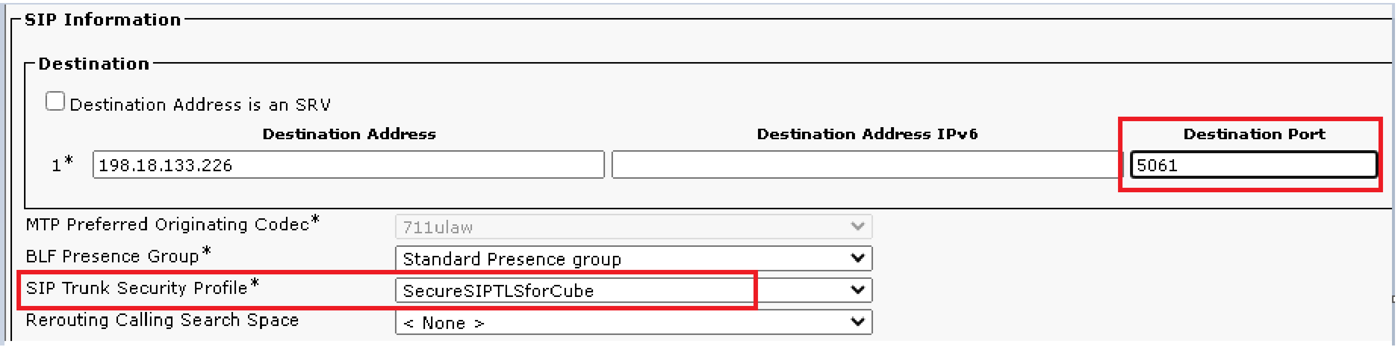
□ Unattended Port

☑ 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*	When using both sRTP and TLS
Route Class Signaling Enabled*	Default
Use Trusted Relay Point*	Default

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

6. Change（更改）SIP Trunk Security Profile 到SecureSIPTLSForCube.



SIP Information

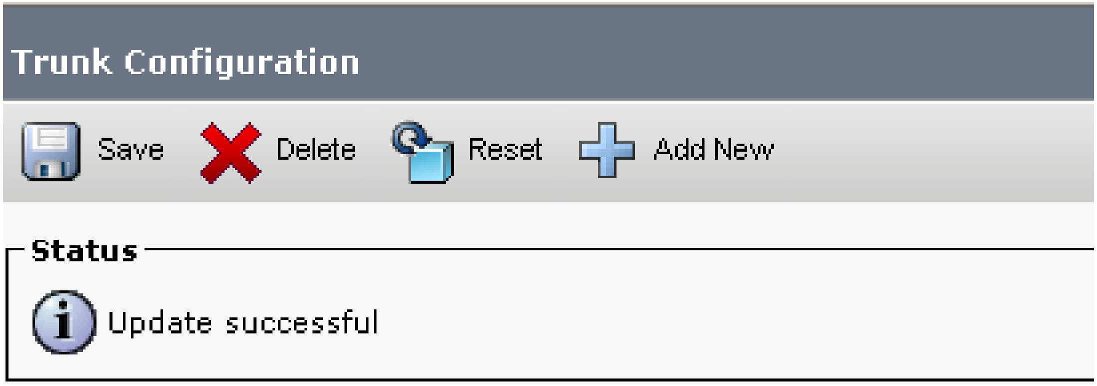
Destination

□ 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 >

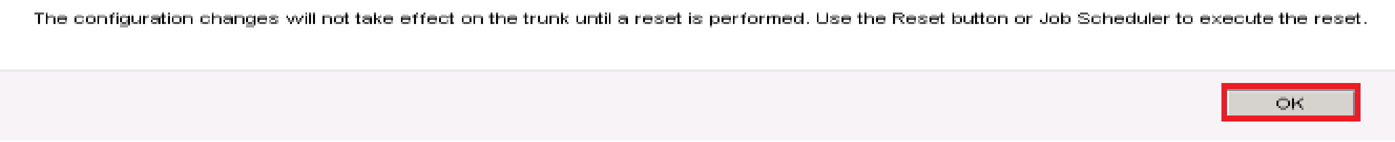
7. 点击Save 然后Rest 到save 并应用更改。



Trunk Configuration

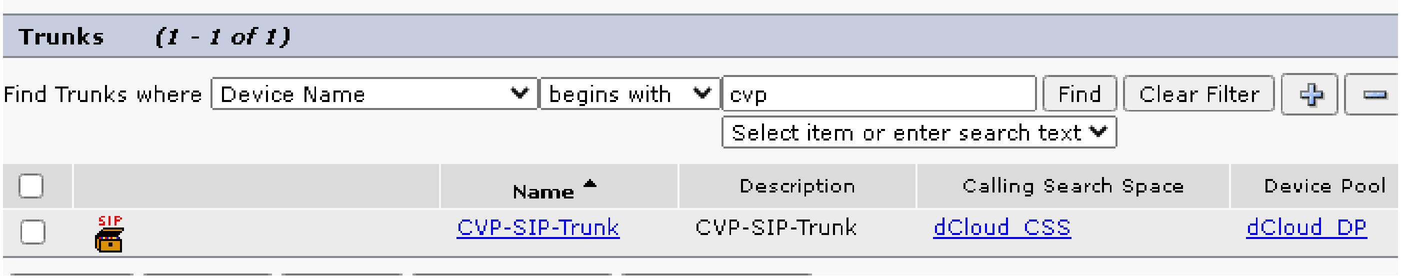
Status

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.

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

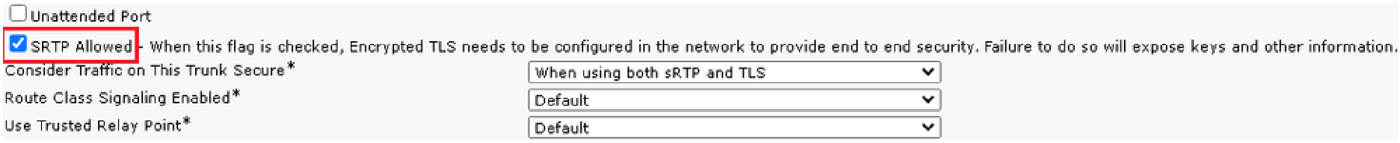


Trunks (1 - 1 of 1)

Find Trunks where Device Name begins with cvp

□		Name	Description	Calling Search Space	Device Pool
□	SIP	CVP-SIP-Trunk	CVP-SIP-Trunk	dCloud_CSS	dCloud_DP

9. 点击 CVP-SIP-Trunk 打开CVP中继配置页面。
10. 在 Device Information 部分，检查 SRTP Allowed 复选框以启用SRTP。

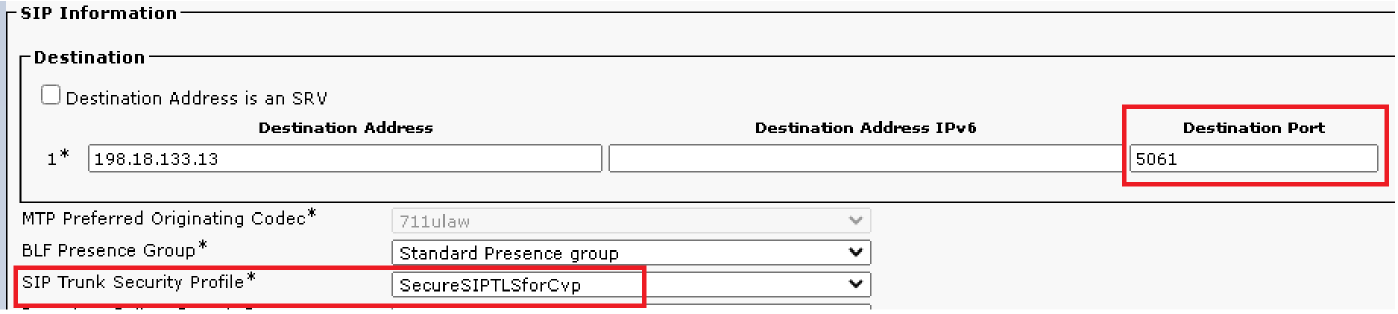


□ Unattended Port

☑ 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*	When using both sRTP and TLS
Route Class Signaling Enabled*	Default
Use Trusted Relay Point*	Default

11. 向下滚动到 SIP Information 部分，更改 Destination Port 到 5061.
12. Change（更改） SIP Trunk Security Profile 到 SecureSIPTLSForCvp.



SIP Information

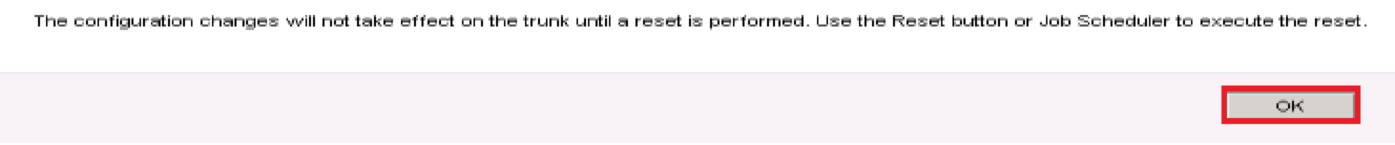
Destination

□ 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

13. 点击 Save 然后 Rest 到 save 并应用更改。



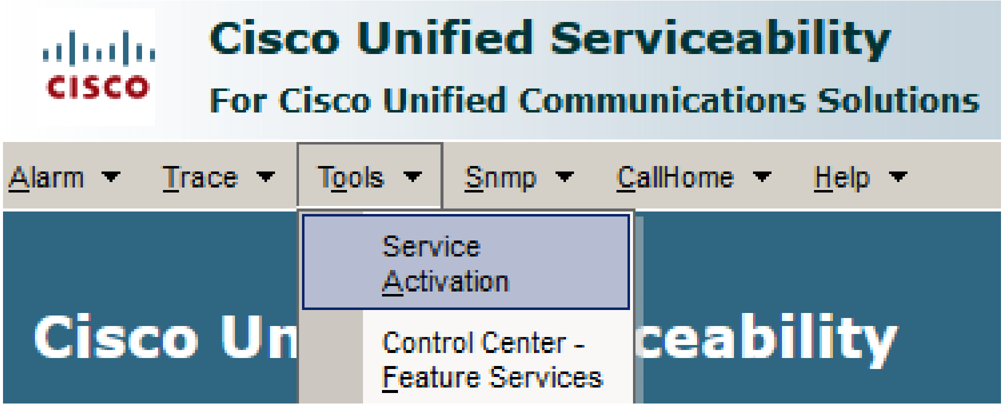
The configuration changes will not take effect on the trunk until a reset is performed. Use the Reset button or Job Scheduler to execute the reset.

安全代理与CUCM的设备通信

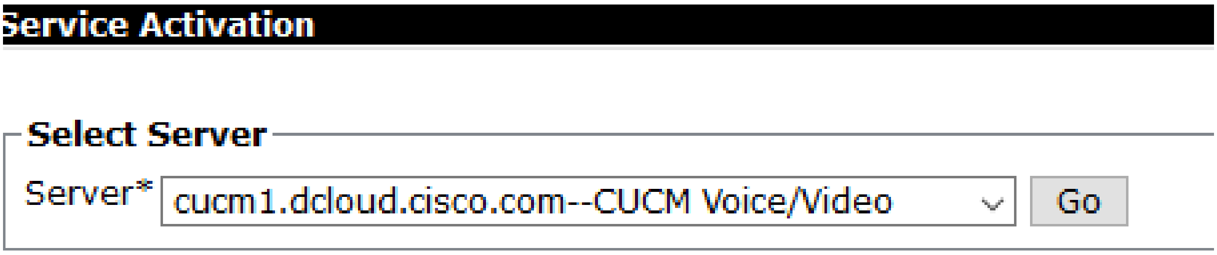
要启用设备的安全功能，必须安装本地重要证书(LSC)并将安全配置文件分配给该设备。LSC拥有终端的公钥，该公钥由CUCM CAPF私钥签名。默认情况下，它不会安装在电话上。

步骤：

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


cisco
Cisco Unified Serviceability
For Cisco Unified Communications Solutions
Alarm
Trace
Tools
Snmp
CallHome
Help
Service Activation
Control Center - Feature Services
Cisco Un
ceability

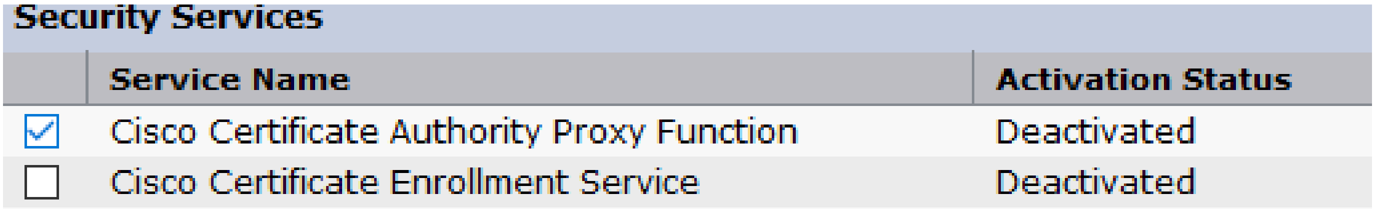
3. 选择CUCM服务器并单击 Go.


Service Activation

Select Server

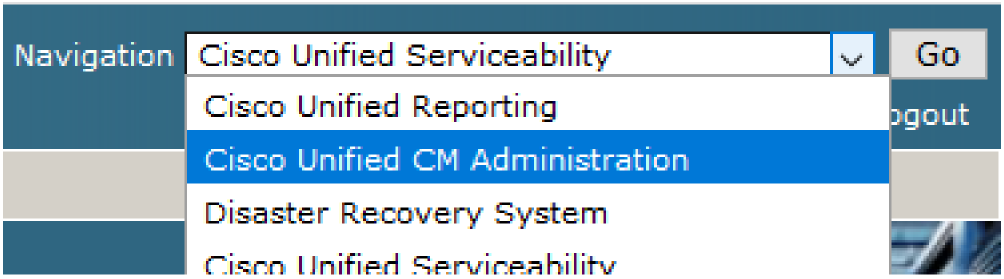
Server* cucm1.dcloud.cisco.com--CUCM Voice/Video

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

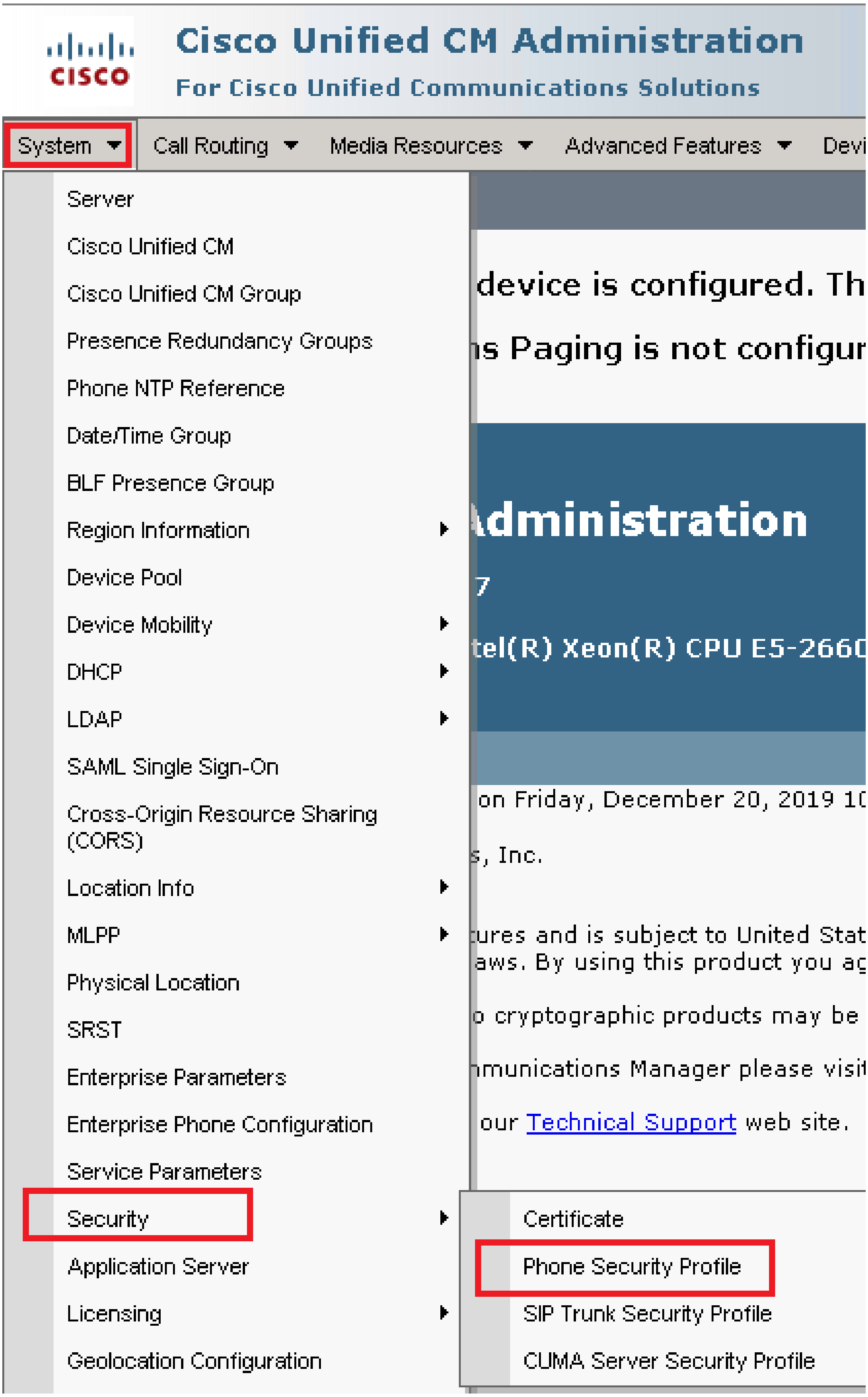

Security Services

	Service Name	Activation Status
☑	Cisco Certificate Authority Proxy Function	Deactivated
□	Cisco Certificate Enrollment Service	Deactivated

5. 确保服务已激活，然后导航至CUCM管理。

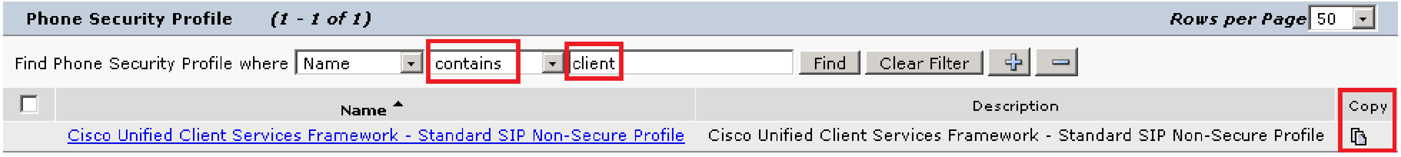

Navigation
Cisco Unified Serviceability
Go
Cisco Unified Reporting
Cisco Unified CM Administration
Disaster Recovery System
Cisco Unified Serviceability
ogout

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
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
Certificate
Phone Security Profile
SIP Trunk Security Profile
CUMA Server Security Profile
device is configured. Th
ıs Paging is not configur
ıdministration
7
tel(R) Xeon(R) CPU E5-2660
on Friday, December 20, 2019 10
s, Inc.
tures and is subject to United Stat
aws. By using this product you ag
o cryptographic products may be
ımunications Manager please visit
our Technical Support web site.

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. 点击复制图标 以便复制此配置文件
。

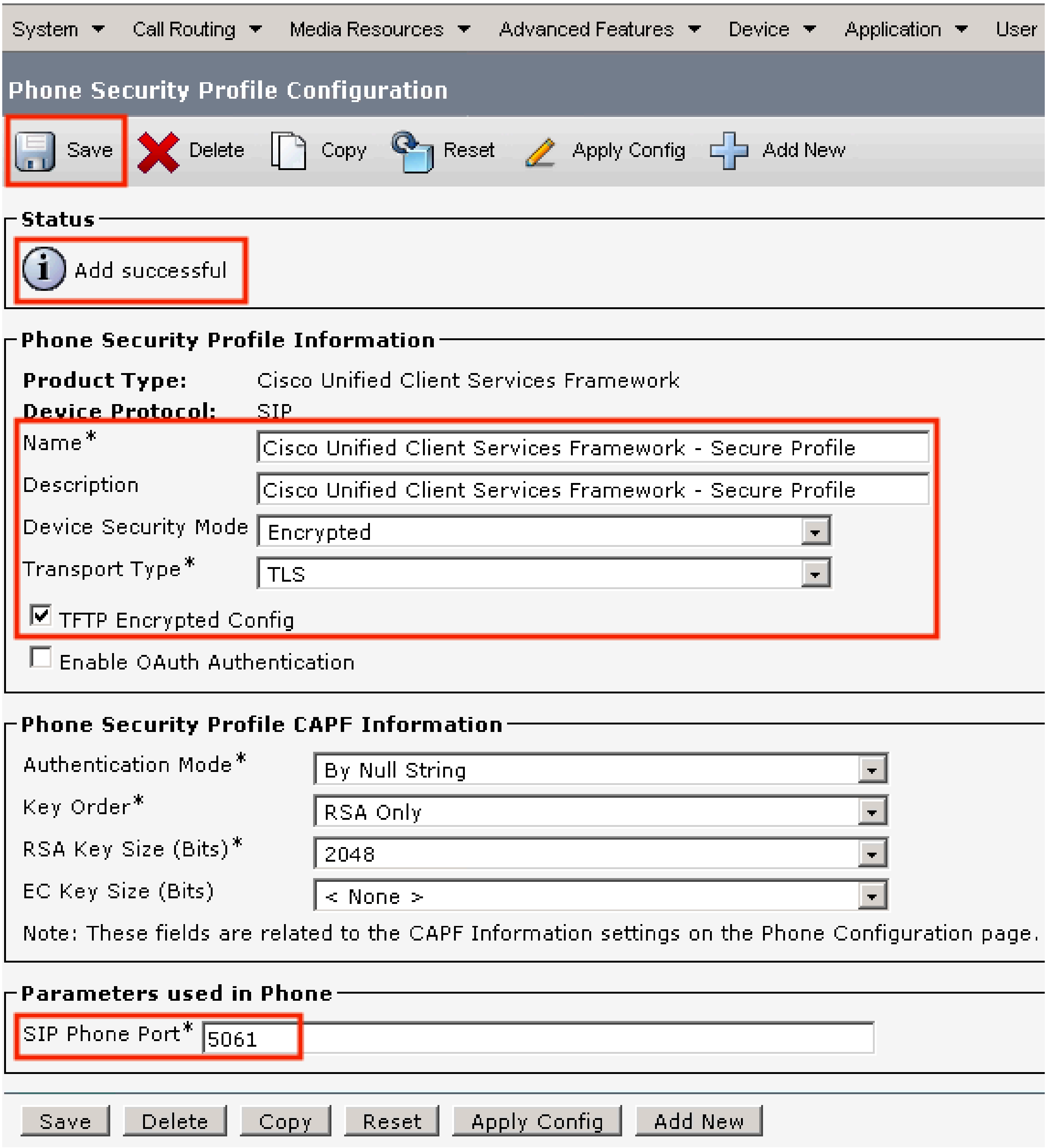


Phone Security Profile *(1 - 1 of 1)* **Rows per Page** 50

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. C更改此图像中的参数，然后单击 Save 在页面左上角。



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 >

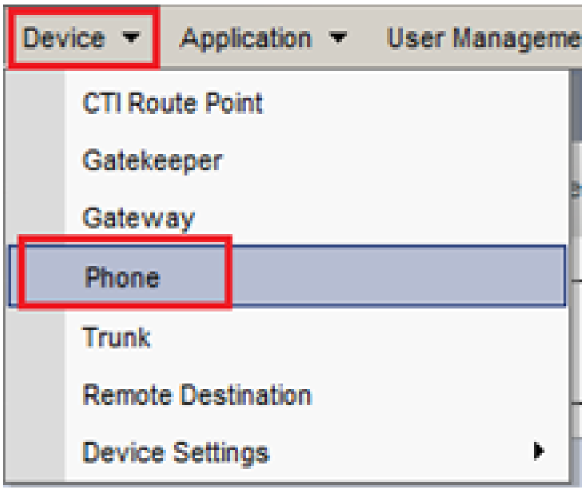
Note: These fields are related to the CAPF Information settings on the Phone Configuration page.

Parameters used in Phone

SIP Phone Port* 5061

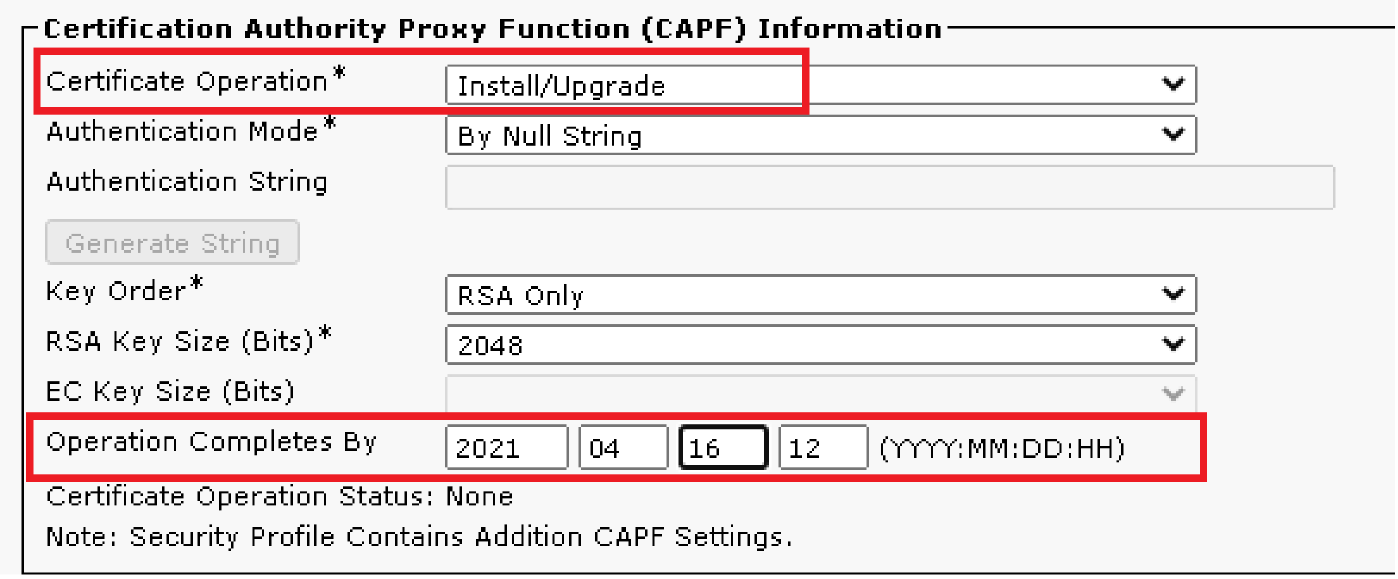
Save Delete Copy Reset Apply Config Add New

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，请点击“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。



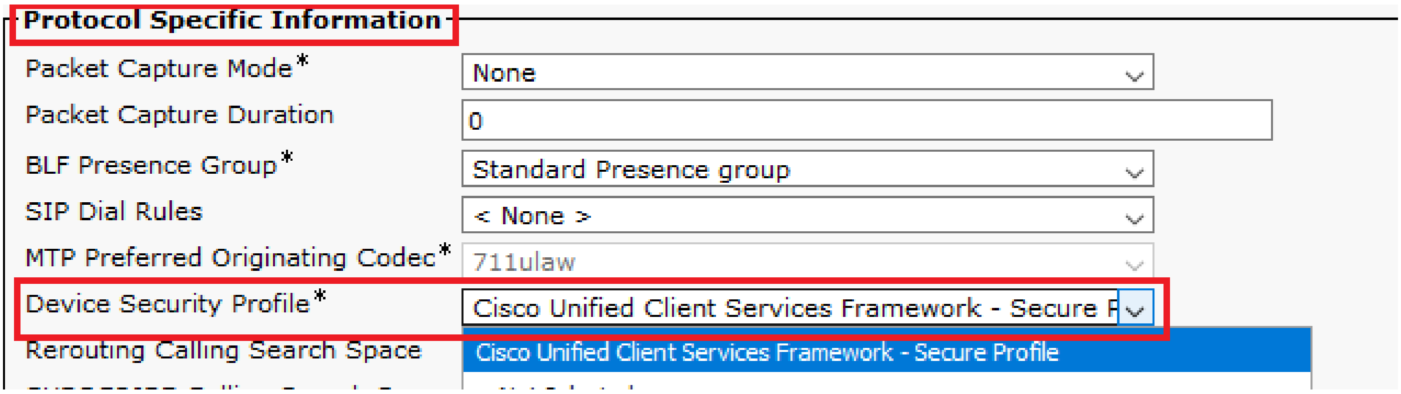
Certification Authority Proxy Function (CAPF) Information

Certificate Operation*	Install/Upgrade
Authentication Mode*	By Null String
Authentication String	
Generate String	
Key Order*	RSA Only
RSA Key Size (Bits)*	2048
EC Key Size (Bits)	
Operation Completes By	2021 04 16 12 (YYYY:MM:DD:HH)

Certificate Operation Status: None

Note: Security Profile Contains Addition CAPF Settings.

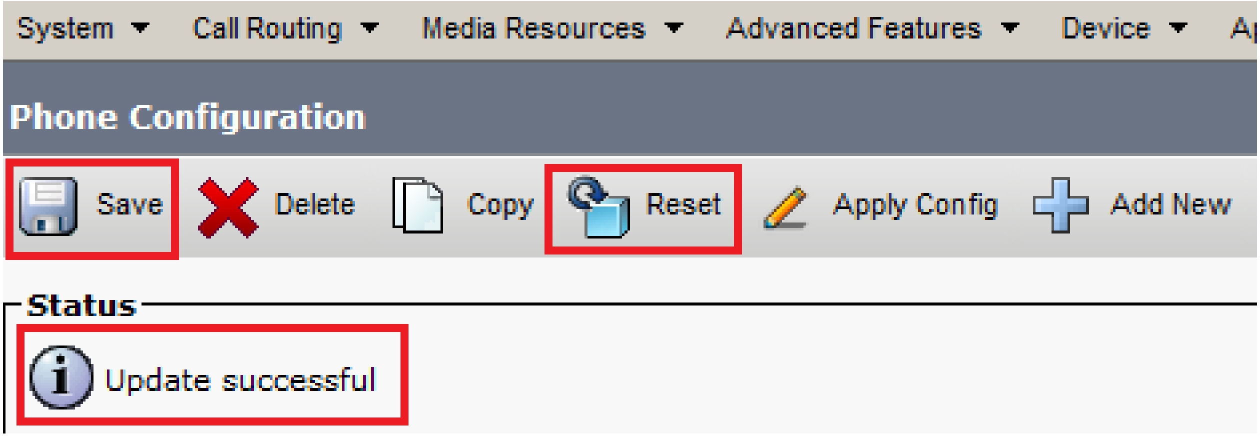
12. 查找 Protocol Specific Information 部分并更改 Device Security Profile 到 Cisco Unified Client Services Framework – Secure Profile.



Protocol Specific Information

Packet Capture Mode*	None
Packet Capture Duration	0
BLF Presence Group*	Standard Presence group
SIP Dial Rules	< None >
MTP Preferred Originating Codec*	711ulaw
Device Security Profile*	Cisco Unified Client Services Framework - Secure P
Rerouting Calling Search Space	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.

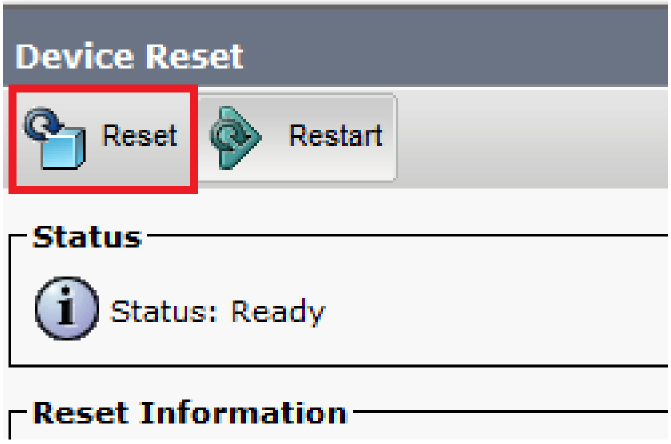


Phone Configuration

Status

Update successful

14. 系统将打开一个弹出窗口，单击 Reset 确认操作。



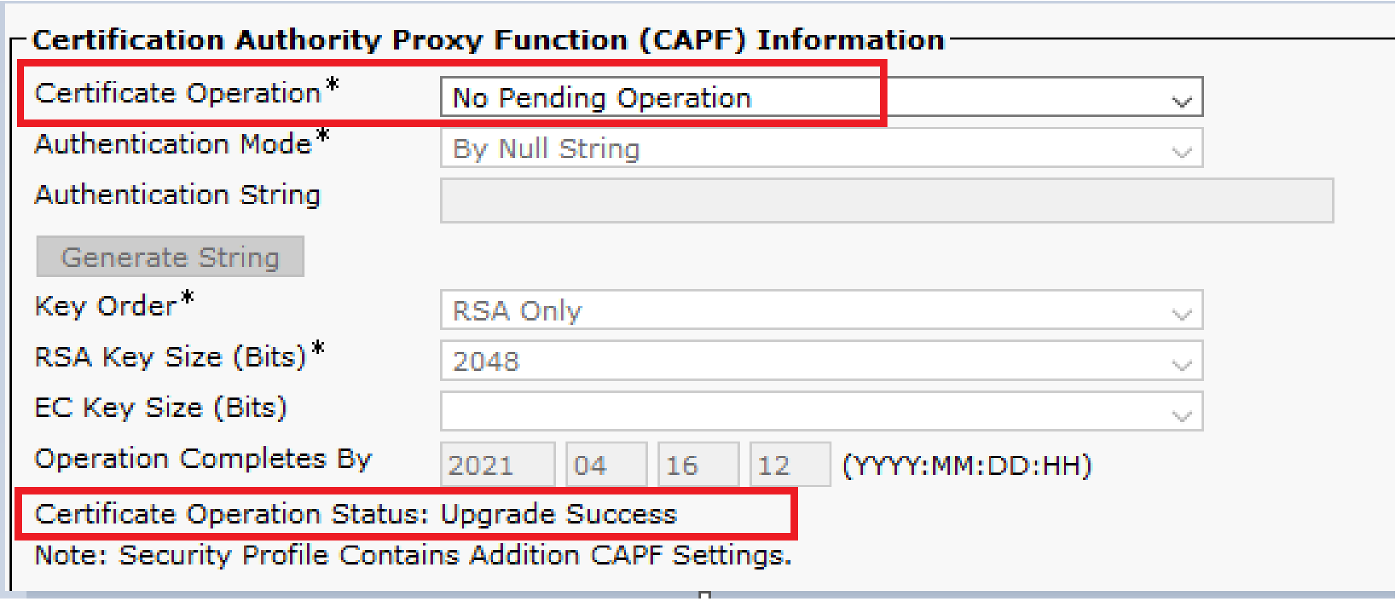
Device Reset

Status

Status: Ready

Reset Information

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.



Certification Authority Proxy Function (CAPF) Information

Certificate Operation*	No Pending Operation
Authentication Mode*	By Null String
Authentication String	
Generate String	
Key Order*	RSA Only
RSA Key Size (Bits)*	2048
EC Key Size (Bits)	
Operation Completes By	2021 04 16 12 (YYYY:MM:DD:HH)

Certificate Operation Status: Upgrade Success

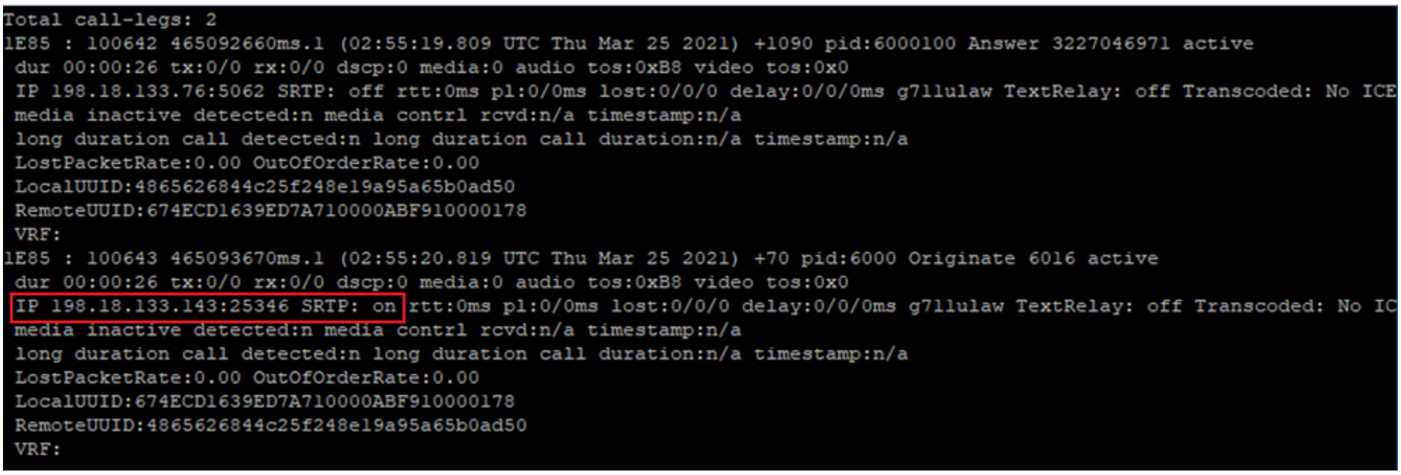
Note: Security Profile Contains Addition CAPF Settings.

16. 请参阅第步中的相同步骤。7 - 13，用于保护您想通过CUCM使用安全SIP和RTP的其他代理的设备。

验证

要验证RTP是否受到适当保护，请执行以下步骤：

1. 向联系中心发出测试呼叫，并监听IVR提示。
2. 同时，打开到vCUBE的SSH会话，并运行以下命令：
   show call active voice brief

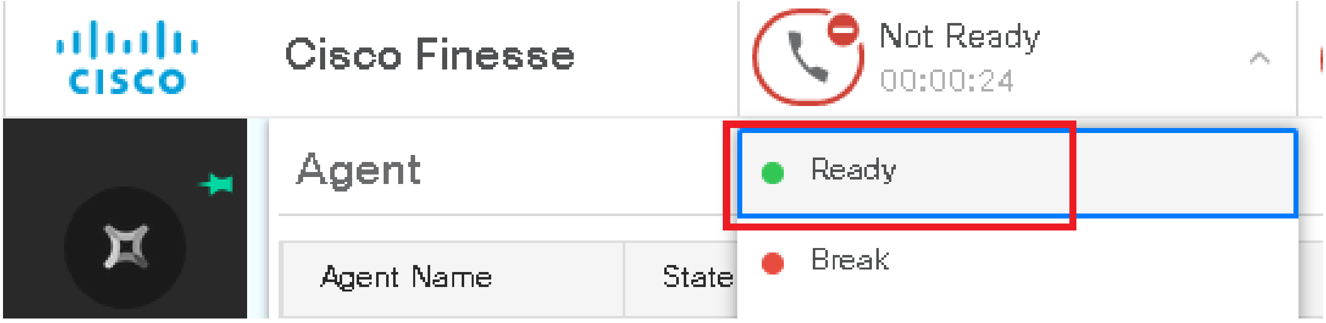


```
Total call-legs: 2
1E85 : 100642 465092660ms.1 (02:55:19.809 UTC Thu Mar 25 2021) +1090 pid:6000100 Answer 3227046971 active
 dur 00:00:26 tx:0/0 rx:0/0 dscp:0 media:0 audio tos:0xB8 video tos:0x0
 IP 198.18.133.76:5062 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off Transcoded: 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 IC
 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:
```

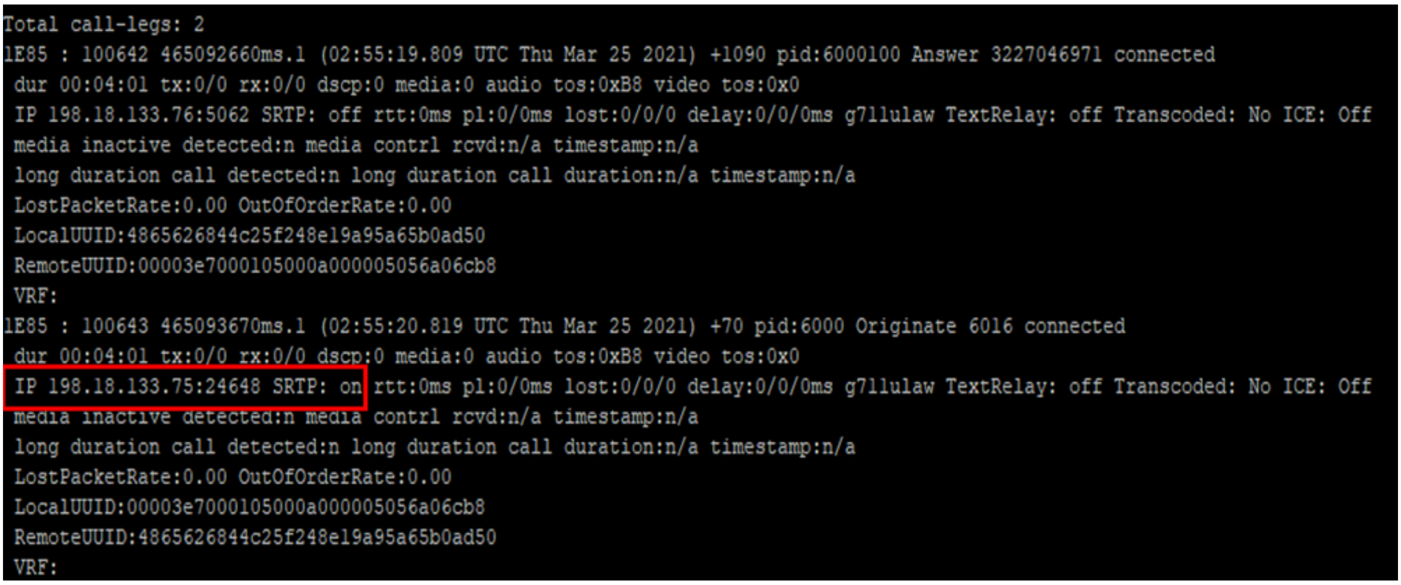
提示：检查SRTP是否 on 在CUBE和VVB之间(198.18.133.143)。如果是，这可以确认CUBE和VVB之间的RTP流量是安全的。

3. 让座席可以应答呼叫。

.



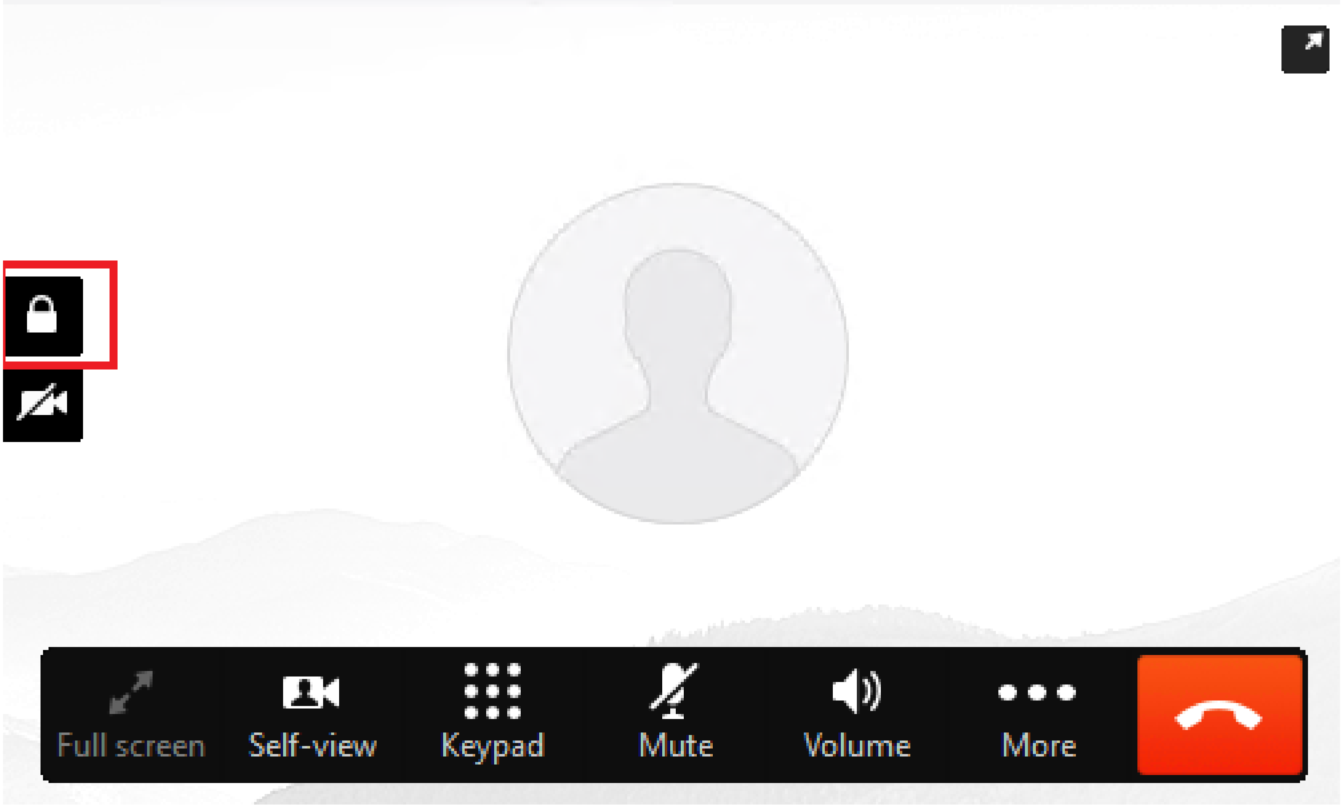
4. 座席将被保留，呼叫将被路由至座席。应答呼叫。
5. 呼叫连接到座席。返回vCUBE SSH会话，并运行以下命令：
   show call active voice brief



```
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:
```

提示：检查SRTP是否 on 在CUBE和座席的电话(198.18.133.75)之间。如果是，这可以确认CUBE和代理之间的RTP流量是安全的。

6. 此外，一旦呼叫连接，座席设备上会显示安全锁.这还证实RTP流量是安全的。



要验证SIP信号是否正确安全，请参阅配置安全SIP信令文章。

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）。