Configure Secure RTP in Contact Center Enterprise

Contents

Introduction

This document describes how to secure Real-time Transport Protocol (SRTP) Traffic in Contact Center Enterprise (CCE) comprehensive call flow.

Prerequisites

Certificates generation and import are out of the scope of this document, so certificates for Cisco Unified Communication Manager (CUCM), Customer Voice Portal (CVP) Call Server, Cisco Virtual Voice Browser (CVVB), and Cisco Unified Border Element (CUBE) have to be created and imported to the respective components. If you use self-signed certificates, certificate exchange has to be done among different components.

Requirements

Cisco recommends that you have knowledge of these topics:

- CCE
- CVP
- CUBE
- CUCM
- CVVB

Components Used

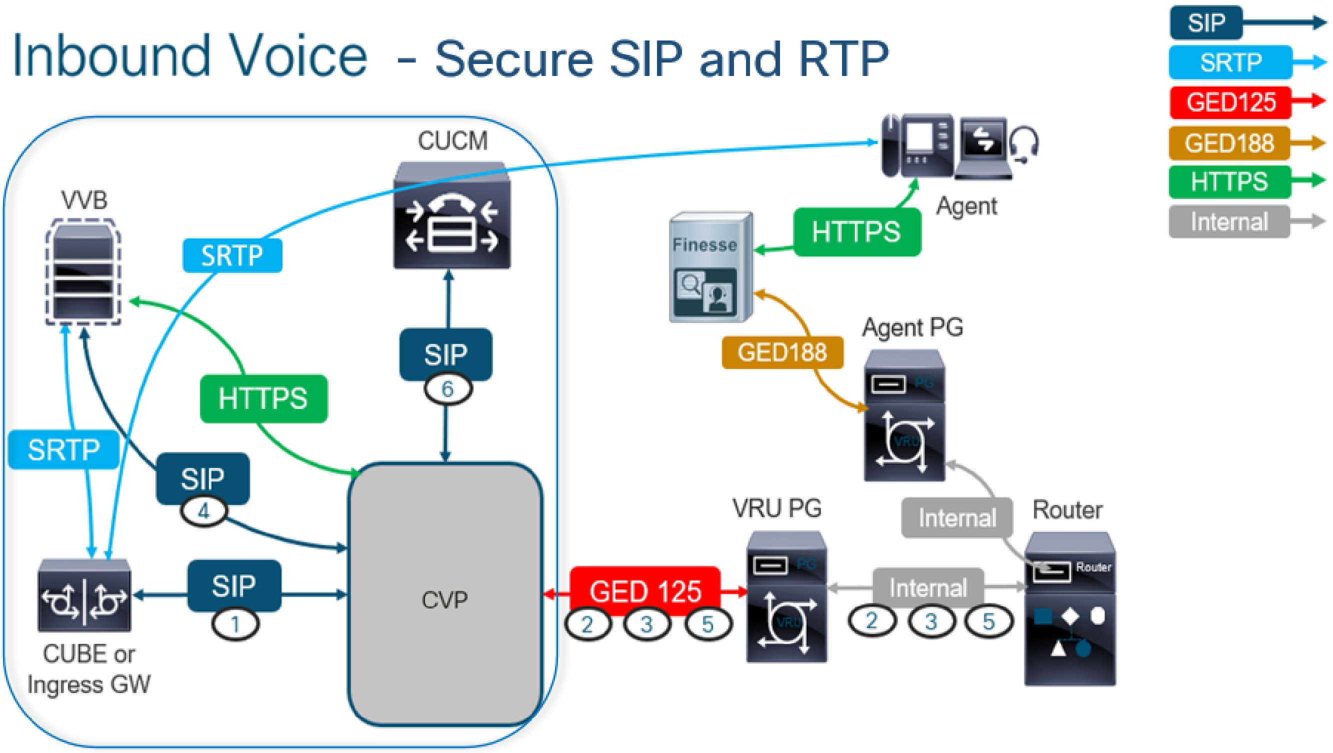
The information in this document is based on Package Contact Center Enterprise (PCCE), CVP, CVVB, and CUCM version 12.6, but it is also applicable to the previous versions.

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. If your network is live, ensure that you understand the potential impact of any command.

Configure

> **Note**: In the contact center comprehensive call flow, In order to enable secure RTP, secure SIP signals must be enabled. Therefore, configurations in this document enable both secure SIP and SRTP.

The next diagram shows the components engaged in SIP signals and RTP in the contact center comprehensive call flow. When a voice call comes to the system, it first comes via the ingress gateway or CUBE, so start the configurations on CUBE. Next, configure CVP, CVVB, and CUCM.



Task 1: CUBE Secure Configuration

In this task, you configure CUBE to secure SIP protocol messages and RTP.

Required configurations:

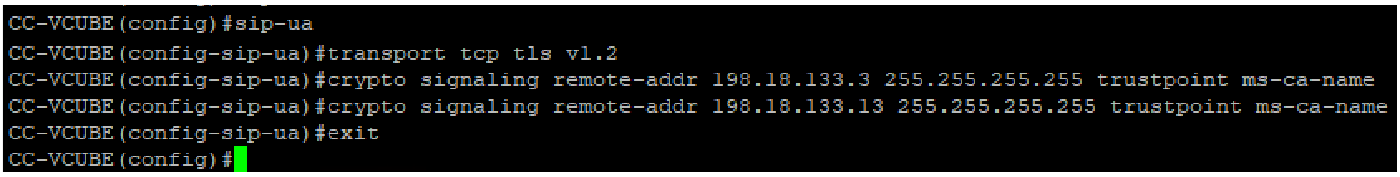
- Configure a Default Trustpoint for the SIP UA
- Modify the Dial-peers to use TLS and SRTP

Steps:

1. Open an SSH session to CUBE.

2. Run these commands to have the SIP stack use the CA certificate of the CUBE. CUBE establishes SIP TLS connection from/to CUCM (198.18.133.3) and CVP (198.18.133.13):

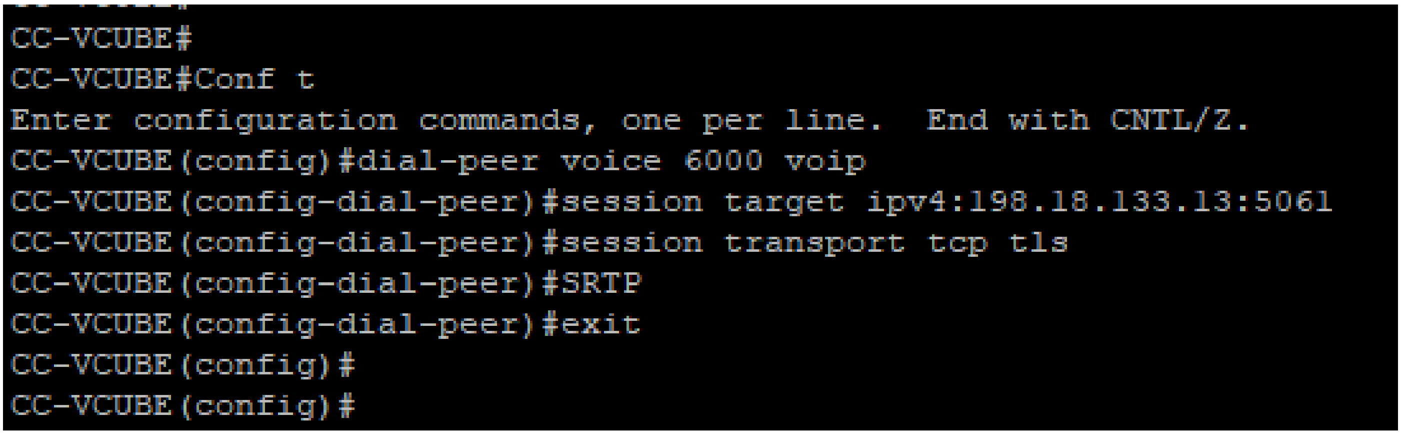
Conf t Sip-ua Transport tcp tls v1.2 crypto signaling remote-addr 198.18.133.3 255.255.255.255 trustpoint ms-ca-name crypto signaling remote-addr 198.18.133.13 255.255.255.255 trustpoint ms-ca-name exit



```
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. Run these commands to enable TLS on the outgoing dial peer to CVP. In this example, dial-peer tag 6000 is used to route calls to CVP:

Conf t dial-peer voice 6000 voip session target ipv4:198.18.133.13:5061 session transport tcp tls srtp exit



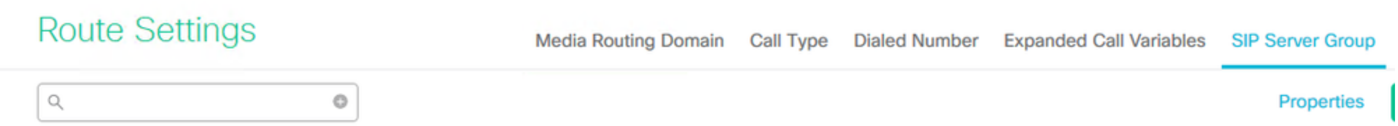
```
CC-VCUBE#
CC-VCUBE#Conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CC-VCUBE(config)#dial-peer voice 6000 voip
CC-VCUBE(config-dial-peer)#session target ipv4:198.18.133.13:5061
CC-VCUBE(config-dial-peer)#session transport tcp tls
CC-VCUBE(config-dial-peer)#SRTP
CC-VCUBE(config-dial-peer)#exit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

Task 2: CVP Secure Configuration

In this task, configure the CVP call server to secure the SIP protocol messages (SIP TLS).

Steps:

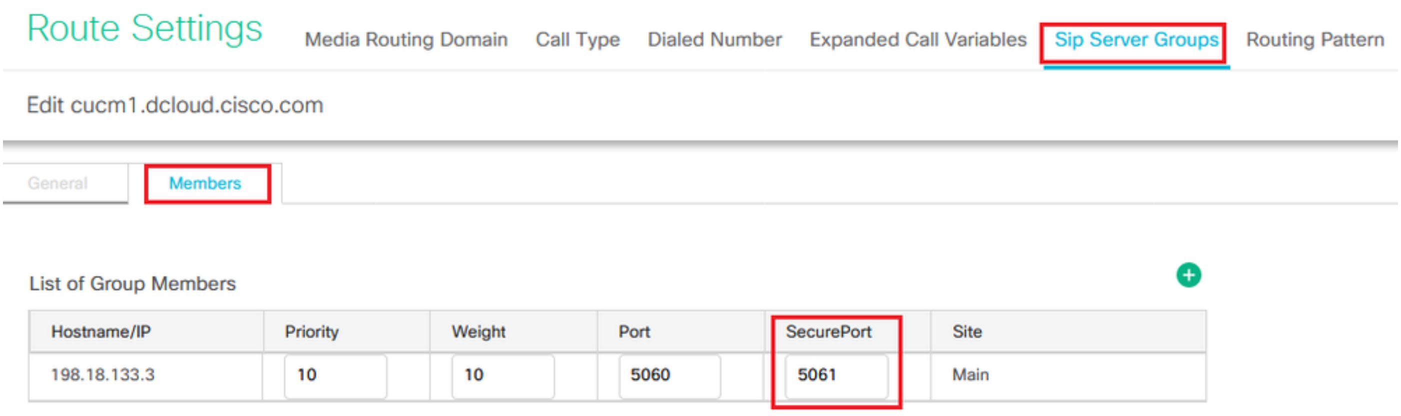
1. Login to the UCCE Web Administration.
2. Navigate to Call Settings > Route Settings > SIP Server Group.



Based on your configurations, you have SIP Server Groups configured for CUCM, CVVB, and CUBE. You need to set secure SIP ports to 5061 for all of them. In this example, these SIP server groups are used:

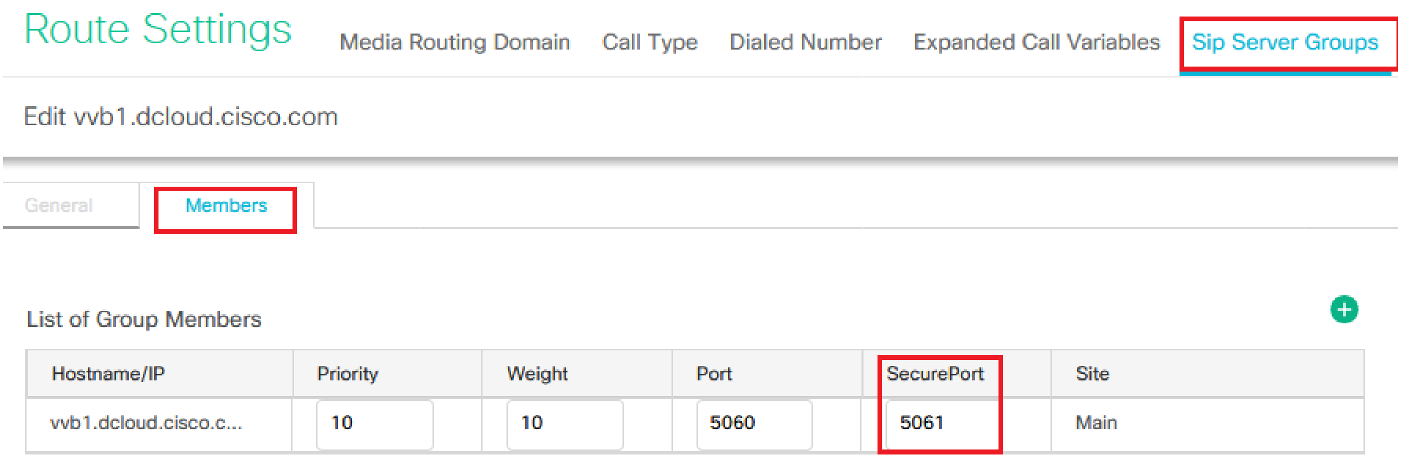
- cucm1.dcloud.cisco.com for CUCM
- vvb1.dcloud.cisco.com for CVVB
- cube1.dcloud.cisco.com for CUBE

3. Click cucm1.dcloud.cisco.com,and then in the Members tab that shows the details of SIP Server Group Configurations. Set SecurePort to 5061 and click Save.



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

4. Click vvb1.dcloud.cisco.com and then in the Members tab, set the **SecurePort** to 5061 and click Save.



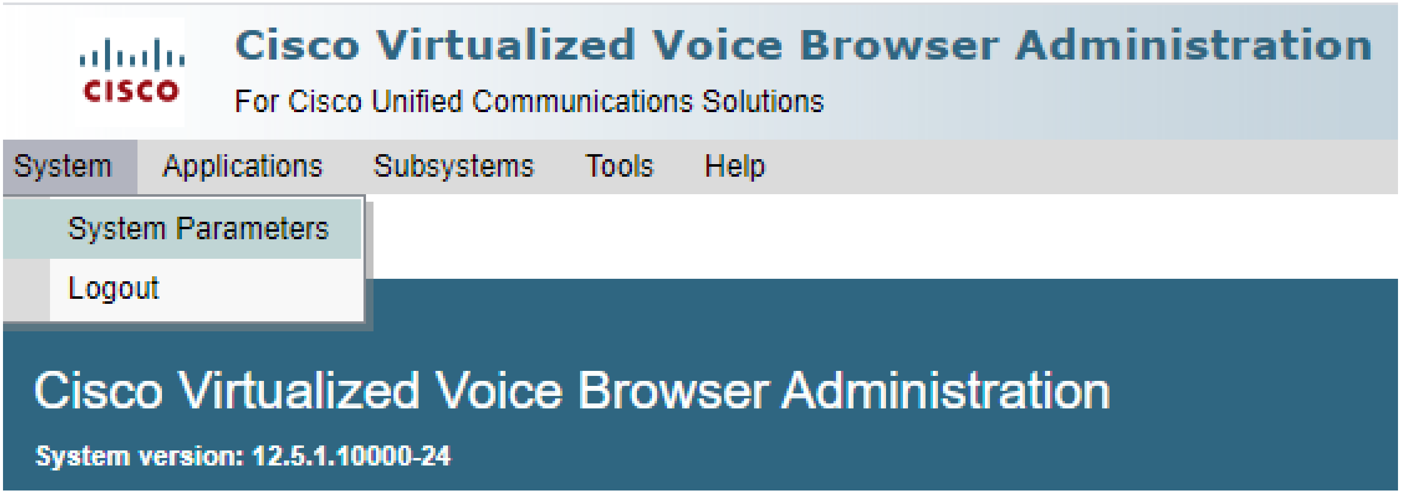
Hostname/IP	Priority	Weight	Port	SecurePort	Site
vvb1.dcloud.cisco.c...	10	10	5060	5061	Main

Task 3: CVVB Secure Configuration

In this task, configure CVVB to secure the SIP protocol messages (SIP TLS) and SRTP.

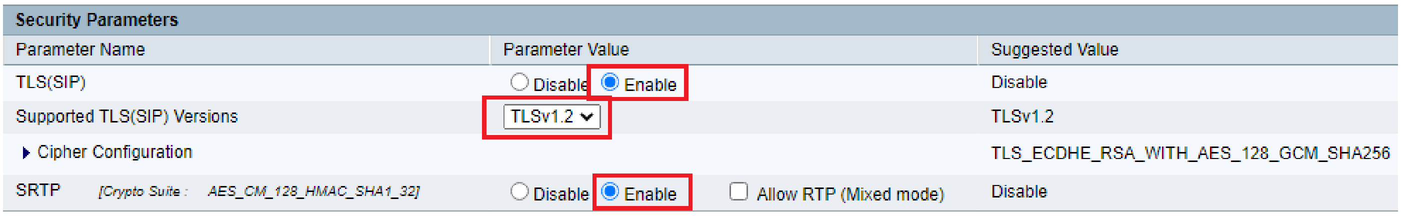
Steps:

1. Open the Cisco VVB Admin page.
2. Navigate to 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

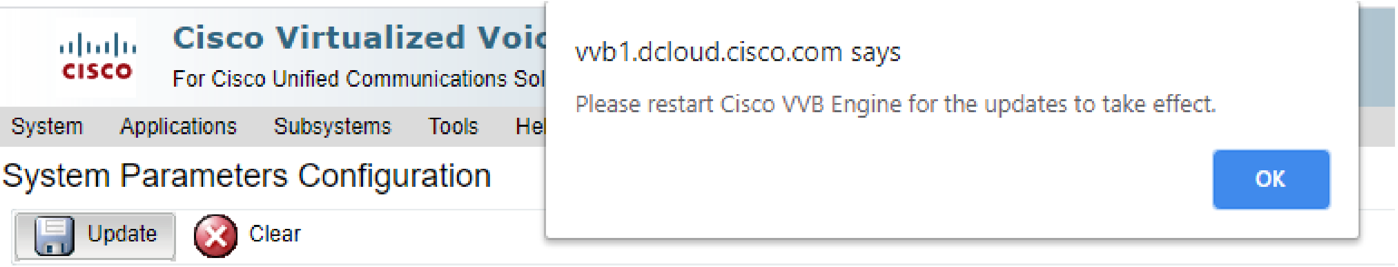
3. On the Security Parameters section, choose Enable for TLS (SIP) . Keep the Supported TLS(SIP) version as

TLSv1.2 and choose Enable for 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. Click **Update**. Click Ok when prompted to restart the CVVB engine.

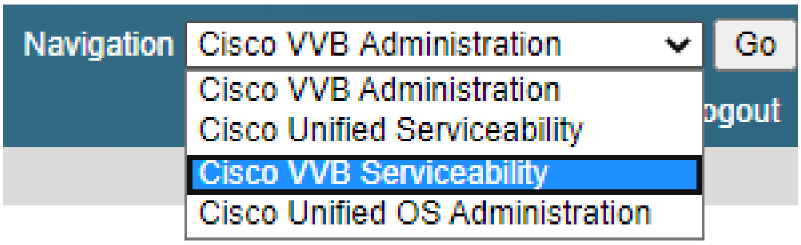


System Parameters Configuration

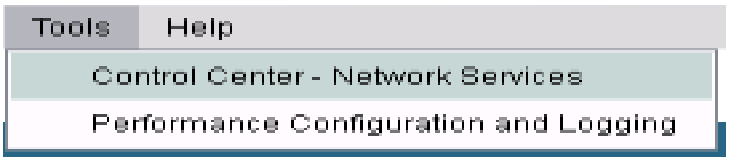
vvb1.dcloud.cisco.com says

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

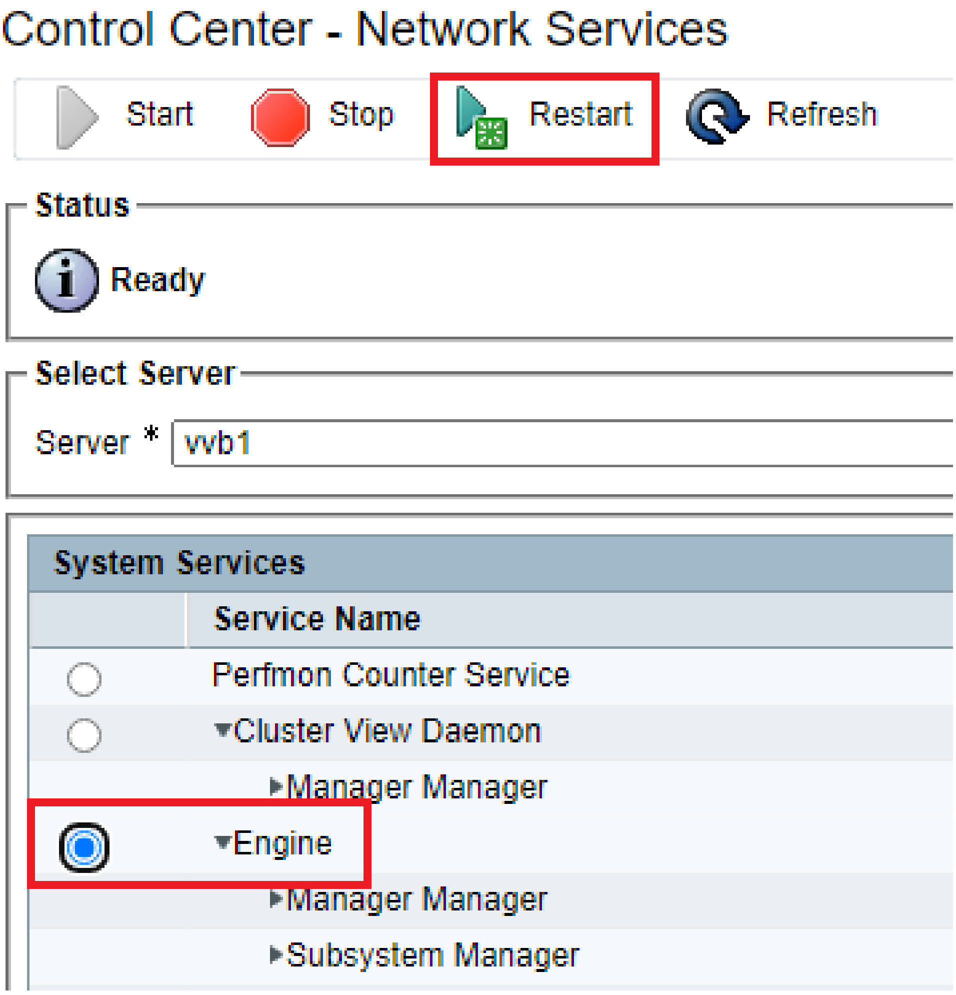
5. These changes require a restart of the Cisco VVB engine. In order to restart the VVB engine, navigate to the Cisco VVB Serviceability , then click **Go**.



6. Navigate to Tools > Control Center – Network Services.


Tools
Help
Control Center - Network Services
Performance Configuration and Logging

7. Choose Engine and click 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

Task 4: CUCM Secure Configuration

In order to secure SIP messages and RTP on CUCM, perform these configurations:

- Set CUCM Security Mode to Mixed Mode
- Configure SIP Trunk Security Profiles for CUBE and CVP
- Associate SIP Trunk Security Profiles to Respective SIP Trunks and enable SRTP
- Secure Agents' device Communication with CUCM

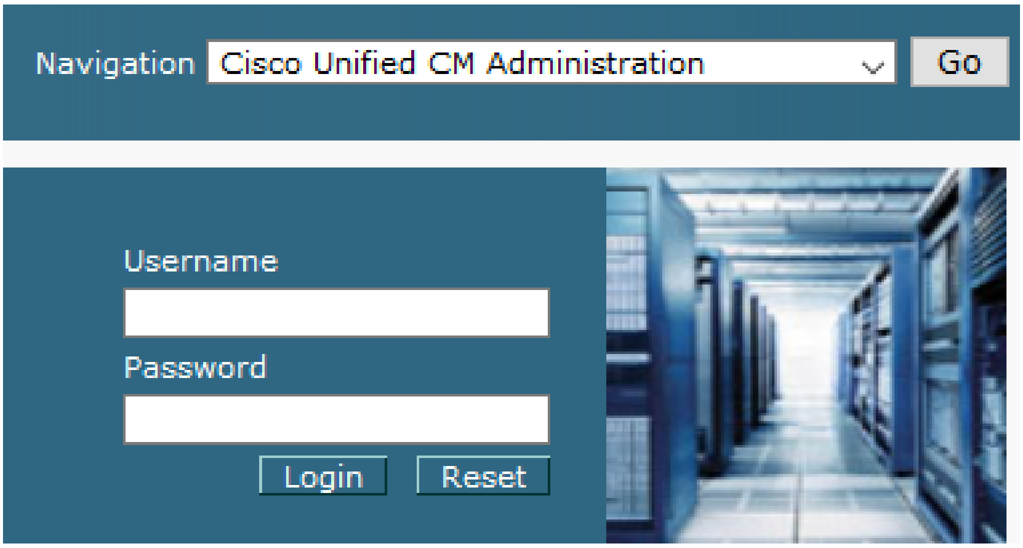
Set CUCM Security Mode to Mixed Mode

CUCM supports two security modes:

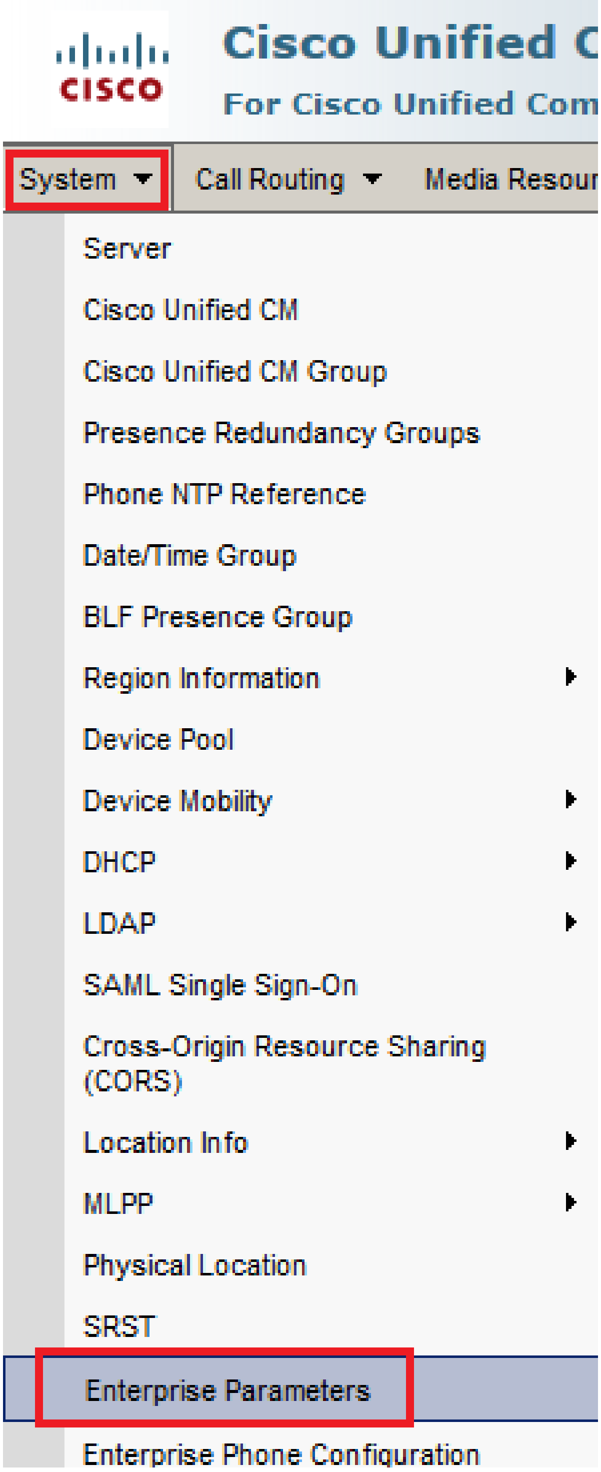
- Non-secure mode (default mode)
- Mixed mode (secure mode)

Steps:

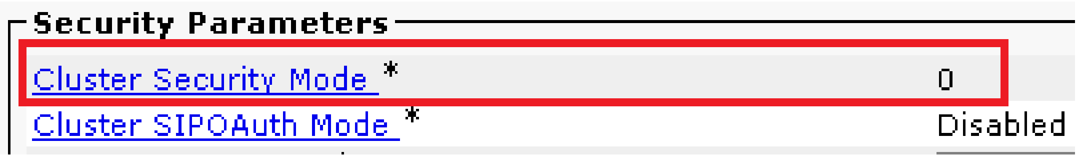
1. Log in to the CUCM administration interface.



2. When you log in to the CUCM, you can navigate to **System > Enterprise Parameters**.



3. Under the Security Parameters section, check if the Cluster Security Mode is set to **0**.



Security Parameters

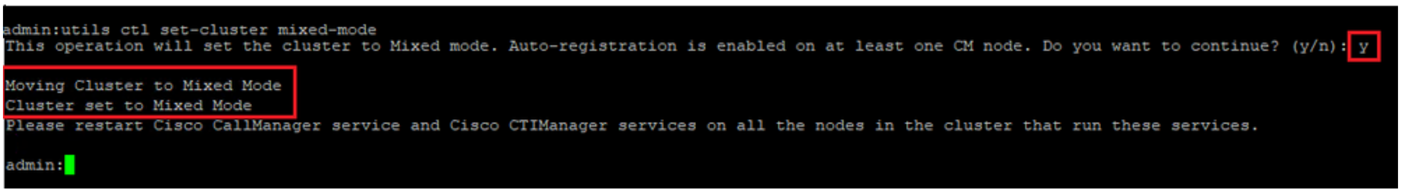
Cluster Security Mode * 0

Cluster SIPOAuth Mode * Disabled

4. If Cluster Security Mode is set to 0, this means cluster security mode is set to non-secure. You need to enable the mixed Mode from CLI.
5. Open an SSH session to the CUCM.
6. Upon successful login to CUCM via SSH, run this command:

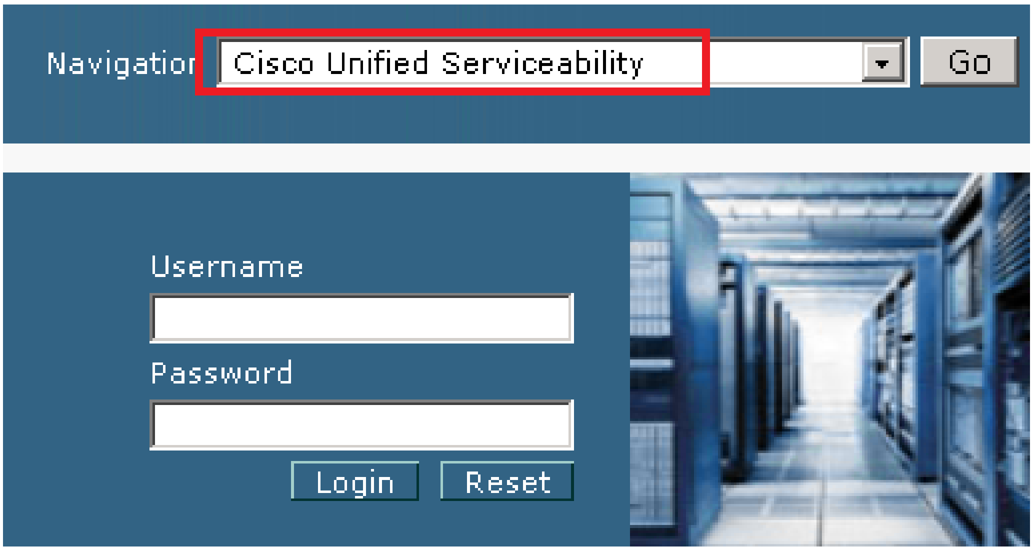
utils ctl set-cluster mixed-mode

7. Type y and click Enter when prompted. This command sets cluster security mode to mixed mode.



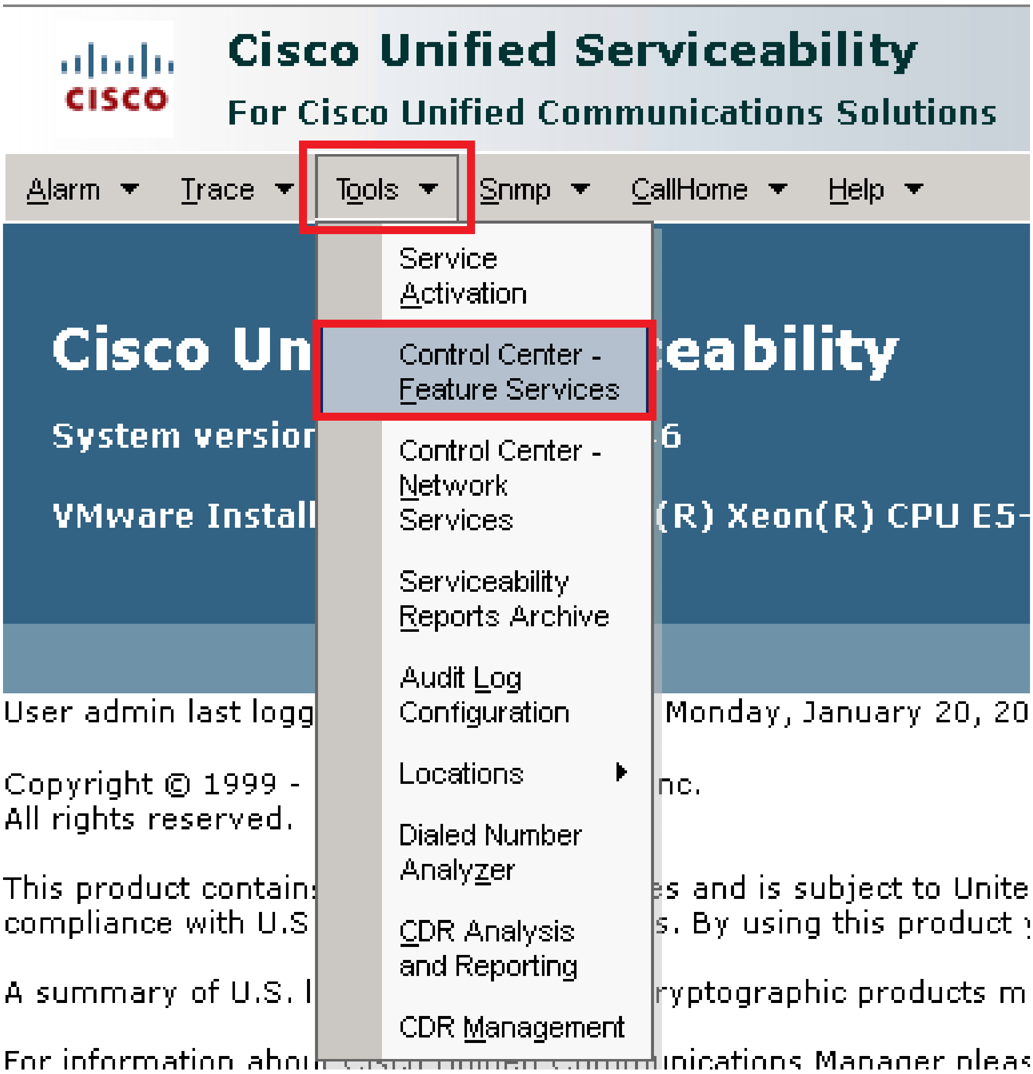
```
admin:utils ctl set-cluster mixed-mode
This operation will set the cluster to Mixed mode. Auto-registration is enabled on at least one CM node. Do you want to continue? (y/n): y

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. For the changes to take effect, restart the Cisco CallManager and the Cisco CTIManager services.
9. In order to restart the services, navigate and log in to **Cisco Unified Serviceability.**

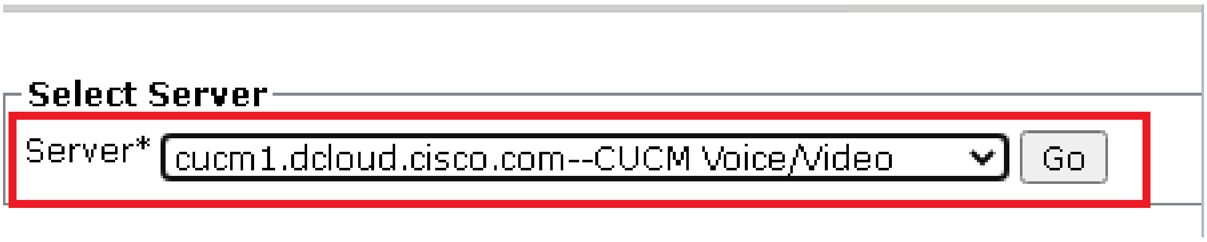


Navigation Cisco Unified Serviceability

10. After successful login, navigate to 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 unications Manager pleas

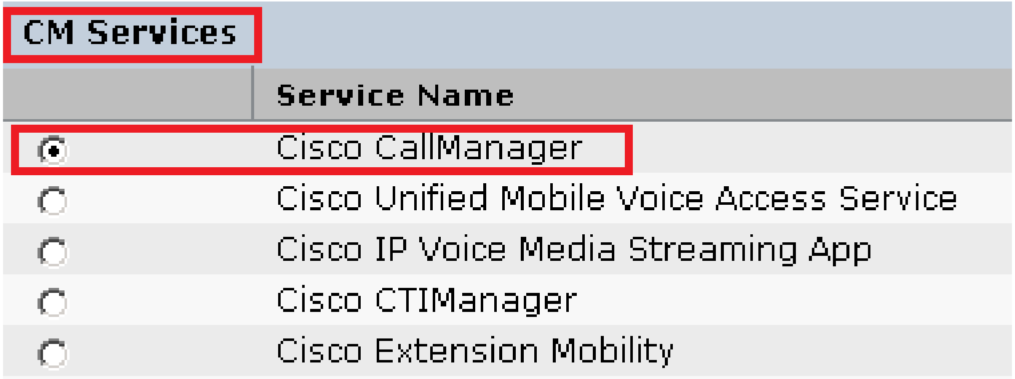
11. Choose the server and then click Go.



Select Server

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

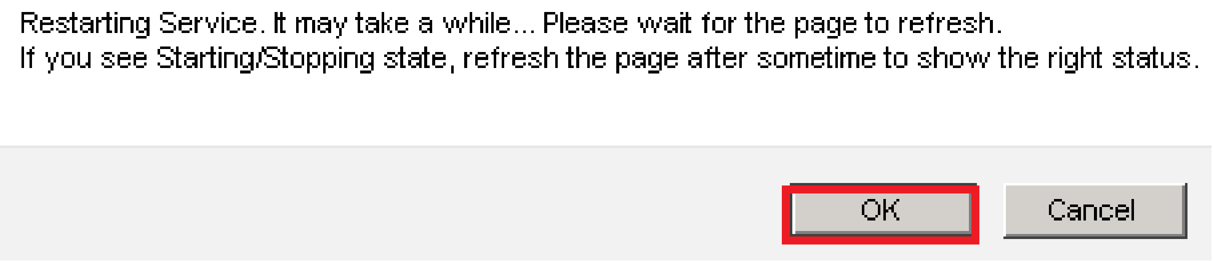
12. Underneath CM services, choose the Cisco CallManager , then click Restart button at the top of the page.



CM Services

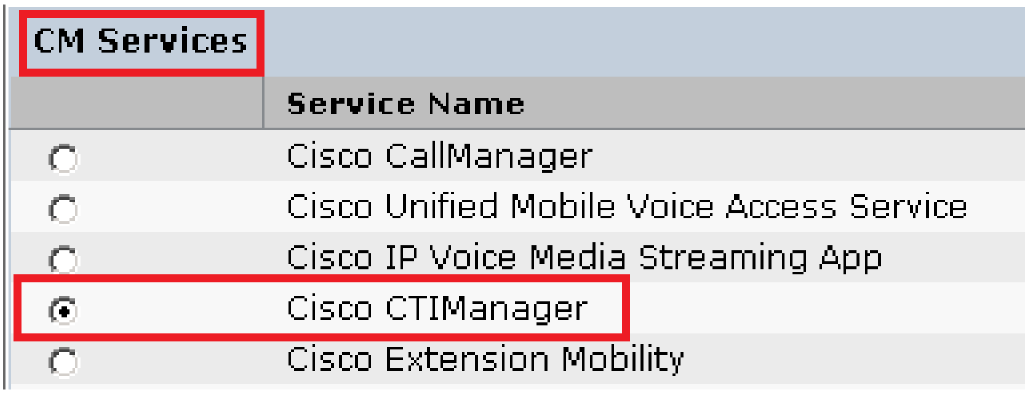
	Service Name
●	Cisco CallManager
○	Cisco Unified Mobile Voice Access Service
○	Cisco IP Voice Media Streaming App
○	Cisco CTIManager
○	Cisco Extension Mobility

13. Confirm the pop-up message and click OK. Wait for the service to successfully restart.



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.

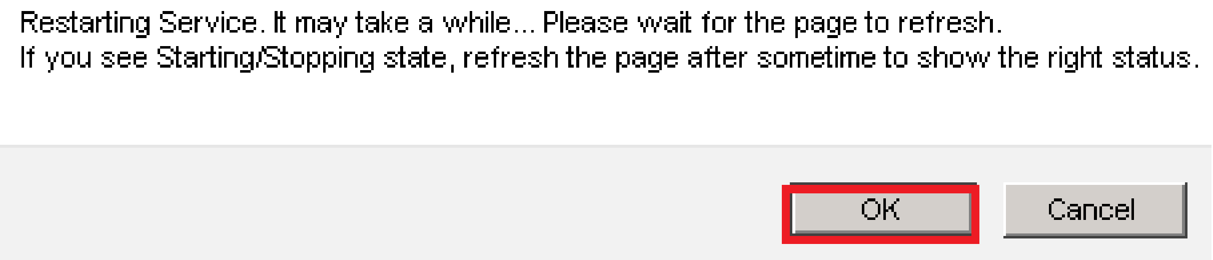
14. After the successful restart of Cisco CallManager, choose the **Cisco CTIManager** then click Restart button to restart Cisco CTIManager service.



CM Services

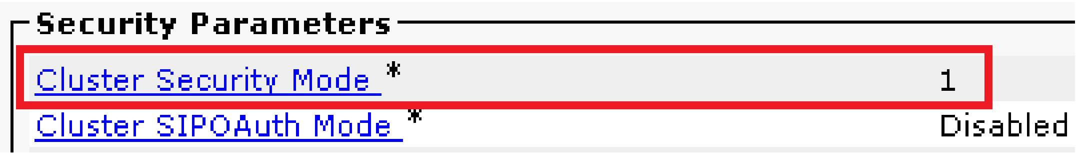
	Service Name
○	Cisco CallManager
○	Cisco Unified Mobile Voice Access Service
○	Cisco IP Voice Media Streaming App
●	Cisco CTIManager
○	Cisco Extension Mobility

15. Confirm the pop-up message and click OK. Wait for the service to successfully restart.



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. After successful services restart, in order to verify cluster security mode is set to mixed mode, navigate to CUCM administration as explained in Step 5. and then check the Cluster Security Mode. Now it must be set to 1.



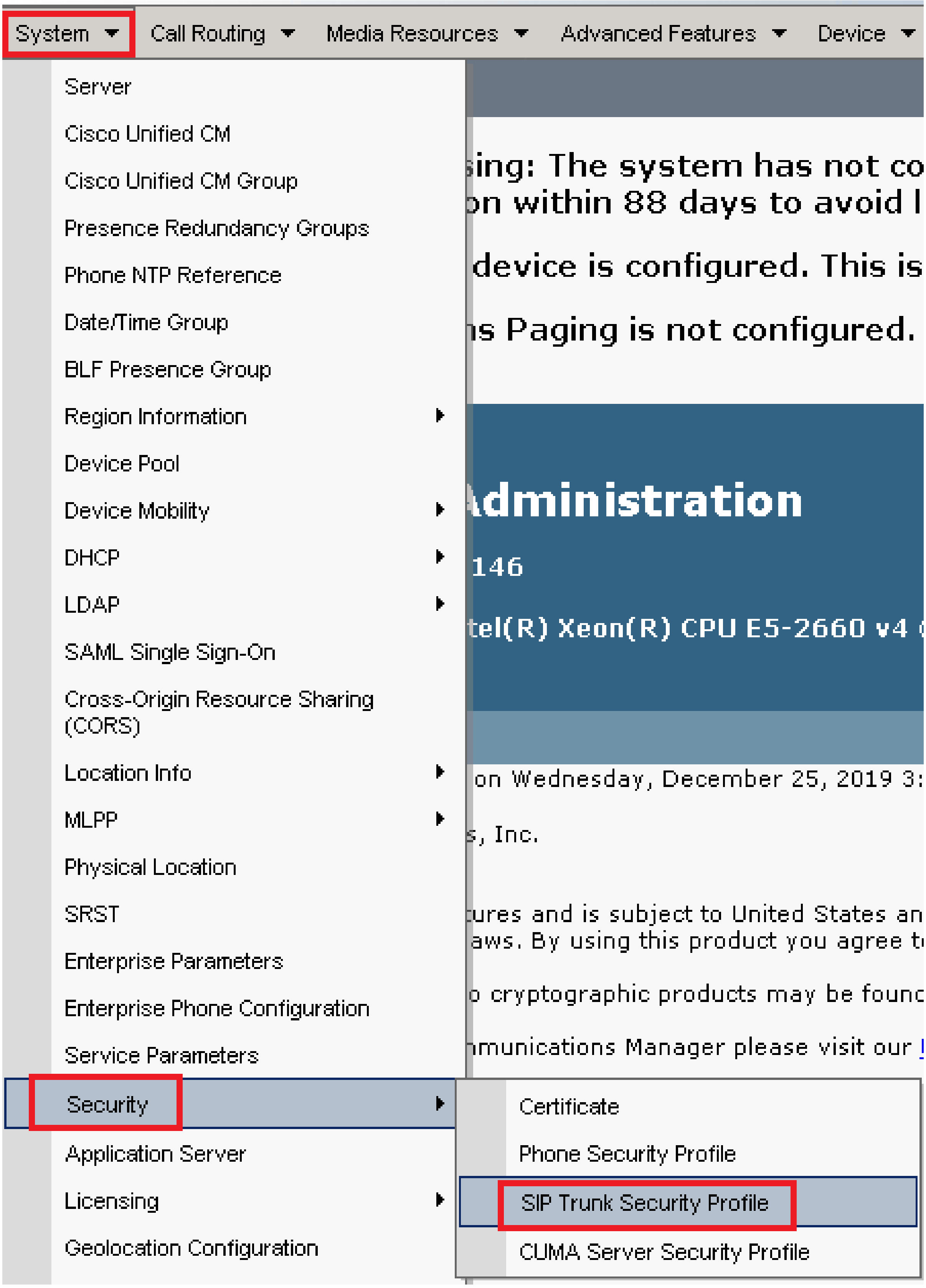
Security Parameters

Cluster Security Mode * 1
Cluster SIPOAuth Mode * Disabled

Configure SIP Trunk Security Profiles for CUBE and CVP

Steps:

1. Log in to the CUCM administration interface.
2. After successful login to CUCM, navigate to System > Security > SIP Trunk Security Profile in order to create a device security profile for CUBE.



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

device is configured. This is

ns Paging is not configured.

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

on Wednesday, December 25, 2019 3:

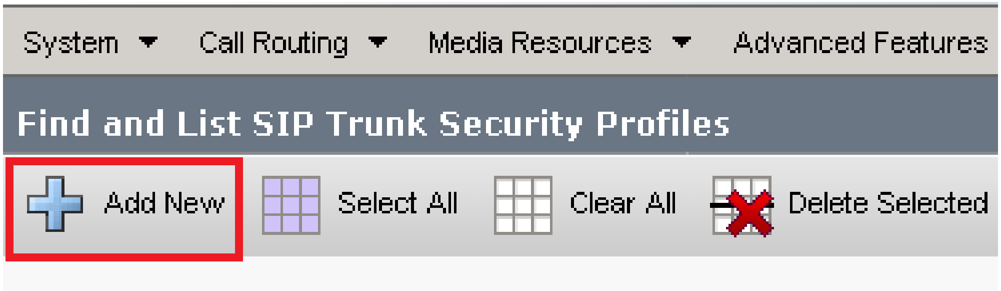
s, Inc.

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

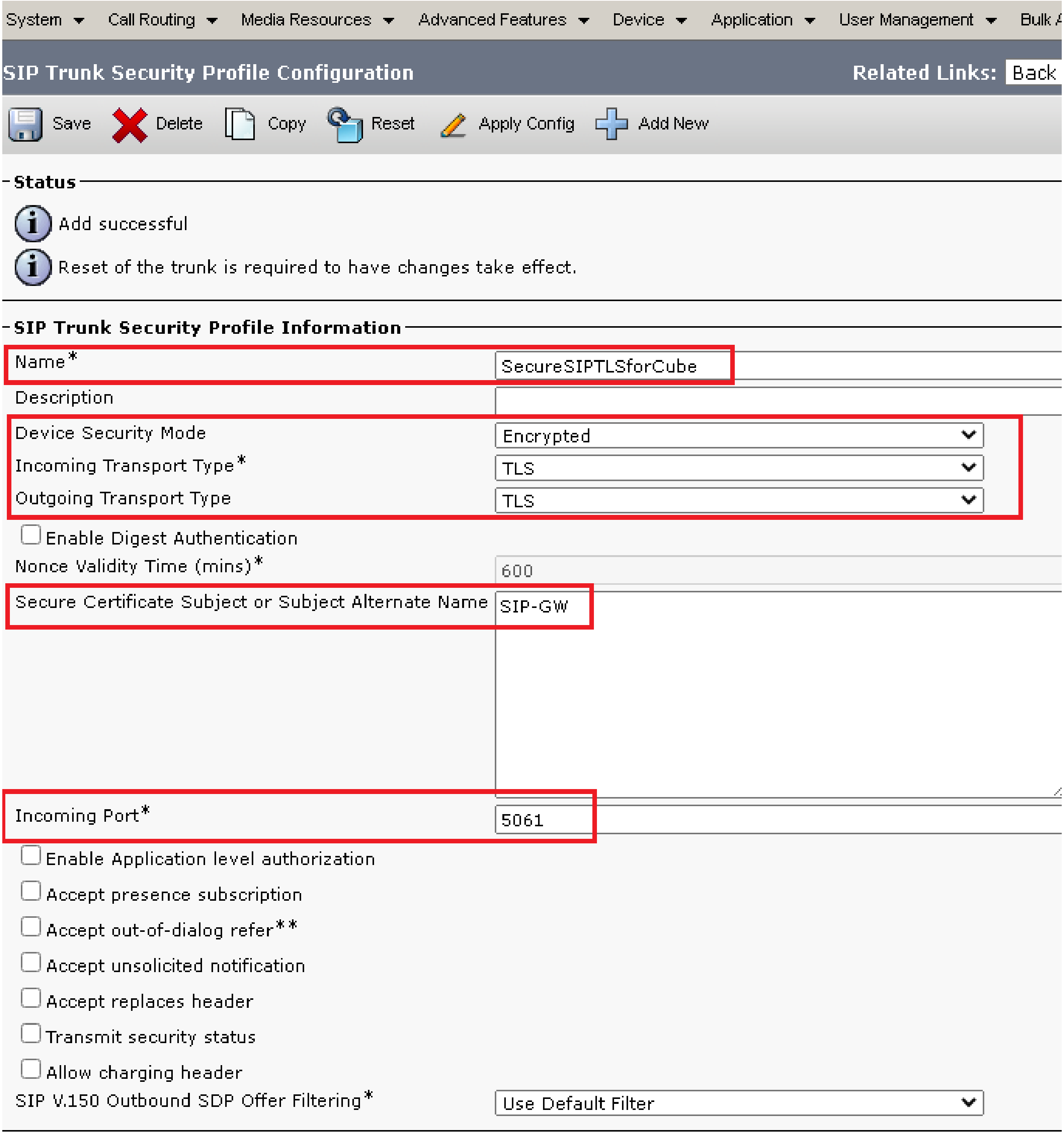
o cryptographic products may be found

nmunications Manager please visit our

3. On the top left, click **Add New** to add a new profile.



4. Configure SIP Trunk Security Profile as this image and then click Save at the bottom left of the page.



Status

Add successful

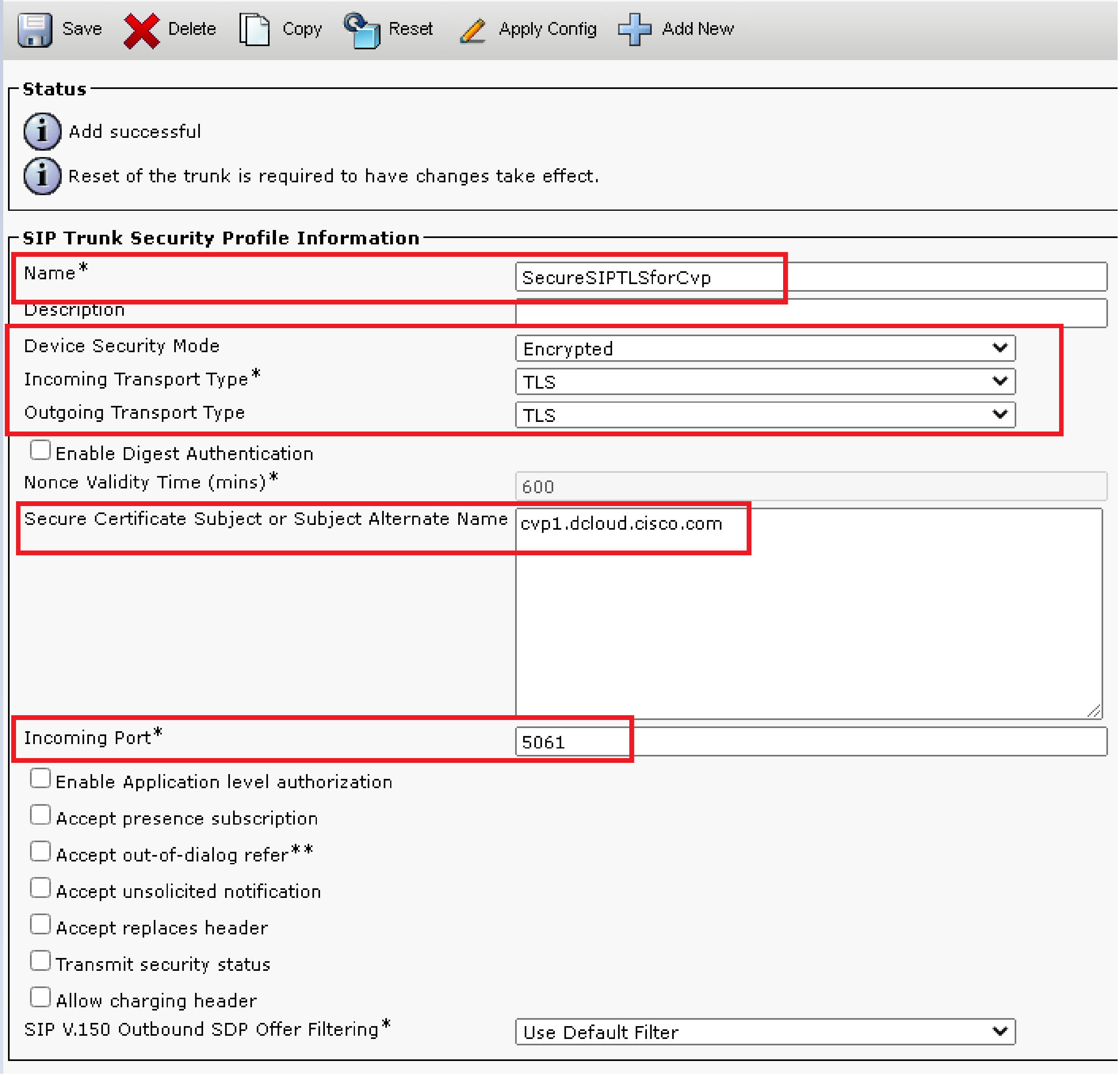
Reset of the trunk is required to have changes take effect.

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. Ensure to set the Secure Certificate Subject or Subject Alternate Name to the Common Name (CN) of the CUBE certificate as it must match.

6. Click Copy button and change the Name to SecureSipTLSforCVP. Change Secure Certificate Subject to the CN of the CVP call server certificate as it must match. Click **Save** button.



Status

Add successful

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

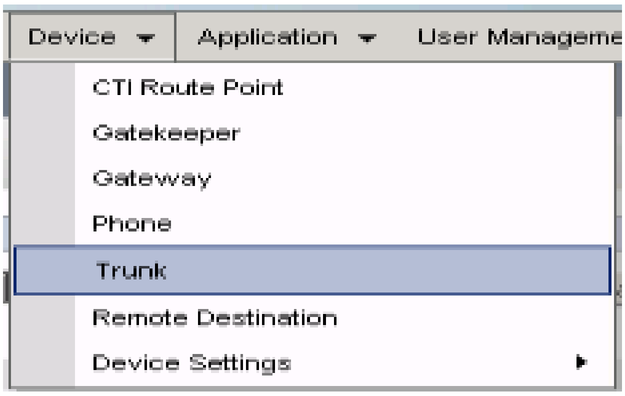
SIP Trunk Security Profile Information

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

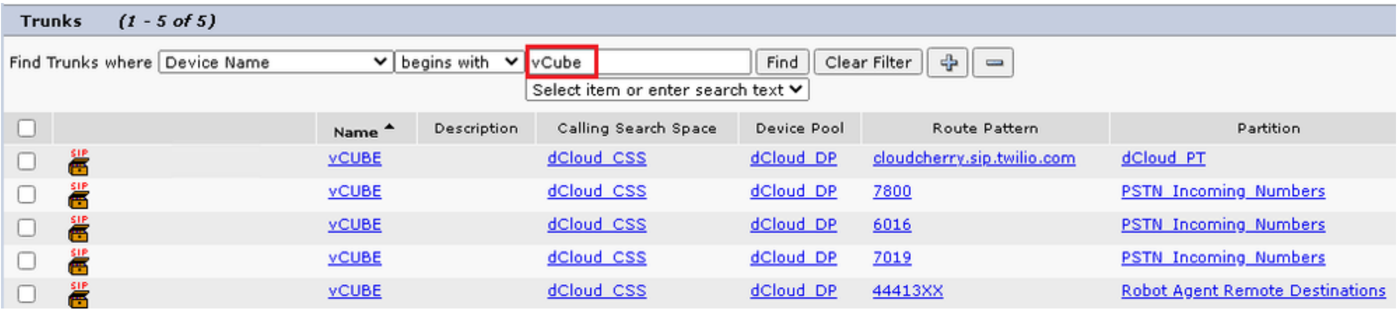
Associate SIP Trunk Security Profiles to Respective SIP Trunks and Enable SRTP

Steps:

1. On the CUCM Administration page, navigate to Device > Trunk.



2. Search for CUBE trunk. In this example, the CUBE trunk name is vCube , then click Find.



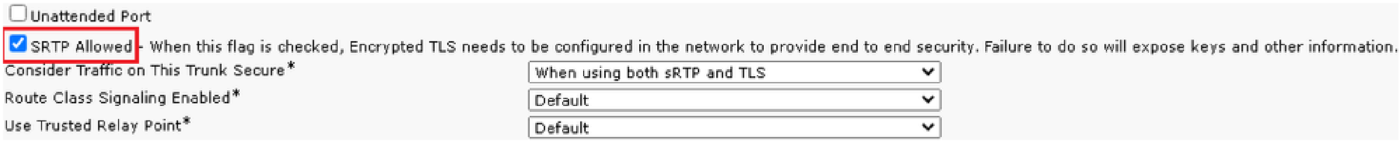
Trunks *(1 - 5 of 5)*

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. Click vCUBE to open the vCUBE trunk configuration page.
4. In Device Information section, check the SRTP Allowed check box in order to enable SRTP.

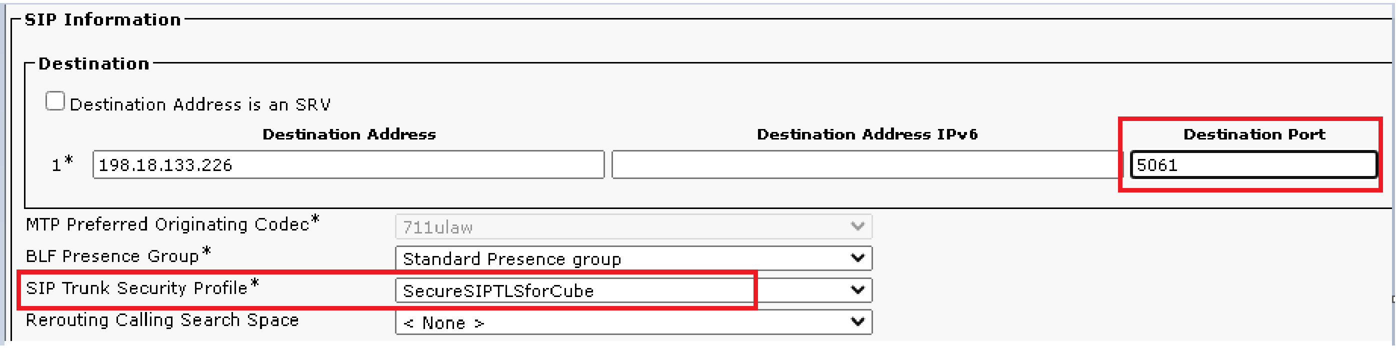


□ Unattended Port

☑ 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. Scroll down to the SIP Information section, and change the Destination Port to 5061.
6. Change SIP Trunk Security Profile to SecureSIPTLSForCube.



SIP Information

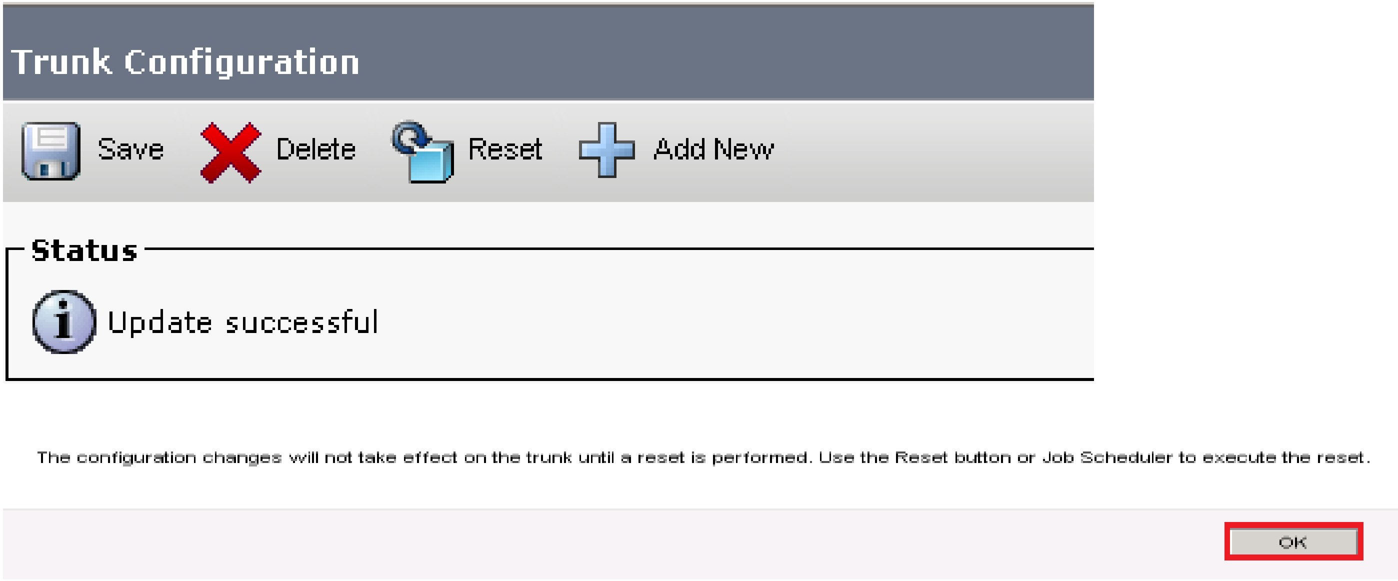
Destination

□ 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. Click Save then Rest to save and apply changes.

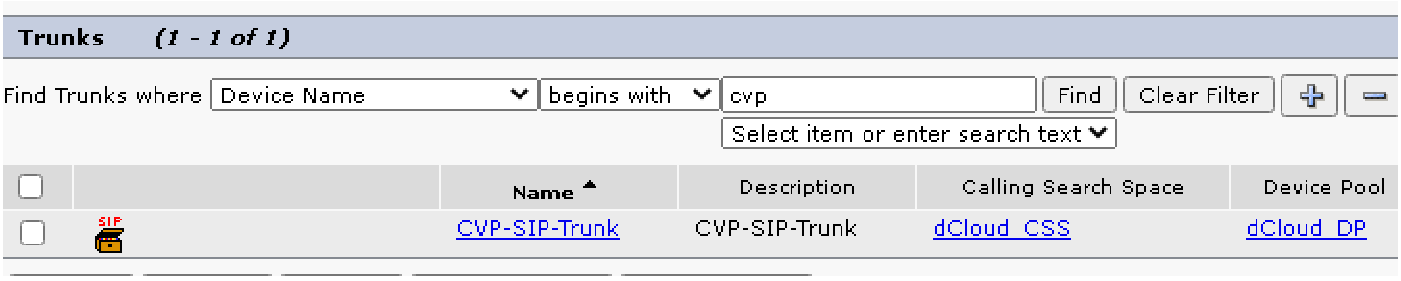


Status

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. Navigate to Device > Trunk, search for CVP trunk, in this example CVP trunk name is cvp-SIP-Trunk. Click Find.



Trunks (1 - 1 of 1)

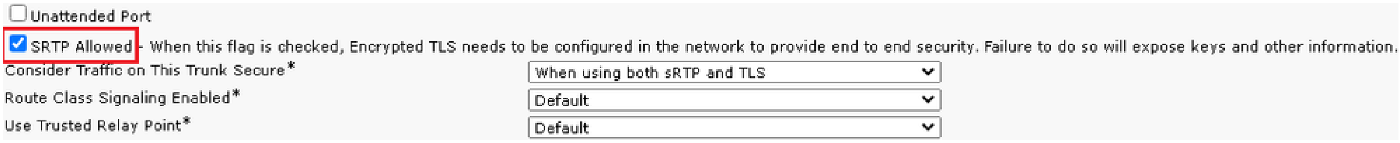
Find Trunks where Device Name begins with cvp

Select item or enter search text

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

9. Click CVP-SIP-Trunk to open the CVP trunk configuration page.

10. In Device Information section, check SRTP Allowed check box in order to enable SRTP.



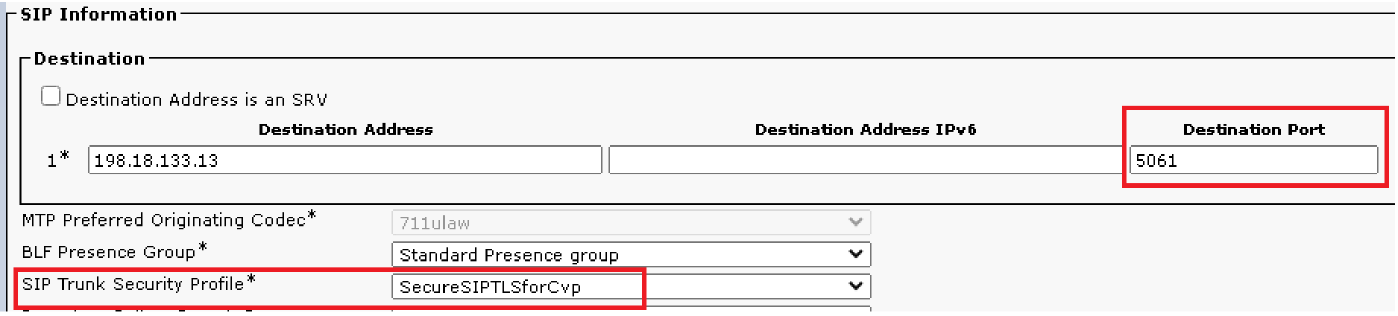
☐ Unattended Port

☑ 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. Scroll down to the SIP Information section, change the Destination Port to 5061.

12. Change SIP Trunk Security Profile to SecureSIPTLSForCvp.



SIP Information

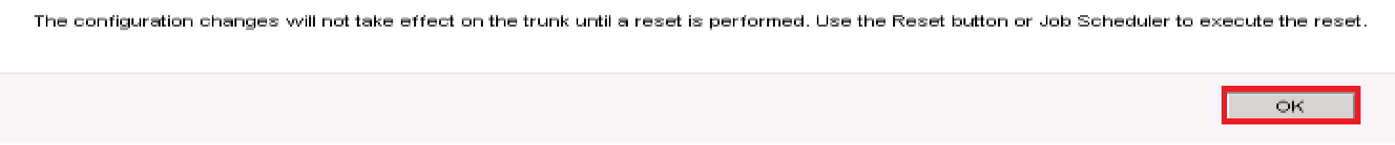
Destination

☐ 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. Click Save then Rest to save and apply changes.



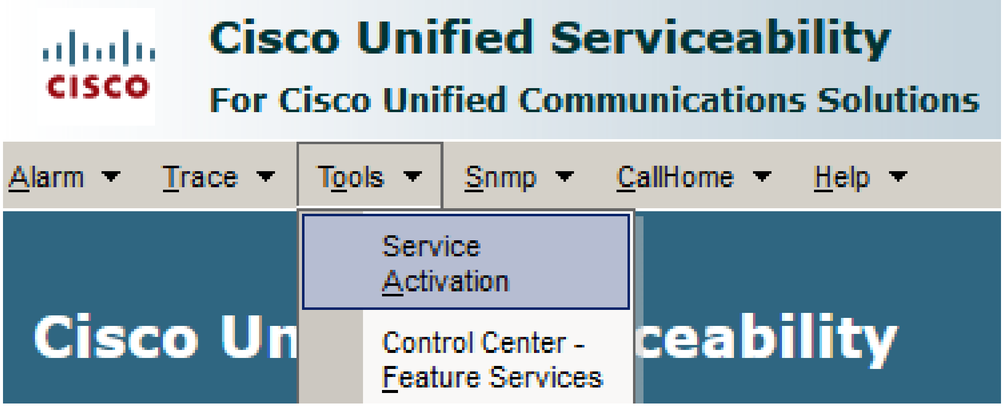
The configuration changes will not take effect on the trunk until a reset is performed. Use the Reset button or Job Scheduler to execute the reset.

Secure Agents’ Device Communication with CUCM

In order to enable security features for a device, you must install a Locally Significant Certificate (LSC) and assign the security profile to that device. The LSC possesses the public key for the endpoint, which is signed by the CUCM CAPF private key. It is not installed on phones by default.

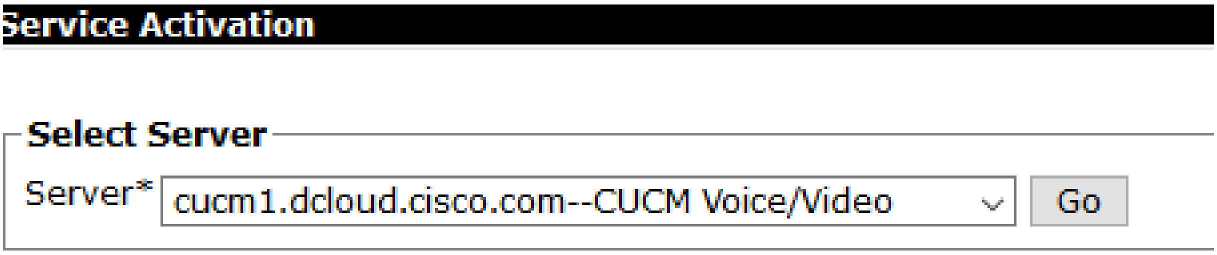
Steps:

1. Log in to Cisco Unified Serviceability interface.
2. Navigate to 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. Choose the CUCM server and click Go.

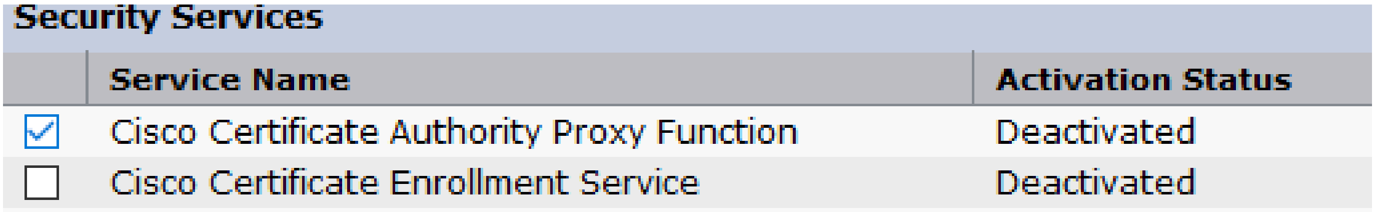


Service Activation

Select Server

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

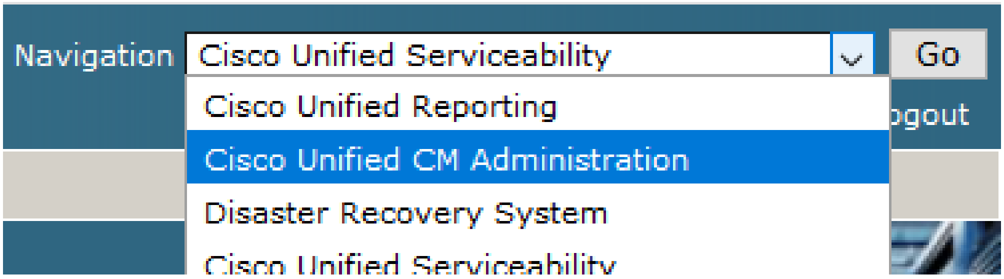
4. Check Cisco Certificate Authority Proxy Function and click Save to activate the service. Click Ok to confirm.



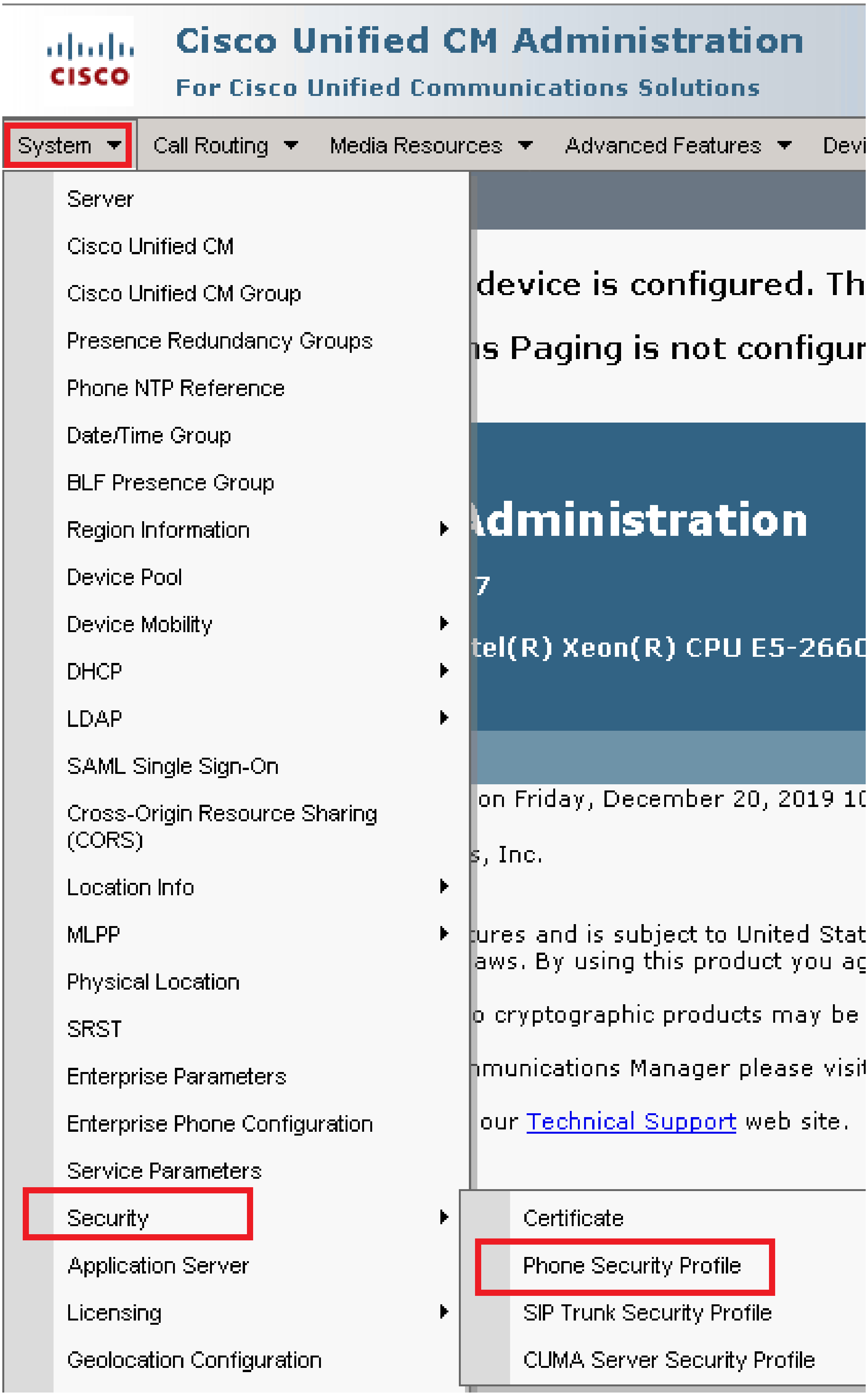
Security Services

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

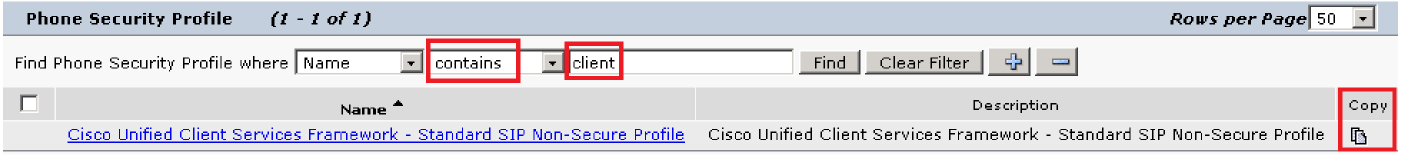
5. Ensure the service is activated then navigate to CUCM administration.


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

6. After successful login to CUCM administration, navigate to System > Security > Phone Security Profile in order to create a device security profile for the agent device.


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
is Paging is not configur
Administration
7
tel(R) Xeon(R) CPU E5-266
on Friday, December 20, 2019 1
s, Inc.
tures and is subject to United Stat
aws. By using this product you ag
o cryptographic products may be
mmunications Manager please visit
our Technical Support web site.

7. Find the security profile respective to your agent device type. In this example, a soft phone is used, so choose Cisco Unified Client Services Framework - Standard SIP Non-Secure Profile. Click copy icon 📋 in order to copy this profile.

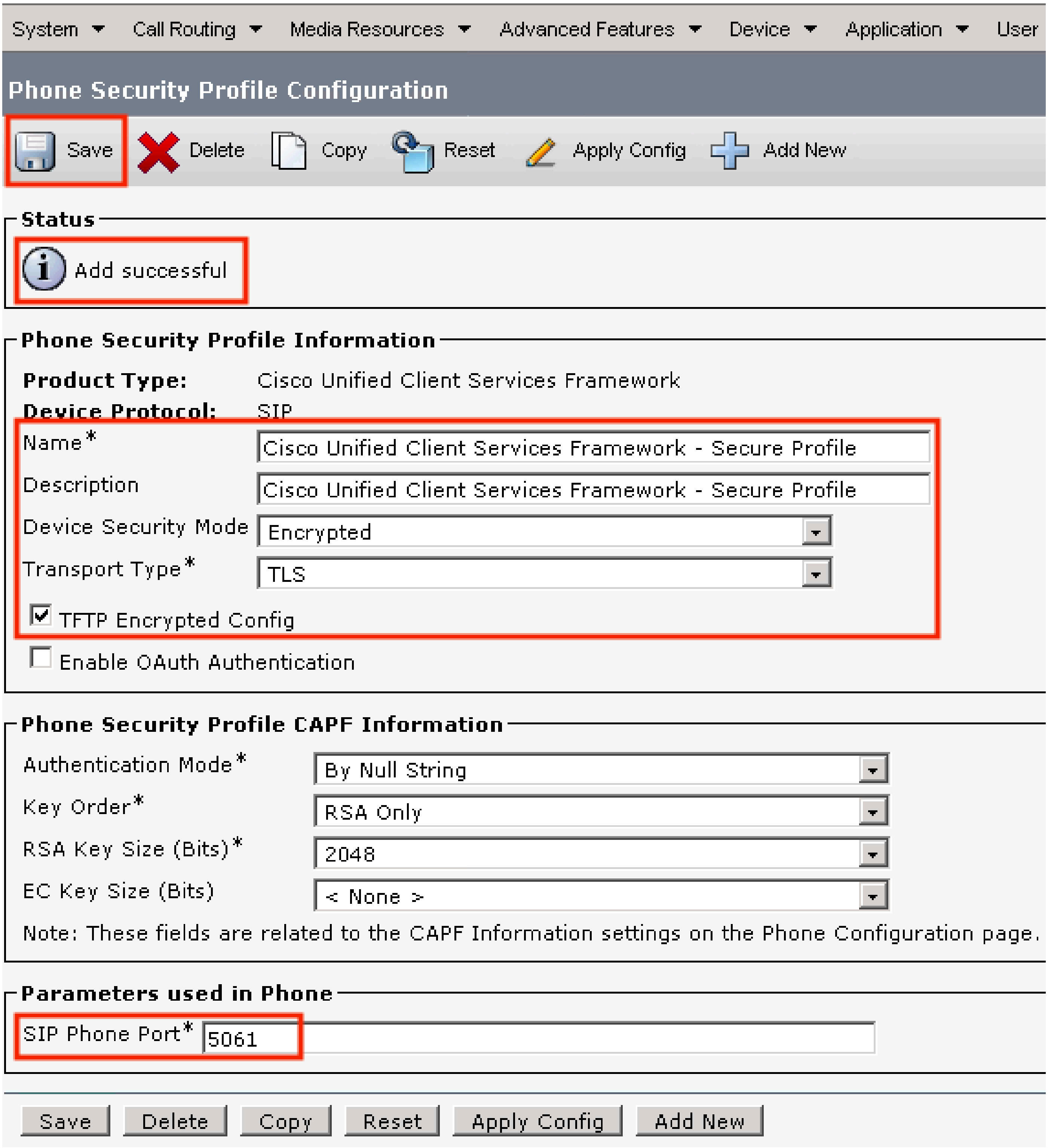


Phone Security Profile (1 - 1 of 1) Rows per Page 50

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. Rename the profile to Cisco Unified Client Services Framework - Secure Profile. Change the parameters as in this image then click Save at the top left of the page.



Phone Security Profile Configuration

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

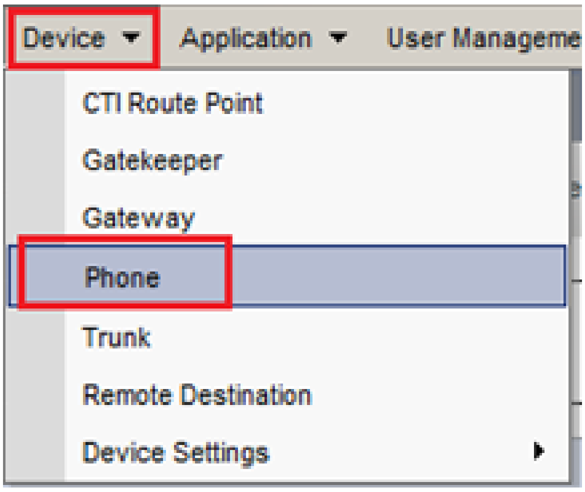
Authentication Mode*	By Null String
Key Order*	RSA Only
RSA Key Size (Bits)*	2048
EC Key Size (Bits)	< None >

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

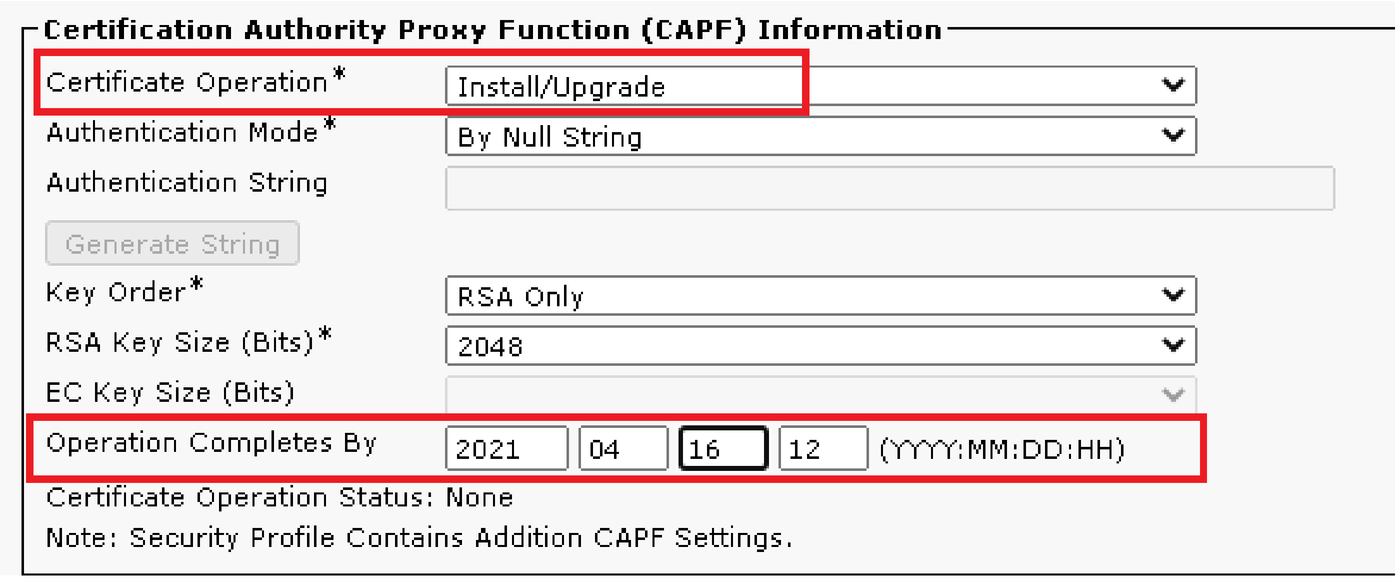
Parameters used in Phone

SIP Phone Port* 5061

9. After the successful creation of the phone device profile, navigate to Device > Phone.



10. Click Find to list all available phones then click agent phone.
11. Agent phone configuration page opens. Find Certification Authority Proxy Function (CAPF) Information section. In order to install LSC, set Certificate Operation to Install/Upgrade and Operation Completes by to any future date.

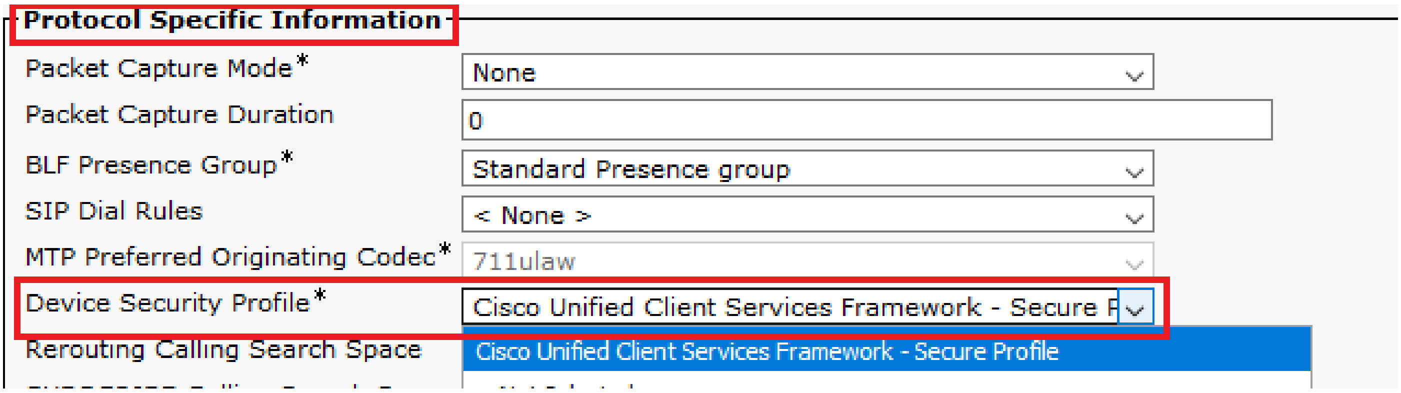


Certification Authority Proxy Function (CAPF) Information

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.

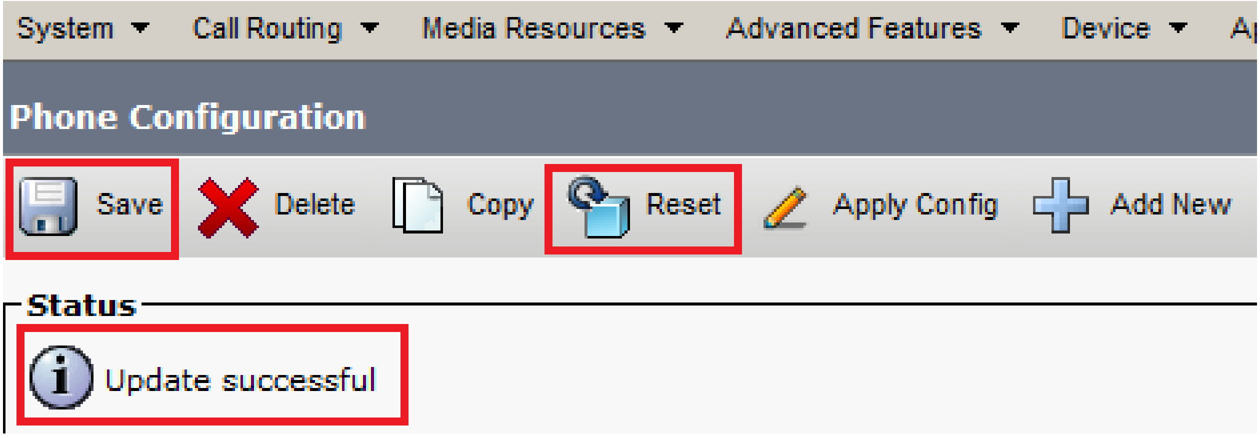
12. Find Protocol Specific Information section and change the Device Security Profile to Cisco Unified Client Services Framework – Secure Profile.



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. Click Save at the top left of the page. Ensure the changes are saved successfully, then click Reset.

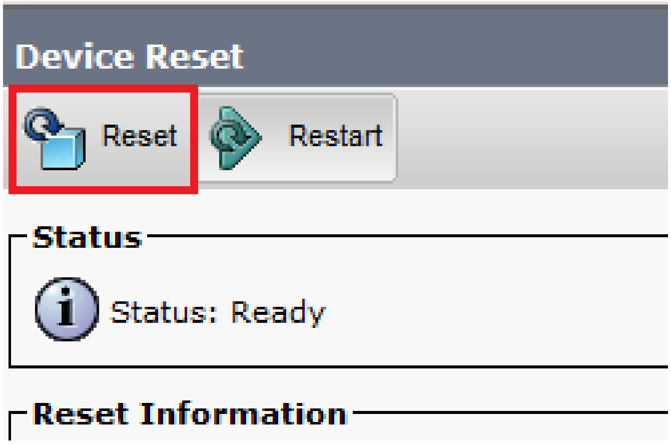


Phone Configuration

Status

Update successful

14. A pop-up window opens, click Reset to confirm the action.



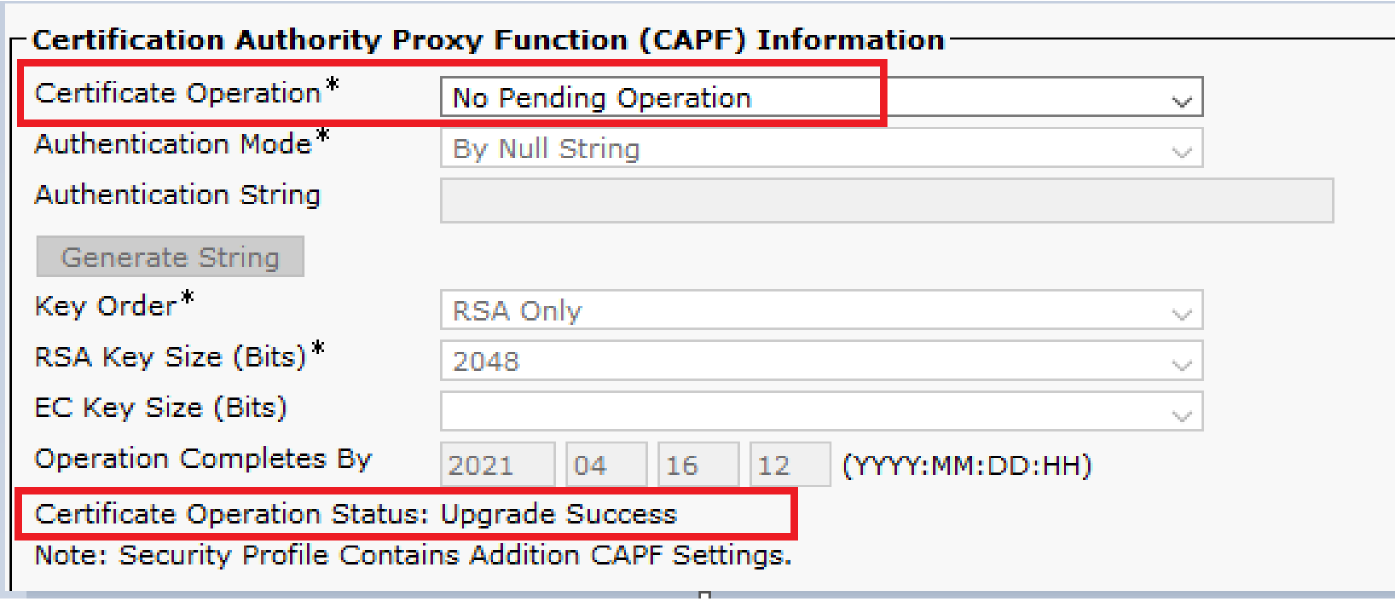
Device Reset

Status

Status: Ready

Reset Information

15. After the agent device registers once again with CUCM, refresh the current page and verify the LSC is installed successfully. Check Certification Authority Proxy Function (CAPF) Information section, Certificate Operation must be set to No Pending Operation and Certificate Operation Status is set to Upgrade Success.



Certification Authority Proxy Function (CAPF) Information

Certificate Operation*	No Pending Operation
Authentication Mode*	By Null String
Authentication 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

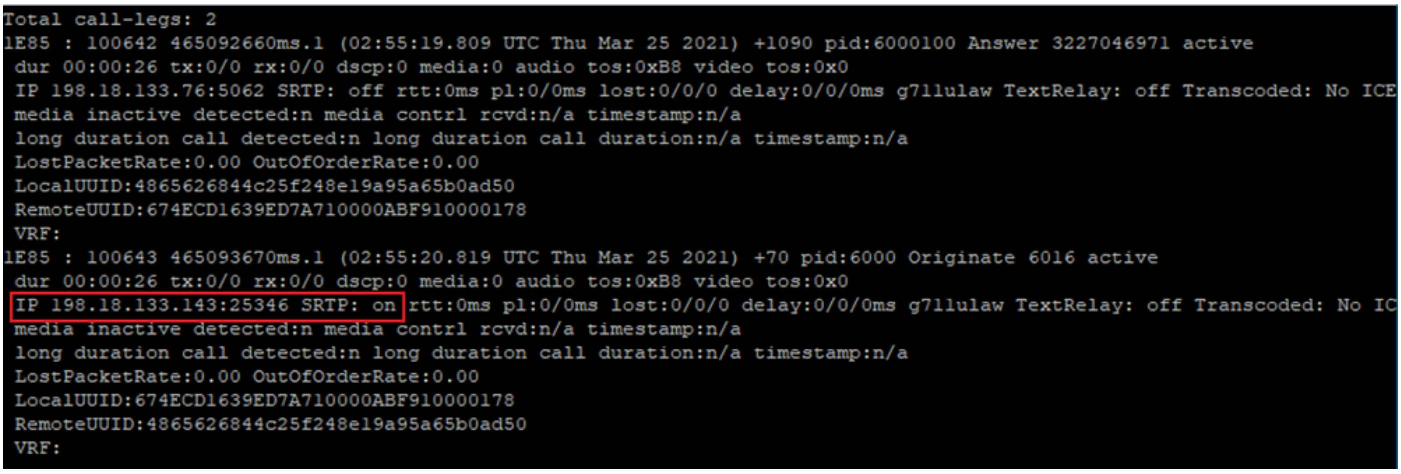
Note: Security Profile Contains Addition CAPF Settings.

16. Refer to the same steps from Step. 7 - 13 to secure other agents' devices that you want to use secure SIP and RTP with CUCM.

Verify

In order to validate RTP is properly secured, perform these steps:

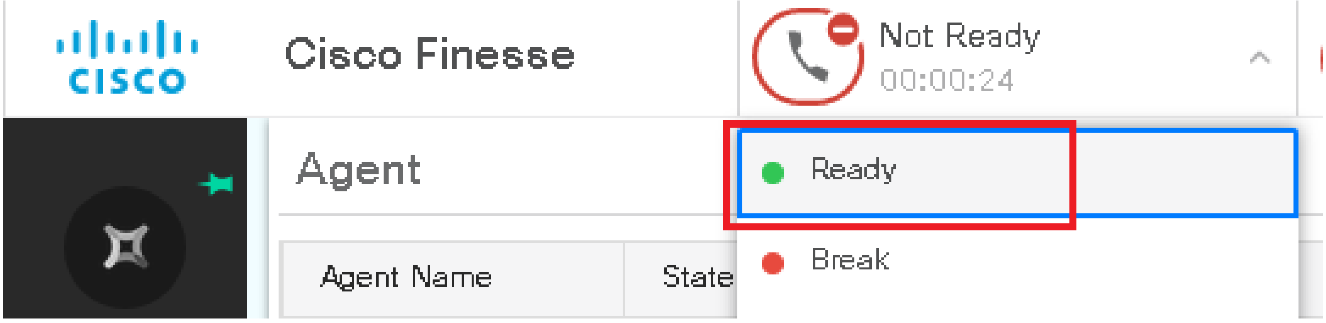
1. Make a test call to the contact center, and listen to IVR prompt.
2. At the same time, open the SSH session to vCUBE, and run this command:
   show call active voice brief



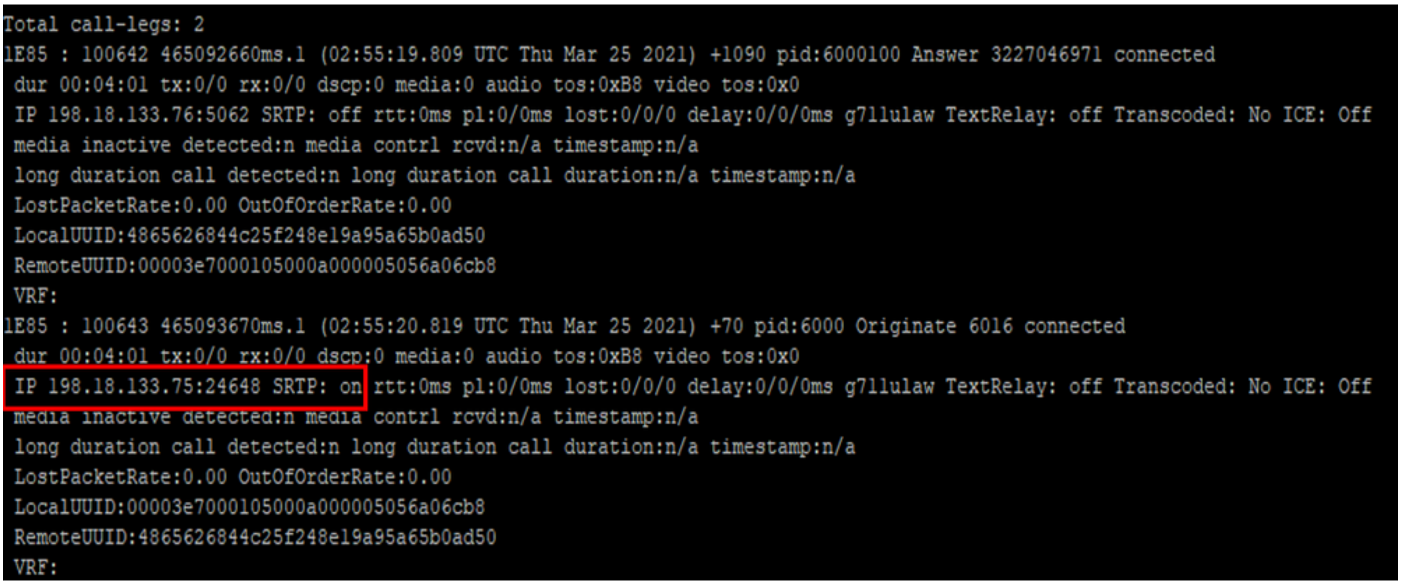
```
Total call-legs: 2
1E85 : 100642 465092660ms.1 (02:55:19.809 UTC Thu Mar 25 2021) +1090 pid:6000100 Answer 3227046971 active
 dur 00:00:26 tx:0/0 rx:0/0 dscp:0 media:0 audio tos:0xB8 video tos:0x0
 IP 198.18.133.76:5062 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off Transcoded: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

Tip: Check if the SRTP is on between CUBE and VVB (198.18.133.143). If yes, this confirms RTP traffic between CUBE and VVB is secure.

3. Make an agent available to answer the call.
   .



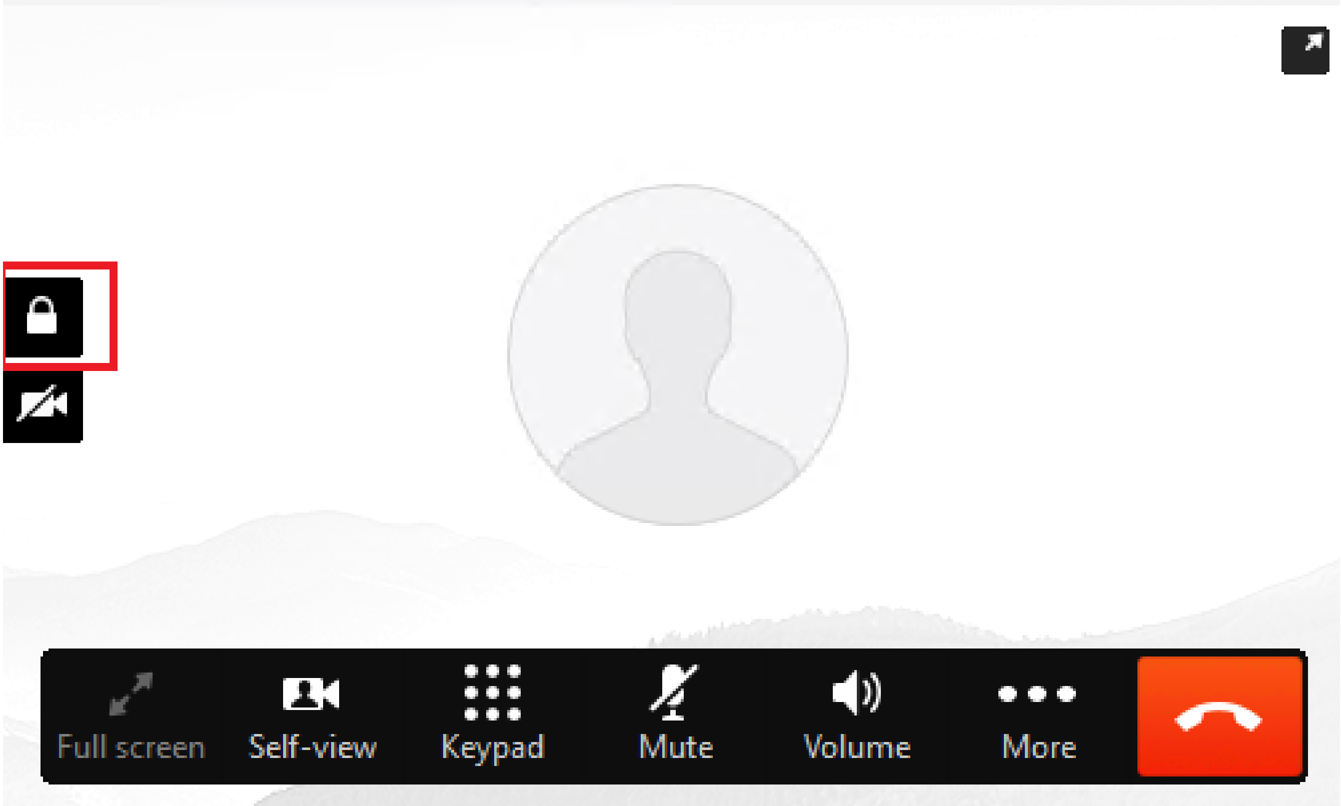
4. The agent gets reserved and the call is routed to the agent. Answer the call.
5. The call gets connected to the agent. Go back to the vCUBE SSH session, and run this command:
   show call active voice brief



```
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:
```

Tip: Check if the SRTP is `on` between CUBE and the agents' phones (198.18.133.75). If yes, this confirms RTP traffic between CUBE and Agent is secure.

6. Also, once the call is connected, a security lock is displayed on the agent device. This also confirms the RTP traffic is secure.



To validate that the SIP signals are properly secured, refer to [Configure Secure SIP Signaling](#) article.