Configure Secure SIP Signaling in Contact Center Enterprise

Contents

Introduction

This document describes how to secure Session Initiation Protocol (SIP) signaling 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

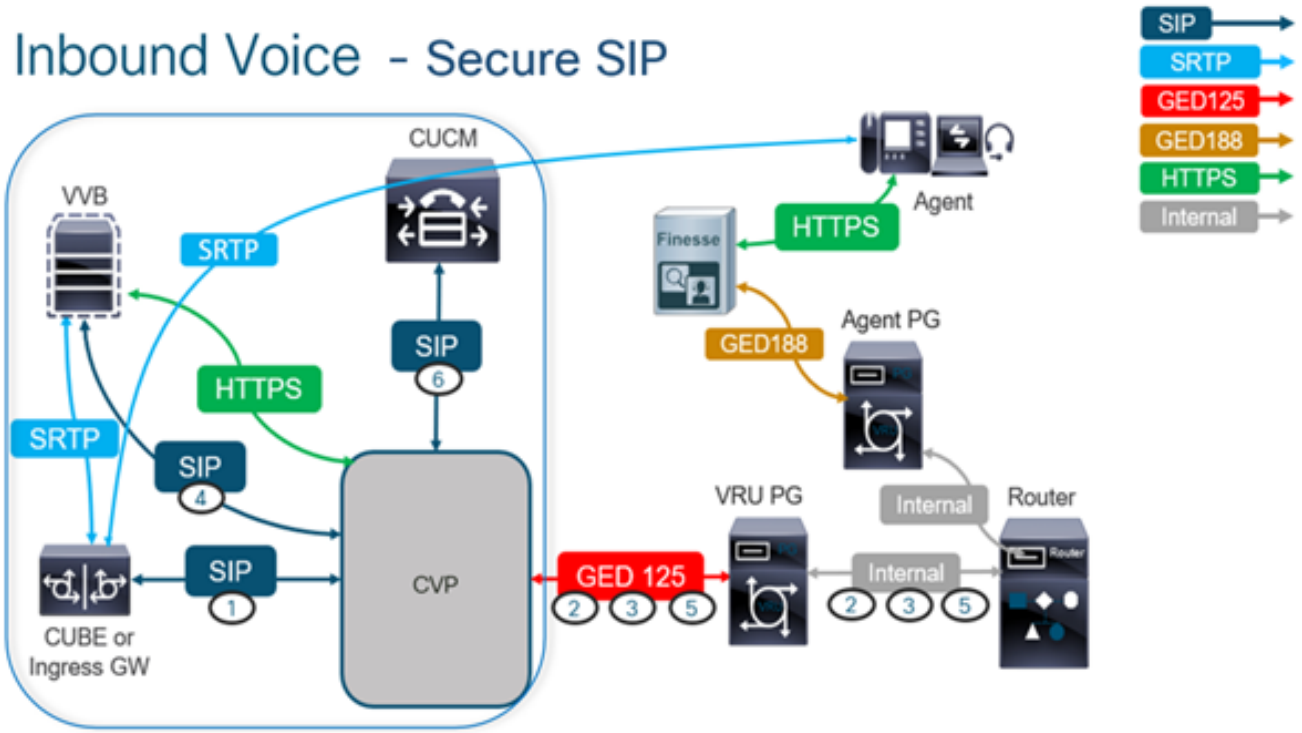
Components Used

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 earlier 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

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



Task 1. CUBE Secure Configuration

In this task, configure CUBE to secure the SIP protocol messages.

Required configurations:

- Configure a Default Trustpoint for the SIP User Agent (UA)
- Modify the Dial-peers to use Transport Layer Security (TLS)

Steps:

1. Open Secure Shell (SSH) session to CUBE.
2. Run these commands to have the SIP stack use the Certificate Authority (CA) certificate of the CUBE. CUBE establishes a 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 exit

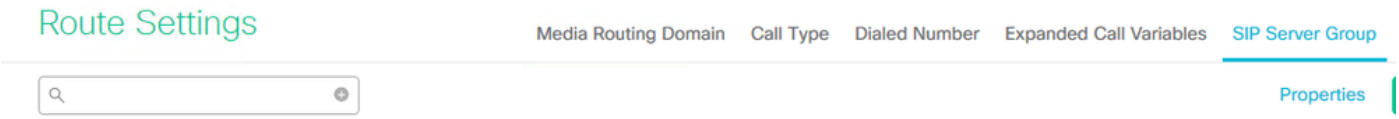
```
CC-VCUBE#
CC-VCUBE#Conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CC-VCUBE(config)#dial-peer voice 6000 voip
CC-VCUBE(config-dial-peer)#session target ipv4:198.18.133.13:5061
CC-VCUBE(config-dial-peer)#session transport tcp tls
CC-VCUBE(config-dial-peer)#
CC-VCUBE(config-dial-peer)#exit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

Task 2. CVP Secure Configuration

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

Steps:

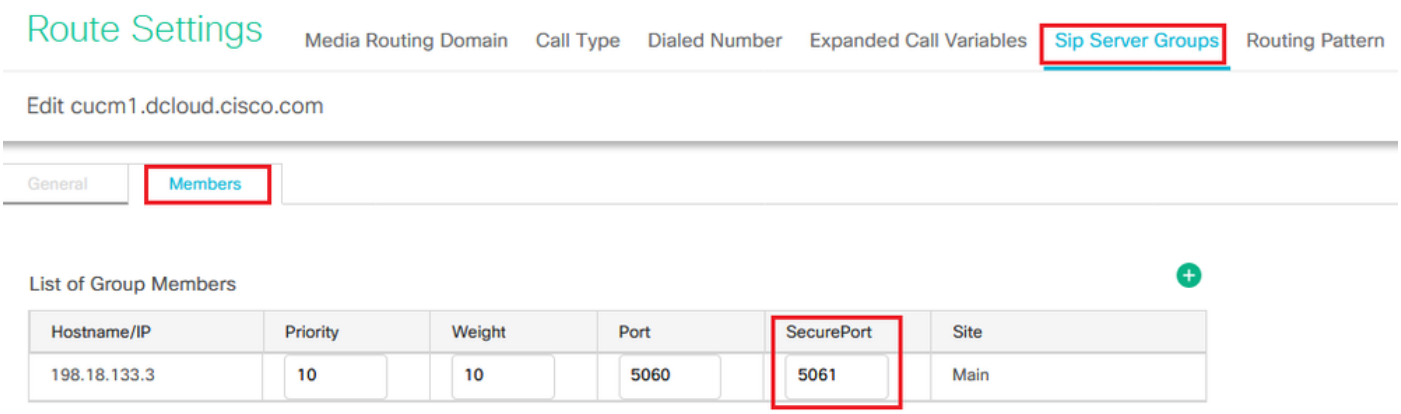
1. Log in toUCCE Web Administration.
2. Navigate to Call Settings > Route Settings > SIP Server Group.



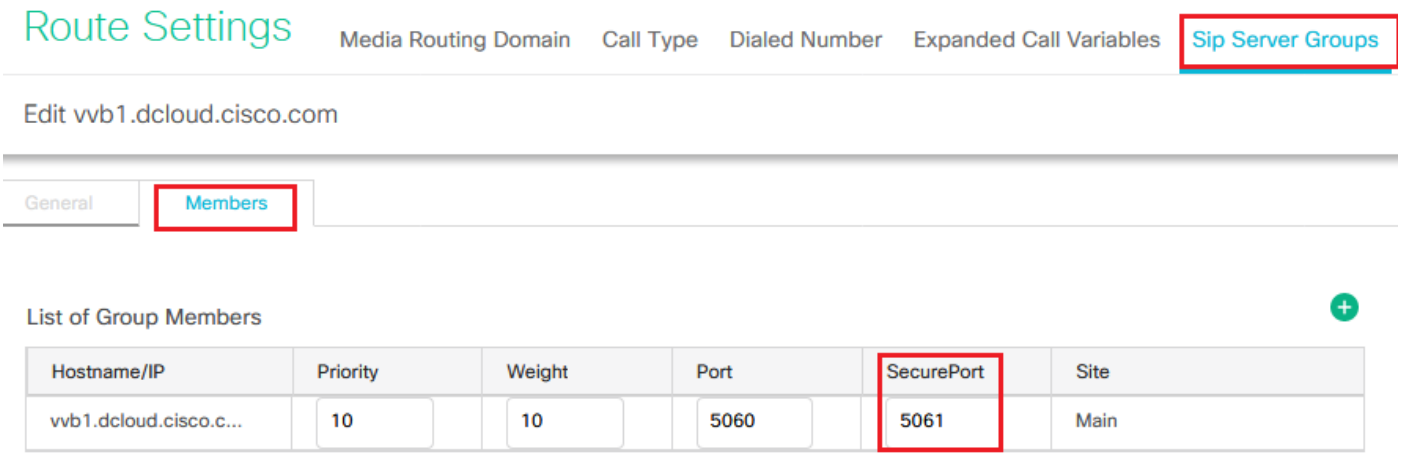
Based on your configurations, you have SIP Server Groups configured for CUCM, CVVB, and CUBE. You need to set secure SIP ports to 5061 for all of them. In this example, these SIP server groups are used:

- 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, which shows the details of the SIP Server Group Configuration. Set SecurePort to 5061 and click Save .



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

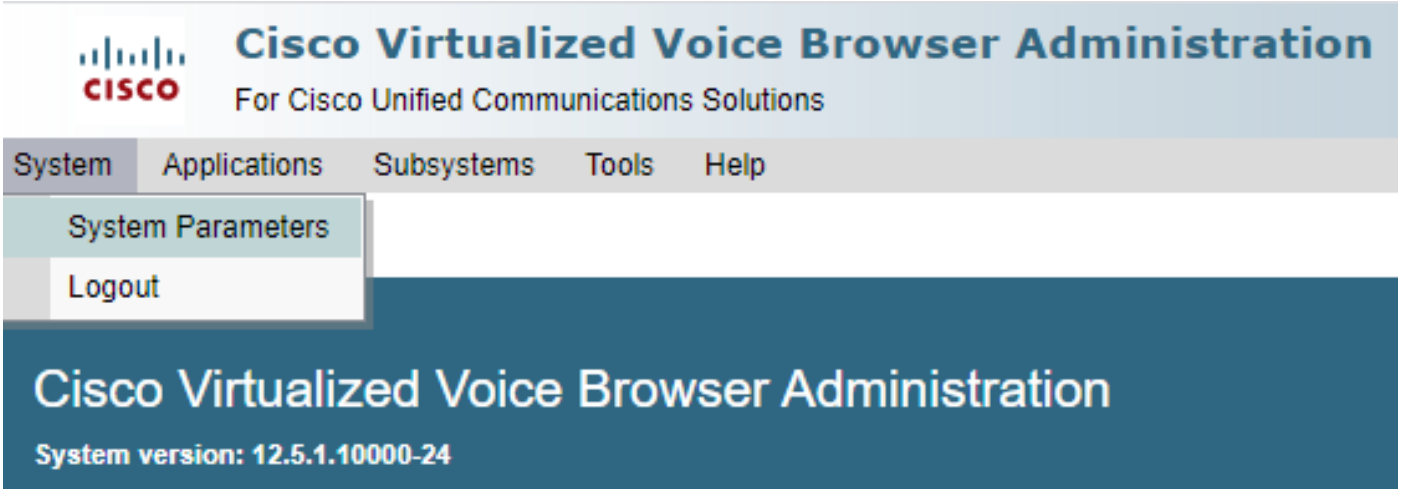


Task 3. CVVB Secure Configuration

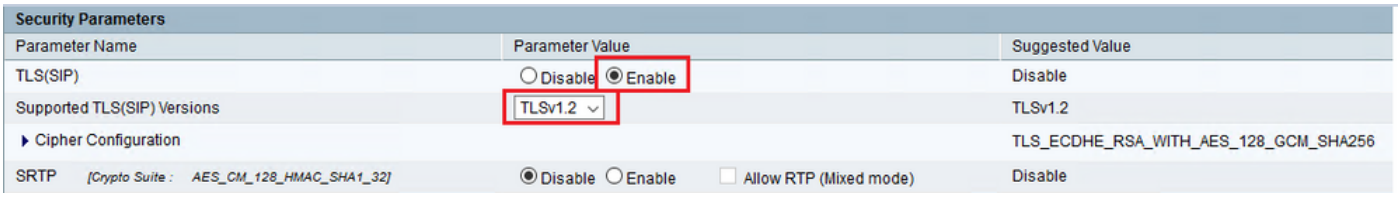
In this task, configure CVVB to secure the SIP protocol messages (SIP TLS).

Steps:

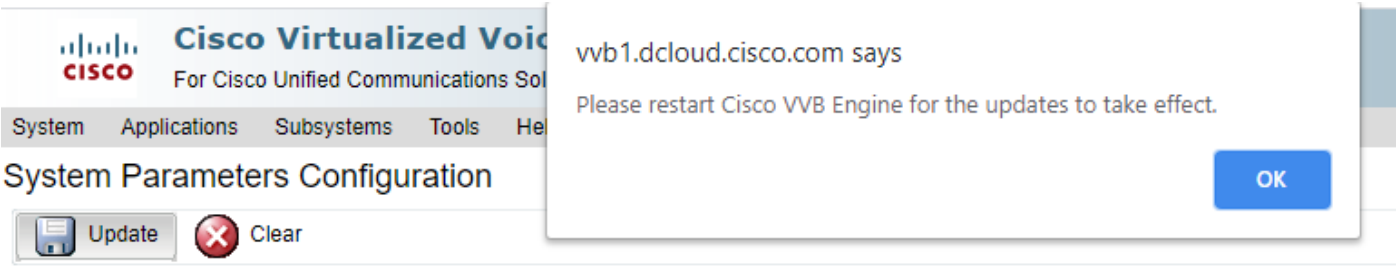
1. Log in to **Cisco VVB Administration** page.
2. Navigate to System > System Parameters.



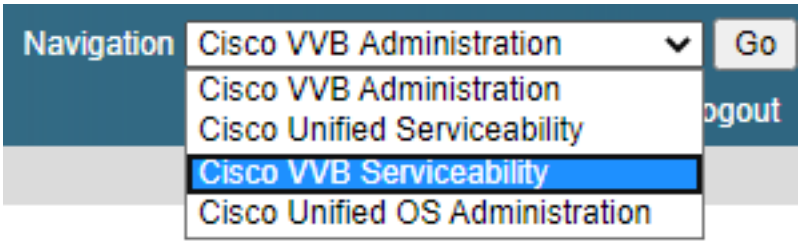
3. In the Security Parameters section, choose Enable for TLS(SIP) . Keep Supported TLS(SIP) version as TLSv1.2.



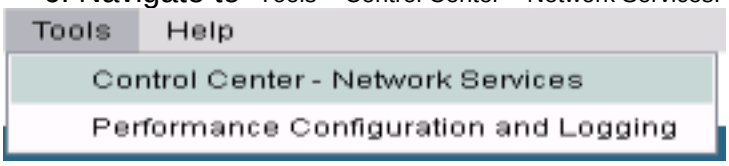
4. Click **Update**. Click Ok when prompted to restart CVVB engine.



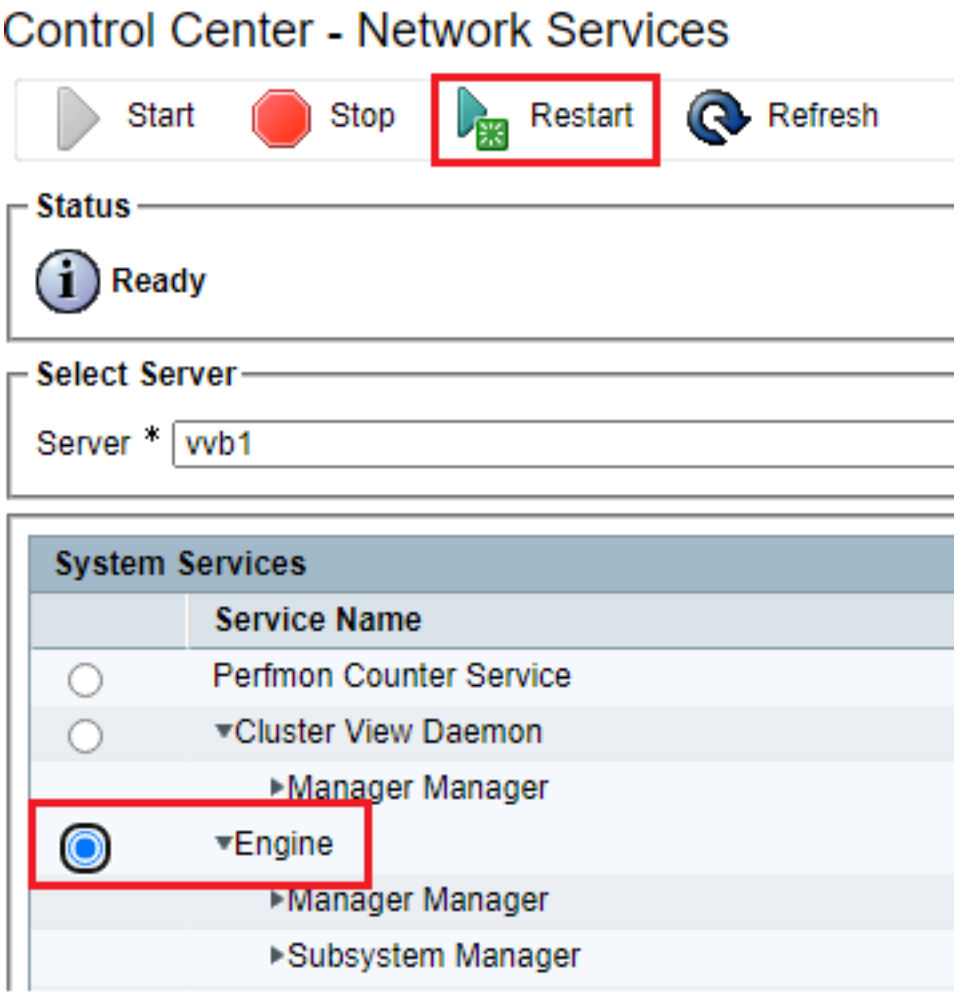
5. These changes require a restart of the Cisco VVB engine. In order to restart the VVB engine, navigate to Cisco VVB Serviceability then click **Go**.



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



7. Choose Engine and click Restart.



Task 4. CUCM Secure Configuration

In order to secure SIP messages on CUCM, perform the next 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
- Secure Agents' Device Communication with CUCM

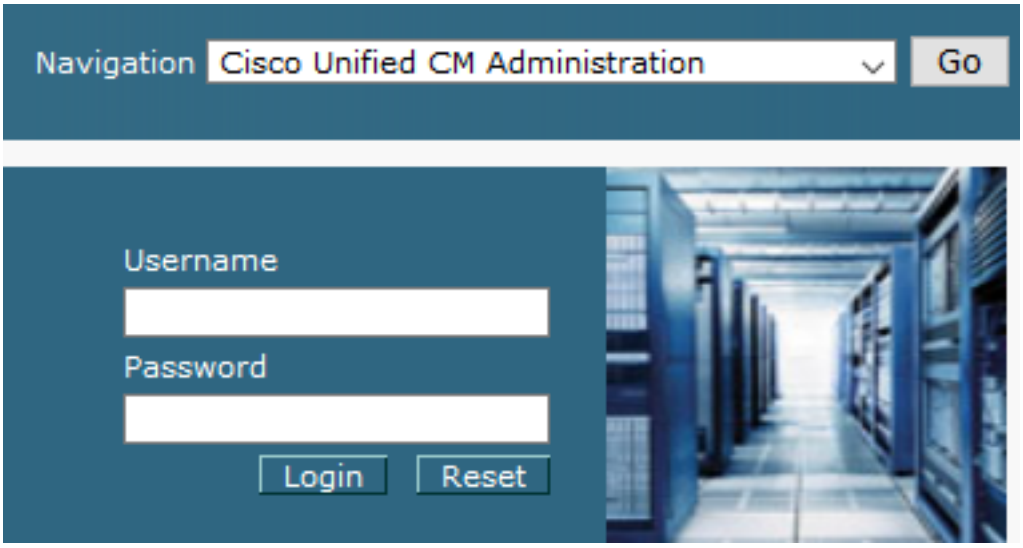
Set CUCM Security Mode to Mixed Mode

CUCM supports two security modes:

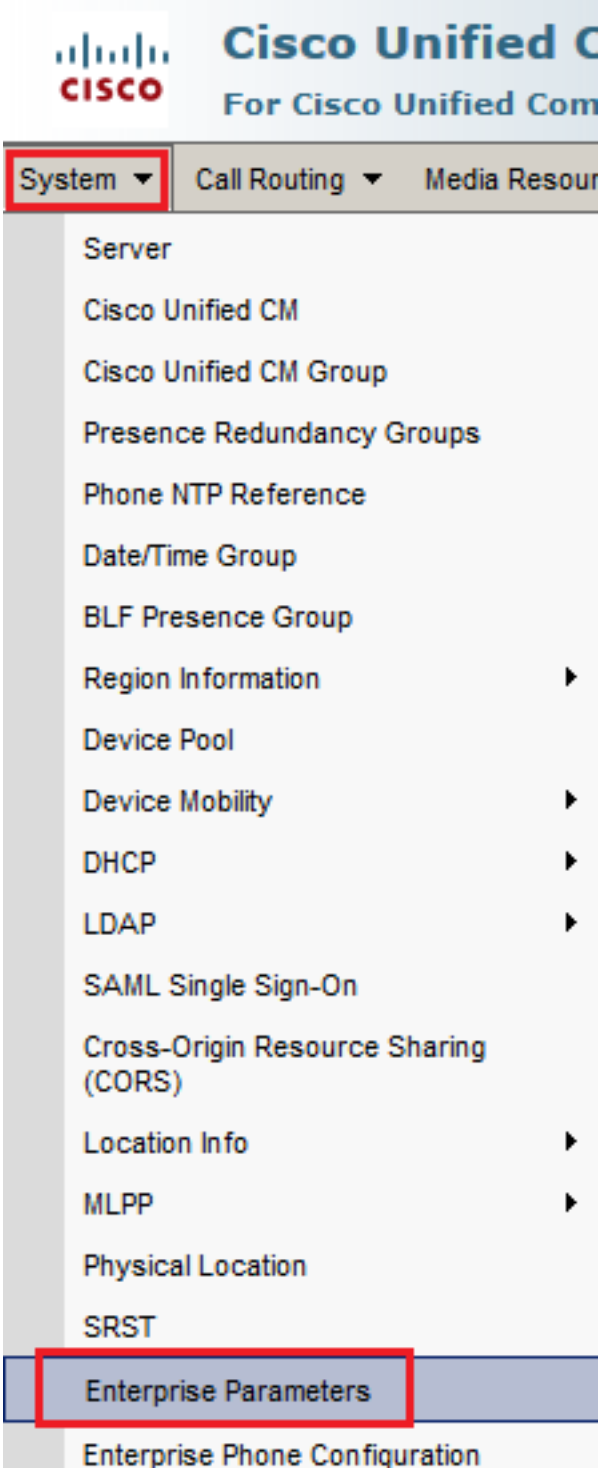
- Non-secure mode (default mode)
- Mixed mode (secure mode)

Steps:

1. In order to set the security mode to Mixed Mode, log in to Cisco Unified CM Administration interface.



2. After you have successfully logged in to CUCM, navigate to System > Enterprise Parameters.



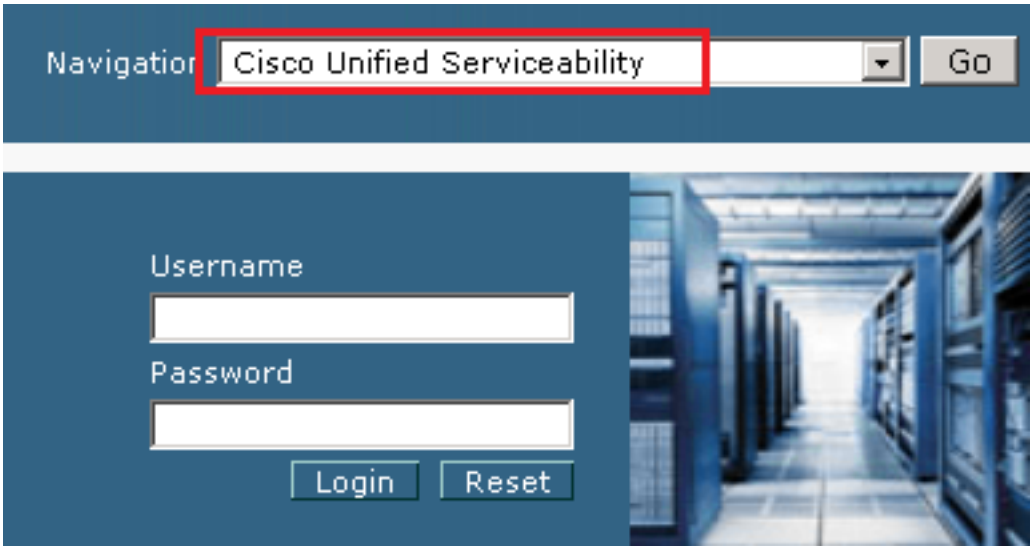
3. Underneath the Security Parameters Section, check if Cluster Security Mode is set to **0**.

4. If Cluster Security Mode is set as 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. After you have successfully logged to CUCM via SSH, run this command: utils ctl set-cluster mixed-mode

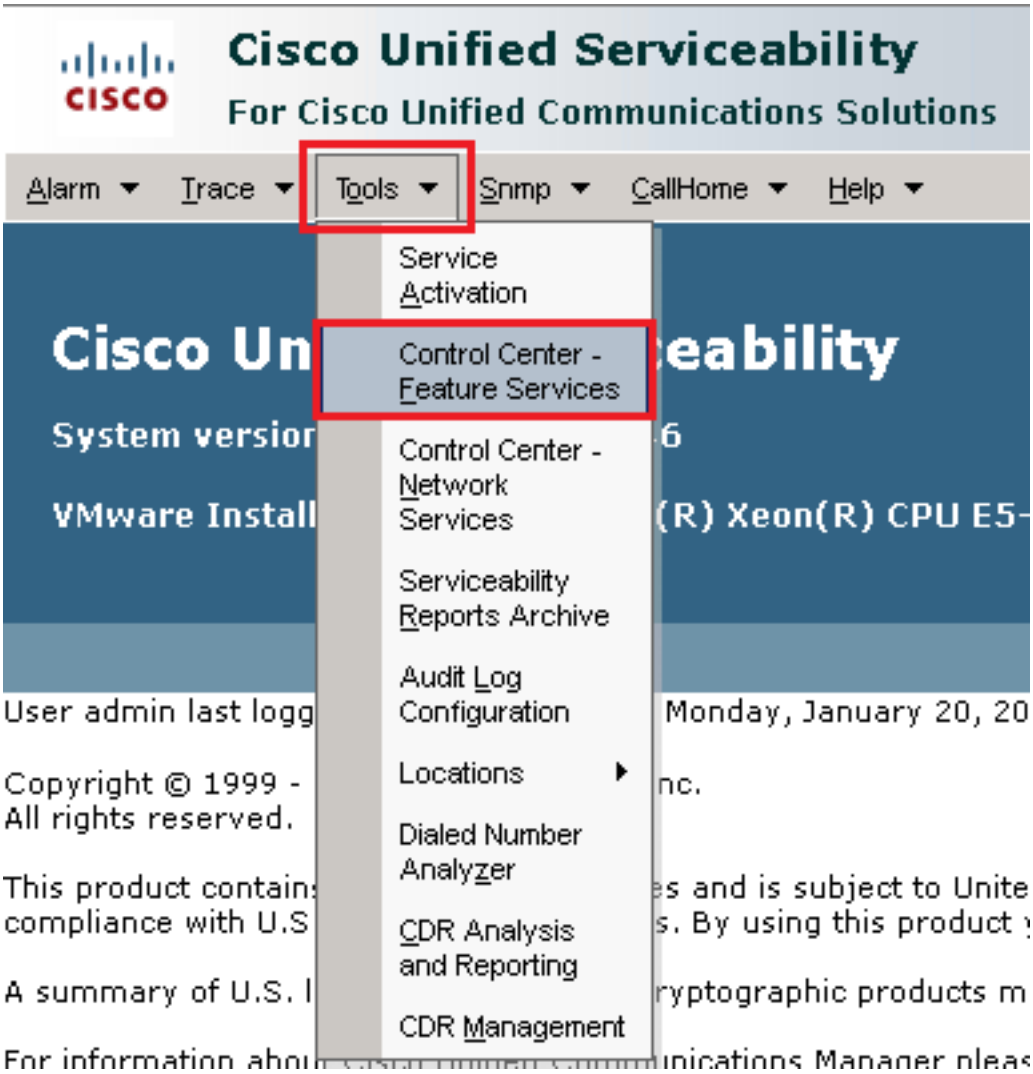
7. Type y and click **Enter** when prompted. This command sets cluster security mode to mixed mode.

```
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 Cisco CallManager and Cisco CTIManager services.
9. In order to restart the services, navigate and log in to Cisco Unified Serviceability.

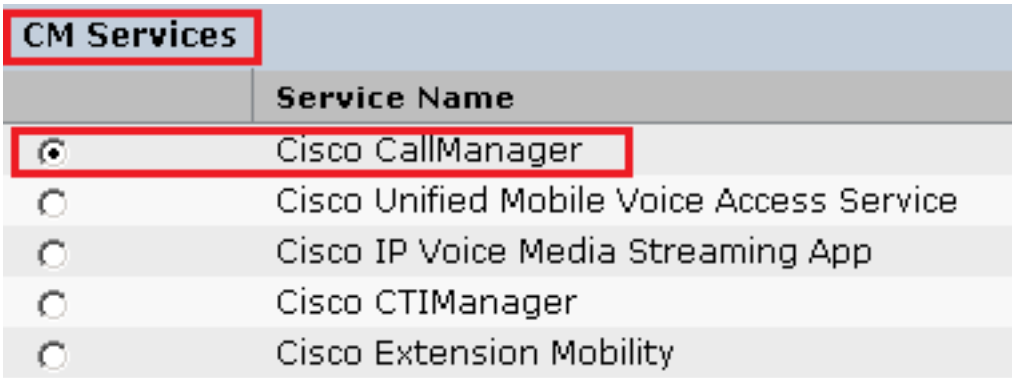


10. After you have successfully logged in, navigate to Tools > Control Center – Feature Services.

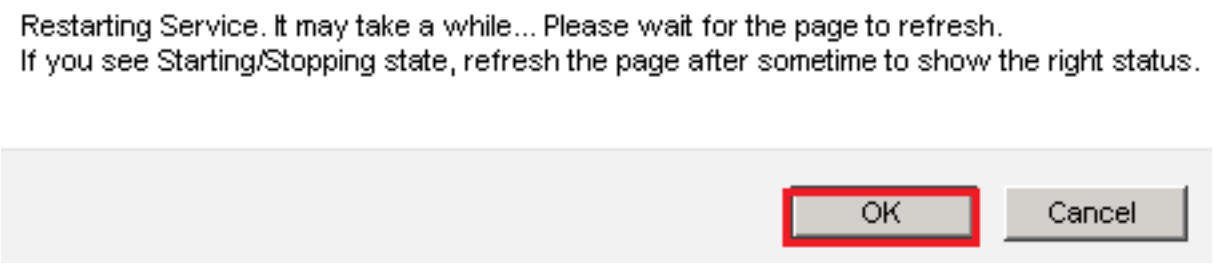


11. Choose the server then click **Go**.

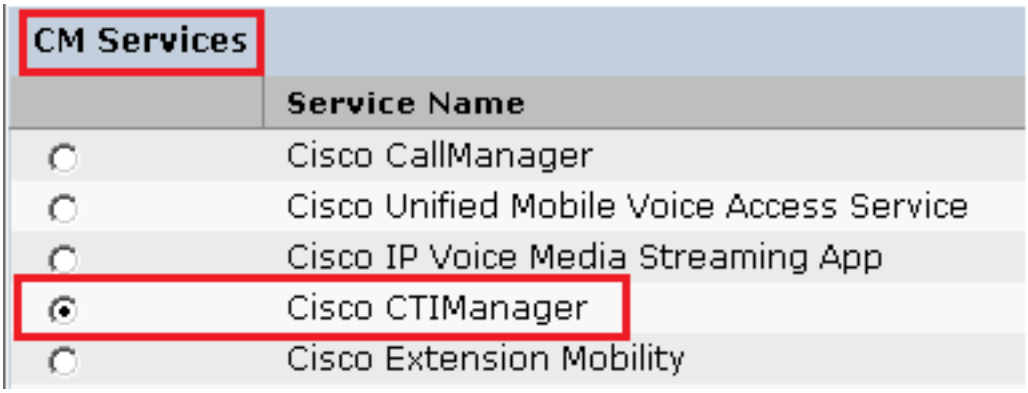
12. Underneath the CM services, choose Cisco CallManager then click Restart button on top of the page.



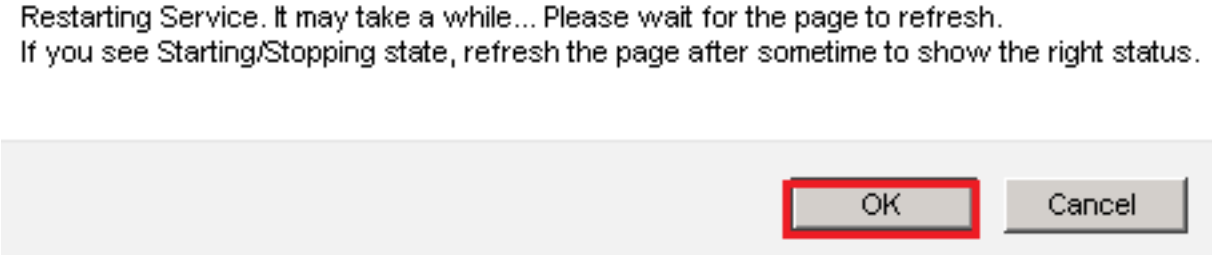
13. Confirm the pop-up message and click **OK**. Wait for the service to successfully restart.



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



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

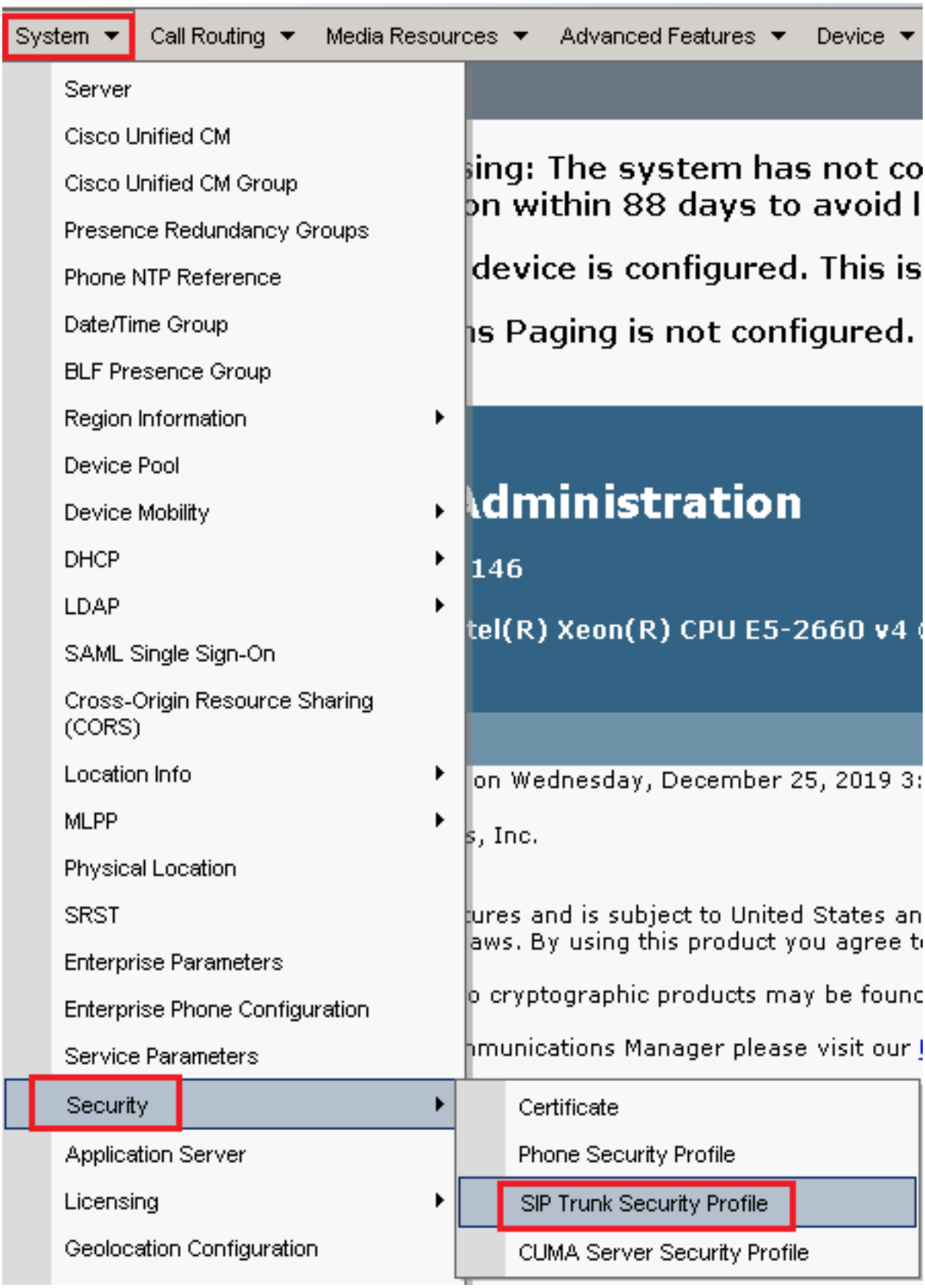


16. After services successfully restart, verify cluster security mode is set to mixed mode, navigate to CUCM administration as explained in Step 5. then check the **Cluster Security Mode**. Now it must be set to **1**.

Configure SIP Trunk Security Profiles for CUBE and CVP

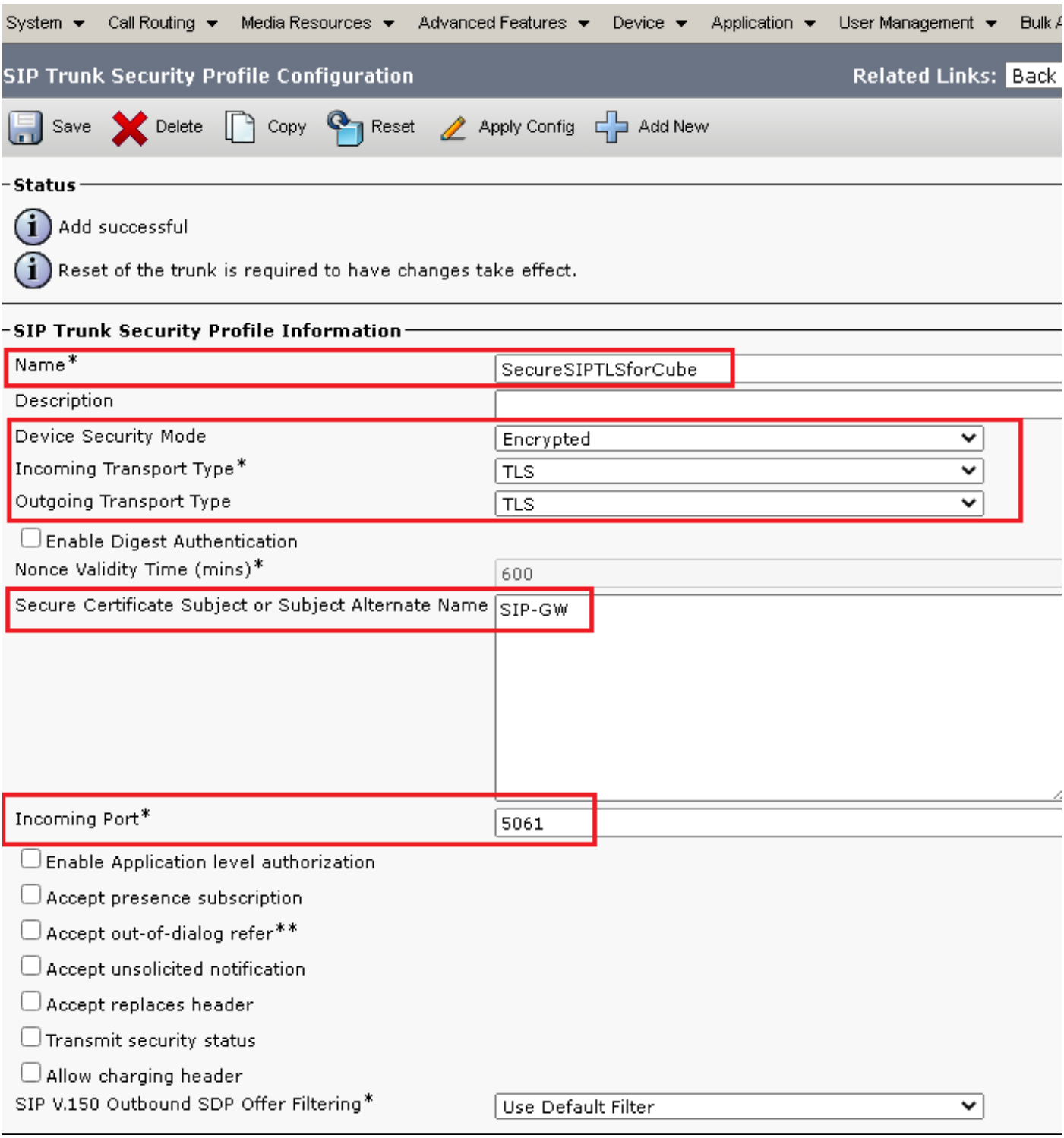
Steps:

1. Log in to 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.



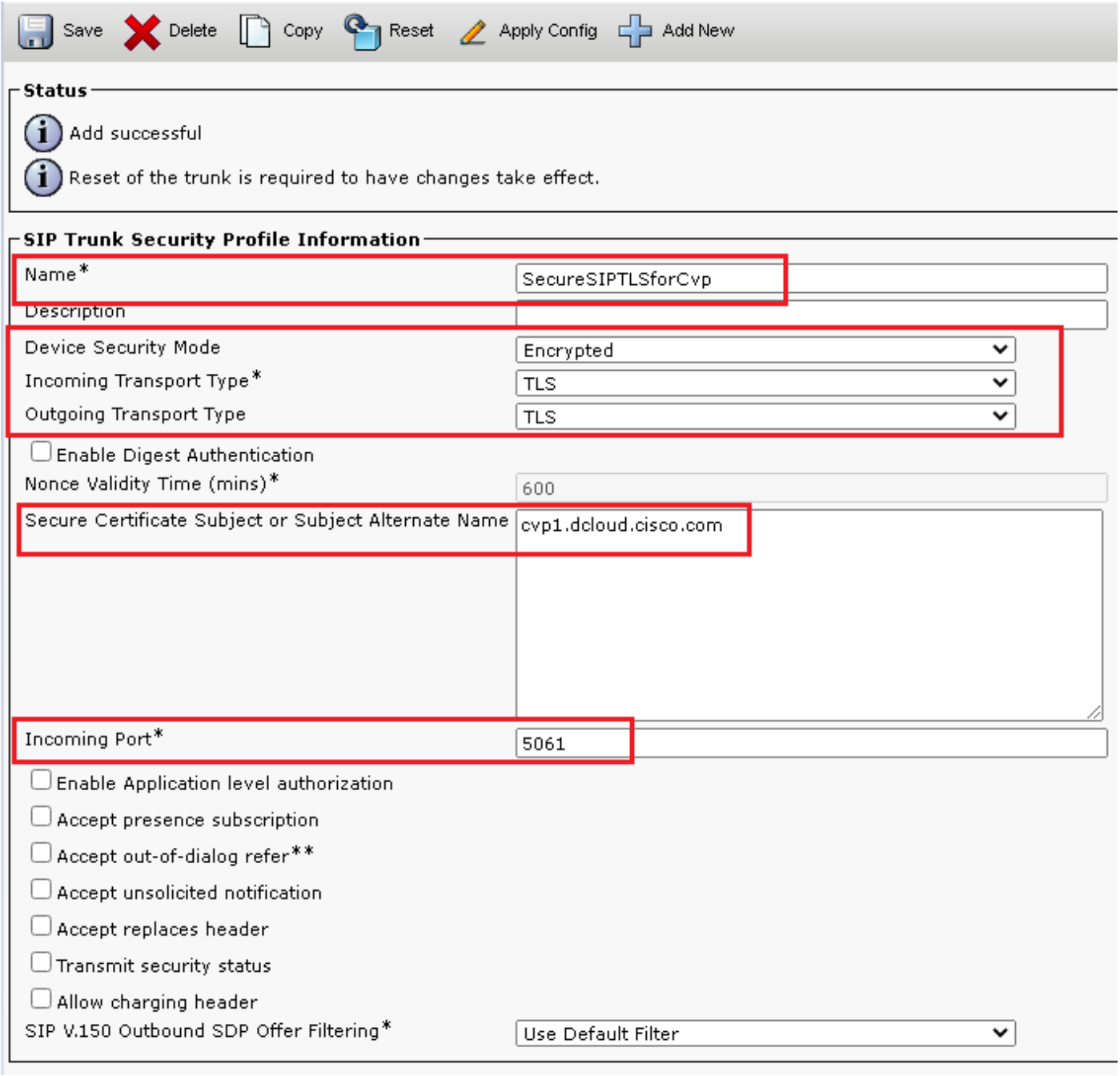
3. On the top left, click Add New in order to add a new profile.

4. Configure SIP Trunk Security Profile as shown in this image then click Save at the bottom left of the page to Save it.



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.

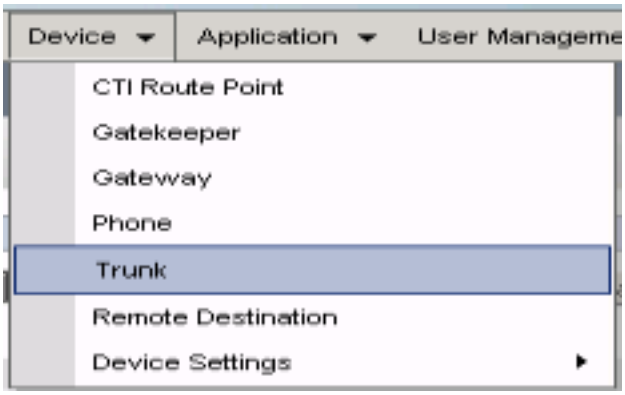
6. Click Copy button and change the Name to SecureSipTLSforCVP and the Secure Certificate Subject to the CN of the CVP call server certificate as it must match. Click Save button.



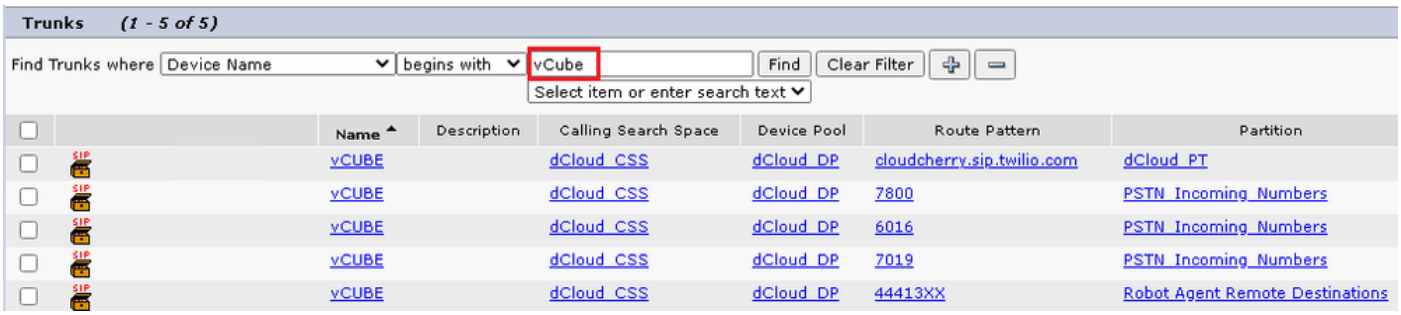
Associate SIP Trunk Security Profiles to Respective SIP Trunks

Steps:

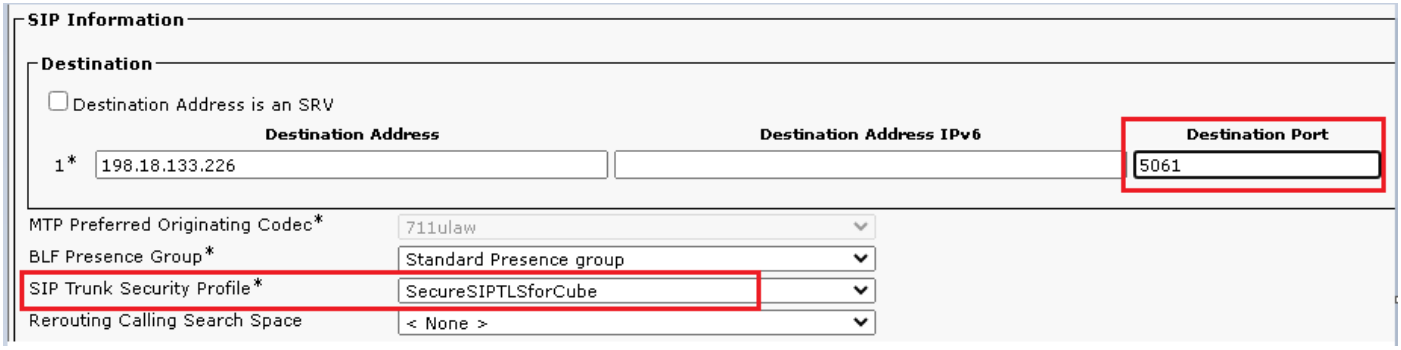
1. On the CUCM Administration page, navigate to Device > Trunk.



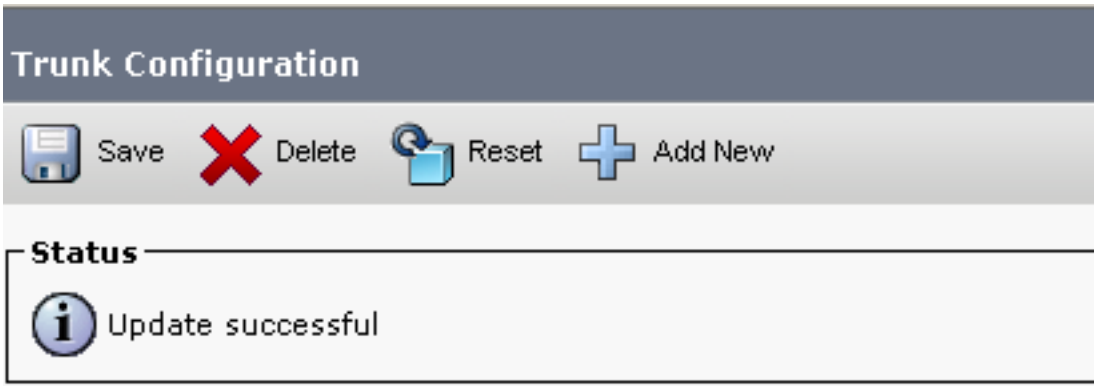
2. Search for CUBE trunk. In this example, the CUBE trunk name is vCube . Click **Find**.



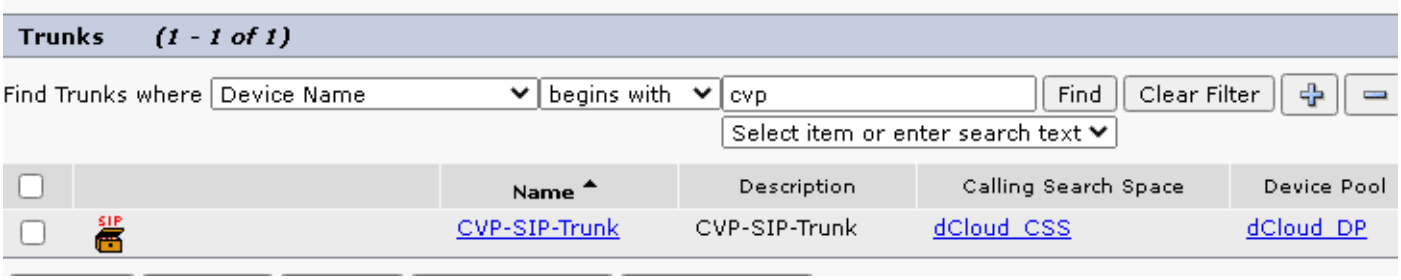
3. Click vCUBE to open the vCUBE trunk configuration page.
4. Scroll down to SIP Information section, and change the Destination Port to 5061.
5. Change SIP Trunk Security Profile to SecureSIPTLSForCube.



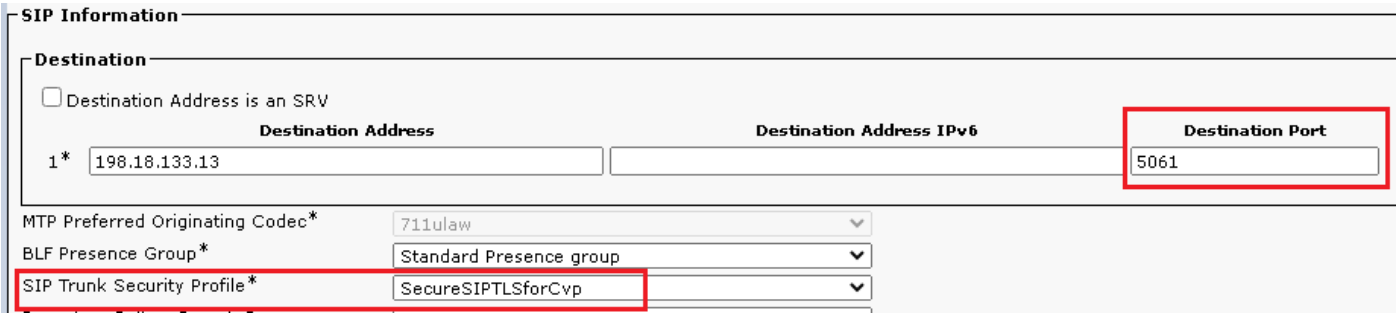
6. Click Save then Rest in order to Save and apply changes.



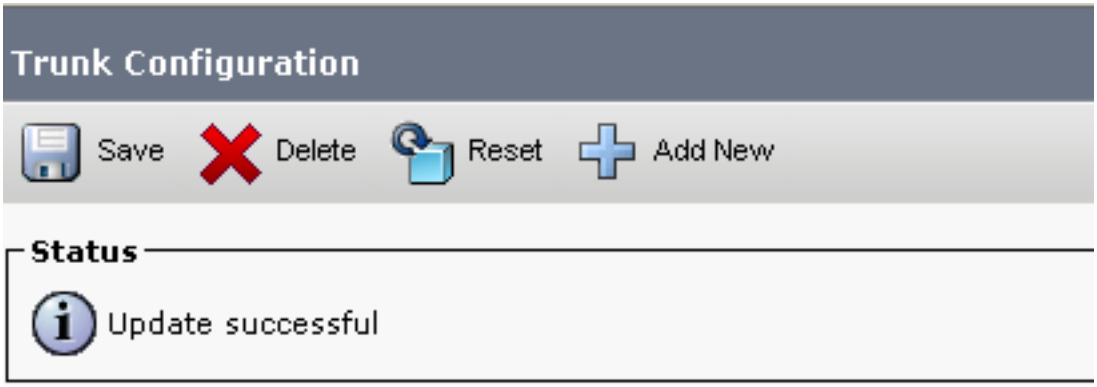
7. Navigate to Device > Trunk, and search for CVP trunk. In this example, the CVP trunk name is cvp-SIP-Trunk . Click **Find**.



8. Click CVP-SIP-Trunk in order to open the CVP trunk configuration page.
9. Scroll down to SIP Information section, and change Destination Port to 5061 .
10. Change SIP Trunk Security Profile to SecureSIPTLSForCvp.



11. Click Save then Rest in order to save and apply changes.



Secure Agents' Device Communication with CUCM

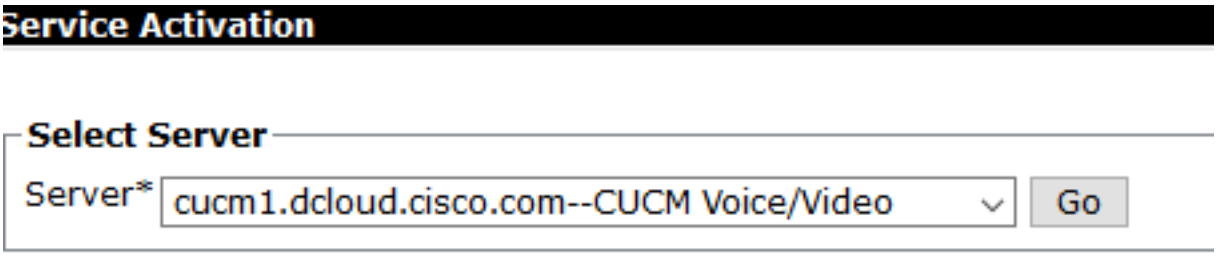
In order to enable security features for a device, you must install a Locally Significant Certificate

(LSC) and assign a security profile to that device. The LSC possesses the public key for the endpoint, which is signed by the Certificate Authority Proxy Function (CAPF) private key. It is not installed on phones by default.

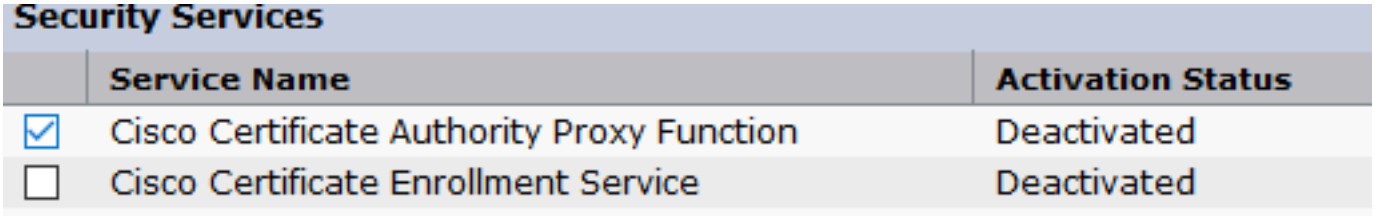
Steps:

1. Log in to Cisco Unified Serviceability Interface.
2. Navigate to Tools > Service Activation.

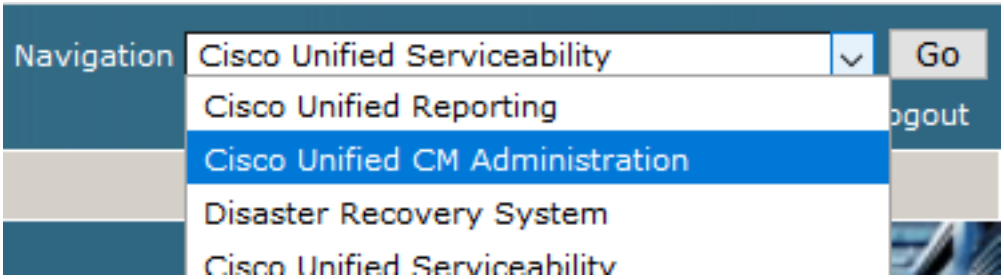
3. Choose the CUCM server and Click Go .



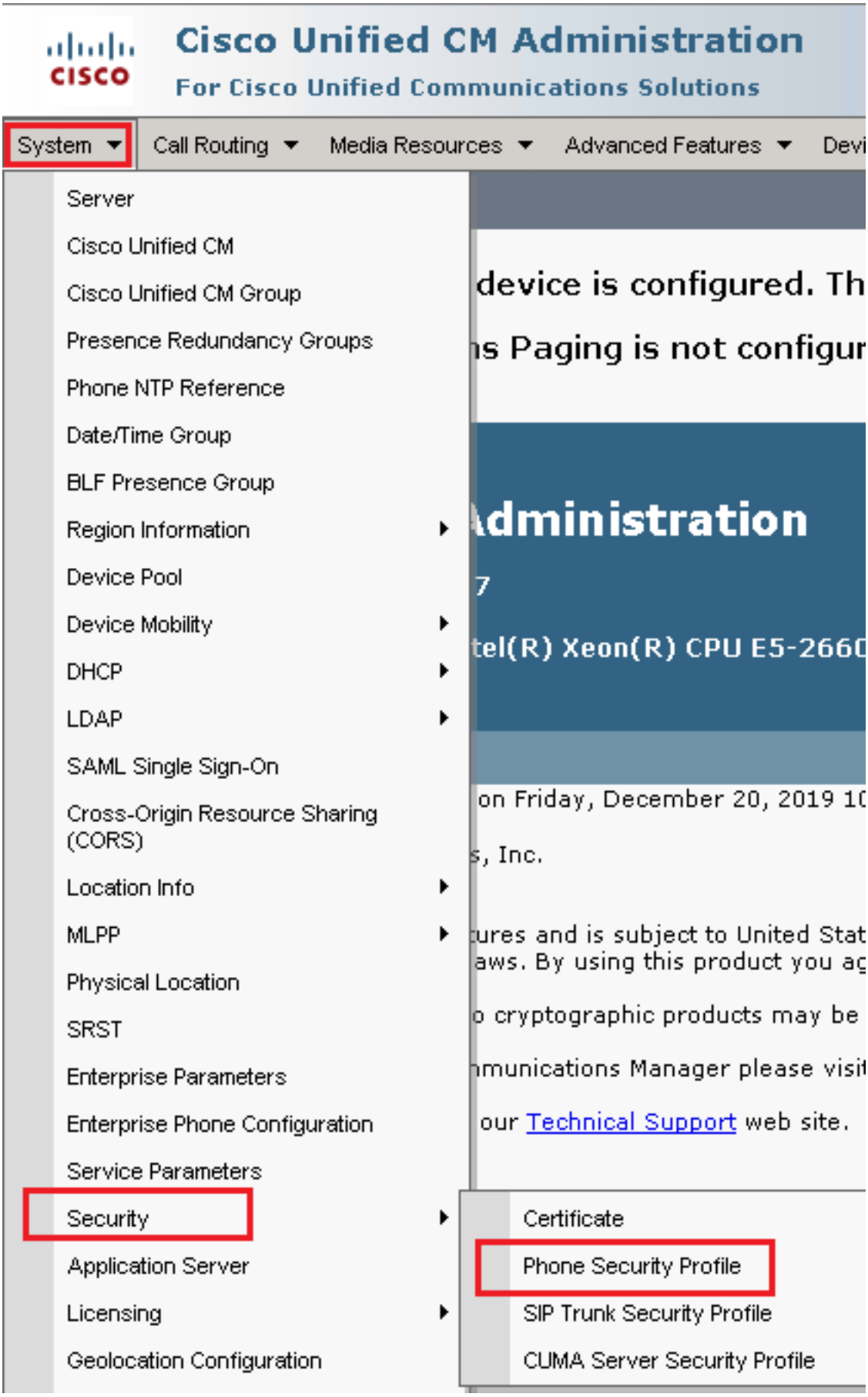
4. Check Cisco Certificate Authority Proxy Function and click Save to activate the service. Click Ok to confirm.



5. Ensure the service is activated then navigate to Cisco Unified CM Administration.

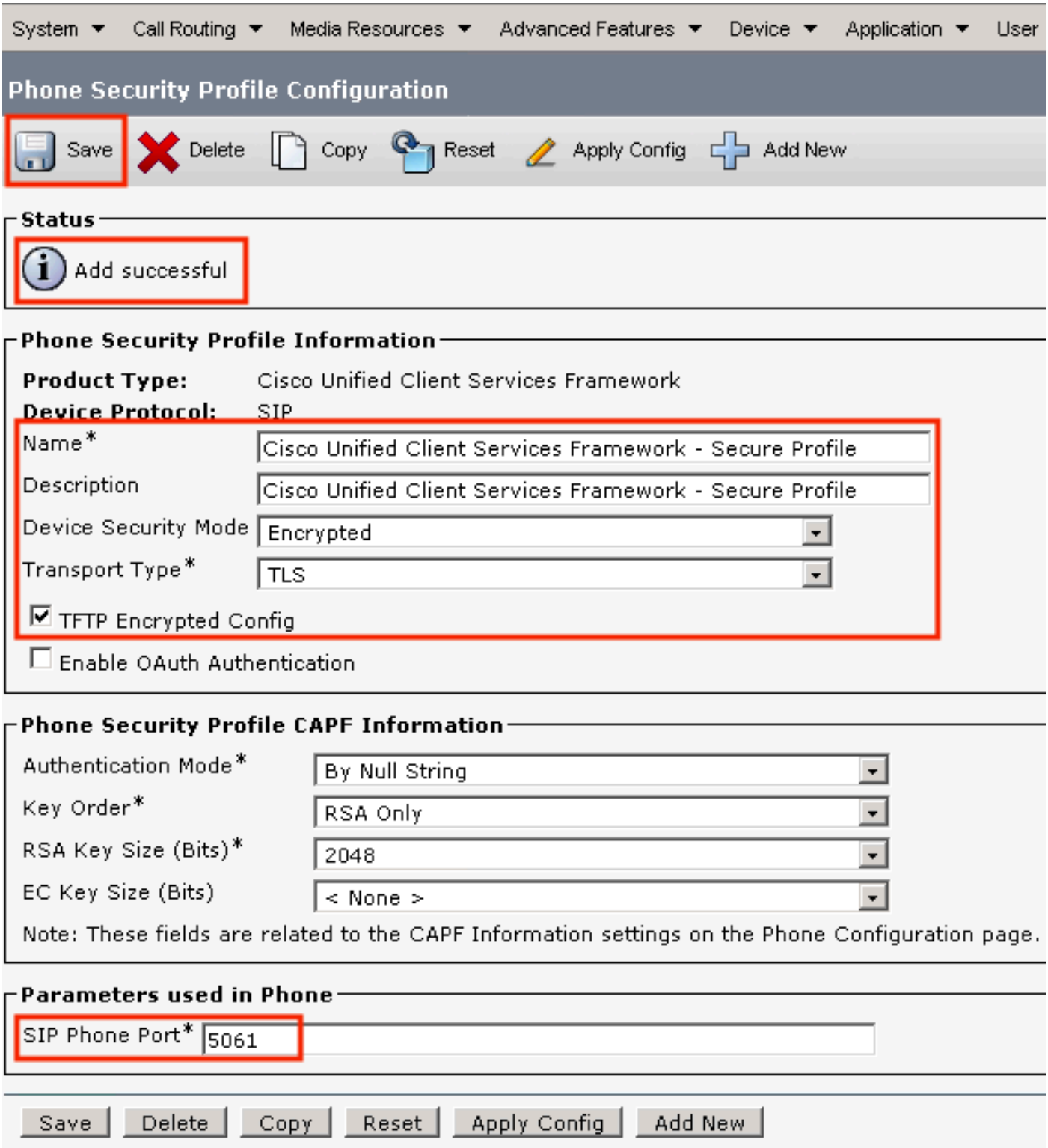


6. After you have successfully logged in to CUCM administration, navigate to System > Security > Phone Security Profile in order to create a device security profile for the agent device.

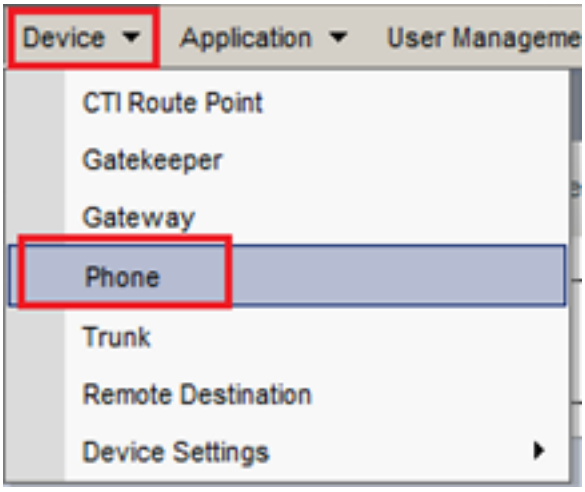


7. Find the security profiles respective to your agent device type. In this example, a soft phone is used, so choose Cisco Unified Client Services Framework - Standard SIP Non-Secure Profile . Click Copy in order to copy this profile.

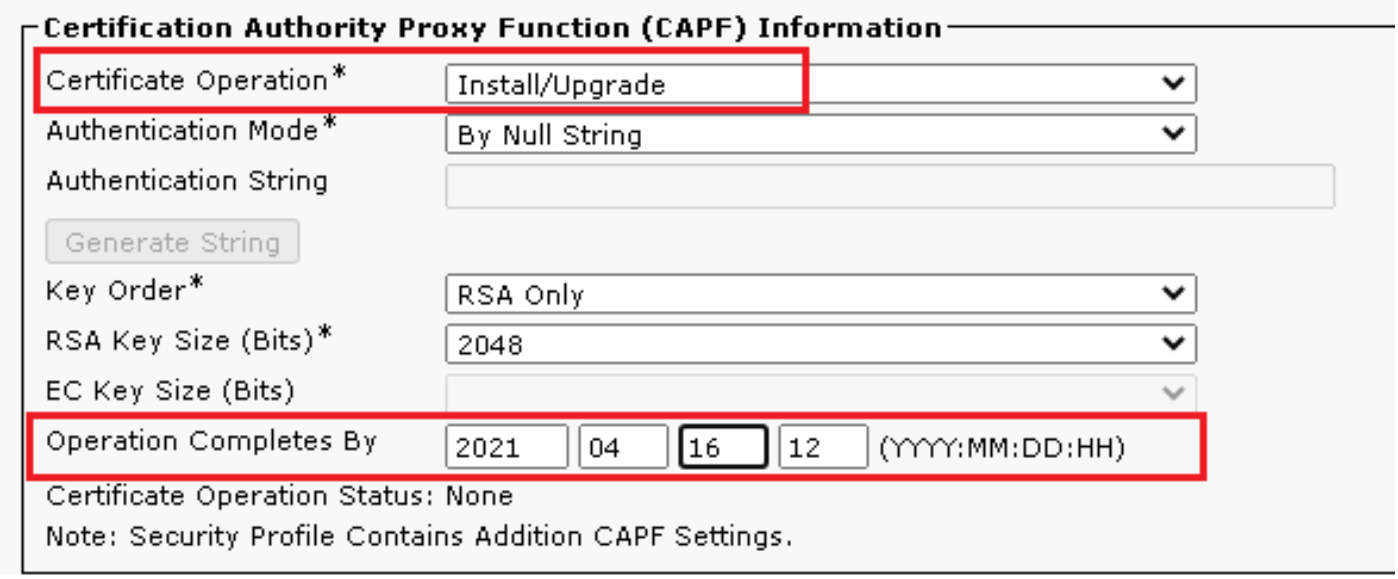
8. Rename the profile to Cisco Unified Client Services Framework - Secure Profile,change the parameters as shown in this image, then click Save at the top left of the page.



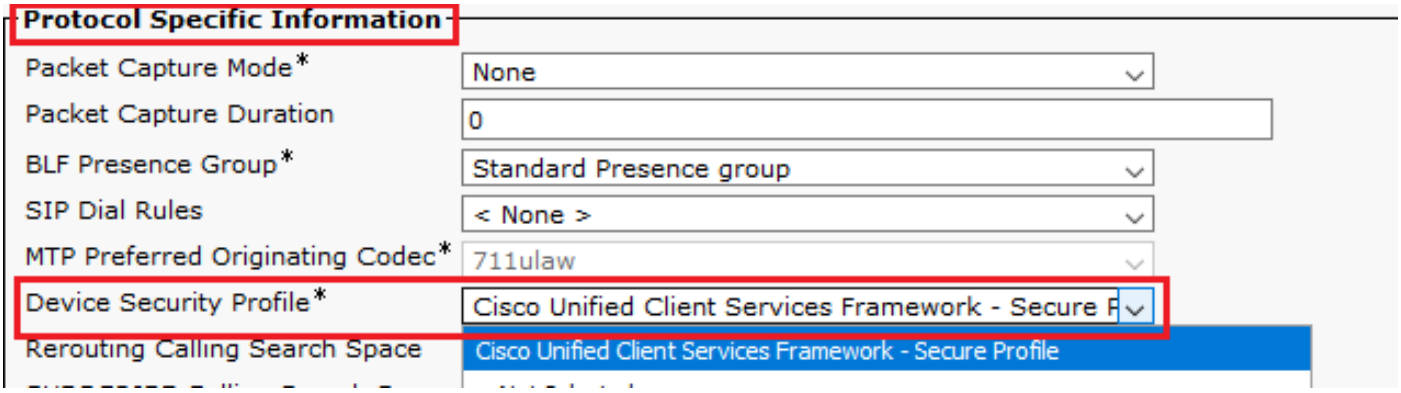
9. After the successful creation of the phone device profile, navigate to Device > Phone.



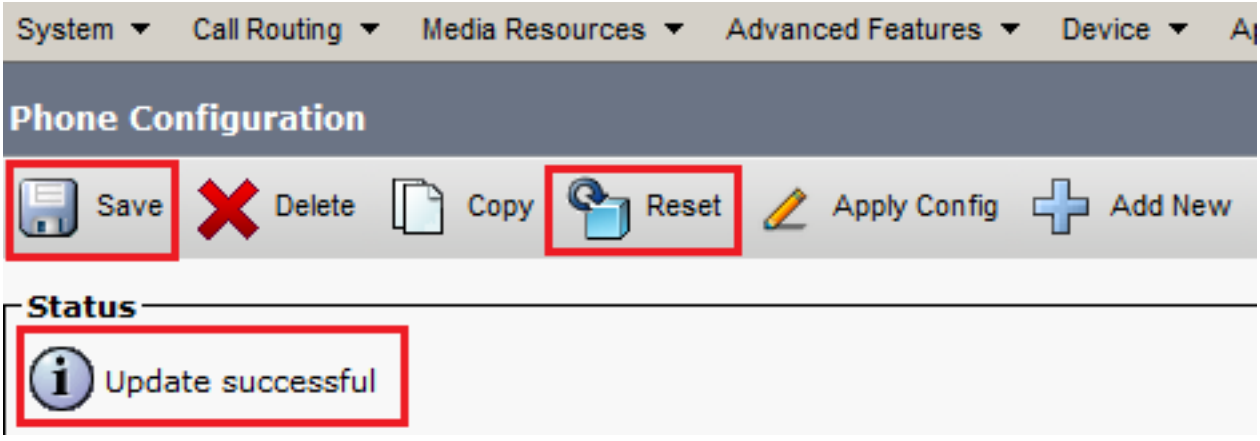
10. Click Find in order to list all available phones, then click agent phone.
11. Agent phone configuration page opens. Find Certification Authority Proxy Function (CAPF) Information section. In order to install LSC, set Certificate Operation to Install/Upgrade and Operation Completes by to any future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



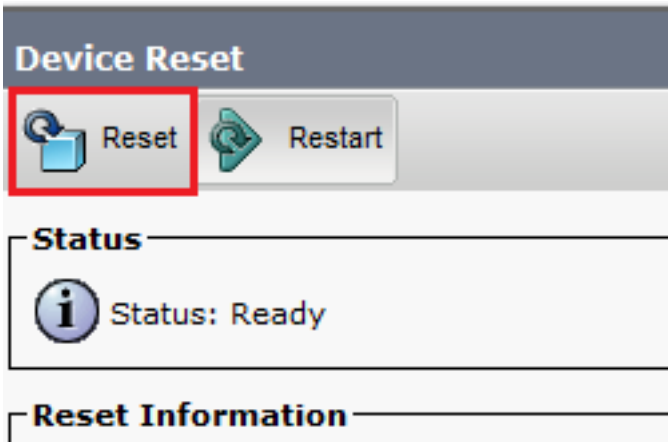
12. Find Protocol Specific Information section. Change Device Security Profile to Cisco Unified Client Services Framework – Secure Profile.



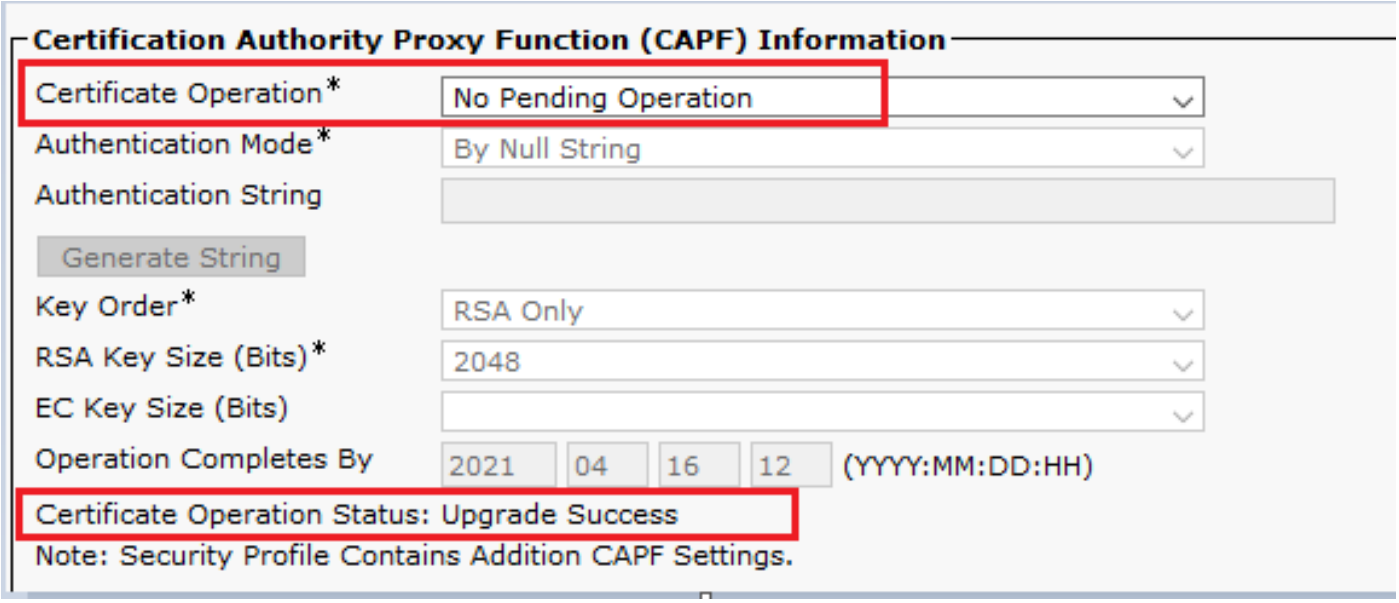
13. Click Save at the top left of the page. Ensure the changes are saved successfully and click Reset.



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



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 .



16. Refer Steps. 7-13 in order to secure other agents devices that you want to use to secure SIP with CUCM.

Verify

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

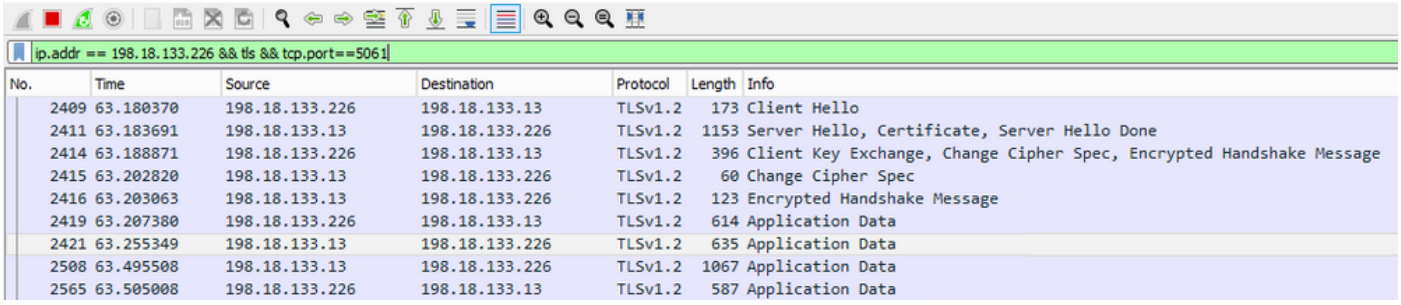
1. Open SSH session to vCUBE, run the command show sip-ua connections tcp tls detail , and confirm that there is no TLS connection established at the moment with CVP (198.18.133.13).

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

---------Printing Detailed Connection Report---------
Note:
 ** Tuples with no matching socket entry
    - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port>'
      to overcome this error condition
 ++ Tuples with mismatched address/port entry
    - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port> id <connid>'
      to overcome this error condition

Remote-Agent:198.18.133.3, Connections-Count:1
  Remote-Port Conn-Id Conn-State  WriteQ-Size Local-Address TLS-Version
  =========== ======= =========== =========== ============= ===========
        44868      49 Established           0             -     TLSv1.2

Remote-Agent:198.18.133.13, Connections-Count:0


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

SIP Options

Note: At this moment, only one active TLS session with CUCM, for SIP Options is enabled on CUCM (198.18.133.3). If no SIP Options are enabled, no SIP TLS connection exists.

2. Log in to CVP and start Wireshark.
3. Make a test call to contact center number.
4. Navigate to the CVP session; on Wireshark, run this filter in order to check SIP signaling with CUBE:
   ip.addr == 198.18.133.226 && tls && tcp.port==5061



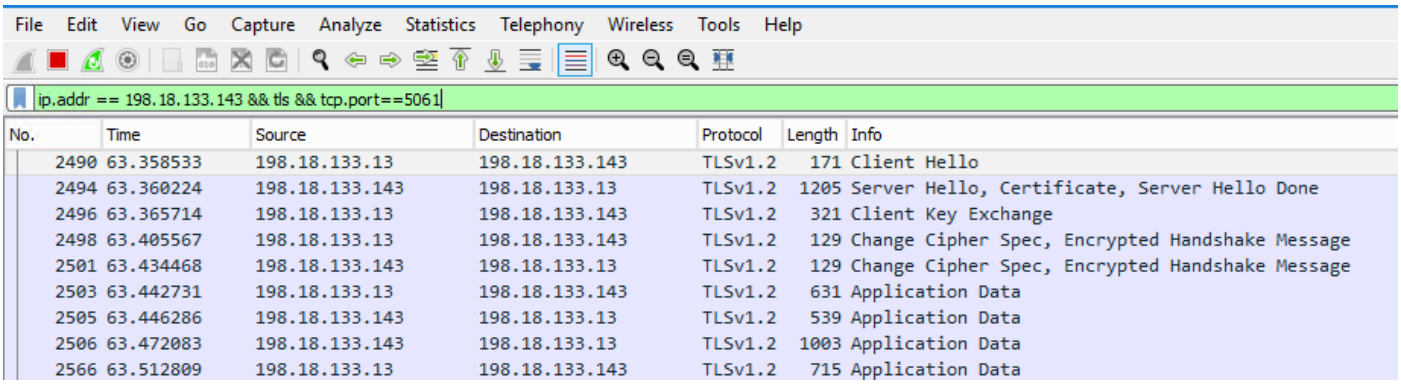
ip.addr == 198.18.133.226 && tls && tcp.port==5061

No.	Time	Source	Destination	Protocol	Length	Info
2409	63.180370	198.18.133.226	198.18.133.13	TLSv1.2	173	Client Hello
2411	63.183691	198.18.133.13	198.18.133.226	TLSv1.2	1153	Server Hello, Certificate, Server Hello Done
2414	63.188871	198.18.133.226	198.18.133.13	TLSv1.2	396	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
2415	63.202820	198.18.133.13	198.18.133.226	TLSv1.2	60	Change Cipher Spec
2416	63.203063	198.18.133.13	198.18.133.226	TLSv1.2	123	Encrypted Handshake Message
2419	63.207380	198.18.133.226	198.18.133.13	TLSv1.2	614	Application Data
2421	63.255349	198.18.133.13	198.18.133.226	TLSv1.2	635	Application Data
2508	63.495508	198.18.133.13	198.18.133.226	TLSv1.2	1067	Application Data
2565	63.505008	198.18.133.226	198.18.133.13	TLSv1.2	587	Application Data

Check: Is SIP over TLS connection established? If yes, the output confirms SIP signals between CVP and CUBE are secured.

5. Check the SIP TLS connection between CVP and CVVB. In the same Wireshark session, run this filter:

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



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
2490	63.358533	198.18.133.13	198.18.133.143	TLSv1.2	171	Client Hello
2494	63.360224	198.18.133.143	198.18.133.13	TLSv1.2	1205	Server Hello, Certificate, Server Hello Done
2496	63.365714	198.18.133.13	198.18.133.143	TLSv1.2	321	Client Key Exchange
2498	63.405567	198.18.133.13	198.18.133.143	TLSv1.2	129	Change Cipher Spec, Encrypted Handshake Message
2501	63.434468	198.18.133.143	198.18.133.13	TLSv1.2	129	Change Cipher Spec, Encrypted Handshake Message
2503	63.442731	198.18.133.13	198.18.133.143	TLSv1.2	631	Application Data
2505	63.446286	198.18.133.143	198.18.133.13	TLSv1.2	539	Application Data
2506	63.472083	198.18.133.143	198.18.133.13	TLSv1.2	1003	Application Data
2566	63.512809	198.18.133.13	198.18.133.143	TLSv1.2	715	Application Data

Check: Is SIP over TLS connection established? If yes, the output confirms SIP signals between CVP and CVVB are secured.

6. You can also verify the SIP TLS connection with CVP from CUBE. Navigate to the vCUBE SSH session, and run this command to check secure sip signals:
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:
```

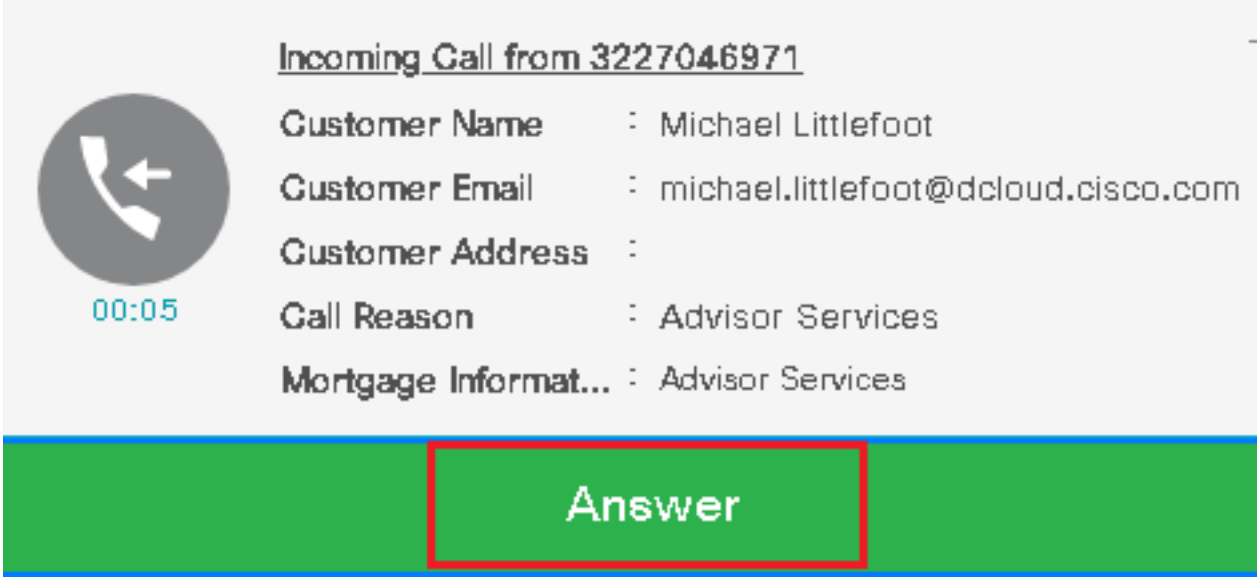
Check: Is SIP over TLS connection established with CVP? If yes, the output confirms SIP signals between CVP and CUBE are secured.

7. At this moment, the call is active and you hear Music on Hold (MOH) as there is no agent available to answer the call.

8. Make the agent available to answer the call.

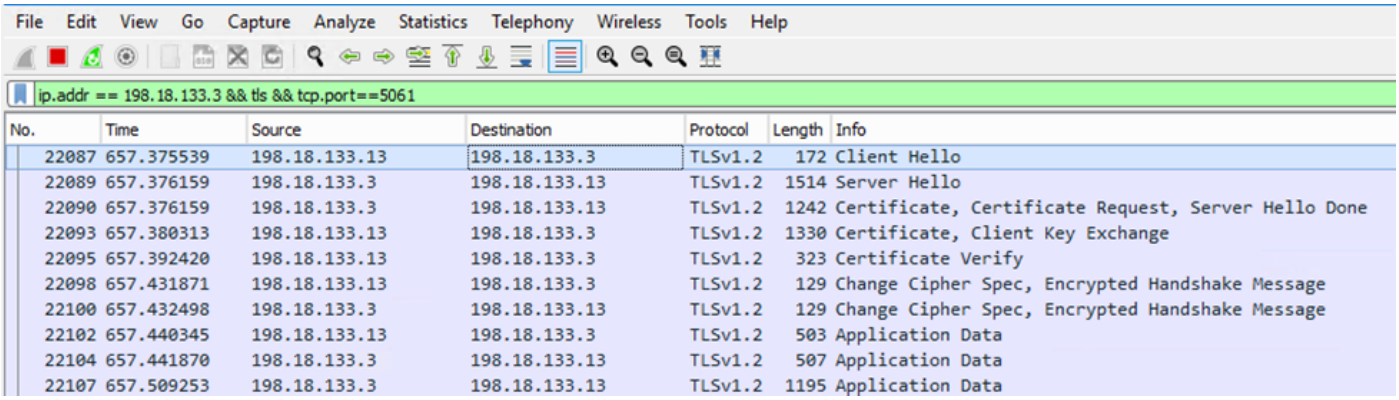
.

9. Agent gets reserved and the call is routed to him/her. Click Answer to answer the call.



10. Call connects to the agent.

11. In order to verify SIP signals between CVP and CUCM, navigate to the CVP session, and run this filter in Wireshark:
ip.addr == 198.18.133.3 && tls && tcp.port==5061



No.	Time	Source	Destination	Protocol	Length	Info
22087	657.375539	198.18.133.13	198.18.133.3	TLSv1.2	172	Client Hello
22089	657.376159	198.18.133.3	198.18.133.13	TLSv1.2	1514	Server Hello
22090	657.376159	198.18.133.3	198.18.133.13	TLSv1.2	1242	Certificate, Certificate Request, Server Hello Done
22093	657.380313	198.18.133.13	198.18.133.3	TLSv1.2	1330	Certificate, Client Key Exchange
22095	657.392420	198.18.133.13	198.18.133.3	TLSv1.2	323	Certificate Verify
22098	657.431871	198.18.133.13	198.18.133.3	TLSv1.2	129	Change Cipher Spec, Encrypted Handshake Message
22100	657.432498	198.18.133.3	198.18.133.13	TLSv1.2	129	Change Cipher Spec, Encrypted Handshake Message
22102	657.440345	198.18.133.13	198.18.133.3	TLSv1.2	503	Application Data
22104	657.441870	198.18.133.3	198.18.133.13	TLSv1.2	507	Application Data
22107	657.509253	198.18.133.3	198.18.133.13	TLSv1.2	1195	Application Data

Check: Are all SIP communications with CUCM (198.18.133.3) over TLS? If yes, the output confirms SIP signals between CVP and CUCM are secured.

Troubleshoot

If TLS is not established, run these commands on CUBE to enable debug TLS to troubleshoot:

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