Configure and Troubleshoot Secure Integration Between CUCM and CUC

Contents

Introduction

This document describes the configuration, verification and troubleshoot of the secure connection between the Cisco Unified Communication Manager (CUCM) and Cisco Unity Connection (CUC) server.

Prerequisites

Requirements

Cisco recommends that you have knowledge of CUCM.

Refer to Cisco Unified Communications Manager Security Guide for more details.

> **Note**: It must be set to mixed mode in order to make secure integration working correctly.

Encryption must be enabled for Unity Connection 11.5(1) SU3 and later.

CLI command "utils cuc encryption <enable/disable>"

Components Used

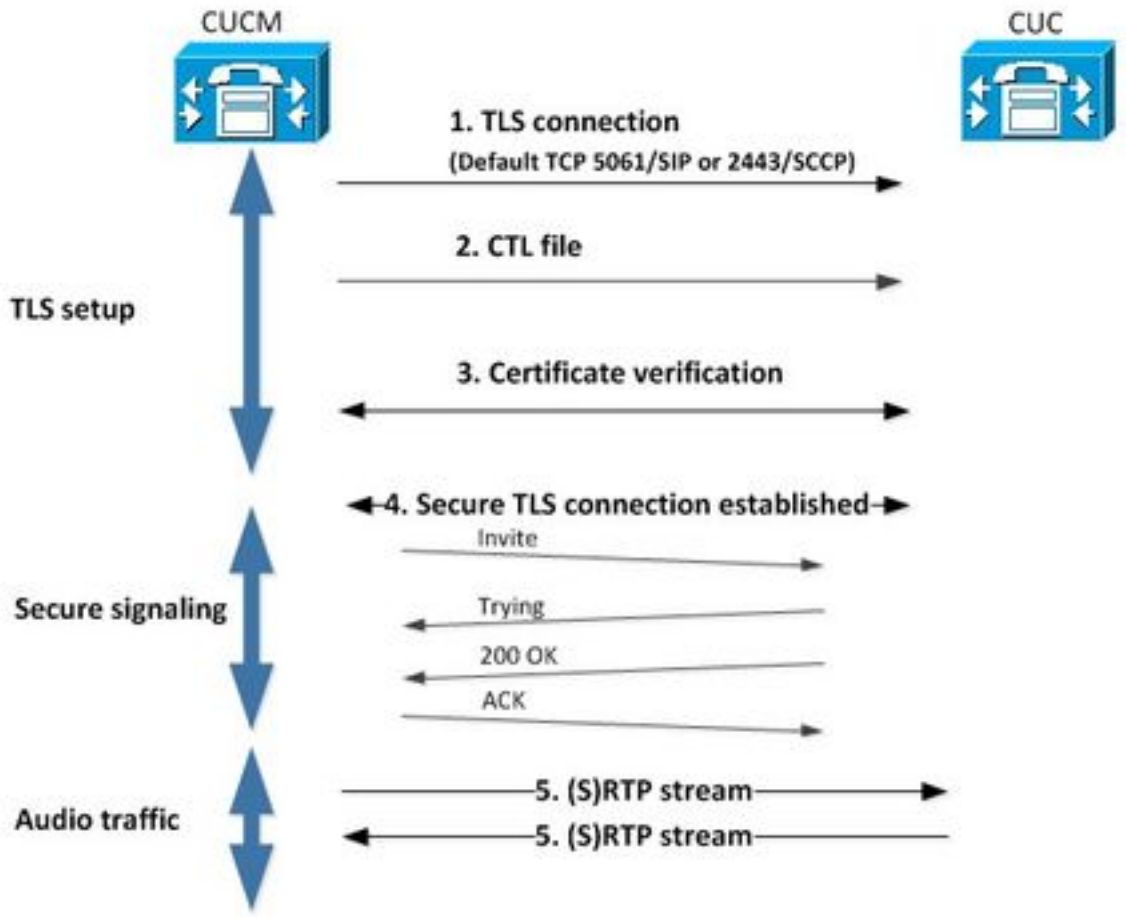
The information in this document is based on these software and hardware versions:

- CUCM version 10.5.2.11900-3.
- CUC version 10.5.2.11900-3.

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, make sure that you understand the potential impact of any command.

Diagram

This diagram briefly explains the process that helps establish a secure connection between CUCM and CUC:



1. Call Manager sets up a secure Transport Layer Security (TLS) connection to CUC server either on port 2443 Skinny Call Control Protocol (SCCP) or 5061 Session Initiation Protocol based (SIP) on the protocol used for integration.

2. CUC server downloads the Certificate Trust List (CTL) file from TFTP server (one time process), extracts the CallManager.pem certificate and stores it.

3. CUCM server offers the Callmanager.pem certificate which is verified against the CallManager.pem certificate obtained in the previous step. In addition, CUC certificate is being verified against a CUC root certificate stored in CUCM. Note that the root certificate must be uploaded into CUCM by the administrator.

4. If verification of the certificates is successfull, secure TLS connection is established. This connection is used to exchange encrypted SCCP or SIP signaling.

5. Audio traffic can be exchanged either as Real-time Transport Protocol (RTP) or SRTP.

> **Note**: When you establish a TLS communication, CUCM and CUC use TLS mutual authentication. Refer to RFC5630 for more information.

Configure - Secure SIP Trunk

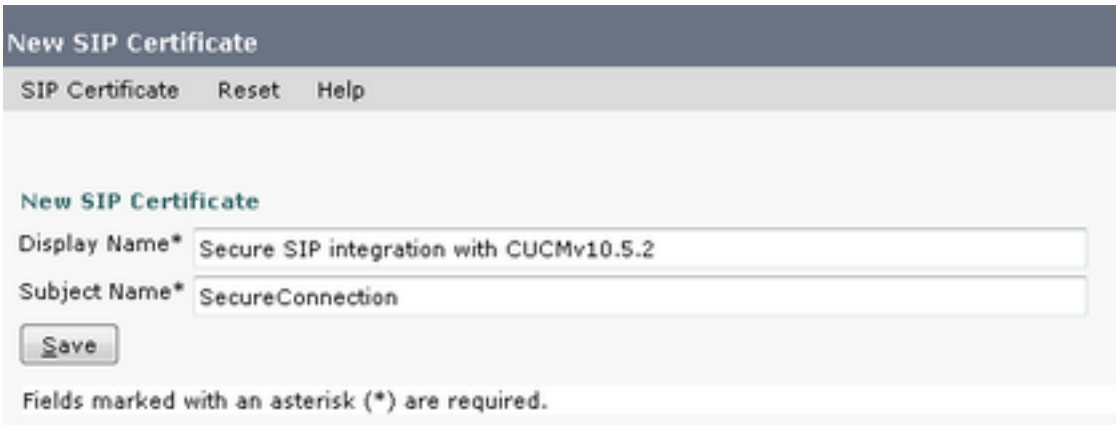
Configure CUC

1. Add SIP certificate

Navigate to **CUC Administration > Telephony Integrations > Security > SIP Certificate > Add new**

- Display Name: <any meaningful name>
- Subject Name: <any name for example, **SecureConnection**>

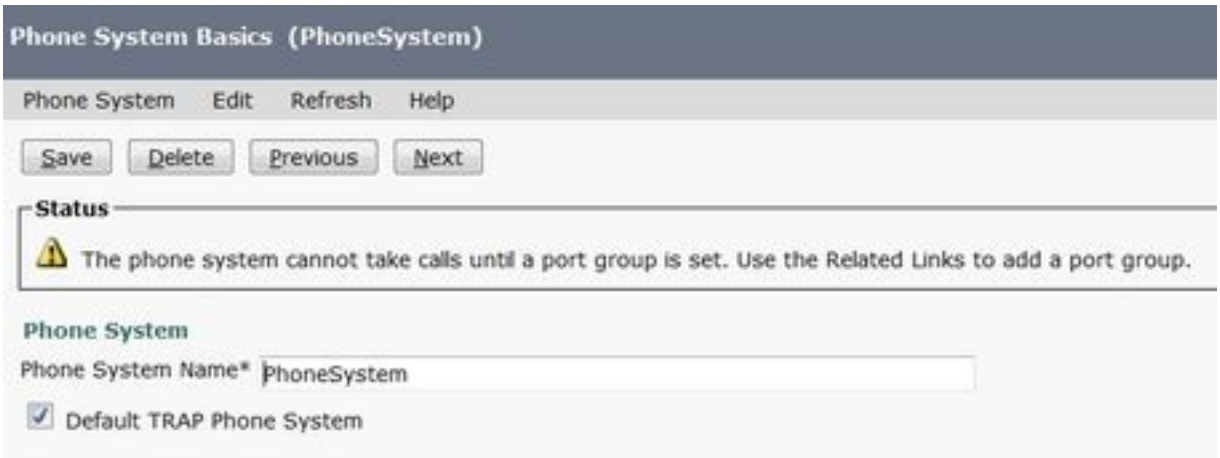
  Note: Subject Name must match the X.509 Subject Name in SIP trunk security profile (configured in step 1 of CUCM configuration later in this document).



  Note: The certificate is generated and signed by the CUC root certificate.

2. Create New Phone System or Modify Default One

Navigate to **Telephony Integration > Phone System**. You can use the phone system that already exists or create a new one.



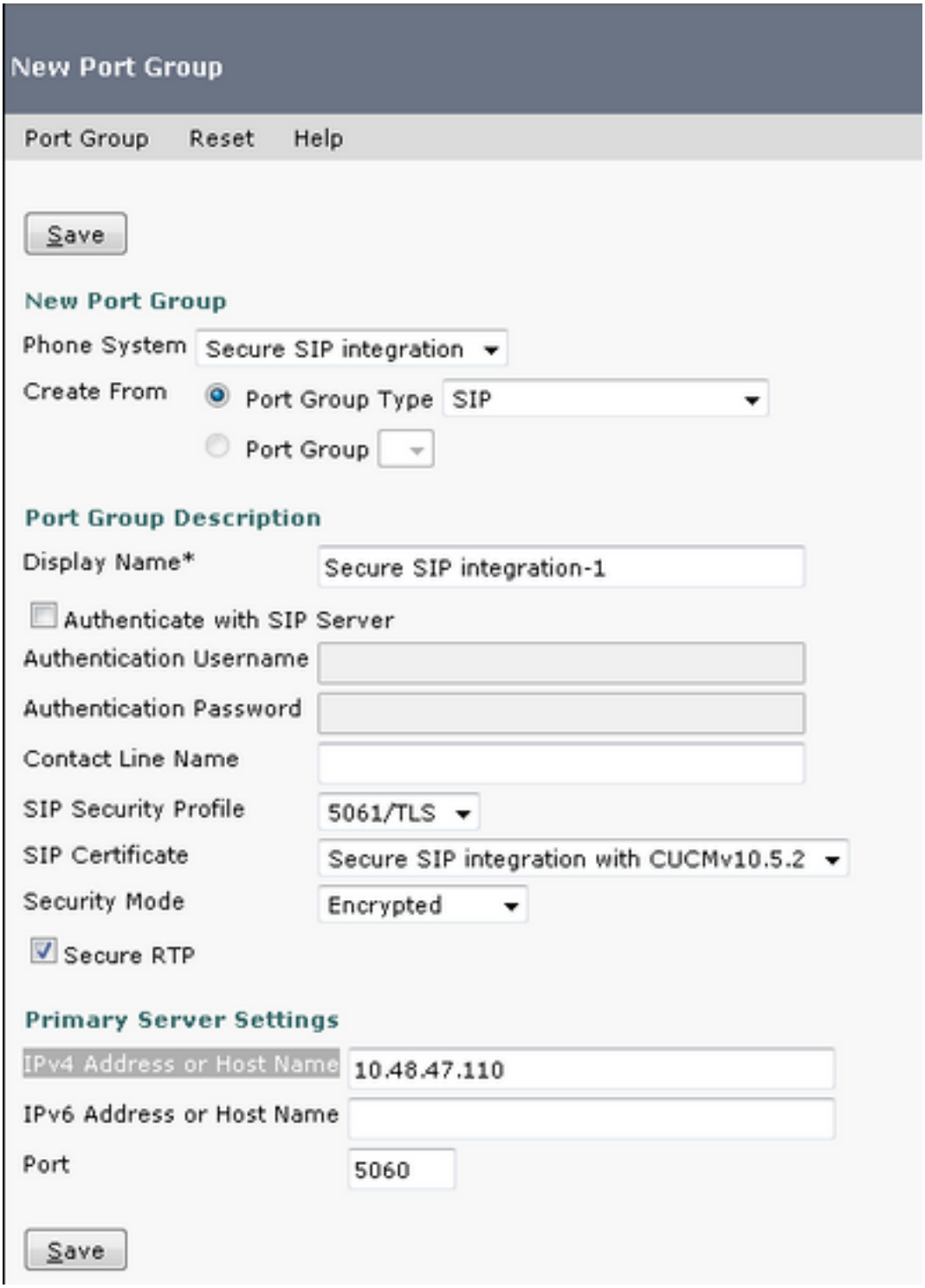
3. Add a New Port Group

On the Phone System Basics page, in the Related Links drop-down box, select Add Port Groupand select Go. In the configuration window, enter this information:

- Phone System:
- Create From: Port Group Type SIP
- SIP Security Profile: 5061/TLS
- SIP Certificate:

- Security Mode: Encrypted
- Secure RTP: Checked
- IPv4 Address or Host Name:

Hit Save.



4. Edit Servers

Navigate to **Edit > Servers** and add TFTP server from the CUCM cluster as shown in this image.

Note: It's important to provide correct TFTP address. CUC server downloads the CTL file from this TFTP as explained.

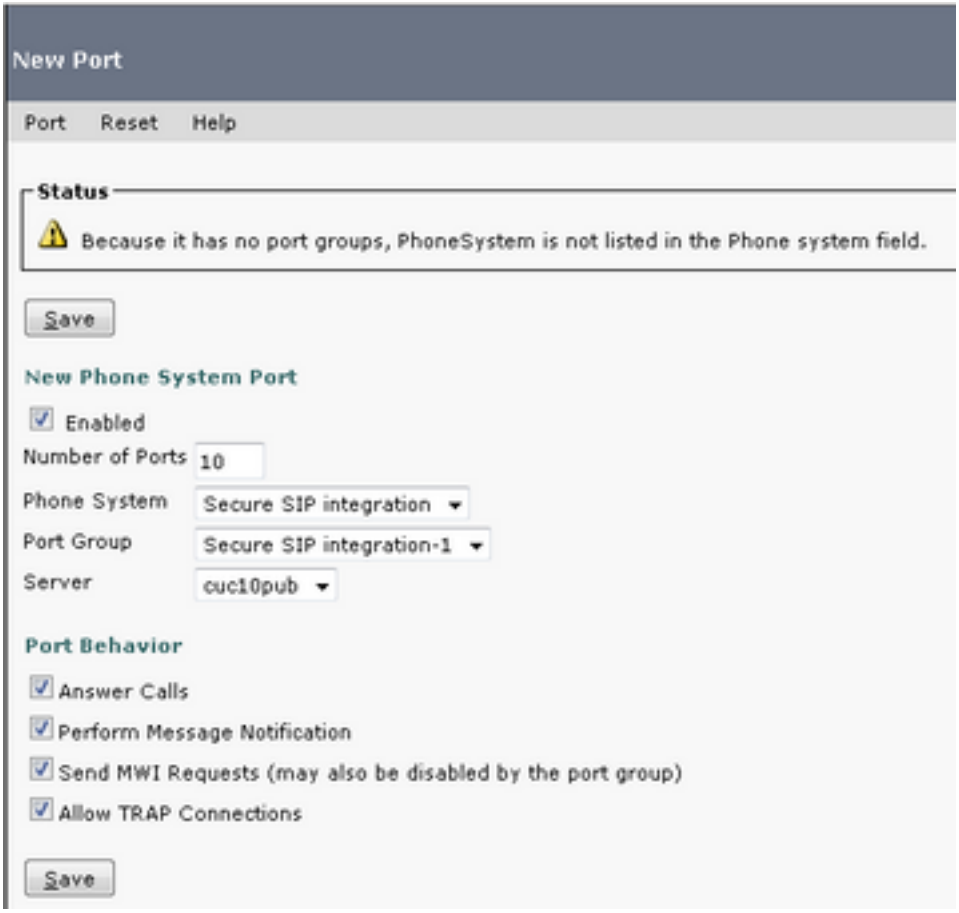
5. Reset the Port Group

Go back to **Port Group Basics** and reset port group as prompted by the system as shown in this image.

6. Add Voice Mail Ports

On the Port Group Basics page, in the Related Links drop-down box, select **Add Ports** and select **Go**. In the configuration window, enter this information:

- Enabled: Checked
- Number of Ports:
- Phone System:
- Port Group:
- Server:
- Port behavior:



7. Download CUC Root Certificate

Navigate to **Telephony Integrations > Security > Root Certificate**, right click on the URL to save the certificate as a file named <filename>.0 (the file extension must be .0 rather than .htm)' and hit save as shown in this image.

Configure CUCM

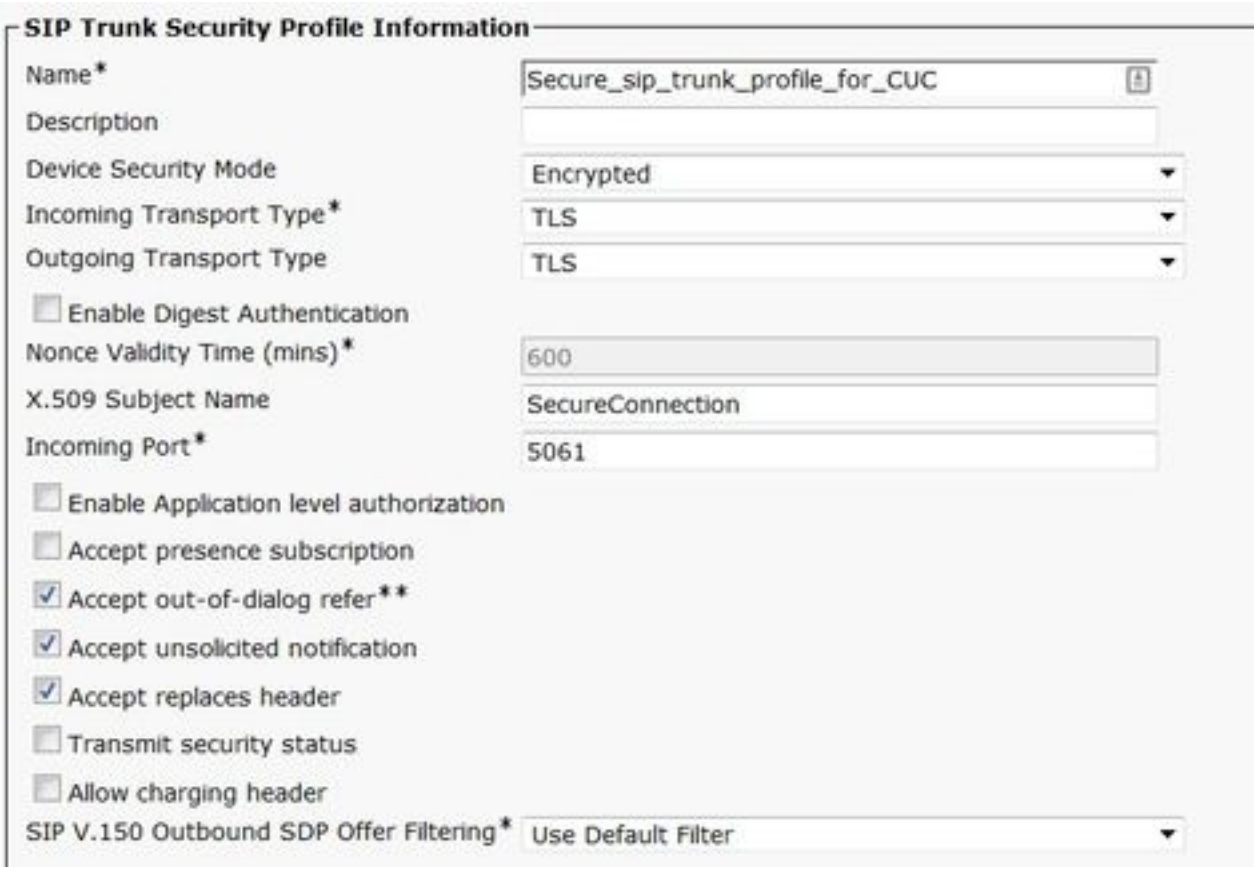
1. Configure SIP Trunk Security Profile for Trunk towards CUC

Navigate to **CUCM Administration > System > Security > SIP Trunk Security Profile > Add new**

Ensure that these fields are properly filled in:

- Device Security Mode: Encrypted
- X.509 Subject Name: SecureConnection>
- Accept out-of-dialog refer: checked
- Accept unsolicited notification: checked
- Accept replaces header: checked

Note: X.509 Subject Name must match the Subject Name field in the SIP certificate on the Cisco Unity Connection server (configured in step 1 of CUC configuration).



2. Configure SIP Profile

Navigate to **Device > Device Settings > SIP Profile** if you need to apply any specific settings. Otherwise, you can use Standard SIP Profile.

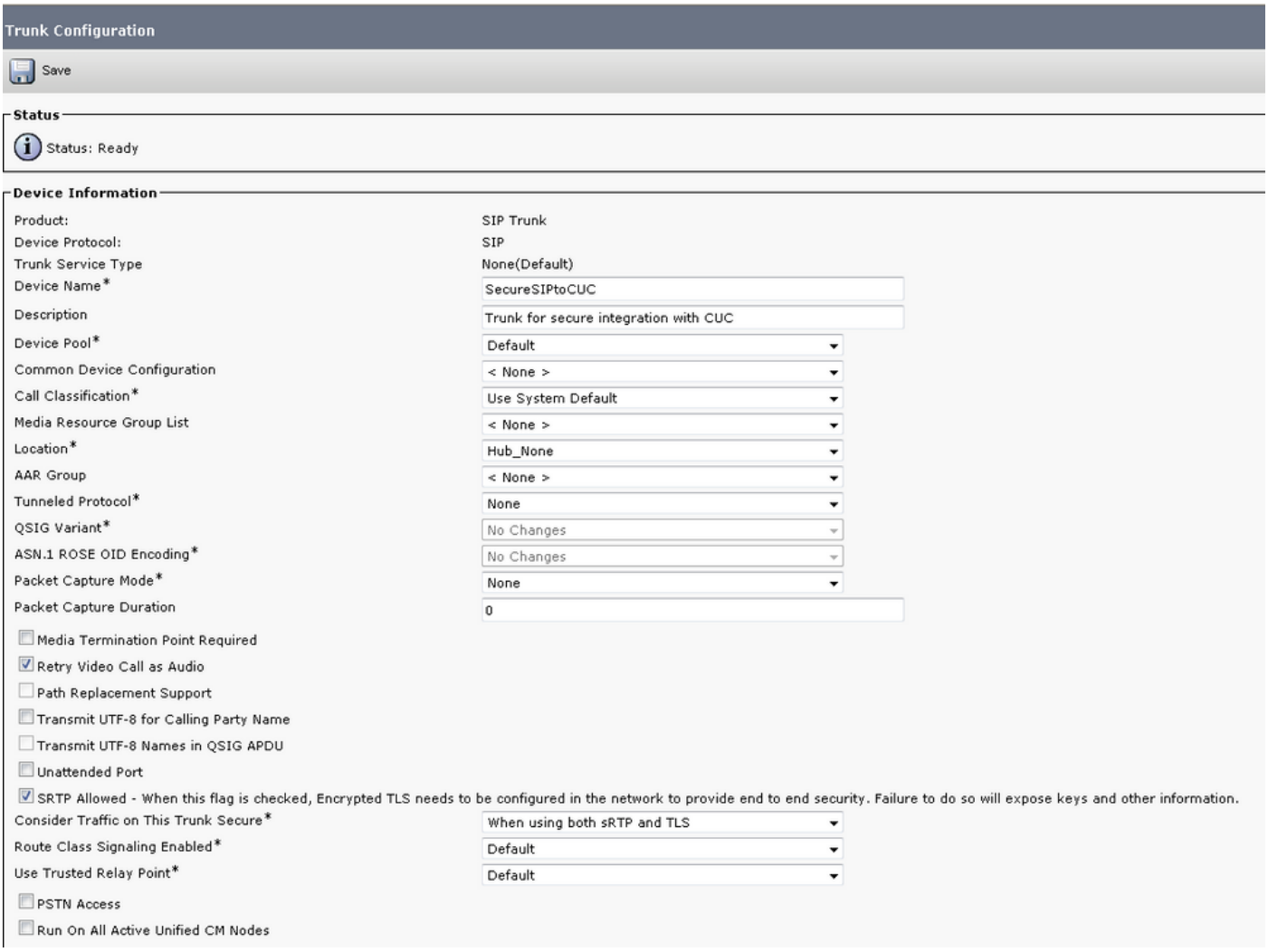
3. Create SIP trunk

Go to **Device > Trunk > Add new**.Create a SIP trunk which will be used for secure integration with Unity Connection as shown in this image.

In the Device Information section of trunk configuration, enter this information:

- Device name:
- Device pool:
- SRTP allowed: Checked

Note: Ensure that the CallManager group (in Device pool configuration) contains all servers configured in CUC (**Port group > Edit > Servers**).

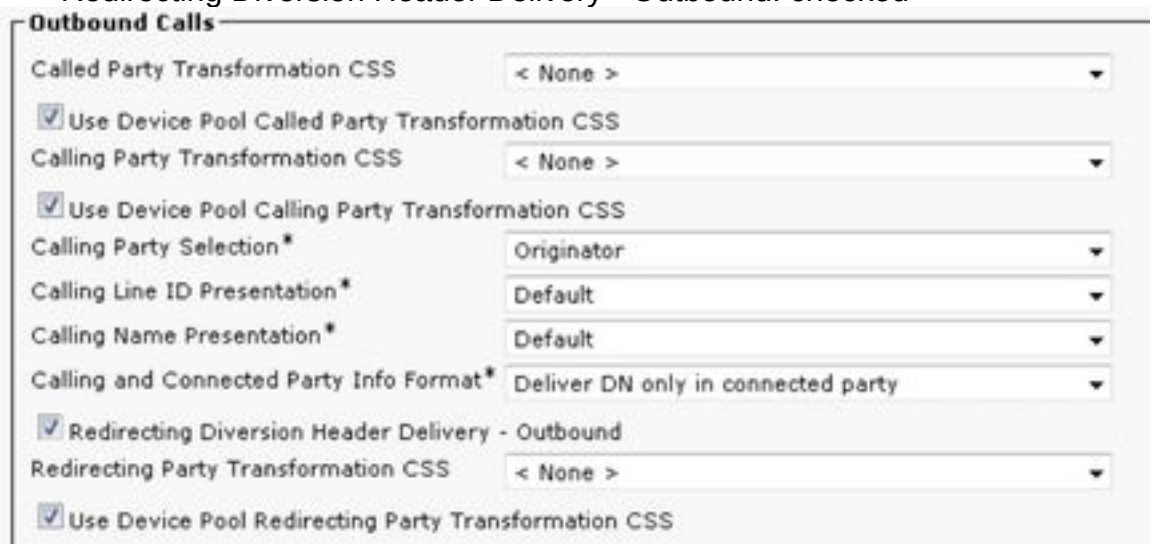


In the Inbound Calls section of trunk configuration, enter this information:

- Calling Search Space:
- Redirecting Diversion Header Delivery - Inbound: Checked

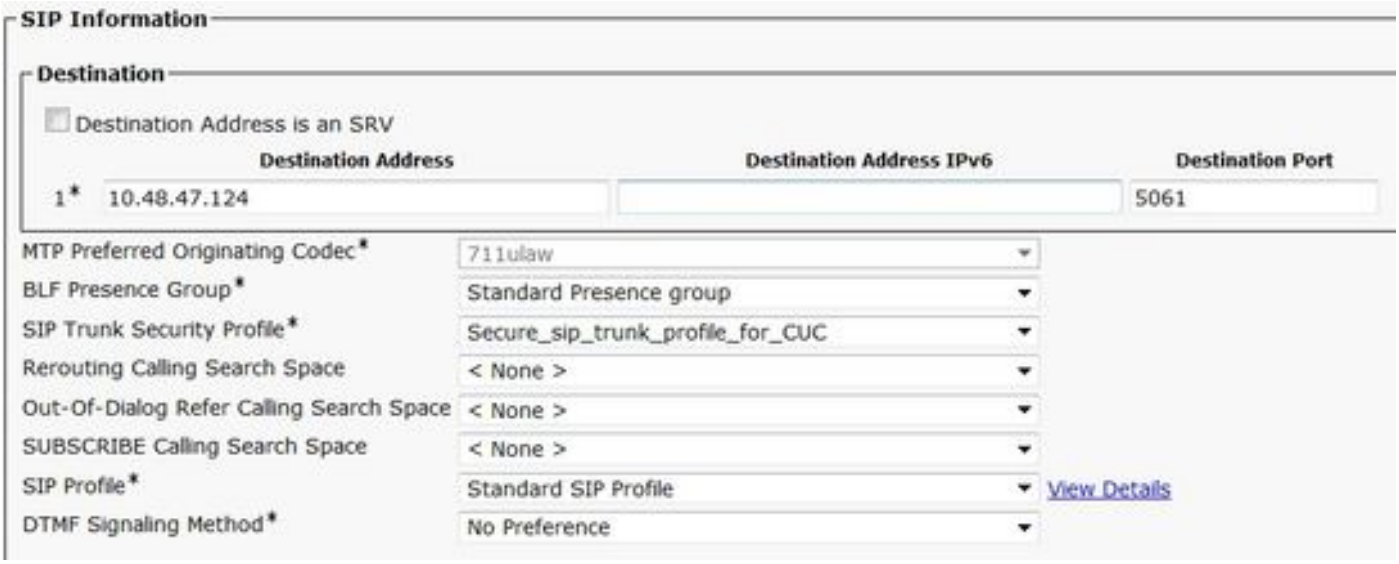
In the Oubound Calls section of trunk configuration, enter this information:

- Redirecting Diversion Header Delivery - Outbound: checked



In the SIP Information section of trunk configuration, enter this information:

- Destination Address:
- SIP Trunk Security Profile:
- Rerouting Calling Search Space:
- Out-of-Dialog Refer Calling Search Space:
- SIP Profile:

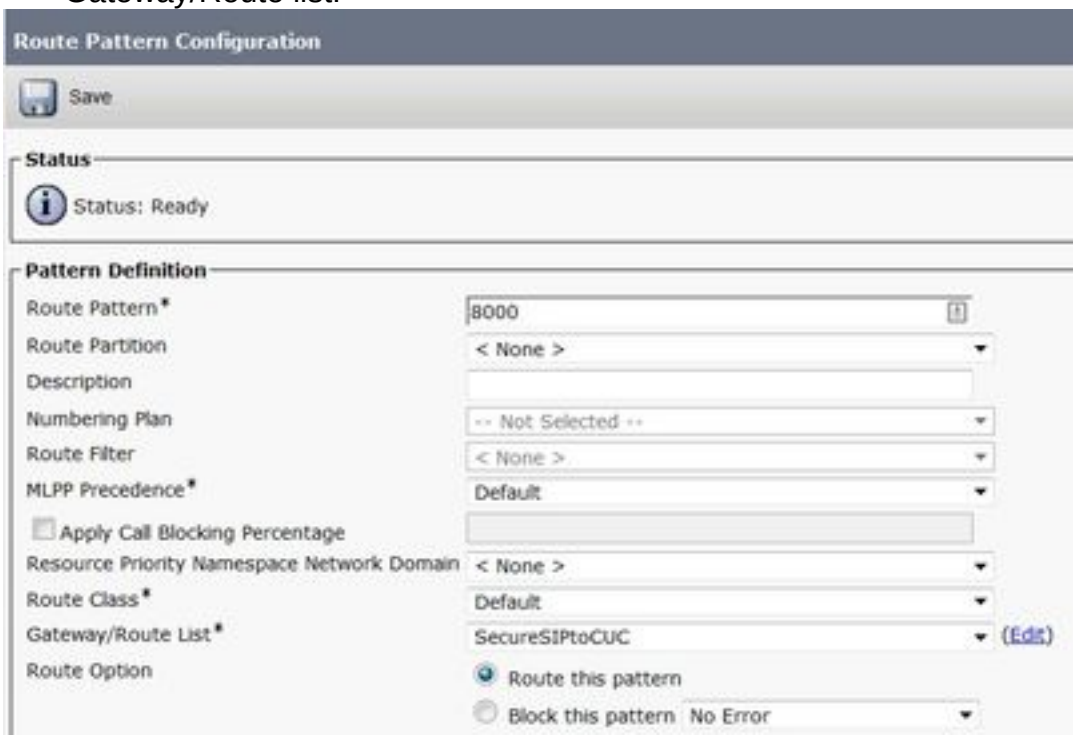


Adjust other settings according to your requirements.

4. Create a Route Pattern

Create a route pattern that points to the configured trunk (**Call Routing > Route/Hunt > Route Pattern**). Extension entered as a route pattern number can be used as a voicemail pilot. Enter this information:

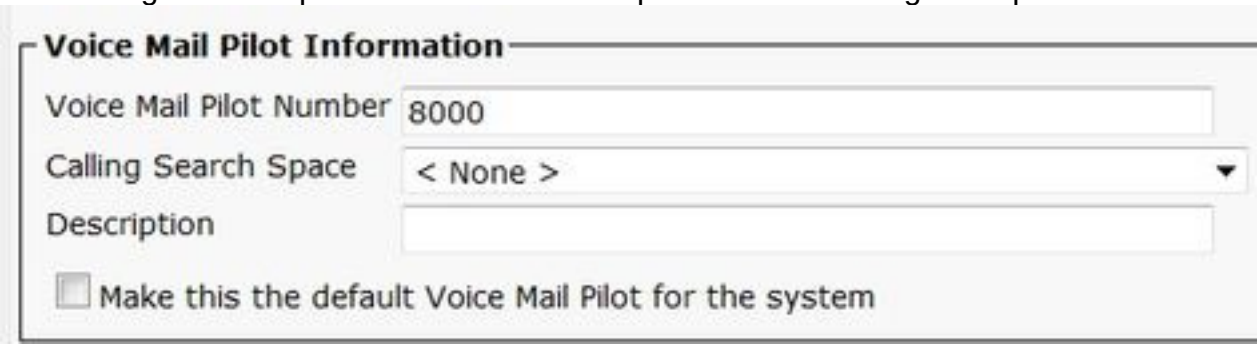
- Route pattern:
- Gateway/Route list:



5. Create a Voice Mail Pilot

Create a voice mail pilot for the integration (**Advanced Features > Voice Mail > Voice Mail Pilot**). Enter these values:

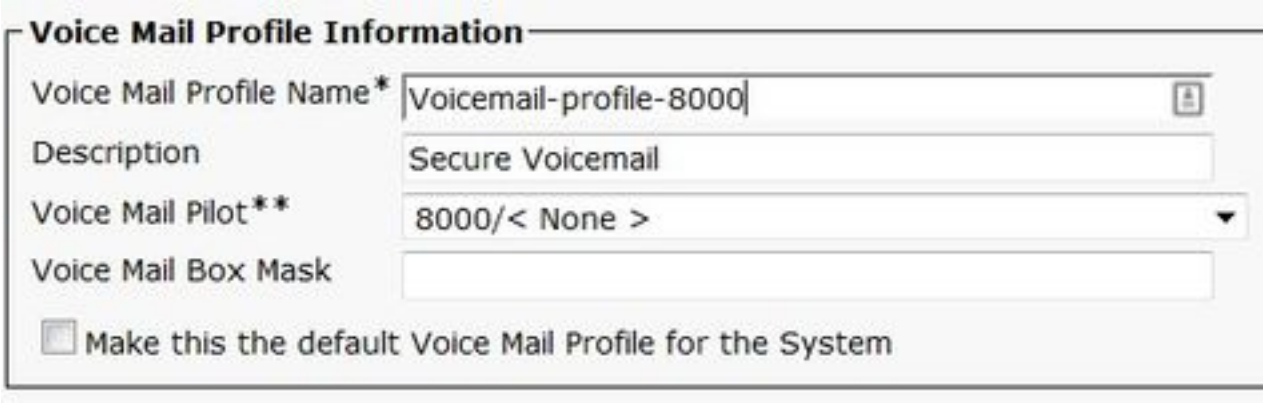
- Voice Mail Pilot Number:
- Calling Search Space: that includes partitions containing route pattern used as a pilot>



6. Create Voice Mail Profile

Create a voice mail profile in order to link all the settings together (**Advanced Features > Voice Mail > Voice Mail Profile). Enter the following information:**

- Voice Mail Pilot:
- Voice Mail Box Mask:

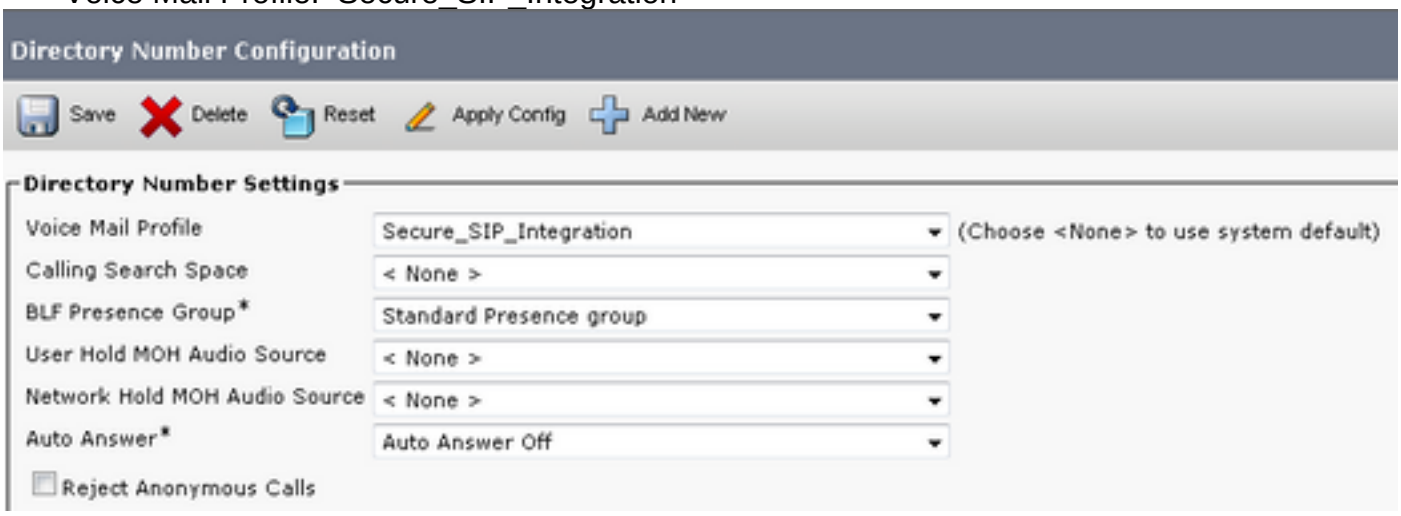


7. Assign Voice Mail Profile to the DNs

Assign the voicemail profile to the DNs intended to use a secure integration. Do not forget to click 'Apply Config' button after changing DN settings:

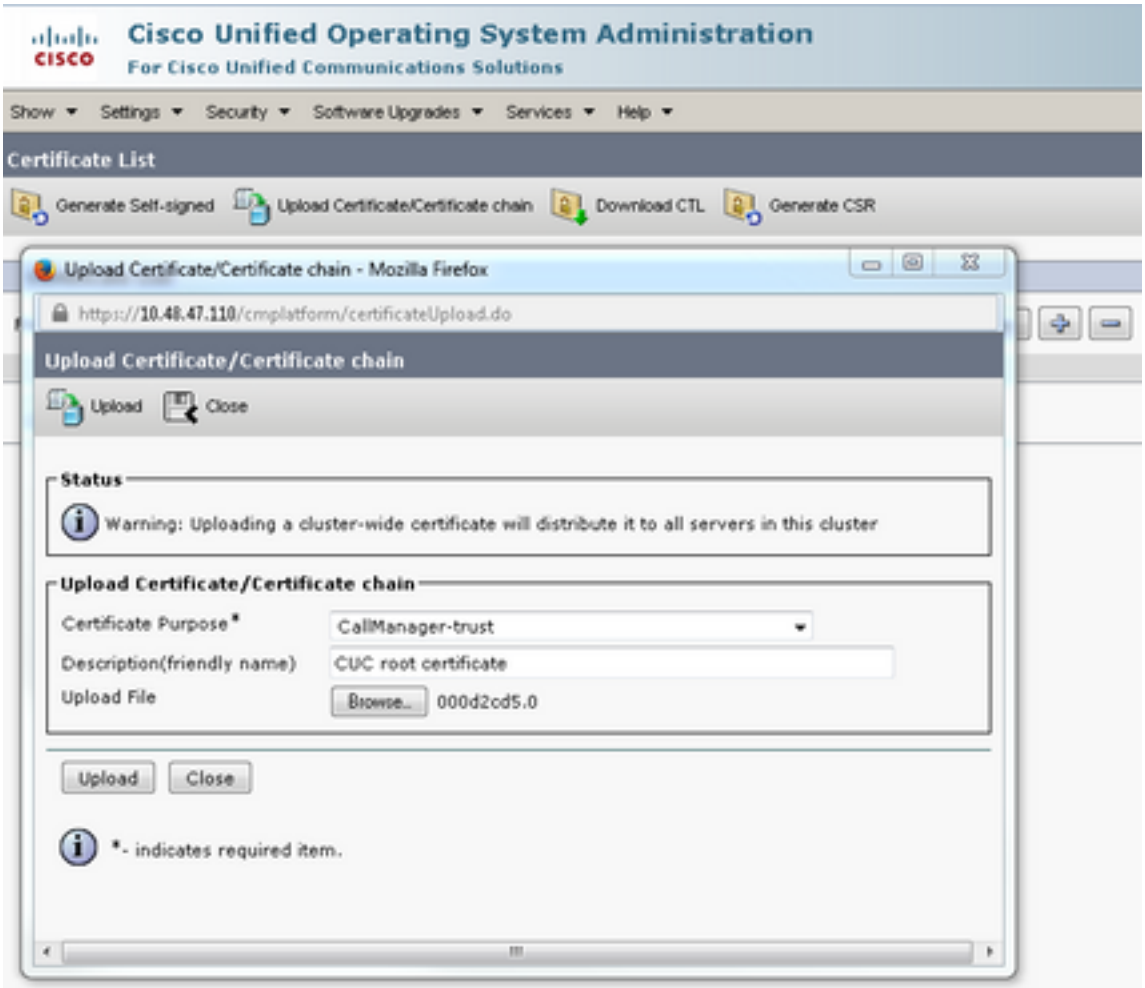
Navigate to: **Call Routing > Directory number** and change the following:

- Voice Mail Profile: Secure_SIP_Integration



8. Upload CUC Root Certificate as CallManager-trust

Navigate to **OS Administration > Security > Certificate Management > Upload Certificate/Certificate Chain** and upload the CUC root certificate as **CallManager-trust** on all nodes configured to communicate with CUC server.



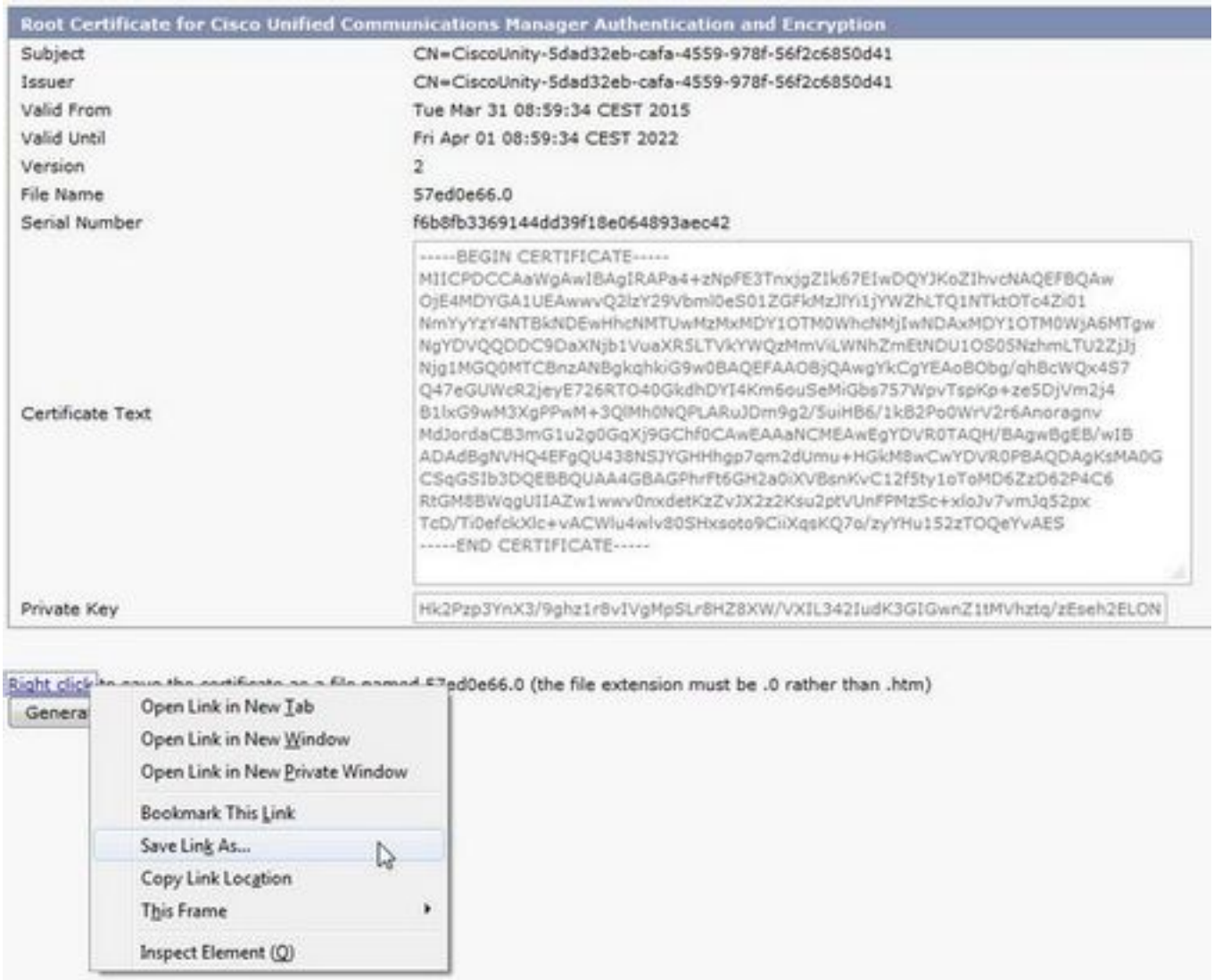
Note: Cisco CallManager service needs to be restarted after the certificate is uploaded in order for the certificate to take effect.

Configure Secure SCCP Ports

Configure CUC

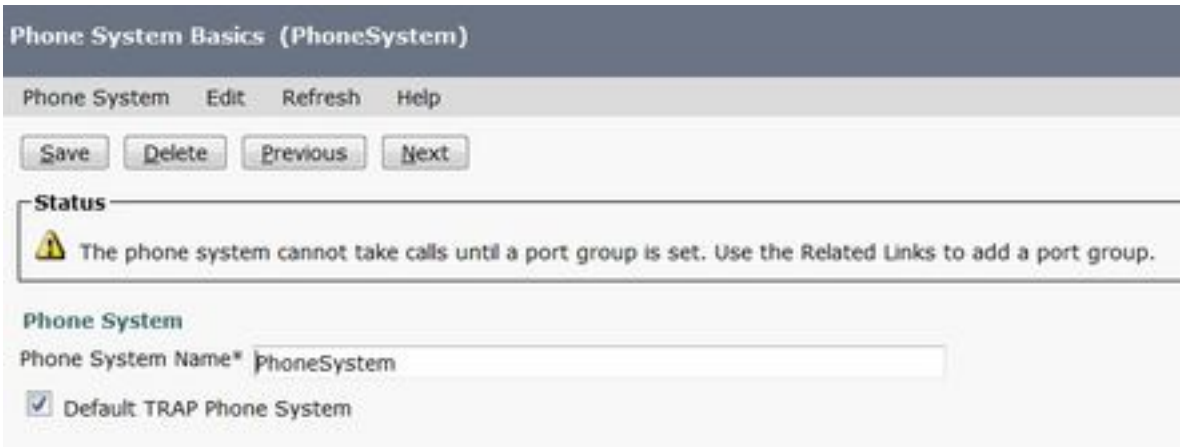
1. Download the CUC Root Certificate

Navigate to **CUC Administration > Telephony Integration > Security > Root Certificate.** Right click on the URL to save the certificate as a file named <filename>.0 (the file extension must be .0 rather than .htm)' and hit S**ave**:



2. Create Phone System / Modify the One that Exists.

Navigate to **Telephony Integration > Phone** system. You can use the phone system that already exists or create a new one.

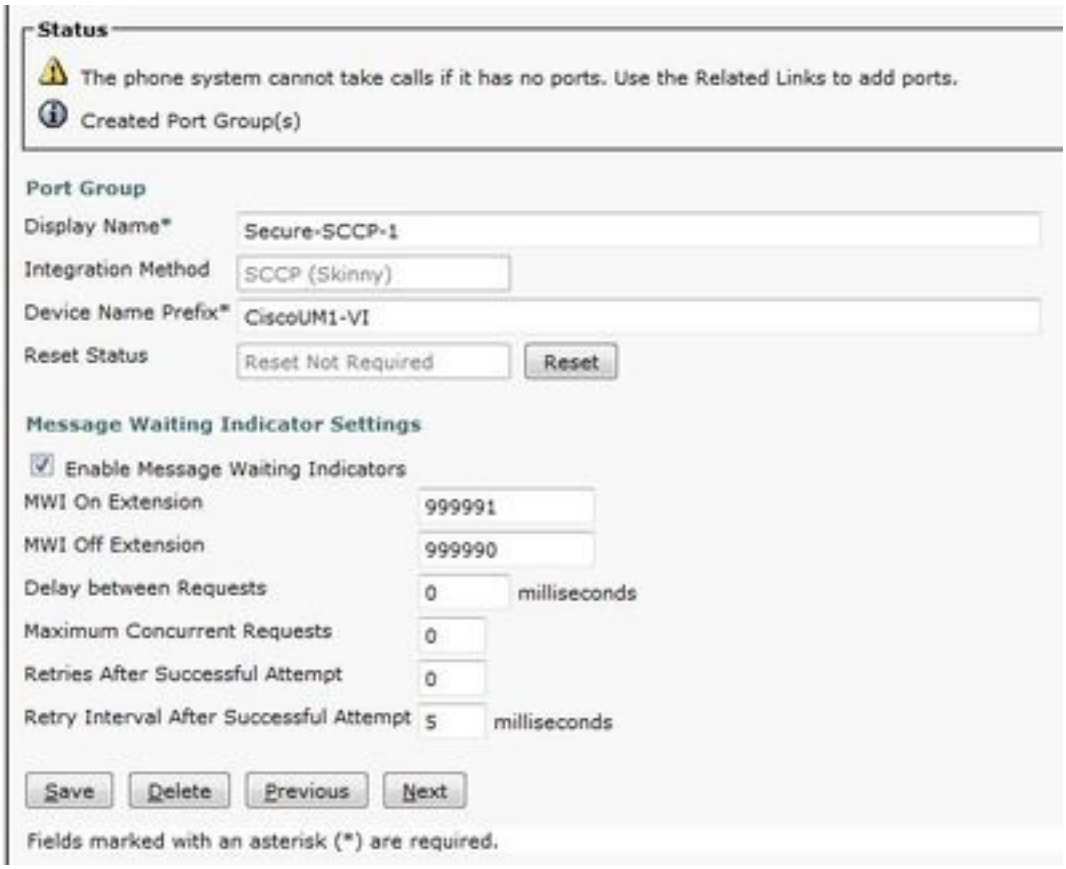


3. Add a New SCCP Port Group

On the Phone System Basics page, in the Related Links drop-down box, select **Add Port Group** and select **Go**. In the configuration window, enter this information:

- Phone system:
- Port group type: SCCP
- Device Name prefix*: CiscoUM1-VI
- MWI On extension:
- MWI Off extension:

Note: This configuration must match the configuration on CUCM.



4. Edit Servers

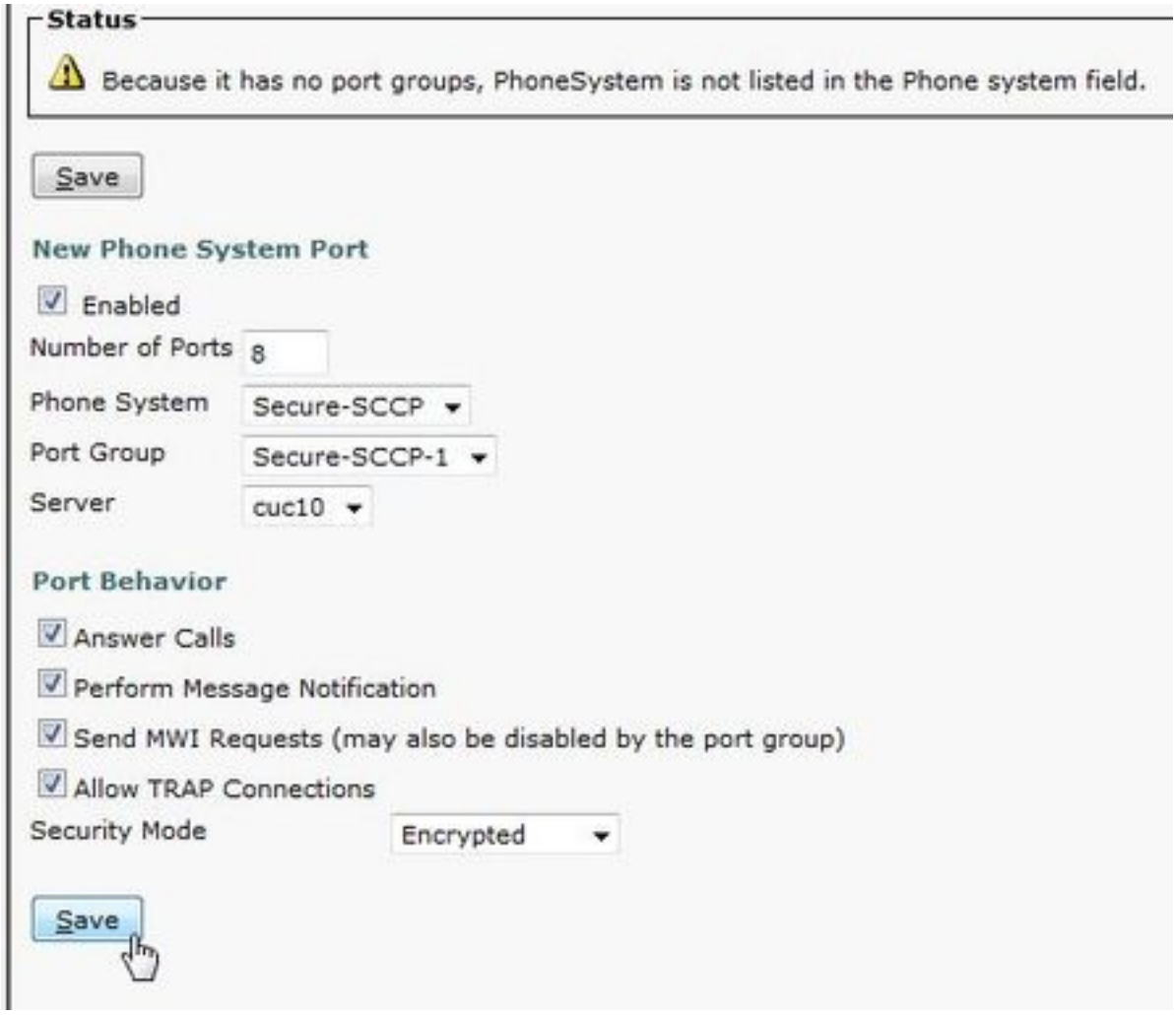
Navigate to **Edit > Servers** and add TFTP server from the CUCM cluster.

Note: It's important to provide correct TFTP address. CUC server downloads the CTL file from this TFTP as explained.

5. Add Secure SCCP ports

On the Port Group Basics page, in the Related Links drop-down box, select **Add Ports** and select **Go**. In the configuration window, enter this information:

- Enabled: checked
- Number of Ports:
- Phone System:
- Port Group:
- Server:
- Port behavior:
- Security Mode: **Encrypted**

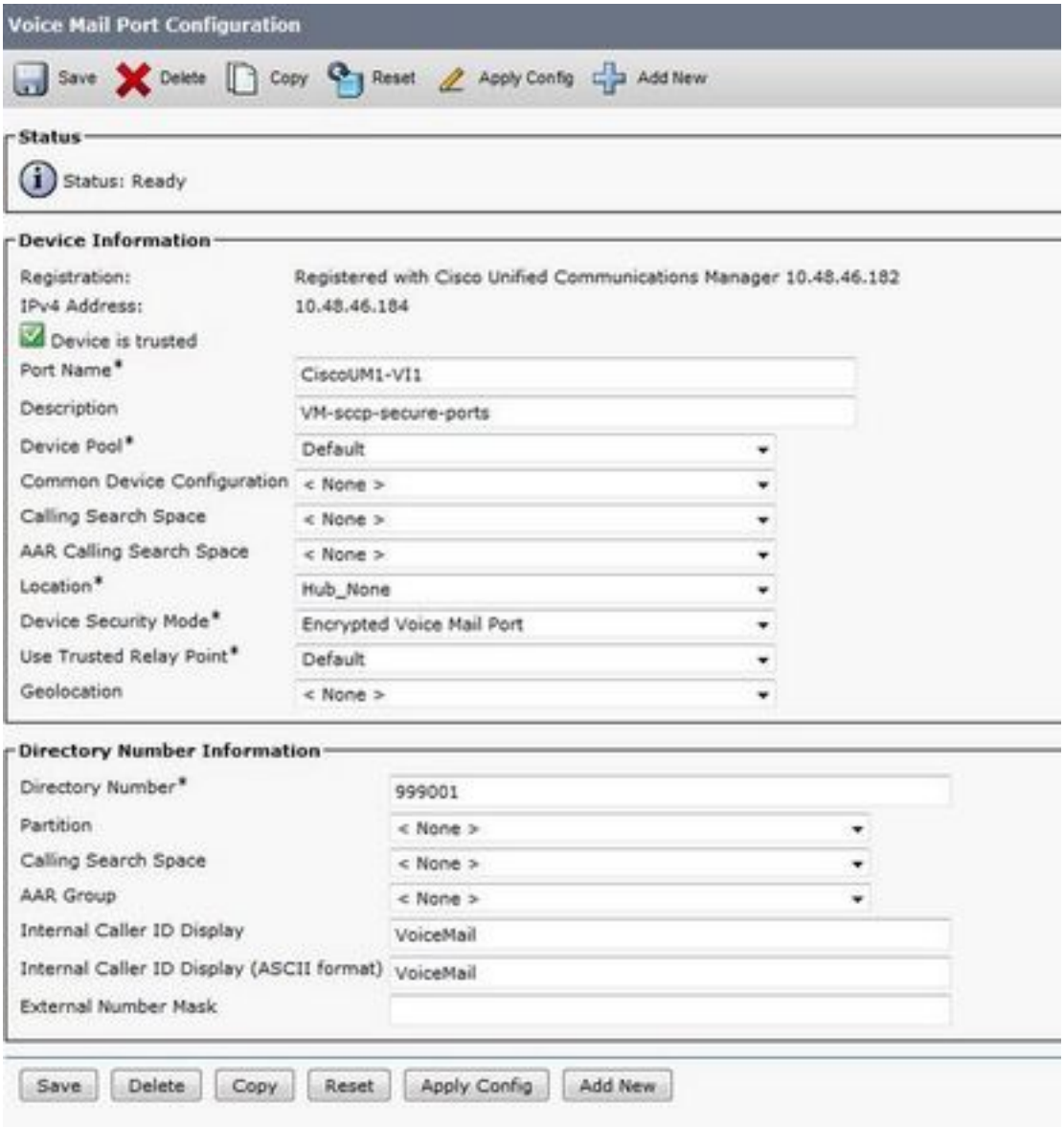


Configure CUCM

1. Add Ports

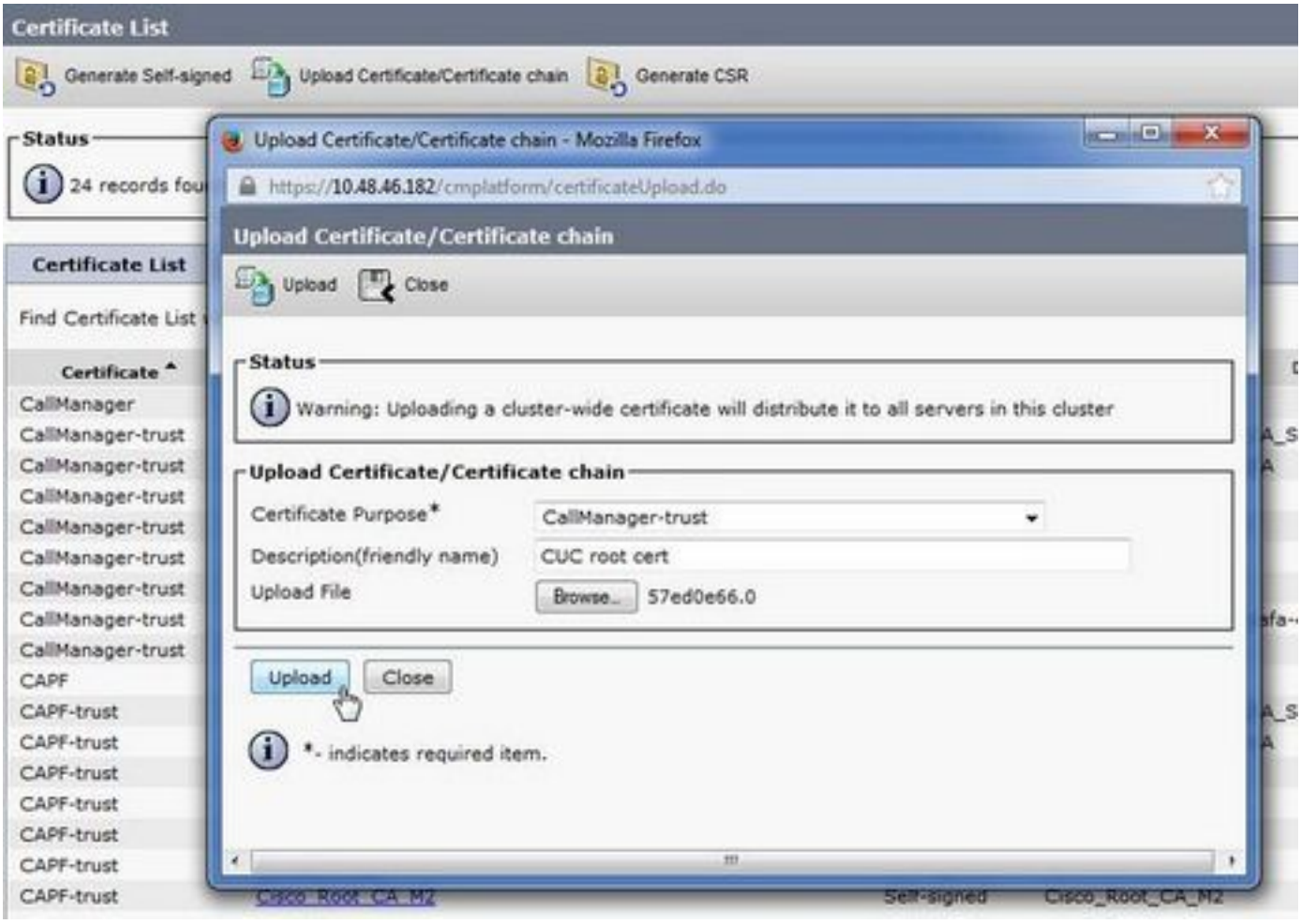
Navigate to **CUCM Administration > Advanced features > Voice Mail Port Configuration > Add New.**

Configure SCCP voice mail ports as usual. The only difference is in Device Security Mode under the port configuration where the Encrypted Voice Mail Port option needs to be seleted.



2. Upload CUC Root Certificate as CallManager-trust

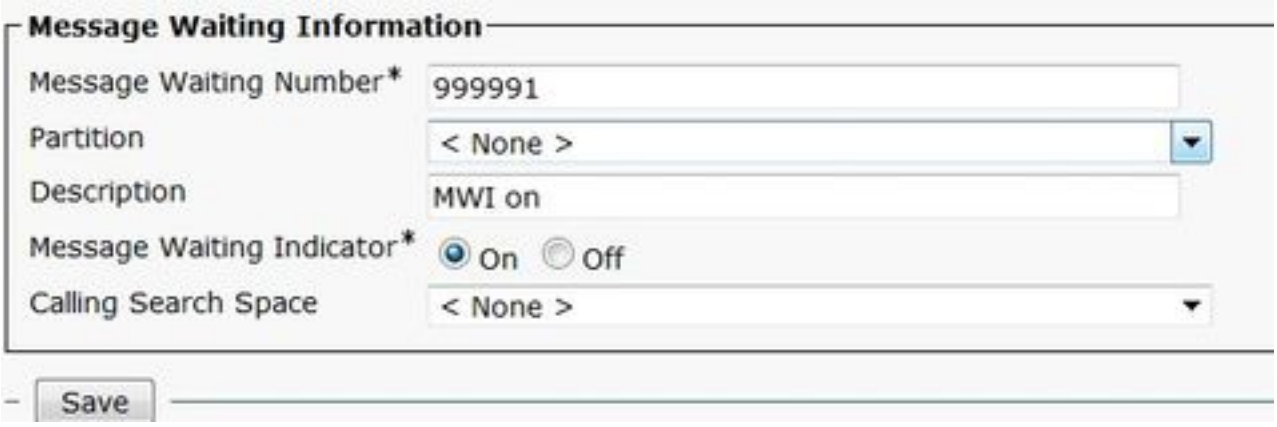
Navigate to **OS Administration > Security > Certificate Management > Upload Certificate/Certificate Chain** and upload the CUC root certificate as **CallManager-trust** on all nodes configured to communicate with the CUC server.

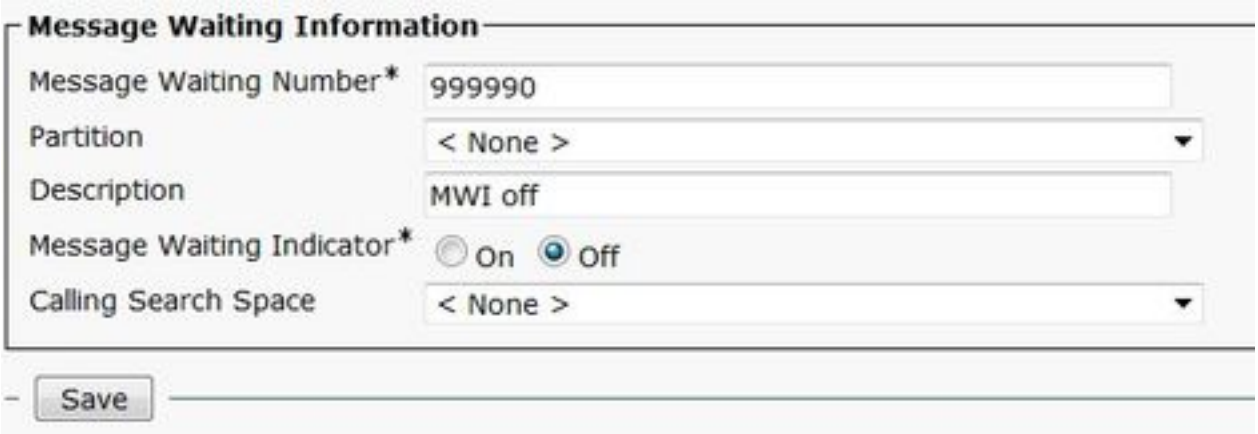


Note: Cisco CallManager service needs to be restarted after the certificate is uploaded in order for the certificate to take effect.

3. Configure Message Waiting Information (MWI) On/Off Extensions

Navigate to **CUCM Administration > Advanced Features > Voice Mail Port Configuration** and configure **MWI On/Off Extensions.** The MWI numbers must match the CUC configuration.

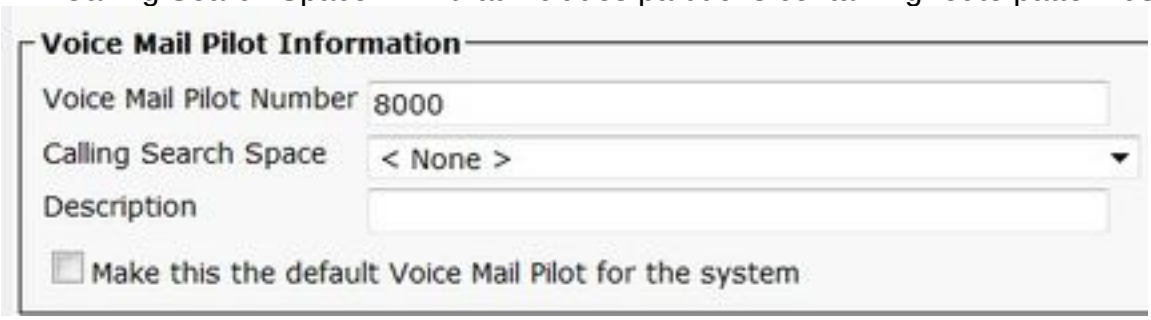




4. Create Voice Mail Pilot

Create a voice mail pilot for the integration (**Advanced Features > Voice Mail > Voice Mail Pilot**). Enter these values:

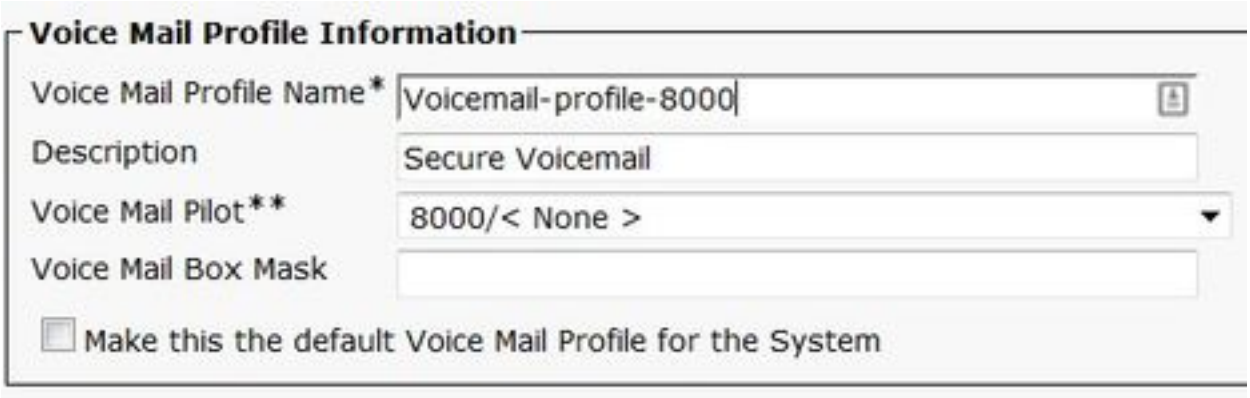
- Voice Mail Pilot Number:
- Calling Search Space: that includes partitions containing route pattern used as a pilot>



5. Create Voice Mail Profile

Create a voice mail profile in order to link all the settings together (**Advanced Features > Voice Mail > Voice Mail Profile). Enter this information:**

- Voice Mail Pilot:
- Voice Mail Box Mask:

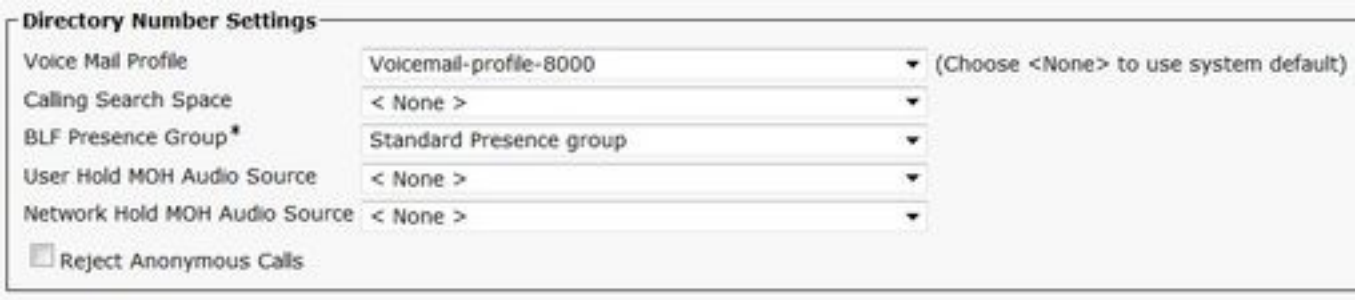


6. Assign Voice Mail Profile to the DNs

Assign the voice mail profile to the DNs that intend to use a secure integration. Click **Apply Config** button after the DN settings are changed:

Navigate to **Call Routing > Directory number** and change to:

- Voice Mail Profile: Voicemail-profile-8000

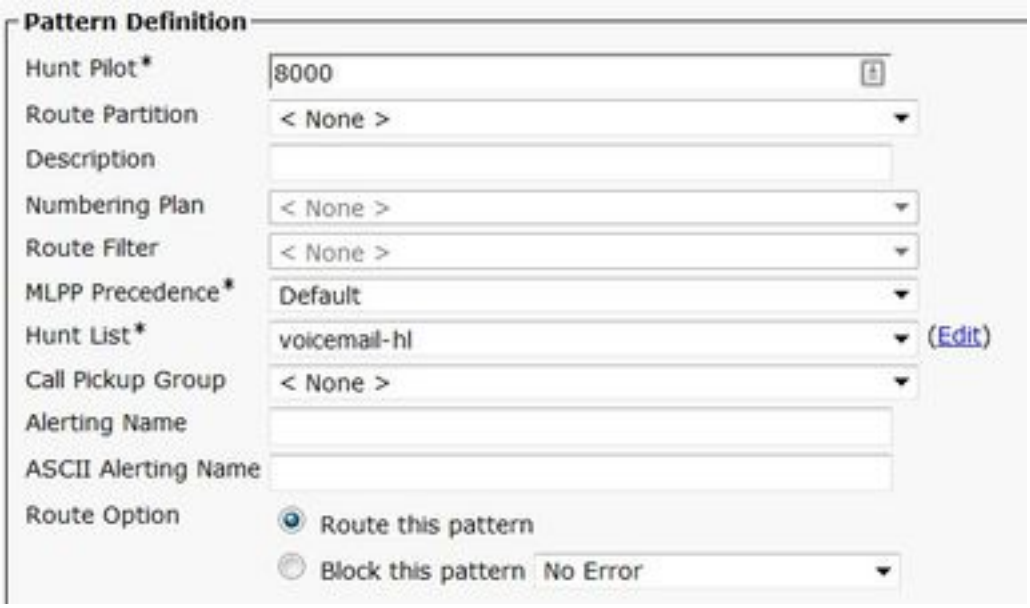


7. Create a Voice Mail Hunt Group

a) Add a new **Line group** (**Call Routing > Route/Hunt > Line group**)

b) Add a new voice mail **Hunt list** (**Call Routing > Route/Hunt > Hunt List**)

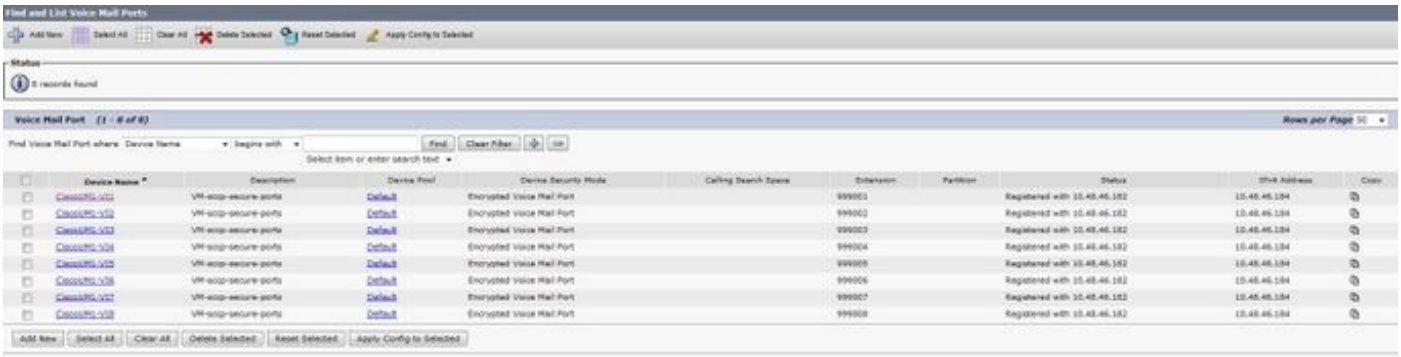
c) Add a new **Hunt Pilot** (**Call Routing > Route/Hunt > Hunt Pilot**)



Verify

SCCP Ports Verification

Navigate to **CUCM Administration > Advance Features > Voice Mail > Voice Mail Ports** and verify the port registration.



Press the V**oice Mail** button on the phone to call voice mail. You should hear the opening greeting if the user's extension is not configured on the Unity Connection system.

Secure SIP Trunk Verification

Press the **Voice Mail** button on the phone to call voice mail. You should hear the opening greeting if the user's extension is not configured on the Unity Connection system.

Alternatively, you can enable SIP OPTIONs keepalive to monitor the SIP trunk status. This option can be enabled in the SIP profile assigned to the SIP trunk. Once this is enabled you can monitor the Sip trunk status via **Device > Trunk** as shown in this image.

Secure RTP Call Verification

Verify whether the padlock icon is present on calls to Unity Connection. It means RTP stream is encrypted (Device Security profile must be secure in order for it to work) as shown in this image.

Troubleshoot

1. General Troubleshooting Tips

Follow these steps in order to troubleshoot the secure integration:

- Verify the configuration.
- Ensure that all related services are running. (CUCM - CallManager, TFTP, CUC - Conversation Manager)
- Make sure that ports required for secure communication between servers are open in the network (TCP port 2443 for SCCP integration and TCP 5061 for SIP integration).
- If all this is correct then proceed with the collection of traces.

2. Traces to Collect

Collect these traces to troubleshoot the secure integration.

- Packet capture from CUCM and CUC
- CallManager traces
- Cisco Conversation Manager traces

Refer to these resources for additional information about:

How to do a packet capture on CUCM:

http://www.cisco.com/c/en/us/support/docs/voice-unified-communications/unified-communications-manager-version-50/112040-packet-capture-cucm-00.html

How to enable traces on CUC server:

http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/10x/troubleshooting/guide/10xcuctsgx/10xcuctsg010.html

Common Issues

Case 1: Unable to Establish a Secure Connection (Unknown CA Alert)

After the packet capture is collected from either of the server, the TLS Session is established.

1	0.000000	130.235.201.241	130.235.203.249	TCP	instl_boots > https [SYN] Seq=0 Win=16384 Len=0 MSS=1460
2	0.000452	130.235.203.249	130.235.201.241	TCP	https > instl_boots [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=
3	0.000494	130.235.201.241	130.235.203.249	TCP	instl_boots > https [ACK] Seq=1 Ack=1 Win=17520 Len=0
4	0.001074	130.235.201.241	130.235.203.249	SSL	Client Hello
5	0.001341	130.235.203.249	130.235.201.241	TCP	https > instl_boots [ACK] Seq=1 Ack=141 Win=6432 Len=0
6	0.005269	130.235.203.249	130.235.201.241	TLSv1	Server Hello,
7	0.005838	130.235.203.249	130.235.201.241	TLSv1	Certificate, Server Hello Done
8	0.006480	130.235.201.241	130.235.203.249	TCP	instl_boots > https [ACK] Seq=141 Ack=1895 Win=17520 Len=0
9	0.012905	130.235.201.241	130.235.203.249	TLSv1	Alert (Level: Fatal, Description: Unknown CA)
10	0.013244	130.235.201.241	130.235.203.249	TCP	instl_boots > https [RST, ACK] Seq=148 Ack=1895 Win=0 Len=0
11	0.072262	130.235.201.241	130.235.203.249	TCP	instl_bootc > https [SYN] Seq=0 Win=16384 Len=0 MSS=1460
12	0.072706	130.235.203.249	130.235.201.241	TCP	https > instl_bootc [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=
13	0.072751	130.235.201.241	130.235.203.249	TCP	instl_bootc > https [ACK] Seq=1 Ack=1 Win=17520 Len=0

The client issued alert with a fatal error of Unknown CA to the server, just because the client could not verify the certificate sent by the server.

There are two possibilities:

1) CUCM sends the alert Unknown CA

- Verify that the current CUC root certificate is uploaded on the server that communicates with the CUC server.
- Ensure that the CallManager service is restarted on the corresponding server.

2) CUC sends the alert Unknown CA

- Verify that the TFTP IP address is correctly entered in the **Port Group > Edit > Servers** configuration on the CUC server.
- Verify that the CUCM TFTP server is reachable from the Connection server.
- Ensure that the CTL file on the CUCM TFTP is current (compare output of "show ctl" with certificates as seen on OS Admin page). Re-run the CTLClient if it's not.
- Reboot the CUC server OR delete and re-create the port group to re-download the CTL file from the CUCM TFTP.

Case 2: Unable to Download CTL File from CUCM TFTP

This error is seen in the Conversation Manager Traces:

```
MiuGeneral,25,FAILED Port group 'PhoneSystem-1' attempt set InService(true), error retrieving
server certificates.
MiuGeneral,25,Error executing tftp command 'tftp://10.48.47.189:69/CTLFile.tlv' res=68 (file not
found on server)
MiuGeneral,25,FAILED Port group 'PhoneSystem-1' attempt set InService(true), error retrieving
server certificates.
Arbiter,-1,Created port PhoneSystem-1-001 objectId='7c2e86b8-2d86-4403-840e-16397b3c626b' as
ID=1
MiuGeneral,25,Port group object 'b1c966e5-27fb-4eba-a362-56a5fe9c2be7' exists
MiuGeneral,25,FAILED SetInService=true parent port group is out of service:
```

Solution:

1. Double check that the TFTP server is correct in the **Port group > Edit > Servers** configuration.

2. Verify that the CUCM cluster is in secure mode.

3. Verify that the CTL file exist on the CUCM TFTP.

Case 3: Ports do not Register

This error is seen in the Conversation Manager Traces:

```
MiuSkinny,23,Failed to retrieve Certificate for CCM Server <CUCM IP Address>
MiuSkinny,23,Failed to extract any CCM Certificates - Registration cannot proceed. Starting
retry timer -> 5000 msec
MiuGeneral,24,Found local CTL file [/tmp/aaaaaaaa-xxxx-xxxx-xxxx-xxxxxxxxxxxx.tlv]
MiuGeneral,25,CCMCertificateCache::RetrieveServerCertificates() failed to find CCM Server '<CUCM
IP Address>' in CTL File
```

Solution:

1. This is most likely due to mismatch in md5 checksum of CTL file on CUCM and CUC as a result of regeneration of

certificates. Restart the CUC server to refresh the CTL file.

Cisco Internal Information

Alternatively, you can remove the CTL file from root as follow:

Delete the CTL file from /tmp/ folder and reset Port Group. You can do an md5 checksum on the file

and compare before deleting it:

CUCM: [root@vfrscucm1 trust-certs]# md5sum /usr/local/cm/tftp/CTLFile.tlv

e5bf2ab934a42f4d8e6547dfd8cc82e8 /usr/local/cm/tftp/CTLFile.tlv

CUC: [root@vstscuc1 tmp]# cd /tmp

[root@vstscuc1 tmp]# ls -al *tlv

-rw-rw-r--. 1 cucsmgr cuservice 6120 Feb 5 15:29 a31cefe5-9359-4cbc-a0f3-52eb870d976c.tlv

[root@vstscuc1 tmp]# md5sum a31cefe5-9359-4cbc-a0f3-52eb870d976c.tlv

e5bf2ab934a42f4d8e6547dfd8cc82e8 a31cefe5-9359-4cbc-a0f3-52eb870d976c.tlv

Additionally, you might refer to the this troubleshooting guide:

Defects

CSCum48958 - CUCM 10.0 (ip address length is incorrect)

CSCtn87264 - TLS connection fails for secure SIP ports

CSCur10758 - Unable to purge revoked certificates Unity Connection

CSCur10534 - Unity Connection 10.5 TLS/PKI inter-op redundant CUCM

CSCve47775 - Feature request for a method to update and review the CUCM's CTLFile on the CUC