Configuration Example for Secure SIP Integration Between CUCM and CUC based on Next Generation Encryption (NGE)

Contents

Introduction

This document describes the configuration and verification of the secure SIP connection between the Cisco Unified Communication Manager (CUCM) and Cisco Unity Connection (CUC) server using Next Generation Encryption.

Next Generation Security over SIP interface restricts SIP interface to use Suite B ciphers based on TLS 1.2, SHA-2 and AES256 protocols. It allows the various combinations of ciphers based on the priority order of RSA or ECDSA ciphers. During the communication between Unity Connection and Cisco Unified CM, both ciphers and third party certificates are verified at both the ends. Below is the configuration for Next Generation Encryption support.

If you plan to use the certificates signed by third party Certification Authority then start with Certificate signing at the end of the configuration section (Configure - Signing the EC key based certificates by third party CA)

Prerequisites

Requirements

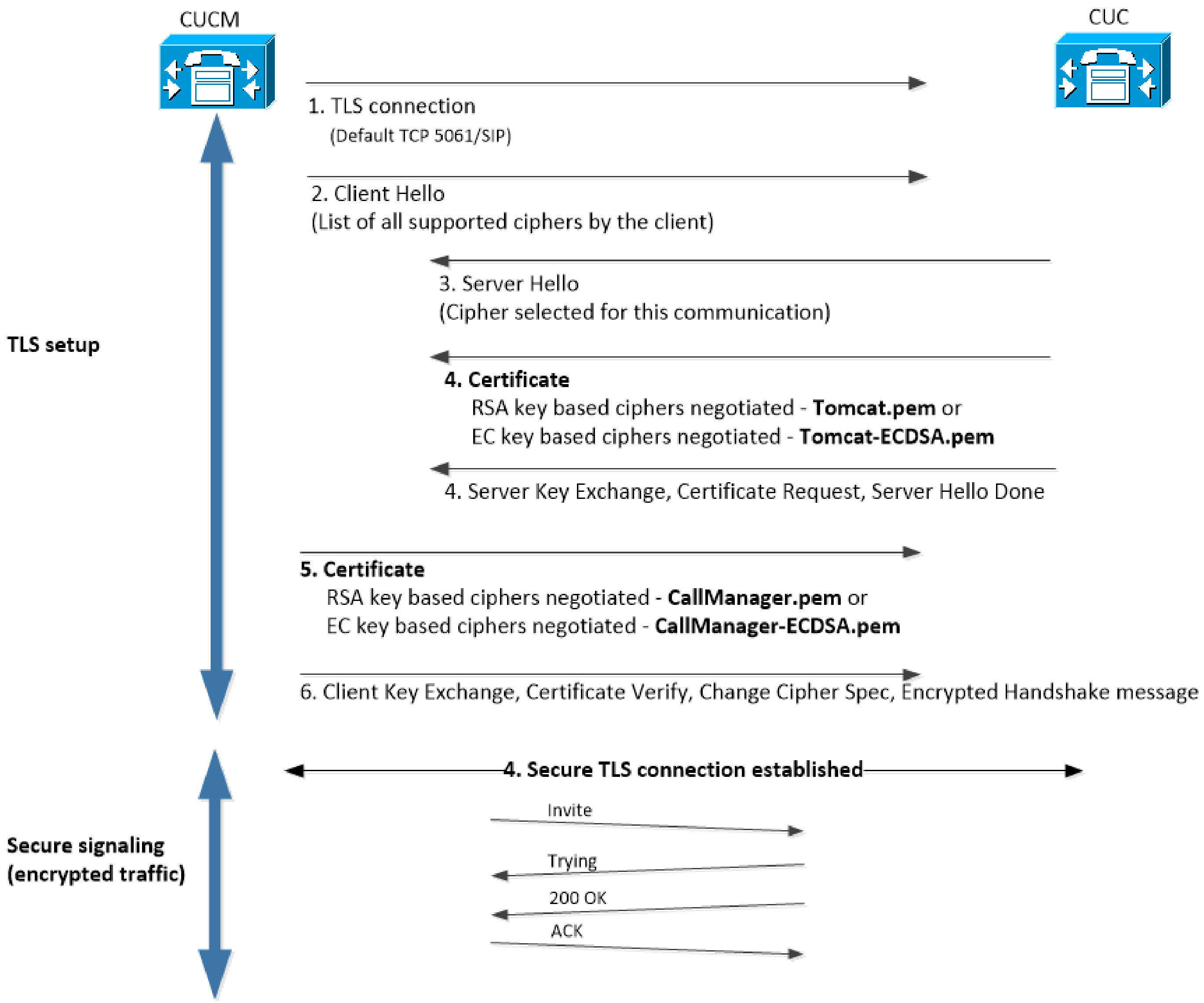
The information in this document is based on these software and hardware versions:

CUCM version 11.0 and later in Mixed mode
CUC version 11.0 and later

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.

Network Diagram

This diagram briefly explains the process that helps establish a secure connection between CUCM and CUC once the Next generation encryption support is enabled:


CUCM
CUC
1. TLS connection
(Default TCP 5061/SIP)
2. Client Hello
(List of all supported ciphers by the client)
3. Server Hello
(Cipher selected for this communication)
TLS setup
4. Certificate
RSA key based ciphers negotiated - Tomcat.pem or
EC key based ciphers negotiated - Tomcat-ECDSA.pem
4. Server Key Exchange, Certificate Request, Server Hello Done
5. Certificate
RSA key based ciphers negotiated - CallManager.pem or
EC key based ciphers negotiated - CallManager-ECDSA.pem
6. Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake message
4. Secure TLS connection established
Invite
Trying
200 OK
ACK
Secure signaling
(encrypted traffic)

Certificate requirements

These are the certificate exchange requirements once the Next generation encryption support is enabled on Cisco Unity Connection.

- **RSA key based ciphers negotiated**

CUCM certificate used	CUC certificate used	Certs to upload to CUCM	Certs to upload to CUC
CallManager.pem (self-signed)	Tomcat.pem (self-signed)	Tomcat.pem to be uploaded into CUCM > CallManger-trust	None.
CallManager.pem (CA signed)	Tomcat.pem (CA signed)	CUC root & intermediate CA certificate[*1] to be uploaded into CUCM > CallManager-trust	CUCM root & intermediate certificate[*2] to be uploaded CUC > CallManager-trust.
CallManager.pem (CA signed)	Tomcat.pem (self-signed)	Tomcat.pem to be uploaded into CUCM > CallManger-trust	CUCM root & intermediate certificate to be uploaded ir CUC > CallManager-trust.
CallManager.pem (self-signed)	Tomcat.pem (CA signed)	CUC root & intermediate CA certificate to be uploaded into CUCM > CallManager-trust	None.

[*1]CUC root & intermediate CA certificate refers to CA certificate which signed the Unity connection Tomcat certificate (Tomcat.pem).

[*2]CUCM root & intermediate CA certificate refers to CA certificate which signed the CUCM CallManager certificate (Callmanager.pem).

- **EC Key Based ciphers negotiated**

CUCM certificate used	**CUC certificate used**	**Certs to upload to CUCM**	**Certs to upload to CUC**
CallManager-ECDSA.pem (self-signed)	Tomcat-ECDSA.pem (self-signed)	Tomcat-ECDSA.pem to be uploaded into CUCM > CallManger-trust	None.
CallManager-ECDSA.pem (CA signed)	Tomcat-ECDSA.pem (CA signed)	CUC root & intermediate CA certificate[*1] to be uploaded into CUCM > CallManager-trust	CUCM root & intermediate CA certificate[*2] to be uploaded into CUC > CallManager-trust.
CallManager-ECDSA.pem (CA signed)	Tomcat-ECDSA.pem (self-signed)	Tomcat-ECDSA.pem to be uploaded into CUCM > CallManger-trust.	CUCM root & intermediate CA certificate to be uploaded into CUC > CallManager-trust.
CallManager-ECDSA.pem (self-signed)	Tomcat-ECDSA.pem (CA signed)	CUC root & intermediate CA certificate to be uploaded into CUCM > CallManager-trust	None.

[*1] CUC root & intermediate CA certificate refers to CA certificate which signed the Unity connection EC based Tomcat certificate (Tomcat-ECDSA.pem).

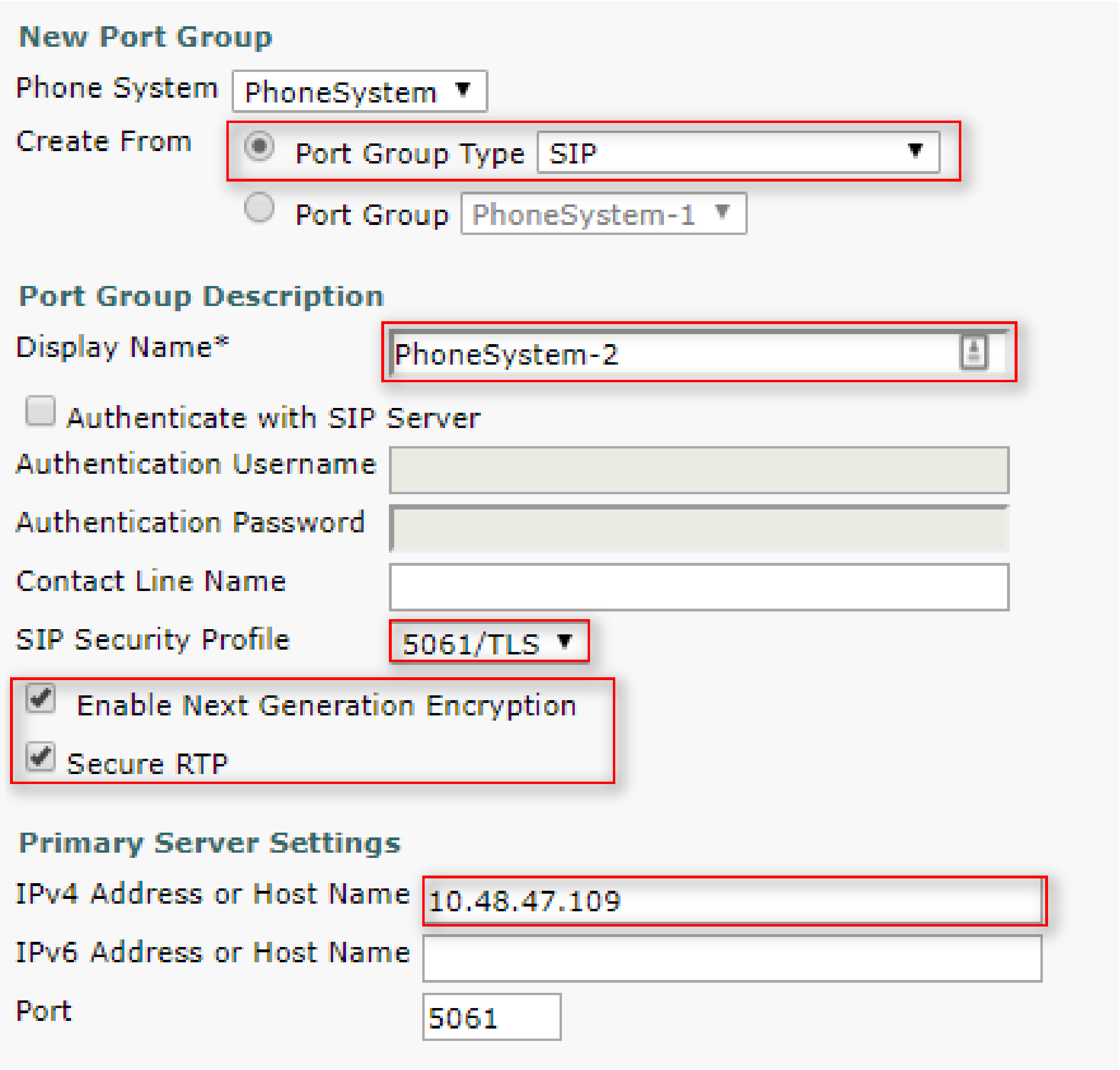
[*2] CUCM root & intermediate CA certificate refers to CA certificate which signed the CUCM CallManager certificate (CallManager-ECDSA.pem).

1. **Note**: Tomcat-ECDSA.pem certificate is called CallManager-ECDSA.pem in 11.0.1 versions of CUC. From CUC 11.5.x the certificate has been renamed to Tomcat-ECDSA.pem.

Configure - Cisco Unity Connection (CUC)

1. Add a New Port Group

Navigate to Cisco Unity Connection Administration page > Telephony integration > Port group and Click on Add New. Make sure to check the Enable Next Generation Encryption checkbox.



New Port Group

Phone System: PhoneSystem ▼

Create From: ● Port Group Type: SIP ▼

○ Port Group: PhoneSystem-1 ▼

Port Group Description

Display Name*: PhoneSystem-2

☐ Authenticate with SIP Server

Authentication Username:

Authentication Password:

Contact Line Name:

SIP Security Profile: 5061/TLS ▼

☑ Enable Next Generation Encryption

☑ Secure RTP

Primary Server Settings

IPv4 Address or Host Name: 10.48.47.109

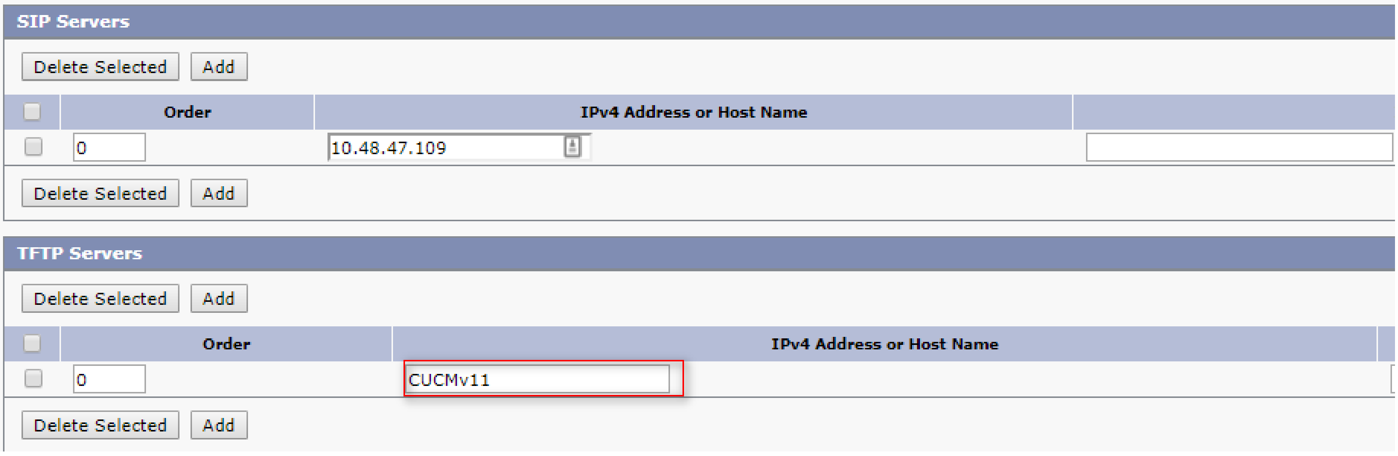
IPv6 Address or Host Name:

Port: 5061

1. **Note**:Unity Connection's Cisco Tomcat certificate will be used during SSL handshake once the Enable Next Generation Encryption checkbox is enabled.
   - In case ECDSA based cipher is negotiated then EC key based tomcat-ECDSA certificate is used in SSL handshake.
   - In case RSA based cipher is negotiated then RSA key based tomcat certificate is used in SSL handshake.

2. Add the TFTP server reference

On the Port Group Basics page, navigate to Edit > Servers and add FQDN of TFTP server of your CUCM cluster. FQDN/Hostname of the TFTP server must match the Common name (CN) of CallManager certificate. IP address of the server will not work and it will result in failure to download the ITL file. The DNS name must be therefore resolvable via configured DNS server.



SIP Servers

□	Order	IPv4 Address or Host Name	
□	0	10.48.47.109	

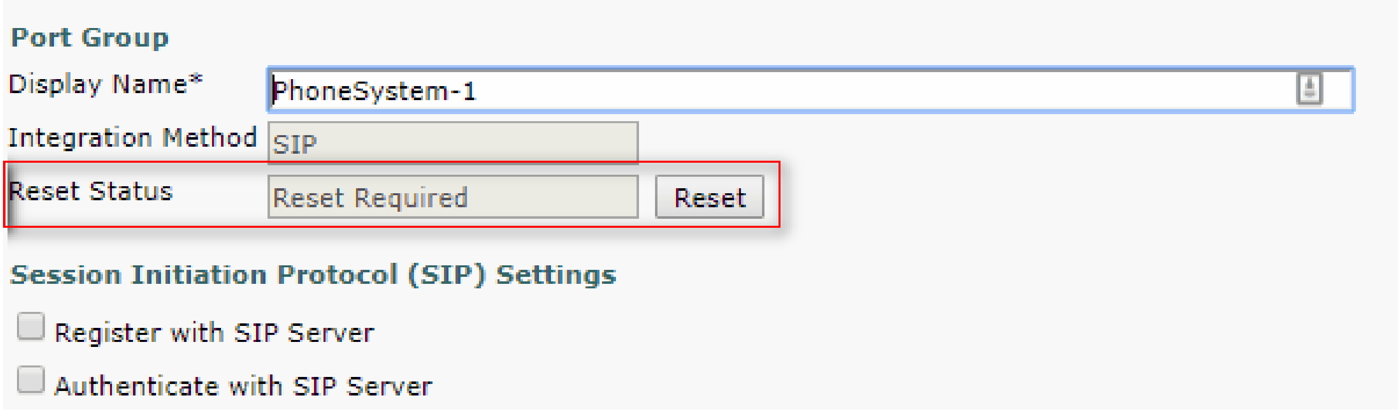
TFTP Servers

□	Order	IPv4 Address or Host Name
□	0	CUCMv11

Restart Connection Conversation Manager on each node by navigating to Cisco Unity Connection Serviceability > Tools > Service Management. This is mandatory for the configuration to take effect.

1. **Note**: Unity connection downloads ITL file (ITLfile.tlv) from CUCM's TFTP using https protocol on secure 6972 port (URL: https://<CUCM-TFTP-FQDN>:6972/ITLFile.tlv). CUCM must be in the mixed mode since CUC is looking for the "CCM+TFTP" function certificate from the ITL file.

Navigate back to Telephony integration > Port group > Port Group Basics configuration page and reset your newly added Port group.



Port Group

Display Name* PhoneSystem-1

Integration Method SIP

Reset Status Reset Required

Session Initiation Protocol (SIP) Settings

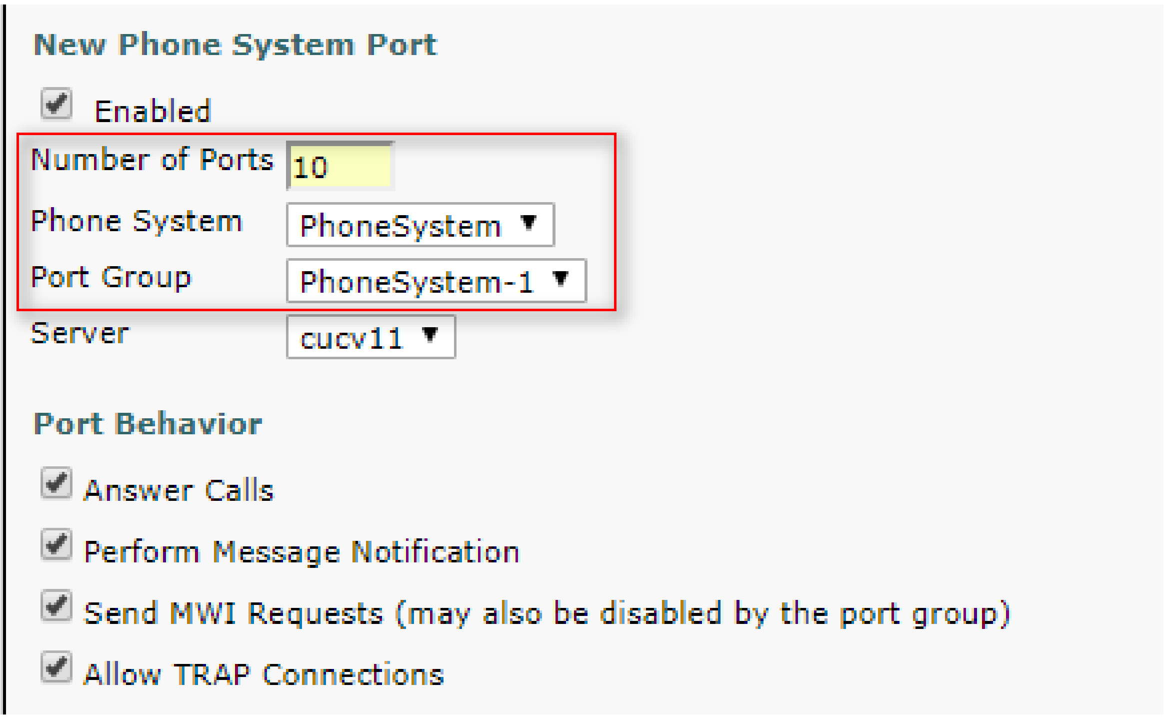
□ Register with SIP Server

□ Authenticate with SIP Server

1. **Note**: Every time the port group is reset, the CUC server will update its locally stored ITL file by connecting to CUCM server.

3. Add Voice Mail Ports

Navigate back to Telephony integration > Port and click on Add new to add port to your newly created port group.



New Phone System Port

☑ Enabled

Number of Ports: 10

Phone System: PhoneSystem

Port Group: PhoneSystem-1

Server: cucv11

Port Behavior

☑ Answer Calls

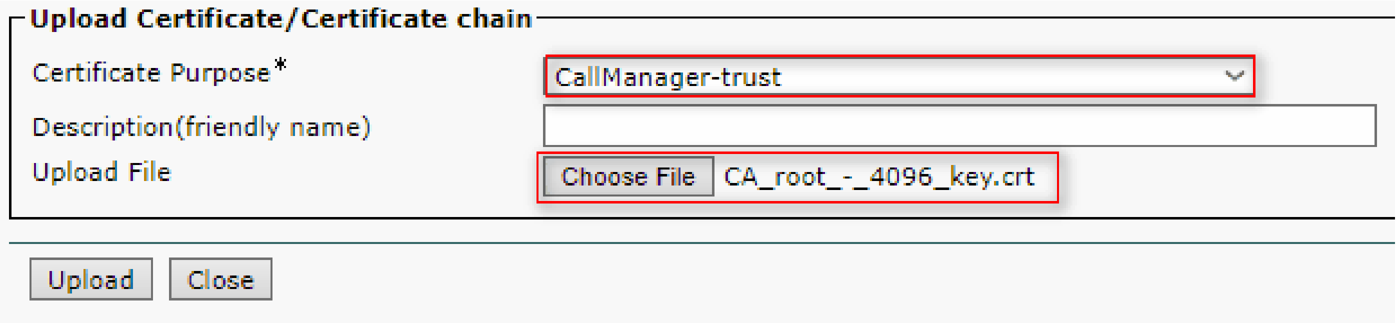
☑ Perform Message Notification

☑ Send MWI Requests (may also be disabled by the port group)

☑ Allow TRAP Connections

4. Upload CUCM Root and intermediate certificate of the third party CA

In case of third party certificates, you must upload the Root and Intermediate certificate of the third party Certification Authority on CallManager-trust of Unity Connection. This is needed only if 3rd party CA signed your Call Manager certificate. Perform this action by navigating to Cisco Unified OS Administration > Security > Certificate Management and click on Upload Certificate.



Upload Certificate/Certificate chain

Certificate Purpose*: CallManager-trust

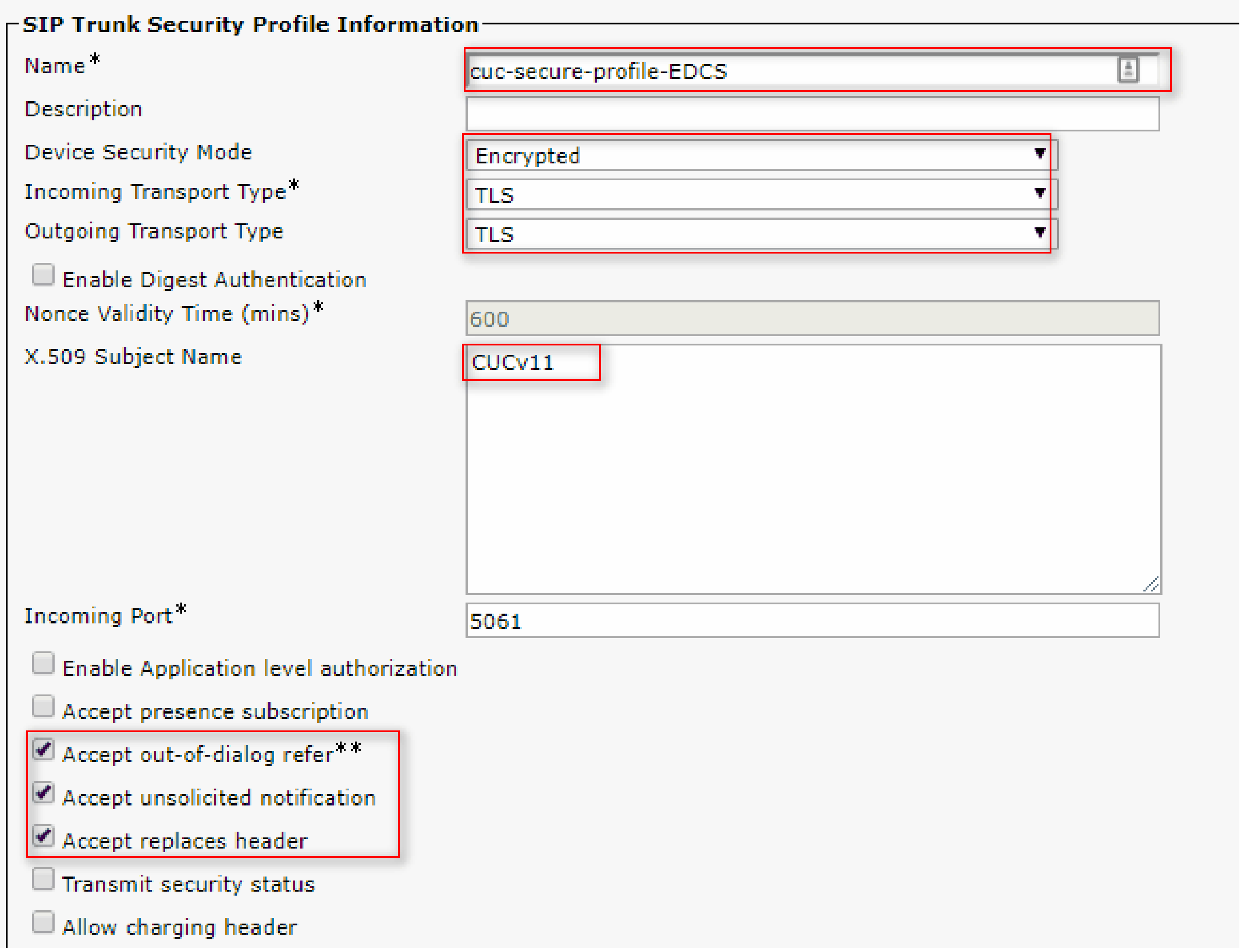
Description(friendly name):

Upload File: Choose File CA_root_-_4096_key.crt

Configure - Cisco Unified CM (CUCM)

1. Create a SIP trunk security profile

Navigate to CUCM Administration > System > Security > SIP Trunk Security Profile and add a new profile. X.509 Subject Name must match the FQDN of the CUC server.



SIP Trunk Security Profile Information

Name*	cuc-secure-profile-EDCS
Description	
Device Security Mode	Encrypted
Incoming Transport Type*	TLS
Outgoing Transport Type	TLS
□ Enable Digest Authentication	
Nonce Validity Time (mins)*	600
X.509 Subject Name	CUCv11
Incoming Port*	5061

□ Enable Application level authorization

□ Accept presence subscription

☑ Accept out-of-dialog refer**

☑ Accept unsolicited notification

☑ Accept replaces header

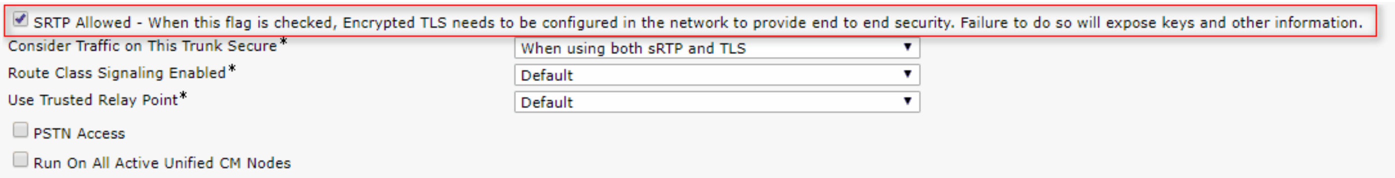
□ Transmit security status

□ Allow charging header

1. **Note**: CLI command "show cert own tomcat/tomcat.pem" can display the RSA key based tomcat certificate on Unity Connection. It's CN must match the X.509 Subject name configured on CUCM. The CN is equal to FQDN/Hostname of the Unity server. The EC key based certificate contains the FQDN/hostname in its Subject Alternate Name (SAN) field.

2. Create a secure SIP Trunk

Navigate to Device > Trunk > Click and Add new and create a standard SIP trunk which will be used for secure integration with Unity Connection.

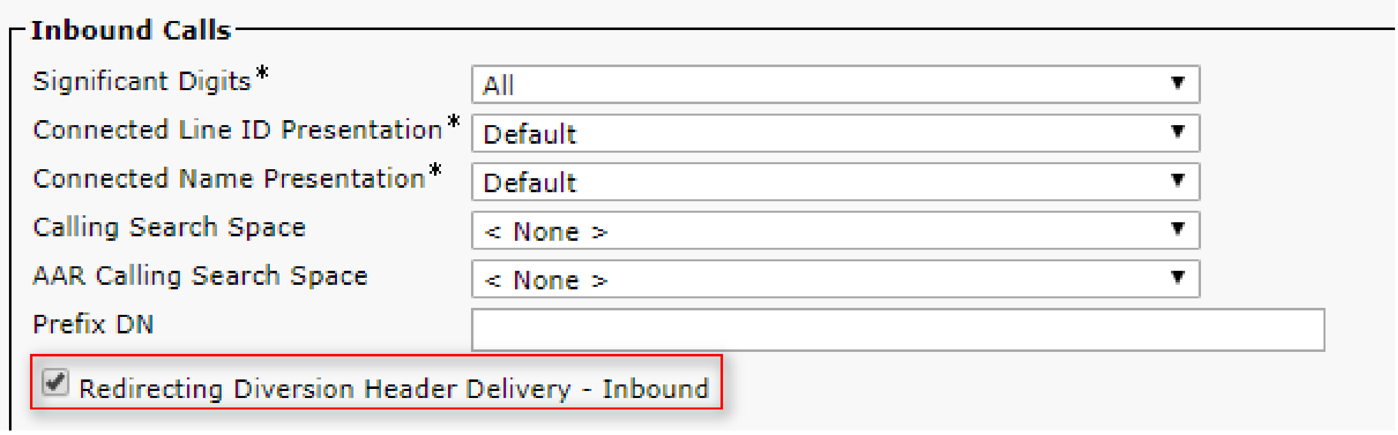


☑ SRTP Allowed - When this flag is checked, Encrypted TLS needs to be configured in the network to provide end to end security. Failure to do so will expose keys and other information.

Consider Traffic on This Trunk Secure*	When using both sRTP and TLS
Route Class Signaling Enabled*	Default
Use Trusted Relay Point*	Default

□ PSTN Access

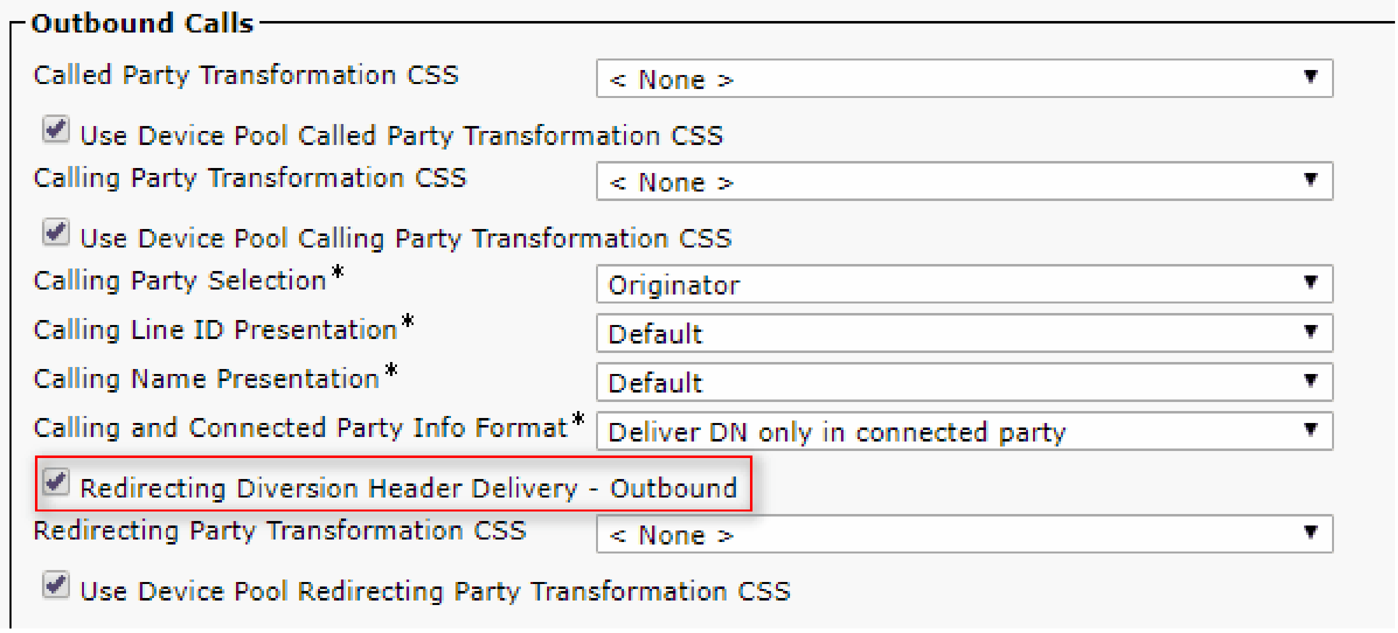
□ Run On All Active Unified CM Nodes



Inbound Calls

Significant Digits*	All
Connected Line ID Presentation*	Default
Connected Name Presentation*	Default
Calling Search Space	< None >
AAR Calling Search Space	< None >
Prefix DN	

☑ Redirecting Diversion Header Delivery - Inbound



Outbound Calls

Called Party Transformation CSS	< None >

☑ Use Device Pool Called Party Transformation CSS

Calling Party Transformation CSS	< None >

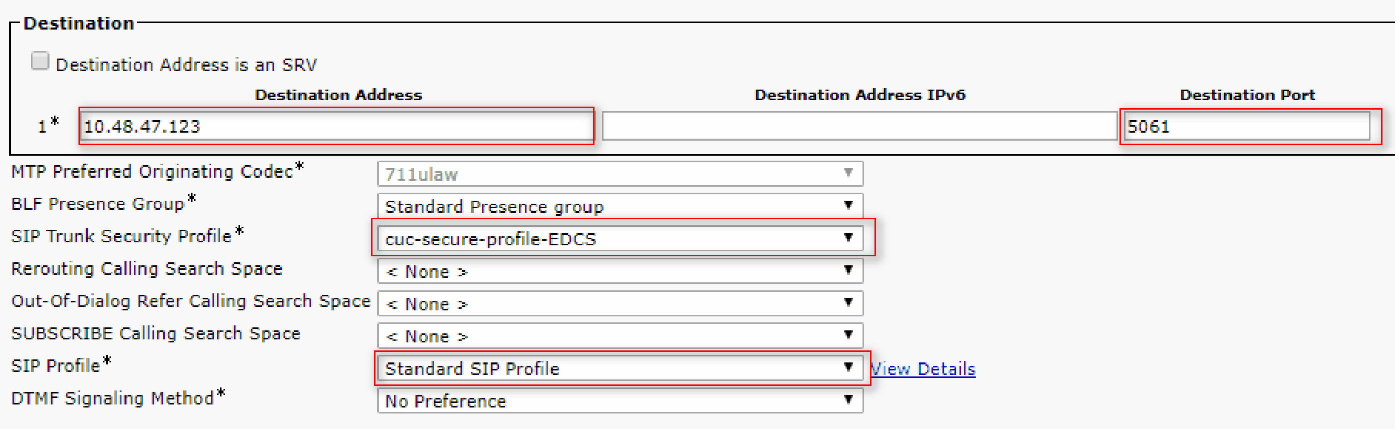
☑ Use Device Pool Calling Party Transformation CSS

Calling Party Selection*	Originator
Calling Line ID Presentation*	Default
Calling Name Presentation*	Default
Calling and Connected Party Info Format*	Deliver DN only in connected party

☑ Redirecting Diversion Header Delivery - Outbound

Redirecting Party Transformation CSS	< None >

☑ Use Device Pool Redirecting Party Transformation CSS



Destination

□ Destination Address is an SRV

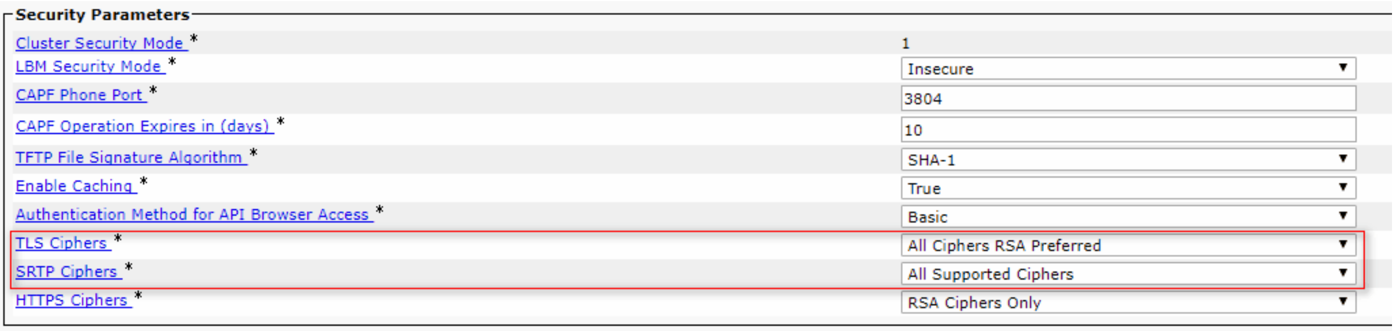
	Destination Address	Destination Address IPv6	Destination Port
1*	10.48.47.123		5061

MTP Preferred Originating Codec*	711ulaw
BLF Presence Group*	Standard Presence group
SIP Trunk Security Profile*	cuc-secure-profile-EDCS
Rerouting Calling Search Space	< None >
Out-Of-Dialog Refer Calling Search Space	< None >
SUBSCRIBE Calling Search Space	< None >
SIP Profile*	Standard SIP Profile
DTMF Signaling Method*	No Preference

3. Configure TLS and SRTP ciphers

1. **Note**: The negotiation between Unity Connection and Cisco Unified Communications Manager depends on the TLS cipher configuration with the following conditions: When Unity Connection acts as server, TLS cipher negotiation is based on the preference selected by Cisco Unified CM.In case ECDSA based cipher is negotiated then EC key based tomcat-ECDSA certificates are used in SSL handshake.In case RSA based cipher is negotiated then RSA key based tomcat certificates are used in SSL handshake.When Unity Connection acts as client, TLS cipher negotiation is based on the preference selected by Unity Connection.

Navigate to Cisco Unified CM > Systems > Enterprise Parameters and select the appropriate cipher option from the TLS and SRTP Ciphers from drop-down list.

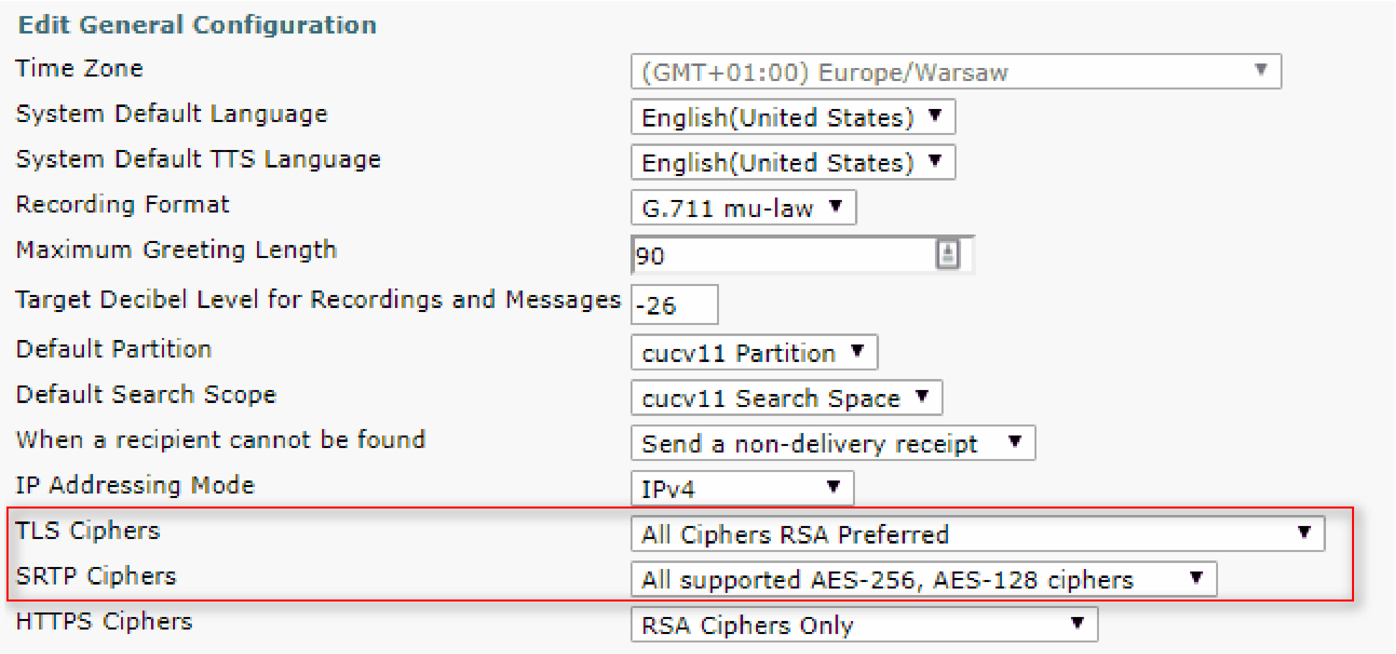


Security Parameters

Cluster Security Mode *	1
LBM Security Mode *	Insecure
CAPF Phone Port *	3804
CAPF Operation Expires in (days) *	10
TFTP File Signature Algorithm *	SHA-1
Enable Caching *	True
Authentication Method for API Browser Access *	Basic
TLS Ciphers *	All Ciphers RSA Preferred
SRTP Ciphers *	All Supported Ciphers
HTTPS Ciphers *	RSA Ciphers Only

Restart the Cisco Call Manager service on each node by navigating to Cisco Unified Serviceability page, Tools > Control Centre-Feature Services and select Cisco Call Manager under CM Services

Navigate to Cisco Unity Connection Administration page > System Settings > General Configurations and select the appropriate cipher option from the TLS and SRTP Ciphers from drop-down list.



Edit General Configuration

Time Zone	(GMT+01:00) Europe/Warsaw
System Default Language	English(United States)
System Default TTS Language	English(United States)
Recording Format	G.711 mu-law
Maximum Greeting Length	90
Target Decibel Level for Recordings and Messages	-26
Default Partition	cucv11 Partition
Default Search Scope	cucv11 Search Space
When a recipient cannot be found	Send a non-delivery receipt
IP Addressing Mode	IPv4
TLS Ciphers	All Ciphers RSA Preferred
SRTP Ciphers	All supported AES-256, AES-128 ciphers
HTTPS Ciphers	RSA Ciphers Only

Restart Connection Conversation Manager on each node by navigating to Cisco Unity Connection Serviceability > Tools > Service Management.

TLS Cipher options with Priority order

TLS Cipher Options	**TLS Ciphers in Priority Order**
Strongest- AES-256 SHA-384 Only: RSA Preferred	• TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
Strongest-AES-256 SHA-384 Only: ECDSA Preferred	• TLS_ECDHE_ECDSA_WITH_AES_256_GCM_384 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SH
Medium-AES-256 AES-128 Only: RSA Preferred	• TLS_ECDHE_RSA_WITH_AES_256_GCM_SH • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

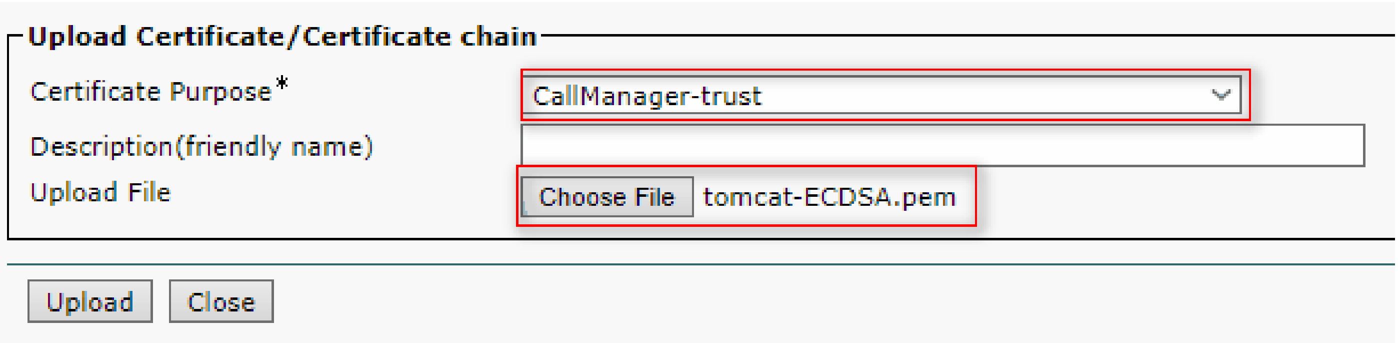
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SH TLS_ECDHE_ECDSA_WITH_AES_128_GCM_ 256
Medium-AES-256 AES-128 Only: ECDSA Preferred	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_ 384 TLS_ECDHE_RSA_WITH_AES_256_GCM_SH TLS_ECDHE_ECDSA_WITH_AES_128_GCM_ 256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SH
All Ciphers RSA Preferred (Default)	TLS_ECDHE_RSA_WITH_AES_256_GCM_SH TLS_ECDHE_ECDSA_WITH_AES_256_GCM_ 384 TLS_ECDHE_RSA_WITH_AES_128_GCM_SH TLS_ECDHE_ECDSA_WITH_AES_128_GCM_ 256 TLS_RSA_WITH_AES_128_CBC_SHA
All Ciphers ECDSA Preferred	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_ 384 TLS_ECDHE_RSA_WITH_AES_256_GCM_SH TLS_ECDHE_ECDSA_WITH_AES_128_GCM_ 256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SH TLS_RSA_WITH_AES_128_CBC_SHA

SRTP Cipher Options in Priority order

SRTP Cipher Option	SRTP in Priority Order
All supported AES-256, AES-128 ciphers	AEAD_AES_256_GCM AEAD_AES_128_GCM AES_CM_128_HMAC_SHA1_32
AEAD AES-256, AES-28 GCM-based ciphers	AEAD_AES_256_GCM AEAD_AES_128_GCM
AEAD AES256 GCM-based ciphers only	AEAD_AES_256_GCM

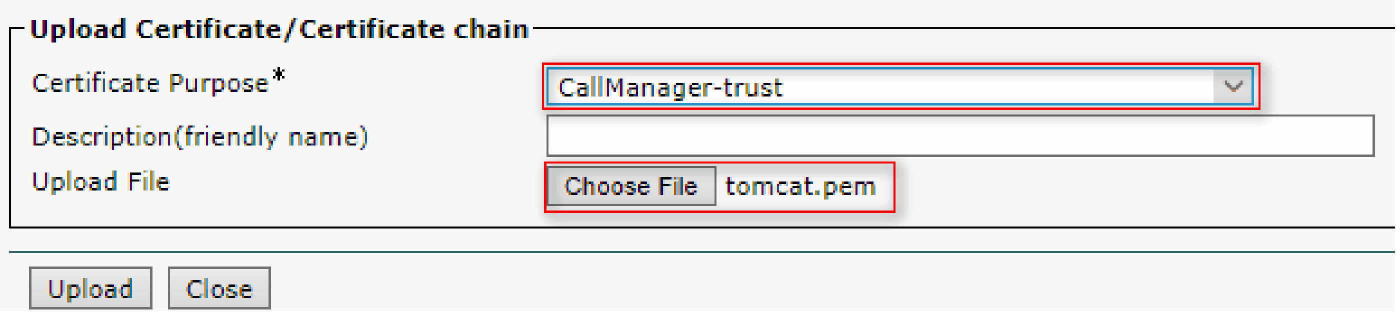
4. Upload CUC Tomcat certificates (RSA & EC based)

Navigate to OS Administration > Security > Certificate Management and upload both CUC Tomcat certificates (RSA & EC based) into the CallManager-trust store.



Upload Certificate/Certificate chain

Certificate Purpose*	CallManager-trust
Description(friendly name)	
Upload File	Choose File tomcat-ECDSA.pem

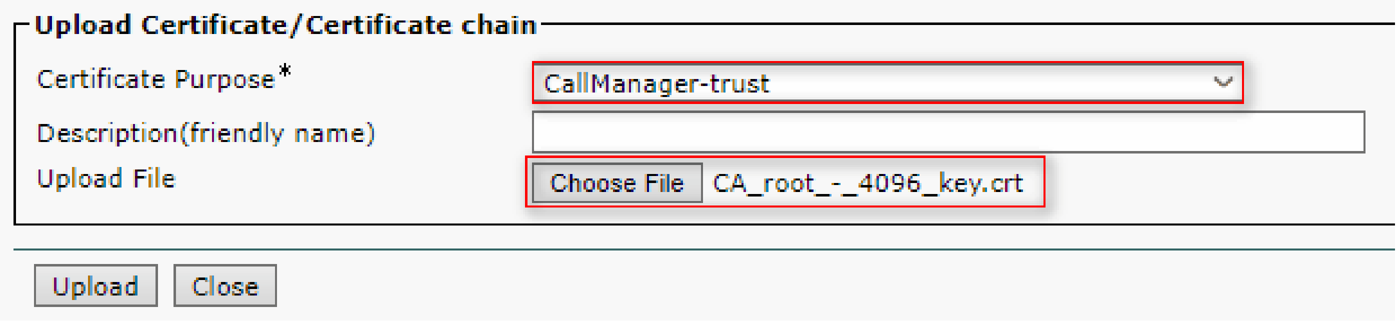


Upload Certificate/Certificate chain

Certificate Purpose*	CallManager-trust
Description(friendly name)	
Upload File	Choose File tomcat.pem

1. **Note**: Uploading both Unity Tomcat certificates is not mandatory if ECDSA ciphers are negotiated only. In such case EC based Tomcat certificate is enough.

In case of third party certificates, you must upload the root and Intermediate certificate of the third party Certification Authority. This is needed only if 3rd party CA signed your Unity Tomcat certificate.



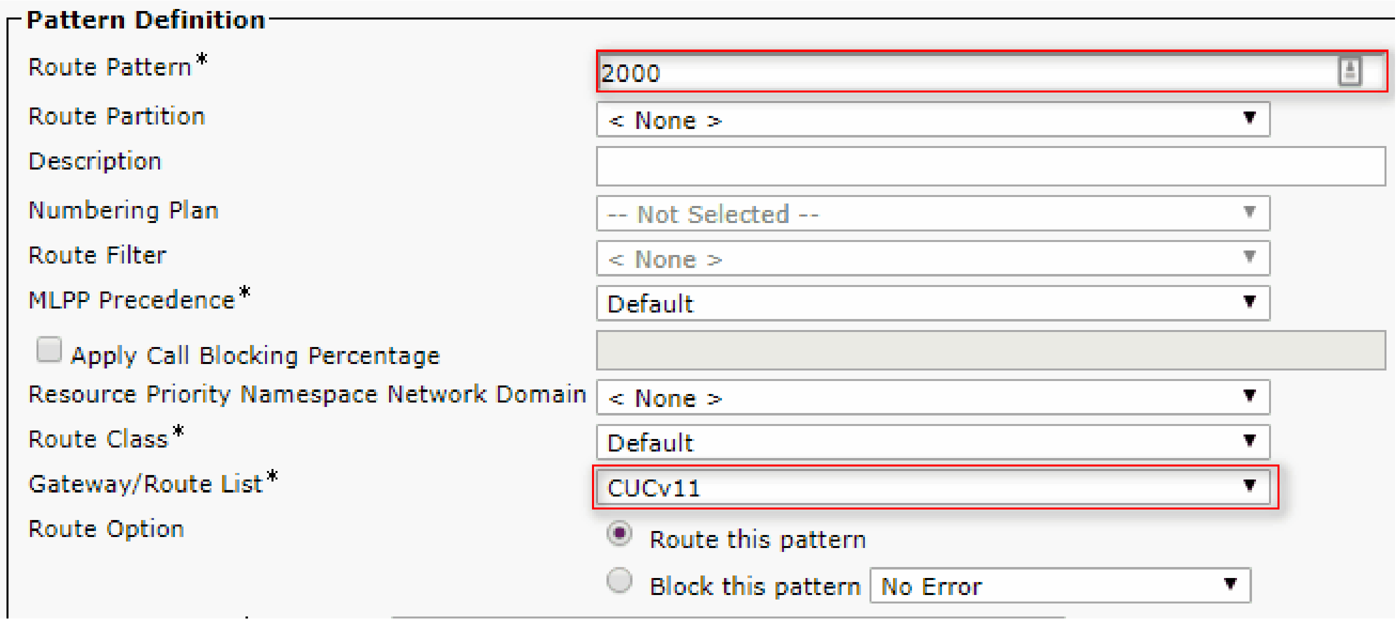
Upload Certificate/Certificate chain

Certificate Purpose*	CallManager-trust
Description(friendly name)	
Upload File	Choose File CA_root_-_4096_key.crt

Restart the Cisco Call Manager process on all nodes to apply the changes.

5. Create Route pattern

Configure a route pattern that points to the configured trunk by navigating to Call Routing > Route/Hunt > Route Pattern. Extension entered as a route pattern number can be used as a voicemail pilot.



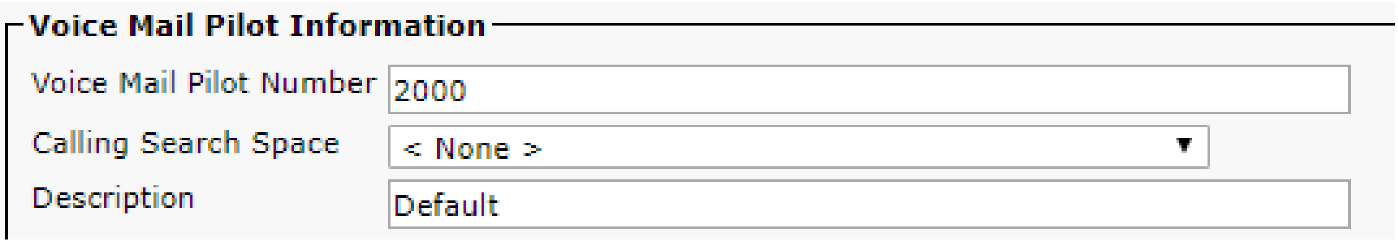
Pattern Definition

Route Pattern*	2000
Route Partition	< None >
Description	
Numbering Plan	-- Not Selected --
Route Filter	< None >
MLPP Precedence*	Default
□ Apply Call Blocking Percentage	
Resource Priority Namespace Network Domain	< None >
Route Class*	Default
Gateway/Route List*	CUCv11
Route Option	● Route this pattern ○ Block this pattern No Error

6. Create Voicemail Pilot, Voicemail Profile and assign it to the DNs

Create a voice mail pilot for the integration by going to Advanced Features > Voice Mail > Voice

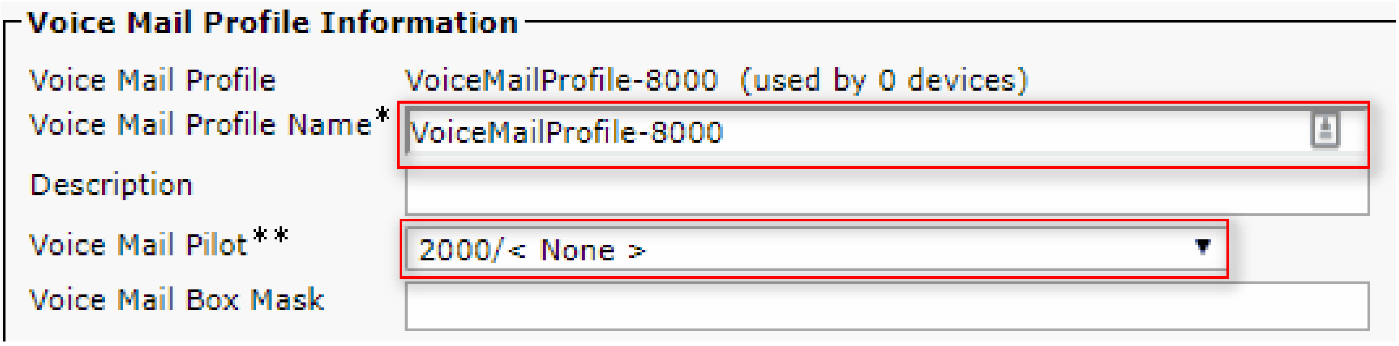
Mail Pilot.



Voice Mail Pilot Information

Voice Mail Pilot Number	2000
Calling Search Space	< None >
Description	Default

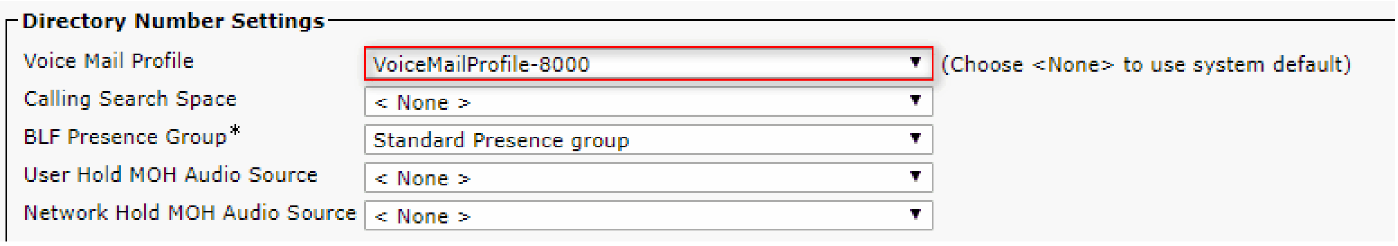
Create a voice mail profile in order to link all the settings together Advanced Features > Voice Mail > Voice Mail Profile



Voice Mail Profile Information

Voice Mail Profile	VoiceMailProfile-8000 (used by 0 devices)
Voice Mail Profile Name*	VoiceMailProfile-8000
Description	
Voice Mail Pilot**	2000/< None >
Voice Mail Box Mask	

Assign the newly created voice mail profile to the DNs intended to use the secure integration by going to Call Routing > Directory number



Directory Number Settings

Voice Mail Profile	VoiceMailProfile-8000	(Choose <None> to use system default)
Calling Search Space	< None >	
BLF Presence Group*	Standard Presence group	
User Hold MOH Audio Source	< None >	
Network Hold MOH Audio Source	< None >	

Configure - Signing the EC key based certificates by third party CA (optional)

The certificates might be signed by a third party CA before setting up the secure integration between the systems. Follow the following steps to sign the certificates on both systems.

Cisco Unity Connection

1. Generate Certificate signing request (CSR) for CUC Tomcat-ECDSA and have the certificate signed by third party CA
2. CA provides Identity certificate (CA signed certificate) and CA certificate (CA root certificate) which must be uploaded as follow:
   Upload CA root certificate into the tomcat-trust store
   Upload Identity certificate into the tomcat-EDCS store
3. Restart Conversation Manager on CUC

Cisco Unified CM

1. Generate CSR for CUCM CallManager-ECDSA and have the certificate signed by third party CA

2. CA provides Identity certificate (CA signed certificate) and CA certificate (CA root certificate) which must be uploaded as follow:
   Upload CA root certificate into the callmanager-trust store
   Upload Identity certificate into the callmanager-EDCS store
3. Restart Cisco CCM and TFTP services on each node

The same process will be used to sign RSA key based certificates where CSR is generated for CUC Tomcat certificate and CallManager certificate and uploaded into the tomcat store and callmanager store respectively.

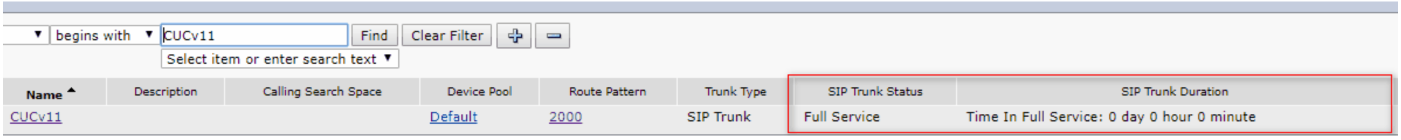
Verify

Use this section to confirm that your configuration works properly.

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.

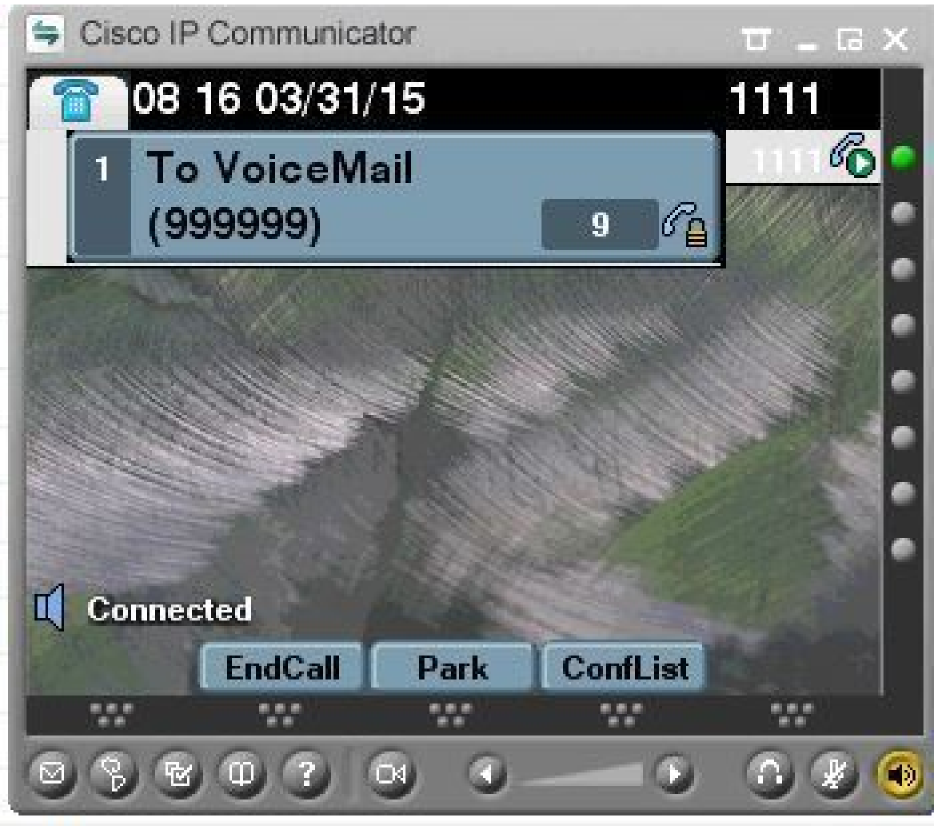
Alternatively, you can enable SIP OPTIONs keepalive to monitor the SIP trunk status. This option can be enabled in the SIP profile assigned to the SIP trunk. Once this is enabled you can monitor the Sip trunk status via Device > Trunk as shown below:



Name	Description	Calling Search Space	Device Pool	Route Pattern	Trunk Type	SIP Trunk Status	SIP Trunk Duration
CUCv11			Default	2000	SIP Trunk	Full Service	Time In Full Service: 0 day 0 hour 0 minute

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



Related Information

- SIP Integration Guide for Cisco Unity Connection Release 11.x