

Configure and Troubleshoot Secure Integration Between CUCM and CUC

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Diagram](#)

[Configure - Secure SIP Trunk](#)

[Configure CUC](#)

[1. Add SIP certificate](#)

[2. Create New Phone System or Modify Default One](#)

[3. Add a New Port Group](#)

[4. Edit Servers](#)

[5. Reset the Port Group](#)

[6. Add Voice Mail Ports](#)

[7. Download CUC Root Certificate](#)

[Configure CUCM](#)

[1. Configure SIP Trunk Security Profile for Trunk towards CUC](#)

[2. Configure SIP Profile](#)

[3. Create SIP trunk](#)

[4. Create a Route Pattern](#)

[5. Create a Voice Mail Pilot](#)

[6. Create Voice Mail Profile](#)

[7. Assign Voice Mail Profile to the DNs](#)

[8. Upload CUC Root Certificate as CallManager-trust](#)

[Configure Secure SCCP Ports](#)

[Configure CUC](#)

[1. Download the CUC Root Certificate](#)

[2. Create Phone System / Modify the One that Exists.](#)

[3. Add a New SCCP Port Group](#)

[4. Edit Servers](#)

[5. Add Secure SCCP ports](#)

[Configure CUCM](#)

[1. Add Ports](#)

[2. Upload CUC Root Certificate as CallManager-trust](#)

[3. Configure Message Waiting Information \(MWI\) On/Off Extensions](#)

[4. Create Voice Mail Pilot](#)

[5. Create Voice Mail Profile](#)

[6. Assign Voice Mail Profile to the DNs](#)

[7. Create a Voice Mail Hunt Group](#)

[Verify](#)

[SCCP Ports Verification](#)

[Secure SIP Trunk Verification](#)

[Secure RTP Call Verification](#)

[Troubleshoot](#)

[1. General Troubleshooting Tips](#)

[2. Traces to Collect](#)

[Common Issues](#)

[Case 1: Unable to Establish a Secure Connection \(Unknown CA Alert\)](#)

[Case 2: Unable to Download CTL File from CUCM TFTP](#)

[Case 3: Ports do not Register](#)

[Defects](#)

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

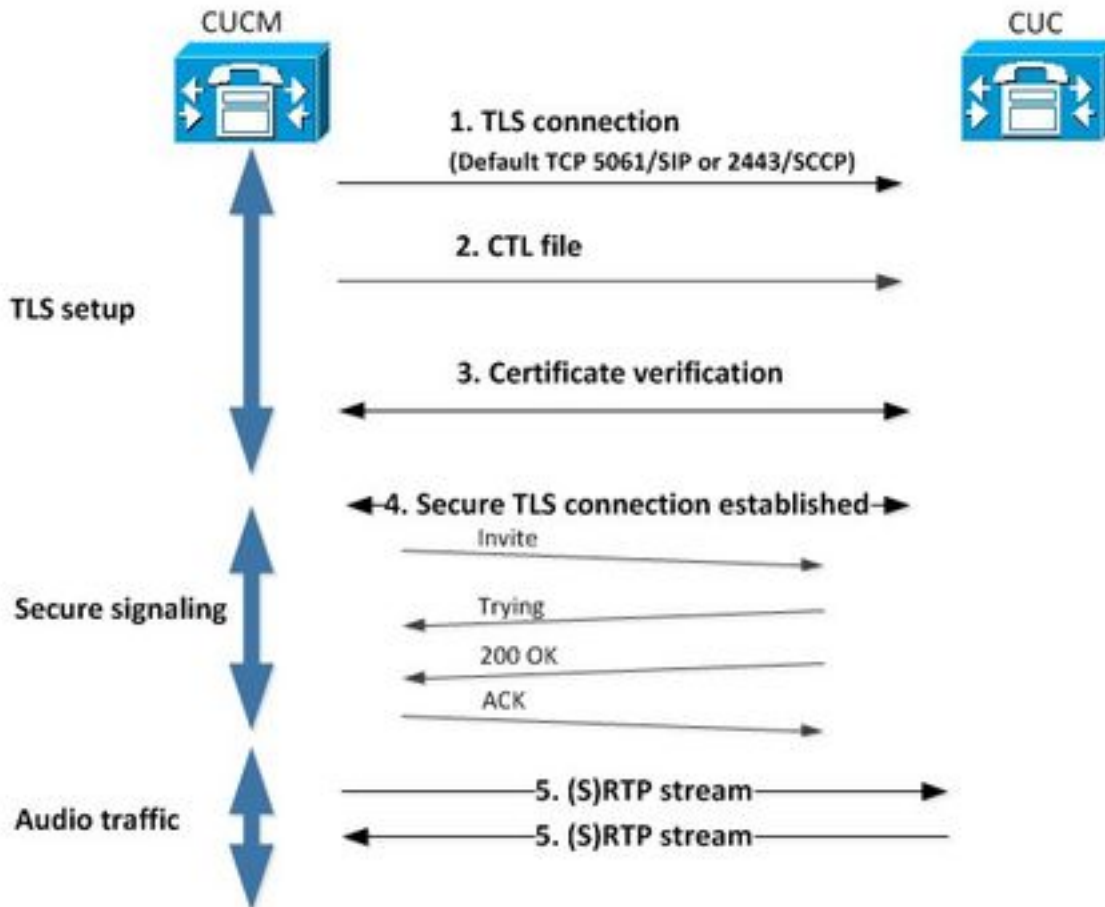
The information in this document is based on these software and hardware versions:

- 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 successful, 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 Group and 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.

New Port Group

Port Group Reset Help

New Port Group

Phone System

Create From Port Group Type Port Group

Port Group Description

Display Name*

Authenticate with SIP Server

Authentication Username

Authentication Password

Contact Line Name

SIP Security Profile

SIP Certificate

Security Mode

Secure RTP

Primary Server Settings

IPv4 Address or Host Name

IPv6 Address or Host Name

Port

4. Edit Servers

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

SIP Servers

| <input type="checkbox"/> | Order | IPv4 Address or Host Name |
|--------------------------|-------|---|
| <input type="checkbox"/> | 0 | 10.48.47.110 <input type="button" value="⌵"/> |

TFTP Servers

| <input type="checkbox"/> | Order | IPv4 Address or Host Name |
|--------------------------|-------|---------------------------|
| <input type="checkbox"/> | 0 | 10.48.47.110 |

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.

Port Group Basics (Secure SIP integration-1)

Port Group Edit Refresh Help

Status

The phone system cannot take calls if it has no ports. Use the Related Links to add ports.

One or more port groups need to be reset.

Port Group

Display Name*

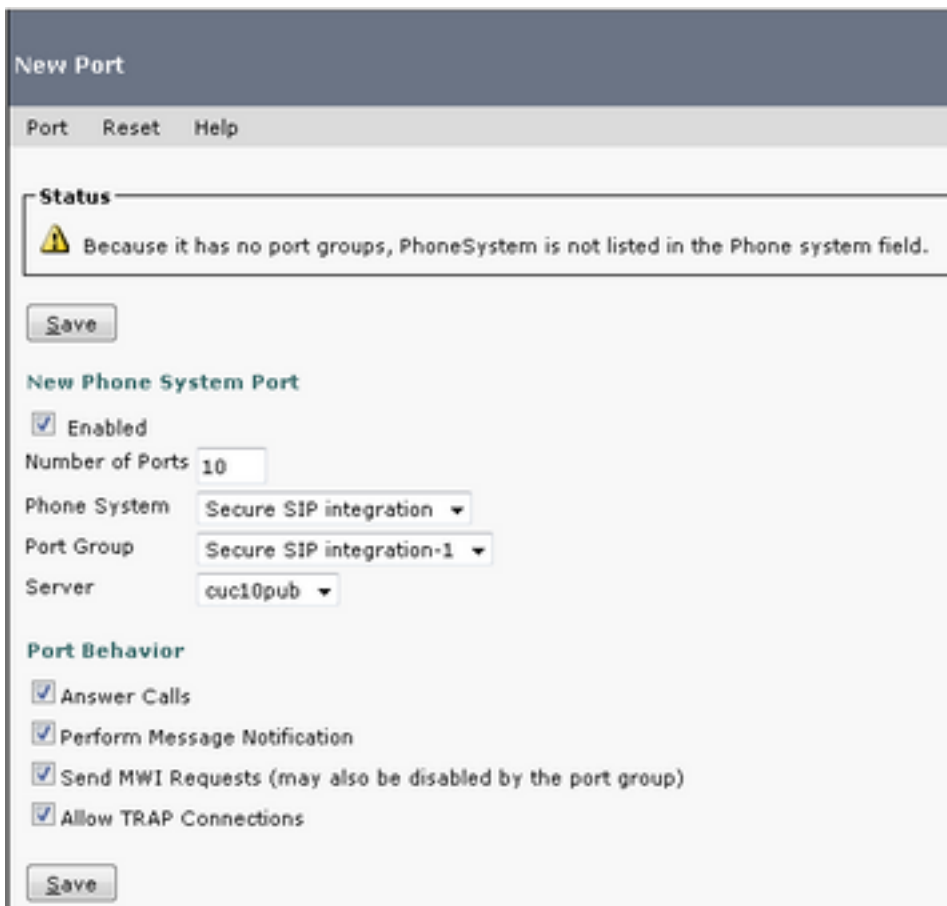
Integration Method

Reset Status

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).

The screenshot shows the configuration page for a SIP Trunk Security Profile. The title is "SIP Trunk Security Profile Information". The fields are as follows:

| | |
|---|----------------------------------|
| Name* | Secure_sip_trunk_profile_for_CUC |
| Description | |
| Device Security Mode | Encrypted |
| Incoming Transport Type* | TLS |
| Outgoing Transport Type | TLS |
| <input type="checkbox"/> Enable Digest Authentication | |
| Nonce Validity Time (mins)* | 600 |
| X.509 Subject Name | SecureConnection |
| Incoming Port* | 5061 |
| <input type="checkbox"/> Enable Application level authorization | |
| <input type="checkbox"/> Accept presence subscription | |
| <input checked="" type="checkbox"/> Accept out-of-dialog refer** | |
| <input checked="" type="checkbox"/> Accept unsolicited notification | |
| <input checked="" type="checkbox"/> Accept replaces header | |
| <input type="checkbox"/> Transmit security status | |
| <input type="checkbox"/> Allow charging header | |
| SIP V.150 Outbound SDP Offer Filtering* | Use Default Filter |

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.

| Trunk Information | |
|---------------------|---------------|
| Trunk Type* | SIP Trunk |
| Device Protocol* | SIP |
| Trunk Service Type* | None(Default) |

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**).

Trunk Configuration

Save

Status

Status: Ready

Device Information

| | |
|-----------------------------|---------------------------------------|
| Product: | SIP Trunk |
| Device Protocol: | SIP |
| Trunk Service Type | None(Default) |
| Device Name* | SecureSIPtoCUC |
| Description | Trunk for secure integration with CUC |
| Device Pool* | Default |
| Common Device Configuration | < None > |
| Call Classification* | Use System Default |
| Media Resource Group List | < None > |
| Location* | Hub_None |
| AAR Group | < None > |
| Tunneled Protocol* | None |
| QSIG Variant* | No Changes |
| ASN.1 ROSE OID Encoding* | No Changes |
| Packet Capture Mode* | None |
| Packet Capture Duration | 0 |

Media Termination Point Required
 Retry Video Call as Audio
 Path Replacement Support
 Transmit UTF-8 for Calling Party Name
 Transmit UTF-8 Names in QSIG APDU
 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 |

PSTN Access
 Run On All Active Unified CM Nodes

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

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

Inbound Calls

Significant Digits* All

Connected Line ID Presentation* Default

Connected Name Presentation* Default

Calling Search Space AllPhones

AAR Calling Search Space < None >

Prefix DN

Redirecting Diversion Header Delivery - Inbound

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

- Redirecting Diversion Header Delivery - Outbound: checked

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

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:

SIP Information

Destination

Destination Address is an SRV

| | Destination Address | Destination Address IPv6 | Destination Port |
|----|---------------------|--------------------------|------------------|
| 1* | 10.48.47.124 | | 5061 |

MTP Preferred Originating Codec* 711ulaw

BLF Presence Group* Standard Presence group

SIP Trunk Security Profile* Secure_sip_trunk_profile_for_CUC

Rerouting Calling Search Space < None >

Out-Of-Dialog Refer Calling Search Space < None >

SUBSCRIBE Calling Search Space < None >

SIP Profile* Standard SIP Profile [View Details](#)

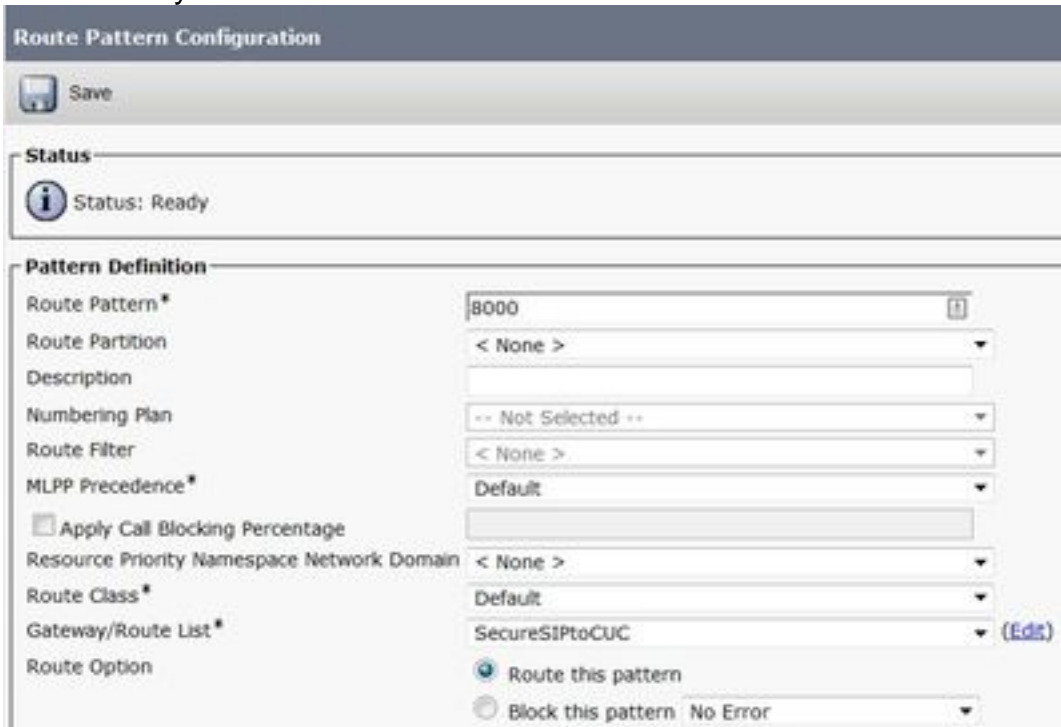
DTMF Signaling Method* No Preference

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:



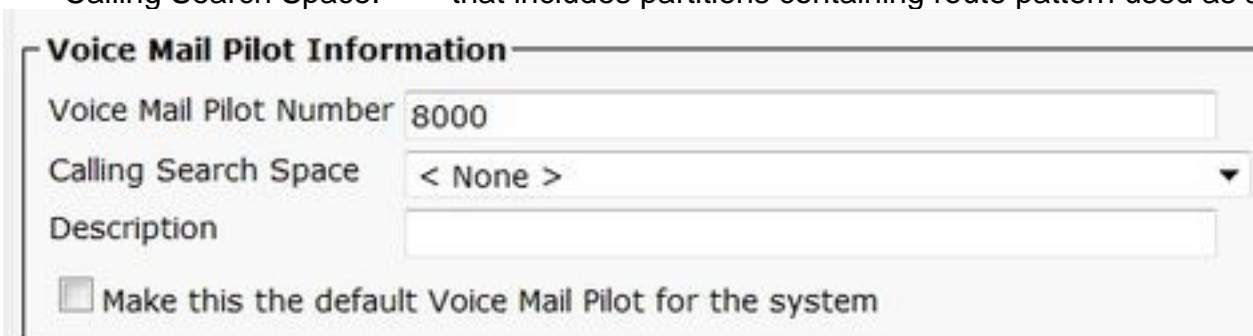
The screenshot shows the 'Route Pattern Configuration' window. At the top, there is a 'Save' button. Below it, the 'Status' section shows 'Status: Ready'. The main 'Pattern Definition' section contains the following fields:

| | |
|---|--|
| Route Pattern* | 8000 |
| Route Partition | < None > |
| Description | |
| Numbering Plan | -- Not Selected -- |
| Route Filter | < None > |
| MLPP Precedence* | Default |
| <input type="checkbox"/> Apply Call Blocking Percentage | |
| Resource Priority Namespace Network Domain | < None > |
| Route Class* | Default |
| Gateway/Route List* | SecureSIPtoCUC (Eds) |
| Route Option | <input checked="" type="radio"/> Route this pattern <input type="radio"/> Block this pattern No Error |

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>



The screenshot shows the 'Voice Mail Pilot Information' form with the following fields:

| | |
|--|----------|
| Voice Mail Pilot Number | 8000 |
| Calling Search Space | < None > |
| Description | |
| <input type="checkbox"/> Make this the default Voice Mail Pilot for the system | |

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:

Voice Mail Profile Information

Voice Mail Profile Name* Voicemail-profile-8000

Description Secure Voicemail

Voice Mail Pilot** 8000/< None >

Voice Mail Box Mask

Make this the default Voice Mail Profile for the System

7. Assign Voice Mail Profile to the DN's

Assign the voicemail profile to the DN's 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

Directory Number Configuration

Save Delete Reset Apply Config Add New

Directory Number Settings

Voice Mail Profile Secure_SIP_Integration (Choose <None> to use system default)

Calling Search Space < None >

BLF Presence Group* Standard Presence group

User Hold MOH Audio Source < None >

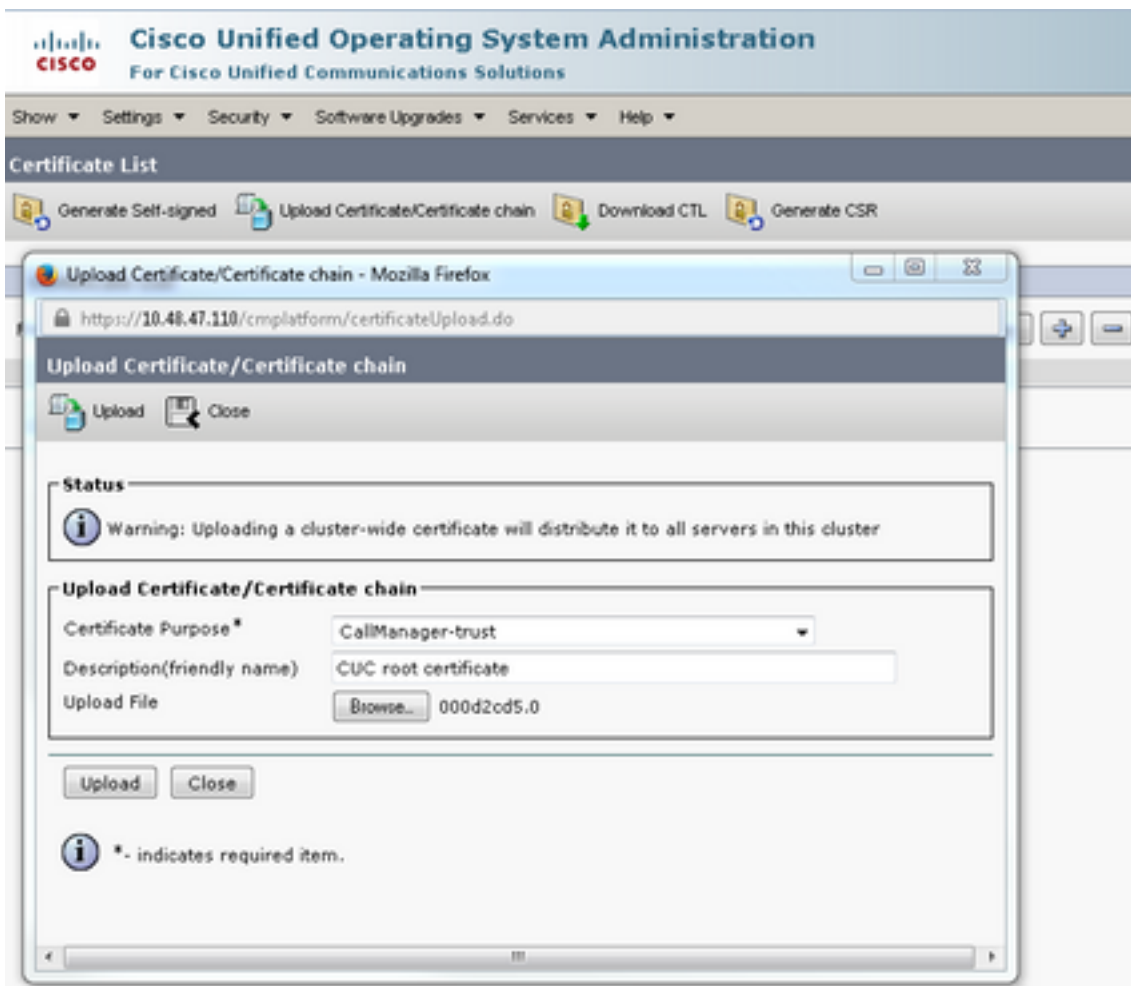
Network Hold MOH Audio Source < None >

Auto Answer* Auto Answer Off

Reject Anonymous Calls

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

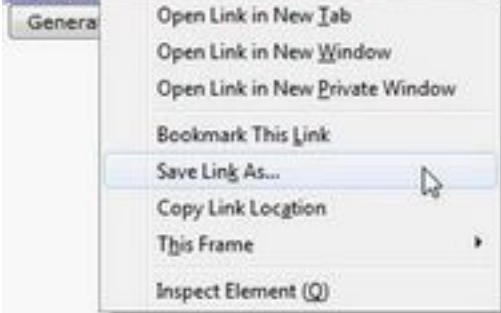
Configure CUC

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 **Save**:

| Root Certificate for Cisco Unified Communications Manager Authentication and Encryption | |
|---|---|
| Subject | CN=CiscoUnity-5dad32eb-cafa-4559-978f-56f2c6850d41 |
| Issuer | CN=CiscoUnity-5dad32eb-cafa-4559-978f-56f2c6850d41 |
| Valid From | Tue Mar 31 08:59:34 CEST 2015 |
| Valid Until | Fri Apr 01 08:59:34 CEST 2022 |
| Version | 2 |
| File Name | 57ed0e66.0 |
| Serial Number | f6b8fb3369144dd39f18e064893aec42 |
| Certificate Text | <pre>-----BEGIN CERTIFICATE----- MIICPDCCAaWgAwIBAgIRAPa++zNpFE3TnxjgZ1k67E1wDQYJKoZIhvcNAQEFBQAw OjE4MDYGA1UEAwwvQ2lzY29Vbml0eS01ZGFkMzJlYy1jYWZlLTQ1NTktOTc0Zj01 NmYyYzY4NTBkNDEwHhcNMTUwMzY2MDY1OTM0WWhcNMjIwNDAxMDY1OTM0WjA6MTgw NgYDVQQLDDB9DaxNjb1VuaXR5LTkYVWQzMmVlLWVhZmZmLWZmZmZmLWZmZmZmLWZmZmZm Njg1MGQ0MTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAoBOBg/qh8cWQx457 Q47eGUWcR2jeyE726RTO40GkdhDYI4Km6ouSeMiGbs757WpvtspKp+zeSDjVm2j4 B1lxG9wM3XgPPwM+3QIMh0NQLARuJdm9g2/5uiHB6/1k82Po0WvV2r6Anoragrv Md3ordaCB3mG1u2g0GqXj9GChf0CAwEAAANCMEEAwEgYDVR0TAQH/BAGwBgEB/wIB ADAdBgNVHQ4EFgQU438N5JYGHhgp7qm2dUmu+HGkM8wCwYDVR0PBAQDAgKsMA0G CSqGSIb3DQEBBQUAA4GBAGPhrFt6GH2a0iXV8bnKvC12f5ty1eTeMD6ZzD62P4C6 RtGM88WqGU1IAZw1www0nxdetKzZvJX2z2Ksu2ptVUnFPMZSc+xl0jv7vmJq52px TcD/Ti0efckXlc+vACWlu4wlv20SHxsoto9CiiXqsKQ7e/zyYHu152zTOQeYvAES -----END CERTIFICATE-----</pre> |
| Private Key | Hk2Pzp3YnX3/9ghz1r8v1VgMpSLr8HZ8XW/VXIL342IudK3G1GwnZ1IMvhztq/zEseh2ELON |

Right click to save the certificate as a file named 57ed0e66.0 (the file extension must be .0 rather than .htm)



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.

Phone System Basics (PhoneSystem)

Phone System Edit Refresh Help

Save Delete Previous Next

Status

The phone system cannot take calls until a port group is set. Use the Related Links to add a port group.

Phone System

Phone System Name* PhoneSystem

Default TRAP Phone System


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.

Status

 The phone system cannot take calls if it has no ports. Use the Related Links to add ports.

 Created Port Group(s)

Port Group

Display Name*

Integration Method

Device Name Prefix*

Reset Status

Message Waiting Indicator Settings

Enable Message Waiting Indicators

MWI On Extension

MWI Off Extension

Delay between Requests milliseconds

Maximum Concurrent Requests

Retries After Successful Attempt

Retry Interval After Successful Attempt milliseconds

Fields marked with an asterisk (*) are required.

4. Edit Servers

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

| SIP Servers | | |
|---|-------|---------------------------|
| <input type="button" value="Delete Selected"/> <input type="button" value="Add"/> | | |
| <input type="checkbox"/> | Order | IPv4 Address or Host Name |
| <input type="checkbox"/> | 0 | 10.48.47.110 |
| <input type="button" value="Delete Selected"/> <input type="button" value="Add"/> | | |
| TFTP Servers | | |
| <input type="button" value="Delete Selected"/> <input type="button" value="Add"/> | | |
| <input type="checkbox"/> | Order | IPv4 Address or Host Name |
| <input type="checkbox"/> | 0 | 10.48.47.110 |
| <input type="button" value="Delete Selected"/> <input type="button" value="Add"/> | | |


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**

Status

 Because it has no port groups, PhoneSystem is not listed in the Phone system field.

New Phone System Port

Enabled

Number of Ports

Phone System

Port Group

Server

Port Behavior

Answer Calls

Perform Message Notification

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

Allow TRAP Connections

Security Mode

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 selected.

Voice Mail Port Configuration

Save Delete Copy Reset Apply Config Add New

Status

Status: Ready

Device Information

Registration: Registered with Cisco Unified Communications Manager 10.48.46.182
 IPv4 Address: 10.48.46.184
 Device is trusted
 Port Name* CiscoUM1-VI1
 Description VM-sccp-secure-ports
 Device Pool* Default
 Common Device Configuration < None >
 Calling Search Space < None >
 AAR Calling Search Space < None >
 Location* Hub_None
 Device Security Mode* Encrypted Voice Mail Port
 Use Trusted Relay Point* Default
 Geolocation < None >

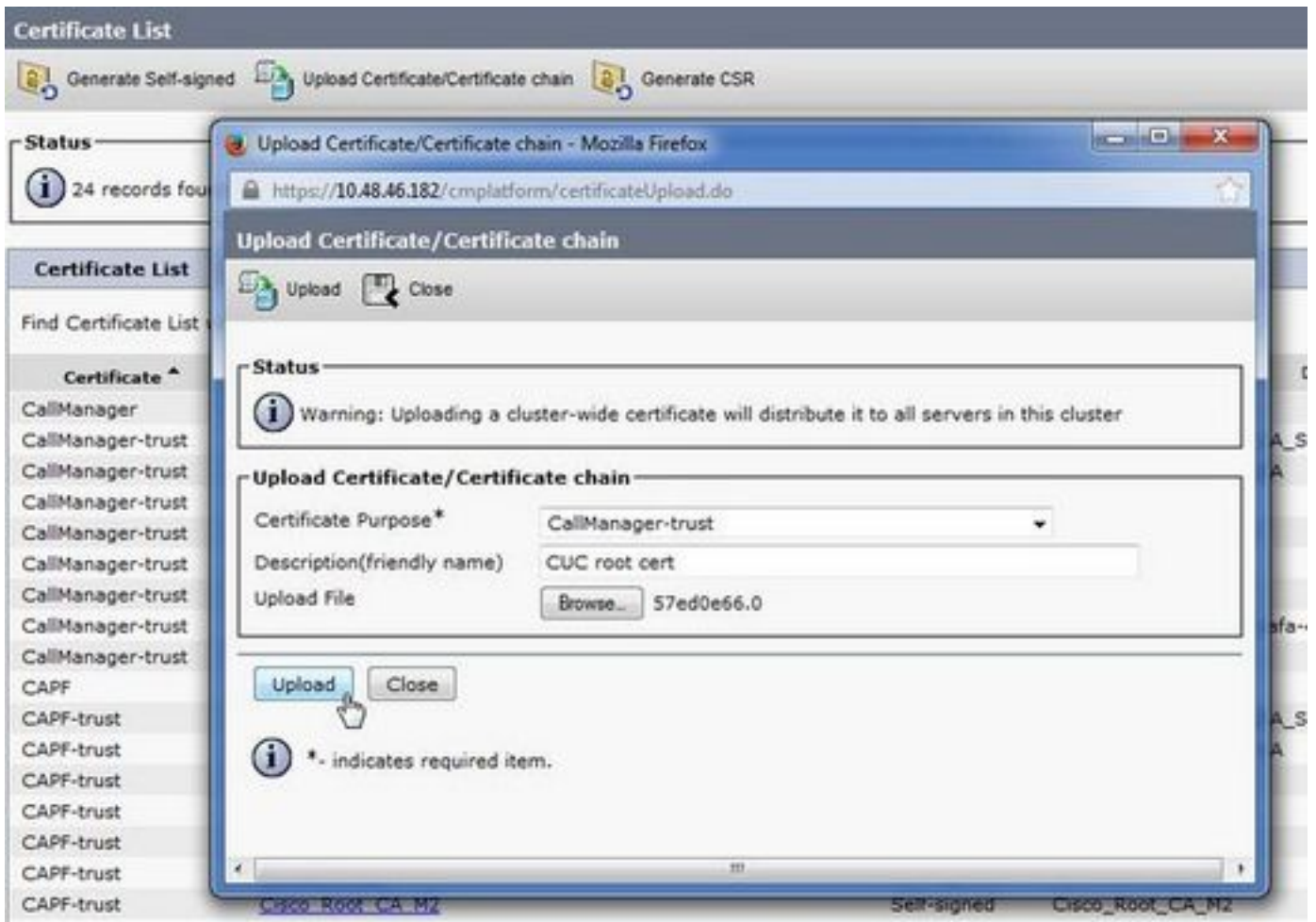
Directory Number Information

Directory Number* 999001
 Partition < None >
 Calling Search Space < None >
 AAR Group < None >
 Internal Caller ID Display VoiceMail
 Internal Caller ID Display (ASCII format) VoiceMail
 External Number Mask

Save Delete Copy Reset Apply Config Add New

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.

| Message Waiting Information | |
|-----------------------------|---|
| Message Waiting Number* | 999991 |
| Partition | < None > |
| Description | MWI on |
| Message Waiting Indicator* | <input checked="" type="radio"/> On <input type="radio"/> Off |
| Calling Search Space | < None > |

Message Waiting Information

Message Waiting Number* 999990

Partition < None >

Description MWI off

Message Waiting Indicator* On Off

Calling Search Space < None >

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>

Voice Mail Pilot Information

Voice Mail Pilot Number 8000

Calling Search Space < None >

Description

Make this the default Voice Mail Pilot for the system

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:

Voice Mail Profile Information

Voice Mail Profile Name* Voicemail-profile-8000

Description Secure Voicemail

Voice Mail Pilot** 8000/< None >

Voice Mail Box Mask

Make this the default Voice Mail Profile for the System

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

| Directory Number Settings | |
|---|--|
| Voice Mail Profile | Voicemail-profile-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 > |
| <input type="checkbox"/> Reject Anonymous Calls | |

7. Create a Voice Mail Hunt Group

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

| - Line Group Information | |
|--------------------------|-------------------|
| Line Group Name* | voicemail-lg |
| RNA Reversion Timeout* | 10 |
| Distribution Algorithm* | Longest Idle Time |

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

| Hunt List Information | |
|---|--------------|
| <input checked="" type="checkbox"/> Device is trusted | |
| Name* | voicemail-hl |
| Description | |
| Cisco Unified Communications Manager Group* | Default |
| <input checked="" type="checkbox"/> Enable this Hunt List (change effective on Save; no reset required) | |
| <input checked="" type="checkbox"/> For Voice Mail Usage | |

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

| Pattern Definition | |
|---------------------|--|
| Hunt Pilot* | 8000 |
| Route Partition | < None > |
| Description | |
| Numbering Plan | < None > |
| Route Filter | < None > |
| MLPP Precedence* | Default |
| Hunt List* | voicemail-hl (Edit) |
| Call Pickup Group | < None > |
| Alerting Name | |
| ASCII Alerting Name | |
| Route Option | <input checked="" type="radio"/> Route this pattern <input type="radio"/> Block this pattern No Error |

Verify

SCCP Ports Verification

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

| Device Name | Description | Device Pool | Device Security Mode | Calling Search Space | Extension | Partition | Status | SIP Address | Clear |
|-------------|---------------------|-------------|---------------------------|----------------------|-----------|-----------|------------------------------|--------------|-------|
| CM0025-101 | VM-ecp-secure-ports | Default | Encrypted Voice Mail Port | | 99901 | | Registered with 10.45.46.182 | 10.45.46.184 | |
| CM0025-102 | VM-ecp-secure-ports | Default | Encrypted Voice Mail Port | | 99902 | | Registered with 10.45.46.182 | 10.45.46.184 | |
| CM0025-103 | VM-ecp-secure-ports | Default | Encrypted Voice Mail Port | | 99903 | | Registered with 10.45.46.182 | 10.45.46.184 | |
| CM0025-104 | VM-ecp-secure-ports | Default | Encrypted Voice Mail Port | | 99904 | | Registered with 10.45.46.182 | 10.45.46.184 | |
| CM0025-105 | VM-ecp-secure-ports | Default | Encrypted Voice Mail Port | | 99905 | | Registered with 10.45.46.182 | 10.45.46.184 | |
| CM0025-106 | VM-ecp-secure-ports | Default | Encrypted Voice Mail Port | | 99906 | | Registered with 10.45.46.182 | 10.45.46.184 | |
| CM0025-107 | VM-ecp-secure-ports | Default | Encrypted Voice Mail Port | | 99907 | | Registered with 10.45.46.182 | 10.45.46.184 | |
| CM0025-108 | VM-ecp-secure-ports | Default | Encrypted Voice Mail Port | | 99908 | | Registered with 10.45.46.182 | 10.45.46.184 | |

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.

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.

| Name | Description | Calling Search Space | Device Pool | Route Pattern | Partition | Route Group | Priority | Trunk Type | SIP Trunk Status | SIP Trunk Duration |
|----------------|-------------|----------------------|-------------|---------------|-----------|-------------|----------|------------|------------------|---|
| SecureSIPtoCUC | | | Default | | | | | SIP Trunk | No Service | Time not 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.



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>

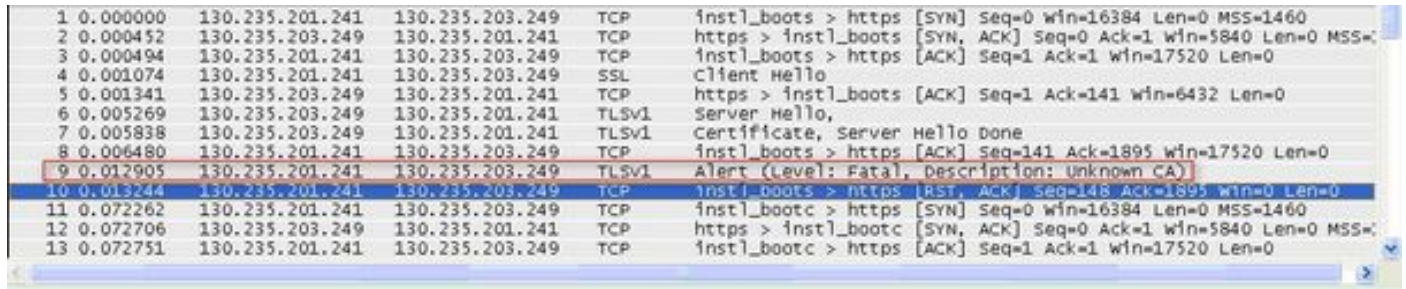
How to enable traces on CUC server:

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



| Time | Source IP | Destination IP | Protocol | Source Port | Destination Port | Details |
|-------------|-----------------|-----------------|----------|-------------|------------------|---|
| 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-xxxxxxxxxxxxx.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