

Beveiligde integratie tussen CUCM en CUC configureren en oplossen van problemen

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Diagram](#)

[Configureren - Secure SIP Trunk](#)

[CUC configureren](#)

[1. SIP-certificaat toevoegen](#)

[2. Maak een nieuw telefoonsysteem of wijzig standaard één](#)

[3. Voeg een nieuwe poortgroep toe](#)

[4. servers bewerken](#)

[5. Reset de poortgroep](#)

[6. Spraakmailpoorten toevoegen](#)

[7. CUC-basiscertificaat downloaden](#)

[CUCM configureren](#)

[1. SIP Trunk-beveiligingsprofiel voor Trunk naar CUC configureren](#)

[2. SIP-profiel configureren](#)

[3. SIP-romp maken](#)

[4. Een routepatroon maken](#)

[5. Een spraakpostbus maken](#)

[6. Spraakmailprofiel maken](#)

[7. Spraakmailprofiel aan de DNS's toewijzen](#)

[8. CUC-basiscertificaat uploaden als CallManager-trust](#)

[Secure SCCP-poorten configureren](#)

[CUC configureren](#)

[1. Download het CUC-wortelcertificaat](#)

[2. Maak een telefoonsysteem / wijzig het bestaande.](#)

[3. Voeg een nieuwe SCCP-poortgroep toe](#)

[4. servers bewerken](#)

[5. Voeg beveiligde SCCP-poorten toe](#)

[CUCM configureren](#)

[1. Poorten toevoegen](#)

[2. CUC-basiscertificaat uploaden als CallManager-trust](#)

[3. MWI-uitbreidingen \(Message Waiting Information\) op/uit](#)

[4. Spraakmailstuurprogramma maken](#)

[5. Spraakmailprofiel maken](#)

[6. Spraakmailprofiel aan de DNS's toewijzen](#)

[7. Maak een spraak-mailhunting-groep](#)

[Verifiëren](#)

[SCCP-poortverificatie](#)

[Secure SIP Trunk-verificatie](#)

[Secure RTP-gespreksverificatie](#)

[Problemen oplossen](#)

[1. Algemene tips voor probleemoplossing](#)

[2. Te verzamelen sporen](#)

[Veelvoorkomende problemen](#)

[Zaak 1: Kan geen beveiligde verbinding instellen \(onbekende CA-waarschuwing\)](#)

[Zaak 2: Kan CTL-bestand niet downloaden van CUCM TFTP](#)

[Zaak 3: Poorten niet registreren](#)

[Defecten](#)

Inleiding

Dit document beschrijft de configuratie, verificatie en probleemoplossing van de beveiligde verbinding tussen de Cisco Unified Communications Manager (CUCM)- en Cisco Unity Connection-server (CUC).

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben over CUCM.

Raadpleeg de [Cisco Unified Communications Manager security gids](#) voor meer informatie.

Opmerking: Deze moet op gemengde modus worden ingesteld om een veilige integratie te waarborgen.

Encryptie moet worden ingeschakeld voor Unity Connection 11.5(1) SU3 en hoger.

CLI-opdracht "utils cuc-encryptie <Enable/blocks>"

Gebruikte componenten

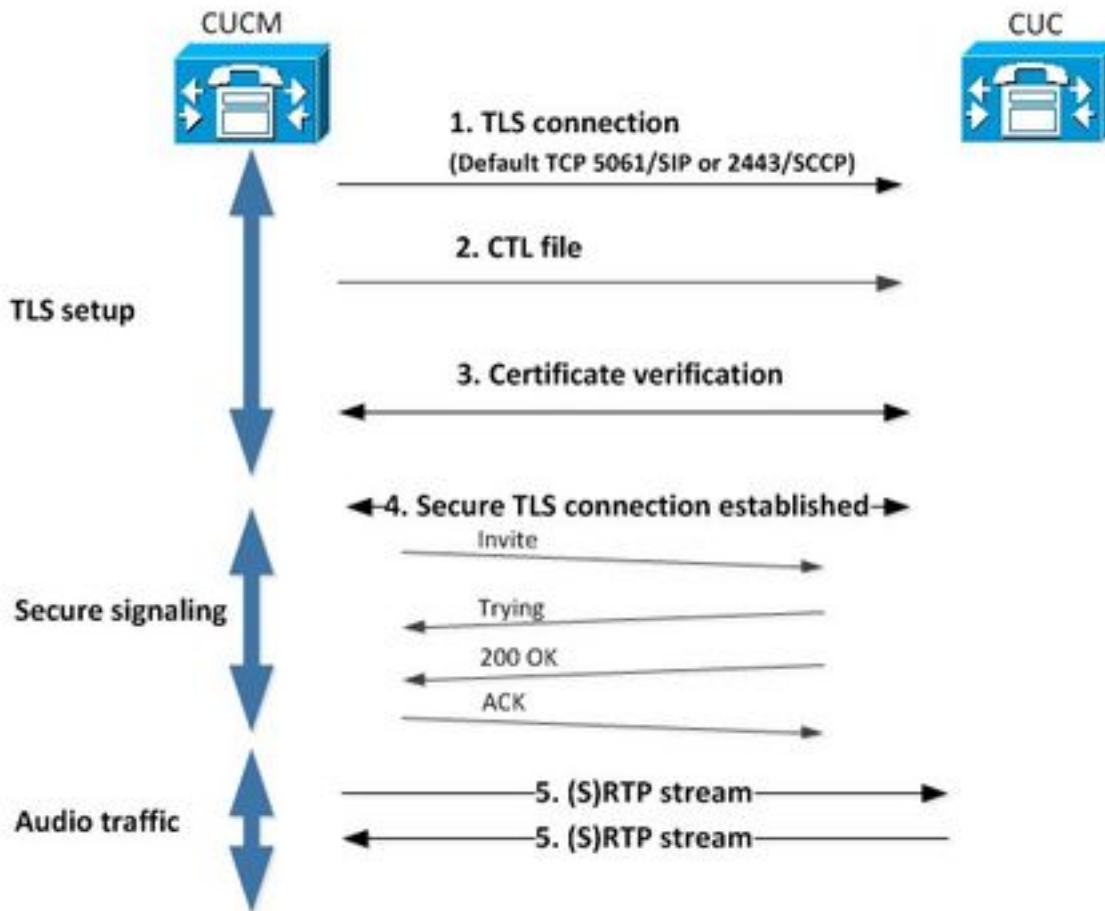
De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- CUCM versie 10.5.2.1900-3.
- CUC versie 10.5.2.1900-3.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Diagram

In dit diagram wordt kort het proces uitgelegd dat helpt een beveiligde verbinding tussen CUCM en CUC tot stand te brengen:



1. Call Manager stelt een beveiligde transportlaag security (TLS) verbinding naar CUC-server in op poort 2443 Sony Call Control Protocol (SCCP) of 5061 Session Initiation Protocol (SIP) op basis van het protocol dat voor integratie is gebruikt.

2. CUC-server downloads het CTL-bestand (certificaatlijst) van TFTP-server (één keer proces), haalt het CallManager.pem-certificaat uit en slaat het op.

3. De CUCM-server biedt het CallManager.pem-certificaat aan, dat wordt geverifieerd aan de hand van het CallManager.pem-certificaat dat in de vorige stap is verkregen. Bovendien wordt het CUC-certificaat gecontroleerd aan de hand van een CUC-wortelcertificaat dat in CUCM is opgeslagen. Merk op dat het basiscertificaat door de beheerder in CUCM moet worden geüpload.

4. Indien de verificatie van de certificaten succesvol is, wordt een beveiligde TLS-verbinding tot stand gebracht. Deze verbinding wordt gebruikt om gecodeerde SCCP of SIP-signaling uit te wisselen.

5. Audio-verkeer kan worden uitgewisseld via Real-time Transport Protocol (RTP) of SRTP.

Opmerking: Wanneer u een TLS-communicatie instelt, gebruiken CUCM en CUC TLS wederzijdse authenticatie. Raadpleeg RFC5630 voor meer informatie.

Configureren - Secure SIP Trunk

CUC configureren

1. SIP-certificaat toevoegen

Navigeren in naar **CUC-beheer > TelePresence-integraties > Security > SIP-certificaat > Toevoegen nieuwe software**

- Naam weergeven: <elke betekenisvolle naam>
- Naam van het onderwerp: <een naam, bijvoorbeeld, **SecureConnection**>

Opmerking: de Onderwerp Naam moet overeenkomen met de X.509 Onderwerp Naam in het veiligheidsprofiel van de RFstam in SIP (gevormd in stap 1 van de configuratie van CUCM later in dit document).

Opmerking: Het certificaat wordt gegenereerd en ondertekend door het CUC root certificaat.

2. Maak een nieuw telefoonsysteem of wijzig standaard één

Navigeer naar **telefonie integratie > telefoonsysteem**. U kunt het telefoonsysteem gebruiken dat al bestaat of een nieuw systeem maken.

3. Voeg een nieuwe poortgroep toe

Selecteer in de pagina Telefoonsysteem basisinformatie in het vervolgkeuzevenster Verwante links de optie Port Groepering toevoegen en selecteer Ga. Voer in het configuratievenster deze

informatie in:

- Telefoonsysteem:
- Van: SIP voor poortgroepen
- SIP-beveiligingsprofiel: 5061/TLS
- SIP-certificaat:
- Beveiliging: Versleuteld
- Secure RTP: gecontroleerd
- IPv4-adres of hostnaam:

Hit Save.

New Port Group

Port Group Reset Help

Save

New Port Group

Phone System Secure SIP integration ▾

Create From Port Group Type SIP ▾
 Port Group ▾

Port Group Description

Display Name* Secure SIP integration-1

Authenticate with SIP Server

Authentication Username

Authentication Password

Contact Line Name

SIP Security Profile 5061/TLS ▾

SIP Certificate Secure SIP integration with CUCMv10.5.2 ▾

Security Mode Encrypted ▾

Secure RTP

Primary Server Settings

IPv4 Address or Host Name 10.48.47.110

IPv6 Address or Host Name

Port 5060

Save

4. servers bewerken

Navigeer om > **servers** te **bewerken** en TFTP server toe te voegen uit de CUCM cluster zoals in deze afbeelding weergegeven.

The image shows two screenshots of a configuration interface. The top screenshot is titled "SIP Servers" and contains a table with one row. The table has columns for "Order" (value: 0) and "IPv4 Address or Host Name" (value: 10.48.47.110). Below the table are "Delete Selected" and "Add" buttons. The bottom screenshot is titled "TFTP Servers" and contains a table with one row. The table has columns for "Order" (value: 0) and "IPv4 Address or Host Name" (value: 10.48.47.110). Below the table are "Delete Selected" and "Add" buttons.

Opmerking: Het is belangrijk om het juiste TFTP-adres te geven. CUC server downloads het CTL bestand uit dit TFTP zoals uitgelegd.

5. Reset de poortgroep

Ga terug naar **Port Group Basics** en stel poortgroep opnieuw in zoals gevraagd door het systeem zoals in deze afbeelding.

The image shows a screenshot of the "Port Group Basics (Secure SIP integration-1)" configuration page. At the top, there are tabs for "Port Group", "Edit", "Refresh", and "Help". Below the tabs are "Save", "Delete", "Previous", and "Next" buttons. A "Status" section contains two warning icons with the following text: "The phone system cannot take calls if it has no ports. Use the Related Links to add ports." and "One or more port groups need to be reset." Below the status section, the "Port Group" configuration is shown with a "Display Name*" field containing "Secure SIP integration-1", an "Integration Method" dropdown set to "SIP", and a "Reset Status" field set to "Reset Required" with a "Reset" button.

6. Spraakmailpoorten toevoegen

Selecteer in de pagina Port Group Basics, in het vervolgkeuzevenster Verwante links, de optie **Add Port** en selecteer **Go**. Typ deze informatie in het configuratievenster:

- Ingeschakeld: gecontroleerd
- Aantal poorten:

- Telefoonsysteem:
- Poortgroep:
- Server:
- Poortgedrag:

7. CUC-basiscertificaat downloaden

Navigeer naar **Telefonieintegraties > Beveiliging > Opstartcertificaat**, klik met de rechtermuisknop op de URL om het certificaat op te slaan als een bestand met de naam <filename>.0 (de bestandsextensie moet .0 in plaats van .htm)' en druk op Opslaan zoals in deze afbeelding wordt weergegeven.



CUCM configureren

1. SIP Trunk-beveiligingsprofiel voor Trunk naar CUC configureren

Navigeren in naar **CUCM-beheer > Systeem > Security > SIP Trunk-beveiligingsprofiel > Nieuwe toevoegen**

Zorg ervoor dat deze velden goed ingevuld zijn:

- Apparaatbeveiligingsmodus: Versleuteld
- X.509 Onderwerp Naam: Secure-verbinding>
- Uitgebreid dialoogvenster accepteren: gecontroleerd
- Ongevraagde kennisgeving aanvaarden: gecontroleerd
- Accept vervangt kop: gecontroleerd

Opmerking: X.509 Onderwerp Naam moet overeenkomen met het veld Naam onderwerp in het SIP-certificaat op de Cisco Unity Connection-server (geconfigureerd in stap 1 van de CUC-configuratie).

The screenshot shows the 'SIP Trunk Security Profile Information' configuration page. 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. SIP-profiel configureren

Navigeer naar **Apparaat > Apparaatinstellingen > SIP Profile** als u bepaalde instellingen moet toepassen. Anders kunt u gebruikmaken van het standaard SIP-profiel.

3. SIP-romp maken

Ga naar **apparaat > Trunk > Nieuwe gereedschappen toevoegen**. Maak een SIP-romp die gebruikt zal worden voor beveiligde integratie met Unity Connection zoals in deze afbeelding.

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

Voer in het gedeelte Apparaatinformatie van de hoofdconfiguratie deze informatie in:

- Apparaatnaam:
- Apparaatpool:
- SRTP toegestaan: gecontroleerd

Opmerking: Zorg ervoor dat de CallManager-groep (in de configuratie van het apparaat) alle servers in CUC bevat (**poortgroep > Bewerken > 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
<input type="checkbox"/> Media Termination Point Required	
<input checked="" type="checkbox"/> Retry Video Call as Audio	
<input type="checkbox"/> Path Replacement Support	
<input type="checkbox"/> Transmit UTF-8 for Calling Party Name	
<input type="checkbox"/> Transmit UTF-8 Names in QSIG APDU	
<input type="checkbox"/> Unattended Port	
<input checked="" type="checkbox"/> 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
<input type="checkbox"/> PSTN Access	
<input type="checkbox"/> Run On All Active Unified CM Nodes	

Voer in het gedeelte Inbound van de hoofdconfiguratie deze informatie in:

- Zoekruimte bellen:
- Levering van afleidingsheader - inkomende: gecontroleerd

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 de buurt De sectie van de boomstam van configuratie, ingaat deze informatie:

- Levering via omleidingsheader - Uitvoer: gecontroleerd

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

Voer in het gedeelte Informatie over SIP van de boomconfiguratie deze informatie in:

- Bestemmingsadres:
- SIP Trunk-beveiligingsprofiel:
- Rerouting van de zoekruimte:
- Uitgebreid overzicht raadt het bellen van zoekruimte aan:
- SIP-profiel:

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

Pas andere instellingen aan volgens uw vereisten.

4. Een routepatroon maken

Maak een routepatroon dat naar de geconfigureerde stam wijst (**Oproeroutering > Route/Hunt > Routepatroon**). Uitbreiding ingevoerd als een routepatroonnummer kan worden gebruikt als voicemail-piloot. Voer deze informatie in:

- Routepatroon:
- Gateway/route-lijst:

The screenshot shows the 'Route Pattern Configuration' window. At the top, there is a 'Save' button. Below it, the 'Status' is 'Ready'. The '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. Een spraakpostbus maken

Maak een voicemail-piloot voor de integratie (**geavanceerde functies > Voice Mail > Voice Mail-Pilot**). Voer deze waarden in:

- Spraakcontrolenummer:
- Zoekruimte bellen: die onderdelen bevatten die routepatroon bevatten dat als piloot wordt gebruikt>

The screenshot shows the 'Voice Mail Pilot Information' window. It contains 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. Spraakmailprofiel maken

Maak een voicemailprofiel om alle instellingen samen te voegen (**geavanceerde functies > Voice Mail > Voice Mail Profile**). Geef de volgende informatie op:

- Spraakmailpilot:
- Bericht per e-mail:

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. Spraakmailprofiel aan de DNS's toewijzen

Pas het voicemailprofiel aan de DNA's toe, bedoeld om een veilige integratie te gebruiken. Vergeet niet om op de knop "Config toepassen" te klikken na het wijzigen van de DNS-instellingen:

Navigeren in: **Oproeroutering > Directory-nummer** en wijziging van het volgende:

- Spraakprofiel: Secure_SIP_integratie

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 >

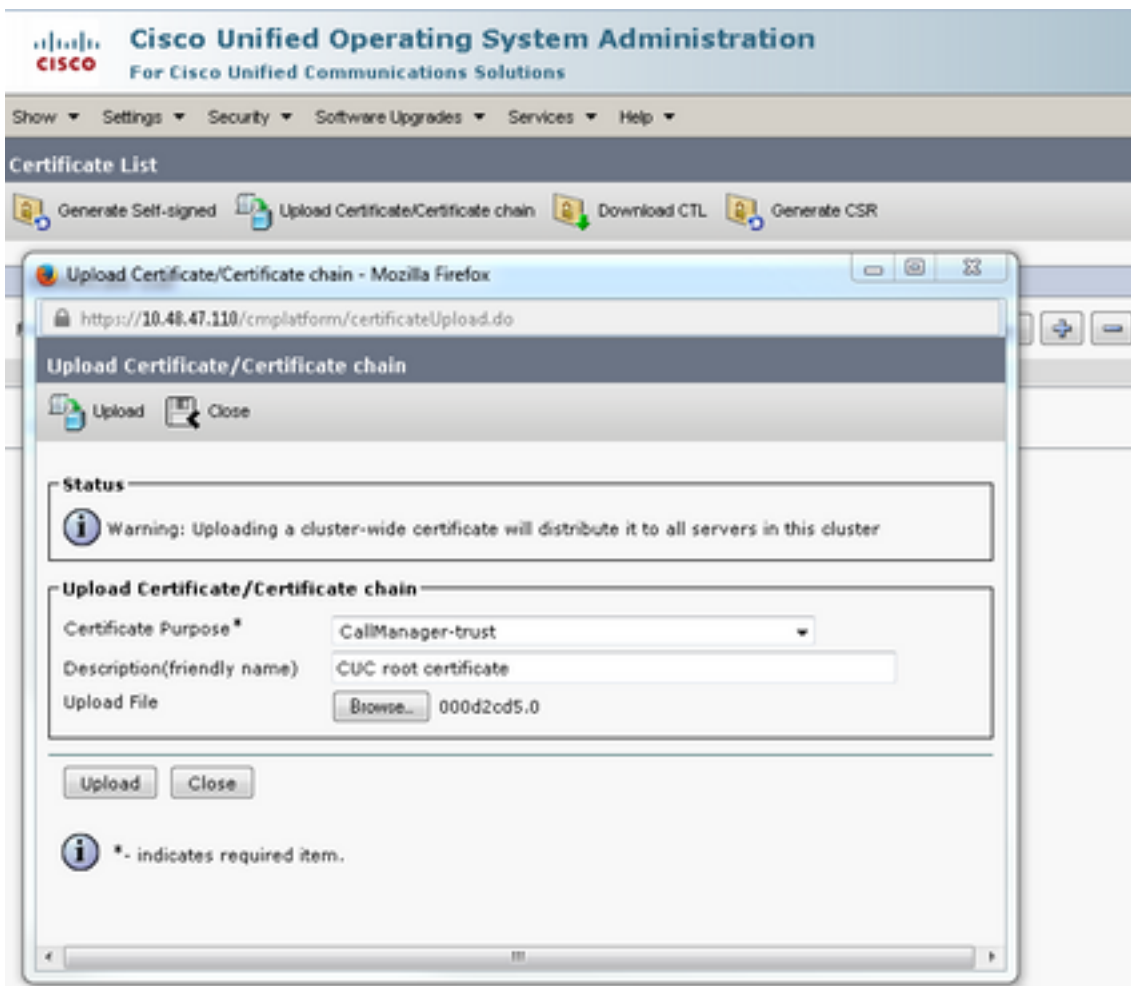
Network Hold MOH Audio Source < None >

Auto Answer* Auto Answer Off

Reject Anonymous Calls

8. CUC-basiscertificaat uploaden als CallManager-trust

Navigeer naar **OS-beheer > Beveiliging > certificaatbeheer > Upload certificaatketen** en uploaden het CUC-basiscertificaat als **CallManager-trust** op alle knooppunten die zijn geconfigureerd voor communicatie met CUC-server.



Opmerking: de service van Cisco CallManager moet opnieuw worden gestart nadat het certificaat is geüpload om het certificaat in werking te kunnen stellen.

Secure SCCP-poorten configureren

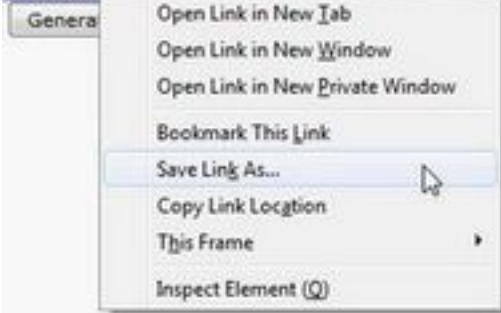
CUC configureren

1. Download het CUC-wortelcertificaat

Navigeer naar **CUC-beheer > Telephony-integratie > Security > Root-certificaat**. Klik met de rechtermuisknop op de URL om het certificaat op te slaan als een bestand met de naam <bestandsnaam>.0 (de bestandsextensie moet .0 in plaats van .htm)' en druk op **Opslaan**:

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 NmYyYzY4NTBkNDEwHhcNMTUwMzY1OTM0WWhcNMjEwNDAxMDY1OTM0WjA6MTgw NgYDVQDDC9DaxNjb1VuaXR5LTkYwQzMmVilWNhZmEtNDU1OS05NzhmLTU2ZjJj Njg1MGQ0MTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAoBObg/qh8cWQx457 Q47eGUWcR2jeyE726RTO40GkdhDYI4Km6ouSeMiGbs757WpvTspKp+zeSDjVm2j4 B1lxG9wM3XgPPwM+3QIMh0NQPLARuJdm9g2/5uiHB6/1k82Po0Wrv2r6Anoragrv Md3ordaCB3mG1u2g0GqXj9GChf0CAwEAANCMEEAwEgYDVR0TAQH/BAgwBgEB/wIB ADAdBgNVHQ4EFgQU438N5JYGHhgp7qm2dUmu+HGkM8wCwYDVR0PBAQDAGKsMA0G CSqGSIb3DQEBBQUAA4GBAGPhrFt6GH2a0iXV8bnKvC12f5ty1eTeMD6ZzD62P4C6 RtGM88WqGU1IAZw1www0nxdetKzZvJX2z2Ksu2ptVUnFPMzSc+xloJv7vmJq52px 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. Maak een telefoonsysteem / wijzig het bestaande.

Navigeer naar **telefonie integratie > Phone-system**. U kunt het telefoonsysteem gebruiken dat al bestaat of een nieuw systeem maken.

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*

Default TRAP Phone System


3. Voeg een nieuwe SCCP-poortgroep toe


Selecteer in de pagina Basisbeginselen van het telefoonsysteem in het vervolgkeuzevenster **Verwante links** de optie **Poortgroep toevoegen** en selecteer **Ga**. Voer in het configuratievenster deze informatie in:

- Telefoonsysteem:
- Poortgroep type: SCCP
- voorvoegsel apparaatnaam*: Cisco UM1-VI
- MWI Bij uitbreiding:
- Uitbreiding MWI uit:

Opmerking: Deze configuratie moet overeenkomen met de configuratie op 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. servers bewerken

Navigeer om > servers uit te werken en TFTP server toe te voegen uit de 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"/>		


Opmerking: Het is belangrijk om het juiste TFTP-adres te geven. CUC server downloads het CTL bestand uit dit TFTP zoals uitgelegd.

5. Voeg beveiligde SCCP-poorten toe

Selecteer in de pagina Basisbeginselen van de poortgroep, in het vervolgkeuzevenster Verwante Links de optie **Ports toevoegen** en selecteer **Ga**. Voer in het configuratievenster deze informatie in:

- Ingeschakeld: gecontroleerd
- Aantal poorten:
- Telefoonsysteem:
- Poortgroep:
- Server:
- Poortgedrag:
- Beveiliging: **Versleuteld**

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

CUCM configureren

1. Poorten toevoegen

Navigeren in om **CUCM-beheer > Geavanceerde functies > Configuratie van spraak-mail-poorten > Nieuw toevoegen.**

Configureer de spraakpoorten van de SCCP zoals gebruikelijk. Het enige verschil is in de Apparaatbeveiligingsmodus onder de poortconfiguratie waarin de optie Versleuteld Voice Mailpoort moet worden geselecteerd.

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 >

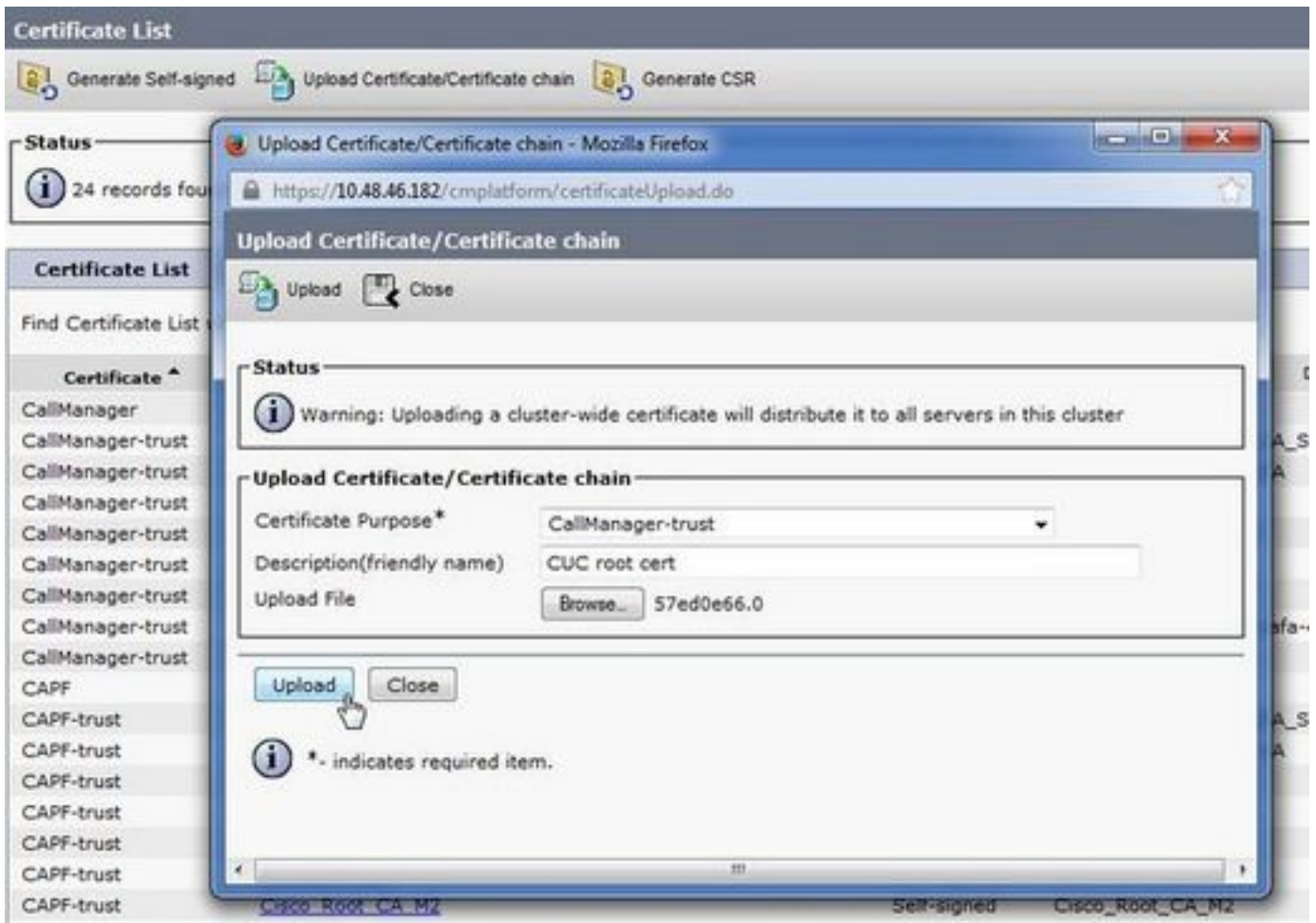
Directory Number Information

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. CUC-basiscertificaat uploaden als CallManager-trust

Navigeer naar **OS-beheer > Beveiligingsbeheer > certificaatbeheer > Upload certificaatketen** en uploaden het CUC-basiscertificaat als **CallManager-trust** op alle knooppunten die zijn geconfigureerd voor communicatie met de CUC-server.



Opmerking: de service van Cisco CallManager moet opnieuw worden gestart nadat het certificaat is geüpload om het certificaat in werking te kunnen stellen.

3. MWI-uitbreidingen (Message Waiting Information) op/uit

Navigeer naar CUCM-beheer > Geavanceerde functies > Spraakpoortconfiguratie en stel MWI-aan/uit-uitbreidingen in. De MWI-nummers moeten overeenkomen met de CUC-configuratie.

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 >

Save

Message Waiting Information

Message Waiting Number* 999990

Partition < None >

Description MWI off

Message Waiting Indicator* On Off

Calling Search Space < None >

Save

4. Spraakmailbijlage maken

Maak een voicemail-piloot voor de integratie (**geavanceerde functies > Voice Mail > Voice Mail-Pilot**). Voer deze waarden in:

- Spraakcontrolenummer:
- Zoekruimte bellen: die onderdelen bevatten die routepatroon bevatten dat als piloot wordt gebruikt>

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. Spraakmailprofiel maken

Maak een voicemailprofiel om alle instellingen samen te voegen (**geavanceerde functies > Voice Mail > Voice Mail Profile**). Voer deze informatie in:

- Spraakmailpiloot:
- Bericht per e-mail:

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. Spraakmailprofiel aan de DNS's toewijzen

Pas het voicemailprofiel toe aan de DNA's die van plan zijn een veilige integratie te gebruiken. Klik op de knop **Config** nadat de DNS-instellingen zijn gewijzigd:

Navigeren in op **Oproeroutering > Directory number** en wijzigen in:

- **Spraakprofiel: Spraak-profiel-8000**

Directory Number Settings

Voice Mail Profile	<input type="text" value="Voicemail-profile-8000"/>	(Choose <None> to use system default)
Calling Search Space	<input type="text" value="< None >"/>	
BLF Presence Group*	<input type="text" value="Standard Presence group"/>	
User Hold MOH Audio Source	<input type="text" value="< None >"/>	
Network Hold MOH Audio Source	<input type="text" value="< None >"/>	

Reject Anonymous Calls

7. Een hunting-groep voor Voice Mail maken

a) Voeg een nieuwe groep van de Lijn toe (Oproeroutering > Route/Hunt > Lijngroep)

Line Group Information

Line Group Name*	<input type="text" value="voicemail-lg"/>
RNA Reversion Timeout*	<input type="text" value="10"/>
Distribution Algorithm*	<input type="text" value="Longest Idle Time"/>

b) Voeg een nieuwe lijst van de hunting voor spraak-mail toe (Oproeroutering > Route/Tunt > Taaklijst)

Hunt List Information

Device is trusted

Name*	<input type="text" value="voicemail-hl"/>
Description	<input type="text"/>
Cisco Unified Communications Manager Group*	<input type="text" value="Default"/>

Enable this Hunt List (change effective on Save; no reset required)

For Voice Mail Usage

c) Voeg een nieuwe Tunt piloot toe (Oproeroutering > Route/Hunt > Taakpijp)

Pattern Definition

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

Verifiëren

SCCP-poortverificatie

Navigeer naar **CUCM-beheer > Voorspelfuncties > Voice Mail > Voice Mail-poorten** en controleer de poortregistratie.

Device Name	Description	Device Pool	Device Security Mode	Calling Search Space	Extension	Partition	Status	IP Address	Clear
CiscoRS-102	VM-ecp-secure-ports	Default	Encrypted Voice Mail Port		999001		Registered with 10.45.46.182	10.45.46.184	
CiscoRS-103	VM-ecp-secure-ports	Default	Encrypted Voice Mail Port		999002		Registered with 10.45.46.182	10.45.46.184	
CiscoRS-104	VM-ecp-secure-ports	Default	Encrypted Voice Mail Port		999003		Registered with 10.45.46.182	10.45.46.184	
CiscoRS-105	VM-ecp-secure-ports	Default	Encrypted Voice Mail Port		999004		Registered with 10.45.46.182	10.45.46.184	
CiscoRS-106	VM-ecp-secure-ports	Default	Encrypted Voice Mail Port		999005		Registered with 10.45.46.182	10.45.46.184	
CiscoRS-107	VM-ecp-secure-ports	Default	Encrypted Voice Mail Port		999006		Registered with 10.45.46.182	10.45.46.184	
CiscoRS-108	VM-ecp-secure-ports	Default	Encrypted Voice Mail Port		999007		Registered with 10.45.46.182	10.45.46.184	
CiscoRS-109	VM-ecp-secure-ports	Default	Encrypted Voice Mail Port		999008		Registered with 10.45.46.182	10.45.46.184	

Druk op de knop **Voice Mail** op de telefoon om spraakmail te bellen. U dient de openingsgroet te horen als de extensie van de gebruiker niet is ingesteld op het Unity Connection-systeem.

Secure SIP Trunk-verificatie

Druk op de knop **Voice Mail** op de telefoon om spraakmail te bellen. U dient de openingsgroet te horen als de gebruikersuitbreiding niet is ingesteld op het Unity Connection-systeem.

In plaats hiervan kunt u ook SIP OPTION's in stand houden om de SIP-boomstamstatus te controleren. Deze optie kan in het SIP-profiel worden ingeschakeld dat aan de SIP-stam is toegewezen. Als deze optie is ingeschakeld, kunt u de status van de Sip-romp bewaken via **Apparaat > Trunk** zoals in deze afbeelding wordt weergegeven.

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-gespreksverificatie

Controleer of het pictogram van het hangslot aanwezig is op oproepen naar Unity Connection. Het betekent dat de RTP-stream versleuteld is (het profiel voor apparaatbeveiliging moet beveiligd zijn om het te laten werken) zoals in deze afbeelding.



Problemen oplossen

1. Algemene tips voor probleemoplossing

Volg deze stappen om een oplossing voor de beveiligde integratie te vinden:

- Controleer de configuratie.
- Zorg ervoor dat alle verwante services actief zijn. (CUCM - CallManager, TFTP, CUC - Conversation Manager)
- Zorg ervoor dat poorten die vereist zijn voor beveiligde communicatie tussen servers, geopend zijn in het netwerk (TCP poort 2443 voor SCCP-integratie en TCP 5061 voor SIP-integratie).
- Als dit allemaal juist is, moet u de sporen verzamelen.

2. Te verzamelen sporen

Verzamel deze sporen om de veilige integratie te verhelpen.

- PacketCapture van CUCM en CUC
- CallManager-sporen
- Cisco Conversation Manager-sporen

Raadpleeg deze bronnen voor aanvullende informatie over:

Hoe voert u een pakketvastlegging op CUCM uit:

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

Hoe kunt u sporen op CUC-server inschakelen:

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

Veelvoorkomende problemen

Zaak 1: Kan geen beveiligde verbinding instellen (onbekende CA-waarschuwing)

Nadat de pakketvastlegging van een van de servers is verzameld, wordt de TLS-sessie ingesteld.

```
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
```

De client gaf een waarschuwing met een fatale fout van Onbekende CA aan de server, alleen omdat de client het certificaat niet kon controleren dat door de server werd verzonden.

Er zijn twee mogelijkheden:

1) CUCM stuurt de waarschuwing Onbekende CA

- Controleer dat het huidige CUC root certificaat wordt geüpload op de server die communiceert met de CUC server.
- Zorg ervoor dat de CallManager-service opnieuw op de betreffende server is gestart.

2) CUC verstuurt de waarschuwing Onbekende CA

- Controleer dat het TFTP IP-adres correct is ingevoerd in de **Port Group > Bewerken > configuratie van servers** op de CUC-server.
- Controleer dat de CUCM TFTP-server bereikbaar is vanaf de verbindingsserver.
- Zorg ervoor dat het CTL-bestand op CUCM TFTP actueel is (vergelijk uitvoer van "show ctl" met certificaten zoals gezien op OS Admin-pagina). Draai de CTLClient opnieuw als dit niet het geval is.
- Start de CUC server opnieuw of verwijder en ontwerp de poortgroep opnieuw om het CTL-bestand opnieuw te downloaden van CUCM TFTP.

Zaak 2: Kan CTL-bestand niet downloaden van CUCM TFTP

Deze fout wordt in de Traces van de Conversation Manager gezien:

```
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:

Oplossing:

1. Controleer of de TFTP-server correct is in de poortgroep > **Bewerken** > configuratie van servers.
2. Controleer dat het CUCM-cluster in veilige modus staat.
3. Controleer dat het CTL-bestand op CUCM TFTP bestaat.

Zaak 3: Poorten niet registreren

Deze fout wordt in de Traces van de Conversation Manager gezien:

```
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
```

Oplossing:

1. Dit is waarschijnlijk het gevolg van een foutieve vergelijking in md5-checksum van het CTL-bestand op CUCM en CUC als gevolg van regeneratie van het CTL-bestand certificaten. Start de CUC server opnieuw om het CTL-bestand te verfrissen.

Cisco interne informatie

U kunt ook het CTL-bestand als volgt uit wortel verwijderen:

Verwijdert het CTL-bestand uit /tmp/map en stelt poortgroep opnieuw in. U kunt een md5-checksum op het bestand uitvoeren

en vergelijk voordat u het verwijdert:

```
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-klant 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-
```

Bovendien kunt u naar de deze handleiding voor probleemoplossing verwijzen:

Defecten

[CSCum48958](#) - CUCM 10.0 (ip-adreslengte is onjuist)

[CSCtn87264](#) - TLS-verbinding mislukt voor beveiligde SIP-poorten

[CSCur10758](#) - kan herroepen certificaten niet verwijderen Unity Connection

[CSCur10534](#) - Unity Connection 10.5 TLS/PKI redundante CUCM

[CSCve4775](#) - Aanvraag voor functies voor een methode om het CUCM-bestand op het CUC-bestand te uploaden en te bekijken