Configuratievoorbeeld voor beveiligde SIP-integratie tussen CUCM en CUC op basis van next-generation encryptie (NGE)

Inhoud

Inleiding

Dit document beschrijft de configuratie en verificatie van de beveiligde SIP-verbinding tussen de Cisco Unified Communications Manager (CUCM) en Cisco Unity Connection (CUC)-server met behulp van encryptie van de volgende generatie.

Security over SIP-interface van de volgende generatie beperkt de SIP-interface tot het gebruik van Suite B-telefoons op basis van TLS 1.2, SHA-2 en AES256-protocollen. Het maakt de verschillende combinaties van ciphers mogelijk op basis van de prioritaire volgorde van RSA- of ECDSA-ciphers. Tijdens de communicatie tussen Unity Connection en Cisco Unified CM worden zowel cifen als derden-certificaten aan beide uiteinden geverifieerd. Hieronder staat de

configuratie voor de ondersteuning van Next Generation Encryption.

Als u van plan bent de certificaten te gebruiken die door een certificeringsinstantie van derden zijn ondertekend, dan start u met de certificaatondertekening aan het eind van de configuratie sectie (Configuratie - Ondertekening van de op EC gebaseerde certificaten door derden CA)

Voorwaarden

Vereisten

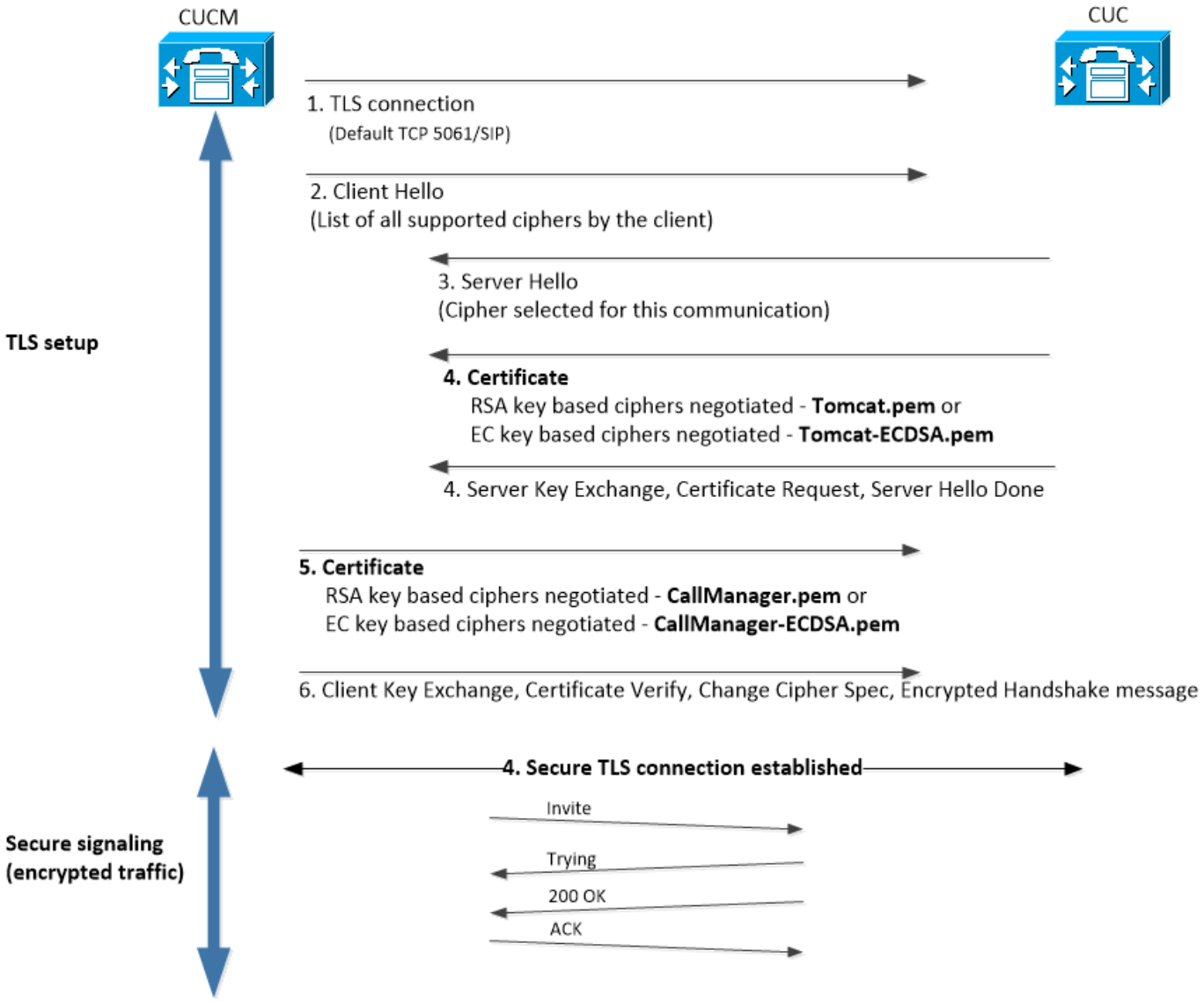
De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

CUCM versie 11.0 en hoger in gemengde modus
CUC versie 11.0 en hoger

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.

Netwerkdiagram

In dit diagram wordt kort het proces uitgelegd dat helpt een beveiligde verbinding tussen CUCM en CUC tot stand te brengen nadat de volgende generatie coderingsondersteuning is ingeschakeld:



Certificaatvereisten

Dit zijn de vereisten voor certificaatuitwisseling wanneer de ondersteuning voor volgende generatie van codering is ingeschakeld op Cisco Unity Connection.

- **Op RSA-toets gebaseerde ciphers onderhandeld**

Gebruikte CUCM-certificaat	Gebruikte CUC-certificaat	Certificaten om te uploaden naar CUCM	Certificaten om te uploaden naar CUC
CallManager 4.000 (zelf-ondertekend)	Tomcat.pem (zelf ondertekend)	Tomcat.pem die in CUCM wordt geüpload > CallManager-trust	None.
CallManager 4.000 (CA ondertekend)	Tomcat.pem (CA ondertekend)	CUC root en intermediair CA-certificaat*1 dat moet worden geüpload naar CUCM > CallManager-trust	CUCM root en intermediair certificaat*2 dat moet worde geüpload naar CUC > CallManager-trust.
CallManager 4.000 (CA ondertekend)	Tomcat.pem (zelf ondertekend)	Tomcat.pem die in CUCM wordt geüpload > CallManager-trust	CUCM root en intermediair certificaat dat in CUC > CallManager-trust moet wo geüpload.
CallManager 4.000	Tomcat.pem (CA	CUC root en intermediair CA-	None.

(zelf-ondertekend)	ondertekend)	certificaat dat in CUCM moet worden geüpload > CallManager-trust

*1 CUC root & intermediair CA-certificaat verwijst naar CA-certificaat dat het certificaat Unity Connection Tomcat (Tomcat.pem) heeft ondertekend.

*2 CUCM root & intermediair CA-certificaat verwijst naar CA-certificaat dat het CUCM CallManager-certificaat (CallManager.pem) heeft ondertekend.

- EG-sleutelspelers overeengekomen

Gebruikte CUCM-certificaat	Gebruikte CUC-certificaat	Certificaten om te uploaden naar CUCM	Certificaten om te uploaden naar CUC
CallManager-ECDSA.pem (zelf-ondertekend)	Tomcat-ECDSA.pem (zelf ondertekend)	Tomcat-ECDSA.pem die in CUCM wordt geüpload > CallManager-trust	None.
CallManager-ECDSA.pem (CA ondertekend)	Tomcat-ECDSA.pem (ondertekend door CA)	CUC root en intermediair CA-certificaat*1 dat moet worden geüpload naar CUCM > CallManager-trust	CUCM root en intermediair CA certificaat*2 dat moet worden geüpload naar CUC > CallManager-trust.
CallManager-ECDSA.pem (CA ondertekend)	Tomcat-ECDSA.pem (zelf ondertekend)	Tomcat-ECDSA.pem die in CUCM wordt geüpload > CallManager-trust.	CUCM root en intermediair CA-certificaat dat in CUC > CallManager-trust moet worden geüpload.
CallManager-ECDSA.pem (zelf-ondertekend)	Tomcat-ECDSA.pem (ondertekend door CA)	CUC root en intermediair CA-certificaat dat in CUCM moet worden geüpload > CallManager-trust	None.

*1 Certificaat CUC root & intermediair CA verwijst naar CA-certificaat dat het certificaat Unity Connection EC-gebaseerde Tomcat-certificaat (Tomcat-ECDSA.pem) heeft ondertekend.

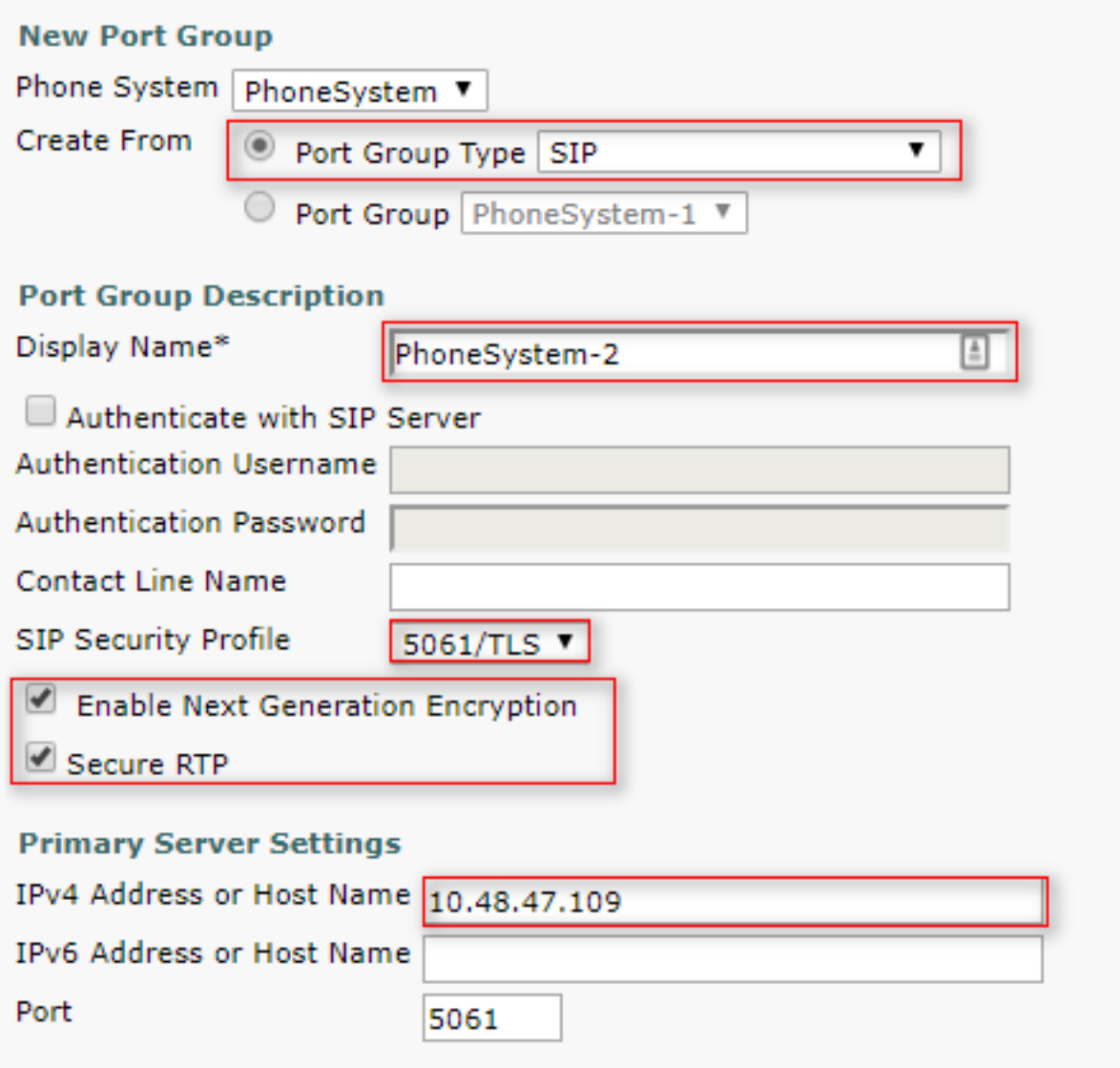
*2 CUCM root & intermediair CA-certificaat verwijst naar CA-certificaat dat het CUCM CallManager-certificaat (CallManager-ECDSA.pem) heeft ondertekend.

1. Opmerking: Het certificaat Tomcat-ECDSA.pem wordt CallManager-ECDSA.pem genoemd in 11.0.1 versies van CUC. Vanaf CUC 11.5.x wordt het certificaat omgedoopt tot Tomcat-ECDSA.pem.

Configureren - Cisco Unity Connection (CUC)

1. Voeg een nieuwe poortgroep toe

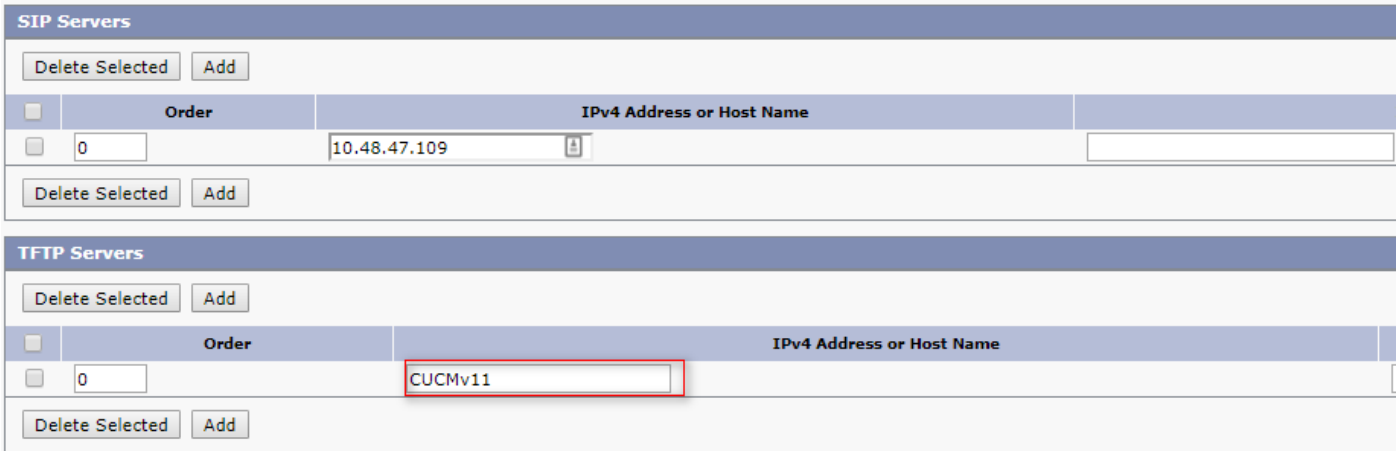
Blader naar Cisco Unity Connection-beheerpagina > Telefonieintegratie > poortgroep en klik op Add New. Controleer het vakje Encryptie inschakelen van de volgende generatie.



1. **Opmerking**: het Cisco Tomcat-certificaat van Unity Connection wordt gebruikt tijdens SSL-handdruk nadat het selectieknop Encryptie van de volgende generatie inschakelen is ingeschakeld.
    - Indien het op ECDSA gebaseerde algoritme wordt onderhandeld, dan wordt het op EC-toets gebaseerde certificaat gebruikt in SSL handshake.
    - Indien op RSA gebaseerd algoritme wordt onderhandeld, dan wordt op RSA gebaseerde het certificaat van de Tomatkist gebruikt in SSL handdruk.

2. Voeg de TFTP-serverreferentie toe

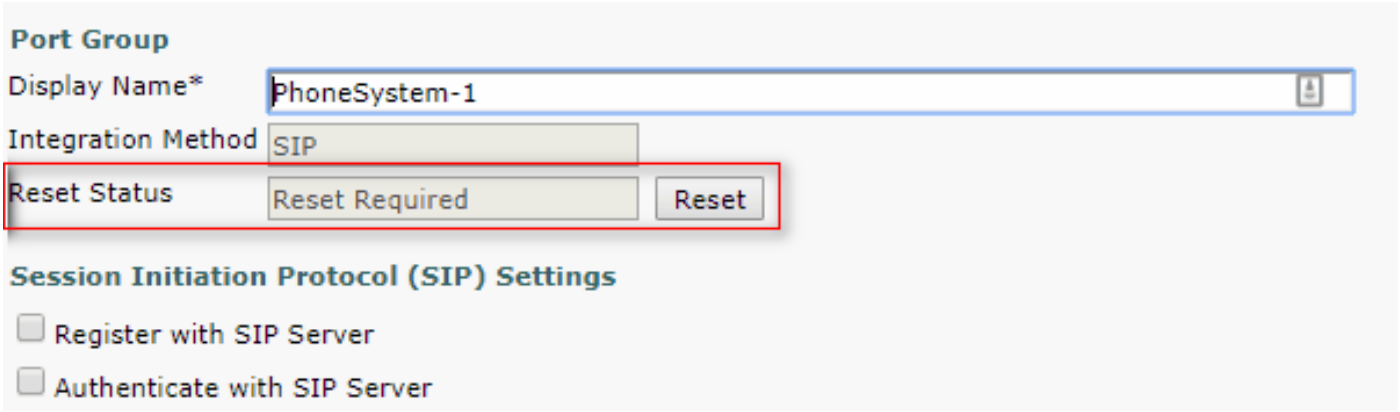
In de pagina Basisbeginselen van de Port Group, navigeer om > servers uit te werken en voeg FQDN van TFTP server van uw CUCM cluster toe. FQDN/Hostname van de TFTP-server moet overeenkomen met de GN-naam (Common Name) van CallManager-certificaat. IP-adres van de server werkt niet en het resulteert in het niet downloaden van het ITL-bestand. De DNS-naam moet daarom via een geconfigureerde DNS-server kunnen worden opgelost.



Start Connection Conversation Manager op elk knooppunt door te navigeren naar Cisco Unity Connection Services > Tools > Service Management. Dit is verplicht voor de configuratie.

1. Opmerking: Unity Connection downloads ITL-bestand (ITLfile.tlv) van CUCM's TFTP met behulp van https-protocol op beveiligde 6972-poort (URL: https://<CUCM-TFTP-FQDN>:6972/ITLFile.tlv). CUCM moet in de gemengde modus zijn actief omdat CUC op zoek is naar het "CCM+TFTP"-functiecertificaat uit het ITL-bestand.

Navigeer terug naar integratie via telefonie > Port group > Port Group > Basics configuratie pagina en stel uw nieuwe toegevoegde poortgroep opnieuw in.



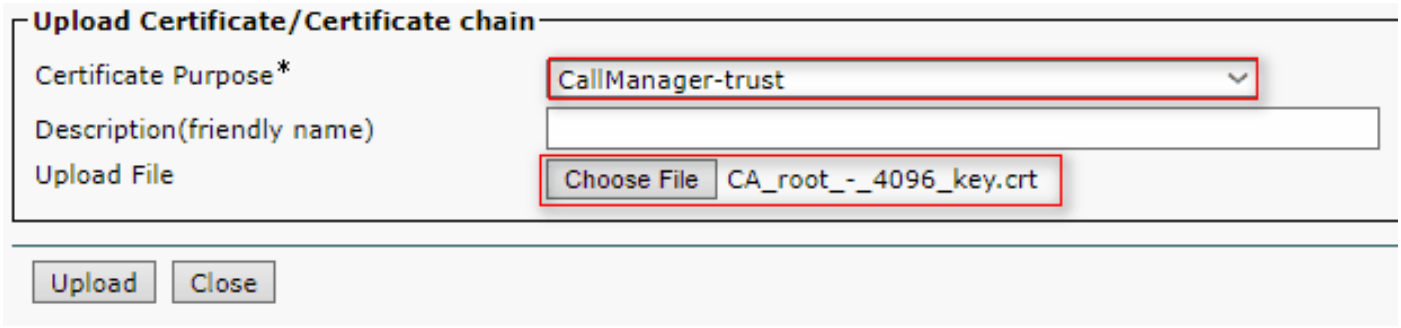
1. Opmerking: Telkens wanneer de poortgroep wordt hersteld, zal de CUC server zijn lokaal opgeslagen ITL-bestand bijwerken door verbinding te maken met de CUCM-server.

3. Spraakmailpoorten toevoegen

Navigeer terug naar integratie Telephony > Port en klik op Add new om poort toe te voegen aan uw nieuwe poortgroep.

4. CUCM-voet uploaden en tussentijds certificaat van derde partij CA

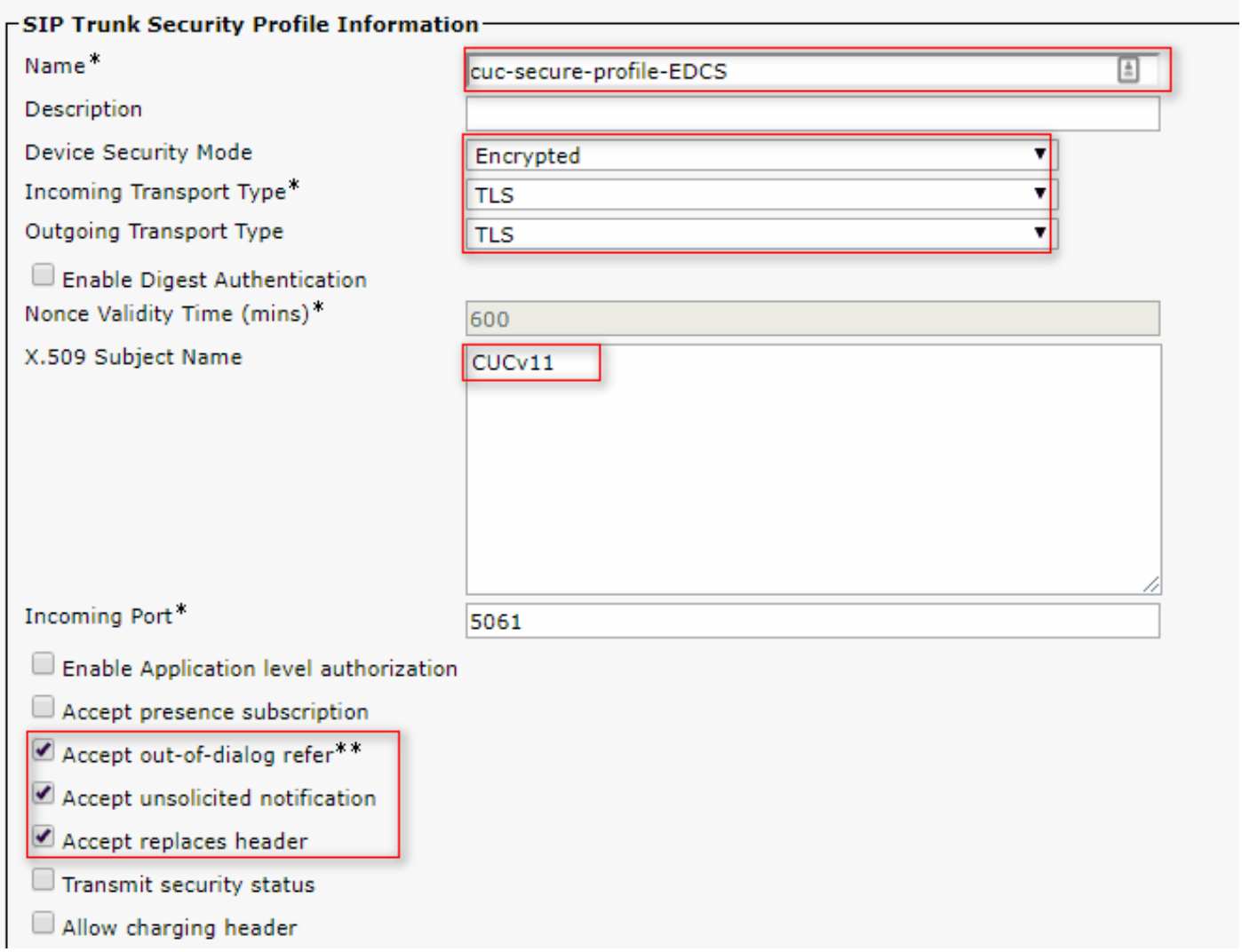
In het geval van certificaten van derden, moet u het certificaat van de Opstarten en het certificaat van de Intermediate van de certificeringsinstantie van de derde op CallManager-vertrouwen van Unity Connection uploaden. Dit is alleen nodig als de VKV van derden uw Call Manager-certificaat heeft ondertekend. Voer deze actie uit door te navigeren naar Cisco Unified OS-beheer > Beveiliging > certificaatbeheer en klik op Upload-certificaat.



Configureren - Cisco Unified CM (CUCM)

1. Maak een SIP-romp beveiligingsprofiel

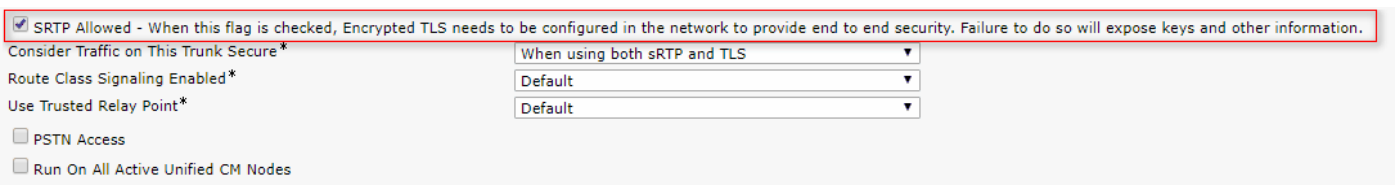
Navigeer naar CUCM-beheer > Systeem > Security > SIP Trunk-beveiligingsprofiel en voeg een nieuw profiel toe. X.509 Onderwerp-naam moet overeenkomen met FQDN van de CUC-server.

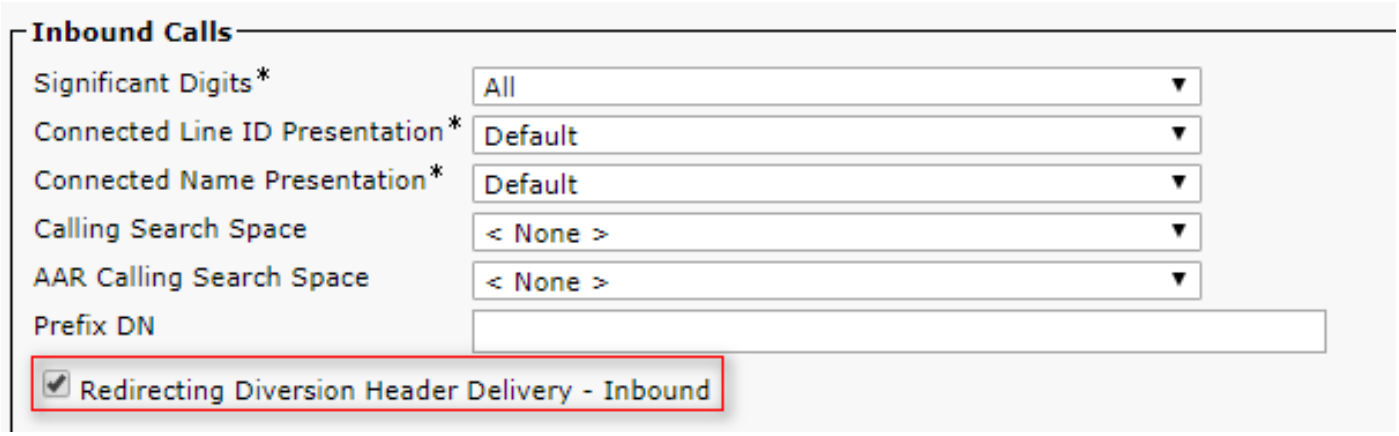


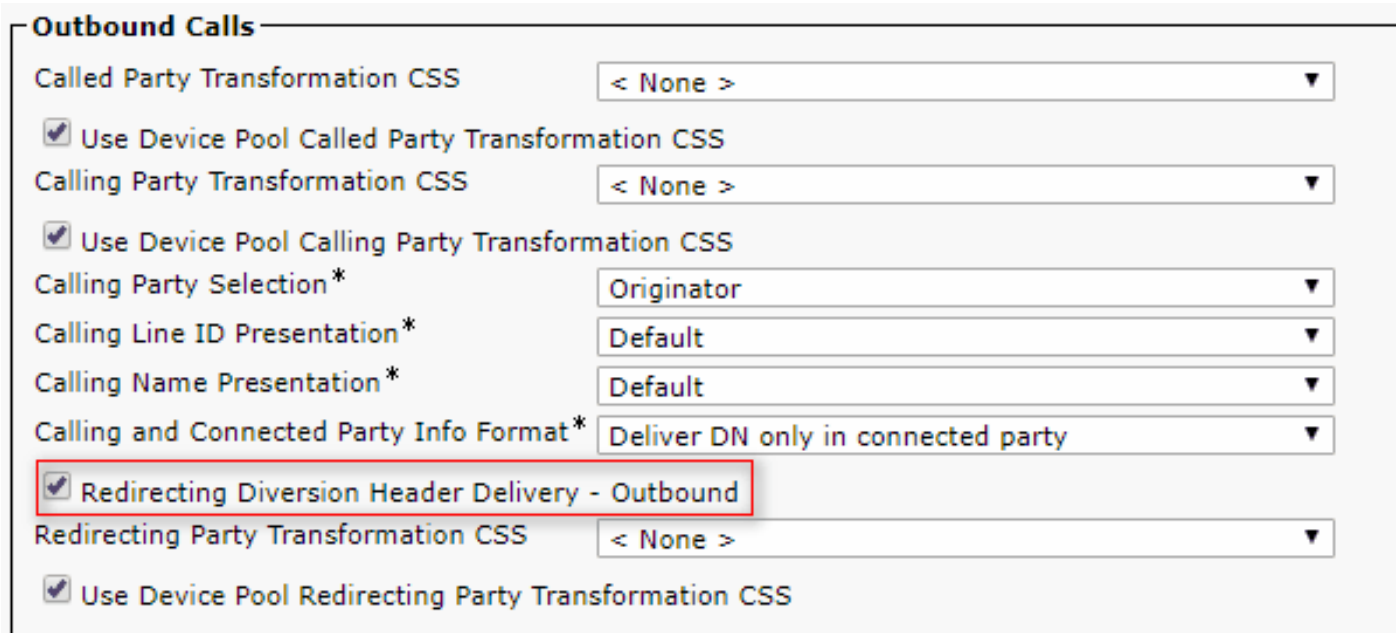
1. **Opmerking**: CLI-opdracht "show cert own tomcat/tomcat.pem" kan de RSA-toets op basis van certificaat op Unity Connection weergeven. Hij moet overeenkomen met de X.509 Onderwerp naam die op CUCM is ingesteld. De CN is gelijk aan FQDN/Hostname van de Unity server. Het op EC-toets gebaseerde certificaat bevat de FQDN/hostname in het veld Onderwerp Alternate Name (SAN).

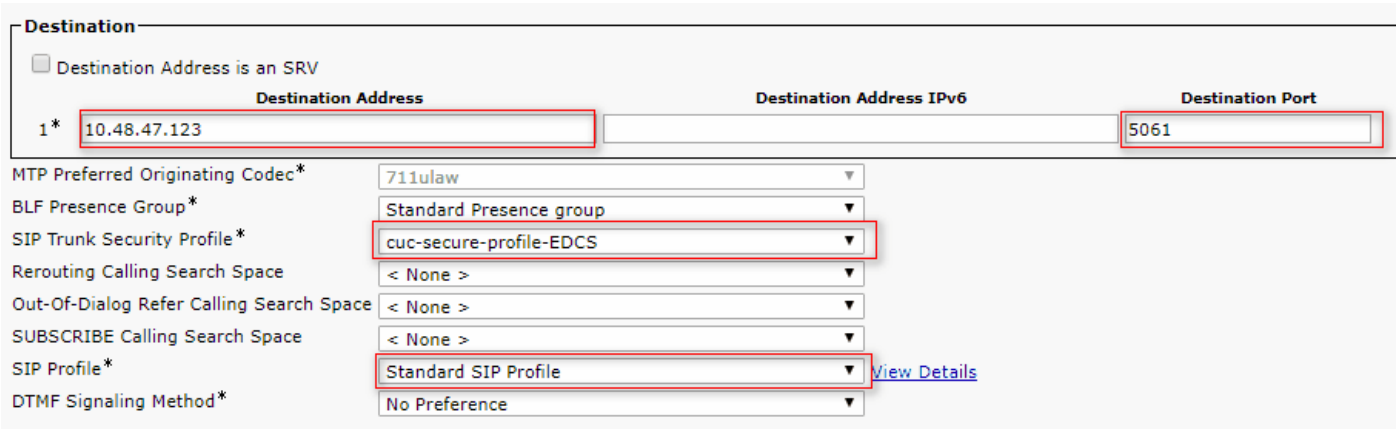
2. Maak een beveiligde SIP-trunk

Navigeren in naar apparaat > Trunk > Klik en voeg nieuw toe en creëer een standaard SIP stam die voor veilige integratie met Unity Connection zal worden gebruikt.







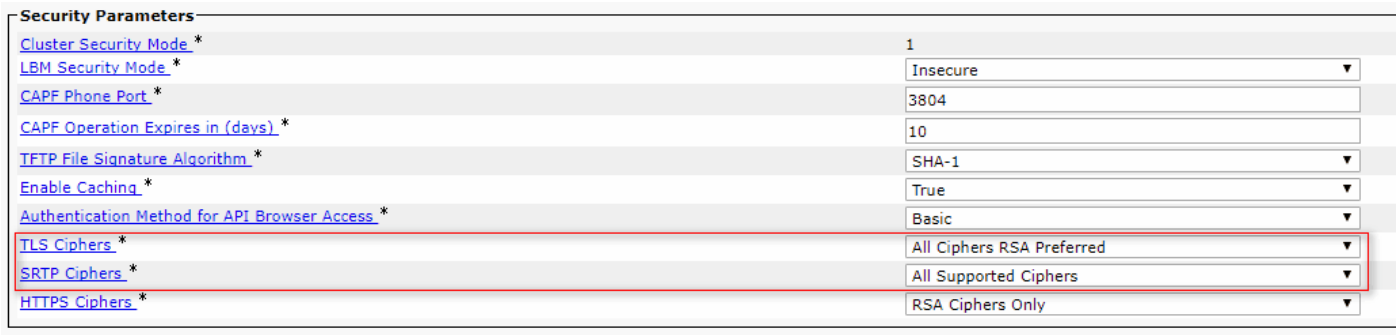


3. TLS- en SRTP-telefoons configureren

1. Opmerking: De onderhandeling tussen Unity Connection en Cisco Unified Communications Manager is afhankelijk van de configuratie van het TLS-algoritme met de volgende voorwaarden: Wanneer Unity Connection als server optreedt, is de TLS-algoritme-onderhandeling gebaseerd op de voorkeur die is geselecteerd door Cisco Unified CM.Indien het op ECDSA gebaseerde algoritme wordt onderhandeld, dan worden de op EC-toets gebaseerde certificaten gebruikt in SSL handshake.Indien op RSA gebaseerd algoritme wordt onderhandeld dan is op RSA gebaseerd om certificaten worden gebruikt in SSL handshake.Wanneer Unity Connection als client optreedt, is de onderhandeling over TLS-

algoritmen gebaseerd op de voorkeur die is geselecteerd door Unity Connection.

Navigeer naar Cisco Unified CM > Systems > Enterprise parameters en selecteer de gewenste algoritme optie uit de TLS- en SRTP-cifers in de vervolgkeuzelijst.



Start de Cisco Call Manager-service voor elk knooppunt opnieuw door te navigeren naar Cisco Unified Service pagina, Gereedschappen > Control Center-functieservices en selecteer Cisco Call Manager onder CM-services

Navigeer naar Cisco Unity Connection Management-pagina > Systeeminstellingen > Algemene configuraties en selecteer de juiste algoritme optie uit de vervolgkeuzelijst TLS- en SRTP-cips.

Start Connection Conversation Manager op elk knooppunt door te navigeren naar Cisco Unity Connection Services > Tools > Service Management.

TLS-kabelopties met prioriteitsvolgorde

TLS-nummeropties	TLS-cips in prioriteitsvolgorde
Alleen sterker-AES-256 SHA-384: RSA voorkeur	• TLS_ECDHE_RSA_MET_AES_256_GCM_SHA384 • TLS_ECDHE_ECDSA_MET_AES_256_GCM_SHA384
alleen Stronst-AES-256 SHA-384: ECDSA geselecteerd	• TLS_ECDHE_ECDSA_MET_AES_256_GCM_A384 • TLS_ECDHE_RSA_MET_AES_256_GCM_SH4

Alleen middelgrote AES-256 AES-128: RSA voorkeur	• TLS_ECDHE_RSA_MET_AES_256_GCM_SH 4 • TLS_ECDHE_ECDSA_MET_AES_256_GCM_ A384 • TLS_ECDHE_RSA_MET_AES_128_GCM_SH 6 • TLS_ECDHE_ECDSA_MET_AES_128_GCM_ A256 • TLS_ECDHE_ECDSA_MET_AES_256_GCM_ A384
Alleen middelgrote AES-256 AES-128: ECDSA geselecteerd	• TLS_ECDHE_RSA_MET_AES_256_GCM_SH 4 • TLS_ECDHE_ECDSA_MET_AES_128_GCM_ A256 • TLS_ECDHE_RSA_MET_AES_128_GCM_SH 6 • TLS_ECDHE_RSA_MET_AES_256_GCM_SH 4 • TLS_ECDHE_ECDSA_MET_AES_256_GCM_ A384
Alle ciphers RSA voorkeur (standaard)	• TLS_ECDHE_RSA_MET_AES_128_GCM_SH 6 • TLS_ECDHE_ECDSA_MET_AES_128_GCM_ A256 • TLS_RSA_MET_AES_128_CBC_SHA • TLS_ECDHE_ECDSA_MET_AES_256_GCM_ A384 • TLS_ECDHE_RSA_MET_AES_256_GCM_SH 4
Alle cifers ECDSA voorgedragen	• TLS_ECDHE_ECDSA_MET_AES_128_GCM_ A256 • TLS_ECDHE_RSA_MET_AES_128_GCM_SH 6 • TLS_RSA_MET_AES_128_CBC_SHA

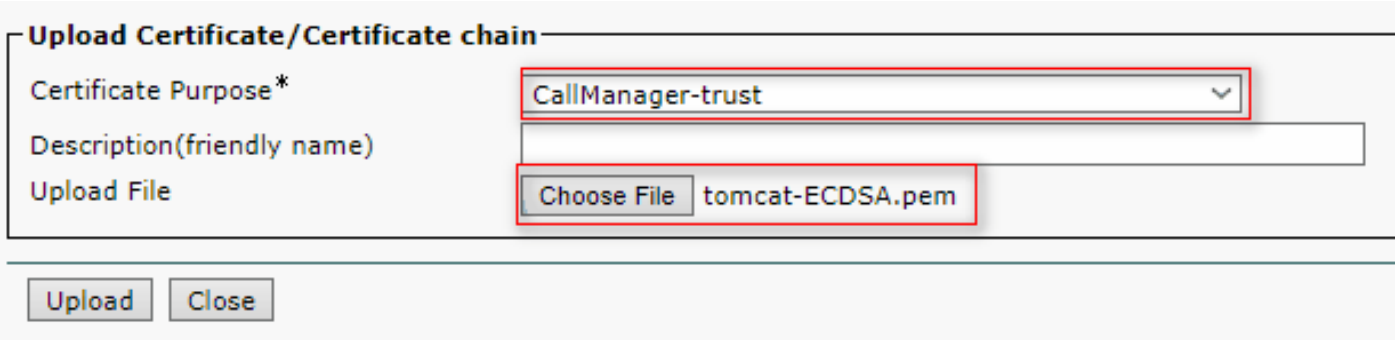
SRTP-clientopties in prioriteitsvolgorde

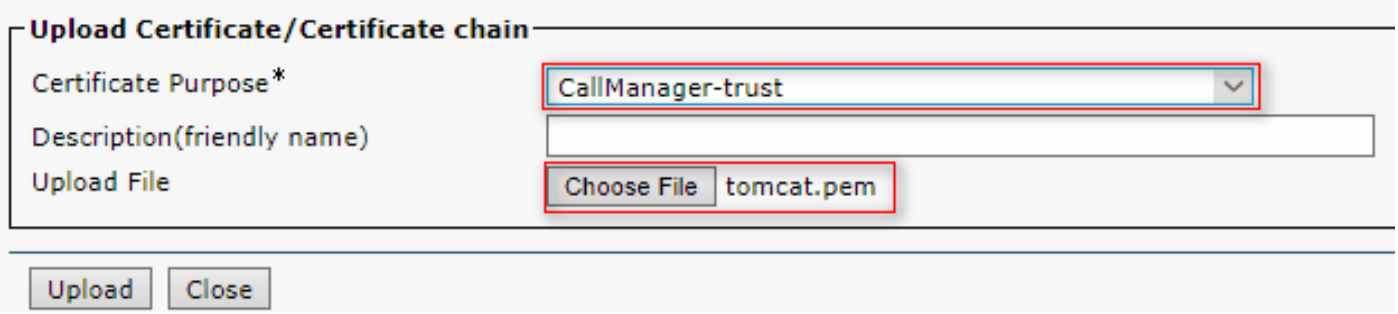
SRTP-koperoptie	SRTP-in prioriteitsvolgorde
Alle ondersteunde AES-256-, AES-128-telefoons	• AEAD_AES_256_GCM • AEAD_AES_128_GCM • AES_CM_128_HMAC_SHA1 _32
AEAD AES-256, AES-28 op GCM gebaseerde cifers	• AEAD_AES_256_GCM • AEAD_AES_128_GCM
Alleen AEAD AES256 op GCM-gebaseerde microfoon	• AEAD_AES_256_GCM

4. CUC-videocertificaten uploaden (RSA & EC-gebaseerd)

Navigeer naar OS-beheer > Beveiliging > certificaatbeheer en uploaden beide CUC-certificaten

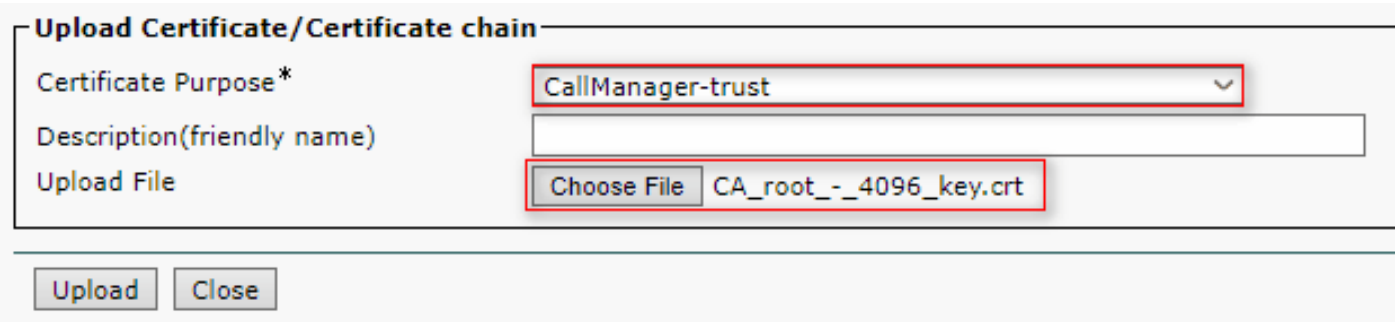
(RSA & EC-gebaseerd) in de CallManager-trust winkel.





1. **Opmerking**: het uploaden van beide Unity Tomcat-certificaten is niet verplicht indien alleen ECDSA-ciphers zijn onderhandeld. In dat geval is het EG-certificaat van Tomcat voldoende.

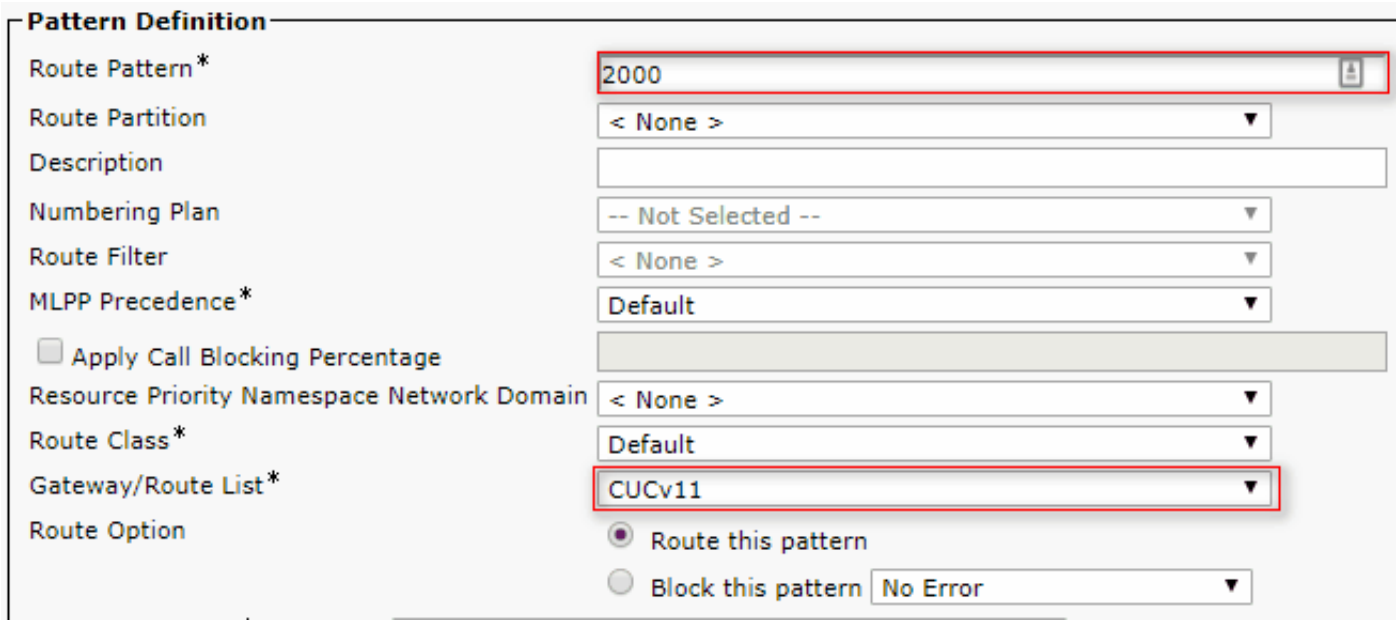
In het geval van certificaten van derden, moet u het wortel- en Intermediate certificaat van de certificeringsinstantie van derden uploaden. Dit is alleen nodig als de derde partij uw Unity Tomcat-certificaat heeft ondertekend.



Start het Cisco Call Manager-proces op alle knooppunten opnieuw om de wijzigingen toe te passen.

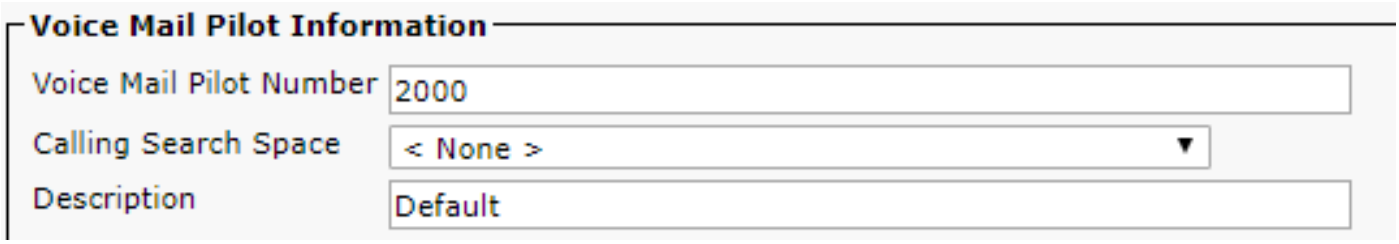
5. Routepatroon maken

Configuratie van een routepatroon dat aan de gevormde boomstam door te navigeren om het Routing > Route/Tunt > Routepatroon te bellen. Uitbreiding ingevoerd als een routepatroonnummer kan worden gebruikt als voicemail-piloot.

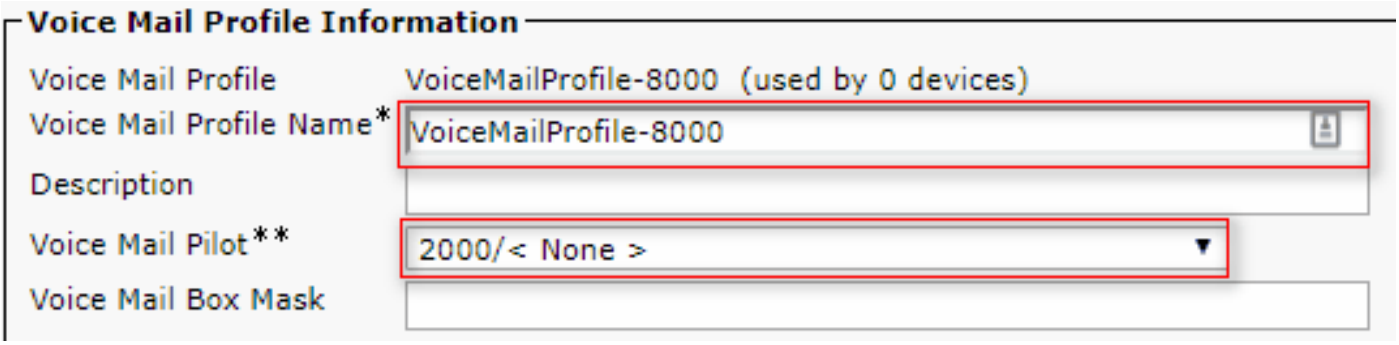


6. Maak een voicemail-piloot, voicemail-profiel en verdeel het aan de DNA's

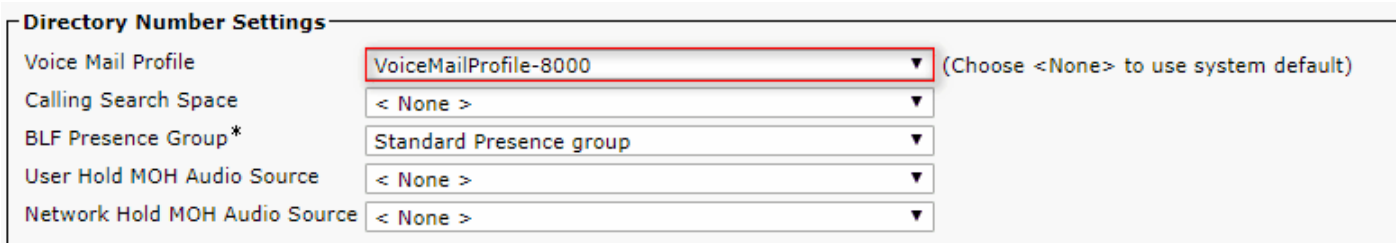
Maak een spraak-mailpiloot voor de integratie door naar geavanceerde functies > Voice Mail > Voice Mail Pilot te gaan.



Een voicemailprofiel maken als u alle instellingen aan elkaar wilt koppelen met geavanceerde functies > Voice Mail > Voice Mail Profile



Pas het nieuwe spraakpostprofiel toe aan de DNS's die bedoeld zijn om de beveiligde integratie te gebruiken door routing > Directory-nummer te bellen



Configureer - Ondertekening van de op de EG-toets gebaseerde certificaten door derden CA (optioneel)

De certificaten kunnen door een derde partij CA worden ondertekend alvorens de beveiligde integratie tussen de systemen tot stand te brengen. Volg de volgende stappen om de certificaten op beide systemen te ondertekenen.

Cisco Unity Connection-encryptie

1. Genereert certificaataanvraag (CSR) voor CUC Tomcat-ECDSA en laat het certificaat ondertekend door derde partij CA zien
2. CA biedt identiteitsbewijs (CA-ondertekend certificaat) en CA-certificaat (CA-basiscertificaat) dat als volgt moet worden geüpload:
   CA-basiscertificaat uploaden naar de tomcat-trust winkel
   Identiteitscertificaat uploaden naar de tomcat-EDCS-winkel
3. Conversation Manager opnieuw starten op CUC

Cisco Unified CM

1. CSR genereren voor CUCM CallManager-ECDSA en laat het certificaat ondertekend door derden CA zien
2. CA biedt identiteitsbewijs (CA-ondertekend certificaat) en CA-certificaat (CA-basiscertificaat) dat als volgt moet worden geüpload:
   Upload CA root certificaat in de callmanager-trust winkel
   Identiteitscertificaat uploaden naar de callmanager-EDCS-winkel
3. Start Cisco CCM- en TFTP-services op elk knooppunt opnieuw

Hetzelfde proces wordt gebruikt voor het ondertekenen van op RSA-codes gebaseerde certificaten waarin CSR gegenereerd is voor CUC Tomcat-certificaat en CallManager-certificaat en in respectievelijk de tomatenwinkel en de callmanager-winkel geüpload is.

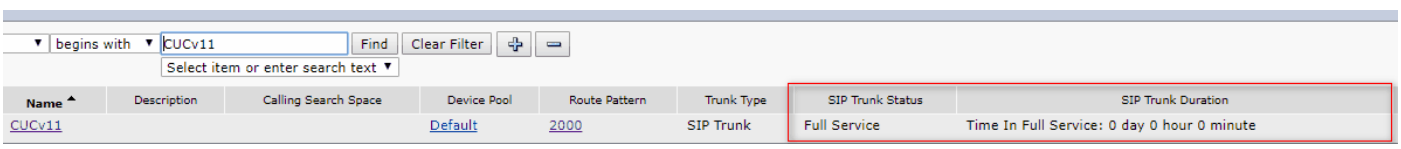
Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Secure SIP Trunk-verificatie

Druk op de knop Voice Mail aan 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.

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-stam controleren via Apparaat > Trunk zoals hieronder wordt weergegeven:



Secure RTP-gespreksverificatie

Controleer of het pictogram van het hangslot aanwezig is op oproepen naar Unity Connection. Dit betekent dat de RTP-stroom versleuteld is (het profiel voor apparaatbeveiliging moet beveiligd zijn zodat het kan werken) zoals in deze afbeelding wordt weergegeven.

Gerelateerde informatie

- SIP-integratiegids voor Cisco Unity Connection release 11.x