Exemple de configuration pour l'intégration SIP sécurisée entre CUCM et CUC basée sur le cryptage nouvelle génération (NGE)

Contenu

Introduction

Ce document décrit la configuration et la vérification de la connexion SIP sécurisée entre Cisco Unified Communication Manager (CUCM) et le serveur Cisco Unity Connection (CUC) à l'aide du chiffrement de nouvelle génération.

L'interface Security over SIP de nouvelle génération limite l'interface SIP à utiliser des algorithmes de chiffrement Suite B basés sur les protocoles TLS 1.2, SHA-2 et AES256. Il permet les différentes combinaisons de chiffrement en fonction de l'ordre de priorité des chiffrement RSA ou ECDSA. Lors de la communication entre Unity Connection et Cisco Unified CM, les certificats de

chiffrement et de tiers sont vérifiés aux deux extrémités. Vous trouverez ci-dessous la configuration de la prise en charge du chiffrement de nouvelle génération.

Si vous prévoyez d'utiliser les certificats signés par une autorité de certification tierce, commencez par signer le certificat à la fin de la section de configuration (Configurer - Signature des certificats basés sur la clé CE par une autorité de certification tierce)

Conditions préalables

Conditions requises

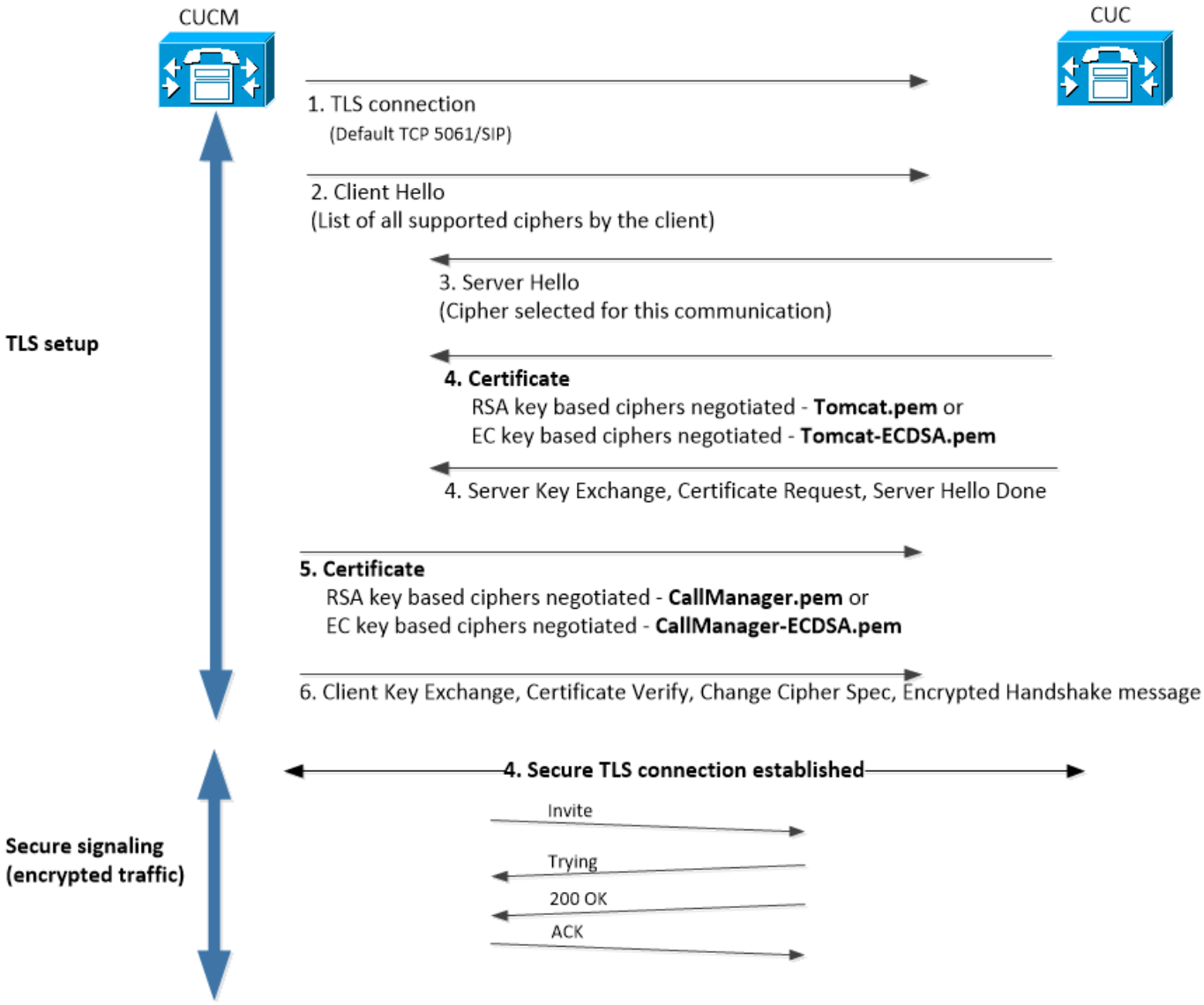
Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

CUCM version 11.0 et ultérieure en mode Mixed
CUC version 11.0 et ultérieure

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.

Diagramme du réseau

Ce diagramme explique brièvement le processus qui permet d'établir une connexion sécurisée entre CUCM et CUC une fois que la prise en charge du chiffrement de nouvelle génération est activée :



Exigences en matière de certificat

Il s'agit des conditions d'échange de certificats une fois que la prise en charge du chiffrement de nouvelle génération est activée sur Cisco Unity Connection.

- **Chiffres basés sur les clés RSA négociés**

Certificat CUCM utilisé	Certificat CUC utilisé	Certificats à télécharger sur CUCM	Certificats à télécharger ver CUC
CallManager.pem (autosigné)	Tomcat.pem (auto-signé)	Tomcat.pem à télécharger dans CUCM > CallManager-trust	Aucune.
CallManager.pem (CA signé)	Tomcat.pem (CA signé)	Certificat CA racine et intermédiaire CUC[*1] à télécharger dans CUCM > CallManager-trust	Certificat CA racine et intermédiaire CUCM[*2] à télécharger dans CUC > CallManager-trust.
CallManager.pem (CA signé)	Tomcat.pem (auto-signé)	Tomcat.pem à télécharger dans CUCM > CallManager-trust	Certificat CA racine et intermédiaire CUCM à télécharger dans CUC > CallManager-trust.
CallManager.pem	Tomcat.pem (CA	Certificat CUC racine et CA	Aucune.

(autosigné)	signé)	intermédiaire à télécharger dans CUCM > CallManager-trust

*1Le certificat d'autorité de certification racine et intermédiaire CUC fait référence au certificat d'autorité de certification qui a signé le certificat Tomcat de connexion Unity (Tomcat.pem).

*2Le certificat d'autorité de certification racine et intermédiaire CUCM fait référence au certificat d'autorité de certification qui a signé le certificat CallManager CUCM (Callmanager.pem).

- **Chiffrement basé sur les clés EC négocié**

Certificat CUCM utilisé	Certificat CUC utilisé	Certificats à télécharger sur CUCM	Certificats à télécharger vers CUC
CallManager-ECDSA.pem (autosigné)	Tomcat-ECDSA.pem (autosigné)	Tomcat-ECDSA.pem à télécharger dans CUCM > CallManager-trust	Aucune.
CallManager-ECDSA.pem (CA signé)	Tomcat-ECDSA.pem (CA signé)	Certificat CA racine et intermédiaire CUC*1 à télécharger dans CUCM > CallManager-trust	Certificat CA racine et intermédiaire CUCM*2 à télécharger dans CUC > CallManager-trust.
CallManager-ECDSA.pem (CA signé)	Tomcat-ECDSA.pem (autosigné)	Tomcat-ECDSA.pem à télécharger dans CUCM > CallManager-trust.	Certificat CA racine et intermédiaire CUCM à télécharger dans CUC > CallManager-trust.
CallManager-ECDSA.pem (autosigné)	Tomcat-ECDSA.pem (CA signé)	Certificat CUC racine et CA intermédiaire à télécharger dans CUCM > CallManager-trust	Aucune.

*1 certificat CUC racine et CA intermédiaire fait référence au certificat CA qui a signé le certificat Tomcat basé sur Unity Connection EC (Tomcat-ECDSA.pem).

*2 Le certificat d'autorité de certification racine et intermédiaire CUCM fait référence au certificat d'autorité de certification qui a signé le certificat CallManager CUCM (CallManager-ECDSA.pem).

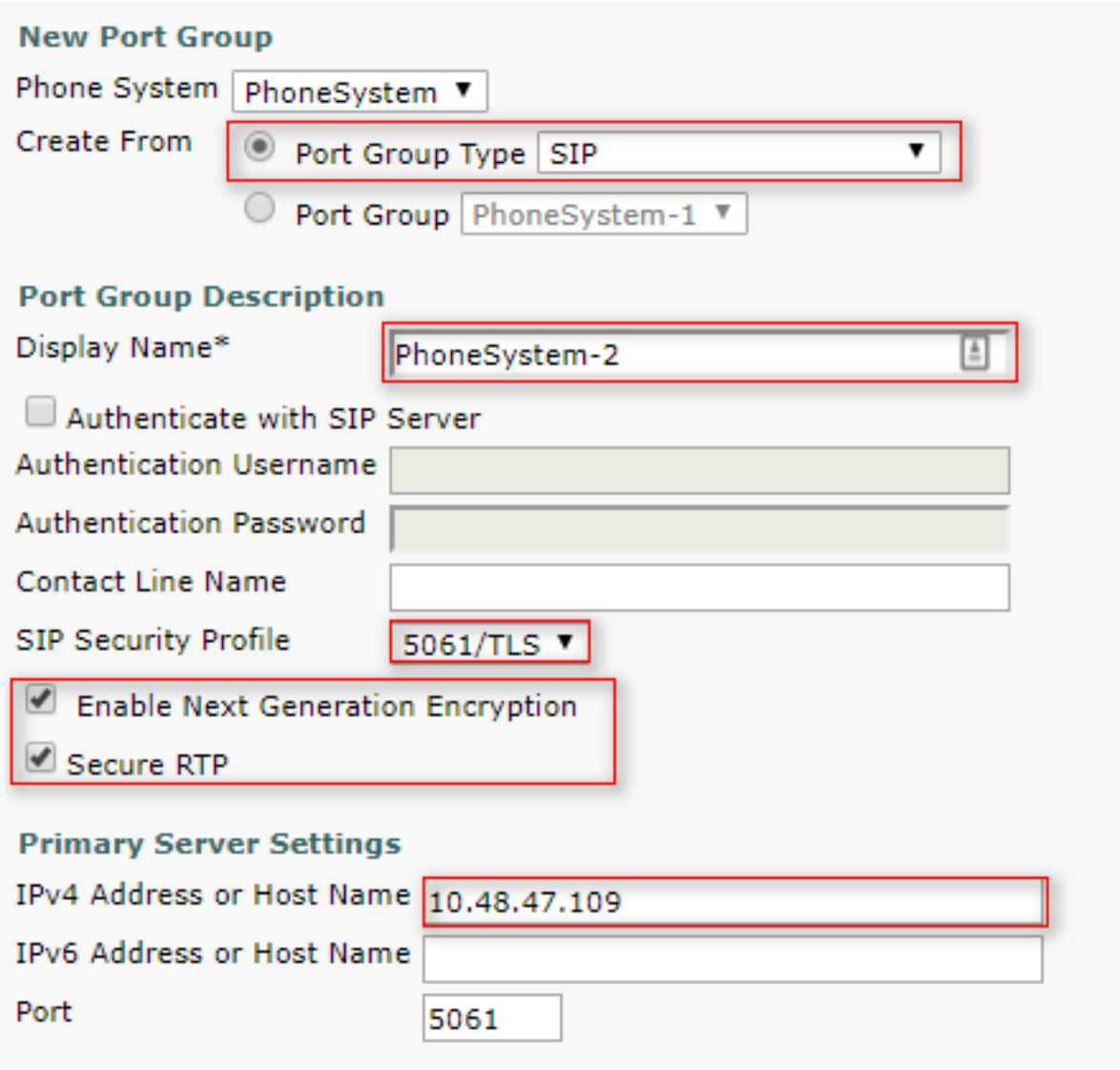
1. **Note**: Le certificat Tomcat-ECDSA.pem est appelé CallManager-ECDSA.pem dans les versions 11.0.1 de CUC. À partir de CUC 11.5.x, le certificat a été renommé Tomcat-ECDSA.pem.

Configurer - Cisco Unity Connection (CUC)

1. Ajouter un nouveau groupe de ports

Accédez à la page Cisco Unity Connection Administration > Telephony intégration > Port group et

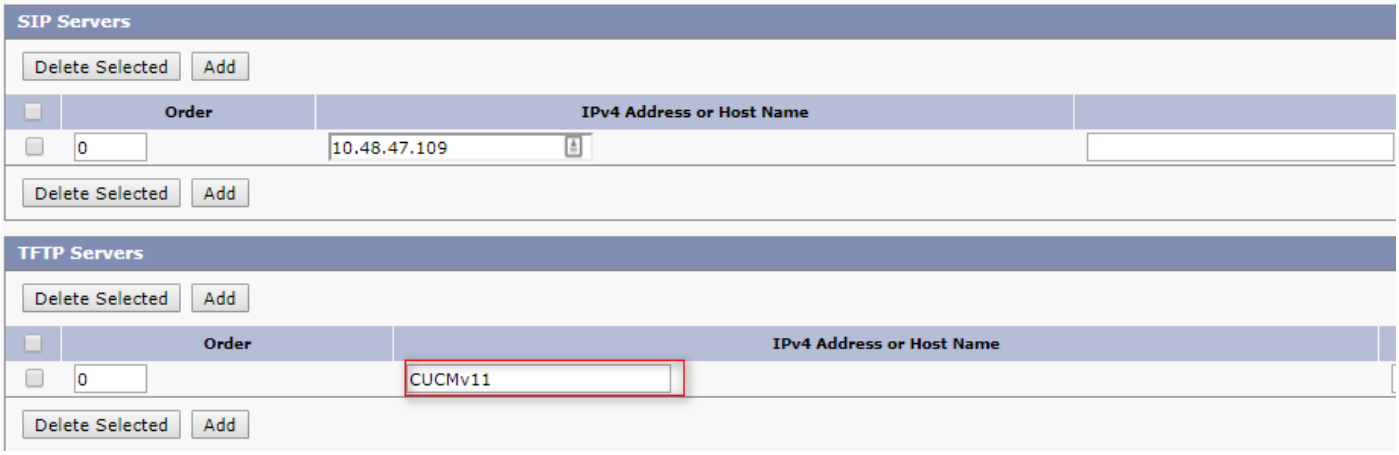
cliquez sur Add New. Cochez la case Activer le chiffrement nouvelle génération.



1. **Remarque** : le certificat Cisco Tomcat de Unity Connection sera utilisé lors de la connexion SSL une fois que la case Activer le chiffrement nouvelle génération est activée.
   · Dans le cas où le chiffrement ECDSA est négocié, le certificat ECDSA basé sur la clé EC est utilisé dans la connexion SSL.
   · Si le chiffrement basé sur RSA est négocié, le certificat tomcat basé sur la clé RSA est utilisé dans la connexion SSL.

2. Ajouter la référence du serveur TFTP

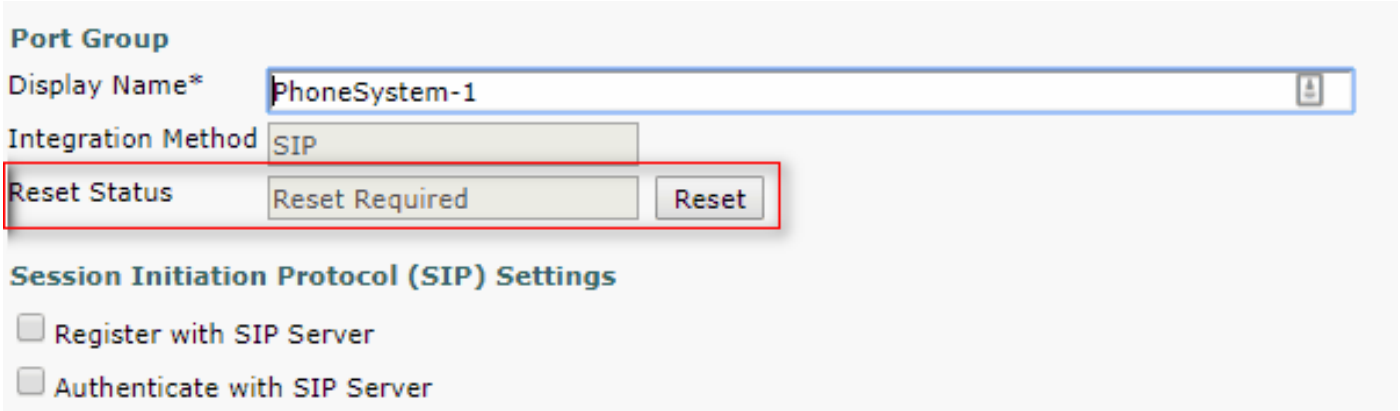
Sur la page Notions de base sur le groupe de ports, accédez à Edition > Serveurs et ajoutez le nom de domaine complet du serveur TFTP de votre cluster CUCM. Le nom de domaine complet/nom d'hôte du serveur TFTP doit correspondre au nom commun (CN) du certificat CallManager. L'adresse IP du serveur ne fonctionnera pas et ne pourra pas télécharger le fichier ITL. Le nom DNS doit donc pouvoir être résolu via le serveur DNS configuré.



Redémarrez Connection Conversation Manager sur chaque noeud en accédant à Cisco Unity Connection Serviceability > Tools > Service Management. Ceci est obligatoire pour que la configuration prenne effet.

1. **Note**: Unity connection télécharge le fichier ITL (ITLfile.tlv) à partir du TFTP de CUCM à l'aide du protocole https sur le port 6972 sécurisé (URL : https://<CUCM-TFTP-FQDN>:6972/ITLFile.tlv). CUCM doit être en mode mixte, car CUC recherche le certificat de fonction « CCM+TFTP » à partir du fichier ITL.

Revenez à la page Intégration de téléphonie > Groupe de ports > Configuration de base du groupe de ports et réinitialisez votre nouveau groupe de ports.



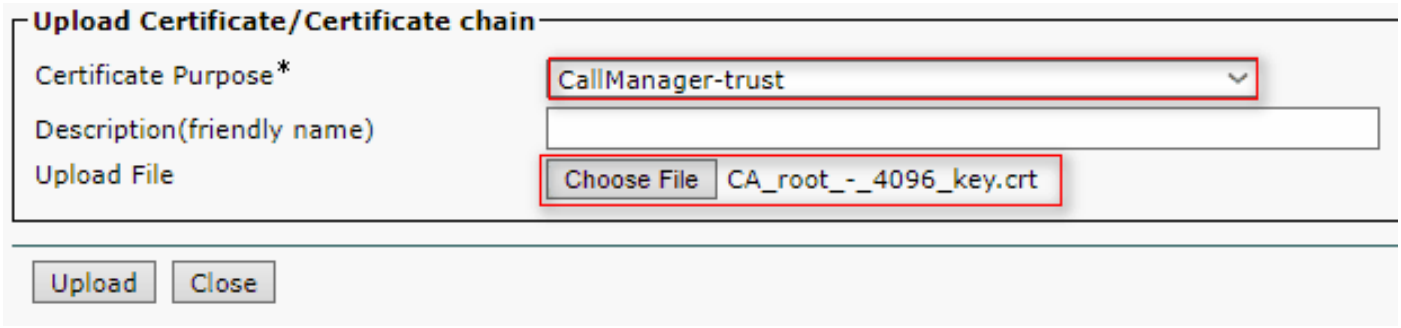
1. **Note**: Chaque fois que le groupe de ports est réinitialisé, le serveur CUC met à jour son fichier ITL stocké localement en se connectant au serveur CUCM.

3. Ajouter des ports de messagerie vocale

Revenez à Intégration téléphonique > Port et cliquez sur Ajouter nouveau pour ajouter un port à votre nouveau groupe de ports.

4. Télécharger le certificat racine et intermédiaire CUCM de l'autorité de certification tierce

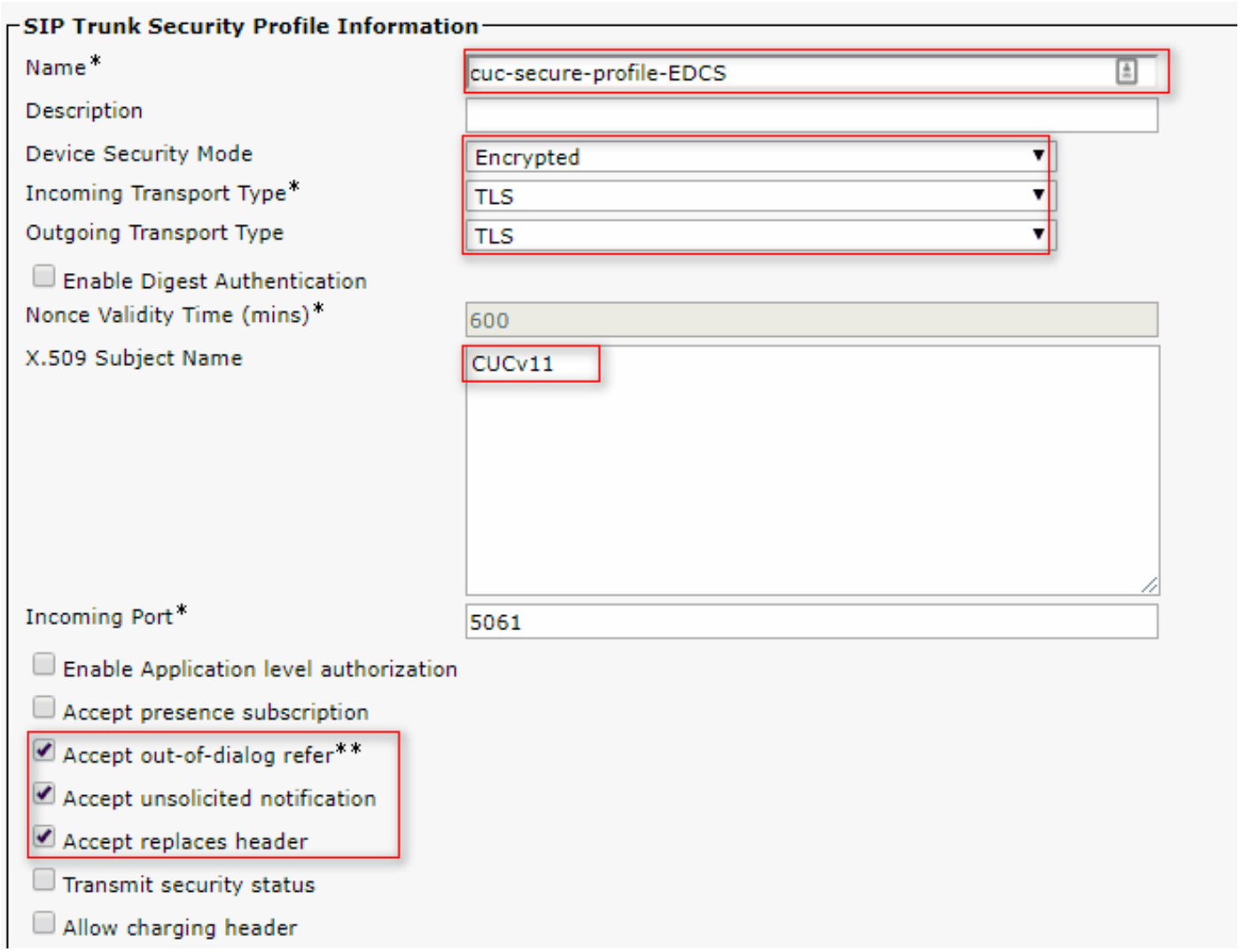
Dans le cas de certificats tiers, vous devez télécharger le certificat racine et intermédiaire de l'autorité de certification tierce sur CallManager-trust de Unity Connection. Ceci est nécessaire uniquement si l'autorité de certification tierce a signé votre certificat Call Manager. Pour effectuer cette action, accédez à Cisco Unified OS Administration > Security > Certificate Management et cliquez sur Upload Certificate.



Configurer - Cisco Unified CM (CUCM)

1. Créer un profil de sécurité de liaison SIP

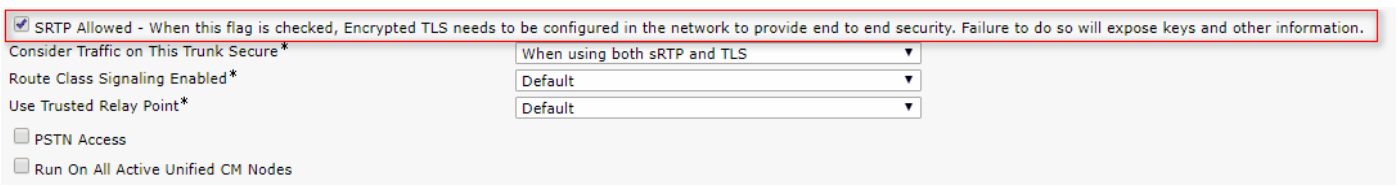
Accédez à CUCM Administration > System > Security > SIP Trunk Security Profile et ajoutez un nouveau profil. Le nom de sujet X.509 doit correspondre au nom de domaine complet du serveur CUC.

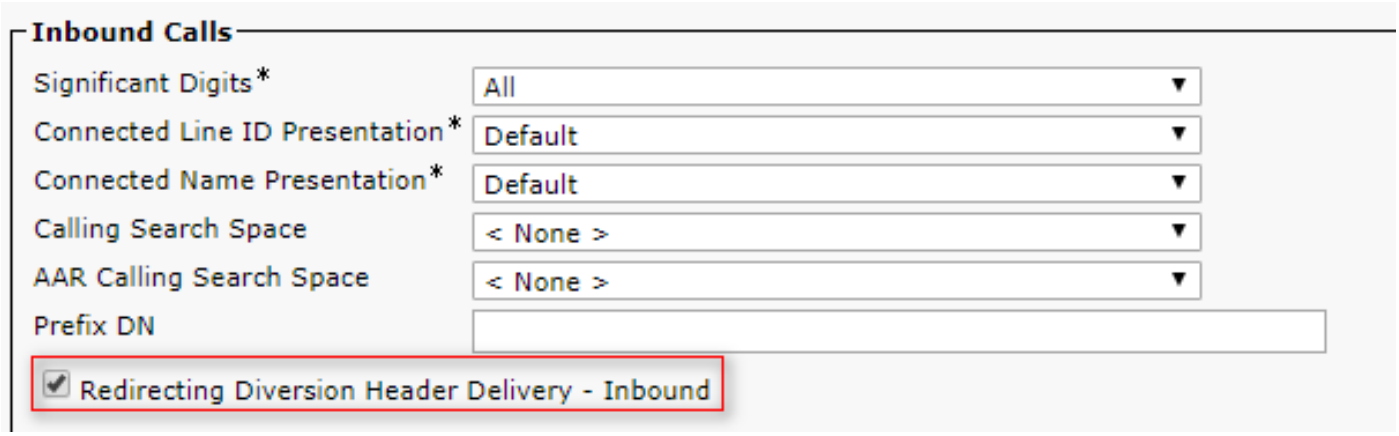


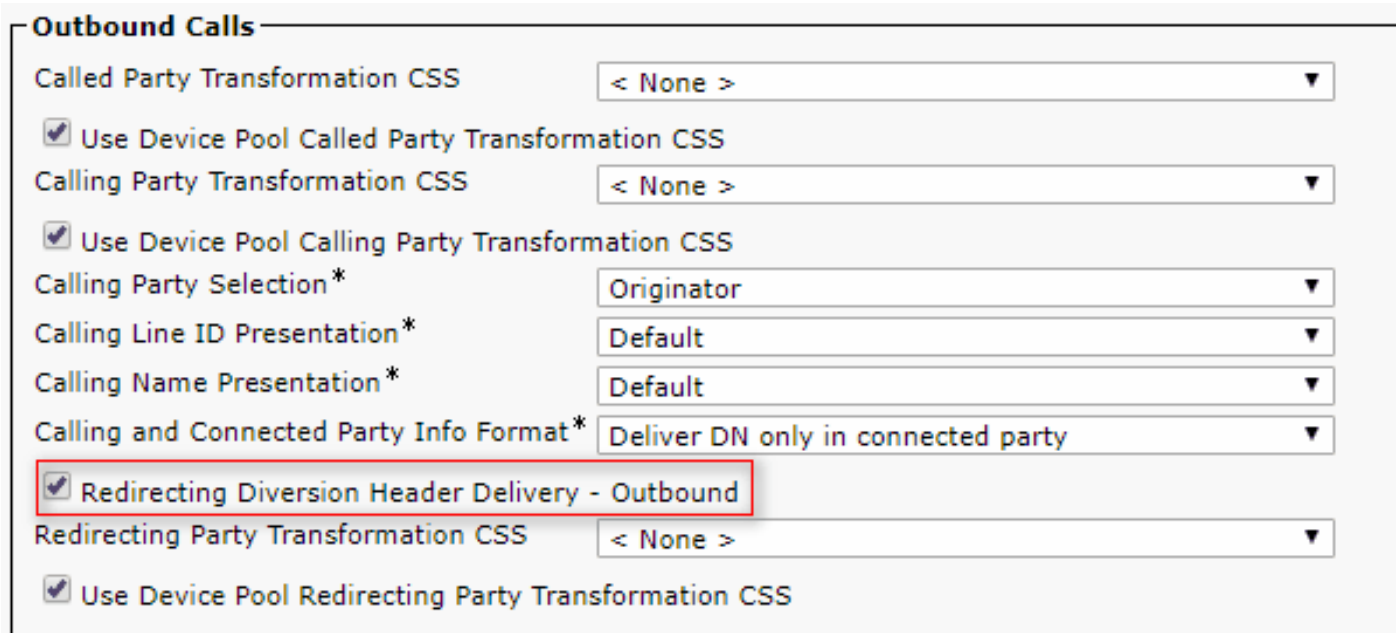
1. **Remarque** : la commande CLI « show cert own tomcat/tomcat.pem" peut afficher le certificat tomcat basé sur la clé RSA sur Unity Connection. Il doit correspondre au nom d'objet X.509 configuré sur CUCM. Le CN est égal au nom de domaine complet/nom d'hôte du serveur Unity. Le certificat basé sur la clé CE contient le nom de domaine complet/nom d'hôte dans son champ Nom de domaine secondaire (SAN).

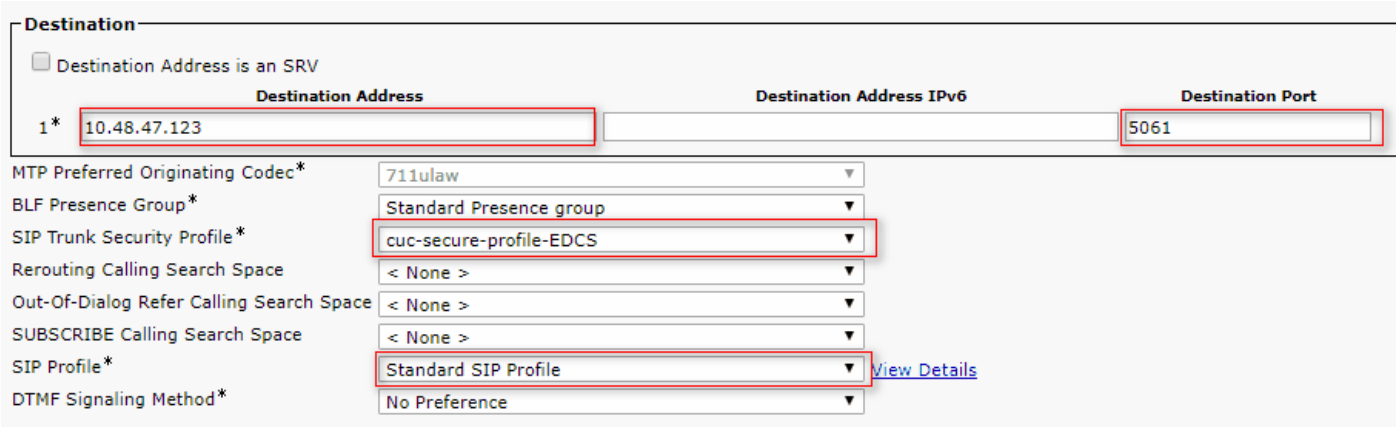
2. Créer une liaison SIP sécurisée

Naviguez jusqu'à Device > Trunk > Cliquez sur Add new et créez une liaison SIP standard qui sera utilisée pour une intégration sécurisée avec Unity Connection.







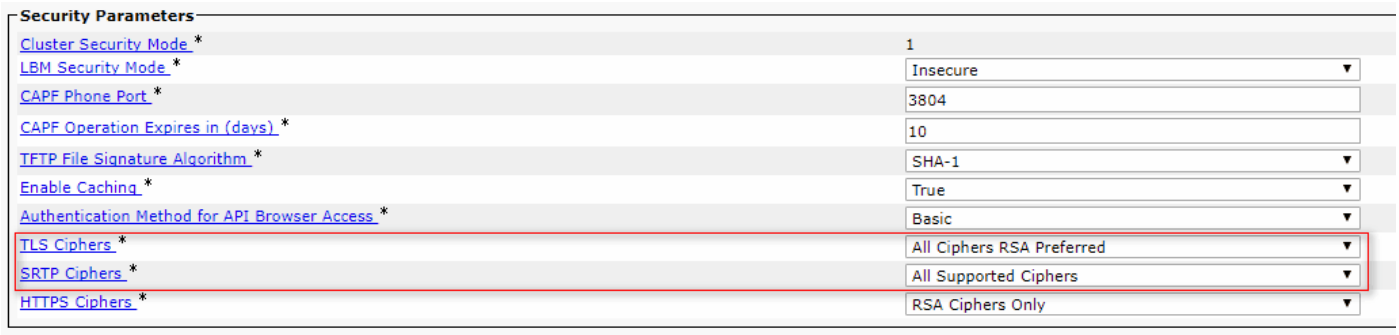


3. Configurer les chiffrement TLS et SRTP

1. **Note**: La négociation entre Unity Connection et Cisco Unified Communications Manager dépend de la configuration du chiffrement TLS avec les conditions suivantes : Lorsque Unity Connection agit en tant que serveur, la négociation du chiffrement TLS est basée sur la préférence sélectionnée par Cisco Unified CM.Dans le cas où le chiffrement ECDSA est négocié, les certificats ECDSA basés sur la clé EC sont utilisés dans la connexion SSL.Dans le cas où le chiffrement basé sur RSA est négocié, les certificats basés sur les clés RSA sont utilisés dans la connexion SSL.Lorsque Unity Connection agit en tant que client, la négociation du chiffrement TLS est basée sur la préférence sélectionnée par Unity

Connection.

Accédez à Cisco Unified CM > Systems > Enterprise Parameters et sélectionnez l'option de chiffrement appropriée dans la liste déroulante TLS and SRTP Ciphers.



Redémarrez le service Cisco Call Manager sur chaque noeud en accédant à la page Cisco Unified Serviceability, Tools > Control Center-Feature Services et sélectionnez Cisco Call Manager sous CM Services

Accédez à la page Cisco Unity Connection Administration > System Settings > General Configurations et sélectionnez l'option de chiffrement appropriée dans la liste déroulante TLS and SRTP Ciphers.

Redémarrez Connection Conversation Manager sur chaque noeud en accédant à Cisco Unity Connection Serviceability > Tools > Service Management.

Options de chiffrement TLS avec ordre de priorité

Options de chiffrement TLS	Chiffres TLS en ordre de priorité
Plus solide - AES-256 SHA-384 uniquement : RSA préféré	• TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_A384 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SH
Strongest-AES-256 SHA-384 uniquement : ECDSA préféré	

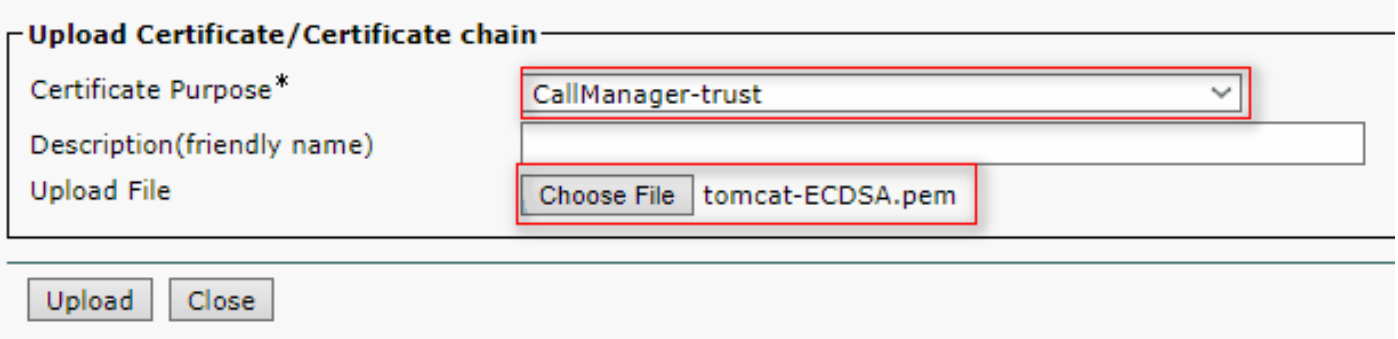
Moyen-AES-256 AES-128 uniquement : RSA préféré	4 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SH 4 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM _SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SH 6 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_ A256 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_ A384 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SH
Moyen-AES-256 AES-128 uniquement : ECDSA préféré	4 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_ A256 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SH 6 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SH 4 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_ A384
Tous les chiffrement RSA favoris (par défaut)	• TLS_ECDHE_RSA_WITH_AES_128_GCM_SH 6 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_ A256 • TLS_RSA_WITH_AES_128_CBC_SHA • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_ A384 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SH 4
Tous les chiffrements ECDSA favoris	• TLS_ECDHE_ECDSA_WITH_AES_128_GCM_ A256 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SH 6 • TLS_RSA_WITH_AES_128_CBC_SHA

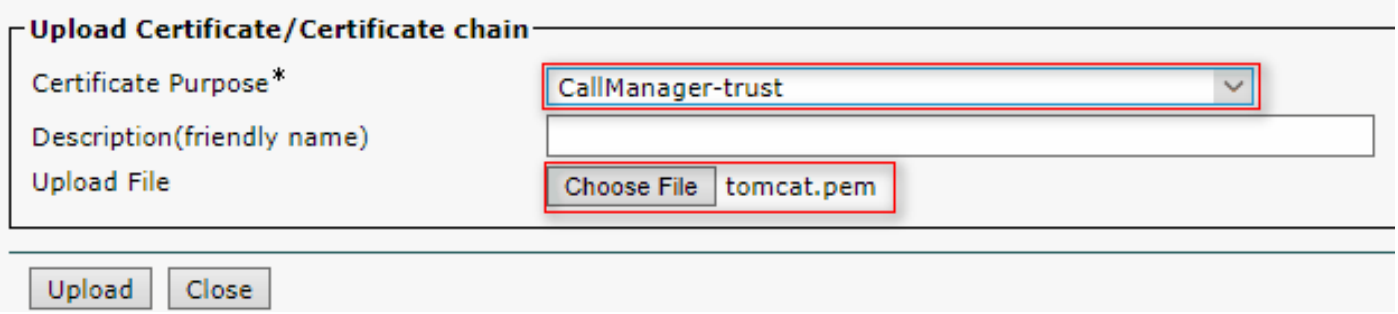
Options de chiffrement SRTP dans l'ordre de priorité

Option de chiffrement SRTP	SRTP dans l'ordre de priorité
Tous les chiffrement AES-256 et AES-128 pris en charge	• AEAD_AES_256_GCM • AEAD_AES_128_GCM • AES_CM_128_HMAC_SHA1 _32
AEAD AES-256, chiffrement AES-28 GCM	• AEAD_AES_256_GCM • AEAD_AES_128_GCM
Chiffres AEAD AES256 GCM uniquement	• AEAD_AES_256_GCM

4. Télécharger les certificats CUC Tomcat (basés sur RSA et EC)

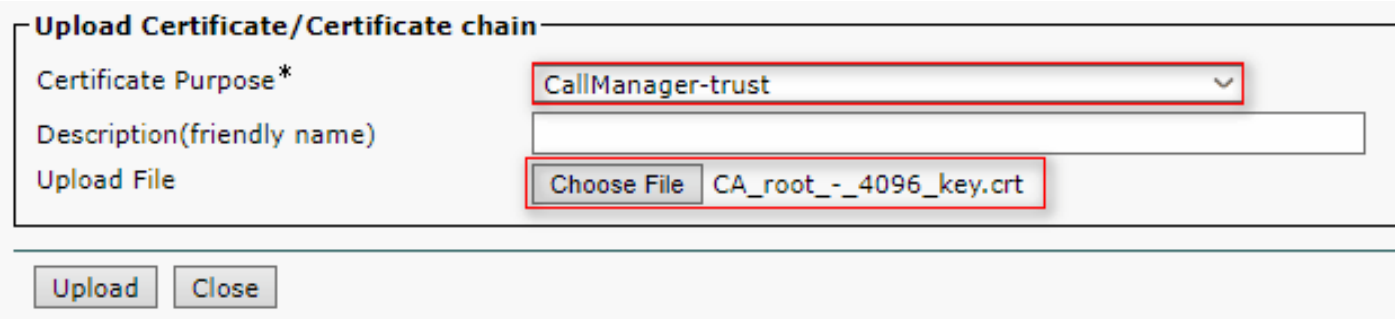
Accédez à Administration du système d'exploitation > Sécurité > Gestion des certificats et téléchargez les deux certificats Tomcat CUC (basés sur RSA et EC) dans le magasin CallManager-trust.





1. **Remarque** : le téléchargement des deux certificats Unity Tomcat n'est pas obligatoire si les chiffrement ECDSA sont négociés uniquement. Dans ce cas, le certificat Tomcat basé sur EC est suffisant.

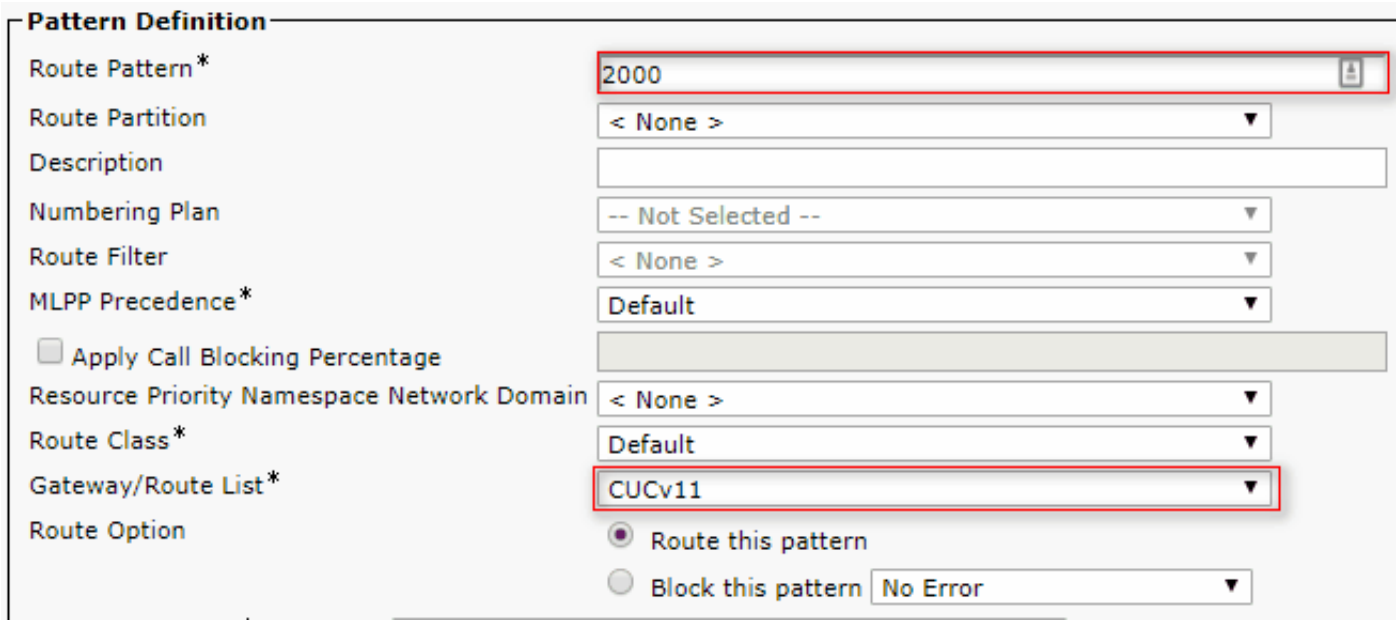
Dans le cas de certificats tiers, vous devez télécharger le certificat racine et le certificat intermédiaire de l'autorité de certification tierce. Ceci est nécessaire uniquement si l'autorité de certification tierce a signé votre certificat Unity Tomcat.



Redémarrez le processus Cisco Call Manager sur tous les noeuds pour appliquer les modifications.

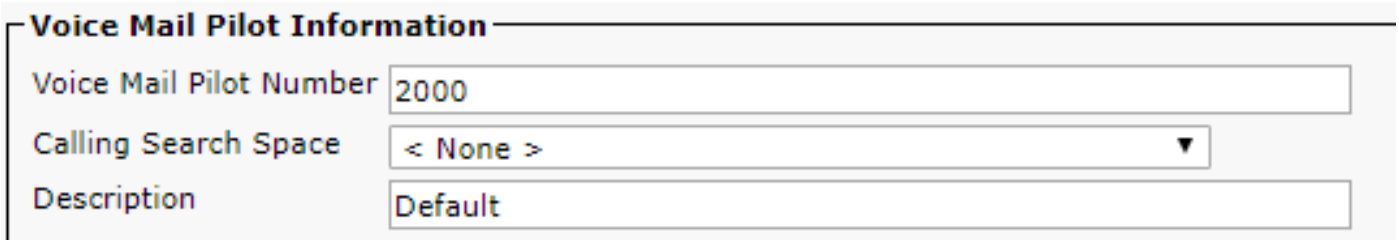
5. Créer un modèle de route

Configurez un modèle de route qui pointe vers l'agrégation configurée en naviguant jusqu'à Call Routing > Route/Hunt > Route Pattern. Le poste entré comme numéro de modèle de route peut être utilisé comme pilote de messagerie vocale.

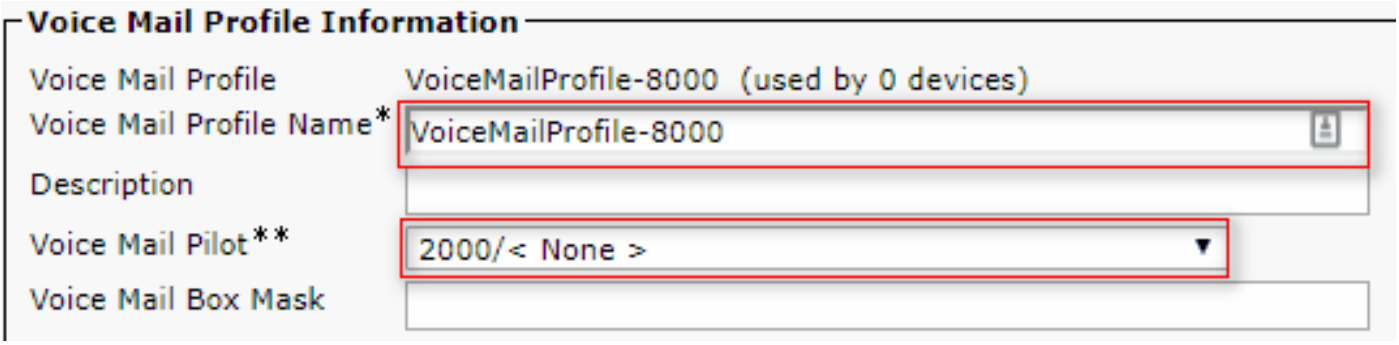


6. Créer un pilote de messagerie vocale, un profil de messagerie vocale et l'affecter aux numéros de répertoire

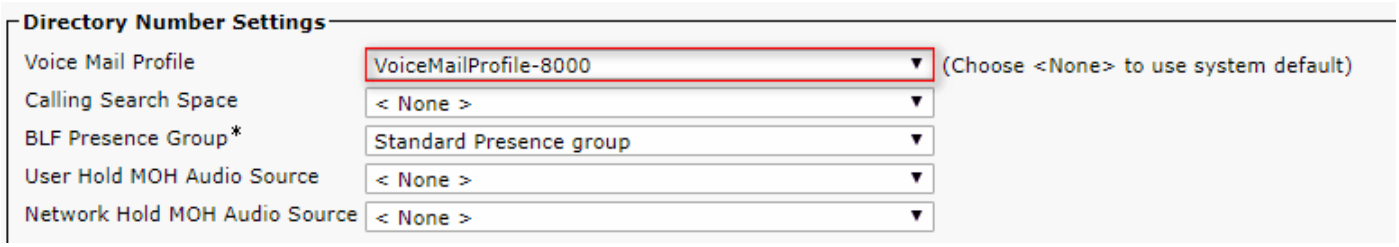
Créez un pilote de messagerie vocale pour l'intégration en accédant à Fonctionnalités avancées > Messagerie vocale > Pilote de messagerie vocale.



Créez un profil de messagerie vocale afin de lier tous les paramètres ensemble Fonctionnalités avancées > Messagerie vocale > Profil de messagerie vocale



Affectez le profil de messagerie vocale nouvellement créé aux numéros de répertoire destinés à utiliser l'intégration sécurisée en accédant à Call Routing > Directory number



Configurer - Signature de certificats basés sur la clé CE par une autorité de certification tierce (facultatif)

Les certificats peuvent être signés par une autorité de certification tierce avant de configurer l'intégration sécurisée entre les systèmes. Procédez comme suit pour signer les certificats sur les deux systèmes.

Cisco Unity Connection

1. Générer une demande de signature de certificat (CSR) pour CUC Tomcat-ECDSA et faire signer le certificat par une autorité de certification tierce
2. L'autorité de certification fournit un certificat d'identité (certificat signé par l'autorité de certification) et un certificat d'autorité de certification (certificat racine de l'autorité de certification) qui doivent être téléchargés comme suit :
   Télécharger le certificat racine CA dans le magasin tomcat-trust
   Télécharger le certificat d'identité dans le magasin tomcat-EDCS
3. Redémarrer le gestionnaire de conversations sur CUC

Cisco Unified CM

1. Générer CSR pour CUCM CallManager-ECDSA et faire signer le certificat par une autorité de certification tierce
2. L'autorité de certification fournit un certificat d'identité (certificat signé par l'autorité de certification) et un certificat d'autorité de certification (certificat racine de l'autorité de certification) qui doivent être téléchargés comme suit :
   Télécharger le certificat racine CA dans le magasin callmanager-trust
   Télécharger le certificat d'identité dans le magasin callmanager-EDCS
3. Redémarrer les services Cisco CCM et TFTP sur chaque noeud

Le même processus sera utilisé pour signer des certificats basés sur des clés RSA, où CSR est généré pour le certificat Tomcat CUC et le certificat CallManager et chargé dans le magasin tomcat et le magasin callmanager respectivement.

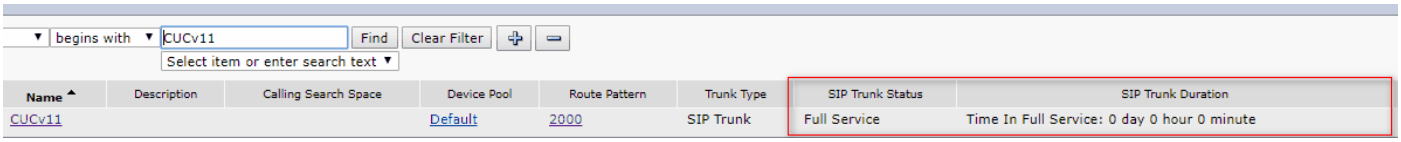
Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

Vérification de la ligne principale SIP sécurisée

Appuyez sur le bouton Messagerie vocale du téléphone pour appeler la messagerie vocale. Vous devez entendre le message d'accueil d'ouverture si le poste de l'utilisateur n'est pas configuré sur le système Unity Connection.

Vous pouvez également activer le keepalive des OPTIONS SIP pour surveiller l'état de la liaison SIP. Cette option peut être activée dans le profil SIP attribué à la ligne principale SIP. Une fois cette option activée, vous pouvez surveiller l'état de la liaison SIP via Device > Trunk, comme indiqué ci-dessous :



Vérification des appels RTP sécurisés

Vérifiez si l'icône de cadenas est présente sur les appels vers Unity Connection. Cela signifie que le flux RTP est chiffré (le profil de sécurité du périphérique doit être sécurisé pour qu'il fonctionne) comme le montre cette image

Informations connexes

- Guide d'intégration SIP pour Cisco Unity Connection version 11.x