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

Contenu

Introduction

Ce document décrit la configuration et la vérification de la connexion sécurisée de SIP entre le serveur du gestionnaire (CUCM) et du Cisco Unity Connection de Cisco Unified Communications (CUC) utilisant le cryptage de nouvelle génération.

La Sécurité de nouvelle génération au-dessus de l'interface de SIP limite l'interface de SIP pour utiliser des chiffrements de la suite B basés sur les protocoles 1.2, SHA-2 et AES256 de TLS. Il permet les diverses combinaisons des chiffrements basés sur la commande prioritaire des chiffrements RSA ou ECDSA. Pendant la transmission entre l'Unity Connection et le Cisco Unified CM, des chiffrements et les Certificats de tiers sont vérifiés les aux deux les extrémités. Est ci-dessous la configuration pour la prise en charge du chiffrement de nouvelle génération.

Si vous prévoyez de utiliser les Certificats signés par autorité de certification de tiers alors

commencent par le certificat signant à la fin de la section de configuration (configurez - en signant les Certificats basés par clé EC par le tiers CA)

Conditions préalables

Conditions requises

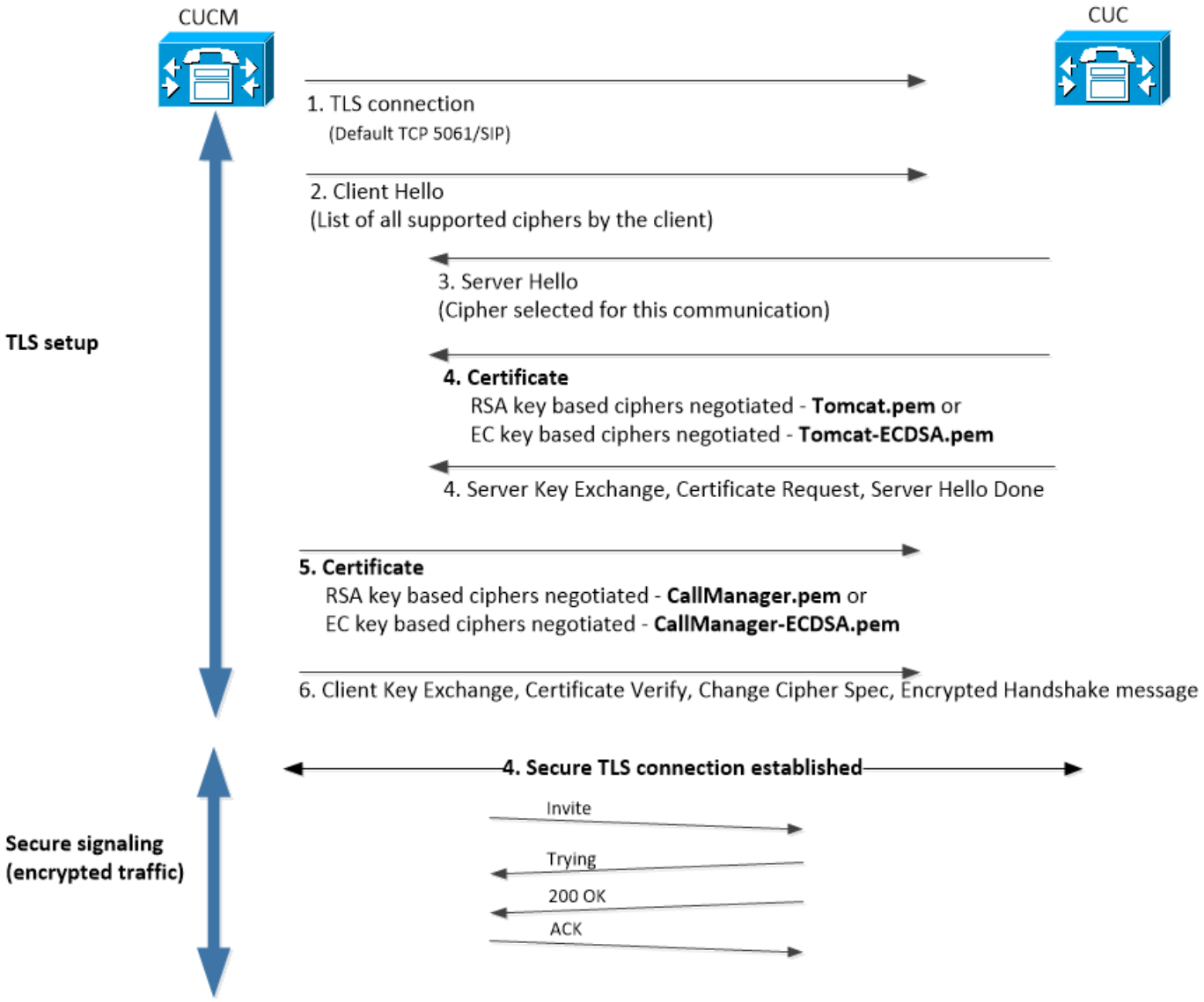
Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

Version 11.x et ultérieures CUCM dans le mode mixte
Version 11.x et ultérieures CUC

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Diagramme du réseau

Ce diagramme explique brièvement le processus que les aides établissent une connexion sécurisée entre CUCM et CUC une fois la nouvelle génération que la prise en charge du chiffrement est activée :



Conditions requises de certificat

Ce sont les conditions requises d'échange de certificat une fois que la prise en charge du chiffrement de nouvelle génération est activée sur le Cisco Unity Connection.

Auto-signé Certificats utilisés :

- Connexion d'Unity
  Aucun besoin de télécharger n'en délivrent un certificat. Le serveur d'Unity Connection téléchargera automatiquement l'ITLfile du serveur TFTP spécifié pendant la configuration et la confiance CallManager.pem et CallManager-EC.pem pendant la négociation de TLS.

- Cisco Unified CM
  Vous devez télécharger le Tomcat.pem et le Tomcat-EC.pem de la connexion d'Unity dans la mémoire de CallManager-confiance sur CUCM

Les Certificats CA de tierce partie utilisés :

- Connexion d'Unity

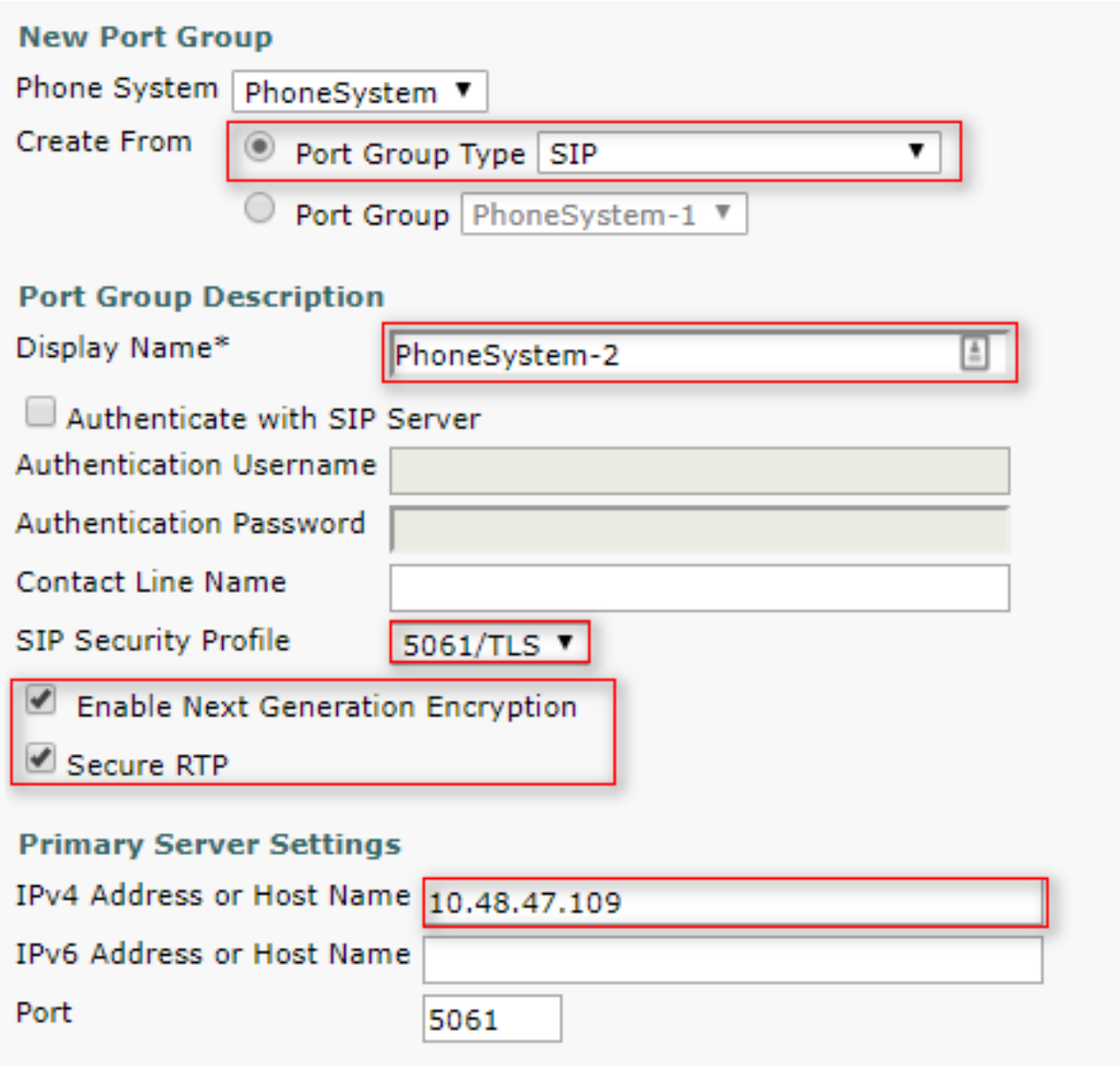
Vous devez télécharger la racine et tous les Certificats intermédiaires de l'autorité de certification de tiers de la CallManager-confiance de l'Unity Connection. Sur cela, le serveur de connexion téléchargera automatiquement l'ITLfile du serveur TFTP spécifié pendant la configuration et la confiance CallManager.pem et CallManager-EC.pem pendant la négociation de TLS.

- Cisco Unified CM
  Vous devez télécharger la racine et tous les Certificats intermédiaires de l'autorité de certification de tiers de la CallManager-confiance de l'Unified CM.

Configurez - Cisco Unity Connection (CUC)

1. Ajoutez un nouveau groupe de port

Naviguez vers la page de gestion de Cisco Unity Connection > l'intégration de téléphonie > le groupe de port et cliquez sur en fonction Add nouveau. Veillez à vérifier la case à cocher de cryptage de nouvelle génération d'enable.



1. **Note**: Le certificat de Cisco Tomcat de l'Unity Connection sera utilisé pendant la prise de contact SSL une fois que la case à cocher de cryptage de nouvelle génération d'enable est

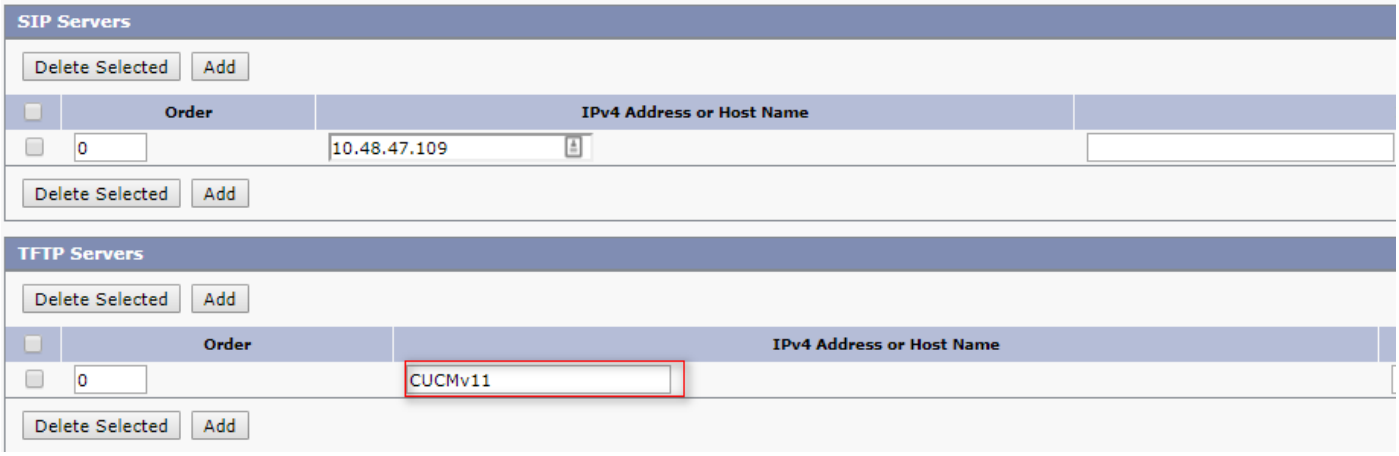
activée.

• Au cas où le chiffrement basé par ECDSA serait négocié alors le certificat basé principal EC Tomcat-ECDSA est utilisé dans la prise de contact SSL.

• Au cas où le chiffrement basé par RSA serait négocié alors le certificat de chat basé par clé RSA est utilisé dans la prise de contact SSL.

2. Ajoutez la référence de serveur TFTP

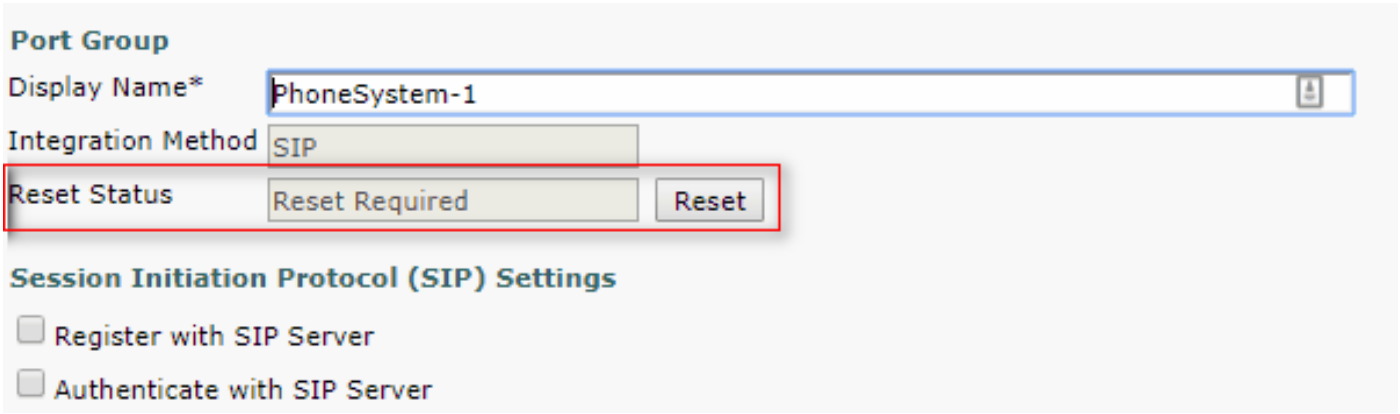
Sur le groupe de port que les fondements paginent, naviguent pour éditer > des serveurs et pour ajouter le FQDN du serveur TFTP de votre batterie CUCM. FQDN/Hostname du serveur TFTP doit apparier le nom commun (NC) du certificat de CallManager. L'adresse IP du serveur ne fonctionnera pas et elle aura comme conséquence le manque de télécharger le fichier ITL. Le nom DNS doit être donc résoluble par l'intermédiaire du serveur DNS configuré.



Redémarrez le gestionnaire de conversation Connection sur chaque noeud en naviguant vers l'utilité > les outils > la gestion des services de Cisco Unity Connection. Il est obligatoire pour que la configuration la prenne effet ce.

1. **Note**: Le fichier ITL de téléchargements de connexion d'Unity (ITLfile.tlv) du TFTP de CUCM utilisant le protocole de https relatif à 6972 sécurisés mettent en communication (URL : https://<CUCM-TFTP-FQDN>:6972/ITLFile.tlv). CUCM doit être dans le mode mixte puisque CUC recherche le certificat de fonction « CCM+TFTP » à partir du fichier ITL.

Naviguez de nouveau à la page de configuration de fondements d'intégration de téléphonie > de groupe de port > de groupe de port et remettez à l'état initial votre groupe nouvellement ajouté de port.



1. **Note**: Chaque fois le groupe de port est remis à l'état initial, le serveur CUC mettra son

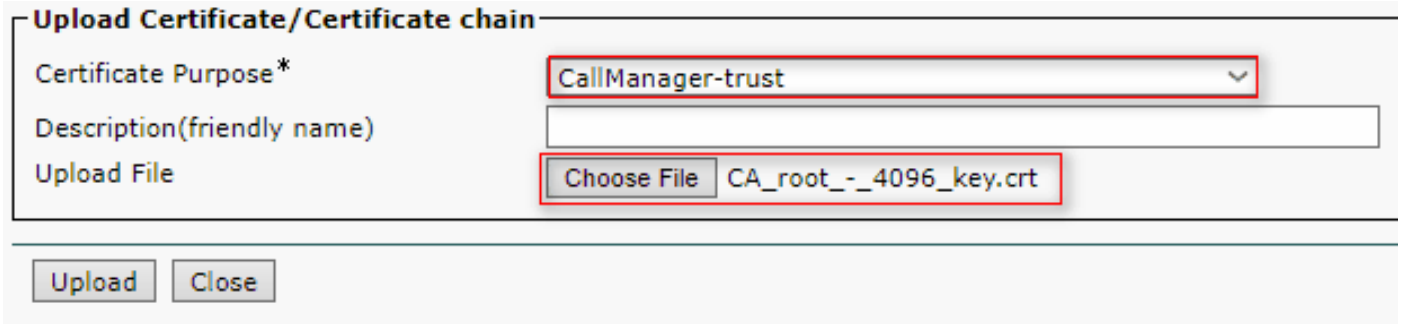
dossier à jour localement enregistré ITL en se connectant au serveur CUCM.

3. Ajoutez les ports de messagerie vocale

Naviguez de nouveau à l'intégration > au port de téléphonie et cliquez sur en fonction Add nouveau pour ajouter le port à votre groupe de création récente de port.

4. Racine du téléchargement CUCM et certificat intermédiaire du tiers CA

En cas de Certificats de tiers, vous devez télécharger la racine et le certificat intermédiaire de l'autorité de certification de tiers de la CallManager-confiance de l'Unity Connection. Ceci est nécessaire seulement si le tiers CA signait votre certificat de gestionnaire d'appel. Exécutez cette action en naviguant vers la gestion de SYSTÈME D'EXPLOITATION de Cisco Unified > la Gestion de Sécurité > de certificat et cliquez sur en fonction le certificat de téléchargement.

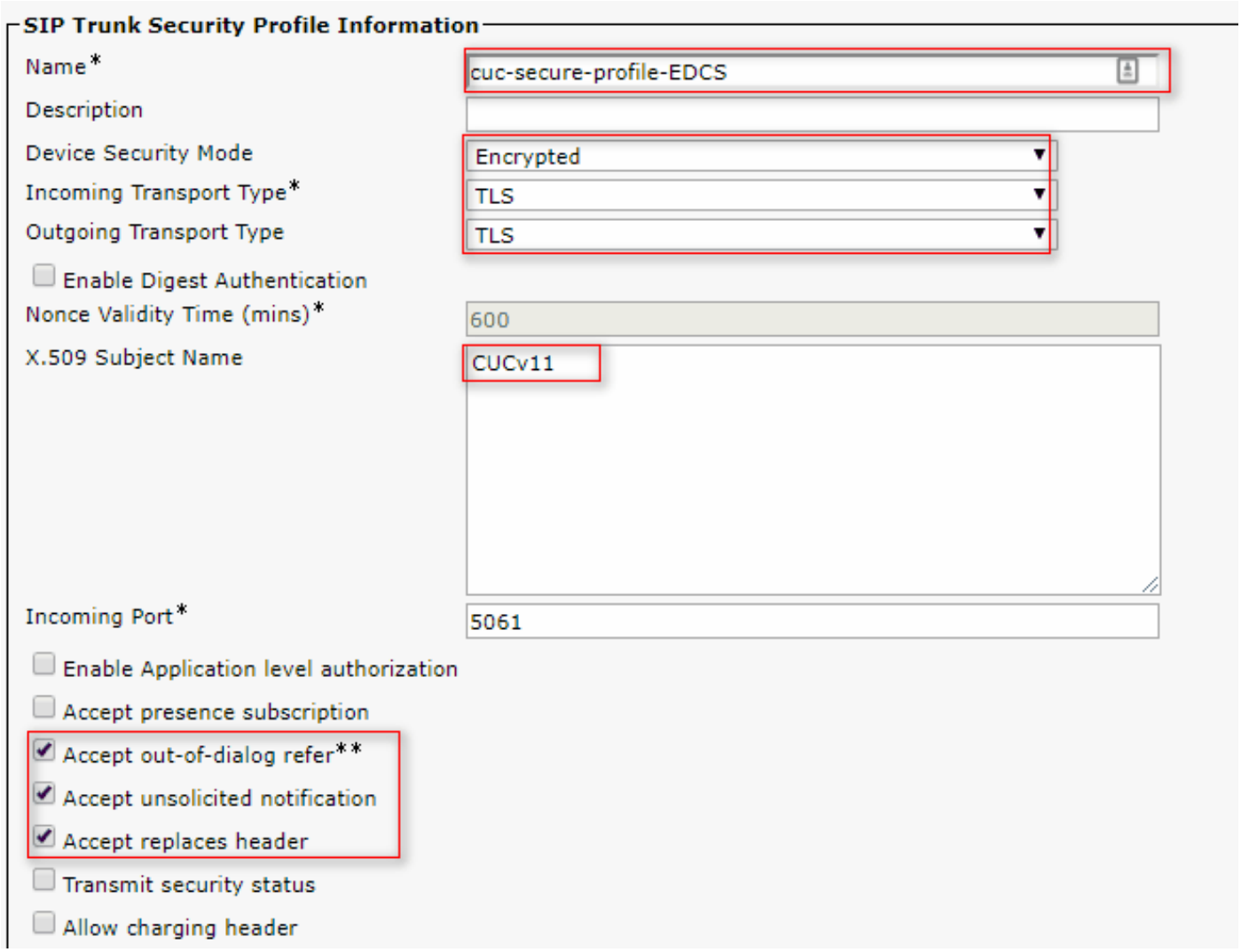


Configurez - Cisco Unified CM (CUCM)

1. Créez un profil de Sécurité de joncteur réseau de SIP

Naviguez profil de Sécurité vers la gestion CUCM > le système > la Sécurité > de SIP joncteur réseau et ajoutez un nouveau profil. Le nom du sujet X.509 doit apparier le FQDN du serveur

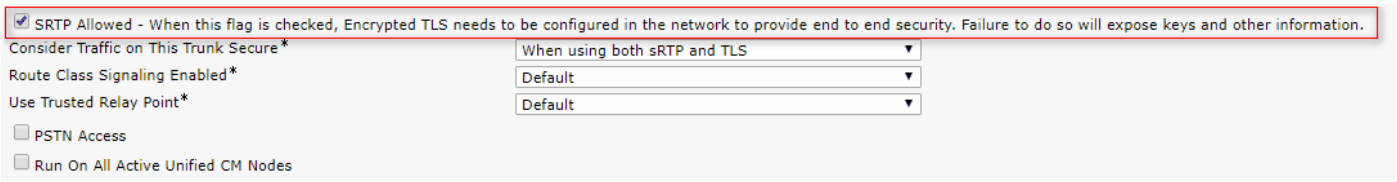
CUC.

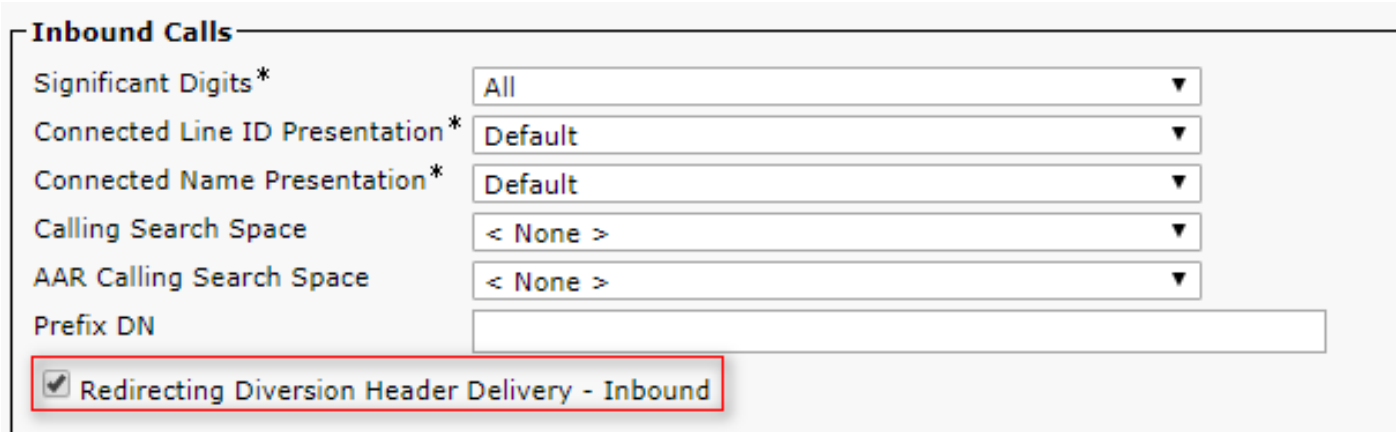


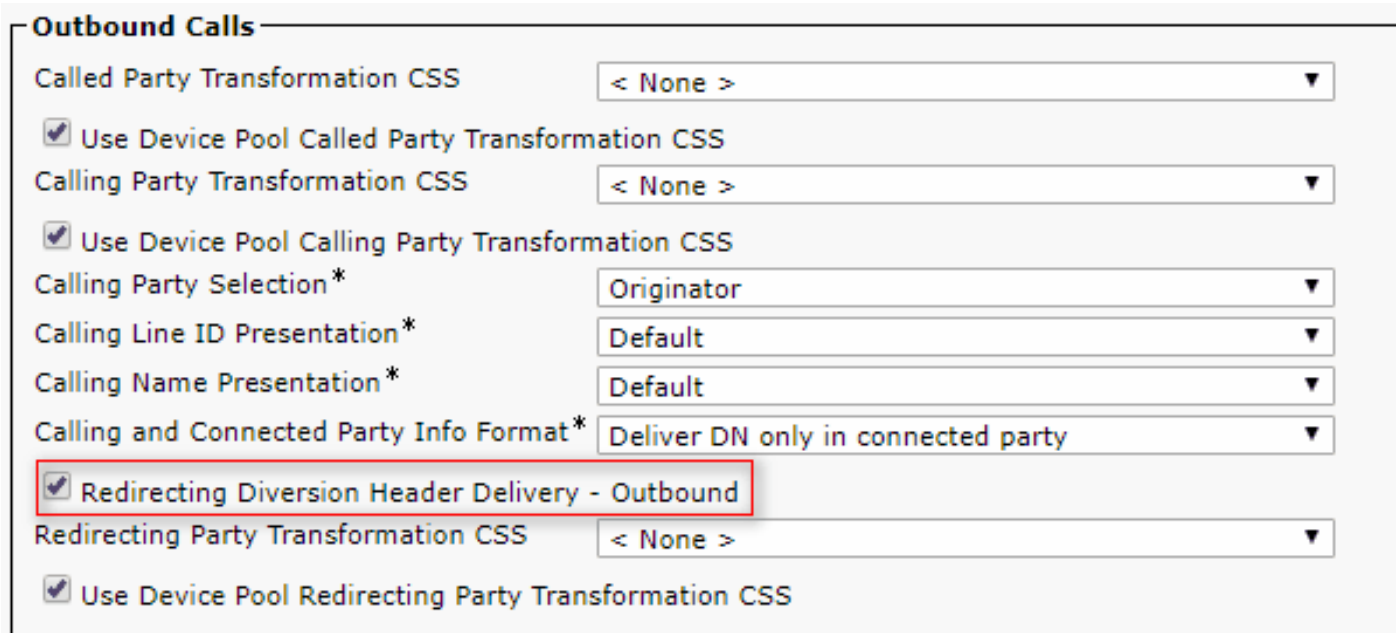
1. **Note**: La commande « CERT CLI d'exposition posséder le chat/tomcat.pem » peut afficher le certificat de chat basé par clé RSA sur l'Unity Connection. C'est NC doit apparier le nom du sujet X.509 configuré sur CUCM. La NC est égale à FQDN/Hostname du serveur d'Unity. Le certificat basé par clé EC contient le FQDN/hostname dans son domaine soumis du nom secondaire (SAN).

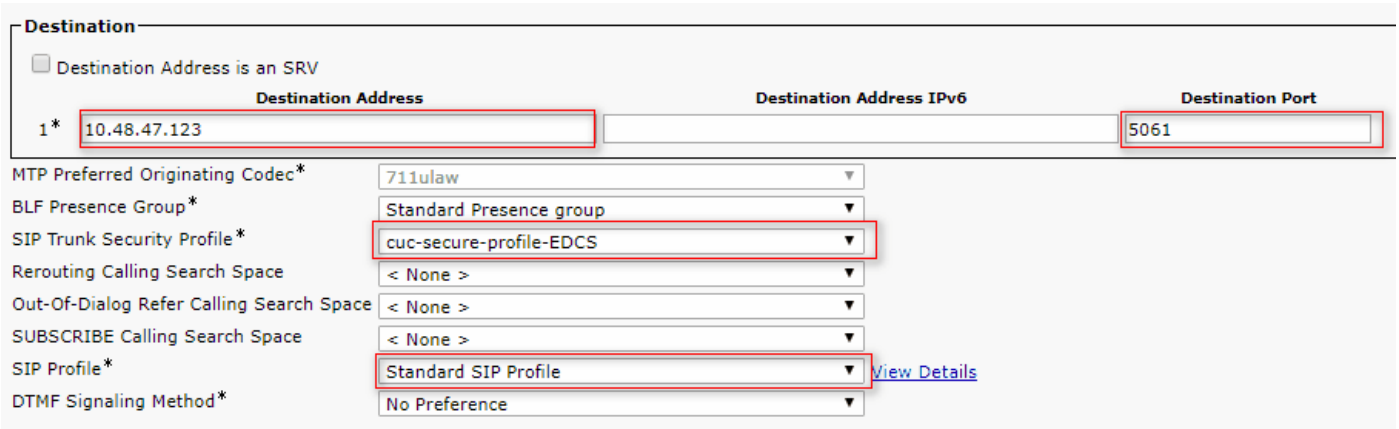
2. Créez un joncteur réseau sécurisé de SIP

Naviguez vers le périphérique > le joncteur réseau > le clic et ajoutez nouveau et créez un joncteur réseau standard de SIP qui sera utilisé pour l'intégration sécurisée avec l'Unity Connection.







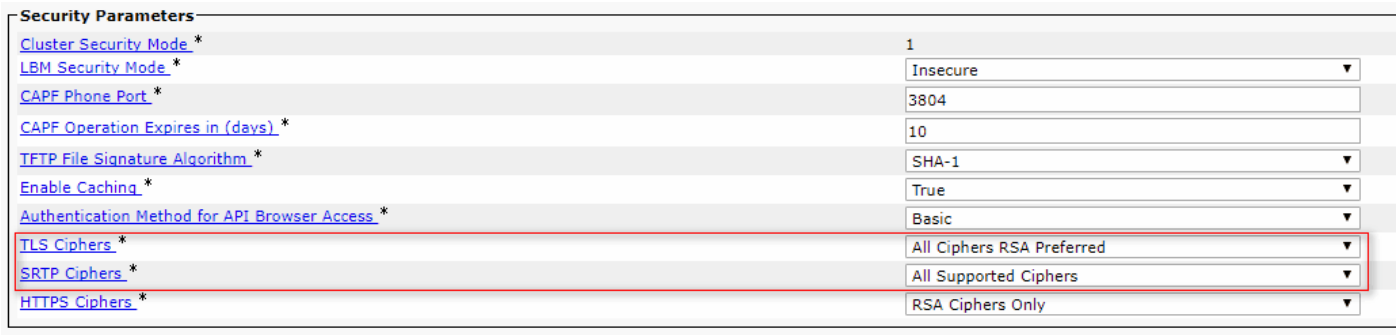


3. Configurez les chiffrements de TLS et SRTP

1. **Note**: La négociation entre l'Unity Connection et le Cisco Unified Communications Manager dépend de la configuration de chiffrement de TLS dans les conditions suivantes : Quand l'Unity Connection agit en tant que serveur, la négociation de chiffrement de TLS est basée sur la préférence sélectionnée par Cisco Unified CM.Au cas où le chiffrement basé par ECDSA serait négocié alors des Certificats basés principaux EC Tomcat-ECDSA sont utilisés dans la prise de contact SSL.Au cas où le chiffrement basé par RSA serait négocié alors des Certificats de chat basés par clé RSA sont utilisés dans la prise de contact SSL.Quand l'Unity Connection agit en tant que client, la négociation de chiffrement de TLS

est basée sur la préférence sélectionnée par l'Unity Connection.

Naviguez vers le Cisco Unified CM > les systèmes > les paramètres d'entreprise et sélectionnez l'option appropriée de chiffrement des chiffrements de TLS et SRTP de la liste déroulante.



Redémarrez le service de Cisco Call manager sur chaque noeud en naviguant vers la page d'utilité de Cisco Unified, les outils > les services de Centre-caractéristique de contrôle et sélectionnez le Cisco Call manager sous des services cm

Naviguez vers la page > les paramètres système > les configurations générales de gestion de Cisco Unity Connection et sélectionnez l'option appropriée de chiffrement des chiffrements de TLS et SRTP de la liste déroulante.

Redémarrez le gestionnaire de conversation Connection sur chaque noeud en naviguant vers l'utilité > les outils > la gestion des services de Cisco Unity Connection.

Options de chiffrement de TLS avec la commande prioritaire

Options de chiffrement de TLS	Chiffrements de TLS dans la commande prioritaire
L'AES-256 le plus fort SHA-384 seulement : RSA préférée	• TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
Strongest-AES-256 SHA-384 seulement : ECDSA préféré	• TLS_ECDHE_ECDSA_WITH_AES_256_GCM_A384 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SH

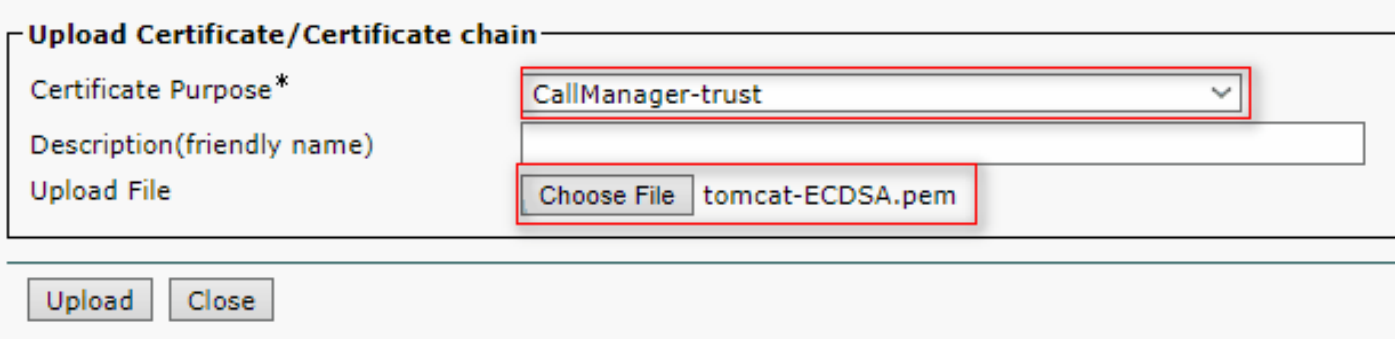
Medium-AES-256 AES-128 seulement : RSA préférée	4 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SH 4 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM _SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SH 6 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_ A256 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_ A384 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SH
Medium-AES-256 AES-128 seulement : 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 chiffrements RSA préférés (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 préférés	• TLS_ECDHE_ECDSA_WITH_AES_128_GCM_ A256 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SH 6 • TLS_RSA_WITH_AES_128_CBC_SHA

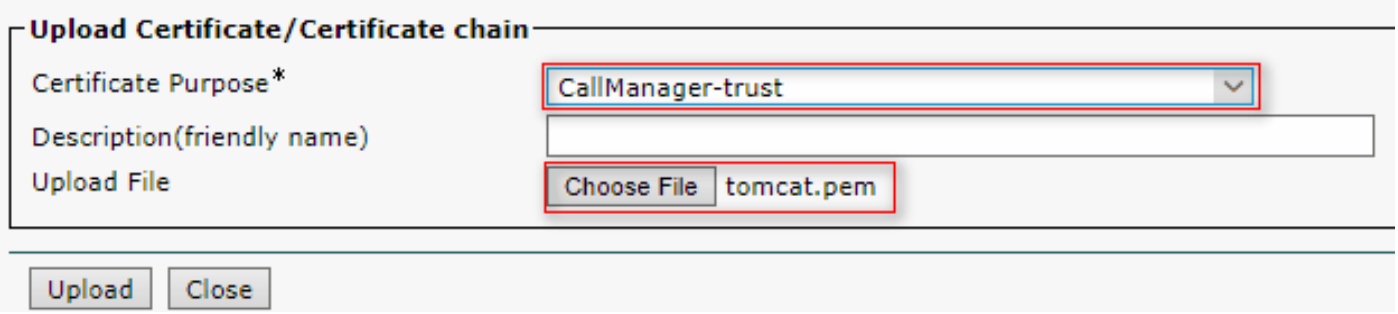
Options de chiffrement SRTP dans la commande prioritaire

Option de chiffrement SRTP	SRTP dans la commande prioritaire
Tout l'AES-256 pris en charge, chiffrements AES-128	• AEAD_AES_256_GCM • AEAD_AES_128_GCM • AES_CM_128_HMAC_SHA1_3 2
AEAD AES-256, chiffrements AES-28 basés sur GCM	• AEAD_AES_256_GCM • AEAD_AES_128_GCM
Chiffrements basés sur GCM AEAD AES256 seulement	• AEAD_AES_256_GCM

4. Certificats du téléchargement CUC Tomcat (RSA et EC basées)

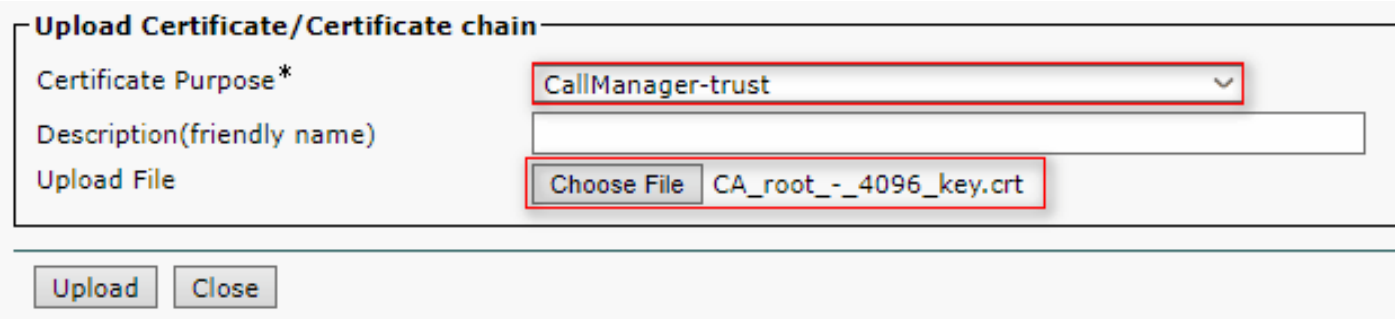
Naviguez vers la gestion de SYSTÈME D'EXPLOITATION > la Gestion de Sécurité > de certificat et téléchargez les deux Certificats CUC Tomcat (RSA et EC basées) dans la mémoire de CallManager-confiance.





1. **Note**: Télécharger les deux Certificats de Tomcat d'Unity n'est pas obligatoire si des chiffrements ECDSA sont négociés seulement. Dans une telle EC de cas basée le certificat de Tomcat est assez.

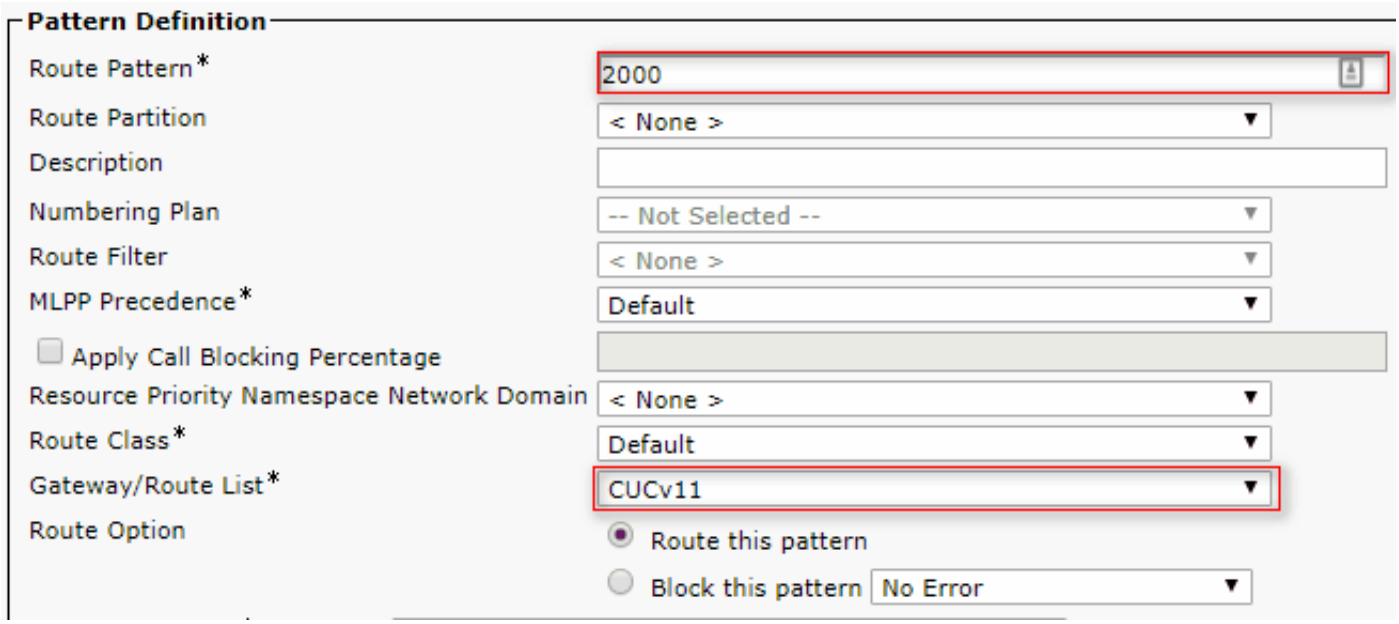
En cas de Certificats de tiers, vous devez télécharger la racine et le certificat intermédiaire de l'autorité de certification de tiers. Ceci est nécessaire seulement si le tiers CA signait votre certificat de Tomcat d'Unity.



Redémarrez le processus de Cisco Call manager sur tous les Noeuds pour appliquer les modifications.

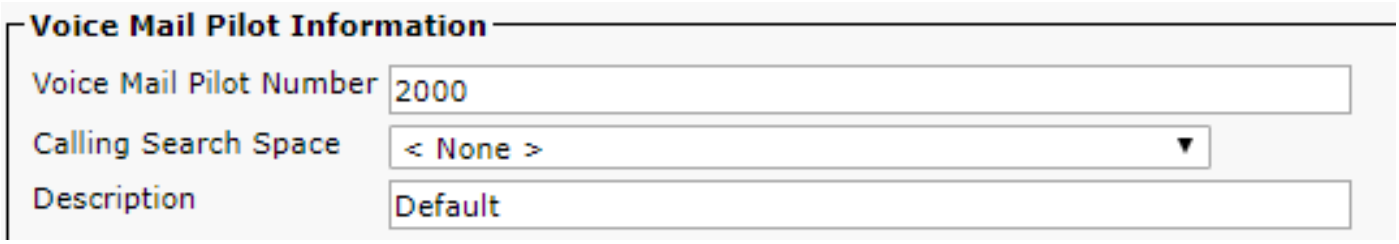
5. Créez le modèle d'artère

Configurez un modèle d'artère qui des points au joncteur réseau configuré en naviguant vers le routage d'appels > l'artère/recherche > le modèle d'artère. L'extension écrite comme nombre de modèle d'artère peut être utilisée en tant que pilote de messagerie vocale.

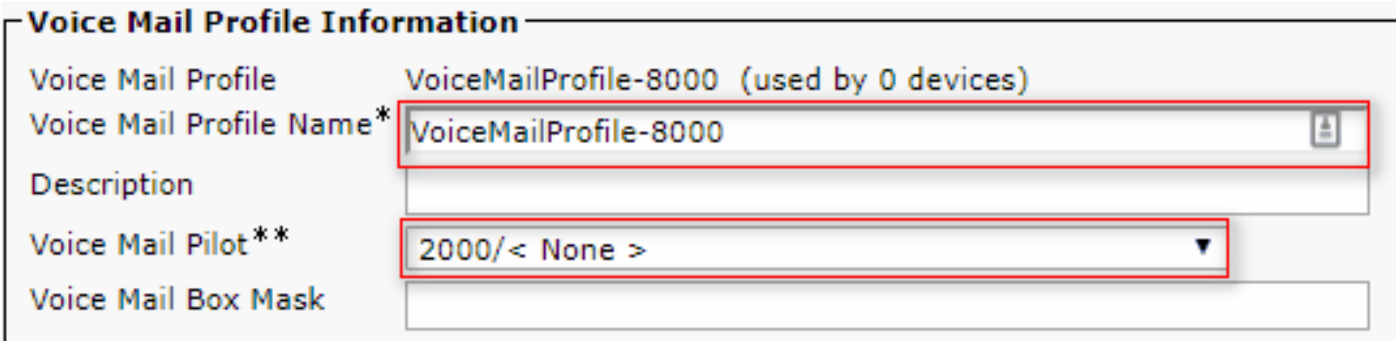


6. Créez le pilote de messagerie vocale, profil de messagerie vocale et affectez-le aux dn

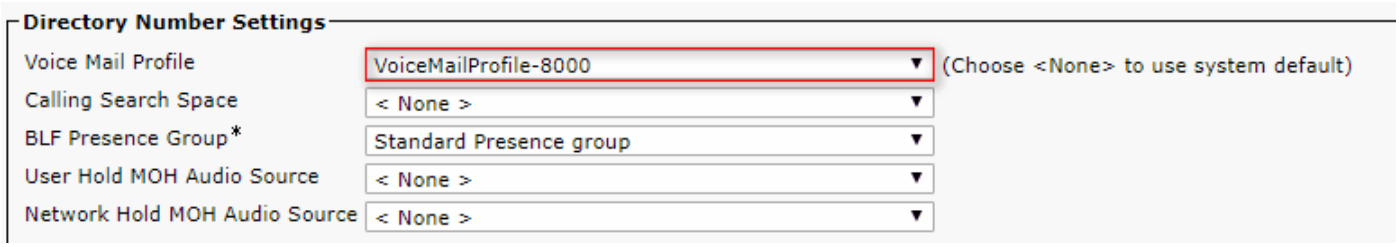
Créez un pilote de messagerie vocale pour l'intégration en allant à la fonctionnalité avancée > à la messagerie vocale > au pilote de messagerie vocale.



Créez un profil de messagerie vocale afin de joindre tous les fonctionnalité avancée de configurations ensemble > messagerie vocale > profil de messagerie vocale



Assignez le profil de création récente de messagerie vocale aux dn destinés pour utiliser l'intégration sécurisée en allant au nombre de routage d'appels > de répertoire



Configurez - La signature de la clé EC a basé des Certificats par le tiers le CA (facultatif)

Les Certificats pourraient être signés par un tiers CA avant d'installer l'intégration sécurisée entre les systèmes. Suivez les étapes suivantes pour signer les Certificats sur les deux systèmes.

Cisco Unity Connection

1. Générez la demande de signature de certificat (CSR) de CUC Tomcat-ECDSA et faites signer le certificat par le tiers CA
2. Le CA fournit le certificat d'identité (certificat signé CA) et le certificat de CA (certificat racine CA) qui doivent être téléchargés comme suivent :
   Téléchargez le certificat racine CA dans la mémoire de Tomcat-confiance
   Téléchargez le certificat d'identité dans la mémoire de Tomcat-EDCS
3. Gestionnaire de conversation de reprise sur CUC

Cisco Unified CM

1. Générez le CSR pour le CallManager-ECDSA CUCM et faites signer le certificat par le tiers CA
2. Le CA fournit le certificat d'identité (certificat signé CA) et le certificat de CA (certificat racine CA) qui doivent être téléchargés comme suivent :
   Téléchargez le certificat racine CA dans la mémoire de CallManager-confiance
   Téléchargez le certificat d'identité dans la mémoire de CallManager-EDCS
3. Redémarrez Cisco CCM et les services TFTP sur chaque noeud

Le même processus sera utilisé pour signer les Certificats basés par clé RSA où le CSR est généré pour le certificat CUC Tomcat et le certificat de CallManager et téléchargé dans la mémoire de chat et la mémoire de callmanager respectivement.

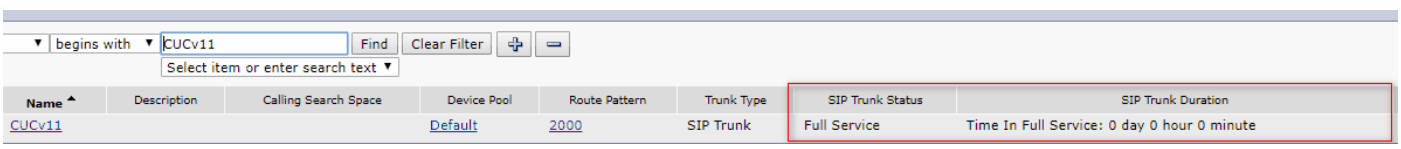
Vérifiez

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

Sécurisez la vérification de joncteur réseau de SIP

Appuyez sur le bouton de messagerie vocale au téléphone pour appeler la messagerie vocale. Vous devriez entendre le message d'accueil d'ouverture si l'extension de l'utilisateur n'est pas configurée sur le système d'Unity Connection.

Alternativement, vous pouvez permettre à la keepalive d'options de SIP de surveiller l'état de jonction de SIP. Cette option peut être activée dans le profil de SIP assigné au joncteur réseau de SIP. Une fois que ceci est activé vous pouvez surveiller l'état de jonction de sip par l'intermédiaire du périphérique > du joncteur réseau comme affiché ci-dessous :



Vérification sécurisée d'appel de RTP

Vérifiez si l'icône de cadenas est présente aux appels à l'Unity Connection. Il signifie que flot de RTP est chiffré (le profil de sécurité des périphériques doit être sécurisé pour qu'il fonctionne) suivant les indications de cette image

Informations connexes

- Guide d'intégration de SIP pour la release 11.x de Cisco Unity Connection