Configuration et dépannage de l'intégration sécurisée entre CUCM et CUC

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Diagramme
- Configuration - Liaison SIP sécurisée
  - Configurer CUC
    - 1. Ajouter un certificat SIP
    - 2. Créer un nouveau système téléphonique ou modifier le système par défaut
    - 3. Ajouter un nouveau groupe de ports
    - 4. Modifier les serveurs
    - 5. Réinitialisez le groupe de ports
    - 6. Ajouter des ports de messagerie vocale
    - 7. Télécharger le certificat racine CUC
  - Configurer CUCM
    - 1. Configurer le profil de sécurité de la liaison SIP pour la liaison vers CUC
    - 2. Configuration du profil SIP
    - 3. Créer une ligne principale SIP
    - 4. Créer un motif de routage
    - 5. Créer un pilote de messagerie vocale
    - 6. Créer un profil de messagerie vocale
    - 7. Attribuer un profil de messagerie vocale aux DN
    - 8. Télécharger le certificat racine CUC comme CallManager-trust
- Configuration des ports SCCP sécurisés
  - Configurer CUC
    - 1. Téléchargez le certificat racine CUC
    - 2. Créer un système téléphonique / Modifier celui qui existe.
    - 3. Ajouter un nouveau groupe de ports SCCP
    - 4. Modifier les serveurs
    - 5. Ajout de ports SCCP sécurisés
  - Configurer CUCM
    - 1. Ajouter des ports
    - 2. Télécharger le certificat racine CUC comme CallManager-trust
    - 3. Configuration des postes d'activation/désactivation MWI (Message Waiting Information)
    - 4. Créer un pilote de messagerie vocale
    - 5. Créer un profil de messagerie vocale
    - 6. Attribuer un profil de messagerie vocale aux DN
    - 7. Créer un groupe de recherche de messagerie vocale
- Vérifier
  - Vérification des ports SCCP
  - Vérification de la liaison SIP sécurisée

Vérification d'appel RTP sécurisé

Dépannage

1. Conseils généraux de dépannage

2. Traces à collecter

Problèmes courants

Cas 1 : Impossible d'établir une connexion sécurisée (alerte CA inconnue)

Cas 2 : Impossible de télécharger le fichier CTL à partir de CUCM TFTP

Cas 3 : Les ports ne sont pas enregistrés

Défauts

Introduction

Ce document décrit la configuration, la vérification et le dépannage de la connexion sécurisée entre Cisco Unified Communication Manager (CUCM) et le serveur Cisco Unity Connection (CUC).

Conditions préalables

Exigences

Cisco recommande que vous ayez connaissance de CUCM.

Référez-vous au Guide de sécurité de Cisco Unified Communications Manager pour plus de détails.

Remarque : Il doit être défini sur le mode mixte pour que l'intégration sécurisée fonctionne correctement.

Le chiffrement doit être activé pour Unity Connection 11.5(1) SU3 et versions ultérieures.

Commande CLI « utils cuc encryption <enable/disable> »

Composants utilisés

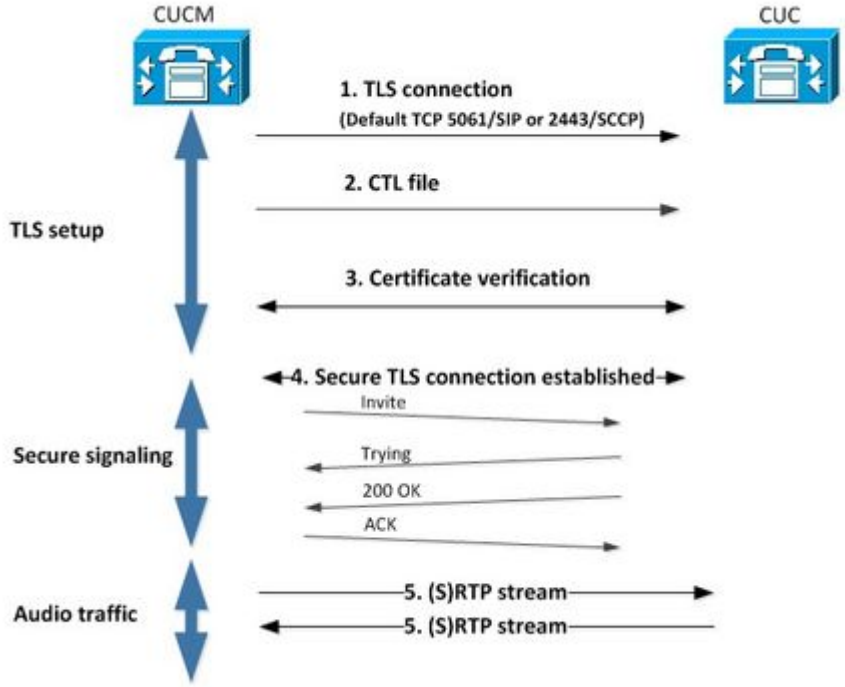
Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- CUCM version 10.5.2.11900-3.
- CUC version 10.5.2.11900-3.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Diagramme

Ce schéma explique brièvement le processus qui permet d'établir une connexion sécurisée entre CUCM et CUC :



1. Call Manager établit une connexion TLS (Transport Layer Security) sécurisée au serveur CUC sur le port 2443 SCCP (Skinny Call Control Protocol) ou 5061 SIP (Session Initiation Protocol) sur le protocole utilisé pour l’intégration.

2. Le serveur CUC télécharge le fichier CTL (Certificate Trust List) à partir du serveur TFTP (processus unique), extrait le certificat CallManager.pem et le stocke.

3. Le serveur CUCM offre le certificat Callmanager.pem qui est vérifié par rapport au certificat CallManager.pem obtenu à l'étape précédente. En outre, le certificat CUC est vérifié par rapport à un certificat racine CUC stocké dans CUCM. Notez que le certificat racine doit être téléchargé dans CUCM par l'administrateur.

4. Si la vérification des certificats réussit, une connexion TLS sécurisée est établie. Cette connexion est utilisée pour échanger des signaux SCCP ou SIP chiffrés.

5. Le trafic audio peut être échangé en tant que Real-time Transport Protocol (RTP) ou SRTP.

Remarque : Lorsque vous établissez une communication TLS, CUCM et CUC utilisent l'authentification mutuelle TLS. Référez-vous à RFC5630 pour plus d'informations.

Configuration - Liaison SIP sécurisée

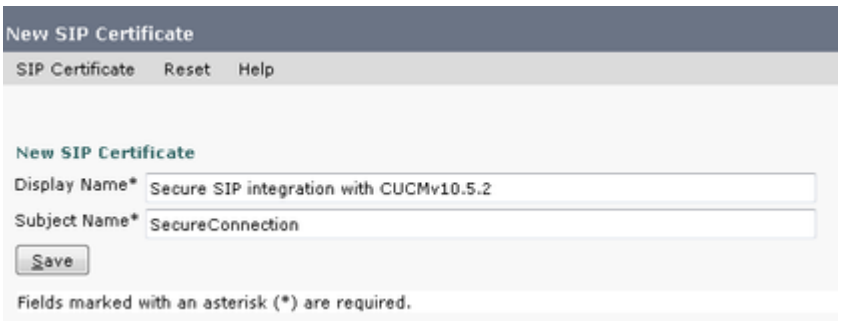
Configurer CUC

1. Ajouter un certificat SIP

Accédez à CUC Administration > Telephony Integrations > Security > SIP Certificate > Add new

- Nom complet : <tout nom significatif>
- Nom du sujet : <tout nom, par exemple, SecureConnection>

Remarque : le nom du sujet doit correspondre au nom du sujet X.509 dans le profil de sécurité de la ligne principale SIP (configuré à l'étape 1 de la configuration de CUCM plus loin dans ce document).

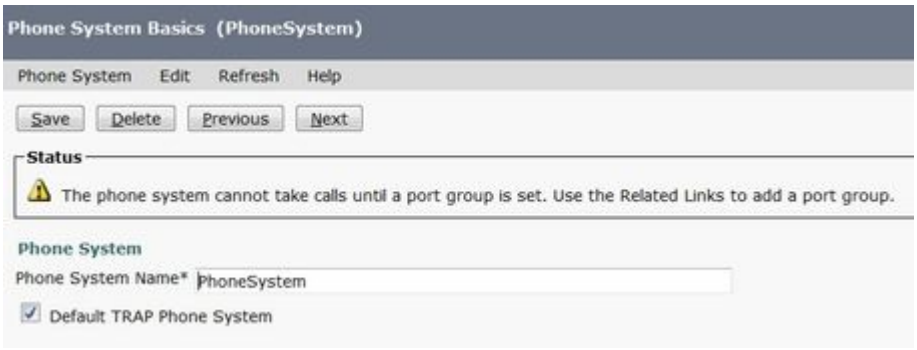


Remarque : Le certificat est généré et signé par le certificat racine CUC.

2. Créer un nouveau système téléphonique ou modifier le système par défaut

Accédez à Telephony Integration > Phone System. Vous pouvez utiliser le système téléphonique

existant ou en créer un nouveau.

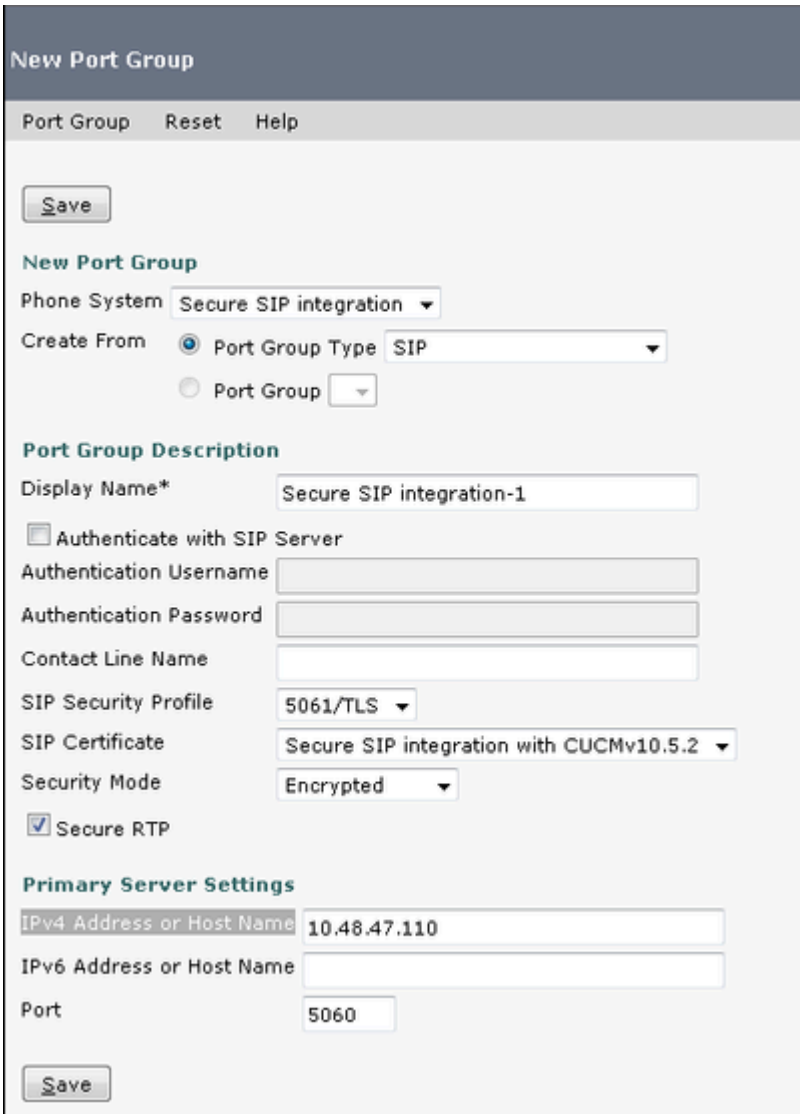


3. Ajouter un nouveau groupe de ports

Sur la page Phone System Basics, dans la zone déroulante Related Links, sélectionnez Add Port Group et cliquez sur Go. Dans la fenêtre de configuration, saisissez les informations suivantes :

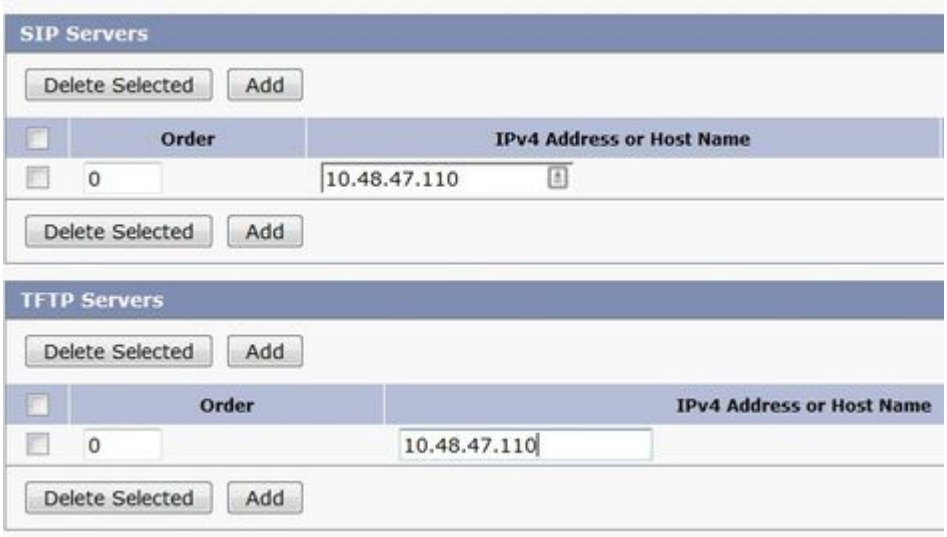
- Système téléphonique :
- Créer à partir de : Type de groupe de ports SIP
- Profil de sécurité SIP : 5061/TLS
- Certificat SIP :
- Mode de sécurité : Chiffré
- RTP sécurisé : Coché
- Adresse IPv4 ou nom d'hôte :

Appuyez sur Enregistrer.



4. Modifier les serveurs

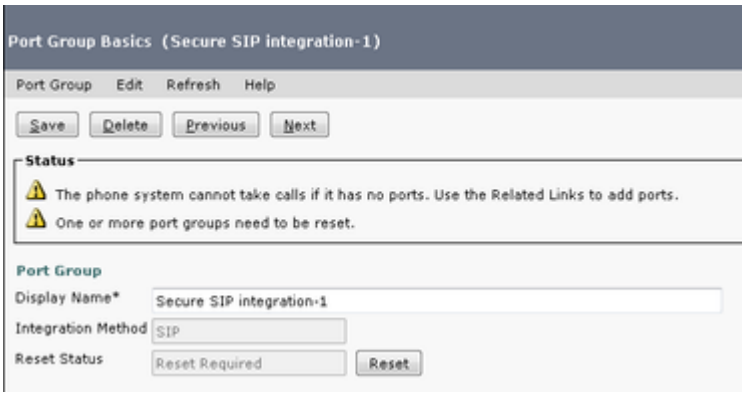
Naviguez jusqu'à Edit > Servers et ajoutez le serveur TFTP à partir du cluster CUCM comme illustré dans cette image.



Remarque : Il est important de fournir une adresse TFTP correcte. Le serveur CUC télécharge le fichier CTL à partir de ce TFTP comme expliqué.

5. Réinitialisez le groupe de ports

Revenez à Notions de base sur les groupes de ports et réinitialisez le groupe de ports en fonction des invites du système, comme illustré dans cette image.

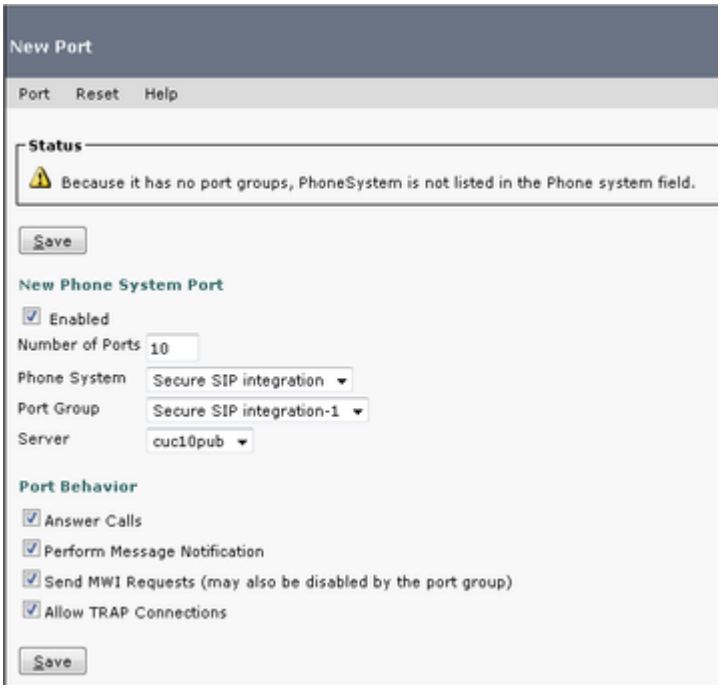


6. Ajouter des ports de messagerie vocale

Sur la page Notions de base sur les groupes de ports, dans la liste déroulante Liens associés, sélectionnez Ajouter des ports et sélectionnez Exécuter. Dans la fenêtre de configuration, entrez les informations suivantes :

- Activée: Coché
- Nombre de ports :
- Système téléphonique :

- Groupe de ports :
- Serveur :
- Comportement du port :



7. Télécharger le certificat racine CUC

Accédez à Telephony Integrations > Security > Root Certificate, cliquez avec le bouton droit sur l'URL pour enregistrer le certificat en tant que fichier nommé <filename>.0 (l'extension de fichier doit être .0 plutôt que .htm)' et cliquez sur save comme illustré dans cette image.



Configurer CUCM

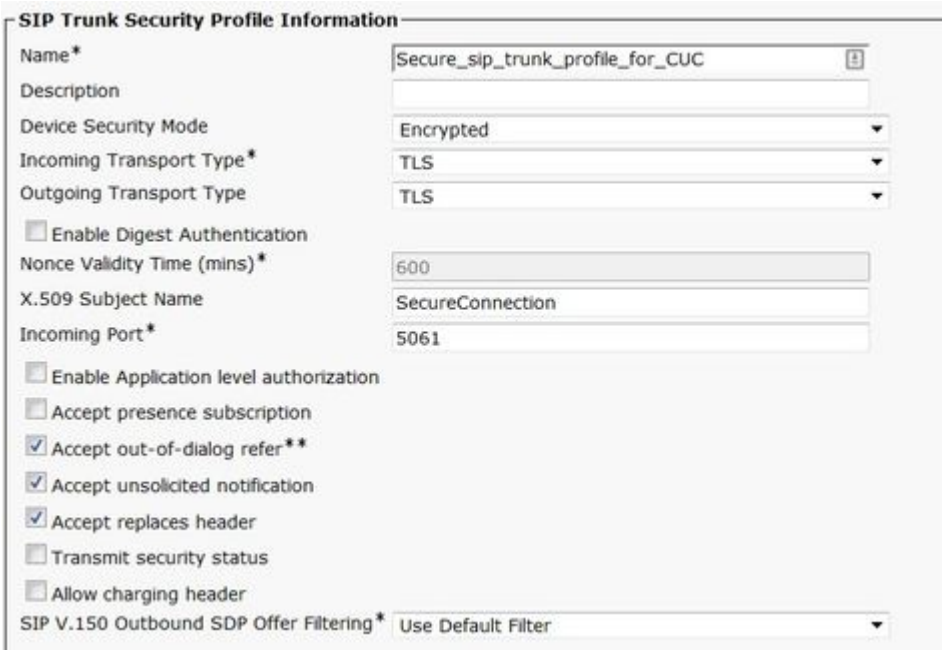
1. Configurer le profil de sécurité de la liaison SIP pour la liaison vers CUC

Accédez à CUCM Administration > System > Security > SIP Trunk Security Profile > Add new

Assurez-vous que ces champs sont correctement remplis :

- Mode de sécurité des périphériques : Chiffré
- Nom du sujet X.509 : Connexion sécurisée>
- Accepter hors dialogue se référer : quadrillé
- Accepter les notifications non sollicitées : quadrillé
- Accepter remplace en-tête : quadrillé

Remarque : Le nom du sujet X.509 doit correspondre au champ Nom du sujet dans le certificat SIP sur le serveur Cisco Unity Connection (configuré à l'étape 1 de la configuration CUC).

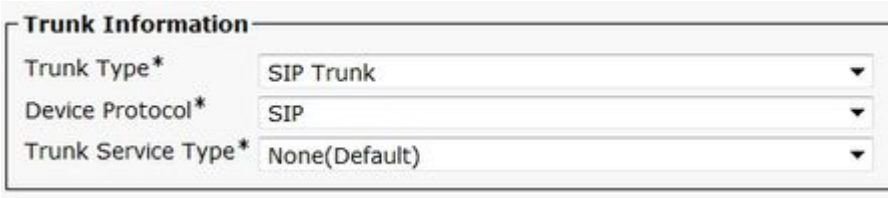


2. Configuration du profil SIP

Accédez à Device > Device Settings > SIP Profile si vous devez appliquer des paramètres spécifiques. Sinon, vous pouvez utiliser le profil SIP standard.

3. Créer une ligne principale SIP

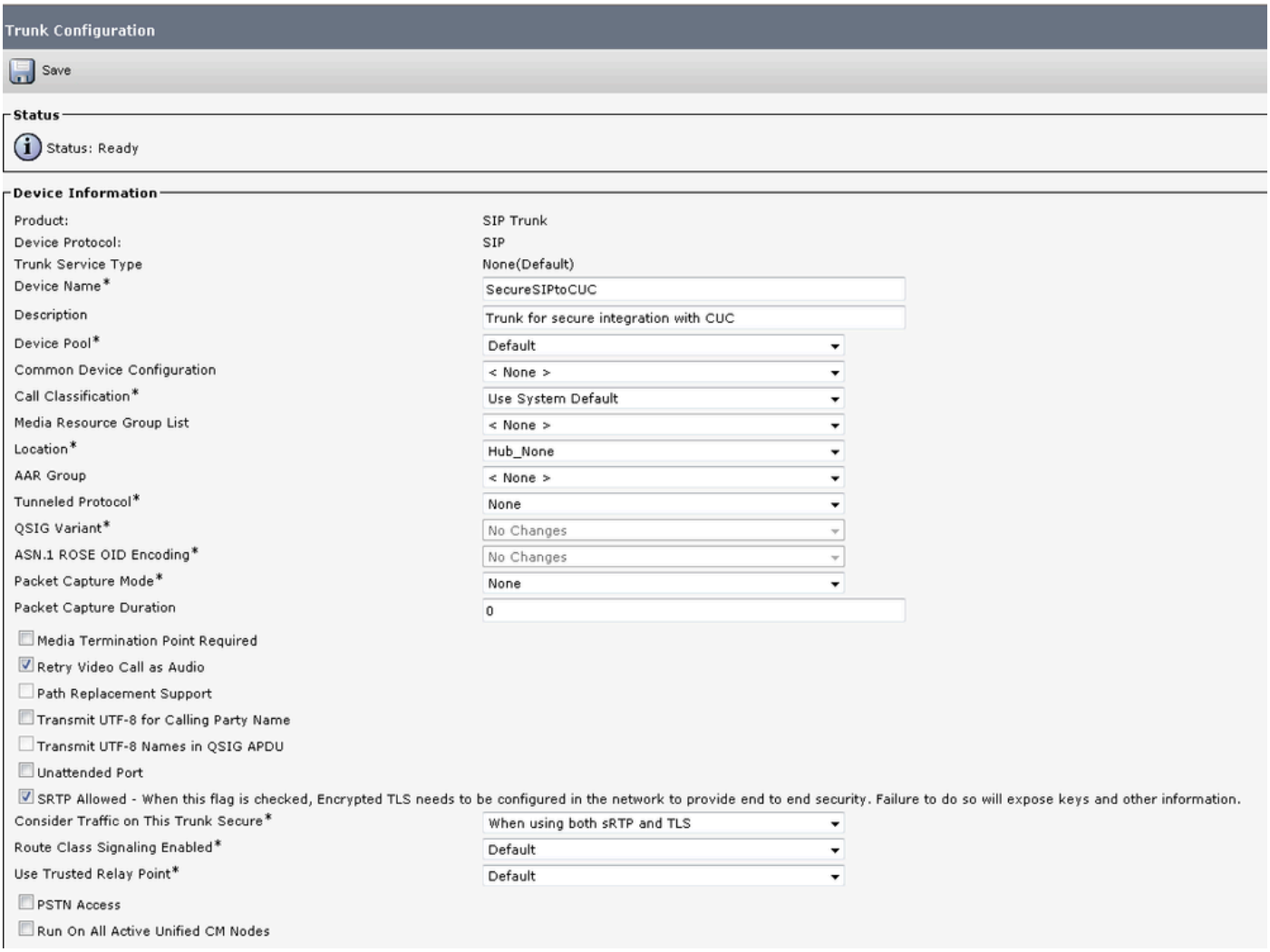
Accédez à Device > Trunk > Add new.Créez une ligne principale SIP qui est utilisée pour l'intégration sécurisée avec Unity Connection comme illustré dans cette image.



Dans la section Device Information de la configuration d'agrégation, entrez les informations suivantes :

- Nom du périphérique :
- Groupe de périphériques:
- SRTP autorisé : Coché

Remarque : Assurez-vous que le groupe CallManager (dans la configuration du pool de périphériques) contient tous les serveurs configurés dans CUC (Groupe de ports > Modifier > Serveurs).



Dans la section Appels entrants de la configuration de jonction, entrez les informations suivantes :

- Espace de recherche des appels :
- Redirection de remise d'en-tête de renvoi - Entrant : Coché



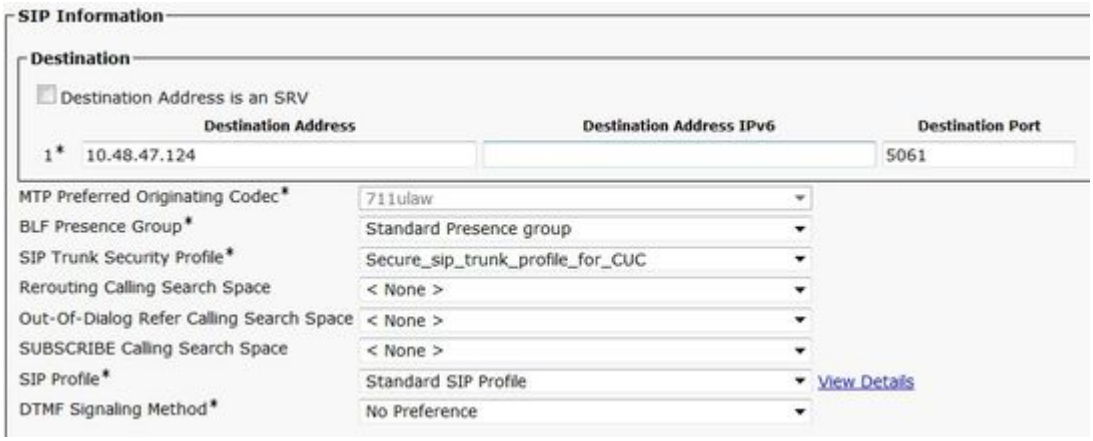
Dans la section Appels sortants de la configuration de ligne réseau, entrez les informations suivantes :

- Redirection de remise d'en-tête de renvoi - Sortant : quadrillé



Dans la section SIP Information de la configuration de la ligne principale, saisissez les informations suivantes :

- adresse de destination:
- Profil de sécurité de la ligne principale SIP :
- Reroutage Espace de recherche des appels :
- Out-of-Dialog Référez Espace de recherche d'appels :
- Profil SIP :

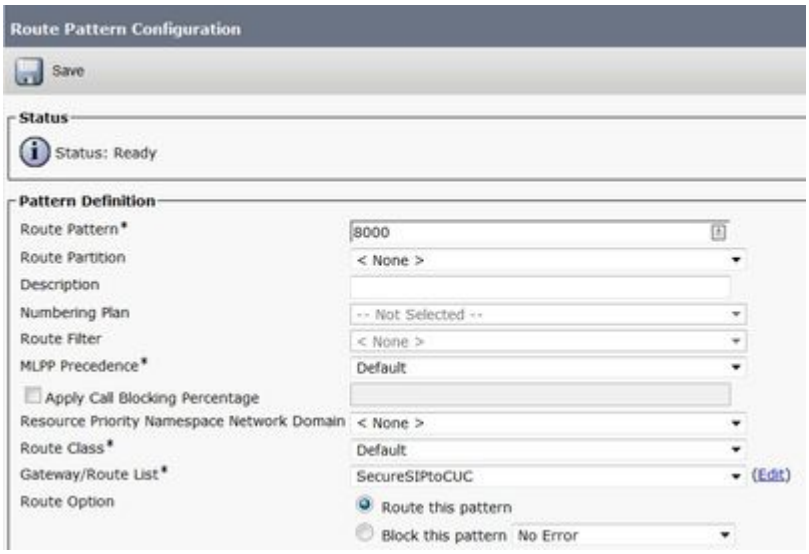


Réglez les autres paramètres en fonction de vos besoins.

4. Créer un motif de routage

Créez un modèle de route qui pointe vers l'agrégation configurée (Routage des appels > Route/Hunt > Modèle de route). Le poste saisi comme numéro de modèle de routage peut être utilisé comme pilote de messagerie vocale. Saisissez les informations suivantes :

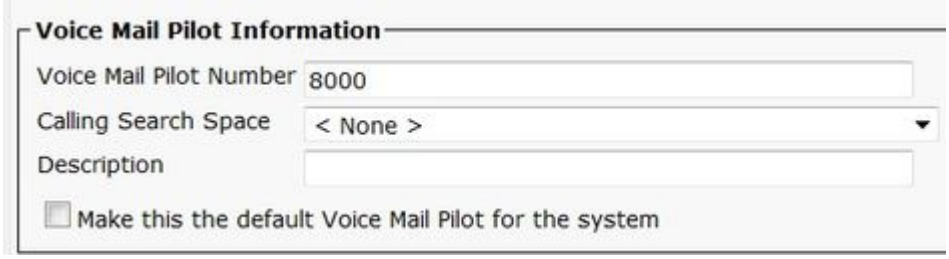
- Modèle de route :
- Liste des passerelles/routes :



5. Créer un pilote de messagerie vocale

Créez un pilote de messagerie vocale pour l'intégration (Fonctionnalités avancées > Messagerie vocale > Pilote de messagerie vocale). Entrez les valeurs suivantes :

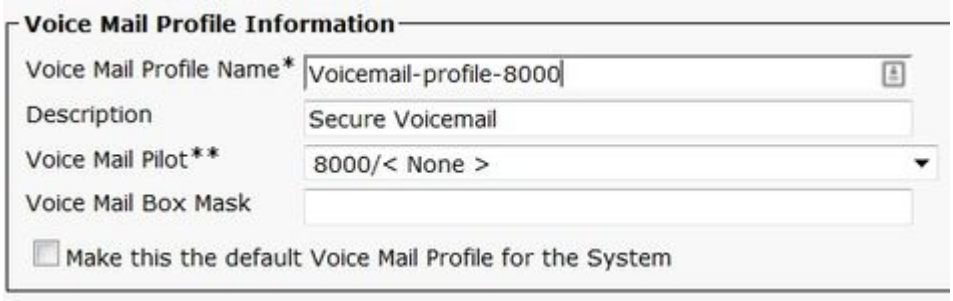
- Numéro pilote de la messagerie vocale :
- Espace de recherche des appels : qui inclut des partitions contenant un modèle de route utilisé comme pilote>



6. Créer un profil de messagerie vocale

Créez un profil de messagerie vocale afin de lier tous les paramètres ensemble (Advanced Features > Voice Mail > Voice Mail Profile). Saisissez les informations suivantes :

- Pilote de messagerie vocale :
- Masque de boîte vocale :

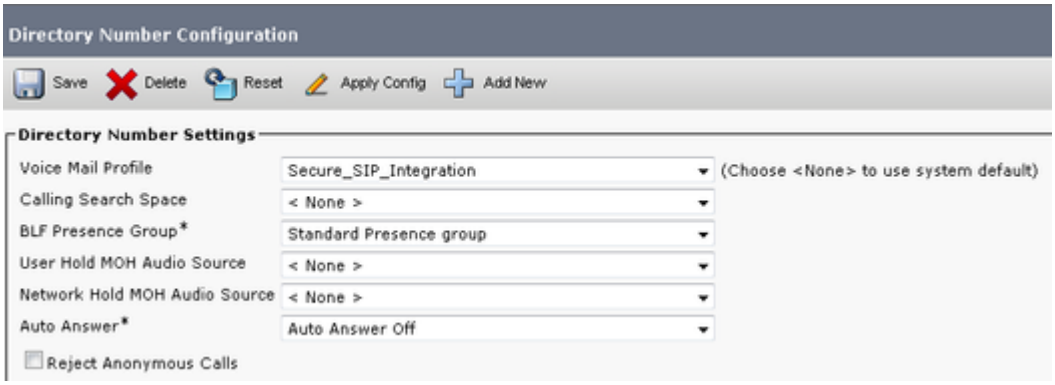


7. Attribuer un profil de messagerie vocale aux DN

Attribuez le profil de messagerie vocale aux DN destinés à utiliser une intégration sécurisée. N'oubliez pas de cliquer sur le bouton « Apply Config » après avoir modifié les paramètres DN :

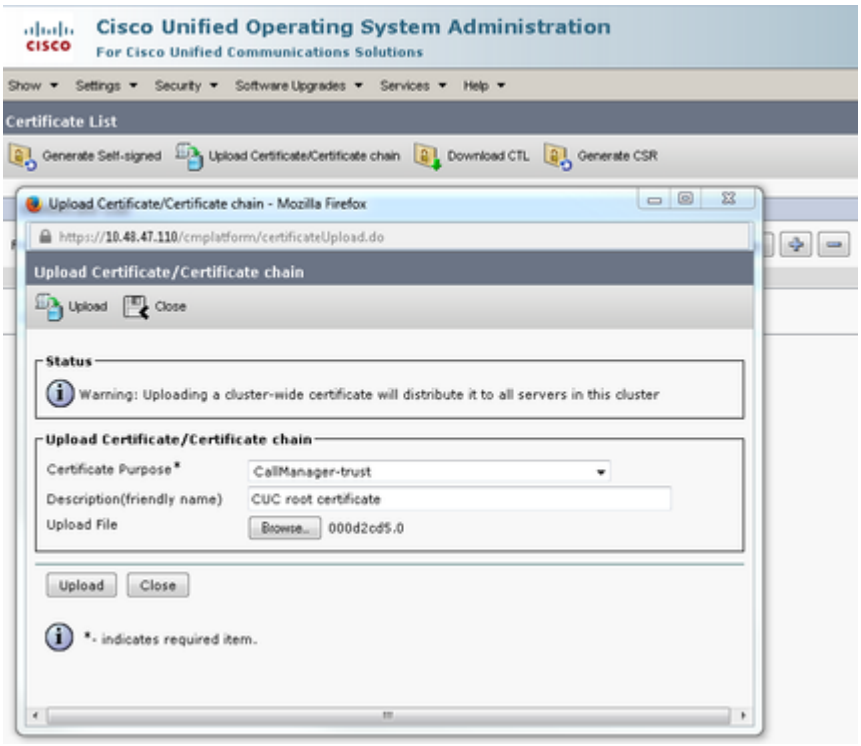
Naviguez jusqu'à l'adresse : Routage des appels > Numéro et modification du répertoire :

- Profil de messagerie vocale : Intégration_SIP_sécurisée



8. Télécharger le certificat racine CUC comme CallManager-trust

Accédez à OS Administration > Security > Certificate Management > Upload Certificate/Certificate Chain et téléchargez le certificat racine CUC en tant que CallManager-trust sur tous les noeuds configurés pour communiquer avec le serveur CUC.



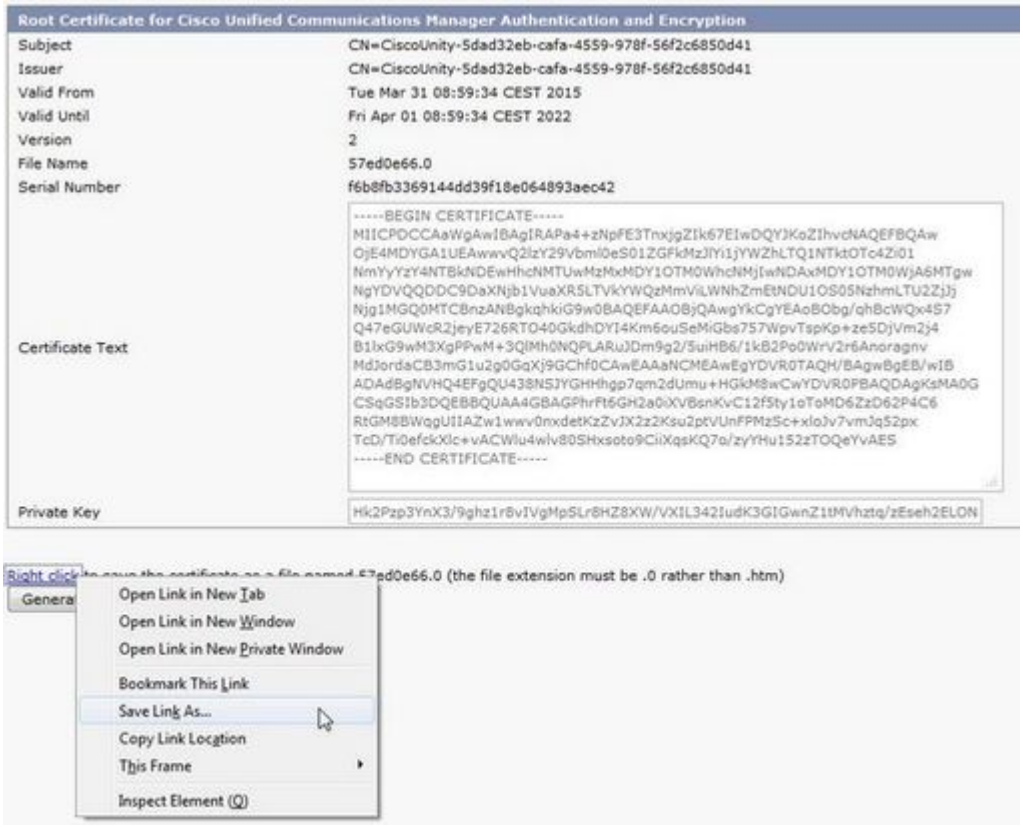
Remarque : le service Cisco CallManager doit être redémarré après le téléchargement du certificat pour que le certificat prenne effet.

Configuration des ports SCCP sécurisés

Configurer CUC

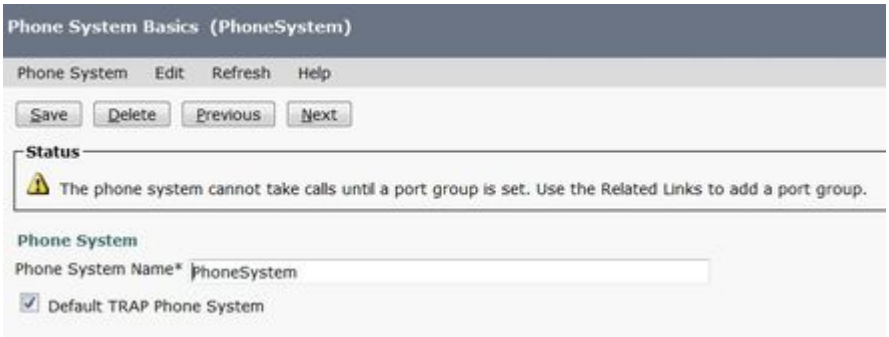
1. Télécharger le certificat racine CUC

Accédez à CUC Administration > Telephony Integration > Security > Root Certificate. Cliquez avec le bouton droit sur l'URL pour enregistrer le certificat en tant que fichier nommé <nom du fichier>.0 (l'extension du fichier doit être .0 au lieu de .htm)' et cliquez sur Enregistrer :



2. Créer un système téléphonique / Modifier celui qui existe.

Accédez à Telephony Integration > Phone system. Vous pouvez utiliser le système téléphonique existant ou en créer un nouveau.



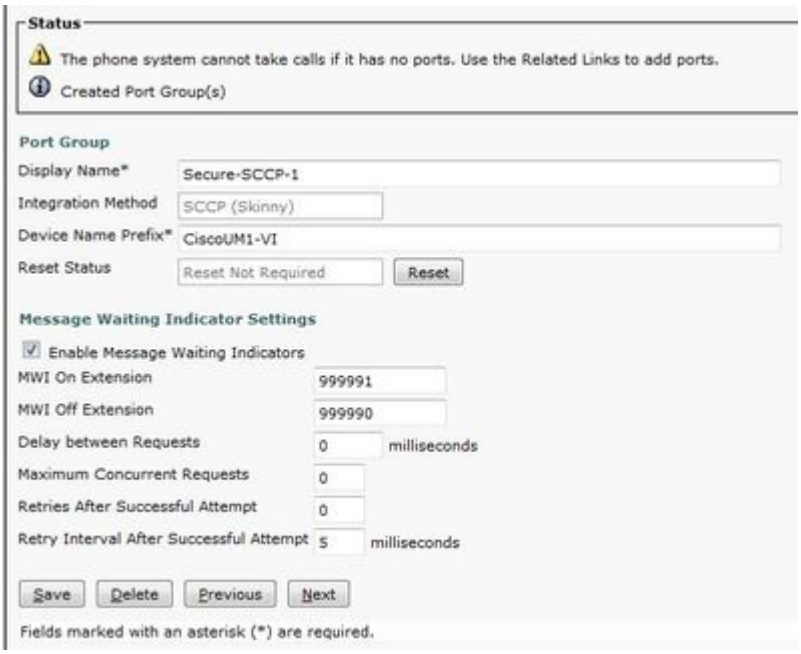
3. Ajouter un nouveau groupe de ports SCCP

Sur la page Phone System Basics, dans la zone déroulante Related Links, sélectionnez Add Port Group et sélectionnez Go. Dans la fenêtre de configuration, saisissez les informations suivantes :

- Système téléphonique :
- Type de groupe de ports : SCCP
- Préfixe du nom du périphérique* : CiscoUM1-VI

- MWI sur poste :
- Extension MWI désactivée :

Remarque : Cette configuration doit correspondre à celle de CUCM.



4. Modifier les serveurs

Naviguez jusqu'à Edit > Servers et ajoutez le serveur TFTP à partir du cluster CUCM.

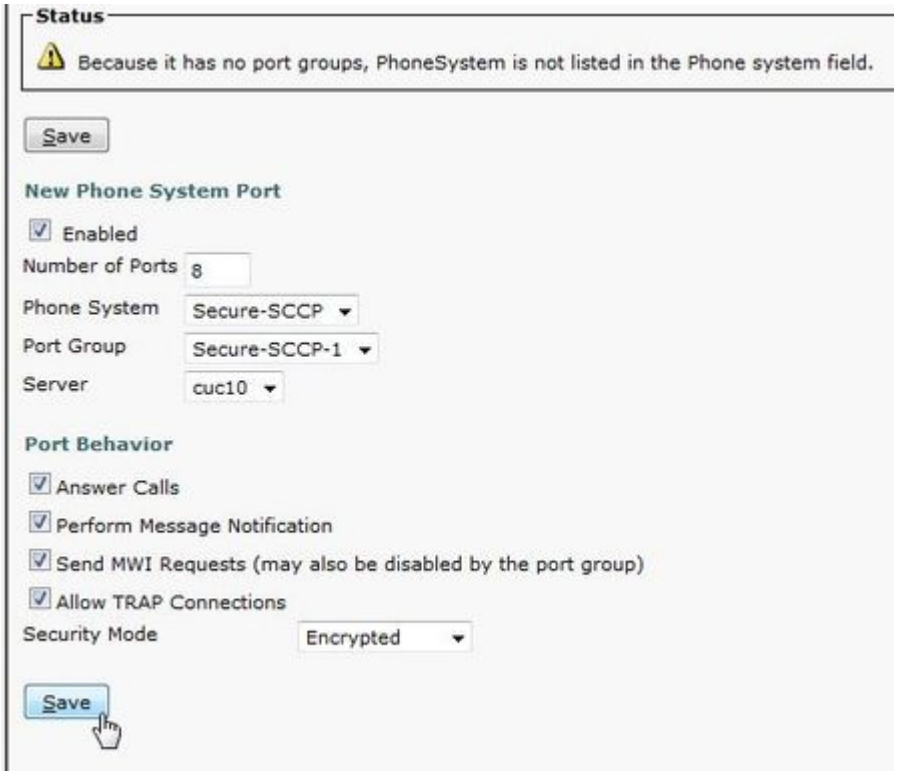


Remarque : Il est important de fournir une adresse TFTP correcte. Le serveur CUC télécharge le fichier CTL à partir de ce TFTP comme expliqué.

5. Ajout de ports SCCP sécurisés

Sur la page Notions de base sur les groupes de ports, dans la liste déroulante Liens associés, sélectionnez Ajouter des ports et sélectionnez Exécuter. Dans la fenêtre de configuration, entrez les informations suivantes :

- Activée: quadrillé
- Nombre de ports :
- Système téléphonique :
- Groupe de ports :
- Serveur :
- Comportement du port :
- Mode de sécurité : Chiffré



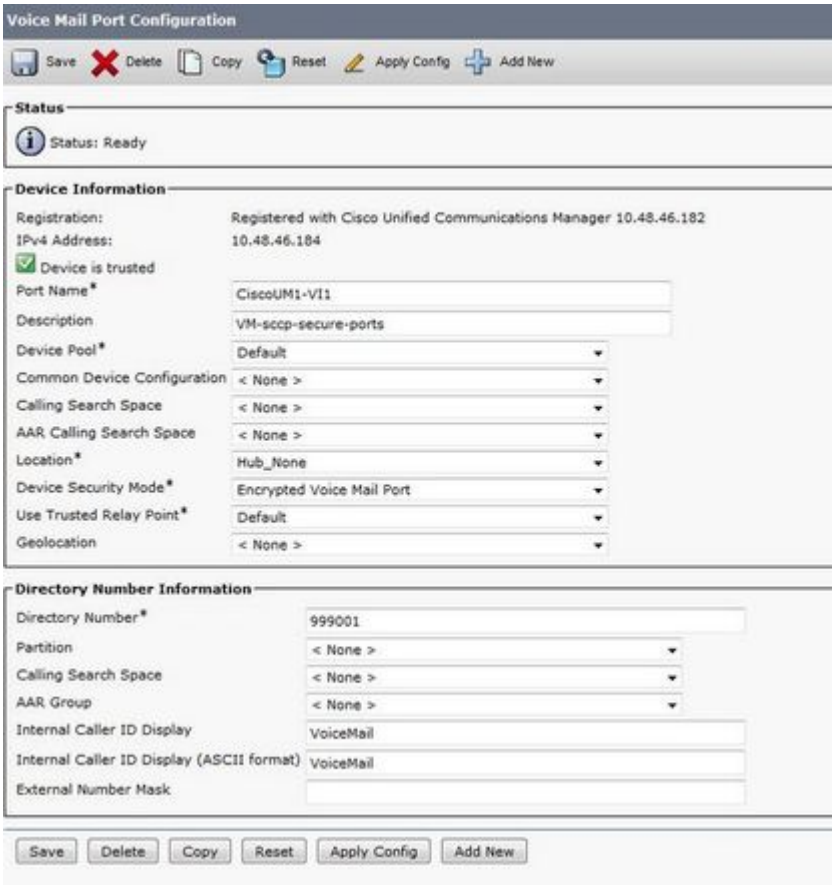
Configurer CUCM

1. Ajouter des ports

Naviguez jusqu'à CUCM Administration > Advanced features > Voice Mail Port Configuration > Add New.

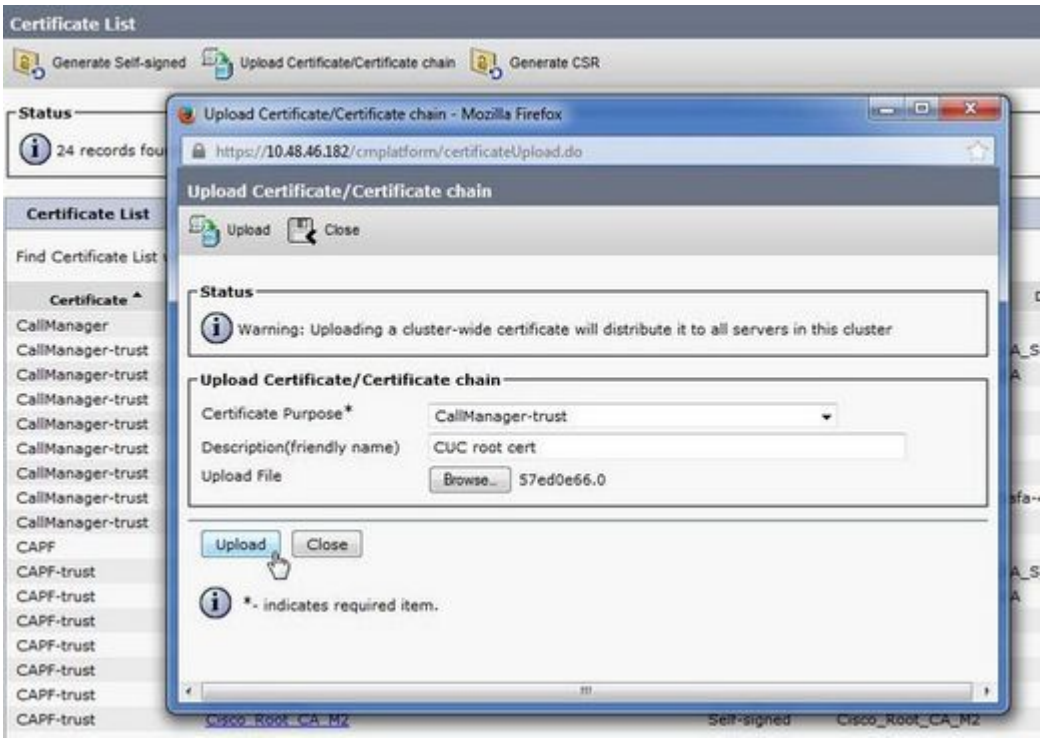
Configurez les ports de messagerie vocale SCCP comme d'habitude. La seule différence est le

mode de sécurité du périphérique dans la configuration du port où l'option Port de messagerie vocale chiffrée doit être sélectionnée.



2. Télécharger le certificat racine CUC comme CallManager-trust

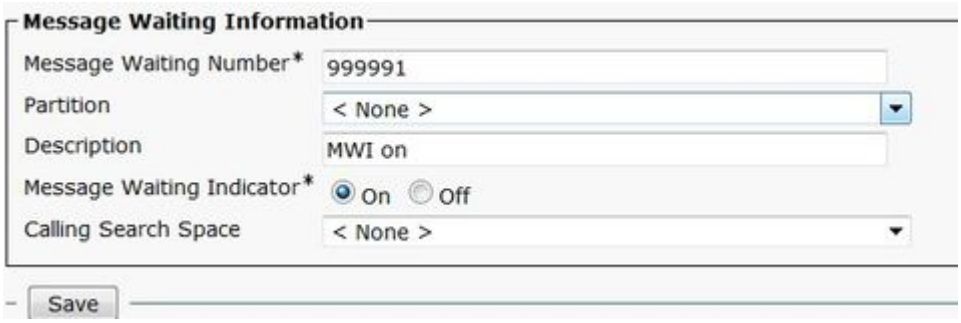
Accédez à OS Administration > Security > Certificate Management > Upload Certificate/Certificate Chain et téléchargez le certificat racine CUC en tant que CallManager-trust sur tous les noeuds configurés pour communiquer avec le serveur CUC.

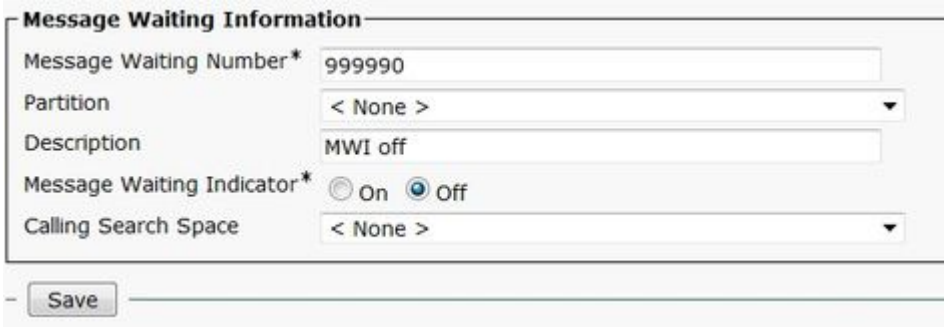


Remarque : le service Cisco CallManager doit être redémarré après le téléchargement du certificat pour que le certificat prenne effet.

3. Configuration des postes d'activation/désactivation MWI (Message Waiting Information)

Accédez à CUCM Administration > Advanced Features > Voice Mail Port Configuration et configurez les extensions On/Off MWI. Les numéros MWI doivent correspondre à la configuration CUC.

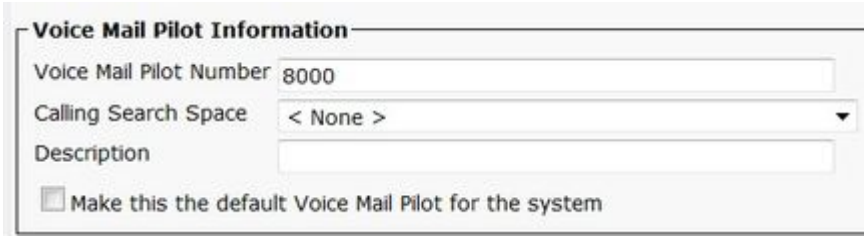




4. Créer un pilote de messagerie vocale

Créez un pilote de messagerie vocale pour l'intégration (Fonctionnalités avancées > Messagerie vocale > Pilote de messagerie vocale). Entrez les valeurs suivantes :

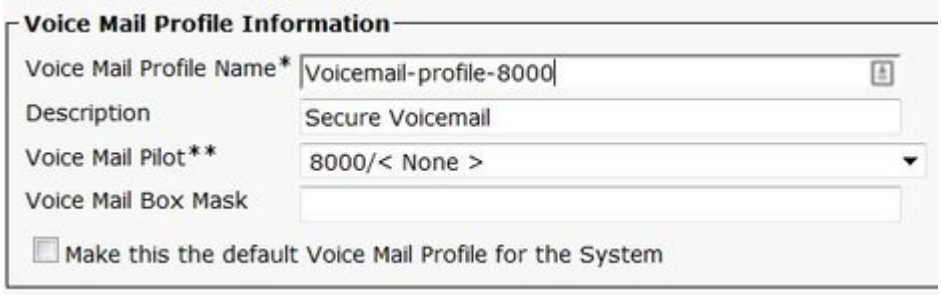
- Numéro pilote de la messagerie vocale :
- Espace de recherche des appels : qui inclut des partitions contenant un modèle de route utilisé comme pilote>



5. Créer un profil de messagerie vocale

Créez un profil de messagerie vocale afin de lier tous les paramètres ensemble (Advanced Features > Voice Mail > Voice Mail Profile). Saisissez les informations suivantes :

- Pilote de messagerie vocale :
- Masque de boîte vocale :

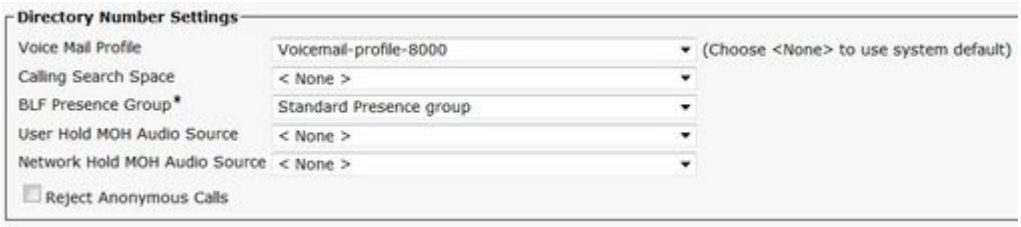


6. Attribuer un profil de messagerie vocale aux DN

Attribuez le profil de messagerie vocale aux DN qui souhaitent utiliser une intégration sécurisée. Cliquez sur le bouton Apply Config après la modification des paramètres DN :

Accédez à Call Routing > Directory number et passez à :

- Profil de messagerie vocale : Voicemail-profile-8000

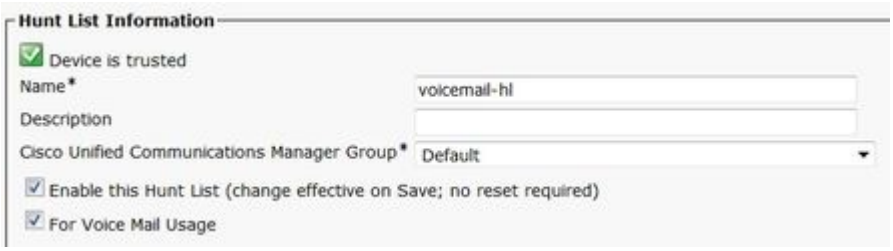


7. Créer un groupe de recherche de messagerie vocale

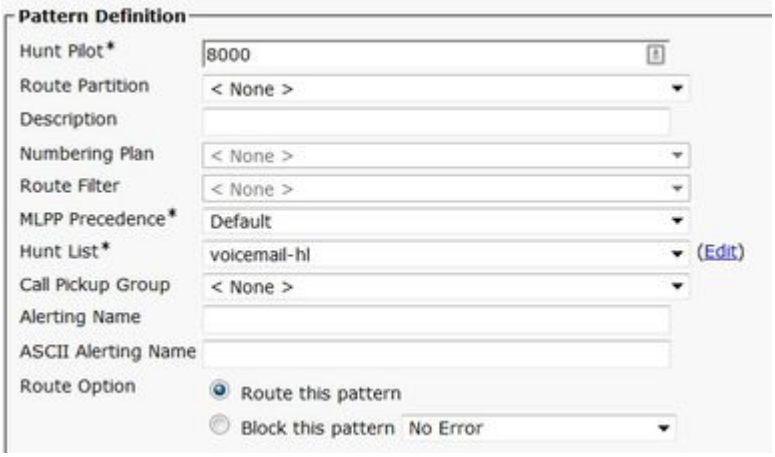
a) Ajouter un nouveau groupe de lignes (Routage des appels > Route/Recherche > Groupe de lignes)



b) Ajouter une nouvelle liste de recherche de messagerie vocale (Routage d'appels > Routage/recherche > Liste de recherche)



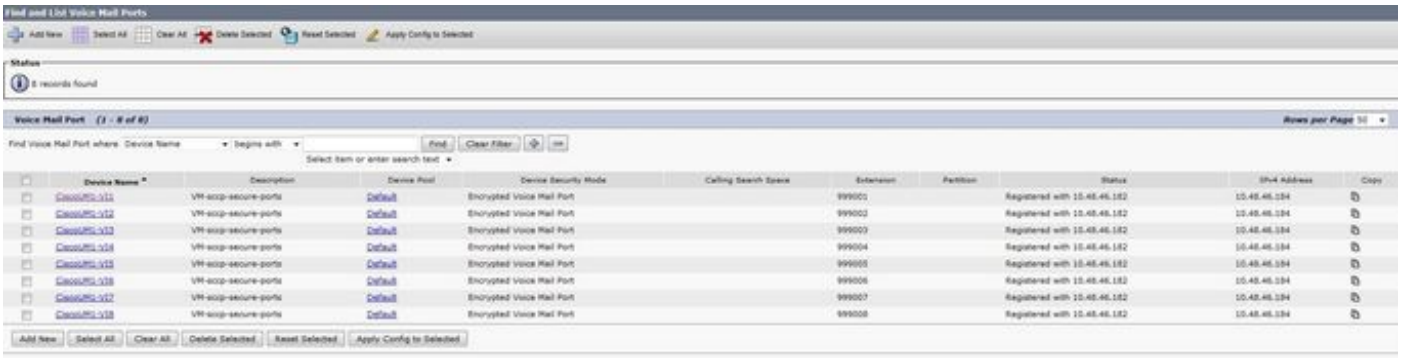
c) Ajouter un nouveau pilote de recherche (Routage d'appels > Route/Recherche > Pilote de recherche)



Vérifier

Vérification des ports SCCP

Accédez à CUCM Administration > Advance Features > Voice Mail > Voice Mail Ports et vérifiez l'enregistrement du port.



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

Vérification de la liaison SIP sécurisée

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

Vous pouvez également activer les options SIP keepalive pour surveiller l'état de la ligne principale SIP. Cette option peut être activée dans le profil SIP attribué à la ligne principale SIP.

Une fois que ceci est activé, vous pouvez surveiller l'état de la ligne principale Sip via Device > Trunk comme montré dans cette image.



Vérification d'appel RTP sécurisé

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 illustré dans cette image.



Dépannage

1. Conseils généraux de dépannage

Suivez ces étapes afin de dépanner l'intégration sécurisée :

- Vérifiez la configuration.
- Assurez-vous que tous les services associés sont en cours d'exécution. (CUCM - CallManager, TFTP, CUC - Conversation Manager)
- Assurez-vous que les ports requis pour une communication sécurisée entre les serveurs sont ouverts sur le réseau (port TCP 2443 pour l'intégration SCCP et TCP 5061 pour

l'intégration SIP).
- Si tout cela est correct, poursuivez avec la collecte de traces.

2. Traces à collecter

Collectez ces traces pour dépanner l'intégration sécurisée.

- Capture de paquets à partir de CUCM et CUC
- Suivi CallManager
- Suivi de Cisco Conversation Manager

Reportez-vous à ces ressources pour plus d'informations sur :

Comment effectuer une capture de paquets sur CUCM :

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

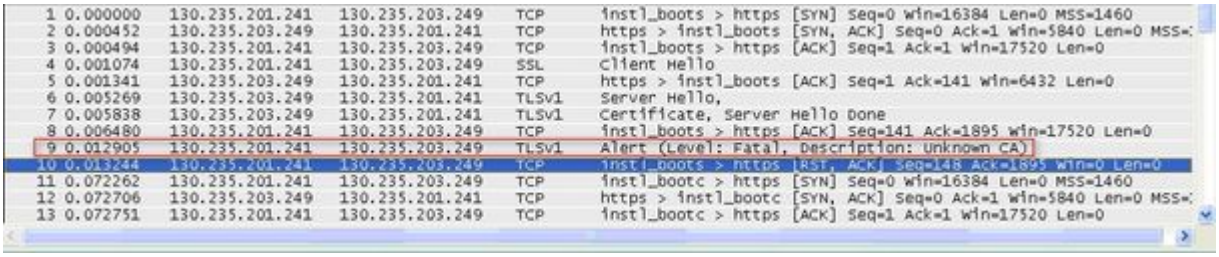
Comment activer les suivis sur le serveur CUC :

http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/10x/troubleshooting/guide/10xcuctsgx/1

Problèmes courants

Cas 1 : Impossible d'établir une connexion sécurisée (alerte CA inconnue)

Une fois que la capture de paquets est collectée à partir de l'un des serveurs, la session TLS est établie.



Le client a émis une alerte avec une erreur irrécupérable Unknown CA au serveur, simplement parce que le client n'a pas pu vérifier le certificat envoyé par le serveur.

Il existe deux possibilités :

1) CUCM envoie l'alerte CA inconnue

- Vérifiez que le certificat racine CUC actuel est téléchargé sur le serveur qui communique avec le serveur CUC.
- Assurez-vous que le service CallManager est redémarré sur le serveur correspondant.

2) CUC envoie l'alerte CA inconnue

- Vérifiez que l'adresse IP TFTP est correctement entrée dans le groupe de ports > Edit > Servers configuration sur le serveur CUC.
- Vérifiez que le serveur TFTP CUCM est accessible à partir du serveur Connection.
- Assurez-vous que le fichier CTL sur le TFTP CUCM est à jour (comparez le résultat de « show ctl » avec les certificats comme vu sur la page OS Admin). Exécutez à nouveau CTLClient si ce n'est pas le cas.
- Redémarrez le serveur CUC OU supprimez et recréez le groupe de ports pour télécharger à nouveau le fichier CTL à partir du serveur TFTP CUCM.

Cas 2 : Impossible de télécharger le fichier CTL à partir de CUCM TFTP

Cette erreur apparaît dans les traces de Conversation Manager :

<#root>

```
MiuGeneral,25,FAILED Port group 'PhoneSystem-1' attempt set InService(true), error retrieving server ce
MiuGeneral,25,Error executing tftp command

'tftp://10.48.47.189:69/CTLFile.tlv' res=68 (file not found on server)


MiuGeneral,25,FAILED Port group 'PhoneSystem-1' attempt set InService(true),

error retrieving server certificates.


Arbiter,-1,Created port PhoneSystem-1-001 objectId='7c2e86b8-2d86-4403-840e-16397b3c626b' as ID=1
MiuGeneral,25,Port group object 'b1c966e5-27fb-4eba-a362-56a5fe9c2be7' exists
MiuGeneral,25,FAILED SetInService=true parent port group is out of service:
```

Solution :

1. Vérifiez à nouveau que le serveur TFTP est correct dans le groupe Port > Edit > Servers configuration.

2. Vérifiez que le cluster CUCM est en mode sécurisé.

3. Vérifiez que le fichier CTL existe sur le serveur TFTP CUCM.

Cas 3 : Les ports ne sont pas enregistrés

Cette erreur apparaît dans les traces de Conversation Manager :

```
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
MiuGeneral,24,Found local CTL file [/tmp/aaaaaaaa-xxxx-xxxx-xxxx-xxxxxxxxxxxx.tlv]
MiuGeneral,25,CCMCertificateCache::RetrieveServerCertificates() failed to find CCM Server '<CUCM IP Add
```

Solution :

1. Cela est probablement dû à une incohérence dans la somme de contrôle md5 du fichier CTL sur CUCM et CUC à la suite de la régénération de

certificats. Redémarrez le serveur CUC pour actualiser le fichier CTL.

Défauts

CSCum48958 - CUCM 10.0 (la longueur de l'adresse IP est incorrecte)

CSCtn87264 - La connexion TLS échoue pour les ports SIP sécurisés

CSCur10758 - Impossible de purger les certificats révoqués Unity Connection

CSCur10534 - CUCM redondant entre opérations TLS/PKI Unity Connection 10.5

CSCve4775 - Demande de fonctionnalité pour une méthode de mise à jour et de révision du fichier CTLF du CUCM sur le CUC

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.