

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

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Diagramme](#)

[Configuration - Trunk SIP sécurisé](#)

[Configurer CUC](#)

[1. Ajouter un certificat SIP](#)

[2. Créer un nouveau système téléphonique ou en modifier un par défaut](#)

[3. Ajouter un nouveau groupe de ports](#)

[4. Modifier les serveurs](#)

[5. Réinitialiser 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. Configurer le profil SIP](#)

[3. Créer une liaison SIP](#)

[4. Créer un modèle de route](#)

[5. Créer un pilote de messagerie vocale](#)

[6. Créer un profil de messagerie vocale](#)

[7. Attribuer un profil de messagerie vocale aux numéros de répertoire](#)

[8. Télécharger le certificat racine CUC en tant que CallManager-trust](#)

[Configuration des ports SCCP sécurisés](#)

[Configurer CUC](#)

[1. Télécharger 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. Ajouter des ports SCCP sécurisés](#)

[Configurer CUCM](#)

[1. Ajouter des ports](#)

[2. Télécharger le certificat racine CUC en tant que CallManager-trust](#)

[3. Configurer les extensions MWI \(Message Waiting Information\) activées/désactivées](#)

[4. Créer un pilote de messagerie vocale](#)

[5. Créer un profil de messagerie vocale](#)

[6. Attribuer un profil de messagerie vocale aux numéros de répertoire](#)

[7. Créer un groupe de recherche de messagerie vocale](#)

[Vérification](#)

[Vérification des ports SCCP](#)

[Vérification de la liaison SIP sécurisée](#)

[Vérification des appels RTP sécurisés](#)

[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 du TFTP CUCM](#)

[Cas 3 : Les ports ne s'inscrivent pas](#)

[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

Conditions requises

Cisco vous recommande de connaître CUCM.

Reportez-vous au [Guide de sécurité de Cisco Unified Communications Manager](#) pour plus de détails.

Note: Il doit être configuré en 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>` »

Components Used

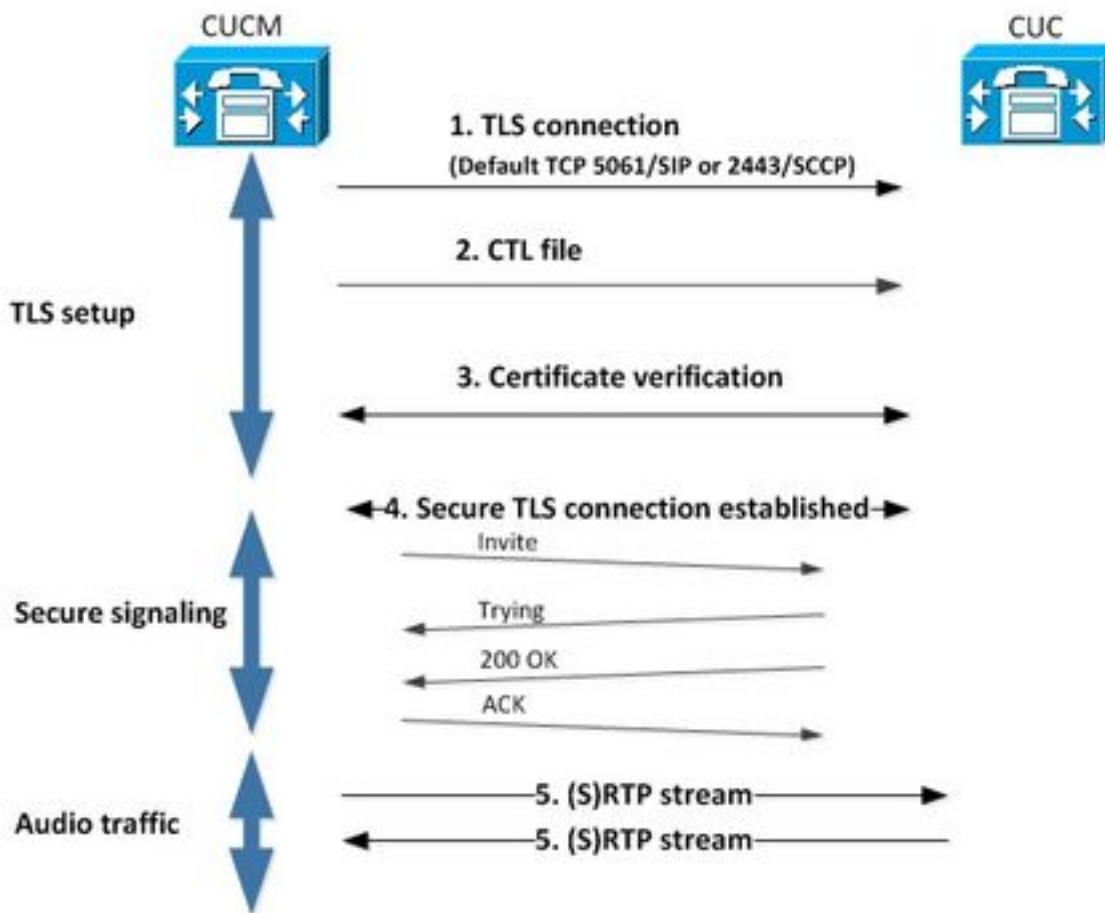
Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- CUCM version 10.5.2.11900-3.
- CUC version 10.5.2.1900-3.

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. If your network is live, make sure that you understand the potential impact of any command.

Diagramme

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



1. Call Manager configure une connexion TLS (Transport Layer Security) sécurisée au serveur CUC sur le port 2443 SCCP (Skinny Call Control Protocol) ou SIP (Session Initiation Protocol) 5061 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 est réussie, 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 sous la forme de protocole de transport en temps réel (RTP) ou SRTP.

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

Configuration - Trunk SIP sécurisé

Configurer CUC

1. Ajouter un certificat SIP

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

- Nom d'affichage : <nom significatif>
- Nom du sujet : <n'importe quel 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 CUCM plus loin dans ce document).

New SIP Certificate

SIP Certificate Reset Help

New SIP Certificate

Display Name* Secure SIP integration with CUCMv10.5.2

Subject Name* SecureConnection

Save

Fields marked with an asterisk (*) are required.

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

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

Accédez à **Intégration téléphonique > Système téléphonique**. Vous pouvez utiliser le système téléphonique existant ou en créer un nouveau.

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* PhoneSystem

Default TRAP Phone System

3. Ajouter un nouveau groupe de ports

Sur la page Notions de base sur le système téléphonique, dans la zone de liste déroulante Liens associés, sélectionnez Ajouter un groupe de ports et sélectionnez Exécuter. Dans la fenêtre de configuration, saisissez les informations suivantes :

- Système téléphonique :
- Créer à partir de : SIP de type de groupe de ports
- SIP Security Profile: 5061/TLS
- Certificat SIP :
- Mode de sécurité : crypté
- RTP sécurisé : vérifié
- Adresse IPv4 ou nom d'hôte :

Appuyez sur Enregistrer.

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. Modifier les serveurs

Accédez à **Edit > Servers** et ajoutez un serveur TFTP à partir du cluster CUCM comme illustré dans cette image.

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.

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

5. Réinitialiser le groupe de ports

Revenez aux **Notions de base sur les groupes de ports** et réinitialisez le groupe de ports comme demandé par le système, comme illustré dans cette image.

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 buttons for "Save", "Delete", "Previous", and "Next". 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 menu set to "SIP", and a "Reset Status" dropdown menu set to "Reset Required" with a "Reset" button next to it.

6. Ajouter des ports de messagerie vocale

Sur la page Notions de base sur le groupe de ports, dans la liste déroulante Liens associés, sélectionnez **Ajouter des ports** et sélectionnez **Atteindre**. Dans la fenêtre de configuration,

saisissez les informations suivantes :

- Activée: Coché
- Nombre de ports :
- Système téléphonique :
- Groupe de ports :
- Serveur :
- Comportement des ports :

New Port

Port Reset Help

Status

⚠ Because it has no port groups, PhoneSystem is not listed in the Phone system field.

Save

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

Save

7. Télécharger le certificat racine CUC

Accédez à **Telephony Integrations > Security > Root Certificate**, cliquez avec le bouton droit de la souris sur l'URL pour enregistrer le certificat sous la forme d'un fichier nommé <nom de fichier>.0 (l'extension du fichier doit être .0 plutôt que .htm) et appuyez sur save comme indiqué 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 du périphérique : crypté
- X.509 Nom du sujet : SecureConnection>
- Accepter la référence hors-boîte de dialogue : cochée
- Accepter la notification non sollicitée : cochée
- Accepter remplace l'en-tête : coché

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

SIP Trunk Security Profile Information

| | |
|---|----------------------------------|
| 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. Configurer le 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 liaison SIP

Accédez à **Device > Trunk > Add new**. Create a SIP trunk qui sera utilisé pour l'intégration sécurisée avec Unity Connection comme illustré dans cette image.

Trunk Information

| | |
|---------------------|---------------|
| Trunk Type* | SIP Trunk |
| Device Protocol* | SIP |
| Trunk Service Type* | None(Default) |

Dans la section Device Information (Informations sur le périphérique) de la configuration de liaison, saisissez les informations suivantes :

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

Note: 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**).

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 |

Media Termination Point Required
 Retry Video Call as Audio
 Path Replacement Support
 Transmit UTF-8 for Calling Party Name
 Transmit UTF-8 Names in QSIG APDU
 Unattended Port
 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
 PSTN Access
 Run On All Active Unified CM Nodes

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

- Espace de recherche d'appels :
- Redirection de la remise de l'en-tête de dérivation - Entrant : vérifié

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

Dans la boîte de dialogue Sortant Section Appels de la configuration de liaison, entrez les informations suivantes :

- Redirection de la remise de l'en-tête de dérivation - Sortant : vérifié

Outbound Calls

Called Party Transformation CSS

Use Device Pool Called Party Transformation CSS

Calling Party Transformation CSS

Use Device Pool Calling Party Transformation CSS

Calling Party Selection*

Calling Line ID Presentation*

Calling Name Presentation*

Calling and Connected Party Info Format*

Redirecting Diversion Header Delivery - Outbound

Redirecting Party Transformation CSS

Use Device Pool Redirecting Party Transformation CSS

Dans la section SIP Information de la configuration de liaison, entrez les informations suivantes :

- Adresse de destination:
- Profil de sécurité de la liaison SIP :
- Réacheminement de l'espace de recherche d'appels :
- Espace de recherche d'appels de référence hors boîte de dialogue :
- Profil SIP :

SIP Information

Destination

Destination Address is an SRV

| | Destination Address | Destination Address IPv6 | Destination Port |
|----|---|--------------------------|-----------------------------------|
| 1* | <input type="text" value="10.48.47.124"/> | <input type="text"/> | <input type="text" value="5061"/> |

MTP Preferred Originating Codec*

BLF Presence Group*

SIP Trunk Security Profile*

Rerouting Calling Search Space

Out-Of-Dialog Refer Calling Search Space

SUBSCRIBE Calling Search Space

SIP Profile* [View Details](#)

DTMF Signaling Method*

Réglez les autres paramètres en fonction de vos besoins.

4. Créer un modèle de route

Créez un modèle de route qui pointe vers l'agrégation configurée (**Routage d'appels > Route/Hunt > Route Pattern**). Le poste entré comme numéro de modèle de route peut être utilisé comme pilote de messagerie vocale. Entrez les informations suivantes :

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

Route Pattern Configuration

Save

Status
 Status: Ready

Pattern Definition

Route Pattern* 8000

Route Partition < None >

Description

Numbering Plan -- Not Selected --

Route Filter < None >

MLPP Precedence* Default

Apply Call Blocking Percentage

Resource Priority Namespace Network Domain < None >

Route Class* Default

Gateway/Route List* SecureSIPtoCUC (Edit)

Route Option
 Route this pattern
 Block this pattern No Error

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 d'appels : qui inclut les partitions contenant le modèle de route utilisé comme pilote>

Voice Mail Pilot Information

Voice Mail Pilot Number 8000

Calling Search Space < None >

Description

Make this the default Voice Mail Pilot for the system

6. Créer un profil de messagerie vocale

Créez un profil de messagerie vocale afin de lier tous les paramètres ensemble (**Fonctionnalités avancées > Messagerie vocale > Profil de messagerie vocale**). Saisissez les informations suivantes :

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

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. Attribuer un profil de messagerie vocale aux numéros de répertoire

Attribuez le profil de messagerie vocale aux numéros de répertoire destinés à utiliser une intégration sécurisée. N'oubliez pas de cliquer sur le bouton Appliquer la configuration après avoir modifié les paramètres DN :

Accédez à : **Call Routing > Directory number** et modifiez les éléments suivants :

- Messagerie vocale Profile: Secure_SIP_Integration

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 >

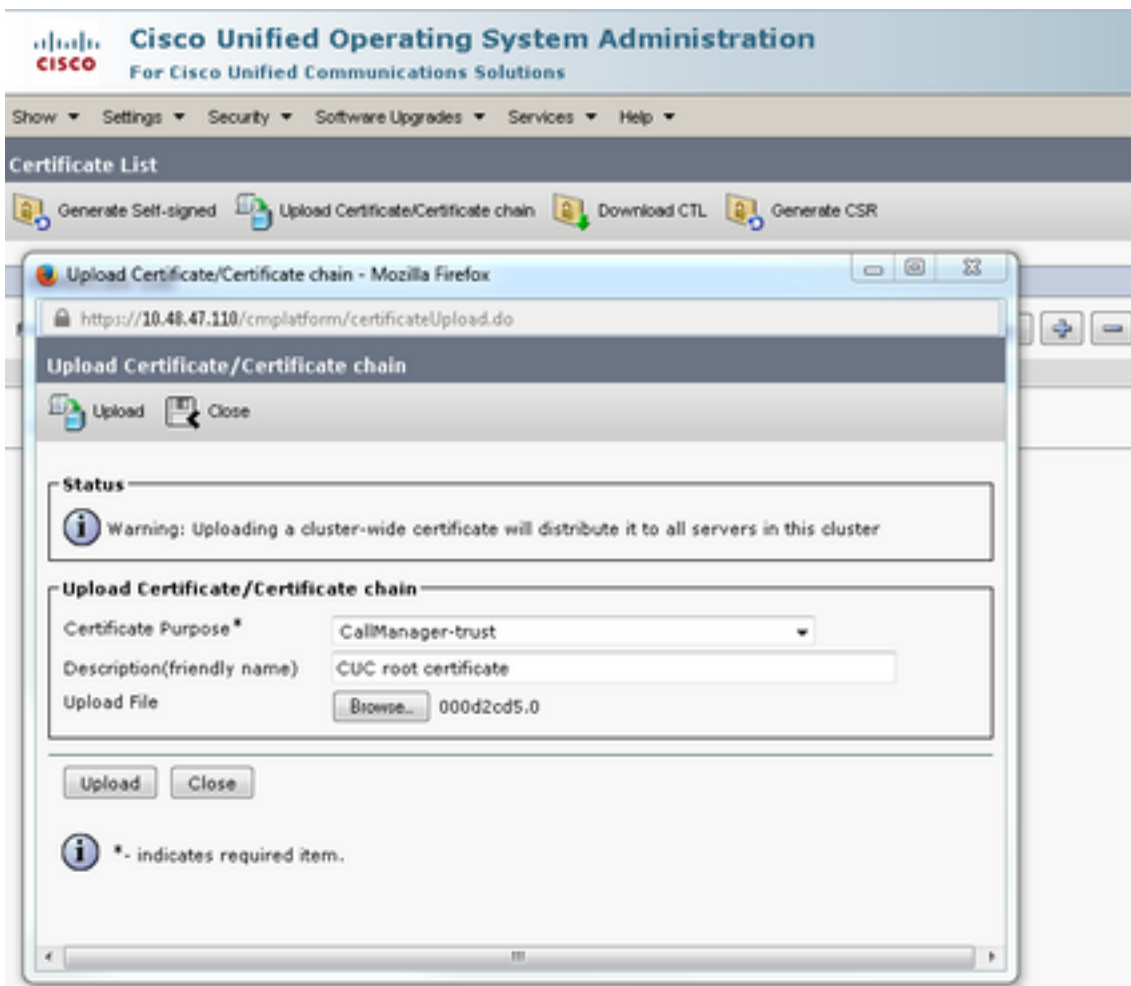
Network Hold MOH Audio Source < None >

Auto Answer* Auto Answer Off

Reject Anonymous Calls

8. Télécharger le certificat racine CUC en tant que CallManager-trust

Accédez à **Administration du système d'exploitation > Sécurité > Gestion des certificats > Télécharger la chaîne de certificats/certificats** 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 afin que le certificat prenne effet.

Configuration des ports SCCP sécurisés

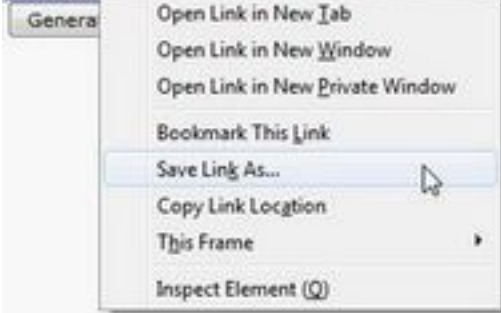
Configurer CUC

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 sous la forme d'un fichier nommé <nom de fichier>.0 (l'extension du fichier doit être .0 plutôt que .htm) et cliquez sur **Enregistrer** :

| 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 OjE4MDYGA1UEAwwvQ2lzY29Vbml0eS01ZGFkMzJlYy1jYWZlLnQ1NTktOTc4Zj01 NmYyYzY4NTBkNDEwHhcNMTUwMzYxMDY1OTM0WWhcNMjEwNDAxMDY1OTM0WjA6MTgw NgYDVQQLDDB9DaxNjb1VuaXR5LTkYwQzMmVilWNhZmEtNDU1OS05NzhmLTU2Zj01 Njg1MGQ0MTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAoBOBg/qh8cWQx457 Q47eGUWcR2jeyE726RTO40GkdhDYI4Km6ouSeMiGbs757WpvtspKp+zeSDjVm2j4 B1lxG9wM3XgPPwM+3QIMh0NQLARuJdm9g2/5uiHB6/1k82Po0Wrv2r6Anoragrv Md3ordaCB3mG1u2g0GqXj9GChf0CAwEAaANCMEEAwEgYDVR0TAQH/BAgwBgEB/wIB ADAdBgNVHQ4EFgQU438N5JYGHhgp7qm2dUmu+HGkM8wCwYDVR0PBAQDAGKsMA0G CSqGSIb3DQEBBQUAA4GBAGPhrPt6GH2a0iXV8bnKvC12f5ty1eTeMD6ZzD62P4C6 RtGM8BWqGU1IAZw1www0nxdetKzZvJX2z2Ksu2ptVUnFPMzSc+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. Créer un système téléphonique / Modifier celui qui existe.

Accédez à **Intégration téléphonique > système téléphonique**. Vous pouvez utiliser le système téléphonique existant ou en créer un nouveau.

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. Ajouter un nouveau groupe de ports SCCP


Sur la page Notions de base sur le système téléphonique, dans la liste déroulante Liens associés, sélectionnez **Ajouter un groupe de ports** et sélectionnez **Aller**. Dans la fenêtre de configuration, saisissez les informations suivantes :

- Système téléphonique :
- Type de groupe de ports : SCCP
- Préfixe de nom de périphérique* : CiscoUM1-VI
- Extension MWI On :
- Extension MWI Off :

Note: Cette configuration doit correspondre à celle de 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. Modifier les serveurs

Accédez à **Edit > Servers** et ajoutez le serveur TFTP à partir du cluster CUCM.

SIP Servers

| <input type="checkbox"/> | Order | IPv4 Address or Host Name |
|--------------------------|-------|---|
| <input type="checkbox"/> | 0 | 10.48.47.110 <input type="button" value="📄"/> |

TFTP Servers

| <input type="checkbox"/> | Order | IPv4 Address or Host Name |
|--------------------------|-------|---------------------------|
| <input type="checkbox"/> | 0 | 10.48.47.110 |


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

5. Ajouter des ports SCCP sécurisés

Sur la page Notions de base sur le groupe de ports, dans la liste déroulante Liens associés, sélectionnez **Ajouter des ports** et sélectionnez **Atteindre**. Dans la fenêtre de configuration, saisissez les informations suivantes :

- Activée: vérifié
- Nombre de ports :
- Système téléphonique :
- Groupe de ports :
- Serveur :
- Comportement des ports :
- Mode de sécurité : **crypté**

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

Configurer CUCM

1. Ajouter des ports

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

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 >

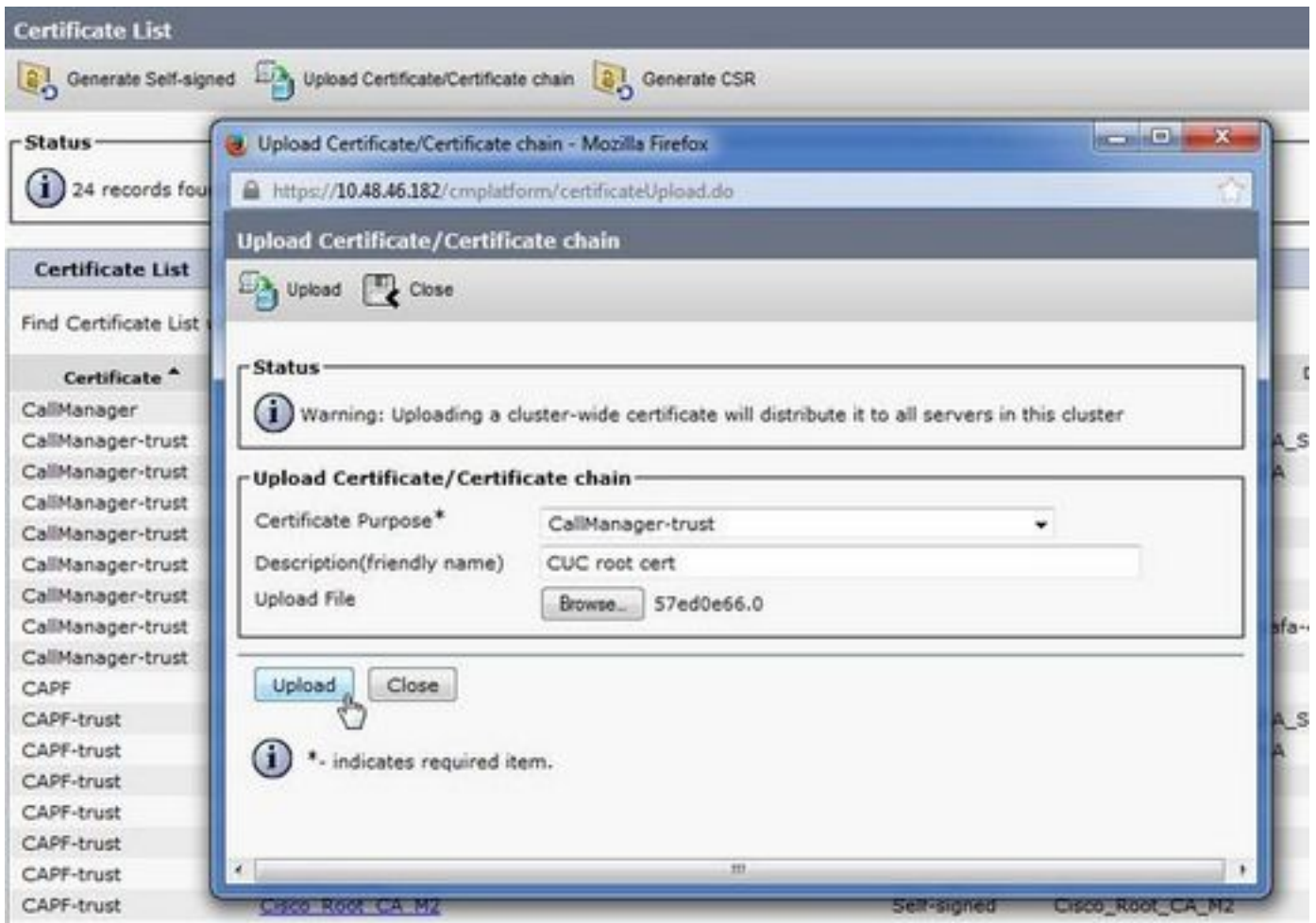
Directory Number Information

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. Télécharger le certificat racine CUC en tant que CallManager-trust

Accédez à **Administration du système d'exploitation > Sécurité > Gestion des certificats > Télécharger la chaîne de certificats/certificats** 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 afin que le certificat prenne effet.

3. Configurer les extensions MWI (Message Waiting Information) activées/désactivées

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

| 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 > |

Message Waiting Information

Message Waiting Number* 999990

Partition < None >

Description MWI off

Message Waiting Indicator* On Off

Calling Search Space < None >

Save

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 d'appels : qui inclut les partitions contenant le modèle de route utilisé comme pilote>

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. Créer un profil de messagerie vocale

Créez un profil de messagerie vocale afin de lier tous les paramètres ensemble (**Fonctionnalités avancées > Messagerie vocale > Profil de messagerie vocale**). Entrez les informations suivantes :

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

Voice Mail Profile Information

Voice Mail Profile Name* Voicemail-profile-8000

Description Secure Voicemail

Voice Mail Pilot** 8000/< None >

Voice Mail Box Mask

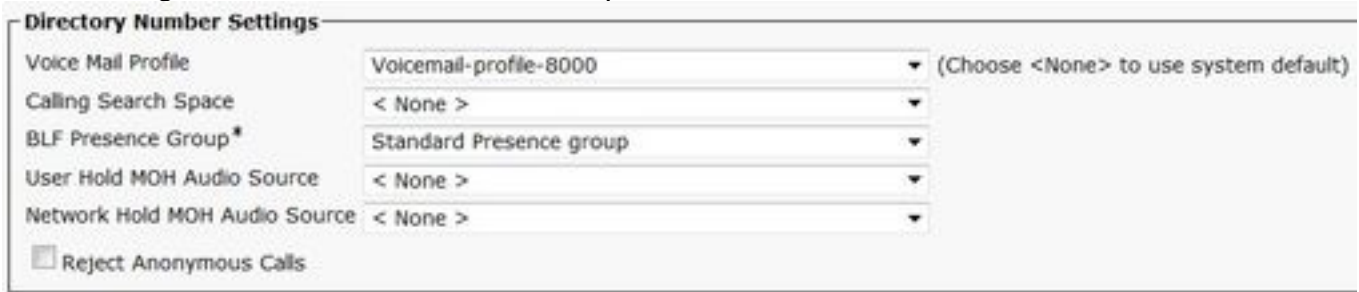
Make this the default Voice Mail Profile for the System

6. Attribuer un profil de messagerie vocale aux numéros de répertoire

Attribuez le profil de messagerie vocale aux numéros de répertoire qui ont l'intention d'utiliser une intégration sécurisée. Cliquez sur le bouton **Apply Config** après la modification des paramètres DN

Accédez à **Routage des appels > Numéro de répertoire** et passez à :

- Messagerie vocale Profile: Voicemail-profile-8000



Directory Number Settings

| | | |
|-------------------------------|-------------------------|---------------------------------------|
| Voice Mail Profile | Voicemail-profile-8000 | (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 > | |

Reject Anonymous Calls

7. Créer un groupe de recherche de messagerie vocale

a) Ajouter un nouveau groupe de lignes (Routage d'appels > Route/Hunt > Groupe de lignes)



- Line Group Information

| | |
|-------------------------|-------------------|
| Line Group Name* | voicemail-1g |
| RNA Reversion Timeout* | 10 |
| Distribution Algorithm* | Longest Idle Time |

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



Hunt List Information

Device is trusted

| | |
|---|--------------|
| Name* | voicemail-hl |
| Description | |
| Cisco Unified Communications Manager Group* | Default |

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

For Voice Mail Usage

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

Pattern Definition

Hunt Pilot*

Route Partition

Description

Numbering Plan

Route Filter

MLPP Precedence*

Hunt List* (Edit)

Call Pickup Group

Alerting Name

ASCII Alerting Name

Route Option Route this pattern
 Block this pattern

Vérification

Vérification des ports SCCP

Accédez à **CUCM Administration > Advanced Features > Voice Mail > Voice Mail Ports** et vérifiez l'enregistrement des ports.

Find and List Voice Mail Ports

Status

0 records found

Voice Mail Port (1 - 8 of 8)

Rows per Page 10

| Device Name | Description | Device Pool | Device Security Mode | Calling Search Space | Extension | Partition | Status | IP Address | Clear |
|-------------|---------------------|-------------|---------------------------|----------------------|-----------|------------------------------|------------|--------------|--------------------------------------|
| CUCM501-001 | VN-ecp-secure-ports | Default | Encrypted Voice Mail Port | 999001 | 999001 | Registered with 10.48.46.182 | Registered | 10.48.46.184 | <input type="button" value="Clear"/> |
| CUCM501-002 | VN-ecp-secure-ports | Default | Encrypted Voice Mail Port | 999002 | 999002 | Registered with 10.48.46.182 | Registered | 10.48.46.184 | <input type="button" value="Clear"/> |
| CUCM501-003 | VN-ecp-secure-ports | Default | Encrypted Voice Mail Port | 999003 | 999003 | Registered with 10.48.46.182 | Registered | 10.48.46.184 | <input type="button" value="Clear"/> |
| CUCM501-004 | VN-ecp-secure-ports | Default | Encrypted Voice Mail Port | 999004 | 999004 | Registered with 10.48.46.182 | Registered | 10.48.46.184 | <input type="button" value="Clear"/> |
| CUCM501-005 | VN-ecp-secure-ports | Default | Encrypted Voice Mail Port | 999005 | 999005 | Registered with 10.48.46.182 | Registered | 10.48.46.184 | <input type="button" value="Clear"/> |
| CUCM501-006 | VN-ecp-secure-ports | Default | Encrypted Voice Mail Port | 999006 | 999006 | Registered with 10.48.46.182 | Registered | 10.48.46.184 | <input type="button" value="Clear"/> |
| CUCM501-007 | VN-ecp-secure-ports | Default | Encrypted Voice Mail Port | 999007 | 999007 | Registered with 10.48.46.182 | Registered | 10.48.46.184 | <input type="button" value="Clear"/> |
| CUCM501-008 | VN-ecp-secure-ports | Default | Encrypted Voice Mail Port | 999008 | 999008 | Registered with 10.48.46.182 | Registered | 10.48.46.184 | <input type="button" value="Clear"/> |

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.

Vérification de la liaison 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 dans cette image.

| Trunks (1 - 1 of 1) | | | | | | | | | | |
|--|-------------|----------------------|-------------|---------------|-----------|-------------|----------|------------|------------------|---|
| Find Trunks where: Device Name begins with [] Find Clear Filter [] [] | | | | | | | | | | |
| Select item or enter search text [] | | | | | | | | | | |
| 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 |

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.



Dépannage

1. Conseils généraux de dépannage

Suivez ces étapes afin de dépanner l'intégration sécurisée :

- Vérifier la configuration
- Vérifiez que tous les services associés sont en cours d'exécution. (CUCM - CallManager, TFTP, CUC - Conversation Manager)
- Assurez-vous que les ports requis pour la 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, passez à la collection 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

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 traces sur le serveur CUC :

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

Problèmes courants

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

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

```

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

```

Le client a émis une alerte avec une erreur irrécupérable d'autorité de certification inconnue 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 chargé 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 Autorité de certification inconnue

- Vérifiez que l'adresse IP TFTP est correctement entrée dans la configuration **Groupe de ports > Modifier > Serveurs** sur le serveur CUC.
- Vérifiez que le serveur TFTP CUCM est accessible à partir du serveur Connection.
- Assurez-vous que le fichier CTL sur CUCM TFTP est à jour (comparez la sortie de « show ctl » avec les certificats comme indiqué sur la page d'administration du système d'exploitation). Si ce n'est pas le cas, réexécutez CTLClient.
- Redémarrez le serveur CUC OU supprimez et recréez le groupe de ports pour télécharger à nouveau le fichier CTL à partir du TFTP CUCM.

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

Cette erreur apparaît dans les traces de Conversation Manager :

```
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:
```

Solution :

1. Vérifiez deux fois que le serveur TFTP est correct dans le **groupe de ports > Modifier > configuration des serveurs**.
2. Vérifiez que le cluster CUCM est en mode sécurisé.
3. Vérifiez que le fichier CTL existe sur CUCM TFTP.

Cas 3 : Les ports ne s'inscrivent pas

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 -> 5000 msec  
MiuGeneral,24,Found local CTL file [/tmp/aaaaaaaa-xxxx-xxxx-xxxx-xxxxxxxxxxxx.tlv]  
MiuGeneral,25,CCMCertificateCache::RetrieveServerCertificates() failed to find CCM Server '<CUCM IP Address>' in CTL File
```

Solution :

1. Ceci est probablement dû à une non-correspondance dans la somme de contrôle md5 du fichier CTL sur CUCM et CUC suite à la régénération de certificats. Redémarrez le serveur CUC pour actualiser le fichier CTL.

Informations internes Cisco

Vous pouvez également supprimer le fichier CTL de la racine comme suit :

Supprimez le fichier CTL du dossier /tmp/ et réinitialisez le groupe de ports. Vous pouvez faire une somme de contrôle md5 sur le fichier

et comparez avant de le supprimer :

```
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 cuservice 6120 fév 5 15:29 a31cefe5-9359-4cbc-a0f3-52eb870d976c.tlv
```

```
[root@vstscuc1 tmp]# md5sum a31cefe5-9359-4cbc-a0f3-52eb870d976c.tlv
```

```
e5bf2ab934a42f4d8e6547dfd8cc82e8 a31cefe5-9359-4cbc-a0f3-52eb870d976c.tlv
```

En outre, vous pouvez consulter le présent guide de dépannage :

Défauts

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

[CSCtn87264](#) - Échec de la connexion TLS pour les ports SIP sécurisés

[CSCur10758](#) - Impossible de purger les certificats révoqués Unity Connection

[CSCur10534](#) - Unity Connection 10,5 TLS/PKI, CUCM redondant inter-op

[CSCve47775](#) - Demande de fonctionnalité pour une méthode de mise à jour et de révision du CTLFile du CUCM sur le CUC