

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

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Diagramme du réseau](#)

[Conditions requises de certificat](#)

[Configurez - Cisco Unity Connection \(CUC\)](#)

1. [Ajoutez un nouveau groupe de port](#)
2. [Ajoutez la référence de serveur TFTP](#)
3. [Ajoutez les ports de messagerie vocale](#)
4. [Racine du téléchargement CUCM et certificat intermédiaire du tiers CA](#)

[Configurez - Cisco Unified CM \(CUCM\)](#)

1. [Créez un profil de Sécurité de joncteur réseau de SIP](#)
2. [Créez un joncteur réseau sécurisé de SIP](#)
3. [Configurez les chiffrements de TLS et SRTP](#)
4. [Certificats du téléchargement CUC Tomcat \(RSA et EC basées\)](#)
5. [Créez le modèle d'artère](#)
6. [Créez le pilote de messagerie vocale, profil de messagerie vocale et affectez-le aux dn](#)

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

[Vérifiez](#)

[Sécurisez la vérification de joncteur réseau de SIP](#)

[Vérification sécurisée d'appel de RTP](#)

[Informations connexes](#)

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 :

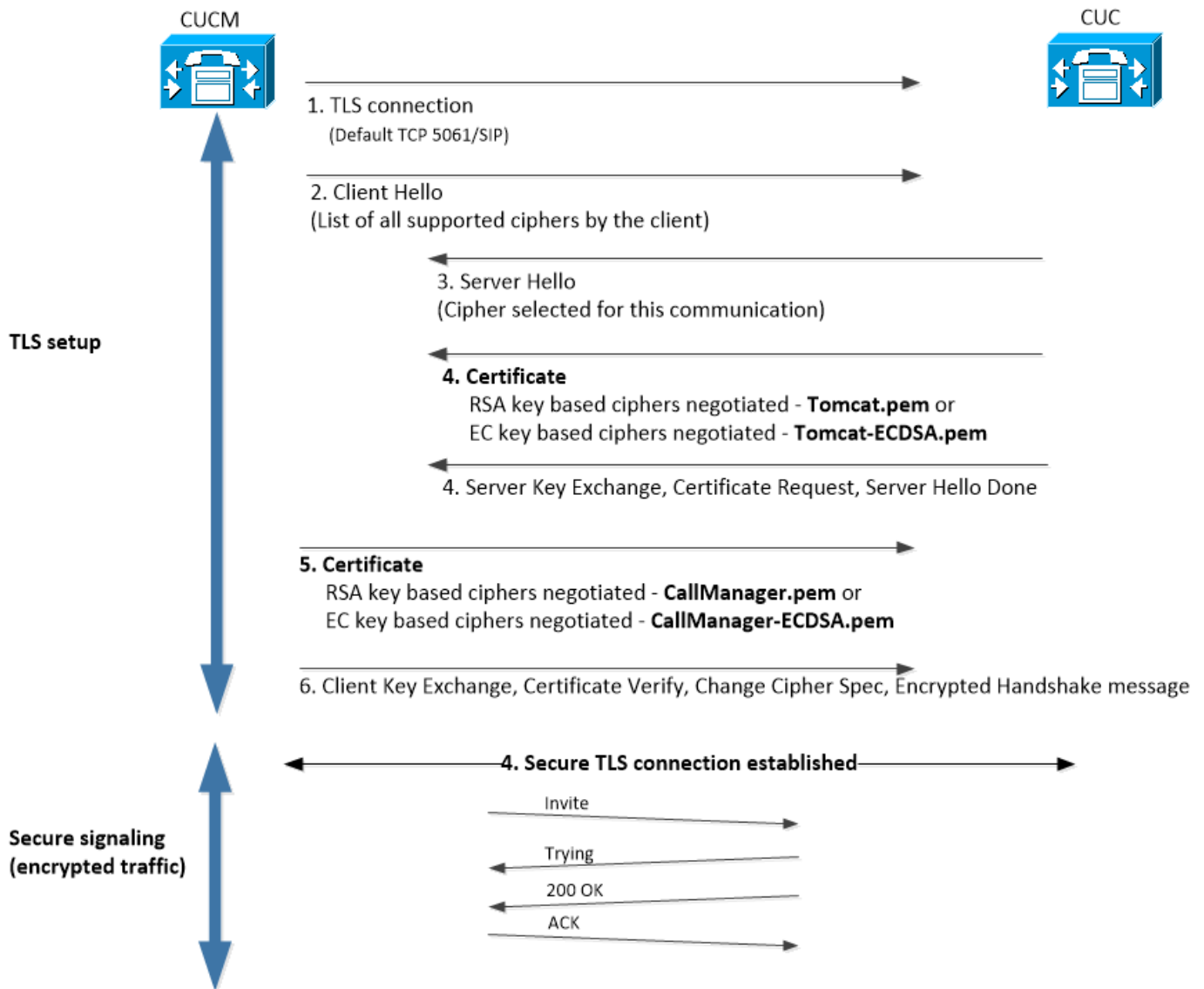
Version 11.x et ultérieures CUCM dans le mode mixte

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.

New Port Group

Phone System

Create From Port Group Type Port Group

Port Group Description

Display Name*

Authenticate with SIP Server

Authentication Username

Authentication Password

Contact Line Name

SIP Security Profile

Enable Next Generation Encryption

Secure RTP

Primary Server Settings

IPv4 Address or Host Name

IPv6 Address or Host Name

Port

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.

The image shows two configuration panels. The top panel is titled 'SIP Servers' and contains a table with columns for 'Order' and 'IPv4 Address or Host Name'. The first row has '0' in the Order column and '10.48.47.109' in the IPv4 Address or Host Name column. Below the table are 'Delete Selected' and 'Add' buttons. The bottom panel is titled 'TFTP Servers' and contains a similar table. The first row has '0' in the Order column and 'CUCMv11' in the IPv4 Address or Host Name column. Below the table are 'Delete Selected' and 'Add' buttons.

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.

The image shows the 'Port Group' configuration page. The 'Display Name*' field contains 'PhoneSystem-1'. The 'Integration Method' dropdown is set to 'SIP'. The 'Reset Status' field shows 'Reset Required' and there is a 'Reset' button next to it. Below this is the 'Session Initiation Protocol (SIP) Settings' section with two unchecked checkboxes: 'Register with SIP Server' and 'Authenticate with SIP Server'.

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.

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

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.

Upload Certificate/Certificate chain

Certificate Purpose*

Description(friendly name)

Upload File

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.

SIP Trunk Security Profile Information

Name* cuc-secure-profile-EDCS

Description

Device Security Mode Encrypted

Incoming Transport Type* TLS

Outgoing Transport Type TLS

Enable Digest Authentication

Nonce Validity Time (mins)* 600

X.509 Subject Name CUCv11

Incoming Port* 5061

Enable Application level authorization

Accept presence subscription

Accept out-of-dialog refer**

Accept unsolicited notification

Accept replaces header

Transmit security status

Allow charging header

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.

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

Inbound Calls

Significant Digits*	All
Connected Line ID Presentation*	Default
Connected Name Presentation*	Default
Calling Search Space	< None >
AAR Calling Search Space	< None >
Prefix DN	
<input checked="" type="checkbox"/> Redirecting Diversion Header Delivery - Inbound	

Outbound Calls

Called Party Transformation CSS	< None >
<input checked="" type="checkbox"/> Use Device Pool Called Party Transformation CSS	
Calling Party Transformation CSS	< None >
<input checked="" type="checkbox"/> Use Device Pool Calling Party Transformation CSS	
Calling Party Selection*	Originator
Calling Line ID Presentation*	Default
Calling Name Presentation*	Default
Calling and Connected Party Info Format*	Deliver DN only in connected party
<input checked="" type="checkbox"/> Redirecting Diversion Header Delivery - Outbound	
Redirecting Party Transformation CSS	< None >
<input checked="" type="checkbox"/> Use Device Pool Redirecting Party Transformation CSS	

Destination

<input type="checkbox"/> Destination Address is an SRV			
	Destination Address	Destination Address IPv6	Destination Port
1*	10.48.47.123		5061
MTP Preferred Originating Codec*	711ulaw		
BLF Presence Group*	Standard Presence group		
SIP Trunk Security Profile*	cuc-secure-profile-EDCS		
Rerouting Calling Search Space	< None >		
Out-Of-Dialog Refer Calling Search Space	< None >		
SUBSCRIBE Calling Search Space	< None >		
SIP Profile*	Standard SIP Profile	View Details	
DTMF Signaling Method*	No Preference		

3. Configurez les chiffrements de TLS et SRTP

- 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.

Security Parameters	
Cluster Security Mode *	1
LBM Security Mode *	Insecure
CAPF Phone Port *	3804
CAPF Operation Expires in (days) *	10
TFTP File Signature Algorithm *	SHA-1
Enable Caching *	True
Authentication Method for API Browser Access *	Basic
TLS Ciphers *	All Ciphers RSA Preferred
SRTP Ciphers *	All Supported Ciphers
HTTPS Ciphers *	RSA Ciphers Only

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.

Edit General Configuration

Time Zone	(GMT+01:00) Europe/Warsaw
System Default Language	English(United States)
System Default TTS Language	English(United States)
Recording Format	G.711 mu-law
Maximum Greeting Length	90
Target Decibel Level for Recordings and Messages	-26
Default Partition	cucv11 Partition
Default Search Scope	cucv11 Search Space
When a recipient cannot be found	Send a non-delivery receipt
IP Addressing Mode	IPv4
TLS Ciphers	All Ciphers RSA Preferred
SRTP Ciphers	All supported AES-256, AES-128 ciphers
HTTPS Ciphers	RSA Ciphers Only

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

L'AES-256 le plus fort SHA-384 seulement : RSA préférée

Strongest-AES-256 SHA-384 seulement : ECDSA préféré

Chiffrements de TLS dans la commande prioritaire

- 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

Medium-AES-256 AES-128 seulement : RSA préférée

Medium-AES-256 AES-128 seulement : ECDSA préféré

Tous les chiffrements RSA préférés (par défaut)

Tous les chiffrements ECDSA préférés

- 4
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- 4
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- 4
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- 4
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- 4
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- 6
- TLS_RSA_WITH_AES_128_CBC_SHA

Options de chiffrement SRTP dans la commande prioritaire

Option de chiffrement SRTP

Tout l'AES-256 pris en charge, chiffrements AES-128

AEAD AES-256, chiffrements AES-128 basés sur GCM

Chiffrements basés sur GCM AEAD AES256 seulement

SRTP dans la commande prioritaire

- AEAD_AES_256_GCM
- AEAD_AES_128_GCM
- AES_CM_128_HMAC_SHA1_32
- AEAD_AES_256_GCM
- AEAD_AES_128_GCM
- 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.

Upload Certificate/Certificate chain

Certificate Purpose*

Description(friendly name)

Upload File tomcat-ECDSA.pem

Upload Certificate/Certificate chain

Certificate Purpose*

Description(friendly name)

Upload File tomcat.pem

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.

Upload Certificate/Certificate chain

Certificate Purpose*

Description(friendly name)

Upload File CA_root_-_4096_key.crt

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.

Pattern Definition

Route Pattern*	2000
Route Partition	< None >
Description	
Numbering Plan	-- Not Selected --
Route Filter	< None >
MLPP Precedence*	Default
<input type="checkbox"/> Apply Call Blocking Percentage	
Resource Priority Namespace Network Domain	< None >
Route Class*	Default
Gateway/Route List*	CUCv11
Route Option	<input checked="" type="radio"/> Route this pattern <input type="radio"/> Block this pattern No Error

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.

Voice Mail Pilot Information

Voice Mail Pilot Number	2000
Calling Search Space	< None >
Description	Default

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

Voice Mail Profile Information

Voice Mail Profile	VoiceMailProfile-8000 (used by 0 devices)
Voice Mail Profile Name*	VoiceMailProfile-8000
Description	
Voice Mail Pilot**	2000/< None >
Voice Mail Box Mask	

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

Directory Number Settings

Voice Mail Profile	VoiceMailProfile-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 >	

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 suit :
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 suit :
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 :

Name	Description	Calling Search Space	Device Pool	Route Pattern	Trunk Type	SIP Trunk Status	SIP Trunk Duration
CUCv11			Default	2000	SIP Trunk	Full Service	Time In Full Service: 0 day 0 hour 0 minute

Vérification sécurisée d'appel de RTP

Vérifiez si l'icône de cadenas est présente aux appels à l'Unity Connection. Il signifie que le flux 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](#)