

Configurer la signalisation SIP sécurisée dans Contact Center Enterprise

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configurer](#)

[Tâche 1. Configuration sécurisée CUBE](#)

[Tâche 2. Configuration sécurisée CVP](#)

[Tâche 3. Configuration sécurisée CVVB](#)

[Tâche 4. Configuration sécurisée CUCM](#)

[Définir le mode de sécurité CUCM sur Mixed Mode](#)

[Configuration des profils de sécurité de la ligne principale SIP pour CUBE et CVP](#)

[Associer des profils de sécurité de liaison SIP aux liaisons SIP respectives](#)

[Communication sécurisée des périphériques des agents avec CUCM](#)

[Vérifier](#)

[Dépannage](#)

Introduction

Ce document décrit comment sécuriser la signalisation SIP (Session Initiation Protocol) dans le flux d'appels complet de Contact Center Enterprise (CCE).

Conditions préalables

La génération et l'importation de certificats n'étant pas couvertes par ce document, les certificats pour Cisco Unified Communication Manager (CUCM), le serveur d'appels Customer Voice Portal (CVP), Cisco Virtual Voice Browser (CVVB) et Cisco Unified Border Element (CUBE) doivent être créés et importés dans les composants respectifs. Si vous utilisez des certificats auto-signés, l'échange de certificats doit être effectué entre différents composants.

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- CCE
- CVP
- CUBE
- CUCM
- CVVB

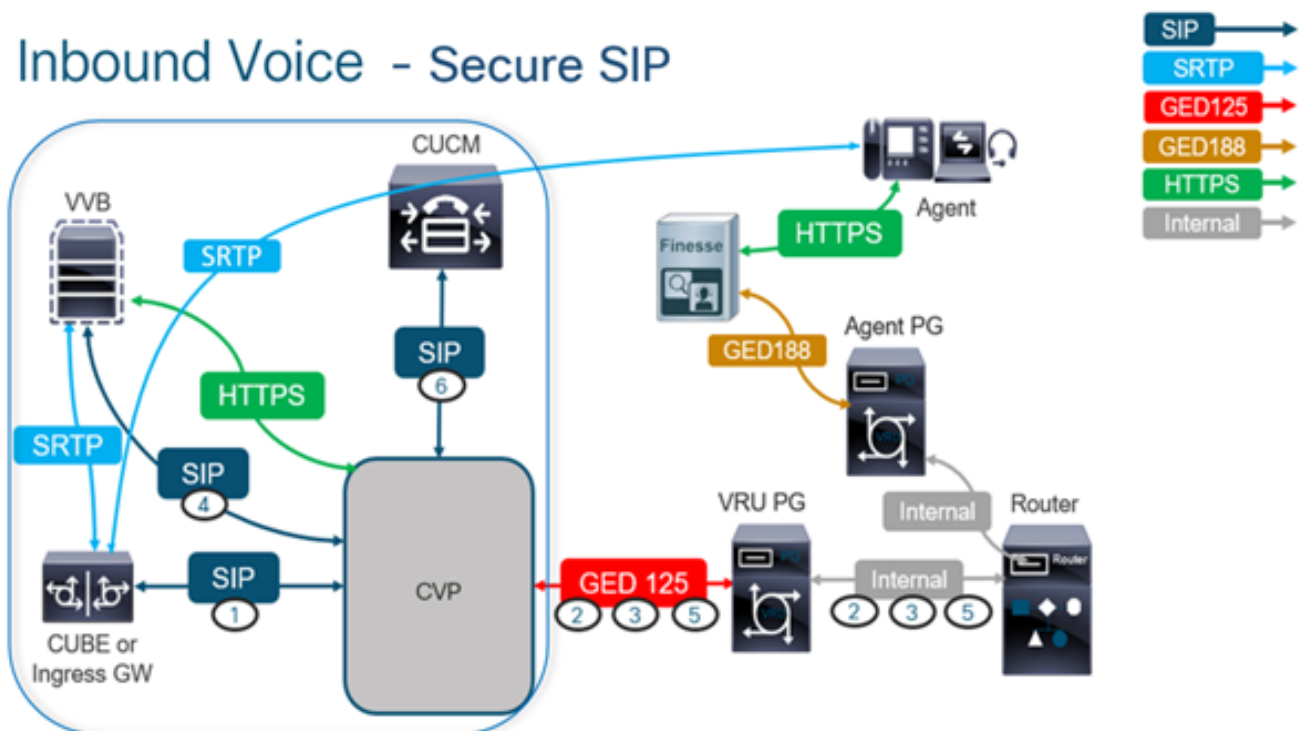
Composants utilisés

Les informations contenues dans ce document sont basées sur Package Contact Center Enterprise (PCCE), CVP, CVVB et CUCM version 12.6, mais elles s'appliquent également aux versions antérieures.

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.

Configurer

Le schéma suivant montre les composants impliqués dans la signalisation SIP dans le flux d'appels complet du centre de contact. Lorsqu'un appel vocal arrive sur le système, il arrive d'abord via la passerelle d'entrée ou CUBE. Par conséquent, démarrez les configurations SIP sécurisées sur CUBE. Configurez ensuite CVP, CVVB et CUCM.



Tâche 1. Configuration sécurisée CUBE

Dans cette tâche, configurez CUBE pour sécuriser les messages du protocole SIP.

Configurations requises :

- Configuration d'un point de confiance par défaut pour l'agent utilisateur SIP
- Modifier les terminaux de numérotation dial-peer pour utiliser TLS (Transport Layer Security)

Étapes :

1. Ouvrez une session Secure Shell (SSH) vers CUBE.
2. Exécutez ces commandes pour que la pile SIP utilise le certificat de l'autorité de certification

du CUBE. CUBE établit une connexion SIP TLS de/vers CUCM (198.18.133.3) et CVP (198.18.133.13).

```
conf t sip-ua transport tcp tls v1.2 crypto signaling remote-addr 198.18.133.3 255.255.255.255 trustpoint ms-ca-name crypto signaling remote-addr 198.18.133.13 255.255.255.255 trustpoint ms-ca-name exit
```

```
CC-VCUBE(config)#sip-ua
CC-VCUBE(config-sip-ua)#transport tcp tls v1.2
CC-VCUBE(config-sip-ua)#crypto signaling remote-addr 198.18.133.3 255.255.255.255 trustpoint ms-ca-name
CC-VCUBE(config-sip-ua)#crypto signaling remote-addr 198.18.133.13 255.255.255.255 trustpoint ms-ca-name
CC-VCUBE(config-sip-ua)#exit
CC-VCUBE(config)#
```

3. Exécutez ces commandes pour activer TLS sur le terminal de numérotation dial-peer sortant vers CVP. Dans cet exemple, la balise dial-peer 6000 est utilisée pour acheminer les appels vers CVP.

```
Conf t dial-peer voice 6000 voip session target ipv4:198.18.133.13:5061 session transport tcp tls exit
```

```
CC-VCUBE#
CC-VCUBE#Conf t
Enter configuration commands, one per line. End with CNTL/Z.
CC-VCUBE(config)#dial-peer voice 6000 voip
CC-VCUBE(config-dial-peer)#session target ipv4:198.18.133.13:5061
CC-VCUBE(config-dial-peer)#session transport tcp tls
CC-VCUBE(config-dial-peer)#
CC-VCUBE(config-dial-peer)#exit
CC-VCUBE(config)#
```

Tâche 2. Configuration sécurisée CVP

Dans cette tâche, configurez le serveur d'appels CVP pour sécuriser les messages de protocole SIP (SIP TLS).

Étapes :

1. Se connecter à UCCE Web Administration.
2. Naviguez jusqu'à [Call Settings > Route Settings > SIP Server Group](#).

Route Settings

Media Routing Domain Call Type Dialed Number Expanded Call Variables **SIP Server Group**

Properties

Selon vos configurations, vous avez configuré des groupes de serveurs SIP pour CUCM, CVVB et CUBE. Vous devez définir les ports SIP sécurisés sur 5061 pour chacun d'entre eux. Dans cet exemple, les groupes de serveurs SIP suivants sont utilisés :

- [cucm1.dcloud.cisco.com](#) pour CUCM
- [vvb1.dcloud.cisco.com](#) pour CVVB
- [cube1.dcloud.cisco.com](#) pour CUBE

3. Cliquer [cucm1.dcloud.cisco.com](#) et ensuite dans le **Members** , qui affiche les détails de la configuration du groupe de serveurs SIP. Jeu SecurePort par 5061 et cliquez sur **Save** .

Edit cucm1.dcloud.cisco.com

General

Members

List of Group Members



Hostname/IP	Priority	Weight	Port	SecurePort	Site
198.18.133.3	10	10	5060	5061	Main

4. Cliquer `vvb1.dcloud.cisco.com` et ensuite dans le **Members** s'affiche. Définissez SecurePort sur 5061 et cliquez sur **Save**.

Edit vvb1.dcloud.cisco.com

General

Members

List of Group Members



Hostname/IP	Priority	Weight	Port	SecurePort	Site
vvb1.dcloud.cisco.c...	10	10	5060	5061	Main

Tâche 3. Configuration sécurisée CVVB

Dans cette tâche, configurez CVVB pour sécuriser les messages de protocole SIP (SIP TLS).

Étapes :

1. Se connecter à **Cisco VVB Administration** s'affiche.
2. Naviguez jusqu'à **System > System Parameters**.

Cisco Virtualized Voice Browser Administration
For Cisco Unified Communications Solutions

System Applications Subsystems Tools Help

System Parameters
Logout

Cisco Virtualized Voice Browser Administration
System version: 12.5.1.10000-24

3. Dans la **Security Parameters** , sélectionnez **Enable** pour TLS(SIP) . Conserver **Supported TLS(SIP)**

version **comme** TLSv1.2.

Security Parameters		
Parameter Name	Parameter Value	Suggested Value
TLS(SIP)	<input type="radio"/> Disable <input checked="" type="radio"/> Enable	Disable
Supported TLS(SIP) Versions	TLSv1.2	TLSv1.2
▶ Cipher Configuration		TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
SRTSP	<input checked="" type="radio"/> Disable <input type="radio"/> Enable <input type="checkbox"/> Allow RTP (Mixed mode)	Disable

4. Cliquez sur Update. Cliquer ok lorsque vous êtes invité à redémarrer le moteur CVVB.

The screenshot shows the Cisco Virtualized Voice Administration interface. A notification dialog box is displayed over the configuration page, stating: "vwb1.dcloud.cisco.com says Please restart Cisco VVB Engine for the updates to take effect." The dialog has an "OK" button. In the background, the "System Parameters Configuration" page is visible, with "Update" and "Clear" buttons.

5. Ces modifications nécessitent un redémarrage du moteur Cisco VVB. Pour redémarrer le moteur VVB, accédez à Cisco VVB Serviceability puis cliquez sur **Go**.

The screenshot shows the navigation menu of the Cisco VVB Administration interface. The "Cisco VVB Serviceability" option is highlighted in blue. Other options include "Cisco VVB Administration", "Cisco Unified Serviceability", and "Cisco Unified OS Administration". A "Go" button is visible next to the selected option.

6. Naviguez jusqu'à **Tools > Control Center – Network Services**.


The screenshot shows the navigation menu of the Cisco VVB Administration interface. The "Control Center - Network Services" option is highlighted in green. Other options include "Tools" and "Help".

7. Choisir Engine et cliquez sur **Restart**.

Control Center - Network Services



Status

 Ready

Select Server

Server *

System Services	
	Service Name
<input type="radio"/>	Perfmon Counter Service
<input type="radio"/>	▼Cluster View Daemon
	▶Manager Manager
<input checked="" type="radio"/>	▼Engine
	▶Manager Manager
	▶Subsystem Manager

Tâche 4. Configuration sécurisée CUCM

Afin de sécuriser les messages SIP sur CUCM, effectuez les configurations suivantes :

- Définir le mode de sécurité CUCM sur Mixed Mode
- Configuration des profils de sécurité de la ligne principale SIP pour CUBE et CVP
- Associer des profils de sécurité de liaison SIP aux liaisons SIP respectives
- Communication sécurisée des périphériques des agents avec CUCM

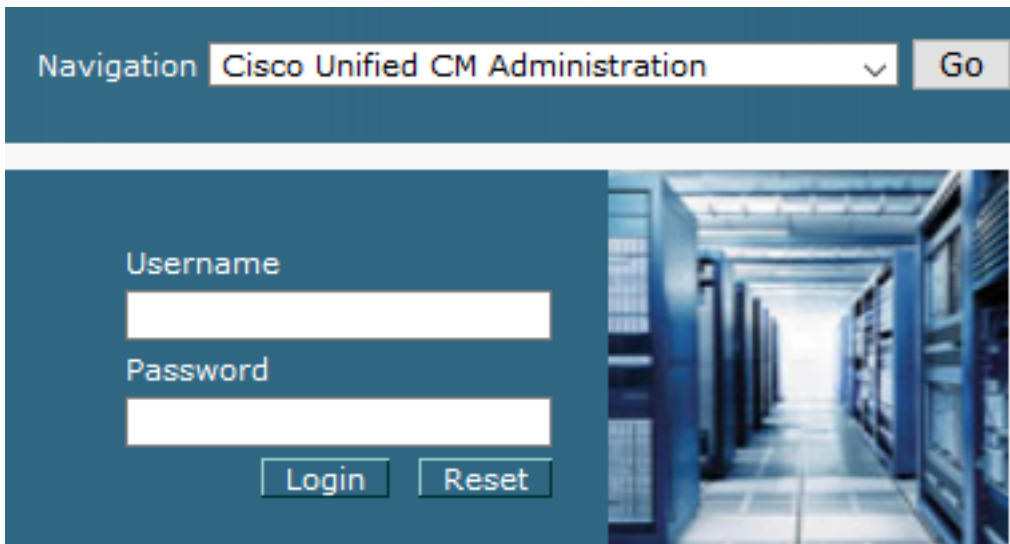
Définir le mode de sécurité CUCM sur Mixed Mode

CUCM prend en charge deux modes de sécurité :

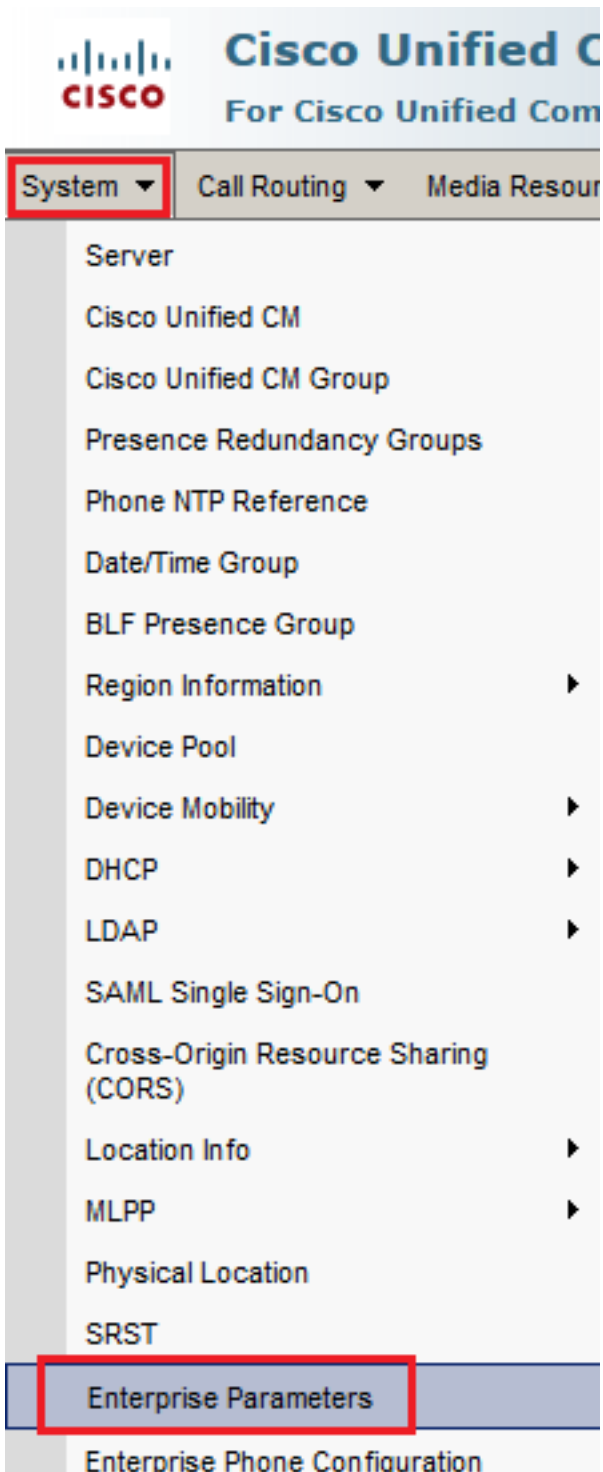
- Mode non sécurisé (mode par défaut)
- Mode mixte (mode sécurisé)

Étapes :

1. Afin de définir le mode de sécurité sur Mixed Mode, connectez-vous à Cisco Unified CM Administration interface.



2. Une fois que vous êtes connecté à CUCM, accédez à [System > Enterprise Parameters](#).



3. Sous le Security Parameters Section, vérifiez si Cluster Security Mode est défini sur 0.



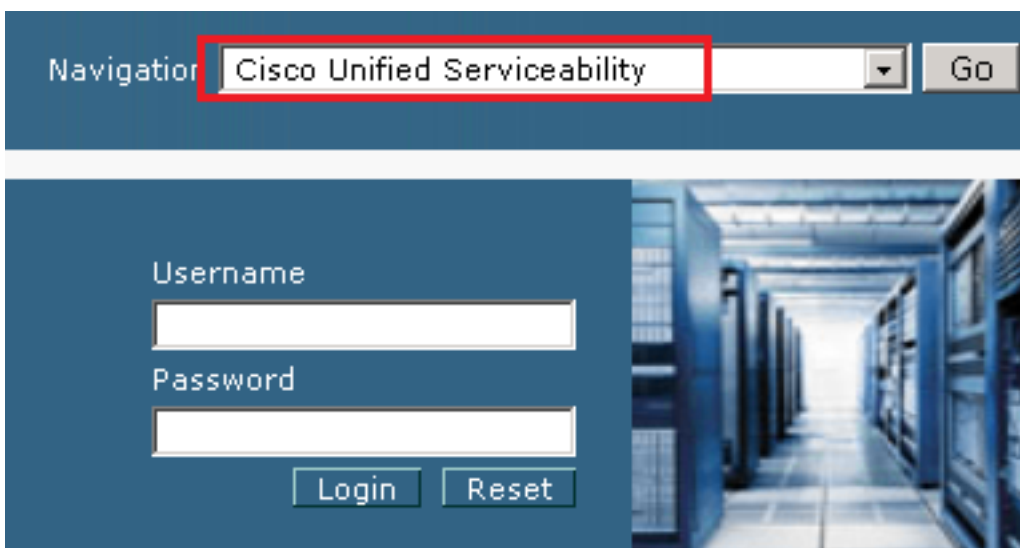
4. Si le mode de sécurité du cluster est défini sur 0, cela signifie que le mode de sécurité du cluster est défini sur non sécurisé. Vous devez activer le mode mixte à partir de l'interface de ligne de commande.
5. Ouvrez une session SSH sur le CUCM.
6. Après vous être connecté à CUCM via SSH, exécutez cette commande : `utils ctl set-cluster mixed-`

mode

7. Type **y** et cliquez sur **Entrée** lorsque vous y êtes invité. Cette commande définit le mode de sécurité du cluster sur le mode mixte.

```
admin:utils ctl set-cluster mixed-mode
This operation will set the cluster to Mixed mode. Auto-registration is enabled on at least one CM node. Do you want to continue? (y/n): y
Moving Cluster to Mixed Mode
Cluster set to Mixed Mode
Please restart Cisco CallManager service and Cisco CTIManager services on all the nodes in the cluster that run these services.
admin:
```

8. Pour que les modifications prennent effet, redémarrez Cisco CallManager et Cisco CTIManager services.
9. Afin de redémarrer les services, naviguez et connectez-vous à Cisco Unified Serviceability.



10. Une fois que vous êtes connecté, accédez à **Tools > Control Center – Feature Services**.

Cisco Unified Serviceability
For Cisco Unified Communications Solutions

Alarm ▾ Trace ▾ **Tools ▾** Snmp ▾ CallHome ▾ Help ▾

Service Activation

Control Center - Feature Services

Control Center - Network Services

Serviceability Reports Archive

Audit Log Configuration

Locations ▶

Dialed Number Analyzer

CDR Analysis and Reporting

CDR Management

System version
VMware Install

User admin last logged in
Copyright © 1999 - All rights reserved.
This product contains... compliance with U.S.
A summary of U.S. I...
For information about...

11. Sélectionnez le serveur, puis cliquez sur **Go**.

Select Server

Server*

12. Sous les services CM, sélectionnez **Cisco CallManager** puis cliquez sur **Restart** en haut de la page.

CM Services	
	Service Name
<input checked="" type="radio"/>	Cisco CallManager
<input type="radio"/>	Cisco Unified Mobile Voice Access Service
<input type="radio"/>	Cisco IP Voice Media Streaming App
<input type="radio"/>	Cisco CTIManager
<input type="radio"/>	Cisco Extension Mobility

13. Confirmez le message contextuel et cliquez sur **OK**. Attendez que le service redémarre correctement.

Restarting Service. It may take a while... Please wait for the page to refresh.
If you see Starting/Stopping state, refresh the page after sometime to show the right status.



14. Après un redémarrage réussi de Cisco CallManager, choisissez Cisco CTIManager puis cliquez sur **Restart** bouton de redémarrage Cisco CTIManager service.

CM Services	
	Service Name
<input type="radio"/>	Cisco CallManager
<input type="radio"/>	Cisco Unified Mobile Voice Access Service
<input type="radio"/>	Cisco IP Voice Media Streaming App
<input checked="" type="radio"/>	Cisco CTIManager
<input type="radio"/>	Cisco Extension Mobility

15. Confirmez le message contextuel et cliquez sur **OK**. Attendez que le service redémarre correctement.

Restarting Service. It may take a while... Please wait for the page to refresh.
If you see Starting/Stopping state, refresh the page after sometime to show the right status.



16. Une fois les services redémarrés, vérifiez que le mode de sécurité du cluster est défini sur le mode mixte, accédez à l'administration de CUCM comme expliqué à l'étape 5. Vérifiez ensuite la **Cluster Security Mode**. Maintenant, il doit être défini sur **1**.

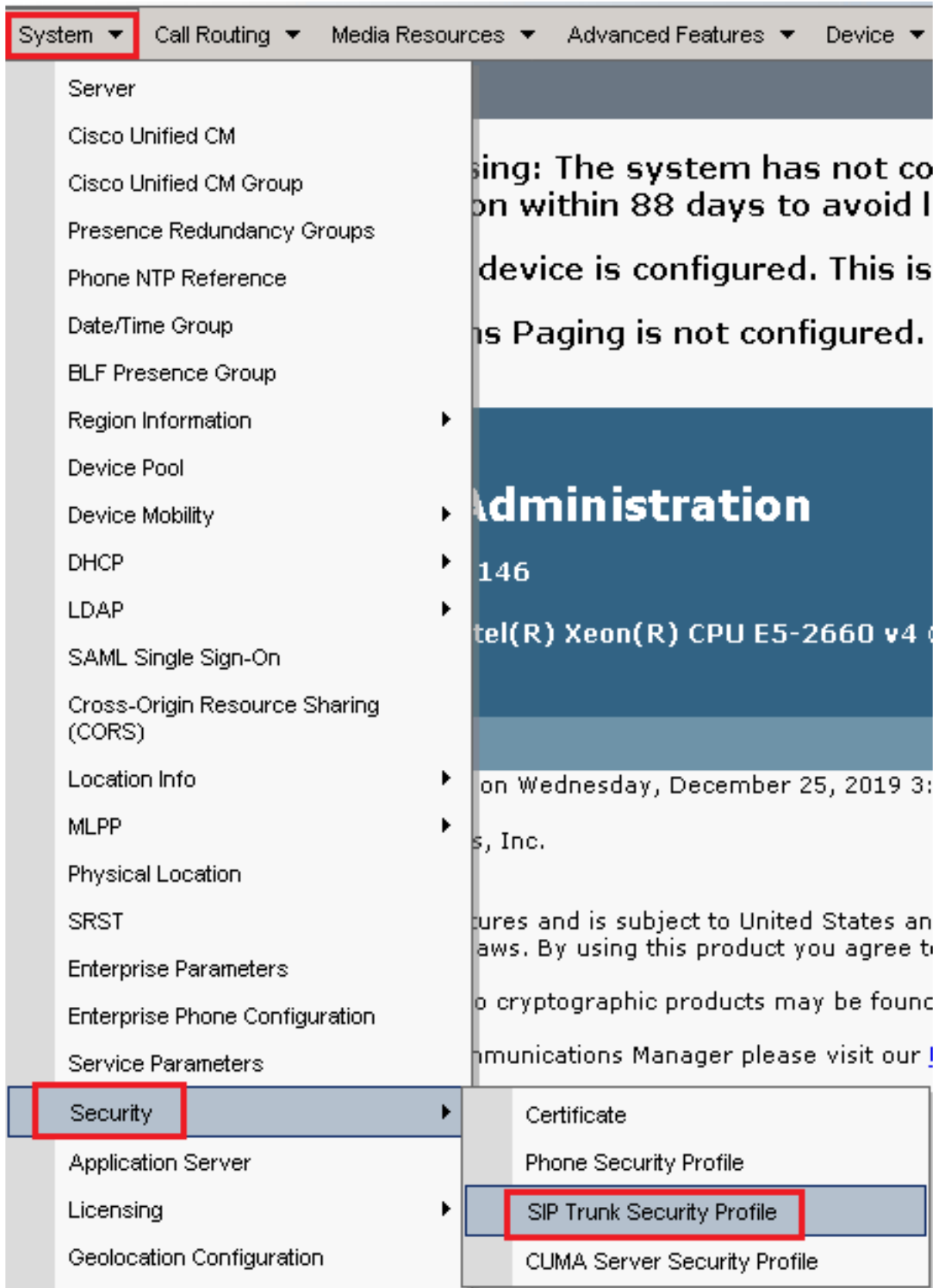
Security Parameters	
Cluster Security Mode *	1
Cluster SIPOAuth Mode *	Disabled

Configuration des profils de sécurité de la ligne principale SIP pour CUBE et CVP

Étapes :

1. Se connecter à CUCM administration interface.

2. Après vous être connecté à CUCM, accédez à System > Security > SIP Trunk Security Profile afin de créer un profil de sécurité de périphérique pour CUBE.



3. En haut à gauche, cliquez sur Add New afin d'ajouter un nouveau profil.

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features







Find and List SIP Trunk Security Profiles

 Add New  Select All  Clear All  Delete Selected



4. Configurer SIP Trunk Security Profile comme le montre cette image, puis cliquez sur **Save** en bas à gauche de la page pour **Save** le.

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk A

SIP Trunk Security Profile Configuration Related Links: [Back](#)

 Save  Delete  Copy  Reset  Apply Config  Add New

- Status -

-  Add successful
-  Reset of the trunk is required to have changes take effect.

- SIP Trunk Security Profile Information -

Name*	SecureSIPTLSforCube
Description	
Device Security Mode	Encrypted ▾
Incoming Transport Type*	TLS ▾
Outgoing Transport Type	TLS ▾
<input type="checkbox"/> Enable Digest Authentication	
Nonce Validity Time (mins)*	600
Secure Certificate Subject or Subject Alternate Name	SIP-GW
Incoming Port*	5061
<input type="checkbox"/> Enable Application level authorization	
<input type="checkbox"/> Accept presence subscription	
<input type="checkbox"/> Accept out-of-dialog refer**	
<input type="checkbox"/> Accept unsolicited notification	
<input 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 ▾

5. Assurez-vous de définir le Secure Certificate Subject or Subject Alternate Name au nom commun (CN) du certificat CUBE car il doit correspondre.

6. Cliquez sur Copy et de modifier le Name par SecureSipTLSforCVP et la Secure Certificate Subject au CN du certificat du serveur d'appels CVP car il doit correspondre. Cliquer Save s'affiche.

Status

- Add successful
- Reset of the trunk is required to have changes take effect.

SIP Trunk Security Profile Information

Name* SecureSIPTLSforCvp

Description

Device Security Mode Encrypted

Incoming Transport Type* TLS

Outgoing Transport Type TLS

Enable Digest Authentication

Nonce Validity Time (mins)* 600

Secure Certificate Subject or Subject Alternate Name cvp1.dcloud.cisco.com

Incoming Port* 5061

Enable Application level authorization

Accept presence subscription

Accept out-of-dialog refer**

Accept unsolicited notification

Accept replaces header

Transmit security status

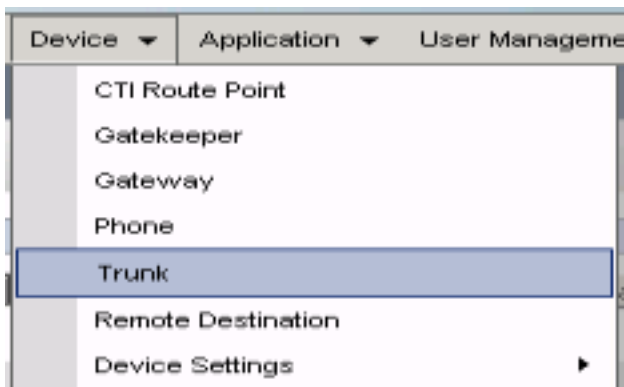
Allow charging header

SIP V.150 Outbound SDP Offer Filtering* Use Default Filter

Associer des profils de sécurité de liaison SIP aux liaisons SIP respectives

Étapes :

1. Sur la page CUCM Administration, accédez à Device > Trunk.



2. Recherchez la ligne principale CUBE. Dans cet exemple, le nom de la liaison CUBE est vCube . Cliquez Find.

Trunks (1 - 5 of 5)

Find Trunks where Device Name begins with vCube Find Clear Filter

Name	Description	Calling Search Space	Device Pool	Route Pattern	Partition
vCUBE	dCloud_CSS	dCloud_CSS	dCloud_DP	cloudcherry.sip.twilio.com	dCloud_PT
vCUBE	dCloud_CSS	dCloud_CSS	dCloud_DP	7800	PSTN_Incoming_Numbers
vCUBE	dCloud_CSS	dCloud_CSS	dCloud_DP	6016	PSTN_Incoming_Numbers
vCUBE	dCloud_CSS	dCloud_CSS	dCloud_DP	7019	PSTN_Incoming_Numbers
vCUBE	dCloud_CSS	dCloud_CSS	dCloud_DP	44413XX	Robot Agent Remote Destinations

3. Cliquez sur vCUBE pour ouvrir la page de configuration de la liaison vCUBE.

4. Faites défiler jusqu'à SIP Information , puis modifiez la Destination Port par 5061.

5. Changement SIP Trunk Security Profile par SecureSIPTLSForCube.

SIP Information

Destination

Destination Address is an SRV

Destination Address	Destination Address IPv6	Destination Port
1* 198.18.133.226		5061

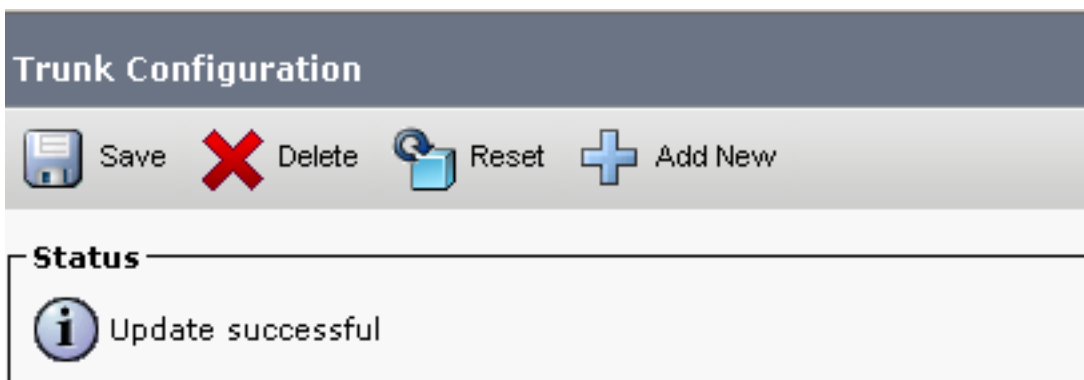
MTP Preferred Originating Codec* 711ulaw

BLF Presence Group* Standard Presence group

SIP Trunk Security Profile* SecureSIPTLSforCube

Rerouting Calling Search Space < None >


6. Cliquez Save puis Rest afin de Save et d'appliquer les modifications.



The configuration changes will not take effect on the trunk until a reset is performed. Use the Reset button or Job Scheduler to execute the reset.

OK

7. Naviguez jusqu'à **Device > Trunket** recherchez la ligne principale CVP. Dans cet exemple, le nom de la liaison CVP est **cvp-SIP-Trunk** . Cliquez **Find**.

Trunks (1 - 1 of 1)				
Find Trunks where				
<input type="checkbox"/>	Device Name	begins with	cvp	Find
Clear Filter <input type="button" value="+"/> <input type="button" value="-"/>				
Select item or enter search text				
<input type="checkbox"/>	Name ^	Description	Calling Search Space	Device Pool
<input type="checkbox"/>	 CVP-SIP-Trunk	CVP-SIP-Trunk	dCloud_CSS	dCloud_DP






8. Cliquez **CVP-SIP-Trunk** afin d'ouvrir la page de configuration du trunk CVP.

9. Faites défiler jusqu'à **SIP Information** et de modifier **Destination Port** par **5061** .

10. Changement **SIP Trunk Security Profile** par **SecureSIPTLSForCvp**.

SIP Information		
Destination		
<input type="checkbox"/> Destination Address is an SRV		
Destination Address	Destination Address IPv6	Destination Port
1* 198.18.133.13		5061
MTP Preferred Originating Codec*	711ulaw	
BLF Presence Group*	Standard Presence group	
SIP Trunk Security Profile*	SecureSIPTLSforCvp	

11. Cliquez **Save** puis **Rest** afin de save et d'appliquer les modifications.

Trunk Configuration	
 Save	 Delete
 Reset	 Add New
Status	
 Update successful	

The configuration changes will not take effect on the trunk until a reset is performed. Use the Reset button or Job Scheduler to execute the reset.

OK

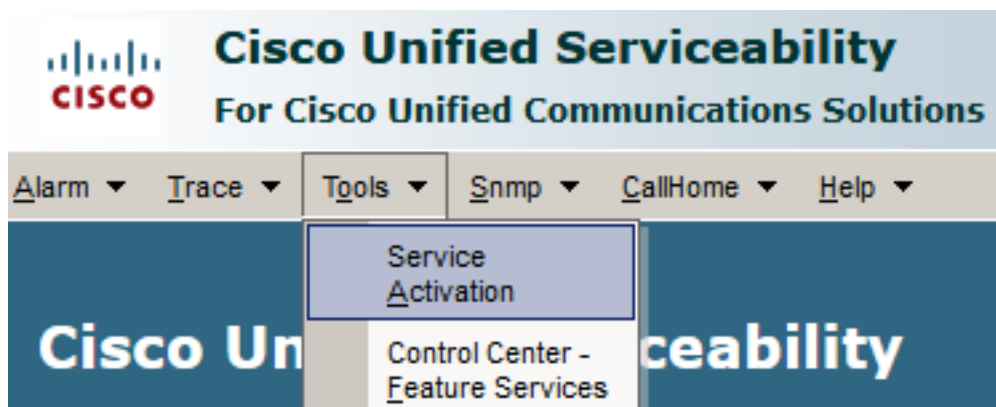
Communication sécurisée des périphériques des agents avec CUCM

Afin d'activer les fonctions de sécurité pour un périphérique, vous devez installer un certificat LSC

(Locally Significant Certificate) et attribuer un profil de sécurité à ce périphérique. Le LSC possède la clé publique pour le terminal, qui est signée par la clé privée CAPF (Certificate Authority Proxy Function). Il n'est pas installé sur les téléphones par défaut.

Étapes :

1. Se connecter à Cisco Unified Serviceability Interface.
2. Naviguez jusqu'à `Tools > Service Activation`.



3. Sélectionnez le serveur CUCM et cliquez sur `Go`.

Service Activation

Select Server

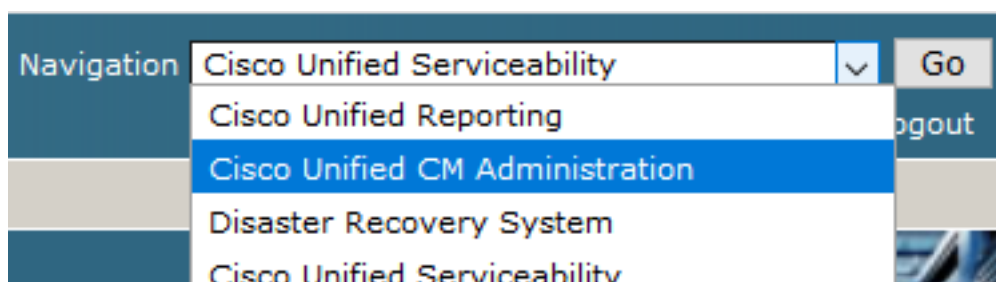
Server*

4. Cliquez sur `Cisco Certificate Authority Proxy Function` et cliquez sur `Save` pour activer le service. Cliquez sur `Ok` pour confirmer.

Security Services

	Service Name	Activation Status
<input checked="" type="checkbox"/>	Cisco Certificate Authority Proxy Function	Deactivated
<input type="checkbox"/>	Cisco Certificate Enrollment Service	Deactivated

5. Assurez-vous que le service est activé, puis accédez à `Cisco Unified CM Administration`.



6. Une fois que vous êtes connecté à l'administration de CUCM, accédez à `System > Security > Phone Security Profile` afin de créer un profil de sécurité de périphérique pour le périphérique

agent.

The screenshot shows the Cisco Unified CM Administration web interface. At the top, the Cisco logo and the title "Cisco Unified CM Administration" are visible, along with the subtitle "For Cisco Unified Communications Solutions". Below the header is a navigation bar with several menu items: "System", "Call Routing", "Media Resources", "Advanced Features", and "Device". The "System" menu is expanded, showing a list of sub-items. The "Security" item is highlighted with a red box. A secondary menu is open under "Security", listing "Certificate", "Phone Security Profile", "SIP Trunk Security Profile", and "CUMA Server Security Profile". The "Phone Security Profile" item is also highlighted with a red box. The background of the page shows a blurred view of a configuration page with some text visible, including "device is configured. The", "Paging is not configur", and "Administration".

7. Recherchez les profils de sécurité correspondant au type de périphérique de votre agent. Dans cet exemple, un téléphone logiciel est utilisé, alors choisissez Cisco Unified Client Services

Framework - Standard SIP Non-Secure Profile . Cliquez Copy  afin de copier ce profil.

Phone Security Profile (1 - 1 of 1) Rows per Page 50







Find Phone Security Profile where Name contains client Find Clear Filter + -

Name	Description	Copy
Cisco Unified Client Services Framework - Standard SIP Non-Secure Profile	Cisco Unified Client Services Framework - Standard SIP Non-Secure Profile	


8. Renommer le profil en Cisco Unified Client Services Framework - Secure Profile, modifiez les paramètres comme indiqué dans cette image, puis cliquez sur Save en haut à gauche de la page.

System Call Routing Media Resources Advanced Features Device Application User

Phone Security Profile Configuration

 Save  Delete  Copy  Reset  Apply Config  Add New

Status

 Add successful

Phone Security Profile Information

Product Type: Cisco Unified Client Services Framework
Device Protocol: SIP

Name* Cisco Unified Client Services Framework - Secure Profile
Description Cisco Unified Client Services Framework - Secure Profile
Device Security Mode Encrypted
Transport Type* TLS

TFTP Encrypted Config
 Enable OAuth Authentication

Phone Security Profile CAPF Information

Authentication Mode* By Null String
Key Order* RSA Only
RSA Key Size (Bits)* 2048
EC Key Size (Bits) < None >

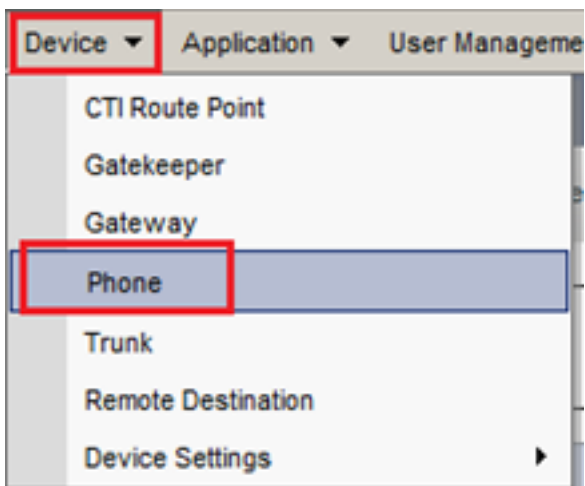
Note: These fields are related to the CAPF Information settings on the Phone Configuration page.

Parameters used in Phone

SIP Phone Port* 5061

Save Delete Copy Reset Apply Config Add New

9. Une fois le profil de périphérique téléphonique créé, accédez à Device > Phone.



10. Cliquer Find pour afficher la liste de tous les téléphones disponibles, cliquez sur téléphone de l'agent.
11. La page Agent phone configuration s'ouvre. Rechercher Certification Authority Proxy Function (CAPF) Information de l'Aide. Afin d'installer LSC, définissez Certificate Operation par Install/Upgrade et Operation Completes by à une date ultérieure.

Certification Authority Proxy Function (CAPF) Information

Certificate Operation*	Install/Upgrade
Authentication Mode*	By Null String
Authentication String	<input type="text"/>
<input type="button" value="Generate String"/>	
Key Order*	RSA Only
RSA Key Size (Bits)*	2048
EC Key Size (Bits)	<input type="text"/>
Operation Completes By	2021 04 16 12 (YYYY:MM:DD:HH)

Certificate Operation Status: None
 Note: Security Profile Contains Addition CAPF Settings.

12. Rechercher Protocol Specific Information de l'Aide. Changement Device Security Profile par Cisco Unified Client Services Framework – Secure Profile.

Protocol Specific Information

Packet Capture Mode*	None
Packet Capture Duration	0
BLF Presence Group*	Standard Presence group
SIP Dial Rules	< None >
MTP Preferred Originating Codec*	711ulaw
Device Security Profile*	Cisco Unified Client Services Framework - Secure F
Rerouting Calling Search Space	Cisco Unified Client Services Framework - Secure Profile

13. Cliquer Save en haut à gauche de la page. Vérifiez que les modifications ont été

enregistrées et cliquez sur **Reset**.

The screenshot shows the top navigation bar with menus: System, Call Routing, Media Resources, Advanced Features, Device, and Agent. Below is the 'Phone Configuration' section. A toolbar contains icons for Save, Delete, Copy, Reset, Apply Config, and Add New. The 'Reset' icon is highlighted with a red box. Below the toolbar is a 'Status' section with a message: 'Update successful', which is also highlighted with a red box.

14. Une fenêtre contextuelle s'ouvre, cliquez sur **Reset** pour confirmer l'action.

The screenshot shows a 'Device Reset' dialog box. It has two buttons: 'Reset' and 'Restart'. The 'Reset' button is highlighted with a red box. Below the buttons is a 'Status' section with a message: 'Status: Ready'. Below that is a 'Reset Information' section.

15. Une fois que le périphérique agent s'est à nouveau enregistré auprès de CUCM, actualisez la page en cours et vérifiez que le contrôleur LSC est correctement installé.

Chèque Certification Authority Proxy Function (CAPF) Information section, Certificate Operation doit être défini sur No Pending Operation, et Certificate Operation Status est défini sur Upgrade Success .

The screenshot shows the 'Certification Authority Proxy Function (CAPF) Information' configuration page. The 'Certificate Operation' dropdown is set to 'No Pending Operation' and is highlighted with a red box. Other settings include: Authentication Mode: By Null String; Authentication String: (empty field); Generate String: (button); Key Order: RSA Only; RSA Key Size (Bits): 2048; EC Key Size (Bits): (empty field); Operation Completes By: 2021 04 16 12 (YYYY:MM:DD:HH). At the bottom, the 'Certificate Operation Status' is 'Upgrade Success', which is highlighted with a red box. A note at the bottom states: 'Note: Security Profile Contains Addition CAPF Settings.'

16. Reportez-vous aux étapes. 7-13 afin de sécuriser les autres agents et les périphériques que

vous souhaitez utiliser pour sécuriser SIP avec CUCM.

Vérifier

Afin de valider que la signalisation SIP est correctement sécurisée, effectuez ces étapes :

1. Ouvrez une session SSH sur vCUBE, exécutez la commande `show sip-ua connections tcp tls detail`, et vérifiez qu'aucune connexion TLS n'est établie avec CVP (198.18.133.13).

```
CC-VCUBE#show sip-ua connections tcp tls detail
Total active connections      : 1
No. of send failures         : 0
No. of remote closures      : 34
No. of conn. failures        : 0
No. of inactive conn. ageouts : 12
TLS client handshake failures : 0
TLS server handshake failures : 0

-----Printing Detailed Connection Report-----
Note:
** Tuples with no matching socket entry
  - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port>'
    to overcome this error condition
++ Tuples with mismatched address/port entry
  - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port> id <connid>'
    to overcome this error condition

Remote-Agent:198.18.133.3, Connections-Count:1
  Remote-Port Conn-Id Conn-State WriteQ-Size Local-Address TLS-Version
  =====
  44868      49 Established      0          -          TLSv1.2

Remote-Agent:198.18.133.13, Connections-Count:0

----- SIP Transport Layer Listen Sockets -----
  Conn-Id      Local-Address
  =====
  0            [0.0.0.0]:5061:
```



Remarque : actuellement, une seule session TLS active avec CUCM, pour les options SIP, est activée sur CUCM (198.18.133.3). Si aucune option SIP n'est activée, aucune connexion SIP TLS n'existe.

2. Connectez-vous à CVP et démarrez Wireshark.
3. Effectuez un test d'appel vers le numéro du centre de contact.
4. Accédez à la session CVP ; sur Wireshark, exécutez ce filtre afin de vérifier la signalisation SIP avec CUBE :
`ip.addr == 198.18.133.226 && tls && tcp.port==5061`

No.	Time	Source	Destination	Protocol	Length	Info
2409	63.180370	198.18.133.226	198.18.133.13	TLSv1.2	173	Client Hello
2411	63.183691	198.18.133.13	198.18.133.226	TLSv1.2	1153	Server Hello, Certificate, Server Hello Done
2414	63.188871	198.18.133.226	198.18.133.13	TLSv1.2	396	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
2415	63.202820	198.18.133.13	198.18.133.226	TLSv1.2	60	Change Cipher Spec
2416	63.203063	198.18.133.13	198.18.133.226	TLSv1.2	123	Encrypted Handshake Message
2419	63.207380	198.18.133.226	198.18.133.13	TLSv1.2	614	Application Data
2421	63.255349	198.18.133.13	198.18.133.226	TLSv1.2	635	Application Data
2508	63.495508	198.18.133.13	198.18.133.226	TLSv1.2	1067	Application Data
2565	63.505008	198.18.133.226	198.18.133.13	TLSv1.2	587	Application Data

Vérification : la connexion SIP sur TLS est-elle établie ? Si oui, la sortie confirme que les signaux SIP entre CVP et CUBE sont sécurisés.

5. Vérifiez la connexion SIP TLS entre CVP et CVVB. Dans la même session Wireshark, exécutez ce filtre :

```
ip.addr == 198.18.133.143 && tls && tcp.port==5061
```

No.	Time	Source	Destination	Protocol	Length	Info
2490	63.358533	198.18.133.13	198.18.133.143	TLSv1.2	171	Client Hello
2494	63.360224	198.18.133.143	198.18.133.13	TLSv1.2	1205	Server Hello, Certificate, Server Hello Done
2496	63.365714	198.18.133.13	198.18.133.143	TLSv1.2	321	Client Key Exchange
2498	63.405567	198.18.133.13	198.18.133.143	TLSv1.2	129	Change Cipher Spec, Encrypted Handshake Message
2501	63.434468	198.18.133.143	198.18.133.13	TLSv1.2	129	Change Cipher Spec, Encrypted Handshake Message
2503	63.442731	198.18.133.13	198.18.133.143	TLSv1.2	631	Application Data
2505	63.446286	198.18.133.143	198.18.133.13	TLSv1.2	539	Application Data
2506	63.472083	198.18.133.143	198.18.133.13	TLSv1.2	1003	Application Data
2566	63.512809	198.18.133.13	198.18.133.143	TLSv1.2	715	Application Data

Vérification : la connexion SIP sur TLS est-elle établie ? Si oui, la sortie confirme que les signaux SIP entre CVP et CVVB sont sécurisés.

6. Vous pouvez également vérifier la connexion SIP TLS avec CVP depuis CUBE. Accédez à la session SSH vCUBE et exécutez cette commande pour vérifier les signaux SIP sécurisés :

```
show sip-ua connections tcp tls detail
```



```

CC-VCUBE#show sip-ua connections tcp tls detail
Total active connections      : 2
No. of send failures         : 0
No. of remote closures       : 0
No. of conn. failures        : 0
No. of inactive conn. ageouts : 0
TLS client handshake failures : 0
TLS server handshake failures : 0

-----Printing Detailed Connection Report-----
Note:
** Tuples with no matching socket entry
  - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port>'
    to overcome this error condition
++ Tuples with mismatched address/port entry
  - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port> id <connid>'
    to overcome this error condition

Remote-Agent:198.18.133.3, Connections-Count:1
  Remote-Port Conn-Id Conn-State  WriteQ-Size Local-Address TLS-Version
  =====
      38896      2 Established      0           -           TLSv1.2

Remote-Agent:198.18.133.13, Connections-Count:1
  Remote-Port Conn-Id Conn-State  WriteQ-Size Local-Address TLS-Version
  =====
      5061      3 Established      0           -           TLSv1.2

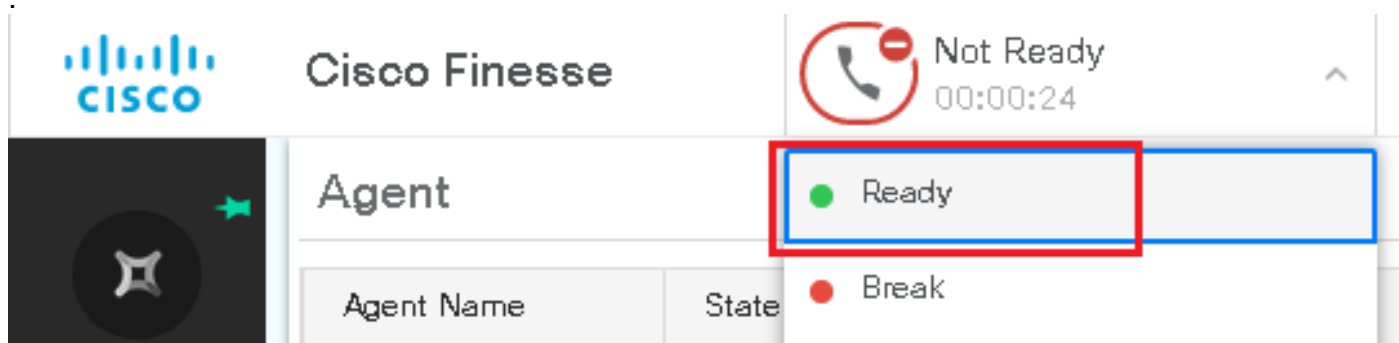
----- SIP Transport Layer Listen Sockets -----
  Conn-Id          Local-Address
  =====
      0            [0.0.0.0]:5061:

```

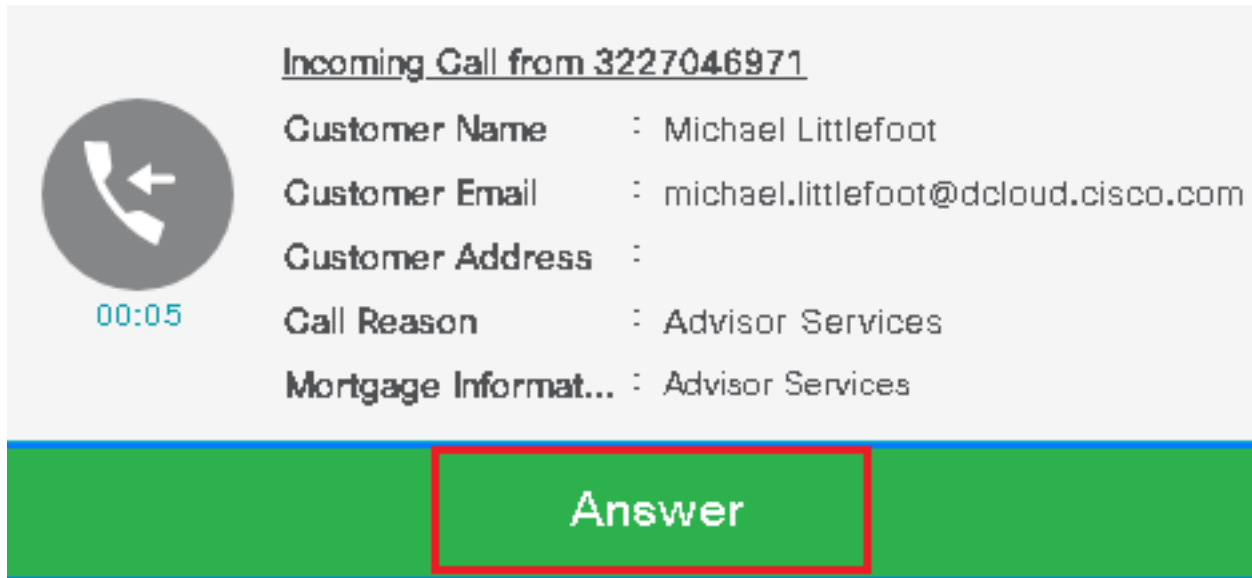
Vérification : la connexion SIP sur TLS est-elle établie avec CVP ? Si oui, la sortie confirme que les signaux SIP entre CVP et CUBE sont sécurisés.

7. À ce moment, l'appel est actif et vous entendez MUSIQUE D'ATTENTE (MOH) car aucun agent n'est disponible pour répondre à l'appel.

8. Rendre l'agent disponible pour répondre à l'appel.



9. L'agent est réservé et l'appel lui est acheminé. Cliquer Answer pour répondre à l'appel.



Incoming Call from 3227046971

Customer Name : Michael Littlefoot
Customer Email : michael.littlefoot@dcloud.cisco.com
Customer Address :
Call Reason : Advisor Services
Mortgage Informat... : Advisor Services

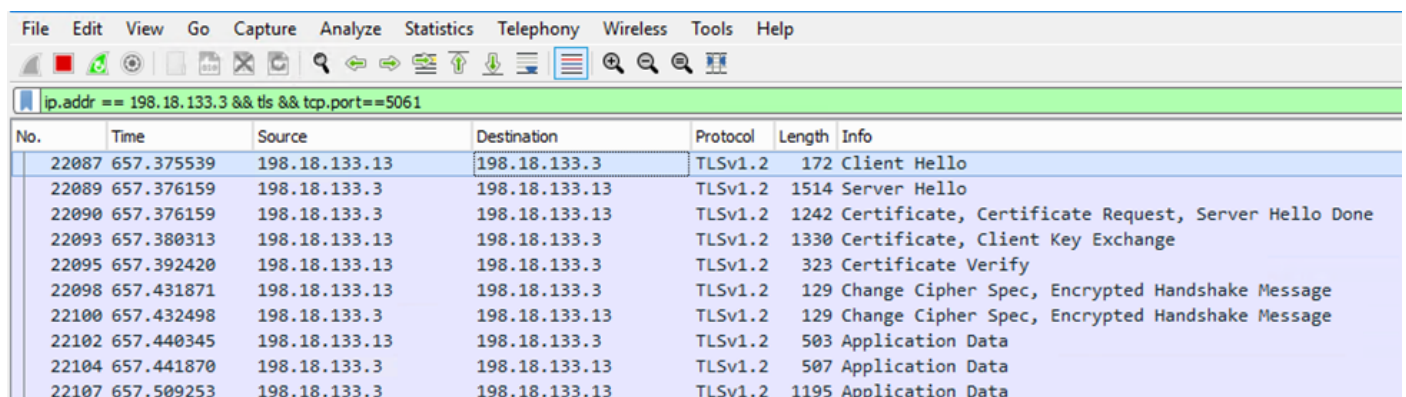
00:05

Answer

10. L'appel se connecte à l'agent.

11. Afin de vérifier les signaux SIP entre CVP et CUCM, accédez à la session CVP et exécutez ce filtre dans Wireshark :

```
ip.addr == 198.18.133.3 && tls && tcp.port==5061
```



No.	Time	Source	Destination	Protocol	Length	Info
22087	657.375539	198.18.133.13	198.18.133.3	TLSv1.2	172	Client Hello
22089	657.376159	198.18.133.3	198.18.133.13	TLSv1.2	1514	Server Hello
22090	657.376159	198.18.133.3	198.18.133.13	TLSv1.2	1242	Certificate, Certificate Request, Server Hello Done
22093	657.380313	198.18.133.13	198.18.133.3	TLSv1.2	1330	Certificate, Client Key Exchange
22095	657.392420	198.18.133.13	198.18.133.3	TLSv1.2	323	Certificate Verify
22098	657.431871	198.18.133.13	198.18.133.3	TLSv1.2	129	Change Cipher Spec, Encrypted Handshake Message
22100	657.432498	198.18.133.3	198.18.133.13	TLSv1.2	129	Change Cipher Spec, Encrypted Handshake Message
22102	657.440345	198.18.133.13	198.18.133.3	TLSv1.2	503	Application Data
22104	657.441870	198.18.133.3	198.18.133.13	TLSv1.2	507	Application Data
22107	657.509253	198.18.133.3	198.18.133.13	TLSv1.2	1195	Application Data

Vérification : toutes les communications SIP avec CUCM (198.18.133.3) sont-elles effectuées via TLS ? Si oui, la sortie confirme que les signaux SIP entre CVP et CUCM sont sécurisés.

Dépannage

Si TLS n'est pas établi, exécutez ces commandes sur CUBE pour activer la commande debug TLS pour le dépannage :

- Debug ssl openssl errors
- Debug ssl openssl msg
- Debug ssl openssl states

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.