

Configurer le protocole RTP sécurisé dans Contact Center Enterprise

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configurer](#)

[Tâche 1 : Configuration sécurisée de CUBE](#)

[Tâche 2 : Configuration sécurisée de CVP](#)

[Tâche 3 : Configuration sécurisée de CVVB](#)

[Tâche 4 : Configuration sécurisée de 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 et activer SRTP](#)

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

[Vérifier](#)

Introduction

Ce document décrit comment sécuriser le trafic SRTP (Real-time Transport 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), Customer Voice Portal (CVP) Call Server, 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

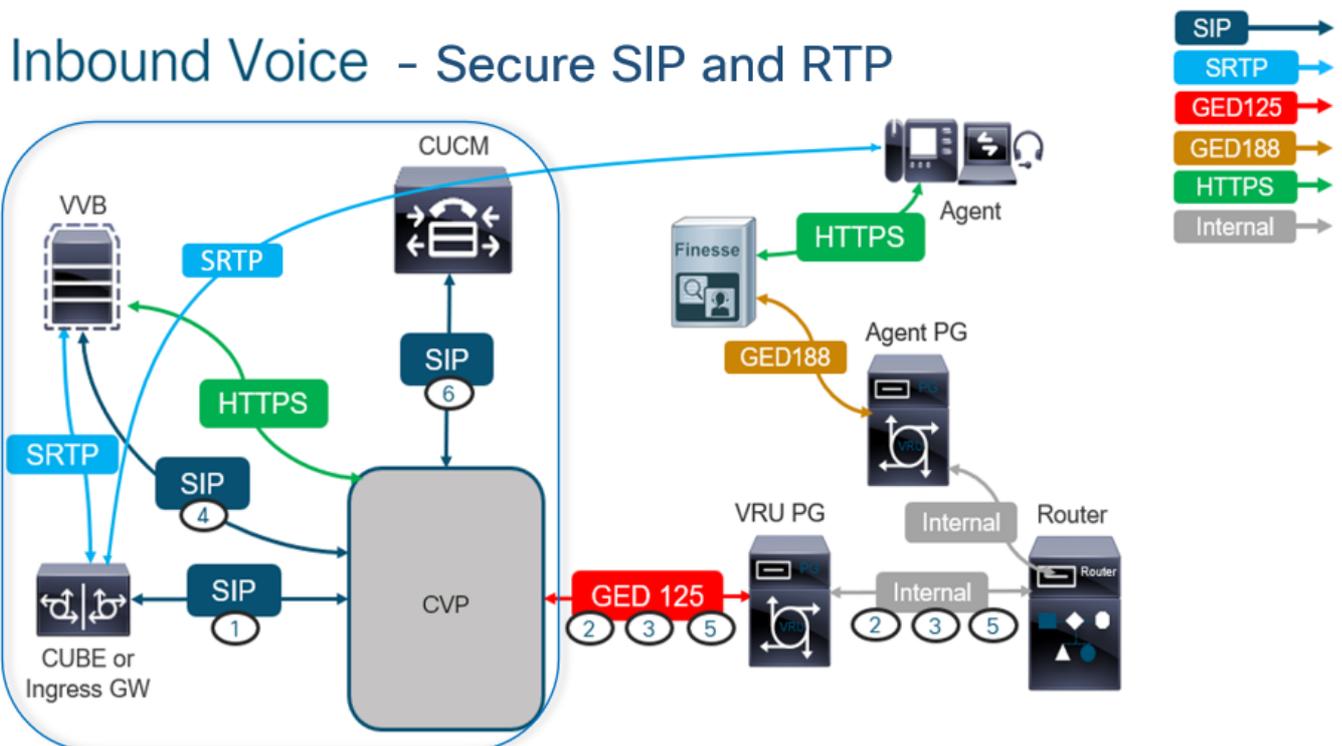
Les informations contenues dans ce document sont basées sur Package Contact Center Enterprise (PCCE), CVP, CVVB et CUCM version 12.6, mais elles s'appliquent également aux versions précédentes.

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

Remarque : dans le flux d'appels complet du centre de contact, pour activer le protocole RTP sécurisé, les signaux SIP sécurisés doivent être activés. Par conséquent, les configurations de ce document permettent à la fois le protocole SIP sécurisé et le protocole SRTP.

Le schéma suivant montre les composants impliqués dans les signaux SIP et RTP 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. Commencez donc les configurations sur CUBE. Configurez ensuite CVP, CVVB et CUCM.



Tâche 1 : Configuration sécurisée de CUBE

Dans cette tâche, vous allez configurer CUBE pour sécuriser les messages de protocole SIP et RTP.

Configurations requises :

- Configurer un point de confiance par défaut pour l'UA SIP
- Modifier les terminaux de numérotation dial-peer pour utiliser TLS et SRTP

Étapes :

1. Ouvrez une session SSH sur CUBE.
2. Exécutez ces commandes pour que la pile SIP utilise le certificat CA 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 srtp exit
```

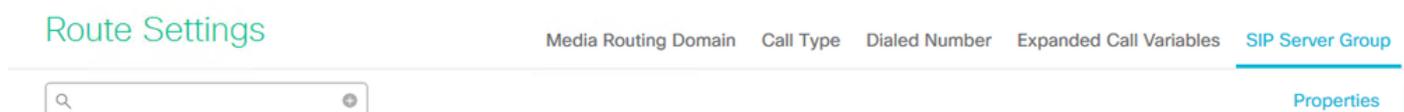
```
CC-VCUBE#
CC-VCUBE#Conf t
Enter configuration commands, one per line. End with CNTL/Z.
CC-VCUBE (config)#dial-peer voice 6000 voip
CC-VCUBE (config-dial-peer)#session target ipv4:198.18.133.13:5061
CC-VCUBE (config-dial-peer)#session transport tcp tls
CC-VCUBE (config-dial-peer)#SRTP
CC-VCUBE (config-dial-peer)#exit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

Tâche 2 : Configuration sécurisée de CVP

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

Étapes :

1. Connectez-vous au UCCE Web Administration.
2. Naviguez jusqu'à Call Settings > Route Settings > SIP Server Group.



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`, puis dans le `Members` qui affiche les détails des configurations de groupe de serveurs SIP. Jeu `SecurePort` par `5061` et cliquez sur `Save`.

Route Settings [Media Routing Domain](#) [Call Type](#) [Dialed Number](#) [Expanded Call Variables](#) **Sip Server Groups** [Routing Pattern](#)

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`, définissez l'option `SecurePort` par `5061` et cliquez sur `Save`.

Route Settings [Media Routing Domain](#) [Call Type](#) [Dialed Number](#) [Expanded Call Variables](#) **Sip Server Groups**

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 de CVVB

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

Étapes :

1. Ouvrez le `Cisco VVB Admin` 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. Sur la page Security Parameters , sélectionnez Enable pour TLS (SIP) . Conservez la Supported TLS(SIP) version as TLSv1.2 et choisissez Enable pour SRTP.

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
SRTP <small>[Crypto Suite : AES_CM_128_HMAC_SHA1_32]</small>	<input type="radio"/> Disable <input checked="" type="radio"/> Enable <input type="checkbox"/> Allow RTP (Mixed mode)	Disable

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

The screenshot shows the 'System Parameters Configuration' page with an 'Update' button. A dialog box is displayed over the page, stating: 'vwb1.dcloud.cisco.com says Please restart Cisco VVB Engine for the updates to take effect.' with an 'OK' button.

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

The screenshot shows the navigation menu with 'Cisco VVB Serviceability' highlighted. Other options include 'Cisco VVB Administration', 'Cisco Unified Serviceability', and 'Cisco Unified OS Administration'. A 'Go' button is visible next to the selected item.

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

The screenshot shows the 'Tools' menu with 'Control Center - Network Services' selected. Other options include 'Performance Configuration and Logging'.

7. Choisir Engine et cliquez sur Restart.

Control Center - Network Services

Start Stop **Restart** Refresh

Status

i 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 de CUCM

Afin de sécuriser les messages SIP et RTP sur CUCM, effectuez ces configurations :

- 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 et activer SRTP
- Communication des périphériques des agents sécurisés avec CUCM

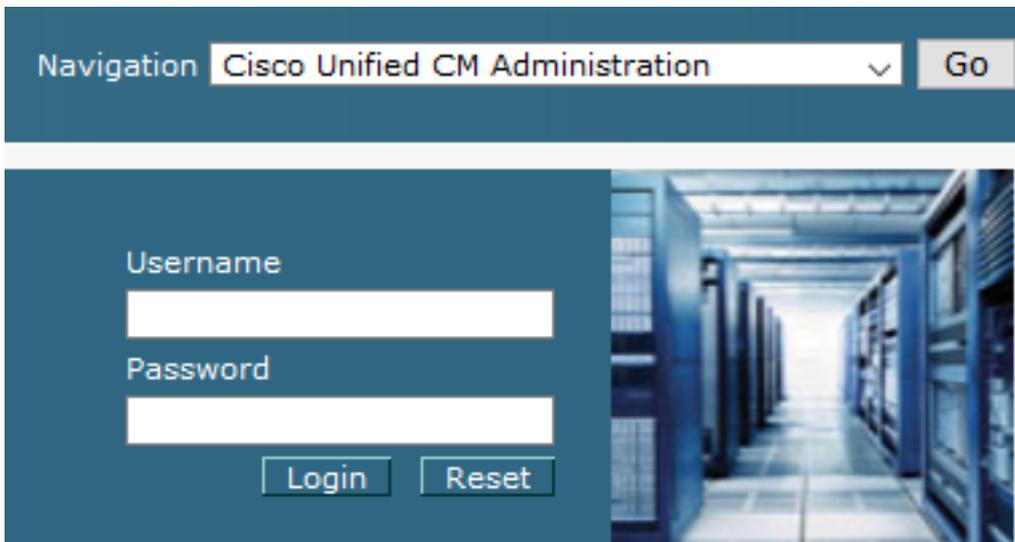
Définir le mode de sécurité CUCM sur Mixed Mode

CUCM prend en charge deux modes de sécurité :

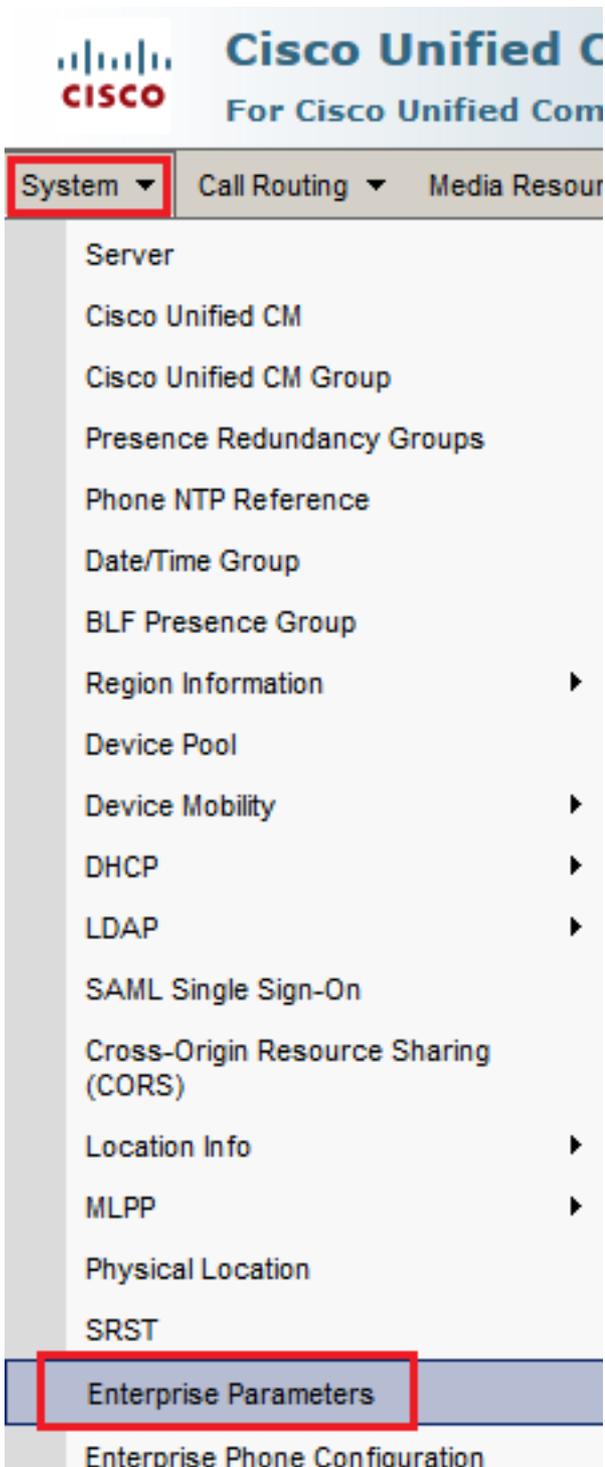
- Mode non sécurisé (mode par défaut)
- Mode mixte (mode sécurisé)

Étapes :

1. Connectez-vous à l'interface d'administration de CUCM.



2. Lorsque vous vous connectez à CUCM, vous pouvez accéder à **System > Enterprise Parameters**.



3. Sous la Security Parameters , vérifiez si la 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. Une fois la connexion à CUCM via SSH réussie, exécutez cette commande :

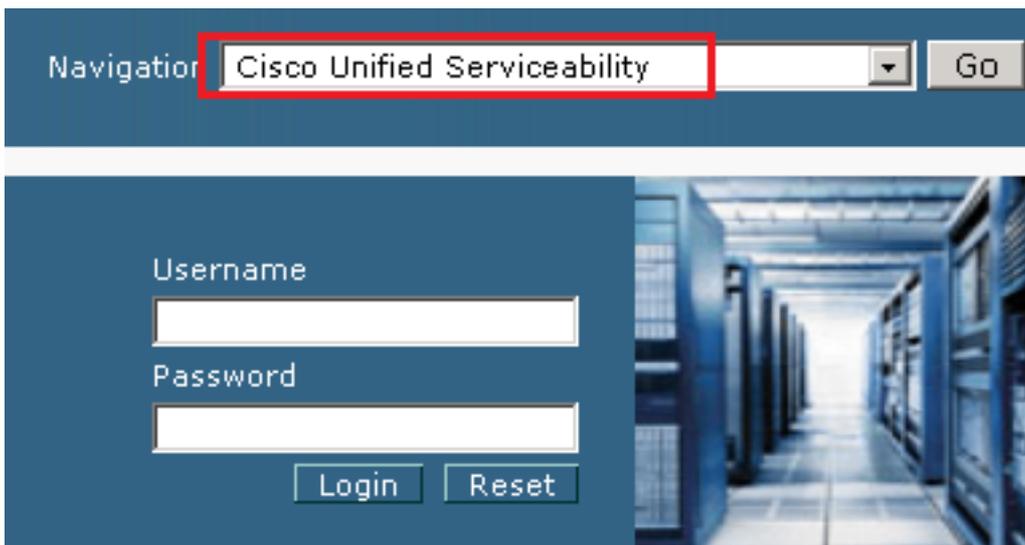
utils ctl set-cluster mixed-mode

7. Type `y` et cliquez sur `Enter` 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 l' Cisco CallManager et la Cisco CTIManager services.

9. Afin de redémarrer les services, naviguez et connectez-vous à Cisco Unified Serviceability.



10. Une fois la connexion établie, 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 Services CM, sélectionnez le 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 le redémarrage réussi de **Cisco CallManager**, sélectionnez la commande **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. Après le redémarrage réussi des services, afin de vérifier 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. et vérifiez ensuite la **Cluster Security Mode**. Maintenant, il doit être défini sur **1**.

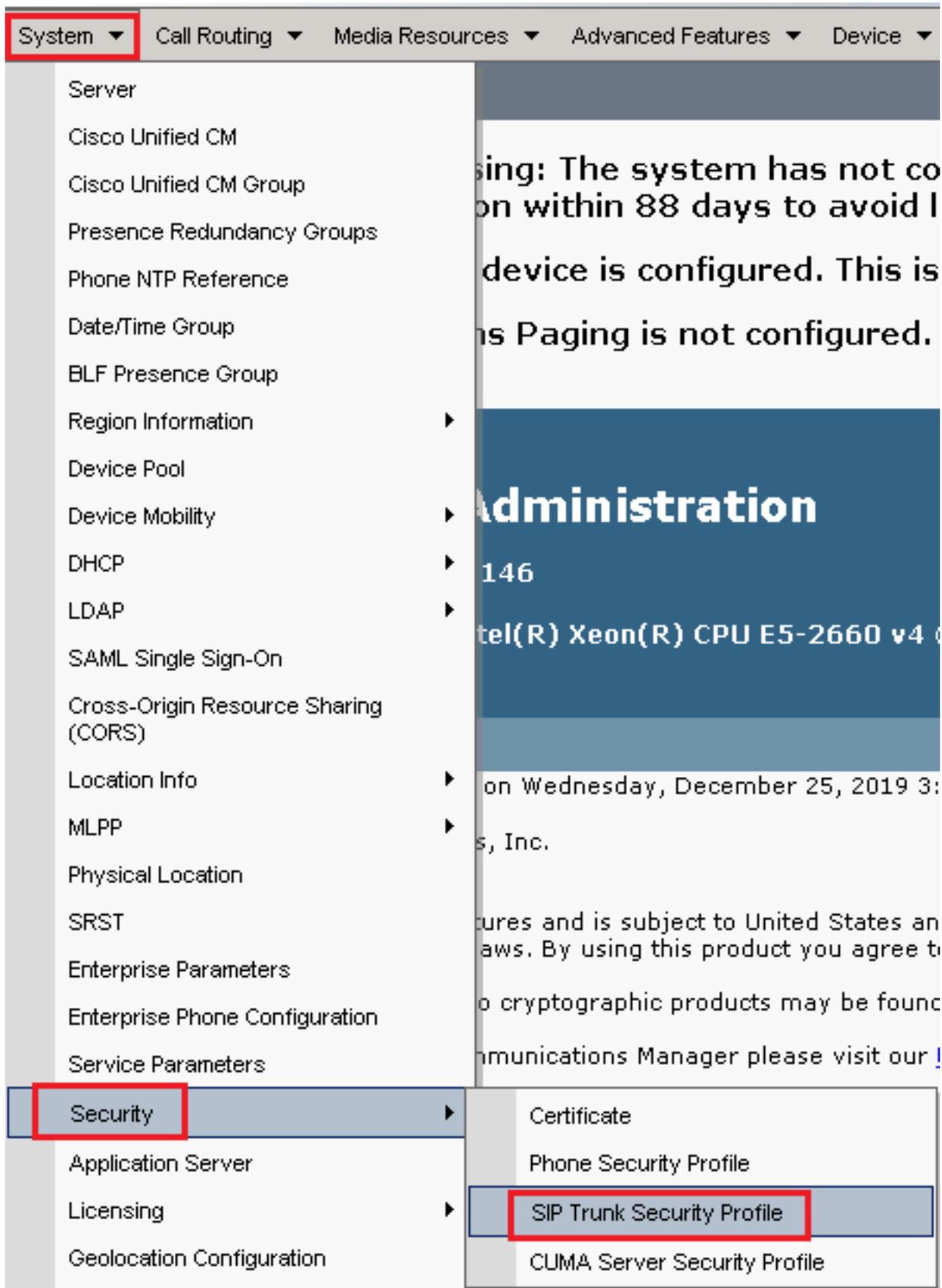
Security Parameters	
Cluster Security Mode *	1
Cluster SIPOAuth Mode *	Disabled

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

Étapes :

1. Connectez-vous à l'interface d'administration de CUCM.

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** pour 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 cette image, puis cliquez sur Save en bas à gauche de la page.

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

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 ▾

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. Changement 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

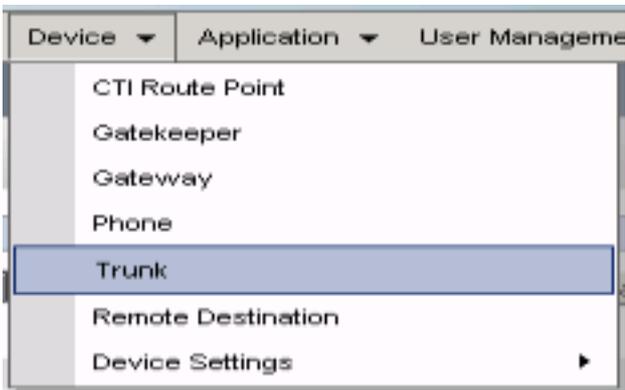
Allow charging header

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

Associer des profils de sécurité de liaison SIP aux liaisons SIP respectives et activer SRTP

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 , puis cliquez sur 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
<input type="checkbox"/>	vCUBE	dCloud_CSS	dCloud_CSS	dCloud_DP	cloudcherry.sip.twilio.com	dCloud_PT
<input type="checkbox"/>	vCUBE	dCloud_CSS	dCloud_CSS	dCloud_DP	7800	PSTN_Incoming_Numbers
<input type="checkbox"/>	vCUBE	dCloud_CSS	dCloud_CSS	dCloud_DP	6016	PSTN_Incoming_Numbers
<input type="checkbox"/>	vCUBE	dCloud_CSS	dCloud_CSS	dCloud_DP	7019	PSTN_Incoming_Numbers
<input type="checkbox"/>	vCUBE	dCloud_CSS	dCloud_CSS	dCloud_DP	44413XX	Robot Agent Remote Destinations

3. Cliquer vCUBE pour ouvrir la page de configuration de l'agrégation vCUBE.

4. Dans Device Information , cochez la case SRTP Allowed afin d'activer SRTP.

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

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

6. Changement SIP Trunk Security Profile par SecureSIPTLSForCube.

SIP Information

Destination

Destination Address is an SRV

1* Destination Address 198.18.133.226 Destination Address IPv6 Destination Port 5061

MTP Preferred Originating Codec* 711ulaw

BLF Presence Group* Standard Presence group

SIP Trunk Security Profile* SecureSIPTLSforCube

Rerouting Calling Search Space < None >

7. Cliquer Save puis Rest par 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

8. Naviguez jusqu'à **Device > Trunk**, recherchez le trunk CVP, dans cet exemple, le nom du trunk CVP est **cvp-SIP-Trunk**. Cliquez **Find**.

Trunks (1 - 1 of 1)

Find Trunks where begins with

<input type="checkbox"/>	Name ^	Description	Calling Search Space	Device Pool
<input type="checkbox"/>	CVP-SIP-Trunk	CVP-SIP-Trunk	dCloud_CSS	dCloud_DP

9. Cliquez **CVP-SIP-Trunk** pour ouvrir la page de configuration de la liaison CVP.
10. Dans **Device Information** section, vérifiez **SRTP Allowed** afin d'activer SRTP.

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*

Route Class Signaling Enabled*

Use Trusted Relay Point*

11. Faites défiler jusqu'à **SIP Information**, modifiez la **Destination Port** par **5061**.

12. Changez **SIP Trunk Security Profile** par **SecureSIPTLSForCvp**.

SIP Information

Destination

Destination Address is an SRV

Destination Address

Destination Address IPv6

Destination Port

1*

MTP Preferred Originating Codec*

BLF Presence Group*

SIP Trunk Security Profile*

13. Cliquez **Save** puis **Rest par 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

Communication sécurisée des périphériques des agents avec CUCM

Afin d'activer les fonctionnalités de sécurité pour un périphérique, vous devez installer un certificat LSC (Locally Significant Certificate) et attribuer le profil de sécurité à ce périphérique. Le LSC possède la clé publique pour le terminal, qui est signée par la clé privée CAPF CUCM. 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

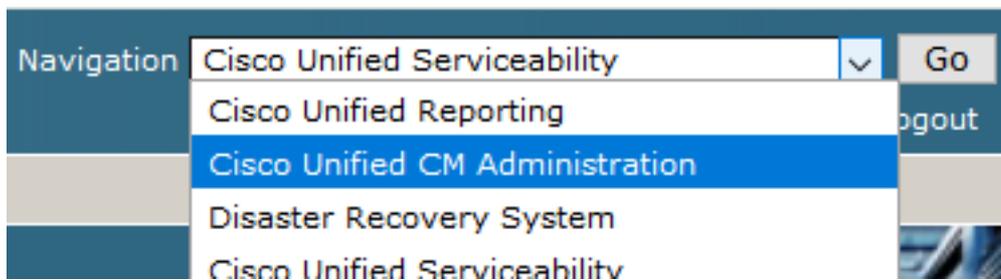
Server*

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 CUCM Administration.



6. Une fois la connexion à l'administration CUCM réussie, accédez à `System > Security > Phone Security Profile` afin de créer un profil de sécurité de périphérique pour le périphérique agent.



Cisco Unified CM Administration

For Cisco Unified Communications Solutions

System ▾

Call Routing ▾

Media Resources ▾

Advanced Features ▾

Devi

Server

Cisco Unified CM

Cisco Unified CM Group

Presence Redundancy Groups

Phone NTP Reference

Date/Time Group

BLF Presence Group

Region Information ▶

Device Pool

Device Mobility ▶

DHCP ▶

LDAP ▶

SAML Single Sign-On

Cross-Origin Resource Sharing (CORS)

Location Info ▶

MLPP ▶

Physical Location

SRST

Enterprise Parameters

Enterprise Phone Configuration

Service Parameters

Security ▶

Application Server

Licensing ▶

Geolocation Configuration

device is configured. The
as Paging is not configur

Administration

7

tel(R) Xeon(R) CPU E5-2660

on Friday, December 20, 2019 10
s, Inc.

ures and is subject to United Stat
aws. By using this product you ac

o cryptographic products may be

munications Manager please visit

our [Technical Support](#) web site.

Certificate

Phone Security Profile

SIP Trunk Security Profile

CUMA Server Security Profile

7. Recherchez le profil 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 sur l'icône Copier  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. Cmodifiez les paramètres comme 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*
 Description
 Device Security Mode
 Transport Type*
 TFTP Encrypted Config
 Enable OAuth Authentication

Phone Security Profile CAPF Information

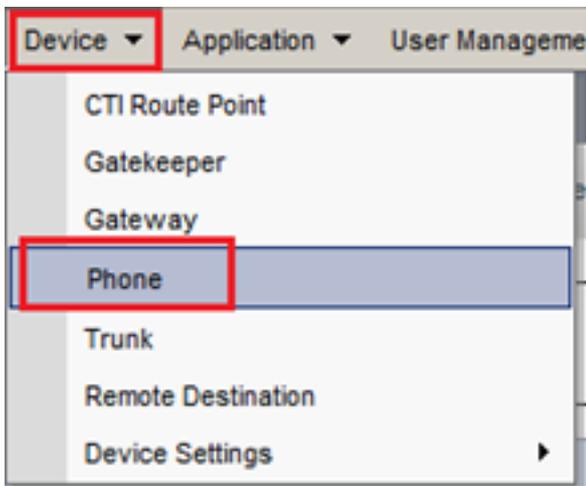
Authentication Mode*
 Key Order*
 RSA Key Size (Bits)*
 EC Key Size (Bits)
 Note: These fields are related to the CAPF Information settings on the Phone Configuration page.

Parameters used in Phone

SIP Phone Port*

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 et de modifier la 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, puis cliquez sur Reset.

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ A

Phone Configuration

 Save
  Delete
  Copy
  Reset
  Apply Config
  Add New

Status

 Update successful

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

Device Reset

 Reset
  Restart

Status

 Status: Ready

Reset Information

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**.

Certification Authority Proxy Function (CAPF) Information

Certificate Operation* No Pending Operation ▾
Authentication Mode* By Null String ▾
Authentication String
Generate String
Key Order* RSA Only ▾
RSA Key Size (Bits)* 2048 ▾
EC Key Size (Bits) ▾
Operation Completes By 2021 04 16 12 (YYYY:MM:DD:HH)
Certificate Operation Status: Upgrade Success
 Note: Security Profile Contains Addition CAPF Settings.

16. Reportez-vous aux mêmes étapes de l'étape. 7 - 13 pour sécuriser les périphériques d'autres agents que vous souhaitez utiliser avec les protocoles SIP et RTP sécurisés avec

CUCM.

Vérifier

Afin de valider que RTP est correctement sécurisé, effectuez ces étapes :

1. Effectuez un appel test au centre de contact et écoutez l'invite IVR.
2. Dans le même temps, ouvrez la session SSH sur vCUBE et exécutez cette commande :
show call active voice brief

```
Total call-legs: 2
1E85 : 100642 465092660ms.1 (02:55:19.809 UTC Thu Mar 25 2021) +1090 pid:6000100 Answer 3227046971 active
dur 00:00:26 tx:0/0 rx:0/0 dscp:0 media:0 audio tos:0xB8 video tos:0x0
IP 198.18.133.76:5062 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off Transcoded: No ICE
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a
LostPacketRate:0.00 OutOfOrderRate:0.00
LocalUUID:4865626844c25f248e19a95a65b0ad50
RemoteUUID:674ECD1639ED7A710000ABF910000178
VRF:
1E85 : 100643 465093670ms.1 (02:55:20.819 UTC Thu Mar 25 2021) +70 pid:6000 Originate 6016 active
dur 00:00:26 tx:0/0 rx:0/0 dscp:0 media:0 audio tos:0xB8 video tos:0x0
IP 198.18.133.143:25346 SRTP: on rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off Transcoded: No ICE
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a
LostPacketRate:0.00 OutOfOrderRate:0.00
LocalUUID:674ECD1639ED7A710000ABF910000178
RemoteUUID:4865626844c25f248e19a95a65b0ad50
VRF:
```

Conseil : vérifiez si le protocole SRTP est on entre CUBE et VVB (198.18.133.143). Si oui, cela confirme que le trafic RTP entre CUBE et VVB est sécurisé.

3. Rendre un agent disponible pour répondre à l'appel.

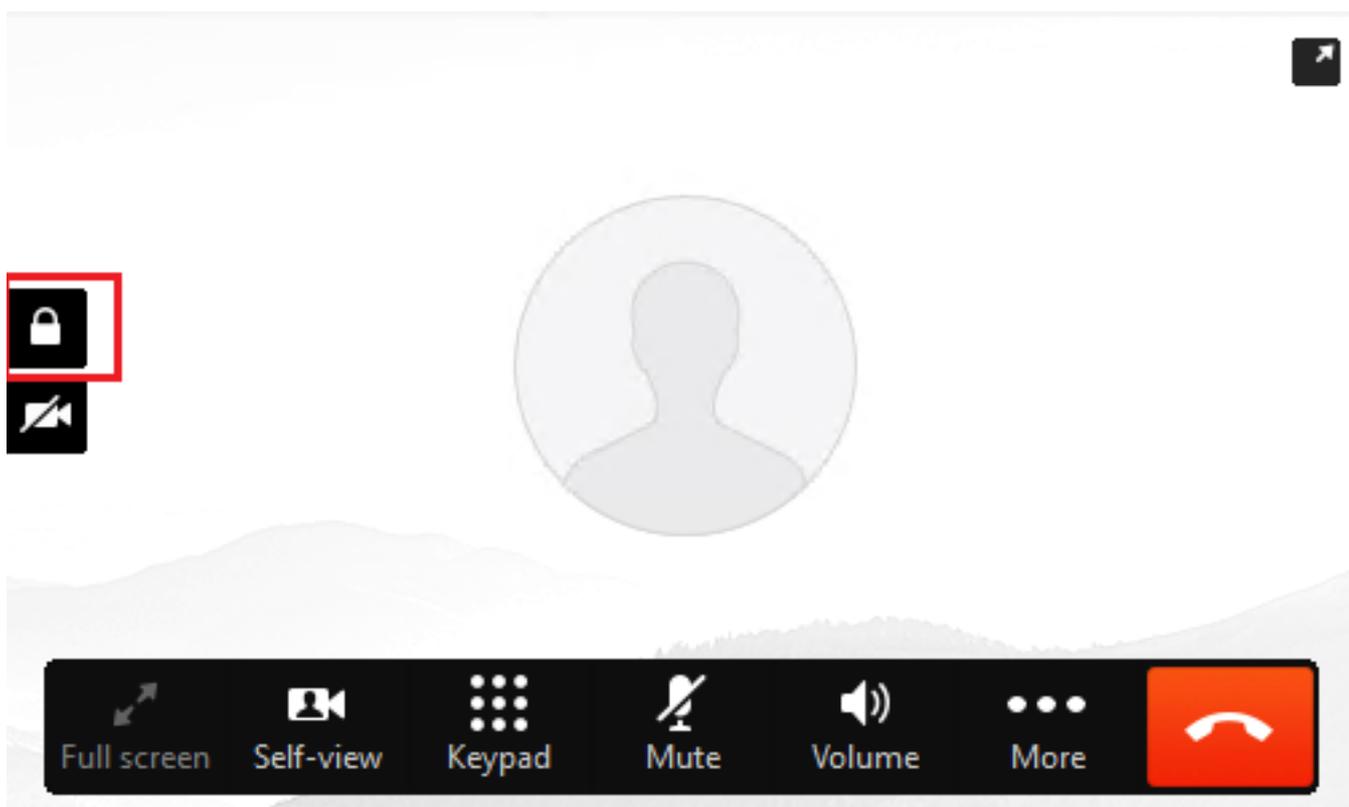


4. L'agent est réservé et l'appel est acheminé vers l'agent. Répondez à l'appel.
5. L'appel est connecté à l'agent. Retournez à la session SSH vCUBE et exécutez cette commande :
show call active voice brief

```
Total call-legs: 2
1E85 : 100642 465092660ms.1 (02:55:19.809 UTC Thu Mar 25 2021) +1090 pid:6000100 Answer 3227046971 connected
dur 00:04:01 tx:0/0 rx:0/0 dscp:0 media:0 audio tos:0xB8 video tos:0x0
IP 198.18.133.76:5062 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off Transcoded: No ICE: Off
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a
LostPacketRate:0.00 OutOfOrderRate:0.00
LocalUUID:4865626844c25f248e19a95a65b0ad50
RemoteUUID:00003e7000105000a000005056a06cb8
VRF:
1E85 : 100643 465093670ms.1 (02:55:20.819 UTC Thu Mar 25 2021) +70 pid:6000 Originate 6016 connected
dur 00:04:01 tx:0/0 rx:0/0 dscp:0 media:0 audio tos:0xB8 video tos:0x0
IP 198.18.133.75:24648 SRTP: on rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off Transcoded: No ICE: Off
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a
LostPacketRate:0.00 OutOfOrderRate:0.00
LocalUUID:00003e7000105000a000005056a06cb8
RemoteUUID:4865626844c25f248e19a95a65b0ad50
VRF:
```

Conseil : vérifiez si le protocole SRTP est on entre CUBE et les téléphones des agents (198.18.133.75). Si oui, cela confirme que le trafic RTP entre CUBE et l'agent est sécurisé.

6. En outre, une fois l'appel connecté, un verrou de sécurité s'affiche sur le périphérique de l'agent. Cela confirme également que le trafic RTP est sécurisé.



Pour vérifier que les signaux SIP sont correctement sécurisés, référez-vous à l'article [Configurer la signalisation SIP sécurisée](#).

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.