Configurer le protocole RTP sécurisé 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 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

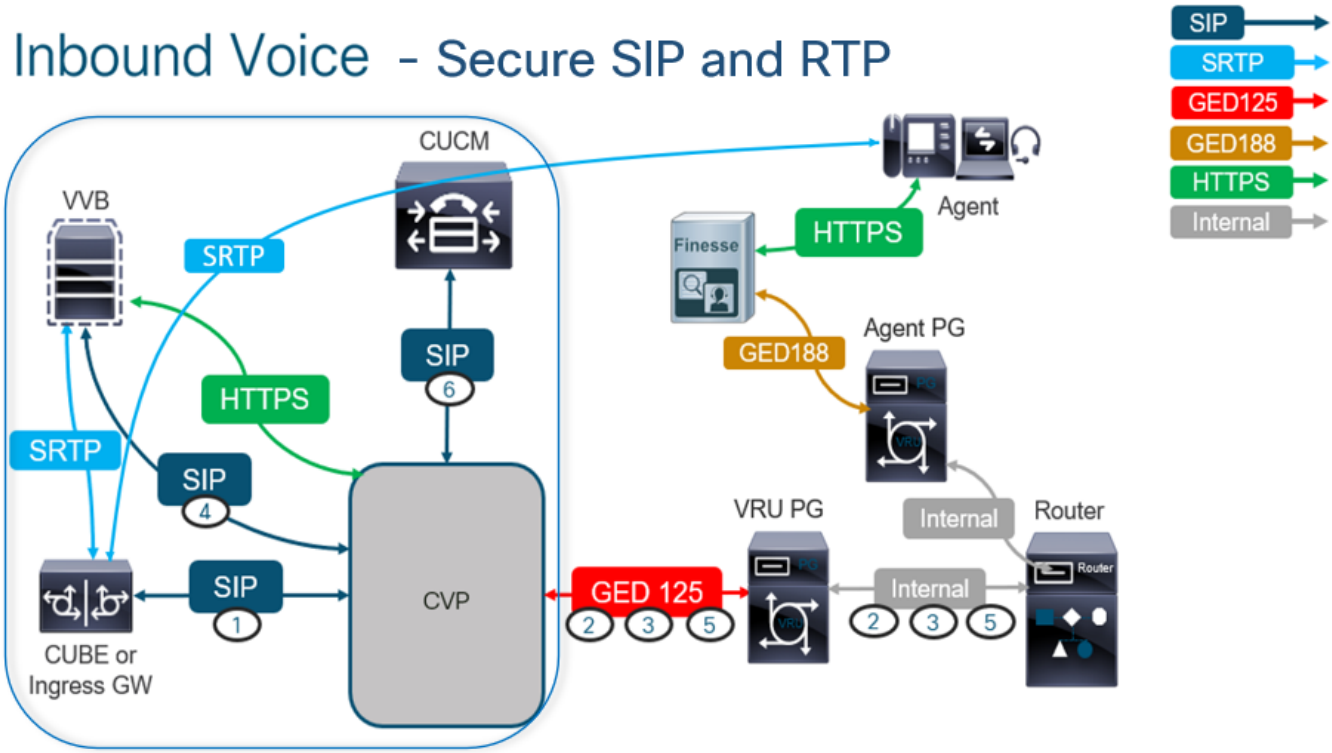
Les informations contenues dans ce document sont basées sur Package Contact Center Enterprise (PCCE), CVP, CVVB et CUCM version 12.6, mais elles s'appliquent également aux versions précédentes.

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 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

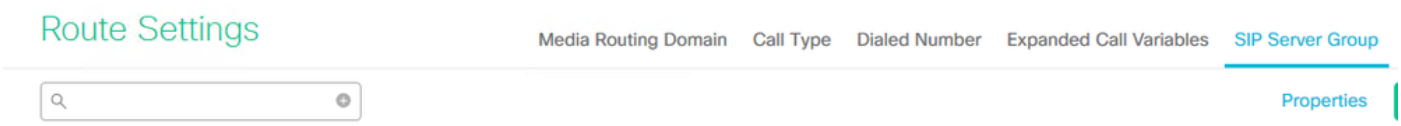
```
CC-VCUBE#
CC-VCUBE#Conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CC-VCUBE(config)#dial-peer voice 6000 voip
CC-VCUBE(config-dial-peer)#session target ipv4:198.18.133.13:5061
CC-VCUBE(config-dial-peer)#session transport tcp tls
CC-VCUBE(config-dial-peer)#SRTP
CC-VCUBE(config-dial-peer)#exit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

Tâche 2: Configuration sécurisée CVP

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

Étapes:

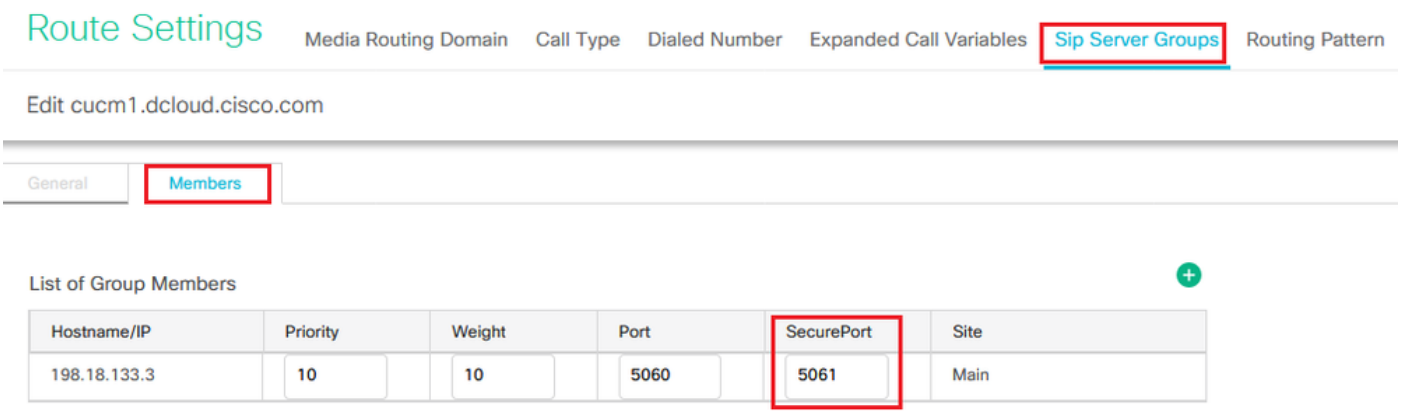
1. Connectez-vous auUCCE Web Administration.
2. Accédez àCall Settings > Route Settings > SIP Server Group.



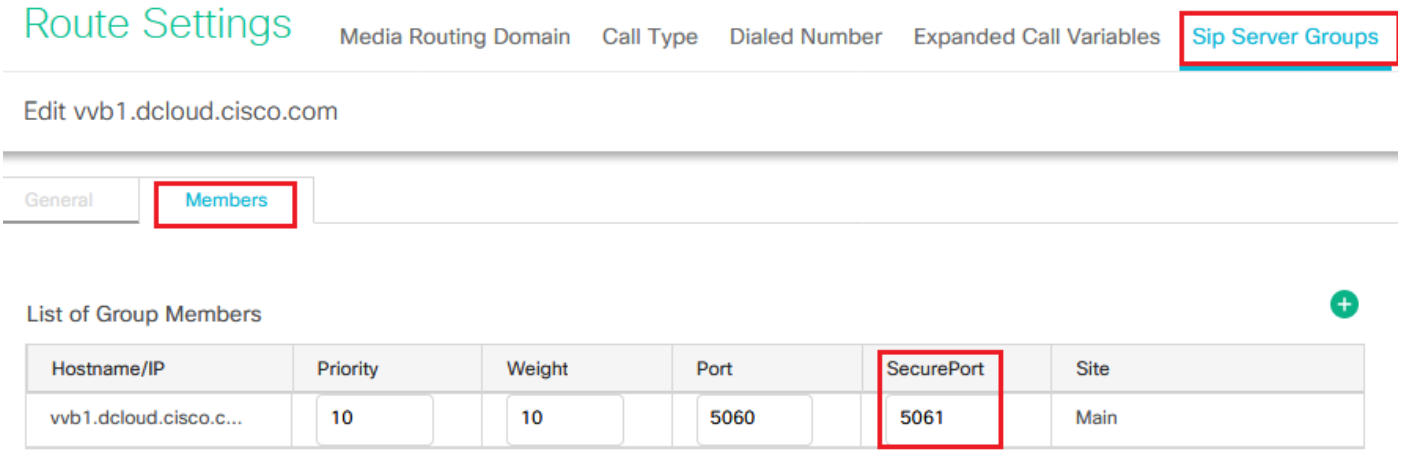
Selon vos configurations, vous avez configuré des groupes de serveurs SIP pour CUCM, CVVB et CUBE. Vous devez définir les ports SIP sécurisés sur 5061 pour chacun d'entre eux. Dans cet exemple, les groupes de serveurs SIP suivants sont utilisés :

- cucm1.dcloud.cisco.com pour CUCM
- vvb1.dcloud.cisco.com pour CVVB
- cube1.dcloud.cisco.com pour CUBE

3. Cliquez surcucm1.dcloud.cisco.com, puis dans l'Membersonglet qui affiche les détails des configurations de groupe de serveurs SIP. DéfinissezSecurePortsur5061et cliquez surSave.



4. Cliquez survvb1.dcloud.cisco.com, puis dans l'Membersonglet, définissez laSecurePortsur5061et cliquez surSave.

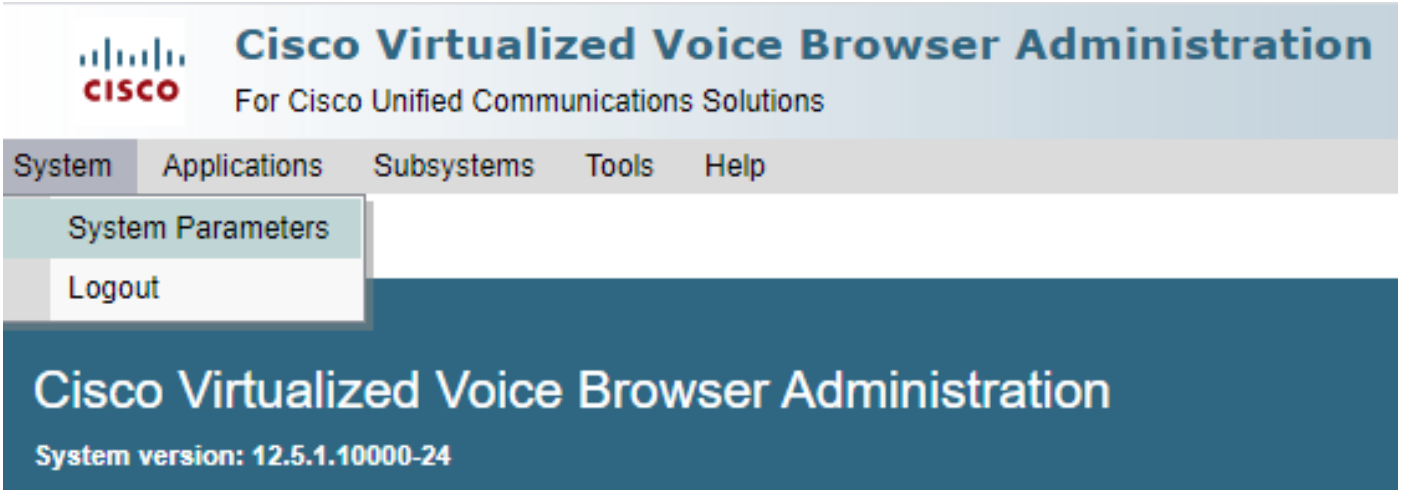


Tâche 3: Configuration sécurisée CVVB

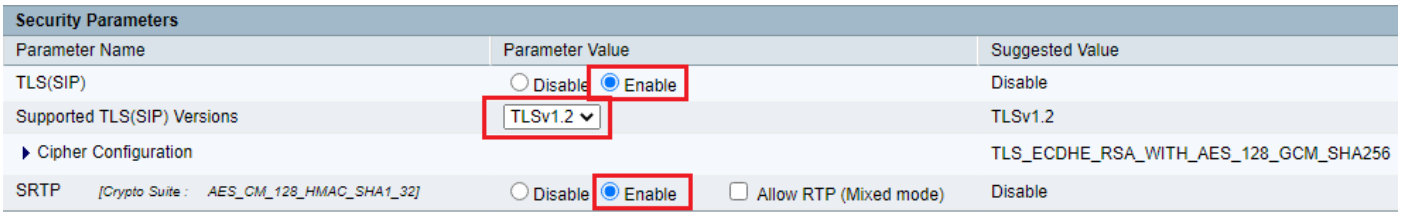
Dans cette tâche, configurez CVVB pour sécuriser les messages de protocole SIP (SIP TLS) et SRTP.

Étapes:

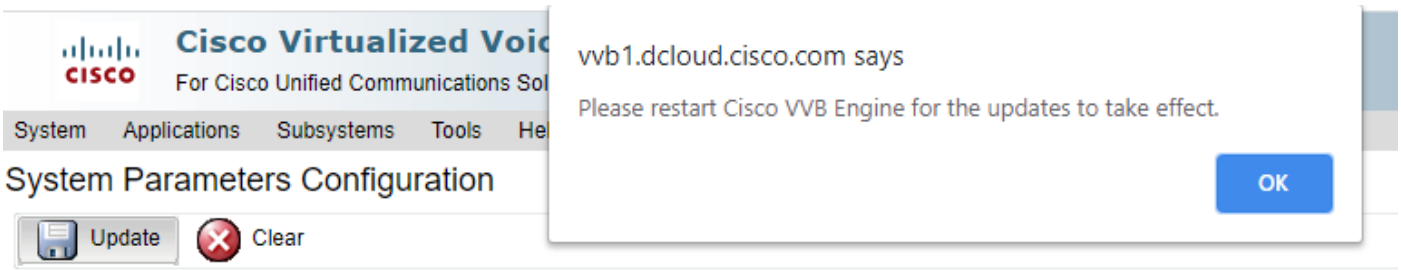
1. Ouvrez laCisco VVB Adminpage.
2. Accédez àSystem > System Parameters.



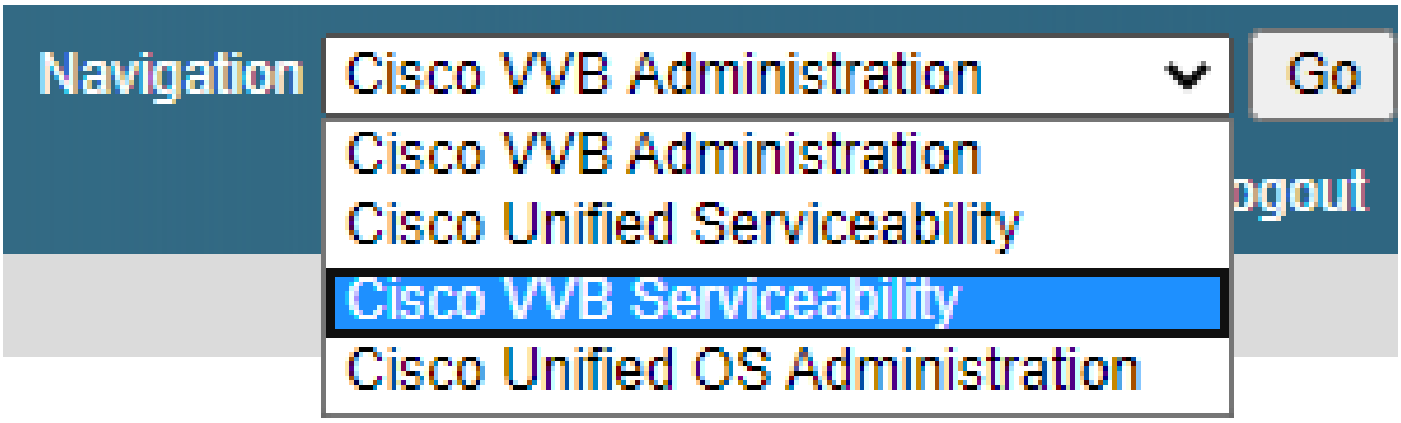
3. Dans la sectionSecurity Parameters, sélectionnezEnablepourTLS (SIP) . Conservez leSupported TLS(SIP) version as TLSv1.2et choisissezEnablepourSRTP.



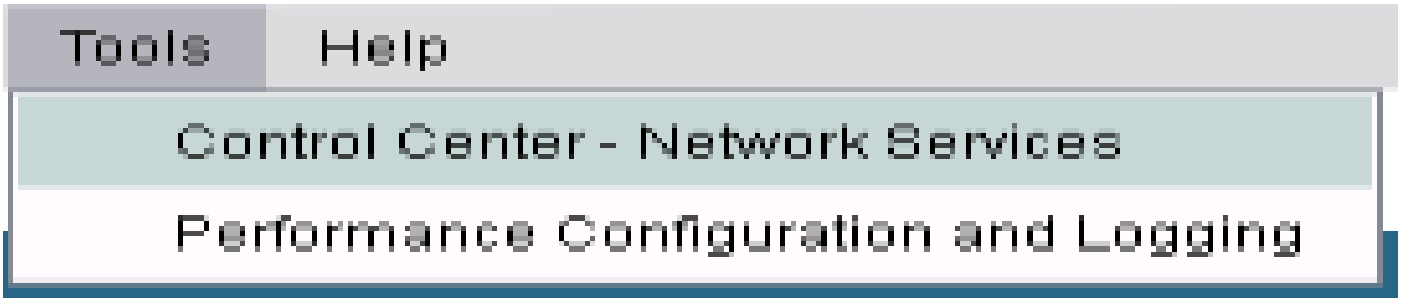
4. Cliquez surUpdate. Cliquez surOklorsque vous êtes invité à redémarrer le moteur CVVB.



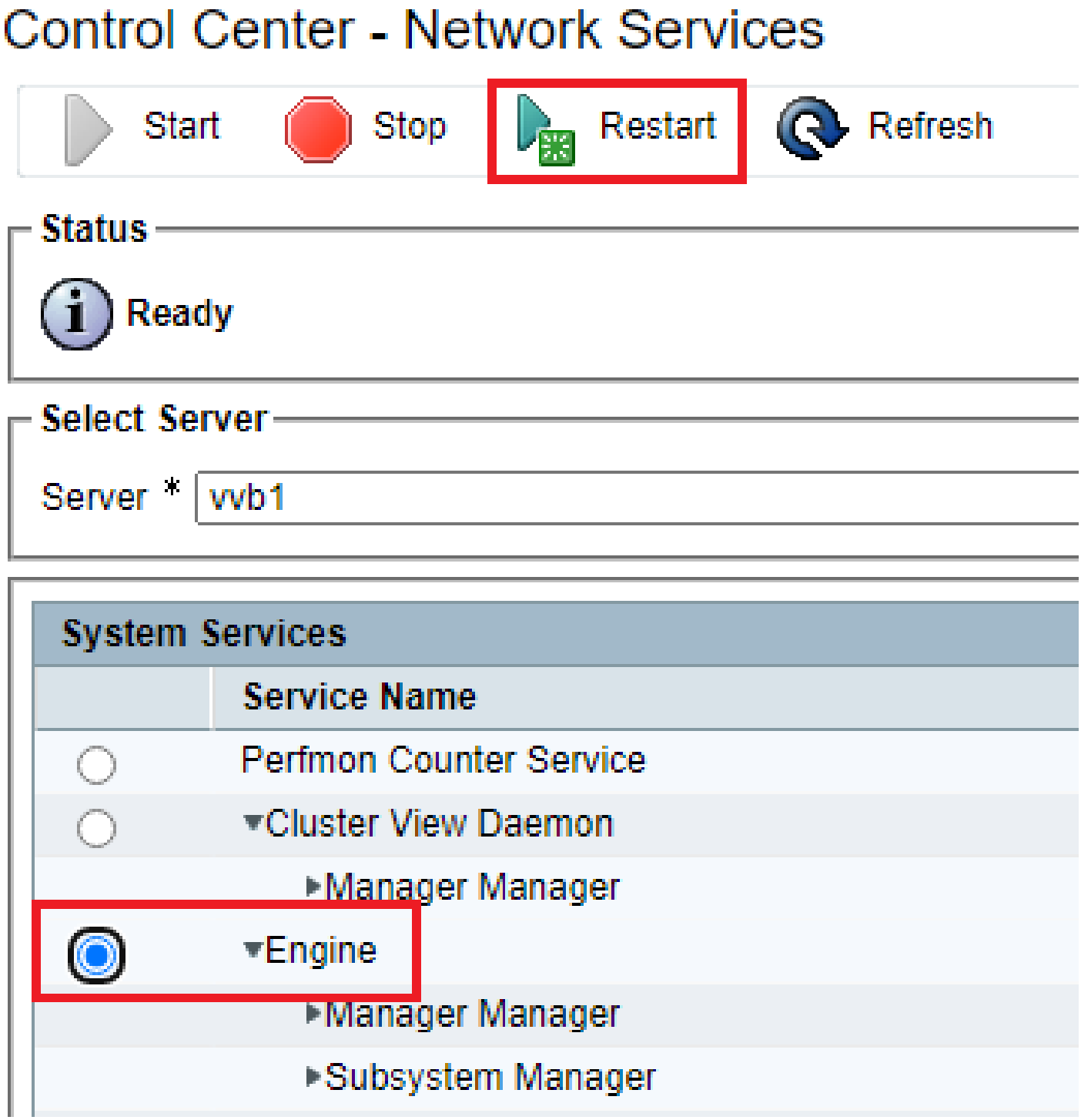
5. Ces modifications nécessitent un redémarrage du moteur Cisco VVB. Pour redémarrer le moteur VVB, accédez à l',Cisco VVB Serviceabilitypuis cliquez surGo.



6. Accédez àTools > Control Center – Network Services.



7. ChoisissezEngineet cliquez surRestart.



Tâche 4: Configuration sécurisée 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

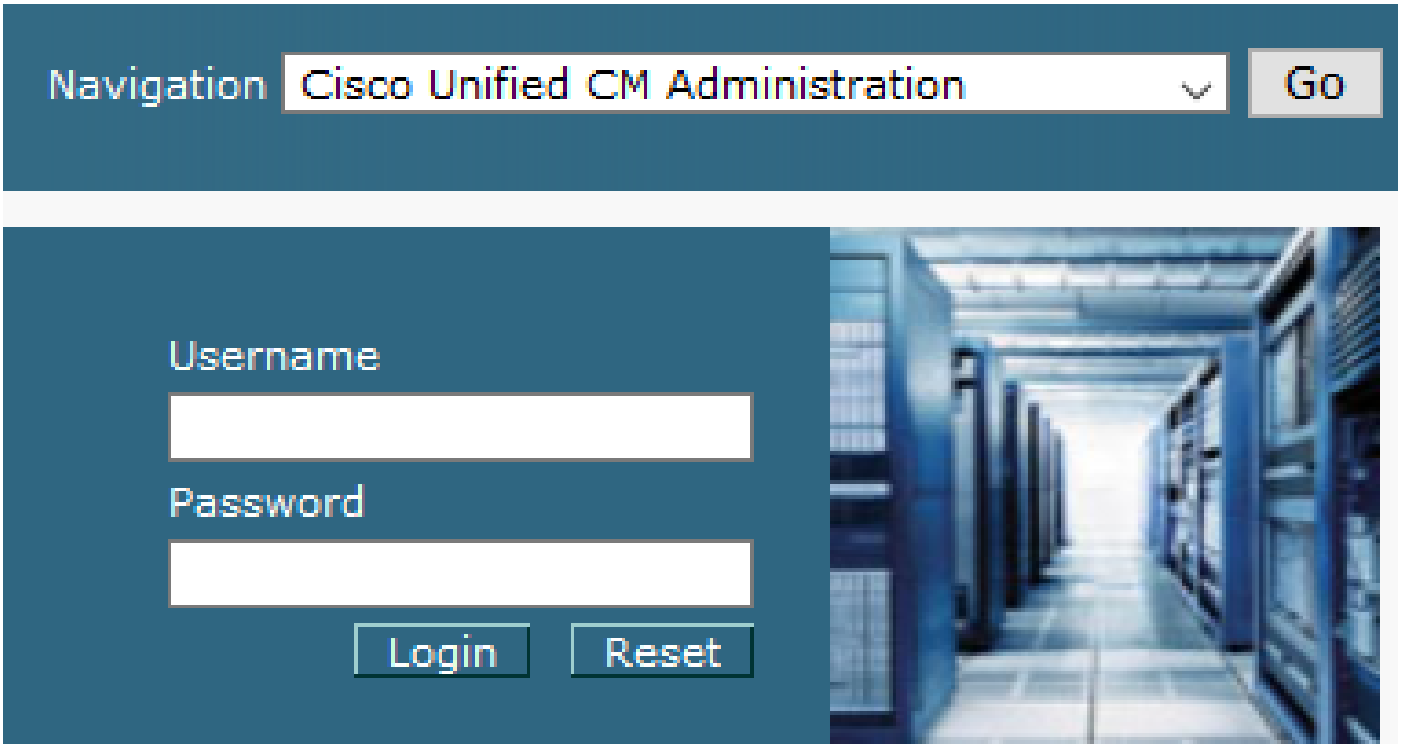
Définir le mode de sécurité CUCM sur Mixed Mode

CUCM prend en charge deux modes de sécurité :

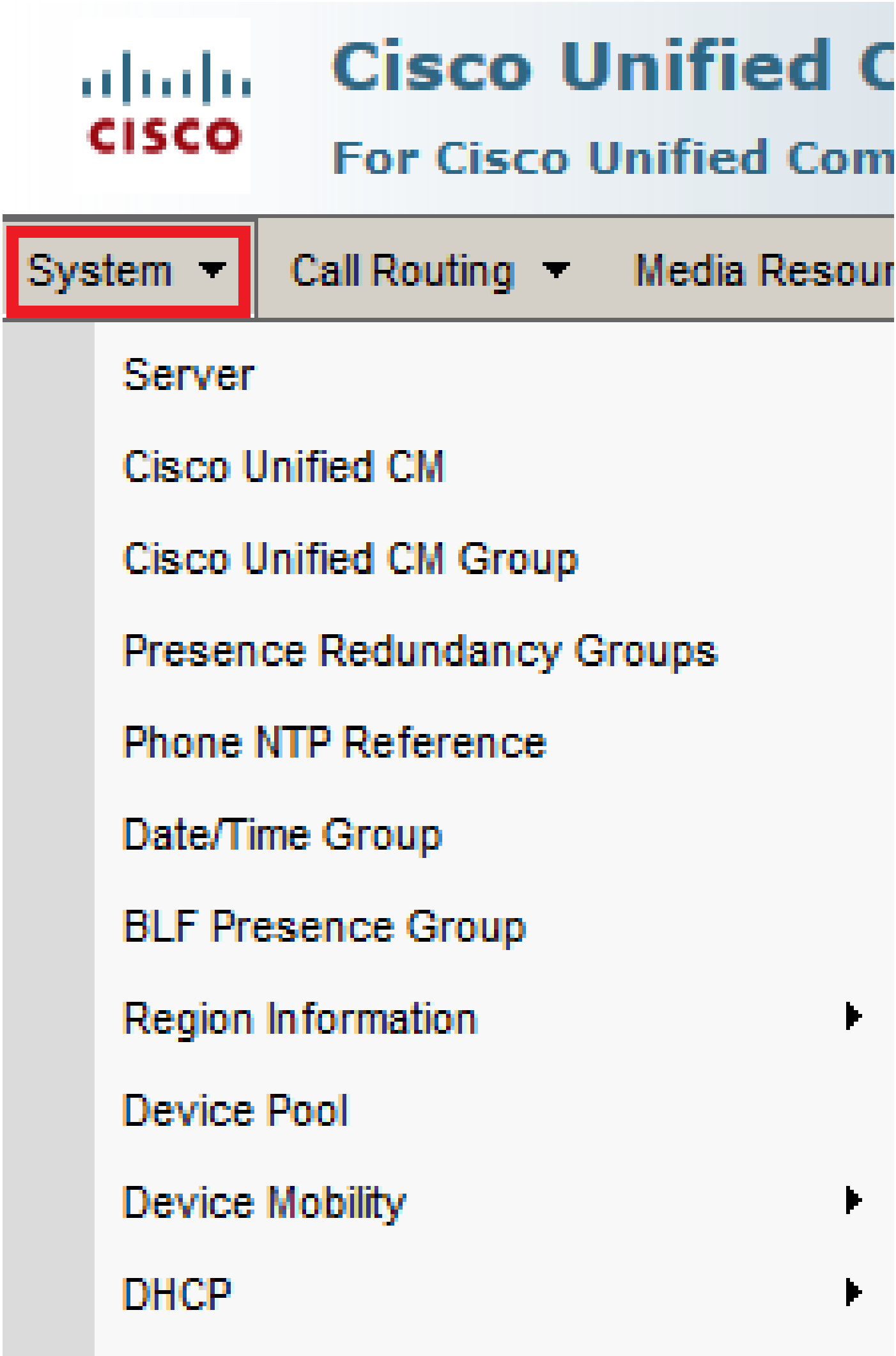
- Mode non sécurisé (mode par défaut)
- Mode mixte (mode sécurisé)

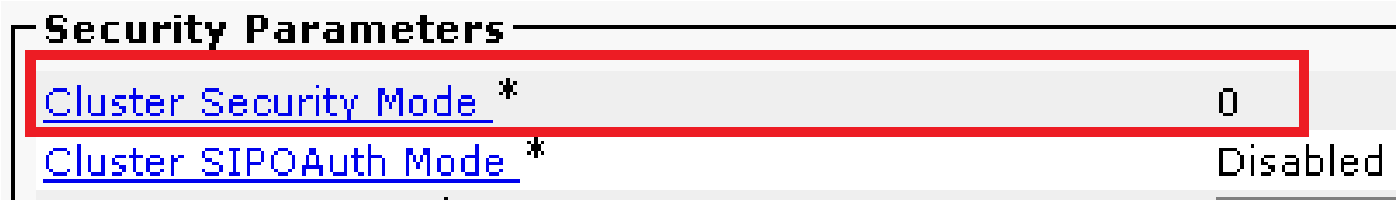
Étapes:

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



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

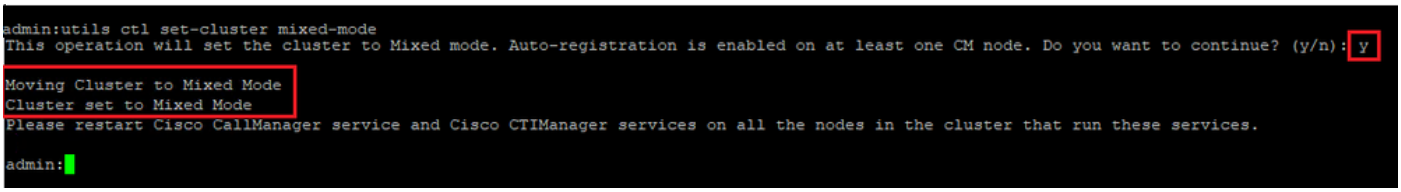

Cisco Unified C
For Cisco Unified Com
System
Call Routing
Media Resour
Server
Cisco Unified CM
Cisco Unified CM Group
Presence Redundancy Groups
Phone NTP Reference
Date/Time Group
BLF Presence Group
Region Information
Device Pool
Device Mobility
DHCP



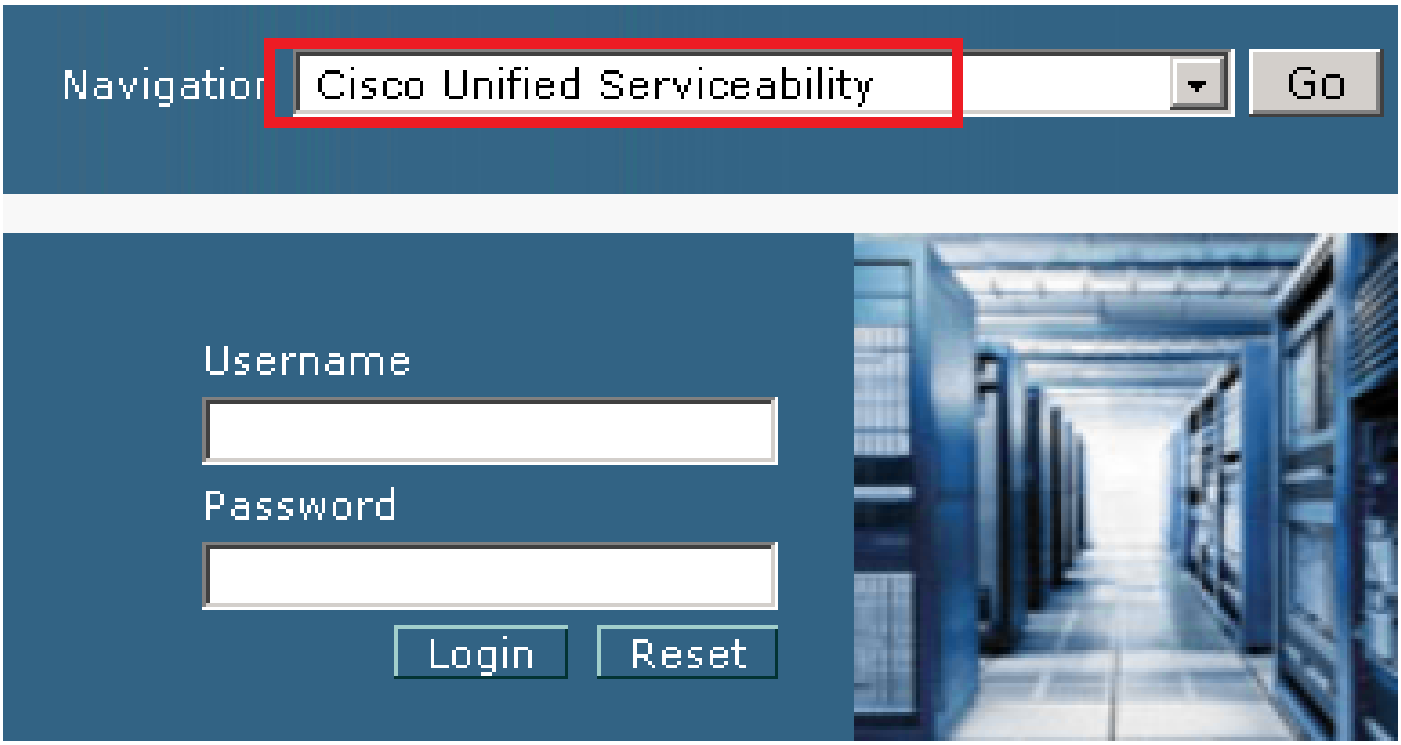
4. Si le mode de sécurité du cluster est défini sur 0, cela signifie que le mode de sécurité du cluster est défini sur non sécurisé. Vous devez activer le mode mixte à partir de l'interface de ligne de commande.
5. Ouvrez une session SSH sur le CUCM.
6. Une fois la connexion à CUCM via SSH réussie, exécutez cette commande :

utils ctl set-cluster mixed-mode

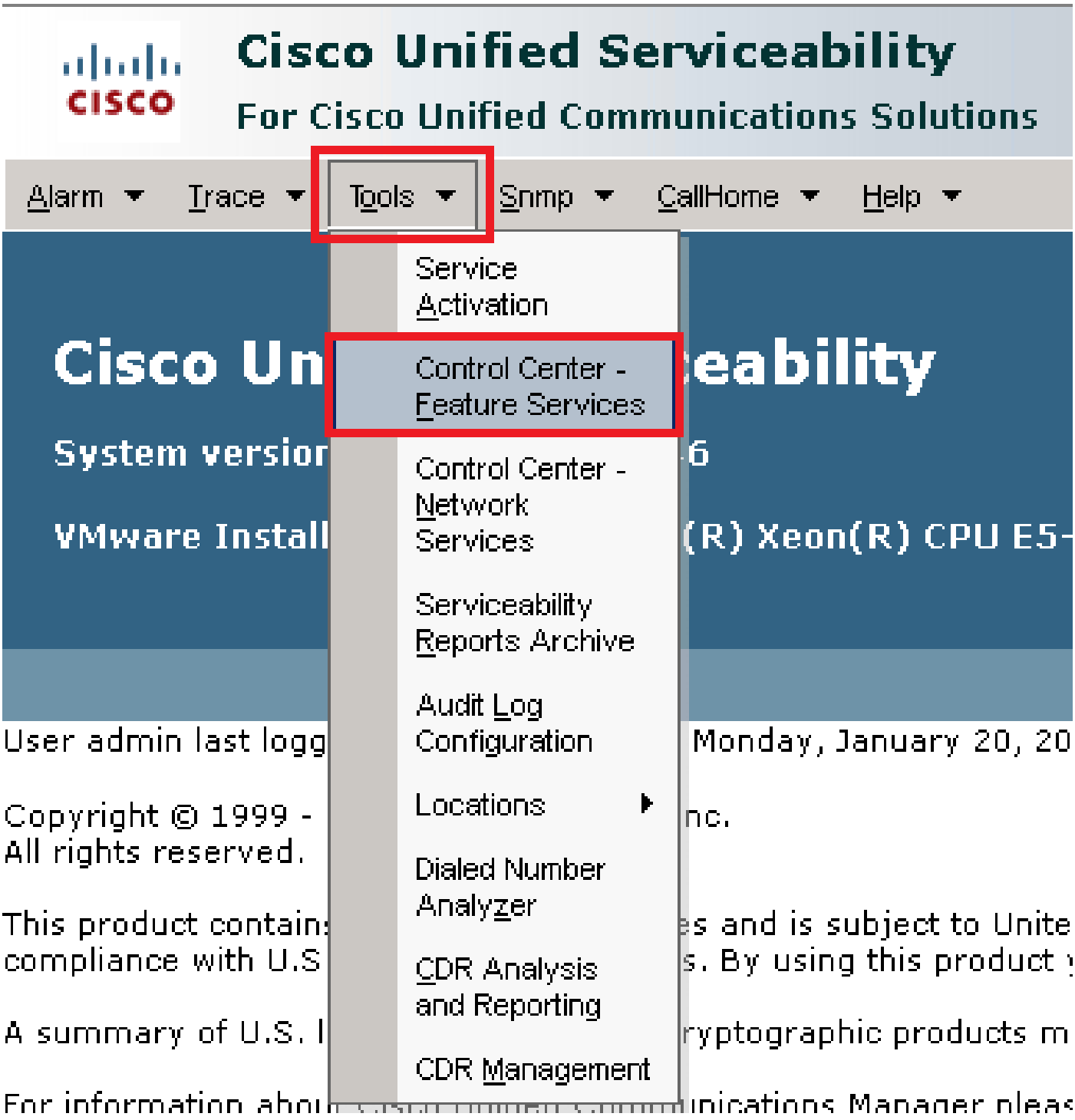
7. Tapezyet cliquez surEnterlorsque vous y êtes invité. Cette commande définit le mode de sécurité du cluster sur le mode mixte.



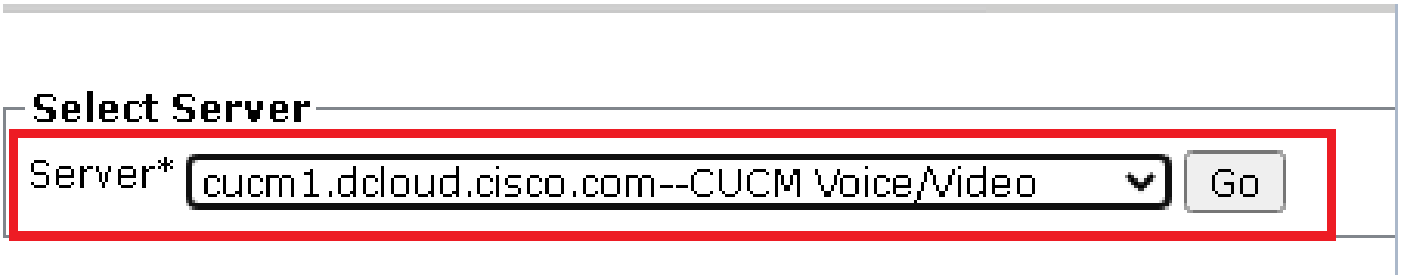
8. Pour que les modifications prennent effet, redémarrez leCisco CallManageret lesCisco CTIManagerservices.
9. Afin de redémarrer les services, naviguez et connectez-vous àCisco Unified Serviceability.



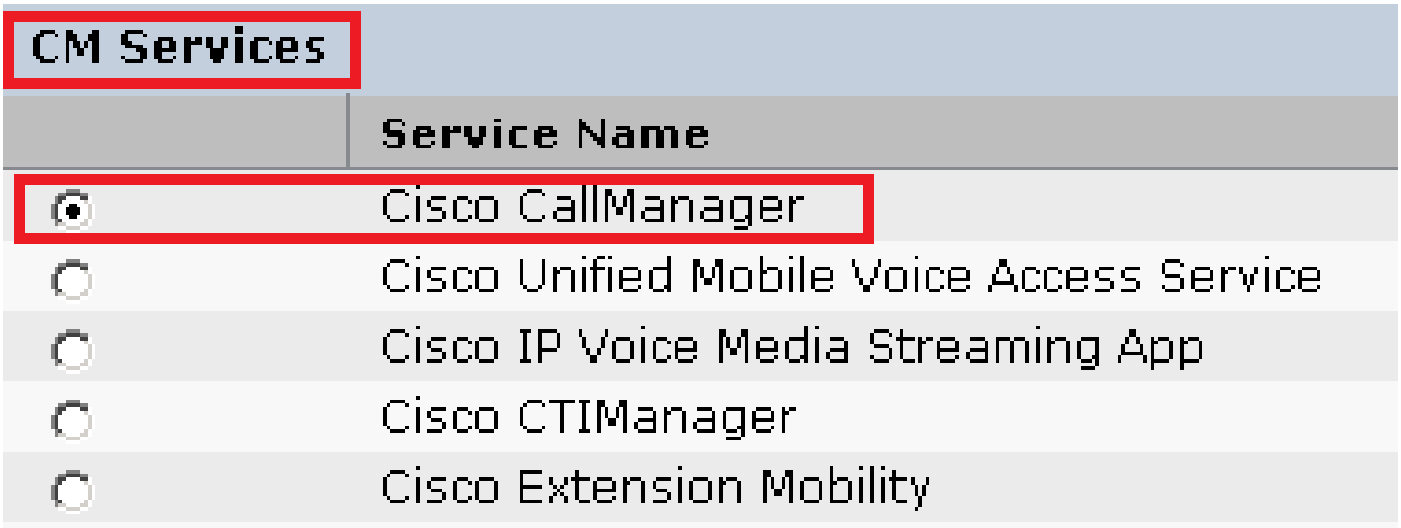
10. Une fois la connexion établie, accédez àTools > Control Center – Feature Services.



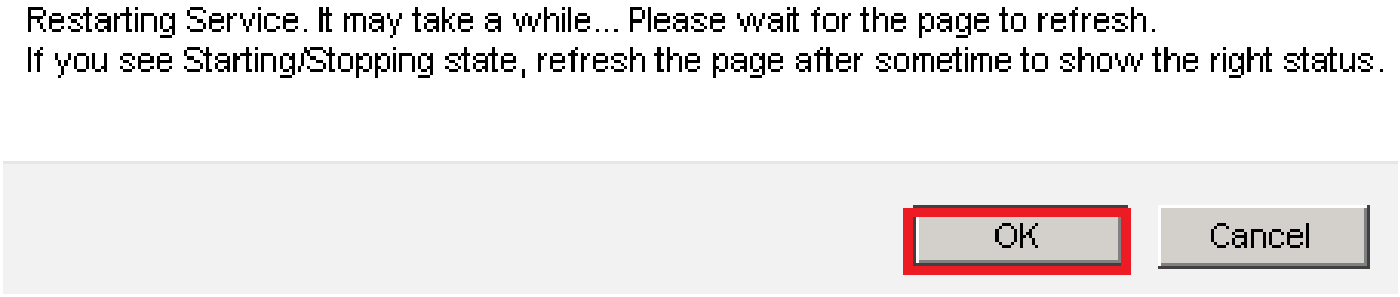
11. Sélectionnez le serveur, puis cliquez surGo.



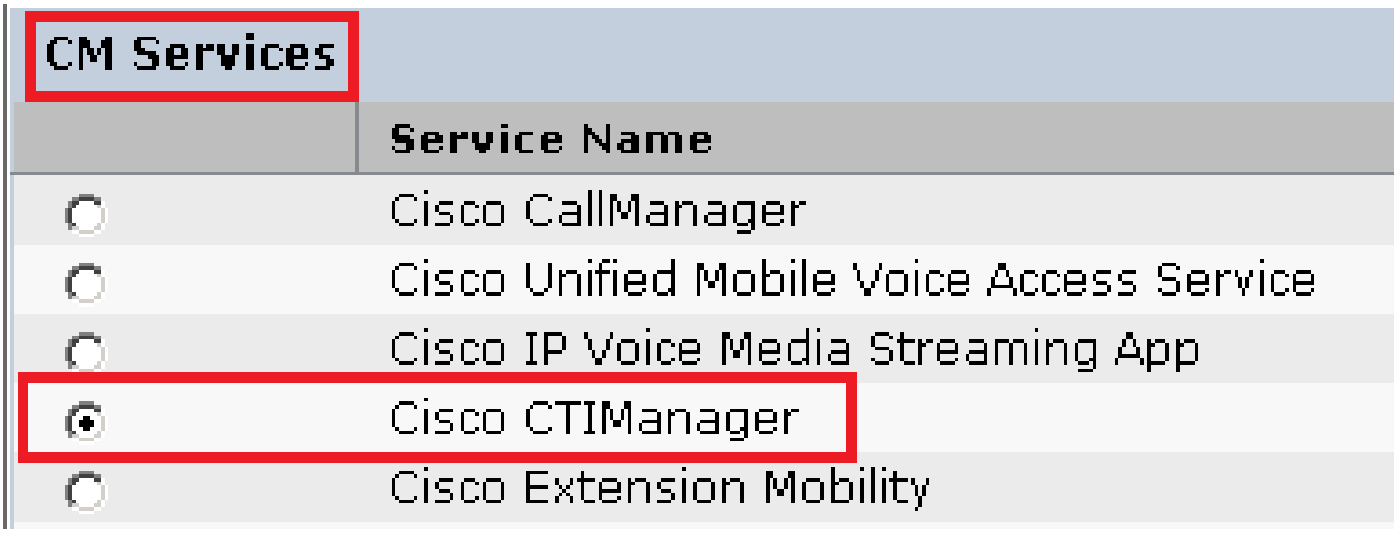
12. Sous Services CM, choisissez laCisco CallManager, puis cliquez surRestartle bouton en haut de la page.



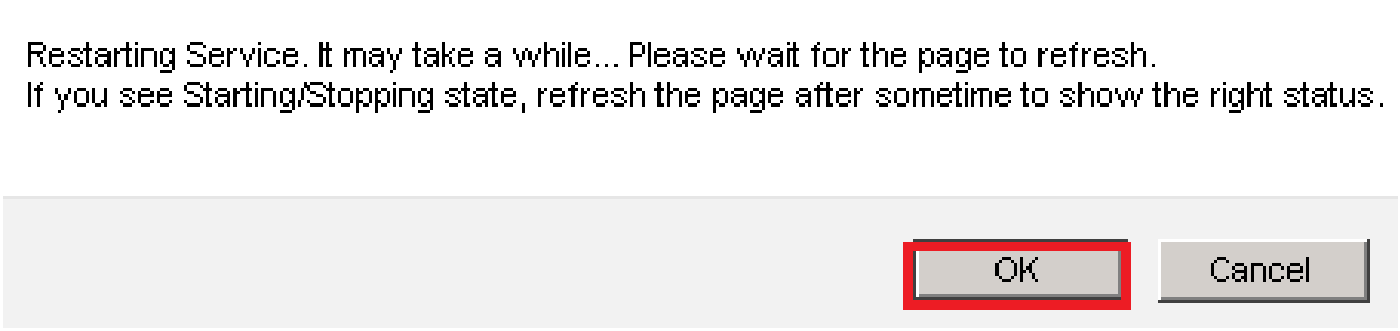
13. Confirmez le message contextuel et cliquez surOK. Attendez que le service redémarre correctement.



14. Après le redémarrage réussi deCisco CallManager, choisissez leCisco CTIManager, puis cliquez surRestartle bouton pour redémarrer Cisco CTIManager service.



15. Confirmez le message contextuel et cliquez surOK. Attendez que le service redémarre correctement.



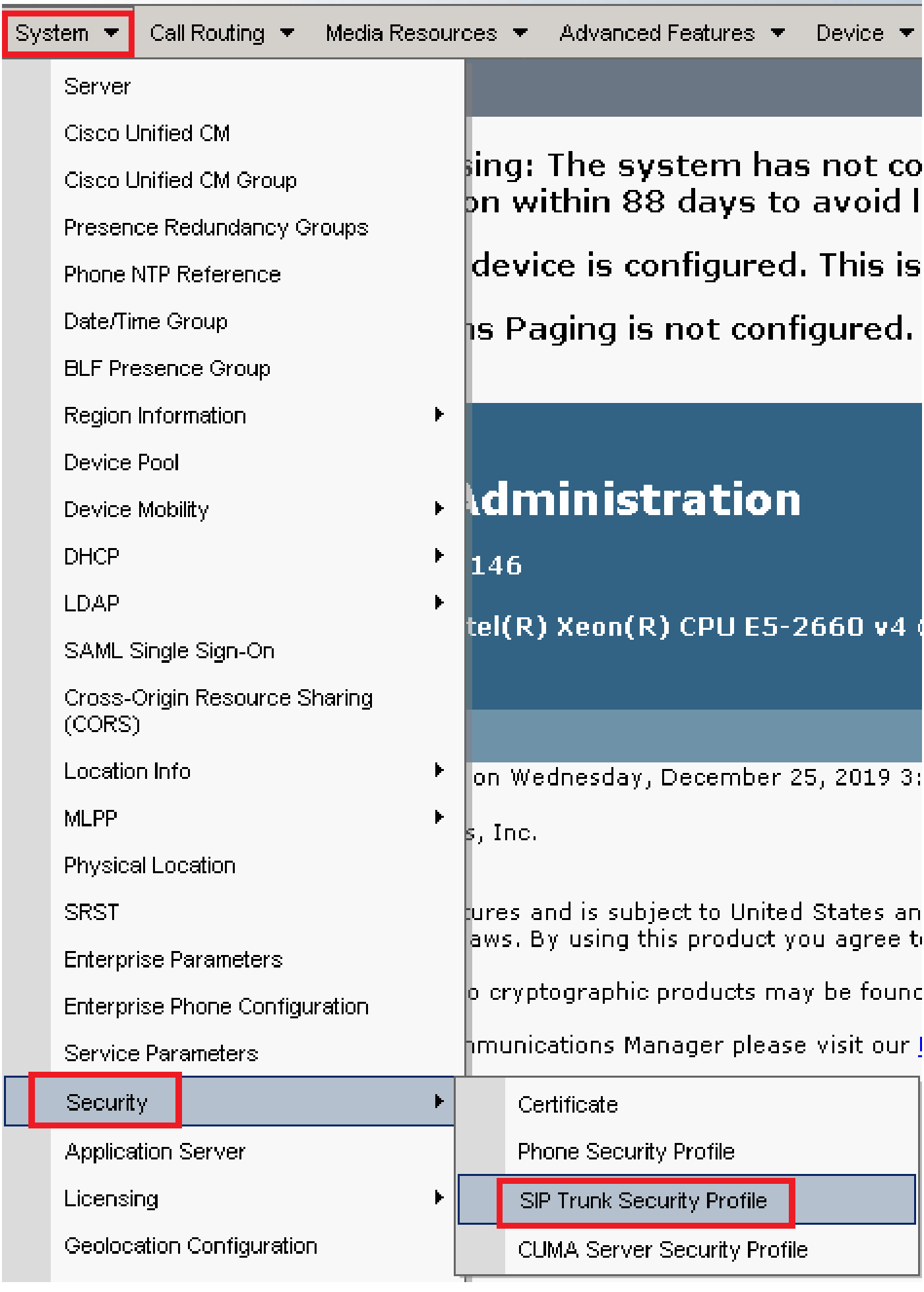
16. Après le redémarrage réussi des services, afin de vérifier que le mode de sécurité du cluster est défini sur le mode mixte, naviguez jusqu'à l'administration de CUCM comme expliqué à l'étape 5. puis vérifiez laCluster Security Mode. Maintenant, il doit être défini sur1.



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

Étapes:

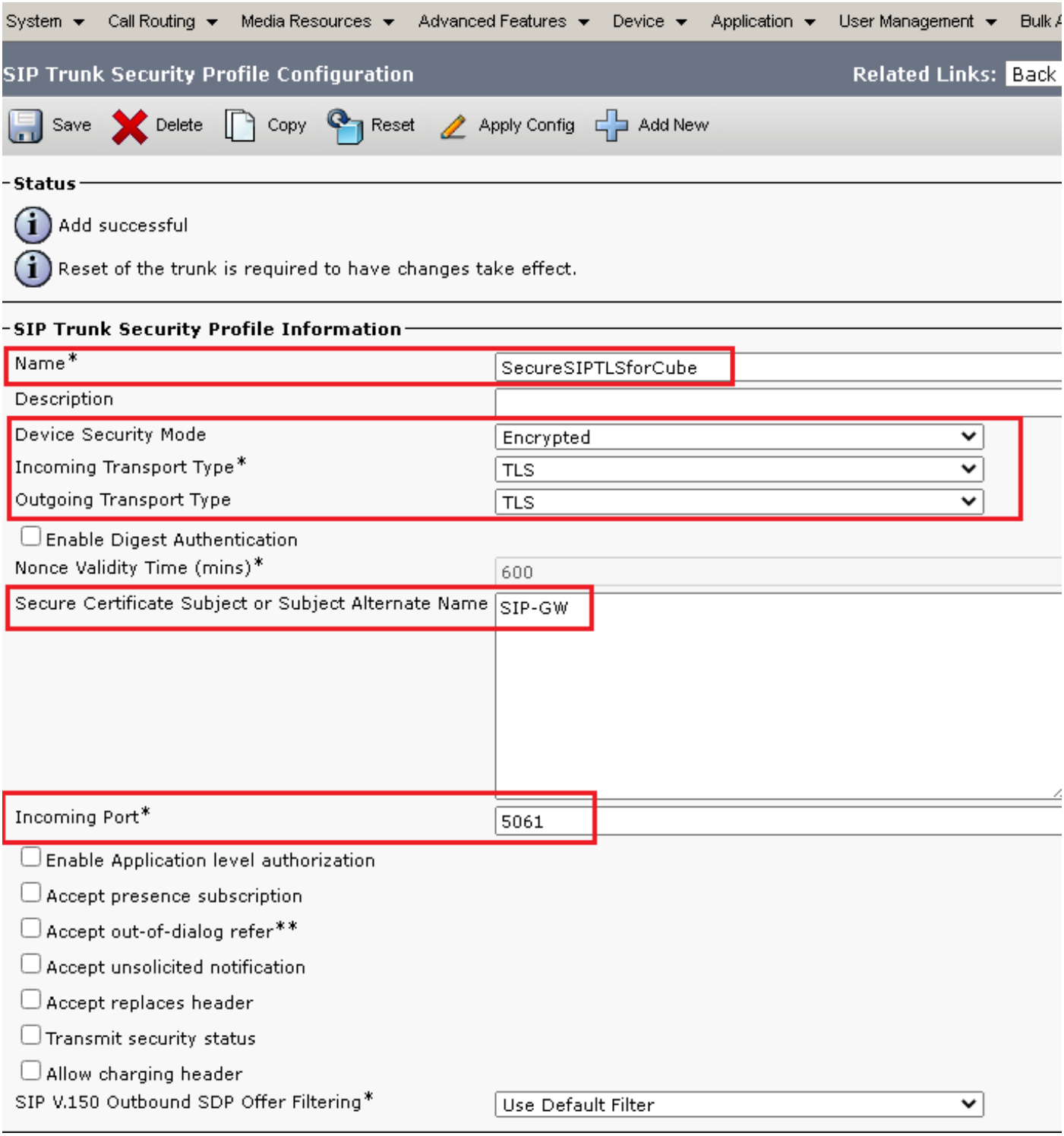
1. Connectez-vous à l'interface d'administration de CUCM.
2. Après avoir réussi à se connecter à CUCM, accédez à pourSystem > Security > SIP Trunk Security Profilecréer un profil de sécurité de périphérique pour CUBE.


System
Call Routing
Media Resources
Advanced Features
Device
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
Certificate
Phone Security Profile
SIP Trunk Security Profile
CUMA Server Security Profile
sing: The system has not co
on within 88 days to avoid l
device is configured. This is
ns Paging is not configured.
dministration
146
tel(R) Xeon(R) CPU E5-2660 v4
on Wednesday, December 25, 2019 3:
s, Inc.
tures and is subject to United States an
aws. By using this product you agree t
o cryptographic products may be found
mmunications Manager please visit our

3. En haut à gauche, cliquez sur Add New pour ajouter un nouveau profil.

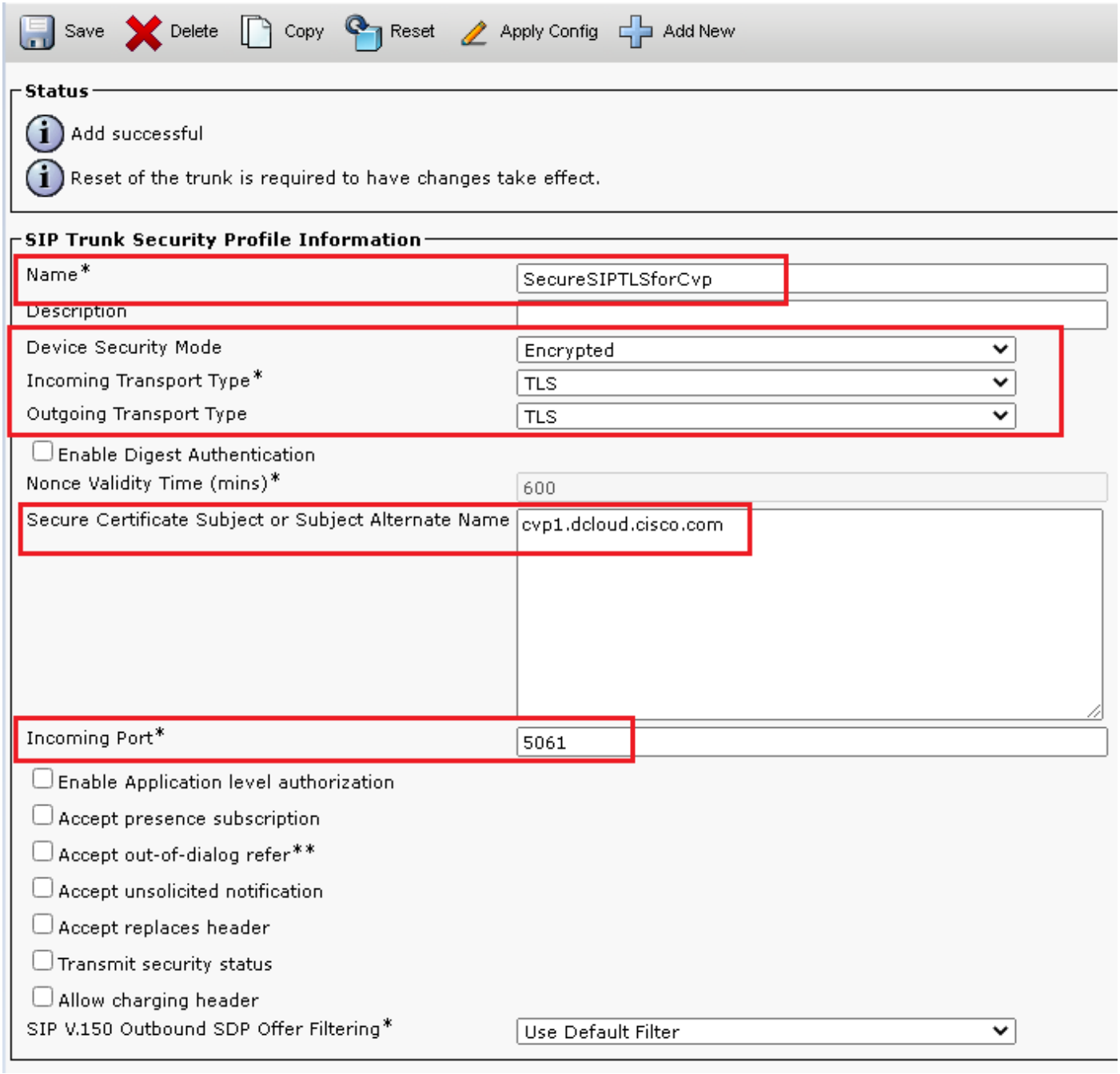


4. ConfigurezSIP Trunk Security Profilecomme image, puis cliquez surSaveen bas à gauche de la page.



5. Assurez-vous de définir leSecure Certificate Subject or Subject Alternate Namenom commun (CN) du certificat CUBE, car il doit correspondre.

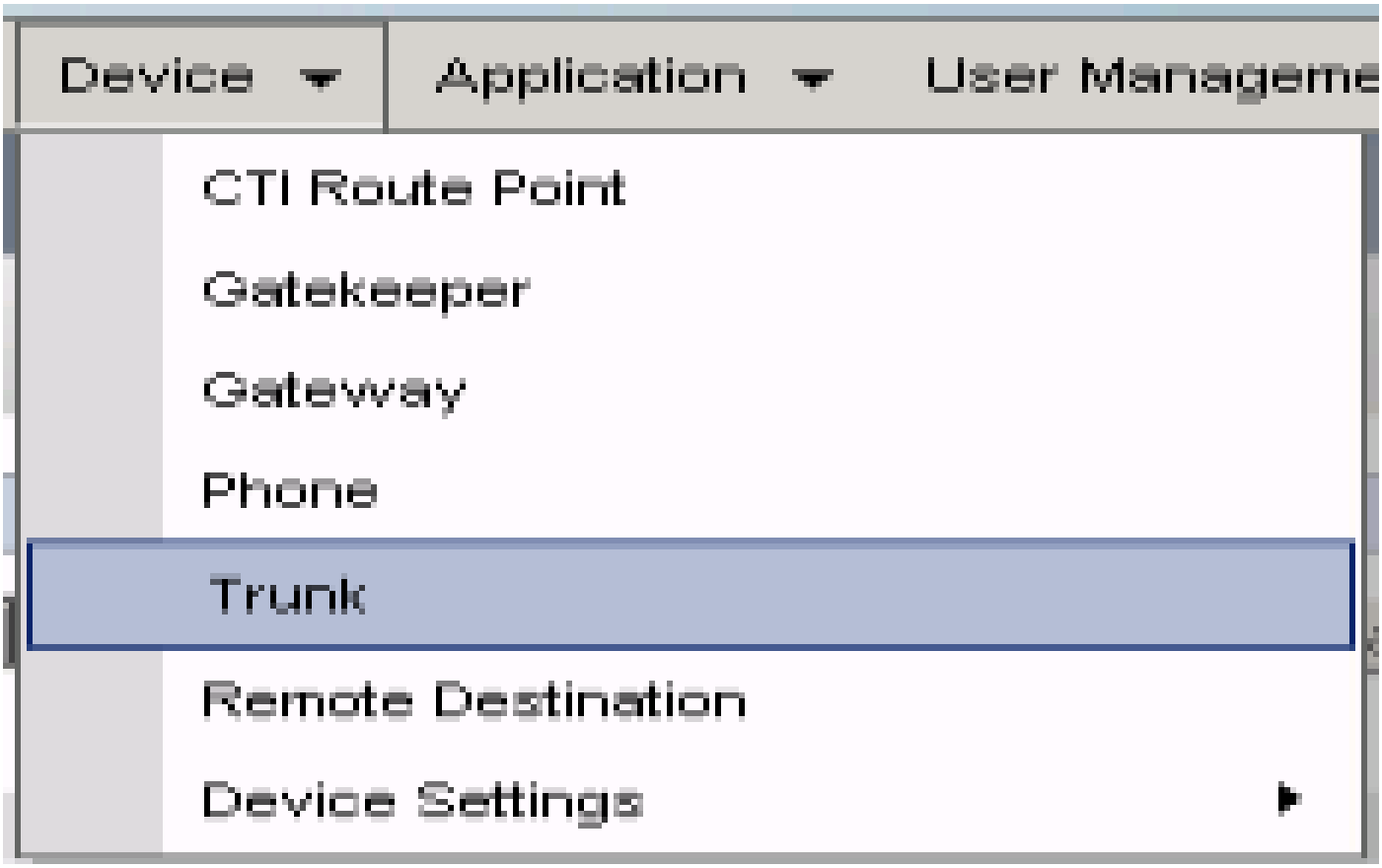
6. Cliquez surCopyle bouton et changez leNameenSecureSipTLSforCVP. RemplacezSecure Certificate Subjectpar le CN du certificat du serveur d'appels CVP car il doit correspondre. Cliquez surSave le bouton.



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

Étapes:

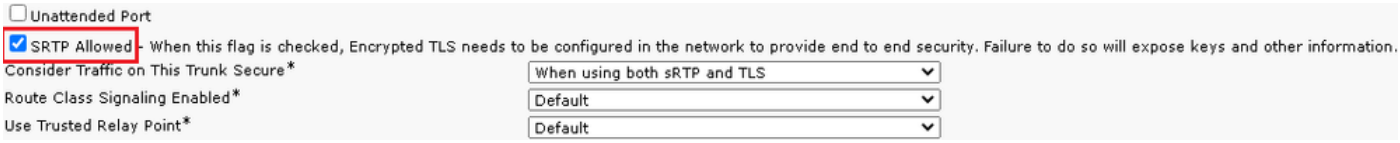
1. Sur la page CUCM Administration, accédez àDevice > Trunk.



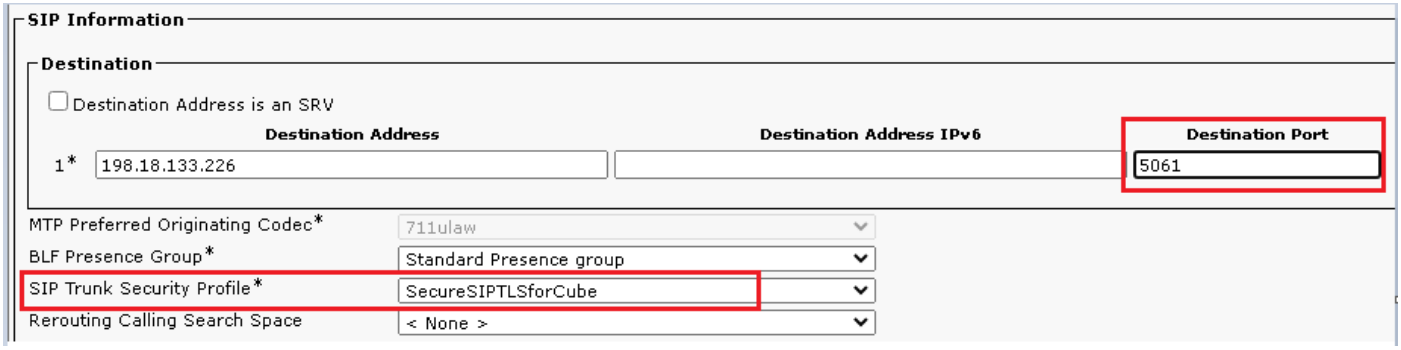
2. Recherchez la ligne principale CUBE. Dans cet exemple, le nom de la liaison CUBE estvCube, puis cliquez surFind.



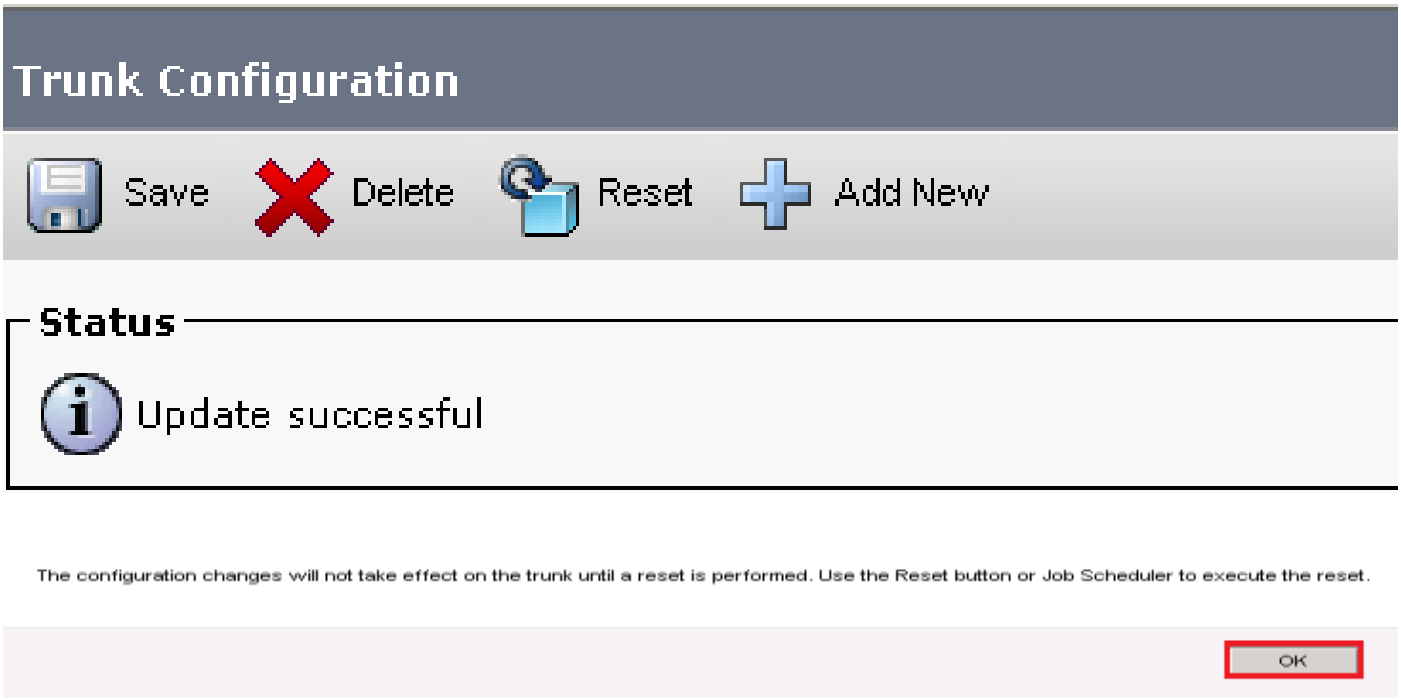
3. Cliquez survCUBEpour ouvrir la page de configuration de la liaison vCUBE.
4. Dans la sectionDevice Information, cochez la caseSRTP Allowedafin d'activer SRTP.



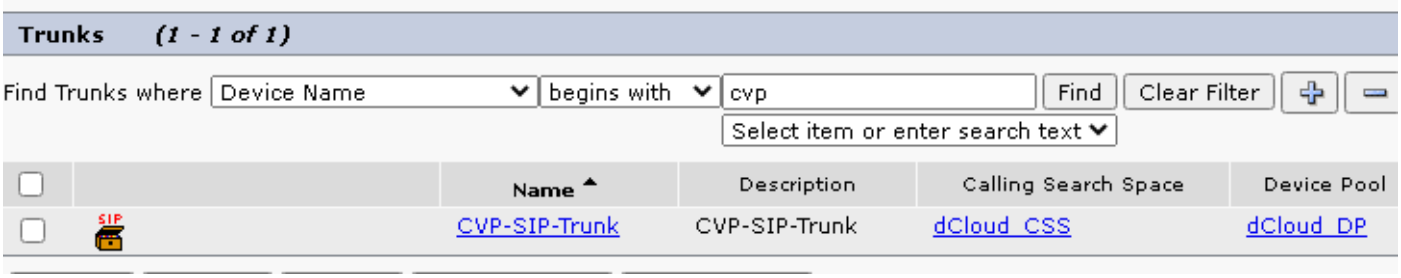
5. Faites défiler jusqu'à la sectionSIP Informationet remplacez laDestination Portpar5061.
6. RemplacezSIP Trunk Security Profileparsecure SIPTLSForCube.



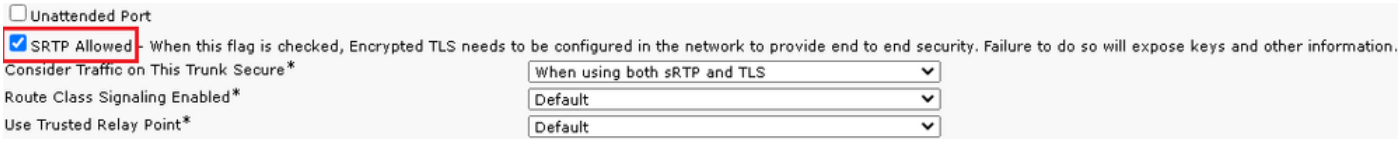
7. Cliquez surSave, puis surRestpour appliquer save les modifications.



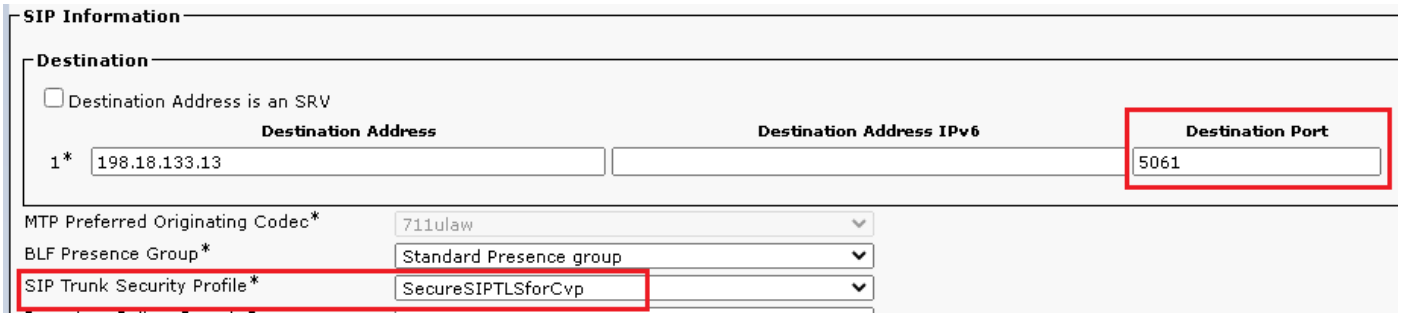
8. Naviguez jusqu'àDevice > Trunk, recherchez la ligne principale CVP, dans cet exemple, le nom de la ligne principale CVP estcvp-SIP-Trunk. Cliquez surFind.



9. Cliquez surCVP-SIP-Trunkpour ouvrir la page de configuration de la liaison CVP.
10. Dans la sectionDevice Information, cochez la caseSRTP Allowedafin d'activer SRTP.



11. Faites défiler jusqu'à la sectionSIP Information, changez laDestination Portenen5061.
12. RemplacezSIP Trunk Security ProfileparSecureSIPTLSForCvp.



13. Cliquez surSavepuis surRestpour appliquer save les modifications.



Communication sécurisée des périphériques des agents avec CUCM

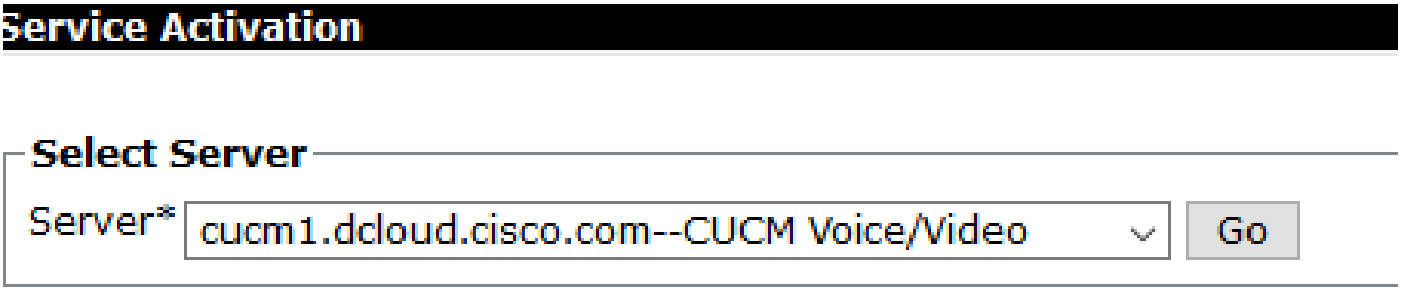
Afin d'activer les fonctionnalités de sécurité pour un périphérique, vous devez installer un certificat LSC (Locally Significative Certificate) et attribuer le profil de sécurité à ce périphérique. Le LSC possède la clé publique pour le terminal, qui est signée par la clé privée CAPF CUCM. Il n'est pas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

Étapes:

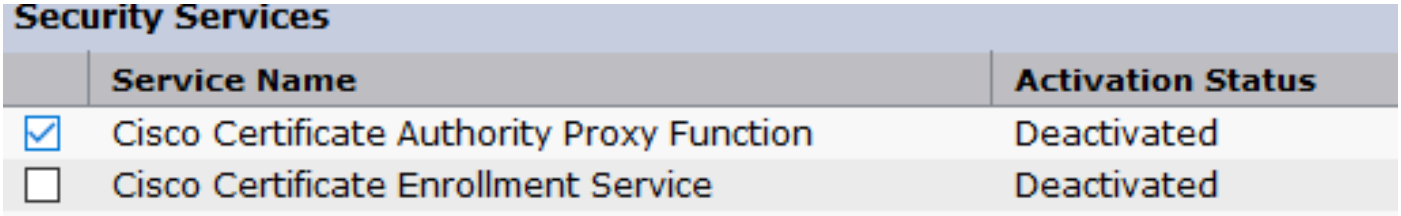
1. Connectez-vous à l'Cisco Unified Serviceabilityinterface.
2. Accédez àTools > Service Activation.



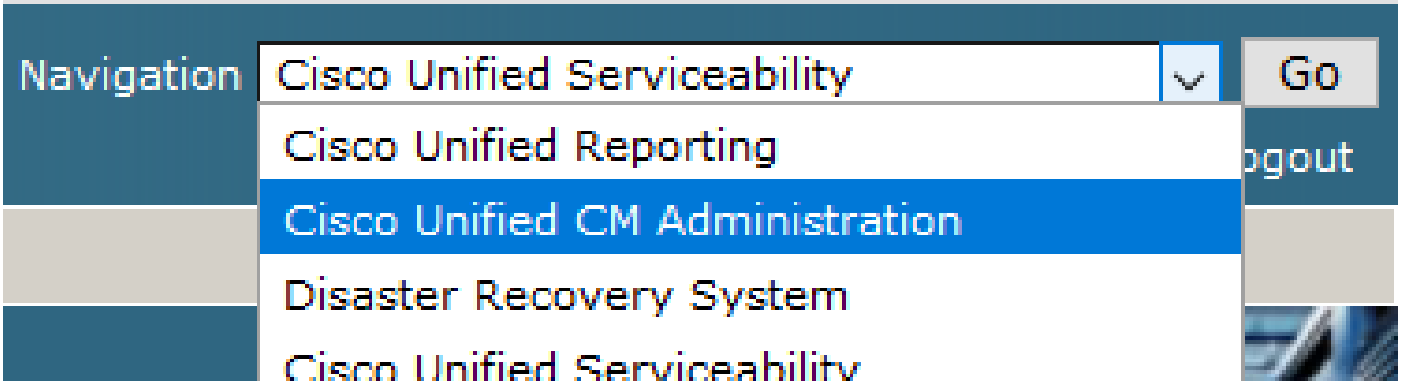
3. Choisissez le serveur CUCM et cliquez surGo.



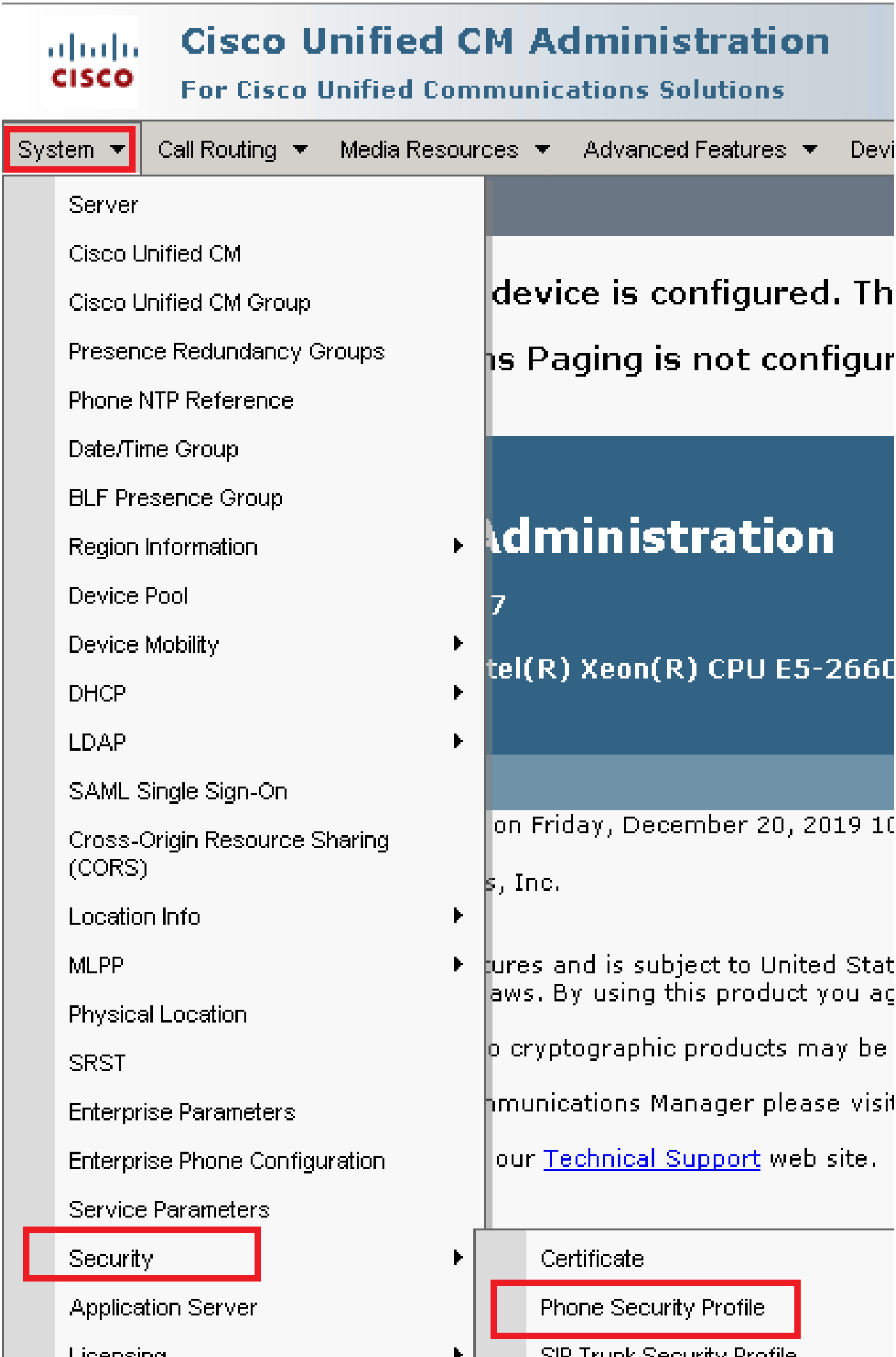
4. CochezCisco Certificate Authority Proxy Functionet cliquez surSave pour activer le service. Cliquez surOkpour confirmer.

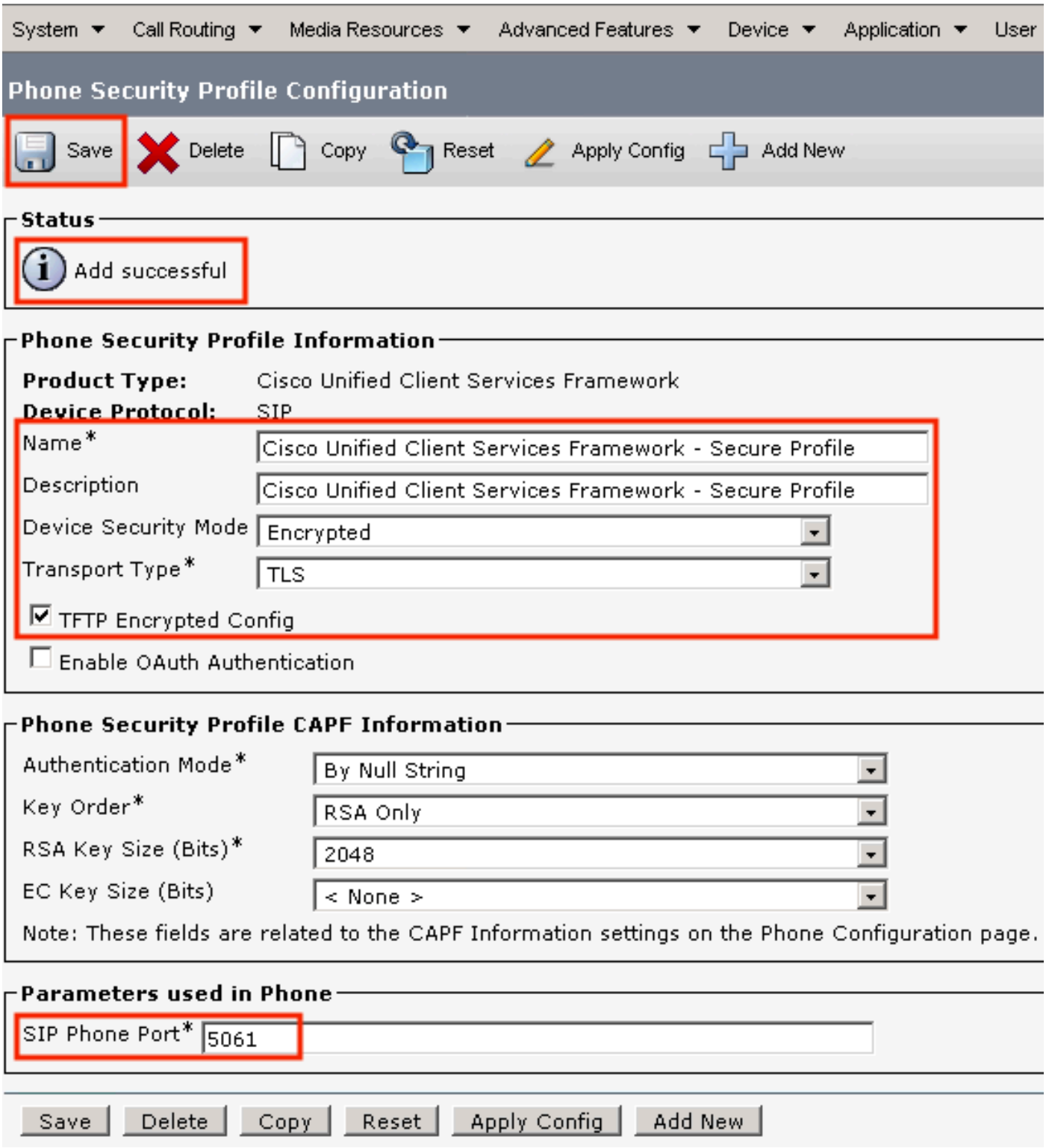


5. Assurez-vous que le service est activé, puis accédez à CUCM Administration.

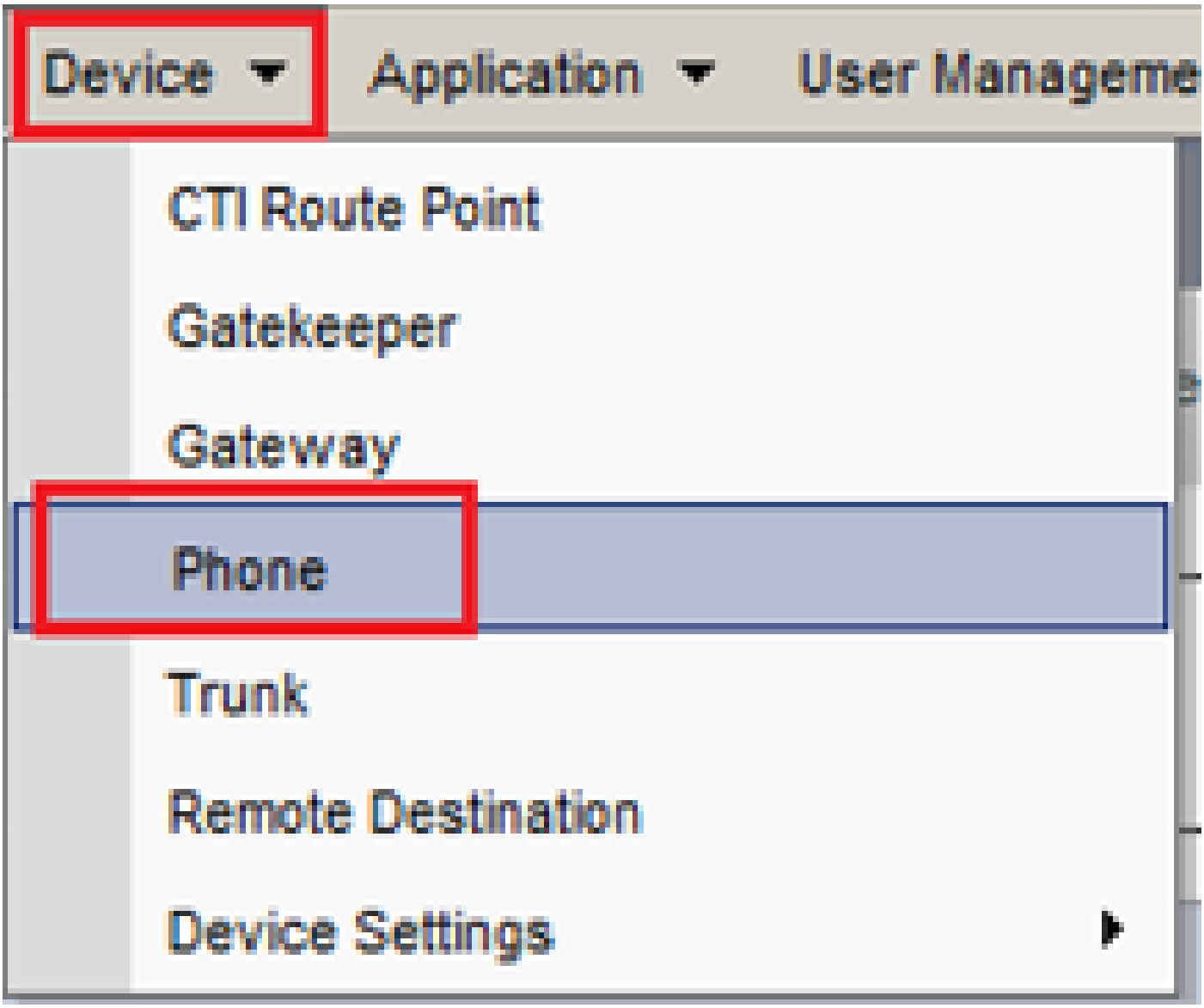


6. Une fois la connexion à l'administration de CUCM réussie, accédez à pourSystem > Security > Phone Security Profilecréer un profil de sécurité de périphérique pour le périphérique agent.

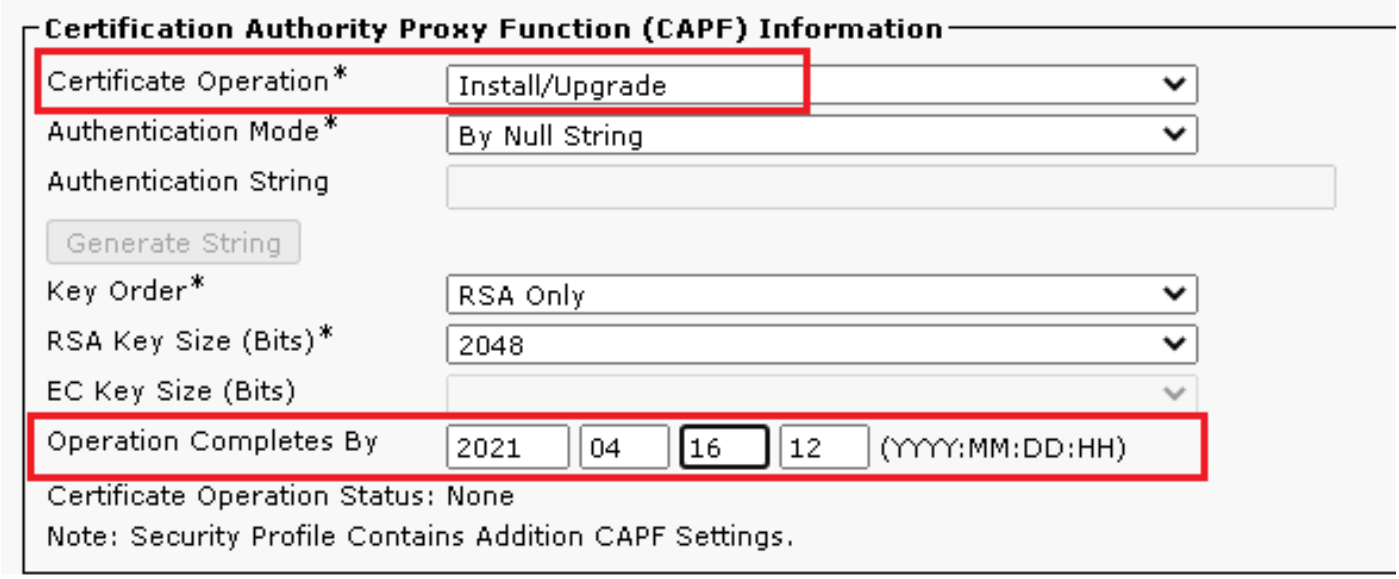

Cisco Unified CM Administration
For Cisco Unified Communications Solutions
System
Call Routing
Media Resources
Advanced Features
Server
Cisco Unified CM
Cisco Unified CM Group
Presence Redundancy Groups
Phone NTP Reference
Date/Time Group
BLF Presence Group
Region Information
Device Pool
Device Mobility
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
Certificate
Phone Security Profile
device is configured. Th
s Paging is not configur
dministration
tel(R) Xeon(R) CPU E5-266
on Friday, December 20, 2019 1
s, Inc.
ures and is subject to United Stat
aws. By using this product you ag
o cryptographic products may be
mmunications Manager please visit
our Technical Support web site.



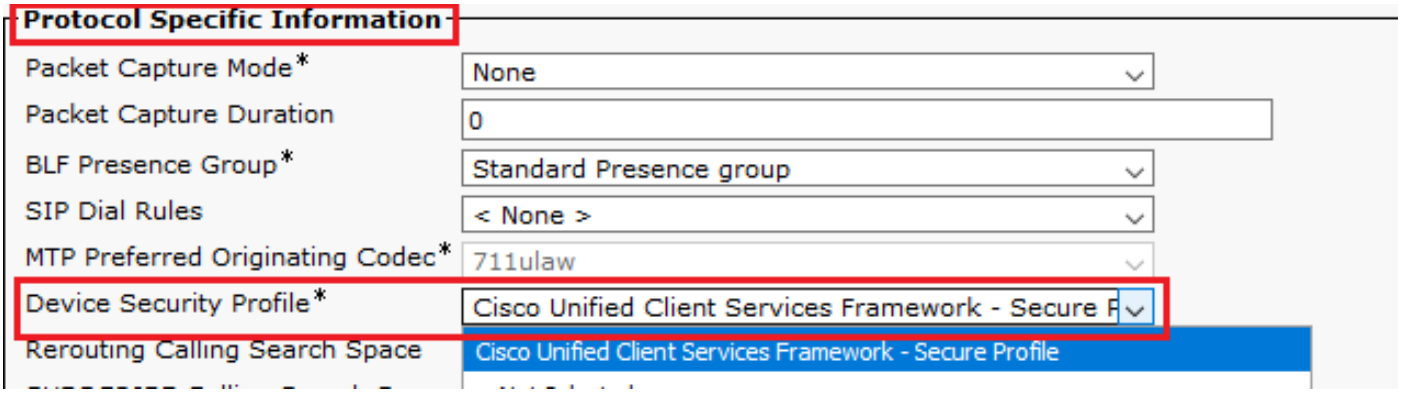
9. Une fois le profil de périphérique téléphonique créé, accédez àDevice > Phone.



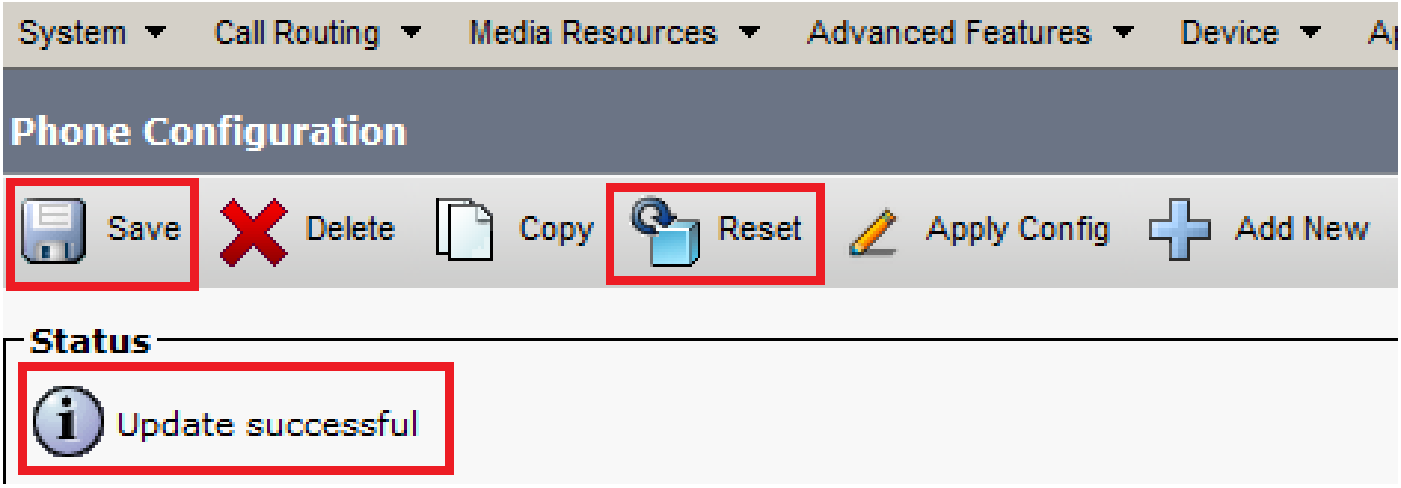
10. Cliquez surFindpour afficher la liste de tous les téléphones disponibles, puis cliquez sur téléphone de l'agent.
11. La page Agent phone configuration s'ouvre. RechercherCertification Authority Proxy Function (CAPF) Informationune section. Afin d'installer LSC, définissezCertificate OperationsurInstall/Upgradeet surOperation Completes bytoute date ultérieure.



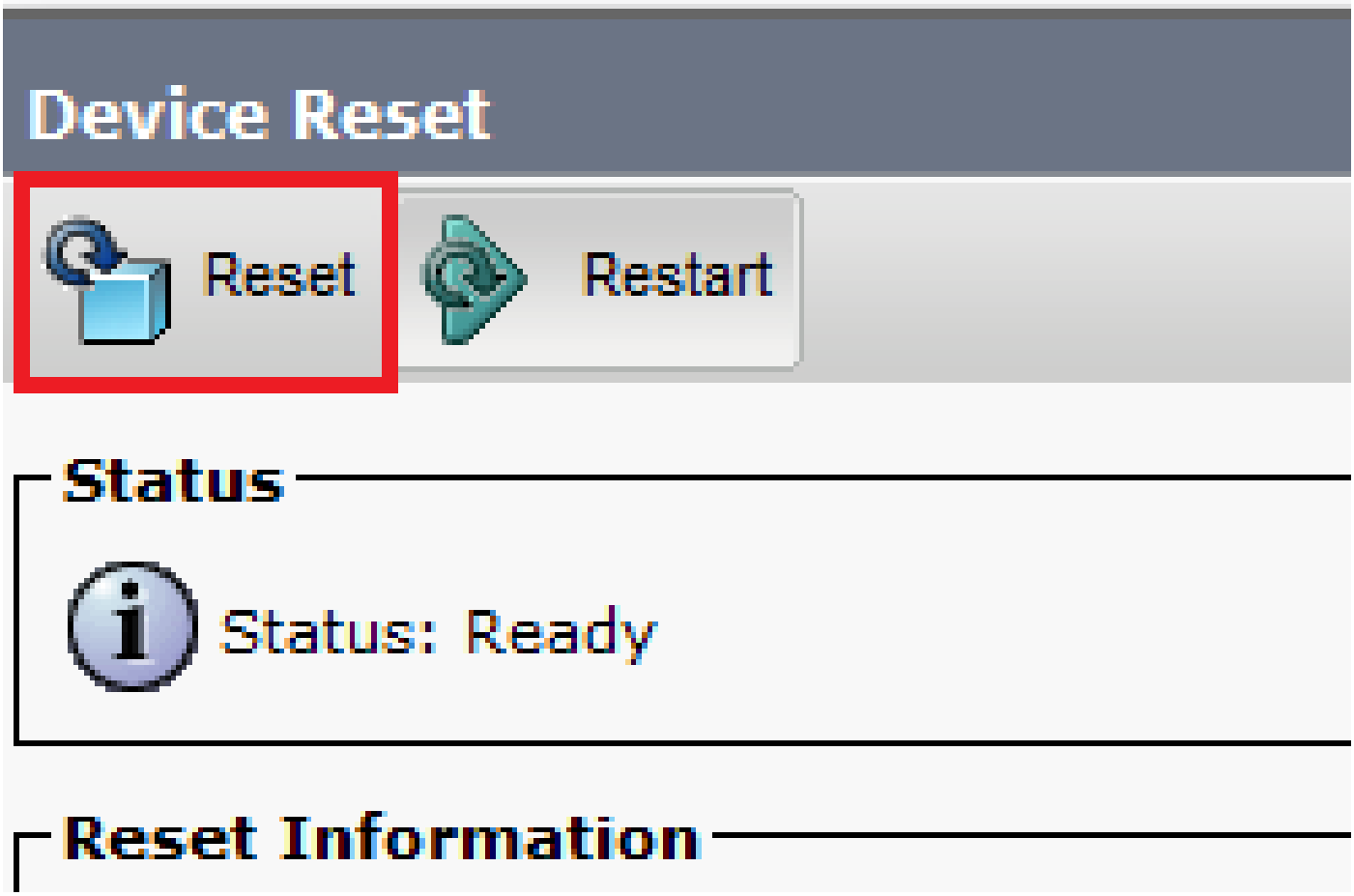
12. Recherchez Protocol Specific Information la section et remplacez la par Device Security Profile Cisco Unified Client Services Framework – Secure Profile.



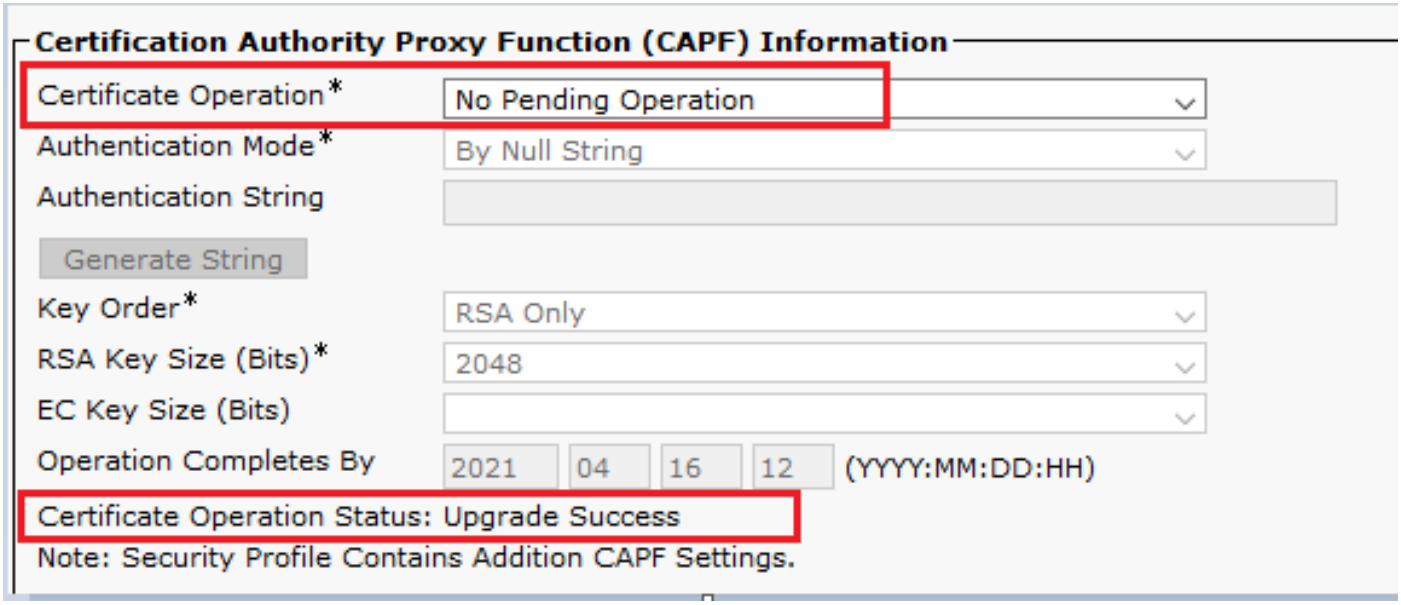
13. Cliquez sur Save en haut à gauche de la page. Vérifiez que les modifications ont été enregistrées, puis cliquez sur Reset.



14. Une fenêtre contextuelle s'ouvre. Cliquez sur Reset pour confirmer l'action.



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. VérifierCertification Authority Proxy Function (CAPF) Informationla section,Certificate Operationdoit être défini surNo Pending Operationet estCertificate Operation Statusdéfini sur Upgrade Success.



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 :

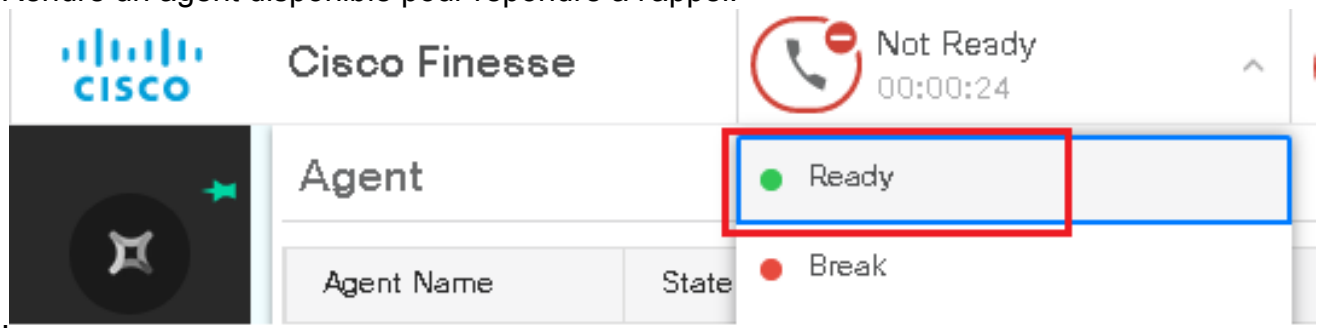
1. Effectuez un appel test au centre de contact et écoutez l'invite IVR.
2. Dans le même temps, ouvrez la session SSH sur vCUBE et exécutez cette commande :

   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 IC
 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 compris 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.



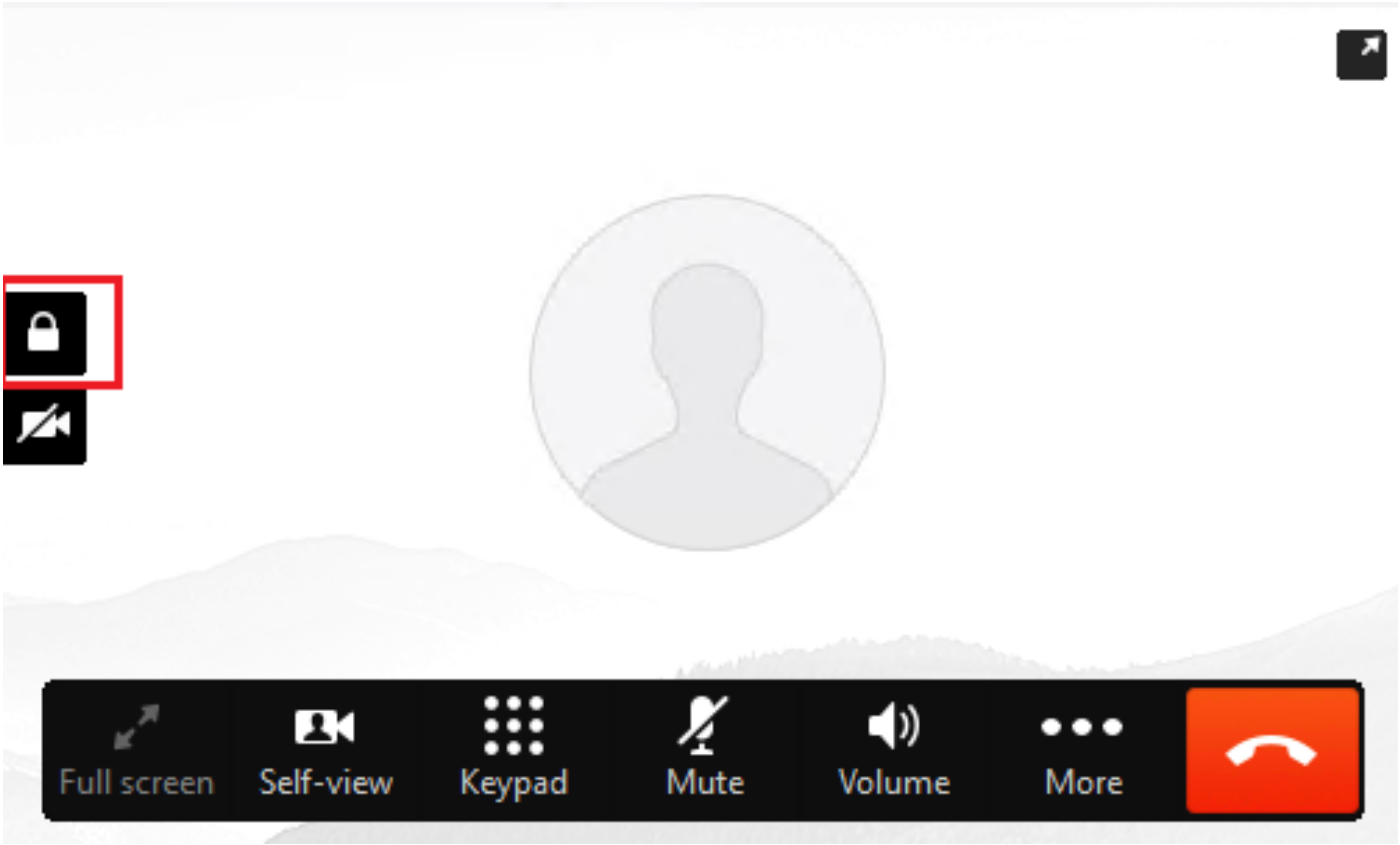
4. L'agent est réservé et l'appel est acheminé vers l'agent. Répondez à l'appel.
5. L'appel est connecté à l'agent. Retournez à la session SSH vCUBE et exécutez cette commande :

   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 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.