

# Sécurisez le joncteur réseau de SIP exemple entre CUCM et VCS configuration

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Configurez](#)

[Diagramme du réseau](#)

[Obtenez le certificat VCS](#)

[Générez et téléchargez le certificat Auto-signé par VCS](#)

[Ajoutez le certificat Auto-signé du serveur CUCM au serveur VCS](#)

[Certificat de téléchargement de serveur VCS au serveur CUCM](#)

[Connexion de SIP](#)

[Vérifiez](#)

[Dépannez](#)

[Informations connexes](#)

## Introduction

Ce document décrit comment installer une connexion sécurisée de Protocole SIP (Session Initiation Protocol) entre Cisco Unified Communications Manager (CUCM) et le serveur de communication vidéo Cisco TelePresence (VCS).

Les CUCM et les VCS sont étroitement intégrés. Puisque des points finaux visuels peuvent être enregistrés sur le CUCM ou le VCS, les joncteurs réseau de SIP doivent exister entre les périphériques.

## Conditions préalables

### Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Unified Communications Manager
- Serveur de communication vidéo Cisco TelePresence
- Certificats

## Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques. Cet exemple utilise la version de logiciel X7.2.2 de Cisco VCS et la version 9.x CUCM.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

## Configurez

Assurez-vous que les Certificats sont valides, ajoutez les Certificats aux serveurs CUCM et VCS de sorte qu'ils fassent confiance aux Certificats de chacun, puis établissent le joncteur réseau de SIP.

## Diagramme du réseau

### Obtenez le certificat VCS

Par défaut, tous les systèmes VCS été livré avec le certificat provisoire. À la page d'admin, naviguez vers la **Gestion de maintenance > de certificat > le certificat de serveur**. Cliquez sur le **certificat de serveur d'exposition**, et une nouvelle fenêtre s'ouvre avec les données brutes du certificat :

C'est un exemple des données brutes de certificat :

```
-----BEGIN CERTIFICATE-----
MIIDHzCCAoigAwIBAgIBATANBgkqhkiG9w0BAQUFADCBMjFDMEEGA1UECgw6VGvt
cG9yYXJ5IENlcnRpZmljYXR1IDU4Nzc0NWYwLTI5YTAzMTE4LTAwNTA1
Njk5NWl0YjFDMEEGA1UECww6VGvtcG9yYXJ5IENlcnRpZmljYXR1IDU4Nzc0NWYw
LTI5YTAzMTE4LTAwNTA1Njk5NWl0YjEOMAwGA1UEAwwFY2lzy28wHhcN
MTMwOTMwMDCxNzIwWhcNMTQwOTMwMDCxNzIwWjCBMjFDMEEGA1UECgw6VGvtcG9y
YXJ5IENlcnRpZmljYXR1IDU4Nzc0NWYwLTI5YTAzMTE4LTAwNTA1Njk5
NWl0YjFDMEEGA1UECww6VGvtcG9yYXJ5IENlcnRpZmljYXR1IDU4Nzc0NWYwLTI5
YTAzMTE4LTAwNTA1Njk5NWl0YjEOMAwGA1UEAwwFY2lzy28wDQYJ
KoZiHvcNAQEBBQADgY0AMIGJAoGBAKWvob+Y1zrKoAB5BvPsGR7aVfmTYPiP0I/
L21fyjjo05qv9lzDCgy7PFZPkDld/DNLiGp1jjUqdfFV+64r8OkESwBO+4DFlut
tWZLQ1uKzzdsMZ/b41mEtosElHNxH7rDYQsqdRA4ngNDJVlOgVFCEV4c7ZvAV4S
E8m9YNY9AgMBAAGjczBxMAKGA1UdEwQCMAAwJAYJYIZIAyb4QgENBBcWFVRlBxBv
cmFyeSBDZXJ0aWZpY2F0ZTAZBgNVHQ4EFgQU+knGYkeeIWqAJORhzQqRCHba+nEw
HwYDVR0jBBgwFoAUpHCEOXsBH1AzZN153S/Lv6cxNDIwDQYJKoZIhvcNAQEFBQAD
gYEAZklIMSfi49p1jIYqYdOAIjOiaShYVfqGUUMFr4V1hokM90ByGGTbx8jx6Y/S
p1SyT4ilU5uiY0DD18EkLzt8y3jFNPmHYAw/f2fB9J3mDAqbiQdmbLAeD2RRUsy7
1Zc3zTl6WL6hsj+90GAsI/TGthQ2n7yUWPl6CevopbJeliA=
-----END CERTIFICATE-----
```

Vous pouvez décoder le certificat et voir les données de certificat par l'utilisation d'OpenSSL sur votre ordinateur local ou l'utilisation d'un décodeur en ligne de certificat tel que le [client SSL](#) :

## Générez et téléchargez le certificat Auto-signé par VCS

Puisque chaque serveur VCS a un certificat avec le même nom commun, vous devez mettre de nouveaux Certificats sur le serveur. Vous pouvez choisir d'utiliser les Certificats auto-signés ou les Certificats signés par l'Autorité de certification (CA). Voyez la [création et l'utilisation de certificat de TelePresence Cisco avec le guide de déploiement de Cisco VCS](#) pour des détails de cette procédure.

Cette procédure décrit comment employer le VCS lui-même pour générer un certificat auto-signé, puis télécharge ce certificat :

1. Ouvrez une session comme racine au VCS, commencez OpenSSL, et générez une clé privée :

```
~ # openssl
OpenSSL> genrsa -out privatekey.pem 1024
Generating RSA private key, 1024 bit long modulus
.....+++++
.....+++++
e is 65537 (0x10001)
```

2. Employez cette clé privée afin de générer une demande de signature de certificat (CSR) :

```
OpenSSL> req -new -key privatekey.pem -out certcsr.pem
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:BE
State or Province Name (full name) [Some-State]:Vlaams-Brabant
Locality Name (eg, city) []:Diegem
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Cisco
Organizational Unit Name (eg, section) []:TAC
Common Name (e.g. server FQDN or YOUR name) []:radius.anatomy.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
OpenSSL> exit
```

3. Générez le certificat auto-signé :

```
~ # openssl x509 -req -days 360 -in certcsr.pem -signkey privatekey.pem -out vcscert.pem
Signature ok
subject=/C=BE/ST=Vlaams-Brabant/L=Diegem/O=Cisco/OU=TAC/CN=radius.anatomy.com
Getting Private key
~ #
```

4. Confirmez que les Certificats sont maintenant disponibles :

```
~ # ls -ltr *.pem
-rw-r--r-- 1 root root 891 Nov 1 09:23 privatekey.pem
-rw-r--r-- 1 root root 664 Nov 1 09:26 certcsr.pem
-rw-r--r-- 1 root root 879 Nov 1 09:40 vcscert.pem
```

5. Téléchargez les Certificats avec [WinSCP](#), et téléchargez-les sur la page Web ainsi le VCS peut utiliser les Certificats ; vous avez besoin de la clé privée et du certificat généré :



télécharger le fichier de nouveau au VCS :

Le VCS fera confiance maintenant aux Certificats offerts par CUCM.

5. Répétez cette procédure pour tous les serveurs VCS.

## Certificat de téléchargement de serveur VCS au serveur CUCM

Le CUCM doit faire confiance aux Certificats offerts par le VCS.

Cette procédure décrit comment télécharger le certificat VCS que vous avez généré sur le CUCM comme certificat de CallManager-confiance :

1. À la page de gestion de SYSTÈME D'EXPLOITATION, naviguez vers la **Gestion de Sécurité** > de **certificat**, écrivez le nom de certificat, parcourez à son emplacement, et cliquez sur Upload le **fichier** :
2. Téléchargez le certificat de tous les serveurs VCS. Faites ceci sur chaque serveur CUCM qui communiquera avec le VCS ; c'est typiquement tous les Noeuds qui exécutent le service de CallManager.

## Connexion de SIP

Une fois que des Certificats sont validés et les deux systèmes se font confiance, configurez la zone voisine sur VCS et le joncteur réseau de SIP sur CUCM. Voyez la [TelePresence Cisco Cisco Unified Communications Manager avec le guide de déploiement de Cisco VCS \(joncteur réseau de SIP\)](#) pour des détails de cette procédure.

## Vérifiez

Confirmez que la connexion de SIP est en activité dans la zone voisine sur VCS :

## Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

## Informations connexes

- [TelePresence Cisco Cisco Unified Communications Manager avec le guide de déploiement de Cisco VCS \(joncteur réseau de SIP\)](#)

- [Guide de l'administrateur de serveur de communication vidéo Cisco TelePresence](#)
- [Création et utilisation de certificat de TelePresence Cisco avec le guide de déploiement de Cisco VCS](#)
- [Guide d'administration de système d'exploitation de Cisco Unified Communications](#)
- [Guide d'administration de Cisco Unified Communications Manager](#)
- [Support et documentation techniques - Cisco Systems](#)