

# CUCM と VCS 間のセキュア SIP トランクの設定例

## 目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ネットワーク図](#)

[VCS 証明書の取得](#)

[VCS 自己署名証明書の生成およびアップロード](#)

[CUCM サーバから VCS サーバへの自己署名証明書の追加](#)

[VCS サーバから CUCM サーバへの証明書のアップロード](#)

[SIP 接続](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

## 概要

このドキュメントでは、Cisco Unified Communications Manager ( CUCM ) と Cisco TelePresence Video Communication Server ( VCS ) との間にセキュアな Session Initiation Protocol ( SIP ) 接続をセットアップする方法を説明します。

CUCM と VCS は密接に統合されます。ビデオ エンドポイントは CUCM または VCS のどちらにでも登録できるため、この 2 台のデバイス間に SIP トランクが存在する必要があります。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- Cisco Unified Communications Manager
- Cisco TelePresence Video Communication Server
- 証明書

## 使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。この例では、Cisco VCS ソフトウェア バージョン X7.2.2 と CUCM バージョン 9.x を使用します。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

## 設定

証明書が有効であることを確認してから、CUCM サーバと VCS サーバが互いの証明書を信頼するように両方のサーバに証明書を追加します。その後、SIP トランクを確立します。

## ネットワーク図

### VCS 証明書の取得

デフォルトでは、すべての VCS システムに仮証明書が付属しています。管理ページで、[Maintenance] > [Certificate management] > [Server certificate] に移動します。[Show server certificate] をクリックします。新しいウィンドウが開き、証明書の raw データが表示されます。

証明書の raw データの例は次のとおりです。

```
-----BEGIN CERTIFICATE-----
MIIDHzCCAoigAwIBAgIBATANBgkqhkiG9w0BAQUFADCbmjFDMEEGA1UECgw6VGvt
cG9yYXJ5IENlcnRpZmljYXRlIDU4Nzc0NWYwLTI5YTAzMTRlMy1hNTE4LTAwNTA1
Njk5NWl0YjFDMEEGA1UECww6VGvtcG9yYXJ5IENlcnRpZmljYXRlIDU4Nzc0NWYw
LTI5YTAzMTRlMy1hNTE4LTAwNTA1Njk5NWl0YjEOMAwGA1UEAwFY2lZy28wHhcN
MTMwOTMwMDcxNzIwWWhcNMTQwOTMwMDcxNzIwWjCBMjFDMEEGA1UECgw6VGvtcG9y
YXJ5IENlcnRpZmljYXRlIDU4Nzc0NWYwLTI5YTAzMTRlMy1hNTE4LTAwNTA1Njk5
NWl0YjFDMEEGA1UECww6VGvtcG9yYXJ5IENlcnRpZmljYXRlIDU4Nzc0NWYwLTI5
YTAzMTRlMy1hNTE4LTAwNTA1Njk5NWl0YjEOMAwGA1UEAwFY2lZy28wZ8wDQYJ
KoZiHvcNAQEBBQADgY0AMIGJAoGBAKWvob+Y1zrKoAB5BvPsGR7aVfmTYPipL0I/
L21fyyjo05qv9lzDCgy7PFZPpkD1d/DNLlGpljjUqdfFV+64r8OkESwBO+4DFlut
tWZLQ1uKzzdsMvZ/b41mEtosElHNxH7rDYQsqdRA4ngNDJv10gVFCEV4c7ZvAV4S
E8m9YNY9AgMBAAGjczBxMAkGA1UdEwQCMAAwJAYJYIZIAyb4QgENBBcWFVR1bXBv
cmFyeSBBDZXXJ0aWZpY2F0ZTAZBgNVHQ4EFgQU+knGYkeeiWqAjoRhZQqRCHba+nEw
HwYDVR0jBBgwFoAUpHCEOXsBH1AzZN153S/Lv6cxNDIwDQYJKoZIhvcNAQEFBQAD
gYEAZklIMSfi49pljIYqYdOAIjOiaShYVfqGUUMFr4V1hokM90ByGGTbx8jx6Y/S
p1SyT4ilU5uiY0DD18EkLzt8y3jFNPmHYAw/f2fB9J3mDAqbiQdmbLAeD2RRUsy7
1Zc3zTl6WL6hsj+90GAsI/TGthQ2n7yUWPl6CevopbJeliA=
-----END CERTIFICATE-----
```

証明書をデコードし、ローカル PC での OpenSSL またはオンライン証明書デコーダ ([SSL Shopper](#) など) を使用して証明書のデータを表示できます。

### VCS 自己署名証明書の生成およびアップロード

すべての VCS サーバの証明書には同じ共通名が使用されているため、新しい証明書をサーバ上に配置する必要があります。自己署名証明書を使用することも、認証局 (CA) から署名を受けた証明書を使用することもできます。この手順について詳しくは、『[Cisco VCS を使用した Cisco TelePresence 証明書の作成および使用 展開ガイド](#)』を参照してください。

以下の手順で、VCS 自体を使用して自己署名証明書を生成し、その証明書をアップロードする方法を説明します。

1. root として VCS にログインし、OpenSSL を起動して、秘密キーを生成します。

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

2. 生成した秘密キーを使用して証明書署名要求 (CSR) を生成します。

```
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. 自己署名証明書を生成します。

```
~ # 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. 証明書が使用可能になったことを確認します。

```
~ # 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. [WinSCP](#) で証明書をダウンロードし、Web ページに証明書をアップロードして VCS が使用できるようにします。秘密キーと生成された証明書の両方が必要です。



これで、VCS は CUCM が提示する証明書を信頼するようになります。

5. すべての VCSV サーバについて、以上の手順を繰り返します。

## VCS サーバから CUCM サーバへの証明書のアップロード

CUCM は VCS によって提示された証明書を信頼する必要があります。

以下の手順で、生成した VCS 証明書を CallManager-Trust 証明書として CUCM にアップロードする方法を説明します。

1. [OS Administration] ページで、[Security] > [Certificate Management] に移動し、証明書の名前を入力してその場所を参照し、[Upload File] をクリックします。
2. すべての VCS サーバから証明書をアップロードします。このステップは、VCS と通信するすべての CUCM サーバで行う必要があります。これは通常、CallManager サービスを実行しているすべてのノードです。

## SIP 接続

証明書が検証されて両方のシステムが互いを信頼するようになったら、VCS 上にネイバーゾーンを設定し、CUCM 上に SIP トランクを設定します。この手順について詳しくは、『[Cisco VCS \( SIP トランク \) を使用した Cisco TelePresence Cisco Unified Communications Manager 展開ガイド](#)』を参照してください。

## 確認

VCS 上のネイバーゾーンで SIP 接続がアクティブであることを確認します。

## トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

## 関連情報

- [Cisco VCS \( SIP トランク \) を使用した Cisco TelePresence Cisco Unified Communications Manager 展開ガイド](#)
- [Cisco TelePresence Video Communication Server 管理者ガイド](#)
- [Cisco VCS を使用した Cisco TelePresence 証明書の作成および使用 展開ガイド](#)
- [Cisco Unified Communications オペレーティングシステム管理ガイド](#)
- [Cisco Unified Communications Manager 管理ガイド](#)

- [テクニカルサポートとドキュメント - Cisco Systems](#)