Secure SIP Trunk between CUCM and VCS Configuration Example

Document ID: 116730

Contributed by Kristof Van Coillie, Cisco TAC Engineer.
Nov 12, 2013

Contents

Introduction

This document describes how to set up a secure Session Initiation Protocol (SIP) connection between the Cisco Unified Communications Manager (CUCM) and the Cisco TelePresence Video Communication Server (VCS).

The CUCM and VCS are closely integrated. Because video endpoints can be registered either on the CUCM or the VCS, SIP trunks must exist between the devices.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Unified Communications Manager
- Cisco TelePresence Video Communication Server
- Certificates

Components Used

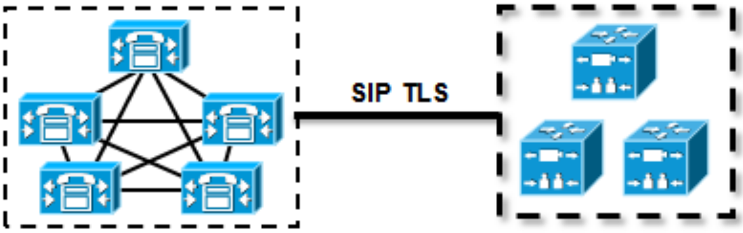
This document is not restricted to specific software and hardware versions. This example uses Cisco VCS software version X7.2.2 and CUCM version 9.x.

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. If your network is live, make sure that you understand the potential impact of any command.

Configure

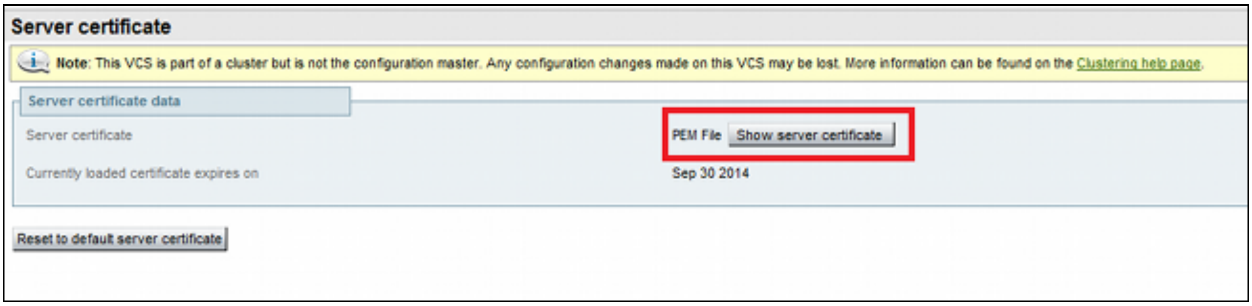
Ensure that the certificates are valid, add the certificates to the CUCM and VCS servers so that they trust each other's certificates, then establish the SIP trunk.

Network Diagram



Obtain VCS Certificate

By default, all VCS systems come with temporary certificate. On the admin page, navigate to ***Maintenance*** > ***Certificate management*** > ***Server certificate***. Click ***Show server certificate***, and a new window opens with the raw data of the certificate:



Server certificate

Note: This VCS is part of a cluster but is not the configuration master. Any configuration changes made on this VCS may be lost. More information can be found on the Clustering help page.

Server certificate data

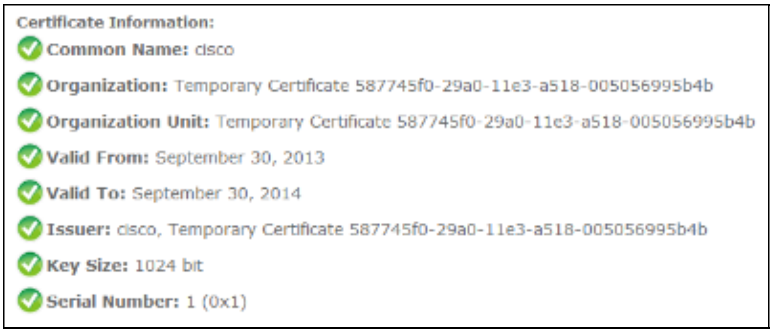
Server certificate PEM File

Currently loaded certificate expires on Sep 30 2014

This is an example of the raw certificate data:

```
-----BEGIN CERTIFICATE-----
MIIDHzCCAoigAwIBAgIBATANBgkqhkiG9w0BAQUFADCBmjFDMEEGA1UECgw6VGVt
cG9yYXJ5IENlcnRpZmljYXRlIDU4Nzc0NWYwLTI5YTAtMTFlMy1hNTE4LTAwNTA1
Njk5NWI0YjFDMEEGA1UECww6VGVtcG9yYXJ5IENlcnRpZmljYXRlIDU4Nzc0NWYw
LTI5YTAtMTFlMy1hNTE4LTAwNTA1Njk5NWI0YjEOMAwGA1UEAwwFY2lzY28wHhcN
MTMwOTMwMDcxNzIwWhcNMTQwOTMwMDcxNzIwWjCBmjFDMEEGA1UECgw6VGVtcG9y
YXJ5IENlcnRpZmljYXRlIDU4Nzc0NWYwLTI5YTAtMTFlMy1hNTE4LTAwNTA1Njk5
NWI0YjFDMEEGA1UECww6VGVtcG9yYXJ5IENlcnRpZmljYXRlIDU4Nzc0NWYwLTI5
YTAtMTFlMy1hNTE4LTAwNTA1Njk5NWI0YjEOMAwGA1UEAwwFY2lzY28wgZ8wDQYJ
KoZIhvcNAQEBBQADgY0AMIGJAoGBAKWvob+Y1zrKoAB5BvPsGR7aVfmTYPipL0I/
L21fyyjoO5qv9lzDCgy7PFZPxkD1d/DNLIgp1jjUqdfFV+64r8OkESwBO+4DFlut
tWZLQ1uKzzdsmvZ/b41mEtosElHNxH7rDYQsqdRA4ngNDJVlOgVFCEV4c7ZvAV4S
E8m9YNY9AgMBAAGjczBxMAkGA1UdEwQCMAAwJAYJYIZIAYb4QgENBBcWFVRlbXBv
cmFyeSBDZXJ0aWZpY2F0ZTAdBgNVHQ4EFgQU+knGYkeeiWqAjORhzQqRCHba+nEw
HwYDVR0jBBgwFoAUpHCEOXsBH1AzZN153S/Lv6cxNDIwDQYJKoZIhvcNAQEFBQAD
gYEAZklIMSfi49p1jIYqYdOAIjOiashYVfqGUUMFr4V1hokM90ByGGTbx8jx6Y/S
p1SyT4ilU5uiY0DD18EkLzt8y3jFNPmHYAw/f2fB9J3mDAqbiQdmbLAeD2RRUsy7
1Zc3zTl6WL6hsj+90GAsI/TGthQ2n7yUWPl6CevopbJe1iA=
-----END CERTIFICATE-----
```

You can decode the certificate and see the certificate data through the use of OpenSSL on your local PC or the use of an online certificate decoder such as SSL Shopper :



Certificate Information:

✓ Common Name: cisco

✓ Organization: Temporary Certificate 587745f0-29a0-11e3-a518-005056995b4b

✓ Organization Unit: Temporary Certificate 587745f0-29a0-11e3-a518-005056995b4b

✓ Valid From: September 30, 2013

✓ Valid To: September 30, 2014

✓ Issuer: cisco, Temporary Certificate 587745f0-29a0-11e3-a518-005056995b4b

✓ Key Size: 1024 bit

✓ Serial Number: 1 (0x1)

Generate and Upload VCS Self−Signed Certificate

Because every VCS server has a certificate with the same Common Name, you need to put new certificates on the server. You can choose to use self−signed certificates or certificates signed by the Certificate Authority (CA). See the Cisco TelePresence Certificate Creation and Use With Cisco VCS Deployment Guide for details of this procedure.

This procedure describes how to use the VCS itself to generate a self−signed certificate, then upload that certificate:

1. Log in as root to the VCS, start OpenSSL, and generate a private key:

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

2. Use this private key in order to generate a certificate signing request (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
```

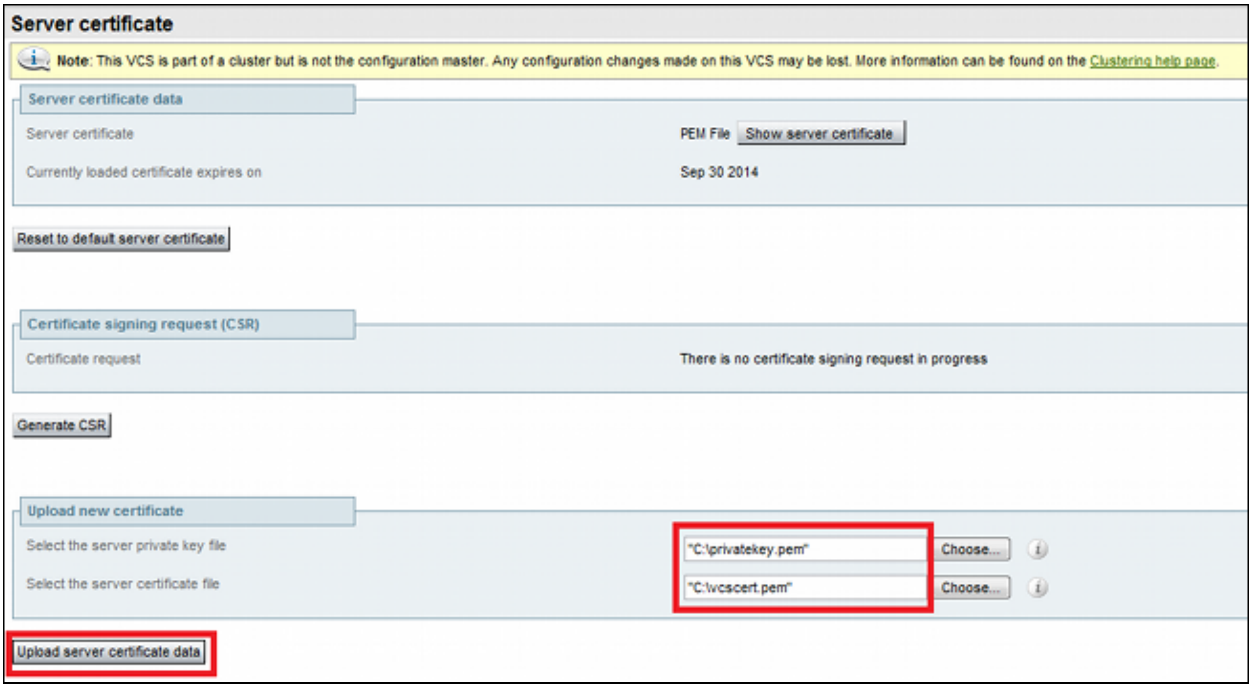
3. Generate the self−signed certificate:

```
~ # 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. Confirm that the certificates are now available:

```
~ # 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. Download the certificates with WinSCP , and upload them on the webpage so the VCS can use the certificates; you need the both private key and the generated certificate:



Server certificate

Note: This VCS is part of a cluster but is not the configuration master. Any configuration changes made on this VCS may be lost. More information can be found on the Clustering help page.

Server certificate data

Server certificate: PEM File [Show server certificate]

Currently loaded certificate expires on: Sep 30 2014

[Reset to default server certificate]

Certificate signing request (CSR)

Certificate request: There is no certificate signing request in progress

[Generate CSR]

Upload new certificate

Select the server private key file: "C:\privatekey.pem" [Choose...]

Select the server certificate file: "C:\vcscert.pem" [Choose...]

[Upload server certificate data]

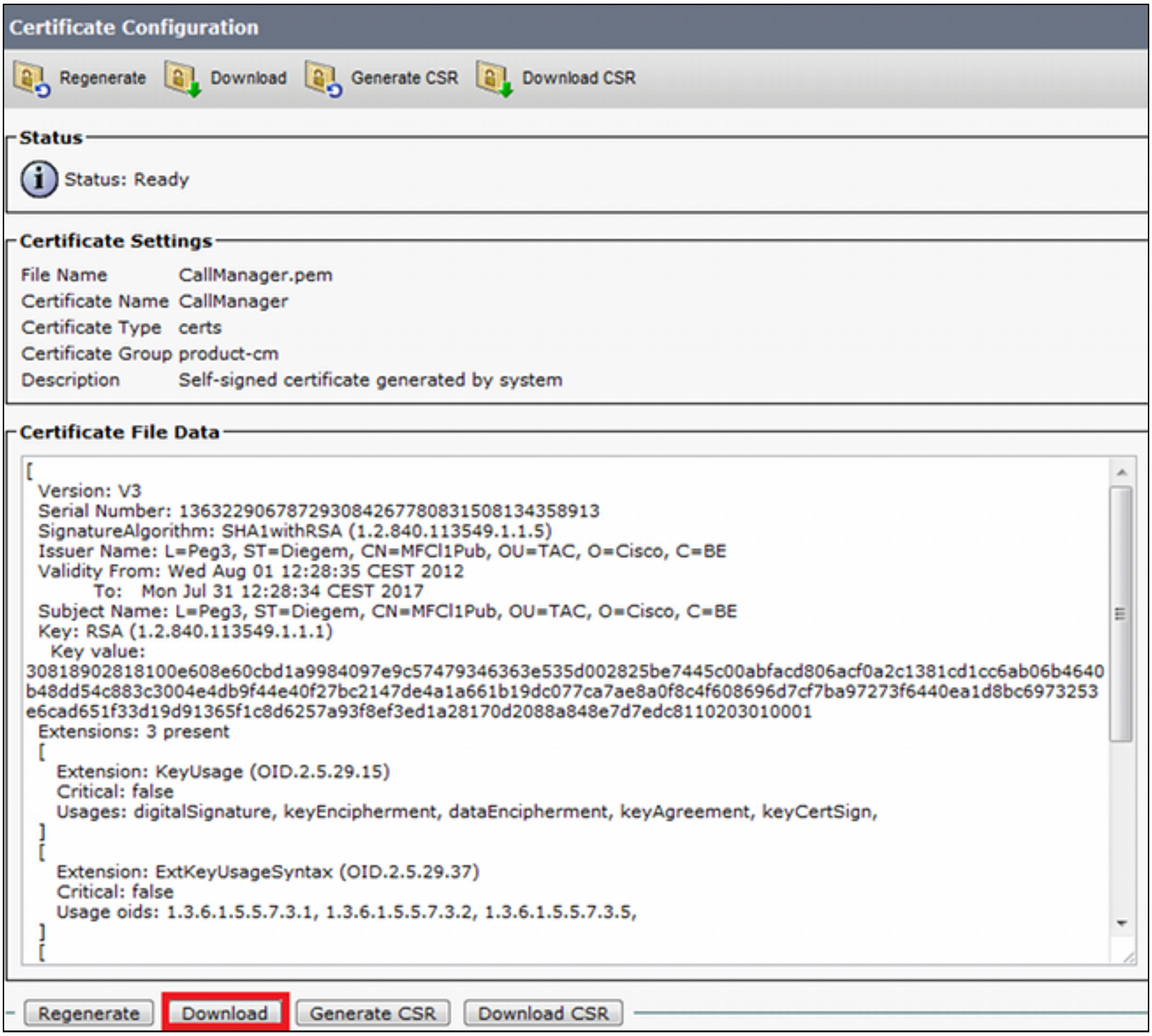
6. Repeat this procedure for all VCS servers.

Add Self−Signed Certificate from CUCM Server to VCS Server

Add the certificates from the CUCM servers so that the VCS will trust them. In this example, you are using the standard self−signed certificates from CUCM; CUCM generates self−signed certificates during installation so you do not need to create those as you did on the VCS.

This procedure describes how to add a self−signed certificate from the CUCM server to the VCS server:

1. Download the CallManager.pem certificate from the CUCM. Log into the OS Administration page, navigate to ***Security*** > ***Certificate Management***, then select and download the self−signed CallManager.pem certificate:



Certificate Configuration

Status

Status: Ready

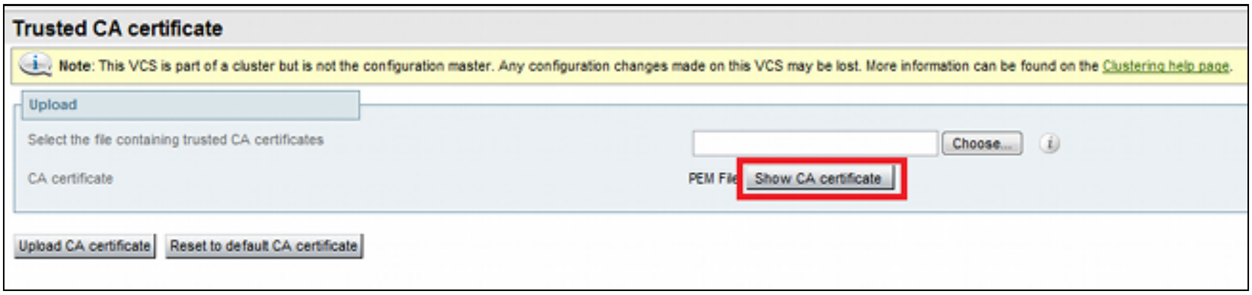
Certificate Settings

File Name	CallManager.pem
Certificate Name	CallManager
Certificate Type	certs
Certificate Group	product-cm
Description	Self-signed certificate generated by system

Certificate File Data

```
[
  Version: V3
  Serial Number: 136322906787293084267780831508134358913
  SignatureAlgorithm: SHA1withRSA (1.2.840.113549.1.1.5)
  Issuer Name: L=Peg3, ST=Diegem, CN=MFCl1Pub, OU=TAC, O=Cisco, C=BE
  Validity From: Wed Aug 01 12:28:35 CEST 2012
           To:   Mon Jul 31 12:28:34 CEST 2017
  Subject Name: L=Peg3, ST=Diegem, CN=MFCl1Pub, OU=TAC, O=Cisco, C=BE
  Key: RSA (1.2.840.113549.1.1.1)
    Key value:
30818902818100e608e60cbd1a9984097e9c57479346363e535d002825be7445c00abfacd806acf0a2c1381cd1cc6ab06b4640
b48dd54c883c3004e4db9f44e40f27bc2147de4a1a661b19dc077ca7ae8a0f8c4f608696d7cf7ba97273f6440ea1d8bc6973253
e6cad651f33d19d91365f1c8d6257a93f8ef3ed1a28170d2088a848e7d7edc8110203010001
  Extensions: 3 present
  [
    Extension: KeyUsage (OID.2.5.29.15)
    Critical: false
    Usages: digitalSignature, keyEncipherment, dataEncipherment, keyAgreement, keyCertSign,
  ]
  [
    Extension: ExtKeyUsageSyntax (OID.2.5.29.37)
    Critical: false
    Usage oids: 1.3.6.1.5.5.7.3.1, 1.3.6.1.5.5.7.3.2, 1.3.6.1.5.5.7.3.5,
  ]
  [
```

2. Add this certificate as a trusted CA certificate on the VCS.On the VCS, navigate to ***Maintenance*** > ***Certificate management*** > ***Trusted CA certificate***, and select ***Show CA certificate***:



Trusted CA certificate

Note: This VCS is part of a cluster but is not the configuration master. Any configuration changes made on this VCS may be lost. More information can be found on the Clustering help page.

Upload

Select the file containing trusted CA certificates

CA certificate PEM File

A new window opens with all certificates that are currently trusted.

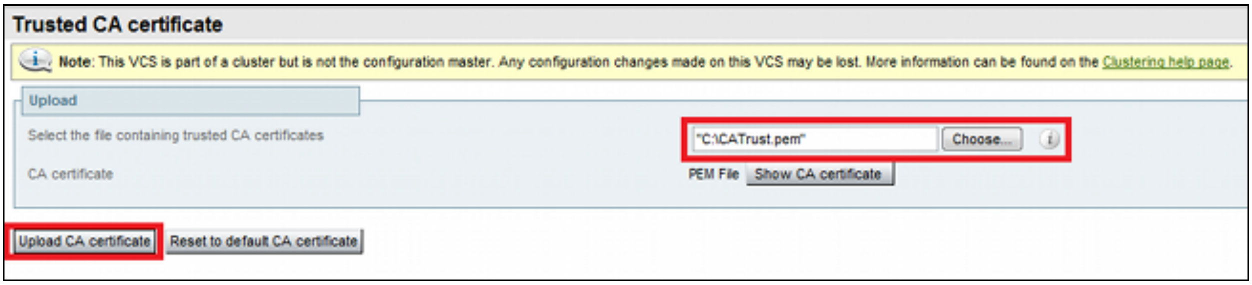
3. Copy all of the currently trusted certificates to a text file. Open the CallManager.pem file in a text editor, copy its content, and add that content to the bottom of the same text file after the currently trusted certificates:

```
CallManagerPub
======================
-----BEGIN CERTIFICATE-----
```

```
MIICmDCCAgGgAwIBAgIQZo7WOmjKYy9JP228PpPvgTANBgkqhkiG9w0BAQUFADBe
MQswCQYDVQQGEwJCRTEOMAwGA1UEChMFQ2lzY28xDDAKBgNVBAsTA1RBQzERMA8G
A1UEAxMITUZDbDFQdWIxDzANBgNVBAgTBkRpZWdlbTENMAsGA1UEBxMEUGVnMzAe
Fw0xMjA4MDExMDI4MzVaFw0xNzA3MzExMDI4MzRaMF4xCzAJBgNVBAYTAkJFMQ4w
DAYDVQQKEwVDaXNjbzEMMAoGA1UECxMDVEFDMREwDwYDVQQDEwhNRkNsMVB1YjEP
MA0GA1UECBMGRGllZ2VtMQ0wCwYDVQQHEwRQZWczMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQDmCOYMvRqZhAl+nFdHk0Y2PlNdACglvnRFwAq/rNgGrPCiwTgc
0cxqsGtGQLSN1UyIPDAE5NufROQPJ7whR95KGmYbGdwHfKeuig+MT2CGltfPe6ly
c/ZEDqHYvGlzJT5srWUfM9GdkTZfHI1iV6k/jvPtGigXDSCIqEjn1+3IEQIDAQAB
o1cwVTALBgNVHQ8EBAMCArwwJwYDVR0lBCAwHgYIKwYBBQUHAwEGCCsGAQUFBwMC
BggrBgEFBQcDBTAdBgNVHQ4EFgQUK4jYX6O6BAnLCalbKEn6YV7BpkQwDQYJKoZI
hvcNAQEFBQADgYEAkEGDdRdMOtX4ClhEatQE3ptT6L6RRAyP8oDd3dIGEOYWhA2H
Aqrw77loieva297AwgcKbPxnd5lZ/aBJxvmF8TIiOSkjy+dJW0asZWfei9STxVGn
NSr1CyAt8UJh0DSUjGHtnv7yWse5BB9mBDR/rmWxIRrlIRzAJDeygLIq+wc=
-----END CERTIFICATE-----
```

If you have multiple servers in the CUCM cluster, add all of them here.

4. Save the file as CATrust.pem, and click ***Upload CA certificate*** in order to upload the file back to the VCS:



Trusted CA certificate

Note: This VCS is part of a cluster but is not the configuration master. Any configuration changes made on this VCS may be lost. More information can be found on the Clustering help page.

The VCS will now trust the certificates offered by CUCM.

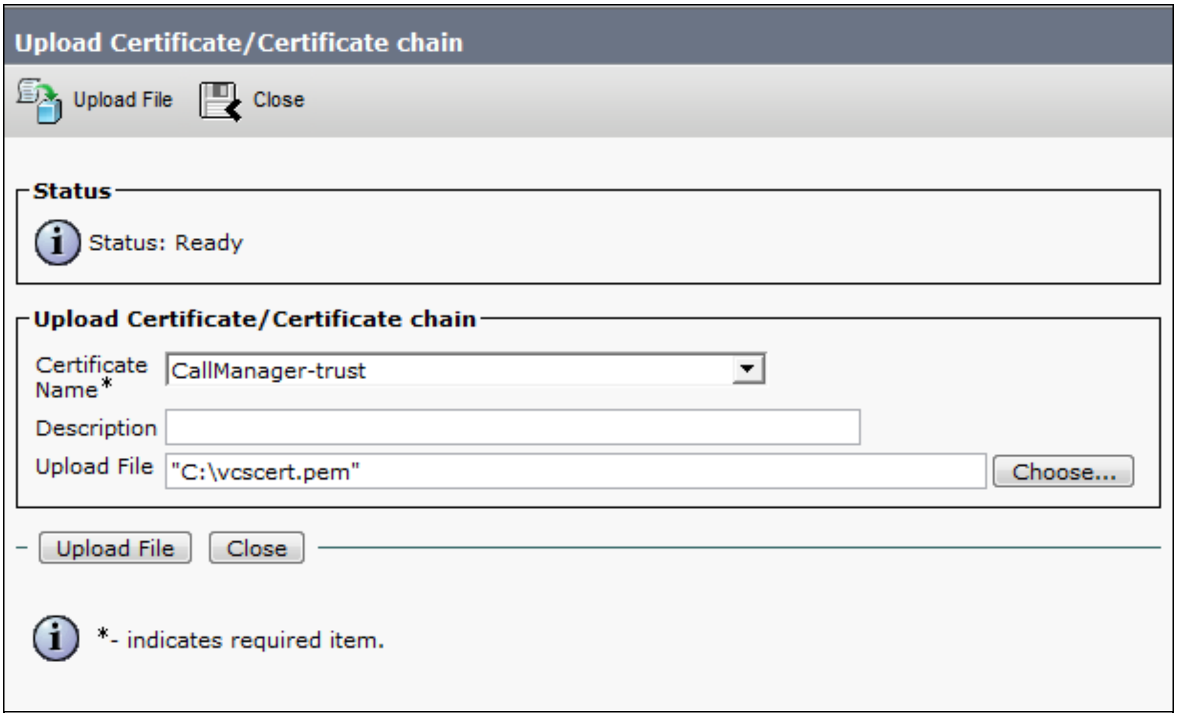
5. Repeat this procedure for all VCS servers.

Upload Certificate from VCS Server to CUCM Server

The CUCM needs to trust the certificates offered by the VCS.

This procedure describes how to upload the VCS certificate you generated on the CUCM as a CallManager−Trust certificate:

1. On the OS Administration page, navigate to ***Security*** > ***Certificate Management***, enter the certificate name, browse to its location, and click ***Upload File***:



Upload Certificate/Certificate chain

Status

Status: Ready

Upload Certificate/Certificate chain

Certificate Name*: CallManager-trust

Description:

Upload File: "C:\vcscert.pem"

*- indicates required item.

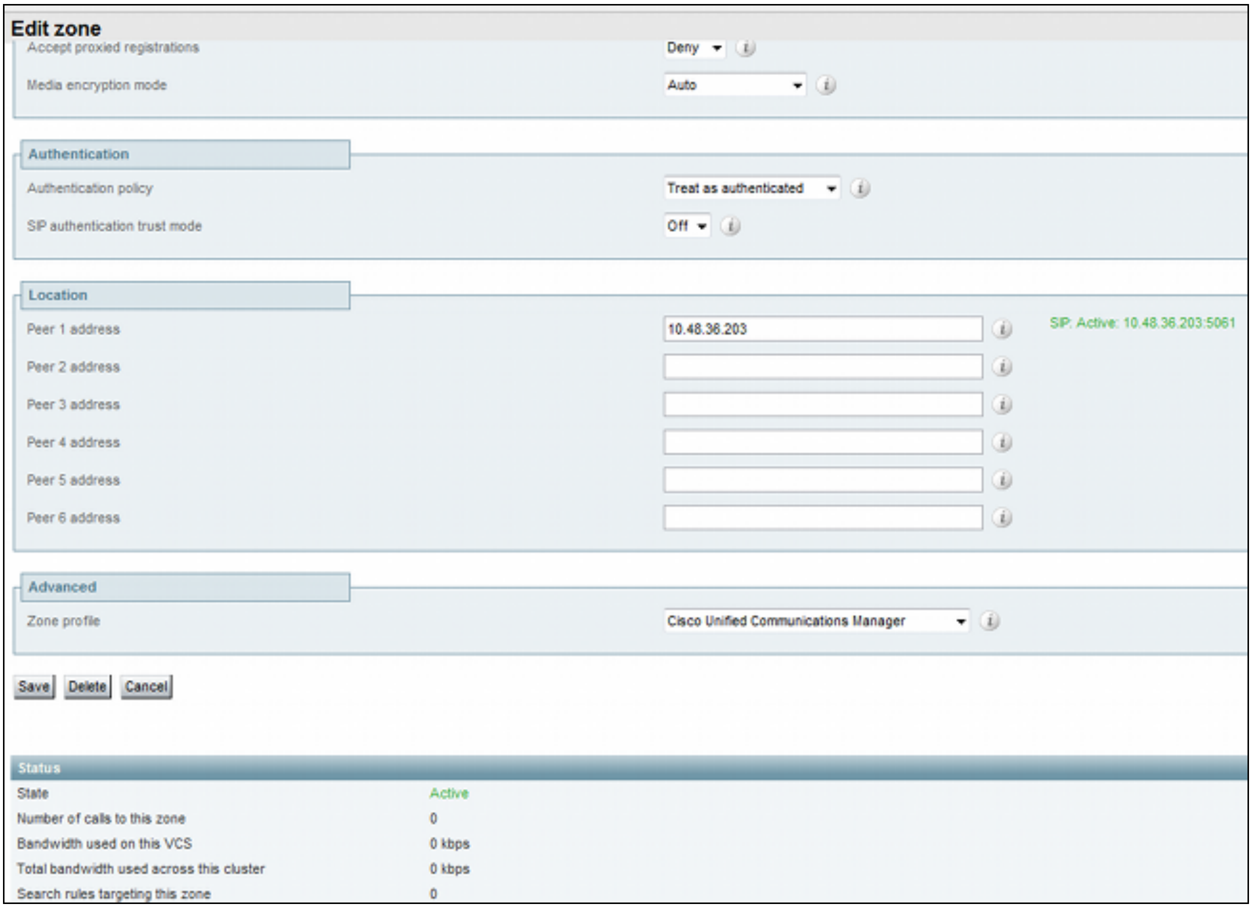
2. Upload the certificate from all VCS servers. Do this on every CUCM server that will communicate with the VCS; this is typically all nodes that are running the CallManager Service.

SIP Connection

Once certificates are validated and both systems trust each other, configure the Neighbor Zone on VCS and the SIP Trunk on CUCM. See the Cisco TelePresence Cisco Unified Communications Manager with Cisco VCS (SIP Trunk) Deployment Guide for details of this procedure.

Verify

Confirm that the SIP connection is active in the Neighbor Zone on VCS:



Edit zone

Accept proxied registrations: Deny

Media encryption mode: Auto

Authentication

Authentication policy: Treat as authenticated

SIP authentication trust mode: Off

Location

Peer 1 address: 10.48.36.203 — SIP: Active: 10.48.36.203:5061

Peer 2 address:

Peer 3 address:

Peer 4 address:

Peer 5 address:

Peer 6 address:

Advanced

Zone profile: Cisco Unified Communications Manager

Status

State	Active
Number of calls to this zone	0
Bandwidth used on this VCS	0 kbps
Total bandwidth used across this cluster	0 kbps
Search rules targeting this zone	0

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- ***Cisco TelePresence Cisco Unified Communications Manager with Cisco VCS (SIP Trunk) Deployment Guide***
- ***Cisco TelePresence Video Communication Server Administrator Guide***
- ***Cisco TelePresence Certificate Creation and Use With Cisco VCS Deployment Guide***
- ***Cisco Unified Communications Operating System Administration Guide***
- ***Cisco Unified Communications Manager Administration Guide***
- ***Technical Support & Documentation − Cisco Systems***