Exemplo de configuração de tronco SIP seguro entre CUCM e VCS

Contents

Introduction

Este documento descreve como configurar uma conexão segura do Session Initiation Protocol (SIP) entre o Cisco Unified Communications Manager (CUCM) e o Cisco TelePresence Video Communication Server (VCS).

O CUCM e o VCS estão intimamente integrados. Como os endpoints de vídeo podem ser registrados no CUCM ou no VCS, os troncos SIP devem existir entre os dispositivos.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Unified Communications Manager
- Servidor de comunicação por vídeo Cisco TelePresence
- Certificados

Componentes Utilizados

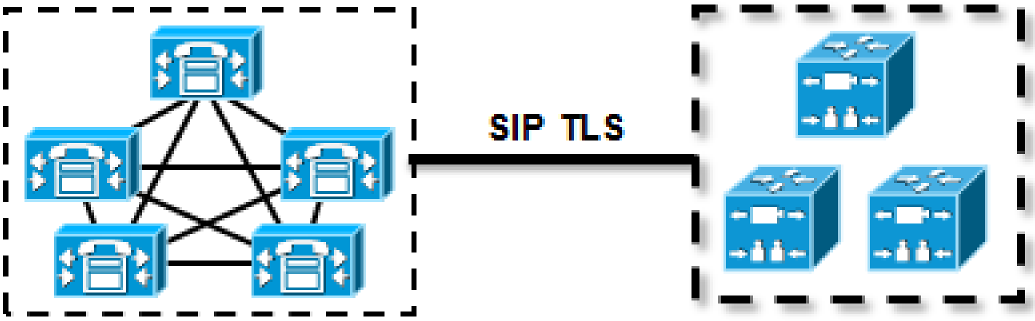
Este documento não se restringe a versões de software e hardware específicas. Este exemplo usa o software Cisco VCS versão X7.2.2 e CUCM versão 9.x.

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.

Configurar

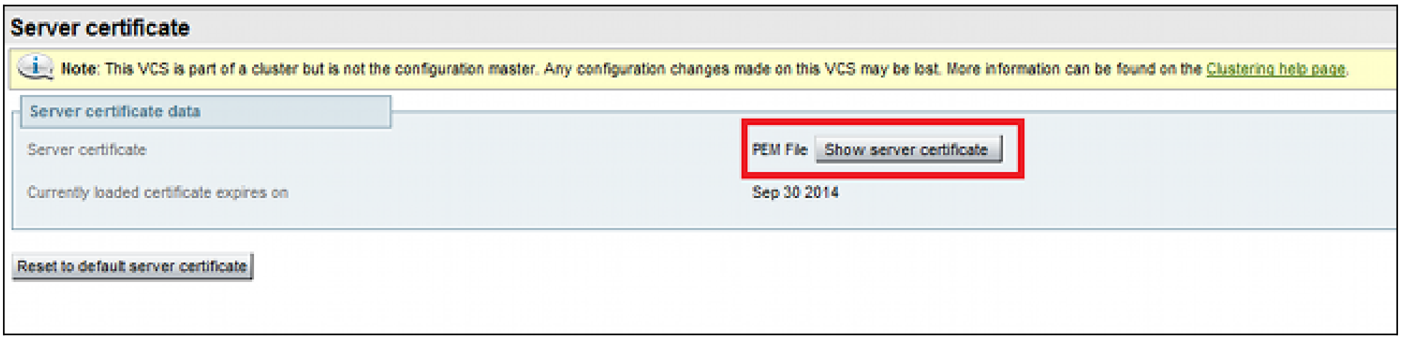
Verifique se os certificados são válidos, adicione os certificados aos servidores CUCM e VCS para que eles confiem nos certificados uns dos outros e estabeleça o tronco SIP.

Diagrama de Rede



Obter certificado VCS

Por padrão, todos os sistemas VCS vêm com certificado temporário. Na página admin, navegue para **Manutenção** > **Gerenciamento de certificado** > **Certificado do servidor**. Clique em **Mostrar certificado do servidor** e uma nova janela será aberta com os dados brutos do certificado:



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

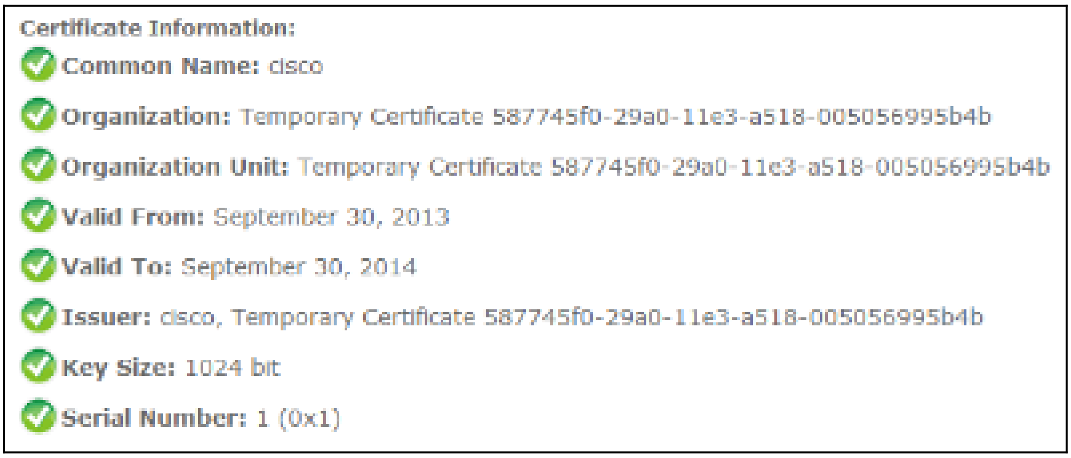
[Reset to default server certificate]

Este é um exemplo dos dados brutos do certificado:

```
-----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-----
```

Você pode decodificar o certificado e ver os dados do certificado usando o OpenSSL em seu computador local ou usando um decodificador de certificado online, como o 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)

Gerar e carregar certificado autoassinado VCS

Como cada servidor VCS tem um certificado com o mesmo nome comum, você precisa colocar novos certificados no servidor. Você pode optar por usar certificados autoassinados ou certificados assinados pela Autoridade de Certificação (CA). Consulte o Cisco TelePresence Certificate Creation and Use With Cisco VCS Deployment Guide para obter detalhes deste procedimento.

Este procedimento descreve como usar o próprio VCS para gerar um certificado autoassinado e depois carregar esse certificado:

1. Faça login como raiz no VCS, inicie o OpenSSL e gere uma chave privada:

   ```
   ~ # openssl
   OpenSSL> genrsa -out privatekey.pem 1024
   Generating RSA private key, 1024 bit long modulus
   ..................................++++++
   ................++++++
   e is 65537 (0x10001)
   ```
2. Use esta chave privada para gerar uma CSR (solicitação de assinatura de certificado):

```
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
```

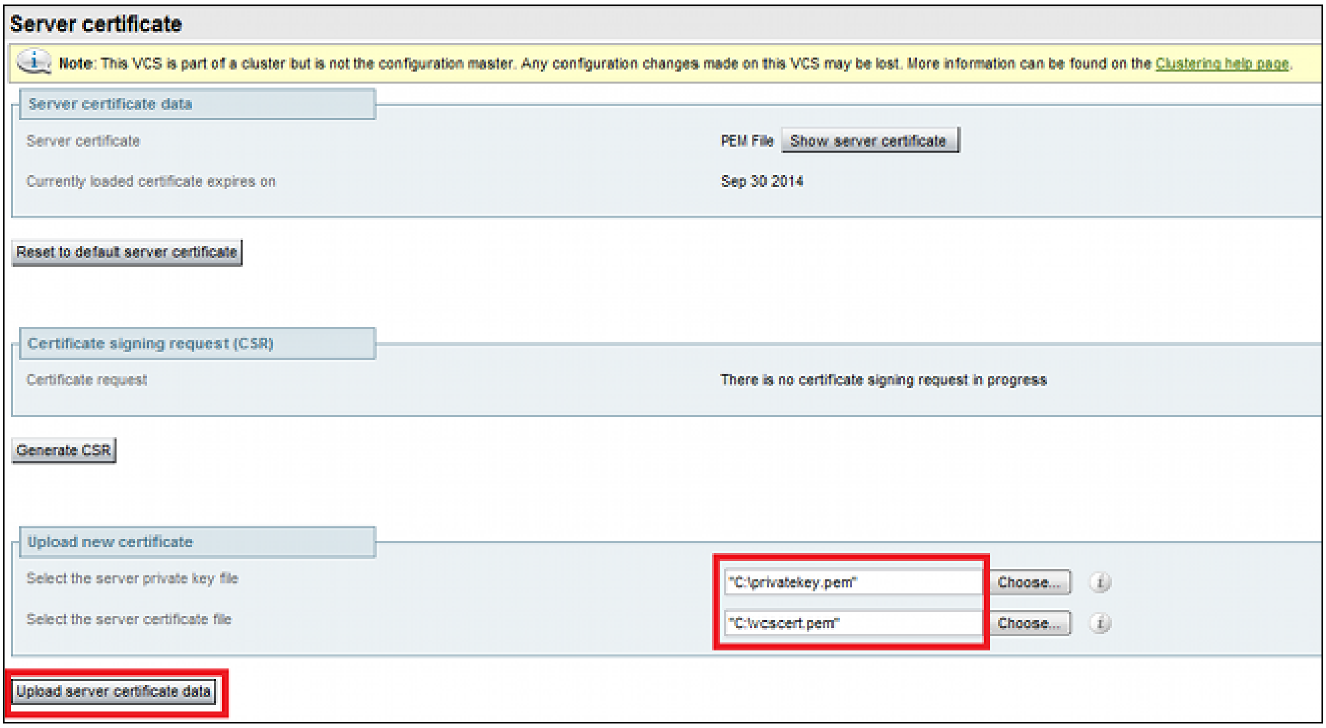
3. Gerar o certificado autoassinado:

```
~ # 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. Confirme se os certificados estão disponíveis:

```
~ # 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. Baixe os certificados com WinSCP e carregue-os na página da Web para que o VCS possa usar os certificados; você precisa da chave privada e do certificado gerado:



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

Certificate signing request (CSR)

Certificate request: There is no certificate signing request in progress

Upload new certificate

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

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

Show server certificate
Reset to default server certificate
Generate CSR
Choose...
Choose...
Upload server certificate data

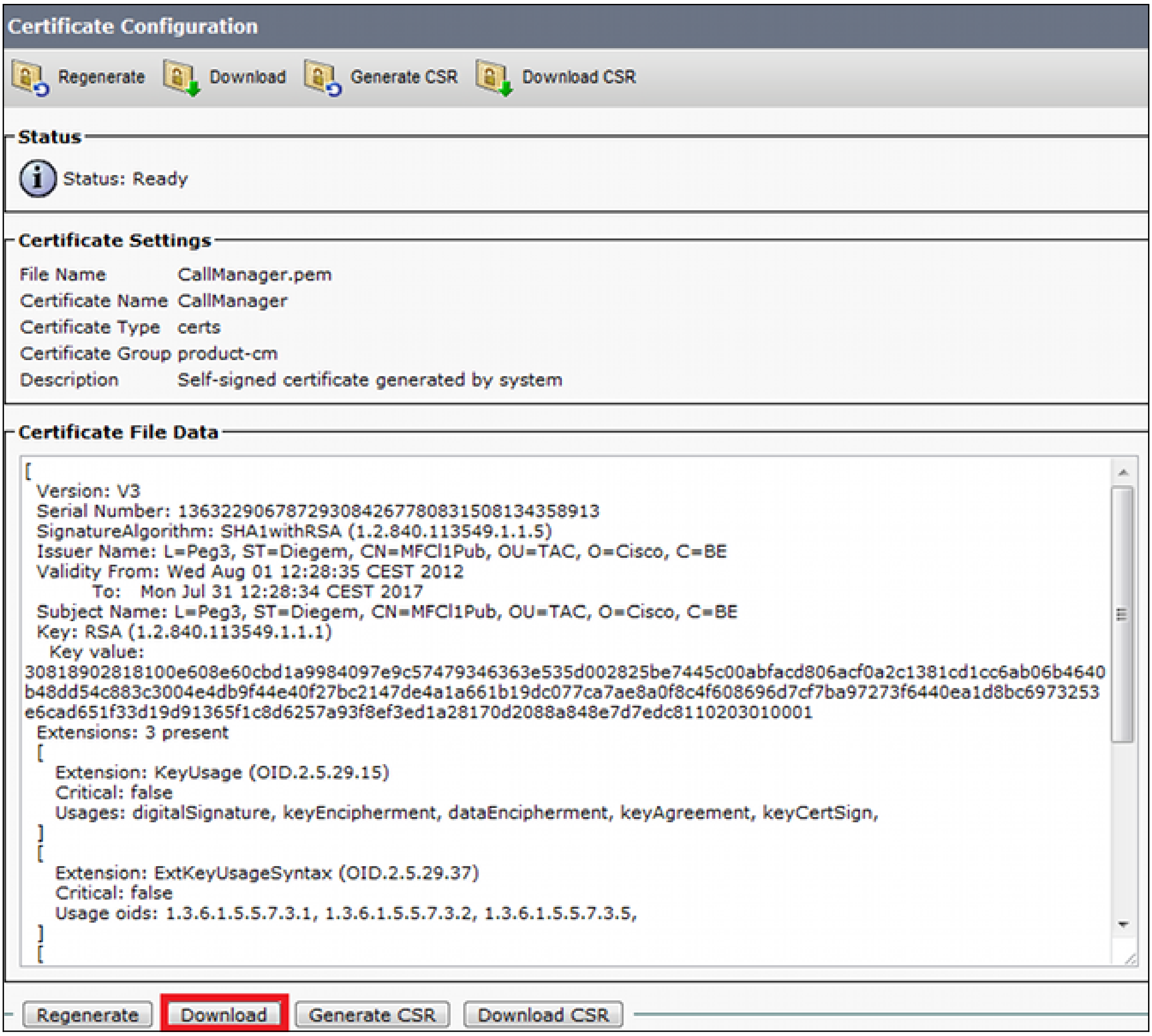
6. Repita esse procedimento para todos os servidores VCS.

Adicionar certificado autoassinado do servidor CUCM para o servidor VCS

Adicione os certificados dos servidores CUCM para que o VCS confie neles. Neste exemplo, você está usando os certificados padrão autoassinados do CUCM; O CUCM gera certificados autoassinados durante a instalação para que você não precise criá-los como fez no VCS.

Este procedimento descreve como adicionar um certificado autoassinado do servidor CUCM ao servidor VCS:

1. Baixe o certificado CallManager.pem do CUCM. Efetue login na página OS Administration, navegue para **Security** > **Certificate Management** e, em seguida, selecione e baixe o certificado autoassinado CallManager.pem:



Status

Status: Ready

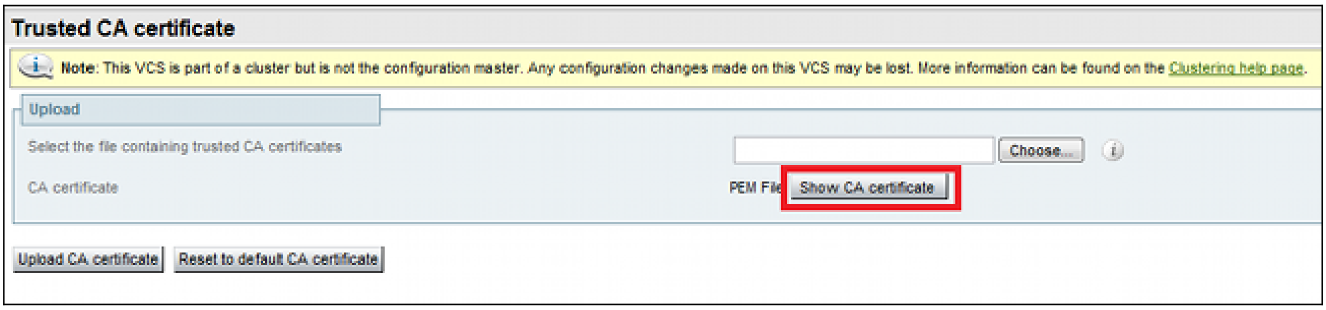
Certificate Settings

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. Adicione este certificado como um certificado de CA confiável no VCS. No VCS, navegue para **Manutenção** > **Gerenciamento de certificado** > **Certificado de CA confiável** e selecione **Mostrar certificado de CA**:



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.

Select the file containing trusted CA certificates

CA certificate PEM File

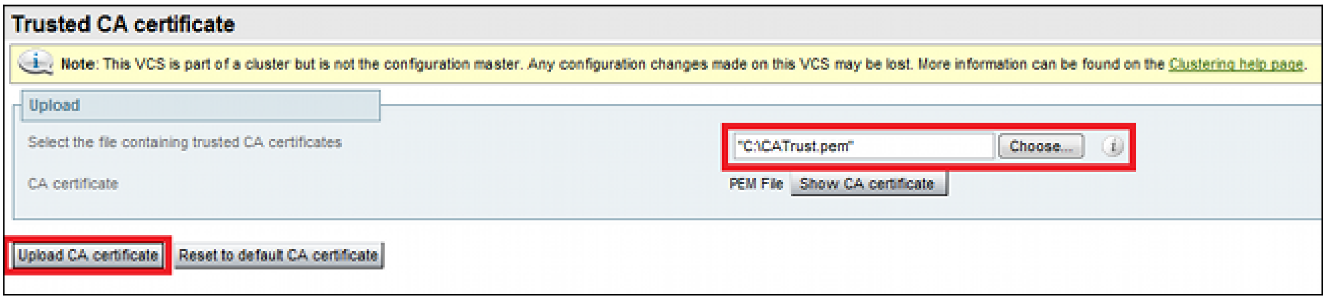
Uma nova janela é aberta com todos os certificados confiáveis no momento.

3. Copiar todos os certificados confiáveis no momento para um arquivo de texto. Abra o arquivo CallManager.pem em um editor de texto, copie seu conteúdo e adicione esse conteúdo à parte inferior do mesmo arquivo de texto após os certificados atualmente confiáveis:

```
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-----
```

Se você tiver vários servidores no cluster CUCM, adicione todos eles aqui.

4. Salve o arquivo como CATrust.pem e clique em **Upload CA certificate** para carregar o arquivo de volta ao 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.

Upload

Select the file containing trusted CA certificates "C:\CATrust.pem"

CA certificate PEM File

O VCS agora confiará nos certificados oferecidos pelo CUCM.

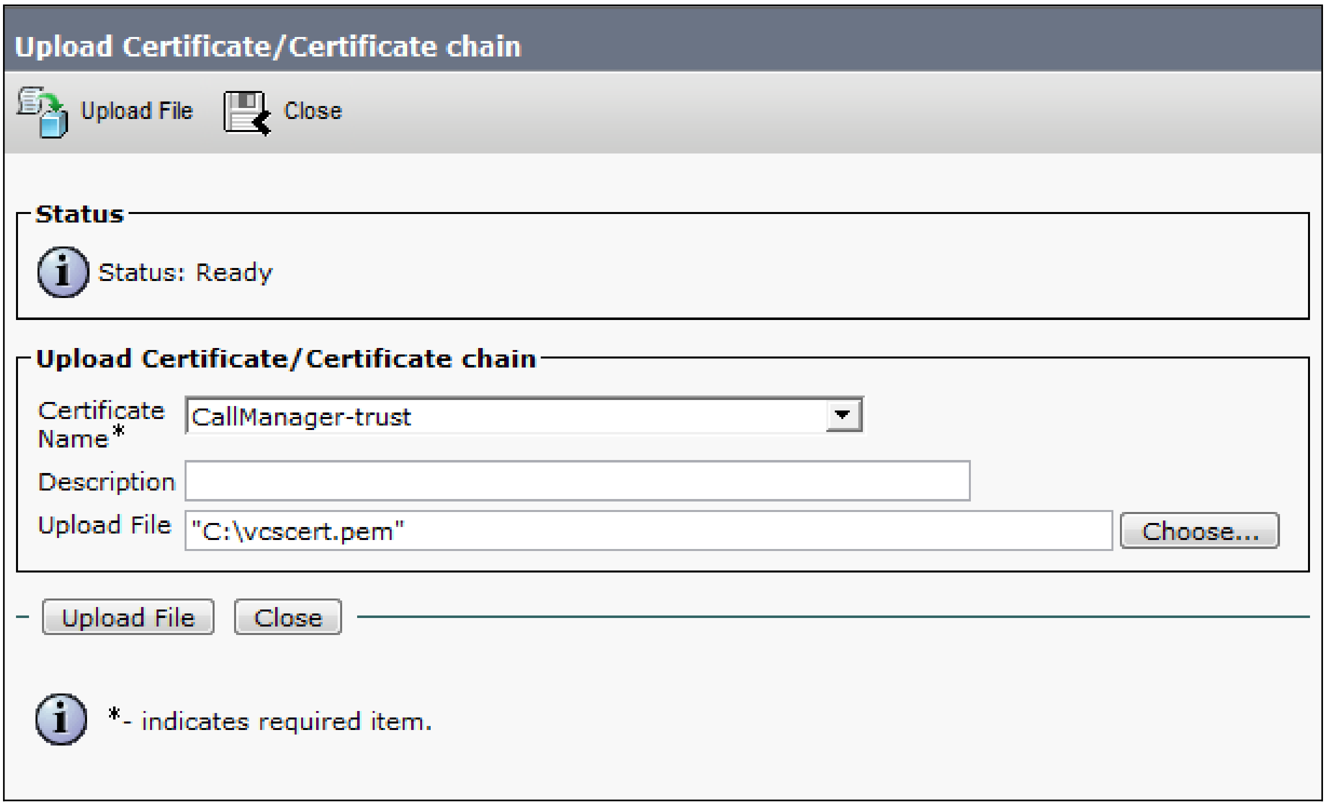
5. Repita esse procedimento para todos os servidores VCS.

Carregar certificado do servidor VCS para o servidor CUCM

O CUCM precisa confiar nos certificados oferecidos pelo VCS.

Este procedimento descreve como carregar o certificado VCS gerado no CUCM como um certificado CallManager-Trust:

1. Na página OS Administration, navegue até **Security** > **Certificate Management**, digite o nome do certificado, navegue até o local e clique em **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.

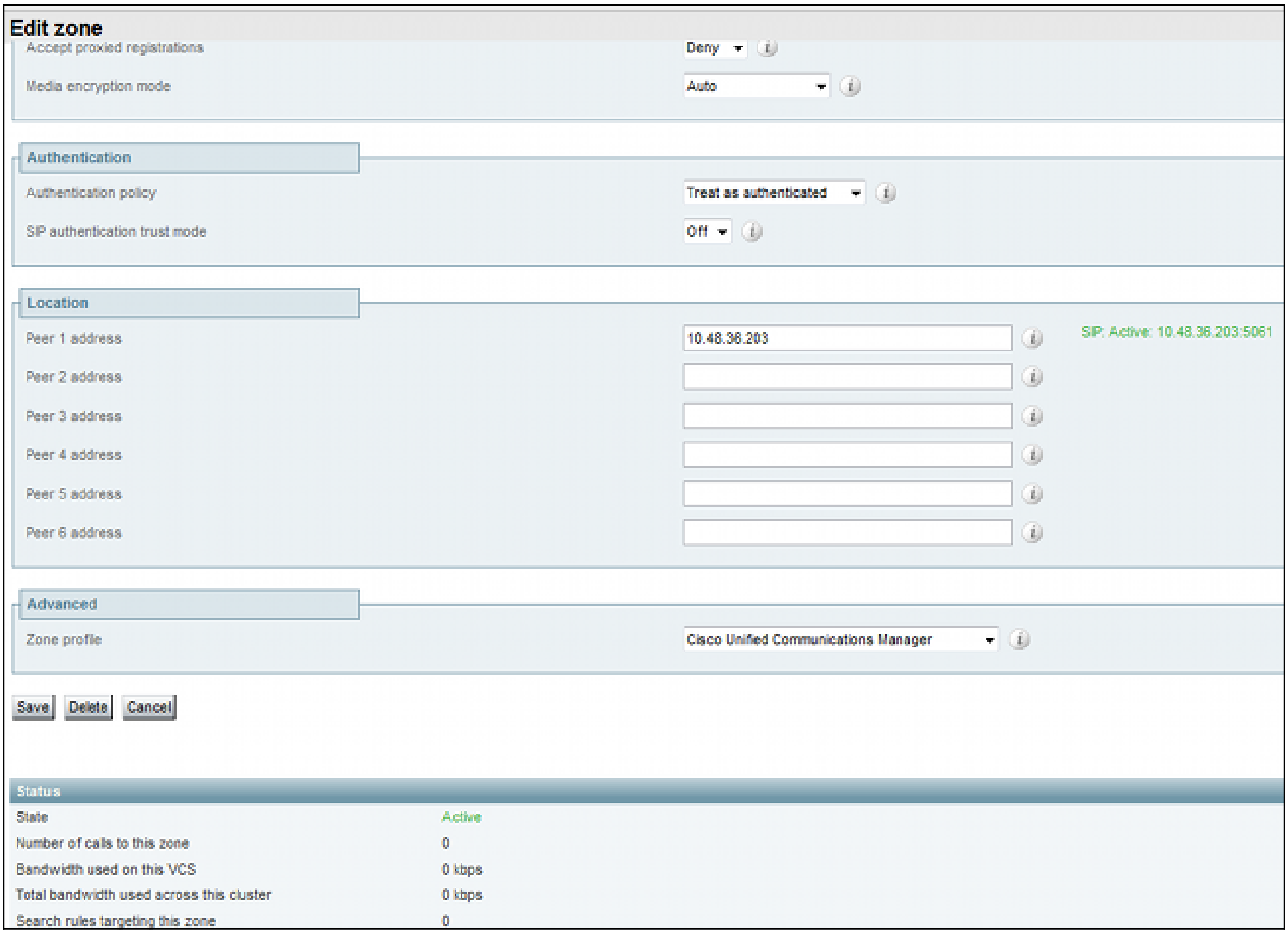
2. Carregue o certificado de todos os servidores VCS. Faça isso em cada servidor CUCM que se comunicará com o VCS; geralmente, são todos os nós que estão executando o serviço CallManager.

Conexão SIP

Depois que os certificados forem validados e ambos os sistemas confiarem um no outro, configure a Zona Vizinha no VCS e o Tronco SIP no CUCM. Consulte o Guia de implantação do Cisco TelePresence Cisco Unified Communications Manager com Cisco VCS (tronco SIP) para obter detalhes desse procedimento.

Verificar

Confirme se a conexão SIP está ativa na zona vizinha no 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

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Guia de implantação do Cisco TelePresence Cisco Unified Communications Manager com Cisco VCS (tronco SIP)
- Guia do administrador do servidor de comunicação por vídeo Cisco TelePresence
- Criação e uso do certificado Cisco TelePresence com o guia de implantação do Cisco VCS
- Manual de administração do sistema operacional do Cisco Unified Communications
- Guia de administração do Cisco Unified Communications Manager
- Suporte Técnico e Documentação - Cisco Systems