CUCM和VCS之间的安全SIP中继配置示例

目录

简介

本文档介绍如何在Cisco Unified Communications Manager(CUCM)和Cisco TelePresence Video Communication Server(VCS)之间建立安全会话初始协议(SIP)连接。

CUCM和VCS紧密集成。由于视频终端可以在CUCM或VCS上注册，设备之间必须存在SIP中继。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco Unified Communications Manager
- 思科网真视频通信服务器
- 证书

使用的组件

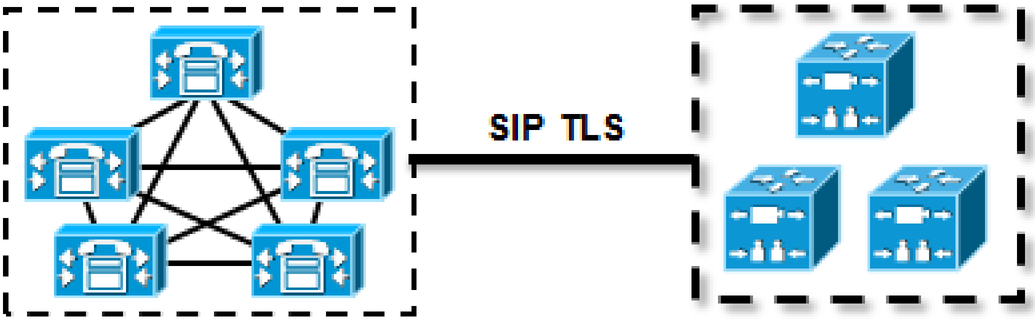
本文档不限于特定的软件和硬件版本。本示例使用Cisco VCS软件版本X7.2.2和CUCM版本9.x。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

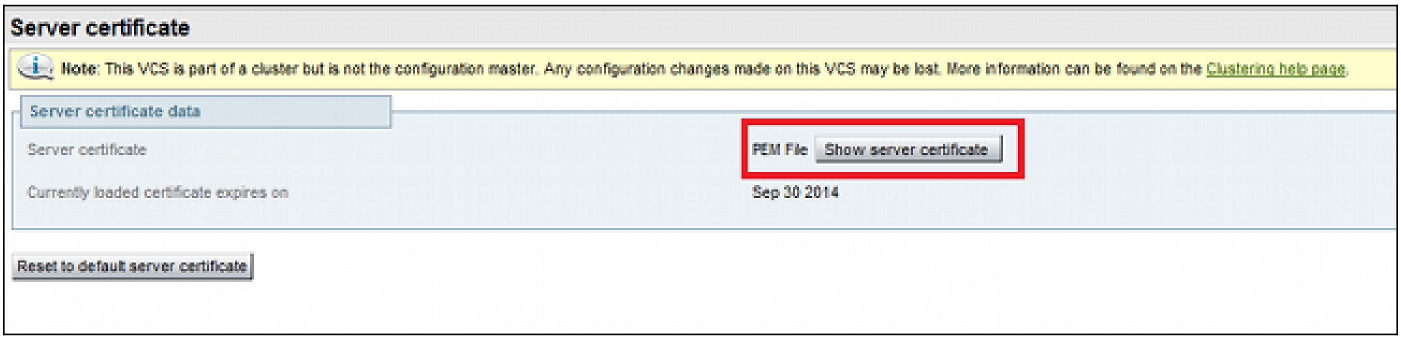
确保证书有效，将证书添加到CUCM和VCS服务器，使它们信任彼此的证书，然后建立SIP中继。

网络图



获取VCS证书

默认情况下，所有VCS系统都带有临时证书。在管理页面上，导航到**维护** > **证书管理** > **服务器证书**。单击**Show server certificate**，将会打开一个新窗口，其中包含证书的原始数据：



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

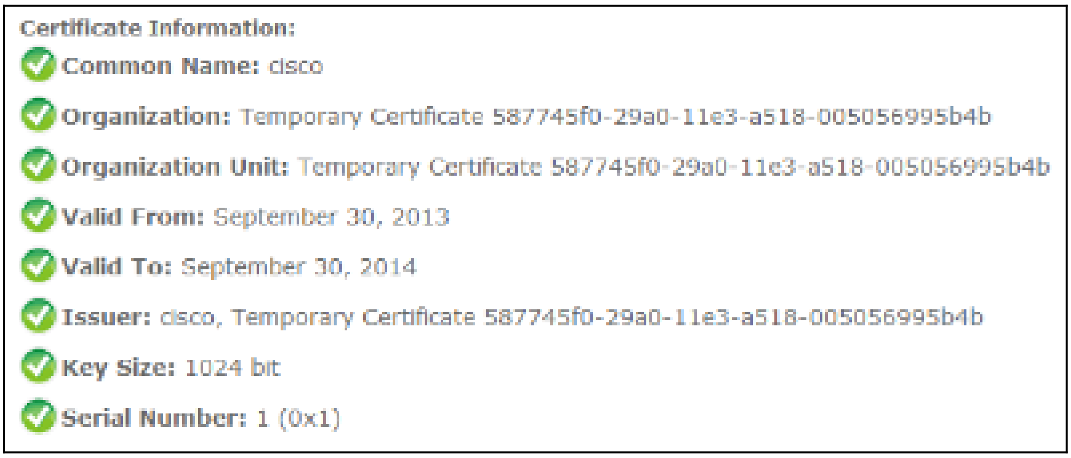
[Reset to default server certificate]

以下是原始证书数据的示例：

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

您可以在本地PC上使用OpenSSL或使用在线证书解码器(例如SSL Shopper)对证书进行解码并查看证书数据:



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)

生成并上传VCS自签名证书

由于每个VCS服务器都有一个具有相同公用名称的证书，因此您需要将新证书放在服务器上。您可以选择使用自签名证书或由证书颁发机构(CA)签名的证书。 有关此过程的详细信息，请参阅Cisco TelePresence Certificate Creation and Use with Cisco VCS Deployment Guide。

此过程介绍如何使用VCS本身生成自签名证书，然后上传该证书：

1. 以root用户身份登录到VCS，启动OpenSSL并生成私钥：

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

2. 使用此私钥生成证书签名请求(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
```

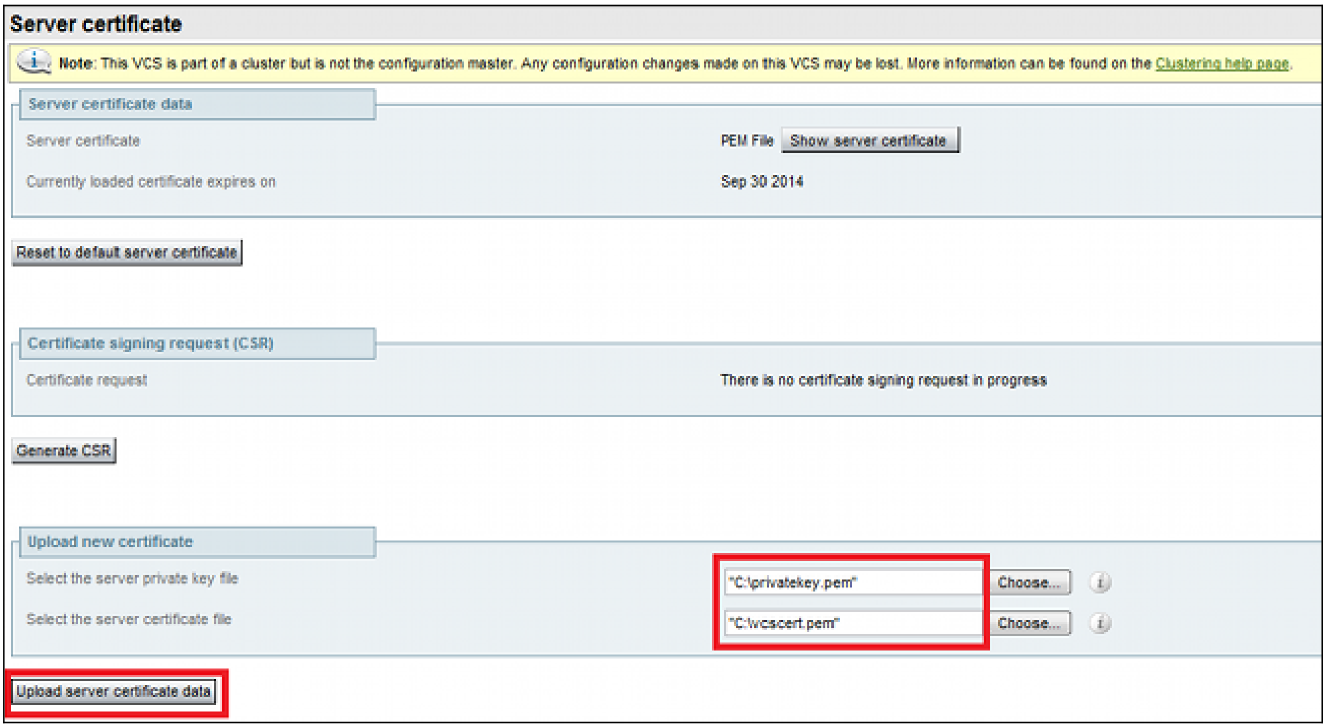
3. 生成自签名证书：

```
~ # 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. 确认证书现在可用：

```
~ # 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. 使用WinSCP下载证书，并将证书上传到网页上，以便VCS可以使用证书；您需要私钥和生成的证书：



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

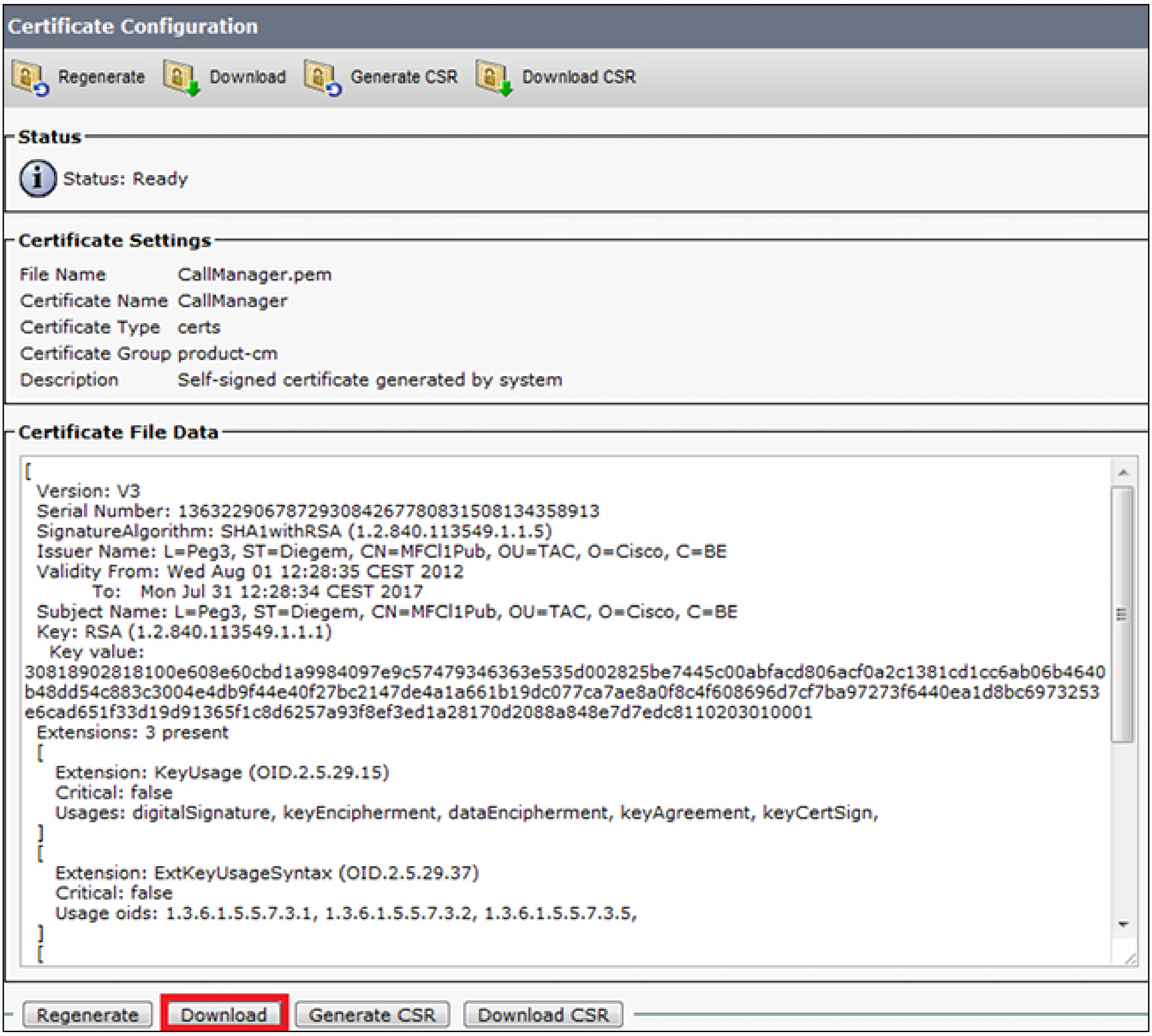
6. 对所有VCS服务器重复此过程。

将自签名证书从CUCM服务器添加到VCS服务器

添加来自CUCM服务器的证书，以便VCS信任它们。在本示例中，您使用的是来自CUCM的标准自签名证书；CUCM会在安装期间生成自签名证书，因此您无需像在VCS上那样创建这些证书。

此过程介绍如何从CUCM服务器向VCS服务器添加自签名证书：

1. 从CUCM下载CallManager.pem证书。登录到OS Administration页面，导航到**Security** > **Certificate Management**，然后选择并下载自签名CallManager.pem证书：



Certificate Configuration

Status

Status: Ready

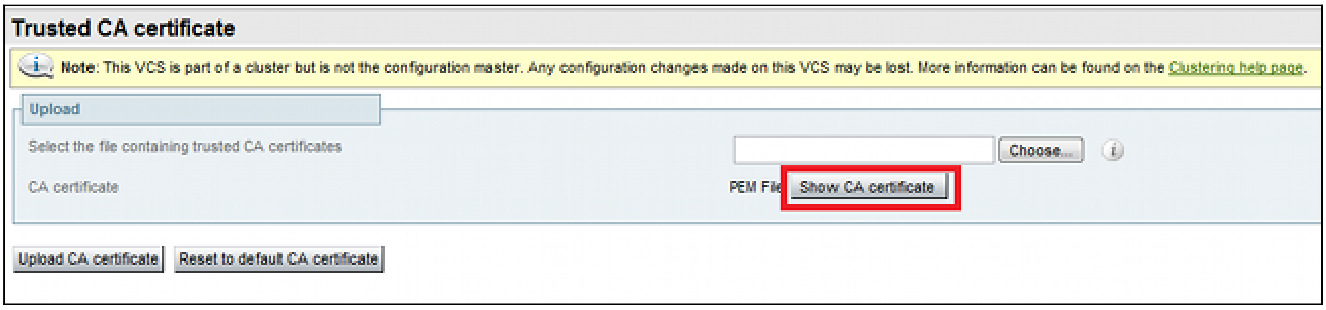
Certificate Settings

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. 将此证书添加为VCS上的受信任CA证书。在VCS上，导航到**维护** > **证书管理** > **受信任CA证书**，然后选择**显示CA证书**:



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

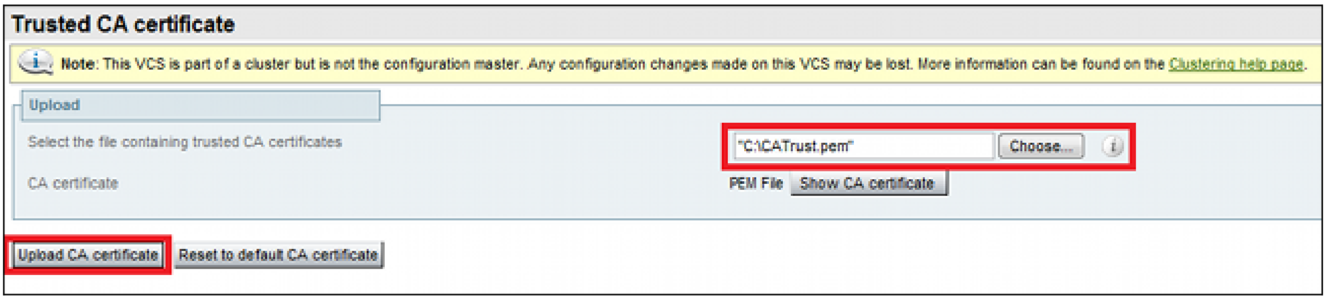
系统打开一个新窗口，显示当前信任的所有证书。

3. 将当前受信任的所有证书复制到文本文件。在文本编辑器中打开CallManager.pem文件，复制其内容，然后将该内容添加到当前受信任证书后的同一文本文件的底部：

```
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-----
```

如果CUCM集群中有多个服务器，请在此处添加所有服务器。

4. 将文件另存为CATrust.pem，然后单击**Upload CA certificate**将文件上传回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" Choose...

CA certificate: PEM File Show CA certificate

VCS现在将信任CUCM提供的证书。

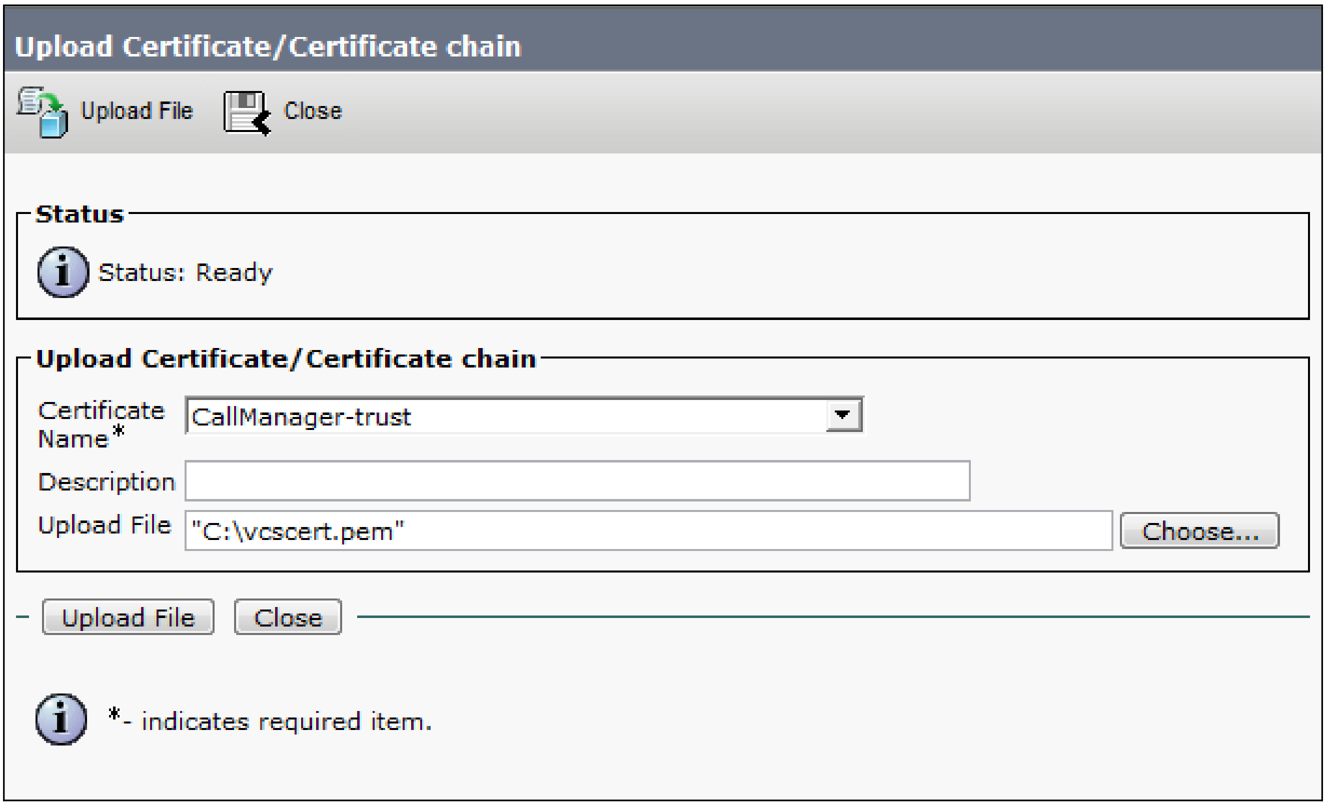
5. 对所有VCS服务器重复此过程。

将证书从VCS服务器上传到CUCM服务器

CUCM需要信任VCS提供的证书。

此过程介绍如何上传在CUCM上生成的VCS证书作为CallManager-Trust证书：

1. 在OS Administration页面上，导航到**Security** > **Certificate Management**，输入证书名称，浏览到其位置，然后点击**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.

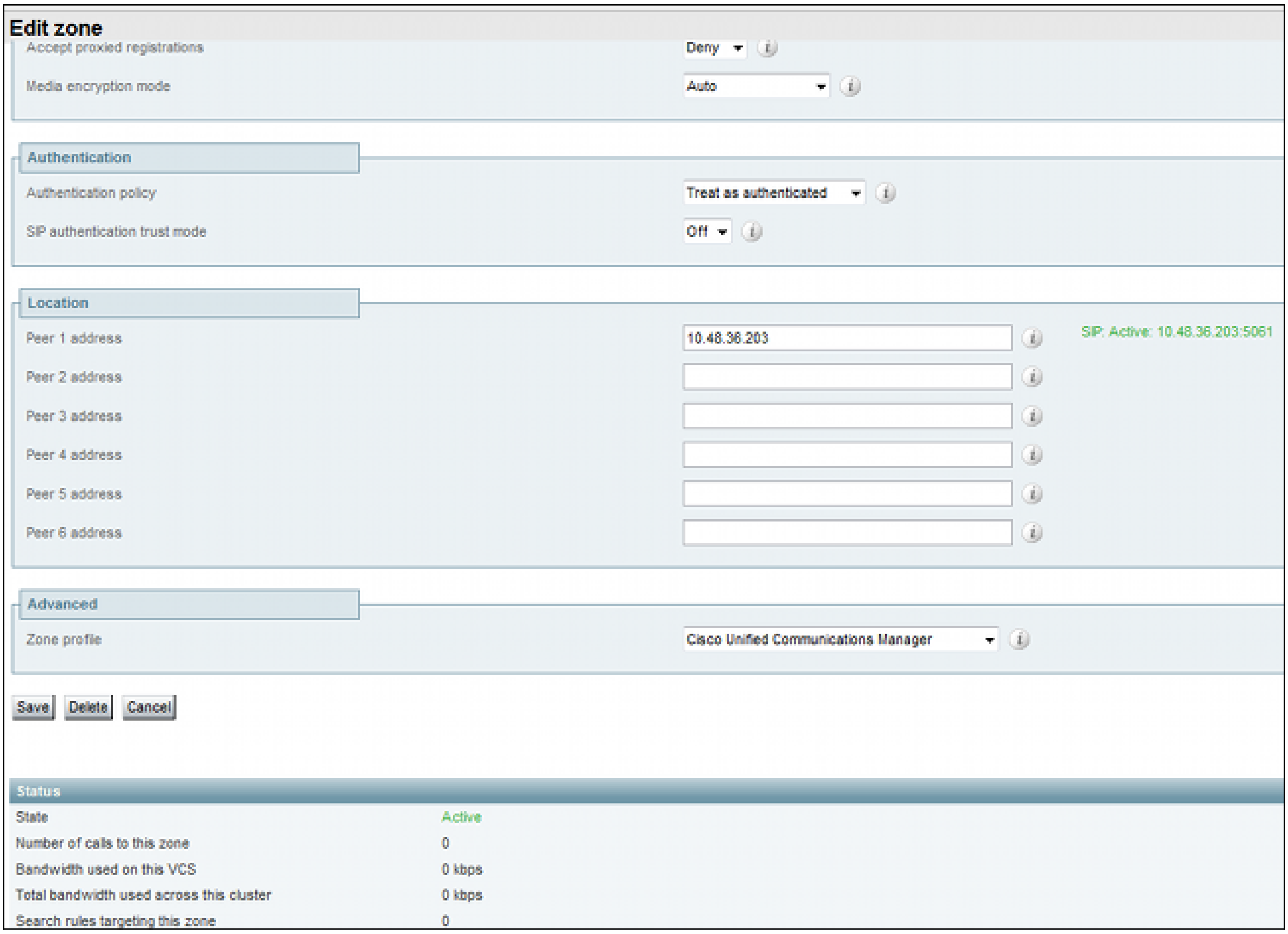
2. 从所有VCS服务器上传证书。在将要与VCS通信的每个CUCM服务器上执行此操作；这通常是运行CallManager服务的所有节点。

SIP连接

验证证书且两个系统相互信任后，在VCS上配置邻居区域并在CUCM上配置SIP中继。有关此过程的详细信息，请参阅Cisco TelePresence Cisco Unified Communications Manager with Cisco VCS（SIP中继）部署指南。

验证

确认SIP连接在VCS的邻居区域中处于活动状态：



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

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- Cisco TelePresence Cisco Unified Communications Manager with Cisco VCS（SIP中继）部署指南
- 思科网真视频通信服务器管理员指南
- Cisco TelePresence Certificate Creation and Use with Cisco VCS部署指南
- 思科统一通信操作系统管理指南
- Cisco Unified Communications Manager管理指南
- 技术支持和文档 - Cisco Systems