Secure SIP Trunk tussen CUCM en VCS-configuratievoorbeeld

Inhoud

Inleiding

Dit document beschrijft hoe u een beveiligde Session Initiation Protocol (SIP)-verbinding kunt instellen tussen Cisco Unified Communications Manager (CUCM) en Cisco TelePresence Video Communication Server (VCS).

CUCM en VCS zijn nauw geïntegreerd. Omdat video-eindpunten op CUCM of VCS kunnen worden geregistreerd, moeten er tussen de apparaten SIP-trunks bestaan.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Unified Communications Manager
- Cisco TelePresence Video Communication Server-modules
- Certificaten

Gebruikte componenten

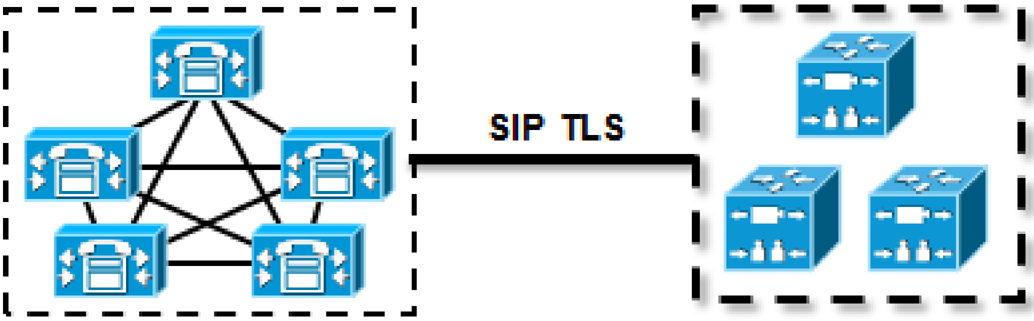
Dit document is niet beperkt tot specifieke software- en hardware-versies. Dit voorbeeld gebruikt Cisco VCS-softwareversie X7.2.2 en CUCM versie 9.x.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Configureren

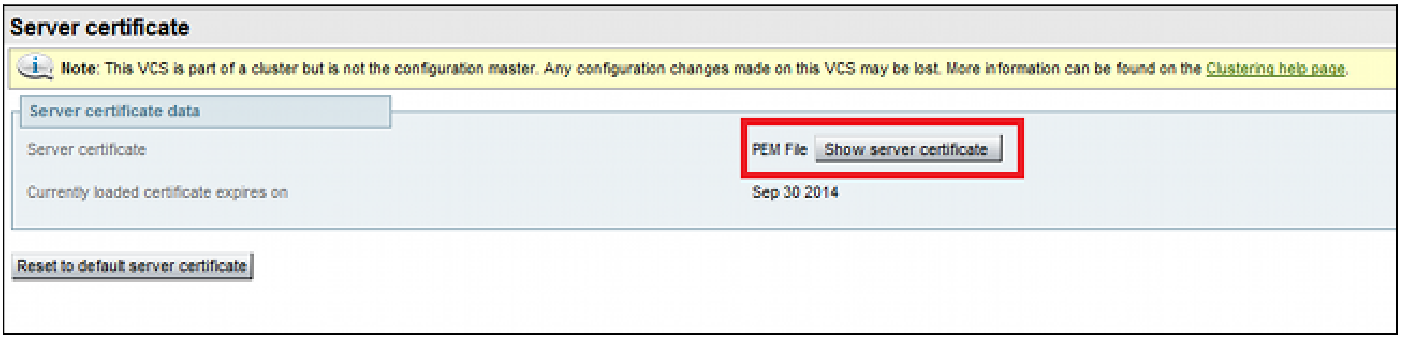
Zorg ervoor dat de certificaten geldig zijn, voeg de certificaten aan de CUCM- en VCS-servers toe zodat zij elkaars certificaten vertrouwen en stel vervolgens de SIP-stam in.

Netwerkdiagram



VCS-certificaat verkrijgen

Standaard worden alle VCS-systemen voorzien van een tijdelijk certificaat. Ga op de admin pagina naar **Onderhoud** > **certificaatbeheer** > **servercertificaat**. Klik op **servercertificaat tonen** en er wordt een nieuw venster geopend met de ruwe gegevens van het certificaat:


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

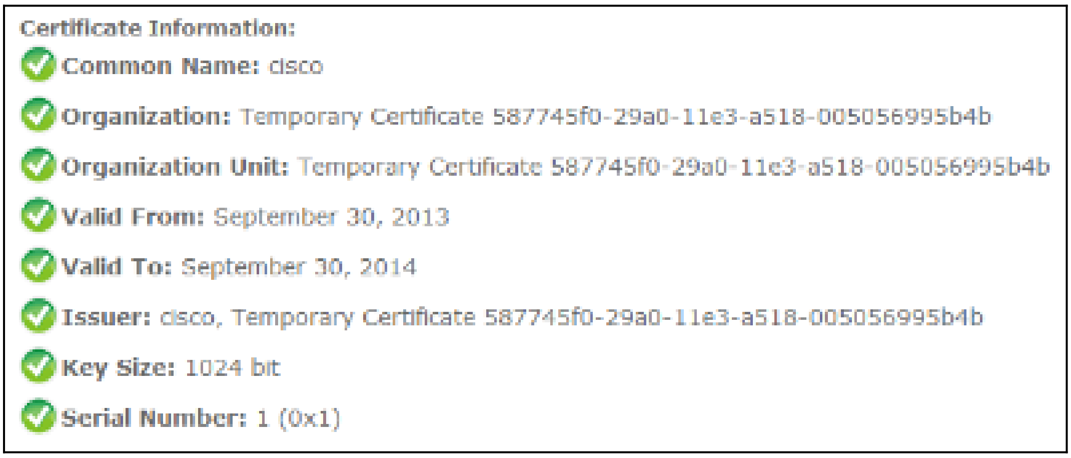
Currently loaded certificate expires on: Sep 30 2014

Dit is een voorbeeld van de gegevens van het ruwe certificaat:

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

U kunt het certificaat decoderen en de certificaatgegevens bekijken door het gebruik van OpenSSL op uw lokale pc of door het gebruik van een online certificeringsdecoder zoals 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)

VCS-zelfondertekend certificaat genereren en uploaden

Omdat elke VCS-server een certificaat met dezelfde gemeenschappelijke naam heeft, moet u nieuwe certificaten op de server plaatsen. U kunt ervoor kiezen zelfgetekende certificaten of certificaten te gebruiken die zijn ondertekend door de certificaatinstantie (CA). Zie de Cisco TelePresence-certificaatcreatie en het gebruik met Cisco VCS-implementatiegids voor meer informatie over deze procedure.

In deze procedure wordt beschreven hoe u de VCS zelf kunt gebruiken om een zelf-ondertekend certificaat te genereren en vervolgens het certificaat te uploaden:

1. Log in als wortel aan VCS, start OpenSSL en genereer een privésleutel:

   ```
   ~ # openssl
   OpenSSL> genrsa -out privatekey.pem 1024
   Generating RSA private key, 1024 bit long modulus
   ..................................++++++
   ................++++++
   e is 65537 (0x10001)
   ```
2. Gebruik deze privé-toets om een certificaatgebarende aanvraag (CSR) te genereren:

```
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
```

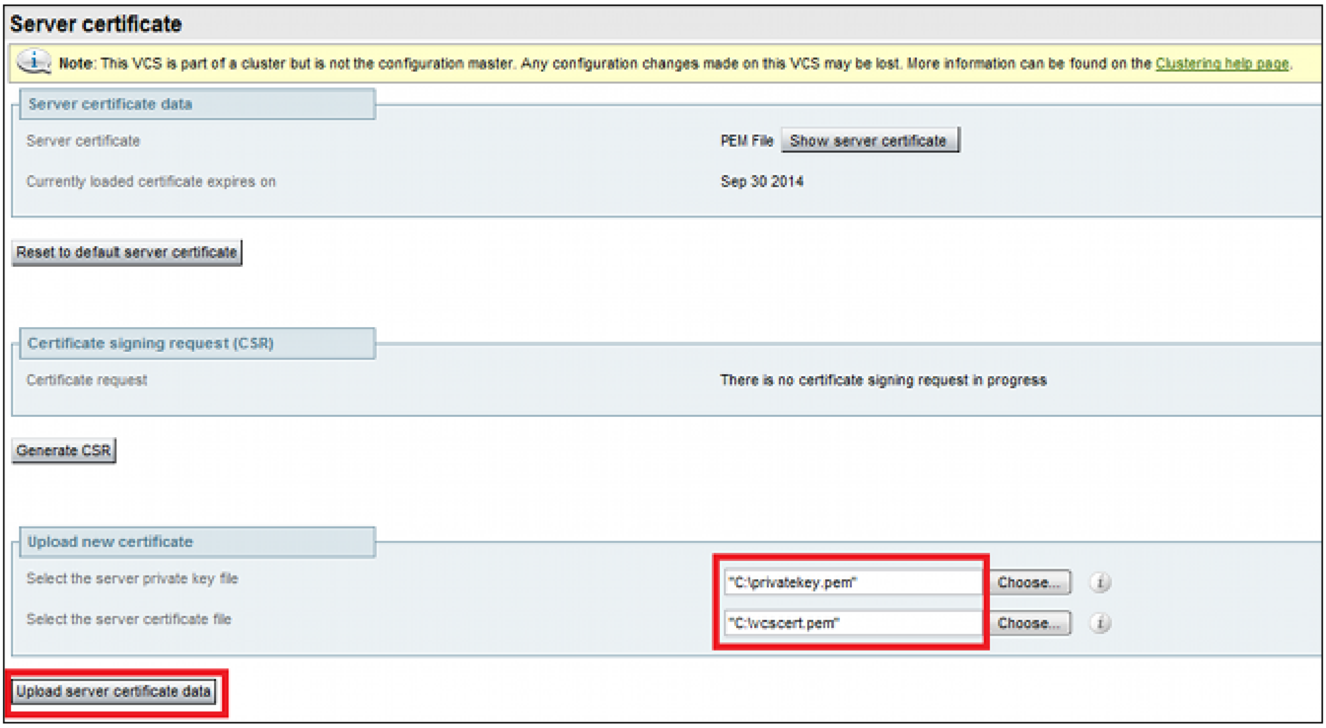
3. Het zelf-ondertekende certificaat genereren:

```
~ # 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. Bevestig dat de certificaten nu beschikbaar zijn:

```
~ # 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. De certificaten met WinSCP downloaden en op de webpagina uploaden, zodat de VCS de certificaten kan gebruiken; u hebt zowel de privétoets als het gegenereerde certificaat nodig:



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

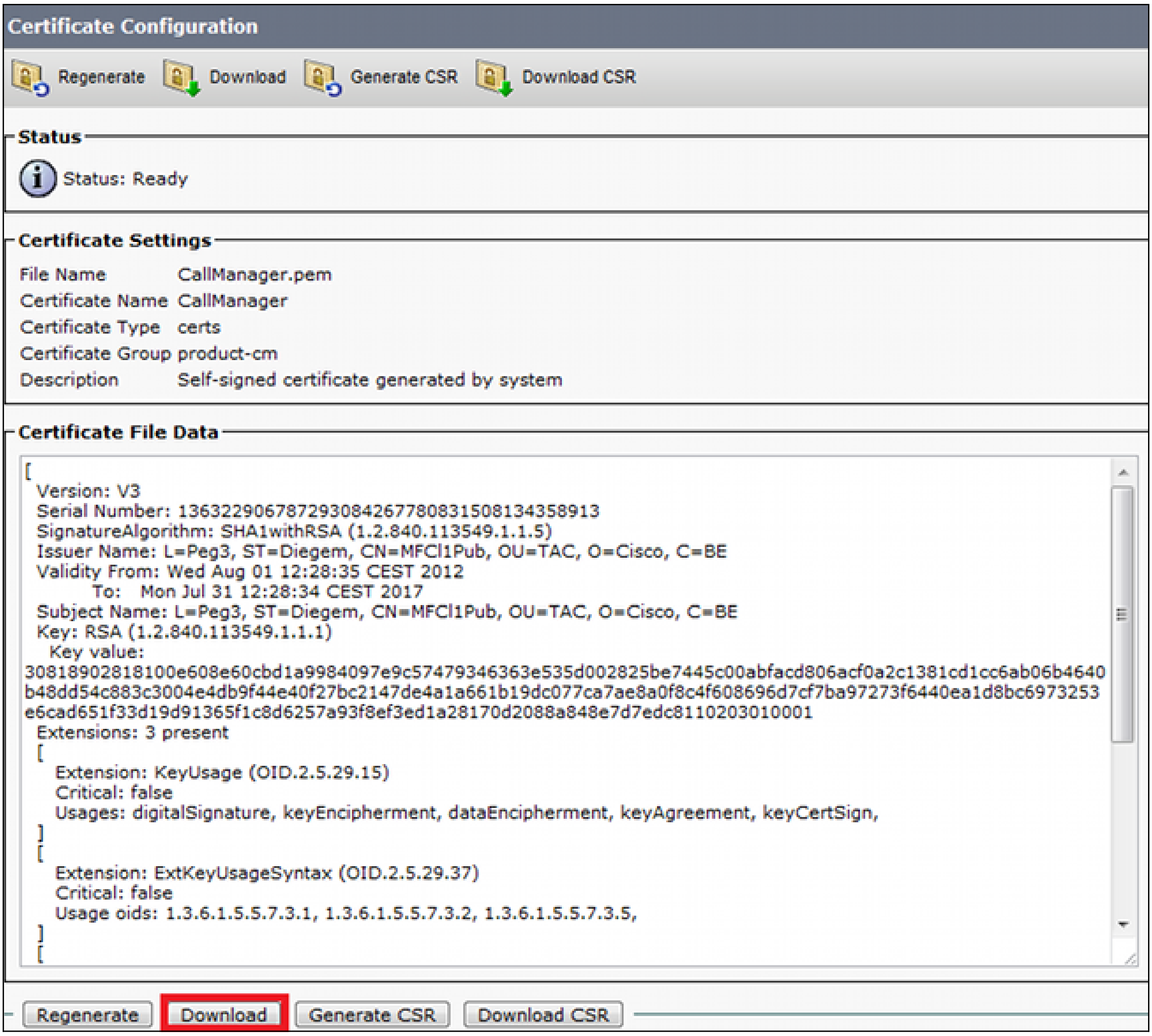
6. Herhaal deze procedure voor alle VCS-servers.

Toevoegen zelfondertekend certificaat van CUCM Server aan VCS Server

Voeg de certificaten toe van de CUCM-servers zodat de VCS ze zal vertrouwen. In dit voorbeeld gebruikt u de standaard zelfondertekende certificaten van CUCM; CUCM genereert zelfondertekende certificaten tijdens de installatie zodat u deze niet hoeft te maken zoals u op de VCS hebt gedaan.

In deze procedure wordt beschreven hoe een zichzelf ondertekend certificaat van de CUCM-server aan de VCS-server moet worden toegevoegd:

1. Download het CallManager.pem certificaat van CUCM. Log in op de pagina OS-beheer, navigeer naar **security** > **certificaatbeheer** en selecteer vervolgens het zelf-getekende CallManager.pem-certificaat:



Status

Status: Ready

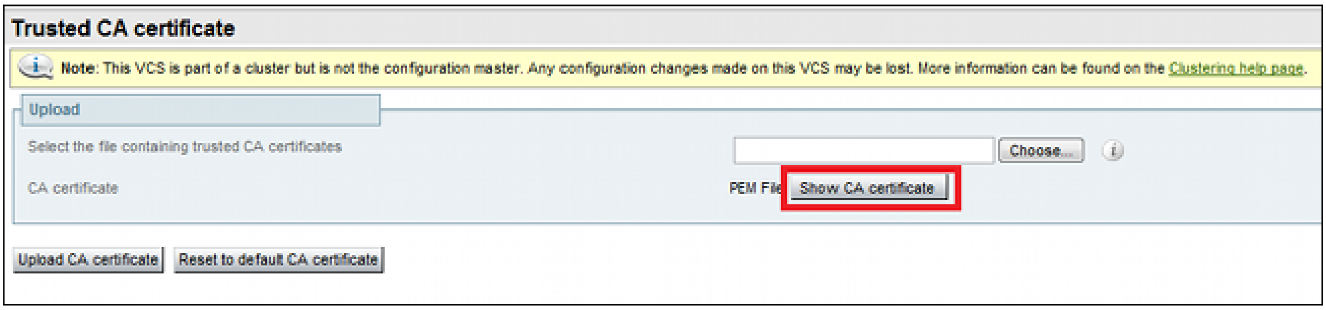
Certificate Settings

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. Voeg dit certificaat toe als een betrouwbaar CA-certificaat op de VCS.Ga op de VCS naar **Onderhoud** > **certificaatbeheer** > **Trusted CA-certificaat** en selecteer **CA-certificaat tonen**:



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
Choose...
CA certificate
PEM File
Show CA certificate
Upload CA certificate
Reset to default CA certificate

Een nieuw venster wordt geopend met alle certificaten die op dit moment worden vertrouwd.

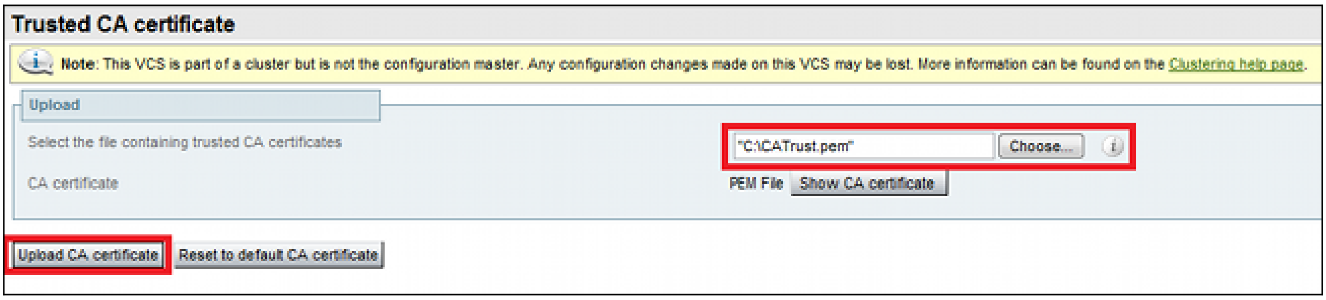
3. Kopieer alle momenteel vertrouwde certificaten naar een tekstbestand. Open het bestand CallManager.pem in een teksteditor, kopieer de inhoud ervan en voeg die inhoud toe aan de onderkant van hetzelfde tekstbestand na de momenteel vertrouwde certificaten:

```
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-----
```

Als u meerdere servers in de CUCM-cluster hebt, kunt u deze allemaal hier toevoegen.

4. Sla het bestand op als CATroest.pem en klik op **CA-certificaat uploaden** om het bestand terug te uploaden naar de 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

Upload CA certificate | Reset to default CA certificate

De VCS zal nu de door CUCM aangeboden certificaten vertrouwen.

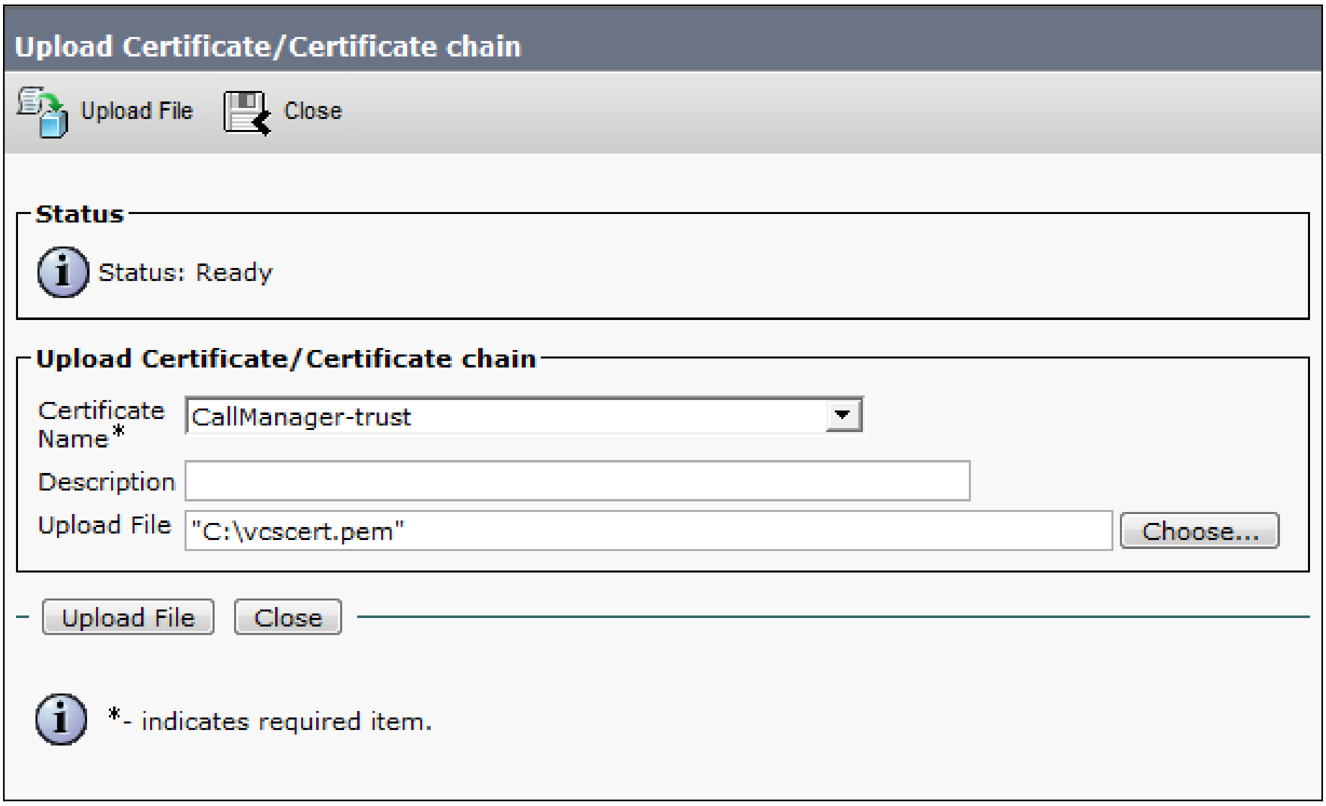
5. Herhaal deze procedure voor alle VCS-servers.

Uploadcertificaat van VCS-server naar CUCM-server

Het CUCM moet vertrouwen hebben in de door de VCS aangeboden certificaten.

In deze procedure wordt beschreven hoe u het VCS-certificaat dat u op CUCM hebt gegenereerd, kunt uploaden als een CallManager-Trust-certificaat:

1. Ga in de pagina OS-beheer naar **Security** > **certificaatbeheer**, voer de certificaatnaam in, blader naar de locatie en klik op **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.

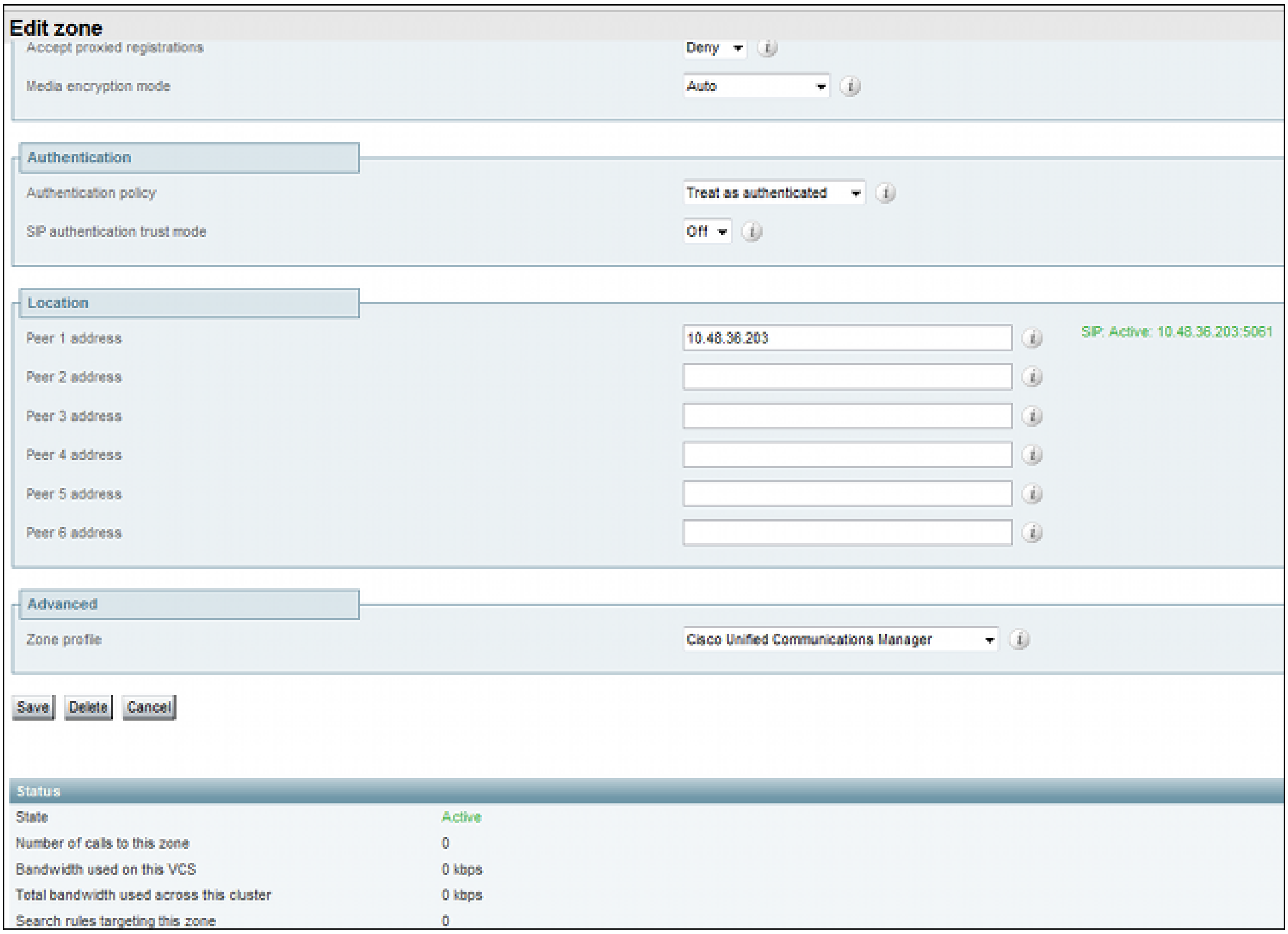
2. Upload het certificaat vanaf alle VCS-servers. Doe dit op elke CUCM-server die met de VCS zal communiceren; Dit zijn doorgaans alle knooppunten die de CallManager Service uitvoeren.

SIP-verbinding

Zodra de certificaten worden gevalideerd en beide systemen elkaar vertrouwen, moet u de buurzone op VCS en de SIP Trunk op CUCM configureren. Zie de Cisco TelePresence Cisco Unified Communications Manager met Cisco VCS (SIP Trunk)-implementatiegids voor meer informatie over deze procedure.

Verifiëren

Bevestig dat de SIP-verbinding actief is in de buurzone op 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

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

- Cisco TelePresence Cisco Unified Communications Manager met Cisco VCS (SIP Trunk)-implementatiegids
- Cisco TelePresence Video Communication Server-beheerdershandleiding
- Cisco TelePresence-certificeringsgids voor maken en gebruiken met Cisco VCS-implementatiegids
- Cisco Unified Communications besturingssysteembeheerdershandleiding
- Cisco Unified Communications Manager-beheerdershandleiding
- Technische ondersteuning en documentatie – Cisco Systems