Ejemplo de configuración de enlace troncal SIP seguro entre CUCM y VCS

Contenido

[Introducción](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Configurar](#)
[Diagrama de la red](#)
[Obtener certificado de VCS](#)
[Generar y cargar certificado autofirmado de VCS](#)
[Agregar certificado autofirmado del servidor CUCM al servidor VCS](#)
[Cargar certificado del servidor VCS al servidor CUCM](#)
[Conexión SIP](#)
[Verificación](#)
[Troubleshoot](#)
[Información Relacionada](#)

Introducción

Este documento describe cómo configurar una conexión segura de protocolo de inicio de sesión (SIP) entre Cisco Unified Communications Manager (CUCM) y Cisco TelePresence Video Communication Server (VCS).

CUCM y VCS están estrechamente integrados. Como los terminales de vídeo se pueden registrar en CUCM o VCS, deben existir enlaces troncales SIP entre los dispositivos.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

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

Componentes Utilizados

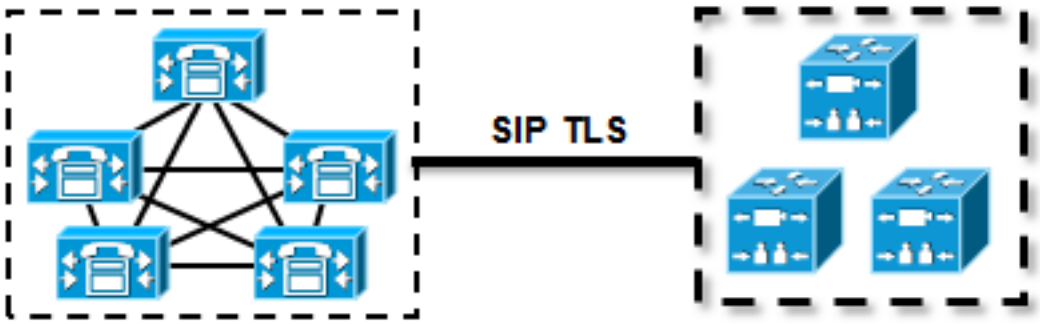
Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware. Este ejemplo utiliza la versión X7.2.2 del software Cisco VCS y la versión 9.x de CUCM.

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

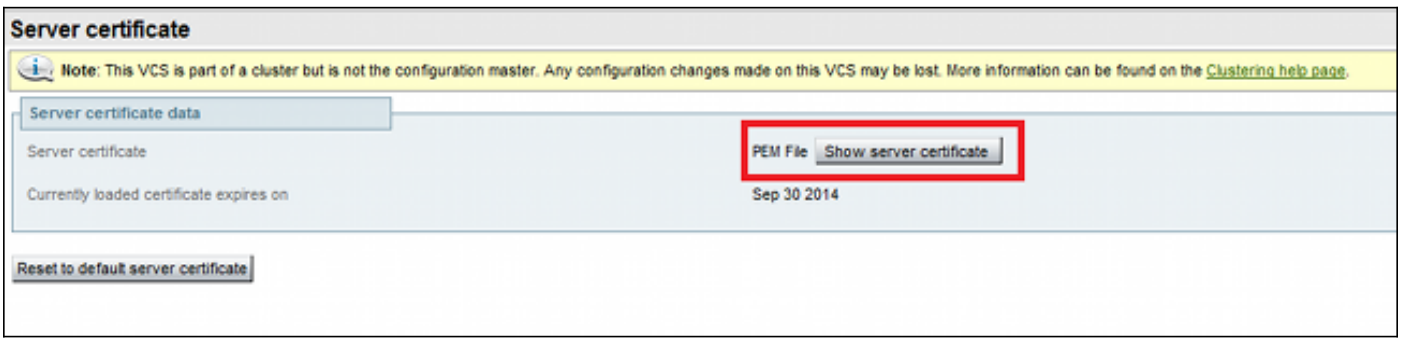
Asegúrese de que los certificados son válidos, agregue los certificados a los servidores CUCM y VCS para que confíen en los certificados de los demás y, a continuación, establezca el troncal SIP.

Diagrama de la red



Obtener certificado de VCS

De forma predeterminada, todos los sistemas VCS incluyen un certificado temporal. En la página de administración, navegue hasta **Mantenimiento > Administración de certificados > Certificado de servidor**. Haga clic en **Show server certificate**, y se abrirá una nueva ventana con los datos sin procesar del certificado:



Este es un ejemplo de los datos del certificado sin procesar:

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

Puede decodificar el certificado y ver los datos del certificado mediante el uso de OpenSSL en su equipo local o el uso de un decodificador de certificados en línea como SSL Shopper :

Generar y cargar certificado autofirmado de VCS

Dado que cada servidor VCS tiene un certificado con el mismo nombre común, debe colocar certificados nuevos en el servidor. Puede optar por utilizar certificados autofirmados o certificados firmados por la Autoridad de certificación (CA). Consulte la Guía de creación y uso de certificados de Cisco TelePresence con Cisco VCS Deployment Guide para obtener detalles sobre este procedimiento.

Este procedimiento describe cómo utilizar el propio VCS para generar un certificado autofirmado y, a continuación, cargarlo:

1. Inicie sesión como root en el VCS, inicie OpenSSL y genere una clave privada:

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

2. Utilice esta clave privada para generar una solicitud de firma de certificado (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
```

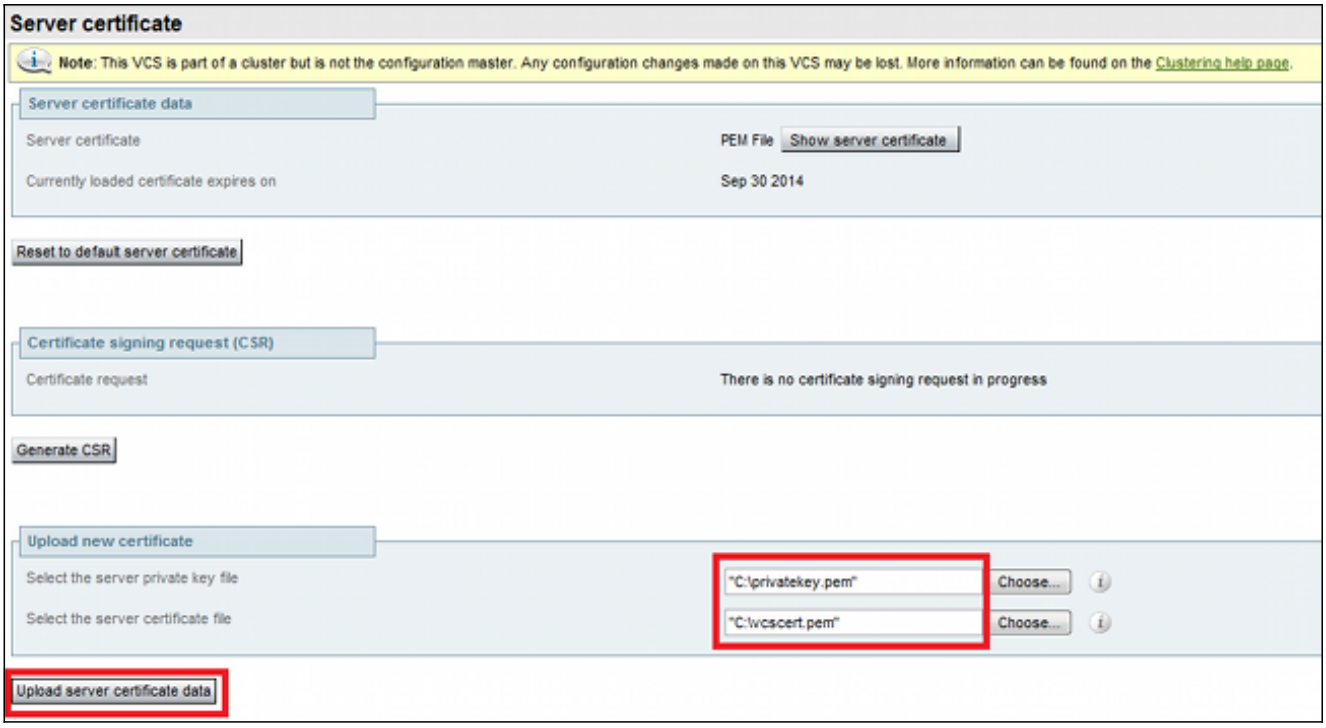
3. Genere el certificado autofirmado:

```
~ # 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 que los certificados ya están disponibles:

```
~ # 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. Descargue los certificados con WinSCP y cárguelos en la página web para que el VCS pueda utilizar los certificados; necesita la clave privada y el certificado generado:



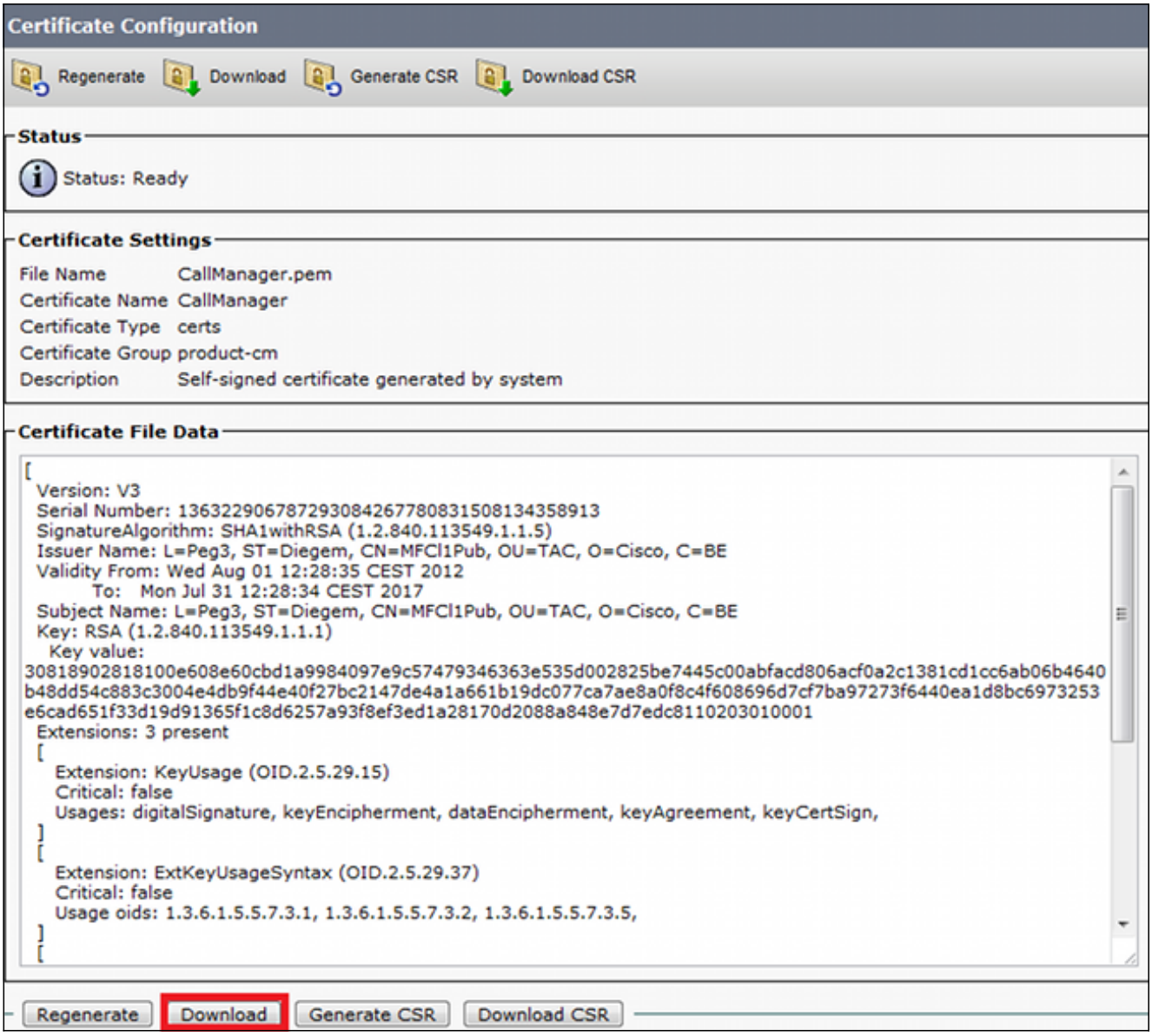
6. Repita este procedimiento para todos los servidores VCS.

Agregar certificado autofirmado del servidor CUCM al servidor VCS

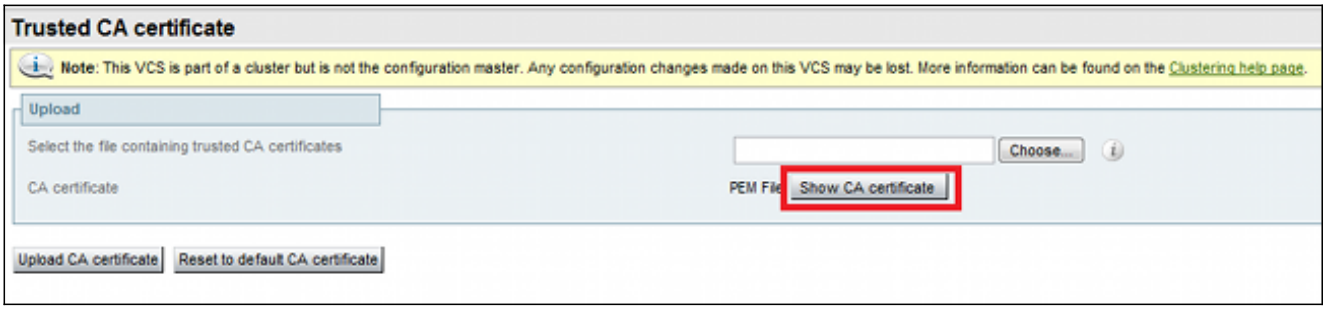
Agregue los certificados de los servidores de CUCM para que VCS confíe en ellos. En este ejemplo, está utilizando los certificados autofirmados estándar de CUCM; CUCM genera certificados autofirmados durante la instalación, por lo que no es necesario crearlos tal y como hizo en el VCS.

Este procedimiento describe cómo agregar un certificado autofirmado del servidor de CUCM al servidor VCS:

1. Descargue el certificado CallManager.pem de CUCM. Inicie sesión en la página Administración del sistema operativo, navegue hasta **Seguridad > Administración de certificados**, luego seleccione y descargue el certificado autofirmado CallManager.pem:



2. Agregue este certificado como certificado de CA de confianza en el VCS.En el VCS, navegue hasta **Mantenimiento > Administración de certificados > Certificado de CA de confianza** y seleccione **Mostrar certificado de CA**:



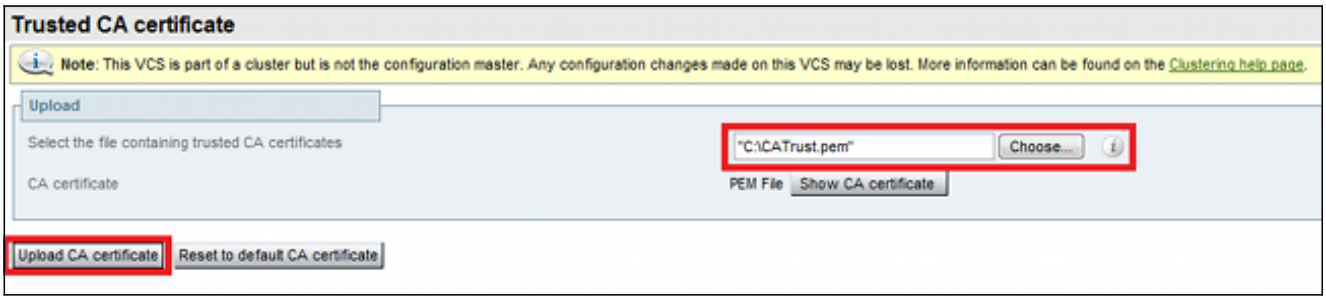
Se abre una nueva ventana con todos los certificados actualmente fiables.

3. Copie todos los certificados actualmente fiables en un archivo de texto. Abra el archivo CallManager.pem en un editor de texto, copie su contenido y agréguelo al final del mismo archivo de texto después de los certificados actualmente confiables:

```
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-----
```

Si tiene varios servidores en el clúster de CUCM, agréguelos todos aquí.

4. Guarde el archivo como CATrust.pem y haga clic en **Cargar certificado de CA** para cargar el archivo nuevamente en el VCS:



VCS confiará ahora en los certificados ofrecidos por CUCM.

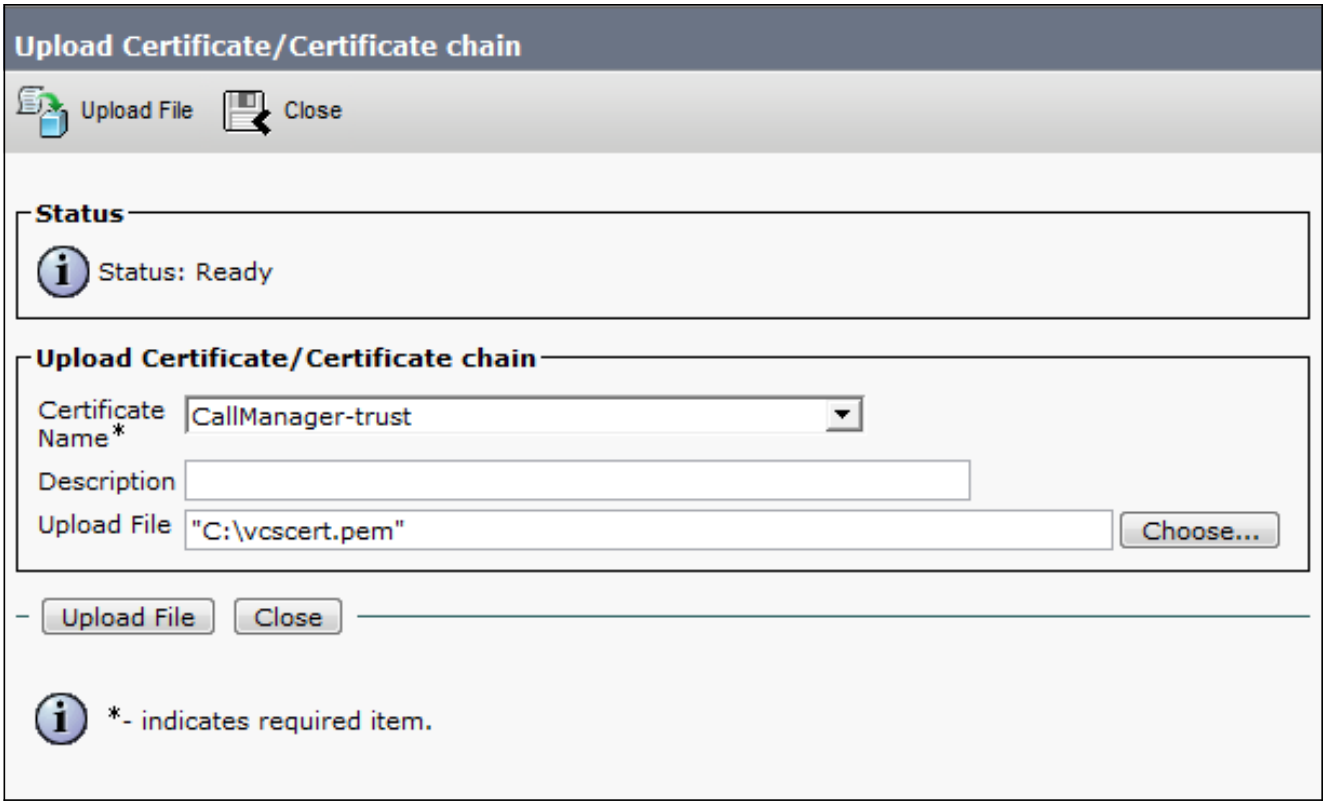
5. Repita este procedimiento para todos los servidores VCS.

Cargar certificado del servidor VCS al servidor CUCM

CUCM debe confiar en los certificados que ofrece VCS.

Este procedimiento describe cómo cargar el certificado VCS que generó en CUCM como un certificado CallManager-Trust:

1. En la página Administración del sistema operativo, navegue hasta **Seguridad > Administración de certificados**, ingrese el nombre del certificado, navegue hasta su ubicación y haga clic en **Cargar archivo**:



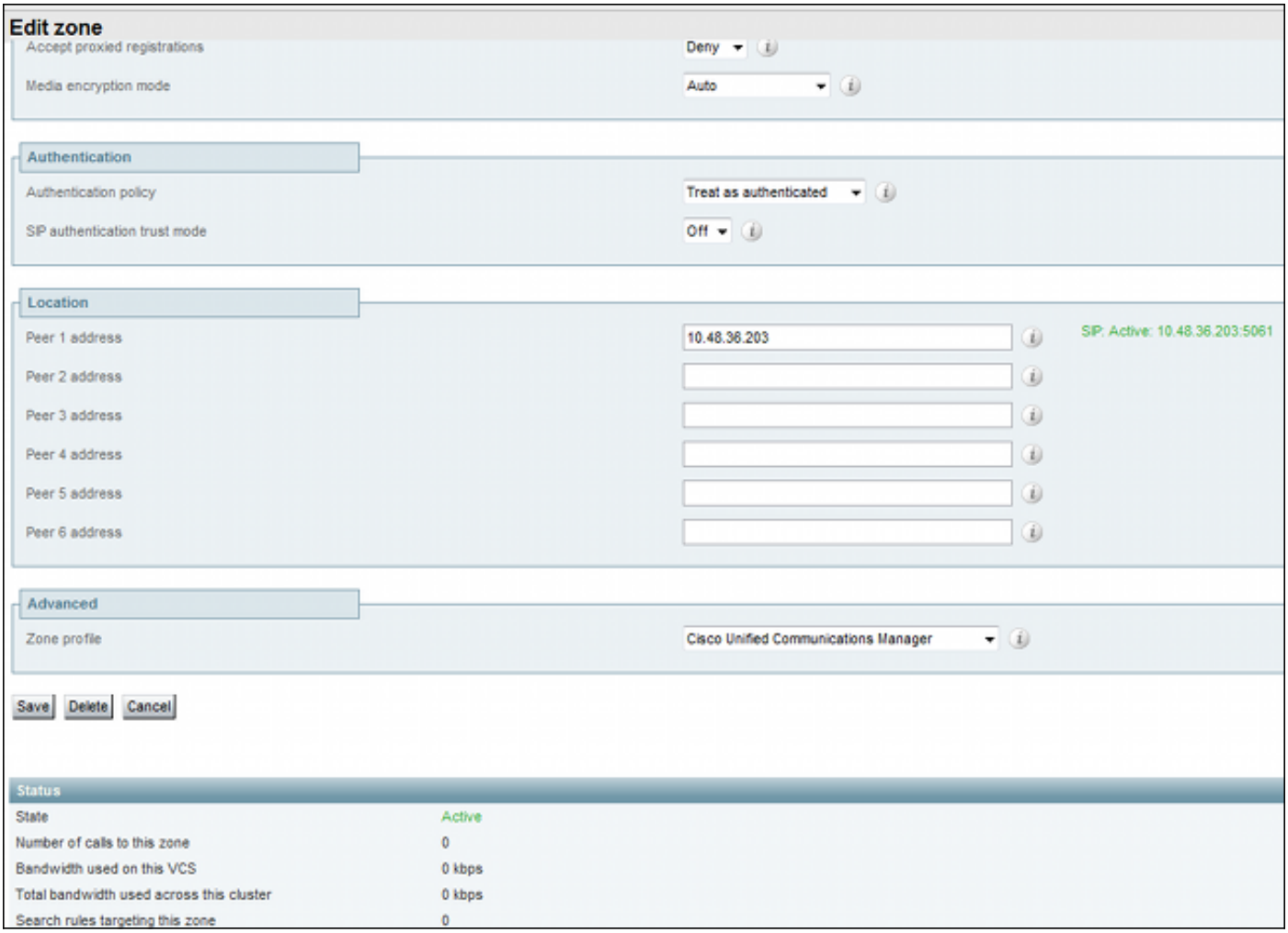
2. Cargue el certificado de todos los servidores VCS. Haga esto en cada servidor CUCM que se comunique con el VCS; generalmente se trata de todos los nodos que ejecutan el servicio CallManager.

Conexión SIP

Una vez que se validen los certificados y ambos sistemas confíen entre sí, configure la zona vecina en VCS y el troncal SIP en CUCM. Consulte la Guía de implementación de Cisco TelePresence Cisco Unified Communications Manager with Cisco VCS (SIP Trunk) para obtener detalles sobre este procedimiento.

Verificación

Confirme que la conexión SIP está activa en la zona vecina en VCS:



Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Cisco TelePresence Guía de implementación de Cisco Unified Communications Manager con Cisco VCS (SIP Trunk)
- Guía del administrador de Cisco TelePresence Video Communication Server
- Guía de implementación de creación y uso de certificados de Cisco TelePresence con Cisco VCS
- Guía de administración del sistema operativo Cisco Unified Communications
- Guía de administración de Cisco Unified Communications Manager
- Soporte Técnico y Documentación - Cisco Systems