

# Asegure el trunk del SORBO entre el ejemplo de configuración CUCM y del VCS

## Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de la red](#)

[Obtenga el certificado del VCS](#)

[Genere y cargue el certificado autofirmado del VCS](#)

[Agregue el certificado autofirmado del servidor CUCM al servidor del VCS](#)

[Cargue el certificado del servidor del VCS al servidor CUCM](#)

[SORBA la conexión](#)

[Verificación](#)

[Troubleshooting](#)

[Información Relacionada](#)

## Introducción

Este documento describe cómo configurar una conexión segura del Session Initiation Protocol (SIP) entre el administrador de las Comunicaciones unificadas de Cisco (CUCM) y el servidor de la comunicación mediante video del Cisco TelePresence (VCS).

Los CUCM y el VCS se integran de cerca. Porque los punto final de video se pueden registrar en el CUCM o el VCS, los trunks del SORBO deben existir entre los dispositivos.

## Prerequisites

### Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Administrador de las Comunicaciones unificadas de Cisco
- Servidor de la comunicación mediante video del Cisco TelePresence
- Certificados

## Componentes Utilizados

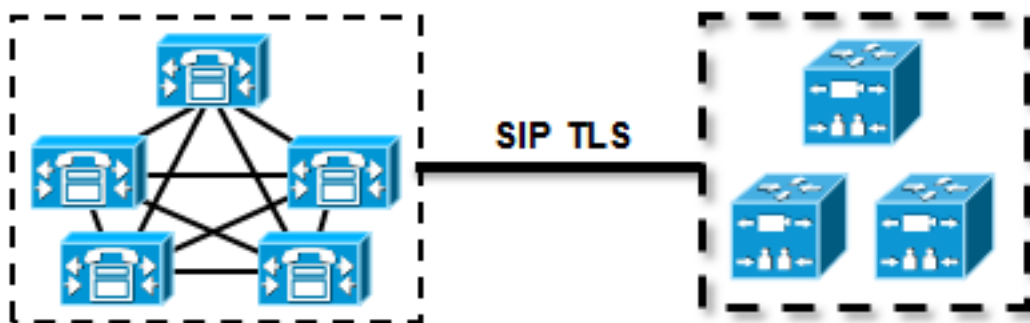
Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware. Este ejemplo utiliza la versión de software X7.2.2 del VCS de Cisco y la versión 9.x CUCM.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

## Configurar

Asegúrese de que los Certificados son válidos, agregue los Certificados a los servidores CUCM y del VCS de modo que confíen en los Certificados de cada uno, después establecen el trunk del SORBO.

### Diagrama de la red



### Obtenga el certificado del VCS

Por abandono, todos los sistemas del VCS vienen con el certificado temporal. En la página de administración, navegue al Certificate Management (Administración de certificados) > al **certificado de servidor del mantenimiento**. Haga clic el **certificado de la show server**, y una nueva ventana se abre con los datos sin procesar del 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

Currently loaded certificate expires on Sep 30 2014

Reset to default server certificate

PEM File **Show server certificate**

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

```
-----BEGIN CERTIFICATE-----
MIIDHzCCAoigAwIBAgIBATANBgkqhkiG9w0BAQUFADCBMjFDMEEGA1UECgw6VGvt
cG9yYXJ5IENlcnRpZmljYXRlIDU4Nzc0NWYwLTI5YTAzMTR1My1hNTE4LTAwNTA1
Njk5NWl0YjFDMEEGA1UECww6VGvtcG9yYXJ5IENlcnRpZmljYXRlIDU4Nzc0NWYw
LTI5YTAzMTR1My1hNTE4LTAwNTA1Njk5NWl0YjEOMAwGA1UEAwwFY2l2Y28wHhcN
MTMwOTMwMDCxNzIwWWhcNMTQwOTMwMDCxNzIwWjCBMjFDMEEGA1UECgw6VGvtcG9y
YXJ5IENlcnRpZmljYXRlIDU4Nzc0NWYwLTI5YTAzMTR1My1hNTE4LTAwNTA1Njk5
NWl0YjFDMEEGA1UECww6VGvtcG9yYXJ5IENlcnRpZmljYXRlIDU4Nzc0NWYwLTI5
YTAzMTR1My1hNTE4LTAwNTA1Njk5NWl0YjEOMAwGA1UEAwwFY2l2Y28wZ8wDQYJ
KoZlHvcNAQEBBQADgY0AMIGJAoGBAKWvob+Y1zrKoAB5BvPsGR7aVfmTYPiP0I/
L21fyYj005qv91zDCgy7PFZPxD1d/DNLlGp1jjUqdfFV+64r80kESwBO+4DFlut
tWZLQ1uKzzdsmvZ/b41mEtosElHNxH7rDYQsqdRA4ngNDJv1OgVFCEV4c7ZvAV4S
E8m9YNY9AgMBAAGjczBxMAKGA1UdEwQCMAAwJAYJYIZIAYb4QgENBBcWFVR1bXBv
cmFyeSBBDZXJ0aWZpY2F0ZTAzZmVhZDQ4EFgQU+knGYkeeiWqAjoRhZQqRCHba+nEw
HwYDVR0jBBGwFoAUpHCEOXsBH1AzZN153S/Lv6cxNDIwDQYJKoZIhvcNAQEFBQAD
gYEAZk1IMSfi49p1jIYqYdOAIjOiaashYVfqGUUMFr4V1hokM90ByGGTbx8jx6Y/S
p1SyT4ilU5uiY0DD18EkLzt8y3jFNPmHYAw/f2fB9J3mDAqbiQdmbLAeD2RRUsy7
1Zc3zTl6Wl6hsj+90GAsI/TGthQ2n7yUWPl6CevopbJeliA=
-----END CERTIFICATE-----
```

Usted puede decodificar el certificado y ver los datos del certificado con el uso del OpenSSL en su PC local o el uso de un decodificador en línea del certificado tal como [comprador SSL](#):



## Genere y cargue el certificado autofirmado del VCS

Porque cada servidor del VCS tiene un certificado con el mismo Common Name, usted necesita poner los nuevos Certificados en el servidor. Usted puede elegir utilizar los certificados autofirmados o los Certificados firmados por el Certificate Authority (CA). Vea la [creación y el uso del certificado del Cisco TelePresence con el Guía de despliegue del VCS de Cisco](#) para los detalles de este procedimiento.

Este procedimiento describe cómo utilizar el VCS sí mismo para generar un certificado autofirmado, después carga ese certificado:

1. Inicie sesión como raíz al VCS, comience el 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 un pedido 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 están disponibles ahora:

```
~ # 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 carguelos en la página web así que el VCS puede utilizar los Certificados; usted necesita la clave privada y el certificado generado:

**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:\vcs-cert.pem" [Choose...](#) ⓘ

[Upload server certificate data](#)

6. Relance este procedimiento para todos los servidores del VCS.

## Agregue el certificado autofirmado del servidor CUCM al servidor del VCS

Agregue los Certificados de los servidores CUCM de modo que el VCS los confíe en. En este ejemplo, usted está utilizando los certificados autofirmados estándar de CUCM; CUCM genera los certificados autofirmados durante la instalación así que usted no necesita crear éstos como usted hizo en el VCS.

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

1. Descargue el certificado CallManager.pem del CUCM. El registro en la página de administración OS, navega a la Seguridad > a CertificateManagement, **después** selecciona y descarga el certificado uno mismo-firmado CallManager.pem:

**Certificate Configuration**

Regenerate Download Generate CSR Download CSR

---

**Status**

**i** 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
  Signature Algorithm: SHA1withRSA (1.2.840.113549.1.1.5)
  Issuer Name: L=Peg3, ST=Diegem, CN=MFC1Pub, 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=MFC1Pub, 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,
  ]
]
```

Regenerate **Download** Generate CSR Download CSR

2. Agregue este certificado como certificado de CA de confianza en el VCS. On el VCS, navegue al Certificate Management (Administración de certificados) del **mantenimiento > confiaba en el certificado de CA**, y seleccionan el **certificado de CA de la demostración**:

**Trusted CA certificate**

**i** 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... **i**

CA certificate PEM File **Show CA certificate**

Upload CA certificate Reset to default CA certificate

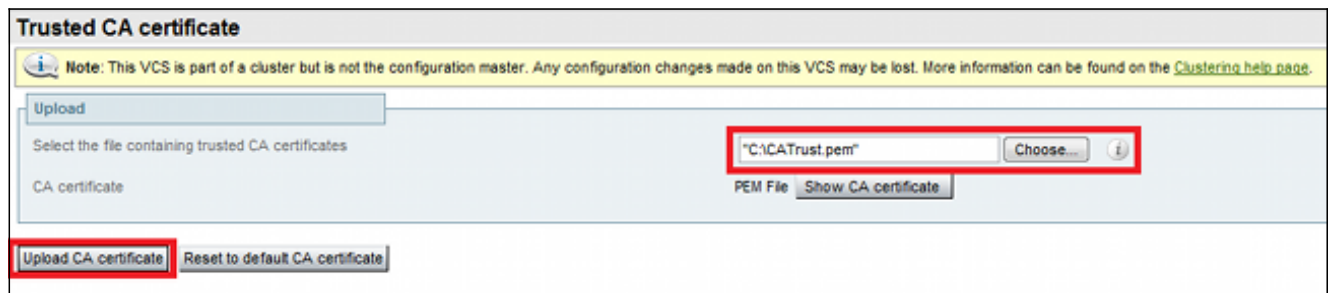
Una nueva ventana se abre con todos los Certificados que se confien en actualmente.

3. Copie todos los actualmente certificados confiables a un archivo de texto. Abra el archivo CallManager.pem en un editor de textos, copie su contenido, y agregue ese contenido a la parte inferior del mismo archivo de texto después actualmente de los certificados confiables:

```
CallManagerPub
=====
-----BEGIN CERTIFICATE-----
MIICmDCCAgGgAwIBAgIQZo7W0mjKYy9JP228PpPvgTANBgkqhkiG9w0BAQUFADBe
MQswCQYDVQQGEwJCRTEOMAwGA1UEChMFQ2l2Y28xDDAKBgNVBAsTA1RBQzERMA8G
A1UEAxMITUZDbDFQdWIxZDZANBgNVBAgTBkRlZDZANBgNVBAgTBkRlZDZANBgNV
AwEw0xMjA4MDExMDI4MzVaFw0xNzA3MzExMDI4MzRaMF4xMzA3MzExMDI4MzRa
DAYDVQQKEwVDbzEMMAoGA1UECjxMDVEFDMREwDwYDVQDEwNRkNsMVB1YjEP
MA0GA1UECBMGRG1lZ2VtMQ0wCwYDVQQHEwRlZDZANBgNVBAsTA1RBQzERMA8G
A4GNADCBiQKBgQDmCOYmVrQzHh1+nFdHk0Y2P1NdACglvnRFwAq/rNgGrPCiwTgc
0cxqsGtGQLSN1UyIPDAE5NufROQPJ7whR95KgmYbGdwHfKeuig+MT2CG1tfPe6ly
c/ZEDqHYvG1zJT5srWUfM9GdkTzfHI1iV6k/jvPtGigXDSCiqEjn1+3IEQIDAQAB
o1cwVTALBgNVHQ8EBAMCARwwJwYDVR01BCAwHgYIKwYBBQUHAWEGCCsGAQUFBwMC
BggrBgEFBQcDBTAdBgNVHQ4EFgQUK4jYX6O6BAnLCalbKE6YV7BpkQwDQYJKoZI
hvcNAQEFBQADgYEAkEGDdRdM0tX4ClhEatQE3ptT6L6RRAYP8oDd3dIGEYOWhA2H
Aqrw771oieva297AwgcKbPxnd51Z/aBJxvmF8TIIOSkky+dJW0asZWfei9STxVGn
NSr1CyAt8UJh0DSUjGHtnv7yWse5BB9mBDR/rmWxIRr1IRzAJDeygLIq+wc=
-----END CERTIFICATE-----
```

Si usted tiene los servidores múltiples en el CUCM agrupan, agregan todos aquí.

4. Salve el archivo como CATrust.pem, y haga clic el **certificado de UploadCA** para cargar el archivo de nuevo al VCS:



El VCS ahora confiará en los Certificados ofrecidos por CUCM.

5. Relance este procedimiento para todos los servidores del VCS.

## Cargue el certificado del servidor del VCS al servidor CUCM

El CUCM necesita confiar en los Certificados ofrecidos por el VCS.

Este procedimiento describe cómo cargar el certificado del VCS que usted generó en el CUCM como certificado de la CallManager-confianza:


1. En la página de administración OS, navegue al Certificate Management (Administración de certificados) de la **Seguridad**, ingrese el nombre del certificado, hojee a su ubicación, y haga clic el **archivo de la carga**:

### Upload Certificate/Certificate chain

Upload File Close

---

**Status**

 Status: Ready

---


**Upload Certificate/Certificate chain**

Certificate Name\*

Description

Upload File

---

 \*- indicates required item.

2. Cargue el certificado de todos los servidores del VCS. Haga esto en cada servidor CUCM que comunique con el VCS; éste es típicamente todos los Nodos que están dirigiendo el servicio de CallManager.

## Conexión del SORBO

Una vez que se validan los Certificados y ambos sistemas se confían en, configure la zona vecina en el VCS y el trunk del SORBO en CUCM. Vea al [administrador de las Comunicaciones unificadas de Cisco del Cisco TelePresence con el Guía de despliegue del VCS de Cisco \(trunk del SORBO\)](#) para los detalles de este procedimiento.

## Verificación

Confirme que la conexión del SORBO es activa en la zona vecina en el VCS:



### Edit zone

Accept proxied registrations Deny ⓘ

Media encryption mode Auto ⓘ

---

**Authentication**

Authentication policy Treat as authenticated ⓘ

SP authentication trust mode Off ⓘ

---

**Location**

Peer 1 address  ⓘ SP: 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

## Troubleshooting

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

## Información Relacionada

- [Administrador de las Comunicaciones unificadas de Cisco del Cisco TelePresence con el Guía de despliegue del VCS de Cisco \(trunk del SORBO\)](#)
- [Guía de Administrador del servidor del comunicación mediante video del Cisco TelePresence](#)
- [Creación y uso del certificado del Cisco TelePresence con el Guía de despliegue del VCS de Cisco](#)
- [Guía de administración del sistema operativo de las Comunicaciones unificadas de Cisco](#)
- [Guía del control del administrador de las Comunicaciones unificadas de Cisco](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)