

Sicherer SIP-Trunk zwischen CUCM und VCS - Konfigurationsbeispiel

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[VCS-Zertifikat anfordern](#)

[Selbstsigniertes VCS-Zertifikat generieren und hochladen](#)

[Hinzufügen eines selbstsignierten Zertifikats vom CUCM-Server zum VCS-Server](#)

[Zertifikat vom VCS-Server auf den CUCM-Server hochladen](#)

[SIP-Verbindung](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird die Einrichtung einer sicheren SIP-Verbindung (Session Initiation Protocol) zwischen dem Cisco Unified Communications Manager (CUCM) und dem Cisco TelePresence Video Communication Server (VCS) beschrieben.

CUCM und VCS sind eng integriert. Da Videoendpunkte entweder am CUCM oder am VCS registriert werden können, müssen SIP-Trunks zwischen den Geräten vorhanden sein.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

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

Verwendete Komponenten

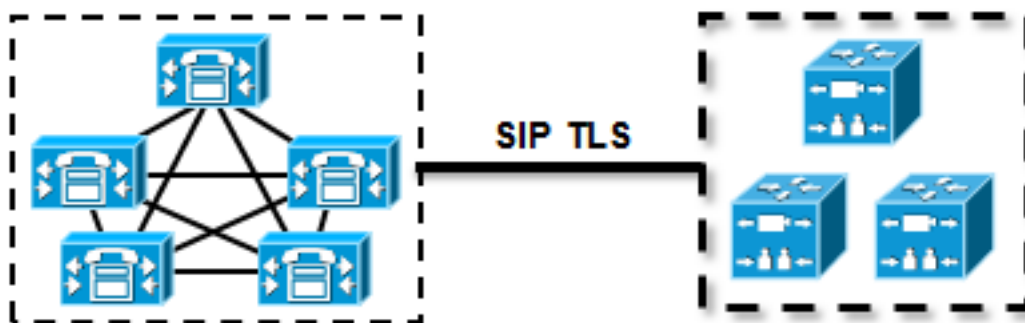
Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt. In diesem Beispiel wird die Cisco VCS Software-Version X7.2.2 und die CUCM-Version 9.x verwendet.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konfigurieren

Stellen Sie sicher, dass die Zertifikate gültig sind, und fügen Sie die Zertifikate den CUCM- und VCS-Servern hinzu, damit diese den Zertifikaten der anderen vertrauen. Richten Sie dann den SIP-Trunk ein.

Netzwerkdiagramm



VCS-Zertifikat anfordern

Standardmäßig enthalten alle VCS-Systeme ein temporäres Zertifikat. Navigieren Sie auf der Admin-Seite zu **Maintenance > Certificate management > Server certificate**. Klicken Sie auf **Serverzertifikat anzeigen**, und ein neues Fenster mit den Rohdaten des Zertifikats wird geöffnet:

The screenshot shows the 'Server certificate' configuration page. At the top, there is a note: '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](#).' Below the note, there is a section for 'Server certificate data' with a 'Server certificate' field. To the right of this field is a button labeled 'Show server certificate' with 'PEM File' next to it, which is highlighted with a red box. Below this, it says 'Currently loaded certificate expires on Sep 30 2014'. At the bottom left, there is a button labeled 'Reset to default server certificate'.

Dies ist ein Beispiel für die Rohdaten des Zertifikats:

```

-----BEGIN CERTIFICATE-----
MIIDHzCCAoigAwIBAgIBATANBgkqhkiG9w0BAQUFADCBMjFDMEEGA1UECgw6VGVT
cG9yYXJ5IENlcnRpZmljYXR1IDU4Nzc0NWYwLTI5YTAzMTEyMTF1My1hNTE4LTAwNTA1
Njk5NWl0YjFDMEEGA1UECww6VGVTcG9yYXJ5IENlcnRpZmljYXR1IDU4Nzc0NWYw
LTI5YTAzMTEyMTF1My1hNTE4LTAwNTA1Njk5NWl0YjEOMAwGA1UEAwwFY21zY28wHhcN
MTMwOTMwMDcxNzIwWWhcNMTQwOTMwMDcxNzIwWjCBMjFDMEEGA1UECgw6VGVTcG9y
YXJ5IENlcnRpZmljYXR1IDU4Nzc0NWYwLTI5YTAzMTEyMTF1My1hNTE4LTAwNTA1Njk5
NWl0YjFDMEEGA1UECww6VGVTcG9yYXJ5IENlcnRpZmljYXR1IDU4Nzc0NWYwLTI5
YTAzMTEyMTF1My1hNTE4LTAwNTA1Njk5NWl0YjEOMAwGA1UEAwwFY21zY28wgZ8wDQYJ
KoZiHvcNAQEBBQADgY0AMIGJAoGBAKWvob+Y1zrKoAB5BvPsGR7aVfmTYPiPL0I/
L21fyjjo05qv91zDCgy7PFZPxD1d/DNLIgpljjUqdfFV+64r8OkESwBO+4DFlut
tWZLQ1uKzzdsMvZ/b41mEtosELHNxH7rDYQsqdRA4ngNDJVL0gVFCEV4c7ZvAV4S
E8m9YNY9AgMBAAGjczBxMAKGA1UdEwQCAAwJAYJYIZIAyB4QgENBBcWFVR1bXBv
cmFyeSBDZSJ0aWZpY2F0ZTAdBgNVHQ4EFgQU+knGYkeeiWqAjORhzQqRCHba+nEw
HwYDVR0jBBgwFoAUPhCEOXsBH1AzZN153S/Lv6cxNDIwDQYJKoZIhvcNAQEFBQAD
gYEAZklIMSfi49p1jIYqYdOAIjOiaShYVfqGUUMFr4V1hokM90ByGGTbx8jx6Y/S
p1SyT4ilU5uiY0DD18EkLzt8y3jFNPmHYAw/f2fB9J3mDAqbiQdmbLAeD2RRUsy7
1Zc3zTl6WL6hsj+90GAsI/TGthQ2n7yUWP16CevopbJe1iA=
-----END CERTIFICATE-----

```

Sie können das Zertifikat dekodieren und die Zertifikatdaten anzeigen, indem Sie OpenSSL auf Ihrem lokalen PC verwenden oder einen Online-Zertifikatdecoder wie [SSL Shopper](#) verwenden :

Certificate Information:

- ✓ **Common Name:** disco
- ✓ **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:** disco, Temporary Certificate 587745f0-29a0-11e3-a518-005056995b4b
- ✓ **Key Size:** 1024 bit
- ✓ **Serial Number:** 1 (0x1)

Selbstsigniertes VCS-Zertifikat generieren und hochladen

Da jeder VCS-Server über ein Zertifikat mit dem gleichen Common Name verfügt, müssen Sie neue Zertifikate auf dem Server platzieren. Sie können selbst signierte Zertifikate oder Zertifikate verwenden, die von der Zertifizierungsstelle signiert wurden. Einzelheiten zu diesem Verfahren finden Sie im [Cisco TelePresence Certificate Creation and Use With Cisco VCS Deployment Guide](#).

In diesem Verfahren wird beschrieben, wie Sie mit dem VCS ein selbstsigniertes Zertifikat generieren und anschließend hochladen:

1. Melden Sie sich als Root beim VCS an, starten Sie OpenSSL, und generieren Sie einen privaten Schlüssel:

```

~ # openssl
OpenSSL> genrsa -out privatekey.pem 1024
Generating RSA private key, 1024 bit long modulus
.....++++++
.....++++++

```

```
e is 65537 (0x10001)
```

2. Verwenden Sie diesen privaten Schlüssel, um eine Zertifikatssignierungsanforderung (Certificate Signing Request, CSR) zu generieren:

```
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. Selbstsigniertes Zertifikat generieren:

```
~ # 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. Vergewissern Sie sich, dass die Zertifikate jetzt verfügbar sind:

```
~ # 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. Laden Sie die Zertifikate mit [WinSCP herunter](#) und laden Sie sie auf die Webseite hoch, damit der VCS die Zertifikate verwenden kann. Sie benötigen den privaten Schlüssel und das generierte Zertifikat:

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:\vcs-cert.pem" ⓘ

6. Wiederholen Sie dieses Verfahren für alle VCS-Server.

Hinzufügen eines selbstsignierten Zertifikats vom CUCM-Server zum VCS-Server

Fügen Sie die Zertifikate der CUCM-Server hinzu, sodass der VCS sie als vertrauenswürdig einstuft. In diesem Beispiel verwenden Sie die selbstsignierten Standardzertifikate von CUCM. CUCM generiert selbstsignierte Zertifikate während der Installation, sodass Sie diese nicht wie auf dem VCS erstellen müssen.

Dieses Verfahren beschreibt, wie Sie dem VCS-Server ein selbstsigniertes Zertifikat vom CUCM-Server hinzufügen:

1. Laden Sie das Zertifikat "CallManager.pem" vom CUCM herunter. Melden Sie sich auf der Seite "OS Administration" an, navigieren Sie zu **Security > Certificate Management**, und wählen Sie das selbstsignierte Zertifikat CallManager.pem aus, und laden Sie es herunter:

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

- Fügen Sie dieses Zertifikat als vertrauenswürdiges Zertifizierungsstellenzertifikat zum VCS hinzu. Navigieren Sie auf dem VCS zu **Wartung > Zertifikatsverwaltung > Vertrauenswürdiges Zertifizierungsstellenzertifikat**, und wählen Sie **Zertifizierungsstellenzertifikat anzeigen** aus:

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

Es wird ein neues Fenster mit allen Zertifikaten geöffnet, die derzeit als vertrauenswürdige gelten.

- Kopieren Sie alle derzeit vertrauenswürdigen Zertifikate in eine Textdatei. Öffnen Sie die Datei CallManager.pem in einem Texteditor, kopieren Sie deren Inhalt, und fügen Sie diesen Inhalt nach den derzeit vertrauenswürdigen Zertifikaten am Ende derselben Textdatei hinzu:

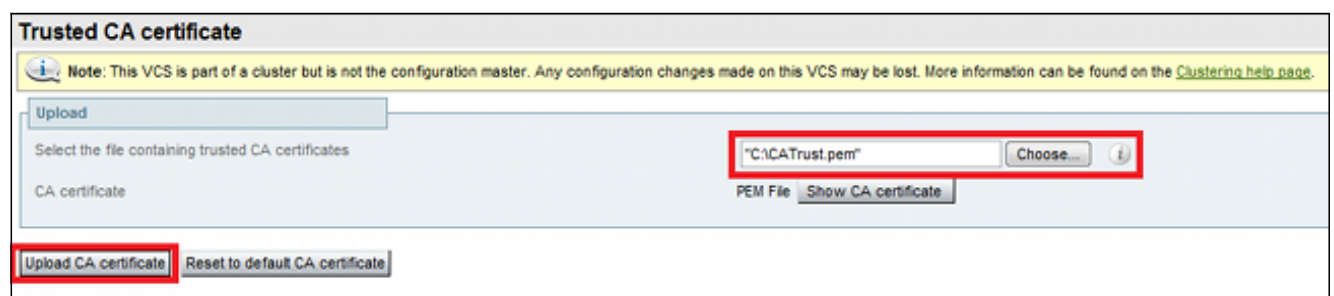
```

CallManagerPub
=====
-----BEGIN CERTIFICATE-----
MIICmDCCAgGgAwIBAgIQZo7WomjKYy9JP228PpPvgTANBgkqhkiG9w0BAQUFADBe
MQswCQYDVQQGEwJCRTEOMAwGA1UEChMFQ2l2Y28xDDAKBgNVBAsTA1RBQzERMA8G
A1UEAxMITUZDbDFQdWlxdzANBgNVBAGTBkRpbWdlbTENMAAGA1UEBxMEUGVnmZAE
Fw0xMjA4MDExMDI4MzVaFw0xNzA3MzExMDI4MzRaMF4xMzA1BGNBAYTAKJFMQ4w
DAYDVQQKEwVDAxNjBzEMMAoGA1UECxMDVEFDMREwDwYDVQQDEWhNRkNsMVB1YjEP
MA0GA1UECBMGRGlZ2VtMQ0wCwYDVQQHEwRQZwczMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQDmCOYmVrQZha1+nFdHk0Y2PlNdACglvnRFwAq/rNgGrPCiwTgc
0cxqsGtGQLSN1UyIPDAE5NuFRQPJ7whR95KGmYbGdwhfKeuig+MT2CGLtfPe6ly
c/ZEDqHYvGlzJT5srWUfm9GdkTZfHI1iV6k/jvPtGigXDSCIqEjn1+3IEQIDAQAB
o1cwVTALBgNVHQ8EBAMCARwwJwYDVR0lBCAwHgYIKwYBBQUHAWEGCCSGAQUFBwMC
BggrBgEFBQcDBTADBgNVHQ4EFgQUK4jYX6O6BANLCalbKE6YV7BpkQwDQYJKoZI
hvcNAQEFBQADgYEAkEGDdRdMOtX4ClhEatQE3ptT6L6RRAYP8oDd3dIGEYOWhA2H
Aqrw771oieva297AwgcKbPxnd5lZ/aBJxvmF8TIioskgy+dJW0asZWfei9STxVGn
NSr1CyAt8UJh0DSUjGHTnv7yWse5BB9mBDR/rmWxIRr1IRzAJDeygLIq+wc=
-----END CERTIFICATE-----

```

Wenn sich im CUCM-Cluster mehrere Server befinden, fügen Sie alle Server hier hinzu.

- Speichern Sie die Datei unter dem Namen CATrust.pem, und klicken Sie auf **CA-Zertifikat hochladen**, um die Datei wieder in den VCS hochzuladen:



Der VCS vertraut nun den vom CUCM angebotenen Zertifikaten.

- Wiederholen Sie dieses Verfahren für alle VCS-Server.



Zertifikat vom VCS-Server auf den CUCM-Server hochladen

Der CUCM muss den vom VCS angebotenen Zertifikaten vertrauen.


In diesem Verfahren wird beschrieben, wie Sie das auf dem CUCM generierte VCS-Zertifikat als CallManager-Trust-Zertifikat hochladen:

- Navigieren Sie auf der Seite "OS Administration" zu **Security > Certificate Management**, geben Sie den Zertifikatsnamen ein, navigieren Sie zu seinem Speicherort, und klicken Sie auf **Upload File (Datei hochladen)**:

Upload Certificate/Certificate chain

 Upload File  Close

Status


 Status: Ready

Upload Certificate/Certificate chain

Certificate Name*

Description

Upload File

 *- indicates required item.

2. Laden Sie das Zertifikat von allen VCS-Servern hoch. Führen Sie dies auf jedem CUCM-Server aus, der mit dem VCS kommuniziert. Dies sind in der Regel alle Knoten, auf denen der CallManager-Dienst ausgeführt wird.

SIP-Verbindung

Nachdem die Zertifikate validiert wurden und sich beide Systeme gegenseitig vertrauen, konfigurieren Sie die Nachbarzone auf dem VCS und den SIP-Trunk auf dem CUCM. Einzelheiten zu diesem Verfahren finden Sie im [Bereitstellungsleitfaden für Cisco TelePresence Cisco Unified Communications Manager mit Cisco VCS \(SIP-Trunk\)](#).

Überprüfung

Vergewissern Sie sich, dass die SIP-Verbindung in der Nachbarzone des VCS aktiv ist:

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 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

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- [Cisco TelePresence Cisco Unified Communications Manager mit Cisco VCS \(SIP-Trunk\) - Implementierungsleitfaden](#)
- [Administratoranleitung für Cisco TelePresence Video Communication Server](#)
- [Cisco TelePresence - Erstellung und Verwendung von Zertifikaten mit Cisco VCS - Implementierungsleitfaden](#)
- [Administrationsleitfaden für das Cisco Unified Communications-Betriebssystem](#)
- [Cisco Unified Communications Manager - Administratorhandbuch](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)