

CUCM과 VCS 간 보안 SIP 트렁크 컨피그레이션 예

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[네트워크 다이어그램](#)

[VCS 인증서 얻기](#)

[VCS 자체 서명 인증서 생성 및 업로드](#)

[CUCM 서버에서 VCS 서버로 자체 서명 인증서 추가](#)

[VCS 서버에서 CUCM 서버로 인증서 업로드](#)

[SIP 연결](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[관련 정보](#)

소개

이 문서에서는 CUCM(Cisco Unified Communications Manager)과 Cisco VCS(TelePresence Video Communication Server) 간에 SIP(Secure Session Initiation Protocol) 연결을 설정하는 방법에 대해 설명합니다.

CUCM과 VCS는 긴밀하게 통합됩니다. 비디오 엔드포인트는 CUCM 또는 VCS에 등록할 수 있으므로 디바이스 간에 SIP 트렁크가 있어야 합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

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

사용되는 구성 요소

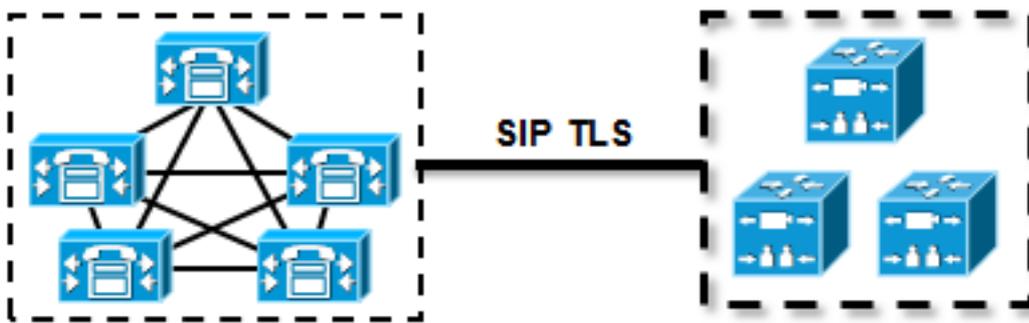
이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다. 이 예에서는 Cisco VCS 소프트웨어 버전 X7.2.2 및 CUCM 버전 9.x를 사용합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

인증서가 유효한지 확인하고 인증서를 CUCM 및 VCS 서버에 추가하여 서로의 인증서를 신뢰한 다음 SIP 트렁크를 설정합니다.

네트워크 다이어그램



VCS 인증서 얻기

기본적으로 모든 VCS 시스템은 임시 인증서와 함께 제공됩니다. 관리자 페이지에서 **Maintenance > Certificate management > Server certificate**로 이동합니다. Show server certificate(서버 인증서 표시)를 클릭하면 인증서의 원시 데이터와 함께 새 창이 열립니다.

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

원시 인증서 데이터의 예입니다.

-----BEGIN CERTIFICATE-----

MIIDHzCCAoigAwIBAgIBATANBgkqhkiG9w0BAQUFADCbmjFDMEEGA1UECgw6VGvt

```
cG9yYXJ5IENlcnRpZmljYXRlIDU4Nzc0NWYwLTI5YTAtMTF1My1hNTE4LTAwNTA1
Njk5NWl0YjFDMEEGA1UECww6VGVTcG9yYXJ5IENlcnRpZmljYXRlIDU4Nzc0NWYw
LTI5YTAtMTF1My1hNTE4LTAwNTA1Njk5NWl0YjEOMAwGA1UEAwFY21zY28wHhcN
MTMwOTMwMdcxNzIwWWhcNMTQwOTMwMdcxNzIwWjCBMjFDMEEGA1UECgw6VGVTcG9y
YXJ5IENlcnRpZmljYXRlIDU4Nzc0NWYwLTI5YTAtMTF1My1hNTE4LTAwNTA1Njk5
NWl0YjFDMEEGA1UECww6VGVTcG9yYXJ5IENlcnRpZmljYXRlIDU4Nzc0NWYwLTI5
YTAtMTF1My1hNTE4LTAwNTA1Njk5NWl0YjEOMAwGA1UEAwFY21zY28wZ8wDQYJ
KoZlhcNAQEBBQADgY0AMIGJAoGBAKWvob+Y1zrKoAB5BvPsGR7aVfmTYPipL0I/
L21fyYjo05qv91zDCgy7PFZPxd1d/DNLlIgp1jUqdfFV+64r8OkESwBO+4DFlut
tWZLQ1uKzzdsMvZ/b41mEtosElHNxH7rDYQsqdRA4ngNDJv1OgVFCEV4c7ZvAV4S
E8m9YNY9AgMBAAGjczBxMAkGA1UdEwQCAAwJAYJYIZIAyB4QgENBBcWFVR1bXBv
cmFyeSBZDZXJ0aWZpY2F0ZTAdBgNVHQ4EFgQU+knGYkeeiWqA jORhzQqRCHba+nEw
HwYDVR0jBBGwFoAUpHCEOXsBH1AzZN153S/Lv6cxNDIwDQYJKoZIhvcNAQEFBQAD
gYEAZklIMSfi49p1jIYqYdOAIjOiashYVfqGUUMFr4V1hokM90ByGGTbx8jx6Y/S
p1SyT4ilU5uiY0DD18EkLzt8y3jFNPmHYAw/f2fB9J3mDAqbiQdmbLAeD2RRUsy7
1Zc3zTl6WL6hsj+90GAsI/TGthQ2n7yUWPl6CevopbJeliA=
-----END CERTIFICATE-----
```

로컬 PC에서 OpenSSL을 사용하거나 [SSL Shopper](#)와 같은 온라인 인증서 디코더를 사용하여 인증서를 디코딩하고 인증서 데이터를 볼 수 있습니다.

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 자체 서명 인증서 생성 및 업로드

모든 VCS 서버에는 동일한 Common Name의 인증서가 있으므로 서버에 새 인증서를 배치해야 합니다. 자체 서명 인증서 또는 CA(Certificate Authority)에서 서명한 인증서를 사용하도록 선택할 수 있습니다. 이 절차에 대한 자세한 [내용은 Cisco TelePresence 인증서 생성 및 Cisco VCS와 함께 사용](#) 구축 설명서를 참조하십시오.

이 절차에서는 VCS 자체를 사용하여 자체 서명 인증서를 생성한 다음 해당 인증서를 업로드하는 방법을 설명합니다.

1. VCS에 루트로 로그인하고 OpenSSL을 시작하고 개인 키를 생성합니다.

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

2. CSR(Certificate Signing Request)을 생성하려면 이 개인 키를 사용합니다.

```
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. 자체 서명 인증서를 생성합니다.

```
~ # 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. 이제 인증서를 사용할 수 있는지 확인합니다.

```
~ # 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. WinSCP로 [인증서](#)를 다운로드하고 웹 페이지에 업로드하여 VCS에서 인증서를 사용할 수 있도록 합니다. 개인 키와 생성된 인증서가 모두 필요합니다.

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. 모든 VCS 서버에 대해 이 절차를 반복합니다.

CUCM 서버에서 VCS 서버로 자체 서명 인증서 추가

VCS가 인증서를 신뢰하도록 CUCM 서버에서 인증서를 추가합니다. 이 예에서는 CUCM의 표준 자체 서명 인증서를 사용합니다. CUCM은 설치하는 동안 자체 서명 인증서를 생성하므로 VCS에서 생성했던 것과 같은 인증서를 생성할 필요가 없습니다.

이 절차에서는 CUCM 서버에서 VCS 서버로 자체 서명 인증서를 추가하는 방법에 대해 설명합니다

1. CUCM에서 CallManager.pem 인증서를 다운로드합니다. OS Administration(OS 관리) 페이지에 로그인하여 **Security(보안) > Certificate Management(인증서 관리)**로 이동한 다음 자체 서명 CallManager.pem 인증서를 선택하여 다운로드합니다.

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. 이 인증서를 VCS의 신뢰할 수 있는 CA 인증서로 추가합니다. VCS에서 **Maintenance > Certificate management > Trusted CA certificate**로 이동하고 **Show CA certificate**를 선택합니다.

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

현재 신뢰할 수 있는 모든 인증서가 포함된 새 창이 열립니다.

3. 현재 신뢰할 수 있는 모든 인증서를 텍스트 파일에 복사합니다. 텍스트 편집기에서 CallManager.pem 파일을 열고 내용을 복사한 다음 현재 신뢰할 수 있는 인증서 다음에 같은 텍스트 파일의 맨 아래에 해당 내용을 추가합니다.

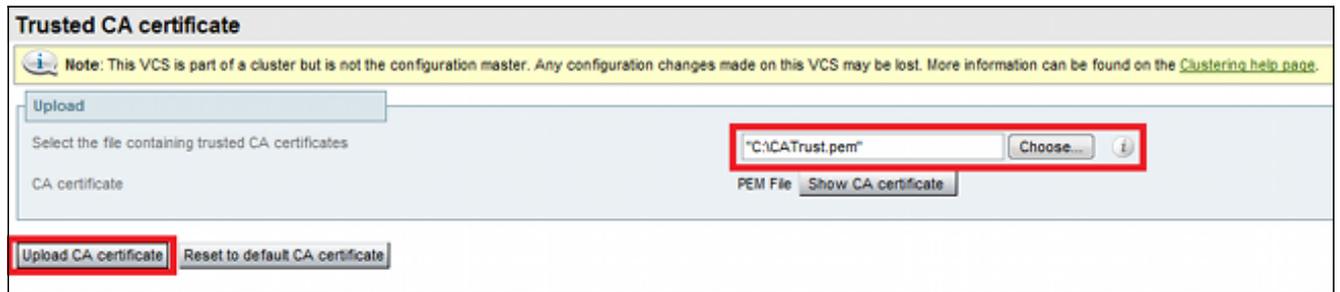
```

CallManagerPub
=====
-----BEGIN CERTIFICATE-----
MIICmDCCAgGgAwIBAgIQZo7W0mjKYy9JP228PpPvgTANBgkqhkiG9w0BAQUFADBe
MQswCQYDVQQGEwJCRTEOMAwGA1UEChMFQ21zY28xDDAKBgNVBAsTA1RBQzERMA8G
A1UEAxMITUZDbDFQdWlxdzANBgNVBAGTBkRpbWdlbTENMAAsGA1UEBxMEUGVnMzAe
Fw0xMjA4MDExMDI4MzVaFw0xNzA3MzExMDI4MzRaMF4xChzAJBgNVBAYTAkJKMQ4w
DAYDVQQKEwVDaXNjbzEMMAoGA1UECjMDVEFDMREwDwYDVQQDEwhNRkNsMVB1YjEP
MA0GA1UECBMGRG1lZ2VtMQ0wCwYDVQQHEwRQZWczMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQDmCOYmVrQzHAl+nFdHk0Y2P1NdACg1vnRFwAq/rNgGrPCiwTgc
0cxqsGtGQLSN1UyIPDAE5NufROQPJ7whR95KGmYbGdwHfKeuig+MT2CG1tfPe6ly
c/ZEDqHYvG1zJT5srWUFm9GdkTzfHI1iV6k/jvPtGigXDSCIqEjn1+3IEQIDAQAB
o1cwVTALBgNVHQ8EBAMCArwwJwYDVR01BCAwHgYIKwYBBQUHAWEGCCsGAQUFBwMC
BggrBgEFBQcDBTAdBgNVHQ4EFgQUK4jYX6O6BAnLCalbKE6YV7BpkQwDQYJKoZI
hvcNAQEFBQADgYEAkEGDdRdMOTX4ClhEatQE3ptT6L6RRAyP8oDd3dIGEYOWhA2H
Aqrw771oieva297AawgKbPxnd51Z/aBJxvmF8TIIOSkgy+dJW0asZWfei9STxVGn
NSr1CyAt8UJh0DSUjGHtnv7yWse5BB9mBDR/rmWxIRr1IRzAJDeygLIq+wc=
-----END CERTIFICATE-----

```

CUCM 클러스터에 여러 서버가 있는 경우 여기에 모든 서버를 추가합니다.

4. 파일을 CATrust.pem으로 저장하고 Upload CA certificate(CA 인증서 업로드)를 클릭하여 파일을 VCS에 다시 업로드합니다.



이제 VCS가 CUCM에서 제공하는 인증서를 신뢰합니다.

5. 모든 VCS 서버에 대해 이 절차를 반복합니다.

VCS 서버에서 CUCM 서버로 인증서 업로드

CUCM은 VCS에서 제공하는 인증서를 신뢰해야 합니다.

이 절차에서는 CUCM에서 생성한 VCS 인증서를 CallManager-Trust 인증서로 업로드하는 방법에 대해 설명합니다.

1. OS Administration(OS 관리) 페이지에서 **Security(보안) > Certificate Management(인증서 관리)**로 이동하여 인증서 이름을 입력하고 해당 위치를 찾은 다음 **Upload File(파일 업로드)**를 클릭합니다.

Upload Certificate/Certificate chain

 Upload File
 Close

Status

 Status: Ready

Upload Certificate/Certificate chain

Certificate Name*

Description

Upload File

 *- indicates required item.

2. 모든 VCS 서버에서 인증서를 업로드합니다. VCS와 통신할 모든 CUCM 서버에서 이 작업을 수행합니다. 일반적으로 CallManager 서비스를 실행 중인 모든 노드입니다.

SIP 연결

인증서가 검증되고 두 시스템이 서로를 신뢰하면 VCS의 Neighbor Zone 및 CUCM의 SIP Trunk를 구성합니다. 이 절차에 대한 자세한 내용은 [내용은 Cisco TelePresence Cisco Unified Communications Manager with Cisco VCS\(SIP Trunk\) 구축 가이드를 참조하십시오.](#)

다음을 확인합니다.

SIP 연결이 VCS의 네이버 영역에서 활성 상태인지 확인합니다.

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

문제 해결

현재 이 설정에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

- [Cisco TelePresence Cisco Unified Communications Manager with Cisco VCS\(SIP Trunk\) 구축 설명서](#)
- [Cisco TelePresence Video Communication Server 관리자 설명서](#)
- [Cisco TelePresence 인증서 생성 및 Cisco VCS와 함께 사용 구축 설명서](#)
- [Cisco Unified Communications 운영 체제 관리 설명서](#)
- [Cisco Unified Communications Manager 관리 설명서](#)
- [기술 지원 및 문서 - Cisco Systems](#)