为CUCM、IP电话和CUBE之间的SIP TLS和SRTP配置企业CA（第三方CA）签名证书并对其进行故障排除

目录

简介

本文档介绍使用企业证书颁发机构(CA)（第三个）在思科统一通信管理器(CUCM)、IP电话和思科统一边界元素(CUBE)之间的会话发起协议(SIP)传输层安全(TLS)和安全实时传输协议(SRTP)的配置示例参与方CA)已签名的证书，并使用通用企业CA为所有网络组件（包括IP电话、CUCM、网关和CUBE等思科通信设备）签署证书。

先决条件

要求

Cisco 建议您了解以下主题：

- 企业CA服务器已配置
- CUCM集群配置为混合模式，IP电话注册为安全模式（加密）
- CUBE基本语音服务VoIP和拨号对等体配置已完成

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Windows 2008服务器 — 证书颁发机构
- CUCM 10.5
- CUBE - 3925E，带Cisco IOS® 15.3(3)M3
- CIPC

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

CUBE上的安全语音通信可分为两部分

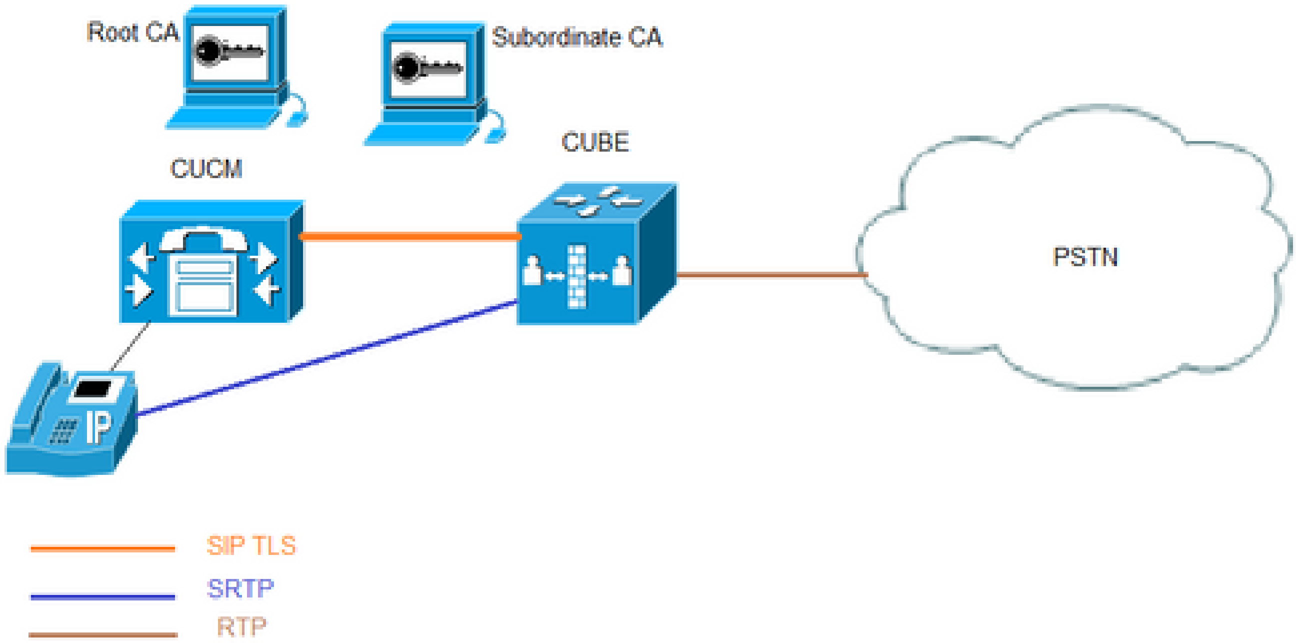
- 安全信令 — CUBE使用TLS保护SIP信令和互联网协议安全(IPSec)，以保护H.323上的信令
- 安全介质 — 安全实时传输协议(SRTP)

CUCM证书颁发机构代理功能(CAPF)为电话提供本地有效证书(LSC)。因此，当CAPF由外部CA签名时，它将充当电话的从属CA。

要了解如何获取CA签名的CAPF，请参阅：

配置

网络图



在此设置中，使用根CA和一个从属CA。所有CUCM和CUBE证书都由从属CA签名。

配置CUBE

生成RSA密钥对。

此步骤生成私钥和公钥。

在本例中，CUBE只是一个标签，它可以是任何内容。

```
CUBE-2(config)#crypto key generate rsa general-keys label CUBE modulus 2048
```

```
The name for the keys will be: CUBE

% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 12 seconds)

CUBE-2(config)#
```

2.为从属CA和根CA创建信任点，从属CA信任点用于SIP TLS通信。

在本示例中，从属CA的信任点名称为SUBCA1，而根CA的信任点名称为ROOT。

```
enrollment terminal pem allow manual cut-and-paste certificate enrollment. pem keyword is used
to issue certificate requests or receive issued certificates in PEM-formatted files through the
console terminal.
```

此步骤中使用的主题名称必须与CUCM SIP中继安全配置文件上的X.509主题名称匹配。最佳实践是使用主机名和域名（如果启用了域名）。

关联在步骤1中创建的RSA密钥对。

```
crypto pki trustpoint SUBCA1
enrollment terminal pem
serial-number none
ip-address none
subject-name CN=CUBE-2
revocation-check none
rsakeypair CUBE

crypto pki trustpoint ROOT
enrollment terminal
revocation-check none
```

3.生成CUBE证书签名请求(CSR)。

crypto pki enroll命令会生成提供给企业CA的CSR，以获取签名的证书。

```
CUBE-2(config)#crypto pki enroll SUBCA1
% Start certificate enrollment ..

% The subject name in the certificate will include: CN=CUBE-2
% The subject name in the certificate will include: CUBE-2
Display Certificate Request to terminal? [yes/no]: yes
Certificate Request follows:

-----BEGIN CERTIFICATE REQUEST-----
MIICjjCCAXYCAQAwKDEPMA0GA1UEAxMGQ1VCRS0yMRUwEwYJKoZIhvcNAQkCFgZD
VUJFLTIwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDAmVvufevAg1ip
Kn8FhWjFlNNUFMqkgh2Cr1IMV+ovR2HyPTFwgr0XDhZHMSsnBw67Ttze3Ebxxoau
cBQcIASZ4hdTSIgjxG+9YQacLm9MXpfxHp5kcICzSfSllrTexArTQglW8+rErYpk
2THN1S0PC4cRlBwoUCgB/+KCDkjJkUy8eCX+Gmd+6ehRKEQ5HdFHEfUr5hc/7/pB
liHietNKSxYEOr9TVZPiRJrtpUPMRMZElRUm7GoxBrCWIXVdvEAGC0Xqd1ZVLlTz
z2sQQDqvJ9fMN6fngKv2ePr+f5qejWVzGO0DFVQs0y5x+Yl+pHbsdV1hSSnPpJk6
TaaBmX83AgMBAAGgITAfBgkqhkiG9w0BCQ4xEjAQMA4GA1UdDwEB/wQEAwIFoDAN
BgkqhkiG9w0BAQUFAAOCAQEArWMJbdhlU8VfaF1cMJIbr569BZT+tIjQOz3OqNGQ
QpzHwclLoaKuC5pc/u0hw14MGS6Z440Iw4zK2/5bb/KL47r8H3d7T7PYMfK6lAzK
sU9Kf96zTvHNWl9wXImB5blJfRLXnFWXNsVEF4FjU74plxJL7siaa5e86eNy9deN
20iKjvP8o4MgWewILrD01YZMDMDS1Uy82kWI6hvXG5+xBT5A1lo2xCj1S9y6/D4d
f0ilDZvaQk+7jjBCzLv5hET+1neoQBw52e7RWU8s2biQw+7TEAdO8NytF3q/mA/x
```

```
bUKw5wT4pgGUJcDAWej3ZLqP91g5yyd9MiCdCRY+3mLccQ==
-----END CERTIFICATE REQUEST-----

---End - This line not part of the certificate request---

Redisplay enrollment request? [yes/no]: no
CUBE-2(config)#
```

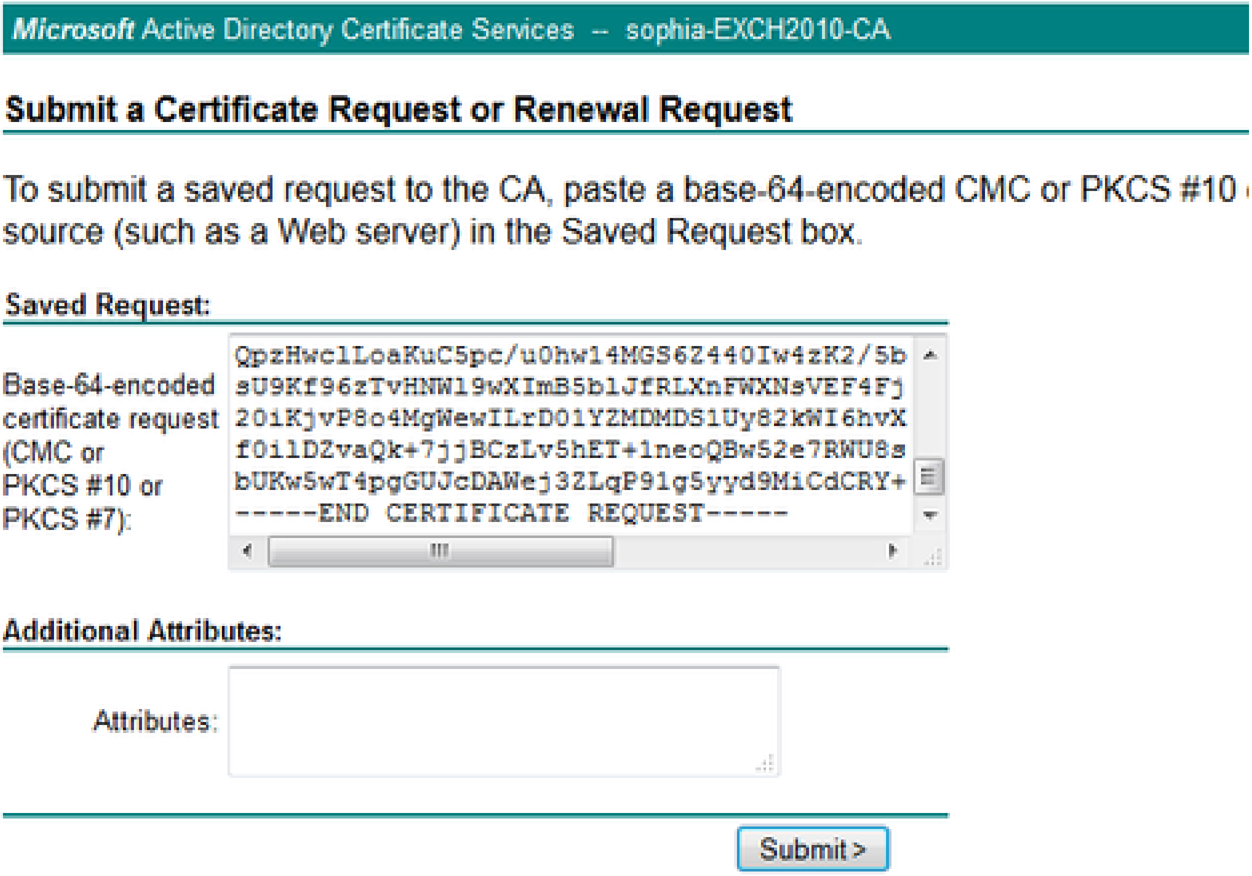
将BEGIN CERTIFICATE REQUEST与END CERTIFICATE REQUEST之间的输出复制到记事本文件中。

CUBE CSR将具有以下关键属性：

```
 Attributes:
Requested Extensions:
X509v3 Key Usage: critical
Digital Signature, Key Encipherment
```

4. 从从属CA获取CA证书根CA，然后获取CA证书和签名CUBE证书。

要获取签名的CUBE证书，请使用步骤3中生成的CSR。映像来自Microsoft CA Web服务器。



Microsoft Active Directory Certificate Services -- sophia-EXCH2010-CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10
source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
QpzHwclLoaKuC5pc/u0hw14MGS6Z440Iw4zK2/5b
sU9Kf96zTvHNW19wXImB5b1JfRLXnFWXNsVEF4Fj
20iKjvP8o4MgWewILrD01YZMDMDS1Uy82kWI6hvX
f0ilDZvaQk+7jjBCzLv5hET+1neoQBw52e7RWU8s
bUKw5wT4pgGUJcDAWej3ZLqP91g5yyd9MiCdCRY+
-----END CERTIFICATE REQUEST-----
```

Additional Attributes:

Attributes:

5.导入根CA和从属CA的CA证书。

在记事本中打开证书，将内容从BEGIN CERTIFICATE REQUEST复制并粘贴到END CERTIFICATE REQUEST。

```
CUBE-2(config)#crypto pki authenticate SUBCA1

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIFhDCCBGygAwIBAgIKYZVFyQAAAAAAFjANBgkqhkiG9w0BAQUFADBQMRIwEAYK
CZImiZPyLGQBGRYCbGkxFjAUBgoJkiaJk/IsZAEZFgZzb3BoaWExIjAgBgNVBAMT
GXNvcGhpYS1XSU4tM1MxOEpDM0xNMkEtQ0EwHhcNMTQwOTI1MDAwNzU2WhcNMTYw
OTI1MDAxNzU2WjBJMRIwEAYKCZImiZPyLGQBGRYCbGkxFjAUBgoJkiaJk/IsZAEZ
FgZzb3BoaWExGzAZBgNVBAMTEnNvcGhpYS1FWENIMjAxMC1DQTCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBAJK+Nmz4rieYfr9gH3ISTuYz3TWpafpjDJ7l
7kIwwwC28TvjFl5vrKEiaPyFzxL5TEHaWQ9YAo/WMdtuyF7aB+pLJ1soKcZxtrGv
gTMtuphcJ5Fpd4368lR8ZXJiAT/Dz+Nsh4PC9GUUKQeycyRDeOBz08vL5pLj/W99
b8UMUlVOqBu4e1ZwxWPMFxB7zOeYsCfXMnGFUlp3HFdWZczgK3ldNO9I0X+p70UP
R0CQpMEQxuheqv9kazIIJKfNH8N0qO8IHl76Y32vUzLg3uvZgqWG6hGch/gjm4L/
1KmdZTNSH8H7Kf6vG6PNWrXWwLNkhrWaYEryHelIshEj7ZUeB8sCAwEAAaOCAmUw
ggJhMBIGCSsGAQQBgjcVAQQFAgMBAAEwIwYJKwYBBAGCNxUCBBYEFLnnd8HnCfKE
isPgI58Oog/LqwVSMB0GA1UdDgQWBBSsdYJZIU9IXyGm9aL67+8uDhM/EzAZBgkr
BgEEAYI3FAIEDB4KAFMAdQBiAEMAQTAOBgNVHQ8BAf8EBAMCAYYwDwYDVR0TAQH/
BAUwAwEB/zAfBgNVHSMEGDAWgBTvo1P6OP4LXm9RDv5MbIMk8jnOfDCB3QYDVR0f
BIHVMIHSMIHPoIHMoIHJhoHGbGRhcDovLy9DTj1zb3BoaWEtV0lOLTNTMThKQzNM
TTJBLUNBLENOPVdJTi0zUzE4SkMzTE0yQSxDTj1DRFAsQ049UHVibGljJTIwS2V5
JTIwU2VydmljZXMsQ049U2VydmljZXMsQ049Q29uZmlndXJhdGlvbixEQz1zb3Bo
aWEsREM9bGk/Y2VydGlmaWNhdGVSZXZvY2F0aW9uTGlzdD9iYXNlP29iamVjdENs
YXNzPWNSTERpc3RyaWJ1dGlvblBvaW50MIHJBggrBgEFBQcBAQSBvDCBuTCBtgYI
KwYBBQUHMAKGgalsZGFwOi8vL0NOPXNvcGhpYS1XSU4tM1MxOEpDM0xNMkEtQ0Es
Q049QUlBLENOPVB1YmxpYyUyMEtleSUyMFNlcnZpY2VzLENOPVNlcnZpY2VzLENO
PUNvbmZpZ3VyYXRpb24sREM9c29waGlhLERDPWxpP2NBQ2VydGlmaWNhdGU/YmFz
ZT9vYmplY3RDbGFzcz1jZXJ0aWZpY2F0aW9uQXV0aG9yaXR5MA0GCSqGSIb3DQEB
BQUAA4IBAQBj/+rX+9NJiSZq1YwQXkLq6+LUh7OkCoeCHHfBGUaS+gvbYQ5OVwJI
TlPTj4YNh62A6pUXplo8mdxKxOmZeRLTYgf9Q/SiOY+qoxJ5zNliSqlRU4E02sRz
wrzfaQpLGgyHXsyK1ABOGRgGqqWqZ7oXoKMRNmO+eu3NzBs4AVAAfL8UhFCv4IVx
/t6qIHY6YkNMVByjZ3MdFmohepN5CHZUHIvrOv9eAiv6+Vaan2nTeynyy7WnEv7P
+5L2kEFOSfnL4Zt2tEMqc5WyX6yjxDWmII0DTSyRshmxAoYlo3EJHwW+fIocdmIS
hgWDzioZ70SM9mJqNReHMC1jL3FD2nge
-----END CERTIFICATE-----

Trustpoint 'SUBCA1' is a subordinate CA and holds a non self signed cert
Certificate has the following attributes:
Fingerprint MD5: C420B7BB 88A2545F E26B0875 37D9EB45
Fingerprint SHA1: 110AF87E 53E6D1C2 19404BA5 0149C5CA 2CF2BE1C

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported

CUBE-2(config)#
CUBE-2(config)#crypto pki authenticate ROOT

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIDezCCAmOgAwIBAgIQMVF/OWq+ELxFC2IdUGvd2jANBgkqhkiG9w0BAQUFADBQ
MRIwEAYKCZImiZPyLGQBGRYCbGkxFjAUBgoJkiaJk/IsZAEZFgZzb3BoaWExIjAg
BgNVBAMTGXNvcGhpYS1XSU4tM1MxOEpDM0xNMkEtQ0EwHhcNMTQwOTEzMjMzODA2
WhcNMTkwOTEzMjM0ODA1WjBQMRIwEAYKCZImiZPyLGQBGRYCbGkxFjAUBgoJkiaJ
k/IsZAEZFgZzb3BoaWExIjAgBgNVBAMTGXNvcGhpYS1XSU4tM1MxOEpDM0xNMkEt
Q0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC4aywr1oOpTdTrM8Ya
R3RkcahbbhR3q7P1luTDUDNM5Pi6P8z3MckfjB/yy6SWr1QnddhyvMG6IGNtVxJ4
eyw0c7jbArXWOemGLOt454A0mCfcbwMhjQBycg9SM1r1Umzad7kOCzj/rD6hMbC4
jXpg6uU8g7eB3LzN1XF93DHjxYCBKMIeG45pqmsOc3mUj1CbCtnYXgno+mfhNzhR
HSth02z4XlGm99v46j/PqGjNRq4WKCwDc45SG3QjJDqDxnRJPKtRdNva66UJfDJp
```

```
4YMXQxOSkKMtDEDhH/Eic7CrJ3EywpUpMZAmqh4bmQ7Vo2pnRTbYdaAv/+yr8sMj
+FU3AgMBAAGjUTBPMAsGA1UdDwQEAwIBhjAPBgNVHRMBAf8EBTADAQH/MB0GA1Ud
DgQWBBTvo1P6OP4LXm9RDv5MbIMk8jnOfDAQBgkrBgEEAYI3FQEEAwIBADANBgkq
hkiG9w0BAQUFAAOCAQEAmd7hJ2EEUmuMZrc/qtSJ223loJlpKEPMVi7CrodtWSgu
5mNt1XsgxijYMqD5gJe1oq5dmv7efYvOvI2WTCXfwOBJ0on8tgLFwp1+SUJWs95m
OXTyoS9krsI2G2kQkjQWniMqPdNxpmJ3C4WvQLPLwtEOSRZRBvsKy6lczrgrV2mZ
kx12n5YGrGcXSblPPUddlJep1l8U+AQC8wkSzfJu0yHJwoH+lrIfgqKUee4x7z6s
SCaGddCYr3OK/3Wzs/WjSO2UETvNL3NEtWHDc2t4Y7mmIMSDvGjHZUgGZotwc9kt
9f2dZA0rtgBq4IDtpxkR3CQaauB7wUCpzemHzf+z9Q==
-----END CERTIFICATE-----

Certificate has the following attributes:
Fingerprint MD5: 511E1008 6D315E03 4B748601 7EE1A0E5
Fingerprint SHA1: 8C35D9FA 8F7A00AC 0AA2FCA8 AAC22D5F D08790BB

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported

CUBE-2(config)#
```

6.导入CUBE签名的证书。

在记事本中打开证书，将内容从BEGIN CERTIFICATE REQUEST复制并粘贴到END CERTIFICATE REQUEST。

```
CUBE-2(config)#crypto pki import SUBCA1 certificate

Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIEAjCCAuqgAwIBAgIKQZZrHQABAAAAEzANBgkqhkiG9w0BAQUFADBJMRIwEAYK
CZImiZPyLGQBGRYCbGkxFjAUBgoJkiaJk/IsZAEZFgZzb3BoaWExGzAZBgNVBAMT
EnNvcGhpYS1FWENIMjAxMC1DQTAeFw0xNTA0MDEwMDEzNDFaFw0xNjA0MDEwMDIz
NDFaMBExDzANBgNVBAMTBkNVQkUtMjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBAMCZW+5968CDWKkqfwWFaMWU01QUyqSCHYKvUgxX6i9HYfI9MXCCvRcO
FkcxKycHDrtO3N7cRvHGhq5wFBwgBJniF1NIiCPEb71hBpwub0xel/EenmRwgLNJ
9KWWtN7ECtNCCVbz6sStimTZMc3VLQ8LhxGUHChQKAH/4oIOSMmRTLx4Jf4aZ37p
6FEoRDkd0UcR9SvmFz/v+kGWIeJ600pLFgQ6v1NVk+JEmu2lQ8xExkSVFSbsajEG
sJYhdV28QAYLRep3VlUuVPPPaxBAOq8n18w3p+eAq/Z4+v5/mp6NZXMY7QMVVCzT
LnH5iX6kdux1XWFJKc+kmTpNpoGZfzcCAwEAAaOCASIwggEeMA4GA1UdDwEB/wQE
AwIFoDAdBgNVHQ4EFgQU9PbHMHSkYrjJ2+/+hSSMEoma0QIwHwYDVR0jBBgwFoAU
rHWCWSFPSF8hpvWi+u/vLg4TPxMwTwYDVR0fBEgwRjBEoEKgQIY+ZmlsZTovL0VY
Q0gyMDEwLnNvcGhpYS5saS9DZXJ0RW5yb2xsL3NvcGhpYS1FWENIMjAxMC1DQSgx
KS5jcmwwbQYIKwYBBQUHAQEEYTBfMF0GCCsGAQUFBzAChlFmaWxlOi8vRVhDSDIw
MTAuc29waGlhLmxpL0NlcnRFbnJvbGwvRVhDSDIwMTAuc29waGlhLmxpX3NvcGhp
YS1FWENIMjAxMC1DQSgxKS5jcnQwDAYDVR0TAQH/BAIwADANBgkqhkiG9w0BAQUF
AAOCAQEAe7EAoXKIAij4vxZuxROOFOfsmjcojU31ac5nrLCbq/FyW7eNblphL0NI
Dt/DlfZ5WK2q3Di+/UL1lDt3KYt9NZ1dLpmccnipbbNZ5LXLoHDkLNqt3qtLfKjv
J6GnnWCxLM18lxm1DzZT8VQtiQk5XZ8SC78hbTFtPxGZvfX70v22hekkOL1Dqw4h
/3mtaqxfnslB/J3Fgps1och45BndGiMAWavzRjjOKQaVLgVRvVrPIy3ZKDBaUleR
gsy5uODVSrhwMo3z84r+f03k4QarecgwZE+KfXoTpTAfhiCbLKw0ZyRMXXzWqNfl
iotEQbs52neCwXNwV24aOCChQMw2xw==
-----END CERTIFICATE-----

% Router Certificate successfully imported

CUBE-2(config)#
```

7.将TCP TLS配置为传输协议。

这可以在全局级别或拨号对等体级别执行。

```
 voice service voip
sip
session transport tcp tls
```

8.为sip-ua分配信任点，此信任点将用于CUBE和CUCM之间的所有sip信令：

```
 sip-ua
crypto signaling remote-addr <cucm pub ip address> 255.255.255.255 trustpoint SUBCA1
crypto signaling remote-addr <cucm sub ip address> 255.255.255.255 trustpoint SUBCA1
```

或者，可以为来自多维数据集的所有sip信令配置默认信任点：

```
 sip-ua
crypto signaling default trustpoint SUBCA1
```

9.启用SRTP。

这可以在全局级别或拨号对等体级别执行。

```
Voice service voip
srtp fallback
```

10.对于SRTP和实时传输协议(RTP)网际互联，需要安全转码器。

如果Cisco IOS®版本为15.2.2T(CUBE 9.0)或更高版本，则可以配置本地转码接口(LTI)转码器以最小化配置。

LTI转码器不需要SRTP-RTP呼叫的公钥基础设施(PKI)信任点配置。

```
 dspfarm profile 1 transcode universal security
codec g711ulaw
codec g711alaw
codec g729ar8
codec g729abr8
maximum sessions 10
associate application CUBE
```

如果Cisco IOS®低于15.2.2T，则配置SCCP转码器。

SCCP转码器需要信令信任点，但是，如果使用同一路由器托管转码器，则同一信任点(SUBCA1)可用于CUBE和转码器。

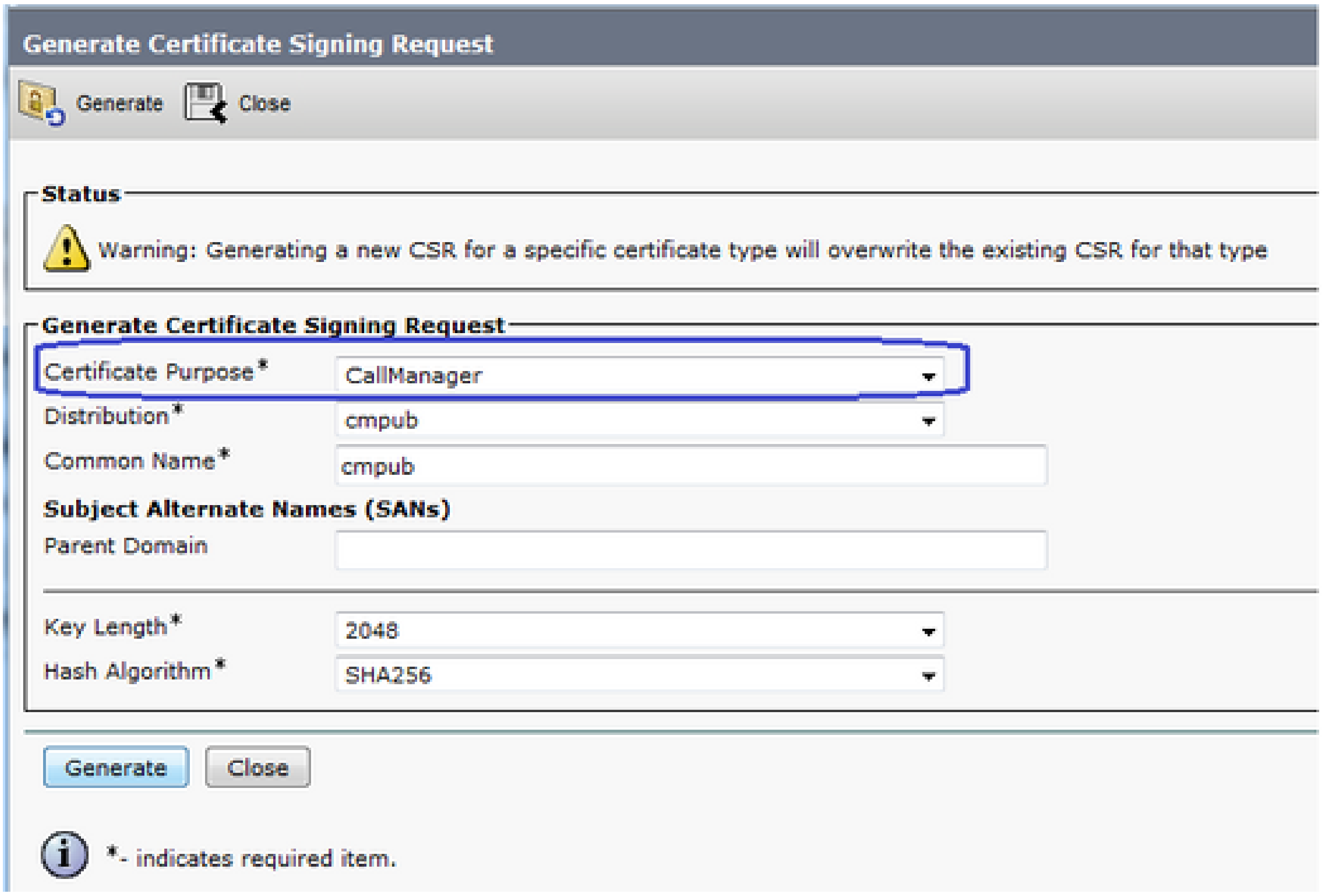
```
sccp local GigabitEthernet0/2
sccp ccm 10.106.95.153 identifier 1 priority 1 version 7.0
sccp
!
sccp ccm group 1
bind interface GigabitEthernet0/0
associate ccm 1 priority 1
associate profile 2 register secxcode
!
dspfarm profile 2 transcode universal security
```

```
trustpoint SUBCA1
codec g711ulaw
codec g711alaw
codec g729ar8
codec g729abr8
maximum sessions 10
associate application SCCP

telephony-service
secure-signaling trustpoint SUBCA1
sdspfarm units 1
sdspfarm transcode sessions 10
sdspfarm tag 1 secxcode
max-ephones 1
max-dn 1
ip source-address 10.106.95.153 port 2000
max-conferences 8 gain -6
transfer-system full-consult
```

配置CUCM

1.在所有CUCM节点上生成CallManager CSR。

导航至**CM OS Administration > Security > Certificate Management > Generate Certificate Signing Request**，如图所示。



Generate Certificate Signing Request

Status

Warning: Generating a new CSR for a specific certificate type will overwrite the existing CSR for that type

Generate Certificate Signing Request

Certificate Purpose* CallManager

Distribution* cmpub

Common Name* cmpub

Subject Alternate Names (SANs)

Parent Domain

Key Length* 2048

Hash Algorithm* SHA256

*- indicates required item.

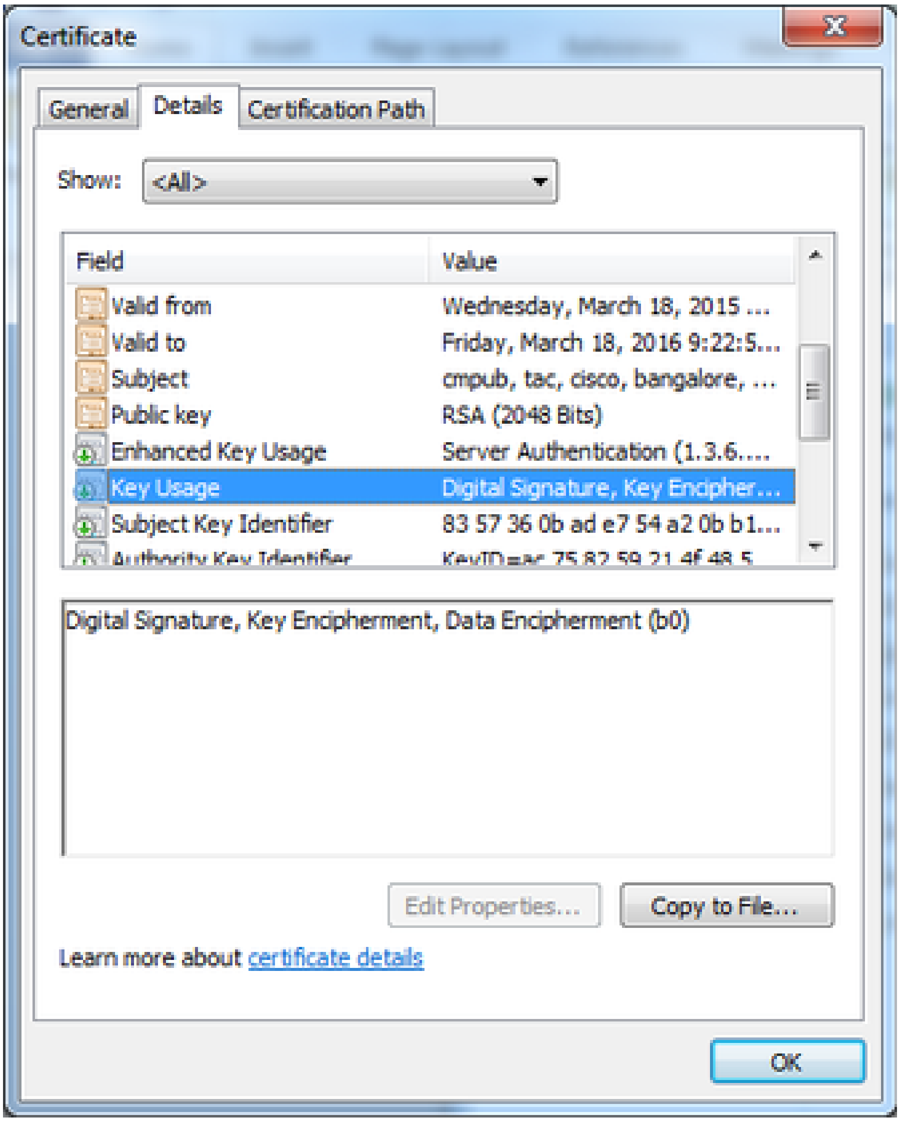
CallManager CSR将具有以下关键属性：

```
Requested Extensions:
X509v3 Extended Key Usage:
TLS Web Server Authentication, TLS Web Client Authentication, IPSec End System
```

```
X509v3 Key Usage:
Digital Signature, Key Encipherment, Data Encipherment, Key Agreement
```

2.获取由从属CA签名的所有CM节点的CallManager证书。

使用步骤1中生成的CSR。任何Web服务器证书模板都会工作，确保签名证书至少具有以下密钥使用属性：**数字签名、密钥加密、数**据加密，如图所示。

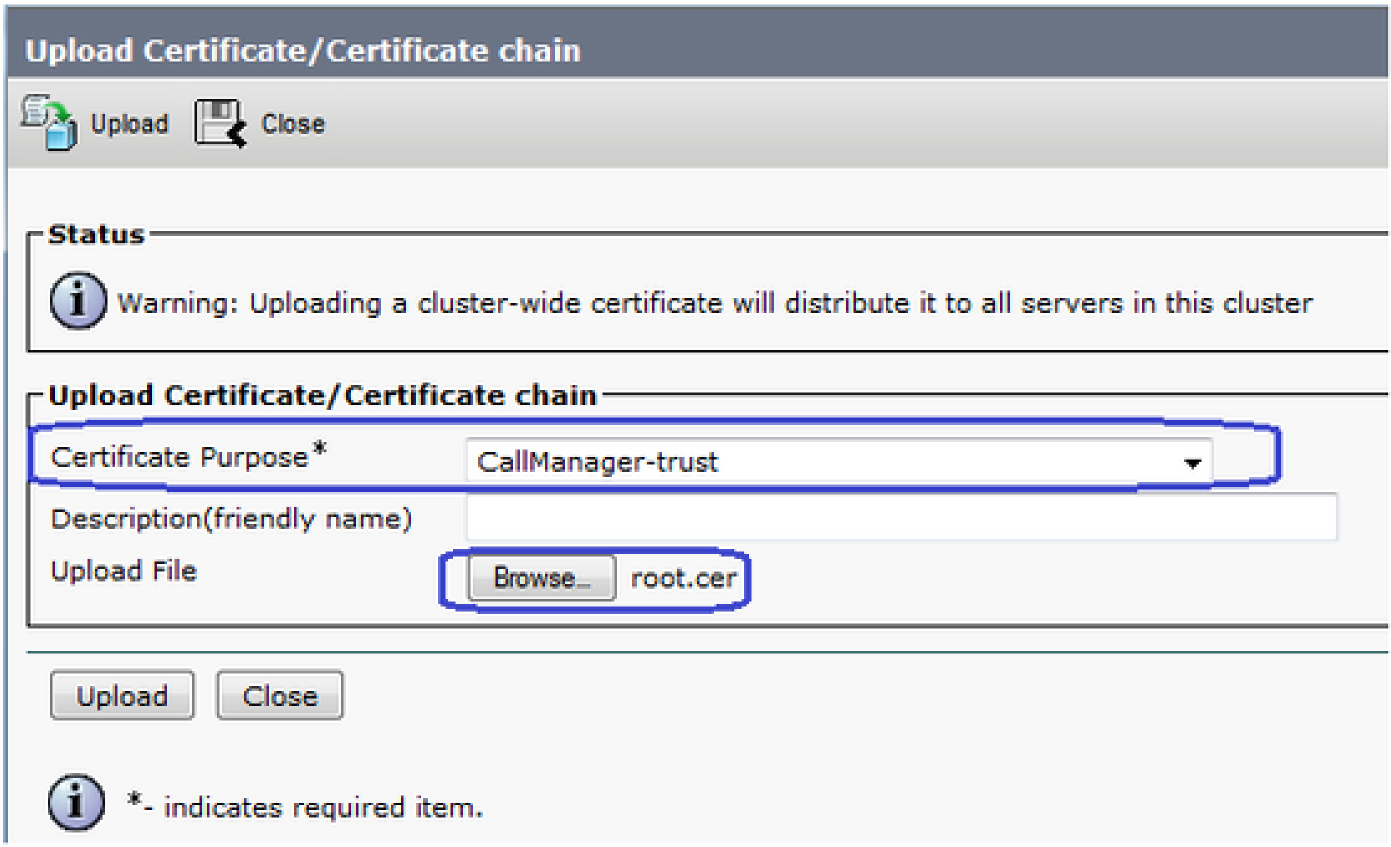


Field	Value
Valid from	Wednesday, March 18, 2015 ...
Valid to	Friday, March 18, 2016 9:22:5...
Subject	cmpub, tac, cisco, bangalore, ...
Public key	RSA (2048 Bits)
Enhanced Key Usage	Server Authentication (1.3.6....
Key Usage	Digital Signature, Key Encipher...
Subject Key Identifier	83 57 36 0b ad e7 54 a2 0b b1...
Authority Key Identifier	KeyID=ac 75 82 59 21 4f 48 5

Digital Signature, Key Encipherment, Data Encipherment (b0)

3.从根CA和从属CA上传CA证书作为CallManager-Trust。

导航至**CM OS Administration > Security > Certificate Management > Upload Certificate/Certificate链**，如图所示。


Upload Certificate/Certificate chain

Status

Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster

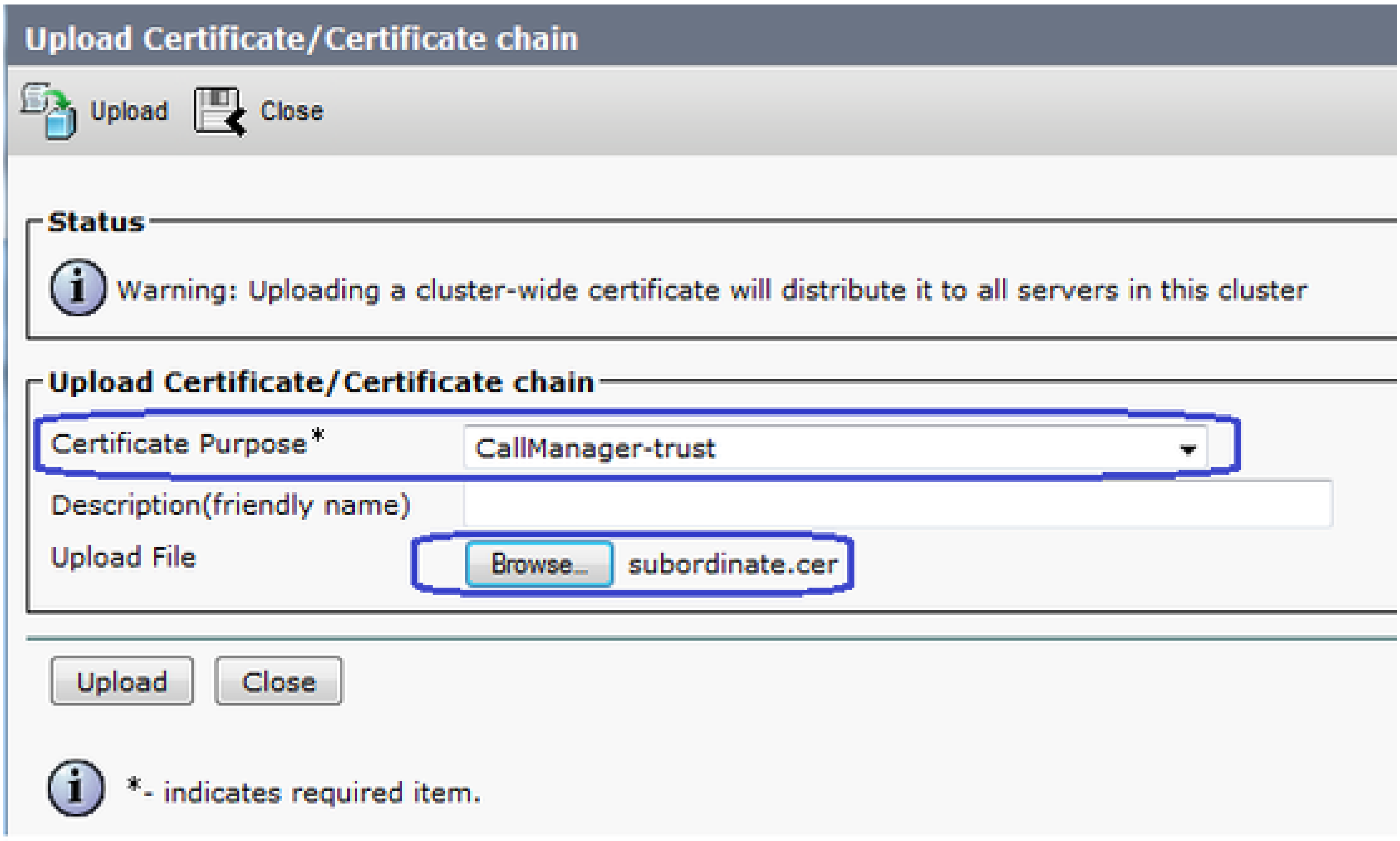
Upload Certificate/Certificate chain

Certificate Purpose* CallManager-trust

Description(friendly name)

Upload File Browse... root.cer

*- indicates required item.


Upload Certificate/Certificate chain

Status

Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster

Upload Certificate/Certificate chain

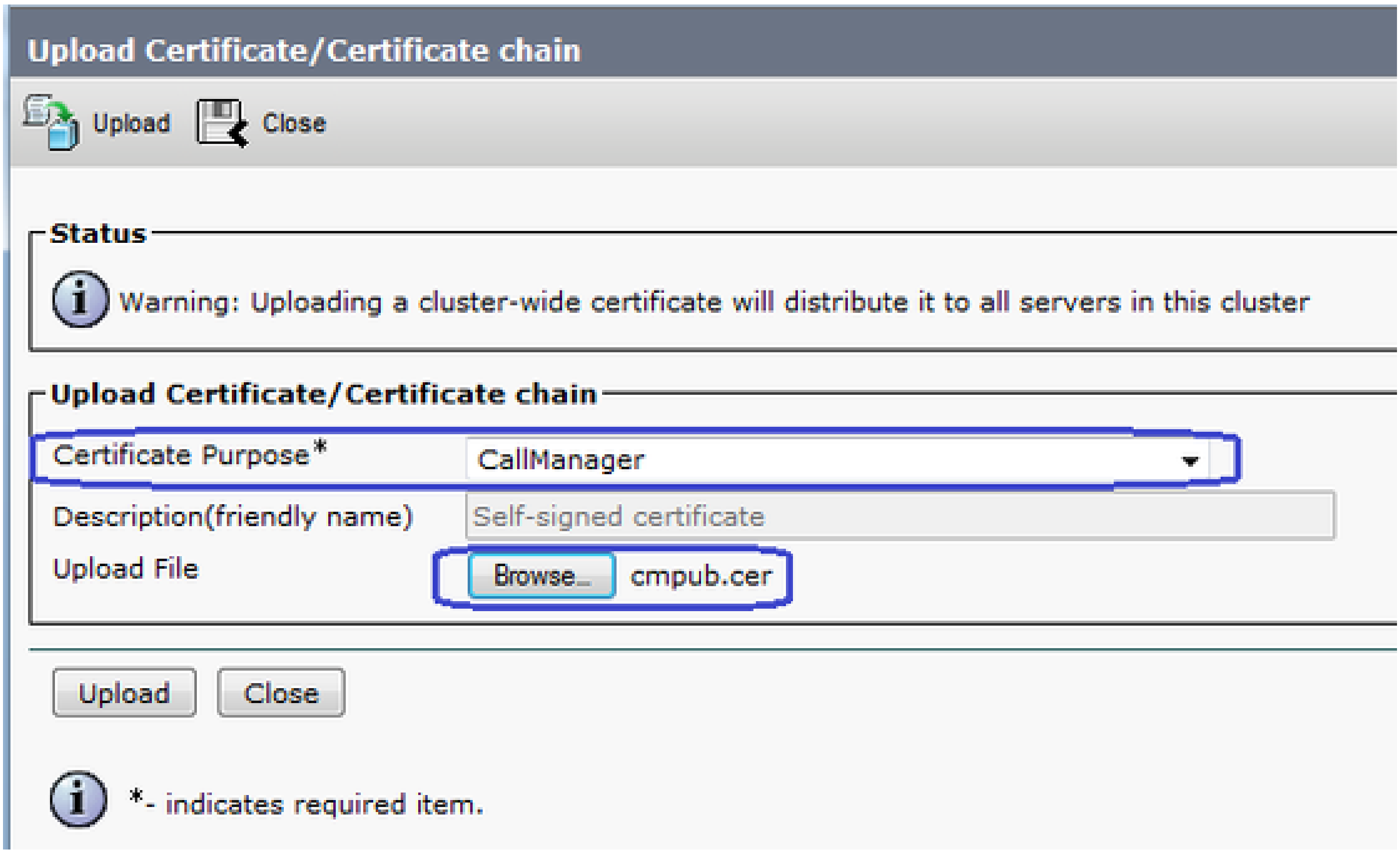
Certificate Purpose* CallManager-trust

Description(friendly name)

Upload File Browse... subordinate.cer

*- indicates required item.

4.如图所示，将CallManager签名证书上载为CallManager。



Upload Certificate/Certificate chain

Status

Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster

Upload Certificate/Certificate chain

Certificate Purpose* CallManager

Description(friendly name) Self-signed certificate

Upload File Browse... cmpub.cer

*- indicates required item.

5.在发布服务器上更新证书信任列表(CTL)文件（通过CLI）。

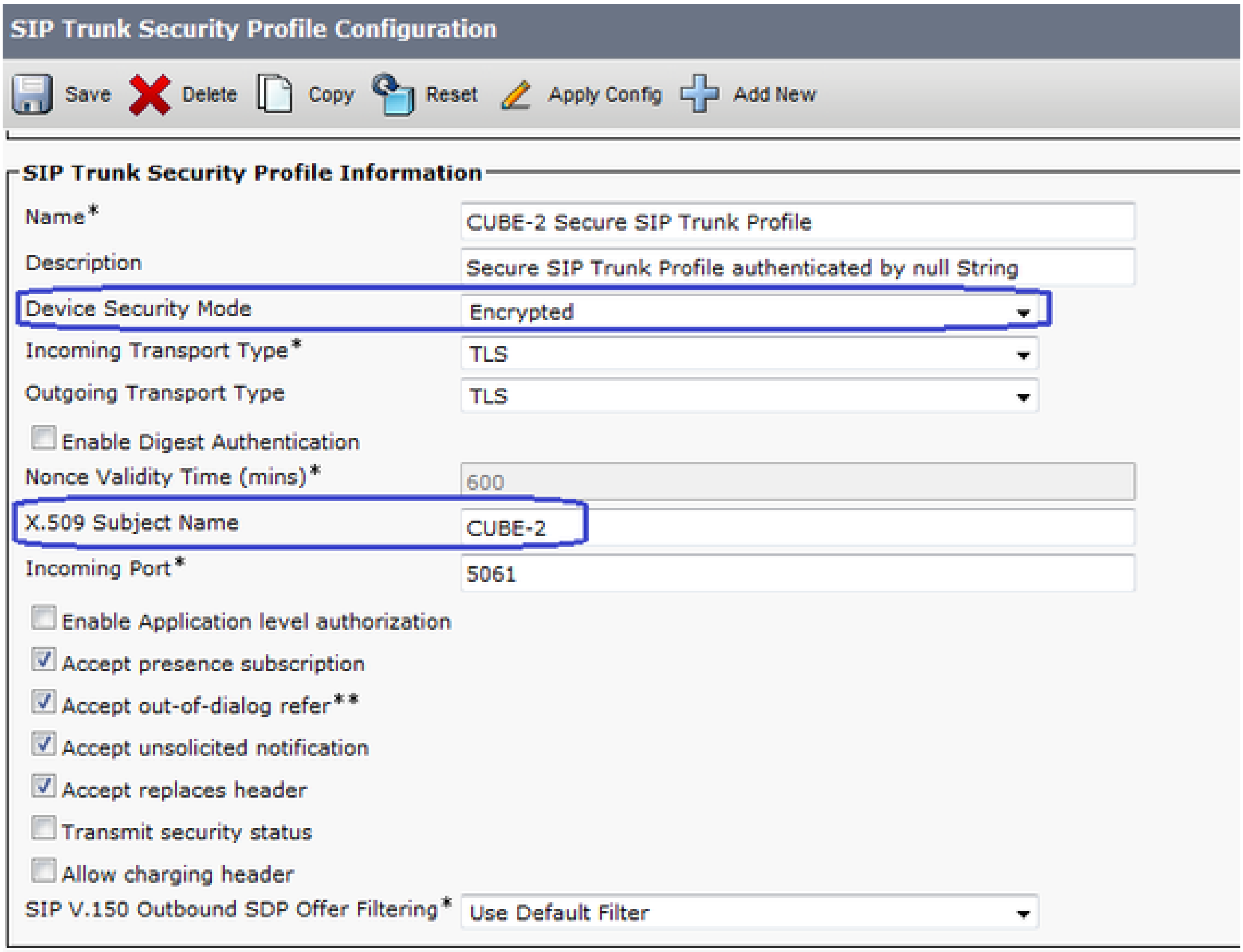
```
admin:utils ctl update CTLFile
This operation will update the CTLFile. Do you want to continue? (y/n):

Updating CTL file
CTL file Updated
Please Restart the TFTP and Cisco CallManager services on all nodes in the cluster that run
these services
admin:
```

6. 在所有节点上重新启动CallManager和TFTP服务，在发布服务器上重新启动CAPF服务。

7.创建新的SIP中继安全配置文件。

在CM Administration上，导航至**System > Security > SIP Trunk Security Profiles > Find**。

复制现有非安全SIP中继配置文件以创建新的安全配置文件，如此映像所示。

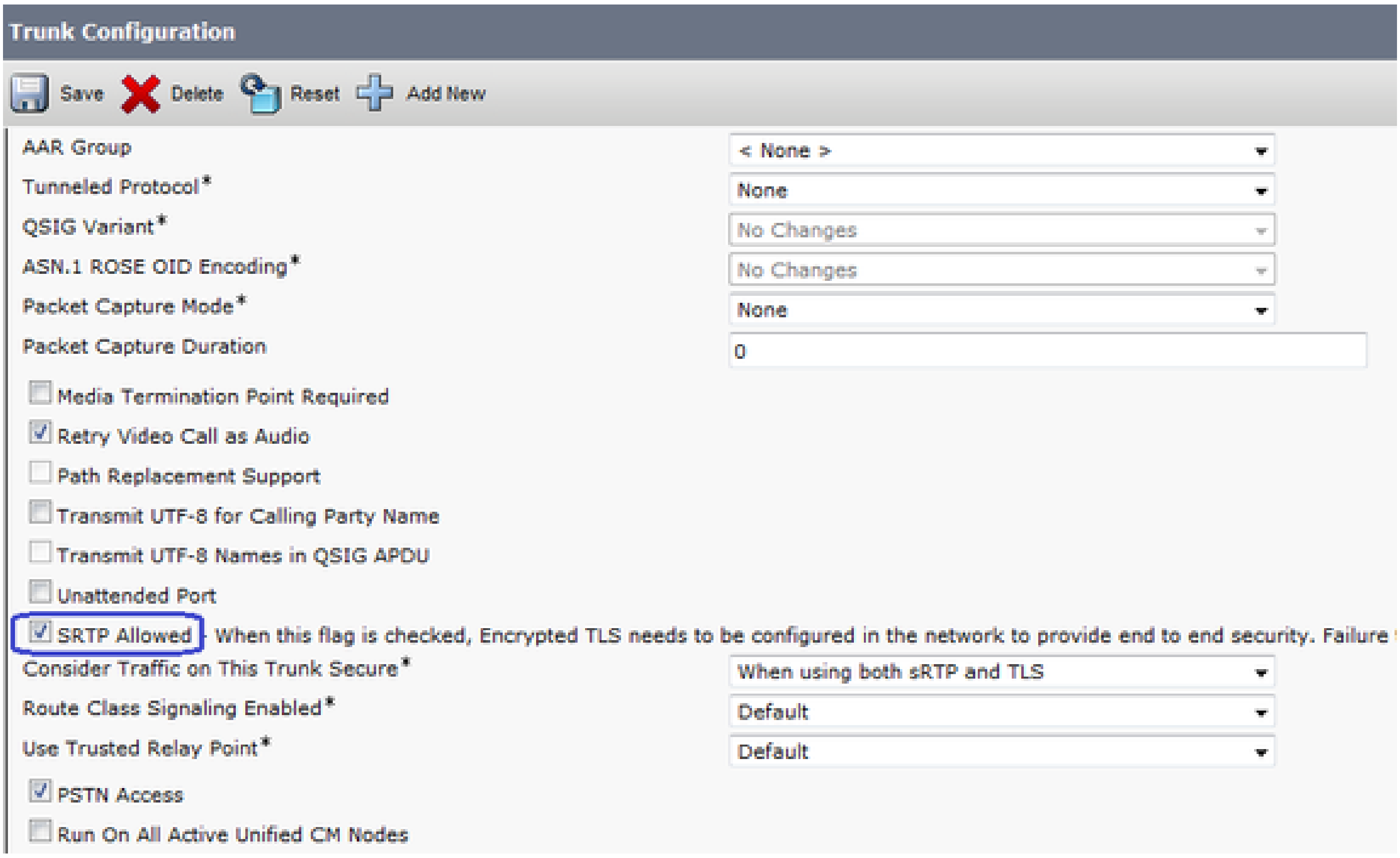


SIP Trunk Security Profile Information

Name*	CUBE-2 Secure SIP Trunk Profile
Description	Secure SIP Trunk Profile authenticated by null String
Device Security Mode	Encrypted
Incoming Transport Type*	TLS
Outgoing Transport Type	TLS
□ Enable Digest Authentication	
Nonce Validity Time (mins)*	600
X.509 Subject Name	CUBE-2
Incoming Port*	5061
□ Enable Application level authorization	
☑ Accept presence subscription	
☑ Accept out-of-dialog refer**	
☑ Accept unsolicited notification	
☑ Accept replaces header	
□ Transmit security status	
□ Allow charging header	
SIP V.150 Outbound SDP Offer Filtering*	Use Default Filter

8. 创建到CUBE的SIP中继。

如图所示，在SIP中继上启用SRTP允许。



Trunk Configuration

AAR Group: < None >

Tunneled Protocol*: None

QSIG Variant*: No Changes

ASN.1 ROSE OID Encoding*: No Changes

Packet Capture Mode*: None

Packet Capture Duration: 0

□ Media Termination Point Required

☑ Retry Video Call as Audio

□ Path Replacement Support

□ Transmit UTF-8 for Calling Party Name

□ Transmit UTF-8 Names in QSIG APDU

□ Unattended Port

☑ SRTP Allowed - When this flag is checked, Encrypted TLS needs to be configured in the network to provide end to end security. Failure

Consider Traffic on This Trunk Secure*: When using both sRTP and TLS

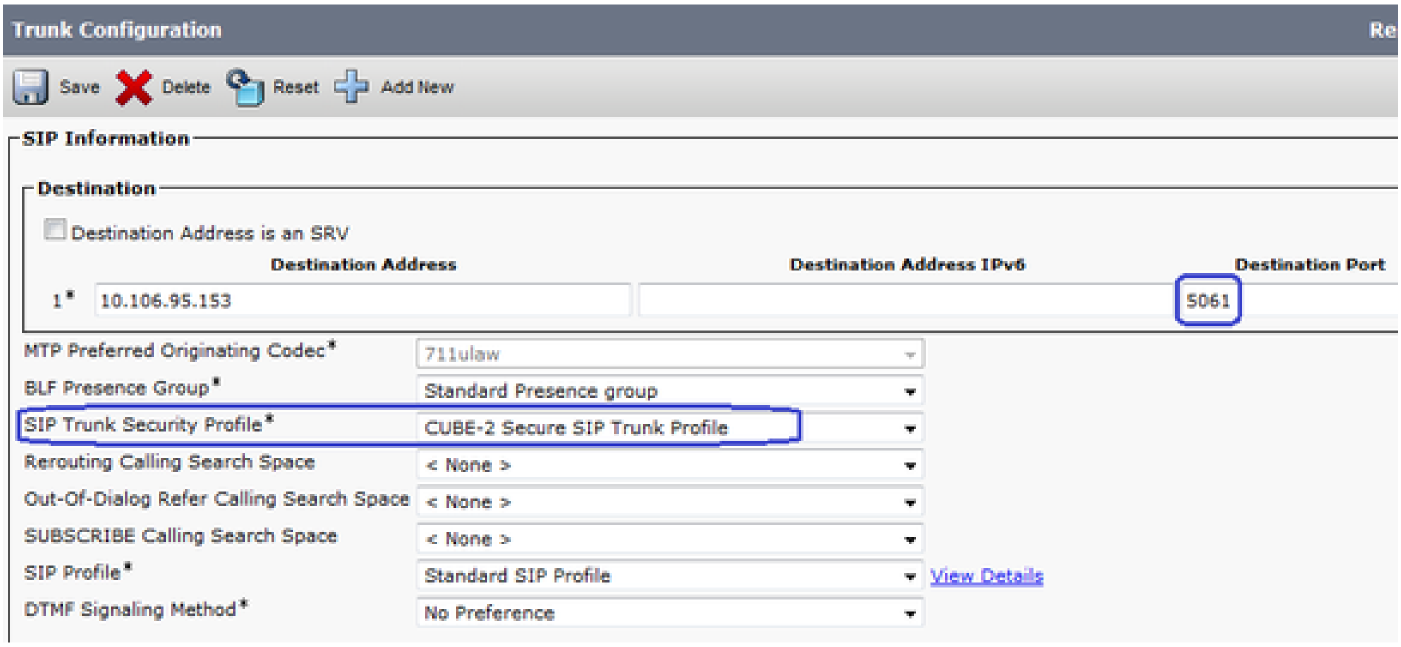
Route Class Signaling Enabled*: Default

Use Trusted Relay Point*: Default

☑ PSTN Access

□ Run On All Active Unified CM Nodes

配置目标端口5061(TLS)并在SIP中继上应用新安全SIP中继安全配置文件，如图所示。



Trunk Configuration

SIP Information

Destination

□ Destination Address is an SRV

	Destination Address	Destination Address IPv6	Destination Port
1*	10.106.95.153		5061

MTP Preferred Originating Codec*: 711ulaw

BLF Presence Group*: Standard Presence group

SIP Trunk Security Profile*: CUBE-2 Secure SIP Trunk Profile

Rerouting Calling Search Space: < None >

Out-Of-Dialog Refer Calling Search Space: < None >

SUBSCRIBE Calling Search Space: < None >

SIP Profile*: Standard SIP Profile View Details

DTMF Signaling Method*: No Preference

验证

使用本部分可确认配置能否正常运行。

```
show sip-ua connections tcp tls detail
show call active voice brief
```

```
e.g.

Secure-CUBE#show sip-ua connections tcp tls detail
Total active connections : 2
No. of send failures : 0
No. of remote closures : 13
No. of conn. failures : 0
No. of inactive conn. ageouts : 0
TLS client handshake failures : 0
TLS server handshake failures : 0

---------Printing Detailed Connection Report---------
Note:
** Tuples with no matching socket entry
- Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port>'
to overcome this error condition
++ Tuples with mismatched address/port entry
- Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port> id <connid>'
to overcome this error condition

Remote-Agent:10.106.95.151, Connections-Count:2
Remote-Port Conn-Id Conn-State WriteQ-Size Local-Address
=========== ======= =========== ========== ===========
5061 16 Established 0 10.106.95.153
57396 17 Established 0 10.106.95.153


-------------- SIP Transport Layer Listen Sockets ---------------
Conn-Id Local-Address
=========== ============================
2 [10.106.95.153]:5061
```

使用LTI转码器时，会捕获show call active voice brief命令的输出。

```
Telephony call-legs: 0
SIP call-legs: 2
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 2
1283 : 33 357052840ms.1 (23:57:23.929 IST Sun Feb 15 2015) +2270 pid:3 Answer 3001 active
dur 00:00:08 tx:383/61280 rx:371/59360 dscp:0 media:0 audio tos:0xB8 video tos:0x0
IP 10.106.95.132:17172 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay:
off Transcoded: Yes
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a
LostPacketRate:0.00 OutOfOrderRate:0.00

1283 : 34 357052840ms.2 (23:57:23.929 IST Sun Feb 15 2015) +2270 pid:1 Originate 2001 active
dur 00:00:08 tx:371/60844 rx:383/62812 dscp:0 media:0 audio tos:0xB8 video tos:0x0
IP 10.65.58.24:24584 SRTP: on rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off
Transcoded: Yes
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a
LostPacketRate:0.00 OutOfOrderRate:0.00
```

此外，当在Cisco IP电话和CUBE或网关之间进行SRTP加密呼叫时，IP电话上会显示锁图标。

故障排除

本部分提供了可用于对配置进行故障排除的信息。

这些调试有助于排除PKI/TLS/SIP/SRTP问题。

```
debug crypto pki{ API | callbacks | messages | scep | server | transactions | validation }
debug ssl openssl { errors | ext | msg | states }
debug srtp {api | events }
debug ccsip {messages | error | events | states | all }
debug voip ccapi inout
```