

配置并且排除SIP的TLS和SRTP企业CA (第三方CA)签名的证书故障在CUCM、IP电话和多维数据集之间

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[背景信息](#)

[Configure](#)

[Network Diagram](#)

[配置多维数据集](#)

[配置CUCM](#)

[Verify](#)

[Troubleshoot](#)

Introduction

本文描述配置示例会话初始化协议(SIP)传输层安全(TLS)和安全的实时传输协议(SRTP)在Cisco Unified通信管理器(CUCM)，IP电话和Cisco Unified Border Element (多维数据集)之间与包括Cisco通信设备类似IP电话、CUCM、网关和多维数据集的使用企业Certificate Authority (CA) (第三方CA)签名的证书和使用普通的企业CA签署证书所有网络组件的。

Prerequisites

Requirements

Cisco 建议您了解以下主题：

- 企业配置CA服务器
- CUCM簇在混合模式被配置，并且IP电话在安全模式注册(被加密)
- 多维数据集基本的语音服务VoIP和Dial Peer配置被执行

Components Used

本文档中的信息基于以下软件和硬件版本：

- Windows 2008服务器-认证机关
- CUCM 10.5
- 多维数据集-与Cisco IOS的3925E 15.3(3) M3
- CIPC

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.

背景信息

在多维数据集的安全的语音通信可以分开成两部分

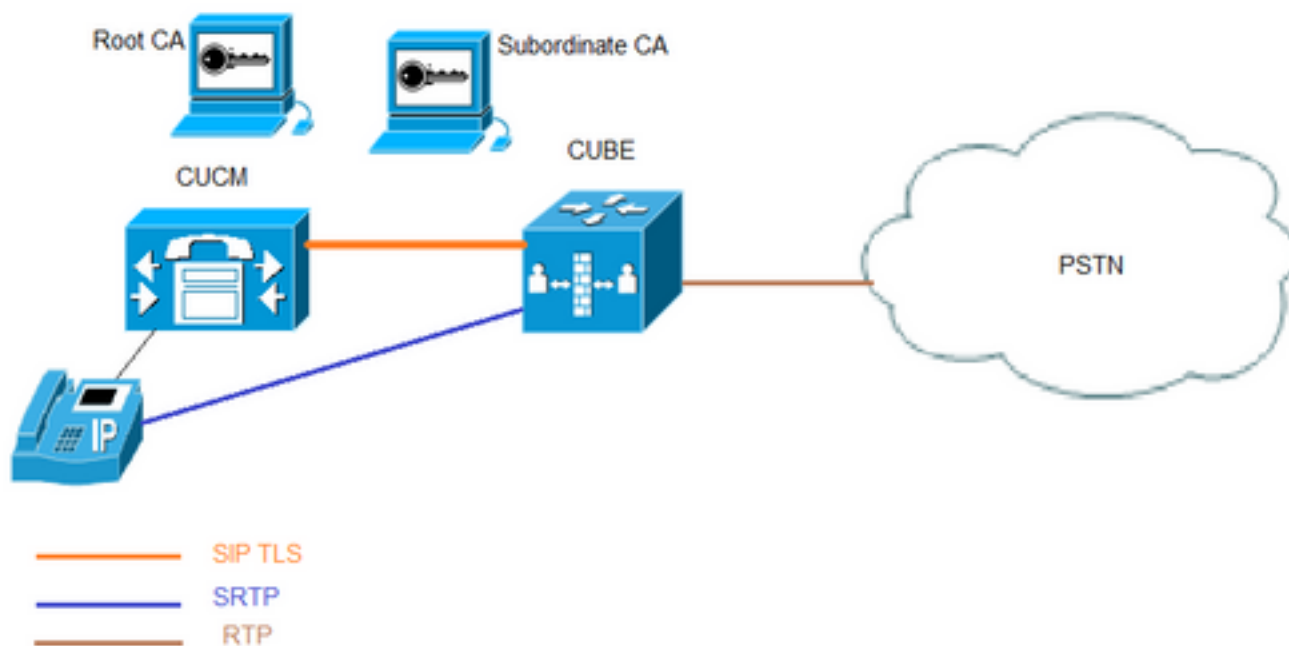
- 获取信令-求使用TLS的立方获取在SIP和互联网协议安全(IPSec)为了获取发信号的发信号在H.323
- 获取媒体-获取实时传输协议(SRTP)

CUCM认证机关代理功能(CAPF)提供局部重要的认证(LSC)给电话。因此，当CAPF由外部CA时签字，它作为电话的辅助CA。

为了知道如何获得CA签名的CAPF，请参见以下：

Configure

Network Diagram



在此设置，使用根CA和一个辅助CA。所有CUCM和多维数据集证书由辅助CA签字。

配置多维数据集

生成一RSA密钥对。

此步骤生成专用和公共密钥。

在本例中，多维数据集是标签，这可以是任何。

```
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. 创建辅助CA和根CA的一信任点，辅助CA信任点使用SIP TLS通信。

在本例中，信任点名字对于辅助CA是SUBCA1，并且对于根CA它是ROOT。

```
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)#
```

用于此步骤的主题名称在CUCM SIP Trunk安全配置文件的X.509主题名称必须配比。(如果域名是启用的)，最佳实践是使用主机名以域名。

关联在Step1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
rsaкеypair CUBE
```

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

3. 生成多维数据集认证署名请求(CSR)。

crypto pki登记提供给企业CA为了获得签名的证书的命令生产CSR。

```
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
VUJFLTIwggeiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAAoIBAQDAmVvufevAg1ip
Kn8FhWjFlnNUFMqkggh2Cr1IMV+ovR2HyPTFwgr0XDhZHMSSnBw67Ttze3Ebxxoau
cBQcIASZ4hdTSIgjxG+9YQacLm9MXpfxHp5kcICzSfS1lrTexArTQglW8+rErYpk
2THN1S0PC4crlBwoUCgB/+KCDkjJkUy8eCX+Gmd+6ehRKEQ5HdFHEfUr5hc/7/pB
```

```
liHietNKSxYEOr9TVZPiRjRtpUPMRMZE1RUm7GoxBrCWIXVdvEAGC0Xqd1ZVL1Tz
z2sQQDqvJ9fMN6fngKv2ePr+f5qe jWVzGO0DFVQs0y5x+Yl+pHbsdV1hSSnPPjk6
TaaBmX83AgMBAAGgITafBgkqhkiG9w0BCQ4xEjAQMA4GA1UdDwEB/wQEAwIFoDAN
BgkqhkiG9w0BAQUFAAOCAQEAQArWMJbdhlU8VfaF1cMJibr569BZT+tIjQOz3OqNGQ
QpzHwclLoaKuC5pc/u0hw14MGS6Z440Iw4zK2/5bb/KL47r8H3d7T7PYMfK61AzK
sU9Kf96zTvHNWl9wXImB5blJfRLXnFWXNsVEF4FjU74plxJL7siasa5e86eNy9deN
20iKjvP8o4MgWewILrD01YZMDMDS1Uy82kWI6hvXG5+xBT5A1lo2xCj1S9y6/D4d
f0ilDZvaQk+7jjBCzLv5hET+1neoQBw52e7RWU8s2biQw+7TEAd08NytF3q/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)#
```

复制之间输出开始证书请求对END证书请求并且储存它在记事本文件。

多维数据集CSR将有这些关键属性：

```
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-----
MIICjjCCAxyCAQAwKDEPMA0GA1UEAxMQQ1VCRS0yMRUwEwYJKoZIhvcNAQkCFgZD
VUJFLTlWggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDAmVvufevAglip
Kn8FhWjFlnNUFMqkgh2Cr1IMV+ovR2HyPTfwgr0XDhZHMSSnBw67Ttze3Ebxoau
cBQcIASZ4hdTSIgjxG+9YQacLm9MXpfXhp5kcICzSfS1lrTexArTQglW8+rErYpk
2THN1S0PC4crlBwoUCGB/+KCDkjkUy8eCX+Gmd+6ehrKEQ5HdFHEfUr5hc/7/pB
liHietNKSxYEOr9TVZPiRjRtpUPMRMZE1RUm7GoxBrCWIXVdvEAGC0Xqd1ZVL1Tz
z2sQQDqvJ9fMN6fngKv2ePr+f5qe jWVzGO0DFVQs0y5x+Yl+pHbsdV1hSSnPPjk6
TaaBmX83AgMBAAGgITafBgkqhkiG9w0BCQ4xEjAQMA4GA1UdDwEB/wQEAwIFoDAN
BgkqhkiG9w0BAQUFAAOCAQEAQArWMJbdhlU8VfaF1cMJibr569BZT+tIjQOz3OqNGQ
QpzHwclLoaKuC5pc/u0hw14MGS6Z440Iw4zK2/5bb/KL47r8H3d7T7PYMfK61AzK
sU9Kf96zTvHNWl9wXImB5blJfRLXnFWXNsVEF4FjU74plxJL7siasa5e86eNy9deN
20iKjvP8o4MgWewILrD01YZMDMDS1Uy82kWI6hvXG5+xBT5A1lo2xCj1S9y6/D4d
f0ilDZvaQk+7jjBCzLv5hET+1neoQBw52e7RWU8s2biQw+7TEAd08NytF3q/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)#
```

4.从辅助CA获得CA证书根CA、然后CA证书和签字的多维数据集认证。

为了获得在第3.步签署了多维数据集认证，使用生成的CSR。镜像是从Microsoft CA Web服务器。

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
sU9Kf96zTvHNWl9wXImB5b1JfRLXnFWXNsVEF4Fj
20iKjvP8o4MgWewILrD01YZMDMDS1Uy82kWI6hvX
f0i1DZvaQk+7jjBCzLv5hET+1neoQBw52e7RWU8s
bUKw5wT4pgGUJcDAWej3ZLqP91g5yyd9MiCdCRY+
-----END CERTIFICATE REQUEST-----
```

Additional Attributes:

Attributes:

Submit >

5. 根CA和辅助CA导入CA证书。

打开在记事本的认证，并且复制和粘贴内容从开始证书请求对END证书请求。

```
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-----
```

```
MIIFhDCCBGygAwIBAgIKYZVFyQAAAAAFjANBgkqhkiG9w0BAQUFADBQMRwEAYK
CZImiZPyLQGQBGryCbGkxFjAUBgoJkiaJk/IsZAEZFgZzb3BoaWEExIjAgBgNVBAMT
GXNvcGhpYS1XSU4tM1MxOEpdM0xNMkEtQ0EwHhcNMTQwOTI1MDAwNzU2WhcNMTYw
OTI1MDAxNzU2WjBjMjRwEAYKZImiZPyLQGQBGryCbGkxFjAUBgoJkiaJk/IsZAEZ
FgZzb3BoaWEExGzAZBgNVBAMTEhNvcGhpYS1FWENIMjAxMjQ0ZDQ0TCASIDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBAAJK+Nmz4rieYfr9gH3ISTuYz3TWpafpJdJ7l
7kIwwc28TvJf15vrKEiaPyFzxL5TEHaWQ9YAo/WmdtuyF7aB+pLJlsoKcZxtrGv
gTmtuphcJ5Fpd4368lR8ZXJiAT/Dz+Nsh4PC9GUUKQeycyRDeOBz08vL5pLj/W99
b8UMU1VOqBu4e1ZwxWPMFxB7z0eYsCfXMnGFUlp3HFdWZczgK3ldNO9I0X+p70UP
R0CQpMEQxuheqv9kazI1JKfNH8N0q08IHl76Y32vUzLg3uvZgqWG6hGch/gjm4L/
1KmdZTNSH8H7Kf6vG6PNWrXWwLNkhrWaYeryHelIshEj7ZUeB8sCAwEAAAOCAmUw
ggJhMBIGCSsGAQQBgjcVAQQFAgMBAEEwIwYJKwYBBAGCNxUCBBYEFLnnd8HnCFKE
isPgI580og/LqwVSMB0GA1UdDgQWBBSsdYJZIU9IXyGm9aL67+8uDhM/EzAZBgkr
BgEEAYI3FAIEDB4KAFMADQBiAEMAQTAOBgNVHQ8BAf8EBAMCAYYwDwYDVR0TAQH/
BAUwAwEB/zAfBgNVHSMGDAWgBTvo1P6OP4LXm9RDv5MbIMk8jnOfDCB3QYDVR0f
BIHVMiHSMIHPOIHM0IHJhoHGGRhcDovLy9DTj1zb3BoaWEtV01OLTNTMTkKzNM
TTJBLUNBLENOPVdJTi0zUzE4SkMzTE0yQSxDtj1DRFAsQ049UHVibGljJTJwS2V5
JTIwU2VydmljZXMzQ049U2VydmljZXMzQ049Q29uZmlndXJhdGlvbixEQz1zb3Bo
aWEsREM9bGk/Y2VydGlmawNhdGV5Z2F0aW9uTG1zdD9iYXNlP29iamVjdENS
YXNzPWNSTERpc3RyaWJldGlvblBvaW50MIHJBggrBgEFBQcBAQSBvDCBuTCBtgYI
KwYBBQUHMAKGgalsZGFwOi8vL0NOPXNvcGhpYS1XSU4tM1MxOEpdM0xNMkEtQ0Es
Q049QU1BLENOPVBlYmtpYyUyMETleSUyMFNlcnZpY2VzLENOPVBlcnZpY2VzLENO
```

```
PUNvbmZpZ3VyYXRpb24sREM9c29waGhhLERDPWxpP2NBQ2VydGhmaWNhdGU/YmFz
ZT9vYmp1Y3RDbGFzc21jZXJ0aWZpY2F0aW9uQXV0aG9yaXR5MA0GCSqGSIB3DQEB
BQUAA4IBAQBj/+rX+9NjISZqlYwQXkLq6+LUh7OkCoeCHHfBGUaS+gvyYQ5OVwJI
TlPTj4Ynh62A6pUXplo8mdxKxOmZeRLTYgf9Q/SiOY+qoxJ5zNlISqlRU4E02sRz
wrzfaQpLggyHXsyK1ABOGRGgqQWz7oXoKMRNmO+eu3NzBs4AVAAfL8UhfCv4IVx
/t6qIHY6YkNMVByjz3MdFmohepN5CHZUHIvrOv9eAiv6+Vaan2nTeyny7WnEv7P
+5L2kEFOSfnL4Zt2tEMq5WyX6yJxDWmII0DTSyRshmxAoYl03EJHwW+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  
MRIwEAYKCZImiZPyLGBGRYCbGkxFljAUBgoJkiaJk/IsZAEZFgZzb3BoaWEwIjAg  
BgNVBAMTGXNvcGhpYS1XSU4tM1MxOEpmDM0xNMkEtQ0EwHhcNMTQwOTEzMTMzODAx  
WhcNMTEwOTEzMTMzODAxM1MxOEpmDM0xNMkEtQ0EwGgEiMA0GCSqGSIB3DQEB  
AQUAA4IBDwAwggEKAoIBAQc4aywr1oOpTdTTrM8YaR3Rkcahbbhr3q7P1luTDUDNM5P  
i6P8z3MckfjB/yy6SWr1QnddhvMG6IGNtVxJ4eyw0c7jBArXWOemGLOt454A0mCf  
cbwMhjQBycg9SM1r1Umzad7kOCzj/rD6hMbc4jXpg6uU8g7eB3LzN1XF93DHjxY  
CBKMIeG45pqmsOc3mUj1CbCtnYXgno+mfhNzhRHStH2z4XlGm99v46j/PqGjNRq4  
WKCwDc45SG3QjJDQDxnRJPkTRdNva66UJfDJp4YMXQxOSkKMTDEDhH/Eic7CrJ3E  
yWpUpMZAmqh4bmQ7Vo2pnRTbYdaAv/+yr8sMj+FU3AgMBAAGjUTBPMAsGA1UdDwQEA  
wIBhjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBTvo1P6OP4LXm9RDv5MbIMk8jnOf  
DAQBgkrBgEEAYI3FQEEAwIBADANBgkqhkiG9w0BAQUFAAOCAQEAmD7hJ2EEUmuMZrc/ct  
SJ2231oJlpKEPMVi7CrodtWSgu5mNt1Xsgxi jYMqD5gJe1oq5dmv7efYvOvI2WTCXf  
wOBJ0on8tgLFwpl+SUJWs95mOXTyoS9krsI2G2kQkjqWniMqPdNxpMj3C4WvQLPLwtE  
OSRZRBvsKy6lczrgrV2mZkx12n5YGrGcXSblPPUddlJep118U+AQC8wksZfJu0yHJwoH+lr  
IfgqKUee4x7z6sSCaGddCYr3OK/3Wzs/WjSO2UETvNL3NEtWHDC2t4Y7mmIMSDvGjH  
ZUGZotwc9kt9f2dZA0rtgBq4IDtpxkR3CQaaub7wUCpzemHzf+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. 导入多维数据集签名的证书。
```

打开在记事本的认证，并且复制和粘贴内容从开始证书请求对END证书请求。

```
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-----
MIIEAjCCAuqgAwIBAgIKQZrHQABAAAAEzANBgkqhkiG9w0BAQUFADBjMREwEAYK
CZImiZPYLQBGRYCbGkxJfAUBgoJkiaJk/IsZAEZFgZzb3BoaWExGzAZBgNVBAMT
EnNvcGhpYS1FWENIMjAxMClDQTAeFw0xNTA0MDEwMDEzNDFAFw0xNjA0MDEwMDIz
NDFAmBExDzANBgNVBAMTBkNVQkUtMjCCASIdQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBAMCZW+5968CDWkKqfWwFAMWU01QUyqSCHYKvUgxX6i9HYfI9MXCCvRcO
FkcxKycHDrT03N7cRvHGhq5wFBwgBJniF1NIiCPEb71hBpwub0xel/EenRwglNJ
9KWWtN7ECTNCCVbz6sStimTZMc3VLQ8LhxGUHChQKAH/4oIOSMmRTLx4Jf4aZ37p
6FEoRdkd0UcR9SvmFz/v+kGWIeJ600pLFgQ6v1NVk+JEmu2lQ8xExkSVFSbsajEG
sJYhdv28QAYLRep3VlUuVPPpaxBAOq8n18w3p+eAq/Z4+v5/mp6NZXMY7QMVCzT
LnH5iX6kdux1XWFJKc+kmTpNpoGZfzcCAwEAAaOCASIdggEeMA4GA1UdDwEB/wQE
AwIFoDAdBgNVHQ4EFgQU9PbHMHSkYrjJ2+/+hSSMEoma0QIwHwYDVR0jBBgwFoAU
rHWCWSFSPF8hPvWi+u/vLg4TPxMwTwYDVR0fBEgwRjBEoEKgQIY+ZmlsZTovL0VY
Q0gyMDEwLnNvcGhpYS5saS9DZXJ0RW5yb2xsL3NvcGhpYS1FWENIMjAxMClDQSGx
KS5jcmwWbQYIKwYBBQUHAQEETBfMF0GCCsGAQUFBzAChlFmaWx1oi8vRVhDSDIw
MTAuc29waGhhLmXpL0N1cnRfbnJvbGwvRVhDSDIwMTAuc29waGhhLmXpX3NvcGhp
YS1FWENIMjAxMClDQSGxKS5jcnQwDAYDVR0TAQH/BAIwADANBgkqhkiG9w0BAQUF
AAOCAQEAE7EAoXKIAi4vxZuxROOFofsmjcojU31ac5nrLCbq/FyW7eNblphL0NI
Dt/DlfZ5WK2q3Di+/UL1ldt3KYt9NZ1dLpmccnipbbNZ5LXL0HDkLnqt3qtLfKjv
J6GnnWCxLM18lxm1DzZT8VQtIqk5XZ8SC78hbTFtPxGZvfX70v22hekkOL1DqW4h
/3mtaqxfns1B/J3Fgpls1och45BndGiMAWavzRjjOKQaVLgVRvVrPIy3ZKDBaUleR
gsy5uODVSRhwMo3z84r+f03k4QarecgwZE+KfXoTpTafhiCbLk0ZyRMXXzWqNfl
iotEQbs52neCwXNwV24aOCChQMw2xw==
-----END CERTIFICATE-----
```

% Router Certificate successfully imported

CUBE-2(config)#

7. 配置TCP TLS作为传输协议。

这可以执行在全局或在拨号点级别。

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-----
MIIEAjCCAuqgAwIBAgIKQZrHQABAAAAEzANBgkqhkiG9w0BAQUFADBjMREwEAYK
CZImiZPYLQBGRYCbGkxJfAUBgoJkiaJk/IsZAEZFgZzb3BoaWExGzAZBgNVBAMT
EnNvcGhpYS1FWENIMjAxMClDQTAeFw0xNTA0MDEwMDEzNDFAFw0xNjA0MDEwMDIz
NDFAmBExDzANBgNVBAMTBkNVQkUtMjCCASIdQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBAMCZW+5968CDWkKqfWwFAMWU01QUyqSCHYKvUgxX6i9HYfI9MXCCvRcO
FkcxKycHDrT03N7cRvHGhq5wFBwgBJniF1NIiCPEb71hBpwub0xel/EenRwglNJ
9KWWtN7ECTNCCVbz6sStimTZMc3VLQ8LhxGUHChQKAH/4oIOSMmRTLx4Jf4aZ37p
6FEoRdkd0UcR9SvmFz/v+kGWIeJ600pLFgQ6v1NVk+JEmu2lQ8xExkSVFSbsajEG
sJYhdv28QAYLRep3VlUuVPPpaxBAOq8n18w3p+eAq/Z4+v5/mp6NZXMY7QMVCzT
LnH5iX6kdux1XWFJKc+kmTpNpoGZfzcCAwEAAaOCASIdggEeMA4GA1UdDwEB/wQE
AwIFoDAdBgNVHQ4EFgQU9PbHMHSkYrjJ2+/+hSSMEoma0QIwHwYDVR0jBBgwFoAU
rHWCWSFSPF8hPvWi+u/vLg4TPxMwTwYDVR0fBEgwRjBEoEKgQIY+ZmlsZTovL0VY
Q0gyMDEwLnNvcGhpYS5saS9DZXJ0RW5yb2xsL3NvcGhpYS1FWENIMjAxMClDQSGx
KS5jcmwWbQYIKwYBBQUHAQEETBfMF0GCCsGAQUFBzAChlFmaWx1oi8vRVhDSDIw
MTAuc29waGhhLmXpL0N1cnRfbnJvbGwvRVhDSDIwMTAuc29waGhhLmXpX3NvcGhp
YS1FWENIMjAxMClDQSGxKS5jcnQwDAYDVR0TAQH/BAIwADANBgkqhkiG9w0BAQUF
```

```
AAOCAQEAE7EAoXKIAIj4vxZuxROOFOfsmjcojU31ac5nrLCBq/FyW7eNblphL0NI
Dt/DlFz5WK2q3Di+/UL1ldt3KYt9NZ1dLpmccnipbbNZ5LXL0HDkLNqt3qtLfKjv
J6GnnWCxLM18lxmlDzZT8VQtiQk5XZ8SC78hbTFtPxGZvfX70v22hekkOL1Dqw4h
/3mtaQxfns1B/J3Fgps1och45BndGiMAWavzRjjOKQaVLgVRvVrPIy3ZKDBaUleR
gsy5uODVsrhwMo3z84r+f03k4QarecgwZE+KfXoTpTafhiCbLkKw0ZyRMXXzWqNfl
iotEQbs52neCwXNwV24aOCChQMw2xw==
-----END CERTIFICATE-----
```

% Router Certificate successfully imported

CUBE-2(config)#

8. 为SIP UA分配信任点，此信任点将使用在多维数据集和CUCM之间的所有饮者信令：

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

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

```
-----BEGIN CERTIFICATE-----
MIIEAjCCAuqgAwIBAgIKQZrHQABAAAAEzANBgkqhkiG9w0BAQUFADBjMIRwEAYK
CZImiZPyLQGBGRYCbGkxFlAUBgoJkiaJk/IsZAEZFgZzb3BoaWEeXGZAZBgNVBAMT
EnNvcGhpYS1FWENIMjAxMCI1DQTAeFw0xNTA0MDEwMDEzNDFAFw0xNjA0MDEwMDIz
NDFAmBExDzANBgNVBAMTBkNVQkUtMjCCASiWdQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBAMCZW+5968CDWkKqfwwFAMWU01QUyqSCHYKvUgX6i9HYfI9MXCCvRcO
FkcxKycHDr03N7cRvHGhq5wFBwgBjNiF1NIiCPEb71hBpwub0xel/EenmRwgLNJ
9KWWtN7ECTNCCVbz6sStimTZMc3VLQ8LhxGUHChQKAH/4oIOSMmRTLx4Jf4aZ37p
6FEoRdkd0UcR9SvmFz/v+kGWIeJ600pLFgQ6v1NVk+JEmu2lQ8xExkSVFSbsajEG
sJYhdV28QAYLRep3VlUuVPPpaxBAOq8n18w3p+eAq/Z4+v5/mp6NZXMY7QMVCzT
LnH5iX6kdux1XWFJKc+kmTpNpGZfzcCAwEAaOCASiWggEeMA4GA1UdDwEB/wQE
AwIFoDAdBgNVHQ4EFgQU9PbHMHSkYrjJ2+/+hSSMEoma0QIwHwYDVR0jBBgwFoAU
rHWCWSFSPF8hPvWi+u/vLg4TPxMwTwYDVR0fBEGwRjBEoEKgQIY+ZmlsZTovL0VY
Q0gyMDEwLnNvcGhpYS5saS9DZXJ0RW5yb2xsL3NvcGhpYS1FWENIMjAxMCI1DQSGx
KS5jcmwwbQYIKwYBBQUHAQEETBTFMF0GCCsGAQUFBzAChlFmaWx1Oi8vRVhDSDIw
MTAuc29waG1hLmXpL0N1cnRfbnJvbGwvRVhDSDIwMTAuc29waG1hLmXpX3NvcGhp
YS1FWENIMjAxMCI1DQSGxKS5jcnQwDAYDVR0TAAQH/BAlwADANBgkqhkiG9w0BAQUF
AAOCAQEAE7EAoXKIAIj4vxZuxROOFOfsmjcojU31ac5nrLCBq/FyW7eNblphL0NI
Dt/DlFz5WK2q3Di+/UL1ldt3KYt9NZ1dLpmccnipbbNZ5LXL0HDkLNqt3qtLfKjv
J6GnnWCxLM18lxmlDzZT8VQtiQk5XZ8SC78hbTFtPxGZvfX70v22hekkOL1Dqw4h
/3mtaQxfns1B/J3Fgps1och45BndGiMAWavzRjjOKQaVLgVRvVrPIy3ZKDBaUleR
gsy5uODVsrhwMo3z84r+f03k4QarecgwZE+KfXoTpTafhiCbLkKw0ZyRMXXzWqNfl
iotEQbs52neCwXNwV24aOCChQMw2xw==
-----END CERTIFICATE-----
```

% Router Certificate successfully imported

CUBE-2(config)#

或者，默认信任点可以为从多维数据集的所有饮者信令被配置：

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

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

```
-----BEGIN CERTIFICATE-----
MIIEAjCCAuqgAwIBAgIKQZrHQABAAAAEzANBgkqhkiG9w0BAQUFADBjMIRwEAYK
CZImiZPyLQGBGRYCbGkxFlAUBgoJkiaJk/IsZAEZFgZzb3BoaWEeXGZAZBgNVBAMT
EnNvcGhpYS1FWENIMjAxMCI1DQTAeFw0xNTA0MDEwMDEzNDFAFw0xNjA0MDEwMDIz
NDFAmBExDzANBgNVBAMTBkNVQkUtMjCCASiWdQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBAMCZW+5968CDWkKqfwwFAMWU01QUyqSCHYKvUgX6i9HYfI9MXCCvRcO
FkcxKycHDr03N7cRvHGhq5wFBwgBjNiF1NIiCPEb71hBpwub0xel/EenmRwgLNJ
9KWWtN7ECTNCCVbz6sStimTZMc3VLQ8LhxGUHChQKAH/4oIOSMmRTLx4Jf4aZ37p
6FEoRdkd0UcR9SvmFz/v+kGWIeJ600pLFgQ6v1NVk+JEmu2lQ8xExkSVFSbsajEG
sJYhdV28QAYLRep3VlUuVPPpaxBAOq8n18w3p+eAq/Z4+v5/mp6NZXMY7QMVCzT
LnH5iX6kdux1XWFJKc+kmTpNpGZfzcCAwEAaOCASiWggEeMA4GA1UdDwEB/wQE
AwIFoDAdBgNVHQ4EFgQU9PbHMHSkYrjJ2+/+hSSMEoma0QIwHwYDVR0jBBgwFoAU
rHWCWSFSPF8hPvWi+u/vLg4TPxMwTwYDVR0fBEGwRjBEoEKgQIY+ZmlsZTovL0VY
Q0gyMDEwLnNvcGhpYS5saS9DZXJ0RW5yb2xsL3NvcGhpYS1FWENIMjAxMCI1DQSGx
KS5jcmwwbQYIKwYBBQUHAQEETBTFMF0GCCsGAQUFBzAChlFmaWx1Oi8vRVhDSDIw
MTAuc29waG1hLmXpL0N1cnRfbnJvbGwvRVhDSDIwMTAuc29waG1hLmXpX3NvcGhp
YS1FWENIMjAxMCI1DQSGxKS5jcnQwDAYDVR0TAAQH/BAlwADANBgkqhkiG9w0BAQUF
AAOCAQEAE7EAoXKIAIj4vxZuxROOFOfsmjcojU31ac5nrLCBq/FyW7eNblphL0NI
Dt/DlFz5WK2q3Di+/UL1ldt3KYt9NZ1dLpmccnipbbNZ5LXL0HDkLNqt3qtLfKjv
J6GnnWCxLM18lxmlDzZT8VQtiQk5XZ8SC78hbTFtPxGZvfX70v22hekkOL1Dqw4h
/3mtaQxfns1B/J3Fgps1och45BndGiMAWavzRjjOKQaVLgVRvVrPIy3ZKDBaUleR
gsy5uODVsrhwMo3z84r+f03k4QarecgwZE+KfXoTpTafhiCbLkKw0ZyRMXXzWqNfl
iotEQbs52neCwXNwV24aOCChQMw2xw==
-----END CERTIFICATE-----
```


10. 对于SRTP和实时传输协议(RTP)互连网络，需要安全的转码器。

如果Cisco IOS版本是15.2.2T (多维数据集9.0)或以后然后，本地转码的接口(LTI)转码器可以是配置使配置减到最小。

LTI转码器不需要SRTP-RTP呼叫的公共密钥基础设施(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在15.2.2T之下，则请配置SCCP转码器。

SCCP转码器将需要发信号的信任点，然而，如果同一路由器用于主机转码器然后同样信任点(SUBCA1)可以用于多维数据集以及转码器。

```
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. 生成呼叫管理器CSR在所有CUCM节点。

如镜像所显示，连接对CM OS管理> Security > Certificate Management >生成认证署名请求。

Generate Certificate Signing Request

Generate Close

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

Generate
Close

*- indicates required item.

呼叫管理器CSR将有这些关键属性：

```

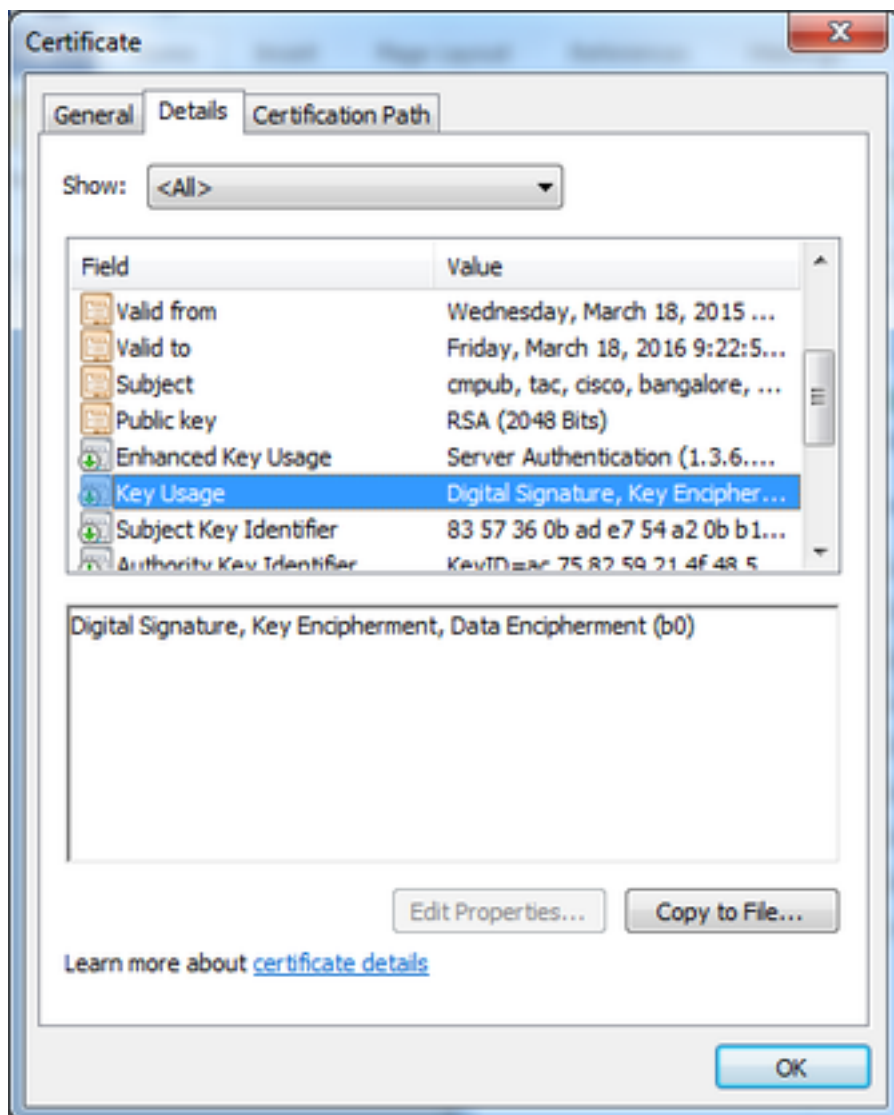
sccp local GigabitEthernet0/2
sccp ccm 10.106.95.153 identifier 1 priority 1 version 7.0
sccp
!
sccp ccm group 1
bind interface GigabitEthernet0/0
associate ccm 1 priority 1
associate profile 2 register secxcode
!
dspfarm profile 2 transcode universal security
trustpoint SUBCA1
codec g711ulaw
codec g711alaw
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

```

2. 获得辅助CA签字的所有CM节点的呼叫管理器认证。

请使用生成的CSR在Step1。所有Web服务器认证模板将工作，保证签名的证书有至少这些密钥用法属性：**数字签名**，**关键编码**，如镜像所显示的**数据编码**。



3. 从根CA和辅助CA的加载CA证书作为呼叫管理器信任。

如镜像所显示，连接到CM OS管理> Security > Certificate Management >加载认证/证书链。

Upload Certificate/Certificate chain

Upload Close

Status

i 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

Upload Close

i *- indicates required item.

Upload Certificate/Certificate chain

Upload Close

Status

i 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

Upload Close

i *- indicates required item.

4. 如镜像所显示，加载呼叫管理器签名的证书作为呼叫管理器。

Upload Certificate/Certificate chain

Upload Close

Status

i 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

Upload Close

i *- indicates required item.

5. 更新在发布人的证书信任列表(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. 重新启动呼叫管理器和TFTP服务在所有节点和CAPF服务在发布人。

7. 创建新的SIP Trunk安全配置文件。

在CM管理，请连接对**系统 > Security > SIP Trunk安全配置文件 > 查找**。

如此镜像所显示，复制存在非安全的SIP Trunk配置文件创建新的安全的配置文件。

SIP Trunk Security Profile Configuration

Save  Delete  Copy  Reset  Apply Config  Add New

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
<input type="checkbox"/> Enable Digest Authentication	
Nonce Validity Time (mins)*	600
X.509 Subject Name	CUBE-2
Incoming Port*	5061
<input type="checkbox"/> Enable Application level authorization	
<input checked="" type="checkbox"/> Accept presence subscription	
<input checked="" type="checkbox"/> Accept out-of-dialog refer**	
<input checked="" type="checkbox"/> Accept unsolicited notification	
<input checked="" type="checkbox"/> Accept replaces header	
<input type="checkbox"/> Transmit security status	
<input type="checkbox"/> Allow charging header	
SIP V.150 Outbound SDP Offer Filtering*	Use Default Filter

8.创建SIP Trunk对多维数据集。

在SIP Trunk允许的Enable (event) SRTP如镜像所显示。

Trunk Configuration

Save Delete Reset Add New

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

配置目的地端口5061 (TLS)如镜像所显示，并且适用在SIP Trunk的新的安全的SIP Trunk安全配置文件。

Trunk Configuration

Save Delete Reset Add New

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

Verify

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
```

当使用时，输出的show call active voice brief命令是获取的LTI转码器。

```
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
```

并且，当SRTP被加密的呼叫被做在Cisco IP电话之间和多维数据集或者网关时，锁图标在IP电话显示。

Troubleshoot

本部分提供了可用于对配置进行故障排除的信息。

这些调试为排除PKI/TLS/SIP/SRTP问题故障是有用的。

```
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
```