

配置在CUCM-CUBE/CUBE-SBC之间的SIP TLS

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[网络图](#)

[配置步骤](#)

[验证](#)

[故障排除](#)

[目录](#)

简介

本文帮助配置SIP传输层安全(TLS)在Cisco Unified Communications管理器(CUCM)和Cisco Unified Border Element (多维数据集)之间

[先决条件](#)

思科推荐有这些主题知识

- SIP协议
- 安全证书

[要求](#)

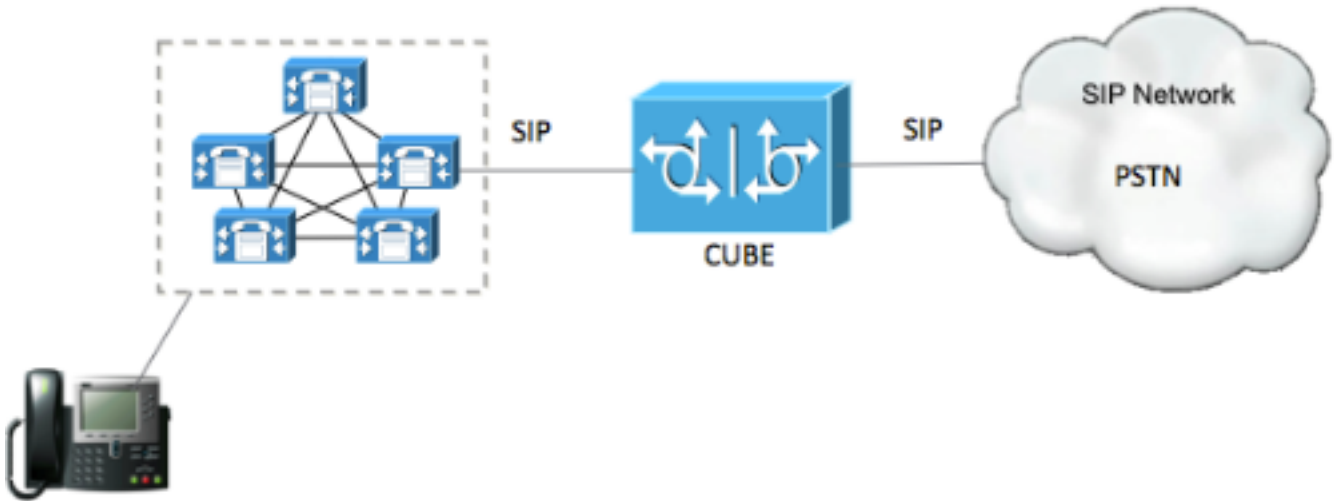
- 日期和时间在终端(推荐必须配比有同样Ntp source)。
- CUCM必须在混合模式。
- TCP连接要求(任何传输防火墙的开放端口5061)。
- 多维数据集必须有安全，并且UCK9准许已安装。

[使用的组件](#)

- SIP
- Selfsigned证书

配置

网络图



配置步骤

步骤1.创建信任点为了有CUBE的selfsigned证书

```
crypto pki trustpoint CUBEtest(this can be any name)
  enrollment selfsigned
  serial-number none
  fqdn none
  ip-address none
  subject-name cn= ISR4451-B.cisco.lab !(this has to match the router's host name)
  revocation-check none
  rsakeypair ISR4451-B.cisco.lab !(this has to match the router's host name)
```

第二步：一旦信任点创建您运行crypto命令pki登记CUBEtest为了获得自己签署的certificates

```
crypto pki enroll CUBEtest
% The fully-qualified domain name will not be included in the certificate
Generate Self Signed Router Certificate? [yes/no]: yes
```

如果登记正确您必须期待此输出

```
Router Self Signed Certificate successfully created
```

第三步：在您请获取证书后，您需要导出它

```
crypto pki export CUBEtest pem terminal
```

上述命令必须生成下面的证书

% Self-signed CA certificate:

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

```
MIIBgDCCASqgAwIBAgIBATANBgkqhkiG9w0BAQUFADAeMRwwGgYDVQQDExNjU1I0
NDUxLUIuY21zY28ubGF1bG4XDTE1MTIxNTAxNTAxNVoXDTIwMDEwMTAwMDAwMFow
HjEcMBoGA1UEAxMTSVNSNDQ1MS1CLmNpc2NvLmxhYjBcMA0GCSqGSIb3DQEBAQUA
A0sAMEgCQQDgtZ974Tfv+pngsl+cCeLz/e0b2zq6CrIj4T1t+NSlG5sJMj919/ix
7Fa6DG33LmEYUmlNntkLaz+8UNDAyBZrAgMBAAGjUzBRMA8GA1UdEwEB/wQFMAMB
Af8wHwYDVR0jBBGwFoAU+Yy1UqKdb+rrINc7tZcrdIRMKPowHQYDVR0OBBYEFpM
tVKinW/q6yDXO7WXK3SETCj6MA0GCSqGSIb3DQEBBQUAA0EADQXG2FYZ/MSewjSH
T88SHXq0EVqcLrgGpScwcpbR1mKFppIhDVaJfH/FC6jnkGW7JFWcekA5Kp0tzYx4
LDQaxQ==
```

-----END CERTIFICATE-----

% General Purpose Certificate:

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

```
MIIBgDCCASqgAwIBAgIBATANBgkqhkiG9w0BAQUFADAeMRwwGgYDVQQDExNjU1I0
NDUxLUIuY21zY28ubGF1bG4XDTE1MTIxNTAxNTAxNVoXDTIwMDEwMTAwMDAwMFow
HjEcMBoGA1UEAxMTSVNSNDQ1MS1CLmNpc2NvLmxhYjBcMA0GCSqGSIb3DQEBAQUA
A0sAMEgCQQDgtZ974Tfv+pngsl+cCeLz/e0b2zq6CrIj4T1t+NSlG5sJMj919/ix
7Fa6DG33LmEYUmlNntkLaz+8UNDAyBZrAgMBAAGjUzBRMA8GA1UdEwEB/wQFMAMB
Af8wHwYDVR0jBBGwFoAU+Yy1UqKdb+rrINc7tZcrdIRMKPowHQYDVR0OBBYEFpM
tVKinW/q6yDXO7WXK3SETCj6MA0GCSqGSIb3DQEBBQUAA0EADQXG2FYZ/MSewjSH
T88SHXq0EVqcLrgGpScwcpbR1mKFppIhDVaJfH/FC6jnkGW7JFWcekA5Kp0tzYx4
LDQaxQ==
```

-----END CERTIFICATE-----

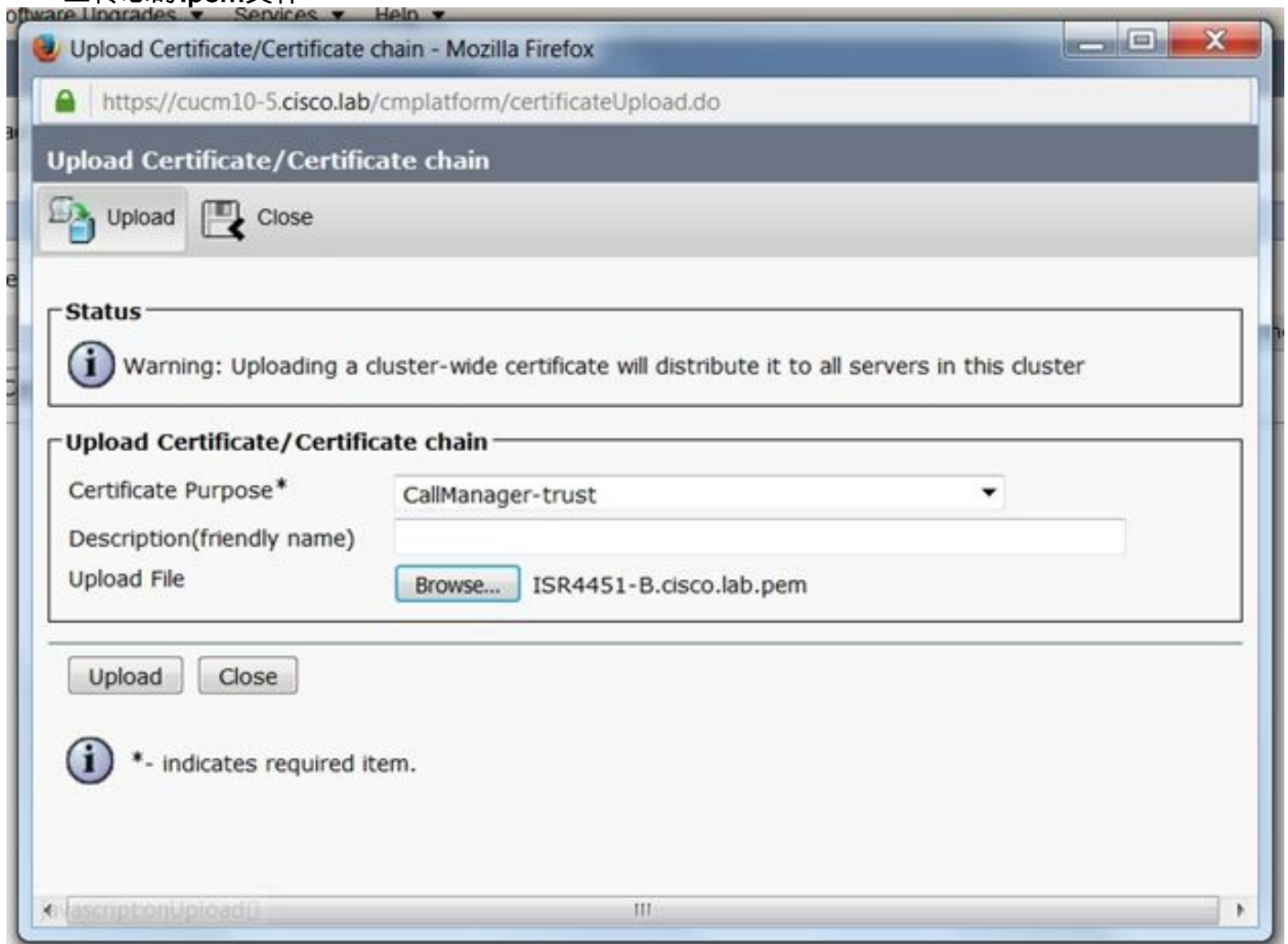
复制以上生成的自签证书并且粘贴它到有文件扩展.pem的一个文本文件

下面的示例被命名作为ISR4451-B.ciscolab.pem



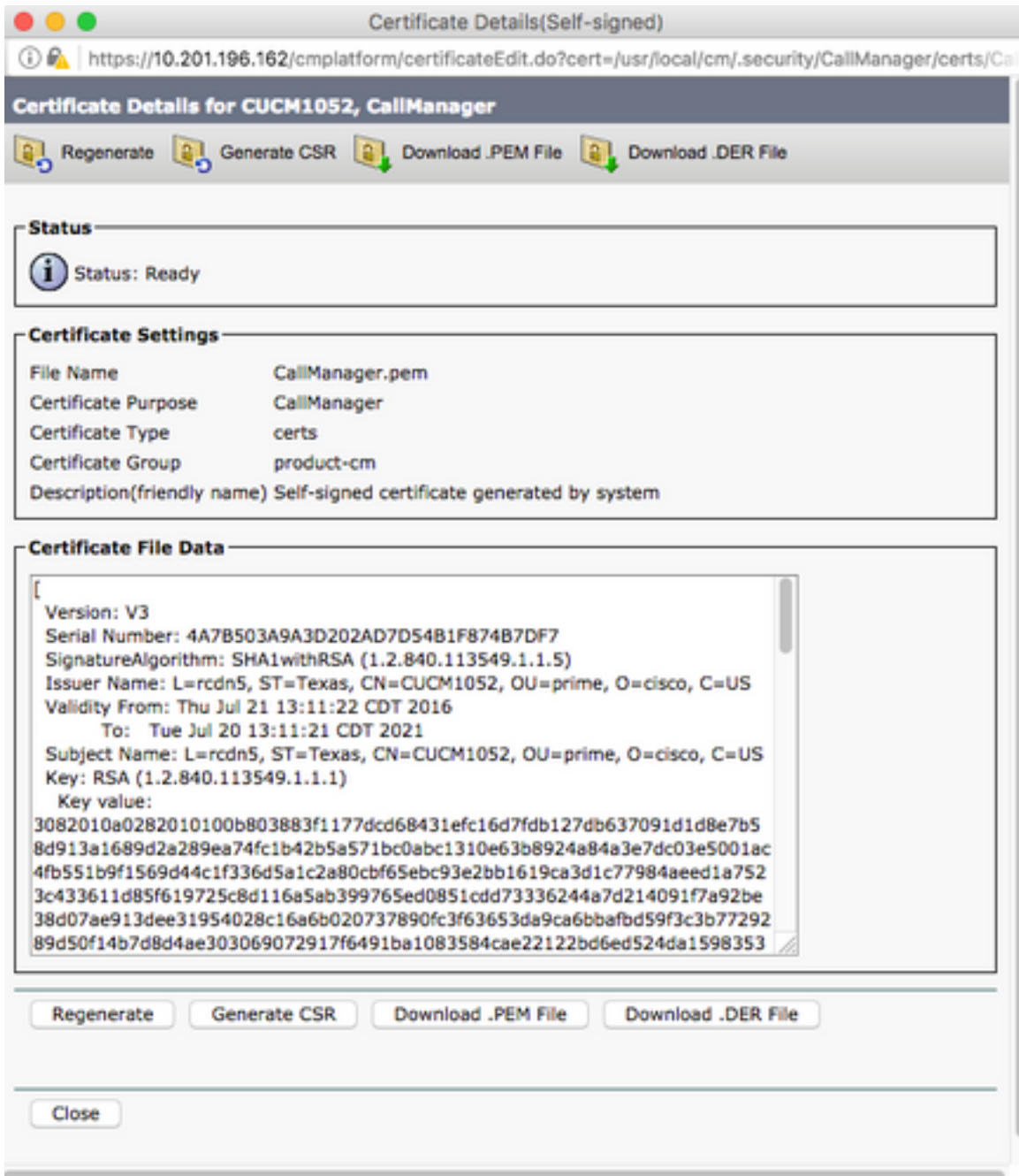
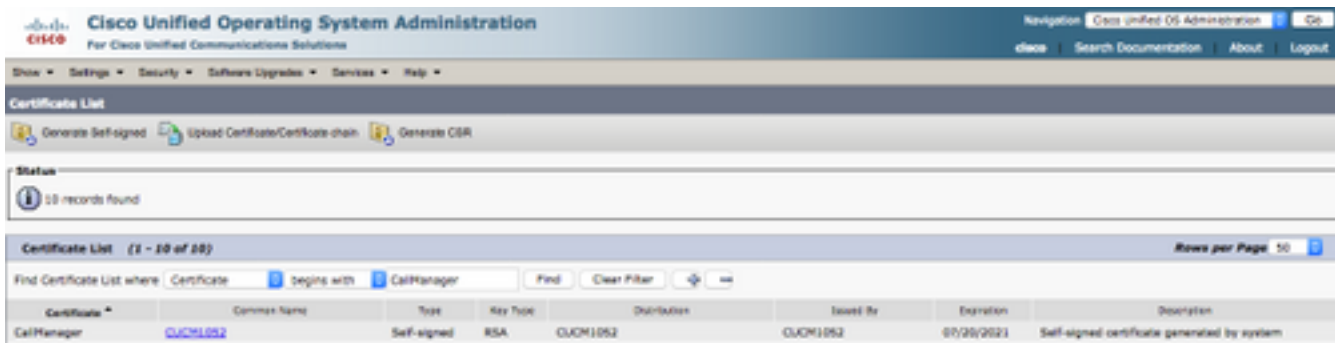
步骤4.上传多维数据集证书对CUCM

- CUCM OS Admin > Security > Certificate Management > 加载证书/证书链
- 证书目的= CallManager托拉斯
- 上传您的.pem文件



步骤5.下载CallManager自签名证书

- 查找说CallManager的证书
- 点击主机名
- 点击下载PEM文件
- 保存它到您的计算机



步骤6.上传Callmanager.pem证书求立方

- 打开Callmanager.pem用文本文件编辑器
- 复制文件的整个内容
- 运行此on命令多维数据集

crypto pki trustpoint CUCMHOSTNAME

```
enrollment terminal
revocation-check none
```

```
crypto pku authenticate CUCMHOSTNAME
```

```
(PASTE THE CUCM CERT HERE AND THEN PRESS ENTER TWICE)
```

You will then see the following:

Certificate has the following attributes:

```
Fingerprint MD5: B9CABE35 24B11EE3 C58C9A9F 02DB16BC
```

```
Fingerprint SHA1: EC164F6C 96CDC1C9 E7CA0933 8C7518D4 443E0E84
```

```
% Do you accept this certificate? [yes/no]: yes
```

If everything was correct, you should see the following:

```
Trustpoint CA certificate accepted.
```

```
% Certificate successfully imported
```

步骤7.配置SIP使用CUBE的selfsigned证书信任点

```
sip-ua
```

```
crypto signaling default trustpoint CUBEttest
```

步骤8.配置有TLS的拨号对端

```
dial-peer voice 9999 voip
```

```
answer-address 35..
```

```
destination-pattern 9999
```

```
session protocol sipv2
```

```
session target dns:cucm10-5
```

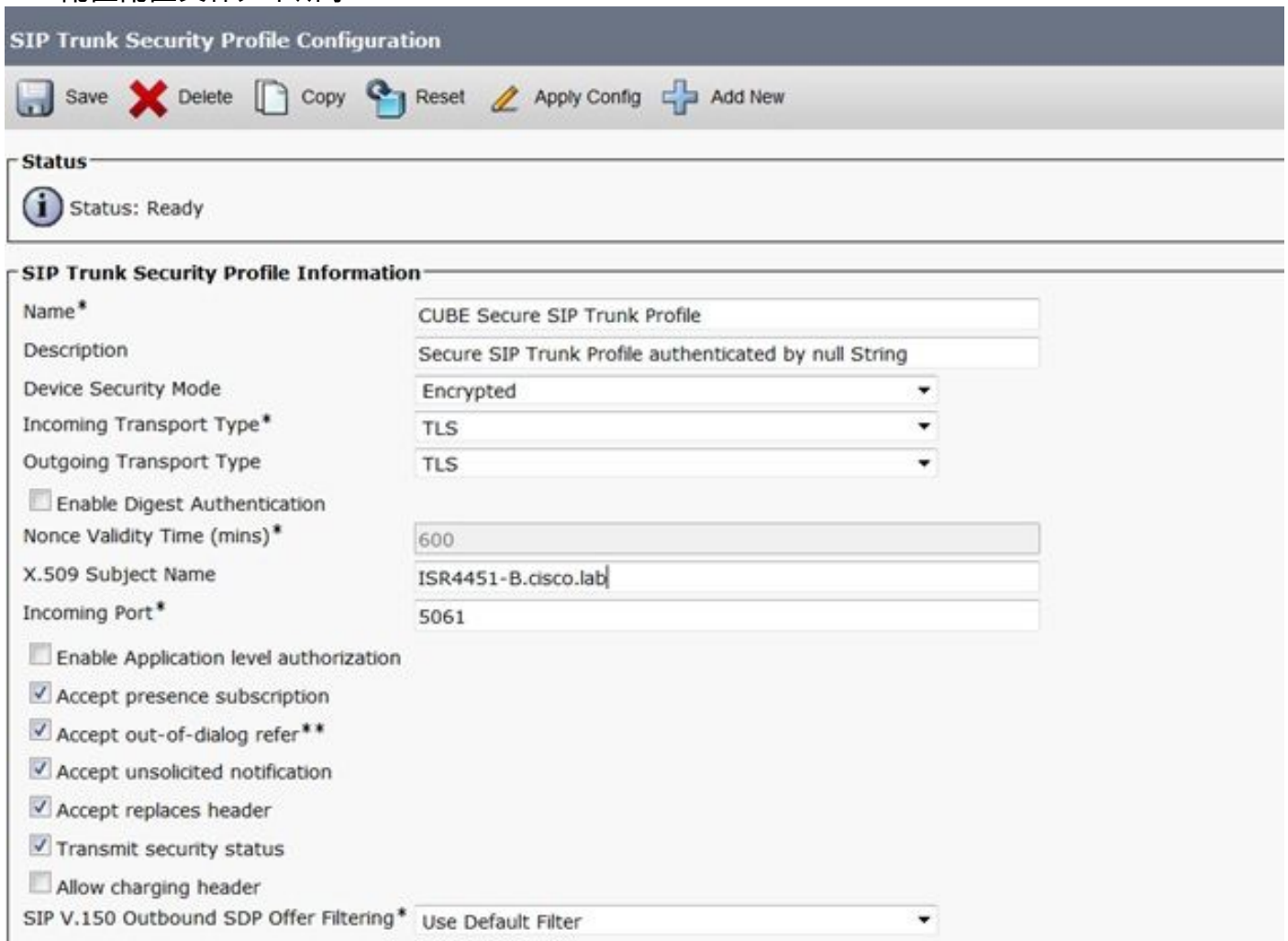
```
session transport tcp tls
```

```
voice-class sip options-keepalive
```

```
srtplib
```

步骤9.配置CUCM SIP中继安全配置文件

- CUCM管理员页面>System > Security > SIP中继安全配置文件
- 配置配置文件如下所示



SIP Trunk Security Profile Configuration

Save Delete Copy Reset Apply Config Add New

Status
Status: Ready

SIP Trunk Security Profile Information

Name* CUBE 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 ISR4451-B.cisco.lab

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

Note: 是极其重要的X.509字段匹配您以前配置的CN名称，当您生成自签名证书时

步骤10.配置在CUCM的—SIP中继

- 保证允许的SRTP复选框被检查
- 配置适当的地址并且保证用端口5061替换端口5060
- 保证选择在步骤9)创建的正确Sip中继安全配置文件(

SIP Information

Destination

Destination Address is an SRV

Destination Address	Destination Address IPv6	Destination Port
1* 10.201.160.12		5061

MTP Preferred Originating Codec* 711ulaw

BLF Presence Group* Standard Presence group

SIP Trunk Security Profile* ISR4451-B 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-options [View Details](#)

DTMF Signaling Method* No Preference

- 保存并且重置中继。

验证

因为您在CUCM的已启用选项PING，SIP中继必须在FULL服务状态

Name	Description	Calling Search Space	Device Pool	Route Pattern	Partition	Route Group	Priority	Trunk Type	SIP Trunk Status	SIP Trunk Duration
ISR4451-B			0711-Secure					SIP Trunk	Full Service	Time In Full Service: 0 day 0 hour 0 minute

SIP中继线状态显示服务周到。

拨号对端状态显示和跟随：

```
show dial-peer voice summary
```

TAG	TYPE	MIN	OPER	PREFIX	DEST-PATTERN	FER	THRU	SESS-TARGET	STAT	PORT
9999	voip	up	up		9999	0	syst	dns:cucm10-5		active

故障排除

启用并且收集这些调试输出

```
debug crypto pki api
debug crypto pki callbacks
debug crypto pki messages
debug crypto pki transactions
debug ssl openssl errors
debug ssl openssl msg
debug ssl openssl states
debug ip tcp transactions
debug ccsip verbose
```

WebEx录音链路：

<https://goo.gl/QOS1iT>