使用CA签名证书在CUCM-CUBE/CUBE-SBC之间配置SIP TLS

目录

简介

本文档介绍如何在Cisco Unified Communication Manager(CUCM)和Cisco Unified Border Element(CUBE)之间配置SIP传输层安全(TLS)，并且使用证书颁发机构(CA)签名的证书。

先决条件

思科建议了解这些主题

- SIP 协议
- 安全证书

要求

- 终端上的日期和时间必须匹配（建议使用相同的NTP源）。
- CUCM必须处于混合模式。
- 需要TCP连接（在任何传输防火墙上打开端口5061）。
- CUBE必须安装安全和统一通信K9(UCK9)许可证。

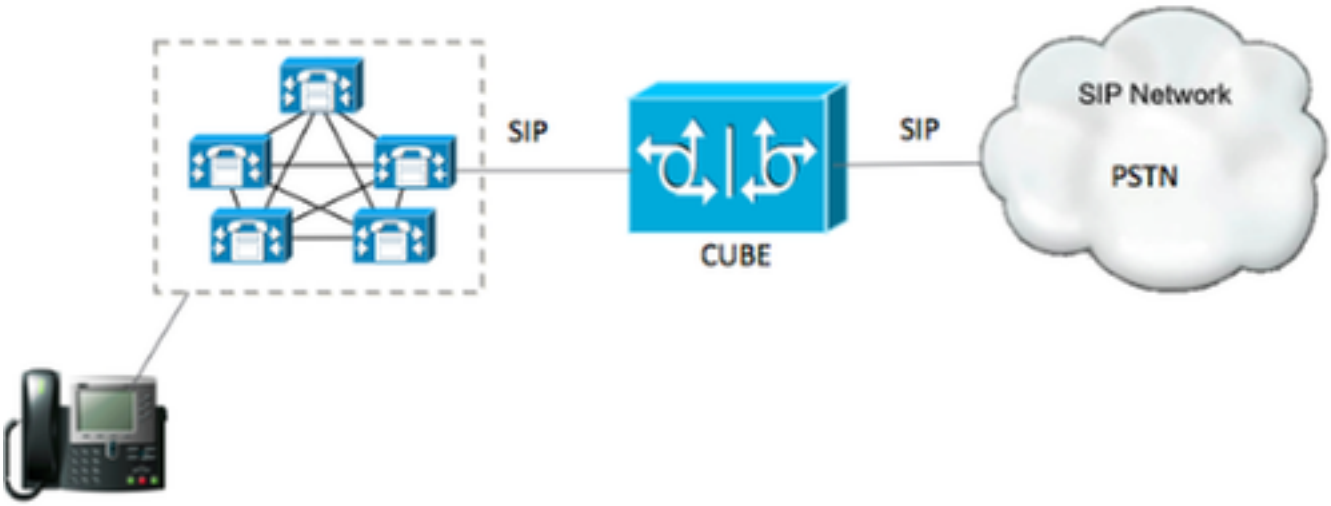
注意：对于Cisco IOS-XE 16.10版奖励，平台已移至智能许可。

使用的组件

- SIP
- 证书颁发机构签名的证书
- 思科IOS和IOS-XE网关2900 / 3900 / 4300 / 4400 / CSR1000v / ASR100X版本：15.4+
- 思科统一通信管理器 (CUCM)版本：10.5+

配置

网络图



配置

步骤1.您将使用以下命令创建与根证书的证书长度匹配的RSA密钥：

```
Crypto key generate rsa label TestRSAkey exportable modulus 2048
```

此命令创建长度为2048位（最大值为4096）的RSA密钥。

步骤2.使用以下命令创建信任点以保存CA签名的证书：

```
 Crypto pki trustpoint CUBE_CA_CERT
   serial-number none
   fqdn none
   ip-address none
   subject-name cn=ISR4451-B.cisco.lab !(this has to match the router's hostname
[hostname.domain.name])
   revocation-check none
   rsakeypair TestRSAkey !(this has to match the RSA key you just created)
```

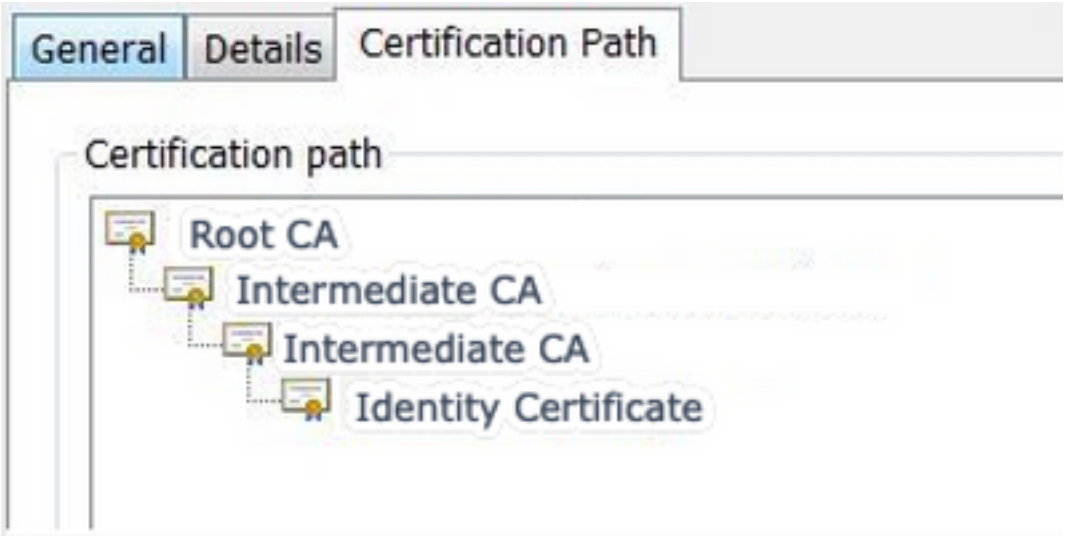
第 3 步： 既然您拥有我们的信任点，您将使用以下命令生成我们的CSR请求：

```
 Crypto pki enroll CUBE_CA_CERT
```

回答屏幕上的问题，然后复制CSR请求，将其保存到文件，然后将其发送到CA。

步骤4.您需要了解根证书链是否有任何中间证书；如果没有中间证书颁发机构，请跳至步骤7，否则，请在步骤6继续。

步骤5.创建一个信任点以保存根证书，另外，创建一个信任点以保存任何中间CA，直到签署CUBE证书的中间CA（请参阅下图）。



在本示例中，1级是根CA，2级是第一个中间CA，3级是对CUBE证书签名的CA，因此，您需要创建信任点来使用这些命令保存前2个证书。

```
Crypto pki trustpoint Root_CA_CERT
Enrollment terminal pem
Revocation-check none

Crypto pki authenticate Root_CA_CERT
Paste the X.64 based certificate here

Crypto pki trustpoint Intermediate_CA
Enrollment terminal
Revocation-check none

Crypto pki authenticate Intermediate_CA
```

步骤 6　在收到我们的CA签名证书后，您将对信任点进行身份验证，信任点需要在CUBE证书之前保存CA的证书；允许导入证书的命令是，

```
Crypto pki authenticate CUBE_CA_CERT
```

步骤7.安装证书后，需要运行此命令以导入CUBE证书

```
  Crypto pki import CUBE_CA_CERT cert
```

步骤8.配置SIP-UA以使用您创建的信任点

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

步骤 9　配置拨号对等体，如下所示：

```
  dial-peer voice 9999 voip
  answer-address 35..
  destination-pattern 9999
  session protocol sipv2
  session target dns:cucm10-5
```

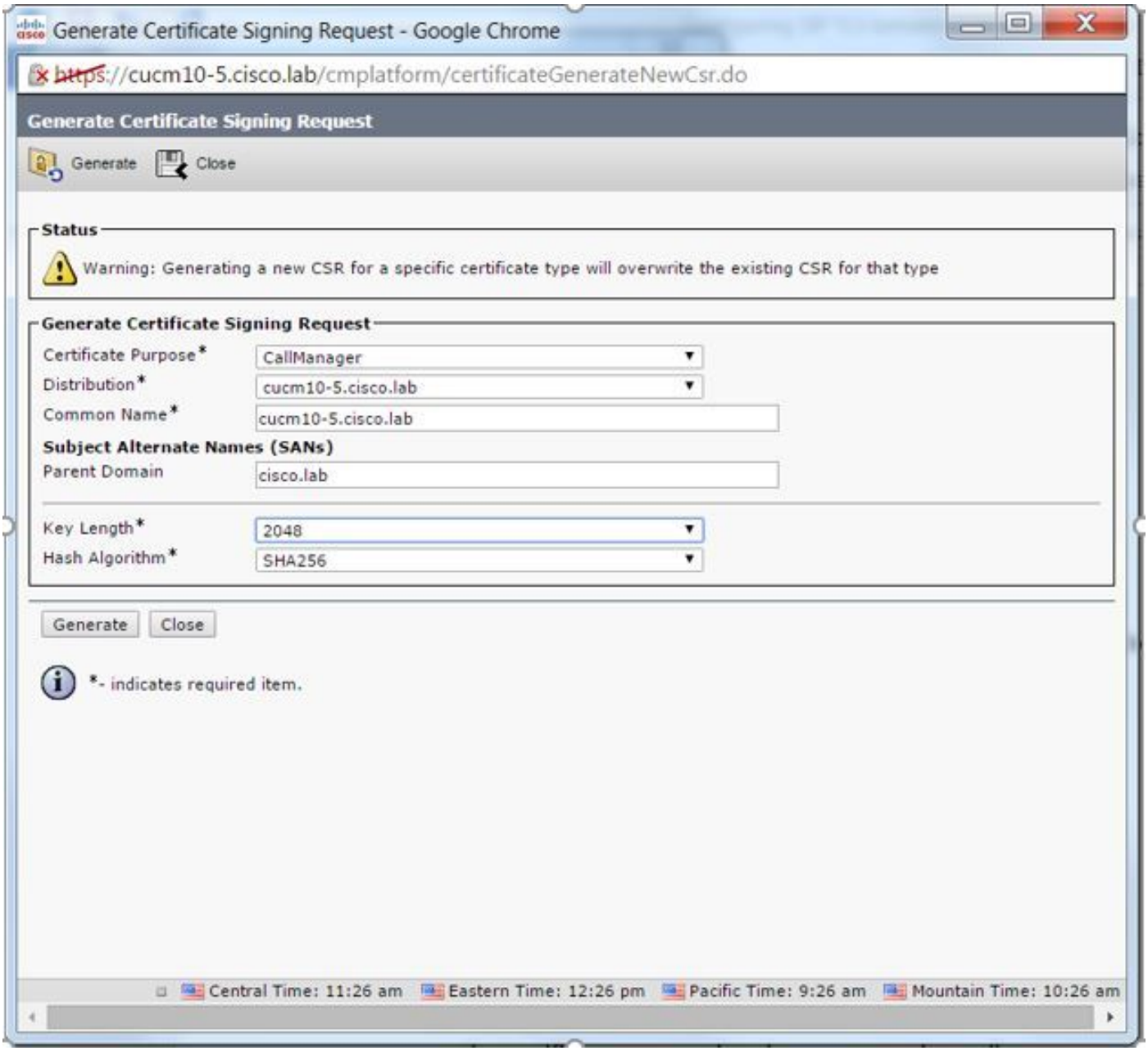
```
 session transport tcp tls
 voice-class sip options-keepalive
 srtp
```

这样，CUBE配置即已完成。

步骤 10 现在，您将生成我们的CUCM CSR，请遵循以下说明

- 登录到CUCM OS管理员
- 点击安全
- 点击证书管理。
- 点击生成CSR

CSR请求需要如下所示：



步骤11.下载CSR并将其发送到CA。

步骤12.将CA签名的证书链上传到CUCM，步骤如下：

- 点击安全，然后点击证书管理。
- 点击上传证书/证书链。

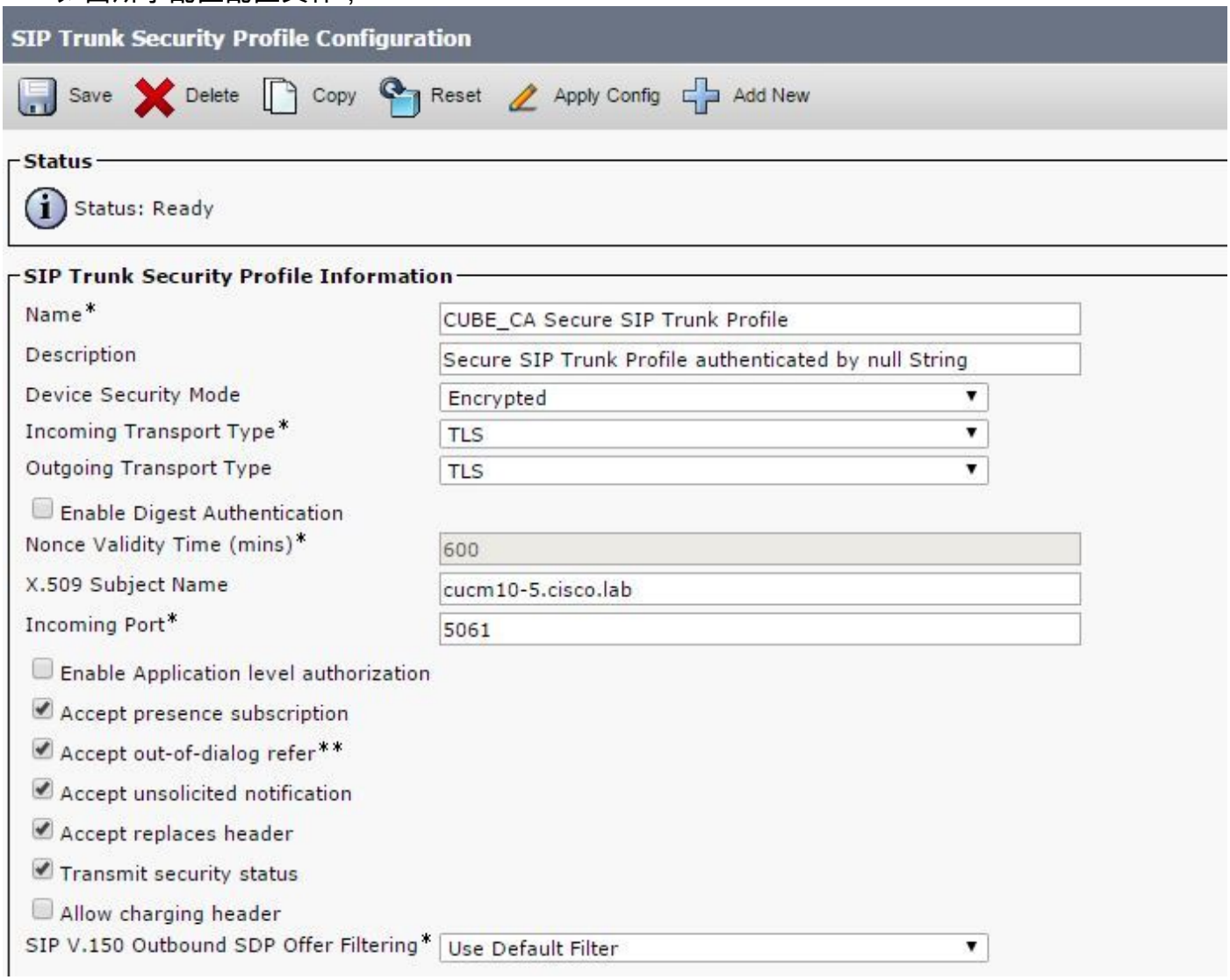
- 在“证书用途”下拉菜单中，选择call manager。
- 浏览到您的文件。
- 点击上传。

步骤13.登录CUCM CLI并运行此命令

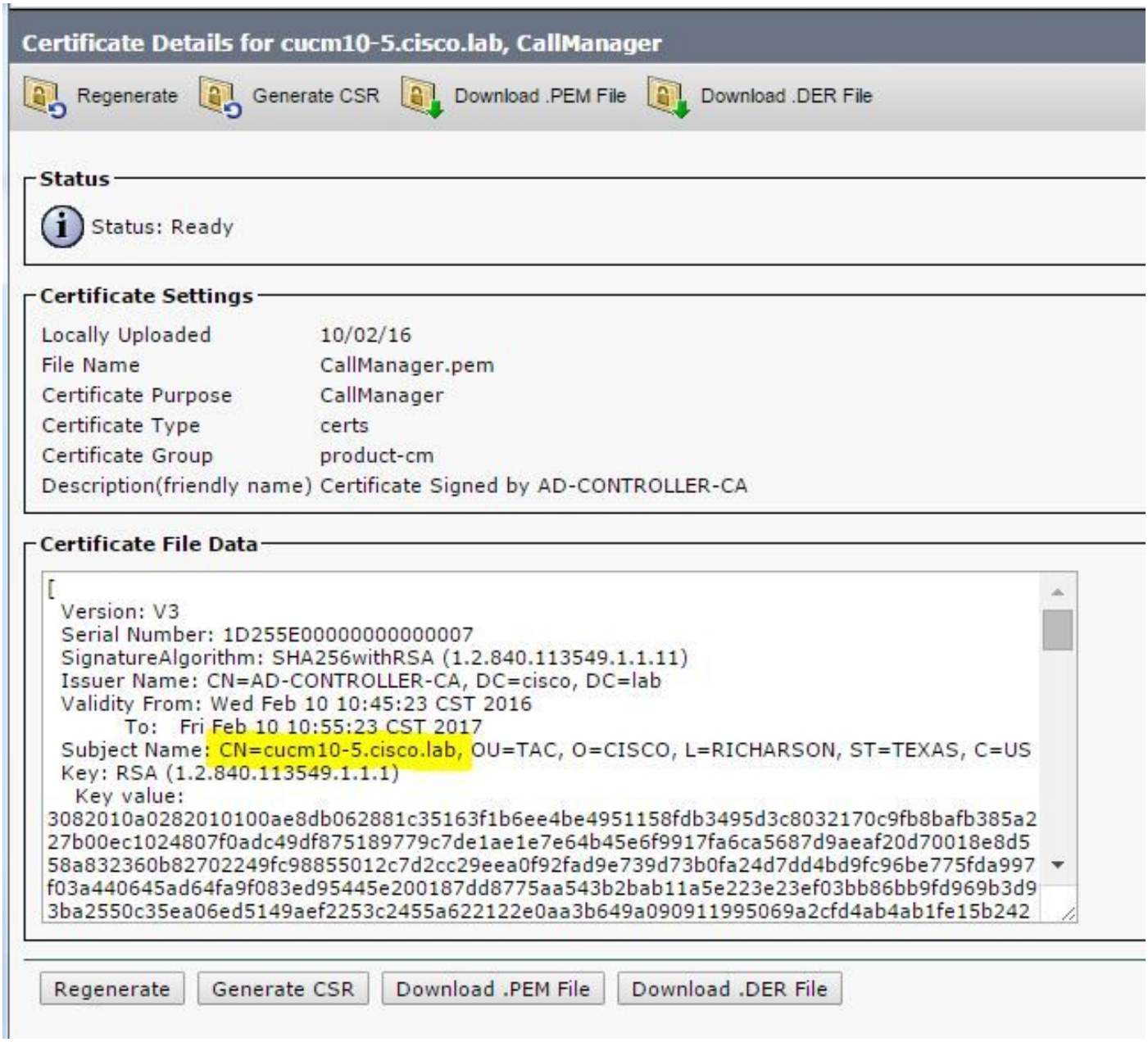
```
utils ctl update CTLFile
```

步骤14.配置CUCM SIP中继安全配置文件

- 依次点击系统、安全和sip中继安全配置文件
- 如图所示配置配置文件，



注意：在本例中，X.509使用者名称必须与CUCM证书使用者名称匹配，如图像突出显示部分所示。



步骤15.像在CUCM上通常那样配置SIP中继

- 确保选中SRTP Allowed复选框。
- 配置正确的目标地址，并确保将端口5060替换为端口5061。
- 在SIP中继安全配置文件上，确保选择在步骤14中创建的SIP配置文件名称。

验证

此时，如果所有配置都正常，

在CUCM上，SIP中继状态显示Full Service，如图所示。

Name	Description	Calling Search Space	Device Pool	Route Pattern	Partition	Route Group	Priority	Trunk Type	SIP Trunk Status	SIP Trunk Duration
ISR4451-B			G711-Secure					SIP Trunk	Full Service	Time In Full Service: 0 day 0 hour 0 minute

在CUBE上，拨号对等体显示以下状态：

```
TAG    TYPE  MIN  OPER PREFIX    DEST-PATTERN      FER THRU SESS-TARGET    STAT PORT
KEEPALIVE

9999   voip  up   up             9999               0  syst dns:cucm10-5                active
```

此过程同样适用于其他路由器，唯一的区别是上传第三方提供的证书而不是执行上传CUCM证书的步骤。

故障排除

在CUBE上启用这些调试

```
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
```