

在CUCM-CUBE/CUBE-SBC之间配置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

本文档帮助在思科统一通信管理器(CUCM)和思科统一边界元素(CUBE)之间配置SIP传输层安全(TLS)

先决条件

思科建议了解这些主题

- SIP 协议
- 安全证书

要求

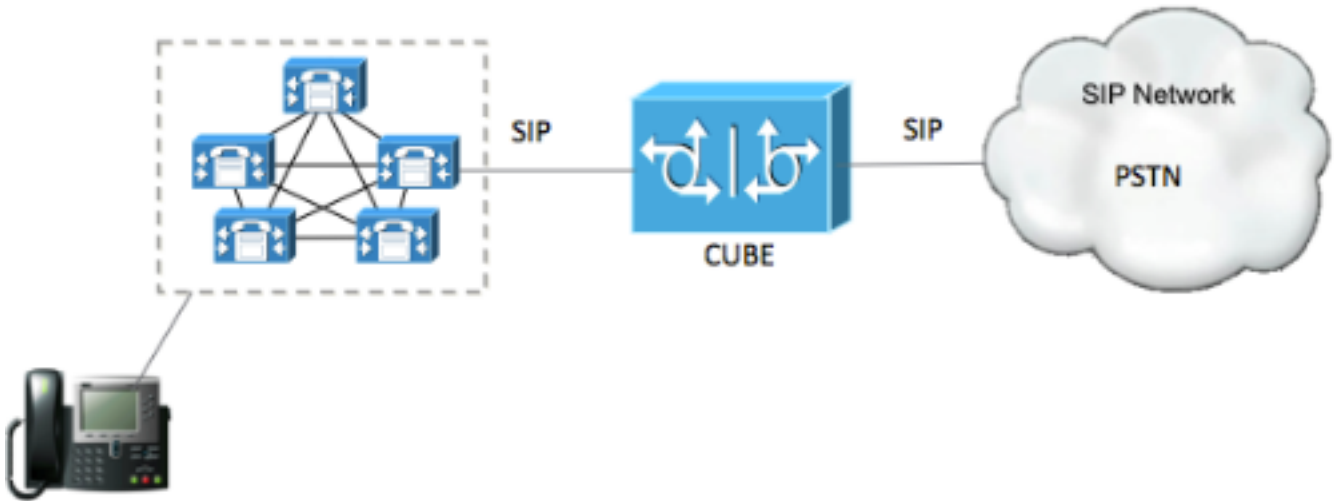
- 终端上的日期和时间必须匹配 (建议使用相同的NTP源) 。
- CUCM必须处于混合模式。
- 需要TCP连接 (在任何传输防火墙上打开端口5061) 。
- CUBE必须安装安全许可证和UCK9许可证。

使用的组件

- SIP
- 自签名证书

配置

网络图



配置步骤

步骤1: 创建信任点以保存CUBE的自签名证书

```
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)
```

步骤2.创建信任点后，运行命令**Crypto pki enroll CUBEtest**以获取自签名证书

```
crypto pki enroll CUBEtest

% The fully-qualified domain name will not be included in the certificate

Generate Self Signed Router Certificate? [yes/no]: yes
```

如果注册正确，则必须预期此输出

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

步骤3.获取证书后，需要将其导出

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

以上命令必须生成以下证书

% 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:

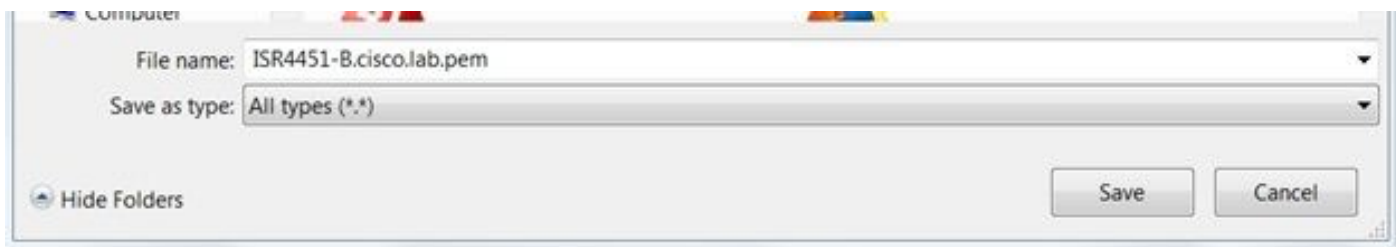
-----BEGIN CERTIFICATE-----

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

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

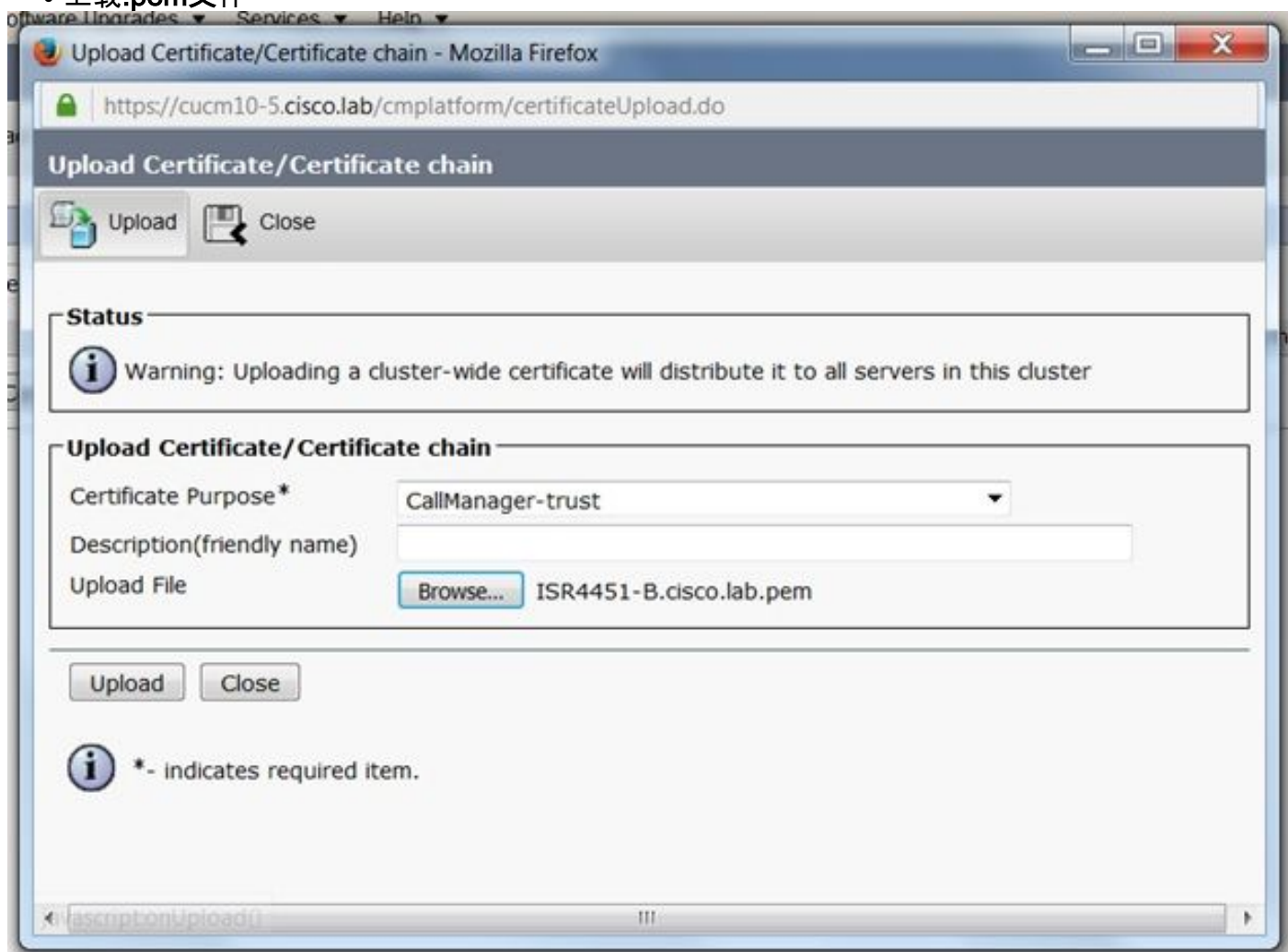
复制上述生成的自签名证书并将其粘贴到文件扩展名为.pem的文本文件

以下示例命名为ISR4451-B.ciscolab.pem



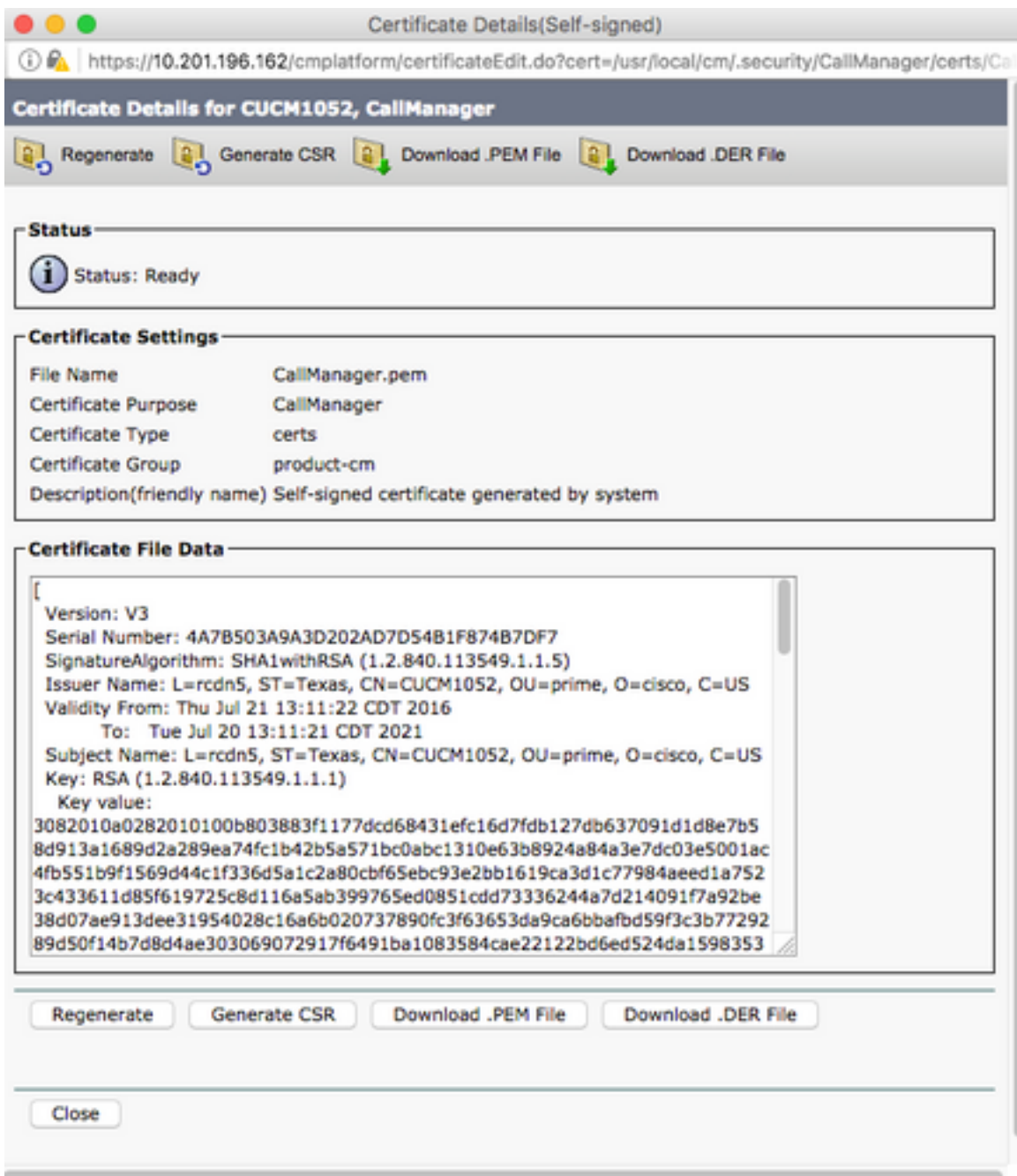
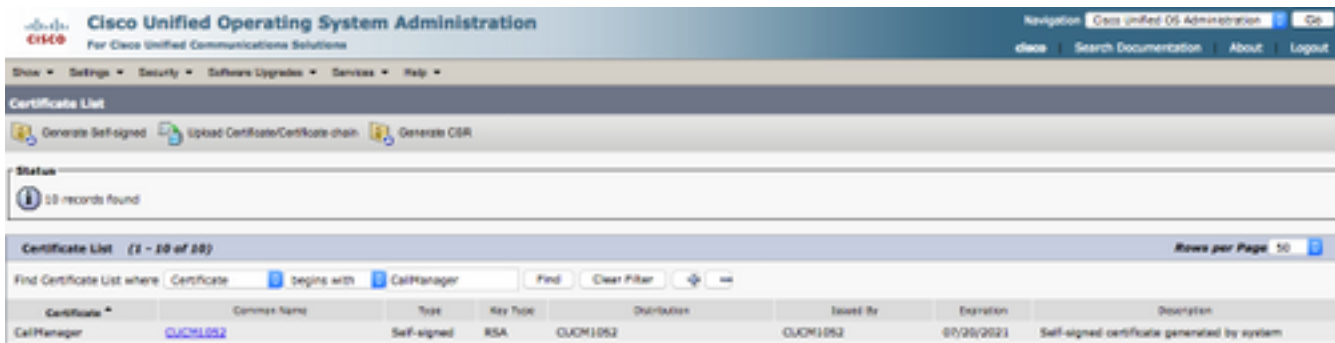
步骤4.将CUBE证书上传到CUCM

- CUCM OS Admin > Security > Certificate Management > Upload Certificate/Certificate chain
- 证书用途= CallManager-Trust
- 上载.pem文件



步骤5.下载Call Manager自签名证书

- 查找显示Callmanager的证书
- 单击主机名
- 点击下载PEM文件
- 将其保存到计算机



步骤6. 将Callmanager.pem证书上传到CUBE

- 使用文本文件编辑器打开Callmanager.pem
- 复制文件的整个内容
- 在CUBE上运行以下命令

```
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.将SIP配置为使用CUBE的自签名证书信任点

sip-ua

crypto signaling default trustpoint CUBEtest

步骤8.使用TLS配置拨号对等体

dial-peer voice 9999 voip

answer-address 35..

destination-pattern 9999

session protocol sipv2

session target dns:cucm10-5

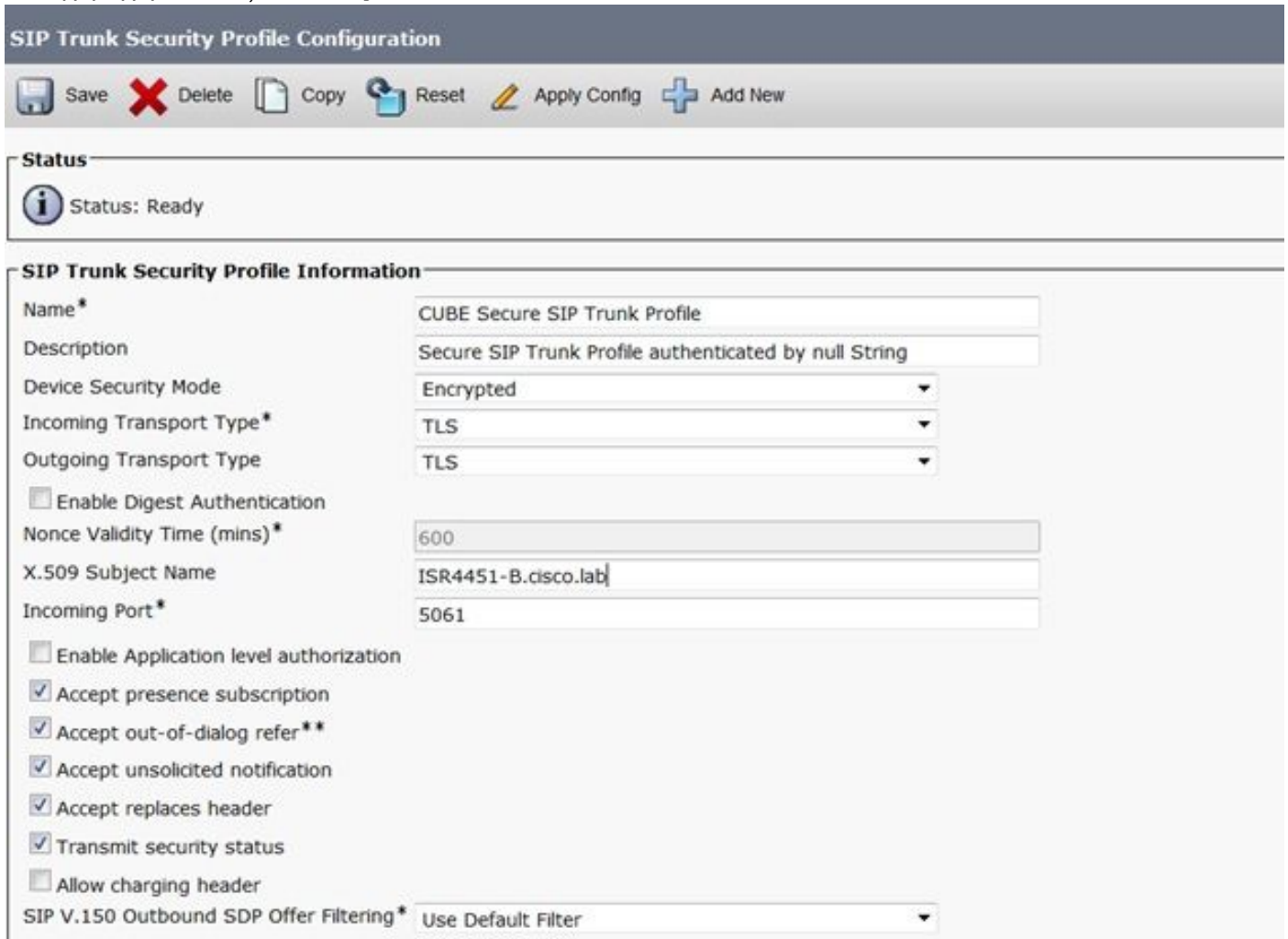
```
session transport tcp tls
```

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

```
srtplib
```

步骤9.配置CUCM SIP中继安全配置文件

- CUCM Admin页面> System > Security > SIP Trunk Security Profile
- 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

注意： 生成自签名证书时，X.509字段与您之前配置的CN名称匹配至关重要

步骤10.在CUCM上配置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
- 确保选择正确的SIP中继安全配置文件（在步骤9中创建）

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

- 保存并重置中继。

验证

由于您在CUCM上启用了OPTIONS PING，因此SIP中继必须处于FULL SERVICE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中继状态显示完全服务。

拨号对等体状态显示如下：

```
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

启用并收集这些调试的输出

```
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录制链接：

<https://goo.gl/QOS1iT>