

使用CA签名证书在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](#)

[验证](#)

[故障排除](#)

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。

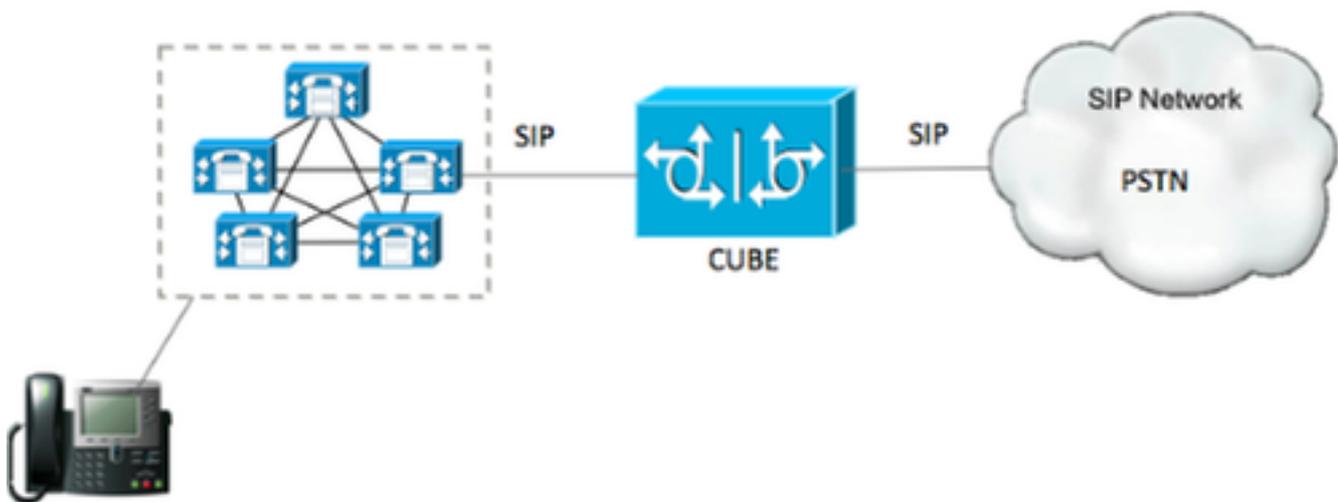
注意：对于Cisco IOS-XE 16.10版奖励，平台已移至智能许可。

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
rsaкеypair TestRSAkey !(this has to match the RSA key you just created)
```

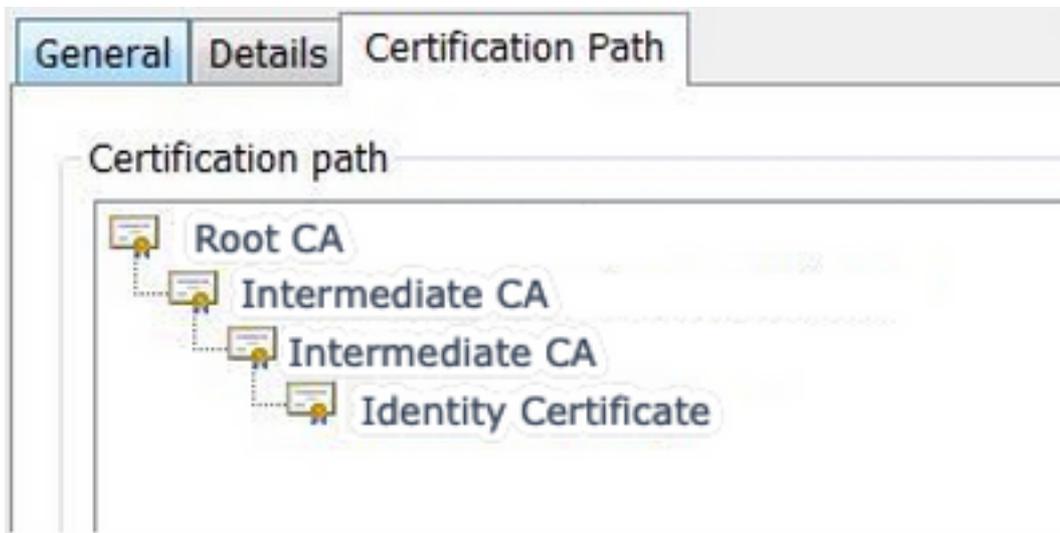
第3步：既然您拥有我们的信任点，您将使用以下命令生成我们的CSR请求：

```
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：

Generate Certificate Signing Request - Google Chrome

https://cucm10-5.cisco.lab/cmplatform/certificateGenerateNewCsr.do

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* cucm10-5.cisco.lab

Common Name* cucm10-5.cisco.lab

Subject Alternate Names (SANs)

Parent Domain cisco.lab

Key Length* 2048

Hash Algorithm* SHA256

Generate Close

*- indicates required item.

Central Time: 11:26 am Eastern Time: 12:26 pm Pacific Time: 9:26 am Mountain Time: 10:26 am

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，

SIP Trunk Security Profile Configuration

Save Delete Copy Reset Apply Config Add New

Status

 Status: Ready

SIP Trunk Security Profile Information

| | |
|---|--|
| Name* | <input type="text" value="CUBE_CA Secure SIP Trunk Profile"/> |
| Description | <input type="text" value="Secure SIP Trunk Profile authenticated by null String"/> |
| Device Security Mode | <input type="text" value="Encrypted"/> |
| Incoming Transport Type* | <input type="text" value="TLS"/> |
| Outgoing Transport Type | <input type="text" value="TLS"/> |
| <input type="checkbox"/> Enable Digest Authentication | |
| Nonce Validity Time (mins)* | <input type="text" value="600"/> |
| X.509 Subject Name | <input type="text" value="cucm10-5.cisco.lab"/> |
| Incoming Port* | <input type="text" value="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 checked="" type="checkbox"/> Transmit security status | |
| <input type="checkbox"/> Allow charging header | |
| SIP V.150 Outbound SDP Offer Filtering* | <input type="text" value="Use Default Filter"/> |

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。

Certificate Details for cucm10-5.cisco.lab, CallManager

Regenerate
 Generate CSR
 Download .PEM File
 Download .DER File

Status

Status: Ready

Certificate Settings

| | |
|----------------------------|--|
| Locally Uploaded | 10/02/16 |
| File Name | CallManager.pem |
| Certificate Purpose | CallManager |
| Certificate Type | certs |
| Certificate Group | product-cm |
| Description(friendly name) | Certificate Signed by AD-CONTROLLER-CA |

Certificate File Data

```
[
Version: V3
Serial Number: 1D255E0000000000000007
SignatureAlgorithm: SHA256withRSA (1.2.840.113549.1.1.11)
Issuer Name: CN=AD-CONTROLLER-CA, DC=cisco, DC=lab
Validity From: Wed Feb 10 10:45:23 CST 2016
           To: Fri Feb 10 10:55:23 CST 2017
Subject Name: CN=cucm10-5.cisco.lab, OU=TAC, O=CISCO, L=RICHARSON, ST=TEXAS, C=US
Key: RSA (1.2.840.113549.1.1.1)
Key value:
3082010a0282010100ae8db062881c35163f1b6ee4be4951158fdb3495d3c8032170c9fb8bafb385a2
27b00ec1024807f0adc49df875189779c7de1ae1e7e64b45e6f9917fa6ca5687d9aeaf20d70018e8d5
58a832360b82702249fc98855012c7d2cc29eea0f92fad9e739d73b0fa24d7dd4bd9fc96be775fda997
f03a440645ad64fa9f083ed95445e200187dd8775aa543b2bab11a5e223e23ef03bb86bb9fd969b3d9
3ba2550c35ea06ed5149aef2253c2455a622122e0aa3b649a090911995069a2cfd4ab4ab1fe15b242
]
```

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。

SIP Information

Destination

Destination Address is an SRV

| Destination Address | Destination Address IPv6 | Destination Port |
|---------------------|--------------------------|------------------|
| 1* [redacted] | | 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

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 | | | 0711-Service | | | | | 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
```