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

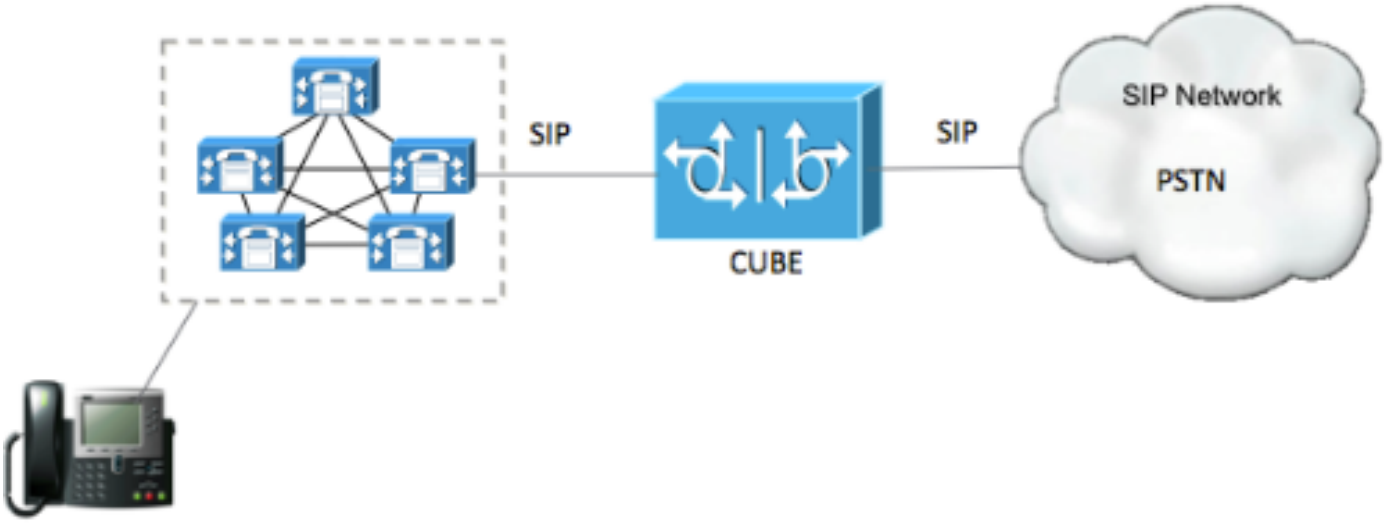
- 终端上的日期和时间必须匹配（建议使用相同的NTP源）。
- CUCM必须处于混合模式。
- 需要TCP连接（任何传输防火墙上的开放端口5061）。
- CUBE必须安装安全许可证和UCK9许可证。

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，请运行命令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，您必须看到此输出

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

步骤3.获取证书后，需要导出证书

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

上述命令必须生成以下证书

```
% Self-signed CA certificate:
-----BEGIN CERTIFICATE-----
MIIBgDCCASqgAwIBAgIBATANBgkqhkiG9w0BAQUFADAeMRwwGgYDVQQDExNJU1I0
NDUxLUIuY2lzY28ubGFiMB4XDTE1MTIxNTAxNTAxNVoXDTIwMDEwMTAwMDAwMFow
HjEcMBoGA1UEAxMTSVNSNDQ1MS1CLmNpc2NvLmxhYjBcMA0GCSqGSIb3DQEBAQUA
A0sAMEgCQQDGtZ974Tfv+pngs1+cCeLZ/e0b2zq6CrIj4T1t+NSlG5sjMJ919/ix
7Fa6DG33LmEYUM1NntkLaz+8UNDAyBZrAgMBAAGjUzBRMA8GA1UdEwEB/wQFMAMB
Af8wHwYDVR0jBBgwFoAU+Yy1UqKdb+rrINc7tZcrdIRMKPowHQYDVR0OBBYEFPmM
tVKinW/q6yDXO7WXK3SETCj6MA0GCSqGSIb3DQEBBQUAA0EADQXG2FYZ/MSewjSH
T88SHXq0EVqcLrgGpScwcpbR1mKFPpIhDVaJfH/FC6jnkGW7JFWcekA5Kp0tzYx4
LDQaxQ==
-----END CERTIFICATE-----

% General Purpose Certificate:
-----BEGIN CERTIFICATE-----
MIIBgDCCASqgAwIBAgIBATANBgkqhkiG9w0BAQUFADAeMRwwGgYDVQQDExNJU1I0
NDUxLUIuY2lzY28ubGFiMB4XDTE1MTIxNTAxNTAxNVoXDTIwMDEwMTAwMDAwMFow
HjEcMBoGA1UEAxMTSVNSNDQ1MS1CLmNpc2NvLmxhYjBcMA0GCSqGSIb3DQEBAQUA
A0sAMEgCQQDGtZ974Tfv+pngs1+cCeLZ/e0b2zq6CrIj4T1t+NSlG5sjMJ919/ix
7Fa6DG33LmEYUM1NntkLaz+8UNDAyBZrAgMBAAGjUzBRMA8GA1UdEwEB/wQFMAMB
Af8wHwYDVR0jBBgwFoAU+Yy1UqKdb+rrINc7tZcrdIRMKPowHQYDVR0OBBYEFPmM
```

```
tVKinW/q6yDXO7WXK3SETCj6MAOGCSqGSIb3DQEBBQUAAOEADQXG2FYZ/MSewjSH

T88SHXqOEVqcLrgGpScwcpbR1mKFPpIhDVaJfH/FC6jnkGW7JFWcekA5KpOtzYx4

LDQaxQ==

-----END CERTIFICATE-----
```

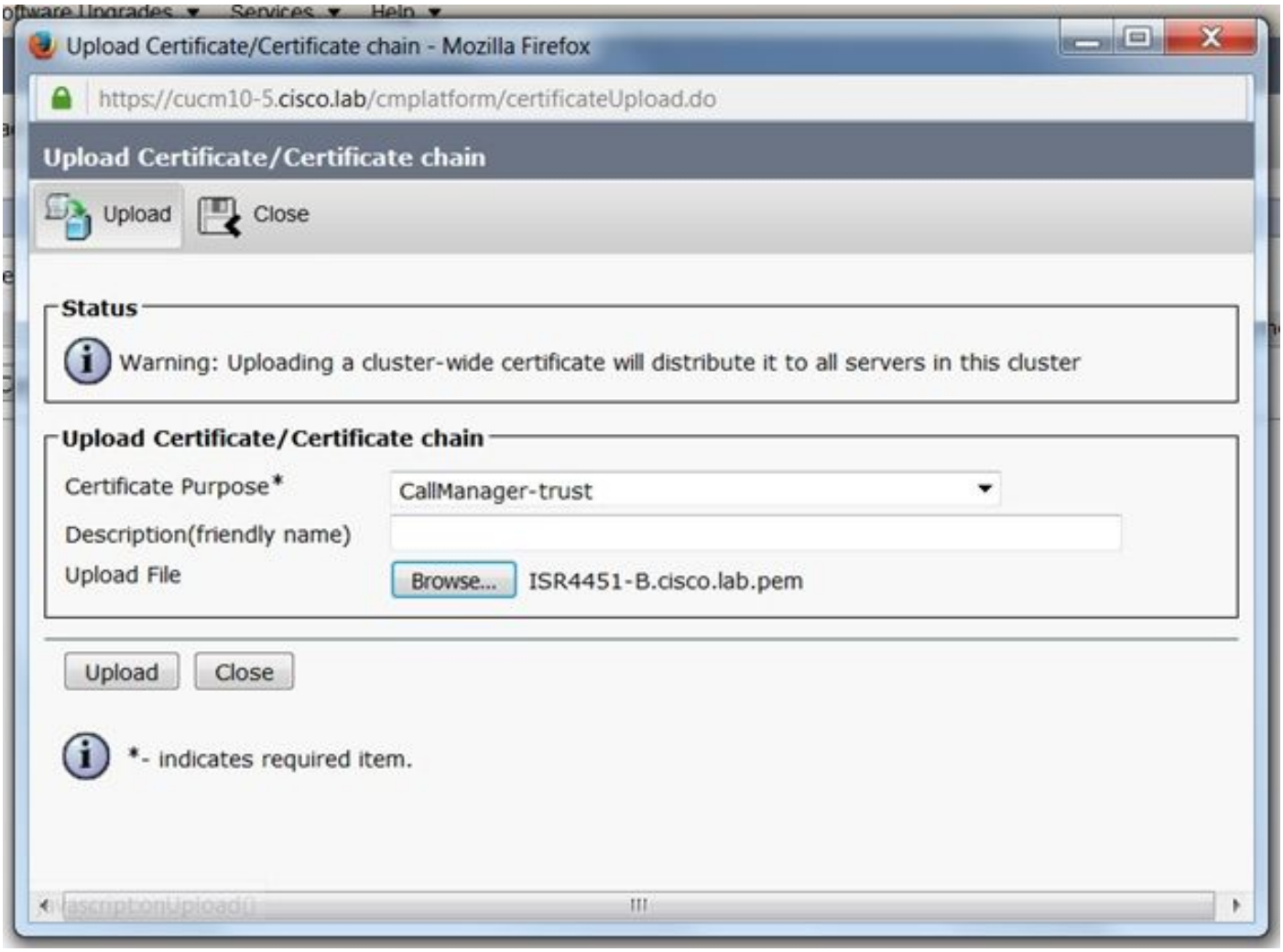
复制上述生成的自签名证书并将其粘贴到文件扩展名为.pem的文本文件

以下示例命名为ISR4451-B.ciscolab.pem



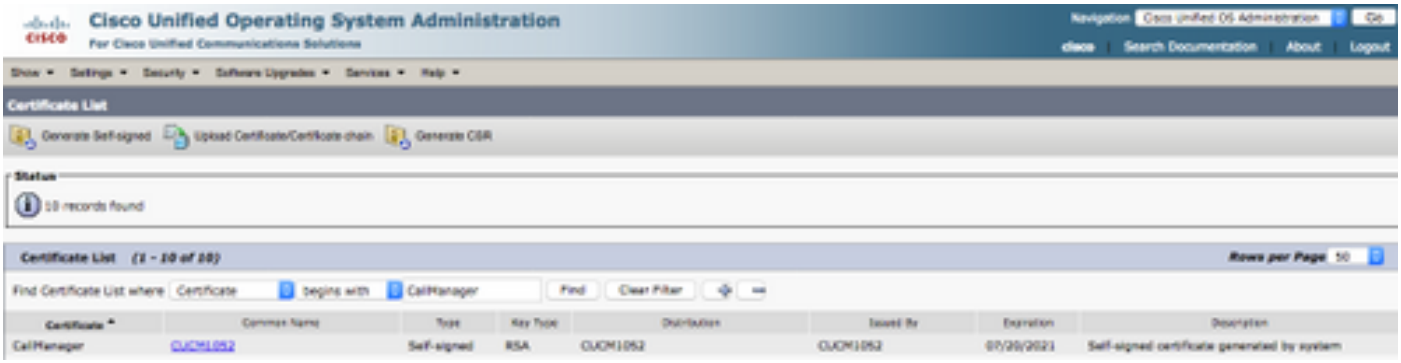
步骤4.将CUBE证书上传到CUCM

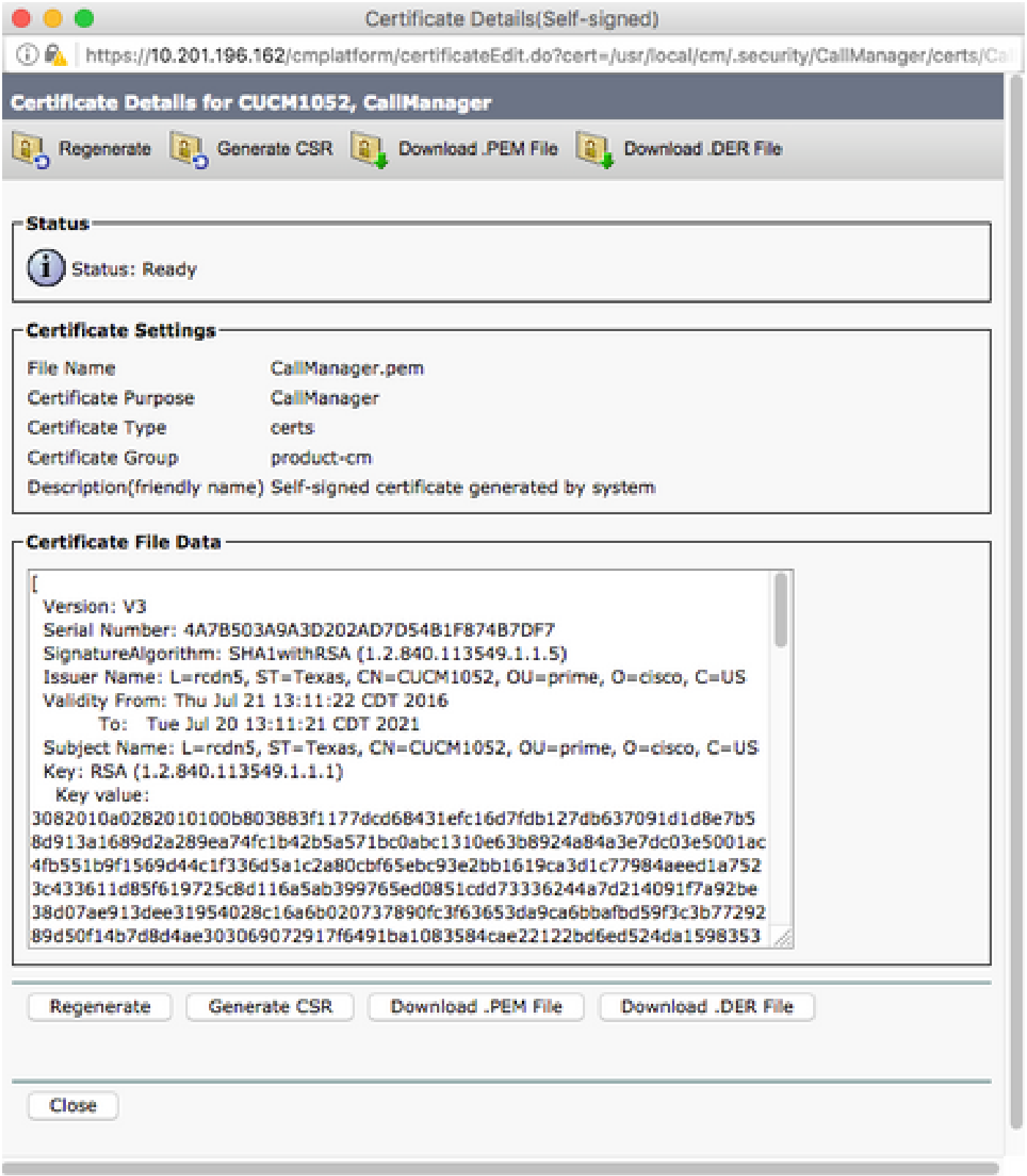
- CUCM OS Admin > Security > Certificate Management > Upload Certificate/Certificate chain
- 证书用途= CallManager-Trust
- 上传。pem文件



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
- 将其保存到您的计算机





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
- 复制文件的全部内容
- 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

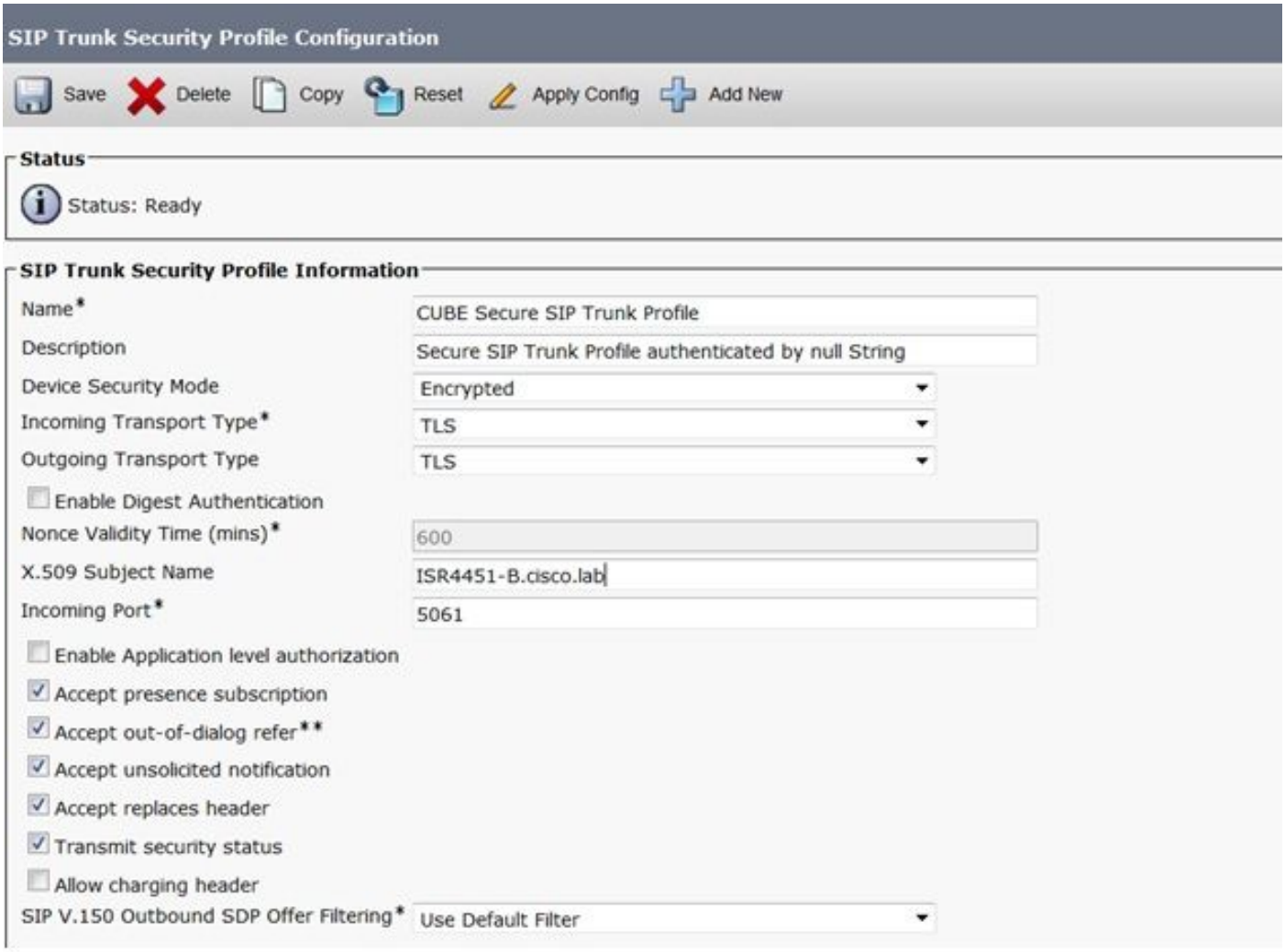
session transport tcp tls

voice-class sip options-keepalive

srtp
```

步骤9.配置CUCM SIP中继安全配置文件

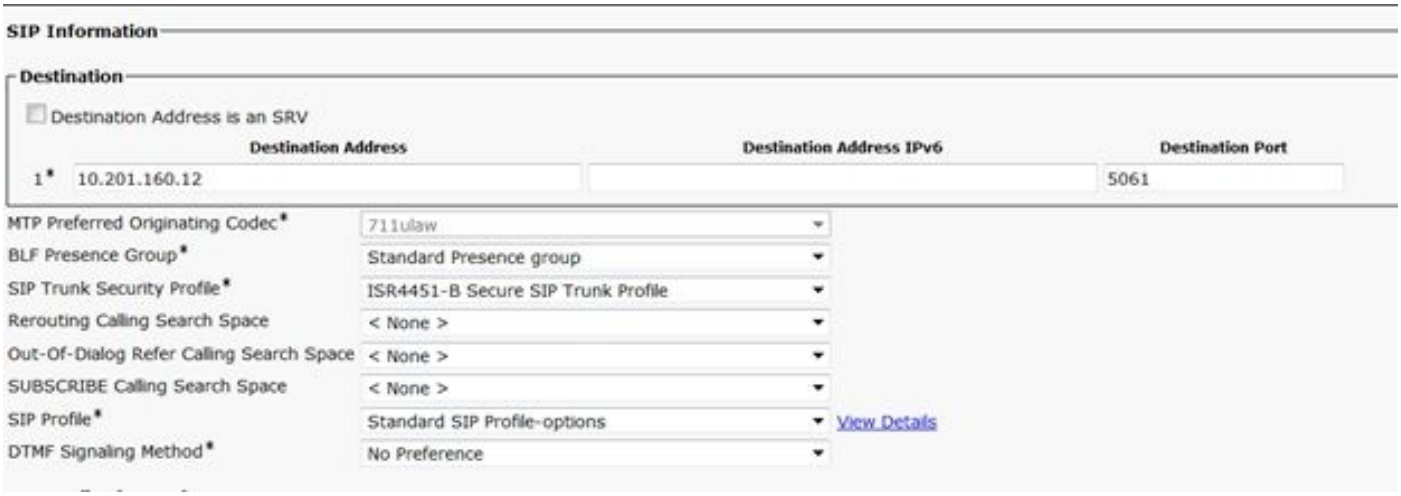
- CUCM Admin page > System > Security > SIP Trunk Security Profile
- 配置配置文件，如下所示



注意： 在生成自签名证书时，X.509字段与之前配置的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
- 配置正确的目的地址并确保将端口5060替换为端口5061
- 确保选择正确的Sip中继安全配置文件（已在步骤9中创建）



- 保存并重置中继。

验证

由于您在CUCM上启用了选项PING，因此SIP中继必须处于完全服务状态



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    KEEPALIVE

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

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。