Configurar TLS SIP entre CUCM-CUBE/CUBE-SBC

Contents

Table Of Contents

Introduction

Este documento ajuda a configurar o SIP Transport Layer Security (TLS) entre o Cisco Unified Communication Manager (CUCM) e o Cisco Unified Border Element (CUBE)

Prerequisites

A Cisco recomenda ter conhecimento desses assuntos

- Protocolo SIP
- Certificados de segurança

Requirements

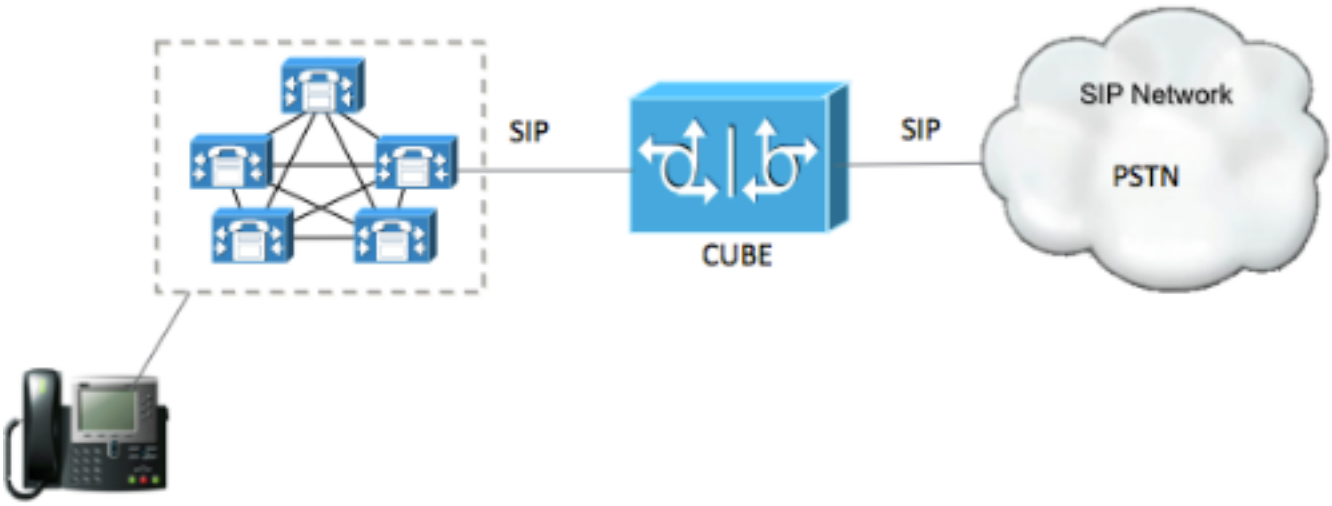
- A data e a hora devem coincidir nos endpoints (recomenda-se ter a mesma origem NTP).
- O CUCM deve estar em modo misto.
- A conectividade TCP é necessária (porta aberta 5061 em qualquer firewall de trânsito).
- O CUBE deve ter a segurança e as licenças UCK9 instaladas.

Componentes Utilizados

- SIP
- Certificados autoassinados

Configurar

Diagrama de Rede



Configuration Steps

Etapa 1. Criar um ponto de confiança para manter o certificado autoassinado do CUBE

```
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)
```

Etapa 2. Uma vez criado o ponto de confiança, você executa o comando **Crypto pki enroll CUBE test** para obter certificados autoassinados

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

Se a inscrição estiver correta, você deve esperar a saída

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

Etapa 3. Depois de obter o certificado, você precisa exportá-lo

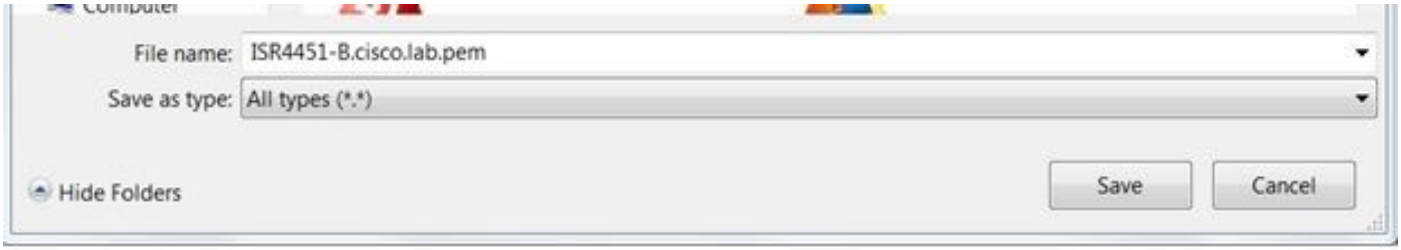
```
crypto pki export CUBEtest pem terminal
```

O comando acima deve gerar o certificado abaixo

```
% 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/q6yDXO7WXK3SETCj6MA0GCSqGSIb3DQEBBQUAA0EADQXG2FYZ/MSewjSH

T88SHXq0EVqcLrgGpScwcpbR1mKFPpIhDVaJfH/FC6jnkGW7JFWcekA5Kp0tzYx4

LDQaxQ==

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

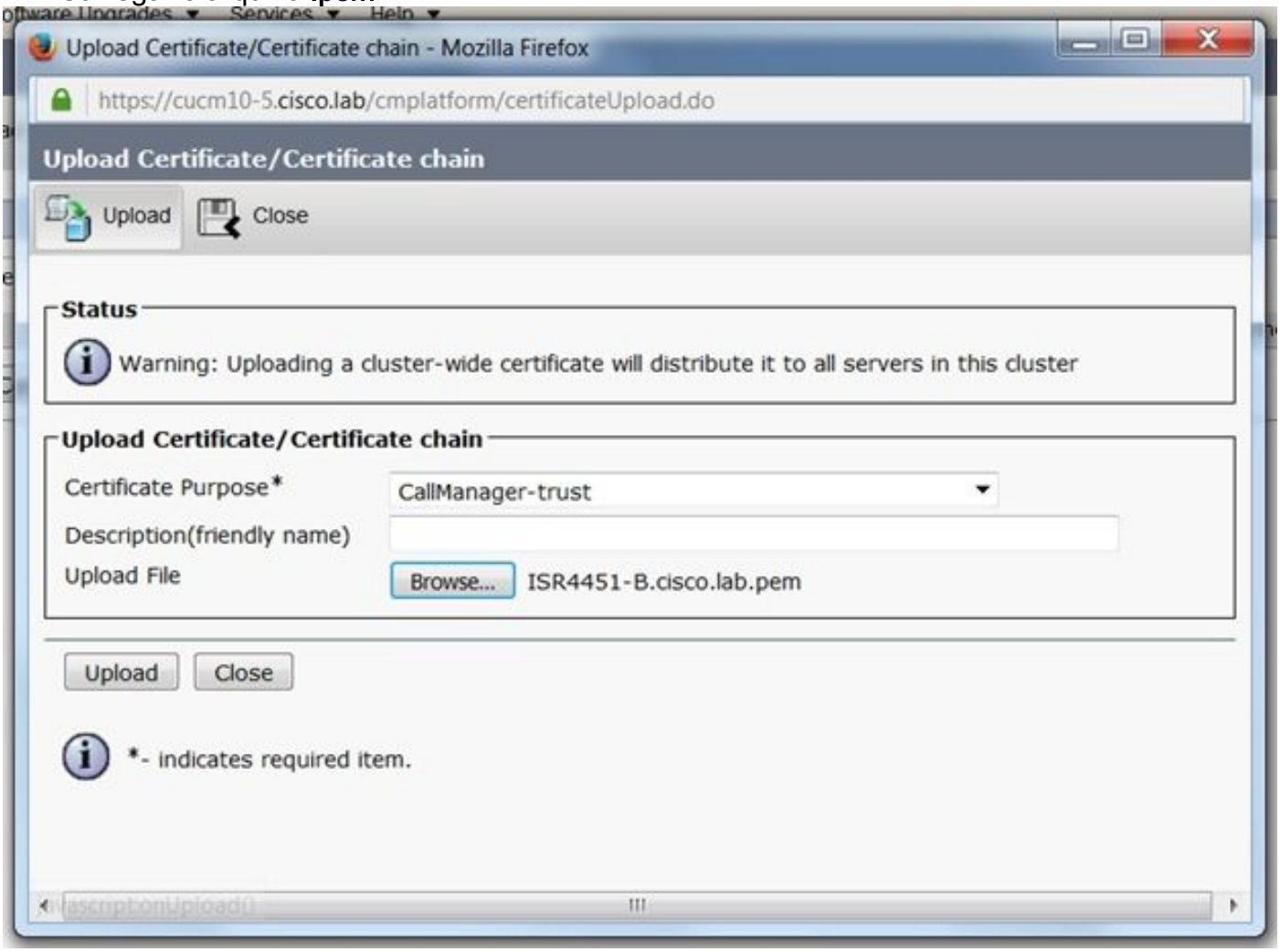
Copie o certificado autoassinado gerado acima e cole-o em um arquivo de texto com extensão de arquivo **.pem**

O exemplo abaixo é nomeado como ISR4451-B.ciscolab.pem



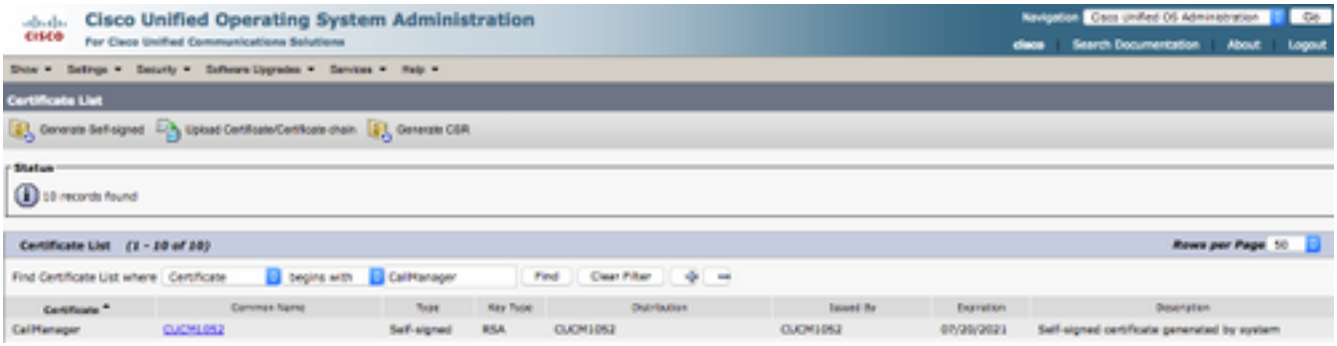
Etapa 4. Carregar o certificado do CUBE para o CUCM

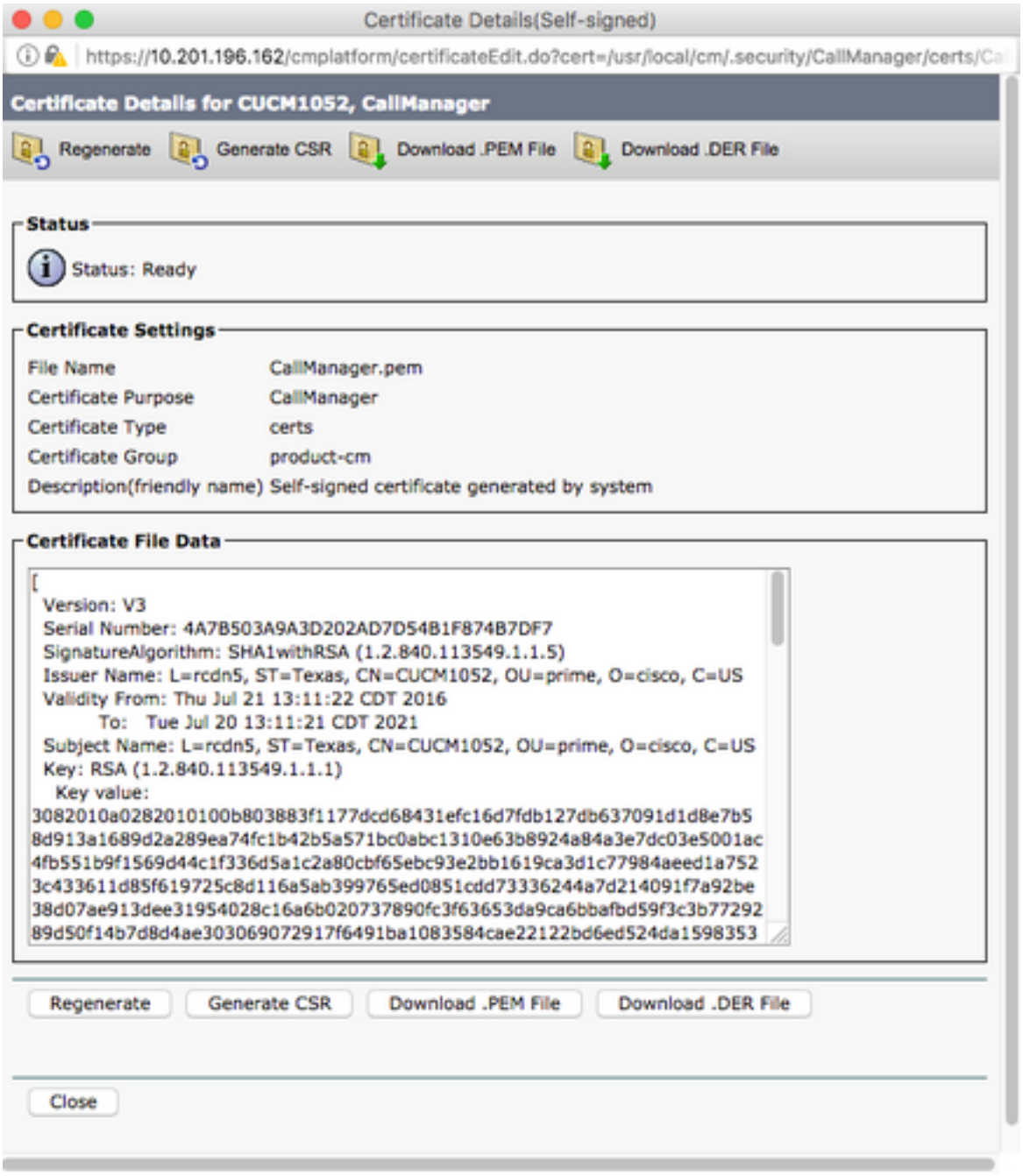
- Administrador do SO CUCM > Segurança > Gerenciamento de certificado > Carregar certificado/cadeia de certificados
- Finalidade do certificado = CallManager-Trust
- Carregar o arquivo **.pem**



Etapa 5. Baixar o certificado autoassinado do Call Manager

- Localize o certificado que diz Callmanager
- Clique no nome do host
- Clique em baixar arquivo PEM
- Guardar no computador





Etapa 6. Carregue o certificado Callmanager.pem para CUBE

- Abra o Callmanager.pem com um editor de arquivos de texto
- Copiar todo o conteúdo do arquivo
- Execute estes comandos no CUBE

```
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
```

Passo 7. Configurar o SIP para usar o ponto de confiança de certificado autoassinado do CUBE

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

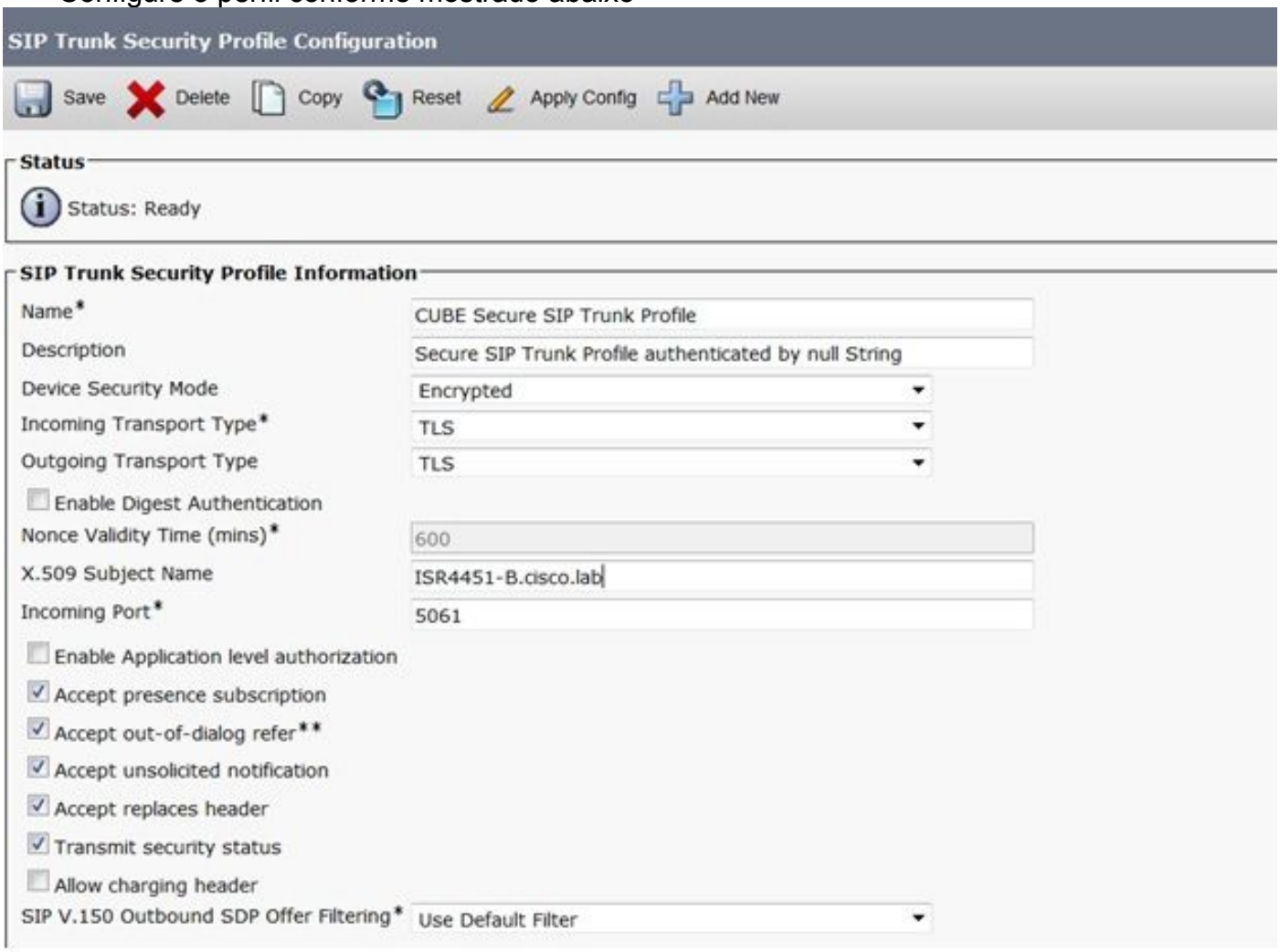
Etapa 8. Configurar os correspondentes de discagem com TLS

```
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
```

Etapa 9. Configurar um perfil de segurança de tronco SIP do CUCM

- Página do administrador do CUCM > Sistema > Segurança > Perfil de segurança do tronco SIP
- Configure o perfil conforme mostrado abaixo



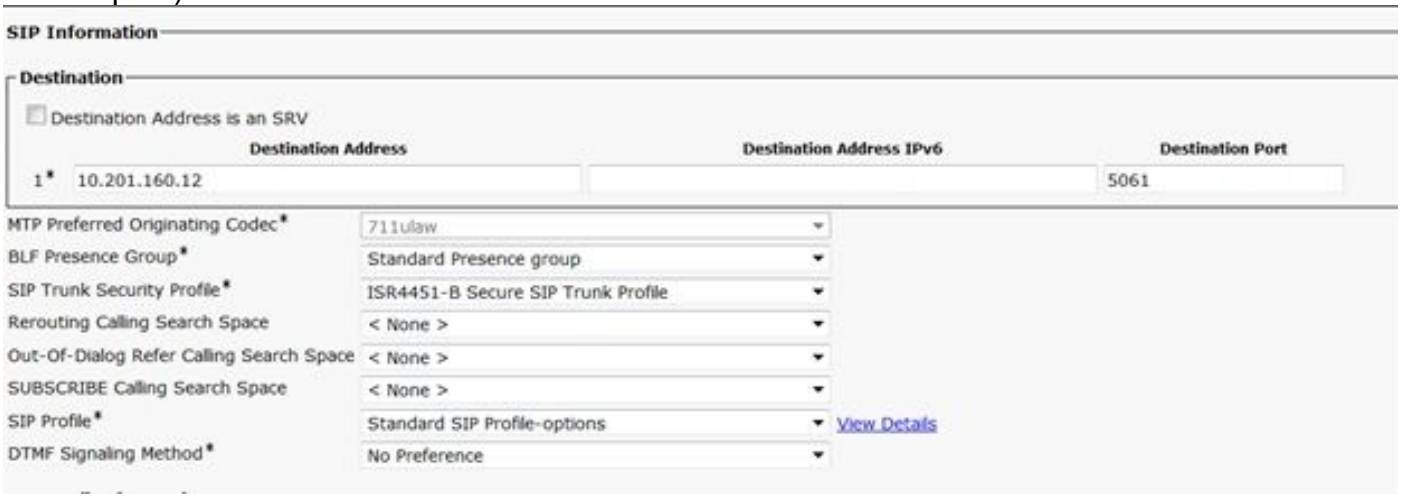
Observação: é extremamente importante que o campo X.509 corresponda ao nome CN configurado anteriormente enquanto você gerava o certificado autoassinado

Etapa 10. Configurar um tronco SIP no CUCM

- Verifique se a caixa de seleção SRTP permitido está marcada
- Configure o endereço de destino apropriado e certifique-se de substituir a porta 5060 pela

porta 5061

- Certifique-se de selecionar o perfil de segurança de tronco Sip correto (que foi criado na Etapa 9)



- Salve e reinicie o tronco.

Verificar

Como você ativou o PING DE OPÇÕES no CUCM, o tronco SIP deve estar no estado SERVIÇO COMPLETO

O status do tronco SIP mostra o serviço completo.

O status do peer de discagem é mostrado da seguinte maneira:

```
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
```

Troubleshoot

Habilitar e coletar a saída dessas depurações

```
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
```

Link de gravação do Webex:

https://goo.gl/QOS1iT