Configuración de SIP TLS entre CUCM-CUBE/CUBE-SBC

Contenido

Table Of Contents

Introducción

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

Prerequisites

Cisco recomienda tener conocimiento de estos temas

- Protocolo SIP
- Certificados de seguridad

Requirements

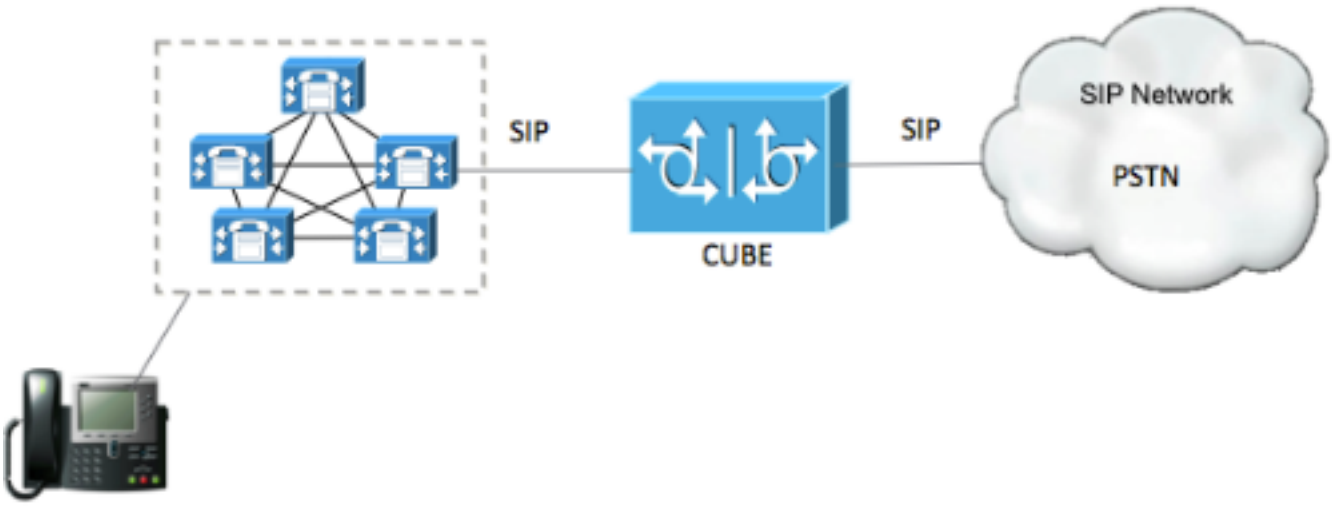
- La fecha y la hora deben coincidir en los puntos finales (se recomienda tener el mismo origen NTP).
- CUCM debe estar en modo mixto.
- Se requiere conectividad TCP (puerto abierto 5061 en cualquier firewall de tránsito).
- El CUBE debe tener instalada la seguridad y las licencias UCK9.

Componentes Utilizados

- SIP
- Certificados autofirmados

Configurar

Diagrama de la red



Configuration Steps

Paso 1. Cree un punto de confianza para conservar el certificado autofirmado de 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)
```

Paso 2. Una vez creado el punto de confianza, ejecuta el comando **Crypto pki enroll CUBEtest** para obtener certificados autofirmados

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

Si la inscripción fue correcta, debe esperar este resultado

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

Paso 3. Después de obtener el certificado , debe exportarlo

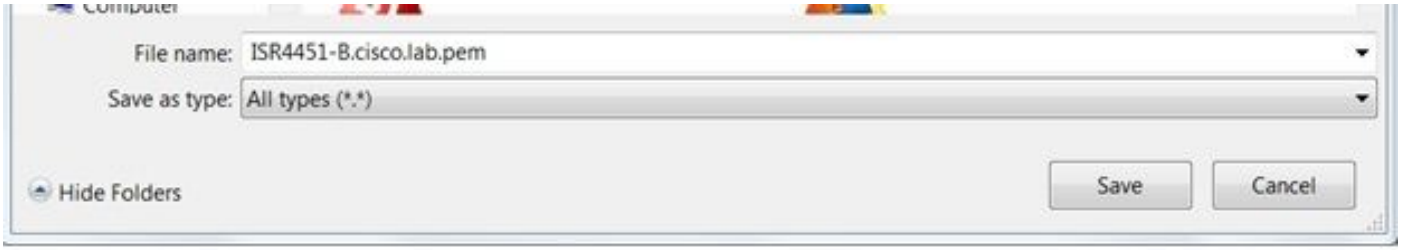
```
crypto pki export CUBEtest pem terminal
```

El comando anterior debe generar el siguiente certificado

```
% 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-----
```

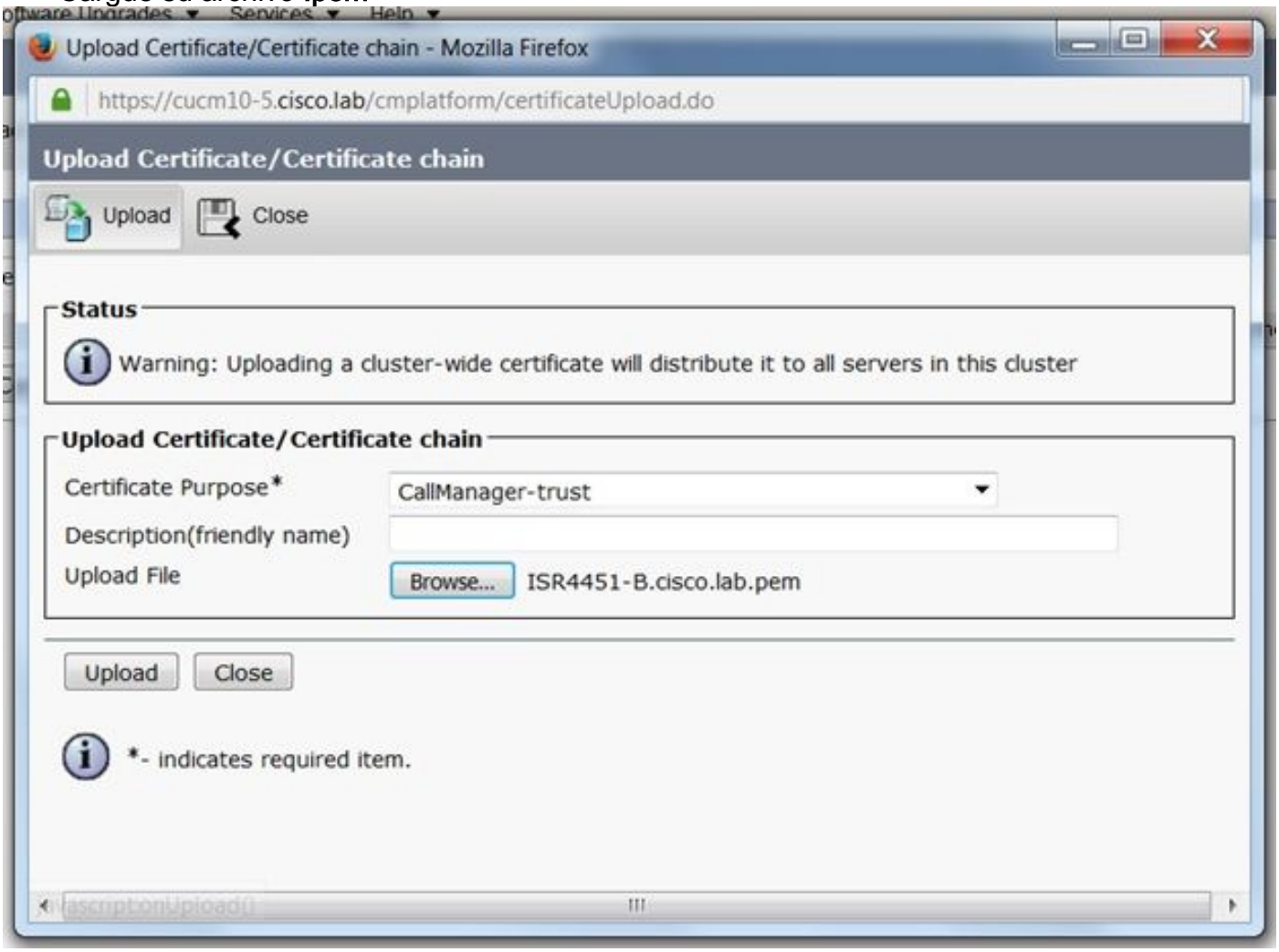
Copie el certificado autofirmado generado anteriormente y péguelo en un archivo de texto con extensión de archivo **.pem**

El siguiente ejemplo se denomina ISR4451-B.ciscolab.pem



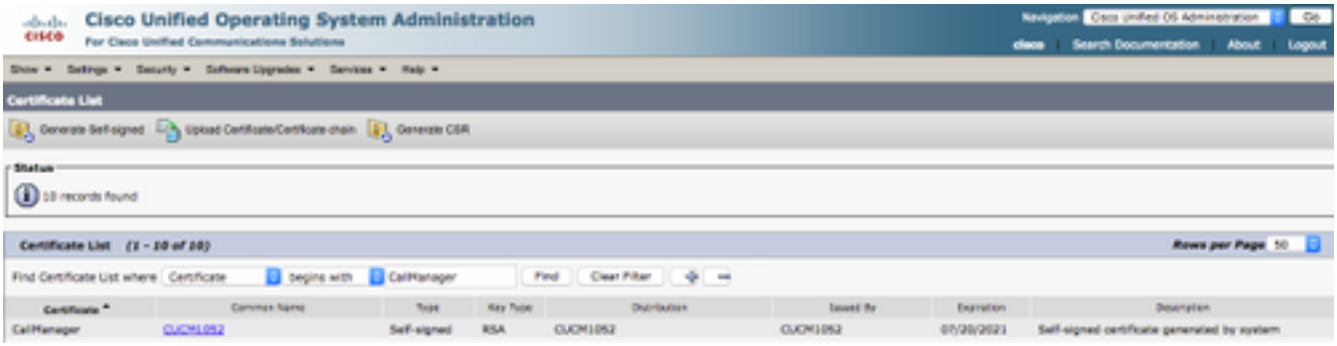
Paso 4. Cargar el certificado CUBE en CUCM

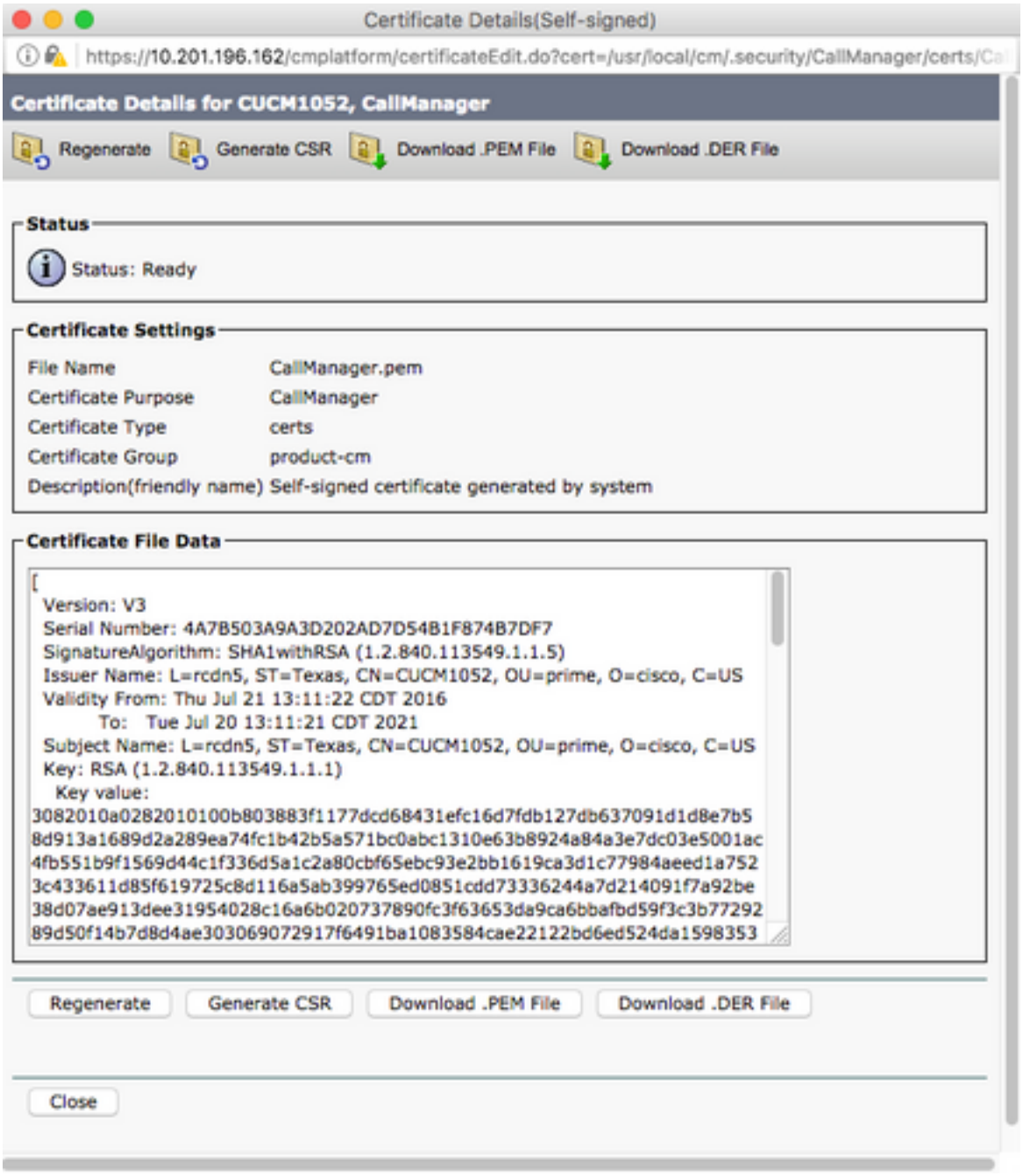
- CUCM OS Admin > Security > Certificate Management > Upload Certificate/Certificate chain
- Objetivo del certificado = CallManager-Trust
- Cargue su archivo **.pem**



Paso 5. Descargue el certificado autofirmado del Call Manager

- Busque el certificado que indica Callmanager
- Haga clic en el nombre de host
- Haga clic en Descargar archivo PEM
- Guárdelo en el ordenador





Paso 6. Cargue el certificado Callmanager.pem en CUBE

- Abra Callmanager.pem con un editor de archivos de texto
- Copiar todo el contenido del archivo
- Ejecute estos comandos en el 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
```

Paso 7. Configuración de SIP para utilizar el punto de confianza de certificados autofirmado de CUBE

```
sip-ua

 crypto signaling default trustpoint CUBEtest
```

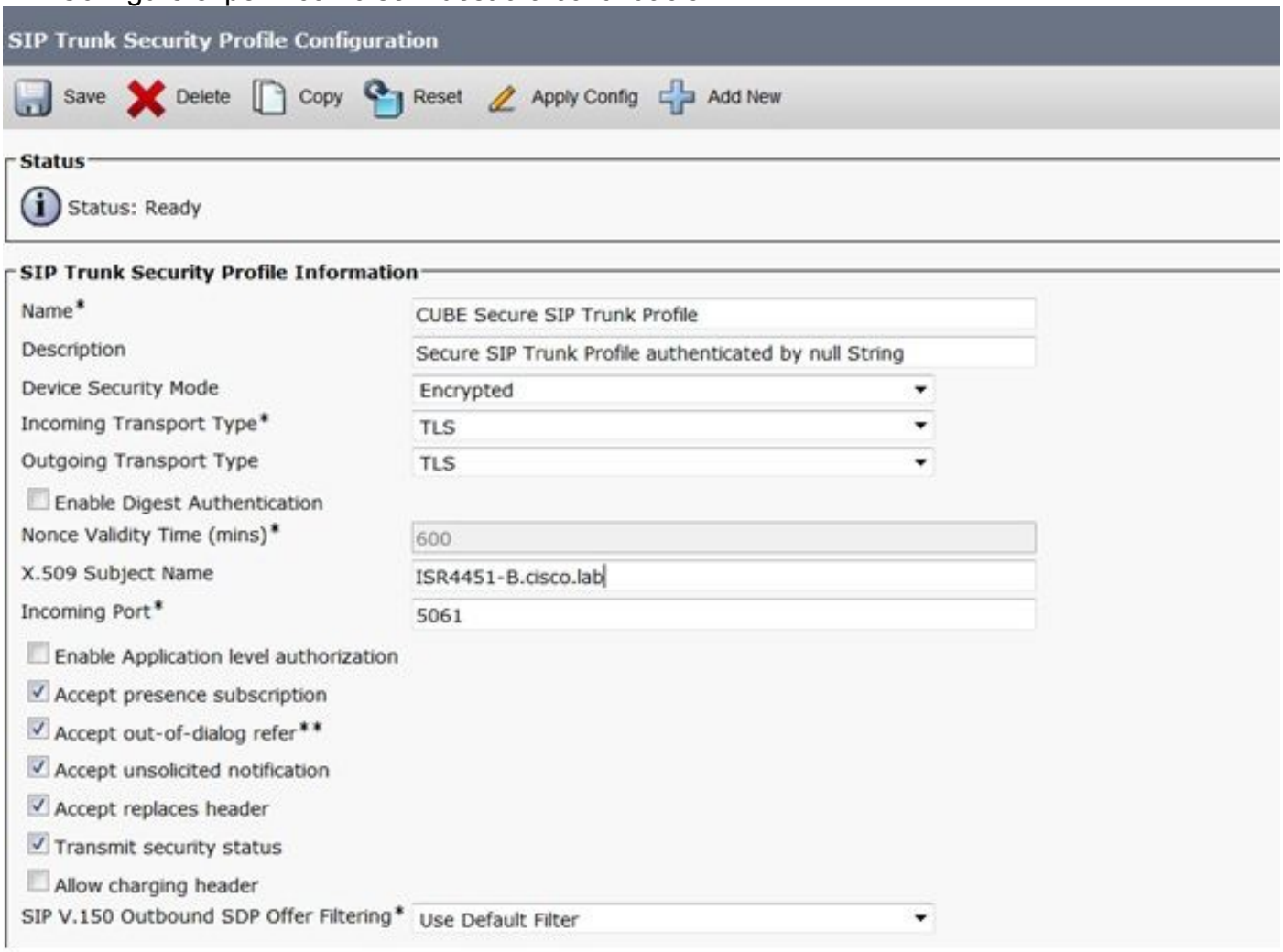
Paso 8. Configure los pares de marcado con TLS

```
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
```

Paso 9. Configuración de un perfil de seguridad troncal SIP de CUCM

- Página de administración de CUCM > System > Security > SIP Trunk Security Profile
- Configure el perfil como se muestra a continuación



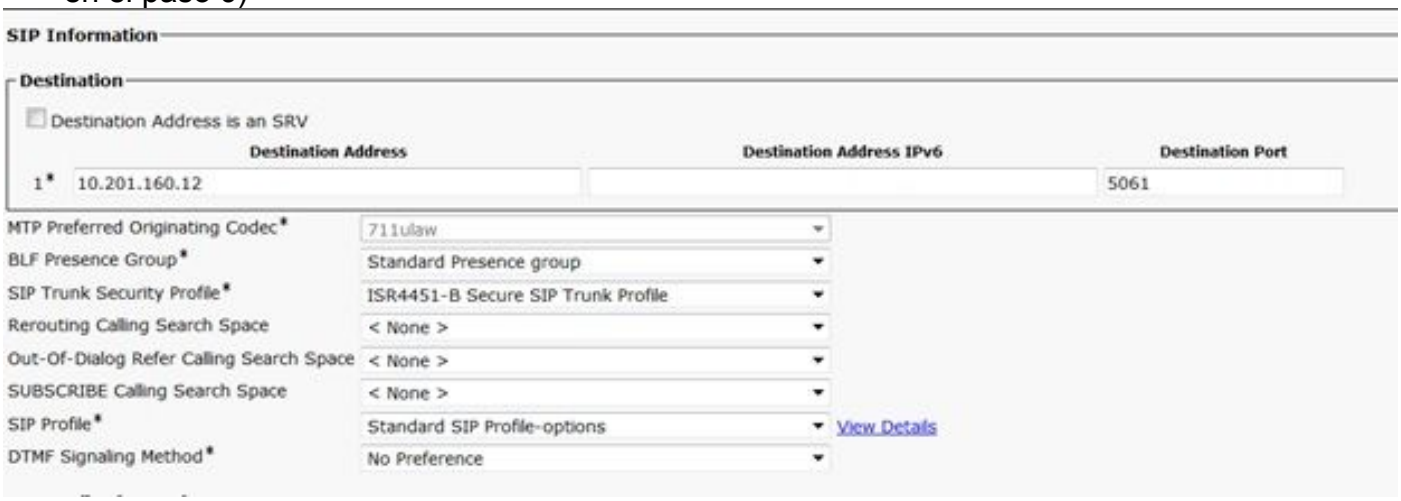
Nota: Es de vital importancia que el campo X.509 coincida con el nombre CN que configuró anteriormente mientras generaba el certificado autofirmado

Paso 10. Configuración de un tronco SIP en CUCM

- Asegúrese de que la casilla de verificación SRTP allowed esté marcada
- Configure la dirección de destino adecuada y asegúrese de reemplazar el puerto 5060 por el

puerto 5061

- Asegúrese de seleccionar el perfil de seguridad del enlace troncal Sip correcto (que se creó en el paso 9)



- Guarde y restablezca el tronco.

Verificación

Puesto que ha activado OPTIONS PING en CUCM, el troncal SIP debe estar en estado DE SERVICIO COMPLETO

El estado del troncal SIP muestra el servicio completo.

El estado del par de marcado muestra lo siguiente:

```
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 y recopilar el resultado de estas depuraciones

```
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
```

Enlace de grabación de Webex:

https://goo.gl/QOS1iT