SORBO TLS de la configuración entre CUCM-CUBE/CUBE-SBC

Contenido

Contenidos

Introducción

Este documento ayuda al SORBO Transport Layer Security (TLS) de la configuración entre Cisco unificó el administrador de la comunicación (CUCM) y el Cisco Unified Border Element (el CUBO)

Prerequisites

Cisco recomienda tener conocimiento de estos temas

- Protocolo del SORBO
- Certificados de la Seguridad

Requisitos

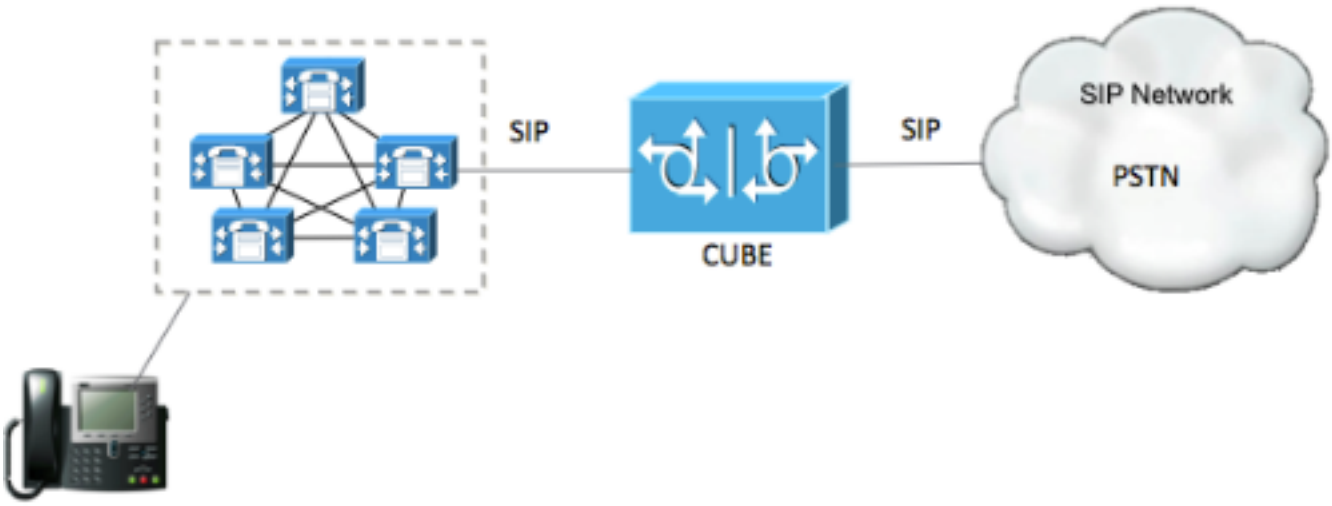
- La fecha y hora debe hacer juego en los puntos finales (se recomienda para tener la misma fuente NTP).
- CUCM debe estar en el modo mezclado.
- Se requiere la Conectividad TCP (el puerto abierto 5061 en ningunos transita el Firewall).
- El CUBO debe tener la Seguridad y las licencias UCK9 instaladas.

Componentes Utilizados

- SORBO
- Certificados de Selfsigned

Configurar

Diagrama de la red



Pasos para la configuración

Paso 1. Cree un trustpoint para sostener el certificado selfsigned del CUBO

```
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 que se crea la punta de la confianza usted funciona con el comando crypto que el **pki alista CUBEtest** para conseguir los certerticates uno mismo-firmados

```
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 estaba correcta usted debe contar con la esta salida

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

Paso 3. Después de que su obtenga el certificado, usted necesita exportarlo

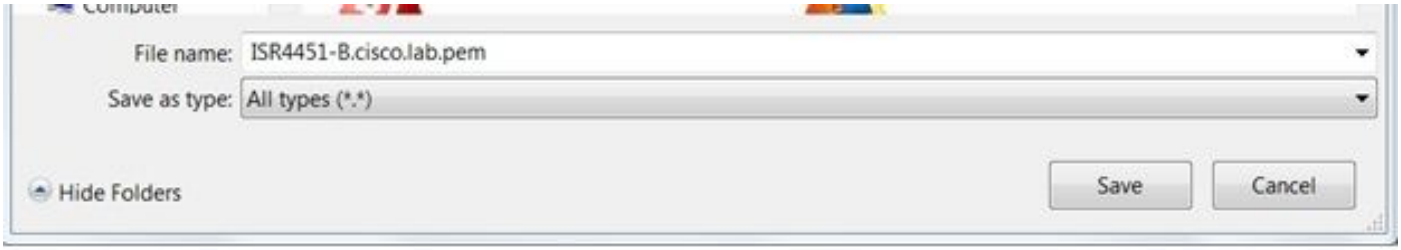
```
crypto pki export CUBEtest pem terminal
```

El comando antedicho debe generar el certificado abajo

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

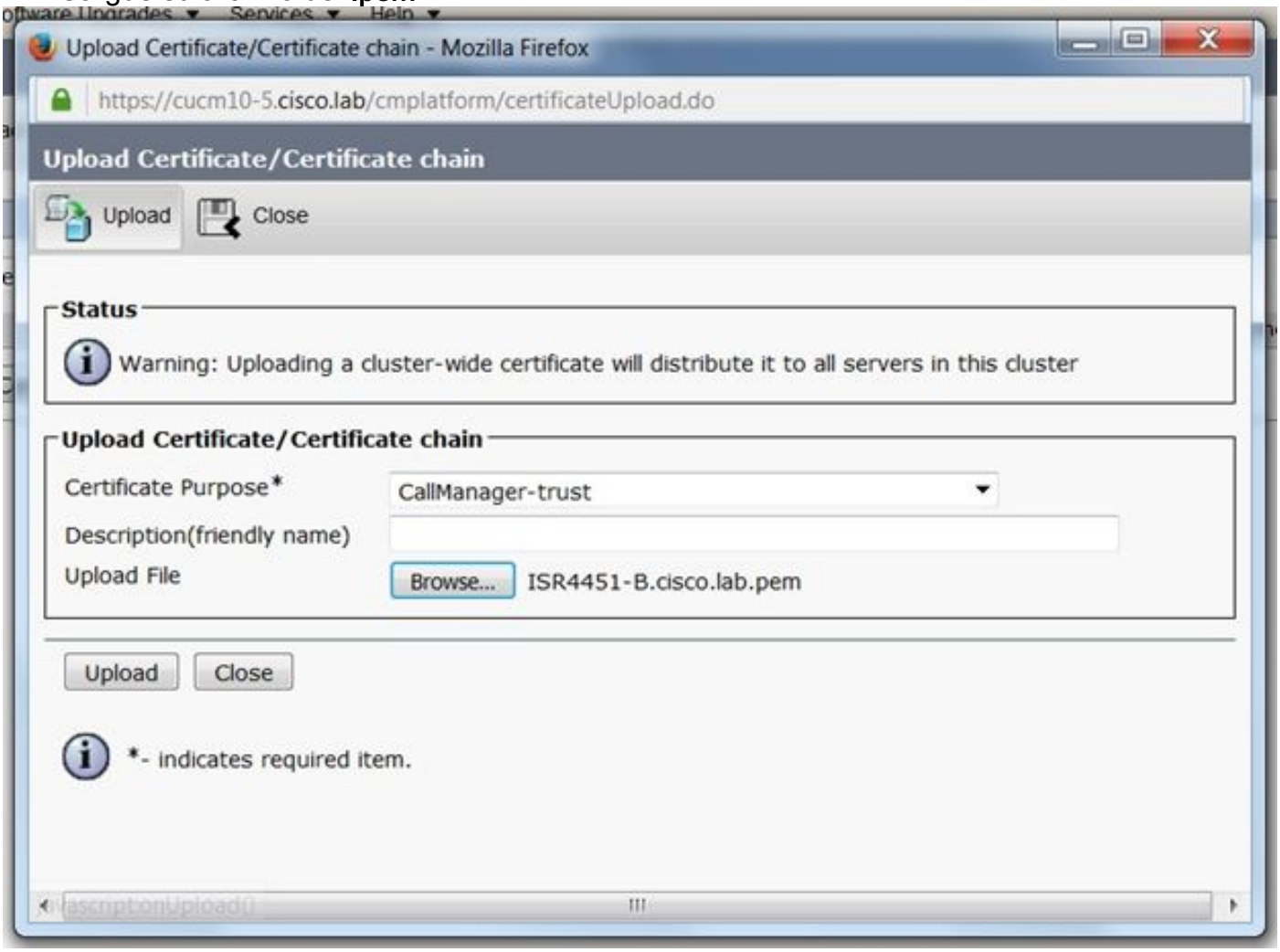
Copie el certificado firmado arriba generado del uno mismo y pegúelo a un archivo de texto con el **.pem de la** extensión de archivo

El ejemplo abajo se nombra como ISR4451-B.ciscolab.pem



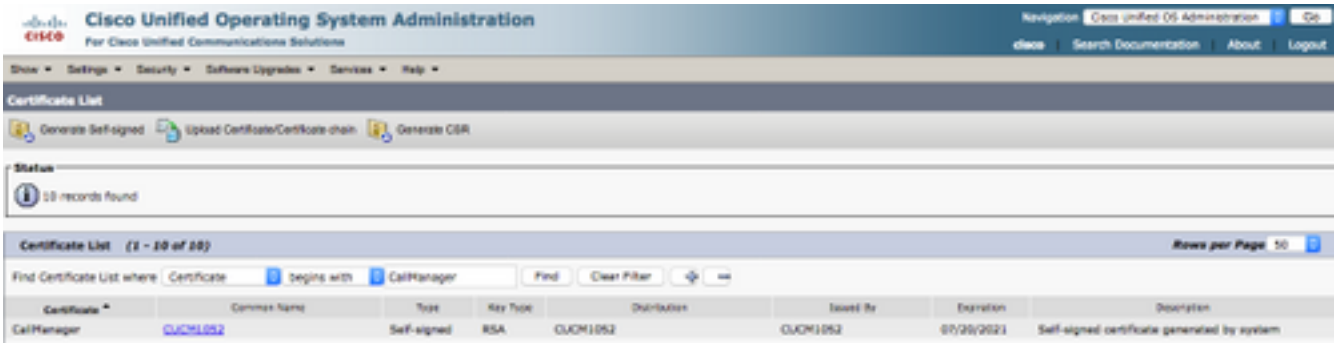
Paso 4. Cargue el certificado del CUBO al CUCM

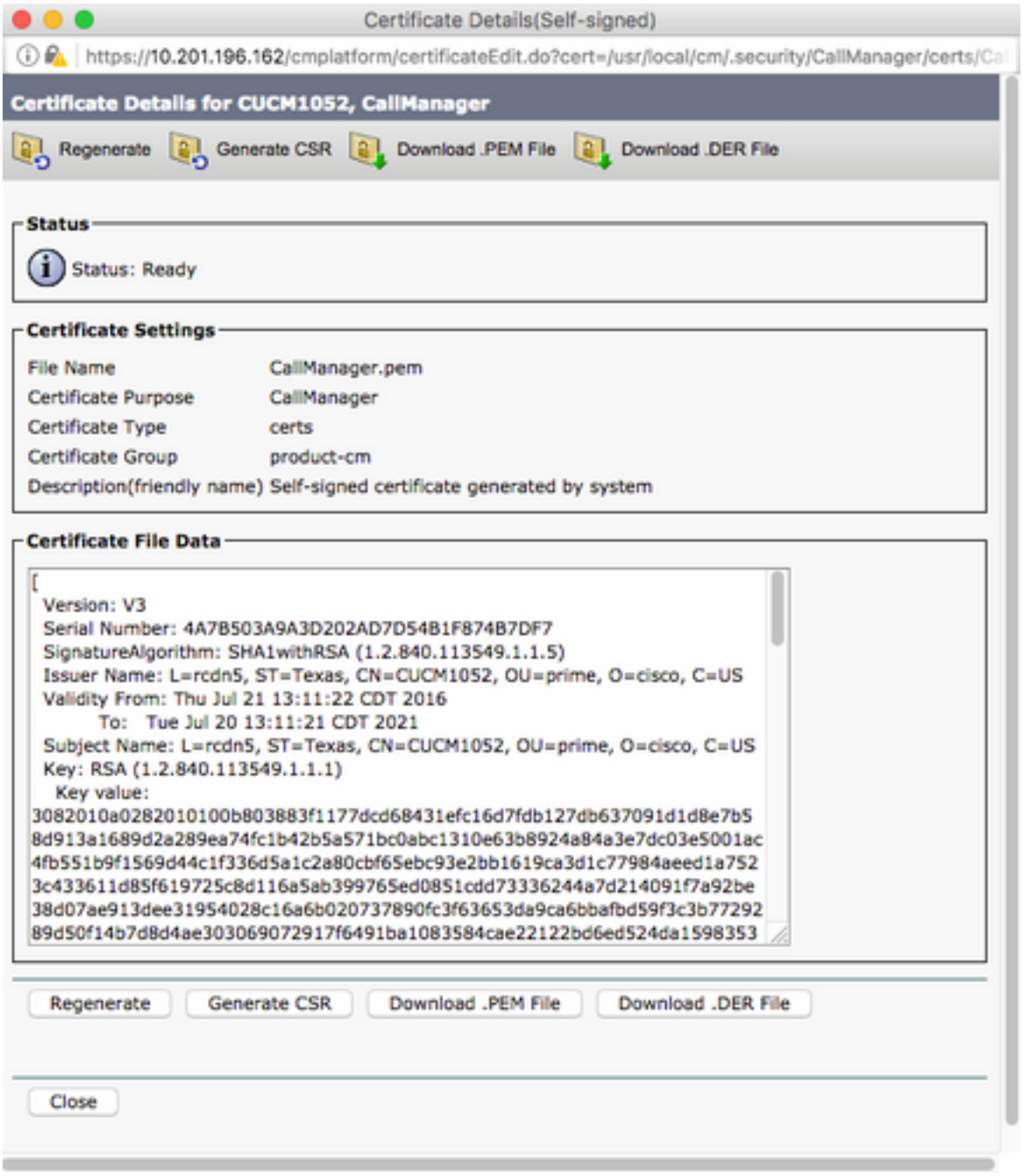
- Certificate Management (Administración de certificados) del > Security (Seguridad) CUCM OS Admin > certificado/Cadena de certificados de la carga
- Propósito = CallManager-confianza del certificado
- Cargue su archivo del **.pem**



Paso 5. Descargue el certificado autofirmado del administrador de llamada

- Encuentre el certificado que dice Callmanager
- Haga clic en el nombre del host
- Haga clic en el archivo de la descarga PEM
- Sálvelo a su ordenador





Paso 6. Cargue el certificado Callmanager.pem PARA CUBICAR

- Abra el Callmanager.pem con un editor del archivo de texto
- Copie el contenido del conjunto del archivo
- Ejecute esto ordena en el CUBO

```
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. Configure el SORBO para utilizar el trustpoint selfsigned del certificado del CUBO

```
sip-ua

 crypto signaling default trustpoint CUBEtest
```

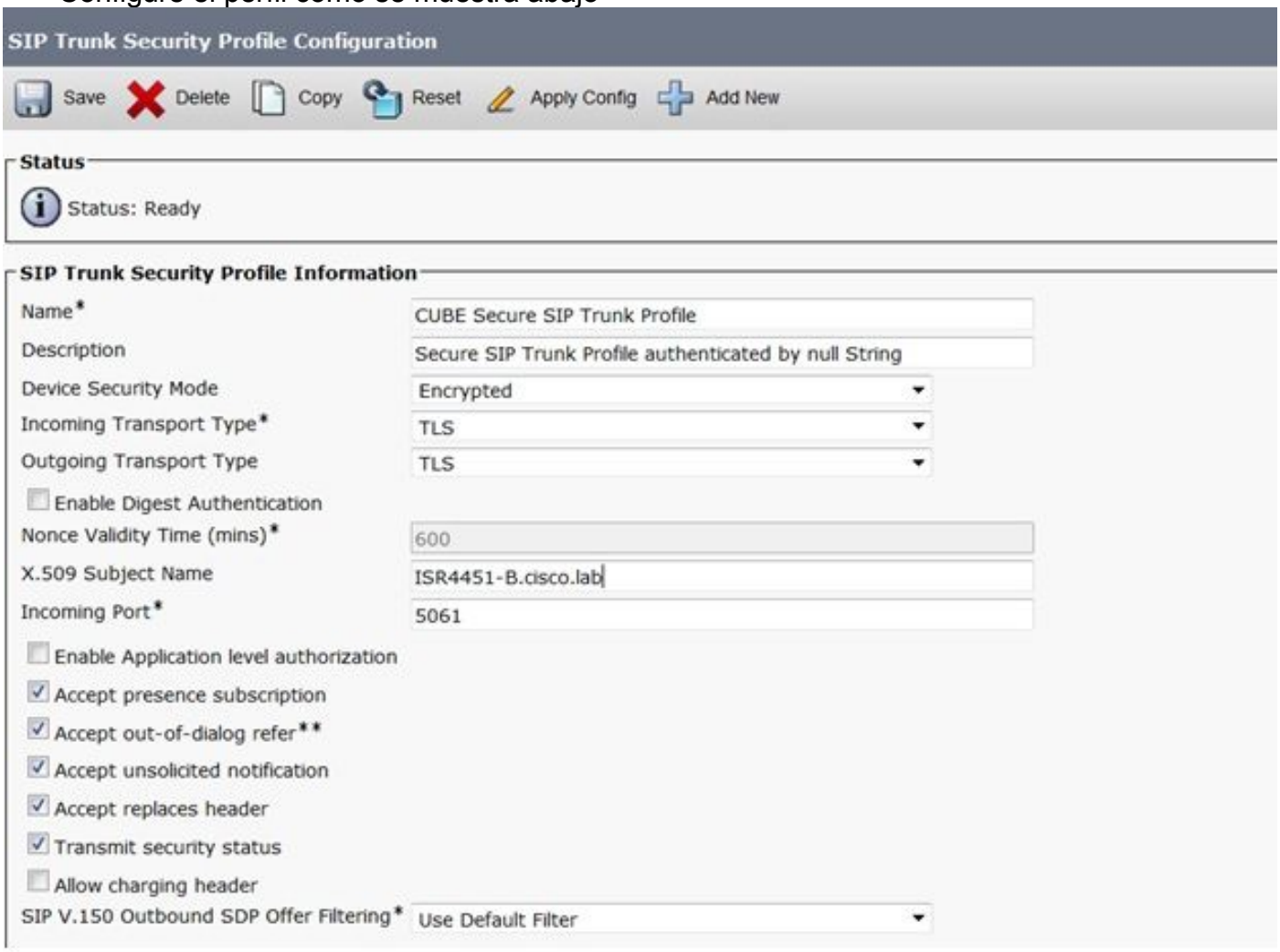
Paso 8. Configure a los dial peer con TLS

```
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. Configure un perfil de seguridad del trunk del SORBO CUCM

- >Security (Seguridad) de la página de administración > del sistema CUCM > perfil de seguridad del trunk del SORBO
- Configure el perfil como se muestra abajo



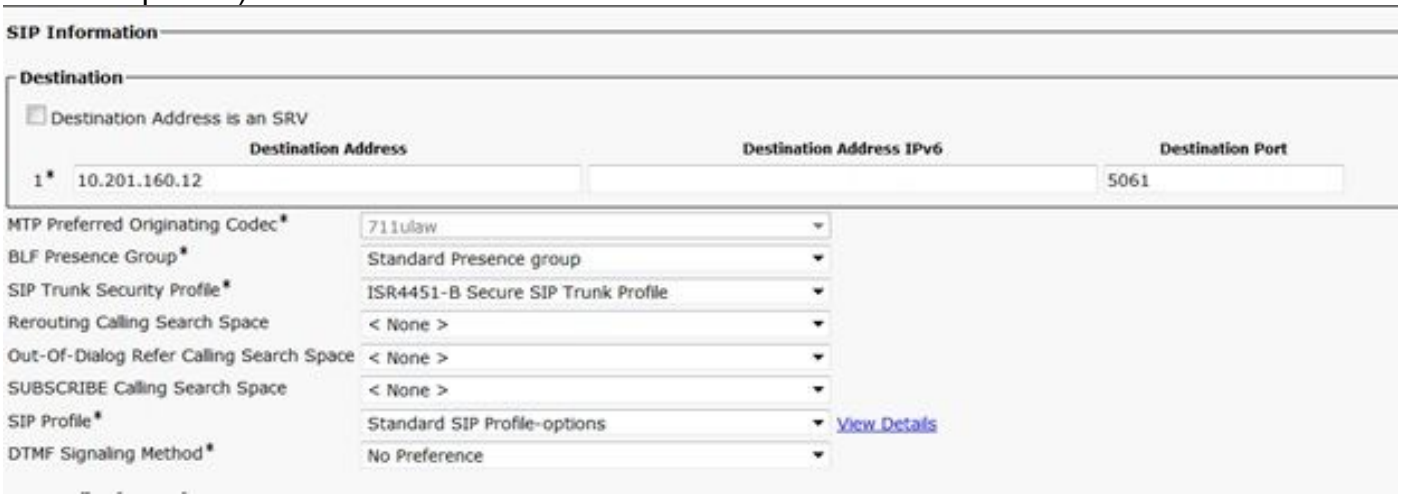
Note: Es críticamente importante que el campo X.509 hace juego el nombre CN que usted configuró previamente mientras que usted generaba el certificado autofirmado

Paso 10. Configure un trunk del SORBO en CUCM

- Asegúrese que la casilla de verificación permitida SRTP esté marcada
- Configure el direccionamiento de destino correcto y asegúrelo para substituir el puerto 5060

por el puerto 5061

- Asegure para seleccionar el perfil de seguridad correcto del trunk del sorbo (que fue creado en el paso 9)



- Salve y reajuste el trunk.

Verificación

Puesto que usted las OPCIONES habilitadas HACE PING en el CUCM, el trunk del SORBO debe estar en el estado de servicio FULL

El servicio completo de la demostración del estado del tronco del SORBO.

La demostración del estatus del dial peer como siguen:

```
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
```

Troubleshooting

Habilite y recoja la salida de estos debugs

```
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 la grabación del WebEx:

https://goo.gl/QOS1iT