Configuración de SIP TLS entre CUCM-CUBE/CUBE-SBC con certificados firmados por CA

Contenido

Introducción

Este documento describe cómo configurar SIP Transport Layer Security (TLS) entre Cisco Unified Communication Manager (CUCM) y Cisco Unified Border Element (CUBE) con certificados firmados por la Autoridad de Certificación (CA).

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 instaladas las licencias de seguridad y Unified Communication K9 (UCK9).

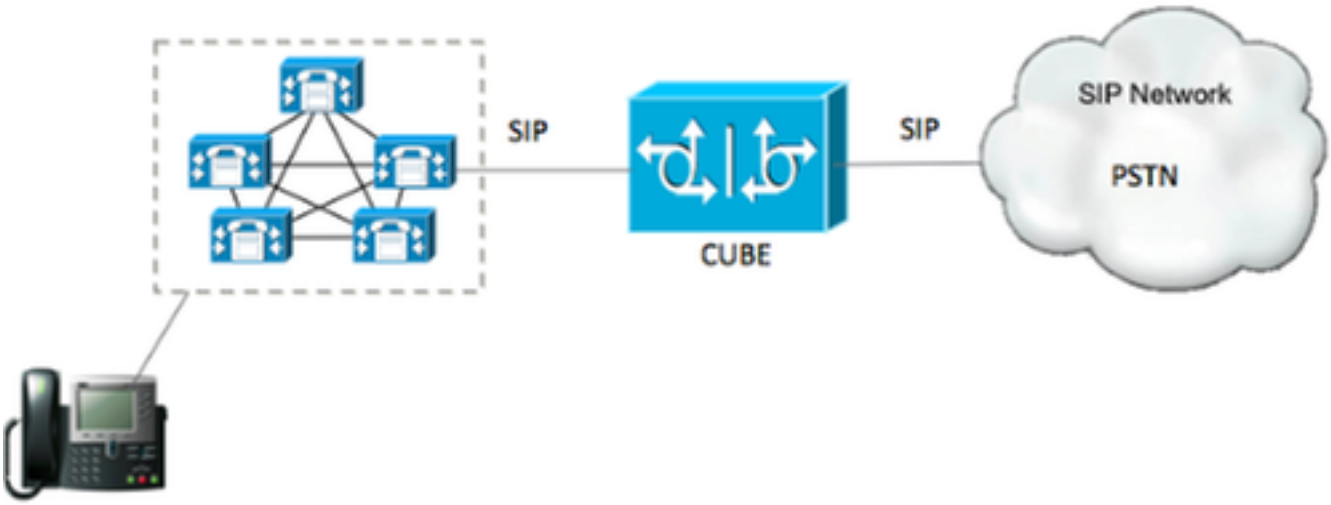
Nota: Para Cisco IOS-XE versión 16.10 en adelante, la plataforma ha pasado a las licencias inteligentes.

Componentes Utilizados

- SIP
- Certificados firmados por la autoridad certificadora
- Gateways Cisco IOS e IOS-XEVersiones 2900/3900/4300/4400/CSR1000v/ASR100X: 15,4+
- Cisco Unified Communications Manager (CUCM)Versiones: Más de 10,5

Configurar

Diagrama de la red



Configuración

Paso 1. Va a crear una clave RSA que coincida con la longitud del certificado raíz mediante el comando:

```
Crypto key generate rsa label TestRSAkey exportable modulus 2048
```

Este comando crea una clave RSA con una longitud de 2048 bits (el máximo es 4096).

Paso 2. Cree un punto de confianza para conservar nuestro certificado firmado por CA mediante comandos:

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

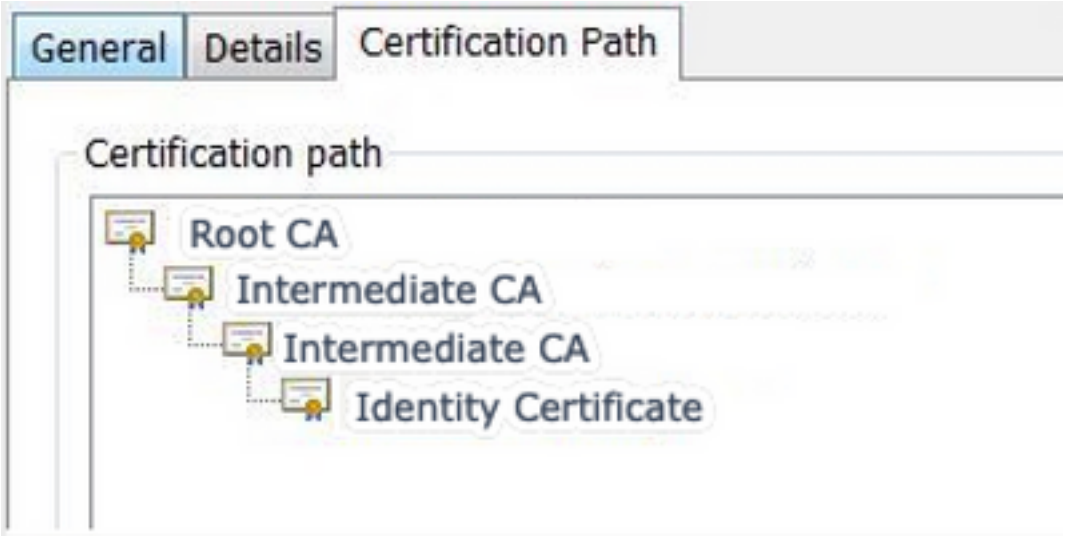
Paso 3. Ahora que cuenta con nuestro punto de confianza, generará nuestra solicitud de CSR con los siguientes comandos:

```
 Crypto pki enroll CUBE_CA_CERT
```

Responda a las preguntas en la pantalla y, a continuación, copie la solicitud CSR, guárdela en un archivo y envíela a la CA.

Paso 4. Debe averiguar si la cadena de certificados raíz tiene certificados intermedios; en caso de que no haya autoridades de certificados intermedios, pase al paso 7; de lo contrario, continúe en el paso 6.

Paso 5. Cree un punto de confianza para conservar el certificado raíz, además, cree un punto de confianza para conservar cualquier CA intermedia hasta el que firme nuestro certificado CUBE (consulte la imagen a continuación).



En este ejemplo, el nivel 1st es la CA raíz, el nivel 2nd es nuestra primera CA intermedia, el nivel 3rd es la CA que firma nuestro certificado CUBE y, por lo tanto, necesita crear un punto de confianza para mantener los primeros 2 certificados con estos comandos.

```
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
```

Paso 6. Después de recibir nuestro certificado firmado por CA, va a autenticar el punto de confianza, el punto de confianza necesita retener el certificado de CA justo antes del certificado de CUBE; el comando que permite importar el certificado es,

```
Crypto pki authenticate CUBE_CA_CERT
```

Paso 7. Una vez que tenga instalado nuestro certificado, debe ejecutar este comando para importar nuestro certificado CUBE

```
  Crypto pki import CUBE_CA_CERT cert
```

Paso 8. Configure SIP-UA para utilizar el punto de confianza que creó

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

Paso 9. Configure los pares de marcado como se muestra a continuación:

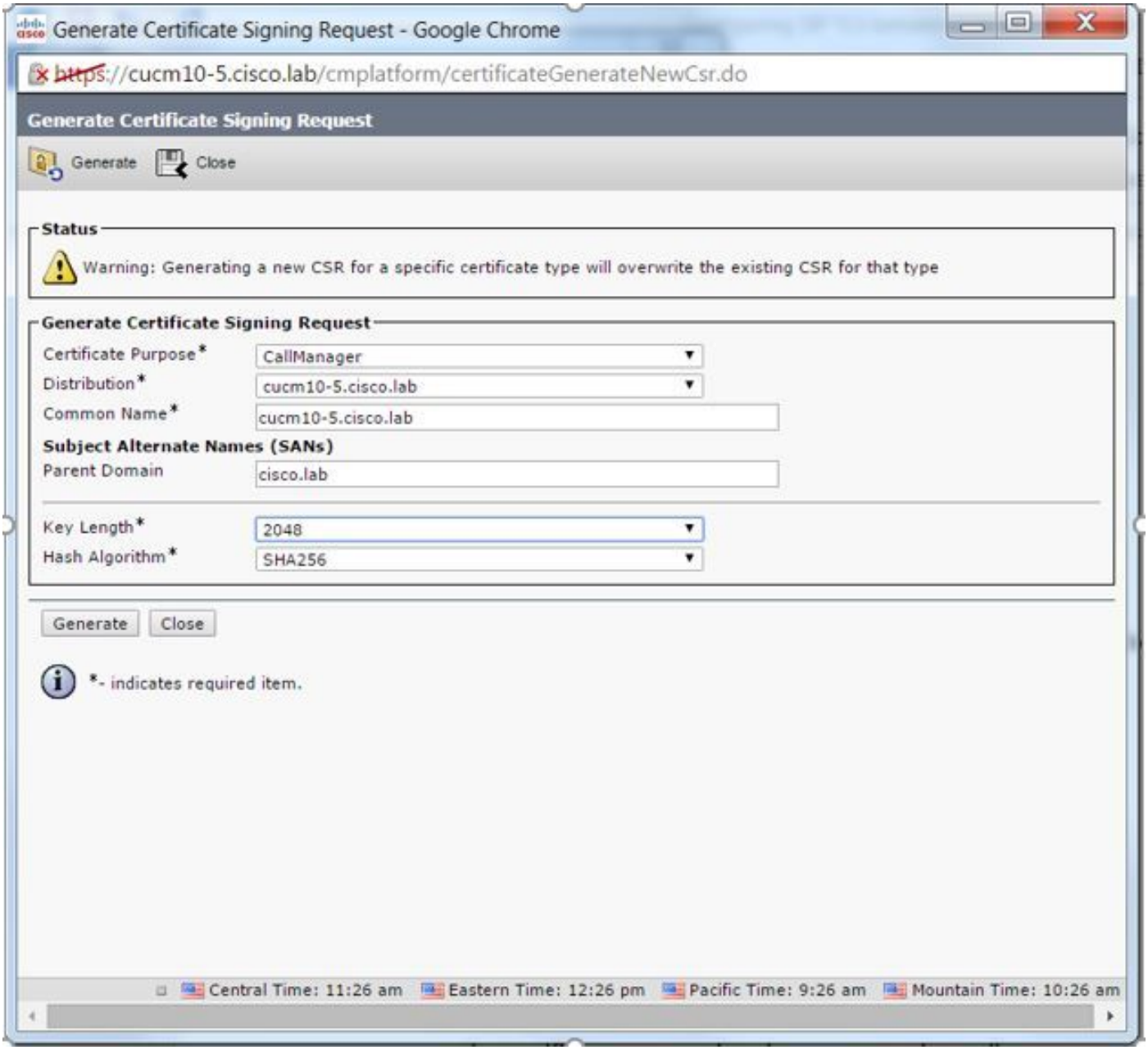
```
dial-peer voice 9999 voip
answer-address 35..
destination-pattern 9999
session protocol sipv2
session target dns:cucm10-5
session transport tcp tls
voice-class sip options-keepalive
srtp
```

Con esto, la configuración de CUBE está completa.

Paso 10. Ahora, va a generar nuestra CSR de CUCM, siga estas instrucciones

- Inicie sesión en el administrador de CUCM OS
- Haga clic en Security (Seguridad)
- Haga clic en Administración de certificados.
- Haga clic en Generar CSR

La solicitud CSR debe verse como la siguiente:



Paso 11. Descargue el CSR y envíelo a la CA.

Paso 12. Cargue la cadena de certificados firmados por CA en CUCM , los pasos son:

- Haga clic en Security (Seguridad) y luego en Certificate Management (Administración de certificados).
- Haga clic en Cargar certificado/cadena de certificado.
- En el menú desplegable de propósito del certificado, seleccione Call Manager.
- Busque el archivo.
- Haga clic en Cargar.

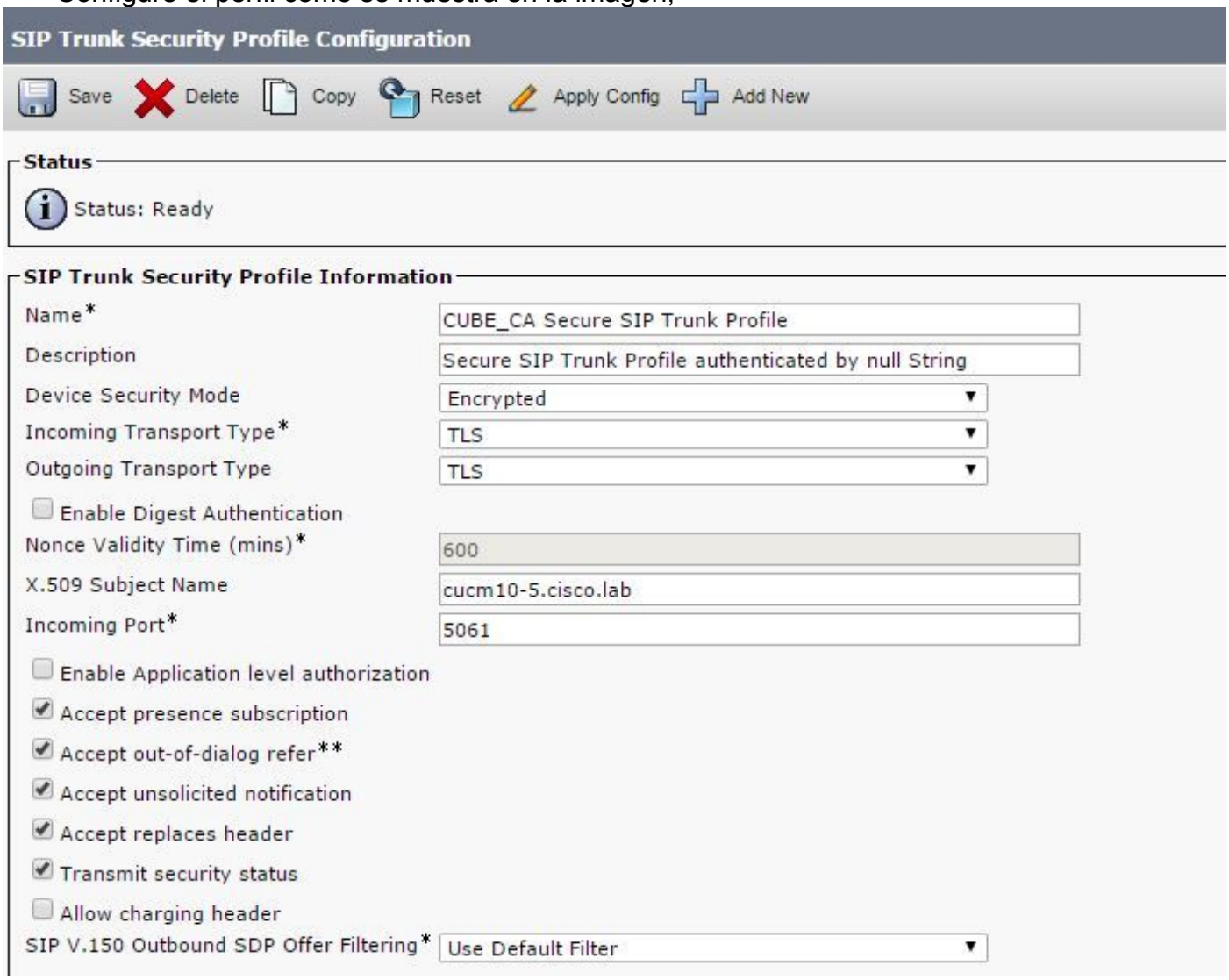
Paso 13. Inicie sesión en CUCM CLI y ejecute este comando

```
utils ctl update CTLFile
```

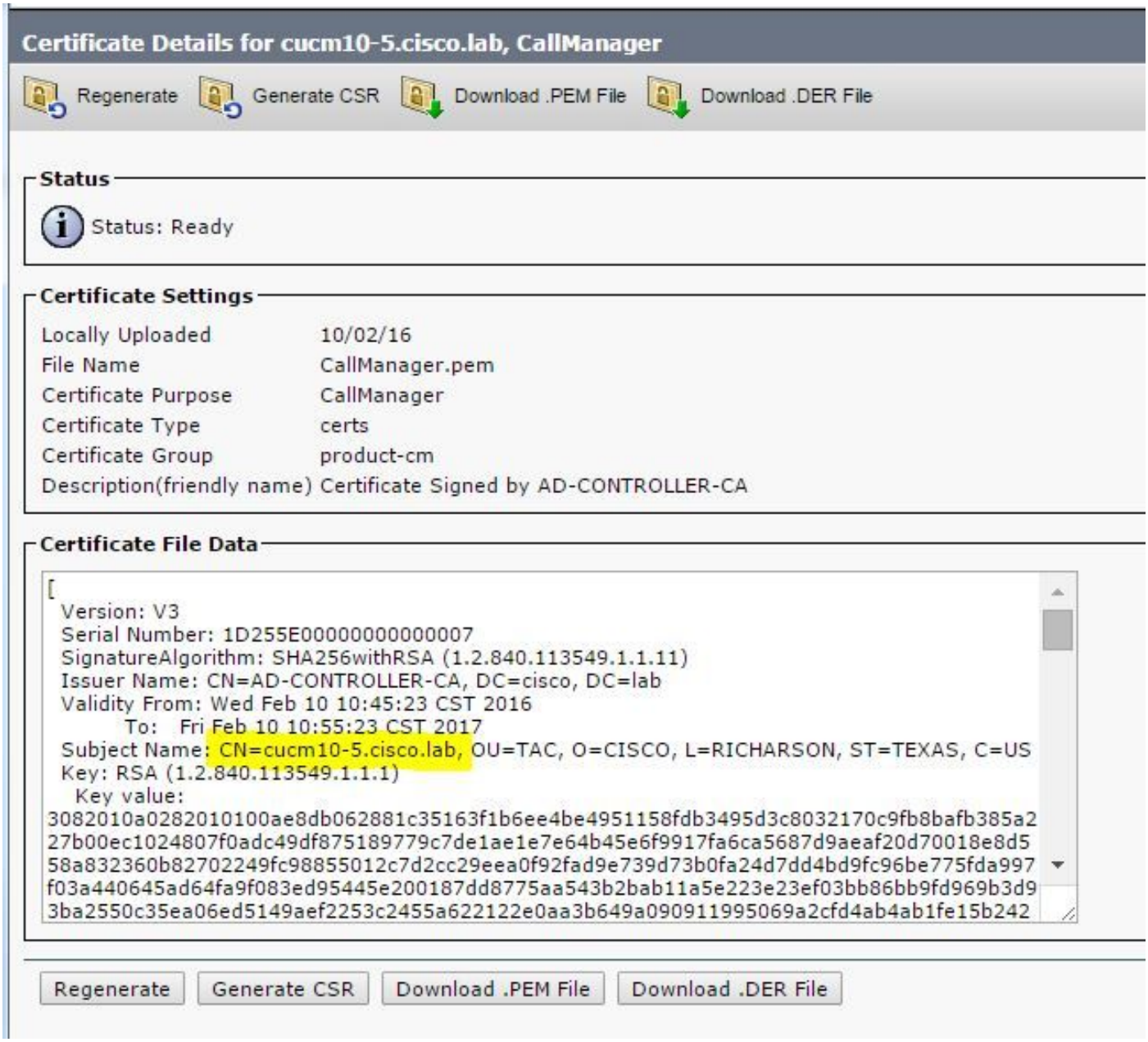
Paso 14. Configuración de un perfil de seguridad troncal SIP de CUCM

- Haga clic en el sistema y, a continuación, en la seguridad y, a continuación, seleccione el perfil de seguridad del tronco

- Configure el perfil como se muestra en la imagen,



Nota: En este caso, el nombre del asunto X.509 debe coincidir con el nombre del asunto del certificado CUCM, como se muestra en la parte resaltada de la imagen.



Paso 15. Configure un enlace troncal SIP como lo haría normalmente 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.
- En el perfil de seguridad del troncal SIP, asegúrese de seleccionar el nombre del perfil SIP creado en el paso 14.

Verificación

En este momento, si toda la configuración es correcta,

En CUCM, el estado del troncal SIP muestra Full Service , como se muestra en la imagen,

En CUBE, el par de marcado muestra este estado:

```
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
```

Este mismo proceso se aplica a otros routers, la única diferencia es que en lugar de un paso para cargar el certificado de CUCM, cargue el certificado proporcionado por terceros.

Troubleshoot

Habilitar estas depuraciones en CUBE

```
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
```