Configure SIP TLS between CUCM-CUBE/CUBE-SBC

Contents

Table Of Contents

Introduction

This document helps configure SIP Transport Layer Security (TLS) between Cisco Unified Communication Manager (CUCM) and Cisco Unified Border Element (CUBE)

Prerequisites

Cisco recommends to have knowledge of these subjects

- SIP protocol
- Security Certificates

Requirements

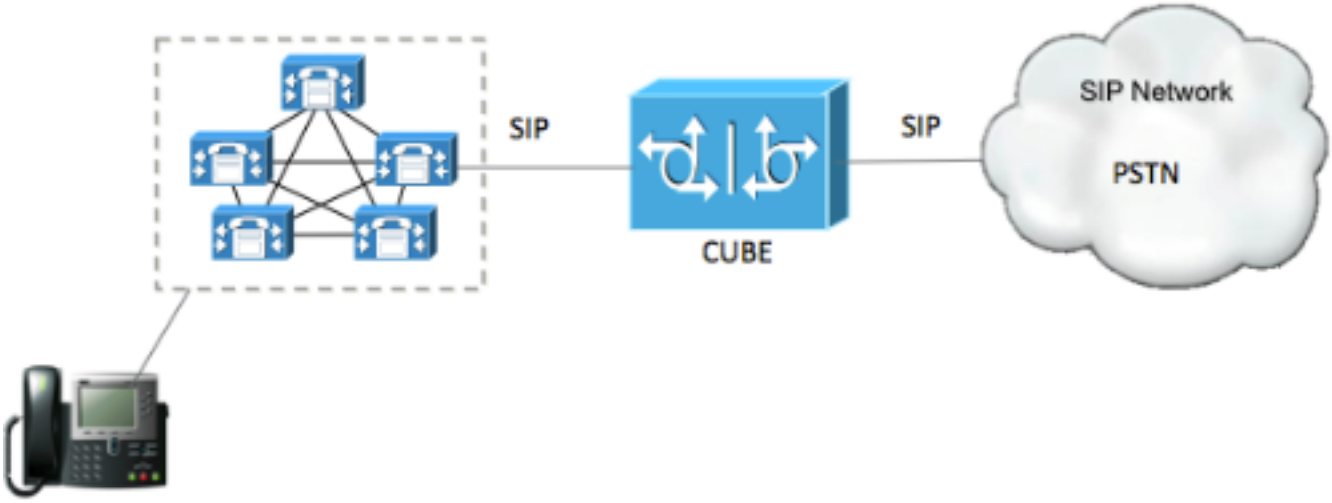
- Date and time must match on the endpoints (it is recommended to have the same NTP source).
- CUCM must be in mixed mode.
- TCP connectivity is required (Open port 5061 on any transit firewall).
- The CUBE must have the security and UCK9 licenses installed.

Components Used

- SIP
- Selfsigned certificates

Configure

Network Diagram



Configuration steps

Step 1. Create a trustpoint in order to hold CUBE's selfsigned certificate

```
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)
```

Step 2. Once the trust point is created you run the command **Crypto pki enroll CUBEtest** in order to get self-signed certerticates

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

If enrollment was correct you must expect the this output

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

Step 3. After your obtain certificate , you need to export it

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

The above command must generate the below certificate

```
% Self-signed CA certificate:
```

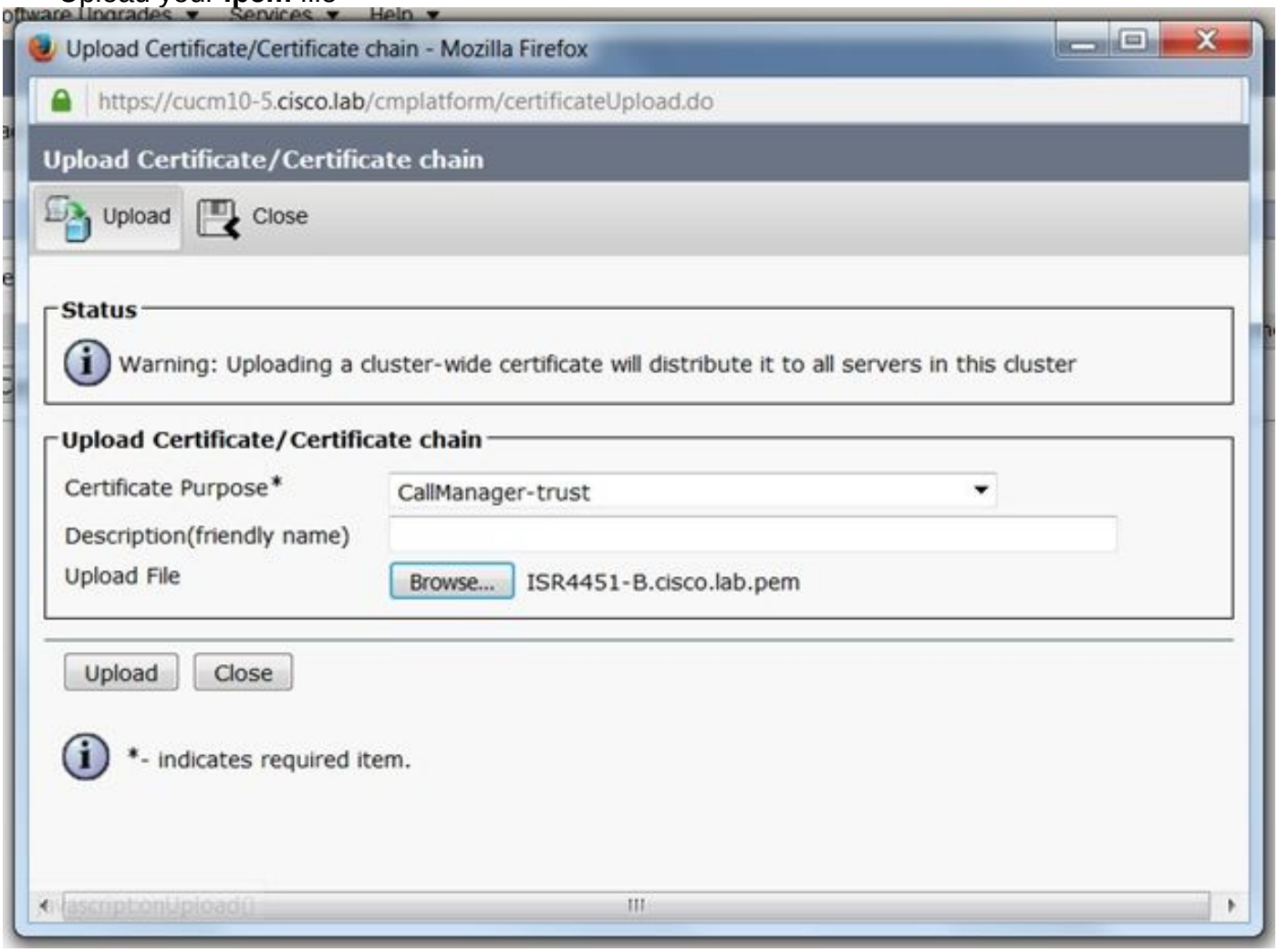
```
-----BEGIN CERTIFICATE-----
MIIBgDCCASqgAwIBAgIBATANBgkqhkiG9w0BAQUFADAeMRwwGgYDVQQDExNJU1I0
NDUxLUIuY2lzY28ubGFiMB4XDTE1MTIxNTAxNTAxNVoXDTIwMDEwMTAwMDAwMFow
HjEcMBoGA1UEAxMTSVNSNDQ1MS1CLmNpc2NvLmxhYjBcMA0GCSqGSIb3DQEBAQUA
A0sAMEgCQQDGtZ974Tfv+pngs1+cCeLZ/e0b2zq6CrIj4T1t+NSlG5sjMJ919/ix
7Fa6DG33LmEYUM1NntkLaz+8UNDAyBZrAgMBAAGjUzBRMA8GA1UdEwEB/wQFMAMB
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-----
```

Copy the above generated Self signed certificate and paste it to a text file with file extension **.pem**

Example below is named as ISR4451-B.ciscolab.pem

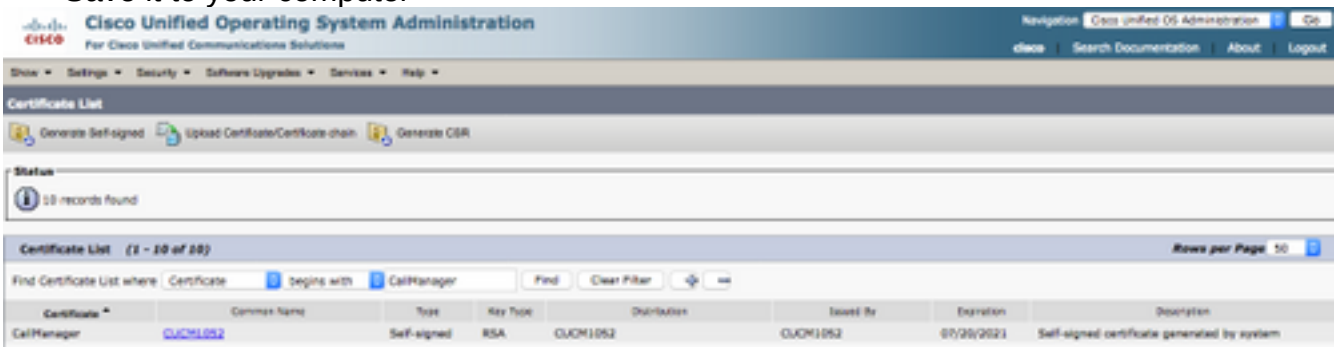
Step 4. Upload the CUBE certificate to the CUCM

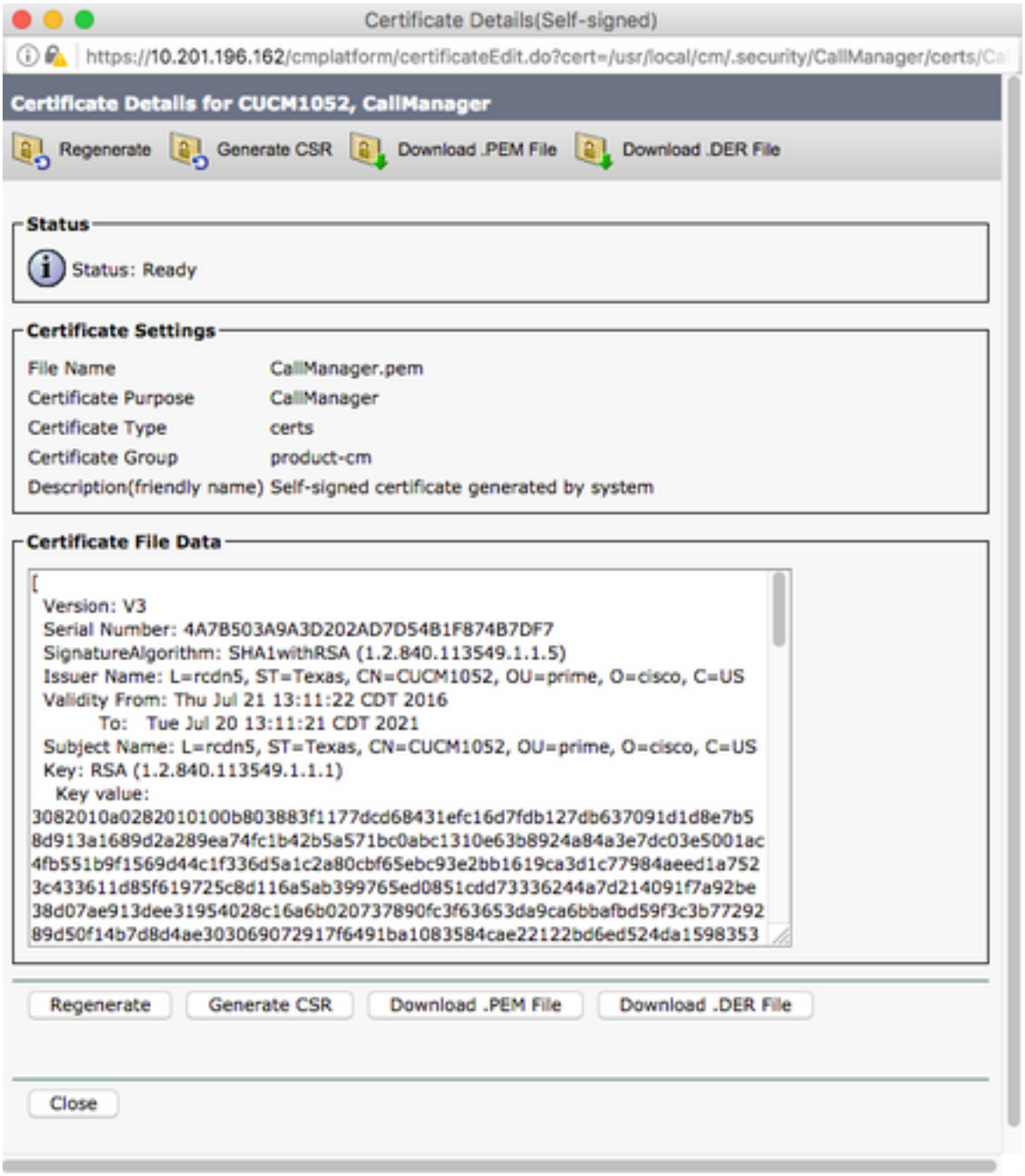
- CUCM OS Admin > Security > Certificate Management > Upload Certificate/Certificate chain
- Certificate Purpose = CallManager-Trust
- Upload your **.pem** file



Step 5. Download the Call manager self-signed certificate

- Find the certificate that says Callmanager
- Click on the host name
- Click on download PEM file
- Save it to your computer





Step 6. Upload the Callmanager.pem certificate to CUBE

- Open the Callmanager.pem with a text file editor
- Copy the whole content of the file
- Run the this commands on the 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
```

Step 7. Configure SIP to use CUBE's selfsigned Certificate trustpoint

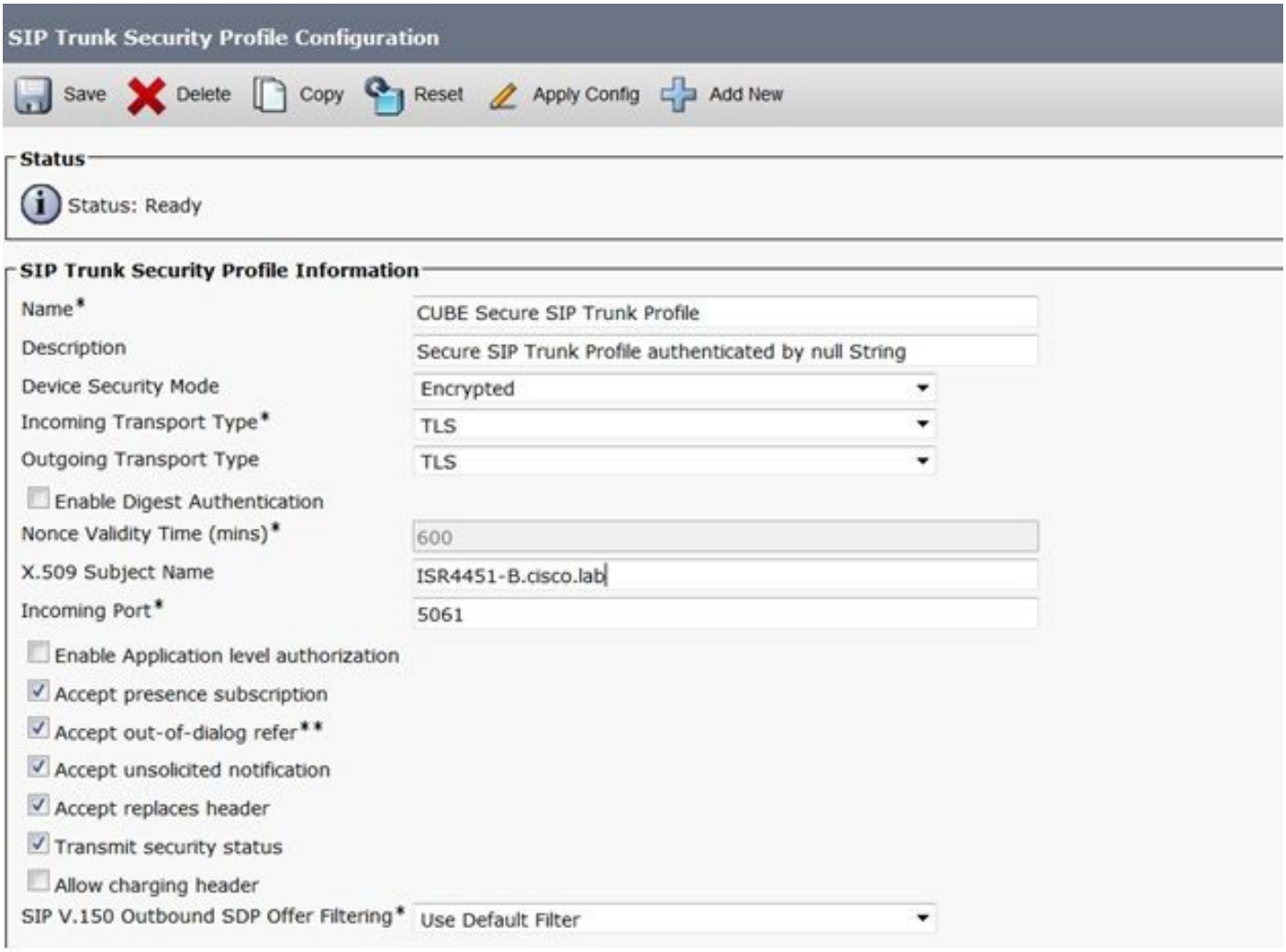
```
sip-ua

 crypto signaling default trustpoint CUBEtest
```

Step 8. Configure the dial peers with 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
```

Step 9. Configure a CUCM SIP trunk security profile

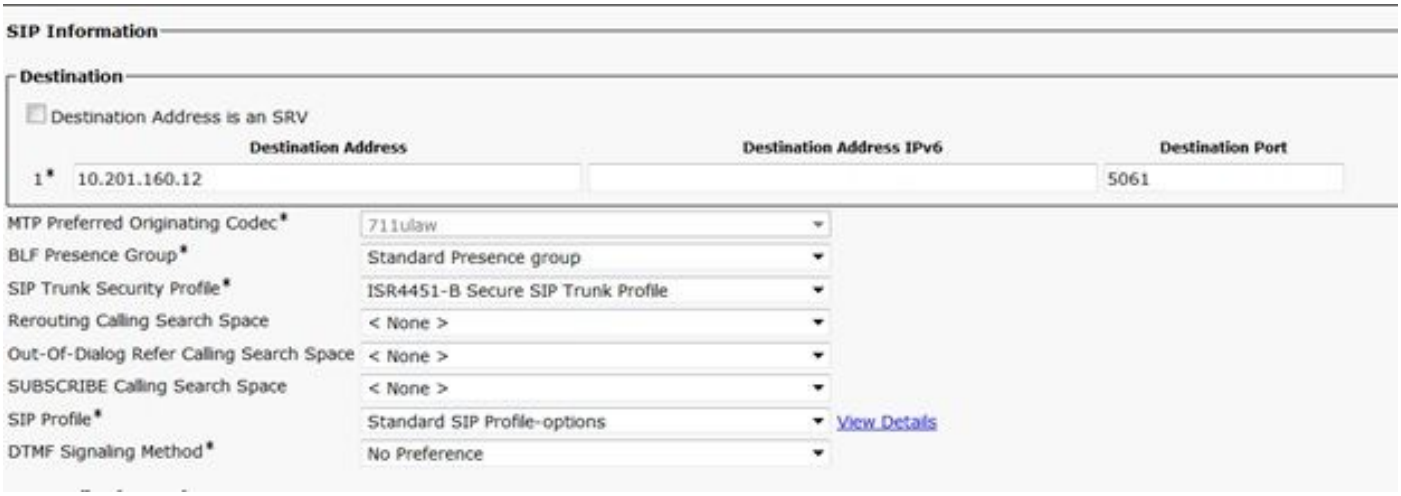
- CUCM Admin page > System > Security > SIP Trunk Security Profile
- Configure the profile as shown below



Note: It is critically important that the X.509 field matches the CN name you configured previously while you were generating the self-signed certificate

Step 10. Configure a SIP trunk on CUCM

- Ensure the SRTP allowed check box is checked
- Configure the proper destination address and Ensure to replace port 5060 with port 5061
- Ensure to select the correct Sip Trunk Security profile (which was created in Step 9)



- Save and reset the trunk.

Verify

Since you enabled OPTIONS PING on the CUCM, SIP trunk must be in FULL SERVICE state

The SIP trunk status show full service.

The dial peer status show as follow:

```
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

Enable and collect the output of these 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
```

Webex Recording link:

https://goo.gl/QOS1iT