

SIP-TELEFOONS configureren tussen CUCM-CUBE/CUBE-SBC met CA-ondertekende certificaten

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuratie](#)

[Verifiëren](#)

—

[Problemen oplossen](#)

Inleiding

Dit document beschrijft hoe u SIP Transport Layer Security (TLS) kunt configureren tussen Cisco Unified Communications Manager (CUCM) en Cisco Unified Border Element (CUBE) met door certificeringsinstanties (CA) ondertekende certificaten.

Voorwaarden

Cisco adviseert om kennis van deze onderwerpen te hebben

- SIP-protocol
- Security certificaten

Vereisten

- Datum en tijd moeten op de eindpunten overeenkomen (aanbevolen wordt om dezelfde NTP-bron te hebben).
- CUCM moet in gemengde modus worden geplaatst.
- TCP-connectiviteit is vereist (Open poort 5061 op elke transitfirewall).
- De CUBE moet de security en Unified Communications K9 (UCK9) licenties hebben geïnstalleerd.

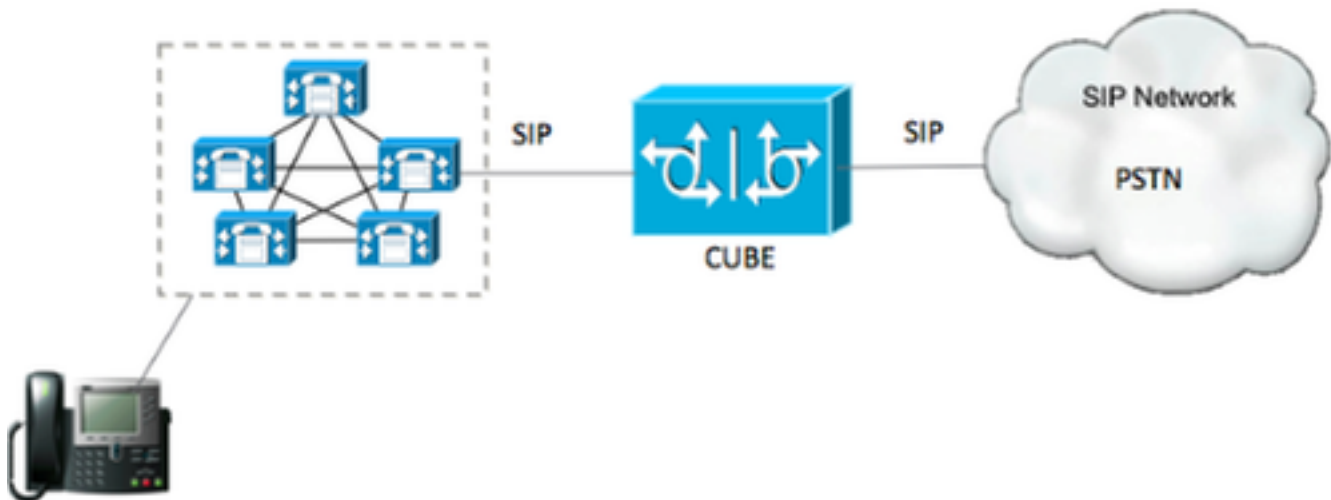
Opmerking: Voor Cisco IOS-XE versie 16.10 heeft het platform zich verplaatst naar slimme licenties.

Gebruikte componenten

- SIP
- Certificaten van certificeringsinstanties
- Cisco IOS en IOS-XE gateways 2900 / 3900 / 4300 / 4400 / CSR1000v / ASR100X versies: 15,4+
- Cisco Unified Communications Manager (CUCM) Versies: 10,5+

Configureren

Netwerkdigram



Configuratie

Stap 1. U gaat met behulp van deze opdracht een RSA-toets definiëren die overeenkomt met de certificaatlengte van het wortelcertificaat:

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

Deze opdracht maakt een RSA-toets met een lengte van 2048 bits (het maximum is 4096).

Stap 2. Maak een betrouwbaar punt om ons CA-ondertekend certificaat te houden met opdrachten:

```
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)
```

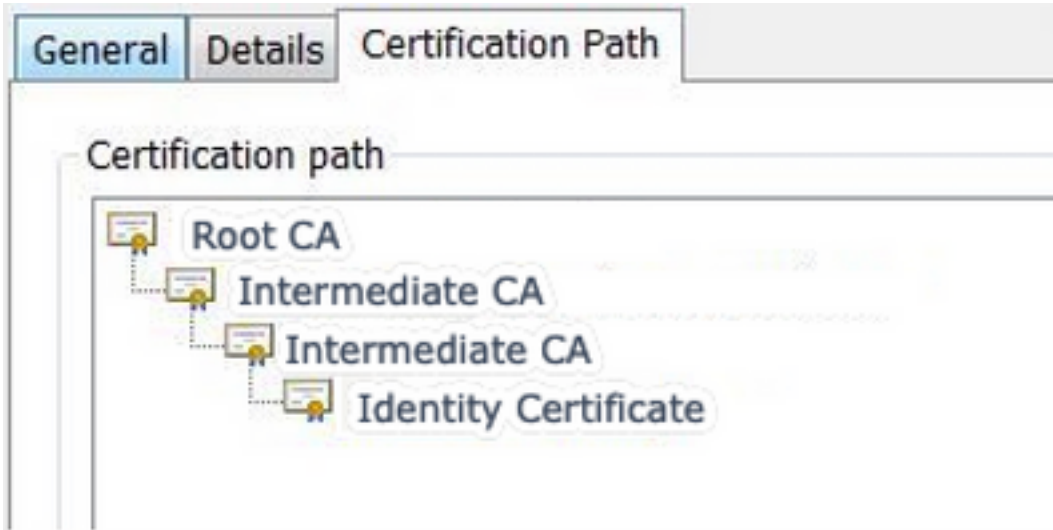
Stap 3. Nu u ons vertrouwde punt hebt, zult u ons CSR-verzoek met de onderstaande opdrachten genereren:

```
Crypto pki enroll CUBE_CA_CERT
```

Beantwoord de vragen op het scherm en kopieer vervolgens het CSR-verzoek, bewaar het in een bestand en verstuur het naar de CA.

Stap 4. U moet weten of de keten van het wortelcertificaat tussentijdse certificaten heeft; indien er geen intermediaire certificeringsinstanties zijn , stap 7 , anders , voort in stap 6 .

Stap 5. Maak een trust punt om het certificaat van de Opstarten te houden, plus, om een trust point te maken om een intermediaire CA te houden tot het punt dat ons CUBE-certificaat ondertekend heeft (zie afbeelding hieronder).



In dit voorbeeld, het 1^{ste} niveau is de Root CA, het 2^e niveau is onze eerste intermediaire CA, het 3rd niveau is de CA die ons CUBE certificaat ondertekenen, en dus moet u een betrouwbaar punt creëren om de eerste 2 certificaten met deze opdrachten te bezitten.

```
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
```

Stap 6. Nadat u ons door CA ondertekend certificaat hebt ontvangen, gaat u het vertrouwenspunt echt maken, dan moet de trustpoint het certificaat van de CA vlak voor het CUBE-certificaat in zijn bezit hebben. de opdracht die invoer van het certificaat mogelijk maakt, is:

```
Crypto pki authenticate CUBE_CA_CERT
```

Stap 7. Nadat u ons certificaat hebt geïnstalleerd, moet u deze opdracht uitvoeren om uw CUBE-certificaat te importeren

```
Crypto pki import CUBE_CA_CERT cert
```

Stap 8. Configureer de SIP-UA met het door u aangelegde betrouwbaar punt

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

Stap 9. Configureer kiestoon zoals hieronder wordt weergegeven:

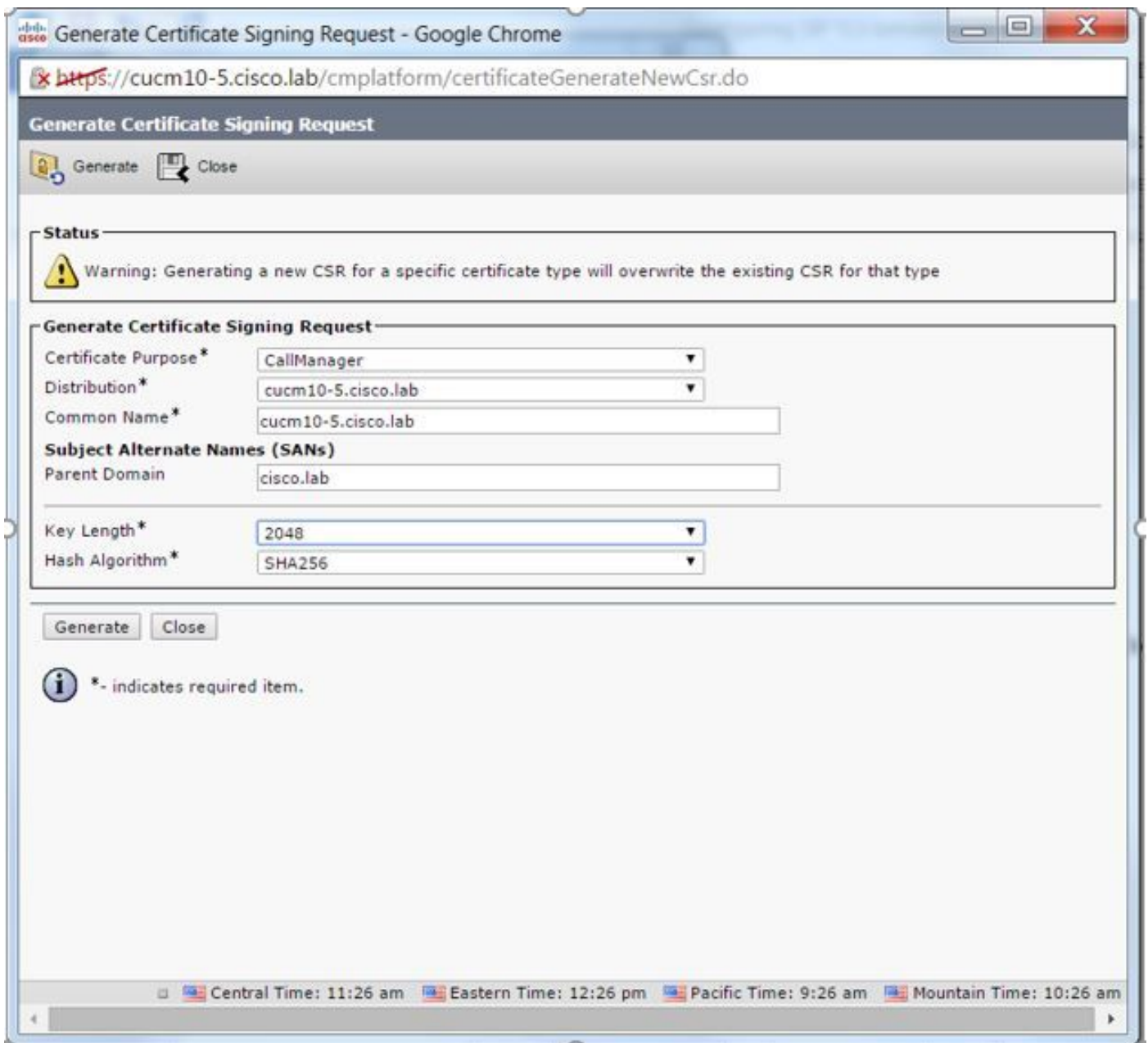
```
dial-peer voice 9999 voip
answer-address 35..
destination-pattern 9999
session protocol sipv2
session target dns:cucm10-5
session transport tcp tls
voice-class sip options-keepalive
srtp
```

Hierdoor is de CUBE-configuratie voltooid.

Stap 10. U gaat nu onze CUCM CSR genereren, volgt u de onderstaande instructies

- Inloggen op CUCM OS-beheerder
- Klik op beveiliging
- Klik op certificaatbeheer.
- Klik op om CSR te genereren

Het CSR-verzoek moet hieronder worden weergegeven:



Stap 11. Download de CSR en stuur het naar de CA.

Stap 12. Upload de door CA ondertekende certificeringsketen naar CUCM, stappen zijn:

- Klik op beveiliging en vervolgens op certificaatbeheer.
- Klik op het uploaden van certificaat/certificeringsketen.
- Selecteer in het vervolgkeuzemenu voor de certificaatfunctie de optie Call Manager.
- Bladeren naar je bestand.
- Klik op het uploaden.

Stap 13. Meld u aan bij de CUCM CLI en voer deze opdracht uit

```
utils ctl update CTLFile
```


Stap 14. Configuratie van een CUCM SIP-routerbeveiligingsprofiel

- Klik op het systeem, dan veiligheid en dan sloop het veiligheidsprofiel van de boomstam
- Het profiel configureren zoals in de afbeelding wordt getoond,

SIP Trunk Security Profile Configuration

 Save  Delete  Copy  Reset  Apply Config  Add New

Status

 Status: Ready

SIP Trunk Security Profile Information

Name*	<input type="text" value="CUBE_CA Secure SIP Trunk Profile"/>
Description	<input type="text" value="Secure SIP Trunk Profile authenticated by null String"/>
Device Security Mode	<input type="text" value="Encrypted"/>
Incoming Transport Type*	<input type="text" value="TLS"/>
Outgoing Transport Type	<input type="text" value="TLS"/>
<input type="checkbox"/> Enable Digest Authentication	
Nonce Validity Time (mins)*	<input type="text" value="600"/>
X.509 Subject Name	<input type="text" value="cucm10-5.cisco.lab"/>
Incoming Port*	<input type="text" value="5061"/>
<input type="checkbox"/> Enable Application level authorization	
<input checked="" type="checkbox"/> Accept presence subscription	
<input checked="" type="checkbox"/> Accept out-of-dialog refer**	
<input checked="" type="checkbox"/> Accept unsolicited notification	
<input checked="" type="checkbox"/> Accept replaces header	
<input checked="" type="checkbox"/> Transmit security status	
<input type="checkbox"/> Allow charging header	
SIP V.150 Outbound SDP Offer Filtering*	<input type="text" value="Use Default Filter"/>

Opmerking: in dit geval moet de X.509-onderwerpregel overeenkomen met de CUCM-onderwerpregel zoals in het gemarkeerde gedeelte van de afbeelding wordt weergegeven.

Certificate Details for cucm10-5.cisco.lab, CallManager

Regenerate
 Generate CSR
 Download .PEM File
 Download .DER File

Status

Status: Ready

Certificate Settings

Locally Uploaded: 10/02/16
 File Name: CallManager.pem
 Certificate Purpose: CallManager
 Certificate Type: certs
 Certificate Group: product-cm
 Description(friendly name): Certificate Signed by AD-CONTROLLER-CA

Certificate File Data

```

[
Version: V3
Serial Number: 1D255E0000000000000007
SignatureAlgorithm: SHA256withRSA (1.2.840.113549.1.1.11)
Issuer Name: CN=AD-CONTROLLER-CA, DC=cisco, DC=lab
Validity From: Wed Feb 10 10:45:23 CST 2016
To: Fri Feb 10 10:55:23 CST 2017
Subject Name: CN=cucm10-5.cisco.lab, OU=TAC, O=CISCO, L=RICHARSON, ST=TEXAS, C=US
Key: RSA (1.2.840.113549.1.1.1)
Key value:
3082010a0282010100ae8db062881c35163f1b6ee4be4951158fdb3495d3c8032170c9fb8bafb385a2
27b00ec1024807f0adc49df875189779c7de1ae1e7e64b45e6f9917fa6ca5687d9aeaf20d70018e8d5
58a832360b82702249fc98855012c7d2cc29eea0f92fad9e739d73b0fa24d7dd4bd9fc96be775fda997
f03a440645ad64fa9f083ed95445e200187dd8775aa543b2bab11a5e223e23ef03bb86bb9fd969b3d9
3ba2550c35ea06ed5149aef2253c2455a622122e0aa3b649a090911995069a2cfd4ab4ab1fe15b242
  
```

Stap 15. Configureer een SIP-stam zoals u normaal met CUCM zou doen

- Zorg ervoor dat het selectieknop SRTP is ingeschakeld.
- Configureer het juiste doeladres en zorg ervoor dat u poort 5060 door poort 5061 vervangt.
- Zorg ervoor dat in het SIP stam veiligheidsprofiel de SIP profielnaam die op stap 14 is gemaakt, selecteert.

SIP Information

Destination

Destination Address is an SRV

Destination Address	Destination Address IPv6	Destination Port
1* [redacted]		5061

MTP Preferred Originating Codec* 711ulaw
 BLF Presence Group* Standard Presence group
 SIP Trunk Security Profile* ISR4451-B Secure SIP Trunk Profile
 Rerouting Calling Search Space < None >
 Out-Of-Dialog Refer Calling Search Space < None >
 SUBSCRIBE Calling Search Space < None >
 SIP Profile* Standard SIP Profile-options [View Details](#)
 DTMF Signaling Method* No Preference

Verifiëren

Als alle configuratie nu goed is,

Op CUCM toont de status van de SIP-stam de volledige service, zoals in de afbeelding wordt getoond.

Name ^	Description	Calling Search Space	Device Pool	Route Pattern	Partition	Route Group	Priority	Trunk Type	SIP Trunk Status	SIP Trunk Duration
ISR4451-B			0711-Secure					SIP Trunk	Full Service	Time In Full Service: 0 day 0 hour 0 minute

Op CUBE toont de dial-peer deze status:

```
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
```

Dit zelfde proces is van toepassing op andere routers, het enige verschil is dat in plaats van stappen te ondernemen om het CUCM-certificaat te uploaden, het certificaat dat door derden is geleverd te uploaden.

Problemen oplossen

Schakel deze apparaten op CUBE in

```
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
```