

CUCCM-cube/CUBE-SBC نېب SIP TLS نېوكت CA نم ءءقووملا تاءاهشلا مادختساب

تايوتحمل

[ءمءملا](#)

[ءيساسالابلطتملا](#)

[تابلطتملا](#)

[ءمدختسملا تانوكملا](#)

[نېوكتلا](#)

[ءكبشلالل طيطلختلا مسرلا](#)

[نېوكتلا](#)

[ءحصلال نم ققحتلا](#)

[ءءالصل او ءاطءال فاشكسا](#)

ءمءملا

ءءوملا تالاصتالا ريم نېب (TLS) لقلنلا ءقبط نام نېوكت ءي فيك دنننسملا اءه فصي
ءءرم نم ءءقووملا تاءاهشلا مادختساب Cisco نم (CUBE) ءءوملا ءءل رصنعو Cisco نم (CUCCM)
(CA) قيءصتلا.

ءيساسالابلطتملا

تاعوضوملا هءب ءءرملااب Cisco يءصوت

- SIP لوكوورب
- نامال تاءاهش

تابلطتملا

- رءصم سفن كيءل نوكي ناب يءصوي) ءي ءهاللا طاقن عم تقول او ءي راتلا قباطتي ناب ءءي (NTP).
- طلءءملا ءءولاي في CUCCM نوكي ناب ءءي.
- (تيءنارلل ءي ءءم راءءي أءل 5061 ءوتءملا ءءنملا) بولطم TCP لاصتا.
- K9 (UCK9) ءءوملا لاصتالا او نامال صيءارت ءل بعءملا يءءءي ناب ءءي.

ءل يءساسال ماعنللا لقلنا، 16.10 راءءال Cisco IOS-XE ءءنربل ءبسنلاب: ءءءالم
ءي ءءل صيءءرلا.

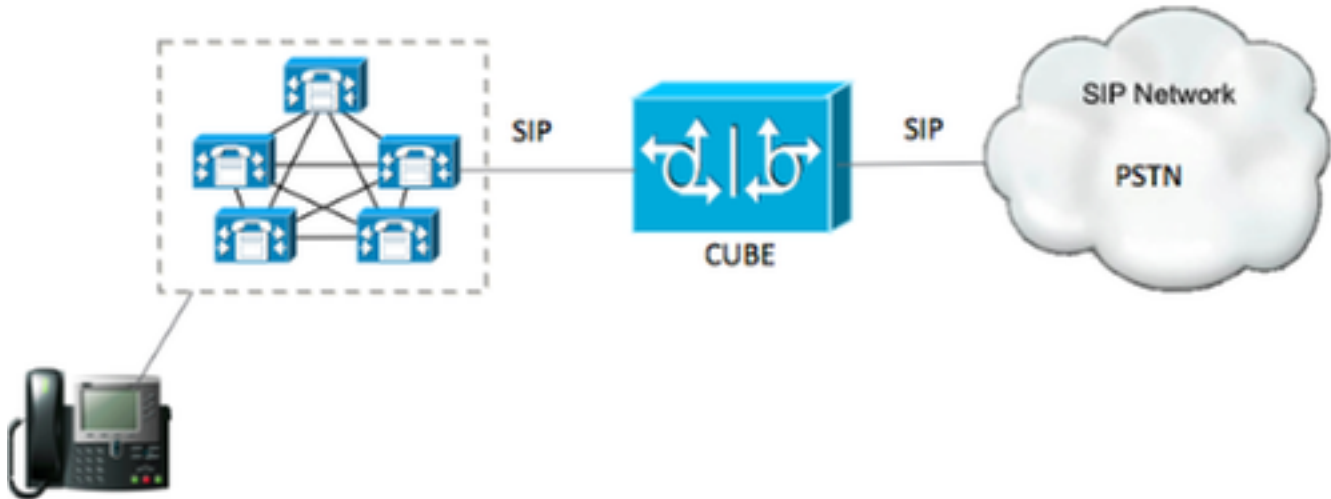
ءمدختسملا تانوكملا

- SIP
- تاءاهشلا ءيءهل ءءقووملا تاءاهشلا

- Cisco IOS و IOS-XE اإلارادص 2900 / 3900 / 4300 / 4400 / CSR1000v / ASR100X: 15.4+
- Cisco Unified Communications Manager (CUCM) اإلارادص 10.5+ جم انرب

نېوكتال

ةكبشلل يطيختال مسرلا



نېوكتال

مادختساب رذجال ةداهشلل ةداهشلل لوط قباطي RSA حاتفم عاشن اىل ا بهاذ تنأ 1. ةوطخال رمال:

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

(4096 وه ىصقألا دل) تب 2048 لوطب RSA حاتفم عاشن اىل رمال اذه موقى

رمأوال مادختساب CA لبق نم ةعقوملا انتداهشب ظافتحالل ةقث ةطقن عاشن اىل 2. ةوطخال:

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

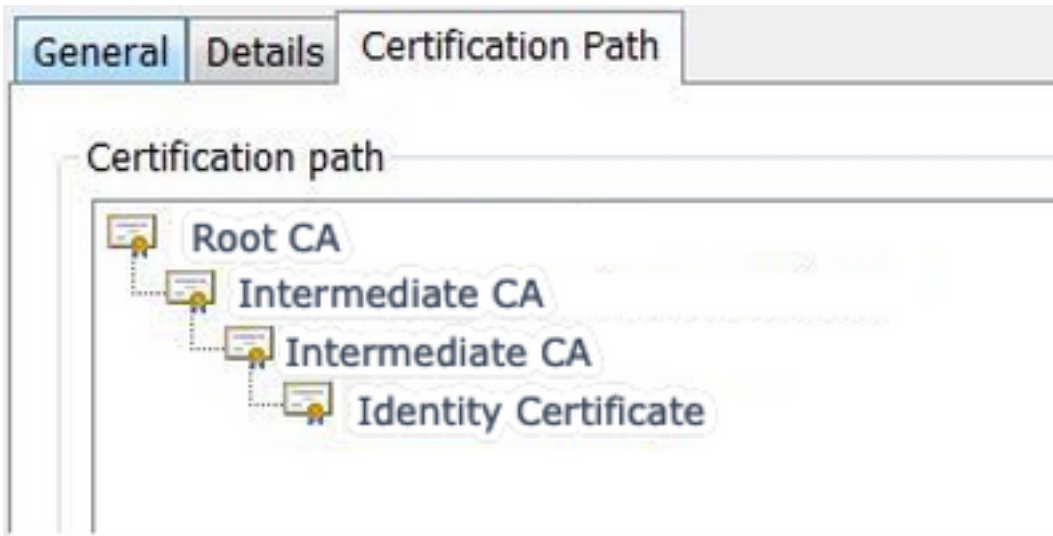
CSR بلط عاشن اىل موقتس ، انب ةصاخال ةقثال ةطقن كىدل حبصأ نأ دعب نألا 3. ةوطخال ةىلال رمالال مادختساب انب صاخال:

```
Crypto pki enroll CUBE_CA_CERT
```

CA. اىل هل سرأ مث فلم يف هظفحاو ، CSR بلط خسنا مث ، ةشاشلا اىل ةلئسألا اىل بجا

، ةطيسو تاداهش اىل ةوتحت رذجال تاداهشلا ةلسلس تناك اذا ام فرعت نأ جاتحت 4. ةوطخال 6. ةوطخال يف رمتسا ، اىل ، 7 ةوطخال اىل لقتنا ، ةطيسو ةداهش عجارم دوجو مدع ةلاح يف

عاشنإب مق ،كلذىلى إفاضاإلاب ،رذجالا ةداهشب طاافتحالل ةقث ةطقن عاشنإب مق .5 ةوطخال
عجار) انب ةصاخلا بعكمالا ةداهش عقوي ىتح طسوتم قدصم عجرم ياب طاافتحالل ةقث ةطقن
(هاندا ةروصلا).



طيسولا قدصملا عجرملا وه يثالثا يوتسملاو ،ca رذجالا وه لوالا يوتسملا ،لاثملا اذه يف
،انب ةصاخلا بعكمالا ةداهش عيقوتب موقى يذلا قدصملا عجرملا وه ثالثا يوتسملاو ،لوالا
رماولا هذه عم لوالا ةيثلثا تاداهشلاب طاافتحالل TrustPoint عاشنإلى جاتحت ،يثلثلابو

```
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
```

جاتحت ،TrustPoint ةقداصمب موقتس ،CA لبق نم ةعقوملا انتداهش مالتسإ دعب .6 ةوطخال
حمسي يذلا رمألا ،CUBE ةداهش لبق ةرشابم قدصملا عجرملا ةداهش لمح لىلى TrustPoint
،وه ةداهشلا داري تساب

```
Crypto pki authenticate CUBE_CA_CERT
```

بعكمالا ةداهش داري تسال رمألا اذه ليغش تل جاتحت ،انتداهش تيبتت درجمب .7 ةوطخال
انب ةصاخلا

```
Crypto pki import CUBE_CA_CERT cert
```

هئاشنإب تمق يذلا TrustPoint مادختسال SIP-UA نيوكتب مق .8 ةوطخال

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

هاندأ حضوم وه امك بلطال نارقأ نيوكت 9. ةوطخل

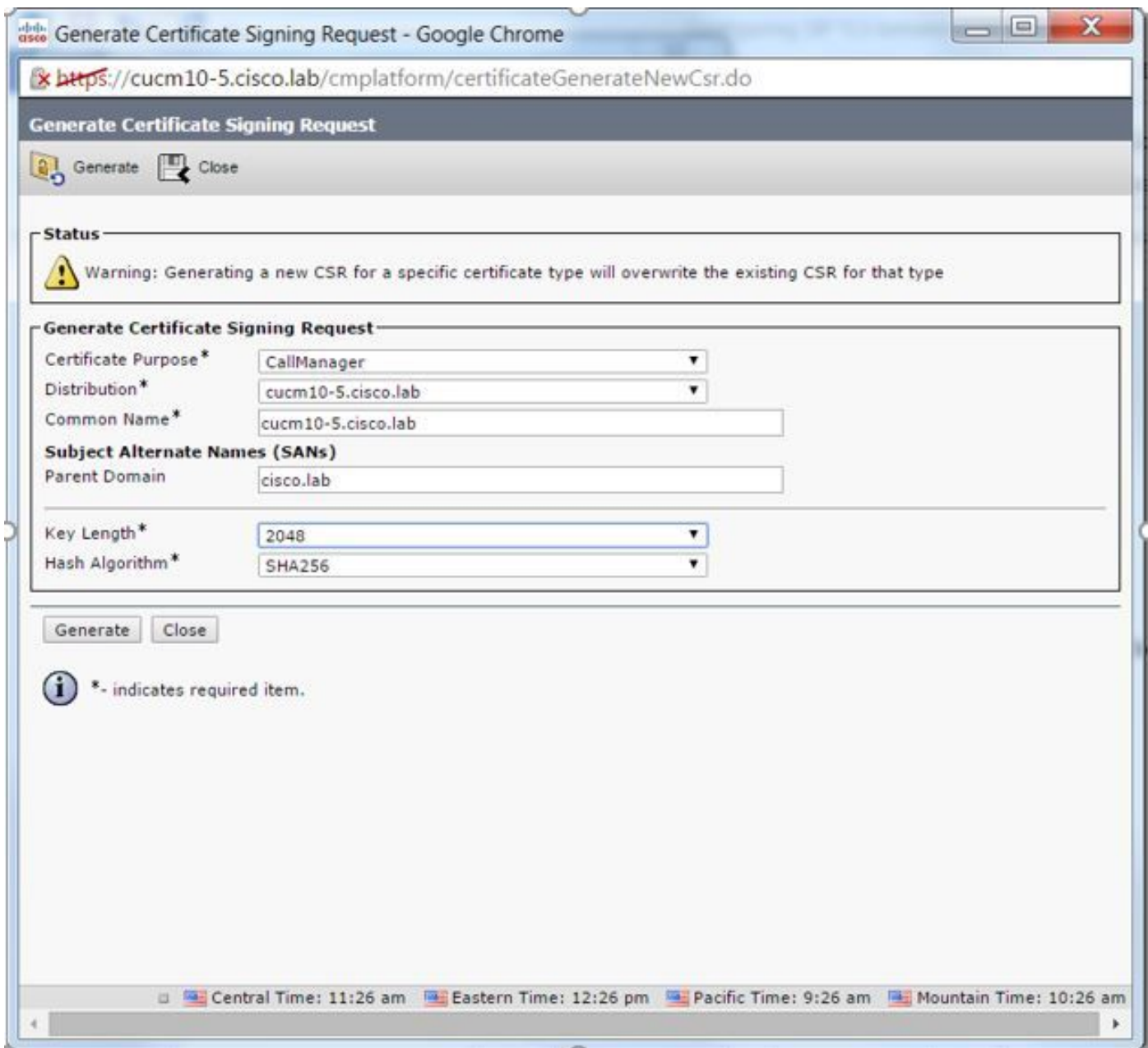
```
dial-peer voice 9999 voip
answer-address 35..
destination-pattern 9999
session protocol sipv2
session target dns:cucm10-5
session transport tcp tls
voice-class sip options-keepalive
srtp
```

المتكم بعكمال نيوكت نوكي، اذهبو

هاندأ تاميلعتل عبتا، انب صاخل CUCM CSR عاشنإب موقت فوس، نآال 10. ةوطخل

- CUCM OS لوؤسم ىلإ لوخدلا ليحست
- نيماأتل ىل ع رقنا
- تاداهشلا ةرادإ ىل ع رقنا
- CSR عاشنإ قوف رقنا

هاندأ بولطمال وه تاكرشلل ةيعامتجالا ةيلوؤسمال بلط نوكي نأ بجي



CA. إلى هلا س راو CSR لي زنتب مق 11. ةوطخل

يه تاوطلخا، CUCM إلى CA نم ةع قوملا تاداهشلا ةلسلس ليحت 12. ةوطخل

- تاداهشلا ةرادا مئ ني مأللا إلى ع رقنا
- ليحتلا تاداهش/تاداهش ةلسلس إلى ع رقنا
- تامالكمل ري دم دح، ةداهشلا ضرغل ةلدسنملا ةمئاقلا يف
- ك فلم إلى لوصولل ضارعتسالا
- ليحت قوف رقنا

رمألا اذه لغشو CUCM رمأا رطس ةهجاو إلى لوخدلا لچس 13. ةوطخل

```
utils ctl update CTLFile
```


CUCM لاصتا طخ نامأ فيرعت فلم نيوكت 14. ةوطخل

- لاصتالا طخ نامأ فيرعت فلم دح مئ ني مأللا مئ، ماظنلا إلى ع رقنا
- ةروصللا يف حضورم وه امك في صوتلا نيوكت مق

SIP Trunk Security Profile Configuration

Save Delete Copy Reset Apply Config Add New

Status

 Status: Ready

SIP Trunk Security Profile Information


Name*	CUBE_CA Secure SIP Trunk Profile
Description	Secure SIP Trunk Profile authenticated by null String
Device Security Mode	Encrypted ▼
Incoming Transport Type*	TLS ▼
Outgoing Transport Type	TLS ▼
<input type="checkbox"/> Enable Digest Authentication	
Nonce Validity Time (mins)*	600
X.509 Subject Name	cucm10-5.cisco.lab
Incoming Port*	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*	Use Default Filter ▼

CUCM ةداهش عوضوم مسا X.509 عوضوم مسا قباطي نأ بجي ،ةلاحلا هذه يف :ةظحالم ةروصلا نم زربملا عزجلا يف حضوم وه امك .

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

 Regenerate  Generate CSR  Download .PEM File  Download .DER File

Status

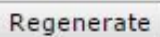
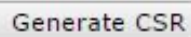
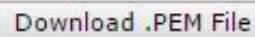
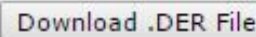
 Status: Ready

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
]
```

CUCM يلى عداة لعفت امك SIP لاصتا طخ نيوكت 15. ةوطخل

- اهب حومس الم SRTP رايتخاله ةناخ دي دجت نم دكأت.
 - 5061 ءانيم عم 5060 ءانيم لدبت سي نأ تنمضو ناو نع ةياغ بس انملا تل كش.
 - مت يذال SIP فيرعت فلم مسا دي دجت نم دكأت، SIP لاصتا طخ نامأ فيرعت فلم يف.
14. ةوطخل يف هؤاشن

SIP Information

Destination

Destination Address is an SRV

Destination Address

Destination Address IPv6

Destination Port

1*

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

ةحصلا نم ققحتلا

ةحصلا نم ققحتلا تاي لمع عيمج تناك اذا ، تقولا اذه في

ةروصلا في حضورم وه امك ، ةلماكل ةمدخل CUCM على SIP لاصتا طخ ةلاح رهظت

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

ةلاحلا هذه بلطلال ريظن يدبي CUBE على

```
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
لبيمحت ةوطخ نم ال دب هنا وه ديحولال قرفلا ، رخالال تاهجوملا على اهسفن ةيلعملال هذه قبطنت
ثلاث فرط نم ةمدقولال ةداهشلا لبيمحت ب مق ، CUCM ةداهش
```

اهحالص او ءاطخالال فاشكتسا

بعكملا على اذه ءاطخالال حيحصت نيكمت

```
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
```


ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسمل اذ ه Cisco ت مچرت
ملاعلاء ن أ عي مچ ي ف ن ي م دخت سمل ل معد ي و تح م مي دقت ل ة ي رش ب ل و
امك ة ق ي قد ن و ك ت ن ل ة ي ل أ ة مچرت ل ض ف أ ن أ ة ظ حال م ي ج ر ي . ة ص ا خ ل م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (رف و ت م ط بار ل ا) ي ل ص أ ل ا ي ز ي ل ج ن ا ل ا دن تسمل ا