

使用CA簽名證書在CUCM-CUBE/CUBE-SBC之間配置SIP TLS

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[網路圖表](#)

[組態](#)

[驗證](#)

[疑難排解](#)

簡介

本文檔介紹如何使用證書頒發機構(CA)簽名的證書在思科統一通訊管理器(CUCM)和思科統一邊界元素(CUBE)之間配置SIP傳輸層安全(TLS)。

必要條件

思科建議瞭解以下主題

- SIP通訊協定
- 安全憑證

需求

- 端點的日期和時間必須匹配 (建議使用相同的NTP源) 。
- CUCM必須處於混合模式。
- 需要TCP連線 (任何傳輸防火牆上的開放埠5061) 。
- CUBE必須安裝安全和統一通訊K9(UCK9)許可證。

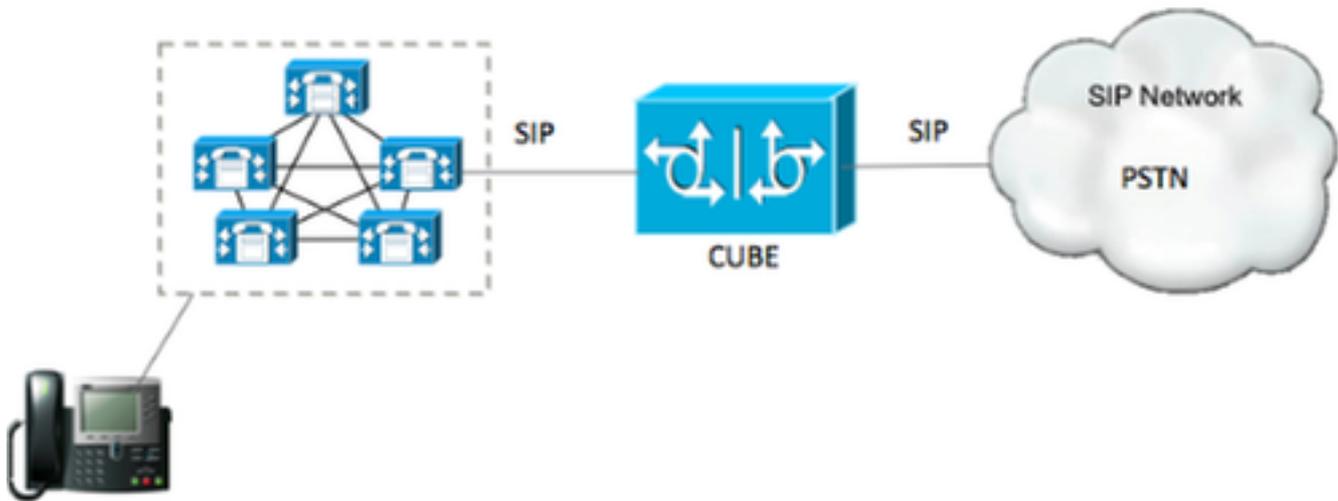
附註：對於Cisco IOS-XE版本16.10，平台已移至智慧許可。

採用元件

- SIP
- 證書頒發機構簽名的證書
- Cisco IOS和IOS-XE網關2900 / 3900 / 4300 / 4400 / CSR1000v / ASR100X版本：15.4+
- 思科整合通訊管理員(CUCM)版本：10.5+

設定

網路圖表



組態

步驟1. 您將使用命令建立與根證書的證書長度匹配的RSA金鑰：

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

此命令建立長度為2048位 (最大為4096) 的RSA金鑰。

步驟2. 使用命令建立信任點以儲存CA簽名的證書：

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

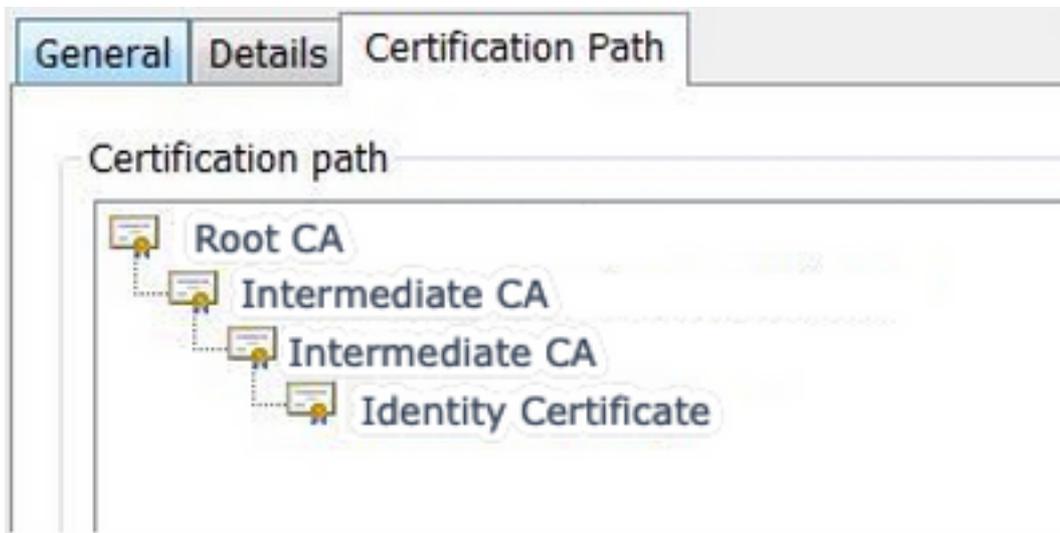
步驟3. 現在您已擁有我們的信任點，您將使用以下命令生成我們的CSR請求：

```
Crypto pki enroll CUBE_CA_CERT
```

回答螢幕上的問題，然後複製CSR請求，將其儲存到檔案，然後傳送給CA。

步驟4. 您需要瞭解根憑證鏈結是否有任何中間憑證；如果沒有中間證書頒發機構，跳轉到步驟7，否則繼續步驟6。

步驟5. 建立信任點以儲存根證書，另外建立信任點以儲存任何中間CA，直到對CUBE證書進行簽名的CA (請參閱下圖)。



在本例中，第1級是根CA，第2級是第一個中間CA，第3級是簽署CUBE證書的CA，因此，您需要建立一個信任點以使用這些命令持有前2個證書。

```
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
```

步驟6. 收到我們的CA簽名證書後，您將驗證信任點，信任點需要持有CA的證書在CUBE證書之前；允許匯入憑證的命令為，

```
Crypto pki authenticate CUBE_CA_CERT
```

步驟7. 安裝我們的證書後，需要運行此命令才能匯入我們的CUBE證書

```
Crypto pki import CUBE_CA_CERT cert
```

步驟8. 配置SIP-UA以使用您建立的信任點

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

步驟9. 配置撥號對等體，如下所示：

```
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
```

這樣，CUBE配置就完成了。

步驟10。現在，您將生成我們的CUCM CSR，請按照以下說明操作

- 登入到CUCM作業系統管理員
- 點選安全
- 按一下證書管理。
- 按一下產生CSR

CSR要求需如下圖所示：

Generate Certificate Signing Request - Google Chrome

https://cucm10-5.cisco.lab/cmplatform/certificateGenerateNewCsr.do

Generate Certificate Signing Request

Generate Close

Status

Warning: Generating a new CSR for a specific certificate type will overwrite the existing CSR for that type

Generate Certificate Signing Request

Certificate Purpose* CallManager

Distribution* cucm10-5.cisco.lab

Common Name* cucm10-5.cisco.lab

Subject Alternate Names (SANs)

Parent Domain cisco.lab

Key Length* 2048

Hash Algorithm* SHA256

Generate Close

*- indicates required item.

Central Time: 11:26 am Eastern Time: 12:26 pm Pacific Time: 9:26 am Mountain Time: 10:26 am

步驟11.下載CSR並將其傳送到CA。

步驟12.將CA簽名的證書鏈上傳到CUCM，步驟如下：

- 依次按一下「security (安全)」和「certificate management (證書管理)」。
- 按一下「upload certificate/certificate chain」。

- 在證書用途下拉選單中，選擇call manager。
- 瀏覽到您的檔案。
- 點選上傳。

步驟13.登入到CUCM CLI並運行此命令

```
utils ctl update CTLFile
```

步驟14.配置CUCM SIP中繼安全配置檔案

- 依次按一下system、security和sip trunk security profile
- 設定設定檔，如下圖所示，

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"/>

注意：在這種情況下，X.509使用者名稱必須與CUCM證書使用者名稱相匹配，如影象的突出顯示部分所示。

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
]
```

步驟15.像通常在CUCM上那樣配置SIP中繼

- 確保選中SRTP Allowed覈取方塊。
- 配置正確的目的地址，並確保用埠5061替換埠5060。
- 在SIP中繼安全配置檔案中，確保選擇在步驟14中建立的SIP配置檔名稱。

SIP Information

Destination

Destination Address is an SRV

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

MTP Preferred Originating Codec*

BLF Presence Group*

SIP Trunk Security Profile*

Rerouting Calling Search Space

Out-Of-Dialog Refer Calling Search Space

SUBSCRIBE Calling Search Space

SIP Profile* [View Details](#)

DTMF Signaling Method*

驗證

此時，如果所有配置都正常，

在CUCM上，SIP中繼狀態顯示完全服務（如圖所示）

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

在CUBE上，撥號對等體顯示以下狀態：

```
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
```

此流程同樣適用於其他路由器，唯一的區別在於上傳第三方提供的證書而不是上傳CUCM證書的步驟。

疑難排解

在CUBE上啟用這些調試

```
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
```