

在CUCM 15上配置安全臨時會議

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

簡介

本文檔介紹在CUCM 15上配置安全Ad Hoc會議。

必要條件

需求

思科建議您瞭解以下主題：

- CUCM
- VG (語音閘道)
- 安全性概念

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- CUCM (混合模式) 版本：15.0.0.98100-196
- CISCO2921版本：15.7(3)M4b (用作CA和安全會議網橋)
- NTP伺服器
- 3 8865NR IP電話

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

任務1.配置安全會議網橋並註冊到CUCM。

步驟 1.配置Public Key Infrastructure伺服器和信任點。

步驟 1.1.配置NTP伺服器和HTTP伺服器。

```
VG-CME-1(config)#ntp server x.x.x.x (IP address of the NTP server)
VG-CME-1(config)#ip http server
```

步驟 1.2. 配置Public Key Infrastructure伺服器。

```
VG-CME-1(config)#crypto pki server testCA
VG-CME-1(cs-server)#database level complete
VG-CME-1(cs-server)#database url nvram:
VG-CME-1(cs-server)#grant auto
VG-CME-1(cs-server)#lifetime certificate 1800
```

步驟 1.3.為testCA配置信任點。

```
VG-CME-1(config)#crypto pki trustpoint testCA
VG-CME-1(ca-trustpoint)#enrollment url http://x.x.x.x:80 (IP Address of testCA)
VG-CME-1(ca-trustpoint)#revocation-check none
VG-CME-1(ca-trustpoint)#rsakeypair testCA
```

步驟 1.4.等待約30秒，然後發出命令no shutdown以啟用testCA伺服器。

```
VG-CME-1(config)#crypto pki server testCA
VG-CME-1(cs-server)#no shutdown
%Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key
% or type Return to exit
Password:

Re-enter password:
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 2 seconds)

% Certificate Server enabled.
```

步驟 2.為安全會議網橋配置信任點並將其註冊到testCA。

步驟 2.1. 為安全會議網橋配置信任點，並將其命名為SecureCFB。

```
VG-CME-1(config)#crypto pki trustpoint SecureCFB
VG-CME-1(ca-trustpoint)#enrollment url http://x.x.x.x:80 (IP Address of testCA)
VG-CME-1(ca-trustpoint)#serial-number none
VG-CME-1(ca-trustpoint)#fqdn none
VG-CME-1(ca-trustpoint)#ip-address none
VG-CME-1(ca-trustpoint)#subject-name cn=SecureCFB
VG-CME-1(ca-trustpoint)#revocation-check none
VG-CME-1(ca-trustpoint)#rsakeypair SecureCFB
```

步驟 2.2. 驗證SecureCFB並鍵入「yes」以接受證書。

```
VG-CME-1(config)#crypto pki authenticate SecureCFB
Certificate has the following attributes:
  Fingerprint MD5: 383BA13D C37D0E5D 9E9086E4 8C8D1E75
  Fingerprint SHA1: 6DB8F323 14BBFBFF C36C224B B3404513 2FDD97C5

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
```

步驟 2.3. 註冊SecureCFB並設定密碼。

```
VG-CME-1(config)#crypto pki enroll SecureCFB
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
password to the CA Administrator in order to revoke your certificate.
For security reasons your password will not be saved in the configuration.
Please make a note of it.

Password:
Re-enter password:

% The subject name in the certificate will include: cn=SecureCFB
% The fully-qualified domain name will not be included in the certificate
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose SecureCFB' command will show the fingerprint.
```

步驟 3. 在安全關聯網橋上配置CUCM的信任點。

步驟 3.1. 從CUCM下載CallManager證書並複製pem檔案(思科統一作業系統管理>安全>證書管理)。

The screenshot shows the Cisco Unified Operating System Administration interface. The main window displays a list of certificates under the heading "Certificate List (1 - 42 of 42)". The first certificate, "CallManager", is highlighted with a red box. Its details are shown in a pop-up window titled "Certificate Details for CUCMPUB15.uc.com, CallManager". The details include:

- Status:** Ready
- Certificate Settings:**
 - File Name: CallManager.pem
 - Certificate Purpose: CallManager
 - Certificate Type: certs
 - Certificate Group: product-cm
 - Description: Self-signed certificate generated by system
- Certificate File Data:**
 - Version: 3 (0x2)
 - Serial Number: 61:00:28:ab:59:38:cc:7f:75:0c:e0:c8:e8:78:30:cd
 - Signature Algorithm: sha256WithRSAEncryption
 - Issuer: C = CN, O = cisco, OU = a, CN = CUCMPUB15.uc.com, ST = c, L = b
 - Validity:
 - Not Before: Sep 8 10:15:06 2023 GMT
 - Not After: Sep 6 10:15:05 2028 GMT
 - Subject: C = CN, O = cisco, OU = a, CN = CUCMPUB15.uc.com, ST = c, L = b
 - Subject Public Key Info:
 - Public Key Algorithm: rsaEncryption
 - RSA Public-Key: (2048 bit)
 - Modulus:

At the bottom of the details window, the "Download .PEM File" button is highlighted with a red box.

下載CallManager證書

步驟 3.2.配置信任點，貼上pem檔案並鍵入yes以接受證書。

```
VG-CME-1(config)#crypto pki trustpoint cucm-pub
VG-CME-1(ca-trustpoint)# enrollment terminal
VG-CME-1(ca-trustpoint)# revocation-check none
VG-CME-1(ca-trustpoint)# crypto pki authenticate cucm-pub
```

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

```
-----BEGIN CERTIFICATE-----
MIIDozCCAougAwIBAgIQYQAoq1k4zH91DOAM6HgWzTANBgkqhkiG9w0BAQsFADBC
MQswCQYDVQQGEwJDTjEOMAwGA1UECgwFY2lZy28xCjAIBgNVBAsMAWExGTAXBgNV
BAMMEENVQ01QVUlxNS51Yy5jb20xCjAIBgNVBAGMAWMxCjAIBgNVBACMAWIwHhcN
MjMwOTA4MTAxNTA2WhcNMjMwOTA4MTAxNTA1WjBcMQswCQYDVQQGEwJDTjEOMAwG
A1UECgwFY2lZy28xCjAIBgNVBAsMAWExGTAXBgNVBAMMEENVQ01QVUlxNS51Yy5j
b20xCjAIBgNVBAGMAWMxCjAIBgNVBACMAWIwggEiMA0GCSqGSIb3DQEBAQUAA4IB
DwAwggEKAoIBAQD4Xfdl9MwYy/bSDXzGjtd301vYqKdRqpVYpWD7E+Nrh7zRgHh+
M7gAeqdRCSC/iKUF2g44RCrJlM0C/9xN3pxvOnNequg/Tv0wjpHm0X2O4x0daH+F
AwEIWNyZzVUQ6+2xtkTuUcqeXDnnbS6fLladP/CfgQwKX5U1Ec575ypUet6Fp2n2
4UouLQ5iFEMmX9gzGR7YKjeE+t61X5NmvYc6IyP8MH77sgvti7+xJurIUnvBFG2
ELXM0rL7uUoqw/rjMT6XxK+0ft4bkOsVnjl+vOUUBUoTcbFFrsfrOnVQjPJhHue
MLAaRzkDo5p1xo+UnNgv2uSH9HAID/NS1VTDAGMBAAGjYTBfMAsGA1UdDwQEAwIC
tDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwHQYDVR0OBBYEFKrlBeQi
```

```
OF6Hp0QCUfVYzKWiX2hMBIGA1UdEwEB/wQIMAYBAf8CAQAwDQYJKoZIhvcNAQEL
BQADggEBAJSw2vOwJ4UatmkaFpeLc9B1YZr8X6BkxBY1skW2qOLps61ysjDG61VQ
GjxpPLMY1ISyIVr5dqGyjaGLCUDUUCu66zEPxFNGnSYimBBhGR6NrDyo4YjOk+S
1I3TfRK+2F9NMhW2xTvuygoXLtyibvrZULhNo3vDPYQdTe1z54oQNU4BD8P+MCq9
+MzltCXEpVU6Jp71zC5HY+GF+Ab/xKBNzDjyY+OT8BFiO2wC8aaEaBvByNRzCSPD
MpU5cRaKvIp2pszoR9mG3Rls4CkK93OX/OzFqklemDmY5WcylcCsybxAMbjdBDY9
err7iQZzjoW3eD5HxJKyVsfjDRtqg8=
-----END CERTIFICATE-----
```

Certificate has the following attributes:

Fingerprint MD5: 259A3F16 A5111877 901F00C8 F58C5CE3

Fingerprint SHA1: E4E91B76 B09C8BDF 81169444 BF5B4D77 E0738987

% Do you accept this certificate? [yes/no]: yes

Trustpoint CA certificate accepted.

% Certificate successfully imported

步驟 4. 配置CUCM以信任安全會議橋。

步驟 4.1. 複製通用證書，並將其另存為SecureCFB.pem檔案。複製CA證書，然後將其另存為testCA.pem檔案。

```
VG-CME-1(config)#crypto pki export SecureCFB pem terminal
```

```
% CA certificate:
```

```
-----BEGIN CERTIFICATE-----
```

```
MIIIBzCCAWSgAwIBAgIBATANBgkqhkiG9w0BAQQFADARMQ8wDQYDVQQDEwZ0ZXN0
Q0EwHhcNMjQwNTUwMDg0NDI3WWhcNMjcwNTEwMDg0NDI3WjARMQ8wDQYDVQQDEwZ0
ZXN0Q0EwGz8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAM2Lqils9nddFOx/YN7y
hhp9KGI2Eb8Zxq9E2mXfKpHOpbcGEic5ain+rXf1qauA8/pNYwvBurAZm2pWzFHQ
q4qGL8KWDwJCPTwPI5rJOJAMlYzMh4WdQerWP4iEI2LGtxCb1q8b3w0wJE0Q2OG4
4kDSeArkKe0cb26WZC1oVK1jAgMBAAGjYzBhMA8GA1UdEwEB/wQFMAMBAf8wDgYD
VR0PAQH/BAQDAGGMB8GA1UdIwQYMBaAFJOFqPH+VBcd01d9SzcPhNkWGqcWMB0G
A1UdDgQWBBSThaxj/IQXHdNXfUswqYTZFhqnFjANBgkqhkiG9w0BAQQFAAOBgQAS
V8x9QjJ5pZKmezDYvxPDfe4chlKCD7o8JOcutSdAi7H+2Z+GO4CF55EDTZdLZPtn
GwQ01gbtDX07PTroYRWOSZLSJSdPQITJ3WDNR+NBhZjfe6EzfsLasD8L0VYG96GX
vjRQbdRmqbrG5H0ZUuZ0cu93AXjnRI2nLoAkKcrjcQ==
-----END CERTIFICATE-----
```



```
% General Purpose Certificate:
```

```
-----BEGIN CERTIFICATE-----
```

```
MIIIB6jCCAVogAwIBAgIBAjANBgkqhkiG9w0BAQUFADARMQ8wDQYDVQQDEwZ0ZXN0
Q0EwHhcNMjQwNTUwMDg1NTA4WWhcNMjcwNTEwMDg0NDI3WjAUMRIwEAYDVQQDEwIT
ZWN1cmVDRklwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALhk11yOPnUNTjEQ
JLJIMPnoc6Zb9vDrGollMdsz/cZwKtiGCS9PYYxwcPBEExOOR+XrE9MmEO7L/tr6n
NkKz84ddWNz0gg6wHWM9gcje22blsleU6UCxo4ovra2pExXphusqEmg5yLQwyeJc
5JqcoAYXuRpnKLTfn5Nnh6iUCsWrAgMBAAGjTzBNMAsGA1UdDwQEAwIFoDAfBgNV
HSMEGDAWgBSThaxj/IQXHdNXfUswqYTZFhqnFjAdBgNVHQ4EFgQU3y9zfDoTJ8WV
XlpX3wdcieq1zpkwDQYJKoZIhvcNAQEFBQADgYEABfaa6ppqRaDyfpW/tu5pXBRHP
SfZzpv+4ktsjAiOG7oGJGT0RpnuikCq+V2oucJbtWWAPbvX+ZBG3Eogi1c2GoDLK
yYvuaf9zBJHicM5mv6x81qxLF7FKZaepQSYwsQUP50/uKXa0435Kj/CZoLpKhXR2
v/p2jzF9zyPIBuQGEOEo=
-----END CERTIFICATE-----
```

步驟 4.2. 上傳SecureCFB.pem到CUCM上的CallManager-trust儲存(思科統一作業系統管理>安全>證書管理)。

Upload Certificate/Certificate chain

 Upload  Close

Status



Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster

Upload Certificate/Certificate chain

Certificate Purpose*

tomcat-trust

Description(friendly name)

Upload File

Choose File

SCFB.pem

Upload

Close



*- indicates required item.

上傳SecureCFB.pem

步驟 5.在VG上配置安全會議橋。

```
VG-CME-1(config)#voice-card 0
```

```
VG-CME-1(config-voicecard)# dsp service dspfarm
```

```
VG-CME-1(config)#dspfarm profile 666 conference security
```

```
VG-CME-1(config-dspfarm-profile)# trustpoint SecureCFB
```

```
VG-CME-1(config-dspfarm-profile)# codec g711ulaw
```

```
VG-CME-1(config-dspfarm-profile)# codec g711alaw
```

```
VG-CME-1(config-dspfarm-profile)# codec g729r8
```

```
VG-CME-1(config-dspfarm-profile)# maximum sessions 4
```

```
VG-CME-1(config-dspfarm-profile)# associate application SCCP
```

```
VG-CME-1(config)#sccp local GigabitEthernet 0/1
```

```
VG-CME-1(config)#sccp ccm x.x.x.x identifier 666 version 7.0+ (IP address of CUCM)
```

```
VG-CME-1(config)#sccp
```

```
VG-CME-1(config)#sccp ccm group 666
```

```
VG-CME-1(config-sccp-ccm)# associate ccm 666 priority 1
```

```
VG-CME-1(config-sccp-ccm)# associate profile 666 register SecureCFB
```

```
VG-CME-1(config)#dspfarm profile 666 conference security
```

```
VG-CME-1(config-dspfarm-profile)# no shutdown
```

步驟 6.在CUCM上配置安全會議橋(Cisco Unified CM管理>媒體資源>會議橋>新增)。

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

Conference Bridge Configuration

Save Delete Copy Reset Apply Config Add New

Status

Status: Ready

Conference Bridge Information

Conference Bridge : SecureCFB (SecureCFB)
Registration: Registered with Cisco Unified Communications Manager CUCMPUB15
IPv4 Address: 10.124.42.5

IOS Conference Bridge Info

Conference Bridge Type* **Cisco IOS Enhanced Conference Bridge**

Device is trusted

Conference Bridge Name* **SecureCFB**

Description: SecureCFB

Device Pool*: Default ▾

Common Device Configuration: < None > ▾

Location*: Hub_None ▾

Device Security Mode* **Encrypted Conference Bridge**

Use Trusted Relay Point*: Default ▾

Save Delete Copy Reset Apply Config Add New

配置安全會議網橋

任務2.使用安全模式註冊3部8865NR IP電話。

在IP電話上將裝置安全配置檔案設定為加密模式。

Protocol Specific Information

Packet Capture Mode* None ▾

Packet Capture Duration: 0

BLF Presence Group* Standard Presence group ▾

SIP Dial Rules: < None > ▾

MTP Preferred Originating Codec* 711ulaw ▾

Device Security Profile* Universal Device Template - Security Profile - Encryl ▾

Rerouting Calling Search Space: < None > ▾

SUBSCRIBE Calling Search Space: < None > ▾

SIP Profile*: < None > ▾ [View Details](#)

Digest User: < None > ▾

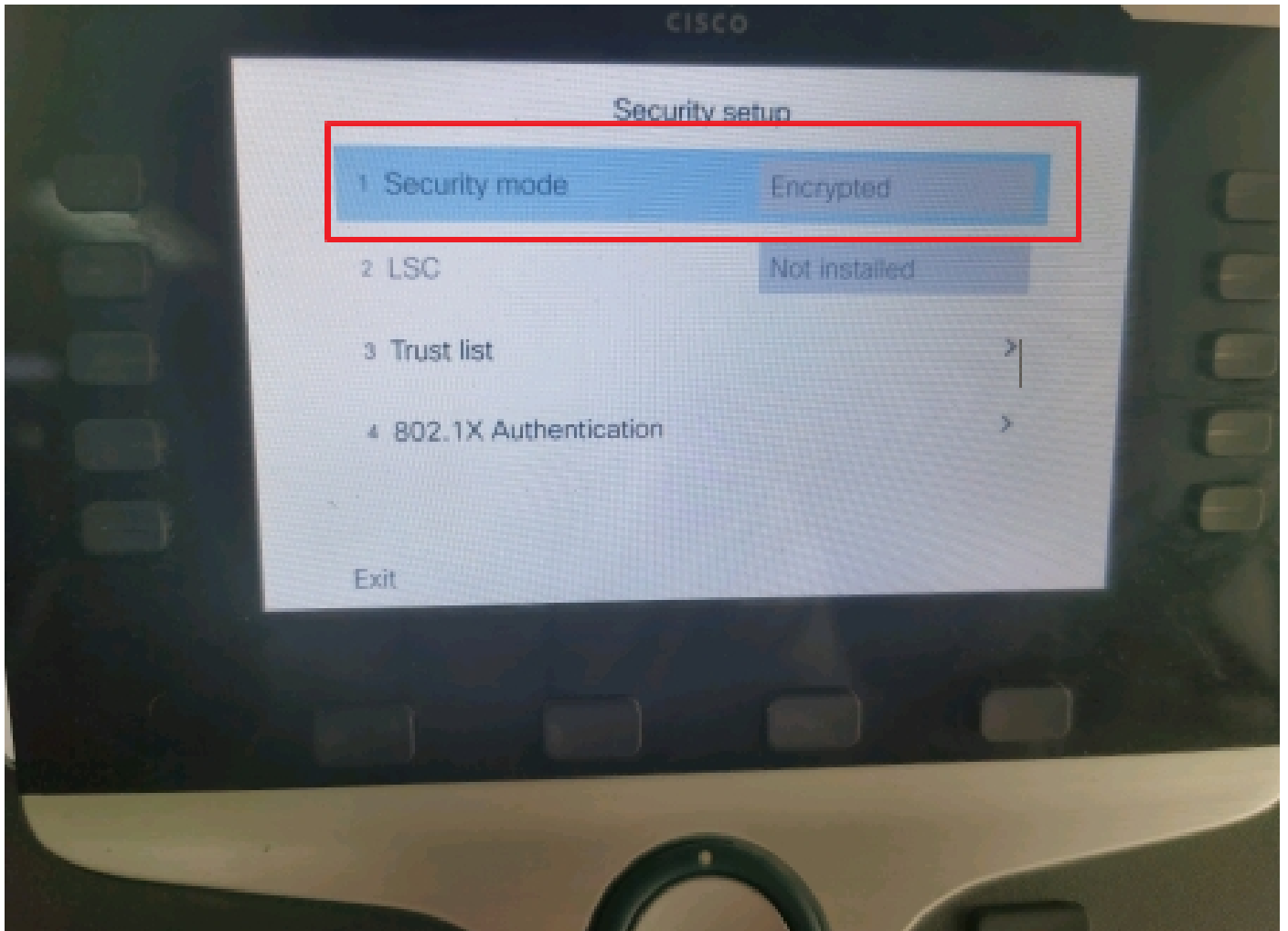
Media Termination Point Required

Unattended Port

Require DTMF Reception

將裝置安全配置檔案設定為加密模式

IP電話在Admin settings > Security Setup下顯示Security mode with Encrypted。




安全模式已加密

任務3.使用安全會議網橋配置媒體資源組清單並將其分配給IP電話。

步驟 1.建立媒體資源組MRG_SecureCFB並向其分配SecureCFB(Cisco Unified CM管理>媒體資源>媒體資源組)。

Media Resource Group Configuration

 Save  Delete  Copy  Add New

 Status: Ready

Media Resource Group Status

Media Resource Group: SecureCFB (used by 0 devices)

Media Resource Group Information

Name*
Description

Devices for this Group

Available Media Resources**

Selected Media Resources*

Use Multi-cast for MOH Audio (If at least one multi-cast MOH resource is available)

建立媒體資源組MRG_SecureCFB

步驟 2. 建立媒體資源組清單MRGL_SecureCFB並向其分配MRG_SecureCFB(Cisco Unified CM管理>媒體資源>媒體資源組清單)。

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk A

Media Resource Group List Configuration

Save

Status
 Status: Ready

Media Resource Group List Status
 Media Resource Group List: New

Media Resource Group List Information
 Name*

Media Resource Groups for this List
 Available Media Resource Groups

Selected Media Resource Groups

建立媒體資源組清單MRGL_SecureCFB

步驟 3. 將媒體資源組清單MRGL_SecureCFB分配給所有8865NR。

CISCO United CM Administration For Cisco Unified Communications Solutions Skip to Content Navigation Cisco Unified CM

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

Phone Configuration

Related Links: [Back To Find/List](#)

Save Delete Copy Reset Apply Config Add New

7	Add a new SD	<input checked="" type="checkbox"/> Device is Active
8	Add a new SD	<input checked="" type="checkbox"/> Device is trusted
9	Add a new SD	MAC Address* <input type="text" value="A4B439D38E15"/> (SEPA4B439D38E15)
10	Add a new SD	Description <input type="text" value="SEPA4B439D38E15"/>
----- Unassigned Associated Items -----		
11	Add a new SD	Current On-Premise Onboarding Method is set to Autoregistration. Activation Code will only apply to onboarding via MRA.
12	Alerting Calls	<input type="checkbox"/> Require Activation Code for Onboarding
13	All Calls	<input type="checkbox"/> Allow Activation Code via MRA
14	Answer Oldest	Activation Code MRA Service Domain <input type="text" value="-- Not Selected --"/> View Details
15	Add a new BLF Directed Call Park	Device Pool* <input type="text" value="test"/> View Details
16	Call Park	Common Device Configuration <input type="text" value="< None >"/> View Details
17	Call Pickup	Phone Button Template* <input type="text" value="Standard 8865NR SIP"/>
18	CallBack	Softkey Template <input type="text" value="< None >"/>
19	Do Not Disturb	Common Phone Profile* <input type="text" value="Standard Common Phone Profile"/> View Details
20	Group Call Pickup	Calling Search Space <input type="text" value="< None >"/>
21	Hunt Group Logout	AAR Calling Search Space <input type="text" value="< None >"/>
22	Intercom [1] - Add a new Intercom	Media Resource Group List <input type="text" value="MRGL_SecureCFB"/>
23	Malicious Call Identification	User Hold MOH Audio Source <input type="text" value="< None >"/>
24	Max M...	Network Hold MOH Audio Source <input type="text" value="< None >"/>
		Location* <input type="text" value="Hub_None"/>
		AAR Group <input type="text" value="< None >"/>
		User Locale <input type="text" value="< None >"/>

分配媒體資源組清單

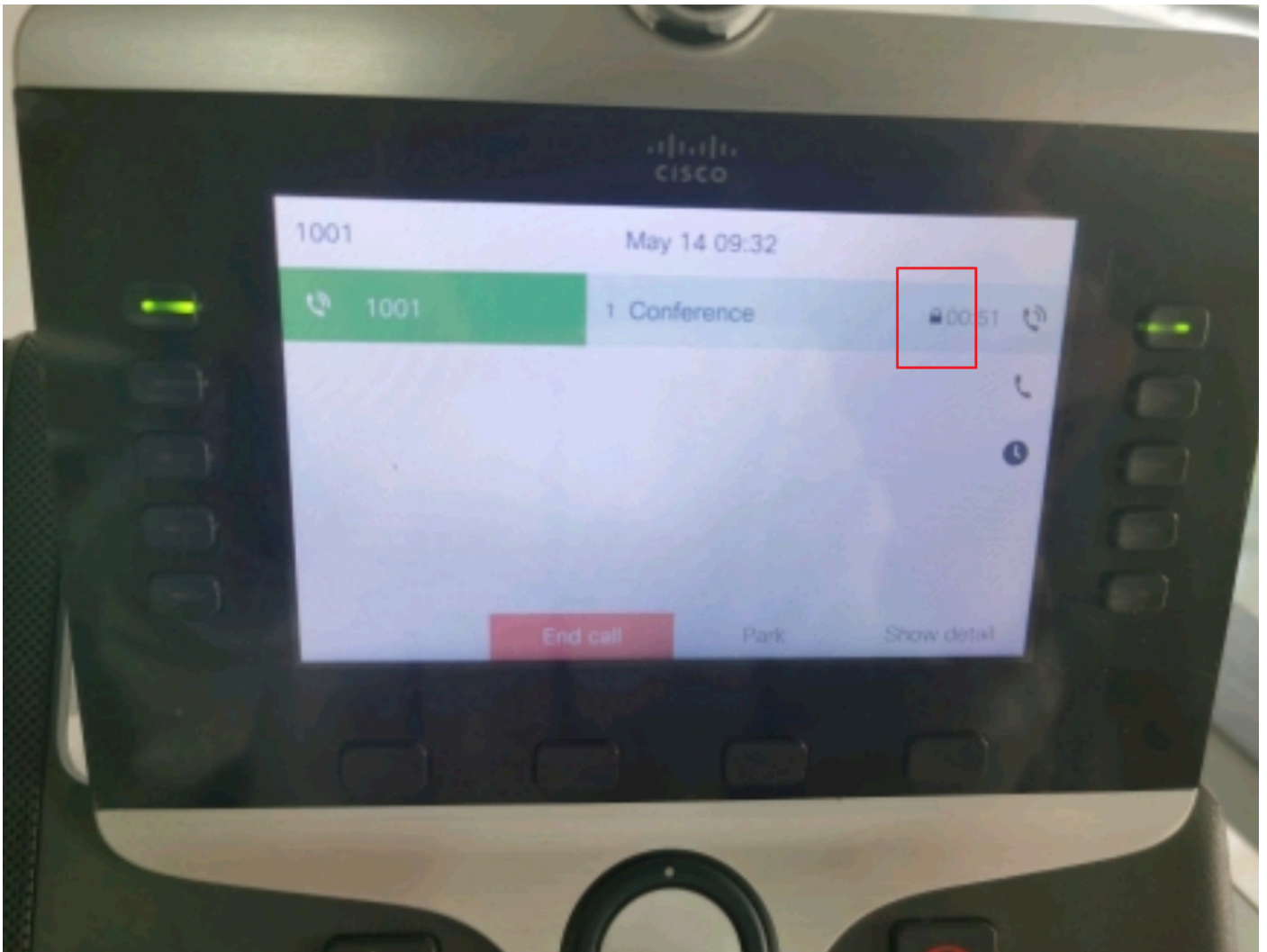
驗證

IP電話1與DN 1001、IP電話2與DN 1002、IP電話3與DN 1003。

測試步驟。

1. 1001呼叫1002。
2. 1001新聞記者會軟鍵並撥打1003。
3. 1001新聞記者會軟鍵讓安全臨時會議參與。

Cisco IP電話顯示會議安全圖示，以指示呼叫已加密。



測試呼叫已加密

疑難排解

透過RTMT收集下一個資訊。

Cisco CallManager (呼叫日誌提供有關呼叫的資訊，sdl資料夾包含CUCM跟蹤)。

從SDL追蹤軌跡可看到，當1001 press conference soft key傳送一個SIP REFER訊息給會議1002和1003。

00018751.002 |17:53:18.056 | 應用資訊 |SIPTcp - wait_SdlReadRsp : 埠51320索引7上來自x.x.x.x的傳入SIP TCP消息，2039位元組：

[587, NET]

請參閱SIP : CUCMPUB15 SIP/2.0

透過 : SIP/2.0/TLS x.x.x.x : 51320 ; branch=z9hG4bK4d786568

發件人 : "1001" <sip : 1001@x.x.x.x> ; tag=a4b439d38e15003872a7c133-28fd5212

收件人 : <sip : CUCMPUB15>

電話ID : a4b439d3-8e150010-2f865ab1-7160f679@x.x.x.x

Session-ID :

b14c8b6f00105000a000a4b439d38e15 ; remote=00000000000000000000000000000000

日期 : 2024年5月14日星期二09:53:17葛林威治標準時間

CSeq : 1000參考

使用者代理 : Cisco-CP8865NR/14.2.1

接受 : application/x-cisco-remotecc-response+xml

截止日期 : 60

最大轉發數 : 70

聯絡人 : <sip : 8a854224-e17e-93da-8e71-

6a2796f28fc7@x.x.x.x:51320 ; transport=tls> ; +u.sip ! devicename.ccm.cisco.com="SEPA4B439D38E1

推薦人 : 「1001」 <sip : 1001@x.x.x.x>

請參閱 : cid : 3e94126b@x.x.x.x

內容ID : <3e94126b@x.x.x.x>

允許 : ACK、BYE、CANCEL、INVITE、NOTIFY、OPTIONS、REFER、REGISTER、UPDATE、SUBSCRIBE

內容長度 : 1069

內容型別 : application/x-cisco-remotecc-request+xml

Content-Disposition : 會話 ; 處理=必需

< ? xml version="1.0" encoding="UTF-8" ? >

<x-cisco-remotecc-request>

<softkeyeventmsg>

<softkeyevent>會議</softkeyevent>

<dialogid>

<callid>a4b439d3-8e150007-1991b55f-00f9dcf7@x.x.x.x</callid>

<localtag>a4b439d38e1500333f1eb5d4-68656916</localtag>

<remotetag>171-ca425666-d5e7-42aa-a428-23dde46063a5-17600290</remotetag>

</dialogid>

<linenumber>0</linenumber>

<participantnum>0</participantnum>

<consultdialogid>

<callid>a4b439d3-8e150008-415a60f5-7c35c82d@x.x.x.x</callid>

<localtag>a4b439d38e15003562c2c59a-69dbf571</localtag>

<remotetag>176-ca425666-d5e7-42aa-a428-23dde46063a5-17600292</remotetag>

</consultdialogid>

<state>>false</state>

<joindialogid>

<callid></callid>

<localtag></localtag>

<remotetag></remotetag>

</joindialogid>

<eventdata>

<invocationtype>explicit</invocationtype>

</eventdata>

<userdata></userdata>

<softkeyid>0</softkeyid>

<applicationid>0</applicationid>

</softkeyeventmsg>

</x-cisco-remotecall-request>

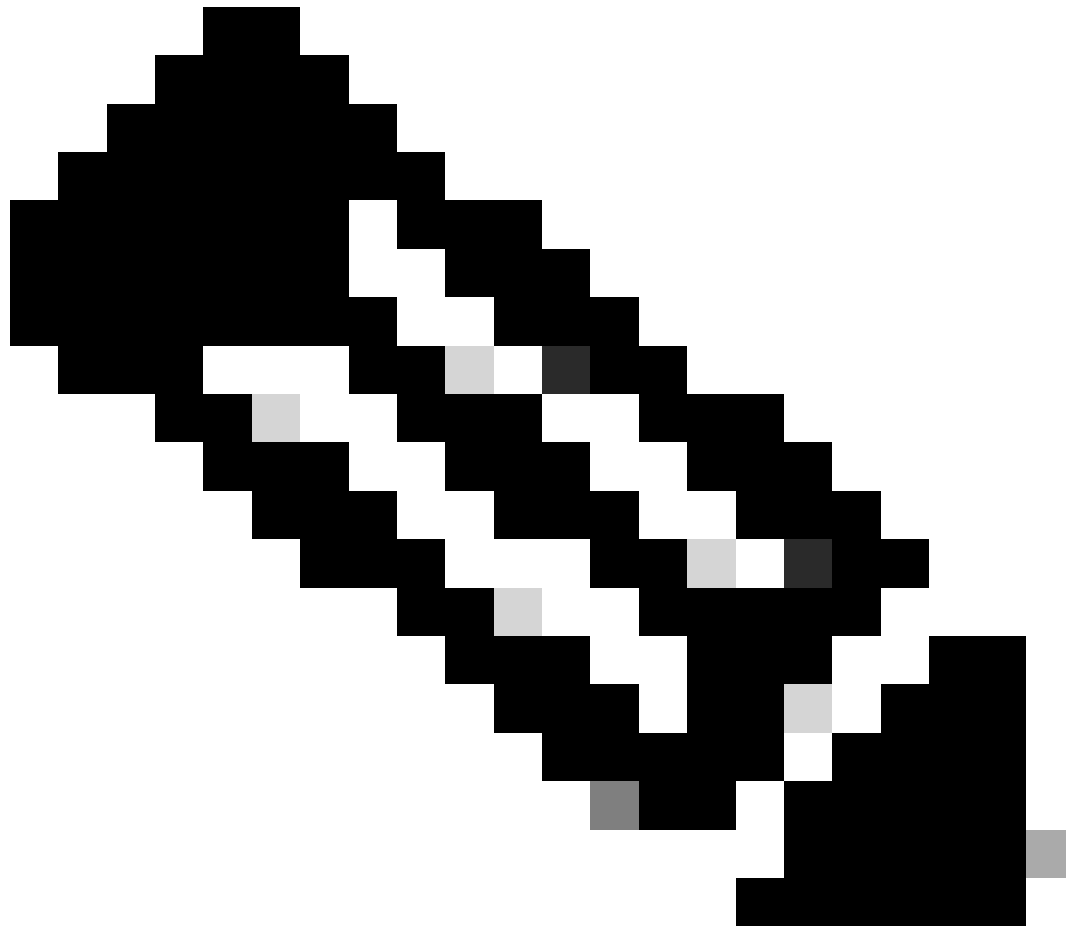
00018751.003 |17:53:18.056 | 應用資訊 |SIPTcp - SignalCounter = 300

然後，CUCM進行數字分析，最後路由到裝置SecureCFB。

```
00018997.000 |17:53:18.134 |SdlSig |CcRegisterPartyB |tcc_register_party_b
|Cdcc(1,100,39,7) | 副本(1,100,38,1) |1,100,251,1.33^^^*
|[R : N-H : 0 , N : 2 , L : 0 , V : 0 , Z : 0 , D : 0] CI=17600297 CI.branch=0 CSS= AdjunctCSS=
cssIns=0 aarCSS= aarDev=F FQDN=pi=0si1 CallRef=0 OLC=1 Name=locale : 1名稱 : 4
Unicode名稱 : pi : 0EncodeType=10 qsig-encodeType=10 ConnType=3 Xfer模式8 ConnTime=3
nwLoc=0IpAddrMode=0 ipAddrType=0 ipv4=x.x.x.x : 0 region=Default capCount=6 devType=1
mixerCId=16778218 mediaReq=0 portToPort.loc=0 MOH.userHoldID=0 MOH.netHoldID=0
MOH.supp=1 devName=SECURECFB mobileDev Name= origEMCCallingDevName=
mobilePartyNumber=pi=0si1 mobileCallType=0 ctiActive=F ctiFarEndDev=1 ctiCCMId=1
devCepn=38281c14-d78f-46d6-8199-63297bcfddae lineCepn= activeCaps=0 VideoCall=F
MMUpdateCapMask=0x3e MMCap=0 x1 SipConfig : BFCAAllowed=F IXAllowed=F devCap=0
CryptoCapCount=6 secure=3 loginId= UnicodeName : retriedVideo=FFromTag=ToTag=CallId=
UAPortFlag=F wantDTMFRecep=1 provOOB=0 support DTMF=1 DTMF Cfg=1 DTMF PT=()
DTMF reqMed=1 is prefAltScript=F cdpnPatternUsage=2 audioPtyId=0 doNotAppendLineCSS=F
callingDP= BCUpdate=0 ccBearCap.itc=0 ccBearCap.itr=0 protected=1 flushCapIns=0
geolocInfo=locPkid= locName= deductBW=FateShareId=
videoTrafficClass=UnspecifiedBridgeParticipant ID callingUsr= remoteClusterID=
isEMCCDevice=F dtmCall=F dtmPrimaryCI=0 dtmMediaFPid=(0,0 , 0) dtmMcNodeId=0
dtmMTPForDTMFTranslation=F emc=T QSIGIMERoute=0 eoUpdt=1 vCTCUpdt=1
honorCodec=FHonorUpdt=1Final calledPartition= cTypeUpdt=0 BibEnabled=0
RecordingQSIGAPDUSupported=F FarEndDeviceName=潛在Caps=null icidVal= icidGenAddr=
oioi= tioi= ptParams= CAL={v=-1 , m=-1 , tDev=F , res=F , devType=0}
displayNameUpdateFieldFlag=0 CFBCtrlSeclcon=F =F外部演示資訊[ pi=0si1locale : 1名稱 :
Unicode名稱 : pi : 0 mlsCallExternal=F ] ControlProcessType=0
controlProcessTypeUpdateFieldFlag=1 origPi=0
```

相關資訊

- https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/security/15_0/cucm_b_security-guide-release-15.pdf
- [思科技術支援與下載](#)



注意：Unified Communications Manager支援集群內中繼(ICT)、H.323中繼/網關和MGCP網關上的安全會議；但是，運行版本8.2或更早版本的加密電話將恢復為ICT和H.323呼叫的RTP，並且媒體不會得到加密。如果會議涉及SIP中繼，則安全會議狀態為非安全。此外，SIP中繼信令不支援向集群外的參與者傳送安全會議通知。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。