在CUCM上配置安全临时会议15

目录

简介

本文档介绍如何在CUCM 15上配置安全临时会议。

先决条件

要求

Cisco 建议您了解以下主题：

- CUCM
- VG（语音网关）
- 安全概念

使用的组件

本文档中的信息基于以下软件和硬件版本：

- CUCM（混合模式）版本：15.0.0.98100-196
- CISCO2921版本：15.7(3)M4b（用作CA和安全会议网桥）
- NTP 服务器
- 3台8865NR IP电话

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

任务1.配置安全会议网桥并注册到CUCM。

步骤1:配置Public Key Infrastructure服务器和信任点。

步骤 1.1配置NTP服务器和HTTP服务器。

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

步骤 1.2 配置Public Key Infrastructure服务器。

```
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
```

步骤 1.3为testCA配置信任点。

```
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
```

步骤 1.4等待约30秒，然后发出命令no shutdown以启用testCA服务器。

```
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.
```

第二步：为安全会议网桥配置信任点并将其注册到testCA。

步骤 2.1 为安全会议网桥配置信任点并将其命名为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
```

步骤 2.2验证SecureCFB并键入“yes”以接受证书。

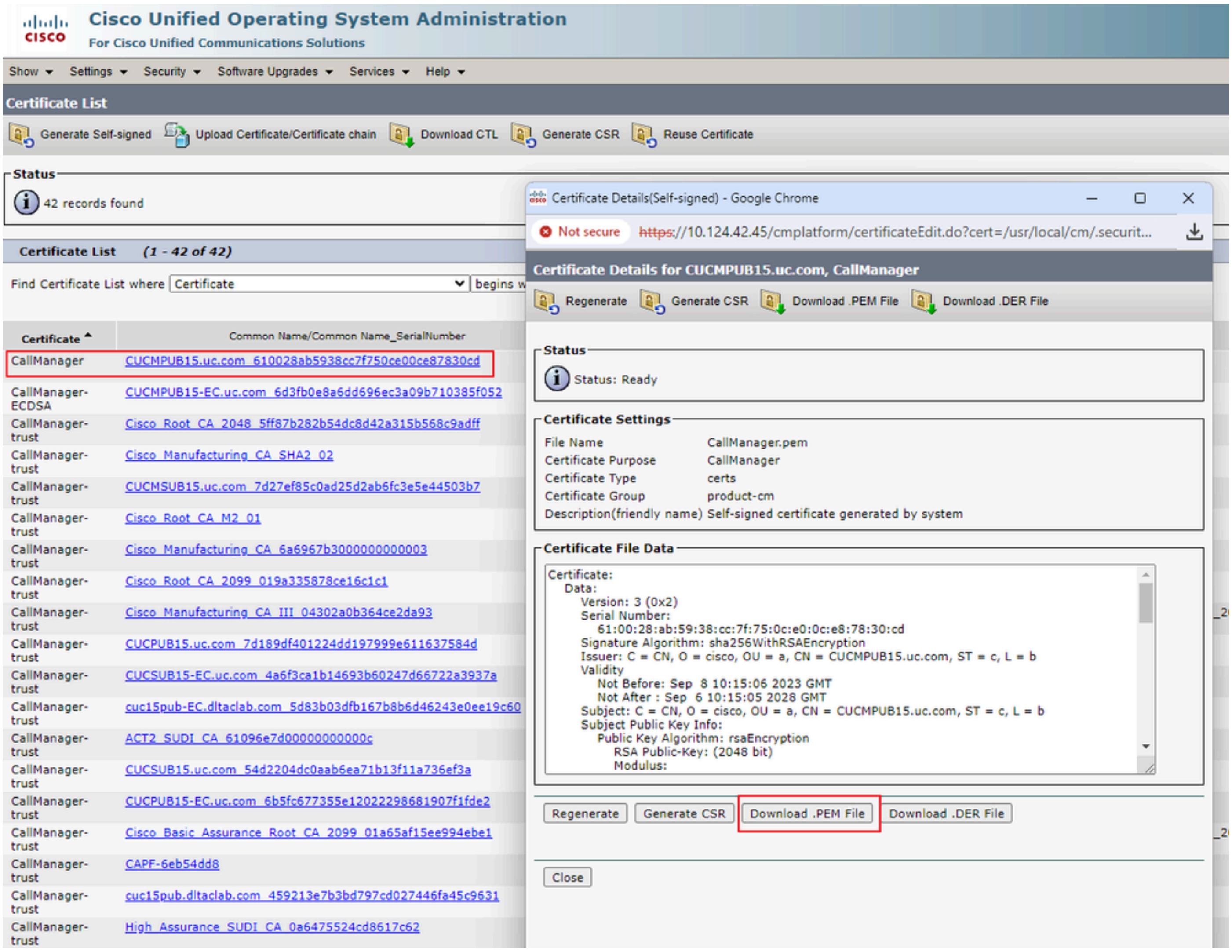
```
VG-CME-1(config)#crypto pki authenticate SecureCFB
Certificate has the following attributes:
      Fingerprint MD5: 383BA13D C37D0E5D 9E9086E4 8C8D1E75
     Fingerprint SHA1: 6DB8F323 14BBFBFF C36C224B B3404513 2FDD97C5

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

步骤 2.3注册SecureCFB并设置密码。

```
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' commandwill show the fingerprint.
```

第三步：在安全相关性网桥上配置CUCM的信任点。

步骤 3.1从CUCM下载CallManager证书并复制pem文件(Cisco Unified OS Administration > Security > Certificate Management)。


Cisco Unified Operating System Administration
For Cisco Unified Communications Solutions
Show
Settings
Security
Software Upgrades
Services
Help
Certificate List
Generate Self-signed
Upload Certificate/Certificate chain
Download CTL
Generate CSR
Reuse Certificate
Certificate Details(Self-signed) - Google Chrome
Not secure
https://10.124.42.45/cmplatform/certificateEdit.do?cert=/usr/local/cm/.securit...
Regenerate
Generate CSR
Download .PEM File
Download .DER File
Close

Status

42 records found

Certificate List (1 - 42 of 42)

Find Certificate List where Certificate begins w

Certificate	Common Name/Common Name_SerialNumber
CallManager	CUCMPUB15.uc.com_610028ab5938cc7f750ce00ce87830cd
CallManager-ECDSA	CUCMPUB15-EC.uc.com_6d3fb0e8a6dd696ec3a09b710385f052
CallManager-trust	Cisco_Root_CA_2048_5ff87b282b54dc8d42a315b568c9adff
CallManager-trust	Cisco_Manufacturing_CA_SHA2_02
CallManager-trust	CUCMSUB15.uc.com_7d27ef85c0ad25d2ab6fc3e5e44503b7
CallManager-trust	Cisco_Root_CA_M2_01
CallManager-trust	Cisco_Manufacturing_CA_6a6967b3000000000003
CallManager-trust	Cisco_Root_CA_2099_019a335878ce16c1c1
CallManager-trust	Cisco_Manufacturing_CA_III_04302a0b364ce2da93
CallManager-trust	CUCPUB15.uc.com_7d189df401224dd197999e611637584d
CallManager-trust	CUCSUB15-EC.uc.com_4a6f3ca1b14693b60247d66722a3937a
CallManager-trust	cuc15pub-EC.dltaclab.com_5d83b03dfb167b8b6d46243e0ee19c60
CallManager-trust	ACT2_SUDI_CA_61096e7d00000000000c
CallManager-trust	CUCSUB15.uc.com_54d2204dc0aab6ea71b13f11a736ef3a
CallManager-trust	CUCPUB15-EC.uc.com_6b5fc677355e12022298681907f1fde2
CallManager-trust	Cisco_Basic_Assurance_Root_CA_2099_01a65af15ee994ebe1
CallManager-trust	CAPF-6eb54dd8
CallManager-trust	cuc15pub.dltaclab.com_459213e7b3bd797cd027446fa45c9631
CallManager-trust	High_Assurance_SUDI_CA_0a6475524cd8617c62

Certificate Details for CUCMPUB15.uc.com, CallManager

Status

Status: Ready

Certificate Settings

File Name	CallManager.pem
Certificate Purpose	CallManager
Certificate Type	certs
Certificate Group	product-cm
Description(friendly name)	Self-signed certificate generated by system

Certificate File Data

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            61:00:28:ab:59:38:cc:7f:75:0c:e0:0c: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:
```

下载CallManager证书

步骤 3.2配置信任点，粘贴pem文件，键入yes以接受证书。

```
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
BAMMEENVQ01QVUIxNS51Yy5jb20xCjAIBgNVBAgMAWMxCjAIBgNVBAcMAWIwHhcN
MjMwOTA4MTAxNTA2WhcNMjgwOTA2MTAxNTA1WjBcMQswCQYDVQQGEwJDTjEOMAwG
A1UECgwFY2lzY28xCjAIBgNVBAsMAWExGTAXBgNVBAMMEENVQ01QVUIxNS51Yy5j
b20xCjAIBgNVBAgMAWMxCjAIBgNVBAcMAWIwggEiMA0GCSqGSIb3DQEBAQUAA4IB
DwAwggEKAoIBAQD4Xfdl9MWY/bSDXzGjtd301vYqKdRpqVYpWD7E+NrH7zRgHhz+
M7gAeqdRCSC/iKUF2g44rCRjlM0C/9xN3pxvOnNequg/Tv0wjpHm0X2O4x0daH+F
AwElWNYZZvUQ6+2xtkTuUcqeXDnnbS6fLIadP/CfgQwKX5U1Ec575ypUet6Fp2n2
4UouLQ5iFEMmX9gzGR7YKjeE+t61X5NmvYc6IyP8MH77sgvti7+xJurlJUnvBFG2
ELXM0rL7uUoqw/rjMT6XxK+0Ft4bkOsVnjI+vOUUBUoTcbFFrsfrcOnVQjPJhHue
MLAaRzkDo5p1xo+UnNgv2uSH9HAID/NS1VTDAgMBAAGjYTBfMAsGA1UdDwQEAwIC
tDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwHQYDVR0OBBYEFKrIBeQi
```

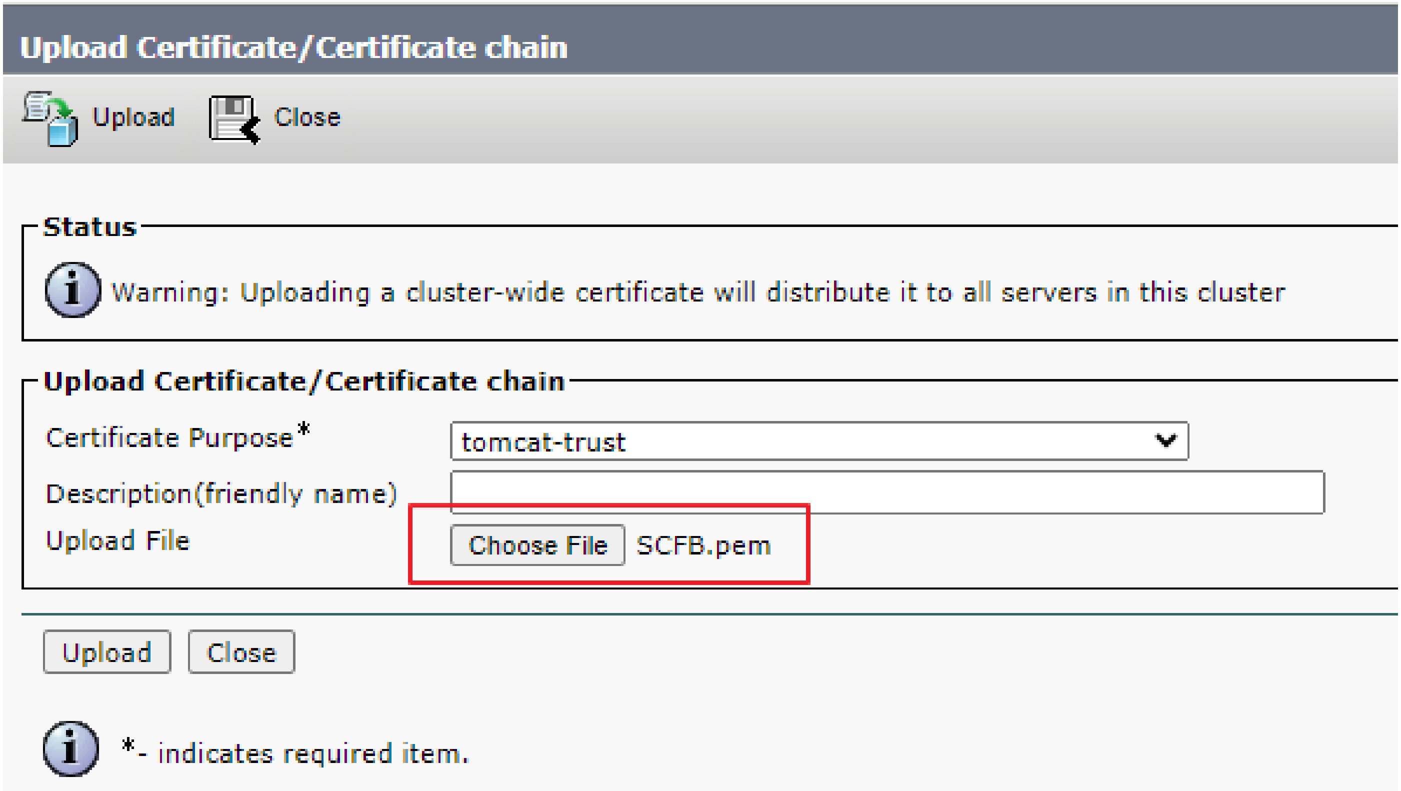
```
OF6Hp0QCUfVYzKWiXx2hMBIGA1UdEwEB/wQIMAYBAf8CAQAwDQYJKoZIhvcNAQEL
BQADggEBAJSw2vOwJ4UatmkaFpeLc9B1YZr8X6BkxBY1skW2qOLps61ysjDG61VQ
GjxpPLMY1ISyIVr5dqGyjcaGLCUDUUcu66zEPxFNGnSYimBBhGR6NrDyo4YjOk+S
1I3TfRK+2F9NMhW2xTvuygoXLtyibvrZULhNo3vDPYQdTe1z54oQNU4BD8P+MCq9
+MzltCXEpVU6Jp71zC5HY+GF+Ab/xKBNzDjyY+OT8BFiO2wC8aaEaBvByNRzCSPD
MpU5cRaKVip2pszoR9mG3Rls4CkK93OX/OzFqkIemDmY5WcylcCsybxAMbjdBDY9
err7iQZzjoW3eD5HxJKyvSffjDRtqg8=
-----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
```

第四步：配置CUCM以信任安全会议网桥。

步骤 4.1复制通用证书，并将其另存为SecureCFB.pem文件。复制CA证书，然后将其另存为testCA.pem文件。

```
VG-CME-1(config)#crypto pki export SecureCFB pem terminal
% CA certificate:
-----BEGIN CERTIFICATE-----
MIIB+zCCAWSgAwIBAgIBATANBgkqhkiG9w0BAQQFADARMQ8wDQYDVQQDEwZ0ZXN0
Q0EwHhcNMjQwNTEwMDg0NDI3WhcNMjcwNTEwMDg0NDI3WjARMQ8wDQYDVQQDEwZ0
ZXN0Q0EwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAM2LqiIs9nddFOx/YN7y
hhp9KGl2Eb8Zxq9E2mXfKpHOpbcGEic5ain+rXf1qauA8/pNYwvBurAZm2pWzFHQ
q4qGL8KWDwJCPTwPI5rJOJAMIYzMh4WdQerWP4iEI2LGtxCb1q8b3w0wJE0Q2OG4
4kDSeArkKe0cb26WZC1oVK1jAgMBAAGjYzBhMA8GA1UdEwEB/wQFMAMBAf8wDgYD
VR0PAQH/BAQDAgGGMB8GA1UdIwQYMBaAFJOFqPH+VBcd01d9SzCphNkWGqcWMB0G
A1UdDgQWBBSThajx/lQXHdNXfUswqYTZFhqnFjANBgkqhkiG9w0BAQQFAAOBgQAS
V8x9QjJ5pZKmezDYvxPDFe4chIkCD7o8JOcutSdAi7H+2Z+GO4CF55EDTZdLZPtn
GwQ01gbtDX07PTrOYRWOSZLSJSdPQlTJ3WDNr+NBhZjfe6EzfsLasD8L0VYG96GX
vjRQbdRmqbrG5H0ZUUz0cu93AXjnRl2nLoAkKcrjcQ==
-----END CERTIFICATE-----

% General Purpose Certificate:
-----BEGIN CERTIFICATE-----
MIIB6jCCAVOgAwIBAgIBAjANBgkqhkiG9w0BAQUFADARMQ8wDQYDVQQDEwZ0ZXN0
Q0EwHhcNMjQwNTEwMDg1NTA4WhcNMjcwNTEwMDg0NDI3WjAUMRIwEAYDVQQDEwlT
ZWN1cmVDRkIwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALhk11yOPnUNtjEQ
JLJIMPnoc6Zb9vDrGoIlMdsz/cZwKTiGCs9PYYxwcPBExOOR+XrE9MmEO7L/tR6n
NkKz84ddWNz0gg6wHWM9gcje22bIsIeU6UCxo4ovra2pExXphusqEmg5yLQwyeJc
5JqcoAYXuRpnKLTfn5Nnh6iUCsWrAgMBAAGjTzBNMAsGA1UdDwQEAwIFoDAfBgNV
HSMEGDAWgBSThajx/lQXHdNXfUswqYTZFhqnFjAdBgNVHQ4EFgQU3y9zfDoTJ8WV
XIpX3wdcieq1zpkwDQYJKoZIhvcNAQEFBQADgYEABfaa6pqRaDyfpW/tu5pXBRHP
SfZzpv+4ktsjAiOG7oGJGT0RpnuiKCq+V2oucJBtWWAPbVx+ZBG3Eogi1c2GoDLK
yYvuaf9zBJHIcM5mv6x81qxLF7FKZaepQSYwsQUP50/uKXa0435Kj/CZoLpKhXR2
v/p2jzF9zyPIBuQGOEo=
-----END CERTIFICATE-----
```

步骤 4.2将SecureCFB.pem上传到CUCM上的CallManager-trust存储区(Cisco Unified OS Administration > Security > Certificate Management)。



Upload Certificate/Certificate chain

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: SCFB.pem

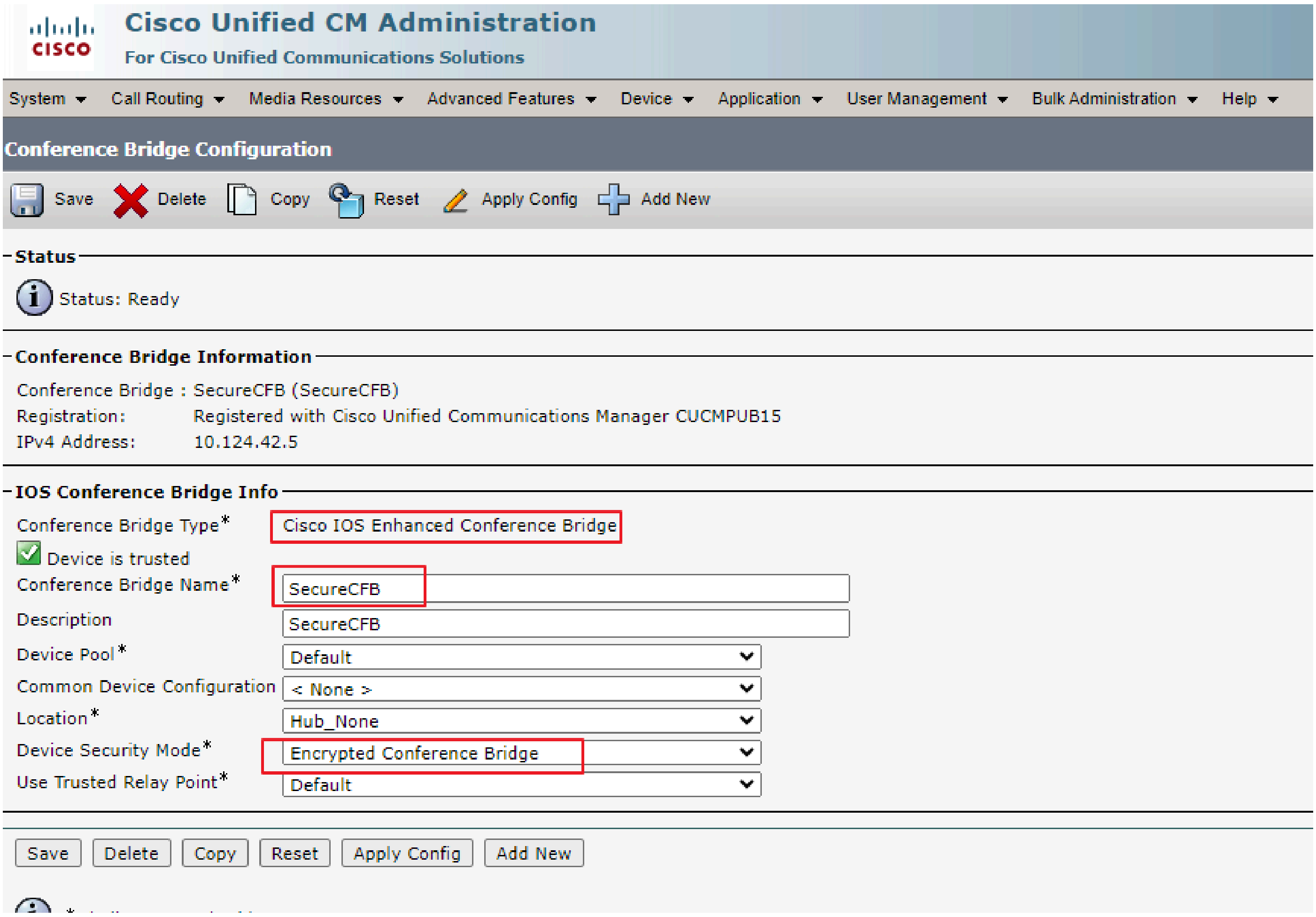
*- indicates required item.

上传SecureCFB.pem

第五步：在VG上配置安全会议网桥。

```
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
```

第六步：在CUCM上配置安全会议桥(Cisco Unified CM管理>媒体资源>会议桥>新增)。



Conference Bridge Configuration

Status

Status: Ready

Conference Bridge Information

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

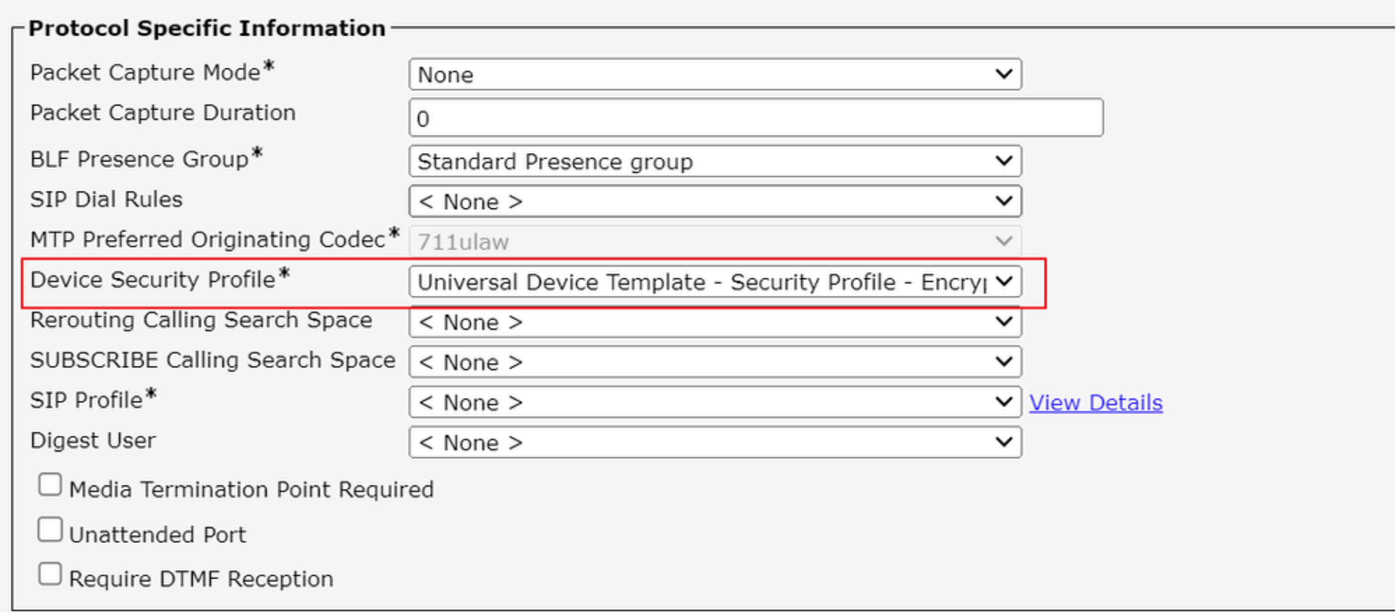
IOS Conference Bridge Info

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

配置安全会议网桥

任务2.使用安全模式注册3台8865NR IP电话。

在IP电话上将设备安全配置文件设置为加密模式。



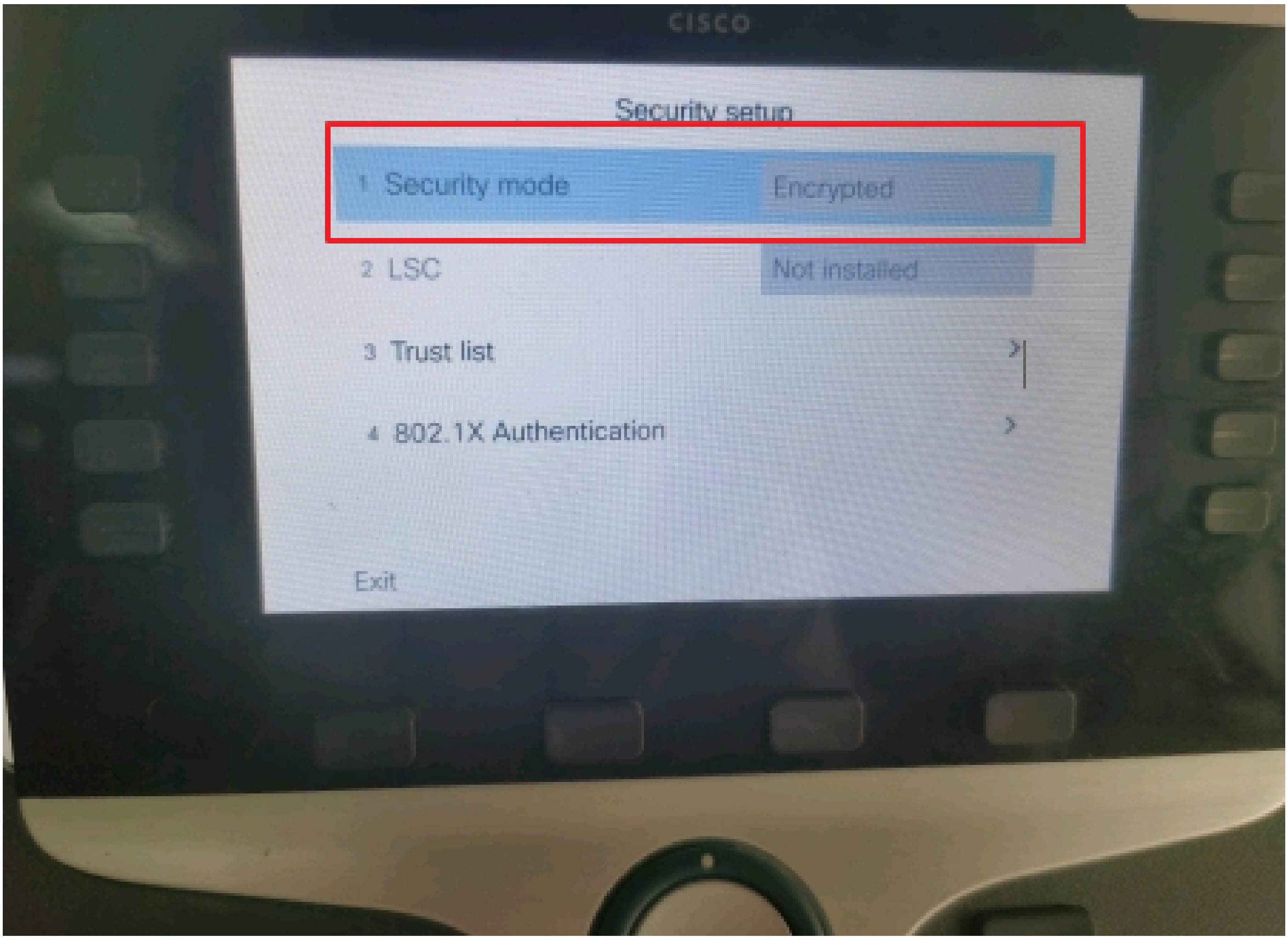
Protocol Specific Information

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 - Encryı
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

将设备安全配置文件设置为加密模式

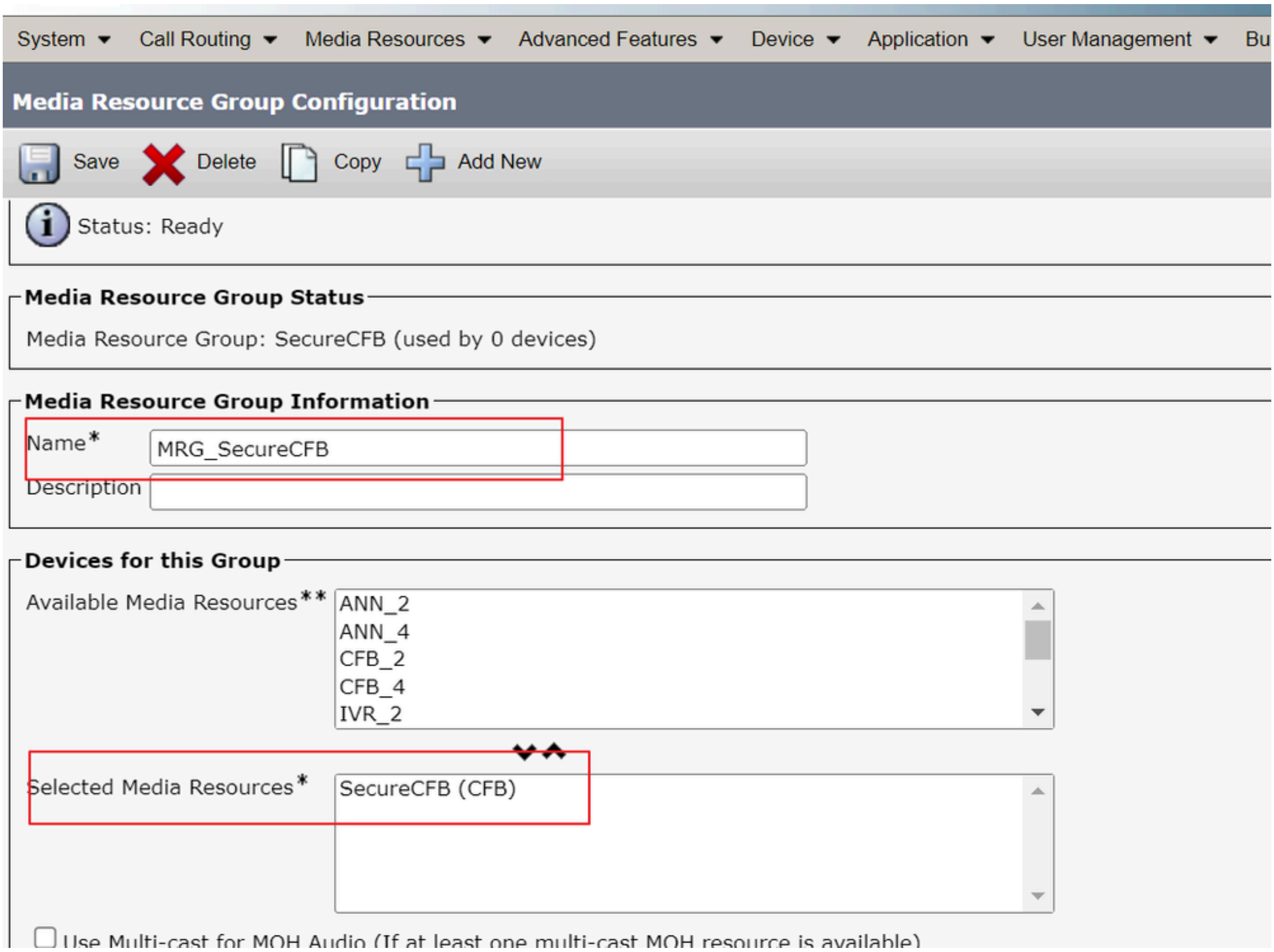
IP电话在Admin settings > Security Setup下显示Security mode with Encrypted。



安全模式已加密

任务3.使用安全会议网桥配置媒体资源组列表并将其分配给IP电话。

步骤1:创建媒体资源组MRG_SecureCFB并向其分配SecureCFB(Cisco Unified CM管理>媒体资源>媒体资源组)。



Media Resource Group Configuration

Status: Ready

Media Resource Group Status

Media Resource Group: SecureCFB (used by 0 devices)

Media Resource Group Information

Name* MRG_SecureCFB

Description

Devices for this Group

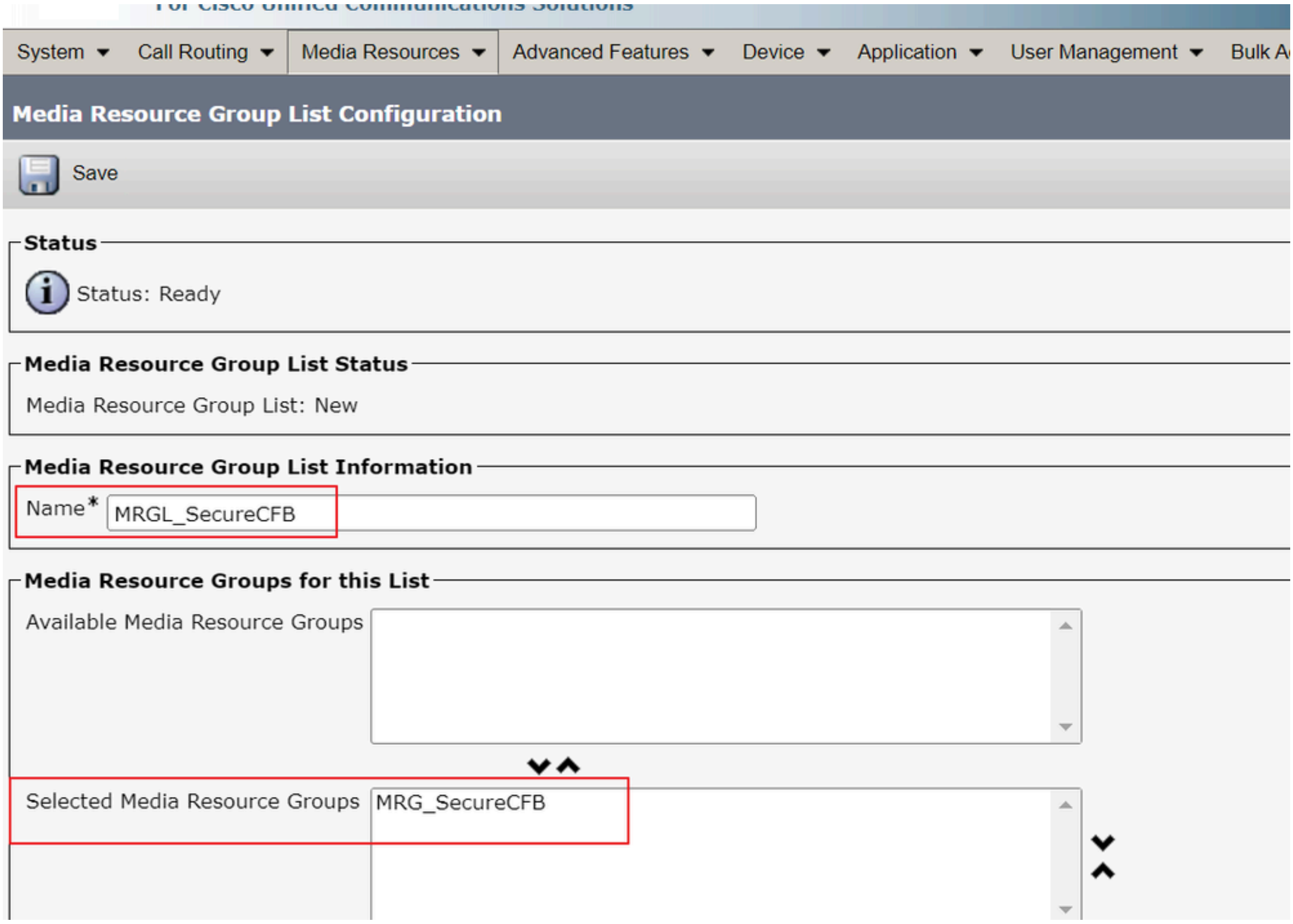
Available Media Resources** ANN_2, ANN_4, CFB_2, CFB_4, IVR_2

Selected Media Resources* SecureCFB (CFB)

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

创建媒体资源组MRG_SecureCFB

第二步：创建媒体资源组列表MRGL_SecureCFB并向其分配MRG_SecureCFB(Cisco Unified CM管理>媒体资源>媒体资源组列表)。



Media Resource Group List Configuration

Status

Status: Ready

Media Resource Group List Status

Media Resource Group List: New

Media Resource Group List Information

Name* MRGL_SecureCFB

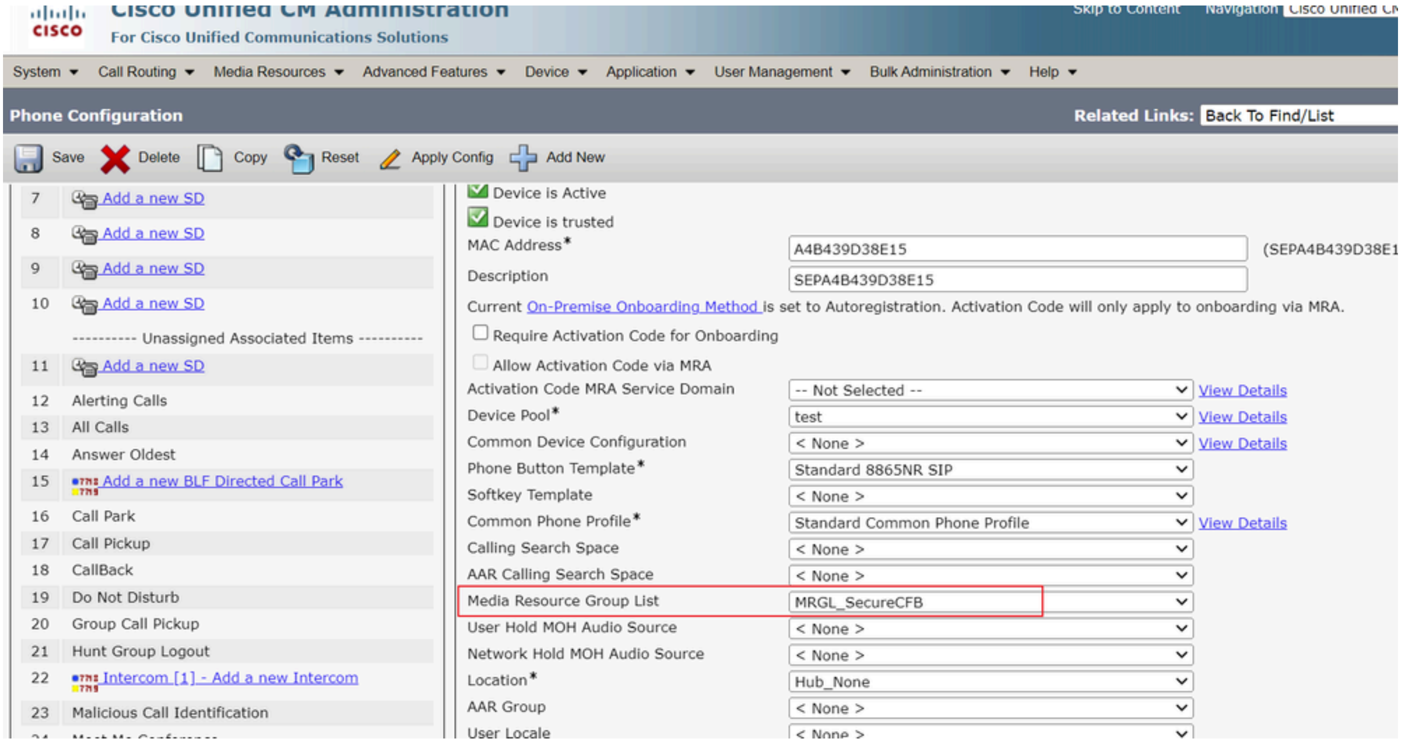
Media Resource Groups for this List

Available Media Resource Groups

Selected Media Resource Groups MRG_SecureCFB

创建媒体资源组列表MRGL_SecureCFB

第三步：将媒体资源组列表MRGL_SecureCFB分配给所有8865NR。



Phone Configuration

7 Add a new SD
8 Add a new SD
9 Add a new SD
10 Add a new SD
---------- Unassigned Associated Items ----------
11 Add a new SD
12 Alerting Calls
13 All Calls
14 Answer Oldest
15 Add a new BLF Directed Call Park
16 Call Park
17 Call Pickup
18 CallBack
19 Do Not Disturb
20 Group Call Pickup
21 Hunt Group Logout
22 Intercom [1] - Add a new Intercom
23 Malicious Call Identification

☑ Device is Active

☑ Device is trusted

MAC Address*	A4B439D38E15 (SEPA4B439D38E1
Description	SEPA4B439D38E15

Current On-Premise Onboarding Method is set to Autoregistration. Activation Code will only apply to onboarding via MRA.

□ Require Activation Code for Onboarding

□ Allow Activation Code via MRA

Activation Code MRA Service Domain	-- Not Selected --
Device Pool*	test
Common Device Configuration	< None >
Phone Button Template*	Standard 8865NR SIP
Softkey Template	< None >
Common Phone Profile*	Standard Common Phone Profile
Calling Search Space	< None >
AAR Calling Search Space	< None >
Media Resource Group List	MRGL_SecureCFB
User Hold MOH Audio Source	< None >
Network Hold MOH Audio Source	< None >
Location*	Hub_None
AAR Group	< None >
User Locale	< None >

分配媒体资源组列表

验证

IP电话1带DN 1001、IP电话2带DN 1002、IP电话3带DN 1003。

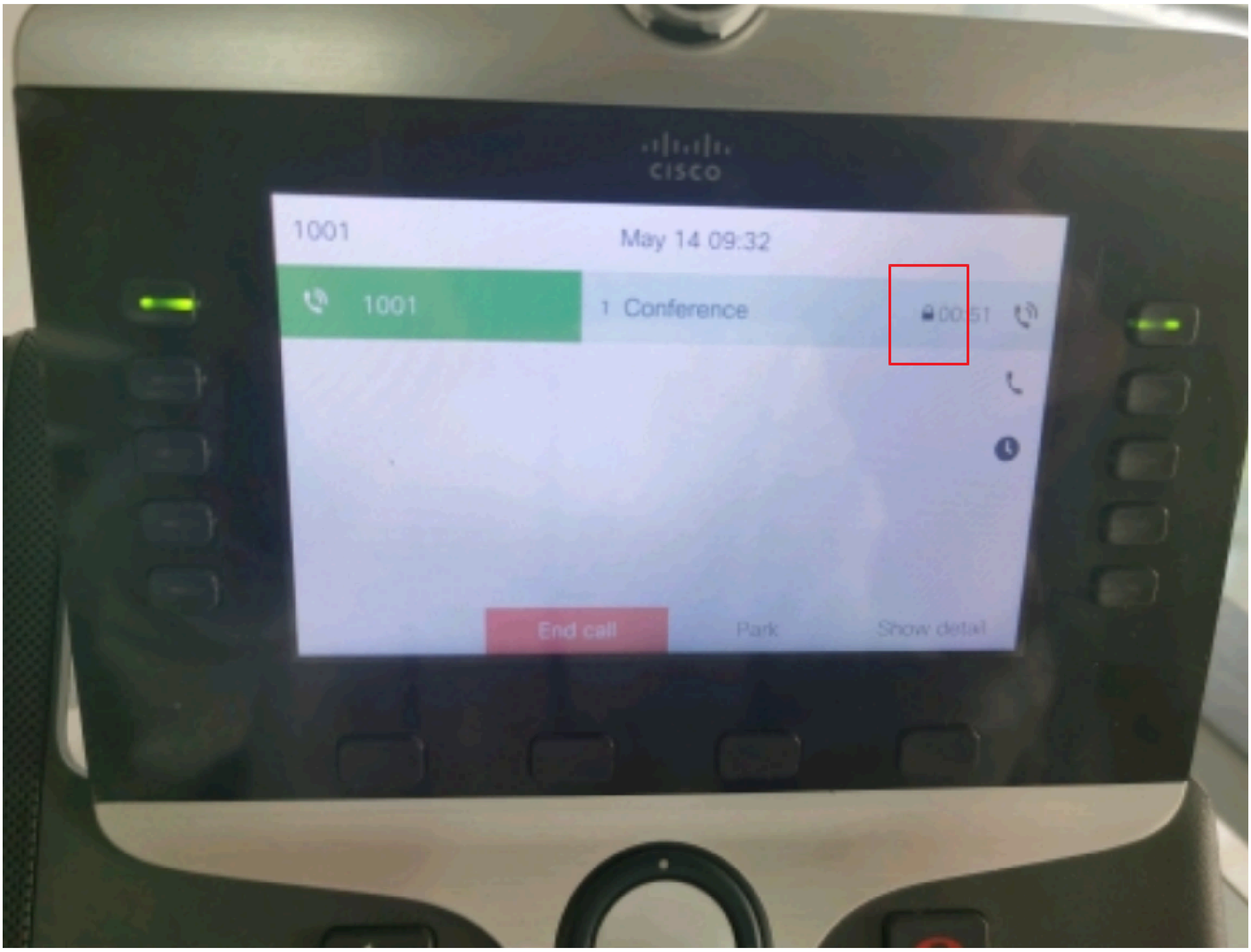
测试步骤。

1. 1001呼叫1002。

2. 1001按会议软键并呼叫1003。

3. 1001新闻发布会软键让安全临时会议参与进来。

Cisco IP电话显示会议安全图标以表示呼叫已加密。



测试调用已加密

故障排除

通过RTMT收集下一个信息。

Cisco CallManager（calllogs提供有关呼叫的信息，sdl文件夹包含CUCM跟踪）。

从SDL跟踪中可以看到，当1001按会议软键向会议1002和1003时，1001会发送SIP REFER消息。

```
00018751.002 |17:53:18.056 | 应用信息  |SIPTcp - wait_SdlReadRsp：从2039字节的端口51320索引7上的x.x.x.x传入的SIP TCP消息：
[587，NET]
请参阅sip：CUCMPUB15 SIP/2.0
通过：SIP/2.0/TLS x.x.x.x：51320；branch=z9hG4bK4d786568
发件人："1001" <sip：1001@x.x.x.x>；tag=a4b439d38e15003872a7c133-28fd5212
收件人：<sip：CUCMPUB15>
呼叫ID：a4b439d3-8e150010-2f865ab1-7160f679@x.x.x.x
会话 ID：b14c8b6f00105000a000a4b439d38e15；remote=00000000000000000000000000000000
日期： 2024年5月14日星期二09:53:17 GMT
CSeq： 1000参考
用户代理：Cisco-CP8865NR/14.2.1
接受：application/x-cisco-remotecc-response+xml
过期时间：60
最大转发数：70
联系人：<sip：8a854224-e17e-93da-8e71-6a2796f28fc7@x.x.x.x:51320；transport=tls>；+u.sip！devicename.ccm.cisco.com="SEPA4B439D38E1
推荐人：“1001”<sip：1001@x.x.x.x>
请参阅：cid：3e94126b@x.x.x.x
内容ID： <3e94126b@x.x.x.x>
允许：ACK、BYE、CANCEL、INVITE、NOTIFY、OPTIONS、REFER、REGISTER、UPDATE、SUBSCRIBE
内容长度：1069
内容类型：application/x-cisco-remotecc-request+xml
Content-Disposition： session；handling=required
<？xml version="1.0" encoding="UTF-8"？>
```

```
<x-cisco-remotecc-request>
  <softkeyeventmsg>
    <softkeyevent>会议</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-remotecc-request>

00018751.003 |17:53:18.056 | 应用信息  |SIPTcp - SignalCounter = 300
```

然后，CUCM执行数字分析，最后路由到设备SecureCFB。

```
00018997.000 |17:53:18.134 |SdlSig   |CcRegisterPartyB                   |tcc_register_party_b
|Cdcc(1,100,39,7)               |Cc(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名称： 4
Unicode名称： pi： 0 encodeType=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.MRGLPkid= MOH.userHoldID=0
MOH.netHoldID=0 MOH.supp=1 devName=SECURECFBmobileDev Name=
origEMCCCallingDevName= 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： BFCPAllowed=F
IXAllowed=F devCap=0 CryptoCapCount=6 secure=3 loginId= UnicodeName：
retriedVideo=FFromTag=ToTag=CallId= UAPortFlag=F wantDTMFRecep=1 provOOB=0 supp
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=nullPkid= locName=
deductBW=FateShareId=
videoTrafficClass=UnspecientbridgeParticipantParticipantBridgeParticipant ID callingUsr=
remoteClusterID= isEMCCDevice=F dtmCall=F dtmPrimaryCI=0 dtmMediaIFPid=(0,0，0,0)
dtmMcNodeId=0 dtmMTPForDTMFTranslation=F emc=T QSIGIMERoute=Eo=0 eoUpdt=1
vCTCUpdt=1 honorFowor荣誉升级=1Final calledPartition= cTypeUpdt=0 BibEnabled=0
RecordingQSIGAPDUSupported=F FarEndDeviceName=LatentCaps=null icidVal= icidGenAddr=
oioi= tioi= ptParams= CAL={v=-1， m=-1， tDev=F， res=F， devType=0}
displayNameUpdateFieldFlag=0 CFBCtrlSecIcon=FBeforeAnn F外部演示信息[ pi=0si1locale：
1名称： Unicode名称： pi： 0 mIsCallExternal=F ] ControlProcessType=0
controlProcessTypeUpdateFieldFlag=1 origPi=0
```

相关信息

- https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/security/15_0/cucm_b_security-guide-release-15.pdf
- 思科技术支持和下载

注意：Unified Communications Manager支持集群内中继(ICT)、H.323中继/网关和MGCP网关上的安全会议；但是，运行版本8.2或更早版本的加密电话将恢复到ICT和H.323呼叫的RTP，并且媒体不会加密。如果会议涉及SIP中继，则安全会议状态为非安全。此外，SIP中继信令不支持向集群外的参与者发送安全会议通知。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。