

CUCMでのセキュアなアドホック会議の設定15

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

はじめに

このドキュメントでは、CUCM 15でのセキュアなアドホック会議の設定について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- CUCM
- VG (音声ゲートウェイ)
- セキュリティの概念

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- CUCM (混合モード) バージョン : 15.0.0.98100-196
- CISCO2921バージョン : 15.7(3)M4b (CAおよびセキュア会議ブリッジとして使用)
- NTP サーバ
- 3 8865NR IP電話

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

タスク 1.セキュア会議ブリッジを設定し、CUCMに登録します。

ステップ 1 : 公開キーインフラストラクチャサーバとトラストポイントを設定します。

ステップ 1.1 : NTPサーバとHTTPサーバを設定します。

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

ステップ 1.2 : 公開キーインフラストラクチャサーバを設定します。

```
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
```

ステップ 1.3 : testCAのトラストポイントを設定します。

```
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
```

ステップ 1.4 : 30秒ほど待機してから、no shutdownコマンドを発行して、testCAサーバを有効にします。

```
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.
```

ステップ 2 : セキュア会議ブリッジのトラストポイントを設定し、testCAに登録します。

ステップ 2.1 : セキュアな会議ブリッジのトラストポイントを設定し、SecureCFBという名前を付けます。

```
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
```

ステップ 2.2 : SecureCFBを認証し、「yes」と入力して証明書を受け入れます。

```
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.
```

ステップ 2.3 : SecureCFBを登録し、パスワードを設定します。

```
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.
```

ステップ 3 : セキュアコンファレンスブリッジでのCUCMのトラストポイントの設定

ステップ 3.1 : CUCMからCallManager証明書をダウンロードし、pemファイル(Cisco Unified OS Administration >セキュリティ>証明書管理)をコピーします。

The screenshot shows the Cisco Unified Operating System Administration interface. The top navigation bar includes 'Show', 'Settings', 'Security', 'Software Upgrades', 'Services', and 'Help'. The main content area is titled 'Certificate List' and features several action buttons: 'Generate Self-signed', 'Upload Certificate/Certificate chain', 'Download CTL', 'Generate CSR', and 'Reuse Certificate'. Below these is a 'Status' section indicating '42 records found'. A table of certificates is displayed, with the first row highlighted in red:

Certificate	Common Name/Common Name_SerialNumber
CallManager	CUCMPUB15.uc.com_610028ab5938cc7f750ce00ce87830cd
CallManager-ECDSA	CUCMPUB15-EC.uc.com_6d3fb0e8a5dd696ec3a09b710385f052
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_61096e7d000000000000c
CallManager-trust	CUCSUB15.uc.com_54d2204dc0aab6ea71b13f11a736ef3a
CallManager-trust	CUCPUB15-EC.uc.com_6b5fc677355e1202298681907f1fde2
CallManager-trust	Cisco_Basic_Assurance_Root_CA_2099_01a65af15ee9944e1
CallManager-trust	CAPF-6eb54dd8
CallManager-trust	cuc15pub.dltaclab.com_459213e7b3bd797cd027446fa45c9631
CallManager-trust	High_Assurance_SUDI_CA_0a6475524cd8617c62

To the right, a 'Certificate Details for CUCMPUB15.uc.com, CallManager' dialog box is open. It shows the 'Status' as 'Ready' and 'Certificate Settings' including 'File Name: CallManager.pem', 'Certificate Purpose: CallManager', 'Certificate Type: certs', 'Certificate Group: product-cm', and 'Description: Self-signed certificate generated by system'. The 'Certificate File Data' section displays the following details:

```

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:

```

At the bottom of the dialog, there are buttons for 'Regenerate', 'Generate CSR', 'Download .PEM File', and 'Download .DER File'. The 'Download .PEM File' button is highlighted with a red box.

CallManager証明書のダウンロード

ステップ 3.2 : トラストポイントを設定し、pemファイルを貼り付け、証明書を受け入れるようにyesと入力します。

```

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
MQswCQYDVQQGEwJDTjEOMAwGA1UECgwFY2lzY28xCjAIBGNVBAAsMAWExGTAXBgNV
BAMMEENVQ01QVUlxNS51Yy5jb20xCjAIBGNVBAgMAWMxMjA1WjBcMQswCQYDVQQGEwJDTjEOMAwG
A1UECgwFY2lzY28xCjAIBGNVBAAsMAWExGTAXBgNVBAAMMEENVQ01QVUlxNS51Yy5j
b20xCjAIBGNVBAgMAWMxMjA1WjBcMQswCQYDVQQGEwJDTjEOMAwGA1UECgwFY2lzY28x
CjAIBGNVBAgMAWMwggEiMA0GCSqGSIb3DQEBAQUAA4IB
DwAwggEKAAoIBAQD4XfdI9MwY/bSDXzGjtd301vYqKdRpqVYpWD7E+NrH7zRgHhz+
M7gAeqdRCSC/iKUF2g44rCRjIM0C/9xN3pxvOnNequg/Tv0wjPm0X2O4x0daH+F
AwElWNYZZvUQ6+2xtkTuUcqexDnnbS6fLladP/CfgQwKX5U1Ec575ypUet6Fp2n2
4UouLQ5iFEMmX9gzGR7YKjeE+t61X5NmvYc6lyP8MH77sgvti7+xJurJJUnvBFG2
ELXM0rL7uUoqw/rjMT6XxK+0Ft4bkOsVnjl+vOUUBUoTcbFFrsfrConVQjPhHue
MLAaRzkDo5p1xo+UnNgv2uSH9HAID/NS1VTDAgMBAAGjYTBfMAsGA1UdDwQEAwIC

```

```
tDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAWIwHQYDVR0OBBYEFKriBeQi
OF6Hp0QCufVYzKWiXx2hMBIGA1UdEwEB/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

ステップ 4 : セキュアな会議ブリッジを信頼するようにCUCMを設定します。

ステップ 4.1 : 汎用証明書をコピーし、SecureCFB.pemファイルとして保存します。CA証明書をコピーし、testCA.pemファイルとして保存します。

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

```
% CA certificate:
```

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

```
MIIIB+zCAAwSgAwIBAgIBATANBgkqhkiG9w0BAQQFADARMQ8wDQYDVQQDEwZ0ZXN0
Q0EwHhcNMjQwNTEwMDg0NDI3WWhcNMjcwNTEwMDg0NDI3WjARMQ8wDQYDVQQDEwZ0
ZXN0Q0EwGz8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAM2Lqils9nddFOx/YN7y
hhp9KGI2Eb8Zxq9E2mXfKpHOpbcGEic5ain+rXf1qauA8/pNYwvBurAZm2pWzFHQ
q4qGL8KWDwJCPTwPI5rJOJAMiYzMH4WdQerWP4iEI2LGtxCb1q8b3w0wJE0Q2OG4
4kDSeArkKe0cb26WZC1oVK1jAgMBAAGjYzBhMA8GA1UdEwEB/wQFMAMBAf8wDgYD
VR0PAQH/BAQDAGGMB8GA1UdIwQYMBaAFJOFqPH+VBcd01d9SzcPhNkWGqcWMB0G
A1UdDgQWBBSThaxj/IQXHdNXfUswqYTZFhqnFjANBgkqhkiG9w0BAQQFAAOBQAS
V8x9QjJ5pZKmezDYvxPDFe4chlKCD7o8JOcutSdAi7H+2Z+GO4CF55EDTZdLZPtn
GwQ01gbtDX07PTroYRWOSZLSJSdPQITJ3WDNR+NBhZjfe6EzfsLasD8L0VYG96GX
vjRQbdRmqbrG5H0ZUUz0cu93AXjnRI2nLoAkKcrjcQ==
-----END CERTIFICATE-----
```



```
% General Purpose Certificate:
```

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

```
MIIIB6jCCAVOGAwIBAgIBAjANBgkqhkiG9w0BAQUFADARMQ8wDQYDVQQDEwZ0ZXN0
Q0EwHhcNMjQwNTEwMDg1NTA4WWhcNMjcwNTEwMDg0NDI3WjAUMRIwEAYDVQQDEwIT
ZWN1cmVDRklwZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALhk11yOPnUNTjEQ
JLJIMPnoc6Zb9vDrGollMdsz/czWKTiGCS9PYYxwcPBExOOR+XrE9MmEO7L/tr6n
NkKz84ddWNz0gg6wHWM9gcje22blsleU6UCxo4ovra2pExXphusqEmg5yLQwyeJc
5JqcoAYXuRpnKLTfn5Nnh6iUCsWrAgMBAAGjTzBNMAsGA1UdDwQEAwIFoDAfBgNV
HSMEGDAWgBSThaxj/IQXHdNXfUswqYTZFhqnFjAdBgNVHQ4EFgQU3y9zfDoTJ8WV
XlpX3wdcieq1zpkwDQYJKoZIhvcNAQEFBQADgYEABfaa6ppqRaDyfpW/tu5pXBRHP
SfZzpv+4ktsjAiOG7oGJGT0RpnuikCq+V2oucJbtWWAPbvX+ZBG3Eogi1c2GoDLK
yYvuaf9zBJHicM5mv6x81qxLF7FKZaepQSYwsQUP50/uKXa0435Kj/CzoLpKhXR2
v/p2jzF9zyPIBuQGEOEo=
-----END CERTIFICATE-----
```

ステップ 4.2 : SecureCFB.pemをCUCMのCallManager-trustストアにアップロードします(Cisco Unified OS Administration > Security > Certificate Management)。

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.

SecureCFB.pemのアップロード

ステップ 5 : VGでのセキュア会議ブリッジの設定

```
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
```

手順 6 : CUCMでセキュアな会議ブリッジを設定します(Cisco Unified CM Administration >メディアリソース>会議ブリッジ>新規追加)。



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*
 Device is trusted
Conference Bridge Name*
Description
Device Pool*
Common Device Configuration
Location*
Device Security Mode*
Use Trusted Relay Point*

セキュアな会議ブリッジの設定

タスク 2. セキュリティモードで3 8865NR IP Phoneを登録します。

IP Phoneでデバイスセキュリティプロファイルを暗号化モードに設定します。

Protocol Specific Information

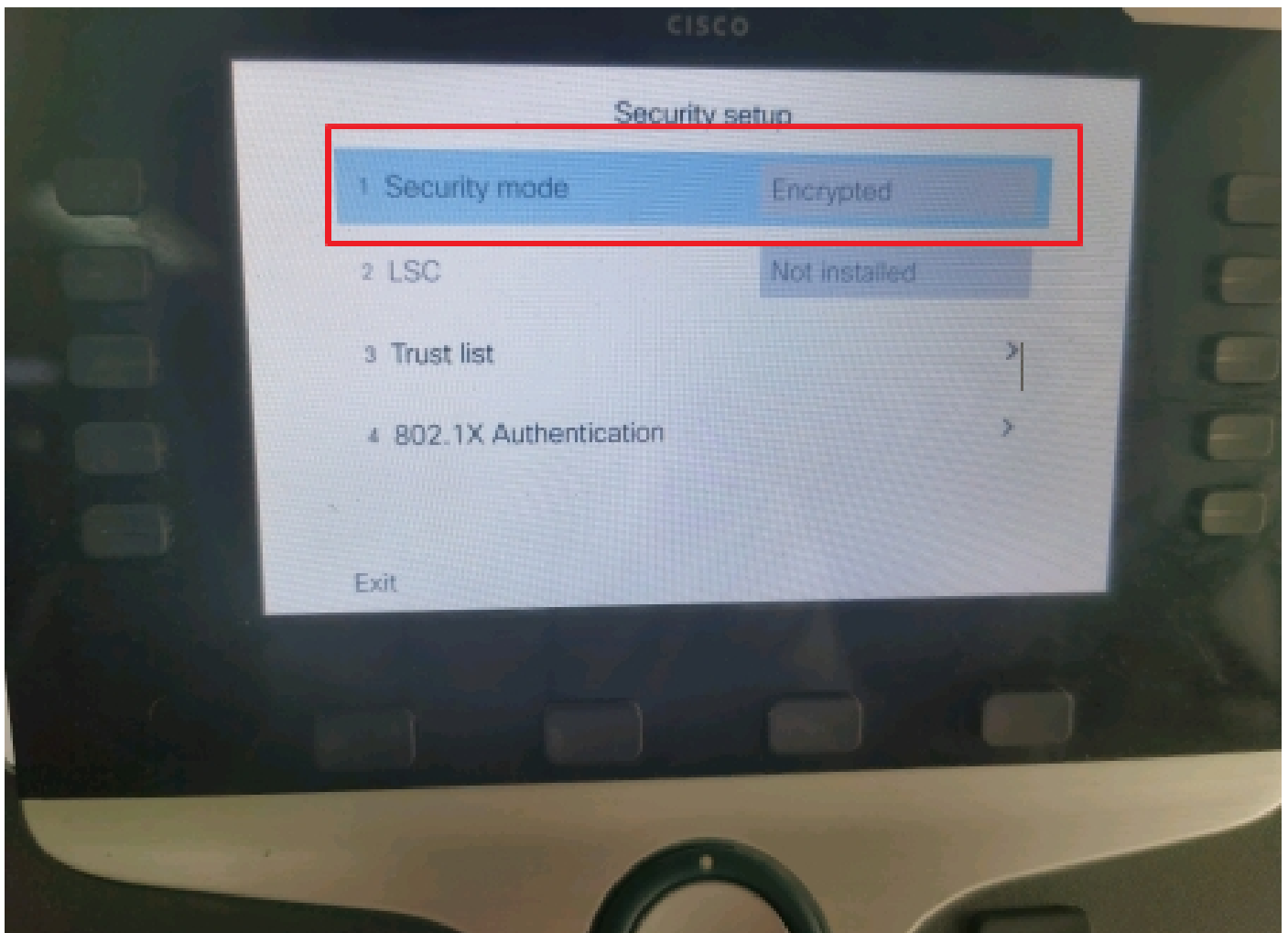
Packet Capture Mode*
Packet Capture Duration
BLF Presence Group*
SIP Dial Rules
MTP Preferred Originating Codec*

Rerouting Calling Search Space
SUBSCRIBE Calling Search Space
SIP Profile* [View Details](#)
Digest User
 Media Termination Point Required
 Unattended Port
 Require DTMF Reception

デバイスセキュリティプロファイルを暗号化モードに設定

Admin Settings > Security Setupで、IP Phoneに「Security mode with Encrypted」と表示されま

す。




セキュリティモードは暗号化されました

タスク 3.メディアリソースグループリストにセキュアな会議ブリッジを設定し、それをIP Phoneに割り当てます。

ステップ 1 : メディアリソースグループMRG_SecureCFBを作成し、それにSecureCFBを割り当てます(Cisco Unified CM Administration > Media Resources > Media Resources Group)。

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**
ANN_2
ANN_4
CFB_2
CFB_4
IVR_2

Selected Media Resources*

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

メディアリソースグループMRG_SecureCFBの作成

ステップ 2 : メディアリソースグループリストMRGL_SecureCFBを作成し、それにMRG_SecureCFBを割り当てます(Cisco Unified CM Administration > Media Resources > Media Resources Group List)。

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

メディアリソースグループリストMRGL_SecureCFBの作成

ステップ 3 : メディアリソースグループリストMRGL_SecureCFBをすべての8865NRに割り当てます。

CISCO United CM Administration For Cisco Unified Communications Solutions

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 >"/>
		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 >"/>

メディアリソースグループリストの割り当て

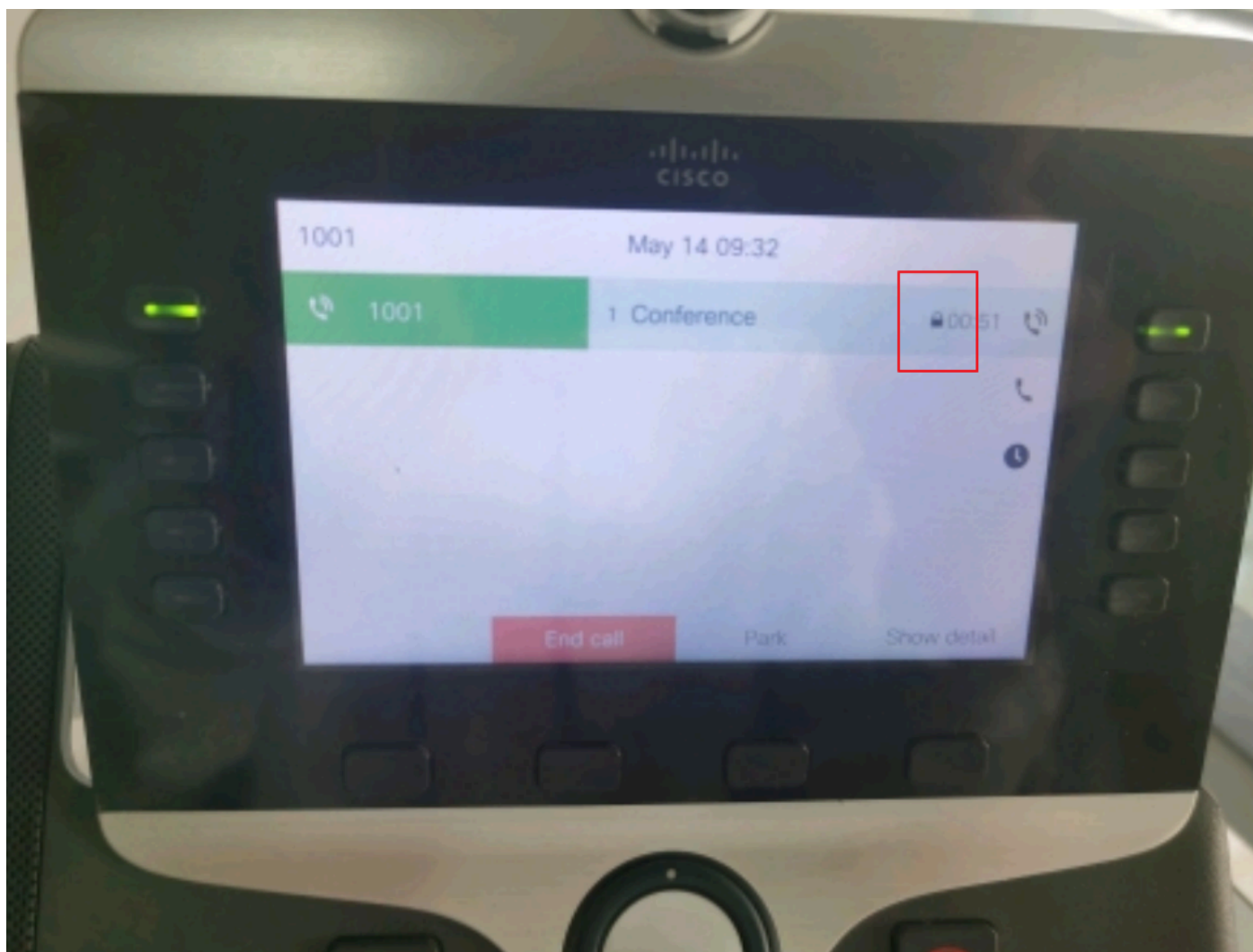
確認

IP Phone 1はDN 1001で、IP Phone 2はDN 1002で、IP Phone 3はDN 1003です。

テスト手順。

1. 1001から1002にコールします。
2. 1001会議ソフトキーを押して、1003に発信します。
3. 1001 Secure Ad Hoc Conferenceを含めるには、会議ソフトキーを押します。

Cisco IP Phoneには、コールが暗号化されたことを示す会議セキュリティアイコンが表示されます。



テストコールは暗号化されました

トラブルシュート

RTMTを介して次の情報を収集します。

Cisco CallManager (コールログはコールに関する情報を提供し、sdlフォルダにはCUCMトレースが含まれます)。

SDLトレースから、1001が会議ソフトキーを会議1002と会議1003に押すと、1001がSIP REFERメッセージを送信することがわかります。

00018751.002 |17:53:18.056 |アプリ情報 |SIPTcp - wait_SdlReadRsp: x.x.x.xからの着信SIP TCPメッセージ(ポート51320インデックス7、2039バイト):

[587 , ネット]

SIP:CUCMPUB15 SIP/2.0を参照

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

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

宛先 : <sip:CUCMPUB15>

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

セッション

ID:b14c8b6f00105000a000a4b439d38e15;remote=00000000000000000000000000000000

日付 : 2024年5月14日 (火) 09:53:17 GMT

CSeq:1000参照

ユーザエージェント : Cisco-CP8865NR/14.2.1

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

有効期限 : 60

最大転送数 : 70

連絡先 : <sip:8a854224-e17e-93da-8e71-6a2796f28fc7@x.x.x.x:51320;transport=tls>;+u.sip!devicename.ccm.cisco.com="SEPA4B439D38E15"

Referred-By: "1001" <sip:1001@x.x.x.x>

参照先 : cid:3e94126b@x.x.x.x

コンテンツId: <3e94126b@x.x.x.x>

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

コンテンツ長 : 1069

コンテンツタイプ : application/x-cisco-remotecc-request+xml

Content-Disposition : セッション ; 処理=必須

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

<x-cisco-remotecc-request>

<ソフトキーイベントメッセージ>

<softkeyevent>会議</softkeyevent>

<ダイヤルID>

<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>

<コンサルトディアログID>

<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>

<結合ディメンションid>

<callid></callid>

<localtag></localtag>

<remotetag></remotetag>

</joindialogid>

<イベントデータ>

<invocationtype>明示的</invocationtype>

</eventdata>

<userdata></userdata>

<softkeyid>0</softkeyid>

<applicationid>0</applicationid>

</softkeyeventmsg>

</x-cisco-remotecc-request>

00018751.003 |17:53:18.056 |アプリ情報 |SIPTcp - SignalCounter = 300

その後、CUCMは番号分析を行い、最終的にデバイスSecureCFBにルーティングします。

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 Name: 4 UnicodeName: pi: 0
encodeType=10 qsig-encodeType=10 ConnType 3 XferMode=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 Name=SECUREFB mobileDevName=
origEMCCallingDevName= mobilePartyNumber=pi=0si1 mobileCallType=0 ctiActive=F
ctiFarEndDev=1 ctiCCMId=1 devCepn=38281c14-d78f-46d6-8199-63297bcfdcae lineCepn=
activeCaps=0 VideoCall MMUpdateCapMask=0x3e MMCap=0x1 SipConfig: BFCPAllowed=F
IXAllowed=F devCap=0 CryptoCapCount=6 secure=3 loginId= UnicodeName:
retriedVideo=FFromTag=ToTag=CallId= UAPortFlag=FwantDTMFRecep=1 provOOB=p dtmf=1
DTMF Cfg=1 DTMF PT=() DTMF reqMed=1 isPrefAltScript=F cdpnPatternUsage=2 audioPtyId=0
doNotAppendLineCSS=F callingDP= BCUpdate=0 ccBearCap.itc=0 ccBearCap.l=0
ccBearCap.itr=0 protected=1flushCapIns=0 geoloc info=null locPkid= locName= deductBW=F
fateShareId= videoTrafficClass=Unspecified bridgeParticipantID callingUsr= remoteClusterID=
isEMCCDevice=F dtmCall=F dtmPrimaryCI=0 dtmMediaFPid=(0,0,0,0) dtmMcNodeId=0
dtmMTPForDTMFTRanATION=SIATION F EMC=T QSIGIMERoute=F eo=0 eoUpdt=1
vCTCUpdt=1 honorCodec=F honorUpdt=1 finalCalledPartition= cTypeUpdt=0 BibEnabled=0
RecordingQSIGAPDUSupported=F FarEndDeviceName=PotentialCaps=null icidVal=
icidGenAddr= oi= ptParams={CAL= -1, M=-1, TDev=F, RES=F, DEVType=0}
DISPLAYNameUpdateFieldFlag=0 CFBCtrlSecICon=F connBeforeANN=F外部プレゼンテーショ
ン情報[pi=0si1locale: 1名前 : UnicodeName: pi: 0 mlsCallExternal=F] ControlProcessType=0
controlProcessTypeUpdateFieldFlag=1 origPi=0

関連情報

- https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/security/15_0/cucm_b_security-guide-release-15.pdf
- [シスコのテクニカルサポートとダウンロード](#)



注：トランクおよびゲートウェイ経由のセキュアな会議Unified Communications Managerは、クラスタ内トランク(CT)、H.323トランク/ゲートウェイ、およびMGCPゲートウェイ経由のセキュアな会議をサポートしています。ただし、リリース8.2以前を実行している暗号化された電話機は、CTおよびH.323コールのRTPに戻り、メディアは暗号化されません。会議にSIPトランクが含まれている場合、セキュアな会議のステータスは非セキュアになります。また、SIPトランクシグナリングでは、クラスタ外の参加者に対するセキュアな会議通知はサポートされていません。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。