

Configurer une conférence ad hoc sécurisée sur CUCM 15

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configurer](#)

[Vérifier](#)

[Dépannage](#)

[Informations connexes](#)

Introduction

Ce document décrit la configuration de la conférence ad hoc sécurisée sur CUCM 15.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- CUCM
- VG (Voice Gateway)
- Concept de sécurité

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- CUCM (mode mix) version : 15.0.0.98100-196
- CISCO2921 version : 15.7(3)M4b (à utiliser comme CA et pont de conférence sécurisé)
- Serveur NTP
- Téléphone IP 3 8865NR

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configurer

Tâche 1. Configurez Secure Conference Bridge et inscrivez-vous à CUCM.

Étape 1. Configurez le serveur d'infrastructure à clé publique et le point de confiance.

Étape 1.1. Configurez le serveur NTP et le serveur HTTP.

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

Étape 1.2. Configurez le serveur d'infrastructure à clé publique.

```
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
```

Étape 1.3. Configurez le point de confiance pour testCA.

```
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
```

Étape 1.4. Attendez environ 30 secondes, puis émettez la commande no shutdown afin d'activer le serveur testCA.

```
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.
```

Étape 2. Configurez le point de confiance pour le pont de conférence sécurisé et enregistrez-le auprès de testCA.

Étape 2.1. Configurez le point de confiance pour le pont de conférence sécurisé et nommez-le

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
```

Étape 2.2. Authentifiez SecureCFB et tapez « yes » pour accepter le certificat.

```
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.
```

Étape 2.3. Inscrivez SecureCFB et définissez un mot de passe.

```
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.
```

Étape 3. Configurez le point de confiance pour CUCM sur Secure Concerence Bridge.

Étape 3.1. Téléchargez le certificat CallManager depuis CUCM et copiez le fichier pem (Administration de Cisco Unified OS > Sécurité > Gestion des certificats).

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

Status
42 records found

Certificate List (1 - 42 of 42)

Find Certificate List where Certificate begins with

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

Certificate Details for CUCMPUB15.uc.com, CallManager

Regenerate Generate CSR Download .PEM File Download .DER File

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:

Regenerate Generate CSR **Download .PEM File** Download .DER File

Close

Télécharger le certificat CallManager

Étape 3.2. Configurez le point de confiance, collez le fichier pem, et tapez yes afin d'accepter le certificat.

```
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
MQswCQYDVQQGEwJDTjEOMAwGA1UECgwFY2lzY28xY28xY28xY28xY28xY28xY28x
BAMMEENVQ01QVUlxNS51Yy5jb20xY28xY28xY28xY28xY28xY28xY28xY28xY28x
MjMwOTA4MTAxNTA2WHhcnMjMwOTA4MTAxNTA2WHhcnMjMwOTA4MTAxNTA2WHhcnMj
A1UECgwFY2lzY28xY28xY28xY28xY28xY28xY28xY28xY28xY28xY28xY28xY28x
b20xY28xY28xY28xY28xY28xY28xY28xY28xY28xY28xY28xY28xY28xY28xY28x
DwAwggEKAoIBAQAQD4XfdI9MwY/bSDXzGjtd301vYqKdRqVYpWD7E+Nrh7zRgHhz+
M7gAeqdRCSC/iKUF2g44rCRjIM0C/9xN3pxvOnNeqg/Tv0wjpHm0X2O4x0daH+F
AwEIWNyZzVUQ6+2xtkTuUcqeXDnnbS6fLladP/CfgQwKX5U1Ec575ypUet6Fp2n2
4UouLQ5iFEMmX9gzGR7YKjeE+t61X5NmvYc6lyP8MH77sgvti7+xJurJJUnvBFG2
ELXM0rL7uUoqw/rjMT6XxK+0Ft4bkOsVnjl+vOUUBUoTcbFFrsfrOnVQjPjHue
MLAaRzkDo5p1xo+UnNgv2uSH9HAID/NS1VTDAGMBAAGjYTBfMAsGA1UdDwQEAwIC
```

```
tDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAWlwHQYDVR0OBBYEFKriBeQi
OF6Hp0QCUfVYzKWix2hMBIGA1UdEwEB/wQIMAYBAf8CAQAwDQYJKoZIhvcNAQEL
BQADggEBAJSw2vOwJ4UatmkaFpeLc9B1YZr8X6BkxBY1skW2qOLps61ysjDG61VQ
GjxpPLMY1ISyIvR5dqGyjaGLCUDUUcu66zEPxFNGnSYimBBhGR6NrDyo4YjOk+S
1I3TfRK+2F9NMhW2xTvuygoXLtyibvrZULhNo3vDPYQdTe1z54oQNU4BD8P+MCq9
+MzltCXEpVU6Jp71zC5HY+GF+Ab/xKBNzDjyY+OT8BFiO2wC8aaEaBvByNRzCSPD
MpU5cRaKvip2pszoR9mG3Rls4CkK93OX/OzFqklemDmY5WcylcCsybxAMbjdBDY9
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

Étape 4. Configurez CUCM afin d'approuver le pont de conférence sécurisé.

Étape 4.1. Copiez le certificat à usage général et enregistrez-le dans un fichier SecureCFB.pem. Copiez le certificat CA et enregistrez-le en tant que fichier testCA.pem.

```
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/IQXHdNXfUswqYTZFhqnFjANBgkqhkiG9w0BAQQFAAOBgQAS
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-----
```

Étape 4.2. Téléchargez SecureCFB.pem vers le magasin de confiance CallManager sur CUCM (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.

[Télécharger SecureCFB.pem](#)

Étape 5. Configurer le pont de conférence sécurisé sur VG.

```
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
```

Étape 6. Configurer le pont de conférence sécurisé sur CUCM (Administration Cisco Unified CM > Ressources multimédias > Pont de conférence > Ajouter nouveau).

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

Configurer le pont de conférence sécurisé

Tâche 2. Enregistrez 3 téléphones IP 8865NR en mode de sécurité.

Définissez le profil de sécurité du périphérique en mode Chiffré sur le téléphone IP.

Protocol Specific Information

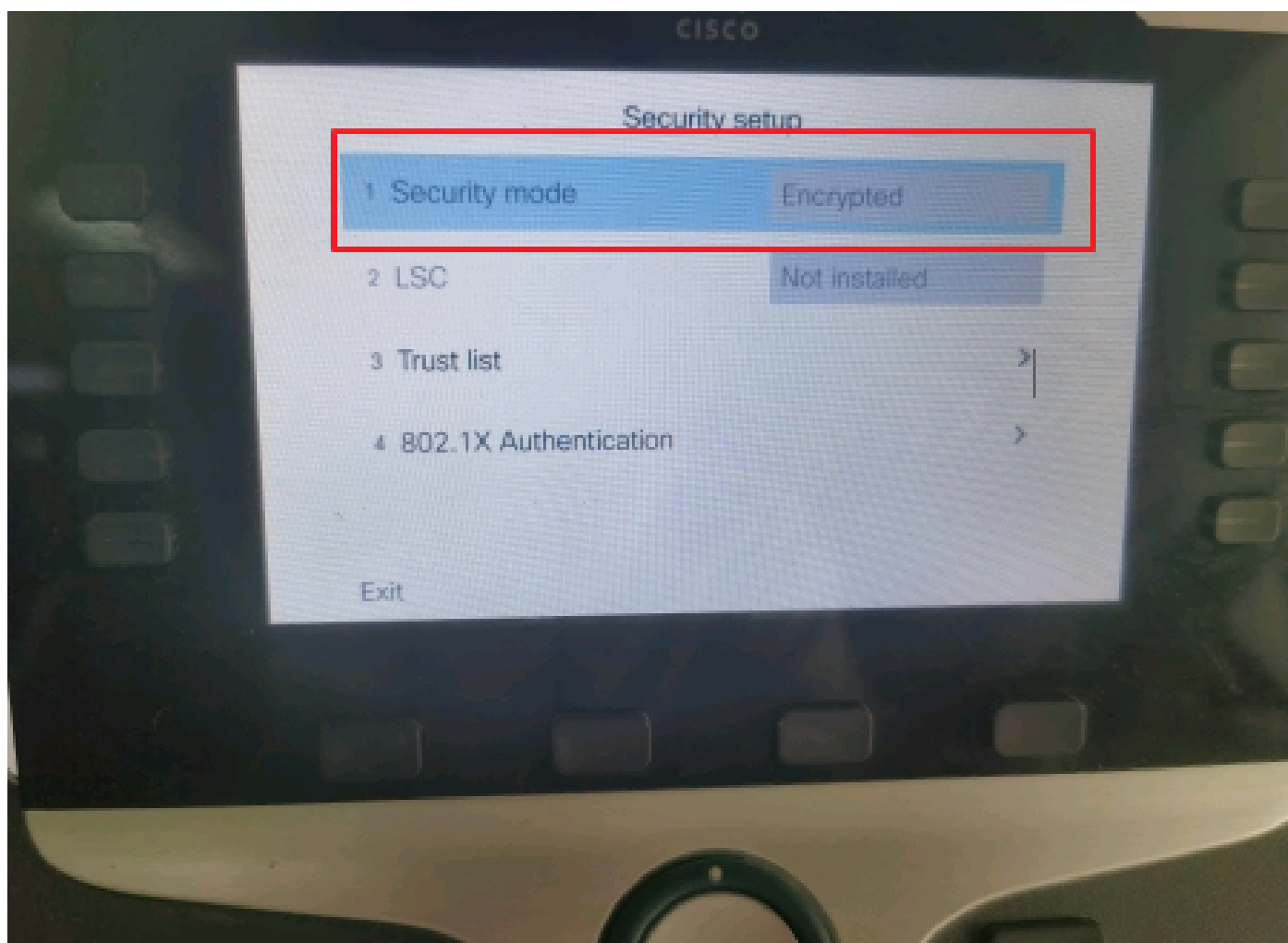
Packet Capture Mode* None ▾
 Packet Capture Duration 0
 BLF Presence Group* Standard Presence group ▾
 SIP Dial Rules < None > ▾
 MTP Preferred Originating Codec* 711ulaw ▾
Device Security Profile* Universal Device Template - Security Profile - Encryl ▾
 Rerouting Calling Search Space < None > ▾
 SUBSCRIBE Calling Search Space < None > ▾
 SIP Profile* < None > ▾ [View Details](#)
 Digest User < None > ▾

Media Termination Point Required
 Unattended Port
 Require DTMF Reception

Définir le profil de sécurité du périphérique en mode Chiffré

Le téléphone IP affiche le mode de sécurité avec crypté sous Paramètres admin > Configuration

de la sécurité.




Le mode de sécurité était Chiffré

Tâche 3. Configurez la liste des groupes de ressources multimédias avec le pont de conférence sécurisé et attribuez-la aux téléphones IP.

Étape 1. Créez un groupe de ressources multimédias MRG_SecureCFB et attribuez-lui SecureCFB (Administration Cisco Unified CM > Ressources multimédias > Groupe de ressources multimédias).

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)

Créer un groupe de ressources multimédias MRG_SecureCFB

Étape 2. Créez une liste de groupes de ressources multimédias MRGL_SecureCFB et attribuez-lui MRG_SecureCFB (Administration Cisco Unified CM > Ressources multimédias > Liste de groupes de ressources multimédias).

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

Créer une liste de groupes de ressources multimédias MRGL_SecureCFB

Étape 3. Attribuez la liste des groupes de ressources multimédias MRGL_SecureCFB à tous les 8865NR.

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	<input type="checkbox"/> Require Activation Code for Onboarding
12	Alerting Calls	<input type="checkbox"/> Allow Activation Code via MRA
13	All Calls	Activation Code MRA Service Domain <input type="text" value="-- Not Selected --"/> View Details
14	Answer Oldest	Device Pool* <input type="text" value="test"/> View Details
15	Add a new BLF Directed Call Park	Common Device Configuration <input type="text" value="< None >"/> View Details
16	Call Park	Phone Button Template* <input type="text" value="Standard 8865NR SIP"/>
17	Call Pickup	Softkey Template <input type="text" value="< None >"/>
18	CallBack	Common Phone Profile* <input type="text" value="Standard Common Phone Profile"/> View Details
19	Do Not Disturb	Calling Search Space <input type="text" value="< None >"/>
20	Group Call Pickup	AAR Calling Search Space <input type="text" value="< None >"/>
21	Hunt Group Logout	Media Resource Group List <input type="text" value="MRGL_SecureCFB"/>
22	Intercom [1] - Add a new Intercom	User Hold MOH Audio Source <input type="text" value="< None >"/>
23	Malicious Call Identification	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 >"/>

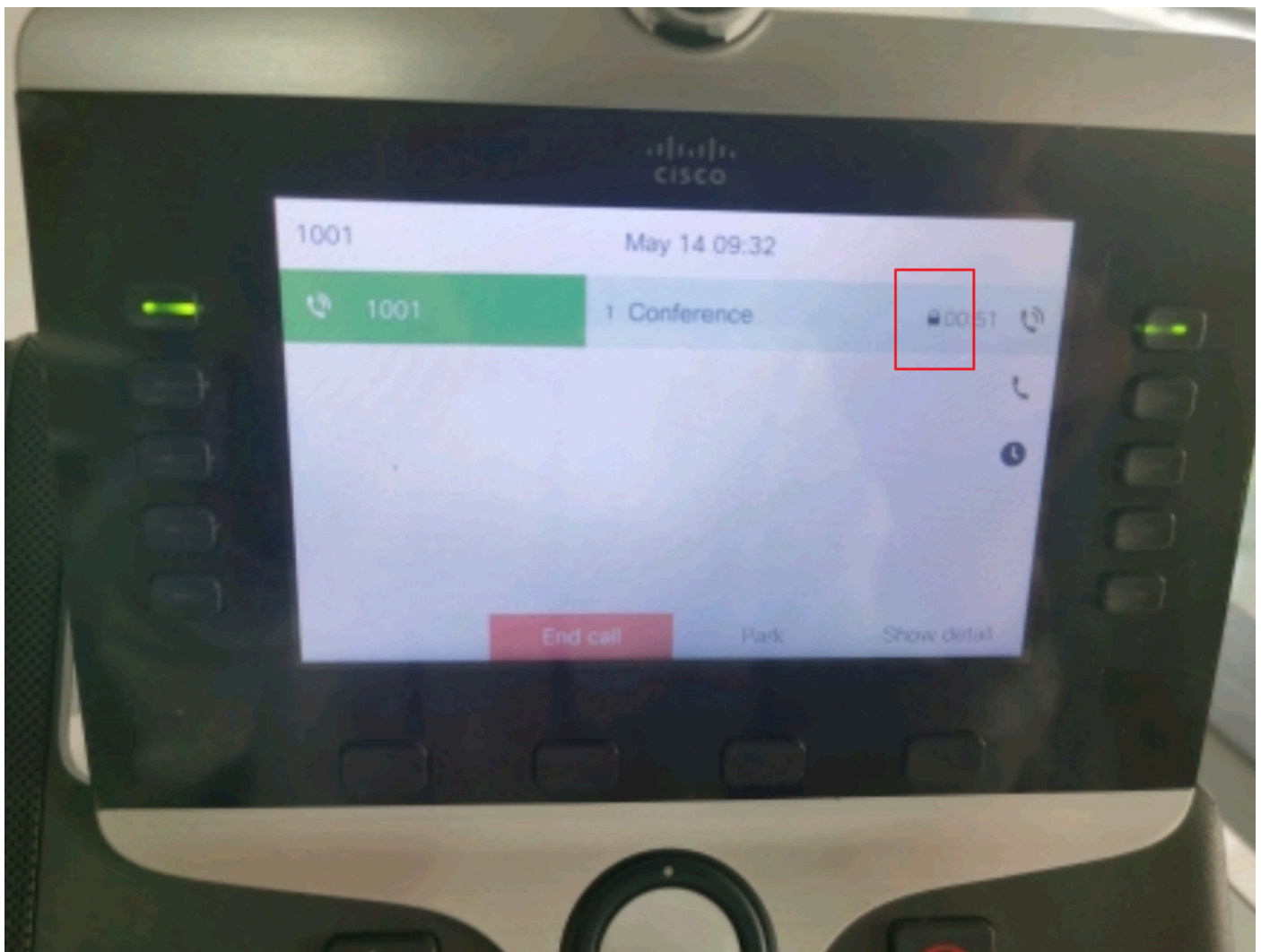
Vérifier

Téléphone IP 1 avec DN 1001, Téléphone IP 2 avec DN 1002, Téléphone IP 3 avec DN 1003.

Étape de test.

1. Appelez le 1001.
2. 1001 appuyez sur la touche de fonction conference et appelez le 1003.
3. Touche de fonction 1001 de la conférence de presse pour impliquer la conférence ad hoc sécurisée.

Les téléphones IP Cisco affichent une icône de sécurité de conférence pour indiquer que l'appel a été chiffré.



L'appel test a été chiffré

Dépannage

Collecter les informations suivantes via RTMT.

Cisco CallManager (les journaux d'appels fournissent des informations sur les appels, le dossier sdl contient des traces CUCM).

À partir de la trace SDL, il apparaît que 1001 envoie un message SIP REFER lorsque 1001 appuie sur la touche de fonction conference pour accéder aux conférences 1002 et 1003.

00018751.002 |17:53:18.056 |InfoApp |SIPTcp - wait_SdlReadRsp : message TCP SIP entrant de x.x.x.x sur le port 51320 index 7 avec 2039 octets :

[587,NET]

REFER sip:CUCMPUB15 SIP/2.0

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

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

À : <sip : CUCMPUB15>

ID d'appel : a4b439d3-8e150010-2f865ab1-7160f679@x.x.x.x

ID de session : b14c8b6f00105000a000a4b439d38e15 ;
remote=00000000000000000000000000000000

Date : Mar, 14 mai 2024 09:53:17 GMT

CSeq : 1000 REFER

User-Agent : Cisco-CP8865NR/14.2.1

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

Expire : 60

Max-Forwards : 70

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

Référencé par : "1001" <sip:1001@x.x.x.x>

Référez-vous à : cid:3e94126b@x.x.x.x

ID de contenu : <3e94126b@x.x.x.x>

Autoriser : ACK, BYE, ANNULER, INVITER, NOTIFIER, OPTIONS, RÉFÉRER, S'INSCRIRE, METTRE À JOUR, S'INSCRIRE

Longueur du contenu : 1069

Content-Type : application/x-cisco-remotecc-request+xml

Content-Disposition : session ; handling=requis

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

<x-cisco-remotecc-request>

<softkeyeventmsg>

<softkeyevent>Conférence</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>

<données d'événement>

<invocationtype>explicite</invocationtype>

</eventdata>

```
<userdata></userdata>
<softkeyid>0</softkeyid>
<applicationid>0</applicationid>
</softkeyeventmsg>
</x-cisco-remotecp-request>
```

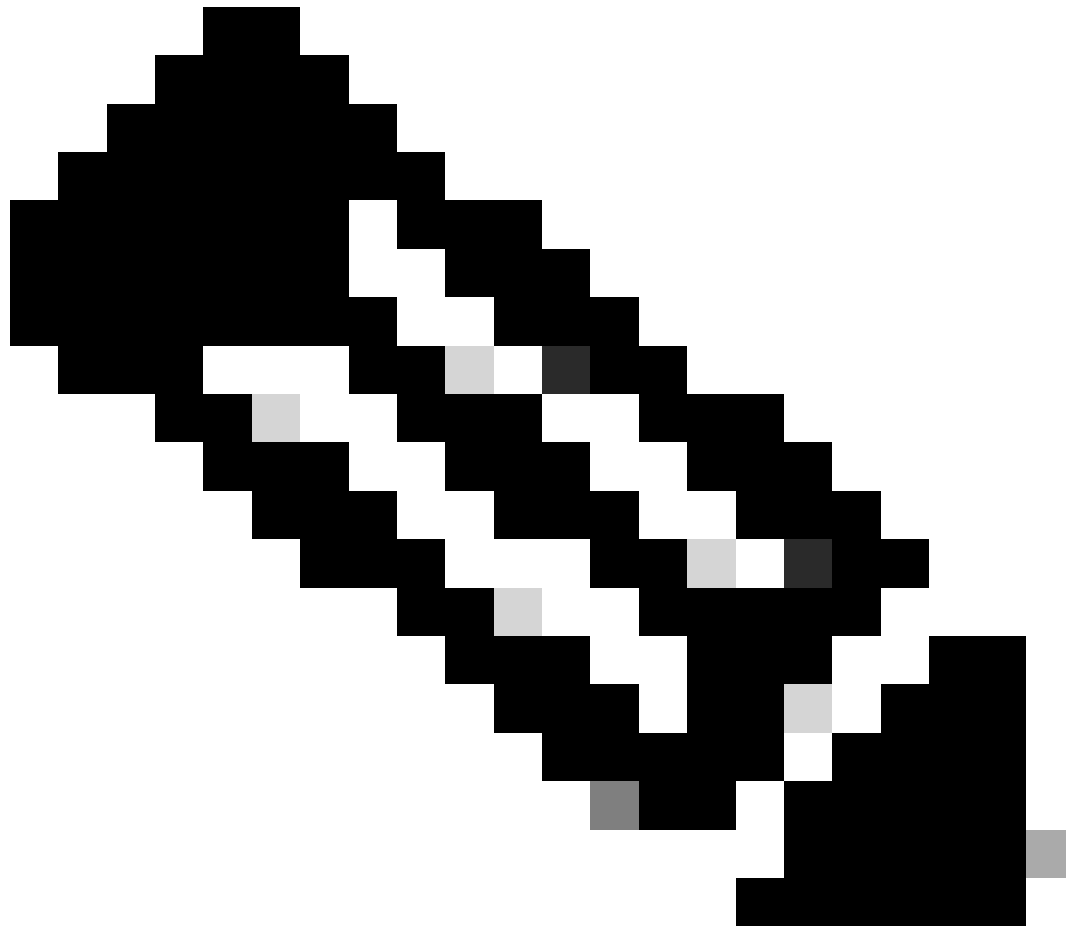
00018751.003 |17:53:18.056 |InfoApp |SIPTcp - SignalCounter = 300

Ensuite, CUCM effectue l'analyse des chiffres et enfin les routes vers le périphérique SecureCFB.

```
00018997.000 |17:53:18.134 |SdISig |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 Unicode Name :
pi : 0 encodeType=10 qsig-encodeType=10 ConnType=3 XferMode=8 ConnTime=3 nwLoc=0Ip
AddrMode=0 ipAddrType=0 ipv4=x.x.x.x : 0 region=Default capCount=6 devType=1
mélangeurCid=16778218 mediaReq=0 portToPort.loc=0 MOH.MRGLPkid= MOH.userHoldID=0
MOH.netHoldID=0 MOH.supp=1 devName=SECURECFB mobileDevName=
origEMCCallingDevName= mobilePartyNumber=pi=0si1 mobileCallType=0 cti=F
ctiFarEndDev=1 ctiCCMId=1 devCepn=38281c14-d78f-46d6-8199-63297bcfdcae lineCepn=
activeCaps=0 VideoCall=F MMUpdateCapMask=0x3e MMCap=0x1 SipConfig : BFCPAllowed=F
IXAllowed=F devCap=0 CryptoCapCount=6 secure=3 loginId=Unsecure CodeName :
retryVideo=FromTag=ToTag=CallId= UAPortFlag=F wantDTMFRecep=1 provOOB=0 supp
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=1 flushCapIns=0 geolocInfo=null locPkid= locName= deductBW=F
fateShareId= videoTrafficClass=Pont non spécifiéParticipantID callingUser= remoteClusterID=
isEMCCDevice=F dtmCall=F dtmPrimaryCI=0 dtmMediaFPid=(0,0,0) dtmMcNodeId=0 dtm
MTPForDTMFTranslation=F emc=T QSIGIMERoute=F eo=0 eoUpdt=1 vCTCUpdt=1
honoreCodec=F honoreUpdt=1 finalCalledPartition= 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
CFBCtrlSecCon=F connBeforeANN=F Infos sur la présentation externe [ pi=0si1locale : 1 Nom :
UnicodeName : pi : 0 mIsCallExternal=F ] ControlProcessType=0
controlProcessTypeUpdateFieldFlag=1 origPi=0
```

Informations connexes

- https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/security/15_0/cucm_b_security-guide-release-15.pdf
- [Assistance technique de Cisco et téléchargements](#)



Remarque : conférence sécurisée sur des liaisons et des passerelles Unified Communications Manager prend en charge la conférence sécurisée sur des liaisons intercluster (ICT), des liaisons/passerelles H.323 et des passerelles MGCP. Toutefois, les téléphones cryptés exécutant la version 8.2 ou antérieure reviennent au protocole RTP pour les appels ICT et H.323 et les supports ne sont pas cryptés. Si une conférence implique une liaison SIP, l'état de la conférence sécurisée est non sécurisé. En outre, la signalisation SIPtrunk ne prend pas en charge les notifications de conférence sécurisées pour les participants hors cluster.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.