

Configuración de conferencias ad hoc seguras en CUCM 15

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Verificación](#)

[Troubleshoot](#)

[Información Relacionada](#)

Introducción

Este documento describe la configuración de la Conferencia Ad Hoc Segura en CUCM 15.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- CUCM
- VG (Gateway de voz)
- Concepto de seguridad

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- CUCM (modo mix) versión: 15.0.0.98100-196
- CISCO2921 versión: 15.7(3)M4b (se utiliza como CA y puente de conferencia seguro)
- Servidor NTP
- 3 teléfonos IP 8865NR

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Tarea 1. Configure Secure Conference Bridge y regístrese en CUCM.

Paso 1. Configure el servidor de infraestructura de clave pública y el punto de confianza.

Paso 1.1. Configure el servidor NTP y el servidor HTTP.

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

Paso 1.2. Configure el servidor de infraestructura de clave pública.

```
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
```

Paso 1.3. Configure el punto de confianza para la CA de prueba.

```
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
```

Paso 1.4. Espere alrededor de 30 segundos, luego ejecute el comando no shutdown para habilitar el servidor 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.
```

Paso 2. Configure el punto de confianza para el puente de conferencia seguro y regístrelo en testCA.

Paso 2.1. Configure el punto de confianza para el puente de conferencia seguro y denomínelo

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
```

Paso 2.2. Autentique SecureCFB y escriba 'yes' para aceptar el certificado.

```
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.
```

Paso 2.3. Inscriba SecureCFB y establezca una contraseña.

```
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.
```

Paso 3. Configure el punto de confianza para CUCM en Secure Concerence Bridge.

Paso 3.1. Descargue el certificado de CallManager de CUCM y copie el archivo pem (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

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	CUCMPUB15.uc.com_7d189df401224dd197999e611637584d
CallManager-trust	CUCSUB15-EC.uc.com_4a6f3ca1b14693b60247d66722a3937a
CallManager-trust	cuc15pub-EC.dltaclab.com_5d830b3dfb167b8b6d46243e0ee19c60
CallManager-trust	ACT2_SUDI_CA_61096e7d000000000000c
CallManager-trust	CUCSUB15.uc.com_54d2204dc0aab6ea71b13f11a736ef3a
CallManager-trust	CUCMPUB15-EC.uc.com_6b5fc677335e12022986819071fde2
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

Descargar certificado de CallManager

Paso 3.2. Configure Trust Point, pegue el archivo pem y escriba yes para aceptar el certificado.

```
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
DwAwggEKAoIABQD4Xfdl9MwYy/bSDXzGjtd301vYqKdRqpVYpWD7E+Nrh7zRgHh+
M7gAeqdRCSC/iKUF2g44RCRjIM0C/9xN3pxvOnNequg/Tv0wjpHm0X2O4x0daH+F
AwEIWNyZzVUQ6+2xtkTuUcqeXDnnbS6fLladP/CfgQwKX5U1Ec575ypUet6Fp2n2
4UouLQ5iFEMmX9gzGR7YKjeE+t61X5NmvYc6IyP8MH77sgvti7+xJurIUnvBFG2
ELXM0rL7uUoqw/rjMT6XxK+0ft4bkOsVnjl+vOUUBUoTcbFFrsfrOnVQjPJhHue
MLAaRzkDo5p1xo+UnNgv2uSH9HAID/NS1VTDAGMBAAGjYTBfMAsGA1UdDwQEAwIC
tDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwHQYDVR0OBBYEFKrlBeQi
```

```
OF6Hp0QCUfVYzKWiX2hMBIGA1UdEwEB/wQIMAYBAf8CAQAwDQYJKoZIhvcNAQEL
BQADggEBAJSw2vOwJ4UatmkaFpeLc9B1YZr8X6BkxBY1skW2qOLps61ysjDG61VQ
GjxpPLMY1ISylVr5dqGyjaGLCUDUUcu66zEPxFNGnSYimBBhGR6NrDyo4YjOk+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

Paso 4. Configure CUCM para confiar en el puente de conferencia seguro.

Paso 4.1. Copie el certificado de uso general y guárdelo como un archivo SecureCFB.pem. Copie el certificado de la CA y guárdelo como archivo testCA.pem.

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

```
% CA certificate:
```

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

```
MIIIBzCCAWSgAwIBAgIBATANBgkqhkiG9w0BAQQFADARMQ8wDQYDVQQDEwZ0ZXN0
Q0EwHhcNMjQwNTEwMDg0NDI3WhcNMjcwNTEwMDg0NDI3WjARMQ8wDQYDVQQDEwZ0
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
Q0EwHhcNMjQwNTEwMDg1NTA4WhcNMjcwNTEwMDg0NDI3WjAUMRIwEAYDVQQDEwIT
ZWN1cmVDRklwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALhk11yOPnUNTjEQ
JLJIMPnoc6Zb9vDrGollMdsz/czWkTiGCS9PYYxwcPBExOOR+XrE9MmEO7L/tr6n
NkKz84ddWNz0gg6wHWM9gcje22blsleU6UCxo4ovra2pExXphusqEmg5yLQwyeJc
5JqcoAYXuRpnKLTfn5Nnh6iUCsWrAgMBAAGjTzBNMAsGA1UdDwQEAwIFoDAfBgNV
HSMEGDAWgBSThaxj/IQXHdNXfUswqYTZFhqnFjAdBgNVHQ4EFgQU3y9zfDoTJ8WV
XlpX3wdcieq1zpkwDQYJKoZIhvcNAQEFBQADgYEABfaa6ppqRaDyfpW/tu5pXBRHP
SfZzpv+4ktsjAiOG7oGJGT0RpnuikCq+V2oucJbtWWAPbVx+ZBG3Eogi1c2GoDLK
yYvuaf9zBJHicM5mv6x81qxLF7FKZaepQSYwsQUP50/uKXa0435Kj/CZoLpKhXR2
v/p2jzF9zyPIBuQGEOEo=
-----END CERTIFICATE-----
```

Paso 4.2. Cargue SecureCFB.pem en el almacén de confianza de CallManager en 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.

Cargar SecureCFB.pem

Paso 5. Configure el puente de conferencia seguro en 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
```

Paso 6. Configure Secure Conference Bridge en CUCM (Administración de Cisco Unified CM > Recursos multimedia > Conference Bridge > Agregar nuevo).

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

Configurar puente de conferencia seguro

Tarea 2. Registre 3 teléfonos IP 8865NR con modo de seguridad.

Establezca Device Security Profile en el modo cifrado del teléfono 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 > ▾

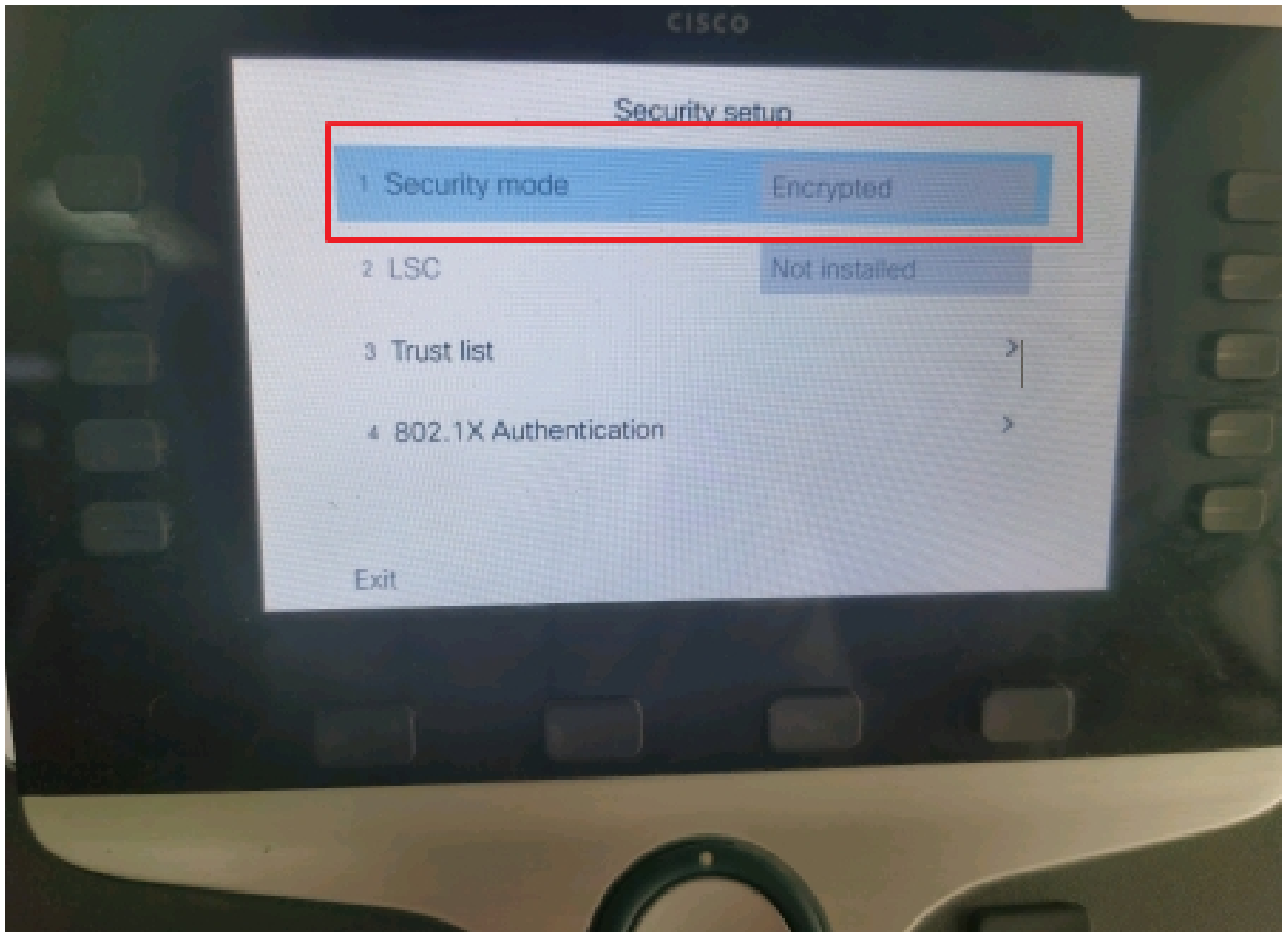
Media Termination Point Required

Unattended Port

Require DTMF Reception

Establecer el perfil de seguridad del dispositivo en modo cifrado

El teléfono IP muestra el modo de seguridad con cifrado en Admin settings > Security Setup.




El modo de seguridad estaba cifrado

Tarea 3. Configure la lista de grupos de recursos de medios con Secure Conference Bridge y asígnela a los teléfonos IP.

Paso 1. Cree un grupo de recursos de medios MRG_SecureCFB y asígnele SecureCFB (Administración de Cisco Unified CM > Recursos de medios > Grupo de recursos de medios).

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)

Creación de un grupo de recursos de medios MRG_SecureCFB

Paso 2. Cree una lista de grupos de recursos de medios MRGL_SecureCFB y asígnele MRG_SecureCFB (Administración de Cisco Unified CM > Recursos de medios > Lista de grupos de recursos de medios).

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

Creación de una Lista de Grupos de Recursos de Medios MRGL_SecureCFB

Paso 3. Asigne la lista de grupos de recursos de medios MRGL_SecureCFB a todo el 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	Meet Me Conference	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 >"/>

Asignar lista de grupos de recursos de medios

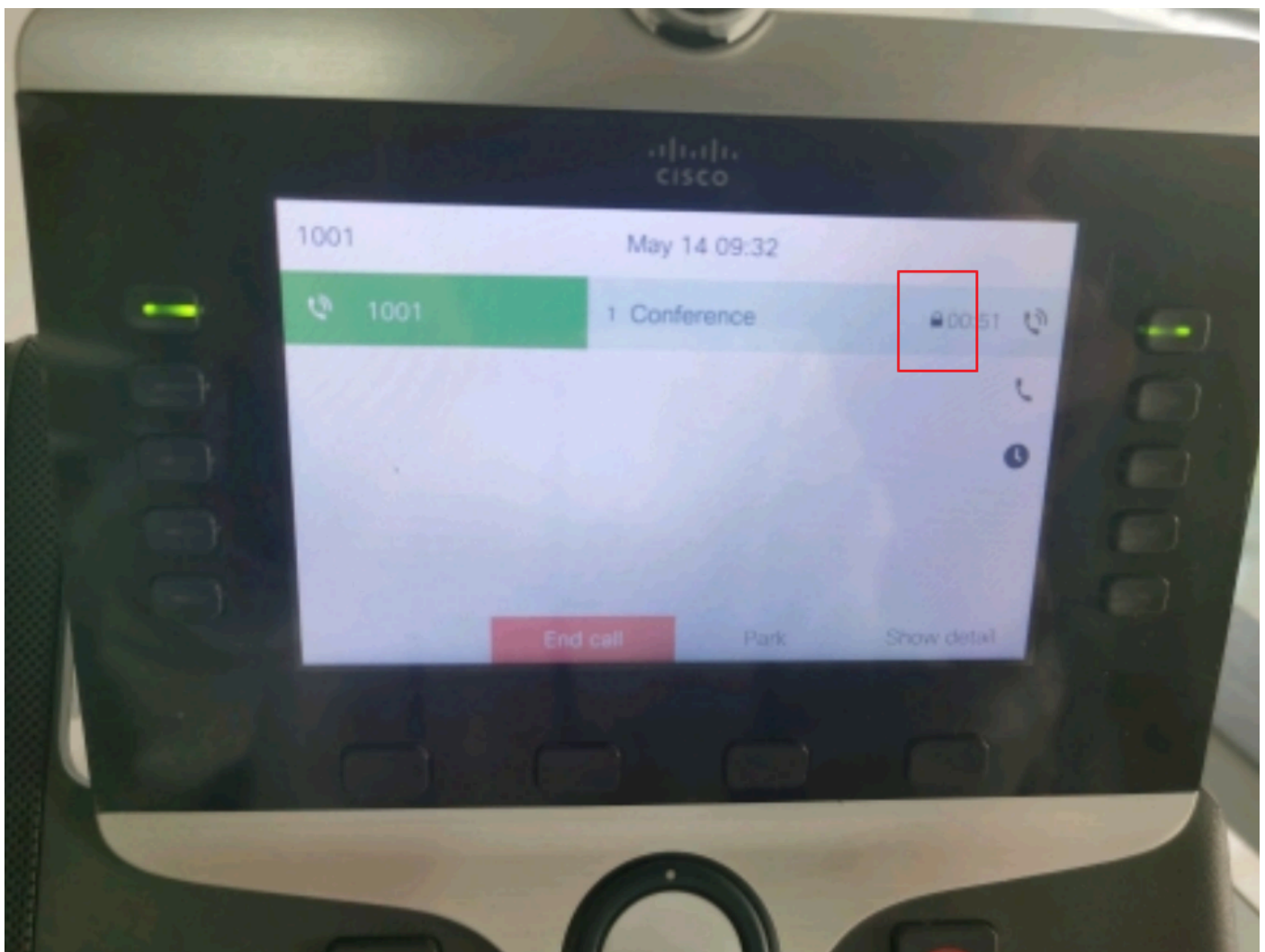
Verificación

IP Phone 1 con DN 1001, IP Phone 2 con DN 1002, IP Phone 3 con DN 1003.

Paso de prueba.

1. 1001 llame al 1002.
2. Tecla programable de conferencia de prensa 1001 y llame al 1003.
3. Tecla programable de la conferencia de prensa 1001 para hacer participar a la Conferencia ad hoc segura.

Los teléfonos IP de Cisco muestran un icono de seguridad de conferencia para indicar que la llamada fue cifrada.



La llamada de prueba estaba cifrada

Troubleshoot

Recopile la siguiente información mediante RTMT.

Cisco CallManager (los registros de llamadas proporcionan información sobre las llamadas, la carpeta sdl contiene seguimientos de CUCM).

Desde el seguimiento de SDL, se observa que 1001 envía un mensaje SIP REFER cuando 1001 presiona la tecla programable de la conferencia a las conferencias 1002 y 1003.

00018751.002 |17:53:18.056 |AppInfo |SIPTcp - wait_SdlReadRsp: Mensaje TCP SIP entrante de x.x.x.x en el puerto 51320 índice 7 con 2039 bytes:

[587,NETO]

REFER sip:CUCMPUB15 SIP/2.0

Vía: SIP/2.0/TLS x x x x 51320;branch=z9hG4bK4d786568

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

Para: <sip:CUCMPUB15>

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

ID de sesión:

b14c8b6f00105000a000a4b439d38e15;remote=00000000000000000000000000000000

Fecha: martes 14 de mayo de 2024 09:53:17 GMT

CSeq: 1000 REFER

Agente de usuario: Cisco-CP8865NR/14.2.1

Aceptar: application/x-cisco-remote-response+xml

Caducidad: 60

Reenvíos máximos: 70

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

Referencia: "1001" <sip:1001@x.x.x.x>

Consulte: cid:3e94126b@x.x.x.x

Content-Id: <3e94126b@x.x.x.x>

Permitir:

ACK,BYE,CANCEL,INVITE,NOTIFY,OPTIONS,REFER,REGISTER,UPDATE,SUBSCRIBE

Longitud del contenido: 1069

Tipo de contenido: application/x-cisco-remote-request+xml

Content-Disposition: session;handling=required

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

<x-cisco-remote-request>

<softkeyeventmsg>

<softkeyevent>Conferencia</softkeyevent>

<dialgid>

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

<localtag>a4b439d38e1500333f1eb5d4-68656916</localtag>

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

</dialgid>

<linenumber>0</linenumber>

<participantnum>0</participantnum>

<consultdialgid>

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

<localtag>a4b439d38e15003562c2c59a-69dbf571</localtag>

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

</consultdialgid>

<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-remote-request>

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

A continuación, CUCM realiza un análisis de dígitos y, por último, enruta al dispositivo 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 Name: 4 UnicodeName: pi: 0
encodeType=10 qsig-encodeType=10 ConnType=3 XferMode=8 ConnTime=3 nwLoc
IpAddrMode=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=SECURECFB mobileDevName=
origEMCCCallingDevName= mobilePartyNumber=pi 0si1 mobileCallType=0 ctiActive=F
ctiFarEndDev=1 ctiCCMId=1 devCepn=38281c14-d78f-46d6-8199-63297bcfdade lineCepn=
activeCaps=0 VideoCall=F MMMUpdateCapMask=0x3e MMCap=0x1 SipMask: BFCPAllowed=F
IXAAllow F devCap=0 CryptoCapCount=6 secure=3 loginId= UnicodeName:
retriesVideo=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
destinationShareId= videoTrafficClass=BridgeParticipantID no especificado callingUser=
remoteClusterID= isEMCCDevice=F dtmCall=F dtmPrimaryCI=0 dtmMedia IFPid=(0,0,0,0)
dtmMcNodeId=0 dtmMTPForDTMFTranslation=F emc=T QSIGIMERoute=F eo=0 eoUpdt=1
vCTCUpdt=1 honorCodec=F honorUpdt=1 finalCalledPartition= cTypeUpdt=0 BibEnabled=0
RecordingQSIGAPDUSupported=F FarEndDeviceName=LatentCaps=icidVal= icidGenAddr= oioi=
tioi= ptParams= CAL={v=-1, m=-1, tDev=F, res=F, devType=0} displayNameUpdateFieldFlag=0
CFBCtrlSecCon=F connBeforeANN=F Información de presentación externa [pi=0si1locale: 1
Nombre: UnicodeName: pi: 0 mlsCallExternal=F] ControlProcessType=0
controlProcessTypeUpdateFieldFlag=1 orig Pi=0

Información Relacionada

- https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/security/15_0/cucm_b_security-guide-release-15.pdf
- [Soporte técnico y descargas de Cisco](#)



Nota: Conferencia segura a través de troncales y gateways Unified Communications Manager admite conferencias seguras a través de troncales intracluster (ICT), troncales/gateways H.323 y gateways MGCP; sin embargo, los teléfonos cifrados que ejecutan la versión 8.2 o anteriores vuelven a RTP para las llamadas ICT y H.323, y los medios no se cifran. Si una conferencia incluye un troncal SIP, el estado de la conferencia segura es no seguro. Además, la señalización de troncales SIP no admite notificaciones de conferencia seguras a participantes fuera del clúster.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).