Configura conferenza ad hoc sicura su CUCM 15

Sommario

Introduzione

Questo documento descrive la configurazione della Secure Ad Hoc Conference su CUCM 15.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- CUCM
- VG (Voice Gateway)
- Concetto di sicurezza

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- CUCM (modalità mix) versione: 15.0.0.98100-196
- Versione CISCO 2921: 15.7(3)M4b (da utilizzare come CA e Secure Conference Bridge)
- Server NTP
- 3 8865NR IP Phone

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Attività 1. Configurare Secure Conference Bridge e registrarsi a CUCM.

Passaggio 1. Configurare il server dell'infrastruttura a chiave pubblica e il trust point.

Passaggio 1.1. Configurare il server NTP e HTTP.

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

Passaggio 1.2. Configurare il server dell'infrastruttura a chiave pubblica.

```
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
```

Passaggio 1.3. Configurare il trust point per 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
```

Passaggio 1.4. Attendere circa 30 secondi, quindi usare il comando no shutdown per abilitare il server 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.
```

Passaggio 2. Configurare il trust point per Secure Conference Bridge e registrarlo per verificare la CA.

Passaggio 2.1. Configurare il trust point per Secure Conference Bridge e denominarlo 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
```

Passaggio 2.2. Autenticare SecureCFB e digitare 'yes' per accettare il certificato.

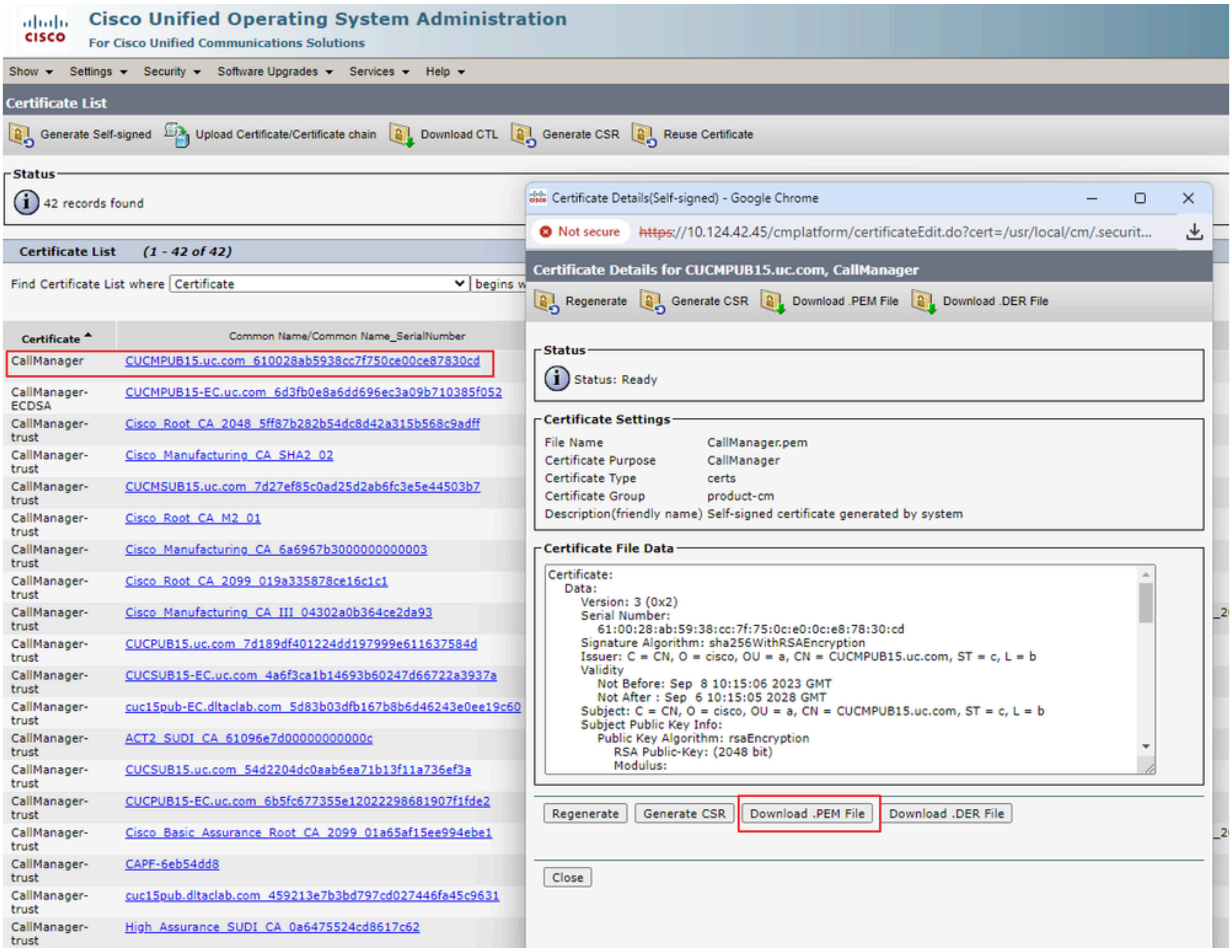
```
VG-CME-1(config)#crypto pki authenticate SecureCFB
Certificate has the following attributes:
      Fingerprint MD5: 383BA13D C37D0E5D 9E9086E4 8C8D1E75
     Fingerprint SHA1: 6DB8F323 14BBFBFF C36C224B B3404513 2FDD97C5

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

Passaggio 2.3. Registrare SecureCFB e impostare una password.

```
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.
```

Passaggio 3. Configurare il trust point per CUCM su Secure Concerence Bridge.

Passaggio 3.1. Scaricare il certificato CallManager da CUCM e copiare il file 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
Certificate Details(Self-signed) - Google Chrome
Not secure
https://10.124.42.45/cmplatform/certificateEdit.do?cert=/usr/local/cm/.securit...
Certificate Details for CUCMPUB15.uc.com, CallManager
Regenerate
Generate CSR
Download .PEM File
Download .DER File
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

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:
```

Scarica certificato di CallManager

Passaggio 3.2. Configurare il trust point, incollare il file pem e digitare yes per accettare il certificato.

```
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
```

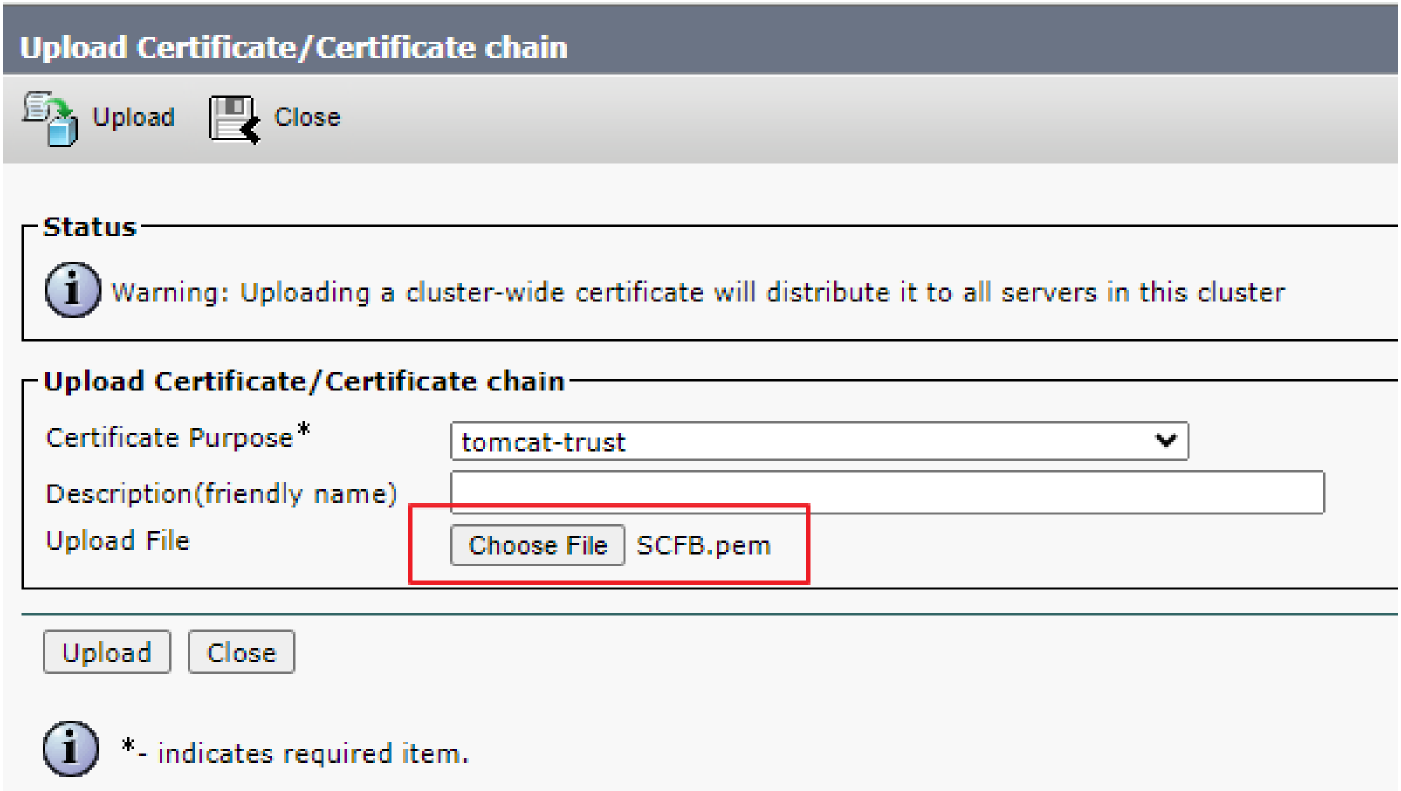
```
tDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwHQYDVR0OBBYEFKrIBeQi
OF6Hp0QCUfVYzKWiXx2hMBIGA1UdEwEB/wQIMAYBAf8CAQAwDQYJKoZIhvcNAQEL
BQADggEBAJSw2vOwJ4UatmkaFpeLc9B1YZr8X6BkxBY1skW2qOLps61ysjDG61VQ
GjxpPLMY1ISyIVr5dqGyjcaGLCUDUUcu66zEPxFNGnSYimBBhGR6NrDyo4YjOk+S
1I3TfRK+2F9NMhW2xTvuygoXLtyibvrZULhNo3vDPYQdTe1z54oQNU4BD8P+MCq9
+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
```

Passaggio 4. Configurare CUCM per considerare attendibile il bridge per conferenze sicuro.

Passaggio 4.1. Copiare il certificato di utilizzo generale e salvarlo come file SecureCFB.pem. Copiare il certificato CA e salvarlo come file testCA.pem.

```
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-----
```

Passaggio 4.2. Caricare SecureCFB.pem nell'archivio di attendibilità CallManager su CUCM (Cisco Unified OS Administration > Security > Certificate Management).



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

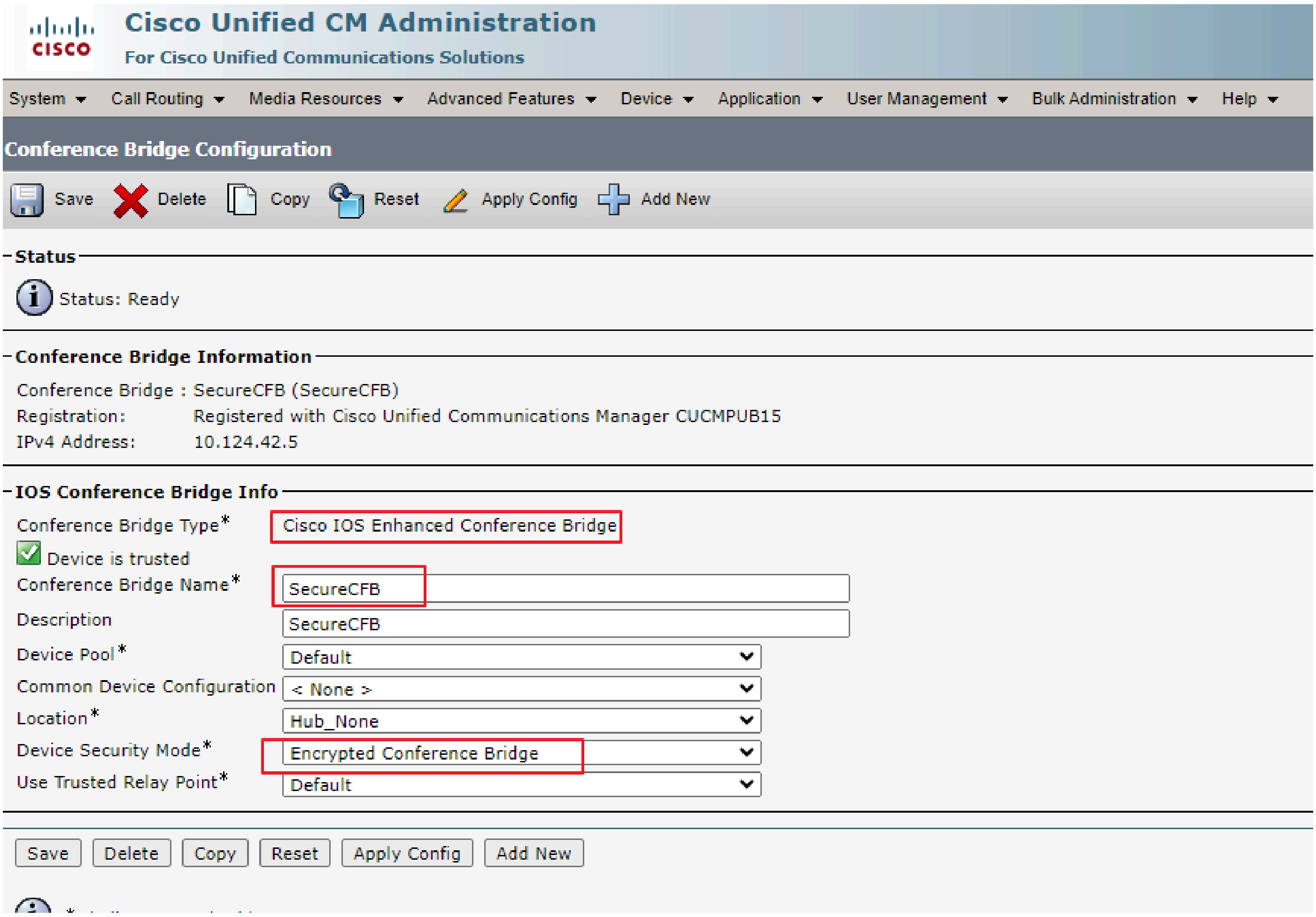
*- indicates required item.

Caricare SecureCFB.pem

Passaggio 5. Configurare Secure Conference Bridge su 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
```

Passaggio 6. Configurare Secure Conference Bridge su CUCM (Cisco Unified CM Administration > Media Resources > Conference Bridge > 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

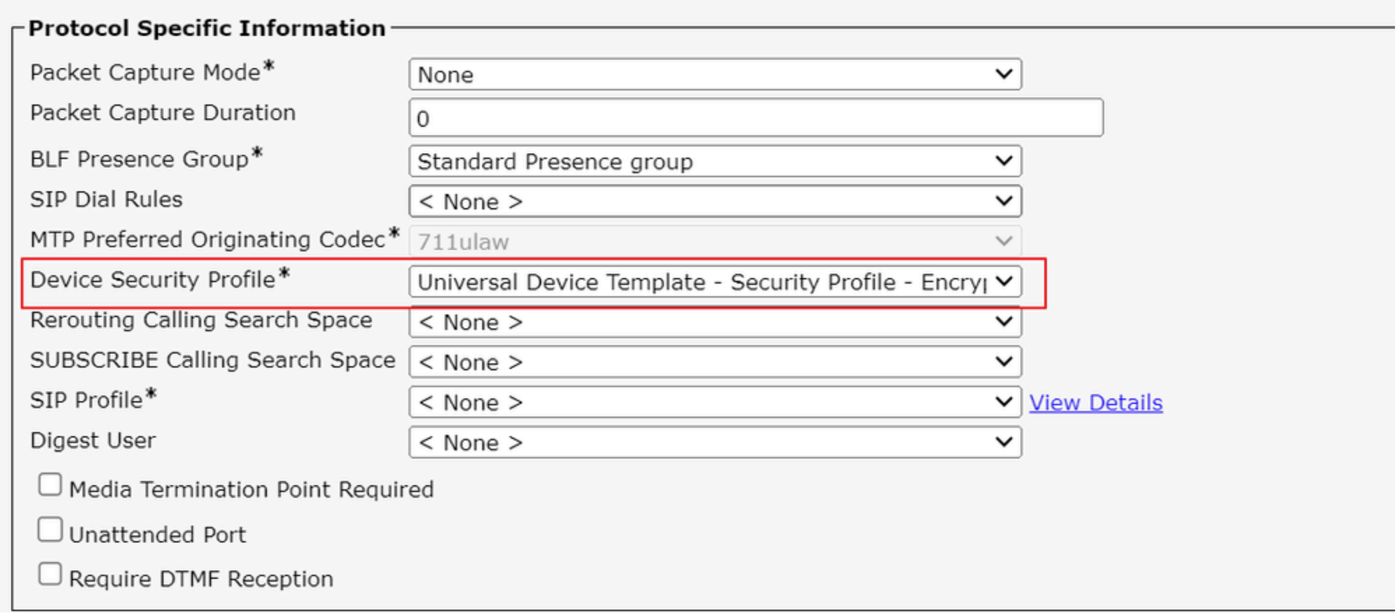
IOS Conference Bridge Info

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

Configura Secure Conference Bridge

Attività 2. Registra 3 8865NR IP Phone con modalità di sicurezza.

Impostare il profilo di sicurezza del dispositivo sulla modalità crittografata sul telefono IP.



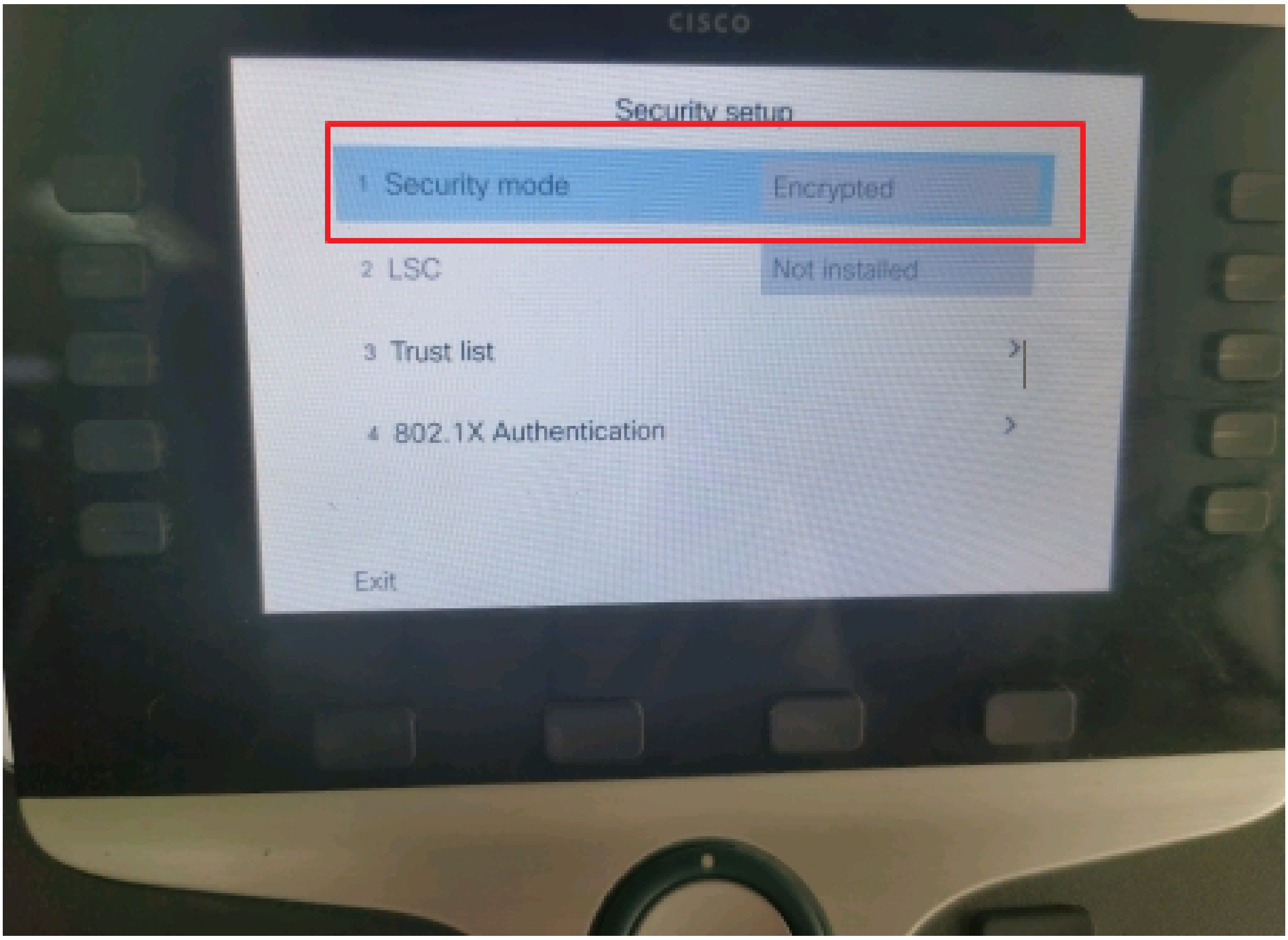
Protocol Specific Information

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 - Encry|
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

Imposta il profilo di sicurezza del dispositivo sulla modalità crittografata

IP Phone mostra la modalità di sicurezza con Encrypted in Admin settings > Security Setup.



Security setup

1 Security mode Encrypted

2 LSC Not installed

3 Trust list

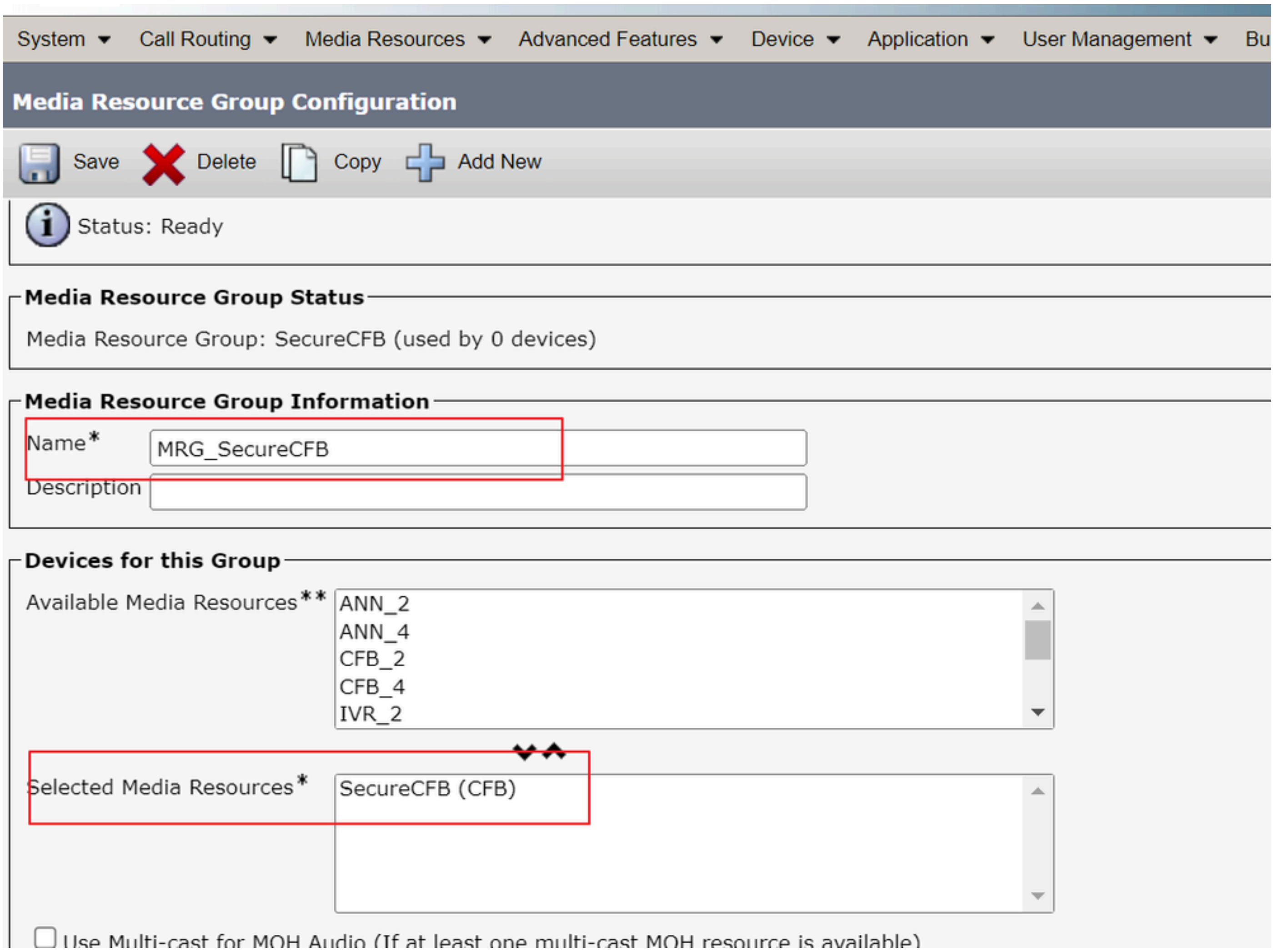
4 802.1X Authentication

Exit

La modalità di protezione è stata crittografata

Attività 3. Configurare l'elenco dei gruppi di risorse multimediali con Secure Conference Bridge e assegnarlo ai telefoni IP.

Passaggio 1. Creare un gruppo di risorse multimediali MRG_SecureCFB e assegnargli SecureCFB (Cisco Unified CM Administration > Media Resources > Media Resources Group).



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

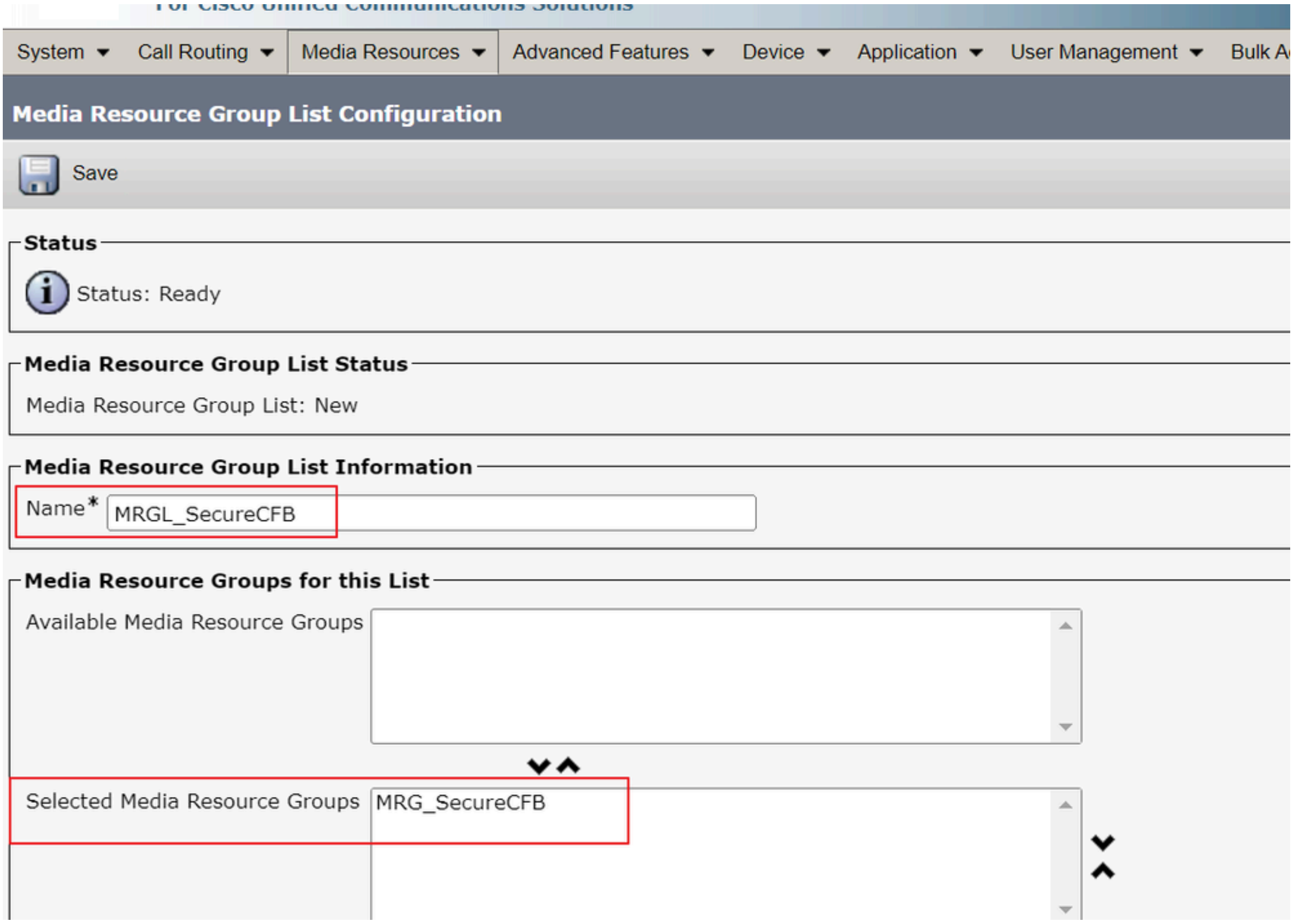
Available Media Resources** ANN_2, ANN_4, CFB_2, CFB_4, IVR_2

Selected Media Resources* SecureCFB (CFB)

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

Creare un gruppo di risorse multimediali MRG_SecureCFB

Passaggio 2. Creare un elenco di gruppi di risorse multimediali MRGL_SecureCFB e assegnargli MRG_SecureCFB (Cisco Unified CM Administration > Risorse multimediali > Elenco gruppi risorse multimediali).



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

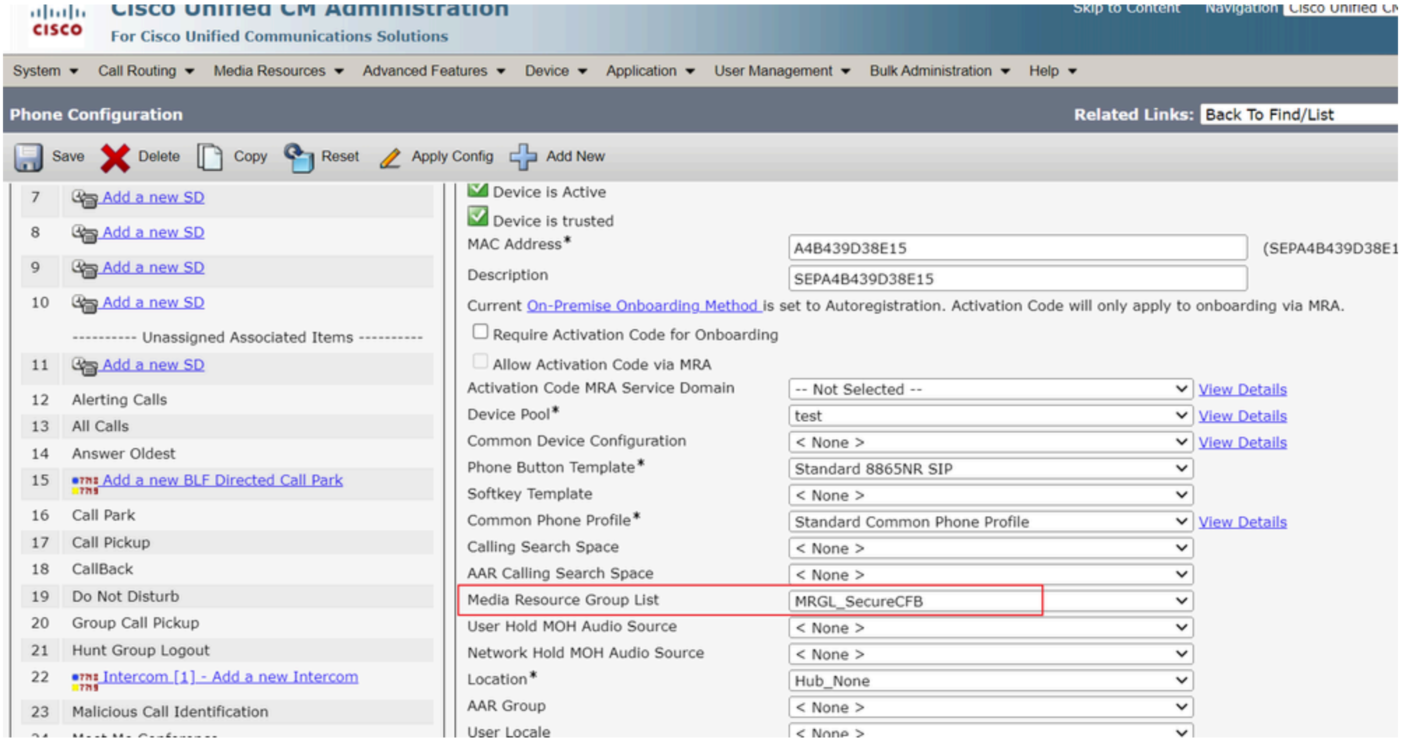
Media Resource Groups for this List

Available Media Resource Groups

Selected Media Resource Groups MRG_SecureCFB

Creazione di un elenco di gruppi di risorse multimediali MRGL_SecureCFB

Passaggio 3. Assegnare l'elenco dei gruppi di risorse multimediali MRGL_SecureCFB a tutti gli switch 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 --	View Details
Device Pool*	test	View Details
Common Device Configuration	< None >	View Details
Phone Button Template*	Standard 8865NR SIP	
Softkey Template	< None >	
Common Phone Profile*	Standard Common Phone Profile	View Details
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 >	

Assegna elenco gruppi di risorse multimediali

Verifica

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

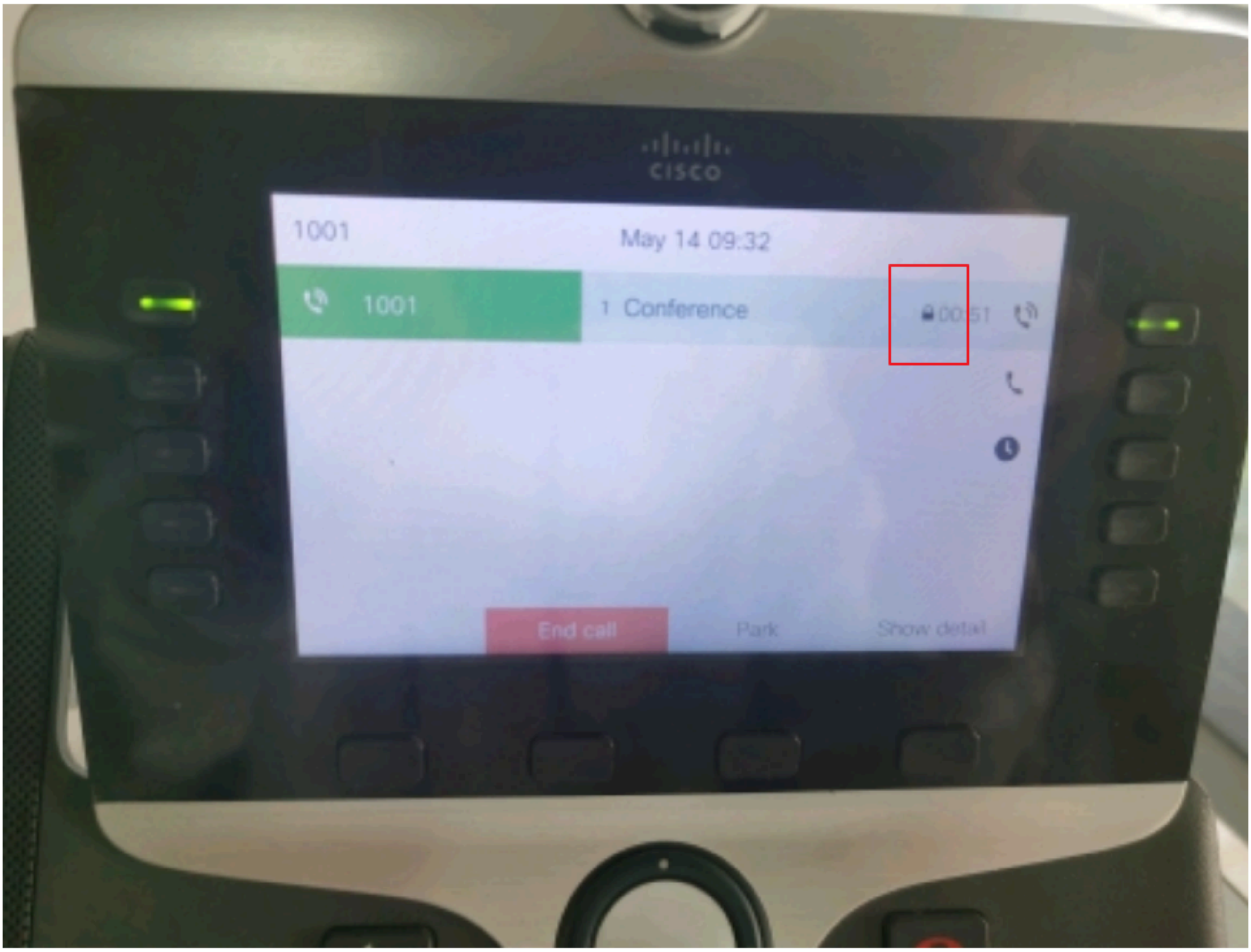
Passaggio di test.

1. 1001 chiamare 1002.

2. 1001 tasto video della conferenza stampa e chiamare il 1003.

3. Tasto soft della conferenza stampa 1001 per coinvolgere la Secure Ad Hoc Conference.

I Cisco IP Phone visualizzano un'icona di sicurezza della conferenza per indicare che la chiamata è stata crittografata.



Chiamata di prova crittografata

Risoluzione dei problemi

Raccogliere le informazioni successive tramite RTMT.

Cisco CallManager (calllogs fornisce informazioni sulle chiamate; sdl folder contains CUCM traces).

Da SDL Trace, è possibile notare che 1001 invia un messaggio SIP REFERENCE quando il tasto video della conferenza stampa 1001 è impostato su conference 1002 e 1003.

```
00018751.002 |17:53:18.056 |AppInfo  |SIPTcp - wait_SdlReadRsp: messaggio TCP SIP in arrivo da x.x.x.x sulla porta 51320 index 7 con 2039 byte:

[587,NETTO]

SIP:CUCMPUB15 SIP/2.0

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

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

A: <sip:CUCMPUB15>

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

ID sessione: b14c8b6f00105000a000a4b439d38e15;remoto=00000000000000000000000000000000

Data: mar, 14 maggio 2024 09:53:17 GMT

CSeq: 1000 REFERENCE

Agente utente: Cisco-CP8865NR/14.2.1

Accetta: application/x-cisco-remotec-response+xml

Scade: 60

Max in avanti: 70

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

Autore segnalazione: "1001" <sip:1001@x.x.x.x>

Fare riferimento a: cid:3e94126b@x.x.x.x

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

Consenti: ACK,BYE,ANNULLA,INVITA,NOTIFICA,OPZIONI,RIF,REGISTRA,AGGIORNA,SOTTOSCRIVI

Content-Length: 1.069

Content-Type: application/x-cisco-remote-request+xml
```

```
Content-Disposition: sessione;gestione=obbligatorio
<?xml version="1.0" encoding="UTF-8"?>
<x-cisco-remote-request>
  <softkeyeventmsg>
    <softkeyevent>Conferenza</softkeyevent>
    <iddialogo>
      <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>
    <dati evento>
      <invocationtype>explicit</invocationtype>
    </eventdata>
    <dati utente></dati utente>
    <softkeyid>0</softkeyid>

    <applicationid>0</applicationid>

  </softkeyeventmsg>

</x-cisco-remote-request>

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

Quindi, CUCM esegue l'analisi delle cifre e infine instrada verso il dispositivo SecureCFB.

```
00018997.000 |17:53:18.134 |FirmaSD   |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 devName=SECURECFB mobileDevName=
origEMCallingDevName= mobilePartyNumber=pi=0si1 mobileCallType=0 ctiActive=F
ctiFarEndDev=1 ctiCCMId=1 devCepn=38281c14-d78f-46d6-8199-63297bcfddddae lineCepn=
activeCaps=0 VideoCall=F MMMMuUpdateCapMask=0x3e MMCap x1 SipConfig:
BFCPAllowed=F IXAllowed=F devCap=0 CryptoCapCount=6 secure=3 loginId= UnicodeName:
retriedVideo=FromTag=ToTag=CallId= UAPortFlag=F wantDTMFRecep=1 provOB=0 supp
DTMF=1 DTMF Cfg=1 DTMF PT=() DTMF reqMed=1 isPrefAltScript=F cdpn nUsage=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=Unspecified bridgeParticipantID callingUser= remoteClusterID=
isEMIS CDevice=F dtmCall=F dtmPrimaryCI=0 dtmMediaIFPid=(0,0,0) dtmMcNodeId=0
dtmMTPForDTMFTranslation=F emc=T QSIGIMERoute=F eo=0 eoUpdt=1 vCTCUpdt=1
onoreCodec=F onoreUpdt=1 finalCalledPartition= cTypeUpdt=0 BibEnabled=0
QSIGAPDUSupported=F FarEndDeviceName=LatentCaps=null icidVal= icidGenAddr= oioi= tioi=
ptParams= CAL={v=-1, m=-1, tDev=F, res=F, devType=0} displayNameUpdateFieldFlag=0
CFBCtrlSecIcon=F connBeforeANN=F Presentazione esterna Info [ pi=0si1locale: 1 Nome:
UnicodeName: pi: 0 mIsCallExternal ] TipoProcesso=0 tipoProcessoAggiornaFlag=1 origPi=0
```

Informazioni correlate

- https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/security/15_0/cucm_b_security-guide-release-15.pdf
- Supporto tecnico Cisco e download

Nota: Secure Conference over Trunks and Gateways Unified Communications Manager supporta le conferenze sicure su trunk intracluster (ICT), trunk/gateway H.323 e gateway MGCP. Tuttavia, i telefoni crittografati con la versione 8.2 o precedenti tornano al protocollo RTP per le chiamate ICT e H.323 e i supporti non vengono crittografati. Se una conferenza include un SIPtrunk, lo stato della conferenza protetta è non protetto. Inoltre, la segnalazione SIPtrunk non supporta le notifiche di conferenza sicure ai partecipanti esterni al cluster.