

CUCM에서 Secure Ad Hoc 컨퍼런스 구성 15

목차

- [소개](#)
 - [사전 요구 사항](#)
 - [요구 사항](#)
 - [사용되는 구성 요소](#)
 - [구성](#)
 - [다음을 확인합니다.](#)
 - [문제 해결](#)
 - [관련 정보](#)
-

소개

이 문서에서는 CUCM 15의 Secure Ad Hoc Conference(Secure Ad Hoc 컨퍼런스) 구성에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- CUCM
- VG(음성 게이트웨이)
- 보안 개념

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- CUCM(혼합 모드) 버전: 15.0.0.98100-196
- CISCO2921 버전: 15.7(3)M4b(CA 및 보안 컨퍼런스 브리지로 사용)
- NTP 서버
- 3 8865NR IP Phone

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

작업 1. Secure Conference Bridge를 구성하고 CUCM에 등록합니다.

1단계. 공개 키 인프라 서버 및 신뢰 지점을 구성합니다.

1.1단계. NTP 서버 및 HTTP 서버를 구성합니다.

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

1.2단계. 공개 키 인프라 서버를 구성합니다.

```
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
```

1.3단계. testCA에 대한 신뢰 지점을 구성합니다.

```
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
```

1.4단계. 약 30초 정도 기다린 다음 testCA 서버를 활성화하기 위해 no shutdown 명령을 실행합니다.

```
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.
```

2단계. Secure Conference Bridge의 Trust Point를 구성하고 이를 testCA에 등록합니다.

2.1단계. Secure Conference Bridge에 대한 신뢰 지점을 구성하고 이름을 SecureCFB로 지정합니다.

```
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
```

2.2단계. 인증서를 수락하려면 SecureCFB를 인증하고 'yes'를 입력합니다.

```
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.
```

2.3단계. SecureCFB를 등록하고 비밀번호를 설정합니다.

```
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.
```

3단계. Secure Concession Bridge에서 CUCM의 신뢰 지점을 구성합니다.

3.1단계. CUCM에서 CallManager 인증서를 다운로드하고 pem 파일(Cisco Unified OS Administration > Security > Certificate Management)을 복사합니다.

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_01a65af15ee9944be1
CallManager-trust	CAPF-6eb54dd8
CallManager-trust	cuc15pub.dltaclab.com_459213e7b3bd797cd027446fa45c9631
CallManager-trust	High_Assurance_SUDI_CA_0a6475524cd8617c62

Certificate Details(Self-signed) - Google Chrome

Not secure https://10.124.42.45/cmplatform/certificateEdit.do?cert=/usr/local/cm/secure...

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

CallManager 인증서 다운로드

3.2단계. 인증서를 승인하려면 Trust Point를 구성하고 pem 파일을 붙여넣은 다음 yes를 입력합니다.

```
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
DwAwggEKAoIBAQD4XfdI9MwY/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

4단계. 보안 컨퍼런스 브리지를 신뢰하도록 CUCM을 구성합니다.



4.1단계. 범용 인증서를 복사하여 SecureCFB.pem 파일로 저장합니다. CA 인증서를 복사하여 testCA.pem 파일로 저장합니다.

```
VG-CME-1(config)#crypto pki export SecureCFB pem terminal
% CA certificate:
-----BEGIN CERTIFICATE-----
MIIB+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-----
MIIB6jCCAvoGAWIBAgIBAJANBgkqhkiG9w0BAQUFADARMQ8wDQYDVQQDEwZ0ZXN0
Q0EwHhcNMjQwNTEwMDg1NTA4WWhcNMjcwNTEwMDg0NDI3WjAUMRIwEAYDVQQDEwIT
ZWN1cmVDRklwZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALhk11yOPnUNTjEQ
JLJIMPnoc6Zb9vDrGollMdsz/czWKTiGCS9PYYxwcpBExOOR+XrE9MmEO7L/tr6n
NkKz84ddWNz0gg6wHWM9gcje22blsleU6UCxo4ovra2pExXphusqEmg5yLQwyeJc
5JqcoAYXuRpnKLTfn5Nnh6iUCsWrAgMBAAGjTzBNMAsGA1UdDwQEAwIFoDAfBgNV
HSMEGDAWgBSThaxj/IQXHdNXfUswqYTZFhqnFjAdBgNVHQ4EFgQU3y9zfDoTJ8WV
XlpX3wdcieq1zpkwDQYJKoZIhvcNAQEFBQADgYEABfaa6ppqRaDyfpW/tu5pXBRHP
SfZzpv+4ktsjAiOG7oGJGT0RpnuikCq+V2oucJbtWWAPbvX+ZBG3Eogi1c2GoDLK
yYvuaf9zBJHicM5mv6x81qxLF7FKZaepQSYwsQUP50/uKXa0435Kj/CzoLpKhXR2
v/p2jzF9zyPIBuQGEOEo=
-----END CERTIFICATE-----
```

4.2단계. CUCM의 CallManager-trust 저장소에 SecureCFB.pem을 업로드합니다(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 업로드

5단계. VG에서 보안 전화회의 브리지를 구성합니다.

```
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
```

6단계. CUCM에서 보안 컨퍼런스 브리지 구성(Cisco Unified CM Administration(Cisco Unified CM 관리) > Media Resources(미디어 리소스) > Conference Bridge(컨퍼런스 브리지) > Add New(새로 추가))



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*

- Save
- Delete
- Copy
- Reset
- Apply Config
- Add New

보안 전화회의 브리지 구성

작업 2. 보안 모드로 3 8865NR IP Phone을 등록합니다.

IP Phone에서 Device Security Profile(디바이스 보안 프로파일)을 Encrypted(암호화) 모드로 설정합니다.

Protocol Specific Information

Packet Capture Mode*

Packet Capture Duration

BLF Presence Group*

SIP Dial Rules

MTP Preferred Originating Codec*

Device Security Profile*

Rerouting Calling Search Space

SUBSCRIBE Calling Search Space

SIP Profile* [View Details](#)

Digest User

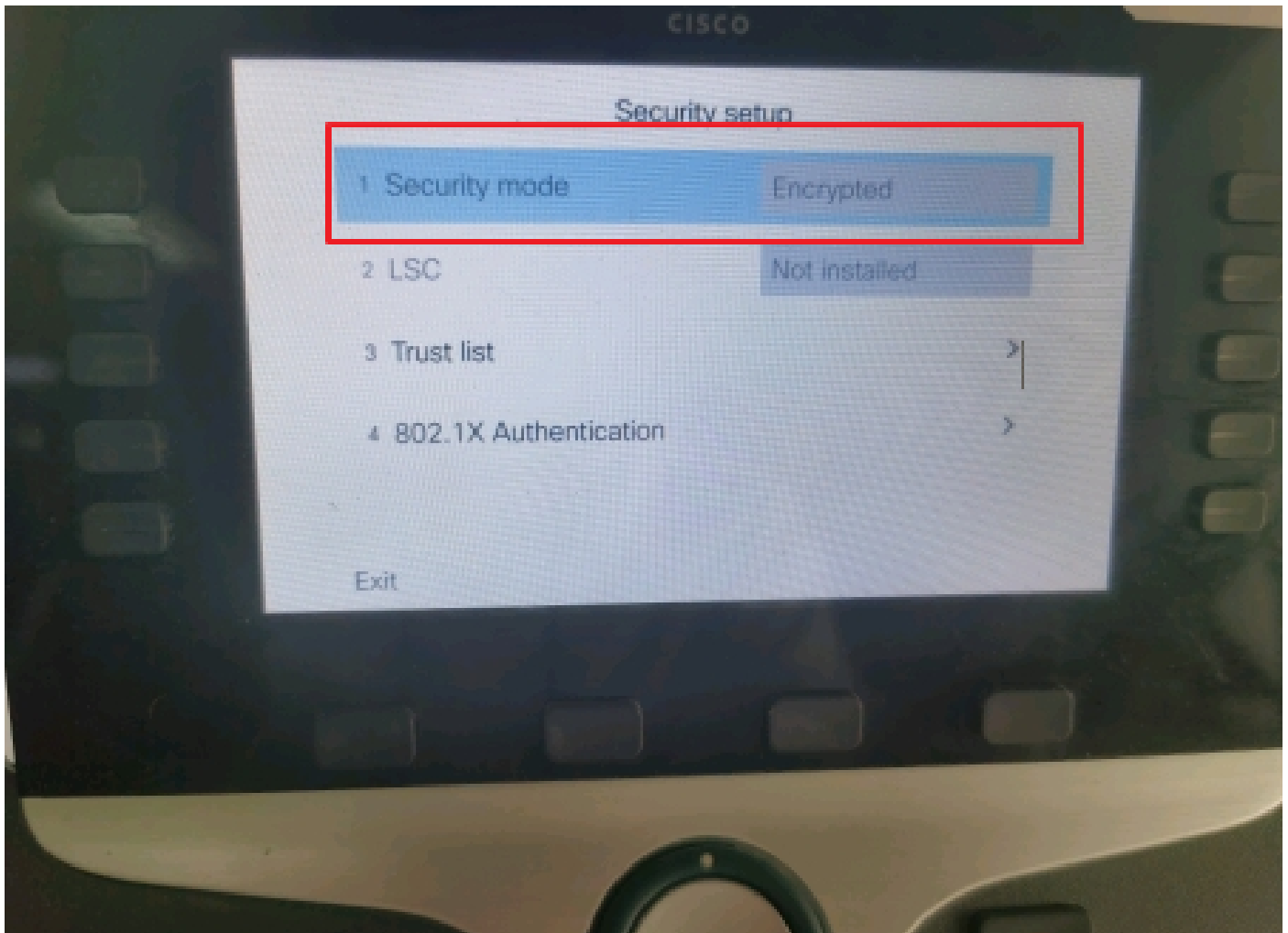
Media Termination Point Required

Unattended Port

Require DTMF Reception

디바이스 보안 프로필을 암호화 모드로 설정

IP Phone(IP 전화)은 Admin settings(관리 설정) > Security Setup(보안 설정)에서 Encrypted(암호화 됨)로 보안 모드를 표시합니다.




보안 모드가 암호화되었습니다.

작업 3. Secure Conference Bridge로 미디어 리소스 그룹 목록을 구성하고 IP Phone에 할당합니다.

1단계. 미디어 리소스 그룹 MRG_SecureCFB를 만들고 SecureCFB를 할당합니다(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*
SecureCFB (CFB)

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

미디어 리소스 그룹 MRG_SecureCFB 만들기

2단계. 미디어 리소스 그룹 목록 MRGL_SecureCFB를 만들고 여기에 MRG_SecureCFB를 할당합니다(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

미디어 리소스 그룹 목록 만들기 MRGL_SecureCFB

3단계. 모든 8865NR에 미디어 리소스 그룹 목록 MRGL_SecureCFB를 할당합니다.

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	Max M...	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 >"/>

미디어 리소스 그룹 목록 할당

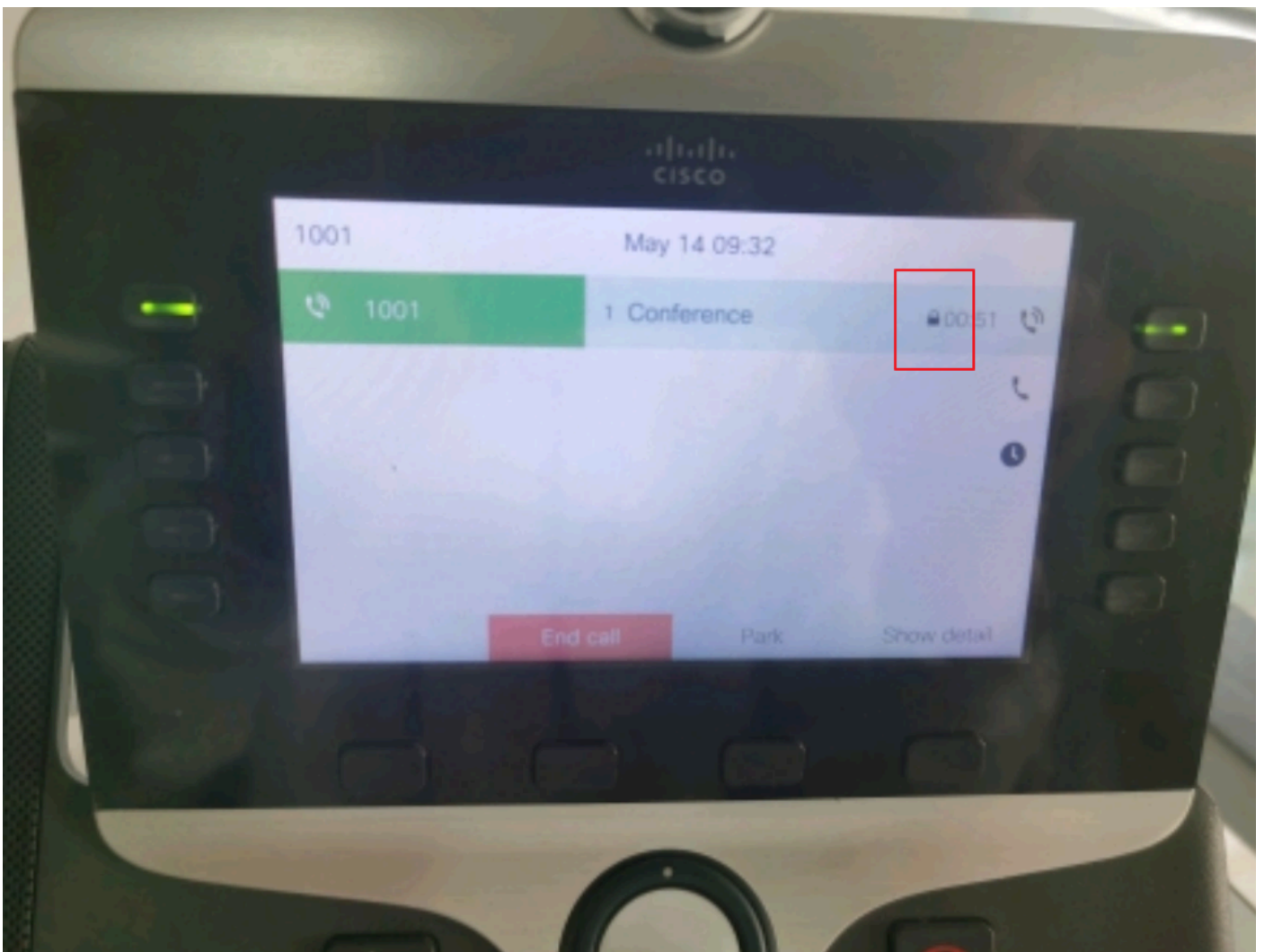
다음을 확인합니다.

IP Phone 1(DN 1001), IP Phone 2(DN 1002), IP Phone 3(DN 1003)

테스트 단계.

1. 1001. 1002에 전화
2. 1001 기자회견 소프트키 및 1003에 전화
3. 1001 보안 임시 회의를 포함하는 기자회견 소프트 키.

Cisco IP Phone은 통화가 암호화되었음을 나타내기 위해 전화회의 보안 아이콘을 표시합니다.



테스트 호출이 암호화되었습니다.

문제 해결

RTMT를 통해 다음 정보를 수집합니다.

Cisco CallManager(calllogs는 통화에 대한 정보를 제공하며 sdi 폴더에는 CUCM 추적이 포함됨)

SDL 추적에서는 1001 Press Conference 소프트 키가 1002 및 1003으로 전송될 때 1001에서 SIP REFER 메시지를 전송하는 것을 확인할 수 있습니다.

00018751.002 |17:53:18.056 |앱 정보 |SIPTcp - wait_SdlReadRsp: 포트 51320 인덱스 7의 x.x.x.x에서 2039바이트로 들어오는 SIP TCP 메시지:

[587,NET]

SIP: CUCMPUB15 SIP/2.0 참조

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

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

받는 사람: <sip:CUCMPUB15>

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

세션 ID: b14c8b6f00105000a000a4b439d38e15;remote=00000000000000000000000000000000

날짜: 2024년 5월 14일 화요일 09:53:17 GMT

CSeq: 1000 참조

사용자 에이전트: Cisco-CP8865NR/14.2.1

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

만료: 60

최대 전달: 70

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

참조자: "1001" <sip:1001@x.x.x.x>

참조: cid:3e94126b@x.x.x.x

콘텐츠 ID: <3e94126b@x.x.x.x>

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

Content-Length: 1069

Content-Type(콘텐츠 유형): application/x-cisco-remotecc-request+xml

Content-Disposition: 세션;처리=필수

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

<x-cisco-remotecc-request>

<softkeyeventmsg>

<softkeyevent>회의</softkeyevent>

<대화 상자>

<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>

<상담 대화 상자>

<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>

<조인디알가드>

<callid></callid>

<localtag></localtag>

<remotetag></remotetag>

</joindialogid>

<이벤트 데이터>

<invocationtype>명시적</invocationtype>

</eventdata>

<userdata></userdata>

<softkeyid>0</softkeyid>

<applicationid>0</applicationid>

</softkeyeventmsg>

</x-cisco-remotecc-request>

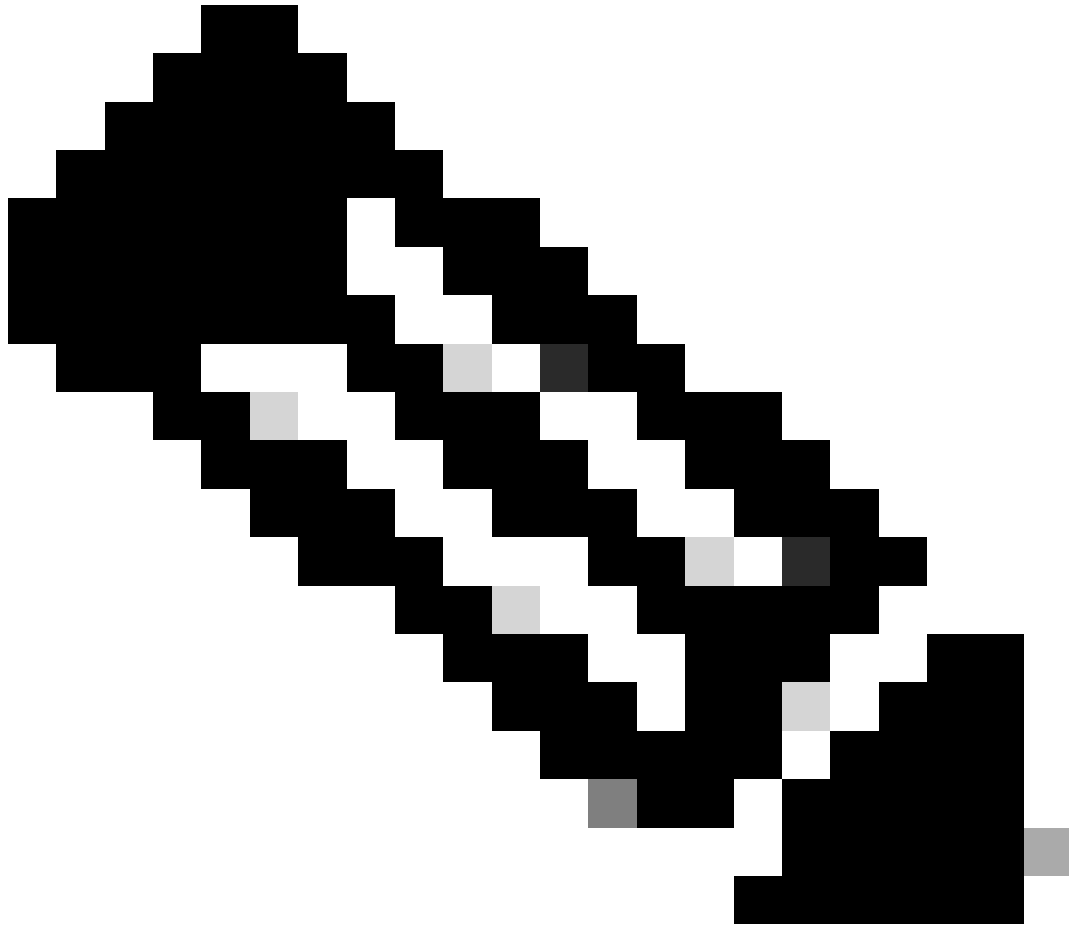
00018751.003 |17:53:18.056 |앱 정보 |SIPTcp - 신호 카운터 = 300

그런 다음 CUCM은 숫자 분석을 수행하고 마지막으로 디바이스 SecureCFB로 라우팅합니다.

```
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 이름: 4 유니코드 이름: pi: 0
encodeType=10 qsig-encodeType=10 ConnType=3 XferMode=8 ConnTime=3
nwLoc=0IpAddrMode=0 ipAddrType=0 ipv4.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 dev38281Cepn=1 d78f-46d6-8199-63297bcfddae lineCepn=
activeCaps=0 VideoCall=F MMUpdateCapMask=0x3e MMCap=0x1 SipConfig: BFCPAllowed=F
IXAllowed=F devCap=0 CryptoCapCount=6 secure=3 loginId= UnicodeName:
retriedVideo=FFromTag=ToTag=CallId= UAPortFlag=F wantDTFRecep=1 provOOB=0 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= deductBW=F fateShareId=
videoClass=Unspecified bridgeParticipantParticipantIDcallingCallingName= remoteClusterID=
isEMCCDevice=F dtmCall=F dtmPrimaryCI=0 dtmMediaFPid=(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 FAREndDevice NAME=LatENTCapS=NULL ICIDVal=
ICIDGenAddr= OIOI= TIOI= PTParAMS= CAL={v=-1, m=-1, tDev=F, res=F, devType=0}
displayNameUpdateFieldFlag=0 CFBCtrlSeclcon=F connBeforeANN=F 외부 프레젠테이션 정보 [
pi=0si1locale: 1 이름: UnicodeName: pi: 0 mlsCallExternal=F ] ControlProcessType=0
controlProcessTypeUpdateFieldFlag=1 origPi=0
```

관련 정보

- https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/security/15_0/cucm_b_security-guide-release-15.pdf
- [Cisco 기술 지원 및 다운로드](#)



참고: Secure Conference Over Trunks and Gateways Unified Communications Manager는 클러스터 내 트렁크(CT), H.323 트렁크/게이트웨이 및 MGCP 게이트웨이를 통한 보안 컨퍼런스를 지원합니다. 그러나 릴리스 8.2 이하를 실행 중인 암호화된 전화는 CT 및 H.323 통화에 대한 RTP로 되돌아가고 미디어는 암호화되지 않습니다. 전화회의에 SIPtrunk가 포함된 경우 보안 전화회의 상태는 비보안입니다. 또한 SIPtrunk 시그널링은 클러스터 외부 참가자에 대한 보안 전화회의 알림을 지원하지 않습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.