

Configureren van beveiligde ad-hocconferentie op CUCM 15

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft de configuratie van de beveiligde ad-hocconferentie op CUCM 15.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- CUCM
- VG (spraakgateway)
- Beveiligingsconcept

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- CUCM (mix mode) versie: 15.0.0.98100-196
- Cisco 2921 versie: 15.7(3)M4b (gebruikt als CA en Secure Conference Bridge)
- NTP-server
- 3 865NR IP-telefoon

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

Taak 1. Configureer beveiligde conferentiebrug en registreer deze naar CUCM.

Stap 1. Configuratie van publieke sleutelinfrastructuurserver en Trust Point.

Stap 1.1. Configureer de NTP-server en HTTP-server.

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

Stap 1.2. Configuratie van openbare sleutelinfrastructuurserver.

```
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
```

Stap 1.3. Stel Vertrouwingspunt in voor 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
```

Stap 1.4. Wacht ongeveer 30 seconden en geef de opdracht geen shutdown uit om testCA server in te schakelen.

```
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.
```

Stap 2. Configureer Vertrouwpunt voor Secure Conference Bridge en registreer dit om CA te testen.

Stap 2.1. Configureer Vertrouwpunt voor Secure Conference Bridge en geef deze de naam

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
```

Stap 2.2. Verifieer SecureCFB en typ 'ja' om het certificaat te aanvaarden.

```
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.
```

Stap 2.3. Noteer SecureCFB en stel een wachtwoord in.

```
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.
```

Stap 3. Configureer Vertrouwpunt voor CUCM op Secure Concerence Bridge.

Stap 3.1. Download het CallManager-certificaat van CUCM en kopieer het pem-bestand (Cisco Unified OS-beheer > Beveiliging > certificaatbeheer).


```
tDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAWIwHQYDVR0OBBYEFKriBeQi
OF6Hp0QCufVYzKWiXx2hMBIGA1UdEwEB/wQIMAYBAf8CAQAwDQYJKoZIhvcNAQEL
BQADggEBAJSw2vOwJ4UatmkaFpeLc9B1YZr8X6BkxBY1skW2qOLps61ysjDG61VQ
GjxpPLMY1ISyIvR5dqGyjaGLCUDUUCu66zEPxFNGnSYimBBhGR6NrDyo4YjOk+S
1I3TfRK+2F9NMhW2xTvuygoXLtyibvrZULhNo3vDPYQdTe1z54oQNU4BD8P+MCq9
+MzltCXEpVU6Jp71zC5HY+GF+Ab/xKBNzDjyY+OT8BFiO2wC8aaEaBvByNRzCSPD
MpU5cRaKvip2pszoR9mG3Rls4CkK93OX/OzFqklemDmY5WcylcCsybxAMbjdBDY9
err7iQZzjoW3eD5HxJKyVsfjDRtqg8=
-----END CERTIFICATE-----
```

Certificate has the following attributes:

```
Fingerprint MD5: 259A3F16 A5111877 901F00C8 F58C5CE3
Fingerprint SHA1: E4E91B76 B09C8BDF 81169444 BF5B4D77 E0738987
```

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

Stap 4. Configureer CUCM om de Secure Conference Bridge te vertrouwen.



Stap 4.1. Kopieert het certificaat voor algemene doeleinden en sla het op als een SecureCFB.pem-bestand. Kopieer het CA-certificaat en sla het op als testCA.pem-bestand.

```
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
A1UdDgQWBBSThajx/IQXHdNXfUswqYTZFhqnFjANBgkqhkiG9w0BAQQFAAOBgQAS
V8x9QjJ5pZKmezDYvxPDFe4chlKCD7o8JOcutSdAi7H+2Z+GO4CF55EDTZdLZPtn
GwQ01gbtDX07PTroYRWOSZLSJSdPQITJ3WDNR+NBhZjfe6EzfsLasD8L0VYG96GX
vjRQbdRmqbrG5H0ZUuZ0cu93AXjnRI2nLoAkKcrjcQ==
-----END CERTIFICATE-----
```

```
% General Purpose Certificate:
-----BEGIN CERTIFICATE-----
MIIB6jCCAvoGAWIBAgIBAJANBgkqhkiG9w0BAQUFADARMQ8wDQYDVQQDEwZ0ZXN0
Q0EwHhcNMjQwNTEwMDg1NTA4WWhcNMjcwNTEwMDg0NDI3WjAUMRIwEAYDVQQDEwIT
ZWN1cmVDRklwZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALhk11yOPnUNTjEQ
JLJIMPnoc6Zb9vDrGollMdsz/czWKTiGCS9PYYxwcpBExOOR+XrE9MmEO7L/tr6n
NkKz84ddWNz0gg6wHWM9gcje22blsleU6UCxo4ovra2pExXphusqEmg5yLQwyeJc
5JqcoAYXuRpnKLTfn5Nnh6iUCsWrAgMBAAGjTzBNMAsGA1UdDwQEAwIFoDAfBgNV
HSMEGDAWgBSThajx/IQXHdNXfUswqYTZFhqnFjAdBgNVHQ4EFgQU3y9zfDoTJ8WV
XlpX3wdcieq1zpkwDQYJKoZIhvcNAQEFBQADgYEABfaa6ppqRaDyfpW/tu5pXBRHP
SfZzpv+4ktsjAiOG7oGJGT0RpnuikCq+V2oucJbtWWAPbvX+ZBG3Eogi1c2GoDLK
yYvuaf9zBJHicM5mv6x81qxLF7FKZaepQSYwsQUP50/uKXa0435Kj/CZoLpKhXR2
v/p2jzF9zyPIBuQGEOEo=
-----END CERTIFICATE-----
```

Stap 4.2. Upload SecureCFB.pem naar CallManager-trust store op CUCM (Cisco Unified OS-beheer > Security > certificaatbeheer).

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.

Upload SecureCFB.pem

Stap 5. Configureer beveiligde vergaderbrug op 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
```

Stap 6. Configureer beveiligde conferentiebrug op CUCM (Cisco Unified CM-beheer > Media Resources > Conference Bridge > Add New).

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

Configureren van beveiligde vergaderbridge

Taak 2. Registreer 3 865NR IP-telefoons met beveiligingsmodus.

Stel het beveiligingsprofiel voor een apparaat in op de versleutelde modus op IP-telefoon.

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

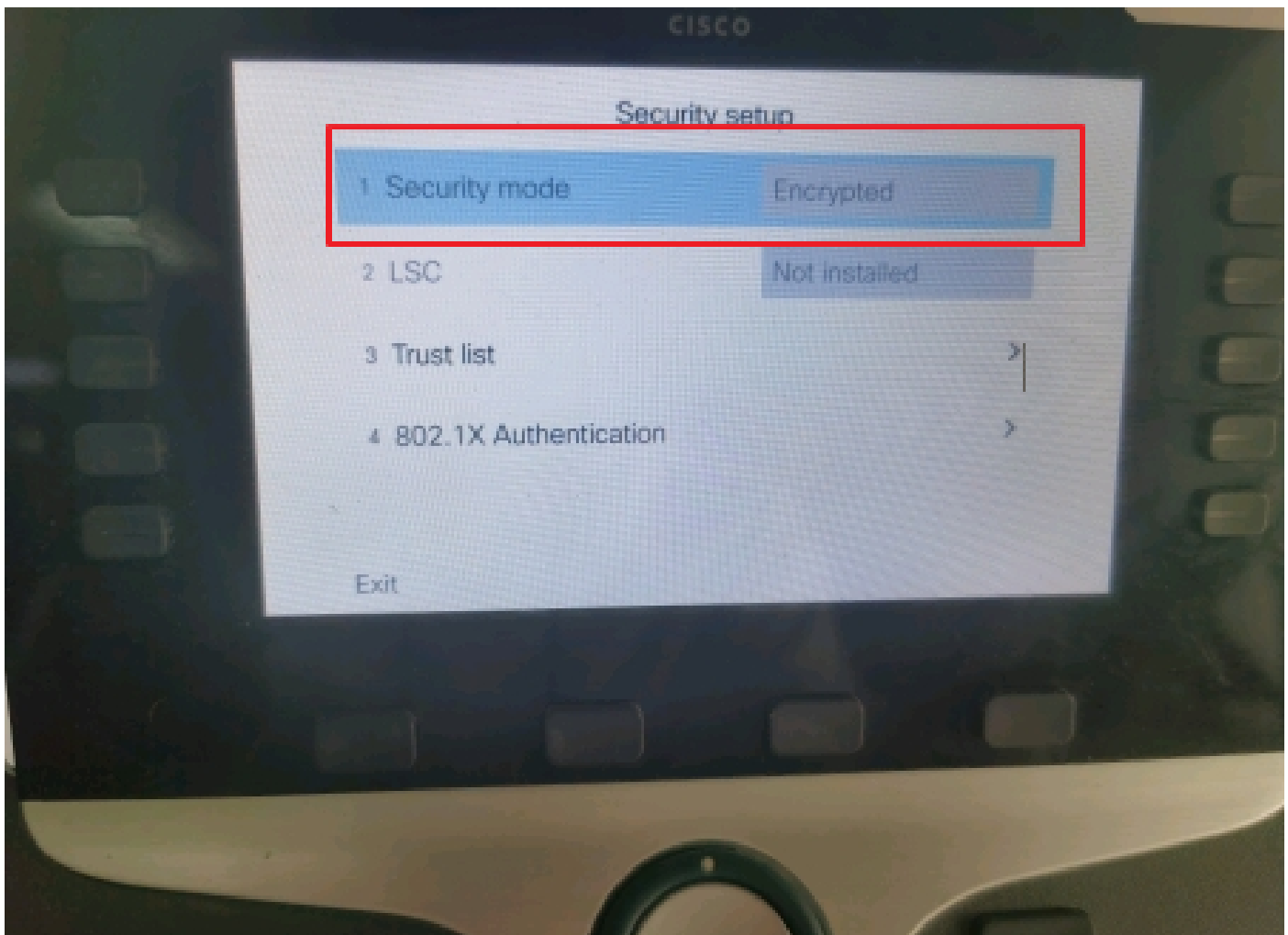
Unattended Port

Require DTMF Reception

Beveiligingsprofiel voor apparaat instellen op Versleutelde modus

IP-telefoon toont de beveiligingsmodus met Versleuteld onder Beheer instellingen > Security

Setup.




De security modus is versleuteld

Taak 3. Configureer de lijst met mediareources met Secure Conference Bridge en wijs deze toe aan de IP-telefoons.

Stap 1. Maak een Media Resource Group MRG_SecureCFB en wijs SecureCFB eraan toe (Cisco Unified CM-beheer > Media Resources > Media Resources groep).

Media Resource Group Configuration

 Save  Delete  Copy  Add New

 Status: Ready

Media Resource Group Status

Media Resource Group: SecureCFB (used by 0 devices)

Media Resource Group Information

Name*
Description

Devices for this Group

Available Media Resources**
ANN_2
ANN_4
CFB_2
CFB_4
IVR_2

Selected Media Resources*

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

Een mediagroep met resourcegroep MRG_SecureCFB maken

Stap 2. Maak een lijst met mediareources MRGL_SecureCFB en wijs MRG_SecureCFB eraan toe (Cisco Unified CM-beheer > Media Resources > Lijst met mediareources).

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

Een mediagroep maken MRGL_SecureCFB

Stap 3. Wijs de Media Resource Group List MRGL_SecureCFB toe aan alle 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 >"/>

Lijst met mediageresources toewijzen

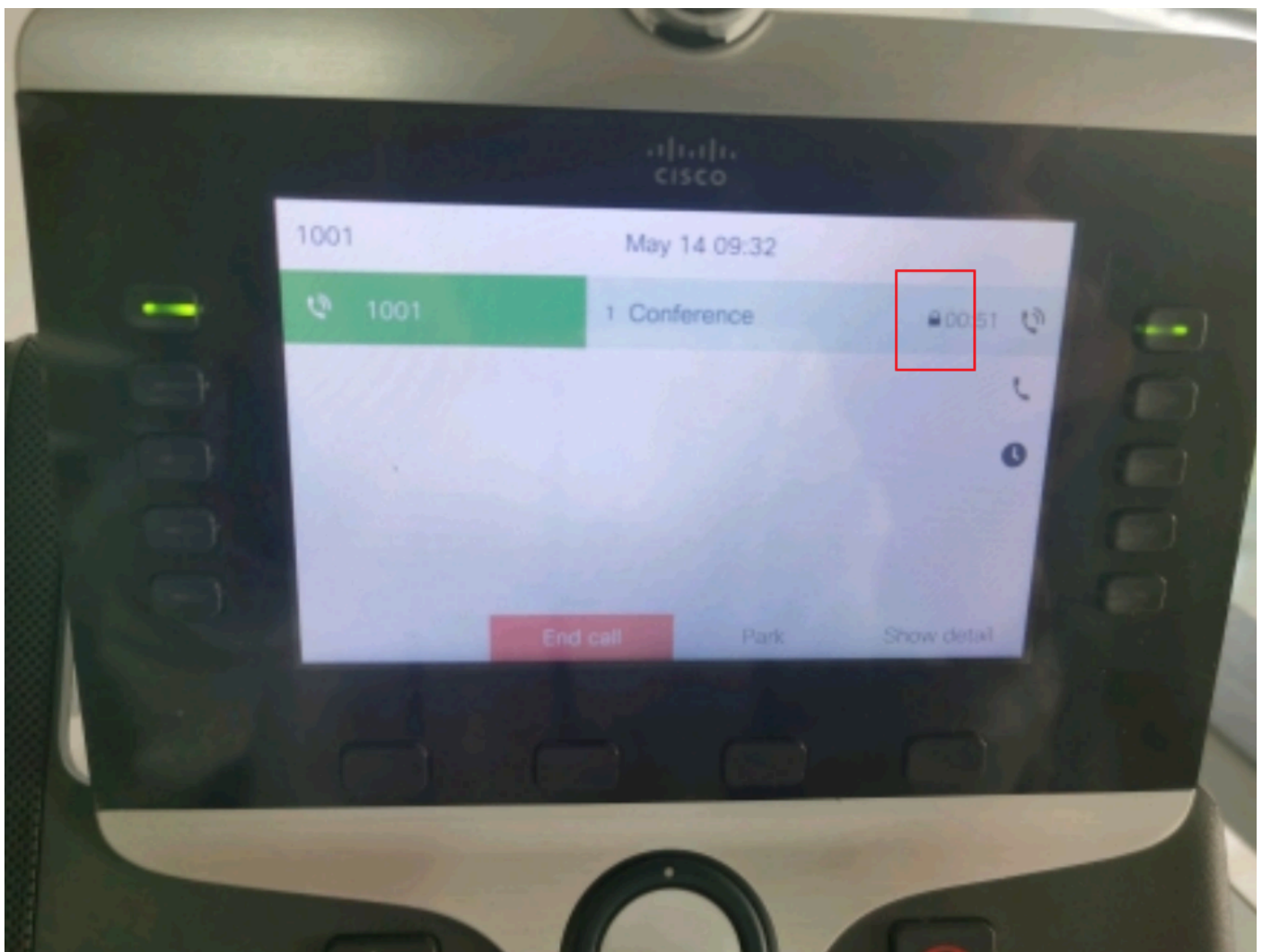
Verifiëren

IP-telefoon 1 met ISDN 1001, IP-telefoon 2 met DN 1002, IP-telefoon 3 met DN 1003.

Teststap.

1. 1001 oproep 1002.
2. 1001 persconferentie zachte sleutel en oproep 1003.
3. 1001 de zachte sleutel van de persconferentie om de Veilige Ad hoc Conferentie te impliceren.

Cisco IP-telefoons geven een pictogram voor conferentiebeveiliging weer om aan te geven dat de oproep is versleuteld.



De testoproep is versleuteld

Problemen oplossen

Verzamel de volgende informatie via RTMT.

Cisco CallManager (calllogs geeft informatie over de gesprekken, sdl-map bevat CUCM-sporen).

Uit het SDL-spoor blijkt dat 1001 een SIP REFER-bericht verstuurt als 1001 een zachte sleutel voor de persconferentie naar de conferenties 1002 en 1003.

00018751.002 | 17:53:18.056 |AppInfo |SIPTcp - wait_SdlReadRsp: Inkomend SIP TCP-bericht van x.x.x.x op poort 51320 index 7 met 2039 bytes:

[587,NET]

REFERENTIE SIP:CUMPUB15 SIP/2.0

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

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

Aan: <SIP:CUCMPUB15>

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

Session-ID:

b14c8b6f00105000a000a4b439d38e15;afstandsbediening=00000000000000000000000000000000

Datum: Tuin, 14 mei 2024 09:53:17 GMT

Nasdaq: 1000 REFERENTIE

User-Agent: Cisco-CP865NR/14.2.1

Aanvaarden: toepassing/x-cisco-remotecc-response+xml

Verloopt: 60

Max-voorwaarts: 70

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

Aanbevolen door: "1001" <SIP:1001@x.x.x.x>

Raadpleeg: cid:3e94126b@x.x.x.x

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

Toestaan: TERUG, BYE, ANNULEREN, UITNODIGEN, MELDEN, OPTIES, VERWIJZEN, REGISTREREN, BIJWERKEN, ABONNEREN

Content-Lengte: 1069

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

Content-Disposition: sessie;handling=vereist

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

<x-cisco-afstandsbediening-verzoek>

<softkeyeventsg>

<softkeyevent>Conferentie</softkeyevent>

<dialogid>

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

<localtag>a4b439d38e1500333f1eb5d4-68656916</localtag>

<remotetag>171~ca425666-d5e7-42a-a428-23de46063a5-17600290</remotetag>

</dialogid>

<linnumber>0</linnumber>

<participantnum>0</participantnum>

<dialogid van consultant>

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

<localtag>a4b439d38e15003562c2c59a-69dbf571</localtag>

<remotetag>176~ca425666-d5e7-42a-a428-23de46063a5-17600292</remotetag>

</dialogid van consultant>

<staat>vals</state>

<joindialogid>

<callid></callid>

<localtag></localtag>

<remotetag></remotetag>

</joindialogid>

<eventgegevens>

<invocationtype>expliciet</invocationtype>

</eventgegevens>

<userdata></userdata>

<softkeyid>0</softkeyid>

<applicatie-id>0</applicatie-id>

</softkeyeventmsg>

</x-cisco-Remote-request>

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

Dan, doet CUCM cijferanalyse en leidt tenslotte naar apparaat 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
Naam: 4 UnicodeName: pi: 0 encodeType=10 qsig-encodeType=10 ConnType=3 XferMode=8
ConnTime=3 nwLoc=0 drMode=0 ipAddrType=0 ipv4=x.x.x.x:0 regio=Default capCount=6
devType=1 mixerCId=16778218 mediaReq=0 portToPort.loc=0 MOH.MRGLPkid=
MOH.userHoldID=0 MOH.netHoldID=0 MOH.sup=1 devName=SECUREFB mobileDevName=
origEMCCallingDevName= mobilePartyNumber=pi=mobileCallType=0 Active=F ctiFarEndDev=1
ctiCCMId=1 devCepn=38281c14-d78f-46d6-8199-63297bcfdde-lijnCepn= activeCaps=0
VideoCall=F MUpdateCapMask=0x3e MMCap=0x1 SipConfig: BFCPAllows=F IXAllows=F
devCap=0 CryptoCapCount=beveiligd=6 ID= UnicodeName:
retryVideo=FFromTag=ToTag=CallId= UAPortFlag=F wantDTMFRecep=1 provOOB=0
ondersteuning DTMF=1 DTMF CFG=1 DTMF PT=() DTMF reqMed=1 isPrefAltScript=F
cdpnPatternUsage=2 audioPtyID=0 doNotAppendCSS=F callDP= BCUpdate=0
ccBearCapCapCapCSS=0 ccBearCap.l=0 ccBearCap.itr=0 protected=1 flushCapIns=0
geolocInfo=null locPkid= locName= deductBW=F fateShareID= videoTrafficClass=Niet
gespecificeerd bridgeParticipantID callUsr= remoteClusterID= isEMCCDevice=F dtmCall=F
dtmPrimaryCI=0 dtmMediaIFP=(0,0,0) dtmID NodeId=0 dtmMTPForDTMFTranslation=F emc=T
QSIGIMERoute=F eo=0Updt=1 vCTCUpdt=1 honecodec=F honingUpdt=1 finaleCallPartition=
cTypeUpdt=0 BibEnabled=0 OpnameQSIGAPDUSupported=F
FarEndDeviceName=LatentCaps=nullVal=GenAddr= oioi= tioi="Params= {v=-1, m=-1, tDev=F,
res=F, devType=0} displayNameUpdateFieldFlag=0 CFBCccSecIcon=F contentBeforeANN=F
externe presentatieinfo [pi=0si1locale: 1 Naam: UnicodeName: pi: 0 mlsCallExternal=F]
ControlProcessType=0 controleProcessTypeUpdateFieldFlag=1 origPi=0

Gerelateerde informatie

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



Opmerking: Secure Conference Over Trunks en Gateways Unified Communications Manager ondersteunt beveiligde conferentie via intracluster-trunks (ICT's), H.323-trunks/gateways en MGCP-gateways; versleutelde telefoons die release 8.2 of eerder gebruiken, keren echter terug naar RTP voor ICT- en H.323-gesprekken en de media worden niet versleuteld. Als een conferentie een SIP-trunk omvat, is de beveiligde conferentiestatus onveilig. Bovendien ondersteunt SIPtrunk-signalering geen beveiligde conferentiemeldingen aan deelnemers buiten het cluster.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.