Configurar conferência ad hoc segura no CUCM 15

Contents

Introdução

Este documento descreve a configuração da Secure Ad Hoc Conference no CUCM 15.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- CUCM
- VG (Gateway de voz)
- Conceito de segurança

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Versão do CUCM (modo misto): 15.0.0.98100-196
- CISCO2921 versão: 15.7(3)M4b (use como CA e Secure Conference Bridge)
- Servidor NTP
- 3 Telefone IP 865NR

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Tarefa 1. Configure o Secure Conference Bridge e registre no CUCM.

Etapa 1. Configurar o servidor de infraestrutura de chave pública e o Ponto de Confiança.

Etapa 1.1. Configure o servidor NTP e o 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
```

Etapa 1.2. Configurar o servidor de infraestrutura de chave 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
```

Etapa 1.3. Configure o ponto de confiança para 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
```

Etapa 1.4. Aguarde cerca de 30 segundos e execute o comando no shutdown para habilitar o 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.
```

Etapa 2. Configure o ponto de confiança para ponte de conferência segura e registre-o para testCA.

Etapa 2.1. Configure o ponto de confiança para Secure Conference Bridge e nomeie-o

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
```

Etapa 2.2. Autentique SecureCFB e digite 'yes' para aceitar o certificado.

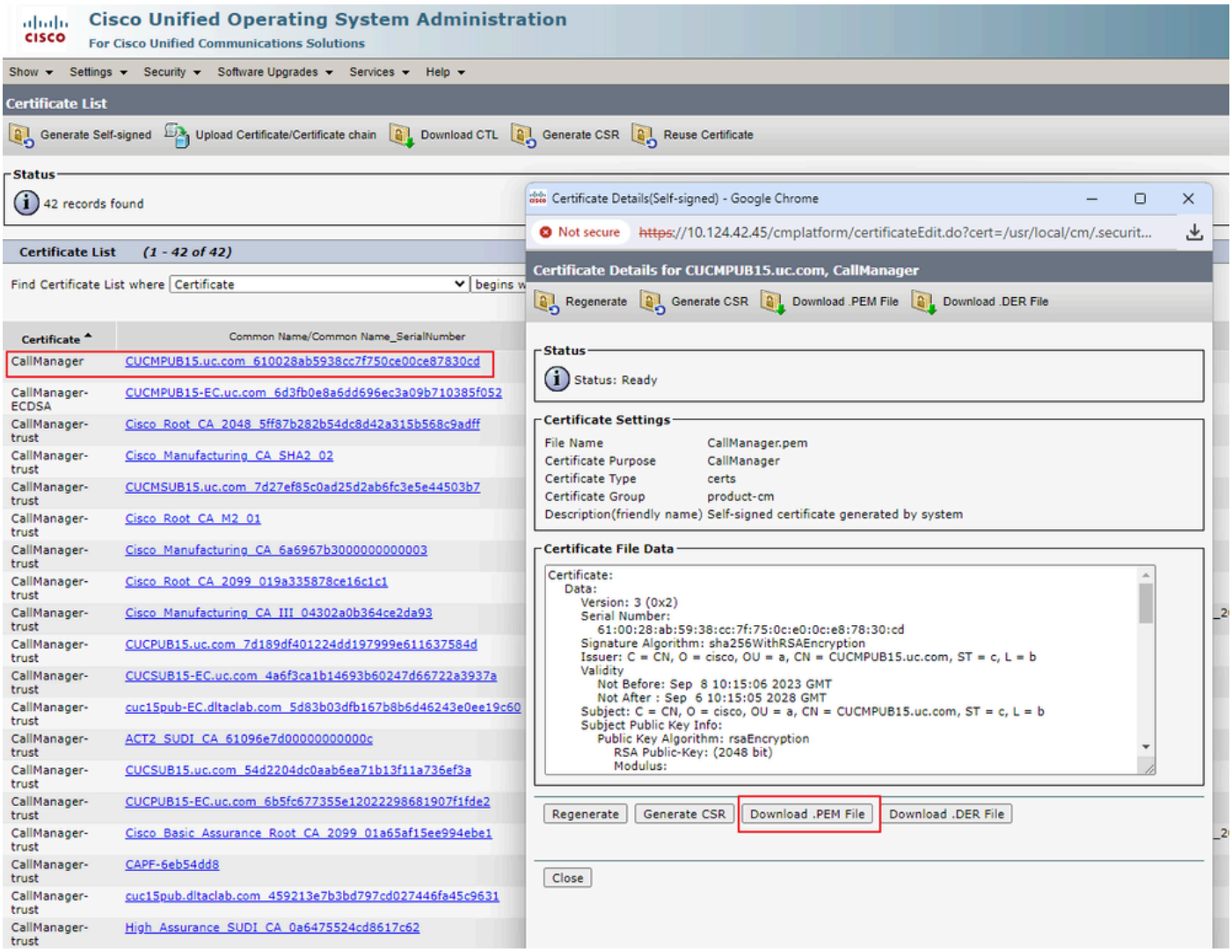
```
VG-CME-1(config)#crypto pki authenticate SecureCFB
Certificate has the following attributes:
      Fingerprint MD5: 383BA13D C37D0E5D 9E9086E4 8C8D1E75
     Fingerprint SHA1: 6DB8F323 14BBFBFF C36C224B B3404513 2FDD97C5

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

Etapa 2.3. Inscreva o SecureCFB e defina uma senha.

```
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.
```

Etapa 3. Configure o ponto de confiança para CUCM no Secure Concerence Bridge.

Etapa 3.1. Baixe o certificado do CallManager do CUCM e copie o arquivo pem (Cisco Unified OS Administration > Security > Certificate Management).



Baixar certificado do CallManager

Etapa 3.2. Configure o ponto de confiança, cole o arquivo pem e digite yes para aceitar o 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
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
```

Etapa 4. Configure o CUCM para confiar na ponte de conferência Secure.

Etapa 4.1. Copie o Certificado de Uso Geral e salve-o como um arquivo SecureCFB.pem. Copie o certificado CA e salve-o como o arquivo 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-----

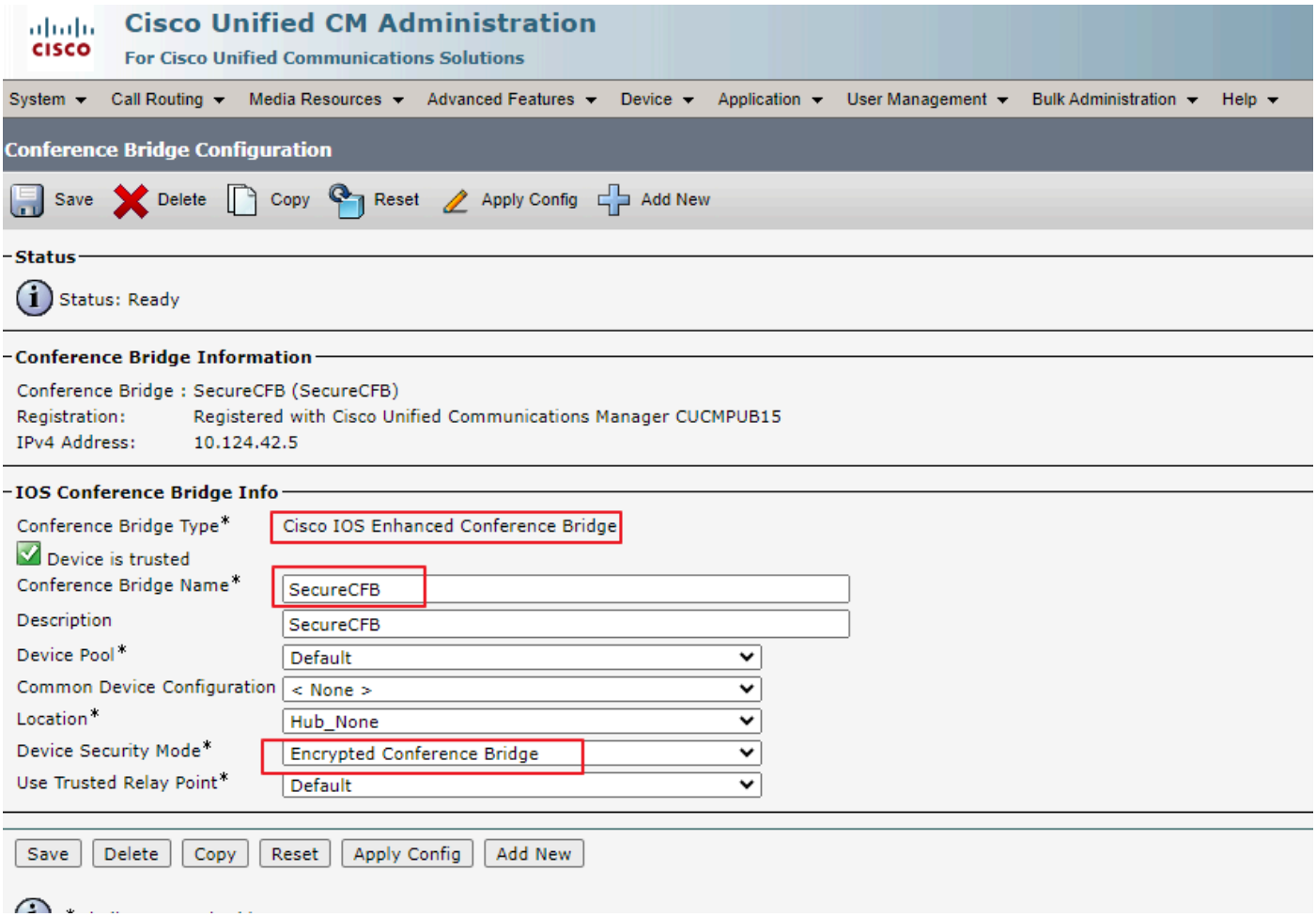
Etapa 4.2. Carregue o SecureCFB.pem no armazenamento CallManager-trust no CUCM (Cisco Unified OS Administration > Segurança > Gerenciamento de Certificado).

Carregar SecureCFB.pem

Etapa 5. Configure o Secure Conference Bridge no 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
```

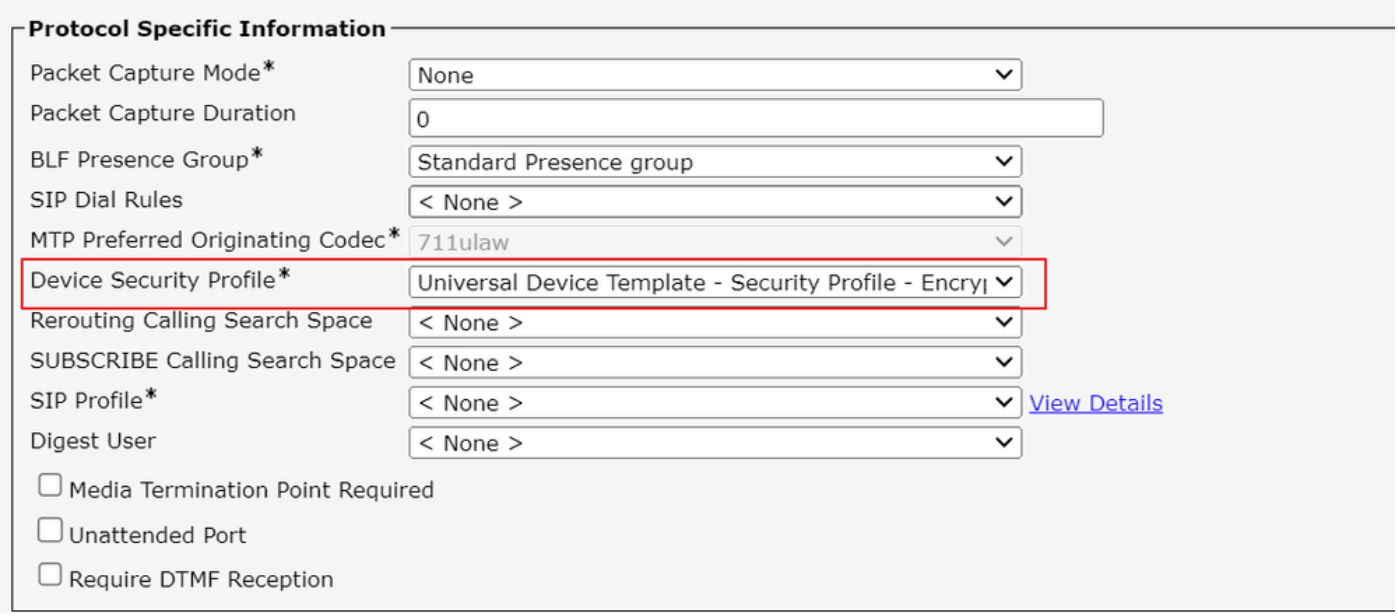
Etapa 6. Configure o Secure Conference Bridge no CUCM (Cisco Unified CM Administration > Recursos de mídia > Conference Bridge > Adicionar novo).



Configurar ponte de conferência segura

Tarefa 2. Registre 3 telefones IP 865NR com modo de segurança.

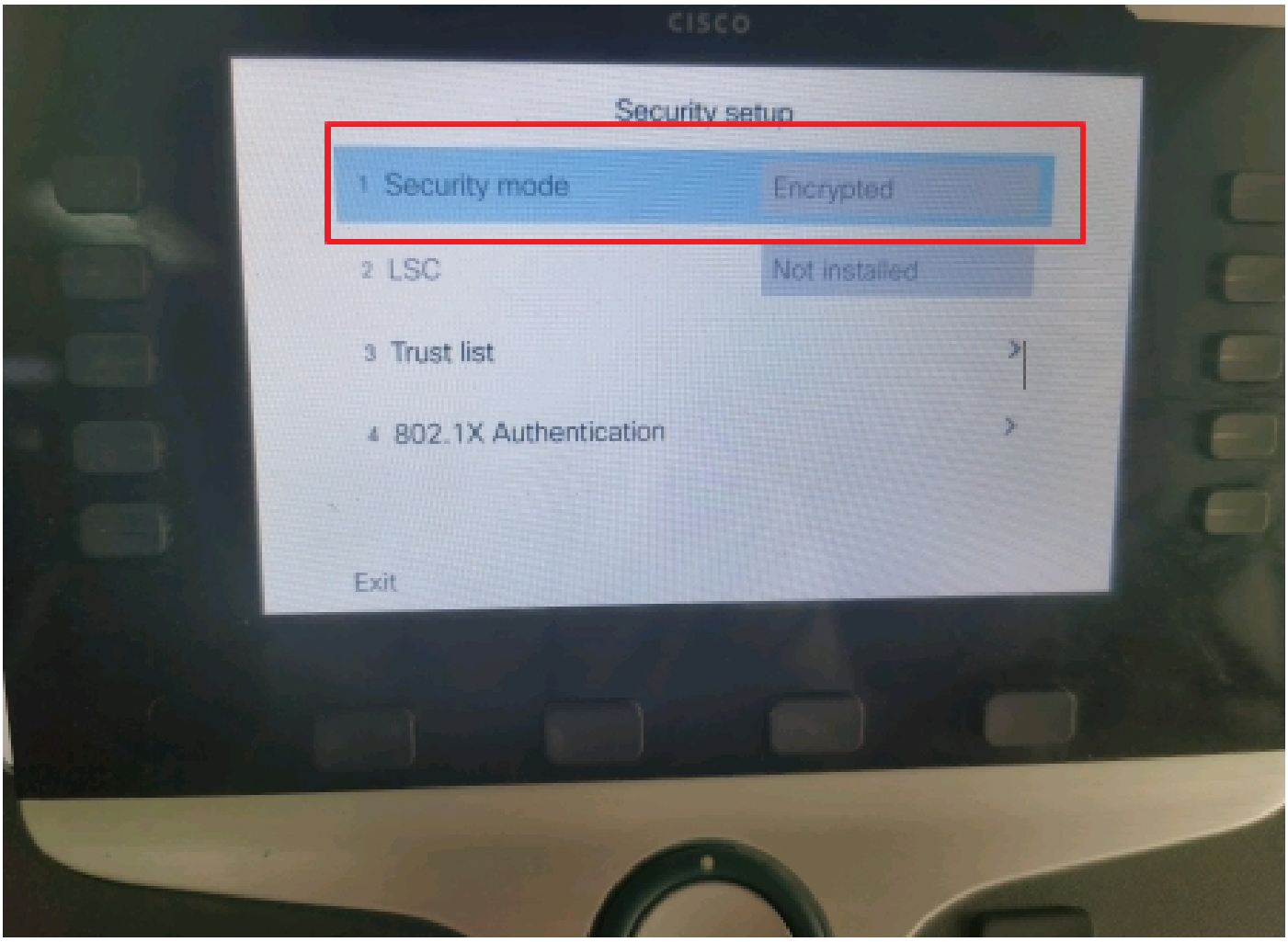
Defina o perfil de segurança do dispositivo para o modo criptografado no telefone IP.



Definir o perfil de segurança do dispositivo para o modo criptografado

O telefone IP mostra o modo de segurança com Criptografado em Configurações do

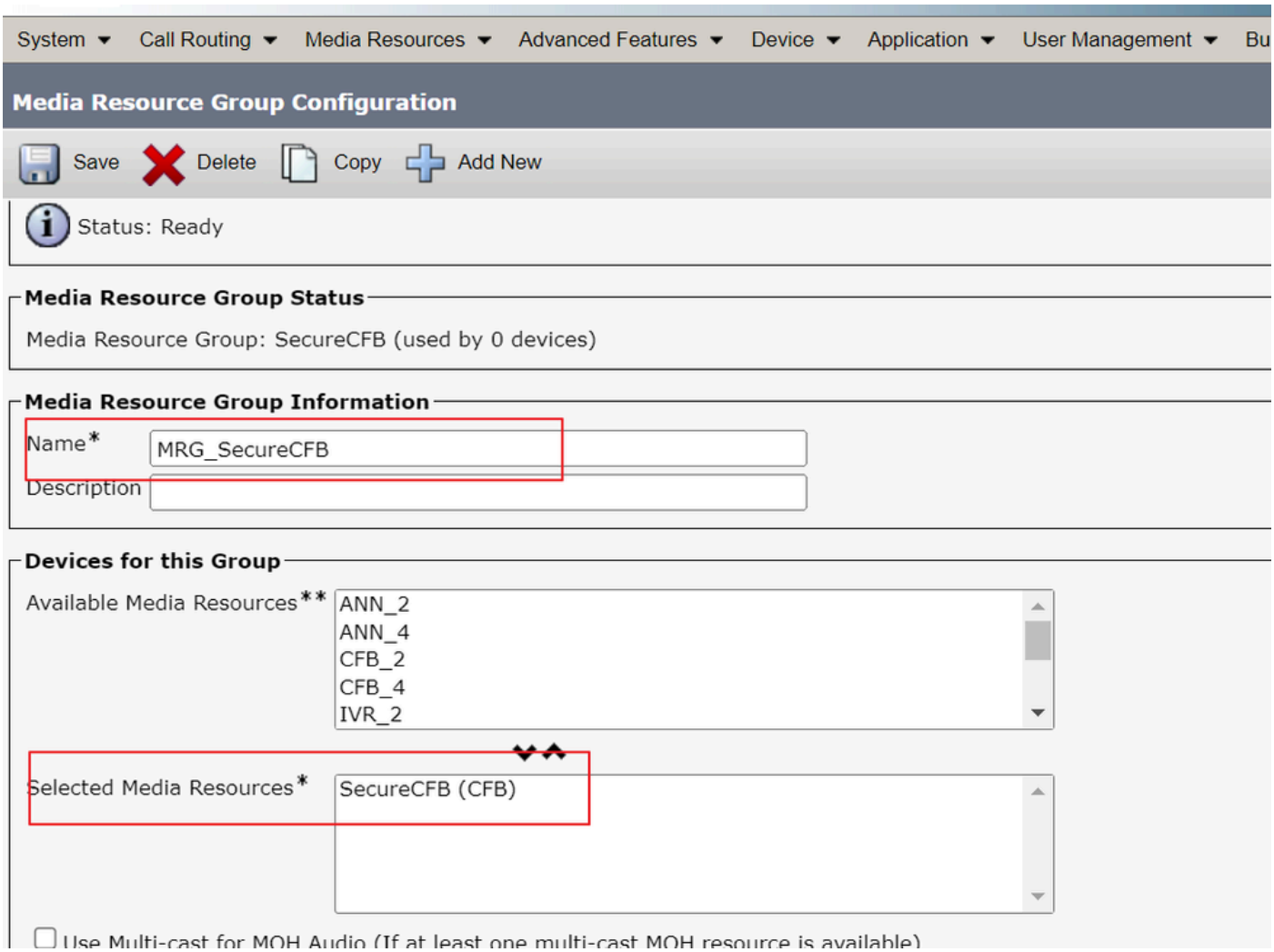
administrador > Configuração de segurança.



O modo de segurança foi criptografado

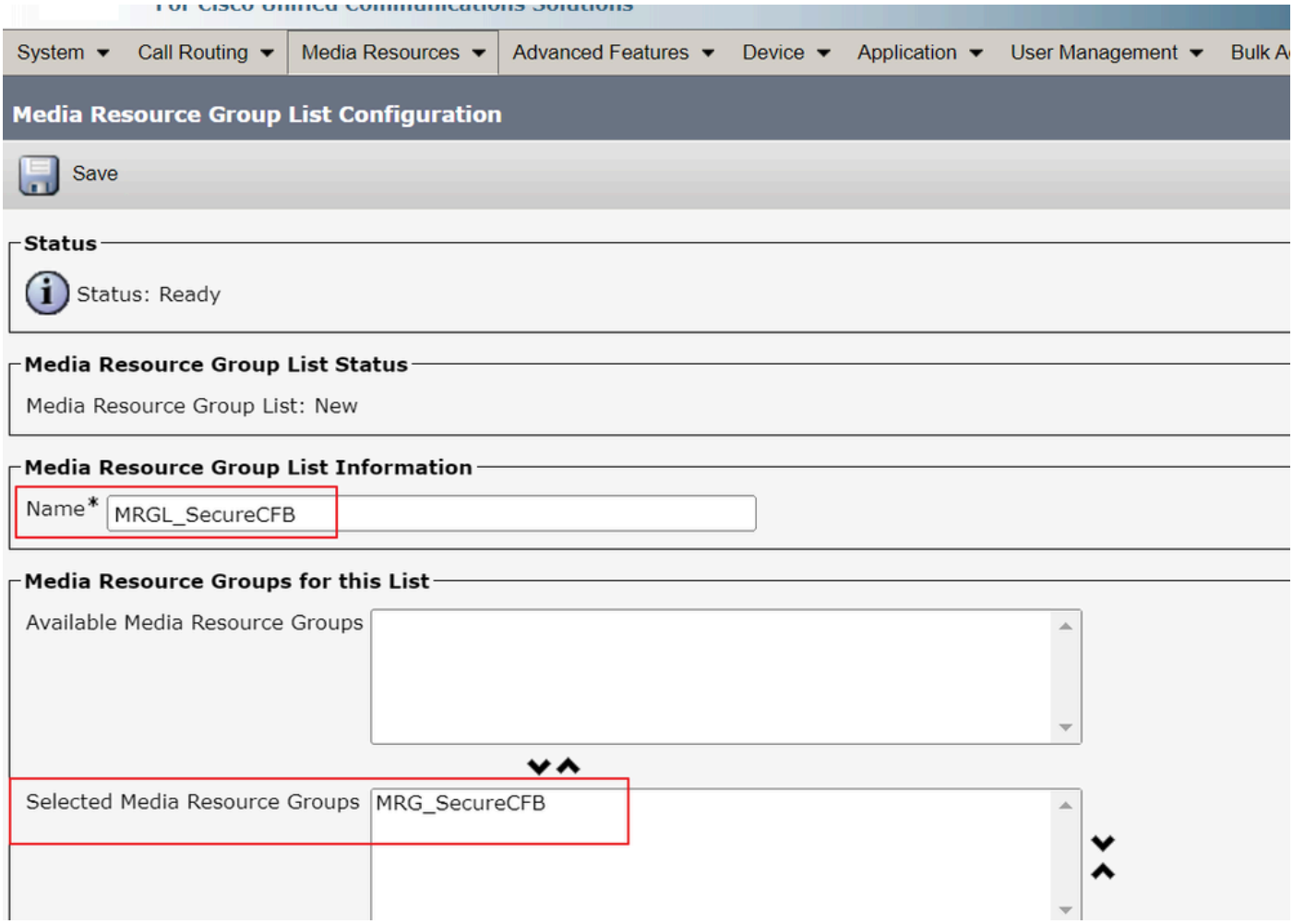
Tarefa 3. Configure a lista de grupos de recursos de mídia com ponte de conferência segura e atribua-a aos telefones IP.

Etapa 1. Crie um Grupo de Recursos de Mídia MRG_SecureCFB e atribua SecureCFB a ele (Cisco Unified CM Administration > Recursos de Mídia > Grupo de Recursos de Mídia).



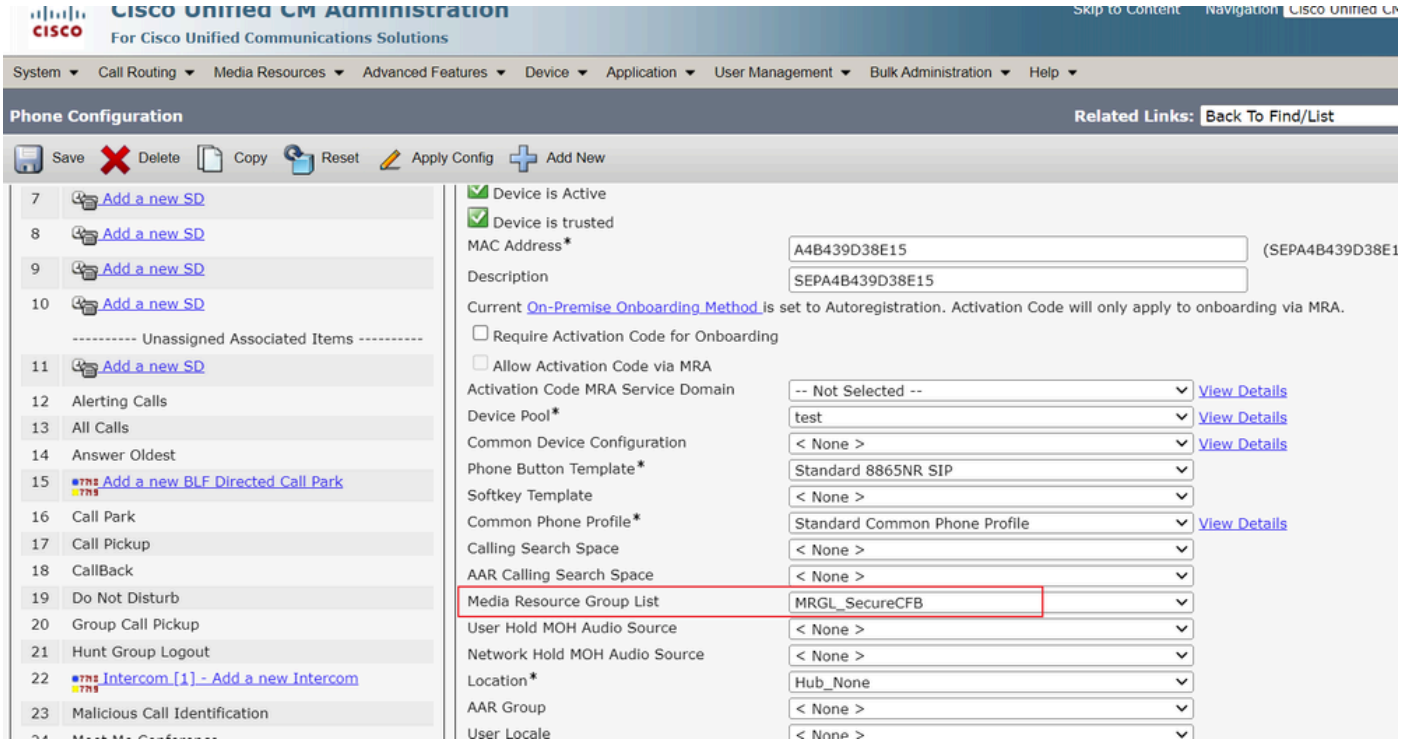
Crie um grupo de recursos de mídia MRG_SecureCFB

Etapa 2. Crie uma lista de grupos de recursos de mídia MRGL_SecureCFB e atribua MRG_SecureCFB a ela (Cisco Unified CM Administration > Recursos de mídia > Lista de grupos de recursos de mídia).



Criar uma lista de grupos de recursos de mídia MRGL_SecureCFB

Etapa 3. Atribua a lista de grupos de recursos de mídia MRGL_SecureCFB a todos os 865NR.



Atribuir lista de grupos de recursos de mídia

Verificar

Telefone IP 1 com DN 1001, Telefone IP 2 com DN 1002, Telefone IP 3 com DN 1003.

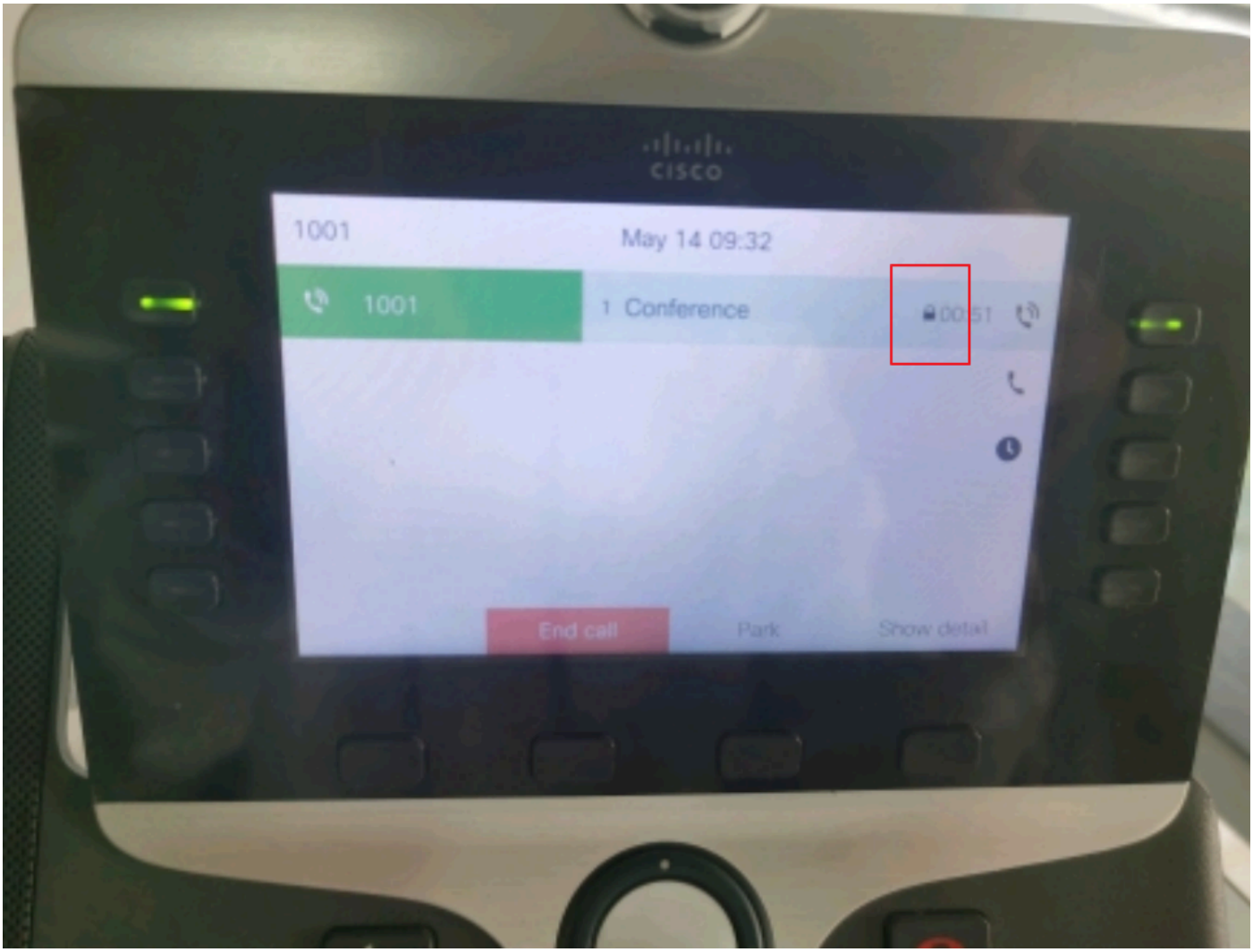
Etapa de teste.

1. 1001 ligue para 1002.

2. 1001 pressione a tecla virtual da conferência e ligue para 1003.

3. 1001 pressione a tecla virtual da conferência para envolver a Secure Ad Hoc Conference.

Os telefones IP da Cisco exibem um ícone de segurança de conferência para indicar que a chamada foi criptografada.



A chamada de teste foi criptografada

Troubleshooting

Colete as próximas informações via RTMT.

Cisco CallManager (registros de chamadas fornecem informações sobre as chamadas, a pasta

sdl contém rastreamentos CUCM).

A partir do rastreamento SDL, é visto que 1001 envia uma mensagem SIP REFER quando 1001 pressiona a tecla virtual da conferência para conferência 1002 e 1003.

00018751.002 |17:53:18.056 |InfoAplicativo |SIPTcp - wait_SdlReadRsp: mensagem SIP TCP de entrada de x.x.x.x no índice de 51320 da porta 7 com 2039 bytes:

[587,LÍQUIDO]

CONSULTE sip:CUCMPUB15 SIP/2.0

Via: 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 da chamada: a4b439d3-8e150010-2f865ab1-7160f679@x.x.x.x

ID da sessão: b14c8b6f00105000a000a4b439d38e15;remote=00000000000000000000000000000000

Data: Ter, 14 de maio de 2024 09:53:17 GMT

CSeq: 1000 REFER

Agente de usuário: Cisco-CP8865NR/14.2.1

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

Expira em: 60

Encaminhamentos Máximos: 70

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

Indicado por: "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

Comprimento do conteúdo: 1069

Tipo de conteúdo: application/x-cisco-remotecc-request+xml

Disposição de conteúdo: sessão;tratamento=necessário

```xml
<?xml version="1.0" encoding="UTF-8"?>
<x-cisco-remotecc-request>
  <softkeyeventmsg>
    <softkeyevent>Conferência</softkeyevent>
    <dialogid>
      <callid>a4b439d3-8e150007-1991b55f-00f9dcf7@x.x.x.x</callid>
      <localtag>a4b439d38e1500333f1eb5d4-68656916</localtag>
      <remotetag>171~ca425666-d5e7-42aa-a428-23dde46063a5-17600290</remotetag>
    </dialogid>
    <linenumber>0</linenumber>
    <participantnum>0</participantnum>
    <consultdialogid>
      <callid>a4b439d3-8e150008-415a60f5-7c35c82d@x.x.x.x</callid>
      <localtag>a4b439d38e15003562c2c59a-69dbf571</localtag>
      <remotetag>176~ca425666-d5e7-42aa-a428-23dde46063a5-17600292</remotetag>
    </consultdialogid>
    <state>falso</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-remotecc-request>
```

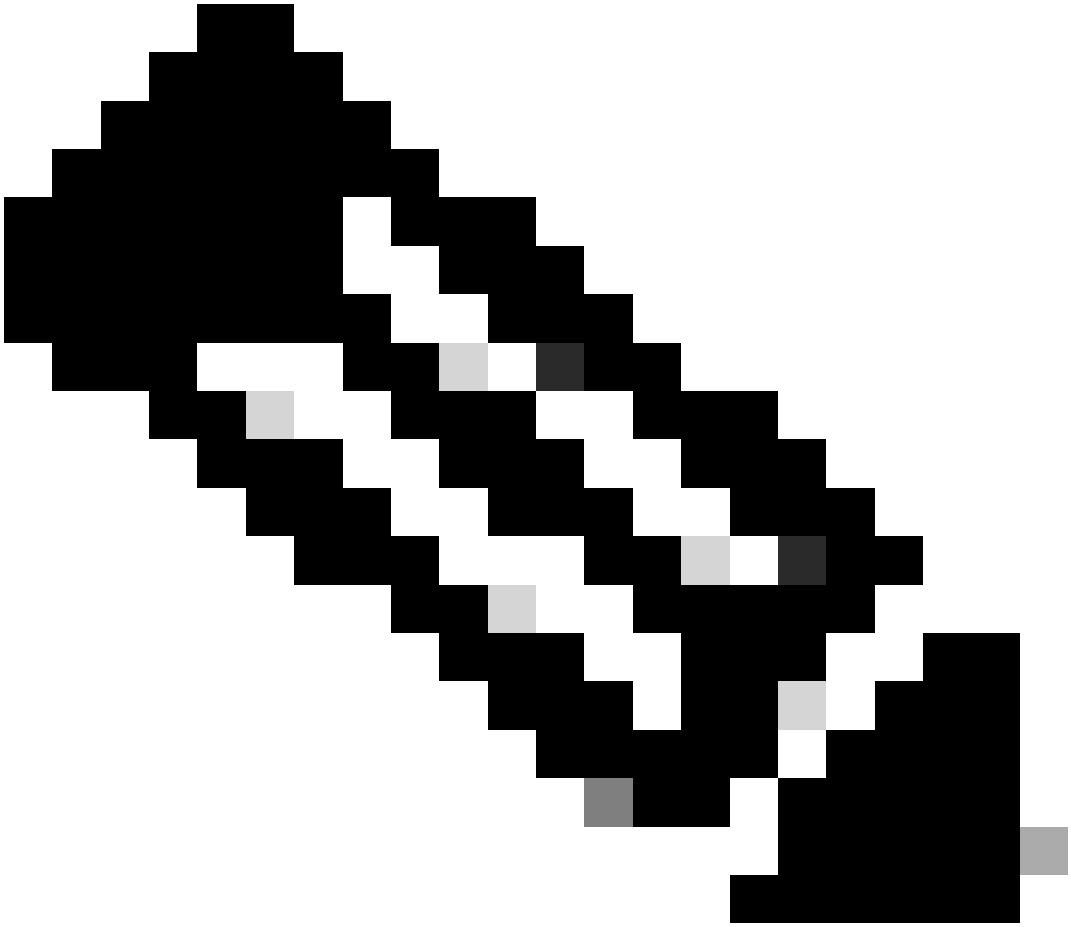

00018751.003 |17:53:18.056 |InfoAplicativo |SIPTcp - SignalCounter = 300

Em seguida, o CUCM faz a análise de dígitos e finalmente roteia para o SecureCFB do dispositivo.

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 wLoc=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= origEMCCCallingDev Nome= mobilePartyNumber=pi=0si1 mobileCallType=0 ctiActive=F ctiFarEndDev=1 ctiCCMId=1 devCepn=38281c14-d78f-46d6-8199-63297bcfddae lineCepn= ativeCaps=0 VideoCall=F MMUpdateCapMask=0x3e MMCap=0x1 SipConfig: BFCPA Permitido=F IXAllowed=F devCap=0 CryptoCapCount=6 secure=3 loginId= UnicodeName: retryVideo=FromTag=ToTag=CallId= UAPortFlag=F wantDTMFRecep=1 provOOB=0 supp DTMF=1 DTMF Cfg=1 DTMF PT=() DTMF reqMed=1 isPrefAltScript=F cdpn PatternUsage=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= deduztBW=F destinationShareId= videoTrafficClass=bridgeParticipantID não especificado callingUsr remoteClusterID= isEMCCDevice=F dtmCall=F dtmPrimaryCI=0 dtmMediaIFPid=(0,0,0,0) dtmMcNodeId=0 dtmMTPForDTMFTranslation=F emc=T QSIGIMERoute=F eo=0 eoUpdt=1 vCTCUpdt=1 honraCodec=F honraUpdt=1 finalCalledPartition= c TypeUpdt=0 BibEnabled=0 RecordingQSIGAPDUSupported=F FarEndDeviceName=LatentCaps=null icidVal= icidGenAddr= oioi= tioi= ptParams= CAL={v=-1, m=-1, tDev=F, res=F, devType=0} displayNameUpdateFieldFlag=0 CFBCtrlSecIcon=F connBeforeANN=F Informações de Apresentação Externa [pi=0 si1localidade: 1 Nome: UnicodeName: pi: 0 mIsCallExternal=F] ControlProcessType=0 controlProcessTypeUpdateFieldFlag=1 origPi=0

Informações Relacionadas

- https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/security/15_0/cucm_b_security-guide-release-15.pdf
- Suporte técnico e downloads da Cisco



Observação: o Secure Conference Over Trunks and Gateways Unified Communications Manager suporta conferência segura sobre troncos intracluster (ICTs), troncos/gateways H.323 e gateways MGCP; no entanto, os telefones criptografados que estiverem executando a versão 8.2 ou anterior revertem para RTP para chamadas ICT e H.323, e a mídia não é criptografada. Se uma conferência envolve um tronco SIP, o status de conferência seguro é não seguro. Além disso, a sinalização SIPtrunk não suporta notificações de conferência seguras para participantes fora do cluster.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.