

# Konfigurieren einer sicheren Ad-hoc-Konferenz auf CUCM 15

## Inhalt

---

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

---

## Einleitung

In diesem Dokument wird die Konfiguration der sicheren Ad-hoc-Konferenz auf CUCM 15 beschrieben.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- CUCM
- VG (Voice Gateway)
- Sicherheitskonzept

### Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- CUCM-Version (Mischmodus): 15.0.0.98100-196
- CISCO2921 Version: 15.7(3)M4b (als CA und Secure Conference Bridge verwenden)
- NTP-Server
- 3 IP-Telefon 8865NR

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

# Konfigurieren

Aufgabe 1: Konfigurieren von Secure Conference Bridge und Registrieren beim CUCM

Schritt 1: Konfigurieren Sie den Public Key-Infrastrukturserver und den Vertrauenspunkt.

Schritt 1.1: Konfigurieren des NTP- und HTTP-Servers

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

Schritt 1.2: Konfigurieren Sie den Public Key-Infrastrukturserver.

```
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
```

Schritt 1.3: Vertrauenspunkt für testCA konfigurieren

```
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
```

Schritt 1.4: Warten Sie etwa 30 Sekunden, und geben Sie dann den Befehl no shutdown ein, um den testCA-Server zu aktivieren.

```
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.
```

Schritt 2: Konfigurieren Sie Trust Point für Secure Conference Bridge, und registrieren Sie ihn für testCA.

Schritt 2.1: Konfigurieren Sie Trust Point für Secure Conference Bridge, und nennen Sie es

## 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
```

Schritt 2.2: Authentifizieren Sie SecureCFB, und geben Sie "yes" ein, um das Zertifikat zu akzeptieren.

```
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.
```

Schritt 2.3: Registrieren Sie SecureCFB, und legen Sie ein Kennwort fest.

```
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.
```

Schritt 3: Konfigurieren des Vertrauenspunkts für CUCM auf der sicheren Konferenzbrücke

Schritt 3.1: Laden Sie das CallManager-Zertifikat vom CUCM herunter, und kopieren Sie die PEM-Datei (Cisco Unified OS Administration > Security > Certificate Management).

The screenshot shows the Cisco Unified Operating System Administration interface. On the left, the 'Certificate List' is displayed with 42 records found. The first record, 'CallManager', is highlighted with a red box. Its details are shown in a pop-up window on the right. The 'Certificate Details' window shows the status as 'Ready' and provides options to regenerate, generate CSR, download PEM file, or download DER file. The 'Certificate File Data' section shows the following information:

```

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:

```

CallManager-Zertifikat herunterladen

Schritt 3.2: Konfigurieren Sie den Vertrauenspunkt, fügen Sie die PEM-Datei ein, und geben Sie yes ein, um das Zertifikat zu akzeptieren.

```

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
DwAwggEKAoIBAQD4Xfd9MwY/bSDXzGjtd301vYqKdRqVYpWD7E+Nrh7zRgHhz+
M7gAeqdRCSC/iKUF2g44rCRjIM0C/9xN3pxvOnNeqg/Tv0wjpHm0X2O4x0daH+F
AwEIWNyZzVUQ6+2xtkTuUcqeXDnnbS6fLladP/CfgQwKX5U1Ec575ypUet6Fp2n2
4UouLQ5iFEMmX9gzGR7YKjeE+t61X5NmvYc6lyP8MH77sgvti7+xJurJJUnvBFG2
ELXM0rL7uUoqw/rjMT6XxK+0Ft4bkOsVnjl+vOUUBUoTcbFFrsfrOnVQjPjHue
MLAaRzkDo5p1xo+UnNgv2uSH9HAID/NS1VTDAGMBAAGjYTBfMAsGA1UdDwQEAwIC

```

```
tDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAWlwHQYDVR0OBBYEFKriBeQi
OF6Hp0QCUfVYzKWiXx2hMBIGA1UdEwEB/wQIMAYBAf8CAQAwDQYJKoZIhvcNAQEL
BQADggEBAJSw2vOwJ4UatmkaFpeLc9B1YZr8X6BkxBY1skW2qOLps61ysjDG61VQ
GjxpPLMY1ISyIVr5dqGyjcaGLCUDUUCu66zEPxFNGnSYimBBhGR6NrDyo4YjOk+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

Schritt 4: Konfigurieren Sie CUCM so, dass die sichere Konferenz-Bridge vertrauenswürdig ist.

Schritt 4.1: Kopieren Sie das Zertifikat für allgemeine Dienste, und speichern Sie es als Datei SecureCFB.pem. Kopieren Sie das Zertifizierungsstellenzertifikat, und speichern Sie es als Datei testCA.pem.

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

```
% CA certificate:
```

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

```
MIIIBzCCAWSgAwIBAgIBATANBgkqhkiG9w0BAQQFADARMQ8wDQYDVQQDEwZ0ZXN0
Q0EwHhcNMjQwNTEwMDg0NDI3WhcNMjQwNTEwMDg0NDI3WjARMQ8wDQYDVQQDEwZ0
ZXN0Q0EwGZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAM2Lqils9nddFOx/YN7y
hhp9KGI2Eb8Zxq9E2mXfKpHOpcGEic5ain+rXf1qauA8/pNYwvBurAZm2pWzFHQ
q4qGL8KWDwJCPTwPI5rJOJAMIYzMH4WdQerWP4iEI2LGtxCb1q8b3w0wJE0Q2OG4
4kDSeArkKe0cb26WZC1oVK1jAgMBAAGjYzBhMA8GA1UdEwEB/wQFMAMBAf8wDgYD
VR0PAQH/BAQDAgGMB8GA1UdIwQYMBaAFJOFqPH+VBcd01d9SzcPhNkWGqcWMB0G
A1UdDgQWBBSThajx/IQXHdNXfUswqYTZFhqnFjANBgkqhkiG9w0BAQQFAA0BgQAS
V8x9Qj5pZKmezDYvxPDFe4chIkCD7o8JocutSdAi7H+2Z+GO4CF55EDTZdLZPtn
GwQ01gbtDX07PTroYRWOSZLSJSdPQITJ3WDNR+NBhZjfe6EzfsLasD8L0VYG96GX
vjRQbdRmqbrG5H0ZUUz0cu93AXjnRI2nLoAkKcrjcQ==
-----END CERTIFICATE-----
```



```
% General Purpose Certificate:
```

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

```
MIIIB6JCCAVOgAwIBAgIBAJANBgkqhkiG9w0BAQUFADARMQ8wDQYDVQQDEwZ0ZXN0
Q0EwHhcNMjQwNTEwMDg1NTA4WhcNMjQwNTEwMDg0NDI3WjAUMRIwEAYDVQQDEwIT
ZWN1cmVDRklwZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALhk11yOPnUNTjEQ
JLJIMPnoc6Zb9vDrGollMdsz/cZwKTiGcs9PYYxwcpBExOOR+XrE9MmEO7L/tR6n
NkKz84ddWNz0gg6wHWM9gcje22blsleU6UCxo4ovra2pExXphusqEmg5yLQwyeJc
5JqcoAYXuRpnKLTfn5Nnh6iUCsWrAgMBAAGjTzBNMAsGA1UdDwQEAwIFoDAfBgNV
HSMEGDAWgBSThajx/IQXHdNXfUswqYTZFhqnFjAdBgNVHQ4EFgQU3y9zfDoTJ8WV
XlpX3wdcieq1zpkwDQYJKoZIhvcNAQEFBQADgYEABfaa6ppRaDyfpW/tu5pXBRHP
SfZzpv+4ktsjAiOG7oGJGTORpnuiKCq+V2oucJBTWWAPvVx+ZBG3Eogi1c2GoDLK
yYvuaf9zBJHlcM5mv6x81qxLF7FKZaepQSYwsQUP50/uKXa0435Kj/CZoLpKhXR2
v/p2jzF9zyPIBuQGOEo=
-----END CERTIFICATE-----
```

Schritt 4.2: Laden Sie SecureCFB.pem in den CallManager-Vertrauensspeicher auf dem CUCM hoch (Cisco Unified OS-Verwaltung > Sicherheit > Zertifikatsverwaltung).

## 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 hochladen*

## Schritt 5: Konfigurieren von Secure Conference Bridge auf 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
```

## Schritt 6: Konfigurieren Sie Secure Conference Bridge auf dem CUCM (Cisco Unified CM-Verwaltung > Medienressourcen > Konferenzbrücke > Neu hinzufügen).

**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

Sichere Konferenzbrücke konfigurieren

Aufgabe 2: Registrieren Sie 3 8865NR IP-Telefone mit Sicherheitsmodus.

Setzen Sie das Gerätesicherheitsprofil auf dem IP-Telefon auf den verschlüsselten Modus.

**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

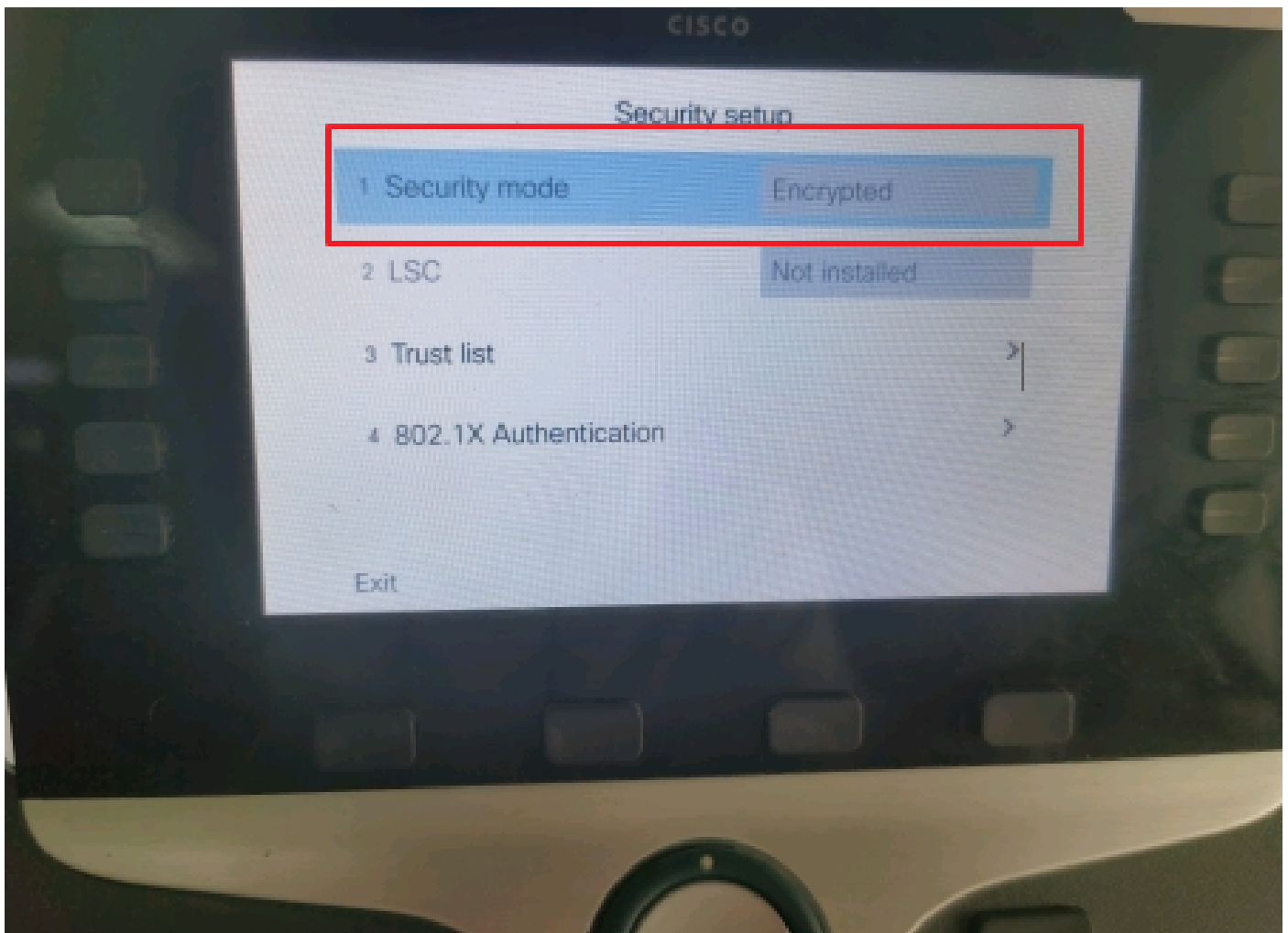
Unattended Port

Require DTMF Reception

Gerätesicherheitsprofil auf verschlüsselten Modus setzen

Auf dem IP-Telefon wird unter Admin settings > Security Setup (Admin-Einstellungen >

Sicherheitseinrichtung) der Sicherheitsmodus mit der Option Encrypted (Verschlüsselt) angezeigt.



Der Sicherheitsmodus war verschlüsselt.


**Aufgabe 3:** Konfigurieren Sie die Liste der Medienressourcengruppen mit Secure Conference Bridge, und weisen Sie sie den IP-Telefonen zu.

**Schritt 1:** Erstellen Sie eine Medienressourcengruppe MRG\_SecureCFB, und weisen Sie ihr SecureCFB zu (Cisco Unified CM-Verwaltung > Medienressourcen > Medienressourcengruppe).



## 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)

Erstellen einer Medienressourcengruppe MRG\_SecureCFB

Schritt 2: Erstellen Sie eine MRGL\_SecureCFB-Liste für Medienressourcengruppen, und weisen Sie dieser MRG\_SecureCFB zu (Cisco Unified CM-Verwaltung > Medienressourcen > Liste für Medienressourcengruppen).

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

Erstellen einer Medienressourcengruppen-Liste MRGL\_SecureCFB

Schritt 3: Weisen Sie allen 8865NR die MRGL\_SecureCFB-Liste der Medienressourcengruppen zu.

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	<a href="#">Add a new SD</a>	<input checked="" type="checkbox"/> Device Is Active
8	<a href="#">Add a new SD</a>	<input checked="" type="checkbox"/> Device is trusted
9	<a href="#">Add a new SD</a>	MAC Address* <input type="text" value="A4B439D38E15"/> (SEPA4B439D38E15)
10	<a href="#">Add a new SD</a>	Description <input type="text" value="SEPA4B439D38E15"/>
----- Unassigned Associated Items -----		
11	<a href="#">Add a new SD</a>	Current <a href="#">On-Premise Onboarding Method</a> 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 --"/> <a href="#">View Details</a>
15	<a href="#">Add a new BLF Directed Call Park</a>	Device Pool* <input type="text" value="test"/> <a href="#">View Details</a>
16	Call Park	Common Device Configuration <input type="text" value="&lt; None &gt;"/> <a href="#">View Details</a>
17	Call Pickup	Phone Button Template* <input type="text" value="Standard 8865NR SIP"/>
18	CallBack	Softkey Template <input type="text" value="&lt; None &gt;"/>
19	Do Not Disturb	Common Phone Profile* <input type="text" value="Standard Common Phone Profile"/> <a href="#">View Details</a>
20	Group Call Pickup	Calling Search Space <input type="text" value="&lt; None &gt;"/>
21	Hunt Group Logout	AAR Calling Search Space <input type="text" value="&lt; None &gt;"/>
22	<a href="#">Intercom [1] - Add a new Intercom</a>	Media Resource Group List <input type="text" value="MRGL_SecureCFB"/>
23	Malicious Call Identification	User Hold MOH Audio Source <input type="text" value="&lt; None &gt;"/>
		Network Hold MOH Audio Source <input type="text" value="&lt; None &gt;"/>
		Location* <input type="text" value="Hub_None"/>
		AAR Group <input type="text" value="&lt; None &gt;"/>
		User Locale <input type="text" value="&lt; None &gt;"/>

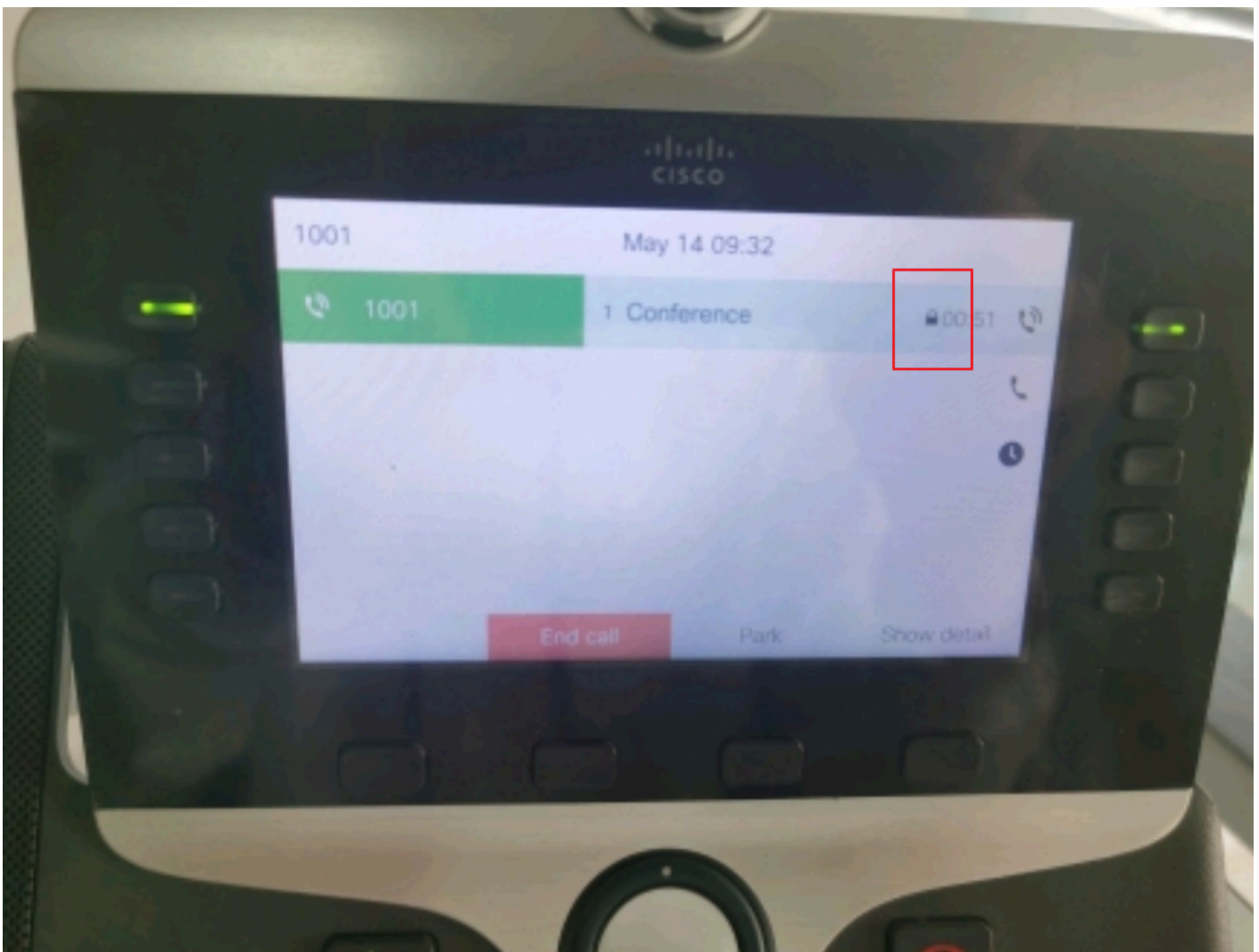
## Überprüfung

IP-Telefon 1 mit DN 1001, IP-Telefon 2 mit DN 1002, IP-Telefon 3 mit DN 1003

Testschritt.

1. 1001 Anruf 1002.
2. 1001 drücken Sie die Softtaste für die Pressekonferenz, und rufen Sie die 1003 an.
3. 1001 drücken Sie die Softtaste für die Pressekonferenz, um die sichere Ad-hoc-Konferenz einzubeziehen.

Cisco IP-Telefone zeigen ein Symbol für die Konferenzsicherheit an, um anzuzeigen, dass der Anruf verschlüsselt war.



Testanruf wurde verschlüsselt

## Fehlerbehebung

Sammeln Sie die nächsten Informationen per RTMT.

Cisco CallManager (Anrufprotokolle enthalten Informationen zu den Anrufen, der SDL-Ordner enthält CUCM-Ablaufverfolgungen).

Der SDL Trace zufolge sendet 1001 eine SIP REFER-Nachricht, wenn der Softkey 1001 für die Pressekonferenz an die Konferenznummern 1002 und 1003 gesendet wird.

00018751.002 | 17:53:18.056 |AppInfo |SIPTcp - wait\_SdlReadRsp: Eingehende SIP-TCP-Nachricht von x.x.x.x an Port 51320, Index 7, mit 2039 Byte:

[587,NET]

SIP BEACHTEN:CUCMPUB15 SIP/2.0

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

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

An: <sip:CUCMPUB15>

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

Sitzungs-ID:

b14c8b6f00105000a000a4b439d38e15;remote=00000000000000000000000000000000

Datum: Dienstag, 14. Mai 2024 09:53:17 Uhr GMT

CSeq: 1000 REFER

Benutzer-Agent: Cisco-CP8865NR/14.2.1

Akzeptieren: Anwendung/x-cisco-remote-response+xml

Gültig bis: 60

Max. Vorwärts: 70

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

Referenziert von: "1001" <sip:1001@x.x.x.x>

Siehe auch: cid:3e94126b@x.x.x.x

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

Zulassen: AKTIVIEREN, BYE, ABBRECHEN, EINLADEN, BENACHRICHTIGEN, OPTIONEN, REFER, REGISTRIEREN, AKTUALISIEREN, ABONNIEREN

Inhaltslänge: 1069

Inhaltstyp: Anwendung/x-cisco-remote-request+xml

Content-Disposition: session;handling=required

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

<x-cisco-remote-request>

<softkeyeventmsg>

<softkeyevent>Konferenz</softkeyevent>

<Dialog>

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

<localtag>a4b439d38e1500333f1eb5d4-68656916</localtag>

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

</dialogid>

<Linenummer>0</Linenummer>

<Teilnehmer>0</Teilnehmer>

<Gesprächsleitfaden>

<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>

<Ereignisdaten>

<invocationtype>Expliziter</invocationtype>

</eventdata>

```
<Benutzerdaten></Benutzerdaten>

<softkeyid>0</softkeyid>

<Anwendungs-ID>0</Anwendungs-ID>

</softkeyeventmsg>
```

```
</x-cisco-remote-request>
```

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

Anschließend führt der CUCM eine Ziffernanalyse durch und leitet das Gerät schließlich an SecureCFB weiter.

```
00018997.000 | 17:53:18.134 |SdlSigns |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 Unicode Name: 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 mixerCI d=16778218 mediaReq=0 portToPort.loc=0 MOH.MRGLPkid=
MOH.userHoldID=0 MOH.netHoldID=0 MOH.supp=1 devName=SECURECFB mobileDevName=
origEMCCallingDevName= mobilePartyNumber=pi=0si1 mobile CallType=0 ctiActive=F
ctiFarEndDev=1 ctiCCMId=1 devCepn=38281c14-d78f-46d6-8199-63297bcfd date lineCepn=
activeCaps=0 VideoCall=F MMUpdateCap Mask=0x3e MMCap=0x1 SipConfig: BFCPAllowed=F
IXAllowed=F devCap=0 CryptoCapCount=6 secure=3 loginId= UnicodeName:
retryVideo=FromTag=ToTag=CallId= UAPortFlag=F want DTMF Cfg=1 DTMF PT=() DTMF
reqMed=1 isPrefAltScript=F cdpnPatternUsage=2 audioPtyId=0 doNotAppendLineCSS=F
callsDP= BCUpp date=0 ccBearCap.itc=0 ccBearCap.l=0 ccBearCap.itr=0 protected=1
flushCapIns=0 geolocInfo=null locPkid= locName= deductBW=F fateShareId=
videoTrafficClass=Nicht angegebener BridgeTeilnehmer ID callsUsr= remoteClusterID=
isEMCCDevice=F dtmCall=F dtmPrimaryCI=0 dtmMediaFPid=(0,0,0,0) dtmMcNodeId=0
dtmMTPForDTMFTranslation=F emc=T QSIGIMER oute=F eo=0 eoUpdt=1 vCTCUpdt=1
honorCodec=F honorUpdt=1 finalCalledPartition= cTypeUpdt=0 BibEnabled=0
RecordingQSIGAPDUSupported=F FarEndDeviceName=LatentCaps=null icidVal= icid GenAddr=
oioi= tioi= ptParams= CAL={v=-1, m=-1, tDev=F, res=F, devType=0}
displayNameUpdateFieldFlag=0 CFBCtrlSecIcon=F connBeforeANN=F Externe Präsentationsinfo
[ pi=0si1locale: 1 Name: UnicodeName: pi: 0 mlsCallExternal=F ] ControlProcessType=0
controlProcessTypeUpdateFieldFlag=1 origPi=0
```

## Zugehörige Informationen

- [https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cucm/security/15\\_0/cucm\\_b\\_security-guide-release-15.pdf](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/security/15_0/cucm_b_security-guide-release-15.pdf)
- [Technischer Support und Downloads von Cisco](#)



Hinweis: Sichere Konferenzen über Trunks und Gateways Unified Communications Manager unterstützt sichere Konferenzen über Intercluster-Trunks (ICTs), H.323-Trunks/Gateways und MGCP-Gateways. Verschlüsselte Telefone mit Version 8.2 oder früher werden jedoch für ITK- und H.323-Anrufe auf RTP zurückgesetzt, und die Medien werden nicht verschlüsselt. Wenn eine Konferenz einen SIP-Trunk umfasst, ist der sichere Konferenzstatus nicht sicher. Darüber hinaus unterstützt die SIP-Trunk-Signalisierung keine sicheren Konferenzbenachrichtigungen für Teilnehmer außerhalb des Clusters.

---

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.