

Konfigurieren von Cisco Meeting Server und Ad-hoc-CUCM-Konferenzen

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Konfigurieren von CMS](#)

[Konfigurieren des CUCM](#)

[Überprüfen](#)

[Fehlerbehebung](#)

Einführung

Dieses Dokument beschreibt die Schritte zur Konfiguration von Ad-hoc-Konferenzen mit Cisco Meeting Server (CMS) und Cisco Unified Communications Manager (CUCM).

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- CMS-Bereitstellung und -Konfiguration
- CUCM-Endpunktregistrierung und Trunk-Erstellung
- Signierte Zertifikate

Verwendete Komponenten

- CUCM
- CMS Server 2.0.X und höher
- Webadmin- und Call Bridge-Komponenten müssen bereits im CMS konfiguriert sein.
- Interne DNS-Datensätze (Domain Name System) für Call Bridge und Webadmin, auflösbar in CMS-Server-IP-Adresse
- Interne Zertifizierungsstelle (Certificate Authority, CA), um das Zertifikat mit erweiterter Schlüsselverwendung von Webserver und Webclient-Authentifizierung zu signieren
- Signierte Zertifikate für Transport Layer Security (TLS)-Kommunikation

Hinweis: Selbstsignierte Zertifikate werden für diese Bereitstellung nicht unterstützt, da sie die Webserver- und Webclientauthentifizierung benötigen, die nicht in selbstsignierten Zertifikaten hinzugefügt werden kann

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen. Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt, es müssen jedoch die Mindestanforderungen an die Softwareversion erfüllt werden.

Konfigurieren

Konfigurieren von CMS

Schritt 1: Erstellen Sie ein Administratorbenutzerkonto mit API-Berechtigungen.

- Öffnen Sie eine Secure Shell (SSH)-Sitzung mit dem Mainboard Management Processor (MMP).
- Um ein Benutzerkonto auf Admin-Ebene hinzuzufügen, führen Sie den Befehl **user add <username> <role> aus.**
- Geben Sie das Passwort ein, wie im Bild gezeigt.

```
cb1> user add apiadmin admin
Please enter new password:
Please enter new password again:
Success
```

Schritt 2: Generieren Sie die Zertifikate.

- Führen Sie den Befehl **pki csr <Dateiname> CN:<Common Name> subjectAltName:<subject alternative names> aus.**
- Verwenden Sie die Informationen entsprechend Ihren Anforderungen.

```
Dateiname      zertrümmern
KN             tptac9.com
subjectAltName cmsadhoc.tptac9.com,10.106.81.32
```

- Verwenden Sie keine Platzhalter, um das Zertifikat zu generieren. Ein Zertifikat mit Platzhaltern wird vom CUCM nicht unterstützt.
- Stellen Sie sicher, dass das Zertifikat mit dem erweiterten Webserver und der Webclientauthentifizierung für die Schlüsselerzeugung signiert ist.

Hinweis: Um für alle Services dasselbe Zertifikat zu verwenden, muss der Common Name (CN) der Domänenname sein, und der Name der anderen CMS-Dienste muss als Subject Alternative Name (SAN) angegeben werden. In diesem Fall wird die IP-Adresse auch vom Zertifikat signiert und von jedem Computer, auf dem das Root-Zertifikat installiert ist, als vertrauenswürdig eingestuft.

Konfigurieren des CUCM

Schritt 1: Laden Sie die Zertifikate in den CUCM-vertrauenswürdigen Speicher hoch.

- Das Stammzertifikat kann von der internen Webschnittstelle der Zertifizierungsstelle heruntergeladen werden.

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, [install this CA certificate](#).

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA certificate:

Current [tptac9-WIN-TI6UAFTSEEV-CA-1] ▲

Encoding method:

- DER
 Base 64

[Install CA certificate](#)


[Download CA certificate](#)

- Fügen Sie das Call Bridge-Zertifikat und das Paketzertifikat (Zwischenstation und Root) zum CallManager-Vertrauensspeicher hinzu.

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*
 Description(friendly name)
 Upload File CA-cert.cer

 Upload  Close

Status

 Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster

Upload Certificate/Certificate chain

Certificate Purpose*
 Description(friendly name)
 Upload File certall.cer

Wenn Sie separate Zertifikate für Call Bridge und Webadmin haben, stellen Sie sicher, dass Sie Folgendes hochladen:

- Die Webadmin-, Anruf-Bridge- und Root-Zertifikate an Call Manager Trust Store auf CUCM

Hinweis: Der CUCM-SIP-Trunk kann als nicht sicherer SIP-Trunk erstellt werden. Wenn dies der Fall ist, muss das Anruf-Bridge-Zertifikat nicht in den CallManager-Vertrauensspeicher hochgeladen werden. Es muss jedoch das Root-Zertifikat hochladen, das das Webadmin-Zertifikat signiert hat.

Schritt 2: Konfigurieren eines sicheren SIP-Trunk-Profiles

- Öffnen Sie die CUCM-Webschnittstelle.
- Navigieren Sie zu **System > Security > SIP Trunk Security Profile**.
- Wählen Sie **Neu hinzufügen aus**
- Geben Sie die Werte mit den richtigen Informationen ein.

Name Geben Sie einen Namen ein, z. B. CMS-Trunk-32.

Gerätesicherheitsmodus Wählen Sie Verschlüsselt aus

Eingehender Transporttyp TLS auswählen

Ausgehender Transporttyp TLS auswählen

X.509-Betreffname Geben Sie den CN des Call Bridge-Zertifikats ein, und verwenden Sie separate Namen mit Kommas.

Eingehender Port Geben Sie den Port ein, an den TLS-Anfragen empfangen werden sollen. Der Standardwert ist 5061.

- Wählen Sie **Speichern**

SIP Trunk Security Profile Information	
Name*	CMS-Trunk-32
Description	10.106.81.32
Device Security Mode	Encrypted
Incoming Transport Type*	TLS
Outgoing Transport Type	TLS
<input type="checkbox"/> Enable Digest Authentication	
Nonce Validity Time (mins)*	600
X.509 Subject Name	cmsadhoc.tptac9.com,tptac9.com,10.106.81.32
Incoming Port*	5061

Schritt 3: SIP-Trunk erstellen

- Navigieren Sie zu **Gerät >Trunk**.
- Wählen Sie **Neu hinzufügen aus**
- Wählen Sie **SIP-Trunk** für den **Trunk-Typ aus**.
- **Weiter** auswählen
- Geben Sie die entsprechenden Werte ein.

Gerätename Geben Sie einen Namen für den SIP-Trunk ein, z. B. **CMS-Abhishek-32**.

Zieladresse Geben Sie die CMS-IP-Adresse oder den Call Bridge FQDN ein, z. B. **10.106.81.32**.

- Zielport** Geben Sie den Port ein, an dem das CMS die TLS-Kommunikation abhört, z. B. **5061**.
- SIP-Trunk-Sicherheitsprofil** Wählen Sie das in Schritt 2 erstellte sichere Profil aus, **CMS-Trunk-32**.
- SIP-Profil** Wählen Sie **Standard-SIP-Profil für TelePresence-Konferenzen** aus.

SIP Information

Destination Address is an SRV

Destination Address	Destination Address IPv6	Destination Port	Status	Status Reason	Duration
1* 10.106.81.32		5061	up		Time Up: 0 day 0 hour 0 minutes

MTP Preferred Originating Codec* 711ulaw

BLF Presence Group* Standard Presence group

SIP Trunk Security Profile* CMS-Trunk-32

Rerouting Calling Search Space < None >

Out-Of-Dialog Refer Calling Search Space < None >

SUBSCRIBE Calling Search Space < None >

SIP Profile* Standard SIP Profile For TelePresence Conferencing [View Details](#)

DTMF Signaling Method* No Preference

Schritt 4: Konferenzbrücke erstellen

- Navigieren Sie zu **Medienressourcen > Konferenzbrücke**.
- Neu hinzufügen
- Wählen Sie **Cisco TelePresence Conductor** aus dem Dropdown-Menü **Conference Bridge** aus.

Hinweis: Ab CUCM-Version 11.5.1 SU3 kann die **Cisco Meeting Server**-Option im Dropdown-Menü als **Conference Bridge Type (Konferenzbrücken)** ausgewählt werden.

- Geben Sie die richtigen Informationen ein.

Name der Konferenzbrücke

Geben Sie einen Namen für dieses Gerät ein, z. B. **CMS-Adhoc**

Beschreibung

Geben Sie eine Beschreibung für diese Konferenzbrücke ein, z. B. **10.106.81.32**.

SIP-Trunk

Wählen Sie den in Schritt 3 erstellten SIP-Trunk aus, **CMS-Abhi 32**.

SIP-Trunk-Ziel als HTTP-Adresse überschreiben

Aktivieren Sie dieses Kontrollkästchen, wenn ein anderer Name erforderlich ist.

Hostname/IP-Adresse

Geben Sie den Hostnamen oder die IP-Adresse des CMS ein, z. B. **10.106.81.32**.

Benutzername

Geben Sie den in CMS erstellten Benutzer mit API-Berechtigung ein, z. B. **admin**.

Kennwort

Geben Sie das Kennwort des API-Benutzers ein.

Kennwort bestätigen

Geben Sie das Kennwort erneut ein.

HTTPS verwenden

Aktivieren Sie das Kontrollkästchen. Dies ist für die CMS-Verbindung erforderlich.

HTTP-Port

Geben Sie den CMS-Webadmin-Port ein, z. B. **443**.

Conference Bridge Configuration
Relat

Save Copy Reset Apply Config Add New

Status

Status: Ready

Conference Bridge Information

Conference Bridge : CMS-Adhoc-32 (10.106.81.32)
 Registration: Registered with Cisco Unified Communications Manager CUCM115
 IPv4 Address: 10.106.81.32

Device Information

Conference Bridge Type* Cisco TelePresence Conductor
 Device is trusted
 Conference Bridge Name*
 Description
 Conference Bridge Prefix
 SIP Trunk*
 Allow Conference Bridge Control of the Call Security Icon

HTTP Interface Info

Override SIP Trunk Destination as HTTP Address

Hostname/IP Address

1

Username*
 Password*
 Confirm Password*

Use HTTPS

HTTP Port*

- Wählen Sie **Speichern**

Hinweis: Das Feld **Hostname (FQDN des CMS) und/oder IP-Adresse** muss im Webadmin-Zertifikat, im **Common Name** oder im Feld **Subject Alternative Name** enthalten sein, um eine sichere Verbindung zu ermöglichen.

- Öffnen Sie nach der Erstellung der Konferenzbrücke den Abschnitt **Cisco Unified Serviceability**.
- Navigieren Sie zu **Tools > Control Center - Feature Services**.
- Wählen Sie im Dropdown-Menü den CUCM Publisher-Knoten aus.
- **Gehe** auswählen
- Wählen Sie den **Cisco CallManager-Service** aus.
- Wählen Sie **Neustart** aus

Vorsicht: Wenn der CallManager-Dienst neu gestartet wird, bleiben die verbundenen Anrufe erhalten, aber einige Funktionen sind während dieses Neustarts nicht verfügbar. Es sind keine neuen Anrufe möglich. Der Neustart des Service dauert je nach CUCM-Workload etwa 5 bis 10 Minuten. Führen Sie diese Aktion mit Vorsicht durch und stellen Sie sicher, dass Sie sie während eines Wartungsfensters ausführen.

Schritt 5: Die CMS-Bridge wurde erfolgreich beim CUCM registriert.

- Gehen Sie zu **Medienressourcen > Medienressourcengruppe**.
- Klicken Sie auf **Neu hinzufügen**, um eine neue Medienressourcengruppe zu erstellen, und geben Sie einen Namen ein.
- Verschieben Sie die Konferenzbrücke (CMS) in diesem Fall aus dem Feld **Verfügbare Medienressourcen** in das Feld **Ausgewählte Medienressourcen**.
- Klicken Sie auf **Speichern**

Media Resource Group Configuration

Save Delete Copy Add New

Status

Status: Ready

Media Resource Group Status

Media Resource Group: CMS MRG (used by 45 devices)

Media Resource Group Information

Name* CMS MRG

Description

Devices for this Group

Available Media Resources**

ANN_2
CFB_2
IVR_2
MOH_2
MTP_2

Selected Media Resources*

cmslab1.acanotaclab.com (CFB)

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

Save Delete Copy Add New

Schritt 6: Fügen Sie die Medienressourcengruppen (MRGs) den Medienressourcengruppen-Listen (MRGLs) hinzu.

- Gehen Sie zu **Medienressourcen > Liste der Medienressourcengruppen**.
- Klicken Sie auf **Neu hinzufügen**, um eine neue Medienressourcengruppe zu erstellen, und geben Sie einen Namen ein, oder wählen Sie eine vorhandene MRGL aus, und klicken Sie auf diese, um sie zu bearbeiten.
- Verschieben Sie eine oder mehrere der im Feld **Verfügbare Medienressourcengruppen** erstellten Medienressourcengruppen in die **ausgewählten Medienressourcengruppen**.
- Klicken Sie auf **Speichern**

Media Resource Group List Configuration

Save Delete Copy Add New

Status
 Status: Ready

Media Resource Group List Status
 Media Resource Group List: CMS MRGL (used by 45 devices)

Media Resource Group List Information
 Name* CMS MRGL

Media Resource Groups for this List

Available Media Resource Groups
 CMS Cluster 1 MRGL
 CMS Cluster 2 MRGL
 CMS Cluster 3 MRGL
 CMS Cluster MRG
 softwareBridge

Selected Media Resource Groups
 CMS MRG

Save Delete Copy Add New

Schritt 7: Hinzufügen einer MRGL zu einem Gerätepool oder -gerät

Je nach Implementierung kann entweder ein Gerätepool konfiguriert und auf Endpunkte angewendet werden, oder ein einzelnes Gerät (ein Endpunkt) kann einer bestimmten MRGL zugewiesen werden. **Wenn eine MRGL sowohl für den Gerätepool als auch für einen Endpunkt angewendet wird, haben die Endpunkteinstellungen Vorrang.**

- Gehen Sie zu **System >> Gerätepool**
- Erstellen Sie einen neuen Gerätepool, oder verwenden Sie einen vorhandenen Gerätepool. Klicken Sie auf **Neu hinzufügen**.

Device Pool Configuration

Save

Status: Ready

Device Pool Information

Device Pool: New

Device Pool Settings

Device Pool Name*

Cisco Unified Communications Manager Group*

Calling Search Space for Auto-registration

Adjunct CSS

Reverted Call Focus Priority

Intercompany Media Services Enrolled Group

Roaming Sensitive Settings

Date/Time Group*

Region*

Media Resource Group List

Schritt 8: So fügen Sie dem Endpunkt einen Gerätepool hinzu und fügen dem Endpunkt MRGL hinzu

- Gehe zu **Gerät> Telefone**
- Klicken Sie auf **Suchen**, und wählen Sie das Gerät aus, um die Gerätepool-Einstellungen auf
- Anwenden des erstellten Gerätepools und der MRGL in den oben beschriebenen Schritten
- **Speichern, Konfig. übernehmen und zurücksetzen**

Neustarten und Registrieren des Endgeräts

Phone Configuration

Save Delete Copy Reset Apply Config Add New

Modify Button Items

1 [rns Line \[1\] - 6000 \(no partition\)](#)

----- Unassigned Associated Items -----

2 [rns Line \[2\] - Add a new DN](#)

Product Type: Cisco Spark Room Kit
Device Protocol: SIP

Real-time Device Status

Registration: Registered with Cisco Unified Communications Manager 10.104.215.207
IPv4 Address: [10.104.130.54](#)
Active Load ID: ce-9.3.1-61bfa3834f2-2018-05-04
Inactive Load ID: None
Download Status: None

Device Information

Device is Active
 Device is trusted
MAC Address*
Description
Device Pool* [View Details](#)
Common Device Configuration [View Details](#)
Phone Button Template*
Common Phone Profile* [View Details](#)
Calling Search Space
AAR Calling Search Space
Media Resource Group List

Schritt 9: Konfiguration auf einem Endgerät

- **Anmeldung** bei **Web-GUI** des Endgeräts
- Gehen Sie zu **Setup > Configuration > Conference > Multipoint Mode**
- Wählen Sie **CUCMediaResourceGroupList** aus

Multipoint Mode

CUCMMediaResourceGroupList

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

- Öffnen Sie die CUCM-Webschnittstelle.
- Navigieren Sie zu **Gerät > Trunks**.
- Wählen Sie den SIP-Trunk aus, der auf das CMS verweist.
- Stellen Sie sicher, dass sich die Trunks im Zustand **Full-Service** befinden.
- Navigieren Sie zu **Medienressource > Conference Bridge**.
- Wählen Sie die CMS-Konferenzbrücke aus.
- Stellen Sie sicher, dass sie mit CUCM registriert ist.

Ad-hoc-Anrufe tätigen

- Anruf von EndpunktA registriert für CUCM (MRGL hinzugefügt) an einem anderen EndpunktB
- Klicken Sie auf EndgerätA auf **Hinzufügen**, wählen Sie EndpunktC.
- Endgerät A wird zurückgestellt.
- Klicken Sie auf **Zusammenführen**
- Überprüfen der Verbindung der Anrufe in CMS
- Öffnen Sie die CMS-Webschnittstelle.
- Navigieren Sie zu **Status > Anrufe**.

Zum Testen wurden drei Endgeräte für Ad-hoc-Audio-/Videokonferenzen verwendet

Status	Configuration	Logs
Active Calls		
Filter	<input type="text"/>	<input type="button" value="Set"/> Show only calls with alarms <input type="button" value="Set"/>
Conference: 001036010001 (3 active calls)		
<input type="checkbox"/>	SIP 6000@acanotaclab.com [less] (incoming, unencrypted)	
	call duration	22 seconds
	incoming media	AAC (64.0 Kb/s), H.264, 1920 x 1080 29.9fps, 1.96 Mb/s
	outgoing media	OPUS, H.264, 1920 x 1080 29.9fps, 929 Kb/s
	additional protocols	unencrypted Active Control
	remote address	6000@acanotaclab.com
	SIP call ID	4b85f100-be01ff13-8efd1-cfd7680a@10.104.215.207
<input type="checkbox"/>	SIP abhi [less] (incoming, unencrypted)	
	call duration	22 seconds
	incoming media	AAC (64.0 Kb/s), H.264, 1920 x 1080 29.9fps, 1.94 Mb/s
	outgoing media	AAC, H.264, 1920 x 1080 30.3fps, 1.33 Mb/s
	additional protocols	unencrypted Active Control
	remote address	2333@acanotaclab.com
	SIP call ID	4b85f100-be01ff13-8efd3-cfd7680a@10.104.215.207
<input type="checkbox"/>	SIP sakatuka [less] (incoming, unencrypted)	
	call duration	22 seconds
	incoming media	AAC (64.0 Kb/s), H.264, 1920 x 1080 29.9fps, 1.94 Mb/s
	outgoing media	AAC, H.264, 1920 x 1080 29.9fps, 1.19 Mb/s
	additional protocols	unencrypted Active Control
	remote address	1105@acanotaclab.com
	SIP call ID	4b85f100-be01ff13-8efd2-cfd7680a@10.104.215.207

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.