

Configurer les conférences ad hoc pour le serveur de réunion Cisco et CUCM

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Configuration](#)

[Configurer CMS](#)

[Configurer le CUCM](#)

[Vérification](#)

[Dépannage](#)

Introduction

Ce document décrit les étapes pour configurer des conférences ad hoc avec le serveur de réunion Cisco (CMS) et le gestionnaire de communications unifiées de Cisco (CUCM).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Déploiement et configuration de CMS
- Enregistrement d'un point d'extrémité CUCM et création d'une ligne principale
- Certificats signés

Components Used

- CUCM
- Serveur CMS 2.0.x et version ultérieure
- Les composants de Webadmin et du pont d'appel doivent déjà être configurés sur CMS
- Les enregistrements internes du système de nom de domaine (DNS) pour le pont d'appel et Webadmin, pouvant mener à l'adresse IP du serveur CMS
- L'autorité de certification (CA) interne afin de signer le certificat avec usages de clé étendus (Extended Key Usage) pour l'authentification au serveur Web et au client Web.
- Certificats signés pour la communication avec la couche de sécurité pour le transport (Transport Layer Security ou TLS)

Note: Les certificats autosignés ne sont pas pris en charge pour ce déploiement, car ils nécessitent l'authentification au serveur Web et au client Web qu'il n'est pas possible d'ajouter dans les certificats autosignés

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes. Ce document n'est pas limité à des versions spécifiques du logiciel et du matériel; il faut toutefois que les exigences en matière de version minimale du logiciel soient satisfaites.

Configuration

Configurer CMS

Étape 1. Créez un compte d'utilisateur administrateur avec les privilèges API (Application Program Interface).

- Ouvrir une session SSH (Secure Shell) sur le processeur de gestion principal (MMP)
- Afin d'ajouter un compte d'utilisateur admin, exécutez la commande **useradd <username> <role>**
- Entrez votre mot de passe, comme le montre l'image :

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

Étape 2. Générez les certificats.

- Exécutez la commande **pki csr <nom du fichier> CN:<nom commun> subjectAltName:<noms alternatifs de sujet>**
- Utilisez les informations en fonction de vos exigences.

Nom de fichier certall

CN tptac9.com

subjectAltName cmsadhoc.tptac9.com,10.106.81.32

- N'utilisez pas les caractères génériques pour générer le certificat. Un certificat avec des caractères génériques n'est pas pris en charge par CUCM
- Assurez-vous que le certificat est signé avec une authentification au serveur Web et au client Web à usages de clé étendus (Extended Key Usage).

Note: Pour utiliser le même certificat pour tous les services, le nom usuel (CN) doit être le nom de domaine et le nom des autres services CMS doit être inclus en tant qu'autre nom du sujet (SAN). Dans ce cas, l'adresse IP est également signée par le certificat et tous les ordinateurs qui ont le certificat racine installé lui font confiance.

Configurer le CUCM

Étape 1. Téléchargez les certificats dans le magasin de confiance CUCM.

- Le certificat racine peut être téléchargé depuis l'interface Web interne Certificate Authority

(autorité de certification)

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](#)

- Ajouter le certificat du pont d'appel et le certificat de l'offre groupée (intermédiaire et racine) au magasin CallManager-trust

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*

CallManager-trust ▾

Description(friendly name)

Upload File

Choose File CA-cert.cer

Upload

Close

 Upload  Close

Status



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

Upload Certificate/Certificate chain

Certificate Purpose*

CallManager-trust ▾

Description(friendly name)

Upload File

Choose File certall.cer

Upload

Close

Si vous avez des certificats distincts pour Call Bridge et Webadmin, assurez-vous de télécharger :

- Magasin d'approbation Webadmin, Call Bridge et Root Certificate vers Call Manager sur CUCM

Note: La ligne principale SIP de CUCM peut être créée en tant que ligne principale SIP non sécurisée; si c'est le cas, il n'est pas obligatoire de téléverser le certificat du pont d'appel au stockage de confiance CallManager-trust store, mais il est nécessaire de téléverser le certificat racine ayant signé le certificat webadmin au stockage de confiance CallManager-trust store.

Étape 2. Configurez un profil de liaison SIP sécurisé.

- Ouvrez l'interface Web de CUCM
- Naviguez jusqu'à **System > Security > SIP Trunk Security Profile (Système > Sécurité > Profil de sécurité de la ligne principale SIP)**
- Sélectionnez **Add New (ajouter nouveau)**
- Entrez les valeurs avec les informations adéquates

Name (nom)	Entrez un nom, par exemple CMS-Trunk-32
(Device Security Mode) Mode de sécurité du périphérique	Sélectionnez Encrypted (chiffré)
Incoming Transport Type (type de transport entrant)	Sélectionnez TLS
Outgoing Transport Type (type de transport sortant)	Sélectionnez TLS
Nom du sujet x.509	Entrez le CN du certificat du pont d'appel, les noms séparés par des virgules
Incoming Port (port entrant)	Entrez le port qui recevra les requêtes TLS. Par défaut, il s'agit du port 5061

- Sélectionnez **Save (enregistrer)**

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

Étape 3. Créer une liaison SIP

- Naviguez jusqu'à **Device > Trunk (Périphérique > Ligne principale)**
- Sélectionnez **Add New (ajouter nouveau)**
- Sélectionnez **SIP Trunk (ligne principale SIP) pour le Trunk Type (type de ligne principale)**
- Sélectionnez **Next (suivant)**
- Entrez les valeurs qui s'appliquent.

Nom du périphérique	Entrez un nom pour la ligne principale SIP, par exemple CMS-Abhishek-32
Adresse de destination	Entrez l'adresse IP CMS ou le FQDN du pont d'appel, par exemple 10.106.81.32

Destination Port (port de destination)

Entrez le port où le CMS reçoit les communications TLS, par exemple **5061**

Profil de sécurité de la ligne principale SIP

Sélectionnez le profil sécurisé créé à l'étape 2, **CMS-Trunk-32**

Profil SIP

Sélectionnez **Standard SIP Profile for TelePresence Conferencing (profil SIP standard pour TelePresence Conferencing)**

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

Étape 4. Créer le pont de conférence

- Naviguez jusqu'à **Media Resources > Conference Bridge (Ressources multimédias > Passerelle de conférence)**
- Sélectionnez **Add New** (ajouter nouveau)
- Sélectionnez **Cisco TelePresence Conductor** du menu déroulant **Conference Bridge** (passerelle de conférence)

Note: À partir de la version 11.5.1 SU3 de CUCM, l'option **Cisco Meeting Server (serveur de réunion Cisco)** est disponible pour être sélectionnée comme **Conference Bridge Type (type de passerelle de conférence)** dans le menu déroulant

- Entrez l'information adéquate

Conference Bridge Name (nom de la passerelle de conférence)

Entrez un nom pour ce périphérique, par exemple **CMS-Adhoc-32**

Description

Entrez une description pour cette passerelle de conférence, par exemple **10.106.81.32**

SIP Trunk (ligne principale SIP)

Sélectionnez la ligne principale SIP créée à l'étape 3 : **CMS-Abhishek-32**

Override SIP Trunk Destination as HTTP Address (donner la priorité à l'adresse HTTP pour la destination de la ligne principale SIP)

Cochez cette case au cas où un autre serveur soit obligatoire

Adresse IP ou nom d'hôte

Entrez le nom d'hôte ou l'adresse IP de votre serveur CMS, par exemple **10.106.81.32**

Nom d'utilisateur

Entrez l'utilisateur créé dans CMS doté des privilèges d'API, par exemple **admin**

Mot de passe

Entrez le mot de passe de l'utilisateur utilisé pour l'API

Confirm password (confirmation du mot de passe)

Entrez le mot de passe une deuxième fois

Use HTTPS (utiliser HTTPS)

Cochez la case, cela est nécessaire pour la connexion CMS

HTTP Port (port HTTP)

Entrez le port webadmin de CMS, par exemple **443**

Conference Bridge Configuration
Relat

Save
 Delete
 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*

- Sélectionnez **Save (enregistrer)**

Note: Le champ du nom d'hôte (FQDN de CMS) et/ou de l'adresse IP doit être inclus dans le certificat Webadmin, dans le champ Common Name (nom usuel) ou Subject Alternative Name (autre nom du sujet) afin de permettre une connexion sécurisée

- Après la création de la passerelle de conférence, ouvrez la section **Cisco Unified Serviceability**
- Naviguez jusqu'à **Tools > Control Center - Feature Services (Outils > Centre de contrôle - Services de fonctionnalité**
- Dans le menu déroulant, sélectionnez CUCM publisher node (nœud de publication CUCM)
- Sélectionnez **Go (aller)**
- Sélectionnez le **service Cisco CallManager**
- Sélectionnez **Restart (redémarrer)**

Attention : Lorsque le service CallManager est redémarré, les appels connectés restent, mais certaines fonctionnalités ne sont pas disponibles au cours de ce redémarrage. Aucun nouvel appel n'est possible. Le redémarrage de service prend entre 5 et 10 minutes, selon la charge de travail de CUCM. Effectuez cette action avec précaution et assurez-vous de la faire lors d'une période de maintenance.

Étape 5. Le pont CMS est correctement enregistré dans CUCM

- Rendez-vous à **Media Resources (ressources multimédias) > Media Resource Group (groupe de ressources multimédias)**
- Cliquez sur Add New (ajouter nouveau) pour créer un nouveau groupe de ressources multimédias et entrez un nom
- Déplacez la passerelle de conférence (CMS) dans ce cas à partir de la boîte **Available Media Resources (ressources multimédias disponibles)** vers la boîte **Selected Media Resources (ressources multimédias sélectionnées)**
- Cliquez sur **Save (enregistrer)**

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*

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

Étape 6. Ajouter les groupes de ressources multimédias (MRG) aux listes de groupes de ressources multimédias (MRGL)

- Rendez-vous à **Media Resources (ressources multimédias) > Media Resource Group List (liste des groupes de ressources multimédias)**
- Cliquez sur Add New (ajouter nouveau) pour créer une nouvelle liste des groupes de ressources média et entrez un nom, ou sélectionnez un MRGL existant et cliquez dessus pour le modifier.
- Déplacez un ou plusieurs des groupes de ressources multimédias créés à partir de la boîte **Available Media Resource Groups (groupes de ressources multimédias disponibles)** vers la

boîte Selected Media Resource Groups (groupes de ressources multimédias sélectionnés)

- Cliquez sur **Save (enregistrer)**

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*

Media Resource Groups for this List

Available Media Resource Groups

▼ ▲

Selected Media Resource Groups

▼ ▲

Save Delete Copy Add New

Étape 7 : ajoutez MRGL à un pool de périphériques ou à un périphérique

Selon la mise en œuvre, on peut soit appliquer un regroupement de périphériques à des points de terminaison, ou attribuer un périphérique individuel (un point de terminaison) à une MRGL spécifique. **Si une MRGL est appliquée à la fois à un regroupement de périphériques et à un point de terminaison, les paramètres du point de terminaison auront préséance.**

- Rendez-vous à **System (système) >> Device Pool (regroupement de périphériques)**
- Créez un nouveau regroupement de périphériques (New Device Pool) ou utilisez un regroupement de périphériques existant. Cliquez sur Add New (ajouter nouveau)

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

Étape 8 : Pour ajouter le pool de périphériques au point de terminaison et ajouter MRGL au point de terminaison

- Rendez-vous à **Device > Phones (Périphérique > Téléphones)**
- Cliquez sur Find (trouver) et sélectionnez le périphérique pour lequel vous voulez modifier les paramètres du regroupement de périphériques (Device Pool)
- Appliquez le regroupement de périphériques (Device Pool) et la MRGL créés dans les étapes ci-dessus :
- **Save (enregistrer), Apply Config and Reset (appliquer la configuration et réinitialiser)**

Le point de terminaison va réinitialiser et s'enregistrer

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

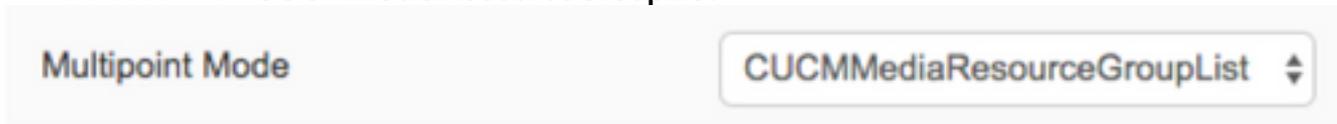
Registration: Registered with Cisco Unified Communications Manager 10.104.215.207
IPv4 Address: [10.104.130.54](#)
Active Load ID: ce-9.3.1-61bfa3834f2-2018-05-04
Inactive Load ID: None
Download Status: None

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

Étape 9 : Configuration sur un point de terminaison

- Connectez-vous au web-gui du point de terminaison
- Rendez-vous à **Setup (paramétrage) > Configuration > Conference > Multipoint Mode (Configuration > Conférence > Mode multipoint)**
- Sélectionnez **CUCMMediaResourceGroupList**



Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

- Ouvrez l'interface Web de CUCM
- Naviguez jusqu'à **Device > Trunks (Périphérique > Lignes principales)**
- Sélectionnez la ligne principale SIP qui pointe vers CMS
- Assurez-vous que la ligne principale est dans l'état **Full Service (service complet)**
- Naviguez jusqu'à **Media Resource > Conference Bridge (Ressource multimédia > Passerelle de conférence)**
- Sélectionnez la passerelle de conférence CMS
- Assurez-vous qu'elle est enregistrée avec CUCM

Passez un appel ad hoc

- Appelez du point de terminaison A (EndpointA) enregistré dans CUCM (MRGL ajouté) vers un autre point de terminaison B (EndpointB)
- Sur le point de terminaison A (EndpointA), cliquez sur Add (ajouter), composez le point de terminaison C (EndpointC)
- Le point de terminaison A (EndpointA) entrera en attente
- Cliquez sur Merge (fusionner)
- Valider que les appels sont connectés dans CMS
- Ouvrez l'interface Web de CMS
- Naviguez jusqu'à **Status > Calls (État > Appels)**

Afin de tester, 3 points de terminaison ont été utilisés pour la conférence ad hoc audio/vidéo

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

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.