

Cisco Meeting Server および CUCM のアドホック会議の設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[CMS の設定](#)

[CUCM の設定](#)

[確認](#)

[トラブルシューティング](#)

概要

このドキュメントでは、Cisco Meeting Server (CMS) および Cisco Unified Communications Manager (CUCM) でアドホック会議を設定する手順について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- CMS の導入と設定
- CUCM エンドポイントの登録とトランクの作成
- 署名証明書

使用するコンポーネント

- CUCM
- CMS サーバ 2.0.X 以降
- CMS で Webadmin および Call Bridge コンポーネントがすでに設定済みであること
- Call Bridge および Webadmin 用の内部ドメイン ネーム システム (DNS) レコード (CMS サーバの IP アドレスに解決可能)
- Web サーバ認証と Web クライアント認証の拡張キー使用法で証明書に署名するための内部認証局 (CA)
- Transport Layer Security (TLS) 通信用の署名付き証明書

注：この導入では、自己署名証明書に追加できない Web サーバおよび Web クライアント認証が必要であるため、自己署名証明書はサポートされていません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。このドキュメントは特定のソフトウェアおよびハードウェアのバージョンに限定されているわけではありませんが、ソフトウェアの最小バージョンの要件を満たす必要があります。

設定

CMS の設定

ステップ 1：アプリケーション プログラム インターフェイス（API）権限を持つ管理者ユーザ アカウントを作成します。

- メインボード管理プロセッサ（MMP）へのセキュア シェル（SSH）セッションを開きます。
- 管理者レベルのユーザ アカウントを追加するには、`user add <username> <role>` コマンドを実行します。
- 図に示すようにパスワードを入力します。

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

ステップ 2：証明書を作成します。

- `pki csr <file name> CN:<common name> subjectAltName:<subject alternative names>` コマンドを実行します
- 要件に応じて次の情報を使用します。

```
ファイル名      certall
CN              tptac9.com
subjectAltName cmsadhoc.tptac9.com,10.106.81.32
```

- 証明書の生成には、ワイルドカードを使用しないでください。ワイルドカードを使用した証明書は CUCM でサポートされていません。
- Web サーバ認証と Web クライアント認証の拡張キー使用法で証明書が署名されていることを確認します。

注：すべてのサービスに対して同じ証明書を使用するには、共通名（CN）がドメイン名である必要があります。他の CMS サービスの名前がサブジェクト代替名（SAN）として含まれている必要があります。この場合、IP アドレスも証明書によって署名されており、ルート証明書がインストールされているすべてのマシンで信頼されています。

CUCM の設定

ステップ 1：CUCM 信頼ストアに証明書をアップロードします。

- ルート証明書は、内部認証局の Web インターフェイスからダウンロードできます。

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](#)

- Call Bridge証明書とバンドル証明書（中間およびルート）をCallManager信頼ストアに追加します

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

Call BridgeとWebadminに対して別々の証明書がある場合は、アップロードを確認してください。

- Webadmin、Call Bridge、およびルート証明書からCall ManagerへのCUCMの信頼ストア

注：CUCM の SIP トランクは、非セキュア SIP トランクとして作成できます。その場合、Call Bridge 証明書を CallManager 信頼ストアにアップロードする必要はありませんが、webadmin 証明書に署名したルート証明書を CallManager 信頼ストアにアップロードする必要があります。

ステップ 2： SIP トランク プロファイルを設定します。

- CUCM Web インターフェイスを開きます。
- [システム (System)] > [セキュリティ (Security)] > [SIP トランク セキュリティ プロファイル (SIP Trunk Security Profile)] に移動します。
- [新規追加 (Add New)] を選択します。
- 適切な情報を使用して値を入力します。

[名前(Name)]	名前を入力します (CMS-Trunk-32 など) 。
[デバイスセキュリティモード (Device Security Mode)]	[暗号化 (Encrypted)] を選択します。
[着信転送タイプ (Incoming Transport Type)]	[TLS] を選択します
[発信転送タイプ (Outgoing Transport Type)]	[TLS] を選択します
[X.509 のサブジェクト名 (X.509 Subject Name)]	Call Bridge 証明書の CN を入力します (名前はカンマで区切ります) 。
[着信ポート (Incoming Port)]	TLS 要求を受信するポートを入力します。デフォルトは 5061 です。

- [保存 (Save)] を選択します。

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

ステップ 3： SIP トランクを作成します。

- [デバイス (Device)] > [トランク (Trunk)] に移動します。
- [新規追加 (Add New)] を選択します。
- [トランク タイプ (Trunk Type)] で [SIP トランク (SIP Trunk)] を選択します。
- [次へ (Next)] を選択します。
- 該当する値を入力します。

Device Name	SIP トランクの名前を入力します (CMS-Trunk-32 など) 。
送信先アドレス	CMS の IP アドレスまたは Call Bridge の FQDN を入力します (10.106.81.32 など) 。
宛先ポート	CMS が TLS 通信をリッスンするポートを入力します (5061 など) 。
SIP トランク セキュリティ プロファイル	ステップ 2 で作成したセキュア プロファイル (CMS-Trunk-32) を選択します。

SIP プロファイル

[TelePresence 会議用標準 SIP プロファイル (Standard SIP Profile for TelePresence Conferencing)] を選択します。

SIP Information						
Destination						
<input type="checkbox"/> 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 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					

ステップ 4 : 会議ブリッジを作成します。

- [メディアリソース (Media Resources)] > [会議ブリッジ (Conference Bridge)] に移動します。
- [新規追加 (Add New)] を選択します。
- [会議ブリッジ (Conference Bridge)] ドロップダウン メニューで、[Cisco TelePresence Conductor] を選択します。

注 : CUCM バージョン 11.5.1 SU3 以降では、[会議ブリッジ タイプ (Conference Bridge Type)] ドロップダウン メニューで [Cisco Meeting Server] オプションを選択できます。

- 適切な情報を入力します。

Conference Bridge Name

説明

SIP トランク

[HTTP アドレスとして SIP トランク接続先をオーバーライド (Override SIP Trunk Destination)]

[ホスト名/IP アドレス (Hostname/IP Address)]

ユーザ名

Password

パスワードの確認

[HTTPS の使用 (Use HTTPS)]

[HTTP ポート (HTTP Port)]

このデバイスの名前を入力します (CMS-Adhoc-32 など)。

この会議ブリッジの説明を入力します (10.106.81.32 など)。

ステップ 3 で作成した SIP トランク (CMS-Abhishek-32) を選択します。

別の名前が必要な場合は、このボックスをオンにします。

CMS のホスト名または IP アドレスを入力します (10.106.81.32 など)。

CMS で作成された、API 権限を持つユーザを入力します (admin など)。

API ユーザのパスワードを入力します。


パスワードをもう一度入力します。

このチェック ボックスをオンにします。これは CMS 接続のために必要です。

CMS webadmin ポートを入力します (443 など)。

Conference Bridge Configuration Relat

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*

- [保存 (Save)] を選択します。

注：セキュア接続を実現するには、ホスト名 (CMS の FQDN) および/または IP アドレスフィールドを、Webadmin 証明書の共通名またはサブジェクト代替名フィールドに含める必要があります。





- 会議ブリッジを作成したら、[Cisco Unified Serviceability] セクションを開きます。
- [ツール (Tools)] > [コントロール センター - 機能サービス (Control Center - Feature Services)] の順に移動します。
- ドロップダウンメニューから、CUCM パブリッシャ ノードを選択します。
- [移動 (Go)] を選択します。
- [Cisco CallManager サービス (Cisco CallManager service)] を選択します。
- [リスタート (Restart)] を選択します。

注意：CallManager サービスを再起動する場合、接続されたコールはそのままですが、一部の機能はこの再起動中には使用できなくなります。新しいコールを行うことはできません。サービスの再起動は、CUCM のワークロードによって 5 ~ 10 分程度かかります。このアクションは慎重に実行し、必ずメンテナンス期間中に行います。


ステップ 5：CMS ブリッジが正常に CUCM に登録されます。

- [メディア リソース (Media Resource)] > [メディア リソース グループ (Media Resource Group)] に移動します。
- [新規追加 (Add New)] をクリックして、新しいメディア リソース グループを作成し、名前を入力します。
- このケースでは、会議ブリッジ (cms) を [使用可能なメディア リソース (Available Media Resources)] ボックスから [選択されたメディア リソース (Selected Media Resources)] ボックスに移動します。
- [Save] をクリックします。

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

ステップ 6 : メディア リソース グループ リスト (MRGL) にメディア リソース グループ (MRG) を追加します。

- [メディア リソース (Media Resource)] > [メディア リソース グループ リスト (Media Resource Group List)] に移動します。
- [新規追加 (Add New)] をクリックして新しいメディア リソース グループ リストを作成し、名前を入力するか、または既存の MRGL を選択して編集します。
- 作成したメディア リソース グループを、[使用可能なメディア リソース グループ (Available Media Resource Groups)] ボックスから [選択されたメディア リソース グループ (Selected Media Resource Groups)] ボックスに移動します。
- [Save] をクリックします。

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

ステップ7：デバイスプールまたはデバイスへのMRGLの追加

実装に応じて、デバイスプールを設定してエンドポイントに適用するか、または個々のデバイス（エンドポイント）を特定のMRGLに割り当てることができます。MRGLがデバイスプールとエンドポイントの両方に適用されている場合は、エンドポイントの設定が優先されます。

- [システム (System)] > [デバイスプール (Device Pool)] に移動します。
- 新しいデバイスプールを作成するか、または既存のデバイスプールを使用します。[新規追加 (Add New)] をクリックします。

Device Pool Configuration

Save

Status: Ready

Device Pool Information

Device Pool: New

Device Pool Settings

Device Pool Name* CMS-Adhoc-DevicePool

Cisco Unified Communications Manager Group* Default

Calling Search Space for Auto-registration < None >

Adjunct CSS < None >

Reverted Call Focus Priority Default

Intercompany Media Services Enrolled Group < None >

Roaming Sensitive Settings

Date/Time Group* CMLocal

Region* Default

Media Resource Group List CMS MRGL

ステップ8 : デバイスプールをエンドポイントに追加し、MRGLをエンドポイントに追加します

- [デバイス (Device)] > [電話 (Phones)] に移動します。
- [検索 (Find)] をクリックして、デバイスプール設定を変更するデバイスを選択します。
- 上記のステップで作成したデバイスプールと MRGL を適用します。
- [保存 (Save)]、[設定の適用 (Apply Config)]、[リセット (Reset)] をクリックします。

エンドポイントが再起動し、登録されます。

Phone Configuration

Save Delete Copy Reset Apply Config Add New

Modify Button Items

1 Line [1] - 6000 (no partition)

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

2 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* 0896AD2D9DB2

Description SPARK KIT

Device Pool* CMS-Adhoc-DevicePool [View Details](#)

Common Device Configuration < None > [View Details](#)

Phone Button Template* Standard Cisco Spark Room Kit

Common Phone Profile* Standard Common Phone Profile [View Details](#)

Calling Search Space < None >

AAR Calling Search Space < None >

Media Resource Group List CMS MRGL

手順 9 : エンドポイントの設定を行います。

- エンドポイントの Web GUI にログインします。
- [セットアップ (Setup)] > [設定 (Configuration)] > [会議 (Conference)] > [マルチポイントモード (Multipoint Mode)] に移動します。
- CUCMMediaResourceGroupList を選択します。

Multipoint Mode

CUCMMediaResourceGroupList

確認

ここでは、設定が正常に機能しているかどうかを確認します。

- CUCM Web インターフェイスを開きます。
- [デバイス (Device)] > [トランク (Trunk)] に移動します。
- CMS をポイントする SIP トランクを選択します。
- トランクがフル サービス状態であることを確認します。
- [メディアリソース (Media Resource)] > [会議ブリッジ (Conference Bridge)] に移動します。
- CMS 会議ブリッジを選択します。
- CUCM に登録されていることを確認します。

アドホックコールを行います。

- CUCM (追加した MRGL) に登録されている EndpointA から別の EndpointB にコールします。
- EndpointA で、[追加 (Add)] をクリックして、EndpointC にダイヤルします。
- EndpointA は保留中になります。
- [マージ (Merge)] をクリックします。
- CMS でコールが接続されていることを確認します。
- CMS Web インターフェイスを開きます。
- [ステータス (Status)] > [コール (Call)] に移動します。

テストのために、3つのエンドポイントがアドホック音声/ビデオ会議に使用されました。

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

トラブルシューティング

現在、この設定に関する特定のトラブルシューティング情報はありません。