

Cisco Meeting Server 2.9 から 3.0 以降へのスムーズなアップグレードのためのガイダンス

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[アップグレードに関する重要な情報](#)

[考慮事項の概要](#)

[ライセンス](#)

[Webbridge \(WebRTCおよびCMAクライアント \)](#)

[Web GUIの変更](#)

[レコーダ/ストリーマ](#)

[Cisco Expresswayの考慮事項](#)

[CMSエッジ](#)

[CMS\(Acano\)Xシリーズ](#)

[SIPエッジ](#)

[詳細情報](#)

[ライセンス：アップグレード前にライセンスを確認する](#)

[アップグレード後にPMPライセンスが割り当てられるユーザ数を決定する](#)

[十分なSMPライセンスがありますか？](#)

[CMMの設定](#)

[Webbridgeの設定 \(WebRTCおよびCMAクライアント \)](#)

[Webアプリユーザー空間作成権限](#)

[チャット機能](#)

[WebRTCポイントツーポイントコール](#)

[注目すべきwebBridge設定の変更](#)

[Web GUIから削除された\[External Access\]セクション](#)

[録画またはストリーミング](#)

[Recorder](#)

[ストリーマ](#)

[Expresswayの考慮事項](#)

[CMSエッジ](#)

概要

このドキュメントでは、バージョン2.9以前を実行しているCisco Meeting Serverの導入を3.0以降にアップグレードする際の課題と、スムーズなアップグレードプロセスのためにそれらの問題を処理する方法について説明します。

削除された機能:XMPPが削除されました (WebRTCに影響します)、トランク/ロードバランサ、

変更された機能:レコーダとストリーマがSIPになり、webbridgeはwebbridge3に置き換えられました

このドキュメントでは、アップグレードの前に考慮する必要があるトピックのみを取り上げています。3.Xで使用可能なすべての新機能をカバーしていません。

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管理
- CMSアップグレード
- 証明書の作成と署名

ここで述べたことは、さまざまな文書で概説されています。 [CMSのインストールと設定ガイド](#) および [CMS製品リリースノート](#) など、機能に関してさらに詳しい説明が必要な場合は、製品のリリースノートを読み、プログラミングガイドおよび導入ガイドを参照することをお勧めします。

使用するコンポーネント

このドキュメントの情報は、Cisco Meeting Serverに基づくものです。

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。

背景説明

このドキュメントは、すでにCMS 2.9.x（またはそれ以前）を導入している場合のガイダンスを目的としています。単一の統合または復元力の有無や、CMS 3.0へのアップグレードを計画している場合は関係ありません。このドキュメントの情報は、CMSのすべてのモデルに関連しています。

注：XシリーズをCMS 3.0にアップグレードすることはできません。できるだけ早くXシリーズサーバを交換する必要があります。

アップグレードに関する重要な情報

CMSのアップグレードでサポートされている唯一の方法は、ステップアップグレードです。このドキュメントの執筆時点では、CMS 3.5がリリースされています。CMS 2.9を使用している場合は、段階的にアップグレードする必要があります(2.9 → 3.0 → 3.1 → 3.2 → 3.3 → 3.4 → 3.5(アップグレードプロセスはCMS 3.5の時点で変更されているため、リリースノートを注意深く読んでください!!))。

ステップアップグレードを実行せず、異常な動作が発生している場合は、TACからダウングレードと最初からやり直しを要求されることがあります。

また、CMS 3.4では、CMSはスマートライセンスを使用する必要があります。 CMS 3.4以降にアップグレードしても、従来のライセンスを使用することはできません。 スマートライセンスを設定していない限り、CMS 3.4以降にアップグレードしないでください。

考慮事項の概要

次の質問を使用して、自分の状況に関連するセクションに移動します。 各考慮事項は、このドキュメントで説明されている詳細な説明へのハイパーリンクを示しています。

ライセンス

アップグレードの前に、サーバに十分なパーソナルマルチパーティ(PMP)/共有マルチパーティ(SMP)ライセンスがありますか。

3.0では、ユーザがサインインしていなくても、PMPライセンスが割り当てられます。たとえ10000、LDAPを介してユーザをインポートしたが、PMPライセンスが100だけある場合、3.0にアップグレードするとすぐにコンプライアンスから外れます。この使用例では、userProfileが設定されているテナントやsystem/profilesを確認し、値がtrueのhasLicenseを持つuserProfileが設定されているかどうかを確認します。

APIでuserProfileを確認し、hasLicense=trueが設定されているかどうかを確認する方法 (PMPライセンスユーザを意味します) については、このセクションで詳しく説明 [しています](#)。

現在のcms.licファイルにPMP/SMPライセンスはありますか。

3.0以降のライセンス動作の変更により、アップグレードを実行する前に、十分なPMP/SMPライセンスがあるかどうかを確認する必要があります。これについては、このセクションで詳しく [説明します](#)。

Cisco Meeting Manager(CMM)を導入していますか。

ライセンスの処理方法が変更されたため、CMS 3.0にはCMM 3.0が必要です。90日間のレポートで過去90日間のライセンス使用量を確認できるため、環境を3.0にアップグレードする前にCMM 2.9を導入することをお勧めします。これについては、このセクションで詳しく [説明します](#)。

Smart Licensingはありますか。

ライセンスの処理方法が変更されたため、CMS 3.0にはCMM 3.0が必要です。CMMを介してスマートライセンスをすでに使用している場合は、クラスタにPMPライセンスとSMPライセンスが関連付けられていることを確認します。

Webbridge (WebRTCおよびCMAクライアント)

CMS 2.9でWebRTCを使用していますか。

CMS 3.0でWebbridgeが大幅に変更されました。 webbridge2からwebbridge3への移行およびWebアプリケーションの使用に関するガイダンスについては、 [このセクション](#) で説明します。

ユーザはCMAシッククライアントを使用していますか。

これらのクライアントはXMPPベースであるため、XMPPサーバが削除されているため、アップグレード後にこれらのクライアントを使用することはできません。これが使用例に当てはまる場合は、このセクションで詳細を確認[できます](#)。

WebRTCでチャットを使用しますか。

チャット機能は3.0でWebアプリから削除されました。CMS 3.2では、チャットが再導入されましたが、永続的ではありません。この機能の詳細については、[このセクション](#)を参照してください。

ユーザはWebRTCからデバイスへのポイントツーポイントコールを実行しますか。

CMS 3.0では、Webアプリケーションユーザは別のデバイスに直接ダイヤルできなくなりました。次に、ミーティングスペースに参加し、同じアクションを実行する参加者をミーティングに追加する権限を持つ必要があります。この部品の詳細については、[このセクション](#)を参照してください。

ユーザはWebRTCから独自のcoSpaceを作成しますか。

3.0では、Webアプリケーションユーザがクライアントから独自のスペースを作成できるようにするには、APIでcoSpaceTemplateを作成し、ユーザに割り当てる必要があります。これは、LDAPインポート中に手動または自動で行うことができます。CanCreateCoSpacesがUserProfileから削除されます。この機能の詳細については、[このセクション](#)を参照してください。

Web GUIの変更

Web管理GUIでwebBridge設定を行っていますか。

webBridge設定は3.0ではGUIから削除されているため、APIでwebbridgeを設定し、APIでwebBridgeProfilesを設定できるようにGUIでの現在の設定をメモする必要があります。この変更の詳細については、このセクションを参照[してください](#)。

Web管理GUIで外部設定を設定していますか。

CMS 3.1では、GUIから外部設定が削除されました。CMS 3.0以前のWeb管理GUI([Configuration] → [General] → [External Settings])でWebbridge URLまたはIVRを設定している場合、これらはWebページから削除されているため、APIで設定する必要があります。3.1にアップグレードする前の設定はAPIに追加されないため、手動で行う必要があります。この変更の詳細については、このセクションを参照[してください](#)。

レコーダ/ストリーマ

現在、CMSレコーダやストリーマを使用していますか。

CMSレコーダとストリーマコンポーネントが、XMPPベースではなくSIPベースになりました。したがって、XMPPを削除する場合は、アップグレード後にこれらの設定を調整する必要があります。この変更の詳細については、このセクションを参照[してください](#)。

Cisco Expresswayの考慮事項

Expresswayを使用してWebRTCをプロキシしている場合、現在のCisco Expresswayのバージョンはいくつですか。

CMS 3.0にはExpressway 12.6以降が必要です。このWebRTCプロキシ機能の詳細については、[このセクション](#)を参照してください。

CMSエッジ

現在、ご使用の環境にCMSエッジはありますか。

CMS EdgeはCMS 3.1に再導入され、外部接続のスケラビリティが向上しています。この部品の詳細については、[このセクション](#)を参照してください。

CMS(Acano)Xシリーズ

現在、ご使用の環境にxシリーズサーバはありますか。

これらのサーバはCMS 3.0にアップグレードできないため、すぐに交換する必要があります (3.0にアップグレードする前に、仮想マシンまたはCMSアプライアンスに移行してください)。これらのサーバに関するサポート終了のお知らせは、このリンクで[確認できます](#)。

SIPエッジ

現在、ご使用の環境でSIP Edgeを使用していますか。

Sip EdgeはCMS 3.0で完全に廃止されました。CMSにSIPコールを取り込むには、Cisco Expresswayを使用する必要があります。組織のExpresswayの入手方法については、シスコ代理店にお問い合わせください。

詳細情報

ライセンス : アップグレード前にライセンスを確認する

コンプライアンス違反のライセンスステータスは、2.xバージョンから3.0以降にアップグレードする際に最も影響する問題です。このセクションでは、スムーズなアップグレードに必要なPMP/SMPライセンスの量を決定する方法について説明します。

導入を3.0にアップグレードする前に、CMM 2.9を導入し、[Licenses] タブの90日レポートをチェックして、ライセンスの使用状況がCMSノードで現在割り当てられているライセンスの量を下回っていないかどうかを確認します。

Cisco Meeting Management

Notifications LDAP/admin Administrator

Licenses

Cluster: CMS VM Cluster Download 90 day report

Meetings		In compliance			
	Allocated	90 day peak		Allocated	90 day peak
Shared Multiparty Plus	100	2	Personal Multiparty Plus	100	9

Recording or Streaming		In compliance	
Allocated	90 day peak		
20	2		

Traditional licensing (cms.licファイルがCMSノードにローカルでインストールされている) を使用する場合は、CMSライセンスファイルで、各CMSノードのパーソナルライセンスと共有ライセンスの数量(100 / 100)を確認します (各callBridgeノードからWinSCPを介してダウンロード)。

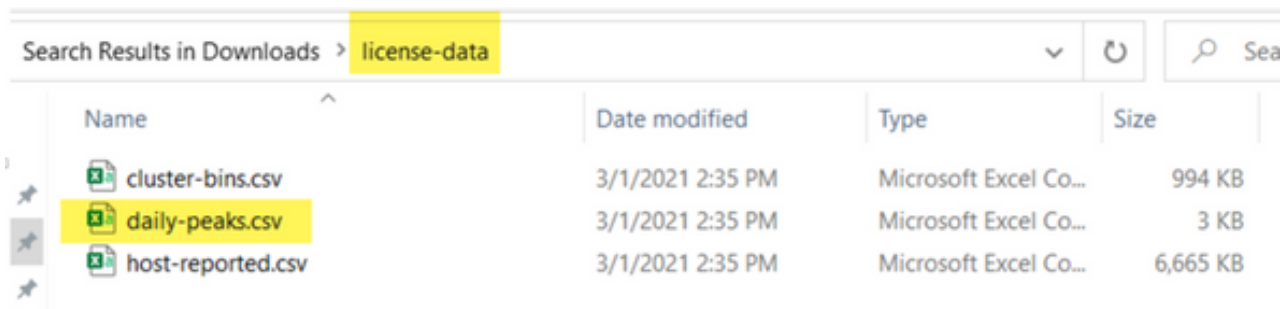
```

],
"issued_to": "Darren McKinnon - TAC",
"notes": "Darren McKinnon - TAC",
"features":
{
  "callbridge":
  {
    "expiry": "2100-Jan-03"
  },
  "webbridge3":
  {
    "expiry": "2100-Jan-03"
  },
  "customizations":
  {
    "expiry": "2100-Jan-03"
  },
  "recording":
  {
    "expiry": "2100-Jan-03",
    "limit": "10"
  },
  "personal":
  {
    "expiry": "2100-Jan-03",
    "limit": "100"
  },
  "shared":
  {
    "expiry": "2100-Jan-03",
    "limit": "100"
  },
  "streaming":
  {
    "expiry": "2100-Jan-03",
    "limit": "10"
  }
}

```


Smart Licensingをすでに使用している場合は、CMSサーバのCisco Software Smartポータルで割り当てられているPMP/SMPライセンスの数を確認します。

90日レポート(Zipファイル名はlicense-data.zip)を開き、daily-peaks.csvという名前のファイルを開きます。



Name	Date modified	Type	Size
cluster-bins.csv	3/1/2021 2:35 PM	Microsoft Excel Co...	994 KB
daily-peaks.csv	3/1/2021 2:35 PM	Microsoft Excel Co...	3 KB
host-reported.csv	3/1/2021 2:35 PM	Microsoft Excel Co...	6,665 KB

Excelで、PMP列をZでAにソートして上位の値を取得し、SMP列に対して同じ処理を実行します。このファイルに表示される値は、CMSライセンスファイルで使用可能なライセンスよりも低いのですか。そうであれば、問題なく完全に準拠しています。そうでない場合は、[CMS導入ガイド](#)のセクション1.7.3の図6に示すように、警告やエラーが発生します。このセクションでは、セクション1.7.4と同様に詳細な情報を参照できます。

図に示すように、2.1667のSMPライセンスが使用されており、過去90日間のピーク時と同じPMPライセンスはありません。cms.licファイルには、ライセンスのタイプごとに100ユニットが示されているため、このセットアップは完全に準拠しています。したがって、このセットアップでCMS 3.0にアップグレードする際のライセンスに関する問題はありません。ただし、セットアップでLDAPを介して10,000人のユーザがインポートされた場合には、問題が引き続き発生する可能性があります。その時点では100のPMPライセンスしかありませんが、10000 (hasLicenseがTrueに設定されたuserProfileを使用) を割り当てるため、この場合、3.0にアップグレードするとすぐにコンプライアンス違反となります。詳細については、次のセクションを参照してください。

date	pmp	smp	rec/str
12/10/2020	0	2.166666667	0
12/3/2020	0	2	0
1/7/2021	0	2	0
1/8/2021	0	2	0
1/14/2021	0	2	0
1/15/2021	0	2	0
1/26/2021	0	2	0
1/27/2021	0	2	0
2/19/2021	0	2	0
2/20/2021	0	2	0
1/11/2021	0	1.333333333	0
12/9/2020	0	1.166666667	0
1/12/2021	0	1.166666667	0
1/21/2021	0	1.166666667	0
2/8/2021	0	1.166666667	0
2/25/2021	0	1.166666667	0

アップグレード後にPMPライセンスが割り当てられるユーザ数を決定する

インポートされ、`hasLicense=true`で`userProfile`を使用するすべてのユーザには、CMS 3.0でPMPライセンスが自動的に割り当てられます。

APIで、所有している`userProfiles`の数を確認し、それらのいずれかに「`hasLicense=true`」が設定されているかどうかを確認します。その場合は、それらの`userProfiles`が割り当てられている場所を確認する必要があります。

`userProfiles`は、次のいずれかのレベルで割り当てることができます。

1. `LdapSources`
2. テナント
3. システム/プロファイル

割り当てられた`userProfiles`の3つの場所すべてに`hasLicense=true`があることを確認します。

1. `LdapSources`/テナント

テナントまたは`userProfile`を使用している`ldapSource`ごとに、`hasLicense`パラメータが`True`に設定されている場合、その`ldapSource`でインポートされたユーザにPMPライセンスが割り当てられます。テナントがある場合は、テナントIDをクリックして`userProfile`が割り当てられているかどうかを確認し、その`userProfile`が「`hasLicense=true`」で設定されているかどうかを確認する必要があります。テナントは存在しないが、`userProfile`セットが存在する場合は、それをクリックして「`hasLicense=true`」が設定されているかどうかを確認します。どちらかの方法に「`hasLicense=true`」がある場合は、「`api/v1/users`」のGETを実行し、`ldapSource`に関連付けられた`ldapmapping`上の`jidMapping`に使用されるドメインをフィルタリングすることで、インポートされたユーザの数を確認できます。

注：これは、作成したActiveDirectoryマッピングとフィルタを使用して確認する必要がある場合など、他の状況ではより複雑になる可能性があります。

ステップ1:`ldapSource`からマッピングIDを見つけます。

ステップ2:`ldapMappings`を検索して`jidMapping`を見つけます。

ステップ3:`jidMapping`で使用されているドメインを`api/v1/users`で検索します。

ステップ4：各`ldapSource`から見つかったユーザを追加します。LDAPインポートされたユーザのうち、PMPライセンスが必要なユーザの数。

/api/v1/ldapSources/9ec2c58e-38e5-4b11-af64-d6ac28e62387

Related objects: [/api/v1/ldapSources](#) 1 [ldapSource](#)

Table view XML view

Object configuration	
name	
server	3472dd67-4075-4816-6fdb-fe8e10f8b4f8
mapping	5fcd57a-1e31-4717-a0cd-4875f14b2db8
tenant	8fca8c38-ed94-5603-9419-51abea6dfc2
haveTo	DControl5.DControl
/api/v1/ldapMappings 2 ldapMappings	

= start < prev 1 - 3 (of 3) next > Create new Table view XML view

object id	ldapMapping
186205f-5d31-4b8c-96c1-a2bc162a8fa4	\$SAMAAccountNames@damckin.local
5fcd57a-1e31-4717-a0cd-4875f14b2db8	\$SAMAAccountNames@simpsons.local
cf609fa7-b668-4cfe-92d6-c5d975e0bb7	\$SAMAAccountNames@familyguy.local

[/api/v1/users](#) 3 [users](#)

= start < prev 1 - 4 (of 4) next > simpsons Filter Table view XML view

object id	user/id
2e2ed242-1b0d-4695-8da3-10e354603689	bart@simpsons.local
b285eb97-98f5-478b-9977-0d8c3d2f1d53	homer@simpsons.local
68599e67-193e-4269-b5a2-be81b920df7	lisa@simpsons.local
0ace6dee-98ef-4305-b339-0831086db496	marge@simpsons.local

2. システム/プロファイル

userProfileがsystem/profilesレベルで設定され、そのuserProfileに「hasLicense=true」が設定されている場合、サーバのアップグレード時にCMSにインポートされたすべてのユーザにPMPライセンスが割り当てられます。10,000人のユーザをインポートしたがPMPが100個しかない場合、CMS 3.0にアップグレードする際にコンプライアンス違反が発生し、コールの開始時に30秒間の画面メッセージと音声プロンプトが表示される可能性があります。

システムレベルのuserProfileがユーザがPMPを取得することを示している場合は、`/api/v1/users`に移動して、合計ユーザ数を確認します。

`/api/v1/users` Will show total number of imported users

= start < prev 1 - 9 (of 9) next > Filter Table view XML view

object id	user/id	ten
18a6595a-33a0-4fd0-8761-5030249e0301	Lois@familyguy.local	85d7c06-1253-461f-bb1a-fe49fd7004e8
84a2dbbe-34d5-4a02-a003-2cf34fb59f73	brian@familyguy.local	85d7c06-1253-461f-bb1a-fe49fd7004e8
86e2f6a6-55fc-443e-b7ae-66a200191cac	connor@damckin.local	
44800633-fb41-4928-b0f5-339c64fcb67	darren@damckin.local	
d8c1786c-288c-99e5-a6d9-8cb192425b7f	homer@simpsons.local	8fca8c38-ed94-5603-9419-51abea6dfc2
a1105eb2-49f1-4ba5-8deb-c1e3d74b4084	janette@damckin.local	
b6f80307-d879-4863-8e00-667e403e5a2e	meg@familyguy.local	85d7c06-1253-461f-bb1a-fe49fd7004e8
32a615e6-ca2e-4489-a5db-d65e83b067a9	peter@familyguy.local	85d7c06-1253-461f-bb1a-fe49fd7004e8
f1c47991-5173-4daa-bb59-2140c8ca01f6	stewie@familyguy.local	85d7c06-1253-461f-bb1a-fe49fd7004e8

以前にLDAPからすべてのユーザをインポートしたが、そのリストから特定のサブセットのみをインポートする必要があることに気付いた場合は、ldapSourceに適切なフィルタを作成して、PMPライセンスを割り当てるユーザだけをインポートします。ldapSourceでフィルタを修正し、`/api/v1/ldapsync`で新しいLDAP同期を実行します。これにより、目的のユーザのみがインポートされ、この以前のインポートの他のユーザはすべて削除されます。

注：これを正しく実行し、新しいインポートで不要なユーザだけが削除された場合、残りのユーザのcoSpace CallIDとシークレットは変更されませんが、間違って実行すると、すべてのcallIDとシークレットが変更される可能性があります。この問題が懸念される場合は、これを試みる前にデータベースノードのバックアップを作成してください。

十分なSMPライセンスがありますか？

CMM 90 Day Reportから毎日のピークを見ていたとき、ピークをカバーするのに十分なSMPライセンスをすでに持っていますか。SMPライセンスは、会議の所有者にPMPライセンスが割り当てられていない場合（coSpace所有者、アドホック会議、TMSスケジュール会議など）に使用さ

れます。意図的にSMPを使用していて、ピーク時間をカバーするのに十分な時間がある場合は、これで問題ありません。SMPの90日間のピークをチェックし、それらが消費される理由が不明な場合は、ここでチェックすべきことがあります。

1. userProfileを介してCMSでPMPライセンスを割り当てられたユーザにマージに使用するデバイスが関連付けられていない場合、(CUCMからエスカレーションされた)アドホックコールはSMPライセンスを使用します。CUCMは、会議をエスカレーションするユーザのGUIDを提供します。そのGUIDが、割り当てられたPMPライセンスを使用してインポートされたMeeting ServerのLDAPユーザに対応する場合、そのユーザのライセンスが使用されます。
2. coSpace所有者にPMPライセンスが割り当てられていない場合、それらの特定のcoSpaceへのコールではSMPライセンスが使用されます。
3. 会議がTMSバージョン15.6以降でスケジュールされていた場合、会議の所有者はCMSに送信され、そのユーザにPMPライセンスが割り当てられていない場合、その会議はSMPライセンスを使用します。

CMMの設定

CMS 3.0と同様に、CMSが正常に機能するにはCMM 3.0が必要です。CMSのライセンスはCMMが担当するため、CMSを3.0にアップグレードする場合は、CMMサーバが必要です。アップグレードする前にライセンスの使用量を確認できるように、CMS 2.9を使用している間にCMM 2.9を展開することをお勧めします。

CMMは、追加されたすべてのcallBridgeでSMPおよびPMPライセンスとcallBridgeライセンスをチェックします。クラスタ内のさまざまなデバイスの中で最も高い番号を使用します。

たとえば、CMS1に20のPMPライセンスと10のSMPライセンスがあり、CMS2に40のPMPライセンスと5のSMPライセンスがある場合、CMMは40のPMPライセンスと10のSMPライセンスを使用するとレポートします。

インポートされたユーザよりも多くのPMPライセンスがある場合、PMP (またはSMP) ライセンスに関連する問題は発生しませんが、90日のピークを確認した結果、使用可能時間を超える時間が使用されていることが判明した場合でも、CMS 3.0にアップグレードし、CMMの90日間トライアルライセンスを使用してライセンスを整理するか、アップグレード前に措置を講じることができます。

The screenshot displays the Cisco Meeting Management interface for license management. The main content area shows a table of licenses for the 'CMS VM Cluster'. The table is organized into sections for 'Meetings' and 'Recording or Streaming', both marked as 'In compliance'. The 'Meetings' section includes two license types: 'Shared Multiparty Plus' and 'Personal Multiparty Plus'. The 'Recording or Streaming' section shows a single license type. A 'Download 90 day report' button is visible in the top right corner of the license table area. The left sidebar contains navigation options, with 'Licenses' highlighted.

License Type	Allocated	90 day peak
Shared Multiparty Plus	100	2
Personal Multiparty Plus	100	9
Recording or Streaming	20	2

Webbridgeの設定 (WebRTCおよびCMAクライアント)

CMS 3.0ではXMPPサーバコンポーネントが削除され、これによりwebBridgeとCMAシックスクライアントを使用する機能が削除されます。 WebBridge3は、ブラウザを使用してWebアプリケーションユーザ（以前のWebRTCユーザ）を会議に接続するために使用されます。 3.0にアップグレードする場合は、webbridge3を設定する必要があります。

注：CMS 3.0へのアップグレード後、CMAシックスクライアントが機能しない

このビデオでは、webbridge 3証明書を作成するプロセスについて説明します。

<https://video.cisco.com/video/6232772471001>

3.0にアップグレードする前に、お客様はWebbridge3の設定方法を計画する必要があります。最も重要な手順を以下に示します。

1. webbridge3のキーと証明書チェーンが必要です。古いwebbridge証明書は、証明書にwebbridge3を実行しているSubject Alternative Name(SAN)/Common Name(CN)としてCMSサーバのすべてのFQDNまたはIPアドレスが含まれており、次のいずれかが満たされている場合に使用できます。

a. 証明書に拡張キー使用法がありません（クライアントまたはサーバとして使用できます）。

b. 証明書にはクライアント認証とサーバ認証の両方があります。HTTP証明書では実際にはサーバ認証のみが必要ですが、C2W証明書ではサーバとクライアントの両方が必要です）。

2. 「webbridge3 https」証明書の新しい証明書を作成する場合は、（Webアプリケーションの使用時にクライアントで証明書の警告が表示されないように）公開署名することを推奨します。これと同じ証明書を「webbridge3 c2w cert」に使用できます。この証明書には、SAN/CN内のwebbridgeサーバのFQDNが必要です。

3. CallBridgeは、webbridge3 c2w listenコマンドで設定されたポートを使用して、新しいwebbridge3と通信する必要があります。これは、449などの任意の使用可能なポートにすることができます。ユーザは、callbridgeがこのポートでwebbridge3と通信でき、必要に応じて事前にファイアウォールを変更できることを確認する必要があります。「webbridge https」がリスンに使用するポートと同じにすることはできません。

CMSを3.0にアップグレードする前に、「backup snapshot <servername_date>」を使用してバックアップを取り、callbridgeノードのwebadminページにログインして、すべてのXMPP設定とWebbridge設定を削除することをお勧めします。次に、サーバ上のMMPに接続し、SSH接続経路でxmppとwebbridgeを持つすべてのコアサーバで次の手順を実行します。

1. xmpp disable
2. xmpp reset
3. xmpp certs none
4. xmpp domain none
5. webbridge disable
6. webbridge listen none
7. webbridge certs none
8. webbridge trust none

3.0にアップグレードしたら、以前webbridgeを実行していたすべてのサーバでwebbridge3を設定することから始めます。これらのサーバを指すDNSレコードがすでに存在するため、これを行う必要があります。したがって、ユーザがwebbridge3に送信された場合、要求を処理する準備が

整っていることを確認できます。

Webbridge3の設定 (すべてのSSH接続)

ステップ1:webbridge3 httpリスニングポートを設定します。

Webbridge3 https listen a:443

ステップ2 : ブラウザ接続用にwebbridge3の証明書を設定します。これはブラウザに送信される証明書であり、ブラウザが接続を信頼するためにブラウザで使用されるFQDNを含むパブリック認証局(CA)によって署名される必要があります。

Webbridge3 https certs wb3.key wb3trust.cer(これは信頼チェーンである必要があります。先頭にエンドエンティティを持つ信頼証明書を作成し、次に中間CAを順に作成し、RootCAで終了します)。

```
-----BEGIN CERTIFICATE-----  
Entity cert ← wb3/cb cert  
-----END CERTIFICATE-----  
-----BEGIN CERTIFICATE-----  
Intermediate cert  
-----END CERTIFICATE-----  
-----BEGIN CERTIFICATE-----  
root cert  
-----END CERTIFICATE-----  
single carriage return at end
```

ステップ3:callBridgeからwebbridge(c2w)への接続をリッスンするために使用するポートを設定します。 webbridge3 httpsリッスンポートには443が使用されるため、この設定は449などの別の使用可能なポートにする必要があります。

Webbridge3 c2w listen a:449

4. c2w信頼のためにwebbridgeがcallbridgeに送信する証明書を設定する

Webbridge3 c2w certs wb3.key wb3trust.cer

5. WB3がcallBridge証明書を信頼するために使用する信頼ストアを設定します。これは、callbridge CAバンドルで使用される証明書と同じである必要があります(また、先頭に中間証明書のバンドルを使用し、末尾にルートCAを使用し、その後にシングルキャリッジリターンを使用する必要があります)。

Webbridge3 c2w trust rootca.cer

6. webbridge3を有効にします

Webbridge3 enable

```

Usage:
webbridge3
webbridge3 restart
6 webbridge3 enable
webbridge3 disable
1 webbridge3 https listen <interface:port whitelist>
2 webbridge3 https certs <key-file> <crt-fullchain-file>
webbridge3 https certs none
webbridge3 http-redirect (enable [port]|disable)
3 webbridge3 c2w listen <interface:port whitelist>
4 webbridge3 c2w certs <key-file> <crt-fullchain-file>
webbridge3 c2w certs none
5 webbridge3 c2w trust <crt-bundle>
webbridge3 c2w trust none
webbridge3 options <space-separated options>
webbridge3 options none
webbridge3 status

```

CallBridge設定の変更 (SSH接続上のすべて)

ステップ1:webbridge3 c2w証明書に署名したCA証明書/バンドルを使用してcallBridge信頼を設定します。

Callbridge trust c2w rootca.cer

ステップ2:callBridgeを再起動して、新しい信頼を有効にします。 これにより、この特定のcallBridge上のすべてのコールがドロップされるため、注意して使用してください。

Callbridge restart

webBridge3に接続するためのcallBridgeのAPI設定

1. APIでPOSTを使用して新しいwebBridgeオブジェクトを作成し、webbridge c2wインターフェイスのホワイトリスト (webbridge3設定のステップ3) で設定されたFQDNとポートを使用してURL値を指定します

c2w://webbridge.darmckin.local:449

この時点でWebbridge3が再び動作し、スペースをゲストとして参加させることができます。また、以前にユーザをインポートした場合は、ユーザがサインインできる必要があります。

Webアプリユーザー空間作成権限

WebRTCで独自のスペースを作成できることに慣れていませんか。 CMS 3.0では、Webアプリケーションユーザは自分のCoSpaceを作成できません。ただし、CoSpaceテンプレートが割り当てられている必要があります。

coSpaceTemplateが割り当てられている場合でも、他のユーザがダイヤルインできるスペースは作成されません (URIなし、コールIDまたはパスコードなし)。ただし、coSpaceに「addParticipantAllowed」を含むcallLegProfileがある場合は、そのスペースからダイヤルアウトできます。

新しいスペースへのコールに使用できるダイヤル文字列を設定するには、coSpaceTemplateに

accessMethodTemplateの設定が必要です(2.9リリースノート – https://www.cisco.com/c/dam/en/us/td/docs/conferencing/ciscoMeetingServer/Release_Notes/Version-2-9/Cisco-Meeting-Server-Release-Notes-2-9-6.pdfを参照)。

APIで、coSpaceTemplate(s)を作成してからaccessMethodTemplate(s)を作成し、そのcoSpaceTemplateをldapUserCoSpaceTemplateSourcesに割り当てるか、またはapi/v1/usersでcoSpaceTemplateをユーザに手動で割り当てることができます。

複数のCoSpaceTemplatesおよびaccessMethodsTemplatesを作成して割り当てることができます。詳細については、CMS APIガイド (<https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-programming-reference-guides-list.html>)を参照してください。

The screenshot displays the API interface for managing CoSpaceTemplates. At the top, the URL `/api/v1/coSpaceTemplates/b03dbf12-c480-487e-b4d8-955e491ff074` is highlighted. Below it, the 'Related objects' section lists `/api/v1/coSpaceTemplates/b03dbf12-c480-487e-b4d8-955e491ff074/accessMethodTemplates`, which is also highlighted with a yellow box and pointed to by a red arrow. The main section shows the 'Object configuration' for the CoSpaceTemplate, with fields: name (First CoSpaceTemplate), callProfile (008e1aa7-0079-4d65-b6ae-fb218bd2e6b4), callLegProfile (ef583b0e-a6fe-49cf-bece-b557332a76bf), and numAccessMethodTemplates (2). Below this is a form to modify the CoSpaceTemplate, with fields for name, description, callProfile, callLegProfile, and dialInSecurityProfile, each with a 'Choose' button. At the bottom, the URL `/api/v1/coSpaceTemplates/b03dbf12-c480-487e-b4d8-955e491ff074/accessMethodTemplates` is highlighted with a yellow box, and a form to create a new AccessMethodTemplate is visible, with fields for name, uriGenerator, callLegProfile, generateUniqueCallId, and dialInSecurityProfile, each with a 'Choose' button and a 'Create' button.

CoSpaceTemplate (API設定)

[Name] : coSpaceTemplateに付ける任意の名前。

説明:必要に応じて簡単な説明。

callProfile: White callProfileこのテンプレートで作成したスペースを使用しますか？指定されていない場合は、システム/プロファイルレベルで設定されている内容が使用されます。

calllegProfile:このテンプレートで作成したスペースで使用するcalllegProfileはどれか？指定されていない場合は、システム/プロファイルレベルで設定されている内容が使用されます。

dialInSecurityProfile:このテンプレートで作成されたスペースで使用するdialInSecurityProfileを選択してください。指定されていない場合は、システム/プロファイルレベルで設定されている内容が使用されます。

AccessMethodTemplate (API構成)

[Name] : coSpaceTemplateに付ける任意の名前。

uriGenerator: このアクセスメソッドテンプレートのURI値の生成に使用される式。使用できる文字セットは、'a' ~ 'z'、'A' ~ 'Z'、'0' ~ '9'、'!'、'_'、'-'、および'\$'です。空でない場合は、'\$'文字を1つだけ含める必要があります。例えば、\$.spaceはユーザーがスペースを作成するときに指定した名前を使用し、それに「.space」を追加します。「Team Meeting」と入力すると、URL「Team.Meeting.space@domain」が作成されます。

callLegProfile:このテンプレートで作成されたaccessMethodsで使用するcallLegProfileはどれか？指定されていない場合は、設定されているCoSpaceTemplateレベルを使用し、設定されていない場合は、システム/プロファイルレベルの内容を使用します。

generateUniqueCallId:コスペースのグローバルIDをオーバーライドする、このアクセスメソッドの一意の数値IDを生成するかどうか。

dialInSecurityProfile:このテンプレートで作成されたアクセスメソッドで使用するdialInSecurityProfileを指定してください。指定されていない場合は、設定されているCoSpaceTemplateレベルを使用し、設定されていない場合は、システム/プロファイルレベルの内容を使用します。

チャット機能

CMS 3.0では常設チャット機能が削除されましたが、CMS 3.2ではスペース内の非常設チャットが返されました。チャットはWebアプリケーションユーザが利用でき、どこにも保存されません。CMS 3.2がインストールされると、Webアプリケーションユーザはデフォルトで会議中にメッセージを交換できます。これらのメッセージは会議中にのみ使用でき、参加後に交換されたメッセージのみが表示されます。遅れて参加したり、前のメッセージに戻ってスクロールしたりすることはできません。

WebRTCポイントツーポイントコール

CMS 2.9.xでは、WebRTC参加者はクライアントから他の連絡先に直接ダイヤルできました。CMS 3.0以降では、これは不可能になりました。ユーザはサインインしてスペースに参加する必要があります。そこから、callLegProfileに権限がある場合(addParticipantsパラメータをTrueに設定)、他の連絡先を追加できます。これにより、CMSは参加者にダイヤルアウトし、CMSのスペースで会議を行います。

注目すべきwebBridge設定の変更

CMS 3.0および3.1では、GUIからwebbridge設定の一部が削除または再配置されています。ユーザに一貫したエクスペリエンスを提供するには、これらの設定をAPIで設定する必要があります。3.xでは、api/v1/webBridgesおよびapi/v1/webBridgeProfilesを使用します。

現在の設定内容を確認して、3.0にアップグレードするときに、それに応じてAPIでwebbridgeおよびwebbridgeプロファイルを設定できるようにします。

The image displays three sequential screenshots of the Lync Edge settings GUI, illustrating the removal of certain configuration options over time:

- CMS 2.9.x:** Shows the 'Web bridge settings' section (highlighted with a red box) containing fields for 'Guest account client URI', 'Guest account JID domain' (tp1ab2.local), 'Guest access via ID and passcode' (secure: require passcode to be supplied with ID), 'Guest access via hyperlinks' (allowed), 'User sign in' (allowed), and 'Joining scheduled Lync conferences by ID' (not allowed). Below it is the 'IVR' section with 'IVR numeric ID' (7772) and 'Joining scheduled Lync conferences by ID' (not allowed). The 'External access' section (also highlighted with a red box) includes 'Web Bridge URI' (https://14.49.25.94) and 'IVR telephone number'. A 'Submit' button is at the bottom.
- CMS 3.0:** The 'Web bridge settings' section has been removed. The 'External access' section remains, with the same 'Web Bridge URI' and 'IVR telephone number' fields. The 'Lync Edge settings' section above it includes 'Server address', 'Username', and 'Number of registrations'. The 'IVR' section is also present.
- CMS 3.1:** The 'External access' section has also been removed. Only the 'Lync Edge settings' and 'IVR' sections remain.

3.0では、GUIでWebブリッジ設定が削除され、CMS 3.1では外部アクセスフィールドも削除されました。

GUIでのWebブリッジの設定

- **ゲストアカウントクライアントURI**：これはwebBridgeを見つけるためにcallBridgeによって使用されました。 WebRTCの導入に複数のwebBridgeが存在する場合、このフィールドは空白である必要があり、callBridgeが接続する必要がある各webBridgeの api/v1/webbridgesに一意のURLが必要です。このフィールドの内容をすべて削除し、APIにwebBridgeが設定されていることを確認します。
- **Guest Account Jid Domain**：これはCMS 3.0では使用されなくなり、削除できます。
- **IDおよびパスコードによるゲストアクセス**:CMS 3.0では削除され、置き換えられませんでした。
- **Hyper Links経由のゲストアクセス**:APIのwebBridgeProfilesで「AllowSecrets」を設定して設定できるようになりました。

The image shows two versions of the "/api/v1/webBridges" API form. The top version, labeled "CMS 2.9.x", includes fields for url, resourceArchive, tenant, tenantGroup, idEntryMode, allowWeblinkAccess, showSignIn, resolveCoSpaceCallIds, resolveLyncConferenceIds, callBridge, and callBridgeGroup. The bottom version, labeled "CMS 3.0", shows a simplified form with url, tenant, tenantGroup, callBridge, callBridgeGroup, and webBridgeProfile. Both forms have a "Create" button at the bottom.

CMS 3.0では、複数のフィールドが/api/v1/webBridgesから削除されています。

- **resourceArchive**:webbridgeProfilesに追加されました。
- **idEntryMode** : 廃止されました。
- **allowWeblinkAccess**:allowSecretsとしてwebBridgeProfilesに追加されました。
- **showSignIn**:userPortalEnabledとしてwebBridgeProfilesに追加されました。
- **resolveCoSpaceCallIds**:webbridgeProfilesに追加されました。
- **resolveLyncConferenceIDs**:webbridgeProfilesに追加されました。

The image shows the "/api/v1/webBridgeProfiles" API form for "CMS 3.0 onward". It includes fields for name, resourceArchive, allowPasscodes, allowSecrets, userPortalEnabled, allowUnauthenticatedGuests, resolveCoSpaceCallIds, and resolveCoSpaceUris. A "Create" button is located at the bottom.

WebBridgeProfile

- **resourceArchive** : カスタム背景を使用し、リソースアーカイブがWebサーバに保存されている場合は、ここにURLを入力します。
- **allowPasscodes**:falseの場合、ユーザはゲストとして会議に参加できません。ユーザはサインインするか、スペース情報とシークレットを含むURLのみを使用できます
- **allowSecrets** : これがfalseに設定されている場合、ユーザは https://meet.company.com/meeting/040478?secret=gPDnucF8is4W1cS87_l.zwなどのURLを使用してスペースに参加できません。ユーザは <https://meet.company.com> を使用し、コールID/会議ID/URIとPIN/パスコードが設定されている場合は入力する必要があります。

- **userPortalEnabled** : これがfalseに設定されている場合、Webアプリケーションポータルへのランディングページにサインインオプションは表示されません。設定されている場合、コールID/会議ID/URIおよびPIN/パスコードを入力するためのフィールドのみが表示されます。
- **allowUnauthenticatedGuests**:Falseに設定すると、ゲストは会議IDとシークレットを含む完全なURLを使用しても、会議に参加できません。 Falseの場合、サインインできるユーザーのみが会議に参加できます。 例 : User2がUser1の会議のURLを使用しようとしています。 URLを入力した後、User2はUser1の会議を続行するためにサインインする必要があります。
- **resolveCoSpaceCallIds**:Falseに設定すると、ゲストはURIとPIN/パスコード(PIN)を入力しないと会議に参加できません。 コールID/会議ID/数値IDは受け付けられません。
- **resolveCoSpaceUris** - 3つの設定が可能 : off、domainSuggestionDisabled、およびdomainSuggestionEnabled。このwebBridgeがcoSpaceおよびcoSpace accessMethod SIP URIを受け入れるかどうか (訪問者がcospace会議に参加できるようにするため)。
- 'off'に設定すると、URIによる参加が無効になります。
- 「*domainSuggestionDisabled*」に設定すると、URIによる参加が有効になりますが、このwebBridgeProfileを使用するwebBridgeでは、URIのドメインが自動補完または検証されません。
- 「*domainSuggestionEnabled*」に設定すると、URIによる参加が有効になり、このwebBridgeProfileを使用してwebBridgeでURIのドメインを自動補完および検証できます。

Web GUIから削除された[External Access]セクション

CMS 3.1では、Web GUIから[External Access]セクションが削除されました。 アップグレード前にこれらの設定を行っていた場合は、APIのwebbridgeProfilesで再設定する必要があります。

External access

Web Bridge URI

IVR telephone number

最初に、前のセクションで説明したようにwebbridgeProfileを作成する必要があります。 webbridgeProfileを作成したら、新しく作成したwebBridgeProfileの下にあるAPIで使用可能なリンクを使用して、IVR番号やWeb Bridge URIを作成できます。



webBridgeProfileごとに最大32のIVR番号または32のwebbridgeAddressesを作成できます

録画またはストリーミング

CMS 2.9.x以前のレコーダおよびストリーマコンポーネントはXMPPクライアントで、CMS 3.0が

らはSIPベースになっています。 これにより、APIのデフォルトのレイアウトを使用して、録音とストリーミングのレイアウトを変更できるようになりました。 また、レコーディング/ストリーミングセッションで名前ラベルが表示されるようになりました。 レコーダおよびストリーミング機能の詳細については、CMS 3.0リリースノート

(https://www.cisco.com/c/dam/en/us/td/docs/conferencing/ciscoMeetingServer/Release_Notes/Version-3-0/Cisco-Meeting-Server-Release-Notes-3-0.pdf)を参照してください。

レコーダまたはストリーマが2.9.xで設定されている場合は、MMPおよびAPIの設定を再設定して、アップグレード後もこれらの設定が引き続き機能するようする必要があります。

CMSを3.0にアップグレードする前に、「backup snapshot <servername_date>」を使用してバックアップを取り、callbridgeノードのwebadminページにログインして、すべてのXMPP設定を削除することをお勧めします。 次に、サーバ上のMMPに接続し、SSH接続経由でxmppを持つすべてのコアサーバで次の手順を実行します。

1. xmpp disable
2. xmpp reset
3. xmpp certs none
4. xmpp domain none

Recorder

MMP

図は、レコーダーが設定されたときにCMS 2.9.1で見られる設定の例と、3.0へのアップグレード直後の状態を示しています。

```
CMSRecorder> recorder
Enabled                : true
Interface whitelist    : a:443
Key file               : recorder.key
Certificate file       : recorder.cer
CA Bundle file        : rootca.cer
Trust bundle          : onecert.cer
NFS domain name       : 14.49.25.22
NFS directory         : E/Shares/Recordershare
Resolution            : 720p
CMSRecorder> █
```

```
CMSRecorder> recorder
Enabled                : false
SIP interfaces        : none
SIP key file          : none
SIP certificate file  : none
SIP traffic trace     : Disabled
NFS domain name       : 14.49.25.22
NFS directory         : E/Shares/Recordershare
Resolution            : 720p
Call Limit            : none
CMSRecorder> █
```

アップグレード後、レコーダを再設定する必要があります。

ステップ1:SIPリスニングインターフェイスを設定します。

recorder sip listen a 5060 5061(SIPレコーダがTCPおよびTLSをリッスンするように設定されているインターフェイスとポート。TLSを使用しない場合は、「recorder sip listen a 5060 none」を使用できます)

ステップ2:TLS接続を使用している場合にレコーダが使用する証明書を設定します。

recorder sip certs <key-file> <crt-file> [crt-bundle](これらの証明書がない場合、tlsサービスはレコーダで開始されません。レコーダはcrt-bundleを使用してcallBridge証明書を confirms)。)

ステップ3 : コール制限を設定します。

レコーダの制限<0-500|none>(サーバが処理できる同時録音の制限数を設定します。この表はドキュメントに記載されており、レコーダの制限はサーバ上のリソースに合わせる必要があります)。

Table 6: Internal SIP recorder performance and resource usage

Recording Setting	Recordings per vCPU	RAM required per recording	Disk budget per hour	Maximum concurrent recording
720p	2	0.5GB	1GB	40
1080p	1	1GB	2GB	20
audio	16	100MB	150MB	100

Key point to note (applies to new internal recorder component only):

- Performance scales linearly adding vCPUs up to the number of host physical cores.

API

api/v1/callProfilesでは、sipRecorderUriを設定する必要があります。これは、録音を開始する必要があるときにcallBridgeがダイヤルするURIです。このURIのドメインをアウトバウンドルールテーブルに追加し、使用するSIPプロキシとしてレコーダ (またはコール制御) をポイントする必要があります。

Object configuration	
recordingMode	automatic
sipRecorderUri	recorder@recorder.com

次の図は、[Configuration] > [Outbound Calls] にあるアウトバウンドルールのレコーダコンポーネントへの直接ダイヤルを示しています。

Outbound calls

Filter: Submit

	Domain	SIP proxy to use	Local domain	Local from domain	Trunk type	Behavior	Priority	Encryption
<input type="checkbox"/>	recorder.com	14.49.17.246:5061	Recorder	<use local contact domain>	Standard SIP	Continue	1	Encrypted
<input type="checkbox"/>	streamer.com	14.49.17.246:5001		<use local contact domain>	Standard SIP	Continue	1	Encrypted
<input type="checkbox"/>	recorder.com	14.49.17.246	Streamer	<use local contact domain>	Standard SIP	Stop	0	Auto
<input type="checkbox"/>	streamer.com	14.49.17.246:5000		<use local contact domain>	Standard SIP	Stop	0	Auto

この図は、コール制御(Cisco Unified Communications Manager(CUCM)やExpresswayなど)を介したレコーダコンポーネントへのコールを示しています。

Outbound calls

Filter

	Domain	SIP proxy to use	Local contact domain	Local from domain	Trunk type	Behavior	Priority	Encryption
<input type="checkbox"/>	recorder.com	14.49.17.229		<use local contact domain>	Standard SIP	Continue	1	Encrypted
<input type="checkbox"/>	streamer.com	14.49.17.229		<use local contact domain>	Standard SIP	Continue	1	Encrypted
<input type="checkbox"/>	recorder.com	14.49.17.252		<use local contact domain>	Standard SIP	Stop	0	Auto
<input type="checkbox"/>	streamer.com	14.49.17.252		<use local contact domain>	Standard SIP	Stop	0	Auto
					Standard SIP	Stop	0	Auto

CUCM (green arrow pointing to 14.49.17.229)

Expressway (red arrow pointing to 14.49.17.252)

注：レコーダでSIP TLSを使用するように設定し、コールが失敗した場合は、MMPの callBridgeノードでTLS SIP検証が有効になっているかどうかを確認します。MMPコマンドは「`tls sip`」です。レコーダ証明書がcallBridgeによって信頼されていないため、コールが失敗する可能性があります。これをテストするには、「`tls sip verify disable`」を使用してcallBridgeでこれを無効にします。

複数のレコーダ？

説明に従って各ルールを設定し、それに応じてアウトバウンドルールを調整します。レコーダに直接送信する方法を使用する場合は、既存のレコーダへの送信規則を動作"続行"に変更し、優先順位が最初の規則より1低い以前の規則の下に新しい送信規則を追加します。最初のレコーダがコール制限に達すると、488 Inacceptable hereをcallBridgeに返信し、callBridgeは次のルールに進みます。

レコーダのロードバランシングを行う場合は、コール制御を使用し、コール制御ルーティングを調整して、複数のレコーダにコールを発信できるようにします。

ストリーマ

MMP

2.9.xから3.0へのアップグレード後、ストリーマを再設定する必要があります。

ステップ1:SIPリスニングインターフェイスを設定します。

`streamer sip listen a 6000 6001` (SIPストリーマがTCPおよびTLSをリッスンするように設定されているインターフェイスとポート)。TLSを使用しない場合は、「`streamer sip listen a 6000 none`」を使用できます)

ステップ2:TLS接続を使用している場合にストリーマが使用する証明書を設定します。

`streamer sip certs <key-file> <cert-file> [crt-bundle]`(これらの証明書がない場合、tlsサービスはストリーマで開始されません。ストリーマはcrt-bundleを使用してcallBridge証明書を confirms)。)

ステップ3：コール制限の設定

`streamer limit <0-500|none>`(サーバが処理できる同時ストリーム数の制限を設定します。この表はドキュメントに記載されており、ストリーマの制限はサーバ上のリソースに合わせる必要があります)。

Table 7: Internal SIP streamer recommended specifications

Number of vCPUs	RAM	Number of 720p streams	Number of 1080p streams	Number of audio-only streams
4	4GB	50	37	100
4	8GB	100	75	200
8	8GB	200	150	200

Key points to note (applies to both new internal recorder and streamer components):

- Number of vCPUs should not oversubscribe the number of physical cores.
- Maximum number of 720p streams supported is 200 regardless of adding more vCPUs
- Maximum number of 1080p streams supported is 150 regardless of adding more vCPUs.
- Maximum number of audio-only streams supported is 200 regardless of adding more vCPUs.

API

api/v1/callProfilesでは、sipStreamUriを設定する必要があります。これは、ストリーミングを開始する必要があるときにcallBridgeがダイヤルするURIです。このURIのドメインをアウトバウンドルールテーブルに追加し、使用するSIPプロキシとしてストリーマ（またはコール制御）をポイントする必要があります。

/api/v1/callProfiles/a7f80cbd-5c0b-4888-b3cb-5109408a1dec

Related objects: [/api/v1/callProfiles](#)

Table view XML view

Object configuration	
streamingMode	automatic
sipStreamUri	stream@streamer.com

次の図は、[Configuration] > [Outbound Calls] にあるアウトバウンドルールのストリーマコンポーネントへの直接ダイヤルを示しています。

Outbound calls

Filter

	Domain	SIP proxy to use	Local contact domain	Local from domain	Trunk type	Behavior	Priority	Encryption
<input type="checkbox"/>	recorder.com	14.49.17.246:5061	Recorder	<use local contact domain>	Standard SIP	Continue	1	Encrypted
<input type="checkbox"/>	streamer.com	14.49.17.246:5001	Streamer	<use local contact domain>	Standard SIP	Continue	1	Encrypted
<input type="checkbox"/>	recorder.com	14.49.17.246		<use local contact domain>	Standard SIP	Stop	0	Auto
<input type="checkbox"/>	streamer.com	14.49.17.246:6000		<use local contact domain>	Standard SIP	Stop	0	Auto
<input type="checkbox"/>					Standard SIP	Stop	0	Auto

この図は、コール制御(Cisco Unified Communications Manager(CUCM)やExpresswayなど)を介したレコーダコンポーネントへのコールを示しています。

Outbound calls

Filter

	Domain	SIP proxy to use	Local contact domain	Local from domain	Trunk type	Behavior	Priority	Encryption
<input type="checkbox"/>	recorder.com	14.49.17.229		<use local contact domain>	Standard SIP	Continue	1	Encrypted
<input type="checkbox"/>	streamer.com	14.49.17.229		<use local contact domain>	Standard SIP	Continue	1	Encrypted
<input type="checkbox"/>	recorder.com	14.49.17.252		<use local contact domain>	Standard SIP	Stop	0	Auto
<input type="checkbox"/>	streamer.com	14.49.17.252		<use local contact domain>	Standard SIP	Stop	0	Auto
					Standard SIP	Stop	0	Auto

Annotations: A green arrow points from the 'SIP proxy to use' column to the 'Local contact domain' column. A red arrow points from the 'SIP proxy to use' column to the 'SIP proxy to use' column. A blue 'CUCM' label is placed above the 'Local contact domain' column. A red 'Expressway' label is placed above the 'SIP proxy to use' column.

注：ストリーマでSIP TLSを使用するように設定し、コールが失敗する場合は、MMPの callBridgeノードでTLS SIP検証が有効になっているかどうかを確認します。 MMPコマンドは「tls sip」です。 ストリーマ証明書がcallBridgeによって信頼されていないため、コールが失敗する可能性があります。 これをテストするには、「tls sip verify disable」を使用してcallBridgeでこれを無効にします。

複数のストリーマ？

説明に従って各ルールを設定し、それに応じてアウトバウンドルールを調整します。 ストリーマに直接適用する方法を使用する場合は、既存のレコーダーへのアウトバウンド規則を「続行」の動作に変更し、優先度が最初の規則より1低い以前の規則の下に新しいアウトバウンド規則を追加します。 最初のストリーマがコール制限に達すると、488 Inacceptable hereをcallBridgeに送り返し、callBridgeは次のルールに進みます。

ストリーマのロードバランシングを行う場合は、コール制御を使用してコール制御ルーティングを調整し、複数のストリーマにコールを発信できるようにします。

Expresswayの考慮事項

Cisco Expressway for Web Proxyを使用する場合は、CMSのアップグレード前に、ExpresswayでX12.6以上が実行されていることを確認する必要があります。これは、Webプロキシが機能し、サポートされるためにCMS 3.0が必要です。

CMS 3.0で使用すると、ExpresswayよりもWebアプリ参加者のキャパシティが増加します。 大規模なOVA Expresswayの場合、予想される容量は150のフルHDコール(1080p30)または200のその他のタイプのコール(720p30など)です。 この容量は、Expresswayをクラスタ化することによって増やすことができます。最大6ノード(4はスケーリングに使用し、2は冗長性に使用するため、最大600のフルHDコール、または800のその他のタイプのコールまで可能)。

Table 3: Cisco Meeting Server web app call capacities – external calling

Setup	Call Type	CE1200 Platform	Large OVA Expressway
Cisco Expressway Pair (X12.6 or later)	Full HD	150	150
	Other	200	200

CMSエッジ

CMS Edgeは、外部Webアプリケーションセッション用にExpresswayよりも高い容量を提供するため、CMS 3.1に再導入されました。推奨される設定は2つあります。

スモールエッジ仕様

4 GB RAM、4 vCPU、1 Gbpsネットワークインターフェイス

このVM Edge仕様は、1つのCMS1000音声およびビデオロード容量 (48 x 1080p、96 x 720p、192 x 480p、および1000音声コール) をカバーするのに十分なパワーを備えています。

導入には、CMS1000ごとに1台のsmallエッジサーバを使用するか、CMS2000ごとに4台のsmallエッジサーバを使用することをお勧めします。

大規模エッジ仕様

8 GB RAM、16 vCPU、10 Gbpsネットワークインターフェイス

このVM Edge仕様は、350 x 1080p、700 x 720p、1000 x 480p、および3000 x音声コールの単一のCMS2000音声およびビデオ容量をカバーするのに十分なパワーを備えています。

導入には、CMS2000またはCMS1000ごとに1台の大規模エッジサーバを使用することをお勧めします。

Type of Calls	1 x 4 vCPU VM call capacity	1 x 16 vCPU VM call capacity
Full HD calls, 1080p30 video	100	350
HD calls, 720p30 video	175	700
SD calls, 448p30 video	250	1000
Audio Calls (G.711)	850	3000

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。