Cisco Webex イネーブルメントラボ v5

最終更新日：2020 年 5 月 16 日

このラボについて

この事前設定済みラボのガイドには、次の内容が含まれています。

制限/免責事項

本ガイドのシナリオは、このラボで指定された要件を満たしながら、Cisco® Webex Control Hub ソリューションを設定する 1 つの方法を示すものです。お客様の環境や目標/要件によって、さまざまな方法があります。設計やインストールを実際に行う前に、最新のすべてのシスコ公式マニュアルに必ず目を通してください。このラボは主に教材としての利用を意図しています。特定の情報をお伝えするために、場合によってはベストプラクティスに従っていないことがあります。

カスタマイズオプション

このラボに関連するカスタマイズオプションはありません。

要件

表 1 に、このデモンストレーションの要件の概要を示します。

表 1. 要件

必須	オプション
Cisco AnyConnect® クライアント ラップトップ Webex Calling 対応 Cisco Multiplatform Phone（MPP）（デスクトップ/モバイルコールクライアントも使用可能） Room デバイスには下記のいずれかが必要： Cisco Webex DX/Board/Room Kit	なし

このソリューションについて

Cisco Webex® は、ビデオ会議（Webex® Meetings）、チームコラボレーション（Webex Teams™）、クラウドコール（Webex Calling）などのさまざまなサービスで構成されています。

Cisco Webex Meetings の概要

デジタル時代の現在、実際に出かけるコストや手間をかけずに国境を越えて簡単に連携できますが、人間関係は依然として重要です。ビデオは、ソーシャルメディアから友人や家族との個人的な会話に至るまで、日常のやりとりの隅々に広がっています。健全なビジネスは固い人間関係から始まります。そして、固い人間関係は、強固なコミュニケーションを基盤として築かれます。そのため Cisco Webex Meetings では、コミュニケーションとコラボレーションの中心としてビデオを位置づけ、1 億 3000 万人以上の人々が最高の状態で対面できるようにサポートしています。

Cisco Webex Meetings を利用すれば、何百キロ離れていても、すべてのメンバーが同じ資料を見て、同じ音声を聴きながら連携して効果的に作業することが簡単にできるようになります。企業内でも、外部からでも、モバイルやデスクトップ、あるいはビデオルームデバイス（サードパーティ製デバイスを含む）を使用して誰でも会議に参加できます。簡単で一貫性のある会議エクスペリエンスのため、複雑な技術に煩わされることがなく、全員が会議に 100% 集中できます。組織には、ビデオ会議エクスペリエンスの複雑さを解消し、同じ会議アプリで明瞭な音声とコンテンツ共有を両立できるソリューションが必要なのです。Cisco Webex を利用すれば、信頼性に優れ、より効果的で安全な会議を実現できます。

Cisco Webex Meetings には次のようなメリットがあります。

- デバイスを問わないシンプルなビデオファーストのエクスペリエンス
    - ビデオ機能とコンテンツ共有機能が統合されたビデオファーストの会議に参加すれば、顧客、パートナー、従業員とのコラボレーションをより効果的に行うことができます。出張する必要はありません。
    - シスコの実績あるビデオルームデバイスと Webex Meetings を組み合わせることで、実際と同様の会議を実現できます。
    - サードパーティ製のビデオデバイスから参加することもできます。Microsoft Skype for Business でも可能です。
    - ビデオシステムのプロキシミティ検出機能を利用して会議に簡単にコールバックできます。
- 業界トップクラスのモバイルエクスペリエンス
- 会議のスケジュール設定や参加が容易
    - ダウンロードやプラグインは不要です。ブラウザでの業界トップクラスの操作性を誇る Webex Web アプリを利用して、会議に簡単に参加できます。主要なブラウザですべてのミーティング機能を利用可能です。
    - すべてのデバイスで一貫した参加方式：大きな緑色のボタンをタップするだけです。
    - デスクトップ、モバイル、ビデオ、ブラウザなど、あらゆるデバイスから簡単に会議に参加したり、会議を主催したりできます。ダウンロードやプラグインは必要ありません。
    - モバイルデバイスであっても、@webex キーワードを追加するだけで簡単に会議のスケジュールを設定できます。現在の市場でトップクラスの簡単さです。
- よく利用するツールに統合可能
- セキュアでスケーラブルなグローバルプラットフォームで提供され、妥協のないエクスペリエンスを実現
    - 業界トップクラスのシスコの専門知識に基づいて構築されたマルチレイヤセキュリティにより、ユーザエクスペリエンスを犠牲にすることなく、会議に伴う心配を解消します。
    - 音声の統合
    - イベント、トレーニング、リモートサポートなどの専門的な会議向けの専用ソリューション

Cisco Webex Teams の概要

かつてないほどビジネスのイノベーションが急速に進展し、競争が激化しています。ビジネスの成否は、どれだけチームが俊敏になれるかにかかっています。チームには、社内の同僚だけでなく、外部の専門家やパートナーのエコシステムも含まれます。このようなチームをサポートするには、メンバーを簡単に統合し、高い生産性で連携して作業できるようにするツールが必要です。また、ますます複雑になるセキュリティ要件やコンプライアンス要件にも対応する必要があります。これらの要件は、お客様の情報を安全に保護するための鍵となります。それでは、Cisco Webex によって実現されるチーム コラボレーション エクスペリエンスについて見ていきましょう。

Cisco Webex Teams は、場所や時間を問わずにユーザがチームワークを維持できる、使いやすいコラボレーション ソリューションです。Webex Teams アプリケーションを使用すれば、短期間のプロジェクトの実施から長期的なビジネスチャンスの獲得まで、あらゆることを対象にセキュアな仮想ワークスペースを構築できます。メッセージングとファイル共有により日々の共同作業がシンプルになります。また、サードパーティ製アプリケーションも統合できるため、シームレスなワークフローを実現できます。リアルタイムにコミュニケーションをとれるため、生産性とチームワークが向上します。すぐに通話を開始したり、ボタンをタッチするだけで画面を共有できる高画質のビデオ会議を開催したりできる上、会議後も接続を維持できます。デジタルホワイトボードにアイデアを表現すれば、同僚がいつでも意見を追加できます。チームでの作業が会議室に移れば、Webex Teams も会議室で利用できます。アプリケーションを Webex デバイスに接続するだけで、ワイヤレスで会議を開始し、画面を共有したり、実際の大きさでホワイトボードの描画をキャプチャしたりすることができます。これが Webex Teams の特長です。すべての作業を円滑に進めることができます。ぜひご利用ください。

コミュニケーション ソリューションは、モバイルに対応し、迅速にコラボレーションを実施できるものでなければなりません。そのためには、インフラストラクチャとアプリケーションにおける技術革新とモバイルデバイスが必要です。Cisco Webex のサービスを利用すれば、業界をリードするコミュニケーションツールを緊密に統合して実際と同様の会議を開催し、すぐにコミュニケーションをとることができます。これまでにないコラボレーション体験を実現できるのは、シスコのクラウドだけです。Webex Teams は継続的なデリバリモデルを採用しているため、機能が定期的にリリースされます。help.webex.com をチェックして常に最新の情報を確認してください。

チームワークを促進するためのツール

メッセージングとコンテンツ共有：Webex Teams と Spaces を利用すれば、メンバーが簡単に連携できます。メッセージ送信、会議、ファイル共有、ホワイトボード機能により、電子メールやインスタントメッセージを探し続ける時間が短縮され、仕事に集中できます。

チームベースの会議：生産性が大きく向上します。スペース内では誰でも会議のスケジュールを設定して開始したり、記録したりできます。会議後もワークスペースが接続されているため、作業を継続できます。

ホワイトボード：アプリでスケッチを共有できます。また、Cisco Webex Board のオールインワン ワイヤレス プレゼンテーション、デジタルホワイトボード、ビデオ会議機能を利用すれば、Cisco Webex Teams の機能がさらに強化されます。

通話：アプリ、IP 電話、会議室のビデオデバイスのどこからでも通話できます。Cisco Webex Calling でクラウドに導入することも、オンプレミスまたはパートナーがホストするテレフォニーサービスに接続することも可能です。

統合およびボット：Webex Teams でつながることで、限られたシステムとアプリでの運用が可能になります。統合機能によりワークフローを効率化し、ボットでアクションを自動化できます。詳細については、Webex App Hub を参照してください。

Cisco Webex ハイブリッドサービス

Cisco Webex ハイブリッドサービスを利用すれば、オンプレミスのユニファイド コミュニケーションとコラボレーションの効果が向上します。ハイブリッドサービスによって、既存のネットワークリソースとオンプレミスのユニファイド コミュニケーション サービスをクラウド内の Cisco Webex Teams プラットフォームに簡単に接続できます。そのため非常に優れたコラボレーション機能を利用できるようになり、一貫性のあるユーザエクスペリエンスと管理者エクスペリエンスが実現されます。

クラウドのコラボレーションサービスを利用する組織がますます増えています。なぜでしょうか。クラウドサービスには以下のような特長があるからです。

- 短時間で簡単に導入可能
- オンプレミスシステムの先行設備投資が不要
- IT スタッフの負荷を軽減して、他の優先事項に注力できる

しかし多くの組織では、すべてのサービスをクラウドに移行することが不可能であるか、あるいはそれを望んでいません。オンプレミスで保有するすべての資産を更新するには時期尚早である場合が多く、単に既存のコラボレーションツールをクラウドのツールで強化すればよいと考える組織も少なくありません。しかしながら、クラウドとオンプレミスのツールが混在し、それらが一体となって機能していない場合には、ユーザ エクスペリエンスやツールの一貫性がなくなり、分断される恐れもあります。

シスコはこの問題を、Cisco Webex ハイブリッドサービスによって解決します。このサービスでは、オンプレミスで保有する資産とクラウド内の Cisco Webex Teams を接続することで、統合された単一のエクスペリエンスを実現します。Webex Teams の機能を必要とする組織では、その機能を現在展開している資産と統合することで、優れたエンドユーザ エクスペリエンスや管理者エクスペリエンスを実現できます。

利用可能なハイブリッドサービス

ハイブリッド カレンダー サービス：このサービスでは、オンプレミスの Microsoft Exchange や、Office 365、Google カレンダーと、Cisco Webex Teams および Cisco Webex Meetings 機能が統合されます。ハイブリッド カレンダー サービスでは、会議をスケジュールすると、Cisco Webex Teams ワークスペースが自動的に作成されます。たとえば、会議の招待状の場所欄に「@meet」というキーワードを追加すると、自動的に Cisco Webex Teams ワークスペースが作成され、会議の招待状に会議参加情報が設定されます。ワークスペースが不要な場合は、招待状の場所フィールドに「@webex」というキーワードを追加すると、ワークスペースは作成されずに、会議の参加情報が自動的に設定されます。ハイブリッド カレンダー サービスを使用すると、Cisco Webex ユーザはボタンを 1 回押すだけで、アプリ内およびビデオデバイス上のほぼすべての会議に参加できます。

ハイブリッド ディレクトリ サービス：このサービスでは、Active Directory が Cisco Webex Teams に接続されるため、Cisco Webex Teams アプリからすべての社内連絡先を参照できます。そのため、クリックするだけで会議、メッセージ、通話を実行できます。また、Microsoft Active Directory と Cisco Webex Teams ユーザ管理システム間でユーザを同期できます。ハイブリッド ディレクトリ サービスでは、Microsoft Active Directory ユーザと Cisco Webex Teams が自動的に同期されるため、ユーザの管理（作成、更新、削除）がシンプルになり、Cisco Webex Teams のユーザ情報が常に最新の状態に維持されます。

Cisco Webex Video Mesh：この革新的な機能により、Cisco Webex ビデオ会議機能をオンプレミスとクラウドのどちらに導入するかという判断が不要になります。このサービスでは、Cisco Webex Meetings エンジンをオンプレミスに配置し、ローカルでメディアを処理します。そのためインターネット帯域幅が最適化され、オンプレミスと同じビデオ品質が得られます。またそれは、シンプルで柔軟性に優れた新機能が、クラウドから繰り返し迅速に提供されることで実現されます。

ハイブリッド データ セキュリティ サービス：セキュリティを重視するお客様に最適なシスコのハイブリッド データ セキュリティ サービスは、お客様がオンプレミスで暗号鍵を所有して管理できるようにすることで、業界標準のデータセキュリティの一歩先を行きます。また、エンドツーエンドで暗号化することで、すべてのメッセージ、ファイル、ホワイトボードが常に安全で利用可能な状態に保たれます。暗号化しても、検索などの機能はすべて利用できます。Cisco Webex Teams では、データのプライバシーが確保されます。すべてのコンテンツ、メッセージ、ファイルだけでなく、ホワイトボードの描画も対象です。

Cisco Webex デバイス向けハイブリッドコールサービス：このサービスは非常に柔軟性に優れているため、オンプレミスとクラウドに登録済みのエンドポイントを組み合わせて利用する組織に最適です。

ハイブリッドコールサービスを利用すれば、Cisco Webex Places に登録した Room デバイス、Desk デバイス、Cisco Webex Board デバイスにハイブリッドコール機能を追加できます。クラウドに登録された Cisco Webex デバイスでハイブリッドコールサービスを有効にすると、企業内のシステムにも接続できます。Webex Places 内の Cisco Webex デバイスは、既存のオンプレミスダイヤルプランに組み込まれ、ユーザの内線番号や PSTN にコールしたり、コールを受信したりできるようになります。

この機能により、オンプレミスに登録されたエンドユーザのデバイスとクラウドに登録されたデバイス間でシームレスにコールを転送できます。

Cisco Webex Calling 概要

オンプレミスの PBX に代わってグローバルに利用できるマルチテナントのクラウドベース ソリューションを待ち望んでいた企業に、信頼できるブランドから満を持しての登場です。Cisco Webex Calling は、毎月のサブスクリプションサービスとして、従来の PBX の機能をすべて提供します。特長は次のとおりです。

- エンタープライズグレードの高度な PBX 機能の数々
- モバイルユーザおよびデスクトップユーザ向け Cisco Webex Calling アプリと Cisco Webex Teams コラボレーションアプリの統合による充実したユーザエクスペリエンス
- Cisco Webex Meetings と、Cisco IP フォン 6800/7800/8800 シリーズ デスクフォン、アナログ ATA をはじめとする Webex デバイスによる統合ユーザエクスペリエンス
- 世界各地に分散し、地理的な冗長性が確保されたデータセンターからの提供
- サービスを利用できる国がすべての地域で増加中
- Cisco Collaboration Flex Plan を通じて、オンプレミスの Cisco Unified Communications Manager（UCM）ライセンスへの既存の投資を保護
- クラウドおよび、クラウドとオンプレミスのハイブリッド導入をサポートし、お客様のペースでスムーズにクラウドに移行可能

トポロジ

このデモンストレーションでは、サーバとして仮想マシンを数台使用します。ほとんどのサーバは、管理者レベルのアカウントですべて設定できます。管理者アカウントの詳細については、本ラボガイドの手順およびサーバ詳細表で説明しています。

図 1. dCloud のトポロジ

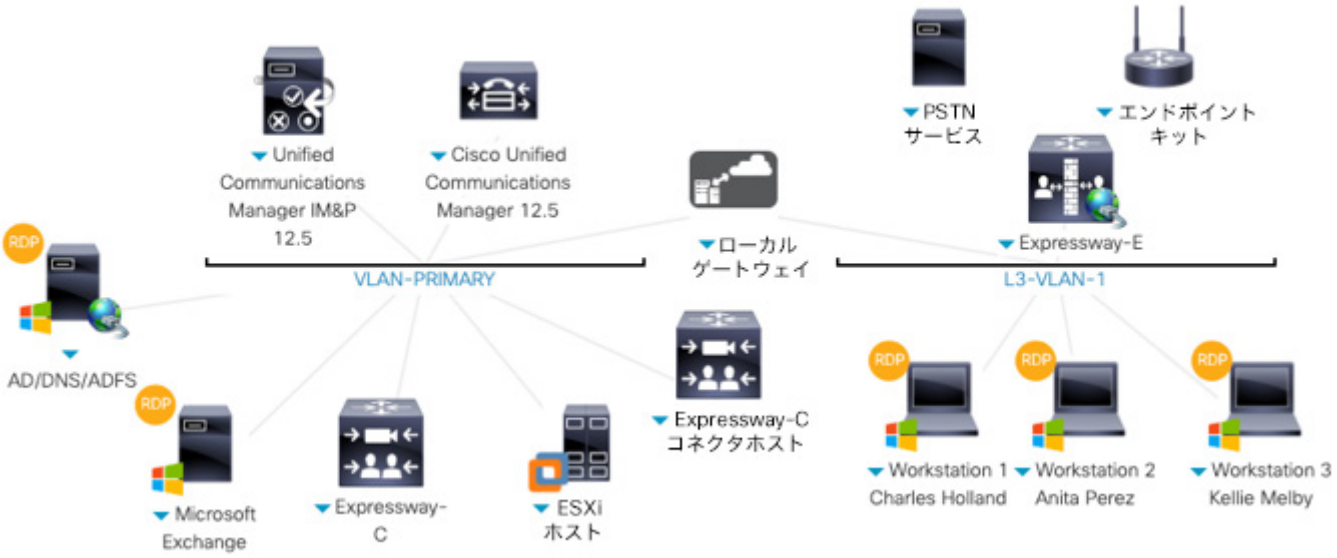


表 2. 機器の詳細

名前	説明	ホスト名（FQDN）	IP アドレス	ユーザ名	パスワード
CUCM1	Cisco Unified Communications Manager 12.5	cucm1.dcloud.cisco.com	198.18.133.3	administrator	dCloud123!
IM & P	IM & Presence 12.5	cup1.dcloud.cisco.com	198.18.133.4	administrator	dCloud123!
Exp-C	Expressway-C（コア）X12.5	vcsc.dcloud.cisco.com	198.18.133.152	admin	dCloud123!
Exp-E	Expressway-E（エッジ）X12.5	vcse.cbXXX.dc-YY.com	パブリック IP（セッションの詳細情報を参照）	admin	dCloud123!
Exp-Base	Expressway-C コネクタホスト X12.5	exp-cc.dcloud.cisco.com	198.18.133.223	admin	dCloud123!
ESXi ホスト	VMware ESXi 6.5 ホスト	esxi1.dcloud.cisco.com	198.18.134.27	root	dCloud123!
Webex-VMN	Cisco Webex Video Mesh Node	vmn1.dcloud.cisco.com	198.18.135.21	admin	dCloud123!
ローカルゲートウェイ	CSR1000V	N/A	198.18.133.226	admin	dCloud123!
AD1	Active Directory、DNS、AD FS	ad1.dcloud.cisco.com	198.18.133.1	administrator	dCloud123!

Exchange	Microsoft Exchange 2016	mail1.dcloud.cisco.com	198.18.133.2	administrator	dCloud123!
Workstation 1	Windows 10	wkst1.dcloud.cisco.com	198.18.1.36	cholland	dCloud123!
Workstation 2	Windows 10	wkst2.dcloud.cisco.com	198.18.1.37	aperez	dCloud123!
Workstation 3	Windows 10	wskt3.dcloud.cisco.com	198.18.1.38	kmelby	dCloud123!

セッションユーザ

表 3 には、セッションで使用可能な事前設定済みユーザの詳細情報が記載されています。

表 3. ユーザの詳細

ユーザ名	ユーザ ID	パスワード	エンドポイントデバイス	内線番号	導入モデル
Charles Holland	cholland	dCloud123!	Cisco Jabber/Teams	6018	ハイブリッド
Anita Perez	aperez	dCloud123!	Cisco Jabber/Teams	6017	ハイブリッド
Kellie Melby	kmelby	dCloud123!	Cisco Jabber/Teams	6050	ハイブリッド
Rebekah Melby	kmelby	dCloud123!	Cisco Calling アプリまたは MPP	86022	クラウド
Taylor Bard	tbard	dCloud123!	Teams/Cisco Calling アプリまたは MPP	86021	クラウド

はじめに

プレゼンテーションの前に

Cisco dCloud では、実際の対象者の前でプレゼンテーションを行う前に、アクティブなセッションを使用して、このドキュメントのタスクを実施しておくことを強く推奨します。そうすることで、ドキュメントとコンテンツの構成に慣れることができます。

場合によっては、環境を元の構成にリセットするため、このガイドのシナリオを完了した後に新しいセッションをスケジュールする必要があります。

プレゼンテーションを成功させるには入念な準備が不可欠です

次の手順に従ってコンテンツのセッションをスケジュールし、プレゼンテーション環境を設定します。

1. dCloud セッションを開始します。[手順を見る] [英語]（講師がいる場合はスキップ）

注：セッションがアクティブになるまで、最長で 45 分かかることがあります。

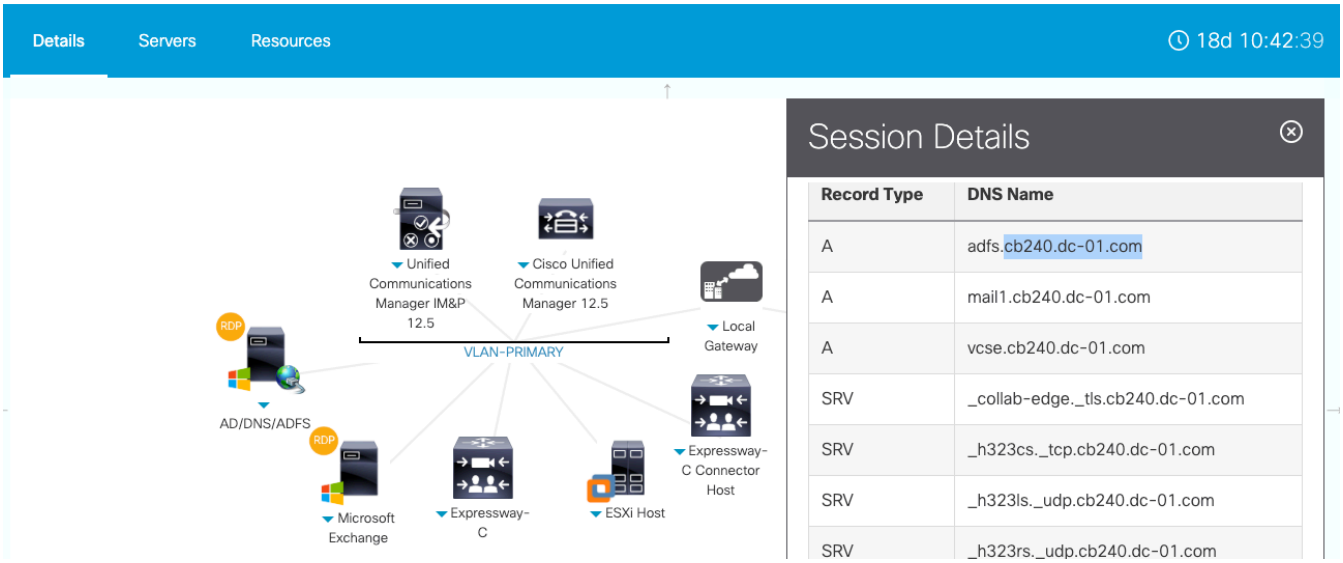
2. [表示（View）] をクリックしてアクティブなセッションを開きます（講師がいる場合はスキップ）。

3. スタンドアロンのラップトップまたは他のデバイスから直接セッションに接続する場合は、**ラップトップ**に Cisco AnyConnect をインストールし、Cisco dCloud ユーザインターフェイスで AnyConnect のログイン情報を使ってアクセスします。[手順を見る] [英語]
   - **推奨方法：Cisco AnyConnect** [手順を見る] [英語] および**ラップトップのローカル RDP クライアント**を使用します。
   - **Windows ユーザ：**各仮想マシンへの接続を保存する場合、適切なバージョンの Remote Desktop Manager を使用することをお勧めします。マネージャの例としては、Microsoft 社の **Remote Desktop Connection Manager**（https://www.microsoft.com/en-us/download/details.aspx?id=44989）があります。
   - **Mac ユーザ：**仮想マシンに接続するには、**Microsoft Remote Desktop（MRD）**[] または **CoRD** [] アプリケーションを使用することをお勧めします。MRD は、Mac App Store から無料でダウンロードできます。CoRD は http://cord.sourceforge.net/ から無料でダウンロードできます。どちらのアプリケーションを使用しても、各仮想マシンの接続を保存できます。**Mac に付属している Microsoft リモート デスクトップ クライアントは使用しないでください。AD1 および Mail1 仮想マシンとの接続にセキュリティ上の問題があります。**
4. このラボでは、Multiplatform Phone（MPP）ファームウェアでデスクフォンをロードする必要があります。
5. Room デバイス（DX/Room Kit/Webex Board）でも vCE8.1 以降のファームウェアが必要です。講師がいる場合は、講師が適切なファームウェアを Room デバイスにインストールしています。Room デバイスを更新するもう 1 つの方法として、cisco.com から **.pkg** ファイルをダウンロードして、デバイスを直接アップグレードすることもできます。**ヒント：**アップグレードプロセスについては、http://upgrade.cisco.com/ を参照してください。
6. 各デバイスのファームウェアが適切なことを確認したら、デバイスを初期設定にリセット（初期設定状態でない場合）してからラボを開始します（講師がいる場合はスキップ）。

注：正しい結果が得られるように、Web ブラウザには Firefox または Chrome を使用してください。

7. Cisco Webex ハイブリッドサービスのデモンストレーションを行うために、ラボでは Cisco Jabber を使用します。また、dCloud ルータを追加し、物理的な電話機をセルフプロビジョニングすることで、ハイブリッドサービスのデモンストレーションを行うこともできます。
8. このラボを実行するには、dCloud ダッシュボードのセッションページにある、[セッションの詳細（Session Details）] タブの情報が必要になります。Collaboration Edge ドメイン情報を取得してください。セッションごとにドメインは異なります。次の図はあくまで 一例です。実際のセッションで次の図の情報は使用しないでください。ラボの途中で参照できるように、この情報をメモしておくことを強くお勧めします。

[セッションの詳細（Session Details）] タブの例



シナリオ 1. 最初のラボの概要およびセットアップ

このシナリオでは、基本ラボのセットアップについて詳しく説明します。また、この後完了する必要があるいくつかの初期タスクについても説明します。Webex のトライアル版はすでに開始されています。また、お客様の組織管理者である Charles Holland は、パスワードをすでに **dCloud123!** に設定しています。お客様向けトライアルを作成する手順は次のリンクより確認できます。https://help.webex.com/ja-jp/npv2y12/Set-Up-a-Cisco-Webex-Trials-Program-for-Customers

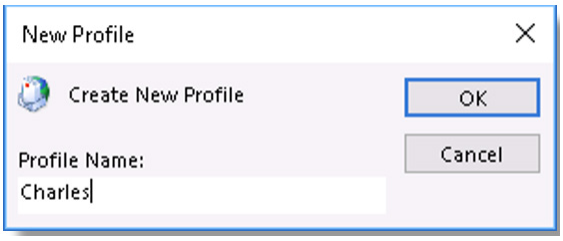
ラボで使用するユーザも設定済みで、パスワードは **dCloud123!** に設定されています。そのため、アカウントをアクティブにしてパスワードを設定する時間を他のトピックに当てることができます。ユーザが設定されていない組織では、1 人ずつユーザを追加する、CSV ファイルをインポートする、ディレクトリコネクタを使用する、のいずれかの方法、またはすべての方法を組み合わせてユーザを作成します。ディレクトリコネクタを使用して Microsoft Active Directory からユーザをインポートする手順については、付録 C を参照してください。ユーザがすでに設定されていても、ディレクトリコネクタの設定手順を確認したい場合は、手順を実施することもできます。

手順

初期の自動化スクリプトによってトライアル環境が作成され、Charles のパスワードが設定済みであることを確認します。

1. ラボセッションにまだ接続していない場合は、**Cisco AnyConnect** を使用して **VPN 接続**します。ログイン情報は、講師から提供されるか、アクティブなセッションの [セッションの詳細（Session Details）] タブに記載されています。
2. Workstation 1（**198.18.1.36**）への RDP 接続を確立し、ユーザ名：**dcloud\cholland**、パスワード：**dCloud123!** でログインします。セキュリティの警告が発生した場合はすべて無視するか受け入れます。
3. タスクバーのアイコン [] をクリックして **Microsoft Outlook** を開きます。
4. プロファイル名に **Charles** と入力し、[OK] をクリックします。

新規プロファイル



5. [受信トレイ（Inbox）] に、「Cisco Webex トライアルへようこそ（Welcome to Cisco Webex Trial）」という件名の電子メールと「パスワードが更新されました（Your password was updated）」という件名の電子メールがあります。件名が「Webex ラボ警告（WEBEX LAB WARNING）」となっている場合は、その電子メールを読んで、ラボの設定に問題がなかったか確認します。

6. Office 365 のシナリオを実行する場合は、件名が「**クラウドトライアル電子メールアドレス（CLOUD TRIALS EMAIL ADDRESS）**」となっている電子メールから、**trial** で始まる電子メールアドレスを取得します。Office 365 トライアル版を作成した場合は、必ず一意の電子メールアドレスを使用することになります。この電子メールアドレスは、Charles Holland の電子メールボックスにルーティングされます。
7. Chrome Web ブラウザを開いて **https://admin.webex.com** にアクセスし、**cholland@cbXXX.dc-YY.com** と入力します。[サインイン（Sign In）] をクリックします。
8. パスワード：**dCloud123!** を入力し、[サインイン（Sign In）] をもう一度クリックします。
9. **サービス利用規約**に関するプロンプトが表示されたら、[同意する（Accept）] をクリックします。
10. これで Cisco Webex Control Hub にログインできました。ここからが、組織の設定に一番時間がかかる部分です。このポータルでは、Webex サービスを設定します。最初のページは [概要（Overview）] です。このページでは、利用可能なすべてのサービスとそのステータスを簡単に確認できます。また、重要な情報に関する通知メッセージも表示されます。

ユーザライセンスの自動割り当て

Control Hub では、すべての新規ユーザにユーザライセンスを自動的に割り当てることができます。そのためには、自動割り当てテンプレートを作成する必要があります。

1. Control Hub で [ユーザ（Users）] に移動し、[ユーザの管理（Manage Users）] をクリックします。ユーザリストには、事前に設定された 8 人のユーザが表示されます。
2. [ライセンス（Licenses）] セクションで、[自動割り当てテンプレートの設定（Set up Auto-Assign Template）] をクリックします。
3. [メッセージング（Messaging）] 列で、**Webex Teams** の横にあるチェックボックスをオンにします。
4. [会議（Meeting）] 列で、すべてのチェックボックスをオンにします。
5. ご覧のように、このページで他のライセンスを割り当てることができます。ここでは、前述のライセンスのみを割り当てます。
6. [次へ（Next）] をクリック後、[保存（Save）] をクリックします。
7. [ユーザの管理（Manage Users）] をもう一度クリックします。
8. [ライセンス（Licenses）] セクションに [アクティブ（Activated）] と示されています。
9. 省略記号 [▪ ▪ ▪] をクリックします。ここで、既存のテンプレートの変更、非アクティブ化、削除を行えます。設定はそのままにします。
10. [ユーザの管理（Manage Users）] ウィンドウを閉じます。

ユーザの変換

組織の電子メールドメインを使用して Webex サービスにサインアップしたユーザを管理する場合は、対象ユーザの移行を組織に申請します。ユーザを申請すると、ライセンスを割り当てることができます。

ユーザアカウントを組織に申請する場合、即時移行を選択できます。組織に即時移行を申請したユーザは、すぐに移行されます。ユーザに、サインインページへのリンクが記載された電子メールが送信されます。サインインページでは、古いアカウントの処理方法に関して次のオプションがあります。

- 古いアカウントに関連付けられている電子メールアドレスを変更する
- 古いアカウントとコンテンツを削除する

ユーザの後日移行を選択した場合、ユーザは、14 日以内に古いアカウントの処理方法を決定する必要があります。ユーザが Webex Teams アカウントにサインアップした場合、ユーザは Webex Teams での会話内容を古いアカウントから新しいアカウントに移行できます。14 日以内に古いアカウントの処理方法を決めなければ、ユーザは自動的に移行されます。またその場合、Webex Teams での会話内容も自動的に移行されます。

ユーザの後日移行を選択した場合、サインインページへのリンクが記載された電子メールが送信されます。サインインする際に、次のオプションがあります。

- 古いアカウントに関連付けられている電子メールアドレスを変更する
- 古いアカウントから新しいアカウントに Webex Teams での会話内容を転送する
- 古いアカウントとコンテンツを削除する

ユーザを移行するオプションを選択できるようになるには、ドメインの確認または申請が必要です。これはすでに完了しています。この手順については、こちらを参照してください。

1. [概要（Overview）] ページに移動します。
2. [オンボーディング（Onboarding）] カードには、少なくとも 2 人の新規ユーザ候補が表示されています。このユーザは、ある時点で Webex Teams にサインインしたユーザです。ユーザを新しいお客様組織に移行することもできます。
3. [確認（Review）] リンクをクリックします（[ユーザ（Users）] > [ユーザの管理（Manage Users）] > [ユーザの移行（Convert Users）] の順にクリックしてこのページに移動することもできます）。
4. 新しいウィンドウで、移行候補リストに少なくとも 2 人のユーザが表示されます（RDP ウィンドウのサイズが小さい場合は、画面上にユーザが表示されない場合があります）。ユーザの横のチェックボックスをオンのままにします。
5. [Webex Teams での会話内容を新ユーザに引き継ぐ（Allow users to bring their Webex Teams conversations with them）] の横のチェックボックスをオンにして、ユーザが以前の会話内容を引き継げるようにします。
6. [次へ（Next）] をクリックします。
7. 自動割り当てテンプレートを作成しているため、これらの新しいユーザには、先に選択したサービスが自動的に割り当てられます。[保存（Save）] をクリック後、[終了（Finish）] をクリックします。
8. [ユーザ（Users）] ページが表示され、ユーザが追加されたことを確認できます。

ユーザ事前設定の検証

前述したように、ラボの基本設定ではユーザが事前に設定されています。事前設定されているユーザには、Webex Teams と Webex Team Meetings サービスも設定されています。

1. ユーザリストからユーザを選択します。
2. ポップアップウィンドウに、ユーザに設定されているサービスの概要が表示されます。[編集（Edit）] をクリックします。
3. 次のポップアップウィンドウで、各ユーザに設定されているサービスが少なくとも 2 つ（Webex Teams と Webex Team Meetings）表示されます。ラボの後半では、他のユーザに別のサービスを設定します。ここでは [キャンセル（Cancel）] をクリックします。
4. このページでは、ユーザごとに複数のハイブリッドサービスを設定することもできます。これは別のシナリオで実施します。
5. [管理者権限（Administrator Roles）] をクリックします。
6. ここでは、ユーザに Control Hub へのアクセス権を設定できます。フルアクセス権を設定することも、制限付きのアクセス権を設定することもできます。

Charles の Webex Meetings にパーソナルルームが設定されていることを確認する

Charles は、ラボ全体で自分の Webex Meetings パーソナルルームを利用します。そのため、Control Hub にいる間に先に進んで、Charles に Webex Meetings が設定され、パーソナルルームがセットアップされていることを確認します。

1. ユーザリストから **Charles** を選択します。
2. Charles のサービスで [会議（Meeting）] をクリック後、[会議サイトのURL（meeting site URL）] をクリックします。
3. 下にスクロールし、[ユーザ権限（User Privileges）] をクリックします。
4. [パーソナルルーム（Personal Room）] と [ビデオシステムから会議に参加（Join meetings from video systems）] がオンになっていることを確認します。いずれかがチェックされていない場合は、ここでチェックして [保存（Save）] をクリックします。

Control Hub のタイムアウト

Control Hub と Webex Teams の Web クライアントのログインタイムアウト時間を設定できるようになったため、ラボでの作業がやりやすくなっています。Control Hub のデフォルトのログインタイムアウト時間は 20 分です。ラボでは、[タイムアウトなし（No timeout）] に設定して、ログインしなおす回数を減らすことができます。

1. [設定（Settings）] に移動し、[アイドルタイムアウト（Idle Timeouts）] まで下にスクロールします。

2. [Webex Controlアイドルタイムアウト（Webex Control Idle timeout）] セクションで、[Control Hubタイムアウト（Control Hub timeout）] ドロップダウンメニューを [タイムアウトなし（No Timeout）] に変更します。実稼働環境では、タイムアウトなしに設定するとセキュリティチームから問題視される可能性があります。このパラメータを設定する際には、組織のセキュリティガイドラインに従ってください。

O365 事前設定（オプション）

ラボの後半では、Microsoft O365 と統合します。統合するには、独自の O365 サイトが必要です。独自のサイトがない場合は、O365 トライアルサイトをすぐに作成できます。O365 トライアルサイトを作成して完全に設定するには時間がかかる（最大 60 分程度）ため、ここで O365 トライアルサイトの作成を開始して、統合シナリオを開始するまでにプロセスをすべて完了しておくことを強くお勧めします。O365 の統合を予定している場合は、しばらく時間がかかる場合があります。シナリオ 8 に進み、**O365 と Webex Teams の初期統合**セクションを完了してから、シナリオ 2 に戻ります。O365 統合シナリオを実施する予定がない場合は、このままラボを進めます。

シナリオ 2. Room デバイスと機能の設定

このシナリオでは、Room デバイス（DX/SX/Room Kit/Room 55 ~ 70/MX/Webex Board）を登録し、組織の顔認識機能と Webex Assistant も有効にします。

組織のデバイス機能の設定

1. このセクションでは、組織の**顔認識機能**と Webex Assistant を設定します。
2. **Cisco Webex Control Hub**（https://admin.webex.com）にログインしているブラウザウィンドウに戻ります。
3. [設定（Settings）] タブをクリックします。
4. [顔認識（Facial Recognition）] セクションまで下にスクロールし、[設定の確認（Review Setting）] をクリックします。
5. 次のポップアップウィンドウで、[名前ラベルをオンにする（Turn On Name Labels）] をクリックします。
6. ユーザは、顔認識機能を有効にする前にサービスにオプトインする必要があります。カメラ付きのコンピュータまたはモバイルデバイスで https://settings.webex.com/main/profile/name-label/enroll にアクセスします。
7. Taylor Bard（**tbard@cbXXX.dc-YY.com/dCloud123!**）でログインします。
8. ログインしたら [開始（Get started）] をクリックします。
9. プロンプトが表示されたら、カメラへのアクセスを許可します。指示に従い、[写真を撮る（Take photo）] をクリックします
10. 写真を撮ったら、[完了（Done）] をクリックします。
11. **Control Hub** に戻ります。
12. [デバイス（Devices）] ページで [Cisco Webex アシスタント（Cisco Webex Assistant）] セクションまで下にスクロールし、チェックボックスをオンにして有効にします。
13. これで、組織内でサポートされているすべてのデバイスで Webex Assistant が有効になりました。サポートされているデバイスの一覧と使用方法については、こちらをご覧ください。ユーザは、[設定（Settings）] メニューで各デバイスの Webex Assistant を個別にオン/オフすることができます。

Room デバイスの追加

1. [デバイス（Devices）] に移動します。
2. [デバイスの追加（Add Device）] をクリックします。
3. [場所（Place）] を選択し、[次へ（Next）] をクリックします。
4. [新規のプレース（New Place）] を選択します。ボックスが表示されたら場所の名前を入力します。

5. [次へ（Next）] をクリックします。
6. [その他のCisco Webexデバイス（Other Cisco Webex Device）] を選択し、[次へ（Next）] をクリックします。
7. [無料通話（Free Calling）] を選択したまま、[次へ（Next）] をクリックします。

次の画面に、DX/SX/Room Kit/Room 55 ~ 70/MX/Webex Board に入力する 16 桁のコードが表示されます。このコードはこれ以降の手順で使用します。以下の手順は、初期設定の状態から開始しています。ラボではこの手順で実施することをお勧めします。

8. Room デバイスの [ようこそ（Welcome）] 画面で、[開始（Start）] をタップします。
9. [ネットワーク（network）] 画面で、**青色の右矢印**をタップします。
10. [通話サービスの選択（Choose a call service）] で、[Cisco Webex] を選択します。
11. 管理ポータルで示された **16 桁のコード**を入力し、**青色の右矢印**をタップします。ホーム画面が表示されるまで、設定を続けます。
12. 管理ポータルに戻り、[ ] をクリックします。

Room デバイスが Cisco Webex に登録されています。登録された Room デバイスは、Cisco Webex Control Hub の [デバイス（Devices）] ページにオンラインとして表示されます（ページの更新が必要な場合があります）。

デバイスの一括追加

1. Control Hub からデバイスを一括で追加することもできます。
2. [デバイスの追加（Add Device）] をクリックします。
3. [CSVファイルのインポート/アップロード（Import/Upload CSV file）] をクリックします。
4. 次のポップアップウィンドウで、[CSVテンプレートのダウンロード（download CSV template）] をクリックします。
5. CSV ファイルを開くと、デバイスを一括で追加するために必要なテンプレートが表示されます。
6. 実稼働環境では、CSV ファイルに入力し、インポート機能を使用してデバイスを追加します。ラボではデバイスが限られているため、インポートする必要はありません。[キャンセル（Cancel）] をクリックします。

Room デバイスの管理

場合によっては、会議室内の複数のデバイスをペアリングするために超音波のレベルを下げるなど、Room デバイスの設定を変更する必要があります。Cisco Webex 管理ポータルでは、Room デバイスの設定を簡単に変更できます。デバイスをリモートから設定する場合、Control Hub を利用する方法と、デバイスの Web ポータルから直接設定する方法の 2 つがあります。

1. [デバイス（Devices）] ページで、前のセクションで追加したデバイスを選択します。

2. ポップアップウィンドウで [設定（Configurations）] セクションまで下にスクロールし、[詳細設定（Advanced Configurations）] の横にあるリンク（[XXX設定にアクセス（Access XXX Configurations）]）をクリックします。このウィンドウでは、ネットワークに直接アクセスせずに、さまざまなデバイスを設定できます。
3. **ultra** を検索し、表示された [音声（Audio）] > [超音波（Ultrasound）] > [最大レベル（MaxVolume）] > [オプション（option）] の順にクリックします。
4. スライダを利用して、レベルを **20** まで下げ、[適用（Apply）] をクリックします。

注：複数の Room デバイスがあるトレーニング環境では、必要に応じてレベルをさらに下げて、周りの人のデバイスとペアリングしないようにしてください。レベルを下げたら、ペアリングさせる Room デバイスにモバイル端末を近づける必要があります。

5. [⊗] をクリックします。
6. 設定可能なその他のオプションを自由に確認してください。完了したら [閉じる（Close）] をクリックします。

ネットワーク経由でコンピュータからデバイスにアクセスできる場合は、[デバイス管理（Devices Admin）] ページに直接アクセスすることもできます。

注：このセクションを完了するには、コンピュータと Room デバイスが同じネットワーク上にあること、または、コンピュータからネットワークを介して Room デバイスにアクセスできることを確認する必要があります。同じネットワーク上にあり、スプリットトンネリングが有効になっているために AnyConnect を利用して dCloud に接続している場合は、アクセスできるはずです。デバイスにアクセスできない場合は、AnyConnect を切断する必要があります。ラボ内の Workstation 1 または Workstation 2 仮想マシンから Room デバイスにアクセスすることはできません。

7. Cisco Webex Control Hub（https://admin.webex.com）にログイン中のもう 1 つのブラウザウィンドウ（ラボ内の Workstation 1 のブラウザではない）に戻ります。
8. [デバイス（Devices）] タブをクリックします。
9. 前のセクションで追加した Room デバイスを選択します。
10. ポップアップウィンドウでページの最下部までスクロールし、[Webポータルの起動（Launch Web Portal）] をクリック後、[続行（Proceed）] をクリックします。
11. ネットワークがルーティングされてデバイスにアクセスする場合は、[システム情報（System Information）] ページが表示されます。
12. [管理（Management）] ページでその他の設定を自由に確認してください。終了したら、Room デバイスのタブを閉じます。

デバイスブランディング

管理者は、Control Hub を使用してデバイスのブランディングを設定し、デバイスに表示されるメッセージをカスタマイズすることもできます。

1. Webex Control Hub で、[デバイス（Devices）] タブをクリックします。
2. [ブランディング（Branding）] セクションまでスクロールします。ブランディングを変更できるさまざまなオプションがあります。ブランディング例を表示するには、[例を参照する（See examples）] をクリックします。
3. 各オプションの状態（ウェイクアップフロー（Wake-up flow）」および アウェイク状態（Awake State））を確認したら、[完了（Done）] をクリックします。
4. [すべてのデバイスに対する帰社のブランドビジュアルをアップロードする（Upload your company's brand visuals for all devices）] オプションボタンを選択します。
5. アップロードボックスの下に、ブランドイメージとロゴの推奨サイズが表示されます。Google イメージ検索で **3840 X 2160 の写真**や **272 X 272 のイメージ**などを検索すれば、テストに使用するサンプルのブランドイメージやロゴをすぐに見つけられます。推奨サイズを超えている場合は、イメージのサイズが変更されたことを示すメッセージが表示されます。この処理には、数分かかる場合があります。
6. 背景やロゴのイメージを選択したら、アップロードボックスを使用してイメージをアップロードし、[保存（Save）] をクリックします。
7. しばらくすると、イメージが Room デバイスに表示されます。

Cisco Webex Teams モバイルアプリ

1. 現在設定されている機能をテストする前に、iOS または Android デバイスでアプリストアを開き、**Cisco Webex Teams アプリ**をダウンロードします。すでに Cisco Webex Teams がインストールされている場合は、一度ログアウトします。
2. Cisco Webex Teams に Taylor Bard（**tbard@cbXXX.dc-YY.com/dCloud123!**）でログインします。プロファイルの初期設定画面をスキップして、アプリケーションにアクセスします。Kellie Melby（**kmelby@cbXXX.dc-YY.com/dCloud123!**）で別のクライアントにログインします（**メールアドレスを入力した後にアクティベーションメッセージを受信した場合は、以下の注を参照してください**）。

注：ラボユーザでログインした際に、ユーザアカウントをアクティブにするように求められた場合、アクティブにするためユーザの電子メールにアクセスする必要があります。そのためには、https://mail1.dcloud.cisco.com/owa にアクセスし、dcloud\ユーザ名/dCloud123! でログインします（ユーザ名はすべて名前の最初の文字と姓）。セッション VPN で独自のブラウザを使用するか、ラボ内のワークステーションのいずれかを利用して接続する必要があります。電子メールにログインしたら、Webex Teams アカウントをアクティブにすることに関する最新の電子メールを探します。見つからない場合は、前のログインページで [再送（Resend）] リンクをクリックします。電子メール内の [今すぐ開始する（Get Started Now）] リンクをクリックし、プロンプトが表示されたら、パスワードに dCloud123! と入力します（6桁の番号が記載された電子メールを受け取った場合は、その番号を前の Web ページに入力します）。

3. アプリでは [超音波の使用（Use Ultrasound）] がデフォルトでオンになっているため、アプリを開くと、[メッセージ（Message）] リストに Room デバイスが表示されています。ペアリングされない場合は、モバイルデバイスを Room デバイスに近づけてください。複数の Room システムがあるトレーニング環境では、モバイルデバイスを適切な Room デバイスにペアリングできない場合があります。自動でペアリングできない場合は、以下の手順を試して手動でペアリングします。
    a. Taylor のアバターをタップし、[デバイス（Devices）] をタップします。
    b. [手動接続オプション（Manual Connection Option）]をオンにします。
    c. [スペース（Spaces）] リストに戻り、[デバイスに接続（Connect to a device）] をタップします。
    d. デバイスに設定した名前を検索します。
    e. PIN を入力するよう求められたら、ビデオデバイスの右上に表示されている番号を入力します。
4. Taylor を Room デバイスに接続したまま **Kellie** を検索してコールし、Kellie のクライアントからコールに応答します。
5. ハウリングしないようにエンドポイントを**ミュートします**。
6. Cisco Webex Teams アプリにコールが表示されたら、Room デバイスから応答します。ハウリングしないように Kellie のクライアントをミュートします。
7. Room デバイスとクライアント間でビデオ通話を行っています。名前ラベルが設定されていれば、Webex に登録されている DX、SX、MX、Room シリーズ デバイス、Webex Boards に表示されます。名前ラベルは、Webex に登録されている Room シリーズ デバイスと Webex Boards から送信されます。名前ラベルの最新情報については、こちらを参照してください。
8. 画面をタップしてメニューオプションを表示し、**省略記号**アイコン [] をタップして、Room デバイスから自分のモバイルに通話を転送します。
9. [通話を移動（Move Call）] をタップすると、検出されたデバイスが表示されます。後は [移動（Move）] ボタンをタップするだけです。
10. これで、モバイルデバイスによるビデオ通話が確立されます。
11. モバイルデバイスからRoomデバイスに通話を戻すには、上記のステップ 8 と 9 を繰り返して、モバイルデバイスからRoomデバイスに通話を転送します。
12. [] をタップして、通話を終了します。

注：この通話転送機能は Cisco Webex Teams デスクトップクライアントでも利用できます。アクティブな通話ウィンドウで [通話を移動（Move call）] をクリックするだけで、Room デバイスまたはデスクトップに転送できます。

DX ホワイトボード機能

DX での通話中にホワイトボード機能を利用できるようになりました。ホワイトボード機能はスペース外の通話でも利用できますが、ドキュメントは保存できません。ホワイトボードの内容を保存する場合は、スペース内から発信された通話でなければなりません。

1. **Webex Teams クライアント**を **DX** にペアリングし、Webex Teams クライアントの別のユーザへの通話を開始します。これは、1 対 1 またはグループスペースでの会議で実行できます。
2. 通話/会議に接続した後、DX の**ホワイトボード**アイコンをタップし、[新しいホワイトボード（New whiteboard）] を選択します。
3. DX で描画を開始すると、ペアリングしたモバイルクライアントでホワイトボードを表示/編集できることがわかります。また、通話/会議中の他のユーザも表示/編集できます。
4. 完了したら、通話/会議を終了します。

Room デバイスのアラート

デバイスがオフラインになったときや、問題が発生した場合/解決された場合にデバイスからアラートを送信し、状況を通知することができます。アラート機能は、デバイス全体で有効にすることも、デバイスごとに個別に有効にすることもできます。ここではデバイス全体で有効にします。

1. お客様向けの Webex Control Hub で、[デバイス（Devices）] タブをクリックします。
2. ページの右上にある [マイアラート（My Alerts）] をクリックします（デバイスごとに有効にする場合は、[アラートの管理（Manage Alerts）] をクリックします）。
3. [デバイスがオフラインまたはオンラインになったらアラートを表示してください] と [デバイスに問題が発生した場合、または問題が解決した場合にアラートを表示してください]、両方をオンにしてアラートを有効にします。
4. 登録済みの Room デバイスの電源をオフにします。
5. Workstation 1 で Charles の Webex Teams クライアントにログインします（**cholland@cbXXX.dc-YY.com/dCloud123!**）。
6. 数分で、**Control Hub Alerts** ボットからデバイスがオフラインになったことを通知するアラートが送信されます。これらの通知は、アラートを設定した管理者に送信されることに注意してください。
7. アラートを受信したら、デバイスの電源を再度オンにします。

ここまでで、モバイルアプリおよび Room デバイスの通話/共有機能をテストしました。

Room デバイスソフトウェア

Control Hub 内では、Room デバイスソフトウェアを細かく制御できるだけでなく、安定版およびプレビュー版ソフトウェアに関する詳細情報を取得することもできます。

1. お客様向け Webex Control Hub で、[デバイス（Devices）] タブをクリックします（すでにページに表示されています）。
2. ページ上部の [ソフトウェア（Software）] をクリックします。
3. このページでは、Stableソフトウェア（安定版）およびPreviewソフトウェア（プレビュー版）に関する情報を得られます。ほとんどの場合、ユーザにはStableソフトウェア（安定版）を利用させたいと考えるでしょう。名前の通り最も安定したバージョンで、TAC がサポートしているからです。一方、特別なケースでは、通常はまだ利用できない新しい機能を試したい場合があります。その場合は、Previewソフトウェア（プレビュー版）を使用します。
4. [Stableソフトウェア（Stable software）] セクションまで下にスクロールします。

このセクションでは、Stableソフトウェア（安定版）を使用しているデバイス数を確認できます。[デバイスの表示（View Devices）] をクリックすると、安定版ソフトウェアを実行しているデバイスのリストが表示されます。また、現在のバージョンと今後のバージョンのリリース日も表示されます。

5. [詳細を表示（Show Details）] をクリックします。
6. このリリースでの変更内容を確認できます。[詳細をお読みください（Read more）] をクリックすると、機能の詳細が表示されます。
7. [Previewソフトウェア（Preview software）] セクションまで下にスクロールします。
8. ここでは、[Stableソフトウェア（Stable software）] セクションと同じ情報を確認でき、さらにバグを報告する機能もあります。プレビュー版ソフトウェアでは TAC のサポートが受けられないことに注意してください。
9. ページの下部には、古いバージョンのソフトウェアのリリース情報を確認できるリンクがあります。
10. すべての Room デバイスには、デフォルトでStableソフトウェア（安定版）が導入されています。Previewソフトウェア（プレビュー版）でデバイスを動作させたい場合は、各デバイスを個別に変更する必要があります。プレビュー版ソフトウェアは、Room デバイスと同じ [場所（Place）] にあります。
11. [プレース（Places）] に移動します。
12. Room デバイスを追加したときに作成した場所を選択します。
13. ポップアップウィンドウの [デバイス設定（Device Settings）] セクションに、デバイスが動作しているソフトウェアチャネルが表示されます。
14. ドロップダウンリストを利用して、ソフトウェアチャネルを [プレビュー（Preview）] に変更します。
15. 数分でソフトウェアがダウンロードされ、インストールされた後リブートされます。安定版に戻りたい場合は、このリストボックスを使用していつでもデバイスをダウングレードできます。

シナリオ 3. Webex ハイブリッド カレンダー サービス（クイックセットアップ）

ハイブリッド カレンダー サービスを使用すると、オンプレミスの Microsoft Exchange、Office 365、Google の G Suite カレンダー（Google カレンダー）環境を Cisco Webex に統合できます。統合することで、会議のスケジュール設定と参加が容易になります（特にモバイルの場合）。プラグインは必要ありません。

ハイブリッド カレンダー サービスでは、Cisco Call Control を使用していません。ハイブリッド カレンダー サービスを使用すると、サードパーティの UC ソリューションを使用している場合でも、Cisco Webex ユーザに機能を拡張できます。

シンプルな会議のスケジューリング

カレンダー招待状の [場所（Location）] フィールドにスケジュール設定用キーワードと修飾子を入力すると、簡単に会議のスケジュールを設定できます。

表 4. シンプルな会議のスケジューリング

実行する内容	[場所（Location）] フィールドに指定できるキーワード
会議用の Cisco Webex Teams スペースを作成するか、Cisco Webex Teams から会議をホストする	@webex:space @meet @meet:space @spark（廃止）
Webex パーソナルルーム用のクリック可能なリンクを含める	@webex @webex:myroom @meet:myroom 自分のパーソナルルーム URL（例：https://<会社名>.webex.com/meet/<ホスト ID>）

会議リストと参加ボタン

Cisco Webex Teams の会議リストを使用すると、今後 4 週間に予定されている会議を確認できます。会議が開始される 5 分前に、会議リストに [参加（Join）] ボタンが表示され、予定されている会議の通知が届きます。

ユーザは、Cisco Webex Room、デスクデバイス、Webex Board を会議に追加して利用することができます。デバイスでハイブリッド カレンダー サービスが有効になっている場合は、緑色の [参加（Join）] ボタンがデバイスに表示されます（[参加（Join）] ボタンはワンボタン機能とも呼ばれます。Cisco Unified Communications Manager に登録され、Cisco TelePresence Management Suite によって管理されるデバイスでも使用できます）。ハイブリッド カレンダー サービス対応の Room デバイスおよびデスクデバイスでも、招待された会議を会議リストに表示できます。

詳細な設定ガイドについては、https://www.cisco.com/go/hybrid-services-calendar を参照してください。

クイックセットアップ情報

このシナリオでは、新しい機能に専念できるように、クイックステップを利用してハイブリッド カレンダー コネクタを設定します。カレンダーサービスは、次のシナリオである、Webex Edge for Devices のテストをできるように設定する必要があります。すべての設定を通しで行ったことがなく、設定していない内容を確認したい場合は、付録 E ですべての手順を確認できます。

Expressway-C コネクタホストの設定

次に、Cisco Webex ハイブリッドサービスで使用する、新しい Expressway-C コネクタホストをカスタマー組織に追加します。この Expressway-C サーバには、Cisco Webex ハイブリッド カレンダー サービスおよびコールサービスで必要なすべてのコネクタが含まれています。以下の手順は、ラボ内の Workstation 1 から実行する必要があります。

1. 開いている Cisco Webex Control Hub に戻ります。**Charles Holland** でログインしたままで、セッション **VPN** への接続も維持されていることを確認します。
2. ポータルの左側のメニューで、[サービス（Services）] をクリックします。
3. [Exchangeハイブリッドカレンダー（Hybrid Calendar Exchange）] で、[セットアップ（Set up）] をクリックします。
4. [ハイブリッドカレンダーサービスの設定（Hybrid Calendar Service Setup）] ポップアップウィンドウで、[次へ（Next）] をクリックします。
5. 最初のオプションボタンを選択してボックスに **exp-cc.dcloud.cisco.com** と入力し、[次へ（Next）] をクリックします。
6. クラスタ名として **HS Cluster 1** と入力します。
7. もう一度 [次へ（Next）] をクリックします。
8. [次へ（Next）] を再度クリックすると、新しいブラウザタブが開き、Expressway にアクセスします。セキュリティの警告が出ても、無視するか同意してそのまま続行してください。
9. ユーザ名：**admin**、パスワード：**dCloud123!** で Expressway にログインします（あらかじめ入力されています）。
10. [この信頼に必要なExpressway CA証明書をシスコが管理する（I want Cisco to manage the Expressway CA certificates required for this trust）] チェックボックスをオンにします。
11. [ソフトウェアの更新および接続の検証（Update software & verify connection）] をクリックします。
12. 検証できたら、[登録（Register）] をクリックします（Webex にログインするようにプロンプトが表示されたら、ユーザ名とパスワードに **cholland@cbXXX. dc-YY. com/dCloud123!** を入力します）。
13. 次の画面で、[Expresswayへのアクセスを許可（Allow Access to the Expressway）] チェックボックスをオンにし、[続行（Continue）] をクリックします。

しばらくすると Expressway に戻り、2 つのハイブリッド サービス コネクタがダウンロードされてインストールされます。2 つのコネクタは、管理コネクタとカレンダーコネクタです。管理コネクタは、Expressway-C サーバ上のすべてのコネクタを管理します。3 番目のコネクタであるコールコネクタは、このラボでハイブリッドコールサービスを有効にした時点でインストールされます。

Exchange の事前設定

Microsoft Exchange は、疑似アカウントと、Cisco Webex カレンダーサービスで使用するスロットリングポリシーを利用して事前に設定されています。疑似アカウントをサービスアカウントとして使用するには、メールが有効になっているアカウントとして設定する必要があります。このアカウントは管理者である必要はありませんが、メールボックスが設定されていなければなりません。必要な疑似アカウントの詳細については、こちらをクリックしてください。このラボでは、**hcalendar** というアカウントを疑似アカウントとして使用します。参考までに、hcalendar 疑似アカウントを使用して Exchange を設定するコマンドを次に示します。

a. New-ManagementRoleAssignment -Name CalendarConnectorAcct -Role ApplicationImpersonation -User dcloud\hcalendar
b. New-ThrottlingPolicy -Name " CalendarConnectorPolicy" -EWSMaxConcurrency unlimited -EWSMaxBurst unlimited -EWSRechargeRate unlimited -EWSCutOffBalance unlimited -EWSMaxSubscriptions 5000
c. set-ThrottlingPolicyAssociation -Identity dcloud\hcalendar -ThrottlingPolicy CalendarConnectorPolicy
d. New-Mailbox -Name 'Webex Room Device' -Alias 'webexrd' -room

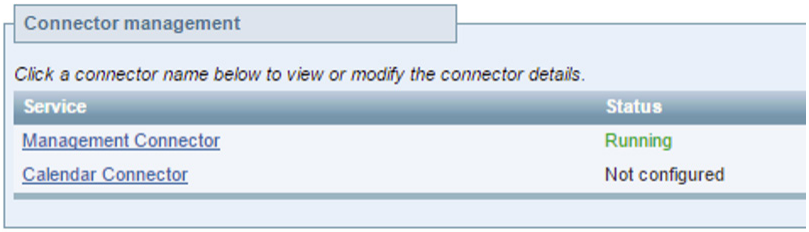
Microsoft Exchange に Expressway-C をリンクする

ここでスクリプトを使用して、Cisco Webex カレンダーサービス用の Expressway-C ホストを設定します。

注：前述のように、設定内容を確認する手順は、**付録 E** を参照してください。付録 E は、スクリプトが失敗した場合にも役立ちます。

1. スクリプトを開始する前に、Workstation 1 でコネクタのステータスが次のスクリーンショットのようになっていることを確認してください。このページはすでに開いているはずです。開いていない場合は、Expressway-C（**198.18.133.223**）にアクセスし、ログイン（**admin/dCloud123!**）して、[アプリケーション（Applications）] > [ハイブリッドサービス（Hybrid Services）] > [コネクタ管理（Connector Management）] に移動します。

[コネクタ管理（Connector Management）]



2. Workstation 1 のデスクトップで **Webex** フォルダを開きます。
3. **config_calendar.bat** ファイルをダブルクリックし、スクリプトをすべて実行します。エラーのためにボタンを再度クリックするよう求められますが、無視してかまいません。
4. Internet Explorer が閉じたら次のセクションに進みます。Workstation 1 へのリモート接続はそのままにします。

Charles のカレンダーサービスの有効化

Charles のカレンダーサービスを手動で設定します。CSV テンプレートを使用して、複数のユーザを一括して設定できます。

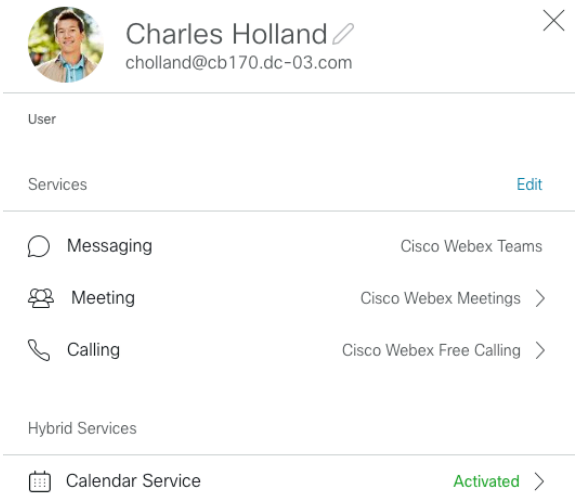
1. Cisco Webex Control Hub に戻ります。
2. 左側のメニューで [ユーザ（Users）] をクリックします。
3. リストから [Charles Holland] を探してクリックします。
4. [ハイブリッドサービス（Hybrid Services）] セクションの [カレンダーサービス（Calendar Service）] をクリックします。
5. [カレンダーサービス（Calendar Service）] の横のトグルボタンをクリックしてオンにし、[保存（Save）] をクリックします。

ステータスが [アクティベーション保留中（Pending Activation）] から [アクティベーション済み（Activated）] に変わるまで約 5 分かかります。

注：各ユーザが Cisco Webex Teams クライアントに一度ログインするまで、カレンダーサービスのアクティベーションは開始されません。これはカレンダーサービスだけでなく、すべてのサービスで同じです。

6. Charles のカレンダーサービスがアクティブになっていることを確認します。なっていない場合でも、ラボではとりあえずそのまま続行します。次のシナリオでテストする際に、Charles のアカウントをアクティブにする必要があります。

Charles でアクティブになったカレンダーサービス



注：Control Hub でユーザがアクティブと表示されるまで時間がかかることがあります。Expressway-C コネクタホストではアクティブになったユーザがすぐに表示される場合があります。コネクタホストで、[アプリケーション（Applications）] > [ハイブリッドサービス（Hybrid Services）] > [カレンダーサービス（Calendar Service）] > [カレンダーコネクタステータス（Calendar Connector Status）] の順に移動します。ユーザがアクティブになっている場合は、[正常にサブスクライブされたユーザ（Successfully Subscribed Users）] の横にユーザ数が表示されます。

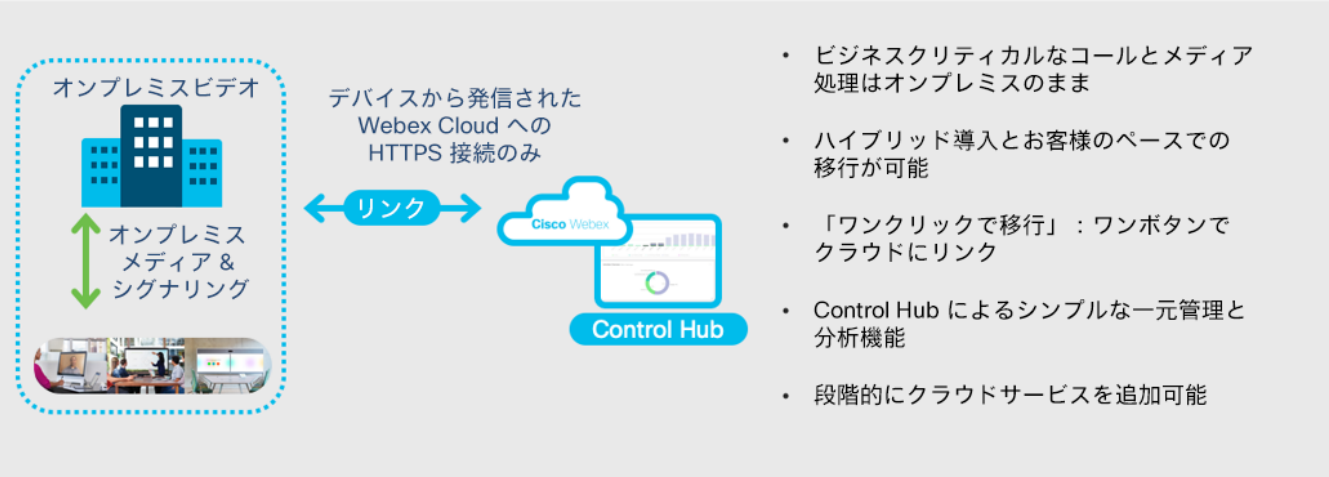
7. これでカレンダーサービスが設定されましたが、まだテストすることはできません。Webex Edge for Devices のシナリオでテストが完了します。まだ Room デバイスもカレンダーサービス用に変更していません。次のシナリオでデバイスを UCM に登録すると、クラウドに登録した場合と同じように動作するため、その際に変更します。

シナリオ 4. Webex Edge for Devices

このシナリオでは、Webex Edge for Devices Connector ツールのインストールと設定について説明します。

顧客は、オンプレミスに登録するタイプとクラウドに登録するタイプの 2 のデプロイ方法に分かれています。オンプレミスで展開した事例が多くありますが、最近では、アイディエーション/コ・クリエーション、インテリジェンス/AI、大規模環境の一元管理、アナリティクスなどのイノベーションはクラウドでの展開をすることが多くなっています。

お客様はクラウドへの移行をしようとしていますが、多くの場合、非常に大規模なオンプレミスの資産を移行するには時間がかかります。また、移行戦略を策定する必要もあります。さらに、クラウドの機能が必要であるものの、エンドポイントをリプレイスすることはできないといったことにも対応できなければなりません。



Webex Edge for Devices Connector ツールは、次の 2 つの異なる運用方式に対応しています。

- オンプレミスに登録済みの Webex デバイスを Webex Cloud に一括移行する
- オンプレミスに登録済みの Webex デバイスを Webex Control Hub にリンクし、Webex Cloud 機能を利用できるようにする

この演習では、Webex Cloud 機能をオンプレミスに登録済みの Webex デバイスで利用できるようにする 2 番目の方式のみ実施します。

クラウドオンボーディングによって、複数の Cisco Webex デバイスを一括してクラウドに登録できます。

Webex Edge for Devices により、コールとメディア処理はオンプレミスのまま Cisco Webex Cloud の機能を利用できます。

特長と利点

表 5. 特長と利点：Webex デバイスのリンク

特長	利点
メディアはローカルのままデバイスのコールを制御	メディアはオンプレミスのままビジネスクリティカルなコール制御機能を利用可能 - クラウドに接続できない場合でも対応可能
拡張性に優れた管理/分析機能	Cisco Webex Control Hub を活用して可視性を強化：一元管理 - デバイス分析による過去の使用状況を詳細に把握可能 - デバイスのステータスに関するプロアクティブなアラート
クラウドサービスとイノベーションを利用可能	- Webex デバイスでハイブリッド カレンダー サービスとOne Button to Push機能をTMS/TMSXEなしでサポート。 - Webex Assistantを利用可能
非常に簡単なセットアップ	ファイアウォールで追加のポート開放が不要 - クラウドには HTTPS で接続

概要 - 必要な手順

1. Webex Edge for Devices Connector ツールをダウンロードしてインストールする
2. Webex Edge for Devices Connector ツール用のアプリケーションアカウントを設定する
3. MRA を利用して Webex デバイスを Unified CM に登録する
4. Webex Edge for Devices Connector ツールを Unified CM に接続する設定を行う
5. Webex Edge for Devices Connector ツールを利用してデバイスを Webex Control Hub にリンクする
6. 新たにリンクされた Webex デバイスにクラウド機能を設定する
7. クラウド機能をテストする

Webex Edge for Devices Connector ツールのインストール

ここで、Webex Edge for Devices Connector ツールをダウンロードしてインストールします。**Workstation 1** で実行します。

1. Workstation 1（**198.18.1.36**）にまだ接続していない場合は、接続します。
   - ユーザ名：dcloud\cholland
   - パスワード：dCloud123!
2. Chrome を開き、Cisco Webex Control Hub（**admin.webex.com**）に戻り、必要に応じて **cholland@cbXXX.dc-YY.com/dCloud123!** でログインします。
3. Webex Control Hub で [デバイス（Devices）] に移動します。
4. [デバイス（Devices）] ウィンドウの右上にある [リソース（Resources）] をクリックします。
5. [ツール（Tools）] まで下にスクロールします。**Cisco Webex Device Connector** のタイルで [ダウンロード（Download）] をクリックします。
6. [Windowsのダウンロード（Download for Windows）] を選択します。**Workstation 1** のデスクトップにダウンロードファイル（devicetool.msi）が保存されます。ダウンロードが正常に完了したら、[完了（Done）] をクリックします。
7. **devicetool.msi** ファイルをダブルクリックして、インストールプロセスを開始します。[実行（Run）] をクリックして続行します。Cisco Webex Device Connector のセットアップ画面が表示されます。
8. [次へ（Next）] をクリックして続行します。[ライセンス契約（License Agreement）] ボックスをオンにして [次へ（Next）] をクリックします。インストール先はデフォルトのままにして [次へ（Next）] をクリックし、[インストール（Install）] をクリックします。完了したら [完了（Finish）] をクリックします。

Webex Edge for Devices Connector ツール用のアプリケーションアカウントを設定する

Webex Edge for Devices Connector ツールが Unified CM を検索してリンク用の関連デバイスのリストを見つけるには、**標準 AXL API アクセス**権限を設定したアプリケーションユーザを作成する必要があります。Webex Edge for Devices Connector ツールは、このアカウントを使用して Unified CM と通信します。このラボでは、このユーザは事前に作成されています。付録 B に、このユーザを作成して権限を割り当てる手順を示しています。このラボの他の箇所でも使用できるように、ユーザには他の権限も設定されていますが、標準 AXL API アクセス権限があれば、Webex Edge for Devices Connector ツールは Unified CM と通信できます。

注：CSV または TMS Overview Export 機能を利用してデバイスをリンクする場合は、アプリケーションアカウントは不要です。

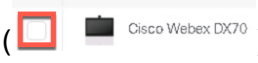
MRA を利用して Webex デバイスを Unified CM に登録する

Webex Edge for Devices は、オンプレミスに登録済みの Webex デバイスが Webex Cloud 機能を利用できるように設計されています。ラボでこのデモンストレーションを行うには、Webex デバイスが Unified CM に登録されている必要があります。このラボでは、Expressway がこれらのサービス用にすでに設定されているため、Webex デバイスを Unified CM に登録する最も簡単な方法は、dCloud ラボの Expressway で MRA を使用することです。

注：Webex Room デバイスを Webex Control Hub にすでに登録している場合は、Webex Control Hub の登録を解除し、Webex デバイスを初期設定に戻す必要があります。次の手順では、デバイスの登録を解除し、初期設定に戻す方法について説明します。Webex デバイスを Webex Control Hub に登録していない場合は、次のステップ 6 にスキップします。

1. **Workstation 1** からブラウザウィンドウに戻ります。Cisco Webex Control Hub にログインしたままになっているはずです。
2. [デバイス（Devices）] に移動します。クラウド登録済みの Webex デバイスがここに表示されます。Webex デバイス名をクリックし、右側のポップアップカードで画面を下にスクロールして、デバイスの MAC アドレスを確認します。MAC アドレスを選択してコピーします。このアドレスは後で必要になります。

推奨：デスクトップに新しいメモ帳ファイルを作成し、そこに MAC アドレスを貼り付けます。MAC アドレスの区切り文字は削除する必要があります。たとえば、AB:1D:2C:38:82:6E は、メモ帳ファイルに AB1D2C38826E として保存します。

3. デバイスの左側にある [デバイス（Device）] ページに戻ります。小さなチェックボックス（ 

）がありますので、オンにします。この行は **1 つのデバイスが選択されている**ことを示し、その右側にはごみ箱アイコンがあり、[デバイスの削除（Delete Devices）] ボタンがついています。[デバイスの削除（Delete Devices）] をクリックします。
4. [デバイスの削除（Delete Devices）] ダイアログボックスが表示され、削除の確認を求められます。[削除して空にする（Delete resulting empty places）] の横にあるチェックボックスをオンにし、赤い [削除（Delete）] ボタンを押します。削除されたら、[完了（Done）] をクリックします。
5. Webex デバイスで画面左上の [デバイス名（Device Name）] をクリック後、[設定（Settings）] > [初期設定に戻す（Factory Reset）] の順に選択し、[リセット（Reset）] を再度クリックして確定します。
6. Workstation 1 の新しいブラウザタブで、[コラボレーション管理リンク（Collaboration Admin Links）] > [Cisco Unified Communications Manager] の順に移動します。
7. [Cisco Unified Communications Manager] をクリックし、次の情報に基づいてログインします（事前に入力されています）。
   - ユーザ名：administrator
   - パスワード：**dCloud123!**
8. [デバイス（Device）] > [電話機（Phone）] を選択し、[検索（Find）] をクリックします。

9. ラボの基本設定では、各種の一般的なデバイスが事前に設定されています。事前設定されているデバイスには、Cisco Webex DX70、DX80、Room Kit、Room Kit Mini などがあります。各デバイスが Charles Holland に割り当てられ、Charles の内線番号 **6018** が設定されています。別のデバイスを使用する場合は、事前に設定されたデバイスの設定内容を手動でコピーする必要があります。次の手順では、事前設定されたデバイスを変更します。
10. 使用するデバイスを見つけ、**SEP** で始まる**デバイス名**をクリックします。
11. [電話設定（Phone Configuration）] ページで、デバイスの実際の MAC アドレスを [MAC アドレス（MAC Address）] フィールドに入力します。すでにクラウドに登録されている場合は、上記の MAC アドレスを控えておきます。登録されていない場合、MAC アドレスはデバイスの底面のラベルに記載されています。
12. [プロダクト固有の設定（Product Specific Configuration Layout）] セクションまで下にスクロールします。セクション内のリストで [SystemUnit] をクリックすると、[全般設定（General Settings）] と [CrashReporting] オプションが表示されます。[全般設定（General Settings）] で [名前（Name）] フィールドを探し、デバイスに名前を付けます。
13. [保存（Save）]、[OK]、[設定の適用（Apply Config）]、[OK] の順にクリックします。
14. デバイスが初期状態にリセットされると、[ようこそ（Welcome）] 画面が表示されます。[開始（Start）] を選択し、画面の上部にある、**次を示す青い矢印**をクリックします。
15. [その他のサービス（Other Services）] > [Expressway経由Cisco UCM（Cisco UCM via Expressway）] を選択し、次のように入力します。
    - ユーザ名：**cholland**
    - パスワード：**dCloud123!**
    - ドメイン：cbXXX.dc-YY.com
16. 右上の**青い矢印**を選択すると、[セットアップ完了（Setup Done!）] メッセージが表示されます。
17. ブラウザの Unified CM タブに戻り、Charles Holland に属するデバイスを表示するページを更新します。[リアルタイムデバイスステータス（Real-Time Device Status）] は次のようになります。
    - 登録：**Cisco Unified Communications Manager cucm1.dcloud.cisco.com に登録済み**
    - IPv4 アドレス：**198.18.133.152**

Webex Edge for Devices Connector ツールの設定

1. Workstation 1 に戻ります。
2. Webex Edge for Devices Connector ツールをまだ起動していない場合は、Workstation 1 の Windows Start ボタンをクリックします。[最近追加されたもの（Recently Added）] の下に表示されている Cisco Webex Device Connector をクリックします。

3. ツールの起動ページで、Cisco Webex Administrator のユーザ名とパスワードを求められます。次のように入力します。
   - ユーザ名：**cholland@cbXXX.dc-YY.com**
   - [サインイン（Sign In）] をクリックします。
   - パスワード：**dCloud123!**
4. [どのようなサポートが必要ですか（What would you like help with?）] 画面で、[オンプレミス登録済みデバイス用のクラウド機能（I want cloud features for my on-premises registered devices）] を選択します。
5. [Webex Edge for Devicesの設定（Configure Webex Edge for Devices）] 画面で、[Cisco Unified Communications Managerに登録済みのデバイスをリンクする（Link devices registered with Cisco Unified Communications Manager）] を選択します。

注：ラボ内の Webex デバイスは Unified CM に登録されています。他に Webex デバイスをリンクする方法として、CSV をインポートするか、TMS Overview Export でエクスポートしたファイルをインポートするオプションがあります。これらのその他のオプションは [設定（configuration）] 画面に表示されていますが、このラボでは説明しません。

6. 次の画面で以下のように入力します。
   - ホスト：**cucm1.dcloud.cisco.com**
   - ユーザ名（標準 AXL API アクセス権限）：**webex**
   - パスワード：**dCloud123!**
7. [接続（Connect）] をクリックします。
8. エラーページで、[証明書を検証せずに進む（Proceed without certificate validation）] をクリックします。

注：ラボでは自己署名証明書を使用します。自己署名証明書は、Webex Device Connector ツールのユーザ証明書ディレクトリには追加されていません。「接続に失敗しました」というメッセージが表示されるのはそのためです。

9. これで、クラウドにリンクできる Webex デバイスのリストが表示されます。Charles Holland に登録したデバイスの横にある [リンク（Link）] をクリックします。
10. ステータスが [リンク（Link）] から [リンク中（Linking）] に変わります。リンクが完了すると、ステータスは [リンク済み（Linked） Linked] に変わります。

クラウド機能の設定

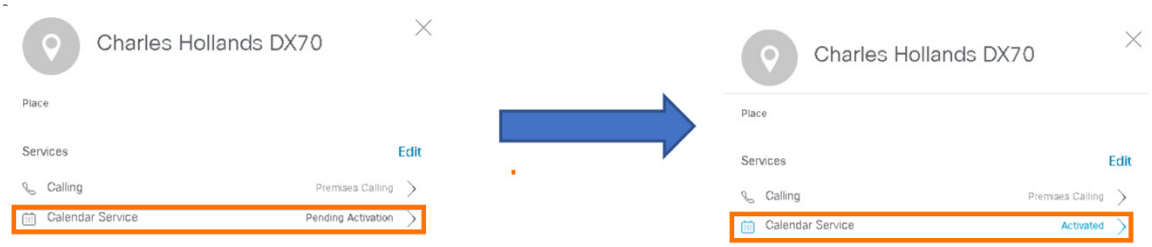
重要：このセクションでは、Webex デバイスのハイブリッド カレンダー サービスを有効にします。Webex Control Hub でコアサービスをまだ設定していない場合は、このセクションに進む前に、シナリオ 3（Exchange オンプレミス）またはシナリオ 8（Exchange オンライン）に進み、対象ユーザのハイブリッド カレンダー コア サービス、Webex サイト設定、カレンダーサービスを有効にします。

1. **Cisco Webex Control Hub**（https://admin.webex.com）にログインしているブラウザウィンドウに戻ります。
2. Cisco Webex Control Hub で [場所（Place）] に移動します。

前のセクションの Webex デバイスリンクプロセスで作成した新しい場所が表示されます。この場所には、Unified CM でデバイスに入力したのと同じ名前が付けられていて、Webex デバイスが含まれています。

3. **場所名**をクリックします。ブラウザウィンドウの右側にポップアップウィンドウが表示されます。
4. [サービス（Services）] エリアの [編集（Edit）] をクリックします。
5. [サービスの編集（Edit Services）] 画面で、**カレンダーサービス**が非アクティブになっていることがわかります。トグルをクリックしてサービスをアクティブにし、[次へ（Next）] をクリックします。
6. リソースのメールボックスに設定済みの電子メールアドレス **webexrd@cbXXX.dc-XX.com** を入力します（Exchange に事前に設定されています）。
7. [保存（Save）] をクリックします。
8. **Webex デバイスのカレンダーサービス**が表示され、ステータスは [アクティベーション保留中（Pending Activation）] と表示されます。しばらくすると [アクティベート済み（Activated）] に変わります。

アクティブになったカレンダーサービス



会議用の Cisco Webex Teams スペースの作成テスト、または OBTP 付き Cisco Webex Teams を利用した会議のホスト

1. Workstation 1 にまだ接続していない場合は、Workstation 1（**198.18.1.36**）への RDP 接続を確立し、以下のログイン情報でログインします。
   - ユーザ名：**dcloud\cholland**
   - パスワード：**dCloud123!**
2. **Outlook** をまだ開いていない場合は、タスクバーのアイコン [ ] をクリックして開きます。
3. Outlook の下部にある [カレンダー（Calendar）] をクリックし、[新規会議（New Meeting）] [New Meeting] をクリックします。

4. Anita Perez、Taylor Bard、Kellie Melby を [宛先（To）] 行に追加します。
5. 適切な [件名（Subject）] を入力します。
6. [場所（Location）] に以下のいずれかを入力してスペース会議を作成します。
   - @webex:space
   - @meet
   - @meet:space
7. OBTP を利用する場合は、[場所（Location）] フィールドの後ろにある [ルーム...（Rooms...）] ボタンをクリックします。
8. Exchange Server で以前作成した Room メールボックスを選択し、[OK] をクリックします。
9. 場所の更新ポップアップには [いいえ（No）] をクリックします。
10. ワークステーションの時計に基づいて、今日の開始時間（先の時間）を設定します。OBTP と会議通知が機能するように、10 分以上先の時間を設定します。
11. 必要に応じて、メッセージの本文に適切な文を入力します。
12. 上記のいずれかのキーワードが [場所（Location）] フィールドに設定されていることを確認し、[送信（Send）] をクリックします。

カレンダーコネクタによって [場所（Location）] フィールドのキーワードが読み取られ、Webex Teams スペース情報が会議の招待状に設定されます。また Cisco Webex Teams スペースが作成され、すべての参加者が登録されます。しばらくしてから作成した会議を開くと、Webex Meetings 情報が招待状の最下部に表示されています。情報が表示されない場合は、会議を閉じて、しばらくしてから再度開きます。

13. Workstation 1 の Webex Teams クライアントを起動し、**cholland@cbXXX.dc-YY.com/dCloud123!** でログインします。
14. スペースキーワードを使用した場合は、アカウント内に、会議の招待状の件名と同じ名前のスペースが作成されています。
15. **スペース**をクリックすると、そのスペースにも会議の詳細が表示されていることがわかります。
16. **会議** [19] アイコンをクリックして、会議リストを表示します。会議を選択して、Room デバイスを含む参加者を確認します。ユーザが招待を受け入れたかどうかも確認できます。
17. Room デバイスに表示されている会議も確認します。
18. スケジュールされた会議の 6 分前に Webex Teams アプリで参加通知を受信したら、[通知（notification）]、[ビデオで参加（Join With Video）] の順にクリックします。

注：時間を節約するため、このスペース会議が開始されるのを待っている間に、次のセクションで示す別の Webex Meetings のスケジュールを設定します。

19. Room デバイスで、Charles がすでに会議に参加していることを確認します。[参加（Join）] をタップして、進行中の会議に直接参加します。
20. 完了したら、会議を終了します。他のキーワードを使用して、いろいろな会議を自由に設定してください。

OBTP 付き Webex パーソナルルームへのリンクを含めるテスト

ここで OBTP 付き Webex Meeting を設定する機能をテストします。

1. 前の会議がまだ進行中の場合は、カレンダーでその会議を右クリックし、[会議のキャンセル（Cancel Meeting）] を選択後、[キャンセルの送信（Send Cancelation）] をクリックして Room デバイスを解放します。Room デバイスを二重に予約することはできません。
2. Outlook の下部にある [カレンダー（Calendar）] をクリックし、[新規会議（New Meeting）] [

] をクリックします。
3. Anita Perez、Taylor Bard、Kellie Melby を [宛先（To）] 行に追加します。
4. 適切な [件名（Subject）] を入力します。
5. [場所（Location）] に次のいずれかのアドレスを入力し、自分の Webex パーソナルルームを使用する会議を作成します。
   - @webex
   - @webex:myroom
   - @meet:myroom
   - https://cbXXXYY.webex.com/meet/cholland
6. OBTP を利用する場合は、[場所（Location）] フィールドの後ろにある [ルーム...（Rooms...）] ボタンをクリックします。
7. Exchange Server で以前作成した Room メールボックスを選択し、[OK] をクリックします。
8. 場所の更新ポップアップには [いいえ（No）] をクリックします。
9. ワークステーションの時計に基づいて、今日の開始時間（先の時間）を設定します。One Button to Push機能 と会議通知が機能するように、10 分以上先の時間を設定します。
10. 必要に応じて、メッセージの本文に適切な文を入力します。
11. キーワードがまだ [場所（Location）] フィールドに設定されていることを確認し、[送信（Send）] をクリックします。

これでカレンダーコネクタによって [場所（Location）] フィールドからキーワードが読み取られ、会議がセットアップされます。しばらくしてから作成した会議を開くと、Webex Meetings 情報が招待状の最下部に表示されています。情報が表示されない場合は、会議を閉じて、しばらくしてから再度開きます。

12. スケジュールされた会議の 6 分前にホストの Charles が Webex Teams アプリで参加通知を受信したら、[通知（notification）]、[ビデオで参加（Join With Video）] の順にクリックします。
13. Room デバイスで、Charles がすでに会議に参加していることを確認します。[参加（Join）] ボタンを押して、進行中の会議に直接参加します。
14. 完了したら、会議を終了します。

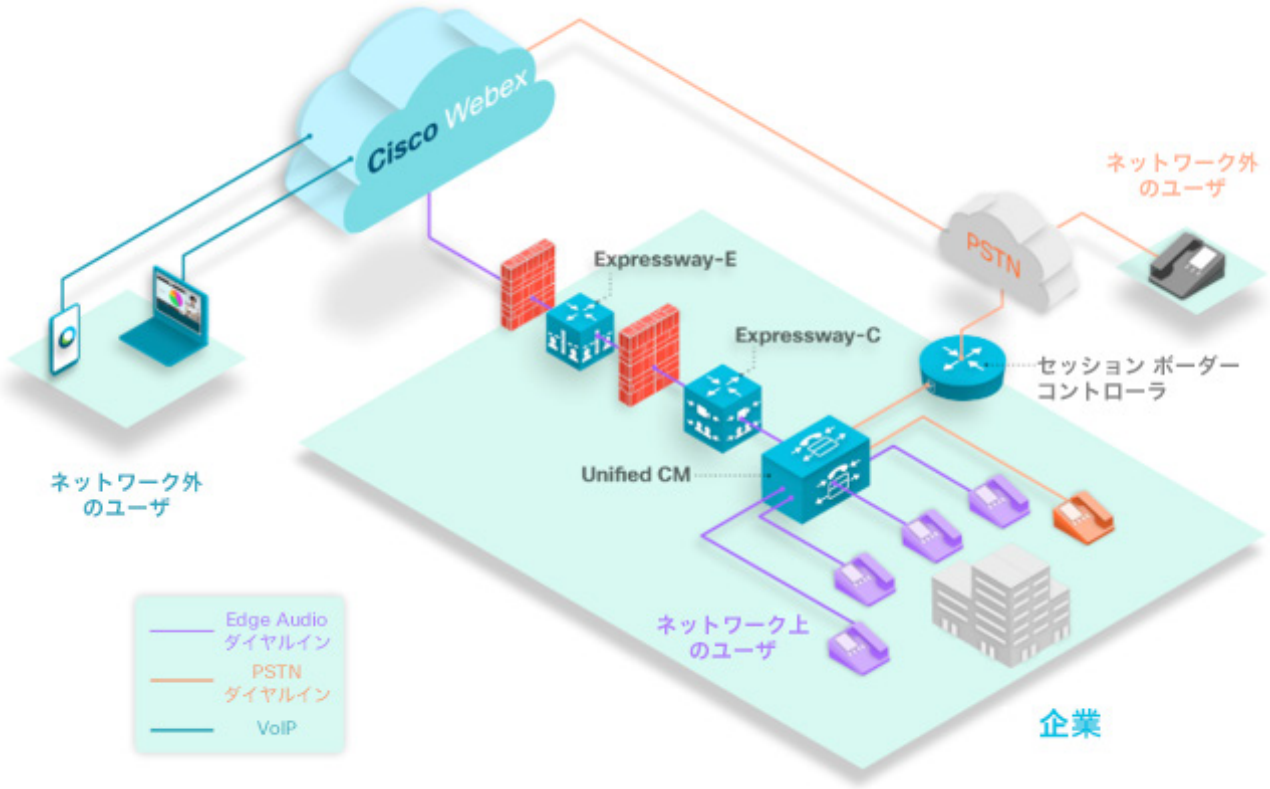
ここまでで、キーワード機能を使用した Exchange ハイブリッド カレンダー サービス、およびOne Button to Push機能、会議リスト、参加通知のテストができました。

シナリオ 5. Webex Edge Audio

このシナリオでは、Cisco Webex Edge Audio ソリューションを設定します。この設定は、Cisco Webex Edge Audio お客様向け設定ガイドに記載されている設定に従います。

Edge Audio は、企業内から発信されたコールが、社内ネットワーク、インターネットを経て、クラウドに届く音声ソリューションです。同様に、会議中に Webex から発信されたコールはインターネット経由でルーティングされ、オンプレミスの音声ルーティング機能を利用します。

ダイヤルインシナリオ

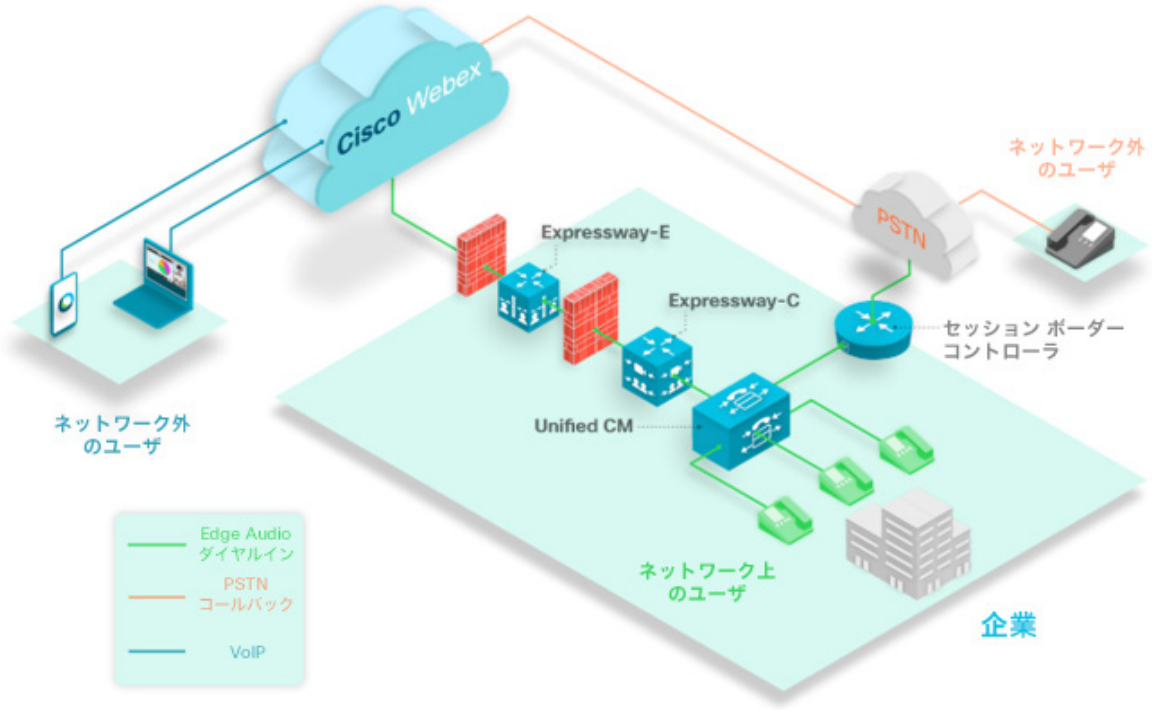


上の図は、一般的なダイヤルインシナリオを示しています。紫色の電話は、Edge Audio で設定された番号に電話をかけるダイヤルインユーザを示しています。Edge Audio で設定された番号にダイヤルするネットワーク上の全ユーザのコールは、Unified CM および Expressway を経由して Webex Cloud にルーティングされます。

オレンジ色の電話は、Edge Audio 経由でルーティングするように設定されていない番号を使用して会議にダイヤルインする企業内のユーザを示しています。このユーザは設定されていない番号にダイヤルするため、コールはセッション ボーダー コントローラ、PSTN を経由して Webex Cloud にルーティングされます。

グレーの電話は、ネットワーク外のユーザを示しています。ネットワーク外のユーザが Webex Meetings にダイヤルインしても、Edge Audio 経由でルーティングされません。ネットワーク外のユーザのコールは、PSTN 経由で Webex Cloud にルーティングされます。

コールバックシナリオ



上の図は、一般的なコールバックシナリオを示しています。緑色の電話は、コールが自分にルーティングされるように設定されているネットワーク上のコールバックユーザを示しています。

グレーの電話は、ネットワーク外のユーザを示しています。ネットワーク外のユーザが音声会議に参加する際にコールバックオプションを選択すると、コールは PSTN 経由で Webex Cloud にルーティングされます。

このガイドでは、社内から Webex Cloud へのコール（ダイヤルイン）に関して、ネットワークコンポーネント、Unified CM、Expressway-C、Expressway-E を設定する方法および、Webex から社内へのコール（コールバック）の処理方法を説明しています。

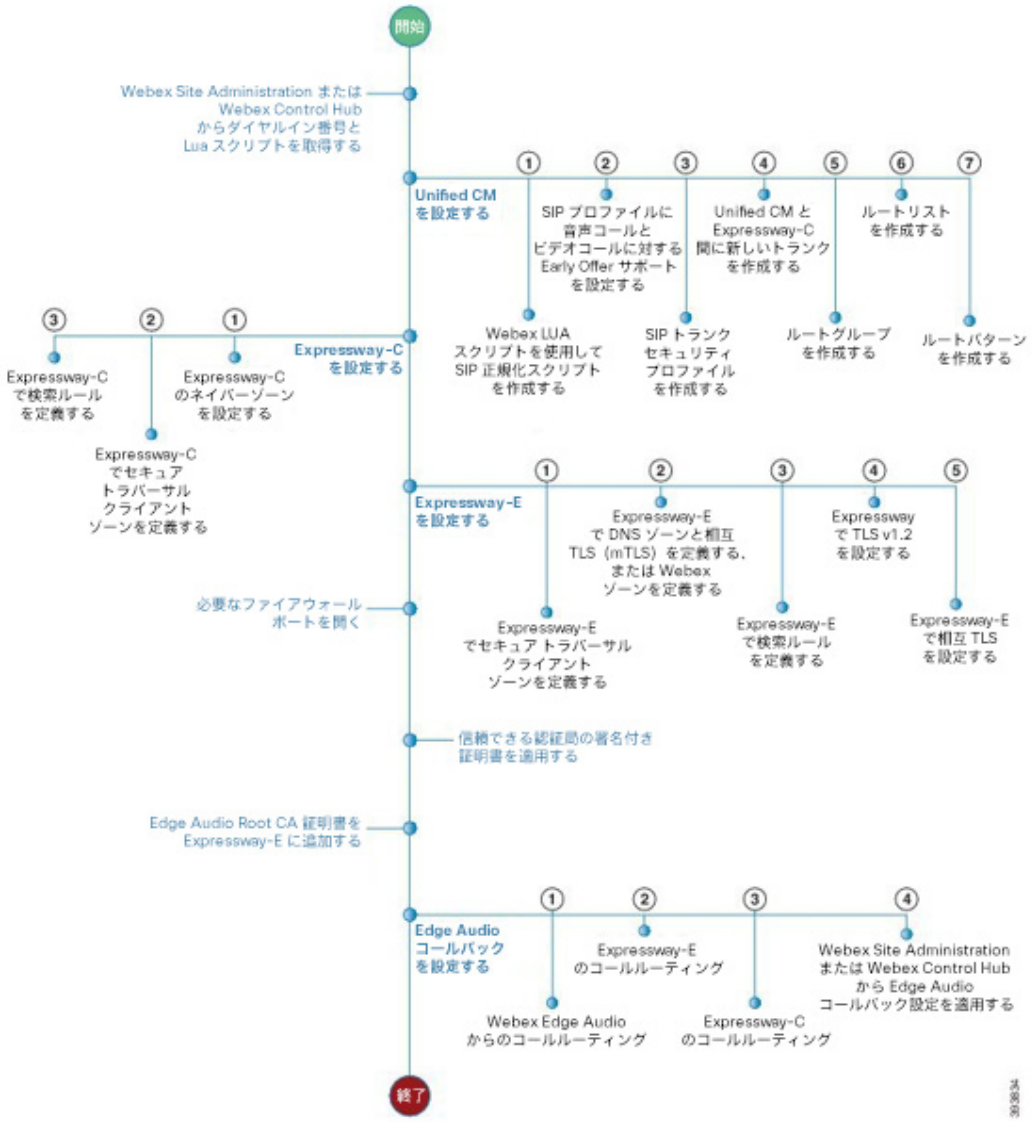
Edge Audio を設定するには、まず Cisco Webex Site Administration または Cisco Webex Control Hub から必要なダイヤルイン情報（ダイヤルイン番号と Lua 正規化スクリプト）を収集する必要があります。この情報を使用して、ユーザが Webex サービスにダイヤルインする際に使用するダイヤルイン番号を設定します。

Edge Audio の設定には、大きく次の 4 つの手順があります。

- ダイヤルイン番号と Lua スクリプトを取得する
- Unified CM を設定する
- Expressway-C を設定する
- Expressway-E を設定する

これらの各手順について次の図に示し、このシナリオで詳しく説明します。

詳細設定手順



Edge Audio で使用する Lua スクリプト

Webex 番号を使用するコールを Webex Cloud にルーティングするには、Webex 番号を使用して Unified CM でコールルーティングルールを指定する必要があります。Unified CM でトランクを作成するには（Lua）正規化スクリプトも必要です。これらの電話番号と Lua スクリプトは Webex Site Administration または Control Hub から収集できます。

Webex Site Administration で Webex サイトを管理している場合、またはサイトリンクプロセスを完了している場合は、指示に従って Webex Site Administration からダイヤルイン番号と Lua スクリプトを収集します（このラボでは詳細に説明しません）。

Webex Control Hub で Webex サイトをセットアップして管理している場合は、Webex Control Hub からダイヤルイン番号と Lua スクリプトを収集します（このラボでの詳細な手順は以下のとおり）。

Edge Audio は、Lua スクリプトを使用して適切にコールをルーティングするグローバルサービスです。Lua スクリプトは、次のようにコールを変換します。

- Expressway が Edge Audio にコールをルーティングできるように、リクエスト URI のホスト部分を更新する。
- Webex サイトを参照するリクエスト URI に x-cisco-site-uuid パラメータを追加する。
- Edge Audio での処理に必要な SIP To ヘッダーのユーザ部分を更新する。

Webex Control Hub からダイヤルイン番号と Lua スクリプトを収集する

1. Workstation 1 で **Cisco Webex Control Hub** に戻ります。
2. [サービス（Services）] に移動します。[ミーティング（Meeting）] で [サイト（Sites）] をクリックします。
3. 後で使用するので、リストされているサイトの **URL** をメモしておいてください。サイトを選択し、ポップアップウィンドウで [サイトを構成する（Configure Site）] をクリックします。
4. [共通設定（Common Settings）] の次の画面で、[Edge Audio] をクリックします。
5. [ダイヤルイン設定（Dial-in Settings）] で、[ここをクリック（Click here）] をクリックしてダイヤルイン番号を展開します。
6. dCloud セッションが確立されているデータセンターの**電話番号**を 1 つ書き留めるか、キャプチャします。この番号は後で使用します。セッションに割り当てられたドメインに基づいて、次の表で場所を判断します。

表 6. Webex ダイヤルイン番号

dCloud データセンター	国/電話ラベル
米国西部（dc-05）または米国東部（dc-01）	米国有料電話番号（指定された都市の番号を 1 つ選択）
EMEAR（dc-03）	United Kingdom Toll
APJ（dc-02）	Singapore Toll

7. ダイヤルイン番号の一番下までスクロールし、[Luaスクリプトを生成（Generate Lua Script）] をクリックし、[エクスポート（Export）] をクリックします。
8. **.lua** スクリプトが Workstation 1 のデスクトップに保存されます。
9. ポップアップウィンドウを閉じます。

Cisco Unified Communication Manager の設定

社内から Webex Cloud にコールをルーティングするには、Unified CM Administration でルーティングルールとトランクを設定する必要があります。

Webex LUA スクリプトを使用して SIP 正規化スクリプトを作成する

Webex Control Hub からエクスポートした Lua スクリプトを使用して、Unified CM で新しい SIP 正規化スクリプトを作成します。

1. Unified CM にログインしていない場合は、新しいブラウザタブで [コラボレーション管理リンク（Collaboration Admin Links）] > [Cisco Unified Communications Manager] の順に移動します。
2. [Cisco Unified Communications Manager] をクリックし、次の情報に基づいてログインします（事前に入力されています）。
   - ユーザ名：administrator
   - パスワード：dCloud123!
3. [デバイス（Device）] > [デバイス設定（Device Settings）] > [SIP正規化スクリプト（SIP Normalization Script）] の順に移動します。
4. [新規追加（Add New）] をクリックします。
5. スクリプトに **cbXXXYY_webex_edge_audio** などの名前を付けます（XXX と YY は、セッションの Webex サイト名に対応します）。その他の設定はすべてデフォルトのままにします。
6. ページの下部にある [ファイルのインポート（Import File）] をクリックします。
7. [ファイルの選択（Choose File）] をクリックし、デスクトップに以前エクスポートした **.lua** スクリプトを選択します。
8. [ファイルのインポート（Import File）]、[閉じる（Close）] の順にクリックします。インポートすると、[コンテンツ（Content）] ボックスに Lua スクリプトが表示されます。
9. [保存（Save）] をクリックします。

音声コールとビデオコールに対する Early Offer サポートを SIP プロファイルに設定する

このラボでは、新しい SIP プロファイルを作成します。すでに SIP プロファイルに Early Offer を設定している場合は、新たに作成せずにその SIP プロファイルを使用します。

1. [デバイス（Device）] > [デバイスの設定（Device Settings）] > [SIPプロファイル（SIP Profile）] の順に移動して、[検索（Find）] をクリックします。
2. [Cisco VCS用の標準SIPプロファイル（Standard SIP Profile For Cisco VCS）] の横の**コピー**アイコン [] をクリックします。
3. **Edge_Audio** という名前を付けます。

4. ページ下部の [音声コールとビデオコールに対するEarly Offerサポート（Early Offer support for voice and video calls）] で [ベストエフォート（MTPの挿入なし）（Best Effort (no MTP inserted)）] を選択します。
5. [保存（Save）] をクリックします。

SIP トランク セキュリティ プロファイルの作成

1. [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）] の順に選択し、[新規追加（Add New）] をクリックします。
2. トランクに **Edge_Audio** という名前を付けます。
3. [デバイスセキュリティモード（Device Security Mode）] で、選択項目を [非セキュア（Non Secure）] のままにします。実稼働環境では、[暗号化（Encrypted）] を選択する場合があります。
4. [着信ポート（Incoming Port）] に **5070** と入力します（5060 または 5061 の代わりに競合していないポートを使用します）。
5. [保存（Save）] をクリックします。

Edge Audio と G.722/G.711 コーデック

Edge Audio は G.722 および G.711 コーデックに対応しています。Edge Audio を利用するために Unified CM でこれらのコーデックを設定する必要はありませんが、これらのコーデックは他のコーデックよりも使用する帯域幅が少ないため、設定すると展開するサービスの品質を向上させることができます。このラボでは、例として別のリージョンとデバイスプールを作成します。実稼働環境では、G.722 および G.711 用に設定されたデバイスプールおよびリージョンがすでに存在する場合があります。その場合は、Edge Audio 用に新たに設定する必要はありません。

1. このラボでは、Unified CM G.722 はすでにアドバタイズされていますが、設定の参考として、[システム（System）] > [エンタープライズパラメータ（Enterprise Parameters）] の順に移動し、[G.722コーデックのアドバタイズ（Advertise G.722 Codec）] で [有効（Enabled）] を選択します。次に [保存（Save）] をクリックします。
2. [システム（System）] > [リージョン情報（Region Information）] > [リージョン（Region）] の順に移動し、[新規追加（Add New）] をクリックします。
3. 名前を **Edge_Audio** とし、[保存（Save）] をクリックします。
4. [リージョン（Regions）] リストから [デフォルト（Default）] と [Edge_Audio] の両方を選択します。
5. [オーディオコーデックの優先リスト（Audio Codec Preference List）] では、[初期設定Lossy圧縮（Factory Default Lossy）] を選択します。
6. [最大オーディオビットレート（Maximum Audio Bit Rate）] では、[64 kbps (G.722, G.711)] を選択します。
7. [保存（Save）] をクリックします。

次に、リージョンの設定先となるデバイスプールを設定します。

8. [システム（System）] > [デバイスプール（Device Pool）] の順に移動し、[検索（Find）] をクリックします。
9. **dCloud_DP** の横の**コピー**アイコンをクリックします。
10. Device Pool NameにEdge_Audio という名前を付けます。
11. [リージョン（Region）] で [Edge_Audio] を選択し、[保存（Save）] をクリックします。

Unified CM と Expressway-C 間に新しいトランクを作成する

Expressway-C では、既存のトランクを変更するのではなく、新しいトランクを作成する必要があります。

1. [デバイス（Device）] > [トランク（Trunk）] を選択し、[新規追加（Add New）] をクリックします。
2. [トランクタイプ（Trunk Type）] で [SIPトランク（SIP Trunk）] を選択します。タイプは [なし（None）] のままにして [次へ（Next）] をクリックします。
3. 以下の表に従ってパラメータを設定します。

表 7. Edge Audio SIP トランクの設定

設定対象	設定内容
[デバイス名（Device Name）]	Edge_Audio
[デバイスプール（Device Pool）]	Edge_Audio
[インバウンドコール（Inbound Calls）] > [コーリングサーチスペース（Calling Search Space）]	Call_Everyone
[SIP情報（SIP information）] > [接続先アドレス（Destination Address）]	198.18.133.152（Exp-C アドレス。5060 ポートも確保する）
[SIP情報（SIP Information）] > [SIPトランクセキュリティプロファイル（SIP Trunk Security Profile）]	Edge_Audio
[SIP情報（SIP Information）] > [SIPプロファイル（SIP Profile）]	Edge_Audio
[SIP情報（SIP Information）] > [DTMFシグナリング方式（DTMF Signaling Method）]	RFC 2833
正規化スクリプト（Normalization Script）	cbXXXYY_webex_edge_audio

4. [保存（Save）]、[OK]、[リセット（Reset）]、[リセット（Reset）]、[閉じる（Close）] の順にクリックします。

ルートグループの作成

1. [コールルーティング（Call Routing）] > [ルート/ハント（Route/Hunt）] > [ルートグループ（Route Group）] の順に移動し、[新規追加（Add New）] をクリックします。
2. [ルートグループ名（Route Group Name）] に **Edge_Audio_RG** と入力します。
3. [使用可能なデバイス（Available Devices）] ボックスから [Edge_Audio] を選択し、[ルートグループに追加（Add to Route Group）] をクリックします。
4. [保存（Save）] をクリックします。

ルートリストの作成

1. [コールルーティング（Call Routing）] > [ルート/ハント（Route/Hunt）] > [ルートリスト（Route List）] の順に移動し、[新規追加（Add New）] をクリックします。
2. [名前（Name）] に **Edge_Audio_RL** と入力します。
3. [Cisco Unified Communications Managerグループ（Cisco Unified Communications Manager Group）]で、[デフォルト（Default）] を選択します。
4. [保存（Save）] をクリックします。
5. ページを更新したら、[ルートグループを追加（Add Route Group）] をクリックします。
6. [ルートグループ（Route Group）] ドロップダウンリストから [Edge_Audio_RG-[NON-QSIG]] を選択します。
7. [保存（Save）] をクリックし、[OK] をクリックします。

ルートパターンの作成

以前収集した電話番号は、ルートパターンとして設定する必要があります。この電話番号は、ユーザが Webex Meetings を開始したり参加したりするためにダイヤルする番号です。

これらの番号には、Edge Audio で使用できるすべての番号が含まれています。設定、国、地域によっては、すべての番号のルートパターンを作成する必要がない場合もあります。

このラボでは、リスト内の 1 つの番号に対するルートパターンを設定します。ラボを実施している dCloud データセンターに対応する正しいダイヤルイン番号を選択する必要があります。まだ番号を取得していない場合は、Control Hub のページから取得する必要があります。

1. [コールルーティング（Call Routing）] > [ルート/ハント（Route/Hunt）] > [ルートパターン（Route Pattern）] の順に移動し、[新規追加（Add New）] をクリックします。
2. 以下の表に従ってパラメータを設定します。

表 8. ルートパターンの設定

設定対象	設定内容
[パターン定義（Pattern Definition）] > [ルートパターン（Route Pattern）]	シナリオの最初で取得した番号からプラス（+）を除きます。たとえば、取得した番号が +44-203-478-5290 だった場合、[ルートパターン（Route Pattern）] には 442034785290 と入力します。後で必要になるため、この番号を控えておきます。
[パターン定義（Pattern Definition）] > [ルートパーティション（Route Partition）]	Base_PT
[パターン定義（Pattern Definition）] > [ゲートウェイ/ルートリスト（Gateway/Route List）]	Edge_Audio_RL

3. [保存（Save）]、[OK]、[OK] の順にクリックします。

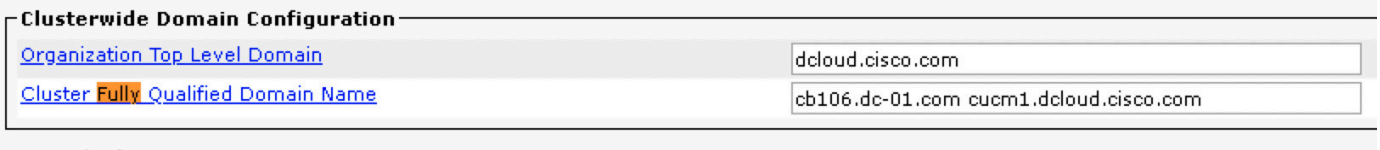
クラスタ完全修飾ドメイン名（Cluster FQDN）の設定

Unified CM にコールを適切にルーティングするためには、[クラスタの完全修飾ドメイン名（Cluster Fully Qualified Domain Name）] を更新してラボセッションに設定されたドメインを追加する必要があります。

1. [システム（System）] > [エンタープライズパラメータ（Enterprise Parameters）] に移動します。
2. 「**fully**」で検索すると、[クラスタの完全修飾ドメイン名（Cluster Fully Qualified Domain Name）] が見つかります。

ラボの基本設定では **cucm1.dcloud.cisco.com** がすでに設定されています。ボックスの設定をそのままにして、cucm1.dcloud.cisco.com エントリの前にラボセッションのドメインを追加し、スペースで区切ります。たとえば、ドメインが cb106.dc-01.com である場合、設定は **cb106.dc-01.com cucm1.dcloud.cisco.com** となります（以下の例を参照してください）。

クラスタの完全修飾ドメイン名の設定



3. [保存（Save）] をクリックします。

Expressway-C の設定

Expressway-C のネイバーゾーンの設定

1. 新しいブラウザタブで、[コラボレーション管理リンク（Collaboration Admin Links）] > [Cisco Expressway-C] の順に移動します。
2. **admin/dCloud123!** でログインします（あらかじめ入力されています）。
3. [設定（Configuration）] > [ゾーン（Zones）] > [ゾーン（Zones）] を選択し、[新規（New）] をクリックします。
4. 以下の表に従ってパラメータを設定します。

表 9. Edge Audio Expressway-C UCM ネイバーゾーンの設定

設定対象	設定内容
[設定（Configuration）] > [名前（Name）]	UCM Neighbor for Edge Audio
[設定（Configuration）] > [タイプ（Type）]	[ネイバー（Neighbor）]
[H.323] > [モード（Mode）]	オフ
[SIP] > [ポート（Port）]	5070（SIP トランク セキュア プロファイルと同じポート番号）

設定対象	設定内容
[SIP] > [トランスポート（Transport）]	TCP
[認証（Authentication）] > [認証ポリシー（Authentication policy）]	[認証済みとして扱う（Treat as Authenticated）]
[ロケーション（Location）] > [ピア1アドレス（Peer 1 Address）]	cucm1.dcloud.cisco.com
[詳細（Advanced）] > [ゾーンプロファイル（Zone Profile）]	[カスタム（Custom）]
[詳細（Advanced）] > [SIPパラメータの保持（SIP parameter preservation）]	オン

5. [ゾーンの作成（Create Zone）] をクリックします。

Expressway-C トラバーサル クライアント ゾーンの設定

1. [ゾーン（Zones）] ページで [新規（New）] をクリックします。
2. 以下の表に従ってパラメータを設定します。

表 10. Edge Audio Expressway-C トラバーサル クライアント ゾーンの設定

設定対象	設定内容
[設定（Configuration）] > [名前（Name）]	Traversal Client for Edge Audio
[設定（Configuration）] > [タイプ（Type）]	[トラバーサルクライアント（Traversal client）]
[接続ログイン情報（Connection credentials）] > [ユーザ名（Username）]	cisco2
[接続ログイン情報（Connection credentials）] > [パスワード（Password）]	dCloud123!
[H.323] > [モード（Mode）]	オフ
[SIP] > [ポート（Port）]	7005
[SIP] > [メディア暗号化モード（Media encryption mode）]	[強制暗号化（Force encrypted）]
[SIP] > [SIPパラメータの保持（SIP parameter preservation）]	オン
[ロケーション（Location）] > [ピア1アドレス（Peer 1 Address）]	vcse.cbXXX.dc-YY.com

3. [ゾーンの作成（Create Zone）] をクリックします。

Expressway-C 検索ルールの設定

1. [設定（Configuration）] > [ダイヤルプラン（Dial Plan）] > [検索ルール（Search Rules）] の順に移動し、[新規（New）] をクリックします。
2. 以下の表に従ってパラメータを設定します。

表 11. Edge Audio Expressway-C 検索ルールの設定

設定対象	設定内容
[設定（Configuration）] > [ルール名（Rule Name）]	Outbound Edge Audio
[設定（Configuration）] > [プライオリティ（Priority）]	98
[設定（Configuration）] > [プロトコル（Protocol）]	SIP
[設定（Configuration）] > [送信元（Source）]	[指定（Named）]
[設定（Configuration）] > [送信元名（Source Name）]	UCM Neighbor for Edge Audio
[設定（Configuration）] > [リクエストの認証が必要（Request must be authenticated）]	[必要（Yes）]
[設定（Configuration）] > [一致した場合（On successful match）]	[停止（Stop）]
[設定（Configuration）] > [転送先（Target）]	Traversal Client for Edge Audio

3. [検索ルールの作成（Create search rule）] をクリックします。

Expressway-E の設定

Expressway-E セキュア トラバーサル サーバ ゾーンの設定

1. Workstation 1 の新しいブラウザタブで、[コラボレーション管理リンク（Collaboration Admin Links）] > [Cisco Expressway-E] の順に移動します。
2. **セキュリティ警告**のプロンプトが表示されたら、同意して続行します。**admin/dCloud123!** でログインします。
3. [設定（Configuration）] > [ゾーン（Zones）] > [ゾーン（Zones）] を選択し、[新規（New）] をクリックします。
4. 以下の表に従ってパラメータを設定します。

表 12. Edge Audio Expressway-E トラバーサルサーバゾーンの設定

設定対象	設定内容
[設定（Configuration）] > [名前（Name）]	Traversal Server for Edge Audio
[設定（Configuration）] > [タイプ（Type）]	[トラバーサルサーバ（Traversal server）]
[接続ログイン情報（Connection credentials）] > [ユーザ名（Username）]	cisco2
[H.323] > [モード（Mode）]	オフ
[SIP] > [ポート（Port）]	7005
[SIP] > [メディア暗号化モード（Media encryption mode）]	[自動（Auto）]（デフォルト）
[SIP] > [SIPパラメータの保持（SIP parameter preservation）]	オン
[認証（Authentication）] > [認証ポリシー（Authentication policy）]	[認証済みとして扱う（Treat as Authenticated）]

5. [ゾーンの作成（Create Zone）] をクリックします。

Expressway-E Webex ゾーンの設定（X8.11 以降）

注：このラボでは、Expressway のバージョンは X8.11 以上です。それよりも前のバージョンではこのゾーンは設定できないため、通常の DNS ゾーンを使用する必要があります。必要な設定を表示するには**ここ**をクリックします。

1. [ゾーン（Zones）] ページで [新規（New）] をクリックします。
2. [タイプ（Type）] では [Webex] を選択します。
3. [ゾーンの作成（Create Zone）] をクリックします。

Expressway-E 検索ルールの設定

1. [設定（Configuration）] > [ダイヤルプラン（Dial Plan）] > [検索ルール（Search Rules）] の順に移動し、[新規（New）] をクリックします。
2. 以下の表に従ってパラメータを設定します。

表 13. Edge Audio Expressway-E 検索ルールの設定

設定対象	設定内容
[設定（Configuration）] > [ルール名（Rule Name）]	Outbound Edge Audio
[設定（Configuration）] > [プライオリティ（Priority）]	98
[設定（Configuration）] > [プロトコル（Protocol）]	SIP
[設定（Configuration）] > [送信元（Source）]	[指定（Named）]
[設定（Configuration）] > [送信元名（Source Name）]	Traversal Server for Edge Audio
[設定（Configuration）] > [リクエストの認証が必要（Request must be authenticated）]	[必要（Yes）]
[設定（Configuration）] > [一致した場合（On successful match）]	[停止（Stop）]
[設定（Configuration）] > [転送先（Target）]	[Webexゾーン（Webex Zone）]

3. [検索ルールの作成（Create search rule）] をクリックします。

Expressway-E 相互 TLS の設定

1. [設定（Configuration）] > [プロトコル（Protocols）] > [SIP] の順に移動します。
2. [相互TLS（Mutual TLS）] モードでは、[オン（On）] を選択します（[相互TLSポート（Mutual TLS port）] では 5062 のデフォルトポートのままにします）。
3. [保存（Save）] をクリックします。

注：実稼働環境での次の手順は、適切なファイアウォールポートが開いているか確認すること、および適切な証明書が Expressway-E にインストールされていることを確認することです。これらの作業はすでに基本ラボで実施されています。必要な手順の詳細については、「**必要なファイアウォールポートを開く**」を参照してください。

Edge Audio コールバックの設定

次は Edge Audio コールバックの設定です。コールバックの設定を開始する前に、次の事項を考慮して DNS SRV レコードをサイトに設定する必要があります。

- DNS SRV は Expressway-E の相互 TLS ポート（ポート 5062）をポイントしている必要がある。
- DNS SRV は、それぞれにポート 5062 が設定されたすべての Expressway-E ターゲット A レコードをクラスタ内に含める必要がある。

この設定は、dCloud プラットフォームの DNS サーバですでに完了しています。ポート 5062 で MTLS を許可するように、**_sips._tcp.mtls.cbXXX.dc-YY.com** SRV レコードがセッションに設定されています。

Webex Edge Audio からのコールルーティング

E.164 番号が Expressway-E を通過し、設定に基づいてコールがルーティングされるようにする必要があります。これにより、ネットワーク上のユーザのコールが適切にルーティングされ、Unified CM や、携帯電話に接続しているユーザなどのネットワーク外のユーザにつながります。また、通話料不正行為などを防止するために、Expressway-E にコールポリシールールを適用します。また、Webex からの Edge Audio インバウンドコールを許可するために、新しいコールポリシールールも作成します。

Expressway-E のコールルーティング

1. Expressway-E で [設定（Configuration）] > [ダイヤルプラン（Dial plan）] > [検索ルール（Search rules）] の順に移動し、先ほど作成した**Outbound Edge Audio** 検索ルールの横にある [複製（Clone）] をクリックします。
2. 以下の表に従ってパラメータを変更します。

注：正規表現パターンを追加する際には、末尾にスペースを含めないことが重要です。

表 14. Edge Audio Expressway-E 検索ルールの設定

設定対象	設定内容
[設定（Configuration）] > [ルール名（Rule Name）]	Inbound Edge Audio
[設定（Configuration）] > [送信元名（Source Name）]	[Webexゾーン（Webex Zone）]
[設定（Configuration）] > [モード（Mode）]	[エイリアスパターンマッチ（Alias pattern match）]
[設定（Configuration）] > [パターンタイプ（Pattern type）]	[正規表現（Regex）]

設定対象	設定内容
[設定（Configuration）] > [パターン文字列（Pattern string）]	(.*)@mtls\.cbXXX\.dc-YY\.com;.*x-cisco-webex-service=audio（XXX と YY は自分のセッションドメイン情報に置き換える）
[設定（Configuration）] > [パターン動作（Pattern behavior）]	[置き換え（Replace）]
[設定（Configuration）] > [文字列の置き換え（Replace string）]	\1@cbXXX.dc-YY.com（XXX と YY は自分のセッションドメイン情報に置き換える）
[設定（Configuration）] > [転送先（Target）]	Traversal Server for Edge Audio

3. [検索ルールの作成（Create search rule）] をクリックします。

コールポリシールール

次に、インボウンド Webex Edge Audio コールを許可する新しいポリシールールを作成します。

1. Expressway-E で [設定（Configuration）] > [コールポリシー（Call Policy）] > [ルール（Rules）] の順に移動し、[新規（New）] をクリックします。
2. 以下の表に従ってパラメータを変更します。

表 15. Edge Audio Expressway-E コールポリシールールの設定

設定対象	設定内容
[送信元タイプ（Source Type）]	[ゾーン（Zone）]
[発信元ゾーン（Originating Zone）]	[Webexゾーン（Webex Zone）]
[宛先パターン（Destination pattern）]	.*

3. [追加（Add）] をクリックします。
4. リストの下部にある新しい **Webex ゾーン**ルールを見つけ、上向き矢印 [ ] を使用して、コールポリシーリストの一番上に移動します。

Expressway-C のコールルーティング

1. Expressway-C で [設定（Configuration）] > [ダイヤルプラン（Dial plan）] > [検索ルール（Search rules）] の順に移動し、先ほど作成した**Outbound Edge Audio** 検索ルールの横にある [複製（Clone）] をクリックします。
2. 以下の表に従ってパラメータを変更します。

表 16. Edge Audio Expressway-C 検索ルールの設定

設定対象	設定内容
[設定（Configuration）] > [ルール名（Rule Name）]	Inbound Edge Audio
[設定（Configuration）] > [送信元名（Source Name）]	Traversal Client for Edge Audio
[設定（Configuration）] > [転送先（Target）]	UCM Neighbor for Edge Audio

3. [検索ルールの作成（Create search rule）] をクリックします。

Edge Audio コールバック設定を Control Hub から適用する

1. Control Hub（admin.webex.com）に戻り、[サービス（Services）] に移動します。[ミーティング（Meeting）] で [サイト（Sites）] をクリックします。
2. リストからサイトを選択し、ポップアップウィンドウで [サイトを構成する（Configure Site）] をクリックします。
3. [共通設定（Common Settings）] の次の画面で、[Edge Audio] をクリックします。Webex Edge は、内線番号を使用したコールバックをサポートしています。
4. [国/地域（Country/Region）] で [内線番号（Extension）] を選択します。
5. [Expressway DNS SRV] には、**mtls.cbXXX.dc-YY.com** を入力します。
6. [追加（Add）] をクリックします（接続チェックの状態は [成功（Successful）] になります）。
7. [国/地域（Country/Region）] の [コールバック設定（Callback Settings）] で、以下の表の dCloud データセンターリストに基づいて地域を選択します。

表 17. コールバック設定

dCloud データセンター	ダイヤルイン番号
米国西部（dc-05）または米国東部（dc-01）	米国（1）
EMEAR（dc-03）	英国（44）
APJ（dc-02）	シンガポール（65）

8. [Expressway DNS SRV] には、**mtls.cbXXX.dc-YY.com** を入力します。
9. [追加（Add）] をクリックします（接続チェックの状態は [成功（Successful）] になります）。
10. **重要**：ページの下部までスクロールし、[設定の適用（Apply Settings）] をクリックして [OK] をクリックします。
11. [設定の適用（Apply Settings）] ボタンをクリック後、ボタンがグレー表示になっていることを確認します。

注：設定を適用した後、コールバック国はすぐに Control Hub に表示されますが、設定がデータベースに適用されるまで最大 30 分かかることがあります。設定がデータベースに適用されるまで、コールは前に設定された国の設定でルーティングされます。

12. また、このページで、[PSTN音声を使用したコールの再試行（Retry call using PSTN Audio）] がデフォルトで設定されていることを確認します。1 つ以上の国で Edge Audio コールバックが有効になっている場合、Webex は、インターネット経由でコールをルーティングします。デフォルトでは、DNS、TCP、TLS 接続に問題がある場合や、380 または 400 ~ 699 の SIP エラーコードが返ってきてコールが失敗した場合は、Webex は PSTN 接続を利用してコールを再試行します。

Webex Edge Audio のテスト

1. Workstation 1 で Cisco Jabber クライアントを開いてサインインします。電子メールアドレスには **cholland@cbXXX.dc-YY.com**、ユーザ名/パスワードには **cholland/dCloud123!** を指定します。

2. Workstation 1 内の Web ブラウザまたは自分の Web ブラウザを使用して、**https://cbXXXYY.webex.com**（このシナリオの最初に Control Hub から取得した自分のセッションの Webex URL）に移動します。

注：Webex Meetings サイトの URL が機能しない場合は、Control Hub で URL を確認してください。[サービス（Services）] > [会議（Meeting）] > [サイト（Sites）] > [サイト名（Site Name）] の順に移動します。使用可能なその他の URL には、https://cbXXXYYa.webex.com、https://cbXXXYYb.webex.com、https://cbXXXYYc.webex.com があります。

3. まだ自動的にサインインしていない場合は、Charles Holland（**cholland@cbXXX.dc-YY.com/dCloud123!**）でサインインします。
4. [会議を開始（Start Meeting）] をクリックします。
5. Webex Meetings アプリをダウンロードするようにプロンプトが表示される場合があります。Webex Meetings アプリケーションがまだインストールされていない場合は、ダウンロードしてインストールしてください。アプリケーションを開き、Charles のアカウントでサインインします。ブラウザを使用して参加する場合は、[ブラウザで参加（Join from your browser）] をクリックします。
6. Webex Meetings アプリケーションで、[会議を開始（Start Meeting）] をクリックします（ブラウザを使用している場合は、次の手順に進みます。また、プロンプトが表示されるすべてのコーチマークを実行します）。
7. 画面の左上にある**会議情報**アイコン [ ] をクリックします（マウスを動かすと表示されます）。
8. [会議番号（Meeting Number）] と [出席者ID（Attendee ID）] を取得します。
9. 以前 Cisco Jabber から Unified CM にルートパターンとして設定した**正確な**番号をダイヤルして Webex のダイヤルインを Jabber でテストします。
10. 接続してプロンプトが表示されたら、[コールイン（Call In）] 画面に表示された [会議ID（Meeting ID）] と [出席者番号（Attendee Number）] を入力します。

これで Webex Meetings に Edge Audio 経由で接続されます。

Expressway-C または E にログオンして Expressway を経由していることを確認し、ゾーンを表示できます。Edge Audio の 1 コールと以前に作成した Webex ゾーンが表示されます。

11. 次に、コールバックをテストします。まず、フル桁の電話番号をテストします。
12. Jabber から Webex Meetings へのコールを切断しますが、Webex Meetings はアクティブのままにします。
13. Meetings アプリで**その他のオプション**アイコン [ ] をクリックし、[音声接続（Audio connection）] を選択します。次に [ピックリスト（picklist）] ドロップダウンをクリックし、[コールバック（Call me）] を選択します。
14. 国コード（米国のデータセンターの場合は **+1**、EMEAR データセンターの場合は **+44**、APJ データセンターの場合は **+65**）を選択したまま、番号 **972-555-6018** を入力して [接続（Connect）] をクリックします（コンピュータのオーディオに接続されている場合は [スイッチ（Switch）]）。
15. Cisco Jabber クライアントが鳴ったら、応答します。

16. プロンプトが表示されたら、**1 を押して**会議に参加します。
17. （オプション）Expressway をチェックして、Edge Audio ゾーンを使用したコールを確認します。
18. 完了したら通話を終了します。
19. Charles の内線番号にコールバックします。[コールバック（Call me）] オプションでドロップダウンアイコンをクリックし、[内線にコールバック（Call me at an internal...）] を選択します。
20. 電話番号に **6018** と入力し、[接続（Connect）] をクリックします。
21. コールに応答し、必要に応じて Expressway ゾーンを確認します。
22. 完了したら通話を終了します。

次に PSTN フォールバックをテストします。Charles 向けのセッションに割り当てられた実際の DID を使用してテストします。この番号は、dCloud セッションの詳細ページ、または、Workstation 1 のデスクトップにある **DN_to_DID.txt** という名前のテキストファイルに記載されています。ここでその番号を取得します。また、自分の携帯電話番号を使用することもできます。

まず、Expressway を経由してコールが送信されないようにするには、現在の設定を調整する必要があります。今コールすると、コールは Expressway を経由し、dCloud PSTN にはルーティングされません。Charles の DID 番号を使用した場合、PSTN は、同じ dCloud ゲートウェイ経由で Charles の電話にルーティングし、電話を呼び出します。自分の携帯電話番号にダイヤルし、その番号が、セッションが確立されているデータセンターの国の番号の場合、コールは dCloud PSTN を経由して携帯電話に着信します。ここで電話をかけるテストをし、Edge Audio のゾーン数が 1 に増えることを確認します。

設定を解除するにはさまざまな方法がありますが、このラボでは、Expressway-E でインバウンド検索ルールを無効にすることで解除します。

23. Expressway-E で、[設定（Configuration）] > [ダイヤルプラン（Dial Plan）] > [検索ルール（Search rules）] の順に移動します。
24. [Inbound Edge Audio（Inbound Edge Audio）] の横にあるチェックボックスをオンにし、下部の [無効化（Disable）] をクリックします。

これで、コールが来ても Unified CM へのルートが見つからないため受信できず、代替のフォールバックオプションが選択されます。

25. DID 番号または自分の携帯電話番号を使用して、Charles にコールバックします。[コールバック（Call me）] オプションで、[別の電話を使用（Use a different phone...）] をクリックします。
26. 番号を入力し、[接続（Connect）] をクリックします。フェールオーバーには約 30 ~ 40 秒かかる場合があることに注意してください。
27. フォールバックのテストが完了したら、忘れずに **Expressway-E** で**検索ルール**を有効に戻します。

シナリオ 6. Webex Video Mesh

このシナリオでは、Webex Video Mesh サービスを設定する手順を確認します。Cisco Webex Video Mesh は、オンプレミスとクラウドのリソースをブリッジすることで、ユーザが高品質な音声、ビデオ、コンテンツを利用できる画期的な機能です。

エンドユーザは、高品質な音声、ビデオ、コンテンツ共有を実現する優れた会議エクスペリエンスを求めています。デバイスを問わずに一貫した優れた操作性で会議に参加できることを期待しています。

これは簡単なことではありません。IT 部門にとって、すべてのユーザに優れたエクスペリエンスを提供することも大切ですが、拡張性、信頼性を確保し、コストを削減する必要もあります。クラウドベースまたはオンプレミスベースの会議を導入するかどうかは、最も難しい意思決定の 1 つです。各会議の導入モデルには、それぞれに独自の利点があり、IT 部門はその中から選択する必要があります。

Cisco Webex Video Mesh は、Webex Video Mesh Node ソフトウェアを使用します。Webex Video Mesh Node は、Cisco UCS® サーバにインストールされ、Cisco Webex Control Hub で管理されます。Video Mesh Node をネットワークにインストールすると、クラウド内の Cisco Webex サービスと通信し、Cisco Webex サービスまたは Cisco Unified CM に登録されているデバイスで使用できます。

会議に参加すると、デバイスはクラウド内の Cisco Webex と通信して、会議に最適な Video Mesh Node を見つけます。次に、メディア（音声、ビデオ、コンテンツ）が Video Mesh Node に送信されて処理されます。Video Mesh Node は、エンタープライズ ネットワーク上に単一ノードとして導入することもできますが、クラウドとオンプレミスが連携した複数ノードとして導入して会議を作成することも可能です。いずれの場合も、ユーザエクスペリエンスはまったく同じです。

特長と利点

表 18. 特長と利点

特長	利点
Cisco Webex オンプレミス会議の参加者向けのメディアをローカルで処理	コール処理のためにメディアがクラウドを行き来することがなくなります。メディアはオンプレミスで処理されるため以下の利点があります。 - 遅延の短縮による品質の向上 - 他のユーザや会議への接続スピードがアップ - インターネット帯域幅の使用効率向上によるコスト削減
オンプレミスリソースが枯渇した場合や使用できない場合のクラウドへの自動オーバーフロー	信頼性の向上
オンプレミスとクラウド全体での管理と可視性の一元化	- ツールの集約：Cisco Webex Control Hub と呼ばれる単一の一元化された管理ポータルでオンプレミスのメディアノードと Cisco Webex 組織を管理 - 管理者が一元的にリソース使用状況を可視化し、キャパシティ使用率を正確に把握可能 - リソースプランニングと利用率管理のシンプル化
自動ソフトウェア更新	容易な保守：Video Mesh Node は、オンプレミスの Cisco Webex サービスに対する拡張機能です。クラウドに展開されるセキュリティ修正、バグ修正、機能拡張などのソフトウェアアップデートと同期されます。
導入が容易	- 各 Cisco Webex Video Mesh Node の導入時間はわずか 10 分 - 導入が容易で、必要に応じてキャパシティを追加可能
Cisco Webex Meetings を購入した場合に機能が付属	低コスト：追加のサブスクリプション料金や超過料金は不要。

初期導入を含むすべてのセットアップ手順については、Cisco Webex Video Mesh 導入ガイドを参照してください。

Video Mesh Node の導入

ここでは、Video Mesh Node をダウンロードし、VMware ESXi ホストに導入します。**Workstation 1** で実行します。

1. **198.18.1.36** の Workstation 1 に接続します。
   - ユーザ名：**dcloud\cholland**
   - パスワード：**dCloud123!**
2. Chrome を開き、Cisco Webex Control Hub（**admin.webex.com**）に戻り、必要に応じて **cholland@cbXXX.dc-YY.com/dCloud123!** でログインします。
3. ポータル内の左側のメニューで、[サービス（Services）] をクリックします。
4. [ビデオ メッシュ（Video Mesh）] で [セットアップ（Set up）] をクリックします。
5. [いいえ、ソフトウェアをインストールして設定する必要があります（No, I need to install and configure the software）] を選択します。
6. **重要**：[キャパシティ制限付きの90日間デモ（Limited capacity 90 day demo）] を選択します（ラボではキャパシティをすべて利用することはありません）。
7. [次へ（Next）] をクリックし、[OK] をクリックします。
8. **videomesh_demo.ova** が Workstation 1 のデスクトップにダウンロードされるまで待ちます。
9. ova のダウンロードが完了したら、デスクトップまたはタスクバーのアイコン  をクリックして VMware vSphere クライアントを開きます。
10. **root/dCloud123!** で **esxi1** にログインします。
11. [ファイル（File）] > [OVFテンプレートの導入（Deploy OVF Template）] をクリックします。
12. デスクトップを参照して、ダウンロードした **videomesh_demo.ova** を選択し、[次へ（Next）] をクリックします。
13. [OVFテンプレートの詳細（OVF Template Details）] ページで、[次へ（Next）] をクリックします。
14. [名前（name）] に **vmn1** と入力し、[次へ（Next）] をクリックします。

重要：[シンプロビジョニング（Thin Provision）] を選択し、[次へ（Next）] をクリックします（ラボで機能するのはシンプロビジョニングのみです）。

15. デフォルトの [ネットワークマッピング（Network Mapping）] のまま、[次へ（Next）] をクリックします。

注：Video Mesh Node ではデュアル NIC を使用できますが、ラボではシングル NIC を使用します。

16. [導入後に起動（Power on after deployment）] チェックボックスをオンにし、[終了（Finish）] をクリックします。

17. OVA が導入されたら [閉じる（Close）] をクリックします。

18. ホスト **esxi1** を展開し、**vmn1** 仮想マシンを選択します。

19. [コンソール（Console）] タブをクリックします。

メディアノードが起動していることを確認します。画面が更新されなくなり、**ciscoecp_** の後に数字と文字が追加された文字列がログインプロンプトに表示されるまで待ちます（**localhost** ではありません）。画面の更新が停止したら、ウィンドウ内をクリックして Enter キーを押します。電源を入れた後、ノードが完全に起動するまで数分かかります。

20. admin/cisco でログインします。

21. プロンプトが表示されたら、`(current) UNIX password:` `cisco` と入力します。

22. 新しいパスワードとして `dCloud123!` を入力します（2 回入力する必要があります）。

23. パスワードのリセットが成功したら、セキュリティ警告では Enter を押します。

24. 下矢印を押して [2 設定の編集（Edit Configuration）] に移動し、Enter を押します。

注：実稼働環境でデュアル NIC を設定している場合、オプション 5 も設定します。

25. Enter を押して次に進みます。

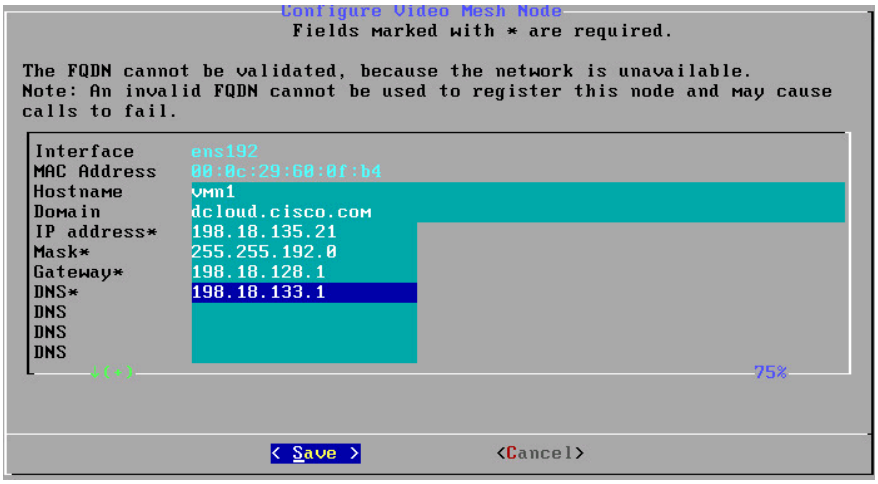
26. Enter を押して [静的（Static）] を選択します。

27. 以下の表に従って次のパラメータを設定します。

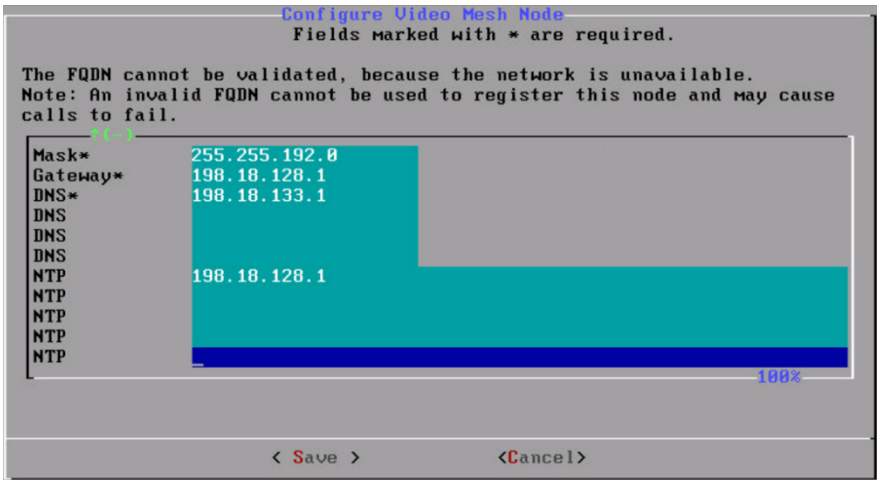
表 19. Video Mesh Node の設定

設定対象	設定内容
[ホスト名（Hostname）]	vmn1
[ドメイン（Domain）]	dcloud.cisco.com
[IPアドレス（IP Address）]	198.18.135.21
[マスク（Mask）]	255.255.192.0
[ゲートウェイ（Gateway）]	198.18.128.1
[DNS]	198.18.133.1
[NTP]	198.18.128.1（見つかるまでスクロールします。他の NTP サーバはクリアします）

Video Mesh Node の設定



Video Mesh Node の設定（続き）



28. [保存（Save）] を選択して **Enter** を押します。
29. **Enter** を押し、[変更を保存して再起動（Save Changes & Reboot）] を選択します。
30. **Enter** を押して、[完了（Done）] を選択します。
31. マウスをコンソールウィンドウから離すには、**Ctrl+Alt** キーを押します。
32. **vSphere Client** を最小化できます。

注：以下で Video Mesh Node を登録する際には、再起動に約 2 分かかることに注意してください。

Video Mesh Node Control Hub の設定

次に、Cisco Webex Meetings サービスで使用する、新しい Video Mesh Node をカスタマー組織に追加します。

1. **Cisco Webex Control Hub** に戻ります。
2. ポータル内の左側のメニューで、[サービス（Services）] をクリックします。
3. [Video Mesh] で [セットアップ（Set up）] をクリックします。
4. [はい、Video Mesh Nodeを登録する準備ができています（Yes, I'm ready to register my Video Mesh Node）] をオンのまま、[次へ（Next）] をクリックします。

これは最初のノードとクラスタであるため、新しいクラスタを作成する必要があります。

5. [新規クラスターを作成する（Create a new cluster）] オプションボタンを選択します。
6. 最初のボックスに **Video Mesh Cluster 1** と入力します。
7. 2 番目のボックスに **vmn1.dcloud.cisco.com** と入力します。
8. [次へ（Next）] をクリックします。
9. すべてに目を通しますが、[サービス設定（Service Configuration）] の内容はそのままにしておき、[次へ（Next）] をクリックします。
10. [アップグレードスケジュール（Upgrade Schedule）] の設定はそのままにして [次へ（Next）] をクリックします。
11. [SIP TLS設定（SIP TLS Configuration）] ページで [次へ（Next）] をクリックします。
12. [ノードに進む（Go to Node）] をクリックします（追加時にエラーが表示される場合、以下の注を参照）。

注：Video Mesh Node の Web ページを表示するには、ポップアップを許可している必要があります。ブラウザでポップアップが許可されていないと、Video Mesh Node の Web ページを表示できません。また、Chrome で [詳細（Advanced）] をクリックし、警告が表示されたら [はい（Yes）] をクリックして続行します。

13. ブラウザで、Video Mesh Node の新しいタブが開きます。証明書に関する警告にすべて同意します。必要に応じて Charles でログインします（**cholland@cbXXX.dc-YY.com/dCloud123!**）。ページが完全に開いたら、[Webex Video Mesh Nodeへのアクセスを許可する（Allow Access to the Webex Video Mesh Node）] のチェックボックスをオンにします。
14. [続行（Continue）] をクリックします。
15. クラウドに接続すると、[登録完了（Registration Complete）] 画面が表示されます。ブラウザタブを閉じます。

接続後はそれ以上の設定は必要ありません。Webex Control Hub で、Video Mesh Node の管理が自動的に開始されます。管理ポータルに戻ると、ノード/サービスの登録解除/非アクティブ化、別のクラスタへのノードの移動、ビデオ品質の変更、管理電子メール通知の更新を実施できます。

ラボは Video Mesh Node のデモ版を使用しているので、設定した CPU 数に関するアラームが表示されます。このアラームは予期されたことであり、無視してかまいません。また、クラウドに接続すると、ファームウェアが自動的にアップグレードされます。アップグレード中何度か再起動される際は、[停止（Outage）] と表示されます。アップグレードが完了すると [運用中（Operational）] に変わります。

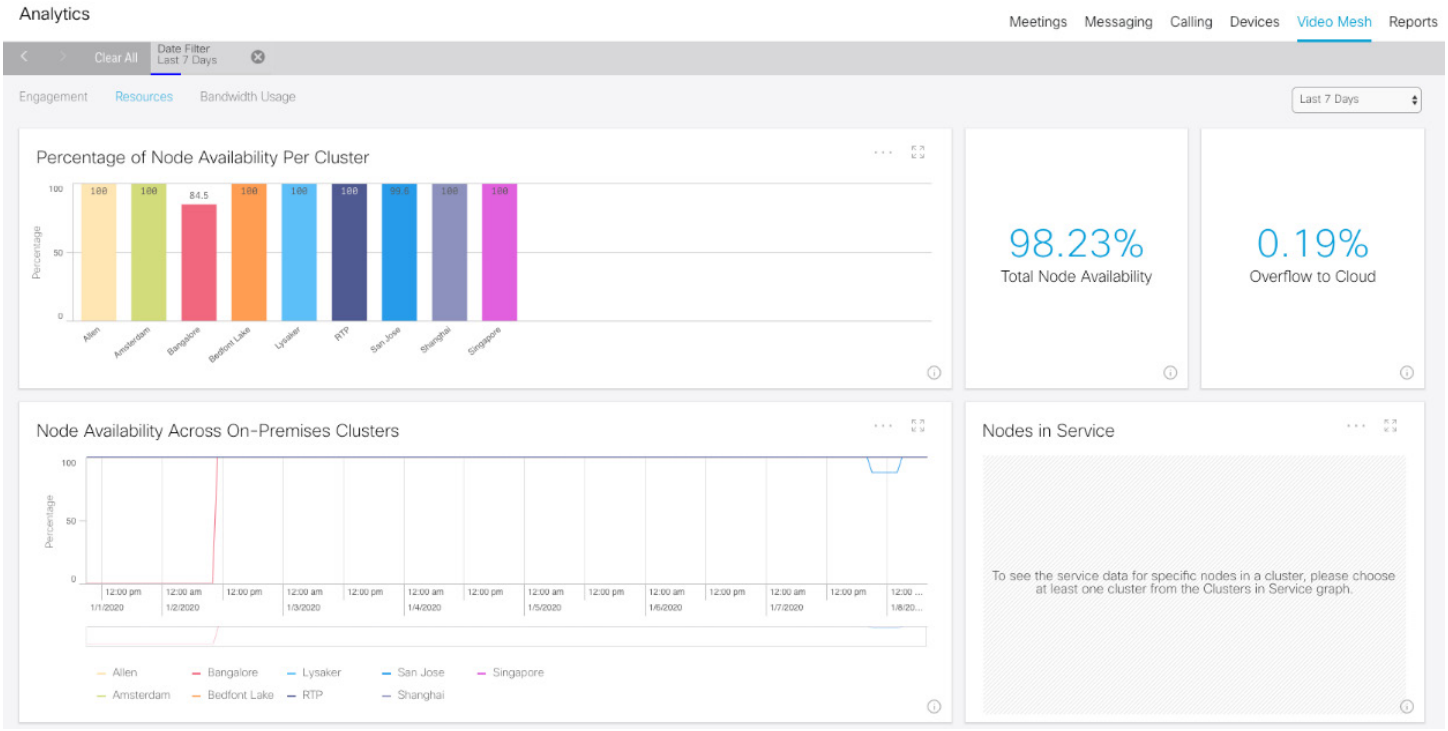
アクセス可能なローカル管理ページもあります。

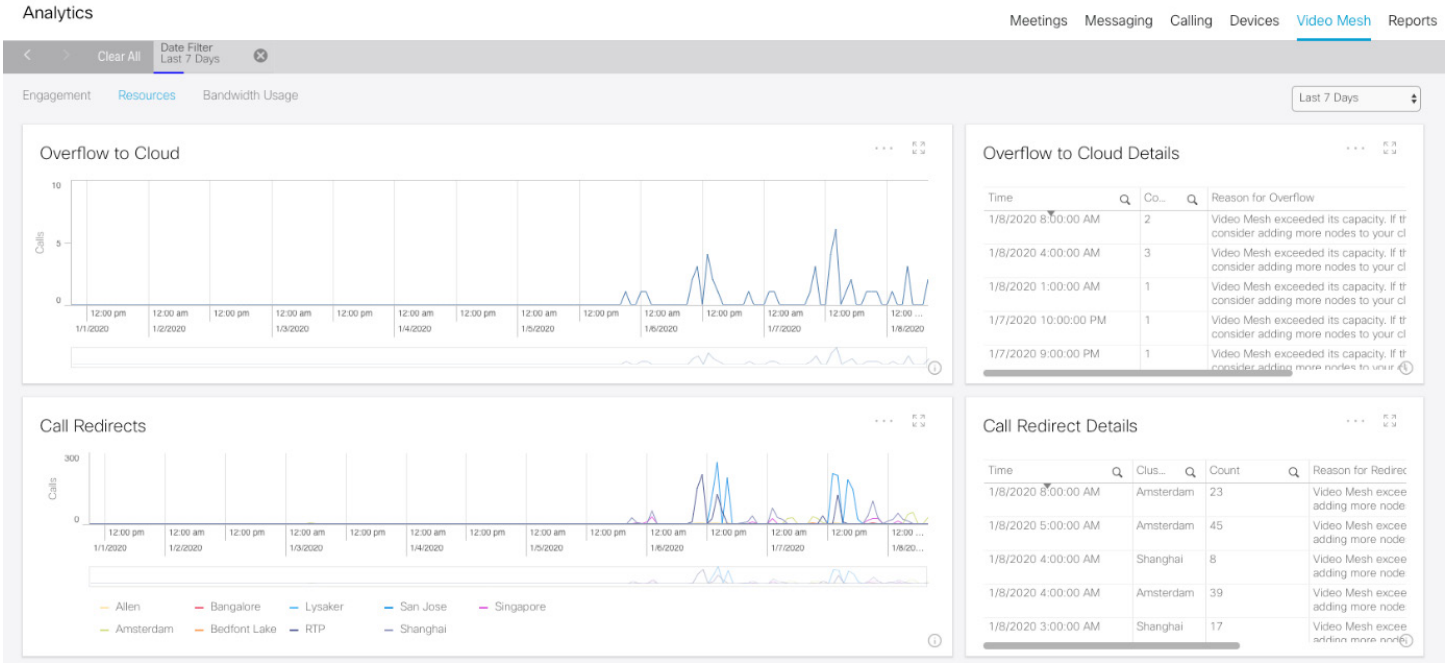
1. Workstation 1 から https://vmn1.dcloud.cisco.com/setup にアクセスします。
2. ログイン情報は、最初に設定した CLI のユーザ名/パスワードセットになります。このラボでは **admin/dCloud123!** です。ログイン情報を入力してログインします。
3. 最初に表示されるページは [概要（Overview）] ページです。このページには、ノードに関する情報とノードの状態および接続テスト機能が表示されます。後でテストコールを行う際に、このページに戻ればノードを超えたコールを確認できます。
4. [ネットワーク（Network）] に移動します。このページでは、ホスト、NTP、ネットワーク設定を更新することもできます。
5. [トラブルシューティング（Troubleshooting）] に移動します。このページでは、シスコにログを送信したり、パケットをキャプチャしたりすることができます。トラブルシューティングに使用できるさまざまなツールもあります。オプションを自由に確認してください。

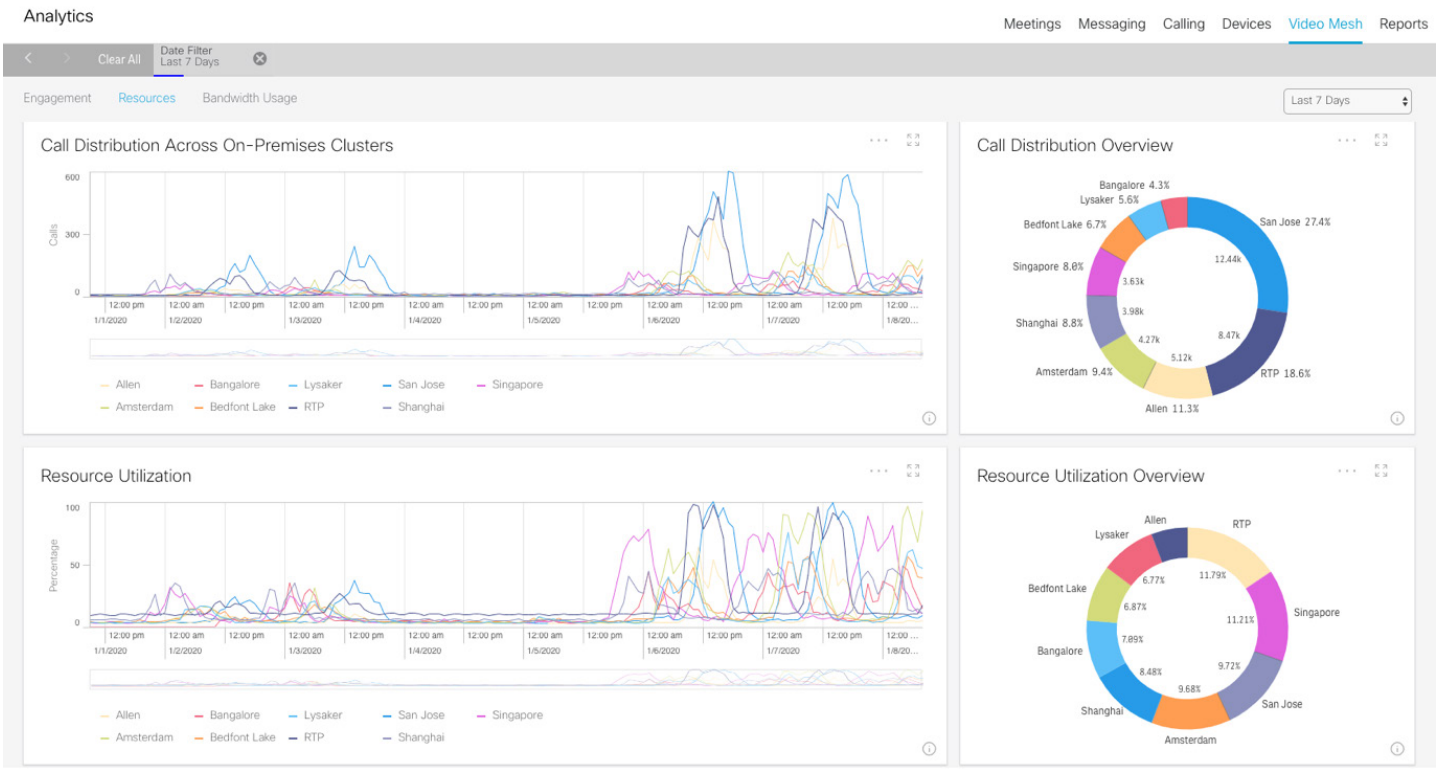
メディアノードで使用率レポートを表示するには、**Control Hub** の [分析（Analytics）] タブに移動します。ページ右上の [Video Mesh] をクリックします。Cisco Webex Control Hub には、キャパシティプランニングとキャパシティレポート用に、組織全体の会議アクティビティのシンプルなスナップショットを作成する機能があります。オーバーフローの発生場所やオーバーフローの量などをすばやく評価できます。それにより管理者は、傾向を分析してオンプレミスにキャパシティの追加が必要かどうかを判断し、必要な場合は、Video Mesh Node の追加を計画できます。

レポートはほぼリアルタイムの約 1 分ごとに更新されます。新しい導入レポートでは、異なるクラスタにあるデバイスの種類が表示されます。残念ながら、dCloud で作成するトライアル組織ではレポートを表示できません。以下に示すのは、レポートのサンプルスクリーンショットです。

Video Mesh Node レポート







Video Mesh に Unified CM SIP トラフィックルーティングを設定する

Video Mesh Node に Cisco Webex Meetings 用 SIP ダイヤルイン/ダイヤルアウトをルーティングするため、SIP トランクを設定します。SIP デバイスは直接接続できないため、Unified CM を設定してオンプレミス SIP デバイスと Video Mesh クラスタ間の関係を確立する必要があります。高い可用性を備え、デバイス障害に対応できる、クラスタ設定を反映したトランク ルーティング ポリシーを作成できます。Unified CM Session Management Edition（SME）を使用している場合、Session Management クラスタ内の Unified CM サーバ間でインバウンドコールとアウトバウンドコールが均等に分散されるよう、Unified CM SME とリーフシステムにトランクを設定します。

通常各サイトには、関連付けられている専用の Unified CM クラスタがあります。各クラスタは、クラスタ間の SIP トランクを介して接続されます。また、Video Mesh Node 向けに、ローカルサイトに対するコールイントランクが設定されます。

障害やオーバーフロー状態に対応できるように設定することもできます。そのような設定をすることで、システムが停止した場合や、Video Mesh クラスタのキャパシティの上限に達した場合に対応できます。クラスタとの間で SIP 会議またはコールを確立できない場合、会議/コールはオーバーフローします。

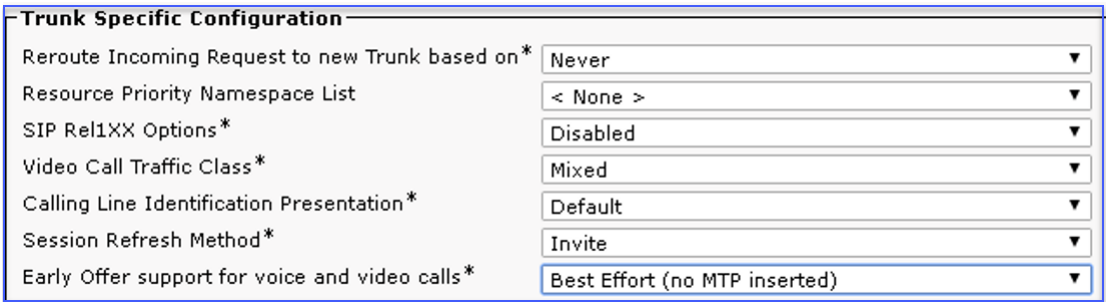
1. Workstation 1（**198.18.1.36 – cholland/dCloud123!**）に戻り、**Chrome** を開きます（開いていない場合）。
2. Unified CM にログインしていない場合は、ホームページから、[コラボレーション管理リンク（Collaboration Admin Links）] > [Cisco Unified Communication Manager] へ移動します。

3. [Cisco Unified Communications Manager] リンクを選択し、**administrator/dCloud123!** でログインします（あらかじめ入力されています）。

まず、新しい SIP プロファイルを作成する必要があります。

4. [デバイス（Device）] > [デバイスの設定（Device Settings）] > [SIPプロファイル（SIP Profile）] の順に移動して、[検索（Find）] をクリックします。
5. リスト内の [Cisco VCS用標準SIPプロファイル（Standard SIP Profile For Cisco VCS）] の横にあるコピーアイコン [ ] をクリックします。
6. 名前に **Video_Mesh** と入力します。
7. [トランク固有の設定（Trunk Specific Configuration）] まで下にスクロールし、[音声コールとビデオコールに対するEarly Offerサポート（Early Offer support for voice and video calls）] を [ベストエフォート（MTPの挿入なし）（Best Effort (no MTP inserted)）] に設定します。

Early Offer



8. [保存（Save）] をクリックします。

次に、SIP セキュリティプロファイルを作成します。

9. [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）] を選択します。
10. [新規追加（Add New）] をクリックします。
11. 名前に **Video_Mesh** と入力します。
12. デフォルト設定のまま [保存（Save）] をクリックします。

次に、Video Mesh Node へのトランクを作成します。

- Unified CM のみの導入の場合、トランクを 1 つだけ追加します。
- SME を導入する際は、Unified CM と SME 間のトランクと、SME と Video Mesh Node 間のトランクをそれぞれ追加します。いずれのトランクにも以下の同じ内容を設定します。

13. [デバイス（Device）] > [トランク（Trunk）] を選択し、[新規追加（Add New）] をクリックします。

14. 次の画面で、[トランクタイプ（Trunk Type）] に [SIPトランク（SIP Trunk）] を選択します。
15. その他はデフォルト値のままにして、[次へ（Next）] をクリックします。
16. 以下の表に従ってパラメータを設定します。

表 20. ハイブリッドサービスのトランク設定

設定対象	設定内容
[デバイス情報（Device Information）] > [デバイス名（Device Name）]	Video_Mesh
[デバイス情報（Device Information）] > [デバイスプール（Device Pool）]	dCloud_DP
[アウトバウンドコール（Outbound calls）] > [発呼側および接続側情報形式（Calling and Connected Party Info Format）]	[接続側でURIおよびDNを配信（可能な場合）（Deliver URI and DN in connected party, if available）]（この設定により ID を混在させることができ、SIP トランクが企業側のディレクトリ URI を Cisco Webex に送信できるようになります）
[SIP情報（SIP information）] > [接続先アドレス（Destination Address）]	198.18.135.21（HMN アドレス、ポートは 5060 のまま）
[SIPトランクセキュリティプロファイル（SIP Trunk Security Profile）]	Video_Mesh
[SIPプロファイル（SIP Profile）]	Video_Mesh

17. [保存（Save）]、[OK]、[リセット（Reset）]、[リセット（Reset）]、[閉じる（Close）] の順にクリックします。

次に、Video Mesh Node へのコール用に新しいルートグループを作成します。

18. [コールルーティング（Call Routing）] > [ルート/ハント（Route/Hunt）] > [ルートグループ（Route Group）] を選択してから、[新規追加（Add New）] をクリックします。
19. 名前に **Video_Mesh_RG** と入力します。
20. [配信アルゴリズム（Distribution Algorithm）] を [トップダウン方式（Top Down）] に変更します。
21. [ルートグループメンバー情報（Route Group Member Information）] セクションで [Video_Mesh] を選択し、[ルートグループに追加（Add to Route Group）] をクリックして追加します。
22. バックアップパスで **SIP_Trunk_To_Exp-C** デバイスを選択し、[ルートグループに追加（Add to Route Group）] をクリックします。

このトランクは、Video Mesh Node ルートが利用できない、またはキャパシティの制限によりクラウドへのオーバーフローが発生した場合に、B2B コールに使用されます。トップダウン方式のアルゴリズムを使用すると、Video Mesh Node が常に最初に使用されます。

23. [選択したデバイス（Selected Devices）] ボックスの先頭に **Video_Mesh** トランクが表示されていることを確認し、[保存（Save）] をクリックします。

次に、Video Mesh Node および Expressway へのコール用に新しいルートリストを作成します。

24. [コールルーティング（Call Routing）] > [ルート/ハント（Route/Hunt）] > [ルートリスト（Route List）] を選択し、[新規追加（Add New）] をクリックします。
25. 名前に **Video_Mesh_RL** と入力します。

26. [Cisco Unified Communications Managerグループ（Cisco Unified Communications Manager Group）] を [デフォルト（Default）] に設定します。
27. [保存（Save）] をクリックします。
28. [ルートリストメンバー情報（Route List Member Information）] セクションで [ルートグループの追加（Add Route Group）] をクリックし、[Video_Mesh_RG-[NON-QSIG]] を選択します。
29. その他の設定はデフォルト値のままにして [保存（Save）] をクリック後、[OK] をクリックします。
30. [保存（Save）] をクリックします。

次に Webex サイト用の SIP ルートパターンを作成します。すべての Webex サイトに一致するデフォルトのパターンを作成します。

31. [コールルーティング（Call Routing）] > [SIPルートパターン（SIP Route Pattern）] を選択し、[新規追加（Add New）] をクリックします。
32. [IPv4パターン（IPv4 Pattern）] では、Webex URL として ***.webex.com** と入力します。
33. [ルートパーティション（Route Partition）] で [Base_PT] を選択します。
34. [SIPトランク/ルートリスト（SIP Trunk/Route List）] で、[Video_Mesh_RL] を選択します。
35. [保存（Save）] をクリックします。

Webex 機能の有効化

この後のラボで使用する、Charles の Webex 機能を有効にします（Webex Edge Audio シナリオがすでに終了している場合はスキップできます）。

1. Control Hub に戻って、必要に応じて Charles の以下のログイン情報でログインし直します。
   - ユーザ名：**cholland@cbXXX.dc-YY.com**
   - パスワード：**dCloud123!**
2. [ユーザ（Users）] をクリックします。
3. リストから **Charles Holland** を選択します。
4. [サービス（Services）] で [会議（Meeting）] をクリックします。
5. 会議サイトの **URL** をクリックします。
6. [ユーザ権限（User Privileges）] をクリックします。
7. [パーソナルルーム（Personal Room）] と [ビデオシステムから会議に参加（Join meetings from video systems）] がオンになっていることを確認します（なっていなければオンにし、[保存] をクリックします）。

Video Mesh Node で Webex Collaboration Meeting Room を利用した会議のホスト

以前、Webex サイト（*.webex.com）を示す SIP ルートパターンを Unified CM に作成しました。Collaboration Meeting Room（CMR）へのコールを Video Mesh Node でホストするには、Webex サイトに対する共通設定の CMR セクションで設定を変更し、Video Mesh Node が Webex に接続できるようにする必要があります。デフォルトの設定では、CMR 会議はクラウドでホストされ、常に Expressway を経由してルーティングされます。

1. Control Hub で [サービス（Services）] をクリックします。
2. [会議（Meeting）] で [サイト（Sites）] をクリックします。
3. リストからサイトを選択し、ポップアップウィンドウで [サイトを構成する（Configure Site）] をクリックします。
4. [共通設定（Common Settings）] で、[Collaboration Meeting Rooms (CMR)] をクリックします。
5. [メディアリソースタイプ（Media Resource Type）] ページの上部で [ビデオメッシュ（Video Mesh）] を選択し、右下の [更新（Update）] をクリックします。

注：更新をクリックした後に設定が適用されるまで約 30 分かかります。また、以前追加した Video Mesh Node のサービスに対する更新がすべて完了していることを確認する必要もあります。さらに、Video Mesh カードの下部でステータスが [運用中（Operational）] になっていることの確認も必要です。

これで、Video Mesh Node を使用してオンプレミスのユーザが Webex Meetings に接続するように設定されました。

Video Mesh Node を使用したオンプレミスデバイスのテスト

オンプレミスのデバイスが Video Mesh Node を使用して Webex Meetings に接続する設定をラボで検証する一番簡単な方法は、ワークステーションで Jabber を使用して Webex サイトにコールし、コールが Expressway を通過するかどうかを確認することです。

1. **Workstation 1** で **Cisco Jabber** を開き、以下のログイン情報を使用してログインします（ログインしていない場合）。
   - 電子メール：**cholland@cbXXX.dc-YY.com**
   - ユーザ名：**cholland**
   - パスワード：**dCloud123!**
2. 新しい Chrome タブを開き、[コラボレーション管理リンク（Collaboration Admin Links）] > [Cisco Expressway-C] に移動します（コネクタホストではありません）。
3. **admin/dCloud123!** でログインします（あらかじめ入力されています）。
4. [設定（Configuration）] > [ゾーン（Zones）] > [ゾーン（Zones）] に移動します。

コールが Expressway を通過するのをモニタリングします。コールが Expressway を通過している場合は、**Traversal Client for B2B Video** および **UCM Neighbor for B2B** ゾーンのコール数が **1** になるはずです。この場合、コールは Video Mesh Node でホストされていません。現在は利用中のコールがないため、数は **0** です。次に、Jabber で Webex にコールします。

5. Jabber を開き、meet@cbXXXYY.webex.com にコールします。

注：Webex Meetings サイトの URL が機能しない場合は、Control Hub で URL を確認してください。[サービス（Services）] > [会議（Meeting）] > [サイト（Sites）] > [サイト名（Site Name）] の順に移動します。使用可能なその他の URL には、https://cbXXXYYa.webex.com、https://cbXXXYYb.webex.com、https://cbXXXYYc.webex.com があります。

6. 正常に接続された場合は、「会議番号と # を入力してください（Enter the meeting number, followed by #）」というメッセージが表示されます。

7. コールを接続したまま、[Expressway-Cゾーン（Expressway-C zones）] ページに戻り、更新します。

コール数が 0 のままの場合、Jabber クライアントはコールのルーティングに Video Mesh Node を使用しています。ただし、コール数が 1 になった場合は、コールのルーティングに Expressway が使用されているため、望ましい結果ではありません。これは、クラウドからの接続が反映されていないか、正しく設定されていないことを意味します。前述のように、設定が反映されるまでに約 30 分かかることがあります。また、以前追加した Video Mesh Node をアップグレードしている場合は、Video Mesh Node が完全に動作するまで Expressway ルートが使用されます。そのため、先にラボの残りの部分を続けて、後でテストを実施します。

Video Mesh Node（https://vmn1.dcloud.cisco.com/setup/（**admin/dCloud123!**））に直接アクセスして、[概要（Overview）] ページでノードを通過しているコール数を確認することもできます。

8. コールが自動的に終了しない場合は、コールを終了します。また、Jabber も終了します。

シナリオ 7. Webex Calling

エンタープライズレベルのクラウドコール、モビリティ、PBX 機能を、メッセージング用 Cisco Webex Teams、会議用 Webex Meetings、ソフトクライアントまたはシスコ電話機の通話機能とともに利用できれば素晴らしいことではありませんか。Cisco Webex Calling を利用すれば実現できます。また、100 人以上のユーザがいて、オンプレミスの既存の PBX インフラストラクチャを使用しているお客様がクラウドにスムーズに移行できます。

Cisco Webex Calling の特長：

- テレフォニーユーザと共通エリアのためのコーリングサブスクリプション
- 信頼できる地域のサービスプロバイダーが提供する安全で信頼性の高いクラウドサービス
- モバイルワーカー向けの包括的な通話機能を提供する、デスクトップおよびモバイルデバイス用 Cisco Webex Calling アプリ
- すべてのユーザに Webex Teamsへのアクセスを提供。優れたユニファイド コミュニケーションによるチームコラボレーションを強化
- エンタープライズユーザが求めるプレミアムなミーティング体験を提供する Cisco Webex Meetings（オプション）
- PSTN 接続用ローカルゲートウェイ
- 付加価値リセラー（VAR）チャネルを通じて販売
- Webex ブランド
- PSTN 接続および利用料は別途必要
- Cisco MPP 電話機のみサポート
- Webex Teams クライアントからの発呼

その他の情報および Webex Calling の設定に関する詳細ガイドについては、https://help.webex.com/ja_jp/32gfts/Webex-Calling-Configuration-Workflow のヘルプ記事をご覧ください。

電話番号の追加とロケーションへの割り当て

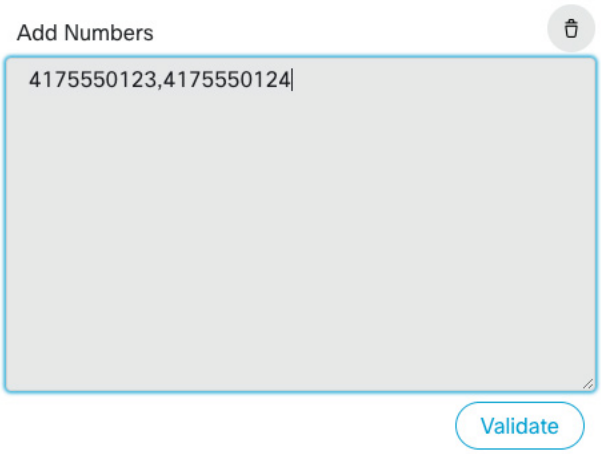
1. Workstation 1 の Webex Control Hub（https://admin.webex.com）で、左側のメニューから [サービス（Services）] を選択します（まだログインしていない場合は、ユーザ名：**cholland@cbXXX.dc-YY.com**/パスワード：**dCloud123!** でログインします）。
2. [コール（Calling）] カードで [番号（Numbers）] をクリックします。

現時点では、ラボ用の電話番号（TN）は設定されていません。各ロケーションでコールするためにメインの電話番号が 1 つ必要で、音声ポータル用にもう 1 つ必要です。今回はラボのため実際にかけられる公衆の電話番号を持っていないため、2 つの仮の番号を設定して進めます。実際にはプロバイダーから本当の電話番号を取得し、組織に追加します。

3. [番号の追加（Add Number Numbers）] をクリックします。
4. [ロケーション（Location）] ドロップダウンメニューから [dCloud] を選択します。

ラボのお客様の全組織は米国（US）で作成されているため、次の手順では、10 桁の仮の米国用番号を 2 つ追加する必要があります。

5. [番号の追加（Add Numbers）] ボックスに **417555** から始まる 2 つの一意の番号を追加します（カンマで区切る）。末尾には 4 つのランダムな数字を入力します。たとえば、**4175550123** と **4175550124** です。
6. [番号の追加（Add number）] ボックスに番号を追加したら、[検証（Validate）] をクリックします。



7. 正しければ、番号が [検証済み番号（Validated Numbers）] ボックスに追加され、次の手順に進むことができます。画面の下部に ⊗ Invalid phone numbers found または ⊗ Unavailable phone numbers found のエラーメッセージが表示されたら、[検証済み番号（Validated Numbers）] ボックスに番号が 2 つ表示されるまで、米国用の別の番号（10 桁の仮の番号）を選択してください。

8. [保存（Save）] をクリックします。
9. ページの上部の [ロケーション（Locations）] をクリックします。
10. **dCloud** のロケーションを選択します。
11. ポップアップウィンドウで [メイン番号（Main Number）] 用のドロップダウンメニューを選択し、前の手順で作成した仮の番号のどちらかを選択します。
12. [ボイスメール番号（Voicemail Number）] 用にもう 1 つの仮の番号を選択します。
13. [保存（Save）] をクリックします。

Webex Calling を Taylor と Rebekah に設定

1. 左側のメニューから [ユーザ（Users）] を選択します。
2. ユーザリストから [Rebekah] を選択し、[編集（Edit）] をクリックします。
3. [Webex Calling] のチェックボックスをオンにして、[エンタープライズ（Enterprise）] オプションボタンを選択します。[次へ（Next）] をクリックします。
4. [場所（Location）] で **dCloud** を選択し、[電話番号（Phone Number）] は [なし（None）] のまま、[内線番号（Extension）] に **86022** と入力します。

注：ラボでユーザと機能の確認に必要なのは内線番号のみです。[電話番号（Phone Number）] オプションは、ユーザの電話機に実際の PSTN 番号を割り当てる際に使用します。ラボでは実際に PSTN サービスを設定することはありません。

5. [完了（Finish）] をクリックします。
6. ポップアップウィンドウで [設定（Settings）] まで下にスクロールし、[コール動作（Calling Behavior）] をクリックします。

Teams ではさまざまな方法でコールできます。デフォルトでは、[設定（Settings）] ページに表示されている組織の設定が適用されます。Rebekah には [Webex Teamsでコール（Calling in Webex Teams）] が設定されていることを確認します。この設定は、組織に対する現時点での設定です。**Webex Calling** サービスを追加して電話番号を設定した際に、このオプションがユーザに対して自動的に選択されています。これはラボで選択する内容のため、変更は必要ありません。

7. Taylor のユーザアカウントを編集し、**Webex Calling Enterprise** サービスを追加して、[内線番号（Extension）] に **86021** を設定します。
8. 後でテストするために、**Webex Calling Enterprise** 用のユーザをもう 1 人設定します。[内線番号（Extension）] には **86024** を設定します。このユーザは、コール機能をテストするためにシステムに発呼します。ラボガイドのこの後のセクションで設定する Room デバイスを使用することもできます。

Global Discovery Service（GDS）を使用して Taylor の Multiplatform Phone（MPP）を設定

Cisco Global Discovery Service（GDS）で生成された 16 桁のアクティベーションコードと Webex Calling プラットフォームを使用して、関連する Webex プラットフォームとデバイスをオンボーディングしてプロビジョニングします。コードは、ユーザ/管理者に対して生成された際に MPP 電話機に設定されます。MPP 電話機は GDS と通信し、電話機をホスティング プラットフォームにリダイレクトします。また、Webex プラットフォームと通信し、アクティベーションコードを使用してプラットフォームに対する認証を行います。認証が成功すると、MPP MAC アドレスがプラットフォームに保存され、電話機にプロビジョニングサーバの場所が設定されます。電話機が再起動し、デバイス管理からユーザ設定がダウンロードされます。

この機能は、次の Cisco MPP デバイスでサポートされています。

- 6821、6841、6851

- 7811、7821、7832、7841、7861
- 8811、8832、8841、8845、8851、8861、8865

MPP 電話機がある場合は、利用する他の電話機と合わせて、以下の指示に従って登録してください。MPP 電話機がない場合は、このラボでは Webex Teams アプリを使用します。MPP 電話機がなく Webex Teams を使用してコールする場合は、次のセクションにスキップします。

1. **Control Hub** で [デバイス（Devices）] をクリックします。
2. [デバイスの追加（Add Device）] をクリックします。
3. [既存のユーザ（Existing User）] を選択し、[次へ（Next）] をクリックします。
4. **Taylor Bard** を検索してリストから選択し、[次へ（Next）] をクリックします。
5. ドロップダウンメニューから**デバイスタイプ**を選択します。
6. [アクティベーションコードを使用（By Activation Code）] を選択した状態で [次へ（Next）] をクリックします。

注：使用している MPP 電話機が初期設定状態でない場合は、ここでリセットします。電話機が初期設定状態で、電源がオンになっている場合は、電話機を再起動して登録プロセスを再度実施します。

7. 初期設定へのリセット後に電話機が起動したら、電話機にアクティベーションコードを入力し、[続行（Continue）] ボタンを押します。

数分後に電話機が再起動して登録されます。登録後、デバイスが Control Hub のデバイスページに表示されるまで数分かかる場合があります。

注：この時点の Control Hub では、電話機のステータスは常に [ステータス機能利用不可（Status Unavailable）] と示されます。電話機のステータス機能はまもなくリリースされる予定ですが、このガイドの執筆時点ではまだリリースされていません。

Room デバイスに Webex Calling を設定

Room デバイスに Webex Calling の電話番号を割り当てることができます。ユーザの場合と同様に、ラボ組織にはクラウド接続 PSTN サービスプロバイダーが設定されていないため、内線番号を割り当てます。

1. **Control Hub** で [場所（Places）] をクリックします。

注：次の手順では、すでに Control Hub にデバイスが追加されていることを前提としています。Control Hub にデバイスが追加されていない場合は、このガイドの「**Room デバイスの追加**」セクションの手順に従って、新しいデバイスを追加します。デバイスが、Webex Edge for Devices シナリオの Unified CM に登録されたままの場合は、最初に作成した場所を削除し、新しい場所を作成してクラウドに登録します。UCM に登録されている場合は、デバイスを初期設定にリセットし、クラウドに登録し直す必要があります。デバイスを登録したら、次の手順に戻ります。手順を確認するだけの場合は、仮のデバイスを追加することもできます。

2. デバイスを選択し、ポップアップウィンドウで [編集（Edit）] をクリックします。

3. [Cisco Webex Calling] オプションボタンを選択し、[次へ（Next）] をクリックします。
4. 内線番号 **86023** を入力し、[保存（Save）] をクリックします。

これで、Room デバイスから他のユーザの内線番号にダイヤルできるようになります。

Webex Calling にソフトウェアクライアントを使用する

他のユーザについては、電話の発着信に Webex Teams を使用します（Taylor 用の MPP 電話機がない場合は、Taylor も Webex Teams を使用します）。

1. 自分のコンピュータまたはモバイルデバイスで他のいずれかのユーザを使用して Webex Teams を開き、ログインします。たとえば、Rebekah のログイン情報は次のようになります。
   - ユーザ名：**rbarretta@cbXXX.dc-YY.com**
   - パスワード：**dCloud123!**

コール機能の設定

クライアントをインストールしてログインしたので、コーリング機能を設定します。最初にすべての設定を行い、最後にまとめてテストします。

新しいコール機能の追加

次に、コール機能を作成します。コール機能をシステムにプロビジョニングするには時間がかかるため、最初に必要な機能をすべて追加してから、後でまとめて設定を行います。

1. Control Hub で [サービス（Services）] に移動し、[コール（Calling）] カードの [機能（Features）] リンクをクリックします
2. [新機能（New Feature）] をクリックし、[自動音声応答（Auto Attendant）] を選択します。
3. [場所（Location）] にドロップダウンメニューから [dCloud] を選択します。
4. [保存（Save）] をクリックします。
5. ポップアップ画面で [新機能（New Feature）] をクリック後、[ハントグループ（Hunt Group）] をクリックします。
6. [場所（Location）]にドロップダウンメニューから [dCloud] を選択します。
7. [保存（Save）] をクリックします。
8. [新機能（New Feature）] をクリック後、[ページンググループ（Paging Group）] をクリックします。
9. [場所（Location）] に [dCloud] を選択します。
10. [保存（Save）] をクリックします。

11. [新機能（New Feature）] をクリックし、[コールキュー（Call Queue）] をクリックします。

12. [場所（Location）] に [dCloud] を選択します。

13. [保存（Save）] をクリックします。

自動音声応答、**コールキュー**、**ハントグループ**、**ページンググループ**の 4 つの機能が追加されました。

コール機能の設定

すべての機能がプロビジョニングされるまでの間に、先に進んでいくつかの機能を設定できます。最初はハントグループです。

ハントグループの設定

次に、すでに追加しているハントグループを設定します。次のシナリオに基づいてハントグループを設定します。

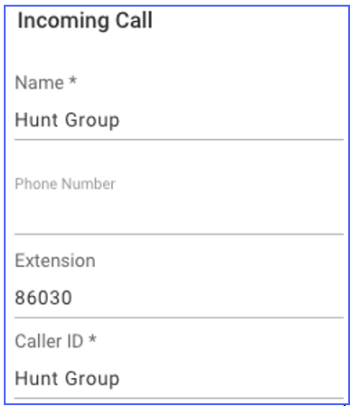
- セールスチームは、かかってきた電話が順番にルーティングされることを希望しています。つまり、1 台の電話が鳴っても応答されない場合、リストに従って次のユーザの電話が鳴るようにしたいということです。
- サポートチームは、最初に対応できるエージェントが電話に応答できるように、すべてのエージェントの電話を一斉に鳴らしてほしいと考えています。

1. [ハントグループ（Hunt Group）] カードで、省略記号 [･･･] をクリックし、[編集（Edit）] をクリックします。

Webex Calling Admin ポータルで新しいタブが開きます。作成した機能ごとに開きます。ここからは、Control Hub に移動して [編集（Edit）] をクリックするのではなく、Webex Calling ポータル内ですべて設定します。

2. **Hunt Group** など、ハントグループに関連する名前を入力します。
3. [電話番号（Phone Number）] で、ドロップダウンリストから [（未指定） ((empty))] を選択します。
4. [内線番号（Extension）] に **86030** を入力します。
5. [発信者ID（Caller ID）] に名前を入力します。

ハントグループの設定



6. ページの右下で [保存（Save）] をクリックします。
7. ページが更新されたら、左側のメニューから [コールルーティング（Call Routing）] をクリックします。
8. [個別着信（One at a time）] オプションボタンを選択します。デフォルトでは [順次着信（Top Down）] が選択されています。このオプションでは、[電話（Phones）] セクションで設定された割り当て順に一度に 1 ユーザずつ呼び出されます。常に同じユーザから始まり、同じ順序で呼び出されます。[割り当て済み（Assigned）] リストの一番上に設定されているユーザが最初に呼び出され、その後はリストされている順序で呼び出されます。コールルーティングの種類と各種類の詳細については、「Calling Admin ポータル：ハントグループを変更する」ページを参照してください。このページにはハントグループの概要も示され、ラボで説明していない設定を含め、設定の詳細が記載されています。
9. [設定された回数呼び出したら先に進む（Advance after a set number of rings）] チェックボックスをオンにし、呼出回数を **3** 回に設定します。
10. ページの右下で [保存（Save）] をクリックします。
11. ページが更新されたら、左側のメニューから [電話（Phones）] をクリックします。
12. [検索と割り当て（Find and Assign）] 内でクリックして検索し、**Taylor Bard** および **Rebekah Barretta** を選択します。
13. ページの右下で [保存（Save）] をクリックします。
14. ページが更新されたら、ページの右上にある [☒] をクリックして、ハントグループの設定を閉じます。

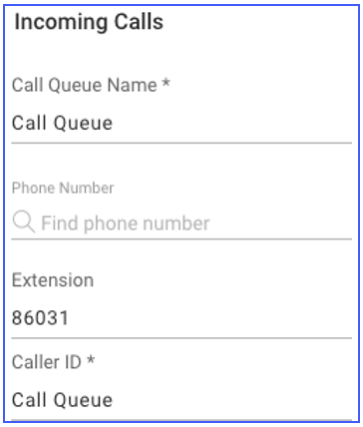
コールキューの設定

コールキューは、電話がかかってきた際に割り当てられたすべてのユーザ（エージェント）が応答できない場合に、クラウドでコールを一時的に保留します。キューに入ったコールは、ユーザ（エージェント）が対応可能になり次第、そのユーザ（エージェント）にルーティングされます。各コールキューにはリード番号が割り当てられます。これは、外部の発信者がコールキューに割り当てられたユーザにアクセスするための電話番号です。コールキューには内線番号も割り当てられ、この番号を内部でダイヤルしてもコールキューに割り当てられているユーザにアクセスできます。

ラボでは、基本のコールキューを設定します。コールキューの詳細やさらに高度な設定については、こちらをクリックしてください。

1. Webex Calling ポータルで [アドバンスドサービス（Advanced Services）] をクリックします。
2. [コールルーティング（Call Routing）] リストで [コールキュー（Call Queues）] をクリックします。
3. Control Hub で以前設定した 1 つのコールキューに対して [割り当て（Assign）] をクリックします。
4. コールキューに **Call Queue** などのキューに関連した名前を入力します。
5. [電話番号（Phone Number）] で、ドロップダウンリストから [（未指定）（(empty)）] を選択します。
6. [内線番号（Extension）] に **86031** を入力します。
7. [発信者ID（Caller ID）] に名前を入力します。

コールキューの設定



8. ページの右下で [保存（Save）] をクリックします。
9. ページが更新されたら、左側のメニューから [キュー設定（Queue Settings）] をクリックします。
10. [応答可能なエージェントにコールが転送されたときに発信者に呼出音を鳴らす（Play ringing tone to callers when their call is sent to an available agent）] チェックボックスをオンにします。
11. [キュー待機時間が過ぎたらコールをオーバーフローとしてマークする（Mark calls as overflow after queue wait time）] のチェックボックスをオンにし、入力欄に **80** を入力します。
12. [詳細設定（Advanced Settings）] を展開します。
13. [ウェルカムメッセージは必須（Welcome message is mandatory）] チェックボックスをオンにします。
14. [キューに入っているコールの推定待ち時間メッセージ（Estimated Wait Message for Queued Calls）] をオンに切り替えます。
15. [キューの位置を通知（Announce Queue Position）] オプションボタンを選択します。
16. [保留音（Hold Music）] をオンに切り替えます。

17. ページの右下で [保存（Save）] をクリックします。
18. ページが更新されたら、左側のメニューから [コールルーティング（Call Routing）] をクリックします。
19. [コールルーティング（Call Routing）] で、[個別着信（One at a time）] を選択します。
20. ページの右下で [保存（Save）] をクリックします。

次に、キューに追加するライセンスとエージェントを割り当てる必要があります。

21. ページが更新されたら、左側のメニューから [エージェント（Agents）] をクリックします。
22. [検索と割り当て（Find and Assign）] 内でクリックして検索し、**Taylor Bard** および **Rebekah Barretta** を選択します。
23. ページの右下で [保存（Save）] をクリックします。
24. ページが更新されたら、ページの右上にある [☒] をクリックして、コールキューを閉じます。

自動音声応答（Auto Attendant）の設定

自動音声応答によって電話に応答し、発信者に対応します。グリーティングメッセージの追加、メニューの設定、コールのルーティング（留守番電話サービス、ハントグループ、ボイスメールボックス、別のユーザへのルーティング）が可能です。24 時間のスケジュールを作成することも、営業時間内または時間外にそれぞれ別のオプションを指定することもできます。発信者 ID 属性に基づいてコールをルーティングする VIP リストを作成したり、特定の市外局番からのコールを異なる方法で処理したりすることもできます。

1. Webex Calling ポータルで [アドバンスドサービス（Advanced Services）] をクリックします。
2. [コールルーティング（Call Routing）] リストで [自動音声応答（Auto Attendants）] をクリックします。
3. 自動音声応答の [割り当て（Assign）] をクリックします。
4. [アテンダント名（Attendant Name）] に名前を入力します。
5. [内線番号（Extension）] に **86020** を入力します。
6. ページの右下で [保存（Save）] をクリックします。
7. ページが更新されたら、左側のメニューから [スケジュール作成（Schedule）] をクリックします。
8. 次の画面で、[タイムスケジュールを編集（Edit Time Schedule）] をクリックします。
9. [スケジュールイベント（Schedule Events）] では、各曜日がイベント名で表されます。日曜日を表す 1 から始まり、2 は月曜日と続きます。ラボを実施する曜日に対応するイベントの [編集（Edit）] をクリックします。たとえば、木曜日にラボを実施する場合は、[イベント5（event 5）] の [編集（Edit）] をクリックします。
10. 正しいイベントを選択したことを確認するには、[定期実行（Recurrence）] をクリックします。[定期実施日（Recur On）] で選択した曜日が表示されます。
11. [イベント（Events）] をクリックします。
12. 曜日を示すように [名前（Name）] を変更して（日曜、月曜、火曜など）、後で確認しやすくします。
13. ラボでは、[終日イベント（All Day Event）] チェックボックスをオンにします。これで、後からテストするときに、コールの時間に関係なく実施できます。

14. [保存（Save）] をクリックします。

他の曜日にラボの使用を計画している場合などを含め、他の曜日のイベントを自由に編集して構いません。

15. 曜日を編集したら [保存する（Save）] をクリックします。
16. [スケジュール（Schedule）] ページの右下にある [保存（Save）] をクリックします。
17. ページが更新されたら、左側のメニューから [メニュー（Menu）] をクリックします。
18. 各番号のドロップダウンメニューを使用して、以下の表にある [営業時間（Business Hours）] のパラメータを設定します。

表 21. 営業時間用の自動音声応答設定

設定対象	設定内容
0	メニューの終了
1	[内線番号でダイヤル（Dial By Extension）]
2	[名前でダイヤル（Dial By Name）]
3	[音声プロンプトなしで内線に転送（Transfer To Extension Without Prompt）] [番号（Number）]：**86021** [説明（Description）]：**Taylor にダイヤル**
4（[さらに表示（Show More）] をクリックして表示）	[音声プロンプトなしで内線に転送（Transfer To Extension Without Prompt）] [番号（Number）]：**86030** [説明（Description）]：**ハントグループ**
5	[音声プロンプトなしで内線に転送（Transfer To Extension Without Prompt）] [番号（Number）]：**86031** [説明（Description）]：**コールキュー**

営業時間用の自動音声応答設定

後で設定した番号をテストしますが、必要に応じて他の番号を自由に設定できます。各オプションの説明やカスタム グリーティング メッセージの設定方法などの詳細については、こちらをクリックしてください。

19. ページの右下で [保存（Save）] をクリックします。
20. ページが更新されたら、ページの右上にある [☒] をクリックして、自動音声応答の設定を閉じます。

次に、自動音声応答の音声プロンプトを録音できるように、音声ポータルのパスワードを設定します。

21. [アドバンスドサービス（Advanced Services）] をクリックし、[サイトパッケージの設定（Site Package Settings）] タブに移動します。
22. リストで [音声ポータル（Voice Portals）] をクリックします。
23. [音声ポータル（Voice Portals）] ページに表示された番号に対して、[アクション（Actions）] > [サービスの編集（Edit Service）] をクリックします。
24. 内線番号に **86032** を入力します。
25. 新しいパスコードとして 1357 と入力し、新しいパスコードを確認します。
26. [保存（Save）] をクリックします。

27. ページが更新されたら、ページの右上にある [✉] をクリックして、音声ポータルの設定を閉じます。

これで、電話をかけて、自動音声応答用の音声プロンプトを録音できるようになります。

28. 自分の電話から**音声ポータル**の内線番号（**86032**）にダイヤルします。
29. 音声プロンプトに従って [*] ボタンを押し、**パスコード**を入力します。
30. メールボックス ID については、**音声ポータル**の内線番号（**86032**）を入力し、続けてシャープ [#] を押します。
31. パスコード **1357** を入力し、[#] を押します。
32. **1** を押して**自動音声応答**グリーティングメッセージを変更します。
33. **1** を押して、営業時間用のグリーティングメッセージを変更します。
34. **1** を押してグリーティングメッセージを変更します。
35. 会社に電話をかけてきた人への挨拶として新しいグリーティングメッセージを録音し、上記で設定したオプションを示します。録音が終了したら、**#** を押します。
36. 録音後、**2** を押して録音したグリーティングメッセージを聞くか、**1** を押して録音をやり直します。
37. 自動音声応答のグリーティングメッセージを作成できたら電話を切ります。

グループコールピックアップ（Group Call Pickup）の設定

グループコールピックアップを使用すると、ユーザは、ピックアップグループ内のユーザにかかってきた電話に応答できます。ピックアップグループは、グループの管理者が定義したサイト内のユーザで構成され、グループコールピックアップ機能が適用されます。グループコールピックアップ機能を使用するには、コールピックアップグループを追加、変更、削除したり、特定のユーザをそのピックアップグループに割り当てたりする必要があります。

コールピックアップサービスを使用するには、次の条件が満たされている必要があります。

- ユーザは、1 つのコールピックアップグループにのみ割り当てることができます。
- コールピックアップグループには、同じサイトのユーザのみ割り当てることができます。
- 1 つのサイトに複数のコールピックアップグループを設定できます。
- コールピックアップグループ名は一意である必要があります。
- ユーザをコールピックアップグループに割り当てると、そのユーザに対して有効になっている Barge-in 制限が解除されます。

1. Webex Calling ポータルで [アドバンスドサービス（Advanced Services）] をクリックします。
2. [コールルーティング（Call Routing）] タブで [コールピックアップ（Call Pickup）] をクリックします。
3. ポップアップ画面で [dCloud] の場所を選択し、[選択（Select）] をクリックします。
4. [追加（Add）] をクリックします。

5. [グループ名（Group Name）] を入力し、[保存（Save）] をクリックします。
6. ページが更新されたら、[選択可能（Available）] セクションで、**Taylor** と **Rebekah** のチェックボックスをオンにし、右矢印 [] をクリックして [割り当て済み（Assigned）] に移動します。
7. [保存（Save）] をクリックします。

コールパーク（Call Park）の設定

コールパーク機能を使用すると、定義されたグループユーザが他のメンバーに対してコールを一旦保留（パーク）することができます。グループの他のメンバーは、保留されたコールを自分の電話機でとることができます。

開始前に把握しておくべき事項：

- ユーザは、1 つのコールパークグループにのみ割り当てることができます。
- コールパークグループには、同じサイトのユーザのみ含めることができます。
- 1 つのサイトに複数のコールパークグループを設定できます。
- コールパークグループ名は一意である必要があります。

1. Webex Calling ポータルで [アドバンスドサービス（Advanced Services）] をクリックします。
2. [コールルーティング（Call Routing）] で [コールパーク（Call Park）] をクリックします。
3. [追加（Add）] をクリックします。
4. [グループ名（Group Name）] を入力し、[保存（Save）] をクリックします。
5. ページが更新されたら、[選択可能（Available）] セクションで、**Taylor** と **Rebekah** のチェックボックスをオンにし、**下矢印** [] をクリックして [割り当て済み（Assigned）] に移動します。
6. [保存（Save）] をクリックします。

ページの上部に [グローバル設定（Global Settings）] ボタンがあります。このボタンを利用すると、登録されているすべてのコールパークグループを設定できます。

ページンググループの設定

グループページングサービスを使用すると、ユーザは電話番号または内線番号にダイヤルして、最大 75 のターゲットユーザで構成されるグループに一方向の通話（放送）を行うことができます。グループページングサービスは、割り当てられたすべてのターゲットへの片方向同時通話（放送）ができるサービスです。システムでページングの準備が整っていることを発信者に通知する機能もあります。放送後、発信者が電話を切ればページングが終了します。

1. Webex Calling ポータルで [アドバンスドサービス（Advanced Services）] をクリックします。

2. [生産性向上サービス（Productivity Services）] タブで [グループページング（Group Paging）] をクリックします。
3. Control Hub ですでに作成してあるページンググループの横の [編集（Edit）] をクリックします。
4. ページンググループに**名前**を付けます。
5. [内線番号（Extension）] に **86033** を入力します。
6. ページの右側の [その他のオプション（More Options）] で [ページング先（Paging Targets）] をクリックします。
7. [選択可能（Available）] セクションで、**Taylor** と **Rebekah** のボックスをオンにし、**下矢印** [] をクリックして [割り当て済み（Assigned）] に移動します。
8. ページの左側で、[発信者（Originators）] をクリックします。
9. ページングの対象者と同じように、ユーザを [割り当て済み（Assigned）] ボックスに移動します。割り当てられたユーザのみがページングを開始できます。
10. ページの右下で [保存（Save）] をクリックします。
11. メインのページンググループのページで、右下の [保存（Save）] をクリックします。

コール機能のテスト

これでコーリング機能がすべて設定できたので、テストします。

注：Webex Calling 機能をテストするには、Webex Calling のテストユーザを設定する必要があります。このセクションでは **Taylor** と **Rebekah** を利用します。

Taylor に割り当てた MPP 電話機を用いるか、Taylor のアカウントで Webex Teams にログインします。Rebekah も Webex Teams クライアントにログインします。前述したように、Taylor と Rebekah はすべてのコーリング機能に対して設定されているため、すべてのコールを開始するには、別のユーザを設定して Webex Teams クライアントにログインするのが最適です。それができない場合は、Taylor または Rebekah のいずれかでコールを開始するようにします。**以下のテストはすべて、3 人目のユーザがコールし、Taylor と Rebekah が応答することを前提にしています。**

自動音声応答、ハントグループ、コールキューのテスト

自動音声応答を設定したときに、グリーティングメッセージを録音し、オプションを設定しました。これらのオプションは、次の表のパラメータを使用して設定したものです。

表 22. 営業時間用の自動音声応答設定

設定対象	設定内容
0	[未使用（Not Used）]
1	[内線番号でダイヤル（Dial By Extension）]

2	[名前でダイヤル（Dial By Name）]
3	[Taylorに直接ダイヤルする（Dial Taylor directly）]
4	[TaylorとRebekahに着信するハントグループに転送する（Transfer to Hunt Group which Taylor and Rebekah are called）]
5	[TaylorとRebekahに着信するコールキューに転送する（Transfer to Call Queue which Taylor and Rebekah are called）]

これらの機能をすべてテストするには、3 人のユーザが必要です。ハントグループとコールキューに Taylor と Rebekah を設定し、電話をかける 3 人目のユーザが両方のユーザへのルーティングをテストできるようにしました。

1. 3 人目のユーザで自動音声応答の内線番号（**86020**）にダイヤルします。
2. **オプション 1** をテストし、Taylor または Rebekah の内線番号を入力します。コールは指定した内線番号に転送されます。
3. **オプション 2** をテストし、キーパッドを使用して Taylor または Rebekah の名前または姓を入力します。最初の 3 文字を入力するとコールが転送されます。コールに応答します。拒否すると、コールはボイスメールに転送されます。
4. **オプション 3** をテストします。Taylor の電話が鳴ります。
5. **オプション 4** をテストします。Taylor または Rebekah（リストで先に記載されているユーザ）の MPP 電話機またはクライアントアプリが鳴り、コールを拒否すると、コールがリストの次のユーザに転送されることを確認します。
6. **オプション 5** をテストします。次の点に注意してください。
   - Taylor と Rebekah のどちらも応答できない状態の場合は、次に応答可能なエージェントを待つように伝える音声プロンプトが再生されます。またこの時、キュー内の自分の順番も通知されます。
   - Taylor または Rebekah が応答可能な場合、MPP 電話機またはクライアントアプリが鳴ります。
   - 着信を拒否すると、コールは他のエージェントに転送されます。
   - 着信に応答せずに、呼出音が鳴ったままにしておくと、設定したタイマーに基づいて発信者に音声プロンプトが流れます。
   - 設定した時間が過ぎると、コールは応答可能な次のユーザに転送され、誰も応答しない場合は最終的に話中として登録されます。

自動音声応答に設定したその他のオプションは自由にテストしてください。

コールピックアップのテスト

次に、コールピックアップ機能をテストします。この機能をすべてテストするには、3 人のユーザが必要です。ピックアップグループには Taylor と Rebekah を設定しています。この場合、どちらかにダイヤルする 3 人目のユーザが必要です。呼び出されなかった方のユーザは、コールをピックアップして代わりに電話に出ることができます。

1. Webex Teams クライアントで 3 人目のユーザから **Rebekah** に発信します。
2. Rebekah では応答しません。Taylor の MPP 電話機またはクライアントアプリで ***98** を押してコールをピックアップします。
3. 終了したら、コールを終了します。

コールパークのテスト

次に、コールパーク機能をテストします。この機能をすべてテストするには、3 人のユーザが必要です。コールパークグループには Taylor と Rebekah を設定しています。この場合、どちらかにダイヤルする 3 人目のユーザが必要です。コールを受けたユーザはパーク保留し、他のユーザまたは同じユーザがコールをピックアップします。

1. Webex Teams クライアントで 3 人目のユーザから Taylor または Rebekah に発信します。
2. MPP 電話機またはクライアントアプリでコールに応答します。次のようにしてコールをパークします。
   - 電話機でコールに応答します。[転送（Transfer）] ソフトキーまたは物理転送ボタンを押します。***68** と入力し、長いビープ音が鳴ったら、先ほどコールしたユーザまたは別のユーザの **5 桁の内線番号**を入力し、続けて **#** キーを押します。コールはその内線番号でパーク保留され、ダイヤルインユーザのクライアントで保留音が聞こえます。
   - 電話機でコールに応答します。[パーク（Park）] ソフトキーを押します。# キーを押して長いビープ音が聞こえたら、もう一度 **#** キーを押して、ユーザの内線番号でコールをパーク保留します。
   - クライアントでコールに応答します。[その他（More）] ボタン [] をクリックし、[転送（Transfer）] を選択します。***68** と入力し、長いビープ音が鳴ったら、先ほどコールしたユーザまたは別のユーザの **5 桁の内線番号**を入力し、続けて **#** キーを押します。コールはその内線番号でパーク保留され、ダイヤルインユーザのクライアントで保留音が聞こえます。
3. 電話機またはクライアントアプリからコールを取るには、***88** をダイヤルします。音声プロンプトが示されたら、コールをパーク保留した 5 桁の内線番号を入力し、続けて **#** キーを押します。
4. コールを終了します。

ページンググループのテスト

次に、ページンググループ機能をテストします（可能な場合）。この機能を使用できるかどうかは環境によります。次の要件を満たす必要があります。

- ページングには、IP アドレス 239.192.16.240 を使用したマルチキャストルーティングが必要です。その IP アドレスがマルチキャストルーティング専用として空いていることを確認します。
- ページンググループは、Cisco IP Phone 7800 または 8800 シリーズでのみ動作します。
- ページンググループには、2 人以上のユーザが必要です。少なくとも 1 台の MPP 電話機が利用できる必要があります。ラボでは、Taylor と Rebekah をページンググループに割り当てていますので、各ユーザに 7800 または 8800 電話機が登録されている必要があります。
- 前述の要件のいずれかが満たされない場合、ページンググループは機能せず、話中音が聞こえるか、その番号が使用できないことを示すメッセージが流れます。

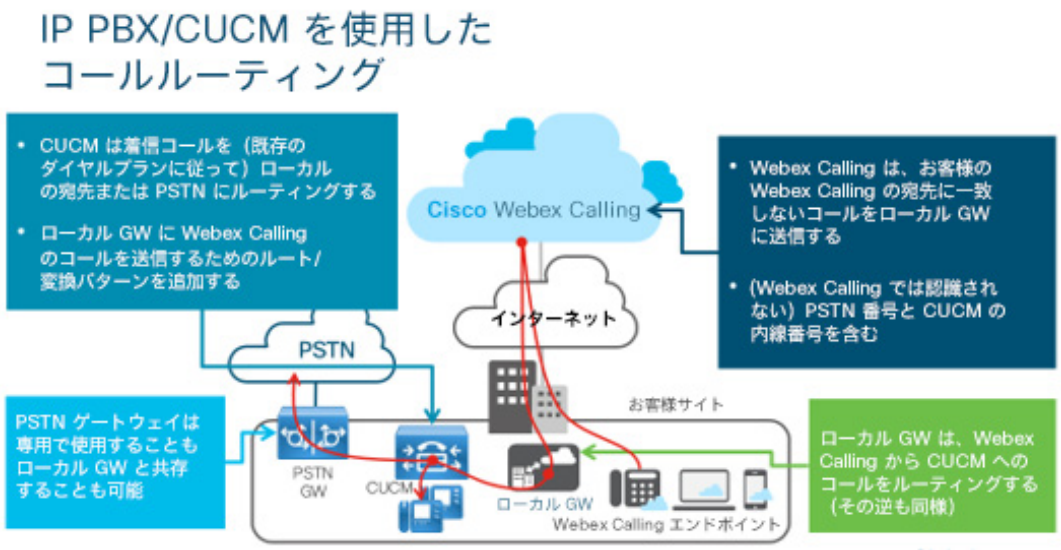
1. Taylor の MPP 電話機からページンググループの内線電話（**86033**）にコールします。

2. グループ内の他のすべての MPP 電話機から**ページング**音が聞こえます。他の電話機で数秒間ページング音が聞こえた後、Taylor の電話で「**ページングシステムの設定が完了しました（Paging system ready）**」というメッセージが聞こえます。メッセージが聞こえた後に Taylor の電話機で話すと、他の電話機で聞くことができます。

ローカルゲートウェイ

これまで PSTN にアクセスせずにすべて内線でテストしてきました。このセクションでは、ローカルゲートウェイ機能について説明します。この機能を使用すると、既存の PSTN を使用して、クラウド登録済みの電話で PSTN 接続を利用できます。自社のサイトにローカルゲートウェイを設定する場合、いくつかオプションがあります。このラボでは、PSTN との間のコールルーティングに Unified CM を使用するローカルゲートウェイを設定します。以下の図を参照してください。

Cisco Unified CM によるローカルゲートウェイ



Unified CM のコールルーティング設定は完了しているため、ローカルゲートウェイの設定に集中できます。dCloud セッションへのコールフローは次のように動作します。

a. コールが dCloud PSTN の DID 番号に着信します。

b. dCloud ゲートウェイはその番号を 4 桁の内線番号に変換し、Unified CM に送信します。

   - この番号は、dCloud セッションの [詳細（Session Details）] ページの [電話番号（Phone Numbers）] セクションで確認できます。また、Workstation 1 のデスクトップにある **DN_to_DID.txt** という名前のテキストファイルでも確認できます。

c. Unified CM の変換パターンは以下の 4 つの内線番号に一致し、プレフィックスとして **8** が付きます。

   - ラボで使用する 4 つの内線番号は、**6020、6021、6022、6023** です。

d. この変換された番号は、ローカルゲートウェイ用に事前設定したトランクにコールを送信する際のルートパターンと一致します。

    - 事前設定されたトランクは、着信ポート **5065** に設定された **SIP トランク セキュリティ プロファイル**を使用します。

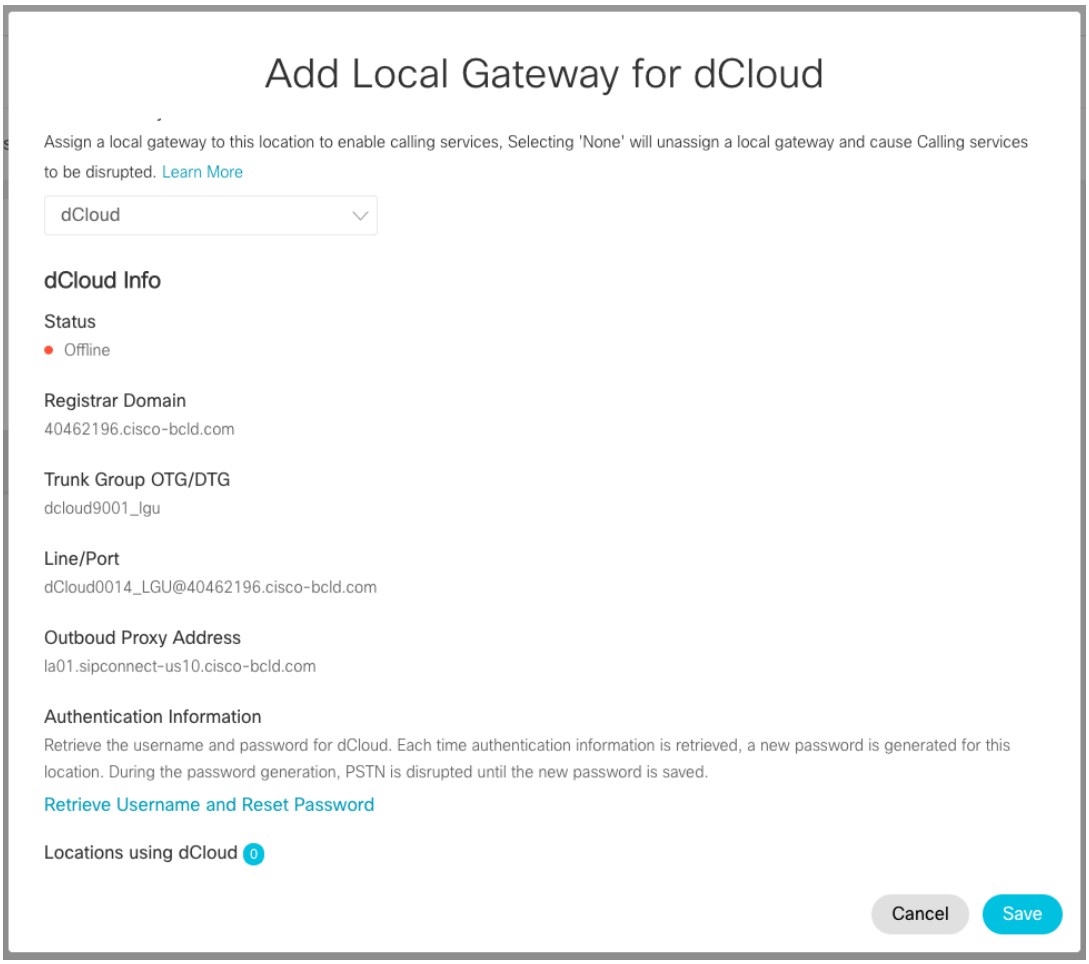
最初のタスクは、Control Hub でローカルゲートウェイを作成することです。ローカルゲートウェイを設定するには、作成後に提供される情報が必要です。

1. Control Hub で [サービス（Services）] に移動し、[コール（Calling）] カードの [ロケーション（Locations）] リンクをクリックします。

各ロケーションにローカルゲートウェイを割り当てることができます。ラボでは、1 つのロケーションにローカルゲートウェイを設定します。ゲートウェイは、dCloud セッションでホストされます。

2. **dCloud** のロケーションを選択します。
3. ポップアップウィンドウで、[ローカルゲートウェイ（Local Gateway）] をクリックします。
4. [編集（Edit）] > [続行（Continue）] > [管理（Manage）] をクリックします。
5. ドロップダウンメニューを使用して、[新しいローカルゲートウェイの作成（Create New Local Gateway）] を選択します。
6. ゲートウェイの名前に **dCloud** と入力し、緑のチェックマーク [✓] をクリックします（**名前を入力してからチェックマークをクリックしてください**）。
7. しばらくすると、ページに情報が表示されます。ローカルゲートウェイを設定する際にこの情報が必要です。**その場で情報を取得します。**Workstation 1 でテキストファイルを開き、そこにコピーすることをお勧めします。**レジストラドメイン、トランクグループ OTG/DTG、ライン/ポート、**および**発信プロキシアドレス**が必要になります。

ローカルゲートウェイの設定例



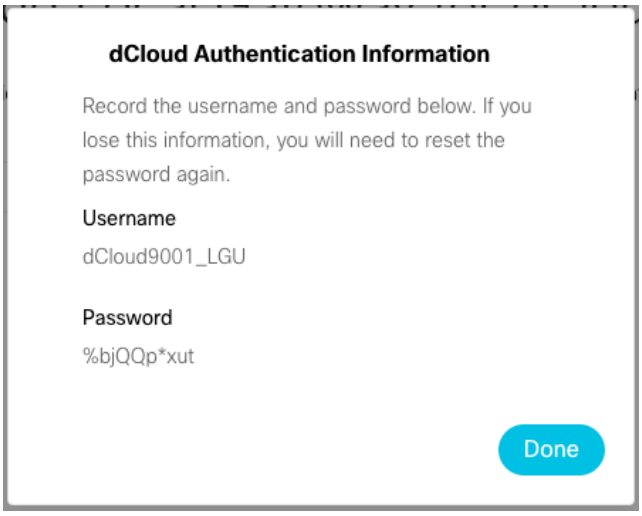
8. 情報を収集したら、ポップアップウィンドウで下にスクロールして [ユーザ名の取得とパスワードのリセット（Retrieve Username and Reset Password）] リンクをクリックします。

パスワードがリセットされることを示すポップアップメッセージが表示されます。ここでは、ユーザ名とパスワードを初めて取得しようとしているので問題ありません。ただし、このリンクをクリックすると常にパスワードがリセットされることを理解しておくことが非常に重要です。前のパスワードでローカルゲートウェイをすでに設定している場合は、このリセットによって Webex へのローカルゲートウェイ接続が切断されます。したがって、この情報を安全な場所に保管し、紛失しないようにします。

9. ポップアップメッセージで [はい（Yes）] をクリックします。

10. [ユーザ名（Username）] と [パスワード（Password）] を取得します。ローカルゲートウェイの設定時にこのログイン情報が必要です。

ローカルゲートウェイのユーザ名とパスワードのサンプル



11. ユーザ名とパスワードを取得できたら、[完了（Done）] をクリックします。
12. すべての情報を収集したら、[PSTN接続を確認（Confirm PSTN Connection）] をクリックします。
13. [ローカルゲートウェイ（Local Gateway）] ドロップダウンメニューで [dCloud] を選択します。
14. 表示された 2 つのボックスをオンにし、[保存（Save）] をクリックします。

ローカルゲートウェイ設定

ここで、前のセクションで取得した情報を使用してローカルゲートウェイを設定します。

注：すべてのコマンドは、Workstation 1 のデスクトップにある LGW_Config .txt という名前のテキストファイルにも記載されていますので、コピーして貼り付ければ簡単に設定できます。

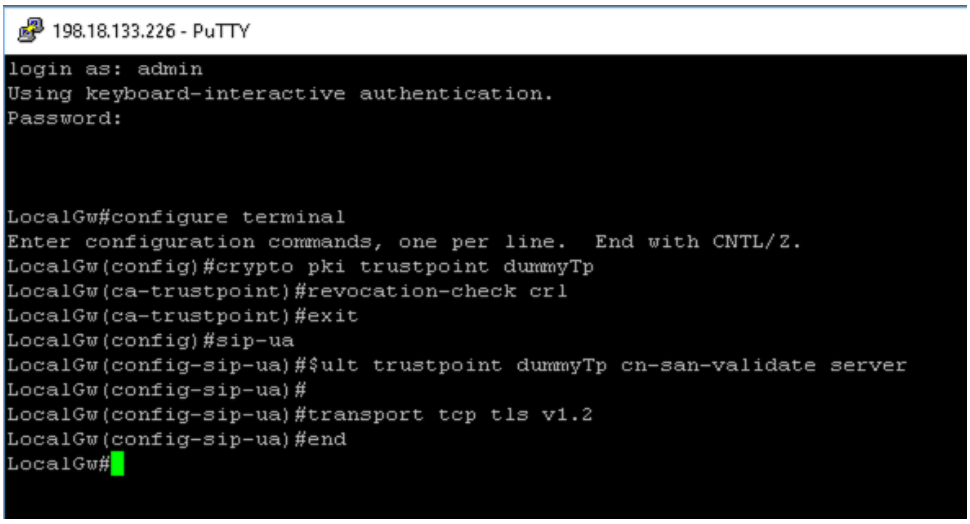
1. Workstation 1 に接続し、デスクトップのアイコン [] を使用して **PuTTY** を開きます（dCloud セッションに VPN 接続している場合は、ローカル SSH クライアントを使用することもできます）。
2. **ローカルゲートウェイ**の接続先が保存されたセッションをダブルクリックして、**198.18.133.226** のローカルゲートウェイに SSH 接続します。
3. **admin/dCloud123!** でログインします。
4. 以下の設定を使用してダミーの PKI トラストポイントを作成し、**dummyTp** という名前を付けます。sip-ua の下でそのトラストポイントをデフォルトのシグナリング トラストポイントとして割り当てます。テナント 200（後述の説明を参照）で設定された発信プロキシが、サーバから受信した CN-SAN リストと一致する場合にのみ LGW が接続を確立するようにするためには、cn-san-validate サーバが必要です。

暗号トラストポイントは、接続をセットアップする際にローカルクライアント証明書（mTLS）が必要ない場合でも、TLS を動作させるために必要です。最後に、次の表に示すように TLS v1.2 だけを明示的に有効して、v1.0 および v1.1 を無効にします。

表 23. ローカル ゲートウェイ トラストポイントの設定

設定内容
configure terminal crypto pki trustpoint dummyTp revocation-check crl exit sip-ua crypto signaling default trustpoint dummyTp cn-san-validate server transport tcp tls v1.2 end

ローカル ゲートウェイ トラストポイントの設定



5. デフォルトのトラストプールバンドルには、Webex への TLS 接続の確立中にサーバ側の証明書を検証する上で必要な DigiCert ルート CA 証明書は含まれていません。以下に示すように、http://www.cisco.com/security/pki から最新の **Cisco Trusted Core Root Bundle** をダウンロードしてトラストプールバンドルを更新する必要があります。

表 24. ローカルゲートウェイ証明書の設定と検証

設定内容
! DigiCert ルート CA 証明書が存在するかどうか確認する show crypto pki trustpool | include DigiCert ! – 存在しない場合は、以下のように更新する configure terminal crypto pki trustpool import clean url http://www.cisco.com/security/pki/trs/ios_core.p7b end ! 検証する show crypto pki trustpool | include DigiCert

6. 次のコマンドを入力して、プラットフォーム上の**ローカルゲートウェイ/CUBE アプリケーション**を有効にします。

表 25. ローカルゲートウェイ設定

設定内容
configure terminal voice service voip ip address trusted list ipv4 85.119.56.128.255.255.255.192 ipv4 85.119.57.128.255.255.255.192 **ipv4 128.177.14.0 255.255.255.128** **ipv4 128.177.36.0 255.255.255.192** **ipv4 135.84.169.0 255.255.255.128** **ipv4 135.84.170.0 255.255.255.128** **ipv4 135.84.171.0 255.255.255.128** **ipv4 135.84.172.0 255.255.255.128** ipv4 185.115.196.0.255.255.255.128 ipv4 185.115.197.0.255.255.255.128 ipv4 199.59.64.0.255.255.255.128 ipv4 199.59.65.0.255.255.255.128 ipv4 199.59.66.0.255.255.255.128 ipv4 199.59.67.0.255.255.255.128 ipv4 199.59.70.0.255.255.255.128 ipv4 199.59.71.0.255.255.255.128 exit allow-connections sip to sip media statistics media bulk-stats no supplementary-service sip refer no supplementary-service sip handle-replaces fax protocol pass-through g711ulaw stun stun flowdata agent-id 1 boot-count 4 stun flowdata shared-secret 7 104D000A061811021F0725282D3B303A sip g729 annexb-all early-offer forced end

上記のコマンドの説明：

`ip address trusted list` - 不正通話行為の防止

正規の VoIP コールの発信元としてローカルゲートウェイが想定しているエンティティ（Webex ピア、Unified CM ノード、IP PSTN など）の発信元 IP アドレスを明示的に設定するコマンドです。LGW のデフォルトでは、信頼できるリストにない IP アドレスからのすべての着信 VoIP コールのセットアップをブロックします。「**session target ip**」が設定されたダイヤルピアからの IP アドレスまたはサーバグループの IP アドレスはデフォルトで信頼されるため、ここで設定する必要はありません。

このリストの IP アドレスは、お客様が接続しているWebex Calling データセンター（プロダクション、ベータ）に応じて、『**Cisco Webex Calling カスタマー向け設定ガイド**』の「**ポートリファレンス情報**」セクションに記載されている IP サブネットと一致している必要があります。先述の設定には、このガイドの執筆時点で存在する Webex データセンターのプロダクション情報が含まれています。最新の情報はガイドを参照してください。

表 1. Webex Calling（プロダクション）

接続目的	送信元アドレス	送信元ポート	プロトコル	宛先アドレス	宛先ポート
Webex Calling へのシグナリングコール（SIP TLS）	ローカルゲートウェイの外部 NIC	8000 ～ 65535	TCP	85.119.56.128/26 85.119.57.128/26 128.177.14.0/25 128.177.36.0/26 135.84.169.0/25 135.84.170.0/25 135.84.171.0/25 135.84.172.0/25 185.115.196.0/25 185.115.197.0/25 199.59.64.0/25 199.59.65.0/25 199.59.66.0/25 199.59.67.0/25 199.59.70.0/25 199.59.71.0/25	8934
	デバイス	5060 ～ 5080			
	アプリケーション	エフェメラル（OS によって異なる）			
Webex Calling へのメディアコール（SRTP）	ローカルゲートウェイの外部 NIC	8000 ～ 48000†	UDP	85.119.56.128/26 85.119.57.128/26 128.177.14.0/25 128.177.36.0/26 135.84.169.0/25 135.84.170.0/25 135.84.171.0/25 135.84.172.0/25	19560 ～ 65535
	デバイス	19560 ～ 19660			
	アプリケーション	エフェメラル			

接続目的	送信元アドレス	送信元ポート	プロトコル	宛先アドレス	宛先ポート
				185.115.196.0/25 185.115.197.0/25 199.59.64.0/25 199.59.65.0/25 199.59.66.0/25 199.59.67.0/25 199.59.70.0/25 199.59.71.0/25	
PSTN ゲートウェイへのシグナリングコール（SIP TLS）	ローカル ゲートウェイの内部 NIC	8000 ～ 65535	TCP	自分の ITSP PSTN GW または Unified CM	PSTN オプションによって異なる（たとえば Unified CM の場合、通常 5060 または 5061）
PSTN ゲートウェイへのメディアコール（SRTP）	ローカル ゲートウェイの内部 NIC	8000 ～ 48000†	UDP	自分の ITSP PSTN GW または Unified CM	PSTN オプションによって異なる（たとえば Unified CM の場合、通常 5060 または 5061）
パブリック アドレス エンドポイントへのシグナリングコール（SIP TLS）	85.119.56.128/26 85.119.57.128/26 128.177.14.0/25 128.177.36.0/26 135.84.169.0/25 135.84.170.0/25	エフェメラル	TCP	エンドポイントの IP	8934

接続目的	送信元アドレス	送信元ポート	プロトコル	宛先アドレス	宛先ポート
	135.84.171.0/25 135.84.172.0/25 185.115.196.0/25 185.115.197.0/25 199.59.64.0/25 199.59.65.0/25 199.59.66.0/25 199.59.67.0/25 199.59.70.0/25 199.59.71.0/25				
デバイスの設定とファームウェアの管理（シスコ デバイス）	Webex Calling デバイス	エフェメラル	TCP	3.20.185.219 3.130.87.169 35.172.26.181 52.86.172.220 72.163.10.134 85.119.56.128/26 85.119.56.198 85.119.57.128/26 85.119.57.198 135.84.169.186 135.84.170.186 173.37.149.125 199.59.64.143 199.59.65.228	80、443

接続目的	送信元アドレス	送信元ポート	プロトコル	宛先アドレス	宛先ポート
				199.59.66.228 199.59.67.143 * ドメイン： • cisco-jp.bcld.webex.com • cisco.broadcloud.com.au • cisco.broadcloud.eu • cisco.broadcloud.eu • webapps.cisco.com • activate.cisco.com • activation.webex.com • cisco.sipflash.com	
				**cloudupgrader.webex.com	**443、6970
デバイス時刻同期（NTP）	Webex Calling デバイス	51494	UDP	85.119.56.128/26 85.119.57.128/26 135.84.169.154 135.84.170.154 199.59.64.152 199.59.65.181 199.59.66.181 199.59.67.152	123
デバイス名の解決	Webex Calling デバイス	エフェメラル	UDP および TCP	ホスト定義	53
アプリケーション設定	Webex Calling アプリケーション	エフェメラル	TCP	64.68.99.6 64.68.100.6 85.119.56.128/26 85.119.57.128/26 128.177.36.138 128.177.14.181	80、443、1081、2208、8443、5222、5280 ～ 5281、52644 ～

接続目的	送信元アドレス	送信元ポート	プロトコル	宛先アドレス	宛先ポート
				135.84.169.150 135.84.169.185 135.84.170.185 199.59.64.140 199.59.67.140 ドメイン： • client-jp.bcld.webex.com • jp.bcld.webex.com • idbroker.webex.com	52645
アプリケーション時刻の同期	Webex Calling アプリケーション	123	UDP	ホスト定義	123
アプリケーション名の解決	Webex Calling アプリケーション	エフェメラル	UDP および TCP	ホスト定義	53
CScan	Webex Calling デバイス	エフェメラル	TCP	135.84.169.183 185.115.196.0/25 199.59.65.243 199.59.67.156	8934 および 80、443

† CUBE メディアのポート範囲は、**rtp-port range** で設定可能

* 電話機を初めてネットワークに接続する、または初期状態にリセット後にネットワークに接続する際に DHCP オプションが設定されていない場合、ゼロタッチプロビジョニングを実現するために電話機はデバイス アクティベーション サーバに接続します。新しい電話機は、webapps.cisco.com ではなく、activate.cisco.com に接続してプロビジョニングを行います。11.2(1) より前のファームウェアリリースを使用する電話機については、引き続き webapps.cisco.com を使用します。ファイアウォールで両方のドメインを許可するように設定することをお勧めします。

** 企業の電話システム（Cisco Unified CM）から Webex Calling に移行する場合にのみ、cloudupgrader.webex.com と 443、6970 ポートを有効にする必要があります。詳細については、upgrade.cisco.com を参照してください。

`media statistics`

LGW でのメディア監視を有効にします。

`media bulk-stats`

コントロールプレーンでバルク統計用にデータを定期取得できるようにします。

`allow-connections sip to sip`

2 つの VoIP SIP コールレッグをブリッジしSIP-SIP通話を有効にします。デフォルトでは無効になっています。

`no supplementary-service sip refer` および `no supplementary-service sip handle-replaces`

REFER を無効にし、Replaces ヘッダーのダイアログ ID をピアのダイアログ ID に置き換えます。

`fax protocol pass-through g711ulaw`

Fax トランスポート用のオーディオコーデックを有効にします。

`stun`

`stun flowdata agent-id 1 boot-count 4`

`stun flowdata shared-secret 7 104D000A061811021F0725282D3B303A`

STUN をグローバルで有効にします。コールが Webex Calling ユーザに戻される場合（着信側と発信側の両方が Webex Calling ユーザで、Webex Calling SBC でメディアをアンカーしている場合など）、ピンホールが開かれていないため、メディアはローカルゲートウェイに到達できません。

ローカルゲートウェイの STUN バインディング機能を使用すると、ローカルで生成された STUN 要求を、ネゴシエート済みのメディアパスを介して送信することができます。STUN はファイアウォールのピンホールを開けるためだけに使用され、Webex Access SBC でメディアをラッチングできるので、共有秘密鍵は任意の値でかまいません。

STUN パスワードは、LGW/CUBE が STUN メッセージを送信するために必要となります。IOS/IOS-XE ベースのファイアウォールは、このパスワードをチェックし、ピンホールを動的に開くように設定することができます（明示的な in/out ルールは不要）。しかし、LGW を導入する場合、Webex SBC サブネットに基づいてアウトバウンド方向でピンホールを開くようにファイアウォールが静的に設定されているため、ファイアウォールは単なるインバウンドの UDP パケットとして処理します。これにより、パケットの内容の確認なしにピンホールが開かれます。

`sip`

`g729 annexb-all`

G729 のすべてのバリアントを許可します。

`sip`

`early-offer forced`

このコマンドは、LGW/CUBE が隣接ピアの確認応答を取得してから SDP 情報を送信させるのではなく、Initial INVITE メッセージに SDP 情報を含めて送信させます。

7. Webex は SIPS URI をサポートしていないため、SIP プロファイルを次のように設定して SIPS URI を SIP に変換する必要があります（ただし、`_sips._tcp.<outbound-proxy>` のように `SRV` クエリには `SIPS` が必要です）。

rule 20 は、1 つの企業内で LGW サイトを一意に識別するために、Control Hub から取得した**トランクグループ OTG/DTG** パラメータを含めるように From ヘッダーを変更します。次の例では **dcloud9001_lgu** が使用されています。これを**トランクグループ OTG/DTG** 情報で置き換えてください。

設定のマッピング例

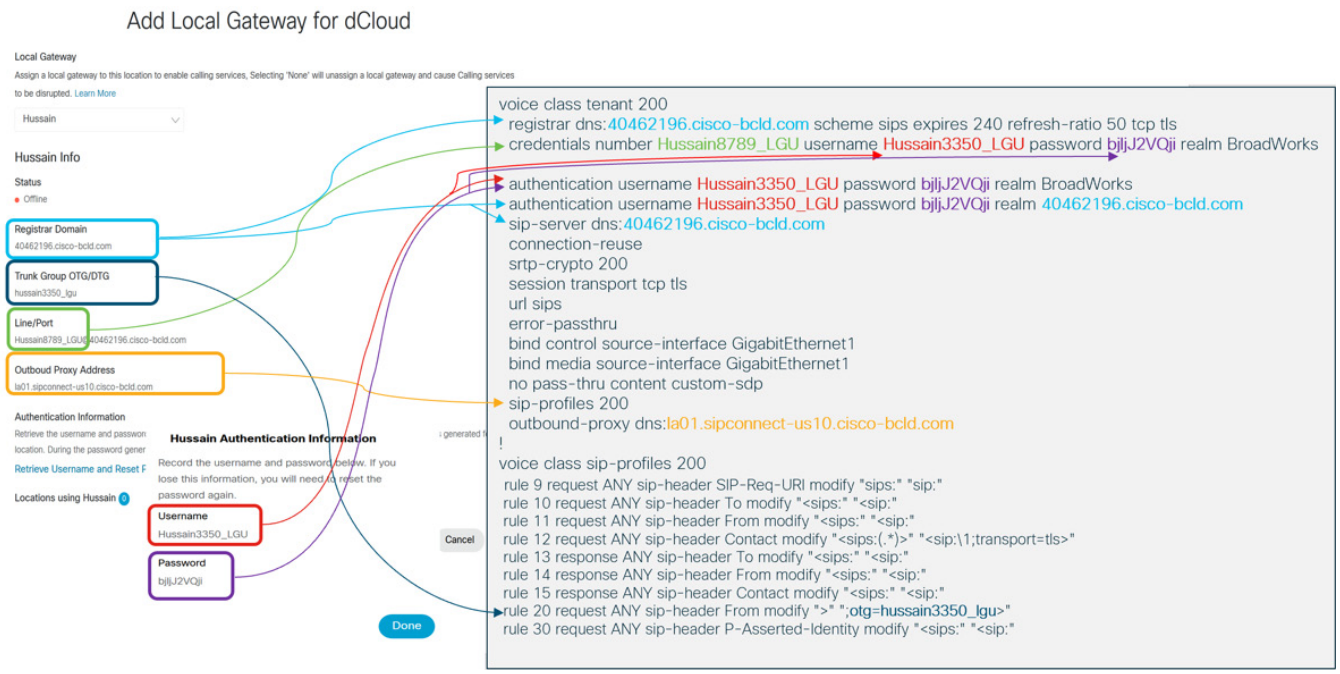


表 26. ローカルゲートウェイ SIP プロファイル設定

設定内容
configure terminal voice class sip-profiles 200 rule 9 request ANY sip-header SIP-Req-URI modify " sips:(.*)" " sip:\1" rule 10 request ANY sip-header To modify " <sips:(.*)" " <sip:\1" rule 11 request ANY sip-header From modify " <sips:" " <sip:\1" rule 12 request ANY sip-header Contact modify " <sips:(.*)>" " <sip:\1;transport=tls>" rule 13 response ANY sip-header To modify " <sips:(.*)" " <sip:\1" rule 14 response ANY sip-header From modify " <sips:(.*)" " <sip:\1" rule 15 response ANY sip-header Contact modify " <sips:(.*)" " <sip:\1" rule 20 request ANY sip-header From modify " >" " ;otg=dcloud9001_lgu>" rule 30 request ANY sip-header P-Asserted-Identity modify " sips:(.*)" " sip:\1"

8. 次の表に示すように、Codec プロファイル、STUN 定義、および SRTP 暗号化スイートを設定します。

表 27. ローカルゲートウェイ設定

設定内容
voice class codec 99 codec preference 1 g711ulaw codec preference 2 g711alaw codec preference 3 g729r8 exit voice class srtp-crypto 200 crypto 1 AES_CM_128_HMAC_SHA1_80 exit voice class stun-usage 200 stun usage firewall-traversal flowdata exit

上記のコマンドの説明：

```
voice class codec 99
```

セッションで g729 と g711（mu と a-law）の両方の Codecを許可します。すべてのダイヤルピアに適用されます。

```
voice class srtp-crypto 200
```

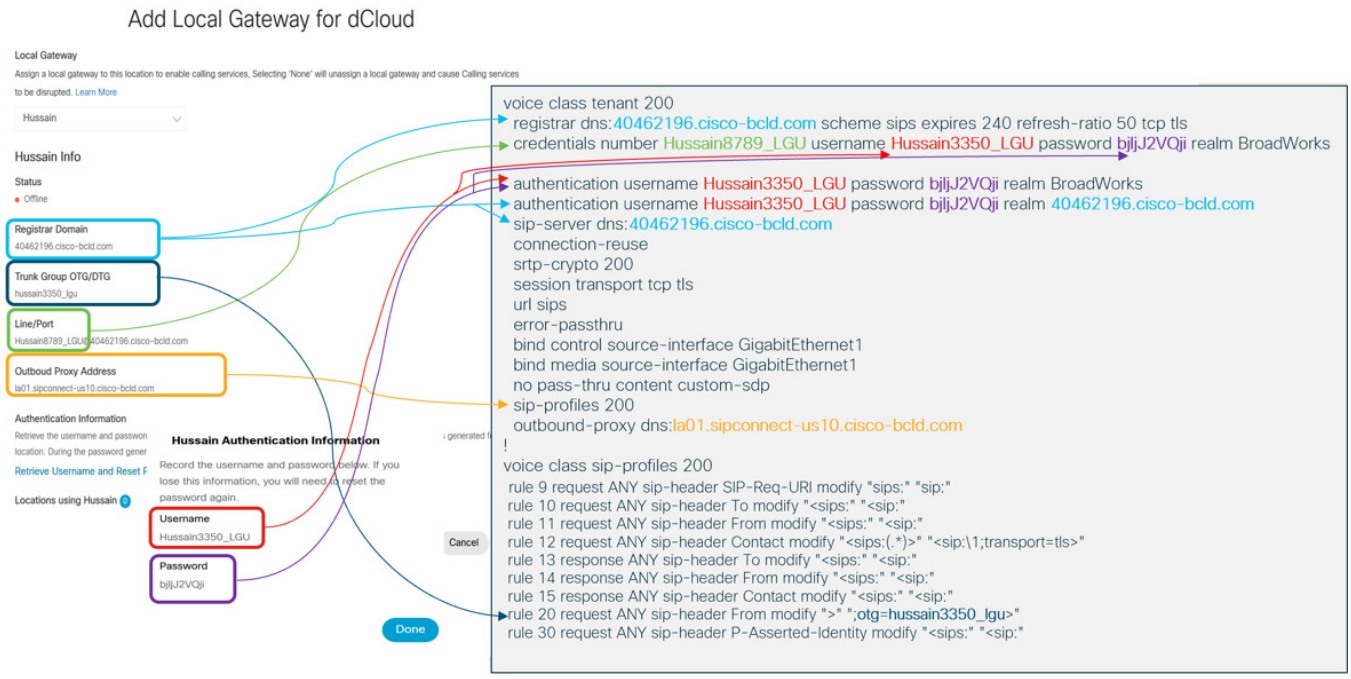
この中で LGW/CUBE の SDP オファーおよびアンサーに SHA1_80 のみ含めるように指定します。Webex Calling は SHA1_80 のみをサポートします。このコマンドは、Webex Calling に対する **voice class tenant 200**（後述の説明を参照）に適用されます。

```
voice class stun-usage 200
```

STUN の使用を定義します。Unified CM 電話機が別の Webex フォンにコールを転送する際に音声パケットの喪失を防ぎます。Webex 向けのすべてのダイヤルピア（2XX タグ）に適用されます。

9. voice class tenant 200 を次のように設定します。ただし、このドキュメントの voice class tenant 200 の下に表示されているとおりに設定するのではなく、以下のマッピングに示されているように Control Hub から取得したパラメータを使用してください。

設定のマッピング例



注：これらの設定例は参考までに示しているだけですので、そのまま使用しないでください。ローカルゲートウェイを追加するときに Control Hub で収集した設定を使用します（以下の表を参照）。

- [登録ドメイン（Registrar Domain）]：**40462196.cisco-bcld.com**
- [トランクグループOTG/DTG（Trunk Group OTG/DTG）]：**dcloud9001_lgu**
- [ライン/ポート（Line/Port）]：**dCloud0014_LGU@40462196.cisco-bcld.com**
- [発信プロキシアドレス（Outbound Proxy Address）]：**la01.sipconnect-us10.cisco-bcld.com**
- [ユーザ名（Username）]：**dCloud9001_LGU**
- [パスワード（Password）]：**%bjQQp*xut**

表 28. ローカル ゲートウェイ テナント設定

設定内容
voice class tenant 200 registrar dns:40462196.cisco-bcld.com scheme sips expires 240 refresh-ratio 50 tcp tls credentials number dCloud0014_LGU username dCloud9001_LGU password %bjQQp*xut realm BroadWorks authentication username dCloud9001_LGU password %bjQQp*xut realm BroadWorks authentication username dCloud9001_LGU password %bjQQp*xut realm 40462196.cisco-bcld.com no remote-party-id sip-server dns:40462196.cisco-bcld.com connection-reuse srtp-crypto 200 session transport tcp tls url sips error-passthru asserted-id pai bind control source-interface GigabitEthernet1 bind media source-interface GigabitEthernet1 no pass-thru content custom-sdp sip-profiles 200 outbound-proxy dns:la01.sipconnect-us10.cisco-bcld.com privacy-policy passthru

上記のコマンドの説明：

`voice class tenant 200`

CUBE のマルチテナント機能は、テナントごとに異なるサービスを提供する SIP トランク上の複数のテナントに対して、特定のグローバル設定を有効にする機能です。

`registrar dns:40462196.cisco-bcld.com scheme sips expires 240 refresh-ratio 50 tcp tls`

ローカルゲートウェイのレジストラサーバ情報を設定します。2 分（240 秒の 50%）間隔で再登録されます。

`credentials number dCloud9001_LGU username dCloud9001_LGU password %bjQQp*xut realm BroadWorks`

トランク登録用のログイン情報。

`authentication username dCloud9001_LGU password %bjQQp*xut realm BroadWorks`

`authentication username dCloud9001_LGU password %bjQQp*xut realm 40462196.cisco-bcld.com`

コールの認証。

`no remote-party-id`

Webex Calling では PAI を使用するため SIP Remote-Party-ID（RPID）ヘッダーを無効化します（PAI は、CLI で asserted-id pai コマンドを使用して有効化します。後述を参照）。

`sip-server dns:40462196.cisco-bcld.com`

Webex Calling サーバ情報。

`connection-reuse`

登録処理とコール処理に同じ永続的接続を使用します。

`srtp-crypto 200`

「**voice class srtp-crypto 200**」で定義された内容を使用します。「voice class srtp-crypto 200」では SHA1_80 を使用するように設定されています。

`session transport tcp tls`

TLS へのトランスポートを設定します。

`url sips`

SRV クエリは、Access SBC でサポートされている SIPS であることが必要です。他のすべてのメッセージは sip-profile 200 によって SIP に変更されます。

`error-passthru`

SIP エラー応答パススルー機能。

`asserted-id pai`

LGW/CUBE で PAI 処理を使用します。

`bind control source-interface GigabitEthernet1`

Webex 側のシグナリング ソース インターフェイス。

`bind media source-interface GigabitEthernet1`

Webex 側のメディア ソース インターフェイス。

`no pass-thru content custom-sdp`”

テナントのデフォルトコマンド。

`sip-profiles 200`

SIPS を SIP に変更し、**voice class sip-profiles 200** で定義されているとおりに INVITE および REGISTER メッセージのライン/ポートを変更します。

`outbound-proxy dns:la01.sipconnect-us90.cisco-bcld.com`

Webex Calling Access SBC情報。

`privacy-policy passthru`

Incoming Leg で受け取ったプライバシーヘッダーの値をOutboud Legに透過します。

10. 次に、以下の音声クラステナントを設定します。

表 29. ローカルゲートウェイ音声クラステナント設定

設定内容
! voice class tenant 100 は CUCM に向かうすべての**発信**ダイヤルピアに適用されます。 voice class tenant 100 session transport udp url sip error-passthru bind control source-interface GigabitEthernet2 bind media source-interface GigabitEthernet2 no pass-thru content custom-sdp ! voice class tenant 300 は、CUCM からのすべての着信ダイヤルピアに適用されます。 voice class tenant 300 bind control source-interface GigabitEthernet2 bind media source-interface GigabitEthernet2 no pass-thru content custom-sdp

11. URI ベースのダイヤル用に次の音声クラス URI を設定します。

表 30. ローカルゲートウェイ音声クラスの設定

設定内容
! - Webex Access SBC のシグナリング VIA ポートを定義します。 voice class uri 200 sip pattern :8934 ! - Webex Calling のトランクに Unified CM シグナリング VIA ポートを定義します。 voice class uri 300 sip pattern :5065

12. 次のように音声クラスサーバグループを設定します。

表 31. ローカル ゲートウェイ サーバ グループの設定

設定内容
voice class server-group 301 ipv4 198.18.133.3 port 5065

この設定では、Unified CM グループのノードに対して、Unified CM トランクのターゲットホストの IP アドレスとポート番号を定義しています。Unified CM は、Webex Calling トランクの着信トラフィックにポート 5065 を使用します。ラボでは、トランクおよびポート番号付きのトランク セキュリティ プロファイルが事前に設定されています。

13. 以下の表に示されるように発信ダイヤルピアを設定します。

表 32. ローカルゲートウェイの発信ダイヤルピア設定

設定内容
! - Webex への発信ダイヤルピア dial-peer voice 201 voip description Outgoing dial-peer to Webex destination-pattern .T session protocol sipv2 session target sip-server voice-class codec 99 dtmf-relay rtp-nte voice-class stun-usage 200 no voice-class sip localhost voice-class sip tenant 200 srtp no vad ! - Unified CM の Webex Calling トランク宛の発信ダイヤルピア dial-peer voice 301 voip description Outgoing dial-peer to Unified CM Webex Calling Trunk for inbound from Webex destination-pattern .T session protocol sipv2 session server-group 301 voice-class codec 99 dtmf-relay rtp-nte voice-class sip tenant 100 no vad

14. 次のようにダイヤルピアグループ（DPG）を設定します。

表 33. ローカルゲートウェイのダイヤルピアグループ設定

設定内容
! - Unified CM --> LGW --> Webex Calling パスのターゲットとして、ダイヤルピアグループ 200 で発信ダイヤルピア 201 を定義 voice class dpg 200 dial-peer 201 preference 1 ! - Webex --> LGW --> Unified CM パスとして、ダイヤルピアグループ 300 で発信ダイヤルピア 301 を定義 voice class dpg 300 dial-peer 301 preference 1

15. 次のように着信ダイヤルピアを設定します。

表 34. ローカルゲートウェイの着信ダイヤルピア設定

設定内容
! - Webex 着信コールレッグ用の着信ダイヤルピア dial-peer voice 200 voip description Incoming dial-peer from Webex session protocol sipv2 destination dpg 300 incoming uri via 200 voice-class codec 99 dtmf-relay rtp-nte voice-class stun-usage 200 voice-class sip tenant 200 srtp no vad ! - Webex を宛先とする Unified CM 着信コールレッグ用の着信ダイヤルピア dial-peer voice 300 voip description Incoming dial-peer from Unified CM for Webex session protocol sipv2 destination dpg 200 incoming uri via 300 voice-class codec 99 dtmf-relay rtp-nte voice-class sip tenant 300 no vad

これで、ローカルゲートウェイの設定は完了です。ここで保存します。

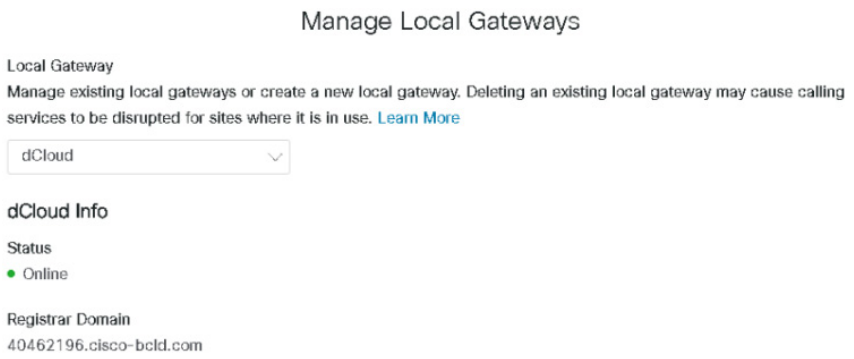
16. コマンドプロンプトで `end` と入力します。
17. 保存するには、`copy run start` と入力し、Enter/Return を 2 回押します。

注：すべてのローカルゲートウェイ設定を 1 ヵ所に表示する方法については、**付録 D** を参照してください。

設定をテストする前に、ローカルゲートウェイが Control Hub でオンラインとして表示されていることを確認します。

18. Control Hub に戻り、必要に応じてログイン（**cholland@cbXXX.dc-YY.com/dCloud123!**）します。
19. [サービス（Services）] に移動し、[コール（Calling）] カードの [ロケーション（Locations）] をクリックします。
20. **dCloud** のロケーションをクリックします。
21. ポップアップウィンドウの [PSTN接続（PSTN Connection）] に [ローカルゲートウェイ（Local Gateway）] 用の [dCloud] が表示されます。[ローカルゲートウェイ（Local Gateway）] をクリックします。
22. [編集（Edit）] > [続行（Continue）] を選択します。
23. ドロップダウンメニューから [dCloud] を選択し、[管理（Manage）] をクリックします。
24. [ステータス（Status）] が [オンライン（Online）] になっているはずです。ステータスを確認したら、**X** をクリックしてウィンドウを閉じます。

オンラインになっている登録済みローカルゲートウェイ



ローカルゲートウェイのテスト

ローカルゲートウェイの設定がすべて終わったので、PSTN や、Unified CM に登録したコールデバイスを利用してコールをテストできます。

MPP/Webex Teams からオンプレミスの Jabber クライアントにコールする

1. Workstation 1 で Jabber を開きます（ラボにログインしていない場合は、**cholland@cbXXX.dc-YY.com** でログインします）。ユーザ名/パスワードのプロンプトが表示されたら、**cholland/dCloud123!** を入力します。
2. MPP または Webex Teams クライアントから、**972-555-6018** にダイヤルします。
3. Jabber でコールに応答します。

ユーザの発信者 ID は、そのユーザに割り当てられていない完全な E.164 番号になっています。これは想定どおりです。ユーザには内線番号しか設定されていないため、システムはその場所に設定されているメインの番号を使用します。dCloud の場所に設定されているメインの番号を確認するには、Control Hub で [サービス（Services）] に移動し、[コール（Calling）] カードの [番号（Numbers）] をクリックします。前に確認した発信者 ID に [Main] のインジケータがついています。この番号は、自動音声応答に対しても設定されています。

もう 1 つ注意すべきなのは、Webex Calling では呼び出し先の番号の先頭に +1 が追加されることです。これは、この場所が米国に設定されているためです。この場所が別の地域に設定されている場合は、呼び出し先の番号にプラス（+）とその国の国コードが付きます。

4. コールを終了します。

オンプレミスの Jabber クライアントから MPP/Webex Teams にコールする

1. Jabber クライアントから、いずれかのユーザまたは自動音声応答の内線番号にダイヤルします。ラボで設定した内線番号は次のとおりです。
   a. 86020 – 自動音声応答
   b. 86021 – Taylor Bard

c. 86022 – Rebekah Barretta

d. 86023 – Room デバイス

2. MPP または Webex Calling クライアントで応答します。

このコールは、事前に設定されたトランク経由でルーティングされます。また、このトランクが設定されたルートリストを指す **860XX** の事前設定済みルートパターンがコールフローで使用されます。

3. コールを終了します。

PSTN から MPP/Webex Teams にコールする

次に、PSTN を利用したコールをテストします。PSTN からダイヤルする DID 番号は、dCloud セッションの詳細に記載されています。また、Workstation 1 のデスクトップにある **DN_to_DID.txt** という名前のテキストファイルにも記載されています。

1. DID 番号を使用して、実際の携帯電話またはデスクフォンからユーザまたは自動音声応答のいずれかにダイヤルします。
2. Webex Teams アプリ/デバイスでコールに応答します。
3. dCloud のコールフローは次のとおりです。
   a. DID コールが dCloud に着信します。
   b. プラットフォーム ゲートウェイが、その DID を 4 桁の内線番号（6XXX または 7XXX）に変換します。
   c. Unified CM には変換パターンがあらかじめ設定されているため、プレフィックスとして 8 が追加されます。
   d. この変換により、事前設定済みの **860XX** ルートパターンに一致します。このルートパターンでは、ローカルゲートウェイの SIP トランクが設定されたルートリストが示されています。SIP トランクはルートグループに設定され、ルートリストに追加されます。
   e. コールはローカルゲートウェイと Webex を経由してユーザの内線番号にルーティングされます。

MPP/Webex Teams から PSTN にコールする

dCloud national では、セッションが存在するデータセンターの地域でコールが可能です。米国西部/東部のデータセンターは、それぞれ **dc-05**、**dc-01** です。EMEAR のデータセンターは **dc-03**、APJ のデータセンターは **dc-02** です。

米国のデータセンターでは、米国内のすべての番号にコールできます。このロケーションは米国向けに設定されているため、Webex では必要に応じてダイヤルされた番号に +1 が追加されることに注意してください。つまり、10 桁の番号または 1 + 10 桁の番号がコールされます。

EMEAR または APJ セッションからのダイヤルは、米国の場合と若干異なります。どのセッションでも、データセンターに関係なく、Webex Calling のロケーションは米国向けに設定されています。そのためラボでは、英国（EMEAR）やシンガポール（APJ）の番号にダイヤルするには、**00 + 国コード**をダイヤルしてから、該当の番号（英国の場合は 10 桁、シンガポールの場合は 8 桁）をダイヤルする必要があります。EMEAR データセンターの場合の国番号は **44**、APJ データセンターの場合の国番号は **65** です。

00 を付けて番号をダイヤルすると、Webex は +1 を追加せずにその番号をそのままルーティングします。Unified CM での EMEAR および APJ セッションのコールフローは次のようになります。

- コールは Unified CM に入り、データセンターに応じて、**00.44!**（英国）または **00.65!**（シンガポール）変換パターンにヒットします。
- 変換パターンによって、番号から **00** が削除され、プラス（**+**）が追加されます。
- 現在 +E.164 番号は +44/+65 のルートパターンのどちらかにヒットし、dCloud PSTN ゲートウェイにルーティングされます。

1. 前述のダイヤルの説明に基づいて、PSTN 番号にダイヤルします。
2. コールに応答します。

着信した発信者 ID 番号は、919、408、44、64 のいずれかの番号（セッションのデータセンターによる）で始まっています。これは、dCloud PSTN のセットアップ方法から想定されたとおりです。発信者 ID は常に、7800 DN にマッピングされるセッションに割り当てられた DID として示されます。

3. コールを終了します。

ローカルゲートウェイのデバッグ

ローカルゲートウェイでコールの確立時に発生した障害をトラブルシューティングするには、次の手順に従います。

表 35. ローカルゲートウェイのデバッグ

設定内容
! - ローカルゲートウェイのロギングバッファでデバッグ情報を収集 ---------- LocalGateway#conf t LocalGateway(config)#no logging console LocalGateway(config)#no logging monitor LocalGateway(config)#service timestamps debug datetime msec LocalGateway(config)#logging buffered 9999999 debugging LocalGateway(config)#service sequence-numbers LocalGateway(config)#no logging rate-limit LocalGateway(config)#exit ! - 次のデバッグコマンドは、このラボで発生したコール障害のトラブルシューティングに有効です。 “debug ccsip message” “debug voip ccapi inout” "show log" コマンドを発行すると、デバッグ情報を確認できます。

シナリオ 8. Webex Teams と O365 の統合

Webex Teams と O365 の初期統合

このセクションでは、Office 365 と Webex の統合機能のセットアップについて説明します。このセクションを完了するには、独自の O365 サイトを使用する必要があります。O365 サイトが利用できない場合は、次のようにしてトライアル版を作成します。

注：O365 トライアル版を作成し、シナリオ 1 ですでにユーザをセットアップしている場合は、**次のセクション**にスキップして構いません。

1. ラボの Workstation 1 で、次の URL に移動します：https://aka.ms/e5trial
2. 最初のボックスに、シナリオ 1 で取得した電子メールアドレスを入力します。電子メールアドレスは **trial** から始まります。
3. [次へ（Next）] をクリック後、[新規アカウントの作成（Create new account）] をクリックします。
4. 次のユーザ情報を入力します。
   - [姓名（First/Last name）]：**Charles Holland**
   - [会社の電話番号（Business Phone number）]：（仮のもので可。例：**417-555-1234**）
   - [会社名（Company name）]：任意のもので可
   - [企業規模（Your Company size）]：任意の規模
   - [国または地域（Country or region）]：**United States**
5. [次へ（Next）] をクリックします。
6. **電話番号**を入力し、ロボットではないことを示してから [検証コードの送信（Send Verification Code）] をクリックします（この番号はテキストメッセージまたは電話を受けられる実際の番号であることが必要です）。（Code:+81 Phone number:90-xxxx-xxxx）
7. 検証コード(Varitification Code)を入力し、[検証（Verify）] をクリックします。
8. **ドメイン名**を入力し、[有効性確認（Check availavitility）] をクリックします。ドメイン名は、後で情報を取得するためだけのものですので任意のもので構いません。
9. 使用可能なドメインを選択したら [次へ（Next）] をクリックします。
10. [ユーザIDの作成（Create user ID）] では、**Charles のユーザ ID**（**cholland**）を使用することもできます。
11. 簡略化のため、パスワードには **dCloud123!** を使用します。
12. [サインアップ（Sign up）] をクリックします。
13. 検証と ID の作成が完了したら、[セットアップに進む（Go to Setup）] をクリックします。

14. [開始（Get Started）] をクリックし、 [セットアップを終了する（Exit setup）] リンクをクリックして以前のドメインページをスキップします。
15. O365 トライアル版をセットアップする場合は、次の点に注意してください。
    - 最初に作成するアカウントの他に、トライアル版のセットアップ手順で O365 ユーザを少なくとも 1 人作成します。この追加アカウントは、O365 ドキュメントで共同編集のテストをする際に使用します。
        - portal.office.com ページにアクセスしたら、[ユーザ（Users）] を展開し、[アクティブユーザ（Active users）] をクリックします。
        - [アクティブユーザ（Active users）] ページで [Add a user] をクリックします。
        - **ユーザ情報**を入力します（簡単にするために、Anita Perez（aperez）など別のラボで使用した情報を利用して構いません）。
        - [パスワード（Password）] をクリックします。[自分でパスワードを作成する（Let me create the password）] を選択し、パスワードを **dCloud123!** に設定して、[ユーザが初回サインイン時にパスワードを変更する（Require this user change their password when they first sign in）] をオフにします。
        - [次へ（Next）] をクリックします。
        - [Office 365 E5] チェックボックスをオンにして、[次へ（Next）] をクリックします。
        - [オプション設定（Optional settings）] ページで [次へ（Next）] をクリックします。
        - [追加の終了（Finish adding）] をクリックし、 [閉じる（Close）] をクリックして**閉じます**。
    - Word アプリケーションのオンライン Outlook はテストに使用しますが、コンピュータにインストールする必要はありません。

重要：O365 ユーザのログイン情報を忘れずに書き留めておいてください。

O365 トライアル版の初期セットアップを完了し、少なくとも 2 人のユーザを作成したら、このセクションを続行します（このトライアルを作成するユーザは、2 人のユーザの内の 1 人に含められます）。

Cisco Webex では、ユーザが Cisco Webex Teams でアクセスするエンタープライズコンテンツ管理プラットフォームを選択できます。これで、作成した O365 トライアル版に接続できるようになります。

1. Webex Control Hub で [サービス（Services）] に移動し、[メッセージ（Message）] カードの [設定（Settings）] をクリックします。
2. [コンテンツ管理（Content Management）] セクションまで下にスクロールし、[設定の編集（Edit Settings）] をクリックします。
3. [Microsoft] のチェックボックスをオンにして、[リンクされたフォルダーを有効にする（Enable linked folders）] オプションボタンをオンにします。
4. トライアルで作成した**ドメイン**（trialdomain.onmicrosoft.com など）を入力します。

5. [保存（Save）] をクリックします。
6. [コンテンツ管理（Content Management）] セクションに戻り、[すべてのユーザをグローバルで有効にする（Globally enable all users）] オプションボタンを選択し、[はい（Yes）] をクリックします（オプションでユーザを個別に有効にすることもできますが、このラボでは、迅速に処理するためにグローバルで有効にしています）。

Azure Active Directory ユーザを Cisco Webex Control Hub に同期する

注：このセクションにジャンプして O365 トライアル版のセットアッププロセスを先に開始した場合は、ここで止めて**シナリオ 2** に戻り、ラボを続けることができます。O365 で OneDrive と SharePoint の準備が完了するまで最大 60 分かかる場合があります。O365 サイトで準備が整うまで、ECM セクションは実施できません。準備ができたかどうか確認するには、O365 管理センター（admin.microsoft.com）に移動して、メニューアイコン [] をクリックします。[設定中...（Setting up...）]（OneDrive [

] または SharePoint [

]）が表示された場合は、ECM セクションはまだ実施できません。

Control Hub でユーザを作成するには、個別に作成する、CSV を利用する、ディレクトリ同期機能を利用する方法があります。このセクションでは、Control Hub を使用して Azure Active Directory（Azure AD）を同期する設定を説明します。Azure AD と同期するのに、オンプレミスのインフラストラクチャやコネクタは必要ありません。この統合機能により、ユーザが Azure AD のアプリケーションで作成/更新/削除されるたびに、ユーザリストが同期されます。オンプレミス環境のドメインコンピュータにインストールされているディレクトリコネクタを使用して、オンプレミスの Active Directory を Control Hub と同期することもできます。これらの手順については、付録 C で説明します。

Azure Active Directory ユーザと Webex Control Hub の統合では、System for Cross-Domain Identity Management（SCIM）API を使用します。SCIM は、ID ドメインまたは IT システム間でユーザ ID 情報を自動的に交換するためのオープンスタンダードです。クラウドベースのアプリケーションとサービスでユーザ ID を簡単に管理できるように設計されています。SCIM は、標準の REST API を使用します。

Azure アプリケーションギャラリーから Cisco Webex を追加する

最初の手順のトライアル作成中に O365 のユーザを 2 人作成しました。次に、Control Hub への同期に使用するアプリケーションを作成します。

1. https://portal.azure.com にアクセスし、O365 管理者としてログインします。
2. 上部の検索ボックスでエンタープライズ アプリケーション（Enterprise applications）を検索し、リストからエンタープライズ アプリケーションを選択します。
3. [新規アプリケーション（New Application）] をクリックします。
4. [ギャラリーから追加（Add from the gallery）] セクションで、**Cisco Webex** を検索します。
5. 検索結果で Cisco Webex を選択し、[追加（Add）] をクリックします。

ユーザ同期用に Azure AD を設定する

この手順に従って Azure AD からのプロビジョニングをセットアップし、自分の組織用のベアラートークンを取得します。この手順では、必須の管理設定や推奨の管理設定を説明します。

まず、Control Hub から自分の組織 ID を取得する必要があります。

1. Webex Control Hub に戻り、左側のメニューの下部にあるお客様名（**CbXXX.Dc-01.Com XXXXX LB Dcloud-Webex-Org**）をクリックします。
2. [情報（Info）] ページにリストされている[組織 ID（Organization ID）]をコピーします。
3. Azure ポータルに戻り、左側のメニューから [プロビジョニング（Provisioning）] を選択します。
4. ドロップダウンメニューを [自動（Automatic）] に変更します。
5. テナントの URL ボックスに https://api.ciscospark.com/v1/scim/{OrgId} と入力します。
    a. URL 内の **{OrgId}** を、先ほど取得した組織 ID に置き換えます。（例：https://api.ciscospark.com/v1/scim/1c618175-e42a-4101-acdd-3ee603811ab2 ）
6. 次の手順に従って**シークレットトークン**を取得します。
    a. 新しいブラウザタブまたはウィンドウで、https://idbroker.webex.com/idb/oauth2/v1/authorize?response_type=token&client_id=C4ca14fe00b0e51efb414ebd45aa88c1858c3bfb949b2405dba10b0ca4bc37402&redirect_uri=http%3A%2F%2Flocalhost%3A3000%2Fauth%2Fcode&scope=spark%3Apeople_read%20spark%3Apeople_write%20Identity%3ASCIM&state=this-should-be-a-random-string-for-security-purpose にアクセスします。
    b. プロンプトが表示されたら、Charles Holland（**cholland@cbXXX.dc-YY.com/dCloud123!**）でサインインします。
    c. [このサイトには接続できません（This site can’t be reached）] エラーページが表示されても無視します。これは正常な状態です。
    d. ブラウザのアドレスバーで、URL の文字列の **Token=** と **&token** の間にある **access_token** をコピーします。この生成されたベアラートークンは、365 日間有効です（その後、期限切れになります）。

アクセストークン

注：このトークンは、安全な場所に保管することをお勧めします。紛失したり、期限切れになったりした場合は、上記のプロセスを実施して新しいベアラートークンを取得する必要があります。

7. Azure ポータルに戻り、上記でコピーしたアクセストークンを [シークレットトークン（Secret Token）] ボックスに貼り付けます。
8. [接続テスト（Test Connection）] をクリックすると、テストに成功したメッセージが表示されます。
9. [通知メール（Notification Email）] ボックスに **cholland@cbXXX.dc-YY.com** と入力し、[障害発生時に電子メール通知を送信する（Send an email notification when a failure occurs）] チェックボックスをオンにします。
10. [保存（Save）] をクリックします。
11. [マッピング（Mappings）] セクションを展開します。
12. [Active DirectoryユーザをCisco Webexに同期する（Synchronize Azure Active Directory Users to Cisco Webex）] リンクをクリックして、デフォルトのマッピングを確認します。
13. デフォルトの設定のままでページの右上にある **X** をクリックし、[プロビジョニング（Provisioning）] ページに戻ります。

デフォルトのマッピング情報を使用し、設定を変更しないことをお勧めします。デフォルトでは、Azure AD の **userPrincipalName** は Control Hub の [電子メールアドレス（email）] にマッピングされます。変更を加えて元に戻す必要がある場合は、[デフォルトマッピングの再設定（Restart default mappings）] チェックボックスをオンにすれば、デフォルト設定に戻ります。

14. 下にスクロールし、[プロビジョニングステータス（Provisioning Status）] を [オン（On）] に切り替えます。
15. [範囲（Scope）] で、[割り当てられたユーザとグループのみ同期（Sync only assigned users and groups）]（デフォルト）を選択します（[範囲（Scope）] が表示されない場合：[保存（Save）] をクリックし、[プロビジョニング（Provisioning）] ページから一度移動して、また戻ります）。
16. [保存（Save）] をクリックします（可能な場合）。

Azure AD のアプリケーションにユーザを追加する

プロビジョニング範囲に全てのユーザとグループ（Sync all users and groups）を指定しなかった場合は、この手順に従って Webex Cloud と同期するユーザを選択します。このオプションを使用すると、Webex 組織内のすべてのアプリケーションにアクセスできるユーザのサブセットを作成できます。

Azure Active Directory は、割り当てと呼ばれる概念を利用して、選択したアプリケーションにアクセスできるユーザを判断します。自動ユーザプロビジョニングでは、Azure AD 内のアプリケーションに割り当てられているユーザ/グループのみが Control Hub に同期されます。

1. **Cisco Webex** アプリケーションの左側のメニューで [ユーザとグループ（Users and groups）] をクリックします。
2. [ユーザの追加（Add User）] をクリックします。

3. 最初の O365 トライアル版では、Azure の基本機能を利用できます。基本機能にはグループ割り当て機能は含まれていません。そのため、[グループ（Groups）] オプションに、[Active Directoryのプランレベルのため、グループに割り当ては適用できません（Groups are not available for assignment due to your Active Directory plan level）] という警告が表示されます。このラボでは、ユーザを個別に追加します。
4. [ユーザ（Users）] をクリックし、リスト内のすべてのユーザを選択します。Room デバイスを作成している場合は、Room デバイスは選択しないでください。
5. 各ユーザを選択したら、[選択（Select）] をクリックして [割り当て（Assign）] をクリックします。
6. ユーザは一定間隔で同期されます。デフォルトでは 40 分ごとです。強制的に同期するには、[プロビジョニング（Provisioning）] ページで [プロビジョニングステータス（Provisioning Status）] を [オフ（Off）] に切り替え、[保存（Save）] をクリックします。その後再度 [プロビジョニングステータス（Provisioning Status）] を [オン（On）] に切り替え、[保存（Save）] をクリックします。
7. プロンプトが表示されたら、[はい（Yes）] をクリックして同期を再起動します。
8. **更新**アイコン [ ] をクリックします。以前アプリケーションに追加したユーザの合計数が表示されます。[プロビジョニング詳細情報の表示（View provisioning details）]を展開すると、最後に完了したサイクルタイムが表示されます。
9. 同期が完了したら Control Hub に戻り、[ユーザ（Users）] をクリックします。これで、アプリケーションに追加された O365 ユーザがユーザリストに表示されます。

ユーザパスワードの設定

O365 の統合をテストするには、O365 から Control Hub に同期されたユーザのパスワードを設定する必要があります。

1. シナリオ 1 で自動割り当てテンプレートを作成した場合、メッセージングおよび会議サービスが自動的に設定されます。[保存（Save）] をクリック後、[終了（Finish）] をクリックします。自動割り当てテンプレートを設定していない場合は各ユーザを選択し、[編集（Edit）] をクリック後、**Webex Teams** 向け [メッセージング（Messaging）] 列と [会議（Meeting）] 列のすべてのボックスをオンにする必要があります。[保存（Save）] をクリック後、[終了（Finish）] をクリックします。
2. Webex アカウントをアクティブにするには、その**ユーザの O365 メールボックス**にログインする必要があります。
3. onmicrosoft.com アカウントにログインするには、https://outlook.office365.com/ に移動してログインします（別のブラウザまたはプライベート/シークレットモードを使用することをお勧めします）。
4. 現在いる場所の**タイムゾーン**を設定します。
5. 次に、Webex Teams アカウントをアクティブにするには、**シスコからの電子メール**を見つけて選択します。
6. 電子メール内の [有効化（Activate）] ボタンをクリックします。
7. パスワードを **dCloud123!** に設定し、[保存してサインイン（Save & Sign In）] をクリックします。
8. Webex Teams のアカウントを有効にするように設定した他のユーザについても、同じ手順を実行します。

O365 向けクラウドベース ハイブリッド カレンダー サービスの導入

Webex Teams は、O365 を使用してハイブリッド カレンダー サービスを利用できます。サービスの設定に Expressway-C コネクタホストは必要ありません。

Control Hub を O365 に接続する

1. Webex Control Hub で、[サービス（Services）] ページに移動します。
2. [ハイブリッドカレンダーOffice 365（Hybrid Calendar Office 365）] カードで [セットアップ（Set Up）] をクリックします。
3. [ハイブリッドカレンダー（Hybrid Calendar）] セットアップ画面で [許可（Authorize）] をクリックします。
4. O365 トライアル版のセットアップに使用する**管理者ユーザの onmicrosoft.com 電子メールアドレス**を入力し、[次へ（Next）] をクリックします。
5. プロンプトが表示されたら、作成した**パスワード**を入力し、[サインイン（Sign in）] をクリックします。
6. [承認（Accept）] をクリックして、**Webex Teams カレンダーサービス**へのアクセス許可を付与します。
7. セットアップした onmicrosoft.com ユーザのいずれかの電子メールアドレスを入力し、[テスト（Test）] をクリックします。
8. [完了（Done）] をクリックします。

O365 を使用したハイブリッド カレンダー サービスをユーザで有効にする

1. Control Hub の [ユーザ（Users）] ページに移動し、**O365 ユーザ**のいずれかを選択します。
2. [カレンダーサービス（Calendar Service）] をクリックします。
3. サービスをオンにし（[]）、[保存（Save）] をクリックします。
4. [カレンダーサービス（Calendar Service）] が [アクティブ（Activated）] になるまで待ちます（テストのために有効にする O365 アカウントは 1 つだけで構いません）。

O365 を使用したハイブリッド カレンダー サービスをデバイスで有効にする

O365 で Room デバイスを作成する

1. Microsoft 365 管理センター（admin.microsoft.com）に移動し、onmicrosoft.com 管理アカウントを使用してログインします。（リソースが表示されない場合はCutomize navigationで追加します。）
2. [すべて表示（Show all）] > [リソース（Resources）] > [部屋および機器（Rooms & equipment）] に移動し、[追加（Add）] をクリックします。

3. [タイプ（Type）] は [部屋（Room）] のままにします。
4. [名前（Name）] と [電子メール（Email）] を設定します。設定した電子メールアドレスを書き留めます。
5. [追加（Add）] をクリックし、追加が完了したら [閉じる（Close）] をクリックします。

Control Hub で場所を追加/編集する

6. Control Hub で [場所（Place）] に移動します。

注：次の手順では、すでに Control Hub にデバイスが追加されていることを前提としています。Control Hub にデバイスが追加されていない場合は、**[デバイスの追加（Add a Device）]** セクションに移動し、手順に従って新しいデバイスを追加します。デバイスが、Webex Edge for Devices シナリオの Unified CM に登録されたままの場合は、最初に作成した場所を削除し、新しい場所を作成してクラウドに登録します。デバイスを登録したら、次の手順に戻ります。手順を確認するだけの場合は、仮のデバイスを追加することもできます。

7. 以前作成した場所を選択し、ポップアップウィンドウで [編集（Edit）] をクリックします（Room デバイスを登録していない場合は、上記の注の手順に従ってください）。
8. [カレンダー（Calendar）] をオフに切り替えて、[保存（Save）] をクリックします（すでにオフになっている場合は、[カレンダー（Calendar）] をオンに切り替え、[次へ（Next）] をクリックして、次の手順をスキップします）。
9. [編集（Edit）] をもう一度クリックし、再び [カレンダー（Calendar）] をオンに切り替えて [次へ（Next）] をクリックします。
10. このセクションの冒頭で設定した O365 ルームリソースの [電子メールアドレス（email address）] を入力し、[保存（Save）] をクリックします。
11. [カレンダーサービス（Calendar Service）] が [アクティブ（Activated）] になるまで待ちます。

O365 を使用したハイブリッド カレンダー サービスのテスト

1. https://outlook.office365.com/ にアクセスし、以前カレンダーサービスを有効にしたユーザでログインします（このページはすでに開いているはずですが、開いていない場合は、別のブラウザまたはプライベート/シークレットモードを使用することをお勧めします）。
2. カレンダーに移動し、[新規イベント（New event）] を作成します。
3. [件名（Title）] を入力します。
4. OBTP については、[参加者の招待（Invite attendees）] フィールドをクリックし、Room デバイスの名前を入力して選択します。また、[招待（invite）] ボックスに 2 人以上のユーザを追加します。
5. 現在のタイムゾーンに基づいて今日の開始時刻（先の時刻）を設定します（タイムゾーンは Outlook に初めてログインしたときに設定しています。タイムゾーン アイコンをクリックして設定することもできます）。OBTP と会議通知が機能するように、10 分以上先の時間を設定します。

6. [場所（Location）] フィールド（ ）に、**@webex:space** または **@meet** などのスケジューリングキーワードのいずれかを入力します。詳細なリストはこちらで確認してください。
7. [送信（Send）] をクリックします。
8. create-a-space キーワードのいずれかを使用した場合は、O365 ユーザで **Webex Teams クライアント**（https://teams.webex.com などの Web クライアント）にログインし、スペースが作成されたことを確認します。また、カレンダーの招待状に参加情報の詳細が表示されていることも確認できます。
9. Webex Teams アプリで参加通知を受信したら（スケジュールした会議の 6 分前）、[通知（notification）]、[ビデオで参加（Join With Video）] の順にクリックします。
10. Room デバイスで、ユーザがすでにミーティングに参加していることがわかります。[参加（Join）] をタップして、進行中の会議に直接参加します。
11. 完了したら、会議を終了します。

ここまでで、キーワード機能を使用したクラウドベースの O365 ハイブリッド カレンダー サービス、およびワンボタン機能、会議リスト、参加通知のテストができました。

O365 を使用したエンタープライズコンテンツ管理（ECM）のテスト

このセクションの冒頭で、ユーザが Webex Teams を使用して O365 アカウントに接続し、OneDrive または SharePoint を使用してコンテンツを共有/編集できるように、すべての設定を完了しました。O365 トライアル版を作成した場合は、Microsoft 社側で OneDrive および SharePoint のセットアップが完了したことを確認する必要があります。準備ができたかどうか確認するには、O365 管理センター（**admin.microsoft.com**）に移動して、メニューアイコン [ ] をクリックします。[設定中...（Setting up...）]（OneDrive [Setting up...] または SharePoint [Setting up...]）が表示された場合は、ECM セクションはまだ実施できません。OneDrive や SharePoint を使用する準備ができても、まだユーザは自分のアカウントに接続してファイルを共有することはできません。まず、O365 Word ドキュメントを作成し、後で使用するために OneDrive に保存します。

テスト用に SharePoint サイトと Word ドキュメントを作成する

1. https://www.office.com に移動し、O365 管理者アカウントでサインインします（理由は後で説明します）。
2. [SharePoint] をクリックし、コーチマークが付いている箇所を自由に確認します。次のページで [サイトの作成（Create site）] をクリックします。
3. [Teamサイト（Team site）] を選択し、サイト名と説明を入力します。
4. プライバシー設定については、[パブリック（Public）] を選択します。組織内の誰でもこのサイトにアクセスできます。
5. [次へ（Next）] をクリックします。
6. 追加の所有者として他のユーザを追加し、[完了（Finish）] をクリックします。

7. コーチマークの箇所を確認したら、左側のメニューで [ドキュメント（Document）] をクリックします。
8. [新規（New）] > [Wordドキュメント（Word document）] をクリックします。
9. ドキュメントにテキストを追加します。ドキュメントは自動的に保存されます。ドキュメント名を変更するには、上部の中央にある [ドキュメント（Document）] で名前をクリックして、新しい名前を入力します。

ドキュメントの編集が完了したら、O365 ユーザ、およびドキュメントの共有/編集ができる別のユーザで Webex Teams デスクトップクライアントにサインインする必要があります。ラボ内の Workstation 1 と 2 で Webex Teams クライアントを使用してテストできます。すでに Charles や Anita でサインインしている場合は、この時点でサインアウトして O365 アカウントでサインインします。

10. **Workstation 1** にて 新しいブラウザタブで、[Cisco Webex Links] > [Download Cisco Webex Teams Desktop Client] の順に移動します。
11. [Download Cisco Webex Teams Desktop Client] をクリックし、Webex Teams クライアントをダウンロード、インストールします。
12. Workstation 1にインストール済みのクライアントはバージョンが古いためこの手順を実施ください。
13. Workstation 2も同様にWebex Teams クライアントをインストールします。
14. **Workstation 1** で Webex Teams にログインした後、**ユーザのアバターサークル**をクリックし、メニューから [設定（Settings）] を選択して、O365 アカウントに接続する必要があります。
15. [アカウント（Accounts）] をクリック後、[アカウントの追加（Add account）] をクリックします。
16. 先にドキュメントを作成した **O365 ユーザ**でログインします。
17. [組織を代表して同意する（Consent on behalf of your organization）] の横にあるチェックボックスをオンにし、[同意（Accept）] をクリックします。

注：O365 管理者はすべてのユーザのアクセス許可に同意できるため、ログイン時にプロンプトは表示されません。ボックスがオンになっていない場合は、すべてのユーザがアクセス許可を受け入れる必要があります。O365 管理者だけに組織の代表として同意するボックスが表示されます。

18. 認証が完了すると、自分のクラウドアカウントが表示されます。[保存（Save）] をクリックします。
19. 他の O365 ユーザを使用して Webex Teams スペースを作成し、会話を開始します。
20. **ペーパークリップ**をクリックし、[OneDriveまたはSharePointからオンラインで共有（Share from OneDrive or SharePoint Online）] を選択します。
21. **ユーザアカウント**をクリックします。
22. [組織を代表して同意する（Consent on behalf of your organization）] の横にあるチェックボックスをオンにし、[同意（Accept）] をクリックします。ユーザにはアクセス許可への同意を求めるプロンプトは表示されません。
23. [共有ライブラリ（Shared Libraries）] で、SharePoint で作成したサイトをクリックし、**ドキュメント**を選択して [開く（Open）] をクリックします。

24. [組織内のユーザ（People in your organization）] は選択したままにします。
25. [編集を許可（Allow editing）] の横にあるチェックボックスをオンにし、[適用（Apply）] をクリックします。
26. Enter を押して、ドキュメントをスペースに送信します。
27. Workstation 2 で別の O365 ユーザを利用して Webex Teams にサインインするか、別のブラウザで Web クライアント（teams.webex.com）を使用します。

ドキュメントを編集するには、このユーザが Webex Teams の O365 に接続する必要があります。

28. スペース内のドキュメントをクリックします。[アカウント（Account）] ウィンドウが開き、O365 アカウントに接続できるようになります。
29. [アカウントの追加（Add account）] をクリックし、他の O365 ユーザでサインインします（今回はアクセス許可への同意を求めるメッセージは表示されません）。
30. クラウドアカウントが表示されたら、[保存（Save）] をクリックします。
31. 次に、スペース内のドキュメントをもう一度選択します。今度は、ドキュメントを編集するために開きます。
32. 必要に応じてドキュメントを編集します。
33. Workstation 1 に戻り、**ドキュメントの編集内容**を確認します。すべてのユーザの編集内容をリアルタイムで確認できます。

SharePoint で作成したサイトをこのスペースにリンクすることもできます。

34. Webex Teams アプリの上部の [コンテンツ（Content）] タブをクリックします。
35. [ファイル（Files）] が選択されている状態で [オンラインフォルダにリンク（Link to Online Folder）] をクリックします。
36. プロンプトが表示されたら、自分の O365 アカウントを選択してパスワードを入力します。
37. ログイン後、[共有ライブラリ（Shared Libraries）] で SharePoint サイト名を選択し、[開く（Open）] をクリックします。
38. [閉じる（Close）] をクリックします。
39. [ファイル（files）] エリアには 2 つのオプションがあります。1 つは [スペースで共有（Shared in space）] で、Webex Cloud ストレージが利用されます。もう 1 つは [フォルダのリンク（Linked folder）] で、SharePoint サイトがストレージに利用されます。[フォルダのリンク（Linked folder）] をクリックします。

SharePoint で先に作成したドキュメントが表示されます。

O365 を使用したエンタープライズコンテンツ管理のテストが完了しました。

Microsoft Teams から Cisco Webex Meetings のスケジューリング、開始、参加を行う

Cisco Webex Meetings アプリを使用してユーザを Webex Meetings に招待すれば、会議に簡単に参加できます。必要なのは、チームが会議に使用する Webex サイトの URL を設定することだけです。このアプリを使用するには、該当の Webex サイトのホストアカウントを持っている必要があります。Webex アカウントがパーソナルルームで有効になっている場合は、このアプリを使用して自分のパーソナルルームの会議へのリンクを共有できます。

Microsoft Office 365 で Cisco Webex Meetings アプリを利用できるようにする

チームの所有者とメンバーが Microsoft Teams ストアで Cisco Webex Meetings アプリを確認してインストールできるようになるためには、Microsoft Office 365 のグローバル管理者が次の手順を実行してアクセス許可を付与する必要があります。

1. **Microsoft Teams 管理センター**（admin.teams.microsoft.com）に移動し、自分の **onmicrosoft.com 管理アカウント**を使用してログインします。
2. [Teams アプリ（Teams apps）] > [アクセス許可ポリシー（Permission policies）] に移動します。
3. [組織全体のアプリ設定（Org-wide app settings）] をクリックし、[サードパーティ製アプリを許可する（Allow third party apps）] がオンになっていることを確認します。このスイッチをオフにすると、すべてのサードパーティ製アプリが無効になります。Microsoft Teams でサードパーティ製アプリが許可されていることを確認します。

Cisco Webex と Microsoft Office 365 を統合するためのサイト設定

1. Control Hub で [サービス（Services）] ページに移動し、[会議（Meeting）] カードの [サイト（Sites）] をクリックします。
2. 後で確認できるようサイトの URL を書き留めてから、**サイトの URL** をクリックします。ポップアップウィンドウで [サイトを構成する（Configure Site）] をクリックします。
3. [共通設定（Common Settings）] で [サイトオプション（Site Options）] をクリックします。
4. [サードパーティの連携（Third-Party Integration）] で、[ユーザーのWebexアカウントメールアドレスとMicrosoft Office 365メールアドレスと一致する場合、ユーザーとこのWebexサイトを自動的につなげる（Automatically link users with this Webex site if their Webex account email address matches their Microsoft Office 365 email address）] をオンにします。
5. [新規権限の追加（Add New Authorization）] をクリックします。
6. O365 admin でサインインしたら、[同意する（Accept）] をクリックしてアクセス許可を付与します。
7. アクセス許可を追加したら [更新（Update）] をクリックします（更新が完了するまで最大 5 分かかります）。

Microsoft Teams で Cisco Webex Meetings を使用できるように設定する

管理タスクが完了したので、ユーザは Microsoft Teams 内で Cisco Webex Meetings アプリを使用できるようになりました。Microsoft Teams を設定する必要があります。ラボでは、Microsoft Teams Web アプリを使用します。

1. Web ブラウザで teams.microsoft.com に移動し、Office 365 管理者ユーザでサインインします。
2. コーチマークの箇所を確認したら、左側のメニューで [Teams] をクリックします。
3. [チームに参加、もしくはチームを作成（Join or create a team）]をクリック後、[チームの作成（Create team）] をクリック後、[最初からチームを構築（Build a team from scratch）] をクリックします。
4. [パブリック（Public）] を選択します。
5. チームに名前を付けて、[作成（Create）] をクリックします。
6. チームが作成されたら、前に作成した他のユーザを追加します。
7. ユーザの追加が完了したら [閉じる（Close）] をクリックします。
8. メインウィンドウで、**タブの追加**アイコン [+] をクリックして新しいタブを開きます。
9. Cisco Webex Meetings アプリを検索して選択します。
10. ポップアップウィンドウで [追加（Add）] をクリックします。次のウィンドウで [保存（Save）] をクリックすると、

新しい **Webex** タブが開きます。チャットは自分のアカウントと Cisco Webex Meetings ボットの間でも開始されます。チャットに移動して、チャットに「**help**」と入力すればコマンドを確認できます。

Webex サイトがまだチームに設定されていないことを示すメッセージが上部に表示されます。次の手順の指示に従います。

11. [投稿（Posts）] タブをクリックします。
12. [新しい会話を開始する（Start a new conversation）] ボックスの下部に **@Cisco Webex Meetings site cbXXXYY.webex.com** と入力します（URL が以前 Control Hub で取得した内容と一致していることを確認します）。
13. ボットがメッセージに実際に記載されていることを確認し、チームにメッセージを送信します。
14. 送信に成功すると、Webex サイトを cbXXXYY.webex.com に変更したことを示すメッセージが表示されます。
15. **Webex** タブに戻り、Webex ルームの詳細が表示されていることを確認します。これで会議を開始できるようになりました。
16. このタブを使用して、インスタント会議を開始したり、会議のスケジュールを設定したりしてみてください。
17. チャネルの [会話（Conversations）] タブ内で **@Cisco Webex Meetings** を使用して、コマンドを実行することもできます。

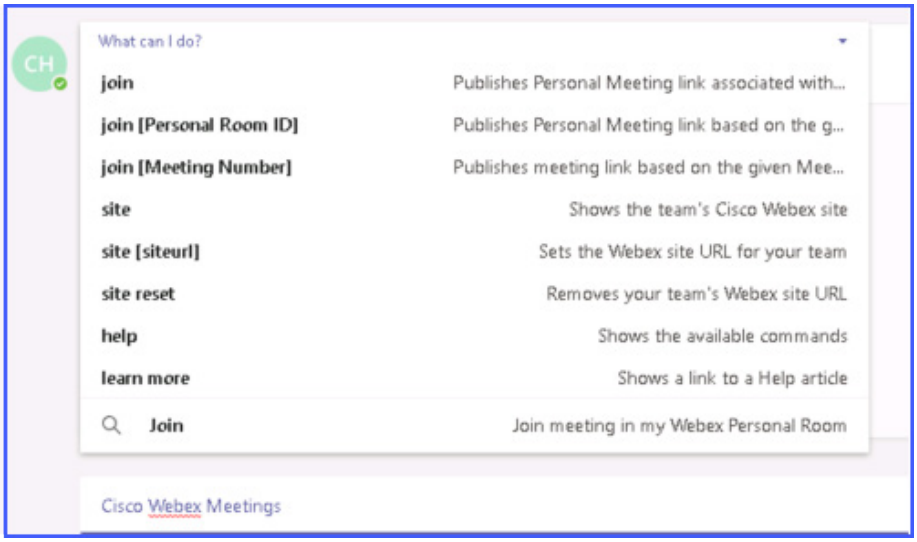
これで、チームに属するすべてのユーザにも同じ Webex タブが作成されました。ラボの他のワークステーションで別のブラウザを開き、別の O365 ユーザで **teams.microsoft.com** にログインすれば Webex タブを確認できます。新しいタブ [Webex New] として表示されます。[一般（General）] チャネルにタブが追加されています。さらにチャネルが必要な場合は、同じ手順でタブを追加できます。

18. Webex タブを追加したチャネルのいずれかで [投稿（Posts）] タブを選択します。

19. チャットボックスに **@Cisco Webex Meetings** と入力し、ボットが表示されたら選択します。

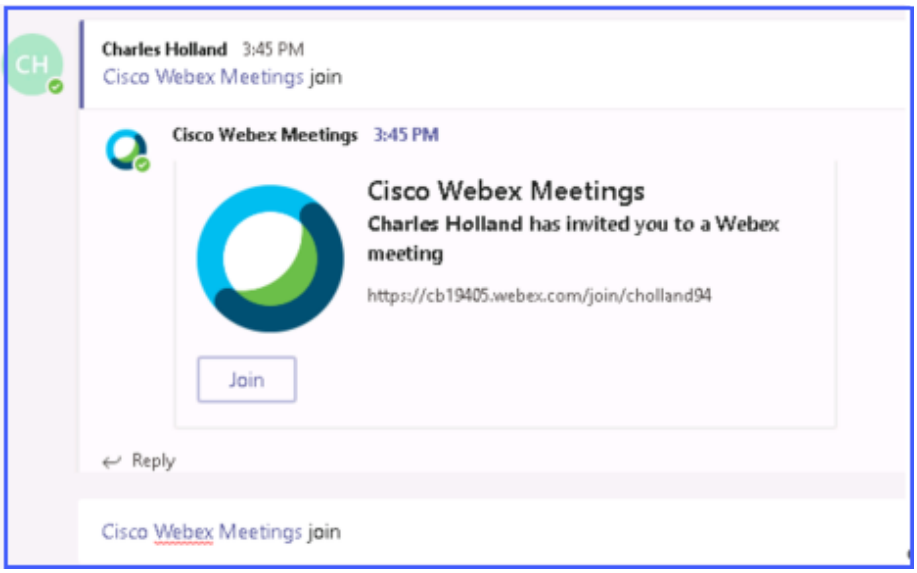
20. ボットを選択した後、[実行できるコマンド（What can I do）] をクリックすれば、コマンドのリストが表示されます。

ボットコマンド



リストされているどのコマンドでも、コマンドをクリックするか、ボックスに入力して自由にテストできます。**join** コマンドを試してみましょう。このコマンドにより、すべてのユーザが会議に簡単に参加できる [参加（Join）] ボタンとチャットへのリンクが表示されます。

Webex Meetings に参加する



シナリオ 9. Webex ハイブリッド メッセージ サービスの設定

このサービスは、組織の Cisco Webex Teams ユーザが、Cisco Unified Communications Manager IM and Presence（UCM IM&P）サービスで他のユーザとメッセージを交換する必要がある場合に最適です。ハイブリッド メッセージ サービスにより、Cisco Webex Teams クライアントと Unified CM IM and Presence サービスに登録されている Cisco Jabber クライアントとの間で 1 対 1 のインスタントメッセージを交換できます。ハイブリッド メッセージ サービスを利用すれば、Cisco Jabber ユーザが、Cisco Webex Teams クライアントのアクティビティに基づいて Teams ユーザのプレゼンスステータスを確認できます。

Webex ハイブリッドメッセージングの概要とセットアップガイドは、こちらを参照してください。

メッセージコネクタの有効化

1. Cisco Webex Control Hub を再度オープンします。ラボ内のWorkstation1から実行する必要があります。
2. 管理ポータルに戻ります。[サービス（Services）] タブの [ハイブリッドメッセージ（Hybrid Message）] カードで [セットアップ（Set Up）] をクリックします。
3. [ハイブリッドメッセージサービスのセットアップ（Hybrid Message Service Setup）] ポップアップウィンドウで [次へ（Next）] をクリックします。
4. [既存のExpresswayクラスタを選択してこのサービスにリソースを追加する（Select an existing Expressway cluster to add resources to this service）] を選択します。ドロップダウン リスト ボックスを使用して [HS Cluster 1] を選択します（これはカレンダーサービスのシナリオで指定した名前です。別の名前を付けた場合は、その名前を選択してください）。

注：ハイブリッド カレンダー セクションをスキップした場合は、新しい Expressway をここで登録する必要があります。これはすでにハイブリッド カレンダー セクションで完了しています。Expressway を登録するには、最初のオプションボタンを選択し、ボックスに exp-cc.dcloud.cisco.com と入力して [次へ（Next）] をクリックします。最後に名前として HS Cluster 1 と入力します。登録したら以下の手順を続行できます。

5. [次へ（Next）] をクリックします。
6. [Expresswayに進む（Go to Expressway）] をクリックします。
7. 次の情報を使ってログインします。
   - ユーザ名：**admin**
   - パスワード：**dCloud123!**

注：繰り返しになりますが、ハイブリッド カレンダー セクションをスキップした場合は、新しい Expressway をここで登録する必要があります。これはすでにハイブリッド カレンダー セクションで完了しています。Expressway を登録するには、[この信頼に必要なExpressway CA証明書はシスコが管理する（I want Cisco to manage the Expressway CA certificates required for this trust）] のチェックボックスをオンにし、[ソフトウェアの更新及び接続の検証（Update softeware & verify connection）] をクリックします。次に、[登録（Register）] をクリックします。次の画面で、[Expresswayへのアクセスを許可（Allow Access to the Expressway）] チェックボックスをオンにし、[続行（Continue）] をクリックします。

すぐに [メッセージコネクタ（Message Connector）] がリストに表示されます。[サービスステータス（Service Status）] が [未インストール（Not installed）] から [インストール中（Installing）] に変わり、最後に [未設定（Not configured）] になります。Expressway ホストのサービスステータスが [未設定（Not configured）] になったら、メッセージコネクタが正常にダウンロードされ、インストールされたことを示しています。

メッセージコネクタ用のアプリケーションアカウントの設定

メッセージコネクタを利用するには、アプリケーションユーザを作成し、**標準 AXL API アクセス**権限を設定する必要があります。メッセージコネクタは、このアカウントを使用して Unified CM IM and Presence サービスと通信します。このラボでは、このユーザは事前に作成されています。付録 B に、このユーザを作成して権限を割り当てる手順を示しています。このユーザには、コールサービスでも使用される他の権限も設定します。ハイブリッド メッセージング サービスに必要なのは、前述の 1 つのロールのみです。

IM and Presence サービスへの接続の設定

ハイブリッド メッセージ サービスを有効にするには、パブリッシャノードのサーバ情報を入力して、メッセージコネクタを IM and Presence サービスクラスタにリンクする必要があります。この手順では、IM and Presence サービスと Cisco Webex Cloud 間にブリッジを作成し、コネクタを 2 つの間のブローカーとして機能させます。

Expressway のコネクタは、ハイブリッド メッセージ サービス クラスタとクラウド間で復元力のある接続を維持します。必要なのは、Expressway-C コネクタの設定にパブリッシャを追加することだけです。特定のノードがクラスタ内でダウンした場合、コネクタは別のサーバに移動します。

1. [コネクタの管理（Connector Management）] ページで、[IM and Presenceサーバの設定（Configure IM and Presence Server）] リンクをクリックします。[アプリケーション（Applications）] > [ハイブリッドサービス（Hybrid Services）] > [メッセージサービス（Message Services）] > [メッセージサービスの設定（Message Service Configuration）] の順に移動することもできます。
2. [新規（New）] をクリックします。
3. 以下の表に従ってパラメータを設定します。

表 36.　Edge Audio Expressway-E トラバーサルサーバゾーンの設定

設定対象	設定内容
IM and Presence パブリッシャノードのアドレス	cup1.dcloud.cisco.com
メッセージコネクタ AXL アカウント名	webex
メッセージコネクタ AXL アカウントパスワード	dCloud123!

4. [追加（Add）] をクリックします。
5. [メッセージコネクタが実行されていないため、ステータス情報はありません（Message Connector is not running, No status info available）] リンクをクリックします（[アプリケーション（Applications）] > [ハイブリッドサービス（Hybrid Services）] > [メッセージサービス（Message Service）] > [メッセージサービスの概要（Message Service Overview）] でも確認できます）。
6. [アクティブ（Active）] 設定で [有効（Enabled）] を選択し、[保存（Save）] をクリックします。
7. [アプリケーション（Applications）] > [ハイブリッドサービス（Hybrid Services）] > [メッセージサービス（Message Services）] > [メッセージサービスのステータス（Message Service Status）] の順に進みます。

[ノードのステータス（Node Status）] は、[動作中（Operational）] になっています。動作中でない場合は、サービスが動作中になるまで待ちます。ページを更新して、更新されたステータスを確認します。

ユーザのハイブリッド メッセージ サービスの有効化

ユーザがハイブリッド メッセージ サービスを利用できるようにするには、該当のユーザでサービスを有効にする必要があります。ラボでは、Anita Perez でこのサービスを有効にします。実稼働環境では、CSV テンプレートを使用して複数のユーザで一度に有効にすることができます。

1. Control Hub のタブを開き、必要に応じてログインします（**cholland@cbXXX.dc-YY.com/dCloud123!**）。
2. [ユーザ（Users）] タブをクリックし、リストから [Anita Perez] を選択します。
3. [ハイブリッドサービス（Hybrid Services）] で [メッセージサービス（Message Service）] をクリックします。
4. [ハイブリッドメッセージサービス（Hybrid Message Service）] をオン（  ）に切り替えて、[保存（Save）] をクリックします。
5. メインのユーザページで、[メッセージングサービス（Messaging Service）] のステータスが [アクティブ（Activated）] に変わるまで待ちます。

ハイブリッド メッセージ サービスのテスト

1. 次のログイン情報を使用して Workstation 2（**198.18.1.37**）に接続します。
   - ユーザ名：**dcloud\aperez**
   - パスワード：**dCloud123!**

2. Workstation 2 で **Webex Teams** クライアントを開き、次のログイン情報でログインします（O365 ユーザでログインしている場合はログアウトします）。
   - ユーザ名：**aperez@cbXXX.dc-YY.com**
   - パスワード：**dCloud123!**
3. Workstation 1 で **Cisco Jabber** を開きます（開いていない場合）。電子メールアドレス **cholland@cbXXX.dc-YY.com** を入力してから、ユーザ名/パスワードとして **cholland/dCloud123!** を入力します。
4. Anita の Webex Teams クライアントから Charles と **1 対 1 の会話**を始めます。Charles にメッセージを送ります。
5. Workstation 1 に戻ると、Charles の Jabber クラウドに、Anita からのメッセージが表示されています。Anita に返答します。また、Anita のステータスが @ Cisco Webex Teams になっていることも確認します。

ユーザが Webex Teams から Cisco Jabber に確実にメッセージを送信できるようになるまでに、最大 1 時間かかる可能性があることに注意してください。テストを実施できなければいったんスキップし、後で戻ってから再開することもできます。

シナリオ 10.　Jabber チームメッセージングモード

この導入オプションでは、お客様のコーリングサービスをオンプレミスで維持しながら、クラウドの Webex Teams メッセージング機能のコアセットを利用できます。お客様は、Jabber アプリケーションで永続的な 1 対 1 のチャットとチームスペース、新しいプレゼンスエクスペリエンス、高度なファイル共有機能、優れた検索機能を利用できます。ユーザが使い慣れている高度なコール機能もそのまま利用できます。さらに良い点として、お客様はオンプレミスのコーリング インフラストラクチャを変更する必要はありません。

チームメッセージングモードには、シスコのお客様第一の姿勢が表れています。このモードでは、お客様の Jabber 環境で新しいチームワークフローを実現できます。Webex プラットフォームの機能を活用して既存のソリューションと統合し、独自のエクスペリエンスを提供します。IT 管理者は、オンプレミスまたはパートナーが管理するコールサービスを活用しながら、クラウドによる新たなエクスペリエンスを提供できます。また、Jabber チームメッセージングモードと Webex Teams は同じクラウドプラットフォームを利用しているため、ネイティブで相互に運用できるというメリットもあります。無理に移行する必要はなく、ユーザが孤立することもありません。シスコが重視しているのは、移行することではなく、クラウドの進化によって生産性の高いユーザワークフローを実現することです。

Jabber のお客様に提案しましょう。チームメッセージングモードを使用してメッセージングをクラウドに移行する方法について検討を始めます。お客様は、メッセージング機能をクラウドに移行することで最新のメッセージング エクスペリエンスのメリットを得ながら、メンテナンスの手間も削減できます。

チームメッセージングモードに含まれている新機能については、こちらからビデオをご覧ください。

Kellie のメッセージングサービスの有効化

1. 次のログイン情報を使用して Workstation 3（**198.18.1.38**）に接続します。
   - ユーザ名：**dcloud\kmelby**
   - パスワード：**dCloud123!**
2. 次のログイン情報で Cisco Jabber を開きます。
   - 電子メール：**kmelby@cbXXX.dc-YY.com**
   - ユーザ名：**kmelby**
   - パスワード：**dCloud123!**

現在 IM and Presence に接続している Kellie には、グループ内のものも含め、多数の連絡先が設定されています。移行時に、これらの連絡先も Webex Teams に移行されます。

3. Webex Control Hub（admin.webex.com）を開き、必要に応じてログインします（**cholland@cbXXX.dc-YY.com/dCloud123!**）。
4. [サービス（Services）] に移動し、[メッセージ（Message）] カードの [設定（Settings）] リンクをクリックします。
5. ページの下までスクロールし、[Jabberチームメッセージングモードを有効にしますか（Enable Jabber team messaging mode）] をオンにします。

注：内部音声サービスドメインが Control Hub に設定されているドメインと異なる場合、最初のボックスをオフにする必要があります。ラボでは、Jabber が Webex Teams ドメインを使用するように設定されています。cbXXX.dc-YY.com で Jabber にログインし、Jabber クライアントに音声サービスドメインを設定します。

6. 両方のボックスをオンにして、[完了（Finish）] をクリックします。
7. [ユーザ（Users）] ページに移動し、リストから [Kellie] を選択します。
8. [サービス（Services）] で [メッセージング（Messaging）] をクリックします。
9. リストされている3 つの切り替えボタン、[Jabberチームメッセージングモードを有効にしますか（Enable Jabber team messaging mode）]、[連絡先の移行が必要です（Contact Migration Required）]、[Jabber通話を有効にする（Enable Jabber calling）] をオンにします。
10. [保存（Save）] をクリックします。
11. Workstation 3 の Kellie で Jabber を終了し（歯車アイコン [⚙] をクリックして [終了（Exit）] を選択）、再度開きます。
12. 実行スピードを上げるため、歯車アイコン [⚙] をクリックし、[ヘルプ（Help）] > [設定の更新（Refresh configuration）] を選択して、[OK] をクリックします。
13. 設定を更新した後 5 分以内に、設定の変更が検出されたことを示す Jabber ポップが Kellie に表示されます。ポップアップが表示されたら、[サインアウト（Sign out）] をクリックします。

チームメッセージングモードで Jabber を使用する

1. Jabber をサインアウトしたら、[サインイン（Sign In）] をクリックします。

Jabber が再開すると、Webex Teams のサインイン画面が表示されます。

2. Kellie の Webex Teams パスワード（**dCloud123!**）を入力し、[サインイン（Sign In）] をクリックします。

[連絡先の移行が必要です（Contact Migration Required）] をオンにしているため、Kellie には連絡先を移行することを示すポップアップが表示されます。

3. [OK] をクリックします。

下部に**コール設定通知 [** **]**が表示されています。SSO はまだ実装されていないため、Unified CM のオンプレミスログイン情報を入力してコール機能を再開する必要があります。

4. Kellie のアバターをクリックし、[設定（Settings）] を選択します。
5. 左側のメニューから [アカウント（Accounts）] を選択します。
6. ユーザ名/パスワードに **kmelby/dCloud123!** と入力し、[適用（Apply）] をクリックします。
7. 更新が正しく適用されたら、[OK] をクリックします。

更新後、すべてのグループと連絡先がそのままの状態であることを確認します。変更の影響を把握するため、この新しいモードで Jabber の操作をテストします。以下を試すことができます。

- Anita とチャットで会話する。
- Kellie の Jabber でコールし、Anita の Teams クライアントに新しいプレゼンスステータスが表示されるのを確認する。
- Jabber で、[+] アイコンを使用して複数のユーザが参加する新しいチームスペースを作成する。
- Contactsグループ名の上に移動して**チャットボタン** [] をクリックし、Jabber グループの新しいスペースを簡単に作成する。

セクションの最初で示したこちらのビデオで、このモードの新機能の概要を把握できます。他のワークフローも自由に試してください。

シナリオ 11.　Webex Teams クライアントの機能

このシナリオでは、Cisco Webex Teams クライアントの新機能をいくつか説明します。このシナリオでは自分のクライアントを使用できますが、手順では Charles と Anita のワークステーションにインストールしたクライアントを利用します。

Workstation 1 と 2にて新しいブラウザタブで、[Cisco Webex Links] > [Download Cisco Webex Teams Desktop Client] の順に移動します。[Download Cisco Webex Teams Desktop Client] をクリックし、Webex Teams クライアントをダウンロード、インストールします。Workstation 1にインストール済みのクライアントはバージョンが古いためこの手順を実施ください。

Webex Teams の最新機能については、https://help.webex.com/ja-jp/8dmbcr/What-s-New-in-Cisco-Webex-Teams を確認してください。

Webex でプレゼンスステータスが変わると、それに応じてアバターも変わります。アバターの各状態の意味については、https://help.webex.com/ja-jp/wghlt5/Webex-Teams-See-People-s-Availability を参照してください。

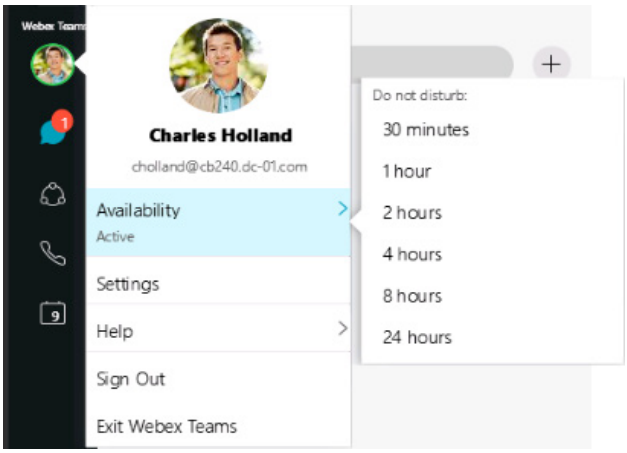
注：現在、プレゼンスステータスは自分の組織内の人しか見られません。

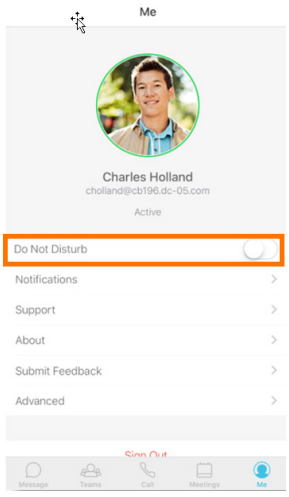
プレゼンス：応答不可（DND）

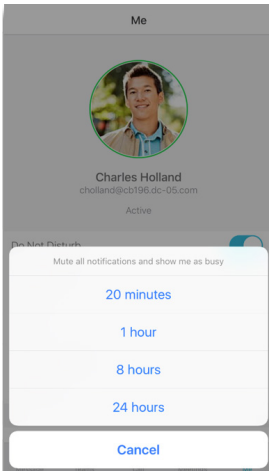
アクティブになってからの時間を示すアクティブステータスに加えて、デスクトップまたはモバイルアプリから DND を設定できるようになりました。

1. まだ設定していない場合は、Workstation 1 で Charles のアカウント：**cholland@cbXXX.dc-YY.com**、パスワード：**dCloud123!** を使用して、Cisco Webex Teams にログインします。
2. Anita とのスペースが作成されていない場合は、[＋] ボタンをクリックし、Anita との 1 対 1 のスペースを開始します。[ユーザに連絡する（Contact a Person）] をクリックし、Anita を検索してスペースに追加します。
3. Anita にメッセージを送信します。
4. Charles の Cisco Webex Teams デスクトップクライアントで Charles のアバターをクリックすると、ステータスが [アクティブ（Active）] と表示されます。[状況（Availability）] をクリックすると、DND タイマーを設定できることがわかります。DND タイマーは、すべてのユーザが確認できます。DND タイマーをモバイルクライアントで設定するには、[自分の情報（Me）] アイコンをタップして [アクティブ（Active）] 切り替えボタンをタップします。

デスクトップおよびモバイル用 DND タイマー







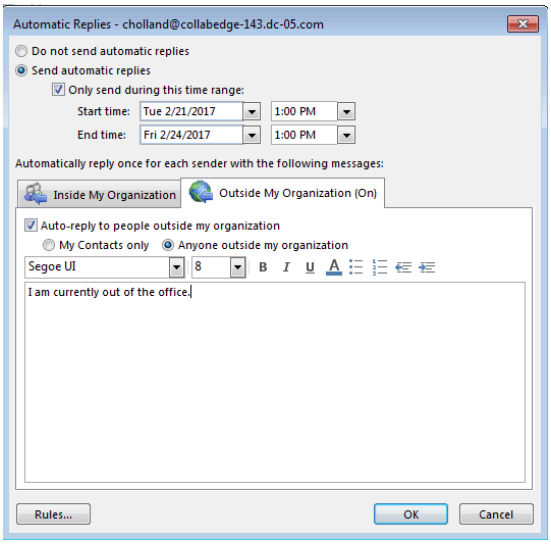
プレゼンス：不在（Out of Office:OoO）

先にラボで設定したカレンダーコネクタを使用すると、Outlook から Webex に不在ステータスを反映させることができます。

注：この機能を利用できるのは、組織内でカレンダーサービスが有効になっていて、ユーザでカレンダーサービスがアクティブになっている場合のみです。

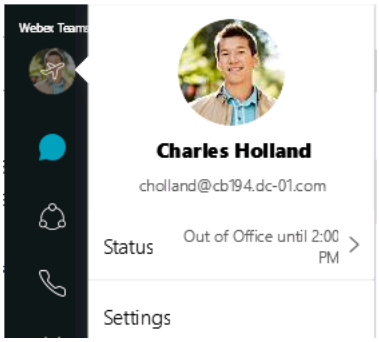
1. Workstation 1 で **Outlook** を開きます。
2. 左上にある [ファイル（File）] タブをクリックします。
3. [自動応答（Automatic Replies）] をクリックします。
4. [応答を自動送信する（Send automatic replies）] オプションボタンを選択します。
5. [次の期間のみ送信する（Only send during this time range）] の横のチェックボックスをオンにします。
6. まだ設定していない場合は、[開始時刻（Start time）] を過去の時刻に設定します（今すぐ有効にするため）。
7. [終了時刻（End time）] に先の時刻を設定します。
8. 下部にあるボックスに、「現在不在にしています」などの**テキスト**を追加します。
9. [組織外向け（Outside My Organization）] タブをクリックします。
10. ここでもボックスに**テキスト**を追加します。
11. [OK] をクリックします。

OoO の設定



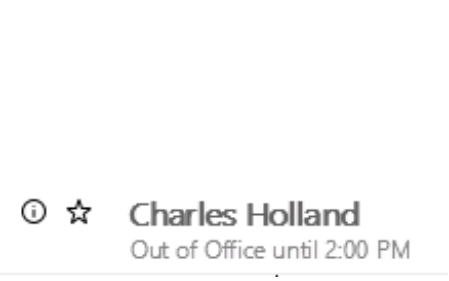
12. Charles の Webex Teams クライアントに戻ります。Webex Teams で、検索、@mentions、1 対 1 のスペースへのアクセスなどのアクションを実行すると、OoO チェックがトリガーされます。設定を変更すると、[設定した終了時刻の1分前まで不在（Out of Office until one minute before the end time you set）] と表示されます。時間範囲を設定していない場合、ステータスは [不在（Out of Office）] とだけ表示されます。スペースを使用して Anita にメッセージを送信することで、OoO の変更をトリガーします。OoO の設定が Webex Teams に反映されるまで数分かかる場合があります。

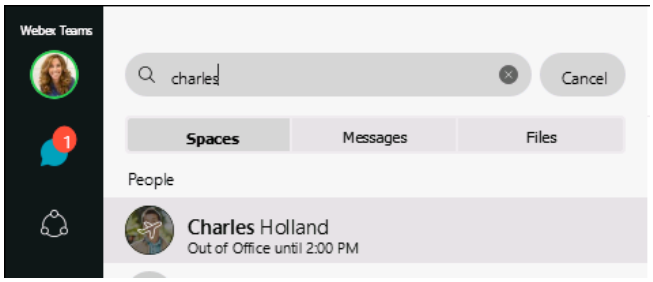
Charles の OoO



13. Anita とのスペースに移動し、Anita にメッセージを送信します。送信すると自分のステータスが変わることを確認できます。変わらなければ、数分待ってから再試行してください。
14. Workstation 2 に移動して、Charles とのスペースにアクセスします。Charles の名前を検索したときと同じように、ここでもステータスが設定されます。

Charles の OoO





Cisco Webex Space Meetings のスケジュール設定

Cisco Webex Teams では、日時がスケジュール済みの会議にスペース内の全員を招待することができます。Microsoft Outlook 用の会議招待状を作成するか、すでに作成済みの場合は、カレンダーに会議情報をコピーすることができます。

Outlook または別のカレンダーで招待状を作成して電子メールアドレスを追加すれば、スペースのメンバーではないユーザも招待できます。スペースのメンバーではないユーザが会議に参加する場合は、スペースのメンバーが 1 人参加し、[招待（Let In）] をクリックするまで**会議ロビー**で待機します。Cisco Webex アカウントを持たないユーザは、会議に参加する前にアカウントを作成するように求められます。Outlook またはその他のカレンダーの招待状から、電子メールアドレスを削除することもできます。

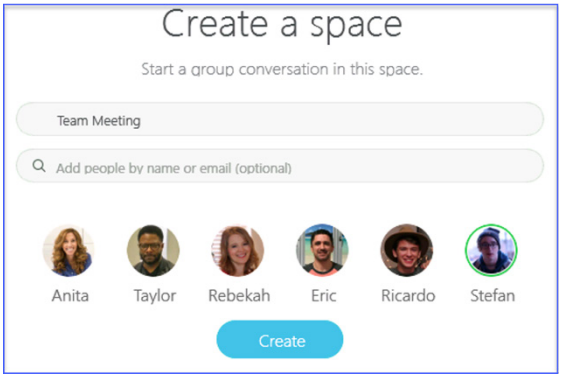
会議スケジュール機能は、次の場合は利用できません。

- 無料アカウントまたはメッセージング専用アカウントのユーザ
- ユーザ数が 26 人以上のスペース

まず Charles と Anita の新しいスペースを作成します。必要に応じて、ユーザをさらに追加できます。

1. **Workstation 1** で **Cisco Webex Teams クライアント**を開きます。
2. プラスアイコン [ ] をクリックし、[スペースの作成（Create a Space）] を選択します。
3. **チームミーティング**などのスペースの**名前**を入力します。
4. 必要に応じて **Anita** や他のユーザを追加します。
5. 追加したら、[作成（Create）] をクリックします。

スペースの作成



6. スペースにメッセージを送信します。
7. [スケジュール（Schedule）]タブを選択し、[ミーティングをスケジュール（Schedule a meeting）] を選択します。
8. [Quick schedule] にて、[開く（Open）] をクリックします。
9. 会議の招待状が表示されるまで待ちます。スペースからすべての情報がコピーされているのを確認できます。
10. 開始時刻や終了時刻の変更、定期会議の追加、メッセージの追加などを自由に試してください。完了したら、[送信（Send）] をクリックします。
11. 作成されたカレンダーエントリを開き、生成された [Cisco Webex Teams会議に参加（Join Cisco Webex Teams Meeting）] リンクをクリックします。
12. 最初に Web ブラウザでリンクを開き、ポップアップで [Webex Teamsを開く（Open Webex Teams）] をクリックする必要があります。
13. [ビデオで開始（Start with Video）] をクリックします。
14. Workstation 2 に移動します。

Charles が会議を開始したため、Anita は自分の Webex Teams デスクトップクライアントで参加通知を受け取ります。すでに参加しているすべての参加者のアバターがスペースに表示されます。今回参加しているのは Charles だけのため、Charles のアバターのみが表示されています。

15. 画面の右下に表示される**トースト**をクリックし、[ビデオで参加（Join With Video）] をクリックします。
16. モバイルクライアントから、スペース内の他のユーザでログインします。
17. モバイルの Webex Teams アプリで [参加（Join）] をタップして、進行中の会議に参加します。会議に Anita と Charles のアバターが表示されていることを確認します。

コール中の画面の共有

デスクトップまたはモバイルアプリから画面を共有できます。

1. デスクトップまたはモバイルアプリのいずれかからのコール中に、画面共有 [] をクリックします。
2. デスクトップアプリの場合は、**共有する画面を選択する**と、画面の共有が開始されます。モバイルアプリではすぐに画面の共有が開始されます。
3. [停止（Stop）] ボタンをクリックすれば共有はいつでも停止できます。

ここまでで、Cisco Webex Meetings とスケジュールされた会議のテストを行いました。会議は接続されているので、コンテンツ共有、メッセージング、ファイルのアップロード/表示、名簿ウィンドウを使用した参加者のミュートなど、他の会議アクティビティを自由にテストしてください。最後の参加者が退出するまで、会議は開催されたままになります。スペースに入って [コール（Call）] をクリックすることで、アドホック会議を開始することもできます。

4. すべての Webex Teams クライアントで通話を終了して、会議を終了します。

会議通知

Webex Teams が今後のミーティングを通知する時期を変更できます。

1. Webex Teams クライアントで **Charles のアバター**をクリックし、[設定（Settings）] を選択します。
2. [通知（Notifications）] を選択します。
3. 右側の [スケジュールされた会議（Scheduled Meetings）] の下で、通知**オプション**を確認できます。

ポップアウトスペース

同時に複数のタスクを実行する場合は、ポップアウトスペースが便利です。複数のスペースを新しい Webex Teams ウィンドウで開くことができます。そのため、他の未読スペースや通知に気を取られることなく、重要なスペースや会話に集中することができます。新しいウィンドウで開くには次の 2 つの方法があります。

- Webex Teams クライアントでスペースを見つけてダブルクリックすれば、別のウィンドウで開きます。
- 別のスペースを右クリックし、[新しいウィンドウで開く（Open in new window）] を選択しても開けます。

スペースのピークモード読み取り

未読メッセージがたまってしまう場合があります。スペースに未読のメッセージがあるのがわかっていてもすぐには対応できないときは、スペースをピークモードに設定します。設定するとスペースは既読としてマークされず、開封確認も送信されません。ただし、返信すると開封確認メッセージが送信されますが、ピークモードは継続します。

1. Workstation 1 の Webex Teams クライアントで、Charles が Anita と共有しているスペースを見つけ、スペースが開かれていないことを確認します。

2. Workstation 2 で、そのスペースにメッセージを送信します。
3. Workstation 1 に戻り、スペースを右クリックして、[スペースのピークモード読み取り（Peek in space）] を選択します。
4. スペース内のメッセージを読むことができますが、未読のままで変わりません。Workstation 2 に戻り、スペースを再度表示します。
5. Charles のアバターが既読になっていないことを確認します。

メッセージオプション

メッセージに返信したり、メッセージを操作したりする、さまざまなオプションがあります。スレッディング、引用、転送、編集、フラグ付与などがあります。

1. Workstation 1 の Webex Teams クライアントでスペースを見つけ、メッセージの上にマウスポインタを合わせます。
2. 自分が送信したメッセージの場合は、鉛筆アイコン [ ] をクリックしてメッセージを編集できます。メッセージを見つけて試してみてください。更新したメッセージを送信すると、メッセージが以前送信された時刻の横に [編集済み（Edited）] という文字が表示されています。
3. また、返信アイコン [ ] を使用してスレッドを開始するオプションもあります。試してみてください。
4. メッセージに返信するもう 1 つのオプションは、引用アイコン [ ] を使用してメッセージを引用することです。この機能で引用したメッセージに自分のメッセージを追加できることを確認します。追加したメッセージを送信すると、最新のメッセージとしてスペースに表示されます。
5. 転送アイコン [ ] を使用すれば、他のスペースにメッセージを転送できます。転送機能では、選択したスペースのメッセージが引用されます。試してみてください。
6. フラグアイコン [ ] を使用してメッセージにフラグを付けることができます。フラグを付けると、後で読み直したいメッセージを整理するのに役立ちます。メッセージにフラグを付けます。
7. 検索バーの下にある [フィルタ（Filter）] オプションを使用すると、**フラグ**を含むさまざまなオプションが表示されます。フィルタ処理に関するすべてのオプションを確認し、**フラグ**オプションをクリックすると、フラグが付いたメッセージが表示されます。リストに表示されたメッセージを選択すると、スペースでそのメッセージがある場所が開き、スペース内のメッセージに直接移動できます。
8. 最後に、ゴミ箱アイコン [ ] を使用してメッセージを削除できます。

ホワイトボード機能を使用して Cisco Webex Teams クライアントでコラボレーションする

これまでも、ファイルの共有やメッセージの送信などのコラボレーションが可能でしたが、ホワイトボード アクティビティが加わったことで、同僚との連携の幅が広がりました。通話中にビジュアルをすばやく作成してスペース内で共有したり、チームと共有したりできます。

1. スケジュールされた会議タスク用に先ほど作成したスペースのユーザを使用して、いずれかの **Cisco Webex Teams クライアント**を開きます。
2. スペース内で**アクティビティメニュー**（省略記号アイコン）をクリックします。
3. [新しいホワイトボード（New whiteboard）] をクリックします。
4. ホワイトボードで何か描き始めます。
5. ホワイトボードを閉じて、ホワイトボードのスナップショットが [コンテンツ（Content）] タブの [ホワイトボード（Whiteboard）] に表示されていることを確認します。
6. 別のクライアントで[コンテンツ（Content）]タブの[ホワイトボード（Whiteboard）] をクリックし、他のユーザが作成したホワイトボードをクリックします。
7. そのクライアントで図を編集します。変更内容が自動的に保存され、他のユーザに対する表示がリアルタイムで更新されます。
8. [新しいホワイトボード（New whiteboards）] をタップ/クリックすれば、ホワイトボードをさらに作成することもできます。
9. 必要に応じて、作成した**ホワイトボードを削除**することもできます。

モデレータ管理スペースとアナウンススペース

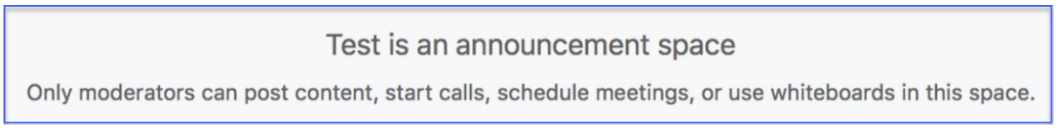
一部の Webex Teams スペースでは、ユーザの追加/削除、スペース名の編集、他のモデレータの割り当てなどのスペース設定を制限することが必要になる場合があります。この場合、任意のスペースをモデレータ管理スペースにすることができます。

1. 以前作成した Team Meeting ルームを選択します。
2. 歯車アイコン [⚙]をクリックし、[スペースのモデレータ管理（Moderate space）] オプションを選択します。ポップアップウィンドウで [はい（Yes）] をクリックします。
3. [ユーザ（People）] タブを選択します。
4. スペースの唯一のモデレータになったことを確認できます。任意のユーザを右クリックして、[モデレータとして割り当て（Assign as moderator）] を選択できます。

アナウンスのためにのみ使用するスペースを作成することが必要になる場合があります。これらのスペースでは、メッセージまたはファイルの投稿、コールの開始、会議のスケジュール、ホワイトボードの作成を実施できるのはモデレータのみです。

5. 歯車アイコン [⚙]を再度クリックして [アナウンスモードをオンにする（Turn on announcement mode）] を選択し、モデレータ管理スペースをアナウンススペースに切り替えます。ポップアップウィンドウで [OK] をクリックします。
6. 参加者がアナウンススペースを確認すると、次のようなメッセージが表示されます。

アナウンススペースのメッセージ



CMR ミーティングの開始/参加

Webex Teams クライアント内で、インスタント CMR 会議を開始したり、ビデオアドレスを使用して会議に参加したりすることができます。

1. **カレンダー**アイコン [15] をクリックします。
2. ページ上部に、パーソナルルームの URL が表示されます。歯車アイコン [⚙] をクリックします。

注：パーソナルルームの詳細が表示されている場合は、この注は無視して構いません。Charles のパーソナルルームのチェックボックスをオンにした場合、同じ日にはパーソナルルームの詳細が自動的に表示されない場合があります。その場合は手動で設定する必要があります。組織内の他のユーザは自動的に設定されます。Charles は組織で最初に作成されたユーザであるため、Charles のデフォルトのパーソナルルームを自動的に設定するためには、優先する Webex サイトを設定する夜間プロセスが先に実行される必要があります。先に進み Charles のパーソナルルームを手動で設定するか、別のユーザを使用すれば、次の手順を実行できます。

ここでは、自分の会議情報をコピーできます。また、[編集（Edit）] リンクをクリックして、URL やホストの PIN などの情報を編集することもできます。

3. クライアントに戻るには、ウィンドウの [キャンセル（Cancel）] をクリックします。
4. ページ上部の[ミーティングを開始（Start Meeting）] ボタンをクリックし、ポップアップするウィンドウで [ミーティングを開始（Start Meeting）] **ボタン**をクリックすると、すぐにパーソナルルームで会議が開始されます。ここでこの操作を自由に試してください。
5. 会議が開始されている場合は、終了して構いません。
6. ページ右上隅で**ビデオアドレスを入力**し、**緑色のボタン**をクリックすると、[ミーティングを開始（Start Meeting）] することができます。ここで任意のビデオアドレスをコールするか、Charles のパーソナルルーム（**cholland@cbXXX.dc-YY.com**）のアドレスを使用して試すことができます。

注：Webex Meetings サイトの URL が機能しない場合は、Control Hub の [サービス（Services）] > [会議（Meeting）] > [サイト（Sites）] > [サイト名（Site Name）] で URL を確認してください。使用できるその他の URL は、https://cbXXXYYa.webex.com、https://cbXXXYYb.webex.com、https://cbXXXYYc.webex.com です。

7. 完了したら、会議を終了します。

コール動作

管理者は、電話番号を呼び出すときの Webex Teams のコール動作を変更できます。これについては、Webex Calling のシナリオでも説明しました。ここでは、ユーザが利用できるその他のコール動作を説明します。

Webex Teams（Unified CM）でのコール

Webex Teams を既存の Unified CM コール制御環境に登録することができます。Cisco Jabber が Cisco Unified Client Services Framework（CSF）デバイスを使用して現在登録しているのと同じ方法です。すでに Cisco Jabber が設定されて機能している場合は、Webex Teams も同じ CSF デバイスを使用して登録することになります。同じ CSF デバイスを使用するため、Teams を Unified CM に登録するように設定している場合は、Jabber と Teams を同時に使用することはできません。Webex Teams が Unified CM に登録されると、デスクフォンの制御や保留/再開などの通話中機能など、より多くのコール機能を利用できるようになります。このコールソリューションの概要および導入ガイドをこちらで確認できます。

ここで、Charles のコール動作を設定します。

1. Control Hub に戻り、[ユーザ（Users）] ページに移動します。
2. リストから **Charles** を選択します。ポップアップウィンドウで [設定（Settings）] セクションまで下にスクロールします。
3. [発信動作（Calling Behavior）] をクリックします。
4. ご覧のように、デフォルトの発信動作は、電話番号をダイヤルする際に [組織の設定：Webex Teamsの発信（Organization Setting: Calling in Webex Teams）] を利用するようになっています。[設定（Settings）] ページで組織の設定を変更できます。ここでは、Charles のコール動作だけを変更します。

注：ご覧のように、さまざまなコール動作が表示されています。ラボではこれらすべてについては説明しませんが、後で自由にテストできます。たとえば、Cisco Jabber アプリを選択すると、Webex Teams からのコールによって Cisco Jabber が起動され、Jabber クライアントを使用して電話番号を呼び出すことになります。このシナリオは、Workstation 2 の Anita でテストできます。

5. [Webex Teams（Unified CM）のコール（Calling in Webex Teams (Unified CM)）] オプションボタンを選択します。
6. [保存（Save）] をクリックします。
7. Workstation 1 に戻り、Cisco Jabber が開いている場合は、サインアウトして終了します。

注：Webex Teams は、Jabber が使用するのと同じ CSF デバイスを使用してコールを行います。両方のアプリで同時に CSF デバイスを使用することはできないため、どちらかのアプリケーションを閉じる必要があります。今 Jabber を閉じたのはそのためです。

8. Webex Teams が開いている場合は、変更後に再起動ボタン [] が表示されます。そのボタンをクリック後、[更新（Update）] をクリックしてクライアントを再起動/更新します。再起動ボタンが表示されない場合は、一度クライアントからサインアウトし、サインインし直します。
9. しばらくすると、クライアントの左下に新しいアイコン [] が表示されます。そのアイコンをクリックして、[電話サービス（Phone Services）] の設定を開きます。この設定は、アバターをクリックし、[設定（Settings）] > [電話サービス（Phone Services）] の順に移動しても開けます。
10. [ユーザ名（username）]/[パスワード（password）] フィールドに **cholland/dCloud123!** と入力し、[保存（Save）] をクリックします。
11. ポップアップメッセージに対して [OK] をクリックします。
12. ログイン情報が適用されると、電話の警告アイコンが表示されなくなります。この状態になれば、コールする準備が完了です。

PSTN 経由でコールの受発信ができるようになります。以前にラボで使用した番号で PSTN とのコールをテストできます。

シナリオ 12.　Webex Meetings のトラブルシューティング

このシナリオでは、Cisco Webex Control のさまざまな機能を実行します。

分析

Cisco Webex Control Hub では、使用状況の傾向を分析して価値のある分析情報を提供し、分析結果を基に詳細な導入戦略を構築することで、チーム間のコラボレーションを最適化して推進できます。高度な分析機能が Webex Control Hub に統合されています。お客様は、組織全体で各種サービスがどのように使用されているかを把握できるため、効果的にサービスの導入を拡大し、生産性を最大限まで向上させられます。管理者はキャパシティとパフォーマンスをモニタし、プロアクティブな管理の一環としてリソース使用率を最適化できます。管理者や IT ヘルプデスクのスタッフは、診断を実行して、短時間で問題を解決できます。

管理者は、直感的なグラフィカル インターフェイスにより、使用状況や導入状況などの重要な情報にアクセスできます。指定したパラメータがリアルタイムで自動的に適用されるため、データをインタラクティブに可視化し、詳しく調査することができます。

標準で過去 90 日間の履歴データにアクセスできます。データは集約され、さまざまなレポートに利用されます。管理者は、Webex Control Hub 内で各種レポートにいつでもアクセスできます。

Pro Pack for Webex Control Hub では機能が追加され、さらに詳細にデータを調査したり、通常ではわからない分析結果間の関連を把握したりできます。時間、場所、人などのさまざまな切り口から、データを調査することができます。また、診断機能も備わっており、会議時間や参加者リストなどの Webex Meetings の詳細情報にリアルタイムでアクセスできます。

残念ながら、ユーザとデバイスの数が少ないラボでは、分析機能とレポートで提供されている内容をすべて確認することはできません。ラボを実施すると一部のデータは得られますが、すべてではありません。[分析（Analytics）] タブを自由にクリックして、各セクション（メッセージング、コール、サポート、Video Mesh、デバイス、会議）のレポートを確認してください。提供されているレポートの詳細情報については、ここをクリックしてください。

トラブルシューティング

Pro Pack for Webex Control Hub では、Webex Meetings のトラブルシューティング機能も提供されています。技術スタッフは、トラブル発生時にリアルタイムで会議を検索し、サポート要求に迅速に対応することができます。ホストの電子メールアドレスと会議 ID のいずれでも会議を検索できます。オプションで過去 7 日間の日付から選択できます。会議の時刻は、管理者のプロファイルに設定されているタイムゾーンに応じて表示されます。ドロップダウンメニューで変更することも可能です。会議が特定されたら、会議 ID、開始時刻、会議時間、会議名、参加者数、ステータスがレポートされます。

管理者は個別の会議にドリルダウンして、参加者やセッションレベルの詳細情報を追加で取得できます。各参加者のデバイス別の接続状況が個別の行に表示されます。音声およびビデオセッションの会議参加時刻と会議時間が各行に表示されます（該当する場合）。

ラボでは、Webex Meetings アプリケーションを使用します。最適な結果を得るには、モバイルデバイスを含む複数のデバイスからダイヤルインすることをお勧めします。モバイルデバイスがローカルのキャリアネットワーク上にある場合、会議に接続する際の品質の低下を確認できます。まず、デバイスのアプリストアを使用して、モバイルデバ

イスに会議アプリをダウンロードする必要があります。また、デスクトップアプリもダウンロードします。デスクトップに会議アプリがインストールされていない場合は、以下の手順でインストールファイルを取得します。ラボのワークステーションまたはローカルワークステーションにインストールできますが、自分のワークステーションを使用することをお勧めします。

Webex Meetings デスクトップ アプリケーションのダウンロードとインストール

次に、Webex Meetings デスクトップ アプリケーションをインストールします。すでにインストールしている場合は、このセクションをスキップできます。

1. Web ブラウザで **https://cbXXXYY.webex.com** にアクセスします。

注：Webex Meetings サイトの URL が機能しない場合は、Control Hub の [サービス（Services）] > [会議（Meeting）] > [サイト（Sites）] > [サイト名（Site Name）] で URL を確認してください。使用可能なその他の URL には、https://cbXXXYYa.webex.com、https://cbXXXYYb.webex.com、https://cbXXXYYc.webex.com があります。

2. Charles のアカウント（**cholland@cbXXX.dc-YY.com/dCloud123!**）でサインインします。
3. 左側のメニューで [ダウンロード（Download）] をクリックします。
4. [ダウンロード（Download）] ボタンをクリックします。
5. ダウンロードしたアプリケーションをインストールし、インストールが完了したら Charles でサインインします。

会議を開始し他のデバイスから参加する

次に、デスクトップアプリを使用して新しい会議を開始し、他のデバイスから参加します。

1. Webex Meetings アプリケーションで、[ミーティングを開始（Start Meeting）] をクリックします。
2. ミーティングの詳細情報を基に、他のデバイスから会議に接続します。デバイスとして、モバイルアプリ（推奨）、Teams アプリ、Room デバイスなどを利用できます。会議の情報は、画面の左上にある情報ボタン [ ] をクリックすれば確認できます。

会議のトラブルシューティング

会議を開始し、別のデバイスから参加したら、ほぼリアルタイムに会議データを確認できるようになります。

1. Webex Control Hub で [トラブルシューティング（Troubleshooting）] をクリックします。
2. [電子メール（Email）] ボックスに Charles の電子メールアドレス（**cholland@cbXXX.dc-YY.com**）を入力し、Enter を押します。
3. ラボで開始した会議は、上部にある [進行中（In Progress）] の会議も含めすべてリストされます。会議をクリックします（会議がリストに表示されるまでに最大 10 分かかる場合があります）。

会議に参加しているユーザとダイヤルインに使用したデバイスに関するグラフが表示されます。すべてのデータが正しく表示されるまでに最大 10 分かかることがあります。更新ボタン [ ] をクリックすると、いつでも最新のデータを取得できます。

4. 接続情報とユーザのリストが表示されます。
5. グラフのいずれかの部分にマウスを動かすと、参加時刻や VoIP の品質など、デバイス/ユーザに関する詳細情報を取得できます。

グラフの右側に凡例が表示されています。接続不良のモバイルデバイスでダイヤルインした場合、品質の低いことを示すデータが赤色で表示されることがあります。

同じくページの右側には、会議のホスト情報や種類などの会議の概要が表示されます。また、会議が記録されたかどうか、画面共有が利用されたかどうかも確認できます。

デフォルトのグラフは、**音声**情報です。

6. [ビデオ（Video）] **タブ**をクリックします。

ビデオの品質、遅延、パケット損失など、音声の場合と同様に、ビデオデータに関する情報が表示されます。

会議に接続したまま、さらに多くのデータを入手できるまで待機して構いません。また、再接続して、品質低下を示すデータが表示されるかどうかも確認できます。また、画面を共有するなど、他の機能も自由にテストしてください。

テストが完了したら、**会議を終了**します。[トラブルシューティング（Troubleshooting）] ページに戻ればいつでも会議データを表示できます。

シナリオ 13.　Pro Pack for Cisco Webex Control Hub

このシナリオでは、Cisco Webex で利用できる多くの Pro Pack 機能を設定します。サービスには、標準と Pro Pack の 2 種類があります。標準サービスは Cisco Webex に無料で付属し、アドオンが追加されていません。Pro Pack アドオンでは新たなサービスが追加されます。Pro Pack for Cisco Webex Control Hub の詳細については、https://help.webex.com/ja-jp/np3c1rm/Pro-Pack-For-Cisco-Webex-Control-Hub を参照してください。

コンプライアンス - eDiscovery 検索/抽出ツール

eDiscovery は標準オファーの Webex に無償で付属しています。ただし標準オファーでは、過去に遡って検索できるのは最大で 90 日です。Pro Pack では期間の制限はありません。

eDiscovery 検索/抽出ツールを使用すると、Cisco Webex Teams スペース内で無制限にデータにアクセスし、情報を検索して取得できます。電子メールアドレス、スペース ID、キーワード、特定の期間を指定して検索条件を絞り込めます。

コンプライアンス担当者として、Cisco Webex Control Hub を使用して Cisco Webex Teams アプリ内のすべての会話を検索できます。また、社内の特定のユーザを検索してそのユーザが共有したコンテンツを抽出し、調査結果レポートを生成できます。さらに、特定のスペースの情報を検索することも可能です。

https://help.webex.com/ja-jp/nr70c1m/Ensure-Regulatory-Compliance-of-Cisco-Webex-Teams-Content にアクセスすれば、eDiscovery に関する詳細情報を確認できます。コンプライアンス担当者のロールや提供されるレポートに関する情報が含まれています。

まず、コンプライアンス担当者のロールをユーザに割り当てる必要があります。このロールを設定できるのは管理者だけです。また、セキュリティ上の理由から、管理者は自分自身にコンプライアンス担当者ロールを割り当てることはできません。

ユーザにコンプライアンス担当者ロールを設定する

1. Control Hub ポータル（https://admin.webex.com）に戻り、必要に応じて Charles でログインします。
2. [ユーザ（Users）] タブをクリックします。
3. ユーザリストから **Eric** を選択します。
4. ポップアップウィンドウで、[サービスへのアクセス（Service Access）] をクリックします。
5. [コンプライアンスオフィサー（Compliance Officer）] のチェックボックスをオンにして、[保存（Save）] をクリックします。

検索用データの生成

検索結果を得るために、ユーザ宛のメッセージをいくつか生成する必要があります。

1. Webex Teams クライアントを使用してメッセージを送信します。既存のスペースを使用しても構いませんし、新規のスペースを作成することもできます。

2. 検索対象になるいくつかの一意の単語を使用してメッセージを作成します。
3. いくつかメッセージを送信したら、次のセクションに移動します。

データの検索と抽出

これで検索対象のメッセージができたので、eDiscovery 検索/抽出ツールを使用してそのデータを検索します。

1. Webex Control Hub から Charles をログアウトして、Eric（**esteele@cbXXX.dc-YY.com/dCloud123!）でログインします。**
2. [利用規約（Terms of Service）] に [同意（Accept）] します。
3. [電子メールアドレス（Email Address）] ボックスに、テストデータを生成したユーザの電子メールアドレスを入力します。スペース ID がわかっている場合は、[スペース名（Space Names）] ボックスに指定してそのスペース内だけを検索することもできます。複数のユーザとスペースを一度に検索することもできます。
4. [レポート名（Report Name）] ボックスに名前を入力します。
5. 画面の右下に表示される [検索およびレポート生成（Search & Generate Report）] ボタンをクリックします。
6. [レポート（Reports）] タブが表示されます。処理が完了するまでしばらく時間がかかります。レポートをダウンロードして表示するには、eDiscovery Download Manager をダウンロードしてインストールする必要があります。
7. 画面右上の [Download Manager] をクリックします。
8. お使いのオペレーティングシステムの [ダウンロード（Download）] ボタンをクリックしてダウンロードし、インストールします。
9. インストールしたら [レポート（Reports）] タブに戻り、生成したレポートの横にあるダウンロードアイコン [ ] をクリックします。
10. プロンプトが表示されたら、[eDiscovery Download Managerを開く（Open eDiscovery Download Manager）] をクリックします。
11. [ダウンロード場所（Download Location）] を選択し、[フルレポート（Full Report）] をクリックします。
12. ダウンロードが完了したら、[フォルダを開く（Open Folder）] をクリックします。

該当のユーザのすべてのメッセージが .eml ファイルに抽出されます。ファイル内で必要なメッセージを検索するには、お使いのオペレーティングシステムの機能を利用する必要があります。テキストエディタまたは電子メールクライアントを使用して、各 .eml ファイルを開きます。

コンプライアンス – DLP およびアーカイブ用のイベント API

標準オファーのお客様でも Pro Pack オファーのお客様でも、イベント API を使用して、既存のデータ損失防止（DLP）ソフトウェアと統合できます。ポリシー違反をチェックし、問題の解決策を講じることもできます。Pro Pack のお客様の場合は、90 日以上前に発生したイベントでもモニタできます。イベントには、スペースへのメッセージやファイルの投稿、ユーザの追加などがあります。また、イベント API を使用して既存のアーカイブソフトウェアと統合し、Cisco Webex データを制限なくアーカイブすることもできます。

DLP またはアーカイブソフトウェアのセットアップは、このラボでは扱いません。ただし、API を手動で実行して取得できるデータを確認することはできます。

イベント API を使用するユーザには、コンプライアンス担当者のロールが設定されている必要があります。

1. eDiscovery ツールに使用したブラウザと同じブラウザで https://developer.webex.com に移動して、**ログイン**します。必要に応じて、コンプライアンス担当者の **Eric**（**esteele@cbXXX.dc-YY.com/dCloud123!**）でログインします。
2. [ドキュメント（Documentation）] リンクをクリックします。
3. 左側の [APIリファレンス（API Reference）] メニューをクリックして展開します。
4. このメニューには、Webex Teams で使用可能なさまざまなパブリック API がすべて表示されます。ここでは、[イベント（Events）] メニューをクリック後、[イベントを一覧表示（List Events）] をクリックします。

これまでに開発者向け Cisco Webex サイトを利用したことがない場合は、テストモードを利用できます。テストモードでは、Web サイトから直接 API を使用して、その動作を確認することができます。ここでは、イベント API を使用して確認します。

5. [試す（Try it）] が選択されていることを確認します。

開発者サイトではログイン時にベアラートークンをすでに入力しているため、後は API を実行するだけです。[クエリパラメータ（Query Parameters）] セクションでは、検索条件を絞り込むことができます。ここでは、すべてのオプションを空のままにします。

6. 下にスクロールし、[実行（Run）] をクリックします。

画面の右側に API の実行結果が表示されます。ご覧のように結果には、スペースにメッセージやファイルを投稿したイベントやユーザを追加したイベントがすべて含まれています。今回は、ユーザの少ない新しい組織を対象に、ラボでこれまでに作成したイベントしか含まれていないため、結果は最小限のものです。スペースへのメッセージの投稿、ファイルのアップロード、ユーザの追加を行うユーザが 100 倍や 1000 倍になると、結果は非常に大量になります。実稼働環境の組織では、このような大量の結果を調べることはありません。そのため、DLP ソフトウェアによってこのデータをキャプチャして分類し、たとえばコンプライアンス違反が発生した場合などにイベントに対処します。また、前述のように、この情報をアーカイブシステムにリダイレクトすれば、データを無制限に保持できます。

コンプライアンス – 柔軟な保持ポリシー

Pro Pack のお客様は、Cisco Webex のユーザが作成して共有するコンテンツの保持期間を、組織のポリシーに合わせて設定することができます。保持時間より古いデータは削除され、回復できません。保持期間は、組織管理者が Control Hub で設定します。

1. Control Hub（https://admin.webex.com/）に戻り、Charles（**cholland@cbXXX.dc-YY.com/dCloud123!**）でログインします。
2. 左側のメニューの [設定（Settings）] をクリックします。
3. ページ下部の [保存期間（Retention）] セクションまでスクロールします。

デフォルトでは、標準ユーザの唯一のオプションである保持期間が [無制限に（Indefinitely）] に設定されています。

4. Pro Pack ユーザの場合は、さまざまなオプションを選択し、利用可能な保持期間を確認できます。

セキュリティ – PIN ロックの適用

コンテンツが Cisco Webex Teams アプリで確実に保護されるように、PIN ロックを設定できます。PIN ロックが有効になっている場合、ユーザは PIN または画面ロックが設定されているモバイルでしか Cisco Webex Teams を使用できません。

1. Control Hub で左側のメニューから [設定（Settings）] をクリックします（前の演習で実施していない場合）。
2. [セキュリティ（Security）] セクションのページ上部で、[ユーザーは、ロック画面により保護されているモバイルデバイス上でのみ Cisco Webex Teams アプリを起動することができます。（Users can only launch the Cisco Webex Teams app on mobile devices protected with lock screens）] というチェックボックスをオンにします。
3. モバイルデバイスで PIN をオフにできる場合は、PIN をオフにしてから Cisco Webex Teams クライアントを開き、ラボのいずれかのユーザでログインしてテストします。

モバイルアプリを開くと、パスコードが必要であることを示すポップアップが表示され、アプリの利用を続けるためには、パスコードを設定する必要があります。設定せずにできるのは、ログアウトすることだけです。

セキュリティ – 外部とのコミュニケーションのブロック

組織のデータを保護し、組織外でデータが共有されないようにするには、組織外の人と Webex Teams スペースでコミュニケーションできるようにするかどうかを制御する必要があります。

1. Control Hub で左側のメニューから [設定（Settings）] をクリックします（前の演習で実施していない場合）。
2. [外部通信（External Communications）] までスクロールします。
3. [外部メッセージングをブロックする（Block your users from inviting external contacts to Cisco Webex Teams spaces and prevent your users from joining external Cisco Webex Teams spaces）] というチェックボックスをオンにします。ポップアップするウィンドウの注記を確認し、チェックボックスをオンにして [完了（Done）] をクリックします。

この設定をしても、スペース内の既存の外部ユーザと既存の外部スペースは削除されません。

この設定は、ボットには適用されません。

組織内のユーザは次のことは実施できません。

- 組織外の人を自分の組織が所有するスペースに追加する
- 組織外のスペースに参加する
- 外部の人が参加するスペースを作成する

組織内のユーザは、次のシナリオでは外部の人にコールできます。

- ユーザが Webex SIP アドレスを使用してコールする場合。詳細については、Cisco WEBEX SIP アドレスを参照してください。
- オンプレミスにコール環境があり、ユーザにハイブリッドコールサービスを割り当てる場合。詳細については、Cisco Webex ハイブリッドコールサービス導入ガイドを参照してください。
- Cisco Webex Calling（旧 Spark Call）を利用してクラウドコールを行い、Cisco Webex Calling（旧 Spark Call）サービスをユーザに割り当てる場合。

4. Webex Teams クライアントを開いて、**cbXXX.dc-YY.com** ドメイン**ではない**ユーザとの 1 対 1 のスペースまたはグループスペースを開始します。

ユーザを追加しようとすると、追加できるのは社内の人のみであることを示すポップアップ警告が表示されます。

5. メッセージで [OK] をクリックします。
6. Webex Teams にログインしている外部アカウントがある場合は、ラボユーザの 1 人をスペースに追加してみてください。

ラボユーザを追加しようとすると、社外からはスペースに参加できないことを示すポップアップ警告が表示されます。

セキュリティ - ファイル共有制御

Cisco Webex Teams でのファイルの共有方法を制御できます。特定の Cisco Webex Teams アプリにポリシー制御を適用してマルウェアを排除し、データ漏洩を防止するために、ユーザによるファイルのダウンロード、プレビュー、Cisco Webex Teams アプリへのアップロードを制限できます。

1. [サービス（Services）] ページに移動し、[メッセージ（Message）] カードの [設定（Settings）] をクリックします。

Cisco Webex Teams のアプリとボットを制限する対象には、次のようにさまざまなタイプがあります。

- ファイルのプレビューとダウンロード
- ファイルのアップロード
- ホワイトボードと注釈追加
- アニメーションされた GIFの共有
- 共有リンクのプレビュー

ポリシーを選択する際に注意すべき点を示します。

- Cisco Webex Teams アプリまたはボットに対して [ファイルのプレビューおよびダウンロード（Preview and download files）] を選択した場合、[フィルのアップロード（Upload files）] も自動的に選択されます。
- ホワイトボード機能と注釈追加機能を制限することを選択した場合、制限は新しいスペースにのみ適用され、ホワイトボード機能や注釈追加機能がすでに設定されている既存のスペースには適用されません。

2. リストされている制限の一部またはすべてを設定します。

ダウンロードとプレビューのセクションでチェックボックスをオンにすると、アップロードのセクションでもチェックボックスがオンになります。アップロードセクションのチェックボックスをオンにしても、ダウンロードとプレビューは変わらず実行できます。

いずれかのオプションをオンにした後、ラボユーザで該当のアプリタイプにアクセスし、無効にしたタスクを実行してみます。

アップロードを無効にした場合、メッセージを送信しようとすると、メッセージを送信できないことを示すエラーメッセージが表示されます。ダウンロードを無効にした場合、アプリではダウンロードできません。

セキュリティ - アクセス権の取り消し

ユーザが携帯電話を紛失した場合や組織を離れた場合、リモートからアクセス権を取り消して、キャッシュされた Cisco Webex のコンテンツを携帯電話からワイプすることができます。

1. Control Hub で [ユーザ（Users）] をクリックします。
2. 以前 Cisco Webex Teams にログインしていたユーザを選択します。
3. [セキュリティ（Security）] をクリックします。
4. ウィンドウの下部で [アクセス権をリセット（Reset Access）] をクリックします。

これで、該当のユーザのトークンがすべて取り消されます。この処理には最大 6 時間かかることに注意してください。ユーザを削除すると、そのユーザのアクセス権もすぐに削除されます。

シナリオ 14.　Webex Board

Cisco Webex Board：チームコラボレーション向けのオールインワンデバイス

Cisco Webex Board を利用すれば、プレゼンテーション、ホワイトボード、ビデオ会議、音声会議、さらには共有コンテンツへの注釈追加などをワイヤレスで実施できます。チームコラボレーションに必要なあらゆる機能をワンタッチで使用可能です。また、Cisco Webex Teams アプリを使用すれば、任意のデバイスで仮想チームメンバーと連携できます。

Cisco Webex Board の主な機能は次のとおりです。

- **ユーザ本位の設計**：タッチベースで使いやすく、高品質なコラボレーション エクスペリエンスが得られます。Cisco Webex Board によって、物理的な会議室でのチームコラボレーションに必要な一般的なツールが、1 つの洗練されたデバイスに統合されます。
- **アプリを通じて仮想チームを連携**：Webex Board で作成したものはすべてクラウドに保存し、仮想ルームに関連付けることができます。Cisco Webex Teams アプリを使用すれば、チームメンバーはどこにいても、物理的な会議室で中断した所から作業を再開できます。
- **ニーズをインテリジェントに予測**：Webex Board は、ユーザが会議室に入ると自動的に起動します。Webex Teams アプリに対応しているデバイスを検出し、通話やホワイトボードを利用したり、プレゼンテーションをワイヤレスで共有したりするなどのアクティビティが提案されます。
- **自然なエクスペリエンスを実現するテクノロジー**：強力な 4K カメラによって、会議室のほぼ全体が、高解像度の広角イメージとしてキャプチャされます。12 個のマイクアレイによって音声が明瞭になり、自動的に増幅と変調がなされるため、会議の参加者全員の声が聞きやすくなります。

このシナリオでは、Cisco Webex Board を使用して、ラボですでにデモンストレーションしたあらゆる機能を実施できます。使用する Webex Board は、ほとんどの場合 Cisco Webex サービスに接続されています。接続されていない場合は、すでにラボで示したその他の Room デバイスの場合と同じように Webex Board を追加します。Webex Board は、このラボで設定した Webex 組織と同じ組織に接続する必要はありません。

ローカル Webex Board の機能

Webex Board は、まずローカルのホワイトボードとして使用できます。

コール

1. Webex Board をタップしてメイン画面を表示します（まだ表示していない場合）。[コール（Call）]、[ホワイトボード（Whiteboard）]、[画面の共有（Share screen）] の 3 つのオプションがあります。ディスプレイ下部の中央にあるホームボタンをタップすれば、いつでもホーム画面に戻れます。
2. [コール（Call）] をタップします。

ここでユーザにダイヤルしてコールすることができます。

3. Webex Board から **username@cbXXX.dc-YY.com** にダイヤルして、ローカルクライアントにログインしているラボ内の Webex Teams ユーザにコールし、Webex Teams クライアントで応答します。ハウリングしないように両側を必ずミュートしてください。
4. Webex Board には、音声やビデオのミュート、音量の変更、コールの終了の各オプションが表示されています。これらのオプションが表示されていない場合は、画面をタップします。画面下から上にスワイプすることで、音量バーが表示され音量をコントロールできます。
5. 通話中はローカルのビデオ映像が消えることがわかります。ビデオ映像を固定表示するには、画面をタップしてから自分のビデオ映像をタップし、[セルフビューの固定表示（Pin selfview）] をタップします。内蔵 4K カメラでカバーできるアングルの広さに注目してください。室内を移動して、ベストオーバービュー機能をテストします。送信するビデオ映像のベストビューを確保するために、ビデオがズームします。
6. 複数人でマイクの音質をテストできる場合は、Webex Teams アプリのユーザを 1 人以上退室させて、Webex Board でそのユーザと会話を続けます。スペースに余裕があれば、Webex Board 会議室内で歩きながら会話を続けます。12 個のマイクアレイが内蔵されているため、Webex Board 会議室内のどこからでも退室したユーザに音声がクリアに伝わります。会議室内に複数のユーザがいる大きなトレーニング環境では、マイクのパフォーマンスが異なる場合があります。マイクが届くおおよその範囲は約 9 m（約 30 フィート）です。
7. ホームボタンを押して [ホワイトボード（Whiteboard）] をタップします。
8. ホワイトボードに何か描きます。
9. Webex Teams クライアント側にホワイトボードがリアルタイムに表示され、変更内容をすぐに確認できます。クライアント側で編集するには、編集ボタン [] をタップまたはクリックします。[完了（Done）] をタップしてから [共有の停止（Stop sharing）] をタップすると、いつでも共有を停止できます。
10. Webex Board から通話を終了するには、画面上部の [通話に戻る（Return to call）] バーをタップし、[X] をタップします。
11. 画面上部の中央にある名前をタップすると、Webex Board の SIP アドレスや設定を表示できます。また、このメニューから Webex Board を再起動することもできます。

画面共有

画面を共有することもできます。

1. ホーム画面から [画面の共有（Share screen）] アイコンをタップします。

画面の共有には、HDMI ケーブルを使用する方法と、Webex Teams クライアントを使用してワイヤレスで共有する方法の 2 つがあります。

2. HDMI ケーブルがある場合は、まずケーブルを使用して画面共有をテストできます。HDMI ポートは、ディスプレイ下部中央付近の背面にあります。

HDMI をテストしたら、Cisco Webex Teams デスクトップクライアントと画面を共有します。

3. Cisco Webex Teams デスクトップクライアントを開き、クライアントの左下にあるペアリングされたボードの名前をクリックし、[画面の共有（Share Screen）] を選択します。
4. 共有する画面またはアプリケーションを選択します。

しばらくすると画面共有が開始されます。停止する場合は、デスクトップ画面上部にある [

] をクリックするか、Webex Board をタップして [共有の停止（Stop sharing）] をタップします。ただし、次のセクションのために画面の共有状態は維持してください。

注釈追加

共有画面に注釈を追加できます。

1. 前のセクションで実施した画面共有を停止した場合は、今すぐ画面を共有してください。
2. **Webex Board** 画面をタップし、画面の左上にある [注釈（Annotate）] ボタンをクリックします。

これにより現在共有している画面がキャプチャされ、注釈を付けることができるようになります。また、デバイスからの画面共有も終了します。

3. 注釈は画面のどの場所にでも自由に付けることができます。
4. 終了したら、画面の左下にある [完了（Done）] ボタンをタップします。画面共有を再開するかどうかを確認するメッセージが表示されます。[停止（Stop）] をタップします。これで注釈画面は閉じられ、Webex Board の **Files** フォルダ内に保存されます。
5. **Files** フォルダに移動します。注釈をつけたスクリーンキャプチャを選択します。この状態からは、画面の左下にある注釈ボタンをタップすることで、そのまま注釈を追加できます。
6. 画面右下のエクスポートボタンをタップし、[Webex Teamsに保存（Save to Webex Teams）] を選択して、Webex Teams スペースに途中経過を保存することもできます。ここで実施します。
7. 次の画面で、自分の作業が選択されていることを確認し、**青い右矢印**をタップして続行します。

次の画面では、以前ペアリングした際の自分の名前が表示されます。作成しようとしている新しいスペースに**他のユーザを追加する**こともできます。

8. 画面をそのままにしておくか、必要に応じて新しいスペースにユーザを追加します。終了したら、**青のチェックマーク**をタップします。
9. Webex Teams クライアントに移動し、新しいスペースが作成され **Whiteboards** コンテナにあるスナップショットが設定されていることを確認します。
10. この新しいスペースにホワイトボードが自動的に接続されています。ホーム画面に移動し、画面下部の [このスペースを閉じる（Close this space）] をタップして閉じます。

ホワイトボード

次に、コールセクションと同様にホワイトボード機能を使用します。

1. ホーム画面から、[ホワイトボード（Whiteboard）] アイコンをタップします。
2. 新しいホワイトボードを起動するか、既存のものを使用します。色は、画面下部に表示されている色を利用します。さまざまな色の他に、すべてクリアする機能を持つ消しゴムも用意されています。Webex Board ペンや指で描画します。[元に戻す（undo）] ボタンもあります。
3. 最初のホワイトボードで描画を終えたら、その描画はそのままにして、画面左下にある [新しいホワイトボード（New whiteboard）] アイコンをタップします。
4. この新しいホワイトボードで**別の図**を描きます。
5. 描き終えたら、画面左下の [すべてのホワイトボード（All whiteboards）] アイコンをタップします。これで、ローカルのホワイトボードがすべて表示されます。

これで、ローカルのホワイトボードがすべて表示されます。

6. 画面左下にある [ゴミ箱（Trash）] アイコンをタップすると、ホワイトボードのすべてまたは一部を削除できます。

各ホワイトボードの右下に円が表示されます。いずれかのホワイトボードをタップすると、この円の中にチェックマークが表示されます。いずれかのホワイトボードにチェックマークを付け、画面左下にある赤いチェックマークアイコンをタップしてから [削除（Delete）] をタップすると、選択したホワイトボードを削除できます。今は削除しないでください。

7. [キャンセル（Cancel）] をタップします。

セキュリティ機能として、Webex Board がスリープ状態になると、ホワイトボードがすべて削除されます。Webex Board を手動でスリープ状態にするには、ホームボタンを長押しします。5 秒間のカウントダウンタイマーが開始されます。

8. ホームボタンを長押しするとスリーププロセスが開始されます。開始した場合でも、Webex Board の画面をタップすると**キャンセル**されます。ホワイトボードに戻り、すべてのホワイトボードを再度表示します。

ローカルホワイトボードのメール送信

会議室でホワイトボードを利用したセッション中に、ホワイトボードを確認するために電子メールで送信したい場合があります。ホワイトボードを電子メールで送信するには、電子メールサーバを設定する必要があります。

1. ホーム画面の一番上にあるボード名をタップし、[設定（Settings）] をタップします。
2. 次の画面で [詳細設定（Advanced Settings）] をタップし、[電子メールサーバの設定（Email server configuration）] をタップします。
3. [電子メールへのエクスポートを有効にする（Enable exporting to email）] をオンに切り替え、SMTPサーバを設定します。
4. 終了したら、**青のチェックマーク**をタップします。
5. ホワイトボードを開き、**いくつかのマーク**を作成します。
6. 終了したら、画面右下の**保存ボタン**をタップして [電子メール（Email）] をタップします。

7. 電子メールを送信するホワイトボードを選択し、**青い矢印**をタップします。
8. 送信先の**電子メールアドレス**を入力し、**青いチェックマーク**をタップして送信します。
9. 電子メールを受信したら、**添付の PDF ファイル**を表示できます。

Webex Board 機能と Webex Teams スペースの連携

Webex Board は単体でも優れた機能ですが、Cisco Webex Teams スペースと接続することでより素晴らしいものになります。新しいスペースを設定し、ドキュメント、プレゼンテーション、写真などのさまざまな種類のファイルを追加できます。スペースを作成したら、スペースにデモユーザを何人か追加します。

ホワイトボードの移動

1. Webex Board の**ホワイトボード**に戻り、すべてのホワイトボードを表示させます（まだ表示していない場合）。
2. いずれかの Webex Teams クライアントで Webex Board とペアリングし、既存のスペースを開くか、新しいスペースを作成します。
3. アクティビティメニューを開きます。メニューの下部にある、[Webex Boardで開く（Open on Webex Board）] を選択します。このオプションは、Webex Board とペアリングしている場合に使用できます。

接続されると、画面のアイコンが増えることに注目してください。また、スペース名が画面の左上に表示され、中央にあった Webex Board 名が表示されなくなります。

4. [ホワイトボード（Whiteboard）] をタップします。

ローカルで作成したすべてのホワイトボードをスペースに移動できるようになったことがわかります。ホワイトボードが複数ある場合は、ホワイトボードをスワイプして、追加するそれぞれのホワイトボードを確認できます。

5. 青色のチェックマークをタップすると、すべてのホワイトボードがスペースに移動します。Webex Board のローカルで作成したすべてのホワイトボードが表示されます。

各クライアントのスペースに、ローカルの Webex Board で作成したすべてのホワイトボードが表示されます。これらのホワイトボードは自由に編集できます。終了したら、ホーム画面に戻ります。

コール（会議）

前に Webex Board から行ったコールはポイントツーポイントコールでした。今度は Webex Meetings を開始するコールを行います。

1. ホーム画面で [コール（Call）] をタップします。

キーボードで番号をダイヤルせずに、そのままスペースをコールします。

このスペースに接続されている他の Webex Teams クライアントで、会議への参加通知を受け取ります。

2. 1 つ以上のクライアントで会議に参加します。
3. 会議中に Webex Board の [ホーム（Home）] ボタンを押します。

会議に複数のクライアントが接続している場合は、各クライアントのビデオが上部のそれぞれの円内に表示されます。一番メインのスピーカーが大きく表示されます。ここではスペース内でホワイトボードを開き、複数のクライアントと同時にホワイトボードを使用できます。Webex Board の別のアプリケーションから切り替えると、リモートユーザのビデオが画面上部に保持され、移動中や作業中にも継続して見ることができます。コールを継続します。

ファイル

1. ホーム画面で [ファイル（Files）] をタップします。
2. スペースで種類の異なるファイルをテストするには、スペースでさまざまな種類のファイル（PowerPoint、Word など）を開きます。利用できるファイルがない場合は、Webex Board で開けるように、ファイルをスペースにアップロードする必要があります。

PowerPoint、Word、PDF を開いた場合は、画面の右側にあるスライドビューアを使用してスライドやページを進めることができます。スライドやページで指を上下にスライドさせると、スライドやページを変更できます。画面をタップして画面右下にある [] アイコンをタップすると、スライドビューの表示/非表示を切り替えることができます。また、2 本の指をドラッグして広げると、ズームできます。ズームは写真などの他の種類のファイルでも使用できます。さまざまな種類のファイルを開いたら、ラボを続行します。

ユーザ

[ユーザ（People）] では、スペース内のユーザのリストを表示できます。通話中は、参加者のリストを表示できます。他のユーザの音声/ビデオをミュートすることもできます。

1. ホーム画面で [ユーザ（People）] をタップします。
2. このスペース内のユーザと、現在通話中の参加者のリストが表示されます。
3. **すべてのデバイス**で通話を終了します。
4. Webex Board の確認が終了したら、画面下部中央の [このスペースを閉じる（Close this space）] をタップします。

スペース名が消え、Webex Board が再度表示されます。また、オプションの数が 3 つに減ります。**ホワイトボード**に戻ると、すべてのホワイトボードがローカルからなくなっていることがわかります。

シナリオ 15.　Webex デバイス用 ebex ハイブリッドコール

Call Service Connect は、Cisco Webex Control Hub と企業の電話システムを接続し、一体として機能させることができるハイブリッドサービスです。オンプレミスのコール制御機能をクラウドに拡張することにより、Webex Cloud デバイスはそれを利用してコールを受発信できます。

組織のコールアクティビティは通常どおり利用できますが、コールアクティビティが Expressway E と C のペアを通じてクラウドに拡張されます。このようにしてユーザが Webex デバイスから PSTN コールを受発信できます。

Call Service Connect では、SIP コールに Expressway のペアが必要になります。このペアは、B2B または MRA 環境にすでに導入されているペアで構いません。

この機能の 2 つの重要な部分は次のとおりです。

- **相互 TLS**：Call Service Connect では、Expressway-E サーバと Cisco Webex Control Hub との間に、相互 TLS 関係を確立する必要があります。このセキュリティ機能により、クラウドと企業のシステムが相互に識別できるようになります。信頼されたルート証明書を両側にインストールする必要があります。
- **Webex-RD（リモートデバイス）（このガイドの執筆時点ではまだ Spark-RD）**：このデバイスは、ユーザの勤務先番号に関連付けられています。それにより、ユーザの Cisco Webex アカウントの SIP ID と企業の SIP ID が関連付けられます。技術的な観点から説明すると、Webex-RD は Cisco Webex からの発信コールをユーザの勤務先番号でマスクします。コールが着信すると、ユーザの Cisco Webex Teams アプリとデスクフォンの両方で呼出音が鳴ります。

この機能は Call Service Aware がベースになっており、インスタントコンテンツ共有、コール履歴に対する迅速なアクセス、任意の場所からリダイヤルできるオプションにより、エンタープライズ コール システムを補完します。Call Service Aware は Call Service Connect をサポートするものであり、前提条件になっています。

以下に、この機能の概要を示します。

- Cisco Webex デバイス用ハイブリッドコールサービスは、オンプレミスの Unified CM で Cisco Webex リモートデバイス（Cisco Webex-RD）を作成/使用して、コールを企業の内線、ユーザ、PSTN にルーティングします。
- オンプレミスの電話機能（保留、転送、会議など）には、Cisco Webex デバイスも含まれます。
- 任意の場所から PSTN またはオンプレミスの内線へのコールは、Unified CM の Cisco Webex-RD に固定されます。
- 詳細な導入ガイドはこちらから参照できます。

Cisco Webex Control Hub Management での Call Service Connect の設定

このセクションでは、Cisco Webex Control Hub の初期設定を行います。設定には、希望する企業のサイト名を指定してすべてのユーザの SIP アドレスを作成する、Call Service Connect を有効にする、相互 TLS を使用する Expressway-E を示す SIP 宛先を指定するなどが含まれます。このラボでは、B2B と MRA を処理する Expressway-C/E ペアが用意されています。また Expressway-E サーバ上の SIP 相互 TLS ポートを示す DNS SRV レコードが必要になります。この SRV は事前設定されてインターネットで公開されているため、セッションで使用することができます。

最初に、ユーザに直接ダイヤルできるように、組織のカスタム SIP ドメインを設定します。

1. **ブラウザ**で Control Hub のタブを再度開きます。
2. 左側のメニューの [設定（Settings）] をクリックします。Control Hub の設定を表示するには、[Cisco Webex CallingのSIPアドレス（SIP Address for Cisco Webex Calling）] セクションまでスクロールします。

SIP ドメインのプレフィックスが表示されています。これは、基本設定中にすでに設定されています。このラボでは、セッションに割り当てられている @cbXXX.dc-YY.com ドメインを使用しています。ラボでは、cbXXXYY に短縮され、ユーザへのダイヤルが簡単になっています。設定後は、プラットフォームで実際の SIP アドレスと DNS レコードが作成され、インターネットでアクセスできるようになります。

ドメイン検証の設定

ドメイン検証は、組織のセキュリティと整合性にとって不可欠な要素です。検証により、Call Service Aware や Call Service Connect などのサービスに必要な特定のドメインを所有しているかどうかが確認されます。

企業にドメインが複数ある場合は、各ドメインを 1 つずつ追加します。たとえば、sales.example.com と support.example.com のユーザがいる場合は、両方のドメインを追加する必要があります。

組織が電子メールアドレスを適用している場合は、ユーザのロックアウトの可能性に関する警告が表示されます。管理者のロックアウトを回避するには、特定の順序でドメインを確認し、削除する必要があります。たとえばドメインを追加する場合は、**管理者ドメインを追加した後で**その他のドメインを追加します。

追加したそれぞれのドメインについて、検証トークンを取得しますので、それらを DNS TXT レコードに追加します。複数のドメインを追加して複数のトークンを取得した場合は、各トークンを個別の DNS TXT レコードに追加することをお勧めします。それができない場合（たとえばプライベートドメインで複数の DNS TXT レコードがサポートされていない場合や、SPF またはカスタムレコードしか編集できない場合）は、手動による検証についてシスコテクニカルサポートにお問い合わせください。

DNS TXT レコードに検証トークンを追加する場合は、次の 2 つのことが推奨されます。

- DNS TXT レコードの最初に、行を分けてトークンを入力します。
- プレフィックス：**cisco-ci-domain-verification=<token>** を付けてトークンを入力します。この一意の ID は以後の検索機能に使用できます。またシスコの検証トークンと、DNS TXT レコード内のその他の情報を区別するためにも役立ちます。

上記の内容は情報提供のみを目的としています。ラボでは、DNS TXT レコードがセッション用にすでに作成されています。ドメインの検証は事前に設定されていますが、確認してみましょう。

[Cisco Webex Calling用SIPアドレス（SIP Address for Cisco Webex Calling）] の上にある [設定（Settings）] ページに [ドメイン（Domains）] セクションがあります。基本設定では、ドメインが事前設定されていることを確認しました。したがって、次の手順は参照のためだけのものであり、ラボで実施する必要はありません（何らかの理由でドメインがリストされておらず検証されていない場合は、以下の手順を実施すれば設定できます）。

1. [ドメインの追加（Add Domain）] をクリックします。
2. セッションに割り当てられたドメインがボックスに表示されます。表示されない場合はここで入力します。
3. [追加（Add）] をクリックします。
4. ステータスが [保留中（pending）] [• pending] として登録されます。
5. **省略記号**アイコン [···] をクリックし、メニューから [ドメインの検証（Verify Domain）] を選択します。

ポップアップ画面が開き、DNS 検証トークンが表示されます。

先に説明したように、検証トークンを取得して、追加するドメインを解決する DNS サーバに TXT レコードを作成します。TXT レコードを作成したら、[検証（Verify）] ボタンをクリックしてドメインを検証します。検証トークンが見つかって一致すると、ドメインのステータスが [検証済み（Verified）] に変わります。

検証トークンを追加できなかった場合は、再度 DNS サーバに追加してください。DNS キャッシュが更新されたら、DNS サーバの TXT レコードについて存続時間（TTL）を確認します。エラーを何時間または何日もキャッシュするように TTL を設定できます。

このラボでは、DNS TXT レコードがすでに追加されているため、新たに追加する必要はありません。

6. [検証（Verify）] をクリックします。

[検証（Verify）] をクリックすると、ステータスが [検証済み（Verified）] [• verified] に変わります。

コールコネクタの有効化

1. [サービス（Services）] タブをクリックします。[ハイブリッドコール（Hybrid Call）] で、[セットアップ（Set up）] をクリックします。
2. [ハイブリッドコールサービスの設定（Hybrid Call Service Setup）] ポップアップウィンドウで、[次へ（Next）] をクリックします。
3. [既存のExpresswayクラスタを選択してこのサービスにリソースを追加する（Select an existing Expressway cluster to add resources to this service）] を選択します。ドロップダウン リスト ボックスを使用して [HS Cluster 1] を選択します（この名前はカレンダーサービスのシナリオで指定したものです。別の名前を付けた場合は、その名前を選択してください）。

注：ハイブリッド カレンダー セクションをスキップした場合は、新しい Expressway をここで登録する必要があります。これはすでにハイブリッド カレンダー セクションで完了しています。Expressway を登録するには、最初の**オプションボタン**を選択し、ボックスに **exp-cc.dcloud.cisco.com** と入力して [次へ（Next）] をクリックします。最後に名前として **HS Cluster 1** と入力します。登録したら以下の手順を続行できます。

4. [次へ（Next）] をクリックします。
5. [Expresswayに進む（Go to Expressway）] をクリックします。
6. **admin/dCloud123!** でログインします。

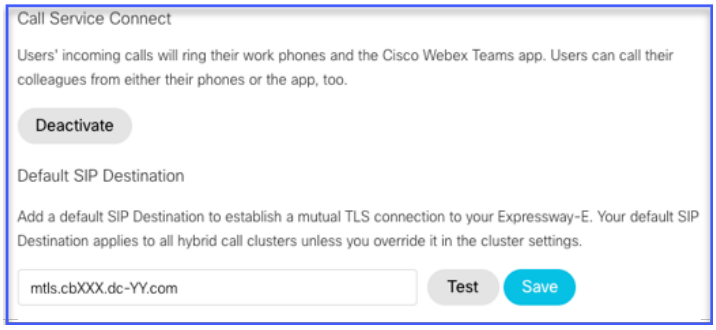
注：繰り返しになりますが、ハイブリッド カレンダー セクションをスキップした場合は、新しい Expressway をここで登録する必要があります。これはすでにハイブリッド カレンダー セクションで完了しています。Expressway を登録するには、[この信頼に必要なExpressway CA証明書はシスコが管理する（I want Cisco to manage the Expressway CA certificates required for this trust）] のチェックボックスをオンにします。次に、[登録（Register）] をクリックします。次の画面で、[Expresswayへのアクセスを許可（Allow Access to the Expressway）] チェックボックスをオンにし、[続行（Continue）] をクリックします。

このサービスをアクティブにすると、新しいコールコネクタのダウンロードが開始され、管理コネクタによって Expressway-C コネクタホストにインストールされます。Expressway ホストの [サービスステータス（Service Status）] が [未設定（Not configured）] になることで、コールコネクタが正常にダウンロードされてインストールされたことがわかります。

Call Service Connect の SIP 宛先設定

1. Control Hub の [サービス（Services）] タブに戻り、[ハイブリッドコール（Hybrid Call）] の [設定の編集（Edit settings）] をクリックします。
2. [コールサービス（Call Service）] ページで、[Call Service Connect] セクションにスクロールします。
3. [アクティブ化（Activate）] をクリックしてサービスを起動します。
4. サービスを起動した後で表示される [SIP宛先（SIP Destination）] ボックスに **mtls.cbXXX.dc-YY.com** と入力し、[保存（Save）] をクリックします（XXX と YY は、セッションに割り当てられている数字に置き換えてください）。

コールサービス設定



これで、セッション用に作成された DNS SRV レコード（**_sips._tcp.mtls.cbXXX.dc-YY.com**）がポイントされます。

このページでは、いつかの項目を設定できます。

[全般（General）] セクションでは、前述のカレンダーサービスや、サービスに影響するアラームやソフトウェアのアップグレードがある場合の電子メール通知などのオプションを利用できます。

[Call Service Connect] セクションの一番下までスクロールすると、自己署名証明書をアップロードするためのオプションがあります。

最後に、このページでサービスを非アクティブ化してすべてのユーザからサービスを削除し、Expressway コネクタホストからコネクタを削除します。

Expressway-C コネクタホストでのコールコネクタの設定

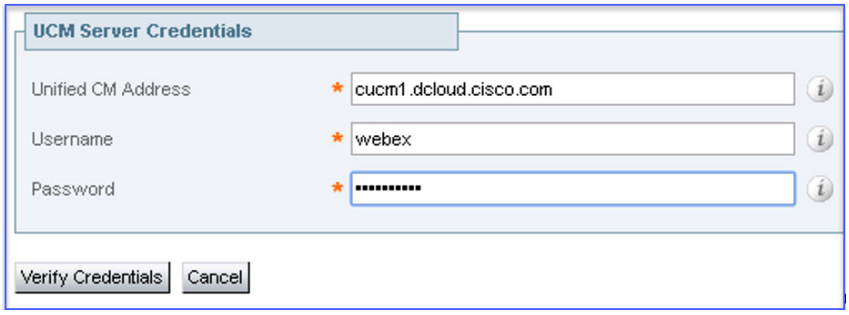
以下のいくつかのセクションでは、Cisco Webex Hybrid Call Service Aware 用に Expressway-C ホストを設定します。

1. ブラウザで以前開いた [Expresswayコネクタホスト（Expressway connector host）] タブに戻ります。
2. [コネクタ管理（Connector Management）] ページで、[コールコネクタ（Call Connector）] リンクをクリックします。また、[アプリケーション（Applications）] > [ハイブリッドサービス（Hybrid Services）] > [コールサービス（Call Service）] > [Unified CMサーバ（Unified CM Servers）] の順に選択して確認することもできます。
3. [設定済みUnified CMサーバ（Unified CM servers configured）] リンクをクリックします。
4. [新規（New）] をクリックします。
5. 以下の表に従ってパラメータを設定します。

表 37. Unified CM サーバ

設定対象	設定内容
[Unified CM アドレス（Unified CM Address）]	cucm1.dcloud.cisco.com
[ユーザ名（Username）]	webex
[パスワード（Password）]	dCloud123!

Unified CM サーバの設定



注：Webex ユーザアカウントは事前に設定されています。このアカウントの作成方法の詳細については、**付録 B** を参照してください。

6. [ログイン情報の確認（Verify Credentials）] をクリックします。
7. ページが更新されると、新しく [Call Service Connectの設定（Call Service Connect Configuration）] セクションが表示されます。
8. 以下の表に従って設定します。

注：ドロップダウン メニューで [自動（Automatic）] に変更すると、残りのフィールドが表示されます。

表 38. Call Service Connect の設定

設定対象	設定内容
[Cisco Webexリモートデバイスの設定タイプ（Cisco Webex Remote Device Configuration Type）]	[自動（Automatic）]
[デバイスプール（Device Pool）]	dCloud_DP
[場所（Location）]	Hub_None
[コーリングサーチスペース（Calling Search Space）]	Call_Everyone
[コーリングサーチスペースの再ルーティング（Reroute Calling Search Space）]	Call_Everyone

9. [追加（Add）] をクリックします。

CTI と AXL のステータスが UNABLE_CONNECT ステータスになる場合があります。このステータスは後で変わるため、**無視して構いません。**

10. [アプリケーション（Applications）] > [ハイブリッドサービス（Hybrid Services）] > [コールサービス（Call Service）] > [コールサービスの概要（Call Service Overview）] の順に移動します。
11. [アクティブ（Active）] ドロップダウンメニューを [有効（Enabled）] に変更し、[保存（Save）] をクリックします。

ページが更新されると、ステータスが実行中 [Running] になります。

Call Service Connect 用 Cisco Unified CM 設定

以下のいくつかのセクションでは、Cisco Webex Hybrid Call Service Connect 用に Expressway-C ホストと Unified CM を設定します。

Cisco Unified Communications Manager を設定し、Expressway-C 経由で Expressway-E から直接コールを受信し、クラウドとエンタープライズ間の URI ルーティングを円滑にすることができます。

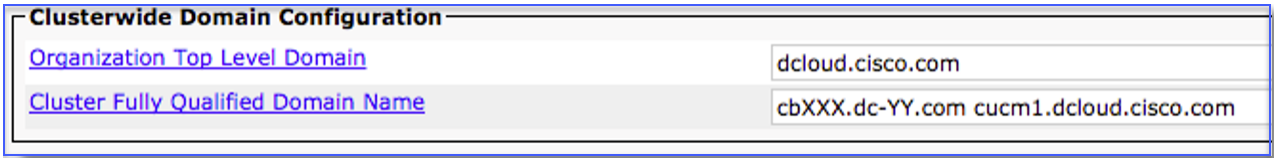
注：Cisco Webex Control Hub は発信者 ID のマスキングをサポートしていません。発信者 ID がブロックされると、実際は同僚と話しているのにゲスト発信者の ID が表示されるなど、コール中に問題が発生する場合があります。このような問題を回避するには、設定に関して全体的に次の点に注意する必要があります。

- Expressway-C と Unified CM の間の SIP トランクは発信者 ID を送信する必要がある

- Call Service Connect で認証されているユーザの発信者 ID は、発信側クラスタおよびクラスタ間トランクなどのコールパス上でブロックされてはならない

1. Web ブラウザの Unified CM（https://198.18.133.3/ccmadmin）タブに戻り、必要に応じて、以下のログイン情報を使用してログインします。
   - ユーザ名：**administrator**
   - パスワード：**dCloud123!**
2. 次に、クラスタの完全修飾ドメイン名パラメータを設定します。すでに Webex Edge Audio シナリオを実施している場合、このタスクは完了しています。この場合は、**ステップ 7 に進みます**。
3. [システム（System）] > [エンタープライズパラメータ（Enterprise Parameters）] に移動します。
4. 「**fully**」で検索（**Ctrl + F**）すると、[クラスタの完全修飾ドメイン名（Cluster Fully Qualified Domain Name）] の設定画面が表示されます。
5. **cucm1.dcloud.cisco.com** の FQDN がすでに設定されています。ボックス内の FQDN はそのままにして、先頭にセッションのドメイン名（**cbXXX.dc-YY.com**）を入力し、2 つのドメイン間にスペースを入れます。XXX と YY は、自分のドメイン情報に置き換えてください。

クラスタの完全修飾ドメイン名



注：Webex で使用するドメイン名がリストの先頭に記載される必要があります。Cisco Webex Control Hub では最初のエントリが使用され、その他のエントリは無視されます。

6. [保存（Save）] をクリックします。

7. [デバイス（Device）] > [デバイス設定（Device Settings）] > [SIPプロファイル（SIP Profile）] に移動し、[検索（Find）] をクリックします。
8. [Cisco VCS用の標準SIPプロファイル（Standard SIP Profile For Cisco VCS）] という既存のプロファイルの横の**コピー**アイコン [] をクリックします。
9. [名前（Name）] を [Cisco Webex Hybrid Call用の標準SIPプロファイル（Standard SIP Profile For Cisco Webex）] に変更します。また、必要に応じて説明を変更します。
10. ページ下部にある [トランク固有の設定（Trunk Specific Configuration）] セクションの [音声コールとビデオコールに対するEarly Offerサポート（Early Offer support for voice and video calls）] 設定で、オプションの [ベストエフォート（MTPの挿入なし）（Best Effort (no MTP inserted)）] を選択します。

音声コールおよびビデオコールに対する Early Offer サポート

11. [保存（Save）] をクリックします。

注：ラボには、MRA および B2B を実行する既存の Expressway-C/E ペアがあるため、異なるポートを使用する別の SIP トランク セキュリティ プロファイルを作成する必要があります。C/E ペアでは現在ポート 5560 が使用されています。ハイブリッドサービスでは 5561 を使用することをお勧めします。

12. [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）] を選択し、[検索（Find）] をクリックします。
13. [非セキュアSIPトランクプロファイル（Non Secure SIP Trunk Profile）] という既存のプロファイルの横の**コピー**アイコン [] をクリックします。
14. [名前（Name）] を [Webex ハイブリッドコール用の非セキュア SIP トランクプロファイル（Non Secure SIP Trunk Profile for Webex Hybrid Call）] に変更し、必要に応じて説明を追加します。
15. [着信ポート（Incoming Port）] を **5561** に変更し、[保存（Save）] をクリックします。
16. [デバイス（Device）] > [トランク（Trunk）] を選択し、[新規追加（Add New）] をクリックします。
17. [トランクタイプ（Trunk Type）] を [SIPトランク（SIP Trunk）] に変更します。その他はデフォルト値のままにして、[次へ（Next）] をクリックします。
18. 以下の表に従って設定します。

表 39.　ハイブリッドサービスのトランク設定

設定対象	設定内容
[デバイス情報（Device Information）] > [デバイス名（Device Name）]	Webex_Hybrid_Call
[デバイス情報（Device Information）] > [デバイスプール（Device Pool）]	dCloud_DP
[アウトバウンドコール（Outbound calls）] > [発呼側および接続側情報形式（Calling and Connected Party Info Format）]	[接続側にのみURIおよびDNを配信（可能な場合）（Deliver URI and DN in connected party, if available）]
[SIP情報（SIP information）] > [接続先アドレス（Destination Address）]	198.18.133.152（B2B/MRA で使用される既存の Expressway-C）
[SIP情報（SIP Information）] > [SIPトランクセキュリティプロファイル（SIP Trunk Security Profile）]	[WebexハイブリッドコールSIPトランクプロファイル（Non Secure SIP Trunk Profile for Webex Hybrid Call）]
[SIP情報（SIP Information）] > [SIPプロファイル（SIP Profile）]	[Cisco Webex用の標準SIPプロファイル（Standard SIP Profile For Cisco Webex）]

19. [保存（Save）]、[OK]、[リセット（Reset）]、[リセット（Reset）]、[閉じる（Close）] の順にクリックします。

最後に、この新しい SIP トランクを Expressway-C サーバに送信する、クラウド URI IPv4 パターンに一致する SIP ルートパターンを設定します。

20. [コールルーティング（Call Routing）] > [SIPルートパターン（SIP Route Pattern）] に移動します。[新規追加（Add New）] をクリックします。

21. 以下の表に従って設定します。

表 40.　SIP ルートパターン

設定対象	設定内容
[IPv4パターン（IPv4 Pattern）]	*.[rooms][calls][meet].webex.com
[説明（Description）]	Cisco Webex へのルーティング
[SIPトランク/ルートリスト（SIP Trunk/Route List）]	Webex_Hybrid_Call

注：ラボで以前 Video Mesh に対して *.webex.com を設定（別のトランクをポイント）したときよりも、より限定したパターンを指定しています。そのトランクは、サポートされていない Video Mesh Node をポイントしています。今回のパターンを使用すると、Expressway が直接ポイントされ、正しいゾーンが使用されます。

22. [保存（Save）] をクリックします。

ハイブリッドコールサービス用 Expressway-E の設定

エンタープライズコールは、Expressway-C/E ペアを経由してルーティングされます。このラボでは、Call Service Connect をサポートするように Expressway サーバを設定します。ラボの Expressway-C/E ペアは MRA と B2B をサポートするように設定されているため、設定済みのトラバーサルゾーンがすでにいくつか存在しています。この既存のトラバーサル設定を変更し、Call Service Connect をサポートする新しい設定を作成します。

1. Workstation 1 のブラウザをまだ開いていない場合は、新しいブラウザタブで [コラボレーション管理リンク（Collaboration Admin Links）] > [Cisco Expressway-E] の順に選択します。
2. 次のログイン情報を使用してログインします。
   - ユーザ名：**admin**
   - パスワード：**dCloud123!**
3. 次に、相互 TLS を設定します。すでに Webex Edge Audio シナリオを実施している場合、これらの手順は完了しているため、**ステップ 8 にスキップ**できます。
4. [設定（Configuration）] > [プロトコル（Protocols）] > [SIP] の順に移動します。
5. [相互TLSモード（Mutual TLS Mode）] で、ドロップダウンメニューから [オン（On）] を選択します。
6. [相互TLSポート（Mutual TLS port）] は **5062** のままにします。
7. [保存（Save）] をクリックします。
8. [設定（Configuration）] > [ゾーン（Zones）] > [ゾーン（Zones）] の順に移動し、[デフォルトゾーン（Default Zone）] のリンクをクリックします。

今回は既存の Expressway-E サーバであるため、[デフォルトゾーンで相互TLSを有効にする（Enable Mutual TLS on Default Zone）] を [オフ（Off）] にする必要がありますが、デフォルトのため、改めて設定する必要はありません。ただし、Call Service Connect 専用の新しい Expressway-E サーバである場合は設定を [オン（On）] にする必要があります。

Expressway-E Webex ゾーンの設定（X8.11 以降）

次に、Expressway-E サーバが Cisco Unified CM と Cisco Webex Control Hub 間のコールを識別してルーティングできるように、新しい DNS ゾーンを作成する必要があります。

1. Expressway-E サーバで、[設定（Configuration）] > [ゾーン（Zones）] > [ゾーン（Zones）] の順に移動し、[新規（New）] をクリックします。

注：このラボでは、Expressway のバージョンは X8.11 以上です。それよりも前のバージョンではこのゾーンは設定できないため、通常の DNS ゾーンを使用する必要があります。必要に応じて設定を表示するには**ここ**をクリックします。Webex Edge Audio セクションでこのゾーンをすでに作成している場合は、次の 3 つのステップをスキップします。

2. [ゾーン（Zones）] ページで [新規（New）] をクリックします。
3. [タイプ（Type）] で [Webex] を選択します。
4. [ゾーンの作成（Create Zone）] をクリックします。

Expressway-C に対するセキュア トラバーサル サーバ ゾーンの設定

Expressway-E に専用のトラバーサルサーバゾーンを作成します。Cisco Webex トラフィックは MRA または B2B と同じトラバーサルゾーン上に共存できますが、Expressway-E に専用のトラバーサルサーバゾーンを作成することをお勧めします（特にハイブリッドコールのシグナリングとメディアを処理する場合）。それにより、B2B または MRA の設定が Cisco Webex のトラフィックに影響することも、その逆もなくなります。

1. [ゾーン（Zones）] ページで [新規（New）] をクリックします。
2. 以下の表に従って設定します。

表 41. Cisco Webex トラバーサルゾーン

設定対象	設定内容
[設定（Configuration）] > [名前（Name）]	Webex ハイブリッドコール用のトラバーサルサーバ
[設定（Configuration）] > [タイプ（Type）]	[トラバーサルサーバ（Traversal server）]
[接続ログイン情報（Connection credentials）] > [ユーザ名（Username）]	cisco
[H.323] > [モード（Mode）]	オフ
[SIP] > [ポート（Port）]	7006
[SIP] > [TLS検証モード（TLS verify mode）]	オン
[SIP] > [TLS検証サブジェクト名（TLS verify subject name）]	vcsc.dcloud.cisco.com
[SIP] > [メディア暗号化モード（Media encryption mode）]	[強制暗号化（Force encrypted）]
[SIP] > [プリロードされたSIPルートのサポート（Preloaded SIP routes support）]	オン
[SIP] > [SIPパラメータの保持（SIP parameter preservation）]	オン

3. [ゾーンの作成（Create Zone）] をクリックします。

Expressway-E の検索ルールの作成

次に、以下を目的とした 2 つの検索ルールを作成します。

- Cisco Webex Control Hub からのコールを識別し、トラバーサルゾーンを経由して Expressway-C にルーティングする
- Cisco Unified CM からのコールを識別し、DNS ゾーンを経由して Cisco Webex Control Hub にルーティングする

1. [設定（Configuration）] > [ダイヤルプラン（Dial Plan）] > [検索ルール（Search Rules）] の順に移動し、[新規（New）] をクリックします。
2. 以下の表に従って設定します。

表 42. Expressway-E の検索ルールの設定

設定対象	設定内容
[設定（Configuration）] > [ルール名（Rule Name）]	着信 Webex ハイブリッドコール
[設定（Configuration）] > [説明（Description）]	Webex から Exp-C にトラフィックをルーティングする
[設定（Configuration）] > [プライオリティ（Priority）]	99
[設定（Configuration）] > [プロトコル（Protocol）]	SIP
[設定（Configuration）] > [送信元（Source）]	[指定（Named）]
[設定（Configuration）] > [送信元名（Source Name）]	[Webexゾーン（Webex Zone）]
[設定（Configuration）] > [一致した場合（On successful match）]	[停止（Stop）]
[設定（Configuration）] > [転送先（Target）]	Webex ハイブリッドコール用のトラバーサルサーバ

3. [検索ルールの作成（Create search rule）] をクリックします。
4. [新規（New）] をクリックします。
5. 以下の表に従って設定します。

表 43. Expressway-E の検索ルールの設定

設定対象	設定内容
[設定（Configuration）] > [ルール名（Rule Name）]	発信 Webex ハイブリッドコール
[設定（Configuration）] > [説明（Description）]	Unified CM から Webex にトラフィックをルーティングする
[設定（Configuration）] > [プライオリティ（Priority）]	99
[設定（Configuration）] > [プロトコル（Protocol）]	SIP
[設定（Configuration）] > [送信元（Source）]	[指定（Named）]
[設定（Configuration）] > [送信元名（Source Name）]	Webex ハイブリッドコール用のトラバーサルサーバ
[設定（Configuration）] > [モード（Mode）]	[エイリアスパターンマッチ（Alias pattern match）]
[設定（Configuration）] > [パターンタイプ（Pattern type）]	[正規表現（Regex）]
[設定（Configuration）] > [パターン文字列（Pattern string）]	.+@.+\.(calls|rooms|meetup)\.webex\.com.*
[設定（Configuration）] > [パターン動作（Pattern behavior）]	[変更なし（Leave）]
[設定（Configuration）] > [一致した場合（On successful match）]	[停止（Stop）]
[設定（Configuration）] > [転送先（Target）]	[Webexゾーン（Webex Zone）]

6. [検索ルールの作成（Create search rule）] をクリックします。

Call Service Connect 用 Expressway-C 設定

次に、Call Service Connect をサポートするように、Expressway-C/E ペアのもう一方を設定します。先に変更した Expressway-E サーバと同様に、既存の設定の変更および新しい設定を行います。

Expressway-E に対するセキュア トラバーサル クライアント ゾーンの設定

Expressway-E サーバのゾーンと同様に、Expressway-C に Cisco Webex 専用のトラバーサルゾーンを作成することをお勧めします。

1. Expressway-C サーバ（**vcsc.dcloud.cisco.com**）をまだ開いていない場合は新しいタブを開き、ユーザ名：**admin**、パスワード：**dCloud123!** でログインします。
2. [設定（Configuration）] > [ゾーン（Zones）] > [ゾーン（Zones）] に移動します。
3. [ゾーン（Zones）] ページで [新規（New）] をクリックします。
4. 以下の表に従って設定します。

表 44. Cisco Webex 用のトラバーサルゾーン

設定対象	設定内容
[設定（Configuration）] > [名前（Name）]	Webex ハイブリッドコール用のトラバーサルクライアント
[設定（Configuration）] > [タイプ（Type）]	[トラバーサルクライアント（Traversal client）]
[接続ログイン情報（Connection credentials）] > [ユーザ名（Username）]	cisco
[接続ログイン情報（Connection credentials）] > [パスワード（Password）]	dCloud123!
[H.323] > [モード（Mode）]	オフ
[SIP] > [ポート（Port）]	7006
[SIP] > [TLS検証モード（TLS verify mode）]	オン
[SIP] > [メディア暗号化モード（Media encryption mode）]	[強制暗号化（Force encrypted）]
[SIP] > [プリロードされたSIPルートのサポート（Preloaded SIP routes support）]	オン
[SIP] > [SIPパラメータの保持（SIP parameter preservation）]	オン
[ロケーション（Location）] > [ピア1アドレス（Peer 1 Address）]	vcse.cbXXX.dc-YY.com

5. [ゾーンの作成（Create Zone）] をクリックします。

各 Unified CM クラスタのネイバーゾーンの作成

ルーティング先の Cisco Unified CM クラスタに対するゾーンを設定します。各ゾーンには、6 つのノードで Cisco Unified Communications Manager クラスタをサポートする、6 つのピアアドレスを設定できます。ゾーンのルーティング先の Cisco Unified Communications Manager クラスタは、ホームクラスタにする必要があります。SME またはその他の中間ルーティングエージェントにすることはできません。

各ゾーンで使用するポートは、Cisco Unified CM で設定される SIP トランクのセキュリティプロファイルによって決まります。これらの Expressway では B2B と MRA が設定されているため、異なるポートを使用して、新しい設定が既存の設定に影響を与えないようにすることをお勧めします。推奨するポートは 5062 ですが、任意のポートを使用できます。このラボでは、先ほど SIP トランク セキュリティ プロファイルで設定したポート 5561 を使用します。Jabber MRA 用の Cisco Unified CM に対する既存のネイバーゾーンを再利用することはありません。

1. Expressway-C の [ゾーン（Zones）] ページで [新規（New）] をクリックします。
2. 以下の表に従って設定します。

表 45. Expressway-C のネイバーゾーンの設定

設定対象	設定内容
[設定（Configuration）] > [名前（Name）]	Webex ハイブリッドコール用 UCM ネイバー
[設定（Configuration）] > [タイプ（Type）]	[ネイバー（Neighbor）]
[H.323] > [モード（Mode）]	オフ
[SIP] > [ポート（Port）]	5561
[SIP] > [トランスポート（Transport）]	TCP
[ロケーション（Location）] > [ピア1アドレス（Peer 1 Address）]	cucm1.dcloud.cisco.com

3. [ゾーンの作成（Create Zone）] をクリックします。

Expressway-C での検索ルールの設定

次に、Expressway-E サーバと同様に、Unified CM とクラウド間でトラフィックをルーティングするための検索ルールを 2 つ作成します。

1. [設定（Configuration）] > [ダイヤルプラン（Dial Plan）] > [検索ルール（Search Rules）] の順に移動し、[新規（New）] をクリックします。
2. 以下の表に従って設定します。

表 46. Expressway-C の検索ルールの設定

設定対象	設定内容
[設定（Configuration）] > [ルール名（Rule Name）]	着信 Webex ハイブリッドコール
[設定（Configuration）] > [説明（Description）]	Exp-E から Unified CM にトラフィックをルーティングする
[設定（Configuration）] > [プライオリティ（Priority）]	99
[設定（Configuration）] > [プロトコル（Protocol）]	SIP
[設定（Configuration）] > [送信元（Source）]	[指定（Named）]
[設定（Configuration）] > [送信元名（Source Name）]	Webex ハイブリッドコール用のトラバーサルクライアント
[設定（Configuration）] > [一致した場合（On successful match）]	[停止（Stop）]
[設定（Configuration）] > [転送先（Target）]	Webex ハイブリッドコール用 UCM ネイバー

3. [検索ルールの作成（Create search rule）] をクリックします。
4. [新規（New）] をクリックします。
5. 以下の表に従って設定します。

表 47. Expressway-C の検索ルールの設定

設定対象	設定内容
[設定（Configuration）] > [ルール名（Rule Name）]	発信 Webex ハイブリッドコール
[設定（Configuration）] > [説明（Description）]	Unified CM から Exp-E にトラフィックをルーティングする
[設定（Configuration）] > [プライオリティ（Priority）]	99
[設定（Configuration）] > [プロトコル（Protocol）]	SIP
[設定（Configuration）] > [送信元（Source）]	[任意（Any）]（デフォルト）
[設定（Configuration）] > [モード（Mode）]	[エイリアスパターンマッチ（Alias pattern match）]
[設定（Configuration）] > [パターンタイプ（Pattern type）]	[正規表現（Regex）]
[設定（Configuration）] > [パターン文字列（Pattern string）]	.+@.+\.(calls|rooms|meetup)\.webex\.com.*
[設定（Configuration）] > [パターン動作（Pattern behavior）]	[変更なし（Leave）]
[設定（Configuration）] > [一致した場合（On successful match）]	[停止（Stop）]
[設定（Configuration）] > [転送先（Target）]	Webex ハイブリッドコール用のトラバーサルクライアント

6. [検索ルールの作成（Create search rule）] をクリックします。

Cisco Webex デバイス用ハイブリッドコールサービスの設定

以下に、機能の概要を示します。

- Cisco Webex デバイス用ハイブリッドコールサービスは、オンプレミスの Unified CM で Cisco Webex リモートデバイス（Cisco Webex-RD）を作成/使用して、コールを企業の内線、ユーザ、PSTN にルーティングします。
- オンプレミスの電話機能（保留、転送、会議など）には、Cisco Webex デバイスも含まれます。
- 任意の場所から PSTN またはオンプレミスの内線へのコールは、Unified CM の Cisco Webex-RD に固定されます。

任意の場所に対するディレクトリ番号の作成

Cisco Unified CM Administration を使用して、後から任意の場所のデバイスに割り当てるディレクトリ番号を設定します。また、ディレクトリ URI をディレクトリ番号に割り当てます。

1. Workstation 1（198.18.1.36）で Chrome を開きます。ホームページで [コラボレーション管理リンク（Collaboration Admin Links）] > [Cisco Unified Communications Manager] を選択します。
2. [Cisco Unified Communications Manager] をクリックして、**administrator/dCloud123!** でログインします。
3. [コールルーティング（Call Routing）] > [ディレクトリ番号（Directory Number）] を選択し、[新規追加（Add New）] をクリックします。
4. 新しいディレクトリ番号に対して、次の表の情報を入力します。

表 48. ディレクトリ番号の設定

設定対象	設定内容
[ディレクトリ番号に関する情報（Directory Number Information）] > [ディレクトリ番号（Directory Number）]	\+19725557800
[ディレクトリ番号に関する情報（Directory Number Information）] > [ルートパーティション（Route Partition）]	Base_PT
[ディレクトリ番号に関する情報（Directory Number Information）] > [呼び出し表示（Alerting Name）]	Hybrid Device
[ディレクトリ番号に関する情報（Directory Number Information）] > [ASCII呼び出し表示（ASCII Alerting Name）]	Hybrid Device
[ディレクトリ番号設定（Directory Number Setting）] > [コーリングサーチスペース（Calling Search Space）]	Call_Everyone

5. [保存（Save）] をクリックします。
6. ページが更新されたら、[ディレクトリURI（Directory URIs）] セクションの URI ボックスに **hdevice@cbXXX.dc-YY.com** と入力します。
7. パーティションに **Base_PT** を選択します。
8. [保存（Save）] をクリックします。

任意の場所に対する Unified CM アカウントの作成

デバイスがクラウドに登録されていても、番号をオンプレミスの Cisco Unified Communications Manager（Unified CM）のアカウントに関連付け、Unified CM のエンドユーザアカウントを使用して場所を表すことができます。場所には、物理的な場所にある、Cisco Webex に登録済みのデバイスが含まれます。

このアカウントは、実際のユーザには関連付けられていません。アカウントはデバイスを示し、Unified CM ダイヤルプールから該当の場所のデバイスに PSTN 番号または内線番号を割り当てます。

ユーザのハイブリッドコール環境用のコールコネクタによって、デバイスを示すアカウントと場所が関連付けられます。コネクタは、その特定の場所にサービスを提供する Unified CM クラスタを識別し、ディレクトリ番号と URI、および Cisco Webex SIP アドレスを割り当てます。また、Cisco Webex リモートデバイス（Cisco Webex - RD）によって、クラウドとオンプレミスのアクティビティが結びつけられます。

考慮すべきポイント：

- 電子メールアドレスのドメインは、Cisco Webex Control Hub で検証済みのドメインエントリの 1 つでなければなりません。
- **Hybrid Call Service Aware と Connect** を組織に対して有効にする必要がありますが、Cisco Webex Control Hub でハイブリッドサービス用に Cisco Webex ユーザアカウントを有効にする必要はありません。
- [メールID（Mail ID）] は Cisco Webex 側の設定値とオンプレミス側の設定値が完全一致する必要があります。
- 電子メールアドレスは一意でなければなりません。複数の Cisco Webex の場所、または、1 人の Cisco Webex ユーザと 1 つの場所で同じアカウントは使用できません。
- ユーザの [ディレクトリURI（Directory URI）] は、該当の場所用に作成したディレクトリ番号のディレクトリ URI と一致する必要があります。
- [電話番号（Telephone Number）] は、ハイブリッドサービスが有効になっている場所に表示される番号です。社内の番号または内線番号も使用できます。1 つの場所に複数のデバイスがある場合は、ディレクトリ番号は、共有回線のように、すべてのデバイスに割り当てられます。技術的な観点から説明すると、この番号へのコールは、割り当てられた Cisco Webex SIP アドレスに送信されます。そのアドレスは、Cisco Webex が該当の場所のすべてのデバイスにフォークするアドレスです。

1. [ユーザ管理（User Management）] > [エンドユーザ（End User）] の順に移動します。
2. [新規追加（Add New）] をクリックします。
3. 新しいディレクトリに対して、次の表の情報を入力します。

表 49.　ユーザ設定

設定対象	設定内容
[ユーザ情報（User Information）] > [ユーザID（User ID）]	hdevice
[ユーザ情報（User Information）] > [姓（Last Name）]	Device
[ユーザ情報（User Information）] > [名（First Name）]	Hybrid
[ユーザ情報（User Information）] > [ディレクトリURI（Directory URI）]	hdevice@cbXXX.dc-YY.com
[ユーザ情報（User Information）] > [電話番号（Telephone Number）]	7800 DN に変換されるハイブリッドデバイス DID については dCloud セッションの詳細情報を参照してください。また、Workstation 1 のデスクトップにある DN_to_DID.txt という名前のテキストファイルでも確認できます。
[ユーザ情報（User Information）] > [メールID（Mail ID）]	hdevice@cbXXX.dc-YY.com

4. [保存（Save）] をクリックします。

ハイブリッドコールの場所の作成および更新

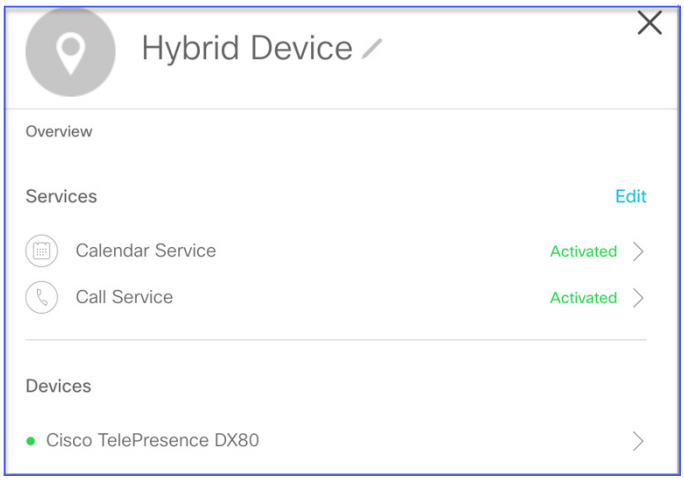
最後のステップでは、Room デバイス用に以前作成した場所を更新します。

1. Cisco Webex Control Hub（https://admin.webex.com）に戻り、[場所（Places）] メニューを選択します。

注：次の手順では、すでに Control Hub にデバイスが追加されていることを前提としています。Control Hub にデバイスが追加されていない場合は、[Roomデバイスの追加（Add a Room Device）] セクションに移動し、手順に従って新しいデバイスを追加します。デバイスが、Webex Edge for Devices シナリオの Unified CM に登録されたままの場合は、最初に作成した場所を削除し、新しい場所を作成してクラウドに登録します。デバイスを登録したら、次の手順に戻ります。手順を確認するだけの場合は、仮のデバイスを追加することもできます。

2. **以前作成した場所**を選択し、ポップアップウィンドウで [編集（Edit）] をクリックします。
3. [ハイブリッドコール（Hybrid Calling）] オプションボタンを選択し、[次へ（Next）] をクリックします。
4. Unified CM 上で設定したメール ID（**hdevice@cbXXX.dc-YY.com**）を入力します。[パスワード（Password）] が事前に入力されている場合は削除して空白のままにします。[保存（Save）] をクリックします。
5. テストする前にコールサービスがアクティブになるのを待ちます（以下の図はコールサービスがアクティブになった状態）。

コールサービスがアクティブになった状態



ハイブリッド Room デバイスのテスト

コールサービスがアクティブになったら、画面左上に DID が表示されます。PSTN 電話からこの番号にダイヤルすると、Room デバイスが鳴ります。また、PSTN への発信も可能です。発信ダイヤルルールとパターンについては、発信ダイヤルパターンおよび国際電話のブロックを参照してください。

注：コールサービスがアクティブになる前に Room デバイスを登録した場合は、DID がすぐに表示されない場合があります。コールサービスがアクティブになっている状態で番号が表示されるまで待ちたくない場合は、デバイスを再起動します。再起動すると番号が表示されます。

シナリオ 16.　シングルサインオン（SSO）

このシナリオでは、Microsoft Azure またはオンプレミスの AD FS を使用してシングルサインオンを設定します。SSO を設定しない場合は、Cisco Webex の基本的な認証機能を使用します。その場合は、各ユーザが最初に Cisco Webex にログインする際に、パスワードを設定する必要があります。これについてはラボで確認しました。SSO では Azure または Active Directory のパスワードを使用できるため、ユーザは Cisco Webex から提供される別のログイン情報ではなく、ドメインのログイン情報を使用して Webex にサインインできます。

一度に設定できるプロバイダーは 1 つだけです。必要に応じて、1 つの設定を無効にして別の設定を有効にすることができます。最初の設定手順では、Microsoft Azure について説明します。O365 と Webex Teams の統合シナリオで作成したトライアル版とユーザを利用します。必要に応じて、独自の O365 組織を使用することもできます。ラボで SSO を設定する 2 番目の手順では、Microsoft AD FS を使用します。どちらの場合も、Cisco Webex メタデータをダウンロードする必要があります。

Cisco Webex メタデータのダウンロード

Cisco Webex メタデータファイルは、AD FS 環境で Cisco Webex 認証サービスと通信するために必要な情報がすべて含まれている XML ファイルです。

1. Control Hub に戻り、必要に応じて Charles でサインインします（**cholland@cbXXX.dc-YY**.com/**dCloud123!**）。
2. [概要（Overview）] ページで、ページ下部の [ライセンス（Licenses）] カードまでスクロールします（変換のために検出されたユーザがいる場合は、[ユーザ（Users）] カードまでスクロールします。このラボではユーザを変換する必要はありません）。
3. [シングルサインオン（Single Sign-On）] の横にある**歯車アイコン** [⚙] をクリックします。
4. [サードパーティのIDプロバイダーを統合する（アドバンスド）（Integrate a 3rd-party identity provider (Advanced)）] オプションボタンをオンにして、[次へ（Next）] をクリックします。
5. [メタデータファイルのダウンロード（Download Metadata File）] ボタンをクリックすると、**idb-meta-<org-ID>-SP.xml** という形式の XML ファイルがダウンロードされ、デスクトップに保存されます。
6. [ディレクトリメタデータのエクスポート（Export Directory Metadata）] 画面を閉じます。
7. Control Hub からロックアウトされないようにするために、O365 管理者に Control Hub の**管理者権限**を設定します。
8. [ユーザ（Users）] に移動し、先ほど作成した O365 管理者を選択します。
9. 下にスクロールして [管理者権限（Administrator Roles）] を選択します。
10. [フル管理者権限（Full administrator privileges）] オプションボタンを選択し、[保存（Save）] をクリックします。

Azure のアプリケーション設定でシングルサインオンを設定する

Azure を利用した SSO の設定に関する詳細については、Cisco Webex Control Hub と Microsoft Azure のシングルサインオン統合を参照してください。次の点に注意してください。

SSO および Cisco Webex Control Hub に関して、IdP は SAML 2.0 仕様に準拠している必要があります。さらに、IdP は、次の方法で設定する必要があります。

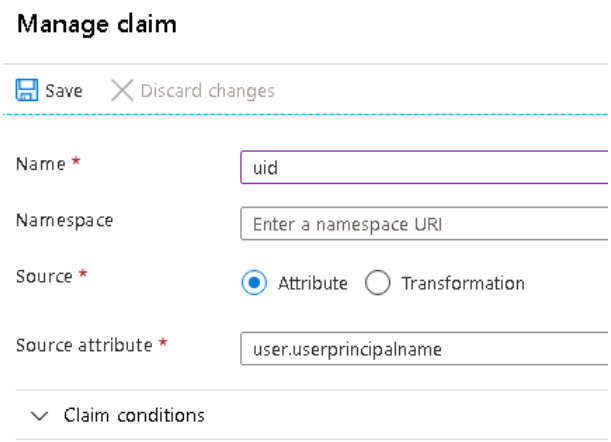
- NameID Format 属性を urn:oasis:names:tc:SAML:2.0:nameid-format:transient に設定する。
- IdP で、Cisco Directory Connector で選択されている属性と一致する値が設定された uid 属性名を含めるか、Cisco Webex ID サービスで選択されている属性と一致するユーザ属性を含むように、要求を設定します（たとえば、E-mail-Addresses や User-Principal-Name などの属性を指定できます）。詳細については、https://www.cisco.com/go/hybrid-services-directory のカスタム属性情報を参照してください。
- サポートされているブラウザを使用します。Mozilla Firefox または Google Chrome の最新バージョンをお勧めします。
- ブラウザのポップアップブロッカーを無効にします。
- Azure Active Directory では、プロビジョニングは手動モードでのみサポートされます。このガイドでは、シングルサインオン（SSO）統合についてのみ説明します。

1. Azure ポータル（https://portal.azure.com）に戻り、O365 管理者でサインインします。
2. 上部の検索ボックスで、**エンタープライズ アプリケーション**を検索し、リストから選択します。
3. ラボですでに Azure のユーザ同期を設定している場合は、アプリケーションの一覧から **Cisco Webex** を選択します。ユーザ同期に使用するのと同じアプリケーションを使用します。まだユーザ同期を設定していない場合は、次の手順に従います。
    a. [新規アプリケーション（New Application）] をクリックします。
    b. [ギャラリーから追加（Add from the gallery）] セクションで、「**Cisco Webex**」を検索します。
    c. 検索結果の [Cisco Webex] を選択し、[追加（Add）] をクリックします。
4. [シングルサインオン（Single sign-on）] タブに移動し、[SAML] を選択します。その他の設定オプションも含め、ページが更新されます。
5. [メタデータファイルのアップロード（Upload metadata file）] をクリックします。
6. ファイルを開くアイコン [] を利用して先にダウンロードしたメタデータ XML ファイルを選択し、[追加（Add）] をクリックします。
7. 表示されたポップアップウィンドウで [応答URL（Reply URL）] ボックスにリストされている完全な URL をコピーし、[サインオンURL（Sign on URL）] ボックスに貼り付けます。

サインオン URL

8. [保存（Save）] をクリックして、ポップアップウィンドウを閉じます。
9. [ユーザ属性と要求（User Attributes & Claims）] の編集アイコン [✎] をクリックします。
10. [必須要求（Required claim）] セクションに **uid** がすでに登録されている場合は、以下の注に進んでください。
11. [新規要求の追加（Add new claim）] をクリックします。
12. 次のように設定します。
    a. [名前（Name）] : **uid**
    b. [ソース（Source）] : [属性（Attribute）]（デフォルト）
    c. [ソース属性（Source attribute）] : **user.userprincipalname**

要求の設定



13. [保存（Save）] をクリックします。

注：Cisco Webex は、通常はユーザの電子メールアドレスに一致する uid 属性があることを想定しています（Azure では通常、userprincipalname にマッピングされます）。その属性は、Webex Control Hub でユーザを作成するために使用される属性と一致する必要があります。

[ユーザ属性と要求（Users Attributes & Claims）] ページに表示されている、この手順で設定した属性以外の属性は、この統合には関係ありません。削除しても、そのままでも構いません。

14. × をクリックして [ユーザ属性および要求（User Attributes & Claims）] ページを閉じます。
15. 左側の [ユーザおよびグループ（Users and Groups）] タブに移動します。
16. すでにユーザ同期タスクを実施している場合は、このアプリケーションにユーザが割り当てられています。割り当てられているユーザはリストに表示されます。ユーザ同期タスクを実施していない場合は、[ユーザの追加（Add user）] をクリックし、アプリケーションに O365 ユーザを追加します。
17. [シングルサインオン（Single sign-on）] ページに戻ります。
18. [SAML 署名証明書（SAML Signing Certificate）] セクションで、[フェデレーションメタデータXML（Federation Metadata XML）] の横にある [ダウンロード（Download）] リンクをクリックし、自分のコンピュータに保存します。

IdP メタデータをインポートし、テスト後にシングルサインオンを有効にする

Azure を設定できたので、Azure ポータルからダウンロードしたメタデータファイルを Control Hub にアップロードする必要があります。

1. Control Hub に戻ります。
2. [設定（Settings）] をクリックし、[認証（Authentication）] セクションまでスクロールします。
3. [シングルサインオン（Single Sign-On）] の [変更（Modify）] をクリックします。
4. [サードパーティのIDプロバイダーを統合する（アドバンスド）（Integrate a 3rd-party identity provider(Advanced)）] オプションボタンをオンにして、[次へ（Next）] をクリックします。
5. Control Hub のメタデータファイルをすでにダウンロードしているので、[次へ（Next）] をクリックします。
6. [ファイル参照（file browser）] リンクをクリックし、Azure ポータルからダウンロードした **Cisco Webex.xml** ファイルを開きます。
7. アップロードが成功したら、[次へ（Next）] をクリックします。
8. [SSO接続のテスト（Test SSO Connection）] をクリックします。
9. 新しいタブが開き、Azure ポータルにログインしているのと同じブラウザを使用している場合は、**シングルサインオンが成功**したことを示すメッセージが表示されます。ログインページが表示されたら、O365 ユーザのいずれかでログインします。

10. SSO テスト用に開いたブラウザタブを閉じます。
11. ページを下にスクロールし、テストが成功したことを確認するためのオプションボタンを選択します。シングルサインオンを有効にし（テストが成功した場合）、[保存（Save）] をクリックします。
12. いずれかの Webex Teams クライアントを使用して、任意の O365 ユーザでサインインし、新しい SSO 認証フローを確認します。

これで、O365 ユーザが Azure SSO を使用して Webex にログインできるようになりました。

オンプレミスの Active Directory サーバにユーザを設定したことに注意してください。これらのユーザは O365 組織には存在しないため、今後ログインできません。再度ログインできるようにするには、SSO を無効にする必要があります。

13. 一旦別のページに移動してから戻って [設定（Settings）] ページを更新し、SSO のステータスが変わっていることを確認する必要があります。SSO が ● Enabled と表示されていない場合はここで確認します。
14. SSO が [有効（Enabled）] と表示されていたら、[変更（Modify）] をクリックします。
15. [組み込みのIDサービスをユーザ認証に使用する（シンプル）（Use the built-in identity service for user authentication (Simple)）] のオプションボタンを選択します。
16. **SSO の警告**ポップアップが表示されたら、[OK] をクリックします。
17. 画面の右下に成功メッセージが表示されます。**X** をクリックして [エンタープライズ設定（Enterprise Settings）] ウィンドウを閉じます。

Cisco Webex 用の AD FS 設定

このセクションでは、Cisco Webex との SSO をサポートするために、セッションの AD サーバにインストールされている AD FS を設定します。このタスクでは自己署名証明書を使用しますが、公的に信頼された署名証明書を使用することを強く推奨します。まもなくわかるように、各デバイスで Cisco Webex を使用するには、AD サーバのルート CA 証明書をインストールする必要があります。公的に信頼された CA を使用して証明書に署名した場合は、すべてのデバイスに手動でルート CA 証明書をインストールする必要はありません。証明書のコモンネーム（CN）は、AD FS の URL に一致している必要があります。

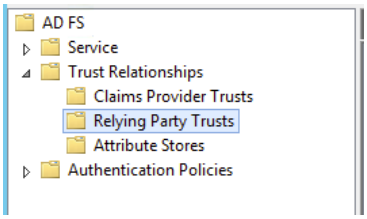
Azure を使用して SSO を設定している場合は、設定を無効にしていることを確認する必要があります。Control Hub で設定できる SSO プロバイダーは 1 つのみです。

注：トポロジでは AD FS プロキシサーバを使用していません。そのため、Webex は AD FS サーバに直接接続されています。この場合、インターネットから内部サーバにアクセスできるため、セキュリティ上の大きなリスクになります。実稼働環境では、ベストプラクティスとして採用すべきではありません。SSO がすでに稼働していて、ユーザが外部から内部リソースにアクセスしている場合は、プロキシサーバを設置します。ただしこのラボでは、AD FS 自体を設定する方法よりも、AD FS で Webex SSO を設定する方法に重点を置いています。ラボでプロキシサーバを使用する場合でも設定は同じであり、このシナリオで示すように、Webex に接続するすべての設定が AD FS サーバで設定されます。

Cisco Webex 用の AD FS 設定

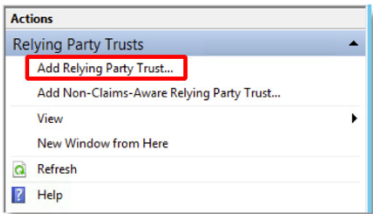
1. AD FS（AD1）サーバ（**198.18.133.1**）に対するリモートデスクトップ接続を確立し、**dcloud\administrator/dCloud123!** でログインします。証明書の警告が表示されたら、[はい（Yes）]/[同意（Accept）]/[続行（Continue）] の順にクリックします。
2. Chrome を開きます。ホームページから、[Cisco Webexリンク（Cisco Webex Links）] > [Cisco Webex Control Hub] に移動します。
3. Charles （**cholland@cbXXX.dc-YY**.com/**dCloud123!**）でサインインします。
4. Azure で使用するためにこのシナリオで以前ダウンロードしたメタデータファイルを、AD サーバにコピーする必要があります。ファイルをダウンロードしていない場合、またはもう一度ダウンロードしたい場合は、次の手順に従います。
    a. [概要（Overview）] ページで、ページ下部の [ライセンス（Licenses）] カードまでスクロールします（変換のために検出されたユーザがいる場合は、[ユーザ（Users）] カードまでスクロールします。このラボではユーザを変換する必要はありません）。
    b. [シングルサインオン（Single Sign-On）] の横にある**歯車アイコン** [] をクリックします。
    c. [サードパーティのIDプロバイダーを統合する（アドバンスド） (Integrate a 3rd-party identity provider (Advanced))] オプションボタンをオンにして、[次へ（Next）] をクリックします。
    d. [メタデータファイルのダウンロード（Download Metadata File）] ボタンをクリックすると、**idb-meta-<org-ID>-SP.xml** という形式の XML ファイルがダウンロードされ、デスクトップに保存されます。
    e. [ディレクトリメタデータのエクスポート（Export Directory Metadata）] 画面は開いたままにします。
5. タスクバーのアイコン [] をクリックして、**AD FS Management** を開きます。
6. [信頼関係（Trust Relationships）] を展開し、[証明書利用者信頼（Relying Party Trusts）] フォルダをクリックします。

証明書利用者信頼



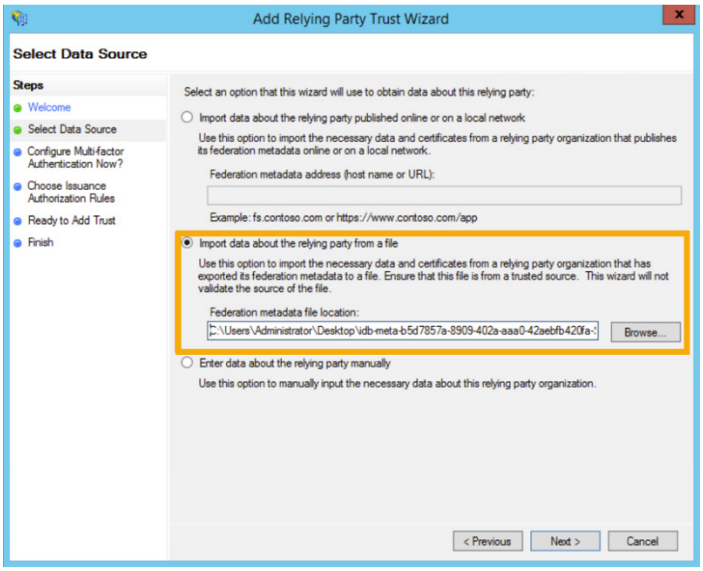
7. [アクション（Actions）] で、[証明書利用者信頼の追加...（Add Relying Party Trust...）] をクリックします。

証明書利用者信頼の追加



8. [開始（Start）] をクリックして信頼ウィザードを開始します。
9. [証明書利用者に関するデータをファイルからインポートする（Import data about the relying party from a file）] オプションボタンをクリックします。
10. [参照（Browse）] をクリックします。Cisco Webex からデスクトップにダウンロードした **idb-meta....xml** メタデータファイルをクリックし、[開く（Open）] をクリックします。

メタデータファイルの選択



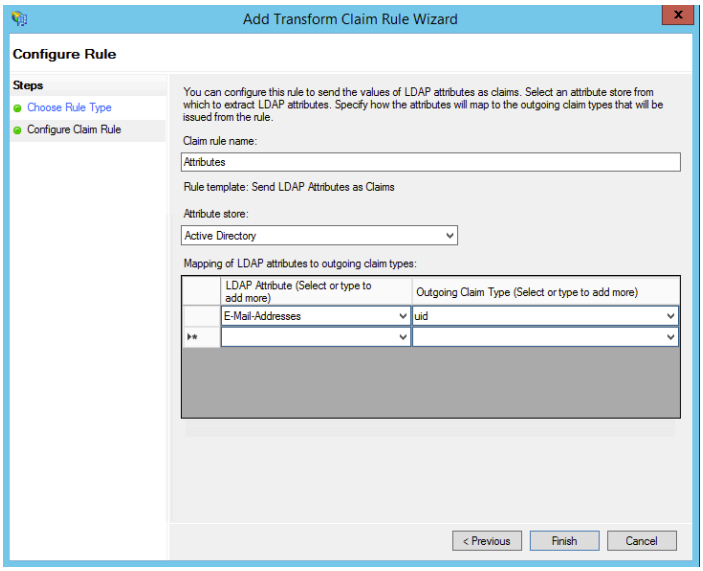
11. [次へ（Next）] をクリックします。
12. [表示名（Display name）] に **Cisco Webex** と入力し、[次へ（Next）] をクリックします。
13. [現時点ではこの証明書利用者信頼に多要素認証を設定しない（I do not want to configure multi-factor authentication settings for this relying party trust at this time）] を選択したまま、[次へ（Next）] をクリックします。
14. [すべてのユーザにこの証明書利用者へのアクセスを許可する（Permit all user to access this relying party）] を選択したまま、[次へ（Next）] をクリックします。
15. [信頼を追加可能（Ready to Add Trust）] 画面で [次へ（Next）] をクリックします。
16. チェックボックスをオンにしたまま [閉じる（Close）] をクリックします。

AD FS 要求ルールを作成して Cisco Webex からの認証を可能にする

最初に、ユーザを識別するために Cisco Webex にマッピングするフィールドを AD FS に示すルールを作成します。

1. [Cisco Webexに関する要求ルールの編集（Edit Claim Rules for Cisco Webex）] ウィンドウで、[ルールの追加...（Add Rule...）] をクリックします。
2. [LDAP属性を要求として送信（Send LDAP Attributes as Claims）] を選択したまま、[次へ（Next）] をクリックします。
3. [要求ルール名（Claim Rule Name）] に **Attributes** と入力します。
4. [属性ストア（Attribute store）] で [Active Directory] をクリックします。
5. 次に示すように、**E-Mail-Addresses** LDAP 属性を **uid** 送信要求タイプにマッピングします。**uid** のタイプはドロップダウンメニューにはないため、手動で入力します。

属性要求ルール



6. [完了（Finish）] をクリックします。
7. [ルールの追加...（Add Rule...）] を再度クリックします。

次のルールでは、Cisco Webex から他の方法では提供されない **spname qualifier** 属性を AD FS に提供します。

8. [要求ルールテンプレート（Claim rule template）] ドロップダウンメニューから [カスタムルールを使用して要求を送信（Send Claims Using a Custom Rule）] を選択し、[次へ（Next）] をクリックします。
9. [要求ルール名（Claim rule name）] ボックスに **custom** と入力します。

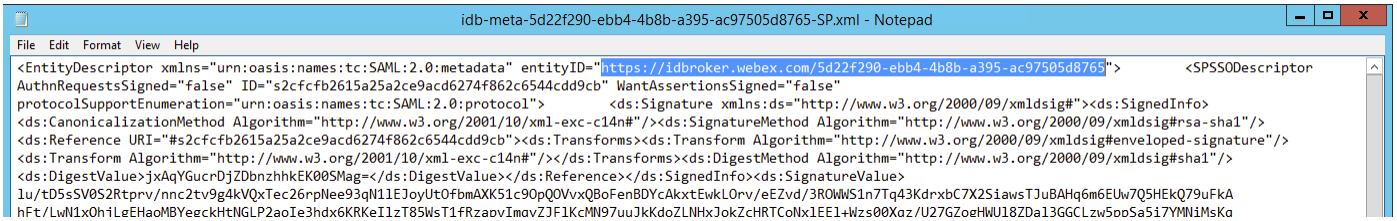
10. デスクトップで **Custom rule.txt** ファイルを開き、ファイル内のテキストをすべてコピーして、[カスタムルール：（Custom rule:）] ボックスに貼り付けます。貼り付けたテキストは、組織に応じて以下のように変更する必要があります。

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"] => issue(Type =
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Issuer = c.Issuer, OriginalIssuer =
c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =
"urn:oasis:names:tc:SAML:2.0:nameid-format:transient",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequalifier"] =
"https://adfs.cbXXX.dc-YY.com/adfs/services/trust",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] =
"https://idbroker.webex.com/35a15b0a-0eg1-4029-9f63-a8c54df5df59");
```

- **cbXXX.dc-YY.com** を、セッションに割り当てられているドメインと置き換えます。
- 最後の URL は、先にダウンロードした Cisco Webex メタデータファイル内の URL に一致するように変更します。ワードパッドまたはメモ帳でその XML ファイルを開き、次のように **EntityDescriptor entityID** タグの先頭に記載されている URL をコピーします。この URL は組織ごとに異なるため、以下のスクリーンショットと同じではありません。

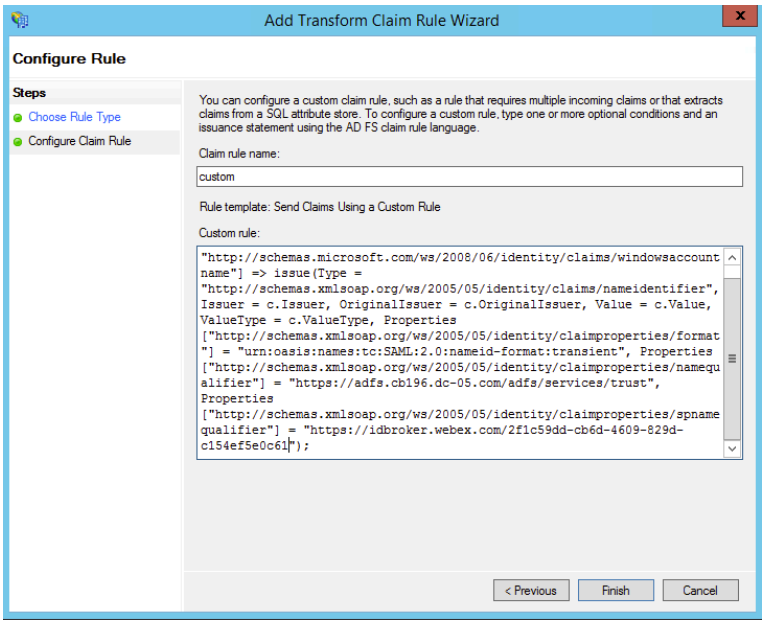
注：XML をメモ帳またはワードパッドで開くと、簡単に URL をコピーできます。

メタデータ XML ファイルの Idbroker URL



10. 作成されたルールは次の図のようになります。

カスタム要求ルール



11. [完了（Finish）] をクリック後、 [OK] をクリックします。

Cisco Webex を設定し、AD FS を SSO ID サービスプロバイダー（IdP）として使用する

次に、AD FS からメタデータをダウンロードして Cisco Webex にアップロードします。

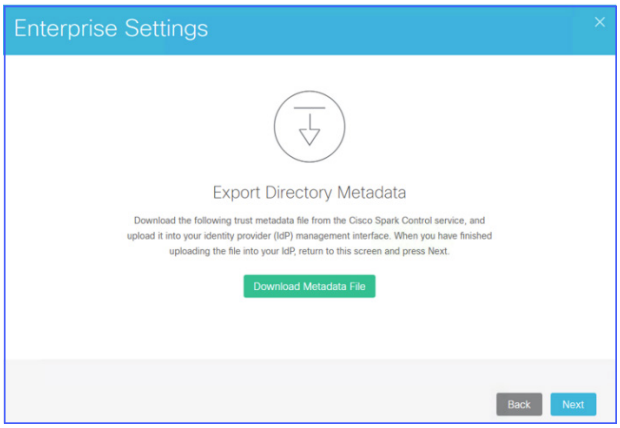
1. AD1 サーバで Chrome を再度開き、新しいタブを開きます。
2. **https://adfs.cbXXX.dc-YY.com/FederationMetadata/2007-06/FederationMetadata.xml** にアクセスします。このセッションに指定されたドメインに一致するように、cbXXX.dc-YY.com の部分を変更する必要があります。
3. 上記アドレスにアクセスしたら、[アドバンスド（Advanced）] をクリック後、[続行（Proceed）] をクリックします。**FederationMetadata.xml** ファイルがデスクトップに自動的にダウンロードされます。
4. デスクトップに移動し、**FederationMetadata.xml** ファイルがあることを確認します。

FederationMetadata.xml ファイルを Webex にアップロードする

次に、AD FS の設定時に作成した FederationMetadata.xml ファイルをアップロードします。

1. Cisco Webex Control Hub 用に開いていた Chrome のタブに戻ります。まだ [ディレクトリメタデータのエクスポート（Export Directory Metadata）] 画面が開いているはずです。

ディレクトリメタデータのエクスポート画面



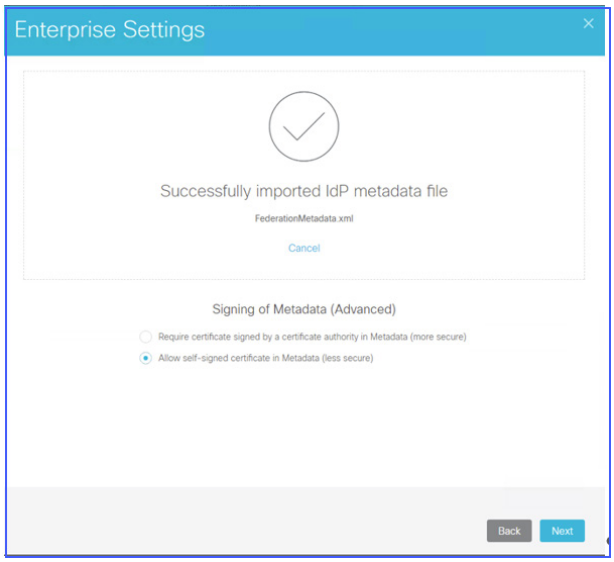
2. [次へ（Next）] をクリックします。
3. 自己署名証明書を使用しているため、[メタデータで自己署名証明書を有効にする（低セキュリティ）（Allow self-signed certificate in Metadata (less secure)）] オプションボタンをオンにします。

注：オプションを表示するには、スクロールが必要な場合があります。これはデフォルトのオプションではないため、ラボで SSO を使用する場合は、必ず選択する必要があります。このオプションが選択されていない場合、FederationMetadata.xml ファイルを正しくアップロードすることもできなくなります。

4. [ファイル参照（file browser）] リンクをクリックします。
5. [開く（Open）] ウィンドウで、デスクトップの **FederationMetadata.xml** ファイルを選択し、[開く（Open）] をクリックします。

[IdPメタデータファイルが正常にインポートされました（Successfully imported IdP metadata file）] メッセージが表示されます。

インポートの成功



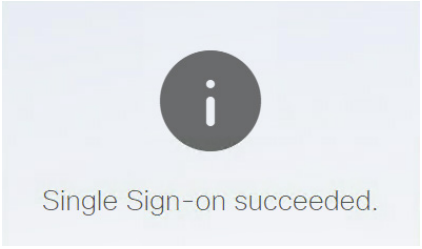
6. [次へ（Next）] をクリックします。
7. [SSO接続のテスト（Test SSO Connection）] をクリックします。

ブラウザで SSO をテストするための新しいタブが開きます。

8. **cholland/dCloud123!** でサインインします。パスワードの途中の「i」に見える文字は数字の 1 であり、感嘆符（!）ではないことに注意してください。

サインインに成功すると、[シングルサインオンに成功（Single Sign-on succeeded）] というメッセージが表示されます。失敗した場合は、以下の失敗した場合の手順を実行してください。

SSO 成功



9. ブラウザタブを閉じます。
10. テストに成功したら、[SSO設定のテスト（Test SSO Setup）] 画面で、[テストに成功しました。シングルサインオンを有効にしてください（The test was successful. Enable Single Sign On）]オプションボタンをオンにして、[保存（Save）] をクリックします。失敗した場合は、2 番目のオプションボタンをクリックし、元に戻って設定を確認し、再度やり直してください。ログイン情報を間違って入力した場合は、ブラウザを閉じてキャッシュされているログイン情報をクリアする必要があります。

組織で SSO が有効になりました。

11. AD1 への **RDP 接続**を閉じます。

重要：基本的な認証機能を使用して Charles として管理ポータルにログインしているブラウザがある場合は、この後のラボで問題が発生しないようにここでログアウトし、SSO ログイン情報を使用してログインし直します。

注：カスタマー組織で SSO が失敗した場合でも、パートナー管理者はパートナーポータルにログインして、カスタマー組織にアクセスできます。ラボでパートナー管理者アカウントへのアクセス権がなく、SSO の無効化が必要な場合は、C:\dcloud フォルダに移動して disable_sso.ps1 ファイルを右クリックし、[PowerShellで実行（Run with PowerShell）] を選択します。スクリプトが完了すると、SSO は該当の組織で無効になります。

ラボでは、Cisco Webex からサインアウトするたびにエラーが表示されます。これは、AD FS で Single Logout Service が設定されていないにもかかわらず、AD FS からダウンロードしたデフォルトのメタデータファイルで設定されているからです。ログアウト時にエラーにならないようにするには、Single Logout を設定するか、FederationMetadata.xml ファイルから次に示す箇所を削除して Webex に再度アップロードします。AD FS Single Logout Service についてはこのラボでは扱いません。

```
<?xml version="1.0"?>
- <EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" entityID="https://adfs.cb196.dc-05.com/adfs/services/trust" ID="_341da458-68d0-4443-a11c-11d59aa39bd2">
  - <IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    + <KeyDescriptor use="encryption">
    + <KeyDescriptor use="signing">
      <SingleLogoutService Location="https://adfs.cb196.dc-05.com/adfs/ls/"
          Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"/>
      <SingleLogoutService Location="https://adfs.cb196.dc-05.com/adfs/ls/"
          Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"/>
      <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</NameIDFormat>
```

Workstation 1 で SSO をテストする

次に、Cisco Webex Teams 用に有効にしたアカウントで SSO を使用したログインをテストします。まず Workstation 1 からテストします。

1. Workstation 1（**198.18.1.36**）にまだ接続していない場合は RDP 接続を確立し、ユーザ名：**dcloud\cholland**、パスワード：**dCloud123!** でログインします。
2. デスクトップ上のアイコンを使用して、**Cisco Webex Teams** を開きます。
3. 利用規約に同意し、Charles の電子メール アドレス（**cholland@cbXXX.dc-YY.com**）を入力して、[次へ（Next）] をクリックします。
4. AD FS シングルサインオンページが表示されます。
5. ユーザ名：**cholland**、パスワード：**dCloud123!**（このラボの全ユーザの Active Directory パスワード）を入力します。

6. [サインイン（Sign In）] をクリックします。

Cisco Webex Teams アプリケーションが SSO を使用してログインできるようになっています。

注：通常このラボでサインインに失敗したメッセージが表示された場合は、複数のユーザアカウントを使用してログインしていることが原因です。ブラウザのキャッシュをクリアしてください。ブラウザを完全に閉じればキャッシュを簡単にクリアできます。ユーザごとに別のブラウザを使用することも有効です。

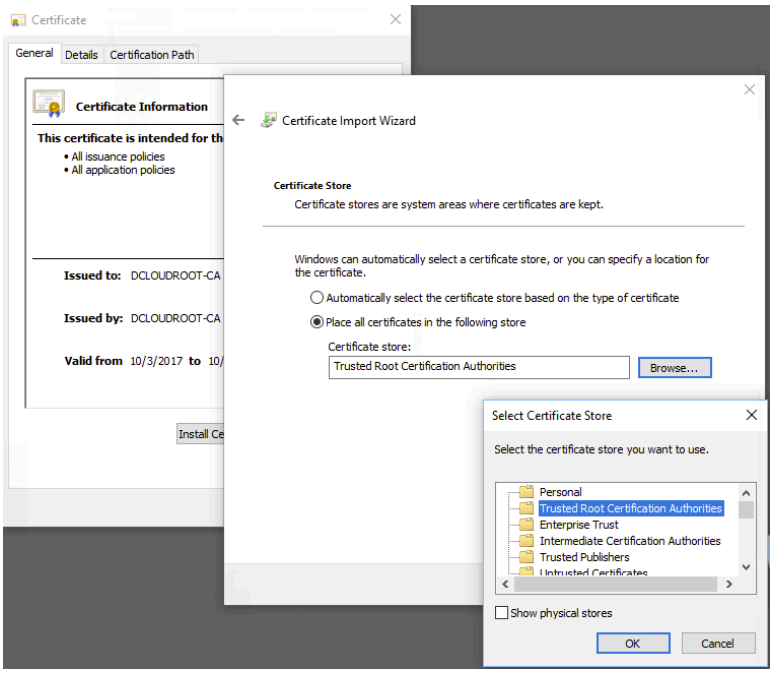
AD CA ルート証明書のインストール

ここでは、AD サーバ用の CA 証明書を自分のラップトップやモバイルデバイスにインストールする方法を示します。先に Workstation 1 で SSO をテストした理由は、Workstation 2 と同様に、すでに CA 証明書がインストールされているためです。このラボでは自己署名証明書を使用しているため、この CA 証明書を自分のコンピュータだけでなくモバイルデバイスにもインストールする必要があります。インストールしない場合は、ユーザの電子メールアドレスを送信した後、Webex Teams アプリに空白の画面が表示されます。

CA 証明書をダウンロードするには、ブラウザを開き、https://dccacert.s3.us-east-2.amazonaws.com/dcloud-AD1-CA.cer にアクセスします。**dcloud-AD1-CA.cer** ファイルがダウンロードされます。

1. デバイスでこの証明書を開いてインストールします。基本的な手順を以下に示します。
    - Mac の場合は、証明書を開いて**ログイン**キーチェーンに**追加**します。
        - 証明書を追加したら、[キーチェーンアクセス（Keychain Access）] ウィンドウ（ウィンドウが開いていない場合は Keychain Access アプリケーションを開く）で **dcloud-ad1-ca** を検索し、証明書を開いてプロパティを表示します。
        - 証明書が開いたら [信頼（Trust）] を展開し、[この証明書を使用している場合（When using this certificate）] ドロップダウン リスト ボックスを [常に信頼（Always Trust）] に変更します。証明書とキーチェーン アクセス ウィンドウを閉じます。

dCloud ルート証明書をインストール



- iOS の場合は、証明書を電子メールで自分に送信し、デバイス上で開いて、画面に従ってインストールします。[設定（Settings）] > [一般（General）] > [詳細（About）] > [証明書の信頼設定（Certificate Trust Settings）] に移動して、インストールした **dcloud-AD1-CA** 証明書を信頼します。
- Android の場合は、**.cer** 拡張子を **.crt** に変更します。証明書を電子メールで自分に送信してデバイス上で開き、画面に従ってインストールします。
- Firefox のような特定の Web ブラウザでは、ブラウザ自体に証明書をインポートしなければならない場合があります。

自分のブラウザで SSO をテストする

このセクションでは、Anita で SSO をテストします。最初に、Anita が Cisco Webex から電子メールを受信しているかどうかを確認します。

1. 自分のコンピュータで別の Web ブラウザを開き、別のユーザで Webex Teams にログインしている場合はブラウザのキャッシュをクリアします。使用中のブラウザでプライベート/匿名モードを使用することもできます。
2. https://teams.webex.com に移動します。
3. 電子メール アドレス（**aperez@cbXXX.dc-YY.com**）を入力し、[続行（Continue）] をクリックします。
4. Cisco dCloud SSO ページに移動します。証明書の警告が表示されたら、同意して続行します（ラボでは自己署名証明書を使用していることに注意してください）。

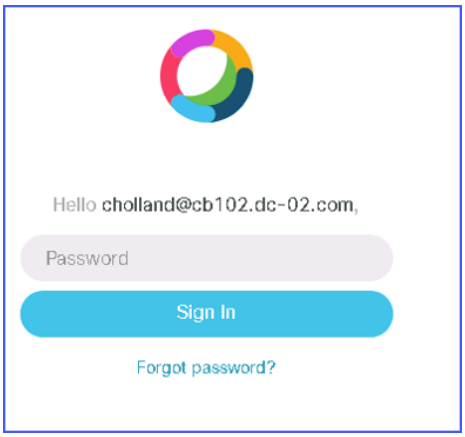
5. **aperez/dCloud123!** でサインインします。
6. これで Webex Teams にログインできます。組織内の任意のユーザで、Web、モバイル、デスクトップなどからログインしてみてください。ユーザのパスワードはすべて **dCloud123!** です。

付録 A.　Cisco Webex パスワードのリセット手順

場合によっては、Cisco Webex ユーザアカウントのパスワードをリセットする必要があります。次に、Charles Holland のパスワードをリセットする手順を示します。

1. Chrome Web ブラウザを開いて https://admin.webex.com にアクセスし、電子メールアドレス（**cholland@cbXXX.dc-YY.com**）を入力します。
2. [次へ（Next）] をクリックします。
3. 次のページで、ドメインの XXX と YY の部分を除き、下の図のようになっていることを確認します。同様であれば、次の手順に進みます。

正しいサインイン画面



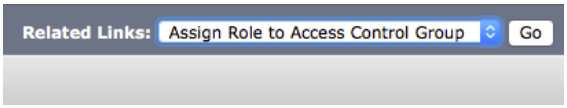
4. 画面が上のようなサインインのイメージであれば、下部の [パスワードを忘れた場合（Forgot password?）] リンクをクリックします。
5. リセット方法を示した電子メールが Charles に送信されています。リモートデスクトップを使用して Workstation 1（**198.18.1.36**）に接続し、ユーザ名：**dcloud\cholland**、パスワード：**dCloud123!** でログインします。Outlook をまだ開いてない場合は開きます（https://mail1.dcloud.cisco.com/owa に移動し、**dcloud\{ユーザ名}**、パスワード **dCloud123!** でサインインすることで、OWA を使用してすべてのユーザの電子メールアカウントにアクセスすることもできます）。
6. 受信トレイに、「**パスワードのリセット（Password Reset）**」という件名の電子メールがあります。そのメール内で、[パスワードのリセット（Reset password）] をクリックします。
7. ブラウザのウィンドウが表示されます。[新しいパスワード（New Password）] ボックスと [新しいパスワードの確認（Confirm new password）] ボックスに「**dCloud123!**」と入力します。
8. [保存してサインイン（Save & Sign In）] をクリックします。
9. ブラウザを閉じて、ラボを続けます。

付録 B.　アプリケーションユーザの作成と確認

以下の手順では、Expressway の Cisco Webex コールコネクタで使用するアプリケーションユーザの作成方法を示します。

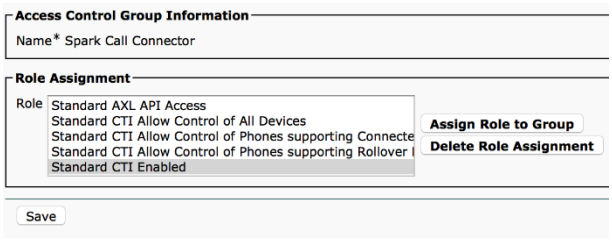
1. https://198.18.133.3/ccmadmin にアクセスします。
2. ユーザ名：administrator、パスワード：dCloud123! でログインします。
3. [ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [アクセスコントロールグループ（Access Control Group）] に移動し、[新規追加（Add New）] をクリックします。
4. 名前に **Webex Call Connector** と入力し、[保存（Save）] をクリックします。
5. [関連リンク（Related Links）] ドロップダウンメニューで [アクセスコントロールグループに権限を割り当て（Assign Role to Access Control Group）] を選択し、[実行（Go）] をクリックします。

[アクセスコントロールグループに権限を割り当て（Assign Role to Access Control Group）]



6. [グループに権限を割り当て（Assign Role to Group）] をクリックし、[検索（Find）] をクリックします。
7. 次のチェックボックスをオンにします。
   - [標準AXL APIによるアクセス（Standard AXL API Access）]
   - [標準CTIによるすべてのデバイスの制御許可（Standard CTI Allow Control of All Devices）]
   - [標準CTIによるConnected Xferおよび設定をサポートする電話の制御許可（Standard CTI Allow Control of Phones supporting Connected Xfer and conf）]
   - [標準CTIによるロールオーバーモードをサポートする電話の制御許可（Standard CTI Allow Control of Phones supporting Rollover Mode）]
   - [標準CTIを有効にする（Standard CTI Enabled）]
8. これらのボックスをオンにしたら、[選択項目の追加（Add Selected）] をクリック後、[保存（Save）] をクリックします。

権限の割り当て



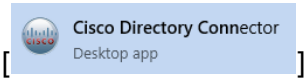
9. [ユーザ管理（User Management）> [アプリケーションユーザ（Application User）] に移動し、[新規追加（Add New）] をクリックします。
10. [ユーザID（User ID）] に **webex** と入力します。
11. [パスワード（Password）] および [パスワードの確認（Confirm Password）] フィールドに **dCloud123!** と入力します。
12. ページの下部にスクロールし、[アクセス制御グループへ追加（Add to Access Control Group）] をクリックします。次に [検索（Find）] をクリックします。
13. [Webexコールコネクタ（Webex Call Connector）] の横にあるチェックボックスをオンにして、[選択項目の追加（Add Selected）] をクリックします。
14. [保存（Save）] をクリックします。

付録 C.　Directory Connectorの設定

Cisco Directory Connectorは、ID を同期するためのオンプレミス アプリケーションです。Active Directory とバックエンドのシスコ ID ストアを同期し、ユーザが Cisco Webex Meetings や Cisco Webex Teams などのシスコ サービスをシームレスに使用できるようにするために不可欠なツールです。

このラボでは、ドメインから Cisco Webex にユーザをインポートするための Active Directory サーバがあります。Directory Connectorは、Workstation 1 にインストールされています。Windows ドメインの信頼されたメンバーであればどこにでもインストールできます。ラボの時間を短縮するために、Directory Connectorは事前にインストールされています。インストールファイルは、顧客管理ポータルの [ユーザ（Users）] > [ユーザの管理（Manage Users）] > [ディレクトリ同期化をオンにする（Turn on Directory Synchronization）] 画面からダウンロードできます。

注：Directory Connectorの詳細を確認するには、**導入ガイド**をダウンロードしてください。

1. Chrome と Outlook を最小化します。タスクバーまたはタスクバーの検索ボックスの**検索**アイコン [] をクリックし、**Cisco Directory Connector** を検索します。見つかったらアプリケーションアイコン [

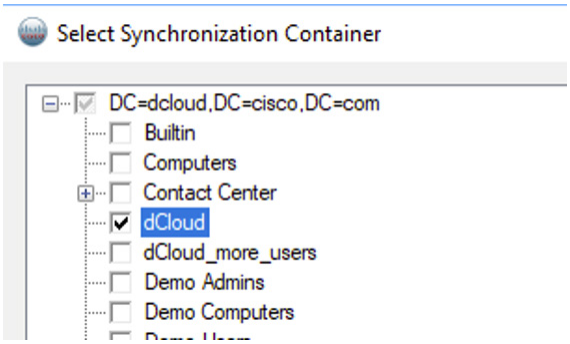
] をクリックします。
2. [Webexにサインイン（Webex sign in）] 画面で、**cholland@cbXXX.dc-YY.com** と入力し、[次へ（Next）] をクリックします。
3. 次のボックスにパスワード **dCloud123!** を入力し、[サインイン（Sign In）] をクリックします。
4. [AD DS] のオプションボタンを選択したまま、[ドメインのロード（Load Domains）] をクリックします。
5. ドロップダウンリストで [dcloud.cisco.com] を選択し、[確定（Confirm）] をクリックします。
6. [自動的にアップグレード（automatically upgrade）] ポップアップウィンドウで [はい（Yes）] をクリックします。
7. ディレクトリコネクタが開いたら、画像（アバター）と合わせて、ユーザが同期されるように設定します。
8. [後で行う（Not Now）] をクリックして、リハーサルは後で実施することにします。
9. 上部にある [設定（Configuration）] タブをクリックします。
10. [オブジェクトの選択（Object Selection）] タブをクリックすると、同期するユーザを指定できます。

[オブジェクトの選択（Object Selection）] ページでは、同期するユーザを選択できます。ディレクトリコネクタは、デフォルトではドメインの全ユーザとグループを同期します。このラボでは、特定の組織単位（OU）内のユーザのみを同期します。

11. [グループ（Groups）] チェックボックスをオフにします。
12. [同期するオンプレミスベースのDN（On Premises Base DNs to Synchronize）] セクションにある [選択（Select）] ボタンをクリックします。
13. 一番上の [DC=dcloud,DC=cisco,DC=com] チェックボックスをオフにして、すべてのチェックボックスの選択を解除します。

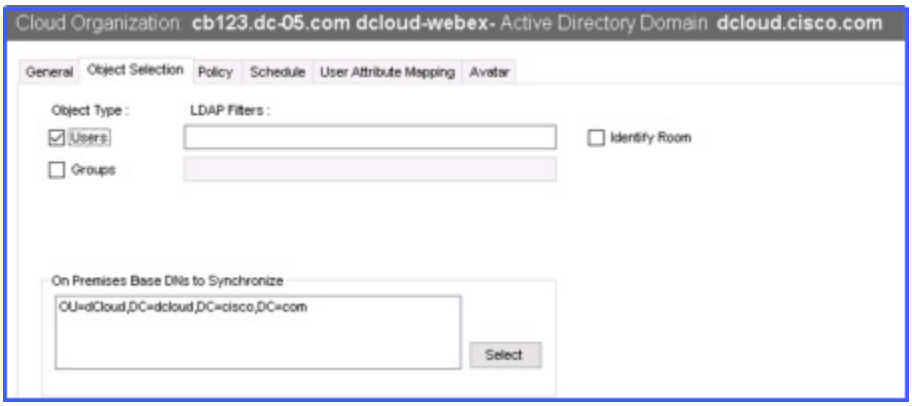
14. [dCloud] チェックボックスをオンにして、[選択（Select）] をクリックします（選択するのは **dCloud** コンテナのみです）。

OU の選択



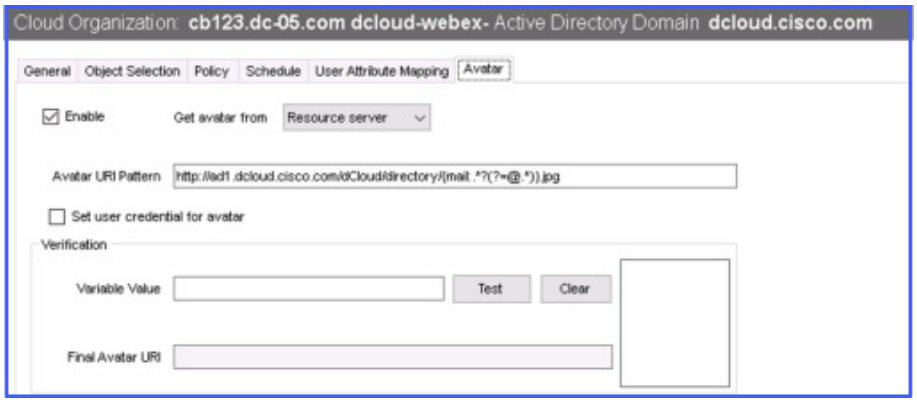
15. クラウド組織名を除き、[オブジェクトの選択（Object Selection）] ページは下のスクリーンショットのようになります。

[オブジェクトの選択（Object Selection）] タブ



16. [アバター（Avatar）] タブをクリックして、[有効（Enabled）] チェックボックスをオンにします。

アバターの有効化



17. [アバターのURIパターン（Avatar URI Pattern）] ボックスに次の URI を入力します。

http://ad1.dcloud.cisco.com/dCloud/directory/{mail: .*?(?=@.*)}.jpg

注：デスクトップに Pattern.txt というテキストファイルがあり、そこからパターンをコピーできます。

18. 画面の最下部にある [適用（Apply）] をクリックします。

19. ポップアップ画面で、[設定変更の適用（Apply Config Changes）] をクリックします。

同期のリハーサルを実施し、適切なユーザが同期されることを確認します。

20. 上部にある [ダッシュボード（Dashboard）] タブをクリックします。

21. [同期のリハーサル（Sync Dry Run）] アイコン [Sync Dry Run] をクリックし、[OK] をクリックします。

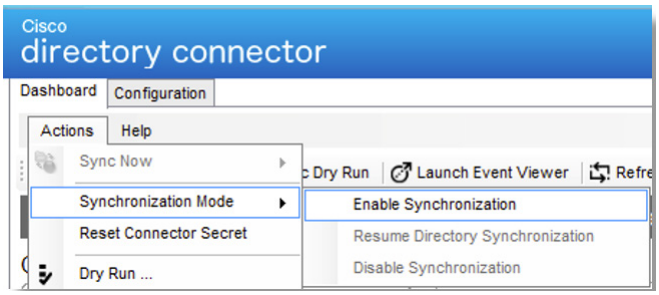
組織に追加される 7 人のユーザ [7 Objects Added] が表示されます。また、一致する 1 つのオブジェクトが Charles Holland のアカウントであることがわかります。このオブジェクトが表示されない場合は、設定をもう一度確認します。

22. [完了（Done）] をクリックします。

次に同期を有効にします。

23. [アクション（Actions）] メニューをクリックし、[同期モード（Synchronization Mode）] > [同期の有効化（Enable Synchronization）] の順に選択します。

同期の有効化



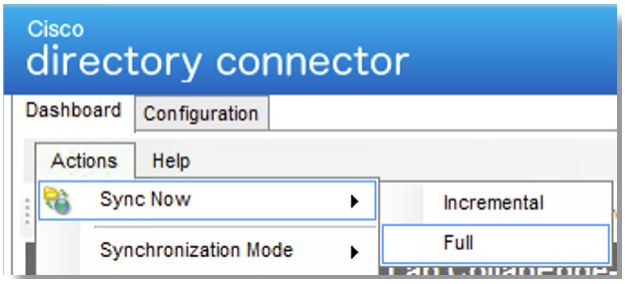
24. すでにリハーサルを実施しているため、ポップアップで [いいえ（No）] をクリックします。

25. ポップアップで [すぐに有効化（Enable Now）] をクリックして、同期を有効にします。

次に完全同期を行います。

26. [アクション（Actions）] メニューをクリックし、[すぐに同期（Sync Now）] > [完全（Full）] の順に選択します。

完全同期



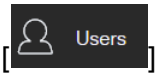
27. ポップアップで [はい（Yes）] をクリックします。

28. [現在の同期（Current Synchronization）] セクションで、ユーザの作成とアバターのアップロードの進行状況を確認できます。同期が完了すると、[前回の同期（Last Synchronization）] セクションに 

のようにステータスが表示されます。

注：同期のエラー/警告が表示された場合は、完全同期をやり直してください。エラー/警告を [イベント（Event）] ビューで確認することもできます。ディレクトリコネクタの [イベントビューアの起動（Launch Event Viewer）] ボタンをクリックすれば確認できます。次に、[アプリケーションとサービスのログ（Applications and Services Logs）] > [シスコディレクトリコネクタ（Cisco Directory Connector）] の順に移動して、すべてのイベントを表示します。

29. Workstation 1 で開いた、Webex Control Hub（https://admin.webex.com）に接続している Chrome Web ブラウザを最大化して、ユーザが同期されていることを確認します。

30. ポータルで、[ユーザ（Users）] タブ [

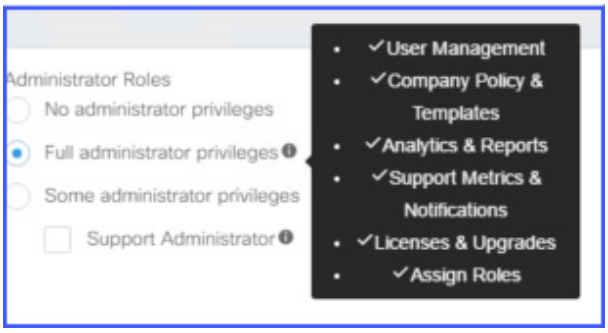
] をクリックします（すでに開いている場合は、ページを更新します）。

31. 8 人のユーザとそれぞれのアバター、電子メールアドレス、名前などのユーザ情報のリストが表示されます。

注：ユーザは、Webex Teams にログインしてアカウントをアクティブにし、パスワードを設定するまで [招待保留中（Invite Pending）] ステータスのままになります。

32. 現時点では、Charles が組織内の唯一の管理者になっています。もう 1 人のエンジニア Taylor Bard が、Webex Control Hub に対する管理アクセス権を必要としています。ユーザリストから [Taylor Bard] を選択します。
33. ポップアップウィンドウで、[ロールとセキュリティ（Roles and Security）] を選択します。
34. [フル管理者権限（Full administrator privileges）] オプションボタンをクリックします。

フル管理者権限



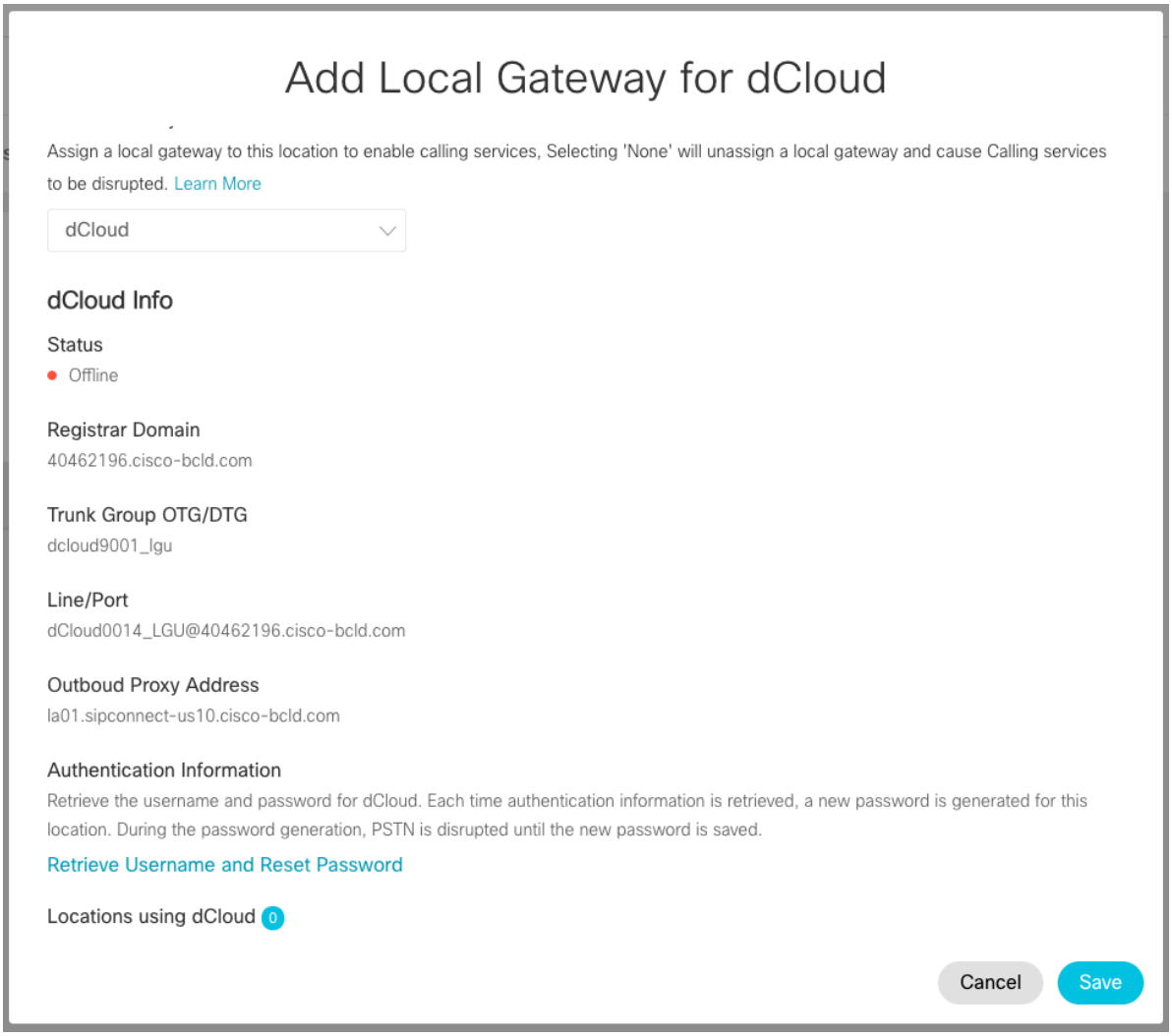
35. [保存（Save）] をクリックします。
36. ユーザを手動で追加するには、後でディレクトリコネクタを無効にする必要があります。ここで先に進み、ディレクトリコネクタを無効にします。
37. ディレクトリコネクタで、[アクション（Actions）] > [同期モード（Synchronization Mode）] > [同期の無効化（Disable Synchronization）] の順に移動します。
38. [はい（Yes）] をクリックして無効にします。
39. Workstation 1 のディレクトリコネクタを閉じます。

これで、お客様のオンプレミス Active Directory を同期して Cisco Webex Control Hub の組織にユーザを設定し、フル管理者権限を持つ管理者をもう 1 人組織に割り当てました。

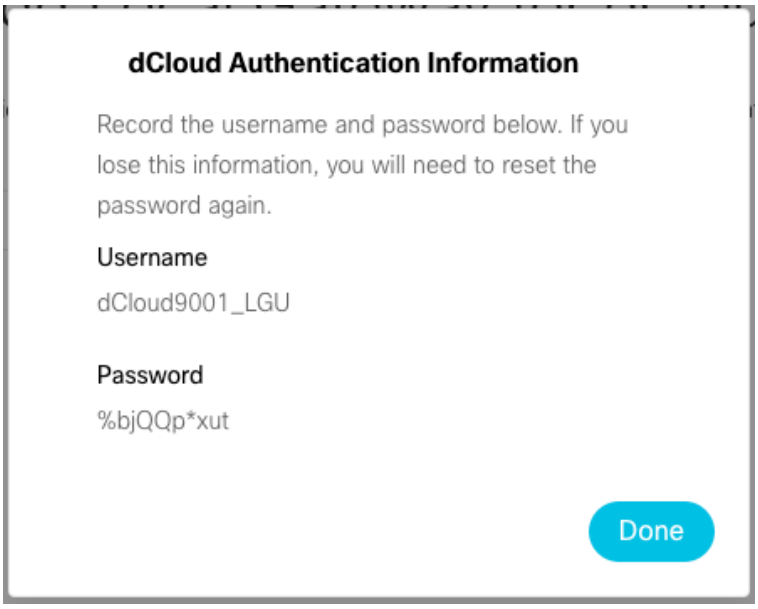
付録 D.　ローカルゲートウェイの全設定

以下は、参照用にラボで実施したローカルゲートウェイの全設定です。赤の項目は、独自のラボ設定が必要な項目であることに注意してください。また、最新の情報は設定ガイドを参考にしてください。以下の図は、設定用に使用したものです。

ローカルゲートウェイの設定例



ローカルゲートウェイのユーザ名とパスワードのサンプル




```
crypto pki trustpoint dummyTp
 revocation-check crl
!
voice service voip
 ip address trusted list
  ipv4 85.119.56.128 255.255.255.192
  ipv4 85.119.57.128 255.255.255.192
  ipv4 185.115.196.0 255.255.255.128
  ipv4 185.115.197.0 255.255.255.128
  ipv4 199.59.64.0 255.255.255.128
  ipv4 199.59.65.0 255.255.255.128
  ipv4 199.59.66.0 255.255.255.128
  ipv4 199.59.67.0 255.255.255.128
  ipv4 199.59.70.0 255.255.255.128
  ipv4 199.59.71.0 255.255.255.128
 media statistics
 media bulk-stats
```

```
 allow-connections sip to sip
 no supplementary-service sip refer
 no supplementary-service sip handle-replaces
 fax protocol pass-through g711ulaw
 stun
  stun flowdata agent-id 1 boot-count 4
  stun flowdata shared-secret 7 104D000A061811021F0725282D3B303A
 sip
  early-offer forced
  g729 annexb-all
!
voice class uri 200 sip
 pattern :8934
!
voice class uri 300 sip
 pattern :5065
voice class codec 99
 codec preference 1 g711ulaw
 codec preference 2 g711alaw
 codec preference 3 g729r8
!
voice class stun-usage 200
 stun usage firewall-traversal flowdata
!
voice class sip-profiles 200
 rule 9 request ANY sip-header SIP-Req-URI modify "sips:(.*)" "sip:\1"
 rule 10 request ANY sip-header To modify "<sips:(.*)" "<sip:\1"
 rule 11 request ANY sip-header From modify "<sips:" "<sip:\1"
 rule 12 request ANY sip-header Contact modify "<sips:(.*)>" "<sip:\1;transport=tls>"
```

```
 rule 13 response ANY sip-header To modify "<sips:(.*)" "<sip:\1"
 rule 14 response ANY sip-header From modify "<sips:(.*)" "<sip:\1"
 rule 15 response ANY sip-header Contact modify "<sips:(.*)" "<sip:\1"
 rule 20 request ANY sip-header From modify ">" ";otg=dcloud9001_lgu>"
 rule 30 request ANY sip-header P-Asserted-Identity modify "sips:(.*)" "sip:\1"
!
voice class dpg 200
 dial-peer 201 preference 1
!
voice class dpg 300
 dial-peer 301 preference 1
!
voice class server-group 301
 ipv4 198.18.133.3 port 5065
voice class tenant 200
  registrar dns:40462196.cisco-bcld.com scheme sips expires 240 refresh-ratio 50 tcp tls
  credentials number dCloud0014_LGU username dCloud9001_LGU password %bjQQp*xut realm BroadWorks
  authentication username dCloud9001_LGU password %bjQQp*xut realm BroadWorks
  authentication username dCloud9001_LGU password %bjQQp*xut realm 40462196.cisco-bcld.com
  no remote-party-id
  sip-server dns:40462196.cisco-bcld.com
  connection-reuse
  srtp-crypto 200
  session transport tcp tls
  url sips
  error-passthru
  asserted-id pai
  bind control source-interface GigabitEthernet1
  bind media source-interface GigabitEthernet1
```

```
  no pass-thru content custom-sdp
  sip-profiles 200
  outbound-proxy dns:la01.sipconnect-us10.cisco-bcld.com
  privacy-policy passthru
!
voice class tenant 100
  session transport udp
  url sip
  error-passthru
  bind control source-interface GigabitEthernet2
  bind media source-interface GigabitEthernet2
  no pass-thru content custom-sdp
!
voice class tenant 300
  bind control source-interface GigabitEthernet2
  bind media source-interface GigabitEthernet2
  no pass-thru content custom-sdp
!
voice class srtp-crypto 200
 crypto 1 AES_CM_128_HMAC_SHA1_80
!
dial-peer voice 201 voip
 description Outgoing dial-peer to Webex
 destination-pattern .T
 session protocol sipv2
 session target sip-server
 voice-class codec 99
 voice-class stun-usage 200
 no voice-class sip localhost
```

```
 voice-class sip tenant 200
 dtmf-relay rtp-nte
 srtp
 no vad
!
dial-peer voice 301 voip
 description Outgoing dial-peer to Unified CM Webex Calling Trunk for inbound
 destination-pattern .T
 session protocol sipv2
 session server-group 301
 voice-class codec 99
 voice-class sip tenant 100
 dtmf-relay rtp-nte
 no vad
!
dial-peer voice 200 voip
 description Incoming dial-peer from Webex
 session protocol sipv2
 destination dpg 300
 incoming uri via 200
 voice-class codec 99
 voice-class stun-usage 200
 voice-class sip tenant 200
 dtmf-relay rtp-nte
 srtp
 no vad
!
dial-peer voice 300 voip
 description Incoming dial-peer from Unified CM for Webex
```

```
 session protocol sipv2
 destination dpg 200
 incoming uri via 300
 voice-class codec 99
 voice-class sip tenant 300
 dtmf-relay rtp-nte
 no vad
!
!
sip-ua
 transport tcp tls v1.2
 crypto signaling default trustpoint dummyTp cn-san-validate server
```

付録 E.　Webex ハイブリッド カレンダー サービスの全設定

ハイブリッド カレンダー サービスを使用すると、オンプレミスの Microsoft Exchange、Office 365、Google の G Suite カレンダー（Google カレンダー）環境を Cisco Webex に統合できます。統合することで、会議のスケジュール設定と参加が容易になります（特にモバイルの場合）。プラグインは必要ありません。

ハイブリッド カレンダー サービスでは、Cisco Call Control を使用していません。ハイブリッド カレンダー サービスを使用すると、サードパーティの UC ソリューションを使用している場合でも、Cisco Webex ユーザに機能を拡張できます。

シンプルな会議のスケジューリング

カレンダー招待状の [場所（Location）] フィールドにスケジュール設定用キーワードと修飾子を入力すると、簡単に会議のスケジュールを設定できます。

表 50.　シンプルな会議のスケジューリング

実行する内容	[場所（Location）] フィールドに指定できるキーワード
会議用の Cisco Webex Teams スペースを作成するか、Cisco Webex Teams から会議をホストする	@webex:space @meet @meet:space @spark（廃止）
Webex パーソナルルーム用のクリック可能なリンクを含める	@webex @webex:myroom @meet:myroom 自分のパーソナルルーム URL（例：https://<会社名>.webex.com/meet/<ホスト ID>）

会議リストと参加ボタン

Cisco Webex Teams の会議リストを使用すると、今後 4 週間に予定されている会議を確認できます。会議が開始される 5 分前に、会議リストに [参加（Join）] ボタンが表示され、予定されている会議の通知が届きます。

ユーザは、Cisco Webex Room、デスクデバイス、Webex Board を会議に追加して利用することができます。デバイスでハイブリッド カレンダー サービスが有効になっている場合は、緑色の [参加（Join）] ボタンがデバイスに表示されます（[参加（Join）] ボタンはOne Button to Push(OBTP)とも呼ばれます。Cisco Unified Communications Manager に登録され、Cisco TelePresence Management Suite によって管理されるデバイスでも使用できます）。ハイブリッド カレンダー サービス対応の Room デバイスおよびデスクデバイスでも、招待された会議を会議リストに表示できます。

詳細な設定ガイドについては、hhttps://www.cisco.com/go/hybrid-services-calendar を参照してください。

Expressway-C コネクタホストの設定

次に、Cisco Webex ハイブリッドサービスで使用する、新しい Expressway-C コネクタホストをカスタマー組織に追加します。この Expressway-C サーバには、Cisco Webex ハイブリッド カレンダー サービスおよびコールサービスで必要なすべてのコネクタが含まれています。

1. 開いている Cisco Webex Control Hub に戻ります。Charles Holland でログインしたままで、セッション VPN への接続も維持されていることを確認します。
2. ポータル内の左側のメニューで、[サービス（Services）] をクリックします。
3. [Exchangeハイブリッドカレンダー（Hybrid Calendar Exchange）] で、[セットアップ（Set up）] をクリックします。
4. [ハイブリッドカレンダーサービスの設定（Hybrid Calendar Service Setup）] ポップアップウィンドウで、[次へ（Next）] をクリックします。
5. 最初のオプションボタンを選択してボックスに **exp-cc.dcloud.cisco.com** と入力し、[次へ（Next）] をクリックします。
6. クラスタ名として **HS Cluster 1** と入力します。
7. もう一度 [次へ（Next）] をクリックします。
8. [次へ（Next）] を再度クリックすると、新しいブラウザタブが開き、Expressway にアクセスします。
9. ユーザ名：**admin**、パスワード：**dCloud123!** で Expressway にログインします
10. [この信頼に必要なExpressway CA証明書をシスコが管理する（I want Cisco to manage the Expressway CA certificates required for this trust）] チェックボックスをオンにします。
11. [ソフトウェアの更新および接続の検証（Update software & verify connection）] をクリックします。
12. 検証できたら、[登録（Register）] をクリックします（Webex にログインするようにプロンプトが表示されたら、ユーザ名とパスワードに **cholland@cbXXX.dc-YY.com/dCloud123!** を入力します）。
13. 次の画面で、[Expresswayへのアクセスを許可（Allow Access to the Expressway）] チェックボックスをオンにし、[続行（Continue）] をクリックします。

しばらくすると Expressway に戻り、2 つのハイブリッド サービス コネクタがダウンロードされてインストールされます。2 つのコネクタは、管理コネクタとカレンダーコネクタです。管理コネクタは、Expressway-C サーバ上のすべてのコネクタを管理します。3 番目のコネクタであるコールコネクタは、このラボでハイブリッドコールサービスを有効にした時点でインストールされます。

Exchange の設定

次に、Cisco Webex カレンダーサービスで使用する疑似アカウントを設定します。疑似アカウントをサービスアカウントとして使用するには、メールが有効になっているアカウントとして設定する必要があります。このアカウントは管理者である必要はありませんが、メールボックスが設定されていなければなりません。このラボでは、Charles のアカウントを疑似アカウントとして使用します。

1. Exchange（MAIL1）サーバ（**198.18.133.2**）へのリモートデスクトップ接続を確立し、次のログイン情報を使用してログインします。
   - ユーザ名：dcloud\administrator
   - パスワード：**dCloud123!**

2. タスクバーにあるアイコン [] をクリックして、**Exchange 管理シェル**を開きます。

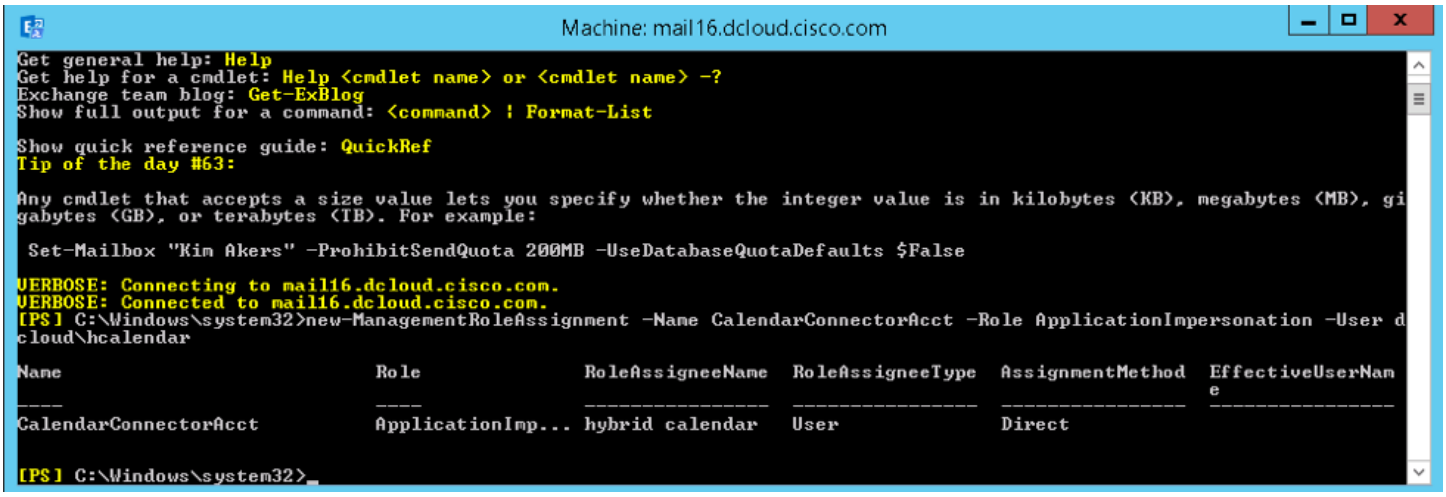
簡単にコマンドをコピーアンドペーストできるように、デスクトップに Calendar Service.txt というテキストファイルが用意されていますので、ファイルを開きます。すでにこの設定を行っている場合は、（管理シェルが開いて [PS] C:\Windows\system32 プロンプトが表示されたら）すべてのコマンドを一度にコピーしてステップ 7 に移ります。

最初に、疑似アカウントとして使用するアカウント（**hcalendar**）を割り当てます。

3. Exchange 管理シェルウィンドウの **[PS]** プロンプトが表示されたら、テキストファイルの最初のコマンドをコピーして貼り付け、**Enter** を押します。コマンドは、次のとおりです。

```
new-ManagementRoleAssignment -Name CalendarConnectorAcct -Role ApplicationImpersonation -User dcloud\hcalendar
```

疑似ロールの追加



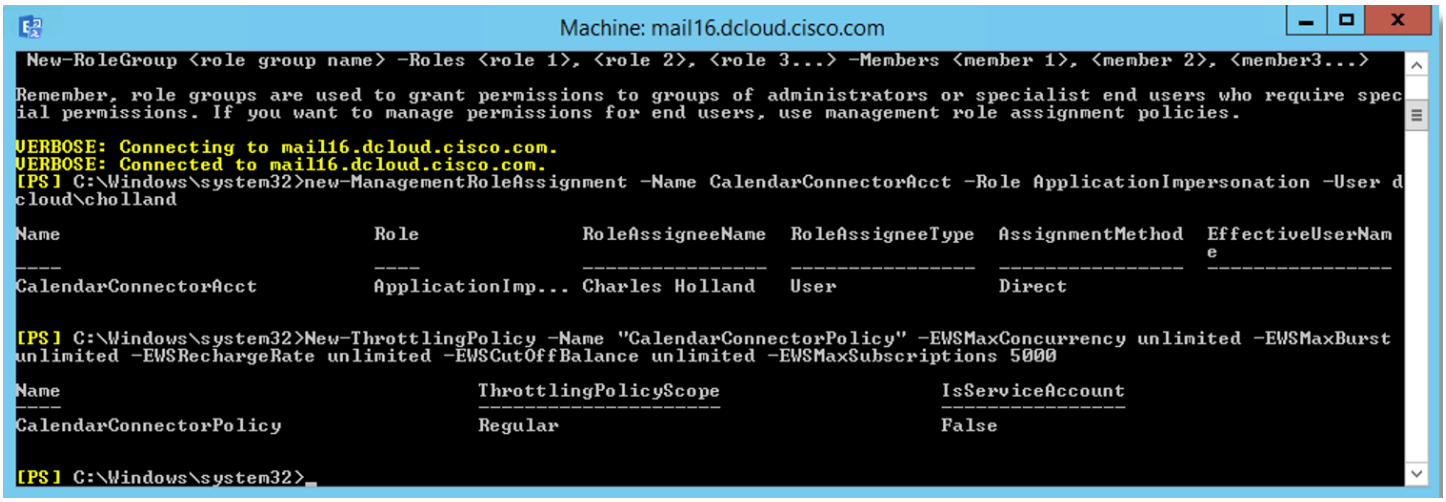
次に、スロットリングポリシーを作成します。カスタム スロットリング ポリシーを作成すると、カレンダーコネクタがスムーズに動作するようになります。

- Exchange Server 2013 では、ポリシーによって疑似アカウントの EWS 制限が除外され、最大同時接続数の問題が解消されます。
- Exchange Server 2010 では、このポリシーがデフォルトのポリシーより優先します。デフォルトのポリシーは、エンタープライズ アプリケーションよりもユーザの負荷を考慮してカスタマイズされています。

4. テキストファイルの 2 番目のコマンドをコピーして Exchange 管理シェルウィンドウに貼り付け、**Enter** を押します。コマンドは、次のとおりです。

```
New-ThrottlingPolicy -Name "CalendarConnectorPolicy" -EWSMaxConcurrency unlimited -EWSMaxBurst unlimited -
EWSRechargeRate unlimited -EWSCutOffBalance unlimited -EWSMaxSubscriptions 5000
```

スロットリングポリシーの追加

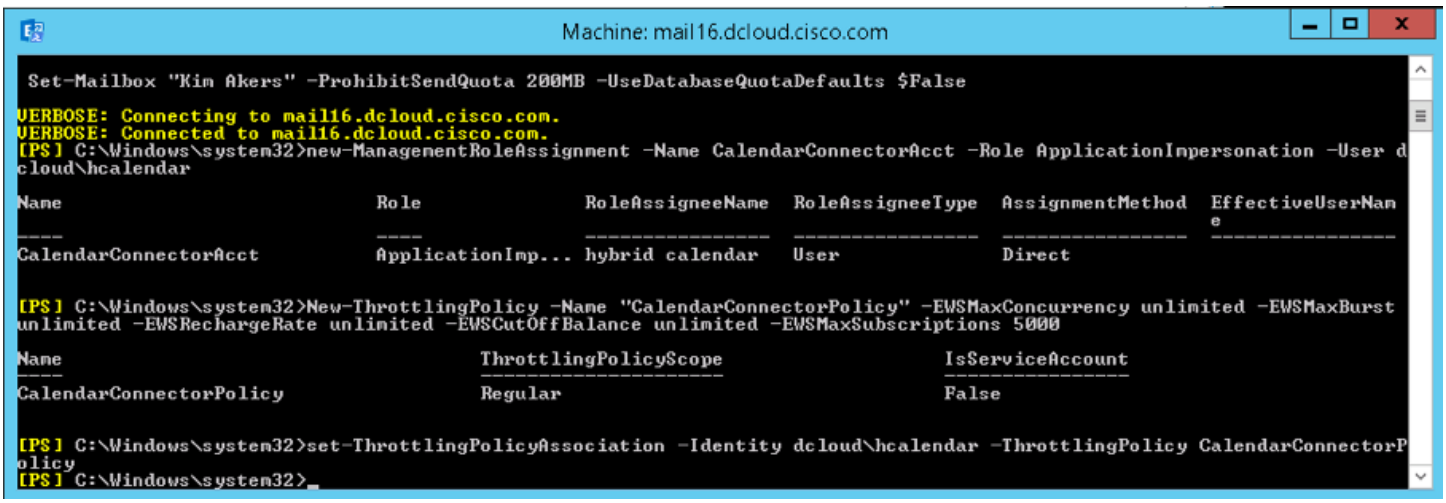


次に、疑似アカウント（**hcalendar**）にスロットリングポリシーを適用します。

5. テキストファイルの 3 番目のコマンドをコピーして Exchange 管理シェルウィンドウに貼り付け、**Enter** を押します。コマンドは、次のとおりです。

```
set-ThrottlingPolicyAssociation -Identity dcloud\hcalendar -ThrottlingPolicy CalendarConnectorPolicy
```

hcalendar にスロットリングポリシーを適用



6. メールボックスに新しいポリシーが適用されていることを確認するには、テキストファイルの 4 番目のコマンドをコピーして Exchange 管理シェルウィンドウに貼り付け、**Enter** を押します。コマンドは、次のとおりです。

```
get-ThrottlingPolicyAssociation -Identity dcloud\hcalendar
```

スロットリングポリシー割り当ての確認

7. ワンボタン機能（OBTP）は後でテストしますが、Exchange Server にログオン中の場合は、先に進んで PowerShell ウィンドウに次のコマンドを入力して、Room デバイス用の Room メールボックスを設定します。

```
New-Mailbox -Name 'Webex Room Device' -Alias 'webexrd' -room
```

注：Microsoft Exchange RPC Client Access サービスを再起動する必要があります。簡単に再起動できるように、バッチファイルが用意されています。

8. デスクトップにある **Restart RPC Client Access.bat** ファイル [

] をダブルクリックして実行します。このバッチファイルは数秒で完了し、終了するとウィンドウが閉じます。
9. **メモ帳**と **Exchange 管理シェル**ウィンドウを閉じ、Exchange サーバに対するリモートデスクトップ接続を終了します。

次に、カレンダーコネクタを Microsoft Exchange にリンクします。

Microsoft Exchange に Expressway-C をリンクする

以下のいくつかのセクションでは、Cisco Webex カレンダーサービス用に Expressway-C ホストを設定します。Cisco Webex で使用する Expressway-C でカレンダーサービスを設定していない場合は、手動で設定する方法を確認しておくことをお勧めします。ただし、SSO についてのラボガイドと同様に、Expressway-C ホスト設定用のクイックスクリプトも用意されています。すでに設定を行っていてそのまま完了したい場合は、カレンダーコネクタのクイック設定セクションにスキップしてください。

1. ブラウザで、[Expressway-Cコネクタホスト（Expressway-C Connector Host）] タブに戻ります。

2. [コネクタマネージャ（Connecter Manager）] ページで、[Microsoft Exchange Serverの設定（Configure Microsoft Exchange Servers）] リンク（[アプリケーション（Applications）] > [ハイブリッドサービス（Hybrid Services）] > [カレンダーサービス（Calendar Service）] > [Microsoft Exchangeの設定（Microsoft Exchange Configuration] でも可）をクリックします。
3. [新規（New）] をクリックします。
4. 以下の表に従ってパラメータを設定します。

表 51. Microsoft Exchange の設定パラメータ

設定対象	設定内容
[サービスアカウントのユーザ名（Service Account Username）]	dcloud\hcalendar
[サービスアカウントのパスワード（Service Account Password）]	dCloud123!
[表示名（Display Name）]	mail16
[タイプ（Type）]	[Exchangeオンプレミス（Exchange On-Premises）]（デフォルト）
[Exchangeサーバの有効化（Enable this Exchange server）]	[はい（Yes）]（デフォルト）
[NTLM認証（NTLM Authentication）]	オン（デフォルト）
[ベーシック認証（Basic Authentication）]	オン（デフォルト）
[TLS検証モード（TLS Verify Mode）]	オフ
[自動検出（Autodiscover）]	[自動検出を使用（Use Autodiscover）]（デフォルト）
[Active Directoryドメイン（Active Directory domain）]	dcloud.cisco.com
[クエリモード（Query Mode）]	ldap
[電子メールアドレス（Email Address）]	cholland@cbXXX.dc-YY.com

注：このラボでは TLS は使用しません。TLS を使用する場合は、Exchange と Expressway に CA 署名証明書をインストールする必要があります。完全な手順については、**セットアップガイド**に記載されています。

5. [追加（Add）] をクリックします。

Webex サイトの設定

次に、Webex Meeting Center と CMR Cloud サイトの詳細を設定します。Webex トライアル版の構築中に作成した Webex サイトを使用します。

実稼働環境で @webex 機能をユーザが使用できるようにするには、次のことを確認します。

- 少なくとも 1 つの Webex Meetings Center に CMR Cloud サイトがある
- 各ユーザの Webex アカウントの電子メールアドレスが、ユーザの Exchange 電子メールアドレスに一致している

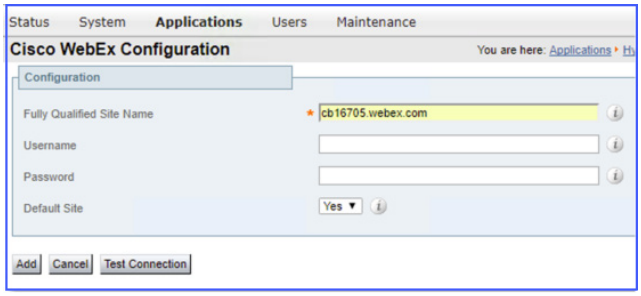
1. Expressway-C コネクタホストで、[アプリケーション（Applications）] > [ハイブリッドサービス（Hybrid Services）] > [カレンダーサービス（Calendar Service）] > [シスコ会議サービスの設定（Cisco Conferencing Services Configuration）] の順に移動します。
2. [新規（New）] をクリックします。
3. 以下の表に従ってパラメータを設定します。

表 52. Cisco WebEx Meetings サイトの設定

設定対象	設定内容
[完全修飾サイト名（Fully Qualified Site Name）]	cbXXXYY.webex.com（Control Hub の [サービス（Services）] でサイト URL を確認できます）
[ユーザ名（Username）]	空白のまま（ボックスに何か表示されている場合は削除します）
[パスワード（Password）]	空白のまま（ボックスに何か表示されている場合は削除します）
[デフォルトサイト（Default Site）]	[はい（Yes）]（デフォルト）

注：Webex Meetings サイトの URL が機能しない場合は、Control Hub で URL を確認してください。[サービス（Services）] > [会議（Meeting）] > [サイト（Sites）] > [サイト名（Site Name）] の順に移動します。使用可能なその他の URL には、https://cbXXXYYa.webex.com、https://cbXXXYYb.webex.com、https://cbXXXYYc.webex.com があります。

Cisco Webex CMR の設定例



4. [追加（Add）] をクリックします。

カレンダーコネクタの起動

1. [アプリケーション（Applications）] > [ハイブリッドサービス（Hybrid Services）] > [コネクタ管理（Connector Management）] の順に移動します。
2. [カレンダーコネクタ（Calendar Connector）] リンクをクリックします。
3. [アクティブ（Active）] ドロップダウンメニューを [有効（Enabled）] に変更します。
4. [保存（Save）] をクリックします。

しばらくするとページが更新され、ステータスが [実行中（Running）] [Running] に変わります。カレンダーコネクタを手動で設定しているため、次のセクション「カレンダーコネクタのクイック設定」はスキップして、「**ユーザのカレンダーサービスの有効化**」セクションに移ります。

ユーザのカレンダーサービスの有効化

2 人のユーザ（Charles と Anita）のカレンダーサービスを有効にします。この 2 人のユーザは手動で設定します。CSV テンプレートを使用して、複数のユーザを一括して設定できます。後ほど、ラボの別のシナリオで、この方法を利用してユーザサービスを一括で設定します。ここでは個別に設定します。

1. Cisco Webex Control Hub に戻ります。
2. 左側のメニューで [ユーザ（Users）] をクリックします。
3. リストから [Charles Holland] を探してクリックします。
4. ポップアップウィンドウで [編集（Edit）] をクリックします。
5. [メッセージング（Messaging）] および [会議（Meeting）] 列のすべてのチェックボックスがオンになっていることを確認し、なっていなければ、すべてオンにして [保存（Save）] をクリックくします。すでに選択されている場合は、[キャンセル（Cancel）] をクリックします。
6. [ハイブリッドサービス（Hybrid Services）] セクションの [カレンダーサービス（Calendar Service）] をクリックします。
7. [カレンダーサービス（Calendar Service）] の横のトグルボタンをクリックしてオンにし、[保存（Save）] をクリックします。

ステータスが [アクティベーション保留中（Pending Activation）] から [アクティベーション済み（Activated）] に変わるまで約 5 分かかります。その間に、**Anita Perez** にも同じサービスを設定します。

注：各ユーザが Cisco Webex Teams クライアントに一度ログインするまで、アクティベーションは開始されません。これまで Anita のアカウントにログインしていないので、彼女のアカウントで Webex サービスを有効にした後で実行します。

8. 左側のメニューで [場所（Places）] をクリックします。
9. 以前作成した場所を選択して [編集（Edit）] をクリックします。

注：Room デバイスの作成をスキップした場合、ここで作成できます。[新しい場所（New Place）] をクリックします。場所に名前を指定し、[次へ（Next）] をクリックします。[その他のCisco Webexデバイス（Other Cisco Webex Device）] を選択し、[次へ（Next）] をクリックします。

10. [カレンダー（Calendar）] オプションをオンに切り替えて、[次へ（Next）] をクリックします。
11. 以前 Exchange で作成した Room メールボックスエイリアスの電子メールアドレス（**webexrd@cbXXX.dc-YY.com**）を入力します。

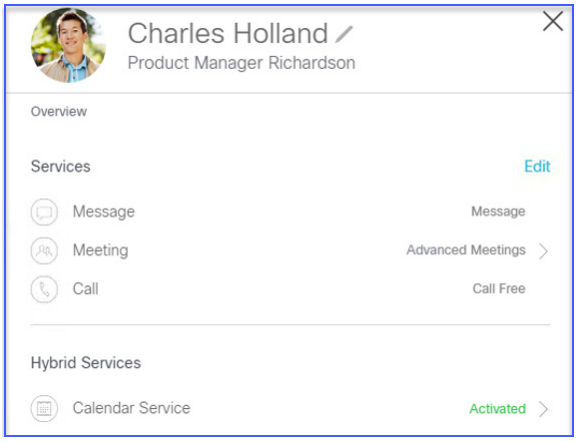
12. [保存（Save）] をクリックします（または新しい場所を作成するだけの場合は、[次へ（Next）] をクリックします）。

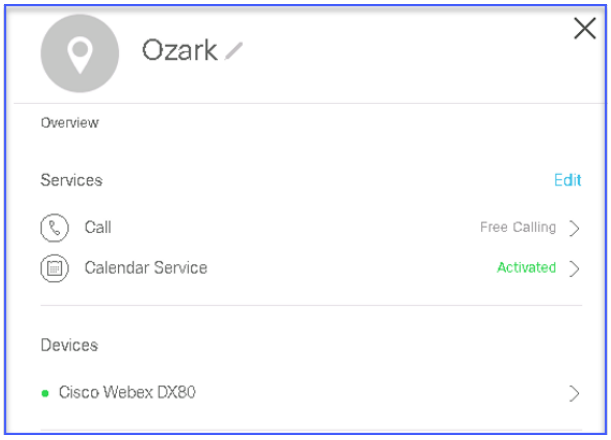
注：新しいデバイスを作成した場合は、Room デバイスにアクティベーションコードを入力します。次に、[場所の追加（Add Place）] ウィンドウを閉じます。

該当の場所の**カレンダーサービス**がアクティブになるまで約 5 分かかります。

13. Charles と Room デバイスの両方でカレンダーサービスがアクティブになっていることを確認します。アクティブになっていない場合は、アクティブになるまで待ちます。次の注を参照してください。

Charles と Room デバイスでアクティブになったカレンダーサービス





注：Control Hub でユーザがアクティブと表示されるまで時間がかかることがあります。Expressway-C コネクタホストではアクティブになったユーザがすぐに表示される場合があります。コネクタホストで、[アプリケーション（Applications）] > [ハイブリッドサービス（Hybrid Services）] > [カレンダーサービス（Calendar Service）] > [カレンダーコネクタステータス（Calendar Connector Status）] の順に移動します。ユーザがアクティブになっている場合は、[正常にサブスクライブされたユーザ（Successfully Subscribed Users）] の横にユーザ数が表示されます。

会議用の Cisco Webex Teams スペースの作成テスト、または OBTP 付き Cisco Webex Teams を利用した会議のホスト

1. Workstation 1 にまだ接続していない場合は、Workstation 1（**198.18.1.36**）への RDP 接続を確立し、以下のログイン情報でログインします。
   - ユーザ名：**dcloud\cholland**
   - パスワード：**dCloud123!**
2. **Outlook** をまだ開いていない場合は、タスクバーのアイコン [] をクリックして開きます。

3. Outlook の下部にある [カレンダー（Calendar）] をクリックし、[新規会議（New Meeting）] [

] をクリックします。
4. Anita Perez、Taylor Bard、Kellie Melby を [宛先（To）] 行に追加します。
5. 適切な [件名（Subject）] を入力します。
6. [場所（Location）] に以下のいずれかのキーワードを入力してスペース会議を作成します。
   - @webex:space
   - @meet
   - @meet:space
7. OBTP の場合は、[場所（Location）] フィールドの最後の [ルーム...（Rooms...）] をクリックします。
8. Exchange Server で以前作成した Room メールボックスを選択し、[OK] をクリックします。
9. 場所の更新ポップアップには [いいえ（No）] をクリックします。
10. ワークステーションの時計に基づいて、今日の開始時間（先の時間）を設定します。OBTP と会議通知が機能するように、10 分以上先の時間を設定します。
11. 必要に応じて、メッセージの本文に適切な文を入力します。
12. 上記のいずれかのキーワードが [場所（Location）] フィールドに設定されていることを確認し、[送信（Send）] をクリックします。

カレンダーコネクタによって [場所（Location）] フィールドのキーワードが読み取られ、Webex Teams スペース情報が会議の招待状に設定されます。また Cisco Webex Teams スペースが作成され、すべての参加者が登録されます。しばらくしてから作成した会議を開くと、Webex Meetings 情報が招待状の最下部に表示されています。情報が表示されない場合は、会議を閉じて、しばらくしてから再度開きます。

13. Workstation 1 の Cisco Webex Teams クライアントを起動し、**cholland@cbXXX.dc-YY.com/dCloud123! でログインします。**
14. スペースキーワードを使用した場合は、アカウント内に、会議の招待状の件名と同じ名前のスペースが作成されています。
15. **スペース**をクリックすると、そのスペースにも会議の詳細が表示されていることがわかります。
16. **会議** [
] アイコンをクリックして、会議リストを表示します。会議を選択して、Room デバイスを含む参加者を確認します。ユーザが招待を受け入れたかどうかも確認できます。
17. スケジュールされた会議の 6 分前に Webex Teams アプリで参加通知を受信したら、[通知（notification）]、[ビデオで参加（Join With Video）] の順にクリックします。

注：時間を節約するため、このスペース会議が開始されるのを待っている間に、次のセクションで示す Webex Meetings 用の別の会議をスケジュールします。

18. Room デバイスで、Charles がすでに会議に参加していることを確認します。[参加（Join）] ボタンを押して、進行中の会議に直接参加します。
19. 完了したら、会議を終了します。他のキーワードを使用して、いろいろな会議を自由に設定してください。

OBTP 付き Webex パーソナルルームへのリンクを含めるテスト

ここで OBTP 付き Webex Meeting を設定する機能をテストします。

1. 前の会議がまだ進行中の場合は、カレンダーでその会議を右クリックし、[会議のキャンセル（Cancel Meeting）] を選択後、[キャンセルの送信（Send Cancelation）] をクリックして Room デバイスを解放します。Room デバイスを二重に予約することはできません。
2. Outlook の下部にある [カレンダー（Calendar）] をクリックし、[新規会議（New Meeting）] [

] をクリックします。
3. **Anita Perez**、**Taylor Bard**、**Kellie Melby** を [宛先（To）] 行に追加します。必要に応じて、自分の電子メールアドレスを追加することもできます。
4. 適切な [件名（Subject）] を入力します。
5. [場所（Location）] に次のいずれかのアドレスを入力してスペース会議を作成します。
   - @webex
   - @webex:myroom
   - @meet:myroom
   - https://cbXXXYY.webex.com/meet/cholland
6. OBTP の場合は、[場所（Location）] フィールドの最後の [ルーム...（Rooms...）] をクリックします。
7. Exchange Server で以前作成した Room メールボックスを選択し、[OK] をクリックします。
8. 場所の更新ポップアップには [いいえ（No）] をクリックします。
9. ワークステーションの時計に基づいて、今日の開始時間（先の時間）を設定します。OBTP と会議通知が機能するように、10 分以上先の時間を設定します。
10. 必要に応じて、メッセージの本文に適切な文を入力します。
11. キーワードがまだ [場所（Location）] フィールドに設定されていることを確認し、[送信（Send）] をクリックします。

これでカレンダーコネクタによって [場所（Location）] フィールドからキーワードが読み取られ、会議がセットアップされます。しばらくしてから作成した会議を開くと、Webex Meetings 情報が招待状の最下部に表示されています。情報が表示されない場合は、会議を閉じて、しばらくしてから再度開きます。

12. スケジュールされた会議の 6 分前にホストの Charles が Webex Teams アプリで参加通知を受信したら、[通知（notification）]、[ビデオで参加（Join With Video）] の順にクリックします。
13. Room デバイスで、Charles がすでに会議に参加していることを確認します。[参加（Join）] ボタンを押して、進行中の会議に直接参加します。
14. 完了したら、会議を終了します。

ここまでで、キーワード機能を使用した Exchange ハイブリッド カレンダー サービス、およびワンボタン機能 (OBTP)、会議リスト、参加通知のテストができました。

お問い合せ先

シスコシステムズ合同会社

〒107 - 6227 東京都港区赤坂 9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp