展開シナリオ

オンプレミス展開

オンプレミス展開とは、社内ネットワークのすべてのサービスをセットアップ、管理、保守する展開です。

次のモードCisco Jabberで展開できます。

- **フル UC**：フル UC モードを展開するには、インスタント メッセージングとプレゼンス機能を有効にし、ボイスメールと会議機能をプロビジョニングし、音声とビデオ用のデバイスを使用してユーザをプロビジョニングします。
- **IM 専用**：IM 専用モードを展開するには、インスタント メッセージングとプレゼンス機能を有効にします。デバイスを使用してユーザをプロビジョニングしないでください。
- **電話機のみのモード**: 電話機のみのモードでは、ユーザのプライマリ認証がCisco Unified Communications Managerになります。電話機専用モードを展開するには、音声とビデオ機能用のデバイスを使用してユーザをプロビジョニングします。また、ボイス メールなどの追加サービスを持つ個人をプロビジョニングできます。

デフォルト製品モードは、ユーザのプライマリ認証が IM and Presence サーバで行われるモードです。

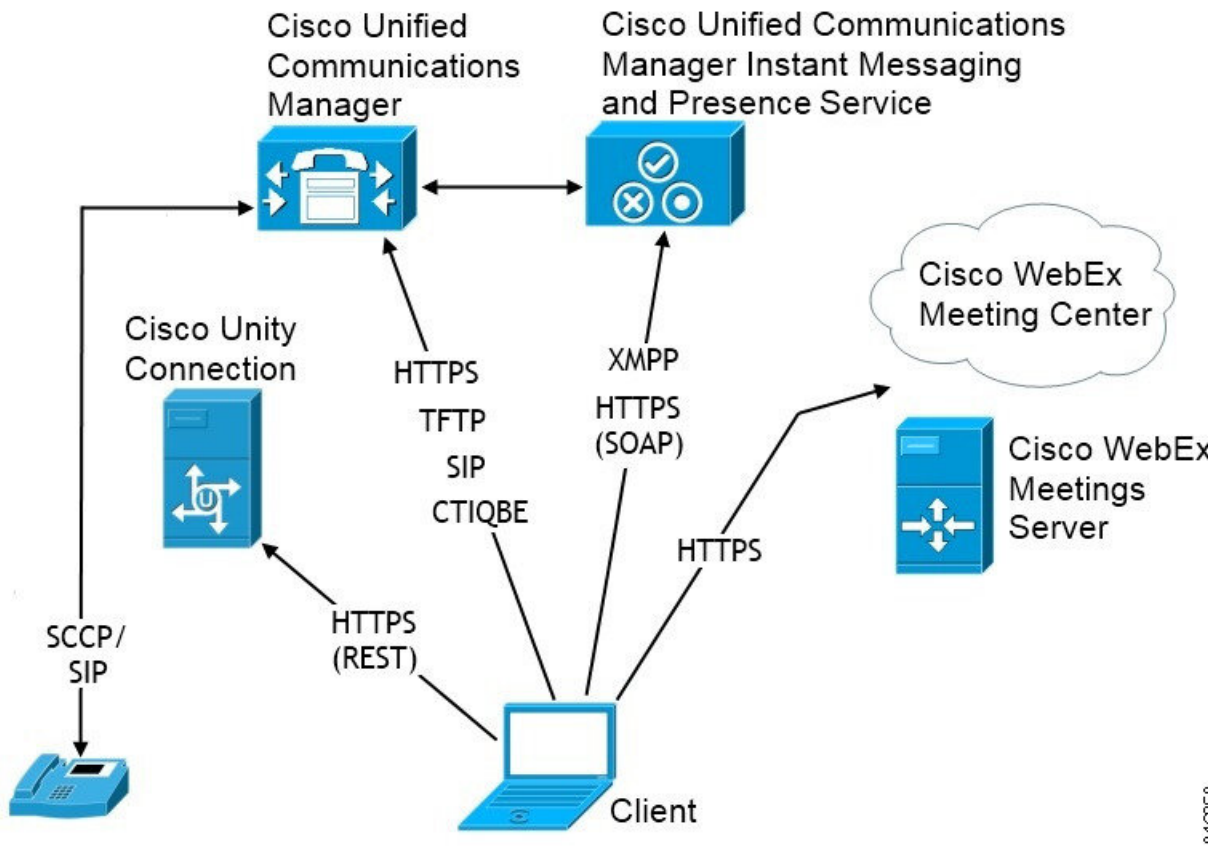
Cisco Unified Communications Manager IM and Presence Service によるオンプレミス展開

Cisco Unified Communications Manager IM and Presence Serviceによるオンプレミス展開で使用可能なサービスは次のとおりです。

- **プレゼンス**：Cisco Unified Communications Manager IM and Presence Service 経由で対応可否を公開し、他のユーザの対応可否をサブスクライブします。
- **IM**：Cisco Unified Communications Manager IM and Presence Service を介して IM を送受信します。
- **ファイル転送**: Cisco Unified Communications Manager IM and Presence Service を介してファイルおよびスクリーンショットを送信および受信します。
- **音声コール**：卓上電話機を介して、またはコンピュータで Cisco Unified Communications Manager を介して音声コールを発信します。
- **ビデオ**—Cisco Unified Communications Managerを通じてビデオ通話を発信します。
- **ボイスメール**—Cisco Unity Connectionを通じてボイスメッセージを送受信します。
- **会議**：次のいずれかと統合します。
  - Cisco Webex Meetings センター—ホステッド会議機能を実現します。
  - Cisco Webex Meetings サーバーオンプレミス会議能力を提供します。

次の図は、Cisco Unified Communications Manager IM and Presence Serviceを使った オンプレミス展開のアーキテクチャを示しています。

図 *1* : 以下のものを使ったオンプレミスの展開 *Cisco Unified Communications Manager IM and Presence Service*



コンピュータ テレフォニー インテグレーション

Windows 版 Cisco JabberおよびMac 版 Cisco Jabber Mac には、サードパーティ製のアプリケーションからCisco Jabberの CTI をサポートしています。

コンピュータ テレフォニーインテグレーション（CTI）を使用すれば、電話コールを発信、受信、および管理しながら、コンピュータ処理機能を利用することができます。CTI アプリケーションを使用すれば、発信者 ID から提供された情報に基づいてデータベースから顧客情報を取得したり、自動音声応答（IVR）システムが収集した情報を利用したりできます。

CTI の詳細については、該当するリリースの『*Cisco Unified Communications Manager*システムガイド の項を参照してください。または、Cisco Unified Communications Manager API を通じ、CTI コントロールのアプリケーションを作成する方法についての詳細は、次の Cisco Developer Network サイトを参照してください。

- Cisco TAPI：https://developer.cisco.com/site/jtapi/overview/
- Cisco JTAPI：https://developer.cisco.com/site/jtapi/overview/

電話機モードでのオンプレミス展開

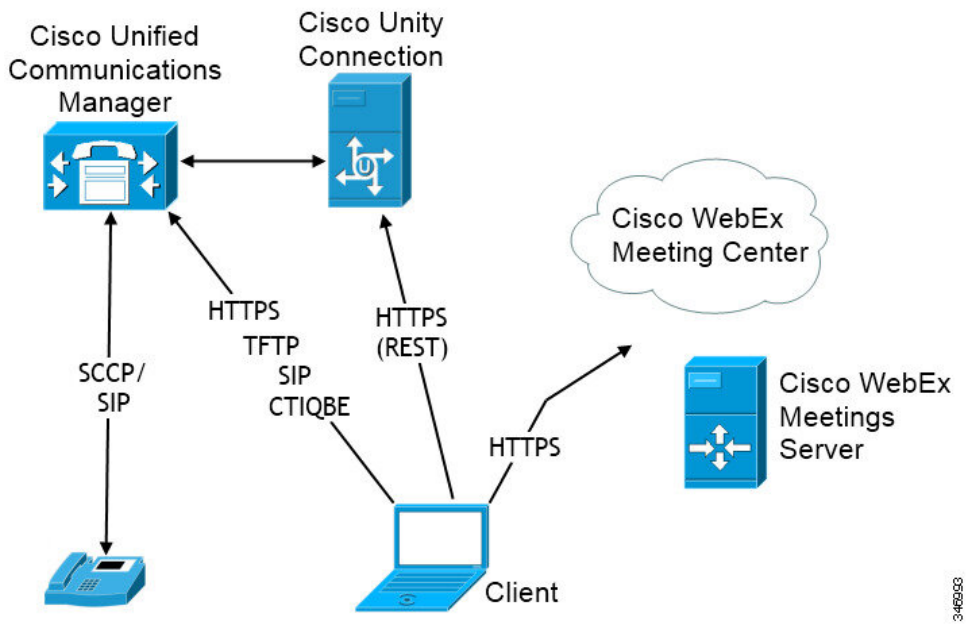
電話機モード展開で使用可能なサービスは次のとおりです。

- **連絡先**：モバイル クライアントのみに適用されます。Cisco Jabber は電話の連絡先アドレス帳から連絡先情報を更新します。
- **音声コール**：卓上電話機を介して、またはコンピュータで Cisco Unified Communications Manager を介して音声コールを発信します。
- **ビデオ**—Cisco Unity Connectionを通じてビデオ通話を発信します。
- **ボイスメール**—Cisco Unity Connectionを通じてボイスメッセージを送受信します。
- **会議**：次のいずれかと統合します。
  - **Cisco Webex Meetingsセンター**—ホステッド会議機能を実現します。
  - **Cisco Webex Meetingsサーバー**—オンプレミス会議能力を提供します。

（注） Android 版 Cisco JabberとiPhone および iPad 版 Cisco Jabberは、電話モードでは会議機能をサポートしません。

次の図は、電話モードでのオンプレミス展開のアーキテクチャを示しています。

図 *2:* 電話機モードでのオンプレミス展開



ソフトフォン

ソフトフォン モードは TFTP サーバから設定ファイルをダウンロードし、SIP に登録済みのエンドポイントとして動作します。クライアントは CCMCIP または UDS サービスを使用して、Cisco Unified Communications Manager に登録するデバイス名を取得します。

デスクフォン

デスクフォン モードは、Cisco Unified Communications Manager との CTI 接続を作成して IP フォンを制御します。クライアントは CCMCIP を使用してユーザに関連付けられたデバイスについての情報を集め、クライアントが制御可能な IP フォンのリストを作成します。

デスクフォン モードの Mac 版 Cisco Jabber は、デスクフォン ビデオをサポートしません。

Extend and Connect

Cisco Unified Communications Manager の Extend and Connect 機能により、ユーザは、公衆電話交換網（PSTN）の電話や構内交換機（PBX）などのデバイスへの通話を制御できます。詳細については、お使いの Cisco Unified Communications Manager リリースの Extend and Connect 機能を参照してください。

Extend and Connect 機能は、Cisco Unified Communications Manager 9.1(1) 以降で使用することをお勧めします。

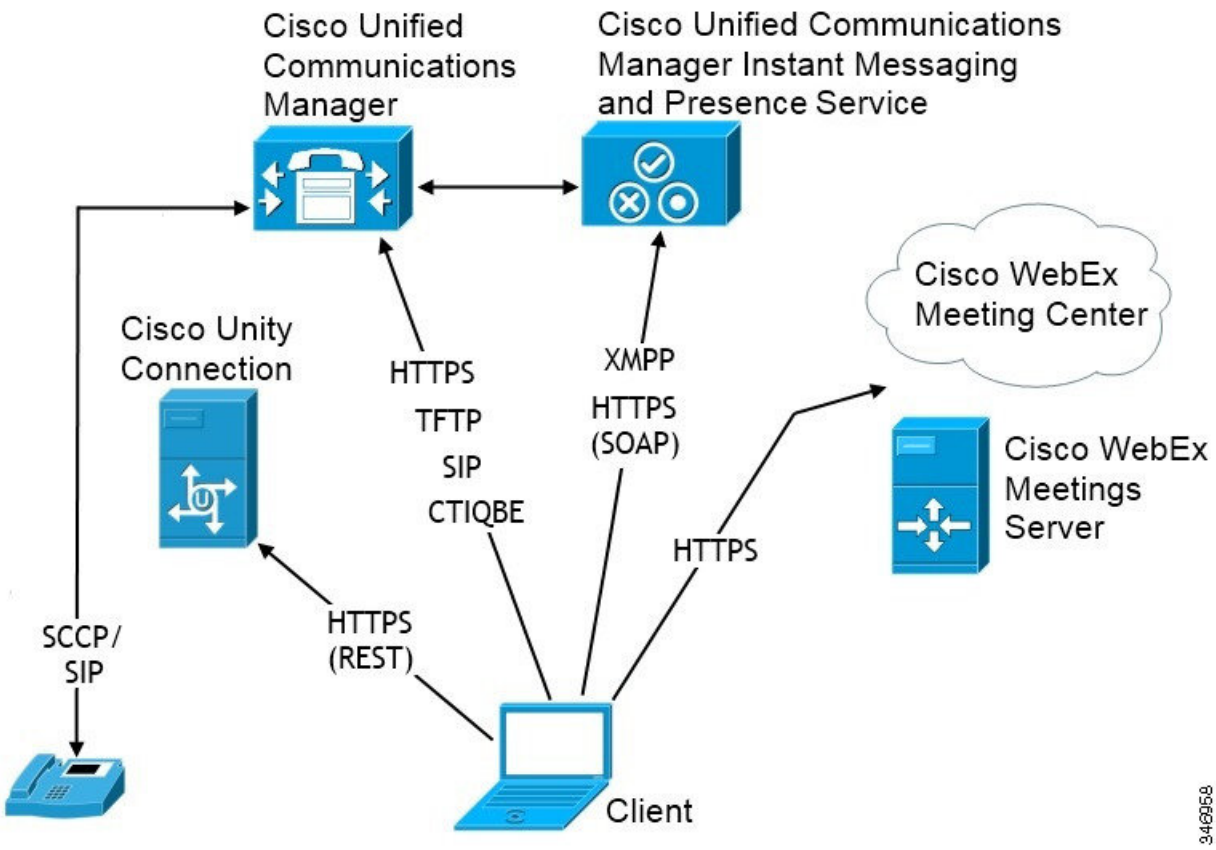
電話モードの展開（連絡先を使用）

連絡先つき電話機モード展開で使用可能なサービスは次のとおりです。

- **連絡先**: Cisco Unified Communications Manager IM and Presence Serviceを通じて連絡先情報を参照できます。
- **プレゼンス**：Cisco Unified Communications Manager IM and Presence Service 経由で対応可否を公開し、他のユーザの対応可否をサブスクライブします。
- **音声コール**：卓上電話機を介して、またはコンピュータで Cisco Unified Communications Manager を介して音声コールを発信します。
- **ビデオ**—Cisco Unified Communications Managerを通じてビデオ通話を発信します。
- **ボイスメール**—Cisco Unity Connectionを通じてボイスメッセージを送受信します。
- **会議**：次のいずれかと統合します。
  - Cisco Webex Meetings センター—ホステッド会議機能を実現します。
  - Cisco Webex Meetings サーバーオンプレミス会議能力を提供します。

次の図は、Cisco Unified Communications Manager IM and Presence Serviceを使った オンプレミス展開のアーキテクチャを示しています。

図 *3:* 電話モードの展開（連絡先を使用）



クラウドベース展開

クラウドベース展開は、Cisco Webexを使ってサービスをホストします。

Cisco Webex メッセンジャーを使ってクラウドとハイブリッドを展開するには、Cisco Webex 管理ツールでクラウドベースの導入を管理および監視します。ユーザのサービスプロファイルを設定する必要はありません。

クラウド展開およびハイブリッド展開の Cisco Webex Platform サービス場合は、Cisco Control Hub を使用して展開を管理および監視します。

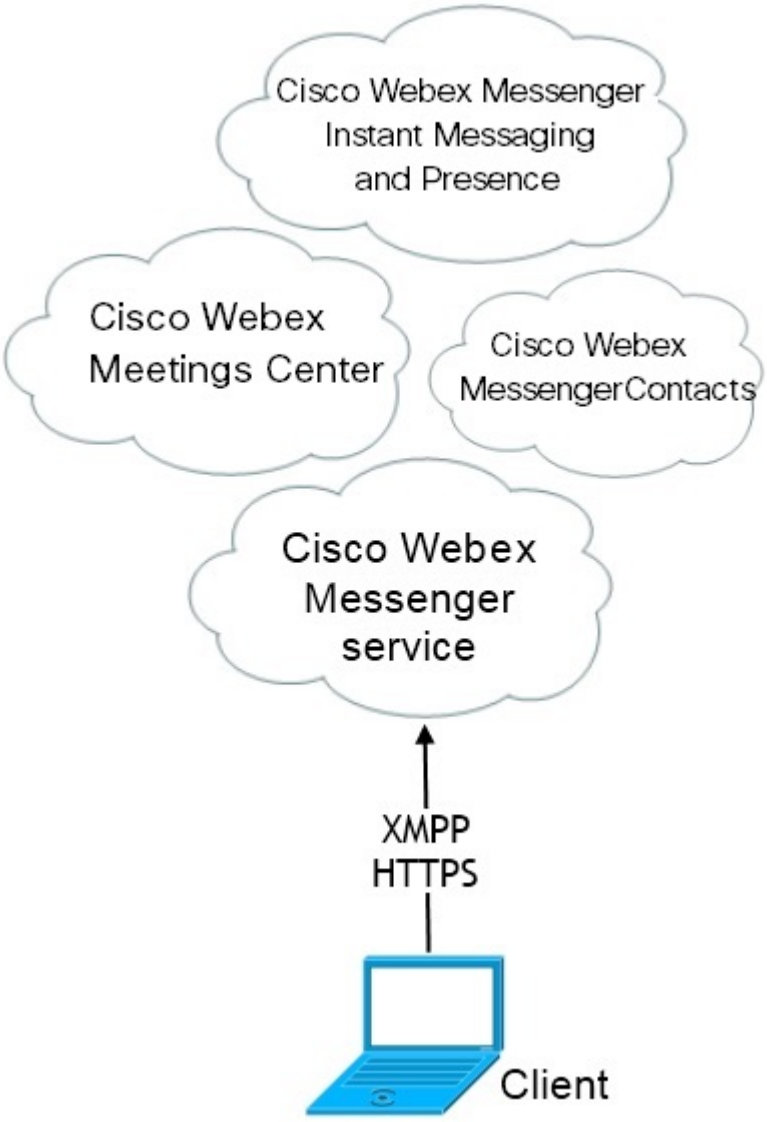
クラウドベース導入での Cisco Webex Messenger サービス。

Webex Messenger を使用したクラウドベースの導入では、次のサービスを利用できます。

- **連絡先ソース**—Cisco Webex Messenger が連絡先の解決を提供します。
- **プレゼンス**—Cisco Webex Messengerによりユーザーは、自分自身のアベイラビリティを表示したり、他のユーザーのアベイラビリティを閲覧したりできます。

- **インスタント メッセージ**—Cisco Webex Messenger ユーザーは、インスタントメッセージを送受信できるようになります。
- **会議**—Cisco Webex Meetings センターは、ホステッド会議機能を提供します。

次の図は、クラウドベース展開のアーキテクチャを示しています。

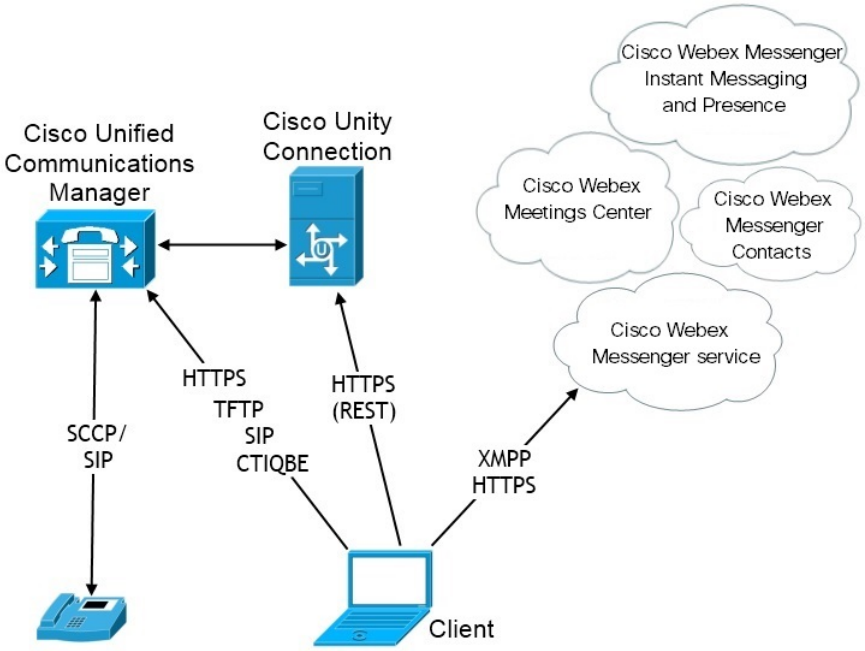


HyDeploymeCisco Webex Messenger Serviceを使ったハイブリッド クラウドベース展開

Webex Messenger サービスを使用したハイブリッド クラウドベースの導入では、次のサービスを利用できます。

- **連絡先ソース**：Cisco Webex Messenger サービスは、連絡先を解決できるようにします。
- **プレゼンス**：Cisco Webex Messenger サービスは、ユーザがアベイラビリティを公開したり、他のユーザのアベイラビリティを登録できるようにします。
- **インスタントメッセージ**：Cisco Webex Messenger サービスは、ユーザがインスタント メッセージを送受信できるようにします。
- **音声**：卓上電話機を介して、またはコンピュータで Cisco Unified Communications Manager を介して音声コールを発信します。
- **ビデオ**—Cisco Unified Communications Managerを通じてビデオ通話を発信します。
- **会議**—Cisco Webex Meetings センターは、ホステッド会議機能を提供します。
- **ボイスメール**—Cisco Unity Connectionを通じてボイスメッセージを送受信します。

次の図は、ハイブリッド クラウドベース展開のアーキテクチャを示しています。



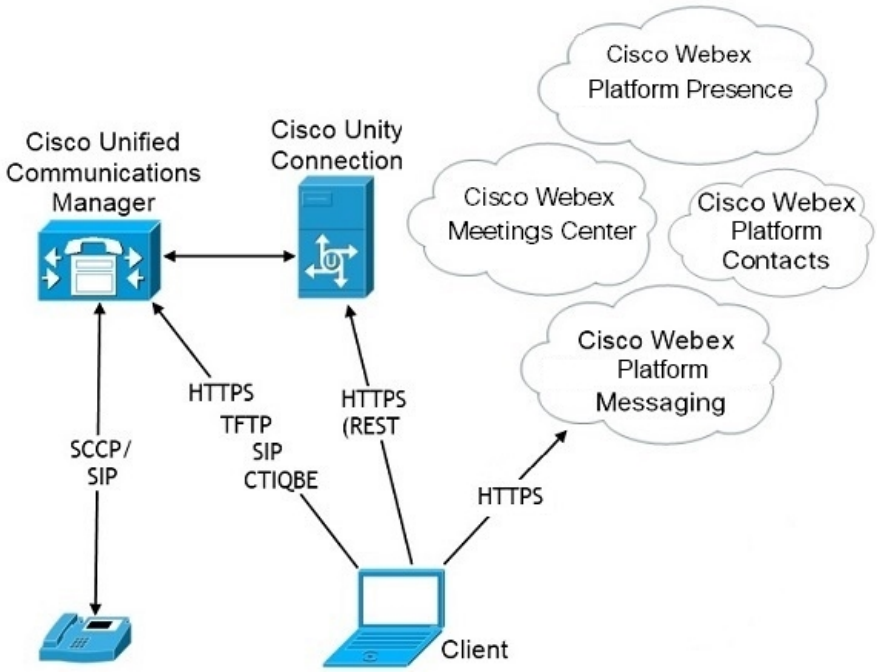
以下のものを使ってハイブリッド クラウドベース展開 Cisco Webex Platform サービス

次の Jabber チームメッセージングモードサービスは、Jabber によるハイブリッドのクラウドベース展開において、 Cisco Webex Platform サービスとともにご利用になれます:

- 連絡先ソース - Cisco Webex Platform サービスが、連絡先を提供します。
- プレゼンス— Cisco Webex Platform サービス によりユーザーは、アベイラビリティを公開したり、他のユーザーのアベイラビリティを閲覧したりできるようになります。

- メッセージング— Cisco Webex Platform サービスによりユーザーは、メッセージの送受信ができるようになります。
- 音声— 卓上電話機またはコンピュータを介して、Cisco UC Managerを使って音声通話を行います。
- ビデオ— Cisco UC Manager を使用してビデオコールを行います。
- 会議— Webex Meeting Center がホスト型ミーティング機能を提供します。
- ボイスメール：Cisco Unity Connection 経由でボイス メッセージを送受信します。

次の図は、 Cisco Webex Platform サービスを使った Jabber のハイブリッド クラウドベース展開のアーキテクチャを示しています。



Jabber チーム メッセージング モードにおける連絡先

サインインフロー

Webex Control Hub でチームメッセージモードを有効にしている間に、ユーザの連絡先を移行する必要があります。

このサインインフローは、ユーザの連絡先を移行するプロセスの概略を示しています。フローは、現在の Jabber の展開にログインしているユーザから開始されます。Jabber チームメッセージモードを有効にして、連絡先を移行します。

1. ユーザは現在の Jabber の展開にログインしており、Cisco UC Manager IM & P または Cisco Webex Messenger に接続しています。

2. 管理者は、Webex Control Hub の設定を変更して、Jabber チームのメッセージモード、オプションで移行、および Jabber のコールを有効にします。
3. 翌日、ユーザは現在の Jabber の展開にログインします。5 分以内に、Jabber はサービス検索プロセスを実行し、そのユーザ向け配置 Cisco Webex Platform サービスが検出されたことを検出します。
4. Jabber は、ユーザが Jabber からメッセージをサインアウトするか、"設定の変更が検出された"かを確認します。
5. ユーザが再度サインインすると、その時点でに認証されます Cisco Webex Platform サービス。
6. 連絡先の移行を有効にした場合、ユーザは Jabber の連絡先を取得するようにメッセージが表示されます。[Ok] をクリックすると、Jabber は連絡先リストのキャッシュを取得して Cisco Webex Platform サービスにアップロードします。ユーザが**キャンセル**を選択すると、Jabber は連絡先リストを移行しません。後で連絡先を検索し、その連絡先を個別に追加できます。

   連絡先移行中は、Jabber は、 Cisco Webex Platform サービスが有効になっている連絡先のみを移行します。Jabber には、 Cisco Webex Platform サービスにカスタム連絡先が保存されないため、それらをユーザの連絡先リストに追加することはできません。
7. Jabber は、 Cisco Webex Platform サービスに接続された後、Cisco UC Manager に接続してサービスプロファイルをダウンロードします。SSO が異なる IdPs で Cisco Webex Platform サービスとUC マネージャーの両方で有効化されている場合、または SSO が 1 つのみで有効化されている場合は、ユーザに資格情報の入力を求めるプロンプトが表示されます。ただし、両方の IdP で SSO がオンになっている場合は、サインインは必要ありません。

Jabber チームメッセージモードの導入に関する考慮事項と連絡先の移行

Cisco Webex Platform サービス組織には、サービスドメインと同じドメインを割り当てる必要があります。これらのドメインが異なるドメインである場合、ユーザは連絡先を移行できません。

仮想環境での展開

仮想環境に Windows 版 Cisco Jabber を展開できます。

仮想環境でサポートされる機能は次のとおりです。

- 他の Cisco Jabber クライアントとのインスタント メッセージングおよびプレゼンス
- デスクフォン制御
- ボイスメール
- Microsoft Outlook 2007、2010、2013 とのプレゼンスの統合
- モバイル & Remote Access（MRA）

仮想環境とローミング プロファイル

仮想環境では、ユーザが常に同じ仮想デスクトップにアクセスするわけではありません。一貫したユーザ エクスペリエンスを保証するために、クライアントが起動されるたびにこれらのファイルにアクセスできる必要があります。Cisco Jabber はユーザーデータを、以下の場所に保存します:

- C:\Users*username*\AppData\Local\Cisco\Unified Communications\Jabber\CSF
  - **連絡先**：連絡先キャッシュ ファイル
  - **履歴**：コールとチャットの履歴
  - **写真キャッシュ**：ディレクトリの画像をローカルにキャッシュ
- C:\Users*username*\AppData\Roaming\Cisco\Unified Communications\Jabber\CSF
  - **コンフィギュレーション**：ユーザ コンフィギュレーション ファイルを保持し、コンフィギュレーション ストア キャッシュを保存
  - **クレデンシャル**：暗号化されたユーザ名とパスワード ファイルを保存

ファイルの暗号化と復号化はWindowsユーザプロファイルにリンクされているため、次のフォルダにアクセスできることを確認してください。

- C:\Users*username*\AppData\Roaming\Microsoft\Crypto
- C:\Users \ *username* \AppData\Roaming\Microsoft\Credentials
- C:\Users*username*\AppData\Local\Microsoft\Crypto
- C:\Users \ *username* \AppData\local\Microsoft\Credentials

（注） 非永続的 Virtual Deployment Infrastructure（VDI）モードで Cisco Jabber を使用している場合、Cisco Jabber クレデンシャル キャッシュはサポートされません。

必要に応じて、ファイルとフォルダを除外リストに追加することによって、それらを同期から除外できます。除外されたフォルダ内のサブフォルダを同期するには、そのサブフォルダを包含リストに追加します。

個人ユーザ設定を保持するには、次を実行する必要があります。

- 次のディレクトリを除外しないでください。
  - AppData\Local\Cisco
  - AppData\Local\JabberWerxCPP
  - AppData\Roaming\Cisco

- AppData\Roaming\JabberWerxCPP

- 次の専用のプロファイル管理ソリューションを使用してください。
  - **Citrix Profile Management**：Citrix 環境向けのプロファイル ソリューションを提供します。仮想デスクトップのホストがランダムに割り当てられる展開では、Citrix Profile Management はインストールされているシステムとユーザ ストア間で各ユーザのプロファイル全体を同期させます。
  - **VMware View Persona Management**：ユーザ プロファイルを保存し、リモート プロファイル リポジトリと動的に同期させます。VMware View Persona Management は Windows ローミング プロファイルを必要としないので、VMware Horizon View ユーザ プロファイルの管理で Windows Active Directory をバイパスできます。Persona Management は、既存のローミング プロファイルの機能を強化します。

VDI 向け Jabber ソフトフォンの展開

コールの発信機能がある仮想環境に Jabber を展開するには、仮想デスクトップインフラストラクチャ用の Jabber ソフトフォンを展開する必要があります。

VDI 用 Jabber ソフトフォンの展開のワークフローは、オンプレミスの環境またはハイブリッド環境で展開している場合に依存するため、アプリケーションがインストールされる前に jabber による展開のワークフローに従い、その時点においては VDI の展開向けJabber のソフトフォン、およびインストールワークフローに従います。

VDI 用 Jabber ソフトフォンのオンプレミスの展開ワークフローを取得するには、*Cisco Jabber* のオンプレミス展開の展開およびインストールワークフローセクションの完全な UC 展開ワークフローを参照してください。

Jabber ソフトフォン向けに VDI のハイブリッド展開ワークフローを取得するには、*Webex Messenger*を使ったハイブリッド展開のワークフロー（クラウド向けワークフローとハイブリッドの展開セクションを参照、Cisco Jabber向けクラウドとハイブリッド展開）をご覧ください。

エンタープライズモビリティ管理の導入

Jabber は、Enterprise Mobility Management (EMM) 展開用に 2 台の SDK ベースクライアントをサポートしています。

- Intune 版 Cisco Jabber
- Cisco Jabber Video for BlackBerry

組織は、これらのクライアントを展開して、Jabber を使用してモバイルデバイスを使用し、「お使いのデバイスを取り込む」ことができるようにポリシーを適用することができます。たとえば、これらのポリシーは次のことを実行できます。

- 安全でない、壊れている、またはルートされているデバイスが使用されないようにします。
- 最小 OS およびアプリバージョンの強制
- ユーザが Jabber でデータをコピーして、別のアプリに貼り付けることを禁止します。

新しいEMMTypeパラメータを使用して、ユーザがログインするための Jabber クライアントを制御します。

メモ　これらのクライアントは、遅延リリースサイクルに従います。クライアントは、Jabber for Android および Jabber for iPhone および iPad の対応するリリース以降にリリースされます。

Intune 版 Jabber を使用した EMM

導入で Intune 版 Jabber クライアントを使用する場合、管理者は Microsoft Azure で管理ポリシーを設定します。ユーザは、アプリストアまたは Google Play ストアから新しいクライアントをダウンロードします。ユーザが新しいクライアントを実行すると、管理者が作成したポリシーを使用して同期が行われます。

注意　Intune 版 Jabber は、iOS プラットフォームで Apple Push Notification (APN) をサポートしていません。Jabber をバックグラウンドに配置する場合、iOS デバイスがチャットメッセージやコールを受信しないことがあります。

（注）　Android デバイスの場合、ユーザは最初に Intune Company Portal をインストールします。次に、ポータルを使用してクライアントを実行します。

Intune 版 Jabber を設定するための一般的なプロセスは次のとおりです。

1. 新しい Azure AD テナントを作成します。
2. 新しい AD ユーザを作成するか、オンプレミスの AD ユーザを同期します。
3. Office 365 グループまたはセキュリティグループを作成し、ユーザを追加します。
4. Intune 版 Jabber クライアントを Microsoft Intune に追加します。
5. Microsoft Intune でポリシーを作成して展開します。
6. ユーザはクライアントにログインして、同期してポリシーを受信します。

この手順の詳細については、Microsoft のマニュアルを参照してください。

次の表は、Cisco Jabber 用のアプリ保護ポリシーでサポートされている Microsoft Intune の制限を示しています。

制約事項	Android	iPhone および iPad
他のアプリにデータを送信する	はい	はい
組織のデータのコピーを保存する	はい	はい
他のアプリへのカット、コピー、貼り付け	はい	はい
スクリーン キャプチャ	対応	該当なし
最大 PIN 試行回数	はい	はい
オフラインの猶予期間	はい	はい
最低要件のアプリ バージョン	はい	はい
脱獄またはルートされるデバイスで使用する	はい	はい
最低要件のデバイスの OS バージョン	はい	はい
最低要件のパッチ バージョン	対応	該当なし
職場 (または学校) のアクセス用アカウント資格情報	はい	はい
アクセス要件を再チェックする	はい	はい

Blackberry 版 Jabber を使用したEMM

導入で BlackBerry 版 Jabber クライアントを使用する場合、管理者は BlackBerry ユニファイド エンドポイントの管理 (UEM) で管理ポリシーを設定します。ユーザは、アプリストアまたは Google Play ストアから新しいクライアントをダウンロードします。Blackberry 版 Jabber は BlackBerry に対応していますが、BlackBerry Marketplace ではまだ入手可能ではありません。

重要 クライアントが BlackBerry を認証中であるため、貴社へのアクセスを許可する必要があります。アクセスを受信するには、お問合せ先 (jabber-mobile-mam@cisco.com) にアクセスして、お客様の BlackBerry UEM サーバからの組織 ID をご提供ください。

新しいクライアントは BlackBerry Dynamics SDK を統合しており、ブラック UEM からポリシーを直接取得することができます。クライアントは、接続とストレージに BlackBerry Dynamics をバイパスします。FIPS 設定は、BlackBerry Dynamics SDK ではサポートされていません。

チャット、音声、およびビデオトラフィックは、BlackBerry インフラストラクチャをバイパスすることになります。クライアントがオンプレミスの場合、すべてのトラフィックに対して Cisco Expressway でのモバイル & Remote Access が必要です。

注意 BlackBerry 版 Jabber は iOS プラットフォームで Apple Push Notification (APN) をサポートしていません。Jabber をバックグラウンドに配置する場合、iOS デバイスがチャットメッセージやコールを受信しないことがあります。

（注） Android での BlackBerry 版 Jabber には Android 6.0 以降が必要です。

iOS での BlackBerry 向け Jabber には iOS 11.0 またはそれ以降が必要です。

BlackBerry Dynamics の場合、管理者は BlackBerry 版 Jabber クライアントの使用を制御するポリシーを設定します。

BlackBerry 版 Jabber を設定するための一般的なプロセスは、次のとおりです。

1. UEM にサーバを作成します。
2. BlackBerry 版 Jabber クライアントを BlackBerry Dynamics に追加します。
3. BlackBerry Dynamics でユーザを作成またはインポートします。

（注） Android ユーザの場合、必要に応じて、BlackBerry Dynamics でアクセスキーを生成できます。

4. UEM にポリシーを作成して導入します。BlackBerry 版 Jabber アプリ設定でのこれらの設定の動作に注意してください。
   - オプションの DLP ポリシーを有効にした場合、BlackBerry は次のものを必要とします。
     - 電子メールの送信に BlackBerry Works を使用します。
     - iOS デバイスの SSO 認証には BlackBerry Access を使用してください。Expressway とユニファイドコミュニケーションマネージャで、iOS 版**ネイティブブラウザの使用**を有効にします。次に、**`ciscojabber`**スキームを BlackBerry UEM で BlackBerry アクセスポリシーに追加します。
   - このリストには、BlackBerry 版 Jabber 導入用のアプリ設定によって設定するのに便利な Jabber パラメータが表示されています。これらのパラメータの詳細については、導入ガイドの *Android*、*iPhone*、*iPad* 版 *Cisco Jabber* の *URL* 設定を参照してください。

フィールド	iOS 対応	Android 対応
Webex Meetings の相互起動の無効化 [1]	はい	はい
サービス ドメイン	はい	はい

フィールド	iOS 対応	Android 対応
音声サービス ドメイン	はい	はい
サービス検出から除外されたサービス	はい	はい
サービス ドメイン SSO 電子メール プロンプト	はい	はい
無効な証明書の動作	はい	はい
テレフォニー有効	はい	はい
URL プロビジョニングの許可	はい	はい
IP モード	はい	はい

[1] Webex Meetings の相互起動を有効にすると、Dynamics 以外のアプリケーションを許可しない BlackBerry Dynamics コンテナで例外として実行できます。

5. ユーザはクライアントにログインします。

この手順の詳細については、BlackBerry のマニュアルを参照してください。

次の表は、Cisco Jabber 用のアプリ保護ポリシーでサポートされている BlackBerry の制限を示しています。

グループ（Group）	機能	Android	iPhone および iPad
ITポリシー	ネットワーク接続なしでデバイスをワイプします	はい	はい
アクティベーション	許可されたバージョン	はい	はい

グループ（Group）	機能	Android	iPhone および iPad
BlackBerry Dynamics	パスワード（Password）	はい	はい
	データ漏洩の防止: BlackBerry Dynamics アプリから BlackBerry Dynamics 以外の アプリにデータをコピーすることはできません	はい	はい
	データ漏洩の防止: BlackBerry Dynamics 以外のアプリから BlackBerry Dynamics アプリにデータをコピーすることはできません	はい	はい
	データ漏洩の防止: Android および Windows 10 デバイスでの画面キャプチャを許可しません	対応	該当なし
	データ漏洩の防止: iOS デバイスで画面の録音と共有を許可しません	該当なし	可
	データ漏洩の防止: iOS デバイスのカスタムキーボードを許可しません	該当なし	可
Enterprise Management Agent のプロファイル	パーソナルアプリコレクションを許可します	はい	はい
コンプライアンス プロファイル	ルート OS または失敗した構成証明	はい	はい
	制限付き OS バージョンがインストールされています	はい	はい
	必要なセキュリティパッチレベルがインストールされていません	対応	該当なし

BlackBerry 版 Jabber の IdP 接続

Android、iPhone および iPad 版 Jabber 導入では、クライアントが DMZ で Id プロバイダー (IdP) プロキシに接続します。次に、プロキシは、内部ファイアウォールの背後にある IdP サーバに要求を渡します。

BlackBerry 版 Jabber では、代替パスを使用できます。BlackBerry UEM の DLP ポリシーを有効にすると、iOS デバイスのクライアントは、安全に IdP サーバに直接トンネルできます。このセットアップを使用するには、導入を次のように設定します。

- Expressway とユニファイド CM で、iOS 版**ネイティブブラウザの使用**を有効にします。
- **Ciscojabber**スキームを blackberry Uem の blackberry アクセスポリシーに追加します。

Android OS 上のBlackBerry 版 Jabber は、SSO のために常に IdP プロキシに接続します。

導入環境に、iOS で動作しているデバイスのみが含まれている場合、DMZ では IdP プロキシは必要ありません。ただし、Android OS 上で動作するデバイスが導入環境に含まれている場合は、IdP プロキシが必要です。

iOS のアプリ転送セキュリティ

iOS には、アプリ転送セキュリティ(ATS)機能が含まれています。ATS では、Jabber for BlackBerry および Jabber for Intune により、信頼できる証明書と暗号化を使用して TLS を介したセキュアなネットワーク接続を実現する必要があります。ATS は、X.509 デジタル証明書を持たないサーバへの接続をブロックします。証明書は次のチェックを通過する必要があります。

- 変更が加えられていないデジタル署名
- 有効な有効期限日
- サーバの DNS 名と一致する名前
- CA からの信頼できるアンカー証明書への有効な証明書のチェーン

（注） iOS の一部である信頼されたアンカー証明書の詳細については、*iOS* で使用可能な信頼されたルート証明書のリスト (https://support.apple.com/en-us/HT204132) を参照してください。システム管理者またはユーザは、同じ要件を満たしている限り、独自の信頼できるアンカー証明書をインストールできます。

ATS の詳細については、セキュアでないネットワーク接続の防止 (https://developer.apple.com/documentation/security/preventing_insecure_network_connections) を参照してください。

Remote Access

ユーザが企業ネットワークの外部の場所から作業にアクセスしなければならないことがあります。Remote Access 用のいずれかのシスコ製品を使用して、ユーザが作業にアクセスできるようにします。

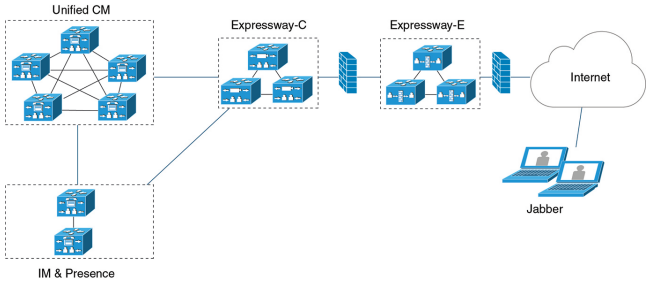
Jabber は、サードパーティ VPN クライアントではテストも検証もされません。

Expressway Mobile and Remote Access

Cisco Unified Communications Manager 用の Expressway for Mobile and Remote Access を使用すると、ユーザは仮想プライベートネットワーク（VPN）を使用しなくても、企業のファイアウォールの外側からコラボレーション ツールにアクセスできます。シスコのコラボレーション ゲートウェイを使用して、クライアントは公衆 Wi-Fi ネットワークやモバイル データ ネットワークなどのリモート ロケーションから社内ネットワークに安全に接続できます。

図 *4 :* クライアントが、*Expressway for Mobile and Remote Access* に接続する方法

次の図は、Expressway for Mobile and Remote Access 環境のアーキテクチャを図示したものです。



Expressway for Mobile and Remote Access を使用した Jabber への初回サインイン

モバイル クライアント向け Cisco Jabber に適用されます。

ユーザは最初に Expressway for Mobile and Remote Access を使用してクライアントにサインインすると、企業のファイアウォールの外からサービスに接続できます。ただし、次の場合は最初に社内ネットワーク内でサインインします。

- 音声サービス ドメインが他のサービス ドメインと異なる場合、ユーザは社内ネットワーク内から `jabber-config.xml` ファイルの適切な音声サービス ドメインを取得する必要があります。ハイブリッド導入の場合、管理者はVoiceServicesDomainパラメータを設定することができます。*Cisco Jabber* のパラメータリファレンスガイドの最新版を参照してください。この場合、ユーザは社内ネットワーク内でサインインする必要はありません。
- Cisco Jabber が CAPF 登録プロセス（セキュア モードまたは混合モードのクラスタを使用する場合に必要）を完了する必要がある場合。

ユーザが Expressway for Mobile and Remote Access 環境でセキュアな電話機を使用している場合、最初のサインインはサポートされません。設定が暗号化された TFTP を含むセキュア プロファイルの場合、最初にオンプレミス内でサインインし、CAPF 登録を可能にする必要があります。Cisco Unified Communications Manager、Expressway for Mobile and Remote Access、および Cisco Jabber の各拡張機能を使用しないと、パブリック ネットワークで最初にサインインすることはできません。ただし、次の項目がサポートされます。

- 暗号化された TFTP（オンプレミスで最初にサインイン）。
- 暗号化されていない TFTP（Expressway for Mobile and Remote Access またはオンプレミスで最初にサインイン）。

サポートされるサービス

次の表に、クライアントが Expressway for Mobile and Remote Access を使用してリモートで Cisco Unified Communications Manager に接続した場合にサポートされるサービスと機能の概要を示します。

表 *1 : Expressway for Mobile and Remote Access* でサポートされるサービスの概要

サービス	サポート対象	非サポート対象
ディレクトリ		
UDS ディレクトリ検索	X	
LDAP ディレクトリ検索		X
ディレクトリ写真解決	X * Cisco Expressway-C 上で HTTP ホワイト リストを使用	
ドメイン内フェデレーション	X * 連絡先検索のサポートは連絡先 ID の形式に依存します。詳細については、以下の注記を参照してください。	
ドメイン間フェデレーション	X	
インスタント メッセージおよびプレゼンス		
オンプレミス	X	
クラウド	X	
チャット	X	
グループ チャット	X	
永続的なチャット	X	
ハイ アベイラビリティ：オンプレミス展開	X	
ファイル転送：オンプレミス展開	X Cisco Unified Communications Manager IM and Presence Service 10.5(2) 以降を使用したファイル転送に使用可能な高度なオプション、後述の注意を参照してください。	

サービス	サポート対象	非サポート対象
ファイル転送：クラウド展開	X	
ビデオ画面共有：BFCP	X（モバイル クライアント向け Cisco Jabber は BFCP 受信のみをサポートします）。	
IM 専用画面の共有		X
オーディオとビデオ		
音声コールとビデオ コール	X * Cisco Unified Communications Manager 9.1(2) 以降	
デスクフォン制御モード（CTI）（デスクトップ クライアントのみ）		X
Extend and connect（デスクトップ クライアントのみ）		X
リモート デスクトップ制御（デスクトップ クライアントのみ）		X
サイレント モニタリングおよびコール録音		X
Dial via Office - リバース（モバイル クライアントのみ）	X	
セッションの永続性		X
アーリー メディア		X
セルフケア ポータル アクセス		X
グレースフル登録	X * Android 版 Cisco Jabber に適用されます。 Jabber for Android は、Expressway for Mobile および Cisco Unified Communications Manager リリース 10.5.(2) 10000-1 の Remote Access に対するグレースフル登録をサポートします。	

サービス	サポート対象	非サポート対象
共有回線	X 前提条件： • Cisco Expressway 8.9.1 以降 • Cisco Unified Communications Manager を 11.5 SU(2) 以降にアップグレード	
ボイスメール		
ビジュアル ボイスメール	X * Cisco Expressway-C 上で HTTP ホワイト リストを使用	
Cisco Webex Meetings		
オンプレミス		X * Jabber 11.6 転送からのオンプレミスの Cisco Webex Meeting Server を除き、サポートされていません。
クラウド	X	
Cisco Webex 画面共有（デスクトップ クライアントのみ）	X	
インストール（デスクトップ クライアント）		
インストーラ更新	X * Cisco Expressway-C 上で HTTP ホワイト リストを使用	X Mac 版 Cisco Jabber ではサポートされない
カスタマイズ		
カスタム HTML タブ		X

サービス	サポート対象	非サポート対象
Enhanced911 プロンプト	X * 企業ネットワークの外部で稼働するすべての Jabber クライアントで Web ページが正しく表示されるようにするには、スクリプトおよびリンク タグが E911NotificationURL パラメータでサポートされていないため、Web ページに静的な HTML ページを指定する必要があります。詳細については、『*Parameter Reference Guide for Cisco Jabber*』の最新版を参照してください。	
セキュリティ		
メディア向け ICE プロトコル	X	
CAPF 登録		X
シングル サインオン	X	
Advanced Encryption Standard（AES）256 および TLS1.2	X * Android 版 Cisco Jabber に適用されます。 Advanced Encryption Standard は社内 Wi-Fi でのみサポートされます	
トラブルシューティング（デスクトップ クライアントのみ）		
問題レポートの生成	X	
問題レポートのアップロード		X
ハイ アベイラビリティ（フェールオーバー）		
音声およびビデオ サービス		X
ボイスメール サービス		X
IM and Presence サービス	X	
連絡先の検索	X	
連絡先の解決	X	

サービス	サポート対象	非サポート対象
構成管理		
高速サインイン	X	
認証および承認		
SSO Jabber ユーザ用の O-Auth サポート	X	

ディレクトリ

クライアントが Expressway for Mobile and Remote Access を使用してサービスに接続した場合は、次の制限付きでディレクトリ統合がサポートされます。

- LDAP を使用した連絡先解決：企業ファイアウォールの外側のクライアントは連絡先解決に LDAP を使用することができません。代わりに、連絡先解決に UDS を使用する必要があります。

  ユーザが企業ファイアウォールの内側にいる場合は、クライアントは連絡先解決に UDS と LDAP のいずれかを使用できます。企業ファイアウォールの内側に LDAP を展開する場合は、LDAP ディレクトリ サーバを Cisco Unified Communications Manager と同期させ、ユーザが企業ファイアウォールの外側にいるときにクライアントを UDS に接続できるようにすることをお勧めします。

- ディレクトリ写真解決：クライアントが連絡先写真を確実にダウンロードできるようにするには、Cisco Expressway-C サーバのホワイト リストに、連絡先写真をホストするサーバを追加する必要があります。Cisco Expressway-C ホワイト リストにサーバを追加するには、[HTTPサーバ許可（HTTP server allow）] 設定を使用します。詳細については、関連する Cisco Expressway のマニュアルを参照してください。

- ドメイン内フェデレーション：ドメイン内フェデレーションを展開して、クライアントがファイアウォールの外側から Expressway for Mobile and Remote Access に接続した場合は、連絡先 ID に次の形式のいずれかが使用されている場合にのみ連絡先検索がサポートされます。

  - sAMAccountName@domain
  - UserPrincipleName(UPN)@domain
  - EmailAddress@domain
  - employeeNumber@domain
  - telephoneNumber@domain

- XMPP を使用するドメイン間フェデレーション：Expressway for Mobile and Remote Access は、XMPP ドメイン間フェデレーション自体を有効にするものではありません。Expressway for Mobile and Remote Access 経由で接続された Cisco Jabber クライアントでは、Cisco Unified Communications Manager IM and Presence で有効になっている XMPP ドメイン間フェデレーションを使用できます。

インスタント メッセージおよびプレゼンス

クライアントが Expressway for Mobile and Remote Access を使用してサービスに接続した場合は、次の制限付きでインスタント メッセージングとプレゼンスがサポートされます。

デスクトップおよびモバイル クライアントのファイル転送には次の制限があります。

- Cisco Webexクラウド展開では、ファイル転送がサポートされます。
- Cisco Unified Communication IM and Presence サービス 10.5(2) 以降を使用したオンプレミス展開では、[マネージドファイル転送（Managed File Transfer）] オプションはサポートされますが、[ピアツーピア（Peer-to-Peer）] オプションはサポートされません。
- Cisco Unified Communications Manager IM and Presence Service 10.0(1) 以前を使用したオンプレミス展開では、ファイル転送がサポートされません。
- 無制限の Cisco Unified Communications Manager IM およびプレゼンスサーバを使用したモバイルおよびRemote Accessの展開の場合、管理ファイル転送はサポートされていません。

音声コールとビデオ コール

クライアントが Expressway for Mobile and Remote Access を使用してサービスに接続した場合は、次の制限付きで音声およびビデオ通話がサポートされます。

- Cisco Unified Communications Manager：Expressway for Mobile and Remote Access は、Cisco Unified Communications Manager バージョン 9.1.2 以降でビデオおよび音声通話をサポートします。
- デスクフォン制御モード（CTI）（デスクトップ クライアントのみ）：クライアントは、エクステンション モビリティを含むデスクフォン制御モード（CTI）をサポートしません。
- Extend and connect（デスクトップ クライアントのみ）：クライアントを以下の目的に使用することはできません。
  - オフィスの Cisco IP 電話 でコールを発信および受信する。
  - 自宅電話、ホテルの電話、またはオフィスのCisco IP電話 で、保留と復帰などの通話中制御を実行する。
- セッション永続性：クライアントが使用するネットワークが切り替わると、音声コールおよびビデオ コールが切断され、復帰できません。たとえば、ユーザがオフィス内で Cisco Jabber コールを開始してから、建物を出て Wi-Fi 接続が切断されると、クライアントが Expressway for Mobile and Remote Access を使用するように切り替わるため、コールが切断されます。
- アーリー メディア：アーリー メディアを使用すれば、クライアントは、接続が確立される前にエンドポイント間でデータを交換できます。たとえば、ユーザが同じ組織に属さない通話者にコールを発信し、相手側がこれを拒否したまたはコールに応答しなかった場合、アーリーメディアによってユーザがビジー トーンを受け取るか、ボイスメールがユーザに送信されます。

Expressway for Mobile and Remote Access を使用している場合は、電話の相手がコールを拒否するか、応答しないと、ビジー トーンが鳴りません。代わりに、ユーザは、コールが終了するまで約 1 分無音を受信します。

- セルフ ケア ポータル アクセス（デスクトップ クライアントのみ）：ユーザは、ファイアウォールの外側にいるときに Cisco Unified Communications Manager のセルフ ケア ポータルにアクセスできません。外部から Cisco Unified Communications Manager のユーザ ページにアクセスできません。

  Cisco Expressway-E は、ファイアウォールの内側のクライアントとユニファイド コミュニケーション サービス間のすべての通信をプロキシします。ただし、Cisco Expressway-E は Cisco Jabber アプリケーションではないブラウザからアクセスされるサービスをプロキシしません。

[ボイスメール（Voicemail）]

ボイスメール サービスは、クライアントが Expressway for Mobile and Remote Access を使用してサービスに接続した場合にサポートされます。

（注） クライアントがボイスメール サービスに確実にアクセスできるようにするには、Cisco Expressway-C サーバのホワイト リストにボイスメール サーバを追加する必要があります。Cisco Expressway-C ホワイト リストにサーバを追加するには、[HTTPサーバ許可（HTTP server allow）] 設定を使用します。詳細については、関連する Cisco Expressway のマニュアルを参照してください。

インストール

Mac 版 Cisco Jabber：クライアントが Expressway for Mobile and Remote Access を使用してサービスに接続した場合は、インストーラ更新がサポートされません。

Windows 版 Cisco Jabber：クライアントが Expressway for Mobile and Remote Access を使用してサービスに接続した場合は、インストーラ更新がサポートされます。

（注） クライアントがインストーラ更新を確実にダウンロードできるようにするには、Cisco Expressway-C サーバのホワイト リストにインストーラ更新をホストするサーバを追加する必要があります。Cisco Expressway-C ホワイト リストにサーバを追加するには、[HTTPサーバ許可（HTTP server allow）] 設定を使用します。詳細については、関連する Cisco Expressway のマニュアルを参照してください。

セキュリティ

クライアントが Expressway for Mobile and Remote Access を使用してサービスに接続した場合は、次の制限付きでほとんどのセキュリティ機能がサポートされます。

- 初期 CAPF 登録：Certificate Authority Proxy Function（CAPF）登録は、Cisco Jabber（または他のクライアント）に証明書を発行する Cisco Unified Communications Manager Publisher 上で動作するセキュリティ サービスです。正常に CAPF を登録するために、クライアントはファイアウォールの内側から接続するか VPN 接続を使用する必要があります。
- エンドツーエンド暗号化：ユーザが Expressway for Mobile and Remote Access 経由で接続し、コールに参加する場合：
  - Cisco Expressway-C と Cisco Unified Communications Manager に Expressway for Mobile and Remote Access を使用して登録されたデバイスとの間のコール パスで、メディアは常に暗号化されます。
  - Cisco Jabber または内部デバイスが暗号化セキュリティ モードに設定されていない場合は、メディアは Cisco Expressway-C と、Cisco Unified Communications Manager にローカルに登録されたデバイスの間のコール パス上で暗号化されません。
  - Cisco Jabber と内部デバイスの両方が暗号化セキュリティ モードに設定されている場合は、メディアが Expressway-C と、Cisco Unified Communnication Manager にローカルに登録されたデバイス間のコール パス上で暗号化されます。
  - Cisco Jabber クライアントが常に Expressway for Mobile and Remote Access を通じて接続されている場合は、エンドツーエンド暗号化を実現するための CAPF 登録は不要です。ただし、Cisco Jabber デバイスは引き続き暗号化セキュリティ モードで設定し、Cisco Unified Communications Manager が混合モードをサポートできるようにする必要があります。
  - 社内ネットワークの外部では、Jabber で送信されたメディアを暗号化するように、パブリッシング Sway-C または社内 Sway-E サーバ上で ICE パススルーサポートを設定することができます。セットアップの詳細については、*Cisco Expressway*を通じたモバイル および *Remote Access*向け展開ガイドを参照してください。

トラブルシューティング

Windows 版 Cisco Jabber のみ。問題レポート アップロード：デスクトップ クライアントが Expressway for Mobile and Remote Access を使用してサービスに接続した場合は、問題レポートが HTTPS 経由で指定された内部サーバにアップロードされるため、問題レポートを送信できません。

この問題を回避するには、ユーザはレポートをローカルに保存し、別の方法でレポートを送信できます。

ハイ アベイラビリティ（フェールオーバー）

ハイ アベイラビリティとは、クライアントがプライマリ サーバに接続できない場合に、サービスをほとんどまたは全く中断させることなく、セカンダリ サーバにフェールオーバーすることを意味します。Expressway for Mobile and Remote Access 上でサポートされるハイ アベイラビリティの場合は、特定のサービスをセカンダリ サーバ（Instant Messaging and Presence など）にフェールオーバーするサーバを意味します。

ハイ アベイラビリティについてサポートされない一部のサービスが Expressway for Mobile and Remote Access 上で使用できます。これは、ユーザが社内ネットワークの外部からクライアントに接続している場合に、Instant Messaging and Presence サーバがフェールオーバーしても、サービスが通常どおり提供されることを意味します。ただし、音声およびビデオサーバまたはボイスメール サーバがフェールオーバーした場合は、関連するサーバがハイ アベイラビリティをサポートしないため、それらのサービスは提供されません。

Cisco AnyConnect の展開

Cisco AnyConnect は、クライアントが Wi-Fi ネットワークやモバイル データ ネットワークなどのリモートの場所から社内ネットワークに安全に接続できるようにするサーバ/クライアント インフラストラクチャを意味します。

Cisco AnyConnect 環境は、次のコンポーネントで構成されます。

- Cisco 適応型セキュリティ アプライアンス：リモート アクセスを保護するためのサービスを提供します。
- Cisco AnyConnect セキュア モビリティ クライアント：ユーザのデバイスから Cisco 適応型セキュリティ アプライアンスへのセキュアな接続を確立します。

このセクションでは、Cisco AnyConnect セキュア モビリティ クライアントを使用して Cisco 適応型セキュリティ アプライアンス（ASA）を展開する場合に考慮すべき情報を提供します。Cisco AnyConnect は、Android 版 Cisco Jabber と iPhone および iPad 版 Cisco Jabber 用にサポートされている VPN です。サポートされていない VPN クライアントを使用している場合は、該当するサード パーティのマニュアルを使用して VPN クライアントがインストールされ、設定されていることを確認します。

Android OS 4.4.x を実行している Samsung デバイスの場合は、Samsung AnyConnect のバージョン 4.0.01128 以降を使用します。Android OS バージョン 5.0 以降の場合は、ソフトウェア バージョンが 4.0.01287 以降の Cisco AnyConnect を使用する必要があります。

Cisco AnyConnect は、Cisco 5500 シリーズ ASA へのセキュアな IPsec（IKEv2）または SSL VPN 接続をリモート ユーザに提供します。また、Cisco AnyConnect は、ASA からまたは社内ソフトウェア展開システムを使用してリモートユーザに展開できます。ASA から展開する場合は、リモートユーザが、クライアントレス SSL VPN 接続を許可するように設定された ASA のブラウザで IP アドレスまたは DNS 名を入力することによって、ASA への初期 SSL 接続を確立します。その後で、ASA が、ブラウザ ウィンドウにログイン画面を表示し、ユーザがログインと認証を満たした場合に、コンピュータのオペレーティング システムにマッチするクライアントをダウンロードします。ダウンロード後、クライアントは自動的にインストールおよび設定され、ASA への IPsec（IKEv2）接続または SSL 接続が確立されます。

Cisco 適応型セキュリティ アプライアンスと Cisco AnyConnect セキュア モビリティ クライアントの要件については、「ソフトウェア要件」のトピックを参照してください。

関連トピック

Cisco ASA シリーズ ドキュメント一覧
Cisco AnyConnect Secure Mobility Client

シングル サインオンを使用した展開

Security Assertion Markup Language（SAML）シングル サインオン（SSO）を使用したサービスを有効にすることができます。SAML SSOは、オンプレミス、クラウド、ハイブリッド展開で使用できます。

次の手順は、ユーザがCisco Jabberクライアントを起動したあとのSAML SSOのサインイン フローを示しています。

1. ユーザがCisco Jabberクライアントを起動します。Webフォームによるサインインをユーザに要求するようにアイデンティティ プロバイダー（IdP）を設定した場合は、クライアント内にそのフォームが表示されます。
2. Cisco Jabberクライアントは、Cisco Webex Messengerサービス、Cisco Unified Communications Manager、またはCisco Unity Connectionに接続されているサービスに対して認証要求を送信します。
3. サービスがIdPに認証を要求するためにクライアントをリダイレクトします。
4. IdPがクレデンシャルを要求します。クレデンシャルは、次のいずれかの方法で指定できます。
   - ユーザ名とパスワードのフィールドがあるフォーム ベースの認証。
   - 統合 Windows 認証（IWA）用 Kerberos（Windows のみ）
   - スマート カード認証（Windows のみ）
   - HTTP 要求時にクライアントがユーザ名とパスワードを提示する、基本的な HTTP 認証方式。
5. IdPがブラウザまたはその他の認証方式にCookieを提供します。IdPがSAMLを使用してIDを認証すると、サービスはクライアントにトークンを提供できます。
6. クライアントが認証用のトークンを使用してサービスにログインします。

認証方式

認証メカニズムはユーザのサインオン方法に影響します。たとえば、Kerberosを使用する場合、クライアントはユーザにクレデンシャルを要求しません。ユーザがすでに認証を提示して、デスクトップへのアクセス権を取得しているからです。

ユーザ セッション

ユーザがセッションにサインインします。セッションからユーザにCisco Jabberサービスを使用する事前定義の時間が提示されます。セッションの継続時間を制御するには、Cookieとトークンのタイムアウト パラメータを設定します。

IdP timeoutパラメータを適切な時間に設定して、ユーザがログインを要求されないようにします。たとえばJabberユーザが外部Wi-Fiへ切り替える場合にはローミング状態になり、そのユーザのラップトップは休止するか、ユーザがアクティブではないためにスリープ状態になります。IdPセッションがまだアクティブであれば、接続を再開した後にユーザがログインする必要はありません。

セッションの有効期限が切れてJabberがサイレント更新できない場合、ユーザ入力が必要となるため、ユーザに再認証が要求されます。この現象は、認証 Cookie が有効でなくなった時点で発生する可能性があります。

Kerberos またはスマート カードが使用されている場合は、スマート カードから PIN が要求されなければ、再認証の操作をする必要はありません。ボイスメール、着信コール、インスタント メッセージングなどのサービスが中断するリスクはありません。

シングル サインオンの要件

SAML 2.0

Cisco Unified Communications Manager サービスを使用する Cisco Jabber クライアントに対してシングル サインオン（SSO）を有効にするには、SAML 2.0 を使用します。SAML 2.0 は SAML 1.1 と互換性がありません。SAML 2.0 標準を使用する IdP を選択します。サポートされている ID プロバイダーは SAML 2.0 に準拠しているため、それらを SSO の実装に使用できます。

サポートされるアイデンティティ プロバイダー

IdP は、Security Assertion Markup Language（SAML）に準拠している必要があります。クライアントは次のアイデンティティ プロバイダーをサポートします。

- Ping Federate 6.10.0.4
- Microsoft Active Directory Federation Services (ADFS) 2.0
- Open Access Manager (OpenAM) 10.1

（注） OpenAM で使用する Globally Persistent Cookie が設定されていることを確認します。

IdP を設定すると、その設定がクライアントへのサインイン方法に影響します。Cookie のタイプ（永続的またはセッション）や認証メカニズム（Kerberos または Web フォーム）などのパラメータによって、ユーザの認証頻度が決定されます。

クッキー

ブラウザでの Cookie 共有を有効にするには、セッション Cookie ではなく、永続的な Cookie を使用します。永続的な Cookie は、ユーザに Internet Explorer を使用しているクライアントまたはその他のデスクトップ アプリケーションで 1 回クレデンシャルを入力するように要求します。セッション Cookie の場合は、ユーザがクライアントを起動するたびにクレデンシャルを入力する必要があります。IdP 上の設定として永続的な Cookie を設定します。Open Access Manager を IdP として使用している場合は、（Realm Specific Persistent Cookie ではなく）Globally Persistent Cookie を設定します。

ユーザが SSO クレデンシャルを使い iPhone および iPad 版 Cisco Jabber へのサインインに成功すると、クッキーはデフォルトで iOS のキーチェーンに保存されます。クッキーが iOS のキー

チェーンにあれば、サインインの最中にクッキーの期限が切れない限り、ユーザは次回以降サインインのクレデンシャルを入力する必要がありません。クッキーは、以下の状況でiOSキーチェーンから自動的に削除されます。

- Cisco Jabber から手動でサインアウトした場合。
- Cisco Jabber がリセットされた場合。
- iOS デバイスをリブートした後
- Cisco Jabber が手動でクローズされた場合。

（注） 埋め込み Safari ブラウザを使用している場合、Jabber は Safari が制御する Cookie を制御することはできません。Jabber ではこれらの Cookie をクリアできないため、Jabber ではこの場合に SSO トークンのみをクリアできます。Safari でユーザの資格情報が永続的な Cookie に存在する場合、Jabber が SSO トークンをクリアした際に、Cookie によりそのユーザは資格情報の再入力を回避できます。

iOS システムがバックグラウンドで実行中の iPhone および iPad 版 Cisco Jabber を停止した場合は、Jabber はユーザがパスワード入力せずに自動的にサインインできるようにします。

必要なブラウザ

ブラウザとクライアント間で認証 Cookie（IdP から発行された）を共有するには、次のブラウザのいずれかをデフォルト ブラウザに指定します。

製品	必要なブラウザ
Windows 版 Cisco Jabber	Internet Explorer[InternetExplorer]
Mac 版 Cisco Jabber	Safari
iPhone および iPad 版 Cisco Jabber	Safari
Android 版 Cisco Jabber	Chrome または Internet Explorer

（注） Android 版 Cisco Jabber で SSO を使用する場合、組み込みブラウザは外部ブラウザと Cookie を共有できません。

シングル サインオンと Remote Access

Expressway Mobile and Remote Access を使用して企業ファイアウォールの外側からクレデンシャルを入力するユーザの場合は、シングル サインオンに次の制限があります。

- シングル サインオン（SSO）は、Cisco Expressway 8.5 と Cisco Unified Communications Manager リリース 10.5.2 以降で使用できます。両方において SSO を有効または無効にする必要があります。
- セキュアな電話機の Expressway for Mobile and Remote Access を介して SSO を使用することはできません。
- 使用するアイデンティティ プロバイダーは内部 URL と外部 URL を同じにする必要があります。URL が異なる場合は、ユーザが企業ファイアウォールの内側と外側の間で移動するときに再度サインインするように要求されることがあります。