アプリケーション

Conference Factory の設定

「Conference Factory」ページ（**[アプリケーション（Applications）] > [Conference Factory]**）では、Conference Factory アプリケーションを有効化または無効化することができ、使用するエイリアスとテンプレートを設定できます。

Conference Factory アプリケーションを使用して、Expressway は Multiway 対応のエンドポイントと会議ブリッジに従って Multiway 機能をサポートします（『Cisco TelePresence Multiway 導入ガイド』を参照してください）。Multiway は、エンドポイントにこの機能が組み込まれていない場合でも、コール中にエンドポイントのユーザが会議を作成できます。

Multiway をサポートするシスコのエンドポイントとインフラストラクチャ製品の最新のリストについては、シスコの担当者にお問い合わせください。

会議の作成プロセス

Multiway 機能をエンドポイントからアクティブ化すると、次のプロセスが行われます。

1. エンドポイントが Expressway 上の Conference Factory にルーティングするように事前に設定されたエイリアスをコールします。
2. Expressway はエンドポイントが Multiway 会議に使用する必要があるエイリアスでエンドポイントに応答します。このエイリアスは MCU にルーティングします。
3. 次に、エンドポイントは指定されたエイリアスを使用して MCU をコールし、他の参加エンドポイントに同じことを実行するように通知します。

設定可能なオプションは次のとおりです。

フィールド	説明（**Description**）	使用方法のヒント
モード（**Mode**）	Conference Factory アプリケーションを有効または無効にします。	
エイリアス（**Alias**）	Multiway機能がアクティブになったときにエンドポイントがダイヤルするエイリアス。これも、Multiway機能の開始に使用できるすべてのエンドポイントに設定する必要があります。例：**multiway@example.com**	
テンプレート(**Template**)	Multiway会議をMCUに作成するためにダイヤルするよう Expressway がエンドポイントに通知するエイリアス。	会議ごとに異なるエイリアスを指定するには、テンプレートの一部として **%%** を使用する必要があります。%% は、Expressway が新しい会議要求を受信するたびに一意の番号によって置換されます。
番号範囲の開始/終了（**Number range start/end**）	会議エイリアスの生成に使用するテンプレートの **%%** を置換する範囲の最初と最後の数値。	たとえば、**テンプレート** 10～999 の歯にの**563%%@example.com**です。最初の会議はエイリアス**563010@example.com**を使用し、次の会議は**563011@example.com**を使用して**563999@example.com**まで続きます。その後、ループして**563010@example.com**から再開します。 （**注**） %% は、範囲の上限値の長さに基づき一定の桁数を表し、必要に応じて先行ゼロが付きます。

（注）

- Conference Factory アプリケーションが有効になっているネットワーク内の VCS のそれぞれで異なる**テンプレート**を使用する必要があります。Expressway がクラスタの一部である場合、クラスタ内のピアごとに異なるテンプレートを使用する必要があります。
- テンプレートが生成するエイリアスは完全修飾 SIP であり、MCU にルーティングする必要があります。MCU はこのエイリアスを処理するように設定する必要があります。MCU では、Conference Factory アプリケーションをサポートするためのその他の特別な設定は必要ありません。
- **[SIP モード（SIP mode）]** を *[オン（On）]*（**[設定（Configuration）]** > **[プロトコル（Protocols）]** > **[SIP]**）に設定する必要があります。H.323 エンドポイントから Conference Factory へのコールを発信するには、**[H.323 モード（H.323 mode）]** も *[オン（On）]*にし（**[設定（Configuration）]** > **[プロトコル（Protocols）]** > **[H.323]**）、**[H.323 <-> SIP 間のインターワーキングモード（H.323 <-> SIP interworking mode）]** が *[登録済みのみ（Registered only）]* または *[オン（On）]* に設定されていることを確認します（**[設定（Configuration）]**>**[プロトコル（Protocols）]**>**[インターワーキング（Interworking）]**）。

Multiway を導入環境で使用するようにネットワークの個々のコンポーネント（エンドポイント、MCU、および Expressway）を設定する方法の詳細については、『Cisco TelePresence Multiway 導入ガイド』を参照してください。

プレゼンスについて

プレゼンスは、エンドポイントの現在のステータス（オフラインか、オンラインか、コール中かなど）について他のユーザに情報を提供するためのエンドポイントの機能です。プレゼンス情報を提供するエンティティやプレゼンス情報を要求できるエンティティをプレゼンティティと呼びます。プレゼンティティは、それ自体のプレゼンス ステータスに関する情報をパブリッシュするとともに、他のプレゼンティティや FindMe ユーザがパブリッシュしている情報をサブスクライブします。

Jabber Video などのプレゼンスをサポートするエンドポイントは、独自のステータス情報をパブリッシュできます。また、Expressway は、H.323 エンドポイントなどプレゼンスをサポートしないエンドポイントが URI 形式のエイリアスで登録されている限り、それらに代わって基本的なプレゼンス情報を提供します。

FindMe を有効になっている場合、Expressway は、FindMe ユーザに設定された各プレゼンティティが提供する情報を集約することによって、その FindMe ユーザに関するプレゼンス情報も提供できます。

Expressway 上のプレゼンス アプリケーションは SIP ベースの SIMPLE 標準規格をサポートします。このアプリケーションは、2 つの個別のサービスから構成されます。具体的には、プレゼンス サーバとプレゼンス ユーザ エージェント（PUA）の 2 つです。これらのサービスは個別にプレゼンスの設定できます。

プレゼンスのステータス ページには、プレゼンス情報を提供するプレゼンティティと、他のユーザに関するプレゼンス情報を要求するユーザの情報が表示されます。ステータス ページは次のように構成されています。

- パブリッシャ（Publishers）
- プレゼンティティ（Presentities）
- サブスクライバ（Subscribers）

（注） 1 つのプレゼンティティがサブスクライブできるのは最大 100 の他のプレゼンティのみであり、そのプレゼンティティをサブスクライブできる他のプレゼンティティは最大 100 のみです。

プレゼンスは、クラスタリングによってサポートされます。

プレゼンス サーバ

Expressway 上のプレゼンス サーバは、その VCS が権限を持つ SIP ドメインのすべてのプレゼンティティのプレゼンス情報の管理を担います。プレゼンス サーバはローカルに登録されているエンドポイントと、SIP プロキシ（別の Expressway など）を介して情報を受信したプレゼンティティの情報を管理できます。

プレゼンス サーバは次のサービスから構成されますが、それらのすべてのサービスは、プレゼンス サーバが有効（または無効）になったときに同時に有効（または無効）になります。

- **パブリケーションマネージャ**：プレゼンティティに関するステータス情報を含む PUBLISH メッセージを受信し、その情報をプレゼンス データベースに書き込みます。PUBLISH はプレゼンス対応のエンドポイントとプレゼンス ユーザ エージェントによって生成されます。
- **サブスクリプションマネージャ**：プレゼンティティのステータスに関する情報を要求する SUBSCRIBE を処理します。SUBSCRIBE メッセージを受信すると、サブスクリプション マネージャはそのプレゼンティティに関する情報の要求をプレゼンティティ マネージャに送信し、返された情報をサブスクライバに転送します。また、サブスクリプション マネージャは、プレゼンティティのステータスが変更されたときにプレゼンティティ マネージャから通知を受信し、その情報をすべてのサブスクライバに送信します。
- **プレゼンティティ マネージャ**：プレゼンス データベースへのインターフェイス。さまざまなデバイスによって提供されたプレゼンス情報を集約して 1 つの特定のプレゼンティティに関する全体的なプレゼンス ステータスを提供する必要がある場合に、FindMe や PUA などの Expressway 機能をサポートするために使用されます。プレゼンティティに関する情報を求める要求をサブスクリプション マネージャから受信した場合、プレゼンティティ マネージャはその特定のプレゼンティティに関連付けられたすべてのエンドポイントで使用可能な情報をプレゼンス データベースに照会します。次に、プレゼンティティ マネージャはこの情報を集約してプレゼンティティの現在のステータスを決定し、それをサブスクリプション マネージャに返します。

- **プレゼンス データベース**：PUBLISH メッセージの形式で受信した現在のプレゼンス情報を格納します。また、NOTIFY メッセージをプレゼンティティ マネージャに送信し、変更があった場合にそれを通知します。

プレゼンスとデバイスの認証

プレゼンス サーバは、すでに認証されているプレゼンス PUBLISH メッセージのみ受け入れます。

- Expressway によるプレゼンス メッセージの認証は、エンドポイントが登録されている場合にはデフォルト サブゾーン（または関連する代替サブゾーン）上の認証ポリシー設定によって制御され（通常のケース）、エンドポイントが登録されていない場合はデフォルト ゾーン上の認証ポリシー設定によって制御されます。
- 関連する **[認証ポリシー（Authentication policy）]** は、*[クレデンシャルを確認する（Check credentials）]* または *[認証済みとして扱う（Treat as authenticated）]* のいずれかに設定されている必要があります。そうでなければ、PUBLISH メッセージは失敗し、エンドポイントはそれぞれのプレゼンス ステータスをパブリッシュできなくなります。

詳細については、「プレゼンスと認証ポリシー」を参照してください。

プレゼンス ユーザ エージェント

プレゼンスをサポートしないエンドポイントは、Expressway の代わりにパブリッシュされたステータスを持つことができます。この情報をパブリッシュするサービスをプレゼンス ユーザ エージェント（PUA）と呼びます。

PUA はローカル登録データベースとコール マネージャから情報を取得し、現在ローカルに登録されている各エンドポイントについて、それらがコール中かどうかを決定します。次に PUA はこのステータス情報を PUBLISH メッセージを介して提供します。

PUA がローカルに登録されているエンドポイントに関するプレゼンス情報を正常に提供するには、次のことが必要です。

- エンドポイントが URI 形式のエイリアスを使用して登録されている必要があります。
- プレゼンス サーバが有効になっている SIP レジストラに URI のドメインの部分のルーティングが可能である必要があります（これは、有効になっている場合にはローカル プレゼンス サーバか、リモート システムの別のプレゼンス サーバかのいずれかです）。

PUA は有効になっている場合は、プレゼンスをすでにサポートしているエンドポイントを含め、Expressway に登録されているすべてのエンドポイントについてのプレゼンス情報を生成します。PUA が提供するステータス情報は次のいずれかです。

- オンライン（*online*）：登録されているが、コール中ではない
- コール中（*in call*）：登録されており、現在コール中

プレゼンス情報の集約

PUA は有効になっている場合は、プレゼンスをすでにサポートしているエンドポイントを含め、Expresswayに登録されているすべてのエンドポイントについてのプレゼンス情報を生成します。ただし、プレゼンスをサポートするエンドポイントは、退席中や応答不可など、より詳細な別のステータスも提供できます。そのため、プレゼンティティ マネージャは PUA が提供する情報を次のように使用します。

- プレゼンス情報が PUA と別のもう 1 つのソースから提供される場合、PUA でないプレゼンス情報を常にPUAプレゼンス情報よりも優先して使用します。これは、情報の別のソースがプレゼンティティ自体であり、その情報のほうがより正確であると考えられるためです。
- プレゼンス情報が PUA と複数の別のソースから提供される場合、プレゼンス サーバはすべてのプレゼンティティからのプレゼンス情報を集約し、*[*オフライン（*offline*）*]* よりも *[*オンライン（*online*）*]*、*[*退席中（*away*）*]* よりも *[*コール中（*in call*）*]* のほうに「「高い関心」」を示します。
- エンドポイントに関する情報が、エンドポイント自体からも、PUAからもパブリッシュされていない場合、エンドポイントのステータスは [オフライン（offline）] になります。PUA が有効になっている場合、*[*オフライン（*offline*）*]* のステータスは、エンドポイントが現在登録されていないことを示します。

FindMe プレゼンス

プレゼンティティ マネージャが FindMe エイリアスの存在についての情報の要求を受信すると、その FindMe エイリアスを構成している各エンドポイントのプレゼンス情報をルックアップします。次に、この情報を次のように集約します。

- FindMe エイリアスが *[*個別（*Individual* ）*]*モードに設定され、その FindMe を構成しているエンドポイントのいずれかがコール中の場合、FindMe プレゼンティティのステータスは *[*コール中（*in call*）*]* と報告されます。
- FindMeエイリアスが *[*グループ（*Group*）*]*モードに設定され、エンドポイントにいずれかがオンライン（コール中でもオフラインでもない）場合、FindMe プレゼンティティのステータスは *[*オンライン（*online*）*]* と報告されます。

再登録更新期間

PUA は、次を受信した時点でプレゼンス情報を更新し、パブリッシュします。

- 登録要求（新規登録の場合）
- 際登録更新（既存の登録の場合）
- 再登録要求
- コールセットアップとクリアダウン情報

非トラバーサル H.323 登録では、デフォルトの登録更新期間は 30 分です。つまり、PUA が既存の登録でVCS上で有効になっている場合は、H.323登録更新を受信し、*[*使用可能（*available*）*]* プレゼンス情報がそのエンドポイントにパブリッシュされるまでに 30 分かかることがあります。

また、H.323 エンドポイントが再登録メッセージを送信せずに使用できなくなった場合、そのステータスが [オフライン（offline）] に変化するのに 30 分かかることがあります。H.323 エンドポイントのプレゼンス情報のパブリケーションをよりタイムリーに行うには、H.323 登録更新期間を短縮する必要があります（**[設定（Configuration）]** > > **[プロトコル（Protocols）]** > **[H.323]** > **[ゲートキーパー（Gatekeeper）]** > **[存続期間（Time to live）]** を使用します）。

SIP のデフォルトの登録更新期間は 60 秒です。したがって、PUA が更新されたプレゼンス情報を SIP エンドポイントの代わりにパブリッシュするのに 1 分もかかりません。

プレゼンスの設定

[プレゼンス（Presence）] ページ（**[アプリケーション（Applications）]** > **[プレゼンス（Presence）]**）を使用して、Expressway 上のプレゼンス サービスを有効にし、設定できます。

これらのサービスは、導入の特性に応じて、それぞれ個別に有効にしたり、無効にしたりできます。デフォルトでは両方とも無効になっています。

（注） プレゼンスサービス が機能するには、**SIP モード**を有効にする必要があります。

プレゼンス ユーザ エージェント

PUA は、登録されているエンドポイントの代わりにプレゼンス情報を提供します。

- *[*有効（*Enabled*）*]*：PUA が有効になっている場合、ローカルに登録されているすべてのエンドポイントがそれら自体のプレゼンス情報もパブリッシュしているかどうかにかかわらず、それらのプレゼンス情報をパブリッシュします。PUAによってパブリッシュされた情報は、エンドポイントのドメインとして機能しているプレゼンス サーバにルーティングされます。これは、ローカル プレゼンス サーバか、（これが無効になっている場合は、そのドメインに権限を持つ別のシステムのプレゼンス サーバである可能性があります。
- *[*無効（*Disabled*）*]*：PUA が無効になっている場合、プレゼンスをサポートするエンドポイントのみがプレゼンス情報をパブリッシュします。プレゼンスをサポートしないエンドポイントの情報は入手できません。

また、[登録済みエンドポイントのデフォルトで公開されるステータス（Default published status for registered endpoints）] も設定できます。これは、「「通話中」」でないときの登録済みエンドポイントについてプレゼンスユーザ エージェントがパブリッシュしたプレゼンティティス テータスです。オプションは [オンライン（Online）] と [オフライン（Offline）] です。

（注）

- これが *[オンライン（Online）]* に設定されている場合、永続的に登録されているビデオエンドポイントと、それらのエンドポイントが含まれている FindMe エンティティは永続的に 「[オンライン（Online）]」 と表示されます。
- 登録されていないエンドポイントのステータスは常に 「[オフライン（Offline）]」 と表示されます。
- Lync クライアントでは 「[オンライン（Online）]」 ステータスは 「[使用可能（Available）]」 と表示されます。

プレゼンス サーバ

プレゼンス サーバは、Expressway が権限を持つ SIP ドメイン内のすべてのプレゼンティティのプレゼンス情報を管理します。

- *[有効（Enabled）]*：ローカル プレゼンス サーバが有効になっている場合、ローカル Expressway が権限を持つ SIP ドメインを対象とする PUBLISH メッセージを処理します。ほかのすべての PUBLISH メッセージが、Expressway の SIP ルーティング ルールに従ってプロキシ経由で送信されます。

（注） SIP ルートは CLI のみを使用して設定されます。

  - プレゼンスサーバは、受信したメッセージが事前認証されている必要があります（プレゼンスサーバは独自の認証チャレンジを実行しません）。PUBLISH メッセージを受信するサブゾーンの**認証ポリシー**が *[クレデンシャルのチェック]* または *[認証済みとして扱われる]* に設定されている場合は、メッセージが拒否されます。

- *[無効（Disabled）]*：ローカルプレゼンスサーバが無効になっている場合、Expressway はローカルに設定されているコールルーティング ルールに従って、1 つ以上のネイバーゾーンにすべての PUBLISH メッセージをプロキシ送信します。ローカル Expressway は、プレゼンティティのドメインに権限があるかどうかに関係なく、これを実行します。これらのネイバーのいずれかにそのドメインの権限があり、そのネイバーでプレゼンス サーバが有効になっている場合、そのネイバーがプレゼンティティのプレゼンス情報を提供します。

プレゼンス サーバが有効になっているかどうかに関係なく、Expressway は次の送信元のいずれかから送信されている場合は PUBLISH メッセージを受信し続けます。

- プレゼンスをサポートするローカルに登録されたエンドポイント
- ローカル PUA（有効になっている場合）
- リモートの SIP プロキシ

（注） プレゼンスサーバは、**Starter Pack** のオプションキーがインストールされている場合は自動的に有効になります。

推奨事項

- **Expressway-E と Expressway-C**：Expressway-E が Expressway-C のトラバーサル サーバとして機能する場合に推奨される設定は、Expressway-E 上で PUA を有効にしてプレゼンス サーバを無効にし、Expressway-C 上でプレゼンス サーバを有効にすることです。これにより、PUA によって生成されるすべての PUBLISH メッセージが確実に Expressway-C にルーティングされます。
- **Expressway ネイバー**：複数の Expressway が互いに隣接する導入環境では、ドメインごとに 1 つのプレゼンス サーバのみを有効にすることを推奨します。これにより、ネットワーク内のすべてのプレゼンティティの情報の中心的なソースが確保されます。
- **Expressway クラスタ**：クラスタ内でのプレゼンスの機能についての情報。

（注） 定義されているトランスフォーメーションも、プレゼンス サーバが処理するパブリケーション、サブスクリプション、および通知の URI に適用されます。

B2BUA（バックツーバック ユーザ エージェント）の概要

B2BUA は SIP コールの両方のエンドポイントの間で動作し、2 つの独立したコール レッグに通信チャネルを分離します。プロキシ サーバとは異なり、B2BUA は処理するコール状態を完全に維持します。コールの両方のレッグは「**コール ステータス（Call status）**」ページと「**コール履歴（Call history）**」ページ上に別個のコールとして表示されます。

B2BUA インスタンスは Expressway でホストされます。これらは次のシナリオで使用されます。

- メディア暗号化ポリシーを適用する場合。この用途では、明示的な B2BUA 設定は必要ではありません。
- ICE メッセージングをサポートする場合。必要になる B2BUA 関連の設定は、ICE コールをサポートするために必要な一連の B2BUA TURN サーバの設定を定義することだけです。
- Expressway と Microsoft SIP ドメインの間の SIP コールをルーティングする場合。これには、Microsoft 相互運用性の設定と B2BUA で使用可能な B2BUA TURN サーバの設定のセットの手動設定が必要です。

B2BUA TURN サーバの設定

[アプリケーション（Applications）] > **[B2BUA]** > **[B2BUA TURN サーバ（B2BUA TURN servers）]** の順に移動し、Expressway B2BUA インスタンスに必要な TURN サーバの詳細を入力します。このページには、現在設定されている TURN サーバのリストが表示されます。このページで TURN サーバを作成、編集、削除できます。

B2BUA は、使用可能なすべてのサーバ間でのランダムなロード バランシングを介して提供する TURN サーバを選択します。B2BUA が選択できるように設定できるサーバの数に制限はありません。

TURN サーバは、ゾーンまたはサブゾーンで有効になっているときに ICE メッセージング用の B2BUA インスタンスによって自動的に使用されます。

Microsoft 相互運用性に TURN サーバを使用するには、**[TURN サービスを提供（Offer TURN services）]** を有効にする必要があります（Microsoft 相互運用性の設定を参照してください）。

表 *1 : TURN* サーバ設定の詳細

フィールド	説明（**Description**）
TURN サーバ アドレス（TURN server address）	ICE コールを確立する（Microsoft Edge などで）ときに提供する TURN サーバの IP アドレス。 TURN サーバは、Expressway-E TURN など、RFC 5245 対応である必要があります。
TURN サーバ ポート（TURN server port）	TURN サーバのリスニング ポート。
説明 （Description）	自由形式の TURN サーバの説明。
TURN サービス ユーザ名（TURN services username）と TURN サービス パスワード（TURN services password）	TURN サーバへのアクセスに必要なユーザ名とパスワード。

Microsoft の相互運用性について

Expressway の Microsoft との相互運用性は、Expressway と Microsoft Skype for Business の間の SIP コールを処理するバックツーバック ユーザ エージェント（B2BUA）に基づいています。

（注） バージョン X8.9 では、Expressway の B2BUA を使用せずに Microsoft のインフラストラクチャと相互運用できます。代わりに、セッション分類検索ルールを使用して、トランスコードをする Cisco Meeting Server にコールをルーティングできます。Expressway 設定ガイドのページに用意されている『*Cisco Meeting Server with Cisco Expressway Deployment Guide*』（旧称『*Cisco ExpresswayTraffic Classification Deployment Guide*』）。

機能

- Microsoft ICE と、シスコのコラボレーション エンドポイントとブリッジの標準ベースのメディアとの間のインターワーク。
- Microsoft クライアントを使用したコールに対するコール保留、コール転送、Multiway のサポート。また、FindMe プレゼンス情報を Microsoft インフラストラクチャと共有できます。
- Microsoft クライアントの画面共有（RDP）の H.264 へのトランスコーディング
- Microsoft SIP からのメッセージングおよびプレゼンスのトラフィックをフィルタリングし、Expressway の音声/ビデオ トラフィックを処理しながら、適切なサーバ、たとえば IM and Presence Service ノードへリダイレクトします。

設定の概要

- 専用の Expressway の Microsoft 相互運用性サービスの選択。
- *Microsoft* 相互運用性キーの追加。
- Microsoft 相互運用性の設定。
- B2BUA の信頼できるホストの設定（シグナリング メッセージを B2BUA に送信できるデバイス）
- B2BUA TURN サーバの設定。（ICE コールを確立するときに B2BUA が使用可能な TURN サーバ）。
- 自動的に設定の設定されたゾーンを介して、Microsoft ドメイン、B2BUA にコールをルーティングするための検索ルールの設定。

  B2BUA を有効にすると、Expressway は自動的に **To Microsoft destination via B2BUA** と呼ばれる構成不可能なネイバーゾーンを作成します。このゾーンは検索ルールの対象にする必要があります。

  このゾーンは B2BUA を無効にしても自動的に削除されません。また、X8.8 へのアップグレード時にこのゾーンがあると古いゾーン名（To Microsoft Lync Server via B2BUA）が存続されます。
- 必要に応じて、Microsoft 相互運用性サービスの再起動サービスを再起動する必要がある場合にシステムが通知します。

Microsoft 相互運用性オプション キーが必要になる理由

Expressway を使用して Microsoft コラボレーションのインフラストラクチャと標準ベースのインフラストラクチャ間のトラフィックを変更する場合に、Expressway-C で（Expressway-C がクラスタ化されている場合は各ピアで）このキーが必要です。次の内容が含まれています。

- Microsoft SIP から標準 SIP コールへのインターワーキング
- 画面共有のトランスコーディング（RDP から BFCP の H.264）
- Microsoft SIP メッセージとプレゼンスの転送（SIP ブローカ）

変更せずに Microsoft のトラフィックをルーティングするために Expressway を使用する場合はこのキーは不要です。たとえば、Cisco Meeting Server がインターワーキングする Microsoft のさまざまな SIP トラフィックを送信するために Expressway の検索ルールを使用する場合です。

機能および制限事項

- 最大同時コール能力は 100 コールです（大規模システムを含む）。コール数が 75 に制限される M5 ベースの小規模システムについては、例外となります。
- 外部トランスコーダ経由でルーティングされたコールは 2 つのコールとしてカウントします。
- コールが Microsoft 相互運用性 B2BUA を通じてルーティングされる場合、B2BUA は常にメディアを取得し、常にシグナリング パスに留まります。B2BUA を通じてルーティングしたコール コンポーネントは、コンポーネント タイプが *Microsoft* 相互運用性であるため、コール履歴の詳細情報で特定できます。
- Microsoft 相互運用性サービスは、エンドポイントと Expressway 間のコール レッグが必要とする追加コール ライセンスを超えて消費しません。
- 設定されたすべての外部トランスコーダがそれらのキャパシティの上限に達した場合、通常はトランスコーダを介してルーティングされるコールが失敗します。コールは通常に接続されますが、トランスコードされません。
- 複数の TURN サーバを Microsoft 相互運用性サービスと共に使用できます。TURN サーバは、Microsoft Edge サーバを通過するコールに必要です。
- エンドポイントと B2BUA 間のコール レッグを制御するために帯域幅を適用できますが、B2BUA と Microsoft のインフラストラクチャ間のコール レッグにはできません。ただし、B2BUA は受信したメディアを何の操作せずに転送するため、Expressway から B2BUA のレッグに適用する帯域幅制御が暗黙的に B2BUA から Microsoft のレッグに適用されます。
- （「**「To Microsoft destination via B2BUA」**」という名前の）構成不可能なネイバーゾーンは、*Microsoft* 相互運用性の特殊なゾーンプロファイルを使用します。手動で設定されたゾーンにこのプロファイルを選択することはできません。
- **Expressway および Cisco Meeting Server を使用したドメイン内 Microsoft 相互運用性**

Microsoft 相互運用性向け Meeting Server を使用する場合、現時点では次のドメイン内または企業内のシナリオに制限が適用されます。

単一のドメイン内、および（サブネットワーク間で内部ファイアウォールを使用するなどの理由により）*Expressway-E/Cisco VCS Expressway* を *Microsoft* のフロントエンドサーバーに**直接接続**する構成では、個別の *Microsoft* ネットワークと標準ベースの *SIP* ネットワークを別々に展開します。たとえば、*1* つの *(*サブ*)* ネットワーク内の *Cisco Unified Call Manager* と、同じドメイン内の *2* 番目 *(*サブ*)* ネットワーク内の *Microsoft*。

この場合、通常、2 つのネットワーク間の Microsoft の相互運用性はサポートされません。また、Meeting Server と Microsoft 間の通話は拒否されます。

回避策：Expressway-E/VCS Expressway を介在させずにドメイン内ネットワークを展開することができない場合（Meeting Server <> Expressway-C/VCS Control <> Microsoft を構成できない場合）の回避策としては、各サブネットに Expressway-C/VCS-C を展開し、サブネット間を通過させるために Expressway-E/VCS-E を配置します。つまり、以下のようになります。

Meeting Server <> Expressway-C/VCS Control <> ファイアウォール <> Expressway-E/VCS Expressway <> ファイアウォール <> Expressway-C/VCS Control <> Microsoft

Microsoft 相互運用性用の Expressway 構成の詳細：

- Cisco Expressway シリーズ設定ガイドのページに用意されている、ご使用のバージョンに対応する『*Cisco Expressway IP Port Usage Configuration Guide*』を参照してください。
- Expressway 構成ガイドページの『*Cisco Expressway* および *Microsoft* インフラストラクチャ導入ガイド』を参照してください。

Microsoft 相互運用性の設定

[アプリケーション（Applications）] > **[B2BUA]** > **[Microsoft 相互運用性（Microsoft Interoperability）]** > **[設定（Configuration）]** の順に移動し、Microsoft 環境への B2BUA の接続を設定して有効にします。

次の表に、設定可能なオプションを記載します。

フィールド	説明（**Description**）	使用方法のヒント
[設定（Configuration）] セクション：		
Microsoft 相互運用性（Microsoft interoperability）	Microsoft 相互運用性サービスを有効または無効にします。	

フィールド	説明（**Description**）	使用方法のヒント
接続先アドレス（Destination address）	ハードウェア ロード バランサ、ディレクタ、またはExpresswayがシグナリング メッセージを送信するフロントエンドプロセッサの IP アドレスまたは完全修飾ドメイン名（FQDN）。	また、B2BUA の信頼できるホストの設定の IP アドレスも設定する必要があります。これらはシグナリング メッセージを Expressway に送信する可能性がある Microsoft システムです。
リスニング ポート（Listening port）	ハードウェア ロード バランサ、ディレクタ、またはExpresswayがシグナリング メッセージを送信するフロントエンドプロセッサの IP ポート。	
シグナリング トランスポート（Signaling transport）	Microsoft インフラストラクチャへの接続に使用するトランスポート タイプ。デフォルトは、[TLS] です。	
[FindMe 統合（FindMe integration）] セクション：		
FindMe ユーザをクライアントとして Microsoft サーバに登録（Register FindMe users as clients to Microsoft server）	コールを FindMe エイリアスに転送したり、FindMe プレゼンス情報を共有したりできるように FindMe ユーザを Microsoft レジストラに登録するかどうかを制御します。デフォルトは [はい（Yes）] です。	この機能は FindMe が有効になっている場合にのみ適用されます。 （注） FindMe ID が Active Directory で有効なユーザである場合のみ FindMe ユーザを Microsoft インフラストラクチャに登録できます（同様に Microsoft クライアントが登録できるのは、所有している有効なアカウントが AD で有効な場合に限ります）。
Microsoft ドメイン（Microsoft domain）	Microsoft サーバで 使用されている SIP ドメイン。Expressway 上にすでに設定されている SIP ドメインのいずれかを選択する必要があります。	このドメインの FindMe の名前のみが Microsoft サーバに登録されます。
[リモート デスクトップ プロトコル（Remote Desktop Protocol）] セクション：		

フィールド	説明（**Description**）	使用方法のヒント
この B2BUA に対して RDP トランスコーディングを有効化	B2BUA がリモートデスクトッププロトコルのトランスコーディングを提供するかどうかを制御します。 この機能には **Microsoft 相互運用性**のオプション キーが必要です。 デフォルトは [いいえ（No）] です。	Microsoft クライアント ユーザにシスコ コラボレーション エンドポイント/会議の参加者との画面共有を可能にするには、このオプションを有効にする必要があります。
[SIP ブローカ（SIP broker）] セクション：		
着信 SIP のブローカを有効化（Enable broker for inbound SIP）	SIP ブローカを切り替え、宛先プレゼンス サーバのリストを開きます。 ブローカは Microsoft SIP を検査し、SIP SIMPLE をユーザが入力する IM and Presence Service ノードにルーティングします。	ブローカが有効でない場合、B2BUA は Microsoft からのすべての着信 SIP の処理を試行します。SIP SIMPLE を受信すると、SIP 音声/ビデオ トラフィックであるかのようにルーティングしようとします。この状況ではおそらく、SIP SIMPLE はコール制御インフラストラクチャによって拒否されます。
プレゼンスの宛先サーバのリスニング ポート（Listening port on presence destination servers）	これは IM and Presence Service ノードに設定されているポートです。	
宛先プレゼンス サーバ 1 ～ 6（Destination presence server 1..6）	IM and Presence Service ノードの IP アドレス、ホスト名、または FQDN。	最大 6 つ入力します。Expressway は活性状態を判別するためにこれらを定期的にポーリングし、ラウンドロビン アルゴリズムを使用してこれらにトラフィックをルーティングします。
TURN セクション：		

フィールド	説明（**Description**）	使用方法のヒント
TURNサービスを提供（Offer TURN services）	B2BUA が TURN サービスを提供するかどうかを制御します。デフォルトは [いいえ（No）] です。	Microsoft Edge サーバを通過するコールに推奨されます。 関連付けられた TURN サーバを設定するには、[B2BUA TURN サーバの設定（Configure B2BUA TURN servers）]B2BUA TURN サーバの設定 をクリックします。
[詳細設定（Advanced settings）]：シスコ カスタマー サポートのアドバイスがあった場合にのみ、高度な設定を変更してください。		
暗号化	B2BUA が暗号化されたコール レッグと暗号化されていないコール レッグをどのように処理するかを制御します。 *[必須（Required）]*：コールの両方のレッグを暗号化する必要があります。 *[自動（Auto）]*：暗号化と非暗号化の組み合わせをサポートします。 デフォルトは [自動（Auto）] です。	B2BUA を介したコールには 2 つのレッグがあります。1 つは B2BUA から標準的なビデオ エンドポイントへのレッグ、もう 1 つは B2BUA から Microsoft クライアントへのレッグです。コールのどちらのレッグも暗号化することも、暗号化しないこともできます。 *[自動（Auto）]* に設定すると、暗号化されたコール レッグと暗号化されていないコール レッグのどのような組み合わせでもコールは確立できます。したがって、コールの一方のレッグを暗号化し、もう一方は暗号化しないこともできます。
B2BUA メディア ポート範囲の開始/終了（B2BUA media port range start/end）	メディアを処理するために B2BUA が使用するポート範囲。	このポート範囲は、この Expressway またはこの Expressway の TURN サーバが使用する他のポート範囲と重複しないことを確認してください。 デスクトップの共有によってコールごとに必要となるメディア ポートの数が増えるため、[この B2BUA に対して RDP トランスコーディングを有効化する（Enable RDP transcoding for this B2BUA）] を有効にしている場合はこの範囲も拡大する必要があります。

フィールド	説明（Description）	使用方法のヒント
ホップ カウント（Hop count）	SIP メッセージに使用する最大転送値を指定します。デフォルトは 70 です。	
セッション更新間隔（Session refresh interval）	SIP コールのセッション更新要求間に許容される最大時間。デフォルトは 1800 秒です。	詳細については、RFC 4028 の *Session-Expires* の定義を参照してください。
最小セッション更新間隔（Minimum session refresh interva）	B2BUA コールのセッション更新間隔を VCS がネゴシエートする最小値。デフォルトは 500 秒です。	詳細については、RFC 4028 の *Min-SE header* の定義を参照してください。
Expressway 通信用の B2BUA のポート（Port on B2BUA for Expressway communications）	Expressway と通信するために B2BUA で使用するポート。	
Microsoft コール通信用の B2BUA のポート（Port on B2BUA for Microsoft call communications）	Microsoft サーバとのコール通信に B2BUA で使用するポート。デフォルトは 65072 です。	
RDP TCP ポート範囲の開始/終了（RDP TCP port range start/end）	トランスコーダ インスタンスが RDP メディアをリッスンする TCP ポートの範囲を定義します。デフォルトは 6000 ～ 6099 です。 （注） ページを保存し、Microsoft 相互運用性サービスを再起動して変更を適用します。	B2BUA で作成された各同時 RDP トランスコーディング セッションには受信ポートが必要です。考えられる同時トランスコード セッションの最大数が 100 であるため、範囲は 100 までに制限されます。

フィールド	説明（**Description**）	使用方法のヒント
RDP UDP ポート範囲の開始/終了（RDP UDP port range start/end）	トランスコーダ インスタンスが H.264 メディアを送信する UDP ポートの範囲を定義します。デフォルトは 6100 ～ 6199 です。 （注） ページを保存し、Microsoft 相互運用性サービスを再起動して変更を適用します。	B2BUA で作成された各同時 RDP トランスコーディング セッションには、結果の H.264 メディアを送信するためのポートが必要です。考えられる同時トランスコード セッションの最大数が 100 であるため、範囲は 100 までに制限されます。
最大 RDP トランスコード セッション数（Maximum RDP transcode sessions）	この Expressway 上での同時 RDP トランスコーディングセッション数を制限します。デフォルト値は 10 です。 （注） ページを保存し、Microsoft 相互運用性サービスを再起動して変更を適用します。	値が高いほど TDP トランスコーディングによってより多くのシステム リソースが消費され、他のサービスに影響が及ぶ可能性があります。最大値は 100 です。 推奨される最大 RDP トランスコードセッション： • 中規模の OVA システム：10 • 大型の OVA/CE1200 システム：20（X8.10 では、大規模システム用に 10 ギガビット NIC を使用する必要がなくなりました。帯域幅制約によっては、1 Gbps の NIC で大規模システムの容量を達成することが可能です。）

B2BUA の信頼できるホストの設定

[アプリケーション（Applications）] > [B2BUA] > [Microsoft 相互運用性（Microsoft Interoperability）] > [信頼できるホスト（Trusted hosts）] に移動し、Expressway が SIP シグナリングを信頼する Microsoft ホストを指定します。

相互運用性サービスは、信頼できるホストのリストにないアドレスからのメッセージは受け入れません。

（注） 信頼できるホスト検証は、Expressway ビデオ ネットワークにインバウンドされる Microsoft クライアントによって開始されるコールにのみ適用されます。コールの開始が Expressway のビデオ ネットワークからのみの場合は、信頼できるホストを設定する必要はありません。

Expressway には現在、25 という信頼できるホスト数の公称制限があります。信頼できるホストが 25 を超えていると、Expressway でアラームが発生します。

実際には、導入環境に必要な場合、25 を超えて信頼できるホストを設定できます。この数を 50 未満に保って、アラームを安全に無視できるようにすることを推奨します。50 を超える必要がある場合は、異なる Gateway Expressway を追加することを推奨します。

設定可能なオプションは次のとおりです。

フィールド	説明	使用方法のヒント
名前	オプションの自由形式の信頼できるホストの説明。	名前は「「信頼」」条件の一部としては使用されません。IP アドレスに依存せず複数のホストを区別しやすくするためだけのものです。
IP address	信頼できるホストの IP アドレス。	
タイプ（Type）	B2BUA にシグナリング メッセージを送信するデバイスのタイプ。 *[Microsoft インフラストラクチャ（Microsoft infrastructure）]*：ハードウェ ロードバランサ、ディレクタ、およびフロントエンド プロセッサなど	

Microsoft 相互運用性サービスの再起動

再起動を行い、Microsoft 相互運用性サービスに変更を適用する必要があることがあります。再起動を必要とするとシステムによってアラームが表示されます。

このサービスを再起動すると、Expressway は再起動しませんが、B2BUA によって管理されているコールはすべてドロップします。

ステップ 1 **[アプリケーション（Applications）] > [B2BUA] > [Microsoft 相互運用性（Microsoft Interoperability）] > [サービスの再起動（Restart service...）]** に移動します

ステップ 2 現在実行されているアクティブなコールの数を確認します。

ステップ 3 [再起動（Restart）] をクリックします。

数秒後にサービスが再起動します。Microsoft 相互運用性の設定ページでサービス ステータスを確認できます。

クラスタ化された Expressway システム

すべてのピアの Microsoft 相互運用性サービスを再起動する必要があります。他のピアのサービスを再起動する前に、プライマリのサービスを設定し、再起動し、確認します。

FindMe について

FindMe はユーザ ポリシーの形式を取り、Expressway がコールを受信したときに特定のユーザまたはグループ宛のコールがどうなるかを決定する一連のルールです。

FindMe 機能によって、企業内の個人またはチームに単一の FindMe ID を割り当てることができます。FindMe アカウントにログインすることで、ユーザは「在宅中」や「社内」などのロケーションのリストをセットアップしてユーザのデバイスとそれらの場所とを関連付けることができます。次に、ユーザは FindMe ID をダイヤルしたときにどのデバイスをコールするかを指定し、それらのデバイスがビジーであったり、応答がない場合にどうするかを指定できます。各ユーザは最大 15 台のデバイスと 10 か所の場所を指定できます。

つまり、コールをする可能性がある発信者には単一の FindMe エイリアスを付与し、そのエイリアスで企業内の個人またはグループに接続できます。発信者は個人またはグループが応答できるすべてのデバイスの詳細を知る必要はありません。

この機能を有効にするには、デスクトップ システムまたは TelePresence Room システム登録ライセンスを購入し、インストールする必要があります。

エンドユーザの FindMe アカウント設定

ユーザは、Cisco TMS プロビジョニングを使用して FindMe の設定を構成できます。TMS プロビジョニングが有効な場合、ユーザは FindMe アカウントを使用して Cisco TMS にログインして、FindMe の設定を管理します。ユーザ アカウントと FindMe データは、TMS Provisioning Extension サービスによって Cisco TMS から Expressway に提供されます。

Expressway は、LDAP サーバーでユーザーを検索するために、**distinguishedName** という名前の属性を検索します。

（注） LDAP サーバーのユーザーレコードに、**distinguishedName** という名前の有効な属性があることを確認します。

FindMe アカウントのセットアップに関する詳細については『FindMe 導入ガイド』を参照してください。

デバイスの指定方法

FindMe アカウントの設定時に、ユーザは FindMe ID へのコールをルーティングするデバイスを指定するように求められます。

エイリアスを指定したり、他の FindMe ID を 1 つ以上のデバイスとして指定することもできます。ただし、このような場合は循環設定を回避するように注意する必要があります。

そのため、デバイスを登録したエイリアスを入力して FindMe ID をコールしたときに呼び出す物理的なデバイスをユーザが指定することを推奨します。

プリンシパル デバイス

FindMe ユーザのアカウントは 1 つ以上のプリンシパル デバイスで設定する必要があります。これらは、そのアカウントに関連付けられたメイン デバイスになります。

ユーザは、プリンシパルデバイスのアドレスを削除または変更できません。これは、基本的な FindMe 設定をユーザが誤って変更することがないようにするためです。

また、プリンシパルデバイスは Expressway が使用し、同じデバイス アドレスが複数の FindMe ID に関連付けられている場合に、どの FindMe ID を**発信者 ID** として表示するかを決定します。管理者（FindMe ユーザ自身ではない）のみが、FindMe ユーザのどのデバイスがプリンシパル デバイスかを設定できます。

FindMe プロセスの概要

Expressway が特定のエイリアス宛のコールを受信すると、ユーザ ポリシーを次のように適用します。

- 最初に、FindMe が有効になっているかどうかを確認します。有効になっている場合は、エイリアスが FindMe ID であるかを確認します。そうであった場合は、そのユーザの FindMe 設定のアクティブな場所に関連付けられたエイリアスにコールを転送します。
- FindMe が有効になっていないか、またはエイリアスが FindMe ID でなかった場合は、Expressway は通常の方法でエイリアスの検索を続行します。

（注） ユーザポリシーは Expressway に設定されているコールポリシーが適用された後に呼び出されます。詳細については 、コールルーティングプロセスを参照してください。

FindMe 導入時の推奨事項

- FindMe ID は URI 形式であり、個人のプライマリ URI である必要があります。
- エンドポイントは既存の FindMe ID と同じエイリアスで登録しないでください。これを防ぐには、拒否リストのすべての FindMe ID を含めます。

例

Example Corp. のユーザは、FindMe ID の形式**john.smith@example.com**を使用しています。ユーザの各エンドポイントは、その物理的な場所を特定するために若干異なるエイリアスで登録されています。たとえば、オフィス エンドポイントは形式**john.smith.office@example.com**でエイリアスに登録され、ホームエンドポイントは**john.smith.home@example.com**として登録されます。

両方のエンドポイントが、FindMe ID がダイヤルされたときに呼び出すデバイスのリストに含まれています。エイリアス**john.smith@example.com**が拒否リストに追加され、個々のエンドポイントがそのエイリアスに登録されるのを防ぐためです。

FindMe の設定

「**FindMe の設定（FindMe configuration）**」ページ（**[アプリケーション（Applications）] > [FindMe]**）を使用して FindMe についてを有効にして設定します。

設定可能なオプションは次のとおりです。

フィールド	説明（**Description**）	使用方法のヒント
FindMe モード（FindMe mode）	FindMeが有効かどうかと、サードパーティ製のマネージャを使用するかどうかを決定します。 *Off*：FindMe を無効にします。 リモートサービス：FindMe を有効にし、オフボックスシステム（TMS など）にある FindMe マネージャを使用します。	コール ポリシーは、FindMe モードに関係なく、常に適用されます。 FindMe を有効にした場合、**クラスタ名**が指定されていることを確認する必要があります（これは、[クラスタリング（Clustering）]ページで行います）。
発信者 ID（Caller ID）	着信コールの発信元が呼び出し先にどのように表示されるかを決定します。 *[着信 ID（Incoming ID）]*：コールが発信されたエンドポイントのアドレスを表示します。 *[FindMe ID]*：発信エンドポイントのアドレスに関連付けられた FindMe ID を表示します。	*FindMe ID* を使用すると、受信者が受信後にそのコールを返した場合は FindMe デバイス アカウントに関連付けられたすべてのデバイスがコールされます。 FindMe ID は送信元エンドポイントが認証されている（または認証済みとして処理されている）場合にのみ表示されます。認証されていない場合、着信 ID が表示されます。詳細については、デバイス認証についてを参照してください。

次のオプションは、**[FindMe モード（FindMe mode）]** が *[リモート サービス（Remote service）]* の場合に適用されます。

フィールド	説明（**Description**）
プロトコル（Protocol）	リモート サービスに接続するために使用するプロトコル。
アドレス（Address）	リモート サーバの IP アドレスまたはドメイン名。
パス（Path）	リモート サービスの URL。
ユーザ名（Username）	リモート サービスにログインして照会するために Expressway が使用するユーザ名。
パスワード（Password）	リモート サービスにログインして照会するために Expressway が使用するパスワード。

FindMe データの管理とストレージ

FindMe を使用し、FindMe データの管理には Cisco TMS を使用する場合は、Cisco TMSPE サービスを設定して Expressway に FindMe データを提供する必要があります。

Cisco TMS プロビジョニング（FindMe を含む）

Cisco TMS プロビジョニングは、Expressway がプロビジョニング データを取得するためのメカニズムです。

- 具体的には、Expressway はこのメカニズムを使用して、エンドポイント デバイスからの Expressway プロビジョニング サーバに対し、ユーザ アカウント、デバイス、電話帳のデータを提供します。
- また、Expressway は FindMe についてを提供するために使用する FindMe アカウントの設定データもこのメカニズムによって取得します。

TMS プロビジョニング サービスを有効にする方法

X8.11 以降、新しいシステムでは Expressway 内の TMS プロビジョニング サービスはデフォルトで無効にされます（既存のシステムを X8.11 以降にアップグレードする場合は、現在の設定が保持されます）。TMS プロビジョニング サービスを有効にするには、次の手順に従います。

（注） プロビジョニングは Cisco Expressway-C と Cisco Expressway-E の両方でサポートされていますが、Cisco Expressway-C と Cisco Expressway-E をペアにした導入環境では Cisco Expressway-C 上で使用することを推奨します。

1. （1 回限り）プロビジョニング サービスがまだ有効にされていない場合、Expressway で次の操作を行って、プロビジョニング サービスを有効にする必要があります。
   1. **[システム（System）]** > **[管理（Administration）]** に移動します。
   2. **[サービス（Services）]** エリアで、**[プロビジョニング サービス（Provisioning services）]** を *[オン（On）]* に設定します。

      これにより、インターフェイスで **[システム（System）]** > **[TMS プロビジョニング拡張サービス（TMS Provisioning Extension services）]** のページにアクセスできるようになります。このページから、Cisco TelePresence Management Suite Provisioning Extension（Cisco TMSPE）とユーザ、デバイス、FindMe、電話帳のプロビジョニング サービスに接続できます。
2. **[システム（System）]** > **[TMS プロビジョニング拡張サービス（TMS Provisioning Extension services）]** に移動します。
3. Cisco TMSPE の接続詳細を指定します（詳細については、「TMS プロビジョニング拡張サービスの設定」を参照してください）。

4. 1 つ以上のプロビジョニング サービス（ユーザ、デバイス、FindMe、電話帳）を有効にします。各サービスについて、次の操作を行います。
   1. **[このサービスに接続（Connect to this service）]** を *[はい（Yes）]* に設定します。
   2. **[ポーリング間隔（Polling interval）]** または **[接続（Connection）]** のデフォルト値を使用しない場合は、必要に応じて値を設定します。

      [デバイス（Devices）] には、[基本グループ（Base Group）] を指定する必要があります。Cisco TMSPE 内で Expressway またはクラスタを識別する ID を入力します。

クラスタとプロビジョニングのサイズの制限

あらゆる規模の Expressway クラスタでサポートされる最大値は次のとおりです。

- 10,000 個の FindMe アカウント
- 10,000 人のプロビジョニングするユーザ
- 200,000 の電話帳エントリ

（注） システムのデバイス登録容量制限が上記の設定よりも大きい場合でも、クラスタごとの FindMe アカウント/ユーザ数は 10,000、プロビジョニングできるデバイス数は 10,000 に制限されます。

10,000 を超えるデバイスをプロビジョニングする必要がある場合、ご使用のネットワークには、適切に設計され、ダイヤル プランが設定された追加の Expressway クラスタが必要になります。

Cisco TMS と Expressway でのプロビジョニングの設定方法の詳細については、『Cisco TMS プロビジョニング拡張導入ガイド』を参照してください。

プロビジョニングに使用される Cisco TMSPE サービス

TMS プロビジョニングが有効になっている場合、Expressway は（Cisco TMS 上でホストされる）次の Cisco TMSPE サービスを使用して Expressway または Expressway クラスタにデータを提供します。

サービス	説明（Description）
ユーザ設定	Expressway が特定のユーザに適用される設定値を使用してデバイスを設定するためのデータを提供します（ユーザは基本的に SIP URI です）。Jabber Video などのデバイスはこのサービスを使用して完全に設定されます。また、TURN サーバ（通常は Expressway-E）への接続詳細も提供します。

サービス	説明（Description）
FindMe	各 FindMe ID に関連付けられているロケーションとデバイスをはじめ、ユーザの FindMe アカウントの詳細を提供します。これにより、Expressway はユーザ ポリシーを適用したり、発信者の送信元アドレスを対応する FindMe ID に変更したりできます。
電話帳	ユーザが電話帳で連絡先を検索するために使用するデータを提供します。電話帳へのアクセスは、（Cisco TMS 内に）定義されているアクセス コントロール リストに従ってユーザ単位で制御されています。
デバイス	Expressway と Cisco TMS 間でプロビジョニング ランセンス情報を交換します。情報は 30 秒ごとに交換されます。Cisco TMS が管理している Expressway クラスタの範囲で使用可能な無償ライセンスの現在の数が Expressway に提供され、Expressway はその Expressway（または Expressway クラスタ）が使用しているプロビジョニング ライセンスのステータスで Cisco TMS を更新します。 デバイス サービスがアクティブになっていない場合は、Expressway のプロビジョニング サーバはデバイスをプロビジョニングできません。

Cisco TMSPE サービスのステータス情報

サービスのステータス情報は、[TMS プロビジョニング拡張サービスのステータス（TMS Provisioning Extension service status）] ページに表示されます。

- Expressway は定期的に Cisco TMSPE サービスをポーリングし、Expressway に保持されているデータが最新の状態に維持されるようにします。ポーリング間隔はサービスごとに定義できます。通常の導入環境では、FindMe とユーザ プロビジョニングのデータを頻繁（2 分ごと）に更新し、電話帳のデータを毎日更新するデフォルトの設定を使用することを推奨します。

  クラスタ化された Expressway では、クラスタ ピアのいずれか 1 つのみが Cisco TMS との物理接続を維持します。Cisco TMS から取得されたデータは Expressway クラスタの複製メカニズムを通じてクラスタ内の他のピア間で共有されます。

- Expressway と Cisco TMS 間のデータの即時再同期は、いつでも行うことができます。それには、**「TMS プロビジョニング拡張サービス（TMS Provisioning Extension services）」** ページで **[完全同期の実行（Perform full synchronization）]** をクリックします。これにより、データが削除されて完全に更新されるまでの数秒間、Expressway 上でサービスが停止します。Cisco TMS 内での最近の更新のみを Expressway に適用する場合は、別の方法として、**[更新の確認（Check for updates）]** をクリックしてください。

Cisco TMSPE サービスの設定の変更

Cisco TMSPE サービスの設定を変更するには、Cisco TMS を使用することを強く推奨します。Expressway でもサービスを設定できますが（**「TMS プロビジョニング拡張サービス**

（**TMS Provisioning Extension services**）」ページ）、このページで行った変更は **Cisco TMS** で適用されません。

Expressway プロビジョニング サーバ

デバイス プロビジョニングが有効にされている場合、Expressway プロビジョニング サーバは Cisco TMS プロビジョニング（FindMe を含む）メカニズムを通じて Cisco TMS が提供したデータを使用して、プロビジョニング関連のサービスをプロビジョニング済みのデバイスに提供します。

Expressway はプロビジョニング データと FindMe データの Expressway への提供に Cisco TelePresence Management Suite Provisioning Extension（Cisco TMSPE）サービスのみをサポートしています。このモードでは、すべてのプロビジョニング データと FindMe データは、Cisco TMS 内のみで管理、維持されます。

プロビジョニング ライセンス

プロビジョニング サーバが同時にプロビジョニングできるデバイスの数には制限があります。Expressway と Cisco TMS は、Cisco TMSPE デバイス サービスを通じて情報を交換することで使用可能なプロビジョニング ライセンスの数を管理します。デバイス サービスがアクティブになっていない場合は、Expressway のプロビジョニング サーバはデバイスをプロビジョニングできません。

Cisco TMS が管理している Expressway クラスタの範囲で使用可能な無償ライセンスの現在の数が Expressway に提供され、Expressway はその Expressway（または Expressway クラスタ）が使用しているプロビジョニング ライセンスのステータスで Cisco TMS を更新します。ライセンスの制限は、デバイス タイプごとに管理できます。

Jabber Video 4.x など、一部のデバイスはプロビジョニングをサインアウト（登録解除）するタイミングを Expressway に通知しません。Expressway は、ライセンスを解放する前に 1 時間のタイムアウト間隔を適用することで、これらのデバイスを管理します。

プロビジョニングとデバイスの認証

プロビジョニング サーバが受信するプロビジョニング要求または電話帳要求は、Expressway へのゾーンまたはサブゾーン エントリ ポイントにおいて、すでに認証されている必要があります。プロビジョニング サーバは、自分自身で認証チャレンジを行うことはありません。未認証のメッセージはすべて拒否されます。

詳細については、「デバイスのプロビジョニングと認証ポリシー」を参照してください。

ハイブリッド サービスとコネクタの管理

ハイブリッド サービス用に Expressways を登録する場合は、ハイブリッド サービスのドキュメントを参照して、ハイブリッド サービスを初めて導入する方法を含め、詳細情報を確認してください。

ハイブリッド サービスとは何か、また、何を実行するか。

Cisco Webex ハイブリッド サービスは、内部施設ベースのソリューションを Cisco Collaboration cloud に結び付け、より優れ、より緊密に統合されたコラボレーション ユーザ エクスペリエンスを実現します。

使用できるサービス

ハイブリッドサービスを購入すると、Cisco Webex Control Hub（Cisco Webex に対する管理インターフェイス）にアクセスできるようになります。Control Hub から、各ハイブリッド サービスの導入サポートに従って、ユーザに対して機能を有効にすることができます。

必要なソフトウェア

ハイブリッドサービスのオンプレミスコンポーネントは「「コネクタ」」と呼ばれ、Expressway ソフトウェアには登録を管理する管理コネクタとその他のコネクタが含まれています。

Expressway をクラウドに登録するまでは、管理コネクタは休止状態になっています。登録すると、新しいバージョンが使用できる場合は、管理コネクタが自動的にダウンロード、インストール、アップグレードされます。

その後で、Control Hub で選択したほかのコネクタが Expressway によってダウンロードされます。これらはデフォルトでは起動しないため、動作させる前に設定する必要があります。

設定が完了すると、Control Hub で設定したソフトウェア アップグレード スケジュールに従って、コネクタが自動的にダウンロードおよびアップグレードを行います。手動による作業は必要ありません。

インストール、アップグレード、またはダウングレードの方法

コネクタは、デフォルトではアクティブ化されていないため、設定し、起動するまでは何も実行しません。これを行うには Expressway にコネクタをインストールした新しいインターフェイスのページを使用します。

コネクタのアップグレードは、Control Hub からも実行でき、アップグレードを承認したときに管理コネクタが新しいバージョンを Expressway にダウンロードします。

また、登録解除もできますが、これを行うことによって Cisco Webex から Expressway が切断され、コネクタと関連設定がすべて削除されます。

（注） 新しいフィーチャと機能を提供するために、クラウドにより提供されるサービスの開発は常に継続されていることから、ハイブリッドサービスでサポートされる Expressway の最小バージョンも変更される場合があります。ハイブリッドサービス展開が機能し続け、公式にサポートされるよう、登録している Expressways を最新の状態を維持するようにしてください。詳細については、Expressway サポート バージョンの説明を参照してください。

ハイブリッド サービスに関する詳細情報の入手先

ハイブリッド サービスは開発が進められており、Expressway よりも頻繁にパブリッシュされる場合があります。そのため、ハイブリッド サービスに関する情報はハイブリッド サービスのドキュメントで維持されており、いくつかの Expressway インターフェイス ページにはそのサイトへのリンクが備わっています。

コネクタ プロキシ

ハイブリッドサービス用にExpresswaysを登録する場合は、ハイブリッドサービスのドキュメントを参照して、ハイブリッドサービスを初めて導入する方法を含め、詳細情報を確認してください。

このプロキシの目的

この Expressway を Cisco Webex に接続するにはプロキシが必要となる場合、**[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 プロキシ（Connector Proxy）]** にあるページを使用します。Expressway はこのプロキシをその他の目的には使用しません。

このプロキシを通過するトラフィックの種類

このプロキシには、アウトバウンド HTTPS とセキュアな Web ソケット接続を処理する能力が必要です。また、これらの接続は基本認証を使用するか、認証なしで Expressway が発信できる必要があります。

プロキシの設定に必要な詳細情報

プロキシのアドレス、リッスンするポート、および基本認証のユーザ名とパスワード（プロキシが認証を必要とする場合）が必要です。

Expressway-E 上の Cisco Webex CA ルート証明書

Cisco Webex クラウド CA ルート証明書は Expressway ソフトウェアにパッケージ化されています。**[証明書の取得（Get certificates）]** をクリックすると、これらの詳細書を使用して着信証明書を検証できるようになります。この決定は、**[証明書の削除（Remove certificates）]** をクリックすることで必要に応じて撤回できます。

Expressway-E はこれらの CA を信頼することで、コラボレーション クラウドのサーバ 証明書を認証して一部の Expressway ベースのハイブリッド サービスに必要な暗号化された接続を確立できます。

（注） ハイブリッドサービス用に Expressway-E を登録することはできません。Cisco Webex クラウドに登録されている Expressway（またはクラスタ）へはセキュアなトラバーサル ゾーンによって接続される必要があります。

[証明書の取得（Get certificates）] をクリックすると、次の CA のルート証明書がインストールされます。

- O = The Go Daddy Group, Inc、OU = Go Daddy Class 2 Certification Authority
- O=GoDaddy.com, Inc., CN=Go Daddy Root Certificate Authority - G2
- O = QuoVadis Limited、CN = QuoVadis Root CA 2
- O = VeriSign, Inc.、OU = Class 3 Public Primary Certification Authority
- O=thawte, Inc., OU=Certification Services Division, OU=(c) 2006 thawte, Inc. - For authorized use only, CN=thawte Primary Root CA
- O=Baltimore, OU=CyberTrust, CN=Baltimore CyberTrust Root
- O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root CA

信頼できる CA のリストを手動で管理する場合は、**[メンテナンス（Maintenance）]** > **[セキュリティ（Security）]** > **[信頼できる CA 証明書（Trusted CA certificate）]** に移動します。詳細については、「信頼されている CA 証明書一覧の管理」を参照してください。

関連資料

- Cisco Webex 署名 CA
- Cisco Webex でサポートされている認証局

Cisco Webex エッジ

Webex Edge Connect の使用（Expressway-C なし）

X 12.5.5 からのビジネス間のケース（MRA ではない）については、Cisco Webex Edge Audio と Webex Edge Connect 製品を使用し、Expressway-C を使用せずに正常にテストされました。したがって、Expressway-E は、Expressway-C を使用せずに Cisco Unified Communications Manager に接続します。このシナリオでは、トラバーサルやファイアウォールは必要ありません。また、Expressway E は Webex Cloud を Cisco Unified Communications Manager に直接接続します。テスト対象の構成では、Cisco Unified Communications Manager と Expressway -E の間にある近隣ゾーンで、インターネットを介した標準的な Webex Edge Audio を使用しています。Webex ゾーンのメディア暗号化モードは、「On」 である必要があります（デフォルトは「[自動（Auto）]」です）。

このシナリオでは、インバウンド接続を内部ファイアウォールで開く必要があります。そのため、通常のデュアル ファイアウォール構成の標準の Expressway デプロイはサポートされて**いません**。Webex Edge Connect で使用するためのみを目的としています。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。