# モバイルおよびリモートアクセスの設定



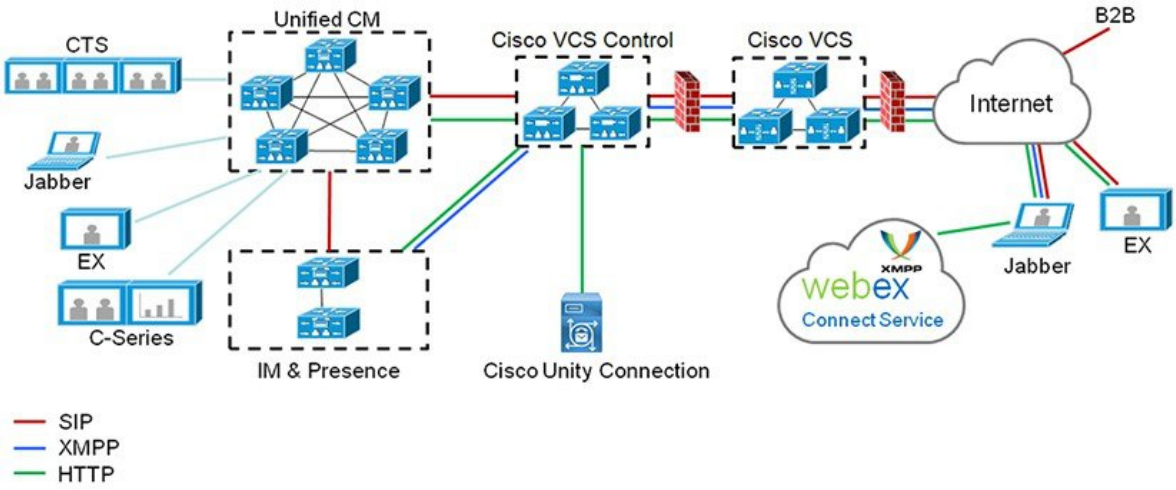
## モバイルおよびリモートアクセスの概要

Unified Communications Manager モバイルおよびリモートアクセスは、Cisco Collaboration Edge アーキテクチャの中核的なコンポーネントです。これを使用することで、Cisco Jabber などのエンドポイントで、エンドポイントがエンタープライズ ネットワーク内にない場合でも、Unified Communications Manager が提供する登録、コール制御、プロビジョニング、メッセージング、およびプレゼンス サービスを使用できます。Cisco Expressway は、モバイル エンドポイントをオンプレミス ネットワークに接続し、Unified CM の登録に対してセキュアなファイアウォール トラバースと回線側のサポートを提供します。

ソリューション全体で提供されるものは以下の通りです。

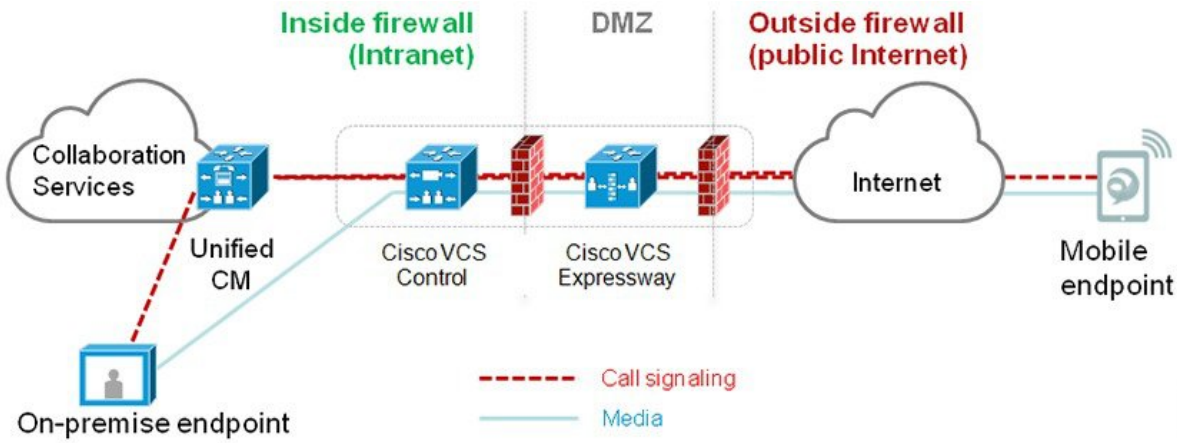
- オフプレミスアクセス：企業ネットワーク外においても、Jabber および EX/MX/SX シリーズ クライアントで一貫したエクスペリエンスを提供
- セキュリティ：セキュアな Business-to-Business（B2B）コミュニケーション
- クラウド サービス：エンタープライズ クラスの柔軟性と拡張性に優れたソリューションにより、さまざまな Cisco Webex 統合およびサービス プロバイダ オファリングに対応
- ゲートウェイと相互運用性サービス: メディアおよびシグナリングの正規化、非標準エンドポイントのサポート

図 *1 : Unified Communications* : モバイルおよびリモートアクセス




サードパーティのSIPまたはH.323デバイスはExpressway-Cに登録でき、必要に応じてSIPトランクを介して統合されたCM登録デバイスと相互運用することもできます。

図 *2 :* 一般的なコール フロー : シグナリングとメディア パス




- Unified CM は、モバイルとオンプレミスの両方のエンドポイントにコール制御を提供します。
- シグナリングは、モバイル エンドポイントと Unified CM の間で Expressway ソリューションを横断します。
- メディアは Expressway ソリューションを横断し、エンドポイント間で直接リレーされます。すべてのメディアが Expressway-C とモバイル エンドポイント間で暗号化されます。

## モバイルおよびリモートアクセスの設定

Cisco Jabber を使用してモバイルおよびリモートアクセス機能を有効にするには、**Unified Communications Manager** の [ユーザプロファイルの設定] ウィンドウでモバイルおよびリモー

トアクセスのユーザポリシーをセットアップします。モバイルおよびリモートアクセスのユーザ ポリシーは、Jabber 以外のエンドポイントでは必要ありません。

また、モバイルおよびリモートアクセスで Cisco Expressway を設定する必要もあります。詳細については、『Cisco Expressway を介したモバイルおよびリモートアクセスの導入ガイド』を参照してください。

# モバイルおよびリモートアクセスの前提条件

### Cisco Unified Communications Managerの要求

以下の要件が適用されます。

- 複数の Unified Communications Manager クラスタを導入する場合は、ILS ネットワークをセットアップします。
- モバイルおよびリモートアクセスでは、展開用の NTP サーバを設定する必要があります。ネットワーク用の NTP サーバが導入されていて、SIPエンドポイントの電話機 NTP リファレンスであることを確認してください。
- メディアパスを最適化するために ICE を導入する場合は、TURN および STUN サービスを提供できるサーバを導入する必要があります。

### DNS 要件

Cisco Expressway との内部接続には、次の Unified Communications Manager をポイントする、ローカルで解決可能な DNS SRV を設定します。

```
_cisco-uds._tcp&lt;domain&gt;
```

モバイルおよびリモートアクセスで使用するすべての Unified Communications ノードに対して、正引きと逆引きの両方のルックアップ用に内部 DNS レコードを作成する必要があります。これにより、IPアドレスまたはホスト名が FQDNの代わりに使用されている場合に、のノードを検索することができます。SRVレコードは、ローカルネットワークの外部で解決できないことを確認します。

### Cisco Expressway の要件

この機能を使用するには、Unified Communications Manager と Cisco Expressway を統合する必要があります。モバイルおよびリモート アクセス用の Cisco Expressway 設定の詳細については、『Cisco Expressway 導入ガイド』の「モバイルおよびリモート アクセス」を参照してください。

Cisco Jabber を使用したモバイルおよびリモートアクセスのアクセス ポリシーをサポートする Expressway の最小リリースは X8.10 です。

### 証明書の前提条件

Unified Communications Manager、IM and Presence Service、および Cisco Expressway-C の間で証明書を交換する必要があります。シスコでは、各システムで同じ CA による CA 署名付き証明書を使用することを推奨します。その場合、次のようになります。

- 各システムに CA ルート証明書チェーンをインストールします（Unified Communications Manager および IM and Presence Service サービスの場合は tomcat 信頼ストアに証明書チェーンをインストールします）。
- Unified Communications Manager の場合は、CA 署名付き tomcat（AXL および UDS トラフィック用）証明書と Cisco CallManager （SIP 用）証明書を要求するための CSR を発行します。
- IM and Presence Service の場合は、CA 署名付き tomcat 証明書を要求するための CSR を発行します。

（注） 別の CA を使用する場合は、各 CA のルート証明書チェーンを Unified Communications Manager、IM and Presence Service サービス、および Expressway-C にインストールする必要があります。

（注） また、 Unified Communications ManagerIM and Presence Serviceとサービスの両方に自己署名証明書を使用することもできます。この場合は、Unified Communications Manager 用の tomcat 証明書と Cisco CallManager 証明書、IM and Presence Service サービス用の tomcat 証明書を Expressway-C にアップロードする必要があります。

# モバイルおよびリモートアクセスの設定タスク フロー

モバイルおよびリモートアクセス エンドポイントを展開するには、これらのタスクを Unified Communications Manager で実行します。

### 手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| **ステップ 1** | Cisco AXL Web Service の有効化 （6 ページ） | パブリッシャ ノードで Cisco AXL Web サービスが有効になっていることを確認します。 |
| **ステップ 2** | ビデオの最大セッションビットレートの設定 （6 ページ） | **オプション**モバイルおよびリモートアクセスのエンドポイントのリージョン固有の設定を指定します。例えば、モバイルおよびリモートアクセスのエンドポイントでビデオを使用する予定がある場合 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | は、**[ビデオコールの最大セッションビットレート]** 設定を増やすのが望ましい場合があります。これは、ビデオ エンドポイントによっては、デフォルト設定の 384 kbps では低すぎる場合があるためです。 |
| **ステップ 3** | モバイルおよびリモートアクセスのデバイス プール設定 （7 ページ） | モバイルおよびリモートアクセスのエンドポイントが使用するデバイス プールに [日時グループ] と [リージョンの設定] を割り当てます。 |
| **ステップ 4** | ICE の設定 （7 ページ） | （**オプション**）ICEはオプションの導入であり、モバイルおよびリモートアクセスおよびTURNサービスを使用して、MRAコールの利用可能なメディアパスを分析し、最適なパスを選択します。ICE を使用すると、コール セットアップ時間が増える可能性がありますが、モバイルおよびリモートアクセス コールの信頼性は向上します。 |
| **ステップ 5** | モバイルおよびリモートアクセス用の電話機セキュリティ プロファイルの設定 （9 ページ） | モバイルおよびリモートアクセスのエンドポイントで使用する電話セキュリティ プロファイルを設定するには、この手順を使用します。 |
| **ステップ 6** | Cisco Jabber ユーザのモバイルおよびリモートアクセスのアクセス ポリシーの設定 （10 ページ） | Cisco Jabber のみ。Cisco Jabber のユーザにモバイルおよびリモートアクセスのアクセスポリシーをセットアップします。Cisco Jabber ユーザは、モバイルおよびリモートアクセスの機能を使用するために、ユーザ プロファイル内でモバイルおよびリモートアクセスのアクセスを使用して有効にする必要があります。 |
| **ステップ 7** | モバイルおよびリモートアクセスのユーザ設定 （12 ページ） | Cisco Jabber のユーザに対しては、セットアップするユーザポリシーをエンドユーザの設定に適用する必要があります。 |
| **ステップ 8** | モバイルおよびリモートアクセス用のエンドポイントを設定します。 （12 ページ） | モバイルおよびリモートアクセス機能を使用するエンドポイントを設定およびプロビジョニングします。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 9 | Cisco Expresswayのモバイルおよびリモートアクセスの設定 （12 ページ） | モバイルおよびリモート アクセスに対して Cisco Expressway を設定します。 |

# Cisco AXL Web Service の有効化

パブリッシャ ノードで Cisco AXL Web サービスが有効になっていることを確認します。

**手順**

**ステップ 1** [Cisco Unified Serviceability] から、以下を選択します。 **[ツール（Tools）] > [サービス アクティベーション（Service Activation）]** を選択します。

**ステップ 2** [サーバ（Server）] ドロップダウン リストからパブリッシャ ノードを選択し、[移動（Go）] をクリックします。

**ステップ 3** **データベースと管理サービス**の下で、**Cisco AXL Web Service** が**有効になっていること**を確認します。

**ステップ 4** サービスがアクティブ化されていない場合は、対応する**チェック**ボックスをオンにし、[保存(Save)] をクリックしてサービスをアクティブにします。

# ビデオの最大セッションビットレートの設定

モバイルおよびリモートアクセスのエンドポイントのリージョンの設定を指定します。多くの場合はデフォルト設定で十分と思われますが、モバイルおよびリモートアクセスのエンドポイントでビデオを使用する予定がある場合は、[リージョンの設定] で **[ビデオコールの最大セッションビットレート]** を上げる必要があります。DX シリーズなどの一部のビデオ エンドポイントでは、デフォルト設定の 384 kbps では低すぎる場合があります。

**手順**

**ステップ 1** [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。 **[システム（System）] > [リージョン情報（Region Information）] > [リージョン（Region）]** を選択します。

**ステップ 2** 次のいずれかの操作を実行します。

- 既存のリージョン内のビットレートを編集するには、[検索（Find）] をクリックしてリージョンを選択します。
- **[新規追加（Add New）]**をクリックして新しいパーティションを作成します。

**ステップ 3** [他のリージョンとの関係を変更（Modify Relationship to other Region] 領域で、[ビデオコールの最大セッションビットレート（Maximum Session Bit Rate for Video Calls）] の新しい設定値を入力します。たとえば、6000 kbps のようになります。

**ステップ 4** [リージョンの設定（Region Configuration）] ウィンドウで、その他のフィールドを設定します。フィールドと設定オプションの詳細については、オンライン ヘルプを参照してください。。

**ステップ 5** **[保存]** をクリックします。

# モバイルおよびリモートアクセスのデバイス プール設定

新しいリージョンを作成した場合は、モバイルおよびリモートアクセスのエンドポイントが使用するデバイス プールにリージョンを割り当てます。

**手順**

**ステップ 1** [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。 **[システム（System）]** > **[デバイス プール（Device Pool）]**。

**ステップ 2** 次のいずれかを実行します。

- **[検索（Find）]**をクリックし、既存のデバイスグループを選択します。
- [新規追加（Add New）] をクリックして新しいデバイス プールを作成します。

**ステップ 3** **デバイスプール名**を入力します。

**ステップ 4** 冗長**Cisco Unified Communications Managerグループ**を選択します。

**ステップ 5** 設定した**日付と時刻**グループを割り当てます。このグループには、モバイルおよびリモートアクセスのエンドポイント用に設定した電話用NTP参照が含まれています。

**ステップ 6** [リージョン] ドロップダウン リストから、モバイルおよびリモートアクセス用に設定したリージョンを選択します。

**ステップ 7** [デバイスプールの設定（Device Pool Configuration）] ウィンドウで、残りのフィールドに入力します。 フィールドと設定オプションの詳細については、オンライン ヘルプを参照してください。

**ステップ 8** **[保存]** をクリックします。

# ICE の設定

モバイルおよびリモートアクセス コールの設定を処理するためにICEを導入する場合は、この手順を使用します。ICEはオプションの導入であり、モバイルおよびリモートアクセスおよびTURNサービスを使用して、MRAコールの利用可能なメディアパスを分析し、最適なパスを選択します。ICE を使用すると、コールセットアップ時間が増える可能性がありますが、モバイルおよびリモートアクセス コールの信頼性は向上します。

### 始める前に

ICEを導入する方法を決定します。電話グループに対するICEは、[共通の電話プロファイルの設定（Common Phone Profile Configuration）] で個別の Cisco Jabber デスクトップ デバイスに対して設定するか、すべての電話に適用するシステム全体のデフォルト設定を使用して設定します。

フォールバックメカニズムとして、ICE は、TURNサーバを使用してメディアをリレーできます。TURNサーバが導入されていることを確認してください。

### 手順

**ステップ 1** Cisco Unified CMの管理：

- システム**の** > **デフォルトを** ICE に設定するには、[システム (Enterprise Phone)] を選択します。
- **デバイス** > **デバイスの設定** > **共通電話プロファイル**を選択して、端末グループにICEを設定し、編集するプロファイルを選択します。
- 個別の Cisco Jabber デスクトップ エンドポイント用の ICE を設定し、編集するエンドポイントを選択するには、**[デバイス（Device）]** > **[電話機（Phone）]** を選択します。

**ステップ 2** 下方向にスクロールして、[対話型接続の確立（ICE）（Interactive Connectivity Establishment (ICE)）] セクションに移動します。

**ステップ 3** [ICE] ドロップダウン リストを [有効（Enabled）] に設定します。

**ステップ 4** **デフォルトの候補タイプ**を設定する：

- **[**ホスト (host)]: ホストデバイスの IP アドレスを選択することによって得られる候補。これはデフォルトです。
- **サーバ再帰**: STUN要求の送信によって取得されるIPアドレスとポートの候補。多くの場合、これはNATのパブリックIPアドレスを表す場合があります。
- **中継**: TURNサーバから取得したIPアドレスとポートの候補。IPアドレスとポートは、TURNサーバによってメディアが中継されるように、TURNサーバに常駐しています。

**ステップ 5** [サーバの再帰アドレス（Server Reflexive Address）] ドロップダウン リストから、このフィールドを [有効（Enabled）] または [無効（Disabled）] に設定することで、STUN と同様のサービスを有効化するかかどうかを選択します。デフォルトの候補としてサーバRelexiveを設定した場合は、このフィールドを有効に設定する必要があります。

**ステップ 6** プライマリサーバーとセカンダリサーバーのipアドレスまたはホスト名を入力します。

**ステップ 7** TURN Server **のトランスポート**タイプを [**自動 (default)]**(**default**setting)、UDP 、TCP、または TLS に設定します。

**ステップ 8** ターンサーバーに**ユーザ名**と**パスワード**を入力します。

**ステップ 9** [保存（Save）] をクリックします。

（注） 共通の電話プロファイル用に ICE を設定した場合は、電話機を使用して、そのプロファイルを使用できるようにする共通の電話プロファイルに電話機を関連付ける必要があります。[電話の設定（Phone Configuration）] ウィンドウから、プロファイルを電話に適用できます。

# モバイルおよびリモートアクセス用の電話機セキュリティプロファイルの設定

モバイルおよびリモートアクセスのエンドポイントで使用する電話セキュリティ プロファイルを設定するには、この手順を使用します。

**手順**

**ステップ 1** [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。 **[システム（System）]** > **[セキュリティ（Security）]** > **[電話セキュリティ プロファイル（Phone Security Profile）]** を選択します。

**ステップ 2** [新規追加] をクリックします。

**ステップ 3** [電話のセキュリティプロファイルのタイプ（Phone Security Profile Type）] ドロップダウン リストから、デバイス タイプを選択します。たとえば、Jabber アプリケーションであれば **Cisco Unified Client Service Framework** を選択できます。

**ステップ 4** [次へ（Next）] をクリックします。

**ステップ 5** プロファイルの**名前**を入力します。モバイルおよびリモートアクセスの場合、名前はFQDN形式である必要があり、エンタープライズ ドメインを含める必要があります。

**ステップ 6** [デバイスのセキュリティモード（Device Security Mode）] ドロップダウン リストから、[暗号化（Encrypted）] を選択します。

（注） このフィールドは、[暗号化（Encrypted）]に設定する必要があります。そうでない場合、Expressway が通信を拒否します。

**ステップ 7** [トランスポートタイプ（Transport Type）] を [TLS] に設定します。

**ステップ 8** このオプションを有効化した電話機ではモバイルおよびリモートアクセスが機能しないため、次の電話機では **[TFTP暗号化設定]** チェックボックスをオフのままにします。DX シリーズ、IP Phone 7800、または IP Phone 8811、8841、8845、8861、および 8865

**ステップ 9** [電話のセキュリティプロファイルの設定（Phone Security Profile Configuration）] ウィンドウで、残りのフィールドを設定します。 フィールドと設定オプションの詳細については、オンライン ヘルプを参照してください。

**ステップ 10** [保存（Save）] をクリックします。

（注） 各モバイルおよびリモートアクセスのエンドポイントの電話機の設定にこのプロファイルを適用する必要があります。

# Cisco Jabber ユーザのモバイルおよびリモートアクセスのアクセス ポリシーの設定

Cisco Jabber のユーザにモバイルおよびリモートアクセスのアクセスポリシーを設定するには、次の手順を使用します。Cisco Jabber ユーザは、モバイルおよびリモートアクセスの機能を使用するために、ユーザ プロファイル内でモバイルおよびリモートアクセスのアクセスを使用して有効にする必要があります。Cisco Jabber を使用したモバイルおよびリモートアクセスのアクセス ポリシーをサポートする Expressway の最小リリースは X8.10 です。

（注） モバイルおよびリモートアクセスのポリシーは、Jabber 以外のユーザには必要ありません。

ユーザ プロファイルの詳細については、『Cisco Unified Communications Manager システム設定ガイド』の「ユーザ プロファイルの概要」章を参照してください。

## 手順

**ステップ 1** [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。 **[ユーザ管理] > [ユーザ設定] > [ユーザ プロファイル]** を選択します。

**ステップ 2** [新規追加] をクリックします。

**ステップ 3** ユーザ プロファイルの [名前（Name）] および [説明（Description）] を入力します。

**ステップ 4** [ユニバーサル デバイス テンプレート（Universal Device Template）] を、ユーザの [デスク フォン（Desk Phones）]、[モバイルおよびデスクトップ デバイス（Mobile and Desktop Devices）]、および [リモート接続先/デバイス プロファイル（Remote Destination/Device Profiles）] に割り当てます。

**ステップ 5** [ユニバーサル回線テンプレート（Universal Line Template）] を割り当て、このユーザプロファイルのユーザの電話回線に適用します。

**ステップ 6** このユーザプロファイルのユーザに自分の電話機をプロビジョニングするセルフプロビジョニング機能の使用を許可するには、次の手順を実行します

a) **[エンドユーザの電話機のプロビジョニングを許可（Allow End User to Provision their own phones）]**のチェックボックスをオンにします。

b) [エンドユーザがプロビジョニングする電話機数を制限（Limit Provisioning once End User has this many phones）] フィールドに、ユーザがプロビジョニングできる電話の最大数を入力します。最大値は 20 です。

c) このプロファイルに関連付けられたユーザに、別のユーザがすでに所有しているデバイスを移行または再割り当てする権限があるかどうかを判断するには、[すでに別のエンドユー

ザに割り当てられた電話機のプロビジョニングを許可する（Allow Provisioning of a phone already assigned to a different End User）] チェックボックスをオンにします。デフォルトでは、このチェックボックスはオフになっています。

**ステップ 7** このユーザプロファイルに関連付けられた Cisco Jabber ユーザがモバイルおよびリモートアクセス機能を使用できるようにするには、**[モバイルおよびリモートアクセスの有効化]**チェックボックスをオンにします。

（注）
- デフォルトでは、このチェックボックスはオンです。このチェックボックスをオフにすると、[Jabber ポリシー（Jabber Policies）] セクションが無効になり、サービスクライアントポリシーオプションは、デフォルトで選択されません。
- この設定は、OAuth 更新ログインを使用している Cisco Jabber のユーザにのみ必須です。Jabber ユーザではない場合、この設定を行わずともモバイルおよびリモートアクセス機能を使用できます。モバイルおよびリモートアクセス機能は、Jabber モバイルおよびリモートアクセスのユーザにのみ適用され、他のエンドポイントやクライアントには適用されません。

**ステップ 8** このユーザプロファイルに Jabber ポリシーを割り当てます。**[Jabber デスクトップクライアントポリシー(Jabber Desktop Client Policy)]**と**[Jabberモバイルクライアントポリシー(Jabber Mobile Client Policy)]**のドロップダウンリストから、次のオプションのいずれかを選択します。

- サービスなし：このポリシーは、すべての Cisco Jabber サービスへのアクセスを禁止します。
- IMとプレゼンスのみ：このポリシーは、インスタントメッセージとプレゼンス機能のみを有効にします。
- IM とプレゼンス、音声とビデオ コール：このポリシーは音声やビデオ デバイスを使うすべてのユーザに対して、インスタントメッセージ、プレゼンス、ボイスメールと会議機能を有効化します。これがデフォルトのオプションです。

（注） Jabber デスクトップクライアントには Windows 版 Cisco Jabber および Mac 版 Cisco Jabber が含まれています。Jabber モバイルクライアントには、iPad/iPhone ユーザ用 Cisco Jabber および Android 版 Cisco Jabber が含まれています。

**ステップ 9** このユーザ プロファイルのユーザが Cisco Unified Communications セルフケア ポータルで Extension Mobility または Extension Mobility Cross Cluster の最大ログイン時間を設定できるようにするには、[エンドユーザにエクステンションモビリティの最大ログイン時間の設定を許可する（Allow End User to set their Extension Mobility maximum login time）] チェックボックスをオンにします。

（注） デフォルトでは [エンドユーザにエクステンションモビリティの最大ログイン時間の設定を許可する（Allow End User to set their Extension Mobility maximum login time）] チェックボックスはオフになっています。

**ステップ 10** **[保存]** をクリックします。

# モバイルおよびリモートアクセスのユーザ設定

Cisco Jabber のユーザの場合、設定したモバイルおよびリモートアクセスのアクセスポリシーは、LDAP 同期中に Cisco Jabber ユーザに関連付ける必要があります。エンド ユーザをプロビジョニングする方法の詳細については、Cisco Unified Communications Manager システム設定ガイド の「エンド ユーザの設定」項を参照してください。

# モバイルおよびリモートアクセス用のエンドポイントを設定します。

モバイルおよびリモートアクセス用のエンドポイントをプロビジョニングし、設定します。

- Cisco Jabber クライアントについては、Cisco Unified Communications Manager システム設定ガイド の「*Cisco Jabber* 構成タスク フロー」項を参照してください。
- その他のエンドポイントについては、Cisco Unified Communications Manager システム設定ガイド の「エンドポイント デバイスの設定」項を参照してください。

# Cisco Expresswayのモバイルおよびリモートアクセスの設定

モバイルおよびリモートアクセス用の Cisco Expressway の設定方法に関しては、『Cisco Expressway 導入ガイド』の「モバイルおよびリモートアクセス」を参照してください。

# 軽量キープアライブを使用した MRA フェールオーバー

エンドポイント登録の場合、高い可用性を備えた Cisco Webex と Cisco Jabber は、Cisco Expressway-E、Cisco Expressway-C、および登録パス内のCisco Unified Communications Manager Administrationといったようなネットワーク要素の障害を検出し、次に利用可能なパスを経由して Unified CM に再登録するために修正措置を取る事が可能になります。

エンドポイントは軽量の STUN キープアティブ メッセージを送信し、登録パスでの接続性を確認します。Unified Communications Managerが軽量 STUN キープアティブ メッセージを受信すると、Cisco Expressway-C IP を検証してメッセージに応答します。Unified CM は、他の IP アドレスから受信された場合、STUN キープアティブ メッセージを破棄します。

登録パス内のノードが失敗した場合、エンドポイントは受信した軽量の STUN キープアティブ応答によって失敗を学習し、今後のメッセージ用に別のルートパスを選択します。このサービスは、ユーザが機能停止や他のメンテナンス モードに関係なく、スムーズで継続的な着信通話および発信通話を実行するのに役立ちます。

詳細については、『Cisco Expressway を介したモバイルおよびリモートアクセスの導入ガイド』を参照してください。