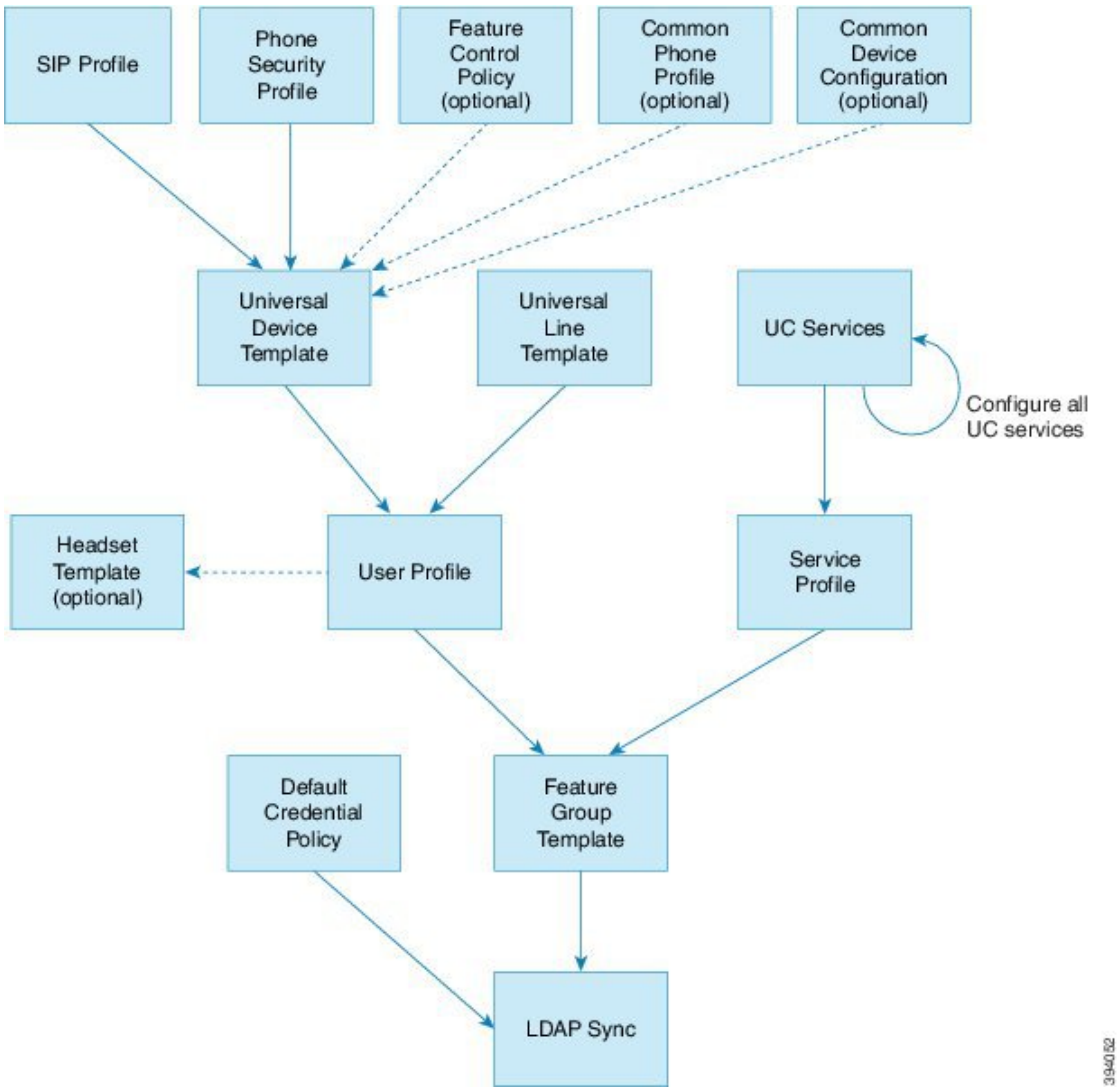
プロビジョニング プロファイルの設定

プロビジョニング プロファイルの概要

Unified Communications Manager では、新規ユーザに割り当てることができる一連のプロファイルとテンプレートが用意されています。 これらのプロファイルと共通設定をあらかじめ設定しておくと、新しいユーザをプロビジョニングしてデバイスを割り当てるときに、適用される設定に基づいてユーザとデバイスが自動的に設定されます。

ユーザをプロビジョニングするときは、必要な設定が含まれるユーザ プロファイルとサービス プロファイルにそのユーザを関連付けます。 さらに、ユーザ用のデバイスを追加するときに、そのユーザのユーザ プロファイルに関連付けられているユニバーサル回線テンプレートとユニバーサル デバイス テンプレートを使用して、デバイスとディレクトリ番号がすばやく設定されます。

次のプロファイルとテンプレートを使用して、ユーザのニーズに基づいて、ユーザとエンドポイントに共通の設定を適用できます。



プロビジョニング プロファイルのタスク フロー

プロビジョニングするユーザとデバイスの数が多い場合は、特定のグループ（たとえばカスタマー サポート）内のユーザに適用されるテンプレートと共通設定を使用してユーザ プロファイルとサービス プロファイルを設定することで、設定プロセスを簡略化できます。

ユーザをプロビジョニングするときは、必要な設定が含まれるユーザプロファイルとサービスプロファイルにそのユーザを関連付けます。 さらに、ユーザ用のデバイスを追加するときに、そのユーザのユーザプロファイルに関連付けられているユニバーサル回線テンプレートとユニバーサル デバイス テンプレートを使用して、デバイスとディレクトリ番号がすばやく設定されます。

次のプロファイルとテンプレートを使用して、ユーザのニーズに基づいて、ユーザとエンドポイントに共通の設定を適用できます。

手順

	コマンドまたはアクション	目的
ステップ 1	SIP プロファイルの設定 （4 ページ）	展開する SIP エンドポイントに関連付けられる共通 SIP 設定を設定します。
ステップ 2	電話機のセキュリティ プロファイルの設定 （5 ページ）	プロビジョニングされたエンドポイントに割り当てるセキュリティ プロファイルを設定します。 TLS および TFTP 暗号化などの設定を割り当てます。
ステップ 3	機能管理ポリシーの作成 （6 ページ）	（オプション）このポリシーを使用すると、特定の機能を有効化して、電話機のソフトキーの外観を制御できます。
ステップ 4	共通の電話プロファイルの作成 （7 ページ）	（オプション）このプロファイルを使用して、エンドポイントのグループに割り当てることができるプロファイルに、TFTP データおよび製品固有の設定のデフォルト値を割り当てます。
ステップ 5	共通デバイス設定の構成 （8 ページ）	（オプション）この設定を使用して、エンドポイントにユーザ固有の設定と IPv6 設定を割り当てます。
ステップ 6	ユニバーサル デバイス テンプレートの設定 （9 ページ）	このテンプレートには、新しくプロビジョニングされた電話を設定するために使用される共通設定が含まれます。設定したプロファイルをこのテンプレートに割り当てることもできます。
ステップ 7	ユニバーサル回線テンプレートの設定 （10 ページ）	このテンプレートには、新しくプロビジョニングされた内線番号を設定するために使用される共通設定が含まれます。 内線用のエンタープライズ番号および E.164 番号も設定できます。
ステップ 8	ユーザ プロファイルの設定 （11 ページ）	デバイス テンプレート、回線テンプレート、および新しくプロビジョニングされるユーザの共通設定を使用して、ユーザ プロファイルを設定します。
ステップ 9	ヘッドセットテンプレートの設定 （12 ページ）	（オプション）シスコ ヘッドセットを使用する場合は、ヘッドセットテンプ

	コマンドまたはアクション	目的
		レートを設定して、設定済みのユーザプロファイルに割り当てます。
ステップ 10	UC サービスの設定 （14 ページ）	IM and Presence Service およびディレクトリ サービスなどの UC サービスを設定します。
ステップ 11	サービス プロファイルの設定 （15 ページ）	プロビジョニングされたユーザに割り当てる UC サービスを含む、サービスプロファイルを作成します。
ステップ 12	機能グループテンプレートの設定 （15 ページ）	LDAP 同期の場合は、LDAP で同期されたユーザに割り当てることができる機能グループテンプレートに、ユーザプロファイルとサービスプロファイルを追加します。
ステップ 13	デフォルトのクレデンシャルポリシーの設定 （16 ページ）	新しくプロビジョニングされるユーザに割り当てるクレデンシャルポリシーを設定します。

次のタスク

- 新しいユーザをプロビジョニングするための LDAP 同期のセットアップ
- LDAP を導入していない場合は、一括管理を使用してユーザを一括でプロビジョニングできます。

SIP プロファイルの設定

共通 SIP 設定を使用して SIP プロファイルを設定するには、この手順を使用します。設定した SIP プロファイルは、SIP デバイスに割り当てることができます。

手順

ステップ 1 Cisco Unified CM Administration で、[デバイス（Device）]>[デバイスの設定（Device Settings）]>[SIPプロファイル（SIP Profile）]を選択します。

ステップ 2 次のいずれかの手順を実行します。

- 既存のプロファイルを編集するには、[検索（Find）]をクリックし、SIP プロファイルを選択します。
- 新しいプロファイルを作成するには、[新規追加] をクリックします。

ステップ 3 プロファイル名を入力します。

ステップ 4 URI ダイヤリングを展開する場合は、[ダイヤル文字列の解釈（Dial String Interpretation）]を設定して、コールをディレクトリ URI または電話番号として処理するかどうかをシステムに指示します。

ステップ 5 [電話で使用されるパラメータ（Parameters Used in Phone）]の下にある DSCP 設定項目を入力して、このプロファイルを使用するコールのタイプに対する QoS 処理を定義します。

ステップ 6 （任意）正規化スクリプトを割り当てる必要がある場合は、[正規化スクリプト（Normalization Script）] ドロップダウン リストからいずれかのデフォルト スクリプトを選択します。

（注） 独自のスクリプトを作成することもできます。 詳細については、『*Cisco Unified Communications Manager* 機能設定ガイド』を参照してください。

ステップ 7 このプロファイルで IPv4 と IPv6 の両方のスタックを同時にサポートする場合は、[ANATの有効化（Enable ANAT）]チェックボックスをオンにします。

ステップ 8 ユーザがプレゼンテーションを共有できるようにするには、[BFCP を使用するプレゼンテーションの共有を許可（Allow Presentation Sharing using BFCP）]チェックボックスをオンにします。

ステップ 9 [SIP プロファイルの設定（SIP Profile Configuration）] ウィンドウで、残りのフィールドを入力します。 フィールドとその設定の詳細については、オンライン ヘルプを参照してください。

ステップ 10 **[保存]** をクリックします。

電話機のセキュリティ プロファイルの設定

エンドポイントの TLS シグナリング、CAPF、ダイジェスト認証の要件などのセキュリティ機能を有効にする場合は、エンドポイントに適用できる新しいセキュリティプロファイルを設定する必要があります。

（注） デフォルトでは、プロビジョニングされたデバイスに SIP phone セキュリティプロファイルを適用しない場合、デバイスは非セキュアプロファイルを使用します。

手順

ステップ 1 Cisco Unified CM Administration から、**[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）]** の順に選択します。

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 [ユニバーサルデバイステンプレート（Universal Device Template）] を選択し、デバイステンプレートを使用してプロビジョニングする際に使用できるプロファイルを作成します。

（注） 必要に応じて、特定のデバイス モデルのセキュリティ プロファイルを作成することもできます。

ステップ 4 プロトコルを選択します。

ステップ 5 [Name] フィールドにプロファイルの適切な名前を入力します。

ステップ 6 TLS シグナリングを使用してデバイスに接続する場合は、[デバイスのセキュリティモード（Device Security Mode）]を [認証済み（Authenticated）]または [暗号化（Encrypted）]に設定し、[トランスポートタイプ（Transport Type）] を [TLS]に設定します。

ステップ 7 （任意）電話でダイジェスト認証を使用する場合は、[OAuth認証の有効化（Enable OAuth Authentication）]チェックボックスをオンにします。

ステップ 8 （任意）暗号化された TFTP を使用する場合は、[TFTP暗号化設定（TFTP Encrypted Config）] チェックボックスをオンにします。

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入力します。 フィールドとその設定の詳細については、オンラインヘルプを参照してください。

ステップ 10 **[保存]** をクリックします。

機能管理ポリシーの作成

機能管理ポリシーを作成するには、次の手順に従います。 このポリシーを使用して、特定の機能を有効化または無効化し、電話に表示されるソフトキーの外観を制御します。

手順

ステップ 1 Cisco Unified CM Administration から、**[デバイス（Device）]** > **[デバイスの設定（Device Settings）]** > **[機能管理ポリシー（Feature Control Policy）]** を選択します。

ステップ 2 次のいずれかの作業を実行します。

- 既存のポリシーの設定を変更するには、検索条件を入力して **[検索（Find）]** をクリックし、結果のリストからポリシーを選択します。
- 新しいポリシーを追加するには、**[新規追加] をクリックします。**

[機能管理ポリシーの設定（Feature Control Policy Configuration）] ウィンドウが表示されます。

ステップ 3 [名前（Name）] フィールドに機能管理ポリシーの名前を入力します。

ステップ 4 [説明（Description）] フィールドに、この機能管理ポリシーの説明を入力します。

ステップ 5 [機能管理セクション（Feature Control Section）]でリストされている各機能に対して、システムデフォルトをオーバーライドするか、次の設定を有効/無効にするかを選択します。

- デフォルトで有効な機能の設定を無効にする場合は、[デフォルトをオーバーライド（Override Default）]チェックボックスをオンにして、[設定を有効にする（Enable Setting）]チェックボックスをオフにします。
- デフォルトで無効な機能の設定を有効にする場合は、[デフォルトをオーバーライド（Override Default）]チェックボックスをオンにして、[設定を有効にする（Enable Setting）]チェックボックスをオンにします。

ステップ 6 **[保存]** をクリックします。

共通の電話プロファイルの作成

共通の電話プロファイルは、そのプロファイルを使用する電話について、TFTP データおよび製品固有の設定のデフォルト値を設定するために使用できる、オプションのプロファイルです。

手順

ステップ 1 Cisco Unified CM Administration から、[デバイス（Device）]>[デバイスの設定（Device Settings）]>[共通の電話プロファイル（Common Phone Profile）]メニューパスを選択して、共通の電話プロファイルを設定します。

ステップ 2 [新規追加] をクリックします。

ステップ 3 プロファイル**名**を入力します。

ステップ 4 プロファイルの [**説明**] を入力します。

ステップ 5 このプロファイルを使用する電話に対して [機能管理ポリシー（Feature Control Policy）を設定する場合は、ドロップダウン リストからポリシーを選択します。

ステップ 6 [共通の電話プロファイルの設定（Common Phone Profile Configuration）]ウィンドウで、残りのフィールドを設定します。 フィールドとその設定の詳細については、オンライン ヘルプを参照してください。

ステップ 7 [製品固有の設定レイアウト（Product-Specific Configuration Layout）] の下にあるフィールドを設定します。 フィールドの説明については、[?] をクリックして、フィールド固有のヘルプを参照してください。

ステップ 8 （任意）モバイルおよびリモートアクセス電話用に Interactive Connectivity Establishment（ICE）を有効化する場合、次の手順を実行します。

a) [ICE] ドロップダウンを [有効（Enabled）]に設定します。

b) [デフォルト候補タイプ（Default Candidate Type）]を次のいずれかに設定します。

- **[**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 アドレスを表している可能性があります。
- **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。

c) 残りの ICE フィールドを設定します。

ステップ 9 **[保存]** をクリックします。

共通デバイス設定の構成

一般的なデバイス構成は、オプションのユーザ固有特徴属性のセットを含む。 IPv6 を導入している場合は、この設定を使用して SIP トランクまたは SCCP 電話に IPv6 優先設定を割り当てることができます。

手順

ステップ 1 Cisco Unified CM Administration から、**[デバイス（Device）]** > **[デバイスの設定（Device Settings）]** > **[共通デバイス設定（Common Device Configuration）]** 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 SIP トランク、SIP 電話または SCCP 電話の場合、[IPアドレッシングモード（IP Addressing Mode）]ドロップダウン リストの値を選択します。

- [IPv4 のみ（IPv4 Only）]—デバイスはメディアやシグナリングに IPv4 アドレスだけを使用します。
- [IPv6 のみ（IPv6 Only）]—デバイスはメディアやシグナリングに IPv6 アドレスだけを使用します。
- [IPv4 および IPv6（IPv4 and IPv6）]—（デフォルト）デバイスはデュアルスタック デバイスで、利用できる IP アドレスのタイプを使用します。 両方の IP アドレスのタイプがデバイスに設定されている場合、デバイスのシグナリングには、[シグナリグ用 IP アドレッシング モード優先設定（IP Addressing Mode Preference for Signaling）]設定を使用し、メディア デバイスには、[メディア用 IP アドレッシング モード優先設定（IP Addressing Mode Preference for Media）]エンタープライズ パラメータの設定を使用します。

ステップ 4 前のステップでIPv6を設定する場合は、[シグナリング(シグナリング)] ドロップダウンリストの ip アドレス指定モードの ip アドレス設定を次のように設定します。

- [IPv4（IPv4）]—デュアル スタック デバイスでシグナリングに IPv4 アドレスを優先して使用します。
- [IPv6（IPv6）]—デュアル スタック デバイスでシグナリングに IPv6 アドレスを優先して使用します。

- [システム デフォルトを使用（Use System Default）]—デバイスは、[シグナリグ用 IP アドレッシング モード優先設定（IP Addressing Mode Preference for Signaling）]エンタープライズ パラメータの設定を使用します。

ステップ 5 **[共通デバイス構成（Common Device Configuration）]** 画面で、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、システムのオンライン ヘルプを参照してください。

ステップ 6 **[保存]** をクリックします。

ユニバーサル デバイス テンプレートの設定

ユニバーサル デバイス テンプレートを使用すると、新しくプロビジョニングしたデバイスに簡単に設定を適用できます。 プロビジョニングされたデバイスは、ユニバーサル デバイス テンプレートの設定を使用します。 さまざまなユーザ グループのニーズを満たすために、異なるデバイス テンプレートを設定できます。 設定したプロファイルをこのテンプレートに割り当てることもできます。

手順

ステップ 1 Cisco Unified CM Administration で、**[ユーザの管理（User Management）] > [ユーザ/電話の追加（User/Phone Add）] > [ユニバーサル デバイス テンプレート（Universal Device Template）]** 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 次の必須フィールドに入力します。

a) テンプレートの [デバイスの説明（Device Description）]を入力します。
b) [デバイスプールタイプ（Device Pool Type）]をドロップダウン リストから選択します。
c) [デバイスのセキュリティプロファイル（Device Security Profile）]をドロップダウン リストから選択します。
d) [SIPプロファイル（SIP Profile）]をドロップダウンリストから選択します。
e) [電話ボタンテンプレート（Phone Button Template）]をドロップダウンリストから選択します。

ステップ 4 [ユニバーサルデバイステンプレートの設定（Universal Device Template Configuration）]ウィンドウで、残りのフィールドを入力します。 フィールドの説明については、オンラインヘルプを参照してください。

ステップ 5 [電話の設定（Phone Settings）]で、次の任意指定のフィールドを入力します。

a) [共通の電話プロファイル（Common Phone Profile）]を設定した場合は、そのプロファイルを割り当てます。
b) [共通デバイス設定（Common Device Configuration）]を設定した場合は、その設定を割り当てます。

c) [機能管理ポリシー（Feature Control Policy）]を設定した場合は、そのポリシーを割り当てます。

ステップ 6 **[保存]** をクリックします。

ユニバーサル回線テンプレートの設定

ユニバーサル回線テンプレートを使用すると、新しく割り当てられたディレクトリ番号に共通の設定を簡単に適用できます。 さまざまなユーザ グループのニーズに合わせて、異なるテンプレートを設定します。

手順

ステップ 1 Cisco Unified CM Administration で、**[ユーザ管理（User Management）]** > **[ユーザ/電話の追加（User/Phone Add）]** > **[ユニバーサル回線テンプレート（Universal Line Template）]** 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 [ユニバーサル回線テンプレートの設定（Universal Line Template Configuration）]ウィンドウで各フィールドを設定します。フィールドとその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 4 代替番号を使用したグローバル ダイヤル プラン レプリケーションを展開する場合は、[エンタープライズ代替番号（Enterprise Alternate Number）]セクションと [+E.164代替番号（+E.164 Alternate Number）]セクションを展開して、次の手順を実行します。

a) [エンタープライズ代替番号の追加（Add Enterprise Alternate Number）]ボタンまたは[+E.164代替番号の追加（Add +E.164 Alternate Number）]ボタンのいずれか、または両方をクリックします。

b) 代替番号への割り当に使用する [番号マスク（Number Mask）]を追加します。 たとえば、4 桁の内線番号では、エンタープライズ番号マスク として 5 XXXX を使用し、+E.164 代替番号マスクとして 1972555XXXX を使用することが考えられます。

c) 代替番号を割り当てるパーティションを割り当てます。

d) ILS を通じてこの番号をアドバタイズする場合は、[ILS経由でグローバルにアドバタイズ（Advertise Globally via ILS）]チェックボックスをオンにします。 アドバタイズされたパターンを使用して一定の代替番号の範囲を要約している場合は、個別の代替番号をアドバタイズする必要はありません。

e) [PSTNフェールオーバー（PSTN Failover）]セクションを展開して、通常のコール ルーティングが失敗した場合に使用する PSTN フェールオーバーとして、[エンタープライズ番号（Enterprise Number）]または [+E.164代替番号（+E.164 Alternate Number）]を選択します。

ステップ 5 **[保存]** をクリックします。

ユーザ プロファイルの設定

ユーザ プロファイルを使用して、ユニバーサル回線テンプレートとユニバーサル デバイス テンプレートをユーザに割り当てます。 さまざまなユーザ グループ用に複数のユーザ プロファイルを設定します。 このサービス プロファイルを使用するユーザに対してセルフプロビジョニングを有効にすることもできます。

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。 **[ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [ユーザプロファイル（User Profile）]**。

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、**[ユニバーサルデバイステンプレート（Universal Device Template）]** を割り当てます。

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) [エンドユーザに自分の電話のプロビジョニングを許可（Allow End User to Provision their own phones）]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エンドユーザーに、別のユーザー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ー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 このユーザープロファイルに関連付けられた Cisco Jabber ユーザー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（Enable Mobile and Remote Access）]** 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になっています。 このチェックボックスをオフにすると、**[クライアントポリシー（Client 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。**[デスクトップ クライアント ポリシー（Desktop Client Policy）]**と**[モバイル クライアント ポリシー（Mobile Client Policy）]**のドロップダウンメニューから、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、音声とビデオ通話：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。

ヘッドセットテンプレートの設定

シスコヘッドセットに適用できるカスタマイズされた設定でヘッドセットテンプレートを設定するには、次の手順を使用します。 カスタマイズしたテンプレートを作成するか、またはシステム定義の標準デフォルトヘッドセットテンプレートを使用することができます。

（注） 標準デフォルトヘッドセット構成テンプレートは、システム定義のテンプレートです。標準デフォルトヘッドセットテンプレートに新しいユーザプロファイルを割り当てることはできますが、テンプレートを編集することはできません。デフォルトでは、すべてのユーザプロファイルがこのテンプレートに割り当てられています。このテンプレートからユーザプロファイルの関連付けを外すには、プロファイルを新しいテンプレートに割り当てる必要があります。

手順

ステップ 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、**[デバイス（Device）][電話機（Phone）]** を選択します。

ステップ 2 次のいずれかを実行します。

- 既存のテンプレートを編集するには、そのテンプレートを選択します。
- 新しいテンプレートを作成するには、既存のテンプレートを選択し、**[コピー(Copy)]** をクリックします。既存の設定が新しいテンプレートに適用されます。

ステップ 3 テンプレートの**[名前（Name）]**と**[説明（Description）]**を追加します。

ステップ 4 [**モデルとファームウェアの**設定（Model and Firmware Settings）] で、カスタマイズしたヘッドセット設定をこのテンプレートに適用するように割り当てます。新しい設定を追加するには、**[**追加 (add)] ボタンをクリックして設定を構成します。

ステップ 5 上下矢印を使用して、このテンプレートに割り当てるユーザプロファイルを**割当済みユーザプロファイル**リストに移動します。これらのプロファイルに割り当てられているすべてのユーザは、このヘッドセットテンプレートにも割り当てられます。

ステップ 6 **[保存]** をクリックします。

ステップ 7 デフォルトの**テンプレート設定**に戻るには、[デフォルトに設定 (Set to Default)] ボタンを使用します。

ステップ 8 **[設定の適用（Apply Config）]** をクリックします。

標準デフォルトヘッドセット構成テンプレートの場合、**[**構成を適用 (Apply Configuration)] ボタンは次の場合有効になります。

- 割当済みユーザプロファイルリストに追加したユーザが所有するデバイス
- 匿名デバイス

カスタマイズされたヘッドセット構成テンプレートでは、**構成を適用**ボタンは、**割当済みユーザプロファイル**リストに追加したユーザが所有するデバイスでのみ有効になります。

UC サービスの設定

ユーザが使用する UC サービス接続を設定するには、次の手順を使用します。 次のUCサービスの接続を設定できます。

- ボイスメール
- メールストア（Mailstore）
- 会議
- ディレクトリ（Directory）
- IM and Presence Service
- [CTI]
- ビデオ会議スケジュールポータルの設定
- Jabberクライアント設定(jabber-config.xml)

（注） フィールドは、設定する UC サービスによって異なる場合があります。

手順

ステップ 1 Cisco Unified CMの管理から、**ユーザの管理>ユーザ設定>UCサービス**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 [UC サービスタイプ (UC Service)] ドロップダウンから、設定する UC サービスを選択し、**[次へ (Next)] をクリックします**。

ステップ 4 **製品タイプ**を選択します。

ステップ 5 [名前（Name）]にサービスの名前を入力します。

ステップ 6 サービスが存在するサーバーの**ホスト名またはIPアドレス**を入力します。

ステップ 7 ポートと**プロトコル**の情報を入力します。

ステップ 8 残りのフィールドを設定します。フィールドとその設定のヘルプについては、オンラインヘルプを参照してください。フィールドオプションは、導入しているUCサービスによって異なります。

ステップ 9 **[保存]** をクリックします。

ステップ 10 必要なすべてのUCサービスをプロビジョニングするまで、この手順を繰り返します。

（注） サービスを複数のサーバに配置する場合は、別のサーバを指す複数の UC サービス接続を設定します。 たとえば、IMとプレゼンスサービスの集中型の導入を行う場合は、別のIM ノードとプレゼンスノードをポイントするように、複数のIMおよびプレゼンスUC サービスを設定することを推奨します。 すべてのUC接続を設定した後、それらをサービスプロファイルに追加することができます。

サービス プロファイルの設定

このプロファイルを使用するエンド ユーザに割り当てる UC サービスを含む、サービス プロファイルを設定します。

始める前に

サービス プロファイルに追加する前に、Unified Communications（UC）サービスをセットアップする必要があります。

手順

ステップ 1 Cisco Unified CM の管理から、**[ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [サービスプロファイル（Service 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 選択したサービス プロファイルの設定の [名前（Name）]を入力します。

ステップ 4 選択したサービス プロファイルの設定の [説明（Description）]を入力します。

ステップ 5 このプロファイルに含める各 UC サービスに、そのサービス用の [プライマリ（Primary）]、[セカンダリ（Secondary）]、および [ターシャリ（Tertiary）] の接続を割り当てます。

ステップ 6 [サービスプロファイルの設定（Service Profile Configuration）]ウィンドウで、残りのフィールドを入力します。 フィールドの詳細については、オンライン ヘルプを参照してください。

ステップ 7 **[保存]** をクリックします。

機能グループ テンプレートの設定

機能グループテンプレートは、プロビジョニングされたユーザ用に、電話、回線、および機能をすばやく設定できるようにすることで、システムの展開をサポートします。 企業の LDAP ディレクトリからユーザを同期している場合は、ディレクトリからユーザを同期させるユーザ プロファイルおよびサービス プロファイルを使用して機能グループ テンプレートを設定します。 このテンプレートを使用して、同期されたユーザに対して IM and Presence Service を有効化することもできます。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] で、**[ユーザ管理（User Management）] > [ユーザ/電話の追加（User/Phone Add）] > [機能グループ テンプレート（Feature Group Template）]** 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 機能グループ テンプレートの [名前（Name）]と [説明（Description）]を入力します。

ステップ 4 このテンプレートを使用するすべてのユーザのホーム クラスタとしてローカル クラスタを使用する場合は、[ホーム クラスタ（Home Cluster）]チェック ボックスをオンにします。

ステップ 5 このテンプレートを使用するユーザがインスタント メッセージおよびプレゼンス情報を交換できるようにするには、[Unified CM IM and Presenceのユーザを有効化（Enable User for Unified CM IM and Presence）]チェックボックスをオンにします。

ステップ 6 ドロップダウン リストから、[サービスプロファイル（Services Profile）]および [ユーザプロファイル（User Profile）]を選択します。

ステップ 7 [機能グループ テンプレートの設定（Feature Group Template Configuration）]ウィンドウの残りのフィールドに入力します。 フィールドの説明については、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。

次のタスク

機能グループ テンプレートと LDAP ディレクトリ同期を関連付け、テンプレートの設定を同期したエンド ユーザに適用します。

デフォルトのクレデンシャル ポリシーの設定

新しくプロビジョニングされたユーザに適用されるクラスタ全体のデフォルトのクレデンシャル ポリシーを設定するには、この手順を使用します。 次の各クレデンシャル タイプに対して、個別のクレデンシャル ポリシーを適用できます。

- アプリケーション ユーザー パスワード
- エンド ユーザー パスワード
- エンド ユーザ PIN

手順

ステップ 1 クレデンシャル ポリシーの設定を入力します。

a) Cisco Unified CM Administration で、**[ユーザ管理] > [ユーザ設定] > [クレデンシャル ポリシーのデフォルト]** を選択します。

b) 次のいずれかを実行します。

- [検索（Find）] をクリックし、既存のクレデンシャル ポリシーを選択します。
- [新規追加（Add New）]をクリックして、新しいクレデンシャル ポリシーを作成します。

c) ABCD や 123456 のようなハッキングされやすいパスワードをシステムにチェックさせる場合は、[単純すぎるパスワードのチェック（Check for Trivial Passwords）]チェックボックスをオンにします。

d) [クレデンシャル ポリシーの設定（Credential Policy Configuration）]ウィンドウの各フィールドに入力します。 フィールドとその設定の詳細については、オンライン ヘルプを参照してください。

e) **[保存]** をクリックします。

f) 他のクレデンシャル タイプ用に別のクレデンシャル ポリシーを作成する場合は、この手順を繰り返します。

ステップ 2 次のいずれかのクレデンシャル タイプにクレデンシャル ポリシーを適用します。

a) Cisco Unified CM Administration で、**[ユーザ管理]** > **[ユーザ設定]** > **[クレデンシャル ポリシーのデフォルト]** を選択します。

b) クレデンシャル ポリシーを適用するクレデンシャル タイプを選択します。

c) [クレデンシャルポリシー（Credential Policy）]ドロップダウンから、このクレデンシャル タイプに適用するクレデンシャル ポリシーを選択します。 たとえば、作成したクレデンシャル ポリシーを選択できます。

d) [クレデンシャルの変更（Change Credential）]フィールドと [クレデンシャルの確認（Confirm Credential）]フィールドの両方にデフォルトのパスワードを入力します。 ユーザが次にログインするときに、これらのパスワードを入力する必要があります。

e) [クレデンシャル ポリシーのデフォルトの設定（Credential Policy Default Configuration）] ウィンドウで、残りのフィールドを設定します。 フィールドとその設定の詳細については、オンライン ヘルプを参照してください。

f) **[保存]** をクリックします。

g) 他のクレデンシャル タイプにクレデンシャル ポリシーを割り当てる場合は、この手順を繰り返します。

（注） また、個々のユーザに対して、**[エンド ユーザの設定]** ウィンドウまたはそのユーザの **[アプリケーション ユーザ設定]** ウィンドウから、特定のユーザクレデンシャルにポリシーを割り当てすることもできます。 クレデンシャル タイプ (パスワードまたは PIN) の隣にある **[クレデンシャルの編集]** ボタンをクリックして、そのユーザの**クレデンシャル設定** を開きます。

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。