



プロビジョニング プロファイルの設定

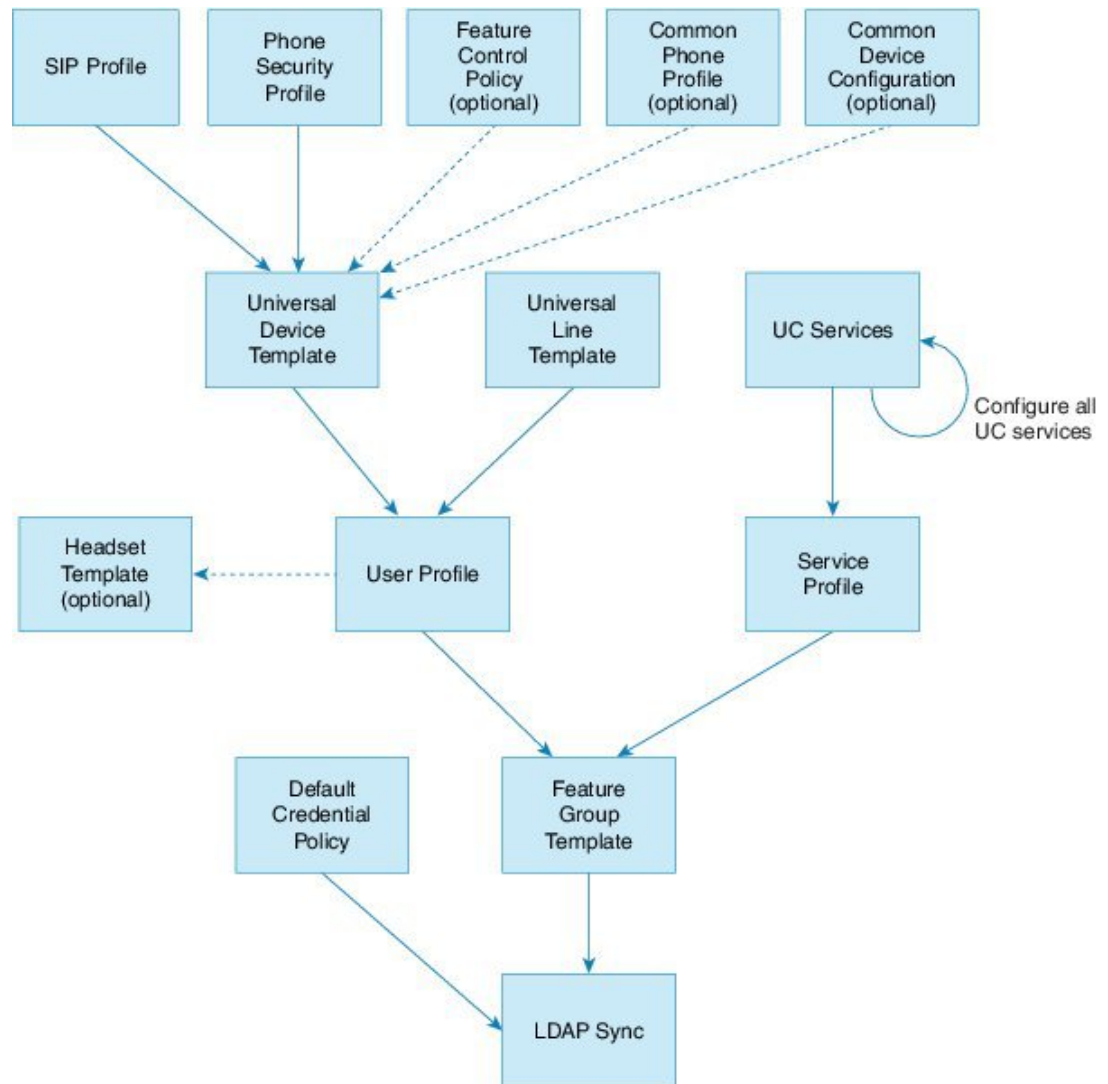
- [プロビジョニング プロファイルの概要 \(1 ページ\)](#)
- [プロビジョニング プロファイルのタスクフロー \(2 ページ\)](#)
- [SIP プロファイルの設定 \(4 ページ\)](#)
- [電話機のセキュリティ プロファイルの設定 \(5 ページ\)](#)
- [機能管理ポリシーの作成 \(6 ページ\)](#)
- [共通の電話プロファイルの作成 \(7 ページ\)](#)
- [共通デバイス設定の構成 \(8 ページ\)](#)
- [ユニバーサル デバイス テンプレートの設定 \(9 ページ\)](#)
- [ユニバーサル回線テンプレートの設定 \(10 ページ\)](#)
- [ユーザープロファイルの設定 \(11 ページ\)](#)
- [ヘッドセットテンプレートの設定 \(13 ページ\)](#)
- [UC サービスの設定 \(14 ページ\)](#)
- [サービス プロファイルの設定 \(15 ページ\)](#)
- [機能グループ テンプレートの設定 \(15 ページ\)](#)
- [デフォルトのクレデンシヤル ポリシーの設定 \(16 ページ\)](#)

プロビジョニング プロファイルの概要

ユニファイドコミュニケーションマネージャには、新しいユーザに割り当てることができるプロファイルとテンプレートのセットが含まれています。これらのプロファイルと共通の設定を事前に設定した場合、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、ユーザとデバイスが適用される設定に基づいて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ているユーザプロファイルとサービスプロファイルにそれらに関連付けます。さらに、ユーザにデバイスを追加すると、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およびユニバーサルデバイステンプレートを使用して、デバイスと電話番号がすぐに設定されます。

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共通の設定をユーザとエンドポイントに適用できます。



25107616

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が多数ある場合は、テンプレートを使用してユーザプロフィールとサービスプロフィールを設定し、特定のグループ (カスタマーサポートなど) のユーザに適用する共通の設定を行うことで、設定プロセスを簡素化できます。

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ているユーザプロフィールとサービスプロフィールにそれらに関連付けます。さらに、ユーザにデバイスを追加すると、そのユーザのユーザプロフィールに関連付けられているユニバーサル回線およびユニバーサルデバイステンプレートを使用して、デバイスと電話番号がすぐに設定されます。

次のプロフィー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共通の設定をユーザとエンドポイントに適用できます。

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の SIP 設定をセットアップします。
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 や 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、TFTP データと製品固有の設定のデフォルトを、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) エンドポイントにユーザ固有の設定と IPv6 設定を割り当てるには、この設定を使用します。
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機の設定に使用される共通の設定が含まれています。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ができます。
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拡張機能を設定するために使用される共通の設定が含まれています。内線用のエンタープライズ番号および E.164 番号を設定することもできます。
ステップ 8	ユーザー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た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。

	コマンドまたはアクション	目的
ステップ 9	ヘッドセットテンプレートの設定 (13 ページ)	(オプション) Cisco ヘッドセットを使用して、設定したユーザプロファイルにヘッドセットテンプレートを割り当てる予定の場合。
ステップ 10	UC サービスの設定 (14 ページ)	IM and Presence Service や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、LDAP 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た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 同期の設定
- LDAP を展開していない場合は、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 から、[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 (Add New)] をクリックします。

- ステップ 3** プロファイルの [名前 (Name)] 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)] で DSCP 設定を指定して、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** (オプション) 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 (Save)] 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 電話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 (Add New)] 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** [名前 (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 (Save)] 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** 次のいずれかの操作を実行します。
- 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 (Add New)] 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 (Save)] 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、プロファイルを使用する電話の TFTP データと製品固有の設定のデフォルト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 (Add New)] をクリックします。

ステップ3 プロファイルの [名前 (Name)] を入力します。

ステップ4 プロファイルの [説明 (Description)] 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 [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 (オプション) モバイルおよびリモートアクセスの電話機用に Interactive Connectivity Establishment (ICE) を有効にするには、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)] : ホストデバイスで IP アドレスを選択することで取得される候補。これはデフォルトです。

- [サーバ再帰 (Server Reflexive)] : STUN 要求を送信することで取得される 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 (Relayed)] : TURN サーバから取得される IP アドレスとポートの候補。IP アドレスとポートは、メディアが TURN サーバを介して中継されるように、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 (Save)] をクリックします。

共通デバイス設定の構成

共通デバイス設定は、任意指定のユーザ固有の機能属性で構成されます。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 (Add New)] 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、[シグナリング用 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 を設定した場合は、[シグナリング用の IP アドレッシングモード (IP Addressing Mode for Signaling)] ドロップダウンリストで IP アドレッシング設定を指定します。

- [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、[シグナリング用 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 [共通デバイス設定 (Common Device 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、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 (Save)] 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がこのテンプレートに割り当てられることもできます。

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 (Add New)] 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 65 Device Pools 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롭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롭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롭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 (Save)] 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 (Add New)] 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てに使用する [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 5XXXX 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 (Save)]をクリックします。

ユーザープロファイルの設定

ユーザー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ー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)]**を選択します。
- ステップ2** [新規追加 (Add New)]をクリックします。
- ステップ3** ユーザープロファイルの[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)]をこのユーザープロファイルのユーザの電話回線に適用するために割り当てます。
- ステップ6** このユーザープロファイルのユーザに自分の電話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
- [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。
 - [エンドユーザのプロビジョニングする電話数を制限 (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。
 - 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 (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。非 Jabber ユーザは、この設定がなくてもモバイルおよびリモートアクセスを使用できます。モバイルおよびリモートアクセス機能は、Jabber のモバイルおよびリモートアクセスユーザにのみ適用され、他のエンドポイントまたはクライアントには適用されません。

ステップ 8 このユーザープロファイルに 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)] および [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、次のいずれかのオプションを選択します。

- [サービスなし (No Service)] : このポリシーでは、すべての Cisco Jabber サービスへのアクセスが禁止されます。
- [IM & Presence のみ (IM & Presence only)] : 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だけを有効にします。
- [IM & Presence、音声およびビデオ通話 (IM & Presence, Voice and Video calls)] : このポリシーは、オーディオまたはビデオデバイスを所有しているすべてのユーザーに対して、インスタントメッセージング、プレゼンス、ボイスメール、および会議機能を有効にします。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 ユーザ用 Cisco Jabber と、Mac ユーザ用 Cisco Jabber が含まれています。Jabber モバイルクライアントには、iPad および iPhone ユーザ用 Cisco Jabber と、Android ユーザ用 Cisco Jabber が含まれています。

ステップ 9 このユーザー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 (Save)] 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、システム定義の標準のデフォルトのヘッドセットテンプレートを使用できます。



- (注) 標準のデフォルトのヘッドセット設定テンプレートは、システム定義のテンプレートです。標準のデフォルトの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解除するには、新しいテンプレートにプロファイルを割り当てる必要があります。

手順

- ステップ 1** Cisco Unified CM Administration から、[デバイス (Device)] > [ヘッドセット (Headset)] > [ヘッドセットテンプレート (Headset Template)] 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、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、このテンプレートに適用するカスタマイズされたヘッドセット設定を割り当てます。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項目を指定します。
- ステップ 5** 上下の矢印を使用して、このテンプレートに割り当てるユーザプロファイルを、[割り当てられているユーザプロファイル (Assigned Users Profiles)] リストボックスに移動します。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 (Save)] 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すには、[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。
- 標準のデフォルトヘッドセット構成テンプレートでは、以下に対して [設定の適用 (Apply Config)] ボタンが有効になります。
- 割り当てられたユーザプロファイルリストに追加したユーザが所有しているデバイス
 - 名前非表示のデバイス

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、[割り当てられているユーザプロフィール (Assigned User Profiles)] リストに追加されたユーザが所有するデバイスに対してのみ [設定の適用 (Apply Config)] ボタンが有効になります。

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
- 会議
- ディレクトリ
- 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 Administration から、[ユーザ管理 (User Management)] > [ユーザ設定 (User Settings)] > [UCサービス (UC Services)] を選択します。
- ステップ 2** [新規追加 (Add New)] をクリックします。
- ステップ 3** [UCサービスタイプ (UC Service Type)] ドロップダウンリストから、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 (Product Type)] 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 (Port)] および [プロトコル (Protocol)] 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詳細については、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 (Save)] 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 and Presence Service の集中展開では、複数の IM and Presence UC サービスがそれぞれ異なる IM and Presence ノードを指すように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 Administration 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 (Add New)] 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 (Save)] 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 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 (Add New)] 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 (Save)] 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クレデンシャルポリシーを設定するには、次の手順を使用します。次の各ログイン情報タイプに対して、個別のログイン情報ポリシーを適用できます。

- アプリケーション ユーザ パスワード
- エンドユーザのパスワード
- 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 から、[ユーザ管理 (User Management)] > [ユーザ設定 (User Settings)] > [クレデンシャルポリシー (Credential Policy)] 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 (Save)] をクリックします。
- f) 他のクレデンシャルタイプのいずれかに対して異なるクレデンシャルポリシーを作成する場合は、これらの手順を繰り返します。

ステップ 2 クレデンシャルポリシーをクレデンシャルタイプのいずれかに適用します。

- a) Cisco Unified CM Administration から、[ユーザ管理 (User Management)] > [ユーザ設定 (User Settings)] > [クレデンシャルポリシーのデフォルト (Credential Policy Default)] 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することもできます。
- 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。ユーザは次のログイン時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 (Save)] をクリックします。
- g) 他のクレデンシャルタイプのいずれかにクレデンシャルポリシーを割り当てる場合は、これらの手順を繰り返します。



-
- (注) 個人ユーザに対して、[エンドユーザの設定 (End User Configuration)] 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の設定 (Application User Configuration)] ウィンドウから、特定のユーザログイン情報にポリシーを割り当てることもできます。ログイン情報タイプ (パスワードまたはPIN) の隣にある[ログイン情報の編集 (Edit Credential)] ボタンをクリックして、そのユーザログイン情報に関する[ログイン情報の設定 (Credential Configuration)] 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。