ユーザ

LDAP 同期の概要

Lightweight Directory Access Protocol（LDAP）の同期は、システムのエンドユーザのプロビジョニングと設定を支援します。LDAP の同期中、システムは外部 LDAP ディレクトリから Cisco Unified Communications Manager データベースにユーザのリストと関連するユーザ データをインポートします。また、従業員のデータの変更を漏らさずに記録するため、定期的な同期スケジュールを設定できます。

ユーザ ID とディレクトリ URI

LDAP ディレクトリ サーバと Cisco Unified Communications Manager を同期させると、次の値を含む属性を使用して、Cisco Unified Communications Manager データベースと Cisco Unified Communications Manager IM and Presence Service データベースの両方でエンド ユーザ設定テーブルを生成できます。

- **ユーザ ID**：Cisco Unified Communications Manager でユーザ ID の値を指定する必要があります。この値はデフォルトの IM アドレス スキームおよびユーザのログインに必要です。デフォルト値は `sAMAccountName` です。

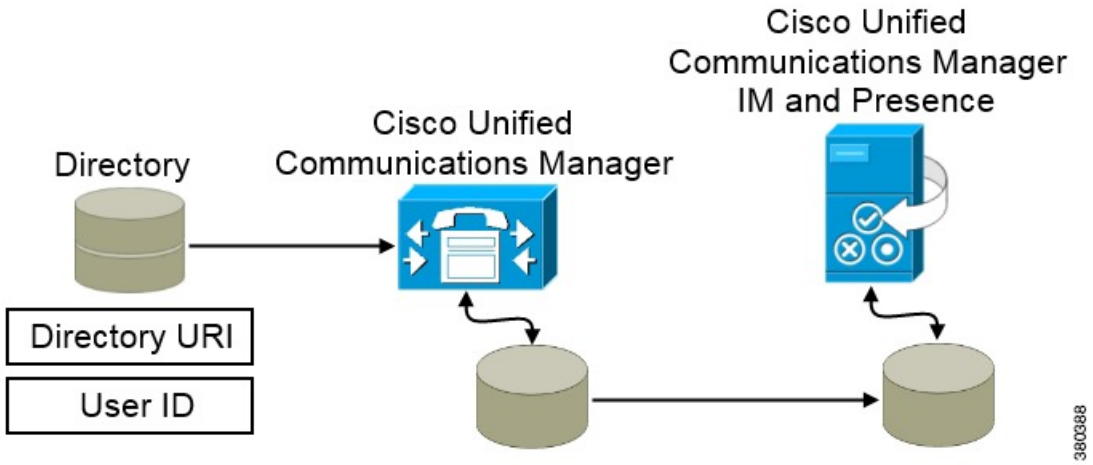
重要 ユーザ ID の属性が `sAMAccountName` 以外の場合で、Cisco Unified Communications Manager IM and Presence Service でデフォルトの IM アドレス方式が使用されている場合は、次のようにクライアント コンフィギュレーション ファイルでパラメータの値として属性を指定する必要があります。

CDI パラメータは `UserAccountName` です。

`<UserAccountName>attribute-name</UserAccountName>`

設定で属性を指定せず、属性が `sAMAccountName` 以外の場合、クライアントはディレクトリ内の連絡先を解決できません。この結果、ユーザはプレゼンスを取得せず、インスタントメッセージを送信または受信できません。

- **ディレクトリ URI**：以下を予定している場合は、ディレクトリ URI の値を指定する必要があります。
  - Cisco Jabber で URI ダイヤルを有効にする。
  - Cisco Unified Communications Manager IM and Presence Service バージョン 10 以降でディレクトリ URI アドレス スキームを使用する。



Cisco Unified Communications Manager がディレクトリ ソースと同期すると、ディレクトリ URI とユーザ ID の値を取得して、それらを Cisco Unified Communications Manager データベースのエンド ユーザ設定テーブルに入力します。

その後で、Cisco Unified Communications Manager データベースが Cisco Unified Communications Manager IM and Presence Service データベースと同期します。その結果、ディレクトリ URI とユーザ ID の値が Cisco Unified Communications Manager IM and Presence Service データベースのエンド ユーザ設定テーブルに入力されます。

ユーザ ワークフローの設定

手順

	コマンドまたはアクション	目的
ステップ 1	サービスのアクティブ化 （3 ページ）	ユーザ設定を LDAP ディレクトリから Cisco Unified Communications Manager と IM and Presence サービスへ同期するために必要なサービスをオンにします。
ステップ 2	LDAP ディレクトリ同期の有効化 （4 ページ）	Cisco Unified Communications Manager が LDAP ディレクトリからユーザ設定を同期できるようにします。**ユーザ ID** について Cisco Unified Communications Manager を同期させる LDAP ディレクトリから属性を選択します。
ステップ 3	LDAP ディレクトリの同期の設定 （5 ページ）	LDAP ディレクトリと同期するよう、Cisco Unified Communications Manager を設定します。自動同期スケジュールを設定し、標準ユーザ フィールドをマップして、アクセス コントロール グループにインポートされたユーザを割り当てます。
ステップ 4	認証オプション （7 ページ）	認証オプションを選択します。 • クライアント内の SAML SSO を有効にします。 • LDAP サーバで認証します。
ステップ 5	同期の実行 （11 ページ）	Cisco Unified Communications Manager とディレクトリ サーバを同期します。
ステップ 6	ユーザへのサービス プロファイルの関連付け （11 ページ）	サービス プロファイルをユーザに関連付けます。
ステップ 7	連絡先リストの一括事前入力 （13 ページ）	ユーザの連絡先リストにデータを挿入します。

サービスのアクティブ化

社内 LDAP サーバを統合する前に、次のサービスをアクティブにする必要があります。

- Cisco DirSync サービス：社内 LDAP ディレクトリでエンドユーザの設定を同期するにはこのサービスをアクティブにする必要があります。
- （Cisco Unified Communications Manager IM and Presence Service）Cisco Sync Agent サービス：このサービスは IM and Presence サービス ノードと Cisco Unified Communications Manager の間でデータの同期を維持します。ディレクトリ サーバとの同期を実行すると、Cisco Unified Communications Manager は次に IM and Presence サービスとデータを同期します。

手順

ステップ 1 Cisco Unified Serviceability から、**[ツール（Tools）]** > **[サービスの有効化（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 ボックスからパブリッシャ ノードを選択します。

ステップ 3 [**ディレクトリ サービス（Directory Services**）] の下の [**Cisco DirSync**] オプション ボタンをクリックします。

ステップ 4 **[保存（Save）]**をクリックします。

ステップ 5 **[ツール（Tools）]** > **[コントロール センタのネットワーク サービス（Control Center - Network Services）]** を選択します。

ステップ 6 [サーバ（Server）] ドロップダウン リスト ボックスから、[IM and Presence サービス（IM and Presence Service）] ノードを選択します。

ステップ 7 [**IM and Presence サービス（IM and Presence Services**）] で、[**Cisco 同期エージェント（Cisco Sync Agent**）] オプション ボタンをクリックします。

ステップ 8 **[保存]** をクリックします。

LDAP ディレクトリ同期の有効化

エンドユーザの設定を社内 LDAP ディレクトリから同期するように Cisco Unified Communications Manager を設定するには、次の手順を実行します。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] で、**[システム（System）]** > **[LDAP]** > **[LDAP システム（LDAP System）]** を選択します。

[LDAP システムの設定（LDAP System Configuration）] ウィンドウが開きます。

ステップ 2 Cisco Unified Communications Manager が LDAP ディレクトリからユーザをインポートすることを許可するには、[LDAP サーバからの同期を有効にする（Enable Synchronizing from LDAP Server）] チェックボックスをオンにします。

ステップ 3 [LDAP サーバ タイプ（LDAP Server Type）] ドロップダウン リスト ボックスから、会社が使用する LDAP ディレクトリ サーバのタイプを選択します。

ステップ 4 [ユーザ ID の LDAP 属性（LDAP Attribute for User ID）] ドロップダウン リスト ボックスから、[エンドユーザ設定（End User Configuration）] ウィンドウの [ユーザ ID（User ID）] フィールドの値について、Cisco Unified Communications Manager を同期させる社内 LDAP ディレクトリの属性を選択します。

この値はデフォルトの IM アドレス スキームおよびユーザのログインに必要です。デフォルト値は `sAMAccountName` です。

設定で属性を指定せず、属性が `sAMAccountName` 以外の場合、クライアントはディレクトリ内の連絡先を解決できません。この結果、ユーザはプレゼンスを取得せず、インスタント メッセージを送信または受信できません。

ステップ 5 **[保存]** をクリックします。

LDAP ディレクトリの同期の設定

LDAP ディレクトリと同期するよう Cisco Unified Communications Manager を設定するには、次の手順を使用します。LDAP ディレクトリの同期により、[**エンド ユーザの設定（End User Configuration**）] ウィンドウに表示されるエンドユーザのデータを外部の LDAP ディレクトリより Cisco Unified Communications Manager データベースへインポートできます。定期的に LDAP ディレクトリの更新が Cisco Unified Communications Manager に伝達されるよう、同期スケジュールをセットアップできます。

フィールドとその説明を含むヘルプは、オンライン ヘルプを参照してください。

手順

ステップ 1 Cisco Unified CM の管理で、**[システム（System）]** > **[LDAP（LADP）]** > **[LDAP ディレクトリ（LDAP Directory）]** 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。

- [**検索（Find**）] をクリックし、既存の LDAP ディレクトリを選択します。
- [**新規追加（Add New**）] をクリックして、新しい LDAP ディレクトリを作成します。

ステップ 3 [**LDAP 構成名（LDAP Configuration Name**）] テキスト ボックスで、LDAP ディレクトリの一意の名前を指定します。

ステップ 4 [**LDAP マネージャ識別名（LDAP Manager Distinguished Name**）] フィールドに、LDAP ディレクトリ サーバにアクセスできるユーザー ID を入力します。

ステップ 5 パスワードの詳細を入力し、確認します。

ステップ 6 [LDAP ディレクトリ同期スケジュール（LDAP Directory Synchronization Schedule）] フィールドに、外部 LDAP ディレクトリとデータ同期を行うために Cisco Unified Communications Manager が使用するスケジュールを作成します。

ステップ 7 [**同期対象の標準ユーザ フィールド（Standard User Fields To Be Synchronized**）] セクションを記入します。各エンドユーザのフィールドで、それぞれLDAP属性を選択します。同期プロセスは LDAP 属性の値を Cisco Unified Communications Manager のエンドユーザ フィールドに割り当てます。

a) [ディレクトリURI（Directory URI）] ドロップダウン リストで、次の LDAP 属性のいずれかを選択します。

- **msRTCSIP-primaryuseraddress**：この属性は、Microsoft Lync または Microsoft OCS が使用されている場合に AD 内で生成されます。これがデフォルト属性です。
- **メール**

ステップ 8 インポートされたすべてのエンドユーザに共通するアクセス コントロール グループにインポートしたエンドユーザを割り当てるには、次の手順を実行してください。

a) [**アクセス コントロール グループに追加（Add to Access Control Group**）] をクリックします。

b) ポップアップ ウィンドウで、インポートしたユーザに割り当てるアクセス コントロール グループごとに、対応するチェックボックスをオンにします。

c) [**選択項目の追加（Add Selected**）] をクリックします。

ユーザを、少なくとも次のアクセス コントロール グループに割り当てる必要があります。

- **Standard CCM End Users**
- [標準 CTI を有効にする（Standard CTI Enabled）]：このオプションは、デスク フォンを制御するために使用します。

セキュア電話機能をユーザにプロビジョニングする場合、**Standard CTI Secure Connection** グループにユーザを割り当てないでください。

電話機のモデルによっては、次のコントロール グループが追加で必要となります。

- Cisco Unified IP Phone 9900、8900、8800 シリーズ、または DX シリーズでは、**[標準 CTI による接続時の転送および会議をサポートする電話の制御（Standard CTI Allow Control of Phones supporting Connected Xfer and conf）]** を選択します。
- Cisco Unified IP Phone 6900 シリーズでは、**[標準 CTI によるロールオーバー モードをサポートする電話の制御（Standard CTI Allow Control of Phones supporting Rollover Mode）]** を選択します。

（注） Cisco Unified Communications Manager 9.x では、[**エンドユーザの設定（End User Configuration**）] ウィンドウ（**[ユーザ管理（User Management**）] > **[エンドユーザ（End User**）]）のアクセス コントロール グループにエンドユーザを割り当てる必要があります。

ステップ 9 [**LDAP サーバ情報（LDAP Server Information**）] エリアで、LDAP サーバのホスト名または IP アドレスを入力します。

ステップ 10 LDAP サーバへのセキュアな接続を作成するには、[**TLS を使用（Use TLS**）] チェックボックスをオンにします。

ステップ 11 **[保存]** をクリックします。

認証オプション

LDAP サーバでの認証

LDAP 認証を有効にして、会社の LDAP ディレクトリに割り当てられているパスワードに対してエンドユーザのパスワードが認証されるようにするには、この手順を実行します。LDAP 認証により、システム管理者は会社のすべてのアプリケーションに対してエンドユーザの 1 つのパスワードを割り当てることができます。この設定は、エンドユーザのパスワードにのみ適用され、エンドユーザの PIN またはアプリケーション ユーザのパスワードには適用されません。ユーザがクライアントにサインインすると、プレゼンス サービスがその認証を Cisco Unified Communications Manager にルーティングします。その後で、Cisco Unified Communications Manager がその認証をディレクトリ サーバに送信します。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] インターフェイスを開きます。

ステップ 2 **[システム（System）]** > **[LDAP]** > **[LDAP 認証（LDAP Authentication）]** を選択します。

ステップ 3 [エンドユーザ用 LDAP 認証の使用（Use LDAP Authentication for End Users）] を選択します。

ステップ 4 必要に応じて、LDAP クレデンシャルとユーザ検索ベースを指定します。

[LDAP認証（LDAP Authentication）] ウィンドウ上のフィールドの詳細については、『*Cisco Unified Communications Manager Administration Guide*』を参照してください。

ステップ 5 **保存**を選択します。

クライアントの LDAP サーバ認証のための設定

LDAP クレデンシャルを使用するための認証の設定では、クライアントも設定する必要があります。

手順

ステップ 1 LDAP_UseCredentialsFrom パラメータで `jabber-config.xml` ファイルを更新します。

例：

<LDAP_UseCredentialsFrom>*CUCM*</LDAP_UseCredentialsFrom>

ステップ 2 Cisco Unified Communications Manager IM and Presence Service および Cisco Unified Communications Manager が展開されているドメインとは別のドメインに LDAP サーバが展開されている場合は、LDAPUserDomain パラメータを設定します。このパラメータを設定しない限り、必須のパラメータである PresenceDomain の値がデフォルトで使用されます。

例：

<LdapUserDomain>*example.com*</LdapUserDomain>

匿名バインドでの認証

LDAP サーバのユーザ認証の手段として、匿名バインドを設定できます。匿名バインドを使用することにより、Jabber の [オプション（Options）] メニューの [アカウント（Accounts）] タブでのクレデンシャル入力を不要にできます。

手順

jabber-config.xml ファイルで、LdapAnonymousBinding パラメータに true または false の値を設定します。

例：

<LdapAnonymousBinding>true</LdapAnonymousBinding>

このパラメータの設定の詳細は、『*Cisco Jabber* パラメータ リファレンス ガイド（*Parameters Reference Guide for Cisco Jabber*）』を参照してください。

手動ユーザ認証

ユーザが必要とするサービスで Jabber クライアントにユーザ自身のクレデンシャルを手動で入力するサービス認証をセットアップできます。

サービス認証が（たとえば、サービスプロファイルまたは LDAP サーバに）設定されていない場合は、ユーザが自分のクレデンシャルを手動で入力するよう求められます。

ユーザのクレデンシャルは Jabber の [**オプション（Option**）] メニューの [**アカウント（Accounts**）] タブに入力します。

クライアント内の SAML SSO の有効化

始める前に

- Cisco Unified Communications Applications 10.5.1 Service Update 1 での SSO の有効化：このサービスで SAML SSO を有効化する方法については、『*SAML SSO Deployment Guide for Cisco Unified Communications Applications, Release 10.5*』を参照してください。
- Cisco Unity Connection バージョン 10.5 で SSO を有効にします。このサービス上での SAML SSO の有効化方法については、『*Managing SAML SSO in Cisco Unity Connection*』を参照してください。

手順

ステップ 1 Webブラウザで証明書を検証できるように、すべてのサーバに証明書を配布してください。これを行わない場合、無効な証明書に関する警告メッセージが表示されます。証明書の検証に関する詳細については、「証明書の検証」を参照してください。

ステップ 2 クライアントの SAML SSO のサービス検出を確認します。クライアントは、標準サービス検出を使用してクライアントの SAML SSO を有効化します。設定パラメータ ServicesDomain、VoiceServicesDomain、および ServiceDiscoveryExcludedServices を使用して、サービス検出を有効化します。サービス検出を有効にする方法の詳細については、「*Remote Access* のためのサービス検出の設定」を参照してください。

ステップ 3 セッションの継続時間を定義します。

セッションは、クッキーおよびトークン値で構成されます。cookie は通常トークンより長く継続します。cookie の寿命はアイデンティティプロバイダーで定義され、トークンの期間はサービスで定義されます。

ステップ 4 SSO を有効にすると、デフォルトで、すべての Cisco Jabber ユーザが SSO を使用してサインインします。管理者は、特定のユーザが SSO を使用する代わりに、Cisco Jabber ユーザ名とパスワードを使用してサインインするようにユーザ単位でこの設定を変更できます。Cisco Jabber ユーザの SSO を無効にするには、SSO_Enabled パラメータの値を FALSE に設定します。

ユーザに電子メールアドレスを尋ねないように Cisco Jabber を設定した場合は、ユーザの Cisco Jabber への最初のサインインが非 SSO になることがあります。展開によっては、パラメータの ServicesDomainSsoEmailPrompt を ON に設定する必要があります。これによって、Cisco Jabber は初めて SSO サインインを実行する際の必要な情報を得ることができます。ユーザが以前 Cisco Jabber にサインインしたことがある場合は、必要な情報が取得済みであるため、このプロンプトは必要ありません。

モバイル クライアントの証明書ベース SSO 認証

この設定は、iPhone および iPad 版 Cisco Jabber にのみ必要です。Android 版 Cisco Jabber には、同様の設定は必要ありません。

この機能を有効にするには、Cisco Unified Communications Manager と Cisco Unity Connection の両方で [iOS での SSO ログイン動作（SSO Login Behavior for iOS）] の設定を同じにします。

Expressway for Mobile and Remote Access により、VCS Expressway 管理コンソールで組み込み Safari ブラウザを使用するように Jabber for iPhone and iPad クライアントを設定します。詳細については、https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-guides-list.htmlのCisco Expresswayインストールガイドを参照してください。

Webex Messenger では共通アイデンティティ（CI）を有効にできません。組み込まれている Safari が、Cisco Jabber for iPhone and iPad でクライアント証明書ベースの SSL 認証を使用してボイスメールに接続できるようにするには、CIを無効にする必要があります。

Cisco Unified Communications Manager での証明書ベース SSO 認証の設定

この設定は Cisco Unified Communications Manager 11.5 以降でのみサポートされます。

手順

ステップ 1 Cisco Unified CM の管理で、**[システム（System）]**> **[エンタープライズ パラメータ（Enterprise Parameters）]** に移動します。

ステップ 2 [SSO 設定（SSO Configuration）] セクションで、[iOS での SSO ログイン動作（SSO Login Behavior for iOS）] までスクロールし、[ネイティブ ブラウザを使用（Use native browser）] を選択します。

ステップ 3 [保存（Save）] を選択します。

Cisco Unity Connection での証明書ベース SSO 認証の設定

手順

ステップ 1 Cisco Unity Connection Administration で、**[システム設定（System Setting）]** > **[エンタープライズ パラメータ（Enterprise Parameters）]** と進みます。

ステップ 2 [SSO 設定（SSO Configuration）] セクションで、[iOS での SSO ログイン動作（SSO Login Behavior for iOS）] までスクロールし、[ネイティブ ブラウザを使用（Use native browser）] を選択します。

ステップ 3 **保存**を選択します。

同期の実行

ディレクトリ サーバを追加し、認証方法を指定した後、Cisco Unified Communications Manager をディレクトリ サーバと同期できます。

手順

ステップ 1 **[システム（System）] > [LDAP] > [LDAP ディレクトリ（LDAP Directory）]** を選択します。

ステップ 2 [検索（Find）] をクリックし、設定した LDAP ディレクトリを選択します。

[LDAP ディレクトリ（LDAP Directory）] ウィンドウが開きます。

ステップ 3 [今すぐ完全同期を実行する（Perform Full Sync Now）] を選択します。

（注） 同期プロセスの完了までに要する時間は、ディレクトリ内のユーザの数によって異なります。ユーザ数が数千にもなる大規模なディレクトリの同期を実施する場合、そのプロセスにはある程度の時間がかかると予想されます。

ディレクトリ サーバからのユーザ データが Cisco Unified Communications Manager データベースに同期されます。その後で、Cisco Unified Communications Manager が IM and Presence サービス データベースにユーザ データを同期します。

ユーザへのサービス プロファイルの関連付け

個別ユーザへのサービス プロファイルの関連付け

サービス プロファイルを個別ユーザへ関連付けます。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] インターフェイスを開きます。

ステップ 2 **[ユーザ管理（User Management）] > [エンド ユーザ（End User）]** を選択します。

[ユーザの検索と一覧表示（Find and List Users）] ウィンドウが開きます。

ステップ 3 [ユーザを次の条件で検索（Find User where）] フィールドで適切なフィルタを指定した後、[検索（Find）] を選択してユーザのリストを取得します。

ステップ 4 対象のユーザ名をリストから選択します。

[エンド ユーザの設定（End User Configuration）] ウィンドウが表示されます。

ステップ 5 [サービスの設定（Service Settings）] セクションを探します。

ステップ 6 [ホーム クラスタ（Home Cluster）] を選択します。

ステップ 7 電話モード展開では、[Unified CM IM and Presence のユーザを有効化（関連付けられている UC サービス プロファイルで IM and Presence を設定）（Enable User for Unified CM IM and Presence (Configure IM and Presence in the associated UC Service Profile)）] オプションが選択されていないことを確認します。

他のすべての展開では、[Unified CM IM and Presenceの ユーザを有効化（関連付けられている UC サービス プロファイルで IM and Presence を設定）（Enable User for Unified CM IM and Presence (Configure IM and Presence in the associated UC Service Profile)）] チェックボックスをオンにします。

ステップ 8 [UC サービス プロファイル（UC Service Profile）] ドロップダウン リストからサービス プロファイルを選択します。

重要 Cisco Unified Communications Manager リリース 9.x のみ：ユーザがインスタント メッセージおよびプレゼンスの機能しか使用しない（IM 専用）場合は、[デフォルトの使用（Use Default）] を選択する必要があります。Cisco Unified Communications Manager リリース 9.x は、[UC サービス プロファイル（UC Service Profile）] ドロップダウン リストから選択された項目に関係なく、デフォルト サービス プロファイルを適用します。

ステップ 9 **保存**を選択します。

ユーザへのサービス プロファイルの一括関連付け

サービス プロファイルを複数のユーザに追加します。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] インターフェイスを開きます。

ステップ 2 **[一括管理（Bulk Administration）] > [ユーザ（Users）] > [ユーザの更新（Update Users）] > [クエリー（Query）]** を選択します。

[更新するユーザの検索と一覧表示（Find and List Users To Update）] ウィンドウが表示されます。

ステップ 3 [ユーザを次の条件で検索（Find User where）] フィールドで適切なフィルタを指定した後、[検索（Find）] を選択してユーザのリストを取得します。

ステップ 4 [次へ（Next）] を選択します。

[ユーザの更新（Update Users Configuration）] ウィンドウが開きます。

ステップ 5 電話機モードの展開では、インスタント メッセージとプレゼンスを無効にし、[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 1 つオンにします。

他のすべての展開では、[Unified CM IM and Presence のユーザを有効化（Enable User for Unified CM IM and Presence）] チェックボックスの両方をオンにします。

ステップ 6 [UC サービス プロファイル（UC Service Profile）] チェックボックスをオンにし、そのドロップダウン リストからサービス プロファイルを選択します。

重要 Cisco Unified Communications Manager リリース 9.x のみ：ユーザがインスタント メッセージおよびプレゼンスの機能しか使用していない（IM 専用）場合は、[デフォルトの使用（Use Default）] を選択する必要があります。

IM 専用ユーザの場合：Cisco Unified Communications Manager リリース 9.x は、[**UC サービスプロファイル（UC Service Profile**）] ドロップダウン リストで選択された項目に関係なく、常に、デフォルト サービス プロファイルを適用します。

ステップ 7 [**ジョブ情報（Job Information**）] セクションで、ジョブをただちに実行するか後で実行するかを指定します。

ステップ 8 [**送信（Submit**）] を選択します。

連絡先リストの一括事前入力

一括管理ツール（BAT）を使用してユーザの連絡先リストを事前に入力することもできます。

これにより、ユーザの連絡先リストを事前に入力して、クライアントの最初の起動後にユーザが連絡先のセットを自動的に入手できるようにします。

Cisco Jabber はクライアント連絡先リストで最大 300 件の連絡先をサポートします。

手順

	コマンドまたはアクション	目的
ステップ 1	ユーザに提供する連絡先リストを定義した CSV ファイルを作成します。	連絡先リストのインポートのための CSV 作成 （13 ページ）
ステップ 2	BAT を使用して一連のユーザに連絡先リストを一括でインポートします。	BAT を使用した連絡先リストのアップロード （15 ページ）

連絡先リストのインポートのための CSV 作成

CSV ファイルの構造

CSV ファイルは、次の形式である必要があります。

<User ID>, <User Domain>, <Contact ID>, <Contact Domain>, <Nickname>, <Group Name>

CSV ファイル エントリの例は、次のとおりです。

```
userA,example.com,userB,example.com,buddyB,General
```

表 *1:* 入力ファイルのパラメータの説明

パラメータ	説明
[ユーザID（ User ID）]	必須パラメータです。IM and Presence Service ユーザのユーザ ID。これには、最大 132 文字を使用できます。
ユーザのドメイン名（User Domain）	必須パラメータです。IM and Presence Service ユーザのプレゼンス ドメイン。これには、最大 128 文字を使用できます。
コンタクト ID（Contact ID）	必須パラメータです。連絡先リスト エントリのユーザ ID。これには、最大 132 文字を使用できます。
Contact Domain（連絡先ドメイン）	必須パラメータです。連絡先リスト エントリのプレゼンス ドメイン。次の制限は、ドメイン名の形式に適用されます。 • 長さは 128 文字以下である必要があります • 数字、大文字と小文字、およびハイフン（-）だけ含めます • ハイフン（-）で開始または終了してはいけません • ラベルの長さは63 文字以下である必要があります • トップ レベル ドメインは文字だけで、少なくとも 2 文字にする必要があります
ニックネーム（Nickname）	連絡先リスト エントリのニックネーム。これには、最大 255 文字を使用できます。
グループ名（Group Name）	必須パラメータです。連絡先リスト エントリが追加されるグループの名前。これには、最大 255 文字を使用できます。

BAT を使用した連絡先リストのアップロード

始める前に

連絡先が入った CSV ファイルを作成します。

手順

ステップ 1 [**Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration**）] インターフェイスを開きます。

ステップ 2 **[一括管理（Bulk Administration）]>[ファイルのアップロード/ダウンロード（Upload/Download Files）]**の順に選択します。

ステップ 3 [**新規追加（Add New**）] を選択します。

ステップ 4 [**ファイル選択（Choose File**）] を選択して、CSV ファイルを検索し選択します。

ステップ 5 ターゲットとして [**連絡先リスト（Contact Lists**）] を選択します。

ステップ 6 トランザクション タイプとして [**ユーザの連絡先のインポート - カスタム ファイル（Import Users' Contacts – Custom File**）] を選択します。

ステップ 7 [**保存（Save**）] を選択してファイルをアップロードします。

UDS 連絡先検索のための認証設定

Cisco Jabber は連絡先を検索する際に認証されたディレクトリ クエリーをサポートします。認証は、Cisco Unified Communications Manager リリース 11.5 以降で設定されます。

手順

ステップ 1 コマンドライン インターフェイスにログインします。

ステップ 2 **utils contactsearchauthentication status** コマンドを実行し、このノードの連絡先検索の認証の設定を確認します。

ステップ 3 連絡先検索の認証の設定が必要な場合、

- 認証を有効にするには、**utils contactsearchauthentication enable** コマンドを実行します。
- 認証を無効にするには、**utils contactsearchauthentication disable** コマンドを実行します。

ステップ 4 すべての クラスタ ノードに対してこの手順を繰り返します。

（注） 変更を有効にするには、電話をリセットする必要があります。

拡張 UDS 連絡先ソースの有効化

始める前に

拡張 UDS の連絡先の検索は、Cisco Unified Communications Manager リリース 11.5(1) 以降でのみ使用可能です。

手順

ステップ 1 [**Cisco Unified CM の管理**（**Cisco Unified CM Administration**）] インターフェイスを開きます。

ステップ 2 **[システム**（**System**）**]** > **[LDAP]** > **[LDAP 検索**（**LDAP Search**）**]** を選択します。

ステップ 3 エンタープライズ LDAP ディレクトリ サーバを使用してユーザー検索を実行するには、[**エンタープライズ ディレクトリ サーバのユーザ検索を有効にする**（**Enable user search to Enterprise Directory Server**）] チェックボックスをオンにします。

ステップ 4 [**LDAP 検索の設定**（**LDAP Search 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 5 **保存**を選択します。