



# Unified Communications Manager のユーザの作成

---

- [同期の有効化 \(1 ページ\)](#)
- [ユーザ ID の LDAP 属性の指定 \(2 ページ\)](#)
- [ディレクトリ URI に対する LDAP 属性の指定 \(2 ページ\)](#)
- [同期の実行 \(3 ページ\)](#)
- [ロールとグループの割り当て \(4 ページ\)](#)
- [認証オプション \(5 ページ\)](#)

## 同期の有効化

ディレクトリ サーバ内の連絡先データが Cisco Unified Communications Manager に複製されていることを確認するには、ディレクトリ サーバと同期する必要があります。ディレクトリ サーバと同期する前に、同期を有効にする必要があります。

### 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 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 3** [LDAP システム情報 (LDAP System Information) ] セクションに移動します。
  - ステップ 4** [LDAP サーバからの同期を有効にする (Enable Synchronizing from LDAP Server) ] を選択します。
  - ステップ 5** [LDAP サーバタイプ (LDAP Server Type) ] ドロップダウンリストから、データの同期元となるディレクトリ サーバのタイプを選択します。
-

### 次のタスク

ユーザ ID の LDAP 属性を指定します。

## ユーザ ID の LDAP 属性の指定

ユーザをディレクトリ ソースから Cisco Unified Communications Manager に同期する場合は、ディレクトリ内の属性からユーザ ID を生成できます。ユーザ ID を保持するデフォルトの属性は、sAMAccountName です。

### 手順

**ステップ 1** [LDAP システムの設定 (LDAP System Configuration) ] ウィンドウで [ユーザ ID 用 LDAP 属性 (LDAP Attribute for User ID) ] ドロップダウン リストを探します。

**ステップ 2** 必要に応じて、ユーザ ID の属性を指定し、[保存 (Save) ] を選択します。

**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 スキーム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 に対する LDAP 属性の指定

Cisco Unified Communications Manager リリース 9.0(1)以降では、ディレクトリ内の属性からディレクトリ URI を生成できます。

### 始める前に

[同期の有効化。](#)

### 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 適切な LDAP ディレクトリを選択するか、[新規追加 (Add New)] を選択して LDAP ディレクトリを追加します。
- ステップ3 [同期対象の標準ユーザ フィールド (Standard User Fields To Be Synchronized)] セクションを探します。
- ステップ4 [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5 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、必要なパラメータを指定した後、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 [新規追加 (Add New)] 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 [LDAP ディレクトリ (LDAP Directory)] ウィンドウで必要な詳細情報を指定します。
- 指定可能な値と形式の詳細については、『[Cisco Unified Communications Manager Administration Guide](#)』を参照してください。
- ステップ4 情報が定期的に同期されることを保証するには、LDAP ディレクトリ同期スケジュールを作成します。
- ステップ5 [保存 (Save)] を選択します。
- ステップ6 [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 がプレゼンス サーバデータベースにユーザ データを同期します。

## ロールとグループの割り当て

どのタイプの展開でも、ユーザを [標準 CCM エンドユーザ (Standard CCM End Users) ] グループに割り当てます。

### 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) ] の順に選択します。  
[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** 一覧からユーザを探して選択します。  
[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 4** [権限情報 (Permission Information) ] セクションを探します。

**ステップ 5** [アクセス コントロール グループに追加 (Add to Access Control Group) ] を選択します。  
[アクセス コントロール グループの検索と一覧表示 (Find and List Access Control Groups) ] ダイアログボックスが開きます。

**ステップ 6** ユーザのアクセス コントロール グループを選択します。

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 グループが追加が必要となります。

- 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。

**ステップ 7** [選択項目の追加 (Add Selected) ] を選択します。  
[アクセス コントロール グループの検索と一覧表示 (Find and List Access Control Groups) ] ウィンドウが終了します。

ステップ 8 [エンドユーザの設定 (End User Configuration)] ウィンドウで [保存 (Save)] を選択します。

## 認証オプション

### クライアント内の SAML SSO の有効化

#### 始める前に

- 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。
- Cisco Webex Messenger のサービスの SSO を有効にすると、Cisco Unified Communications Manager と Cisco Unity Connection をサポートします。  
このサービス上での SAML SSO の有効化方法については、『*Cisco Webex Messenger Administrator's Guide*』の「Single Sign-On」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。

---

Webex Teams を使用して 1 つの資格情報セットを使用して Webex Teams をログインする方法の詳細については、『*Cisco SSO Communications Deployment Guide*』を参照してください。

## 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。
-