



LDAP ディレクトリの設定

- [LDAP 同期の概要 \(1 ページ\)](#)
- [LDAP 同期の前提条件 \(3 ページ\)](#)
- [LDAP 同期の設定タスクフロー \(3 ページ\)](#)

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。インポートしている間に、エンドユーザを設定することもできます。



- (注) Unified Communication Manager は、LDAPS (SSL を使用した LDAP) をサポートしますが、StartTLS を使用した LDAP はサポートしていません。LDAP サーバ証明書を Unified Communication Manager に Tomcat-Trust 証明書としてアップロードします。

サポートされている LDAP ディレクトリの詳細については、*Cisco Unified Communications Manager* と *IM and Presence Service* の互換性マトリクスを参照してください。

LDAP 同期では、以下の機能がアドバタイズされます。

- **エンドユーザのインポート** : LDAP 同期を使用して、システムの初期設定時にユーザー一覧を会社の LDAP ディレクトリから Unified Communication Manager のデータベースにインポートできます。機能グループテンプレート、ユーザプロファイル、サービスプロファイル、ユニバーサルデバイス、回線テンプレートなどの設定項目が設定されている場合は、設定をユーザに適用することができ、また、同期プロセス中に設定したディレクトリ番号とディレクトリ Uri を割り当てることができます。LDAP 同期プロセスは、ユーザーリストとユーザー固有のデータをインポートし、設定した構成テンプレートを適用します。



- (注) 初期同期が実行された以降は、LDAP 同期を編集することはできません。

- **スケジュールされた更新**：Unified Communication Manager をスケジュールされた間隔で複数の LDAP ディレクトリと同期するように設定できます。これによって確実にデータベースが定期的に更新され、すべてのユーザ データを最新に保ちます。
- **エンドユーザの認証**：LDAP 同期を使用して、システムが Cisco Unified Communication Manager データベースではなく、LDAP ディレクトリに対してエンドユーザパスワードを認証するように設定できます。LDAP 認証によって、企業は、すべての企業内アプリケーションに対応する単一のパスワードをエンドユーザに割り当てることができます。この機能は、PIN またはアプリケーションユーザパスワードには適用されません。
- **Cisco モバイルおよびリモートアクセス クライアントおよびエンドポイントのディレクトリサーバユーザ検索**：企業ファイアウォールの外部で操作している場合でも、社内ディレクトリサーバを検索できます。この機能を有効にすると、ユーザデータサービス (UDS) がプロキシとして機能し、Unified Communication Manager データベースにユーザ検索要求を送信する代わりに、それを社内ディレクトリに送信します。

エンドユーザ用 LDAP 認証

LDAP 同期を使用して、システムが Cisco Unified Communications Manager データベースではなく、LDAP ディレクトリに対してエンドユーザパスワードを認証するように設定できます。LDAP 認証によって、企業は、すべての企業内アプリケーションに対応する単一のパスワードをエンドユーザに割り当てることができます。この機能は、PIN またはアプリケーションユーザパスワードには適用されません。

Cisco モバイルおよびリモート アクセス クライアントおよびエンドポイント向けディレクトリ サーバユーザ検索

以前のリリースでは、Cisco モバイルおよびリモートアクセスクライアント（たとえば、Cisco Jabber）またはエンドポイント（たとえば、Cisco DX 80 電話）を使用しているユーザが企業ファイアウォールの外部でユーザ検索を実行した場合、結果は Cisco Unified Communications Manager に保存されたユーザアカウントに基づいていました。データベースには、ローカルで設定されたか、または社内ディレクトリから同期されたユーザアカウントも含まれています。

このリリースでは、Cisco モバイルおよびリモート アクセス クライアントとエンドポイントは、企業ファイアウォールの外部で動作している場合でも、社内ディレクトリサーバを検索できます。この機能を有効にすると、ユーザデータサービス (UDS) がプロキシとして機能し、Cisco Unified Communications Manager データベースにユーザ検索要求を送信する代わりに、それを社内ディレクトリに送信します。

この機能を使用して、次の結果を実現できます。

- **地理的な場所にかかわらず同じユーザ検索結果を配信**：企業ファイアウォール外に接続されている場合でも、モバイルおよびリモートアクセスクライアントとエンドポイントは、社内ディレクトリを使用してユーザ検索を実行できます。

- Cisco Unified Communications Manager データベースに設定されているユーザアカウントの数を減らす: モバイルクライアントが社内ディレクトリ内のユーザを検索できるようになりました。以前のリリースでは、ユーザの検索結果はデータベースに設定されているユーザに基づいています。ユーザの検索に使用するデータベースに対しては、管理者がユーザアカウントを設定または同期する必要がなくなりました。管理者は、クラスタによって提供されているユーザアカウントのみを設定する必要があります。データベース内のユーザアカウントの総数を減らすと、ソフトウェアアップグレードの時間枠が短縮され、データベースの全体的なパフォーマンスが向上します。

この機能を構成するには、LDAP検索構成ウィンドウでエンタープライズディレクトリサーバーのユーザー検索を有効にし、LDAPディレクトリサーバーの詳細を構成する必要があります。詳細については、「[エンタープライズディレクトリ ユーザ検索の設定 \(9 ページ\)](#)」の手順を参照してください。

LDAP 同期の前提条件

前提タスク

LDAP ディレクトリからエンドユーザをインポートする前に、次のタスクを実行します。

- ユーザー アクセスの設定
- クレデンシャル ポリシーの設定
- 機能グループ テンプレートの設定

自分のシステムにデータを同期するユーザについて、アクティブディレクトリサーバ上の電子メール ID フィールドが確実に単一エントリまたは空白になっているようにします。

LDAP 同期の設定タスクフロー

外部LDAPディレクトリからユーザリストをプルし、Unified Communication Manager のデータベースにインポートするには、以下のタスクを使用します。



- (注) LDAPディレクトリをすでに一度同期している場合、外部LDAPディレクトリから新しい項目を同期することはできますが、Unified Communication Manager 内の新しい設定をLDAPディレクトリ同期に追加することはできません。この場合は、一括管理ツールを使用して、ユーザの更新やユーザの挿入などのメニューを使用できます。『Cisco Unified Communications Manager 一括アドミニストレーションガイド』を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	Cisco DirSync サービスの有効化 (4 ページ)	Cisco Unified Serviceability にログインし、Cisco DirSync サービスを有効にします。
ステップ 2	LDAP ディレクトリ同期の有効化 (5 ページ)	Unified Communication Manager の LDAP ディレクトリ同期を有効化します。
ステップ 3	LDAP フィルタの作成 (6 ページ)	(オプション) Unified Communication Manager に社内 LDAP ディレクトリからユーザのサブセットだけを同期するには、LDAP フィルタを作成します。
ステップ 4	LDAP ディレクトリの同期の設定 (6 ページ)	アクセス制御グループ、機能グループのテンプレートとプライマリ エクステンションのフィールド設定、LDAP サーバのロケーション、同期スケジュール、および割り当てなどの LDAP ディレクトリ同期を設定します。
ステップ 5	エンタープライズ ディレクトリ ユーザ検索の設定 (9 ページ)	(オプション) エンタープライズ ディレクトリ サーバユーザを検索するシステムを設定します。システムの電話機とクライアントをデータベースの代わりにエンタープライズ ディレクトリ サーバに対してユーザの検索を実行するように設定するには、次の手順に従います。
ステップ 6	LDAP 認証の設定 (10 ページ)	(オプション) エンドユーザのパスワード認証に LDAP ディレクトリを使用するには、LDAP 認証を設定します。
ステップ 7	LDAP アグリーメント サービスパラメータのカスタマイズ (11 ページ)	(オプション) 任意指定の [LDAP 同期 (LDAP Synchronization)] サービスパラメータを設定します。ほとんどの導入の場合、デフォルト値のままです。

Cisco DirSync サービスの有効化

Cisco Unified Serviceability で Cisco DirSync サービスをアクティブ化するには、次の手順を実行します。社内の LDAP ディレクトリから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化する必要があります。

手順

- ステップ 1 Cisco Unified Serviceability から、[ツール (Tools)] > [サービスのアクティブ化 (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からパブリッシュ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)]の下で、[Cisco DirSync] ラジオ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。

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させるには、以下の手順で Unified Communication Manager を設定します。



- (注) LDAP ディレクトリをすでに一度同期している場合、外部 LDAP ディレクトリから新しい項目を同期することはできませんが、Unified Communications Manager 内の新しい設定を LDAP ディレクトリ同期に追加することはできません。また、機能グループテンプレートやユーザプロフィールなどの基になる構成アイテムの編集を追加することもできません。すでに1回のLDAP同期を完了しており、別の設定でユーザを追加する場合は、ユーザの更新やユーザの挿入などの一括管理メニューを使用できます。

手順

- ステップ 1 Cisco Unified CM Administration から、[システム (System)] > [LDAP] > [LDAPシステム (LDAP System)] を選択します。
- ステップ 2 Unified Communications Manager で LDAP ディレクトリからユーザをインポートするには、[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から、使用する LDAP ディレクトリサーバの種類を選択します。
- 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で、[エンドユーザの設定 (End User Configuration)] ウィンドウの[ユーザID (User ID)] フィールドに関して、Unified Communications Manager で同期する社内 LDAP ディレクトリから属性を選択します。
- ステップ 5 [保存 (Save)] をクリックします。

LDAP フィルタの作成

LDAP フィルタを作成することで、LDAP 同期を LDAP ディレクトリからのユーザのサブセットのみに制限することができます。LDAP フィルタを LDAP ディレクトリに適用する場合、Unified Communications Manager は、フィルタに一致するユーザのみを LDAP ディレクトリからインポートします。



(注) LDAP フィルタを設定する場合は、RFC4515 に指定されている LDAP 検索フィルタ標準に準拠する必要があります。

手順

- ステップ 1 Cisco Unified CM Administration で、[システム (System)] > [LDAP(LDAP)] > [LDAP フィルタ (LDAP Filter)] を選択します。
- ステップ 2 [新規追加 (Add New)] をクリックして、新しい LDAP フィルタを作成します。
- ステップ 3 [フィルタ名 (Filter Name)] テキストボックスに、LDAP フィルタの名前を入力します。
- ステップ 4 [フィルタ (Filter)] テキストボックスに、フィルタを入力します。フィルタは、UTF-8 で最大 1024 文字まで入力できます。また、丸カッコ (()) で囲みます。
- ステップ 5 [保存 (Save)] 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に Unified Communications Manager を設定するには、この手順を使用します。LDAP ディレクトリの同期により、エンドユーザのデータを外部の LDAP ディレクトリから Unified Communication Manager データベースにインポートして、エンドユーザの設定ウィンドウに表示することができます。ユニバーサル回線とデバイステンプレートを使用する機能グループテンプレートがセットアップされている場合は、新しくプロビジョニングされるユーザとその内線番号に自動的に設定を割り当てることができます。



ヒント アクセス制御グループまたは機能グループテンプレートを割り当てる場合は、LDAP フィルタを使用して、インポートを同じ設定要件のユーザグループに限定できます。

手順

- ステップ 1 Cisco Unified CM Administration で、[System (システム)] > [LDAP] > [LDAP Directory (LDAP ディレクトリ)] 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ディレクトリの設定 (LDAP Directory Configuration)] ウィンドウで、次のように入力します。

- a) [LDAP設定名 (LDAP Configuration Name)] フィールドで、LDAP ディレクトリに一意の名前を割り当てます。
- b) [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 ID を入力します。
- c) パスワードの詳細を入力し、確認します。
- d) [LDAPユーザ検索スペース (LDAP User Search Space)] フィールドに、検索スペースの詳細を入力します。
- e) [ユーザ同期用のLDAPカスタムフィルタ (LDAP Custom Filter for Users Synchronize)] フィールドで、[ユーザのみ (Users Only)] または [ユーザとグループ (Users and Groups)] を選択します。
- f) (オプション) 特定のプロファイルに適合するユーザのサブセットのみにインポートを限定する場合は、[グループ用LDAPカスタムフィルタ (LDAP Custom Filter for Groups)] ドロップダウンリストから LDAP フィルタを選択します。

ステップ 4 [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 Unified Communication Manager が使用するスケジュールを作成します。

ステップ 5 [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。同期プロセスが LDAP 属性の値を Unified Communication Manager のエンドユーザ フィールドに割り当てます。

ステップ 6 URIダイヤリングを展開する場合は、ユーザのプライマリディレクトリURIアドレスに使用されるLDAP属性が割り当てられていることを確認してください。

ステップ 7 [同期対象のカスタムユーザフィールド (Custom User Fields To Be Synchronized)] セクションで、必要な LDAP 属性を持つカスタムユーザフィールド名を入力します。

ステップ 8 インポートしたエンドユーザを、インポートしたすべてのエンドユーザに共通するアクセス制御グループに割り当てるには、次の手順を実行します。

- a) [アクセス制御グループに追加 (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、インポートされたエンドユーザに割り当てる各アクセス制御グループごとに、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。

ステップ 9 機能グループ テンプレートを割り当てる場合は、[機能グループテンプレート (Feature Group Template)] ドロップダウンリストからテンプレートを選択します。

(注) エンドユーザは、そのユーザが存在しない初回のみ、割り当てられた機能グループ テンプレートと同期されます。既存の [機能グループ テンプレート (Feature Group Template)] が変更され、関連付けられた LDAP の完全同期が実行される場合、変更点は更新されません。

- ステップ 10** インポートされた電話番号にマスクを適用して、プライマリ内線番号を割り当てるには、次の手順を実行します。
- [挿入されたユーザの新規回線を作成するために、同期された電話番号にマスクを適用する (Apply mask to synced telephone numbers to create a new line for inserted users)] チェックボックスをオンにします。
 - [マスク (Mask)] を入力します。たとえば、インポートされた電話番号が 8889945 である場合、11XX のマスクによって 1145 のプライマリ内線番号が作成されます。
- ステップ 11** 電話番号のプールからプライマリ内線番号を割り当てる場合は、次の手順を実行します。
- [同期された LDAP 電話番号に基づいて作成されなかった場合、プールリストから新しい回線を割り当て (Assign new line from the pool list if one was not created based on a synced LDAP telephone number)] チェックボックスをオンにします。
 - [DN プールの開始 (DN Pool Start)] テキストボックスと [DN プールの終了 (DN Pool End)] テキストボックスに、プライマリ内線番号を選択する電話番号の範囲を入力します。
- ステップ 12** [LDAPサーバ情報 (LDAP Server Information)] セクションで、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 13** TLS を使用して LDAP サーバに対するセキュアな接続を作成する場合は、[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 14** [保存 (Save)] をクリックします。
- ステップ 15** LDAP 同期を完了させるには、[完全同期を今すぐ実行 (Perform Full Sync Now)] をクリックします。それ以外の場合は、スケジュールされた同期を待つことができます。



(注) LDAP で削除されたユーザは、24 時間後に Unified Communications Manager から自動的に削除されます。また、削除されたユーザが次のいずれかのデバイスのモビリティユーザとして設定されている場合、それらの非アクティブデバイスも自動的に削除されます。

- リモート宛先プロファイル
- リモート接続先プロファイルテンプレート
- モバイルスマートクライアント
- CTI リモート デバイス
- Spark リモートデバイス
- Nokia S60
- Cisco Dual Mode for iPhone
- IMS 統合モバイル (ベーシック)
- キャリア統合モバイル
- Cisco Dual Mode for Android

エンタープライズ ディレクトリ ユーザ検索の設定

データベースではなくエンタープライズ ディレクトリ サーバに対してユーザ検索を実行するように、システムの電話機とクライアントを設定するには、次の手順を使用します。

始める前に

- LDAP ユーザ検索に選択するプライマリ、セカンダリ、および第 3 サーバが Unified Communication Manager のサブスクリバ ノードに到達可能なネットワークにあることを確認します。
- [システム (System)] > [LDAP] > [LDAPシステム (LDAP System)] を選択し、[LDAPシステムの設定 (LDAP System Configuration)] ウィンドウの [LDAPサーバタイプ (LDAP Server Type)] ドロップダウンリストから LDAP サーバのタイプを設定します。

手順

- ステップ 1** Cisco Unified CM Administration で、[システム (System)] > [LDAP] > [LDAP 検索 (LDAP Search)] を選択します。
- ステップ 2** 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 3** [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 4** [保存 (Save)] をクリックします。

ディレクトリサーバの UDS 検索のための LDAP 属性

次の表に、ユーザ検索をエンタープライズディレクトリサーバに入力可能にするオプションが有効になっているときに、UDS ユーザ検索リクエストが使用する LDAP 属性を示します。これらのタイプのディレクトリ要求に対しては、UDS はプロキシとして機能し、企業ディレクトリサーバに検索要求をリレーします。



- (注) UDS ユーザの応答タグは、いずれかの LDAP 属性にマップできます。属性のマッピングは、**LDAPサーバタイプ**ドロップダウンリストから選択したオプションによって決定されます。システム > LDAP > LDAPシステム設定ウィンドウからこのドロップダウンリストにアクセスします。

UDS ユーザの応答タグ	LDAP 属性
userName	<ul style="list-style-type: none"> • samAccountName • uid
firstName	givenName
lastName	sn
middleName	<ul style="list-style-type: none"> • initials • middleName
nickName	nickName
displayName	displayName
phoneNumber	<ul style="list-style-type: none"> • telephonenumber • ipPhone
homeNumber	homephone
mobileNumber	mobile
email	mail
directoryUri	<ul style="list-style-type: none"> • msRTCSIP-primaryuseraddress • mail
department	<ul style="list-style-type: none"> • department • 部署番号
manager	manager
title	title
pager	pager

LDAP 認証の設定

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。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。

手順

- ステップ 1 Cisco Unified CM Administration で、[システム (System)] > [LDAP] > [LDAP認証 (LDAP Authentication)] を選択します。
- ステップ 2 [エンドユーザにLDAP認証を使用 (Use LDAP Authentication for End Users)] チェックボックスをオンにして、ユーザ認証に LDAP ディレクトリを使用します。
- ステップ 3 [LDAPマネージャ識別名 (LDAP Manager Distinguished Name)] フィールドに、LDAP ディレクトリへのアクセス権を持つ LDAP マネージャのユーザ ID を入力します。
- ステップ 4 [パスワードの確認 (Confirm Password)] フィールドに、LDAP マネージャのパスワードを入力します。
- ステップ 5 [LDAPユーザ検索ベース (LDAP User Search Base)] フィールドに、検索条件を入力します。
- ステップ 6 [LDAPサーバ情報 (LDAP Server Information)] セクションで、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 7 TLS を使用して LDAP サーバに対するセキュアな接続を作成する場合は、[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 8 [保存 (Save)] をクリックします。

次のタスク

[LDAP アグリーメント サービスパラメータのカスタマイズ \(11 ページ\)](#)

LDAP アグリーメント サービスパラメータのカスタマイズ

LDAP アグリーメントのシステムレベルでの設定をカスタマイズする、任意指定のサービスパラメータを設定するには、この手順を実行します。これらのサービスパラメータを設定しない場合、Unified Communications Manager により、LDAP ディレクトリ統合のデフォルト設定が適用されます。パラメータの説明については、ユーザインターフェイスでパラメータ名をクリックしてください。

サービスパラメータを使用して次の設定をカスタマイズできます。

- [最大アグリーメント数 (Maximum Number of Agreements)] : デフォルト値は 20 です。
- [最大ホスト数 (Maximum Number of Hosts)] : デフォルト値は 3 です。
- [ホスト障害時の再試行の遅延 (秒) (Retry Delay On Host Failure (secs))] : ホスト障害のデフォルト値は 5 です。
- [ホストリスト障害時の再試行の遅延 (分) (Retry Delay On HotList failure (mins))] : ホストリスト障害のデフォルト値は 10 です。
- [LDAP接続のタイムアウト (秒) (LDAP Connection Timeouts (secs))] : デフォルト値は 5 です。
- [遅延同期の開始時間 (分) (Delayed Sync Start time (mins))] : デフォルト値は 5 です。

- [ユーザカスタマーマップの監査時間 (User Customer Map Audit Time)]

手順

- ステップ1 Cisco Unified CM Administration から、[システム (System)]>[サービスパラメータ (Service Parameters)] の順に選択します。
- 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ュノードを選択します。
- ステップ3 [サービス (Service)] ドロップダウンリストボックスから、[Cisco DirSync] を選択します。
- ステップ4 Cisco DirSyncサービスパラメータの値を設定します。
- ステップ5 [保存 (Save)] をクリックします。

LDAP ディレクトリ サービス パラメータ

サービス パラメータ	説明
最大アグリーメント数	設定可能な LDAP ディレクトリの最大数。デフォルトの設定値は20です。
最大ホスト数	フェールオーバー用として設定できるLDAPホスト名の最大数を指定します。デフォルト値は3です。
ホスト障害再試行の遅延 (secs)	ホストで障害が発生した後、Cisco Unified Communications Manager が最初の LDAP サーバ (ホスト名) への接続を再試行する前の遅延秒数です。デフォルト値は5です。
ホストリストの失敗再試行の遅延(mins)	ホストリストで障害が発生した後、Cisco Unified Communications Manager が設定された各 LDAP サーバ (ホスト名) への接続を再試行する前の遅延分数です。デフォルトは10です。
LDAP Connection Timeout (secs)	Cisco Unified Communications Manager が LDAP 接続を確立できる秒数です。指定した時間内に接続を確立できない場合、LDAP サービスプロバイダーは接続試行を中止します。デフォルトは5です。
遅延同期の開始間隔(mins)	Cisco DirSync サービスの起動後に、Cisco Unified Communications Manager がディレクトリ同期プロセスを開始するまでの遅延分数です。デフォルトは5です。

LDAP 同期済みユーザをローカルユーザに変換する

LDAP ディレクトリと Cisco Unified Communications Manager を同期すると、LDAP に同期されたエンドユーザについては、ローカルユーザに変換しないかぎり、[エンドユーザの設定 (End User Configuration)] ウィンドウ内のフィールドは編集できません。

[エンドユーザの設定 (End User Configuration)] ウィンドウで LDAP 同期ユーザのフィールドを編集するには、そのユーザをローカルユーザに変換します。ただし、この変換を行うと、Cisco Unified Communications Manager を LDAP ディレクトリと同期したときにエンドユーザが更新されなくなります。

手順

- ステップ 1 Cisco Unified CM Administration で、[エンドユーザ (End Users)] > [エンドユーザ管理 (End User Management)] を選択します。
- ステップ 2 [検索 (Find)] をクリックして、エンドユーザを選択します。
- ステップ 3 [ローカルユーザへの変換 (Convert to Local User)] ボタンをクリックします。
- ステップ 4 [エンドユーザ設定 (End User Configuration)] ウィンドウでフィールドを更新します。
- ステップ 5 [保存 (Save)] をクリックします。

アクセス制御グループへの LDAP 同期ユーザの割り当て

LDAP と同期するユーザをアクセス制御グループに割り当てるには、次の手順を実行します。

始める前に

エンドユーザと外部 LDAP ディレクトリが同期されるように Cisco Unified Communication Manager を設定する必要があります。

手順

- ステップ 1 Cisco Unified CM Administration で、[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。
- ステップ 3 [アクセス制御グループに追加 (Add to Access Control Group)] ボタンをクリックします。
- ステップ 4 この LDAP ディレクトリのエンドユーザに適用するアクセス制御グループを選択します。
- ステップ 5 [選択項目の追加 (Add Selected)] をクリックします。
- ステップ 6 [保存 (Save)] をクリックします。
- ステップ 7 [完全同期を実施 (Perform Full Sync)] をクリックします。
Cisco Unified Communication Manager が外部 LDAP ディレクトリと同期し、同期したユーザが正しいアクセス制御グループに挿入されます。

- (注) 同期したユーザは、アクセス制御グループを初めて追加した時にのみ、選択したアクセスグループに挿入されます。完全同期の実行後に LDAP に追加するグループは、同期したユーザに適用されません。

XMPP クライアントにおける連絡先検索のための LDAP ディレクトリ統合

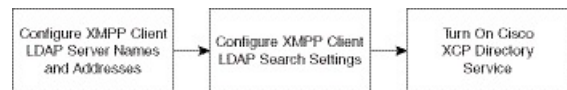
次のトピックでは、サードパーティ製 XMPP クライアントのユーザが LDAP ディレクトリから連絡先を検索および追加できるように IM and Presence Service で LDAP 設定を行う方法について説明します。

IM and Presence Service の JDS コンポーネントは、LDAP ディレクトリとのサードパーティ製 XMPP クライアント通信を処理します。サードパーティ製 XMPP クライアントは、IM and Presence Service の JDS コンポーネントにクエリを送信します。JDS コンポーネントは、プロビジョニングされた LDAP サーバに LDAP クエリを送信し、XMPP クライアントに結果を返します。

ここで説明する設定を実行する前に、XMPP クライアントを Cisco Unified Communications Manager および IM and Presence Service に統合するための設定を実行します。サードパーティ製 XMPP クライアントアプリケーションの統合に関するトピックを参照してください。

図 1: XMPP クライアントにおける連絡先検索のための LDAP ディレクトリ統合のワークフロー

次のワークフローの図は、XMPP クライアントで連絡先を検索するために LDAP ディレクトリを統合する手順の概要です。



次の表に、XMPP クライアントで連絡先を検索するために LDAP ディレクトリを統合するタスクのリストを示します。詳細な手順については、関連するタスクを参照してください。

表 1: XMPP クライアントにおける連絡先検索のための LDAP ディレクトリ統合のタスクリスト

タスク	説明
XMPP クライアントの LDAP サーバの名前とアドレスの設定	LDAP サーバと IM and Presence Service の間で SSL を有効にし、セキュア接続を設定していた場合は、ルート CA 証明書を <code>xmpp-trust-certificate</code> として IM and Presence Service にアップロードします。 ヒント 証明書のサブジェクト CN は LDAP サーバの FQDN と一致する必要があります。

タスク	説明
XMPP クライアントの LDAP 検索の設定	<p>IM and Presence Service でサードパーティ製 XMPP クライアントの連絡先を検索できるように LDAP 検索設定を指定する必要があります。プライマリ LDAP サーバ 1 台とバックアップ LDAP サーバを最大 2 台指定できます。</p> <p>ヒント オプションとして、LDAP サーバから vCard の取得をオンにすることや、vCard を IM and Presence Service のローカル データベースに保存することができます。</p>
Cisco XCP ディレクトリ サービスのオン	<p>サードパーティ製 XMPP クライアントのユーザが LDAP ディレクトリから連絡先を検索および追加できるようにするには、XCP ディレクトリ サービスをオンにする必要があります。</p> <p>ヒント LDAP サーバの設定およびサードパーティ製 XMPP クライアントの LDAP 検索設定を行うまでは、Cisco XCP ディレクトリ サービスをオンにしないでください。そのようにしないと、サービスは実行を停止します。</p>

LDAP アカウント ロックの問題

サードパーティ製 XMPP クライアントに対して設定する LDAP サーバのパスワードを間違えて入力し、IM and Presence Service で XCP サービスを再起動すると、JDS コンポーネントは、不正なパスワードで LDAP サーバに複数回サインインしようとします。数回失敗した後でアカウントをロックアウトするように LDAP サーバが設定されている場合、LDAP サーバはある時点で JDS コンポーネントをロックアウトする可能性があります。JDS コンポーネントが LDAP に接続する他のアプリケーション（IM and Presence Service で必要とは限らないアプリケーション）と同じ資格情報を使用している場合、これらのアプリケーションも LDAP からロックアウトされます。

この問題を解決するには、既存の LDAP ユーザと同じロールと特権を持つ別のユーザを設定し、JDS だけがこの 2 番目のユーザとしてサインインできるようにします。LDAP サーバに間違えたパスワードを入力した場合は、JDS コンポーネントだけが LDAP サーバからロックアウトされます。

XMPP クライアントの LDAP サーバの名前とアドレスの設定

Secure Socket Layer (SSL) を有効にする場合は、LDAP サーバと IM and Presence Service の間にセキュア接続を設定し、cup-xmpp-trust 証明書としてルート認証局 (CA) 証明書を IM and Presence Service にアップロードします。証明書のサブジェクト共通名 (CN) は、LDAP サーバの完全修飾ドメイン名 (FQDN) に一致させる必要があります。

証明書チェーン (ルートノードから信頼できるノードへの複数の証明書) をインポートする場合は、リーフ ノードを除くチェーン内のすべての証明書をインポートします。たとえば、CA が LDAP サーバの証明書に署名した場合は、CA 証明書のみをインポートし、LDAP サーバの証明書はインポートしません。

IM and Presence Service と Cisco Unified Communications Manager 間の接続が IPv4 であっても、IPv6 を使用して LDAP サーバに接続できます。IPv6 がエンタープライズパラメータまたは IM and Presence Service ノードの ETH0 のいずれかで無効になった場合でも、そのノードで内部 DNS クエリを実行し、サードパーティ製 XMPP クライアントの外部 LDAP サーバのホスト名が解決可能な IPv6 アドレスであれば、外部 LDAP サーバに接続できます。



ヒント サードパーティ製クライアントの外部 LDAP サーバのホスト名は [LDAP サーバ - サードパーティ製 XMPP クライアント (LDAP Server - Third-Party XMPP Client)] ウィンドウで設定します。

始める前に

LDAP ディレクトリのホスト名または IP アドレスを取得します。

IPv6 を使用して LDAP サーバに接続する場合は、LDAP サーバを設定する前に、エンタープライズパラメータと展開内の各 IM and Presence Service ノードの Eth0 で IPv6 を有効にします。

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)]> [アプリケーション (Application)]>[サードパーティ製クライアント (Third-Party Clients)]> [サードパーティ製 LDAP サーバ (Third-Party LDAP Servers)] 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 LDAP サーバの ID を入力します。

ステップ 4 LDAP サーバのホスト名を入力します。

IPv6 接続の場合は、LDAP サーバの IPv6 アドレスを入力できます。

ステップ 5 TCP または SSL 接続をリッスンする LDAP サーバのポート番号を指定します。

デフォルトポートは 389 です。SSL を有効にする場合は、ポート 636 を指定します。

ステップ 6 LDAP サーバのユーザ名とパスワードを指定します。これらの値は、LDAP サーバで設定したクレデンシャルと一致する必要があります。

この情報については、LDAP ディレクトリのマニュアルまたは LDAP ディレクトリの設定を確認してください。

ステップ 7 SSL を使用して LDAP サーバと通信するには、[SSL の有効化 (Enable SSL)] をオンにします。

(注) SSL が有効になっている場合、入力するホスト名の値は、LDAP サーバのホスト名または FQDN のいずれかになります。使用される値は、[security certificate CN] または [SAN] フィールドの値と一致する必要があります。

IP アドレスを使用する必要がある場合は、この値も CN フィールドまたは SAN フィールドの証明書で使用する必要があります。

ステップ 8 [保存 (Save)] をクリックします。

ステップ 9 クラスタ内のすべてのノードで Cisco XCP Router サービスを起動します (このサービスがまだ動作していない場合)。



ヒント

- SSL を有効にすると、IM and Presence Service が SSL 接続を確立した後で、SSL 接続の設定およびデータの暗号化と復号化のときにネゴシエーション手順が実行されるため、XMPP の連絡先検索が遅くなる可能性があります。その結果、ユーザが展開内で XMPP の連絡先検索を広範囲に実行する場合、これがシステム全体のパフォーマンスに影響を与えることがあります。
- LDAP サーバの証明書のアップロード後、LDAP サーバのホスト名とポート値で通信を確認するには、証明書インポートツールを使用できます。[Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)] > [システム (System)] > [セキュリティ (Security)] > [証明書インポート ツール (Certificate Import Tool)] を選択します。
- サードパーティ製 XMPP クライアント用の LDAP サーバの設定を更新した場合は、Cisco XCP ディレクトリ サービスを再起動します。[Cisco Unified IM and Presence のサービスアビリティ (Cisco Unified IM and Presence Serviceability)] > [ツール (Tools)] > [コントロール センターの機能サービス (Control Center - Feature Services)] を選択して、このサービスを再起動します。

次のタスク

XMPP クライアントの LDAP 検索の設定に進みます。

XMPP クライアントの LDAP 検索設定

IM and Presence サービスでサードパーティ製 XMPP クライアントの連絡先を検索できるようにする LDAP 検索設定を指定する必要があります。

サードパーティ製 XMPP クライアントは、検索のたびに LDAP サーバに接続します。プライマリ サーバへの接続に失敗すると、XMPP クライアントは最初のバックアップ LDAP サーバを試し、それが使用不可能な場合は、2 番目のバックアップサーバを試します (以下同様)。システムのフェールオーバー中に処理中の LDAP クエリーがあると、その LDAP クエリーは次に使用可能なサーバで完了します。

オプションで LDAP サーバからの vCard の取得をオンにできます。vCard の取得をオンにした場合：

- 社内 LDAP ディレクトリは vCards を保存します。
- XMPP クライアントが自身の vCard、または連絡先の vCard を検索すると、vCard は JDS サービスによって LDAP から取得されます。
- クライアントは、社内 LDAP ディレクトリを編集することを許可されていないため、自身の vCard を設定または変更できません。

LDAP サーバからの vCard の取得をオフにした場合

- IM and Presence サービスはローカル データベースに vCard を保存します。
- XMPP クライアントが自身の vCard、または連絡先の vCard を検索すると、vCard はローカルの IM and Presence サービス データベースから取得されます。
- クライアントは、自身の vCard を設定または変更できます。

次の表はXMPP クライアントの LDAP 検索の設定の一覧です。

表 2: XMPP クライアントの LDAP 検索設定

フィールド	設定
[LDAPサーバタイプ (LDAP Server Type)]	LDAP サーバ タイプをこのリストから選択します。 <ul style="list-style-type: none"> • Microsoft Active Directory • [汎用ディレクトリ サーバ (Generic Directory Server)] : 他のサポートされている LDAP サーバタイプ (iPlanet、Sun ONE、または OpenLDAP) を使用する場合は、このメニュー項目を選択します。
User Object Class	LDAP サーバタイプに適切なユーザ オブジェクト クラスの値を入力します。この値は、LDAP サーバで設定されたユーザ オブジェクト クラスの値と一致する必要があります。 Microsoft Active Directory を使用する場合、デフォルト値は [ユーザ (user)] です。
Base Context (ベース コンテキスト)	LDAP サーバに適切なベース コンテキストを入力します。この値は、LDAP サーバの設定済みドメインおよび/または組織構造と一致する必要があります。
ユーザ属性	LDAP サーバタイプに適切なユーザ属性値を入力します。この値は、LDAP サーバで設定されたユーザ属性値と一致する必要があります。 Microsoft Active Directory を使用する場合、デフォルト値は [sAMAccountName] です。 ディレクトリ URI IM アドレス スキームが使用され、ディレクトリ URI がメールまたは msRTCSIPPrimaryUserAddress にマッピングされた場合、メールまたは msRTCSIPPrimaryUserAddress はユーザ属性として指定する必要があります。
LDAP Server 1 (LDAP サーバ 1)	プライマリ LDAP サーバを選択します。
LDAP Server 2 (LDAP サーバ 2)	(任意) バックアップ LDAP サーバを選択します。
LDAP Server 3 (LDAP サーバ 3)	(任意) バックアップ LDAP サーバを選択します。

始める前に

XMPP クライアントの LDAP サーバの名前とアドレスを指定します。

手順

- ステップ 1 [Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)] > [アプリケーション (Application)] > [サードパーティクライアント (Third-Party Clients)] > [サードパーティ LDAP 設定 (Third-Party LDAP Settings)] を選択します。
- ステップ 2 次の各フィールドに情報を入力します。
- ステップ 3 ユーザが連絡先の vCard を要求し、LDAP サーバから vCard 情報を取得できるようにする場合は、**[LDAP から vCard を作成 (Build vCards from LDAP)]** をオンにします。ユーザが連絡先リストに参加するときにクライアントが自動的に vCard を要求できるようにする場合は、チェックボックスをオフのままにします。この場合、クライアントはローカル IM and Presence サービス データベースから vCard 情報を取得します。
- ステップ 4 vCard FN フィールドを作成するために必要な LDAP フィールドを入力します。ユーザが連絡先の vCard を要求すると、クライアントは、vCard FN フィールドの値を使用して連絡先リストに連絡先の名前を表示します。
- ステップ 5 検索可能な LDAP 属性テーブルで、適切な LDAP ユーザ フィールドにクライアント ユーザ フィールドをマッピングします。

Microsoft Active Directory を使用すると、IM and Presence サービスはテーブルにデフォルト属性値を読み込みます。
- ステップ 6 [保存 (Save)] をクリックします。
- ステップ 7 Cisco XCP Router サービスを起動します (このサービスがまだ動作していない場合)。

ヒント サードパーティ製 XMPP クライアント用の LDAP 検索の設定を更新した場合は、Cisco XCP ディレクトリ サービスを再起動します。**[Cisco Unified IM and Presence のサービスアビリティ (Cisco Unified IM and Presence Serviceability)]** > **[ツール (Tools)]** > **[コントロールセンター - 機能サービス (Control Center - Feature Services)]** を選択して、このサービスを再起動します。

次のタスク

Cisco XCP ディレクトリ サービスをオンに設定します。

Cisco XCP ディレクトリ サービスのオン

サードパーティ製 XMPP クライアントのユーザが LDAP ディレクトリから連絡先を検索および追加できるようにするには、Cisco XCP ディレクトリ サービスをオンにする必要があります。クラスタ内のすべてのノードで Cisco XCP ディレクトリ サービスをオンにします。



-
- (注) LDAP サーバおよびサードパーティ製 XMPP クライアントの LDAP 検索設定を設定するまでは、Cisco XCP ディレクトリ サービスをオンにしないでください。Cisco XCP ディレクトリ サービスをオンにするが、LDAP サーバおよびサードパーティ製 XMPP クライアントの LDAP 検索を設定しない場合、サービスは開始してから再度停止します。
-

始める前に

LDAP サーバおよびサードパーティ製 XMPP クライアントの LDAP 検索を設定します。

手順

-
- ステップ 1** [Cisco Unified IM and Presence のサービスアビリティ (Cisco Unified IM and Presence Serviceability)] > [ツール (Tools)] > [サービスの開始 (Service Activation)] を選択します。
- ステップ 2** [サーバ (Server)] メニューから [IM and Presence サービス (IM and Presence Service)] ノードを選択します。
- ステップ 3** [Cisco XCP ディレクトリ サービス (Cisco XCP Directory Service)] を選択します。
- ステップ 4** [保存 (Save)] をクリックします。
-

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。