LDAP 同期の設定

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 Communications 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 Communications 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一覧を会社の LDAP ディレクトリから Unified Communications 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 テンプレートおよびユニバーサル回線テンプレートなどの項目を事前設定済みである場合は、ユーザに設定を適用することや、設定したディレクトリ番号とディレクトリ URI を同期プロセス中に割り当てることができます。LDAP 同期プロセスは、ユーザおよびユーザ固有のデータのリストをインポートし、セットアップされた設定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 Communications 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 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 MRA 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**：社内ディレクトリ サーバが企業ファイアウォール外で運用されている場合でも検索できます。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 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。

LDAP 同期の前提条件

前提条件のタスク

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 アクセスを設定します。ユーザに割り当てるアクセス制御グループを決定します。ほとんどの導入環境では、デフォルトのグループで十分です。ロールとグループをカスタマイズする必要がある場合は、アドミニストレーション ガイドの「ユーザ アクセスの管理」の章を参照してください。
- 新しくプロビジョニングされたユーザーにデフォルトで適用されるクレデンシャル ポリシーに、デフォルトのクレデンシャルを設定します。
- LDAP ディレクトリからユーザを同期する場合は、機能グループ テンプレートが設定されていることを確認してください。このテンプレートには、ユーザ プロファイル、サービス プロファイル、ユーザの電話と電話の内線に割り当てるユニバーサル回線テンプレートおよびユニバーサル デバイス テンプレートの設定が含まれます。

（注） システムにデータを同期するユーザについては、Active Directory サーバでの電子メール ID フィールドが一意のエントリであるか空白であることを確認してください。

LDAP 同期設定のタスク 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 Communications 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 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。この場合、一括管理ツールと、[ユーザの更新（Update Users）] や [ユーザの挿入（Insert Users）] などのメニューを使用できます。『*Bulk Administration Guide for Cisco Unified Communications Manager*』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 ディレクトリの同期化の有効化 （4 ページ）	Unified Communications 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 （5 ページ）	**オプション**：Unified Communications 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 コントロール 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 サーバの場所、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 （8 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。

	コマンドまたはアクション	目的
ステップ 6	LDAP 認証の設定 （8 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 （9 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問題ありません。

Cisco DirSync サービスの有効化

Cisco DirSync サービスをアクティブにするには、Cisco Unified Serviceability で次の手順を実行します。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。

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。

LDAP ディレクトリの同期化の有効化

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 Communications 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すが、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 プロファイルなどの基板となる設定項目の編集内容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** 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** 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 Communications 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。ユニバーサル回線テンプレートおよびデバイス テンプレートを使用して機能グループ テンプレートを設定済みである場合は、新しくプロビジョニングされた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 コントロール 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（LADP）] > [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ユーザサーチスペース（LDAP User Search Space）] フィールドに、サーチ 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) （任意）。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** 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 Communications 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 Communications 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 ディレクトリの URI アドレスに使用される LDAP 属性を割り当ててください。

ステップ 7 **同期するカスタム ユーザ フィールド** のセクションで、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 コントロール 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 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) [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。

a) [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。

b) [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。

a) [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。

b) [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施（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。

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 Communications Manager のサブスクライバ 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。フィールドおよび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。

（注） OpenLDAP サーバでルーム オブジェクトとして表される会議室を検索するには、カスタム フィルタを (| (objectClass=intOrgPerson)(objectClass=rooms)) に設定します。これにより、Cisco Jabber クライアントは部屋に関連付けられた名前およびダイヤル番号で会議室を検索できます。

会議室は、ルーム オブジェクトの OpenLDAP サーバに、**givenName**、**sn**、**mail**、**displayName**、または **telephonenumber** の属性が設定されていると検索可能です。

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 ユーザ用 LDAP 認証の使用（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 ディレクトリにアクセス権がある 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 （9 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 で、**[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ャ 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。