LDAP ディレクトリの設定

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ディレクトリについては、*Cisco Unified Communications Manager*と*IM*およびプレセンスサービス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、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 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。

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 Mobile および Remote Access クライアントとエンドポイントのディレクトリ サーバ ユーザ検索

以前のリリースでは、Cisco Mobile と Remote Access 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 Mobile および Remote Access 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。

- 地理的な場所に関係なく、同じユーザ検索結果を提供する：モバイルおよび Remote Access 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。企業ファイアウォールの外部で接続されている場合でも実行可能です。

- Cisco Unified Communications Manager データベースに設定されるユーザ アカウントの数を削減する：モバイル クライアントは、社内ディレクトリ内のユーザを検索できます。以前のリリースでは、ユーザ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した。今回のリリースでは、ユーザ検索のためだけにユーザアカウントをデータベースに設定または同期する必要がなくなりました。管理者は、クラスタによって管理されているユーザ アカウントを設定すれば作業が完了します。データベース内のユーザ アカウントの合計数が削減すると、データベース全体のパフォーマンスが改善される一方、ソフトウェア アップグレードの時間枠が短縮されます。

この機能を設定するには、[LDAP 検索の設定（LDAP Search Configuration）] ウィンドウで [企業ディレクトリ サーバでのユーザ検索を有効にする（Enable user search to Enterprise Directory Server）] オプションを有効にし、LDAP ディレクトリ サーバの詳細を設定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 （8 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 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 （5 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。
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**オプションでLDAP同期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、ユニファイドコミュニケーションマネージャ内の新しい設定を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つのLDAP同期を完了していて、別の設定でユーザを追加する必要がある場合は、ユーザの更新やユーザの挿入などのバルク管理メニューを使用できます。

手順

ステップ 1 Cisco Unified CMの管理で、**システム** > **LDAP** > **LDAPシステム** 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**ドロップダウンリストで、**エンドユーザ設定**ウィンドウの**ユーザID**フィールドに関してUnified Communications Managerで同期する社内LDAPディレクトリの属性を選択します。

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 同期を LDAP ディレクトリのユーザのサブネットに制限するには、LDAP フィルタを作成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 の管理（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 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。セットアップ機能を使用している場合は、ユニバーサルラインとデバイステンプレートのグループテンプレートを使用して、新しくプロビジョニングされたユーザとその拡張機能に設定を自動的に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 の管理で、**[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** ウィンドウで、以下を入力します。

a) **LDAP 構成名** フィールドに、一意の LDAP ディレクトリ名を指定します。
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**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** フィールドで、**ユーザのみ** あるいは **ユーザおよびグループ**のどちらかを選択します。
f) （任意）。インポートを特定のプロファイルに適合するユーザのサブセットにのみ限定する場合は、**LDAP カスタム フィルタ** 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) [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** 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） ユーザが存在しない初回のみ、エンド ユーザは割り当てられた**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) **同期された電話番号にマスクを適用して、挿入されたユーザの新しい回線を作成する**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 のマスクで、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**セクションに、LDAP サーバのホスト名あるいは IP アドレスを入力します。

ステップ 13 TLS で LDAP サーバへのセキュアな接続を作成するには、**TLS を使用する** 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同期を完了するには、**完全同期の実行**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** > **LDAP** > **LDAP システム**から、**LDAP システム設定** ウィンドウを開き、**LDAP サーバ タイプ** ドロップダウン リスト から LDAP のタイプを設定します。

手順

ステップ 1 Cisco Unified CM の管理で、**[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。

（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。

ディレクトリ サーバの UDS 検索用の LDAP 属性

次の表に、[エンタープライズ ディレクトリ サーバに対するユーザ検索を有効化（Enable user search to Enterprise Directory Server）] オプションが有効になっている場合に、UDS ユーザ検索要求で使用される LDAP 属性の一覧を示します。このようなタイプのディレクトリ要求の場合、UDS はプロキシとして機能して、社内ディレクトリ 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 属性にマッピングされることがあります。属性のマッピングは、[LDAP サーバ タイプ（LDAP Server Type）] ドロップダウン リストから選択するオプションによって決まります。このドロップダウン リストには、**[システム（System）]** > **[LDAP]** > **[LDAP システムの設定（LDAP System Configuration）]** ウィンドウからアクセスします。

UDS ユーザの応答タグ	LDAP 属性
userName	• samAccountName • uid
firstName	givenName
lastName	sn
middleName	• initials • middleName
nickName	nickName
displayName	displayName
phoneNumber	• telephonenumber • ipPhone
homeNumber	homephone
mobileNumber	mobile

UDS ユーザの応答タグ	LDAP 属性
email	メール アドレス
directoryUri	• msRTCSIP-primaryuseraddress • mail
部署	• 部署 • departmentNumber
manager	manager
タイトル	タイトル
ポケットベル	ポケットベル

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 の管理で、**[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** 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** 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** セクションに、LDAP サーバのホスト名あるいは IP アドレスを入力します。

ステップ 7 TLS で LDAP サーバへのセキュアな接続を作成するには、**TLS を使用する** 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

次の手順を実行して、LDAP契約のシステムレベル設定をカスタマイズするオプションのサービスパラメータを設定します。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ます。

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 LDAP アグリーメント数**デフォルト値は20です。
- **最大ホスト数**デフォルト値は3です。
- **[ホストの失敗時の再試行遅延**(秒)]: ホスト障害のデフォルト値は 5 です。
- **ホストリストが失敗した場合の再試行の遅延（分）**：ホストリストの失敗のデフォルト値は10です。
- **LDAP接続のタイムアウト(secs)**：デフォルト値は5です。
- **LDAP同期の開始間隔**：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**

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。

LDAP ディレクトリ サービスのパラメータ

サービス パラメータ	説明
Maximum Number of Agreements	自分で設定できる LDAP ディレクトリの最大数。デフォルト設定は 20 です。
Maximum Number of Hosts	フェールオーバ用に設定できる LDAP ホスト名の最大数。デフォルト値は 3 です。
Retry Delay on Host Failure (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。

サービス パラメータ	説明
Retry Delay on HostList Failure (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。
Delayed Sync Start Time (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同期済みユーザのローカル ユーザへの変換

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 の管理（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 コントロール 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 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。

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 Communications Manager を設定する必要があります。

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 [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 コントロール 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 コントロール 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 [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 Communications 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 コントロール グループに挿入されます。

（注） 同期したユーザは、アクセス コントロール 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 xmpp-trust-certificate 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。
XMPP クライアントの LDAP 検索の設定	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。 **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。
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、XCP ディレクトリ サービスをオンにする必要があります。 **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。

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って入力し、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 サーバに間違っ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 Server - Third-Party XMPP Client（LDAP サーバ - サードパーティ製 XMPP クライアント）]** 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 Administration（Cisco Unified CM IM and Presence の管理）]** > **[Application（アプリケーション）]** > **[Third-Party Clients（サードパーティ製クライアント）]** > **[Third-Party LDAP Servers（サードパーティ製 LDAP サーバ）]** を選択します。

ステップ 2　**[Add New（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、**[Enable SSL（SSL の有効化）]** をオンにします。

（注） SSL が有効になっている場合、入力できる**ホスト名**の値は、LDAP サーバのホスト名または FQDN です。使用する値は、セキュリティ証明書の **CN** または **SAN** フィールドの値と一致している必要があります。

IP アドレスを使用する必要がある場合は、この値が証明書の **CN** または **SAN** フィールドにも使用されている必要があります。

ステップ 8 **[Save（保存）]** 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 Administration（Cisco Unified CM IM and Presence の管理）]** > **[System（システム）]** > **[Security（セキュリティ）]** > **[Certificate Import Tool（証明書インポート ツール）]** 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 Serviceability（Cisco Unified IM and Presence のサービスアビリティ）]** > **[Tools（ツール）]** > **[Control Center - Feature Services（コントロール センターの機能サービス）]** 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 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しすると、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 Service 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 Service 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 Server Type（LDAP サーバ タイプ）	LDAP サーバ タイプをこのリストから選択します。 • Microsoft Active Directory • [Generic Directory Server（汎用ディレクトリ サーバ）]：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。

フィールド	設定
User Object Class（ユーザ オブジェクト クラス）	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 [user（ユーザ）] 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している必要があります。
User Attribute（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 Administration（Cisco Unified CM IM and Presence の管理）] > [Application（アプリケーション）] > [Third-Party Clients（サードパーティ クライアント）] > [Third-Party LDAP Settings（サードパーティ LDAP 設定）]** を選択します。

ステップ 2 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、**[Build vCards from LDAP（LDAP から vCard を作成）]** 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 Service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 Service 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 **[Save（保存）]** 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 Serviceability（Cisco Unified IM and Presence のサービスアビリティ）]** > **[Tools（ツール）]** > **[Control Center - Feature Services（コントロール センター - 機能サービス）]** 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 Serviceability（Cisco Unified IM and Presence のサービスアビリティ）] > [Tools（ツール）] > [Service Activation（サービスの開始）]** を選択します。

ステップ 2 [Server（サーバ）] メニューから [IM and Presence Service（IM and Presence Service ）] ノードを選択します。

ステップ 3 **[Cisco XCP Directory Service（Cisco XCP ディレクトリ サービス）]** を選択します。

ステップ 4 **[保存 (Save)]** をクリックします。