Cisco Unity Connection を使用した LDAP ディレクトリとの連動

ライトウェイト ディレクトリ アクセス プロトコル（LDAP）は、社内ディレクトリに保存されたユーザー情報にアクセスするための標準方式を Cisco Unity Connection などのアプリケーションに提供します。企業はすべてのユーザ情報を、複数のアプリケーションで利用できる単一リポジトリに集中化させることができます。追加、移動、および変更が簡単なので、保守コストも大幅に削減されます。

- **ユーザー作成**：LDAP ディレクトリからデータをインポートして Unity Connection ユーザーを作成できます。
- **データの同期**：Unity Connection は、Unity Connection データベースのユーザーデータと Active Directory のデータを自動的に同期するように設定されています。
- **シングルサインオン**：Unity Connection Web アプリケーションのユーザー名とパスワードを Active Directory に対して認証するように Unity Connection を設定します。これにより、ユーザーが複数のアプリケーションパスワードを管理する必要がなくなります。（電話パスワードは引き続き、Unity Connection データベース内で管理されます）

Unity Connection は LDAP ディレクトリ内のデータへのアクセスに、標準の LDAPv3 を使用します。Unity Connection が同期用にサポートする LDAP ディレクトリのリストについては、https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/requirements/b_15cucsysreqs.html で入手可能な『Cisco Unity Connection のシステム要件リリース *15*』の「LDAP ディレクトリ統合の要件」の項を参照してください。

- LDAP 同期 （1 ページ）
- LDAP 認証 （9 ページ）

LDAP 同期

LDAP の同期では、Cisco Directory Synchronization（DirSync）という内部ツールを使用して、Cisco Unity Connection ユーザーデータ（氏名、エイリアス、電話番号など）の小さいサブセットと、社内 LDAP ディレクトリ内の対応するデータを同期します。Unity Connection データベー

ス内のユーザーデータを社内LDAPディレクトリ内のユーザーデータと同期するには、次のタスクを実行します。

1. LDAP 同期を設定し、Unity Connection 内のデータと LDAP ディレクトリ内のデータの関係を定義します。「LDAP 同期化の設定 （2 ページ）」の項を参照してください。
2. LDAP ディレクトリからデータをインポートしたり、既存の Unity Connection ユーザーのデータを LDAP ディレクトリ内のデータに関連付けたりして、新しい Unity Connection ユーザーを作成します。「Unity Connection ユーザーを作成する （6 ページ）」の項を参照してください。

Unity Connection にインポートする LDAP ユーザーをさらに制御するために、Unity Connection ユーザーを作成する前に 1 つ以上の LDAP フィルタを作成できます。LDAP ユーザーのフィルタリングを参照してください。

LDAP 同期化の設定

LDAP ディレクトリの同期化を設定する場合は、Cisco Unity Connection サーバーまたはクラスタごとに、最大 20 の LDAP ディレクトリ構成を作成できます。各 LDAP ディレクトリ構成では、1 つのドメインまたは 1 つの組織ユニット（OU）だけをサポートできます。5 つのドメインまたは OU からユーザをインポートする場合は、LDAP ディレクトリ構成を 5 つ作成する必要があります。

Unity Connection ネットワーキングサイトは、サイトに参加している Unity Connection サーバーまたはクラスタごとに最大 20 の LDAP ディレクトリ設定もサポートします。たとえば、サーバーが 5 つあるデジタルネットワークの場合、最大 25 のドメインからユーザーをインポートできます。

160,000 人のユーザーのデータを LDAP ディレクトリと同期できます。

各 LDAP ディレクトリで、次の項目を指定します。

- **設定がアクセスするユーザー検索ベース**：ユーザー検索ベースは、Unity Connection がユーザーアカウントの検索を開始する LDAP ディレクトリツリー内の位置です。Unity Connection は、検索ベースで指定されたツリーまたはサブツリー（ドメインまたは OU）内のユーザーをすべてインポートします。Unity Connection サーバーまたはクラスタは、たとえば同じ Active Directory フォレストなど、同じディレクトリルートを持つサブツリーからだけ、LDAP データをインポートできます。

（注） Unity Connection サーバーの LDAP ディレクトリ設定で指定されたユーザー検索ベースには、合計 120,000 人以下の LDAP ユーザーが含まれている必要があります。Unity Connection ユーザーにならない大量の LDAP ユーザーをインポートすると、メッセージに使用できるディスク容量が減少し、データベースのパフォーマンスが低下し、アップグレードに時間がかかります。

Microsoft Active Directory 以外の LDAP ディレクトリを使用している場合や、ユーザー検索ベースとしてディレクトリのルートを指定する Unity Connection LDAP ディレクトリ設定を作成する場合は、Unity Connection でディレクトリ内のすべてのユーザーに対してデータがインポートされます。Unity Connection にアクセスを許可しないサブツリー（たとえば、サービスアカウントのサブツリー）がディレクトリのルートに含まれている場合、次の手順のいずれかを実行してください。

- 2 つ以上の Unity Connection LDAP ディレクトリ設定を作成し、Unity Connection でアクセスしないユーザーを除外する検索ベースを指定します。
- 1 つ以上の LDAP 検索フィルタを作成します。詳細については、https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/administration/guide/b_15cucsag.html にある『Cisco Unity Connection のシステム アドミニストレーション ガイド リリース15』の「LDAP」の章にある「LDAP ユーザーのフィルタリング」の項を参照してください。

Active Directory 以外のディレクトリの場合、そのために複数の構成を作成することになっても、できるだけ少ない数のユーザーを含む検索ベースを指定して同期に必要な時間を短縮することを推奨します。

Active Directory を使用していて、ドメイン内に子ドメインが存在する場合、各子ドメインにアクセスするための個別の構成を作成する必要があります。Unity Connection は、同期中は Active Directory の照会に従いません。これは、複数のツリーが存在する Active Directory フォレストについても同様です。各ツリーにアクセスするには、1 つ以上の構成を作成する必要があります。この構成では、UserPrincipalName（UPN）属性を Unity Connection の [エイリアス（Alias）] フィールドにマッピングする必要があります。UPN は、フォレスト全体で一意であることが Active Directory によって保証されます。マルチツリーの AD シナリオで UPN 属性を使用する場合の追加の考慮事項については、「認証と Microsoft Active Directory に関するその他の考慮事項 （11 ページ）」の項を参照してください。

サイト内またはサイト間ネットワーキングを使用して、それぞれが LDAP ディレクトリと統合されている 2 つ以上の Unity Connection サーバーをネットワーク化する場合は、別の Unity Connection サーバーのユーザー検索ベースと重複する 1 つの Unity Connection サーバーのユーザー検索ベースを指定したり、複数の Unity Connection サーバーに同じ Unity Connection ユーザのユーザーアカウントとメールボックスを使用したりしないでください。

（注） 1 つまたは複数の Unity Connection サーバーに LDAP フィルタを作成すると、ユーザーの重複を避けることができます。https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/administration/guide/b_15cucsag.html にある『Cisco Unity Connection のシステム アドミニストレーション ガイド リリース15』の「LDAP」の章にある「LDAP ユーザーのフィルタリング」の項を参照してください。

- **Unity Connection が、ユーザー検索ベースで指定されたサブツリーへのアクセスに使用する LDAP ディレクトリ内の管理者アカウント。**

Connection はこのアカウントを使用して、ディレクトリへのバインドを実行し、認証します。検索ベースのすべてのユーザーオブジェクトを「読み取る」ための最小限の権限が設定されており、また、有効期限のないパスワードが設定されている Unity Connection 専用アカウントを使用することを推奨します。（管理者アカウントのパスワードを変更すると、Unity Connection を新しいパスワードで再設定する必要があります）

複数の設定を作成する場合は、設定ごとに 1 つの管理者アカウントを作成し、そのアカウントには、対応するサブツリー内だけのすべてのユーザーオブジェクトの「読み取り」権限を付与することを推奨します。設定を作成する場合、管理者アカウントには完全識別名を入力します。そのため、このアカウントは LDAP ディレクトリ ツリー内の任意の場所に属することができます。

- **Unity Connection が Unity Connection データベースと LDAP ディレクトリを自動的に再同期化する頻度（実行する場合）。**

  再同期化について、次回実行する日時、1 回だけ実行するかスケジュールに従って実行するか、またスケジュールに従う場合は、時間、日、週、または月単位で実行する頻度（6 時間以上）を指定できます。複数の規定で同じ LDAP サーバーを同時に問い合わせることがないように、同期化スケジュールをずらすことをお勧めします。営業時間外に同期が実行されるように、同期スケジュールを設定する。

- **Unity Connection が LDAP データへのアクセスに使用する LDAP サーバーのポート。**
- **オプションで、LDAP サーバーと Unity Connection サーバーの間で転送されるデータの暗号化に SSL を使用するかどうか。**
- **1 つ以上の LDAP サーバ。**

  いくつかの LDAP ディレクトリでは、同期化を試行する際に Unity Connection が使用する LDAP ディレクトリサーバーは、3 つまで指定できます。Unity Connection は、指定された順序でサーバーに接続しようとします。どのディレクトリサーバーも応答しない場合、同期化は失敗します。Unity Connection は、次回にスケジュールされた同期化の時間に再実行します。ホスト名ではなく IP アドレスを使用することで、ドメイン ネーム システム（DNS）の可用性への依存を解消できます。

（注） 同期化のために Unity Connection がアクセスする LDAP ディレクトリサーバーが利用できなくなるときに備えて追加の LDAP ディレクトリサーバーをバックアップとして指定することは、すべての LDAP ディレクトリでサポートされているわけではありません。使用している LDAP ディレクトリが複数のディレクトリサーバーの指定をサポートするかどうかの詳細については、https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/requirements/b_15cucsysreqs.html にある『Cisco Unity Connection のシステム要件リリース 15』の「LDAP ディレクトリ統合の要件」の項を参照してください。

- **LDAP ディレクトリ属性の Unity Connection フィールドへのマッピングについては、下の表に記載されています。**

Unity Connection の [エイリアス（Alias）] フィールドへのマッピングは、すべての構成で同一にする必要があります。LDAP 属性を Unity Connection の [エイリアス（Alias）] フィールドにマッピングする場合は、次の手順を実行します。

- LDAP ディレクトリから Unity Connection にインポートするすべてのユーザーが、その属性で一意の値を持つことを確認します。
- Unity Connection データベース内にすでにユーザーが存在する場合は、ディレクトリからインポートするユーザーの属性の値と、既存の Unity Connection ユーザーの [エイリアス（Alias）] フィールドの値が一致しないことを確認します。

ディレクトリから Unity Connection にインポートするすべてのユーザーについて、LDAP の sn 属性に値が存在する必要があります。sn 属性の値が空白の LDAP ユーザーは、Unity Connection データベースにインポートされません。

LDAP ディレクトリ内のデータの完全性を保護するために、インポートする値は Unity Connection ツールを使用して変更できません。Unity Connection 固有のユーザーデータ（グリーティング、通知デバイス、カンバセーションプリファレンスなど）は Unity Connection で管理され、Unity Connection のローカルデータベースだけに保存されます。

パスワードまたは PIN は、LDAP ディレクトリから Unity Connection データベースにコピーされません。Unity Connection ユーザーを LDAP ディレクトリに対して認証する場合は、「LDAP 認証 （9 ページ）」を参照してください。

表 *1 : Cisco Unity Connection* ユーザーフィールドに *LDAP* ディレクトリ属性をマッピングする

LDAP ディレクトリ属性	Cisco Unity Connection ユーザーフィールド
次のいずれかが必要です。 • samAccountName • メール • employeeNumber • telephoneNumber • userPrincipleName	エイリアス
givenName	名
次のいずれかが必要です。 • middleName • initials	イニシャル
SN	姓
manager	マネージャ
department	部署名
次のいずれかが必要です。 • telephoneNumber • ipPhone	社内電話番号

次のいずれかが必要です。 • mail • samAccountName	社内電子メール アドレス
title	タイトル
homePhone	自宅（インポートされるが、現在は使用されない。Unity Connection Administration では表示されない）
mobile	携帯電話（インポートされるが、現在は使用されない。Unity Connection Administration では表示されない）
pager	ポケットベル（インポートされるが、現在は使用されない。Unity Connection Administration では表示されない）
次のいずれかが必要です。 • msRTCSIP-primaryuseraddress • mail • なし	ディレクトリ URI
表示名	表示名

クラスタリング（アクティブ/アクティブ高可用性）構成の場合、LDAPディレクトリからインポートされたデータも含めて、すべてのユーザーデータは Unity Connection パブリッシャサーバーからサブスクライバサーバーに自動的にレプリケートされます。この構成では、Cisco DirSync サービスはパブリッシャ サーバだけで実行されます。

（注） [内線番号（Extension）] フィールドは、LDAP 電話番号を変更しても更新されません。その結果、必要に応じて、LDAP 電話番号を変更できます。完全に異なる番号を指定することもできます。次回 Connection でデータを LDAP ディレクトリと同期するときに、内線番号は上書きされません。

Unity Connection ユーザーを作成する

LDAP ディレクトリと連動する Unity Connection システムでは、LDAP ディレクトリからデータをインポートするか、既存の Unity Connection ユーザーを変換して LDAP ディレクトリと同期化するか、またはその両方を実行して、Unity Connection ユーザーを作成できます。次の点に注意してください。

- LDAP データをインポートして Unity Connection ユーザーを作成する場合、Unity Connection は表 10-1 で指定された値を LDAP ディレクトリから取得し、指定した Unity Connection ユーザーテンプレートから残りの情報を入力します。
- 既存のユーザーを変換する場合、表 10-1 に示すフィールドの既存の値は、LDAP ディレクトリ内の値で置き換えられます。

- LDAP ディレクトリからインポートするすべてのユーザについて、Unity Connection [エイリアス（Alias）] フィールドにマッピングする LDAP 属性の値は、Unity Connection オブジェクト（スタンドアロンユーザー、LDAPディレクトリからインポート済みのユーザー、AXL を使用して Cisco Unified Communications Manager からインポートされたユーザー、連絡先、同報リストなど）のすべての Unity Connection [エイリアス（Alias）] フィールド内の値と一致してはいけません。
- Unity Connection を LDAP ディレクトリと同期化したら、引き続き、LDAP ディレクトリと連動していない Unity Connection ユーザーを追加できます。AXL サーバーを使用して Cisco Unified Communications Manager からユーザーをインポートして、Unity Connection ユーザーの追加を継続することもできます。
- Unity Connection を LDAP ディレクトリと同期化した後は、新しい LDAP ディレクトリユーザーが自動的に Unity Connection にインポートされることはないため、手動でインポートする必要があります。
- LDAP からユーザーをインポートすると、そのユーザーは Cisco Unity Connection Administration のユーザーページで、「LDAP ディレクトリからインポートされたアクティブ ユーザー」として識別されます。
- その後、社内ディレクトリ内のユーザーデータが変更されると、LDAP ディレクトリから入力された Unity Connection フィールドは、次回にスケジュールされた再同期化の際に LDAP の新しい値で更新されます。

LDAP ユーザーのフィルタリング

さまざまな理由により、Cisco Unity Connection にインポートする LDAP ユーザーをより細かく制御したい場合があります。次に例を示します。

- LDAP ディレクトリが、ユーザ検索ベースの指定では十分に制御できないフラット構造になっている。
- LDAP ユーザーアカウントのサブセットだけを Unity Connection ユーザーにする必要がある。
- LDAP ディレクトリ構造が、Unity Connection へのユーザーのインポート方法に適さない。次に例を示します。
  - 組織ユニットが組織階層に従って設定されており、ユーザーは地理情報によって Unity Connection にマッピングされる場合、この 2 つの間にオーバーラップはほとんどありません。
  - ディレクトリ内のすべてのユーザーが 1 つのツリーまたはドメインに含まれているものの、複数の Unity Connection サーバーをインストールする必要がある場合、複数の Unity Connection サーバー上にユーザーのメールボックスが存在するのを避けるために、回避策を実行する必要があります。

このような場合は、フィルタを作成して、ユーザー検索ベースをより細かく制御することがあります。次の点に注意してください。

- 必要なだけ、いくつでも LDAP フィルタを作成できますが、1 つの Unity Connection ディレクトリ設定で最大 5 台のサーバーまたはクラスタに対してアクティブにできるフィルタは 1 つだけです。
- Unity Connection で LDAP ディレクトリ設定を作成する場合は、ユーザー検索ベースと LDAP フィルタの両方を指定します。必要に応じて、ユーザー検索ベースと連動するフィルタを作成し、作成できる最大 20 の LDAP ディレクトリ設定を指定します。
- 各フィルタは、RFC 4515『Lightweight Directory Access Protocol（LDAP）：String Representation of Search Filters』で規定された LDAP フィルタ構文に従う必要があります。
- フィルタの作成時には、フィルタ構文は検証されません。LDAP ディレクトリ設定でフィルタを指定するときに検証されます。
- フィルタを追加し、すでに LDAP ディレクトリと同期している LDAP ディレクトリ設定に追加する場合、または LDAP ディレクトリ設定ですでに使用されているフィルタを変更する場合は、新しいフィルタまたは Connection にアクセスできるように更新されたフィルタで指定された LDAP ユーザーに対して次の手順に従ってください。

  1. Cisco DirSync サービスを無効にし、再度有効にします。Cisco Unified Serviceability で **[ツール（Tools）] > [サービスの起動（Service Activation）]** の順に選択します。**[Cisco DirSync]** の横にあるチェックボックスをオフにし、**[保存（Save）]** を選択してサービスをオフにします。**[Cisco DirSync]** の横にあるチェックボックスをオンにし、**[保存（Save）]** を選択してサービスをオンにします。
  2. Unity Connection Administration で、フィルタにアクセスする LDAP ディレクトリ設定で、完全同期を実行します（**[完全同期を今すぐ実施（Perform Full Sync Now）]** を選択）。

- フィルタを変更して、前回のフィルタではアクセス可能だったユーザーの一部を除外するフィルタにする場合、現在アクセスできない LDAP ユーザーと同期されている Unity Connection ユーザーは、次にスケジュールされた 2 回の同期または 24 時間以内のいずれか長いほうの期間、スタンドアロン Unity Connection ユーザーに変換されます。このユーザーは引き続き電話を使用して Unity Connection にサインインできます。発信者はその時点でもこのユーザーにメッセージを残すことができ、そのメッセージは削除されません。ただし、Unity Connection がこのようなユーザーの同期を中断している間は、Unity Connection Web アプリケーションにはサインインできません。同期が停止されると、Web アプリケーションのパスワードが Unity Connection アカウントの作成時に割り当てられたパスワードになります。

Unity Connection マルチフォレスト LDAP 同期

マルチフォレスト LDAP インフラストラクチャを使用した Unity Connection 展開は、複数の異種フォレストを統合する単一のフォレスト ビューとして AD LDS を使用することによって、サポートできます。この統合では、LDAP フィルタリングを使用する必要があります。詳細に

ついては、
http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_configuration_example019186a0080b2b103.shtml
にある『マルチフォレスト環境での Unified Communications Manager 統合ディレクトリ統合の構成方法』を参照してください。

LDAP 認証

企業によっては、アプリケーションのシングル サインオン クレデンシャルが必要な場合があります。LDAP ディレクトリ内のユーザの資格情報に対して Unity Connection Web アプリケーションへのサインインを認証するには、LDAP 同期の項の説明に従って、LDAP ディレクトリ内のユーザーデータと Unity Connection ユーザーデータを同期する必要があります。

Unity Connection Web アプリケーション（管理者の Cisco Unity Connection Administration、エンドユーザーの Cisco Personal Communications Assistant）のパスワード、および Unity Connection ボイスメッセージへのアクセスに使用される IMAP 電子メール アプリケーションのパスワードだけは、社内ディレクトリに対して認証されます。LDAP ディレクトリの管理アプリケーションを使用して、これらのパスワードを管理します。認証が有効な場合、パスワードフィールドは Cisco Unity Connection Administration に表示されなくなります。

電話ユーザ インターフェイスまたはボイス ユーザ インターフェイスによる Unity Connection ボイス メッセージへのアクセスでは、引き続き Unity Connection データベースに対して数値パスワード（PIN）による認証が行われます。これらのパスワードは Unity Connection Administration で管理します。ユーザーは、電話インターフェイスまたは Messaging Assistant Web ツールを使用して PIN を管理します。

LDAP 認証がサポートされる LDAP ディレクトリは、同期化をサポートされる LDAP ディレクトリと同じです。https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/requirements/b_15cucsysreqs.html にある『Cisco Unity Connection のシステム要件、リリース *15*』の「LDAP ディレクトリとの統合の要件」の項を参照してください。

LDAP 認証を設定する

LDAP 認証の設定は、同期化の設定よりもずっと簡単です。次の項目を指定するだけです。

- **ユーザ検索ベース。**複数の LDAP 構成を作成した場合、認証の設定時に LDAP 構成で指定したユーザ検索ベースをすべて含むユーザ検索ベースを指定する必要があります。
- **Unity Connection が、検索ベースへのアクセスに使用する LDAP ディレクトリ内の管理者アカウント。**検索ベースのすべてのユーザーオブジェクトを「読み取る」ための最小限の権限が設定されており、また、有効期限のないパスワードが設定されている Unity Connection 専用アカウントを使用することを推奨します。（管理者アカウントのパスワードを変更すると、Unity Connection を新しいパスワードで再設定する必要があります）。管理者アカウントには完全識別名を入力します。そのため、このアカウントは LDAP ディレクトリ ツリー内の任意の場所に属することができます。
- **1 つ以上の LDAP サーバ。**Unity Connection が認証に使用する LDAP ディレクトリ サーバーは、3 つまで指定できます。Unity Connection は、指定された順序でサーバーに接続しよう

とします。どのディレクトリ サーバも応答しない場合、認証は失敗します。ホスト名ではなく IP アドレスを使用することで、ドメイン ネーム システム（DNS）の可用性への依存を解消できます。

LDAP 認証の動作

Cisco Unity Connection で LDAP 同期化および認証が設定されると、社内 LDAP ディレクトリに対するユーザーのエイリアスおよびパスワードの認証は、次のように機能します。

1. ユーザーは HTTPS 経由で Cisco Personal Communications Assistant（PCA）に接続し、エイリアス（たとえば、jsmith）とパスワードを使用して認証を試みます。
2. Unity Connection は、エイリアス jsmith のLDAP クエリを発行します。クエリのスコープについて、Unity Connection は、Cisco Unity Connection Administration で LDAP 同期を構成したときに指定した LDAP 検索ベースを使用します。SSL オプションを選択した場合は、LDAP サーバに送信される情報が暗号化されます。
3. 社内ディレクトリサーバーは、ユーザー jsmith の完全認定者名（DN）で応答します（たとえば、「cn=jsmith, ou=Users, dc=vse, dc=lab」）。
4. Unity Connection はこの完全 DN と、ユーザーが指定したパスワードを使用して、LDAP バインドを試行します。
5. LDAP バインドが成功した場合、Unity Connection はユーザーが Cisco PCA に進むことを許可します。

Unity Connection LDAP ディレクトリ構成で指定されたすべての LDAP サーバーが使用できない場合、Unity Connection Web アプリケーションの認証は失敗し、ユーザーのアプリケーションへのアクセスは許可されません。ただし、電話およびボイス ユーザー インターフェイスの認証はその時点でも機能します。これらの PIN は、Unity Connection データベースに対して認証されるためです。

Unity Connection ユーザーの LDAP ユーザーアカウントが無効または削除された場合、または LDAP ディレクトリ構成が Unity Connection システムから削除された場合、次のことが発生します。

1. 最初に、Unity Connection ユーザーが Unity Connection Web アプリケーションにサインインしようとすると、LDAP 認証は失敗します。これは、Unity Connection がまだ LDAP ディレクトリに対して認証を試みているためです。

   複数の LDAP ユーザ検索ベースにアクセスする複数の LDAP ディレクトリ構成が存在し、構成が 1 つだけ削除された場合は、それに関連付けられたユーザ検索ベース内のユーザだけが影響を受けます。他のユーザー検索ベース内のユーザーは、引き続き Unity Connection Web アプリケーションにログインできます。
2. 最初にスケジュールされた同期化で、ユーザーは Unity Connection 内で「LDAP 非アクティブ」としてマークされています。

   Unity Connection Web アプリケーションにサインインしようとすると、失敗します。

3. ユーザーが「LDAP 非アクティブ」としてマークされた後、24 時間以上経過してから実行される次回のスケジュールされた同期化では、アカウントが LDAP アカウントに関連付けられていたすべての Unity Connection ユーザーは、Unity Connection スタンドアロンユーザーに変換されます。

   各 Unity Connection ユーザーの場合、Unity Connection Web アプリケーションのパスワード、および Unity Connection ボイスメッセージへの IMAP 電子メール アクセスのパスワードは、ユーザーアカウントの作成時に Unity Connection データベースに保存されたパスワードになります。（これは通常、ユーザーの作成に使用されたユーザーテンプレートのパスワードです）。Unity Connection ユーザーはこのパスワードを知らないため、管理者がパスワードをリセットする必要があります。

   電話ユーザ インターフェイスおよびボイス ユーザ インターフェイスの数値パスワード（PIN）は、変更されないままです。

LDAP ユーザーアカウントが無効化または削除されたユーザー、または Unity Connection から削除された LDAP ディレクトリ構成を使用して同期化されていた Unity Connection ユーザーについては、次の点に注意してください。

- Unity Connection が LDAP 同期化ユーザーからスタンドアロンユーザーに変換している間は、ユーザーは引き続き電話で Unity Connection にログインできます。
- このユーザのメッセージは削除されません。
- 発信者はその時点でもこの Unity Connection ユーザーにメッセージを残すことができます。

（注） Unity Connection データと LDAP データを先に同期したときだけ、LDAP 電話番号が Unity Connection 内線番号に変換されます。それ以降のスケジュール設定された同期では、Connection の [内線番号（Extension）] フィールドの値が、LDAP 電話番号の変更によって更新されません。その結果、必要に応じて、LDAP 電話番号を変更できます。完全に異なる番号を指定することもできます。次回 Connection でデータを LDAP ディレクトリと同期するときに、内線番号は上書きされません。

認証と Microsoft Active Directory に関するその他の考慮事項

Active Directory による LDAP 認証を有効にする場合、応答時間を短縮するために、Unity Connection が Active Directory グローバルカタログサーバーに問い合わせるように設定する必要があります。グローバル カタログサーバーへのクエリを有効にするには、Unity Connection Administration でグローバルカタログサーバーの IP アドレスまたはホスト名を指定します。LDAP ポートには、LDAP サーバーと Unity Connection サーバー間で送信するデータの暗号化に SSL を使用しない場合は 3268、SSL を使用する場合は 3269 を指定します。

グローバルカタログサーバーを認証に使用すると、複数のドメインに属する Active Directory からユーザーが同期化される場合、Unity Connection が照会に従うことなく即座にユーザーを認

証できるため、さらに効率化されます。このような場合は、Unity Connection をグローバルカタログサーバにアクセスするように設定し、LDAP ユーザー検索ベースをルートドメインの最上位に設定します。

1 つの LDAP ユーザー検索ベースに複数の名前空間を含めることはできません。そのため、Active Directory フォレストに複数のツリーが存在する場合は、Unity Connection はユーザーの認証に別のメカニズムを使用する必要があります。この構成では、LDAP の userPrincipalName（UPN）属性を Unity Connection の [エイリアス（Alias）] フィールドにマッピングする必要があります。UPN 属性の値は、電子メール アドレス（username@companyname.com）に似ており、フォレスト内で一意にする必要があります。

（注） Active Directory フォレスト内に複数のツリーが存在する場合は、各ユーザの UPN サフィックス（電子メール アドレスの @ マークの後ろの部分）は、ユーザが属するツリーのルート ドメインに対応している必要があります。UPN サフィックスがツリーの名前空間と一致しない場合、Unity Connection ユーザーは Active Directory フォレスト全体に対して認証できません。ただし、別の LDAP 属性を Unity Connection の [エイリアス（Alias）] フィールドにマッピングして、LDAP 連動をフォレスト内の単一のツリーに限定できます。

たとえば、Active Directory フォレストに avvid.info と vse.lab の 2 つのツリーが存在するとします。また、各ツリーには samAccountName が jdoe であるユーザが含まれているとします。Unity Connection は、avvid.info ツリー内の jdoe に対して、次のようにログインの試行を認証します。

1. ユーザー jdoe が HTTPS 経由で Cisco Personal Communications Assistant（PCA）に接続し、UPN（jdoe@avvid.info）とパスワードを入力します。
2. Unity Connection はこの UPN を使用して、Active Directory グローバルカタログサーバーに対して LDAP クエリを実行します。LDAP 検索ベースが UPN サフィックスから判断されます。この場合、エイリアスが jdoe で、LDAP 検索ベースが「dc=avvid, dc=info」です。
3. Active Directory は、このエイリアスに対応する DN を LDAP クエリで指定されたツリー内から検索します。この例では、「cn=jdoe, ou=Users, dc=avvid, dc=info」です。
4. Active Directory がこのユーザーの完全 DN を使用して、LDAP を通じて Unity Connection に応答します。
5. Unity Connection はこの DN と、ユーザーが最初に入力したパスワードを使用して、LDAP バインドを試行します。
6. LDAP バインドが成功した場合、Unity Connection はユーザーが Cisco PCA に進むことを許可します。

LDAP 統合ユーザーと Cisco Unified CM からデータをインポートして作成されたユーザーの比較

Unity Connection を LDAP ディレクトリと統合する代わりに、https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/administration/guide/b_15cucsag/b_15cucsag_chapter_011.html に

ある『*Cisco Unity Connection* のシステム アドミニストレーション ガイド、リリース *15*』の「ユーザー」の章の「AXL を介してユーザーをインポートする」の項で説明されているように、Cisco Unified Communications Manager からデータをインポートしてユーザーを作成することもできます。

次の点に注意してください。

- Cisco Unified CM からユーザーをインポートした場合、および Cisco Unified CM が LDAP ディレクトリと統合されている場合、Unity Connection では自動的に LDAP の同期化または認証へのアクセスが許可されることはありません。Unity Connection ユーザーが LDAP ディレクトリに対して認証されるようにするには、Unity Connection を LDAP ディレクトリと統合する必要もあります。
- Cisco Unified CM からユーザーをインポートする場合は、Cisco Unified CM データへの更新が自動的に Unity Connection サーバーに複製されることはないため、Cisco Unity Connection Administration の [ユーザーを同期（Synch Users）] ページを使用して、随時 Unity Connection ユーザーデータを Cisco Unified CM ユーザーデータと手動で同期する必要があります。Unity Connection を LDAP ディレクトリと統合する場合は、Unity Connection データベース内のデータが LDAP ディレクトリ内のデータと自動的に再同期される日時を指定する、同期スケジュールを定義できます。

LDAP ディレクトリにユーザを追加する場合は、Unity Connection に手動でインポートする必要があることに注意してください。自動同期で Unity Connection データベースが更新されるのは既存のユーザーの新しいデータの場合だけで、新しいユーザーの新しいデータの場合は更新されません。

- Unity Connection を LDAP ディレクトリと統合する場合は、LDAP データベースで Web アプリケーションのパスワードを認証するよう、Unity Connection を設定することができます。Cisco Unified CM からデータをインポートする場合は、Unity Connection で Unity Connection Web アプリケーションのパスワードを維持し、Cisco Unified CM で Cisco Unified CM で Web アプリケーションのパスワードを維持する必要があります。

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。