ユーザ管理

Jabber ID

Cisco Jabber は Jabber ID を使用して、連絡先ソース内の連絡先情報を識別します。

デフォルトの Jabber ID は、ユーザ ID とプレゼンス ドメインを使用して作成されます。

たとえば、Adam McKenzie が `amckenzie` というユーザ ID を持っており、そのドメインが `example.com` である場合、Jabber ID は `amckenzie@example.com` となります。

次の文字は、Cisco Jabber ユーザ ID または電子メール アドレスでサポートされます。

- 大文字 (A から Z)
- 小文字 (a から z)
- 数字（0 ～ 9）
- ピリオド（.）
- ハイフン（-）
- アンダースコア（_）
- チルダ（~）
- Hashtag (#)

連絡先リストに入力する場合、クライアントは Jabber ID を使用して連絡先ソースを検索し、連絡先を解決して、名、姓、その他の連絡先情報を表示します。

IM アドレス スキーム

Cisco Jabber 10.6 以降は、example-us.com や example-uk.com のユーザのようにドメインが同じプレゼンス アーキテクチャ上に存在する場合は、オンプレミス展開用の複数のプレゼンス ドメイン アーキテクチャ モデルをサポートします。Cisco Jabber は Cisco Unified Communications Manager IM and Presence 10.x 以降を使用して柔軟な IM アドレス スキームをサポートします。IM アドレス スキームは Cisco Jabber ユーザを識別する Jabber ID です。

マルチ ドメイン モデルをサポートするには、展開のすべてのコンポーネントに次のバージョンが必要です。

- Cisco Unified Communications IM and Presence サーバ ノードとコール制御ノード バージョン 10.x 以降。
- Windows、Mac、IOS、および Android のバージョン 10.6 以降で実行中のすべてのクライアント。

次のシナリオでは、複数のドメイン アーキテクチャを使用している Cisco Jabber を展開するだけです。

- Cisco Jabber 10.6 以降は、すべてのプラットフォーム（Windows、Mac、IOS、および Android（DX シリーズなどの Android ベースの IP 電話を含む））上の組織内のすべてのユーザに対する新しいインストールとして展開されます。
- プレゼンス サーバ上でドメインまたは IM アドレスを変更する前に、Cisco Jabber がすべてのプラットフォーム（Windows、Mac、IOS、および Android（DX シリーズなどの Android ベースの IP 電話を含む））上のすべてのユーザに対してバージョン 10.6 以降にアップグレードされます。

詳細プレゼンス設定で使用可能な IM アドレス スキームは次のとおりです。

- UserID@[Default Domain]
- Directory URI

UserID@[Default Domain]

User ID フィールドは LDAP フィールドにマップされます。これがデフォルトの IM アドレス スキームです。

たとえば、ユーザの Anita Perez は、アカウント名が aperez で、User ID フィールドが sAMAccountName LDAP フィールドにマップされます。使用されるアドレス スキームは aperez@example.com です。

Directory URI

ディレクトリ URI は、**mail** または **msRTCSIP-primaryuseraddress** LDAP フィールドにマップされます。このオプションは、認証用のユーザ ID に依存しないスキームを提供します。

たとえば、ユーザの Anita Perez は、アカウント名が aperez で、mail フィールドが Anita.Perez@domain.com で、使用されるアドレス スキームが Anita.Perez@domain.com です。

Jabber ID によるサービス ディスカバリ

サービス ディスカバリは、`[userid]@[domain.com]` の形式で入力された Jabber ID を取得し、デフォルトでは、Jabber ID の `domain.com` 部分を取り出して使用可能なサービスを検出します。プレゼンス ドメインがサービス ディスカバリ ドメインと同じではない展開の場合は、次のようにして、インストール時にサービス ディスカバリ ドメイン情報を含めることができます。

- Windows 版 Cisco Jabber では、`SERVICES_DOMAIN` コマンドライン引数を使用してこれを行います。
- Mac 版 Cisco Jabber、Android 版 Cisco Jabber、iPhone および iPad 版 Cisco Jabber では、URL 設定で使用される `ServicesDomain` パラメータを使用してサービス ディスカバリ ドメインを設定できます。

.

SIP URI

SIP URI は各ユーザに関連付けられます。SIP URI には、電子メール アドレス、IMAddress、または UPN を使用できます。

SIP URI は、Cisco Unified Communications Manager の [ディレクトリ URI（Directory URI）] フィールドを使用して設定されます。使用可能なオプションは次のとおりです。

- メール アドレス
- msRTCSIP-primaryuseraddress

ユーザは、SIP URI を入力して、連絡先を検索したり連絡先に電話をかけることができます。

LDAP ユーザ ID

ディレクトリ ソースから Cisco Unified Communications Manager にユーザを同期させる場合は、ディレクトリ内の属性からユーザ ID を入力できます。ユーザ ID を保持するデフォルトの属性は、`sAMAccountName` です。

フェデレーション用ユーザ ID の計画

フェデレーションでは、連絡先の検索中に連絡先を解決するため、Cisco Jabber はそれぞれの連絡先に対して連絡先 ID またはユーザ ID を必要とします。

ユーザ ID の属性を SipUri パラメータに設定します。デフォルト値は `msRTCSIP-PrimaryUserAddress` です。ユーザ ID から削除するプレフィックスがある場合は、UriPrefix パラメータ内の値を設定することができます。*Cisco Jabber* パラメータリファレンスガイドの最新バージョンを参照してください。

ユーザの連絡先写真のプロキシ アドレス

Cisco Jabber は写真サーバにアクセスして、連絡先の写真を取得します。ネットワーク設定に Web プロキシが含まれている場合は、Cisco Jabber が写真サーバにアクセスできることを確認する必要があります。

認証および承認

Cisco Unified Communications Manager の LDAP 認証

ディレクトリ サーバを使用して認証するには、Cisco Unified Communications Manager に LDAP 認証を設定します。

ユーザがクライアントにサインインすると、プレゼンス サーバがその認証を Cisco Unified Communications Manager にルーティングします。次に、Cisco Unified Communications Manager がその認証をディレクトリ サーバにプロキシします。

Cisco Webex Messenger ログイン認証

Cisco Webex 管理ツールを使用してCisco Webex Messenger 認証が設定されます。

ユーザがクライアントにサインインすると、その情報が Cisco Webex Messenger に送信され、認証トークンがクライアントに返送されます。

シングル サインオン認証

シングル サインオン認証は、アイデンティティ プロバイダー（IdP）とサービスを使用して設定されます。

ユーザがクライアントにサインインすると、その情報が IdP に送信され、クレデンシャルが承認されると、認証トークンが Cisco Jabber に返送されます。

iPhone および iPad 版 Cisco Jabber 向けの証明書ベースの認証

Cisco Jabber は、クライアント証明書により IdP サーバで認証されます。この証明書認証により、ユーザ クレデンシャルを入力せずにサーバにサインインできます。クライアントは Safari フレームワークを使用してこの機能を実装します。

要件

- Cisco Unified Communications Manager 11.5、IM and Presence Service 11.5、Cisco Unity Connection 11.5 以降。
- Expressway for Mobile and Remote Access サーバ 8.9 以降。
- ユニファイド コミュニケーション インフラストラクチャに対し SSO が有効。
- Cisco Unified Communications Manager、IM およびプレゼンス サービス、Cisco Unity Connection、IdP サーバを含むすべてのサーバ証明書が CA による署名を持つ。iOS デバイスが OS の信頼認証局を使用する場合、Cisco Jabber アプリをインストールする前に CA 証明書をインストールします。
- Cisco Unified Communications Manager で SSO のネイティブ ブラウザ（Safari に付属）を設定します。詳細については、*Cisco Jabber*向けオンプレミス展開における証明書ベースの SSO 認証セクションを参照してください。
- Expressway for Mobile and Remote Access サーバで SSO のネイティブ ブラウザ（Safari に付属）を設定します。詳細については、https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-guides-list.htmlのCisco Expressway インストールガイドを参照してください。

Cisco 証明書は、EMM ソリューションを用いて iOS デバイスに展開できます。

推奨—Ciscoは、iOS デバイスへの証明書の展開に EMM ソリューションの使用をお勧めします。

Android 版 Cisco Jabber の証明書ベースの認証

Cisco Jabber は、シングル サインオン サーバへのサインインにクライアント証明書を使用します（Webex メッセンジャー とオンプレミス）。

要件

- Android OS 5.0 以降
- シングル サインオンが有効
- Jabber クライアントは、モバイルおよび Remote Access（MRA）と非 MRA 導入モードでサポートされています。
- Jabber は、Android 7.0 以降では無効な証明書に関する通知を常に表示します。Android OS には、カスタム CA 署名付き証明書がインストールされている場合もあります。Android 7.0 を対象とするアプリは、システムによって提供された証明書だけを信頼し、ユーザが追加した認証局を信頼しません。

証明書の導入

Android デバイスでの証明書の展開には EMM ソリューションの使用をお勧めします。

ボイスメール認証

ユーザは Cisco Unity Connection に存在している必要があります。Cisco Unity Connection は、複数の認証タイプをサポートします。Cisco Unified Communications Manager と Cisco Unity Connection が同じ認証を使用している場合、Cisco Jabber は同じクレデンシャルを使用するように設定することをお勧めします。

OAuth

Cisco Jabber が OAuth プロトコルを使用して、サービスに対するユーザのアクセス権を承認するように、Cisco Jabber を設定することができます。ユーザが OAuth 対応環境にサインインする場合、サインインのたびにクレデンシャルを入力する必要がありません。ただし、サーバが OAuth に対応していない場合は、Jabber が適切に機能しないことがあります。

Cisco ユニファイドコミュニケーションマネージャー 12.5 以降を使用している場合は、SIP OAuth を有効にすることもできます。この機能を使用すると、Jabber が SIP に対して承認され、Jabber が TLS を介して SIP サービスに接続できるようになります。また、Jabber はセキュア接続 (sRTP) 経由でメディアを送信できます。SIP OAuth は、セキュリティで保護された SIP およびメディアを有効にするには CAPF 登録が不要であることを意味します。

前提条件：

- 機能するように導入している場合は、OAuth 更新トークンをこれらのすべてのコンポーネントでオンにする必要があります。
- Cisco Unified Communication Manager、Cisco Unified Communication Manager Instant Messaging and Presence、および Cisco Unity Connection のバージョン 11.5(SU3) または 12.0
- Cisco Expressway for Mobile and Remote Access バージョン X8.10 以降
- SIP OAuth向け: Cisco Unified Communication Manager 12.5 以降、Mobile and Remote Access version X12.5 以降向けのCisco Expressway。

OAuth の設定前に、使用する展開の種類を確認します。

- ローカル認証を展開する場合、IdP サーバは不要です。Cisco Unified Communication Manager が認証を行います。
- SSO を設定して、または設定せずに OAuth を設定することができます。SSO を使用している場合は、すべてのサービスで有効になっていることを確認します。If you have an SSO-enabled deployment, then deploy an IdP server, and IdP server is responsible for authentication.

次のサービス上で OAuth を有効にすることができます。

- Cisco Unified Communications Manager
- Cisco Expressway

- Cisco Unity Connection

デフォルトでは、OAuthはこれらのサーバ上で無効です。これらのサーバでOAuthを有効にするには、次の操作を実行します。

- Cisco Unified Communications Manager と Cisco Unity Connection サーバの場合、**[エンタープライズパラメータ設定（Enterprise Parameter configuration）] > [更新ログインフローを使用したOAuth（OAuth with refresh Login Flow）]** に移動します。
- Cisco Expressway-C の場合、**[設定ユニファイドコミュニケーション（Configuration Unified Communication）] > [更新のOAuthトークンで認証する設定（Configuration Authorized by OAuth token with refresh）]** を移動します。

上記のサーバのOAuthの有効と無効を切り替えると、Jabberは設定の再取得間隔でこの切り替えを識別するため、ユーザは Jabber のサインアウトとサインインできます。

サインアウト中、Jabberはキャッシュ内に保存されているユーザクレデンシャルを削除して通常のサインフローでサインインします。この場合、Jabberは最初にすべての設定情報を取得するため、ユーザは Jabber サービスにアクセスできます。

Cisco Unified Communication Manager で OAuth を設定するには、次の操作を実行します。

1. **[Cisco Unified Communication Managerの管理（Cisco Unified Communication Manager Admin）] > [システム（System）] > [エンタープライズパラメータ（Enterprise Parameters）] > [SSO設定（SSO Configuration）]** に移動します。
2. [O-Authアクセストークン期限タイマー（分）（O-Auth Access Token Expiry Timer(minutes)）] を任意の値に設定します。
3. [O-Auth更新トークン期限タイマー（日）（O-Auth Refresh Token Expiry Timer(days)）] を任意の値に設定します。
4. [保存（Save）] ボタンをクリックします。

Cisco Expressway で OAuth を設定するには、次の操作を実行します。

1. **[設定（Configuration）] > [Unified Communications] > [設定（Configuration）] > [MRAアクセスコントロール（MRA Access Control）]** に移動します。
2. [O-Authローカル認証（O-Auth local authentication）] を [オン（On）] に設定します。

Cisco Unity で OAuth を設定するには、次の操作を実行します。

1. **[AuthZサーバ（AuthZ Servers）]** に移動して **[新規追加（Add New）]** を選択します。
2. すべてのフィールドに詳細を入力して、**[証明書エラーを無視する（Ignore Certificate Errors）]** を選択します。
3. [保存（Save）] をクリックします。

制限事項

Jabber が自動侵入防御をトリガーする

状況：

- モバイルおよび Remote Access の展開用の開発者向けの管理者が、OAuth トークン (更新トークンの有無による) に応じた承認用に設定されています。
- Jabber ユーザのアクセス トークンの有効期限が切れています

Jabber は次のいずれかを行います。

- デスクトップの休止状態からの再開
- ネットワーク接続の回復
- 数時間サインアウトした後、高速サインインの試行

動作：

- いくつかの Jabber モジュールが、期限切れのアクセス トークンを使用して Expressway-E で認証を試行します。
- Expressway-E がこれらの要求を（正しく）拒否します。
- 特定の Jabber クライアントからの要求が 6 つ以上ある場合、Expressway-E はその IP アドレスを（デフォルトで）10 分間ブロックします。

症状：

影響を受ける Jabber クライアントの IP アドレスは、HTTP プロキシの認証の失敗カテゴリにある Expressway-E のブロックされたアドレス リストに追加されます。このアドレスは、**システム** > **保護** > **自動検出** > **ブロックされたアドレス** で確認できます。。

回避策：

この問題を回避するには2つの方法があります。つまり、その特定のカテゴリの検出しきい値を上げるか、または影響を受けるクライアントに対して免除を作成できます。免除は実際の環境では実用的でない可能性があるため、ここではしきい値オプションについて説明します。

1. **[システム（System）] > [保護（Protection）] > [自動検出（Automated detection）] > [設定（Configuration）]** に移動します。
2. [HTTPプロキシの認証の失敗（HTTP proxy authorization failure）] をクリックします。
3. [トリガーレベル（Trigger level）] を 5 ～ 10 に変更します。期限が切れたトークンを提示する Jabber モジュールを容認するには 10 で十分です。
4. 設定を保存すると、すぐに有効になります。
5. 影響を受けるクライアントのブロックを解除します。

複数リソースのログイン

ユーザがシステムにログインすると、すべてのCisco Jabberクライアントが次のいずれかのIM and Presence サービス ノードに一括で登録されます。このノードは、IM and Presence サービス環境のアベイラビリティ、連絡先リスト、およびその他の側面を追跡します。

- オンプレミス展開：Cisco Unified Communications Manager IM and Presence Service。
- クラウド展開: Cisco Webex

この IM and Presence サービス ノードは、次の順序で一意のネットワーク ユーザに関連付けられた登録済みクライアントのすべてを追跡します。

1. 2人のユーザ間で新しいIMセッションが開始されると、最初の着信メッセージが受信ユーザのすべての登録済みクライアントにブロードキャストされます。
2. その後で、IM and Presence サービス ノードが登録済みクライアントのいずれかからの最初の応答を待機します。
3. 最初に応答したクライアントは、ユーザが別の登録済みクライアントを使用して返信を開始するまで、着信メッセージの残りを受け取ります。
4. その後で、ノードが以降のメッセージをこの新しいクライアントに再ルーティングします。

（注） ユーザが複数のデバイスにログインするときにアクティブなリソースがない場合は、最も高い優先順位を持つクライアントが最優先されます。プレゼンスの優先順位がすべてのデバイスで同じ場合は、最後にユーザがログインしたクライアントが最優先されます。