ID の管理

ユーザセキュリティの概要

ユーザ アクセス

ユーザセキュリティは、ユーザ、エンドポイント、およびオンラインアクティビティを保護して、より効率的にリスクを関連付けるプラットフォームで構成されています。ユーザがパーソナルデバイスを介してネットワークにログインする傾向がある中で、パーソナルデバイスのセキュリティ保護は、会社が所有するデバイスのセキュリティ保護と同様に重要です。

ユーザとセキュリティの詳細については、『Cisco Unified Communications Manager システム設定ガイド』の**「エンドユーザの設定」**と『Cisco Unified Communications Manager アドミニストレーション ガイド』の**「セキュリティの管理」**を参照してください。

Unified Communications Manager でユーザアクセスを管理するロールに関連付けられているアクセス制御グループにエンドユーザを割り当てます。

アクセス制御は、基本的に、適切なユーザがネットワークにアクセスできるようにすると同時に不適切なユーザをブロックすることができます。アクセス制御は、ネットワークにアクセスしているユーザとデバイスを把握する機能です。これにより、適切なユーザが適切なデバイスを使用して、適切なリソースにアクセスできます。アクセス制御は情報の拡散を制限し、望ましくない訪問者がデータにアクセスするのを防ぎます。

ロールとアクセス制御グループは、Unified Communications Manager に対して複数のレベルのセキュリティを提供します。各ロールは、Unified Communications Manager 内の特定のリソースに対する一連の権限を定義します。ロールをエンドユーザに割り当てて、エンドユーザをアクセス制御グループに割り当てると、エンドユーザーはそのロールによって定義されたアクセス許可を取得します。

インストールの際、Unified Communications Manager は定義済みのデフォルトアクセス制御グループに割り当てられた定義済みのデフォルトロールを備えています。エンドユーザをデフォ

ルトのアクセス制御グループに割り当てることも、新しいアクセス制御グループとロールを設定してアクセス設定をカスタマイズすることもできます。

ユーザとアクセス制御の詳細については、『Cisco Unified Communications Manager システム設定ガイド』の「**エンドユーザの設定**」と『Cisco Unified Communications Manager アドミニストレーション ガイド』の「**ユーザの管理**」を参照してください。

ID の管理

定義された一連の Cisco アプリケーションのうちの 1 つにサインインした後は、SAML シングル サインオン（SSO）を使用して、それらすべてのアプリケーションにアクセスできます。SAML では、信頼できるビジネスパートナー間で、セキュリティに関連した情報交換を記述します。これは、ユーザを認証するために、サービスプロバイダー（Cisco Unified Communications Manager など）が使用する認証プロトコルです。SAML を使用して、アイデンティティプロバイダーとサービスプロバイダーがセキュリティ認証情報を交換します。この機能が安全なメカニズムを提供していることで、さまざまなアプリケーションにわたり、共通のログイン情報や関連情報を使用します。アイデンティティ管理の詳細については、Cisco Unified Communications Manager アドミニストレーション ガイドの「SAML シングルサインオンの管理」を参照してください。

連絡先検索認証

連絡先検索認証では、他のユーザをディレクトリで検索する前に、ユーザ自身を認証する必要があります。連絡先検索認証の詳細については、次のトピックを参照してください。

1. 連絡先検索の認証の電話サポートの確認
2. 連絡先検索の認証の有効化
3. 連絡先検索用のセキュアなディレクトリ サーバの設定

アイデンティティ管理の概要

アイデンティティ管理は、シスココラボレーション導入に必須のコンポーネントです。アイデンティティは多くの場合、ハッカーの主なターゲットとなるため、システムを保護するには、セキュア認証および許可サービスを設定する必要があります。Cisco Unified Communications Manager には、サービスのアイデンティティ、認証、および許可を管理するための複数のオプションがあります。

- サードパーティ アイデンティティ プロバイダーによる SAML SSO の導入
- LDAP 認証
- ローカル DB 認証

SAML SSO の展開

SAML SSO により、企業のセキュリティが向上すると同時に、生産性が向上します。SAML 2.0 プロトコルを使用して、SAML SSO はシスコ コラボレーション インフラストラクチャをサードパーティ アイデンティティ プロバイダーに接続し、ドメイン全体や製品全体にわたって管理者およびクライアントのログイン用のセキュアなログインおよび認証サービスを提供します。アイデンティティ プロバイダーが単一のログインを保存しているため、ワーカーの生産性が向上します。Collaboration アプリケーションの 1 つに正常にログインしたら、再度ログインする必要なしにこれらのアプリケーションにアクセスできます。

SAML SSO は、アイデンティティ フレームワークに次の利点があります。

- 異なるユーザ名およびパスワードの組み合わせを入力する必要がなくなり、パスワードによる疲労が軽減されます。
- アプリケーションをホストしている自社システムからサードパーティのシステムに、認証を転送できます。
- 認証情報を保護して、安全性が向上します。SAML SSO は、暗号化機能により、IdP、サービスプロバイダー、およびユーザ間で転送される認証情報を保護します。SAML SSO では、IdP とサービス プロバイダー間で転送される認証メッセージを外部ユーザから保護することもできます。
- 同じアイデンティティのログイン情報を再入力する時間が省けるため、生産性が向上します。
- パスワードをリセットするためのヘルプデスクへの問い合わせが減るため、コスト削減につながります。

IdP との信頼関係

SAML SSO の導入は、サービスプロバイダー（Cisco Unified Communications Manager）とサードパーティのアイデンティティ プロバイダー間の信頼関係の作成に依存しています。次の 2 つの SSO モードのいずれかを使用して、SAML SSO の関係を設定できます。

- ノード単位の契約：UC メタデータ zip ファイルには、ノードごとに別々の XML ファイルが含まれています。
- クラスタごとの契約：クラスタ用の単一のメタデータファイル

この信頼関係は、最初のメタデータファイルの交換によって作成されます。Cisco UC メタデータファイルは、次の情報を含む XML ファイルです。

- 一意の識別子
- Organization
- この情報の有効期限
- キャッシング期間
- この情報の XML 署名

- 担当者
- エンティティの一意の識別子（エンティティ ID）
- この SAML インスタンスの SAML ロールの説明（アイデンティティ プロバイダー、サービス プロバイダーなど）

許可

IdP によって認証されると、Cisco Unified Communications Manager リソースへのユーザアクセスは、ローカルに設定されているアクセス制御グループと、それらのグループが提供するロールの権限によって決定されます。

SAML SSO の設定とアイデンティティ プロバイダーの要件

アイデンティティ プロバイダーの設定情報や要件など、SAML SSO の詳細については、『*SAML SSO Deployment Guide for Cisco Unified Communications Applications*』を参照してください。

LDAP 認証

SAML SSO を導入しなかった場合に、ユーザを会社の LDAP ディレクトリと同期している場合、LDAP 認証により、会社の LDAP ディレクトリに保存されているログイン情報に対してユーザパスワードを認証できます。このオプションにより、Cisco Unified Communications Manager のアイデンティティ管理システム（IMS）ライブラリは、LDAP が同期されたユーザのユーザパスワードを認証するために、会社の LDAP ディレクトリを使用できます。

エンドユーザは、セルフケアポータルにログインするときに、会社の LDAP ディレクトリで設定されている会社パスワード（AD パスワードなど）を入力します。

このオプションが設定されている場合、

- LDAP からインポートされたユーザのエンド ユーザ パスワードは、シンプル バインド操作によって社内ディレクトリに対して認証される。
- ローカルユーザのエンドユーザパスワードは、Unified CM データベースに対して認証される。
- アプリケーション ユーザ パスワードは、Unified CM データベースに対して認証される。
- エンドユーザ PIN は、Unified CM データベースに対して認証される。

LDAP 認証の設定

エンドユーザパスワードの LDAP 認証を有効にするには、次の手順を使用します。既存の LDAP ディレクトリ同期に LDAP 認証を追加できます。

始める前に

この手順では、LDAP ディレクトリ同期がすでに設定されていることを前提としています。LDAP ディレクトリ同期をまだ設定していない場合は、『System Configuration Guide for Cisco Unified Communications Manager』を参照して同期を設定してください。

ステップ 1 Cisco Unified CMの管理で、**システム** > **LDAP** > **LDAP検索** を選択します。

ステップ 2 [エンドユーザに LDAP 認証を使用する（Use LDAP Authentication for End Users）] チェックボックスをオンにします。

ステップ 3 [LDAP マネージャの識別名（LDAP Manager Distinguished Name）] として、該当する LDAP ディレクトリへのアクセス権を持つ管理ユーザである LDAP Manager の ユーザ ID を入力します。

ステップ 4 [パスワード（Password）] と [パスワードの確認（Confirm the Password）] にパスワードを入力します。

ステップ 5 LDAP ディレクトリサーバのアドレス情報を入力します。

ステップ 6 [LDAP 認証の設定（LDAP Authentication Configuration）] ウィンドウで、残りのフィールドに入力します。

ステップ 7 [保存（Save）] をクリックします。

ローカルデータベース認証

サードパーティ アイデンティティ プロバイダーを使用して SAML SSO を導入しない場合、またはLDAP認証が設定されていない場合は、エンドユーザに対してCisco Unified Communications Manager データベースに対するローカル認証が必要です。このオプションでは、ユーザパスワードがローカルデータベースに保存され、エンドユーザ設定によって管理されます。

アプリケーションユーザとエンドユーザのPINの両方について、ローカルデータベース認証は常に認証の管理に使用されます。次の表に、3 つの主なパスワードタイプと、その管理方法を示します。

表 1:

パスワードタイプ	クレデンシャル管理
エンド ユーザ パスワード	SAML SSO または LDAP 認証を使用しない場合は、エンドユーザパスワードは個々のエンドユーザの [エンドユーザ設定（End User Configuration）] ウィンドウでローカルに管理されます。 すべてのパスワードは、エンドユーザ設定から更新できます。エンドユーザは、セルフケアポータルで自分のパスワードを編集できます。
エンド ユーザ PIN	SAML SSO や LDAP 認証の導入にかかわらず、エンドユーザの PIN は、Cisco Unified CM Administration の [エンドユーザ設定（End User Configuration）] ウィンドウで常に管理されます)。 管理者は、[エンドユーザ設定（End User Configuration）] ウィンドウで既存のエンドユーザの PIN を編集できます。

パスワードタイプ	クレデンシャル管理
アプリケーションユーザ パスワード	SAML SSO や LDAP 認証の導入に関係なく、アプリケーション ユーザ パスワードはローカル データベースに保存され、Cisco Unified CM Administration の [アプリケーション ユーザ設定（Application User Configuration）] ウィンドウで管理されます。

（注） すべてのローカルパスワードと PIN は、暗号化された形式でデータベースに保存されます。

OAuth フレームワーク

OAuth 認証フレームワークは、IETF の RFC 6749 で定義されています。OAuth 2.0 認証プロトコルでは、リソース所有者（Cisco Unified Communications Manager など）は、サードパーティ製アプリケーションがHTTPサービスへの制限されたアクセスを取得するのを許可することができます。Cisco Unified Communications Manager を使用すると、OAuth フレームワークはアクセストークンを使用してアクセスを許可し、トークンを更新してトークンの有効期限を越えてリソースにアクセスできるようにすることができます。OAuthを使用すると、ユーザが情報にアクセスしようとするときに Web サイトでパスワードの入力を求める必要がなくなります。OAuthを使用すると、クライアントがサーバー上のリソースにアクセスするのをユーザー自身が許可します。

Cisco Jabber クライアントは、OAuth 更新ログインを使用して Cisco Unified Communications Manager からリソースにアクセスします。最初のログイン後に、OAuth アクセストークンと更新トークンは、トークンの有効期限を越えて、リソースへのシームレスなアクセスを提供します。

OAuth 更新ログイン

OAuth 更新ログインを使用すると、短い有効期限のアクセストークンによって Jabber を認証し、トークンの有効期限が有効である間、アクセスを許可します（アクセストークンのデフォルトの有効期限は 60 分です)。期間の長い更新トークンは、古いアクセストークンが期限切れになったときに、Jabberに新しいアクセストークンを提供します。更新トークンが有効である限り（デフォルトの有効期間は 60 日）、Jabber クライアントは新しいアクセストークンを動的に取得できます。これにより、ユーザは再認証する必要なしにシームレスにアクセスできます。

OAuth トークンが有効期間の 75% に達するたびに、エンドユーザー アプリケーションは新しいアクセストークンを要求し、CUCMはエンドユーザーを承認する新しいアクセストークンを提供します。更新トークンが存続期間の 100% に達した場合は、新しいアクセストークンを生成する前に、再認証する必要があります。

重要 この機能は、リリース 15 以降の Webex クライアントにのみ適用されます。

Webex クライアントがアクセストークンの更新を要求するたびに、Cisco Unified Communications Manager は、更新トークンの更新機能が Cisco Unified CM および Webex クライアントで有効になっているかどうか、および更新トークンの有効期間が有効期限の 50% に達しているかどうかを確認します。両方の条件が満たされると、アクセストークンの更新プロセス中に更新トークンが自動的に更新され、再認証を必要としないシームレスなアクセスが保証されます。

SIP OAuth モード

SIP OAuth モードは、OAuth フレームワークを強化し、SIP 回線の OAuth アクセス トークンと更新トークンの使用を可能にすることで、Jabber クライアントに LSC 証明書をインストールする必要がなくなります。SIP OAuth モードにより、CAPF なしで Jabber のセキュアな署名とメディアが可能になります。SIP 登録中にトークンの検証が完了します。このモードでは、Jabber は LSC なしで、また、統一された CM で混合モードを有効にする必要なしに、メディアおよびシグナリングの暗号化を実行できます。

OAuth のキーの再生成

署名と OAuth トークンの暗号化に使用されるキーが侵害されたと思われる場合は、次の CLI コマンドを使用して新しいキーを生成します。署名キーは非対称で RSA ベースであるのに対し、暗号キーは対称キーです。

- `set key regen authz encryption`
- `set key regen authz 署名`

（注） OAuth キーが再生成されたら、Jabber OAuth ログインを機能させるために、すべての IM and Presence ノードで Cisco XCP 認証サービスを再起動する必要があります。

SIP OAuth モードの設定

SIP 回線の OAuth 更新ログインを使用できるよう SIP OAuth モードを設定する方法の詳細については、『*Feature Configuration Guide for Cisco Unified Communications Manager*』の「*SIP OAuth* モード」の章を参照してください。

既存の OAuth 更新トークンの取り消し

既存の OAuth 更新トークンを取り消すには、AXL API を使用します。たとえば、ある従業員が退社した場合、この API を使用してその従業員の現在の更新トークンを取り消し、その従業員が新しいアクセストークンを取得したり、企業アカウントへログインできないようにすることができます。API は、AXL クレデンシャルで保護されている REST ベースの API です。任意のコマンドライン ツールを使用して API を呼び出すことができます。次のコマンドは、更新トークンを取り消すために使用できる cURL コマンドの例を示しています。

```
curl -k -u "admin:password" https://<UCMaddress:8443/ssosp/token/revoke?user_id=<end_user>
```

引数の説明

- `admin:password` は、Cisco Unified Communications Manager の管理者アカウントのログイン ID とパスワードです。
- `UCMaddress` は、Cisco Unified Communications Manger のパブリッシャ ノードの FQDN または IP アドレスです。
- `end_user` は、更新トークンを取り消すユーザのユーザ ID です。

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。