アイデンティティ管理

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、脅威をより効率的に関連付けるために、ユーザ、エンドポイント、およびユーザのオンライン活動を保護するプラットフォームで構成されています。個人用デバイスからネットワークにログインするユーザが増加しているため、会社所有のデバイスと同様に個人用デバイスの保護も重要です。

ユーザー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**「エンドユーザーの設定」**と、『『Administration Guide for Cisco Unified Communications Manager』』の**「セキュリティの管理」**を参照してください。

エンドユーザを [ロール] に関連付けられたアクセス コントロール グループに割り当て、ユーザ アクセスを管理します Unified Communications Manager。

アクセスコントロールは、適切なユーザによるネットワークへのアクセスを許可する一方で、同時にアクセスしてはならないユーザをブロックします。アクセスコントロールとは、ネットワークにアクセスしている誰と何を可視化する機能のことです。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るようになります。アクセスコントロールは、情報の広がりを規制し、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 コントロール グループは、複数のレベルのセキュリティを Unified Communications Manager に提供します。 各ロールは、Unified Communications Manager 内の特定のリソースに対する権限のセットを定義します。 エンドユーザーをアクセス コントロール グループに指定した後、ロールを割り当てると、エンドユーザーはロールによって定義されたアクセス許可を取得します。

インストール時に、 Unified Communications Manager には定義済みのデフォルトの役割が事前に定義されたアクセスコントロールグループに割り当てられます。エンドユーザをデフォルト

のアクセスコントロールグループに指定したり、新しいアクセスコントロールグループとロールをセットアップしてアクセス設定をカスタマイズすることができます。

ユーザーおよびアクセス制御の詳細は、『Cisco Unified Communications Manager システム設定ガイド』の **「エンドユーザーの設定」** および『『Administration Guide for Cisco Unified Communications Manager』』の **「ユーザーの管理」** を参照してください。

アイデンティティ管理

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 は信頼できるビジネスパートナー間のセキュリティ関連情報の交換について記述します。 これは、サービス プロバイダー (Cisco Unified Communications Manager など) がユーザを認証するために使用する認証プロトコルです。 SAML では ID プロバイダとサービスプロバイダがセキュリティ認証情報を交換します。 この機能は、さまざまなアプリケーションで共通の資格情報と関連情報を使用するための安全なメカニズムを提供します。 ID 管理の詳細については、「SAML シングルサインオンを管理する 『Administration Guide for Cisco Unified Communications Manager』」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、他のユーザのディレクトリを検索する前に、自分自身を認証する必要があります。 連絡先検索の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. 連絡先検索認証のため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

ID 管理の概要

Identity Management は Cisco Collaboration の展開に不可欠なコンポーネントです。 アイデンティティはしばしばハッカーの主な標的であるため、システムを安全にするために安全な認証および許可サービスを設定することが不可欠です。 Cisco Unified Communications Manager は、サービスの ID、認証、認可を管理するための多くのオプションを提供します。

- サードパーティ ID プロバイダによる SAML SSO 展開
- LDAP 認証
- ローカル DB 認証

SAML SSO の展開

SAML SSO は生産性を向上させると同時に、エンタープライズのセキュリティを向上させます。 SAML SSO は、SAML 2.0 プロトコルを使用して、Cisco Collaboration インフラストラク

チャをサードパーティの ID プロバイダに接続し、異なるドメインや製品の管理者とクライアントのログインに安全なログインと認証サービスを提供します。 ID プロバイダがシングル ログインを保存するため、Worker の生産性が向上します。一度コラボレーション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く、それらのアプリケーションにアクセスできます。

SAML SSO は ID フレームワークに以下の利点を提供します。

- 異なるユーザ名とパスワードの組み合わせを入力する必要性を排除することで、パスワードの手間を軽減します。
- アプリケーションをホストするシステムの認証をサードパーティのシステムに転送します。
- 認証情報を保護および保護します。 SAML SSO は暗号化機能を提供し、IdP、サービスプロバイダー、ユーザ間で受け渡される認証情報を保護します。 SAML SSO は、IdP とサービスプロバイダーの間で受け渡される認証メッセージを外部ユーザから隠すこともできます。
- 同じ ID の資格情報を再入力する時間が短縮されるため、生産性が向上します。
- パスワードのリセットのためのヘルプデスクへの電話が減り、それによりコストが削減され、さらなる節約が可能になります。

IdP との信頼関係

SAML SSO 展開は、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 関係を設定できます。

- ノードごとの配置—UC メタデータの zip ファイルには、各ノードの個別の XML ファイルが含まれています
- クラスターごとの配置 - クラスターの単一のメタデータ ファイル

この信頼関係は、メタデータ ファイルの最初の交換を通じて作成されます。 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
- 組織
- この情報の有効期限
- キャッシュ期間
- この情報の XML 署名
- 連絡先担当者
- 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、サービスプロバイダなど)

認証

IdPにより認証が提供されると、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たアクセスコントロールグループとそれらのグループが提供するロール権限により決定されます。

SAML SSO構成およびIDプロバイダの要件

IDプロバイダの構成情報や要件など、SAML SSOの詳細については、『*Cisco Unified Communications* アプリケーションのための *SAML SSO* 導入ガイド』を参照してください。

[LDAP認証(LDAP Authentication)]

SAML SSOを展開しておらず、ユーザを会社のLDAPディレクトリと同期させている場合、LDAP認証により、会社のLDAPディレクトリに保存されている資格情報と照合してユーザの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Identity Management System (IMS) ライブラリが会社のLDAPディレクトリを使用して、LDAP同期ユーザのユーザパスワードを認証できるようになります。

エンドユーザがセルフケアポータルにログインする場合、会社のLDAPディレクトリで設定されている会社のパスワード(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、簡単なバインド操作によって、企業ディレクトリに対して認証されます。
- 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ます。
- アプリケーションのユーザ パスワードは、Unified CM データベースに対して認証されます。
- エンドユーザの PIN は Unified CM データベースに対して認証されます。

LDAP 認証の設定

この手順を使用して、エンドユーザパスワードのLDAP認証を有効にします。 LDAP認証を既存の LDAP ディレクトリ同期に追加できます。

始める前に

この手順は、既存のLDAPディレクトリ同期が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設定していない場合は、「Cisco Unified Communications Manager 用システム設定ガイド」を参照してセットアップします。

ステップ 1 Cisco Unified CM Administrationから、**[システム（System）] > [LDAP] > [LDAP 認証（LDAP Authentication）]** を選択します。

ステップ 2 **[エンドユーザー用 LDAP 認証の使用（Use LDAP Authentication for End Users）]** チェックボックスをチェックします。

ステップ 3 **LDAP マネージャ識別名**には、LDAP マネージャ (問題の LDAP ディレクトリへのアクセス権限を持つ管理ユーザ) のユーザ ID を入力します。

ステップ 4 **パスワード** を入力し、 **パスワードの再確認** 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、残りのフィールドを入力します。

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

サードパーティの ID プロバイダで SAML SSO を展開していない場合、または LDAP 認証が設定されていない場合、エンドユーザには Cisco Unified Communications Manager データベースに対するローカル認証方式が必要です。 このオプションでは、ユーザ パスワードはローカルデータベースに保存され、[エンド ユーザ設定] で管理されます。

アプリケーションユーザとエンドユーザ PIN の両方について、認証の管理には常にローカルデータベース認証方式が使用されます。 次の表では、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:

パスワードの種類	資格情報の管理
エンド ユーザー パスワード	SAML SSO または LDAP 認証を使用していない場合、エンドユーザのパスワードは個々のエンドユーザの [エンドユーザの設定] 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 [エンドユーザの設定] から更新できます。 エンド ユーザはセルフケア ポータルから自分のパスワードを編集できます。
エンド ユーザ PIN	SAML SSO または LDAP 認証のいずれを展開しているかに関係なく、エンドユーザの PIN は常に Cisco Unified CM 管理の [エンドユーザの構成] ウィンドウで管理されます。 管理者は、[エンドユーザの設定] ウィンドウから既存のエンドユーザ PIN を編集できます。

パスワードの種類	資格情報の管理
アプリケーションユーザーパスワード	SAML SSO または LDAP 認証のどちらを展開しているかに関係なく、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 ユーザの構成] 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、RFC 6749 に基づいて IETF によって定義されています。OAuth 2.0 認証プロトコルにより、リソース所有者 (たとえば、Cisco Unified Communications Manager) は、HTTP サービスへの制限付きアクセスを取得するために、サードパーティのアプリケーションを認証できます。 Cisco Unified Communications Manager では、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提供し、トークンの有効期間中、リソースへのアクセスを提供するためにトークンを更新します。 OAuth により、情報にアクセスしようとするときにウェブサイトがパスワードを要求する必要がなくなります。OAuth では、リソース所有者がクライアントがサーバ上のリソースにアクセスすることを許可します。

Cisco Jabber クライアントは OAuth リフレッシュログインを使用して、Cisco Unified Communications Manager からリソースへのアクセスを取得します。 最初のログインの後、OAuth アクセストークンと更新トークンは、トークンの有効期間中、リソースへのシームレスなアクセスを提供します。

OAuth リフレッシュログイン

OAuth リフレッシュログインでは、短命のアクセストークンにより Jabber が認証され、トークンの寿命中、アクセスが提供されます (アクセストークンのデフォルトの有効期間は 60 分です)。 古いアクセス トークンが期限切れになると、有効期限が長い更新トークンが 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るため、ユーザが再認証する必要なく、シームレスなアクセスを提供できます。

OAuth トークンが有効期間の 75% に達するたびに、エンドユーザの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 はエンドユーザを認証するための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期限の 100% に達した場合、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 Release 15 以降で Webex クライアントにのみ適用できます。

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場合、更新トークンはアクセス トークンの更新プロセス中に自動的に更新されるため、再認証の必要の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します。これにより、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 モードでは、CAPF なしで Jabber の安全な署名とメディアが可能です。 トークンの検証は SIP 登録中に完了します。 このモードでは、Jabber は LSC なしでメディアとシグナリングの暗号化を実行でき、Unified CM で混合モードを有効にする必要はありません。

OAuth のキーの再生成

OAuth トークンの署名と暗号化に使用されるキーが危険にさらされていると思われる場合は、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。

- キー再生認証暗号化設定
- キー再生認証署名設定

（注） OAuth キーが再生成された場合は、Jabber OAuth ログインが動作するように、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 回線に Oauth 更新ログインを使用できるように SIP Oauth モードを設定する方法の詳細については、 *Cisco Unified Communications Manager* 機能設定ガイドの「*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。