クレデンシャル ポリシーの管理

クレデンシャル ポリシーと認証

認証機能は、ユーザの認証、クレデンシャル情報の更新、ユーザイベントとエラーのトラッキングとロギング、クレデンシャル変更履歴の記録、データ ストレージ用のユーザ クレデンシャルの暗号化または復号を行います。

システムは常に、アプリケーション ユーザ パスワードとエンド ユーザ PIN を Unified Communications Manager データベースに照合します。エンド ユーザ パスワードについては、社内ディレクトリまたはデータベースに照合して認証できます。

システムが社内ディレクトリと同期されていれば、Unified Communications Manager または Lightweight Directory Access Protocol（LDAP）のいずれかの認証機能によってパスワードを認証できます。

- LDAP 認証が有効にされている場合、ユーザ パスワードおよびクレデンシャル ポリシーは適用されません。これらのデフォルトは、ディレクトリ同期（DirSync サービス）で作成されたユーザに適用されます。
- LDAP認証を無効にすると、システムはユーザ クレデンシャルをデータベースに照合して認証します。このオプションを使用する場合、クレデンシャル ポリシーを割り当て、認証イベントおよびパスワードを管理することができます。エンドユーザは、電話機のユーザ インターフェイスでパスワードと PIN を変更できます。

クレデンシャル ポリシーは、オペレーティング システムのユーザまたは CLI のユーザには適用されません。オペレーティング システムの管理者は、オペレーティング システムでサポートされている標準のパスワード検証手順を使用します。

データベースにユーザが設定されると、システムはユーザ クレデンシャルの履歴をデータベースに格納して、ユーザがクレデンシャルの変更を要求されたときに以前の情報を入力できないようにします。

クレデンシャル ポリシーの JTAPI および TAPI のサポート

Cisco Unified Communications Manager Java テレフォニー アプリケーション プログラミング インターフェイス（JTAPI）およびテレフォニーアプリケーションプログラミングインターフェイス（TAPI）は、アプリケーションユーザに割り当てられたクレデンシャルポリシーをサポートするため、開発者はパスワードの有効期限、PIN の有効期限、およびクレデンシャル ポリシーの適用ためのロックアウト戻りコードに応答するアプリケーションを作成する必要があります。

アプリケーションは、アプリケーションが使用する認証モデルに関係なく、API を使用してデータベースまたは社内ディレクトリで認証します。

開発者向けの JTAPI および TAPI の詳細については、開発者ガイド（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-programming-reference-guides-list.html）を参照してください。

クレデンシャル ポリシーの設定

クレデンシャル ポリシーは、アプリケーション ユーザとエンド ユーザに適用されます。パスワード ポリシーをエンド ユーザとアプリケーション ユーザに割り当て、PIN ポリシーをエンド ユーザに割り当てます。[クレデンシャル ポリシーのデフォルトの設定（Credential Policy Default Configuration）] に、これらのグループのポリシー割り当てが一覧表示されます。新しいユーザをデータベースに追加すると、システムがデフォルト ポリシーを割り当てます。割り当てられたポリシーを変更したり、ユーザ認証イベントを管理したりできます。

手順

ステップ 1 Cisco Unified CM Administration で、**[ユーザ管理]** > **[ユーザ設定]** > **[クレデンシャル ポリシーのデフォルト]** 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、既存のクレデンシャル ポリシーを選択します。
- [新規追加（Add New）] をクリックして、新しいクレデンシャル ポリシーを作成します。

ステップ 3 [クレデンシャル ポリシーの設定（Credential Policy Configuration）] ウィンドウの各フィールドに入力します。フィールドとその設定の詳細については、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。

クレデンシャル ポリシーのデフォルトの設定

インストール時に、Cisco Unified Communications Manager がスタティック デフォルト クレデンシャル ポリシーをユーザ グループに割り当てます。デフォルト クレデンシャルは提供しません。お使いのシステムが、新しいデフォルト ポリシーを割り当てたり、ユーザの新しいデフォルト クレデンシャルとクレデンシャル要件を設定したりするためのオプションを提供します。

手順

ステップ 1 Cisco Unified CM Administration で、**[ユーザ管理]** > **[ユーザ設定]** > **[クレデンシャル ポリシーのデフォルト]** を選択します。

ステップ 2 [クレデンシャル ポリシー（Credential Policy）] ドロップダウン リスト ボックスから、このグループのクレデンシャル ポリシーを選択します。

ステップ 3 [クレデンシャルの変更（Change Credential）] と [クレデンシャルの確認（Confirm Credential）] の両方にパスワードを入力します。

ステップ 4 このクレデンシャルをユーザに変更させない場合は、[ユーザは変更不可（User Cannot Change）] チェックボックスをオンにします。

ステップ 5 ユーザが次のログイン時に変更する必要がある、一時的なクレデンシャルを設定する場合は、[次回ログイン時に変更必要（User Must Change at Next Login）] チェックボックスをオンにします。

（注） このボックスをオンにすると、ユーザはパーソナル ディレクトリ サービスを使用して PIN を変更できなくなることに注意してください。

ステップ 6 クレデンシャルの期限を設定しない場合は、[有効期限なし（Does Not Expire）] チェックボックスをオンにします。

ステップ 7 **[保存]** をクリックします。

認証アクティビティのモニタ

システムは、最後のハッキング試行時刻や失敗したログイン試行のカウントなどの最新の認証結果を表示します。

システムは、次のクレデンシャル ポリシー イベントに関するログ ファイル エントリを生成します。

- 認証成功
- 認証失敗（不正なパスワードまたは不明）
- 次の原因による認証失敗

- 管理ロック
- ハッキング ロック（失敗したログオン ロックアウト）
- 期限切れソフト ロック（期限切れのクレデンシャル）
- 非アクティブ ロック（一定期間使用されていないクレデンシャル）
- ユーザによる変更が必要（ユーザが変更するように設定されたクレデンシャル）
- LDAP 非アクティブ（LDAP 認証へ切り替えたものの LDAP が非アクティブ）

- 成功したユーザ クレデンシャル更新
- 失敗したユーザ クレデンシャル更新

（注） エンド ユーザ パスワードに対して LDAP 認証を使用する場合は、LDAP は認証の成功と失敗だけを追跡します。

すべてのイベント メッセージに、文字列 「ims-auth」 と認証を試みているユーザ ID が含まれています。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] で、**[ユーザの管理（User Management）] > [エンド ユーザ（End Users）]** を選択します。

ステップ 2 検索条件を入力し、[検索（Find）] をクリックして、表示された一覧からユーザを選択します。

ステップ 3 [クレデンシャルの編集（Edit Credential）] をクリックし、ユーザの認証アクティビティを表示します。

次のタスク

Cisco Unified Real-Time Monitoring Tool（Unified RTMT）を使用してログ ファイルを表示できます。キャプチャされたイベントをレポートに収集することもできます。Unified RTMT の詳細な使用手順については、『*Cisco Unified Real-Time Monitoring Tool Administration Guide*』（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html）を参照してください。

クレデンシャル キャッシングの設定

クレデンシャルキャッシングを有効にすると、システム効率が向上します。システムは、ログイン要求ごとに、データベース ルックアップを実行したり、ストーアド プロシージャを呼び出したりする必要がありません。キャッシュ期間が経過するまでは、関連付けられているクレデンシャル ポリシーが適用されません。

この設定は、ユーザ認証を呼び出すすべての Java アプリケーションに適用されます。

手順

ステップ 1 Cisco Unified CM Administration から、**[システム（System）] > [エンタープライズ パラメータ（Enterprise Parameters）]** を選択します。

ステップ 2 必要に応じて、次のタスクを実行します。

- [キャッシングの有効化（Enable Caching）] エンタープライズ パラメータを [True] に設定します。このパラメータを有効にすると、Cisco Unified Communications Manager は、最大 2 分間、キャッシュされたクレデンシャルを使用します。
- システムがキャッシュされたクレデンシャルを認証に使用しないように、キャッシングを無効にするには、[キャッシングの有効化（Enable Caching）] エンタープライズ パラメータを [False] に設定します。LDAP 認証の場合、この設定は無視されます。クレデンシャル キャッシングでは、ユーザごとに最小量の追加メモリが必要です。

ステップ 3 **[保存（Save）]** をクリックします。

セッション終了の管理

管理者は、各ノードに固有のユーザのアクティブなサインインセッションを終了するために、次の手順を使用できます。

（注）
- 特権レベル 4 を持つ管理者のみが、セッションを終了できます。
- セッション管理では、特定のノード上のアクティブなサインイン セッションを終了します。管理者は、異なるノード間ですべてのユーザセッションを終了する場合には、各ノードにサインインしてセッションを終了する必要があります。

これは、次のインターフェイスに適用されます。

- Cisco Unified CM の管理
- Cisco Unified Serviceability

- Cisco Unified のレポート
- Cisco Unified Communications セルフ ケア ポータル
- Cisco Unified CM IM and Presence の管理
- Cisco Unified IM and Presence サービスアビリティ
- Cisco Unified IM and Presence のレポート

手順

ステップ 1 Cisco Unified OS Administration または Cisco Unified IM and Presence OS Administration から、**[セキュリティ（Security）]** > **[セッション管理（Session Management）]** を選択します。
[セッション管理（Session Management）] ウィンドウが表示されます。

ステップ 2 [ユーザ ID（User ID）] フィールドにアクティブなサインイン ユーザのユーザ ID を入力します。

ステップ 3 [セッションの終了（Terminate Session）] をクリックします。

ステップ 4 [OK] をクリックします。

終了したユーザは、サインインしたインターフェイスページを更新にすると、サインアウトします。監査ログにエントリが作成され、そこに終了した `userID` が表示されます。