クレデンシャル ポリシー

クレデンシャル ポリシーの概要

クレデンシャル ポリシーは、Cisco Unified Communications Manager 内のリソースの認証プロセスを制御します。クレデンシャル ポリシーは、失敗したログイン試行、エンド ユーザ パスワードの有効期限とロックアウト期間、エンドユーザ PIN、アプリケーション ユーザ パスワードなどのパスワード要件とアカウントロックアウトの詳細を定義します。クレデンシャルポリシーは、すべてのエンドユーザ PIN などの特定のクレデンシャル タイプのすべてのアカウントに広く割り当てることも、特定のアプリケーションユーザやエンドユーザ用にカスタマイズすることもできます。

クレデンシャル タイプ

[クレデンシャル ポリシー設定（Credential Policy Configuration）] で、新しいクレデンシャル ポリシーを設定し、次の 3 つのクレデンシャル タイプのそれぞれのデフォルト クレデンシャル ポリシーとして新しいポリシーを適用できます。

- エンド ユーザ PIN
- エンド ユーザ パスワード
- アプリケーション ユーザ パスワード

また、特定のエンド ユーザ PIN、エンド ユーザ パスワード、またはアプリケーション ユーザ パスワードにクレデンシャル ポリシーを適用することもできます。

LDAP 認証が有効になっている場合のログイン情報ポリシー

社内ディレクトリで LDAP 認証用にシステムが設定されている場合は、次の条件を実行します。

- LDAP 認証が有効になっている場合、ログイン情報ポリシーはエンドユーザパスワードに適用されません。
- ログイン情報ポリシーは、LDAP 認証が有効になっているかどうかに関係なく、エンドユーザの PIN とアプリケーション ユーザ パスワードに適用されます。これらのパスワードタイプは、ローカル認証を使用します。

（注） 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。

単純なパスワード

単純なパスワードと PIN を確認するようにシステムを設定できます。単純なパスワードとは、ABCD や 123456 といった容易に推測できるパスワードなどで、これらは簡単にハッキングできるクレデンシャルです。

単純でないパスワードは、次の要件を満たしています。

- 大文字、小文字、数字、記号の 4 種類の文字のうち 3 種類を含んでいる。
- 3 回以上連続して同じ文字や数字を使用していない。
- 繰り返しや、エイリアス、ユーザ名、内線番号を含んでいない。
- 連続する文字または数字で構成されていない。たとえば、654321 または ABCDEFG などのパスワードは許容されません。

PIN には、数字（0 ～ 9）のみを使用できます。単純でない PIN は、次の条件を満たすものとします。

- 3 回以上連続して同じ数字を使用していない。
- 繰り返しや、ユーザの内線番号、メールボックス、またはユーザの反転させた内線番号やメールボックスを含んでいない。
- 3 つの異なる数字を含んでいる。たとえば、121212 などの PIN は単純です。
- ユーザの姓または名の数字表現（たとえば、名前によるダイヤル）が使用されていない。
- たとえば、408408 などの複数の数字の繰り返しや、2580、159、753 などのキーパッド上で直線上にあるダイヤルのパターンを含んでいない。

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。

デフォルトのクレデンシャル ポリシーの設定

新しくプロビジョニングされたユーザに適用されるクラスタ全体のデフォルトクレデンシャルポリシーを設定するには、次の手順を使用します。次の各ログイン情報タイプに対して、個別のログイン情報ポリシーを適用できます。

- アプリケーション ユーザ パスワード
- エンド ユーザのパスワード
- エンドユーザ PIN

手順

Step 1 クレデンシャル ポリシーの設定を入力します。

a) Cisco Unified CM Administration から、**[ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [クレデンシャルポリシー（Credential Policy）]** を選択します。

b) 次のいずれかを実行します。

- **[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。

c) ABCD や 123456 のようなハッキングされやすいパスワードをシステムにチェックさせる場合は、[単純すぎるパスワードのチェック（Check for Trivial Passwords）] チェックボックスをオンにします。

d) [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。

e) [保存（Save）] をクリックします。

f) 他のクレデンシャルタイプのいずれかに対して異なるクレデンシャルポリシーを作成する場合は、これらの手順を繰り返します。

Step 2 クレデンシャルポリシーをクレデンシャルタイプのいずれかに適用します。

a) Cisco Unified CM Administration から、**[ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [クレデンシャルポリシーのデフォルト（Credential Policy Default）]** を選択します。
b) クレデンシャルポリシーを適用するクレデンシャルタイプを選択します。
c) **[クレデンシャルポリシー (Credential policy)]** ドロップダウンから、このクレデンシャルタイプに適用するクレデンシャルポリシーを選択します。たとえば、作成したクレデンシャルポリシーを選択することもできます。
d) [クレデンシャルの変更（Change Credential）] フィールドと [クレデンシャルの確認（Confirm Credential）] フィールドの両方にデフォルトのパスワードを入力します。ユーザは次のログイン時にこれらのパスワードを入力する必要があります。
e) [クレデンシャル ポリシーのデフォルトの設定（Credential Policy Default Configuration）] ウィンドウで、残りのフィールドを設定します。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。
f) [保存（Save）] をクリックします。
g) 他のクレデンシャルタイプのいずれかにクレデンシャルポリシーを割り当てる場合は、これらの手順を繰り返します。

（注） 個人ユーザに対して、[エンドユーザの設定（End User Configuration）] ウィンドウ、またはそのユーザの [アプリケーションユーザの設定（Application User Configuration）] ウィンドウから、特定のユーザログイン情報にポリシーを割り当てることもできます。ログイン情報タイプ（パスワードまたは PIN）の隣にある [ログイン情報の編集（Edit Credential）] ボタンをクリックして、そのユーザログイン情報に関する [ログイン情報の設定（Credential Configuration）] を開きます。

エンドユーザログイン情報またはログイン情報ポリシーの編集

既存のユーザログイン情報を編集する場合、またはユーザログイン情報に割り当てられたポリシーを編集する場合は、次の手順を実行します。ログイン情報をリセットした後は、次のログイン時にユーザがログイン情報を更新する必要があるなどのルールを適用できます。次の場合にこれを行います。

- ローカル DB 認証が設定されている場合にエンドユーザ パスワードをリセットする
- エンドユーザ PIN またはアプリケーション ユーザ パスワードをリセットする
- 特定のユーザログイン情報に割り当てられたログイン情報ポリシーを変更する

手順

Step 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] から、次のいずれかのウィンドウを選択してください。

- エンドユーザーのパスワードと PIN については、**[ユーザ管理（User Management）] > [エンドユーザ（End Users）]]**を選択します。
- アプリケーションのユーザパスワードの場合は、**[ユーザの管理（User Management）] > [アプリケーション ユーザ（Application User）]**を選択します。

Step 2 **[検索（Find）]** をクリックして、該当するユーザを選択します。

Step 3 既存のパスワードまたは PIN を変更する場合、[パスワード（Password）]/[パスワードの確認（Confirm Password）] または [PIN]/[PIN の確認（Confirm PIN）] フィールドに新しいログイン情報を入力し、[保存（Save）] をクリックします。

Step 4 ユーザのログインに割り当てられたログイン情報ポリシーを変更する場合、または次のログイン時にユーザに新しいパスワードまたは PIN の入力を要求するなどのルールを適用する場合は、次の手順を実行します。

a) [パスワード（Password）] または [PIN] の隣にある [ログイン情報の編集（Edit Credential）] ボタンをクリックします。そのユーザログイン情報の [ログイン情報の設定（Credential Configuration）] ウィンドウが開きます。

b) オンプレミスの場合、HTTPのデフォルトは8090、HTTPSのデフォルトは8181です。新しいログイン情報ポリシーを割り当てるには、**[認証ルール（Authentication Rule）]** ドロップダウンリストからポリシーを選択します。

c) オンプレミスの場合、HTTPのデフォルトは8090、HTTPSのデフォルトは8181です。次回のログイン時にパスワードまたは PIN を更新するようにユーザに求める場合は、[ユーザは次のログイン時に変更する必要がある（User Must Change at Next Login）] チェックボックスをオンにします。

d) 残りのフィールドに入力します。フィールドの説明については、オンライン ヘルプを参照してください。

e) [保存（Save）] をクリックします。

PIN同期の有効化

PIN 同期を有効にし、エンドユーザが、エクステンション モビリティ、開催中の会議、モバイル コネクト、および Cisco Unity Connection ボイスメールに同じ PIN を使用してログインできるようにするには、次の手順を実行します。

（注） Cisco Unified Communications Manager パブリッシャ データベース サーバが実行されており、そのデータベースのレプリケーションが完了した場合のみ、Cisco Unity Connection と Cisco Unified Communications Manager 間の PIN の同期に成功します。Cisco Unity Connection で PIN の同期に失敗すると、次のエラーメッセージが表示されます。「CUCMで暗証番号のアップデートに失敗しました。（Failed to update PIN on CUCM.）原因：PIN の取得中にエラーが発生しています。（Reason: Error getting the pin.）」

PIN 同期が有効で、エンドユーザーが PIN を変更した場合は、Cisco Unified Communications Manager で PIN を更新します。この現象は、少なくとも 1 つの構成済みの Unity Connection アプリケーション サーバで、PIN の更新が成功している場合に発生します。

（注） PIN の同期を有効にするには、機能が正常に有効化された後で、管理者がユーザに各自の PIN を変更するよう強制する必要があります。

始める前に

この手順では、すでにアプリケーションサーバが Cisco Unity Connection のセットアップに接続されていることを前提としています。使用していない場合、新しいアプリケーションサーバを追加する方法については、「関連項目」を参照してください。

PIN 同期機能を有効にするには、まず [Cisco Unified OSの管理（Cisco Unified OS Administration）] ページから Cisco Unified Communications Manager tomcat-trust に、有効な証明書をアップロードする必要があります。証明書をアップロードする方法の詳細については、「Cisco Unified Communications Manager アドミニストレーション ガイド」（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html）の「セキュリティ証明書の管理」の章を参照してください。

Cisco Unity Connection サーバのユーザ ID は、Cisco Unified Communications Manager のユーザ ID と一致する必要があります。

手順

Step 1 Cisco Unified CM Administration から、**[システム（System）]>[アプリケーションサーバ（Application Servers）]** を選択します。

Step 2 Cisco Unity Connection をセットアップするアプリケーション サーバを選択します。

Step 3 [エンドユーザのPIN同期（Enable End User PIN Synchronization）] チェックボックスをオンにします。

Step 4 [保存（Save）] をクリックします。

関連トピック

アプリケーション サーバの設定

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

Step 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。

Step 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。

Step 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。また、キャプチャしたイベントをレポートに収集できます。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

Step 1 Cisco Unified CM の管理から、**[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。

Step 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。

Step 3 [保存（Save）] をクリックします。

セッションの終了の管理

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 Administration
- Cisco Unified Serviceability
- Cisco Unified Reporting
- 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

Step 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。

Step 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。

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

Step 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。

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。