資格情報ポリシー

- 資格情報ポリシーの概要 （1 ページ）
- デフォルトのクレデンシャル ポリシーの設定 （3 ページ）
- ユーザ資格情報または資格情報ポリシーの編集 （4 ページ）
- PIN同期の有効化 （5 ページ）
- 認証アクティビティのモニタ （6 ページ）
- クレデンシャル キャッシングの設定 （7 ページ）
- セッション終了の管理 （8 ページ）

資格情報ポリシーの概要

資格情報ポリシーは、Cisco Unified Communications Manager のリソースの認証プロセスを制御します。資格情報ポリシーは、パスワード要件と、エンドユーザのパスワード、エンドユーザのPIN、アプリケーションユーザのパスワードに対する、失敗したログイン試行、有効期限、ロックアウト期間などのアカウントロックアウトの詳細を定義します。資格情報ポリシーは、すべてのエンド ユーザ PIN など、特定の資格情報タイプのすべてのアカウントに広く割り当てたり、特定のアプリケーション ユーザまたはエンド ユーザ向けにカスタマイズしたりできます。

資格情報タイプ

[資格情報ポリシー設定]では、新しい資格情報ポリシーを設定し、その新しいポリシーを次の3つの資格情報タイプのそれぞれに対するデフォルトの資格情報ポリシーとして適用できます。

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

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資格情報ポリシーを適用することもできます。

LDAP 認証が有効な場合の資格情報ポリシー

システムが企業ディレクトリを使用する LDAP 認証用に設定されている場合:

- LDAP 認証が有効な場合、資格情報ポリシーはエンドユーザのパスワードには適用されません。
- 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のパスワードには資格情報ポリシーが適用されます。 これらのパスワードの種類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

簡単なパスワードと PIN をチェックするようにシステムを設定することができます。 簡単なパスワードは簡単にハッキングできる資格情報です。たとえば、「ABCD」をパスワードに使用したり、123456 を PIN に使用したりするなど、簡単に推測できるパスワードです。

簡単でないパスワードは、次の要件を満たします。

- 大文字、小文字、数字、記号の 4 つのうち 3 つ以上が含まれている必要があります。
- 1 つの文字または数字を 4 回以上連続して使用しない。
- エイリアス、ユーザ名、内線を繰り返したり、含めたりしない。
- 連続する文字や数字は使用できません。 例えば、654321 や ABCDEFG のようなパスワードは使用できません。

PIN に使用可能な文字は数字（0 ～ 9）だけです。 単純すぎない PIN とは、次の基準を満たす PIN です。

- 同じ数字を 3 回以上連続して使用しない。
- ユーザの内線番号、メールボックス、またはユーザ内線またはメールボックスの逆を繰り返したり、含めたりしてはなりません。
- 3 つの異なる数字を含める必要があります。 たとえば、121212 などの PIN は単純すぎます。
- ユーザの姓または名の数字表現（名前によるダイヤル）と一致させない。
- 数字の繰り返しグループ（408408 など）、およびキーパッドの直線方向にダイヤルされるパターン（2580、159、753 など）を使用しない。

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のクレデンシャル ポリシーを設定するには、この手順を使用します。 次の各クレデンシャル タイプに対して、個別のクレデンシャル ポリシーを適用できます。

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

ステップ 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 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。

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]** をクリックします。

f) 他のクレデンシャル タイプ用に別のクレデンシャル ポリシーを作成する場合は、この手順を繰り返します。

ステップ 2 次のいずれかのクレデンシャル タイプにクレデンシャル ポリシーを適用します。

a) 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。
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。 ユーザが次にログインするときに、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]** をクリックします。
g) 他のクレデンシャル タイプにクレデンシャル ポリシーを割り当てる場合は、この手順を繰り返します。

（注） また、個々のユーザに対して、**[エンド ユーザの設定]** ウィンドウまたはそのユーザの **[アプリケーション ユーザ設定]** ウィンドウから、特定のユーザクレデンシャルにポリシーを割り当てすることもできます。 クレデンシャル タイプ (パスワードまたは PIN) の隣にある **[クレデンシャルの編集]** ボタンをクリックして、そのユーザの**クレデンシャル設定** を開きます。

ユーザ資格情報または資格情報ポリシーの編集

既存のユーザ資格情報を編集する場合、またはユーザ資格情報に割り当てられているポリシーを編集する場合は、この手順を使用します。 資格情報をリセットした後、ユーザに次回のログイン時に資格情報を更新することを義務付けるなどのルールを適用できます。 次のような場合に、この操作が必要になります。

- ローカル DB 認証が構成されており、エンドユーザのパスワードをリセットしたい場合
- 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したい
- 特定のユーザの資格情報に割り当てられている資格情報ポリシーを変更したい

ステップ 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、**[ユーザー管理（User Management）]** > **[エンドユーザー（End Users）]** を選択してください。

- アプリケーションユーザーのパスワードを設定するには、**[ユーザー管理（User Management）]** > **[アプリケーションユーザー（Application Users）]** を選択します。

ステップ 2 [**検索**] をクリックして適切なユーザを選択します。

ステップ 3 既存のパスワードまたは PIN を変更する場合は、新しい認証情報を **[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）]** フィールドに入力し、**[保存（Save）]** をクリックします。

ステップ 4 ユーザの資格情報に割り当てられている資格情報ポリシーを変更する場合、またはユーザが次回のログイン時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:

a) **[パスワード（Password）]** または **[PIN]** の隣にある **[認証情報の編集（Edit Credential）]** ボタンをクリックします。 そのユーザーの資格情報に対して **[クレデンシャル設定（Credential Configuration）]** ウィンドウが開きます。

b) これはオプションです。 新しい資格情報ポリシーを指定するには、[**認証ルール**] ドロップダウンからポリシーを選択します。

c) これはオプションです。 ユーザーの次回のログイン時にパスワードまたはPINを更新するには、**[ユーザーは次回ログイン時に変更する必要あり（User Must Change at Next Login）]** チェックボックスを選択します。

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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

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。

ステップ 1 Cisco Unified CM Administrationから、**[システム]** > **[企業パラメータ]** 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

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。

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。