



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の概要, 1 ページ](#)
- [クレデンシャルポリシーの設定タスクフロー, 2 ページ](#)

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られることも、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。

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ABCDEFGH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、次の基準を満たしています。

- 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設定タスクフロー

手順

	コマンドまたはアクション	目的
ステップ1	クレデンシャルポリシーの設定, (3 ページ)	エンドユーザとアプリケーションユーザにクレデンシャルポリシーを設定します。
ステップ2	クレデンシャルポリシーのデフォルトクレデンシャルの設定, (3 ページ)	3つのクレデンシャルタイプのいずれか（エンドユーザパスワードとアプリケーションユーザ）にデフォルトのクレデンシャルポリシーとして設定されているクレデンシャルポリシーを適用します。デフォルトのクレデンシャルポリシーは、新規にプロビジョニングされたユーザのクレデンシャルタイプにデフォルトで適用されます。

関連トピック

[エンドユーザへのクレデンシャルポリシーの適用](#)

クレデンシャルポリシーの設定

エンドユーザのPINまたはパスワードなどの特定のクレデンシャルタイプに一致するすべてのクレデンシャルのデフォルトのクレデンシャルポリシーとして適用可能なクレデンシャルポリシーを設定します。

手順

-
- ステップ 1 Cisco Unified CM の管理から、[ユーザの管理 (User Management)] > [クレデンシャルポリシー (Credential Policy)] 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。
-

次の作業

[クレデンシャルポリシーのデフォルトクレデンシャルの設定, \(3 ページ\)](#)

クレデンシャルポリシーのデフォルトクレデンシャルの設定

クレデンシャルポリシーのデフォルトクレデンシャルを設定するには、次の手順を実行します。ユーザが次のログインで変更する必要がある一時的なパスワードを割り当てるために、デフォルトクレデンシャルを割り当てることができます。

はじめる前に

[クレデンシャルポリシーの設定, \(3 ページ\)](#)

手順

-
- ステップ 1 [Cisco Unified CM の管理 (Cisco Unified CM Administration)] で、[ユーザ管理 (User Management)] > [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。
 - 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。
 - 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 (Save)] をクリックします。
-

次の作業

特定のエンドユーザまたは PIN にクレデンシャルポリシーを適用する場合：

- [エンドユーザへのクレデンシャルポリシーの適用](#)