CHAPTER 104

クレデンシャル ポリシーの設定

Cisco Unified Communications Manager の管理ページの［クレデンシャルポリシーの設定（Credential Policy Configuration）］ウィンドウを使用すると、セキュアなユーザ アカウントにクレデンシャル ポリシーを設定できます。

ポリシーは、システム リソースまたはネットワーク リソースへのアクセスを制御する規則のセットで構成されます。クレデンシャル ポリシーは、ユーザ アカウントのパスワード要件およびアカウント ロックアウトを定義します。

ユーザ アカウントに割り当てられたクレデンシャル ポリシーは、Cisco Unified Communications Manager の認証プロセスを制御します。

クレデンシャル ポリシーの追加後は、クレデンシャル タイプまたは個々のアプリケーション ユーザまたはエンド ユーザのデフォルト ポリシーに、新しいポリシーを割り当てることができます。

この章では、クレデンシャル ポリシーの設定方法について説明します。クレデンシャル ポリシー割り当ての詳細については、P.104-8 の「関連項目」を参照してください。

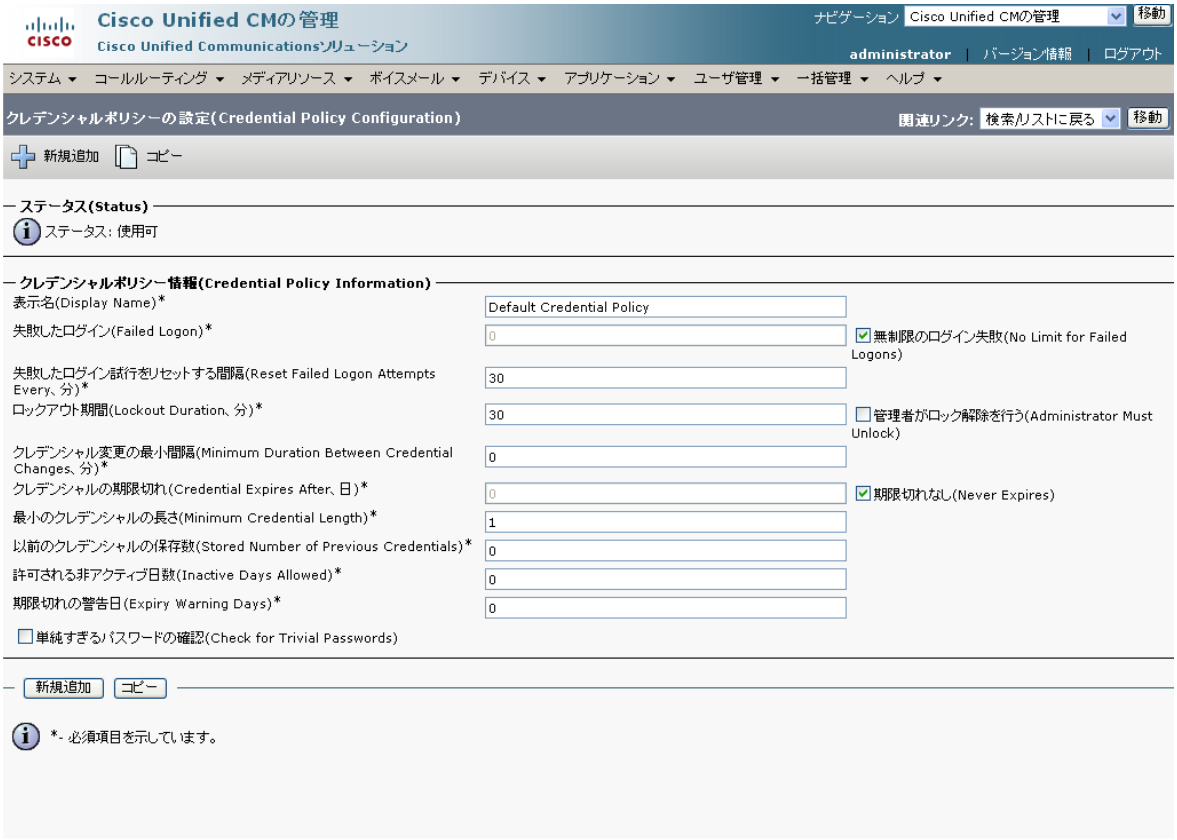
次のトピックでは、クレデンシャル ポリシーの設定について説明します。

デフォルトのクレデンシャル ポリシー

インストール時に、Cisco Unified Communications Manager は、静的なクレデンシャル ポリシーをエンド ユーザ PIN、アプリケーション ユーザ パスワード、およびエンド ユーザ パスワードに割り当てます。ポリシーには、失敗したログインのリセット、ロックアウト期間、有効期間、およびクレデンシャル要件の設定が含まれます。[クレデンシャル ポリシーの設定（Credential Policy Configuration）] ウィンドウを使用すると、システムまたはサイトの新しいクレデンシャル ポリシーを設定できます。静的なポリシーは変更できません。

図 104-1 に、システムのデフォルトのクレデンシャル ポリシー設定を示します。デフォルトのクレデンシャル ポリシーは、インストールとアップグレードを簡単にするために提供されます。この設定は、新しいクレデンシャル ポリシーを追加するときにシステムが提供する、クレデンシャル ポリシーのデフォルト設定とは異なります。

図 104-1　システムのデフォルトクレデンシャル ポリシーの設定



単純すぎるクレデンシャルのチェック

システムには、簡単にハッキングされるクレデンシャルを許可しないようにするための、単純すぎるクレデンシャルのチェックが用意されています。単純すぎるクレデンシャルのチェックを有効にするには、［クレデンシャルポリシーの設定（Credential Policy Configuration）］ウィンドウの［単純すぎるパスワードの確認（Check for Trivial Passwords）］チェックボックスをオンにします。

パスワードには、すべての ASCII 英数字とすべての ASCII 特殊文字が使用できます。単純すぎないパスワードとは、次の基準を満たすパスワードです。

- 使用可能な 4 つの特性（大文字、小文字、数字、記号）のうち、3 つを含む。
- 1 つの文字または数字を 4 つ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。
- 連続した文字または数字で構成しない（たとえば、654321 や ABCDEFG などのパスワードにしない）。

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。
- ユーザの内線またはメールボックス、またはユーザの内線またはメールボックスの逆を繰り返したり、含めたりしない。
- 3 つの異なる数字を含める（たとえば、121212 のような PIN は単純すぎる）。
- 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、113377 など）、またはキーパッドの直線上に並ぶパターン（2580、159、753 など）を含めない。

クレデンシャル ポリシーの検索

ここでは、既存のクレデンシャル ポリシーを検索または確認する方法を説明します。

ステップ 1　**［ユーザ管理］＞［クレデンシャルポリシー］**の順に選択します。

［クレデンシャルポリシーの検索と一覧表示（Find and List Credential Policies）］ウィンドウが表示されます。

ステップ 2　表示するリスト項目をクリックします。

選択したクレデンシャル ポリシーがウィンドウに表示されます。

追加情報

P.104-8 の「関連項目」を参照してください。

クレデンシャル ポリシーの設定

ここでは、新しいクレデンシャル ポリシーの作成方法と、既存のクレデンシャル ポリシーの変更方法を説明します。システムのデフォルトのクレデンシャル ポリシーは変更できません。

手順

ステップ 1　［ユーザ管理］>［クレデンシャルポリシー］の順に選択します。

［クレデンシャルポリシーの検索と一覧表示（Find and List Credential Policies）］ウィンドウが表示されます。

ステップ 2　次のいずれかの作業を行います。

- 新しいポリシーを追加するには、検索ウィンドウの［新規追加］ボタンまたは［新規追加］アイコンをクリックするか、リストからクレデンシャル ポリシーを表示して、［コピー］または［新規追加］ボタンまたはアイコンをクリックします。［新規追加］をクリックすると、各フィールドにデフォルト値が設定された［クレデンシャルポリシーの設定（Credential Policy Configuration）］ウィンドウが表示されます。［コピー］をクリックすると、表示されているポリシーの値が設定された、［クレデンシャルポリシーの設定（Credential Policy Configuration）］ウィンドウが表示されます。ステップ 3 に進みます。
- 既存のエントリを更新するには、変更するポリシーをクリックします。［クレデンシャルポリシーの設定（Credential Policy Configuration）］ウィンドウに、現在の設定値が表示されます。ステップ 3 に進みます。

ステップ 3　適切な設定値を入力します（表 104-1 を参照）。

ステップ 4　［保存］ボタンまたは［保存］アイコンをクリックします。

次の手順

クレデンシャル タイプのデフォルト ポリシーとして新しいクレデンシャル ポリシーを割り当てるには、P.103-2 の「クレデンシャル ポリシーのデフォルトの割り当てと設定」の手順に従います。

個々のユーザに新しいクレデンシャル ポリシーを割り当てるには、P.105-15 の「アプリケーション ユーザのクレデンシャルの管理」および P.106-16 の「エンド ユーザのクレデンシャルの管理」の手順に従います。

追加情報

P.104-8 の「関連項目」を参照してください。

クレデンシャル ポリシーの設定値

表 104-1 では、クレデンシャル ポリシーの設定値について説明します。関連する情報および手順については、P.104-8 の「関連項目」を参照してください。

表 104-1　クレデンシャル ポリシーの設定値

フィールド	説明
［表示名（Display Name）］	クレデンシャル ポリシー名を指定します。 最大 64 文字を入力します。特殊文字のうち、ダッシュ（-）引用符（“”）、バックスラッシュ（\）は使用できません。
［失敗したログイン（Failed Logon）］/［無制限のログイン失敗（No Limit for Failed Logons）］	許可されるログイン試行の失敗回数を指定します。このしきい値に達すると、アカウントがロックされます。 1 ～ 10 の数値を入力します。失敗ログインを無制限に許可するには、**0** を入力するか、［無制限のログイン失敗（No Limit for Failed Logons）］チェックボックスをオンにします。0 よりも大きな値を入力するには、このチェックボックスをオフにします。デフォルト設定は 3 です。
［失敗したログイン試行をリセットする間隔（Reset Failed Logon Attempts Every、分）］	失敗したログイン試行のカウンタをリセットするまでの時間を分単位で指定します。カウンタをリセットすると、ユーザは、再度ログインを試行できるようになります。 1 ～ 120 の数値を入力します。デフォルト設定は 30 です。
［ロックアウト期間（Lockout Duration、分）］/［管理者がロック解除を行う（Administrator Must Unlock）］	失敗したログイン試行回数が指定されているしきい値に達したときに、アカウントをロックする時間を分単位で指定します。 1 ～ 120 の数値を入力します。**0** を入力するか、［管理者がロック解除を行う（Administrator Must Unlock）］チェックボックスをオンにすると、アカウントは管理者が手動でロックを解除するまでロックされたままになります。0 よりも大きな値を入力するには、このチェックボックスをオフにします。デフォルト設定は 30 です。
［クレデンシャル変更の最小間隔（Minimum Duration Between Credential Changes、分）］	ユーザがクレデンシャルを再度変更できるようになるまでの時間を分単位で指定します。 1 ～ 120 の数値を入力します。**0** を入力すると、ユーザがいつでもクレデンシャルを変更できるようになります。0 よりも大きな値を入力するには、このチェックボックスをオフにします。デフォルト設定は 0 です。
［クレデンシャルの期限切れ（Credential Expires After、日）］/［期限切れなし（Never Expires）］	クレデンシャルの有効期限が切れる日数を指定します。 1 ～ 365 の数値を入力します。クレデンシャルの有効期限が切れないようにするには、**0** を入力するか、［期限切れなし（Never Expires）］チェックボックスをオンにします。0 よりも大きな値を入力するには、このチェックボックスをオフにします。0 オプションは、たとえば、セキュリティの低いアカウントや複数ユーザのアカウントに使用します。デフォルト設定は 180 です。
［最小のクレデンシャルの長さ（Minimum Credential Length）］	ユーザ クレデンシャル（パスワードまたは PIN）の最小の長さを指定します。 空白のパスワードは許可されないため、0 は入力しないでください。デフォルト設定は 8 です。最小の設定は 1 以上です。

表 104-1　クレデンシャル ポリシーの設定値（続き）

フィールド	説明
［以前のクレデンシャルの保存数（Stored Number of Previous Credentials）］	ユーザの以前のクレデンシャルを、いくつ保存するかを指定します。この設定によって、ユーザ リストに保存されている、最近使用したクレデンシャルをユーザが設定できないようにします。 0 ～ 25 の数値を入力します。以前のクレデンシャルを保存しないようにするには、**0** を入力します。デフォルト設定は 12 です。
［許可される非アクティブ日数（Inactive Days Allowed）］	パスワードを非アクティブなままにできる日数を指定します。この日数を超えて非アクティブになると、アカウントがロックされます。 0 ～ 5000 の数値を入力します。デフォルト設定は 0 です。
［期限切れの警告日（Expiry Warning Days）］	0 ～ 90 の数値を入力して、ユーザ パスワードが期限切れになる何日前から警告通知の表示を開始するかを指定します。デフォルト設定は 0 です。
［単純すぎるパスワードの確認（Check for Trivial Passwords）］	一般的な単語、文字パターンの繰り返しなど、簡単にハッキングされるクレデンシャルを許可しないようにする必要がある場合は、このチェックボックスをオンにします。このチェックボックスがオンの場合に、クレデンシャルが満たす必要がある条件のリストについては、P.104-3 の「単純すぎるクレデンシャルのチェック」を参照してください。 デフォルト設定では、このチェックボックスはオンです。

クレデンシャル ポリシーの削除

ここでは、Cisco Unified Communications Manager データベースからセキュリティ ポリシーを削除する方法を説明します。

始める前に

（注）　エンドユーザ パスワード、エンドユーザ PIN、アプリケーション ユーザ パスワードのデフォルト ポリシーとして割り当てられているクレデンシャル ポリシーは削除できません。

クレデンシャル ポリシーを使用しているデフォルト ポリシーを検索するには、［クレデンシャルポリシーの設定（Credential Policy Configuration）］ウィンドウの［関連リンク］ドロップダウン リスト ボックスから［**依存関係レコード**］を選択し、［**移動**］をクリックします。

依存関係レコード機能がシステムで使用可能でない場合、［依存関係レコード要約（Dependency Records Summary）］ウィンドウにメッセージが表示され、依存関係レコードを使用可能にするための操作が示されます。このメッセージには、依存関係レコード機能によって CPU に高い負荷がかかることも表示されます。依存関係レコードの詳細については、P.A-4 の「依存関係レコードへのアクセス」を参照してください。

使用中のクレデンシャル ポリシーを削除しようとすると、メッセージが表示されます。現在使用中のクレデンシャル ポリシーを削除するには、ユーザに対して別のクレデンシャル ポリシーを選択するか、新しいポリシーを作成して割り当てる必要があります（P.104-4 の「クレデンシャル ポリシーの設定」を参照）。

手順

ステップ 1　P.104-3 の「クレデンシャル　ポリシーの検索」の手順を使用して、削除するクレデンシャル　ポリシーを検索します。レコードのリストから、削除するポリシーをクリックします。

（注）　該当するエントリの横にあるチェックボックスをオンにして、［**選択項目の削除**］ボタンまたは［**選択項目の削除**］アイコンをクリックすると、［クレデンシャルポリシーの検索と一覧表示（Find and List Credential Policies）］ウィンドウからエントリを削除できます。［**すべてを選択**］ボタンまたは［**すべてを選択**］アイコンをクリックして、［**選択項目の削除**］ボタンまたは［**選択項目の削除**］アイコンをクリックすると、リストのすべてのエントリを削除できます。

ステップ 2　［クレデンシャルポリシーの設定（Credential Policy Configuration）］ウィンドウの［**削除**］アイコンまたは［**削除**］ボタンをクリックすると、ポリシーが削除されます。

ステップ 3　削除操作の確認を求められたら、［**OK**］をクリックすると、ポリシーが削除されます。

追加情報

P.104-8 の「関連項目」を参照してください。

関連項目

- デフォルトのクレデンシャル ポリシー（P.104-2）
- クレデンシャル ポリシーの検索（P.104-3）
- クレデンシャル ポリシーの設定（P.104-4）
- クレデンシャル ポリシーの設定値（P.104-5）
- クレデンシャル ポリシーの削除（P.104-7）
- クレデンシャル ポリシーのデフォルトの検索（P.103-2）
- クレデンシャル ポリシーのデフォルトの割り当てと設定（P.103-2）
- クレデンシャル ポリシーのデフォルトの設定値（P.103-4）
- アプリケーション ユーザのパスワードの変更（P.105-14）
- エンド ユーザのパスワードの変更（P.106-14）
- エンド ユーザの PIN の変更（P.106-15）
- エンド ユーザのクレデンシャルの管理（P.106-16）
- アプリケーション ユーザのクレデンシャルの管理（P.105-15）
- 『*Cisco Unified Communications Manager システム ガイド*』の「アプリケーション ユーザとエンド ユーザ」
- 『*Cisco Unified Communications Manager システム ガイド*』の「アプリケーション ユーザとエンド ユーザの設定チェックリストの管理」
- 『*Cisco Unified Communications Manager システム ガイド*』の「Cisco Unity メッセージングの統合」
- LDAP システムの設定（P.14-1）
- 電話番号の設定（P.57-1）
- CTI ルート ポイントの設定（P.79-1）
- 『*Cisco Unified Communications Manager 機能およびサービス ガイド*』の「Cisco エクステンション モビリティ」