CHAPTER 21

クレデンシャル ポリシー

Cisco Unified Communications Manager は、ユーザのシステム アクセスを許可する前に、ユーザのログイン クレデンシャルを認証します。ユーザ アカウントを保護するには、失敗したログイン試行、ロックアウト期間、パスワード有効期間、およびパスワード要件に関する設定を Cisco Unified Communications Manager の管理ページで指定します。これらの認証規則によって、クレデンシャル ポリシーが構成されます。

クレデンシャル ポリシーの適用対象は、アプリケーション ユーザとエンド ユーザです。管理者は、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。これらのグループのポリシー割り当ては、[クレデンシャルポリシーのデフォルトの設定 (Credential Policy Default Configuration)] に一覧表示されます。

インストール時に、Cisco Unified Communications Manager は静的なデフォルト 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されません。ユーザに新しいデフォルト ポリシーを割り当てて、新しいデフォルト クレデンシャルおよびクレデンシャル要件を設定するためのオプションは、Cisco Unified Communications Manager の管理ページの [クレデンシャルポリシーのデフォルトの設定 (Credential Policy Default Configuration)] ウィンドウにあります。

(注) 空の（ヌル）クレデンシャルはサポートされません。システムで LDAP 認証を使用している場合は、インストール直後にエンド ユーザのデフォルト クレデンシャルを設定する必要があります。設定しないと、ログインが失敗します。

新しいユーザを Cisco Unified Communications Manager データベースに追加すると、デフォルト ポリシーが割り当てられます。ユーザの設定ウィンドウの [クレデンシャルの編集] ボタンを使用して、割り当てられたポリシーを変更し、ユーザ認証イベントを管理することができます。詳細については、「クレデンシャルの管理」（P.20-5）を参照してください。

この章の構成は、次のとおりです。

クレデンシャル ポリシー設定チェックリスト

Cisco Unified Communications Manager は、ユーザのシステム アクセスを許可する前に、ユーザのログイン クレデンシャルを認証します。ユーザ アカウントを保護するには、失敗したログイン試行、ロックアウト期間、パスワード有効期間、およびパスワード要件に関する設定を Cisco Unified Communications Manager の管理ページで指定します。これらの認証規則によって、クレデンシャル ポリシーが構成されます。

クレデンシャル ポリシーの適用対象は、アプリケーション ユーザとエンド ユーザです。管理者は、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。これらのグループのポリシー割り当ては、[クレデンシャルポリシーのデフォルトの設定 (Credential Policy Default Configuration)] に一覧表示されます。

インストール時に、Cisco Unified Communications Manager は静的なデフォルト 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されません。ユーザに新しいデフォルト ポリシーを割り当てて、新しいデフォルト クレデンシャルおよびクレデンシャル要件を設定するためのオプションは、Cisco Unified Communications Manager の管理ページの [クレデンシャルポリシーのデフォルトの設定 (Credential Policy Default Configuration)] ウィンドウにあります。

（注） 空の（ヌル）クレデンシャルはサポートされません。システムで LDAP 認証を使用している場合は、インストール直後にエンド ユーザのデフォルト クレデンシャルを設定する必要があります。設定しないと、ログインが失敗します。

新しいユーザを Cisco Unified Communications Manager データベースに追加すると、デフォルト ポリシーが割り当てられます。ユーザの設定ウィンドウの [クレデンシャルの編集] ボタンを使用して、割り当てられたポリシーを変更し、ユーザ認証イベントを管理することができます。

表 21-1 は、クレデンシャル ポリシーを設定するための一般的な手順とガイドラインを示しています。詳細については、「参考情報」（P.21-5）を参照してください。

表 21-1　クレデンシャル ポリシー設定チェックリスト

設定ステップ		関連した手順と項目
ステップ 1	[クレデンシャルポリシーの設定 (Credential Policy Configuration)] ウィンドウを使用して、デフォルト ポリシー以外のクレデンシャル ポリシーを設定します。	『*Cisco Unified Communications Manager アドミニストレーション ガイド*』の「クレデンシャル ポリシーの設定」
ステップ 2	[クレデンシャルポリシーのデフォルト (Credential Policy Default)] ウィンドウを使用して、新しいクレデンシャル ポリシーを割り当て、アカウント タイプに対して共通パスワードを設定します。	『*Cisco Unified Communications Manager アドミニストレーション ガイド*』の「クレデンシャル ポリシーのデフォルトの設定」 『*Cisco Unified Communications Manager Bulk Administration ガイド*』
ステップ 3	個々のユーザのクレデンシャル設定を管理または監視するには、ユーザの設定ウィンドウの [クレデンシャルの編集] リンクをクリックします。	『*Cisco Unified Communications Manager アドミニストレーション ガイド*』の「エンド ユーザのクレデンシャルの管理」 『*Cisco Unified Communications Manager アドミニストレーション ガイド*』の「アプリケーション ユーザのクレデンシャルの管理」

クレデンシャル ポリシーおよび認証

Cisco Unified Communications Manager の認証機能は、ユーザの認証、クレデンシャルの更新、ユーザ イベントとエラーの追跡およびロギング、クレデンシャルの変更履歴の記録、データ保管のためのユーザ クレデンシャルの符号化とデコード（または暗号化と復号化）を実行します。

システムは、アプリケーション ユーザのパスワードとエンド ユーザの PIN を、常に Cisco Unified Communications Manager データベースと照合して認証します。システムは、エンド ユーザのパスワードを社内ディレクトリまたは Cisco Unified Communications Manager データベースと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化されている場合は、Cisco Unified Communications Manager の認証機能または LDAP によって、このパスワードを認証できます。

- LDAP 認証が有効になっている場合、Cisco Unified Communications Manager の管理ページで設定されたユーザ パスワードとクレデンシャル ポリシーは適用されません。これらのデフォルトは、ディレクトリ同期化（DirSync サービス）で作成されたユーザに適用されます。
- LDAP 認証が無効になっている場合、システムは、ユーザ クレデンシャルを Cisco Unified Communications Manager 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と、管理者はクレデンシャル ポリシーの割り当て、認証イベントの管理、およびパスワードの管理ができます。エンド ユーザは、電話機のユーザ ページでパスワードと PIN を変更できます。

LDAP 認証の詳細については、「ディレクトリの概要」（P.19-1）の章を参照してください。

クレデンシャル ポリシーは、OS ユーザおよび CLI ユーザには適用されません。これらの管理者は、OS がサポートしている標準のパスワード検証手順を使用します。OS のログイン手順については、『*Cisco Unified Communications Operating System Administration Guide*』を参照してください。

クレデンシャルのキャッシュ

管理者がエンタープライズ パラメータ Enable Caching を [True] に設定すると、パフォーマンスを向上させることができます。Cisco Unified Communications Manager が、キャッシュされたクレデンシャルを最長で 2 分間使用できるようになります。ログイン要求が発行されるたびに、Cisco Unified Communications Manager がデータベース検索を実行したり、ストアド プロシージャを起動したりする必要がなくなり、システムの効率が向上します。関連付けられているクレデンシャル ポリシーは、キャッシュ期間が終了するまで利用されません。

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。このエンタープライズ パラメータを [False] に設定すると、キャッシュがオフになり、キャッシュされたクレデンシャルが認証に使用されなくなります。LDAP 認証では、この設定は無視されます。クレデンシャルのキャッシュを実行する場合は、ユーザごとに、ごくわずかな追加メモリが必要になります。

BAT による管理

一括管理ツール（BAT）を使用すると、一連のユーザについて、パスワードや PIN などの一般的なクレデンシャル パラメータを BAT のユーザ テンプレートで定義できます。ユーザ テンプレートを初めて作成するときは、すべてのユーザに静的なデフォルト クレデンシャル ポリシーが割り当てられます。詳細については、『*Cisco Unified Communications Manager Bulk Administration ガイド*』を参照してください。

JTAPI/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 ユーザに関連付けるクレデンシャル ポリシーをサポートしています。クレデンシャル ポリシーを適用するには、パスワード有効期間、PIN 有効期間、およびロックアウト戻りコードに対応でき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、どの認証モデルを使用するかにかかわらず、API を使用し、データベースまたは社内ディレクトリと照合して認証を実行します。

クレデンシャル ポリシーおよび認証をサポートしている新しいエラー文字列については、『*Cisco Unified Communications Manager JTAPI Developers Guide*』および『*Cisco Unified Communications Manager TAPI Developers Guide*』を参照してください。

クレデンシャルの履歴

ユーザがデータベース内に設定されると、ユーザ クレデンシャルの履歴がデータベースに格納されます。ユーザは、クレデンシャルを変更するように求められたとき、以前と同じクレデンシャルを入力することはできません。

認証イベント

管理者は、ユーザの [クレデンシャル設定 (Credential Configuration)] ページでユーザ認証アクティビティを監視し、管理することができます。このページにアクセスするには、ユーザの設定ウィンドウの [クレデンシャルの編集] ボタンを使用します。最後のハック試行時刻、失敗したログイン試行の回数など、最新の認証結果が表示されます。

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*』の「エンドユーザのクレデンシャルの管理」および「アプリケーション ユーザのクレデンシャルの管理」を参照してください。

システムは、次のクレデンシャル ポリシー イベントのログ ファイル エントリを作成します。

- 認証の成功
- 認証の失敗（不正なパスワードまたは未知のパスワード）
- 次の原因による認証の失敗
  - 管理ロック
  - ハック ロック（失敗したログインのロックアウト）
  - 期限切れソフト ロック（有効期限が切れたクレデンシャル）
  - 非アクティブ ロック（クレデンシャルが一定の期間にわたって使用されていない）
  - ユーザによる変更が必要（クレデンシャルが、ユーザによる変更必須として設定されている）
  - LDAP 非アクティブ（LDAP 認証への切り替えと LDAP 非アクティブ）
- ユーザ クレデンシャルの更新の成功
- ユーザ クレデンシャルの更新の失敗

（注） エンド ユーザのパスワードに対して LDAP 認証を使用している場合、LDAP が追跡するのは認証の成否だけです。

イベント メッセージには、常に「ims-auth」という文字列と、認証を試行したユーザの ID が記述されます。

ログ ファイルは、Real-Time Monitoring Tool を使用して表示できます。記録されたイベントを収集して、レポートにすることもできます。詳細については、『*Cisco Unified Real Time Monitoring Tool Administration Guide*』および『*Cisco Unified Communications Manager CDR Analysis and Reporting Administration Guide*』を参照してください。

Data Migration Assistant

Cisco Unified Communications Manager Data Migration Assistant（DMA）では、Cisco Unified Communications Manager のデータは、次に示す Cisco Unified Communications Manager の上位リリースと互換性のある形式に変換されます。

- 5.x リリースからのアップグレードでは、エンド ユーザのパスワードと PIN は自動的に移行される。インストール時に設定したアプリケーション パスワードが、すべてのアプリケーション ユーザに適用されます。
- 4.x リリースからのアップグレードでは、エンド ユーザのクレデンシャルはリセットされる。インストール時、デフォルトのエンド ユーザ パスワードと PIN が照会され、すべてのエンド ユーザにそのクレデンシャルが適用されます。インストール時に設定したアプリケーション パスワードは、すべてのアプリケーション ユーザに適用されます。

DMA の入手、インストール、および使用方法の詳細については、『*Cisco Unified Communications Manager Data Migration Assistant User Guide*』を参照してください。

参考情報

関連項目

- 「クレデンシャル ポリシー設定チェックリスト」（P.21-2）
- 「クレデンシャル ポリシーおよび認証」（P.21-3）
- 「クレデンシャルのキャッシュ」（P.21-3）
- 「BAT による管理」（P.21-3）
- 「JTAPI/TAPI のサポート」（P.21-4）
- 「クレデンシャルの履歴」（P.21-4）
- 「認証イベント」（P.21-4）
- 「Data Migration Assistant」（P.21-5）
- 「ディレクトリの概要」（P.19-1）
- 「アプリケーション ユーザとエンド ユーザ」（P.20-1）
- 『*Cisco Unified Communications Manager アドミニストレーション ガイド*』の「エンド ユーザのクレデンシャルの管理」

- 『*Cisco Unified Communications Manager アドミニストレーション ガイド*』の「アプリケーション ユーザのクレデンシャルの管理」
- 『*Cisco Unified Communications Manager アドミニストレーション ガイド*』の「クレデンシャル ポリシーの設定」
- 『*Cisco Unified Communications Manager アドミニストレーション ガイド*』の「クレデンシャル ポリシーのデフォルトの設定」
- 『*Cisco Unified Communications Manager アドミニストレーション ガイド*』の「LDAP システムの設定」
- 『*Cisco Unified Communications Manager アドミニストレーション ガイド*』の「LDAP ディレクトリの設定」
- 『*Cisco Unified Communications Manager アドミニストレーション ガイド*』の「LDAP 認証の設定」
- 『*Cisco Unified Communications Manager アドミニストレーション ガイド*』の「アプリケーション ユーザの設定」
- 『*Cisco Unified Communications Manager アドミニストレーション ガイド*』の「エンド ユーザの設定」

参考資料

- 『*Installing Cisco Unified Communications Manager Release 8.0(1)*』
- 『*Cisco Unified Communications Operating System Administration Guide*』
- 『*Data Migration Assistant User Guide*』
- 『*Cisco Unified Communications Solution Reference Network Design (SRND)*』
- 『*Cisco Unified Communications Manager 機能およびサービス ガイド*』
- 『*Cisco Unified Serviceability Administration Guide*』
- 『*Cisco Unified Real Time Monitoring Tool Administration Guide*』
- 『*Cisco Unified Communications Manager CDR Analysis and Reporting Administration Guide*』
- 『*Cisco Unified Communications Manager Bulk Administration ガイド*』
- 『*Cisco Unified Communications Manager セキュリティ ガイド*』
- Cisco Unified IP Phone のユーザ マニュアルとリリース ノート（全モデル）