



アプリケーション ユーザの設定

次のトピックでは、アプリケーション ユーザ情報の管理について説明します。

- 「アプリケーション ユーザの設定値」 (P.87-1)
- 「Cisco Unity または Cisco Unity Connection への管理者ユーザの追加」 (P.87-8)
- 「アプリケーション ユーザのパスワードの変更」 (P.87-9)
- 「アプリケーション ユーザのクレデンシャルの管理」 (P.87-9)
- 「クレデンシャルの設定値とフィールド」 (P.87-11)
- 「アプリケーション ユーザとデバイスとの関連付け」 (P.87-12)
- 「関連項目」 (P.87-13)

アプリケーション ユーザの設定値

Cisco Unified Communications Manager の管理ページでは、[ユーザ管理 (User Management)] > [アプリケーション ユーザ (Application User)] メニュー パスを使用して、アプリケーション ユーザを設定します。

Cisco Unified Communications Manager の管理ページの [アプリケーション ユーザの設定 (Application User Configuration)] ウィンドウを使用すると、システム管理者は、Cisco Unified Communications Manager アプリケーション ユーザに関する情報を追加、検索、表示、および保持することができます。

アプリケーション ユーザの設定のヒント



(注)

インストール時に、Cisco Unified Communications Manager のデフォルト アプリケーション ユーザのセットが設定されます。



(注)

Cisco Unity または Cisco Unity Connection の管理者アカウントを追加する場合は、Cisco Unity および Cisco Unity Connection の管理 で定義したものと同一ユーザ名およびパスワードを使用する必要があります。ユーザ ID を使用して、Cisco Unity または Cisco Unity Connection と Cisco Unified Communications Manager の管理 との間の認証を行います。Cisco Unity または Cisco Unity Connection 用の該当する Cisco Unified Communications Manager インテグレーションガイドを参照してください。

[アプリケーションユーザの設定 (Application User Configuration)] ウィンドウの [Cisco Unity アプリケーションユーザの作成 (Create Cisco Unity Application User)] オプションを使用することで、Cisco Unified Communications Manager の管理アプリケーション ユーザを Cisco Unity ユーザまたは Cisco Unity Connection ユーザとして設定できます。その後は、その他の設定値を Cisco Unity または Cisco Unity Connection の管理で設定できます。

このアプリケーション ユーザのユーザ特権レポートを表示するには、[関連リンク (Related Links)] ドロップダウン リスト ボックスから [ユーザ特権レポート (User Privilege Report)] を選択し、[移動 (Go)] をクリックします。

このアプリケーション ユーザの [ユーザ特権 (User Privilege)] ウィンドウが表示されます。ユーザ特権レポートの詳細については、「[ユーザの権限、ユーザ グループ、およびアクセス権の表示](#) (P.90-8) を参照してください。

このアプリケーション ユーザのユーザ特権レポートを表示した後、このアプリケーション ユーザの [アプリケーションユーザの設定 (Application User Configuration)] ウィンドウに戻ることができます。[ユーザ特権 (User Privilege)] ウィンドウの [関連リンク (Related Links)] ドロップダウン リスト ボックスから [アプリケーションユーザに戻る (Back to Application User)] を選択し、[移動 (Go)] をクリックします。

アプリケーション ユーザの設定の次のステップ

このアプリケーション ユーザにデバイスを関連付ける場合は、後述の「[アプリケーション ユーザとデバイスとの関連付け](#)」の手順に進みます。

このアプリケーション ユーザのクレデンシャルを管理する場合は、後述の「[アプリケーション ユーザのクレデンシャルの管理](#)」の手順に進みます。

管理者ユーザを Cisco Unity または Cisco Unity Connection に追加する場合は、後述の「[Cisco Unity または Cisco Unity Connection への管理者ユーザの追加](#) (P.87-8) の手順に進みます。

アプリケーション ユーザの削除のヒント

アプリケーション ユーザを削除する前に、そのエンド ユーザに関連付けられているデバイスまたはプロフィールを削除する必要があるかどうかを判断します。

アプリケーション ユーザに割り当てられているプロフィールおよび権限は、[アプリケーション ユーザの設定 (Application User Configuration)] ウィンドウの [CAPF 情報 (CAPF Information)] 領域および [権限情報 (Permissions Information)] 領域から表示できます。[アプリケーション ユーザの設定 (Application User Configuration)] ウィンドウで、[関連リンク (Related Links)] ドロップダウン リスト ボックスから [依存関係レコード (Dependency Records)] を選択することもできます。依存関係レコードがシステムで使用可能になっていない場合、[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ます。依存関係レコードの詳細については、「[依存関係レコードへのアクセス](#) (P.A-2) を参照してください。

アプリケーション ユーザの削除の次の作業

このユーザが Cisco Unity または Cisco Unity Connection で設定されていた場合、Cisco Unified Communications Manager の管理ページでユーザを削除すると、Cisco Unified Communications Manager とユーザとの関連付けが破棄されます。孤立したユーザは、Cisco Unity または Cisco Unity Connection の管理で削除できます。詳細については、該当する『*User Moves, Adds, and Changes Guide for Cisco Unity Connection*』を参照してください。Cisco Unity の詳細については、該当する『*System Administration Guide for Cisco Unity*』を参照してください。

GUI の使用方法

Cisco Unified Communications Manager の管理の Graphical User Interface (GUI; グラフィカル ユーザ インターフェイス) を使用してレコードを検索、削除、設定、またはコピーする方法については、「[Cisco Unified Communications Manager の管理アプリケーションでの操作](#)」(P.1-13) およびそのサブセクションを参照してください。GUI の使用方法とボタンおよびアイコンの機能の詳細が説明されています。

設定値表

表 87-1 では、アプリケーション ユーザの設定値について説明します。関連する手順については、「[関連項目](#)」(P.87-13) を参照してください。

表 87-1 アプリケーション ユーザの設定値

フィールド	説明
[アプリケーションユーザ情報 (Application User Information)]	
[ユーザ ID(User ID)]	アプリケーション ユーザの固有の識別名を入力します。Cisco Unified Communications Manager では、既存のユーザ ID を変更できます (LDAP サーバとの同期化を使用可能にしていない場合)。英数字 (a ~ z, A ~ Z, 0 ~ 9)、ダッシュ (-)、アンダースコア (_)、またはスペース () を入力することができます。
[パスワード (Password)]	アプリケーション ユーザ パスワードとなる英数字または特殊文字を入力します。割り当てられたクレデンシャル ポリシーで指定されている、最小文字数以上を入力する必要があります。
[パスワードの確認 (Confirm Password)]	ユーザ パスワードをもう一度入力します。
[ダイジェスト信用証明書 (Digest Credentials)]	一連の英数字を入力します。Cisco Unified Communications Manager は、ここで指定したダイジェスト信用証明書を使用して、SIP トランクの確認中に SIP ユーザ エージェントの応答を検証します。 ダイジェスト認証の詳細については、『 <i>Cisco Unified Communications Manager セキュリティ ガイド</i> 』を参照してください。
[ダイジェスト信用証明書の確認 (Confirm Digest Credentials)]	ダイジェスト信用証明書を正しく入力したことを確認するために、このフィールドにその信用証明書を入力します。
[クレデンシャルの編集 (Edit Credential)]	[クレデンシャルの編集 (Edit Credential)] ボタンは、このユーザをデータベースに追加した後で表示されます。 このユーザのクレデンシャルを管理するには、このボタンをクリックします。「 アプリケーション ユーザのクレデンシャルの管理 」(P.87-9) を参照してください。

表 87-1 アプリケーションユーザの設定値 (続き)

フィールド	説明
[プレゼンスグループ (Presence Group)]	<p>このフィールドには、プレゼンス機能を設定します。</p> <p>(注) このアプリケーションユーザをプレゼンスで使わない場合は、プレゼンスグループをデフォルト ([None]) 設定のままにします。</p> <p>ドロップダウンリストボックスから、アプリケーションユーザ用のプレゼンスグループを選択します。選択したグループによって、アプリケーションユーザ (IPMASysUser など) が監視できる対象が指定されます。</p> <p>インストール時に、標準のプレゼンスグループが設定されます。Cisco Unified Communications Manager の管理ページで設定されたプレゼンスグループもドロップダウンリストボックスに表示されます。</p> <p>プレゼンス許可は、プレゼンスグループと連携して、グループ間のプレゼンス要求を許可またはブロックします。グループ間の権限の設定の詳細については、『Cisco Unified Communications Manager 機能およびサービスガイド』の「プレゼンス」の章を参照してください。</p>
[プレゼンスの SUBSCRIBE の許可 (Accept Presence Subscription)]	<p>このフィールドには、プレゼンス許可用のプレゼンス機能を設定します。</p> <p>トランクに適用される [SIP トランクセキュリティプロファイルの設定 (SIP Trunk Security Profile Configuration)] で、アプリケーションレベルの認可を使用可能にした場合は、Cisco Unified Communications Manager がアプリケーションレベルの認可を行います。</p> <p>Cisco Unified Communications Manager がこの SIP トランクアプリケーションユーザからのプレゼンス要求を受け入れることができるようにするには、このチェックボックスをオンにします。</p> <p>[アプリケーションユーザの設定 (Application User Configuration)] ウィンドウでこのチェックボックスをオンにしたが、トランクに適用される [SIP トランクセキュリティプロファイルの設定 (SIP Trunk Security Profile Configuration)] で [アプリケーションレベル認証を有効化 (Enable Application Level Authorization)] チェックボックスをオンにしていない場合は、Cisco Unified Communications Manager によって、トランクに接続されている SIP ユーザエージェントに 403 エラーメッセージが送信されます。</p> <p>認可の詳細については、『Cisco Unified Communications Manager セキュリティガイド』を参照してください。</p>

表 87-1 アプリケーション ユーザの設定値 (続き)

フィールド	説明
[Out-of-Dialog REFER の許可 (Accept Out-of-Dialog REFER)]	<p>トランクに適用される [SIP トランクセキュリティプロファイルの設定 (SIP Trunk Security Profile Configuration)] で、アプリケーションレベルの認可を使用可能にした場合は、Cisco Unified Communications Manager がアプリケーションレベルの認可を行います。</p> <p>Cisco Unified Communications Manager がこの SIP トランク アプリケーション ユーザからの Out-of-Dialog REFER 要求を受け入れることができるようにするには、このチェックボックスをオンにします。たとえば、SIP で開始される転送機能や他の高度な転送関連機能を使用するには、Cisco Unified Communications Manager がこのアプリケーション ユーザの着信 Out-of-Dialog REFER 要求を受け入れることができるようにする必要があります。</p> <p>[アプリケーションユーザの設定 (Application User Configuration)] ウィンドウでこのチェックボックスをオンにしたが、トランクに適用される [SIP トランクセキュリティプロファイルの設定 (SIP Trunk Security Profile Configuration)] で [アプリケーションレベル認証を有効化 (Enable Application Level Authorization)] チェックボックスをオンにしていない場合は、Cisco Unified Communications Manager によって、トランクに接続されている SIP ユーザ エージェントに 403 エラーメッセージが送信されます。</p> <p>認可の詳細については、『Cisco Unified Communications Manager セキュリティガイド』を参照してください。</p>
[Unsolicited NOTIFY の許可 (Accept Unsolicited Notification)]	<p>トランクに適用される [SIP トランクセキュリティプロファイルの設定 (SIP Trunk Security Profile Configuration)] で、アプリケーションレベルの認可を使用可能にした場合は、Cisco Unified Communications Manager がアプリケーションレベルの認可を行います。</p> <p>Cisco Unified Communications Manager がこの SIP トランク アプリケーション ユーザからの Unsolicited NOTIFY を受け入れることができるようにするには、このチェックボックスをオンにします。たとえば、Message Waiting Indication (MWI; メッセージ待機インディケータ) サポートを提供するには、Cisco Unified Communications Manager がこのアプリケーション ユーザの着信 Unsolicited NOTIFY を受け入れることができるようにする必要があります。</p> <p>[アプリケーションユーザの設定 (Application User Configuration)] ウィンドウでこのチェックボックスをオンにしたが、トランクに適用される [SIP トランクセキュリティプロファイルの設定 (SIP Trunk Security Profile Configuration)] で [アプリケーションレベル認証を有効化 (Enable Application Level Authorization)] チェックボックスをオンにしていない場合は、Cisco Unified Communications Manager によって、トランクに接続されている SIP ユーザ エージェントに 403 エラーメッセージが送信されます。</p> <p>認可の詳細については、『Cisco Unified Communications Manager セキュリティガイド』を参照してください。</p>

表 87-1 アプリケーション ユーザの設定値 (続き)

フィールド	説明
[Replacesヘッダーの許可 (Accept Replaces Header)]	<p>トランクに適用される [SIP トランクセキュリティプロファイルの設定 (SIP Trunk Security Profile Configuration)] で、アプリケーションレベルの認可を使用可能にした場合は、Cisco Unified Communications Manager がアプリケーションレベルの認可を行います。</p> <p>Cisco Unified CM がこの SIP トランク アプリケーション ユーザからのメッセージのヘッダー置換を受け入れることができるようにするには、このチェックボックスをオンにします。たとえば、SIP トランク上の外部コールを、在席転送の場合と同様に、外部のデバイスまたは相手に転送するには、このアプリケーション ユーザの REFER および INVITE 内に Replaces ヘッダーを含む SIP 要求を Cisco Unified CM が受け入れることができるようにする必要があります。</p> <p>[アプリケーションユーザの設定 (Application User Configuration)] ウィンドウでこのチェックボックスをオンにしたが、トランクに適用される [SIP トランクセキュリティプロファイルの設定 (SIP Trunk Security Profile Configuration)] で [アプリケーションレベル認証を有効化 (Enable Application Level Authorization)] チェックボックスをオンにしていない場合は、Cisco Unified CM によって、トランクに接続されている SIP ユーザ エージェントに 403 エラー メッセージが送信されます。</p> <p>認可の詳細については、『Cisco Unified Communications Manager セキュリティガイド』を参照してください。</p>
[デバイス情報 (Device Information)]	
[使用可能なデバイス (Available Devices)]	<p>このリスト ボックスには、このアプリケーション ユーザとの関連付けに使用できるデバイスが表示されます。</p> <p>デバイスをこのアプリケーション ユーザに関連付けるには、デバイスを選択し、このリスト ボックスの下にある下矢印をクリックします。</p> <p>このアプリケーション ユーザに関連付けるデバイスがこのペインに表示されない場合は、次のボタンのいずれかをクリックして、他のデバイスを検索します。</p> <ul style="list-style-type: none"> • [別の電話を検索 (Find more Phones)] : このアプリケーション ユーザに関連付ける他の電話機を検索する場合は、このボタンをクリックします。電話機を検索するための [電話の検索と一覧表示 (Find and List Phones)] ウィンドウが表示されます。 • [別のルートポイントを検索 (Find more Route Points)] : このアプリケーション ユーザに関連付ける他のルート ポイントを検索する場合は、このボタンをクリックします。Computer Telephony Integration (CTI; コンピュータ/テレフォニー インテグレーション) ルート ポイントを検索するための [CTI ルートポイントの検索と一覧表示 (Find and List CTI Route Points)] ウィンドウが表示されます。 • [別のパイロットポイントを検索 (Find more Pilot Points)] : このアプリケーション ユーザに関連付ける他のパイロット ポイントを検索する場合は、このボタンをクリックします。パイロット ポイントを検索するための [パイロットポイントの検索と一覧表示 (Find and List Pilot Points)] ウィンドウが表示されます。
[制御するデバイス (Controlled Devices)]	<p>このフィールドには、アプリケーション ユーザに関連付けられているデバイスのリストが表示されます。デバイスを削除するには、デバイス名を選択し、このリスト ボックスの上にある上矢印をクリックします。デバイスを追加するには、[使用可能なデバイス (Available Devices)] リスト ボックスでデバイスを選択し、下矢印をクリックします。</p>

表 87-1 アプリケーション ユーザの設定値 (続き)

フィールド	説明
[CAPF 情報 (CAPF Information)]	
[割り当てられている CAPF プロファイル (Associated CAPF Profiles)]	<p>このペインには、このユーザ用に設定した CAPF プロファイルのインスタンス ID が表示されます。プロファイルを表示または更新するには、インスタンス ID をダブルクリックするか、インスタンス ID をクリックして選択してから [詳細の表示 (View Details)] をクリックします。[アプリケーションユーザ CAPF プロファイルの設定 (Application User CAPF Profile Configuration)] ウィンドウが表示され、現在の設定が表示されます。</p> <p>アプリケーション ユーザ CAPF プロファイルの設定方法については、『Cisco Unified Communications Manager セキュリティ ガイド』を参照してください。</p>
[権限情報 (Permissions Information)]	
[グループ (Groups)]	<p>このリスト ボックスは、アプリケーション ユーザ レコードが保存された後で表示されます。このリスト ボックスには、アプリケーション ユーザが属するグループが表示されます。</p> <p>ユーザを 1 つ以上のグループに追加するには、[ユーザグループに追加 (Add to User Group)] ボタンをクリックします。[ユーザグループの検索と一覧表示 (Find and List User Groups)] ウィンドウが別ウィンドウで表示されます。ユーザを追加するグループを見つけて、そのグループの横にあるチェックボックスをオンにします。次に、ウィンドウの下部にある [選択項目の追加 (Add Selected)] をクリックします。[ユーザグループの検索と一覧表示 (Find and List User Groups)] ウィンドウが閉じ、[アプリケーションユーザの設定 (Application User Configuration)] ウィンドウが表示され、選択したグループが [グループ (Groups)] リスト ボックスに表示されます。</p> <p>グループからユーザを削除するには、[グループ (Groups)] リスト ボックスでグループを選択し、[ユーザグループから削除 (Remove from User Group)] ボタンをクリックします。</p> <p>グループを表示または更新するには、グループ名をダブルクリックするか、グループ名をクリックして選択してから [詳細の表示 (View Details)] をクリックします。[ユーザグループの設定 (User Group Configuration)] ウィンドウが表示され、現在の設定が表示されます。</p> <p>ユーザ グループの検索および設定の詳細については、「ユーザ グループの設定 (P.90-1)」を参照してください。</p>
[権限 (Roles)]	<p>このリスト ボックスは、アプリケーション ユーザが追加され、[グループ (Groups)] リスト ボックスにデータが入力され、ユーザ レコードが保存された後で表示されます。このリスト ボックスには、アプリケーション ユーザに割り当てられている権限が表示されます。</p> <p>権限を表示または更新するには、権限名をダブルクリックするか、権限名をクリックして選択してから [詳細の表示 (View Details)] をクリックします。[権限の設定 (Role Configuration)] ウィンドウが表示され、現在の設定が表示されます。</p> <p>権限を設定する方法の詳細については、「権限の設定 (P.89-1)」を参照してください。</p>

追加情報

「[関連項目 \(P.87-13\)](#)」を参照してください。

Cisco Unity または Cisco Unity Connection への管理者ユーザの追加

[Application Configuration(アプリケーションの設定)] ウィンドウにある [Cisco Unityアプリケーションユーザの作成(Create Cisco Unity Application User)] リンクを使用すると、ユーザを管理者ユーザとして Cisco Unity または Cisco Unity Connection に追加することができます。この方法を使用して、アプリケーションユーザを Cisco Unified Communications Manager の管理ページで設定してから、そのユーザの追加設定を Cisco Unity または Cisco Unity Connection の管理で設定します。

Cisco Unified Communications Manager を Cisco Unity Connection 7.x に統合する場合は、この項で説明している手順を実行する代わりに、Cisco Unity Connection 7.x で使用可能なインポート機能を使用することができます。インポート機能の使用の詳細については、『*User Moves, Adds, and Changes Guide for Cisco Unity Connection 7.x*』を参照してください。

[Cisco Unityユーザの作成(Create Cisco Unity User)] リンクが表示されるのは、該当する Cisco Unity または Cisco Unity Connection ソフトウェアのインストールと設定を行った場合だけです。該当する『*Cisco Unified Communications Manager Integration Guide for Cisco Unity*』または『*Cisco Unified Communications Manager SCCP Integration Guide for Cisco Unity Connection*』を参照してください。

始める前に

Cisco Unity または Cisco Unity Connection にプッシュするユーザの適切なテンプレートを定義していることを確認します。Cisco Unity Connection ユーザの場合は、該当する『*User Moves, Adds, and Changes Guide for Cisco Unity Connection*』を参照してください。Cisco Unity ユーザの場合は、『*System Administration Guide for Cisco Unity*』を参照してください。

手順

-
- ステップ 1** アプリケーション ユーザを検索します。
 - ステップ 2** [関連リンク (Related Links)] ドロップダウン リスト ボックスから [Cisco Unityアプリケーションユーザの作成(Create Cisco Unity Application User)] リンクを選択し、[移動(Go)] をクリックします。
[Cisco Unity ユーザの追加 (Add Cisco Unity User)] ダイアログボックスが表示されます。
 - ステップ 3** [アプリケーションサーバ (Application Server)] ドロップダウン リスト ボックスから、Cisco Unity ユーザまたは Cisco Unity Connection ユーザを作成する Cisco Unity サーバまたは Cisco Unity Connection サーバを選択し、[次へ (Next)] をクリックします。
 - ステップ 4** [アプリケーションユーザテンプレート (Application User Template)] ドロップダウン リスト ボックスから、使用するテンプレートを選択します。
 - ステップ 5** [保存(Save)] をクリックします。

管理者アカウントが Cisco Unity または Cisco Unity Connection に作成されます。[アプリケーションユーザの設定 (Application User Configuration)] ウィンドウで、[関連リンク (Related Links)] 内のリンクが [Cisco Unity ユーザの編集 (Edit Cisco Unity User)] に変わります。これで、Cisco Unity システム管理または Cisco Unity Connection の管理で作成したユーザが表示されるようになります。



(注) Cisco Unity ユーザまたは Cisco Unity Connection ユーザが Cisco Unified CM アプリケーション ユーザと統合された場合、Cisco Unity システム管理または Cisco Unity Connection の管理では [エイリアス] (Cisco Unified Communications Manager の管理ページの [ユーザ ID(User ID)])、[名]、[姓]、[内線] (Cisco Unified Communications Manager の管理ページの [プライマリ内線(Primary Extension)]) の各フィールドを編集できません。これらのフィールドは、Cisco Unified Communications Manager の管理ページだけで更新できます。



(注) Cisco Unity および Cisco Unity Connection は、Cisco Unified Communications Manager からのデータの同期を監視します。Cisco Unity システム管理または Cisco Unity Connection の管理の [ツール] メニューで、同期時間を設定できます。詳細については、Cisco Unity Connection の場合は、該当する『*User Moves, Adds, and Changes Guide for Cisco Unity Connection*』を参照してください。Cisco Unity の場合は、『*System Administration Guide for Cisco Unity*』を参照してください。

追加情報

「関連項目」(P.87-13) を参照してください。

アプリケーション ユーザのパスワードの変更

アプリケーション ユーザのパスワードを変更する手順は、次のとおりです。

手順

- ステップ 1** パスワードを変更するアプリケーション ユーザを見つけます。
[アプリケーション ユーザの設定 (Application User Configuration)] ウィンドウに、選択したアプリケーション ユーザの情報が表示されます。
- ステップ 2** [パスワード (Password)] フィールドで、暗号化されている既存のパスワードをダブルクリックし、新しいパスワードを入力します。
- ステップ 3** [パスワードの確認 (Confirm Password)] フィールドで、暗号化されている既存のパスワードをダブルクリックし、新しいパスワードをもう一度入力します。
- ステップ 4** [保存 (Save)] をクリックします。

追加情報

「関連項目」(P.87-13) を参照してください。

アプリケーション ユーザのクレデンシャルの管理

アプリケーション ユーザのクレデンシャル（関連付けられた認証ルール、関連付けられたクレデンシャル ポリシー、パスワードの最終変更時間など）を変更または表示する手順は、次のとおりです。ユーザのクレデンシャルを編集できるのは、ユーザがデータベースに存在している場合だけです。

[クレデンシャル設定 (Credential Configuration)] ウィンドウでは、割り当てられたクレデンシャル ポリシーと衝突する設定を保存することができません。たとえば、ポリシーで [無期限 (Never Expires)] チェックボックスがオンの場合、[クレデンシャル設定 (Credential Configuration)] ウィンドウで [無期限にする (Does Not Expire)] チェックボックスをオフにして保存することはできません。ただし、[無期限 (Never Expires)] ポリシー設定がオンでない場合、ユーザに別のクレデンシャル期限を設定することはできます ([無期限にする (Does Not Expire)] を含む)。この場合、ユーザ設定がポリシー設定よりも優先されます。

[クレデンシャル設定 (Credential Configuration)] ウィンドウの他の設定と衝突する、[クレデンシャル設定 (Credential Configuration)] ウィンドウの設定変更はできません。たとえば、[ユーザは変更不可 (User Cannot Change)] ボックスがオンの場合は、[ユーザ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オンにできません。

[クレデンシャル設定 (Credential Configuration)] ウィンドウには、イベントのおよその回数が表示されます。このフォームは、次に認証クエリーまたはイベントが発生したときに更新されます。

始める前に

データベースにアプリケーション ユーザを作成します。「[アプリケーション ユーザの設定値](#)」(P.87-1) を参照してください。

手順

-
- ステップ 1** [アプリケーションユーザの検索と一覧表示 (Find and List Application Users)] ウィンドウを使用して、アプリケーション ユーザの設定を検索します ([ユーザ管理 (User Management)] > [アプリケーション ユーザ (Application User)])。
- [アプリケーションユーザの設定 (Application User Configuration)] ウィンドウに、設定情報が表示されます。
- ステップ 2** パスワード情報を変更または表示するには、[パスワード (Password)] フィールドの横にある [クレデンシャルの編集 (Edit Credential)] ボタンをクリックします。[クレデンシャル設定 (Credential Configuration)] ウィンドウが表示されます。
- ステップ 3** ユーザのクレデンシャル データを表示するか、適切な設定値を入力します (表 87-2 を参照)。
- ステップ 4** 設定値を変更した場合は、[保存 (Save)] をクリックします。
-

追加情報

「[関連項目](#)」(P.87-13) を参照してください。

クレデンシャルの設定値とフィールド

表 87-2 では、アプリケーション ユーザおよびエンド ユーザのクレデンシャルの設定値について説明します。これらの設定値は、アプリケーション ユーザまたはエンド ユーザのダイジェスト信用証明書には適用されません。関連する手順については、「[関連項目](#)」(P.87-13) を参照してください。

表 87-2 アプリケーション ユーザおよびエンド ユーザのクレデンシャルの設定値とフィールド

フィールド	説明
[管理者によるロック (Locked by Administrator)]	<p>このアカウントをロックし、ユーザがアクセスできないようにするには、このチェックボックスをオンにします。</p> <p>アカウントのロックを解除し、ユーザがアクセスできるようにするには、このチェックボックスをオフにします。</p> <p>このチェックボックスは、クレデンシャル ポリシーでこのアカウント タイプに [管理者がロック解除を行う (Administrator Must Unlock)] が指定され、アカウントのロックアウトが発生した後で使用します。</p>
[ユーザは変更不可 (User Cannot Change)]	<p>ユーザがこのクレデンシャルを変更できないようにするには、このチェックボックスをオンにします。このオプションは、グループ アカウントに対して使用します。</p> <p>[ユーザは次回ログイン時に変更する必要あり (User Must Change at Next Login)] チェックボックスがオンになっている場合は、このチェックボックスをオンにできません。</p>
[ユーザは次回ログイン時に変更する必要あり (User Must Change at Next Login)]	<p>次のログイン時に、このクレデンシャルの変更をユーザに要求するには、このチェックボックスをオンにします。このオプションは、一時的なクレデンシャルを割り当てた後で使用します。</p> <p>[ユーザは変更不可 (User Cannot Change)] チェックボックスがオンになっている場合は、このチェックボックスをオンにできません。</p>
[無期限にする (Does Not Expire)]	<p>このクレデンシャルの変更をユーザに要求しないようにするには、このチェックボックスをオンにします。このオプションは、セキュリティの低いユーザまたはグループ アカウントに使用できます。</p> <p>オンにしても、ユーザはいつでもこのクレデンシャルを変更できます。このチェックボックスがオフの場合、関連付けられているクレデンシャル ポリシーの有効期限の設定が適用されます。</p> <p>ポリシー設定で [無期限 (Never Expires)] が指定されている場合は、このチェックボックスをオフにできません。</p>
[ハック数のリセット (Reset Hack Count)]	<p>このユーザのハック数をリセットして、[失敗したログイン試行によりロックされた時間 (Time Locked Due to Failed Logon Attempts)] フィールドをクリアするには、このチェックボックスをオンにします。</p> <p>ハック数は、クレデンシャルが不正なために認証に失敗すると増えます。</p> <p>ポリシーで [ログイン失敗無制限 (No Limit for Failed Logons)] が指定されている場合、ハック数は常に 0 になります。</p>
[認証ルール (Authentication Rule)]	このユーザのクレデンシャルに適用するクレデンシャル ポリシーを選択します。
[最終変更時間 (Time Last Changed)]	このフィールドには、このユーザのクレデンシャルが変更された最新の日時が表示されます。
[失敗したログイン試行 (Failed Logon Attempts)]	このフィールドには、成功した最終ログイン、管理者によるこのユーザ クレデンシャルのハック数のリセット、または失敗したログイン試行回数のリセット期間経過の後、失敗したログイン試行回数が表示されます。

表 87-2 アプリケーション ユーザおよびエンド ユーザのクレデンシャルの設定値とフィールド (続き)

フィールド	説明
[失敗した最後のログイン試行時間 (Time of Last Failed Logon Attempt)]	このフィールドには、このユーザのクレデンシャルでログイン試行が失敗した最新の日時が表示されます。
[管理者によりロックされた時間 (Time Locked by Administrator)]	このフィールドには、管理者がこのユーザ アカウントをロックした日時が表示されます。管理者がクレデンシャルのロックを解除すると、このフィールドはブランクになります。
[失敗したログイン試行によりロックされた時間 (Time Locked Due to Failed Logon Attempts)]	このフィールドには、失敗したログイン試行によってユーザ アカウントがロックされた最新の日時が表示されます。ハック ロックアウトの時間は、失敗したログイン試行回数が、適用されているクレデンシャル ポリシーで設定されているしきい値を超えると設定されます。

アプリケーション ユーザとデバイスとの関連付け

アプリケーション ユーザにデバイスを関連付け、アプリケーション ユーザがそのデバイスのコントロール権を持つようにすることができます。電話機などの一部のデバイスは、アプリケーション ユーザが制御できます。CTI ポートなどのその他のデバイスは、ユーザとして指定されるアプリケーションによって制御できます。アプリケーション ユーザが電話機のコントロール権を持つ場合、その電話機の特定の設定値（たとえば、スピードダイヤルや自動転送）を制御できます。

始める前に

アプリケーション ユーザにデバイスを割り当てるには、そのユーザの [アプリケーションユーザの設定 (Application User Configuration)] ウィンドウにアクセスする必要があります。[アプリケーションユーザの検索と一覧表示 (Find and List Application Users)] ウィンドウ ([ユーザ管理 (User Management)] > [アプリケーションユーザ (Application User)]) を使用して、アプリケーションユーザを検索します。[アプリケーションユーザの設定 (Application User Configuration)] ウィンドウが表示された後で、デバイスを割り当てる手順は、次のとおりです。

手順

- ステップ 1** [使用可能なデバイス (Available Devices)] リスト ボックスで、アプリケーション ユーザに関連付けるデバイスを選択し、リスト ボックスの下にある下矢印をクリックします。選択したデバイスは、[制御するデバイス (Controlled Devices)] リストボックスに移動します。
- ステップ 2** 使用可能なデバイスのリストを制限するには、[別の電話を検索 (Find more Phones)] ボタン、[別のルートポイントを検索 (Find more Route Points)] ボタン、または [別のパイロットポイントを検索 (Find more Pilot Points)] ボタンをクリックします。
 - [別の電話を検索 (Find more Phones)] ボタンをクリックすると、[電話の検索と一覧表示 (Find and List Phones)] ウィンドウが表示されます。検索を行って、このアプリケーション ユーザに関連付ける電話機を見つけます。
 - [別のルートポイントを検索 (Find more Route Points)] ボタンをクリックすると、[CTI ルートポイントの検索と一覧表示 (Find and List CTI Route Points)] ウィンドウが表示されます。検索を行って、このアプリケーション ユーザに関連付ける CTI ルートポイントを見つけます。
 - [別のパイロットポイントを検索 (Find more Pilot Points)] ボタンをクリックすると、[パイロットポイントの検索と一覧表示 (Find and List Pilot Points)] ウィンドウが表示されます。検索を行って、このアプリケーション ユーザに関連付けるパイロットポイントを見つけます。

- ステップ 3** アプリケーション ユーザに割り当てるデバイスごとに、前述のステップを繰り返します。
- ステップ 4** 割り当てを完了したら、[保存(Save)] をクリックして、アプリケーション ユーザにデバイスを割り当てます。

追加情報

「関連項目」(P.87-13) を参照してください。

関連項目

- 「アプリケーション ユーザの設定値」(P.87-1)
- 「Cisco Unity または Cisco Unity Connection への管理者ユーザの追加」(P.87-8)
- 「アプリケーション ユーザのパスワードの変更」(P.87-9)
- 「アプリケーション ユーザのクレデンシャルの管理」(P.87-9)
- 「クレデンシャルの設定値とフィールド」(P.87-11)
- 「アプリケーション ユーザとデバイスとの関連付け」(P.87-12)
- 「エンド ユーザの設定値」(P.88-1)
- 「Cisco Unity Connection ボイスメールボックスの作成」(P.88-9)
- 「エンド ユーザのパスワードの変更」(P.88-10)
- 「エンド ユーザの PIN の変更」(P.88-11)
- 「エンド ユーザのクレデンシャルの管理」(P.88-11)
- 「クレデンシャルの設定値とフィールド」(P.88-12)
- 「エンド ユーザのユーザ関連情報の設定」(P.88-13)
- 「エンド ユーザとデバイスとの関連付け」(P.88-15)
- 「Cisco エクステンション モビリティ プロファイルの関連付け」(P.88-17)
- 「LDAP システムの設定」(P.11-1)
- 「権限の設定」(P.89-1)
- 「ユーザ グループの設定」(P.90-1)
- 「ユーザの権限、ユーザ グループ、およびアクセス権の表示」(P.90-8)
- 「電話番号の設定」(P.43-1)
- 「CTI ルート ポイントの設定」(P.64-1)
- 「Cisco Unified IP Phone の設定」(P.67-1)
- 「クレデンシャル ポリシーの設定」(P.86-1)
- 「クレデンシャル ポリシーのデフォルトの設定」(P.85-1)
- 『Cisco Unified Communications Manager システム ガイド』の「クレデンシャル ポリシー」
- 『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 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」

- 『*Cisco Unified Communications Manager システム ガイド*』の「[デバイスの関連付け](#)」
- 『*Cisco Unified Communications Manager 機能およびサービス ガイド*』の「[ユーザへのユーザ デバイス プロファイルの関連付け](#)」
- 『*Cisco Unified Communications Manager 機能およびサービス ガイド*』の「[プロキシ回線サポートのある Cisco Unified Communications Manager Assistant](#)」
- 『*Cisco Unified Communications Manager 機能およびサービス ガイド*』の「[シェアドライン サポートのある Cisco Unified Communications Manager Assistant](#)」
- 『*Cisco Unified Communications Manager システム ガイド*』の「[Cisco Unity メッセージングの連動](#)」
- 『*Cisco Unified Communications Manager 機能およびサービス ガイド*』の「[プレゼンス](#)」

関連資料

- 『*Cisco Unified Communications Manager セキュリティ ガイド*』
- 『*User Moves, Adds, and Changes Guide for Cisco Unity Connection*』
- 『*System Administration Guide for Cisco Unity*』