



アプリケーション ユーザの設定

Cisco Unified Presence の管理ページにある [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、管理者は、Cisco Unified Presence アプリケーション ユーザに関する情報の追加、検索、表示、および保守を行うことができます。

次のトピックには、アプリケーション ユーザ情報の管理に関する情報が含まれています。

- [アプリケーションユーザの検索 \(P.39-2\)](#)
- [アプリケーションユーザの設定 \(P.39-3\)](#)
- [アプリケーションユーザの設定値 \(P.39-4\)](#)
- [アプリケーションユーザパスワードの変更 \(P.39-6\)](#)
- [アプリケーションユーザの信用証明書情報の管理 \(P.39-7\)](#)
- [アプリケーションユーザの信用証明書の設定値およびフィールド \(P.39-8\)](#)

追加情報

P.39-9 の「[関連項目](#)」を参照してください。

アプリケーションユーザの検索

ネットワークにアプリケーションユーザが複数存在する場合があります。Cisco Unified Presence では、具体的な検索条件に基づいて特定のアプリケーションユーザを検索することができます。特定のアプリケーションユーザを検索するには、次の手順を実行します。



(注)

ブラウザセッションでの作業中、Cisco Unified Presence の管理ページにより、アプリケーションユーザ検索の設定が保存されます。他のメニュー項目に移動してからこのメニューに戻ると、検索の設定を変更するか、またはブラウザを閉じるまで、アプリケーションユーザ検索の設定が維持されます。

手順

ステップ 1 [ユーザ管理] > [アプリケーションユーザ] の順に選択します。

[アプリケーションユーザの検索と一覧表示 (Find and List Application Users)] ウィンドウが表示されます。アクティブ (優先) クエリーのレコードもウィンドウに表示される場合があります。

ステップ 2 データベースのすべてのレコードを検索するには、ダイアログボックスが空であることを確認して、**ステップ 3**に進みます。

レコードをフィルタリングするかまたは検索します。

- 最初のドロップダウンリストボックスから検索パラメータを選択します。
- 2 番目のドロップダウンリストボックスから検索パターンを選択します。
- 必要に応じて適切な検索テキストを指定します。



(注)

検索条件を追加するには、[+] ボタンをクリックします。検索条件を追加すると、指定したすべての検索条件に一致するレコードが検索されます。検索条件を削除するには、[-] ボタンをクリックして最後に追加した検索条件を削除するか、[フィルタのクリア] ボタンをクリックして追加したすべての検索条件を削除します。

ステップ 3 [検索] をクリックします。

一致するすべてのレコードが表示されます。[ページあたりの行数] ドロップダウンリストボックスで異なる値を選択すると、各ウィンドウに表示する項目の数を変更できます。



(注)

対象のレコードの隣にあるチェックボックスをオンにしてから [選択項目の削除] をクリックすると、複数のレコードをデータベースから削除できます。[すべてを選択] をクリックしてから [選択項目の削除] をクリックすると、この選択で設定可能なすべてのレコードを削除できます。

ステップ 4 表示されるレコードのリストから、表示対象となるレコードのリンクをクリックします。



(注) ソート順序を逆にするには、必要に応じて、リストのヘッダーにある上向きまたは下向きの矢印をクリックします。

選択した項目がウィンドウに表示されます。

追加情報

P.39-9 の「関連項目」を参照してください。

アプリケーション ユーザの設定

ユーザを追加するには、次の手順に従います。

手順

ステップ 1 [ユーザ管理] > [アプリケーションユーザ] の順に選択します。

[アプリケーションユーザの検索と一覧表示 (Find and List Application Users)] ウィンドウが表示されます。2 つのドロップダウン リスト ボックスを使用してアプリケーション ユーザを検索します。

ステップ 2 [新規追加] をクリックします。

[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ます。

ステップ 3 表 39-1 の説明に従って適切な設定を入力します。

ステップ 4 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] 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] を選択し、[移動] 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レポートを表示した後は、このユーザの [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] 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] を選択し、[移動] をクリックします。

ステップ 5 ユーザ情報を入力したら、[保存] をクリックして変更を保存し、ユーザを追加します。

追加情報

P.39-9 の「関連項目」を参照してください。

アプリケーション ユーザの設定値

表 39-1 で、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、P.39-9 の「[関連項目](#)」を参照してください。

表 39-1 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 ユーザの識別名を入力します。使用できる特殊文字は、ダッシュ (-)、アンダースコア (_)、二重引用符 (") および空白文字です。
パスワード (Password)	英数字または特殊文字を使ってアプリケーション ユーザのパスワードを入力します。割り当てられている信用証明書ポリシーに指定されている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 パスワードを再入力します。
ダイジェスト信用証明書 (Digest Credentials)	ダイジェスト認証中に Cisco Unified Presence を UAS として動作させる場合、このフィールドで指定するダイジェスト信用証明書をチャレンジに使用します。英数字の文字列を入力します。
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の入力が正しいことを確認するために、このフィールドに再度信用証明書を入力します。
クレデンシャルの編集 (Edit Credential)	ユーザをデータベースに追加すると、[クレデンシャルの編集] ボタンが表示されます。 このボタンをクリックして、このユーザの信用証明書情報を管理します。P.39-7 の「 アプリケーション ユーザの信用証明書情報の管理 」を参照してください。
プレゼンスグループ (Presence Group)	ドロップダウン リスト ボックスから、アプリケーション ユーザの [プレゼンスグループ (Presence Group)] を選択します。 インストール時は、Standard Presence Group が設定されています。Cisco Unified Presence の管理ページで設定したプレゼンス 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。

表 39-1 アプリケーションユーザの設定値 (続き)

フィールド	説明
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のレコードが保存された後に表示されます。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 つ以上のユーザ グループに追加するには、[ユーザグループに追加] 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)] ウィンドウが別のウィンドウとして表示されます。ユーザを追加するグループを特定し、それらのグループの隣のチェックボックスをオンにしてから、ウィンドウの下部にある [選択項目の追加] 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 ボックスで対象のグループを強調表示し、[ユーザグループから削除] 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強調表示してから [詳細の表示] をクリックします。現在の設定で [ユーザグループの設定 (User Group Configuration)] ウィンドウが表示されます。</p> <p>ユーザ グループの検索と設定の詳細については、P.41-1 の「ユーザグループの設定」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を追加した後、[グループ (Groups)] リスト ボックスに値を読み込んだ後、およびユーザレコードを削除した後に表示されます。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強調表示してから [詳細の表示] をクリックします。現在の設定で [権限の設定 (Role Configuration)] ウィンドウが表示されます。</p> <p>権限の設定の詳細については、P.40-1 の「権限の設定」を参照してください。</p>

追加情報

[P.39-9 の「関連項目」](#)を参照してください。

アプリケーション ユーザ パスワードの変更

アプリケーションユーザ パスワードを変更するには、次の手順に従います。

手順

ステップ 1 P.39-2 の「[アプリケーションユーザの検索](#)」の手順に従い、パスワードを変更する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)] ウィンドウに、選択したアプリケーションユーザに関する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再入力します。

ステップ 4 [保存] をクリックします。

追加情報

P.39-9 の「[関連項目](#)」を参照してください。

アプリケーションユーザの信用証明書情報の管理

関連付けられた認証ルール、関連付けられた信用証明書ポリシー、アプリケーションユーザの直前のパスワード変更の時刻など、信用証明書の情報を変更または表示するには、次の手順を実行します。ユーザの信用証明書は、データベースにユーザが存在している場合のみ編集できます。

ユーザの [クレデンシャル設定] ウィンドウで割り当てられた信用証明書ポリシーと競合する設定は保存できません。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になっている場合は、[クレデンシャル設定] 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、[無期限にする (Does Not Expire)] を含む、別の信用証明書をユーザに設定することはできます。ポリシーの [無期限にする (Never Expires)] の設定がオンになっていないと、ポリシーの設定はユーザの設定により上書きされます。

ユーザの [クレデンシャル設定] ウィンドウで、他の設定と競合する設定は変更できません。たとえば、[ユーザは変更不可 (User Cannot Change)] チェックボックスがオンの場合、[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することはできません。

信用証明書の設定のウィンドウで報告されるイベント時間は、おおよその時間と考えてください。システムでは、次の認証クエリまたはイベントの時点でこのフォームが更新されます。

開始する前に

データベースにアプリケーションユーザを作成します。P.39-3 の「アプリケーションユーザの設定」を参照してください。

手順

-
- ステップ 1** P.39-2 の「アプリケーションユーザの検索」の手順に従って、アプリケーションユーザの設定を検索します。

[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)] フィールドの隣にある [クレデンシャルの編集 (Edit Credential)] ボタンをクリックします。ユーザの [クレデンシャル設定] ウィンドウが表示されます。

- ステップ 3** ユーザの信用証明書のデータを表示するか、表 39-2 の該当する設定を入力します。

- ステップ 4** 設定を変更した場合は、[保存] をクリックします。
-

追加情報

P.39-9 の「関連項目」を参照してください。

アプリケーションユーザの信用証明書の設定値およびフィールド

表 39-2 で、アプリケーションユーザの信用証明書の設定値について説明します。これらの設定は、アプリケーション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、P.39-9 の「関連項目」を参照してください。

表 39-2 アプリケーションユーザの信用証明書の設定値およびフィールド

フィールド	説明
管理者によるロック (Locked By Administrator)	<p>このチェックボックスをオンにすると、このアカウントはロックされ、このユーザへのアクセスが拒否されます。</p> <p>このチェックボックスをオフにすると、アカウントのロックが解除され、このユーザへのアクセスが許可されます。</p> <p>このチェックボックスは、このアカウントタイプに対し、アカウントのロックアウト後に [管理者がロック解除を行う (Administrator Must Unlock)] を信用証明書のポリシーで指定する場合に使用します。</p>
ユーザは変更不可 (User Cannot Change)	<p>このチェックボックスをオンにすると、このユーザによるこの信用証明書の変更が拒否されます。このオプションはグループアカウントに使用します。</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)] がオンになっていると、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>このチェックボックスをオンにすると、ユーザは次回のログイン時にこの信用証明書を変更する必要があります。このオプションは、一時信用証明書を割り当てた後に使用してください。</p> <p>[ユーザは変更不可 (User Cannot Change)] がオンの場合は、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>このチェックボックスをオンにすると、システムユーザに対するこの信用証明書の変更要求が拒否されます。このオプションは、低セキュリティユーザまたはグループユーザに使用できます。</p> <p>このチェックボックスをオンにしても、ユーザはこの信用証明書をいつでも変更できます。チェックボックスをオフにした場合、関連付けられている信用証明書ポリシーの期限設定が適用されます。</p> <p>ポリシー設定で [無期限 (Does Not Expire)] を指定している場合は、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>このチェックボックスをオンにすると、このユーザのハックカウントがリセットされ、[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 Login Attempts)] フィールドがクリアされます。</p> <p>ハックカウントは、不正な信用証明書により認証が失敗するたびに増えていきます。</p> <p>ポリシーに [ログイン失敗無制限 (No Limit for Failed Logons)] が指定されている場合、ハックカウントは常に 0 になります。</p>

表 39-2 アプリケーションユーザの信用証明書の設定値およびフィールド (続き)

フィールド	説明
認証ルール (Authentication Rule)	このユーザ信用証明書を適用するための信用証明書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、このユーザの信用証明書が最後に変更された日付と時刻が表示されます。
失敗したログイン試行 (Failed Logon Attempts)	このフィールドには、最後の正常なログイン以降、管理者がこのユーザの信用証明書のハック カウントをリセットしたとき以降、または失敗したログイン試行の有効期限が切れてリセットされたとき以降、ログインが失敗した回数が表示されます。
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、このユーザの信用証明書で最後にログインに失敗した日付と時刻が表示されます。
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付と時刻が表示されます。管理者が信用証明書のロックを解除したら、このフィールドは空白になります。
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、ログイン試行に失敗したためにシステムが最後にこのユーザ アカウントをロックした日付と時刻が表示されます。失敗したログイン試行が、適用される信用証明書ポリシーで設定されているしきい値を超過するたびに、ハック ロックアウトの時間が設定されます。

関連項目

- [アプリケーションユーザの検索 \(P.39-2\)](#)
- [アプリケーションユーザの設定 \(P.39-3\)](#)
- [アプリケーションユーザの設定値 \(P.39-4\)](#)
- [アプリケーションユーザ パスワードの変更 \(P.39-6\)](#)
- [アプリケーションユーザの信用証明書情報の管理 \(P.39-7\)](#)
- [アプリケーションユーザの信用証明書の設定値およびフィールド \(P.39-8\)](#)

