CHAPTER 15

Web コンソール ユーザの管理

この章では、ACE Web Application Firewall ManagerWeb コンソール ユーザの管理方法について説明します。内容は次のとおりです。

コンソール ユーザについて

コンソールへのアクセスは、重要なネットワーク セキュリティ ポリシーの開発および監視地点として、厳重に保護する必要があります。認証されたユーザだけが ACE Web Application Firewall Manager Web コンソールにアクセスできます。Web コンソールでは、各ユーザ アカウントに一連の権限を割り当てることで、さらに制限が強化されます。ユーザが実行できる操作は、これらの権限によって決定されます。最後に、ACE Web Application Firewall Manager Web コンソールの各ユーザは、ACE Web Application Firewall Manager の管理者がアクセスを承認したサブポリシーだけを表示または編集できます。

コンソール管理者は、ユーザのタイプ、ロール、ポリシー アクセス権を正しく割り当てることで、ポリシーおよび設定の変更がそれを許可されたユーザだけによって行われることを保証できます。

ACE Web Application Firewall Manager Web コンソールにアクセスするには、まずユーザ名とパスワードの組み合わせを入力し、認証を受ける必要があります。ACE Web Application Firewall Manager は、認証されたユーザ ID に Web コンソールでの一連の権限を対応付けます。次の項では、ACE Web Application Firewall Manager がサポートする認証および認可スキームと、それらを使用するための設定方法について説明します。

Web コンソール ユーザのタイプ

ACE Web Application Firewall Manager Web コンソールでは、複数のユーザ タイプが規定されています。管理者ユーザは最も広範囲な権限を持ち、外部開発者の権限は最も小さくなります。ただし、ユーザが実行できる個々の操作は、ユーザのロールの機能と、特定のポリシーに関連付けられたアクセス権限です。たとえば、コンソールの特定のサブポリシーに従って、アクセス権をユーザに割り当てることができます。サブポリシーには、リソースとオブジェクトのサブセットが含まれ、これらによって ACE Web Application Firewall ポリシー全体が構成されます。

コンソール ユーザのタイプは次のとおりです。

- **管理者**ユーザは、コンソールのすべてのサブポリシーと権限に対して完全なアクセス権を保持しています。ACE Web Application Firewall Manager には、administrator というユーザ アカウントが事前に設定されており、これが管理者ユーザ タイプにあたります。
- **特権ユーザ**は、次のロールのいずれかに従って、ポリシーと設定を変更できます。
  - **Routing** ロールは、ハンドラ、サービス、記述子、ルート、メッセージ変換を作成および設定できます。
  - **Operations** ロールは、ポリシー導入の承認、ポリシーの導入、ポリシーの移動またはアーカイブ、例外処理の設定、ロギング機能の設定ができます。
- **ポリシー表示ユーザ**は、ポリシー情報を表示できますが、編集はできません。

（注）　ユーザが使用できるロール別権限については、オンライン ヘルプの「Console Privileges by User Type and Role」にあるユーザ権限表を参照してください。

管理者ユーザについて

ACE Web Application Firewall Manager Web コンソールには、administrator というユーザ名のローカル ユーザ アカウントが事前に設定されています。このアカウントの削除または権限の変更はできません。administrator アカウントは、ACE Web Application Firewall および Manager でメンテナンスおよび管理タスクを実行するユーザを対象としています。たとえば、administrator ユーザに割り当てられる重要なタスクの一つに、ACE Web Application Firewall Manager がユーザを認証する方法の変更があります。

必要な場合は、管理者ロールを持つ追加のユーザ アカウントを作成できます。administrator ユーザ、または管理者権限を持つユーザ アカウントは、ACE Web Application Firewall および Manager の各機能に無制限にアクセスできます。したがって、このユーザ タイプを割り当てたり、組み込みの administrator アカウントのパスワードを共有する場合は、厳重な注意が必要です。

組み込みの administrator ユーザ アカウントは、ログインの試行に失敗した場合の遮断からは除外されます。しかし、管理者権限を割り当てて作成されたその他のユーザは、この遮断機能が有効な場合は除外されません。詳細については、「ログイン試行に失敗したユーザのブロックの設定」（P.17-4）を参照してください。

認証モード

ACE Web Application Firewall Manager は、Web コンソール ユーザに対する一連の柔軟な認証スキームをサポートします。デフォルトでは、システムはローカル ユーザ アカウントを使用するよう設定されます。ローカル ユーザ アカウントの場合、ログイン時のユーザ認証に使用されるデータは ACE Web Application Firewall Manager 自体に保持されています。別の方法として、ACE Web Application Firewall Manager は LDAP または RADIUS サーバを使用してユーザを認証することもできます。

認証スキームを選択する際、ACE Web Application Firewall Manager がすべてのユーザ アカウントに対して同じ認証メカニズムを使用することに注意してください。たとえば、システムが LDAP を使用するよう設定されている場合、ローカル アカウントを使用する認証を同時に設定できません。選択できる認証スキームは一度に 1 つだけです。

ローカル認証から外部認証に切り替えると、ローカル ユーザ アカウントは使用できなくなり、外部サーバ上で再作成する必要があることに注意してください。このような変更は ACE Web Application Firewall Manager の多数のユーザに影響をおよぼすので、認証モードを切り替える前に、どうすれば

ACE Web Application Firewall Manager で必要なアクセスだけを確実に許可できるかを慎重に検討してください。

ACE Web Application Firewall Manager に外部認証が設定されている場合、ACE Web Application Firewall Manager のツールを使用して有効なユーザ アカウントを作成したり、ユーザのロールを変更したりすることはできません。ユーザのアカウントとロールは、個々のサーバごとに定義および割り当てされるので、追加や変更はそのサーバ上で行う必要があります。

認証モードに関係なく、ACE Web Application Firewall Manager では管理者 ユーザを指定する必要があります。管理者ユーザは、ACE Web Application Firewall Manager の初回設定時と、新しい認証メカニズムに変更する際に定義する必要があります。

ユーザ アカウントの作成

ここでは、ユーザ アカウントの作成方法、ユーザ アカウントへのアクセス権（ロール）の割り当て方法、および、ACE Web Application Firewall Manager がすべてのユーザ アカウントの認証に使用する認証方式の指定方法について説明します。

ローカル ユーザ アカウントは、ACE Web Application Firewall Manager アプライアンス自体に保存されます。これとは対照的に、LDAP 認証には、リモートのアカウント データと認証メカニズムが使用されます。

その他のすべての認証スキームでは、ローカル アカウントとリモート認証が使用されます。つまり、アカウント自体は ACE Web Application Firewall Manager アプライアンスに保存され、ACE Web Application Firewall Manager は外部の RADIUS サーバまたは LDAP ディレクトリを呼び出してユーザを認証します。

（注） LDAP 認証を使用する場合は、ローカル ユーザ アカウントを作成する必要はありません。すべてのユーザ アカウントは、LDAP サーバ上で作成する必要があります。詳細については、「LDAP 認証モードへの切り替え」（P.15-7）を参照してください。

ローカル ユーザ アカウントを作成するには、次の手順を実行します。

ステップ 1　`Administrator` ユーザとして ACE Web Application Firewall Manager Web コンソールにログイン中に、操作メニューの [Administration] セクションで [User Administration] リンクをクリックします。

[User Administration] リンクが表示されていない場合は、[Administration] バナーの横にあるプラス記号（+）をクリックしてメニューを展開します。

ACE Web Application Firewall Manager に [User Administration] ページが表示されます。

ステップ 2　ページ右上の [Create a New User] ボタンをクリックします。

ACE Web Application Firewall Manager に [New User] ページが表示されます。

ステップ 3　[Username] フィールドに、新しいアカウントのユーザ名を入力します。

ステップ 4　[Password] フィールドに、新しいアカウントのパスワードを入力します。

厳密なパスワード オプションが有効になっている（[System Management] > [Manager Settings] > [User Authentication & Security] で指定）と、ACE Web Application Firewall Manager は容易に推測できるパスワードを拒否します。たとえば、日付、社会保障番号、電子メール アドレス、多数の辞書にある単語、名前、その他さまざまなパターンとよく似た言葉などです。

パスワードは、最低 8 文字の英数字だけで構成する必要があります。セキュリティ上の理由により、すべての新規アカウントに対して同じデフォルト パスワードを使用しないでください。

ステップ 5　[Repeat password] フィールドに、[Password] フィールドに入力したのと同じパスワードを入力します。

これらのパスワードは、大文字 / 小文字も含めてまったく同じでなければなりません。

ステップ 6　[User Status] メニューから項目を選択し、アカウントをアクティブにするかどうかを指定します。

デフォルトでは、新規アカウントは [enabled] ステータスで作成されます。現時点でこのユーザにログインを許可しない場合は、[disabled] を選択し、あとからアカウントのステータスを [enabled] に変更できます。

ステップ 7　メニューの次のオプションからユーザのタイプを選択します。

- **Routing** および **Operations** ロールを使用してポリシーおよび設定を編集する必要があるユーザの場合は [Privileged User]。
- [Subpolicies] リスト ボックスで選択されたサブポリシーを表示するが、編集はしないユーザの場合は [Policy View User]。
- サブポリシーの変更や他のユーザの作成および削除など、完全な権限を持つユーザの場合は [Administrator User]。

（注）　ユーザが使用できるロール別権限については、ACE Web Application Firewall Manager Web コンソール オンライン ヘルプの「Console Privileges by User Type and Role」にあるユーザ権限表を参照してください。

ユーザのタイプは、必要に応じて後で変更できます。

ステップ 8　[Privileged User] タイプを選択した場合は、そのユーザのロールを 1 つ以上指定します。

- このユーザに仮想サービスおよびメッセージ処理設定の操作を許可するには、[Routing] ボックスをクリックします。
- このユーザにポリシーの導入、プロセスの制御、ACE Web Application Firewall のマシンレベルの設定を許可するには、[Operations] ボックスをクリックします。

（注）　このロールを持つユーザには、少なくとも **Shared** サブポリシーへのアクセス権が必要です。

ステップ 9　ユーザが表示または編集するサブポリシーを指定します。

- 今後作成されるものも含めて、すべてのサブポリシーへのアクセスを許可するには、[Allow this user to access any subpolicy] をクリックします。
- 強調表示されたリスト アイテムで示されるポリシーへのアクセスだけを許可するには、[Allow this user to access these specified subpolicies] をクリックします。このアイテムを選択した場合、その下に表示されるリストからポリシーを最低 1 つ選択する必要があります。複数のポリシーを選択するには、Ctrl キーを押した状態でクリックします。

  ユーザがサブポリシーの導入を許可されるには、そのサブポリシーだけでなく Shared サブポリシーへのアクセス権も保持している必要があります。

（注）　リストの各サブポリシーへのアクセス許可と、「任意のサブポリシー」へのアクセス許可は違います。新しいサブポリシーが作成されると、「任意のサブポリシー」へのアクセスが許可されている場合に限り、ユーザはその新しいポリシーにアクセスできます。ユーザ アカウントの作成時に、リストされているすべてのサブポリシーへのアクセスを許可した場合、ユーザはそれらのサブポリシーにはアクセスできますが、新しいサブポリシーへのアクセス権はありません。

ステップ 10　[Save Changes] をクリックし、新規アカウントを作成します。新規アカウントを作成せずに終了する場合は、[Cancel] をクリックします。

新規アカウントを有効にすると、そのアカウントの所有者は Web コンソールにログインでき、そのアカウントに割り当てられたロールで利用可能なツールを使用できます。ユーザがログインするためにポリシーを配置する必要はありません。

ユーザ ロールの変更

ユーザ アカウントの作成後、そのアカウントのロールとアクセス権を変更できます。既存のユーザを変更するには、次の手順を実行します。

ステップ 1　`Administrator` ユーザとして、Web コンソールの操作メニューで [User Administration] リンクをクリックします。

[User Administration] ページに、この Manager アプライアンスのユーザ アカウントが表示されます。

ステップ 2　変更するユーザの隣にある [Edit] リンクをクリックします。

ステップ 3　[Edit User] ページで、「ユーザ アカウントの作成」（P.15-3）で説明したコントロールを使用して、ロールやサブポリシー アクセス権など、既存のユーザ設定を変更します。

ステップ 4　[Save Changes] ボタンをクリックし、ユーザ アカウントの変更を保存します。新規アカウントを作成せずに終了する場合は、[Cancel] ボタンをクリックします。変更内容はただちに反映されます。

サブポリシーへのアクセス許可

サブポリシーが作成されると、サブポリシー アクセス権が「任意のポリシー」に設定されている Web コンソール ユーザだけがそのサブポリシーにアクセスできます。「任意のポリシー」アクセス権を持たないユーザにアクセスを許可するには、管理者はサブポリシーの表示または編集を許可する各ユーザの「固有のサブポリシー」アクセス権を変更する必要があります。

アクセスとは、ユーザがサブポリシーを表示する機能を指すことに注意してください。サブポリシーを編集する機能は、ユーザのタイプおよび権限の機能です。

特定のユーザ アカウントが任意のサブポリシーにアクセスできるようにするには、次の手順を実行します。

ステップ 1　`Administrator` ユーザとして、コンソールの操作メニューで [User Administration] リンクをクリックします。

[User Administration] リンクが表示されていない場合は、[Administration] バナーの横にあるプラス記号（+）をクリックしてメニューを展開します。

ステップ 2　編集するユーザ アカウントの隣にある [Edit] ボタンをクリックします。

指定したユーザの [Edit User] ページが表示されます。

ステップ 3　次のいずれかを選択します。

- ユーザがすべての既存のサブポリシーと、今後作成されるポリシーにアクセスできるようにする場合は、[Allow this user to access any subpolicy]。この機能は、サブポリシーへのユーザ アクセスの設定、新規サブポリシーの作成、ポリシーの導入、サブポリシーの承認など、Web コンソールでの特定のタスクで必要です。
- ユーザがアクセスできるサブポリシーを選択して指定する場合は [Allow this user to access these specified subpolicies]。このボタンの下に表示されるサブポリシー リストを必要に応じてクリックし、特定のサブポリシーのセットに対するこのユーザのアクセスを許可または拒否します。このリストで強調表示されているアイテムは、ユーザがアクセスできるサブポリシーを示しています。強調表示されていないサブポリシーは、このユーザには表示されないか、使用できません。複数のサブポリシーを選択するには、Ctrl キーを押した状態でリストのアイテムをクリックします。

（注）　ユーザがサブポリシーの導入を許可されるには、そのサブポリシーおよび Shared サブポリシーへのアクセス権を保持している必要があります。

ステップ 4　[Save Changes] ボタンをクリックし、変更を確定します。

[User Administration] ページにアカウントの変更内容が反映されます。

認証モードの設定

ACE Web Application Firewall Manager でユーザ認証を設定するには、ローカルや LDAP または RADIUS サーバなど、複数の方法があります。ACE Web Application Firewall Manager では、1 つの認証スキームを使用して、すべてのユーザ ログインが認証されます。

デフォルトでは、ACE Web Application Firewall Manager はローカル認証でコンソール ユーザを認証するよう設定されています。この場合、ACE Web Application Firewall Manager はユーザ アカウント情報をローカルで保持、つまり自身のディスクに保存し、外部の認証サービスと接触せずに単独でユーザを認証します。

他の認証方式を使用するには、それを明示してアカウントを設定する必要があります。この方法については、次の項で説明しています。

- 「LDAP 認証モードへの切り替え」（P.15-7）
- 「RADIUS 認証モードへの切り替え」（P.15-9）

LDAP 認証モードへの切り替え

ACE Web Application Firewall Manager では、外部 LDAP ディレクトリを使用して Web コンソールのログイン認定証を認証できます。これにより、既存のユーザ データに基づいて、迅速に Manager へのアクセスを設定できます。

LDAP ディレクトリには、Manager Web コンソールにアクセスする必要があるユーザのアカウント情報が保存されている必要があります。また、管理者やアクセス制御などの標準的な Manager Web コンソール ロールにマップできるグループ定義も格納されている必要があります。特定のサブポリシーへのアクセスも、このグループにマップできます。

LDAP 認証を有効にするには、まず次の情報を収集します。

- LDAP サーバのホスト アドレスとポート番号。これは、ネットワークで表示される LDAP サーバの URL です。このアドレスは、ldap://example.com:389/dc=bar,dc=com のように、LDAP サーバが着信要求をリッスンするポートの番号を示す場合もあります。
- サーバのバインドに使用されるユーザ名やパスワードなどの LDAP バインド情報。ユーザ名は、バインド Distinguished Name（DN; 識別名）です。つまり ACE Web Application Firewall Manager アカウント ユーザ名に対応する識別名でなければなりません。
- 基本 DN。これは、LDAP ディレクトリ内でレコードの検索が開始される DN です。
- LDAP ユーザ レコード。各 ACE Web Application Firewall Manager ユーザ アカウントは、LDAP サーバに有効なユーザ レコードが格納されている必要があります。
- LDAP ユーザ グループ。ACE Web Application Firewall Manager ポリシーで定義された各ロールは、有効なユーザ グループとして LDAP サーバ上で表示される必要があります。このグループの名前は、それに指定される ACE Web Application Firewall Manager ロールと同じである必要はありません。たとえば、「Ops」というグループを作成し、操作ロールを指定することができます。
- ACE Web Application Firewall Manager の管理者ユーザを表す LDAP ユーザ レコード。ACE Web Application Firewall Manager 管理者アカウントは、有効なユーザ レコードとして LDAP サーバ上で表示されます。このユーザの名前は、他の認証スキームを使用する場合のように、「Administrator」である必要はありません。

Web コンソールで LDAP 認証モードを設定する際、LDAP 認証モード設定ページの下部にあるテスト ツールを使用すると、新しい設定が正しいことを確認できます。テストが失敗した場合は、エラーを修正してから LDAP 認証を有効にできます。

LDAP 認証モードを使用するように ACE Web Application Firewall Manager を 設定するには、次の手順を実行します。

ステップ 1　`Administrator` ユーザとして、Web コンソールで [System Management] リンクをクリックします。

ステップ 2　ACE Web Application Firewall Manager 見出しの右側にある [Manager Settings] と表示されたリンクをクリックします。

ACE Web Application Firewall Manager に [Manager Settings] ページが表示されます。

ステップ 3　このページの [User Authentication & Security] セクションで、[Switch to LDAP Authentication] ボタンをクリックします。

コンソールに [LDAP Authentication Mode] ページが表示されます。

ステップ 4　ページ上部の [LDAP Server] セクションに、LDAP サーバのバインドに使用する情報を入力します。

- [Host]。ACE Web Application Firewall Manager がバインドする LDAP ホストの識別名。
- [Port]。LDAP ホストが着信要求を受け入れるポートの番号。

  多くの LDAP サーバは、ポート 389 で着信要求を受け入れます。SSL 要求には、ポート 636 が一般的に使用されます。SSL の使用を予定している場合は、次の手順で説明するように、必ず [Use SSL] チェックボックスを選択してください。
- [Use SSL]。LDAP 要求に SSL を使用する場合は、このボックスをクリックします。LDAP サーバで SSL を使用しない場合は、[Use SSL] ボックスをクリアします。

ステップ 5　セットアップ クエリーを実行する必要がある場合は、[Setup Query] セクションのフィールドを使用して、ACE Web Application Firewall Manager がクエリーの作成に使用する情報を入力します。

- [Bind with DN]。ユーザ名属性をバインドする識別名。
- [Password]。特定のユーザを LDAP サーバで認証する共有秘密。
- [Base DN]。LDAP ディレクトリ内でレコードの検索が開始される DN。
- [Username Attribute]。特定の ACE Web Application Firewall Manager アカウントに割り当てられたユーザ名を指定する LDAP 属性の名前。
- [Perform group query as this user]。このユーザに権限が継承されるグループの名前。

ステップ 6　[Subpolicy-To-Group Mapping] セクションの右カラムで、左カラムに表示された ACE Web Application Firewall Manager サブポリシーに対応する有効な LDAP グループを指定します。

このセクションの左カラムには、現在有効なポリシーの使用可能なサブポリシーがすべて表示されています。少なくとも、このカラムには Shared サブポリシーが必ず含まれています。ポリシーにその他のサブポリシーがある場合は、それもこのカラムに表示されます。

ステップ 7　[Role-To-Group Mapping] セクションの右カラムで、各 ACE Web Application Firewall Manager ロールに対応する有効な LADP グループを指定します。

左カラムには、すべての Manager ユーザ ロールが表示されます。右カラムで、各ロールに対応する各 LDAP グループを指定します。

ステップ 8　ACE Web Application Firewall Manager の [Administrator Authentication] セクションで、ACE Web Application Firewall Manager の管理者である LDAP ユーザの認証に使用する情報を指定します。

a. [Administrator Username] フィールドに、管理者の LDAP ユーザ名を入力します。

（注）　このユーザが Admin ロールで認証されないと、ACE Web Application Firewall Manager は LDAP 認証モードに切り替わりません。

b. [Administrator Password] フィールドに、管理者の LDAP パスワードを入力します。

ステップ 9　LDAP 認証モードを有効にする前に、[Test LDAP Configuration] セクションで設定をテストします。

a. LDAP 認証がアクティブになると ACE Web Application Firewall Manager と連動するユーザ名とパスワードを入力します。

b. [Test] ボタンをクリックします。

ACE Web Application Firewall Manager に認証結果が表示されます。テストが失敗した場合は、LDAP 管理者とともに LDAP 設定を見直してから、操作を続けます。

ステップ 10　新しい設定を確定して LDAP 認証モードを有効にするには、ページ下部の [Switch to LDAP Authentication] ボタンをクリックします。変更を保存せずに [LDAP Authentication Mode] ページを終了するには、[Cancel] ボタンをクリックします。

変更を保存し、その変更が承認されると、次回以降の ACE Web Application Firewall Manager Web コンソールへのログインでは、認証サーバで定義された有効な LDAP ユーザ アカウントを使用する必要があります。

RADIUS 認証モードへの切り替え

RADIUS 認証モードに切り替えるには、次の手順を実行します。

ステップ 1　`Administrator` ユーザとして、コンソールの操作メニューで [System Management] リンクをクリックします。

ステップ 2　ACE Web Application Firewall Manager 見出しの右側にある [Manager Settings] と表示されたリンクをクリックします。

ACE Web Application Firewall Manager に [Manager Settings] ページが表示されます。

ステップ 3　[User Authentication & Security] セクションで [Switch to RADIUS Authentication] ボタンをクリックします。

ACE Web Application Firewall Manager に [RADIUS Authentication Mode] ページが表示されます。

ステップ 4　[Radius Server] セクションに、RADIUS サーバとの接続の認証に必要な情報を入力します。

- [Host]。RADIUS サーバの URL。
- [Port]。RADIUS サーバが着信要求をリッスンするポート。
- [Account Port]。このアカウントが RADIUS サーバ での認証を行うポート。
- [Shared Secret]。ユーザを RADIUS サーバで認証するための値、トークン、またはパスフレーズ。

ステップ 5　ACE Web Application Firewall Manager の [Administrator Authentication] セクションで、[Administrator Username] および [Administrator Password] フィールドに ACE Web Application Firewall Manager の管理者となる RADIUS ユーザのユーザ名とパスワードを入力します。

このユーザ名は、既存のローカル ACE Web Application Firewall Manager アカウントの名前と一致してはいけません。また、ユーザ名とパスワードは、RADIUS システムで正しく認証された RADIUS ユーザ アカウントのものでなければなりません。そうでない場合、Manager Web コンソールの認証モードは変更されません。

ステップ 6　新しい設定を確定して RADIUS 認証モードを有効にするには、ページ下部の [Switch to RADIUS Authentication] ボタンをクリックします。変更を保存せずに [RADIUS Authentication Mode] ページを終了するには、[Cancel] ボタンをクリックします。

変更を保存し、その変更が承認されると、次回以降の ACE Web Application Firewall Manager Web コンソールへのログインでは、認証サーバで定義された有効な RADIUS ユーザ アカウントを使用する必要があります。

ローカル認証モードへの切り替え

LDAP または RADIUS 認証モードでは、[Manager Settings] ページの [User Authentication & Security] セクションに [Switch To Standard Passwords] ボタンが表示されます。このボタンを使用すると、ACE Web Application Firewall Manager でローカルのユーザ名とパスワードの認証を有効にできます。

認証モードをサーバベースからローカル認証に切り替えるには、次の手順を実行します。

ステップ 1　`Administrator` ユーザとして、操作メニューの [System Management] リンクをクリックします。

ステップ 2　ACE Web Application Firewall Manager 見出しの右側にある [Manager Settings] リンクをクリックします。

ACE Web Application Firewall Manager に [Manager Settings] ページが表示されます。

ステップ 3　[User Authentication & Security] セクションの [Switch to Standard Passwords] ボタンをクリックします。

ACE Web Application Firewall Manager に [Standard Passwords Authentication Mode] ページが表示されます。

ステップ 4　新しい設定を確定してローカル認証モードを有効にするには、ページ下部の [Switch To Standard Passwords] ボタンをクリックし、変更を確定します。変更を保存せずに RADIUS または LDAP 認証モード ページを終了するには、[Cancel] ボタンをクリックします。

変更を保存し、その変更が承認されると、次回以降の Web コンソールへのログインでは、ACE Web Application Firewall Manager で定義された有効なローカル ユーザ アカウントを使用する必要があります。

ステップ 5　LDAP 認証モードから切り替えた場合、ACE Web Application Firewall Manager はこれまでに Web コンソールにログインした各 LDAP アカウントに対してローカル ユーザ アカウントを作成します。

これらのアカウントは、パスワードを割り当てるまで使用できません。これらのアカウントをアクティブにするか、削除するか、あるいは新規ローカル アカウントを作成するかを決定します。

- アカウントをアクティブにするには、そのアカウントにパスワードを割り当てます。
- アカウントを非アクティブなままにしておく場合は、特に必要な操作はありません。
- LDAP モードからの切り替えで ACE Web Application Firewall Manager によって作成されたローカル アカウントには、パスワードがありません。パスワードを割り当てないかぎり、このローカル アカウントは使用できません。
- アカウントを削除するには、[Administration] > [User Administration] ページで、アカウントの横にある [Delete] リンクをクリックします。
- 新規アカウントを作成するには、[Administration] > [User Administration page] ページで [Create A New User] ボタンをクリックします。新規アカウントの名前は、LDAP 認証モードからの切り替え時に自動的に生成されたものも含めて、既存アカウントの名前と重複してはいけません。