CHAPTER 33

Web コンソール ユーザの管理

この章では、ACE XML Manager Web 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

主要ネットワーク セキュリティ ポリシーの作成および監視ポイントとして、コンソールへのアクセスは十分に保護する必要があります。認証されたユーザだけが ACE XML Manager Web コンソールにアクセスできます。Web コンソールは、各ユーザ アカウントをユーザが実行できる操作を決定する特権セットに関連付けることで、さらに制約事項を適用します。また、ACE XML Manager Web コンソールの各ユーザは、ACE XML Manager の管理者がアクセスを許可したサブポリシーだけを表示または編集できます。

コンソールの管理者は、ユーザのタイプ、ロール、ポリシー アクセス権限を適切に割り当てることで、ポリシーおよび設定を変更する許可が与えられたユーザだけが変更できるようにすることができます。

ACE XML 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送信して**認証**を行う必要があります。ACE XML Manager は、認証されたユーザ ID を Web コンソール内の権限セットと照合します。ここでは、ACE XML Manager でサポートされる認証スキームおよびそれらのスキーム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 XML Manager Web コンソールにはいくつかのユーザ タイプがあります。Administrator ユーザは最も広範な権限を持ち、外部開発者は権限が最も少なくなります。ただし、ユーザが行える操作は、ユーザのロールおよび特定のポリシーに関連付けられたアクセス権限に依存します。たとえば、コンソール内の特定のサブポリシーへのアクセス権限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、ACE XML Gateway ポリシー全体を構成するリソースおよびオブジェクトのサブセットが含まれます。

コンソール ユーザのタイプは次のとおりです。

- **Administrator** ユーザには、コンソール内のすべてのサブポリシーへのフル アクセス権限およびすべての特権があります。ACE XML Manager には、このユーザ タイプである `Administrator` という名前のユーザ アカウントがあらかじめ設定されています。
- **privileged users** は、次のいずれかのロールに従ってポリシーおよび構成の設定を変更できます。
  - **Access control** ロールは、保護リソースにアクセスできるユーザを制御する設定を行えます。
  - **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** ロールはポリシー配布の承認、ポリシーの配布、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を行えます。
  - **Message log** ロールは、機密情報が含まれることがあるメッセージ トラフィック ログの内容を表示できます。
- **policy view users** は、ポリシー情報を表示できますが、編集できません。
- **external developer** ユーザは、権限が最も制限されています。ACE XML Manager のプロビジョニングされたサービスのディレクトリを表示し、それらのサービスに関して ACE XML Manager が生成する Web Services Description Language（WSDL）ファイルをダウンロードできますが、それ以外のことは行えません。

（注） ロール別のユーザ特権の詳細については、オンライン ヘルプの「Console Privileges by User Type and Role」内のユーザ権限表を参照してください。

Administrator ユーザについて

ACE XML Manager Web コンソールには、`Administrator` という名前のローカル ユーザ アカウントが事前設定されています。このアカウントを削除したり、その特権を変更したりすることはできません。`Administrator` アカウントは、ACE XML Gateway および Manager でのメンテナンスおよび管理作業を行うユーザ用です。たとえば、`Administrator` ユーザの重要な作業の 1 つに、ACE XML Manager によるユーザの認証方法を変更する作業があります。

必要な場合は、Administrator ロールを持つ別のユーザ アカウントを作成できます。`Administrator` ユーザ、つまり Administrator 特権を持つユーザ アカウントは、ACE XML Gateway および Manager のすべての機能に制限なくアクセスできます。そのため、このユーザ タイプを割り当てる場合や事前設定されている `Administrator` アカウントのパスワードを共有する場合は細心の注意が必要です。

事前設定されている `Administrator` ユーザ アカウントは、ログインに失敗した場合のブロッキングから除外されます。ただし、その機能が有効な場合、Administrator 特権で作成されたその他のユーザは除外されません。詳細については、「ログイン試行に失敗したユーザのログイン拒否設定」（P.35-368）を参照してください。

認証モード

ACE XML Manager では、Web コンソール ユーザの認証スキームは柔軟にサポートされています。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に設定されています。ローカル ユーザ アカウントの場合、ログイン時にユーザ認証に使用されたデータは ACE XML Manager に保存されます。または、ACE XML Manager では LDAP または RADIUS サーバに対してユーザを認証することも可能です。

認証スキームを選択する場合、ACE XML Manager はすべてのユーザ 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が必要です。たとえば、システムが LDAP を使用するように設定されていると、ローカル アカウントを使用して認証するように設定することはできません。どちらか一方を選択する必要があります。

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、外部サーバ上でもう一度作成する必要があります。ACE XML Manager の多くのユーザがこうした変更の影響を受ける可能性があるため、認証モードを切り替える前に ACE XML Manager への必要なアクセスを確保する方法を慎重に検討してください。

ACE XML Manager が外部認証用に設定されていると、ACE XML Manager のツールを使用してアクティブなユーザ アカウントの作成やアカウントのロール変更を行うことはできません。ユーザ アカウントおよびロールが別のサーバによって設定され割り当てられているため、追加や変更はそのサーバ上で行う必要があります。

どの認証モードを使用している場合でも、ACE XML Manager では Administrator ユーザを指定する必要があります。このユーザは ACE XML Manager の初期設定時、および新しい認証メカニズムへの変更時には必ず指定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 アカウントを作成する方法、ユーザ アカウントにアクセス権限（ロール）を割り当てる方法、および ACE XML 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法を指定する方法について説明します。

local user account は ACE XML Manager アプライアンスに格納されます。それに対して、LDAP 認証ではリモート アカウント データおよび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。アカウント自体は ACE XML Manager アプライアンスにあり、ACE XML Manager は外部 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.33-355）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手順は、次のとおりです。

ステップ 1　ACE XML Manager Web コンソールに `Administrator` ユーザとしてログインし、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] リンクが表示されない場合は、[Administration] バナーの横のプラス記号（[+]）をクリックしてメニューを開きます。

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

ステップ 2　ページの右上にある [Create a New User] ボタンをクリックします。

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

ステップ 3　[Username] 欄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] 欄に新しいアカウントのパスワードを入力します。

（[System Management] > [Manager Settings] > [User Authentication & Security] で）ストリクト パスワード オプションが有効な場合、ACE XML Manager では日付、社会保障番号、電子メール アドレス、辞書に載っている語、その他のさまざまなパターンに類似したパスワードなど、簡単に推測できるパスワードは拒否されます。

パスワードには英数字だけを 8 文字以上使用します。セキュリティ上の理由から、すべての新しいアカウントに同じデフォルト パスワードを使用しないでください。

ステップ 5　[Repeat password] 欄に [Password] 欄に入力した同じパスワードを入力します。

パスワードは、大文字小文字の区別を含めて完全に一致する必要があります。

ステップ 6　[User Status] メニューで、アカウントがアクティブかどうかを指定します。

デフォルトでは、新しいアカウントは **enabled** ステータスで作成されます。ユーザにログインさせないようにするには、**disabled** を選択します。後で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　メニュー内の次のオプションからユーザのタイプを選択します。

- [Privileged User] は、ポリシーおよび設定を編集する必要があるユーザ用で、**Access Control**、**Message Traffic Log**、**Routing**、および **Operations** ロールを割り当てることができます。
- [Policy View User] は、[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必要はあるが、編集は行わないユーザ用です。
- [External Developer] は、ACE XML Manager のプロビジョニングされたサービスのディレクトリを表示する必要はあるが、編集は行わないユーザ用です。
- [Administrator User] は、すべてのサブポリシーの変更、その他のユーザの作成および削除など、すべての特権を持つユーザ用です。

（注）　ロール別のユーザ特権の詳細については、ACE XML Manager Web コンソールのオンライン ヘルプで「Console Privileges by User Type and Role」のユーザ特権表を参照してください。

ユーザのタイプは後で必要に応じて変更できます。

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

- このユーザがオーセンティケータ、権限付与グループ、プロビジョニング、認証リソースを作成および変更できるようにするには、[Access Control] ボックスをクリックします。
- このユーザが仮想サービスおよびメッセージ処理設定を取り扱うことができるようにするには、[Routing] ボックスをクリックします。
- このユーザがポリシーを配布し、ACE XML Gateway のプロセスおよび機械レベルの設定を制御できるようにするには、[Operations] ボックスをクリックします。

（注）　このロールの場合、ユーザには少なくとも **Shared** サブポリシーへのアクセスが必要です。

- このユーザが（機密情報が含まれることがある）メッセージ トラフィック ログの内容を表示できるようにするには、[Message Traffic Log] オプションを選択します。

（注）　**Message Traffic Log** ロールは単独で割り当てることができません。ユーザに **Message Traffic Log** ロールを割り当てる場合は、別のロールを少なくとも 1 つ割り当てる必要があります。

ステップ 9　ユーザが表示または編集できるサブポリシーを指定します。

- 今後作成されるポリシーを含む、すべての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項目によって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。この項目を選択すると、その下に表示されるリストから少なくとも 1 つのポリシーを選択する必要があります。複数のポリシーを選択する場合は、Ctrl キーを押しながらポリシーをクリックします。

  サブポリシーを配布できる必要があるユーザには、そのサブポリシーおよび Shared サブポリシーへのアクセスが必要です。

（注）　リスト内のすべてのサブポリシーへのアクセス許可は、「any subpolicy」アクセスを許可するのとは同じではありません。新しいサブポリシーが作成されると、ユーザは「any subpolicy」アクセスが許可されている場合に限り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、一覧表示されたすべてのサブポリシーへのアクセスを許可した場合、ユーザは一覧表示されたサブポリシーにはアクセスできますが、新しく作成されたサブポリシーにはアクセスできません。

ステップ 10　[Save Changes] をクリックして、新しいアカウントを作成します。新しいアカウントを作成しないで終了するには、[Cancel] をクリックします。

新しいアカウントを有効にすると、アカウントのオーナーは Web コンソールにログインして、そのアカウントに割り当てられたロールで使用可能なツールを使用できるようになります。ユーザがログインするためにポリシーを導入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に、アカウントのロールおよびアクセス権限を変更できます。既存ユーザを変更する手順は、次のとおりです。

ステップ 1　Web コンソールで `Administrator` ユーザとして、操作メニューの [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　変更するユーザの横にある [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.33-351）で説明されているコントロールを使用して、ロールやサブポリシー アクセス権限などの既存ユーザの設定を変更します。

ステップ 4　[Save Changes] ボタンをクリックしてユーザ アカウントの変更を保存します。新しいアカウントを作成しないで終了するには、[Cancel] ボタンをクリックします。変更はただちに有効になります。

サブポリシーへのアクセスの有効化

サブポリシーを作成すると、サブポリシー アクセスが「any subpolicy」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。「any subpolicy」アクセス権限がないユーザにアクセスを許可するには、サブポリシーを表示または編集できる必要がある各ユーザの「specific subpolicy」アクセス権限を管理者が編集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できることを言います。サブポリシーを編集できるかどうかはユーザのタイプおよび特権によって異なります。

指定ユーザ アカウントがすべてのサブポリシーにアクセスできるようにする手順は、次のとおりです。

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

[User Administration] リンクが表示されない場合は、[Administration] バナーの横のプラス記号（[+]）をクリックしてメニューを開きます。

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

指定ユーザの [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。

- [Allow this user to access any subpolicy] は、ユーザがすべての既存サブポリシーおよびそれ以降に作成されたサブポリシーにアクセスできるようにします。この機能は、Universal Description, Discovery and Integration（UDDI）サーバへの公開、サブポリシーへのユーザ アクセスの設定、新しいサブポリシーの作成、ポリシーの配布、サブポリシーの承認など、Web コンソールでの特定の作業に必要です。
- [Allow this user to access these specified subpolicies] では、ユーザがアクセスできるサブポリシーを選択して指定します。このボタンの下に表示されるサブポリシーのリストで、必要に応じてクリックして特定のサブポリシー 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項目は、ユーザがアクセスできるサブポリシーを表します。強調表示されていないサブポリシーはこのユーザに対して表示されないか、このユーザは使用できません。複数のサブポリシーを選択する場合は、**Ctrl** キーを押しながらリスト内の項目をクリックします。

（注）　サブポリシーを配布できるようにするには、ユーザは Shared サブポリシーだけではなく、そのサブポリシーにもアクセスできる必要があります。

ステップ 4　[Save Changes] ボタンをクリックし、変更をコミットします。

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

認証モードの設定

ACE XML Manager は、ローカル、LDAP、RADIUS サーバなど、さまざまな方法でユーザを認証するように設定できます。ACE XML Manager は、1 つの認証スキームを使用してすべてのユーザ ログインを認証します。

デフォルトでは、ACE XML Manager はローカル認証を使用してコンソール ユーザを認証するように設定されています。この場合、ACE XML Manager は外部認証サービスを使用するのではなく、自身のディスクにユーザ アカウント情報をローカルに保持してユーザを認証します。

別の認証方法を使用するには、次の各項で説明されているようにその認証方法を使用するようにアカウントを明示的に設定する必要があります。

- 「LDAP 認証モードへの切り替え」（P.33-355）
- 「RADIUS 認証モードへの切り替え」（P.33-357）

LDAP 認証モードへの切り替え

ACE XML Manager では、外部 LDAP ディレクトリに対して Web コンソールのログイン クレデンシャルを認証できます。そのため、既存ユーザ データに基づいて Manager のアクセスを迅速に設定できます。

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含まれている必要があります。また、Administrator、Access Control などの標準的な Manager Web コンソール ロールにマッピングできるグループ定義も必要です。特定のサブポリシーへのアクセスはグループにもマッピングできます。

LDAP 認証を有効にするには、最初に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、ネットワーク上で LDAP サーバが表示される URL です。このアドレスは、サーバが着信要求をリッスンするポートの数を指定することがあります（例：ldap://example.com:389/dc=bar,dc=com）。
- LDAP バインディング情報（サーバへのバインドに使用するユーザ名とパスワードを含む）。ユーザ名はバインド Distinguished Name（DN; 認定者名）にする必要があります。これは、ACE XML Manager アカウント ユーザ名に対応する認定者名です。
- ベース DN。これは、LDAP ディレクトリでレコードの検索を開始する DN です。
- LDAP ユーザ レコード。各 ACE XML Manager ユーザ アカウントには LDAP サーバ上の有効なユーザ レコードが必要です。
- LDAP ユーザ グループ。ACE XML Manager ポリシー内で定義されている各ロールは、LDAP サーバ上の有効なユーザ グループとして示される必要があります。グループ名は、そのグループが表す ACE XML Manager ロールと同じである必要はありません。たとえば、Operations ロールを表すグループ名を「Ops」とすることができます。
- ACE XML Manager の管理ユーザを表す LDAP ユーザ レコード。ACE XML Manager の Administrator アカウントは LDAP サーバ上の有効なユーザ レコードとして示されます。他の認証スキームを使用している場合のように、ユーザ名を「Administrator」にす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場合、[LDAP Authentication Mode] 設定ページの最下部にあるテスト ツールを使用して新しい設定が正しいことを確認できます。テストに失敗した場合、エラーを修正してから LDAP 認証を有効にします。

LDAP 認証モードを使用するように ACE XML Manager を設定する手順は、次のとおりです。

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

ステップ 2　ACE XML Manager という見出しの右にある [Manager Settings] リンクをクリックします。

ACE XML 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 [Authentication & Security] セクションにある [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] セクションで、LDAP サーバへのバインドに使用される情報を入力します。

- [Host]。ACE XML Manager がバインドする必要がある LDAP ホストの認定者名。
- [Port]。LDAP ホストが着信要求を受信するポートの数。

  多くの LDAP サーバはポート 389 で着信要求を受信します。SSL 要求の場合はポート 636 が一般的です。SSL を使用する場合は、次の手順で説明されているように [Use SSL] チェックボックスがオンになっていることを確認します。
- [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] ボックスをオフにする必要があります。

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] セクション内の欄を使用して ACE XML 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]。ユーザ名のアトリビュートがバインドする認定者名。
- [Password]。LDAP サーバに対して特定のユーザを認証する共有秘密。
- [Base DN]。LDAP ディレクトリでレコードの検索を開始する DN。
- [Username Attribute]。特定の ACE XML Manager アカウントに関連付けられたユーザ名を指定する LDAP アトリビュートの名前。
- [Perform group query as this user]。このユーザが特権を継承するグループの名前。

ステップ 6　[Subpolicy-To-Group Mapping] セクションの右のカラムで、左のカラムに表示されている ACE XML 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のカラムには、現在の作業ポリシーの使用可能なサブポリシーがすべて表示されます。このカラムには、少なくとも Shared サブポリシーが常に表示されます。ポリシーに他のサブポリシーがあれば、そのサブポリシーも表示されます。

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

左のカラムにすべての Manager ユーザ ロールが表示されます。右のカラムで、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 XML Manager の [Administrator Authentication] セクションで、ACE XML 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] 欄に管理者の LDAP ユーザ名を入力します。

（注）　Admin ロールでこのユーザの認証が正常に行われなかった場合、ACE XML Manager では LDAP 認証モードに切り替わりません。

b.　[Administrator Password] 欄に管理者の LDAP パスワードを入力します。

ステップ 9　[Test LDAP Configuration] セクションで、設定をテストしてから LDAP 認証モードを有効にします。

a.　LDAP 認証がアクティブになったら、ACE XML Manager で有効な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 XML Manager に認証試行の結果が表示されます。認証試行が失敗した場合は、作業を続ける前に LDAP 管理者と LDAP 設定を確認してください。

ステップ 10　新しい設定を受け入れて LDAP 認証モードを有効にするには、ページの最下部にある [Switch to LDAP Authentication] ボタンをクリックします。変更を保存しないで [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、その変更が許可された場合、それ以降 ACE XML Manager Web コンソールにログインするとき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手順は、次のとおりです。

ステップ 1　コンソールで `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 XML Manager という見出しの横にある [Manager Settings] リンクをクリックします。

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

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

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

ステップ 4　[Radius Server] セクションで、RADIUS サーバへ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 サーバで認証するポート
- [Shared Secret]。RADIUS サーバに対してユーザを認証する値、トークン、またはパスフレーズ

ステップ 5　ACE XML Manager の [Administrator Authentication] セクションにある [Administrator Username] 欄および [Administrator Password] 欄に、ACE XML Manager の管理者になる RADIUS ユーザのユーザ名とパスワードを入力します。

ユーザ名は、ACE XML Manager のその他の既存ローカル アカウントのユーザ名と重複しないようにする必要があります。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 アカウントである必要があります。そうでない場合は、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　新しい設定を受け入れて RADIUS 認証モードを有効にするには、ページの最下部にある [Switch to RADIUS Authentication] ボタンをクリックします。変更を保存しないで [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、その変更が許可された場合、それ以降 ACE XML Manager Web コンソールにログインするとき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 XML Manager でローカル ユーザ名とパスワードを使用して認証を行うことができます。

サーバベースからローカル認証に認証モードを変更する手順は、次のとおりです。

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 XML Manager という見出しの右にある [Manager Settings] リンクをクリックします。

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

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

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

ステップ 4　新しい設定を受け入れてローカル認証モードを有効にするには、ページの最下部にある [Switch To Standard Passwords] ボタンをクリックして変更を確定します。変更を保存しないで 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、その変更が許可された場合、それ以降 Web コンソールにログインするときは ACE XML 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は、ACE XML Manager は、それまでに Web コンソールにログインしたことがある各 LDAP アカウントのローカル 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、または新しいローカル 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、パスワードを指定します。
- アカウントを非アクティブのままにしておく場合は何もする必要はありません。
- LDAP モードから切り替えたときに ACE XML 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設定されていません。パスワードを指定しないと、この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の [Delete] リンクをクリックします。
- 新しいアカウントを作成するには、[Administration] > [User Administration] ページで [Create A New User] ボタンをクリックします。新しいアカウントの名前は、LDAP 認証モードから切り替えたときに自動的に作成された名前を含め、既存アカウント名と同じ名前にすることはできません。