CHAPTER 35

Manager の Web コンソールの設定

この章では、ACE XML Manager の Web コンソールの設定方法について説明します。内容は次のとおりです。

Manager SSL 証明書の変更

SSL 証明書は、Web ブラウザと ACE XML Manager の Web コンソール（管理ポート上にあり、デフォルトでは 8243）の間のセキュアな接続に使用されます。インストール時にこの接続を保護する場合は、一時的証明書が使用されます。一時的証明書は、ここで説明するように、ACE XML Manager で作成する永続的な証明書に置き換える必要があります。

（注） ACE XML Manager では、UTF8 形式で秘密鍵を作成できません。ACE XML Manager は、既存の証明書や鍵を UTF8 形式でインポートできますが、これらの作成はできません。

Manager の証明書署名要求（CSR）の作成

ACE XML Manager の SSL 証明書の Certificate Signing Request（CSR; 証明書署名要求）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、操作メニューの [Administration] セクションで [Cluster Management] リンクをクリックします。

[Cluster Management] ページに、この Manager の管理制御内のクラスタが表示されます。複数のクラスタを使用しない場合は、リストには 1 つのクラスタ（デフォルトのクラスタ）しか表示されません。

ステップ 2 [Manage SSL Certificates] ボタンをクリックします。

ステップ 3　証明書署名要求（CSR）を作成するには、[Manage Certificates] ボタン、[Generate New CSR] の順にクリックします（[Manager SSL Certificates] ページの [Outstanding Certificates Signing Requests] エリア内）。

ステップ 4　[Generate Certificate Signing Request] ページで、次のフィールドに入力します。

フィールド	説明
[Common Name]	ID を証明中の個人名またはエンティティ名
[E-mail Address]	CSR に応じて署名された証明書を受信する電子メール アドレス
[Company (O)]	CN が関連付けられている組織名または会社名
[Department (OU)]	組織の組織ユニット名またはサブグループ名
[City]	証明中のエンティティの市区町村
[State]	証明中のエンティティの都道府県
[ISO Country Code]	エンティティの国の 2 文字の International Standards Organization（ISO; 国際標準化機構）コード

ステップ 5　情報の入力が完了したら、[Generate Request] をクリックします。入力した情報を使用して、ACE XML Manager が証明書署名要求（CSR）を作成し、[Certificate Signing Request] ページに表示します。

ステップ 6　CSR データ（`-----BEGIN CERTIFICATE REQUEST-----` という文字列と `-----END CERTIFICATE REQUEST-----` という文字列の間の部分）を、テキスト ファイルまたは電子メール メッセージに表示します。優先度の高い Certificate Authority（CA; 認証局）に CSR データを送信し、署名入りの X.509 証明書に変換します。

（注）　CA 要求フォームで認証タイプの指定を求められる場合があります。その場合は、Apache 形式の証明書を要求して ACE XML Manager で使用します。

ステップ 7　署名入り証明書が到達したら、「Manager SSL 証明書の設定」（P.35-366）の説明に従って ACE XML Manager にインストールします。

（注）　CA が証明書をすぐに返さない場合があります。場合によっては、証明書署名要求への対応に数日かかる場合があります。

Manager SSL 証明書の設定

作成した要求に応じて署名された証明書を受信したら、次の手順で ACE XML Manager の SSL 証明書を CA の署名入り証明書と置き換えます。

ステップ 1　CA から署名入り証明書を受信したら、`Administrator` ユーザとして [Cluster Management] ページに戻ります。

ステップ 2　[Manage Certificates]、[Upload Signed Cert] リンクの順にクリックします（[Outstanding Certificate Signing Requests] ペイン内）。

ステップ 3　[Upload New ACE XML Manager Certificate] ページで、証明書をファイル システムやネットワーク ロケーションからアップロードするか、テキスト フィールドに証明書のテキストをコピーしてアップロードするかを指定します。

ステップ 4　[Upload] ボタンをクリックします。

ステップ 5　証明書を Manager に割り当てるには、[Exit to Cluster Management] ボタンをクリックします。

ステップ 6　[Cluster Management] ページで、証明書を使用するクラスタの横の [edit] リンクをクリックします。この ACE XML Manager の複数のクラスタを管理しない場合は、デフォルトのクラスタの横の [edit] をクリックします。

[SSL Certificate] フィールドには、現在使用されている証明書が表示されます。この値が「Temporary Certificate, Please Regenerate」の場合、デフォルトの証明書はまだ置き換えられていません。このデフォルトの証明書を CA 署名付き証明書に置き換えるまで、この導入は安全とは見なされません。

ステップ 7　[SSL Certificate] フィールドで、アップロードした証明書を選択して [Save Changes] をクリックします。

導入時の URL ベース リソースのリロードの指示

セキュリティ上の理由から、ACE XML Manager はポリシーで使用するリモート リソースを自動的に取得しません。リモートでホストされる最新バージョンのリソース（URL から取得したスキーマや証明書など）があることを確認するには、ポリシーを導入する前にこのようなリソースのリロードが必要になる場合があります。

任意に ACE XML Manager を設定して、コンソール ユーザに対してポリシーの導入前にリソースをリロードするよう指示するプロンプトを表示できます。

（注）　詳細については、「導入時の URL ベース リソースのリロード」（P.29-298）を参照してください。

コンソールでリソース リロードのプロンプトをイネーブルにするには、次の手順を実行します。

ステップ 1　`Administrator` ユーザとして、ACE XML Manager 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　[System Management] ページで、[ACE XML Manager] という見出しの横の [Manager Settings] リンクをクリックします。

ステップ 3　基本設定の [Workflow] ペインで、[Prompt users to reload URL-based resources] チェックボックスをクリックします。

ステップ 4　ページ下部の [Save Changes] ボタンをクリックします。

ステップ 5　リソース リロードのプロンプトがアクティブであることを確認するには、ページ上部の [Deploy Policy] ボタンをクリックして導入を試行します。

リソース リロードのプロンプトがイネーブルの場合は、[Step 1 of 4: URL Resource Refresh] ページが表示されます。[Deploy Policy] ボタンのクリック後に最初に表示される画面としてこのページが表示されない場合は、リソース リロードのプロンプトがイネーブルではありません。

ステップ 6　導入するか、あるいは [Cancel Deployment] ボタンをクリックして導入せずに [Policy Manager] ページに戻ります。

ユーザのアイドル タイムアウトの設定

セキュリティ上、ACE XML Manager の Web コンソールは、設定期間が経過するとアイドル ユーザをコンソールからログオフさせることができます。デフォルトでは、アイドル タイムアウトのセッション期間は 1800 秒（30 分）です。

ACE XML Manager の Web コンソールのアイドル タイムアウト期間を変更するには、次の手順を実行します。

ステップ 1　Administrator ユーザとして、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　[Manager Settings] リンクをクリックします。

ステップ 3　[Idle Session Timeout] フィールドに新しいアイドル タイムアウト値を秒単位で入力します。このフィールドは、[User Authentication & Security] 設定とともに表示されます。

ステップ 4　完了したら、[Save Changes] をクリックします。変更がただちに有効になります。

ログイン試行に失敗したユーザのログイン拒否設定

コンソール ユーザがログイン試行に連続して失敗した場合（デフォルトでは 3 回）、ACE XML Manager はユーザによるコンソール アクセスの連続試行を遮断することができます。ユーザ アカウントは、管理者が直接有効にするまで一時停止のままです。

必要に応じて、次の説明に従ってログイン失敗によるログイン拒否をディセーブルにできます。また、組み込みの `Administrator` ユーザは拒否されません。ただし、Administrator のロールを持つ追加ユーザ アカウントは、ログイン失敗によるログイン拒否の対象となります。

拒否されたユーザを再び有効にするには、次の手順を実行します。

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

ステップ 2　無効なユーザの横の [Edit] ボタンをクリックします。

ステップ 3　ユーザ ステータスを無効から有効に変更します。

ステップ 4　[Save Changes] をクリックします。

Administrator ユーザとして、この機能の一般的な動作を設定するには、次の手順を実行します。

ステップ 1　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　[System Management] ページで、[Manager Settings] リンクをクリックします。

ステップ 3　[Disable User After] と記載されたコントロールを使用してこの機能を設定します。このオプションを有効にすると、ログイン試行の失敗が指定回数に達すると、ユーザはログインを拒否されます。

ステップ 4　完了したら、[Save Changes] をクリックします。

変更がただちに有効になります。

表示する時間帯の設定

ACE XML Gateway は内部クロックに Greenwich Mean Time（GMT; グリニッジ標準時）を使用します。GMT はタイムスタンプの確認、内部ログ データ、およびその他のタイム ベースのサービス処理アクティビティに使用されます。

ただし、ACE XML Manager が使用する時間帯を変更して、ACE XML Manager または Gateway の通常動作を干渉することなく情報を表示できます。

ACE XML Manager の表示する時間帯を変更するには、次の手順を実行します。

ステップ 1　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　[System Management] ページで、[Manager Settings] リンクをクリックします。

ステップ 3　このページのインターフェイスのセクションで、メニューから [Display Time Zone] を選択します。

ステップ 4　[Save Changes] をクリックします。

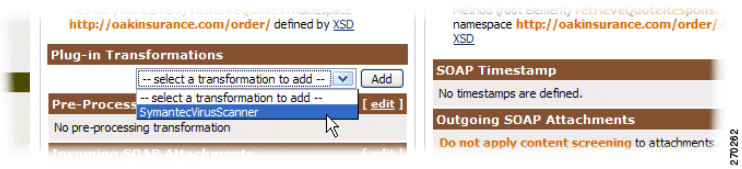
ソフトウェア開発キット（SDK）拡張機能と Web コンソールの統合

システム拡張機能を作成して、ACE XML Gateway の機能をカスタマイズまたは拡張できます。ACE XML Gateway の Software Development Kit（SDK; ソフトウェア開発キット）には、アクセス コントロール、メッセージの変換、およびサービス トラフィックのプロトコルに使用するカスタム モジュールの作成用ツールが含まれています。

（注）　SDK 拡張機能は、仮想サービスのインターフェイスで処理されるトラフィックだけに適用できます。

拡張機能を作成したら、ACE XML Manager アプライアンス ファイル システムに読み込んでポリシーで利用できるようにします。拡張機能の設定は、標準の組み込み型設定パラメータとともに ACE XML Manager の Web コンソールに表示されます。

図 35-1　コンソールでの拡張機能の適用



ポリシーを導入すると、拡張機能がポリシーとともに自動的に ACE XML Gateway に移動します。

（注）　拡張機能の作成については、『*Cisco ACE XML Gateway Developer's Guide*』を参照してください。

使用可能な拡張機能の表示

次の手順で、[System Management] ページから ACE XML Manager に追加した拡張機能の情報を表示できます。

ステップ 1　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　このページの [ACE XML Manager] 設定セクションで、[Extensions Status] ラベルの横の [view status page] リンクをクリックします。

[Extensions Status] ページが表示されます。

ステップ 3　拡張機能の詳細を表示するには、拡張機能名の横のエキスパンダ コントロールをクリックします。

拡張機能開発モード

拡張機能の開発は通常、ACE XML Manager で開発段階とテスト段階を繰り返す反復プロセスです。ACE XML Manager を拡張機能開発モードに設定すると、このプロセスが簡単になります。

SDK 開発モードでは、アプライアンス ファイル システムの拡張ディレクトリに格納された拡張機能が ACE XML Manager によって自動的にリロードされるため、ACE XML Manager を再起動する必要はありません。また、イベント記録がインラインでイベント ログに書き込まれます。

ACE XML Manager を SDK 開発モードに設定するには、次の手順を実行します。

ステップ 1　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　[System Management] ページで、[Manager Settings] リンクをクリックします。

ステップ 3　このページの [General] 設定セクションで、[Enable extension development mode] チェックボックスをオンにします。

ステップ 4　[Save Changes] をクリックします。

変更がただちに有効になります。