Oracle® WebCenter Sites

Web エクスペリエンス管理フレームワーク
管理者ガイド

11*g* リリース 1 (11.1.1)

部品番号 : B69684-01

2012 年 4 月

ORACLE®

Oracle® WebCenter Sites Web エクスペリエンス管理フレームワーク管理者ガイド , 11g リリース 1 (11.1.1)

部品番号 : B69684-01

原本名 : Oracle® WebCenter Sites Administrator's Guide for the Web Experience Management Framework, 11g Release 1 (11.1.1)

原本主著者 : Tatiana Kolubayev、Melinda Rubenau

原本協力者 : Ravi Khanuja

目次

このガイドについて

このガイドでは、WebCenter Sites データベースと通信するアプリケーションに対する Oracle WebCenter Sites ユーザーのアクセスを、WEM (Web エクスペリエンス管理) 管理インタフェースを使用して認可する手順について説明します。最初に WEM フレームワークの概要について説明し、続いて WEM 管理インタフェースを使用してユーザーを作成し、WebCenter Sites で実行されているアプリケーションの使用をそのユーザーに認可するプロセスについて説明します。最後の章は、WEM フレームワークを管理するためのクイック・リファレンスです。

このガイドで説明しているアプリケーションは、旧 FatWire の製品です。命名規則は次のとおりです。

- *Oracle WebCenter Sites* は、以前は *FatWire Content Server* と呼ばれていたアプリケーションの現在の名前です。このガイドでは、*Oracle WebCenter Sites* を *WebCenter Sites* と呼ぶこともあります。
- *Oracle WebCenter Sites: Web エクスペリエンス管理フレームワーク*は、以前は *FatWire Web Experience Management Framework* と呼ばれていた環境の現在の名前です。このガイドでは、*Oracle WebCenter Sites: Web エクスペリエンス管理フレームワーク*を *Web エクスペリエンス管理フレームワーク*または *WEM フレームワーク*と呼ぶこともあります。

対象読者

このガイドは、WebCenter Sites の全体管理者を対象としています。一部の項は、WebCenter Sites の全体管理者とサイト管理者の両方を対象に書かれています。ユーザーは、所属する企業のサイト・デザインおよび WebCenter Sites データベースのオブジェクト (サイト、ユーザー、ロールおよびデータ・モデルなど) について包括的に理解していることが想定されています。また、WebCenter Sites Representational State Transfer (REST) API にも精通しておく必要があります。この API は、WEM フレームワークに付属しています。

関連ドキュメント

詳細は、次のドキュメントを参照してください。

- *『Oracle WebCenter Sites: Web エクスペリエンス管理フレームワーク REST API リソース・リファレンス』*
- *『Oracle WebCenter Sites Web エクスペリエンス管理フレームワーク開発者ガイド』*

表記規則

このガイドでは、次の表記規則を使用します。

- **太字**は、ユーザーが選択するグラフィカル・ユーザー・インタフェース要素を示します。
- *斜体*は、ドキュメントのタイトル、強調、またはユーザーが特定の値を指定する変数を示します。
- 等幅フォントは、ファイル名、URL、サンプル・コード、または画面に表示されるテキストを示します。
- **等幅太字フォント**は、コマンドを示します。

サード・パーティのライブラリ

Oracle WebCenter Sites およびそのアプリケーションには、サード・パーティのライブラリが含まれています。詳細は、*Oracle WebCenter Sites 11gR1: サード・パーティのライセンス*を参照してください。

第 1 章

Oracle WebCenter Sites: WEM フレームワークへようこそ

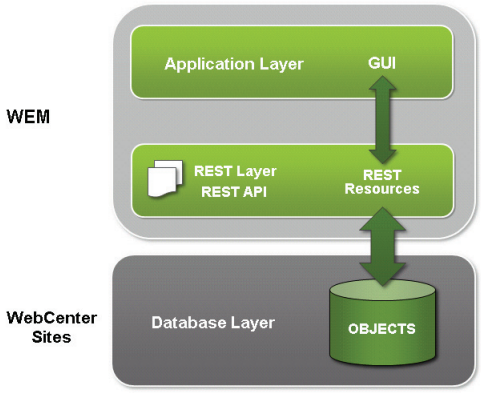
この章では、Oracle WebCenter Sites: Web Experience Management (WEM) Framework およびその管理者の概要について説明します。

この章には次の項が含まれます。

概要

Oracle WebCenter Sites: Web Experience Management (WEM) Framework は、アプリケーションを開発し、それらを Oracle WebCenter Sites に統合するためのテクノロジを提供します。単一の管理インタフェースである WEM Admin には、アプリケーション管理およびユーザー認可が一元化されています。シングル・サインオンを使用すると、ユーザーは一度ログインするだけで、セッションの継続中は使用可能なすべてのアプリケーションにアクセスできます。

WEM フレームワークを使用するには、コンテンツ管理プラットフォームが必要です。このリリースでは、Framework は Oracle WebCenter Sites 上で動作し、WebCenter Sites Representational State Transfer (REST) API に付属しています。WebCenter Sites データベース内のサイト、ユーザーおよびデータ・モデルなどのオブジェクトは、WEM フレームワークで REST リソースにマッピングされます。



WEM フレームワーク上に実装されたアプリケーションは、REST サービスを使用して WebCenter Sites データベースと通信します。このアプリケーションは、WEM Admin で「**アプリケーション**」ページ (図 1) のリスト項目として表示されます。管理者がユーザーを認可する際に、アプリケーションおよびそのリソースへのアクセスが構成されます。そのため、WEM Admin インタフェースでは、**メニュー・バー** のリンクで認可アイテムを (アプリケーションとともに) 公開しています。

図 1: 「アプリケーション」ページ、**WEM Admin**

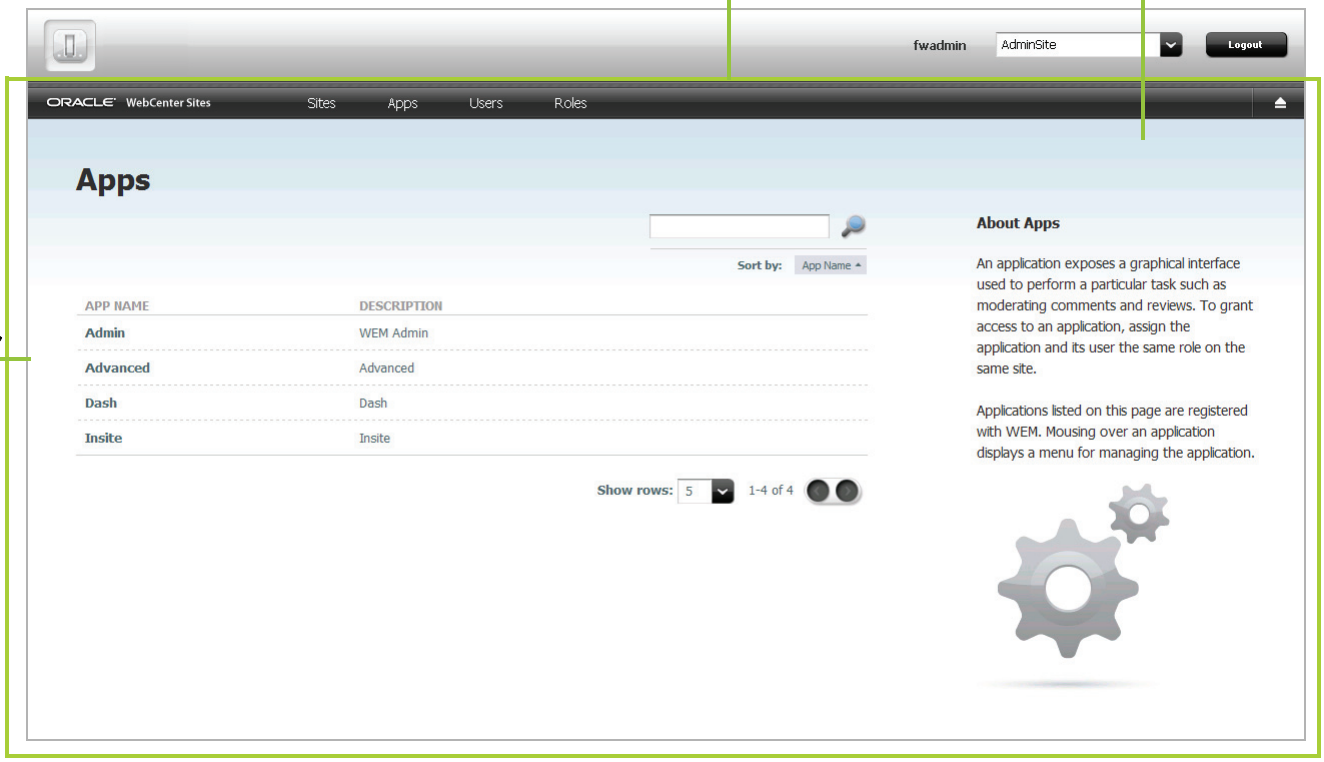
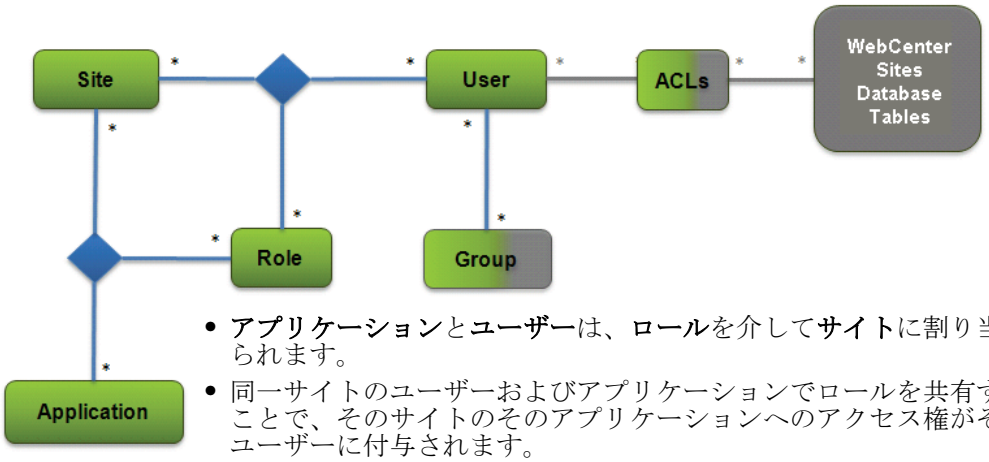


図 2 に示すようにアイテムを結合することによって、ユーザーがアプリケーションを使用できるようにします。

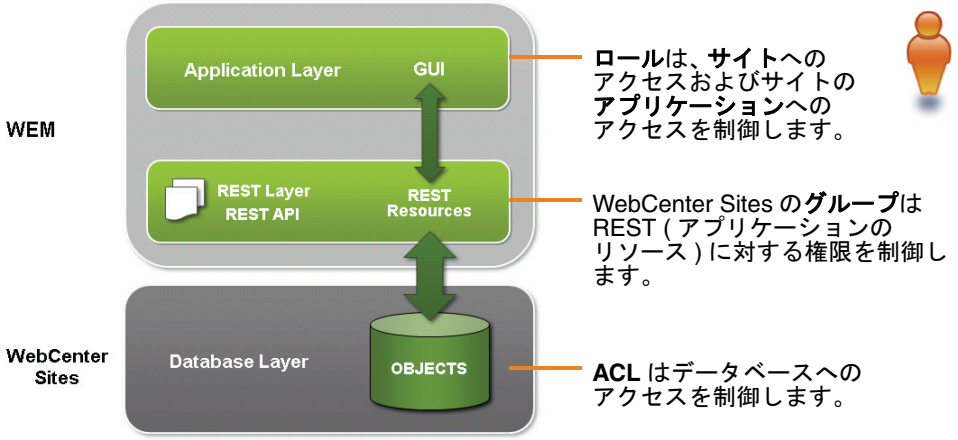
図 2:　　認可モデル



- **アプリケーション**と**ユーザー**は、**ロール**を介して**サイト**に割り当てられます。
- 同一サイトのユーザーおよびアプリケーションでロールを共有することで、そのサイトのそのアプリケーションへのアクセス権がそのユーザーに付与されます。
- ユーザーは**グループ**に割り当てられます。グループは、アプリケーションのリソース (REST レイヤー) へのアクセスを制御します。
- **ACL** はユーザーに割り当てられ、ユーザーにシステムへのアクセス権を付与します。

全体管理者は、WEM Admin を使用して、サイト、アプリケーション、ユーザーおよびロールを作成したり、管理したりできます。グループおよび ACL は、WebCenter Sites Admin インタフェースで構成する必要があります。それらは、WEM Admin のユーザー・アカウントで公開されます。

結合が完了すると、ユーザーは、データベース・レベル、REST レベルおよびアプリケーション・レベルで認可されます。



習熟した WebCenter Sites 管理者であれば、WEM Admin インタフェースによって、アプリケーションへのアクセスを制御するためのサイトおよびロールの用途が広がることを理解するでしょう。ロールをアプリケーション内で使用して、(WebCenter Sites と同様に) インタフェース機能を保護し、それによってアプリケーションのコンテンツへのアクセスを制限できます。

WebCenter Sites と異なり、WEM Admin はデータ・モデルを公開しません。REST API が公開します。この点において WEM Admin は厳密な意味での認可インタフェースと見なすことができ、WebCenter Sites Admin インタフェースはその補助 (ACL およびグループを構成) に使用します。この後は、ユーザーを作成および認可する手順およびサイト管理のガイドラインについて説明します。

管理ロールおよび管理権限

WEM フレームワークでは、全体管理者とサイト管理者の 2 つのタイプの管理者をサポートしています。

全体管理者

全体管理者は、システムを完全に制御し、WEM Admin インタフェースのサイト、アプリケーション、ユーザーおよびロールに対するフル権限を持っています。全体管理者は、WEM Admin を使用して、サイト、アプリケーション、ユーザーおよびロールの追加および削除、それらの詳細の変更、および認可タスクの実行を行うことができます。

WEM フレームワークの全体管理者は、WEM フレームワーク向けに特別に構成されている WebCenter Sites 全体管理者でもあります。デフォルトの全体管理者 (`fwadmin`) は、WebCenter Sites インストール・プロセスの実行中に、自動的に RestAdmin グループに割り当てられて REST サービスへの無制限アクセスを取得し、デフォルトで WEM Admin アプリケーションが実行されている AdminSite 上で有効になっています。***デフォルトの全体管理者は削除しないでください***。

同等な全体管理者を必要な数だけ作成できます。また、既存の全体管理者は、(GeneralAdmin を介して)RestAdmin グループおよび AdminSite に追加することによって変更する必要があります。手順は、20 ページの「ユーザーの作成」を参照してください。WebCenter Sites に対する WEM 関連の詳細は、WebCenter Sites インストレーション・ガイドを参照してください。

サイト管理者

サイト管理者は、全体管理者によって、選択したサイトに割り当てられ、サイトのユーザーおよびアプリケーションを管理します。AdminSite 以外のサイトの `SiteAdmin` ロールが割り当てられたユーザーには、暗黙的に AdminSite の `SiteAdmin` ロールが割り当てられます。***ユーザーに AdminSite のみの `SiteAdmin` ロールを割り当てることはできません。***サイト管理者が WEM Admin インタフェースでアクセスできるのは、「サイト」画面のみです。割り当てられているサイトに対して次の操作を実行できます。

- サイトへのユーザーの割当ておよびサイトからのユーザーの削除
- サイトへのアプリケーションの割当ておよびサイトからのアプリケーションの削除
- サイト・ユーザーのロール割当ての変更
- サイトでのアプリケーションのロール割当ての変更

サイト管理者は、サイト、ユーザーおよびロールを作成、変更または削除できません。(WEM Admin で表示される画面およびインタフェース機能は権限によって決まります。)

WEM フレームワークが稼動している WebCenter Sites システムのサイト管理者は、WEM 向けに特別に構成する必要があります。WebCenter Sites Admin インタフェースで構成されるデフォルトの REST セキュリティ・グループ、SiteAdmin_AdminSite グループに割り当てる必要があります。手順は、20 ページの「ユーザーの作成」を参照してください。

すべての管理者

WEM フレームワークのすべての管理者は、熟練した WebCenter Sites ユーザーである必要があります。

WebCenter Sites のアプリケーション

WebCenter Sites のコントリビュータ・インタフェースおよび Admin インタフェースは、登録済アプリケーションです。これらは、WEM Admin インタフェースの「**アプリケーション**」ページにリストされます。WebCenter Sites ユーザーは、アプリケーション・レベルで認可された後は、WEM フレームワークからアプリケーションにアクセスできます。また、WebCenter Sites アプリケーションには、通常の URL を使用して、引き続き直接アクセス可能です。ログイン画面を次に示します。

サンプル・サイト

使用している WebCenter Sites システムには、サンプル・サイトがインストールされている場合があります。その場合、サンプル・サイトは、WEM Admin インタフェースにカスタム・サイトとともにリストされます。次のサンプル・サイトがあります。

- FirstSiteII
- avisports

クイック・リファレンス

このガイドの最後にあるリファレンス・セクションでは、「クイック・ステップ」を使用して様々な操作の完了手順を示しています。たとえば、ユーザーを WEM フレームワークに追加する必要がある管理者向けに、次のようなクイック・ステップが提示されています。

「管理」アイコンを選択 > **「ユーザー」** > **「ユーザーの追加」** > *必要なフィールドに値を入力* > **「保存して閉じる」**

前述の手順は次のことを意味します。

「管理」アイコンを選択し、**「ユーザー」**メニューを選択し、**「ユーザーの追加」**をクリックし、ユーザー・フォームで必要なフィールドに値を入力し、**「保存して閉じる」**を選択します。

第 2 章

スタート・ガイド

この章では、WEM Admin インタフェースにログインし、移動する手順について説明します。

この章には次の項が含まれます。

ログインおよび「クイック・ツアー」

この項では、Oracle WebCenter Sites にログインすることによって、WEM Admin にアクセスします。サインインすると、WEM フレームワークによってステータスが全体管理者またはサイト管理者に決定され、操作する必要がある画面およびインタフェース機能のみが使用可能になります。**このガイドは全体管理者を対象としています。**全体管理者以外のユーザーには、このガイドの一部の項 (ユーザー作成など) は該当しません。

WEM Admin にアクセスするには :

1. 次の URL で Oracle WebCenter Sites にアクセスします。

   `http://<server>:<port>/<context>/login`

   ここで `<server>` は WebCenter Sites を実行しているサーバーのホスト名または IP アドレス、`<context>` は、サーバー上にデプロイされている Web アプリケーションの名前です。システムの設定によっては、ポート番号も必要になる場合があります。

2. WebCenter Sites のインストール・プロセスで使用した全体管理者としてログインします。

   このガイドでは、全体管理者のデフォルトの資格証明を使用します。

   ユーザー : `fwadmin`
   パスワード : `xceladmin`

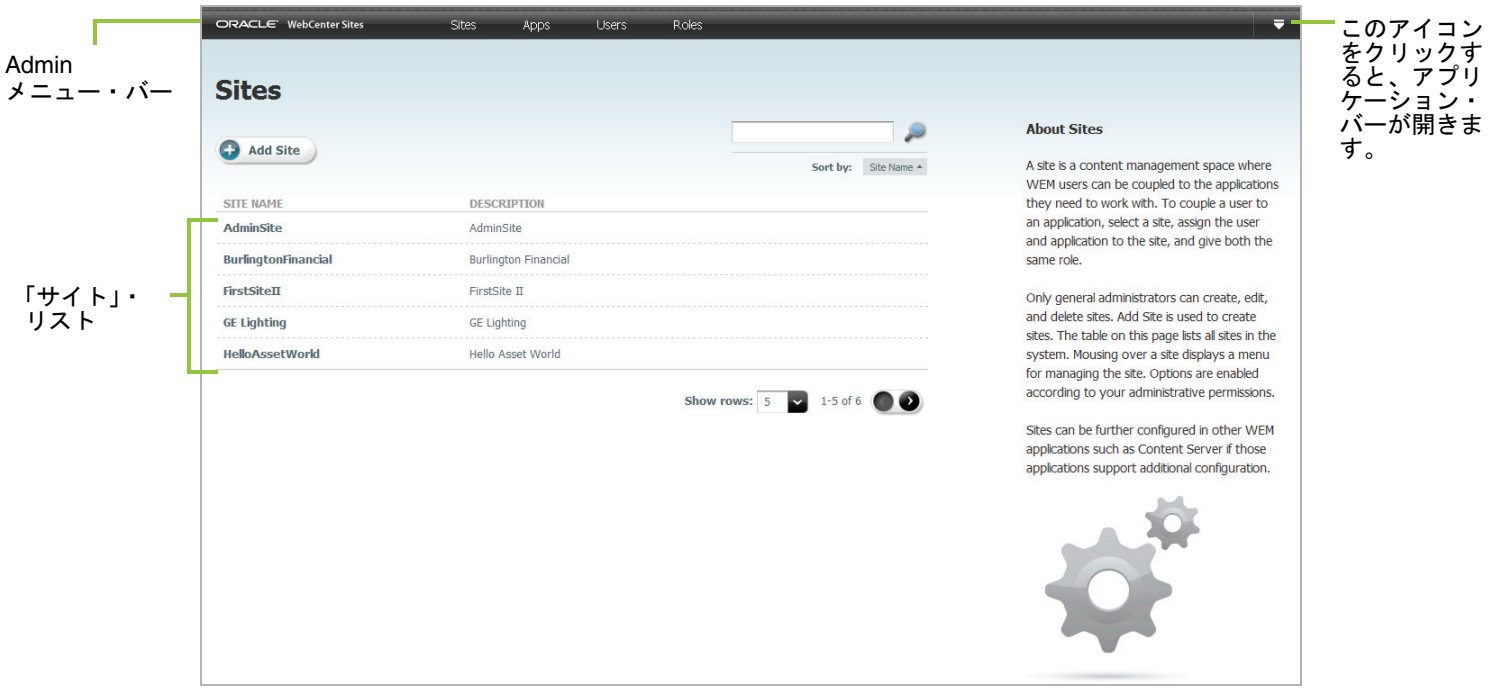
3. 「**ログイン**」をクリックします。

4. 初めてログインする場合またはこれまでアクセスしたことがないサイトにログインする場合、次の画面が表示されます。

AdminSite を選択し、**WEM Admin** アプリケーション アイコンをクリックして、WEM Admin インタフェースを開きます。

最初に表示される画面は、「サイト」画面です。

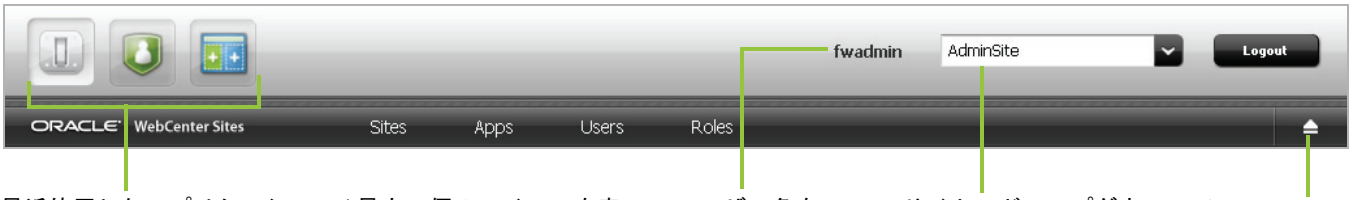
図 3: WEM Admin インタフェースの「サイト」画面



「サイト」画面には、システムのすべてのサイトがリストされます。サイト管理者に表示されるのは、SiteAdmin ロールが割り当てられているサイトのみです。全体管理者としてログインしている場合、「アプリケーション」、「ユーザー」および「ロール」の各画面にもアクセスできます。

5. アプリケーション・バーを開くには、マウスをメニュー・バーの右端の下矢印の上に移動します。このバーには、現在のサイトで使用可能なアプリケーションのアイコン、自身のプロファイルへのリンク、アクセス可能なサイトのドロップダウン・メニュー、ログアウト・ボタンおよびピン・アイコンが表示されます。

図 4: アプリケーション・バー



最近使用したアプリケーション (最大 5 個のアイコンを表示可能)。アプリケーションを使用するには、アイコンをクリックします。

実行中のアプリケーションの数が 5 個より多い場合、「アプリケーションの切替え」ドロップダウン・メニューが表示され、ここに表示されていないアプリケーションも選択できます。「アプリケーションの切替え」メニューからアプリケーションを選択すると、現在表示されているアイコンの中で最も使用頻度の少ないアプリケーションのアイコンが選択したアプリケーションのアイコンに置き換わります。

ユーザー名をクリックすると、自身のプロファイルを管理できます。

サイト・ドロップダウン・メニュー (先行入力検索フィールド)。

現在のサイトが表示されます。

上矢印アイコンをクリックすると、アプリケーション・バーが閉じます (閉じる)。

次の手順

次の章では、WEM Admin インタフェースでユーザーを作成し、アプリケーションの使用を認可する方法について説明します。

第 3 章

ユーザーの作成および認可

この章では、WEM Admin インタフェースでユーザーを作成し、サイトおよびそのサイトで使用可能なアプリケーションを管理するための情報および手順について説明します。

この章には次の項が含まれます。

ユーザーの作成

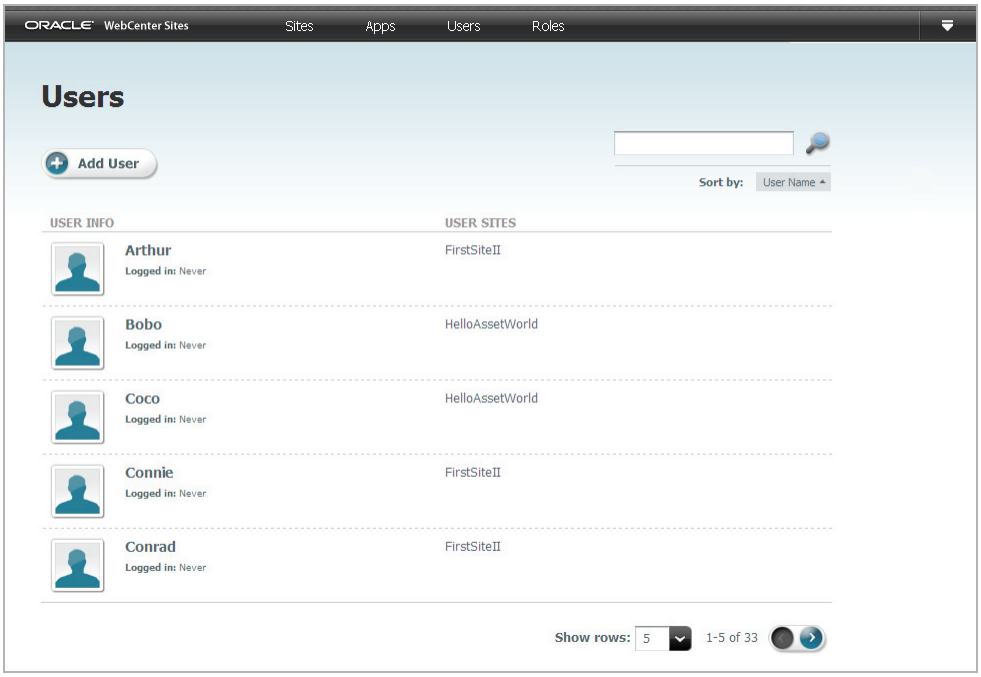
作成できるユーザーのタイプとして、全体管理者、サイト管理者および通常ユーザーがあります。

注意

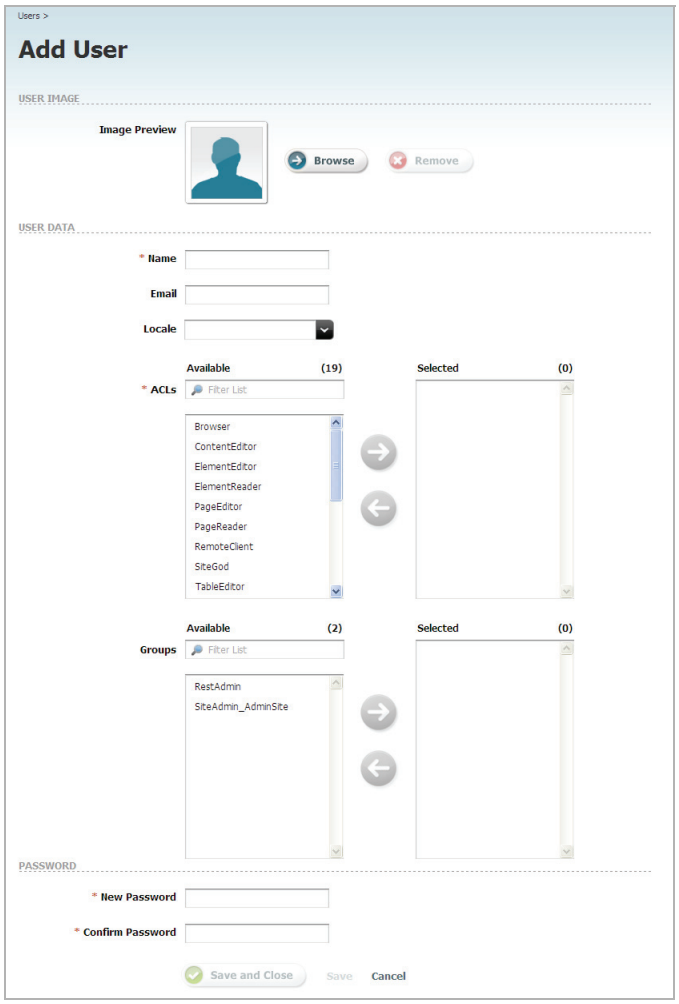
ユーザーを作成できるのは、全体管理者のみです。事前定義済ユーザーの詳細は、31 ページの「事前定義済ユーザーの認可」を参照してください。

ユーザーを作成するには :

1. WebCenter Sites のインストール・プロセスで使用した全体管理者として WEM Admin インタフェースにログインします。
2. Admin メニュー・バーで**「ユーザー」**をクリックします。「ユーザー」画面が表示されます。



3. 「ユーザー」画面で、**「ユーザーの追加」**ボタンをクリックして、「ユーザーの追加」フォームを開きます。



次のフィールドに値を入力します。

- **イメージ・プレビュー**: (オプション) **「参照」**ボタンを使用して、新しいユーザーに写真を関連付けます。
- **名前**: ユーザーがログインする際に使用する名前を入力します。
- **電子メール**: (オプション) 有効な一意の電子メール・アドレスを入力します。
- **ロケール**: (オプション) ユーザーの言語設定を選択します。言語設定を指定しない場合、WEM フレームワークは、ユーザーのブラウザに設定されているデフォルト・ロケールを使用します。
- **ACL**: ACL は、ユーザーによるデータベース表に対するアクセスを制限します。すべてのユーザーに、Browser、ElementReader、PageReader、UserReader および xceleditor が必要です。全体管理者とサイト管理者は、xceladmin も必要です。全体管理者にはさらに TableEditor と UserEditor も必要です (WebCenter Sites Engage を使用する場合は VisitorAdmin も必要)。

- **グループ**: グループは、REST に対するアクセスを提供します。それらは、アプリケーションのリソースへのアクセスの制御に使用します。
  - 全体管理者にするユーザーを作成している場合は、ユーザーを RestAdmin グループ (WebCenter Sites Admin インタフェースで構成されるデフォルト・グループ) に割り当てます。このグループには、REST リソースに対する無制限の権限があります。
  - サイト管理者にするユーザーを作成している場合は、ユーザーを SiteAdmin_AdminSite グループ (WebCenter Sites Admin インタフェースで構成されるデフォルト・グループ) に割り当てます。

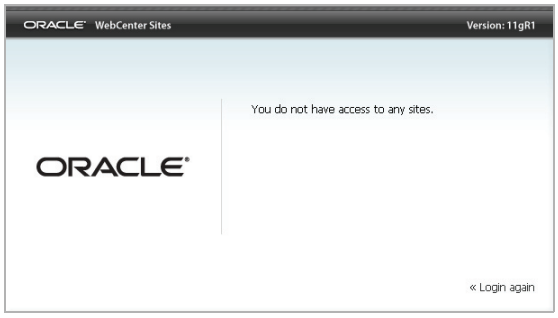
    注意

    グループのセキュリティ構成は、WebCenter Sites Admin インタフェースで実行できます。38 ページの「REST セキュリティ構成の表示」を参照してください。

  - 通常ユーザーを作成している場合は、とりあえずこの手順をスキップします。ユーザーのグループへの割当ては、認可プロセス (「アプリケーション使用のユーザーへの認可」) の一環として 28 ページの手順 4 で実行します。
- **新規パスワード**: パスワードを 6 文字以上で入力します。
- **パスワードの確認**: 上で入力したパスワードを再入力します。

4. **「保存して閉じる」**をクリックします。

   この時点で、ユーザーはログインできますが、どのサイトにもアクセスできないことを示すメッセージが表示されます。



ユーザーを管理者または通常ユーザーとして有効にするには :

5. ユーザーをサイトに割り当てます。
   a. 「ユーザー」画面で、ユーザーの上にマウスを移動して**「ユーザーの管理」**を選択し、**「サイトへの割当て」**をクリックします。
      - 全体管理者にするユーザーを作成している場合は、ユーザーを AdminSite に割り当てます。
      - サイト管理者にするユーザーまたは通常ユーザーを作成している場合は、ユーザーを AdminSite 以外のサイトに割り当てます。

b. 割り当てたサイトでロールをユーザーに割り当てます。

- 全体管理者にするユーザーを作成している場合は、GeneralAdmin を割り当てます。このロールは、システムへのアクセス権をユーザーに付与します。

  これで、ユーザーは、AdminSite で WEM Admin アプリケーションを使用できるようになります。

作成したユーザーは、このメニューから AdminSite にのみアクセスできます。別のサイトにアクセスできるようにするには、ユーザーに目的のサイトでロールを割り当てる必要があります。ロールを割り当ててもそのサイトのアプリケーションへのアクセスが認可されない場合は、ユーザーがそのサイトを選択しても、メニューの下にアプリケーション・アイコンは表示されません。

- サイト管理者にするユーザーを作成している場合は、SiteAdmin ロールを割り当てます。

  AdminSite 以外のサイトで SiteAdmin ロールを割り当てられたユーザーは、暗黙的に AdminSite に割り当てられ、AdminSite の WEM Admin アプリケーションにアクセスできるようになります。ユーザーが WEM Admin アプリケーションでアクセスできるのは「サイト」画面のみです。この画面には、ユーザーに SiteAdmin ロールが割り当てられているサイトのみがリストされます。

作成したユーザーはこのメニューから AdminSite、および SiteAdmin ロールを割り当てられているサイトに、アクセスできます。ユーザーに SiteAdmin ロールを割り当ててもそのサイトのアプリケーションへのアクセスが認可されない場合は、ユーザーがそのサイトを選択しても、メニューの下にアプリケーション・アイコンは表示されません。

- 通常ユーザーを作成している場合は、ユーザーに GeneralAdmin でも SiteAdmin でもないロールを割り当てます。

  これでユーザーは (メニューにリストされている) サイトにアクセスできるようになりますが、ユーザーに割り当てられているロールでそのサイトのアプリケーションへのアクセスが認可されない場合は、メニューの下にアプリケーション・アイコンは表示されません。

6. アプリケーションの使用をユーザーに認可するには、次の項に進みます。

アプリケーション使用のユーザーへの認可

ユーザーは、WebCenter Sites コントリビュータ・インタフェースなどのアプリケーションを使用する認可を必要とします。ユーザーを認可することは、10 ページの図 2 に示す結合を複製することです。

この項ではユーザーを認可する手順を示しますが、主な流れは次のとおりです。

1. サイトを選択または作成する
2. アプリケーションをサイトに割り当てる
3. 同じサイトにユーザーを割り当てて、ユーザーとアプリケーションを結合する
4. ユーザーをグループに割り当てて、ユーザーの REST (アプリケーションのリソース) に対する権限を有効にする

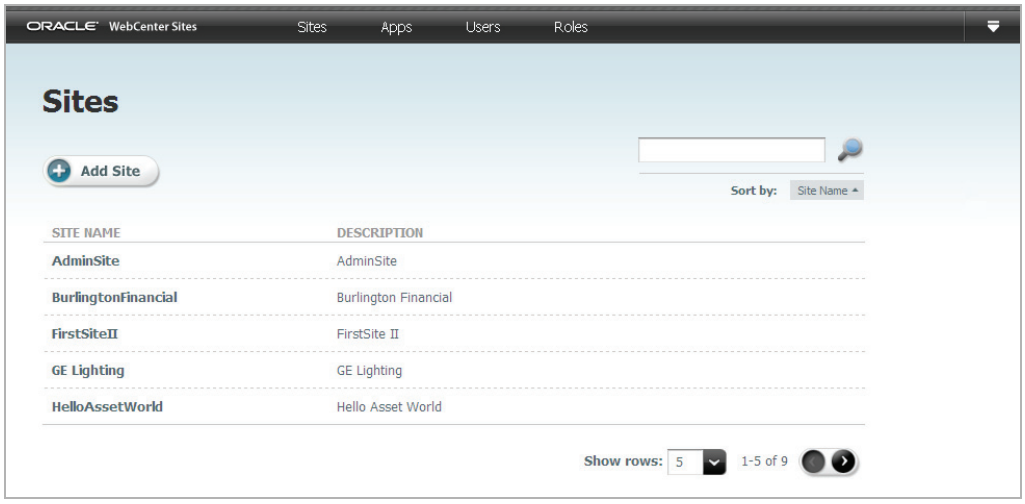
注意

- 全体管理者とサイト管理者はどちらもユーザーを認可できます。
- 特定のサイトのアプリケーションへのアクセスが必要な場合、そのサイトのそのアプリケーションへのアクセスを自身に認可します。
- この後の手順では、複数のアプリケーションおよび複数のユーザーを選択できます。わかりやすくするために、手順では 1 つのアプリケーションおよび 1 人のユーザーを指定します。
- この手順では、認可対象のユーザーは、事前定義済ユーザーが指定されていないアプリケーションを使用するものと想定しています。事前定義済ユーザーの詳細は、31 ページの「事前定義済ユーザーの認可」を参照してください。

ユーザーを認可するには :

1. **サイトを選択または作成します。**

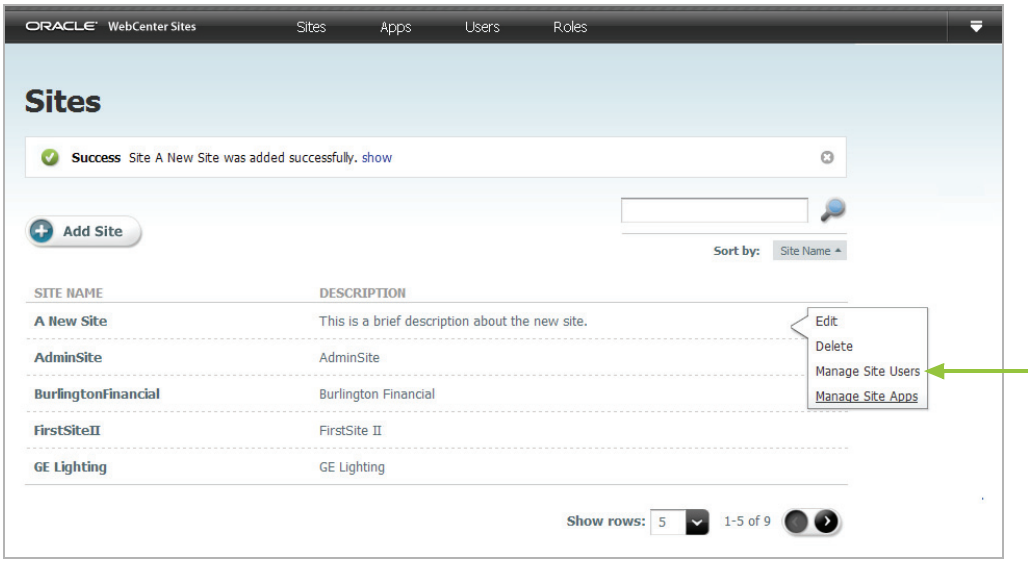
   WEM Admin インタフェースの Admin メニュー・バーで**「サイト」**をクリックします。



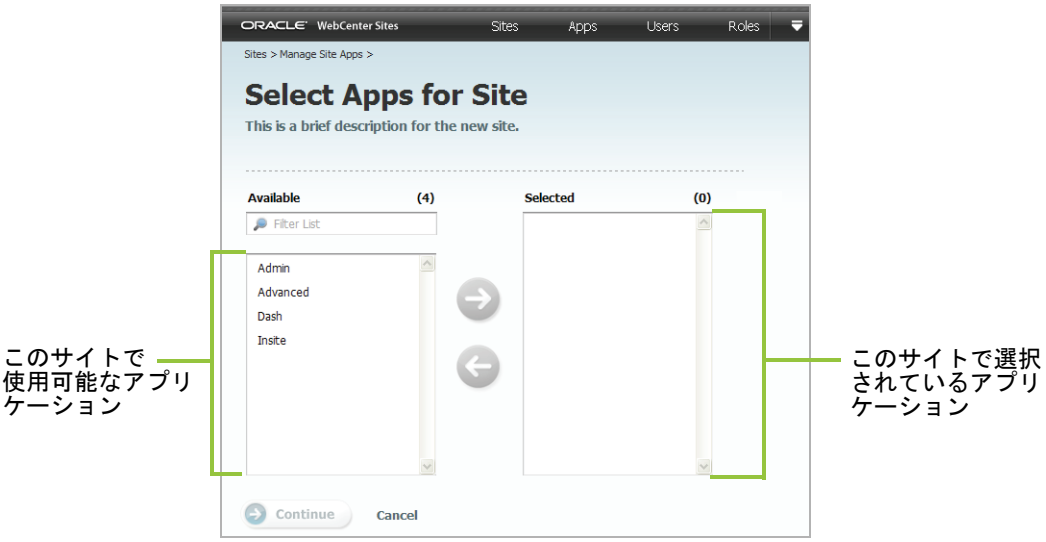
   全体管理者は、サイトを選択するか、または (**「サイトの追加」**をクリックして) サイトを追加できます。サイト管理者は、サイトを選択できます。「サイト」画面には、管理することを許可されているサイトのみがリストされます。

2. **アプリケーションをサイトに割り当てます。**

   a. 「サイト」画面で、サイトの上にマウスを移動して**「サイト・アプリケーションの管理」**をクリックします。



b. 「**アプリケーションの割当て**」をクリックします。



注意

WEM フレームワークにアプリケーションが登録されていない場合、「**アプリケーションの割当て**」ボタンは淡色で表示されます。

1) サイトに割り当てるアプリケーションを選択し、「**選択済**」リスト・ボックスに移動します。(アプリケーションを検索するには、その名前を「**フィルタ・リスト**」フィールドに入力します。結果は「**使用可能**」リスト・ボックスに表示されます)。

2) 「**続行**」をクリックして、ロールをアプリケーションに割り当てます。

c. 「アプリケーションへのロールの割当て」フォームで、アプリケーションに割り当てるロールを選択し、「**選択済**」リスト・ボックスに移動します。

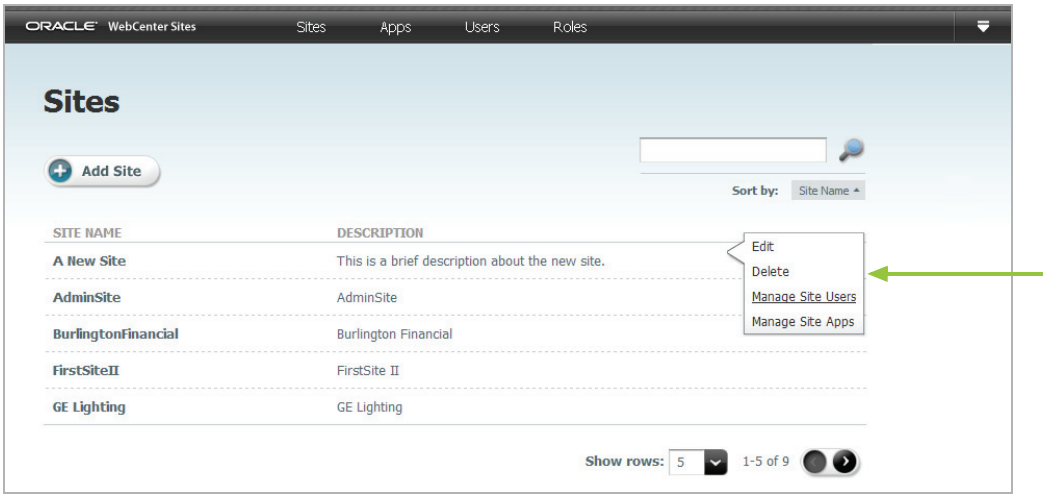
注意

アプリケーションが WebCenter Sites Admin インタフェースである場合は、AdvancedUser ロールを割り当てます。アプリケーションが WebCenter Sites コントリビュータ・インタフェースである場合は、SitesUser ロールを割り当てます。

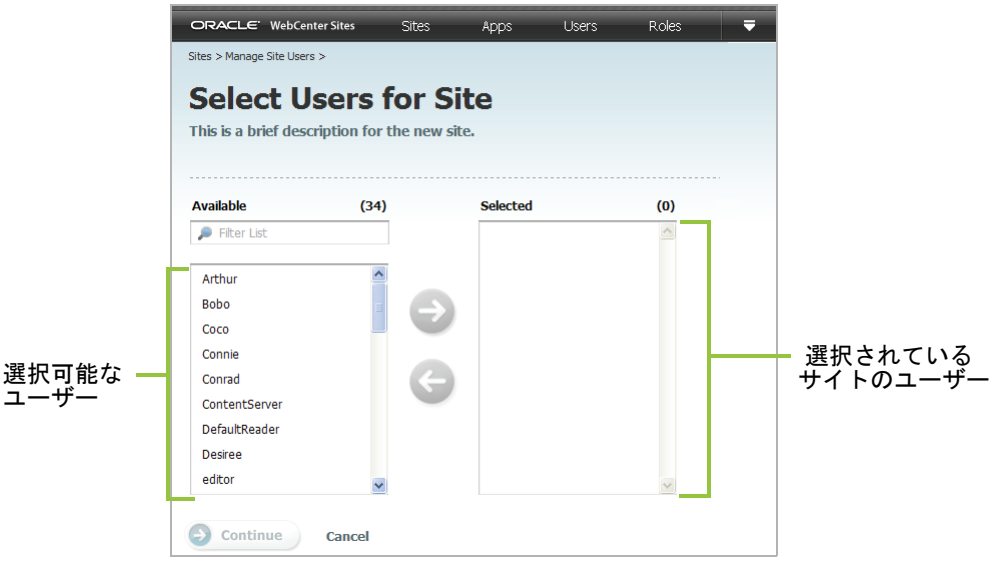
割り当てているロールを記録します。このサイトで、これらのロールのうち少なくとも 1 つをユーザーに割り当てて、ユーザーにこのアプリケーションへのアクセス権を付与します。

d. 「**保存して閉じる**」をクリックします。

3. **ユーザーをサイトに割り当てます。**
   a. Admin メニュー・バーで「**サイト**」をクリックします。
   b. 新しいサイトの名前の上にマウスを移動して「**サイト・ユーザーの管理**」をクリックします。



   c. 「**ユーザーの割当て**」をクリックします。



      1) 「サイトのユーザーの選択」フォームでサイトに割り当てるユーザーを選択し、「**選択済**」リスト・ボックスに移動します。
      2) 「**続行**」をクリックして、ロールをユーザーに割り当てます。

d. ユーザーをアプリケーションに結合します (アプリケーション・レベルの認可)。

「ユーザーへのロールの割当て」フォームで、26 ページの手順 c でアプリケーションに割り当てたロールのうち少なくとも 1 つをユーザーに割り当てます。

注意

- **すべてのアプリケーションの場合。**サイトのユーザーおよびアプリケーションでロールを共有することで、そのサイトのそのアプリケーションへのアクセス権がそのユーザーに付与されます。アプリケーションが WebCenter Sites Admin インタフェースである場合は、AdvancedUser ロールを割り当てる必要があります。アプリケーションが WebCenter Sites コントリビュータ・インタフェースである場合は、SitesUser ロールを割り当てる必要があります。
- **WebCenter Sites 以外のアプリケーションの場合。**アプリケーションにロールによって保護されているインタフェース機能 (「編集」など) がある場合、機能のロール (仕様はアプリケーション開発者から入手可能) のうち少なくとも 1 つをユーザーに割り当てることによって、各機能に対するアクセスを構成します。それによって、ユーザーがアプリケーション・レベルで完全に認可されます。ただし、ユーザーは REST レベルで認可されない限り、アプリケーションのリソースを使用することはできません。**「保存して閉じる」**をクリックして、手順 4 に進みます。
- **WebCenter Sites のアプリケーションおよびユーザーの場合。**WebCenter Sites には、ロールで保護されているインタフェース機能があります。WebCenter Sites で直接構成されているユーザーの場合、そのロールは WEM フレームワークで維持されます。それらは、WEM Admin インタフェースでサイト別にリストされます。また、`application` REST サービスによって、REST レベルで WebCenter Sites ユーザーが認可されます (管理者が手順 4 を実行する必要がなくなります)。**「保存して閉じる」**をクリックして、29 ページの手順 5 に進んでください。

4. ユーザーを REST レベルで認可します。

この手順では、(25 ページの手順 2 で選択した) アプリケーションが使用しているリソースを操作する権限をユーザーに付与します。

前述したように、WEM フレームワークから WebCenter Sites アプリケーションへのアクセスを WebCenter Sites 専用ユーザーに認可している場合は、この手順をスキップします。29 ページの手順 5 に進んでください。

a. Admin メニュー・バーで**「ユーザー」**をクリックします。

b. 「ユーザー」画面で、認可するユーザーの上にマウスを移動して**「編集」**をクリックします。

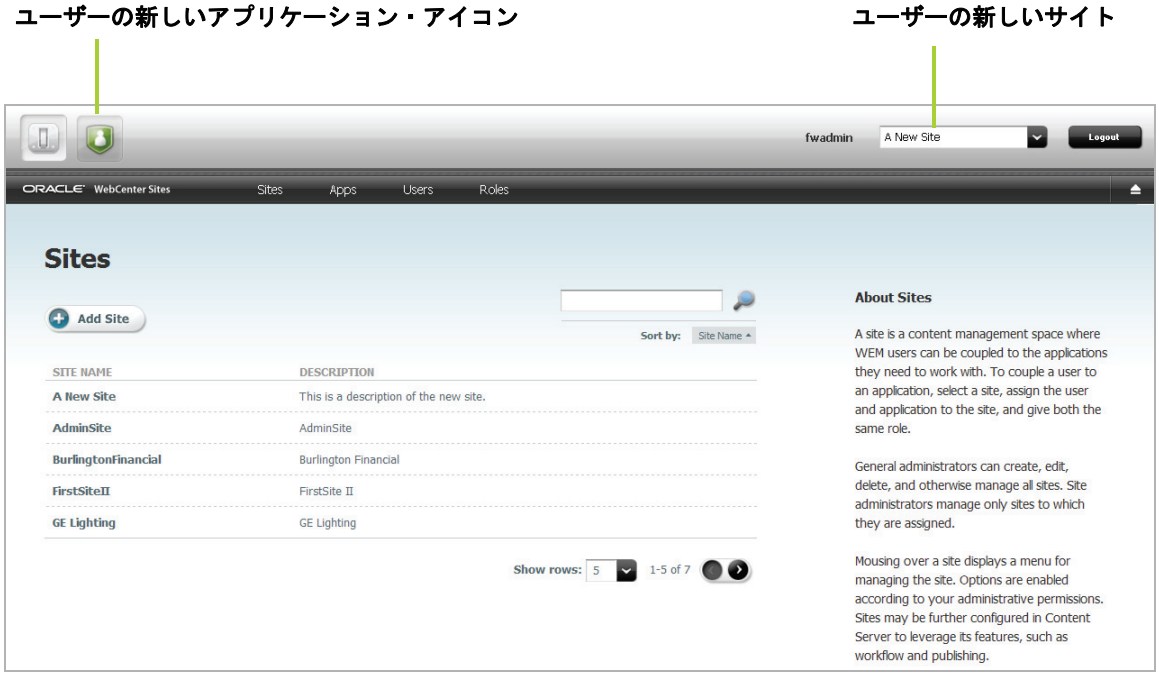
c. 「ユーザーの編集」フォームで、ユーザーのグループを選択します。各グループは、特定のオブジェクト (アセット・タイプ、アセットなど) を操作する特定の権限で構成されています。オブジェクトはアプリケーションが使用する REST リソースにマッピングされています。リストされている REST グループの権限を決定するか、またはグループを作成してその権限を構成するには、37 ページの「アプリケーション・リソースへのアクセスのユーザーへの認可」を参照してください。

d. **「保存して閉じる」**をクリックします。

5. ユーザーが新しいアプリケーションにアクセスできることを検証します。

   ログイン画面にユーザーの新しいサイトが (「サイト」ドロップダウン・メニューに) リストされ、メニューの下にアプリケーション・アイコンが表示されます。

新しいサイトは、ログイン・ユーザーの名前の横のドロップダウン・メニューにもリストされます。アプリケーション・アイコンは、左上隅に表示されます。



6. まだ REST に対する権限をユーザーに付与していない場合、第 4 章「REST セキュリティの構成」の手順を完了してください。

   サイトに割り当てられているユーザーまたはアプリケーション、あるいはその両方を確認または変更する必要がある場合、第 6 章「WEM Admin クイック・リファレンス」を参照してください。

事前定義済ユーザーの認可

開発者は、アプリケーションで事前定義済ユーザーを指定することによって、管理者の認可プロセスを単純化します。各ユーザーを個別に REST レベルで認可するかわりに、事前定義済ユーザーを認可します。アプリケーションへのアクセス権を持つログイン・ユーザーは、事前定義済ユーザーが REST グループに属することを通じて、アプリケーションのリソースにアクセスできます。

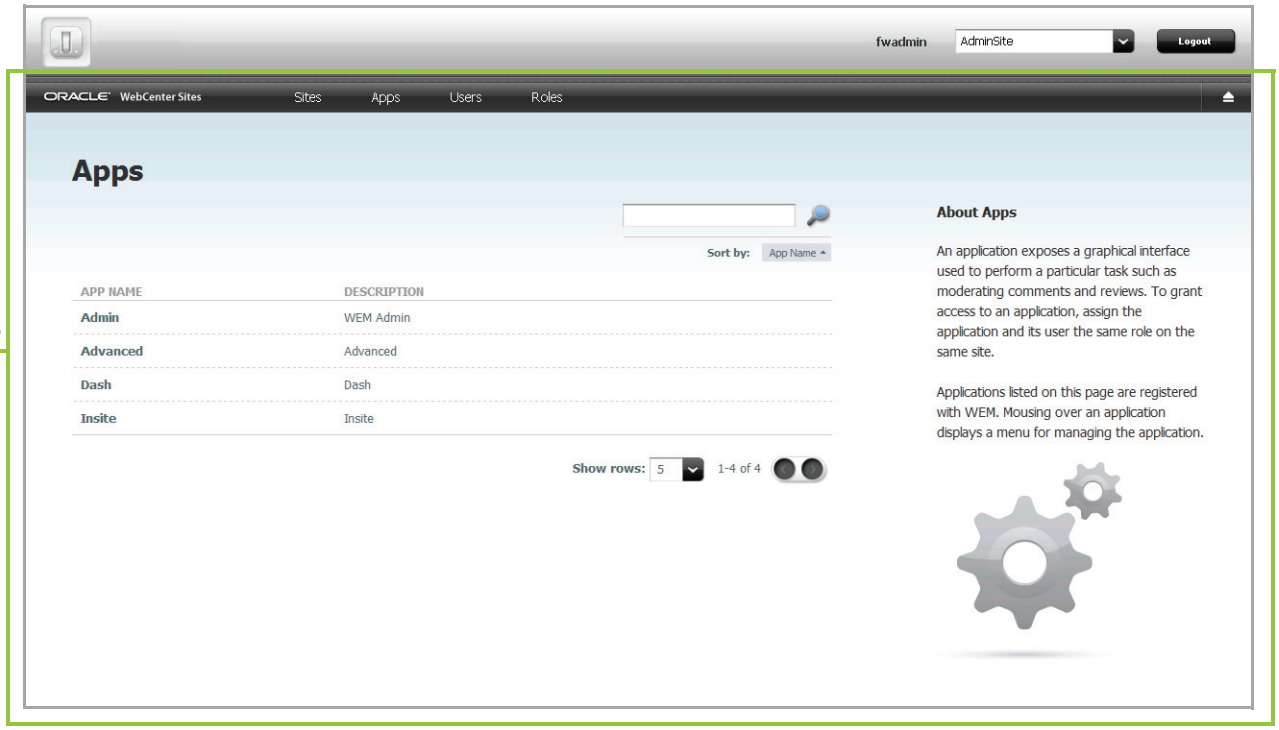
アプリケーションに事前定義済ユーザーが構成されている場合、WEM Admin アプリケーションで次のステップを完了します。

1. 事前定義済ユーザーを作成します。次の情報を準備します。
   - ログイン名。この名前は、アプリケーションで指定されている事前定義済ユーザーの名前と正確に一致する必要があります。
   - パスワード。このパスワードは、アプリケーションで指定されている事前定義済ユーザーのパスワードと正確に一致する必要があります。
   - ACL。ユーザーによるデータベース表に対するアクセスを制限します。事前定義済ユーザーには、アプリケーションにアクセスするログイン・ユーザーの ACL が割り当てられている必要があります。すべてのユーザーに、Browser、ElementReader、PageReader、UserReader および xceleditor が必要です。全体管理者とサイト管理者は、xceladmin も必要です。全体管理者にはさらに TableEditor と UserEditor も必要です (WebCenter Sites Engage を使用する場合は VisitorAdmin も必要)。
   - グループ割当て。(アプリケーション・リソースの管理を)REST レベルでユーザーを認可します。事前定義済ユーザーを使用しない場合にアプリケーション・ユーザーに付与したであろうセキュリティ権限を持つグループに、事前定義済ユーザーを割り当てる必要があります。REST セキュリティの構成の詳細は、第 4 章を参照してください。

   ユーザーを作成する手順の詳細は、20 ページの「ユーザーの作成」を参照してください。
2. 事前定義済ユーザーをアプリケーションに割り当てます。手順は、24 ページの「アプリケーション使用のユーザーへの認可」を参照してください。
3. (24 ページの「アプリケーション使用のユーザーへの認可」の手順を使用して) ユーザーをアプリケーションに割り当てます。ただし、グループへの割当て (28 ページの手順 4) はスキップしてください。

アプリケーション登録の開発者への認可

アプリケーションを WEM フレームワークで公開するには、アプリケーションを登録する、すなわちアセットとして作成して、WEM Admin インタフェースの「アプリケーション」ページに REST サービスを介して表示できるようにする必要があります。これによって、管理者は、ユーザーによるアプリケーション使用を認可できるようになります。



アプリケーション・リスト

通常は、開発者が、自身が作成したアプリケーションを登録します。望ましいのは、プログラムによる方法です。開発者がアプリケーションを手動で登録する場合は、WebCenter Sites Admin インタフェースを使用して、`FW_Application` タイプおよび `FW_View` タイプのアセットを作成する必要があります。これらのアセット・タイプは、AdminSite で有効です。(アプリケーションの登録の基礎情報は、*『Oracle WebCenter Sites Web エクスペリエンス管理フレームワーク管理者ガイド』* を参照してください。)

開発者を認可するには、開発者が全体管理者であること (すなわち、REST サービスも含めて、システムに対する全権限を持っていること) を確認します。全体管理者を作成する手順の詳細は、20 ページの「ユーザーの作成」を参照してください。

開発者への確認

アプリケーションおよびユーザーに対して有効な管理を実践できることを保証するために、WEM フレームワーク向けに作成されているアプリケーションに関する情報をその開発者から入手する必要があります。

リソースとアプリケーション

カスタム構築アプリケーションで使用されているリソースについて、その開発者に確認します。

ユーザーが使用するアセット・タイプ、アセットおよび他のリソースが判明したら、それらのリソースに対してユーザーに付与する必要がある権限 (作成、更新など) を決定し、それらの権限を持つグループにユーザーを割り当てることができます。グループの構成およびユーザーの割当ての詳細は、第 4 章「REST セキュリティの構成」を参照してください。

ロールとアプリケーション

アプリケーションのインタフェース機能がロールで保護されているかどうかを開発者に確認します。

WEM では、アプリケーションへのアクセスを管理するためにロールを使用します。同一サイトのユーザーおよびアプリケーションでロールを共有することで、そのサイトのそのアプリケーションへのアクセス権がそのユーザーに付与されます。また、ロールをアプリケーション・コードで使用して、「編集」などのインタフェース機能を保護できます。ロールで保護されている機能が指定されているアプリケーションでは、アプリケーション・ユーザーは各インタフェース機能と少なくとも 1 つのロールを共有する必要があります。適切な認可を保証するには、24 ページの「アプリケーション使用のユーザーへの認可」を参照してください。

事前定義済ユーザー

アプリケーションで事前定義済ユーザーが構成されているかどうかを開発者に確認します。

アプリケーションで事前定義済ユーザーが指定されている場合、アプリケーションのすべてのユーザーを個別に認可するのではなく、REST レベルで事前定義済ユーザーを認可する必要があります。グループに属していることによって事前定義済ユーザーに付与されているセキュリティ権限は、ログイン・ユーザーがアプリケーションにアクセスする際に、ログイン・ユーザーに付与されます。事前定義者を認可する手順の詳細は、31 ページの「事前定義済ユーザーの認可」を参照してください。

第 4 章

REST セキュリティの構成

この章では、REST セキュリティを構成するための情報および手順について説明します。次の項があります。

- REST 認可
- アプリケーション・リソースへのアクセスのユーザーへの認可
- REST セキュリティ構成リファレンス

REST 認可

REST 認可は、アプリケーションのリソースに対して REST 操作を実行する権限を付与するプロセスです。アプリケーションのリソースは、WebCenter Sites のオブジェクトにマップされます。REST 認可は、「デフォルトですべて拒否」モデルを使用します。すなわち、権限が特定のグループに明示的に付与されていない場合、その権限は拒否されています。アプリケーションのデプロイおよび WEM フレームワークへの登録が完了した後、ユーザーを認可するのは、全体管理者の責任です。

セキュリティ・モデル

WEM セキュリティ・モデルは、WebCenter Sites で事前定義されているオブジェクトとグループ、および WebCenter Sites で作成するアクションをベースにしています (WebCenter Sites のオブジェクトは WEM フレームワークの REST リソースにマッピングされます)。セキュリティは、WebCenter Sites Admin インタフェースで、オブジェクト・タイプごとに構成する必要があります。

- **オブジェクト**は、サイト、ユーザーまたはアセットなどの任意のエンティティを参照する一般的用語です。保護されているオブジェクトとして、次のタイプのオブジェクトがあります。

  - アセット・タイプ
  - サイト
  - ユーザー・ロケール
  - アプリケーション
  - アセット
  - ロール
  - ACL
  - 索引
  - ユーザー
  - グループ

- **セキュリティ・グループ**は、ユーザーの (オブジェクトに対する操作) 権限を一括管理するためにユーザーをグループ化します。
- アクションとは、リスト、先頭、読取り、更新、作成、削除の各セキュリティ権限です。グループには、そのグループに許可されるオブジェクト操作権限が割り当てられます。ACL など、一部のオブジェクトは、リストのみです (REST を介さず WebCenter Sites で直接作成できます)。

セキュリティ構成は、前述のように、次の情報を指定する配列です。

- 保護されているオブジェクト・タイプおよびオブジェクト
- オブジェクトにアクセス可能なグループ
- グループ (およびそのメンバー) がオブジェクトに対して実行できるアクション

REST セキュリティの構成

REST セキュリティの構成手順は、37 ページの「アプリケーション・リソースへのアクセスのユーザーへの認可」を参照してください。

権限解決アルゴリズム

セキュリティ権限を構成する際、権限を適用する対象として、特定のタイプのすべてのオブジェクトまたは特定のタイプの単一オブジェクトを指定できます。たとえば、任意のサイトに対する UPDATE (POST) 権限を付与することは、WEM フレームワークのすべてのサイトの詳細を変更することをグループ内のユーザーに許可することです。FirstSiteII サイトに対する UPDATE (POST) 権限を付与することは、WEM でそのサイトの詳細を変更することをグループ内のユーザーに許可することです。

Asset オブジェクト・タイプの場合、セキュリティ設定を適用するサイトを指定する必要があります。これは、アセットが常に特定のサイトからアクセスされるからです。AssetType オブジェクト・タイプはサブタイプを指定して拡張することができます。サブタイプを使用すると、より詳細にセキュリティを構成できます。たとえば、アセット・タイプ Content_C に対する DELETE 権限を設定すると、REST リソース /types/Content_C に対して DELETE リクエストを実行できます (すなわち、システムから Content_C アセット・タイプを削除できます)。

権限はグループにのみ付与できるので、特定のユーザーの全権限は、そのユーザーが属するすべてのグループを集計するまで明らかになりません。WEM フレームワークには、権限解決アルゴリズムが用意されています。その基本手順を次に示します。

1. REST は、ユーザーが属しているグループを検出します。
2. REST は、どのグループがどの REST リソースに対してどの REST 操作を実行できるかを決定します。サイトまたはサブタイプが指定されている場合は、それぞれ考慮します。
3. REST は、手順 1 と手順 2 の結果を比較します。手順 1 で得られたグループの少なくとも 1 つが手順 2 で得られたグループのリストに存在する場合、アクセスは許可されます。それ以外の場合、アクセスは拒否されます。

アプリケーション・リソースへのアクセスのユーザーへの認可

この項の続きを読む前に、次の手順に関する基本情報として「REST 認可」を読んでください。

- REST セキュリティ構成の表示
- グループの作成
- グループへのユーザーの追加

- REST リソースのセキュリティの構成 .

注意

REST リソースのセキュリティを構成するには、グループが必要です。権限はグループに割り当てます。グループのリストを表示するには、次の手順に進みます。グループを作成するには、40 ページの「グループの作成」を参照してください。

REST セキュリティ構成の表示

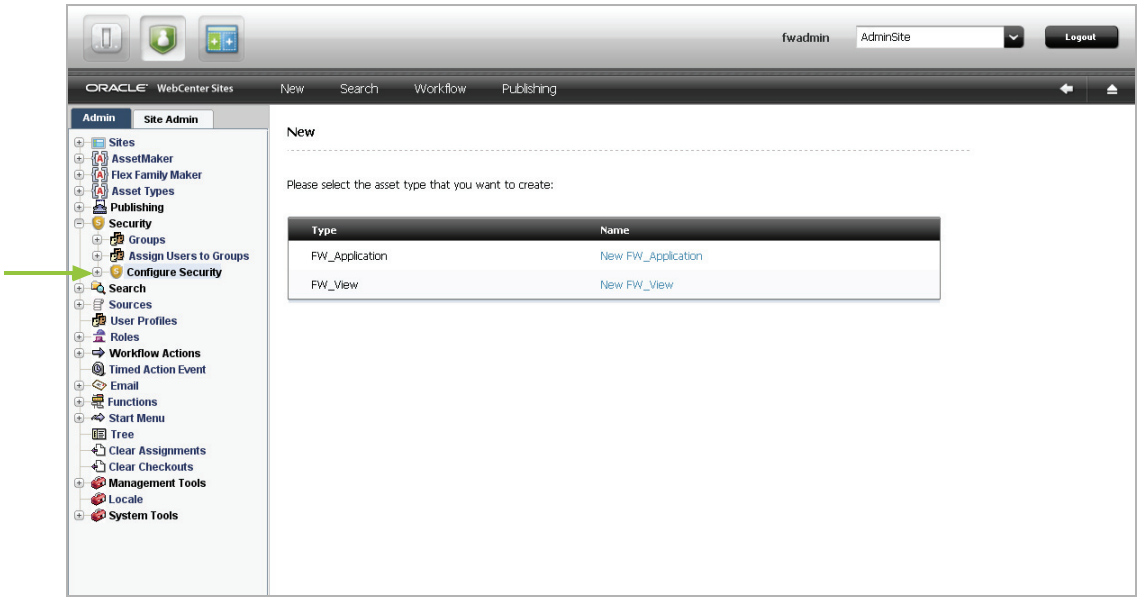
セキュリティ構成では、どのグループがどの REST リソースに対するどの権限を持っているかを指定します。WebCenter Sites では、2 つのデフォルト・グループのセキュリティ構成が定義されています。これらは、RestAdmin と SiteAdmin_AdminSite です。

REST セキュリティ構成を表示するには :

1. 一般的な管理者として、WebCenter Sites Admin インタフェースにログインします。
   a. 次の URL に移動します。

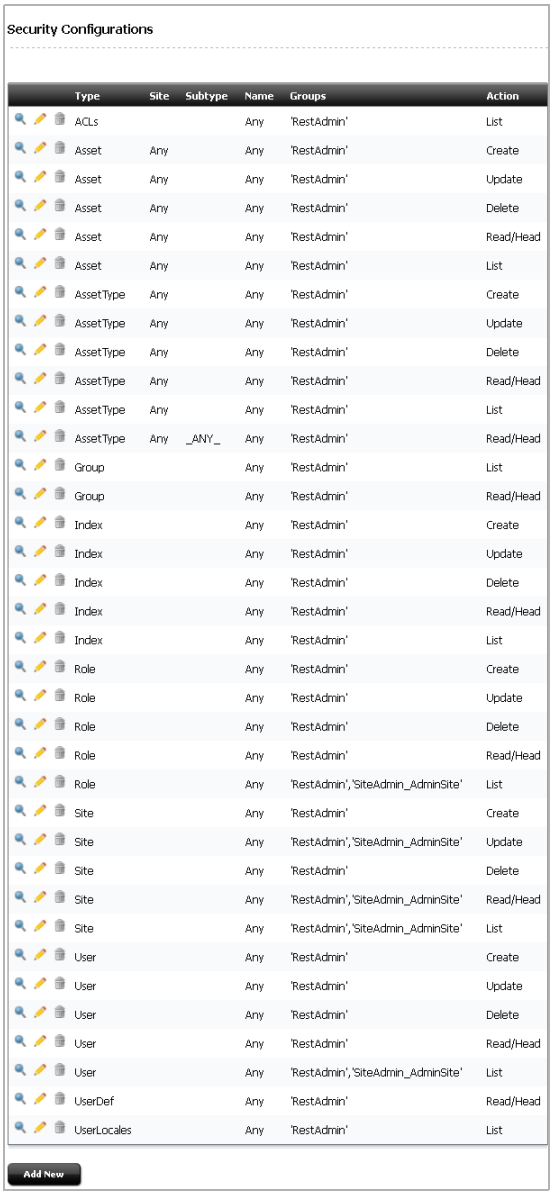
      `http://<server>:<port>/<cs_context>/Xcelerate/LoginPage.html`

   b. ユーザー名とパスワードを入力します。
   c. 「ログイン」をクリックします。
2. 「管理」タブを選択して「セキュリティ」ノードを開き、「セキュリティの構成」をダブルクリックします。



「セキュリティの構成」画面が表示されます。

「セキュリティの構成」画面：



3. 目的に応じて、次の指示に従います。
   - 新しいグループを作成するには、40 ページの「グループの作成」を参照してください。
   - グループにユーザーを追加するには、42 ページの「グループへのユーザーの追加」を参照してください。

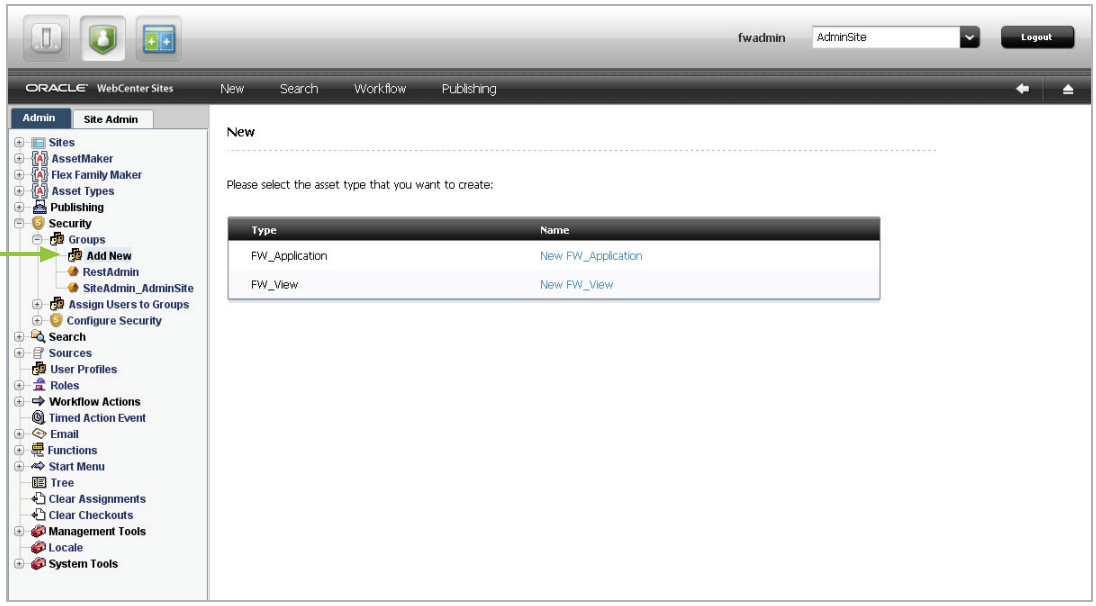
- REST リソースのセキュリティ権限を構成するには、45 ページの「REST リソースのセキュリティの構成」を参照してください。

注意

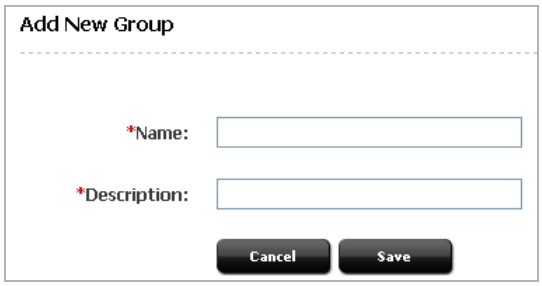
この手順を完了するために、必要なグループが存在することを確認します。権限はグループに割り当てます。

グループの作成

1. 一般的な管理者として、WebCenter Sites Admin インタフェースにログインします。
   a. 次の URL に移動します。
      `http://<server>:<port>/<cs_context>/Xcelerate/LoginPage.html`
   b. ユーザー名とパスワードを入力します。
   c. 「**ログイン**」をクリックします。
2. WebCenter Sites ツリーで「**管理**」タブを選択し、「**セキュリティ**」>「**グループ**」の順に開いて、「**新規追加**」をダブルクリックします。



3. 「新規グループの追加」フォームで、作成するグループの名前と簡単な説明を入力します。



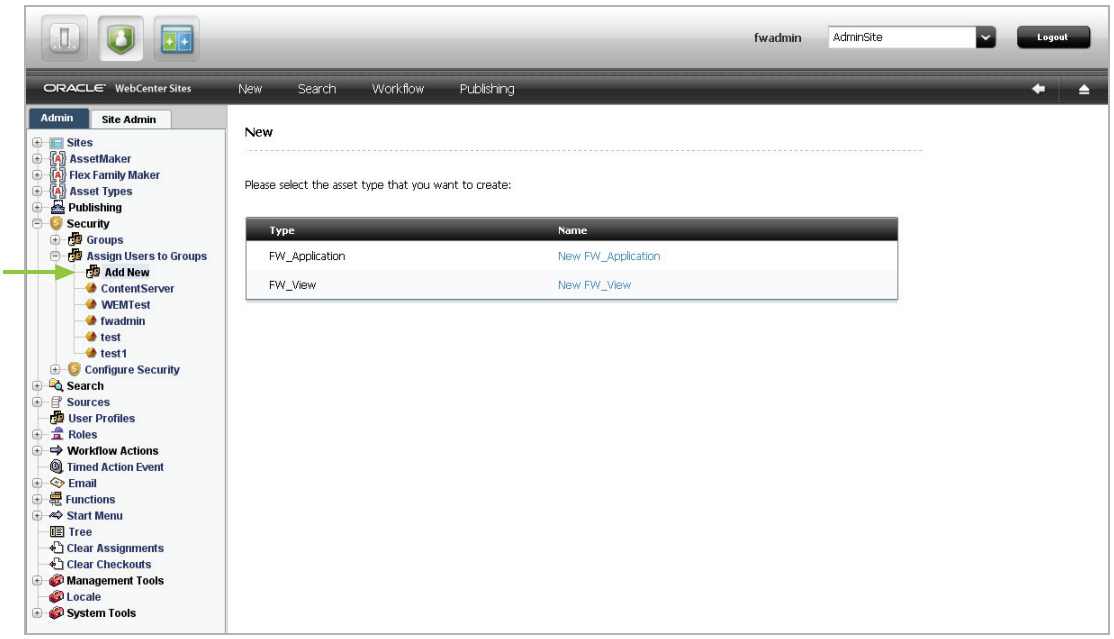
4. **「保存」**をクリックします。
   作成したグループが「管理」タブの「グループ」ノードにリストされます。
5. グループを作成したら、次を実行できます。
   - グループにユーザーを追加します。手順は、42 ページの「グループへのユーザーの追加」を参照してください。
   - グループの REST セキュリティを構成します。手順は、45 ページの「REST リソースのセキュリティの構成」を参照してください。

グループへのユーザーの追加

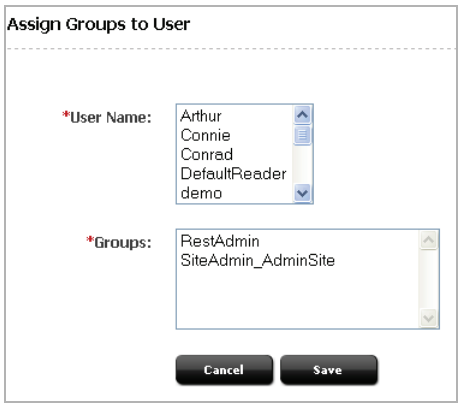
グループにユーザーを追加することによって、ユーザーがアクセスするアプリケーションで使用している REST リソースに対するユーザーの操作権限が決まります。

グループにユーザーを追加するには :

1. 一般的な管理者として、WebCenter Sites Admin インタフェースにログインします。
   a. 次の URL に移動します。
      `http://<server>:<port>/<cs_context>/Xcelerate/LoginPage.html`
   b. ユーザー名とパスワードを入力します。
   c. 「**ログイン**」をクリックします。
2. WebCenter Sites ツリーで「**管理**」タブを選択し、「**セキュリティ**」>「**グループへのユーザーの割当て**」の順に開いて、「**新規追加**」をダブルクリックします。



3. 「ユーザーへのグループの割当て」画面で、ユーザーを選択し、リストされているグループの任意の組合せに対して割り当てます。



注意

グループに割り当てるユーザーがリストに表示されていない場合、そのユーザーはすでにグループのメンバーになっています。このユーザーを別のグループに割り当てるには、手順 5 を参照してください。

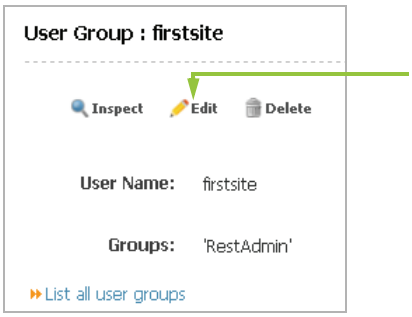
4. **「保存」**をクリックします。

   選択したユーザーは、「管理」タブの「グループへのユーザーの割当て」ノードにリストされます。ユーザーの名前をダブルクリックすると、そのユーザーがメンバーになっているグループが表示されます。

5. (オプション) 特定のグループに割り当てるユーザーの名前が「ユーザー名」フィールドに表示されない場合、次を実行します。

   a. WebCenter Sites ツリーで**「管理」**タブを選択し、**「セキュリティ」> 「グループへのユーザーの割当て」**の順に開いて、別のグループに割り当てるユーザーの名前をダブルクリックします。

   b. ユーザーの「調査」フォームで**「編集」**をクリックすると、「ユーザー・グループの編集」画面が表示されます。



   c. 「グループ」フィールドで、ユーザーを割り当てるグループを選択して**「保存」**をクリックします。

6. グループにユーザーが追加されたので、次を実行できます。

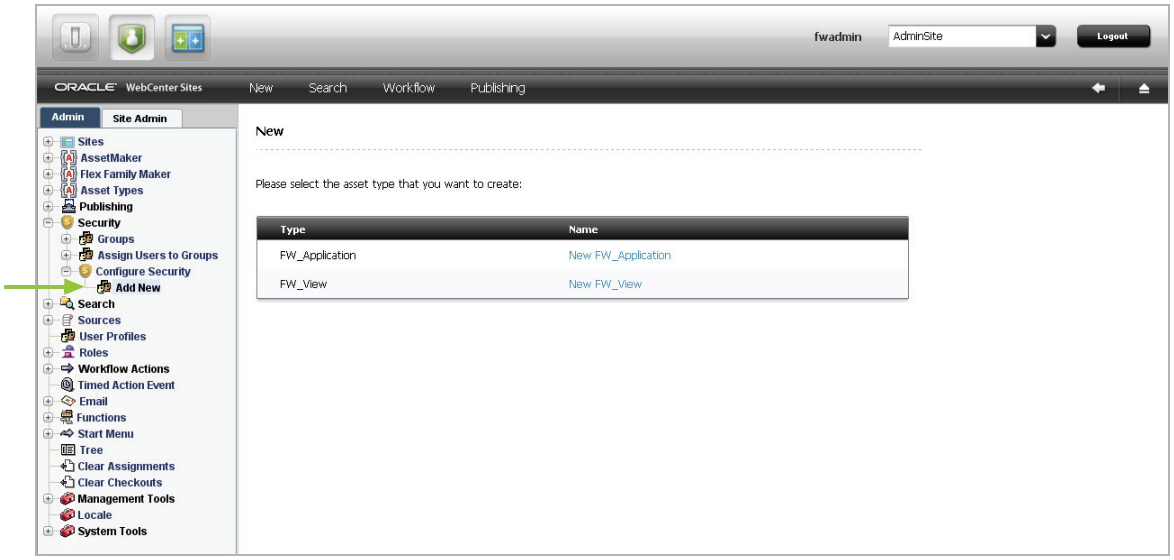
   - 新しいグループを作成します。手順は、40 ページの「グループの作成」を参照してください。
   - グループのセキュリティを構成します。手順は、45 ページの「REST リソースのセキュリティの構成」を参照してください。

REST リソースのセキュリティの構成

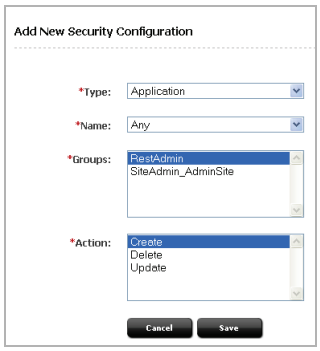
セキュリティを構成する際、どのオブジェクト・タイプおよびオブジェクトにグループがアクセスできる必要があるか、およびどのアクションをグループがオブジェクトに対して実行できるかを指定します。

REST リソースのセキュリティを構成するには :

1. 一般的な管理者として、WebCenter Sites Admin インタフェースにログインします。
   a. 次の URL に移動します。
      `http://<server>:<port>/<cs_context>/Xcelerate/LoginPage.html`
   b. ユーザー名とパスワードを入力します。
   c. 「**ログイン**」をクリックします。
2. WebCenter Sites ツリーで「**管理**」タブを選択し、「**セキュリティ**」>「**セキュリティの構成**」の順に開いて、「**新規追加**」をダブルクリックします。



3. 「新規セキュリティ構成の追加」画面では、オブジェクト・タイプおよびオブジェクトのセキュリティを設定できます。



アプリケーション・リソースのセキュリティを構成することによって、グループに `FW_Application` アセット・タイプおよび `FW_View` アセット・タイプへのアクセス権が付与されます。これらのアセット・タイプは、WEM Admin の**「アプリケーション」**ページのリスト項目として公開できるように、アプリケーションを登録するために使用します。通常は、開発者が、自身が作成したアプリケーションを登録します。望ましいのは、プログラムによる方法です。これらのアセット・タイプおよびアプリケーション登録の詳細は、*『Oracle WebCenter Sites Web エクスペリエンス管理フレームワーク開発者ガイド』*を参照してください。

可能なセキュリティ構成のサマリーは、次のページの表を参照してください。また、*『Oracle WebCenter Sites: Web エクスペリエンス管理フレームワーク REST API リソース・リファレンス』*も参照してください。

表 1: 使用できるアクション (セキュリティ権限)

アクション		説明
L	リスト	指定したリソースの取得をグループに許可します。
R	読取り / 先頭	指定したリソースの読取りをグループに許可します。読取りはリクエストされたリソースを返しますが、先頭はリクエストされたリソースについて記述するメタデータを返します。
C	作成	作成は指定したリソースの作成をグループに許可します。
U	更新	更新は指定したリソースの変更をグループに許可します。 **注意 :** 作成と更新はそれぞれが読取り / 先頭権限とペアになります。これらの権限のどちらかをグループに割り当てると、自動的に読取り / 先頭権限もグループに割り当てられます。
D	削除	指定したリソースの削除をグループに許可します。

表 2: 考えられるセキュリティ構成オプションのサマリー

オブジェクト・タイプ	名前	サブタイプ	サイト	可能なアクション	参照先
ACL	任意			L	49
アプリケーション*	任意			C、U、D	50
	<AppName>			U、D	
アセット	任意		任意	L、R、C、U、D	51
	任意		<SiteName>	L、R、C、U、D	
	<AssetType>		<SiteName>	L、R†、C、U、D	
	<AssetType> と <AssetName>		<SiteName>	R、U、D	
AssetType	任意			L、R、C、D	52
	<AssetType>			R、D	
	<AssetType>	任意		L	
	<AssetType>	<Subtype>		R	
グループ	任意			L	53
	<GroupName>			R	
索引	任意			L、R、C、U、D	54
	<IndexName>			R、U、D	
ロール	任意			L、R、C、U、D	55
	<Role>			R、U、D	
サイト	任意			L、R‡、C、U、D	56
	<SiteName>			R、U、D	

表 2: 考えられるセキュリティ構成オプションのサマリー

オブジェクト・タイプ	名前	サブタイプ	サイト	可能なアクション	参照先
ユーザー	任意			L、R、C、U、D	57
	<UserName>			R、U、D	
UserDef	任意			L	58
UserLocales	任意			L	59

* アプリケーションのセキュリティ設定例は、46 ページの手順 3 を参照してください。
† 読取りは指定されたサイトのアソシエーションの読取りを許可します。
‡ 読取りは指定されたサイトのユーザーおよびアセット・タイプの読取りを許可します。

REST セキュリティ構成リファレンス

このリファレンスは、47 ページの表 2 に対応しています。表で示したセキュリティ構成の詳細について説明します。

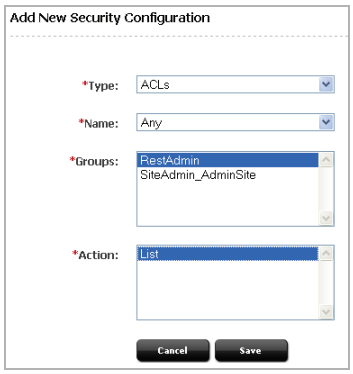
このリファレンスには次の項が含まれます。

- ACL リソースの REST セキュリティの構成
- アプリケーション・リソースの REST セキュリティの構成
- アセット・リソースの REST セキュリティの構成
- アセット・タイプ・リソースの REST セキュリティの構成
- グループ・リソースの REST セキュリティの構成
- 索引付きアセット・タイプ・リソースの REST セキュリティの構成
- ロール・リソースの REST セキュリティの構成
- サイト・リソースの REST セキュリティの構成
- ユーザー・リソースの REST セキュリティの構成
- UserDef リソースの REST セキュリティの構成
- UserLocale リソースの REST セキュリティの構成

ACL リソースの REST セキュリティの構成

ACL に対するセキュリティ権限をグループに割り当てる際、ACL リソース・リストをどのグループが参照できるかを決定します。

図 5: ACL の新しいセキュリティ構成の追加



この構成画面にアクセスするには :

1. WebCenter Sites ツリーで**「管理」**タブを選択し、**「セキュリティ」**> **「セキュリティの構成」**の順に開いて、**「新規追加」**をダブルクリックします。
2. 「タイプ」フィールドで**「ACL」**を選択します。

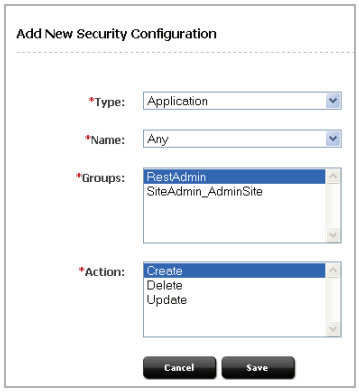
フィールド定義 :

名前	すべての ACL に対する操作権限をグループに付与するオプションのみ選択できます。
グループ	ACL へのアクセス権を付与するグループを選択します。
アクション	グループに割り当てることができるセキュリティ権限として選択できるのは、「ACL」リソース・リストに対する表示権限のみです。

アプリケーション・リソースの REST セキュリティの構成

アプリケーションに対するセキュリティ権限をグループに割り当てる際、指定されたアプリケーションに対してどのグループがどの操作を実行できるかを決定します。

図 6: アプリケーションの新しいセキュリティ構成の追加



この構成画面にアクセスするには :

1. WebCenter Sites ツリーで**「管理」**タブを選択し、**「セキュリティ」**> **「セキュリティの構成」**の順に開いて、**「新規追加」**をダブルクリックします。
2. 「タイプ」フィールドで**「アプリケーション」**を選択します。

フィールド定義 :

名前 グループに操作権限を付与するアプリケーションの名前を選択するか、**「任意」**を選択してすべてのアプリケーションに対する操作権限をグループに付与します。

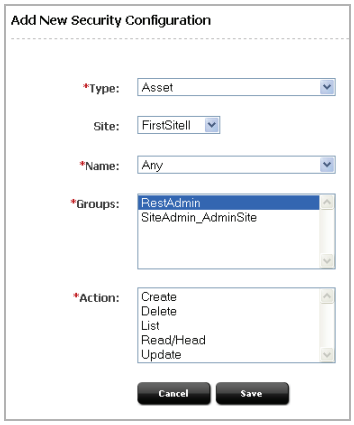
グループ アプリケーションに対する操作権限を付与するグループを選択します。

アクション セキュリティ権限をグループに割り当てます。オプションは、他のフィールドで選択した値によって異なります。たとえば、**「任意」**と**「作成」**を選択した場合、選択したグループのメンバーは、WEM でアプリケーションをアクセス可能にするアセットを作成できるようになります。

アセット・リソースの REST セキュリティの構成

アセットに対するセキュリティ権限をグループに割り当てる際、指定されたアセットに対してどのグループがどの操作を実行できるかを決定します。

図 7:　　アセットの新しいセキュリティ構成の追加



この構成画面にアクセスするには :

1. WebCenter Sites ツリーで**「管理」**タブを選択し、**「セキュリティ」**>**「セキュリティの構成」**の順に開いて、**「新規追加」**をダブルクリックします。
2. 「タイプ」フィールドで**「アセット」**を選択します。

フィールド定義 :

サイト　グループに操作権限を付与するアセットに関連付けられているサイトを選択するか、**「任意」**を選択してシステム全体のすべてのアセットに対する操作権限をグループに付与します。

名前　グループに操作権限を付与するアセットに関連付けられているアセット・タイプを選択するか、**「任意」**を選択してすべてのアセットに対する操作権限をグループに付与します。また、**「参照」**ボタンをクリックして、選択したアセット・タイプの指定したアセットに対する操作権限をグループに付与することもできます。

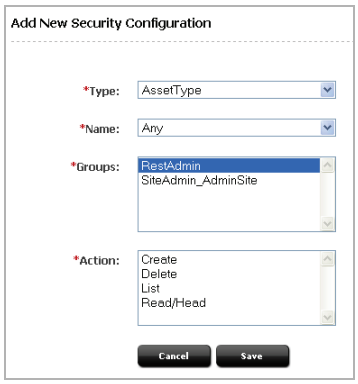
グループ　アセットに対する操作権限を付与するグループを選択します。

アクション　セキュリティ権限をグループに割り当てます。オプションは、他のフィールドで選択した値によって異なります。たとえば、特定のサイト、特定のアセット・タイプおよび**「リスト」**を選択した場合、選択したグループのメンバーは、指定したアセット・タイプのアセットを指定したサイトで検索できるようになります。

アセット・タイプ・リソースの REST セキュリティの構成

アセット・タイプに対するセキュリティ権限をグループに割り当てる際、指定されたアセット・タイプに対してどのグループがどの操作を実行できるかを決定します。

図 8:　　アセット・タイプの新しいセキュリティ構成の追加



この構成画面にアクセスするには :

1. WebCenter Sites ツリーで**「管理」**タブを選択し、**「セキュリティ」**> **「セキュリティの構成」**の順に開いて、**「新規追加」**をダブルクリックします。
2. 「タイプ」フィールドで**「AssetType」**を選択します。

フィールド定義 :

名前　グループに操作権限を付与するアセット・タイプを選択するか、**「任意」**を選択してすべてのアセット・タイプに対する操作権限をグループに付与します。

サブタイプ　(オプション) グループに操作権限を付与するアセット・タイプのサブタイプを選択します。

注意 :「名前」フィールドで**「任意」**オプションを選択した場合、「サブタイプ」フィールドは表示されません。

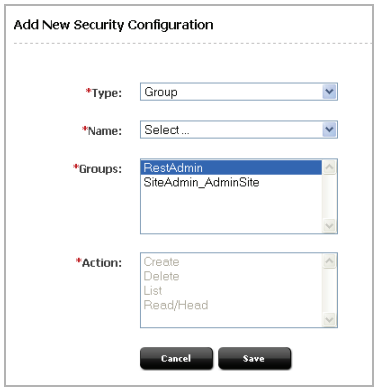
グループ　アセット・タイプに対する操作権限を付与するグループを選択します。

アクション　セキュリティ権限をグループに割り当てます。オプションは、他のフィールドで選択した値によって異なります。たとえば、**「任意」**と**「作成」**を選択した場合、選択したグループのメンバーは、アセット・タイプを作成できるようになります。

グループ・リソースの REST セキュリティの構成

グループに対するセキュリティ権限をグループに割り当てる際、指定されたグループに対してどのグループがどの操作を実行できるかを決定します。

図 9:　　グループの新しいセキュリティ構成の追加



この構成画面にアクセスするには :

1. WebCenter Sites ツリーで**「管理」**タブを選択し、**「セキュリティ」**>**「セキュリティの構成」**の順に開いて、**「新規追加」**をダブルクリックします。
2. 「タイプ」フィールドで**「グループ」**を選択します。

フィールド定義 :

名前　グループに対して操作権限を付与するグループを選択するか、**「任意」**を選択してすべてのグループに対する操作権限をグループに付与します。

グループ　グループに対する操作権限を付与するグループを選択します。

アクション　セキュリティ権限をグループに割り当てます。オプションは、他のフィールドで選択した値によって異なります。たとえば、**「任意」**と**「リスト」**を選択した場合、選択したグループのメンバーは、システムのグループ・リストを表示できるようになります。

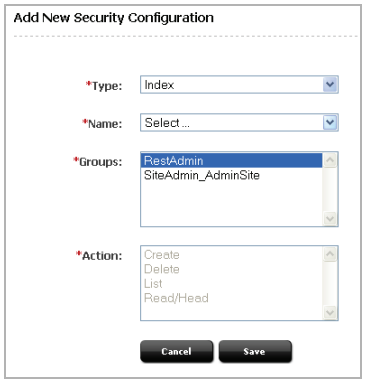
索引付きアセット・タイプ・リソースの REST セキュリティの構成

索引付きアセット・タイプに対するセキュリティ権限をグループに割り当てる際、指定された索引付きアセット・タイプに対してどのグループがどの操作を実行できるかを決定します。

注意

索引付きアセット・タイプのセキュリティを構成する前に、WebCenter Sites の「グローバル検索」および「アセット・タイプ検索」のための索引付けを有効にする必要があります。これらの検索機能が有効になっていない場合、索引付きアセット・タイプのセキュリティを構成することはできません。

図 10:　索引付きアセット・タイプの新しいセキュリティ構成の追加



この構成画面にアクセスするには :

1. WebCenter Sites ツリーで**「管理」**タブを選択し、**「セキュリティ」**>**「セキュリティの構成」**の順に開いて、**「新規追加」**をダブルクリックします。
2. 「タイプ」フィールドで**「索引」**を選択します。

フィールド定義 :

名前　グループに操作権限を付与する索引付きアセット・タイプの名前を選択します。**「任意」**を選択すると、すべての索引付きアセット・タイプに対する操作権限をグループに付与します。**「グローバル」**を選択すると、「グローバル検索」に関連付けられているすべての索引付きアセット・タイプに対する操作権限をグループに付与します。

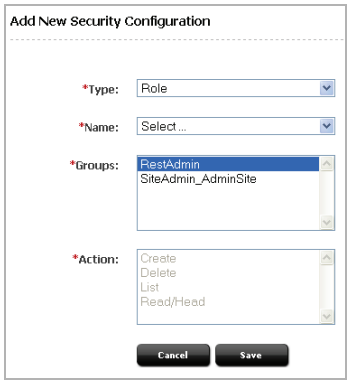
グループ　索引付きアセット・タイプに対する操作権限を付与するグループを選択します。

アクション　セキュリティ権限をグループに割り当てます。オプションは、他のフィールドで選択した値によって異なります。たとえば、**「任意」**と**「リスト」**を選択した場合、選択したグループのメンバーは、システムのすべての索引付きタイプのアセットを検索できるようになります。

ロール・リソースの REST セキュリティの構成

ロールに対するセキュリティ権限をグループに割り当てる際、指定されたロールに対してどのグループがどの操作を実行できるかを決定します。

図 11:　　ロール・リソースに対する新しい REST セキュリティ権限の構成



この構成画面にアクセスするには :

1. WebCenter Sites ツリーで**「管理」**タブを選択し、**「セキュリティ」**> **「セキュリティの構成」**の順に開いて、**「新規追加」**をダブルクリックします。
2. 「タイプ」フィールドで**「ロール」**を選択します。

フィールド定義 :

名前　グループに操作権限を付与するロールの名前を選択するか、**「任意」**を選択してすべてのロールに対する操作権限をグループに付与します。

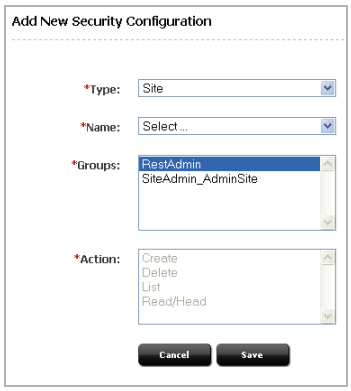
グループ　ロールに対する操作権限を付与するユーザー・グループを選択します。

アクション　セキュリティ権限をグループに割り当てます。オプションは、他のフィールドで選択した値によって異なります。たとえば、**「任意」**と**「作成」**を選択した場合、選択したグループのメンバーは、ロールを作成できるようになります。

サイト・リソースの REST セキュリティの構成

サイトに対するセキュリティ権限をグループに割り当てる際、指定されたサイトに対してどのグループがどの操作を実行できるかを決定します。

図 12:　　サイトの新しいセキュリティ構成の追加



この構成画面にアクセスするには :

1. WebCenter Sites ツリーで**「管理」**タブを選択し、**「セキュリティ」**> **「セキュリティの構成」**の順に開いて、**「新規追加」**をダブルクリックします。
2. 「タイプ」フィールドで**「サイト」**を選択します。

フィールド定義 :

名前　グループに操作権限を付与するサイトの名前を選択するか、**「任意」**を選択してすべてのサイトに対する操作権限をグループに付与します。

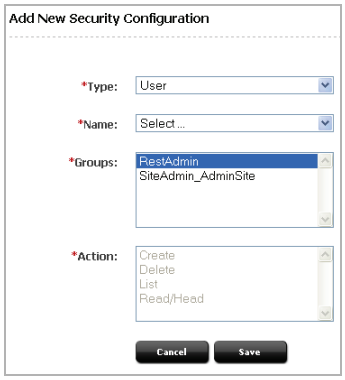
グループ　サイトに対する操作権限を付与するユーザー・グループを選択します。

アクション　セキュリティ権限をグループに割り当てます。メニュー・オプションは、他のフィールドで選択した値によって異なります。たとえば、**「任意」**と**「作成」**を選択した場合、選択したグループのメンバーは、サイトを作成できるようになります。

ユーザー・リソースの REST セキュリティの構成

ユーザーに対するセキュリティ権限をグループに割り当てる際、指定されたユーザーに対してどのグループがどの操作を実行できるかを決定します。

図 13:　　ロールの新しいセキュリティ構成の追加



この構成画面にアクセスするには :

1. WebCenter Sites ツリーで**「管理」**タブを選択し、**「セキュリティ」**> **「セキュリティの構成」**の順に開いて、**「新規追加」**をダブルクリックします。
2. 「タイプ」フィールドで**「ユーザー」**を選択します。

フィールド定義 :

名前　グループに操作権限を付与するユーザーの名前を選択するか、**「任意」**オプションを選択してすべてのユーザーに対する操作権限をグループに付与します。

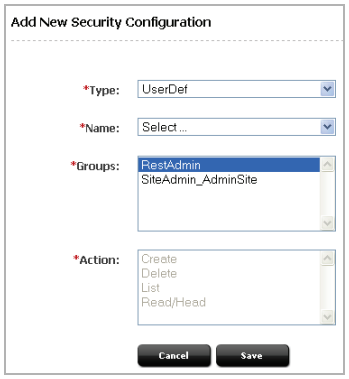
グループ　ユーザーに対する操作権限を付与するグループを選択します。

アクション　セキュリティ権限をグループに割り当てます。メニュー・オプションは、他のフィールドで選択した値によって異なります。たとえば、**「任意」**と**「作成」**を選択した場合、選択したグループのメンバーは、ユーザーを作成できるようになります。

UserDef リソースの REST セキュリティの構成

ユーザー定義に対するセキュリティ権限をグループに割り当てる際、システムのユーザー定義をどのグループが表示できるかを決定します。

図 14:　　ユーザー定義の新しいセキュリティ構成の追加



この構成画面にアクセスするには :

1. WebCenter Sites ツリーで**「管理」**タブを選択し、**「セキュリティ」**>**「セキュリティの構成」**の順に開いて、**「新規追加」**をダブルクリックします。
2. 「タイプ」フィールドで**「UserDef」**を選択します。

フィールド定義 :

名前　すべてのユーザー定義に対する操作権限をグループに付与するオプションのみ選択できます。

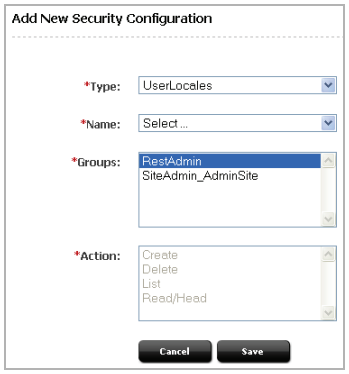
グループ　ユーザー定義に対する表示権限を付与するグループを選択します。

アクション　グループに割り当てることができるセキュリティ権限として選択できるのは、**「読取り / 先頭」**のみです。これを選択すると、選択したグループのメンバーが、システムのユーザー定義を表示できるようになります。

UserLocale リソースの REST セキュリティの構成

ユーザー・ロケールに対するセキュリティ権限をグループに割り当てる際、UserLocale リソース・リストをどのグループが表示できるかを決定します。

図 15:　　ユーザー・ロケールの新しいセキュリティ構成の追加



この構成画面にアクセスするには :

1. WebCenter Sites ツリーで**「管理」**タブを選択し、**「セキュリティ」**>**「セキュリティの構成」**の順に開いて、**「新規追加」**をダブルクリックします。
2. 「タイプ」フィールドで**「UserLocales」**を選択します。

フィールド定義 :

名前	すべてのユーザー・ロケールに対する操作権限をグループに付与するオプションのみ選択できます。
グループ	ユーザー・ロケールに対する表示権限を付与するグループを選択します。
アクション	グループに割り当てることができるセキュリティ権限として選択できるのは、システムのユーザー・ロケールのリストに対する表示権限のみです。

第 5 章

サイトの使用

この章では、WEM Admin で作成されて WebCenter Sites アプリケーションで使用するサイトおよび WebCenter Sites で作成されて WEM Admin アプリケーションで使用するサイトを管理する手順について説明します。

この章には次の項が含まれます。

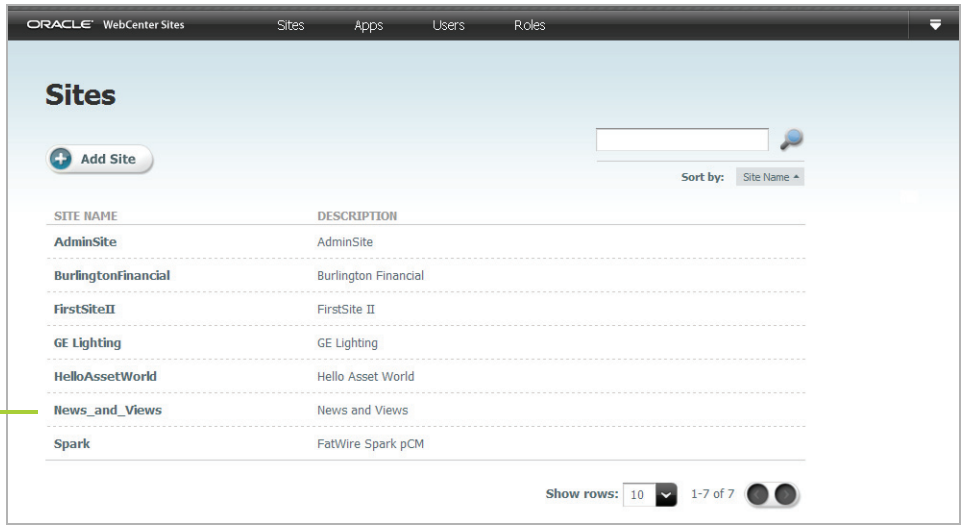
WEM フレームワークでの WebCenter Sites CM サイトの管理

WEM Admin インタフェースを使用してサイトを削除または変更する場合、それらが WebCenter Sites プラットフォームのアクティブなコンテンツ管理サイトではないことを確認します。WEM Admin インタフェースからサイトを削除すると、システムから、さらにサイトが使用されていたすべてのアプリケーションから、サイトが削除されます。ロールなど、他のオブジェクトにも同様の処理が適用されますが、1 つ異なる点があります。

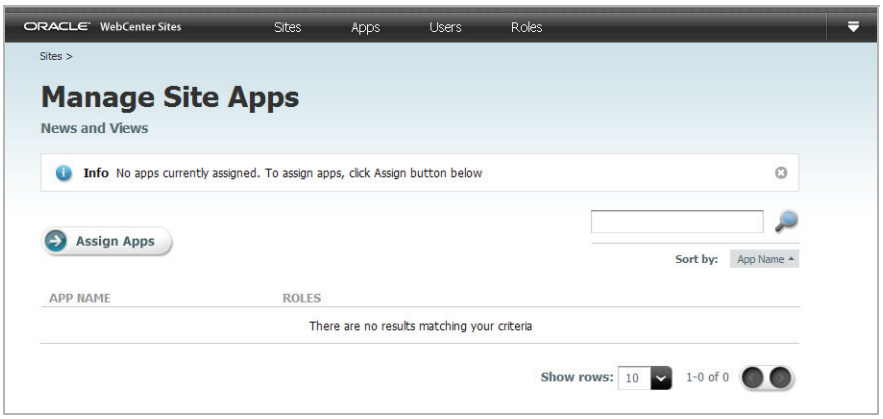
ユーザーおよびアプリケーションに割り当てられているロールを削除しようとすると、ロールを削除するために消去する必要がある依存関係のリストが表示されます。サイトを削除しようとすると、決定を確認するように求められます。サイトのステータスは確認済であることが想定されています。

WebCenter Sites アプリケーションをアクティブな WebCenter Sites CM サイトで稼動するように構成し、自身をそれらのサイトに割り当てることによって、WEM Admin でそれらのサイトを公開して簡単にアクセスできるように設定できます。たとえば、次のようになります。

1. WebCenter Sites Admin インタフェースで「News_and_Views」という名前のサイトを構成すると、このサイトは WEM Admin の「Sites」画面にリストされます。

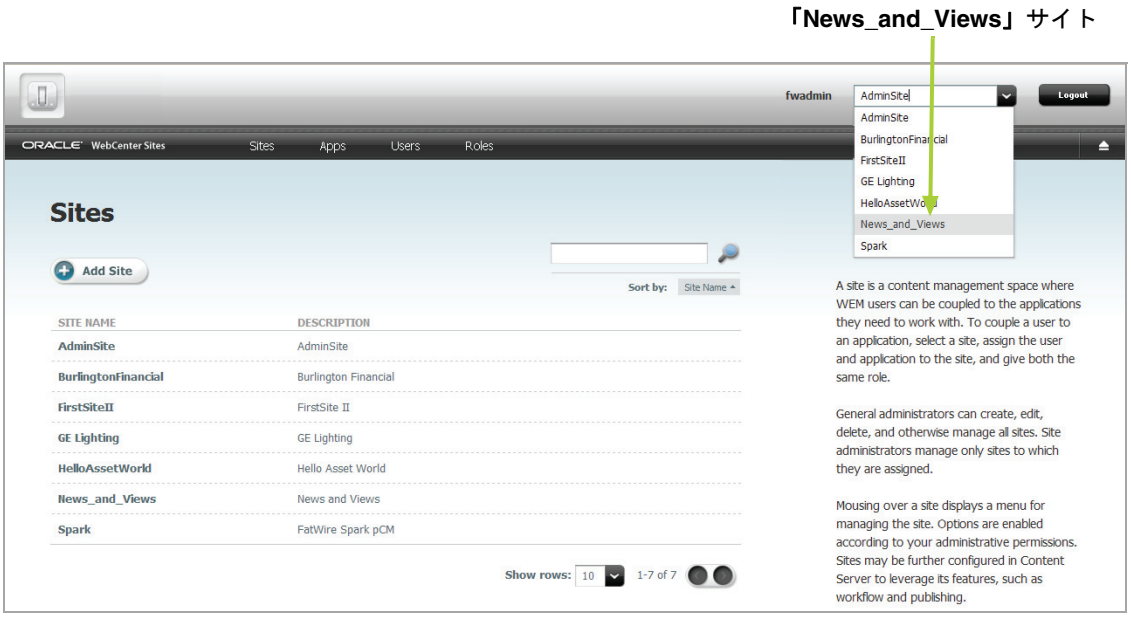


2. **News_and_Views** に移動して「**サイト・アプリケーションの管理**」をクリックします。



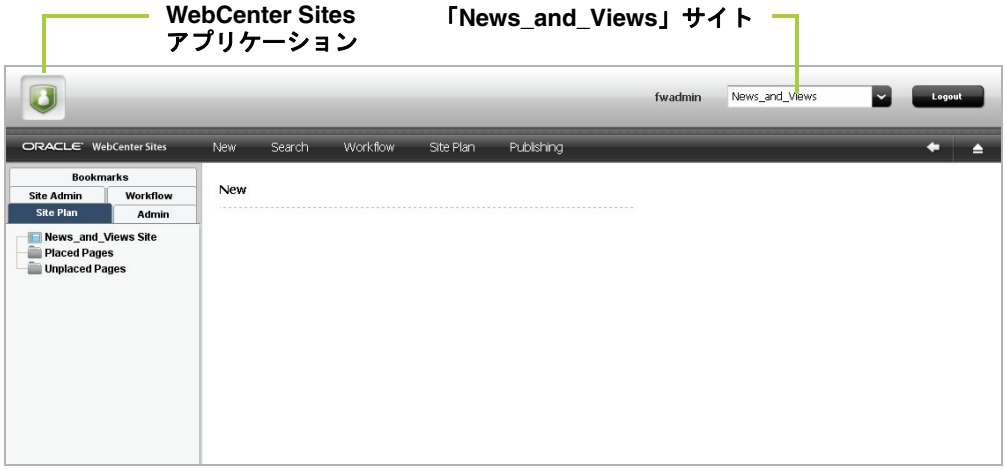
アプリケーションが割り当てられていない場合、サイトは非アクティブとみなされる可能性があります。

3. WebCenter Sites Admin アプリケーションと自身を「News_and_Views」に割り当てると、このサイトがドロップダウン・メニューにオプションとしてリストされます (必要であれば表示を更新してください)。



4. メニューから「**News_and_Views**」を選択すると、ログイン画面が表示されます。ドロップダウン・メニューにこのサイトがリストされています。その下には、WebCenter Sites Admin のアプリケーション・アイコンがあります。

ログインすると、WebCenter Sites Admin アプリケーション・アイコンが左側に、サイトの名前が右側のドロップダウン・メニューに、それぞれ表示されます。この後のアクセスでは、ログインする必要はありません。

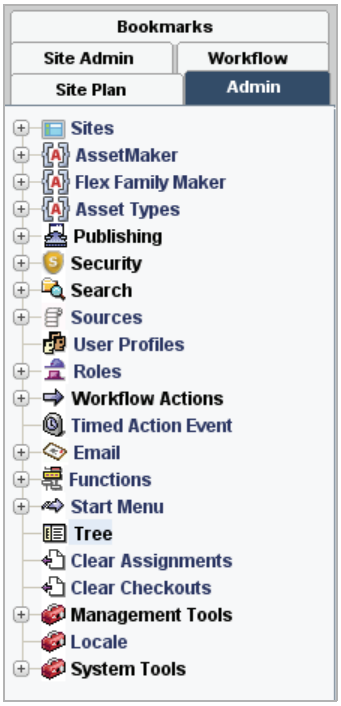


ツリー・タブの有効化

WEM Admin インタフェースで作成されたサイトは、WebCenter Sites Admin インタフェースで公開されますが、WebCenter Sites Admin インタフェースで使用できるように構成されているわけではありません。全体管理者は、タブごとに WebCenter Sites ツリーを有効化することによって、各サイトでの操作を有効化する必要があります。

WEM サイト向けの WebCenter Sites Admin インタフェースのツリーおよびタブの有効化

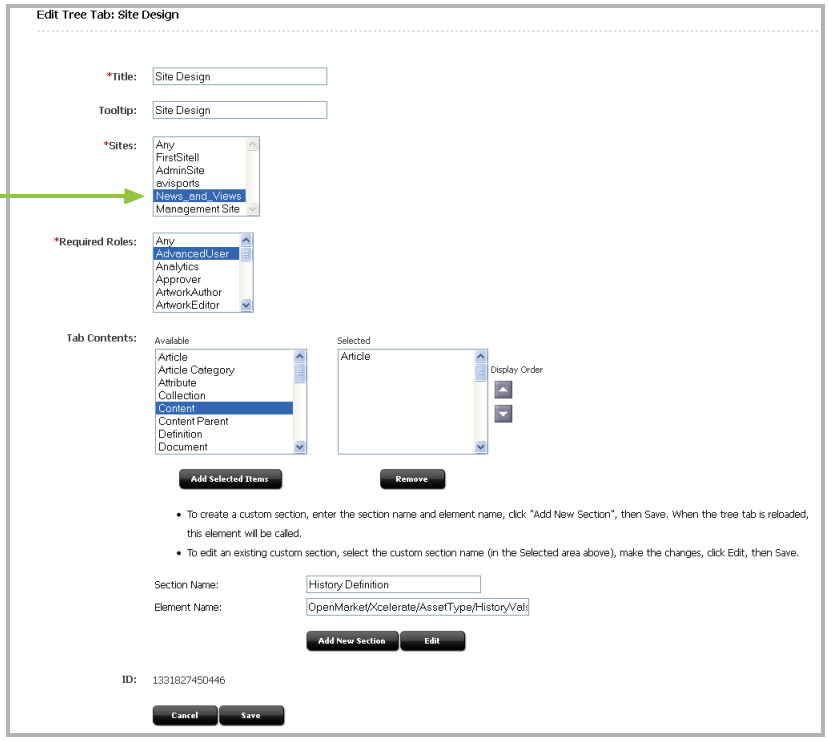
1. 一般的な管理者として、WebCenter Sites Admin インタフェースにログインします。
   a. 次の URL に移動します。
      `http://<server>:<port>/<cs_context>/Xcelerate/LoginPage.html`
   b. ユーザー名とパスワードを入力します。
   c. 「**ログイン**」をクリックします。
2. WEM Admin インタフェースで作成したサイトで必要な WebCenter Sites ツリーのタブを有効化します。
   a. WebCenter Sites ツリーに移動し、「**管理**」タブを選択します。
   b. 「**ツリー**」ノードをダブルクリックします。



   c. 有効化する各タブを個別に選択します。たとえば、「**サイト・デザイン**」タブを有効化するとします。
      1) ツリーのタブのリストから、「**サイト・デザイン**」をクリックします。

2) ツリー・タブフォームで、**「編集」**をクリックします。
(**「サイト・デザイン」**の) 「編集」フォームが表示されます。

[Ctrl] キーを押しながら「サイト・デザイン」タブを有効化するサイトをクリックします。



3) 「サイト」選択ボックスで、タブを有効化する必要があるサイトを選択します。
4) タブへのアクセスを許可するロールを選択します。
5) タブ・コンテンツを選択します。
6) **「保存」**をクリックします。
7) 他のタブを有効化する必要がある場合、**「すべてのツリー・タブのリスト」**(「編集」フォームの一番下) をクリックして、これまでの手順を繰り返します。

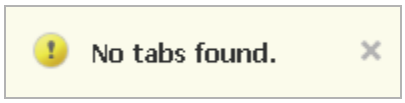
3. WebCenter Sites ツリーとタブをサイトで有効にしたら、次の項に進んで、ツリーとタブが正しく表示されることを確認します。

ツリー・タブが有効化されていることの検証

前の項で有効化したタブへのアクセスは、各タブとロールを共有しているユーザーにのみ許可されます。ツリーとタブが有効化されているサイトごとに検証します。

1. WebCenter Sites Admin インタフェースに、特定のタブ (または特定の複数のタブ) に割り当てられているロールのいずれかを共有するユーザーとしてログインします。
2. サイトを選択します。WebCenter Sites ツリーが、選択したサイトで有効化したタブとともに、表示されます。

3. WebCenter Sites ツリーが有効化されていない場合、次のエラー・メッセージが表示されます。



ユーザーとタブに対するサイトとロールの割当てを検証します。

第 6 章

WEM Admin クイック・リファレンス

この章では、WEM フレームワークに関連付けられているサイト、アプリケーション、ユーザーおよびロールを管理および使用するためのヒントおよびクイック・リファレンスを提供します。次の項が含まれます。

WEM フレームワークを管理するための簡単なヒント

この項の後半の手順を実行する前に、いくつかのヒントを書き留めておきます。

- (オプション)WEM のサイト、ユーザーおよびロールを試す場合、WebCenter Sites CM 専用のサイト、ユーザーおよびロールと区別することをお薦めします。たとえば、サイト / ユーザー / ロールの説明を追加する、名前の前に「WEM_」(あるいは同様の修飾子) を付けるといった方法があります。**サイト、ユーザーまたはロールは、作成後にその名前を変更できないことに注意してください。**
- ユーザー・アカウントには ACL が必要です。ACL を作成できるのは全体管理者のみであり、WebCenter Sites の**「管理」**タブでのみ作成できます。
- ユーザーおよびアプリケーションでロールを共有することで、そのサイトのそのアプリケーションへのアクセス権がそのユーザーに付与されます。
- アプリケーションのインタフェース機能は、ロールで保護できます。ユーザーおよびインタフェース機能でロールを共有することで、そのインタフェース機能へのアクセス権がそのユーザーに付与されます。
- グループは、REST に対するアクセスを提供します。これらは、WebCenter Sites Admin インタフェースで構成する必要があります。
- グループは、アプリケーションのリソースへのアクセスの制御に使用します。

  カスタム構築アプリケーションで事前定義済ユーザーが指定されていない場合、アプリケーション・レベルおよび REST レベルでアプリケーション・ユーザーを認可します。

  カスタム構築アプリケーションで事前定義済ユーザーが指定されている場合、システム・レベル、アプリケーション・レベルおよび REST レベルでそのユーザーを認可します。アプリケーション・ユーザーは、アプリケーション・レベルで認可します。

この項の後半では、WEM Admin インタフェースでサイト、アプリケーション、ユーザーおよびロールを作成および管理する際に参照するためのクイック・リファレンスを提供します。

- サイトの管理
- アプリケーションの管理
- ユーザーの管理
- ロールの管理
- プロファイルの管理

サイトの管理

サイトを作成、編集および削除できるのは、全体管理者のみです。「サイト」画面には、全体管理者とサイト管理者がアクセスできます。

表 3: サイトの管理

管理者	アクション	パス
WEM 全体管理者	サイトの作成	WEM Admin インタフェース > **「サイト」** > **「サイトの追加」** > *フィールドに値を入力* > **「保存して閉じる」** **注意 :** サイトの名前には、英数字のみ使用できます (記号は使用できません)。
	サイトの編集	WEM Admin インタフェース > **「サイト」** > *編集するサイトの上にマウスを移動* > **「編集」** > *フィールドを変更* > **「保存して閉じる」** **注意 :** サイトの名前は変更できません。
	サイトの削除	**1.** WEM Admin インタフェース > **「サイト」** > *削除するサイトの上にマウスを移動* > **「削除」** **2.** 警告ボックスで **「削除」** をクリックします。

表 3: サイトの管理 *(続き)*

管理者	アクション	パス
WEM の全体管理者およびサイト管理者	アプリケーションのサイトへの追加	1. WEM Admin インタフェース > **「サイト」** > *アプリケーションを追加するサイトの上にマウスを移動* > **「サイト・アプリケーションの管理」** > **「アプリケーションの割当て」** 2. 「サイトのアプリケーションの選択」フォームでサイトに追加するアプリケーションを選択し、**「選択済」** リスト・ボックスに移動します。 3. **「続行」** をクリックします。 4. 「アプリケーションへのロールの割当て」フォームでアプリケーションに割り当てるロールを選択し、**「選択済」** リスト・ボックスに移動します。 5. **「保存して閉じる」** をクリックします。 **注意 :** アプリケーションをサイトに追加する別の方法を必要とする全体管理者は、75 ページの「アプリケーションの管理」を参照してください。
	ユーザーのサイトへの割当て	1. WEM Admin インタフェース > **「サイト」** > *ユーザーを割り当てるサイトの上にマウスを移動* > **「サイト・ユーザーの管理」** > **「ユーザーの割当て」** 2. 「サイトのユーザーの選択」フォームでサイトに割り当てるユーザーを選択し、**「選択済」** リスト・ボックスに移動します。 3. **「続行」** をクリックします。 4. 「ユーザーへのロールの割当て」フォームでユーザーに割り当てるロールを選択し、**「選択済」** リスト・ボックスに移動します。 5. **「保存して閉じる」** をクリックします。 **注意 :** ユーザーをサイトに割り当てる別の方法を必要とする全体管理者は、77 ページの「ユーザーの管理」を参照してください。

表 3: サイトの管理 *(続き)*

管理者	アクション	パス
WEM の全体管理者およびサイト管理者 *(続き)*	ロールのユーザーへの再割当て	注意 : WEM でサイトのユーザーのロールを再割当てすると、ユーザーとそのサイトの一部のアプリケーションの結合が解除される可能性があります。 ロールをユーザーに再割当てするには : **1.** WEM Admin インタフェース > **「サイト」** > *ユーザーを変更するサイトの上にマウスを移動* > **「サイト・ユーザーの管理」** **2.** 「サイト・ユーザーの管理」画面 : *サイト・ロールを変更するユーザーの上にマウスを移動* > **「ユーザーへのロールの割当て」** **3.** 「ユーザーへのロールの割当て」フォームで、必要に応じて、新しいロールをサイト・ユーザーに割り当てるか、またはロールの割当てを解除します。 **4.** **「保存して閉じる」**をクリックします。 **注意 :** サイトのユーザーのロールを変更する別の方法を必要とする全体管理者は、77 ページの「ユーザーの管理」を参照してください。
	ロールのアプリケーションへの再割当て	注意 : WEM でサイトのアプリケーションのロールを再割当てすると、アプリケーションとそのサイトの一部のユーザーの結合が解除される可能性があります。 ロールをアプリケーションに再割当てするには : **1.** WEM Admin インタフェース > **「サイト」** > *アプリケーションを変更するサイトの上にマウスを移動* > **「サイト・アプリケーションの管理」** **2.** 「サイト・アプリケーションの管理」画面 : *サイト・ロールを変更するアプリケーションの上にマウスを移動* > **「アプリケーションへのロールの割当て」** **3.** 「アプリケーションへのロールの割当て」フォームで、必要に応じて、新しいロールをアプリケーションに割り当てるか、またはロールの割当てを解除します。 **4.** **「保存して閉じる」**をクリックします。 **注意 :** サイトのアプリケーションのロールを変更する別の方法を必要とする全体管理者は、75 ページの「アプリケーションの管理」を参照してください。

表 3: サイトの管理 *(続き)*

管理者	アクション	パス
WEM の全体管理者およびサイト管理者 *(続き)*	ユーザーのサイトからの削除	**1.** WEM Admin インタフェース > **「サイト」** > *ユーザーを削除するサイトの上にマウスを移動* > **「サイト・ユーザーの管理」** **2.** 「サイト・ユーザーの管理」画面 : *サイトから削除するユーザーの上にマウスを移動* > **「除去」** **3.** 警告ボックスで **「除去」** をクリックします。 **注意 :** 特定のサイトからユーザーを削除する別の方法を必要とする全体管理者は、77 ページの「ユーザーの管理」を参照してください。
	アプリケーションのサイトからの削除	**1.** WEM Admin インタフェース > **「サイト」** > *アプリケーションを削除するサイトの上にマウスを移動* > **「サイト・アプリケーションの管理」** **2.** 「サイト・アプリケーションの管理」画面で *サイトから削除するアプリケーションの上にマウスを移動* > **「除去」** **3.** 警告ボックスで **「除去」** をクリックします。 **注意 :** サイトからアプリケーションを削除する別の方法を必要とする全体管理者は、75 ページの「アプリケーションの管理」を参照してください。

アプリケーションの管理

アプリケーション (その説明) を変更できるのは、全体管理者のみです。「アプリケーション」画面には、全体管理者のみがアクセスできます。

表 4: アプリケーションの管理

アクション	パス
アプリケーションの変更	1. WEM Admin インタフェース > **「アプリケーション」** > *変更するアプリケーションの上にマウスを移動* > **「編集」** > *フィールドを変更:* • **名前 :** 変更できません。 • **ツールチップ :** アプリケーションのアイコンの上にマウスを移動したときに表示される名前。 • **説明 :** アプリケーションの簡単な説明。 2. **「保存して閉じる」** をクリックします。
アプリケーションのサイトへの割当て	1. WEM Admin インタフェース > **「アプリケーション」** > *サイトに割り当てるアプリケーションの上にマウスを移動* > **「アプリケーションの管理」** > **「サイトへの割当て」** 2. 「アプリケーションのサイトの選択」フォームでアプリケーションを割り当てるサイトを選択し、**「選択済」** リスト・ボックスに移動します。 3. **「続行」** をクリックします。 4. 「アプリケーションへのロールの割当て」フォームでアプリケーションに割り当てるロールを選択し、**「選択済」** リスト・ボックスに移動します。 5. **「保存して閉じる」** をクリックします。 **注意 :** アプリケーションをサイトに追加する別の方法は、71 ページの「サイトの管理」 を参照してください。
ロールのアプリケーションへの再割当て	注意 : WEM でサイトのアプリケーションのロールを再割当てすると、アプリケーションとそのサイトの一部のユーザーの結合が解除される可能性があります。 ロールをアプリケーションに再割当てするには : 1. WEM Admin インタフェース > **「アプリケーション」** > *選択したサイトでロールを変更するアプリケーションの上にマウスを移動* > **「アプリケーションの管理」** 2. 「アプリケーションの管理」画面 : *アプリケーションのロールを変更するサイトの上にマウスを移動* > **「アプリケーションへのロールの割当て」** 3. 「アプリケーションへのロールの割当て」フォームで、必要に応じて、ロールをアプリケーションに追加するか、またはロールを削除します。 4. **「保存して閉じる」** をクリックします。 **注意 :** サイトでアプリケーションのロールを変更する別の方法は、71 ページの「サイトの管理」 を参照してください。

表 4: アプリケーションの管理 *(続き)*

アクション	パス
アプリケーションのサイトからの削除	**1.** WEM Admin インタフェース > **「アプリケーション」** > *サイトから削除するアプリケーションの上にマウスを移動* > **「アプリケーションの管理」** **2.** 「アプリケーションの管理」画面で *アプリケーションを削除するサイトの上にマウスを移動* > **「除去」** **3.** 警告ボックスで **「除去」** をクリックします。 **注意 :** アプリケーションをサイトから削除する別の方法は、71 ページの「サイトの管理」を参照してください。

ユーザーの管理

ユーザーを作成、編集および削除できるのは、全体管理者のみです。「ユーザー」画面には、全体管理者のみがアクセスできます。

表 5: ユーザーの管理

アクション	パス
ユーザーの作成	**1.** WEM Admin インタフェース > **「ユーザー」** > **「ユーザーの追加」** > *フィールドに値を入力*: • **ACL**: ACL は、ユーザーによるデータベースに対するアクセス権限を決定します。 **注意 :** WEM Admin インタフェースでは ACL を作成できません。 • **グループ** : グループは、ユーザーによる REST (アプリケーションのリソース) に対するアクセス権限を決定します。次の 2 つのデフォルト・グループが構成されています。 RestAdmin (全体管理者グループ) および SiteAdmin_AdminSite (サイト管理者グループ) **2.** **「保存して閉じる」**をクリックします。 **注意 :** ユーザーはログインすることはできます。サイトおよびアプリケーションにアクセスするには、ユーザーを有効化する必要があります。
ユーザーの有効化	**1.** WEM Admin インタフェース > **「ユーザー」** > *有効化するユーザーの上にマウスを移動* > **「ユーザーの管理」** > **「サイトへの割当て」** **2.** 「ユーザーのサイトの選択」フォーム : • 全体管理者にするユーザーを有効化している場合は、ユーザーを AdminSite に割り当てます。 • サイト管理者にするユーザーを有効化している場合は、ユーザーを AdminSite 以外のサイトに割り当てます。 • 通常ユーザーを有効化している場合は、ユーザーを AdminSite 以外のサイトに割り当てます。 **3.** **「続行」**をクリックします。 **4.** 「ユーザーへのロールの割当て」フォーム : • 全体管理者にするユーザーを有効化している場合は、ユーザーに GeneralAdmin ロールを割り当てます。 • サイト管理者にするユーザーを有効化している場合は、ユーザーに SiteAdmin ロールを割り当てます。 • 通常ユーザーを有効化している場合は、ユーザーに GeneralAdmin でも SiteAdmin でもないロールを割り当てます。 **5.** **「保存して閉じる」**をクリックします。

表 5: ユーザーの管理 *(続き)*

アクション	パス
ユーザーのサイトへの割当て	**1.** WEM Admin インタフェース > **「ユーザー」** > *サイトに割り当てるユーザーの上にマウスを移動* > **「ユーザーの管理」** > **「サイトへの割当て」** **2.** 「ユーザーのサイトの選択」フォームでユーザーに割り当てるサイトを選択し、**「選択済」**リスト・ボックスに移動します。 **3.** **「続行」**をクリックします。 **4.** 「ユーザーへのロールの割当て」フォームでユーザーに割り当てるロールを選択し、**「選択済」**リスト・ボックスに移動します。 **5.** **「保存して閉じる」**をクリックします。 **注意 :** ユーザーをサイトに追加する別の方法は、71 ページの「サイトの管理」を参照してください。
ユーザーの編集	WEM Admin インタフェース > **「ユーザー」** > *変更するユーザーの上にマウスを移動* > **「編集」** > *必要なフィールドを変更* > **「保存して閉じる」** **注意 :** ユーザーを保存した後は、ユーザーの名前は変更できません。
ロールのユーザーへの再割当て	**1.** WEM Admin インタフェース > **「ユーザー」** > *ロールを変更するユーザーの上にマウスを移動* > **「ユーザーの管理」** **2.** 「ユーザーの管理」画面 : *ユーザーのロールを変更するサイトの上にマウスを移動* > **「ユーザーへのロールの割当て」** **3.** 「ユーザーへのロールの割当て」フォームで、必要に応じて、ロールをユーザーに追加するか、またはロールを削除します。 **4.** **「保存して閉じる」**をクリックします。
グループへのユーザーの割当て	**1.** WEM Admin インタフェース > **「ユーザー」** > *グループに割り当てるユーザーの上にマウスを移動* > **「編集」** **2.** 「グループ」フィールドで適切なグループを選択し、**「選択済」**リスト・ボックスに移動します。 **3.** **「保存して閉じる」**をクリックします。 **注意 :** グループは、REST に対するアクセスを提供します。それらは、アプリケーションのリソースへのアクセスの制御に使用します。
ユーザーのサイトからの削除	**1.** WEM Admin インタフェース > **「ユーザー」** > *サイトから削除するユーザーの上にマウスを移動* > **「ユーザーの管理」** > *ユーザーを削除するサイトの上にマウスを移動* > **「除去」** **2.** 警告ボックスで**「除去」**をクリックします。 **注意 :** サイトからユーザーを削除する別の方法は、71 ページの「サイトの管理」を参照してください。
WEM からのユーザーの削除	**1.** WEM Admin インタフェース > **「ユーザー」** > *システムから削除するユーザーの上にマウスを移動* > **「削除」** **2.** 警告ボックスで**「削除」**をクリックします。

ロールの管理

ロールを作成、編集および削除できるのは、全体管理者のみです。「ロール」画面には、全体管理者のみがアクセスできます。

表 6: ロールの管理

アクション	パス
ロールの追加	WEM Admin インタフェース > **「ロール」** > **「ロールの追加」** > *フィールドに値を入力* > **「保存して閉じる」**
ロールの編集	WEM Admin インタフェース > **「ロール」** > *変更するユーザーの上にマウスを移動* > **「編集」** > *必要なフィールドを変更* > **「保存して閉じる」** **注意 :** ロールを保存した後は、ロールの名前は変更できません。
ロールの削除	**1.** WEM Admin インタフェース > **「ロール」** > *削除するロールの上にマウスを移動* > **「削除」** **2.** 警告ボックスで**「削除」**をクリックします。 **注意 :** ロールがユーザーまたはアプリケーション、あるいはその両方に割り当てられている場合、ユーザーおよびアプリケーションからロールを割当て解除するまで、ロールを削除できません。「ロールの依存性」画面が表示されます。依存関係の表を確認します。**「すべての依存性の削除」**は、ロールをそのユーザーおよびアプリケーションから削除し、システムからロールを削除します。

プロファイルの管理

全体管理者は、ユーザー・プロファイルを変更できます。

表 7: プロファイルの管理

ユーザー	アクション	パス
WEM 全体管理者	ユーザーのプロファイルの変更	WEM Admin インタフェース > 「**ユーザー**」> *プロファイルを変更するユーザーの上にマウスを移動* > 「**編集**」> *必要なフィールドを変更* > 「**保存して閉じる**」
WEM のすべてのユーザー	プロファイルの変更	WEM Admin インタフェース > **アプリケーション・バーを開く** > *自身のユーザー名をクリック* > *必要なフィールドを変更* > 「**保存して閉じる**」