FatWire SOFTWARE

Web Experience Management Framework

Version 1.1

Administrator's Guide

Document Revision Date: *Jan. 31, 2012*

FatWire Web Experience Management Framework
Document Revision Date: Jan. 31, 2012
Product Version: 1.1

FatWire Headquarters
FatWire Corporation
330 Old Country Road
Suite 303
Mineola, NY 11501

Table of

Contents

About This Guide

This guide describes the FatWire Web Experience Management Framework, its relationship to FatWire Content Server, and its ability to support the integration of applications with Content Server. This guide also describes the process of authorizing users to access the integrated applications.

Who Should Use This Guide

This guide is intended for administrators who are responsible for configuring user access to applications integrated with FatWire Content Server via the FatWire Web Experience Management Framework.

Related Documents

See the following documents in the FatWire documentation set:

- *FatWire Content Server Administrator's Guide*
- *FatWire Web Experience Management Developer's Guide*
- *FatWire Web Experience Management REST API Resource Reference*

Conventions

The following text conventions are used in this guide:

- **Boldface** type indicates graphical user interface elements that you select.
- *Italic* type indicates book titles, emphasis, or variables for which you supply particular values.
- `Monospace` type indicates file names, URLs, sample code, or text that appears on the screen.
- **`Monospace bold`** type indicates a command.

Third-Party Libraries

FatWire Content Server 7.6 patch 2 and its applications include third-party libraries. For additional information, see *FatWire Content Server 7.6 Patch 2: Third-Party Licenses*.

Chapter 1

Welcome to FatWire WEM Framework

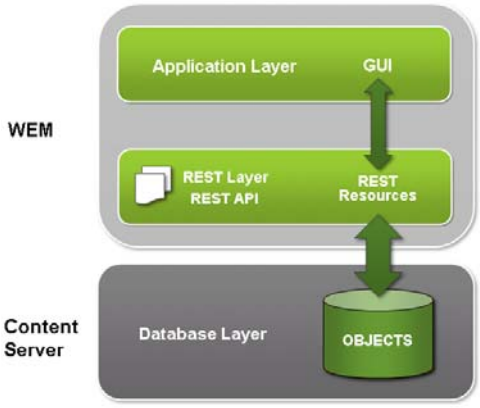
This chapter provides an overview of FatWire Web Experience Management (WEM) Framework and its administrators.

This chapter includes the following sections:

Overview

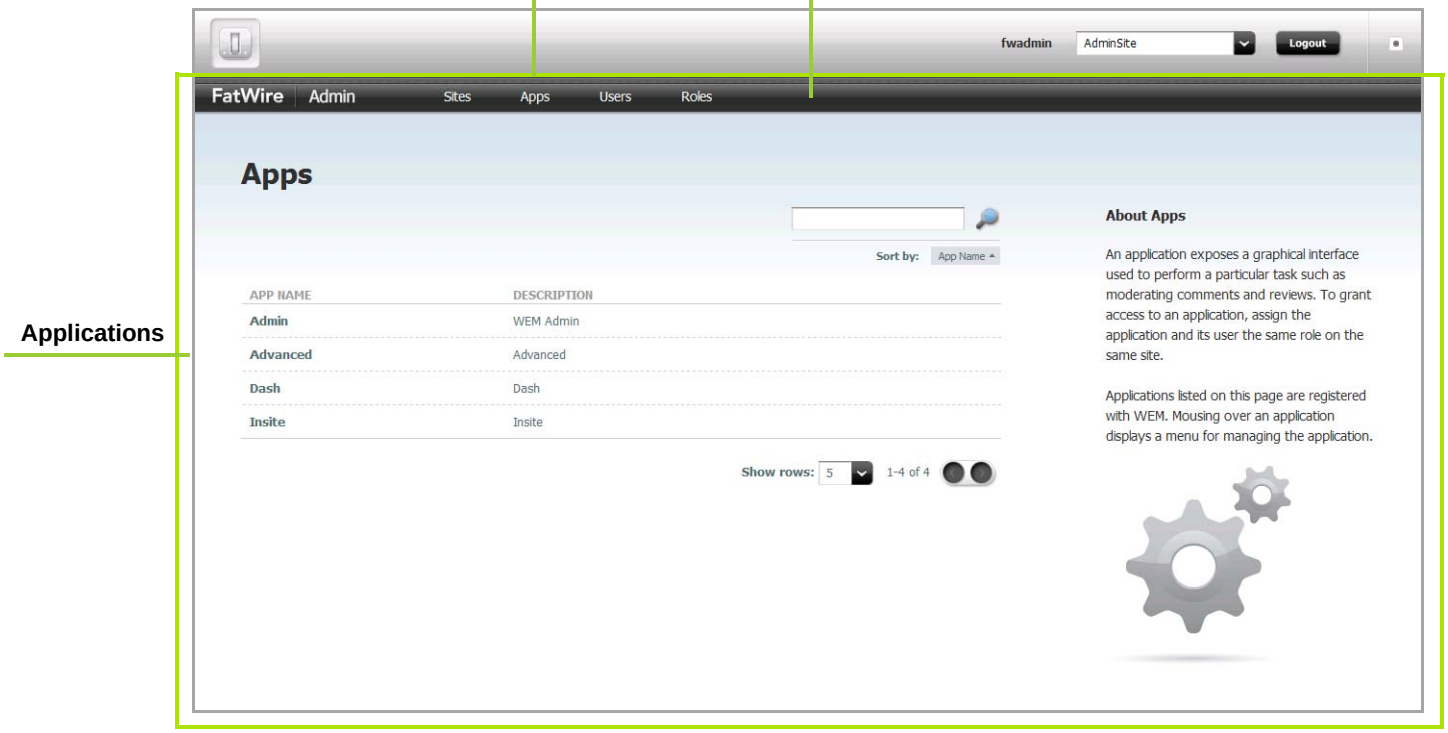
FatWire Web Experience Management (WEM) Framework provides the technology for developing applications to run on the FatWire product suite. A single administrative interface, WEM Admin, supports centralized application management and user authorization. Single sign-on enables users to log in once and gain access to all applications allowed to them during the session.

The WEM Framework requires a content management platform. In this release, the Framework runs on FatWire Content Server and ships with the CS Representational State Transfer (REST) API. Objects in Content Server's database, such as sites, users, and data model map to REST resources in WEM.



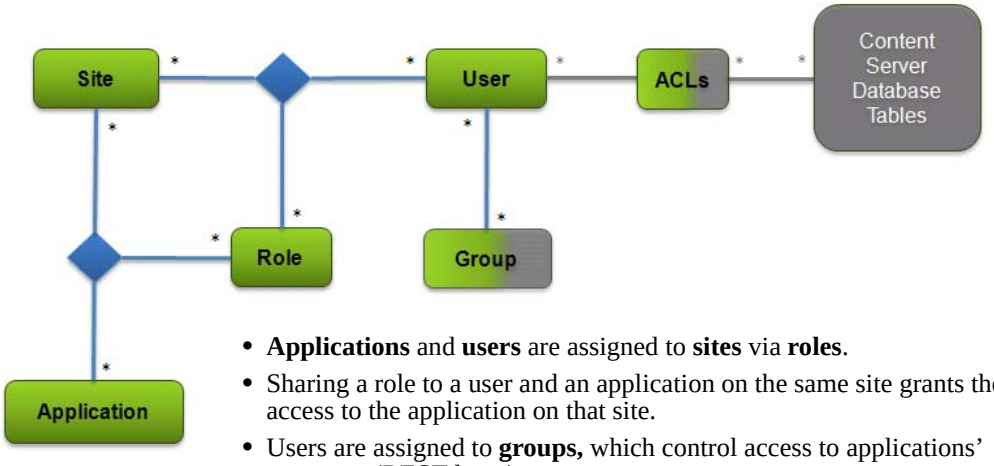
When implemented on WEM, applications communicate with Content Server's database through REST services. The applications appear in WEM Admin as list items on the **Apps** page (Figure 1). Administrators authorize users, which involves configuring access to applications and their resources. To this end, the WEM Admin interface exposes authorization items (along with applications) through links on the **menu bar**.

Figure 1: Apps Page, **WEM Admin**



Coupling the items as shown in Figure 2 enables applications for users.

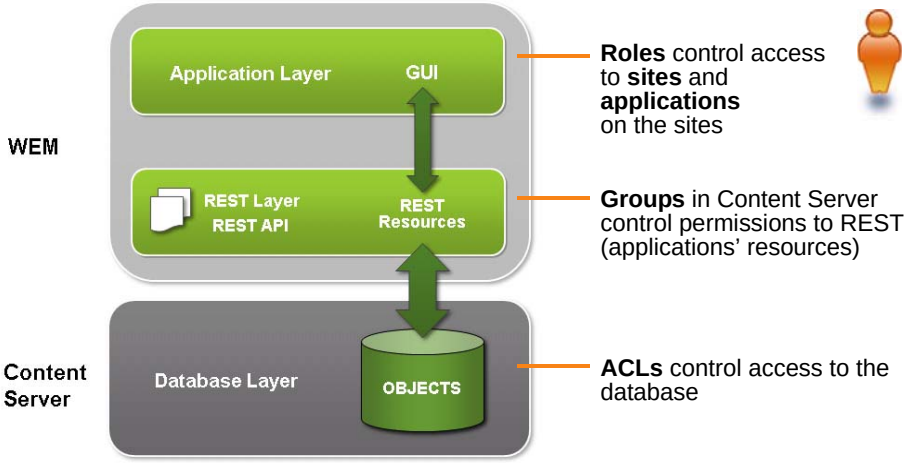
Figure 2: Authorization Model



- **Applications** and **users** are assigned to **sites** via **roles**.
- Sharing a role to a user and an application on the same site grants the user access to the application on that site.
- Users are assigned to **groups,** which control access to applications' resources (REST layer).
- **ACLs** are assigned to users, providing them with access to the system.

Using WEM Admin, general administrators can create and otherwise manage sites, applications, users, and roles. Groups and ACLs must be configured in Content Server Advanced. They are exposed in WEM Admin, in user accounts.

Once the coupling is complete, users are authorized at the database, REST, and application levels.



Experienced Content Server administrators will recognize that the WEM Admin interface extends the use of sites and roles to control access to applications. Roles can also be used within applications to protect interface functions (as in Content Server) and therefore regulate access to the applications' content.

Unlike Content Server, WEM Admin does not expose the data model. The REST API does. In this respect, WEM Admin can be thought of as strictly an authorization interface, supported by Content Server Advanced (for configuring ACLs and groups). The rest of this guide provides instructions for creating and authorizing users, as well as guidelines for managing sites.

Administrative Roles and Permissions

The WEM Framework supports two types of administrators: general and site administrators.

General Administrator

A general administrator has complete control of the system and full permissions to the WEM Admin interface: Sites, Apps, Users, and Roles. Using WEM Admin, general administrators can add and delete sites, applications, users, and roles; modify their details; and perform authorization tasks.

A general administrator in WEM is a Content Server general administrator who is also specially configured for the WEM Framework. During the Content Server installation process, the default general administrator (`fwadmin`) was automatically assigned to the RestAdmin group for unrestricted access to REST services, and enabled on AdminSite where the WEM Admin application runs by default. ***The default general administrator must not be deleted***.

You can create equivalent general administrators, as many as necessary, and you must modify pre-existing general administrators by adding them to the RestAdmin group and AdminSite (via the GeneralAdmin role). Instructions are available in "Creating WEM Users," on page 18. For more information about WEM-related changes to Content Server, see the Content Server rollup installation guide.

Site Administrator

Site administrators are assigned by general administrators to selected sites, where they manage site users and applications. When users are assigned the `SiteAdmin` role in a site other than AdminSite they are implicitly assigned the `SiteAdmin` role in AdminSite. ***Users cannot be assigned the `SiteAdmin` role in only AdminSite***. In the WEM Admin interface, site administrators can access only the "Sites" screen. They can perform the following operations on the sites to which they are assigned:

- Assign and remove users to and from sites
- Assign and remove applications to and from sites
- Modify the role assignments of site users
- Modify the role assignments of applications on the sites

A site admin cannot create, modify, or delete sites, users, and roles. (Your permissions determine which screens and interface functions WEM Admin displays to you.)

Site administrators on Content Server systems running WEM must be specially configured for WEM. They must be assigned to the SiteAdmin_AdminSite group, a default REST security group configured in Content Server Advanced. Instructions are available in "Creating WEM Users," on page 18.

All Administrators

All WEM administrators must be experienced Content Server users.

Content Server Applications

The Content Server interfaces Dash, Advanced, and InSite are registered applications. They are listed on the **Apps** page of the WEM Admin interface. Content Server users can access the applications from WEM once they are authorized at the application level. They can also continue accessing the Content Server applications directly, at the usual URL. The login screen is the following:

Sample Sites

Your Content Server system may have been installed with sample sites, in which case they are listed in the WEM Admin interface, along with your custom sites. The sample sites are:

- FirstSiteII
- BurlingtonFinancial
- GE Lighting
- HelloAssetWorld
- Spark

Quick Reference

The reference section at the end of this guide uses “quick steps” to convey instructions for completing various operations. For example, for administrators who wish to add a user to WEM, the quick step would look like this:

Select **Admin** icon **> Users > Add User >** *fill in the required fields* > **Save and Close**

The steps above mean:

> Select the **Admin** icon, select the **Users** menu, click **Add User**, in the users form fill in the required fields, and then select **Save and Close**.

Chapter 2

Getting Started

This chapter provides instructions for logging in to and navigating the WEM Admin interface.

This chapter contains the following sections:

Logging In and ‘Quick Tour’

WEM is a password-protected framework. When you sign in, WEM determines your status as a general administrator or site administrator and enables only the screens and interface functions that you need to work with. **This guide is for general administrators.** If you are not a general administrator, then certain sections of this guide (such as creating users) do not apply to you.

To log in to WEM

1. Access WEM at the following URL:

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

   where `<server>` is the host name or IP address of the server running WEM, and `<context>` is the name of the web application which was deployed on that server. Depending on how the system was set up, you may also need to include the port number.

2. Log in as the general administrator that was used during the Content Server installation process.

   This guide uses the general administrator’s default credentials:

   User: `fwadmin`

   Password: `xceladmin`

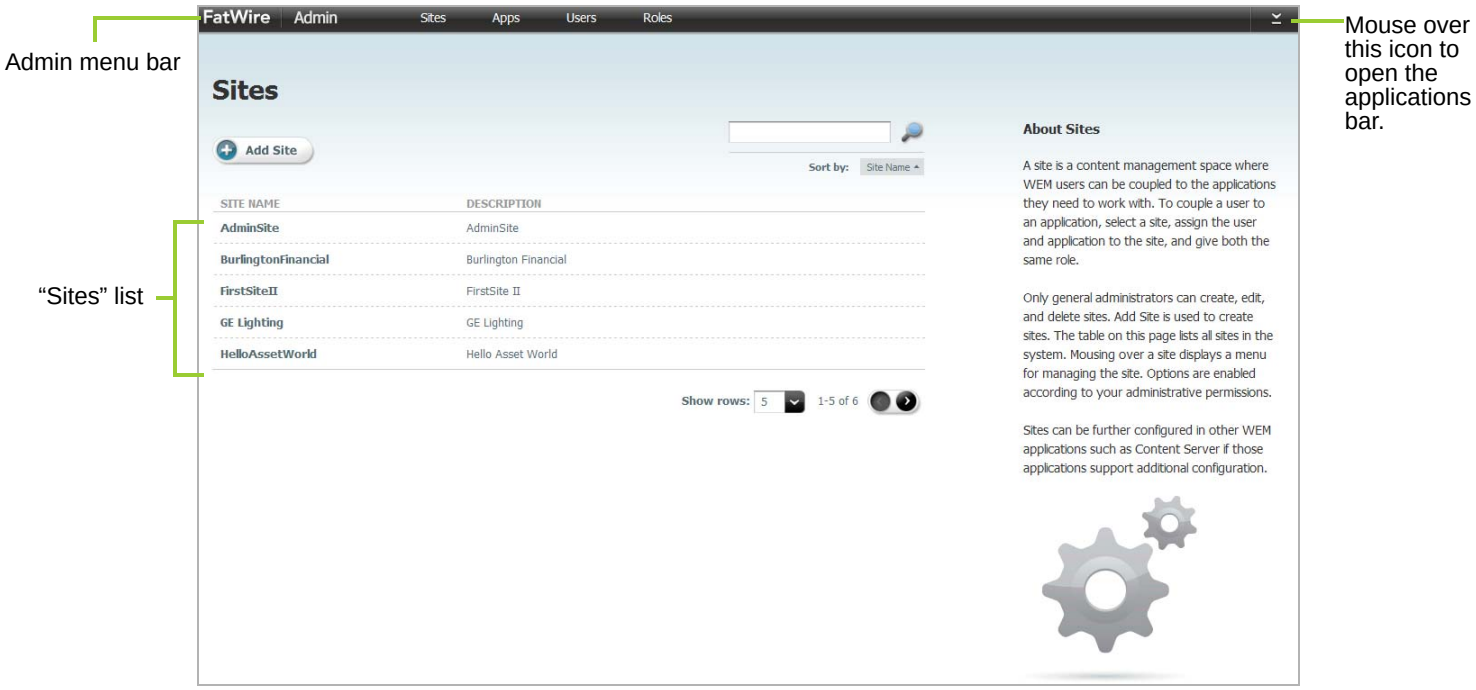
3. Click **Login**.

4. If you are logging in for the first time or in to a site that you have never accessed before, the following screen is displayed:

   Select **AdminSite** and the **Admin** application icon to open the WEM Admin interface.

   The first screen you see is the “Sites” screen.

Figure 3: WEM Admin Interface “Sites” Screen



The “Sites” screen lists all the sites in the system. Site administrators will see only the sites in which they are assigned the SiteAdmin role. If you logged in as a general administrator you also have access to the “Apps,” “Users,” and “Roles” screens.

5. Open the applications bar by mousing over the **down-arrow** at the extreme right of the menu bar. The bar displays the icons of applications that are available to you on the current site, a link to your profile, a drop-down menu of sites accessible to you, the logout button, and the pin icon.

Figure 4: Applications bar

Most recently used applications (up to five icons can be displayed). Click an icon to work with the application.

When more than five applications are running, the “Switch Apps” drop-down menu is displayed for selecting the additional applications. When you select an application from the “Switch Apps” menu, the icon of the selected application replaces the least used application’s icon currently displayed.

Click your user name to manage your profile.

Sites drop-down menu (type-ahead search field).

Your current site is displayed.

Click the pin icon to “pin down” the applications bar (keep it open).

Next Steps

The next chapter shows you how to create users in WEM and authorize them to work with applications.

Chapter 3

Creating and Authorizing Users

This chapter provides information and instructions about creating a user in the WEM Admin interface, and authorizing that user to manage a site and the application(s) available on that site.

This chapter includes the following sections:

Creating WEM Users

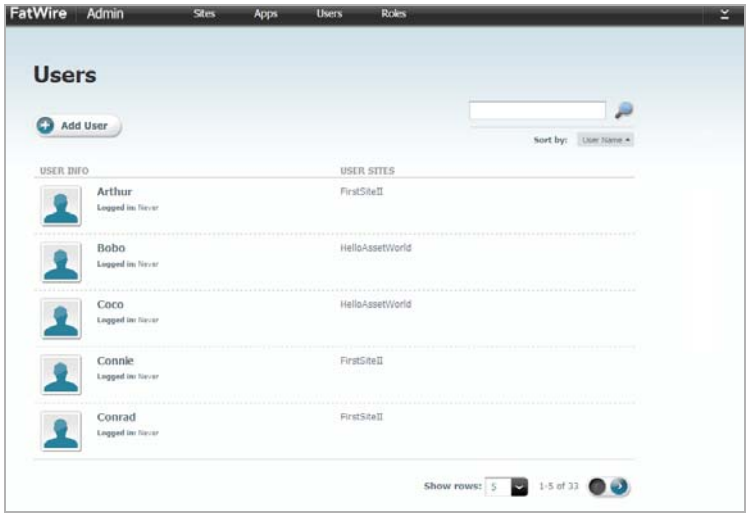
The types of users you can create are general administrators, site administrators, and regular users.

Note

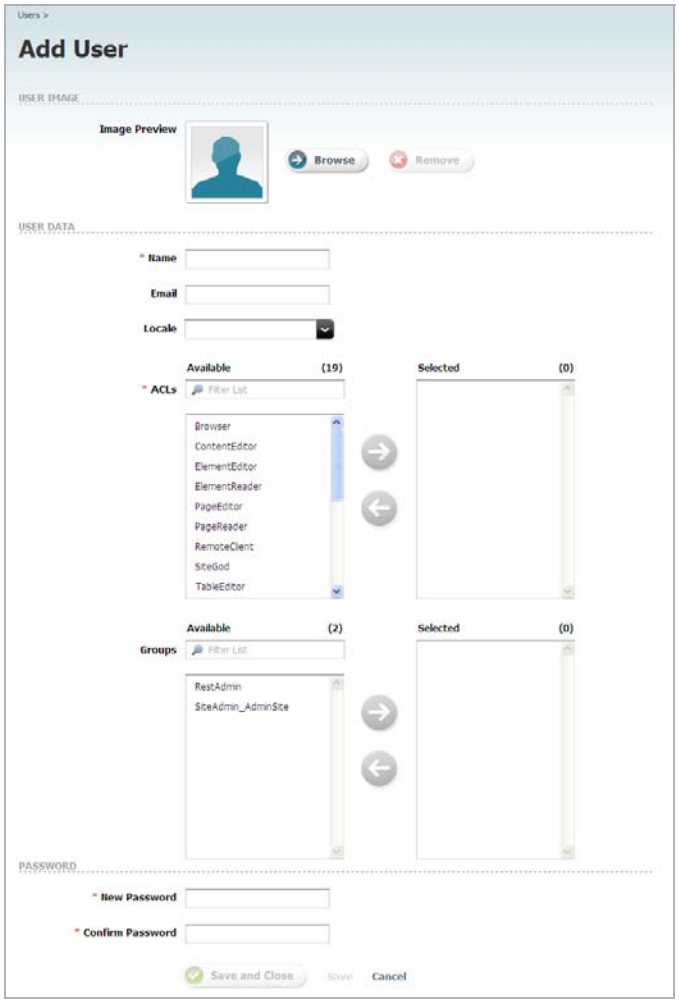
Only general administrators can create users. For information about predefined users, see “Authorizing a Predefined User,” on page 27.

To create the user

1. Log in to the WEM Admin interface as the general administrator that was used during the Content Server installation process.
2. In the Admin menu bar, click **Users**. The “Users” screen is displayed.



3. In the "Users" screen, click the **Add User** button to open the "Add User" form.



Fill in the following fields:

- **Image Preview** – (Optional) Use the **Browse** button to associate a picture with the new user.
- **Name** – Enter a name that the user will use to log in.
- **Email** – (Optional) Enter a valid, unique email address.
- **Locale** – (Optional) Select the user's language preference. If you do not specify a preference, WEM uses the default locale that is set for the user's browser.
- **ACLs** – ACLs regulate the user's access to the database tables. All users require Browser, ElementReader, PageReader, UserReader, and xceleditor. General and site administrators also require xceladmin. General administrators further require TableEditor and UserEditor (and VisitorAdmin, if they use Content Server Engage).

- **Groups** – Groups provide access to REST. They are used to control access to applications' resources.
  - If you are creating a general administrator, assign the user to the RestAdmin group (a default group, configured in Content Server Advanced). This group has unrestricted permissions to REST resources.
  - If you are creating a site administrator, assign the user to the SiteAdmin_AdminSite group (a default group, configured in Content Server Advanced).

> **Note**
>
> Security configurations for groups are available in the Content Server Advanced interface. See "Viewing REST Security Configurations," on page 34.

  - If you are creating a regular user, skip this step, for now. You will assign the user to a group (or groups) in step 4 on page 25, as part of the authorization process ("Authorizing Users to Work with Applications").
- **New Password** – Enter a password that is at least 6 characters long.
- **Confirm Password** – Re-type the password you just entered.

4. Click **Save and Close**.

   At this point the user can log in, but a message will be displayed indicating that the user does not have access to any sites.

To enable the user as an administrator or regular user

5. Assign the user to a site:
   a. From the "Users" screen, mouse over the user, select **Manage User**, and click **Assign to Sites**.
      - If you are creating a general administrator, assign the user to AdminSite.
      - If you are creating a site administrator or regular user, assign the user to a site other than AdminSite.

b. Assign roles to the user on the site:

- If you are creating a general administrator, assign the GeneralAdmin role, which grants the user access to the system.

  The WEM Admin application is now available to the user on AdminSite:

From this menu, the user that you created has access to only AdminSite. To enable access to another site, you must assign the user roles in the desired site. If the roles do not authorize access to any applications on that site, no application icons are displayed below the menu when the user selects the site.

- If you are creating a site administrator, assign the SiteAdmin role.

  A user who is assigned the SiteAdmin role on a site other than AdminSite is implicitly assigned to AdminSite and gains access to the WEM Admin application on AdminSite. In the WEM Admin application, the user can access only the "Sites" screen, which lists only the site(s) in which he is assigned the SiteAdmin role.

From this menu, the user that you created has access to AdminSite and the site in which he is assigned the SiteAdmin role. If the SiteAdmin role does not authorize the user to access any applications on the site in which he is assigned the SiteAdmin role, no application icons are displayed below the menu when the user selects the site.

- If you are creating a regular user, assign the user roles that are not GeneralAdmin or SiteAdmin.

  The user now has access to the site (listed in the menu), but if the user's roles do not authorize access to any applications on that site, no application icons are displayed below the menu.

6. To authorize a user to work with applications, continue to the next section.

Authorizing Users to Work with Applications

Users require authorization to work with applications, such as Content Server's Dash interface. By authorizing a user you are reproducing the couplings shown in Figure 2, on page 9.

This procedure shows you how to authorize a user, which involves:

1. Selecting or creating a site
2. Assigning an application to the site
3. Assigning a user to the same site and coupling the user to the application
4. Assigning the user to a group to enable the user's permissions to REST (applications' resources)

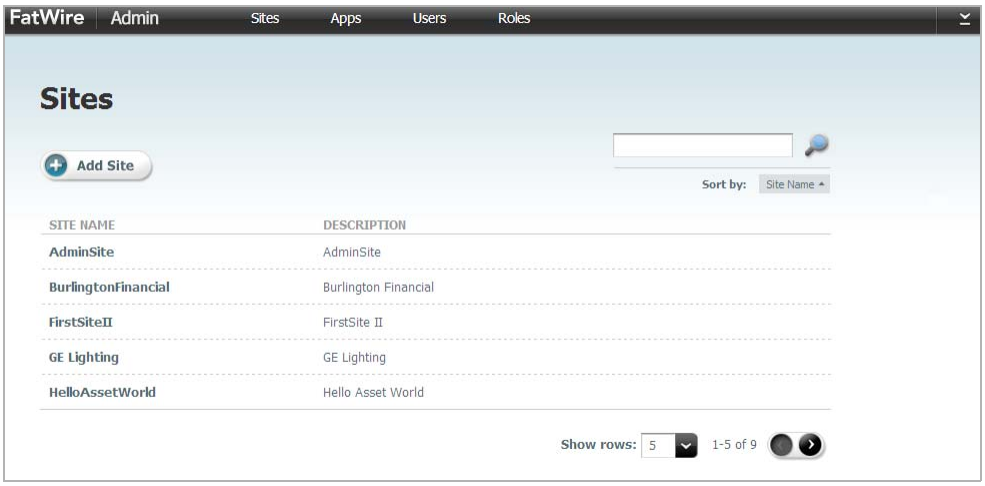
Note

- Both general and site administrators can authorize users.
- If you need access to an application on a given site (Content Server Advanced, for example), authorize yourself to access the application on the site.
- In the steps below, you can select multiple applications and multiple users. For simplicity, instructions specify a single application and user.
- In this procedure, we assume the user you are authorizing will be working with applications that do not specify a predefined user. For information about predefined users, see "Authorizing a Predefined User, on page 27."

To authorize a user

1. **Select or create the site:**

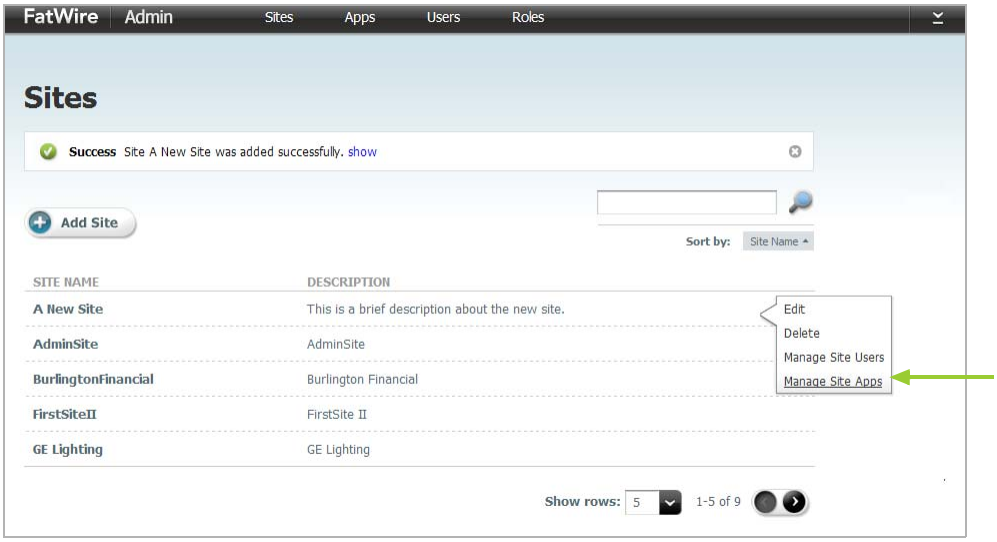
   From the WEM Admin interface, click **Sites** on the Admin menu bar.



   If you are a general administrator you can select a site or add a site (click **Add Site**). If you are a site administrator you can select a site. Your "Sites" screen lists only the sites you are allowed to manage.

2. **Assign an application to the site:**

   a. In the "Sites" screen, mouse over the site's name and click **Manage Site Apps**.



   b. Click **Assign Apps**.

Note

The **Assign Apps** button is dimmed if no applications are registered with WEM.

   1) Select the application you wish to assign to the site and move it to the **Selected** list box. (To search for an application, type its name in the **Filter List** field. The results appear in the **Available** list box).

   2) Click **Continue** to assign roles to the application.

c. In the "Assign Roles to Apps" form, select roles for the application and move them to the **Selected** list box.

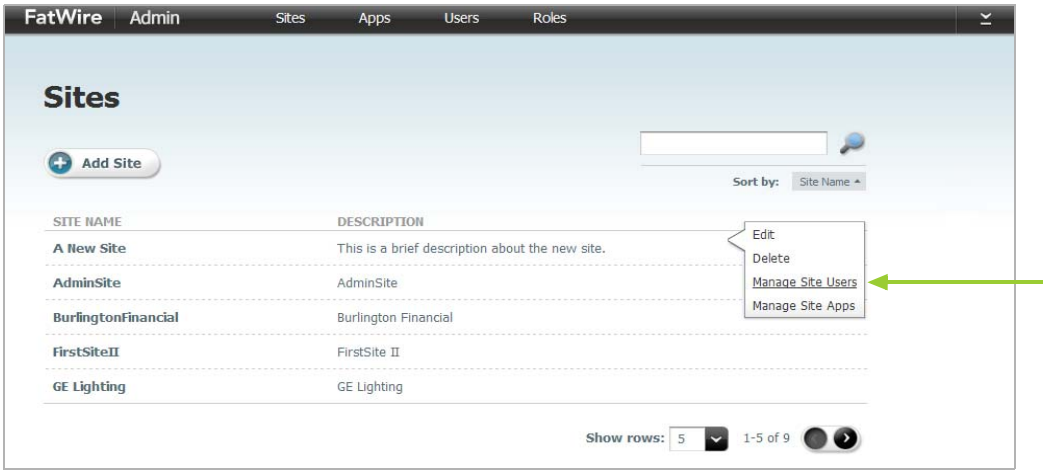
> **Note**
>
> If the application is CS Advanced, assign it the AdvancedUser role. If the application is CS Dash, assign it the DashUser role.
>
> **Take note of the roles you are assigning.** You will assign at least one of those roles to the user on the site to grant the user access to the application.

d. Click **Save and Close**.

3. Assign a user to the site:

a. In the Admin menu bar, click **Sites**.

b. Mouse over the new site's name and click **Manage Site Users**.



c. Click **Assign Users**.

1) In the "Select Users for Site" form, select the user you wish to assign to the site and move the user to the **Selected** list box.
2) Click **Continue** to assign roles to the user.

d. Couple the user to the application (application-level authorization):

In the "Assign Roles to Users" form, assign the user at least one of the roles that you assigned to the application in step c on page 24.

Note

- **For all applications.** Sharing a role to a user and an application on a site grants the user access to the application on that site. If the application is the CS Advanced interface, you must assign the user the AdvancedUser role. If the application is the CS Dash interface, you must assign the user the DashUser role.
- **For applications other than Content Server.** If the application has role-protected interface functions (such as "Edit"), configure access to each function by assigning the user at least one of the function's roles (specifications are available from application developers). The user is then fully authorized at the application level. However, the user will not be able to work with the application's resources until you authorize the user at the REST level. Click **Save and Close** and continue to step 4.
- **For Content Server applications and users.** Content Server has role-protected interface functions. The roles of users configured directly in Content Server are preserved in WEM. They are listed in the WEM Admin interface, site by site. Also, the `application` REST service authorizes Content Server users at the REST level (eliminating step 4 for administrators). Click **Save and Close** and skip to step 5 on page 26.

4. Authorize the user at the REST level:

This step grants the user permissions to operate on resources that are used by the application (selected in step 2 on page 23).

As noted above, skip this step if you are authorizing dedicated Content Server users to access the Content Server applications from WEM. Continue to step 5 on page 26.

a. In the Admin menu bar, click **Users**.

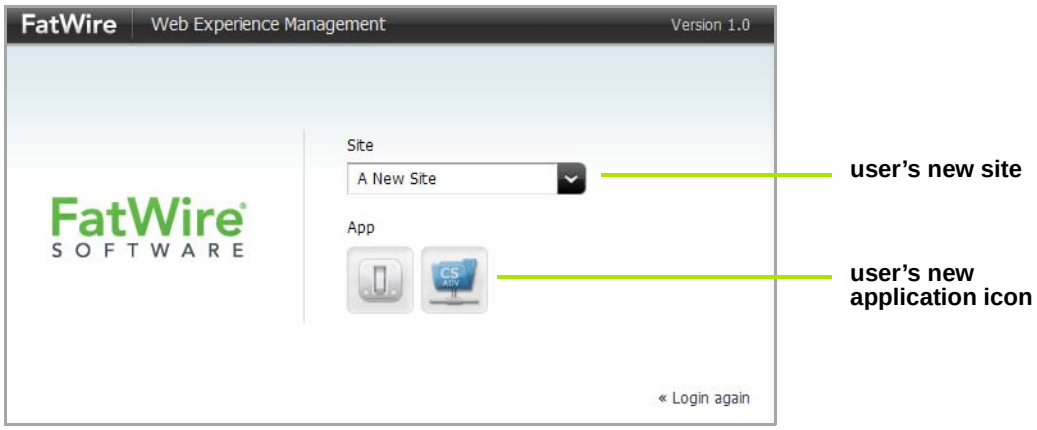
b. In the "Users" screen, mouse over the user you wish to authorize and click **Edit**.

c. In the "Edit User" form, select group(s) for the user. Each group is configured with specific permissions to operate on specific objects (such as asset types and assets), which map to REST resources used by the application. To determine the permissions of the listed REST groups, or to create groups and configure their privileges, see "Authorizing Users to Access Application Resources" on page 33.

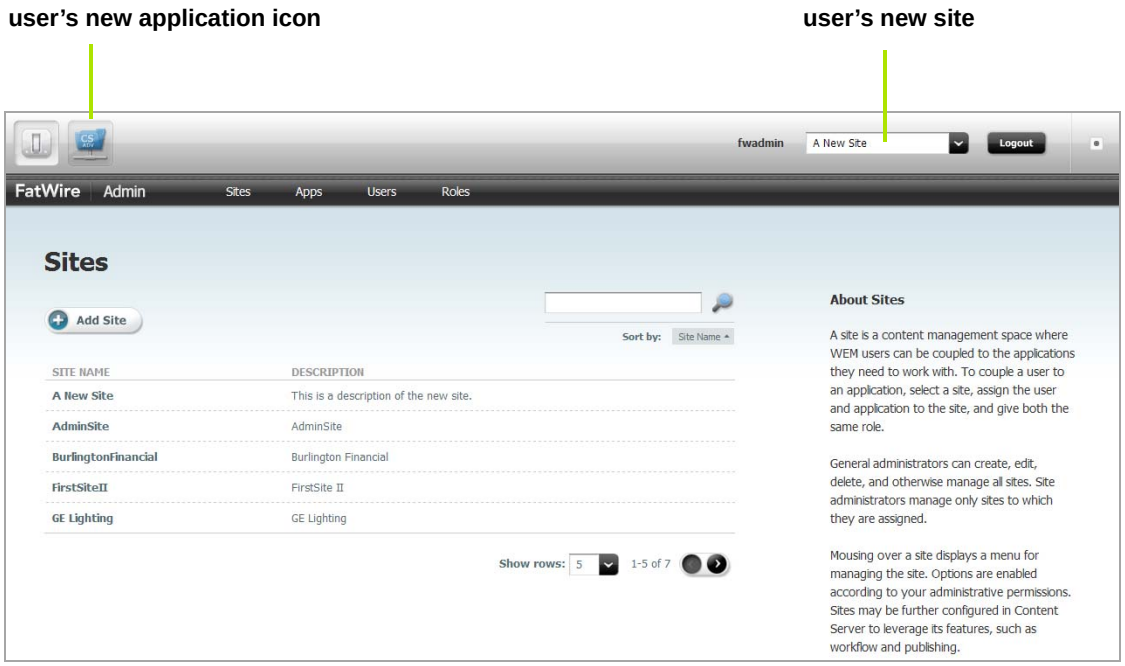
d. Click **Save and Close**.

5. Verify the user's ability to access the new application.

The login screen lists the user's new site (in the "Site" drop-down menu) and displays the application icon below the menu.



The new site is also listed in the drop-down menu next to the name of the logged-in user, and the application icon is displayed in the upper left-hand corner.



6. As a reminder, if you have not yet authorized the user with permissions to REST, complete the steps in Chapter 4, "Configuring REST Security."

If you wish to review or modify the user and/or application assigned to the site, see Chapter 6, "WEM Admin Quick Reference."

Authorizing a Predefined User

Developers specify predefined users in their applications to simplify administrators' authorization processes. Instead of authorizing each user individually at the REST level, you will authorize the predefined user. Logged-in users with access to the application will gain access to the application's resources through the predefined user's membership in REST groups.

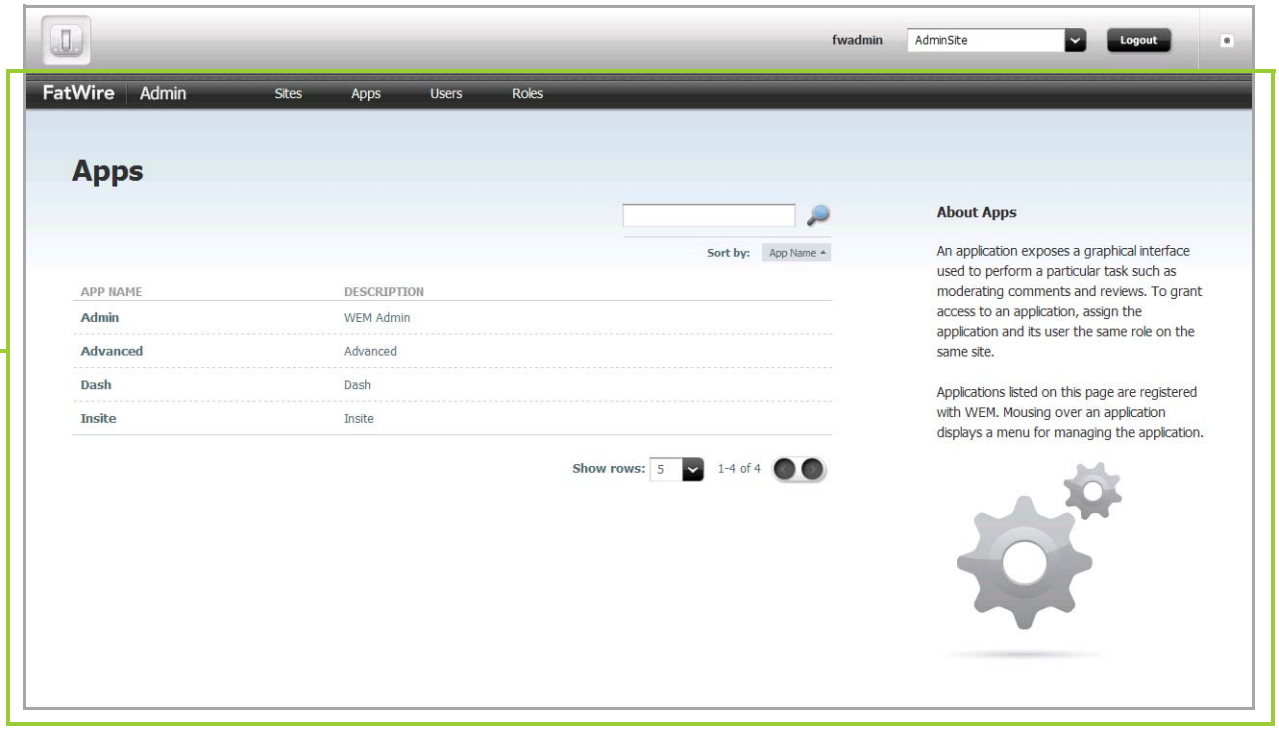
If an application is configured with a predefined user, complete the following steps in the WEM Admin application.

1. Create the predefined user. Have the following information ready:
   - Login name. This name must exactly match the predefined user's name, as specified in the application.
   - Password. The password must exactly match the predefined user's password, as specified in the application.
   - ACLs, which regulate the user's access to the database tables. The predefined user must be assigned the ACLs of the logged-in users who will access the application. All users require Browser, ElementReader, PageReader, UserReader, and xceleditor. General and site admins also require xceladmin. General admins further require TableEditor and UserEditor (and VisitorAdmin, if they use Content Server Engage).
   - Group assignment, which authorizes the user at the REST level (to manage application resources). The predefined user must be assigned to a group with the security privileges that you would otherwise grant to the application users. For information about configuring REST security, see Chapter 4.

   For instructions on creating the user, see "Creating WEM Users," on page 18.
2. Assign the predefined user to the application. For instructions, see "Authorizing Users to Work with Applications," on page 22.
3. Assign users to the application (using the procedure in "Authorizing Users to Work with Applications," on page 22), but skip their assignment to groups (step 4 on page 25).

Authorizing Developers to Register Applications

For applications to be exposed in WEM, they must be registered – that is, created as assets – so they can be displayed through REST services on the Apps page in the WEM Admin interface. Administrators can then authorize users to work with the applications.



Typically, it is developers who register the applications they create. The preferred method is programmatic. If developers choose to register applications manually they must use the Content Server Advanced interface to create assets of type `FW_Application` and `FW_View`. The asset types are enabled on AdminSite. (For background information about registering applications, see the *WEM Framework Developer's Guide*.)

To authorize a developer, ensure the developer is a general administrator (i.e., has complete permissions to the system, including REST services). For instructions on creating a general administrator, see "Creating WEM Users," on page 18.

Ask Your Developers

To ensure your effectiveness in managing applications and users, you will need information from your developers about the applications they have created for WEM.

Resources and Applications

Ask your developers about the resources that are used by custom-built applications.

Once you know which asset types, assets, and other resources users will be working with, you can determine which privileges (such as create, update) the users must be given to those resources and assign the users to groups that have those privileges. Information about configuring groups and assigning users is available in Chapter 4, “Configuring REST Security.

Roles and Applications

Ask your developers whether applications’ interface functions are role-protected.

In WEM, roles are used to manage access to applications. Sharing a role to a user and an application on the same site grants the user access to the application on that site. Roles can also be used in application code to protect interface functions, such as “Edit.” When an application specifies role-protected functions, application users must share at least one role with each interface function.To ensure proper authorization, see “Authorizing Users to Work with Applications,” on page 22.

Predefined Users

Ask your developers whether predefined users are configured in the applications.

If an application specifies a predefined user, you must authorize the predefined user at the REST level, instead of authorizing all application users individually. Security privileges granted to the predefined user by membership in groups will be passed to logged-in users when they access the application. For instructions on authorizing a predefined user, see “Authorizing a Predefined User,” on page 27.

Chapter 4

Configuring REST Security

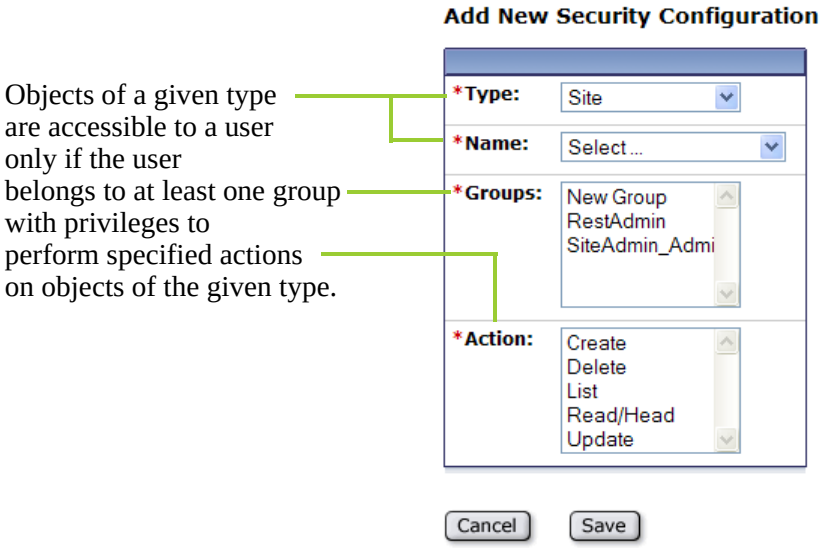
This chapter provides information and instructions about configuring REST security, and contains the following sections:

REST Authorization

REST authorization is the process of granting privileges to perform REST operations on applications' resources, which map to objects in Content Server. REST authorization uses the "deny everything by default" model. If a privilege is not explicitly granted to a particular group, that privilege is denied. General administrators are responsible for authorizing users once the application is deployed and registered with WEM.

Security Model

The WEM security model is based on objects and groups, which are predefined in Content Server, and actions, which you create in Content Server (objects in Content Server map to REST resources in WEM). Security must be configured per object type in Content Server's Advanced interface:



- **Object** is a generic term that refers to any entity such as a site, a user, or an asset. Protected objects are of the following types:

  - Asset Type
  - Asset
  - Index
  - Site
  - Role
  - User
  - User Locale
  - ACL
  - Group
  - Application

- **Security groups** are used to gather users for the purpose of managing their permissions (to operate on objects) simultaneously.
- An action is a security privilege: `LIST`, `HEAD`, `READ`, `UPDATE`, `CREATE`, `DELETE`. Groups are assigned privileges to operate on the objects allowed to the groups. Some objects, such as ACLs, are list-only (they can be created directly in Content Server, but not over REST).

A security configuration is an array, such as shown above, that specifies:

- The protected object type and object(s)
- Groups that are able to access the objects
- Actions that groups (and their members) can perform on the objects

Configuring REST Security

Procedures for configuring REST security are available in “Authorizing Users to Access Application Resources,” on page 33.

Privilege Resolution Algorithm

When configuring a security privilege, you can specify that the privilege applies to all objects of a certain type or a single object of a certain type. For example, granting the privilege to `UPDATE (POST)` any site allows users in the group to modify the details of all sites in WEM. Granting the privilege to `UPDATE (POST)` the FirstSiteII sample site allows users in the group to modify this site’s details in WEM.

The `Asset` object type requires you to specify the site to which the security setting applies, as assets are always accessed from a particular site. The `AssetType` object type can be extended by specifying a subtype, which is used to make the security configuration more granular. For example, setting the `DELETE` privilege on asset type `Content_C` allows a `DELETE` request to be performed on the REST resource `/types/Content_C` (i.e., to delete the `Content_C` asset type from the system).

Because privileges can be granted only to groups, a user’s total privileges are not obvious until they are computed across all of the user’s group. WEM provides a privilege resolution algorithm. Its basic steps are listed below:

1. REST finds the groups in which the user has membership.
2. REST determines which groups can perform which REST operations on which REST resources. If site or subtype is specified, each is taken into account.
3. REST compares the results of steps 1 and 2. If at least one of the groups from step 1 is in the list of groups from step 2, then access is granted. Otherwise, access is denied.

Authorizing Users to Access Application Resources

Before continuing with this section, read the “REST Authorization” section for background information relating to the steps provided below.

- Viewing REST Security Configurations
- Creating a Group
- Adding Users to a Group
- Configuring Security for REST Resources.

Note

Configure security for REST resources requires groups. You will be assigning privileges to the groups. To view the list of groups, continue with the procedure below. To create groups, see “Creating a Group,” on page 36.

Viewing REST Security Configurations

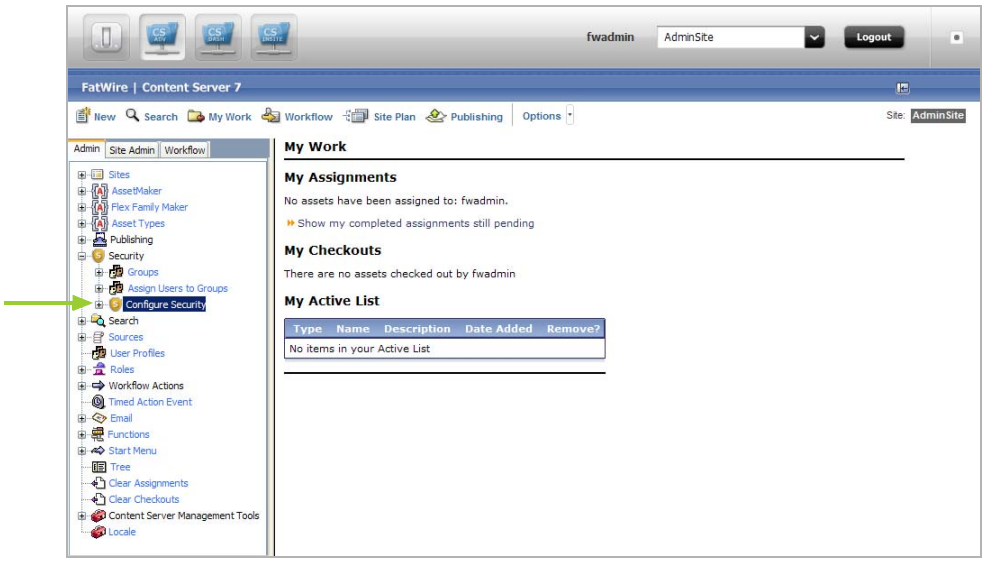
A security configuration identifies which groups have which permissions to which REST resources. Content Server defines security configurations for two default groups. They are RestAdmin and SiteAdmin_AdminSite.

To view REST security configurations

1. Log in to Content Server's Advanced interface as a general administrator:
   a. Navigate to the following URL:

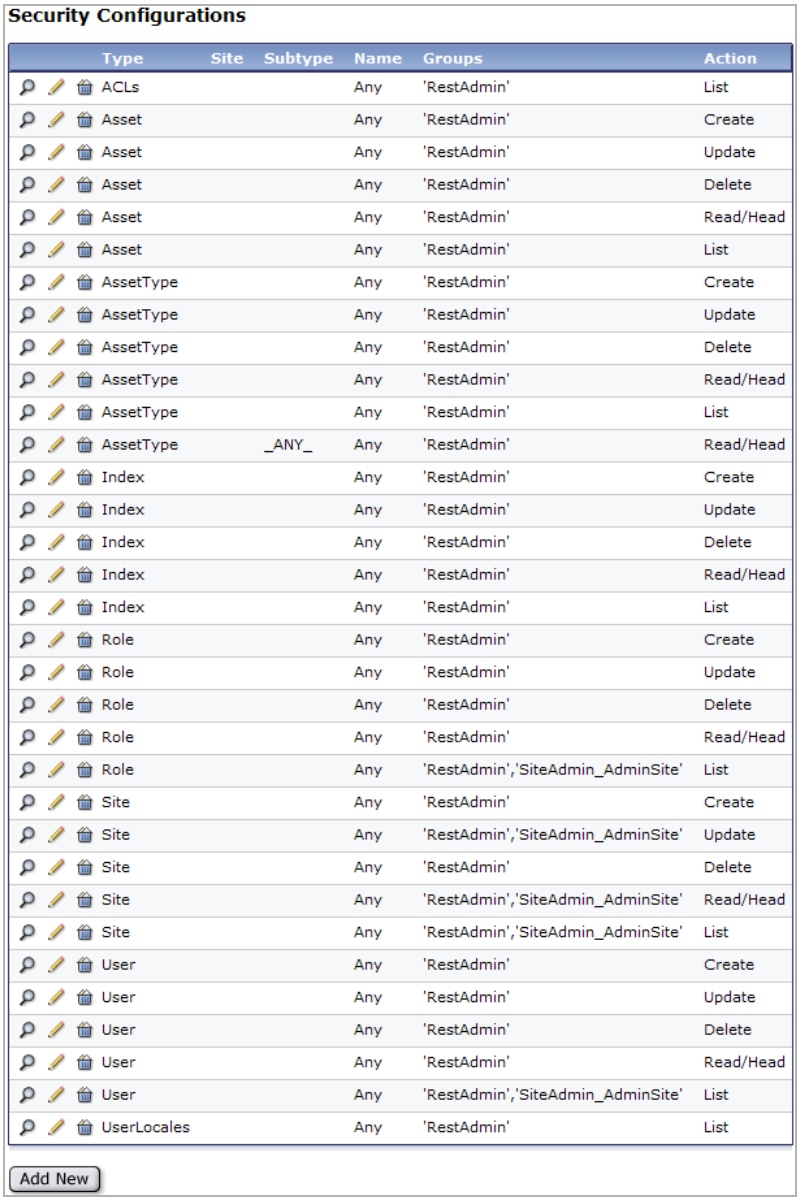
      `http://<server>:<port>/<cs_context>/Xcelerate/LoginPage.html`

   b. Enter your user name and password (which are the same as your WEM login credentials).
   c. Click **Login**.
2. Select the **Admin** tab, expand the **Security** node, and double-click **Configure Security**.



The "Security Configurations" screen is rendered.

"Security Configuration" screen:



Security Configurations

Type	Site	Subtype	Name	Groups	Action
ACLs			Any	'RestAdmin'	List
Asset			Any	'RestAdmin'	Create
Asset			Any	'RestAdmin'	Update
Asset			Any	'RestAdmin'	Delete
Asset			Any	'RestAdmin'	Read/Head
Asset			Any	'RestAdmin'	List
AssetType			Any	'RestAdmin'	Create
AssetType			Any	'RestAdmin'	Update
AssetType			Any	'RestAdmin'	Delete
AssetType			Any	'RestAdmin'	Read/Head
AssetType			Any	'RestAdmin'	List
AssetType		_ANY_	Any	'RestAdmin'	Read/Head
Index			Any	'RestAdmin'	Create
Index			Any	'RestAdmin'	Update
Index			Any	'RestAdmin'	Delete
Index			Any	'RestAdmin'	Read/Head
Index			Any	'RestAdmin'	List
Role			Any	'RestAdmin'	Create
Role			Any	'RestAdmin'	Update
Role			Any	'RestAdmin'	Delete
Role			Any	'RestAdmin'	Read/Head
Role			Any	'RestAdmin','SiteAdmin_AdminSite'	List
Site			Any	'RestAdmin'	Create
Site			Any	'RestAdmin','SiteAdmin_AdminSite'	Update
Site			Any	'RestAdmin'	Delete
Site			Any	'RestAdmin','SiteAdmin_AdminSite'	Read/Head
Site			Any	'RestAdmin','SiteAdmin_AdminSite'	List
User			Any	'RestAdmin'	Create
User			Any	'RestAdmin'	Update
User			Any	'RestAdmin'	Delete
User			Any	'RestAdmin'	Read/Head
User			Any	'RestAdmin','SiteAdmin_AdminSite'	List
UserLocales			Any	'RestAdmin'	List

Add New

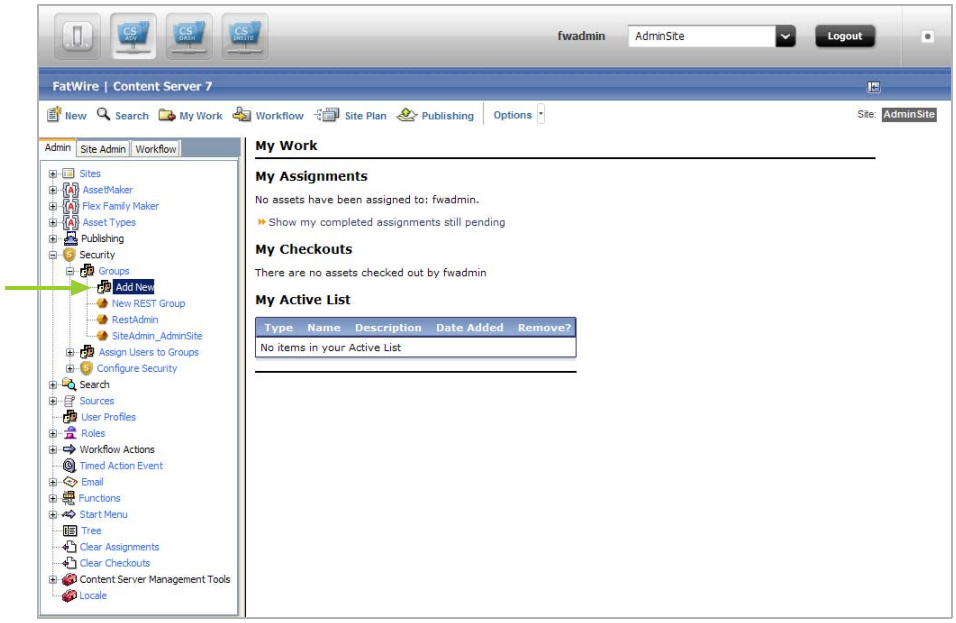
3. Depending on your requirements, continue as follows:
   - To create a new group, see "Creating a Group," on page 36.
   - To add users to a group, see "Adding Users to a Group," on page 37.
   - To configure security privileges for REST resources, see "Configuring Security for REST Resources," on page 39.

Note

To complete this step, ensure that the required groups exist. You will be assigning privileges to the groups.

Creating a Group

1. Log in to Content Server's Advanced interface as a general administrator:
   a. Navigate to the following URL:
      `http://<server>:<port>/<cs_context>/Xcelerate/LoginPage.html`
   b. Enter your user name and password, which are the same as your WEM login credentials.
   c. Click **Login**.
2. In the Content Server tree, select the **Admin** tab, expand **Security** > **Groups**, and double-click **Add New**.



3. In the "Add New Group" form, enter a name and brief description about the group you are creating.

4. Click **Save**.
   The group you created is now listed in the "Admin" tab under the "Groups" node.
5. Now that you have created a group, you can:
   - Add users to the group. For instructions, see "Adding Users to a Group," on page 37.
   - Configure REST security for the group. For instructions, see "Configuring Security for REST Resources," on page 39.

Adding Users to a Group

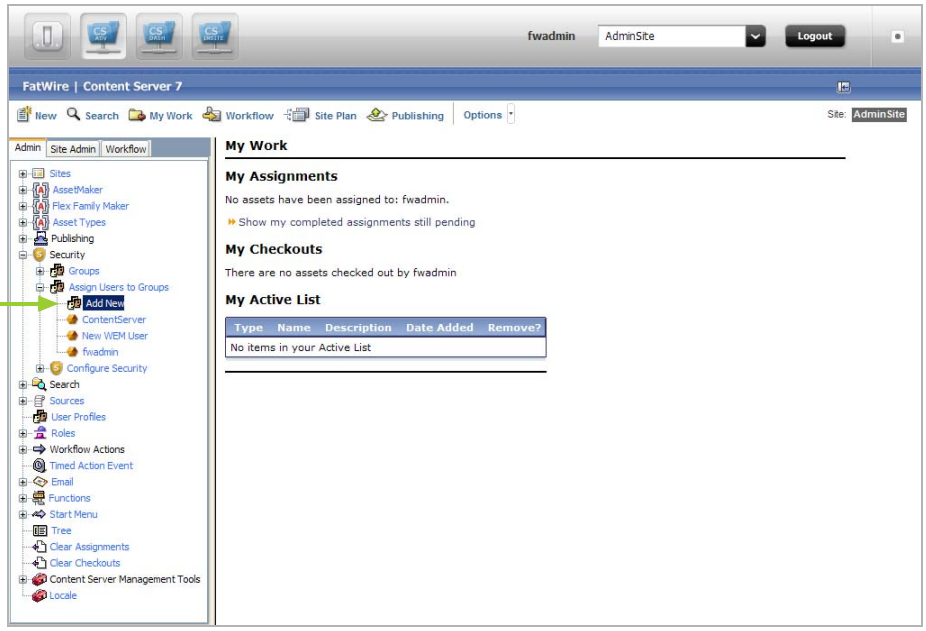
Adding users to a group determines their permissions to operate on REST resources used by the applications the users will access.

To add users to a group

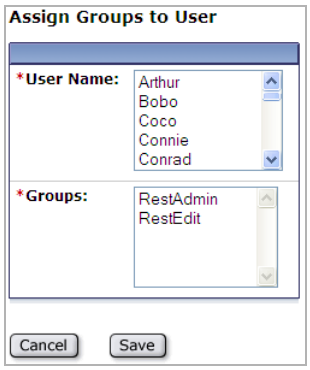
1. Log in to Content Server's Advanced interface as a general administrator:
   a. Navigate to the following URL:

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

   b. Enter your user name and password, which are the same as your WEM login credentials.
   c. Click **Login**.
2. In the Content Server tree, select the **Admin** tab, expand **Security** > **Assign Users to Groups**, and double-click **Add New**.



3. In the "Assign Groups to User" screen, select users and assign them to any combination of the listed groups.



Note

If the user you are looking to assign to the group is not listed, that user is already a member of a group. To assign the user to another group, see step 5.

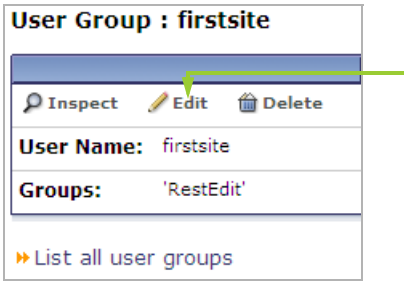
4. Click **Save**.

   The user names you selected are listed in the "Admin" tab, under the "Assign Users to Groups" node. When you double-click a user's name you are able to view the groups to which that user is a member.

5. (Optional) If the name of the user you wish to assign to a given group is not displayed in the "User Name" field, then do the following:

   a. In the Content Server tree, select the **Admin** tab, expand **Security** > **Assign Users to Groups**, and double-click the name of the user you wish to assign to another group.

   b. In the user's "Inspect" form, click **Edit** to render the "Edit User Groups" screen.



   c. In the "Groups" field, select the groups you wish to assign the user to, and then click **Save**.

6. Now that you have added users to a group, you can do the following:

   - Create a new group. For instructions see "Creating a Group," on page 36.
   - Configure security for a group. For instructions, see "Configuring Security for REST Resources," on page 39.

Configuring Security for REST Resources

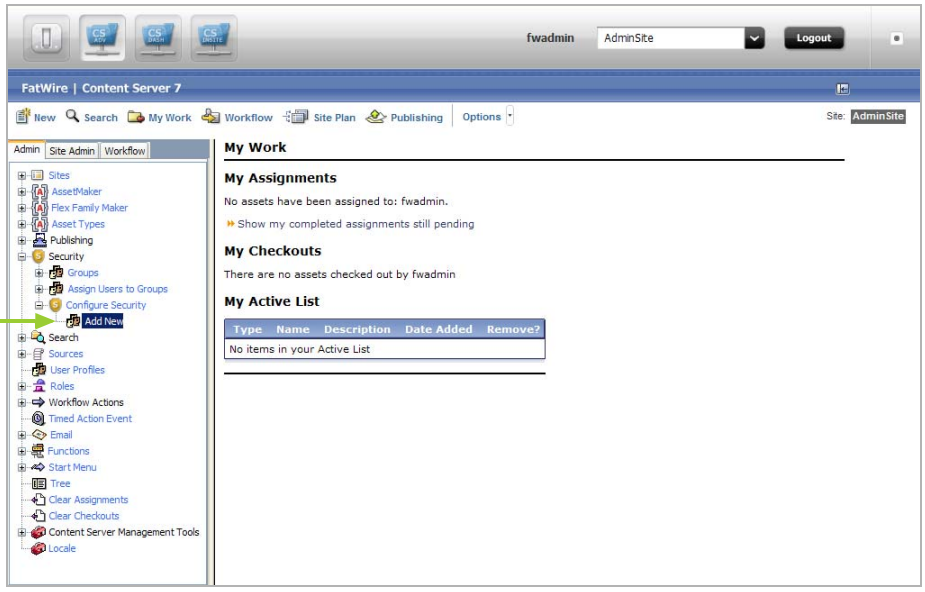
When configuring security, you will specify which object types and objects must be accessible to groups, and which actions the groups can perform on the objects.

To configure security for REST resources

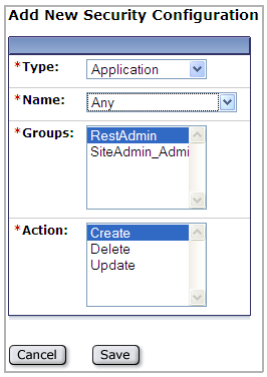
1. Log in to Content Server's Advanced interface as a general administrator:
   a. Navigate to the following URL:

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

   b. Enter your user name and password, which are the same as your WEM login credentials.
   c. Click **Login**.
2. In Content Server's tree select the **Admin** tab, expand **Security** > **Configure Security**, and double-click **Add New**.



3. In the "Add New Security Configuration" screen, you can set security for object types and objects.



The security configuration for the Application resource provides groups with access to the `FW_Application` asset type and `FW_View` asset type. These asset types are used to register applications so they can be exposed as list items on the **Apps** page in WEM Admin. Typically, it is developers who register the applications they create. The preferred method is programmatic. More information about these asset types and registering applications is available in the *WEM Framework Developer's Guide*.

See the tables on the next page for a summary of possible security configurations. See also the *WEM Framework REST API Resource Reference.*

Table 1: Available Actions (Security Privileges)

Action		Description
L	LIST	Allows groups to retrieve specified resources.
R	READ/HEAD	Allows groups to read specified resources. Whereas READ returns the requested resources, HEAD returns metadata describing the requested resources.
C	CREATE	CREATE allows groups to create specified resources.
U	UPDATE	UPDATE allows groups to modify specified resources. **Note:** CREATE and UPDATE are each paired with the READ/HEAD privilege. Assigning one of these privileges to a group automatically assigns the READ/HEAD privilege to the group.
D	DELETE	Allows groups to delete specified resources.

Table 2: Summary of Possible Security Configuration Options

Object Type	Name	Subtype	Site	Possible Actions	See Page ...
ACLs	**Any**			L	42
Application*	**Any**			C, U, D	43
	<AppName>			U, D	
Asset	**Any**		**Any**	L, R, C, U, D	44
	Any		<SiteName>	L, R, C, U, D	
	<AssetType>		<SiteName>	L, R†, C, U, D	
	<AssetType> and <AssetName>		<SiteName>	R†, U, D	
AssetType	**Any**			L, R, C, D	45
	<AssetType>			R, D	
	<AssetType>	**Any**		L	
	<AssetType>	<Subtype>		R	
Group	**Any**			L	46
	<GroupName>			R	
Index	**Any**			L, R, C, U, D	47
	<IndexName>			R, U, D	
Role	**Any**			L, R, C, U, D	48
	<Role>			R, U, D	
Site	**Any**			L, R‡, C, U, D	49
	<SiteName>			R, U, D	
User	**Any**			L, R, C, U, D	50
	<UserName>			R, U, D	
UserDef	**Any**			L	51
UserLocales	**Any**			L	52

* For an example of setting security for applications, see step 3 on page 39.
† READ allows reading associations on the named site.
‡ READ allows reading users and asset types on the named site.

REST Security Configuration Reference

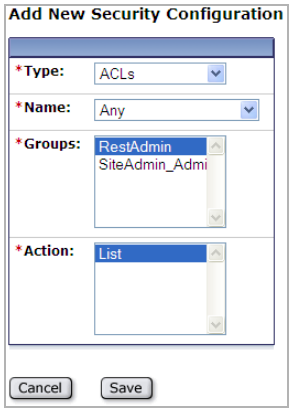
This reference supports Table 2, on page 40. It provides details of the tabulated security configurations.

This reference contains the following sections:

Configuring REST Security for ACL Resources

When assigning groups security privileges to ACLs, you determine which groups will be able to view the ACL resource list.

Figure 5: Add a new security configuration for ACLs



To access this configuration screen:

1. In the Content Server tree, navigate to the **Admin** tab, expand **Security > Configure Security**, and double-click **Add New**.
2. In the "Type" field, select **ACLs**.

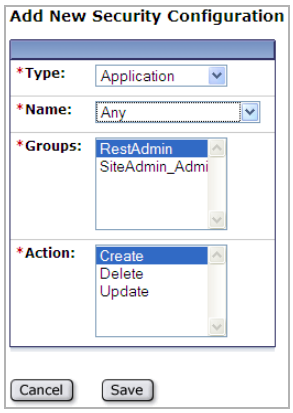
Field Definitions:

Name	The only available option is to make all ACLs available to the group(s).
Groups	Select the group(s) that will have access to the ACLs.
Action	The only available security privilege you can assign to the group(s) is to view the "ACLs" resource list.

Configuring REST Security for Application Resources

When assigning groups security privileges to applications, you determine which groups can perform which operations on the specified applications.

Figure 6: Add a new security configuration for applications



To access this configuration screen:

1. In the Content Server tree, navigate to the **Admin** tab, expand **Security > Configure Security**, and double-click **Add New**.
2. In the “Type” field, select **Application**.

Field Definitions:

Name Select the name of the application you wish to make available to the group(s), or select **Any** to make all applications available to the group(s).

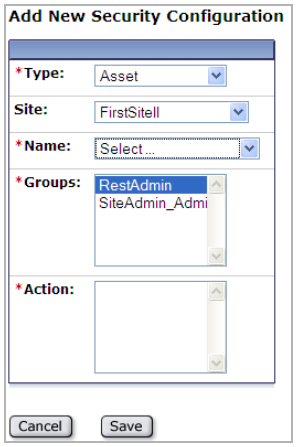
Groups Select the group(s) that will have privileges to operate on the application(s).

Action Assign the security privilege(s) to the group(s). Your options depend on your selections in the previous fields. For example, if you selected **Any** and **Create**, members of your selected groups will be able to create the assets which make the applications accessible in WEM.

Configuring REST Security for Asset Resources

When assigning groups security privileges to assets, you determine which groups can perform which operations on the specified assets.

Figure 7: Add a new security configuration for assets



To access this configuration screen:

1. In the Content Server tree, navigate to the **Admin** tab, expand **Security > Configure Security**, and double-click **Add New**.
2. In the "Type" field, select **Asset**.

Field Definitions:

Site Select the site associated with the asset you wish to make available to the group(s), or select **Any** to make all assets, system wide, available to the group(s).

Name Select the asset type associated with the asset you wish to make available to the group(s), or select **Any** to make all assets available to the group(s). You can also make a specified asset of the selected asset type available to the group(s) by clicking the **Browse** button.

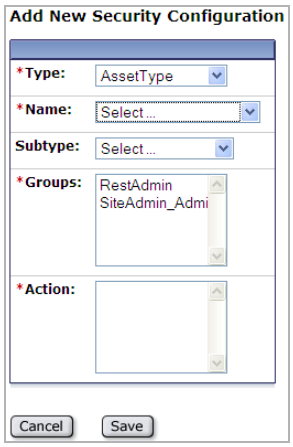
Groups Select the group(s) that will have privileges to operate on the asset(s).

Action Assign the security privilege(s) to the group(s). Your options depend on your selections in the previous fields. For example, if you selected a specific site, a specific asset type, and **List**, members of your selected groups will be able to perform searches in the specified site for assets of the specified asset type.

Configuring REST Security for Asset Type Resources

When assigning groups security privileges to asset types, you determine which groups can perform which operations on the specified asset types.

Figure 8: Add a new security configuration for asset types



To access this configuration screen:

1. In the Content Server tree, navigate to the **Admin** tab, expand **Security > Configure Security**, and double-click **Add New**.
2. In the "Type" field, select **AssetType**.

Field Definitions:

Name Select the asset type(s) you wish to make available to the group(s), or select **Any** to make all asset types available to the group(s).

Subtype (Optional) Select the subtype of the asset type you wish to make available to the group(s).

Note: If you selected the **Any** option in the "Name" field, then the "Subtype" field is not displayed.

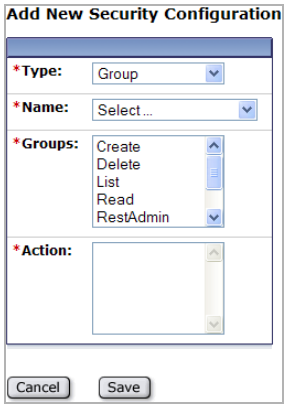
Groups Select the group(s) that will have privileges to operate on the asset type(s).

Action Assign the security privilege(s) to the group(s). Your options depend on your selections in the previous fields. For example, if you selected **Any** and **Create**, members of your selected groups will be able to create asset types.

Configuring REST Security for Group Resources

When assigning groups security privileges to groups, determine which groups can perform which operations on the specified groups.

Figure 9: Add a new security configuration for groups



To access this configuration screen:

1. In the Content Server tree, navigate to the **Admin** tab, expand **Security > Configure Security**, and double-click **Add New**.
2. In the “Type” field, select **Group**.

Field Definitions

Name Select the group(s) you wish to make available to the groups, or select **Any** to make all groups available to the groups.

Groups Select the group(s) that will have privileges to operate on the groups.

Action Assign the security privilege(s) to the group(s). Your options depend on your selections in the previous fields. For example, if you selected **Any** and **List**, members of your selected groups will be able to view a listing of the system’s groups.

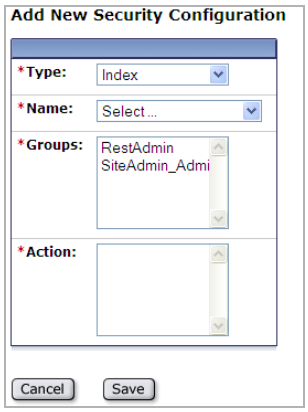
Configuring REST Security for Indexed Asset Type Resources

When assigning groups security privileges to indexed asset types, you determine which groups can perform which operations on the specified indexed asset types.

Note

Before configuring security for indexed asset types, you must enable indexing for Content Server's "Global Search," and "Asset Type Search." If these search features are not enabled, then you will not be able to configure security for indexed asset types.

Figure 10: Add a new security configuration for indexed asset types



To access this configuration screen:

1. In Content Server Advanced, navigate to the **Admin** tab, expand **Security > Configure Security**, and double-click **Add New**.
2. In the "Type" field, select **Index**.

Field Definitions:

Name Select the name of the indexed asset type you wish to make available to the group(s). Select **Any** to make all indexed asset types available to the group(s). Select **Global** to make all indexed asset types associated with the "Global Search" available to the group(s).

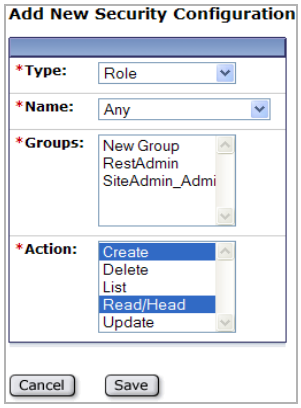
Groups Select the group(s) that will have privileges to operate on the indexed asset type(s).

Action Assign the security privilege(s) to the group(s). Your options depend on your selections in the previous fields. For example, if you selected **Any** and **List**, members of your selected groups will be able to search for assets of all types that are indexed on the system.

Configuring REST Security for Role Resources

When assigning groups security privileges to roles, you determine which groups can perform which operations on the specified roles.

Figure 11: Configure new REST security privileges to role resources



To access this configuration screen:

1. In the Content Server tree, navigate to the **Admin** tab, expand **Security > Configure Security**, and double-click **Add New**.
2. In the “Type” field, select **Role**.

Field Definitions:

Name Select the name of the role you wish to make available to the group(s), or select **Any** to make all roles available to the group(s).

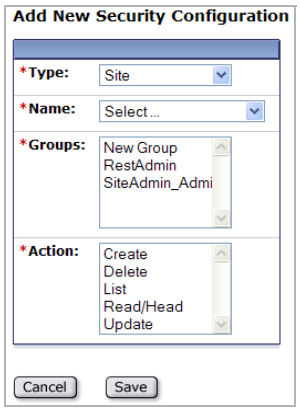
Groups Select the user group(s) that will have privileges to operate on the role(s).

Action Assign the security privilege(s) to the group(s). Your options depend on your selections in the previous fields. For example, if you selected **Any** and **Create**, members of your selected groups will be able to create roles.

Configuring REST Security for Site Resources

When assigning groups security privileges to sites, you determine which groups can perform which operations on the specified sites.

Figure 12: Add a new Site security configuration



To access this configuration screen:

1. In the Content Server tree, navigate to the **Admin** tab, expand **Security > Configure Security**, and double-click **Add New**.
2. In the "Type" field, select **Site**.

Field Definitions:

Name Select the name of the site you wish to make available to groups, or select **Any** to make all sites available to groups.

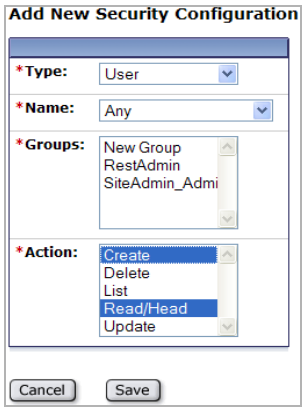
Groups Select the user group(s) that will have privileges to operate on the sites.

Action Assign the security privilege(s) to the group(s). Your menu options depend on your selections in the previous fields. For example, if you selected **Any** and **Create**, members of your selected groups will be able to create sites.

Configuring REST Security for User Resources

When assigning groups security privileges to users, you determine which groups can perform which operations on the specified users.

Figure 13: Add a new Role security configuration



To access this configuration screen:

1. In the Content Server tree, navigate to the **Admin** tab, expand **Security > Configure Security**, and double-click **Add New**.
2. In the “Type” field, select **User**.

Field Definitions:

Name Select the name of the user you wish to make available to groups, or select the **Any** option to make all users available to groups.

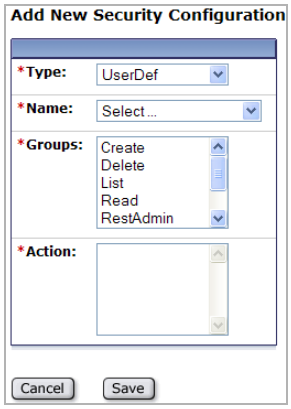
Groups Select the group(s) that will have privileges to operate on the user(s).

Action Assign the security privilege(s) to the group(s). Your menu options depend on your selections in the previous fields. For example, if you selected **Any** and **Create**, members of your selected groups will be able to create users.

Configuring REST Security for UserDef Resources

When assigning groups security privileges to user definitions, you determine which groups can view the system's user definitions.

Figure 14: Add new security configuration for user definitions



To access this configuration screen:

1. In the Content Server tree, navigate to the **Admin** tab, expand **Security > Configure Security**, and double-click **Add New**.
2. In the "Type" field, select **UserDef**.

Field Definitions:

Name The only available option is to make all user definitions available to groups.

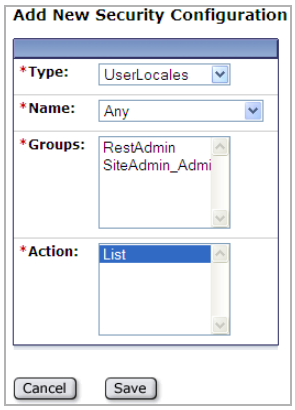
Groups Select the group(s) that will have privileges to view user definitions.

Action The only available security privilege you can assign to the group(s) is **Read/ Head**, which enables the members of your selected groups to view your system's user definitions.

Configuring REST Security for UserLocale Resources

When assigning groups security privileges to user locales, you determine which groups can view the UserLocale resource list.

Figure 15: Add a new User Locale security configuration



To access this configuration screen:

1. In the Content Server tree, navigate to the **Admin** tab, expand **Security > Configure Security**, and double-click **Add New**.
2. In the "Type" field, select **UserLocales**.

Field Definitions:

Name	The only available option is to make all user locales available to groups.
Groups	Select the group(s) that will have privileges to view user locales.
Action	The only available security privilege you can assign to the group(s) is to view a listing of the system's user locales.

Chapter 5

Working with Sites

This chapter provides instructions for managing sites that are created in WEM Admin but used in the Content Server applications, and vice versa.

This chapter contains the following sections:

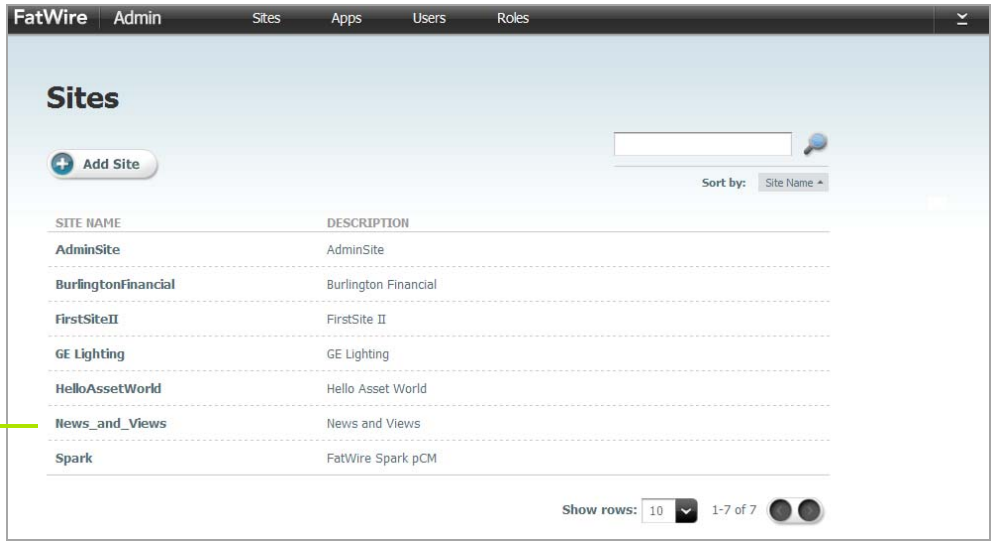
Managing Content Server Sites in the WEM Framework

When using the WEM Admin interface to delete or modify sites, ensure they are not active content management sites in the Content Server platform. Deleting sites from the WEM Admin interface deletes the sites from the system and from any applications where the sites are in use. The same applies to other objects, such as roles, with one difference.

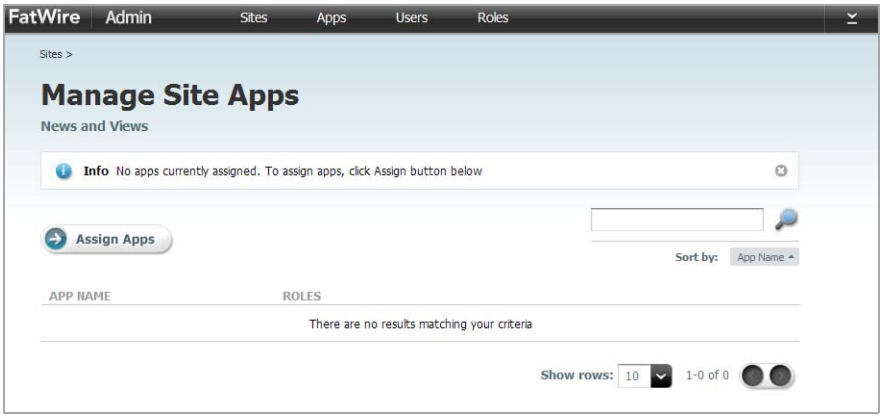
When you attempt to delete a role that is assigned to users and applications, you will be presented with a list of dependencies which you must clear in order to delete the role. When you attempt to delete a site you will be prompted to confirm your decision. It is assumed that you have determined the status of the site.

In WEM Admin you can expose active Content Server sites for quick access by configuring the Content Server applications to run on those sites and assigning yourself to those sites. For example:

1. If you configure a site named “News_and_Views” in Content Server Advanced, the site is listed on the “Sites” screen in WEM Admin:

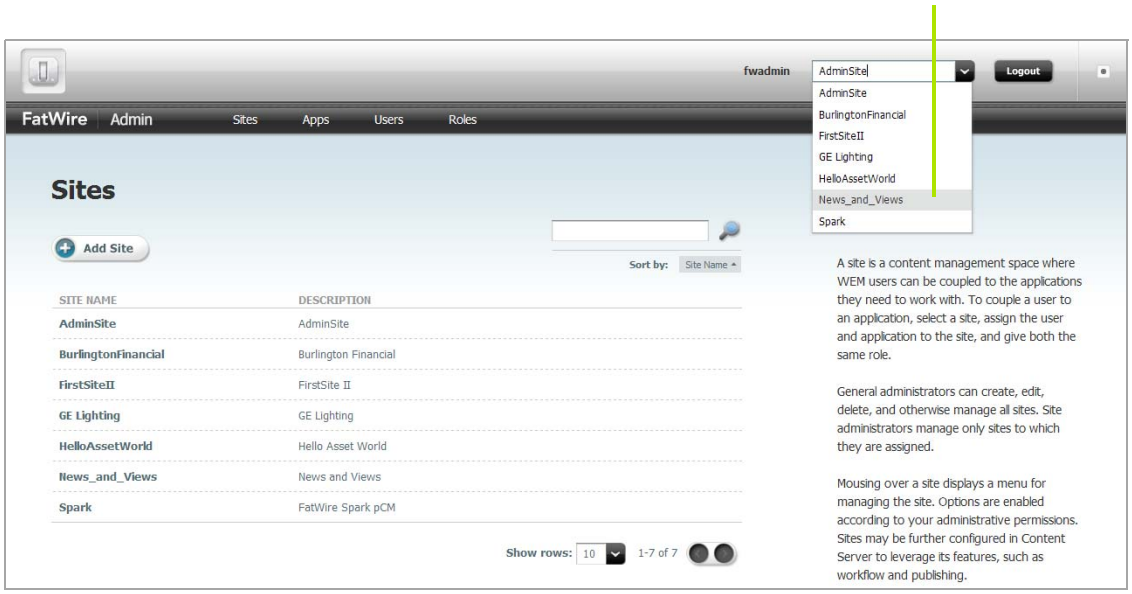


2. Navigate to **News_and_Views** and click **Manage Site Apps**.

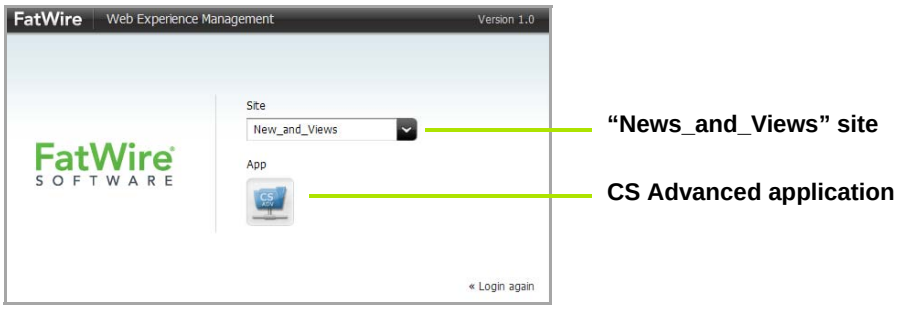


With no assigned applications, the site may be regarded as inactive.

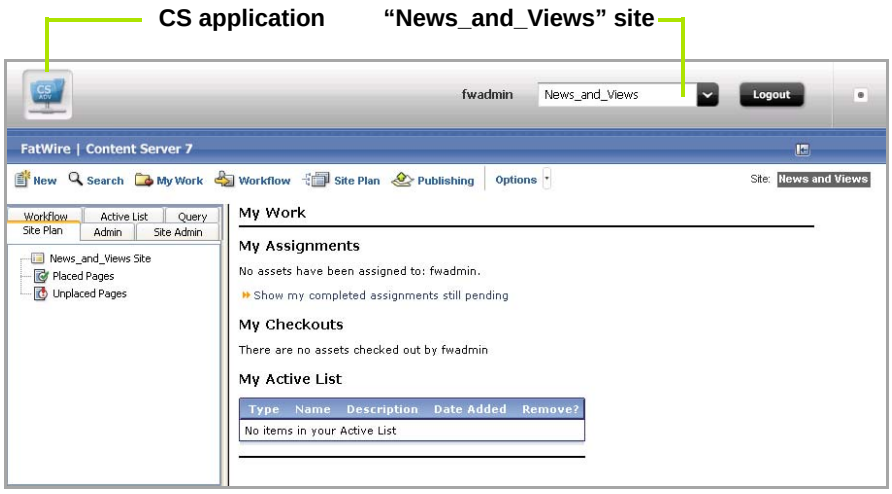
3. When you assign the CS Advanced application and yourself to "News_and_Views," the site is listed as an option in the drop-down menu (refresh the display, if necessary).



4. Selecting **News_and_Views** from the menu displays the login screen. The site is listed in the drop-down menu; below is the application icon.



Once logged in, you will see the CS Advanced application icon at the left and the name of the site at the right, in the drop-down menu. Subsequent access does not require login.



Enabling Tree Tabs

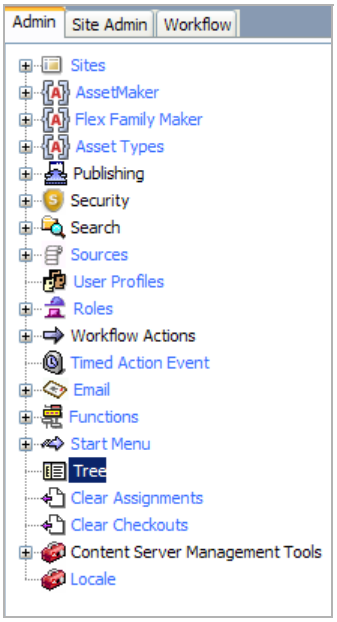
Sites created in the WEM Admin interface are exposed in Content Server Advanced, but not configured for use in Content Server Advanced. A general administrator must enable operations on each site by enabling Content Server's tree, tab by tab.

Enabling the Advanced interface's tree and tabs for a WEM site

1. Log in to Content Server's Advanced interface as a general administrator:
   a. Navigate to the following URL:

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

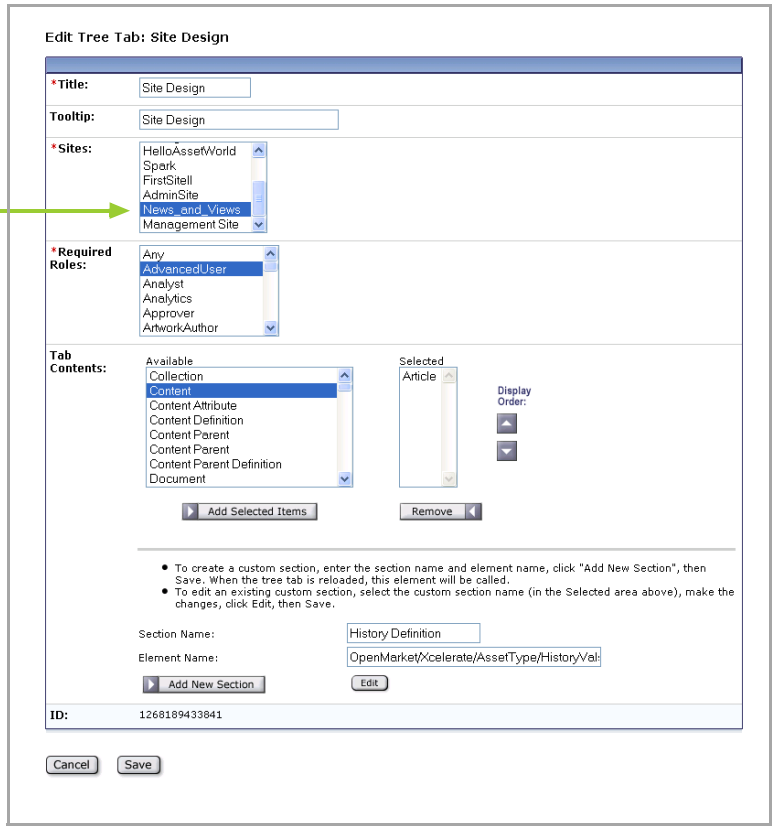
   b. Enter your user name and password, which are the same as your WEM login credentials.
   c. Click **Login**.
2. Enable the relevant Content Server tree tabs for the site that you created in the WEM Admin interface.
   a. Navigate to the Content Server tree and select the **Admin** tab.
   b. Double-click the **Tree** node.



   c. Individually select each tab you wish to enable. For example, suppose you want to enable the **Site Design** tab:
      1) From the list of tree tabs, click **Site Design**.
      2) In the "Tree Tab" form, click **Edit**.

The “Edit” form is rendered (for the **Site Design** tab).

Ctrl-click the sites where you wish to enable the Site Design tab



3) In the “Sites” selection box, select sites on which the tab must be enabled.
4) Select roles that are allowed to access the tab.
5) Select content for the tab.
6) Click **Save**.
7) If you wish to enable additional tabs, click **List all Tree Tabs** (at the bottom of the “Edit” form) and continue as in the steps above.

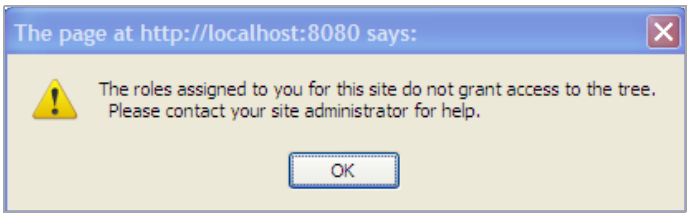
3. Now that you have enabled the Content Server tree and tabs on the sites, continue to the next section to make sure the tree and the tabs are rendered properly.

Verify the Tree Tabs are Enabled

The tabs you have enabled in the previous section are accessible only to users who share a role with each tab. Verify site by site that the tree and tabs are enabled.

1. Log in to Content Server’s Advanced interface as a user who shares one of the roles assigned to a given tab (or tabs).
2. Select the site. You should see the Content Server tree, along with the tabs you enabled for the site.

3. If Content Server's tree is not enabled, you will see the following error message.



Verify the site and role assignments for the user and the tab.

Chapter 6

WEM Admin Quick Reference

This chapter provides you with tips and a quick reference for managing and working with the sites, applications, users, and roles associated with the WEM Framework and includes the following sections:

Quick Tips for Managing WEM

Before following instructions in the rest of this section, take note of a few tips:

- (Optional) If you are experimenting with WEM sites, users, and roles you may want to distinguish them from dedicated Content Server sites, users, and roles. For example, you can add a description for the site/user/role, or prefixing the name with “WEM_” (or a similar qualifier). **Note that once a site, user, or role is created, its name cannot be changed**.
- ACLs are required for user accounts. ACLs can be created only by general administrators and only in Content Server’s **Admin** tab.
- Sharing a role to a user and an application grants the user access to the application in that site.
- Applications can have role-protected interface functions. Sharing a role to a user and an interface function grants the user access to the interface function.
- Groups provide access to REST. They must be configured in Content Server Advanced.
- Groups are used to control access to applications’ resources.

  If a custom-built application does not specify a predefined user, authorize application users at the application and REST levels.

  If a custom-built application specifies a predefined user, authorize that user at the system, application, and REST levels. Authorize application users at the application level.

The rest of this section provides you with a quick reference to help you create and manage sites, applications, users, and roles in WEM:

Managing Sites

Only general administrators can create, edit, and delete sites. The “Sites” screen is accessible to general and site administrators.

Table 3: Managing Sites

Admin	Action	Path
WEM General Admin	Create a site	WEM Admin interface > **Sites** > **Add Site** > *fill in the fields* > **Save and Close** **Note:** A site’s name can only contain alphanumeric characters (no symbols).
	Edit a site	WEM Admin interface > **Sites** > *mouse over the site you wish to edit* > **Edit** > *modify the fields* > **Save and Close** **Note:** You cannot modify the name of a site.
	Delete a site	1. WEM Admin interface > **Sites** > *mouse over the site you wish to delete* > **Delete** 2. In the warning box, click **Delete**.
WEM General and Site Admins	Add an application to a site	1. WEM Admin interface > **Sites** > *mouse over the site you wish to add an application to* > **Manage Site Apps** > **Assign Apps** 2. In the “Select Apps for Site” form, select the applications you wish to add to the site and move them to the **Selected** list box. 3. Click **Continue** 4. In the “Assign Roles to App” form, select the roles you wish to assign to the applications and move them to the **Selected** list box. 5. Click **Save and Close**. **Note:** For general admins who want an alternate way to add an application to a site, see “Managing Applications,” on page 63.
	Assign users to a site	1. WEM Admin interface > **Sites** > *mouse over the site you wish to assign users to* > **Manage Site Users** > **Assign Users** 2. In the “Select Users for Site” form, select users to assign to the site and move them to the **Selected** list box. 3. Click **Continue**. 4. In the “Assign Roles to Users” form, select the roles you wish to assign to the users and move them to the **Selected** list box. 5. Click **Save and Close**. **Note:** For general admins who want an alternate way to assign users to a site, see “Managing Users,” on page 64.

Table 3: Managing Sites *(continued)*

Admin	Action	Path
WEM General and Site Admins *(continued)*	Reassign roles to a user	**Caution:** Reassigning a user's roles on a site in WEM may uncouple the user from certain applications on that site. To reassign roles to a user: 1. WEM Admin interface > **Sites** > *mouse over the site whose user you wish to modify* > **Manage Site Users** 2. In the "Manage Site Users" screen: *mouse over the user whose site roles you wish to modify* > **Assign Roles to User** 3. In the "Assign Roles to User" form, assign new roles to the site user, or unassign roles, as necessary. 4. Click **Save and Close**. **Note:** For general admins who want an alternate way to modify a user's roles in a site, see "Managing Users," on page 64.
	Reassign roles to an application	**Caution:** Reassigning an application's roles on a site in WEM may uncouple the application from certain users on that site. To reassign roles to an application: 1. WEM Admin interface > **Sites** > *mouse over the site whose application you wish to modify* > **Manage Site Apps** 2. In the "Manage Site Apps" screen: *mouse over the application whose site roles you wish to modify* > **Assign Roles to App** 3. In the "Assign Roles to App" form, assign new roles to the application, or unassign roles, as necessary. 4. Click **Save and Close**. **Note:** For general admins who want an alternate way to modify an application's roles in a site, see "Managing Applications," on page 63.
	Remove a user from a site	1. WEM Admin interface > **Sites** > *mouse over the site you wish to remove the user from* > **Manage Site Users** 2. In the "Manage Site Users" screen: *mouse over the user you wish to remove from the site* > **Remove** 3. In the warning box, click **Remove**. **Note:** For general admins who want an alternate way to remove a user from a specific site, see "Managing Users," on page 64.
	Remove an application from a site	1. WEM Admin interface > **Sites** > *mouse over the site you wish to remove an application from* > **Manage Site Apps** 2. In the "Manage Site Apps" screen, *mouse over the application you wish to remove from the site* > **Remove** 3. In the warning box, click **Remove**. **Note:** For general admins who want an alternate way to remove an application from a site, see "Managing Applications," on page 63.

Managing Applications

Only general administrators can modify applications (their descriptions). The "Apps" screen is accessible only to general administrators.

Table 4: Managing Applications

Action	Path
Modify an application	1. WEM Admin interface > **Apps** > *mouse over the application you wish to modify* > **Edit** > *modify the fields:* • **Name** – Cannot be modified. • **Tooltip** – The name that appears when you mouse over an application's icon. • **Description** – Short explanation describing the application. 2. Click **Save and Close**.
Assign an application to a site	1. WEM Admin interface > **Apps** > *mouse over the application you wish to assign to a site* > **Manage App** > **Assign to Sites** 2. In the "Select Sites for App" form, select the sites to which you will assign the application and move them to the **Selected** list box. 3. Click **Continue**. 4. In the "Assign Roles to App" form, select the role(s) you wish to assign to the application and move them to the **Selected** list box. 5. Click **Save and Close**. **Note:** For an alternate way to add an application to a site, see "Managing Sites," on page 61.
Reassign roles to an application	**Caution:** Reassigning an application's roles on a site in WEM may uncouple the application from certain users on that site. To reassign roles to an application: 1. WEM Admin interface > **Apps** > *mouse over the application whose roles you wish to modify for a select site* > **Manage App** 2. In the "Manage App" screen: *mouse over the site in which you wish to modify the application's roles* > **Assign Roles to App** 3. In the "Assign Roles to App" form, add roles to an application, or remove roles, as necessary. 4. Click **Save and Close**. **Note:** For an alternate way to modify an application's roles in a site, see "Managing Sites," on page 61.
Remove an application from a site	1. WEM Admin interface > **Apps** > *mouse over the application you wish to remove from the site* > **Manage App** 2. In the "Manage App" screen, *mouse over the site you wish to remove the application from* > **Remove** 3. In the warning box, click **Remove**. **Note:** For an alternate way to remove an application from a site, see "Managing Sites," on page 61.

Managing Users

Only general administrators can create, edit, and delete users. The “Users” screen is accessible only to general administrators.

Table 5: Managing Users

Action	Path
Create a user	1. WEM Admin interface > **Users** > **Add User** > *fill in the fields*: • **ACLs** – ACLs determine the user’s access permissions to the database. **Note:** You cannot create ACLs in the WEM Admin interface. • **Groups –** Groups determine the user’s access permissions to REST (applications’ resources). Two default groups are configured: RestAdmin (a general administrator group) and SiteAdmin_AdminSite (a site administrator group). 2. Click **Save and Close**. **Note:** The user is able to log in. To access sites and applications, the user must be enabled.
Enable a user	1. WEM Admin interface > **Users** > *mouse over the user you wish to enable* > **Manage User** > **Assign to Sites** 2. In the “Select Sites for User” form: • If you are enabling a general administrator, assign the user to AdminSite. • If you are enabling a site administrator, assign the user to a site other than AdminSite. • If you are enabling a regular user, assign the user to a site other than AdminSite. 3. Click **Continue**. 4. In the “Assign Roles to User” form: • If you are enabling a general administrator, assign the user the GeneralAdmin role. • If you are enabling a site administrator, assign the user the SiteAdmin role. • If you are enabling a regular user, assign the user roles that are not GeneralAdmin or SiteAdmin. 5. Click **Save and Close**.
Assign a user to a site	1. WEM Admin interface > **Users** > *mouse over the user you wish to assign to the site* > **Manage User** > **Assign to Sites** 2. In the “Select Sites for User” form, select the site(s) that you wish to assign to the user and move them to the **Selected** list box. 3. Click **Continue**. 4. In the “Assign Roles to User” form, select the roles you wish to assign to the user and move them to the **Selected** list box. 5. Click **Save and Close**. **Note:** For an alternate way to add a user to a site, see “Managing Sites,” on page 61.
Edit a user	WEM Admin interface > **Users** > *mouse over the user you wish to modify* > **Edit** > *modify the desired fields* > **Save and Close** **Note:** You cannot modify a user’s name once the user is saved.

Table 5: Managing Users *(continued)*

Action	Path
Reassign roles to a user	1. WEM Admin interface > **Users** > *mouse over the user whose roles you wish to modify* > **Manage User** 2. In the "Manage User" screen: *mouse over the site you wish to modify the user's roles in* > **Assign Roles to User** 3. In the "Assign Roles to User" form add roles to a user, or remove roles, as necessary. 4. Click **Save and Close**.
Assign a user to a group	1. WEM Admin interface > **Users** > *mouse over the user you wish to assign to a group* > **Edit** 2. In the "Groups" field, select the appropriate group(s) and move them to the **Selected** list box. 3. Click **Save and Close**. **Note:** Groups provide access to REST. They are used to control access to applications' resources.
Remove a user from a site	1. WEM Admin interface > **Users** > *mouse over the user you wish to remove from a site* > **Manage User** > *mouse over the site you wish to remove the user from* > **Remove** 2. In the warning box, click **Remove**. **Note:** For an alternate way to remove a user from a site, see "Managing Sites," on page 61.
Delete a user from WEM	1. WEM Admin interface > **Users** > *mouse over the user you wish to remove from the system* > **Delete** 2. In the warning box, click **Delete**.

Managing Roles

Only general administrators can create, edit, and delete roles. The “Roles” screen is accessible only to general administrators

Table 6: Managing Roles

Action	Path
Add a role	WEM Admin interface > **Roles** > **Add Role** > *fill in the fields* > **Save and Close**
Edit a role	WEM Admin interface > **Roles** > *mouse over the role you wish to modify* > **Edit** > *modify the desired fields* > **Save and Close** **Note:** You cannot modify a role’s name once the role is saved.
Delete a role	1. WEM Admin interface > **Roles** > *mouse over the role you wish to remove* > **Delete** 2. In the warning box, click **Delete**. **Note:** If the role is assigned to users and/or applications, it cannot be deleted until you unassign the role from the user and applications. You will be presented with the “Role Dependencies” screen is rendered. Review the table of dependencies. **Delete all Dependencies** removes the role from its users and applications and deletes the role from the system.

Managing Profiles

General administrators can modify user profiles.

Table 7: Managing Profiles

User	Action	Path
WEM General Admin	Modify a user's profile	WEM Admin interface > **Users** > *mouse over the user's name whose profile you wish to modify* > **Edit** > *modify the desired fields* > **Save and Close**
All WEM users	Modify your profile	WEM Admin interface > **open the applications bar** > *click your user name* > *modify the desired fields* > **Save and Close**