Introduction to Managing Users

Ever heard a retailer advertise as a "one stop shop" for anything you want? The idea is they have so much stuff that whatever you want is probably there. Liferay's Control Panel is like this. Where do you create Users, Organizations, or Sites? Where do you configure permissions and plugins and pretty much anything else? ou do it from the Control Panel.

The Control Panel is divided into six main areas: Users, Sites, Apps, Configuration, and Workflow. The Users section lets you create and manage Users, Organizations, User Groups, Roles, and Password Policies. If monitoring has been enabled, you can also view all the live sessions of your Users.

Anonymous User: *Anonymous Anonymous* is used for the new Managing User Data functionality. Created the first time an administrator clicks *Delete Personal Data* for a User, *Anonymous Anonymous* is a deactivated User assigned anonymized assets. The Anonymous User is configurable, so the name and configuration details might be different in your virtual instance.

Begin exploring Liferay's User Management functionality by reading about adding and editing users.

Users and Organizations

Users and *Organizations* are fundamental entities. If your site requires people (even just a set of site administrators) to have accounts to do anything, you need to know about users. If your users are at all divided hierarchically, like into departments, you'll find that organizations are helpful.

You're probably not surprised to hear that Users and Organizations are managed in the Control Panel's *Users and Organizations* section. If it were any different, it'd be weird.

Consider the Lunar Resort site. Consider what you'd do if

- An employee leaves the company to join that pesky competitor, Martian Resort and Luxury Spa.
- An employee joins the resort as a new Mechanical Crew member.
- An employee is promoted from Crew Supervisor to Department Head and needs the requisite permissions.
- You need to organize the users by department.
- A new department is added to the Lunar Resort and the employees need their own internal website.
- An employee gets married, and their name changes.

The user tasks listed above are all resolved in the Users and Organizations section of the Control Panel.

What are Users?

In case there's any confusion over the term, a User is an entity that can sign into the portal and do something. Generally a User has more privileges, called Permissions, than a Guest of your site, who does not sign in. Users are assigned Roles, and Roles define the User's privileges.

Understanding Users is pretty straightforward. Organizations are a bit trickier, but a smart administrator like you is undoubtedly up to the challenge. Read more about Organizations here.

The remaining articles in this section give you guidance on managing (creating, deleting, editing, and more) Users and Organizations.

Adding, Editing, and Deleting Users

At the root of managing Users is adding, editing, and deleting them. As long as you're the Administrative user, you can do all these things and more.

Adding Users

Here's how to edit Users:

1. From the Product Menu, click *Control Panel → Users → Users and Organizations*.
2. In the Users tab, click the *Add* button .

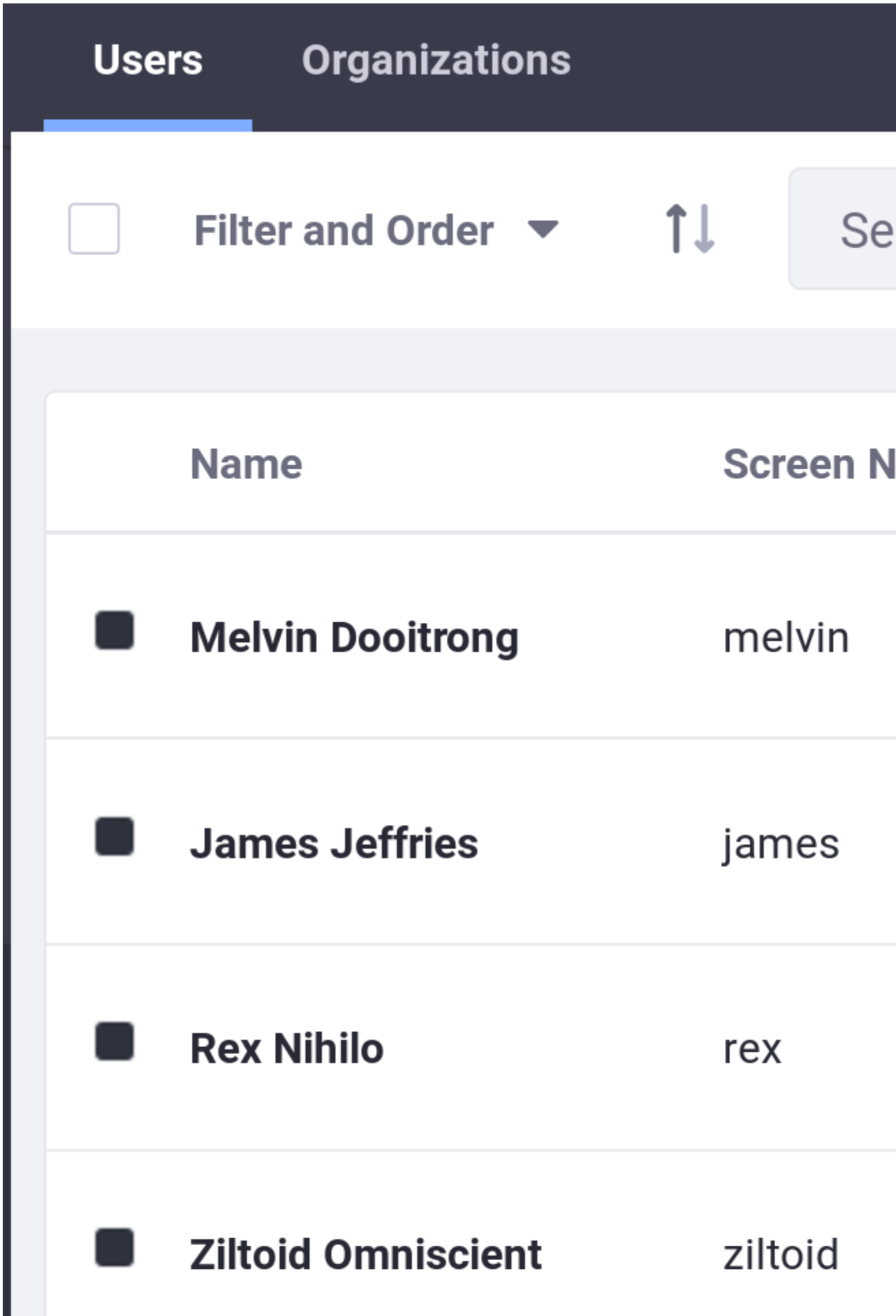
Users
Organizations
Filter and Order
Se
Name
Screen N
Melvin Dooitrong
melvin
James Jeffries
james
Rex Nihilo
rex
Ziltoid Omniscient
ziltoid

Figure 1: Add Users from the Users and Organizations section of the Control Panel.

3. Fill out the Add User form and click *Save*. At a minimum, provide a Screen Name, First Name, Last Name, and Email Address for the User.

   Note: Screen names and email addresses are not interchangeable. A screen name cannot contain an `@` symbol because it is used in the URL to a User's private page.

   The Add User functionality is split over several independent forms. Saving the first form creates the User, and then you'll see a success message saying

```
Success. Your request completed successfully.
```

After submission of the first form, you see a larger form with many sections. The one you're on is the Information section. To the left is a navigation pane where you can continue configuring the user you're adding by clicking through the available sections. The options in the left menu change as you click through the tabs at the top. Peruse the sections for the three tabs (General, Contact, Preferences) and fill in all the applicable information.

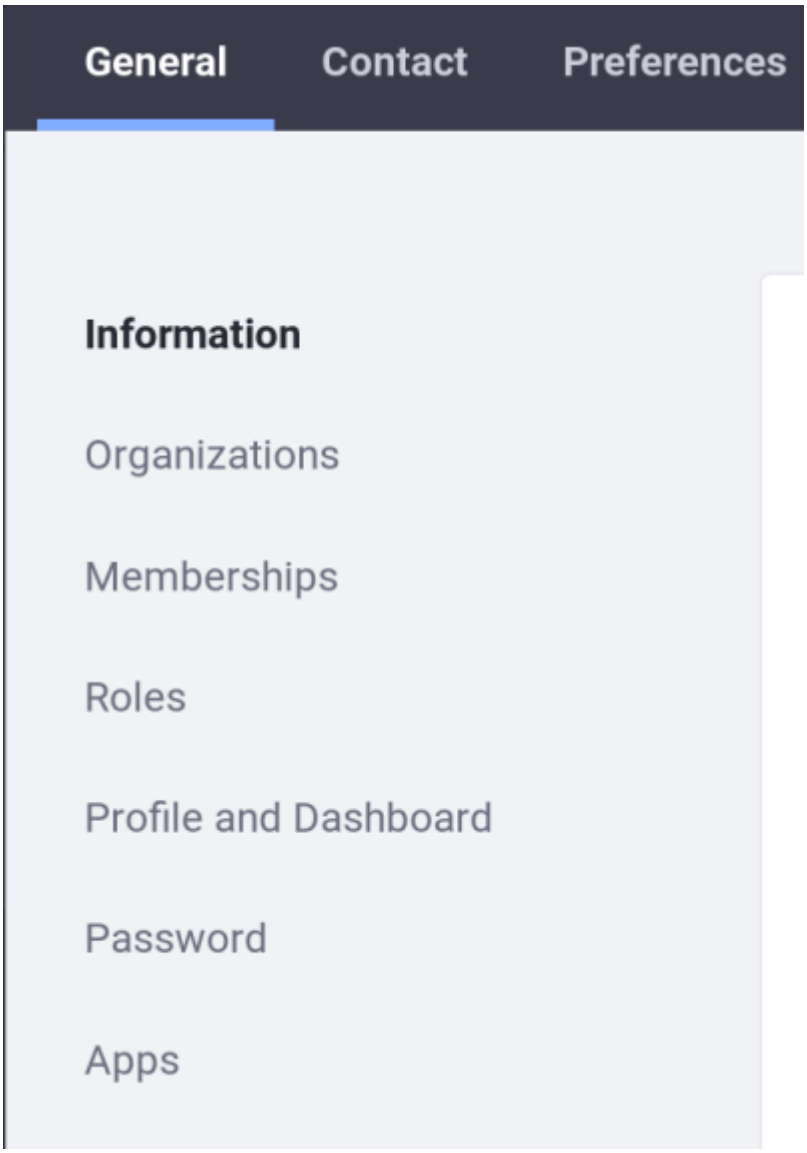

Figure 2: At a minimum, enter a screen name, email address, and first name to create a new user account. Then you'll be taken to the Information form and can continue configuring the user.

You don’t have to fill anything else out right now. Just note that when the user account was created, a password was automatically generated. If Liferay was correctly installed and a mail server was set up, an email message with the User’s new password was sent to the User’s email address.

If you haven’t set up a mail server, click the *Password* item from the General menu and manually set a password for your new user. Enter the new password twice.

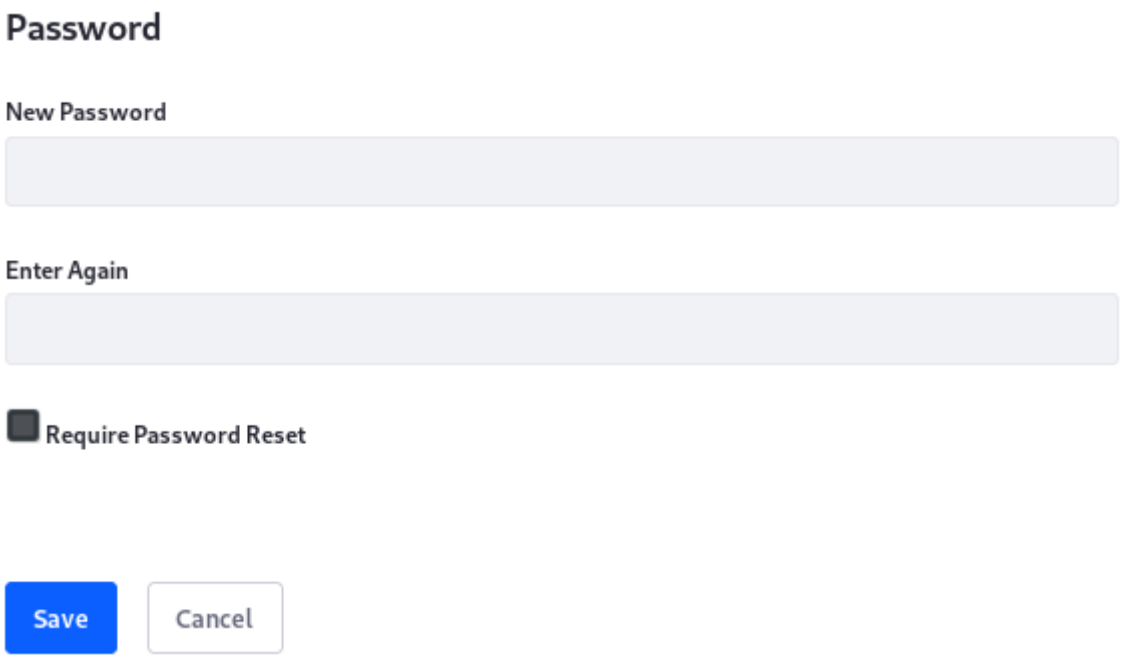

Figure 3: Enter the password twice to manually set the password for a user. If the Password Policy you're using is configured to allow it, select whether to require the user to reset their password the first time they sign in to the portal.

Editing Users

If you click on *Users and Organizations* in the Control Panel, you'll see your own user's account in the list of Users, along with any others. To change something about a particular user, click the *Actions* button (⋮) next to that user.

Choosing *Edit* takes you back to the Edit User page where you can modify any aspect of the User account including the screen name, email address, first name, last name, Site and Organization memberships, Roles, etc.

Choosing *Permissions* allows you to define which Roles have permissions to edit the User.

Choosing *Manage Pages* allows you to configure the personal pages of a User.

Choosing *Impersonate User* opens another browser window that loads the site as if you were the User so you can test your User management on a User to make sure you're achieving the desired behavior, without having to repeatedly log out of your administrator account and into the User's account.

Choosing *Deactivate* deactivates the user's account. The User is still in your database along with all the rest of your Users, but the account is deactivated, so the User cannot sign in to the portal. You can toggle between active and inactive Users in the Users view. If all the Users are active, this filtering option doesn't appear.

Choosing *Erase Personal Data* deletes the User's personal data.

Choosing *Export Personal Data* lets you download the User's personal data.

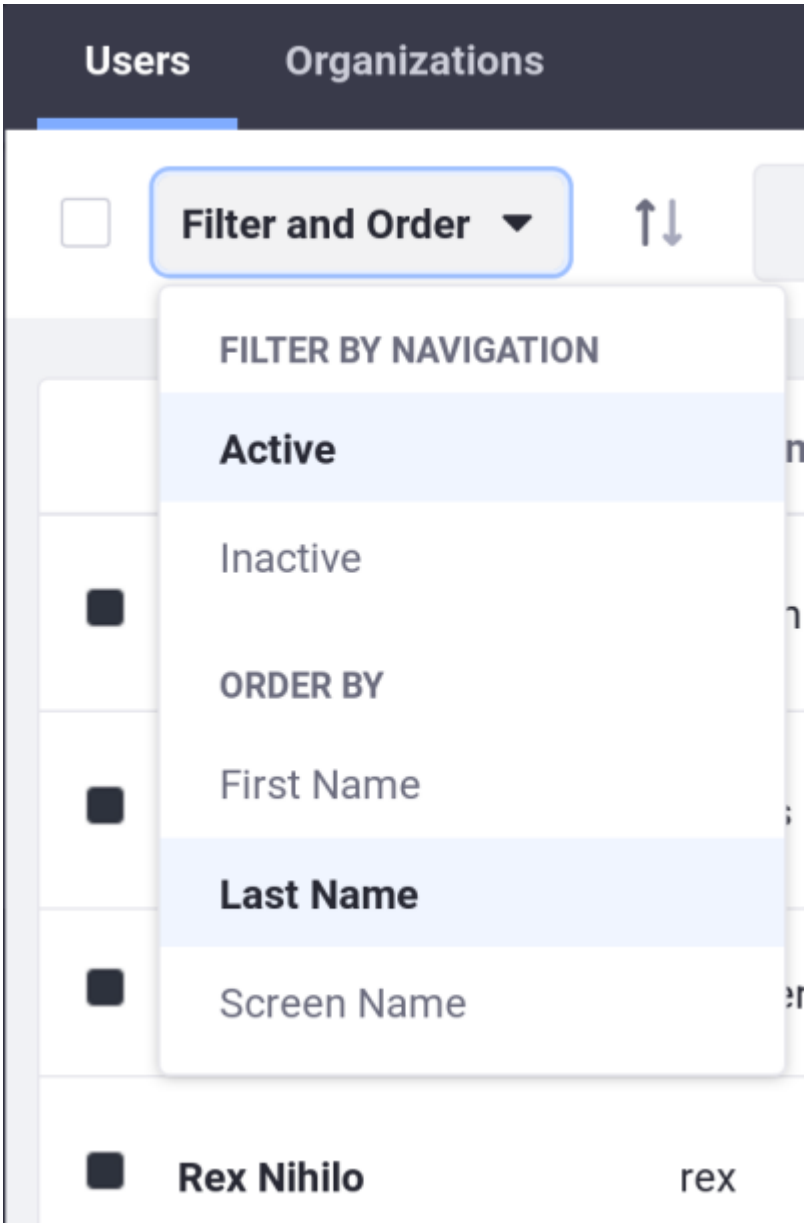

Figure 4: You can choose whether to view active or inactive (deactivated) portal users in the users list found at *Product Menu* → *Control Panel* → *Users* → *Users and Organizations*.

Most Users can't perform any of the above actions. In fact, most Users won't have access to the Control Panel at all. You can perform all of the above functions because you have administrative access.

Deleting Users

You must be careful when deleting Users. To guard against accidental deletion of Users, a two-step process must be followed: deactivate first, then delete.

1. Find the User to delete in the Users tab of *Control Panel → Users → Users and Organizations*. If you have a lot of Users, save time by searching for the User.
2. Click the *Actions* menu for the User and select *Deactivate*. You're asked to confirm that you want to deactivate the User. Click *OK*.

   You'll see a success message and the User disappears, but isn't gone yet.

3. By default the Users table displays only Active users. Click on *Filter and order* in the top of the table and a dropdown menu appears. Click *Inactive*, and you can see the User you just deactivated.
4. Click the Actions menu again, and click *Delete* if you really mean to delete the User. Confirm that you want to delete the User, and now the User is gone. This time, it's for real.

Deactivated Users: Deactivating a User means the User can't log in to the portal. He/she has no more permissions in the Sites and pages of the portal than a guest, although the account still exists in the system.

Users are reactivated when an administrator finds them in the Users table (be sure you're filtering the table results by Deactivated users), clicks the Actions menu, and selects Activate. There's no confirmation window for activation: they're automatically restored to their former status once Activate is clicked.

Now you understand the basic principles of User administration. There are important additional topics in the next article that you should consider mandatory information for all portal administrators, so do continue reading.

User Management: Additional Topics

You've learned the basics on adding and editing Users, but there are additional important topics that go beyond the most basic tasks an administrator must perform. Read on to learn about these.

Password Resets

The Add User functionality includes a *Require Password Reset* checkbox at the bottom of the Password form. The default password policy does not even allow administrators to deselect this option. As the administrator, however, you can modify the default password policy so that this box becomes usable.

1. Navigate to *Password Policies* in Control Panel → Users.
2. Click on the *Default Password Policy*.
3. Deselect the *Change Required* switcher in the Password Changes section. Now you can decide whether users you add must reset their passwords.

See Password Policies for more information on editing the default policy or creating your own.

Adding an Administrative User

If you're setting things up for the first time, you're likely to be using the default administrator account, the account of one of those famous Liferay Administrators, *Test Test* or her cousin, *Joe Bloggs*. Because these are default accounts, hackers know about them, so it's better to set up your own administrator account. Add a user with your information, then give your user account the same administrative rights as the default administrator's account:

1. Click the *Roles* link in the left navigation pane (in the *Edit User* page's *General* tab). This page of the form shows the Roles to which your account is currently assigned. No Roles appear by default (the User role does not appear since it can't be removed).
2. Click *Select* under Regular Roles and assign the Administrator Role to your user account. A dialog box pops up with a list of all the regular (portal-scoped) Roles in the portal. Select the Administrator Role from the list (click *Choose*). The dialog box disappears and the Role is added to the list of

Roles associated with your account. You are now a portal administrator. Log out and then log back in with your own user account.

Power Users: Users are not assigned the Power User Role by default. The Power User Role grants more permissions than the User Role. If the User Role is sufficient for you, ignore the Power User Role. Alternatively, use it to provide a second level of User permissions and assign it to those Users. If there are certain custom permissions that you'd like all of your portal Users to have, you can grant these permissions to the User Role. You can also customize the default Roles a new User receives via *Default User Associations*. This is covered in the article on Instance Settings.

In production, you should always delete or disable the default administrator account to secure your portal.

Gender

To collect data on users' genders, enable the binary gender field in the *Add User* form or create a custom field that meets your needs.

Enable the binary field by including the following in `portal-ext.properties`:

```
`field.enable.com.liferay.portal.kernel.model.Contact.male=true`
```

User Profile Pictures

Users have profile pictures. Administrative Users can upload images in the Edit User form, and any User can update her own account information, including image, from her personal site (*My account → Account Settings*).

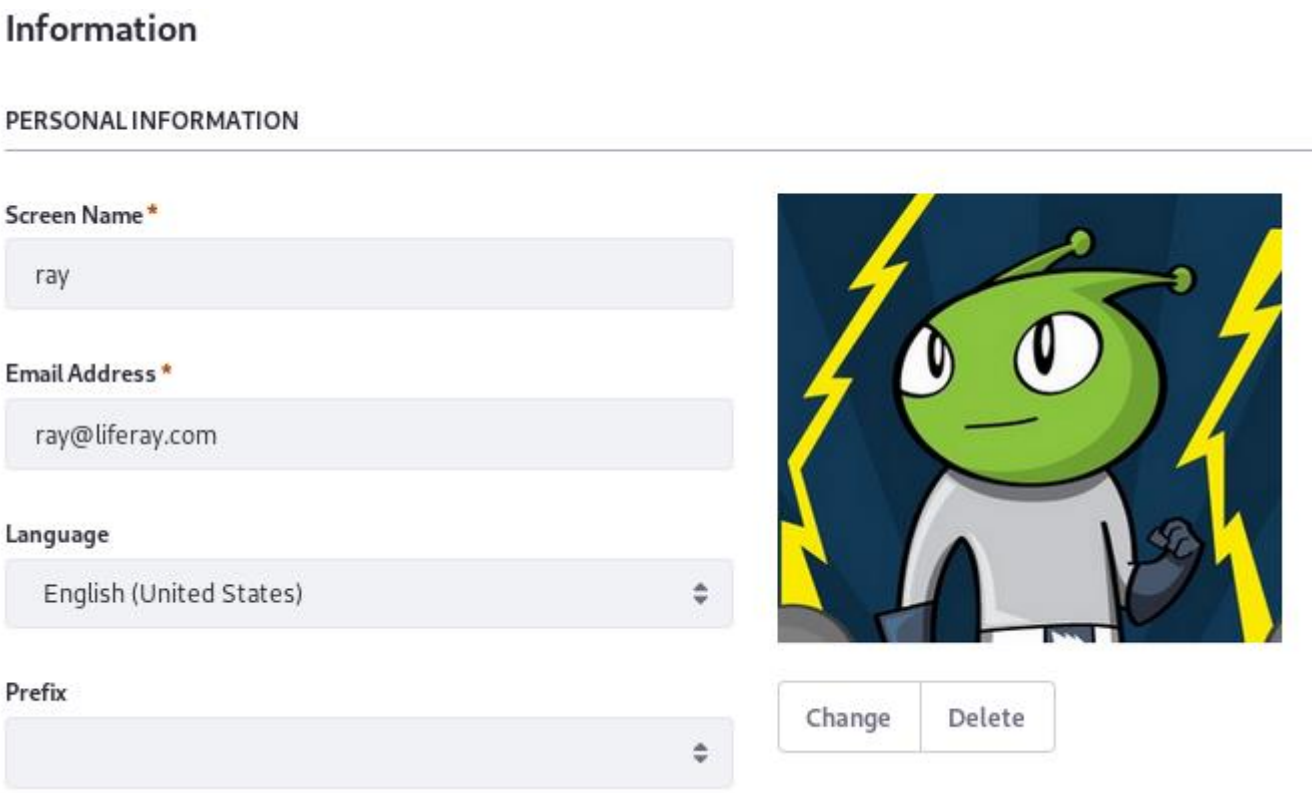

Figure 1: Upload images for user avatars in the Edit User form.

If no image is explicitly uploaded for a User's profile picture, a default User icon is assigned as the User avatar. By default the User's initials are displayed (First Name then Last Name) over a random color.

Figure 2: The default user profile picture is an icon with the user initials over a randomly colored bubble.

If the initials-based approach for generating User profile pictures isn't suitable for your portal, disable the inclusion of Users' initials in the default icons:

1. Navigate to *Control Panel* → *Configuration* → *System Settings*.
2. In the Platform section, click *Users* → *User Images*.
3. Deselect *Use Initials for Default User Portrait*.

Now, instead of the default icon, which is a colorful circle containing the user's initials, the icon is a gray circle containing the approximate shape of a human being.

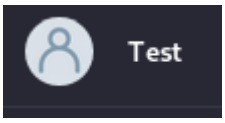

Figure 3: If you disable the default initials-based profile picture, this icon is used instead.

This is just the default. To override it with your own default image:

1. Create at least one image that is a 100x100 px square. Place it somewhere on the application server's classpath. For example, in Tomcat you could place it in the `tomcat/webapps/ROOT/WEB-INF/classes` folder.
2. Set the following property in a `portal-ext.properties` file:

```
image.default.user.portrait=image-filename-here.png
```

   This overrides the value of this portal property:

```
image.default.user.portrait=com/liferay/portal/dependencies/user_portrait.png
```

   NOTE: If you are using the binary field to collect information on users' genders (see above), then you'll have two default images to override. Set these properties instead:

```
image.default.user.female.portrait=image-filename.png
image.default.user.male.portrait=image-filename.png
```

4. Restart the application server.

Note: There's a way to adjust which initials are displayed and in what order, so you can make the default user icon (with the user initials) work for your locale. These settings are configured in a Language Settings module, so kidnap a friendly developer, give him a cup of coffee, and tell him the settings you want to change:

`lang.user.default.portrait=initials` sets the type of icon to use for avatars. The default value is *initials*. If set to initials, the next property configures which initials to display, and in what order. Alternatively, specify *image*, which gives you the same non-initials default image shown above.

`lang.user.initials.fields=first-name,last-name` determines which initials appear in the user portrait and in what order. The setting here only matters if `lang.user.default.portrait` is set to *initials*. Valid values are first name, middle name, last name, with first and last name as the defaults.

Numeric Screen Names

In prior versions, numeric user screen names were disabled out of the box via the default portal property

```
users.screen.name.allow.numeric=false
```

Other user management systems (LDAP, for example) did not have the same restriction, which made importing users more difficult. Administrators first had to set the above property to `true` before importing and hope that no screen names conflicted with site IDs. In Liferay DXP 7.2, this property defaults to `true` and there's no danger of numeric screen names conflicting with site IDs:

```
users.screen.name.allow.numeric=true
```

This means you're free to set a user screen name to *24601*, or whatever other number you can think of, and imports from systems that allow numeric screen names go more smoothly. That's everything you need to know to take advantage of this feature. Keep reading to understand what enabled the change.

Because users have personal sites, the URL to user *24601*'s personal site is

```
http://localhost:8080/web/24601
```

Meanwhile, a default site URL to cleverly named *Test Site* is

```
http://localhost:8080/web/test-site
```

There's no conflict here, but two conditions could easily lead to one:

1. *Test Site*'s group ID matches the number chosen for the user's screen name. Each site has a unique numeric identifier in the database, called group ID. There's nothing stopping it from matching the user's numeric screen name, so it could easily be `24601` just like the hypothetical user above.
2. A site administrator comes along and changes the site's friendly URL to match its `groupId`. Hello, URL conflict! Now the site's URL matches the user's URL:

```
3. http://localhost:8080/web/24601
```

This conflict is no longer possible. In Liferay DXP 7.2, a site's friendly URL is not allowed to be numeric. See for yourself:

1. Navigate to the site's *Configuration* → *Site Settings* → *Site URL* section.
2. In the Friendly URL section, enter *24601* and save the form. A failure message appears if you don't have a user with the matching screen name:

```
3. The friendly URL may conflict with another page.
```

   You'll see this failure message if there's an existing conflict with a user screen name:

```
Please enter a unique friendly URL. Site [user-first-name user-last-name] has the same friendly URL.
```

Next, learn about collecting users in organizations.

Managing Organizations

If you're not entirely sure what Organizations are or whether you need them, start here. This article gets right to the practical stuff: how to manage Organizations.

Adding Organizations

Add an Organization (perhaps start by adding the *Physical Plant Department* organization to the Lunar Resort):

1. Click *Users and Organizations* from Control Panel → Users.
2. Go to the *Organizations* tab and click the *Add* button. Fill out the Name field at a minimum.
3. If you're creating a child Organization, use the Parent Organization *Select* button to select an Organization in the system to be the direct parent. Click the *Remove* button to remove the currently configured parent.
4. Click *Save* when finished filling out the Add Organization form.

As when creating a new user, once you submit the form a success message appears and you have access to a new form which lets you enter additional information about the Organization. Organizations can have associated multiple email addresses, postal addresses, web sites, and phone numbers. The Services link can be used to indicate the operating hours of the Organization, if any.

Tip: After creating an Organization, assign the desired user to the Organization Owner Role. The Organization Owner can do everything that an organization Administrator can. In addition to their full administrative rights within the Organization, they can do these things:

- Appoint other Users to be Organization Administrators
- Appoint other Users to be Organization Owners
- Remove the memberships of other Organization Administrators or Owners

Organization Administrators can't make these Role assignments and can't manage the memberships of other Organization Administrators or Owners.

Editing Organizations

To edit an Organization, go to the Users and Organizations section of the Control Panel and click the *Organizations* tab. All active Organizations are listed. Click the *Actions* button next to an Organization. This shows a list of actions you can perform on this Organization.

- *Edit* lets you specify details about the Organization, including addresses, phone numbers, and email addresses. You can also create a Site for the Organization.
- *Manage Site* lets you create and manage the public and private pages of the Organization's Site. This only appears after a Site has been created for the Organization.
- *Assign Organization Roles* lets you assign Organization-scoped Roles to Users. By default, Organizations are created with three Roles: Organization Administrator, Organization User and Organization Owner. You can assign one or more of these Roles to Users in the Organization. All members of the Organization automatically get the Organization User Role so this Role is hidden when you click Assign Organization Roles.
- *Assign Users* lets you search and select Users to be assigned to this Organization as members.
- *Add User* adds a new User and assigns the User as a member of this Organization.
- *Add Organization* lets you add a child Organization to this Organization. This is how you create hierarchies of Organizations with parent-child relationships.
- *Delete* removes this Organization. Make sure the Organization has no Users in it first. You'll be prompted for confirmation that you want to delete the

Organization. If there are Users in the Organization or if there are sub-Organizations, you must remove the Users and delete the sub-Organizations before deleting the parent Organization.

If you click the Organization name you can view both a list of Users who are members of this Organization and a list of all the sub-Organizations of this Organization.

Organization Types

By default, Liferay DXP only includes the *Organization* type. Configure the existing type or add additional types using the aptly named Organization Type entry in System Settings. There are two main reasons to configure Organization types:

1. Organizations usually correlate to real-life hierarchical structures. Calling them by their real names is helpful for administrators and Users. In the Major League Baseball (MLB) example, *League*, *Division*, and *Team* Organization types are useful.
2. Enforce control over which Organizations can be top level Organizations and the type of sub-Organization allowed for each parent Organization type. For example, MLB would not allow Division Organization types to be sub-Organizations of Team Organizations.

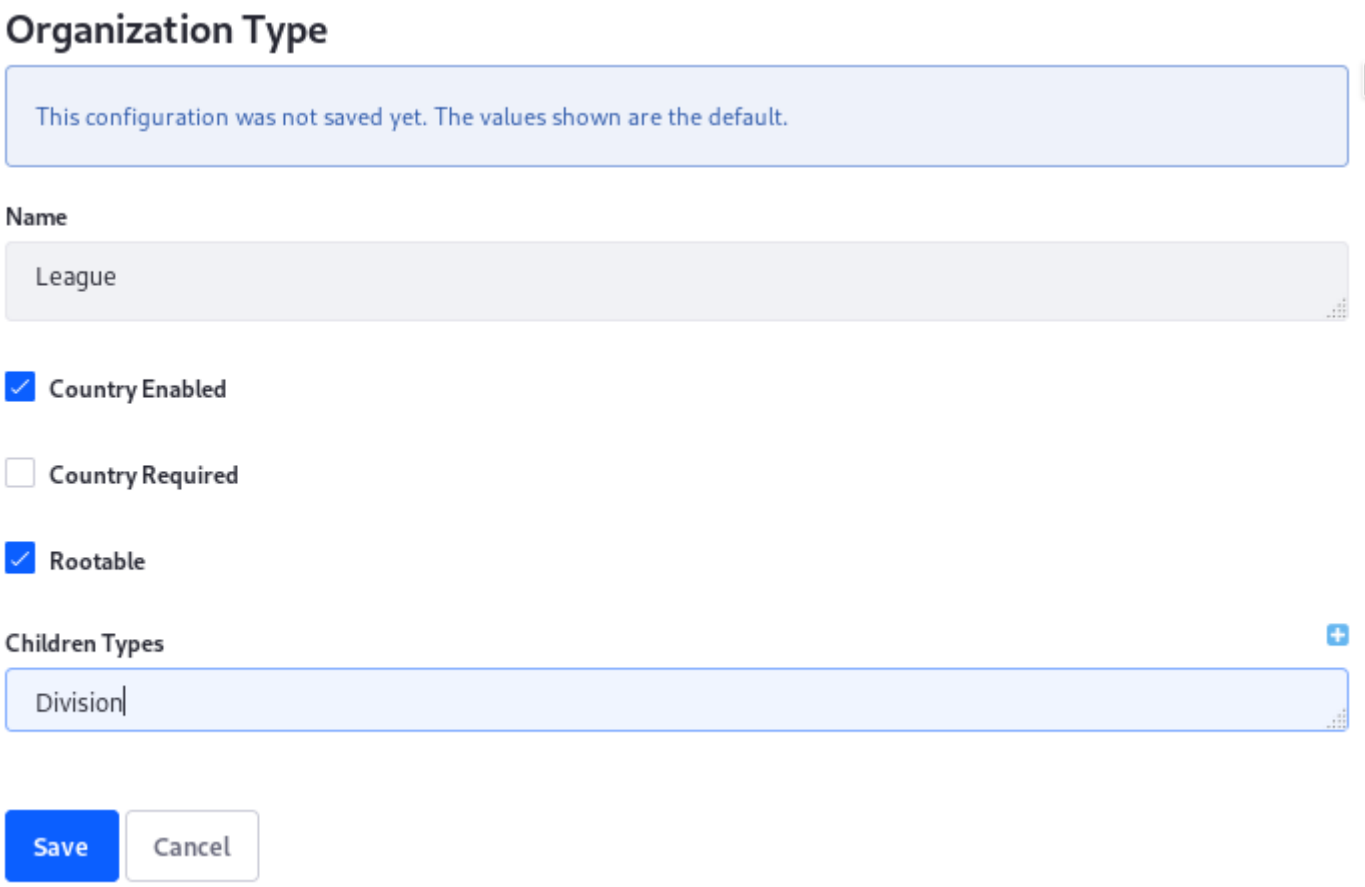

Figure 1: Create new organization types through the System Settings entry called Organization Types.

Check out the configuration options that configure the default *Organization* type and then configure an additional type.

To add another Organization type called *League*, enter these options into the configuration form:

Name: *League*

> Adds League to the list of Organization types that appear in the Add Organization menu.

Country Enabled: *True*

> Enables the Country selection list field on the form for adding and editing League types.

Country Required: *False*

Specifies that the *Country* field is not required when adding a League.

Rootable: *True*

Enables Leagues as a top level Organization. Limit League to sub-Organization status by excluding this property.

Children Types: *Division*

Specifies Division as the only allowable sub-Organization type for the League parent type.

Once you configure additional Organization types and click Save, you'll find your new type(s) available for selection in the Add Organization form.

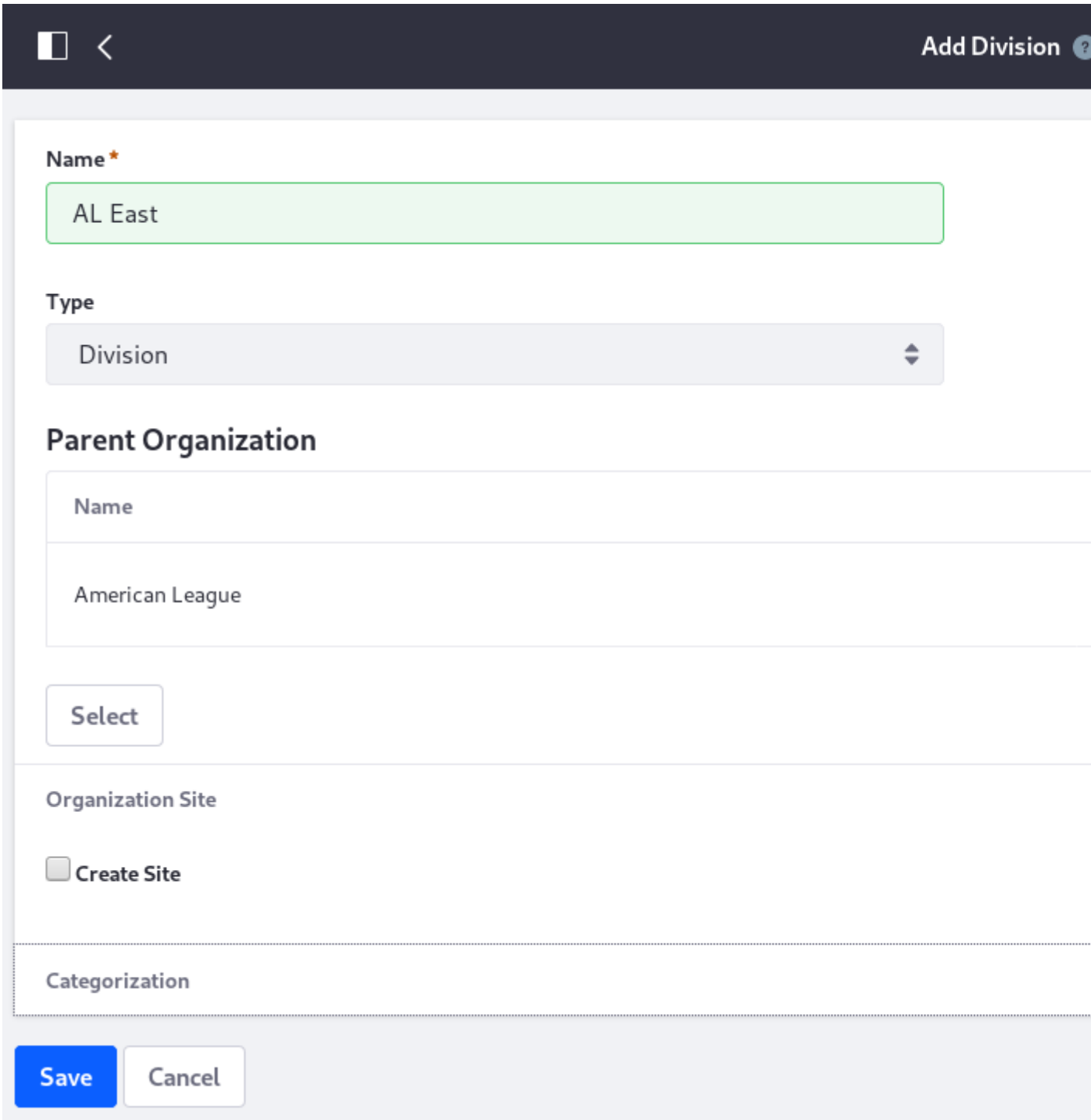

Figure 2: Custom configuration types are available in the Add Organization form.

Users can join or be assigned to Sites when they share a common interest. Users can be assigned to Organizations when they fit into a hierarchical structure. User groups provide a more ad hoc way to group users than sites and Organizations. You'll look at them next.

Roles and Permissions

If a *Role* were to win a Grammy or an Oscar or some other ego-feeding popularity contest, it better remember to thank all its *permissions* groupies during the acceptance speech, because they're the ones doing the real work. The Role is just the pretty face, so to speak.

Roles collect permissions that define a particular function, according to a particular scope. Roles collect permissions, and Users are assigned to Roles.

Note: Roles are assigned to Users, but it's tedious to assign each User to a Role intended for lots of Users. Recall that Users are grouped in Sites, Organizations, and User Groups. Implicitly assign regular scoped permissions to Users by assigning a Role directly to one of these User groupings.

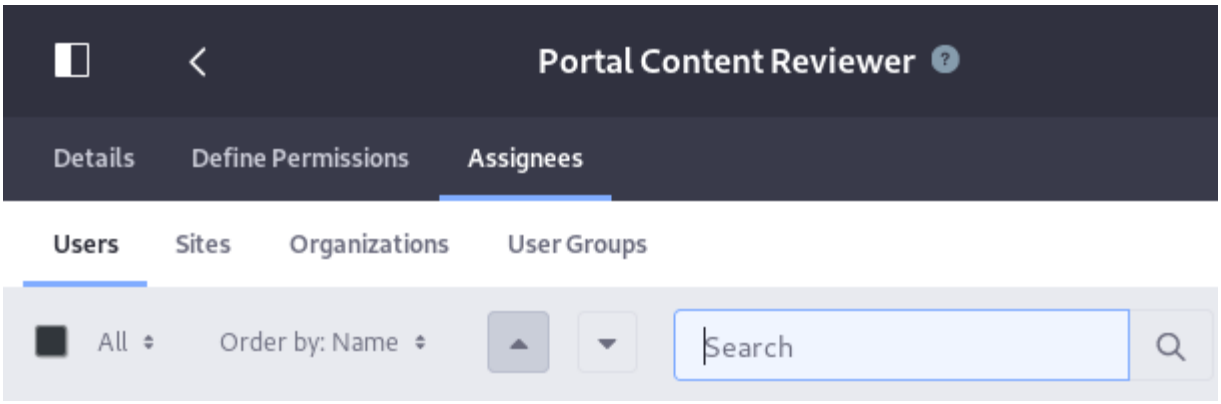

Figure 1: Assign Users to a role, directly or by their association with a Site, Organization, or User Group.

Take a Message Board Administrator Role, for example. A Role with that name should have permissions relevant to the specific Message Board portlets delegated to it. Users with this Role inherit the permissions collected underneath the umbrella of the Role.

In addition to regular Roles, Site Roles, and Organization Roles, there are also Teams. Teams can be created by site administrators within a specific Site. The permissions granted to a Team are defined and applied only within the Team's site. The permissions defined by regular, Site, and Organization Roles, by contrast, are defined at the global level, although they are applied to different scopes.

Regular role

Permissions are defined at the global level and are applied at the global scope.

Site role

Permissions are defined at the global level and are applied to one specific Site.

Organization role

Permissions are defined at the global level and are applied to one specific Organization.

Team

Permissions are defined within a specific Site and are assigned within that specific Site.

Note: Some permissions cannot be handled from the control panel. Asset-level permissions (for instance, permission to edit an individual blog post, or view a folder in the Documents and Media library) are managed from the individual asset. See Widget Permissions for details.

Deleting Asset Containers

A Web Content Folder contains Web Content articles. The Web Content Folder is an asset container, and the Web Content Article is an asset. It's possible to give a Role permission to delete an asset container without giving the Role permission to delete individual assets. In that case, beware: if a Role assignee deletes an asset container with individual assets in it, the individual assets themselves are deleted as well.

Besides Web Content Folders, examples of asset containers include Bookmarks Folders, Message Boards Categories, Wiki Nodes, and Documents and Media Folders.

You might not need to create a Role for a certain functionality. Liferay provides many pre-configured Roles for your convenience.

Default Liferay Roles

In the Roles Application appears a list of all the Roles in Liferay, by scope.

These are some of the pre-configured regular Roles:

- Guest: The Guest role is assigned to unauthenticated users and grants the lowest-level permissions.
- User: The User role is assigned to authenticated Users and grants basic permissions (mostly *Add to Page* permissions for their own Sites).
- Power User: The Power User Role grants more permissions than the User Role. It's an extension point for distinguishing regular Users from more privileged Users. For example, you can set things up so that only Power Users have personal sites.
- Administrator: The administrator Role grants permission manage the entire portal, including global portal settings and individual Sites, Organizations, and Users.

These are some of the pre-configured site roles:

- Site Member: The Site Member Role grants basic privileges within a Site, such as permission to visit the Site's private pages.
- Site Administrator: The Site Administrator Role grants permission to manage *almost* all aspects of a Site including site content, site memberships, and site settings. Site Administrators cannot delete the membership of or remove roles from other Site Administrators or Site Owners. They also *cannot* assign other Users as Site Administrators or Site Owners.
- Site Owner: The Site Owner Role is the same as the Site Administrator Role except that it grants permission to manage *all* aspects of a Site, including permission to delete the membership of or remove Roles from Site Administrators or other Site Owners. They *can* assign other users as Site Administrators or Site Owners.

These are some of the pre-configured organization roles:

- Organization User: The Organization User role grants basic privileges within an Organization. If the Organization has an attached Site, the Organization User Role implicitly grants the Site member Role within the attached Site.
- Organization Administrator: The Organization Administrator Role grants permission to manage *almost* all aspects of an Organization including the Organization's Users and the Organization's Site (if it exists). Organization Administrators cannot delete the membership of or remove Roles from other Organization Administrators or Organization Owners. They also *cannot* assign other Users as Organization Administrators or Organization Owners.
- Organization Owner: The Organization Owner Role is the same as the Organization Administrator Role except that it grants permission to manage *all* aspects of an Organization, including permission to delete the membership of or remove Roles from Organization Administrators or other Organization Owners. They *can* assign other Users as Organization Administrators or Organization Owners.

Tip: It's easy to overlook the differences between owner type roles and administrator type roles for Sites and Organizations. Site and Organization administrators *cannot* remove the administrator or owner Role from any other

administrator or owner, and they *cannot* appoint other Users as site or organization administrators or owners.

In contrast, site and organization owners *can* do those things.

Roles, and the permissions granted with their assignment, are foundational components in Liferay. Understanding their uses and configuration enhances your ability to configure Liferay DXP to suit your organizational needs.

Managing Roles

You manage Roles and Permissions in the Control Panel (*Control Panel → Users → Roles*). There you'll find an application for creating Roles, granting them permissions, and assigning Users to them. Roles can be scoped by portal, Site, or Organization.

Defining a Role's permissions is a topic deserving its own article. Read here about defining a role's permissions.

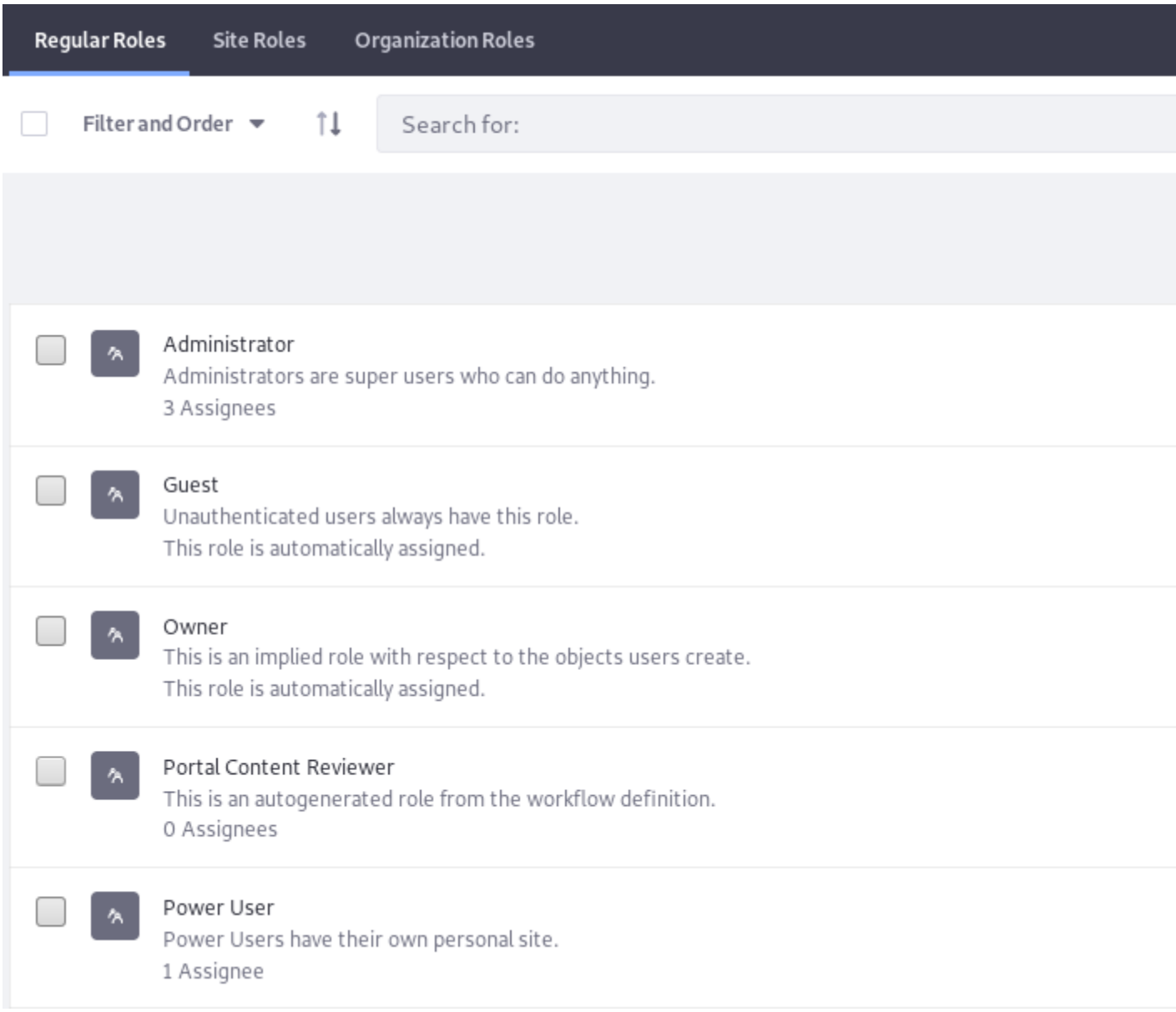

Figure 1: The Roles application lets you add and manage roles for the global (Regular), Site, or Organization scope.

Creating Roles

Determine the scope of the Role you must create. Roles can be scoped globally (Regular Roles), to a specific Site (Site Roles), or to an Organization (Organization Roles).

To create a Role:

1. Click the tab for the proper Role scope, then click the *Add* (+) button.
2. Enter a title and description. The title field is required but the description is optional.
3. Enter a Key, if desired. This required field provides a key that can be used to refer to the Role programmatically. It's auto-populated with the title text, but you can override it if desired.
4. Click *Save*.

Now the Role is present in the database and ready for further configuration.

Assigning Users to a Role

Assign users to a Role in the Assignees tab of the Add/Edit Role form. Roles are assigned to Users, Sites, Organizations, or User Groups. Here's how to assign the User Group Manager Role created in the last section to Users:

1. In the Assignees tab of the Add/Edit Role form, click the second level tab for *Users*.
2. Click the Add button (+).
3. Select the Users you want to add to the Role and click *Add*.

If assigning a group, note that all Users assigned to that group inherit the Role as well.

That's a good start, but your Role isn't worth the database row it occupies without defining permissions for the Role. Read the next article to learn how.

Defining Role Permissions

Roles collect permissions, so when Users are given a Role, they receive all the permissions defined by the Role.

If you create a Role with permission to access something in the Control Panel, keep in mind that the *View Control Panel Menu* permission is automatically granted.

Consider a Role called User Group Manager. Define the permissions for the User Group Manager Role so that assigned Users can add Users to or remove Users from any User Group:

1. Go to the Control Panel and then click on *Users* → *Roles*.
2. On the Regular Roles screen, click *Add* ().
3. After naming your Role, click *Save*.
4. Click on the *Define Permissions* tab.
5. Drill down in the menu on the left to *Control Panel* → *Users* → *User Groups*.
6. Under the *General Permissions* heading, flag *Access in Control Panel* and *View*. This lets user group managers access the User Groups Control Panel portlet and view existing User Groups.
7. Since you want User Group managers to be able to view User Groups and assign members to them, also check the *Assign Members* and *View* permissions under the *Resource Permissions* → *User Group* heading.
8. There's one last necessary permission you might not think of in association with this Role. In *Control Panel* → *Users* → *Users and Organizations*, User Group managers need *View* permission on the User resource. Grant this permission.
9. Click *Save*.

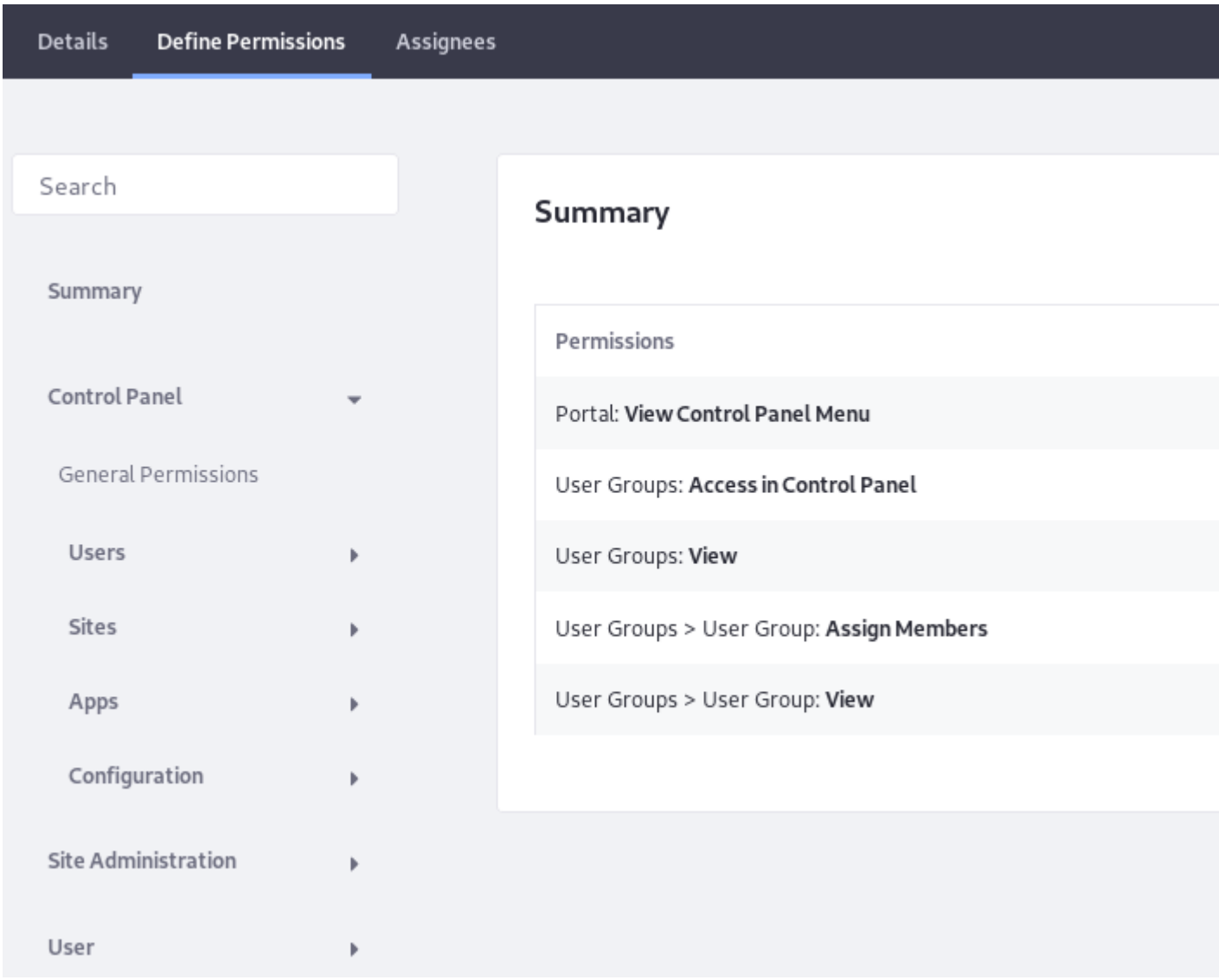

Figure 1: When defining permissions on a Role, the Summary view provides a list of permissions that have already been defined for the role. The area on the left side of the screen lets you drill down through various categories of permissions.

Now the User Group Manager Role has all the permissions necessary for adding Users to User Groups. After all, User Group managers can view User Groups, assign members, and access User Groups in the Control Panel. The permission to view Users in the Control Panel was necessary because you must view Users to assign them as members of a Role. Without this permission, User Group managers see an empty list if they try to add Users to a Role.

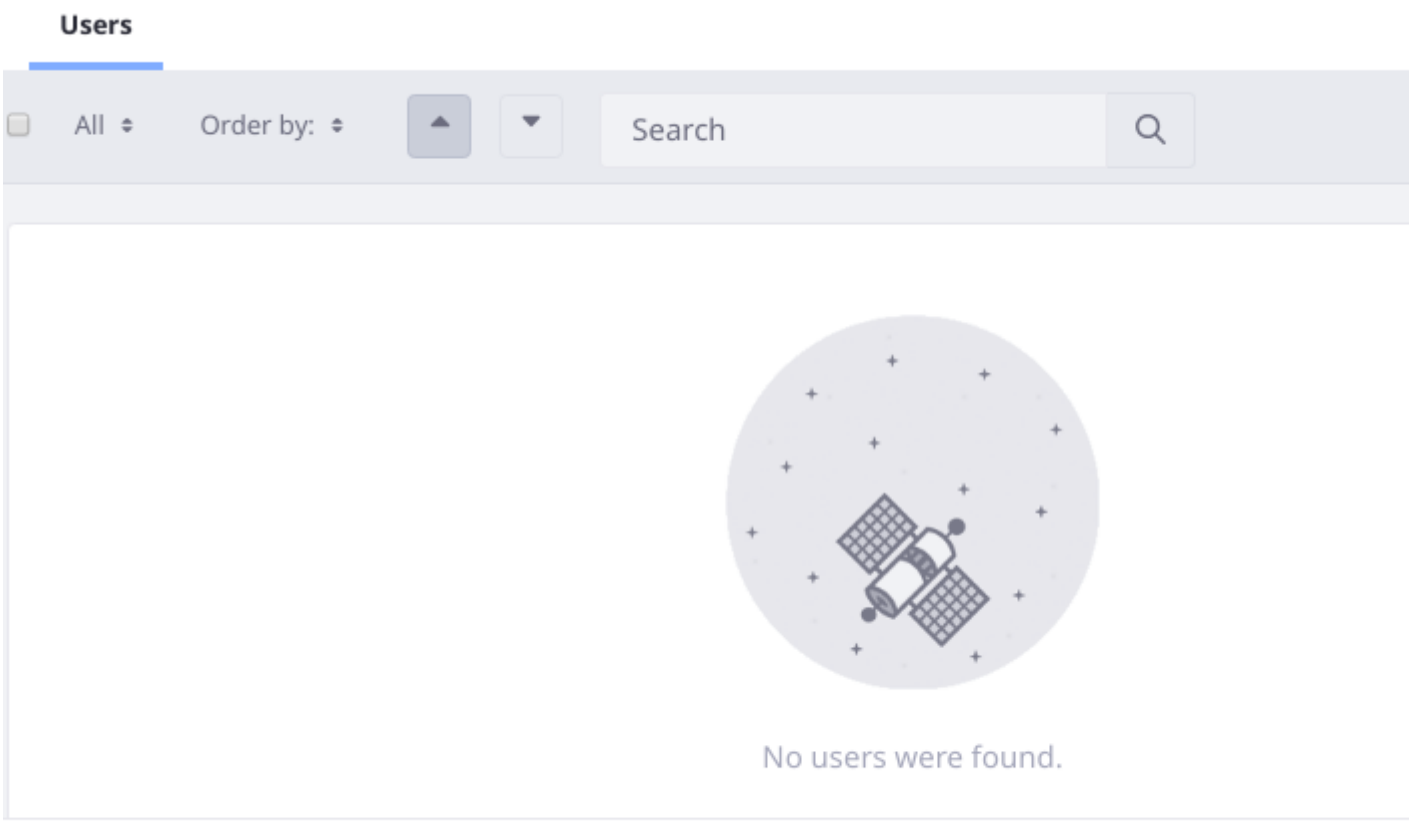

Figure 2: Users assigned to the User Group Manager Role can't find any users to add unless they have view permissions on the User resource.

Note: The Roles application in the Control Panel is not the only place where permissions are configured. You can configure a Role's permissions on a resource at a more granular level. For example, from a particular application instance, click its *Options* ( ) menu and select *Permissions*. There you can configure permissions for the resource that overlap with those configured in the Control Panel's Roles application. However, permissions granted or removed in the Control Panel override those made at the more granular level.

There are three categories of permissions: *Control Panel*, *Site Administration*, and *User*. By default, Users can manage their User accounts via the permissions belonging to the User category. Site Administrators can access the site administration tools belonging to the Site Administration category. Portal Administrators can access the entire Control Panel. For custom Roles, you can mix and match permissions from as many categories as you like.

The permissions in the Site Administration → Applications categories govern the content that can be created by portlets such as the Wiki and Message Boards. If you pick one of the portlets from this list, you see options for defining permissions on its content. For example, if you pick Message Boards, you see permissions for creating categories and threads or deleting and moving topics.

Site application permissions affect the application as a whole. Using the Message Boards as an example, an application permission might define who can add the Message Boards portlet to a page.

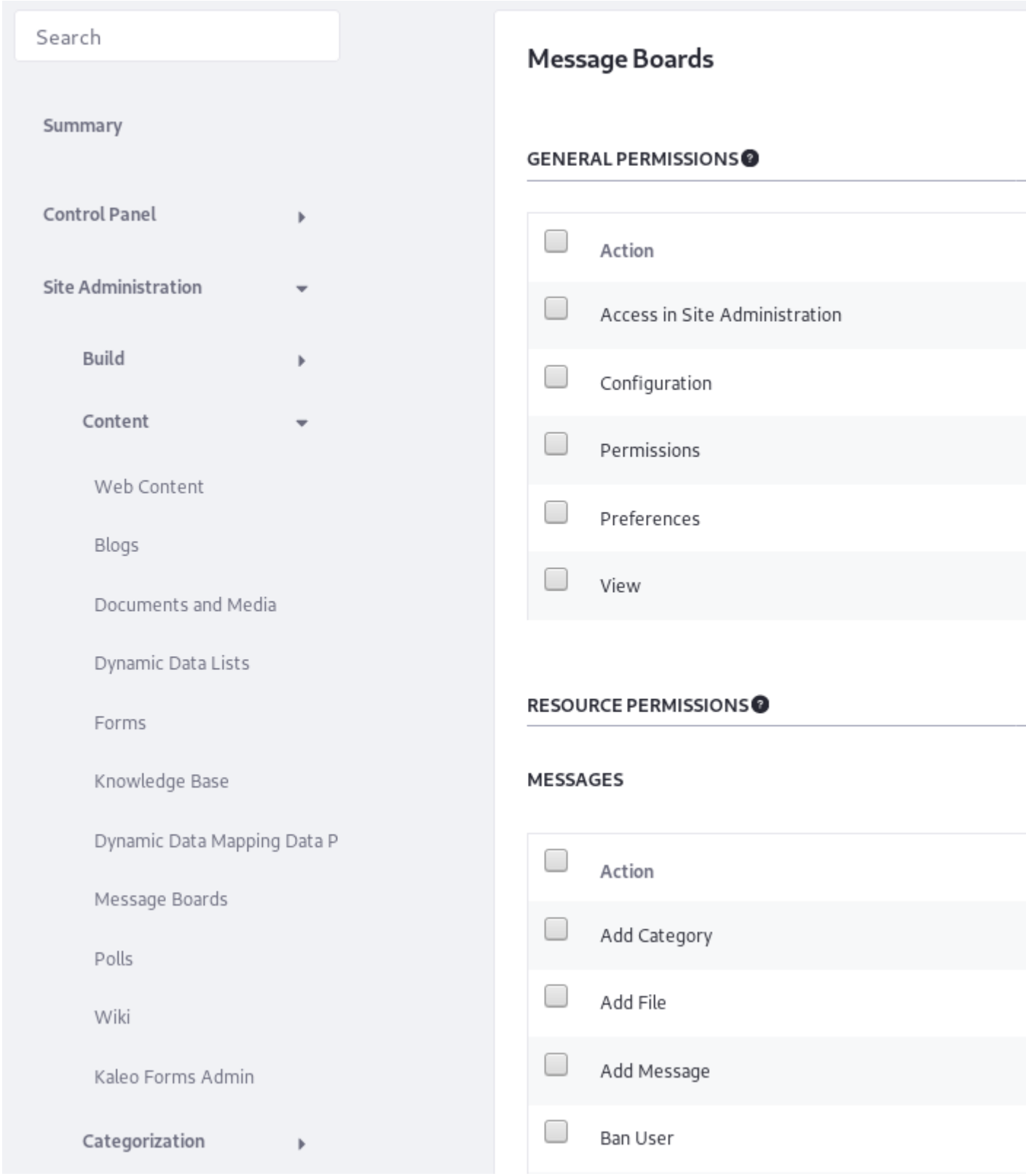

Figure 3: You can fine-tune which actions are defined for a role within a specific application like the Message Boards.

The Control Panel permissions affect how the Control Panel appears to the User in the Control Panel. The Control Panel appears differently for different Users, depending on their permissions. Some Control Panel portlets have a Configuration button, and you can define who gets to see that. You can also fine-tune who gets to see various applications in the Control Panel.

If you want to change the scope of a permission, click the *Change* link next to the gear icon next to the permission and then choose a new scope. After you click *Save*, you'll see a list of all permissions currently granted to the Role. From the Summary view, you can add more permissions or go back to the Role Application default view by clicking on the *Back* () icon.

Sometimes you might find that a certain permission grants more or less access than what you expected—always test your permissions configurations!

Delegating Social Activities Configuration

There's a permission that allows Site administrators to delegate responsibility for configuring social activities to other Users. To add this permission to a Role, click *Actions* next to the desired Role and select *Define Permissions*. Find the *Site Administration → Configuration → Social Activity* permissions category. Flag all of the permissions and then click *Save*:

- Access in Site Administration
- Configuration
- Permissions
- Preferences
- View

Once these permissions are granted, Role assignees can manage the site's Social Activities.

Roles allow portal administrators to define various permissions in whatever combinations they like. This gives you as much flexibility as possible to build the Site you have designed.