

Managing Permissions

jive

Contents

Managing Permissions	2
Starting with User Groups	2
System-Defined User Groups: Everyone and All Registered Users.....	3
Your User Groups.....	3
User Overrides.....	3
Permission Areas	3
Access Rules	4
Setting Permissions	4
Creating User Overrides	4
Managing Administrative Permissions	5
About Administrative Permission Levels.....	5
Setting Administrative Permissions.....	10
Managing Space Permissions	10
Space Permission Inheritance.....	10
Using and Customizing the Default Space.....	11
Setting Permissions for a Space.....	11
Managing Space Permission Levels.....	12
Managing Blog Permissions	15
About Global Blog Permission Levels.....	16
Setting Global Blog Permissions.....	16
Creating User Overrides.....	16
Managing Social Group Permissions	17
About Social Group Permission Levels.....	17
Setting Social Group Permissions.....	17
Creating User Overrides.....	18
Managing Home Page Permissions	18
About Home Page Permission Levels.....	18
Setting Home Page Permissions.....	19
Creating User Overrides.....	19
Managing Private Message Permissions	19
About Private Message Permission Levels.....	19
Setting Private Message Permissions.....	20
Creating User Overrides.....	20
Managing Mobile Permissions	20
About Mobile Permission Levels.....	20
Setting Mobile Permissions.....	21
Creating User Overrides.....	21

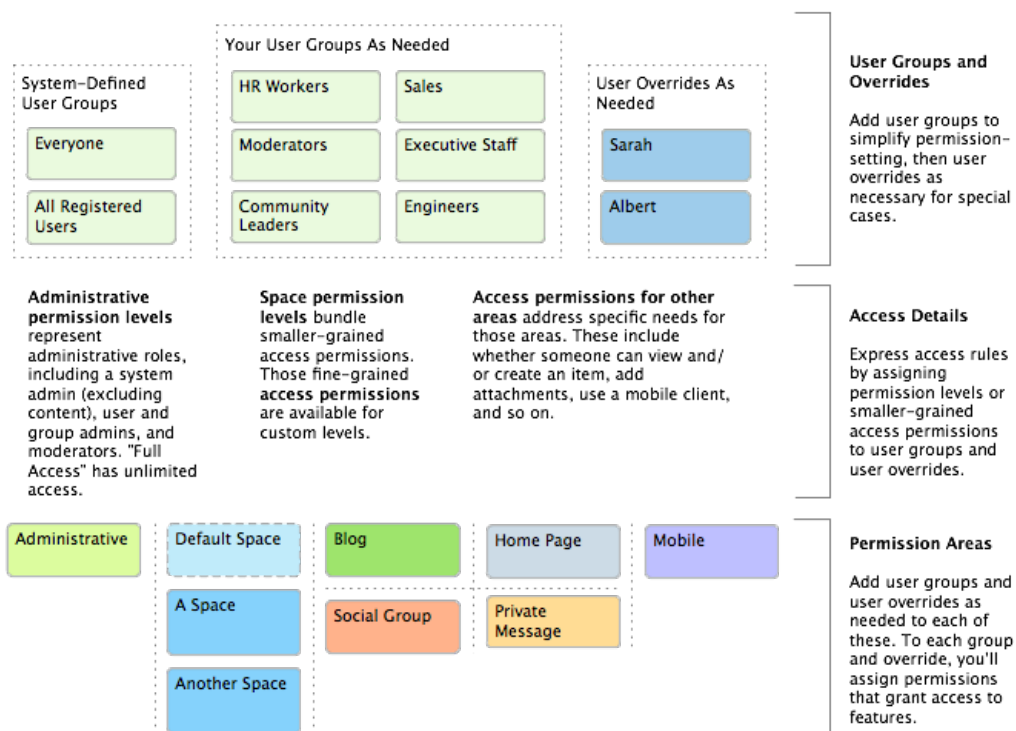
Managing Permissions

Use this guide to learn about granting permissions to people for access to content and administrative features.

When assigning permissions, you follow these basic steps:

1. Create user groups that capture how you want to grant access to the community's features. Each user group you create can represent a different category of people, from a permissions perspective. You might have user groups for administrators, managers, moderators, bloggers, people in the HR department, people in the Products department, and so on. You create user groups based on how you want to structure access to your community's features.
2. In each permissions area (administrative, space, social groups, and so on), add the user groups that should have some form of access to the area. For each group you add, assign permissions that capture that group's access. When you assign permissions, you're usually doing one of the following:
 - Assign a permission level. For administrative permissions and in spaces, you can use permission levels to assign bundled access permissions. You can also create your own space permission level.
 - Assign one or more access permissions. For blogs, social groups, and the rest, you work in a more a la carte way, assigning access by choose from a list of usually fine-grained options.
 - Create a user override for special cases. For example, you might want all but one or two people in a particular user group to have the permissions you assigned to the group. For those one or two, you can create a user override that assigns specific exceptions.

The following illustrates the basic pieces of the permissions model. You grant access to people by assigning to them the permissions offered by each of the permission areas.



Starting with User Groups

You'll ease the job of assigning and managing permissions by starting with a set of user groups that reflect the kinds of access you'll be granting. These groups can be defined in an external user identity system (such as an LDAP system) or in the application database.

The application includes two system-defined user groups: Everyone and All Registered Users. These are a good place to start when managing permissions that are in effect across the community. After you've figured out how permissions should be applied for these broad groups, you can start assigning permissions based to user groups you create.

System-Defined User Groups: Everyone and All Registered Users

The application includes two groups that are defined by the system: Everyone and All Registered Users. Consider whether these groups represent different levels of knowledge or trust about the people in them. You probably feel you have more knowledge or trust about someone who has registered to use the application than you do about someone who is using the application anonymously. These groups provide a convenient, built-in way to manage a people's access to application features.

- **Everyone** includes anyone who visits the site, including anonymous users. Think hard about what you want people to be able to do anonymously, but weigh that against the need to engage people to encourage them to participate. (Note that users who merely view content are not counted among the number of users your license provides for.)
- **All Registered Users** includes people who have entered registration information and logged in for access. Use this group when you want to ensure certain kinds of access go only to people who have an account on the system.

Your User Groups

Your user groups will reflect your community's organizational groups. They could be relatively few, with separate groups for those who manage, moderate, and administer the community. They could also be many, with groups representing departments of a company, people with specific privileges (such as blogging), virtual teams within the organization, and so on.

For more on creating and managing groups, see *Managing User Groups*.

User Overrides

For those cases, when there are exceptions to the rules you've defined, you can create user overrides. User overrides provide a user-by-user way to express those exceptions. You might be further limiting the user's access, but you could also be broadening it, such as to lend an administrative flavor to the user's access.

Permission Areas

Permission areas represent a mix of roles, places, and content types. They include:

- **Administrative** -- administrative and moderation permissions through which people have access to system-wide settings. Most of these provide access to the admin console. With the exception of the Full Access permission level, these don't provide access to content.
- **Space** -- per-space permissions for administering or moderating the space, as well as for working with content there.
- **Blog** -- permissions related to global blogs (such as system and personal blogs) to view and create blogs, comment on global blog posts, and so on.
- **Social group** -- permissions to view and create social groups, as well as work with attachments and images in content there.
- **Home page** -- permissions to create and interact with content that can appear on the communities home page, including announcements, polls, and videos there.
- **Private message** -- permissions to create, send and receive private messages, as well as to add attachments to messages.
- **Mobile** -- permission to access the community from a mobile device, such as an iPhone.

Keep in mind that there are a few wrinkles in the permissions model. For example, the "blogs" area applies only to global blogs, such as system blogs and personal blogs (neither of which belong, strictly speaking to a place). This leaves out blogs in spaces, social groups, and projects, whose permissions are managed in different ways as described in [Managing Blog Permissions](#) (page 15) .

Access Rules

Each permission area exposes its own set of permissions that are based on what you can do in the area. When you add user groups to an area, you assign access from among the permissions that the area offers.

For two of the areas -- administrative and space permissions -- the permissions are bundled into permission levels to make managing permissions for the area easier. In both of these areas, communities tend to set permissions along a similar set of themes. The permission levels are designed to reflect those themes.

Note: You can't break out the bundled permissions in the administrative area as you can with space permissions.

Setting Permissions

You can set home page permissions in the admin console on a permissions page.

1. On the page, under **Groups with access**, assign permissions to user groups:
 - To assign permissions to a user group not yet listed:
 - a. Click **Add group**.
 - b. Enter the name of the user group to add.
 - c. Click the **Select Permissions** button.
 - d. In the dialog box, select check boxes for the permission levels you want to apply for the user group.
 - To edit permissions for a user group already listed:
 - a. Locate the group in the list.
 - b. Next to its permission level, click **edit permissions**.
 - c. In the dialog box, select check boxes for the permission levels you want to apply for the user group.
2. Click the **Set Permissions** button.

Creating User Overrides

Create a user override to grant a particular set of permissions to an individual. You might need to create an override if:

- A person requires a particular set of permissions for an area, but isn't (and shouldn't be) a member of a group to which you've already assigned permissions for the area.
- A person is a member of a group to which you've assigned permissions for an area, but they require a different set of permissions than they've received as a member of the group -- in other words, they're an exception to the rule. For example, you might want to separately define their permissions in order to enhance or limit their access in the area.

Use the following steps to create a user override on the permissions page you're editing:

1. Under **User Overrides**, click **Create a user override**.
2. In the box, start typing the name of the user for whom you want to set the override. Click the popup that displays the user's name.
3. Click the **Set override** button to view the permissions you can set.
4. In the permissions box for the person you selected, select and clear check boxes as needed. In the end you want the list of checked items to reflect the permissions the person should have. Note that you merely clear a check box to remove a permission -- there's no need to explicitly revoke the permission.
5. Click **Set Permissions** to save the override you've created.

Managing Administrative Permissions

Administrative permissions give people the ability to keep the application running. Assign administrative permissions to delegate behind-the-scenes work. Through administrative permissions, people can:

- Make configuration changes to the system.
- Manage spaces.
- Manage user accounts and user groups.

In the UI: Admin Console: Permissions > System Administration

About Administrative Permission Levels

Administrative permission levels represent sets of permissions designed to support specific types of administrative work in the application.

Note: You can't create custom permission levels here, as you can for space permissions.

Permission	Description
Full Access	Gives control over every facet of the system. This level should only be assigned to users who are cleared to administer the system from a technical standpoint. It also gives access to view and administer all content in the system. Full access supercedes all other permissions at the space level and beyond. In other words, with full access, a person can do anything in the application whether or not they're explicitly granted permission to do it.
Manage System	Similar to Full Access, the Manage System permission level grants control over all technical aspects of the admin console. However, unlike Full Access, it does not automatically grant access to all community content. If your system has content in spaces that should be kept confidential, grant this permission to technical administrators instead of Full Access.
Moderate Content	Provides the ability to moderate social group content as well as perform global moderation duties across all spaces. Does not provide admin console access. When this level is granted to a group, all moderated content will pass through their queue before it appears in the community. For more about moderation, see <i>Moderating Content</i> .
Manage Users	Grants access to manage the users of this application. For more on managing users, see <i>Managing User Accounts and User Groups</i> .
Manage Groups	Grants access to create and manage user groups, such as for assigning permissions. For more on groups, see <i>Managing User Accounts and User Groups</i> .

Access to the Admin Console

Administrative permission levels determine access to the admin console. For example, a person who has been assigned the "Manage Users" level wouldn't typically need access to system-related areas of the console other than those for managing user accounts.

The following tables list each page of the console, showing whether someone assigned a particular level will have access to the page.

Dashboard Section

Console Page	Full Access	Manage System	Manage Space*	Manage Users	Manage All User Groups	Manage Particular User Groups**
Dashboard	Yes	Yes	Yes	Yes	Yes	Yes

System Section

Console Page	Full Access	Manage System	Manage Space*	Manage Users	Manage All User Groups	Manage Particular User Groups**
<i>Management</i>	'	'	'	'	'	'
System Information	Yes	Yes	No	No	No	No
License Information	Yes	Yes	No	No	No	No
System Properties	Yes	Yes	No	No	No	No
Locale	Yes	Yes	No	No	No	No
Log Viewer	Yes	Yes	No	No	No	No
Audit Log Viewer	Yes	Yes	No	No	No	No
Query Stats	Yes	Yes	No	No	No	No
<i>Settings</i>	'	'	'	'	'	'
Attachments	Yes	Yes	No	No	No	No
Bridges	Yes	Yes	No	No	No	No
Images	Yes	Yes	No	No	No	No
Caches	Yes	Yes	No	No	No	No
Space	Yes	Yes	No	No	No	No
Discussions	Yes	Yes	No	No	No	No
Documents	Yes	Yes	No	No	No	No
Email Server	Yes	Yes	No	No	No	No
Message Templates	Yes	Yes	No	No	No	No
Mobile	Yes	Yes	No	No	No	No
Feeds	Yes	Yes	No	No	No	No
OpenSearch Engines	Yes	Yes	No	No	No	No
Phrase Substitutions	Yes	Yes	No	No	No	No
Polls	Yes	Yes	No	No	No	No
Private Messages	Yes	Yes	No	No	No	No
Projects	Yes	Yes	No	No	No	No
Search	Yes	Yes	No	No	No	No
Spell Check	Yes	Yes	No	No	No	No
Storage Provider	Yes	Yes	No	No	No	No
Themes	Yes	Yes	No	No	No	No

Console Page	Full Access	Manage System	Manage Space*	Manage Users	Manage All User Groups	Manage Particular User Groups**
Web Services	Yes	Yes	No	No	No	No
Widgets	Yes	Yes	No	No	No	No
Video	Yes	Yes	No	No	No	No
Resource Caching	Yes	Yes	No	No	No	No
<i>Plugins</i>	'	'	'	'	'	'
Installed Plugins	Yes	Yes	No	No	No	No
Add Plugin	Yes	Yes	No	No	No	No
<i>Real-Time</i>	'	'	'	'	'	'
Overview	Yes	Yes	No	No	No	No
Connection	Yes	Yes	No	No	No	No

Space Section

Console Page	Full Access	Manage System	Manage Space*	Manage Users	Manage All User Groups	Manage Particular User Groups**
<i>Management</i>	'	'	'	'	'	'
Summary	Yes	No	Yes	No	No	No
Document Management	Yes	No	Yes	No	No	No
Discussion Management	Yes	No	Yes	No	No	No
Categories Management	Yes	No	Yes	No	No	No
Merge Spaces	Yes	No	Yes	No	No	No
<i>Settings</i>	'	'	'	'	'	'
Space Settings	Yes	No	Yes	No	No	No
Discussion Settings	Yes	No	Yes	No	No	No
Document Settings	Yes	No	Yes	No	No	No
Moderation Settings	Yes	No	Yes	No	No	No
Abuse Settings	Yes	No	Yes	No	No	No
Community Everywhere	Yes	No	Yes	No	No	No
Thread Archive Settings	Yes	No	Yes	No	No	No
Extended Properties	Yes	No	Yes	No	No	No
Filters and Macros	Yes	No	Yes	No	No	No
Gateway Settings	Yes	No	No	No	No	No
Interceptors	Yes	No	No	No	No	No

Blogs Section

Console Page	Full Access	Manage System	Manage Space*	Manage Users	Manage All User Groups	Manage Particular User Groups**
<i>Management</i>	'	'	'	'	'	'
Personal Blogs	Yes	Yes	No	No	No	No
System Blogs	Yes	Yes	No	No	No	No
Comments	Yes	Yes	No	No	No	No
Trackbacks	Yes	Yes	No	No	No	No
Migrate	Yes	Yes	No	No	No	No
<i>Settings</i>	'	'	'	'	'	'
Blog Settings	Yes	Yes	No	No	No	No

People Section

Console Page	Full Access	Manage System	Manage Space*	Manage Users	Manage All User Groups	Manage Particular User Groups**
<i>Management</i>	'	'	'	'	'	'
User Search	Yes	Yes	No	Yes	Yes	Yes
Create User	Yes	Yes	No	Yes	No	No
Group Summary	Yes	Yes	No	No	Yes	Yes
Create Group	Yes	Yes	No	No	Yes	No
User Relationships	Yes	Yes	No	Yes	No	No
<i>Settings</i>	'	'	'	'	'	'
Avatar Settings	Yes	Yes	No	No	No	No
Ban Settings	Yes	Yes	No	No	No	No
Password Reset	Yes	Yes	No	No	No	No
Login Security	Yes	Yes	No	No	No	No
Profile and Homepage	Yes	Yes	No	Yes	No	No
Registration Settings	Yes	Yes	No	Yes	No	No
Status Level Settings	Yes	Yes	No	Yes	No	No
User Data Synchronization Settings	Yes	Yes	No	No	No	No
User Relationship Settings	Yes	Yes	No	Yes	No	No
Profile Image Moderation	Yes	Yes	No	No	No	No

Console Page	Full Access	Manage System	Manage Space*	Manage Users	Manage All User Groups	Manage Particular User Groups**
Delegated Authentication	Yes	Yes	No	No	No	No

Permissions Section

Console Page	Full Access	Manage System	Manage Space*	Manage Users	Manage All User Groups	Manage Particular User Groups**
System Administration	Yes	Yes	No	No	No	No
Space Permissions	Yes	Yes	Yes	No	No	No
Space Permission Levels	Yes	Yes	Yes	No	'	No
Blog Permissions	Yes	Yes	No	No	No	No
Home Page Permissions	Yes	Yes	No	No	No	No
Private Message Permissions	Yes	Yes	No	No	No	No
Mobile Module Permissions	Yes	Yes	No	No	No	No

Reporting Section

Console Page	Full Access	Manage System	Manage Space*	Manage Users	Manage All User Groups	Manage Particular User Groups**
<i>Dashboard</i>	'	'	'	'	'	'
<i>Reports</i>	'	'	'	'	'	'
Main	Yes	Yes	Yes	Yes	Yes	No
People	Yes	Yes	Yes	Yes	Yes	No
Discussions	Yes	Yes	Yes	Yes	Yes	No
Blogs	Yes	Yes	Yes	Yes	Yes	No
Documents	Yes	Yes	Yes	Yes	Yes	No
Tags	Yes	Yes	Yes	Yes	Yes	No
<i>Settings</i>	'	'	'	'	'	'
Analytics	Yes	Yes	No	No	No	No
Third-Party Integration	Yes	Yes	No	No	No	No

* Manage Space permission must be on the specific space for editing.

** Manage Group permission must be on the specific group for editing.

Setting Administrative Permissions

You can set administrative permissions on the System Administration Permissions page in the admin console.

In the UI: Admin Console: Permissions > System Administration

1. In the admin console, go to the **System Administration Permissions** page.
2. To assign permissions to a user group not yet listed:
 - a. Click **Add group**.
 - b. Enter the name of the user group to add.
 - c. Click the **Select Permissions** button.
 - d. In the **System Administration Permissions for <user_group>** dialog box, select check boxes for the permission levels you want to apply for the user group.
3. To edit permissions for a user group already listed:
 - a. Locate the group in the list.
 - b. Next to its permission level, click **edit permissions**.
 - c. In the **System Administration Permissions for <user_group>** dialog box, select check boxes for the permission levels you want to apply for the user group.
4. Click the **Set Permissions** button.

Managing Space Permissions

You assign space permissions to govern the kind of access the people have. Generally speaking, you assign permissions to user groups, then create exceptions as needed by overriding permissions for particular users.

Note: Before you go about assigning permissions, be sure you're familiar with permission levels and how to customize them. For more information, see [Managing Space Permission Levels](#) (page 12) .

At a high level, setting space permissions typically includes these steps:

1. Create user groups that capture how you want to grant access to the community's features.
2. Set default space permissions. These should represent the access you'll most commonly want to provide for new spaces in the community.
3. As you add spaces, decide how to handle setting permissions for each. When someone creates a space, their options typically are:
 - Inherit from the parent space.
 - Start with the parent space's permissions, then customize.
 - Start with the default space's permissions, then customize.
 - Start from scratch (no permissions assigned), then customize.

Note: Permissions in spaces are inherited by projects created inside them. Social groups, on the other hand, are independent of spaces and projects. For more, see [Managing Social Group Permissions](#) (page 17) .

Space Permission Inheritance

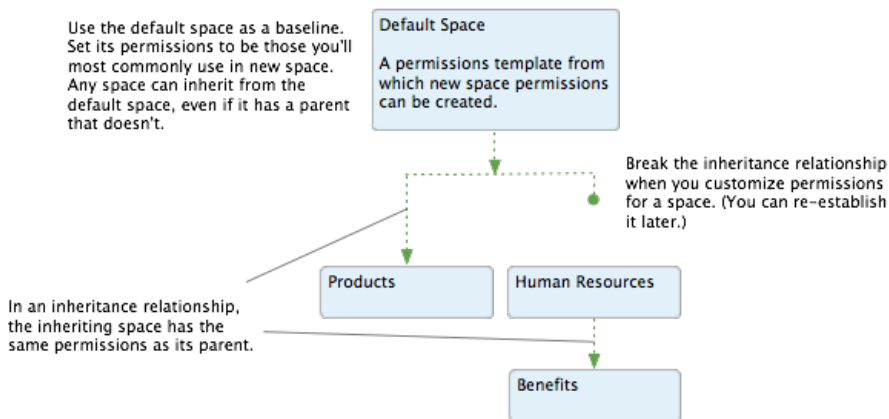
To make managing space permissions easier, an inheritance model provides a way to avoid (when you can) setting specific minute permissions for each new space. Spaces can inherit permissions from their parent or merely use those permissions as a starting point.

As you might expect, the inheritance relationship means that changes to the inherited space's permissions are automatically also changes to permissions in inheriting spaces. A *default space* is provided as starting place for new spaces regardless of where they are in the hierarchy. While not actually a space in other respects -- it can't contain content -- the default space is useful as a permissions template.

Note: The admin console will provide cues about inheritance for a particular space, such as by noting how many spaces inherit permissions from it.

Here are a few important inheritance characteristics to keep in mind when working with the permissions model:

- You can customize the default space permissions to represent a permission set that will be commonly used when creating new spaces. And new space can use these, if only as a starting point.
- A space can inherit its parent space's permissions, a relationship that must be broken before the sub-space's permissions can be customized. For spaces at the top level, the default space is the parent space.
- At any point after a space is created, you can re-establish an inheritance relationship between it and its parent space. When you do, you remove any customizations you've made to permissions in the sub-space (and, of course, in space's that inherit from the sub-space).
- A new space can begin with its parent space's permissions as a starting point only. When it does, those permissions aren't inherited, instead providing a basis for customization.
- A new space can begin with the default space's permissions as a starting point, regardless of where the new space is in the hierarchy.
- A new space can begin with no permissions set, a blank slate that you customize.



Using and Customizing the Default Space

The default space is designed to be a community-wide template for setting permissions in new spaces. It's a good idea to get to know how permissions in the default space are set up and to customize them if needed so that they're useful for creating new spaces in your community. When new spaces are created, they're permissions can be based on the default space's, if only as a starting point to customize.

Customizing Default Space Permissions

You can customize the default space, setting commonly-used permissions that will make sense for new spaces to have.

In the UI: Admin Console: Permissions > Space Permissions

1. In the admin console, on the **Space Permissions** page, click **Edit default space permissions**.
2. On the **Default Space Permissions** page, follow the steps described in **Setting Permissions for a Space**.

Setting Permissions for a Space

You set permissions for a space by adding a user group, then assigning a permission level to the group. Users in that group will have the permissions in the level you assigned. You can edit space permissions in the admin console.

In the UI: Admin Console: Permissions > Space Permissions

Before assigning permissions, be sure you're familiar with permission levels. For more information, see [Managing Space Permission Levels](#) (page 12) .

To set permissions for a space:

1. In the admin console, go to the **Space Permissions** page.
2. Under **View and edit a space's permissions**, type or browse for the name of the space you want to set permission for.
3. On the page describing permissions for the space, assign permissions to user groups:
 - To assign permissions to a group not yet listed:
 - a. Click **Add group**.
 - b. Enter the name of the group to add.
 - c. Select a permission level from the dropdown.
 - d. Click the **Add Group** button.
 - To edit permissions for a group already listed:
 - a. Locate the group in the list.
 - b. Next to its permission level, click **edit**.
 - c. Select a permission level from the dropdown.
 - d. Click **Save**.

Managing Space Permission Levels

Each permission level represents a collection of specific access, including specific permissions for content types and administrative roles. The application includes several permission levels by default, and you can create your own. When you assign permissions to groups for access to a space, you generally assign levels, then customize as needed with overrides for particular users.

When working with space permissions, you might be working with two kinds of levels: those you assign for access to the space as a whole and those you assign for access to particular kinds of content.

- **Space permission levels** capture access to space features at a high level, each bundling fine-grained access to content or administrative roles along a particular theme. The application comes with several predefined levels designed to reflect common roles, including a space administrator, a moderator, a person who can only view content, and so on. See the section on standard permission levels for more on included levels. You can also create your own levels.
- **Content permission levels** bundle fine-grained access to a particular content type. You use content permissions when creating your own permission level or overriding permissions for a certain user. For example, you might create a custom level in which people can create new discussion posts, but only comment on documents (rather than create them).

Note: Permissions in spaces are inherited by projects created inside them. Social groups, on the other hands, are independent of spaces and projects. For more, see [Managing Social Group Permissions](#) (page 17) .

Standard Permission Levels

The application includes several default space permission levels. Designed to meet common permissions needs, these are worth a look if you're starting from scratch (or even revising what you've got). As described below, you can also add your own levels.

Note: To see the list of space levels in the admin console, go to the **Space Permissions Levels** page, then click the **Standard Levels** tab.

The following table lists the default space permission levels, along with a summary of the access granted by each. See the table later in this section for details on specific permissions granted by each.

Levels Described

Space Permission Level	Access Granted
Administer	Design the space layout, read and write for all content types, assign permissions to users and user groups, delete the space.
Moderate	Read and write all content types, edit other people's content.
Create	Read and write all content types.

Space Permission Access Granted Level	
Contribute	Comment on commentable content types, as well as reply to discussion threads.
View	View content.
Discuss (External Only)	Read/write discussions, contribute on all other content types.
No Access	Only applicable when creating a user override. Use this to prevent access to the space and no entitlements are set.

The following table lists each default space permission level, along with the specific permissions granted by each. As described in the section below, when you create a permission level, you can choose from among these.

Access Granted for Each Level

Space Permission Level	View	Create	Reply	Comment	Attach file	Insert image	Rate	Vote	Create Project	Create Annotation	Full Control	Moderate
Administer	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Moderate	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
Create	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Contribute	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No	No
View	Yes	No	No	No	No	No	No	No	No	No	No	No
Discuss (external community)	Yes	Yes	Yes	Yes	No	No	Yes	Yes	No	No	No	No

Custom Permission Levels and User Overrides

When you create a custom permission level or a user override, you're in effect designing exceptions to existing rules. Those exceptions could replace permission levels included by default, permission levels you've created, or one-off overrides for particular users. For example, you might want to create a custom permission level for a group of people who should be the only ones to post to a space's blog. Or you might create a user override for a particular user who will be a space's administrator, managing its permissions, creating spaces beneath it, and so on.

When you create this kind of customization, your options are divided into three categories (described in detail below):

- **No access.** Available for a user override only, this option lets you simply exclude a particular user from access to the space. This is designed as a user-by-user approach. To prevent access for a group of people instead, ensure that those people aren't included in groups that *do* have access. For example, to restrict access to a space that contains sensitive information, create a user group that contains people who should have access, taking care to leave out those people who shouldn't have it.
- **Access space.** Available in custom permission levels and user overrides, this category provides fine-grained control with which you assign permissions specific to each content type. Want to create a permission level that grants access to create discussion threads but only view documents? This is what you want.
- **Manage space.** Available in custom permission levels and user overrides, this category provides a way to create administrative roles for the space. Each space should have an administrator, even if that role is inherited from a parent space. But typically, the roles available in this category will go to very few people.

The following sections give details on the options available for each of the categories.

No Access

The user has no access to the space and won't be able to see content from it. Pretty straightforward.

Access Space

Use this category to craft custom content-specific access in the space. When you select this category while customizing, you have access to a list of the content types, each with a list of the access levels available for it. Choose an access level for each content type.

The following table lists the access levels that each content type permission level includes, along with the specific permissions each allows.

Access Granted for Each Content Type Permission Level

Content Type Permission	View	Create	Reply	Comment	Attach file	Insert image	Rate	Vote
Create	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Create (for discussions)	Yes	Yes	Yes	Yes	No	No	Yes	Yes
Contribute	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
View	Yes	No	No	No	No	No	No	No
Advanced	See the specifics below.							

The **Advanced** access level for each content type provides even finer-grained control of permissions for a content type. After you select **Advanced**, select check boxes for the permissions you want the customization to allow.

The following table lists what's available in the **Advanced** level for each content type.

Access Settings Available for Each Content Type

Content Type	View	Create	Reply	Comment Reply	Attach file	Insert image	Rate	Vote
Document	Yes	Yes	No	Yes	Yes	Yes	Yes	No
Discussion	Yes	Yes	Yes	No	Yes	Yes	No	No
Blog Post	Yes	Yes	No	Yes	Yes	Yes	No	No
Poll	Yes	Yes	No	Yes	No	No	No	Yes
Video	Yes	Yes	No	Yes	No	No	Yes	No

The following are also available as "on or off" options.

Option	Access Granted
Create Project	Create a project in the space.
Create Announcement	Create an announcement in the space.

Manage Space

Use this category to assign administrative roles that are specific to the space. The following table describes the two access levels that are available.

Option	Access Granted
Full Control	Customize the space overview page, edit space details, edit all space content, create subspaces, manage permissions for that space, delete the space, create a category, and manage the space blog.
Moderate	Moderate and edit all content in the space. Selecting this option enables the moderation queue for all content in the space.

Creating a Custom Space Permission Level:

You can create a custom space permission level that you can subsequently use when assigning permissions space by space. You might want to do this, for example, if you think you're going to be using a custom set of permissions in more than one space. If you'll use the customization only once, you might instead want to create a customization that you don't save as a custom level for use in other spaces.

In the UI: Admin Console: Permissions > Space Permission Levels

To create a custom space permission level:

1. In the admin console, go to the **Space Permission Levels** page.
2. On the **Custom Levels** tab, click **Create new permission level**.
3. On the **Create a Custom Permission Level** dialog box, enter a name and description for the permission level. These will help other administrators know the new level's purpose.
4. Under **Access and administration**, select a category for the level, then choose from among the options in the category.
5. Click **Save**.

Managing Blog Permissions

This topic describes the permission settings for global blogs -- that is, blogs that aren't associated with a particular place, such as a space. These include system blogs (which tend to represent the community as a whole) and personal blogs (which represent a particular community member).

Managing permissions for other kinds of blogs varies depending on what kind of place the blog lives in. The following table gives a brief description of each:

Permissions Management for Non-Global Blogs

Blog Location	Permissions Management
Space	You manage permissions for blogs in a space when you manage permissions for the space. For more on space permissions, see Managing Space Permissions (page 10) .
Social group	Access for blogs in social groups are always completely open. That is, if the social group's creator chose to allow a blog for the group, then anyone who's a member of the group can do all of the things there that are allowable for blogs (viewing, posting, and so on). For more information on social group permissions, see Managing Social Group Permissions (page 17) .
Project	Blogs in projects inherit blog permissions from the place the project is in. In other words, a blog for a project in a space inherits blog permissions from the space. For more on space permissions, see Managing Space Permissions (page 10) .

Note: You configure settings and membership for global blogs by using the Blogs tab of the admin console. For more information, see *Administering Global Blogs*.

About Global Blog Permission Levels

Blog permission levels enable people to read and edit global blogs.

Note: You can't create custom permission levels here, as you can for space permissions.

Permission	Access Granted
View blog	View and read all public blog posts.
Create blog	Create/manage a personal blog, and author blog posts in it.
Comment	Leave comments on public blog posts.
Create attachment	Attach files to blog posts (Note: Requires the "Create Blog" permission to be effective).
Insert images	Insert images into blog posts (Note: Requires the "Create Blog" permission to be effective).

Setting Global Blog Permissions

You can set home page permissions in the admin console on the Blog Permissions page.

In the UI: Admin Console: Permissions > Blog Permissions

1. On the page, under **Groups with access**, assign permissions to user groups:
 - To assign permissions to a user group not yet listed:
 - a. Click **Add group**.
 - b. Enter the name of the user group to add.
 - c. Click the **Select Permissions** button.
 - d. In the dialog box, select check boxes for the permission levels you want to apply for the user group.
 - To edit permissions for a user group already listed:
 - a. Locate the group in the list.
 - b. Next to its permission level, click **edit permissions**.
 - c. In the dialog box, select check boxes for the permission levels you want to apply for the user group.
2. Click the **Set Permissions** button.

Creating User Overrides

Create a user override to grant a particular set of permissions to an individual. You might need to create an override if:

- A person requires a particular set of permissions for an area, but isn't (and shouldn't be) a member of a group to which you've already assigned permissions for the area.
- A person is a member of a group to which you've assigned permissions for an area, but they require a different set of permissions than they've received as a member of the group -- in other words, they're an exception to the rule. For example, you might want to separately define their permissions in order to enhance or limit their access in the area.

Use the following steps to create a user override on the permissions page you're editing:

1. Under **User Overrides**, click **Create a user override**.
2. In the box, start typing the name of the user for whom you want to set the override. Click the popup that displays the user's name.
3. Click the **Set override** button to view the permissions you can set.
4. In the permissions box for the person you selected, select and clear check boxes as needed. In the end you want the list of checked items to reflect the permissions the person should have. Note that you merely clear a check box to remove a permission -- there's no need to explicitly revoke the permission.

5. Click **Set Permissions** to save the override you've created.

Managing Social Group Permissions

As with spaces, social groups are places where people can create content such as documents, discussions, blog posts, and the like. Unlike spaces, social groups can't be arranged hierarchically, so there's no permission inheritance relationship among social groups. (An exception to this applies to projects created inside social groups, which inherit content type permission from the social group they're in.)

When you manage social group permissions, you're managing only the access through which people can view create groups, create attachments to content, and insert images. Content type permissions for social groups differ from those in spaces. A social group's manager grants permissions specific to content types by enabling those content types in their group. In other words, unlike content types in spaces, content types in social groups don't expose permission settings in the admin console. Content type permissions for spaces and social groups are independent of one another.

About Social Group Permission Levels

Social group permission levels are designed essentially as a way to manage whether people can see or create social groups. A person with access to create a social group can set the group's level of access and which content types are allowed in the group.

Permissions for each content type in a social group, however, are not configurable. They're essentially unlimited (read, create, comment, attach file, etc.). Projects created inside a social group inherit these permissions.

Note: Be sure to select "View social group" when granting access to create groups. Without that permission, people won't be able to see aspects of the UI through which they can create groups.

The following table lists the permission levels provided for social groups.

Permission	Access Granted
View social group	See the group feature in the UI and read all visible social groups. This is a general visibility option for groups. In other words, it must be selected in order for users to choose "Group" from the New menu in the end user UI.
Create group (public)	Create a new public or members only social group.
Create group (private)	Create a new private or secret social group.
Create attachment	Add an attachment to content in social groups.
Insert images	Add an image to content in social groups.

Setting Social Group Permissions

You can set social group permissions in the admin console on the Social Group Permissions page.

In the UI: Admin Console: Permissions > Social Group Permissions

1. On the page, under **Groups with access**, assign permissions to user groups:
 - To assign permissions to a user group not yet listed:
 - a. Click **Add group**.
 - b. Enter the name of the user group to add.
 - c. Click the **Select Permissions** button.
 - d. In the dialog box, select check boxes for the permission levels you want to apply for the user group.
 - To edit permissions for a user group already listed:
 - a. Locate the group in the list.
 - b. Next to its permission level, click **edit permissions**.

- c. In the dialog box, select check boxes for the permission levels you want to apply for the user group.
2. Click the **Set Permissions** button.

Creating User Overrides

Create a user override to grant a particular set of permissions to an individual. You might need to create an override if:

- A person requires a particular set of permissions for an area, but isn't (and shouldn't be) a member of a group to which you've already assigned permissions for the area.
- A person is a member of a group to which you've assigned permissions for an area, but they require a different set of permissions than they've received as a member of the group -- in other words, they're an exception to the rule. For example, you might want to separately define their permissions in order to enhance or limit their access in the area.

Use the following steps to create a user override on the permissions page you're editing:

1. Under **User Overrides**, click **Create a user override**.
2. In the box, start typing the name of the user for whom you want to set the override. Click the popup that displays the user's name.
3. Click the **Set override** button to view the permissions you can set.
4. In the permissions box for the person you selected, select and clear check boxes as needed. In the end you want the list of checked items to reflect the permissions the person should have. Note that you merely clear a check box to remove a permission -- there's no need to explicitly revoke the permission.
5. Click **Set Permissions** to save the override you've created.

Managing Home Page Permissions

The community's home page is typically seen by everyone at one time or another. Often it's the place people stop first to get a snapshot of what's going on. Because it's so central, it's a great place to put things that should be visible to everyone.

In other words, when setting permissions for the home page, keep in mind that you might want to offer some kinds of access to people who have an active role in the community as a whole, and some kinds more broadly. For example, a community manager could be given permission to create announcements. Other kinds of access, such as vote in polls or rating videos, might keep the community more active if they're more broadly granted.

See About Home Page Permission Levels for the list of levels you can grant.

About Home Page Permission Levels

Home page permission levels enable people to create and interact with content that's displayed on the community's main page.

Note: You can't create custom permission levels here, as you can for space permissions.

Permission	Access Granted
Create announcement	Create announcements that appear on the main (and personalized) homepage.
Create poll	Create polls at the system level.
Vote in polls	Vote in polls created at the system level.
Create video	Create and upload videos in their personal containers.
Rate videos	Rate the videos that appear in user's personal containers.
Comment on videos	Comment on the videos that appear in user's personal containers.

Setting Home Page Permissions

You can set home page permissions in the admin console on the Home Page Permissions page.

In the UI: Admin Console: Permissions > Home Page Permissions

1. On the page, under **Groups with access**, assign permissions to user groups:
 - To assign permissions to a user group not yet listed:
 - a. Click **Add group**.
 - b. Enter the name of the user group to add.
 - c. Click the **Select Permissions** button.
 - d. In the dialog box, select check boxes for the permission levels you want to apply for the user group.
 - To edit permissions for a user group already listed:
 - a. Locate the group in the list.
 - b. Next to its permission level, click **edit permissions**.
 - c. In the dialog box, select check boxes for the permission levels you want to apply for the user group.
2. Click the **Set Permissions** button.

Creating User Overrides

Create a user override to grant a particular set of permissions to an individual. You might need to create an override if:

- A person requires a particular set of permissions for an area, but isn't (and shouldn't be) a member of a group to which you've already assigned permissions for the area.
- A person is a member of a group to which you've assigned permissions for an area, but they require a different set of permissions than they've received as a member of the group -- in other words, they're an exception to the rule. For example, you might want to separately define their permissions in order to enhance or limit their access in the area.

Use the following steps to create a user override on the permissions page you're editing:

1. Under **User Overrides**, click **Create a user override**.
2. In the box, start typing the name of the user for whom you want to set the override. Click the popup that displays the user's name.
3. Click the **Set override** button to view the permissions you can set.
4. In the permissions box for the person you selected, select and clear check boxes as needed. In the end you want the list of checked items to reflect the permissions the person should have. Note that you merely clear a check box to remove a permission -- there's no need to explicitly revoke the permission.
5. Click **Set Permissions** to save the override you've created.

Managing Private Message Permissions

With private messaging, people can send each other messages that aren't visible to everyone else in the way that discussions are. A person receives and reads a private message through the Private Messages tab on their profile.

Note: You're setting permission to use the feature here. If you want to turn the private messaging feature on or off altogether, be sure to see *Configuring Private Message Options*

About Private Message Permission Levels

Private message permission levels merely grant access to the feature to users in the group you assign them to.

The following table lists the permission levels provided for private messaging.

Permission	Access Granted
Enable private messaging	Create, send, and receive private messages.
Create attachment	Attach files to private messages.

Setting Private Message Permissions

You can set home page permissions in the admin console on the Private Message Permissions page.

In the UI: Admin Console: Permissions > Private Message Permissions

- On the page, under **Groups with access**, assign permissions to user groups:
 - To assign permissions to a user group not yet listed:
 - Click **Add group**.
 - Enter the name of the user group to add.
 - Click the **Select Permissions** button.
 - In the dialog box, select check boxes for the permission levels you want to apply for the user group.
 - To edit permissions for a user group already listed:
 - Locate the group in the list.
 - Next to its permission level, click **edit permissions**.
 - In the dialog box, select check boxes for the permission levels you want to apply for the user group.
- Click the **Set Permissions** button.

Creating User Overrides

Create a user override to grant a particular set of permissions to an individual. You might need to create an override if:

- A person requires a particular set of permissions for an area, but isn't (and shouldn't be) a member of a group to which you've already assigned permissions for the area.
- A person is a member of a group to which you've assigned permissions for an area, but they require a different set of permissions than they've received as a member of the group -- in other words, they're an exception to the rule. For example, you might want to separately define their permissions in order to enhance or limit their access in the area.

Use the following steps to create a user override on the permissions page you're editing:

- Under **User Overrides**, click **Create a user override**.
- In the box, start typing the name of the user for whom you want to set the override. Click the popup that displays the user's name.
- Click the **Set override** button to view the permissions you can set.
- In the permissions box for the person you selected, select and clear check boxes as needed. In the end you want the list of checked items to reflect the permissions the person should have. Note that you merely clear a check box to remove a permission -- there's no need to explicitly revoke the permission.
- Click **Set Permissions** to save the override you've created.

Managing Mobile Permissions

With mobile permissions, you set who has access to the community via a mobile device, such as a telephone.

Note: You can also prevent iPhone users from accessing the community by disabling access based on the ID for their phone itself. For more information, see *Managing iPhone Access*.

About Mobile Permission Levels

You can grant (or remove) mobile access to the community.

Note: You can't create custom permission levels here, as you can for space permissions.

Permission	Access Granted
Mobile access	Access Jive SBS using a mobile application, such as for iPhone.

Setting Mobile Permissions

You can set mobile permissions in the admin console on the Mobile Permissions page.

In the UI: Admin Console: Permissions > Mobile Module Permissions

1. On the page, under **Groups with access**, assign permissions to user groups:
 - To assign permissions to a user group not yet listed:
 - a. Click **Add group**.
 - b. Enter the name of the user group to add.
 - c. Click the **Select Permissions** button.
 - d. In the dialog box, select check boxes for the permission levels you want to apply for the user group.
 - To edit permissions for a user group already listed:
 - a. Locate the group in the list.
 - b. Next to its permission level, click **edit permissions**.
 - c. In the dialog box, select check boxes for the permission levels you want to apply for the user group.
2. Click the **Set Permissions** button.

Creating User Overrides

Create a user override to grant a particular set of permissions to an individual. You might need to create an override if:

- A person requires a particular set of permissions for an area, but isn't (and shouldn't be) a member of a group to which you've already assigned permissions for the area.
- A person is a member of a group to which you've assigned permissions for an area, but they require a different set of permissions than they've received as a member of the group -- in other words, they're an exception to the rule. For example, you might want to separately define their permissions in order to enhance or limit their access in the area.

Use the following steps to create a user override on the permissions page you're editing:

1. Under **User Overrides**, click **Create a user override**.
2. In the box, start typing the name of the user for whom you want to set the override. Click the popup that displays the user's name.
3. Click the **Set override** button to view the permissions you can set.
4. In the permissions box for the person you selected, select and clear check boxes as needed. In the end you want the list of checked items to reflect the permissions the person should have. Note that you merely clear a check box to remove a permission -- there's no need to explicitly revoke the permission.
5. Click **Set Permissions** to save the override you've created.