

Managing Permissions

If you're a space or system administrator, use this guide to learn about granting permissions to people for access to content and administrative features.

You set permissions while managing spaces, sub-spaces, and blogs. Most permissions are scoped to the level of the root space (where you set global permissions) or sub-spaces. Sub-spaces inherit permissions from a containing space, but you can augment or revoke inherited permissions at the sub-space level.

Note: You don't manage permissions for social groups in the same way you do for spaces. Permissions changes you make in the admin console have no effect on content permissions for groups. Where a group allows people to view or create content, they have that permission for all content that the group supports.

Your ability to manage permissions in a way that best suits how people use Clearspace is one of the application's most important features. Clearspace uses your permissions settings everywhere — whenever someone does anything with spaces or content. Spaces themselves are designed to support the idea that you'll want to give particular groups of people particular kinds of access to a space's features. A space is a kind of sandbox that you can manage access to with permissions.

For example, a system administrator could give someone permission to *read* documents across the entire application. Then the system or space administrator could give that person permission to *create* new documents only in a particular sub-space (maybe one that corresponds to the department they work in). In another example, in a Marketing Department space everyone might have permissions that allow them to view and post content, but only those product managers with the appropriate permissions will be able to create and approve content — such as brochures and pricing information — that can be accessed by the sales organization.

Summary

- **"Permissions" refers to levels of access for people using Clearspace.** Managing permissions is about answering questions such as "Should a person have the ability to view and edit content in a particular space?" or "Should they be able to create a blog post?" or "Should they moderate content, making changes to content created by others?"
- **System administrators and space administrators can set permissions.** Space administrators can set permissions for the space they're administering, while system administrators can set both global and space permissions.
- **Permissions are inherited and scoped by space.** In Clearspace, you set permissions with the space hierarchy in mind. Clearspace permissions were designed to support the idea that the spaces you create are intended to hold content for a specific group of people (such as a group with a shared interest or organization role). Collecting this content in a space gives you a way to manage it in the best way for its particular set of authors and consumers. That management includes who has access to the content and what kind of access they have.

Note that project permissions are inherited from the space that contains the project. You don't separately manage permissions for a project.

- **By default, no one except the system administrator has permission to do anything.** After you've added user accounts to the system, a system administrator sets about granting permission for what people should be able to do globally (by setting permissions in the root space), then permissions for sub-spaces

are granted or revoked on a space by space basis. (Usually the easiest way to do this is to group people into user groups, then grant or revoke permission to the groups.)

- **Content permissions are separate from administrative permissions.** You grant permissions for what people can do with content (creating, reading, rating, voting, and so on) in a separate part of the admin console UI from where you assign people to be space admins or content moderators. Content and administrative permissions are both inherited in space hierarchies.
- **You manage blog permissions independently.** Blogs are designed to be relatively free-standing (although you can aggregate blogs into spaces). That means that you don't manage blog permissions within the context of managing space permissions. System administrators manage blog permissions using a blogs permissions page. That also applies to project blogs.

User Types: Anyone, Registered, User, and Group

A user type represents a level of knowledge or trust about a person. You probably feel you have more knowledge or trust about someone who has registered to use Clearspace than you do about someone who is using the application anonymously. User types provide a convenient, built-in way to manage a person's access to application features.

Clearspace includes two default user types that you can't delete: *Anyone* and *Registered Users*. Once a user registers, you can assign them permissions as a *User* or as part of a *Group*. This results in four categories of Clearspace users who can receive global permissions.

- An *Anyone* user is simply anyone who visits Clearspace. This user type is a guest or anonymous user. 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.)
- A *Registered User* is someone who has entered registration information and logged in for access. Registered User permissions are globally assigned permissions you give to anyone who registers. A Registered User has the same permissions in a given category as an *Anyone* user if no Registered User permissions have been set. Guest users are registered users whose user name is the email address they gave when they registered. Among registered users, Clearspace provides a way for you to assign permissions according to the following two categories:
 - A *User* is a registered individual.
 - A *Group* is a group of registered individuals. You'll find it useful to create user groups when you want to assign the same set of permissions to a number of people, such as people in a particular department.

Note: Revoking a permission for *Anyone* — that is, putting a red X in the permission box — revokes that permission for registered users also. That's true *whether or not* you explicitly put a green check mark in the permission box for registered users.

Where Do Guest Users Fit In?

If your Clearspace instance is using the document sharing service, you might have *guest* users. You can't configure permissions for guest users. Guest users are those who have access to the service, but not to your Clearspace instance itself. If they've been invited by someone using your Clearspace instance, their names will show up in the admin console's user summary, but their accounts aren't included in your permissions work.

Permission Levels: Admin, Moderator, and Space Feature

A permission level represents access to a particular set of Clearspace features. Permission levels fall into two kinds: those for administrators and moderators that capture access to a set of features and those for end users that capture access to individual features.

- Admin permission levels include system admin, space admin, user admin, group admin. When you grant any of these, you're actually granting access to a set of administrative-type features in Clearspace.
- Moderator permission levels include system admin, root space content moderator, space content moderator. When you grant these, you're granting permission to moderation features through which people allow or reject content others want to publish.
- Space permission levels include more fine-grained access such as whether a person can create documents or projects, or whether they can view a space or create private messages.

The following briefly describes each of the permission levels. Also, see [Feature and UI Access By Permission Type](#) (page 7) for tables that shows who has access to what.

System Admin

Essentially, a system admin can do anything they want to. They have full access to every Clearspace feature at every space level. Generally speaking, though, a good best practice is to delegate lower-level administrative and moderation access to other people. For example, a person who uses a particular sub-space regularly is probably a better person to act as that space's administrator, or to moderate content in the space. Delegating frees the system administrator to focus on system issues, rather than on space or content issues.

For a guide to things only a system administrator can do, see the *System Administrators' Guide*.

Space Admin

A space admin has access to administrative features for the space they've been assigned to administer, along with any sub-spaces beneath it (although their space admin access can be revoked in each of those sub-spaces). A space administrator can create sub-spaces, set content defaults, and set permissions for the space. They can see content that is in a moderator's queue but hasn't been approved yet. They can even designate other space administrators.

You'll find a detailed description of what a space admin can do in *Managing Spaces*.

User Admin and Group Admin

User and group admins can create and edit user and group accounts. These are global permission levels that only a system administrator can grant. A user admin can create and edit user accounts, while a group admin can create and edit group accounts. Neither of these permission level grants a person the ability to set permissions — only to manage account information.

Note that if your Clearspace instance is using LDAP or some other data source that is not writable, having separate user and group admins might not be necessary.

Managing Users and Groups provides more information about what user and group admin can do.

Content Moderator

Granting moderator permission gives someone two kinds of abilities.

- A content moderator has access to certain links for handling content after it's published. Through these they can manage content by editing, moving, and deleting it as the need arises. For example, a content moderator might lock a discussion thread that is no longer useful or move a document to another space. These abilities are inherited by sub-spaces of the space in which the permission is granted.
- A content moderator can approve or reject content before it's published. When moderation is on for the context in which the content was created (such as the space, social group, or even globally), the content moderator for that context will be able to accept or reject the content in a moderation queue. Setting this up involves not only assigning content moderation permission, but also turning on moderation for those kinds of content you want moderated. This ability is not inherited in sub-spaces; the moderator can approve or reject content only in the context where they've been assigned permission.

Where you set content moderator permission depends on *which* content you want moderated. For all, though, you grant content moderator permission in the admin console at Spaces > Permissions > Admins & Moderators.

Note: Access to moderation queues isn't inherited to sub-spaces.

But you'll choose a different scope by selecting the **change space** link on the Admins & Moderators page.

| For Moderation Context | Choose This Scope |
|---|--|
| Documents and discussions in a space or project | Sub-space containing the content or project. |
| Documents and discussions in social groups | Root space (moderator for content in all social groups). |
| Personal blog posts everywhere | Root space (moderator for posts to all personal blogs). |
| Space blog posts in a space or project | Sub-space the blog was created in. |
| Announcements and private messages | Root space (moderator for all announcements and private messages). |

Note that as a failsafe to ensure that moderated requests always have a place to go, new requests are routed in the following order:

1. If content would be moderated at the sub-space level but there's no moderator there, it goes to the root space moderator's queue.
2. If content would be moderated at the root space level but there's no moderator there, it goes to the system administrator's queue.

This applies to new requests only. For example, if a request is in the queue when moderators are removed, the requests will remain in the queue until someone approves or rejects them there. Existing requests won't be routed to the next queue up. If there's only one moderator and that person is deleted from the system, then requests currently in the queue will be orphaned even after a new moderator is assigned to that area. If moderation permissions are merely revoked (or un-granted) for someone, then they'll still have access to the requests currently in the queue but won't be able to approve or reject them.

Keep in mind that in order to have moderators approve and reject content in a moderation queue, moderation will need to be enabled for specific content types in the console at Spaces > Settings > Moderation Settings.

For more on these, see *Managing Spaces*. For a detailed look at what content moderators do, see *Moderating Content*.

Space Feature

For non-administrative people, you can assign fine-grained access to Clearspace features. Features set at the root space level are inherited by sub-spaces.

Note: Space permissions have no effect on permissions in effect in social groups. You can't set these kinds of permissions for social groups.

How Permission Inheritance Works

Permissions you set in a space are inherited by the sub-spaces inside it unless you revoke or grant permissions in those sub-spaces.

Global Space Permissions. A system administrator sets global permissions — whether for all users, specific users, or groups — by setting permissions in the root space. Those permissions are, by default, inherited in all spaces beneath. That applies to both end user permissions — through which people read and create content, for example — and administrative access — such as space administrators, content moderators, and so on.

Sub-Space Permissions. Sub-spaces inherit the permissions of the space that contains them, but a system or space administrator can grant new permissions or revoke permissions according to what's best for the space, effectively overriding inherited permissions.

Note: Permissions are inherited, but other containment-related features are not. For example, searches in a particular space do not return content in its sub-spaces. Also note that access to moderation queues is not inherited; a moderator approves and rejects content only in the area they're assigned to.

When someone accesses content, Clearspace checks permissions as follows:

1. The application examines global permissions — the permissions the person has within the entire Clearspace instance.
2. The application looks at Group permissions for groups the person's user account belongs to.
3. The application applies content permissions at the following levels:
 - Space — Permissions for all people when they log into the space and access space content. Add these permissions to user or group accounts at the space level.
 - Sub-space — Permissions for people in a sub-space. Clearspace checks the person's sub-space permissions to see if they have been modified from the original space-level permissions. If so, when the user accesses content in that space or related sub-spaces, the sub-space permissions override the space permissions. Otherwise, space permissions are inherited by sub-spaces beneath the space.

The following uses snapshots of the admin console permissions pages to show how permission settings are inherited in a space hierarchy. The space hierarchy illustrated here is Root Space > Second-Level Subspace > Third-Level Subspace.

Root Space

| | View Space | Read Document | Read Comment | Rate Document | Create Thread |
|--------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| Anyone * | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Registered Users * | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Global Read/Create Permissions
Permission to view some content granted to Anyone (registered and anonymous users). Permission to rate and create content granted to registered users only. Cleared boxes at the root level mean that permissions aren't granted.

Second-Level Subspace

| | View Space | Read Document | Read Comment | Rate Document | Create Thread |
|--------------------|-------------------------------------|--------------------------|--------------------------|-------------------------------------|-------------------------------------|
| Anyone * | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Registered Users * | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Limiting Space Visibility
Green tint shows how permissions are set in a containing space (the root) as granted. But permission to view **this** subspace is revoked for Anyone (anonymous and registered users), then granted to a group of registered users called hr_workers. Here beneath the root level, cleared boxes mean that these permissions are inherited.

Third-Level Subspace

| | View Space | Read Document | Read Comment | Rate Document | Create Thread |
|--------------------|--------------------------|-------------------------------------|--------------------------|-------------------------------------|-------------------------------------|
| Anyone * | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Registered Users * | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Subspace Inheriting Space Visibility
Green tint shows how permissions are set in a containing space as granted; purple tint shows how permissions are set in a containing space as revoked. Cleared boxes mean that these permissions are inherited.

Note: Revoking a permission for Anyone — that is, putting a red X in the permission box — revokes that permission for registered users also. That's true *whether or not* you explicitly put a green check mark in the permission box for registered users.

Granting New Permissions

You grant permissions — that is, give access to particular people or groups — with the Grant New Permission tab. This works in basically the same way whether you're granting administrative access or access to space features. In both cases, you select the permission you want to grant, enter the name for a user or group account receiving the access, then click Grant New Permission. To grant permissions, in the admin console go to Spaces > Permissions, then select the space you want to grant permission for. Click Admin & Moderator or Space Permissions to reach the page that describes permissions already set for the space.

The following shows the Grant New Permission tab for space features.

[Space List](#) » R and D
 Edit space permissions to set the permissions policies that the space will use.

Note: Checkboxes on this page have three states () Click a checkbox repeatedly to rotate through all three states.

Grant New Permissions

Permission Summary Grant New Permission

Follow the steps below to grant new user or group permissions: (Note, it is not possible to set permissions for "Anyone" or "Registered Users" here. To do this, use the Permissions Summary page(s).)

1 Choose the permission(s): [select all](#)

- View Space
- Read Document
- Read Comment
- Rate Document
- Create Thread
- Create Message
- Create Message Attachment
- Create Document
- Create Document Attachment
- Create Comment
- Create Poll
- Vote in Poll
- Create Announcement
- Create Image
- Create Project

2 Choose a user or group to grant the permission(s) to:

A Specific User:

 Type the username of the person you want to add.
 Don't know the username? Use the [User Picker](#).

A Specific Group: (enter group name - separate multiple group names with commas)

3 Done:

Feature and UI Access By Permission Type

People with certain kinds of permissions have certain access to Clearspace features. These features include those in the admin console and those in the end user interface. This lists user interface features and shows which permission level has access to which feature.

Access to the Admin Console

The admin console is available to system admins, space admins, and user and group admins. In some cases, features available in the console are also available in the Clearspace end user interface. The following table lists the pages of the admin console, indicating who has access to the page: system admin, space/community admin, user admin, or group admin. Page names are linked to related documentation.

| Admin Console Section | Admin Access |
|---------------------------------|--------------|
| Dashboard | |
| System | |
| Management | |
| <i>System Information</i> | System |
| <i>License Information</i> | System |
| <i>System Properties</i> | System |
| <i>Locale</i> | System |
| <i>Log Viewer</i> | System |
| <i>Audit Log Viewer</i> | System |
| <i>Query Stats</i> | System |
| <i>Sending Usage Statistics</i> | System |
| <i>Document Sharing</i> | System |
| Settings | |
| <i>Attachments</i> | System |
| <i>Images</i> | System |
| <i>Caches</i> | System |
| <i>Space/Community</i> | System |
| <i>Discussions</i> | System |
| <i>Documents</i> | System |
| <i>Email Server</i> | System |
| <i>Message Templates</i> | System |
| <i>Feeds</i> | System |
| <i>OpenSearch Engines</i> | System |
| <i>Page Compression</i> | System |
| <i>Phrase Substitutions</i> | System |
| <i>Private Messages</i> | System |
| <i>Projects</i> | System |

| | |
|---------------------------------|---------------------------|
| <i>Search</i> | System |
| <i>Spell Check</i> | System |
| <i>Themes</i> | System |
| <i>Web Services</i> | System |
| <i>Widgets</i> | System |
| Plugins | |
| <i>Installed Plugins</i> | System |
| <i>Add Plugin</i> | System |
| Database Migration | |
| <i>Database Migration</i> | System |
| Real-Time | |
| <i>Overview</i> | System |
| <i>Connection</i> | System |
| <i>Openfire Admin</i> | System |
| Spaces/Communities | |
| Management | |
| <i>Summary</i> | System Space/Community |
| <i>Document Management</i> | System Space/Community |
| <i>Discussion Management</i> | System Space/Community |
| <i>Tag Group Management</i> | System Space/Community |
| <i>Merge Spaces</i> | System Space/Community |
| Settings | |
| <i>Space/Community Settings</i> | System Space/Community |
| <i>Discussion Settings</i> | System Space/Community |

| | |
|------------------------------------|---------------------------|
| <i>Document Settings</i> | System Space/Community |
| <i>Moderation Settings</i> | System Space/Community |
| <i>Abuse Settings</i> | System Space/Community |
| <i>Community Everywhere</i> | System Space/Community |
| <i>Thread Archive Settings</i> | System Space/Community |
| <i>Extended Properties</i> | System Space/Community |
| <i>Filters and Macros</i> | System Space/Community |
| <i>Gateway Settings</i> | System |
| <i>Interceptors</i> | System |
| Permissions | |
| <i>Admins & Moderators</i> | System Space/Community |
| <i>Space/Community Permissions</i> | System Space/Community |
| Blogs | |
| Management | |
| <i>Personal Blogs</i> | System |
| <i>System Blogs</i> | System |
| <i>Comments</i> | System |
| <i>Trackbacks</i> | System |
| <i>Migrate</i> | System |
| Settings | |
| <i>Blog Settings</i> | System |
| Permissions | |
| <i>Global Permissions</i> | System |

| | |
|---|--|
| People | |
| Management | |
| <i>User Summary</i> | System User |
| <i>Create User</i> | System User |
| <i>Group Summary</i> | System Group |
| <i>Create Group</i> | System Group |
| <i>User Search</i> | System User Group |
| <i>User Relationships</i> | System User Group |
| Settings | |
| <i>Avatar Settings</i> | System |
| <i>Ban Settings</i> | System |
| <i>Password Reset</i> | System |
| <i>Profile and Homepage</i> | System User Group |
| <i>Registration Settings</i> | System |
| <i>Status Level Settings</i> | System |
| <i>User Data Synchronization Settings</i> | System User Group |
| <i>User Relationship Settings</i> | System |
| Reporting | |
| Reporting | |
| <i>Main</i> | System Space/Community User Group |

| | |
|--------------------------------|--|
| <i>Tags</i> | System Space/Community User Group |
| <i>Discussions</i> | System Space/Community User Group |
| <i>Documents</i> | System Space/Community User Group |
| <i>Blogs</i> | System Space/Community User Group |
| <i>People</i> | System Space/Community User Group |
| <i>Settings</i> | |
| <i>Third-Party Integration</i> | System |

Access to End User Features

The following sections describes how Clearspace provides access to end user features based on permission levels. Needless to say, whether a given feature — such as the ability to edit a thread — is available to anyone will depend on whether the feature has been enabled for the space's users. These sections focus on typical defaults and illustrate in particular how access is different for administrators and moderators.

Note: Space permissions aren't in effect in social groups.

Access to End User Discussion Features

The following table lists commands for discussions. It shows which commands are available depending on a person's permission level. Some of these are in the Actions list that's displayed when you're viewing the discussion, while others are visible at the bottom of a reply.

| Command | Location | Description | System Admin | Space Admin | Content Moderator | Creator | Viewer |
|-------------|--------------|----------------------------|--------------|-------------|-------------------|---------|--------|
| Edit thread | Actions list | Edit the original message. | ✓ | ✓ | ✓ | ✓ | |

| | | | | | | | |
|-----------------------------------|--------------|---|---|---|---|---|---|
| Lock thread | Actions list | Set the thread so that no one can reply. | ✓ | ✓ | ✓ | | |
| Move thread | Actions list | Move the thread to another space. | ✓ | ✓ | ✓ | | |
| Delete thread | Actions list | Delete the thread from Clearspace | ✓ | ✓ | ✓ | | |
| Receive/ stop email notifications | Actions list | Control email notifications for yourself (as the person logged in). | ✓ | ✓ | ✓ | ✓ | ✓ |
| Send as email | Actions list | Send an email about the thread to other people. | ✓ | ✓ | ✓ | ✓ | ✓ |
| Convert thread to document | Actions list | Create a new document using the text of the thread. | ✓ | ✓ | ✓ | ✓ | ✓ |
| View as PDF | Actions list | View the thread as PDF file. | ✓ | ✓ | ✓ | ✓ | ✓ |
| View print preview | Actions list | View the thread as it will be printed. | ✓ | ✓ | ✓ | ✓ | ✓ |
| Edit | Reply body | Edit the text of a reply. | ✓ | ✓ | ✓ | ✓ | |
| Delete | Reply body | Delete a reply. | ✓ | ✓ | ✓ | ✓ | |

| | | | | | | | |
|--------------------------------|------------|--|---|---|---|---|---|
| Branch | Reply body | Create a new discussion thread using the reply as the first message. | ✓ | ✓ | ✓ | ✓ | |
| Abuse (with reporting enabled) | Reply body | Report an abusive post to administrators. | ✓ | ✓ | ✓ | ✓ | ✓ |
| Reply | Reply body | Add a reply to the thread. | ✓ | ✓ | ✓ | ✓ | ✓ |

Access to End User Document Features

The following table lists commands for documents. It shows which commands are available depending on a person's permission level. All of these are in the Actions list that's displayed when you're viewing the document.

| Command | Location | Description | System Admin | Space Admin | Content Moderator | Creator | Viewer |
|----------------------|--------------|---|--------------|-------------|-------------------|---------|--------|
| Edit document | Actions list | Open the document in the editing window. | ✓ | ✓ | ✓ | ✓ | ✓ |
| Manage versions | Actions list | View the document's version history. | ✓ | ✓ | ✓ | ✓ | ✓ |
| Move document | Actions list | Move the document to another space. | ✓ | ✓ | ✓ | | |
| Manage collaboration | Actions list | Specify who edits and approves the document, and whether comments | ✓ | ✓ | ✓ | ✓ | |

| | | | | | | | |
|----------------------------------|--------------|---|---|---|---|---|---|
| | | are allowed. | | | | | |
| Delete document | Actions list | Delete the document from Clearspace. | ✓ | ✓ | ✓ | ✓ | |
| Receive/stop email notifications | Actions list | Control email notifications for yourself (as the person logged in). | ✓ | ✓ | ✓ | ✓ | ✓ |
| Send as email | Actions list | Send an email about the document to other people. | ✓ | ✓ | ✓ | ✓ | ✓ |
| View as PDF | Actions list | Open the document as PDF file. | ✓ | ✓ | ✓ | ✓ | ✓ |
| View print preview | Actions list | View the document as it will be printed. | ✓ | ✓ | ✓ | ✓ | ✓ |

Access to End User Space Features

A person's access to space-level features is determined by their permissions level. These features are typically available when a person is looking at the space's All Content tab. In addition, a system or space admin has access to the **customize** link on the Overview tab, through which they can customize the layout of the Overview tab.

| Command | Location | Description | System Admin | Space Admin | Content Moderator | Viewer |
|--------------------|--------------|---|--------------|-------------|-------------------|--------|
| Start a discussion | Actions list | Create a new discussion. | ✓ | ✓ | ✓ | ✓ |
| Create a document | Actions list | Create a new document. | ✓ | ✓ | ✓ | ✓ |
| Write a blog post | Actions list | Create a new post to the space's blog. Any set as an author | ✓ | ✓ | ✓ | ✓ |

| | | | | | | |
|------------------------|--------------|---|---|---|---|---|
| | | on the blog can post to it, and only those set as an author can post. | | | | |
| Create an announcement | Actions list | Create an announcement that will be visible in the space. | ✓ | ✓ | ✓ | |
| Create a poll | Actions list | Create a poll that will be visible on the All Content page, or (optionally) the space overview. | ✓ | ✓ | ✓ | ✓ |
| Create a tag group | Actions list | Create a tag group to collect tags. | ✓ | ✓ | | |
| Create a sub-space | Actions list | Create a space that's inside another space. | ✓ | ✓ | | |
| Create a project | Actions list | Create a new project to organize tasks. | ✓ | ✓ | ✓ | ✓ |

Permission Defaults for New Spaces

When you create a new space Clearspace prompts you to select a default access scheme. Each of these -- inherited, open, restricted, and private -- is a kind of security template that's made up of particular permissions settings. After you've created the space, you can edit permissions however you like, of course; the access schemes are really just to get you started quickly. The following illustrates show what you get for each.

Inherited

In the inherited scheme, the newly created sub-space inherits permissions from its immediate parent space. By default, as shown here, the green-tinted permissions are granted, while those without a green tint (but with cleared boxes) are not granted.

Permissions Summary

Permission Summary | Grant New Permission

| | View Space | Read Document | Read Comment | Rate Document | Create Thread | Create Message | Create Message Attachment | Create Document | Create Document Attachment | Create Comment | Create Poll | Vote in Poll | Create Announcement | Create Image | Create Project | Remove |
|--------------------|--------------------------|--------------------------|--------------------------|-------------------------------------|-------------------------------------|-------------------------------------|---------------------------|-------------------------------------|----------------------------|-------------------------------------|--------------------------|-------------------------------------|--------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| User Types | | | | | | | | | | | | | | | | |
| Anyone * | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| Registered Users * | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Users | No user permissions. | | | | | | | | | | | | | | | |
| Groups | No group permissions. | | | | | | | | | | | | | | | |

Save Changes | Cancel

Open

In the open scheme, access is open for registered users but several of the permissions are explicitly revoked for anonymous users. In particular, these users can see the space, documents, and comments, but they can't contribute by creating content, voting in polls, and so on.

Permissions Summary

Permission Summary | Grant New Permission

| | View Space | Read Document | Read Comment | Rate Document | Create Thread | Create Message | Create Message Attachment | Create Document | Create Document Attachment | Create Comment | Create Poll | Vote in Poll | Create Announcement | Create Image | Create Project | Remove |
|--------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| User Types | | | | | | | | | | | | | | | | |
| Anyone * | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Registered Users * | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Users | No user permissions. | | | | | | | | | | | | | | | |
| Groups | No group permissions. | | | | | | | | | | | | | | | |

Save Changes | Cancel

Restricted

The restricted access scheme is designed to exclude anonymous users but provide access for registered users.

Permissions Summary

Permission Summary | Grant New Permission

| | View Space | Read Document | Read Comment | Rate Document | Create Thread | Create Message | Create Message Attachment | Create Document | Create Document Attachment | Create Comment | Create Poll | Vote in Poll | Create Announcement | Create Image | Create Project | Remove |
|--------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| User Types | | | | | | | | | | | | | | | | |
| Anyone * | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Registered Users * | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Users | No user permissions. | | | | | | | | | | | | | | | |
| Groups | No group permissions. | | | | | | | | | | | | | | | |

Save Changes | Cancel

Private

The private scheme revokes permission for everyone except the system administrator. This scheme is useful if you want to create a space that's unavailable to everyone, with the idea that you're going to explicitly allow access only to certain users or groups. After you create the space, you can grant permissions to those who'll be using it.

The screenshot shows a 'Permissions Summary' window with a 'Grant New Permission' button. Below the button is a table with columns for various actions: View Space, Read Document, Read Comment, Rate Document, Create Thread, Create Message, Create Message Attachment, Create Document, Create Document Attachment, Create Comment, Create Poll, Vote in Poll, Create Announcement, Create Image, Create Project, and Remove. The table has two rows: 'Anyone *' and 'Registered Users *'. Each cell in the table contains a red 'X' icon, indicating that permissions are revoked for all actions for both user types. At the bottom of the table, there are 'Save Changes' and 'Cancel' buttons.

| | View Space | Read Document | Read Comment | Rate Document | Create Thread | Create Message | Create Message Attachment | Create Document | Create Document Attachment | Create Comment | Create Poll | Vote in Poll | Create Announcement | Create Image | Create Project | Remove |
|--------------------|-----------------------|---------------|--------------|---------------|---------------|----------------|---------------------------|-----------------|----------------------------|----------------|-------------|--------------|---------------------|--------------|----------------|--------|
| User Types | | | | | | | | | | | | | | | | |
| Anyone * | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| Registered Users * | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| Users | No user permissions. | | | | | | | | | | | | | | | |
| Groups | No group permissions. | | | | | | | | | | | | | | | |

Examples: Setting Global and Space Permissions

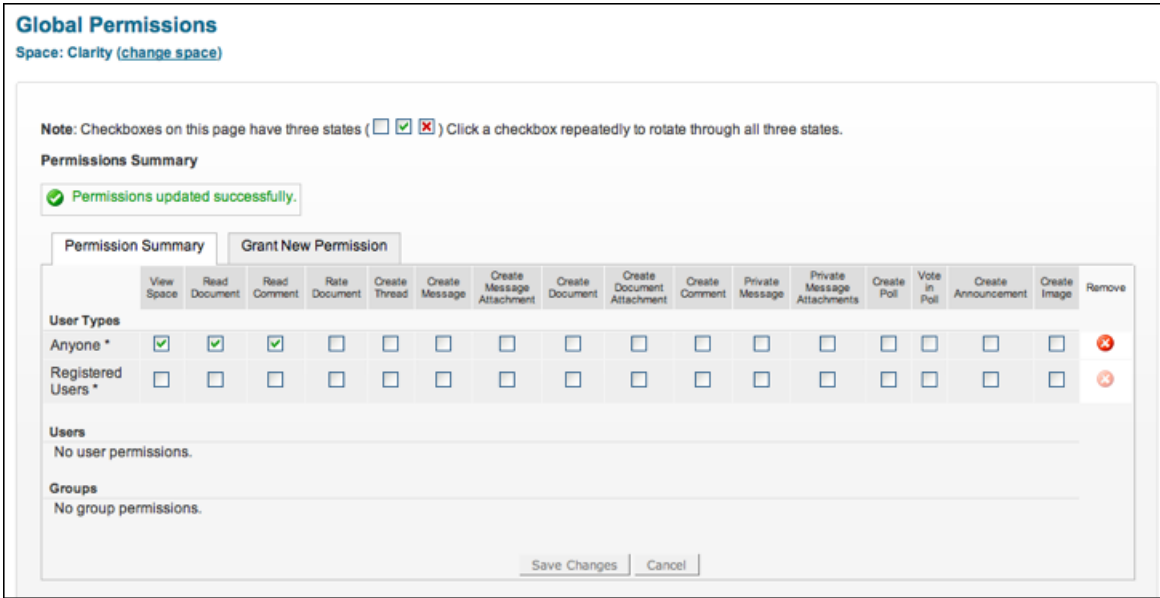
The following lists a few common scenarios describing things you might want to do when managing permissions, along with how to make changes in the admin console to support those scenarios.

Deny all permissions to everyone, but grant certain permissions to certain groups

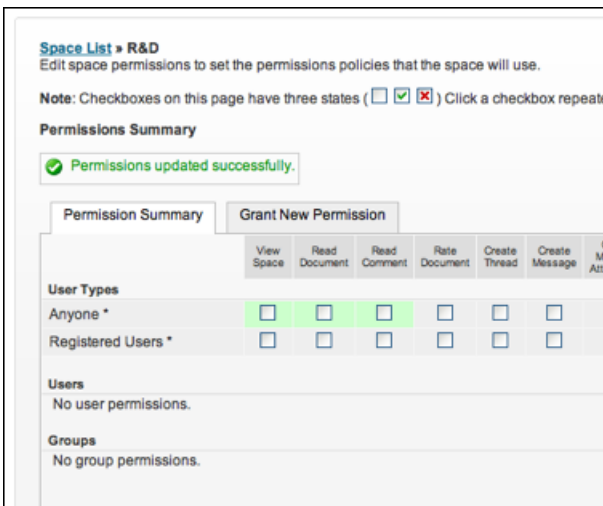
Clear all permission check boxes for the root space, then set permissions in subspaces as needed. Clearing the boxes sets root permissions to their unset state; at the root, that state is "not permitted." In other words, you don't need to first explicitly "revoke" permissions at the root level (with red X marks), then selectively grant them. (You can easily clear all of the boxes in the Anyone or Registered Users rows by clicking the Remove icon at the far right of the row.)

While elsewhere a cleared box means "inherit from the containing space," at the root there's nothing to inherit from. That means that none of your users will be able to use Clearspace (reading or adding content) until you start granting permission by selecting check boxes with check marks. Again, remember that in every space beneath the root, a cleared check box means that permissions are inherited.

In the following summary of the root space permissions, only three actions are allowed: viewing the space, reading documents and reading comments. Unless you grant further permission here or in communities contained by the root, users — registered or anonymous — will be able to do only those three things.



The following summary of R&D, a space under the root, shows that permission to view the space, read its documents, and read its comments is granted because it is inherited from the root space. No other actions are allowed.

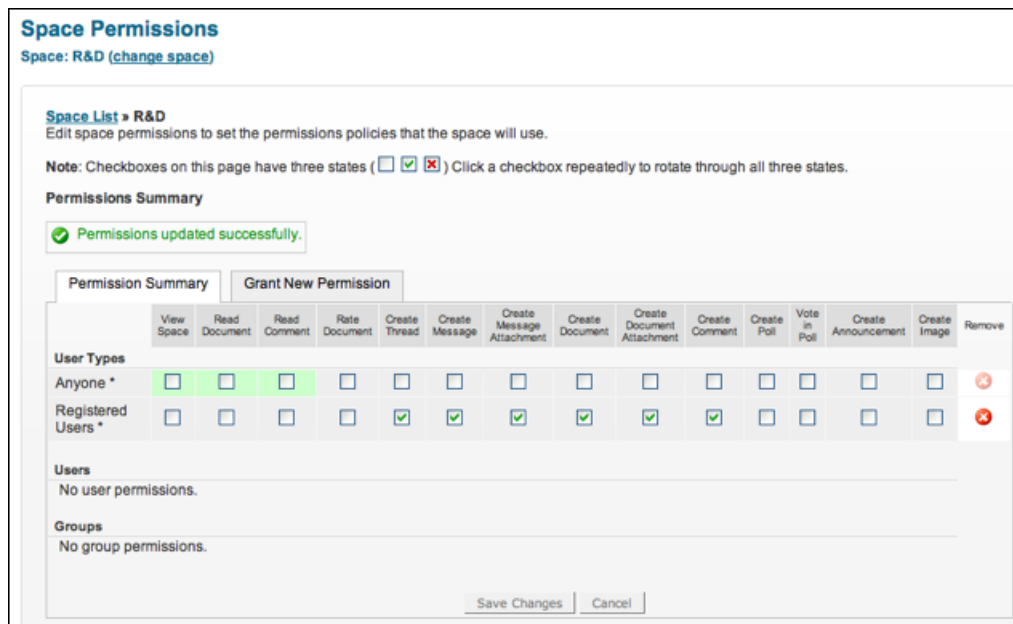


Allow any user to see the content in all communities, but allow only registered users to add or edit content for particular communities

At the root space, in the Anyone row, select the "read"-related permissions (View Space, Read Document, Read Comment) with green check marks. For each of the other actions you want to allow, view the permission summary for the space, then select the check box with a green check mark for Registered Users. (When you grant permission for actions for Anyone users, you don't need to explicitly grant them for Registered Users. Registered Users can do whatever you allow for Anyone users unless you explicitly revoke the permission for Registered Users.)

For example, the following illustration shows the permission summary for R&D, a space contained by the root space. The green tint for the View Space, Read Document and Read Comment actions show that those actions

are allowed for all users because their permissions are inherited from a containing space (in this case, the root) where they're explicitly allowed. Cleared check boxes for the other actions indicate that permissions for those actions are also inherited, but the actions aren't allowed because permission for them hasn't been granted. Check boxes with green check marks indicate that permission for those actions is granted for this space and its sub-communities.



Hide a space from all but a certain group of users

Set permissions as needed for other communities, then revoke View Space permission for Anyone users for the space you want to hide. Finally, create a user group whose members are the users that will have permission to view the "hidden" space, then use a check mark in View Space to explicitly allow that user group to see the space.

The following shows the permission summary for HR, a space contained by the root space. Note that permission for the View Space action is revoked for Anyone users, but it's allowed for the hr_workers user group. This means that no one who isn't a member of hr_workers will be able to see the space. What's more, members of the hr_workers group will be able to do all of the things that registered users can otherwise do in other communities because hr_workers group members are registered users, too. Those allowed actions include everything shown with a green tint, where permission is inherited from the containing space.

In other words, there's no need to explicitly "turn on" permission for an action unless that action is otherwise not allowed. For example, if you wanted hr_workers members to be able to create polls in the HR space, you'd need to put a check mark in the Create Poll check box.

Space Permissions

Space: [HR \(change space\)](#)

[Space List](#) » [HR](#)
 Edit space permissions to set the permissions policies that the space will use.

Note: Checkboxes on this page have three states () Click a checkbox repeatedly to rotate through all three states.

Permissions Summary

✔ Permissions updated successfully.

Permission Summary Grant New Permission

| | View Space | Read Document | Read Comment | Rate Document | Create Thread | Create Message | Create Message Attachment | Create Document | Create Document Attachment | Create Comment | Create Poll | Vote in Poll | Create Announcement | Create Image | Remove |
|----------------------------|-------------------------------------|--------------------------|--------------------------|--------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|--------------------------|--------------------------|-------------------------------------|
| User Types | | | | | | | | | | | | | | | |
| Anyone * | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| Registered Users * | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| Users | No user permissions. | | | | | | | | | | | | | | |
| Groups | | | | | | | | | | | | | | | |
| hr_workers | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |

Deny permission for actions to a particular user

Set permissions as needed for other communities, then revoke permissions for the particular user.

In the following summary of permissions for the HR space, Steve is in the `hr_workers` user group, but his permission for several actions has been revoked. This summary indicates that he can see the HR space (View Space is explicitly checked for `hr_workers`), he can read comments and documents and rate documents (the green tint indicates "allowed" permission for those actions is inherited), but he can't performed the red-Xed actions (the X revokes permission).

There's no need to revoke his permission for Create Poll, Create Announcement, and Create Image because he never had it: permission for those actions is inherited as "not allowed" (there's no green tint that indicates the action is explicitly allowed in a containing space). Note that you might want to explicitly revoke the user's permission (even if it's currently unnecessary) to ensure they're revoked in the event that you later allow that action in a containing space.

Space Permissions

Space: [HR \(change space\)](#)

[Space List](#) > [HR](#)
 Edit space permissions to set the permissions policies that the space will use.

Note: Checkboxes on this page have three states () Click a checkbox repeatedly to rotate through all three states.

Permissions Summary

✔ Permissions updated successfully.

Permission Summary Grant New Permission

| | View Space | Read Document | Read Comment | Rate Document | Create Thread | Create Message | Create Message Attachment | Create Document | Create Document Attachment | Create Comment | Create Poll | Vote in Poll | Create Announcement | Create Image | Remove |
|----------------------------|-------------------------------------|--------------------------|--------------------------|--------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|--------------------------|-------------------------------------|--------------------------|--------------------------|-------------------------------------|
| User Types | | | | | | | | | | | | | | | |
| Anyone * | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| Registered Users * | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| Users | | | | | | | | | | | | | | | |
| steve | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| Groups | | | | | | | | | | | | | | | |
| hr_workers | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |

Setting Personal and System Blog Permissions

Permissions behavior is different between spaces and some blogs. Permissions for blogs are split between blogs that aren't contained by a space, project, or group and those that are, such as system and personal blogs. Here's how it breaks down:

| Blog Type | Permissions You Can Set | Where You Set Permissions in the Console |
|---------------------------|-----------------------------|---|
| System and personal blogs | Create or read these blogs. | Blogs > Permissions > Global Permissions |
| | Post to these blogs. | Spaces (for the containing space) > Permissions > Space Permissions |
| Space and project blogs | Post to these blogs. | Spaces (for the containing space) > Permissions > Space Permissions |
| Group blogs | Post to these blogs. | Spaces (for the root space) > Permissions > Space Permissions |

Note that you can't set "create blog" permission for blogs in spaces, projects, and groups. Instead, whether those contexts have a blog (in other words, whether one is created there) is based on settings someone makes when creating the space, project, or group. Likewise, you can't set "read blog" permission for a space, project, or group -- if there's a blog there, someone with access to that context can read its posts.

Examples: Setting Global Blog Permissions

Here are a few scenarios that illustrate things you might want to do, and how you can set blog permissions to do them. Note that the settings under the Blog tab in the admin console affect top-level (system and personal) blog only. You can manage settings for another kinds of blog by going to that blog's Manage Blog page.

Set permissions to read blogs and create blogs for system and personal blogs

Set global permissions for blogs at the Blogs > Permissions tab in the admin console.

Grant permission for a particular user to post to a particular blog

For a space or project blog, you grant the Create Blog Post permission when settings permissions for the space at Spaces > Permissions > Space Permissions.

For a system or personal blog, go to Blogs > Management > System Blogs and choose System Blogs or Personal Blogs. In the list of blogs, find the one you want to change and click the Edit icon. On the editing page, add the user as an author and click Update Blog.

Admin Console: Blogs > Settings > Global Permissions

Admin Console: Spaces > Permissions > Space Permissions (for the root space)