Roles

A role is a collection of capabilities with permissions assigned to them, that you can assign to specific users in specific contexts of the site.

Assigning system roles

If you assign a system role, then this means the assigned user will have the levels of access and control associated with that role across the entire Totara site. For that reason the default available system roles are only ones which naturally lend themselves to requiring this context.

To assign a system role follow these steps:

1. From the **Administration** block go to *Site administration* > *Users* > *Permissions* > *Assign system roles*.
2. Click the name of the role you wish to assign.
3. Find (or search for) the user in the **Potential users** column.
4. Click the user's name and then the **Add** button.

Repeat these steps until you have added all the users you want before navigating away from the page, there is no save button. If you need to remove any users this is similar to the steps above, but you need to click their name in the **Existing users** column and then click the **Remove** button.

It is also worth noting that users will appear greyed out in the **Existing users** column if they have been assigned a system context role via an audience.

Defining user roles

The **Define roles** page has four tabs: **Manage roles**, **Allow role assignments**, **Allow role overrides** and **Allow role switches**.

The **Manage roles** tab contains a list of roles on your site. The **Edit** column contains icons for editing, deleting, and for moving roles. You can move them up or down in the list (affecting the way that roles are listed around Totara). Below the table is an **Add a new role** button.

If you wish to modify the capabilities for a particular role, you can do so by editing the role. For example you may want to allow trainees to unenrol themselves from a course when using manual enrolment.

Before we can look at creating, editing, and assigning roles in more detail we first need to understand how roles work, including what permissions and capabilities are within Totara Learn.

Role contexts

Roles are available site-wide and can be assigned to a user at various levels:

- **Site:** A role at this level (and it's associated permissions) will apply to the entire Totara Learn site.
- **Category:** A role assigned at this level applies to the entire category and therefore permissions associated with the role would be granted for all courses contained in that category.
- **Course:** A role given to a user within the content/confines of a specific course.
- **Activity level:** A role can be given within an individual activity, and it's permissions would only apply within that activity (it would not apply to the rest of the course or any higher contexts).

These levels act as a hierarchy for permissions, with site being the top and activity level at the bottom. Generally permissions at a lower context will override those at a higher context in the case of a user having been assigned multiple roles. For example if a user is given Trainer access to an individual activity then they will be able to access the activity with Trainer permissions, regardless of their course level permissions.

(This video is taken from the Site-level user management course on the Totara Academy, where you can access more resources and learning materials - including other videos).

Permission levels

Additionally it is also important to understand there are four levels of permissions (which are assigned to capabilities that make up a role):

- **Not set:** The permission hasn't been set for this capability.
- **Allow:** Permission is granted for the capability.
- **Prevent:** Permission is removed for the capability, even if allowed in a higher context.

On this page

Related pages

The Totara Academy has a whole course dedicated to Site-level user management in Totara Learn. Here you can learn more about user management, see best practice, and give it a go yourself.

- **Prohibit:** Permission is completely denied and cannot be overridden at any lower (more specific) context.

Permissions will also act hierarchically, with an **Allow** permission beating a **Prevent** permission in the case of multiple roles. However the **Prohibit** permission cannot be overwritten, regardless of content or anything else.

Although you will not normally need to use **Prohibit**, a good example of when you might need this is if an admin wants to prohibit a specific person from starting new discussions in any forum on the whole site. In this case they can create a role with that capability set to **Prohibit** and then assign it to that user in the site context.

Another example would be if you may have a role called **Trainer** set up to allow trainers to do certain things (and not others), once this role exists you can assign it to someone in a course to make them a **Tra iner** for that course. You could also assign the role to a user in the course category to make them a **Train er** for all the courses under that category. The role could also be assigned to a user just in a single forum, giving that user those capabilities just in that forum.

Check system permissions

The check permissions feature provides a method to view the capabilities for a selected user based on their role assignments. These capabilities determine whether or not the selected user is allowed to perform associated tasks within the system or course.

This can be done by going to *Site administration* > *Users* > *Permissions* > *Check system permissions* fro m the **Administration** block:

1. Enter the user's name into the **Search** field and press **Enter**.
2. Select the correct user from the list.
3. Click **Show this user's permissions**.
4. A list of all permissions for the selected user is displayed.

Use the filter to search the permissions list.

Capabilities

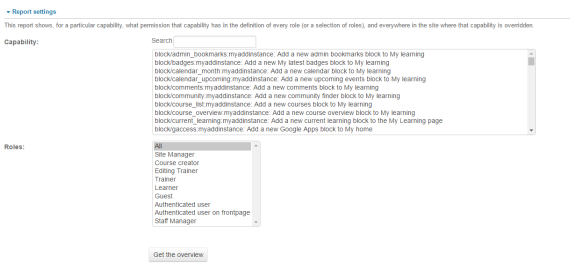
Within Totara capabilities are used to define what a particular role can do in the system. For example the capability **Grade assignment** (also presented as **mod/assign:grade**) is allowed for the Site Manager, Editing Trainer, and Trainer roles at the System level. This means that anyone holding those roles can assign grades on any course they have access to within the system. If this capability was removed from the Trainer role then anyone who was assigned that role would no longer be able to grade assignments. Conversely, if you wish to allow another role, such as Course Creator, to be able to grade assignment then this can be done by editing that role and giving it the **Grade assignment** (**mod/assign:grade**) capability.

Capability overview report

A Site Administrator can generate a capability overview report in *Site administration* > *Users* > *Permissions* > *Capability report.*

The report allows the administrator to select a capability and one or more roles. The report shows the role and its permission level for that capability. The report also shows if that capability was overridden for the role anywhere in the site.

For example, it might show the **gradereport:userview** capability for a Learner role is set at the system level as **Allow** (as is default) and for the Guest role it has been overridden to **Prohibit**.



Managing roles

After looking at Permissions and Capabilities in more detail we can now move on to look at how you can manage roles within Totara. This includes editing existing roles (perhaps to add or remove capabilities) and creating brand new, which should then be tested before they are assigned to any users. Testing new roles is important because sometimes capabilities can have different effects depending on which context levels they are assigned at. Therefore, it is also best to test new roles to make sure they have the intended capabilities and there are no unseen side-effects.

Edit a role

1. Select *Site administration* > *Users* > *Permissions* > *Define roles.*
2. Click the **Edit** icon opposite the role you want to edit.
3. On the **Edit roles** page, change permissions as required.
4. Click the **Save changes** button.

In some circumstances it may be easier to create a new role rather than editing an existing one.

> Role short name is a low level role identifier in which only ASCII alphanumeric characters are allowed.
>
> Do not change short names of standard roles as standard short names are used in some activity processes.

Add a new role

1. Select *Site administration* > *Users* > *Permissions* > *Define roles.*
2. Click **Add a new role** on the **Manage Roles** page.
3. On the **Add a new role** page, give the role a name.
4. Give the role a meaningful short name, the short name is necessary for Totara plugins when they refer to the system roles.
5. Give the role a description (optional).
6. You can base a new role on the permissions set for an existing role, so that you do not start from scratch. Select from the **Legacy role type** option to do this.
7. Set the required permissions.
8. Click **Add a new role** to save your new role.

Test the new role

1. Create a test user and assign the new role to them.
2. Either log out as the administrator and then log in as the test user, or use a different browser to log in as the test user. Role changes only take effect when the user next logs in.

Roles in multiple languages

A role must have a name, if you need to name the role for multiple languages you can use multilang syntax, for example:

```
<span class="multilang" lang="en">Trainer</span>
<span class="multilang" lang="es_es">Manager</span>
```

If you do this make sure the **Multi-language content** filter is enabled on your installation.

Allow role assignment

The **Allow role assignments** tab allows you to define the role a user can assign to another user based on their assigned role.
Using the grid you can allow people who have the roles on the left side to assign some of the column roles to other people.

1. Select *Site administration* > *Users* > *Permissions* > *Define roles*.
2. Click the **Allow role assignments** tab.
3. Find the role you wish to set role assignment permissions for.
4. Click the check box for the roles they are allowed to assign.
5. Click **Save changes**.

Allow role overrides

The **Allow role overrides** tab allows you to define which roles can be overridden by a specific role.

Using the grid you can allow people who have the roles on the left hand side to set overrides for other system roles.

> ⚠ These settings only apply to users who have either the capability **Override permissions for others** (**role:override**) or **Override safe permissions for others** (**role:safeoverride**) allowed.

1. Select *Site administration* > *Users* > *Permissions* > *Define roles*.
2. Click the **Allow role overrides** tab.
3. Find the role you wish to set role override permissions for.
4. Click the check box for the roles they are allowed to set role overrides for.
5. On the **Edit roles** page, change the **Override permissions for others** capability to **Allow**.
6. Click **Save changes**.

Allow role switches

The **Allow role switches** tab allows (or does not allow) users with a specific role to be able to temporarily change their role to another specific role. For example, this might allow users assigned to an Editing Trainer role in a course to see the course from a Learner role perspective. This would be done by clicking 'Learner' in the *Settings* > *Switch role* list.

> ⚠ The selected role must also have the **Switch to other role** (**role:switchroles**) capability to be able to switch.

Unsupported role assignment

Unsupported role assignments are role assignments in contexts that are not marked as suitable for that role, such as course creator in activity or course, or trainer in the user context.

A Site Administrator can check for any unsupported role assignments across the site in *Settings* > *Site administration* > *Users* > *Permissions* > *Unsupported role assignments*.

Role import and export

Sometimes you might want to export or import a role into your system. This could be because you are transferring roles between systems or as a way of backing up the role.

Export role definition to file

To export role definition:

1. Go to *Administration* > *Site administration* > *Users* > *Permissions* > *Define roles*.
2. Click on a role name.
3. Click **Export** button.
4. XML file containing definition of the role is downloaded to your computer.

The definition file includes following data:

- Role name and description.
- Allowed context levels.
- Allow settings for role assignments, overrides, and role switching.
- List of permissions at the system level.

Create new role (import) from definition

To create new role (to import a previously exported role definition):

1. Go to *Administration* > *Site administration* > *Users* > *Permissions* > *Define roles*.
2. Click **Add a new role** button.
3. Upload preset.
4. Click **Continue**.
5. Review new role and scroll down and click **Create this role**.

Reset existing role to definition

To reset role:

1. Go to *Administration* > *Site administration* > *Users* > *Permissions* > *Define roles*.
2. Click on a role name.
3. Click **Reset** button.
4. Upload preset.
5. Select required reset options.

6. Click **Continue**.
7. Review changes of role definition and scroll down and click **Save changes**.

Risks

There are certain risks associated with some capabilities, below is a list of the risks and why you should consider them plus any advice on how to proceed.

Risk	Description
Configuration	You should be aware the some capabilities can allow the holder to change site configurations and behaviours. These are only intended to be allocated to the **Site administrator** and **Manager** roles.
XSS (Cross-Site Scripting)	Certain capabilities could be misused to perform Cross-Site Scripting attacks, such as those capabilities that allow users to post non-checked files and HTML with Javascript. See XSS trusted users for more about how to protect against these attacks. These capabilities are only recommended for **Site administrators** and **Trainers**.
Privacy	Some roles allow access to other users private information, such as non-public profile information. Therefore these capabilities should only be given to **Site administrators** and **Trainers**.
Spam	Some capabilities allow users to add content to the site, such as forum posts, so you should consider whether these could be misused by spammers and only allocate these capabilities where they are needed.
Risks for predefined roles	Certain roles have specific restrictions on them, as listed below: ▪ **Guest:** Only capabilities without any risks are allowed. ▪ **Learner:** Certain capabilities with spam risks are allowed. ▪ **Trainer:** Certain capabilities with XSS and privacy risks are allowed. ▪ **Administrator:** All capabilities are allowed.

Learn more and try it for yourself in the Site-level user management course on the Totara Academy.