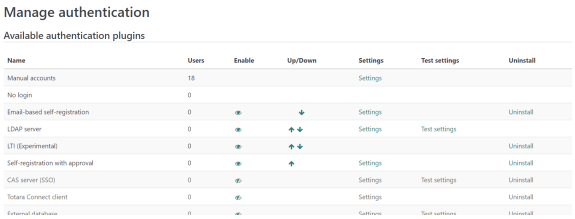
Authentication

Authentication is the process which allows a user to log in to your Totara Learn site.

There are a variety of methods available for user authentication in Totara and any number of available methods may be employed.

Select the method that fits your situation the best. Once you have set up your authentication and set up the courses you can then enrol learners into the courses.



Setting the authentication method

1. Select *Site Administration* > *Plugins* > *Authentication* > *Manage Authentication.*
2. Click **Manage authentications** to set your authentication method.
3. Click the **Show/hide** icon to enable or disable the authentication plugin(s), multiple authentication plugins can be enabled.
4. Use the up/down arrows to change the order of the plugins. Ensure the plugin that handles most of the authentications is at the top of the list.
5. Click **Settings** next to an authentication plugin to configure the plugin properties.
6. Click **Save changes** to save your options.

If you have courses with guest access, set the **Guest login** button to show.

Authentication methods

Authentication methods (also known as authentication plugins) include:

Plugin	Description
Manual accounts	Accounts created manually by an administrator.
No login	Suspends user account.
Email-based self-registration	Enables users to create their own accounts. Read more below.
Self-registration with approval	Enables users to create their own accounts, but prevents them joining the site until they are approved. Read more below.
CAS server (SSO)	Account details are located on an external CAS server.
External database	Account details are located on an external database.
FirstClass server	Account details are located on an external FirstClass server.
IMAP server	Account details are located on an external IMAP server.
LDAP server	Account details are located on an external LDAP server.
MNet authentication	Separate Totara sites can connect and authenticate users.
NNTP server	Account details are located on an external NNTP server.
No authentication	For testing purposes only.
PAM (Pluggable Authentication Modules)	Account details come from the operating system Totara is running on, via PAM (can only be used Linux/Unix).
POP3 server	Account details are located on an external POP3 server.
RADIUS server	Account details are located on an external RADIUS server.

On this page

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.

Shibboleth	Account details are located on an external Shibboleth server.
Web services authentication	Accounts used exclusively by web service clients.

Authentication methods settings

There are a number of settings an authentication method may have, including:

- **Lock user field:** You can lock user profile fields. This is useful for sites where the user profile data is maintained by the administrators manually by editing user records or uploading using the **Upload users** facility.

If you are locking fields that are required by Totara, make sure that you provide that data when creating user accounts or the accounts will be unusable. Consider setting the lock mode to **Unlocked if empty** to avoid this problem.

- **Allow job assignment fields:** The selected Position, Organisation and Manager fields will be available for users when they sign-up

Security risk: Please be aware that while this option is enabled, information about positions, organisation or managers will be public.

- **Password expiry:** Set the length of time the password is valid for and the number of days before the password expiry that a notification is created.

Email-based self-registration

If you have chosen **Email-based self-registration** and wish potential users to be able to create their own accounts, select **Email-based self-registration** from the self registration dropdown menu in the common settings section. Potential users will then be presented with a **Create new account** button on the login page.

The **Email-based self-registration** authentication plugin must be enabled to allow users who previously self-registered via this plugin, to log in with that plugin. Selecting **Email-based self-registration** as the self registration method allows potential users to self register.

Self-registration with approval

The plugin **Self-registration with approval** is slightly different from the **Email-based self-registration** a s it requires a Site administrator or another user with the capability **auth/approved:approve** to approve the registration request before the user is added to the site.

The user registers in the same way as with the **Email-based self-registration** method and gets an email to confirm their email address. The Site administrator (or another user with the capability listed above) can then go to *Site administration* > *Plugins* > *Authentication* > *Self-registration with approval* > *Pending requests* to either approve or reject the user's request. Once this is done, the user will get an email to let them know whether or not they've been approved.

Authentication types

Internal authentication

This type of authentication is used when Totara stores users' passwords and other details in the local Totara database. Authentication plugins such as manual and email are indicated as internal authentication.

External authentication

Other authentication plugins (such as: LDAP or POP3) are indicated as external authentication. With this type of authentication, users' details are not required to be stored in the local Totara database and a user's password field is labelled as 'not cached'.

Multi-authentication

Multi-authentication is supported. Each authentication plugin may be used to find a username/password match. Once found, a user is logged in and alternative plugins are not used. Therefore the plugin which handles the most logins should be moved to the top of the page to ensure minimal load is put on authentication servers.

Common settings

User deletion

Keep username, email, and id number: A deleted user profile fields can be reactivated, their other data will be deleted including but not limited to:

- Appraisals where the user is in the learner role
- Grades
- Tags
- Roles
- Preferences
- User custom fields
- Private keys
- Customised pages
- Facetoface signups
- Feedback360 assignments and responses
- Position assignments
- Programs & certifications
- Goals
- Evidence items
- Scheduled reports
- Reminders
- Course and program enrolments
- Positions manager, appraiser, and temp manager positions will be unassigned
- Audience assignments
- Groups membership
- Messages will be marked as read

Full deletion: This is the default setting.

If a user was deleted with the keep username, email, and id number setting then they will only be able to be fully deleted manually not through the HR import process.

If you want to recover a users record of learning then **Suspend** rather than **Delete** the user.

Self registration

If you want users' to be able to create their own user accounts, i.e. self register, then select **Email-based self-registration** (or any other enabled plugin which can support self registration, like LDAP) from the dropdown menu.

Enabling self registration results in the possibility of spammers creating accounts in order to use forum posts, blog entries etc. for spam. This risk can be minimised by limiting self registration to particular email domains using the **Allowed email domains** option. Alternatively, self registration may be enabled for a short period of time to allow users to create accounts and then later disabled.

Allow login via email

Allow users to use both username and their email address (if unique) for site login.

Allow accounts with same email

If enabled, more than one user account can share the same email address.

This may result in security or privacy issues, for example with the password change confirmation email.

Prevent account creation when authenticating

When a user authenticates, an account on the site is automatically created if it doesn't yet exist. If an external database, such as LDAP, is used for authentication, but you wish to restrict access to the site to users with an existing account only, then this option should be enabled. New accounts will need to be created manually or via the upload users feature. Note that this setting doesn't apply to MNet authentication.

Autofocus login page form

Enabling this option improves usability of the login page so you don't need to navigate to username filed but automatically focusing fields may be considered an accessibility issue.

Guest login button

You can hide or show the guest login button on the login page. Hiding the guest login button disables guest access to your Totara site.

Any user logged in to the system can view any course that allows guest access without enrolling on the course.

Limit concurrent logins

If enabled the number of concurrent browser logins for each user is restricted.

The oldest session is terminated after reaching the limit, please note that users may lose all unsaved work. This setting is not compatible with single sign-on (SSO) authentication plugins.

Alternate login URL

This should be used with care, since a mistake in the URL or on the actual login page can lock you out of your site. If there is a problem, you can remove the entry from your database (table mdl_config) using, e. g., phpmyadmin for mysql.

Forgotten password URL

If your lost password handling is performed entirely outside of Totara; for example, only by a help desk, you can set the URL of that service here. Anybody pressing a **lost password** link in Totara will be redirected to this URL. Custom instructions for logging in can also be created.

This will disable all of Totara's lost password recovery options regardless of authentication method(s) in use!

Allowed and denied email domains

Authentication may be restricted to particular email domains when using Email-based self-registration so that, for example, only learners with an organisation domain email can log in.

Restrict domains when changing email

Enables verification of changed email addresses using allowed and denied email domains settings. If this setting is disabled the domains are enforced only when creating new users.

ReCAPTCHA keys

If ReCAPTCHA has been enabled in the user signup form then a Public (Site) and Private key are required to be entered. The keys are generated by http://www.google.com/recaptcha.

Please note that as of 31 March 2018 reCAPTCHA v1 will no longer work. This means you will need to ensure you have upgraded to the latest minor release for your Totara Learn version and then update your keys so that you can use v2. You can read more on the reCAPTCHA FAQs.

Single sign-on

There are two ways to manage single sign-on in Totara:

- **Totara Connect:** See more on the dedicated Totara Connect page.
- **CAS server (SSO):** See more below.

To determine the best method for your organisation it depends if you are trying to connect multiple Totara sites (Totara Connect) or if you are trying to connect Totara with external services (CAS).

CAS server SSO

To set up CAS follow these steps:

1. Select *Site Administration > Plugins > Authentication > Manage Authentication.*
2. Click the show icon ( ) alongside the **CAS server (SSO)** authentication method.
3. Click **Settings** next to **CAS server (SSO)** to configure the plugin setting.
4. Click **Save changes** to save your options.

As CAS is an external open source solution you can read more about how CAS works on their website.