

# Authentication

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

## Manage authentication

### Available authentication plugins

Name	Users	Enable	Up/Down	Settings	Test settings	Uninstall
Manual accounts	18			Settings		
No login	0					
Email-based self-registration	0		↓	Settings		Uninstall
LDAP server	0		↑ ↓	Settings	Test settings	
LTI (Experimental)	0		↑ ↓			Uninstall
Self-registration with approval	0		↑	Settings		Uninstall
CAS server (SSO)	0			Settings	Test settings	Uninstall
Totara Connect client	0			Settings		Uninstall
External database	0			Settings	Test settings	Uninstall

Authentication is configured separately for the [Totara Mobile app](#). Please note that different options are available for [mobile authentication](#).

## Setting the authentication method

1. Select *Site Administration > Plugins > Authentication > Manage Authentication*.
2. Select **Manage authentications** to set your authentication method.
3. Select 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. Select **Settings** next to an authentication plugin to configure the plugin properties.
6. Select **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. See more on the <a href="#">Email-based self-registration</a> Help page.
LDAP server	Account details are located on an external LDAP server. See the <a href="#">LDAP server</a> Help page for more.
LTI (Experimental)	Use this with the <a href="#">Publish as LTI tool enrolment plugin</a> to allow remote users to access selected courses and activities.
Self-registration with approval	Enables users to create their own accounts, but prevents them joining the site until they are approved. See <a href="#">Self-registration with approval</a> Help page for more.
CAS server (SSO)	Account details are located on an external CAS server.
Totara Connect client	Automatic single sign-on via Totara Connect servers.
External database	Account details are located on an external database.

<b>MNet authentication</b>	Separate Totara sites can connect and authenticate users. The <a href="#">MNet</a> authentication plugin has been deprecated in Totara 13.
<b>OAuth 2</b>	Allows users to login via a Microsoft, Google, or Facebook account. See more on the <a href="#">OAuth 2</a> Help page.
<b>Shibboleth</b>	Account details are located on an external Shibboleth server.
<b>Web services authentication</b>	Accounts used exclusively by web service clients.

## Frequently found settings

There are a number of settings that an authentication method may have, some of the more common ones are listed below.

Setting	Description	Notes
<b>Lock user field</b>	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 <b>Upload users</b> 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 <b>Unlocked if empty</b> to avoid this problem.
<b>Allow job assignment fields</b>	The selected Position, Organisation and Manager fields will be available for users when they sign-up.	<b>Security risk:</b> Please be aware that while this option is enabled, information about positions, organisation or managers will be public.
<b>Password expiry</b>	Set the length of time the password is valid for and the number of days before the password expiry that a notification is created.	-

## Authentication types

Authentication type	Description
<b>Internal authentication</b>	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.
<b>External authentication</b>	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'.
<b>Multi-authentication</b>	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.

## Site settings

There are a number of settings you can configure in the *Plugins > Authentication > Manage authentication* area under **Common settings**.

Setting	Description	Notes
<b>User deletion</b>	<p>This setting allows you to determine what happens to a user account if it is deleted. Select from the following options:</p> <ul style="list-style-type: none"> <li>Full with random surname</li> <li>Full (legacy)</li> <li>Keep username, email and ID number (legacy)</li> </ul> <p>If you choose <b>Keep username, email, and id number</b> then deleted user profile fields can be reactivated however their other data will be deleted including but not limited to; appraisals where the user is in the learner role, grades, and roles.</p>	<p>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.</p> <p>If you want to recover a users record of learning then <b>Suspend</b> rather than <b>Delete</b> the user.</p>

<b>Self registration</b>	If you want users' to be able to create their own user accounts, i.e. self register, then select <b>Email-based self-registration</b> (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 <b>Allowed email domains</b> option. Alternatively, self registration may be enabled for a short period of time to allow users to create accounts and then later disabled.
<b>Allow login via email</b>	Allow users to use both username and their email address (if unique) for site login.	-
<b>Allow accounts with same email</b>	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.
<b>Prevent account creation when authenticating</b>	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.	-
<b>Autofocus login page form</b>	Enabling this option improves usability of the login page so you don't need to navigate to username field but automatically focusing fields may be considered an accessibility issue.	-
<b>Guest login button</b>	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.
<b>Limit concurrent logins</b>	If enabled the number of concurrent browser logins for each user is restricted.	-
<b>Alternate login URL</b>	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 using, e.g., phpmyadmin for MYSQL.	-
<b>Forgotten password URL</b>	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 <b>lost password</b> 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.
<b>Instructions</b>	Enter custom login instructions that will be displayed on the login page. Leaving this blank will display the default instructions.	-
<b>Allowed email domains</b>	A space separated list of allowed email domains, e.g. @totaralearning.com @totara.com	-
<b>Denied email domains</b>	A space separated list of email domains that are not allowed to be registered, e.g. @hotmail.com @gmail.com	-
<b>Restrict domains when changing email</b>	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.	-
<b>reCAPTCHA keys</b>	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 <a href="http://www.google.com/recaptcha">http://www.google.com/recaptcha</a>	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 version and then update your keys so that you can use v2. You can read more on the <a href="#">reCAPTCHA FAQs</a> .

## Single sign-on


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

- **Totara Connect:** See more on the [dedicated Totara Connect](#) page
- **CAS server (SSO):** See more below
- **OAuth 2:** See more on the [dedicated OAuth 2](#) page

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. Select the show icon (  ) alongside the **CAS server (SSO)** authentication method.
3. Select **Settings** next to **CAS server (SSO)** to configure the plugin setting.
4. Select **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](#).

## Totara Academy



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