Security

The Security area can be accessed via the **Administration** block within the **Site administration** menu. It contains a range of security settings for the site, server, and users. It is recommended you check through all options with your Systems/Network administrator before launching your site and discuss any changes with the relevant stakeholders before implementing.

On this page

Related pages

Security advice

It is difficult to offer explicit security advice, as the requirements will vary slightly based on your own organisational preferences and policies. Instead, the below advice highlights recommended best practice and considerations.

Server setup

When considering the server setup for your Totara Learn site the focus should be around balance, deciding how locked down you want the server to be, and how this might impact the ability for external connections. This will ultimately be your decision, but we recommend the following:

- Using SSL.
- Proper setup of dataroot permissions.
- DMZ / secure network setup.

Dataroot permissions

If you follow the recommendation for proper setup of dataroot permissions, there are two main requirements:

1. The dataroot should not be accessible via the web. We recommend that the dataroot be located outside of the web directory (wwwroot).
2. The dataroot ownership and permissions should be configured so they are accessible to the web server process. For maximum security the files should not be read or writable to other users.

Demilitarised zone (DMZ)

For DMZ / secure network setup the exact configuration will depend on your organisation's requirements, however it is important that internal firewalls are configured so that sensitive internal resources cannot be accessed from the machine that is hosting the Totara Learn site (if the Totara Learn site has less strict access control than the sensitive internal systems).

It is important to note that, even without the DMZ, access to the internal system will still be restricted to users who have a Totara Learn login. However given you can enable self registration, that could mean anyone.

As noted above, a lot of these recommendations will be affected by both external requirements (such as compliance) and/or internal company policy. For example, some companies will have their database in a DMZ (demilitarised zone) to avoid DMZ to trusted network interactions. Whereas others will put it on a private sub-network and then pin hole the firewall to allow access. Some will put the entire product in a private sub-network either with or without a VPN for access. Other companies may even create an application specific DMZ data sub-net for the data access of the product thereby giving the best of both worlds, although this is more typical in cloud environments.

For more server security best practice advice you can see the Open Web Application Security Project (or OWASP for short).

Using HTTPS

If you are currently running your site using HTTP then you may wish to transition to HTTPS to ensure extra security for your site. Before doing this it is important to note that any content you have (excluding links) that currently uses HTTP will no longer be able to be embedded once you switch to HTTPS, therefore you will need to check the content can be moved to HTTPS or find new content (you could also change to using links for any HTTP content you need). Once you are happy that your content can manage the change follow these steps:

1. You will need to obtain an SSL certificate from a certificate authority such as Let's Encrypt, which is a free services (other services may charge).
2. After getting the certificate you will then need to enable SSL on your server and apply the certificate. The documentation for your server should explain this process as it can vary.
3. Now you can can setup the Totara Learn site by changing the **$CFGwwwroot** value in your **config.php** file from **http://** to **https://** e.g.

```
$CFG->sslproxy = true;

$CFG->wwwroot = 'https://example.com';
```

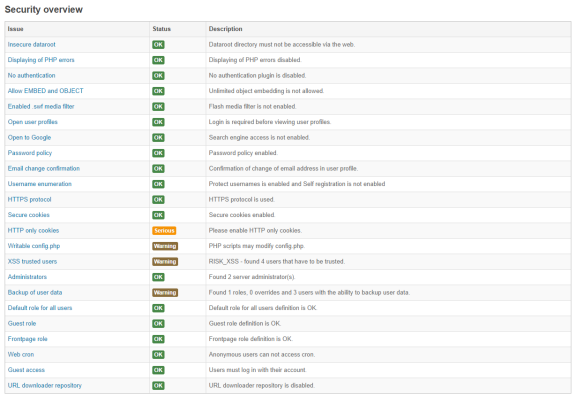
Once this is done you will then need to update any existing content that is using HTTP as this will no longer work (links are fine, other content will need to use HTTPS as well).

Site configuration

Once you have made sure you are happy with the security of the server setup, you should also configure your Totara Learn site to ensure it is secure. Again, a lot of this will depend on the policies and end goals of your organisation. Consider the following carefully:

- Review the security settings to make sure they are appropriate for your organisation.
- Check your sites **Security overview** report for guidance on specific areas to consider/review.

You can get to this page by following the path *Site administration > Reports > Security overview.*



Security overview

Issue	Status	Description
Insecure dataroot	OK	Dataroot directory must not be accessible via the web.
Displaying of PHP errors	OK	Displaying of PHP errors disabled.
No authentication	OK	No authentication plugin is disabled.
Allow EMBED and OBJECT	OK	Unlimited object embedding is not allowed.
Enabled .swf media filter	OK	Flash media filter is not enabled.
Open user profiles	OK	Login is required before viewing user profiles.
Open to Google	OK	Search engine access is not enabled.
Password policy	OK	Password policy enabled.
Email change confirmation	OK	Confirmation of change of email address in user profile.
Username enumeration	OK	Protect usernames is enabled and Self registration is not enabled
HTTPS protocol	OK	HTTPS protocol is used.
Secure cookies	OK	Secure cookies enabled.
HTTP only cookies	Serious	Please enable HTTP only cookies.
Writable config.php	Warning	PHP scripts may modify config.php.
XSS trusted users	Warning	RISK_XSS - found 4 users that have to be trusted.
Administrators	OK	Found 2 server administrator(s).
Backup of user data	Warning	Found 1 roles, 0 overrides and 3 users with the ability to backup user data.
Default role for all users	OK	Default role for all users definition is OK.
Guest role	OK	Guest role definition is OK.
Frontpage role	OK	Frontpage role definition is OK.
Web cron	OK	Anonymous users can not access cron.
Guest access	OK	Users must log in with their account.
URL downloader repository	OK	URL downloader repository is disabled.

You can also look in more detail at the advice and guidance on the specific features of security in the documentation. Please use the Related pages menu to the right to navigate to relevant pages for more advice and guidance relating to security.