admin/setting/httpsecurity

- Secure cookies only
- cURL blocked hosts list
- cURL allowed ports list
- See also

- In Moodle 3.4 onwards, the setting 'Use HTTPS for logins' (loginhttps) has been removed.
- There is a HTTPS conversion tool for converting embedded content to HTTPS.

- 1 Secure cookies only
- 2 cURL blocked hosts list
- 3 cURL allowed ports list
- 4 See also

Secure cookies only

It is recommended to use secure cookies only when serving over SSL. When not serving over SSL, the setting is ignored. In Moodle 3.1.2 onwards, the 'Secure cookies only' default setting is on.

cURL blocked hosts list

This allows you to block Moodle's cURL implementation from accessing the specified hosts, wherever it is used to fetch content (such as by the URL downloader in the file picker). Generally it is recommended that as a minimum this is configured to prevent access to any internal network resources. The following is an example list of hosts which can be configured, which prevents access to various versions of "localhost", as well as an address commonly used by AWS and some other cloud providers to provide meta data about the server instance (169.254.169.254):

```
127.0.0.0/8
192.168.0.0/16
10.0.0.0/8
```

```
172.16.0.0/12
0.0.0.0
localhost
169.254.169.254
0000::1
```

Note: In addition to configuring this at the application level via this setting, it is also recommended that sufficient firewall/network security measures are in place, including restricting access to internal network endpoints to those users/services that require them.

cURL allowed ports list

This allows you to restrict Moodle's cURL implementation to only access the specified list of port numbers, wherever it is used to fetch content (such as by the URL downloader in the file picker). Generally it is recommended that this is configured to only allow standard web ports, as follows:

```
80
443
```

In future, some logical default values such as those above will be configured automatically for new Moodle sites. See MDL-56873 for more details.

Note: In addition to configuring this at the application level via this setting, it is also recommended that sufficient firewall/network security measures are in place, including restricting access to open ports on the internal network to those users/services that require them.

See also

- MDL-55662 for removing the secure cookies only setting

Source: docs.moodle.org/503/en/admin/setting/httpsecurity — MoodleDocs (GPL) · Imported 2026-11-10.

□□□ #3
□ cocobook-sync □□□ 2026-11-10 15:42:27 UTC
□ cocobook-sync □□□ 2026-11-11 00:17:42 UTC