KNOWLEDGE BASE ARTICLE

Moodle MCP (Model Context Protocol)

Moodle MCP is a plugin that connects your Moodle site to EssingtonITS AI assistant or generic AI MCP aware models. Once connected, you can ask the AI questions about your site in plain language and the AI will look up the answers directly from Moodle in real time. You can also ask it to carry out administrative tasks such as enrolling users, creating courses, or awarding badges, all from a single conversation.

AUTHOR
Paul Flanders

PUBLISHED
7 May 2026

DOCUMENT
InfoHub — Knowledge, news, and updates from EssingtonITS

Moodle MCP (Model Context Protocol)

Paul Flanders · 7 May 2026

Every action the AI takes is recorded in a built-in audit log, sensitive personal data is automatically masked, and destructive actions always require an explicit confirmation before anything is changed.

What this product is for

Managing a Moodle site normally means clicking through many different admin screens to find information or carry out tasks. Moodle MCP removes that friction. Instead of navigating menus, you ask a question or describe what you need, and the AI handles the lookup or the action on your behalf.

Common scenarios include:

- Quickly checking which learners in a course have not yet completed a quiz
- Diagnosing a site problem without trawling through log files manually
- Enrolling a group of users into a course in one step
- Getting a completion and grade overview for a course without exporting a report
- Auditing user accounts, roles, or cohort memberships at a glance

Main features

- **Natural language access to Moodle data.** Ask the AI about courses, users, grades, completions, badges, competencies, groups, cohorts, roles, and more. No SQL knowledge required.
- **Administrative write actions.** Create and update users, enrol learners, manage cohorts and groups, create and clone courses, override completions and grades,

award badges, and manage competency frameworks — all through conversation.

- **Bulk operations.** Carry out actions on multiple users or courses in a single step, with per-item results reported back.
- **Pre-built diagnostic workflows.** Ask the AI to run a full site health check, investigate a login problem, diagnose a cron failure, or audit course completions using guided prompts.
- **Append-only audit log.** Every request — successful or not — is recorded with the user, tool used, parameters, result, and execution time. The log cannot be modified or deleted by any tool.
- **Automatic redaction.** Email addresses, phone numbers, IP addresses, and ID numbers are masked in all responses by default, so sensitive personal data is not unnecessarily exposed.
- **Rate limiting.** Requests are limited per token to prevent overload, with separate limits for calls per minute and data volume.
- **Fine-grained permissions.** Each group of tools has its own Moodle capability, so you can control exactly what the AI service account is allowed to access or change.
- **Write safety controls.** Write access can be disabled entirely from one setting. Irreversible actions — such as deleting a course or a user — require an explicit confirmation and cannot be triggered accidentally.
- **No external dependencies.** The plugin is self-contained. There is no external server, no Node.js runtime, and nothing else to install or maintain.

AI Assistant + MCP Integration

When paired with the EITS Moodle AI Assistant, the AI Assistant becomes fully course-aware, giving learners access to intelligent, context-sensitive support directly within Moodle.

Unlike generic AI tools, the Assistant can understand the exact course, module, activity, and learning content the student is currently viewing. This allows learners to ask highly specific questions about the material they are studying and receive relevant, targeted guidance in real time.

The Assistant can:

- Explain difficult concepts in the context of the current lesson
- Answer questions about the exact content being viewed
- Provide clarification without requiring the learner to leave Moodle
- Guide students through activities, resources, and modules
- Deliver subject-specific assistance tailored to the course content
- Reduce confusion and improve learner engagement
- Act as an always-available subject matter expert

Because the Assistant has visibility of the learner’s current course context, responses are significantly more accurate and meaningful than traditional standalone AI chat systems.

This creates a far more personalised and interactive learning experience, helping students remain focused, supported, and engaged throughout their learning journey.

EssingtonITS AI Assistant

Common tasks

Check site health

Ask the AI to run a site health check. It will check the Moodle version, cron status, any failed scheduled tasks, recent PHP errors, and recent failed login attempts, then give you a summary.

Example: "*Run a full site health check.*"

Find out why a user cannot log in

Give the AI the username and ask it to investigate. It will check the account status, authentication method, recent login events, and error log entries for that user.

Example: "*Can you look into why john.smith can't log in?*"

Check course completion

Ask for a completion overview or a per-user breakdown for any course.

Example: "*How many people have completed the Health and Safety Induction course, and who hasn't started yet?*"

Enrol users

Ask the AI to enrol one or more users into a course. You can also enrol an entire cohort at once.

Example: "*Enrol everyone in the New Starters cohort into the Induction course.*"

Create a user account

Ask the AI to create a new user. It will confirm what it is about to do before making any change.

Example: "*Create a new user account for Jane Doe with the username janedoe.*"

Clone a course

Ask the AI to clone an existing course into a new one. It will guide you through choosing a name, category, and what content to include.

Example: "*Clone the Fire Safety course and create a new version for the Warehouse team.*"

Check the audit log

Go to **Site admin → Local plugins → MCP Audit Log** to see a record of every AI action, filterable by tool, user, success or failure, and date range.

Things to know

Write access is off by default

When the plugin is first installed, the AI can only read data — it cannot create, update, or delete anything. To allow write actions, go to **Site admin → Local plugins → Moodle MCP** and enable **Enable write operations**.

Destructive actions require confirmation

Actions that cannot be undone such as deleting a user or a course require an explicit confirmation parameter. The AI cannot trigger these accidentally by misreading an ambiguous instruction. You will always be informed before anything irreversible happens.

Sensitive configuration values are always blocked

The AI cannot read or change passwords, secret keys, tokens, SMTP credentials, or any other sensitive configuration values. This restriction is built into the plugin and cannot be overridden through settings.

Personal data is masked by default

When redaction is enabled (the default), the AI receives masked versions of personal data:

- Email addresses show only the domain part (for example, `j****@example.com`)
- IP addresses are shortened to the first three segments
- Phone numbers show only the last two digits
- ID numbers are replaced with a short code

Users with the Moodle capability to view full user identity receive unmasked values.

Rate limits apply

By default, each token is limited to 120 requests per minute and 20 MB of response data per minute. Write actions count as 2 units. If a limit is exceeded, the AI will receive an error and

will tell you. Limits can be adjusted in the plugin settings.

Each tool group can be switched on or off

In the plugin settings, you can disable individual groups of tools for example, you can allow course lookups but prevent the AI from accessing grade data. Disabled tool groups are hidden from the AI entirely.

The audit log is permanent

Every tool call is written to the audit log and cannot be modified or deleted by any AI action. Log entries are automatically purged after a configurable retention period (default: 365 days).

Bulk operations have hard limits

Bulk actions such as enrolling many users at once are capped at a maximum number of items per operation (default: 500 users, 50 courses). These limits are enforced on the server and cannot be bypassed through the AI.

Troubleshooting

The AI cannot connect to Moodle

- Check that **Enable MCP endpoint** is on in the plugin settings.
- Check that web services and the REST protocol are both enabled in Moodle.
- Confirm the token is valid and has not expired — check **Site admin → Server → Web services → Manage tokens**.
- Confirm the service account is listed as an authorised user for the Moodle MCP external service.

The AI connects but cannot see any tools

- Check that the service account has the **Manager** role at system context, or that a custom role has been assigned with at least `local/mcp:use` and the relevant view capabilities.
- Check that the required tool groups are enabled in the plugin settings.

The AI says write operations are not available

Write access is disabled by default. Go to **Site admin → Local plugins → Moodle MCP** and enable **Enable write operations**.

The connection fails with a certificate error (self-signed TLS)

If your Moodle site uses a self-signed or internally-issued security certificate, some AI clients may refuse the connection. For Claude Code's VS Code extension, you will need to add `NODE_TLS_REJECT_UNAUTHORIZED=0` to the environment settings in `~/.claude/settings.json` and set `insecureSkipVerify: true` in the MCP server configuration. Only do this on a trusted internal network. This workaround is not needed if your site uses a publicly trusted certificate.

Requests are being rejected with a rate limit error

The default limit of 120 calls per minute has been reached. Either wait for the window to reset, or go to **Site admin → Local plugins → Moodle MCP → Rate limiting** and increase the limit.

Cron health tools report an error

This plugin requires Moodle 4.1 or later. On older versions, the cron task data structure differs and some cron health fields may not be available.

Frequently asked questions

Can the AI make changes to my Moodle site without me knowing?

Every action the AI takes is recorded in the audit log, which you can view at any time from the admin area. Write access is also disabled by default and must be explicitly enabled. Irreversible actions require an additional confirmation step.

Is my users' personal data sent to the AI?

When redaction is enabled (the default), personal data such as email addresses and phone numbers is masked before being returned to the AI. The AI sees partial values rather than full ones. Full values are only shown when the Moodle user account running the query has the appropriate identity-viewing capability.

Can the AI access passwords or security keys?

No. Any configuration value related to passwords, keys, tokens, or credentials is permanently blocked. This applies both to reading and writing. The restriction is built into the plugin and cannot be changed through the admin interface.

What happens if I disable write operations?

The AI can still read and query all data normally it just cannot create, update, or delete anything. You can re-enable write access at any time from the plugin settings.

Can I limit which parts of Moodle the AI can access?

Yes. In the plugin settings, each area (courses, users, grades, badges, and so on) has its own enable/disable toggle. You can also control access more precisely using Moodle's capability system by assigning a custom role to the service account that only has the specific capabilities you want to grant.

Does the plugin support multiple AI clients at the same time?

Yes. You can mint separate tokens for separate clients. Each token has its own rate limit window and appears independently in the audit log.

Can I restrict which IP addresses the AI can connect from?

Yes. In the plugin settings, under **Rate limiting**, you can enter a list of allowed IP address ranges. Connections from any other address will be refused.

What AI clients are supported?

Any client that supports the MCP Streamable HTTP protocol (version 2025-03-26). Claude Desktop and Claude Code are both supported and tested. Other compatible MCP clients should also work.

Does this plugin store any data on external servers?

No. The plugin is entirely self-hosted within your Moodle installation. It does not transmit data to any third-party service. Communication happens directly between your AI client and your Moodle server.

What Moodle version is required?

Moodle 4.1 or later, running PHP 8.1 or later.

Summary

Moodle MCP brings AI-assisted administration to your Moodle site without replacing any existing workflows or requiring external services. You can look up information, carry out routine tasks, and investigate problems through natural conversation, while every action remains transparent, controlled, and auditable. Read access is available immediately after installation; write access is opt-in and can be scoped precisely to what each service account is permitted to do.