dream-genie.ai

v1.8.0

MCP Server & Client

Complete guide to the Model Context Protocol server and client. Let AI agents manage your WordPress through conversation.

Version v1.8.0 · March 2026

Table of Contents

1 What is MCP?

MCP (Model Context Protocol) is an open standard created by Anthropic that lets AI models interact with external tools and data sources through a standardized interface. Think of it as USB for AI — any AI agent that speaks MCP can connect to any MCP-compatible server.

dream-genie.ai implements **both sides** of MCP:

- **MCP Server** — turns your WordPress site into a tool server that AI agents (Claude, ChatGPT, Cursor) can control
- **MCP Client** — lets your WordPress connect to external MCP servers to pull in data and capabilities

■ **NOTE:** dream-genie.ai is one of the only WordPress plugins that implements MCP. This gives your site a unique capability that AI agents can leverage.

2 MCP Server

The MCP Server exposes your WordPress site as a set of tools that AI agents can call. When enabled, AI assistants like Claude can:

- Read and search your posts, pages, and WooCommerce products
- Create and update content
- Manage users, options, plugins, and site settings
- Query your database directly (with strict safety controls)
- Execute WP-CLI commands
- Manage WooCommerce orders, customers, and inventory

How It Works

1. The plugin exposes a REST API endpoint at `yoursite.com/wp-json/dreamgenie/v1/mcp`
2. AI agents send JSON-RPC requests to this endpoint with an API key header
3. The server validates the key, checks tool permissions, and executes the requested tool
4. Results are returned as structured JSON that the AI can process

3 Available MCP Tools

Core WordPress Tools

Tool	Description	Tier
list_posts	List posts with filters (type, status, category, date, search)	Free
get_post	Get a single post by ID with full content and meta	Free
create_post	Create a new post/page/CPT with title, content, status, meta	Starter
update_post	Update an existing post's fields	Starter
search_content	Full-text search across all post types	Free
list_users	List WordPress users with role filtering	Pro
get_user	Get user details by ID	Free
manage_options	Read/write WordPress options (strict allowlist)	Pro
manage_plugins	List, activate, deactivate plugins	Pro
query_db	Execute read-only SQL queries (6-layer security)	Agency
wp_cli	Execute WP-CLI commands remotely	Agency
get_site_info	Site URL, name, version, theme, active plugins	Free

4 Server Setup

1. Navigate to **dream-genie.ai** → **MCP Server**.
2. Copy your **MCP Endpoint URL**: `https://yoursite.com/wp-json/dreamgenie/v1/mcp`
3. Click **Generate API Key** to create a new key. Give it a descriptive name (e.g., 'Claude Desktop').
4. Copy the API key — it's shown once, then stored encrypted.
5. Configure the key into your AI agent (see chapters 11–12 for specific instructions).
6. Test the connection by asking the AI agent to 'list the 5 most recent posts on my WordPress site.'

API Key Management

- Create multiple keys for different agents or team members
- Each key can have individual tool permission overrides
- Revoke keys instantly — takes effect immediately
- Keys are stored AES-256 encrypted in the database
- Activity log shows which tools each key has called

5 Security

The MCP Server is hardened with multiple security layers:

query_db — 6-Layer Protection

1. **Semicolons blocked** — prevents statement chaining (SQL injection vector #1)
2. **SQL comments stripped** — removes /* */ and -- comment sequences
3. **Keyword matching** — word-boundary regex blocks DROP, ALTER, INSERT, UPDATE, DELETE, TRUNCATE, GRANT
4. **Table allowlist** — only WordPress core tables + plugin tables are queryable
5. **Row limit** — maximum 100 rows per query (prevents data dumps)
6. **Time-based attack prevention** — SLEEP, BENCHMARK, and timing functions blocked

manage_options — Strict Allowlist

Instead of a blocklist (dangerous — misses new sensitive options), manage_options uses a strict allowlist of safe options. Only options explicitly listed can be read or written. Extensible via the `dreamgenie_mcp_allowed_options` filter.

manage_plugins

- Validates plugins exist in the installed list before any action
- Prevents self-deactivation (can't deactivate dream-genie.ai via MCP)
- Logs all plugin changes to the activity log

6 MCP Client

The MCP Client lets your WordPress connect to external MCP servers — pulling in data and capabilities from other services. This is the reverse of the MCP Server.

Use Cases

- Connect to a company's internal MCP server to access CRM data in flows
- Pull real-time inventory data from a warehouse MCP server
- Access specialized AI tools (code analysis, image processing) via MCP
- Chain multiple MCP servers together in a single flow

Adding an External MCP Server

1. Navigate to **dream-genie.ai** → **MCP Client**.
2. Click **Add Server**.
3. Enter the server's **Endpoint URL** and **API Key**.
4. Click **Test Connection** — the plugin queries the server's tool list.
5. Available tools appear in the list. Toggle which tools you want to use.
6. These tools become available as actions in the Flow Builder.

7 WooCommerce MCP Tools

25 WooCommerce-specific tools (available when WooCommerce is active):

Tool	Description
list_products	List/search products with filters (category, status, price range)
get_product	Full product details (price, stock, variations, images, meta)
create_product	Create simple or variable products with all fields
update_product	Update price, stock, description, images, meta
list_orders	List orders with date/status/customer filters
get_order	Full order details (items, totals, shipping, customer, notes)
update_order_status	Change order status (processing → completed, etc.)
add_order_note	Add a note to an order (visible to admin or customer)
list_customers	List customers with filters
get_customer	Customer details, order history, lifetime value
manage_coupons	Create, update, list, delete discount coupons
get_inventory	Stock levels across all products (low stock alerts)
update_stock	Adjust stock quantities (set, increase, decrease)
list_categories	Product category tree with counts
get_revenue	Revenue reports (daily, weekly, monthly, custom range)

■ **TIP:** With these tools, Claude can manage your entire WooCommerce store through conversation: 'Update the price of Blue Widget to $29.99' or 'Show me orders from last week over $100.'

8 Tool Tier Limits

Tier	Tools Available	Access
Free	4 read-only tools	list_posts, get_post, search_content, get_site_info
Starter	6 tools	Free + create_post, update_post
Pro	All except admin	Starter + list_users, manage_options, WooCommerce tools
Agency	All tools	Pro + query_db, wp_cli, manage_plugins

The `list_tools()` method automatically filters available tools based on the license tier. `call_tool()` returns HTTP 403 if a tool is called that exceeds the tier.

9 Custom Tool Extensions

Developers can register custom MCP tools via WordPress hooks:

```
add_filter( 'dreamgenie_mcp_tools', function( $tools ) {
$tools['my_custom_tool'] = [ 'description' => 'Does something custom',
'parameters' => [ 'param1' => 'string' ], 'callback' => 'my_tool_callback', ];
return $tools; });
```

10 Real-World Use Cases

Scenario	How MCP Enables It
Content Management via AI	Ask Claude: 'Publish a draft blog post about Q2 results' → create_post tool
Inventory Monitoring	Ask: 'Which products are low stock?' → get_inventory tool → AI summarizes
Order Management	Ask: 'Mark order #1234 as shipped' → update_order_status tool
Site Audit	Ask: 'List all deactivated plugins' → manage_plugins tool
Data Analysis	Ask: 'What's our revenue trend this quarter?' → get_revenue + query_db tools
Automated Reporting	Flow: weekly cron → query_db → AI summarize → email report

11 Claude Desktop

To connect Claude Desktop to your WordPress MCP Server:

1. Open Claude Desktop → Settings → Developer → MCP Servers.
2. Click **Add Server**.
3. Enter your MCP endpoint URL and API key from the MCP Server page.
4. Claude will discover available tools automatically.
5. Start a conversation: 'List my 10 most recent blog posts.'

12 Cursor & VS Code

For Cursor IDE or VS Code with Copilot:

1. Open your project's `.cursor/mcp.json` or equivalent config.
2. Add your WordPress MCP server configuration with endpoint URL and API key.
3. Restart the IDE. MCP tools appear in the AI assistant's tool list.
4. Use in conversations: 'Create a new page on my WordPress site with the deployment notes.'

13 Troubleshooting

Symptom	Cause	Fix
'Authentication failed'	Wrong API key or key revoked	Check key in MCP Server page, generate new if needed
'Tool not found'	Tool not available at your tier	Upgrade your license to access more tools
'Permission denied' on query_db	Agency-only tool	Only Agency licenses can use query_db
Slow tool responses	Complex query or slow server	Optimize queries, check server performance
WooCommerce tools missing	WooCommerce not active	Install and activate WooCommerce
Connection timeout from Claude	Firewall blocking or SSL issue	Check server firewall rules, ensure valid SSL cert