AI Gateway

Administrator Guide

The complete reference for security, providers, tokens, tools, and integration

v1.8.0 | speak2web | 2026 | speak2web.com

ABOUT THIS GUIDE

This guide covers every admin page, setting, provider, and maintenance task in AI Gateway v1.8.0. It is written for the WordPress administrator running the plugin on a live site, and for plugin developers integrating their own capabilities into the Gateway. If you are installing AI Gateway for the first time, start with the Quick Start Guide — it gets you to a working authenticated endpoint in seven steps — and come back here for the full picture.

New in v1.8.0: a WooCommerce provider (Section 10), Calendly and Acuity Scheduling providers (Section 12), a standard MCP server endpoint that external clients connect to natively (Section 6), anonymous LatePoint booking (Section 11), and MCP-safe tool names (Section 6.3). Appendix D has the full list.

Section	What it covers
1. Requirements & Installation	Prerequisites, upload, activation, what activation creates
2. The Admin Interface	Three subpages, eight settings tabs, where each setting lives
3. Four-Tier Security Model	The authorization spine — Tier 1 / 2 / 3, and why Tier 4 does not exist
4. Authentication	HMAC Bearer tokens — issue, verify, refresh, revoke, lifetime
5. REST Endpoints	Every route, request shape, and response code
6. Standard MCP Server Endpoint	JSON-RPC 2.0 over Streamable HTTP for external MCP clients
7. Module Registry & Providers	Load order, is_configured() filtering, what makes tools appear
8. EDD Provider	7 Tier-2 tools plus 3 Tier-3 admin tools, credential storage
9. Jira Provider	4 Tier-2 tools plus 1 Tier-3 admin tool, service desk discovery, intent mapping
10. WooCommerce Provider	6 Tier-2 store tools plus 2 Tier-3 admin tools, no credentials required
11. LatePoint Provider	Compound booking tools, LatePoint MCP prerequisites, anonymous booking
12. Calendly & Acuity Providers	Two hosted scheduling platforms, 6 tools each

13. Hybrid Provider	get_full_user_profile and its 5-minute cache
14. External MCP Proxy	Connecting external MCP servers, the one database table
15. Tool Manifest & Tools Page	Double filtering, tier badges, Active vs Inactive
16. Diagnostics Page	Five tabs: tool tester, system status, debug log, abilities, external MCP
17. Security Operations	Rate limiting, HTTPS enforcement, credential encryption, revocation
18. AI Concierge Integration	How Gateway tools auto-appear, and why Tier-3 is excluded
19. Third-Party Providers	Registering your own provider and what you inherit
20. Maintenance & Updates	Shared updater, upgrade checklist, telemetry
21. Uninstall & Data Cleanup	Exactly what deletion removes
22. Troubleshooting	Symptoms, causes, and fixes

1. REQUIREMENTS & INSTALLATION

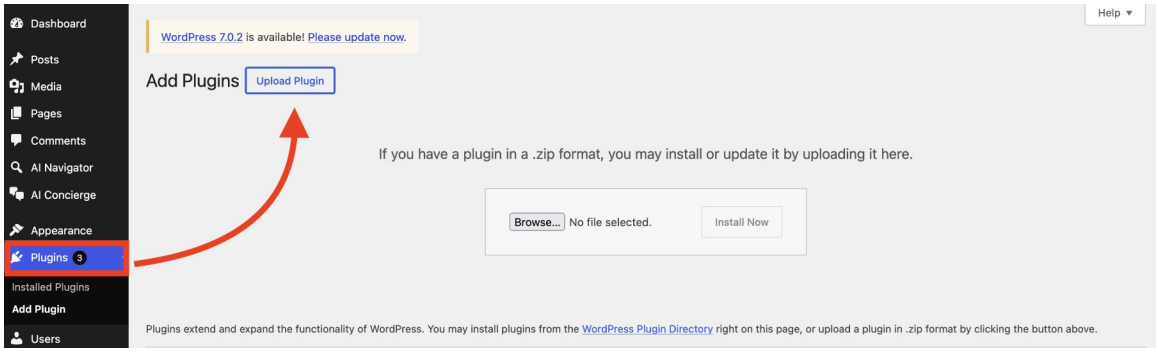
1.1 System requirements

Requirement	Details
WordPress	6.0 or later. 6.9 or later is recommended — the WordPress Abilities API is built into core from 6.9, and is available as a standalone plugin for 6.0 to 6.8.
PHP	7.4 or later.
HTTPS	Enforced on all endpoints by default. HTTP requests are rejected with 403. Disable enforcement only on local development environments (Section 17.2).
Database	One table, s2w_aig_mcp_servers, created idempotently on activation and on the s2w_aig_init hook. It exists only for the external MCP proxy (Section 14).
Licensing	None. AI Gateway is standalone — there is no Pro tier, no license key, and no license class. Every feature in this guide is available on every install.
Plugin family	S2W_INFRA_VERSION 1_2 in this release. AI Navigator and AI Concierge on the same site must run the same infrastructure version — see Section 20.1.
Providers (optional)	Each provider needs its own backing system: EDD, Jira Cloud, WooCommerce, LatePoint, Calendly, or Acuity Scheduling. Gateway does nothing useful until at least one is configured.

1.2 Installation steps

- Log in to your WordPress admin dashboard.
- Go to Plugins → Add New → Upload Plugin.
- Click Choose File and select the s2w-ai-gateway.zip file.
- Click Install Now and wait for the upload to complete.

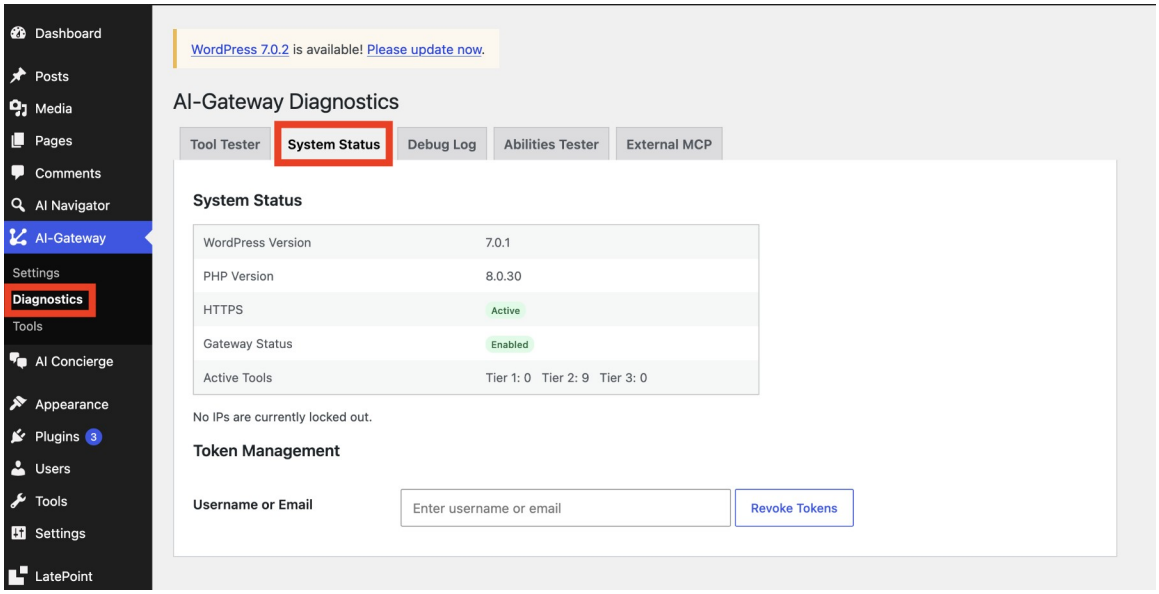
- Click Activate Plugin.
- AI-Gateway appears as a top-level menu in the admin sidebar with three subpages: Settings, Tools, and Diagnostics.



Plugins → Add New → Upload Plugin

After activation The plugin creates the s2w_aig_mcp_servers table (safe to re-activate — creation is idempotent), generates a strong 64-character HMAC signing secret, and enables the gateway with HTTPS enforcement on and a 24-hour token lifetime. No tools are registered yet: the manifest stays empty until you configure a provider.

Verify before configuring Go to AI-Gateway → Diagnostics → System Status and confirm HTTPS shows Active and Gateway Status shows Enabled before you configure providers. Active Tools reading zero across all three tiers is expected on a fresh install.



AI-Gateway → Diagnostics → System Status

2. THE ADMIN INTERFACE

Everything the Gateway exposes to administrators lives under the AI-Gateway top-level menu.

Page	What it is for
Settings	Endpoint URL, kill-switch, HTTPS, token lifetime, rate limits, and one tab per provider. Section 2.1.
Tools	The full tool manifest with tier badges and Active / Inactive status. Section 15.2.
Diagnostics	Tool tester, system status, debug log, abilities tester, and external MCP server management. Section 16.

2.1 Settings tabs

Tab	Contains
General	MCP Endpoint URL (read-only, with a Copy button), Global Kill-Switch, Require HTTPS, and Token Lifetime.
Security	The three rate-limiting parameters applied to the /auth endpoint (Section 17.1).
EDD	Easy Digital Downloads store URL, API key, and API token, plus a Test button (Section 8.3).
Jira	Jira site URL, admin email, API token, service desk discovery, and request-type intent mapping (Section 9.3).
WooCommerce	A single enable toggle. No credentials — the provider reads your store directly (Section 10.2).
Calendly	Personal Access Token (Section 12.1).
Acuity	Acuity User ID and API Key (Section 12.2).
External MCP	Add, test, enable, and remove external MCP servers proxied through the Gateway (Section 14).

2.2 General tab settings

Setting	Details
MCP Endpoint URL	Read-only display of the custom dispatch endpoint for this site, with a Copy button. Configure AI clients and integrations against it.
Global Kill-Switch	"Gateway is enabled", on by default. Unchecking it disables every endpoint immediately — all requests return 503. Use it to cut AI access to the site without deactivating the plugin or losing configuration.
Require HTTPS	On by default. All endpoints reject plain HTTP with 403 while it is on. Disable only in local or development environments.
Token Lifetime (hours)	How long an issued token stays valid. Default 24, range 1 to 720. Changing it affects newly issued tokens only — tokens already in circulation keep the expiry stamped into them.

3. THE FOUR-TIER SECURITY MODEL

Every tool registered in the Gateway is pinned to exactly one security tier. The tier decides who may call the tool and what data it may return. This is the authorization spine of the entire plugin, and it is enforced identically on all three dispatch surfaces.

3.1 Tier definitions

Tier	Who	Token	Data scope
Tier 1 — Public	Anonymous visitors	Not required	Public data only
Tier 2 — User	Any logged-in user	Valid Bearer token	Own data only — identity is taken from the token, never from parameters
Tier 3 — Admin	Administrators	Bearer token with manage_options	Any customer's data
Tier 4 — Never	Nobody, ever	Not applicable	Never registered. The tool does not exist.

No tool declares Tier 1 in this release Every tool shipped in v1.8.0 is Tier 2 or Tier 3, so the Active Tools row on the Diagnostics page correctly reads Tier 1: 0. The tier exists for third-party providers and for future public tools. Anonymous visitors reach LatePoint booking by a different route — through the WordPress Abilities API rather than a Tier-1 tool (Section 11.3).

3.2 Tier 4 — enforcement by omission

Tier 4 is the set of operations AI is never given. They are not disabled by a setting, not hidden behind a capability, and not gated by a confirmation prompt — they are simply never registered as tools, so no dispatch path can reach them. Typical Tier 4 operations:

- Create, edit, or delete a product or download.
- Set or change a price.
- Generate a license key.
- Delete an order.
- Modify another user's license status.

Why this matters No prompt injection, jailbreak, misconfigured persona, or authentication bypass can produce a Tier 4 action, because there is no callable tool to invoke. If a deployment genuinely needs one of these operations, a human administrator performs it in the WordPress admin UI. A unit test asserts that every registered tool declares tier 1, 2, or 3, so this cannot drift silently.

3.3 Tier enforcement at dispatch

When a tool invocation arrives, the Gateway runs the following before any provider code executes:

- HTTPS is enforced if enabled — plain HTTP is rejected with 403.

- The kill-switch is checked — a disabled gateway returns 503.
- The token is verified: signature, revocation (token version), then expiry.
- The WP_User is resolved from the token payload with get_userdata(). AI-supplied parameters are sanitized and used as filtering hints only, never as identity.
- The tool is looked up in the registry. A tool above the caller's tier returns the same not-found response as a tool that does not exist, so higher-tier tool names cannot be probed from a lower-tier token.
- current_user_can() is called for the tool's declared capability. A mismatch returns 403.
- Only then does the provider handler run, scoped to the resolved user.

Identity is never a parameter Tools accept fields such as customer_email or reporter_email so the assistant can filter, but the authenticated identity always comes from the token payload. A Tier-2 tool called with someone else's email returns that caller's own data or nothing at all — never the other user's records.

4. AUTHENTICATION

4.1 Token format

```
token = base64url( payload_json ) + "." + hmac_sha256_hex( encoded_payload, secret )
```

Payload field	Purpose
`user_id`	WordPress user ID. Re-resolved on every dispatch. The AI cannot forge or override it.
`email`	The user's email at issue time. Informational — used for logging and diagnostics only.
`capabilities_snapshot`	Contains manage_options for administrators, otherwise read.
`token_version`	Must be at least the current s2w_aig_token_version user meta value. Incrementing that meta revokes every outstanding token for the user.
`issued_at`	Unix timestamp at issue.
`expires_at`	issued_at plus the configured token lifetime (default 24 hours).

4.2 Issuing a token

POST the WordPress username and an application password to the `/auth` endpoint:

```
curl -X POST https://yoursite.com/wp-json/s2w-ai-gateway/v1/auth \
  -H "Content-Type: application/json" \
  -d '{"username":"admin","password":"your-app-password"}'

# → 200  { "token": "...", "expires_in": 86400 }
```

Always use an Application Password Create one at Users → Profile → Application Passwords → Add

New. Never send a real login password to this endpoint — WordPress rejects login passwords for REST authentication by default, and an application password can be revoked independently without changing the account password.

4.3 Refresh, expiry, and revocation

- **Refresh.** POST an existing token to /auth/refresh to get a new one without re-sending credentials. Refresh tolerates an expired token, but never a revoked one.
- **Expiry.** Set by Token Lifetime on Settings → General — default 24 hours, maximum 720. A shorter lifetime limits the blast radius of a leaked token; a longer one reduces re-authentication for long-running agents.
- **Revocation.** Go to AI-Gateway → Diagnostics → System Status → Token Management, enter a username or email, and click Revoke Tokens. Every token held by that user fails on its next call, including tokens that have not yet expired. Programmatically this is S2W_AIG_Token::revoke($user_id), which increments the token version.
- **Capability drift.** A token carries the capabilities the user had when it was issued. If a user is promoted or demoted, re-issue the token — the Gateway checks the live user's capability at dispatch, so a stale snapshot can only ever lose access, never gain it.

Revocation is checked before expiry A token that is both revoked and expired reports as revoked, not expired. This ordering matters: /auth/refresh forgives expiry, so a revoked-and-expired token reported as merely expired could otherwise be refreshed back into a working token.

4.4 The signing secret

The HMAC secret lives in the `s2w_aig_hmac_secret` option. It is generated on activation and, defensively, on load, so multisite subsites and file-copy deploys that never ran activation still get a per-site secret. It is never rotated automatically — an existing secret is always kept, so live tokens stay valid. Verification fails closed: if the secret is missing, every token is rejected rather than accepted, because an empty HMAC key would make any token verifiable.

5. REST ENDPOINTS

All routes are under the `/wp-json/s2w-ai-gateway/v1/` namespace and all of them honour the HTTPS setting and the kill-switch.

Route	Method	Auth	Purpose
`/auth`	POST	Username + application password	Issue a token. Rate-limited per IP.
`/auth/refresh`	POST	Bearer token (expired accepted)	Return a fresh token without credentials.
`/mcp`	POST	Bearer token	Custom tool dispatch. Body: tool name plus parameters.
`/mcp/tools`	GET	Bearer token (optional)	Tier-filtered manifest. Without a token,

			Tier-1 tools only.
`/mcp-server`	POST	Bearer token (initialize is open)	Standard MCP JSON-RPC 2.0 endpoint (Section 6).

5.1 Response codes

Code	Meaning
`200`	Success.
`401`	Missing, malformed, expired, or revoked token; or a token whose user no longer exists.
`403`	HTTPS required, or authenticated but lacking the capability the tool declares.
`404`	Tool not found — also returned for a tool that exists above the caller's tier.
`429`	Rate limit hit on /auth. The IP is locked out for the configured period.
`503`	The global kill-switch is off.

404 is deliberately ambiguous A Tier-3 tool requested with a Tier-2 token returns the same 404 as a tool that does not exist. This is intentional: it stops an authenticated non-admin from enumerating admin tool names by probing the endpoint.

5.2 Calling a tool

```
curl -X POST https://yoursite.com/wp-json/s2w-ai-gateway/v1/mcp \
  -H "Authorization: Bearer YOUR_TOKEN" \
  -H "Content-Type: application/json" \
  -d '{"tool":"wc-get-my-orders","params":{"limit":5}}'
```

6. STANDARD MCP SERVER ENDPOINT NEW IN 1.8.0

AI Gateway now speaks the Model Context Protocol natively at `/wp-json/s2w-ai-gateway/v1/mcp-server` — JSON-RPC 2.0 over Streamable HTTP. Claude Code, Claude Desktop, Gemini, and any MCP-compatible client connect to it directly, with no custom integration code. The same four-tier model applies; only the wire format differs.

6.1 Supported methods

Method	Behaviour
`initialize`	Open — no token required. Returns the protocol version and server info. The server reports only its major.minor.patch version, so pre-release build identifiers are never disclosed to anonymous callers.
`tools/list`	Requires a Bearer token. Returns the manifest filtered to the caller's tier, in MCP tool

	shape with a JSON Schema for each tool's inputs.
`tools/call`	Requires a Bearer token. Invokes a tool by its normalized name. A tool above the caller's tier returns the same "not found" error as an unknown tool.

6.2 Which endpoint to use

Endpoint	Use it for
`/mcp-server`	External MCP clients — Claude Code, Claude Desktop, Gemini, custom agents.
`/mcp and /mcp/tools`	AI Concierge and direct REST integrations. These remain fully supported.

6.3 MCP-safe tool names

The MCP specification constrains tool names to a restricted character set, which the slash-separated provider names such as `s2w-latepoint/get-services-menu` violate. On the `/mcp-server` surface only, names are normalized to a compliant form, and `tools/call` resolves the normalized name back to the canonical one. Clients that previously dropped LatePoint, Calendly, or Acuity tools now accept the whole manifest. The custom `/mcp` endpoint continues to use canonical names, so existing integrations are unaffected.

Turning the endpoint off The MCP server endpoint is on by default. To disable it without touching the rest of the Gateway, set the `s2w_aig_mcp_server_enabled` option to a falsy value — for example with WP-CLI: `wp option update s2w_aig_mcp_server_enabled 0`. The custom /mcp endpoints are unaffected.

One-click connect is not in this release The endpoint is fully functional and any MCP client can connect to it with a Bearer token, as described in Appendix C. The one-click connect flow for hosted AI clients — where the client negotiates its own credentials instead of being handed a token — is deliberately not part of v1.8.0 and will follow in a later version. That is also why there is no MCP Server tab in Settings.

Ready-to-paste client configuration for Claude Code, Claude Desktop, and Gemini is in Appendix C.

7. MODULE REGISTRY & PROVIDERS

7.1 The registry

Providers are the units that contribute tools. They register themselves with a singleton registry, and the core never references any provider by name — which is what lets third-party plugins participate on equal terms (Section 19).

7.2 Load order

Hook and priority	What registers

`plugins_loaded @ 20`	EDD, Jira, WooCommerce, Calendly, Acuity, and Hybrid providers.
`wp_abilities_api_init @ 20`	LatePoint provider — only if LatePoint's latepoint/get-services ability exists.
`wp_abilities_api_init @ 30`	External MCP proxy provider, contributing the tools of each enabled external server.
`s2w_aig_register_modules`	Third-party providers (Section 19).

7.3 is_configured() filtering

Every provider implements `is_configured()`. An unconfigured provider contributes zero tools to the manifest — this is why EDD tools do not appear until EDD credentials are saved, and why the WooCommerce tools stay absent until the toggle is switched on. The Tools page shows registered tools whether or not their provider is configured, marking them Active or Inactive; the REST manifest returns configured tools only.

The manifest is rebuilt on every request There is no manifest cache to clear. If a provider is configured correctly, its tools appear on the next page load or the next API call. When tools do not appear, the cause is always a failing prerequisite — not a stale cache.

8. EDD PROVIDER

Requires Easy Digital Downloads to be active and EDD API credentials to be saved on Settings → EDD.

8.1 Tier-2 tools (authenticated, own data)

Tool	Returns
`get_customer_details`	The authenticated user's EDD customer record and lifetime value.
`get_customer_orders`	The authenticated user's purchase history — order IDs, products, amounts, dates.
`get_customer_licenses`	The authenticated user's license keys with status, expiry, and activation count.
`get_products`	The active product catalogue with IDs, names, prices, and descriptions.
`get_checkout_url`	A direct checkout URL for a product, optionally for a specific price variation.
`validate_license`	The status of a license key for a given site URL.
`fetch_latest_version`	Whether an EDD-licensed product is up to date, given its license key.

8.2 Tier-3 tools (admin only)

Tool	Returns

`list_recent_sales`	The store-wide transaction log. Defaults to the 20 most recent sales.
`get_store_stats`	A revenue and sales snapshot for the whole store.
`manage_license_activation`	Activate or deactivate any customer's license on a given site URL.

8.3 Configuration

- In WordPress, go to Downloads → Tools → API Keys and generate a key for a user.
- Copy the public key and the token.
- Go to AI-Gateway → Settings → EDD and paste the store URL, API key, and API token.
- Click Save, then use the Test button to confirm the connection.

Credentials are stored AES-256-CBC encrypted (Section 17.3). When a WordPress account uses a different email address from its EDD customer record, set the per-user override in the `s2w_aig_edd_email` user meta field on the user profile.

9. JIRA PROVIDER

Requires a Jira Cloud API token. Ticket creation additionally requires a Jira Service Management service desk.

9.1 Tier-2 tools

Tool	Returns
`search_tickets`	Tickets filed by the authenticated user, with an optional text filter and result limit.
`get_ticket_history`	Comments and status transitions for one of the user's own tickets.
`create_support_ticket`	Creates a service desk request on the user's behalf, routed by intent key (Section 9.4).
`add_ticket_comment`	Adds a comment to one of the user's own tickets.

9.2 Tier-3 tool

Tool	Returns
`transition_ticket`	Moves any ticket through its workflow, given a ticket ID and transition ID. Administrators only.

9.3 Configuration

- Create an API token at id.atlassian.com → Manage profile → Security → API tokens.
- Go to AI-Gateway → Settings → Jira and enter the Jira site URL (yourcompany.atlassian.net), the admin email that owns the token, and the token itself.

- Click Test Jira Connection.
- Click Connect and Discover Service Desks, then select the service desk to use.
- Click Load Request Types to populate the request types available for mapping.
- Click Save. The API token is stored AES-256-CBC encrypted.

9.4 Request type mapping

Ticket creation is driven by an intent map you define. Each row pairs an intent key the assistant can choose (lowercase with underscores), a label shown in the manifest, a description that tells the assistant when to use it, a Jira request type, and optionally a required field value. The descriptions are what the model reads when deciding which intent fits a conversation, so write them the way you would brief a new support agent — concrete and mutually exclusive.

When emails differ between WordPress and Jira, set the per-user override in the `s2w_aig_jira_email` user meta field.

10. WOOCOMMERCE PROVIDER NEW IN 1.8.0

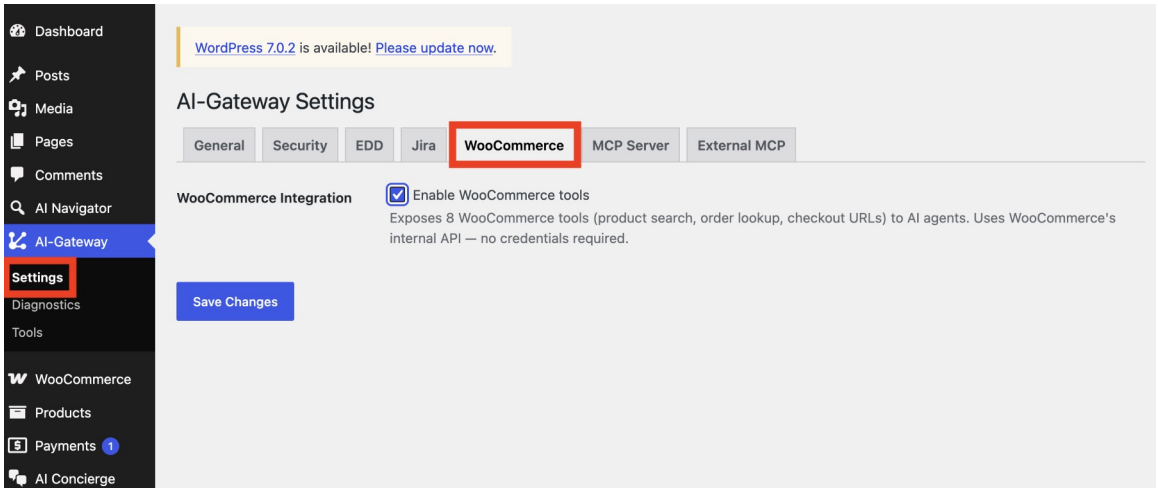
Eight store tools that read WooCommerce directly through its own internal API. No API keys, no consumer secrets, nothing to rotate.

10.1 Tools

Tool	Tier	Returns
`wc-search-products`	2	Product search across the catalogue.
`wc-get-product-details`	2	Full detail for one product, including price, stock, and attributes.
`wc-get-my-orders`	2	The authenticated user's own orders.
`wc-get-order-details`	2	Full detail for one of the user's own orders.
`wc-get-checkout-url`	2	A checkout URL for a product. Refuses IDs that do not resolve to a real product.
`wc-get-product-categories`	2	The product category tree.
`wc-get-customer-by-email`	3	Look up any customer by email address. Administrators only.
`wc-get-all-orders`	3	Search orders across all customers. Administrators only.

10.2 Configuration

Go to AI-Gateway → Settings → WooCommerce, switch Enable WooCommerce tools on, and click Save. The toggle is off by default, so this step is required even on a site where WooCommerce is already active. If WooCommerce is not active, the tab explains that and the toggle has no effect.



AI-Gateway → Settings → WooCommerce — integration toggle

Read-only by design The WooCommerce tools read the catalogue and orders and produce checkout URLs. They never create, edit, or cancel an order, never change a price, and never modify a product — those are Tier 4 operations, and they are not registered (Section 3.2).

11. LATEPOINT PROVIDER

Nine compound Tier-2 booking tools. Compound means each tool wraps several of LatePoint's own abilities into one call shaped for a conversation, so the assistant does not have to chain low-level operations.

11.1 Tools

Tool	What it does
`get-services-menu`	Bookable services with descriptions, pricing, duration, extras, and which staff offer them.
`get-team-members`	The staff who can perform a given service.
`find-available-slots`	Real open slots for a service, agent, and date.
`find-next-available-slots`	The next open slots without a specific date. Past slots for today are filtered out, and today itself is scanned.
`book-appointment`	Writes the booking. Captures customer name and email.
`get-my-bookings`	A customer's upcoming or past bookings.
`get-booking-details`	Full detail for one booking.
`reschedule-booking`	Moves a booking to a new slot.
`cancel-my-booking`	Cancels a booking.

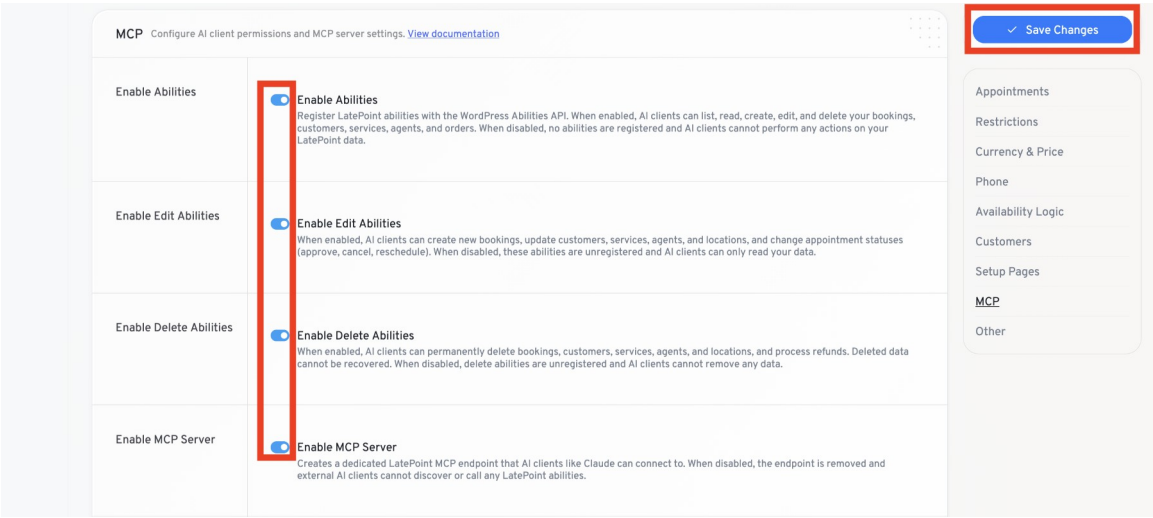
Tool names are prefixed `s2w-latepoint/` in the canonical manifest, and normalized on the /mcp-server endpoint (Section 6.3).

11.2 Prerequisites in LatePoint

There is nothing to configure inside AI Gateway, but LatePoint must expose its abilities first. Go to LatePoint → Settings → MCP and enable:

- **Enable Abilities** — registers LatePoint capabilities with the WordPress Abilities API. Fresh LatePoint installs default this to off, and the Gateway provider stays silently hidden until it is on.
- **Enable Edit Abilities** — required for booking, rescheduling, and cancelling. Without it, only read operations work.
- **Enable MCP Server** — exposes the capabilities for AI-driven scheduling on the site.

Click Save Changes. The provider loads on the next page load. Leave Enable Delete Abilities off — the Gateway booking tools do not need it.



LatePoint → Settings → MCP — abilities and MCP server toggles

11.3 Anonymous booking

New in v1.8.0. Booking no longer requires the visitor to have a WordPress account. The booking tools are registered as WordPress Abilities with a public permission callback, and internally the provider calls LatePoint's own abilities with elevated privileges so that availability lookups and writes succeed for a visitor who is not logged in. This is what lets AI Concierge's booking persona work on a public page.

This applies to the ability path, not the REST endpoints Anonymous access is granted on the WordPress Abilities API surface — the route AI Concierge uses. The Gateway's own /mcp, /mcp/tools, and /mcp-server endpoints are unchanged: they still require a valid Bearer token, and the LatePoint tools remain Tier 2 there.

What anonymous access does and does not open up Ownership is verified by the customer_email input on every read and write against an existing booking, and the responses for "no such booking" and "not your booking" are deliberately identical, so an anonymous caller cannot probe which booking IDs exist. Elevation applies only inside the booking tools' own LatePoint calls — it does not widen the tier model or grant access to any other provider.

Confirmation discipline book-appointment is the canonical write tool. AI Concierge's LatePoint

template persona locks the rule that the visitor must confirm before the tool is called. Unlocking that rule in a persona lets the model book without explicit approval — the single highest-risk persona-design mistake available. Leave it locked.

12. CALENDLY & ACUITY PROVIDERS NEW IN 1.8.0

Two hosted scheduling platforms, six Tier-2 tools each. The difference that matters when choosing: Acuity books directly inside the conversation, while Calendly hands the visitor a secure link to finish on Calendly — a Calendly booking always completes on the Calendly page.

12.1 Calendly

Tool	What it does
`get-event-types`	Bookable event types with name, duration, description, and booking URL.
`get-available-times`	Open slots for an event type within a date window of up to seven days.
`create-scheduling-link`	A single-use booking link the visitor follows to complete the booking.
`get-my-bookings`	A customer's upcoming or past bookings, by email.
`get-reschedule-link`	The official reschedule link for a booking, after verifying the email matches an invitee.
`cancel-booking`	Cancels a booking, after verifying the email matches an invitee.

Configure it on AI-Gateway → Settings → Calendly: paste a Personal Access Token created in Calendly under Integrations and apps → API and webhooks, then Save.

12.2 Acuity Scheduling

Tool	What it does
`get-appointment-types`	Bookable appointment types with name, duration, and price.
`get-availability`	Open times for an appointment type on a given date.
`book-appointment`	Books directly, given a slot datetime and the customer name, email, and optional phone.
`get-my-appointments`	A customer's upcoming or past appointments, by email.
`reschedule-appointment`	Moves an appointment, after verifying ownership by email.
`cancel-appointment`	Cancels an appointment, after verifying ownership by email.

Configure it on AI-Gateway → Settings → Acuity: enter your Acuity User ID and API Key from Acuity's integration settings, then Save. Acuity's API requires a plan that includes API access.

Email verification on write Both providers verify that the supplied customer email matches the booking

owner before rescheduling or cancelling. The assistant supplies the email as a filter; it never grants identity (Section 3.3).

Read-only tools are labelled as such The scheduling tools that only read — event and appointment types, availability, and booking lookups — are annotated read-only in their ability registration, so MCP clients know they are safe to call without asking the visitor to confirm. Booking, rescheduling, and cancellation carry no such annotation and should always be confirmed.

13. HYBRID PROVIDER

One Tier-2 tool, `get_full_user_profile`, which returns the authenticated user's EDD purchase history and Jira tickets in a single call. It registers only when both EDD and Jira are configured. Results are cached per user for five minutes, which keeps a support conversation from re-fetching the same profile on every turn.

14. EXTERNAL MCP PROXY

The proxy lets you connect external MCP servers — your own internal service, a third-party SaaS server — and expose their tools through your Gateway, behind the same authentication and tier model.

14.1 Adding a server

- Go to AI-Gateway → Settings → External MCP and click Add New.
- Enter a display name, the server URL, an auth type (bearer, basic, or none), and the auth value.
- Click Test Connection to verify the handshake and list the tools the server exposes.
- Save. The server can be enabled or disabled at any time without deleting it.

Proxied tools become addressable as `mcp-proxy/<server-slug>/<tool-name>` and a daily background job refreshes each server's tool list. External tools are treated as Tier 2 by default; Tier 3 requires an explicit per-server flag. Disabled servers are skipped entirely when the manifest is built.

14.2 The database table

The proxy owns the only table AI Gateway creates, `{prefix}s2w_aig_mcp_servers`, which stores the slug, display name, URL, auth type, AES-256-CBC encrypted auth value, tier, and enabled flag for each server. It is created idempotently on activation and on the s2w_aig_init hook, so a missing table rebuilds itself on the next admin page load.

15. TOOL MANIFEST & TOOLS PAGE

15.1 How the manifest is filtered

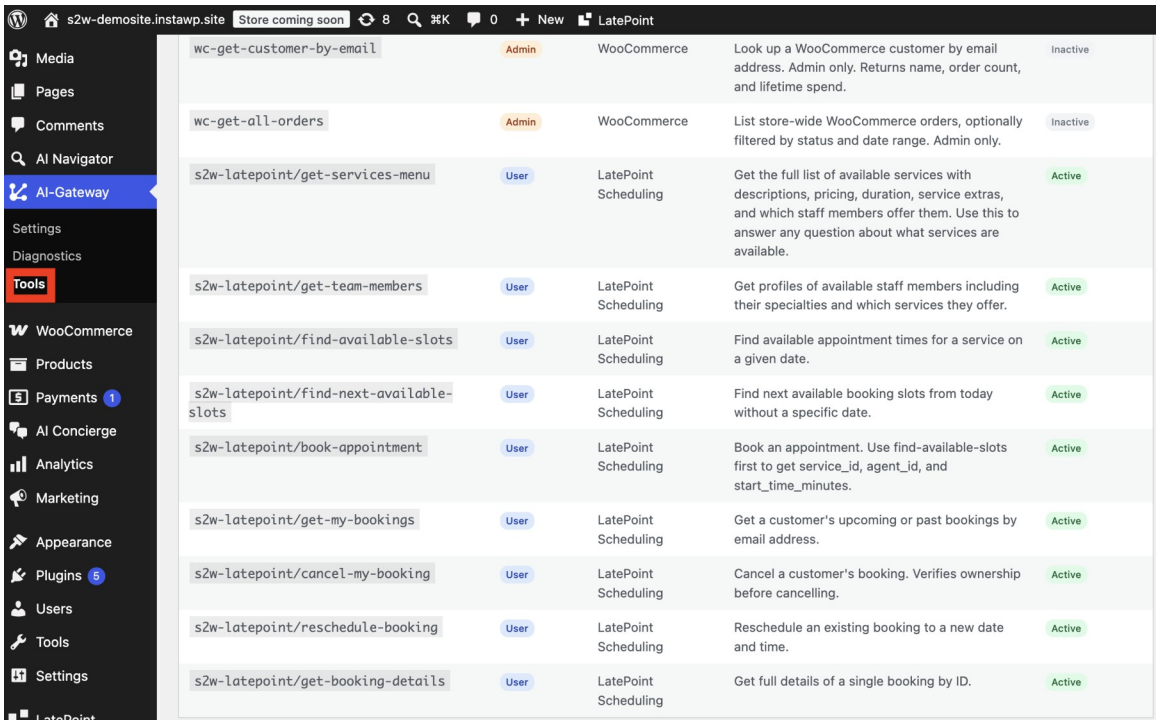
The manifest is filtered twice, in this order:

- By configuration — unconfigured providers contribute nothing.
- By tier against the caller's capability — Tier 1 for anonymous callers, Tier 2 for any authenticated user, Tier 3 only for administrators.

Tools the caller cannot use are absent from the response. They are not returned as locked or unauthorized entries: absent means not for you.

15.2 The Tools page

AI-Gateway → Tools shows the full registered manifest for administrators, with one row per tool: name, tier badge (Public, User, Admin), module, description, and an Active or Inactive status. Active means the provider is configured and the tool is callable now. This page is the fastest way to confirm that a provider you just configured actually took effect.



AI-Gateway → Tools — manifest with tier badges and status

Provider	Tools	Notes
EDD	10 (7 Tier-2, 3 Tier-3)	Customer, purchase, and license lookups
Jira	5 (4 Tier-2, 1 Tier-3)	Ticket search, create, comment, transition
WooCommerce	8 (6 Tier-2, 2 Tier-3)	Products, categories, orders, checkout URL
LatePoint	9 (all Tier-2)	Compound booking tools
Calendly	6 (all Tier-2)	Event types, availability, scheduling links
Acuity	6 (all Tier-2)	Appointment types, availability, direct booking
Hybrid	1 (Tier-2)	Merged EDD and Jira user profile

16. DIAGNOSTICS PAGE

AI-Gateway → Diagnostics has five tabs. Everything runs over AJAX — no page reloads.

Tab	What it does
Tool Tester	Runs a single tool with your own credentials and shows the raw JSON result. Tier-1 and Tier-2 tools only — Tier-3 admin tools are deliberately not testable from this form.
System Status	WordPress and PHP versions, HTTPS status, gateway enabled state, and Active Tools counts per tier. Also holds the Locked IPs table and Token Management.
Debug Log	Per-request log of tool, user, status, and latency. Inactive until S2W_AIG_DEBUG is defined true in wp-config.php. Includes a Clear Log button.
Abilities Tester	Executes any registered WordPress Ability by name in an administrator context and returns the result inline. The tool of choice for debugging third-party ability registration.
External MCP	Manage proxied external MCP servers (Section 14).

16.1 Locked IPs

When an IP trips the /auth rate limit it appears here with its lockout window and an Unblock button. Unblocking clears the lockout immediately — useful when a legitimate integration locked itself out with a stale credential.

16.2 Token management

Enter a username or email and click Revoke Tokens to invalidate every token that user holds. This is the correct response to a leaked token, a departing staff member, or a compromised agent client. It takes effect on the next request; there is no cache to wait out.

Enable the debug log while integrating, not permanently Add `define( 'S2W_AIG_DEBUG', true );` to wp-config.php while you are building an integration — the per-call latency and status view makes tier and parameter problems obvious. Remove it afterwards: the log records every dispatch and grows without bound.

17. SECURITY OPERATIONS

17.1 Rate limiting

Rate limiting protects the /auth endpoint against credential guessing. It is per IP address and configured on Settings → Security.

Parameter	Default	Range
Failed attempts before lockout	5	1 to 100
Window (minutes)	15	1 to 1440
Lockout duration (minutes)	30	1 to 1440

A locked-out IP receives 429 until the lockout expires. State lives in transients — no table, no external dependency, and it clears itself. Limiting is per IP only, so users behind a shared NAT share a budget; this is

a design decision, not a defect. Only the /auth endpoint is rate-limited: tool dispatch is protected by token verification instead.

17.2 HTTPS enforcement

On by default. While enabled, every endpoint rejects plain HTTP with 403, which prevents Bearer tokens from crossing the network in the clear. Disable it only on local development environments. A production site with HTTPS enforcement disabled is a configuration error, not a supported deployment.

17.3 Credential encryption

Secret	Storage
EDD API key and token	AES-256-CBC encrypted in plugin options.
Jira API token	AES-256-CBC encrypted in plugin options.
Calendly token, Acuity API key	AES-256-CBC encrypted in plugin options.
External MCP auth values	AES-256-CBC encrypted in the s2w_aig_mcp_servers table.
HMAC signing secret	Stored as a plugin option. Not encrypted — it is the signing key itself, and it is wiped on uninstall.
Per-user email mappings	Plain user meta. These are addresses the user already owns; they are not secrets.

Rotating WordPress salts invalidates stored credentials The encryption key is derived from the site's WordPress secret keys. Rotating those keys makes every stored provider credential undecryptable — the symptom is a credential test that fails even though the values look right. The fix is to re-enter and re-save each provider's credentials, which re-encrypts them under the new key. Plan salt rotations accordingly.

17.4 The kill-switch

Settings → General → Global Kill-Switch disables every endpoint at once, returning 503 to all callers while leaving configuration, credentials, and tokens intact. It is the correct first move if you suspect an integration is misbehaving: cut access, investigate, then re-enable.

18. AI CONCIERGE INTEGRATION

When AI Concierge is installed on the same site, Gateway tools appear in its Agentic Tools discovery automatically. There is no configuration in either plugin.

18.1 The mechanism

- Gateway registers its tools as WordPress Abilities.
- Concierge scans registered abilities when its one-hour ability cache refreshes. To pick up a newly configured provider immediately, go to AI Concierge → Tools and click Refresh abilities.
- Only Tier-2 abilities are offered for persona assignment. Tier-3 admin tools are excluded at the discovery layer.

- Concierge template personas for LatePoint, Jira, EDD, and WooCommerce have Gateway tools pre-assigned and refuse to go live if the matching provider is not configured.

18.2 Why Tier 3 is excluded

Concierge personas are visitor-facing. Store-wide revenue figures, all-customer order search, and ticket triage should never be reachable from an on-site chat widget, regardless of how a persona is configured. Excluding them at the discovery layer means they are not merely hidden in the UI — they are unassignable.

19. THIRD-PARTY PROVIDERS

Any plugin can contribute tools to the Gateway and inherit its whole security pipeline.

19.1 Registering

```
add_action( 's2w_aig_register_modules', function ( $registry ) {
    $registry->register( new My_Provider() );
} );
```

Method	Responsibility
`get_id()`	A unique provider identifier.
`get_display_name()`	The human-readable name shown on the Tools page.
`is_configured()`	True only when everything the provider needs is present — plugin active, credentials saved.
`get_tools()`	The tool definitions: name, tier, capability, description, parameter schema, and handler.

19.2 What you inherit

- Token verification on every call — signature, revocation, expiry.
- Tier enforcement before your handler runs.
- Capability checking against the capability your tool declares.
- Identity resolution — your handler receives the authenticated user, already resolved.
- Rate limiting, HTTPS enforcement, and credential encryption helpers.

Three rules for provider authors Never accept a user ID or customer ID as a tool parameter — derive identity from the authenticated user the Gateway hands you. Keep Tier-2 tools strictly own-data; if a tool must be site-wide, declare it Tier 3. And never register a destructive operation as a tool at any tier: that is what Tier 4 means (Section 3.2).

20. MAINTENANCE & UPDATES

20.1 The shared updater

AI Gateway, AI Navigator, and AI Concierge share versioned update infrastructure (S2W_INFRA_VERSION 1_2 in this release). When the infrastructure version changes, all installed S2W plugins must update in the same release window — mixing versions in one PHP request causes a "cannot redeclare class" fatal. Updates delivered through speak2web handle this automatically; the one rule is not to hold one plugin back while updating the others.

20.2 Upgrade checklist

- Read the changelog in readme.txt before upgrading.
- Back up the database — the table that matters is s2w_aig_mcp_servers — and note your provider credentials.
- Upload and activate the new version. Any migration runs on the first admin page load.
- Open Diagnostics → System Status and confirm HTTPS, gateway state, and per-tier tool counts.
- Open Tools and confirm the counts match your configured providers.
- Issue a token via /auth and call /mcp/tools with it.
- Invoke one Tier-2 tool with a non-admin token and confirm the response contains only that user's data.
- If AI Concierge is installed, go to AI Concierge → Tools and click Refresh abilities.

20.3 Telemetry

A daily background job reports anonymous interaction counts for managed-update health tracking, then prunes the counters it reported. Nothing personally identifiable is included, and no conversation content is transmitted.

21. UNINSTALL & DATA CLEANUP

Deleting AI Gateway from Plugins → Delete runs a complete sweep:

- Drops the s2w_aig_mcp_servers table.
- Deletes every plugin option — HMAC secret, HTTPS and kill-switch flags, token lifetime, rate-limit configuration and lockout state, all provider credentials, Jira discovery caches, and the debug log.
- Sweeps the dynamic Jira request-type option caches and every AI Gateway transient.
- Clears the scheduled jobs: the external MCP cache refresh and the daily telemetry job.
- Sweeps the daily interaction counters shared across S2W plugins.
- Removes per-user meta: token versions and the EDD and Jira email mappings.

The signing secret is destroyed Because the HMAC secret is deleted, every token ever issued by this install is permanently unverifiable after uninstall. A delete-and-reinstall cycle cannot resurrect old tokens — clients must re-authenticate against the new secret. This is deliberate.

Save your credentials first Provider credentials are encrypted with a key derived from this site's WordPress secrets, and they are deleted on uninstall. Make sure you still have the original EDD, Jira, Calendly, Acuity, and external MCP credentials before you delete the plugin.

22. TROUBLESHOOTING

Symptom	Cause and fix
/auth returns 401 with correct credentials.	The password field must hold a WordPress Application Password, not the login password. Create one at Users → Profile → Application Passwords.
/auth returns 429.	The IP tripped the rate limit. Wait out the lockout, or clear it from Diagnostics → System Status → Locked IPs → Unblock. Adjust the thresholds on Settings → Security.
Every request returns 503.	The Global Kill-Switch is off. Re-enable it on Settings → General.
Every request returns 403 over HTTP.	HTTPS enforcement is on, which is correct for production. Call over HTTPS; disable enforcement only for local development.
A token fails immediately after being issued.	Server clock skew. Tokens carry Unix timestamps and cannot validate against a drifting clock — check NTP on the host.
A token that worked yesterday now returns 401.	It expired — the default lifetime is 24 hours. Use /auth/refresh, or raise Token Lifetime on Settings → General.
A token returns "token revoked".	Someone revoked that user's tokens from Diagnostics, or the user's token version was incremented. Re-authenticate via /auth.
Every token is rejected as unconfigured.	The HMAC secret option is missing — usually a file-copy deploy that never ran activation. Re-activate the plugin; the secret is regenerated, and all existing tokens become invalid.
A configured provider's tools are missing.	is_configured() is returning false. Check that the backing plugin is active, credentials are saved, and the connection test passes. The Tools page shows the tool as Inactive when this is the cause.
LatePoint tools never appear.	LatePoint's own MCP settings are off. Enable Abilities, Edit Abilities, and MCP Server under LatePoint → Settings → MCP, then save (Section 11.2).
LatePoint availability returns no slots.	The service has no agent assigned. Open LatePoint → Services → the service and assign one.
WooCommerce tools missing although WooCommerce is active.	The integration toggle is off by default. Switch it on at Settings → WooCommerce and save.
A tool the user should be able to call returns 404.	It is above the caller's tier — Tier-3 tools return 404, not 403, for non-admin tokens. Use an administrator token.
An MCP client connects but lists no tools.	initialize is open but tools/list requires a token — check the Authorization header actually reaches the server. Also confirm at least one provider is configured.
An MCP client rejects some tool names.	Older Gateway versions exposed slash-separated names. v1.8.0 normalizes names on /mcp-server (Section 6.3) — upgrade, and reconnect the client so it re-reads the manifest.

A credential test fails although the values are correct.	The WordPress secret keys were rotated, so the stored ciphertext can no longer be decrypted. Re-enter and save the credentials (Section 17.3).
External MCP tools fail with a 5xx.	The external server is failing, or its stored credential expired. Use Test Connection on the server record, then check that server's own logs.
Concierge does not see newly configured tools.	Its ability cache refreshes hourly. Go to AI Concierge → Tools and click Refresh abilities.
"Cannot redeclare class S2W_Updater…" fatal.	One S2W plugin updated while its siblings stayed on older infrastructure. Update AI Navigator, AI Concierge, and AI Gateway together, then clear the PHP opcache (Section 20.1).

APPENDIX A — COMPLETE TOOL REFERENCE

Every tool the Gateway can register, by provider. Tools appear in the live manifest only when their provider is configured.

Provider	Tool	Tier
EDD	`get_customer_details`	2
EDD	`get_customer_orders`	2
EDD	`get_customer_licenses`	2
EDD	`get_products`	2
EDD	`get_checkout_url`	2
EDD	`validate_license`	2
EDD	`fetch_latest_version`	2
EDD	`list_recent_sales`	3
EDD	`get_store_stats`	3
EDD	`manage_license_activation`	3
Jira	`search_tickets`	2
Jira	`get_ticket_history`	2
Jira	`create_support_ticket`	2
Jira	`add_ticket_comment`	2
Jira	`transition_ticket`	3
WooCommerce	`wc-search-products`	2
WooCommerce	`wc-get-product-details`	2

WooCommerce	wc-get-my-orders	2
WooCommerce	wc-get-order-details	2
WooCommerce	wc-get-checkout-url	2
WooCommerce	wc-get-product-categories	2
WooCommerce	wc-get-customer-by-email	3
WooCommerce	wc-get-all-orders	3
LatePoint	s2w-latepoint/get-services-menu	2
LatePoint	s2w-latepoint/get-team-members	2
LatePoint	s2w-latepoint/find-available-slots	2
LatePoint	s2w-latepoint/find-next-available-slots	2
LatePoint	s2w-latepoint/book-appointment	2
LatePoint	s2w-latepoint/get-my-bookings	2
LatePoint	s2w-latepoint/get-booking-details	2
LatePoint	s2w-latepoint/reschedule-booking	2
LatePoint	s2w-latepoint/cancel-my-booking	2
Calendly	s2w-calendly/get-event-types	2
Calendly	s2w-calendly/get-available-times	2
Calendly	s2w-calendly/create-scheduling-link	2
Calendly	s2w-calendly/get-my-bookings	2
Calendly	s2w-calendly/get-reschedule-link	2
Calendly	s2w-calendly/cancel-booking	2
Acuity	s2w-acuity/get-appointment-types	2
Acuity	s2w-acuity/get-availability	2
Acuity	s2w-acuity/book-appointment	2
Acuity	s2w-acuity/get-my-appointments	2
Acuity	s2w-acuity/reschedule-appointment	2
Acuity	s2w-acuity/cancel-appointment	2
Hybrid	get_full_user_profile	2
External MCP	mcp-proxy/<server-slug>/<tool-name>	2

APPENDIX B — OPTIONS REFERENCE

The options AI Gateway stores. All are removed on uninstall (Section 21).

Option	Purpose
`s2w_aig_hmac_secret`	Token signing secret. Generated on activation; never rotated automatically.
`s2w_aig_gateway_enabled`	Global kill-switch. Default on.
`s2w_aig_require_https`	HTTPS enforcement. Default on.
`s2w_aig_token_lifetime`	Token lifetime in hours. Default 24, maximum 720.
`s2w_aig_mcp_server_enabled`	The /mcp-server endpoint. Default on; no UI toggle in this release.
`s2w_aig_rate_limit_attempts`	Failed /auth attempts before lockout. Default 5.
`s2w_aig_rate_limit_window`	Rate-limit window in minutes. Default 15.
`s2w_aig_rate_limit_lockout`	Lockout duration in minutes. Default 30.
`s2w_aig_locked_ips`	Current lockout state, surfaced on the Diagnostics page.
`s2w_aig_edd_*`	EDD store URL, API key, and API token (encrypted).
`s2w_aig_jira_*`	Jira site URL, admin email, API token (encrypted), service desk ID, intent map, and discovery caches.
`s2w_aig_wc_enabled`	WooCommerce provider toggle. Default off.
`s2w_aig_calendly_*`	Calendly Personal Access Token (encrypted) and cached user URI.
`s2w_aig_acuity_*`	Acuity User ID and API Key (encrypted).
`s2w_aig_debug_log`	Debug log entries. Populated only when S2W_AIG_DEBUG is defined true.

Per-user meta: `s2w_aig_token_version` (revocation counter), `s2w_aig_edd_email` and `s2w_aig_jira_email` (email mapping overrides).

APPENDIX C — MCP CLIENT CONFIGURATION

All three clients connect to the standard endpoint at `https://yoursite.com/wp-json/s2w-ai-gateway/v1/mcp-server` with a Bearer token issued from /auth (Section 4.2). The plugin package ships the same instructions in docs/mcp-client-setup.md.

C.1 Claude Code

```
claude mcp add --transport http \
  --header "Authorization: Bearer <token>" \
  s2w-ai-gateway https://yoursite.com/wp-json/s2w-ai-gateway/v1/mcp-server
```

This writes to `.mcp.json` at the project root — not `.claude/mcp.json` — using transport type `http`, not sse. Verify with `claude mcp list`.

C.2 Claude Desktop

Use Settings → Connectors → Add custom connector, enter the endpoint URL, and supply the Bearer token when prompted. The Gateway tools then appear in the tool picker.

If the Connectors UI cannot carry the header, wrap the endpoint in a stdio bridge in `claude_desktop_config.json` (requires Node.js):

```
{
  "mcpServers": {
    "s2w-ai-gateway": {
      "command": "npx",
      "args": [
        "-y", "mcp-remote",
        "https://yoursite.com/wp-json/s2w-ai-gateway/v1/mcp-server",
        "--header", "Authorization: Bearer <token>"
      ]
    }
  }
}
```

A note on Claude Desktop Putting `"type": "http"` with headers directly into claude_desktop_config.json does not work — that form is a Claude Code feature. Use the Connectors UI or the bridge above.

C.3 Gemini

The google-genai Python SDK has experimental MCP support: build a Streamable HTTP client session with the mcp SDK, passing the Authorization header, and hand the session to the SDK as a tool. There is no configuration file. The worked example is in docs/mcp-client-setup.md.

C.4 What each token sees

Token holder	Sees
No token	Nothing beyond initialize. Listing and calling both require a token.
Subscriber or customer	Tier-2 tools, scoped to that user's own data.
Administrator	Tier-2 and Tier-3 tools, including store-wide and all-customer lookups.

APPENDIX D — WHAT'S NEW IN V1.8.0

Change	Details
WooCommerce provider	Eight store tools — product search and detail, categories, checkout URL, and order lookups, plus two admin-only tools for customer and all-order search. No credentials required; opt in on Settings → WooCommerce

	(Section 10).
Calendly provider	Six tools for event types, availability, single-use scheduling links, bookings by email, reschedule links, and cancellation (Section 12.1).
Acuity Scheduling provider	Six tools for appointment types, availability, direct booking, appointment lookup, rescheduling, and cancellation (Section 12.2).
Standard MCP server endpoint	/mcp-server speaks MCP JSON-RPC 2.0 over Streamable HTTP, so Claude Code, Claude Desktop, and Gemini connect natively with a Bearer token (Section 6, Appendix C).
Anonymous LatePoint booking	Visitors no longer need a WordPress login for AI Concierge's booking persona to check availability and book. Ownership is still verified by email on every existing booking (Section 11.3).
MCP-safe tool names	Tool names are normalized on the /mcp-server surface to the character set the MCP specification requires, so clients accept the whole manifest (Section 6.3).
LatePoint rescheduling	Customers can move an existing booking instead of cancelling and rebooking (Section 11.1).
Better availability search	find-next-available-slots scans today rather than starting tomorrow and filters out slots that have already passed, and availability no longer skips weekends — days with genuine availability are offered whichever weekday they fall on.
Locale-aware dates	Booking dates and times render in the site's locale and include the weekday, so the assistant quotes appointments in a form customers can read at a glance.
Read-only tool labelling	Scheduling tools that only read are annotated read-only, so MCP clients know which calls are safe to make without confirmation (Section 12).
Correct user context on delegated tools	Tools that delegate to another plugin's abilities now run with the correct WordPress user context, so permission checks resolve as intended.
MCP client connection guide	Step-by-step Claude Code, Claude Desktop, and Gemini configuration ships with the plugin in docs/mcp-client-setup.md (Appendix C).
Security hardening	Tier checks now run on every dispatch surface so higher-tier tool names cannot be probed; token revocation is evaluated before expiry so a revoked token can never be refreshed; token verification fails closed on a missing signing secret; booking and issue-tracker tools strictly enforce record ownership; store and issue-tracker query scope is tightened; credential storage and encryption routines are hardened; and the MCP server discloses only a coarse version to unauthenticated callers.
Deferred to a later release	The one-click connect flow for hosted AI clients is not part of v1.8.0. The MCP endpoint itself is fully functional with a Bearer token (Section 6).

First-time setup? Start with the **AI Gateway Quick Start Guide**. Questions? Visit **speak2web.com**.