

SITE AGENT / HUMAN USER GUIDE

HOW TO USE SITE AGENT.

A plain-English guide to first-time setup, asking questions, reviewing exact plans, making controlled changes, and understanding the safety boundaries.

VERSION 0.2.4 / DEVELOPER TEST BUILD / BACKED-UP TEST SITES

**BACK UP. BUILD KNOWLEDGE.
ASK. REVIEW. VERIFY.**

Site Agent is a private WordPress administration assistant. It lives inside wp-admin, learns from a secret-filtered index of the current site, answers operational questions, and can prepare controlled changes for a human to review and approve.

This guide reflects Site Agent 0.2.4, an early developer build intended for backed-up test sites.

01 / SITE AGENT

BEFORE YOU START

You need:

- an active Site Agent installation;
- a WordPress account with the appropriate Site Agent permissions;
- a recent site backup before testing changes;
- an OpenAI API key with API billing when you want AI chat and planning.

A ChatGPT subscription does not include OpenAI API usage. Site Agent has no public chatbot; its interface is available only to authenticated WordPress administrators and other specifically permitted users.

02 / SITE AGENT

FIRST-TIME SETUP

- 1 Sign in to WordPress and open **Site Agent** in the admin menu.
- 2 Open **Settings**.
- 3 Paste an OpenAI API key and select **Validate and save**. The key is validated, encrypted in WordPress, and never displayed again. If the server supplies the key, the interface reports that it is server-managed instead.
- 4 Open **Knowledge** and select **Rebuild knowledge index**. Wait for the rebuild to finish before relying on chat answers.
- 5 Open **Roles** and confirm who may inspect, propose, execute low-, medium-, or high-risk actions, roll changes back, and manage Site Agent.

03 / SITE AGENT

ASK A QUESTION

Open **Chat**, choose the agent role that best matches the task, and write naturally. The role changes emphasis; WordPress permissions still control what the person may do.

Good starting questions include:

- What changed on my site this week?
- Is anything on my site unhealthy?
- Which pages need attention?

- Which pages use this builder?
- What cron jobs are running?
- What could break if I remove a plugin?

Press **Enter** to send. Use **Shift+Enter** for a new line. Select **New conversation** when you want to clear the visible conversation and begin with a fresh task.

04 / SITE AGENT

REQUEST A CHANGE

Describe the desired result clearly and ask Site Agent to show the exact plan before doing anything.

For a write request, Site Agent does not let the AI modify WordPress directly. It:

- 1 interprets the request;
- 2 validates the action and exact target;
- 3 checks Site Agent and native WordPress permissions;
- 4 calculates the risk;
- 5 displays the exact plan for review;
- 6 runs only the approved plan;
- 7 records supported before-and-after evidence in the Change Ledger.

Read every plan. Confirm the target, fields, status, risk, and expected result before selecting **Approve and execute**. Cancel the plan if anything is unclear or incorrect. High-risk actions receive an additional warning.

05 / SITE AGENT

USE EACH SECTION

CHAT

Ask questions, request diagnostics in plain language, and propose controlled changes. Starter prompts are available when the conversation is empty.

HISTORY

Review the Change Ledger: when a change happened, what action ran, the target, risk, source, and whether a supported rollback is available. Refresh the table to retrieve current entries.

Rollback is targeted and conflict-aware. Site Agent refuses a normal rollback when the target no longer matches the state recorded immediately after the original change. A rollback is not a full-site backup.

KNOWLEDGE

Rebuild the local index, search the indexed evidence directly, and run plugin-removal analysis. The index can include content, plugin and theme metadata, builders, form definitions, cron, roles, safe settings, and database inventory. It excludes credentials, submissions, orders, user records, source code, and secret-like values.

If chat answers seem incomplete after site changes, rebuild the knowledge index and ask again.

Plugin-removal analysis reports bounded evidence such as shortcodes, blocks, content use, options, tables, cron, REST routes, and code references. Evidence can identify risk, but it cannot prove that removal is consequence-free.

ROLES

Assign Site Agent capabilities to WordPress roles. AI roles change the style and focus of answers; they do not override permissions. Give high-risk execution, rollback, and management access only to trusted users.

SETTINGS

Connect or replace the OpenAI key, choose the model, set audit/chat/ledger retention, decide whether redacted conversations are stored locally, and choose whether Site Agent data is removed on uninstall.

ADVANCED

Run measured diagnostics for WordPress, database, cron, memory, storage, and available error-log evidence. Gray results mean WordPress could not obtain decisive evidence; gray does not automatically mean the site is unhealthy.

06 / SITE AGENT

CURRENT CONTROLLED ACTIONS

Site Agent 0.2.4 can prepare controlled actions for:

- creating posts and pages;
- updating approved post/page fields;
- moving posts/pages to Trash;
- updating supported builder metadata;
- updating supported Yoast and Rank Math metadata;
- updating a small allowlist of non-secret core settings;
- activating or deactivating installed plugins on the current site;
- deleting expired transients;
- rolling back supported Change Ledger entries.

Published, scheduled, private, Trash, builder, plugin-state, and rollback operations can be high risk. Site Agent cannot deactivate itself and does not claim network-wide plugin rollback.

07 / SITE AGENT

PRIVACY AND SAFETY

- Site Agent is private to authenticated wp-admin users; it has no public chat endpoint.
- The AI plans but does not have direct write authority.
- Secrets are excluded before indexing and redacted again before provider requests, local conversation storage, audits, and error logs.
- Only bounded evidence relevant to the current question is sent to OpenAI, with provider-side response storage disabled by the plugin.
- Orders, submissions, user records, credentials, raw builder payloads, and change snapshots are not sent to the model.
- Exact plans use a user-bound, single-use approval token that expires after ten minutes.
- Duplicate execution is blocked.

Site Agent cannot replace endpoint security, least privilege, patching, reliable hosting, or complete backups. It also cannot reliably see all hosting telemetry, DNS, vendor accounts, SaaS state, traffic, or server logs.

08 / SITE AGENT

A SAFE WORKING HABIT

Use this sequence for important work:

- 1 Back up the site.
- 2 Rebuild Knowledge after meaningful site changes.
- 3 Ask a focused question.
- 4 Request one clear change.
- 5 Review the exact plan and risk.
- 6 Execute once.
- 7 Verify the real front end and affected workflow.
- 8 Check History for the ledger entry and rollback status.

The guiding phrase is: **Ask your site anything. Tell it what to do.**