lodone

WORDPRESS / ENGLISH EDITION

Your website. Maintained with confidence.

User guide

Installation, daily operation and recovery procedures

FIVE CONNECTED SYSTEMS

Privacy and consent. Backups and recovery.
Security and integrity. Performance and images.
SEO and GEO.

WordPress 6.5+ | PHP 7.4+

lodone.com

READ, CONFIGURE, VERIFY

Contents

Product overview	3	Declaration and consent evidence	26
Requirements and navigation	4	Security checks and login guard	27
Three simple automation controls	5	Malware scan, quarantine and request firewall	28
Automatic optimization of future uploads	6	File integrity and approved baseline	29
Daily checks and login protection rules	7	Database maintenance	30
Review a finding and keep the file	8	SMTP setup and delivery	31
Install, assign and activate	9	Email two-factor authentication	32
First setup and Overview	10	Known vulnerabilities and daily checks	33
What a full backup contains	11	Performance audit and safe profile	34
Create, schedule and preserve copies	12	Browser performance history	35
Backup encryption and recovery key	13	Optimize selected images or all media	36
Restore and migration	14	Progress, savings and restoration	37
Recover after server loss	15	SEO and GEO: expanded audit	38
Verification and external export	16	Optional AI text generation	39
Connect your Dropbox account	17	Google Search Console reporting	40
Connect your Nextcloud account	18	Monthly SEO and GEO growth	41
Nextcloud uploads, progress and recovery	19	Compatibility and data handling	42
Automatic scheduling without visitors	20	A practical maintenance routine	43
Dropbox operation and recovery	21	Troubleshooting: access and recovery	44
Cookie scan and coverage	22	Troubleshooting: scan and optimization	45
Compare consent in the browser	23	Troubleshooting: monitoring	46
Blocking and banner configuration	24	Site acceptance checklist	47
Cookie languages and page selection	25		

Use the checklist at the end to assess results on your own website. A feature description and an operation status do not replace a real restore or user-journey test.

START HERE

Product overview

One administration area for privacy, recovery, protection, speed and search readiness.

Lodone brings essential WordPress maintenance tasks into a licensed plugin. It helps an administrator inspect the current state, make selected changes, preserve recovery copies and review the result. It is suitable for site owners who want these controls together and are prepared to review site-specific findings.

Area	Available functions
Cookies	Public URL discovery in resumable batches; recognised-service blocking; category choices; declaration and consent evidence; on-demand browser comparison of three consent states.
Backups	Database and wp-content archives; recorded file checksums; optional AES-256 encryption; recovery material; resilient progress, diagnostics and retry; automatic Dropbox and Nextcloud upload queues and central scheduling; optional manual WebDAV export.
Security	Configuration audit, login limits, selected hardening, email 2FA, integrity checks, malware-pattern scanning, confirmed quarantine, an optional request firewall, database maintenance and known-vulnerability monitoring.
Performance	Conservative public-page caching and delivery settings; saved browser measurements with before/after history; selected or whole-library image optimization with thumbnails and saved totals.
SEO and GEO	A site-wide 21-check technical audit, metadata and identity markup; compatibility with recognised SEO plugins; optional AI text generation and Search Console reporting.

Read results in context

A score or a completed operation is a report about the checks performed. It is not a security certification, legal assessment, guaranteed speed improvement or promise of search rankings. The detailed findings, errors and public website tests matter more than a single number.

> **Scope of this guide**
> This English guide explains installation and everyday use. Interface labels may differ with the selected language. Cookie banner and declaration language can follow the website automatically or be selected manually.

START HERE

Requirements and navigation

Confirm the environment before enabling changes.

Requirement	Why it matters
WordPress 6.5+ and PHP 7.4+	These are the declared minimum versions. Test on your actual hosting environment.
Administrator access	Protected administration actions require the manage_options capability and an active licence.
Writable storage and ZIP support	Full backups require PHP ZipArchive, readable source files and enough space for archives, temporary files and safety copies.
Outbound HTTPS	Needed for licensing, updates, official WordPress checksums and optional remote processing. Same-site HTTP requests support audits and scanning.
Working email delivery	Needed for email 2FA and alerts. Receiving a test message is the practical check.
Optional integrations	Dropbox and Nextcloud require HTTPS, storage in your own account and working scheduled tasks. Nextcloud also requires a public HTTPS WebDAV endpoint and an app password. Manual WebDAV needs cURL and HTTPS storage. AI generation, the vulnerability feed and Search Console require their own configuration.

Where the controls are

Menu	Key destinations
Lodone licence page	Activate licence or check it again; open available feature sections.
Overview / Monitoring	Module status and latest activity; known vulnerabilities, daily security automation and Google Search Console.
Backups	Create, import, restore and schedule copies; Recovery tab for server-loss guidance and manual export; Cloud storage for account connection and automatic transfers.
Cookies	Overview and scan, Settings, Declaration and Consent log.
Security	Audit, malware scan, quarantine, firewall, login protection, SMTP, email 2FA, logs, file integrity and database maintenance.
Performance	Server audit, delivery settings, browser test and image optimization.
SEO and GEO	Site-wide 21-check audit, content, identity and metadata settings.

There is no separate Maintenance and images menu in the plugin. Recovery belongs to Backups, file integrity and database maintenance belong to Security, and image optimization belongs to Performance.

EVERYDAY USE

Three simple automation controls

Enable routine work from Lodone > Automation. Technical options stay under Advanced.

1. **Automatically optimize new images**
   Enable this to queue future Media Library uploads and their generated thumbnails in the background. This is ongoing consent to send those images through the configured image service. Existing images are not processed retroactively.

2. **Automatically check security**
   Enable daily malware-pattern and file-integrity scans. A separate vulnerability-feed key is needed only for known-vulnerability data; missing that key does not stop local scans.

3. **Strengthen login protection**
   Enable progressive failed-login limits, tracking by IP, username and their combination, generic login errors, and a hidden bot trap on the standard WordPress login form.

4. **Save your choices**
   Select Save automation. Choices are per website. Existing independent security settings are retained; turning off the login enhancement removes its bot trap without disabling independently configured login limits.

> **Advanced controls**
> Expand Advanced to choose the image format and compression or open detailed security limits, report settings and vulnerability-feed configuration. Defaults retain the image format and use lossless compression.

PERFORMANCE

Automatic optimization of future uploads

A saved choice replaces repeated confirmation for new images.

In Automation, enable Automatically optimize new images, expand Advanced if you want WebP or AVIF instead of the original format, choose lossless or smart compression, and save. Smart compression can alter pixels; review its suitability for your content.

After WordPress generates an uploaded image and thumbnails, Lodone queues it for background processing. The browser upload is not held open for image optimization. Existing media can still be processed manually from Speed > Images. Rebuilding attachment metadata does not automatically queue the same upload twice.

The existing image worker processes each size, preserves originals, validates output dimensions and format, and records progress and savings. Review the latest job and persistent Total results under Speed > Images. A queued status is not a completed optimization. Restore originals from the same image screen if needed.

Active overlapping image optimizers pause automatic processing. Busy jobs or temporary start errors are retried up to twelve times at five-minute intervals. The Automation screen shows the latest queuing reason; processing errors appear in the image-job details. Correct the problem and run a manual optimization for any remaining images.

> **Requirements and transfer rules**
> An active licence, outbound HTTPS and working WordPress scheduling are required. Image bytes are transmitted for optimization under the saved consent. Disable the option to stop starting further automatic jobs; an already started job is separate. Original fallback remains; custom HTML and CSS backgrounds may need theme support.

SECURITY

Daily checks and login protection rules

Background checks report findings; they do not remove files.

Automatically check security starts a daily malware-pattern scan and file-integrity check. An already running scan is not restarted. Official WordPress checksum comparison needs access to the WordPress checksum service. Local change comparisons need a previously reviewed and explicitly saved baseline; automation does not silently trust a new baseline.

Known-vulnerability checks use the separately configured feed key. Without it, vulnerability coverage is unavailable while local scans remain scheduled. With it, feed errors are reported independently. Review scan completion, unreadable files, checksum errors and findings in Security; starting a check does not mean it completed.

Scheduled work uses WP-Cron and may run late without visits or a working host scheduler. The backup central wake-up service is not a universal guarantee for every security or image job. Configure optional report recipients and alerts in the advanced monitoring and integrity settings.

Strengthened login protection uses the existing configurable attempt threshold, time window and progressive lockouts. Defaults permit five failed attempts within fifteen minutes, with a fifteen-minute initial block and a configured maximum. Existing custom limits are retained. The hidden form field rejects submissions that fill a field intended to remain empty.

> **Scope and limitations**
> The bot trap targets automated submissions to the standard WordPress login form. It is not CAPTCHA, TOTP or passkey authentication, and does not guarantee bot detection. Custom login forms and API authentication do not gain a visible challenge. Email two-factor authentication remains a separate setting with its own mail requirements.

SECURITY

Review a finding and keep the file

Choose Reviewed - keep file when you have inspected a finding and trust the current contents.

1. **Inspect the exact file**
   Review its location, code, source and purpose. A PHP file inside uploads is a risk indicator, not conclusive evidence of infection. If unsure, seek help before trusting it.

2. **Keep a reviewed file**
   Select Reviewed - keep file on the finding. Administrator access, an active licence and a valid request nonce are required. The server checks the file against the scan SHA-256 before accepting the review.

3. **Review remains visible**
   The file stays in its original location and is labelled as reviewed. The decision records its exact content hash, reviewer and time. Findings remain visible rather than being silently deleted.

4. **Changed file or undo**
   A changed content hash invalidates the review; a new scan can flag it again. Use Undo review to remove a decision at any time. A file changed since the displayed scan cannot be approved from stale results.

Reviewed, unchanged findings are excluded from the unreviewed malware-alert count. Review is a local administrative judgement, not a malware-free certificate, and does not disable file-integrity checks or the request firewall.

> **Quarantine remains separate**
> Back up and quarantine still requires explicit confirmation and a full safety backup before moving the selected file. Keeping a reviewed file neither moves nor deletes it and creates no quarantine action.

START HERE

Install, assign and activate

A downloaded ZIP alone does not enable the licensed tools.

1. **Download the package**
   Sign in at lodone.com/dashboard/ and download the current WordPress plugin ZIP from your licence area.

2. **Assign the website**
   Use the website/domain assignment control in the customer account, enter the intended host and save it. Keep one licence for each website. If the licence is still unassigned, successful plugin activation can assign the current host automatically.

3. **Install in WordPress**
   Open Plugins > Add New Plugin > Upload Plugin. Choose the ZIP, select Install Now, then Activate Plugin.

4. **Activate the licence**
   Open Lodone, paste the licence code and select Activate licence. Confirm that the state becomes Active and that the feature sections open.

5. **Check the domain**
   Compare the assigned website in your customer account with the WordPress site you activated. Resolve any mismatch before configuring the tools.

Licence lifecycle

Without an active licence, protected features and actions are unavailable. Automatic status refresh is due after approximately six hours and depends on WordPress execution. A known licence expiry is checked locally. An explicit invalid response disables the licence; a temporary transport failure can retain a previously valid state for up to 72 hours from the last successful validation.

Stopping renewal leaves access for the paid period. When that period ends or the licence becomes invalid, protected functionality is disabled. Recheck the visible status after account changes rather than relying on an old activation message.

Changing a website or updating

Use Change domain in the customer account, save the target website and select Check licence again in WordPress. Before an update, download a full backup. Use the offered update or replace the existing plugin with the current ZIP. Do not delete it as an update method. Verify the version, licence and saved settings afterwards.

> **Acceptance check**
> An activation success message, the Active status, the assigned host and working feature access should agree. If they do not, stop configuration and follow the licence troubleshooting checks.

START HERE

First setup and Overview

Establish recovery and email before changing security or delivery settings.

Step	Action	Expected evidence
1	Activate the licence and inspect the version.	Active state, correct assigned website and working feature access.
2	Create and download a full backup.	Completed archive, recorded checksum and a usable copy outside the host.
3	Configure SMTP and receive a test email.	Success report plus the actual message in the intended mailbox.
4	Run the Security check and review safe protections.	Individual findings and a report of applied or skipped actions.
5	Review file integrity; approve a baseline only after inspection.	Official core status and a trusted local reference.
6	Scan cookies, classify services and connect the privacy page.	Completed scan without errors and a tested visitor choice flow.
7	Run Performance, establish cache ownership and test images.	One page-cache owner and a representative public-page check.
8	Review SEO/GEO and set backup and integrity schedules.	Reviewed public metadata and a routine for recovery copies.

Use Overview as a work queue

Overall status combines the latest available module results. Good, Warnings and Critical counts help prioritise review. Open the affected module for the finding, the time of the last check and the proposed action. Older results do not automatically describe the current state after a theme, plugin or hosting change.

Needs attention identifies next actions. Last activity helps distinguish a successful operation from a failed or incomplete one. Filters change the view of stored findings; they do not rerun a check.

> **Before automatic fixes**
> The security, performance and SEO safe-action screens request review and confirmation. Their backup warning is not itself evidence that a new backup was created. Create and download your own recovery point before applying these profiles.

RECOVERY

What a full backup contains

A recoverable WordPress package with a defined scope, rather than a complete server image.

Included material	Purpose
database/	WordPress database dump, packaged as SQL or a nested database archive. Treat it as sensitive data.
wp-content/	Readable content files such as plugins, themes, uploads and preserved image originals, subject to exclusions.
smartcare-manifest.json	Creation time, source URLs and paths, database prefix, WordPress/PHP versions, content counts and recorded checksums.
recovery/root/	Existing readable regular .htaccess, robots.txt and web.config files, with recorded hashes.
Safe configuration template	Selected WordPress settings in recovery/wp-config-safe-settings.php.txt, for manual review on the target host.
Environment inventory	Installed plugin and theme versions, active plugin/theme information and loaded PHP extensions.
Recovery instructions	A README describing preparation, restore, host-specific review and post-restore testing.

Exclusions and boundaries

WordPress core, the complete wp-config.php, operating system, hosting control-panel configuration, DNS, certificates, external mailboxes and arbitrary files outside wp-content are not copied. The .user.ini file is deliberately excluded. Reinstall a clean WordPress core and prepare target-host credentials during disaster recovery.

Known backup/download directories, generated caches, selected server-specific drop-ins, upgrade temporary folders and generated builder CSS are excluded to avoid recursive backups and unsafe migration of hosting-specific components. Symbolic links are not a dependable way to include external content. Review custom upload paths and unusual site layouts separately.

Sensitive data and encryption
Database credentials and authentication salts are omitted from the safe configuration export. Database options and plugin/content files can still contain API tokens, personal data or other secrets. Backup encryption is optional and off by default. Store every archive privately, whether encrypted or not.

RECOVERY

Create, schedule and preserve copies

A local backup is useful only while the host and its storage remain accessible.

1. **Create**
   Open Backups and select Create full backup. Allow database, file, archive and verification phases to complete.

2. **Inspect**
   Check Completed, creation time and SHA-256. Creation verifies the ZIP, manifest and database package; deeper SQL validation remains mandatory before restore. A failed operation is not a recovery point.

3. **Download**
   Download the completed copy. Confirm that the local file exists, has a plausible size and can be opened as an archive.

4. **Keep it outside the host**
   Store at least one recent copy on a device or storage location that will survive loss of the WordPress server. Keep the checksum with your recovery record.

Schedule control	Behaviour
Frequency	Disabled, Daily, Weekly or Monthly.
Day	Weekly offers a preferred weekday; Monthly offers the first or last calendar day.
Time	24-hour site time. Eligible Dropbox or Nextcloud setups use central wake-ups; outages can delay execution.
Retention	Local retention: 30, 60 or 90 days. Pending cloud transfers temporarily hold their source copies.
Save schedule	Stores the chosen frequency, day, time and retention. Check that a future run actually produces a completed copy.

Capacity and retention

Allow space for archives, temporary work and a full safety copy before restoration or database cleanup. Preserved image originals increase storage needs. Delete and Delete selected permanently remove the chosen archives after confirmation; keep an independent copy first. Retention does not prove that recent backups completed.

> **Downloaded does not mean safely stored**
> The Recovery screen warns when the latest full copy has not been requested for download. A download request does not prove that the file finished downloading or was stored outside the host. Verify the destination yourself.

RECOVERY

Backup encryption and recovery key

Choose encryption deliberately; it is disabled by default for new installations.

1. **Choose the setting**
   Open Backups > Encryption. Select Encrypt backup archives only if you want new backups protected with AES-256, then save the setting.

2. **Download the recovery key**
   When encryption is enabled, download the recovery-key file and store it separately from the website and backup destination. Do not keep the only copy beside the archives.

3. **Create and verify**
   New manual and scheduled backups follow the saved encryption setting, including copies uploaded to Dropbox or Nextcloud. Existing archives are not changed retroactively.

4. **Restore after server loss**
   On the same installation the stored key can be used. On a replacement installation, provide the recovery key when importing or restoring the encrypted archive.

Important limits

If both the original server and the separately stored recovery key are lost, the encrypted archive cannot be restored. If the host lacks the required encryption support, the plugin reports an error and does not present an unencrypted result as a successful encrypted backup.

Turning encryption off affects only future archives. Unencrypted backups still contain sensitive site data and require private storage and access control.

> **Default behaviour**
> The encryption checkbox is not selected by default. Review the operational trade-off before enabling it: encryption protects stored archives, while recovery depends on preserving the separate key.

RECOVERY

Restore and migration

Importing an archive adds a recovery point; it does not restore the website automatically.

1. **Prepare**
   Choose the correct full Lodone ZIP and download an independent copy. Prefer a staging rehearsal before restoring a live site.

2. **Import if necessary**
   In Backups, choose the archive and select Upload and verify. Chunked upload supports interrupted transfers. Wait for a completed history record.

3. **Reduce concurrent writes**
   Avoid new orders, account changes and form submissions during restoration. Use a maintenance window suitable for the website.

4. **Confirm restore**
   Read the overwrite warning, tick the confirmation and choose Restore for the intended backup. A full safety backup is created before the restore proceeds.

5. **Follow progress**
   Wait for verification, files and database work to finish. Keep the page open during the active operation and inspect errors before retrying.

6. **Test and preserve evidence**
   Check administrator login, pages, media, permalinks, forms and checkout. Retain both the source archive and the safety copy.

What changes during a restore

Restoration writes archive content into wp-content and imports the database. Migration logic handles supported database-prefix, URL and path replacements, including serialised values. Cache and host-specific generated files are handled separately. Root files are not automatically overwritten by a normal content/database restore.

Do not assume a restore removes every extra file already present on the target. A clean destination is preferable after a suspected compromise. Unusual plugins, absolute links embedded in custom code and external services need site-specific verification after migration.

> **Recovery is not a transaction across the whole site**
> The safety copy provides a recovery point, but restoration changes multiple files and database tables. A timeout, incompatible host or file-permission error can leave an incomplete result. Read the operation report and use the retained copies and hosting access to recover deliberately.

RECOVERY

Recover after server loss

You need an accessible off-server archive and a new working WordPress installation.

1. **Find the independent copy**
   Retrieve the recent full ZIP from outside the lost server. A copy kept only on the lost server cannot help.
2. **Prepare the target host**
   Use the recorded WordPress version as the starting point. Create a new database and a new wp-config.php with target-host credentials and new authentication salts.
3. **Install and license Lodone**
   Install the plugin on the target. Assign the licence to that domain in the customer account and activate it.
4. **Import and restore**
   Open Backups, upload and verify the full archive, then confirm Restore. Allow the safety-backup and restore phases to finish.
5. **Review configuration**
   Read the safe configuration template and apply only appropriate settings. Inspect archived .htaccess, robots.txt and web.config before optionally restoring selected roots in Backups > Recovery.
6. **Re-enter protected credentials**
   New authentication salts can make previously encrypted SMTP, WebDAV, cloud or AI credentials unreadable. Re-enter protected credentials, reconnect cloud accounts and test the integrations.
7. **Validate the website**
   Test login, permalinks, media, forms, email, scheduled tasks and payment integrations. Check a controlled order flow before reopening a store.

Optional root-file restoration

In Recovery, choose the full backup and select only the available root files you have reviewed for the new host. Confirm the overwrite. Recorded root checksums are checked and a full safety copy is created first. An Apache rule file is not automatically appropriate for a different web-server configuration.

> **Make recovery measurable**
> Record the archive used, the rehearsal host, start and finish times, checks performed and unresolved issues. Archive validation establishes structural evidence; a successful restore rehearsal establishes that this particular website can operate after restoration.

RECOVERY

Verification and external export

Understand what the checks prove and what remains your responsibility.

Check	Evidence and boundary
Archive consistency	Opens the ZIP, reads entries and checks lengths. Unsafe paths are rejected.
Recorded file hashes	Checks recorded SHA-256 values and verifies that expected entries exist. This detects differences from the recorded archive data.
Database content	Checks the database archive/checksum and validates supported SQL structure. It does not run a full restore rehearsal.
Download checksum	Compares the stored archive checksum before serving the download.
Limits of hashes	A checksum does not prove that the original website was clean. Someone able to alter both archive content and its manifest may also change the recorded hashes.

Manual export to an existing WebDAV folder

1. **Configure**
   In Backups > Recovery, enter your public HTTPS WebDAV folder, username and password. Enable manual export and confirm the configuration.

2. **Export**
   Select a completed full backup and confirm Export selected copy. The archive is streamed to the configured folder; the local copy is retained.

3. **Verify externally**
   The interface records a successful upload response. Open your storage, check the file and preferably retrieve it for a checksum or archive check.

WebDAV remains optional manual export. Automatic Dropbox transfers use the separate Cloud storage tab after you connect your own account and enable uploads. It creates no storage subscription. You must supply an existing reachable destination and sufficient quota. The implementation requires cURL, a public IPv4-resolvable host, valid TLS and a WebDAV endpoint that accepts the upload without redirects.

Storage passwords are encrypted using the installation security keys. Re-enter them after migration to an installation with new salts. An upload failure leaves the local archive available; do not treat a failed export as an external recovery copy.

RECOVERY

Connect your Dropbox account

Your website sends backups to your own Dropbox account and storage.

1. **Connect**
   With an active licence, open Backups > Cloud storage and choose Connect account under Dropbox. Sign in to your own Dropbox and review the requested access. Return to the same signed-in WordPress administrator session over HTTPS.

2. **Enable automatic uploads**
   Select Automatically upload new backups. Connecting the account alone does not turn this on. Choose Keep latest cloud copies (1-100; default 10) and whether to email the site administrator after repeated failure. Select Save preferences.

3. **Set creation separately**
   Open Schedule and retention. Choose Daily, Weekly or Monthly, then the time in the WordPress site time zone and local retention. Save the schedule. Upload settings do not by themselves create new backups.

4. **Confirm automatic scheduling**
   Return to Cloud storage and check Automatic scheduling. Active - central connection is working means the eligible site is registered and a recent central check reached it. No hosting cron configuration is needed for this setup.

5. **Verify the first copy**
   Create a full copy or choose a completed existing copy and Add to upload queue. Wait for Uploaded and 100%. Open Dropbox, locate the archive in the Lodone app folder and retrieve it to verify the file.

Access, storage and account ownership

The configured Dropbox integration is restricted to its application folder. Review this scope on the consent screen. The app folder name follows the registered application name, Lodone Backups. Each customer authorizes their own account; the Lodone owner registers the integration once, and customers do not need to create API keys.

Your Dropbox quota, account policy and service availability apply. The plugin does not supply a storage subscription. Automatic cloud uploads support Dropbox and Nextcloud; manual WebDAV export is a separate workflow.

> **Three separate switches**
> For automatic creation and upload without visitors you need an active licence, a connected Dropbox or Nextcloud account with automatic uploads saved as enabled, and an enabled backup schedule. Connected does not mean that all three conditions are satisfied.

RECOVERY

Connect your Nextcloud account

Send backups directly to your own Nextcloud storage.

1. **Prepare your account**
   Use your own Nextcloud account with enough available space. Lodone does not supply storage. A provider may offer a free allowance; account terms and quotas belong to that provider.

2. **Copy the WebDAV URL**
   In Nextcloud Files, open Settings and copy the WebDAV address. It must be a public HTTPS URL ending in /remote.php/dav/files/your-account-id/. Do not use the dashboard address.

3. **Create an app password**
   In your Nextcloud account security settings, create a dedicated app password for Lodone. Use the account username and this app password, rather than sharing your main login password.

4. **Connect in Lodone**
   Open Backups > Cloud storage > Nextcloud. Enter the WebDAV URL, username and app password, then select Connect and check. Confirm that the connected state appears.

5. **Enable automatic upload**
   Select Automatically upload new backups, choose how many cloud copies to keep and optionally enable failure email notifications. Save the settings. Connecting alone does not enable automatic uploads.

6. **Choose the backup schedule**
   Save a Daily, Weekly or Monthly backup schedule if you also want automatic creation. To transfer an existing completed copy, select it and add it to the upload queue.

> **Keep the recovery key separately**
> If backup encryption is enabled, the encrypted archive is uploaded unchanged. Keep its recovery key outside the website and separately from your only backup copy.

RECOVERY

Nextcloud uploads, progress and recovery

Backup creation and remote upload are separate operations.

Nextcloud uploads run in the background in resumable chunks. You may leave the cloud screen after queuing a completed copy. Progress, queue length and the most recent status are retained. A connected account or a partially uploaded file is not a completed remote backup.

Control or result	Meaning
Uploading / progress	The archive is still being transferred. Large files can require many worker runs; check for continued progress or a recorded error.
Successful upload	The transfer and final remote-file size check completed. Open Nextcloud Files > Lodone > the website-specific folder to locate the archive.
Automatic scheduling	With connected storage, automatic upload and a saved backup schedule, central wake-ups can run eligible backup tasks without visitors. The website, scheduler and storage must remain reachable.
Retries and errors	Temporary failures are retried a bounded number of times. Review the reason after repeated failures, fix credentials, quota or connectivity, and queue the copy again.
Keep latest cloud copies	After a verified new upload, retention removes older successful Lodone copies recorded for this website according to the saved limit. Unrelated Nextcloud files are not retention targets.
Disconnect	Stops future use of that connection. Existing remote archives remain in the storage account. Dropbox settings remain independent.

To recover after server loss, download a completed archive from your Nextcloud account, prepare WordPress and activate Lodone, then upload, verify and restore the copy through Backups. Supply the separate recovery key for an encrypted archive.

> **Credentials and transfer path**
> Nextcloud credentials are encrypted on this WordPress installation. Archive bytes travel directly from your website to your Nextcloud over HTTPS; they do not pass through the Lodone connection service.

RECOVERY

Automatic scheduling without visitors

The Lodone service wakes WordPress; archive creation and transfer stay on your website.

Stage	What happens
1. Eligibility	The plugin checks the active licence, enabled Daily/Weekly/Monthly schedule, connected Dropbox or Nextcloud account and enabled automatic uploads. It registers the eligible website with the Lodone service.
2. Wake-up	The Lodone hosting worker runs every minute and sends authenticated checks to registered sites when due. Requests use per-site signing, timestamps and one-time nonces.
3. Local execution	The plugin verifies the request and asks WordPress cron to run due jobs. Native locking limits overlapping cron execution. This does not require a visitor or an open administration tab.
4. Backup and upload	WordPress creates the archive locally. Completed copies enter each enabled cloud queue and upload directly to your connected account.

Read the Automatic scheduling panel

Status	Meaning and next action
Off	One or more eligibility conditions are missing. Connect Dropbox or Nextcloud, enable and save automatic uploads, enable and save a schedule, and check the licence.
Waiting for the central connection	Registration or a recent check is missing. Keep the site publicly reachable over HTTPS; allow the scheduling endpoint through access rules. If this persists, contact support.
Active	The eligible site is registered and a central check arrived within the last ten minutes. Inspect Last central check and the separate completed-backup/upload status.

Active confirms the connection, not a finished backup. The site, cron endpoint and connected storage must remain reachable. Hosting limits and outages can delay jobs. WordPress scheduling remains a fallback, which can also be delayed without visitors or host cron.

> **No archive relay through Lodone**
> The central scheduler receives licence, domain, callback and scheduling authentication data; it does not relay the backup archive. Disabling the schedule or automatic uploads, disconnecting all eligible cloud storage or losing licence eligibility stops central backup wake-ups. This feature does not replace all unrelated WordPress background-task scheduling.

RECOVERY

Dropbox operation and recovery

Review upload progress separately from backup creation and central connection status.

Behaviour	Meaning
Background transfer	Workers send bounded chunks with a concurrency lock. You may close the administration page. Central wake-ups help run due jobs on eligible sites.
Credential lifecycle	OAuth uses expiring state, PKCE and one-time redemption. App secrets stay on the Lodone server. Client tokens/session data are encrypted with WordPress installation keys.
Token renewal	Access tokens refresh automatically using the offline token. Revoked consent or a provider/account policy change can require reconnection.
Status and retry	Shows queue, percentage, status and time. Failed attempts use increasing delays; five consecutive failed attempts leave Failed and email an opted-in administrator. Successful chunk progress resets that attempt count.
Cloud retention	After a new upload succeeds, older remote IDs recorded as successful uploads from this installation are removed to satisfy the saved count. Unrelated files are not purged.
Changing accounts	A changed account identity clears the queue and retention history. Enable automatic uploads again. Existing files stay in the previous account.
Disconnect	Removes local credentials and pending transfers. It does not delete existing Dropbox files or revoke provider consent; revoke access in Dropbox separately if required.

Upload evidence and recovery

Before transfer, the archive is checked against its stored SHA-256. Completion requires a provider file ID and matching remote byte size. A lost final response may be reconciled by unique filename and size. Uploaded is transfer evidence; retrieve a copy for independent checksum/archive verification.

Dropbox receives the website-produced archive: AES-256 encrypted only when that setting was enabled. Preserve the separate key for encrypted copies. After server loss, retrieve the archive and follow the import/restore procedure. Protected restoration still requires an active licence.

PRIVACY

Cookie scan and coverage

The scanner discovers public URLs and continues in batches; the previous small-page scan limit no longer defines the queue.

1. **Start**
   Open Cookies > Overview and scan, then select Scan website.
2. **Allow discovery**
   The queue collects public posts, pages, products and other public post types, taxonomy and post-type archives, conventional sitemaps and linked same-site public pages.
3. **Inspect progress**
   Read checked/discovered URL counts, failed URLs and unchanged content. Discovery can add URLs while a job runs.
4. **Resolve failures**
   Inspect every failed URL and reason. Correct reachability, response or sitemap issues, then rerun the scan.
5. **Review services**
   Open Declaration, classify detected services and verify the live website before enabling consent.

Later scans and continuation

The job is saved between requests. Cron and the open administration screen advance it in bounded work units. Scan website resumes an active queue. On a new run, unchanged content can skip repeated classification using a fingerprint of returned HTML and cookie headers; requests still have to retrieve the content. Select Inspect unchanged content again when you need a fresh classification pass.

Coverage has a specific meaning

The denominator is the discovered public URL list, not proof that every possible route or visitor state was inspected. Private/password-protected content, login-only journeys, JavaScript-only routes and external hosts are outside that list. Scanned requests do not perform authenticated purchases or execute page JavaScript.

Responses exceeding the inspection limit, failed requests and unsupported redirects are reported. The scanner uses the current website host and port; routes on a separate host are not silently included. Review a catalogue of important journeys, especially contact forms, embeds, product, cart, checkout and account pages.

> **Completion with warnings**
> Processed URLs include failed attempts. A completed scan with unreachable URLs can still enable consent, while those URLs remain visible as warnings. Review the failure list and test important journeys before relying on the coverage figure.

PRIVACY

Compare consent in the browser

Run the page JavaScript on selected public same-site URLs in an isolated browser context.

1. **Prepare**
   Use a supported Chrome or Edge browser. Open Cookies > Overview and scan > Compare in browser. Review the selected public URLs; one run supports up to 20.

2. **Start and keep the tab open**
   Run the comparison. Each URL is loaded in isolated frames for Before consent, Reject all and Accept all. The probe observes resources and storage names, and scrolls to trigger some lazy content.

3. **Inspect phase differences**
   Recognised optional services observed before consent or after rejection require investigation. Services may load after acceptance. Unknown observations are for manual review, not automatically a pass.

4. **Read completeness**
   Unsupported browser isolation, frame/CSP failures, missing consent actions and timeouts produce incomplete results. Correct the cause before relying on the comparison.

5. **Preserve and retest**
   Results remain visible after reload. Review important desktop/mobile journeys and rerun after changing scripts, tags, consent settings or cache behaviour.

Observed evidence	Boundary
Resources	Page-visible resource requests/types, with query/fragment data removed. This is not privileged network interception.
Cookies and storage	Same-origin names/events; values are not retained. HttpOnly cookies, cross-origin frames and inaccessible storage are outside scope.
Execution window	JavaScript runs for a bounded period. Long delays, unperformed clicks, logged-in routes, server-side tracking and other visitor states can be missed.
Consent state	Real Lodone Before/Reject/Accept actions are exercised. Audit choices are excluded from the ordinary visitor consent log.
Isolation	Credentialless frames require browser support and compatible site policies. An unsupported setup fails closed and must not be interpreted as clean.

Meaning of a clean result
No recognised warnings means none were observed for the tested URLs, phases, browser and time window. It does not establish complete website coverage or legal compliance. Combine it with server-scan coverage, manual classifications and real user-journey checks.

PRIVACY

Blocking and banner configuration

Connect service classification, prior blocking and visitor choices.

Control	Effect
Consent interface	After scan and configuration, consent and prior blocking enable automatically. Administrators normally only adjust settings.
Prior blocking	Blocks recognised optional scripts and embeds until the associated category is allowed.
Consent Mode v2 signals	Supplies consent-state signals for supported Google tags; review the tag setup separately.
Consent display and size	Centred popup or responsive bottom bar. Small is the default popup size.
Button colours	Configures primary/secondary action colours and calculated text/hover contrast.
Policy version	Change after material purpose or privacy-policy changes to request a new visitor choice.
Consent validity	30-365 days for saved visitor choices.
Proof retention	30-1095 days for recorded consent evidence.
Privacy page	Select a published page. Optional automatic declaration append is disabled by default.
Hide preference button by device	Affects the floating preference button for desktop, tablet or mobile. Keep an accessible alternative to change consent.

What the blocker can and cannot do

Server-side inspection identifies scripts, embeds, known markers and cookie response headers. The live blocker also observes recognised resources inserted into the visitor page. This improves handling of dynamic additions, but it is not a guarantee that arbitrary custom tracking code is understood. The separate browser comparison executes page JavaScript on selected public URLs within its documented observation window.

A recognised-service block does not stop every possible server-set cookie, custom inline request, third-party tag configuration or storage mechanism. Review unknown services and test real browser network/storage behaviour. Cache, tag-manager and script-delay settings can affect when consent code runs.

> **Test before public reliance**
> In a fresh browser session, reject optional categories and check important pages before consent. Then allow one category, verify the expected service, and withdraw it. Test on mobile and desktop. This is technical validation, not a legal-compliance certificate.

PRIVACY

Cookie languages and page selection

Choose automatic language handling or a fixed language for consent content.

At the top of Cookies > Settings, use the separate administration-language and public-language dropdowns. Automatic administration language follows the WordPress backend language. Automatic public language follows the website locale. A manual choice overrides the corresponding automatic setting. Save cookie settings at the bottom.

The cookie banner and generated cookie declaration support all 24 official EU languages: Bulgarian, Croatian, Czech, Danish, Dutch, English, Estonian, Finnish, French, German, Greek, Hungarian, Irish, Italian, Latvian, Lithuanian, Maltese, Polish, Portuguese, Romanian, Slovak, Slovenian, Spanish and Swedish. This does not translate the website content or third-party plugins.

The selected public language applies to consent labels, category descriptions and generated declaration wording. Check any custom banner text you entered yourself and review the public page after changing language.

1. **Choose the declaration page**
   The WordPress privacy-policy page is selected by default. Pick another published page in the page dropdown if preferred.

2. **Save general settings**
   Select Save cookie settings at the bottom. Open the chosen public page to review the generated list.

3. **Classify services**
   Changing a category in Declaration saves that individual selection automatically. Wait for confirmation. General settings and the page/language selection still require their save button.

> **Recognition and consent**
> Known services are classified by the Lodone catalogue. Unknown entries need review. Functional language preferences such as pll_language are blocked until the matching consent when managed by the supported integration. Recognition alone does not establish full legal compliance.

PRIVACY

Declaration and consent evidence

Review classifications rather than assuming the scanner knows every purpose.

Necessary covers essential sessions, security, cart and consent choices and is always active. **Functional** covers optional functions and embeds. **Statistics** covers usage analytics. **Marketing** covers advertising measurement and personalisation.

Changing a service category in Declaration saves that category automatically. Wait for the saved confirmation; if saving fails, correct the error and retry. General cookie settings use their own Save cookie settings button at the bottom.

Visitor controls

Button	Outcome
Accept all / Reject all	Allows all optional categories, or keeps only Necessary, and records the choice.
Choose settings / Save choices	Opens granular choices and saves the selected combination.
Cookie settings	Reopens preferences so the visitor can change or withdraw consent.
Withdraw optional consent	Withdraws optional choices and attempts to clear recognised optional cookies. It cannot erase inaccessible third-party storage.
Privacy policy	Opens the selected privacy information.

Evidence and publication

Consent log shows recorded actions, category choices, policy version and timestamps. Use Download CSV proof log for an audit export. Consent identifiers are stored as one-way SHA-256 hashes; the consent log does not store raw IP addresses or browser identifiers. Other WordPress plugins or the host may maintain their own logs.

Use the shortcode displayed by the Declaration tab to place the generated service list on a page, or enable the optional append on the selected privacy page. The generated list does not replace a privacy notice that explains the actual processing and relevant parties.

> **After changing tracking**
> Rerun the scan, inspect new and unknown services, review the privacy information and test rejection again. Update the policy version when a renewed choice is appropriate. A service list is only as useful as its classifications and the tested integration.

PROTECTION

Security checks and login guard

Review the assessment, then enable only protections appropriate to the site.

Run security check evaluates signals such as HTTPS, WordPress/plugin updates, PHP, exposed debug settings, file editing, login controls, headers, administrator accounts, email 2FA and available recovery copies. Passed means the particular check found the expected state at that time; it does not mean that the whole site is secure.

Setting or action	Behaviour
Apply safe protections	After confirmation, enables generic login errors, dashboard file-editor restrictions, baseline headers and login tracking. Review the applied/skipped report.
Failed-login guard	Temporarily blocks repeated failed attempts. Configure an attempt limit of 2-50 and a counting window of 1-1440 minutes.
Lockout duration	Initial block 1-1440 minutes; maximum 15-10080 minutes. Progressive doubling can increase repeated blocks up to the maximum.
Tracking signals	IP, username and their combination use one-way hashes for repeated-attempt detection.
IP source	Use the server address by default. Select Cloudflare only when public traffic reaches the origin through that trusted proxy path.
Alerts and retention	Optional administrator alert when a new block starts; configurable security-event retention of 1-365 days.
Unblock	Removes the selected active login restriction.
Authenticated XML-RPC	Optional manual hardening. Not disabled automatically because trusted integrations may need it.

Activity records

Security activity includes plugin activation/deactivation, administrator creation, user-role changes and selected important setting changes. The logs also contain module operation results. It is a selected event history, not a complete forensic record of every server or WordPress action.

> **Security boundary**
> These tools reduce specific account, file and request risks. The request firewall runs inside WordPress and the pattern scanner is not a vulnerability database, server-edge firewall, complete antivirus engine or automatic incident-cleanup system. Keep WordPress, plugins, themes and hosting access maintained independently.

PROTECTION

Malware scan, quarantine and request firewall

Inspect suspicious code and request patterns without treating every match as a confirmed compromise.

1. **Run and review**
   Open Security and start the malware-pattern scan. Review each path, matched pattern, context and risk level. A match is evidence to inspect, not a malware verdict.

2. **Quarantine deliberately**
   For a reviewed suspicious file, confirm the action. Lodone first requires a completed full safety backup, then moves only that file and records a restorable quarantine entry.

3. **Test the website**
   After quarantine, check administration and the affected public features. Restore the exact item from the quarantine list if an authorised feature breaks, then investigate its trusted source.

4. **Configure and monitor**
   Enable the optional request firewall only after review. Test forms, API callbacks, uploads and checkout; then monitor security events and rate-limited email alerts.

Coverage and limits

The scanner covers supported plugin, theme and uploads files for suspicious PHP constructs, encoded payloads, backdoor-style indicators and executable uploads. Exclusions reduce known false positives but cannot prove that a file is safe.

The firewall blocks selected suspicious request patterns inside WordPress and can protect executable uploads. It does not filter traffic before PHP or replace hosting/CDN protection, a vulnerability database or a complete antivirus engine.

> **If compromise is suspected**
> Preserve evidence, restrict access, rotate credentials from a clean device, replace affected code from trusted sources and review the host. Do not approve a new integrity baseline or restore a quarantined file until the cause is understood.

PROTECTION

File integrity and approved baseline

Compare core with official hashes and plugin/theme changes with a reviewed local reference.

1. **Run Check files**
   Open Security > File integrity. The job requests official checksums for the installed WordPress version and locale, then reads files in batches.

2. **Review the report**
   Inspect official core matches, core differences, new/changed/removed files, unreadable paths and any checksum-download error.

3. **Approve a baseline carefully**
   On a reviewed installation, confirm Create approved baseline. It is saved only after successful core verification and without core differences or unreadable paths.

4. **Schedule and alert**
   Optionally enable weekly checking and email changes to the WordPress administrator. Save the schedule and test email delivery.

Coverage and trust

The scan covers wp-admin, wp-includes, plugin and theme directories, root PHP files except wp-config.php, and additional official core-manifest entries. It skips symbolic links. It is not a recursive scan of every uploads file, custom directory, wp-config.php setting or server file.

Core uses the official WordPress checksum reference. Other scanned files use local SHA-256 values. The baseline has an authentication signature tied to WordPress salts; changing salts can invalidate it. A plugin or theme baseline says what existed at approval time, not whether that code is free from malicious logic.

Responding to differences

Expected updates can create many legitimate changes. Compare paths with the intended update and obtain clean files from trusted sources when a core difference is unexpected. Investigate before approving a replacement baseline. Creating a new baseline replaces the comparison reference and can hide previously unexplained changes.

> **Integrity is separate from malware review**
> The integrity report does not delete or repair files. Quarantine is available only from reviewed malware findings and requires a separate confirmed workflow. A clean integrity result is evidence for this check and coverage, not a malware verdict.

PROTECTION

Database maintenance

Remove reviewed obsolete records, with a full safety copy before deletion.

Open Security > Database and select Analyze database. Analysis is read-only. It creates a temporary reviewed batch for the current administrator; select the categories you intend to remove and confirm only after reading the records and counts.

Category	Eligibility and per-analysis limit
Expired temporary data	Expired transient timeout records; up to 500 in a reviewed batch. Related temporary values are deleted through WordPress APIs.
Post revisions	Revision records older than 30 days; up to 200. These are historical edits, not the current published post.
Trashed posts	Non-attachment posts in the trash older than 30 days; up to 200. Removing them is permanent.
Spam comments	Comments marked as spam older than 30 days; up to 200.
Large autoloaded options	Reports the 20 largest automatically loaded options by byte size. It does not delete or change them.
Overdue cron	Reports hooks more than one hour overdue. It does not repair, delete or automatically rerun those jobs.

1. **Review**
   Select only the eligible categories you understand. The analysis snapshot expires after 30 minutes.
2. **Back up and clean**
   Confirm the action. Lodone first creates a full backup; deletion proceeds only after that succeeds.
3. **Read actual counts**
   Eligibility is rechecked against the reviewed records. Reported removals can be lower than the analysis count if records changed.
4. **Repeat if needed**
   Run a new analysis for another batch. Keep the safety-backup ID and verify the site after cleanup.

What cleanup does not mean
This does not optimise every database table, remove all plugin leftovers, change autoload settings or promise a measurable speed gain. Revisions and trash can be useful recovery material; select them only when you accept losing that history.

PROTECTION

SMTP setup and delivery

Confirm receipt in the intended mailbox before relying on alerts or email challenges.

1. **Configure SMTP**
   Enable authenticated SMTP. Enter server hostname, port, SSL/TLS setting, username, password and permitted sender address/name. Follow your mailbox provider configuration.

2. **Save and test**
   Save settings, enter an accessible test recipient and send a test email. Check both the operation report and receipt in the destination mailbox.

3. **Verify user email**
   Check the WordPress user profile address for each user who will receive a login code. The SMTP sender is not automatically the code recipient.

Control	Meaning
Port and encryption	Common combinations are 465/SSL and 587/TLS; use the provider-approved combination.
SMTP password	Encrypted using the installation security keys. New salts after migration can require re-entry. Some providers require an application password or different authentication method.
Sender identity	Use an address your provider permits. A valid account password does not mean any sender domain is accepted.
Test recipient	An accessible real address where you can confirm delivery, not merely a syntactically valid mailbox string.

Delivery and coverage boundaries

A successful send means the transport accepted the operation; it does not prove inbox placement. Check spam, mailbox filters and the actual recipient address. The challenge applies to supported interactive WordPress login; API/application-password paths are not a universal email-2FA barrier.

> **Authentication error or sender rejection**
> Read the specific SMTP error. Verify the full mailbox username, provider credentials, sender identity, encryption and permitted port. Correct domain spelling and account addresses before retrying; avoid repeated blind password changes.

PROTECTION

Email two-factor authentication

Protect supported interactive login with a second email-code step.

1. **Prepare delivery and recovery**
   Complete SMTP setup and receive the test message. Check the protected user's actual WordPress email address. Keep a tested administrator recovery path.
2. **Enable for the user**
   In the Security two-factor section, select Enable for the intended account after the successful SMTP test.
3. **Test a fresh login**
   In a separate signed-out session, enter the account password, receive the email code and select Confirm login.
4. **Review the outcome**
   Confirm that the code goes to the protected user and that a correct challenge allows login. Do not protect every administrator until this workflow works.

Control	Behaviour
Code limits	Six-digit code, 10-minute lifetime and at most five verification attempts.
Send a new code	Subject to a 60-second delay and a limit of three sends within the challenge.
Cancel and sign in again	Ends the current challenge and returns to password login.
Disable	Stops the challenge for the selected user after confirmation.
Invalid user email	A valid account address is required so the challenge has a usable recipient.

Know the protected entry point

The email challenge applies to supported interactive WordPress login. API and application-password paths are not a universal email-2FA barrier. Maintain strong credentials and manage alternate application access independently.

> **If a code does not arrive**
> Check the protected user's address, transport error, spam folder and mailbox rules. The test recipient and SMTP sender can differ from the login-code recipient. A successful send report alone does not prove inbox delivery.

PROTECTION

Known vulnerabilities and daily checks

Compare installed component versions with a current advisory feed and automate recurring review.

1. **Configure the feed**
   Open Monitoring > Automation and enter a Wordfence Intelligence API feed key. The key is stored encrypted on this WordPress installation.
2. **Run the first check**
   Open Monitoring > Vulnerabilities and select Check now. Installed WordPress, plugin and theme versions are compared with the current scanner feed.
3. **Read each finding**
   Review risk, component, installed version, advisory title and the recommended patched version. If no patched version exists, disable and replace the affected component after testing.
4. **Enable daily checks**
   In Automation, enable daily checks, set the report email and save. The background job also starts the malware-pattern scanner.
5. **Verify the schedule**
   Review the displayed next-run time and confirm that a later report has a new timestamp. WordPress scheduled execution must be working.

Alerts and interpretation

Email is sent only when a new problem is found or an automated check fails. No email is not proof that a scheduled run happened; inspect the stored check time and reports. A feed result describes known published vulnerabilities associated with the detected version. It does not prove exploitability on this site or detect every unknown weakness.

Update or replace affected components through a controlled workflow: create a recovery point, review compatibility, apply the trusted update, clear caches and rerun both the vulnerability and malware checks. Do not treat a clean advisory report as a penetration test or a substitute for supported software and hosting controls.

> **External dependency**
> The vulnerability check requires the configured feed and outbound HTTPS. Feed availability, advisory coverage and version matching can affect results. The API key and report mailbox are site-specific operational settings.

SPEED

Performance audit and safe profile

Use one page-cache owner and test the public website after changing delivery.

Run performance check requests the front page twice and reviews internal response time, caching, compression, browser-cache signals, HTML size, initial CSS/JavaScript, autoloaded options and object-cache signals. The summary is Lodone findings, not a public PageSpeed or Core Web Vitals score. An internal request does not represent every visitor device or network.

Setting or action	Effect
Apply safe profile	After confirmation, removes the legacy emoji payload and enables conservative page caching only when no recognised provider owns that layer.
Enable selected optimizations	Master switch for the chosen Lodone performance options.
Public HTML page cache	Available when a recognised overlapping cache provider is not active.
Cache lifetime	1, 6, 12 or 24 hours.
Browser-cache rules	Adds supported static-asset rules on Apache/LiteSpeed-style hosting.
gzip fallback	Requires server support for the relevant compression module.
Additional excluded paths	One relative site path per line; built-in dynamic-request protections remain.
Clear page caches	Clears Lodone and supported provider caches. A host/CDN cache may still require its own purge.

Dynamic-request protection

Recognised cart, checkout, account, session, callback, AJAX, REST and logged-in requests bypass the page cache. Keep ecommerce protection in place and test your own custom dynamic routes. Do not cache personalised output merely because the generic front page works.

> **Conservative changes**
> The safe profile does not aggressively combine, minify or delay CSS/JavaScript. These changes can affect forms, embeds and checkout. When another recognised cache provider owns the layer, Lodone avoids duplicate ownership and does not reconfigure that plugin automatically.

SPEED

Browser performance history

Save comparable before-and-after results from the device and connection used for the test.

1. **Prepare a consistent test**
   Use the same browser, device, connection and cache state for comparisons. Close unrelated heavy tasks and test a representative public home page.

2. **Run the browser test**
   Open Performance > Browser test and start the measurement. Lodone loads the public home page and records the result locally in WordPress.

3. **Read the metrics**
   Review LCP, CLS, TTFB, DOM ready, full load time, resource count, transferred data and oversized-image count.

4. **Compare carefully**
   Apply one intended optimization, clear relevant caches and repeat the test. Use the saved history and before/after comparison with consistent conditions. Inspect forms, account and checkout separately; a faster home page does not prove every route improved.

Metric	Interpretation
LCP	Largest Contentful Paint. Up to 2500 ms is a useful target. A leading approximation marker means the browser used its documented paint fallback because LCP was unavailable.
CLS	Cumulative Layout Shift. Up to 0.1 is a useful target; user interaction and dynamic content can change the observed value.
TTFB	Time to First Byte observed by this browser for this request. It includes the current network and server conditions.
DOM ready / Load	Milestones for document readiness and the load event; neither alone is a complete user-experience score.
Resources / transferred	Counts and transfer volume visible to this run. Browser cache and third-party responses affect the result.
Oversized images	Images whose delivered dimensions or payload merit review; inspect the actual visual role before changing them.

Comparable, not universal
The saved result is a local diagnostic, not a laboratory PageSpeed report or field Core Web Vitals dataset. Compare repeated tests on the same setup and confirm improvements with real public-page behaviour.

SPEED

Optimize selected images or all media

Choose scope, format and compression, then explicitly approve processing.

1. **Open Image optimization**
   Go to Performance > Image optimization. Resolve any warning about an active overlapping image optimizer.
2. **Choose the scope**
   Entire media library includes supported media attachments and their registered thumbnails. Only selected images uses the selected items in the displayed list.
3. **Choose the output**
   Keep original format, WebP or AVIF. Choose Lossless or Smart compression; smart processing can alter pixel detail.
4. **Confirm the transfer**
   Read and tick the approval for external image processing, including thumbnails. Select Optimize images.
5. **Follow the job**
   Discovery prepares the library; processing advances through file-size tasks. Inspect the progress and errors. Use Resume if the active job needs another step.
6. **Inspect the public result**
   Compare representative photos, text in graphics, transparent images and product details. Check mobile and desktop, then clear relevant page caches.

Supported inputs and safe writes

Local JPEG, PNG, WebP and AVIF attachments are supported. Each source must fit the supported per-file size limit and contain no more than 40 megapixels. Files must be inside the local WordPress uploads directory; linked external files are rejected. GIF, SVG, remote media and arbitrary theme assets are outside this optimization workflow.

A whole-library run records the highest eligible attachment ID at the start. Later uploads are handled only if future-upload automation is enabled, or by another manual run. Successful writes preserve an original first. Returned output is checked for expected format and unchanged dimensions; an output that is not smaller is not committed.

> **External processing**
> Image bytes, the licence code, site host and selected processing options are sent via HTTPS to the Lodone image endpoint and the configured external processor. Processing requires service availability and any configured service limits. The customer does not enter a shared provider key in WordPress.

SPEED

Progress, savings and restoration

Current-job statistics and Total results answer different questions.

Metric	How to read it
Processed percent	Finished file-size tasks divided by queued tasks. During discovery the final denominator is not yet known. Failed attempts still advance the task cursor.
Processed images	An attachment is counted as processed when its last queued size was attempted. Check the separate error count for success.
Size before / after	Current-job totals for successful processing responses. A no-smaller result can contribute zero savings.
Saved bytes / percent	(Before - after) / before for the represented data, rather than a simple average of per-image percentages.
Total results	Persistent results from currently valid optimized attachment records and existing source/output files. Counts the selected output once per original size.
Optimized images / sizes	Distinct media attachments with counted smaller output, plus the number of included file sizes. Repeat runs do not add the same size twice.

A savings example

If selected optimized outputs are 60% of the size of the represented originals, the reported savings are 40%. This describes payload sizes, not total server disk reduction. Preserved originals and format variants consume additional disk space. Removing files, restoring originals or changing selected output can change Total results.

Delivery and rollback

Smaller WebP/AVIF variants are inserted through the standard WordPress attachment-image filter with an original fallback. CSS backgrounds, custom HTML, some builders and external/CDN image rendering may need theme integration. A generated variant is not proof that every page serves it.

To undo an optimized attachment, locate it in the image list, confirm and select Restore originals. Lodone checks preserved-original hashes, restores the original file and thumbnails and removes its recorded variants. The totals then reflect the remaining optimized media.

> **100% is not zero errors**
> Open Processing details after completion. Retry or investigate missing files, service rejections and unsupported output rather than describing the whole library as successfully optimized solely from the progress bar.

VISIBILITY

SEO and GEO: expanded audit

Improve technical information while retaining editorial responsibility.

The 21-check audit reviews indexing, titles, descriptions, H1 use, internal links, redirects, sitemap, robots, canonicals, Open Graph, Schema, identity, image ALT, content depth, author context and generative-search readiness. It does not guarantee search or AI inclusion.

Control	Use
Apply safe fixes	After confirmation, enables suitable missing markup, reuses reliable existing public text and adds ALT only when available attachment context supports it. Inspect the action report.
Site owner	Organization, Local business or Person determines the identity type used in supported structured data.
Public identity	Brand/person name, alternate name, phone, email, address, opening hours and official profile URLs. Enter information you intend to publish.
Markup output	Lodone meta descriptions, Open Graph and Schema output when no recognised SEO plugin owns those outputs.
Store identity helper	Copies available public store identity into empty fields; does not automatically publish the WordPress administrator email.
Content tab	Review public pages/posts/products and open their editor to correct content.
Per-page fields	SEO title, meta description, canonical URL and a do-not-index request.

Write for the actual page

Use a specific title and an accurate summary. A blank Lodone title falls back to the WordPress title. Use a canonical override only when another URL is the intended primary version. Check no-index choices carefully; they are requests to search engines, not access controls.

> **Compatibility and outcomes**
> When a recognised SEO plugin owns public metadata, Lodone avoids duplicate meta/canonical/Open Graph/Schema output. Auditing and supported content/image actions remain. These tools do not replace keyword research, editorial strategy or competitor analysis, and no ranking or traffic outcome is guaranteed.

The audit recognises supported Yoast descriptions and uses rendered content and headings where available. Account, registration, test and lesson pages are not treated as ordinary short articles. Review the remaining content findings individually; a word-count warning alone is not an instruction to expand every page.

VISIBILITY

Optional AI text generation

Generate in small reviewed batches and inspect the public changes.

1. **Prepare a recovery point**
   Create and download a full backup before a run that can change metadata or image ALT.
2. **Configure the optional service**
   In SEO/GEO settings, enter your own OpenAI API key, a compatible model and a conservative pages-per-run setting. Save.
3. **Review eligible content**
   Run the audit and inspect public content. Decide whether previously stored Lodone SEO text may be overwritten.
4. **Confirm the action**
   Select Generate and apply professional SEO text (AI). Read the data-transfer warning and approve only the intended processing.
5. **Review the report**
   Inspect changed, failed and skipped items. Open important page editors and check generated titles, descriptions and ALT against the actual content.
6. **Inspect rendered pages**
   Review public source/output after cache purge and correct inaccurate, repetitive or inappropriate generated wording.

Inputs, ownership and cost

This optional workflow uses eligible public page text and supported public images needing ALT. It is not intended for private drafts, customer records or secrets. Your configured AI account is responsible for its service availability and usage charges. Image optimization and AI text generation are separate services with separate configuration.

The pages-per-run setting allows 1-20; smaller batches reduce timeout risk. The model field must match a model compatible with the integration. Availability can change; a rejected service request is reported rather than evidence that content was generated.

> **AI output is a draft to verify**
> A successful API response is not editorial validation. Check names, product claims, legal wording, image descriptions and page intent. Permission to overwrite Lodone text does not mean permission to replace another SEO plugin's public metadata.

VISIBILITY

Google Search Console reporting

Connect read-only search performance data to the technical audit context.

1. **Prepare Google OAuth**
   Create suitable Google OAuth credentials, add the exact Redirect URI shown by Lodone and enable access required for Search Console reporting.

2. **Save the connection settings**
   Open Monitoring > Google Search Console. Enter the OAuth Client ID and client secret, then save. The client secret is stored encrypted on this WordPress installation.

3. **Connect the owner account**
   Select Connect Google Search Console, sign in to the account that can access the website property and approve the requested read-only access.

4. **Choose and verify the property**
   Confirm that the connected Search Console property represents the intended website. A domain-property and URL-prefix property can have different coverage.

5. **Refresh and review**
   Refresh data to display clicks, impressions, CTR, average position and top queries for the last 28 days. Disconnect when the integration is no longer needed.

How to use the data

Search Console results show observed Google Search performance; they do not prove that every public URL is indexed or healthy. Compare low-CTR queries with relevant titles and descriptions, and investigate material position or impression changes alongside the technical audit and actual page content.

The SEO/GEO audit evaluates all supported published public pages, posts and products instead of stopping at the former 250-item cap. It excludes attachments, selected template post types and sensitive WooCommerce system pages. Internal-link findings are capped for practical reporting, and rendered or custom application routes can still require separate checks.

> **Connection boundary**
> The integration requests read-only Search Console access. OAuth availability, account permissions, property selection and Google data freshness affect what is shown. Stored credentials are protected with the site security keys and may need to be re-entered after migration with new salts.

VISIBILITY

Monthly SEO and GEO growth

A recurring improvement plan without paid AI credits.

1. **Open Monthly growth**
   Enable monthly reports in the Lodone Monthly growth section. Use Update monthly plan to collect the current findings manually.

2. **Connect search data if needed**
   To include actual Google results, configure and connect Search Console with an account that has access to the correct property. Adding a domain to Google alone does not connect Lodone.

3. **Review this month's plan**
   Review priorities based on technical SEO/GEO findings and, when available, pages with many impressions but few clicks or declining traffic. Open the affected page to make editorial corrections.

4. **Check results again**
   After making changes, update the plan to see which findings are no longer detected and which remain. Review saved monthly reports and tracked page changes.

5. **Enable optional email**
   Choose the report recipient and enable monthly email if wanted. A successful send status means the mail transport accepted the message; check delivery in the mailbox.

Search Console comparison uses the latest 28-day reporting window and the preceding 28 days. It can show clicks, impressions, CTR and average position where data is available. Without a connected property, the technical improvement plan still works but real search metrics are unavailable.

The plan and history do not require paid AI credits and do not rewrite content automatically. Optional AI text generation is a separate configured service with its own usage charges.

> **Schedule and interpretation**
> Monthly reports use WordPress scheduling and can run late without site visits or a working server cron. Search data is delayed and changes do not prove that Lodone caused them. Rankings and AI visibility are not guaranteed.

OPERATIONS

Compatibility and data handling

Know which actions stay local and which use an external connection.

Workflow	Data and destination
Licensing and updates	Licence code, site/domain and request metadata go to Lodone over HTTPS.
Cookie scanning	Server scan inspects public HTML and response headers. Browser comparison observes page resources/storage names in three consent states; values are not retained. Live blocking runs in visitor browsers.
Backups	Archives stay on the host by default. Downloads, manual WebDAV and enabled cloud transfers create additional copies. Optional AES-256 encryption happens on the website before storage or transfer; it is off by default.
Cloud	Licence/site/callback and OAuth tokens pass over HTTPS through the Lodone connection service. Pending tokens expire after 10 minutes. Archive bytes go directly to your Dropbox. Nextcloud uses direct WebDAV with credentials encrypted locally, outside the Lodone connection service. Central scheduling sends authenticated wake-ups; it does not relay archive bytes.
File integrity	Official checksum lookup sends installed WordPress version and locale to api.wordpress.org. Local file hashes and baseline are kept in WordPress storage.
Images	Selected source files and processing settings leave the host for remote optimization after confirmation. Originals and results remain locally.
SMTP and alerts	Messages go through your configured mail transport to the selected recipients.
AI generation	Eligible public content is sent to the configured AI service only for the confirmed optional action.

Work alongside other plugins

Use one owner for page caching, public SEO markup and image optimization. Detection covers recognised providers, not every custom plugin. A conflict warning is a request to resolve overlapping features, not an instruction to uninstall an unrelated tool. Verify custom integrations and hosting cache layers separately.

Credentials encrypted with WordPress security keys protect stored values against simple database reading; they are not protection against full compromise of both database and configuration. Re-enter protected credentials after a move with new salts. Keep archives, CSV exports and support files private.

> **Custom sites and networks**
> Do not infer multisite/network-wide coverage or unusual directory support from a successful single-site setup. Test custom layouts, reverse proxies, domain mappings, builders and externally hosted media in staging before relying on the relevant workflow.

OPERATIONS

A practical maintenance routine

Keep evidence that recovery, privacy and protection continue to work.

When	Review or action
Weekly	Review Overview, failed operations, update notices, known-vulnerability findings and security events. Check a recent scheduled backup exists. Review the integrity report if enabled.
After new tracking/embeds	Run the cookie scan, classify new services, review the privacy notice and test rejection and withdrawal in a fresh browser.
After theme/plugin changes	Clear caches, run relevant audits and inspect public pages, forms and checkout. Investigate file changes before approving a new baseline.
After new media uploads	Run a new confirmed image job for selected uploads or the library. Review errors and inspect real delivery and visual quality.
Monthly	Verify an off-server copy; inspect storage use, backup retention and totals. Review large autoload options, overdue cron, saved speed history and Search Console trends before manual maintenance.
Before major updates/migration	Create/download a full recovery point; rehearse where practical; preserve settings and access to the old environment.
Periodically	Restore a copy on an isolated test installation and complete the acceptance checklist. Record the result and unresolved differences.

Write down the operating result

Keep a short record: website and version, operation time, archive ID/checksum, important settings, errors and the pages tested. For image jobs, retain the error count and represented before/after sizes. For scans, retain discovered/checked/failed counts. For integrity, retain the baseline date and explanation for accepted changes.

Choose backup frequency according to how much new content or order data you can afford to lose. Choose alert recipients who can act on failures. A saved schedule or an Active central connection is not evidence that the scheduled archive completed. Inspect creation and upload results separately.

> **One change at a time**
> When troubleshooting, change one relevant setting, rerun the affected check and test the real user journey. This makes it easier to identify the cause and to revert a change using your recovery point.

SUPPORT

Troubleshooting: access and recovery

Start with the actual operation message and the relevant environment.

Symptom	Checks and next action
Licence inactive	Check the licence code, assigned host, paid validity and outbound HTTPS. Use Check licence again and verify Active state. Do not rely only on the prior success banner.
ZIP cannot install	Download the current official package. WordPress needs a normal plugin folder containing its main PHP file; avoid re-zipping with altered nested folders.
Backup fails or appears stuck	Read the restored progress. A stopped job becomes Failed. Review its stage, reason, time and diagnostic log; correct the cause and choose Try again. Check ZIP, disk, permissions and PHP limits.
Upload stalls	Keep the upload screen open. Check session, upload/network limits and chunk error messages. Import a supported full archive rather than a generic ZIP.
Checksum or SQL error	Stop. Preserve the original file and compare it with the known-good source/checksum. Do not bypass verification to force restoration.
Restore incomplete	Inspect the phase and error. Preserve both source and safety copies. Check target permissions and PHP/DB compatibility; recover deliberately using the operation evidence.
Email rejected or missing	Read the SMTP error, verify sender/mailbox/domain and provider authentication. If sending succeeds, check the real recipient inbox/spam and mail logs.
Background job stops	Inspect Automatic scheduling, Last central check and cron reachability. Returning to an active task restores recorded progress and prevents a duplicate start; navigation warnings appear while it runs.
WebDAV fails	Check public HTTPS folder, IPv4 DNS, TLS, credentials, quota, cURL and upload permissions. Confirm the local backup remains.
Dropbox unavailable or failed	Check connection, saved automatic-upload setting, quota and status. For automatic creation also check the saved schedule and central check. Reconnect revoked access or contact support; retry a completed copy.

Support evidence
Provide version, WordPress/PHP versions, affected action, exact error text and time, relevant counts and reproducible steps. Remove licence codes, passwords, API keys and personal data from screenshots. Do not email a full database archive unless a private transfer has been arranged.

SUPPORT

Troubleshooting: scan and optimization

A completed job still needs a review of failures and public behaviour.

Symptom	Checks and next action
Consent setup needs attention	Follow the automatic link to the highlighted setting. Select a published privacy page and review prior blocking and classifications. Unreachable URLs remain warnings and should be inspected, but do not automatically make an otherwise completed scan unusable.
Scan coverage looks incomplete	Review discovered URLs and failed items. Compare with important public journeys; private, external and JavaScript-only routes are outside the scanner.
Optional tracking starts too early	Use a fresh browser, inspect network/storage, review service classification and tag configuration, and check script-order/cache interference. Unrecognised custom code needs separate work.
Unexpected file changes	Compare paths with authorised updates. Investigate core differences and unreadable paths. Do not replace the baseline until differences are understood.
Database plan expired	Run Analyze database again. The reviewed plan lasts 30 minutes. Repeat analysis for later batches.
Images show 100% but errors	Inspect Processing details. Progress counts attempted tasks; resolve per-file limits, missing sources or remote service failures before another run.
Zero or lower image savings	The service may not produce a smaller output. Totals cover currently valid smaller selected variants, not every attempted file or a disk-space measurement.
New images unoptimized	Enable automatic optimization in Automation for future uploads, or run another manual job. Check the saved consent, job errors, active optimizers and WordPress scheduling.
WebP/AVIF not shown publicly	Test the standard attachment output, cache and theme. Custom HTML, CSS backgrounds, builders or external delivery may bypass the attachment filter.
Performance/SEO controls disabled	Inspect recognised-provider ownership. Configure one owner for the layer and do not force duplicate output.
AI text missing or inaccurate	Check the failed/skipped report, credentials and supported model. Review generated text manually; a successful request is not an accuracy guarantee.

SUPPORT

Troubleshooting: monitoring

Check credentials, schedules and external-service coverage before repeating a failed request.

Symptom	Checks and next action
Vulnerability check unavailable	Verify the advisory-feed key, outbound HTTPS and API response. Keep installed components updated while the feed is unavailable.
Unexpected vulnerability finding	Confirm component slug and installed version, open the advisory source and review available patched versions. Back up and test before updating or replacing the component.
Daily security report missing	Check Enable daily checks, the report email, WP-Cron execution and the last stored report time. Email is sent only for a new problem or failure.
Daily scan reports failure	Read the stored error, confirm feed access and that the malware scanner can run. Correct the cause, run both checks manually and verify the next scheduled time.
Search Console will not connect	Confirm the OAuth Client ID/secret, exact Redirect URI, enabled Google API, account permission and property access. Reconnect after migration if protected credentials cannot be read.
Search Console report is empty	Check the selected property and date coverage. A new or low-traffic property can legitimately have no rows; Google data is not real-time.
Search Console values look different	Match the same property, 28-day window and query dimensions in Google. Processing delays, privacy thresholds and later data revisions can change figures.

Keep secrets out of support material
Do not include API keys, OAuth client secrets, refresh tokens or licence codes in screenshots or tickets. Share exact error text, timestamps and non-secret property identifiers instead.

VALIDATION

Site acceptance checklist

Use this to evaluate the plugin on a specific website, beyond reading the guide.

Area	Evidence to record
Licence and version	Correct host, active state, installed version and feature access; status after an account change.
Full backup	Completed copy, manifest, checksum and verified off-server file; for encryption, a separate recovery key and tested import.
Cloud automation	Own Dropbox or Nextcloud account, saved uploads and schedule, central check, completed remote archive, available quota and retention.
Restore rehearsal	Successful restoration on an isolated host; pages/media/login work; email and cron retested; controlled form/order flow.
Cookie coverage	Server-scan counts plus browser Before/Reject/Accept results; failed/incomplete URLs and unknown services reviewed.
Consent behaviour	Optional categories rejected before choice; chosen categories work; withdrawal tested; privacy page and evidence record available.
Security	Audit, malware and vulnerability findings reviewed; daily check and alert verified; login recovery, 2FA, firewall and quarantine tested.
Integrity	Official core status, baseline approval date, paths covered and explanations for unexpected differences.
Database	Read-only plan reviewed, safety copy ID retained, selected removals confirmed and site tested afterwards.
Image optimization	Representative visual comparison, per-task errors, size metrics, public format delivery and original restoration tested.
Performance and SEO	Saved before/after history, cache bypass, one output owner, site-wide 21-check review and optional Search Console metrics.

Contact
Product and customer account: https://lodone.com/ and https://lodone.com/dashboard/. Support: info@lodone.com. Include the relevant report, with secrets removed.