NEUTARGET / IMPLEMENTATION

Feature activation guide

A practical handoff for your website, engineering and growth teams.

Installation pack 1.0.3 | 2026-11-21

1. Choose one platform path	2. Connect the outcome	3. Verify received evidence

IN THIS GUIDE

Website behaviour and reporting

Outcomes and campaign measurement

Revenue, refunds and attribution

Paid Acquisition and ROAS

NeuIntel review and questions

NeuSignal conversion delivery

Email alerts and daily briefings

Sharing, public metrics and team access

Sign-in, SSO and data lifecycle

Acceptance record

Use the companion code files for implementation. PDF code may wrap for reading. Keep Get started open for the current verification state.

The installation pack connects your website to NeuTarget. Use this guide for the remaining configuration and for checks against the reports. Available features depend on the current workspace plan, your role and the evidence received. An installed tag does not grant access or configure external providers.

Website behaviour and reporting

Choose a website from Dashboard > Websites, then open Get started for Website setup. Verify a received browser visit before interpreting its reports. Start in Overview and inspect Data quality and Setup checks. Select the intended dates and read the report's timezone, filters and coverage.

Use Campaigns for acquisition activity, Funnel Builder and Friction to investigate observed drop-off, and Revenue or ROAS for financial questions. Analysis contains Attribution, Cohort Retention, Anomaly Detection and Benchmarks. Visitor profiles require permitted declared customer identity. Anonymous network/browser groups do not establish customer retention; an incomplete or unobservable cohort period is not zero returning customers.

Verification: check the correct website and period, then compare the report with activity you performed. Missing context can follow consent or privacy instructions. A zero and an unavailable value mean different things. Keep direct identifiers out of page URLs, UTM parameters and event payloads.

Outcomes and campaign measurement

Use Analysis > Conversion Goals to create reusable completed-action definitions. The website default drives its primary-outcome reports and setup verification. Saving a library definition does not change that default or complete onboarding. For an action outcome, connect the exact event name only after your application confirms success. Follow the installation guide's event example. Purchases use authenticated financial receipts instead.

Each managed campaign selects its own primary outcome and pins an immutable definition. Creating a new definition or changing the website default does not silently replace that campaign's outcome. Adopt another definition through an explicit campaign revision. Archiving prevents new selections while preserving existing pins; replace or clear a selected website default before archiving its goal.

In Campaigns > Overview, review the selected outcome, planned dates and identifiers. Bind exact UTM values and relevant provider cost identifiers before relying on campaign attribution. Campaign links can be shared with authorized workspace members. Personal saved links remain private unless you explicitly copy an independent snapshot into a campaign. Saving a convenience link does not rewrite historical attribution.

Verification: an event received after the website default's effective time verifies that setup definition. Review each campaign with its pinned definition, selected revision and reporting dates. Event completions are counts; converted eligible sessions determine the session conversion rate. Do not interchange those measures. Action targets use event counts; purchase targets retain their currency-specific financial basis. Read partial observation periods before comparing results.

Revenue, refunds and attribution

Use the Shopify path, WooCommerce plugin or your verified server handler. Open Revenue > Financial setup for configuration and Revenue > Revenue analytics for received financial outcomes. Inspect source assurance and each currency separately. Preserve permitted browser session context with the order when available; it can support attribution but does not authenticate a payment.

Verification: reconcile a selected period with your source system using stable order/event IDs and provider occurrence times. Review successful refunds and any chargebacks alongside captures and net revenue. Investigate pending report delivery, unresolved currency and unattributed outcomes. Keep different currencies separate unless a configured dated FX process explicitly converts them. A valid receipt without checkout context remains financial evidence.

Attribution models allocate eligible recorded financial credit across acquisition touches. Read the displayed lookback and coverage. A change in allocation does not change the underlying payment or prove that a campaign caused it. Campaign detail has its own stated financial-credit rule; do not assume every report uses the same method.

Paid Acquisition and ROAS

Use Paid Acquisition > Connected Accounts for Google Ads or Meta Ads authorization. Select the correct provider account and inspect its connection and sync state. Other Paid Acquisition screens own the review: Campaign Mapping links imported spend to campaign context, while Spend Ledger contains supported imported costs and manual/CSV records. Current capabilities and your permissions determine which controls appear.

Verification: compare fresh spend with the provider for the same dates, account and currency. Resolve unmapped campaigns and inspect unattributed financial outcomes before reading ROAS. A planned campaign budget is not recorded spend. The website tracker cannot authorize an ad account or import its costs.

NeuIntel review and questions

Open NeuIntel > Intelligence Review to inspect calculated evidence and measurement gaps for the selected website and period. Reading the calculated review does not call a language model. Generate explanation requests AI interpretation when your analysis allowance permits it. NeuIntel > Chat uses its separate allowance when you send a question.

From a campaign, Discuss with NeuIntel opens the shared panel with that campaign's revision and reporting period. Ask a focused question, check its evidence and distinguish facts from recommendations. Record the next action in the supported review workflow rather than treating an explanation as an automatic configuration change.

Verification: compare the response with the underlying report under the same dates and filters. Missing evidence remains a limit. NeuIntel can explain recorded patterns and suggest actions; it does not establish causality, prove a root cause or repair missing measurement.

NeuSignal conversion delivery

The account-level NeuSignal overview explains the add-on and its access. Inside a selected website, NeuSignal > Destinations owns delivery configuration; NeuSignal > Events shows processing and delivery state. Paid Acquisition connections and imported spend remain separate configuration.

An authorized admin supplies destination credentials through protected settings. Review collection instructions, consent and eligible event sources before enabling delivery. A browser outcome is not automatically an eligible confirmed purchase signal. Consent or required matching context can make a financial event ineligible for delivery without removing the financial receipt from reporting.

Verification: inspect pending, sent, skipped, retry and failure states, then compare the stable event identity with the destination provider's diagnostics. Resolve credentials, mappings or eligibility issues explicitly. Provider acceptance is not proof of advertising uplift.

Email alerts and daily briefings

Within a website, Alerts > Alert Rules configures a supported metric, observation window and threshold, with currency where needed. Review triggered email delivery in Alerts > Delivery History. Queued means pending processing; provider accepted does not prove inbox arrival or reading. WhatsApp alert delivery is unavailable in this release. Daily briefings are separate from alert rules.

For daily briefings, verify your email in the account menu's Sign-in & security, then open Notifications. Add a phone number in Profile if you want WhatsApp. These personal delivery preferences apply across your account, while eligibility is checked for each workspace. A saved preference is not evidence that the current workspace can send to you.

WhatsApp briefings are available to the actual workspace owner with a verified email and a phone number. Admin membership alone does not make someone the owner. Email briefings can reach the owner and eligible members. A non-owner, including a delegated admin, needs the workspace's team-briefing entitlement and explicit briefing access on their membership. An admin manages that permission in Settings > Members & roles; the recipient still controls personal opt-in.

Verification: review current-workspace eligibility, contact details and channel preference, then confirm receipt of an eligible briefing. Delivery also depends on website readiness and the configured sending service. You can turn a saved preference off across eligible workspaces even if current-workspace access has expired. Contact Support when eligibility is correct and delivery still does not arrive. This pack cannot configure platform email or WhatsApp infrastructure.

Sharing, public metrics and team access

Invite colleagues through Settings > Members & roles and assign the minimum suitable workspace role. Membership grants workspace access, not per-website client isolation. Use separate client workspaces where access must be isolated.

Use Reports & Sharing > Public Pages for deliberately published aggregate metrics. Financial publication is an explicit choice; review the retained-history window and any allowed visitor date filters. Use the Traction Report's share controls for a selected-period reporting link. Review its scope and expiry, then manage revocation in

Shared Links. A bearer link or unlisted public page is not confidential access.

Verification: open the shared page in a signed-out browser and check its actual content before sending it. Validate an invited member's workspace and role, then test revocation. No extra website script is required for these controls.

Sign-in, SSO and data lifecycle

Personal password and email verification belong to the account menu's Sign-in & security. Workspace sign-in configuration belongs to Settings > Security policies and requires an admin and current entitlement. Configure your identity provider and required domain verification before enforcing SSO. MFA requirements applied by that identity provider remain its controls. Test the login and recovery path before enforcement. Never include identity-provider secrets in a browser tag or installation archive.

Review Website settings > Privacy and consent for collection instructions and optional identity. Review permitted retention and erasure actions in their current account or website scope. Trial lifecycle and paid retention follow the platform's subscription policies; the pack does not override them. If collection is paused, resolve the website state before expecting new events.

Verification: check role restrictions and the relevant audit entries. Test consent withdrawal, erasure and SSO recovery in an appropriate test environment before relying on the operational procedure.

Acceptance record

Keep an acceptance record per website with its UUID and deployed integration version. Record the tested period and outcome definition, accepted financial receipt IDs where relevant, and the configured connections. Include notification checks and remaining gaps. Use CHECKLIST.md for the handoff.