Configly

Security Overview

How Configly protects your Zendesk configuration data

April 2026

Configly is built and operated by Optegris Ltd, trading as Configly. This document describes what we do today to protect your Zendesk configuration data. Where features are planned but not yet shipped, we say so explicitly.

1. What We Store & What We Don't

What Configly stores

- ✓ Zendesk configuration metadata (triggers, automations, macros, views, fields, SLAs, and similar)
- ✓ Versioned snapshots of configuration state over time
- ✓ Dependency mappings between configuration objects
- ✓ Virtual changes from What-If simulations
- ✓ User account information (name, email, authentication tokens)
- ✓ AI analysis results when you use AI-powered features
- ✓ Activity logs covering significant actions

What Configly does NOT store

- ✗ Ticket data or ticket content
- ✗ Customer PII (end-user names, emails, phone numbers, addresses)
- ✗ Agent conversations or internal notes
- ✗ Attachments or uploaded files
- ✗ Help Centre article content
- ✗ Payment card data (handled directly by Stripe)
- ✗ Zendesk admin or agent passwords

> **Note:** Configuration metadata can incidentally contain business-sensitive information such as organisation names in trigger conditions, customer-identifying tags, or agent names in metadata fields. We treat all configuration data with the protections described below.

2. Encryption

In transit

TLS 1.2+ on all customer-facing HTTPS connections; Let's Encrypt certificates with automated renewal.

Sensitive credentials at rest

Zendesk OAuth access tokens, OAuth refresh tokens, Zendesk API tokens, and GitHub OAuth tokens encrypted with AES-256-GCM (256-bit key, 12-byte IV, 16-byte authentication tag).

Database storage

Configuration metadata, snapshots, and dependency data stored in PostgreSQL on isolated infrastructure. The database is not exposed to the public internet; application servers connect over the local loopback interface only. Database connections are encrypted in transit using TLS; the application enforces `sslmode=require` on every connection.

Encryption key management

Keys stored as environment variables on production infrastructure with restricted filesystem access. KMS integration with rotation support on our roadmap.

3. Infrastructure & Hosting

- **Provider:** DigitalOcean, London (LON1) region
- **Data residency:** UK-hosted by default — no international data transfers
- **Reverse proxy:** Nginx with security headers (HSTS, X-Frame-Options, Referrer-Policy, Permissions-Policy)
- **Process management:** PM2
- **Application monitoring:** Sentry (EU region, GDPR-compliant, Data Processing Agreement signed)

4. Authentication & Access

Connecting your Zendesk instance. Configly uses Zendesk OAuth 2.0. We never see or store your Zendesk admin or agent passwords.

OAuth scopes requested from Zendesk. When you connect a Zendesk instance, Configly asks you to choose one of two access modes:

- **Read-Only** -- Configly requests only the Zendesk `read` OAuth scope. Configly can read configuration objects (triggers, automations, macros, views, fields, SLAs, and similar), users, organisations, and groups, but cannot modify anything in your Zendesk.
- **Read/Write** -- Configly requests the `read write` OAuth scope. Grants the same read access plus the ability to create, update, and delete configuration objects. Required for Apply Changes and GitHub Sync push-back.

Read-Only is the recommended default for new connections. You can upgrade a Read-Only connection to Read/Write at any time from the Configly Connections page, and downgrade back in one click. Neither mode grants access to ticket content, attachments, Help Centre content, or conversation data. We continue to evaluate Zendesk's granular scope system for even narrower permissions in future.

Connecting your GitHub repository. GitHub Sync uses GitHub OAuth 2.0. The repo scope is requested, required to commit your Zendesk configuration as YAML to a repository you nominate. Configly never accesses repositories you do not authorise.

Configly account authentication. Sign in with Google or Microsoft via OAuth, or with an email address and password. Email/password accounts use bcrypt at cost factor 12 with an 8-character minimum. Multi-factor authentication is on our roadmap.

Session management. Sessions are managed by NextAuth using JWT-based session tokens with default cookie protections (HttpOnly, Secure, SameSite=Lax). JWT expiry defaults to 7 days.

Account access controls. Configly currently operates as a single-user application. Multi-user team accounts with role-based access control are on our roadmap.

5. Auditability & Transparency

- **Zendesk audit log visibility** — every API call Configly makes to your Zendesk is visible in your Zendesk native audit log. Configly sends a `User-Agent: Configly/<version>` header on every request, so you can filter your request logs to Configly traffic specifically. You can independently verify what Configly has accessed or changed at any time.
- **Writes are user-initiated** — writes to your Zendesk only happen when you explicitly initiate them via Apply Changes on a Read/Write connection. OAuth token revocation occurs automatically in two places: when you disconnect a Zendesk instance from Configly, and when you delete your Configly account. In both cases, the token Configly held is explicitly revoked at Zendesk.
- **Apply Changes safety** — every operation includes a mandatory change reason, an automatic pre-push snapshot, drift detection against live state, and one-click rollback.

6. Data Retention & Deletion

- **Snapshot retention** — configuration snapshots are retained for the lifetime of your account and remain available for diff and rollback. An automatic retention policy is under evaluation.
- **AI analysis results** — cached to avoid unnecessary cost. Cached results are deleted when you delete your Configly account.
- **User-controlled deletion** — disconnect any Zendesk instance at any time. Disconnection revokes the OAuth token at Zendesk, removes Configly's stored credentials, and removes all associated snapshots, dependency data, virtual changes, and AI analysis results for that instance.
- **Account deletion** — initiated by cancelling your subscription. At end of the cancellation period, Zendesk OAuth tokens are revoked, AI analysis data is removed, all configuration snapshots and dependency data are removed, authentication accounts are removed, and your user record is anonymised. A billing audit record is retained for accounting purposes.

7. Tenant Isolation

Configly is a multi-tenant SaaS application with logical isolation enforced at the application layer. Each customer's data is associated with their user account and every database query is scoped by user. Authorisation checks on each controller verify that requested resources belong to the requesting user before any operation is permitted. Database-level row-security and per-tenant database separation are not currently in use; tenant separation hardening (including database-level controls) is on our roadmap.

8. Logging & Sensitive Data Handling

- **Application logs** — request method, path, response status, and timing. Request bodies and query parameters are not logged. Passwords, OAuth tokens, API keys, and session cookies are never logged.
- **Error monitoring** — application errors sent to Sentry (EU region). Authorisation, cookie, and API key headers are stripped before transmission. Session cookies are redacted from HTTP request context, and email addresses are redacted from error metadata (any field matching an email pattern is replaced with `[email]`). Your Configly user ID is attached so we can correlate events to an account when investigating issues you report.
- **Web server logs** — standard nginx access logs (source IP, request line, response code, referrer, user-agent) retained for 14 days.

9. Backups & Disaster Recovery

Database backups are taken daily and retained on the production host. Off-site backup replication and a documented recovery procedure are on our roadmap as part of forthcoming infrastructure improvements.

10. Subprocessors

Configly uses the following third-party services to deliver the product. Each service receives only the data necessary for its function:

- **Zendesk** — your Zendesk instance; Configly reads configuration and (via Apply Changes) writes configuration
- **GitHub** — if GitHub Sync is enabled, Configly commits your Zendesk configuration as YAML to a repository you nominate
- **Anthropic (Claude)** — powers AI analysis features and the in-product support assistant. For AI analysis: receives configuration object names, conditions, and actions for items you submit. For the support assistant: receives the messages you send and your account identity (name, email, plan tier).
- **Sentry** — error monitoring (EU region, Frankfurt)
- **Stripe** — billing. Receives your billing email and account identifier; payment cards are entered directly into Stripe and never traverse Configly.
- **Brevo** — transactional email delivery (welcome emails, password resets, billing notifications)
- **Google and Microsoft** — if you sign in with these providers, they handle authentication and return your name and email to Configly
- **Google Workspace** — hosts the support@configly.app mailbox. Inbound support emails are received by Google Workspace before being forwarded to our Zendesk instance. Google Workspace therefore processes the content of any email you send to support@configly.app.
- **DigitalOcean** — infrastructure provider (UK region)
- **Google Analytics** — on our marketing site (configly.app) only, to understand visitor patterns. Not loaded inside the Configly application itself.

A current detailed subprocessor list is available on request to security@configly.app.

11. HTTP Security

Standard security headers are set on all responses, including Strict-Transport-Security (HSTS), X-Content-Type-Options (nosniff), X-Frame-Options, and Referrer-Policy. The application uses helmet middleware for header management. CORS policies restrict cross-origin API access to authorised application origins. Public API endpoints (currently in development) require API key authentication.

12. Compliance & Certifications

Today

- ✓ UK Data Protection Act 2018 and UK GDPR compliant
- ✓ Data Processing Agreement available on request
- ✓ Encryption at rest and in transit for sensitive credentials
- ✓ Tenant isolation enforced at the application layer
- ✓ UK-hosted infrastructure (London, LON1)

On the roadmap

- ✗ SOC 2 Type II certification (planned as our customer base grows)
- ✗ ISO 27001 (under evaluation)

13. Incident Response

We acknowledge security reports within 24 hours and notify affected customers of confirmed security incidents within 72 hours of confirmation, in line with UK GDPR breach notification requirements.

14. Responsible Disclosure

If you discover a security vulnerability in Configly, please report it to security@configly.app. We will acknowledge receipt within 24 hours and work with you in good faith to investigate and resolve the issue. We do not currently offer paid bug bounties but will publicly credit researchers who report valid issues responsibly.

15. Contact

SECURITY QUESTIONS AND REPORTS
security@configly.app

GENERAL ENQUIRIES
hello@configly.app

DATA PROTECTION ENQUIRIES
privacy@configly.app

TRUST PAGE
https://configly.app/trust

© 2026 Configly. All rights reserved. | configly.app

This document is provided for informational purposes. For the most current information, visit https://configly.app/trust