FrontierZero

FrontierZero Google Workspace Integration Plan

FrontierZero Customer Security Guide
March 2026

High Level Integration view

FrontierZero acts as a consolidated, continuous security auditor for your Google Workspace environment. By connecting to the Google Admin SDK and Reports API, we provide a unified dashboard that enriches and consolidates data around your organization's identities, detects misconfigurations, and surfaces security risks that are often buried in native logs. By consolidating and enriching the identity, we pick up many risks that were not obvious by reviewing single sources in isolation.

Our goal is to provide Proof of Concept (PoC) access to a closed FrontierZero environment to show how we can help provide additional protection to the Talabat environment. The PoC will take around 1.5hrs and all access/data can be revoked at any time.

Core Pillars of the Integration:

- **Centralised SaaS Identity Consolidation:**
  - Providing real-time visibility and risk alerting of all **third-party** users' access to your SaaS data.
  - Centralising, enriching, and mapping internal users into a single security context location.
  - Instant visibility of orphaned SaaS accounts, and which ex-employees may still have access to.

- **Shadow SaaS/Shadow AI Management:**
  - Identifying, categorising, and revoking all shadow SaaS applications authorized by your users.
  - Identifying, categorising, and revoking shadow AI applications authorized by your users.

- **Identity based SaaS Threat Detection:**
  - Real-time monitoring for abnormal SaaS activities and suspicious account changes.
  - Real-time heat sensor updates on identities being targeted via irregular failed login attempts

1. Automated Sync (API Integration)

This is our preferred/recommended method for 24/7 monitoring. FrontierZero uses OAuth 2.0 to securely access your workspace data without requiring your admin credentials.

Required Read-Only Scopes & Why They Matter

To provide a full security audit, FrontierZero requests the following permissions:

Google Scope	Purpose	Security Importance
.../admin.directory.user.readonly	Profile Metadata	Syncs names, emails, and account status (Suspended/Active).
.../admin.directory.user.security	Shadow SaaS Discovery	This allows FrontierZero to see which 3rd-party OAuth apps users have granted access to. We fetch ClientId and Scopes to detect risky or malicious integrations.
.../admin.reports.audit.readonly	Audit Logs	Ingests events from Login, Drive, and Admin logs to detect brute-force attacks or unauthorized config changes.
.../admin.reports.usage.readonly	Activity Tracking	Monitors the last time a user touched Gmail or Drive to identify dormant accounts.
.../licensing	License Auditing	Maps users to specific SKUs (e.g., Business Starter vs. Enterprise) to identify cost-saving opportunities.

Technical Detail: Organizational Unit (OU) Filtering

FrontierZero respects your organizational boundaries. Our integration allows you to filter API connectivity by orgUnitId.

- **How it works:** When fetching logs or user data, FrontierZero appends the orgUnitID parameter to the API request.
- **The Result:** Our sync engine only "sees" and processes data for the specific departments or teams you choose to manage within FrontierZero.

2. Manual Export (The Point-in-Time Alternative)

If you opt for a manual import instead of the live API, FrontierZero's support team can manually ingest CSV/JSON exports. However, admins must be aware of the inherent limitations of this method.

Limitations of Manual Imports

- **The Timeframe Window:** A manual export is a static snapshot. It only captures activity within a fixed historical window (e.g., the last 7-14 days). Once the file is uploaded, FrontierZero cannot "see" new events until the next manual export is performed.
- **No Real-Time Remediation:** Unlike the API integration—which can trigger automated alerts the moment a threat is detected—manual imports are retrospective and suitable only for periodic compliance audits.

Targeted Data Collection via API

1. Scoped User Discovery

To identify which identities exist within a specific department, you can use the orgUnitPath or query parameters within the Admin SDK.

- **API Endpoint:** GET https://admin.googleapis.com/admin/directory/v1/users
- **Technical Implementation:** We can append a query filter: ?query=orgUnitPath='/Sales/NorthAmerica'.
- **Purpose:** This allows FrontierZero to build an inventory of users strictly within that OU.

2. Shadow SaaS Analysis

Once the user list for an OU is established, you can perform a deep-dive into the security posture of each individual identity to uncover unsanctioned applications.

- **API Endpoint:** GET https://admin.googleapis.com/admin/directory/v1/users/{userKey}/tokens
- **Logic:** For every user discovered in the step above, we fetch their authorized OAuth tokens. This reveals the "Shadow SaaS" footprint—third-party apps that have been granted access to corporate data (e.g., a "PDF Converter" app with full Drive access).

3. Activity Log Filtering (orgUnitID)

For one-time snapshot purposes, you can utilize the orgUnitID parameter in the Reports API.

- **API Endpoint:** GET https://admin.googleapis.com/admin/reports/v1/activity/users/all/applications/{applicationName}?orgUnitID={unique_id}
- **Application Sources:** We specifically monitor the following logs to detect threats:
  - admin: Detects unauthorized configuration changes or privilege escalations.
  - login: Identifies brute-force attempts, suspicious geolocations, and MFA failures.
  - drive: Monitors for mass data exfiltration or risky file-sharing behavior.
  - token: Tracks when new third-party apps are authorized (Shadow SaaS alerts).
  - user_accounts: Detects password changes and account recovery events.

Questions? Email us at: hello@frontierzero.io