OctoFlow for Google Workspace admins

What to allow, what it can access, and how to allow it

Last updated September 20, 2026
octoflowus.com/security · support@octoflowus.com

A user at your company asked to connect OctoFlow to their Google account and saw Access blocked: your institution's admin needs to review OctoFlow (error 400, access_not_configured). That message comes from your Workspace app access control setting, which blocks third party apps until an admin allows them. Nothing is wrong with the user's account. This sheet has what you need to review and allow OctoFlow.

WHAT OCTOFLOW IS

A Chrome side panel and web app for individual salespeople: a map of their own professional relationships, a log of their own outreach, and a task list. It does not read, modify, or extract data from company systems. Account sign in is email and PIN, so OctoFlow works without this Google grant; only Gmail logging and sending wait on your approval.

HOW TO IDENTIFY THE APP

App name	OctoFlow
OAuth client ID	44764321450-d66difvblc3h20vtc4r3hfl2bjssp44p.apps.googleusercontent.com
Google Cloud project number	44764321450
Publisher	OctoFlow LLC, Denver, Colorado. Domain octoflowus.com
Chrome extension ID	aaobogaacakidgajkkfkkafjoeelakdc
Privacy policy	octoflowus.com/privacy
Security overview	octoflowus.com/security

GOOGLE SCOPES IT REQUESTS

gmail.metadata (restricted)	Message headers only: sender, recipient, subject, date, thread id. Google's servers refuse message bodies and attachments under this scope. Used to log emails the user already exchanges with contacts they track and to detect replies.
gmail.send (sensitive)	Sends an email the user wrote in OctoFlow, from their own address through Google's API. Only on the user's action or a campaign the user scheduled.
openid, email	Shows the user which Google account is connected.

Not requested: gmail.readonly, gmail.modify, full mailbox access, Contacts, Calendar, Drive, or any Admin SDK scope.

HOW TO ALLOW IT

1. In the Google Admin console open Security, then Access and data control, then API controls.
2. Under App access control choose Manage Third-Party App Access.
3. Choose Add app, then OAuth App Name Or Client ID. Paste the client ID above and select OctoFlow.
4. Pick the organizational units that should have access, or the whole organization.
5. Set access to Trusted. gmail.metadata is a Google restricted scope, so Limited access is not enough.
6. Save. The user retries Connect in OctoFlow Settings. No reinstall is needed.

If Chrome extensions are also restricted: Devices, then Chrome, then Apps and extensions, then Users and browsers. Add by ID aaobogaacakidgajkkfkkafjoeelakdc and set Allow install.

WHAT YOU CAN RELY ON

- Google has verified this app: OAuth verification approved September 19, 2026 for exactly the two Gmail scopes above, after a CASA Tier 2 (App Defense Alliance) security assessment by TAC Security passed September 15, 2026. Recertified annually.
- Refresh tokens are stored server side in the user's private account record on Google Cloud (us-central1), readable only by OctoFlow's server functions. Disconnecting deletes them, and users can also revoke access from their Google Account permissions page.
- Encrypted in transit (TLS 1.2+) and at rest on Google Cloud. No data is sold or shared. Users can delete their account and all data from Settings.
- OctoFlow's use of Google API data follows the Google API Services User Data Policy, including the Limited Use requirements.