OctoFlow for Microsoft 365 admins

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

Last updated October 23, 2026
octoflowus.com/security · support@octoflowus.com

A user at your company tried to connect OctoFlow to their Microsoft 365 mailbox and saw Need admin approval. That screen comes from your tenant's consent settings, which stop users from allowing third party apps on their own. Microsoft only files a request for you if the admin consent workflow is switched on, so there is usually nothing waiting in your admin center. This sheet is what the app is, what it asks for, and the one click that allows it.

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. The Microsoft connection is optional and per user. It lets a rep send email from their own mailbox through OctoFlow and lets OctoFlow notice replies and bounces to messages that rep sent.

HOW TO IDENTIFY THE APP

App name	OctoFlow
Application (client) ID	a71ba352-085e-4df6-b272-f4c1cf298547
Sign in audience	Multi tenant (accounts in any organizational directory). Delegated permissions only, no application permissions.
Redirect URI	https://us-central1-octoflow-543dd.cloudfunctions.net/emailMsOAuthCallback
Publisher	OctoFlow LLC, Denver, Colorado. Domain octoflowus.com
Chrome extension ID	aaobogaacakidgajkkfkkafjoeelakdc
Privacy policy	octoflowus.com/privacy
Security overview	octoflowus.com/security

MICROSOFT GRAPH PERMISSIONS IT REQUESTS

Mail.Send (delegated)	Sends an email the user wrote in OctoFlow from their own mailbox, or replies inside a thread the user started. Only on the user's action or a campaign the user scheduled. Sent mail is saved to the user's Sent Items.
Mail.Read (delegated)	Reads message headers from the user's Sent Items and Inbox: id, subject, sender, recipients, dates, conversation id and internet message headers. Every request selects those fields only; message bodies and attachments are never requested. Used to match replies and bounces to the OctoFlow contact and to log emails the user already exchanges with people on their map.
User.Read (delegated)	The user's name and address, to show which account is connected.
offline_access	A refresh token so the connection stays alive without signing in again.

Not requested: Mail.ReadWrite, any application permission, Contacts, Calendars, Files, Directory, or anything about other users. No permission applies to anyone who has not connected their own account.

HOW TO ALLOW IT

1. Sign in to Microsoft as a Global Administrator.
2. Open https://login.microsoftonline.com/organizations/adminconsent?client_id=a71ba352-085e-4df6-b272-f4c1cf298547
3. Review the four permissions above and choose Accept. This grants consent for your tenant. Each user still connects their own account; nothing is read until they do.
4. The user retries Connect on the Microsoft card in OctoFlow Settings. No reinstall is needed.
5. To approve per request instead: Entra admin center, Enterprise applications, Consent and permissions, Admin consent settings. Turn on Users can request admin consent to apps they are unable to consent to and add yourself as a reviewer. Requests then appear under Enterprise applications, Admin consent requests.
6. To revoke later: Entra admin center, Enterprise applications, OctoFlow, then Permissions, or delete the enterprise application. A user can also remove it at myapps.microsoft.com.

If Chrome or Edge extensions are restricted: allow extension ID aaobogaacakidgajkkfkkafjoeelakdc in your browser policy. Chrome: Google Admin console, Devices, Chrome, Apps and extensions. Edge: the ExtensionInstallAllowlist policy through Intune or group policy.

WHAT YOU CAN RELY ON

- Delegated permissions only. OctoFlow acts as the signed in user, only for users who connected their own mailbox. There is no application permission and no access to any other mailbox.
- Message bodies are never requested. Every Microsoft Graph read OctoFlow makes selects header fields only: subject, sender, recipients, dates and thread ids.
- 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 at myapps.microsoft.com.
- Encrypted in transit (TLS 1.2+) and at rest. No data is sold or shared. Users can delete their account and all data from Settings.
- The same server code and data handling serve OctoFlow's Gmail connection, which passed a CASA Tier 2 (App Defense Alliance) security assessment by TAC Security in September 2026 and holds Google OAuth verification.