

Share a connection and control access

Explain owner and administrator responsibilities, people and team grants, least privilege, service accounts, and credential protection.

A connection authorizes Vibework to use a specific external account, tenant, database, or service through an integration. Sharing a connection can enable people, agents, and workflows to act on external data, so its access should match the sensitivity and impact of the operations it exposes.

Choose the connection owner

Prefer an organization-owned service account for shared, durable automation when the external system supports one. Use a personal account only when the work is intentionally personal and will stop or transfer cleanly when that person changes roles. Document the business purpose, external owner, and renewal or rotation responsibility.

Grant least-privilege access

1. Open the connection's access or sharing settings as an authorized administrator or owner.
2. Identify the people, teams, agents, or workflows that actually need the connection.
3. Separate harmless read access from operations that write, delete, spend money, change security, or communicate externally when the integration supports that distinction.
4. Grant the narrowest supported access and test with a non-sensitive read or validation operation.
5. Require human review or approval for consequential actions where supported.

Review and remove access

- Review connection membership when a team changes, a project ends, or an external account is replaced.
- Remove stale agents and workflows as well as stale people; automation can retain access after its original owner leaves.
- Reconnect or rotate credentials through the supported authorization flow rather than copying credentials into prompts or instructions.
- Disable the connection promptly when compromise, unexpected activity, or ownership loss is suspected.

Credentials stay private

Users and agents should invoke approved operations without seeing the underlying secret. Never paste passwords, private keys, tokens, OAuth codes, or connection strings into Chat, an agent instruction, a

workflow input, a help request, or a shared document.