

Bolt quickstart.

Bolt running locally in under a minute. One install command, no account, no keys.

Connect your own apps and AI model when you are ready. Free for individuals.

What you'll have running in 60 seconds

- ☒ Bolt desktop app (macOS, Linux, Windows).
- ☒ Embedded PostgreSQL (one-time prewarm during install).
- ☒ The same Aeira Rust crates that power the org editions: ACL evaluator, retrieval, audit chain.
- ☒ A local session on this computer with nothing connected yet. Gmail, Drive and other apps stay locked until you connect them.
- ☒ No identity provider and no account required to start. Add an AI model key when you want to chat.
- ☒ Free for individuals - no time limit, no login required to get going.

Install

One command per platform. The script downloads the installer, prewarms PostgreSQL, and launches the app. Safe to re-run: subsequent runs reuse a per-version on-disk cache and skip the download.

RUN IN TERMINAL · APPLE SILICON & INTEL

```
curl -fsSL https://sparcle.app/install.sh | sh
```

Downloads, installs to /Applications, and launches Bolt.

RUN IN TERMINAL · X86_64

```
curl -fsSL https://sparcle.app/install.sh | sh
```

Installs the .deb on Debian and Ubuntu, or an AppImage in ~/.local/bin without admin rights.

RUN IN POWERSHELL · X86_64

```
irm https://sparcle.app/install.ps1 | iex
```

Marks app as trusted · downloads, installs, and launches Bolt.

Pin a specific version with `BOLT_VERSION`. Useful when you want to reproduce a behavior against an older release.

```
BOLT_VERSION=0.1.174 curl -fsSL https://sparcle.app/install.sh | sh
```

On PowerShell:

```
$env:BOLT_VERSION='0.1.174'; irm https://sparcle.app/install.ps1 | iex .
```

First 60 seconds

- 1 Installer downloads the platform artifact, prewarms PostgreSQL, and launches Bolt.
- 2 Bolt opens ready to use on this computer, with nothing connected. No login. No keys. (After a sign-out, choose Continue as guest to get back to it.)
- 3 Choose which folders Bolt may search, open the launcher, and type. Connect Gmail, Drive or your company sign-in when you are ready.

Five things to try

In order of wow per minute.

1. Search from the launcher

Open the launcher and type. Bolt searches the folders you let it index on this computer, and once you connect Gmail, Drive or other apps, those too, with a link back to each source.

2. Masking at the AI boundary

Paste text with a secret or personal data into an AI chat. Before it leaves for the model, Bolt warns you and offers one-click masking. Only text bound for an AI model is masked; your own tools keep the real values. When your company sets Mask or Block in Bolt's Admin page, that policy is enforced.

3. /discover and /files

Type /discover to find integrations and tools you can add. Type /files to browse files on this computer (/browse works too).

4. Audit chain

Bolt records its decisions in a tamper-evident audit chain. Admins can export the audit log from Settings > Admin as a proof bundle and check it offline, with no database or keys needed.

5. Bring your own LLM

Settings > AI Models: pick OpenAI, Anthropic, Google Gemini, OpenRouter, NVIDIA, Groq, a local Ollama or vLLM model, or any OpenAI-compatible endpoint. The same masking applies to every provider.

Bring your own IdP and data (optional)

The free install works on this computer with nothing connected. When you're ready to point it at your environment:

Company sign-in: Okta, Entra, Google Workspace, Auth0, Zoho or any OIDC provider. SAML for web sign-in. SCIM for provisioning.

Settings → Integrations: 104 first-party connectors. An Airbyte bridge fronts roughly 350 more.

Settings → AI Models: pick OpenAI, Anthropic, Google Gemini, OpenRouter, NVIDIA, Groq, a local Ollama or vLLM model, or any OpenAI-compatible endpoint.

Masking applies the same way to every source and every AI provider.

Data locality



Bolt runs entirely on your machine. The desktop app, the local API sidecar, and embedded PostgreSQL are all local processes.



Bolt sends nothing to Sparcle. Your computer talks only to the services you connect, the AI provider you choose, and GitHub for updates. Masking redacts sensitive fields before text goes to an AI model.



No data is sent to Sparcle servers in any shipping mode. There is no telemetry path that uploads your corpus, queries, or results.

What's next

- [90-day pilot pre-flight checklist \(PDF\)](#) for moving from a single-user install to a real org deployment.
- [System overview](#) if you want the full picture before a pilot.
- [Security and compliance](#) for the threat-model and audit-chain story.
- [Pricing](#) when you're ready to size an org deployment.

 Install issues: re-run the install command (it's idempotent). Anything stuck after that, reach the team via the contact link in the footer.