GEBO.AI SETUP GUIDE · INTEGRATIONS · PAGE 19

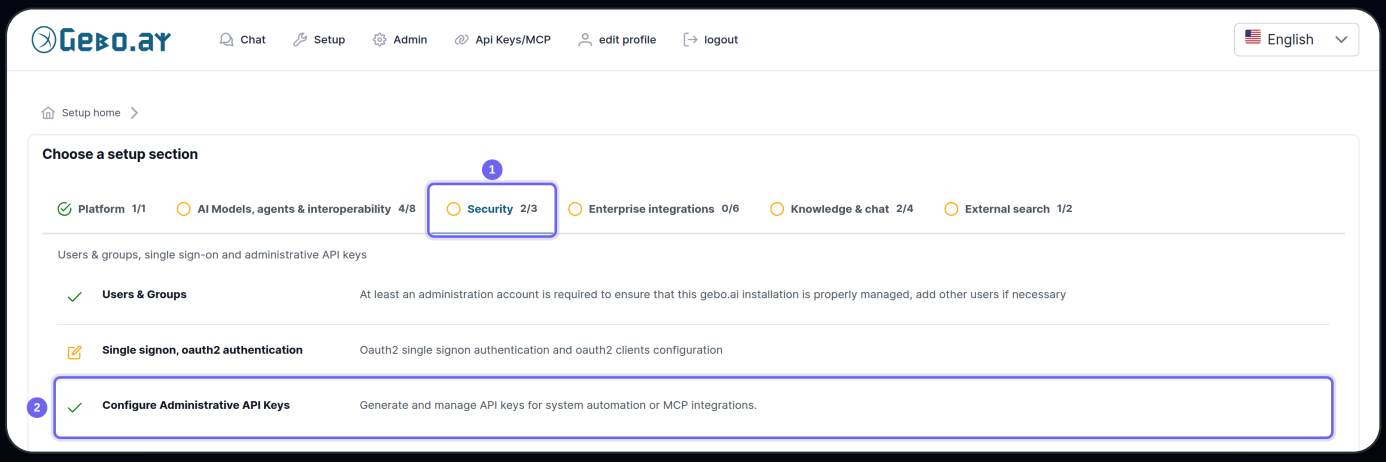
Administrative API keys

Keys an administrator generates on behalf of a user, for scripts, services and integrations that call Gebo.ai, its MCP servers and its A2A endpoints without a person logging in.

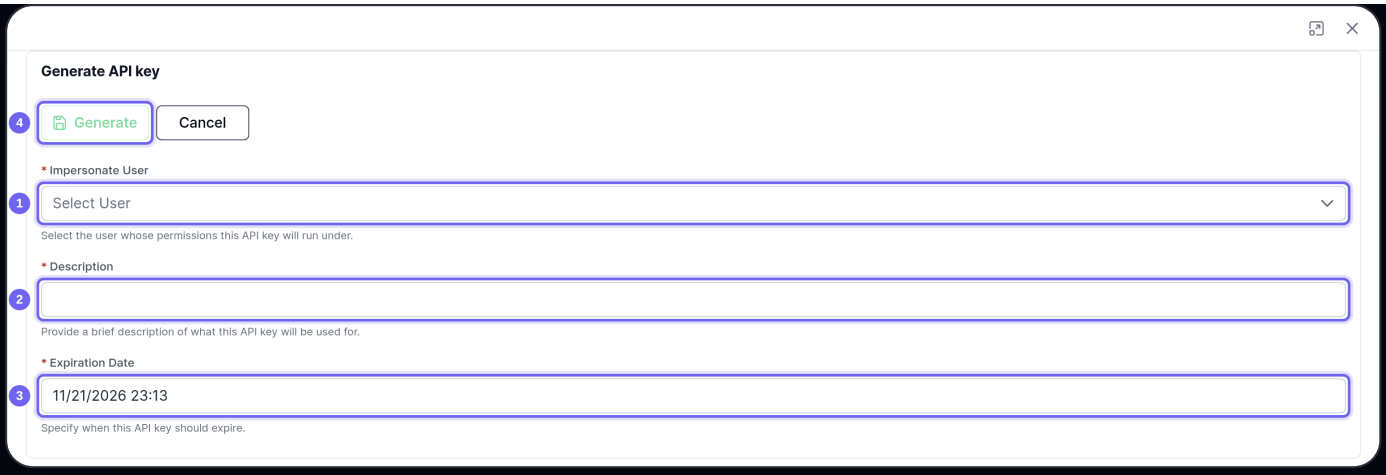
TIME	2 minutes.
YOU NEED	The user the key will act as: a service account created in Admin → Users and groups with the knowledge bases it may read.

1 Generate the key

In **Setup** open **Security** (1) and click **Configure Administrative API Keys** (2), then **Generate new API key**.



The Security tab.



A new administrative API key.

1. **Impersonate User:** the user the key acts as.
2. **Description:** what the key is for.
3. **Expiration Date**.
4. **Generate**: the key is shown once, copy it.

The key is sent as `Authorization: Bearer <key>`, to the REST API, to the exposed MCP servers of page 16 and to the A2A endpoints of page 18.

> **Keep them short-lived**
> A key carries the user's rights for as long as it lives. Give each integration its own key and a short expiration, and delete a key the moment it is no longer needed: the deletion revokes it. People connecting their own tools use personal keys instead (page 16).

← Expose Gebo.ai agents over A2A

Next: LLM usage and costs →