⚠️ **Check your sign-up restrictions**

Your GitLab instance allows anyone to register for an account, which is a security risk on public-facing GitLab instances. You should deactivate new sign ups if public users aren't expected to register for an account.

🔍 Search page

Performance optimization

Various settings that affect GitLab performance.

User and IP rate limits

Set limits for web and API requests. Learn more.

Package registry rate limits

Set rate limits for package registry API requests that supersede the general user and IP rate limits. Learn more.

Files API Rate Limits

Configure specific limits for Files API requests that supersede the general user and IP rate limits.

Search rate limits

Set rate limits for searches performed by web or API requests.

Deprecated API rate limits

Configure specific limits for deprecated API requests that supersede the general user and IP rate limits. Which API requests are affected?

Git LFS Rate Limits

Configure specific limits for Git LFS requests that supersede the general user and IP rate limits. Learn more.

Git SSH operations rate limit

Limit the number of Git operations a user can perform per minute, per repository. Learn more.

Outbound requests

Allow requests to the local network from hooks and integrations. Learn more.

☐ Block all requests, except for IP addresses, IP ranges, and domain names defined in the allowlist
☑ Allow requests to the local network from webhooks and integrations
☑ Allow requests to the local network from system hooks

Local IP addresses and domain names that hooks and integrations can access

example.com, 192.168.1.1, xn--itlab-j1a.com

Requests can be made to these IP addresses and domains even when local requests are not allowed. IP ranges such as `1:0:0:0:0:0:0:0/124` and `127.0.0.0/28` are supported. Domain wildcards are not supported. To separate entries, use commas, semicolons, or newlines. The allowlist can have a maximum of 1000 entries. Domains must be IDNA-encoded. Learn more.

☑ Enforce DNS-rebinding attack protection
Resolve IP addresses for outbound requests to prevent DNS-rebinding attacks.

Rate limit access to specified paths. [Learn more.](#)

Issues Rate Limits

Limit the number of issues and epics per minute a user can create through web and API requests. [Learn more.](#)

Notes rate limit

Set the per-user rate limit for notes created by web or API requests. [Learn more.](#)

Users API rate limit

Set the per-user rate limit for getting a user by ID via the API. [Learn more.](#)

Projects API rate limit

Set the per-IP address rate limit applicable to unauthenticated requests for getting a list of projects via the API. [Learn more.](#)

Members API rate limit

Limit the number of project or group members a user can delete per minute through API requests. [Learn more.](#)

Import and export rate limits

Set per-user rate limits for imports and exports of projects and groups. [Learn more.](#)

Pipeline creation rate limits

Limit the number of pipeline creation requests per minute. This limit includes pipelines created through the UI, the API, and by background processing. [Learn more.](#)