LOGZILLA DOCUMENTATION

API Endpoint Overview

Map of common LogZilla API endpoints for auth, users, dashboards, widgets, triggers, and queries, sourced from lib/logzilla/api/urls.py

LogZilla API · Generated May 3, 2026 · logzilla.ai/docs/logzilla-api/api-endpoint-overview

API Endpoint Overview

A practical map of commonly used API endpoints, sourced from `lib/logzilla/api/urls.py`. For full request/response schemas, filters, and examples, use the interactive docs at `/api/docs`.

- Auth and session
  - `GET/POST/DELETE /api/auth` —- session info, login, logout
  - `POST /api/reset-password`
  - `GET /api/ping`
- Users and access control
  - `GET/POST /api/users` (and `/{id}`)
  - `GET /api/groups`
  - `POST /api/groups`
  - `GET /api/groups/{id}`
  - `PUT /api/groups/{id}`
  - `PATCH /api/groups/{id}`
  - `DELETE /api/groups/{id}`
  - `GET /api/permissions`
- Dashboards and widgets
  - `GET /api/dashboards`
  - `POST /api/dashboards`
  - `GET /api/dashboards/{id}`
  - `PUT /api/dashboards/{id}`
  - `PATCH /api/dashboards/{id}`
  - `DELETE /api/dashboards/{id}`
  - `POST /api/dashboards/{id}/{report|templates|widgets}`
  - `DELETE /api/dashboards/{id}/widgets`
  - `GET /api/widgets`
  - `POST /api/widgets`
  - `GET /api/widgets/{id}`
  - `PUT /api/widgets/{id}`

  - `PATCH /api/widgets/{id}`
  - `DELETE /api/widgets/{id}`
  - `POST /api/widgets/{id}/report`
  - `GET /api/widget-types`
  - `GET /api/widget-presets`
- Events
  - `GET /api/events/{ev_id}`
  - `GET /api/events/{ev_id}/timestamps`
  - `GET /api/events/{ev_id}/triggers`
  - `GET /api/events/{ev_id}/ai`
  - `POST /api/events/{ev_id}/forward`
- Triggers
  - `GET /api/triggers`
  - `POST /api/triggers`
  - `GET /api/triggers/{id}`
  - `PUT /api/triggers/{id}`
  - `PATCH /api/triggers/{id}`
  - `DELETE /api/triggers/{id}`
  - `GET /api/triggers/{id}/history`
  - `POST /api/triggers-validator` —- validate filters
- Notifications
  - `GET /api/notification-groups`
- Queries (generic)
  - `POST /api/query` —- create
  - `GET /api/query/{qid}` —- results (with paging for Search)
  - `GET /api/query/{qid}/{export|recalculate|remove|stop}`
  - `POST /api/query/{qid}/stop`
  - `GET /api/query-types` —- available query types
  - WebSocket: `/ws/live-updates` (see Making Queries)

- Queries (typed)
  - `POST /api/queries/search`
  - `GET /api/queries/search/{qid}`
  - `GET /api/queries/search/{qid}/{export|recalculate|remove|stop}`
  - `POST /api/queries/search/{qid}/stop`
  - `POST /api/queries/lastn`
  - `GET /api/queries/lastn/{qid}`
  - `GET /api/queries/lastn/{qid}/{export|recalculate|remove|stop}`
  - `POST /api/queries/lastn/{qid}/stop`
  - `POST /api/queries/topn`
  - `GET /api/queries/topn/{qid}`
  - `GET /api/queries/topn/{qid}/{export|recalculate|remove|stop}`
  - `POST /api/queries/topn/{qid}/stop`
  - `POST /api/queries/eventrate`
  - `GET /api/queries/eventrate/{qid}`
  - `GET /api/queries/eventrate/{qid}/{export|recalculate|remove|stop}`
  - `POST /api/queries/eventrate/{qid}/stop`
  - `POST /api/queries/processingstats`
  - `GET /api/queries/processingstats/{qid}`
  - `GET /api/queries/processingstats/{qid}/{export|recalculate|remove|stop}`
  - `POST /api/queries/processingstats/{qid}/stop`
  - `POST /api/queries/storagestats`
  - `GET /api/queries/storagestats/{qid}`
  - `GET /api/queries/storagestats/{qid}/{export|recalculate|remove|stop}`
  - `POST /api/queries/storagestats/{qid}/stop`
  - `POST /api/queries/system_cpu`
  - `GET /api/queries/system_cpu/{qid}`
  - `GET /api/queries/system_cpu/{qid}/{export|recalculate|remove|stop}`
  - `POST /api/queries/system_cpu/{qid}/stop`
  - `POST /api/queries/system_df`
  - `GET /api/queries/system_df/{qid}`
  - `GET /api/queries/system_df/{qid}/{export|recalculate|remove|stop}`
  - `POST /api/queries/system_df/{qid}/stop`

- `POST /api/queries/system_iops`
- `GET /api/queries/system_iops/{qid}`
- `GET /api/queries/system_iops/{qid}/{export|recalculate|remove|stop}`
- `POST /api/queries/system_iops/{qid}/stop`
- `POST /api/queries/system_memory`
- `GET /api/queries/system_memory/{qid}`
- `GET /api/queries/system_memory/{qid}/{export|recalculate|remove|stop}`
- `POST /api/queries/system_memory/{qid}/stop`
- `POST /api/queries/system_network`
- `GET /api/queries/system_network/{qid}`
- `GET /api/queries/system_network/{qid}/{export|recalculate|remove|stop}`
- `POST /api/queries/system_network/{qid}/stop`
- `POST /api/queries/system_networkerrors`
- `GET /api/queries/system_networkerrors/{qid}`
- `GET /api/queries/system_networkerrors/{qid}/{export|recalculate|remove|stop}`
- `POST /api/queries/system_networkerrors/{qid}/stop`
- `POST /api/queries/systemstatus`
- `GET /api/queries/systemstatus/{qid}`
- `GET /api/queries/systemstatus/{qid}/{export|recalculate|remove|stop}`
- `POST /api/queries/systemstatus/{qid}/stop`

- Reports

  - `GET /api/reports`
  - `GET /api/reports/{id}` (download via retrieve)
  - `DELETE /api/reports/{id}`
  - `GET /api/reports/{id}/export`
  - `GET /api/reports-templates`
  - `POST /api/reports-templates`
  - `GET /api/reports-templates/{id}`
  - `PUT /api/reports-templates/{id}`
  - `PATCH /api/reports-templates/{id}`
  - `DELETE /api/reports-templates/{id}`
  - `POST /api/reports-templates/{id}/generate`

  - `GET /api/reports-schedules`
  - `POST /api/reports-schedules`
  - `GET /api/reports-schedules/{id}`
  - `PUT /api/reports-schedules/{id}`
  - `PATCH /api/reports-schedules/{id}`
  - `DELETE /api/reports-schedules/{id}`
  - `GET /api/reports-schedules/{id}/reports`
- Settings and system
  - `GET /api/license-info`
  - `GET/POST /api/settings` (and extra configs)
  - `POST /api/settings-update-publish`
  - `GET/POST /api/customer-info`
  - `GET /api/monitor`
- Archives
  - `GET /api/archives`
  - `POST /api/archives`
  - `GET /api/archives/{chunk_ts}`
  - `POST /api/archives/migrate`
  - `DELETE /api/archives/range`
  - `POST /api/archives/remove` (range)
  - `GET /api/archive-restore-logs`
- Forwarder counters
  - `GET /api/forwarder-counters`
- Lookup tools
  - `GET /api/lookup/{dns|whois|mac|cisco-mnemonic|geoip|mswin-eventid|mitre-id}/{pk}`
- Terminals (test utilities)
  - `POST /api/terminals` —- create ephemeral shell session

- Mailer and LDAP tester
  - `POST /api/mailer`
  - `POST /api/ldap-tester`
- App store
  - `GET /api/apps` —- available apps
  - `GET /api/installed-apps`
- Misc
  - `GET /api/async-results`
  - `GET /api/docs`, `GET /api/schema`

Notes:

- All endpoints require a valid user token in `Authorization: token <TOKEN>` unless explicitly marked public. See Getting Started (https://www.logzilla.ai/docs/logzilla-api/getting-started) for token usage.
- The HTTP Receiver (ingestion) is separate and documented under Receiving Data; its interactive docs are typically at `/incoming/docs`.