LOGZILLA DOCUMENTATION

Executive Report

Enable and schedule the LogZilla executive report, a weekly or daily health and security summary delivered by email with an Excel workbook or as JSON

Administration · Generated September 22, 2026 · logzilla.ai/docs/administration/executive-report

Executive Report

The executive report is a scheduled summary written for managers. It covers platform health, security, operations, and identity activity for one week or one day, and compares every figure with the equal period before it.

The report arrives as an HTML email with an Excel workbook attached, and the same content is available as a JSON document through the API. It is built from stored events, the tags the Operations apps add to them, and the platform's own counters. It does not use LogZilla AI, so it runs on every installation.

A new installation comes with the **Weekly Executive Report** for the admin account and a schedule for every Monday at 06:00. The schedule is switched on automatically, once, as soon as the SMTP server or the sender address is changed from its default and the admin account has an email address; until then the report is ready to run from the Reports page. The Exec Report Default Schedule setting turns this off.

Prerequisites

- **Apps.** The report needs the SecOps, GeoIP, ITOps, NetOps, and AuthOps apps, all five at once. They are installed on new installations and added on upgrade to systems that do not have them, so no App Store step is normally required. When one of them is missing, the report is not generated; see Caveats. An app that was uninstalled can be reinstalled from the App Store, and it is also installed again on the next upgrade. See LogZilla Apps (https://www.logzilla.ai/docs/administration/logzilla-apps).
- **Email delivery.** The SMTP mailer must be configured before a scheduled report can be mailed. See Sending E-Mail (https://www.logzilla.ai/docs/administration/sending-email). Without it the report is still generated and remains downloadable from the Reports page. Changing the SMTP server or the sender address from its default also switches on the default weekly schedule of a new installation, provided the admin account has an email address.
- **Links.** The links in the email and the workbook are built from the External Base Url setting under Settings > System Settings > Generic. When it is empty, the server host name is used, which may not resolve for a recipient outside the server's own network. See Server Settings (https://www.logzilla.ai/docs/administration/server-settings).
- **Permissions.** The Reports module requires the Reports permission, and the settings tab requires the Manage Settings permission. See Role Based Access Control (https://www.logzilla.ai/docs/administration/role-based-access-control).

Report Period

The weekly report covers the seven full days before the day it runs, and the daily report covers the previous full day. Days begin at midnight in the server time zone, set by Time Zone under Settings > System Settings > Generic; see Caveats for a period that contains a daylight saving time change. Every figure is compared with the equal period immediately before the reported one, so a weekly report compares the last seven days with the seven days before them.

Scheduling the weekly report early on the first day of the week, for example every Monday at 06:00, keeps the reported period aligned with the calendar week.

Creating and Scheduling the Report

A new installation already has the Weekly Executive Report with an inactive Monday 06:00 schedule for the admin account. Administrators can open it to change the time, enter recipients in **Send email to**, or switch it on by selecting **Active**. A schedule cannot be saved without a recipient. To create another report:

Open **Reports** and select **Build new report**.
Enter a **Name**, set **Source Type** to **Preset**, and select **Weekly Executive Report** or **Daily Executive Report** as the **Preset**.
Choose the **File type**. **JSON** stores the report document as the report file, and **Excel** stores the workbook. The email always carries the workbook, whichever file type is selected.
Select **Add schedule** and choose the **Type**:

- **Scheduled** runs the report on a recurring schedule set in the **Run** picker, until the **Due date**.
- **Once** runs the report at the moment set in **Choose date & time**.
- **Immediate** runs the report once, at the next scheduled report check after the report is saved.

Enter the recipient addresses in **Send email to**, separated by commas, leave **Active** selected, and select **Save changes**. When any address is not valid, the schedule is not saved.
Scheduled runs are picked up within a minute of their due time. Each report has one schedule, and the form offers **Add schedule** only while the report has none.

Times in the **Run** picker are in the server time zone, set by Time Zone under Settings > System Settings > Generic.

Selecting **Generate report** on the Reports list runs the report at once and downloads the report file. A run started this way sends no email; a run started through the API can name recipients, see Reports API (https://www.logzilla.ai/docs/logzilla-api/reports-api).

The Email

The subject line reads `[LogZilla] Weekly Executive Report, <instance>, Sep 1 to Sep 7, 2026`, with the brand replaced when Exec Report Brand Name is set and the wording changed to `Daily` for the daily preset.

The message opens with the buttons **Open the interactive report** and, for a scheduled report, **Change schedule or recipients**. A **Needs attention** list follows, ordered by level: critical, serious, warning, and then info. When no rule matched, the message states that nothing needs attention for the period instead.

Each section then shows its figures as tiles, with the change against the previous period, followed by its top lists drawn as bars. The Excel workbook is attached to every executive report email.

The Workbook

The workbook opens with three cross-section sheets and then one sheet per report section:

Sheet	Contents
Summary	Every figure of every section with its current value, previous value, change, unit, and note
Attention	Every item of the Needs attention list with its level, title, detail, and section
Data	Every point of every daily series, for the reported period and the previous one, ready to filter and pivot
Health at a glance, Security, Operations, Identity	The section's top lists as tables with bar charts, and a column chart per daily series

Cells hold values, never formulas, and timestamps are written as wall clock time in the report time zone. Sheet names are the section titles, cut to the 31 characters Excel allows.

What the Report Contains

Section	Requires	Covers
Health at a glance	No app	Events processed and received, duplicates removed, deduplication, events per day against the licensed limit, storage used, days until storage is full, active, new, and silent hosts, retention, and events by vendor
Security	SecOps, GeoIP	Security events, critical, high, medium, and low threats, failed logins, and distinct attack techniques; top lists by MITRE ATT&CK technique, attack source country, failed login source address, and most targeted host
Operations	ITOps, NetOps	System events, network events, link down events, HA and hardware events, service disruptions, and configuration changes; top lists by link down device, configuration change host, and HA and hardware host
Identity	AuthOps	Successful logins, failed logins, privilege escalations, and account changes; top list of failed logins by user

Attention Rules

Eight rules are evaluated against the finished figures. A rule that does not match contributes nothing to the report.

Rule	Flags when	Setting
License usage	Average events per day reach the warning percentage of the licensed limit, or the critical percentage	Exec Report Epd Warning Pct, Exec Report Epd Critical Pct
License expiring	The license expires within the configured number of days, or has already expired	License Expiration Warning Days (Generic)
Storage full soon	The projected days until storage is full fall below the warning threshold, or below the serious threshold	Exec Report Disk Warning Days, Exec Report Disk Serious Days
Hosts gone silent	A host sent logs during the previous period and none during the reported one	None
New vendors appeared	A vendor sent events during the reported period and none during the previous one	None
Critical threats up	Critical threats reach the minimum event count and rise by the configured percentage or more	Exec Report Threat Min Events, Exec Report Threat Up Pct
Failed logins up	Failed logins reach the minimum event count and rise by the configured percentage or more	Exec Report Failed Auth Min Events, Exec Report Failed Auth Up Pct
Repeated link down	One device reaches the configured number of link down events in the period	Exec Report Link Down Min Events

Each item states its level, a short title, and a sentence of detail. In the JSON document the items that point at specific events also carry the query behind them, so the events can be reproduced in a search. The license and storage items carry no query, because they are read from the license and the storage projection rather than from events.

JSON Export

A report whose file type is JSON is downloaded from the Reports list, or with `GET /api/reports/{id}/export` using an API token. See Getting Started (https://www.logzilla.ai/docs/logzilla-api/getting-started) for token handling and Query API Parameters (https://www.logzilla.ai/docs/logzilla-api/query-api-parameters) for the filter syntax used in the embedded queries.

Each report returned by `GET /api/reports` carries the `schedule` and `template` it was generated from and, for an executive report, the `document_id` of its document. `GET /api/reports?document_id=` with the id from

`meta.document_id` or from the interactive report link returns that report, and `GET /api/reports-schedules/{id}/reports` lists the runs of a schedule.

The document follows the `logzilla.exec-report/1` schema. Its top-level keys are `schema`, `meta`, `period`, `previous_period`, `sections`, and `attention`. Figures that come from an event search carry the query that produced them, so a dashboard widget or a search can reproduce the number. Health figures read from platform counters or storage samples instead carry no query:

```
{
  "schema": "logzilla.exec-report/1",
  "meta": {
    "document_id": "3f6c1d2e-8a4b-4c7e-9d1f-2b5a6c7d8e9f",
    "instance": "lz-prod-01.acme.example",
    "timezone": "UTC",
    "links": {
      "report_url": "https://logzilla.acme.example/reports/executive/3f6c1d2e-8a4b-4c7e-9d1f-
2b5a6c7d8e9f"
    }
  },
  "period": { "kind": "week", "ts_from": 1788220800, "ts_to": 1788825600 },
  "sections": [
    {
      "key": "health",
      "title": "Health at a glance",
      "kpis": [
        {
          "key": "events_processed",
          "label": "Events processed",
          "value": 612400000,
          "previous": 588300000,
          "delta_pct": 4.1,
          "unit": "events",
          "query": { "type": "Search", "filter": [] }
        }
      ]
    }
  ]
}
```

Settings

The report reads its branding, link paths, and thresholds from Settings > System Settings > Executive Report.

Setting	Default	Effect
Exec Report Brand Name	(empty)	Brand name shown in the email and the workbook; empty keeps the LogZilla branding
Exec Report Logo Url	(empty)	Absolute URL of a logo shown in the email in place of the brand name; the workbook always prints the brand name as text
Exec Report View Path	`/reports/executive/{document_id}`	Path behind the Open the interactive report button, appended to the instance URL; empty links the report file download instead
Exec Report Schedule Path	`/reports/schedules/{schedule_id}`	Path behind the Change schedule or recipients link; empty removes the link
Exec Report Epd Warning Pct	`80`	Percentage of the licensed events per day at which the license is flagged as a warning
Exec Report Epd Critical Pct	`100`	Percentage of the licensed events per day at which the license is flagged as critical
Exec Report Disk Warning Days	`60`	Projected days until storage is full below which storage is flagged as a warning
Exec Report Disk Serious Days	`14`	Projected days until storage is full below which storage is flagged as serious
Exec Report Threat Up Pct	`50`	Percentage increase of critical threats over the previous period at which they are flagged
Exec Report Threat Min Events	`100`	Critical threat events needed in the period before the increase is flagged

Setting	Default	Effect
Exec Report Failed Auth Up Pct	`100`	Percentage increase of failed logins over the previous period at which they are flagged; 100 means twice as many
Exec Report Failed Auth Min Events	`1000`	Failed login events needed in the period before the increase is flagged
Exec Report Link Down Min Events	`10`	Link down events on one device in the period at which the device is flagged
Exec Report Default Schedule	on	Creates the Weekly Executive Report and its Monday 06:00 schedule for the admin account on a new installation, and switches the schedule on once the SMTP server or the sender address is changed from its default and the admin account has an email address; off leaves both to be created by hand

The warning percentage must not exceed the critical percentage, and the serious storage threshold must not exceed the warning threshold. Changed values take effect for reports generated after the change is applied; see Server Settings (https://www.logzilla.ai/docs/administration/server-settings) for the YAML and command line form of these keys and for the ways to apply a change.

Caveats

- The **Open the interactive report** button targets a report page that is not part of the current web interface. Setting Exec Report View Path to empty makes the button download the report file instead, and clearing Exec Report Schedule Path removes the schedule link.
- A report has one schedule, and every recipient of that schedule receives the same message at the same time, with all addresses visible in the To header.
- All five apps must be installed at the time of each run. A scheduled run with a required app uninstalled produces no report and no email; the run is recorded as a warning naming the report and the missing apps in the celeryworker log and, with internal events at their default level, in the Logzilla Warnings notifications. The schedule keeps its next run. Generating such a report on demand is refused, and the API response names the missing apps. A report is never generated with a section left out or partially filled.
- The default weekly report is created only by a new installation. Systems upgraded from an earlier release do not receive it, a deleted default schedule is not recreated, and the schedule is not switched on while the setting is off.

- When the reported period or the period before it contains a daylight saving time change, both periods and their daily figures are measured in whole 24-hour steps back from midnight at the end of the reported period. The days before the change therefore begin at 23:00 or 01:00 rather than at midnight, which is visible in the workbook's Data sheet and in the JSON series times. The period named in the email and the workbook is unaffected.
- The report reads the whole period from event storage, so it runs longer on installations with high event volumes or many distinct hosts. It runs in the background and does not block the interface.