

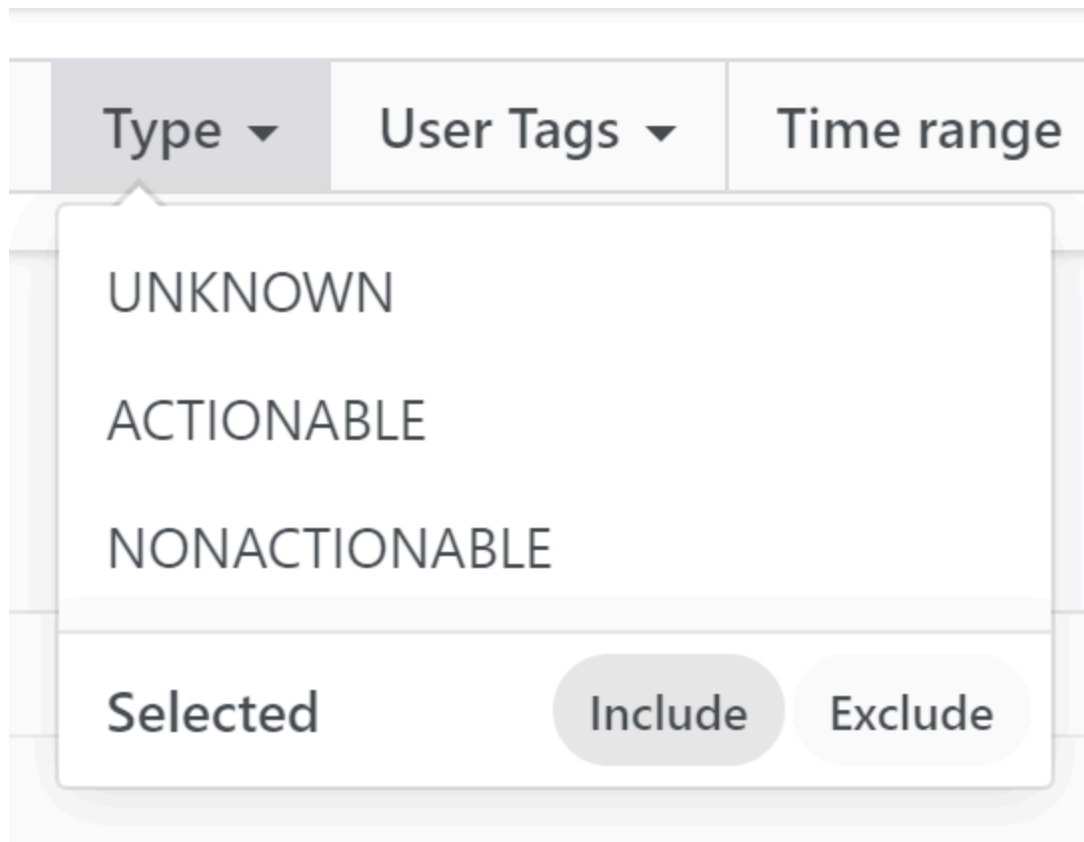
**LOGZILLA DOCUMENTATION**

# Explanation of Actions

LogZilla trigger actions covering Mark As, Send E-mail, Webhook, and Run Script, including event variable substitution and regex capture syntax

## Mark As

This allows users to mark incoming events as Actionable or Non-actionable. This simplifies future searches when using these options from the 'Type' drop down in the search bar.



The value of this is that everyday events that administrators don't need cluttering search results can be marked as Non-actionable, while events like 'low disk space', 'fan failure', or 'CPU over-utilization' can be marked as Actionable.

When searching, events that are not marked with either can be found by selecting the 'Unknown' type.

## Send E-mail

For high priority events, administrators may need immediate notification of occurrence. Selecting this option allows users to enter the address of the person or team responsible.

**Add new trigger** ✕

---

**Name \***

**Event match**  **More** ▾ ✕ **Reset**

---

**Actions**

**Mark as** ⚠ Actionable ✅ Non-Actionable

**Send e-mail**

**To \***

✕

**Subject \***

**Message** ⌕ View available placeholders

---

**Public** Cancel Save changes

Users can also add a Subject and message content for this trigger. Variables that can be used are:

- {{event:host}}
- {{event:severity}}
- {{event:facility}}
- {{event:first\_occurrence}}
- {{event:last\_occurrence}}
- {{event:program}}

- `{{event:cisco_mnemonic}}`
- `{{event:snareid}}`
- `{{event:message}}`
- `{{event:ut:abc}}` (the meaning of this is "user tag named abc")
- `{{regex:message:abc:n}}` (see explanation below)

`Match-Message` can be used to match portions of the event message based on regular expressions. Define one or more patterns in the email template header using lines of the form: `Match-Message-<name>: <regex>`

For example, to capture an endpoint IP address and MAC address: `Match-Message-EndpointIPAddress:`  
`EndpointIPAddress="(\d+\.\d+\.\d+\.\d+)" Match-Message-EndpointMacAddress:`  
`EndpointMacAddress="(?:\w\w:){5}\w\w"`

Then use the extracted values as `{{regex:message:<name>:n}}`, where `n` is 0 for the whole match, or 1, 2, and so on for content of the `n`th parenthesized group in the regular expression. Using the examples above:

```
{{regex:message:EndpointIPAddress:1}}
```

See the Settings sections of the documentation for information on setting SMTP options for email alerts.

## Add note

When an event occurs, other users may need to be given more information to reduce duplication of effort.

Facility ▾ Program ▾ Mnemonic ▾ Type ▾ User Tags ▾ Time range ▾

### Add new trigger ✕

Name \*

Event match  More ▾ User Tags ▾ ✕ Reset

Actions

- Mark as ⚠ Actionable ✔ Non-Actionable
- Send e-mail
- Send webhook
- Add note

Note \*

- Issue notification
- Execute script

Public

## Issue Notification

Selecting this option will produce a notification that will increment in the page header, and show up on the notifications page.

### Add new trigger ✕

**Name \***

**Event match**  **More** ▾ **User Tags** ▾ ✕ Reset

**Actions**

- Mark as ⚠ Actionable ✅ Non-Actionable
- Send e-mail
- Send webhook
- Add note
- Issue notification
- Execute script

[? Learn more: Creating Triggers > Explanation of Actions](#)

Public Cancel Save changes

From the notifications page, users can Search, View, Edit, and Delete notifications. More information on this can be found in the Notifications section of the documentation.

## Execute Script

This option lets users write and execute their own scripts and trigger them whenever an event occurs. Just enter the name of the script to run in the box, and it will run whenever the event recurs. The [Trigger Scripts](https://www.logzilla.ai/docs/creating-triggers/trigger-scripts) (<https://www.logzilla.ai/docs/creating-triggers/trigger-scripts>) section of the documentation provides more information on this feature.

## Edit



Name \*

Device Compliance

Event match

Search in message

More 1

Reset

Actions

Mark as ⚠ Actionable ✔ Non-Actionable



Send e-mail



Send webhook



Add note



Issue notification



Execute script



[custom] compliance.py ✔



Stop riag

[? Learn more: Creating Triggers > Explanation of Actions](#)

Public

Cancel

Save changes

# Trigger Settings

Default Trigger settings can be changed in the Setting menu under System Settings, then Triggers.

The screenshot shows the LogZilla web interface. At the top, there is a navigation bar with the LogZilla logo and menu items: NOTIFICATIONS (with a notification icon), TASKS, TRIGGERS, REPORTS, SETTINGS (highlighted), and HELP. On the right side of the navigation bar, there are system statistics: Total: 246.3m events, 22.87% duplicate events; Today: 18.6m events; Avg. Disk Usage: 59.44%. The user is identified as Admin User with email support@logzilla.net.

Below the navigation bar is a search and filter bar with a 'Query' input field and dropdown menus for Severity, Host, Facility, Program, Mnemonic, Type, User Tags, and Time range. There are buttons for 'Include Archives' and 'Search'.

The main content area is titled 'SETTINGS'. Below this title are tabs for 'My account', 'Users & Groups', 'System Settings' (which is active), and 'App store'.

A warning banner is displayed: "Warning! Changing some of these settings may render your server unusable, proceed with caution."

The 'Triggers' section is expanded in the left sidebar. The main content area shows three configuration options, each with a description and a numeric input field followed by a unit selector:

- E-mails sending period \***: The minimum period in sec between successive trigger emails. Input: 60, Unit: seconds.
- Webhook period \***: The minimum period in sec between successive webhooks. Input: 10, Unit: seconds.
- Script execution period \***: The minimum period in sec between successive script execute. Input: 1, Unit: seconds.

A red asterisk indicates a required field. At the bottom of the settings area is a 'Save changes' button.