LOGZILLA DOCUMENTATION

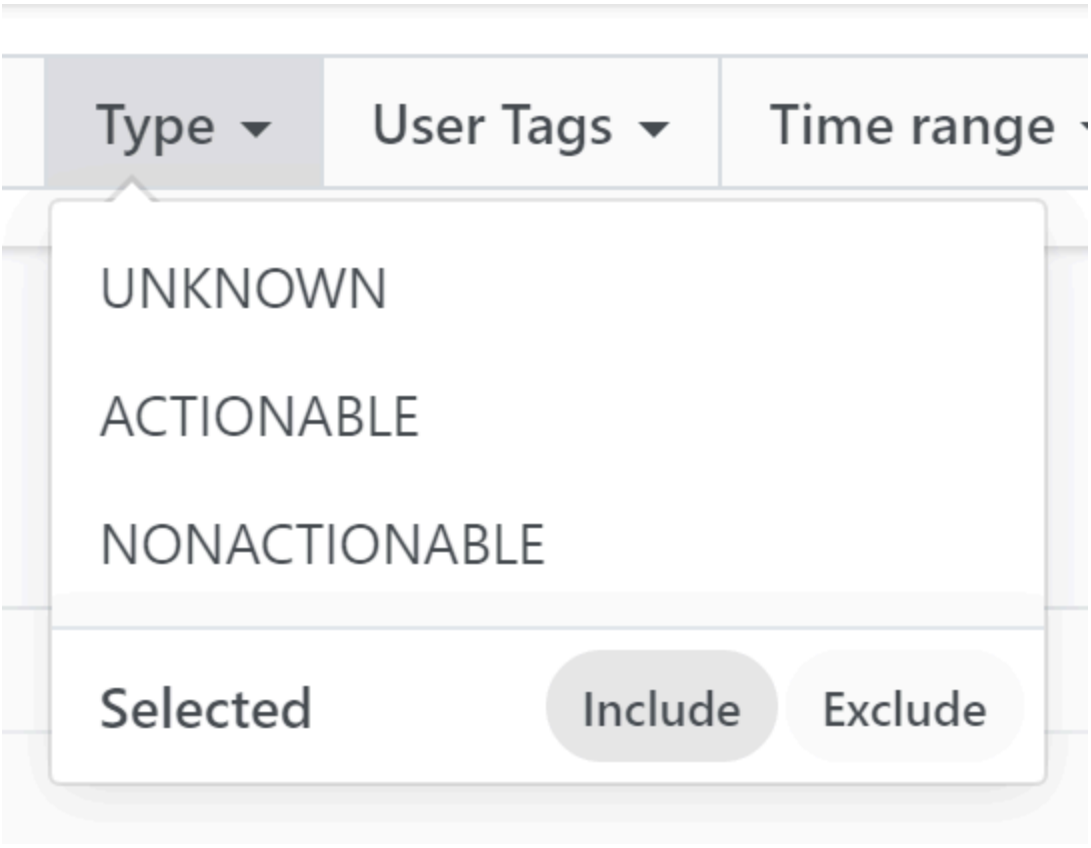
Explanation of Actions

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

LogZilla Triggers · Generated April 27, 2026 · logzilla.ai/docs/creating-triggers/explanation-of-actions

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.

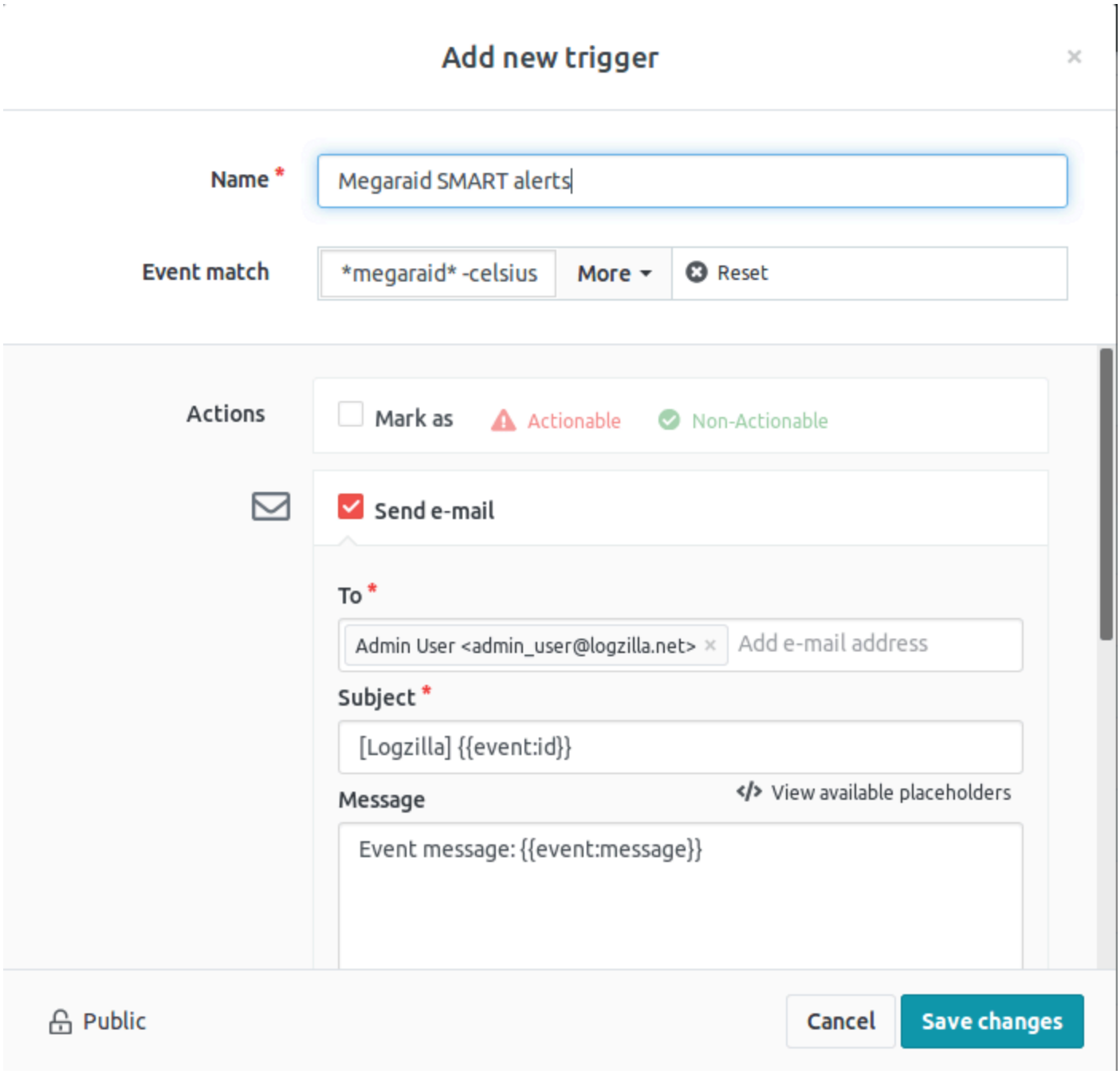


The value of this is that everyday events that administrators don't need cluttering search results can be marked as Non-actionable, while events like 'low disk space', 'fan failure', or 'CPU over-utilization' can be marked as Actionable.

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.



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")
- `{{regexp: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>`

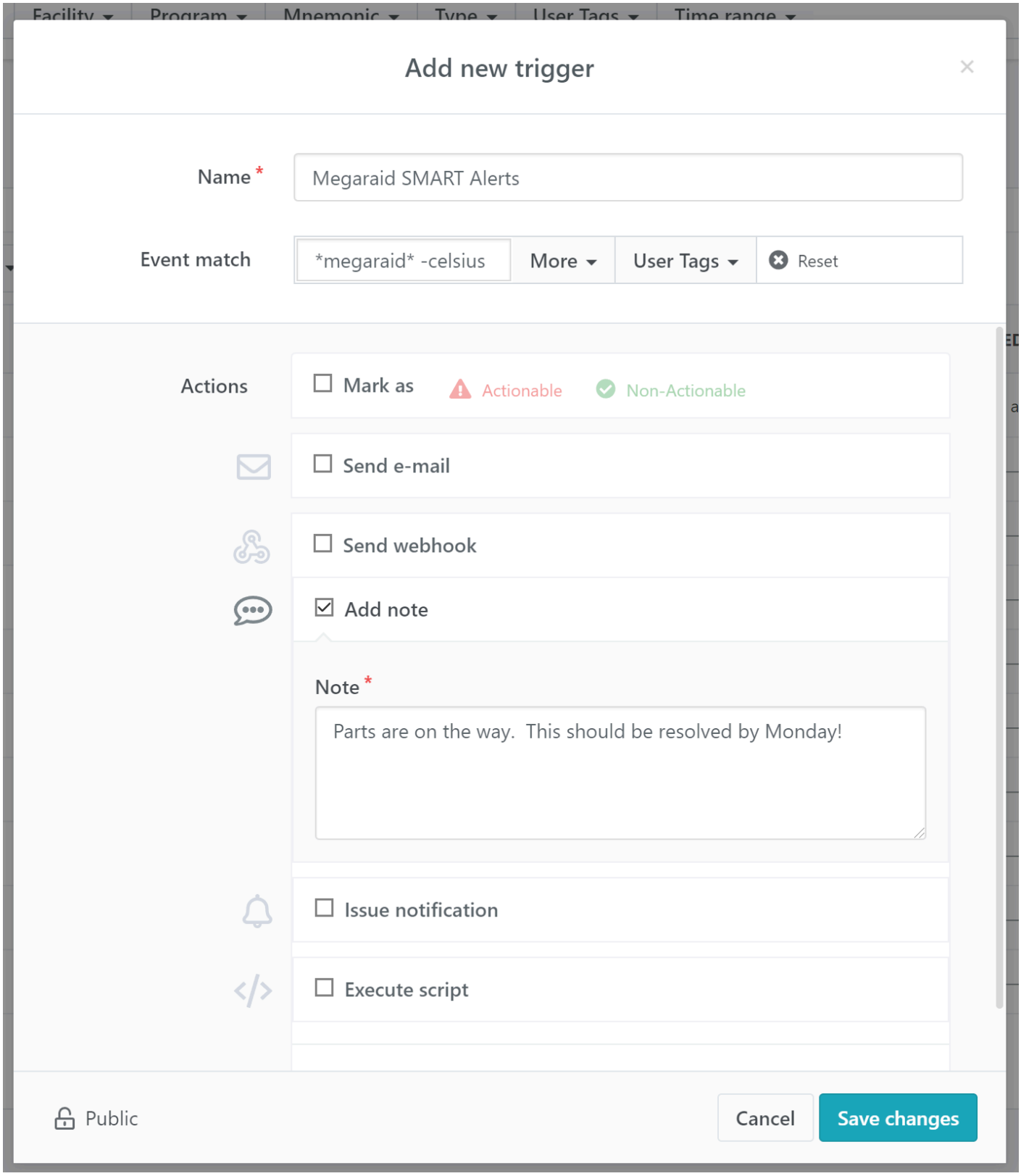
For example, to capture an endpoint IP address and MAC address: `Match-Message-EndpointIPAddress: EndpointIPAddress="(\d+\.\d+\.\d+\.\d+)" Match-Message-EndpointMacAddress: EndpointMacAddress="((?:\w\w:){5}\w\w)"`

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

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

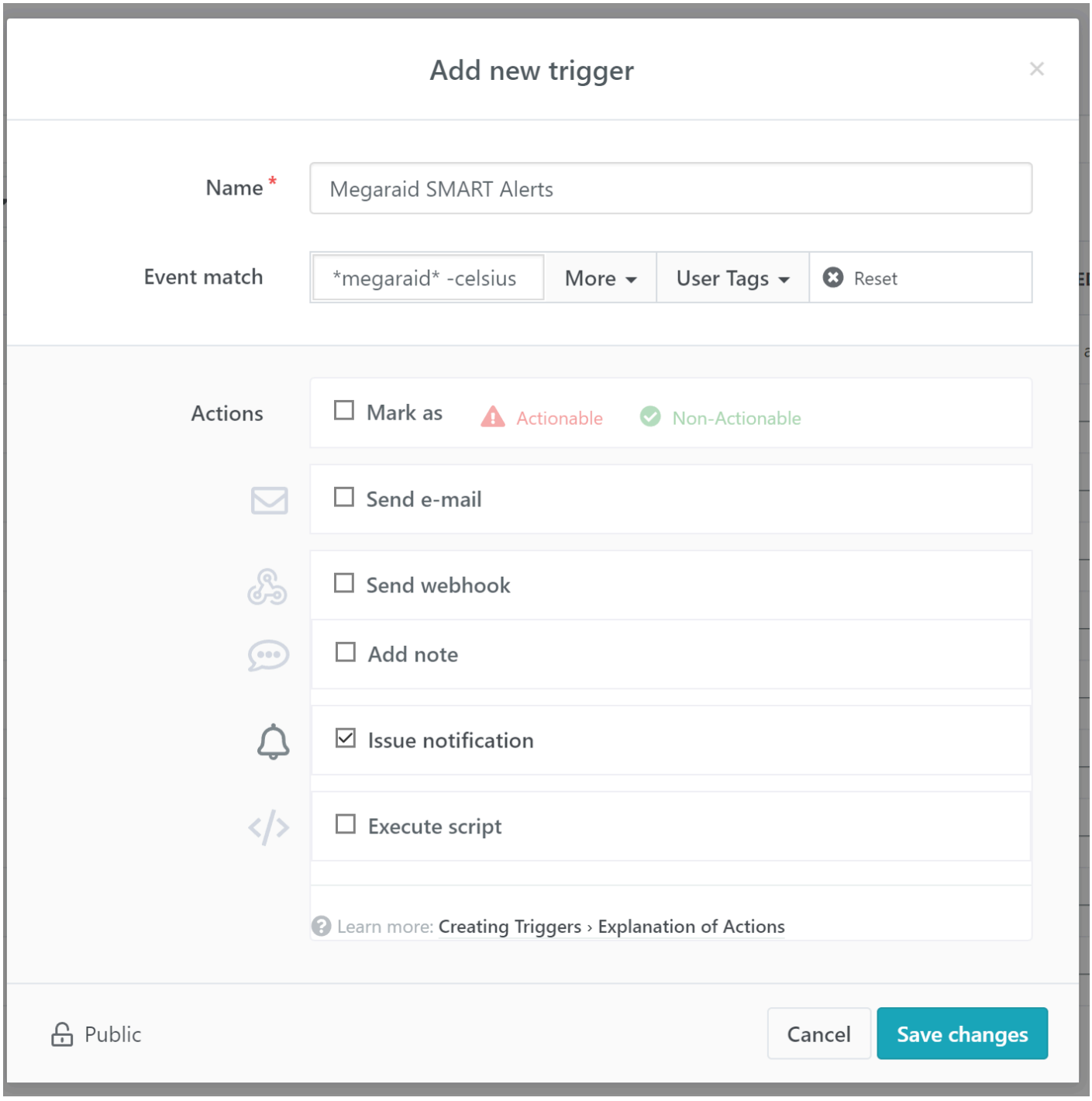
Add note

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 *
Megaraid SMART Alerts
Event match
megaraid -celsius
More
User Tags
Reset
Actions
Mark as
Actionable
Non-Actionable
Send e-mail
Send webhook
Add note
Note *
Parts are on the way. This should be resolved by Monday!
Issue notification
Execute script
Public
Cancel
Save changes

Issue Notification

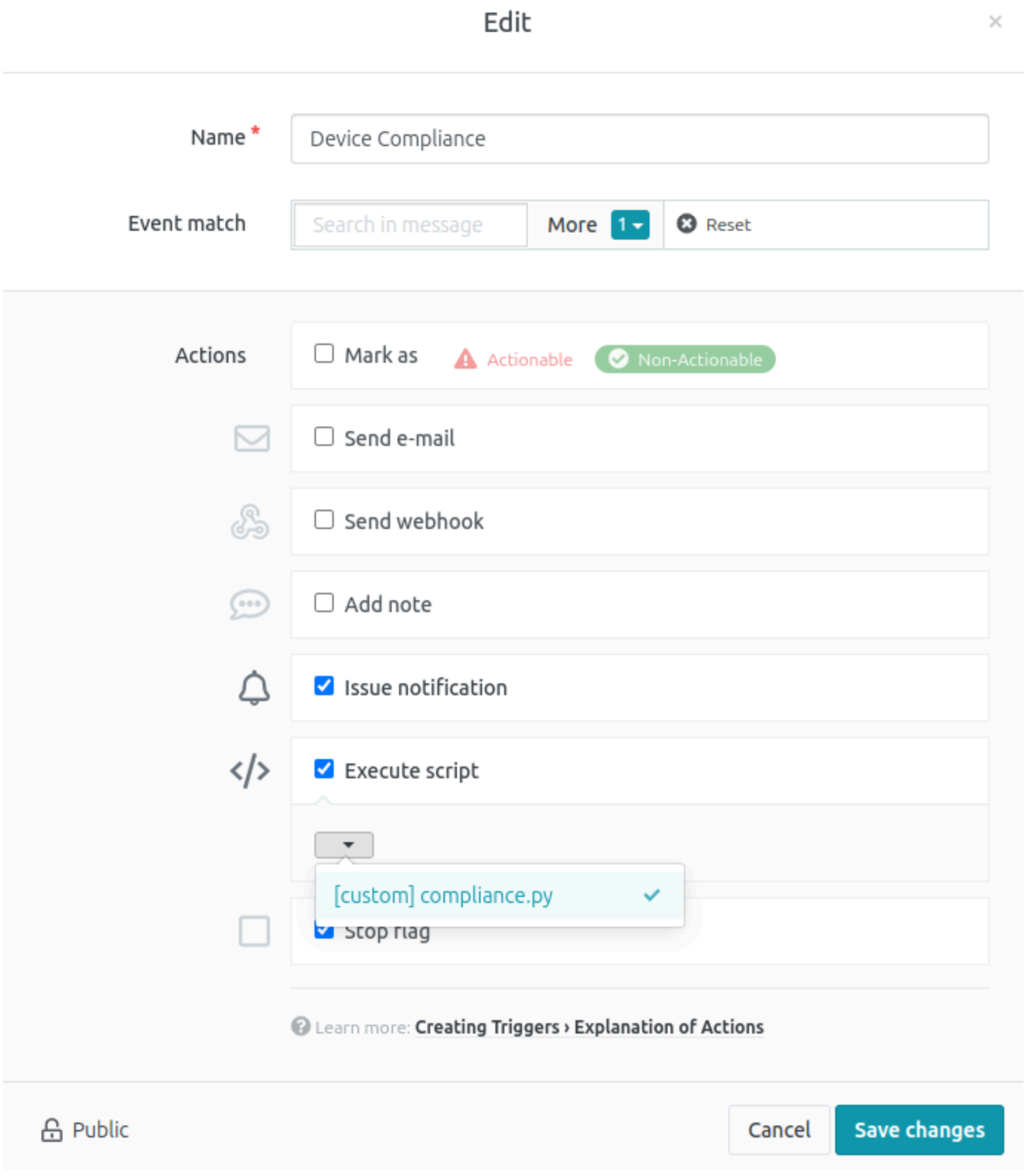
Selecting this option will produce a notification that will increment in the page header, and show up on the notifications page.



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) 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 flag
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.