LOGZILLA DOCUMENTATION

Trigger Page

Create and order LogZilla triggers from the Triggers page, matching on user tags, severity, and message content to drive downstream actions

LogZilla Triggers · Generated May 3, 2026 · logzilla.ai/docs/creating-triggers/trigger-page

Trigger Firing Order

Note that the order in which triggers are listed are the same order they will be matched upon (from top to bottom of the page). Once a match is made and stop flag is enabled for the trigger, no other triggers are processed. Thus, it is important that users start with the most finite matches and prioritize wider ranging matches further down the list.

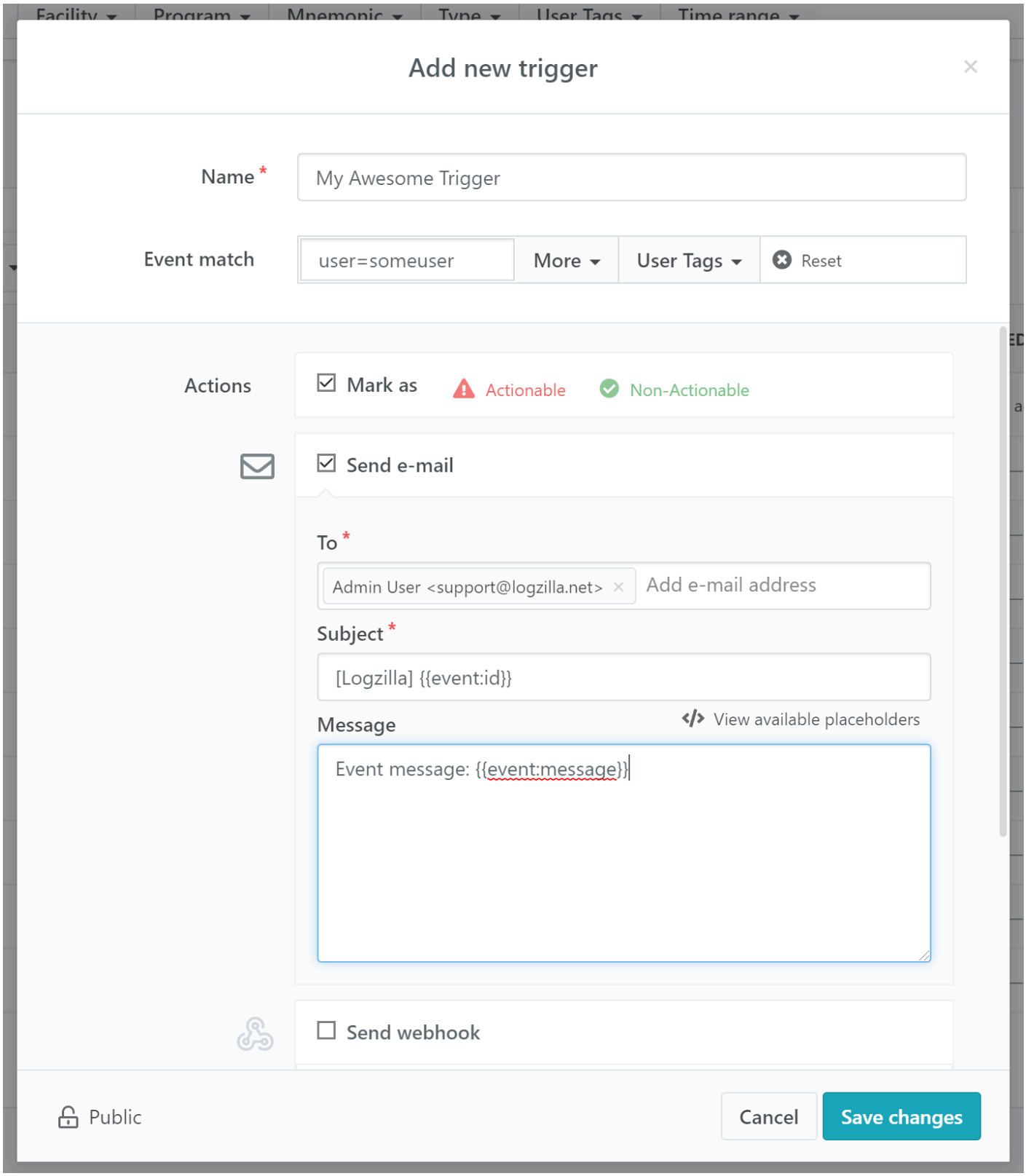
For example, a match on `interface` would match `interface GigabitEthernet1/0/1`, `interface GigabitEthernet1/0/2`, etc., then stop processing further rules.

Instead, users may want a more finite match such as `GigabitEthernet1/0/1` to be ordered higher (or lower depending on the intent).

Creating a Trigger

In the LogZilla UI, click the 'Triggers' link in the top menu. There, users will see a button near the top of the page 'Add new trigger', and below that a list of any triggers already created on the server. Clicking the button will allow users to create a trigger with no pre-set information selected. This is the easiest way to create triggers that will apply to the widest range of conditions.

If users would like to monitor failed logins for all servers, this is the best place to do it. Simply click the button, give the new trigger a name, and enter the search criteria, 'failed login' in the 'Event match' section. By default, 'Issue Notification' is already selected, so for a system wide rule, that's all that is needed. Just click 'Save changes' and the trigger will be active.



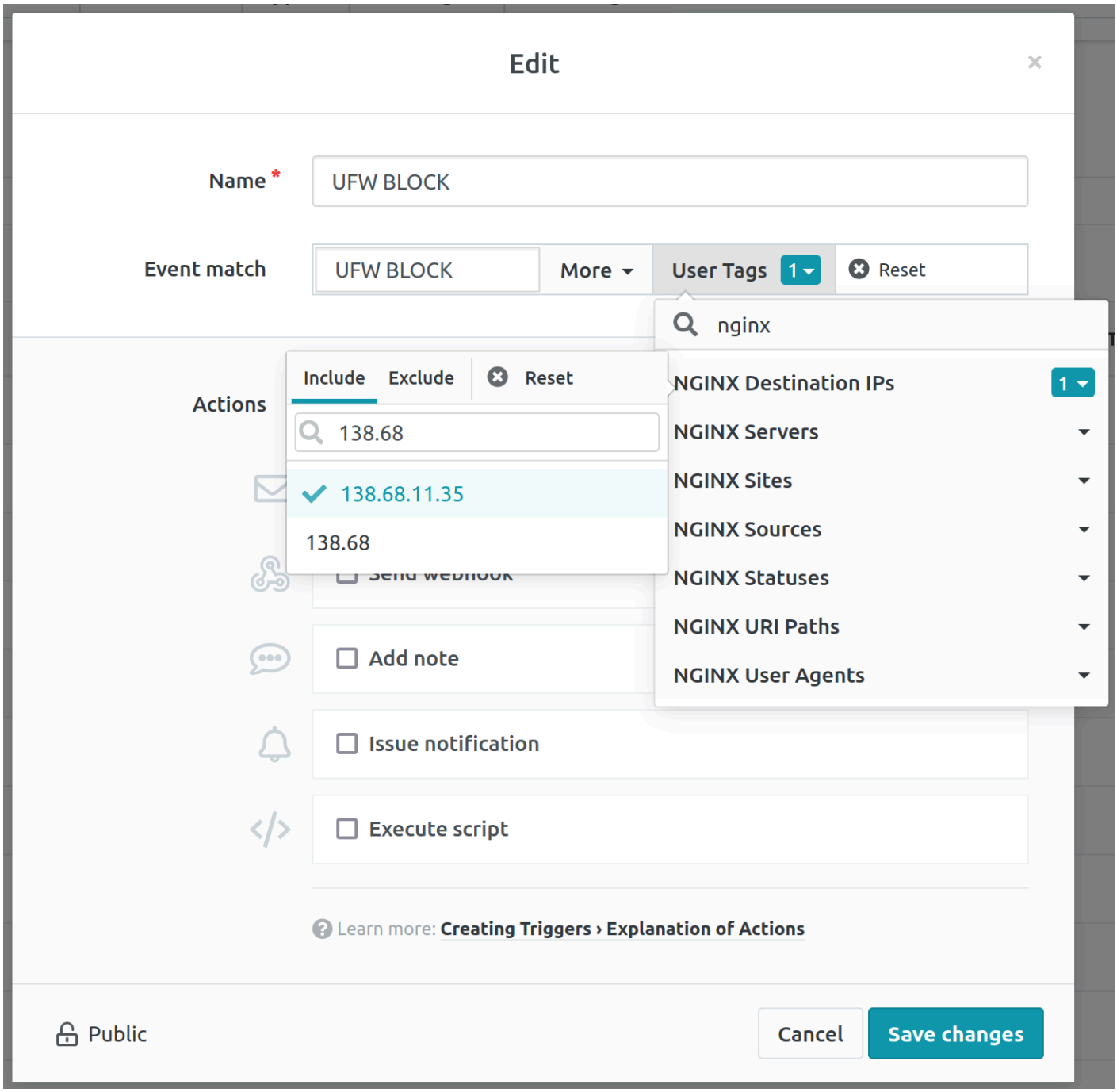
User tags can be used in the filter. User tags are special key/value pairs associated with each individual event. The LogZilla rules can parse the data in each event message and then set specific named (configurable) tags to values from the event data. For

example, some common tags are `DstIP` and `DstPort`, respectively representing the destination IP address and the destination IP port for the given event. User tag `DstIP` could for example have value `192.168.0.2`.

Triggering events can be filtered based on user tags. If the "User Tag" dropdown is selected, optionally at the top of the dropdown a filter for the desired user tag name can be entered (such as if user tag `DstPort` is desired then "Dst" can be entered in the search field at the top of the dropdown, and each user tag with a name containing "Dst", such as `DstPort` will be listed).

Once the desired user tag is shown it can be clicked to open the values dropdown. The values dropdown allows choosing the particular values for the given user tag either to be included or excluded, such that only those events with the chosen values for the designated user tag will cause the trigger, or those with the chosen values will be specifically excluded from causing the trigger. The top of this dropdown as well contains the search box to find particular values of interest. Multiple user tag values can be chosen by clicking on each and a check mark will be shown next to those so designated as an indicator, or the checked ones can be clicked once more to deselect them.

A special value of `*` can be typed in, then selected. This value has special meaning: it selects only those events that have *some* value for the designated user tag. This is useful because not every event may contain every user tag. For example there may be events that have no SrcPort, and those events are not desired to be included. In order to select only those events that have a value for SrcPort, without distinction of what that value is, the `*` filter value should be used.


Edit
Name *
UFW BLOCK
Event match
UFW BLOCK
More
User Tags 1
Reset
nginx
NGINX Destination IPs 1
NGINX Servers
NGINX Sites
NGINX Sources
NGINX Statuses
NGINX URI Paths
NGINX User Agents
Actions
Include
Exclude
Reset
138.68
138.68.11.35
138.68
Add note
Issue notification
Execute script
Learn more: Creating Triggers › Explanation of Actions
Public
Cancel
Save changes