WATS Feature Release Note
Alarms and Notification Webhook action
Preview

Major Feature Areas

Overview

This release introduces new functionality for the existing Alarms and Notifications system, allowing users to set custom webhooks that will run when the alarm is triggered. This provides increased connectivity to external systems, such as ERP, MES, or other third-party platforms, and allows for additional options when designing and introducing Alarms and Notifications on your WATS instance.

Webhooks will be released in a preview state, so functionality and design may change before the full release.

Webhook actions

Webhook actions can be configured in the Alarms and Notifications section of the Control Panel

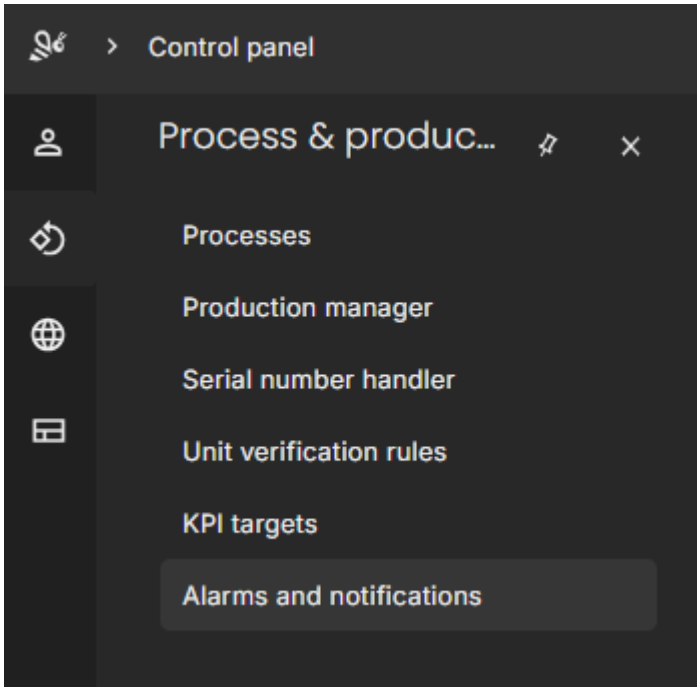

Figure 1: Alarms and Notifications in Control Panel

For each individual rule

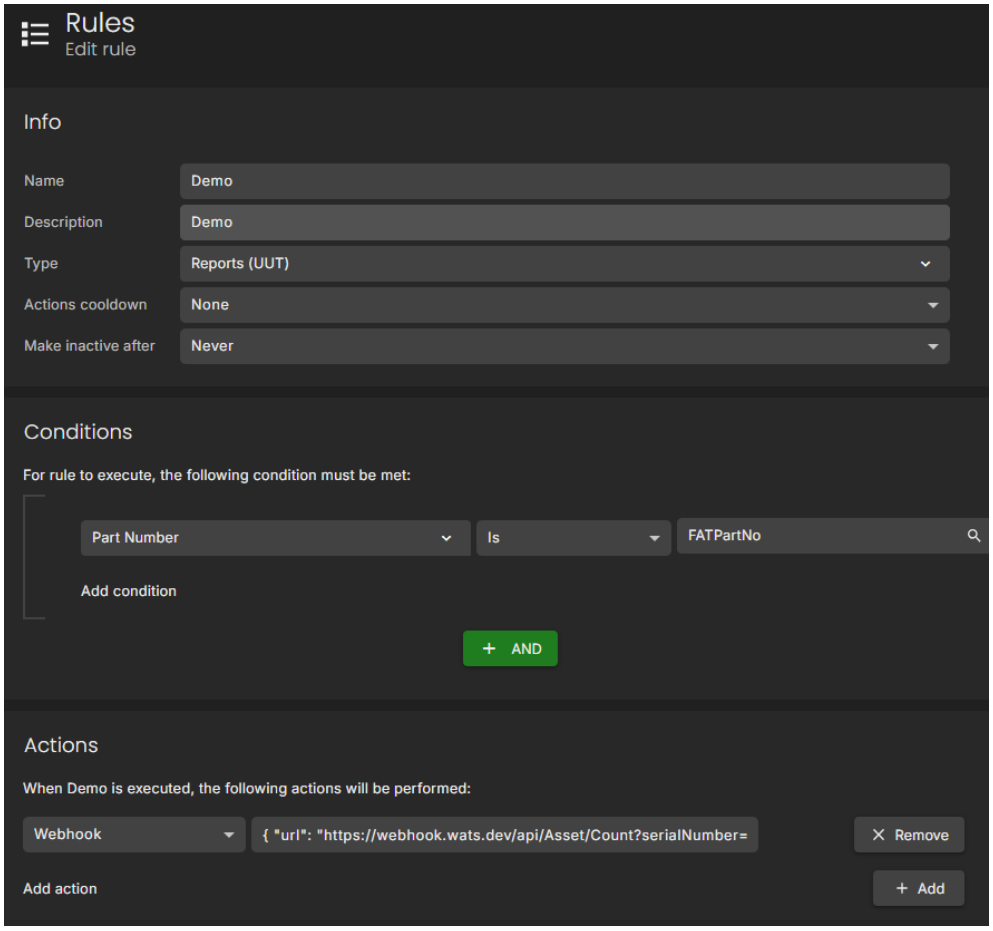

Figure 2: Edit rules showing Webhook action

Information on configuring a webhook can be found in the User Manual under the Alarms and Notifications section or read below.

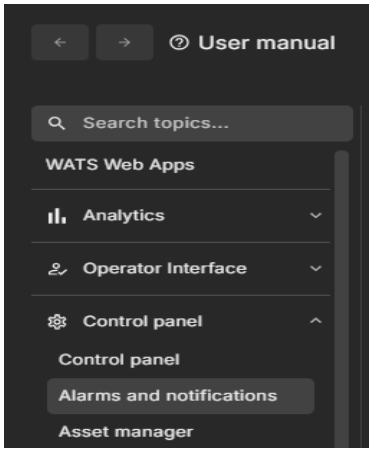

Figure 3: Location of documentation in User Manual

Webhook action sends a http request to a custom endpoint. Specify:

url	URL to the endpoint WATS should call, including https:// and query parameters, if any.
headers	Key-value pairs of any http header values, e.g. Authorization, ETag, or any other, known or custom.
method	Http method to send the request with, i.e. GET, POST, PUT, PATCH, DELETE, etc.
messageType	How the http body of the request will be formatted. Supports sending each rule execution separately, or multiple rule executions in an array.

During preview, the options above need to be specified in a JSON format in the text field like this:

{ "url": "**https://172.192.0.1/watsalarm**", "headers": { "Authorization": "Basic " }, "method": "POST", "messageType": 1 }

where messageType is

0	Send each rule execution in separate http requests.
1	Send all new rule executions in one http request.

Request body

WATS will send a request with an application/json body in this format:

```
{
	"triggerName": "Example trigger",
	"triggerDesc": "Example trigger description",
	"host": "https://yourserver.wats.com",
	"events": [
		{
			"logId": 13,
			"name": "Example trigger",
			"logDate": "2026-05-22T14:05:34.643Z",
			"triggerId": 4,
			...
		},
		{
			"logId": 14,
			"name": "Example trigger",
			"logDate": "2026-05-22T14:05:34.811Z",
```

```
                    "triggerId": 4,
                    ...
                },
        ]
        "event":
        {
                "logId": 13,
                "name": "Example trigger",
                "logDate": "2026-05-22T14:05:34.643Z",
                "triggerId": 4,
                ...
        }
}
```


Either events or event will be present, depending on messageType.
The "..." refers to that each event will have more properties that depend on the rule type and conditions.

Considerations

WATS needs to receive a 2xx http status code back from the endpoint within 100 seconds. If it does not it will consider the request failed and try again.
Each rule can only have one webhook action, and webhook action cannot be combined with other actions.