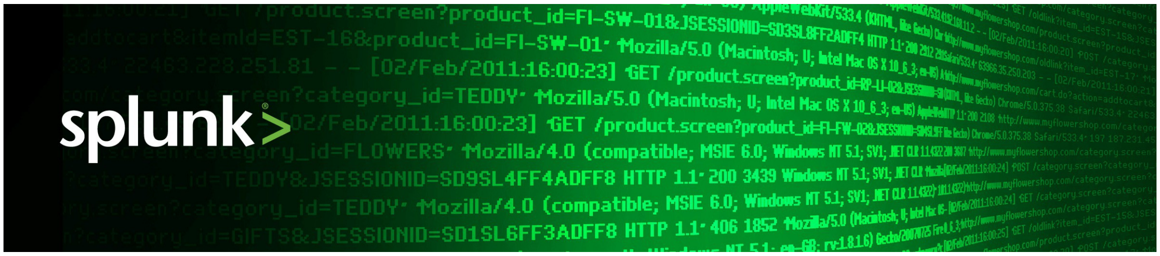

# Splunk® Enterprise Knowledge Manager Manual 7.2.5

## About workflow actions in Splunk Web

Generated: 4/06/2019 9:50 am

# About workflow actions in Splunk Web

Enable a wide variety of interactions between indexed or extracted fields and other web resources with **workflow actions**. Workflow actions have a wide variety of applications. For example, you can define workflow actions that enable you to:

- Perform an external WHOIS lookup based on an IP address found in an event.
- Use the field values in an HTTP error event to create a new entry in an external issue management system.
- Launch secondary searches that use one or more field values from selected events.
- Perform an external search (using Google or a similar web search application) on the value of a specific field found in an event.

In addition, you can define workflow actions that:

- Are targeted to events that contain a specific field or set of fields, or which belong to a particular event type.
- Appear either in field menus or event menus in search results. You can also set them up to only appear in the menus of specific fields, or in all field menus in a qualifying event.
- When selected, open either in the current window or in a new one.

## Define workflow actions using Splunk Web

You can set up workflow actions using Splunk Web. To begin, navigate to **Settings > Fields > Workflow actions**. On the Workflow actions page, you can review and update existing workflow actions by clicking on their names. Or you can click **Add new** to create a new workflow action. Both methods take you to the workflow action detail page, where you define individual workflow actions.

If you're creating a new workflow action, you need to give it a **Name** and identify its **Destination app**.

There are three kinds of workflow actions that you can set up.

| Workflow action type | Description |
|---|---|
| GET workflow | GET workflow actions create typical HTML links to do things like perform Google searches on specific values or run domain name |

| Workflow action type | Description |
|---|---|
| actions | queries against external WHOIS databases. |
| POST workflow actions | POST workflow actions generate an HTTP POST request to a specified URI. This action type enables you to do things like creating entries in external issue management systems using a set of relevant field values. |
| Search workflow actions | Search workflow actions launch secondary searches that use specific field values from an event, such as a search that looks for the occurrence of specific combinations of `ipaddress` and `http_status` field values in your index over a specific time range. |

## Target workflow actions to a narrow grouping of events

When you create workflow actions in Splunk Web, you can optionally target workflow actions to a narrow grouping of events. You can restrict workflow action scope by field, by event type, or a combination of the two.

### *Narrow workflow action scope by field*

You can set up workflow actions that only apply to events that have a specified field or set of fields. For example, if you have a field called `http_status`, and you would like a workflow action to apply only to events containing that field, you would declare *http_status* in the **Apply only to the following fields** setting.

If you want to have a workflow action apply only to events that have a *set* of fields, you can declare a comma-delimited list of fields in **Apply only to the following fields**. When more than one field is listed the workflow action is displayed only if *the entire list* of fields are present in the event.

For example, say you want a workflow action to only apply to events with `ip_client` and `ip_server` fields. To do this, you would enter *ip_client, ip_server* in **Apply only to the following fields**.

Workflow action field scoping also supports use of the wildcard asterisk. For example, if you declare a simple field listing of *ip_** Splunk software applies the resulting workflow action to events with either `ip_client` or `ip_server` as well as a combination of both (as well as any other event with a field that matches *ip_**).

By default the field list is set to *, which means that it matches all fields.

If you need more complex selecting logic, we suggest you use event type scoping instead of field scoping, or combine event type scoping with field scoping.

### *Narrow workflow action scope by event type*

Event type scoping works the same way as field scoping. You can enter a single event type or a comma-delimited list of event types into the **Apply only to the following event types** setting to create a workflow action that only applies to events belonging to that event type or set of event types. You can also use wildcard matching to identify events belonging to a range of event types.

You can also narrow the scope of workflow actions through a combination of fields and event types. For example, if you have a field called `http_status`, but you only want the resulting workflow action to appear in events containing that field if the `http_status` is greater than or equal to 500. To accomplish this, you would need to set up an event type called `errors_in_500_range` that is applied to events matching a search like

```
http_status >= 500
```

Then, you would define a workflow action that has **Apply only to the following fields** set to *http_status* and **Apply only to the following event types** set to *errors_in_500_range*.

For more information about event types, see About event types in this manual.