Mako Webhooks for Splunk

Setup Instructions

August 2021

Document Purpose

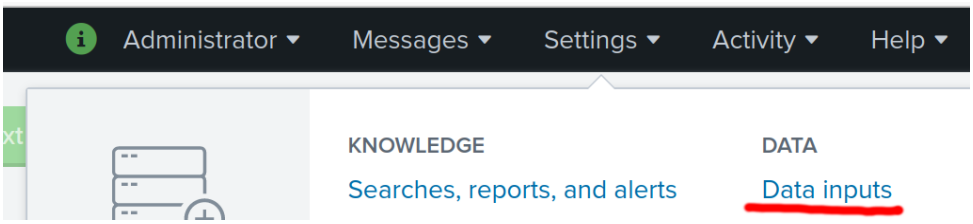
This document defines how to use the webhooks feature of the Mako system to receive notifications in your Splunk service.

Table of Contents

Configuration Steps

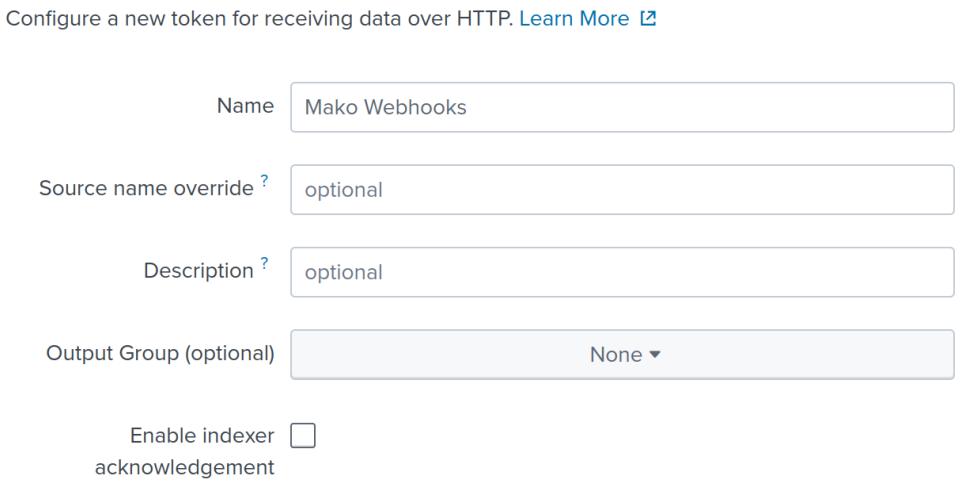
This document assumes you already have a Splunk service installed.

Step 1: Create a new HEC data input in Splunk

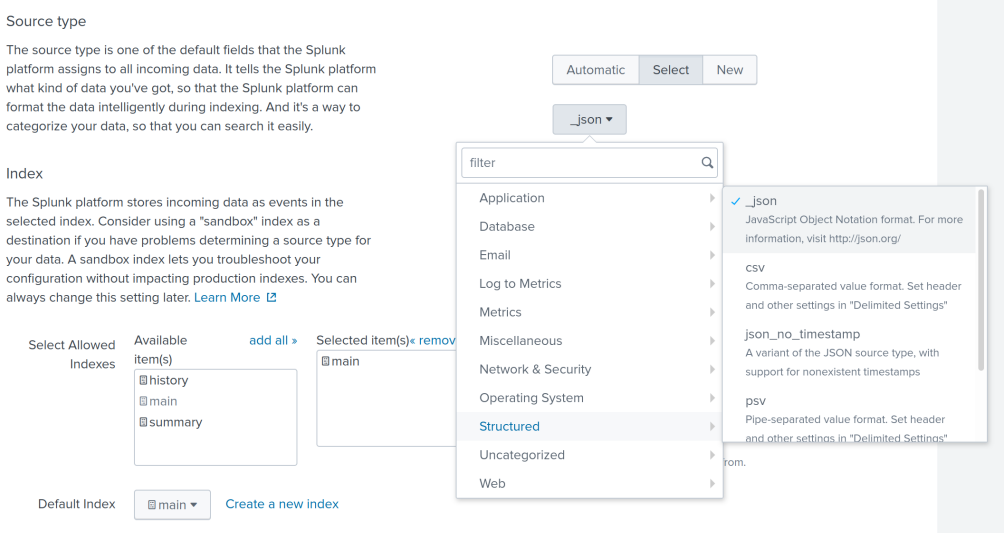


Step 2: Locate "HTTP Event Collector" and click "Add new"

Step 3: Enter a name e.g. "Mako Webhooks" and click "Next"

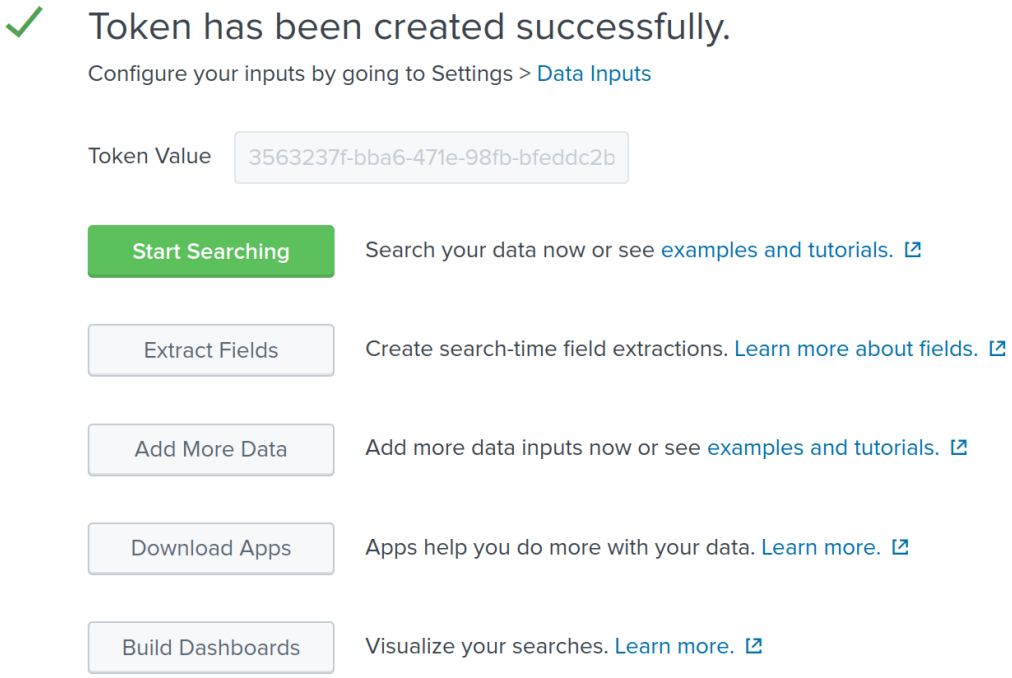


Step 4: Change "Source type" to "_json" - click "Select" -> Structured -> _json. Select the index you want the data stored in, e.g. "main"

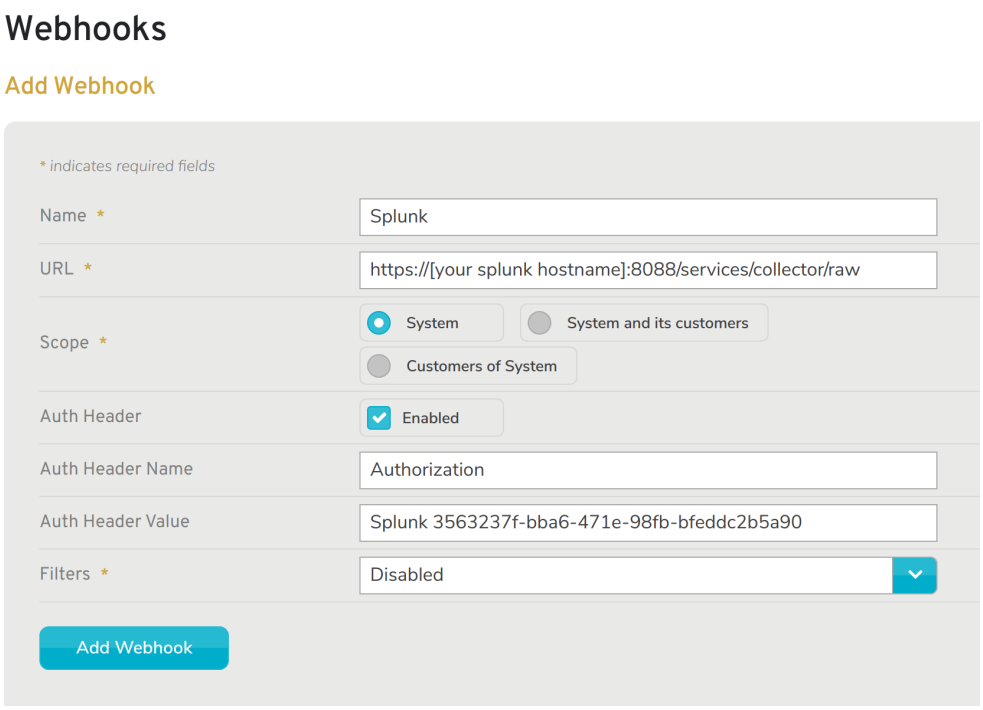


Step 5: Review the changes and click "Next"

Step 6: The token has now been created. Make note of "Token Value" - you will need it Webhook configuration in CMS. Click "Start Searching" and keep the page open.



Step 7: Login to the Mako CMS. Select a company and go to Companies -> Manage X -> API -> Webhooks. Fill in the data using the template below, using your Splunk details and the auth token generated in previous step. Make sure to use appropriate Splunk port and the "raw" collector. Click "Add Webhook".



Step 8: Perform some change to a Mako, e.g. change Mako name. The events will now be in Splunk.