



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

DOCUMENT PURPOSE 2

TABLE OF CONTENTS 2

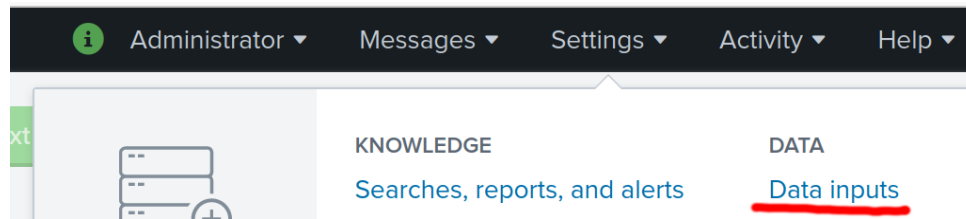
MICROSOFT TEAMS SETUP ERROR! BOOKMARK NOT DEFINED.

SLACK SETUP ERROR! BOOKMARK NOT DEFINED.

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"

Configure a new token for receiving data over HTTP. [Learn More](#)

Name

Source name override ?

Description ?

Output Group (optional)

Enable indexer acknowledgement ☐

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

Source type

The source type is one of the default fields that the Splunk platform assigns to all incoming data. It tells the Splunk platform what kind of data you've got, so that the Splunk platform can format the data intelligently during indexing. And it's a way to categorize your data, so that you can search it easily.

Index

The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. [Learn More](#)

Select Allowed Indexes

add all >

Available item(s)

- history
- main
- summary

Selected item(s) remove

- main

Default Index

main

Create a new index

Automatic Select New

_json

filter

- Application
- Database
- Email
- Log to Metrics
- Metrics
- Miscellaneous
- Network & Security
- Operating System
- Structured
- Uncategorized
- Web

✓ _json

JavaScript Object Notation format. For more information, visit <http://json.org/>

csv

Comma-separated value format. Set header and other settings in "Delimited Settings"

json_no_timestamp

A variant of the JSON source type, with support for nonexistent timestamps

psv

Pipe-separated value format. Set header and other settings in "Delimited Settings"

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.



Token has been created successfully.

Configure your inputs by going to Settings > [Data Inputs](#)

Token Value

Start Searching

Search your data now or see [examples and tutorials](#).

Extract Fields

Create search-time field extractions. [Learn more about fields](#).

Add More Data

Add more data inputs now or see [examples and tutorials](#).

Download Apps

Apps help you do more with your data. [Learn more](#).

Build Dashboards

Visualize your searches. [Learn more](#).

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".

Webhooks

Add Webhook

* indicates required fields

Name *	<input type="text" value="Splunk"/>
URL *	<input type="text" value="https://[your splunk hostname]:8088/services/collector/raw"/>
Scope *	<input checked="" type="radio"/> System <input type="radio"/> System and its customers <input type="radio"/> Customers of System
Auth Header	<input checked="" type="checkbox"/> Enabled
Auth Header Name	<input type="text" value="Authorization"/>
Auth Header Value	<input type="text" value="Splunk 3563237f-bba6-471e-98fb-bfeddc2b5a90"/>
Filters *	<input type="text" value="Disabled"/> <input type="button" value="v"/>

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

	List ▾	Format	20 Per Page ▾
fields	i	Time	Event
>	8/25/21 9:50:26.000 AM	{ [-] makoData: { [+] } text: Address Changed - System, Aardvark, Aardvarkx Mako set to System, Aardvark, Aardvark Name changed from Aardvarkx to Aardvark Unchanged: Company remains unchanged at System Event created by admin2 admin2 (System). } Show as raw text	host = localhost:12313 source = http:Mako Webhooks sourcetype = _json