

PROCESS MANUAL

Document Code: PM-SPI

Splunk

Integration

VERSION 1.0

Send Auditlog data to your Splunk setup.

 **Admin By Request**
By FastTrack Software

Table of Contents

Introduction.....	3
Assumptions / Limitations.....	3
Breakdown of Tasks.....	3
Integration Tasks.....	4
Task A: Set Up a Splunk HEC Channel.....	4
Task B: Define Webhook.....	7
Task C: Receive Events.....	10

Introduction

Splunk is a tool that makes complex data much easier to understand and utilize by collecting, analyzing, and storing it in a structured format, which can then be indexed and searched easily.

We've created an integration which allows you to get Admin By Request Auditlog data sent to your Splunk environment using Splunk's HTTP Event Collection (HEC) functionality combined with Admin By Request webhooks.

This manual provides a step-by-step guide on how to configure the above and make better use of valuable security data collected by Admin By Request.

Assumptions / Limitations

The tasks described in this manual assume that the user has access to Splunk, the Admin By Request User Portal, and some familiarity with both environments.

If you are using Splunk Cloud, this document assumes you have super-admin permissions in order to access Global Settings (required in Task A, step 7).

Breakdown of Tasks

Three tasks are covered in this manual:

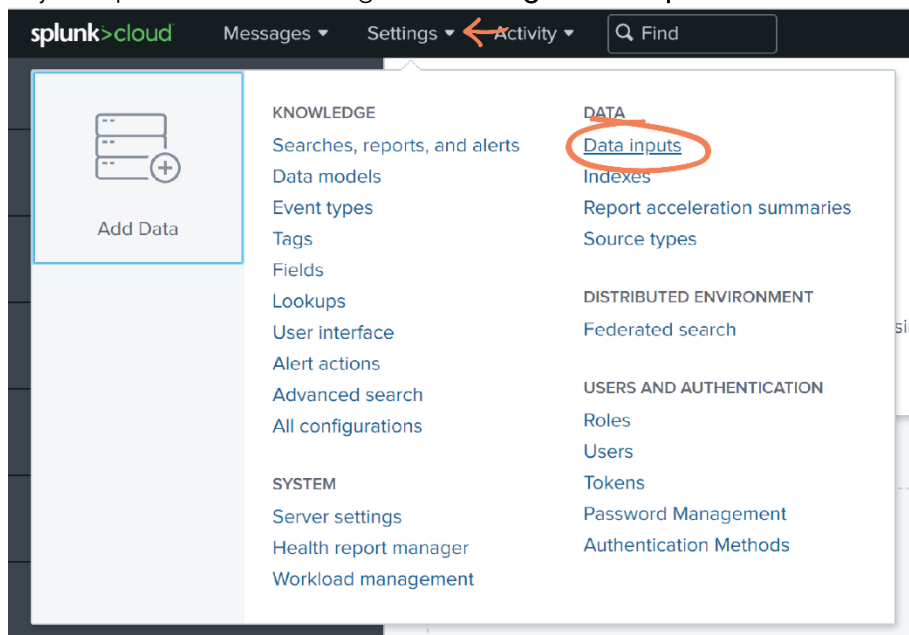
1. Task A: Set Up Splunk HEC Channel
2. Task B: Define Webhook
3. Task C: Receive Events

Integration Tasks

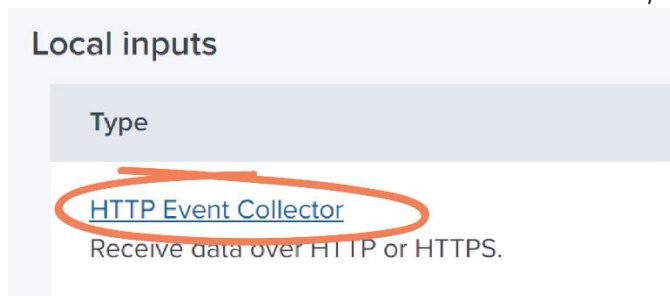
Task A: Set Up a Splunk HEC Channel

HEC is essentially an HTTP endpoint for your Splunk instance with an authorization token, which allows you to send data into Splunk.

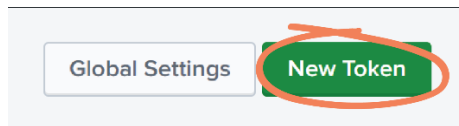
1. In your Splunk instance, navigate to **Settings > Data inputs**:



2. Select **HTTP Event Collector** from the list of *Local inputs*.



3. Click the **New Token** button from the top-right corner:



4. Enter a **Name** and **Description** as desired:

Name

Source name override ?

Description ?

Enable indexer acknowledgement ☐



NOTE: In this example, our Token is called *Admin By Request Events* and the Description reads: *Receives Auditlog data from Admin By Request*.

5. Click **Next** and continue with the setup as appropriate for your organization:

Progress bar: Select Source (filled), Input Settings, Review, Done

< Back **Next >**

6. Click **Review**, then **Submit**:

< Back **Review >** < Back **Submit >**

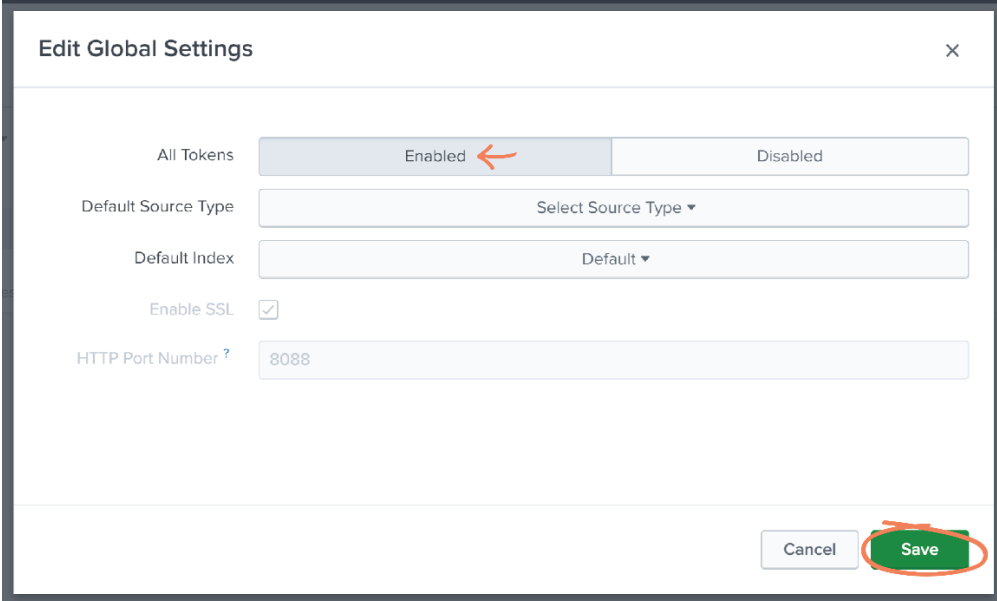
7. Navigate back to the *HTTP Event Collector* page (**Settings > Data inputs > HTTP Event Collector**) and select the **Global Settings** button at the top-right of the page:

Global Settings **New Token**



IMPORTANT: If you are using Splunk Cloud, only the super-admin has access to Global Settings.

8. Ensure the *All Tokens* option is set to **Enabled**, and click **Save**:



Edit Global Settings [X]

All Tokens: Enabled ← Disabled

Default Source Type: Select Source Type ▾

Default Index: Default ▾

Enable SSL: ☒

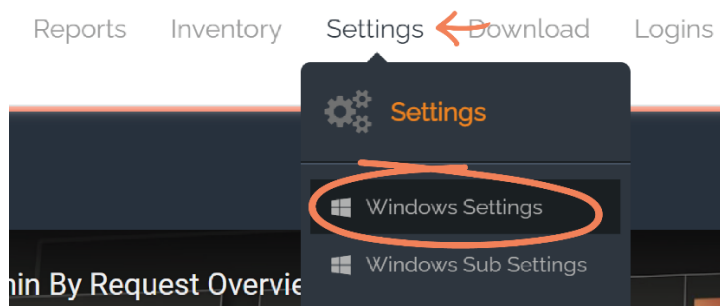
HTTP Port Number ? : 8088

Cancel Save

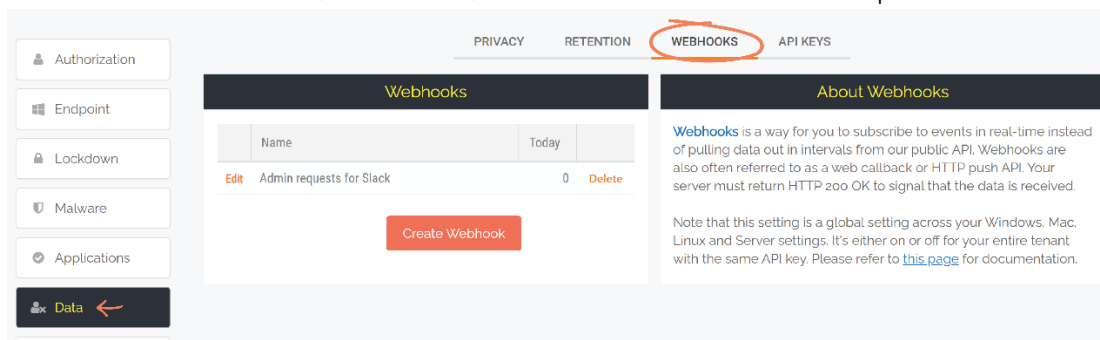
Task B: Define Webhook

With Admin By Request webhooks (also referred to as a web callback or HTTP push API) you can subscribe to events in real-time instead of pulling data out in intervals.

1. In your Admin By Request User Portal, navigate to **Settings > Windows Settings**:



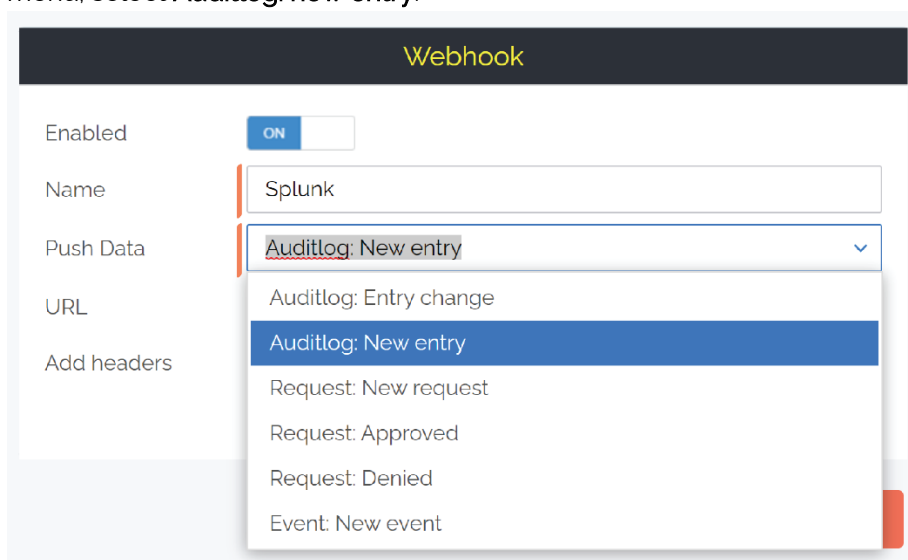
2. From the left-hand menu, select **Data**, and then **Webhooks** from the top tab menu:



3. Select the **Create Webhook** button:

Create Webhook

4. **Name** the new webhook (in this example, *Splunk*), and from the *Push Data* drop-down menu, select **Auditlog: new entry**:



5. In the URL field, a string of the following format is required:

- `https://inputs.pr-d-Your Splunk ID.splunkcloud.com:8088/services/collector/raw`

So, if your Splunk URL is `https://prd-p-xxxxx.splunkcloud.com`, then your HEC URL would look something like:

- `https://inputs.pr-d-xxxxx.splunkcloud.com:8088/services/collector/raw`

If you are using Splunk Cloud, then the Splunk URL might look something like:

- `https://http-inputs-[SPLUNK ID].splunkcloud.com:443/services/collector/raw`

Where [Splunk ID] is your Splunk tenant ID.

! IMPORTANT: Be aware that this may vary based on your Splunk settings. If in doubt, consult your Splunk representative to ensure that you use the correct publicly available HEC endpoint for your Splunk solution.

The screenshot shows a 'Webhook' configuration panel. It includes a toggle for 'Enabled' (ON), a text field for 'Name' (Splunk), a dropdown for 'Push Data' (Auditlog: New entry), a text field for 'URL' (https://inputs.pr-d-xxxxx.splunkcloud.com:8088/services/collector/raw), and a toggle for 'Add headers' (OFF).

6. Set the *Add headers* toggle to **ON**:

A close-up of the 'Add headers' toggle switch, which is circled in red and set to 'ON'.

7. Select **New**:

A button labeled 'New' in orange text.

8. In the **Name** field, type *Authorization*, and in the **Value** field, *Splunk*:

Name	Value	New
Name: <input type="text" value="Authorization"/>	Value: <input type="text" value="Splunk"/>	<input type="button" value="Update"/> <input type="button" value="Cancel"/>

9. Navigate back to your Splunk instance and highlight and copy the **Token Value** provided in the HTTP Event Collector created in Task A:

Token Value

 **NOTE:** The **Token Value** has been blurred out in the above example.

10. Navigate back to your new Header in the Admin By Request User Portal, paste the copied **Token Value** next to *Splunk* in the *Value* field, and click **Update**:

Value:

Splunk

Update

Cancel

11. **Save** the new webhook:

Save

Cancel

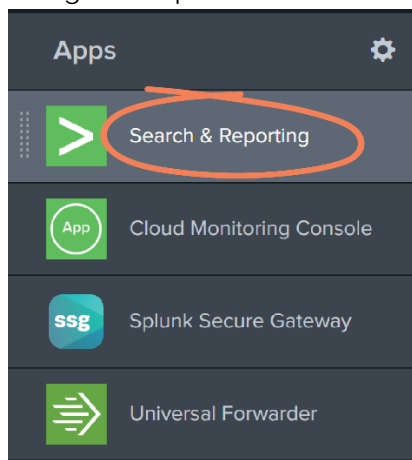
 **NOTE:** The new Splunk webhook is now listed in the Webhooks section:

Webhooks			
	Name	Today	
Edit	Admin requests for Slack	0	Delete
Edit	Splunk	0	Delete
<div>Create Webhook</div>			

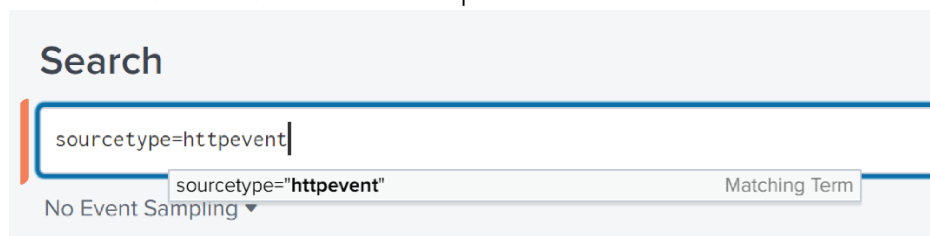
Task C: Receive Events

Auditlog events, such as Requests for elevated access, are now sent to the HEC endpoint.

1. Navigate to Splunk home and select **Search & Reporting** from the left-hand menu:



2. Use the *Search* field to search for http events:



3. Recent Admin By Request events are detailed here. In this example, we see a Request to run Adobe Acrobat DC as Admin, displaying details on *application*, *computer*, *reason* (for request), *scanResults*, and *user*.

i	Time	Event
>	23/08/2022 22:32:34.000	<pre> { [-] application: { [+] } approvedBy: null auditLogLink: https://www.adminbyrequest.com/AuditLog?Page=AppElevations&ID=92588697&ShowFilter=false computer: { [+] } deniedBy: null deniedReason: null elevatedApplications: [[+]] endTime: null endTimeUTC: null id: 111875931 installs: [[+]] reason: Splunk Demo requestTime: 2022-08-24T00:32:29 requestTimeUTC: 2022-08-24T00:32:29 responseTime: null scanResults: [[+]] settingsName: Global startTime: null startTimeUTC: null status: Pending approval statusCode: 4 traceNo: 92588697 type: Run As Admin typeCode: 0 uninstalls: [[+]] user: { [+] } } </pre> <p>Show as raw text</p>



NOTE: Use the + (plus) icon to expand key sections and display more information on each:

```
> 23/08/2022 22:32:34.000 { [-]
  application: { [-]
    file: Acrobat.exe
    name: Adobe Acrobat DC
    path: C:\Program Files\Adobe\Acrobat DC\Acrobat
    preapproved: false
    scanResult: Clean
    scanResultCode: 0
    sha256: 70BB9A2DCC19FA6B15FF974E2A5016D54EDDE9FE0F26B67E6B96D20865CB1517
    threat: null
    vendor: Adobe Inc.
    version: 22.2.20191.0
    virustotalLink: https://www.virustotal.com/latest-scan/70BB9A2DCC19FA6B15FF974E2A5016D54EDDE9FE0F26B67E6B96D20865CB1517
  }
}
```