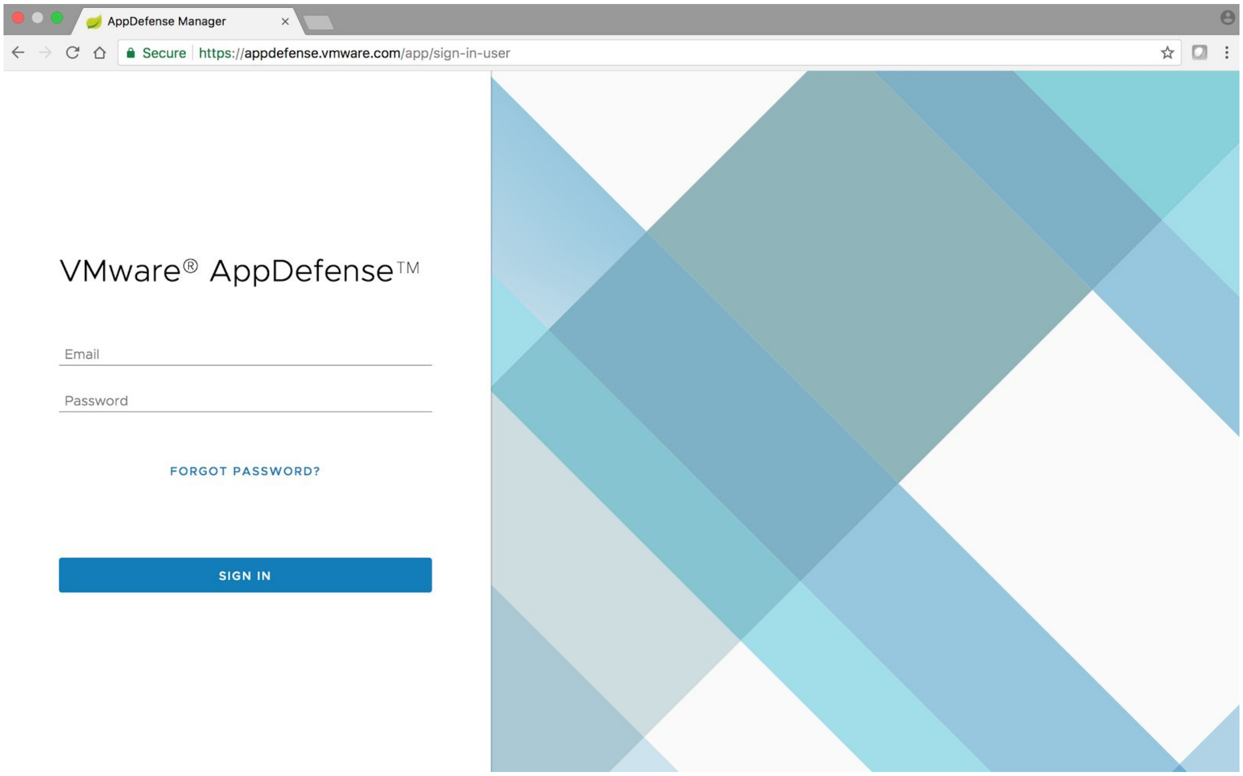
AppDefense Splunk App Configuration Guide

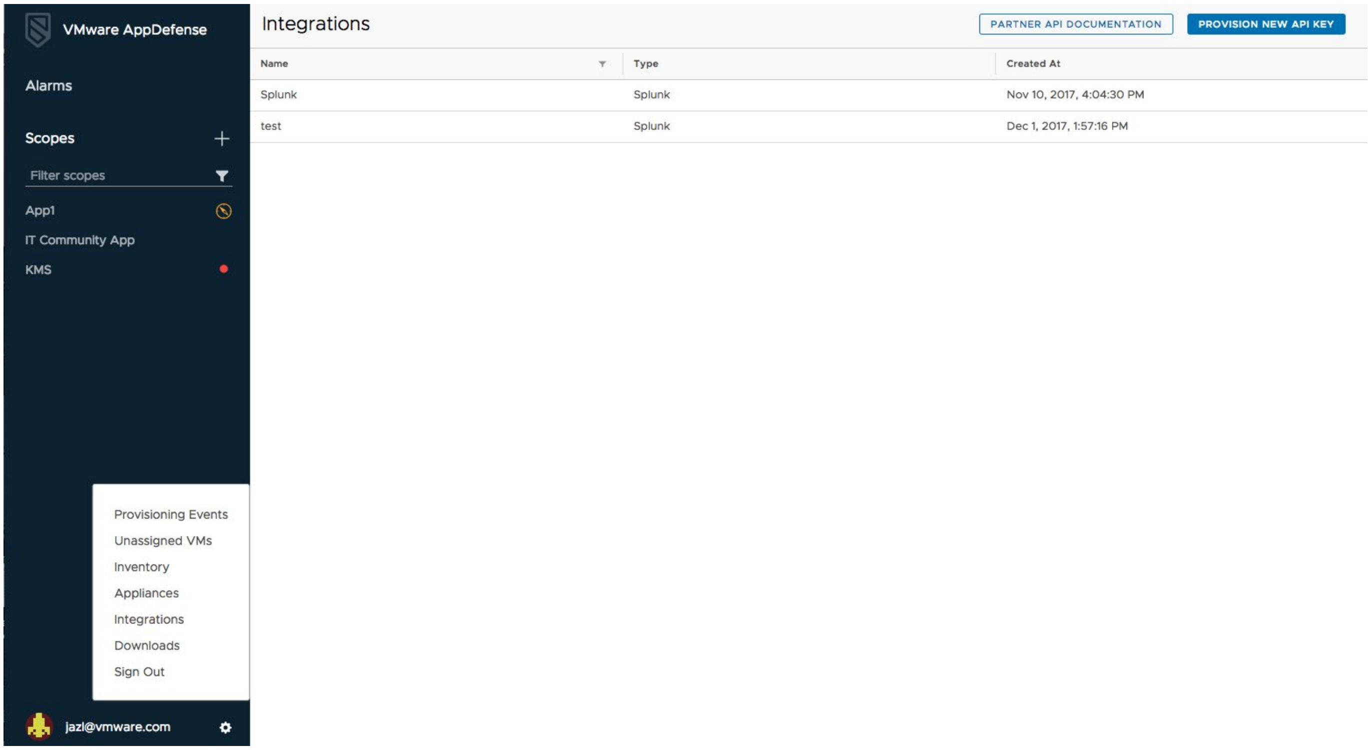
This document covers the steps required to integrate AppDefense with Splunk. Once integrated, the alarms (and their metadata) on AppDefense can be viewed on Splunk. This setup is for standalone Splunk instead where Search Head is same as indexer.

Steps To Integrate On AppDefense

1. Login to your AppDefense account by visiting the URL: https://appdefense.vmware.com.



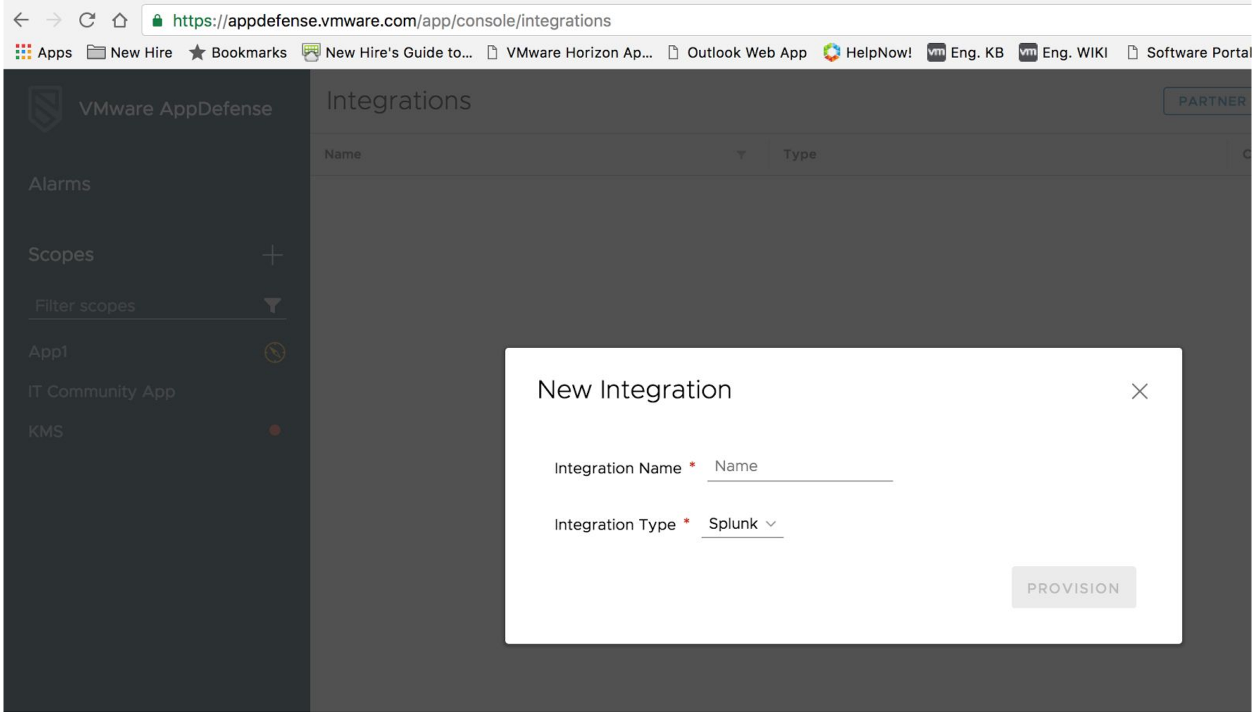
1. Click the setting icon on the lower left side of the panel and Select “Integrations”



Integrations

Name	Type	Created At
Splunk	Splunk	Nov 10, 2017, 4:04:30 PM
test	Splunk	Dec 1, 2017, 1:57:16 PM

2. Click on Provision New API KEY and choose Splunk from the drop-down list

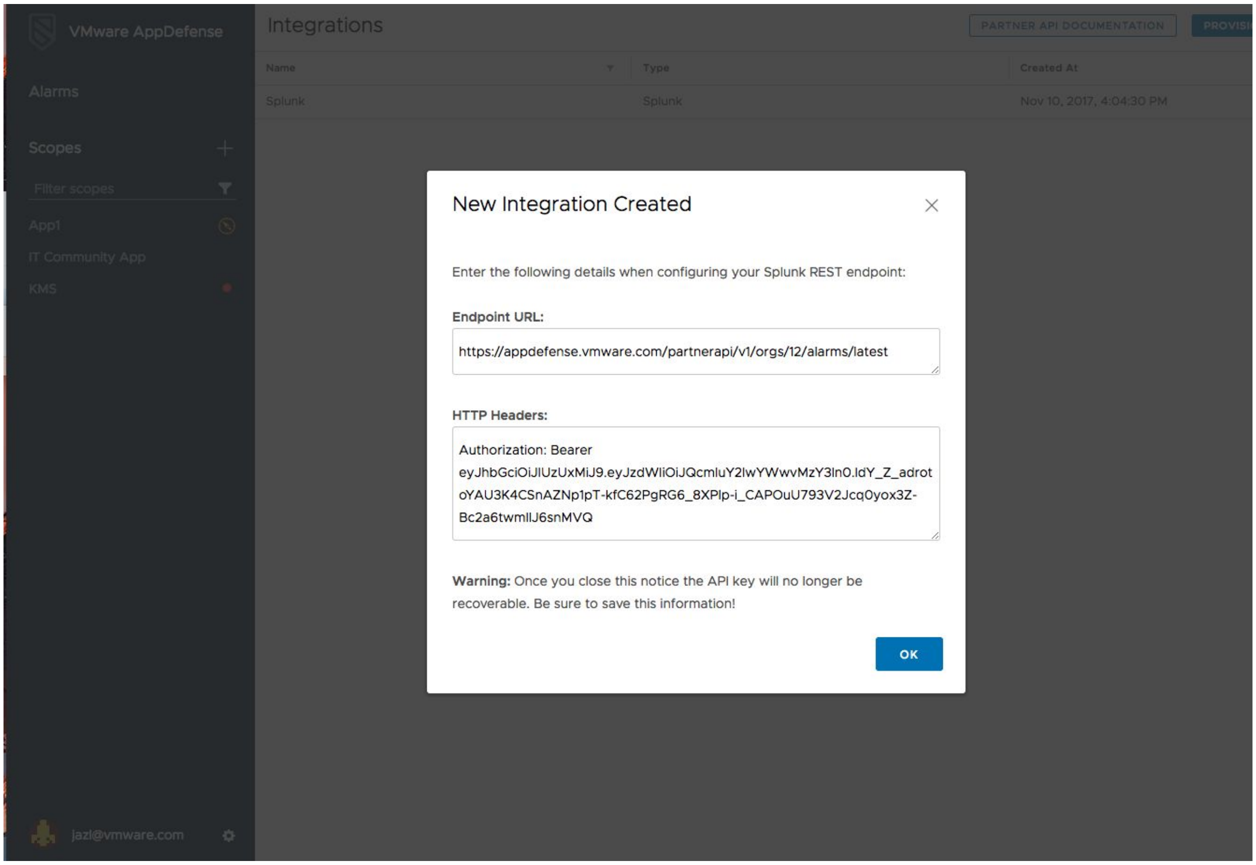


New Integration

Integration Name * Name

Integration Type * Splunk

3. Take a note of the URL and authorization key. The authorization key will need to be stored secretly and cannot be retrieved from AppDefense once the dialog is closed.



Name	Type	Created At
Splunk	Splunk	Nov 10, 2017, 4:04:30 PM

New Integration Created

Enter the following details when configuring your Splunk REST endpoint:

Endpoint URL:

```
https://appdefense.vmware.com/partnerapi/v1/orgs/12/alarms/latest
```

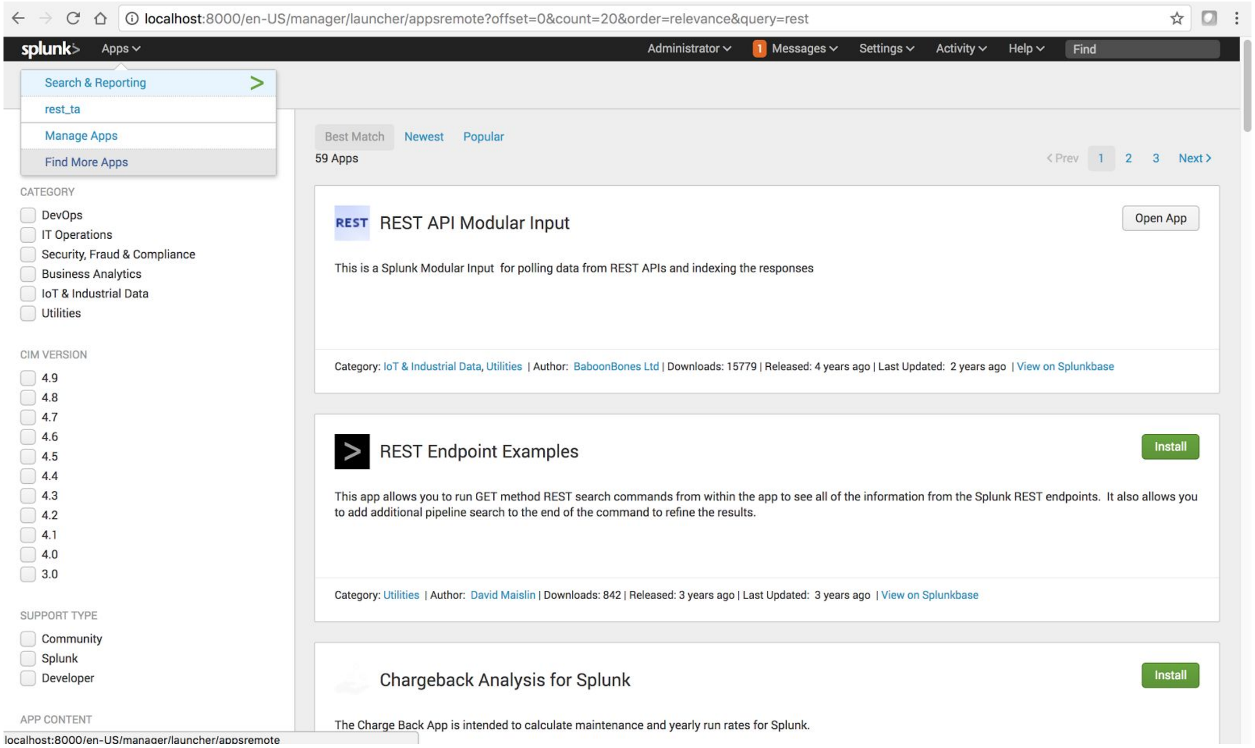
HTTP Headers:

```
Authorization: Bearer
eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJQcmluY2lwYWwvMzY3In0.ldY_Z_adrot
oYAU3K4CSnAZNp1pT-kfC62PgRG6_8XPlp-i_CAPOuU793V2Jcq0yox3Z-
Bc2a6twmlIJ6snMVQ
```

Warning: Once you close this notice the API key will no longer be recoverable. Be sure to save this information!

On Splunk

1. On the Splunk Enterprise front page go to Splunk App. Download the REST API App is named **”REST API Modular Input”**



localhost:8000/en-US/manager/launcher/appsremote?offset=0&count=20&order=relevance&query=rest

REST API Modular Input

This is a Splunk Modular Input for polling data from REST APIs and indexing the responses

Category: IoT & Industrial Data, Utilities | Author: BaboonBones Ltd | Downloads: 15779 | Released: 4 years ago | Last Updated: 2 years ago | View on Splunkbase

REST Endpoint Examples

This app allows you to run GET method REST search commands from within the app to see all of the information from the Splunk REST endpoints. It also allows you to add additional pipeline search to the end of the command to refine the results.

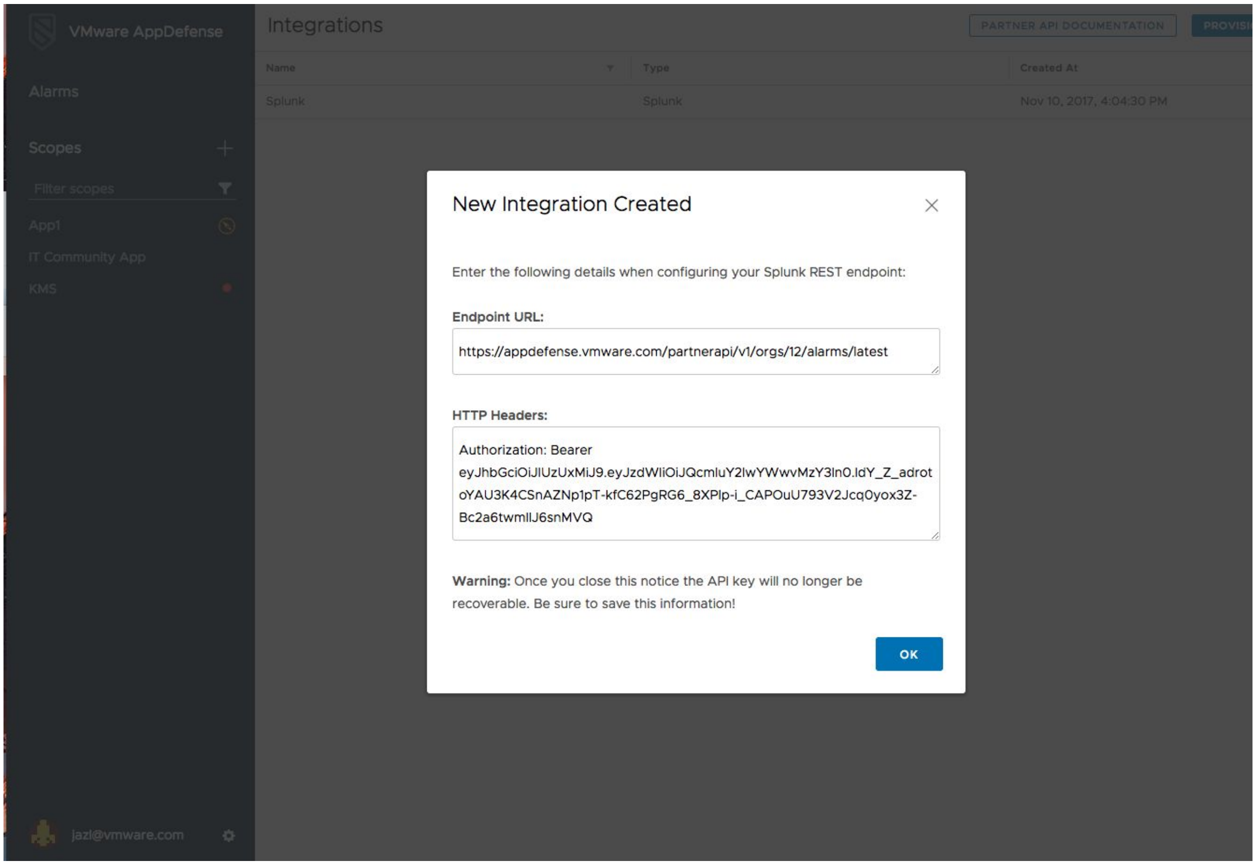
Category: Utilities | Author: David Maislin | Downloads: 842 | Released: 3 years ago | Last Updated: 3 years ago | View on Splunkbase

Chargeback Analysis for Splunk

The Charge Back App is intended to calculate maintenance and yearly run rates for Splunk.

localhost:8000/en-US/manager/launcher/appsremote

2. Once REST App is installed, configure a new REST endpoint. Go to Settings -> Data Input -> REST -> Click New
   a) Index - Create a new Index named “appd”.
   b) Data Input: Go to Splunk Enterprise “Setting” menu click Data Inputs
   c) On the Data Inputs Page Click the “REST” on the local inputs section.
   d) Hit the “New” button to create the new REST data input. Following the following screenshot to fill out the necessary fields.
   e) Endpoint URL - Copy the URL that was exposed by AppDefense when a new Splunk integration was provisioned



Name	Type	Created At
Splunk	Splunk	Nov 10, 2017, 4:04:30 PM

New Integration Created

Enter the following details when configuring your Splunk REST endpoint:

Endpoint URL:

```
https://appdefense.vmware.com/partnerapi/v1/orgs/12/alarms/latest
```

HTTP Headers:

```
Authorization: Bearer
eyJhbGciOiJIUzUxMiJ9.eyJzdWliOiJQcmluY2lwYWwvMzY3In0.ldY_Z_adrot
oYAU3K4CSnAZNp1pT-kfC62PgRG6_8XPlp-i_CAPOuU793V2Jcq0yox3Z-
Bc2a6twmllJ6snMVQ
```

Warning: Once you close this notice the API key will no longer be recoverable. Be sure to save this information!

f) Fill in HTTP Header Properties: The Authorization property is exposed when new Splunk Integration was provisioned on AppDefense. Concatenate it with Content-Type property.

   i. *For example: Authorization=Bearer eyJhbGciOiJIUzUxMiJ9.eyJzdWliOiJQcmluY2lwYWwvMjQ4MCJ9.cbBLUCLfHElp v9NMZmvUQPhCtgnkdg9wmTSXHSrojJSDKtuY0NzHEHeStkQnP16wLQeGKRtDI ISbGdEispbvPw,Content-Type=application/json*

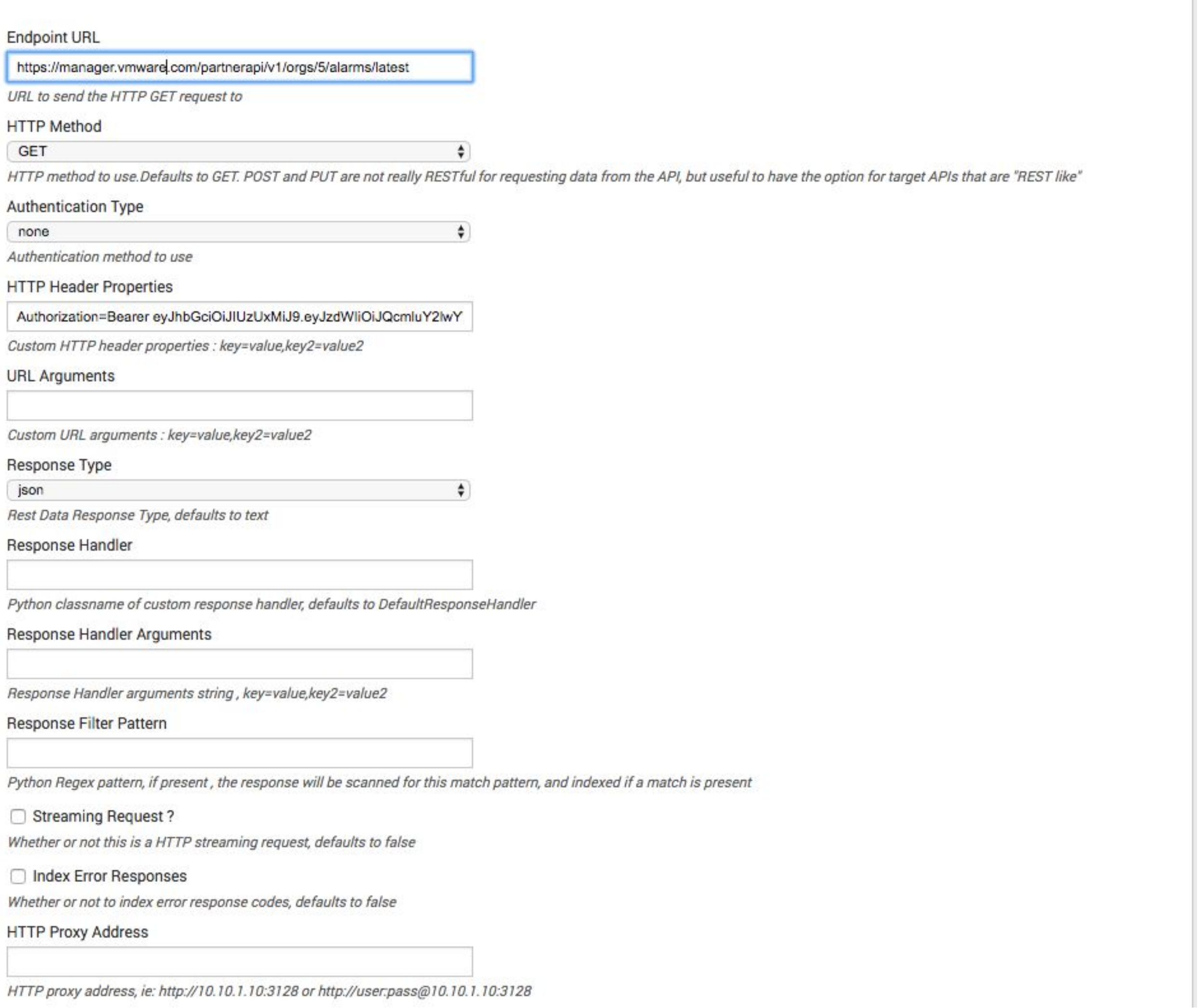
   ii. Please make sure "*Authorization=Bearer*" is appended in the beginning, and "*,Content-Type=application/json*" is included at the end in HTTP Header Properties

g) Select Response type = "json"

h) Change the set sourcetype to '"Manual"

3. Change the source type to "app_defense_alarms"
4. Click the More Setting: Change the Index to "appd".
   Please refer to below sample screen for reference:

Sample screenshot :



Endpoint URL

https://manager.vmware.com/partnerapi/v1/orgs/5/alarms/latest

URL to send the HTTP GET request to

HTTP Method

GET

HTTP method to use.Defaults to GET. POST and PUT are not really RESTful for requesting data from the API, but useful to have the option for target APIs that are "REST like"

Authentication Type

none

Authentication method to use

HTTP Header Properties

Authorization=Bearer eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJQcmluY2lwY

Custom HTTP header properties : key=value,key2=value2

URL Arguments

Custom URL arguments : key=value,key2=value2

Response Type

json

Rest Data Response Type, defaults to text

Response Handler

Python classname of custom response handler, defaults to DefaultResponseHandler

Response Handler Arguments

Response Handler arguments string , key=value,key2=value2

Response Filter Pattern

Python Regex pattern, if present , the response will be scanned for this match pattern, and indexed if a match is present

□ Streaming Request ?

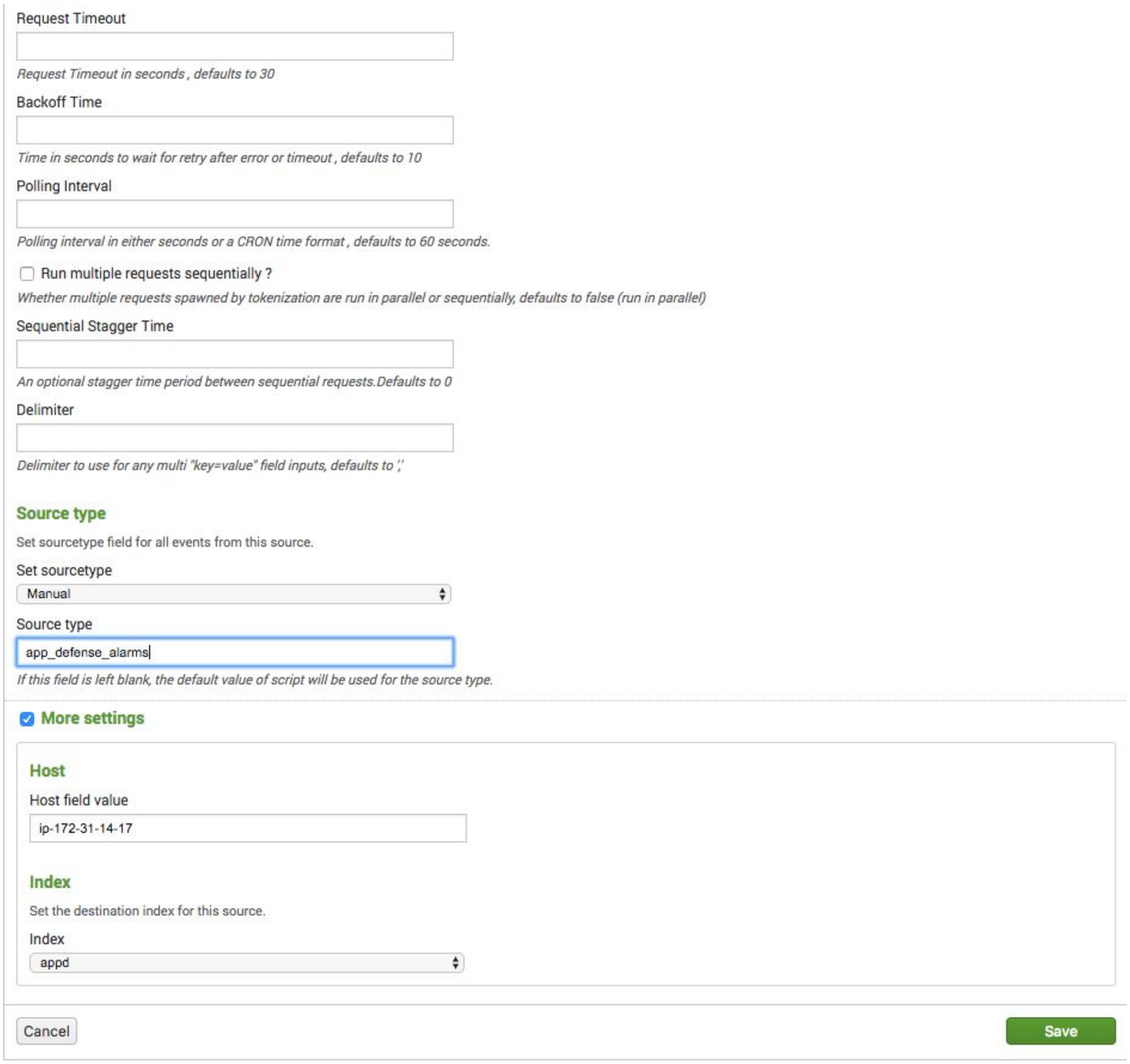
Whether or not this is a HTTP streaming request, defaults to false

□ Index Error Responses

Whether or not to index error response codes, defaults to false

HTTP Proxy Address

HTTP proxy address, ie: http://10.10.1.10:3128 or http://user:pass@10.10.1.10:3128



Request Timeout

Request Timeout in seconds , defaults to 30

Backoff Time

Time in seconds to wait for retry after error or timeout , defaults to 10

Polling Interval

Polling interval in either seconds or a CRON time format , defaults to 60 seconds.

☐ Run multiple requests sequentially ?

Whether multiple requests spawned by tokenization are run in parallel or sequentially, defaults to false (run in parallel)

Sequential Stagger Time

An optional stagger time period between sequential requests.Defaults to 0

Delimiter

Delimiter to use for any multi "key=value" field inputs, defaults to ','

Source type

Set sourcetype field for all events from this source.

Set sourcetype: Manual

Source type: app_defense_alarms

If this field is left blank, the default value of script will be used for the source type.

☑ **More settings**

Host

Host field value: ip-172-31-14-17

Index

Set the destination index for this source.

Index: appd

5. Once the new REST endpoint is created, new alarms from AppDefense should start to show up on Splunk. And they can be searched and played with using query language.