

SecurityBridge Splunk App

Version 4.0.8

Author : Greenace Consultants – Neel Shah

Date : 05th May, 2022

Version	Change History
1.0.0	Initial Version
1.1.1	Added Screenshots and Web Installation Steps
2.0.1	REST API based data onboarding
2.0.3	Minor Version Updates
3.1.0	Support for Splunk 8.x and Python Updates
3.1.8	Minor Version Updates
3.1.9	Splunk AppInspect Changes
4.0.0	Split Main Application from TA and other minor changes
4.0.3	Minor Version Updates
4.0.4	Minor Version Updates
4.0.7	Fixing of Drilldown on Overview Dashboard
4.0.8	Adding Incident Host Dictionary Setup Page to the App

Supported OS

OS
Winsows 7
Windows 8
Windows 10
Windows Server 2012
RHEL 6
RHEL 7
UBUNTU 14

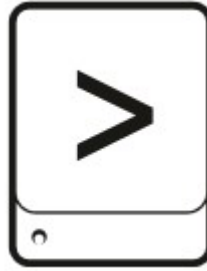
Splunk SecurityBridge App provides an Integration between SecurityBridge tool and Splunk. There are 2 major ways in which The Alerts generated by SecurityBridge app can be onboarded to Splunk. Firstly SecurityBridge app can FTP Generated Alerts to one shared location from where Splunk can read it or Second approach uses REST API based data onboarding. Once the events are in Splunk they can be used to generate reports in SecurityBridge app. Additionally data is already compatible with ES app as the data is CIM (4.12.0) compliant.

Install the App

NOTE: There are multiple ways of deploying apps to Splunk environment, in this document we'll be referring installation via CLI (Command Line Interface)

CASE1: SINGLE STAND ALONE MACHINE (CLI)

Single standalone Splunk Enterprise Installation on Windows/*NIX



1. **Unzip SecurityBridge_App_for_Splunk.spl** and **TA-SecurityBridge.spl**
2. **Copy** the unzipped directory **SecurityBridge_App_for_Splunk** and **TA-SecurityBridge** to **\$SPLUNK_HOME/etc/apps/**
3. **Open CLI** and restart Splunk using **./splunk restart**

CASE2: DISTRIBUTED ARCHITECTURE

Single Indexer Single Search head and Single forwarder (Heavy or Universal) and Deployment server



1. **Unzip** `SecurityBridge_App_for_Splunk.spl` and `TA-SecurityBridge.spl`
2. **Copy** the unzipped directory `SecurityBridge_App_for_Splunk` and `TA-SecurityBridge.spl` to deployment server in the following location
`$SPLUNK_HOME/etc/deployment-apps/`
3. Add following to `serverclass.conf`

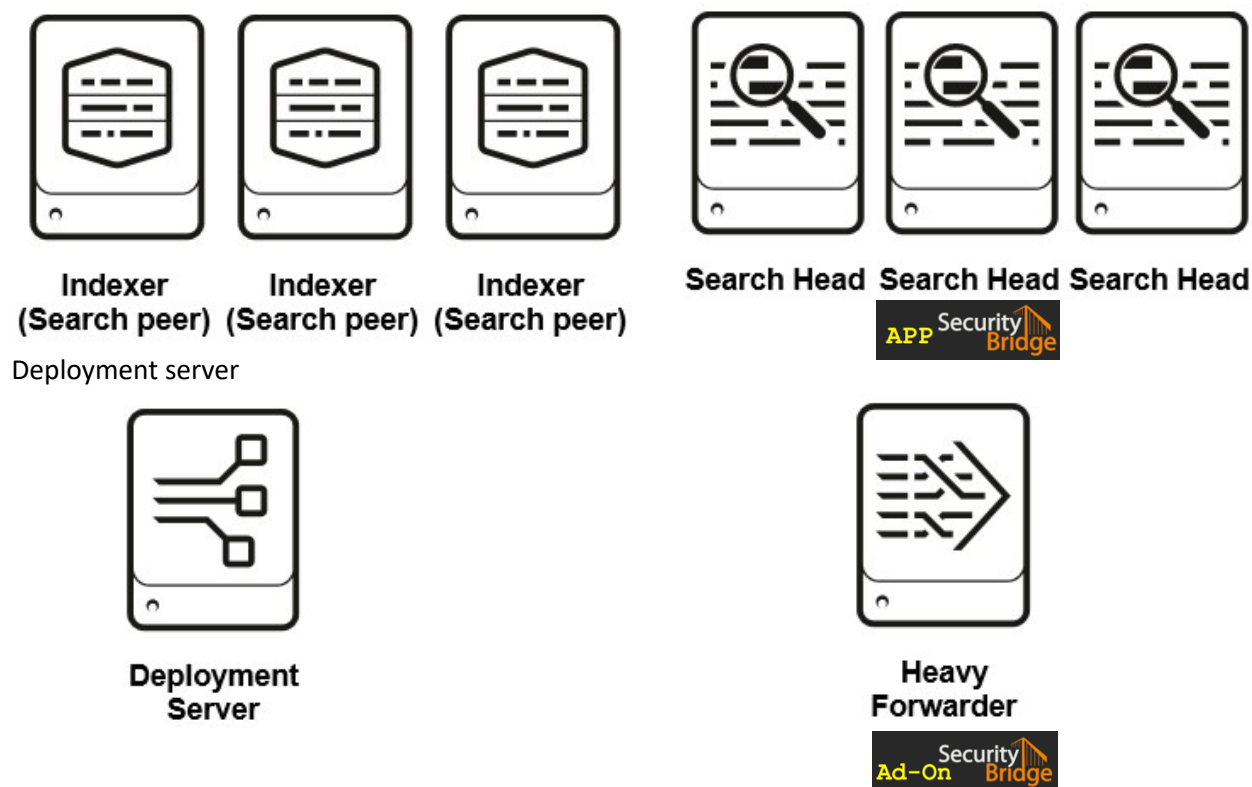
```
[serverClass:<SEARCHHEAD_SERVERCLASS>:app:< SecurityBridge_App_for_Splunk >]
stateOnClient=enabled
restartSplunkd=true
```

```
[serverClass:<HEAVYFORWARDER_SERVERCLASS>:app:<TA-SecurityBridge>]
stateOnClient=enabled
restartSplunkd=true
```

4. **Open CLI** deploy the apps using following command `./splunk reload deploy-server`

CASE3: DISTRIBUTED ARCHITECTURE

Multiple non-clustered Indexers, Multiple non-clustered SearchHeads, Forwarder(Heavy or Universal) and



1. **Unzip** `SecurityBridge_App_for_Splunk.spl` and `TA-SecurityBridge.spl`
2. **Copy** the unzipped directory `SecurityBridge_App_for_Splunk` and `TA-SecurityBridge` to deployment server in the following location `$SPLUNK_HOME/etc/deployment-apps/`
3. Add following to `serverclass.conf`

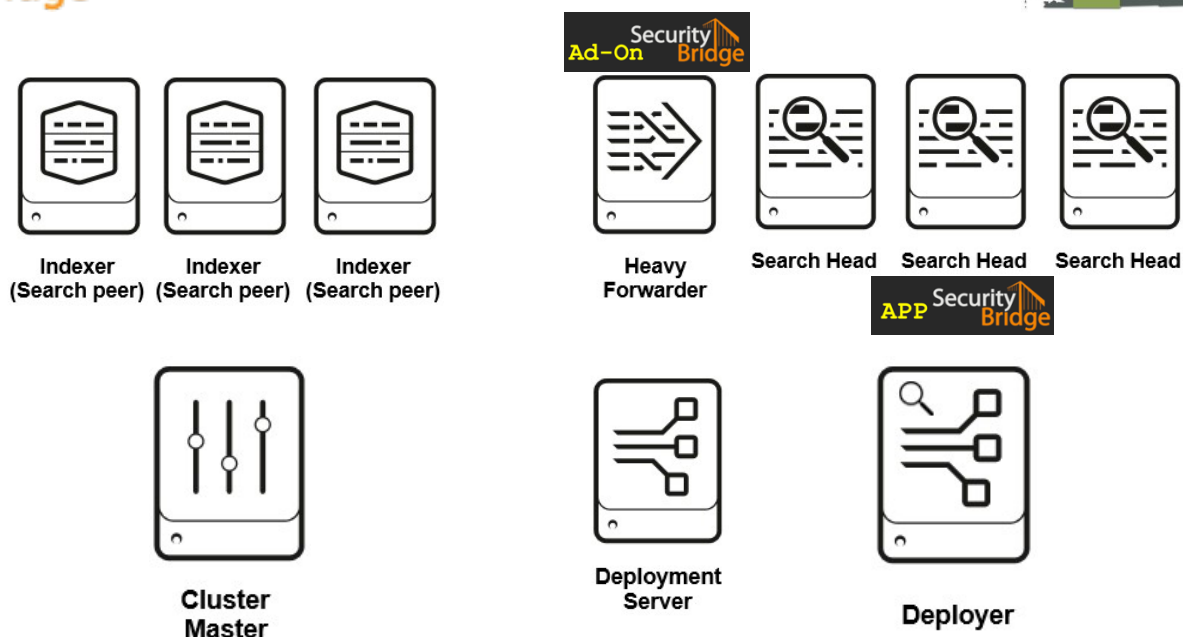
```
[serverClass:<SEARCHHEAD_SERVERCLASS>:app:< SecurityBridge_App_for_Splunk >]
stateOnClient=enabled
restartSplunkd=true
```

```
[serverClass:<HEAVYFORWARDER_SERVERCLASS>:app:<TA-SecurityBridge >]
stateOnClient=enabled
restartSplunkd=true
```

4. **Open CLI** deploy the apps using following command `./splunk reload deploy-server`

CASE4: DISTRIBUTED ARCHITECTURE

Single Site clustered Indexer, Clustered Search heads and Forwarder (Heavy or Universal).



1. **Unzip SecurityBridge_App_for_Splunk.spl** and **TA-SecurityBridge.spl**
2. **Copy SecurityBridge_App_for_Splunk** to Deployer server in the following location
`$SPLUNK_HOME/etc/shcluster/apps/`
3. **Open CLI** on Deployer and deploy the app on Search Head Cluster using following command
`./splunk apply shcluster-bundle -target <URI>:<management_port> -auth <username>:<password>`
5. **Copy** the unzipped directory **TA-SecurityBridge** to deployment server in the following location
`$SPLUNK_HOME/etc/deployment-apps/`
6. Add following to **serverclass.conf**

```
[serverClass:<HEAVYFORWARDER_SERVERCLASS>:app:<TA-SecurityBridge >]
stateOnClient=enabled
restartSplunkd=true
```

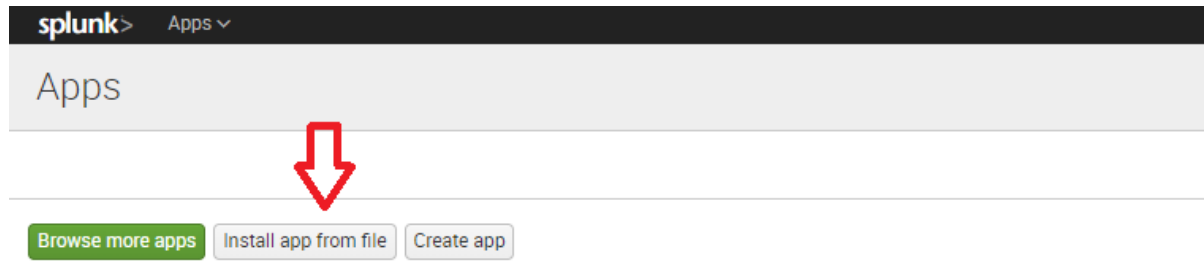
7. **Open CLI** deploy the apps using following command `./splunk reload deploy-server`

CASE5: STANDALONE INSTALLATION (WEB)

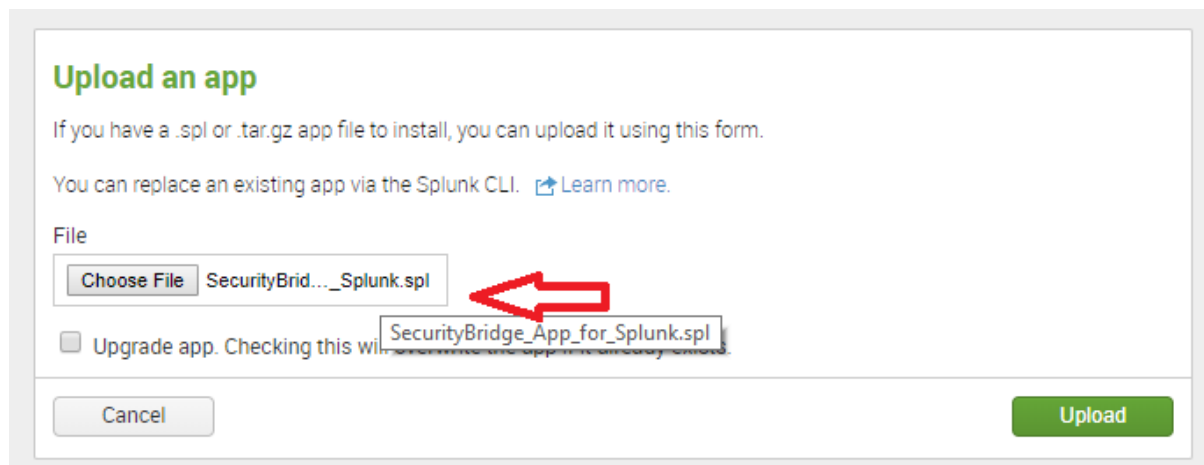
1. On the Splunk Home Page, Click on "Manage Apps"



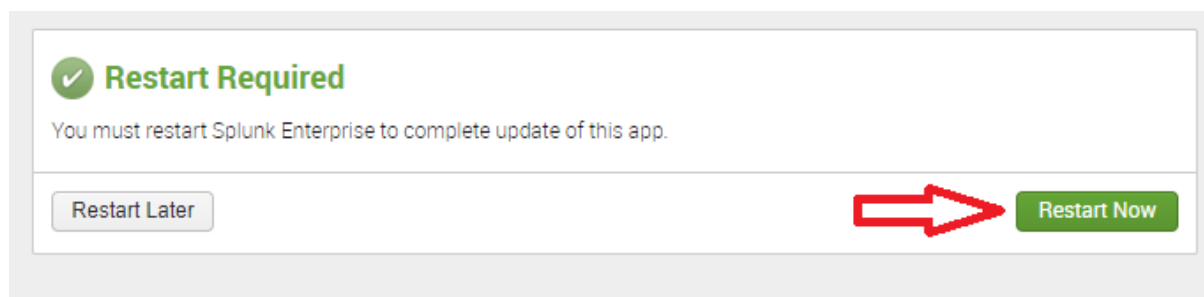
2. On the Manage Apps page, Click on "Install app from file"



3. Select path for SecurityBridge Splunk app and Click "Upload"



4. Splunk will prompt you to restart the machine, please restart

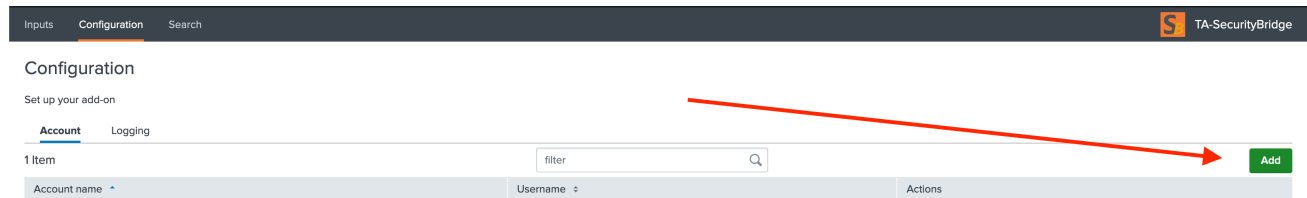


5. Repeat the steps for Ad-On
6. Restart Splunk after installing the app and the ad-on

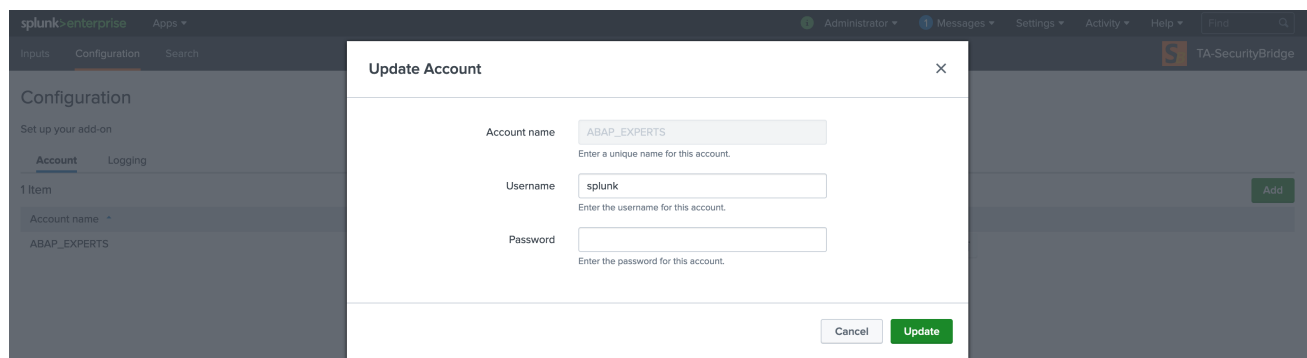
1. After Installation and restart, login to the Splunk web and go to SecurityBridge TA



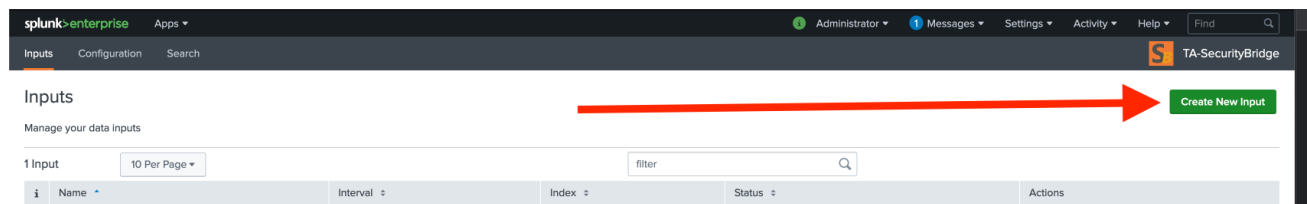
2. Go to configuration Tab and Click 'Add'



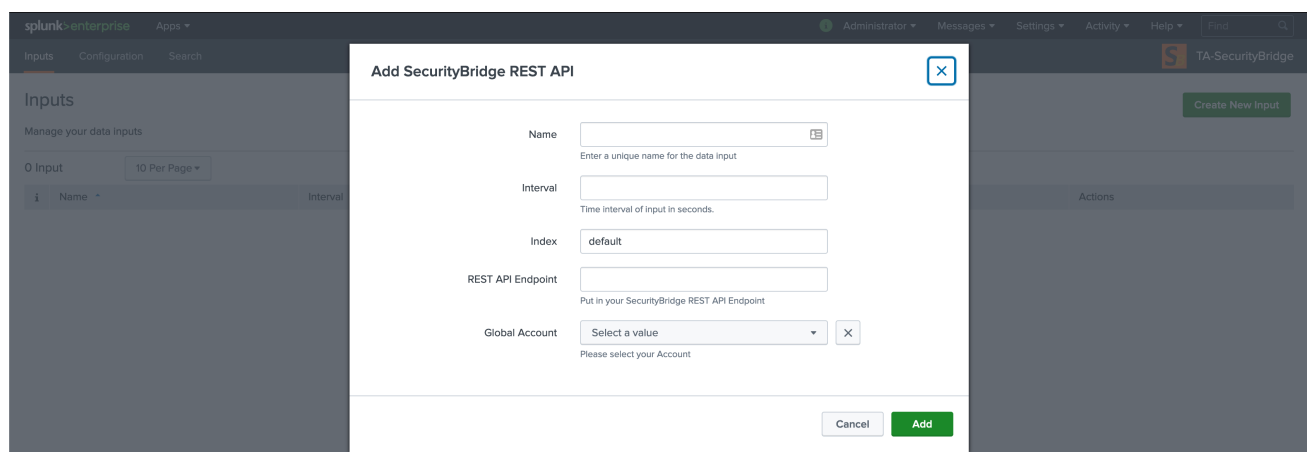
3. Add username and password for your account



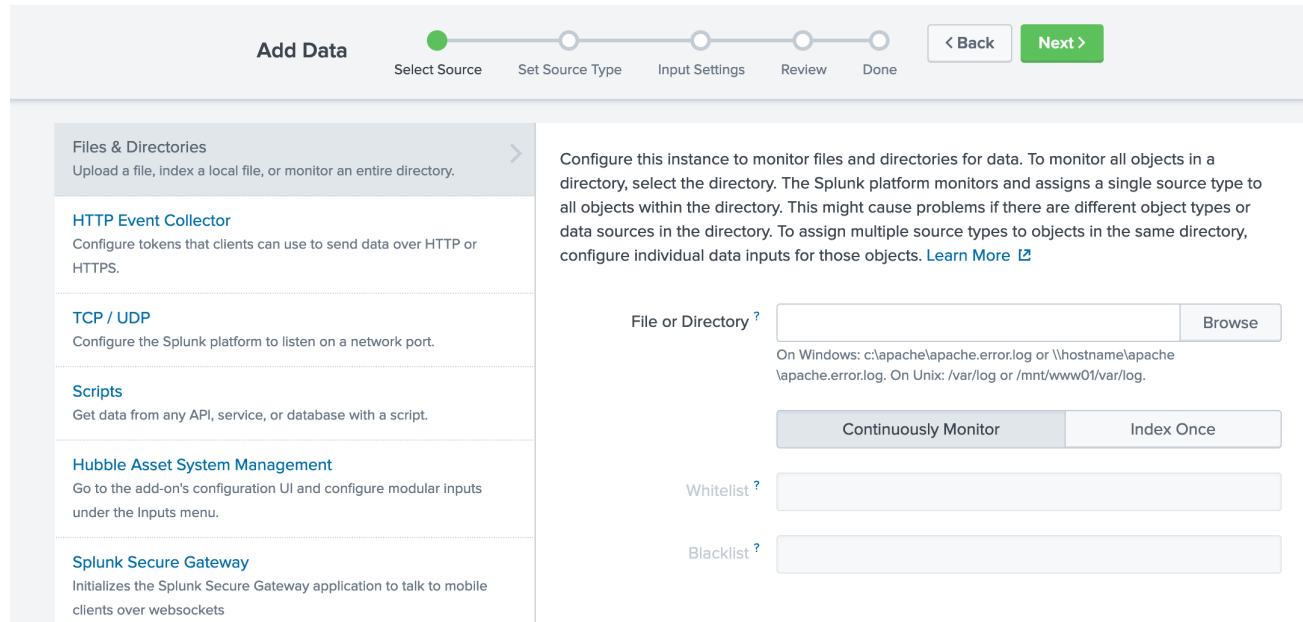
4. Go to inputs tab and click on "Create New Input"



5. Fill in the details and select the index that you want the data to go into.



1. Go to Settings > Add Data > Monitor



- As shown in the above screen shot for File Copy configuration provide full directory path of network shared folder. Than select the OS type on which file should be copied. (In case of Windows system, shared directory path should be starting with '\\\' and for Linux system it should be starting with '/')
- Make sure SourceType is 'sapsb'

Input Settings

Optionally set additional input parameters for this data input as follows:

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.

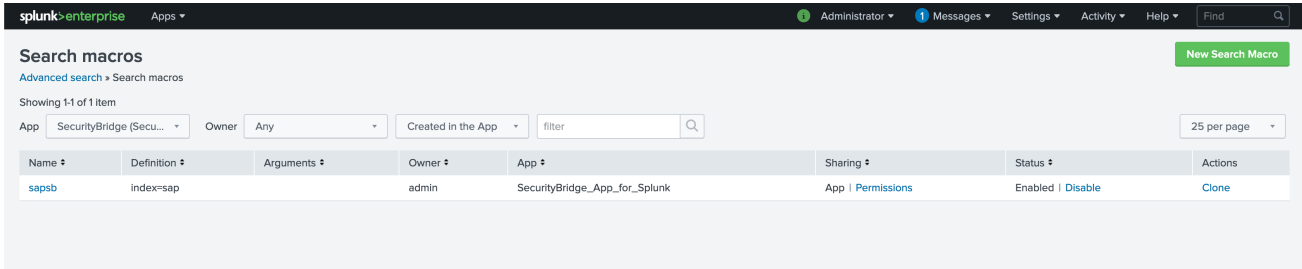
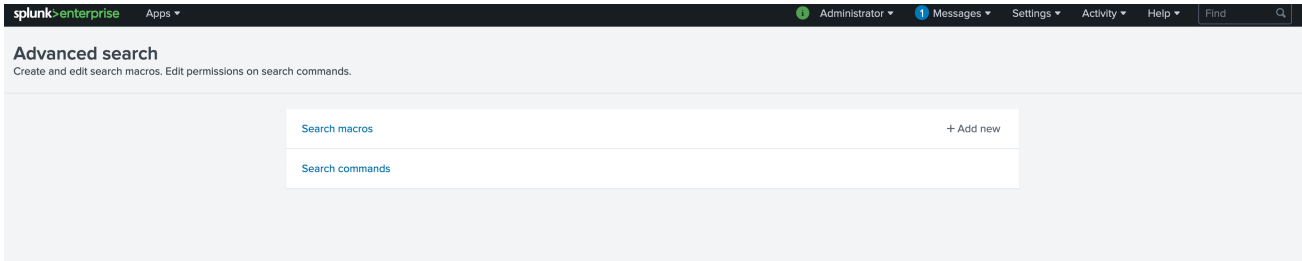
App context

Application contexts are folders within a Splunk platform instance that contain configurations for a specific use case or domain of data. App contexts improve manageability of input and source



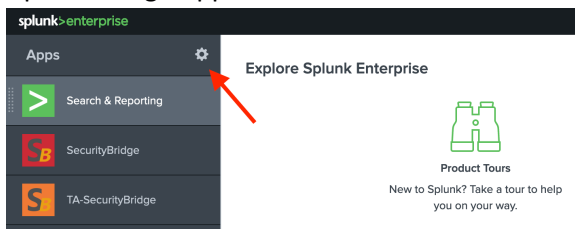
- This will complete the setup and you can start using the Security Bridge app

Make sure the index selected, is added to the macro
Settings > Advanced Settings > Macro > sapsb

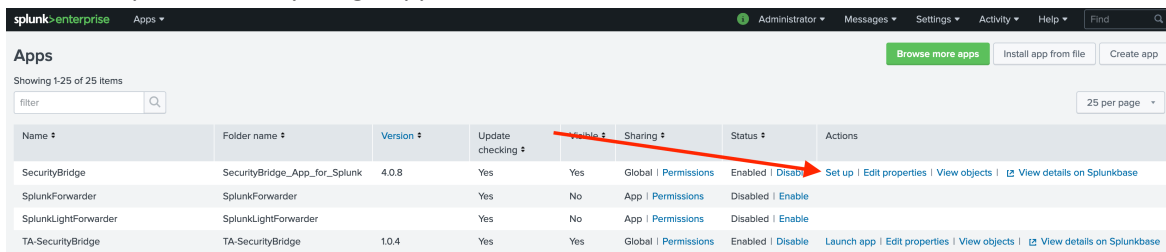


Setting Incident Dictionary Host

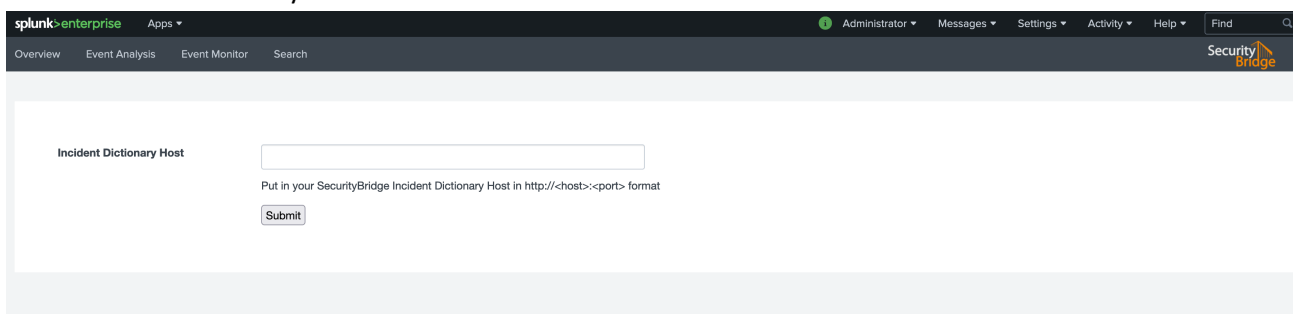
1. Open Manage Apps



2. Click "Setup" for SecurityBridge App

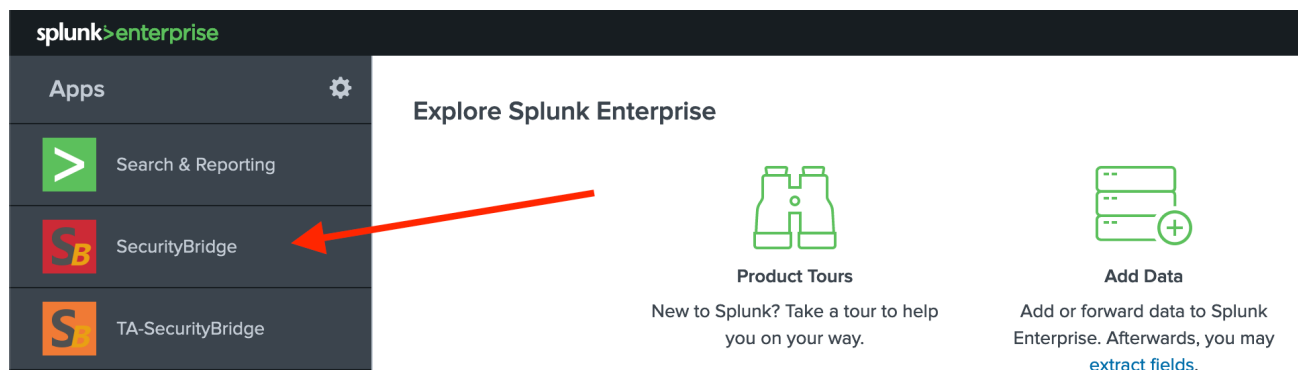


3. Enter Incident Dictionary Host and Click Submit



4. This will enable Incident Dictionary Host Drill Down on "Event Monitor" Dashboard.

Open the app to access the dashboards



THANK YOU