

# SPLUNK INTEGRATION GUIDE

## Synack's Integration with Splunk

Aug 2024

# Index

Synack's integration with Splunk allows customers to digest Synack vulnerability data easily into their Splunk instance. Customers can query the information, view the data on a dashboard, and correlate it with other data elements in Splunk.

To get started with the installation, follow the steps provided below.

<b>Synack API Token Generation</b>	<b>3</b>
<b>Splunkbase Install</b>	<b>4</b>
Splunk User	4
<b>Index creation</b>	<b>5</b>
<b>Configure API token in Splunk App</b>	<b>5</b>
<b>Update API token in Splunk App</b>	<b>6</b>
<b>Synack Dashboards for Splunk</b>	<b>6</b>
<b>Synack Data indexed in Splunk</b>	<b>8</b>
<b>Frequently Asked Questions</b>	<b>9</b>

## Synack API Token Generation

After logging into the Synack Customer Portal as an admin user, navigate to Settings. Click on API and open the Tokens page.

If your Splunk is installed on-premise, you will need the public IP address of your Splunk Enterprise server. Wildcards are supported for the IPv4 field. Please also define an expiration date for this token. If you are using Splunk Cloud, please use the IP address provided to you by Splunk.

Note: the permissions of the Synack User who generates the token apply. We recommend that your Synack Admin generates the token, so that data for all Synack Assessments and Vulnerabilities in the Org is viewable in the Synack App for Splunk. Note: the data available in the Synack App for Splunk will match the data which the user who generated the API Key sees in the Synack Portal.

Click generate and copy the token, you will need this later during the setup process. If you lose the token, you can always navigate to this page to copy it again.

## Splunkbase Install

From your Splunk Console, Install the Synack for Splunk app.

Click Apps -> Manage Apps -> Browse More Apps, Search for Synack then click Install.

Alternatively you may download the app from Splunkbase

<https://apps.splunk.com/app/4288/>

**Note: Before downloading from Splunkbase make sure latest Version 3.0.x is selected**

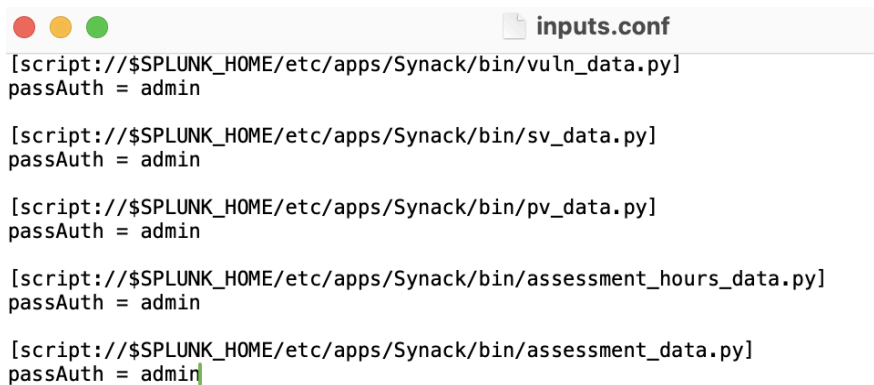
Next click Apps -> Manage Apps -> Install App from File , then choose the synack\_sds.spl file you downloaded

## Splunk User

Synack App for Splunk relies on an assumption that your default Splunk admin account hasn't been renamed or deleted.

If you are using Splunk on-prem, it is expected that your admin account is 'admin'. If you are using Splunk Cloud, it is expected that your admin account is 'sc\_admin'. If this is not so, and your Splunk admin username is different, the Synack App for Splunk will not work. To make it work, you will need to set the correct Splunk admin username in file <YOUR-SPLUNK-HOME>/etc/apps/Synack/local/inputs.conf

Edit the file and set the value of the passAuth parameter to the name of your Splunk admin user in every section of the file. Here is a sample of that file:



```
inputs.conf

[script://$SPLUNK_HOME/etc/apps/Synack/bin/vuln_data.py]
passAuth = admin

[script://$SPLUNK_HOME/etc/apps/Synack/bin/sv_data.py]
passAuth = admin

[script://$SPLUNK_HOME/etc/apps/Synack/bin/pv_data.py]
passAuth = admin

[script://$SPLUNK_HOME/etc/apps/Synack/bin/assessment_hours_data.py]
passAuth = admin

[script://$SPLUNK_HOME/etc/apps/Synack/bin/assessment_data.py]
passAuth = admin
```

## Index creation

**Note:** If you already have a Splunk Index named 'synack' (all lowercase), such as from a previous install of Synack App for Splunk, then you skip this step. To check if you have a previous 'synack' Index, click "Settings" -> "Indexes" and look to see if 'synack' (all lowercase) is present in the list

### Creating New Index

1. From the "Settings menu", click on "Indexes" to create a new Index. This index will act as a repository to store data retrieved from Synack.
2. Click "New Index" and enter synack (all lowercase) as the Index name.
3. From the app dropdown, select "Synack App".
4. Click Save.

## Configure API token in Splunk App

Note: this setup page should be completed by a Splunk user with an Admin role.

After logging into Splunk, from the "Manage Apps" page, search for 'Synack App' for Splunk, and click "Set Up" under "Actions":

[Set up](#) | [Launch app](#) | [Edit properties](#) | [View objects](#)

This will take you to the page to enter your Synack API URL (choose either FedRAMP or Other URL as applicable to you, and shown below) and your Synack API Token. Then click 'Submit'

### Synack App Setup Page

This setup page is used to update the Synack API URL and token used in this Splunk App

Copy and Paste the following URLs into the input box based on your assigned Synack environment:

**Synack FedRamp** <https://api.synack.us>

**All other Synack Customers:** <https://api.synack.com>

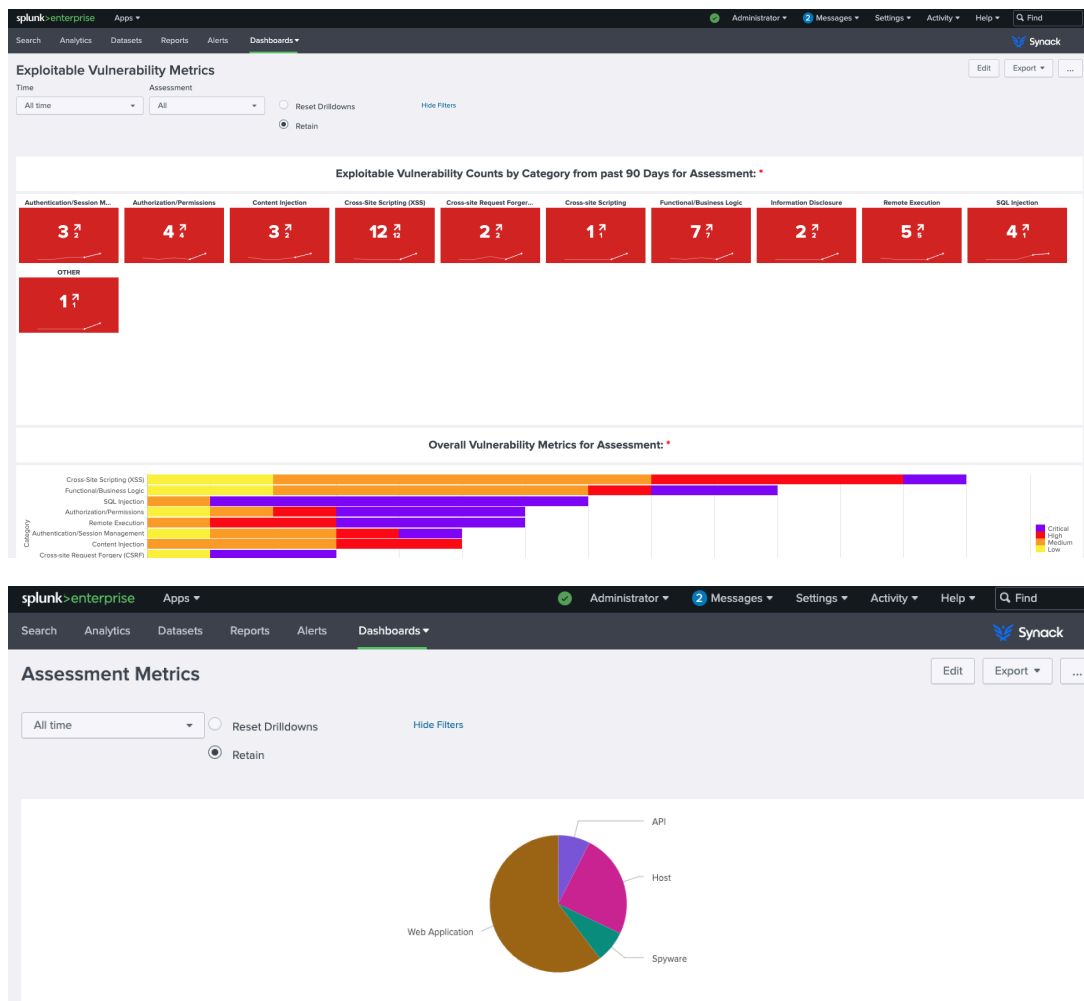
Synack API URL:  Synack API Token:

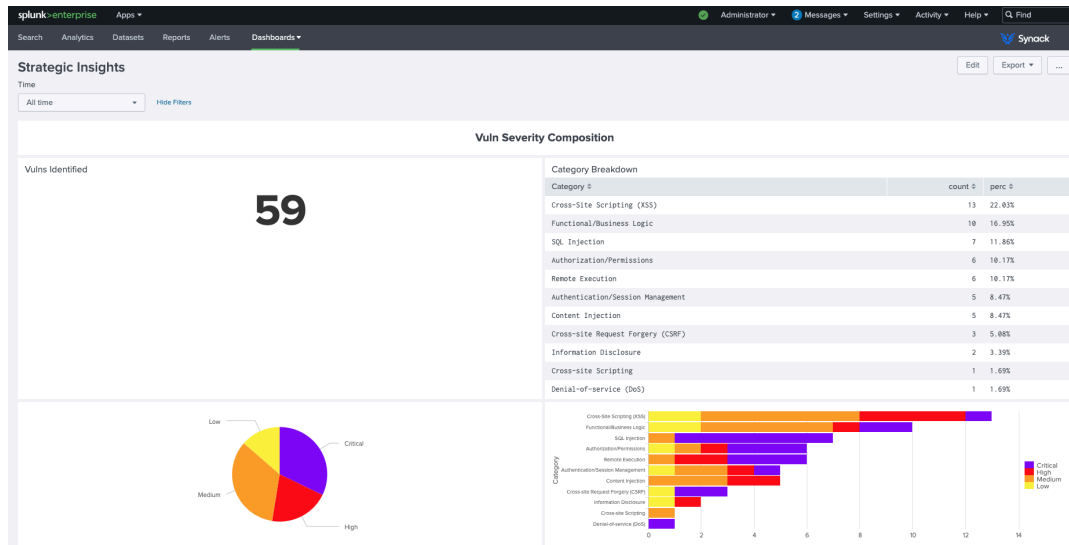
## Update API token in Splunk App

Follow the same steps as documented in the previous section to update the API Token to a new value.

## Synack Dashboards for Splunk

Synack Dashboard for Splunk provides out of the box charts to visualize vulnerability data within your Splunk instance. You can also create your own customized charts and widgets. The Synack dashboard utilizes the vulnerability events stored within the synack (lowercase) index. Vulnerabilities can be filtered by clicking within the views. Below are some samples of the Synack Dashboard views.





Please note that it may take several hours for data to show up initially.

## Synack Data indexed in Splunk

The Synack app utilizes the public APIs made available on the Synack platform. The Synack app for Splunk includes python scripts that query these APIs every hour. All data is indexed in the *synack* index. Each script indexes the data to a different host value. The following host values are available for searching:

- *synack\_vuln*: All exploitable vulnerability data can be found in this host
- *synack\_pv*: This is used for patch verification related data
- *synack\_sv*: This is used for suspected vulnerabilities
- *synack\_assessment*: This is for individual assessment data
- *synack\_assessment\_hours*: This is for # of hours researched related to each assessment



## Frequently Asked Questions

### **I am a FedRAMP customer, are there any extra steps I need to take?**

Yes. If you are using Synack and Splunk instances of FedRAMP there is some whitelisting required to allow secure communication between Synack and Splunk. Please provide Synack Support the IP address of your Splunk Cloud FedRAMP instance so that we can whitelist your Splunk traffic in your Synack portal. [support@synack.com](mailto:support@synack.com)

### **Is there an upgrade path from previous versions of the Synack Splunk App?**

No, because the available reporting of the new (v3.0.x) app is different than for previous versions, the new app requires a fresh install. (Note: if you wish to keep old data, you may optionally keep the old version of the Synack app running in parallel)

### **I followed the instructions in this guide, but I am still not able to see any data. How can I troubleshoot?**

If this is the initial configuration of the app, it can take some time for the initial data pull and indexing. Depending on the amount of data that currently exists in the portal the initial data population could take up to one hour.

If you are not able to visualize any data within the Synack Dashboard on your Splunk instance or perform queries, please ensure that the API token generation was performed from an admin account. The API is RBAC restricted to the level of the user that created it.

### **How can I remove all Synack data from my Splunk and get a fresh start?**

It's simple to remove all data from your Splunk. You can disable the Synack Dashboard app. Finally, delete the synack index from Settings > Data > Indexes.

### **My integration used to work but I am no longer seeing updated vulnerabilities.**

This could be because of the API token being expired. Please check the Synack platform to verify the API token is still active.

It also could be that the index needs additional disk space. Please check the index settings within Splunk.