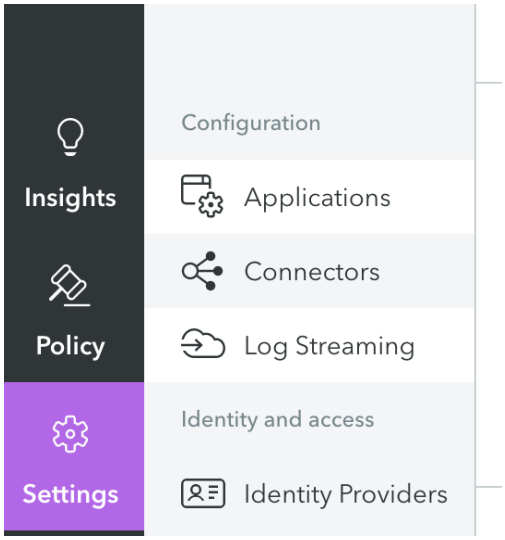
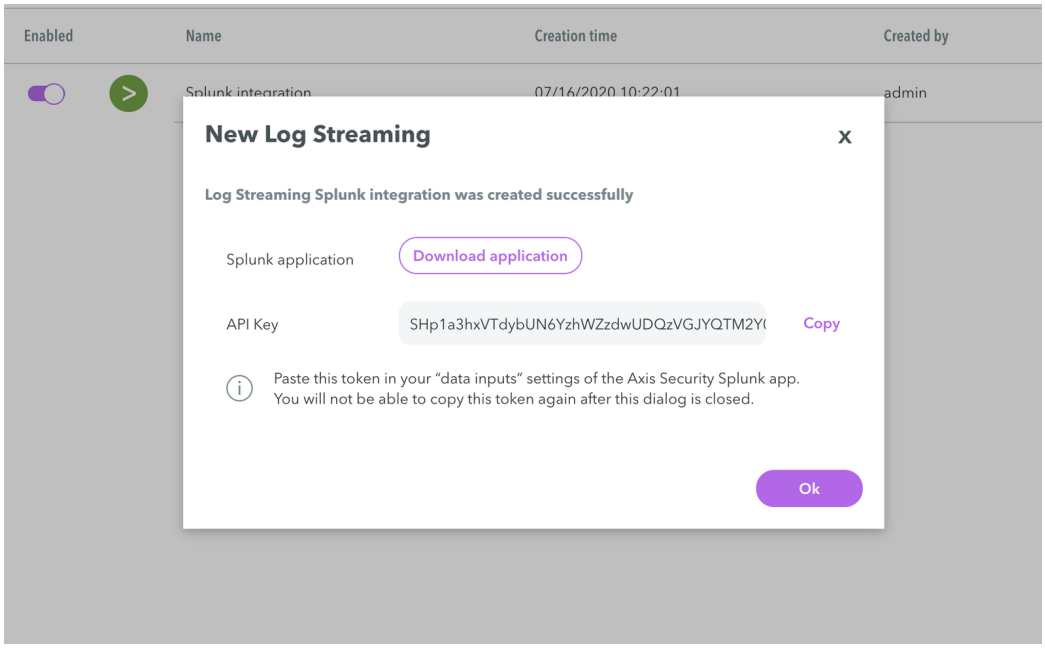
Axis Security Splunk Application Integration Guide

Splunk Enterprise

Installation

1. Create Log Streaming in Management Console

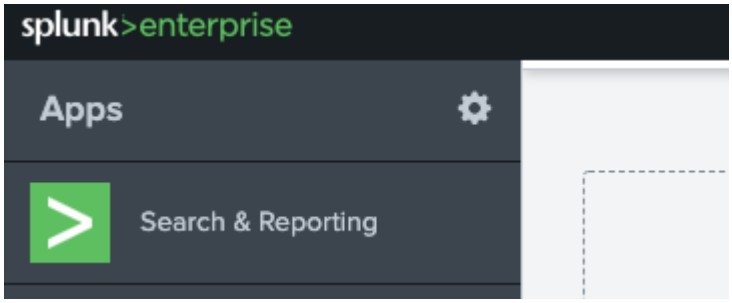




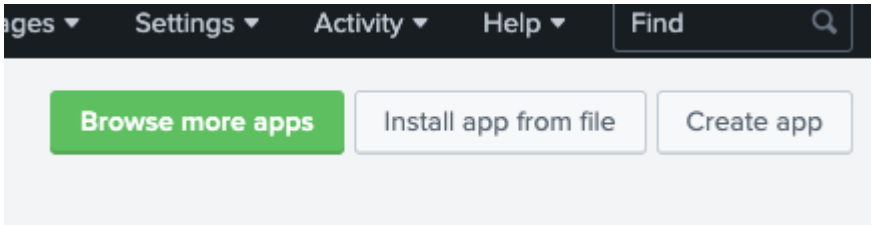
2. Click "Download application", download the app from SplunkBase.
   If you're using **Safari** browser make sure the auto decompression feature is disabled **before downloading**, by doing the following:

a. Click **Preferences**
b. Under the General tab, uncheck the option ***Open "safe" files after downloading***

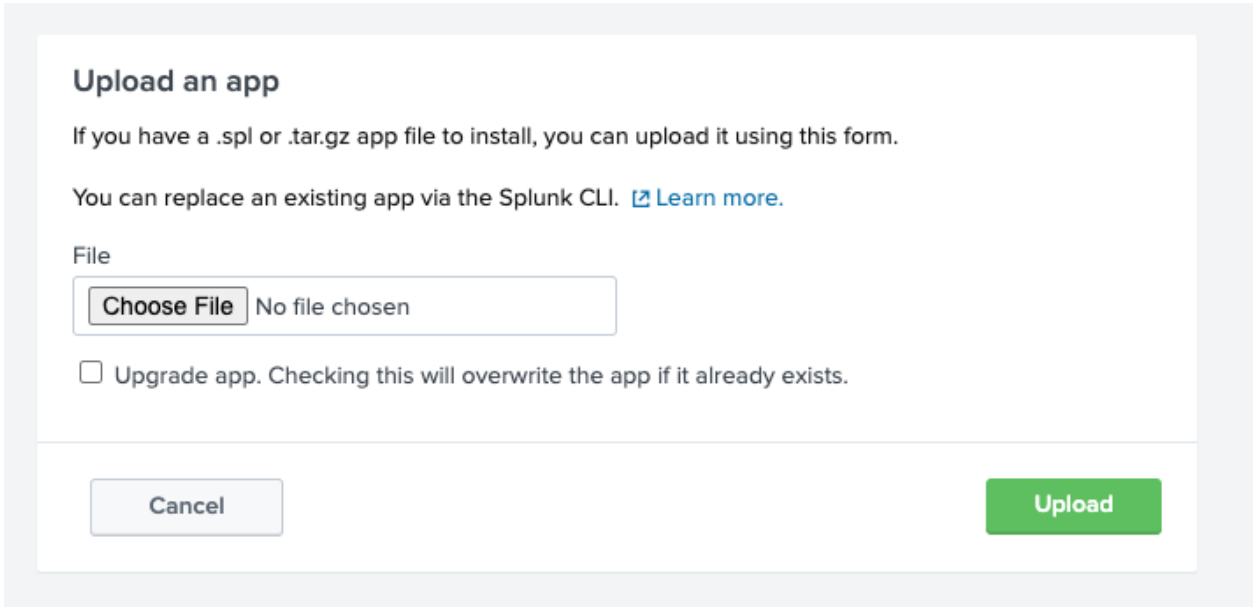
3. Go to Splunk and click on the cog wheel icon (top left).



4. Click "Install app from file" (top right corner)

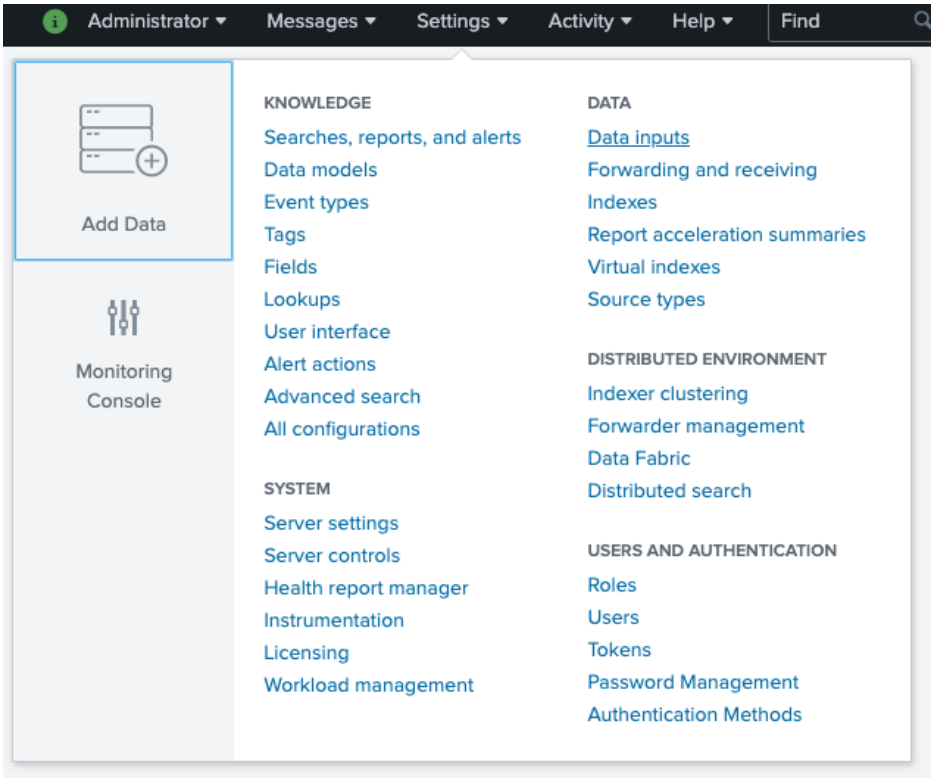


5. Upload the file downloaded from Management Console *("axis_splunk_app.zip")*

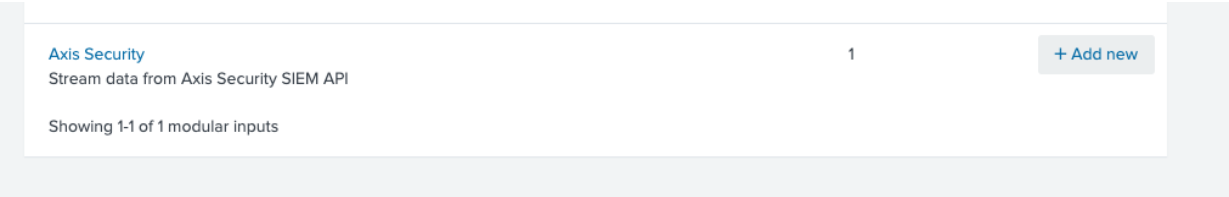


if you're upgrading version, please check the "Upgrade app" checkbox

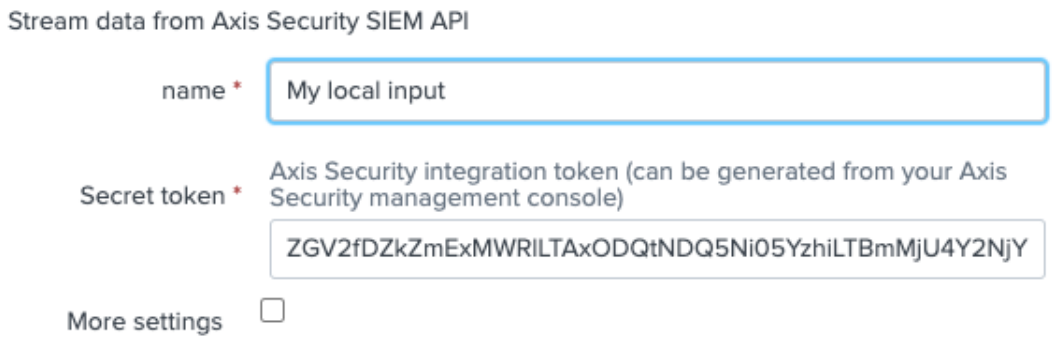
6. Click on “Settings → Data inputs” (top right corner)



7. Click “Add new” next to “Axis Security” modular input

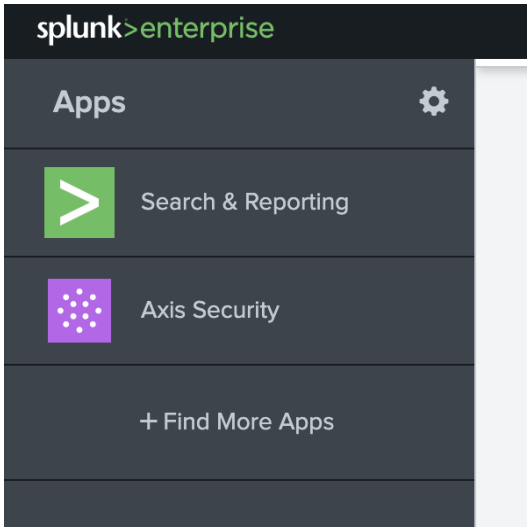


8. Provide a name and paste the token (API key) copied from the Management Console



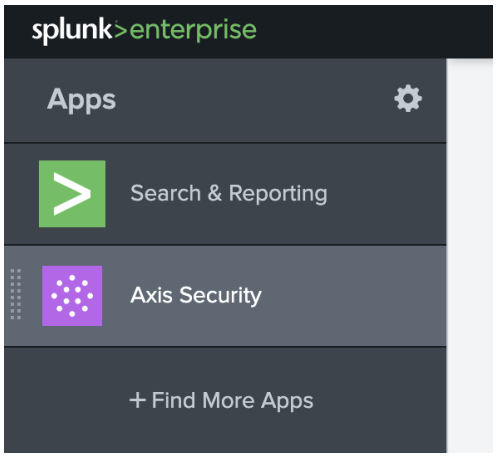
You can change index by checking “More settings” and insert your preferred index (the default index is “main”).

9. In your Splunk main page you should now see “Axis Security” integration

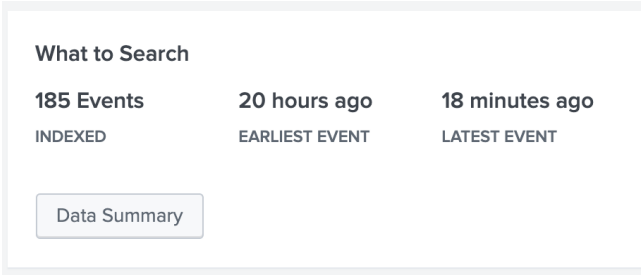


Usage

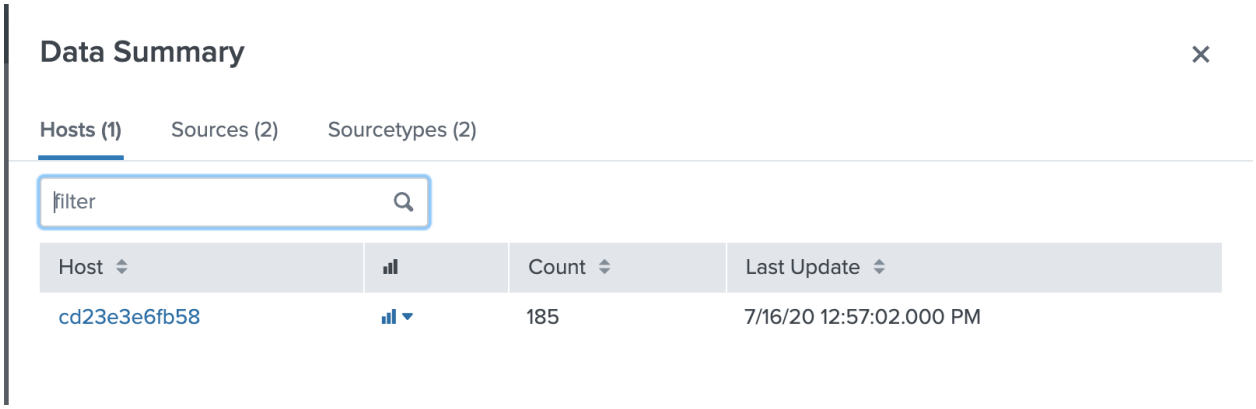
1. Click on the “Axis Security” icon in your Splunk main page.



2. Click on “Data Summary”



3. Select either “Hosts” or “Sources” (either “activityLog” or “auditLog”) or search the relevant index in the top search bar.



4. You should now see your Axis Security’s activity and audit log information.
(*it could take a few minutes until initial data is shown up in your Splunk)*

Universal Forwarder

Installation

Since forwarder has no UI the installation requires access to the forwarder's server.

1) Extract the package:

Run the command (notice the parameters):

```
tar xvzf <tar_folder>/axis_splunk_app.tar.gz -C <path_to_forwarder>/etc/apps
```

2) Configure input

Edit the file:

```
<path_to_forwarder>/etc/apps/axis_splunk_app/default/inputs.conf
```

Choose name for your input and append the lines at the end:

```
[axis_splunk_app://YourInputName]
token = <your_access_token>
index = <your_index> (Optional. Default value - "main")
```

3) Restart Splunk Forwarder

Run the command:

```
<path_to_forwarder>/bin/splunk stop
<path_to_forwarder>/bin/splunk start
```

Note:

When using **Splunk Universal Forwarder** keep in mind that you need to update the Axis Splunk app version **manually** since Universal Forwarder does not support auto update from SplunkBase