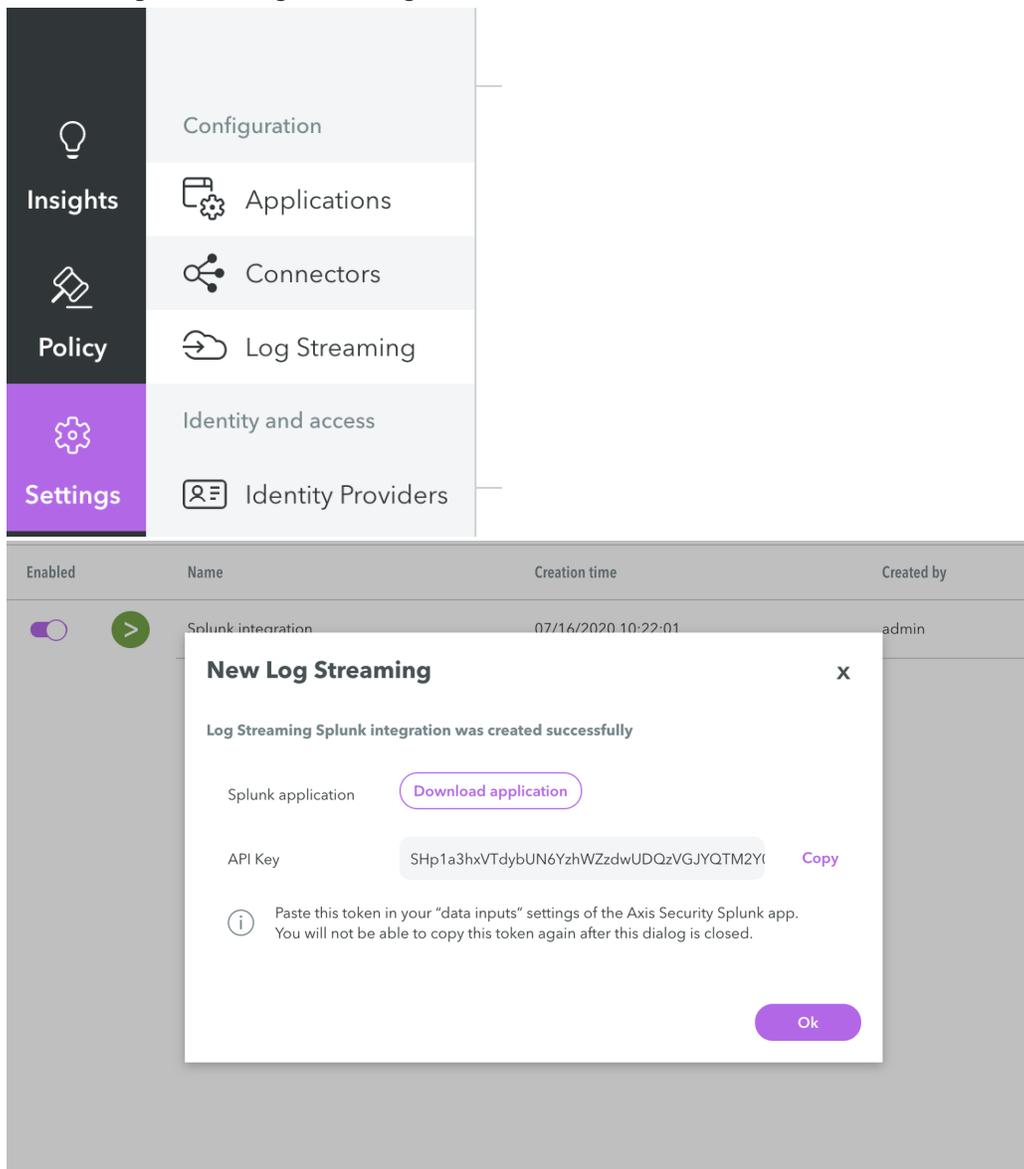


Axis Security Splunk Application Integration Guide

Splunk Enterprise

Installation

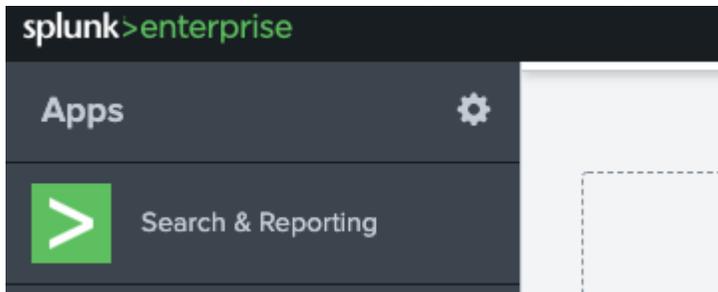
1. Create Log Streaming in Management Console



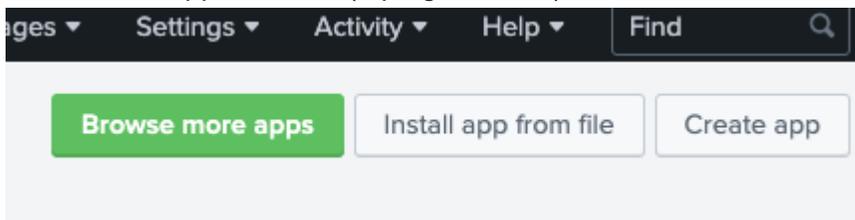
The screenshot shows the Axis Security Management Console interface. On the left, a navigation menu is visible with options: Insights, Policy, and Settings (highlighted in purple). The main content area shows a list of configurations under the 'Log Streaming' section. A 'New Log Streaming' dialog box is open, displaying a success message: 'Log Streaming Splunk integration was created successfully'. The dialog includes a 'Download application' button, an API Key field with the value 'SHp1a3hxVTdybUN6YzhWZzdwUDQzVGJYQTM2YI' and a 'Copy' button, and an 'Ok' button at the bottom. A note at the bottom of the dialog states: 'Paste this token in your "data inputs" settings of the Axis Security Splunk app. You will not be able to copy this token again after this dialog is closed.'

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:

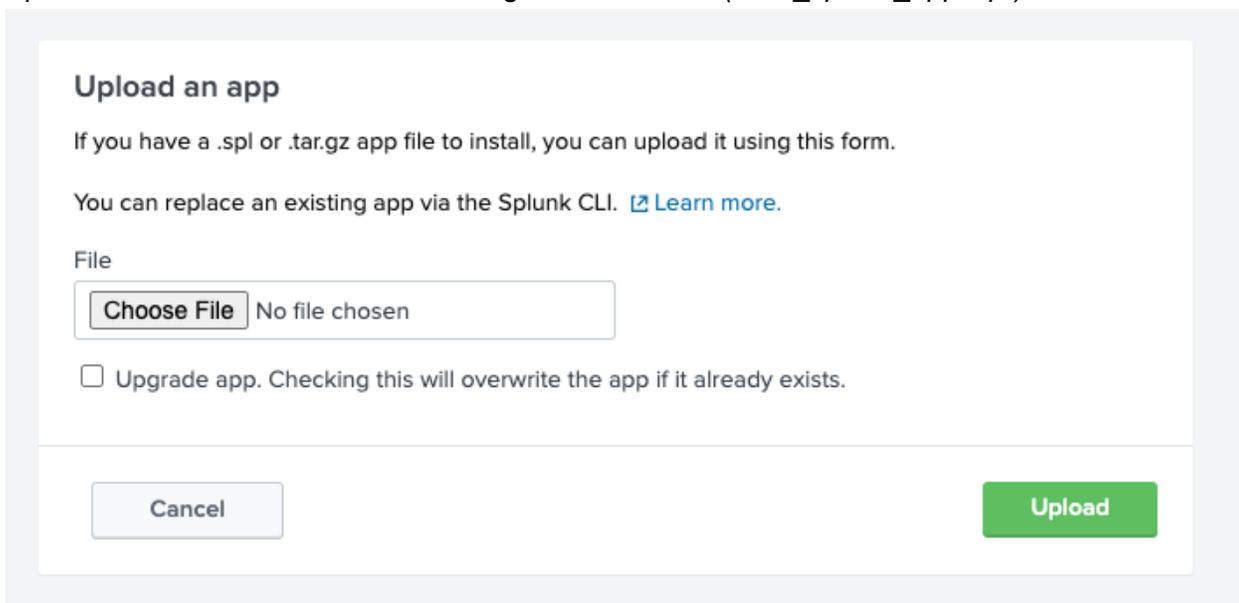
- a. Click **Preferences**
 - b. Under the General tab, uncheck the option *Open "safe" files after downloading*
3. Go to Splunk and click on the cog wheel icon (top left).



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



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

A screenshot of the 'Upload an app' form in the Splunk interface. The form has a white background and a light grey border. It contains the following elements: a title 'Upload an app', a paragraph 'If you have a .spl or .tar.gz app file to install, you can upload it using this form.', a paragraph 'You can replace an existing app via the Splunk CLI. [Learn more.](#)', a 'File' section with a 'Choose File' button and the text 'No file chosen', a checkbox labeled 'Upgrade app. Checking this will overwrite the app if it already exists.', and two buttons at the bottom: 'Cancel' (white with grey border) and 'Upload' (green).

Upload an app

If you have a .spl or .tar.gz app file to install, you can upload it using this form.

You can replace an existing app via the Splunk CLI. [Learn more.](#)

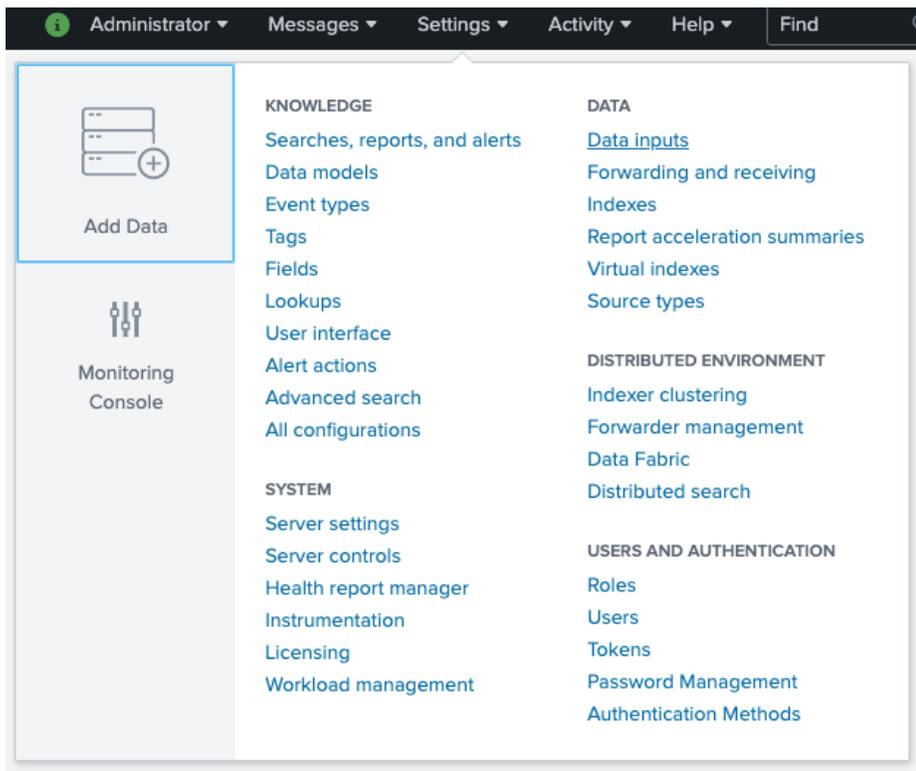
File

No file chosen

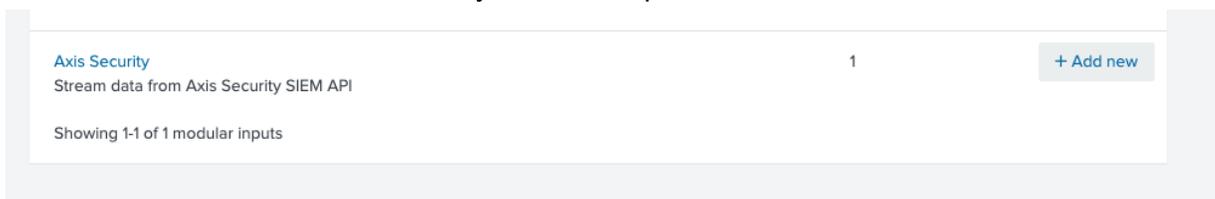
Upgrade app. Checking this will overwrite the app if it already exists.

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

Stream data from Axis Security SIEM API

name *

My local input

Secret token *

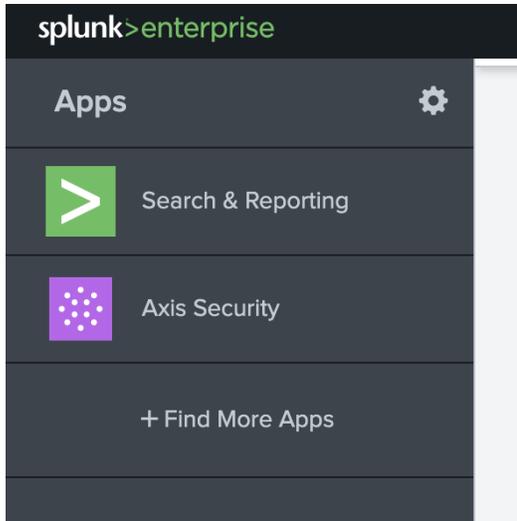
Axis Security integration token (can be generated from your Axis Security management console)

ZGV2fDZkZmExMWRILTaxODQtNDQ5Ni05YzhiLTBmMjU4Y2NjY

More settings

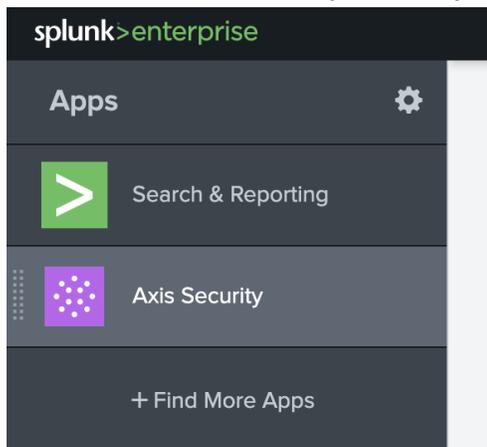
You can change index by checking “More settings” and insert your preferred index (the default index is “main”).

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

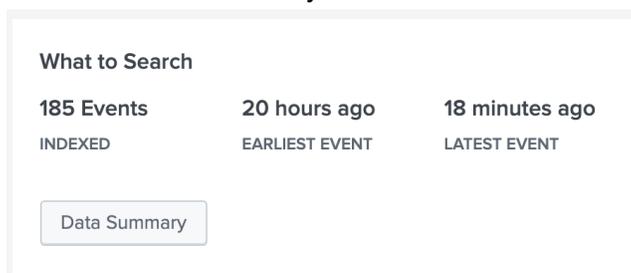


Usage

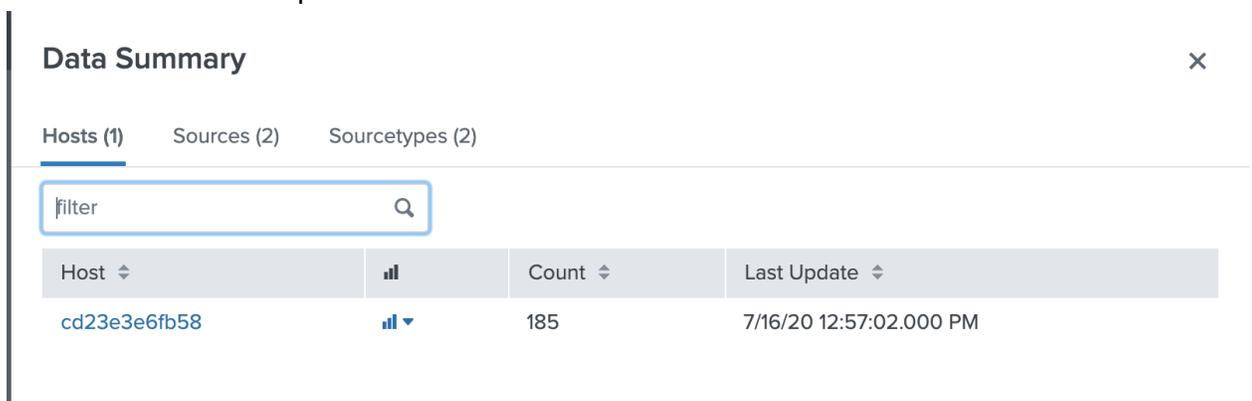
1. Click on the “Axis Security” icon in your Splunk main page.



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