Integrating Splunk as a Data Collector

Version 1.2

Overview

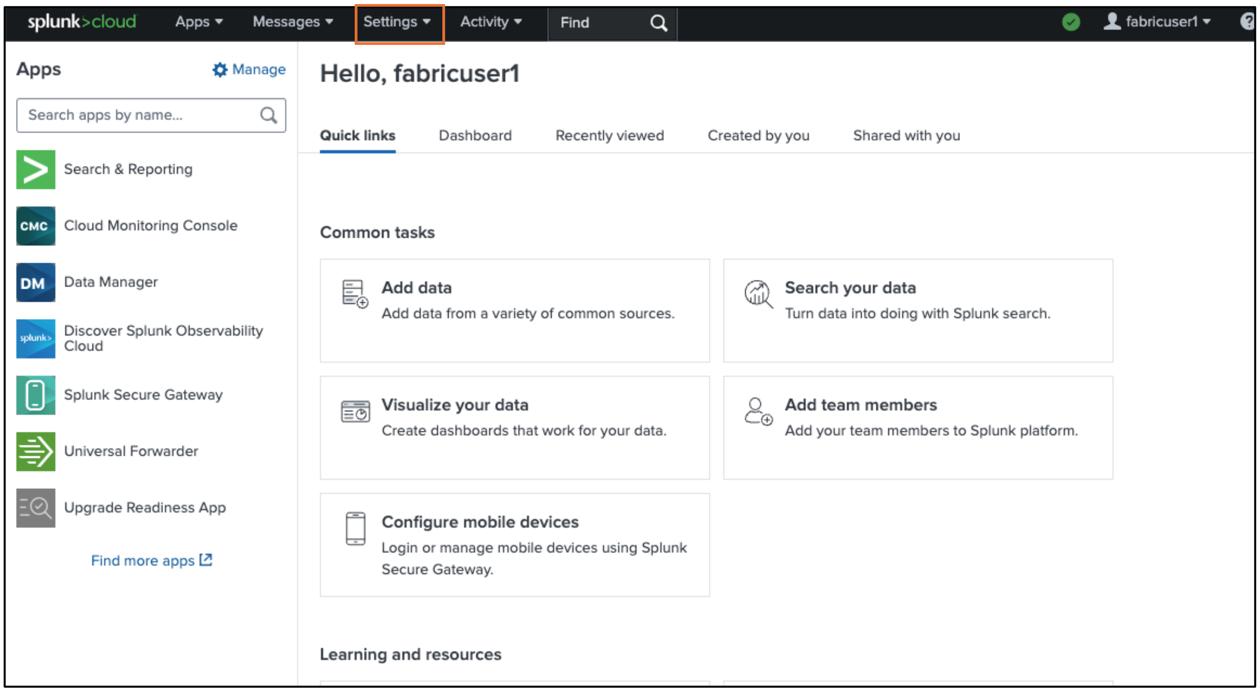
This guide will help you setup Indexes in Splunk to manage Metrics and Events. You will create two Indexes—one for Metrics and one for Events—and configure the settings for data retention and storage. You can use these Index details in the following POST fabric/v4/streamSubscriptions request

```
curl –X
POST 'https://api.equinix.com/fabric/v4/streamSubscriptions'
 -H 'Content-Type: application/json'
 -H ' Authorization: Bearer <Bearer Token>’
 -d '{
     "type": "STREAM_SUBSCRIPTION",
     "name": "jw-splunk-sub-0731",
     "description": "subscription 1",
     "stream": {
         "uuid": "241372e9-79c9-4ef8-b77a-8b8176c2098b4"
     },
     "sink": {
         "uri": "<protocol>://http-inputs-<host>.splunkcloud.com:<port>/<endpoint>",
         "type": "SPLUNK_HEC",
         "settings": {
             "eventIndex": "<name_of_eventIndex>",
             "metricIndex": "<name_of_metricIndex>",
             "source": "<name_of_splunk_hec>"
         },
         "credential": {
             "type": "ACCESS_TOKEN",
             "accessToken": "Splunk <Splunk Access Token>"
         }
     }
 }'
```

Step-by-Step Instructions

1. Log in and Navigate to the Home Page

- Start by logging into your Splunk instance.
- Once logged in, go to the **Home** page.



Hello, fabricuser1

Common tasks

Add data
Add data from a variety of common sources.

Search your data
Turn data into doing with Splunk search.

Visualize your data
Create dashboards that work for your data.

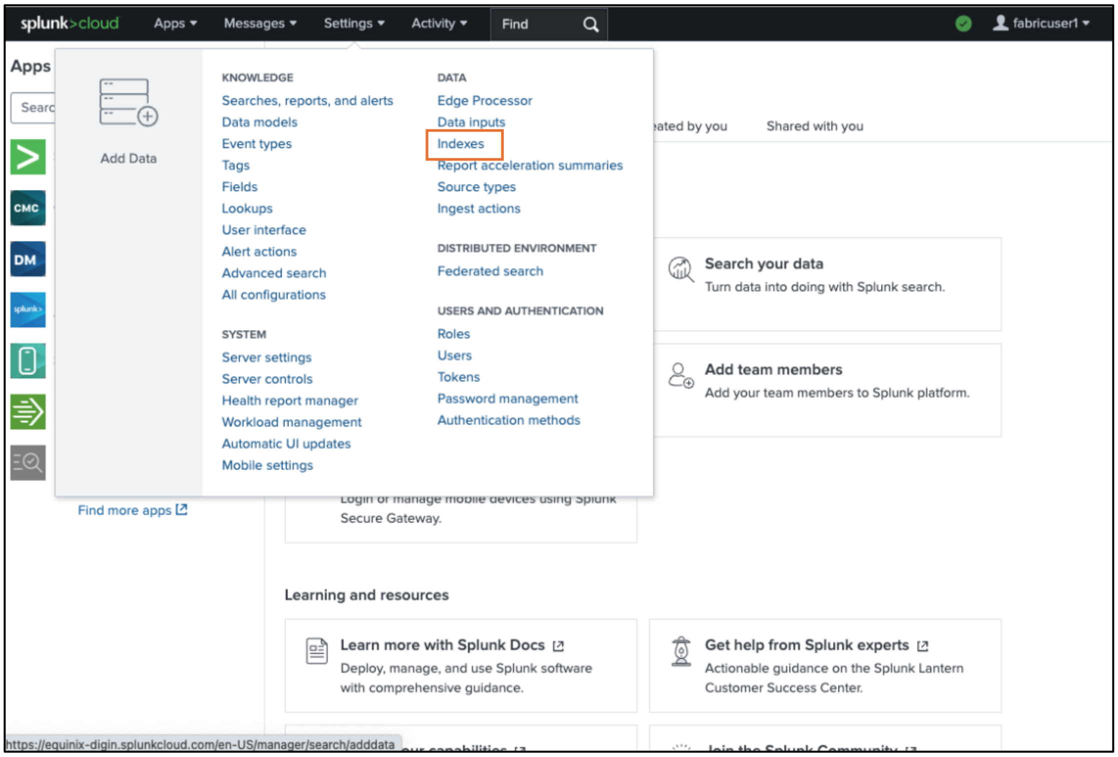
Add team members
Add your team members to Splunk platform.

Configure mobile devices
Login or manage mobile devices using Splunk Secure Gateway.

Learning and resources

2. Access the Settings

- On the Home page, click on **Settings** in the top menu.
- In the Settings menu, navigate to **Indexes** under the "Data" section.



Search your data
Turn data into doing with Splunk search.

Add team members
Add your team members to Splunk platform.

Login or manage mobile devices using Splunk Secure Gateway.

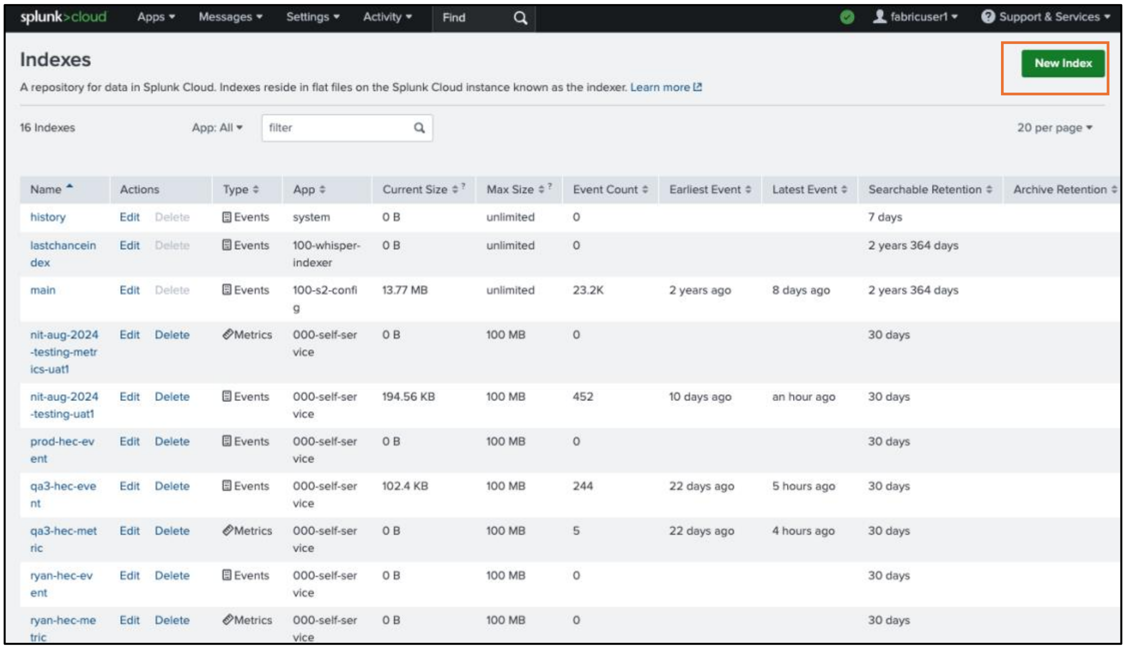
Learn more with Splunk Docs
Deploy, manage, and use Splunk software with comprehensive guidance.

Get help from Splunk experts
Actionable guidance on the Splunk Lantern Customer Success Center.

https://equinix-digin.splunkcloud.com/en-US/manager/search/adddata

3. Create a New Index

- On the Indexes page, click on **New Index** to create a new index.



Indexes

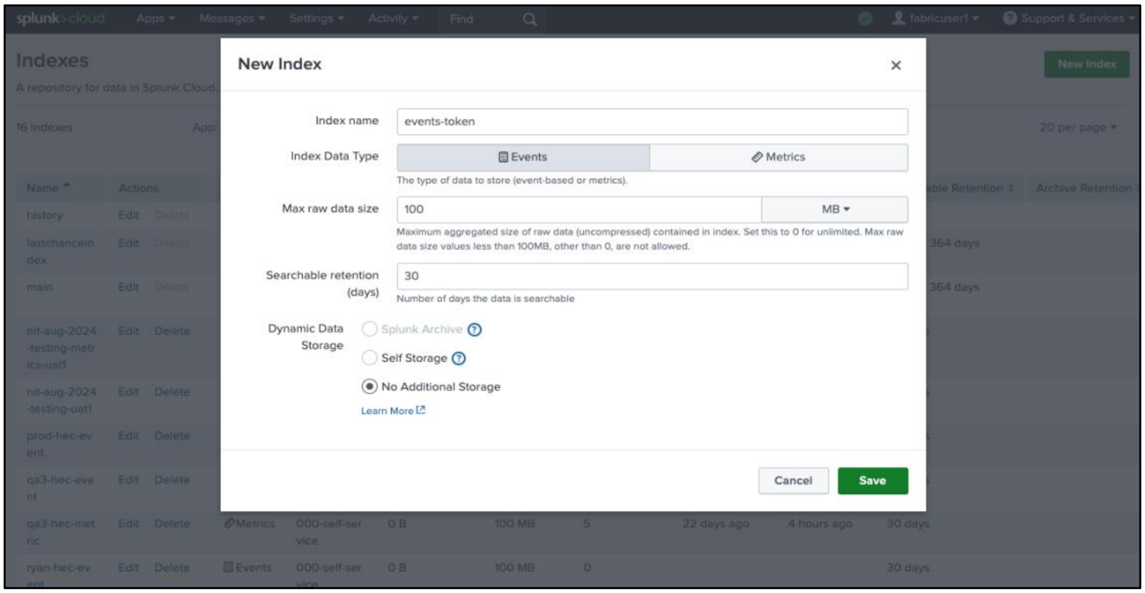
A repository for data in Splunk Cloud. Indexes reside in flat files on the Splunk Cloud instance known as the indexer. Learn more

16 Indexes App: All ▾ filter 20 per page ▾

Name	Actions	Type	App	Current Size	Max Size	Event Count	Earliest Event	Latest Event	Searchable Retention	Archive Retention
history	Edit Delete	Events	system	0 B	unlimited	0			7 days	
lastchanceindex	Edit Delete	Events	100-whisper-indexer	0 B	unlimited	0			2 years 364 days	
main	Edit Delete	Events	100-s2-config	13.77 MB	unlimited	23.2K	2 years ago	8 days ago	2 years 364 days	
nit-aug-2024-testing-metrics-uat1	Edit Delete	Metrics	000-self-service	0 B	100 MB	0			30 days	
nit-aug-2024-testing-uat1	Edit Delete	Events	000-self-service	194.56 KB	100 MB	452	10 days ago	an hour ago	30 days	
prod-hec-event	Edit Delete	Events	000-self-service	0 B	100 MB	0			30 days	
qa3-hec-event	Edit Delete	Events	000-self-service	102.4 KB	100 MB	244	22 days ago	5 hours ago	30 days	
qa3-hec-metric	Edit Delete	Metrics	000-self-service	0 B	100 MB	5	22 days ago	4 hours ago	30 days	
ryan-hec-event	Edit Delete	Events	000-self-service	0 B	100 MB	0			30 days	
ryan-hec-metric	Edit Delete	Metrics	000-self-service	0 B	100 MB	0			30 days	

3.1 Name the Index

- **Name:** Enter a name for your Index. For example, you may name one Index "metrics" and the other "events."



Index name	events-token
Index Data Type	[✓ Events] Metrics The type of data to store (event-based or metrics).
Max raw data size	100 MB ▾ Maximum aggregated size of raw data (uncompressed) contained in index. Set this to 0 for unlimited. Max raw data size values less than 100MB, other than 0, are not allowed.
Searchable retention (days)	30 Number of days the data is searchable
Dynamic Data Storage	○ Splunk Archive ○ Self Storage ● No Additional Storage Learn More

3.2 Select Index Data Type

- **Index Data Type:** If naming the index is for events or metrics, select the respective Index Data Type.

3.3 Set Data Size Limit

- **Data Size:** Set the data size limit for the Index. For example, you can set it to **100 MB**.

3.4 Configure Retention Policy

- **Retention Policy:** Set the retention policy to **30 days**. This means that data older than 30 days will be automatically deleted from the Index.

3.5 Set Dynamic Data Storage

- **Dynamic Data Storage:** Leave the settings as default for dynamic data storage. This ensures that your data is stored efficiently based on Splunk's default storage configuration

- Use above Index details in POST/fabric/v4/ fabric/v4/streamSubscriptions request

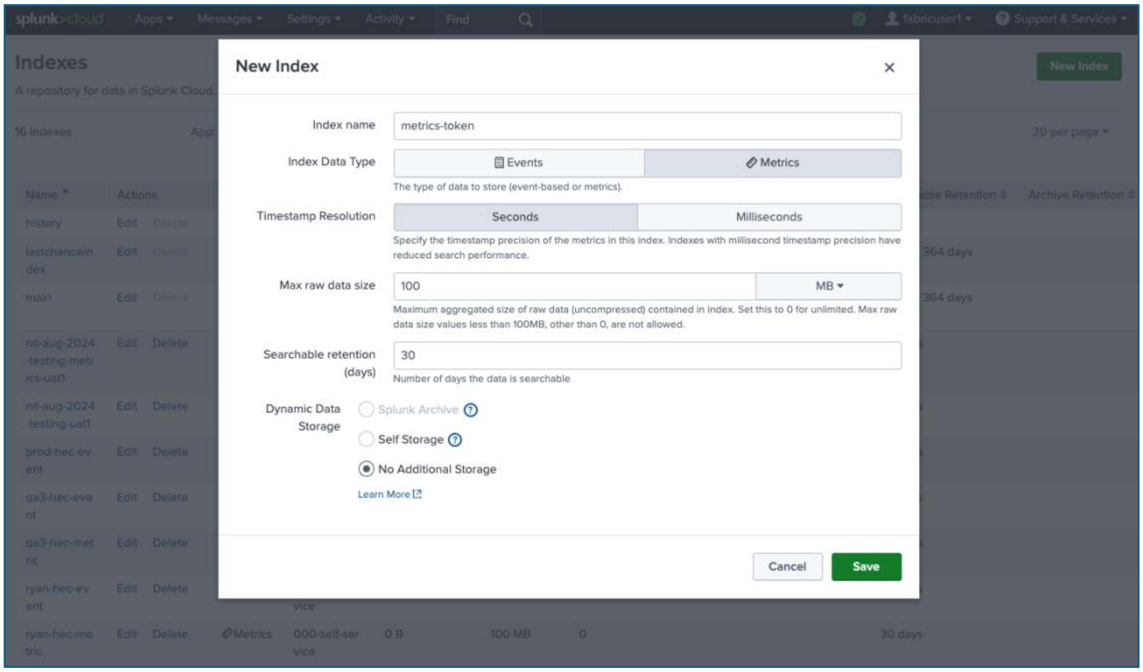
Example:

```
curl -X
POST 'https://api.equinix.com/fabric/v4/streamSubscriptions'
 -H 'Content-Type: application/json' \
 -H ' Authorization: Bearer <Bearer Token>' \
 -d '{
    "type": "STREAM_SUBSCRIPTION",
    "name": "jw-splunk-sub-0731",
    "description": "subscription 1",
    "stream": {
        "uuid": "241372e9-79c9-4ef8-b77a-8b8176c2098b4"
    },
    "sink": {
        "uri": "<protocol>://http-inputs-<host>.splunkcloud.com:<port>/<endpoint>",
        "type": "SPLUNK_HEC",
        "settings": {
            "eventIndex": "events-token",
            "source": "<name_of_splunk_hec>"
        },
        "credential": {
            "type": "ACCESS_TOKEN",
            "accessToken": "Splunk <Splunk Access Token>"
        }

    }
 }'
```

4. Repeat for the Second Index

- Follow the same steps to create a second Index. Make sure to give this Index a different name, such as "metrics" for Metrics data and "events" for Events data.
- After creating both Indexes, review your settings to ensure everything is correct.
- Click **Save** to finalize your Index configuration.



New Index ×

Index name: metrics-token

Index Data Type: Events | **Metrics**

The type of data to store (event-based or metrics).

Timestamp Resolution: **Seconds** | Milliseconds

Specify the timestamp precision of the metrics in this index. Indexes with millisecond timestamp precision have reduced search performance.

Max raw data size: 100 MB

Maximum aggregated size of raw data (uncompressed) contained in index. Set this to 0 for unlimited. Max raw data size values less than 100MB, other than 0, are not allowed.

Searchable retention (days): 30

Number of days the data is searchable

Dynamic Data Storage:
○ Splunk Archive
○ Self Storage
● No Additional Storage

Learn More

Cancel Save

- Use the above Index details in POST/fabric/v4/ fabric/v4/streamSubscriptions request.

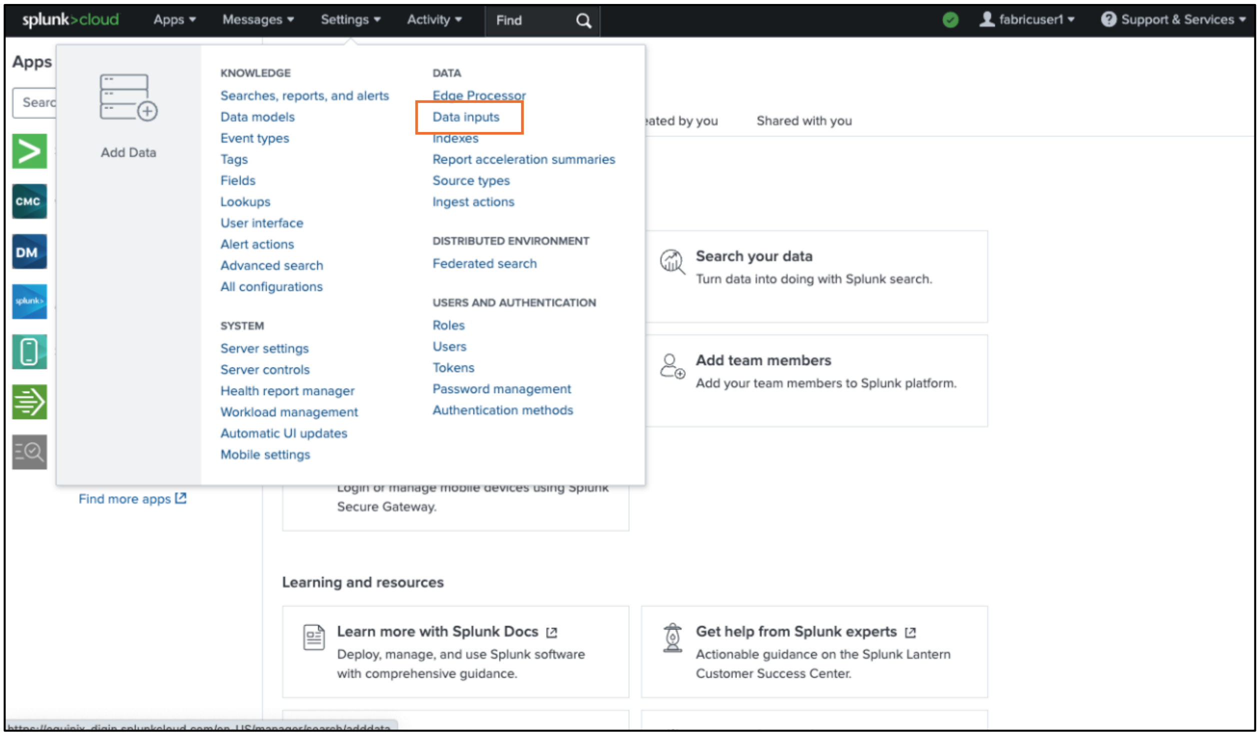
```
curl -X
POST 'https://api.equinix.com/fabric/v4/streamSubscriptions'
-H 'Content-Type: application/json'
-H ' Authorization: Bearer <Bearer Token>’
 -d '{
    "type": "STREAM_SUBSCRIPTION",
    "name": "jw-splunk-sub-0731",
    "description": "subscription 1",
    "stream": {
        "uuid": "241372e9-79c9-4ef8-b77a-8b8176c2098b4"
    },
    "sink": {
        "uri": "<protocol>://http-inputs-<host>.splunkcloud.com:<port>/<endpoint>",
        "type": "SPLUNK_HEC",
        "settings": {
            "metricIndex": "metrics-token",
            "source": "<name_of_splunk_hec>"
        },
        "credential": {
            "type": "ACCESS_TOKEN",
            "accessToken": "Splunk <Splunk Access Token>"
        }
    }
 }'
```

5. Generate Token Value

- Ensure that the token values generated during this process are saved securely. These tokens may be required for further integration or for data ingestion processes.

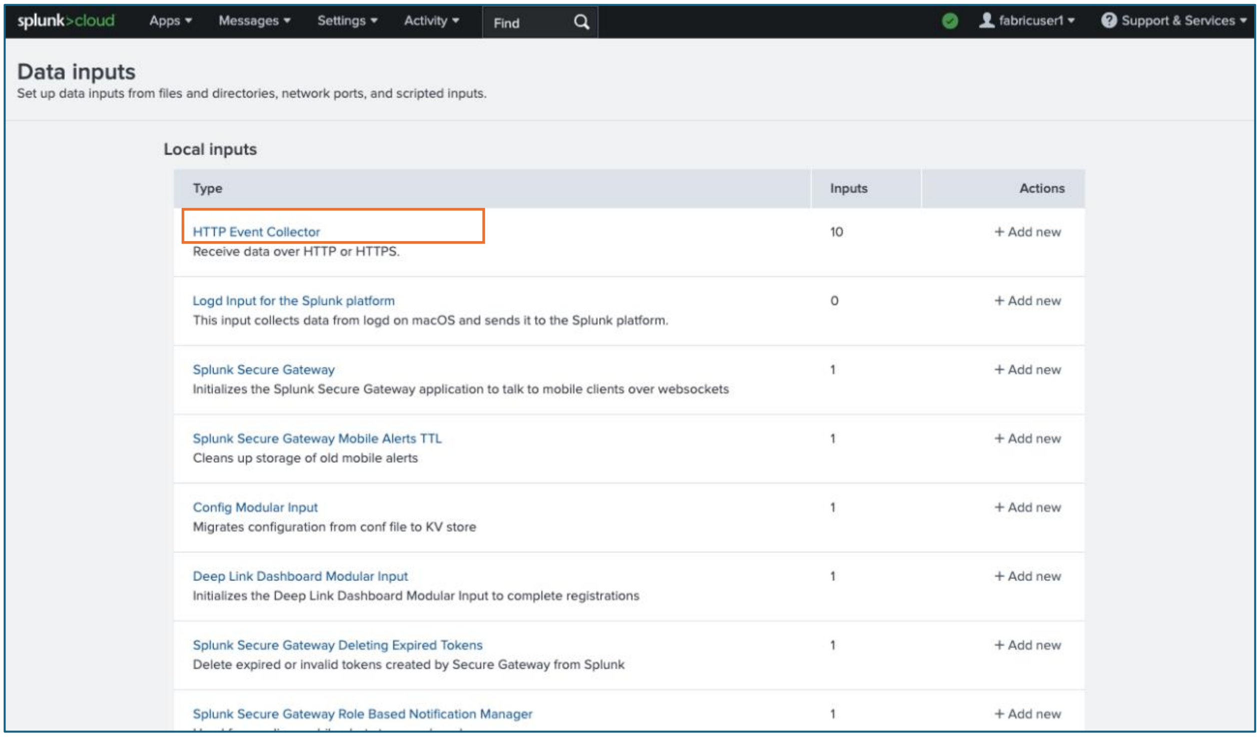
5.1. Navigate to the Splunk Home Page

- On the Home page, go to **Settings** in the top menu.
- Under the "Data" section, click on **Data inputs**.



5.2. Select HTTP Event Collector

- In the Data Inputs section, select **HTTP Event Collector**.



Data inputs

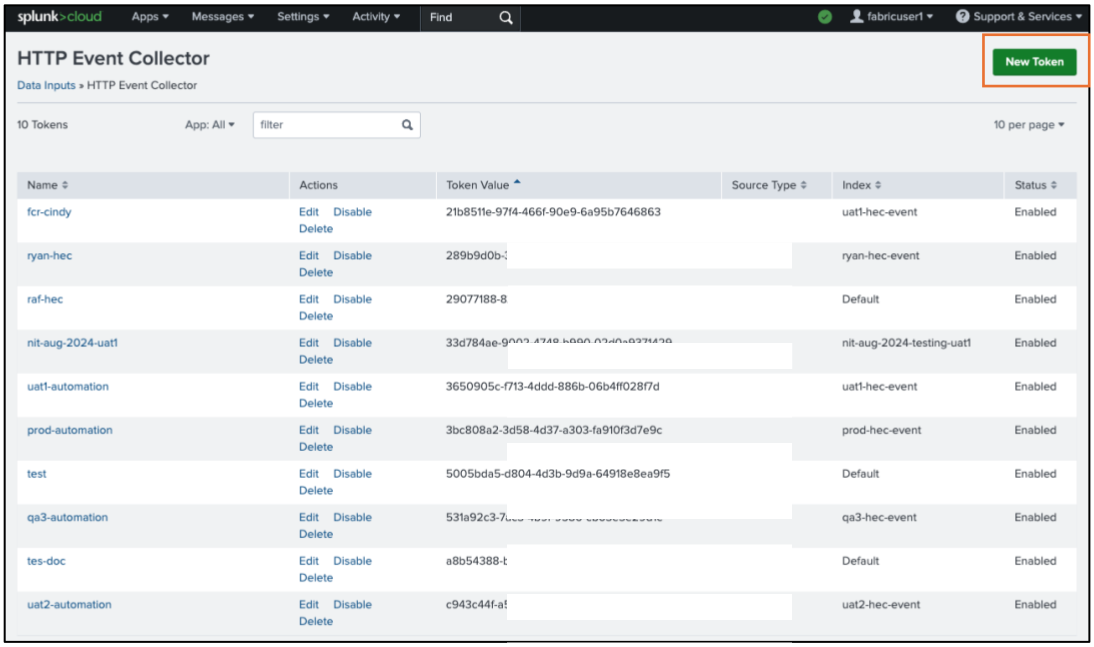
Set up data inputs from files and directories, network ports, and scripted inputs.

Local inputs

Type	Inputs	Actions
HTTP Event Collector Receive data over HTTP or HTTPS.	10	+ Add new
Logd Input for the Splunk platform This input collects data from logd on macOS and sends it to the Splunk platform.	0	+ Add new
Splunk Secure Gateway Initializes the Splunk Secure Gateway application to talk to mobile clients over websockets	1	+ Add new
Splunk Secure Gateway Mobile Alerts TTL Cleans up storage of old mobile alerts	1	+ Add new
Config Modular Input Migrates configuration from conf file to KV store	1	+ Add new
Deep Link Dashboard Modular Input Initializes the Deep Link Dashboard Modular Input to complete registrations	1	+ Add new
Splunk Secure Gateway Deleting Expired Tokens Delete expired or invalid tokens created by Secure Gateway from Splunk	1	+ Add new
Splunk Secure Gateway Role Based Notification Manager	1	+ Add new

5.3 Create a New Token

- Click the **New Token** button to start the setup process for the HTTP Event Collector.



HTTP Event Collector

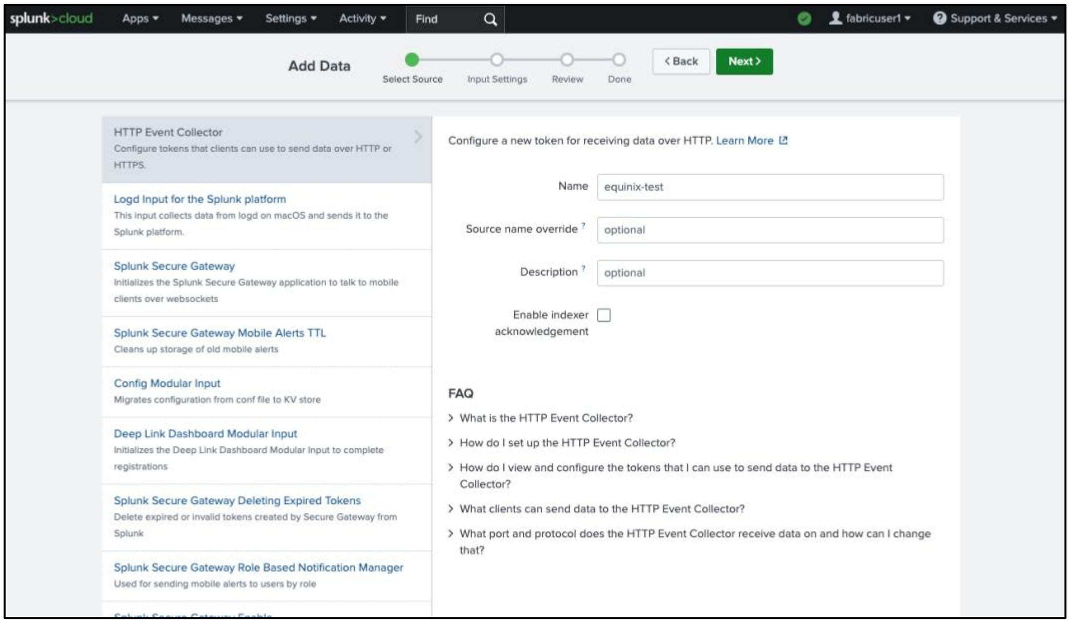
Data Inputs » HTTP Event Collector

10 Tokens

Name ⇕	Actions	Token Value ▴	Source Type ⇕	Index ⇕	Status ⇕
fcr-cindy	Edit Disable Delete	21b8511e-97f4-466f-90e9-6a95b7646863		uat1-hec-event	Enabled
ryan-hec	Edit Disable Delete	289b9d0b-[redacted]		ryan-hec-event	Enabled
raf-hec	Edit Disable Delete	29077188-8[redacted]		Default	Enabled
nit-aug-2024-uat1	Edit Disable Delete	33d784ae-9[redacted]		nit-aug-2024-testing-uat1	Enabled
uat1-automation	Edit Disable Delete	3650905c-f713-4ddd-886b-06b4ff028f7d		uat1-hec-event	Enabled
prod-automation	Edit Disable Delete	3bc808a2-3d58-4d37-a303-fa910f3d7e9c		prod-hec-event	Enabled
test	Edit Disable Delete	5005bda5-d804-4d3b-9d9a-64918e8ea9f5		Default	Enabled
qa3-automation	Edit Disable Delete	531a92c3-7[redacted]		qa3-hec-event	Enabled
tes-doc	Edit Disable Delete	a8b54388-[redacted]		Default	Enabled
uat2-automation	Edit Disable Delete	c943c44f-a[redacted]		uat2-hec-event	Enabled

5.4. Add Data Method

- On the **Add Data Methods** page, the only required input is the name.
- **Name:** Enter a name for your HTTP Event Collector.



HTTP Event Collector
Configure tokens that clients can use to send data over HTTP or HTTPS.

Logd Input for the Splunk platform
This input collects data from logd on macOS and sends it to the Splunk platform.

Splunk Secure Gateway
Initializes the Splunk Secure Gateway application to talk to mobile clients over websockets

Splunk Secure Gateway Mobile Alerts TTL
Cleans up storage of old mobile alerts

Config Modular Input
Migrates configuration from conf file to KV store

Deep Link Dashboard Modular Input
Initializes the Deep Link Dashboard Modular Input to complete registrations

Splunk Secure Gateway Deleting Expired Tokens
Delete expired or invalid tokens created by Secure Gateway from Splunk

Splunk Secure Gateway Role Based Notification Manager
Used for sending mobile alerts to users by role

Configure a new token for receiving data over HTTP. Learn More

Name: equinix-test

Source name override ?: optional

Description ?: optional

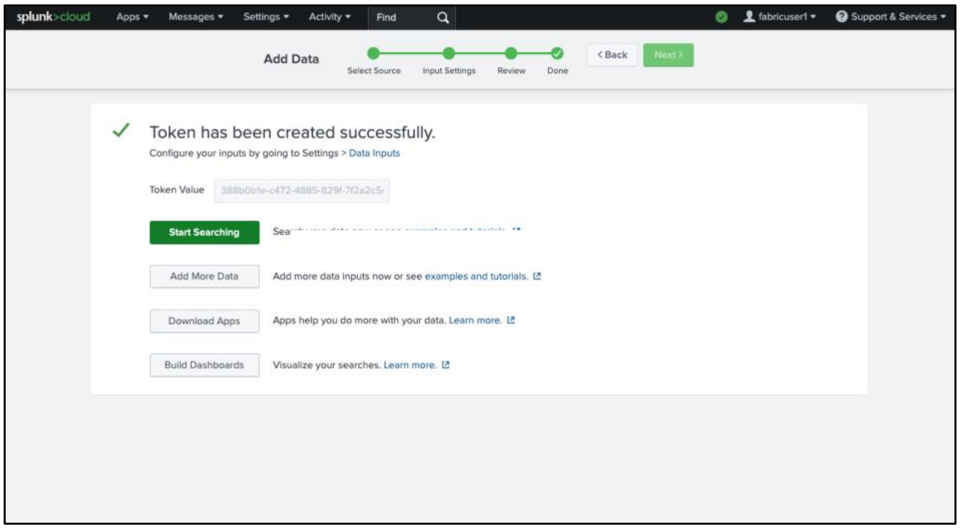
Enable indexer acknowledgement □

FAQ

- › What is the HTTP Event Collector?
- › How do I set up the HTTP Event Collector?
- › How do I view and configure the tokens that I can use to send data to the HTTP Event Collector?
- › What clients can send data to the HTTP Event Collector?
- › What port and protocol does the HTTP Event Collector receive data on and how can I change that?

5.5. Complete the Setup

- After naming your token, click **Next** to move to the **Select Source** step.
- Click **Review** on the **Input Settings** step to review your configurations.
- Finally, click **Submit** on the **Review** step to complete the setup.



✓ Token has been created successfully.

Configure your inputs by going to Settings > Data Inputs

Token Value: 388b0b1e-c472-4885-829f-7f2a2c5

Start Searching — Sea[illegible]

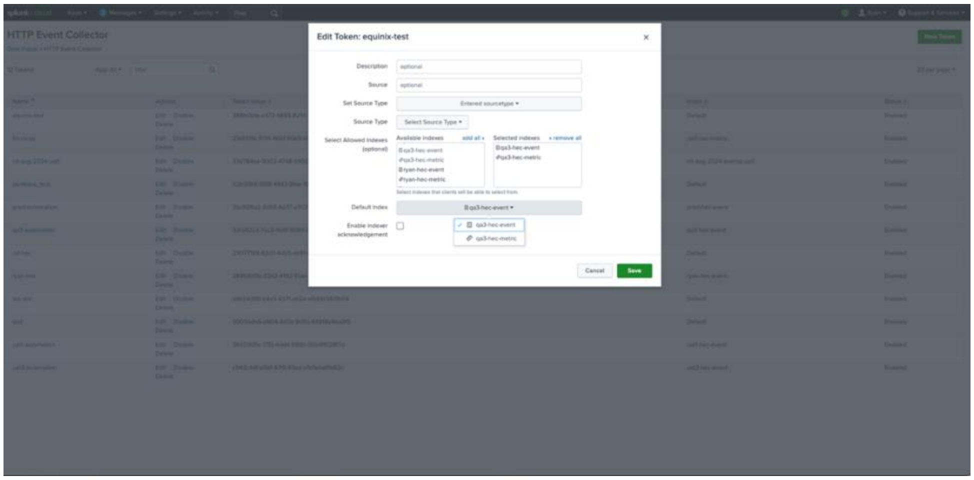
Add More Data — Add more data inputs now or see examples and tutorials.

Download Apps — Apps help you do more with your data. Learn more.

Build Dashboards — Visualize your searches. Learn more.

5.6. Add Event and Metric Indexes to the HTTP Event Collector (HEC)

- In HTTP Event Collector, click “Edit” on your HTTP Event Collector (HEC).
- Select your event and metric indexes.
- Set the event index as your Default Index.



Description: optional

Source: optional

Set Source Type: Entered sourcetype ▾

Source Type: Select Source Type ▾

Select Allowed Indexes (optional): Available indexes (add all »): qa3-hec-event, qa3-hec-metric, ryan-hec-event, ryan-hec-metric; Selected indexes (« remove all): qa3-hec-event, qa3-hec-metric

Select indexes that clients will be able to select from.

Default Index: qa3-hec-event ▾ (✓ qa3-hec-event, qa3-hec-metric)

Enable indexer acknowledgement: □

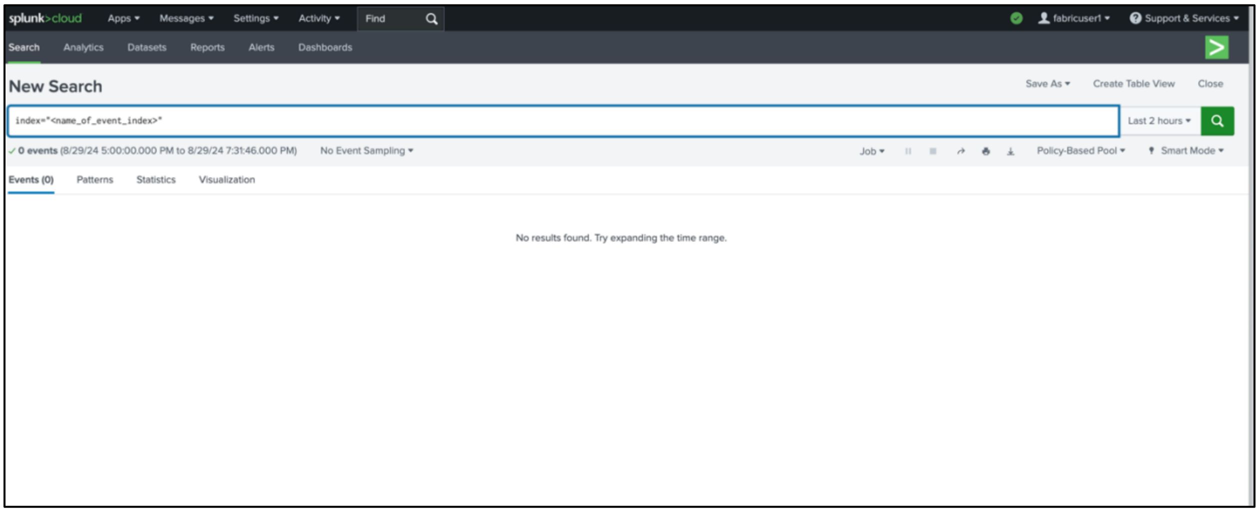
5.7. Copy the Token Value

- Once the setup is complete, a Token value will be generated.
- **Copy this Token value** to your clipboard, as it will be needed later for the POST streamSubscription API in Stream Observability.
- You can use the Splunk token in POST/fabric/v4/ fabric/v4/streamSubscriptions request Example:

```
curl –X
POST 'https://api.equinix.com/fabric/v4/streamSubscriptions'
 -H 'Content-Type: application/json'
 -H ' Authorization: Bearer <Bearer Token>’
 -d '{
     "type": "STREAM_SUBSCRIPTION",
     "name": "jw-splunk-sub-0731",
     "description": "subscription 1",
     "stream": {
         "uuid": "241372e9-79c9-4ef8-b77a-8b8176c2098b4"
     },
     "sink": {
         "uri": "<protocol>://http-inputs-<host>.splunkcloud.com:<port>/<endpoint>",
         "type": "SPLUNK_HEC",
         "settings": {
             "eventIndex": "<name_of_eventIndex>",
             "metricIndex": "<name_of_metricIndex>",
             "source": "<name_of_splunk_hec>"
         },
         "credential": {
             "type": "ACCESS_TOKEN",
             "accessToken": "Splunk <Splunk Access Token>"
         }
     }
 }'
```

6. Search Event

- Go to Home Page. Click on **Search & Reporting**. This will take you to a Splunk search page and search with your index. E.g. index=” <name_of_event_index>”



New Search

```
index="<name_of_event_index>"
```

✓ 0 events (8/29/24 5:00:00.000 PM to 8/29/24 7:31:46.000 PM)

No results found. Try expanding the time range.

- Now that the HTTP Event Collector is set up, you can use the Stream Observability APIs to create a subscription for CloudEvents.
- Use the previously copied Token value from the POST streamSubscription API call to setup your CloudEvents subscription.
- Refer to the “Fabric Observability with Client Sink Integration” document for detailed instructions on how to receive Events using a specific Sink Type.