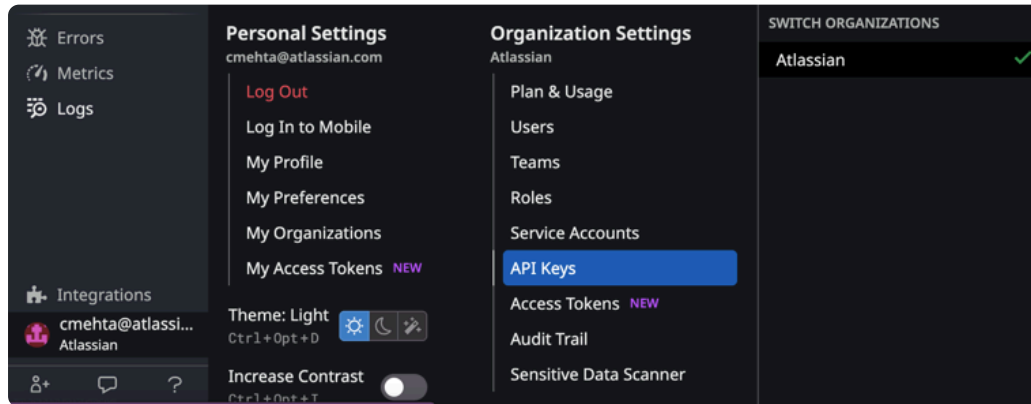


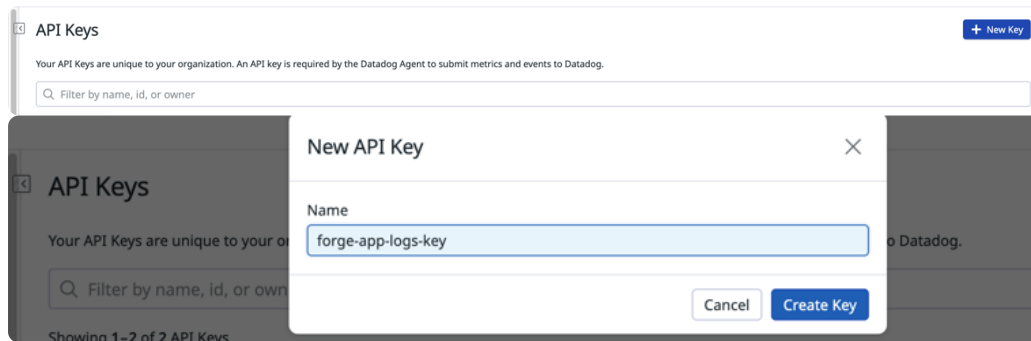
## Forge Logs Export - Setup vendor account

### Datadog

1. Login to your Datadog account.
2. Navigate to API Keys section in Organization Settings.



3. Click on **New Key** and provide your desired name.



4. Copy the key generated to be shared.

New API Key

.....9217

Copy

Name

forge-app-logs-key

Key ID

c7927f12-137e-4dd3-8f39-8ba4170059a1

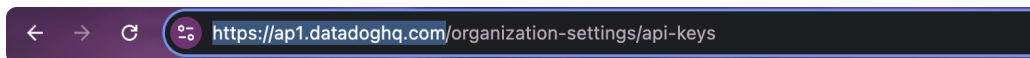
Remote Config

Enabled

Disable

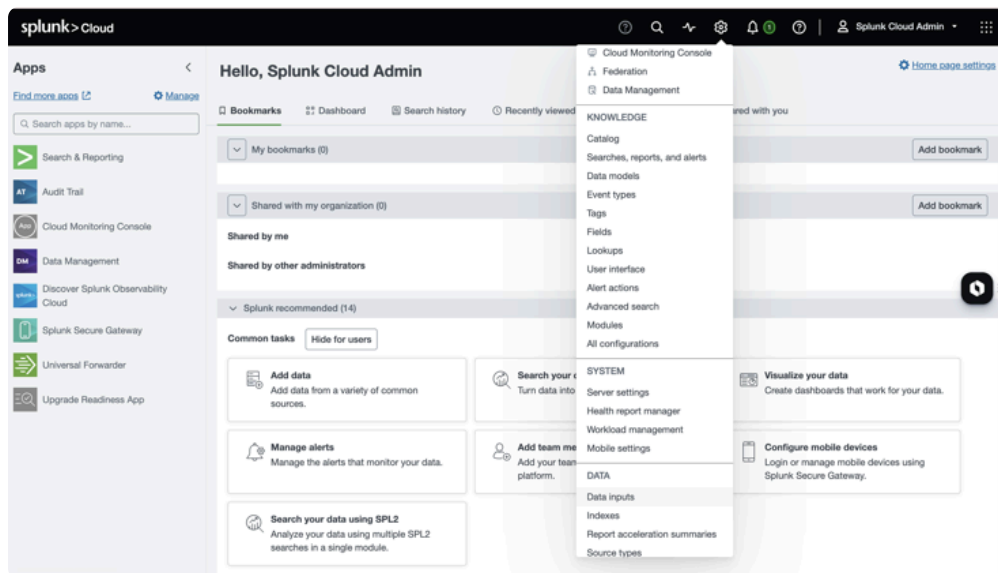
Finish

- You can find the base URL from the browser URL. Final URL will have the format - `https://http-intake.logs.{base}/api/v2/logs` .Sample - `https://http-intake.logs.us3.datadoghq.com/api/v2/logs`



## Splunk

- Login to your Splunk instance.
- Navigate to Settings → Data Inputs.



- Add new HTTP Event Collector

| Local inputs                                                    |        |           |
|-----------------------------------------------------------------|--------|-----------|
| Type                                                            | Inputs | Actions   |
| <b>HTTP Event Collector</b><br>Receive data over HTTP or HTTPS. | 1      | + Add new |

- Give it appropriate name and description. Ensure that **Enable Index Acknowledgement** checkbox is unticked.

Configure a new token for receiving data over HTTP. [Learn More](#)

Name

Source name override ?

Description ?

Enable indexer acknowledgement ? ☐

- Select the desired Source Type, Allowed indices and Default Index. You can expect the incoming logs to flow into the default index.

### 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.

Automatic Select New

**Index**

The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. [Learn More](#)

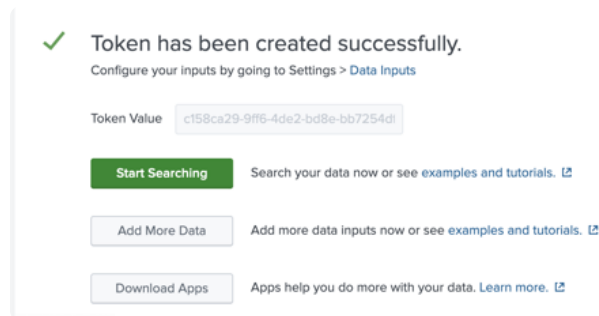
Select Allowed Indexes Available item(s) add all > Selected item(s) < remove all

☐ history  
☐ lastchanceindex  
☐ main  
☐ summary

Select indexes that clients will be able to select from.

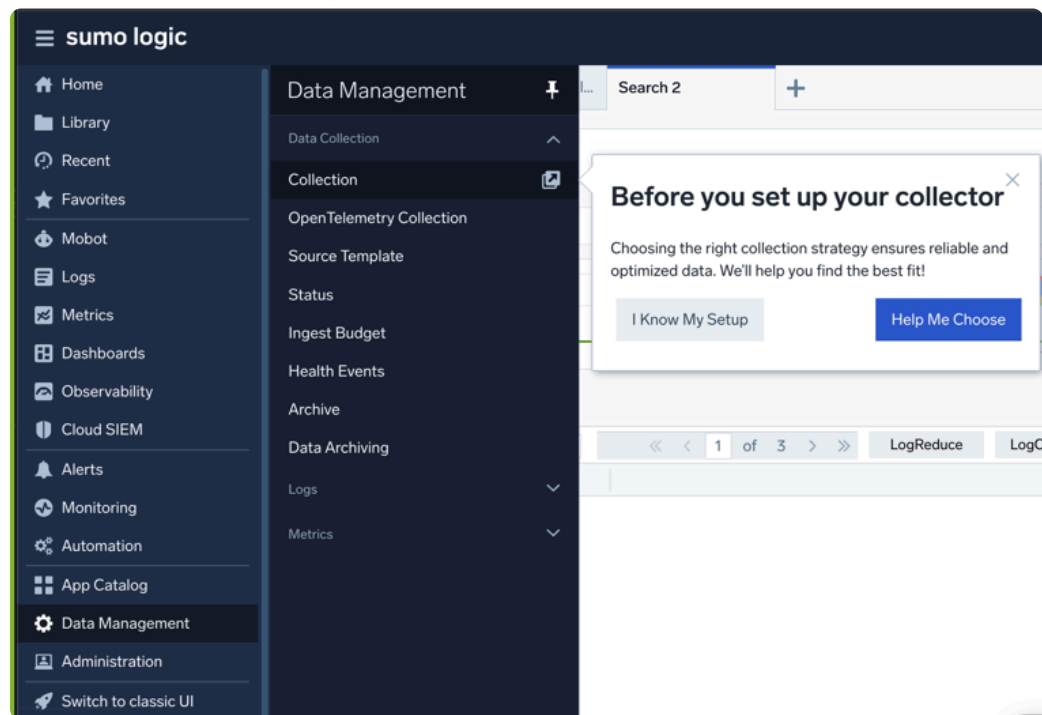
Default Index

- Once you review and Submit, ensure to copy the **Token Value** which is the API key that needs to be shared.

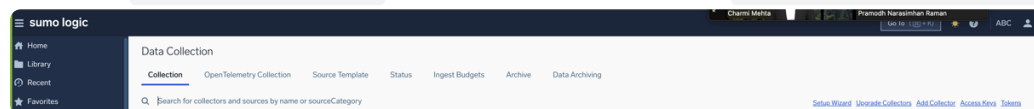


## Sumologic

1. Login to the new UI.
2. Navigate to Data Management → Collection.



3. Click on **Add Collector** in the screen and select **Hosted Collector**.



4. Add Name and other details and create the collector.

×

## Add Hosted Collector

Name \*

Description

Category

Unless overwritten by Source metadata, the Collector will set the Source category of all messages to this value.

Fields/  
Metadata

+Add Field

Time Zone

(UTC) Etc/UTC

Unless overwritten by Source time zone, the Collector will set the Source time zone of all messages to this value.

Cancel

Save

- Against the created collector, select **Add Source** . Select **HTTP Logs & Metrics** . Add Name and other details and click on Save.

Data Collection

Collection

OpenTelemetry Collection

Source Template

Status

Ingest Budgets

Archive

Data Archiving

Q Search for collectors and sources by name or sourceCategory

Setup Wizard Upgrade Collectors Add Collector Access Keys Tokens

Show: All Collectors

Show up to: 10 collectors

Expand: All | None

Name

Health

Type

Status

Source Category

Sources

Last Hour

Messages

Forge Logs collector

Healthy

Hosted

None

None

Add Source

Edit

Delete

Data Collection

Collection

OpenTelemetry Collection

Source Template

Status

Ingest Budgets

Archive

Data Archiving

Collectors and Sources

> Select Source for Collector Forge Logs collector

Q Search Source

Generic

Airtable

Citrix Cloud

Cloud Syslog

CrowdStrike FDR Host Inventory

Gmail Trace Logs

HTTP Logs & Metrics

Data Collection

Collection

OpenTelemetry Collection

Source Template

Sta

Collectors and Sources

 > 

Select Source for Collector Forge Logs collector

 > 

H

HTTP Logs & Metrics

Name

Test source

Description (optional)

Source Host (optional)

Source Category (optional)

Fields/Metadata

| Key              | Value |
|------------------|-------|
| <div>+ Add</div> |       |

Advanced Options for Logs (Optional)

Processing Rules (Optional)

Learn More

Cancel

Save

6. In the HTTP Source Address popup, choose Auth Header and copy the Header and URL details to be shared.

### HTTP Source Address

Use any of the following address type to send data to the Collector. Switching the address type will not impact your data collection [Learn more](#)

**Note: Keep this address private since anyone can use it to send data.**

☐ Presigned URL  
Use a complete URL with embedded authentication

☒ Auth Header  
Use a base URL with separate authentication header

**Header**

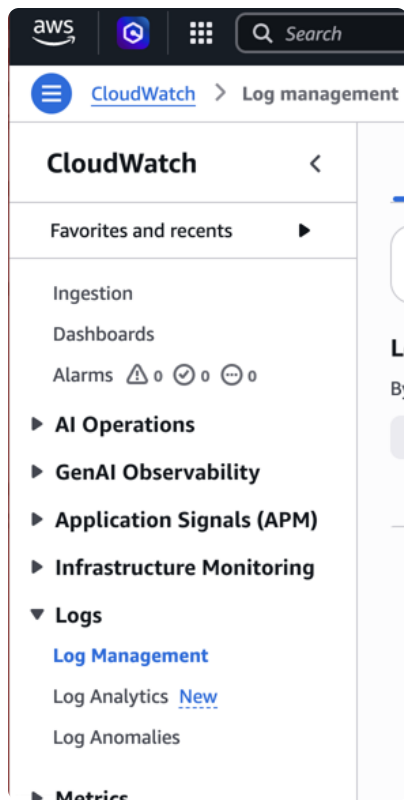
**URL**

## CloudWatch

### Disclaimer

Cloudwatch HTTP log export is only supported in US regions. Ref: [Amazon CloudWatch Logs now supports log ingestion using HTTP-based protocol - AWS](#) .

1. Login to AWS and navigate to CloudWatch → Logs → Log Management.



2. Create a log group with desired details.

### Log group details [Info](#)

CloudWatch Logs offers three log classes: Standard, Infrequent Access, and Delivery. [Learn more about the features offered by each log class.](#)

**Log group name**

**Retention setting**

3 days

**Log class** [Info](#)

Standard

**KMS key ARN - optional**

[Create an AWS KMS key](#)

☐ **Deletion protection**

Deletion protection is turned off by default. Deletion protection helps prevent accidental or unintended deletion of log groups that store critical operational or compliance data.

### Tags

A tag is a label that you assign to an Amazon Web Services resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your Amazon Web Services costs.

No tags are associated with this log group.

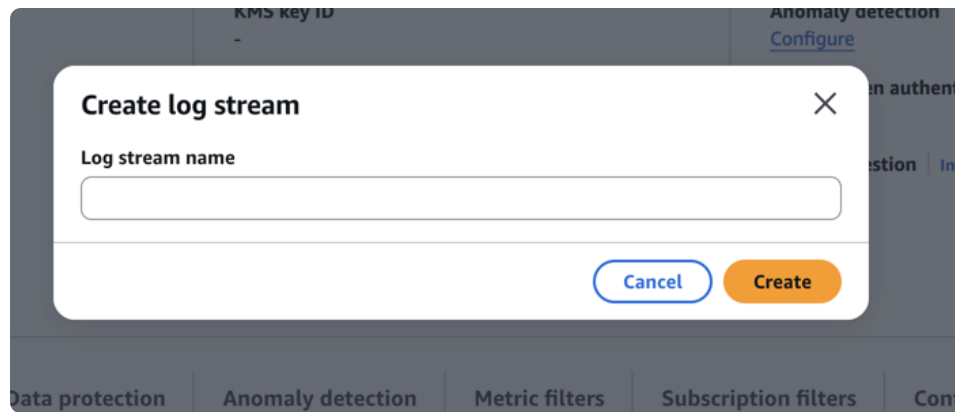
[Add new tag](#)

You can add up to 50 more tag(s).

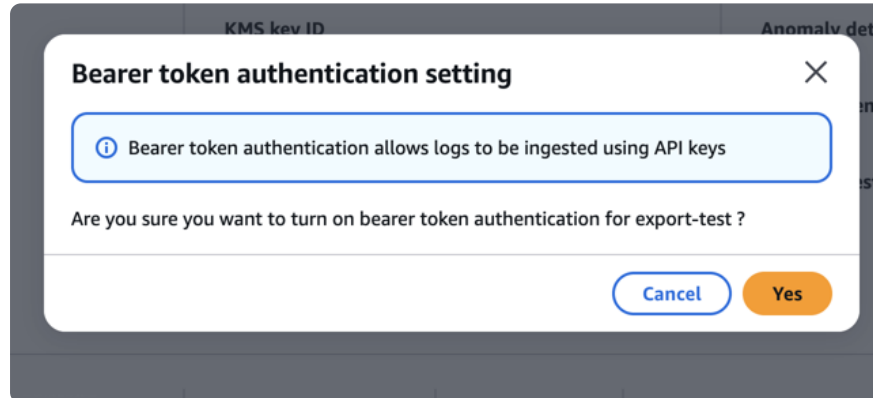
[Cancel](#) [Create](#)

3. Create a log stream within the created log group.

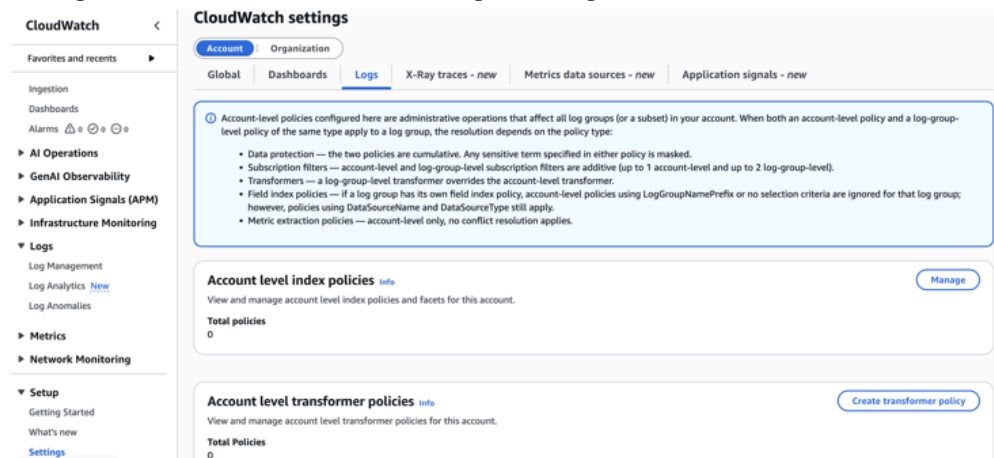




4. On the log group, Actions → Edit Bearer Token Authentication and Enable Authentication.



5. Navigate to CloudWatch → Settings → Logs.



6. Under API Keys section, create a new API Key with desired details and click Generate.
7. Share the API key, log group name and log stream name.

## Required data

1. Developer space ID
2. Vendor (supported ones - datadog, splunk, sumologic, cloudwatch)
3. API key
4. URL (eg: <https://http-intake.logs.us3.datadoghq.com/api/v2/logs>)
5. Deny list of apps if any

6. Allowed env types (supported - production, staging, development)