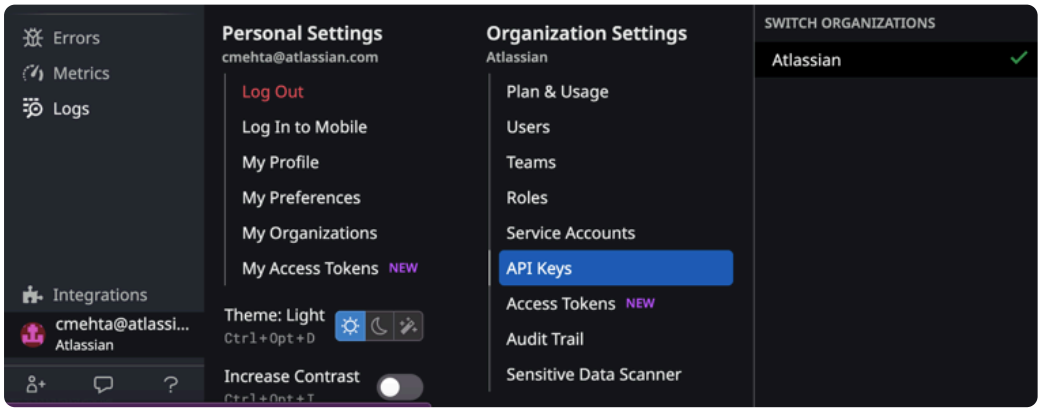
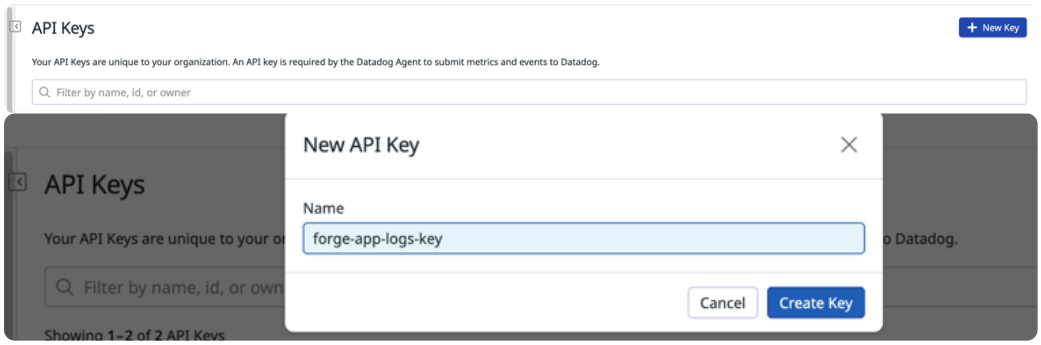
Forge Logs Export - Setup vendor account

Datadog

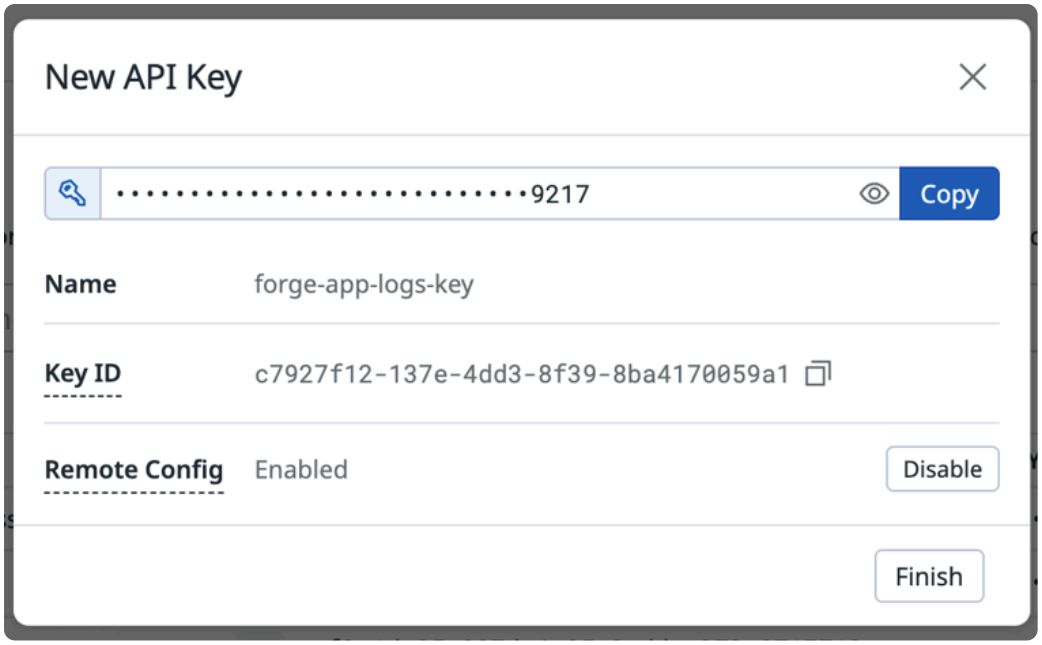
1. Login to your Datadog account.
2. Navigate to API Keys section in Organization Settings.



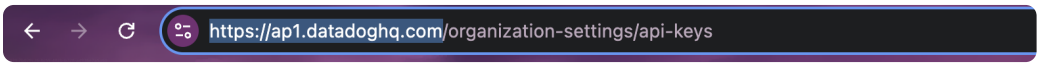
3. Click on `New Key` and provide your desired name.



4. Copy the key generated to be shared.

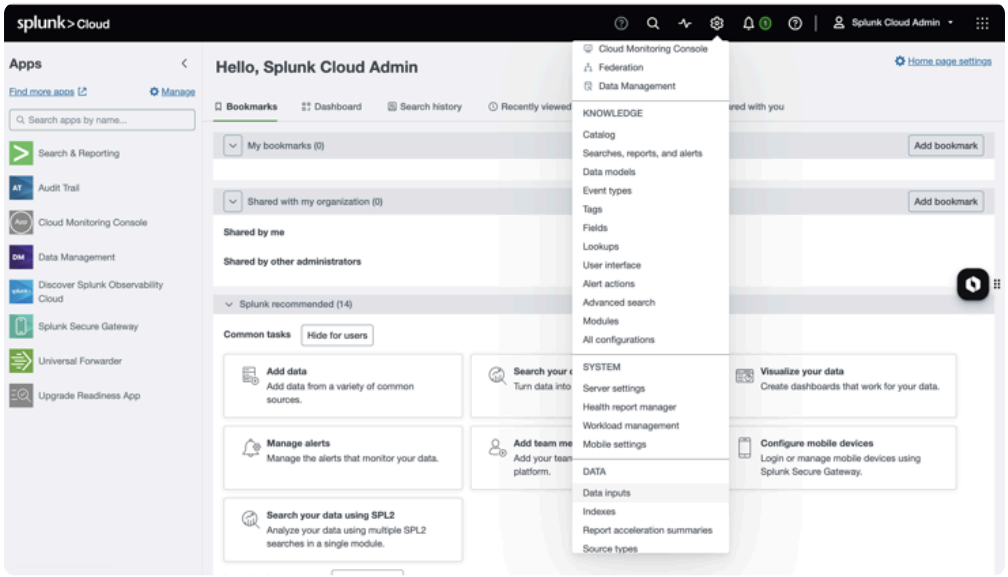


5. You can find the base URL from the browser URL. Final URL will have the format - `https://http-intake.logs.{base}/api/v2/logs` .Sample - `https://http-intake.logs.us3.datadoghq.com/api/v2/logs`

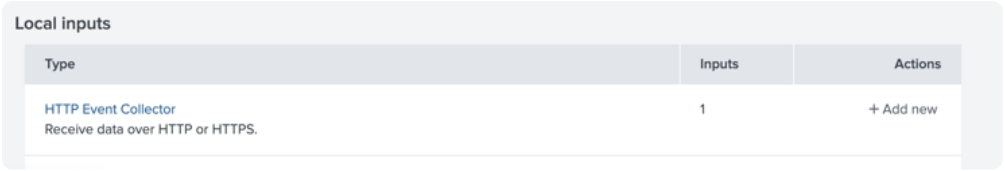


Splunk

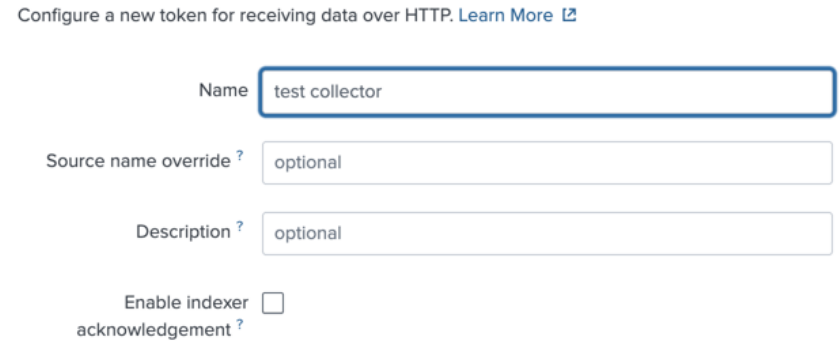
1. Login to your Splunk instance.
2. Navigate to Settings → Data Inputs.



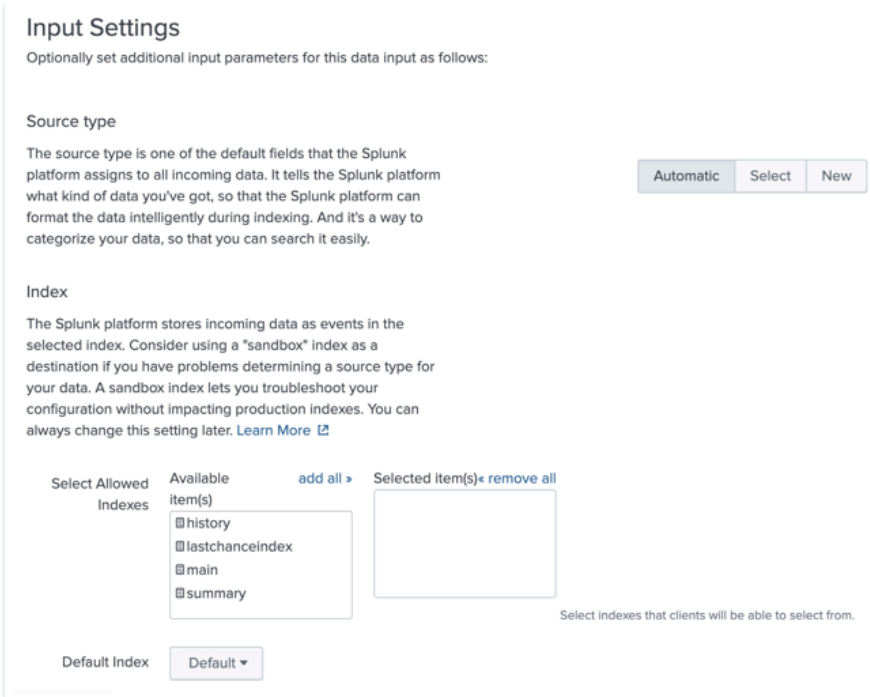
3. Add new HTTP Event Collector



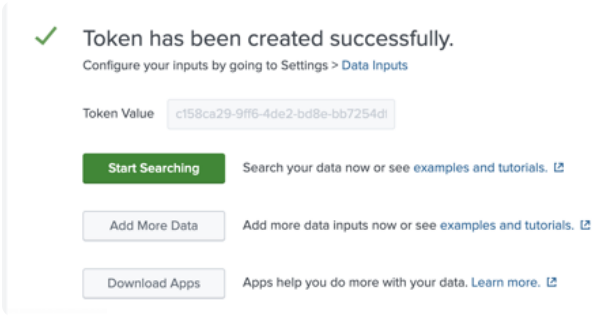
4. Give it appropriate name and description. Ensure that `Enable Index Acknowledgement` checkbox is unticked.



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

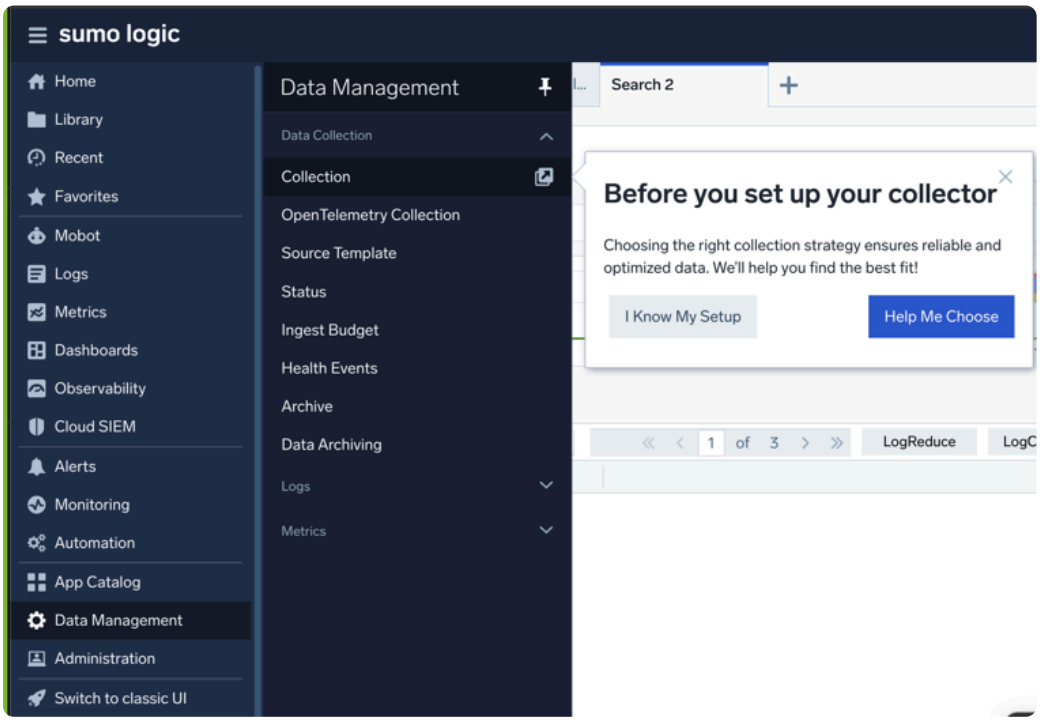


6. Once you review and Submit, ensure to copy the `Token Value` which is the API key that needs to be shared.

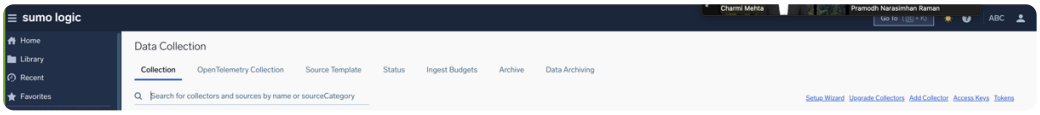


Sumologic

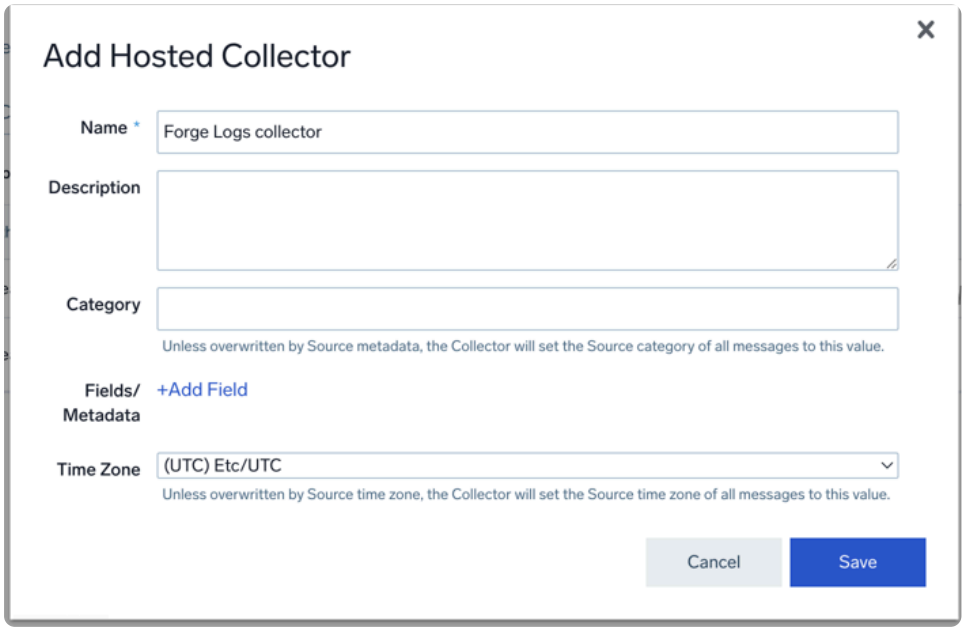
1. Login to the new UI.
2. Navigate to Data Management → Collection.



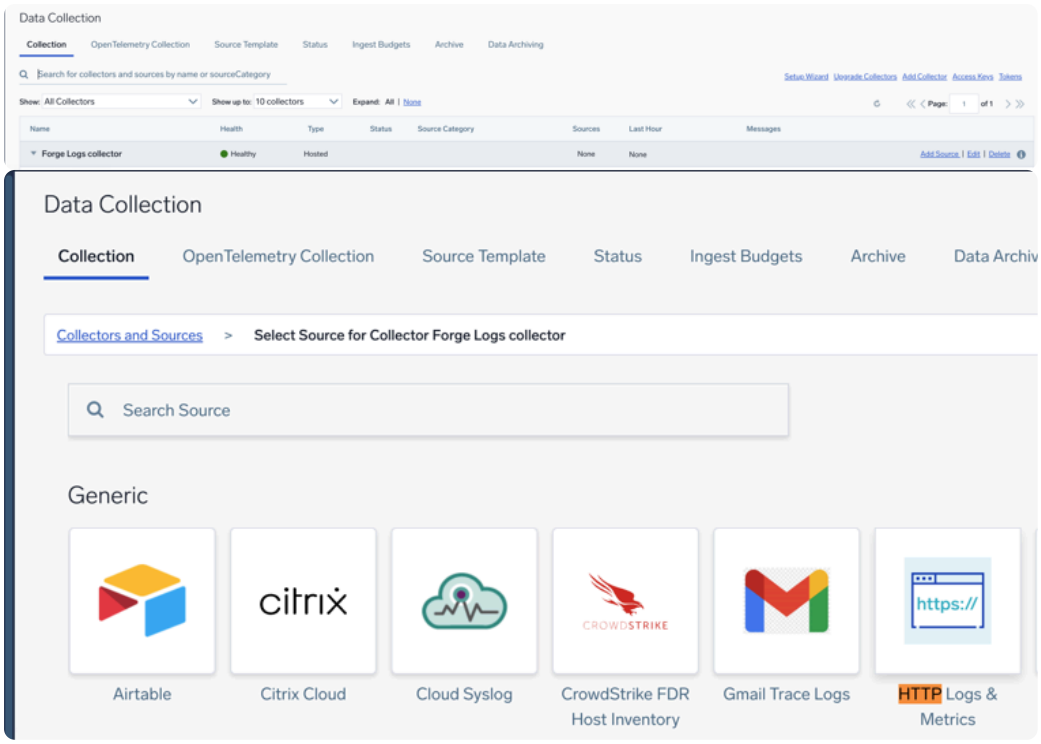
3. Click on `Add Collector` in the screen and select `Hosted Collector`.

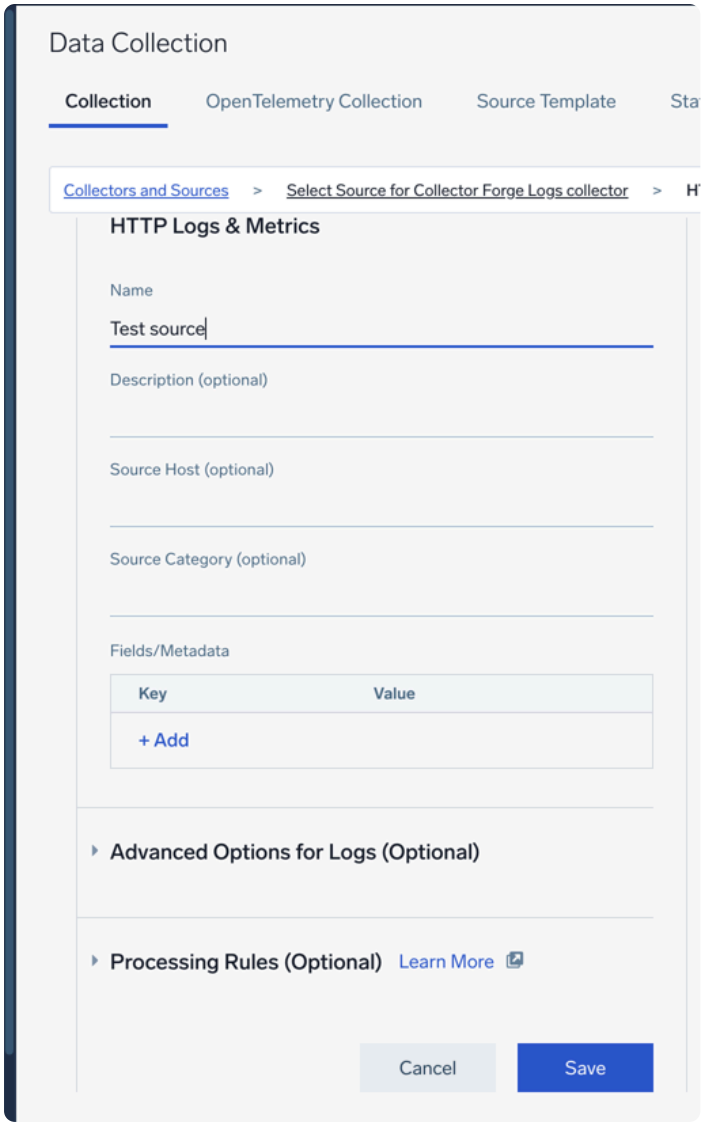


4. Add Name and other details and create the collector.

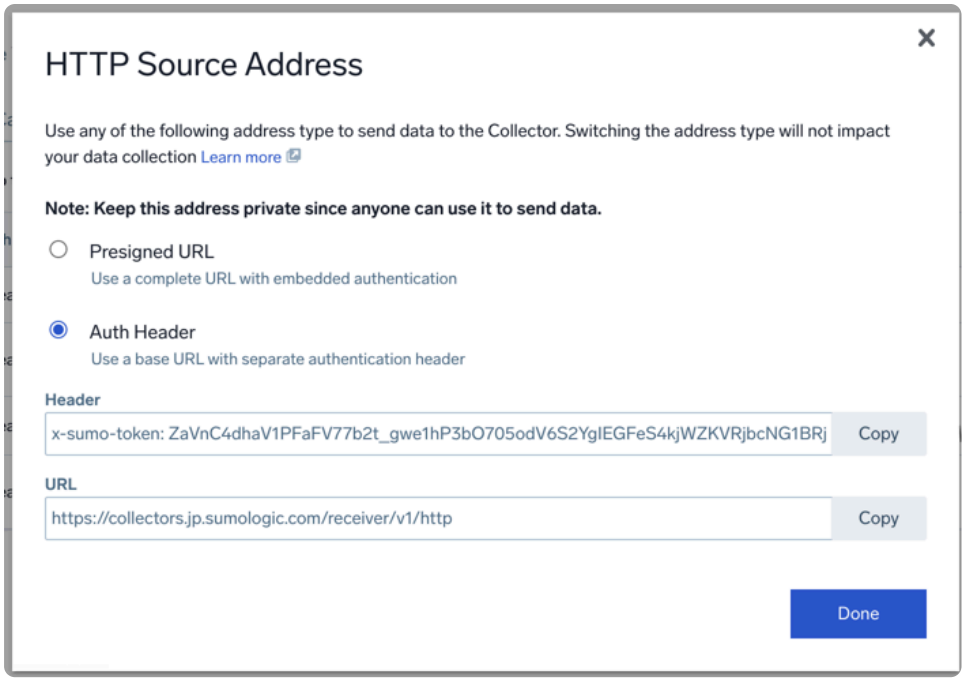


5. Against the created collector, select `Add Source`. Select `HTTP Logs & Metrics`. Add Name and other details and click on Save.





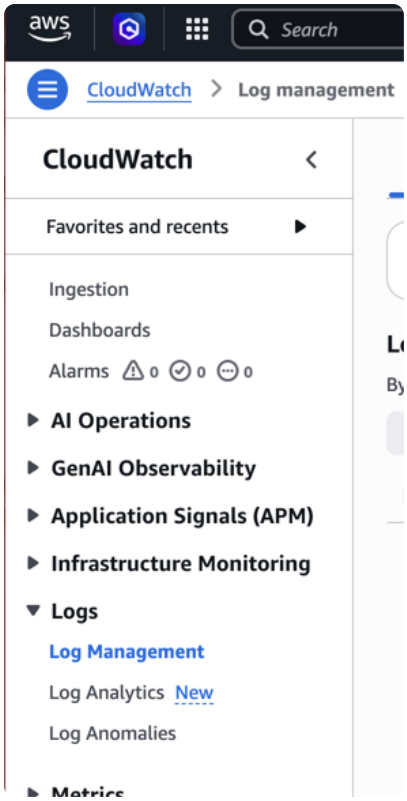
6. In the `HTTP Source Address` popup, choose `Auth Header` and copy the Header and URL details to be shared.



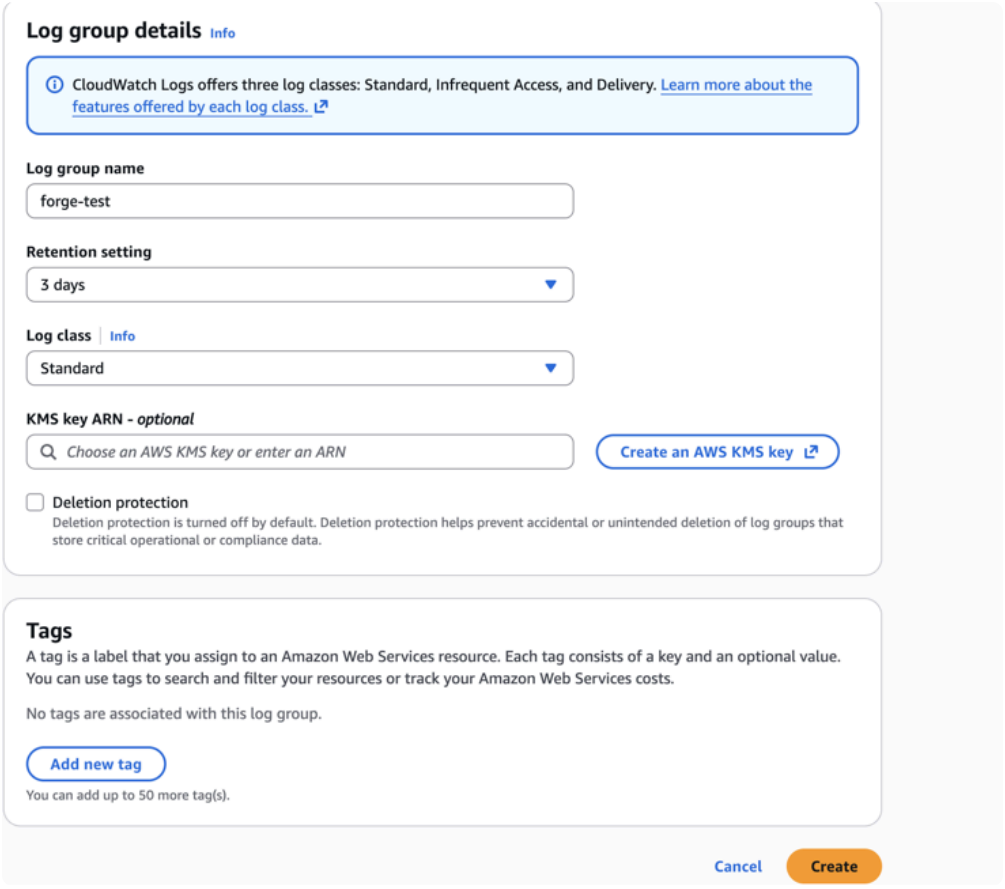
CloudWatch

> **Disclaimer**
>
> Cloudwatch HTTP log export is only supported in US regions. Ref: Amazon CloudWatch Logs now supports log ingestion using HTTP-based protocol - AWS .

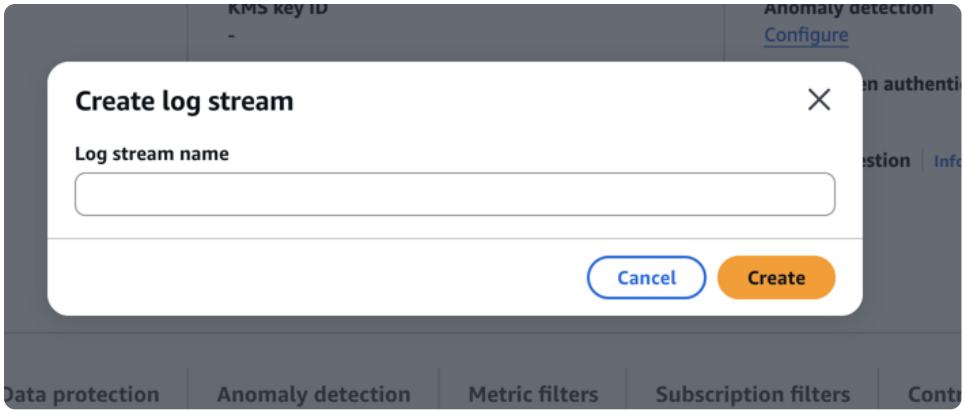
1. Login to AWS and navigate to CloudWatch → Logs → Log Management.



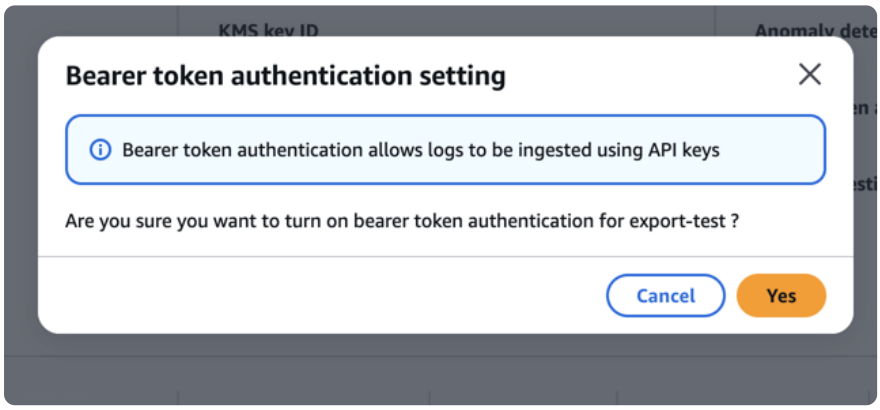
2. Create a log group with desired details.



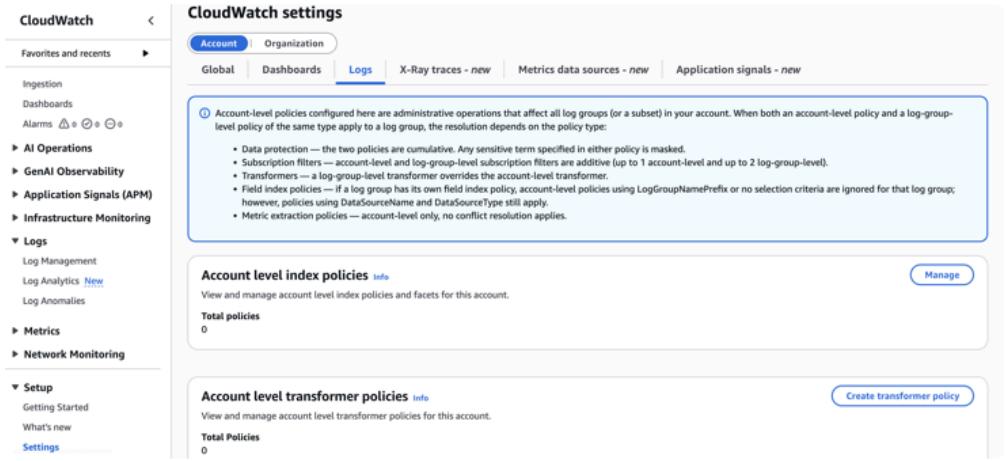
3. Create a log stream within the created log group.



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)