Collect Logs for Lucidum

Collector URL

`https://endpoint4.collection.sumologic.com/receiver/v1/http/ZaVnC4d****EAuUHJQ==`

cURL Examples

The cURL examples below point to the SumoLogic endpoint set up on 12/17/2021 to start developing Lucidum support for SumoLogic.

POST example

```
curl -v -X POST -T /path/to/your/logfile.log https://endpoint4.
collection.sumologic.com/receiver/v1/http/ZaVnC4d****EAuUHJQ==
```

POST gzip compressed data

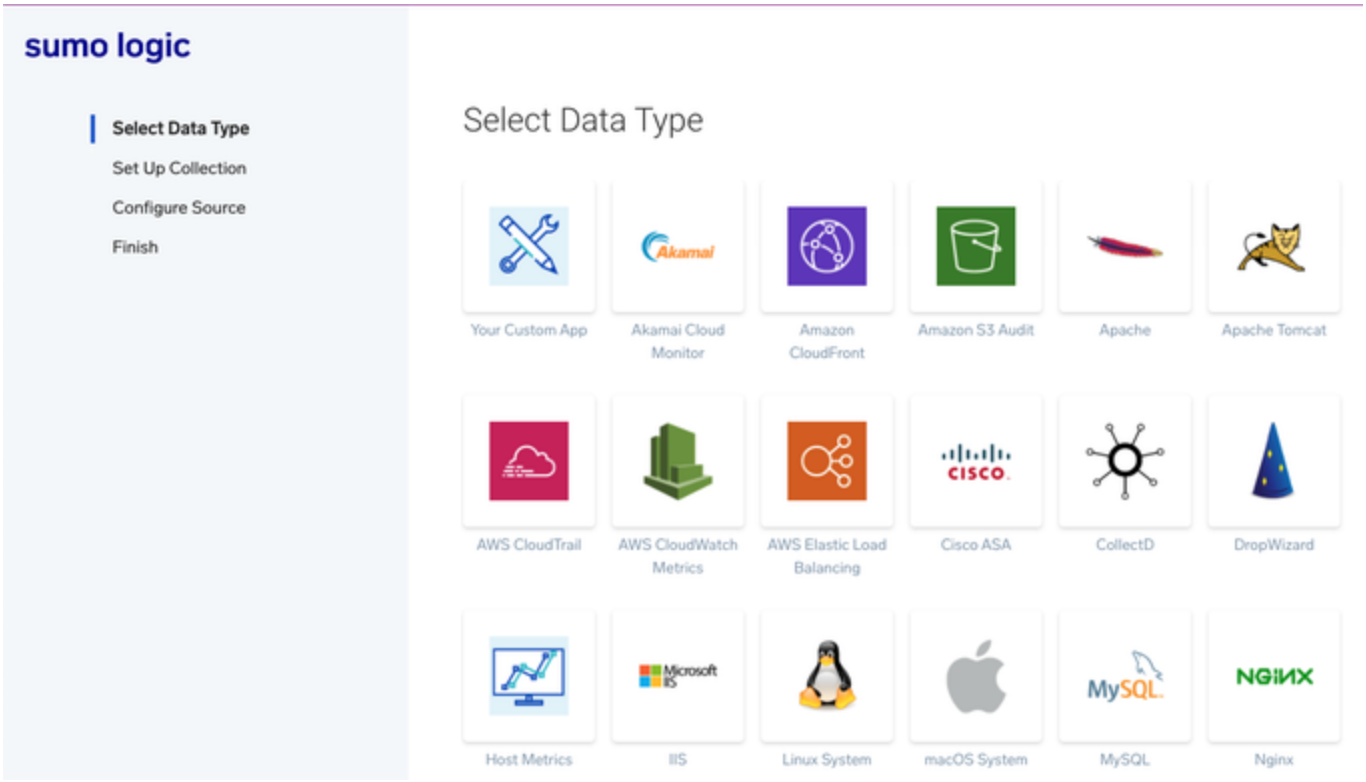
```
curl -v -X POST -T /path/to/your/logfile.log -H 'Content-Encoding:gzip'
https://endpoint4.collection.sumologic.com/receiver/v1/http
/ZaVnC4d****EAuUHJQ==
```

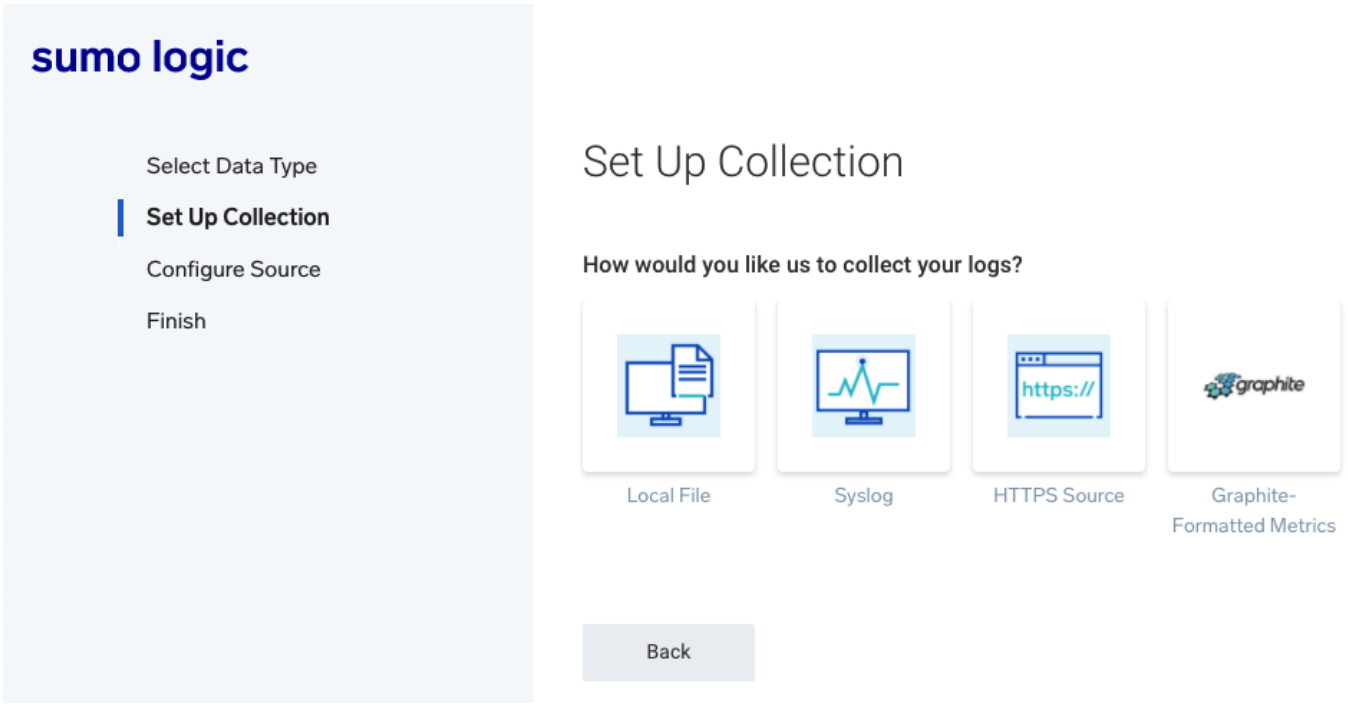
Setup process for setting up a SumoLogic HTTPS Collector for Lucidum

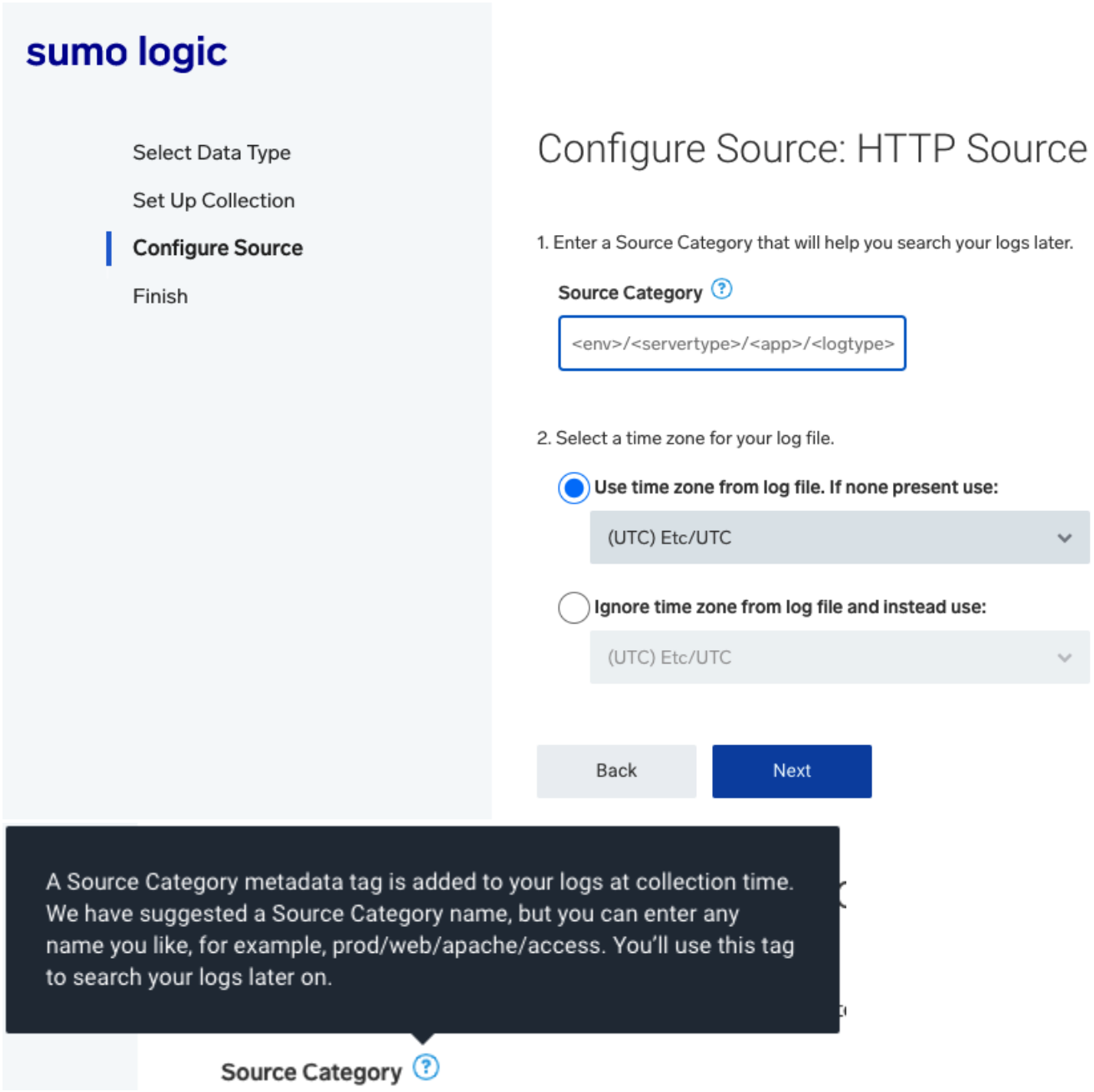
Select the data type “Your Custom App”. At some point, we can work with SumoLogic to add Lucidum to their Data Type tiles.

Customers may want to post different types of notifications/events to different HTTPS collector URLs.

The source category in this example is `/prod/appliance/lucidum/notifications` but it can be anything.


sumo logic
Select Data Type
Set Up Collection
Configure Source
Finish
Select Data Type
Your Custom App
Akamai Cloud Monitor
Amazon CloudFront
Amazon S3 Audit
Apache
Apache Tomcat
AWS CloudTrail
AWS CloudWatch Metrics
AWS Elastic Load Balancing
Cisco ASA
CollectD
DropWizard
Host Metrics
IIS
Linux System
macOS System
MySQL
Nginx


sumo logic
Select Data Type
Set Up Collection
Configure Source
Finish
Set Up Collection
How would you like us to collect your logs?
Local File
Syslog
HTTPS Source
Graphite-Formatted Metrics
Back



A Source Category metadata tag is added to your logs at collection time. We have suggested a Source Category name, but you can enter any name you like, for example, prod/web/apache/access. You'll use this tag to search your logs later on.

Source Category

sumo logic

- Select Data Type
- Set Up Collection
- **Configure Source**
- Finish

Configure Source: HTTP Source

1. Enter a Source Category that will help you search your logs later.

Source Category

/prod/appliance/lucidum/notifications

2. Select a time zone for your log file.

- (●) **Use time zone from log file. If none present use:**
  - (UTC) Etc/UTC
- ( ) **Ignore time zone from log file and instead use:**
  - (UTC) Etc/UTC

Back | Next

sumo logic

- Select Data Type
- Set Up Collection
- **Configure Source**
- Finish

Configure Source: HTTP Source

1. An HTTP Source has been automatically configured for you. Copy the following URL.

```
https://endpoint4.collection.sumologic.com/receiver/v1/http/ZaVnC4dhaV0DVmli0w_CAdev6_uRKLDXT1hoW7MQGYm497C2rFn1Z_5TOySsUE3xP5YGYJ1Jg-OotJyL96rNh8YW26YFqXuOsX4sQBSQ8abx9m9EAuUHJQ==
```

Copy

2. Use the URL as the target for your Source. Learn more
   > View cURL example

Back | Next

2. Use the URL as the target for your Source. Learn more

Hide cURL example

One way to send your logs to Sumo Logic with this URL is to use a cURL command. Enter the path to your logs into the Path field. This inserts the path into the cURL command. Then copy and paste either command option into your terminal.

Path

POST

```
curl -v -X POST -T /path/to/your/logfile.log https://endpoint4.collection.sumologic.com/receiver/v1/http/ZaVnC4dhaV0DVmli0w_CAdev6_uRKLDXT1hoW7MQGYm497C2rFn1Z_5TOySsUE3xP5YGYJ1Jg-OotJyL96rNh8YW26YFqXuOsX4sQBSQ8abx9m9EAuUHJQ==
```

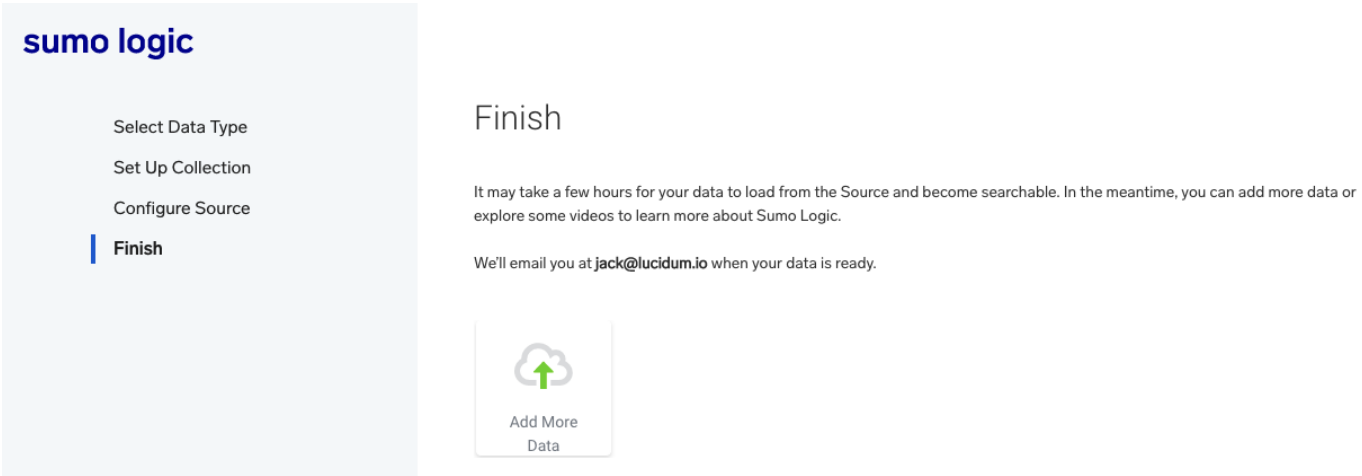
Copy

POST gzip Compressed Data

```
curl -v -X POST -T /path/to/your/logfile.log -H 'Content-Encoding:gzip' https://endpoint4.collection.sumologic.com/receiver/v1/http/ZaVnC4dhaV0DVmli0w_CAdev6_uRKLDXT1hoW7MQGYm497C2rFn1Z_5TOySsUE3xP5YGYJ1Jg-OotJyL96rNh8YW26YFqXuOsX4sQBSQ8abx9m9EAuUHJQ==
```

Copy

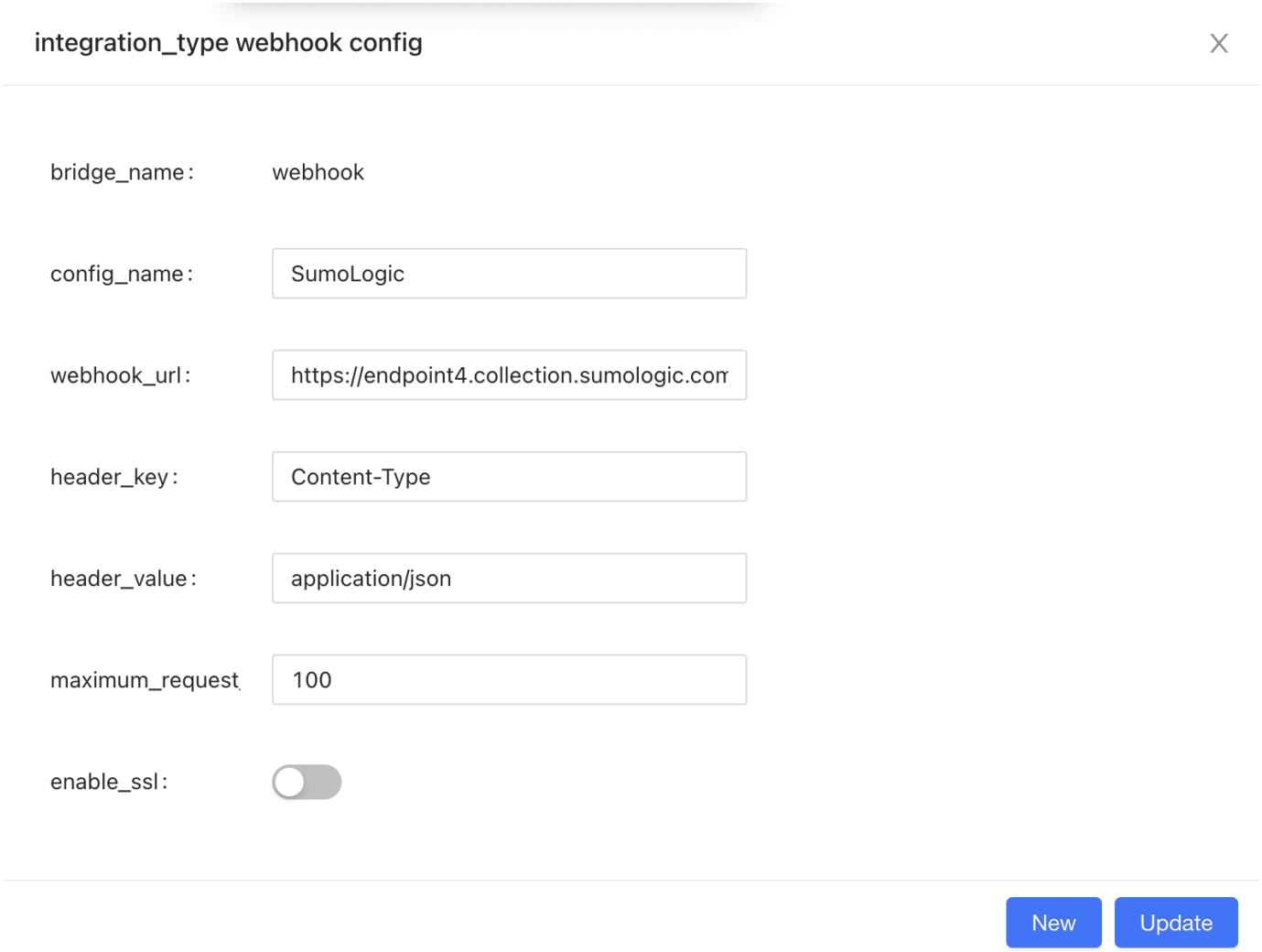
Back Next



Lucidum Setup

Create new Integration

Use the SumoLogic collector URL for the webhook_url.



Create new scheduled action using the Sumo integration

Choose schedule, filter, output fields, Sumo configuration name and then Save and Run.

Set Action

Choose Action — 2 Schedule Action — 3 Configure Action — 4 Preview

Schedule Type: Schedule

Hourly | Daily | Weekly | Monthly

Every 1 hour(s)

At 00 00

0 0 0/1 1/1 * ? *

Rules: Result Count | Greater Than | 0

Previous | Next

Set Action

Choose Action — Schedule Action — 3 Configure Action — 4 Preview

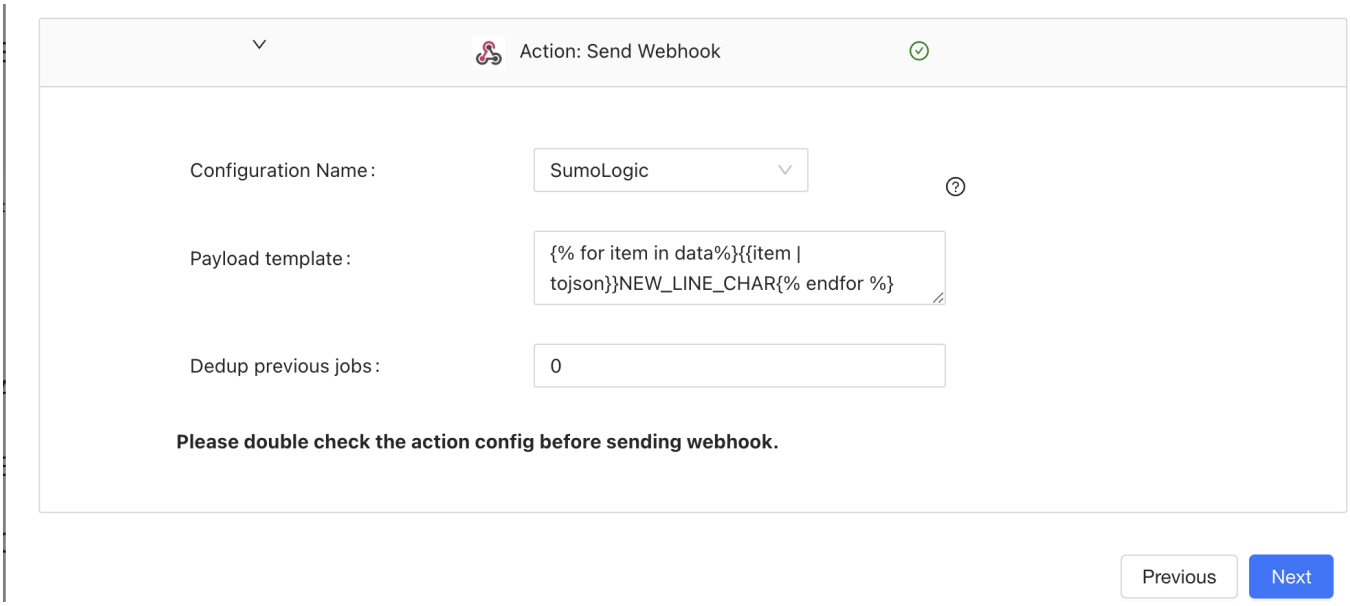
General Settings

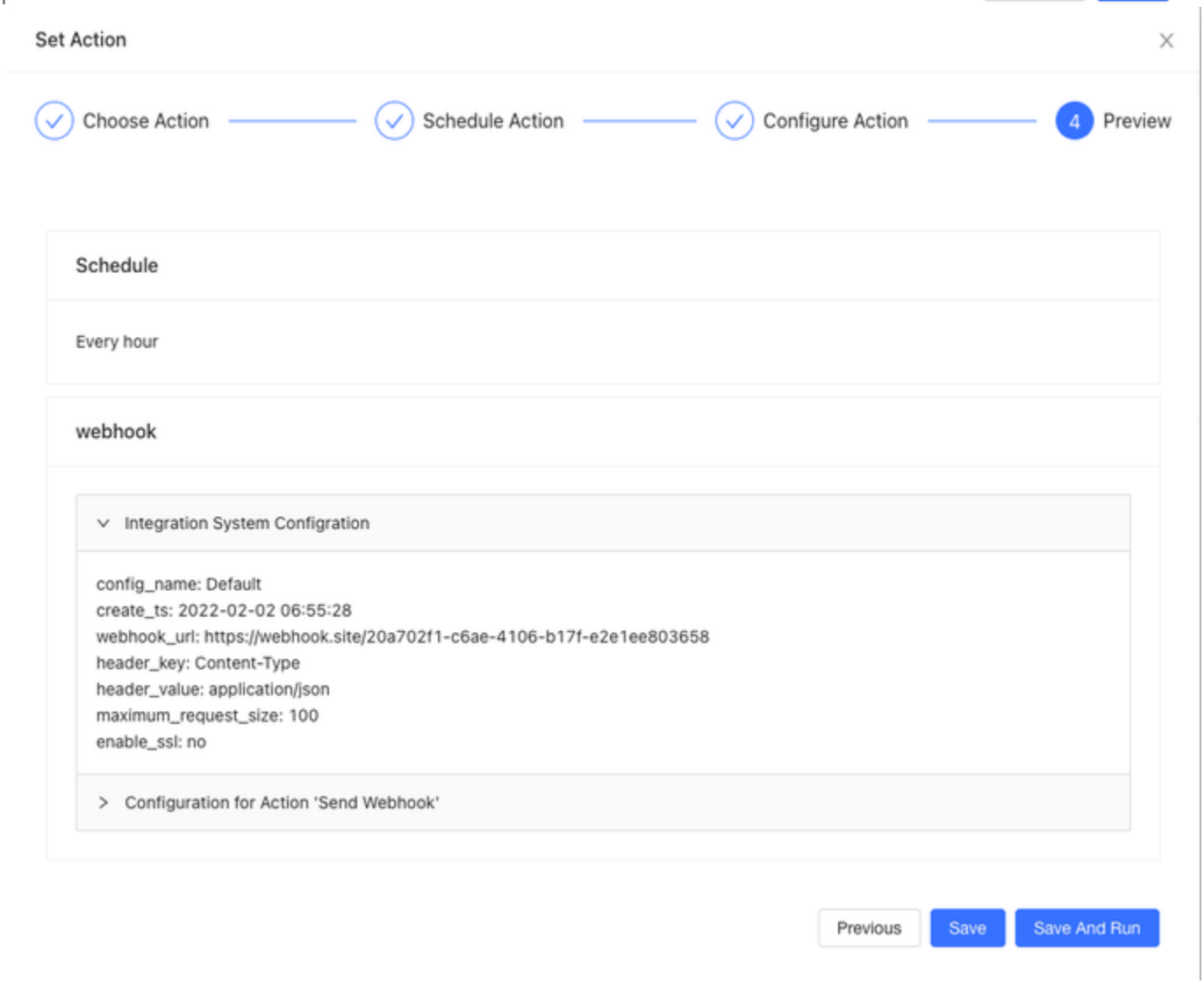
Query Filter: Asset exists

Edit filters

Output Fields: Asset × | First Time Seen × | Last Time Seen × | User Name × | IP Address × | OS and Version × | Serial Number × | MAC Address × | Data Sources × | Location × | Risk Factors × | External Ports × | Ports × | External Services × | Services × | Department × | Manager ×

Action: Send Webhook


Action: Send Webhook
Configuration Name:
SumoLogic
Payload template:
{% for item in data%}{{item | tojson}}NEW_LINE_CHAR{% endfor %}
Dedup previous jobs:
0
Please double check the action config before sending webhook.
Previous
Next


Set Action
Choose Action
Schedule Action
Configure Action
4
Preview
Schedule
Every hour
webhook
Integration System Configration
config_name: Default
create_ts: 2022-02-02 06:55:28
webhook_url: https://webhook.site/20a702f1-c6ae-4106-b17f-e2e1ee803658
header_key: Content-Type
header_value: application/json
maximum_request_size: 100
enable_ssl: no
Configuration for Action 'Send Webhook'
Previous
Save
Save And Run