Beyond Identity Events Data integration with Sumologic

1 Table of Contents

2 Introduction

2.1 About

This guide provides instructions on how to:

- Integrate BI events data with Sumologic

2.2 Prerequisites

Ensure that you have the following:

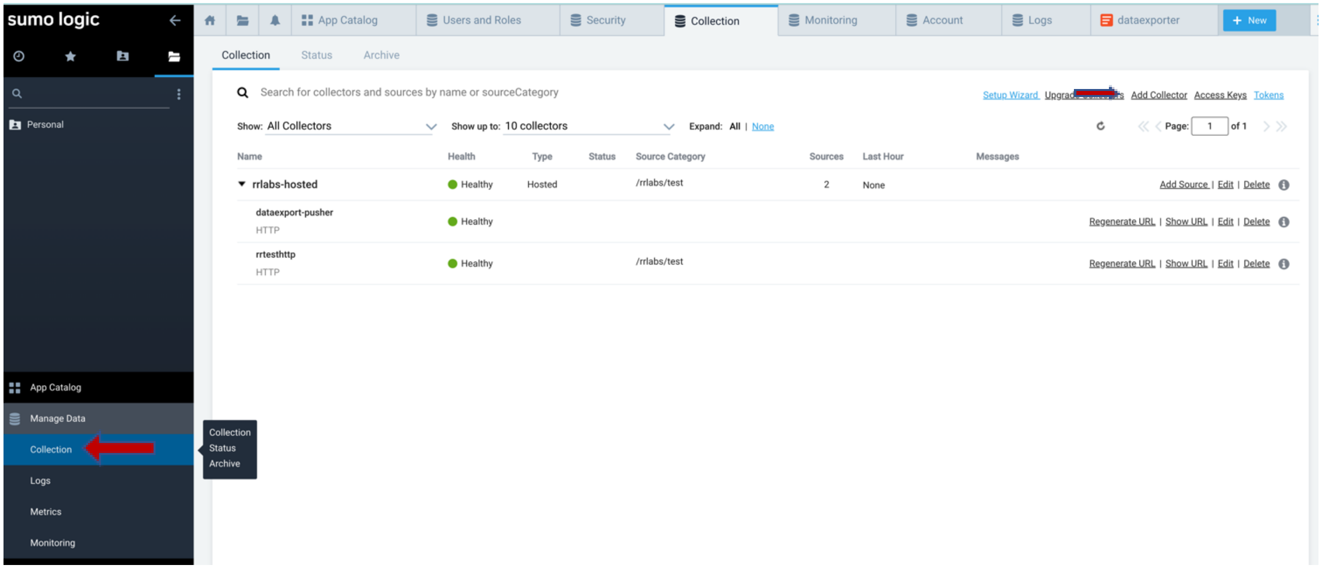
- You have a tenant configured for your organization and able to enroll users.

3 Sumologic configuration

- Create a Hosted Collector
- Add HTTP Log data source to hosted collector
  - Copy the HTTP source address . Provide this to BI SME.

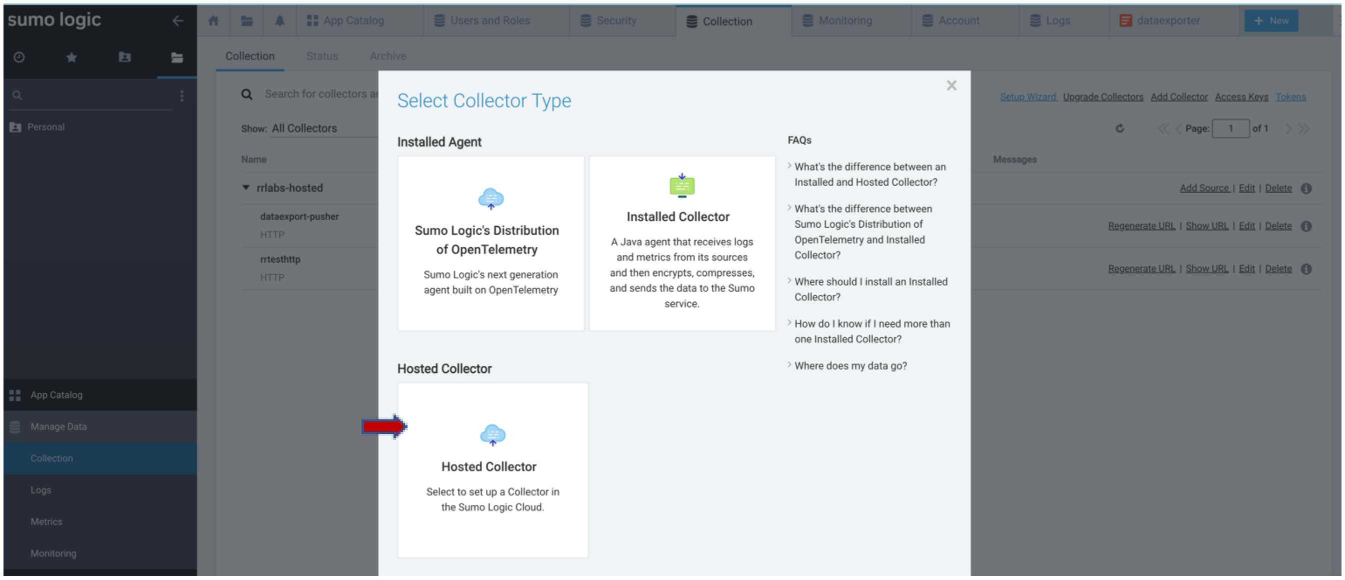
3.1 Create a Hosted Collector

Access your Sumologic tenant URL and login as a user with administrative privileges. In the dashboard, click “Collections” under “Manage Data”



Name	Health	Type	Status	Source Category	Sources	Last Hour	Messages	
rrlabs-hosted	Healthy	Hosted		/rrlabs/test	2	None		Add Source | Edit | Delete
dataexport-pusher HTTP	Healthy							Regenerate URL | Show URL | Edit | Delete
rrtesthttp HTTP	Healthy			/rrlabs/test				Regenerate URL | Show URL | Edit | Delete

On the right-hand side top menu, click "Add Collector". In the "Select Collector Type" screen, click on "Hosted Collector"


Select Collector Type

Installed Agent

Sumo Logic's Distribution of OpenTelemetry

Sumo Logic's next generation agent built on OpenTelemetry

Installed Collector

A Java agent that receives logs and metrics from its sources and then encrypts, compresses, and sends the data to the Sumo service.

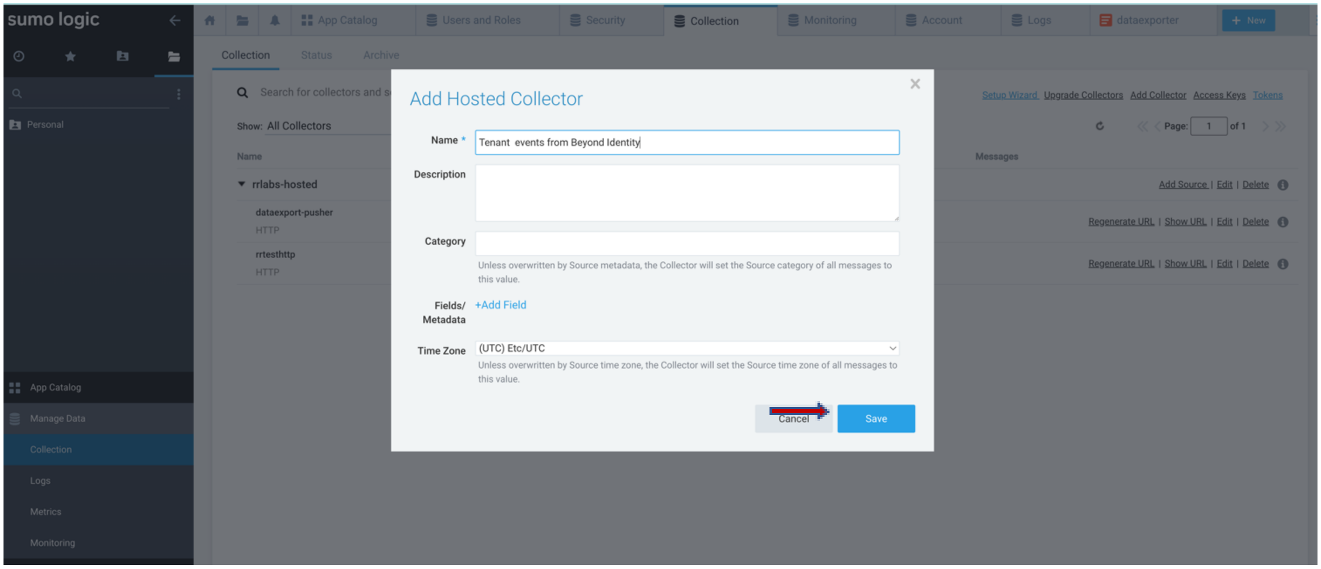
Hosted Collector

Hosted Collector

Select to set up a Collector in the Sumo Logic Cloud.

FAQs

- What's the difference between an Installed and Hosted Collector?
- What's the difference between Sumo Logic's Distribution of OpenTelemetry and Installed Collector?
- Where should I install an Installed Collector?
- How do I know if I need more than one Installed Collector?
- Where does my data go?



Add Hosted Collector

Name * Tenant events from Beyond Identity

Description

Category

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

Fields/ Metadata +Add Field

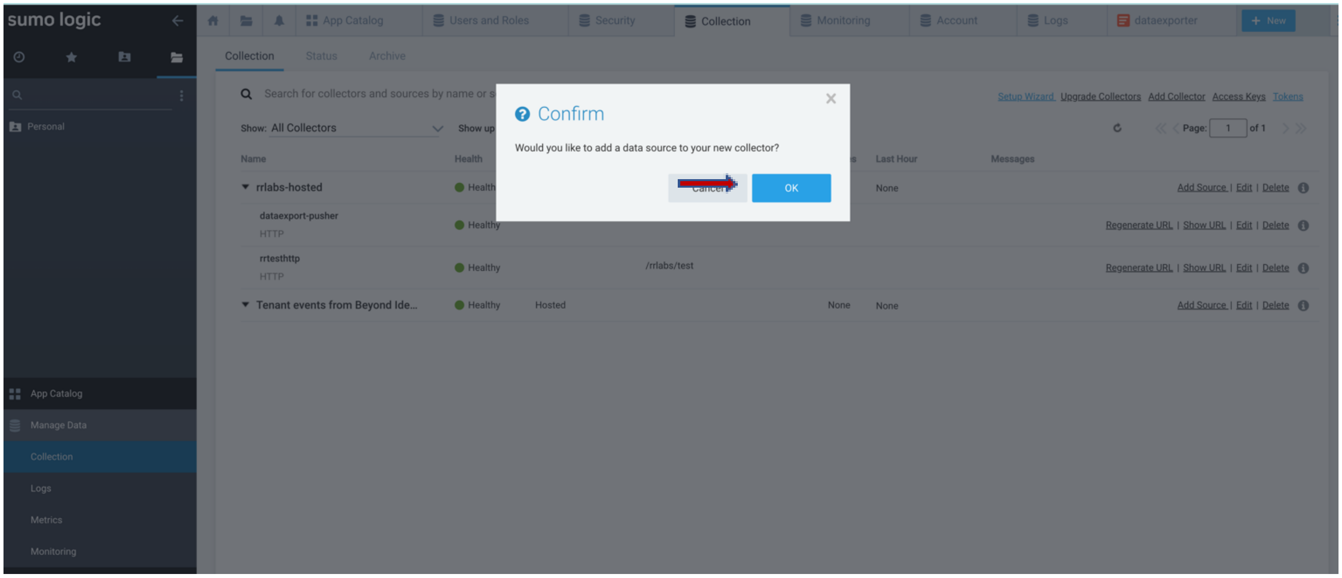
Time Zone (UTC) Etc/UTC

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

Type in a name for the Hosted collector, for example "*Tenant events from Beyond Identity*" and add a relevant description. Leave other fields to the default values. Click "Save"

3.2 Add HTTP Datasource

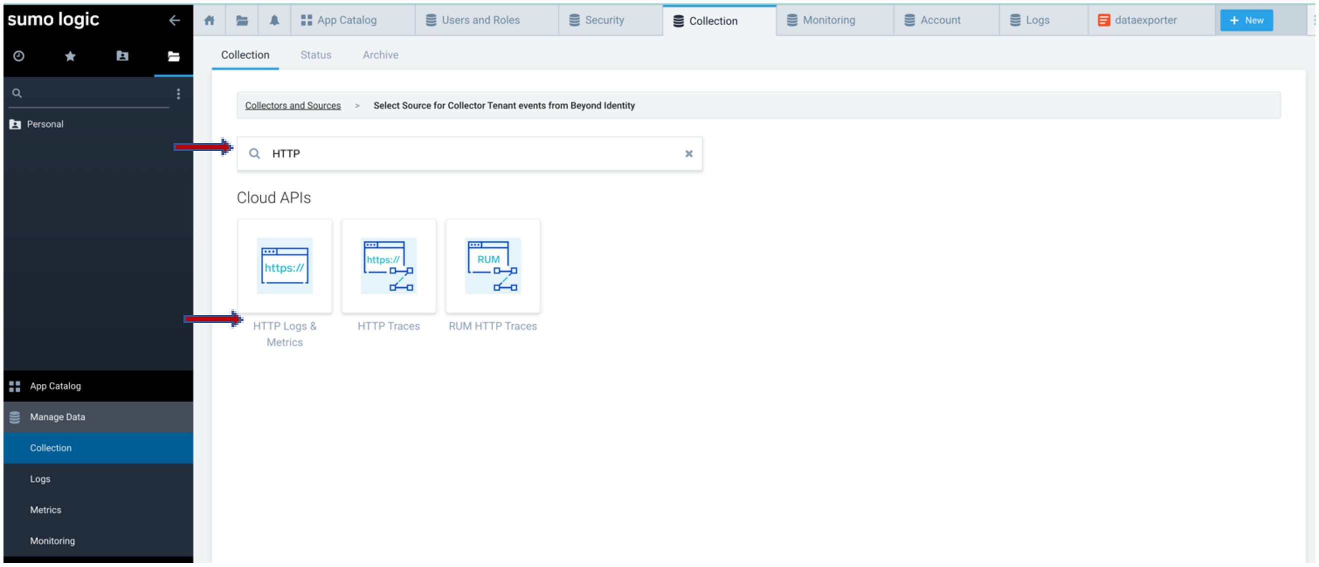
After clicking "Save", you will see the below "Confirm" pop-up to confirm adding a data source. Click "OK"



Confirm

Would you like to add a data source to your new collector?

Type "HTTP" in the search box as shown below. Click on "HTTP Logs & Metrics" in the search results.

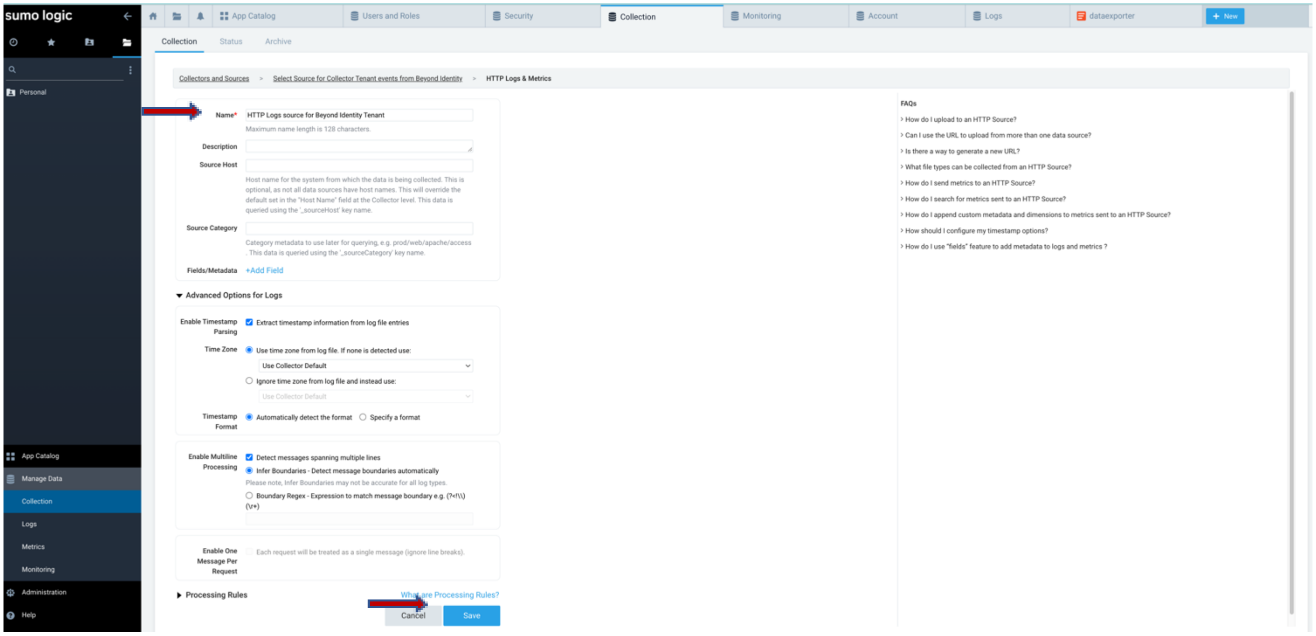


Collectors and Sources > Select Source for Collector Tenant events from Beyond Identity

HTTP

Cloud APIs

Type in "*HTTP Log source for Beyond Identity Tenant*" in the name field. Type in a relevant description in the description field. Leave other values to the defaults. Click "Save"



Collectors and Sources > Select Source for Collector Tenant events from Beyond Identity > HTTP Logs & Metrics

Name* HTTP Logs source for Beyond Identity Tenant
Maximum name length is 128 characters.

Description

Source Host
Host name for the system from which the data is being collected. This is optional, as not all data sources have host names. This will override the default set in the "Host Name" field at the Collector level. This data is queried using the '_sourceHost' key name.

Source Category
Category metadata to use later for querying, e.g. prod/web/apache/access . This data is queried using the '_sourceCategory' key name.

Fields/Metadata

Advanced Options for Logs

Enable Timestamp Parsing ☑ Extract timestamp information from log file entries

Time Zone ● Use time zone from log file. If none is detected use:
Use Collector Default
○ Ignore time zone from log file and instead use:
Use Collector Default

Timestamp Format ● Automatically detect the format ○ Specify a format

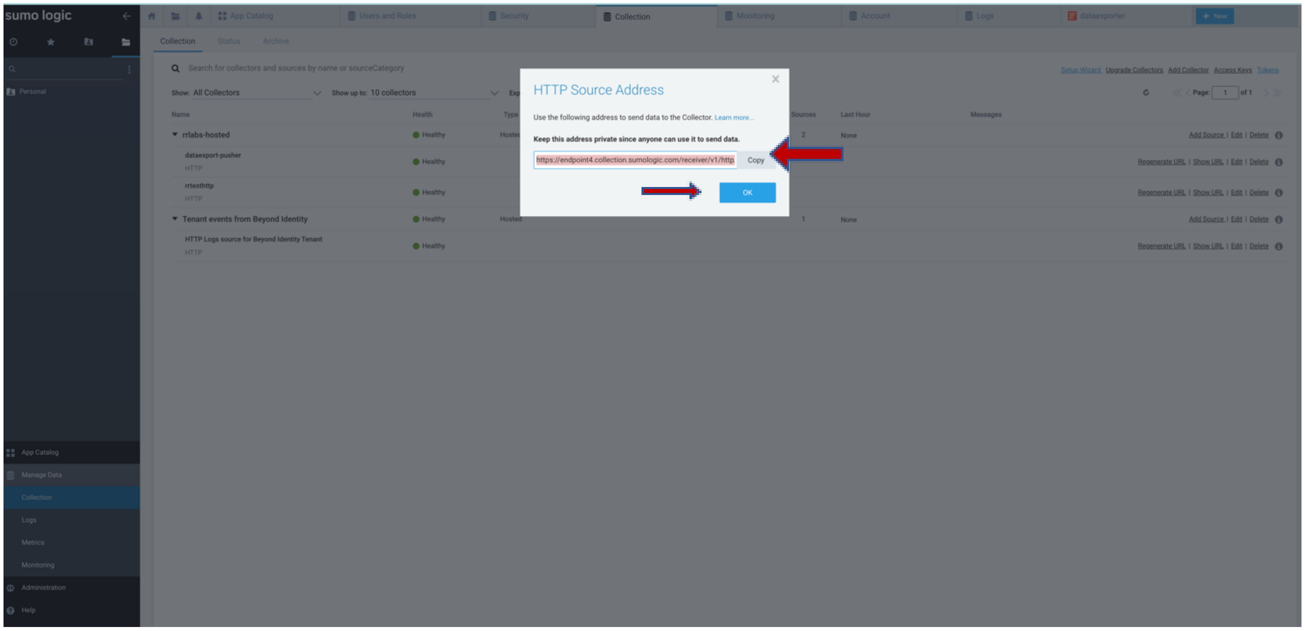
Enable Multiline Processing ☑ Detect messages spanning multiple lines
● Infer Boundaries - Detect message boundaries automatically
Please note, Infer Boundaries may not be accurate for all log types.
○ Boundary Regex - Expression to match message boundary e.g. (?<!\\)(\r+)

Enable One Message Per Request □ Each request will be treated as a single message (ignore line breaks).

Processing Rules

FAQs
- How do I upload to an HTTP Source?
- Can I use the URL to upload from more than one data source?
- Is there a way to generate a new URL?
- What file types can be collected from an HTTP Source?
- How do I send metrics to an HTTP Source?
- How do I search for metrics sent to an HTTP Source?
- How do I append custom metadata and dimensions to metrics sent to an HTTP Source?
- How should I configure my timestamp options?
- How do I use "fields" feature to add metadata to logs and metrics ?

You will see a pop-up screen showing "HTTP Source Address". Click "Copy" to copy the address and provide it to BI SME. Click "OK"



Show: All Collectors Show up to: 10 collectors

Name	Health	Type	Sources	Last Hour	Messages	
rrlabs-hosted	Healthy	Hosted	2	None		Add Source | Edit | Delete
dataexport-pusher HTTP	Healthy					Regenerate URL | Show URL | Edit | Delete
rrtesthttp HTTP	Healthy					Regenerate URL | Show URL | Edit | Delete
Tenant events from Beyond Identity	Healthy	Hosted	1	None		Add Source | Edit | Delete
HTTP Logs source for Beyond Identity Tenant HTTP	Healthy					Regenerate URL | Show URL | Edit | Delete

HTTP Source Address

Use the following address to send data to the Collector. Learn more...

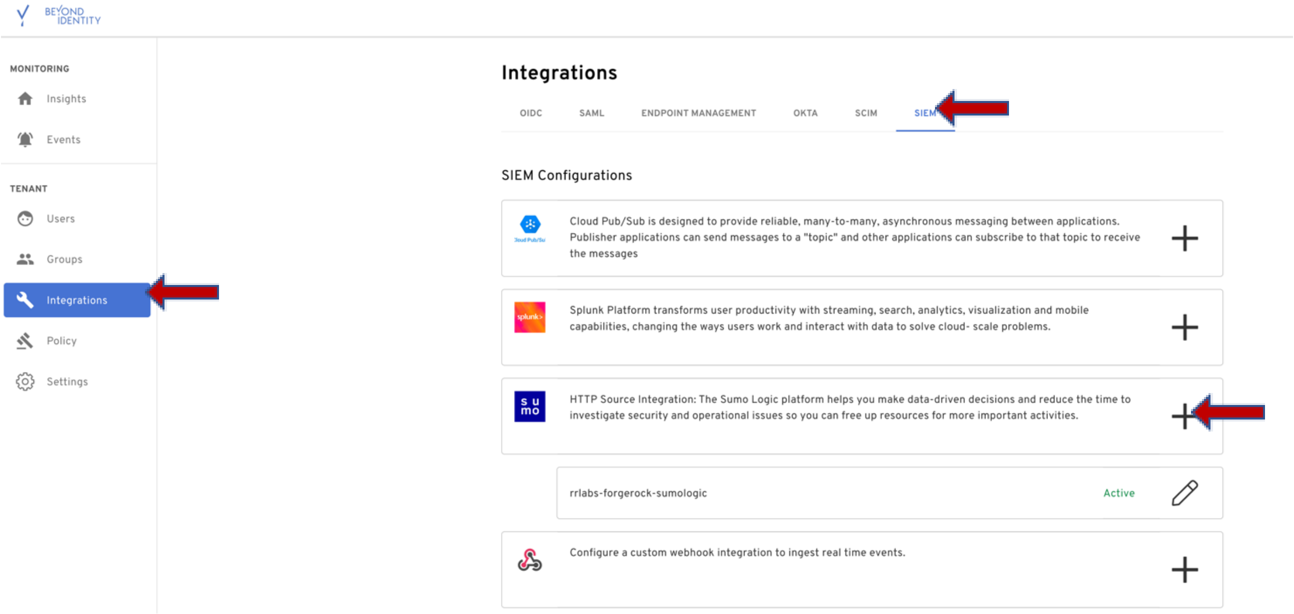
Keep this address private since anyone can use it to send data.

https://endpoint4.collection.sumologic.com/receiver/v1/http Copy

OK

4 Beyond Identity Configuration

The configuration is done using the BI admin console. Access BI admin console through your SSO integration. Click on "Integrations" and click on "SIEM"



Integrations

SIEM Configurations

Cloud Pub/Sub is designed to provide reliable, many-to-many, asynchronous messaging between applications. Publisher applications can send messages to a "topic" and other applications can subscribe to that topic to receive the messages +

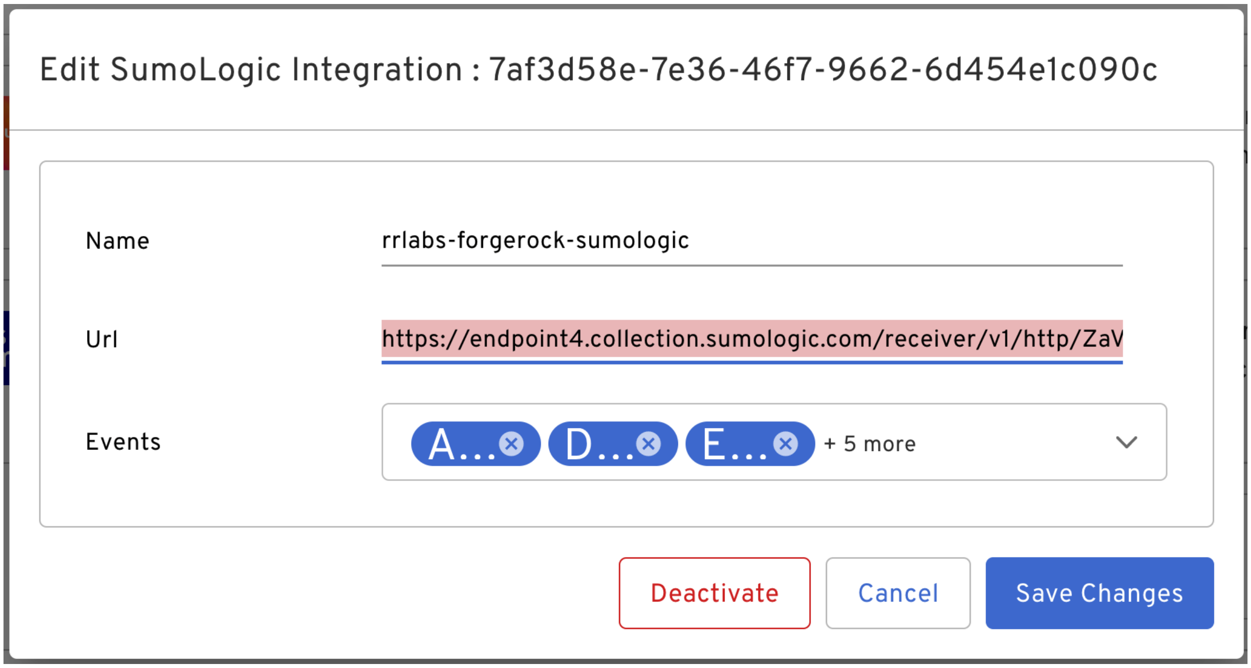
Splunk Platform transforms user productivity with streaming, search, analytics, visualization and mobile capabilities, changing the ways users work and interact with data to solve cloud- scale problems. +

HTTP Source Integration: The Sumo Logic platform helps you make data-driven decisions and reduce the time to investigate security and operational issues so you can free up resources for more important activities. +

rrlabs-forgerock-sumologic Active

Configure a custom webhook integration to ingest real time events. +

Click on the "+" sign next to Sumo. Using HTTP source address copied in section 3.2 fill out the value for Url. Provide a name for the configuration. From the events drop down, "select all" events or one the events you are interested in.



Edit SumoLogic Integration : 7af3d58e-7e36-46f7-9662-6d454e1c090c

Name: rrlabs-forgerock-sumologic

Url: https://endpoint4.collection.sumologic.com/receiver/v1/http/ZaV

Events: A… D… E… + 5 more

Once SIEM configuration is complete in BI admin console, you will be able to see the events in your Sumologic. You can verify with a search in Sumologic, for example

((_collector="*Tenant events from Beyond Identity* "))
AND _source = " *HTTP Log source for Beyond Identity Tenant* "
| sort by event_type

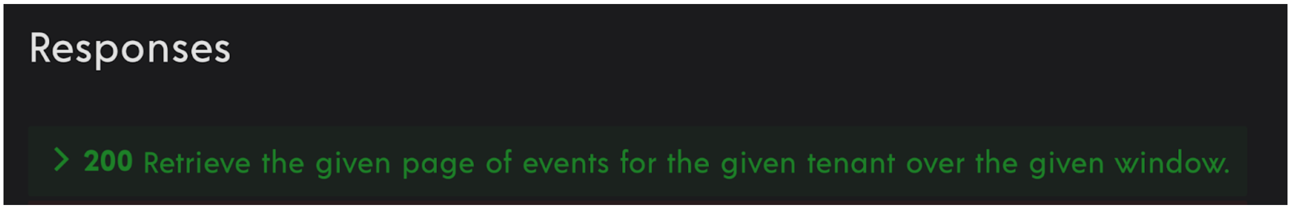
Replace the collector name and HTTP source name with the ones you created

5 Appendix

How to get event types?

Click on https://developer.beyondidentity.com/api/v0#tag/Events/operation/getEvents

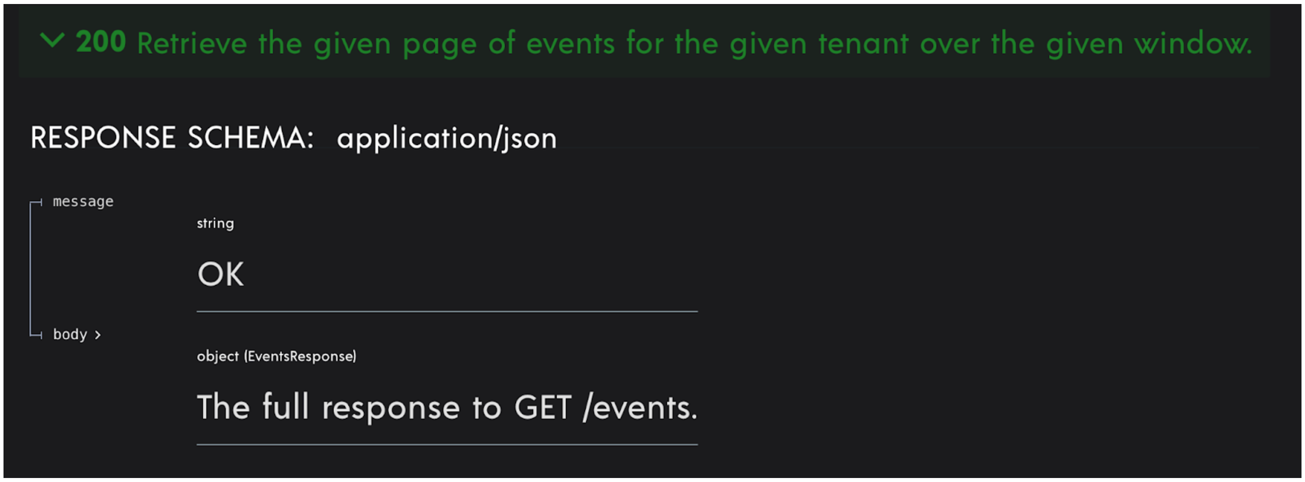
Scroll down



Responses

200 Retrieve the given page of events for the given tenant over the given window.

Click on arrow next to 200



200 Retrieve the given page of events for the given tenant over the given window.

RESPONSE SCHEMA: application/json

message

string

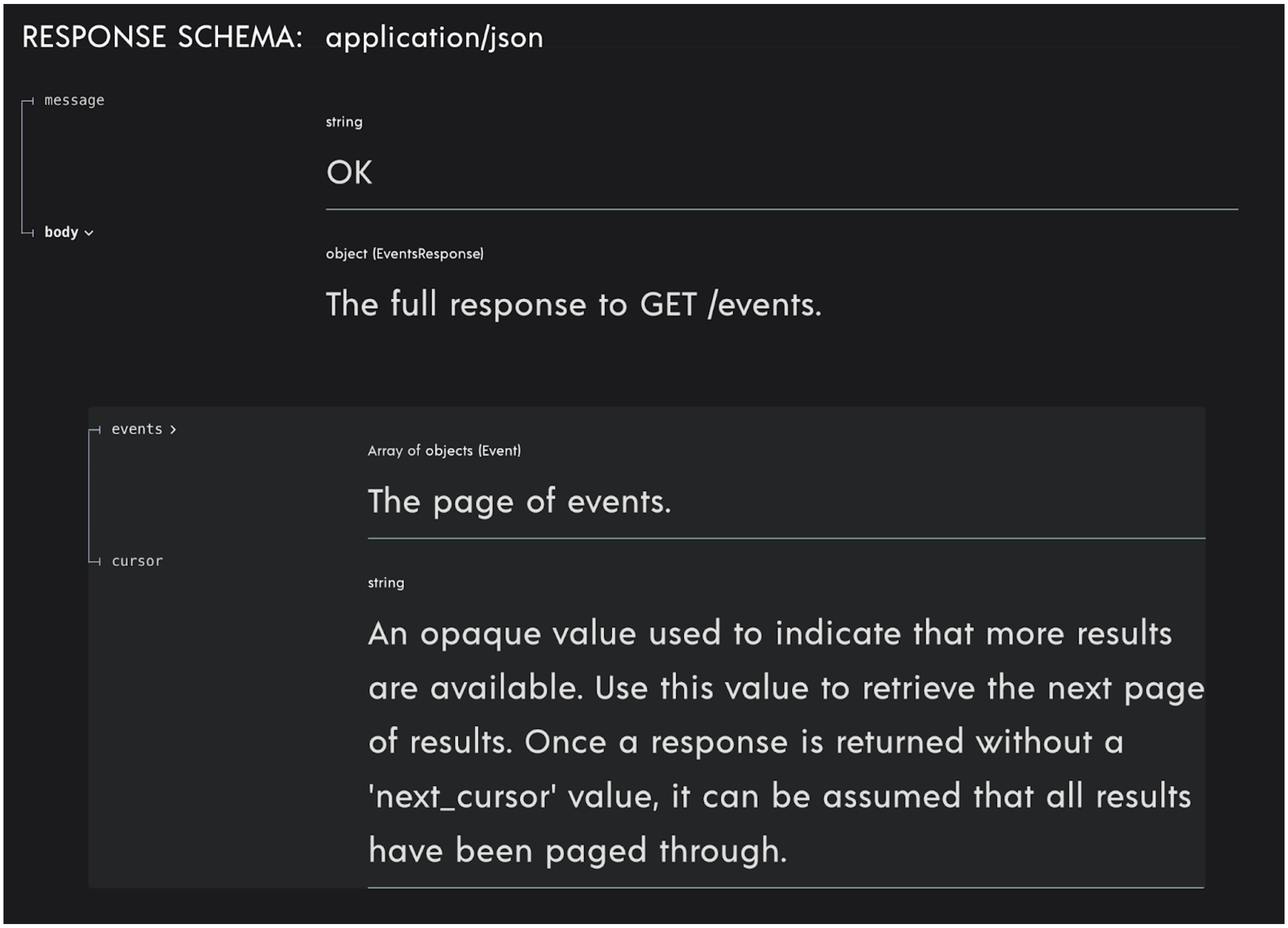
OK

body ›

object (EventsResponse)

The full response to GET /events.

Click on body



RESPONSE SCHEMA: application/json

message

string

OK

body ⌄

object (EventsResponse)

The full response to GET /events.

events ›

Array of objects (Event)

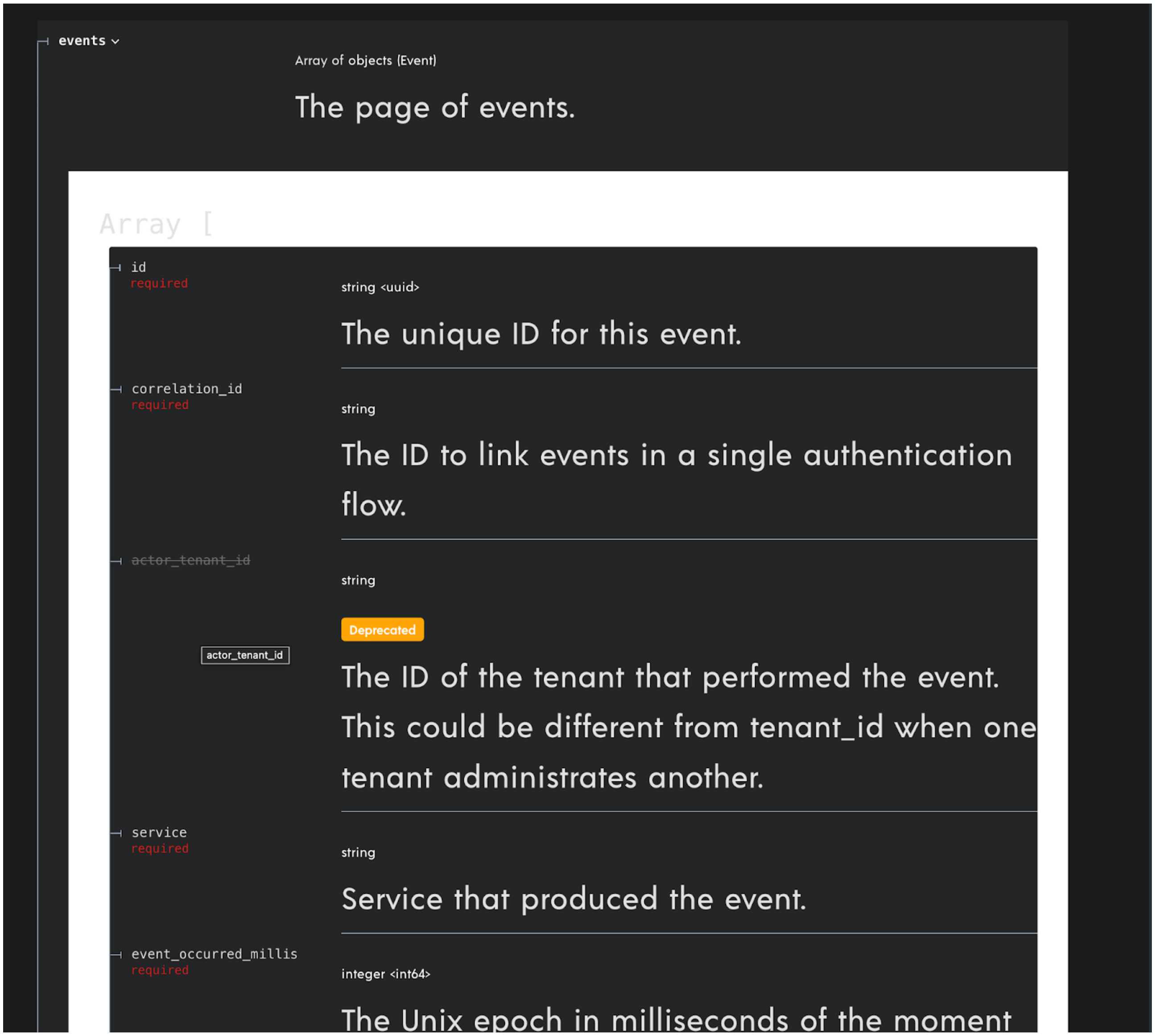
The page of events.

cursor

string

An opaque value used to indicate that more results are available. Use this value to retrieve the next page of results. Once a response is returned without a 'next_cursor' value, it can be assumed that all results have been paged through.

Click on events



events

Array of objects (Event)

The page of events.

Array [

id
required

string <uuid>

The unique ID for this event.

correlation_id
required

string

The ID to link events in a single authentication flow.

~~actor_tenant_id~~

string

The ID of the tenant that performed the event. This could be different from tenant_id when one tenant administrates another.

service
required

string

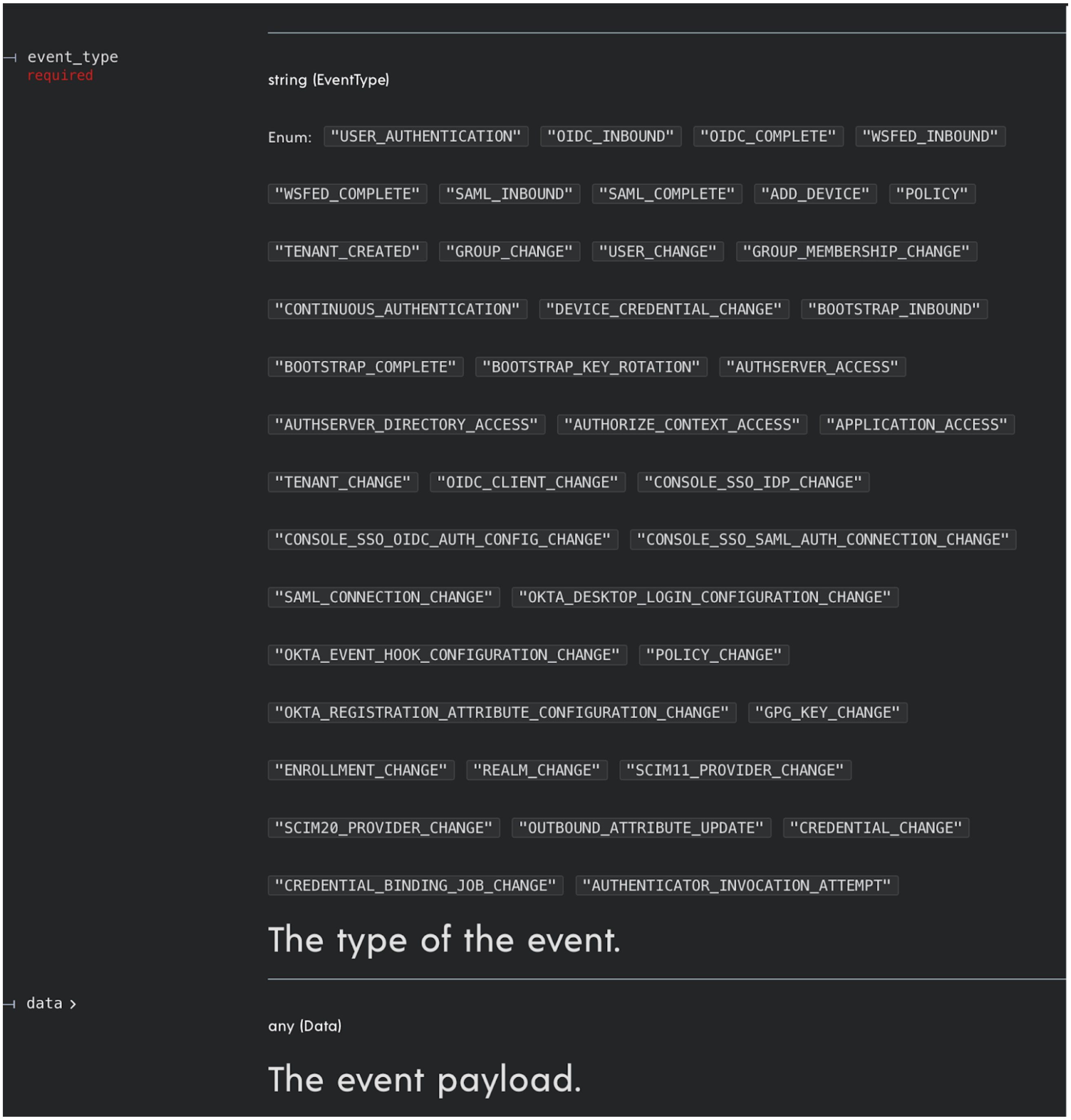
Service that produced the event.

event_occurred_millis
required

integer <int64>

The Unix epoch in milliseconds of the moment

Scroll down



event_type
required

string (EventType)

Enum: "USER_AUTHENTICATION" "OIDC_INBOUND" "OIDC_COMPLETE" "WSFED_INBOUND" "WSFED_COMPLETE" "SAML_INBOUND" "SAML_COMPLETE" "ADD_DEVICE" "POLICY" "TENANT_CREATED" "GROUP_CHANGE" "USER_CHANGE" "GROUP_MEMBERSHIP_CHANGE" "CONTINUOUS_AUTHENTICATION" "DEVICE_CREDENTIAL_CHANGE" "BOOTSTRAP_INBOUND" "BOOTSTRAP_COMPLETE" "BOOTSTRAP_KEY_ROTATION" "AUTHSERVER_ACCESS" "AUTHSERVER_DIRECTORY_ACCESS" "AUTHORIZE_CONTEXT_ACCESS" "APPLICATION_ACCESS" "TENANT_CHANGE" "OIDC_CLIENT_CHANGE" "CONSOLE_SSO_IDP_CHANGE" "CONSOLE_SSO_OIDC_AUTH_CONFIG_CHANGE" "CONSOLE_SSO_SAML_AUTH_CONNECTION_CHANGE" "SAML_CONNECTION_CHANGE" "OKTA_DESKTOP_LOGIN_CONFIGURATION_CHANGE" "OKTA_EVENT_HOOK_CONFIGURATION_CHANGE" "POLICY_CHANGE" "OKTA_REGISTRATION_ATTRIBUTE_CONFIGURATION_CHANGE" "GPG_KEY_CHANGE" "ENROLLMENT_CHANGE" "REALM_CHANGE" "SCIM11_PROVIDER_CHANGE" "SCIM20_PROVIDER_CHANGE" "OUTBOUND_ATTRIBUTE_UPDATE" "CREDENTIAL_CHANGE" "CREDENTIAL_BINDING_JOB_CHANGE" "AUTHENTICATOR_INVOCATION_ATTEMPT"

The type of the event.

data ›

any (Data)

The event payload.

event_type lists all the events