Beyond Identity Events Data integration with Datadog

Table of Contents

1 Introduction

1.1 About

This guide provides instructions on how to:

- Integrate BI events data with Datadog. Datadog only supports events push.

1.2 Prerequisites

Ensure that you have the following:

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

- You have a Datadog account with admin privileges

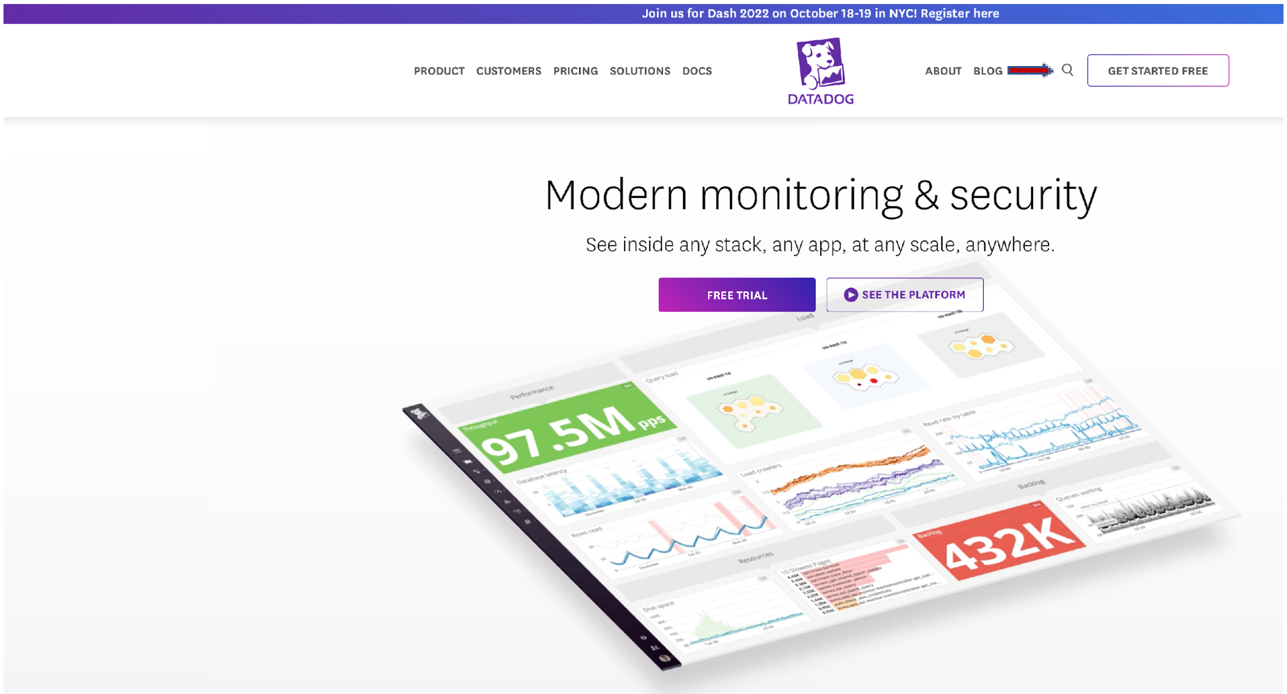
2 Datadog configuration

- Datadog account

- Datadog API key

2.1 Datadog account

You need a Datadog account that allows you to post log data. You can start free by accessing https://www.datadoghq.com and click on “GET STARTED FREE”

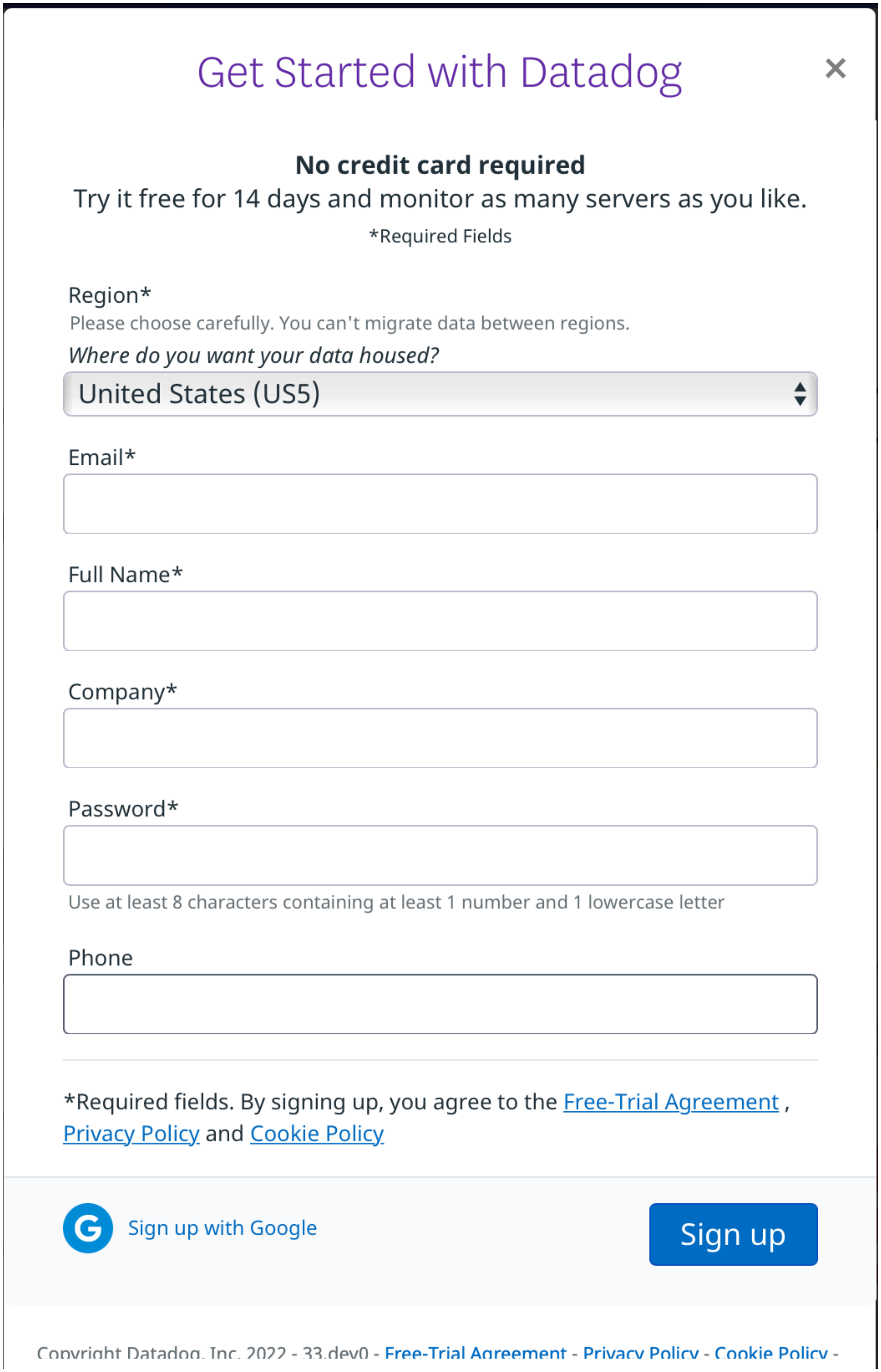


Join us for Dash 2022 on October 18-19 in NYC! Register here

Modern monitoring & security

See inside any stack, any app, at any scale, anywhere.

Fill up a similar form as below to get a free account



Get Started with Datadog

No credit card required

Try it free for 14 days and monitor as many servers as you like.

*Required Fields

Region*

Please choose carefully. You can't migrate data between regions.

Where do you want your data housed?

United States (US5)

Email*

Full Name*

Company*

Password*

Use at least 8 characters containing at least 1 number and 1 lowercase letter

Phone

*Required fields. By signing up, you agree to the Free-Trial Agreement , Privacy Policy and Cookie Policy

Copyright Datadog, Inc. 2022 - 33.dev0 - Free-Trial Agreement - Privacy Policy - Cookie Policy -

The Datadog API endpoint for posting logs will be used to post BI tenant events. The endpoint is https://http-intake.logs.datadoghq.com/api/v2/logs

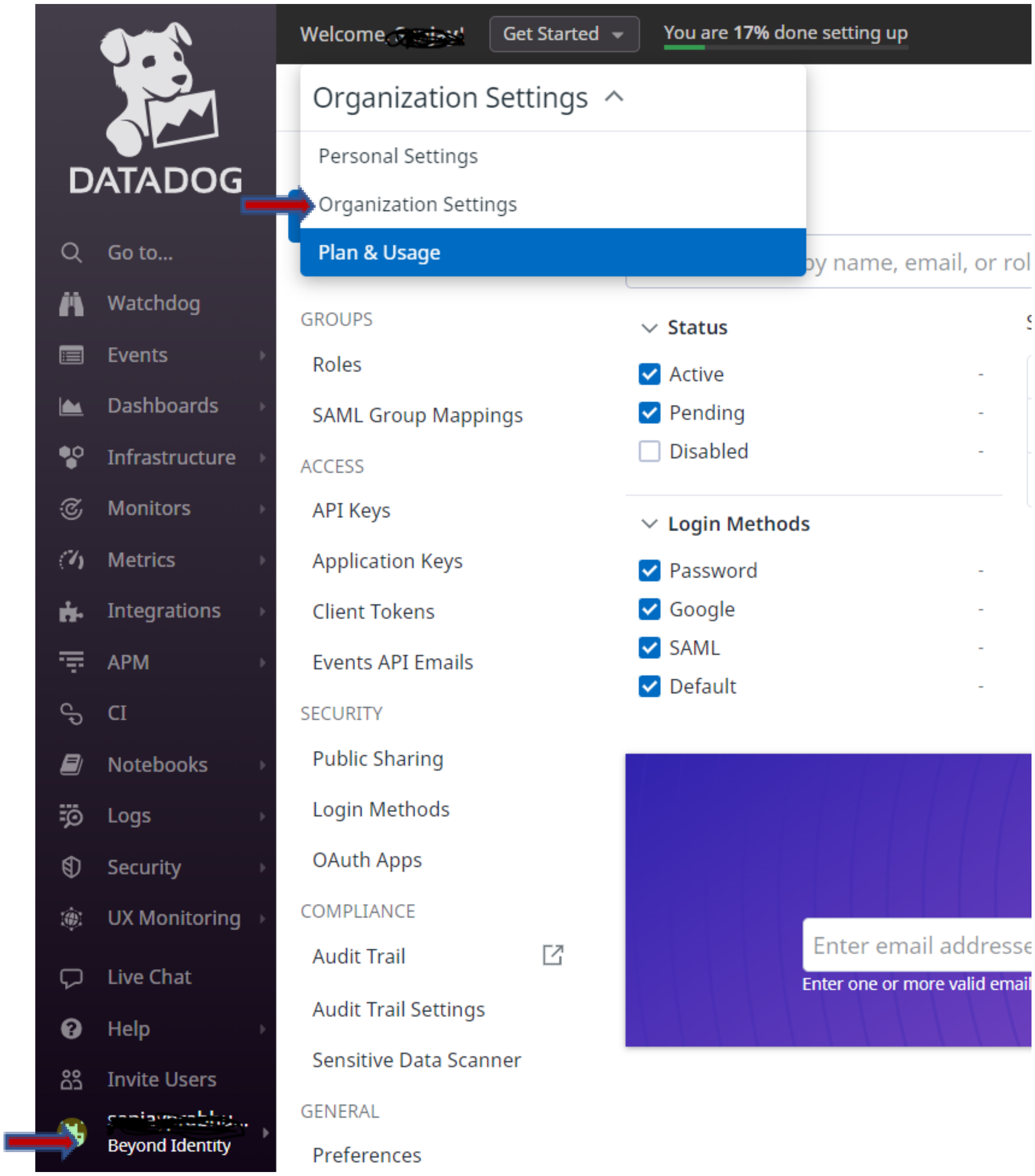
2.2 Datadog API key

The Datadog API key is required by Beyond Identity to post the tenant events into the datadog log aggregator.

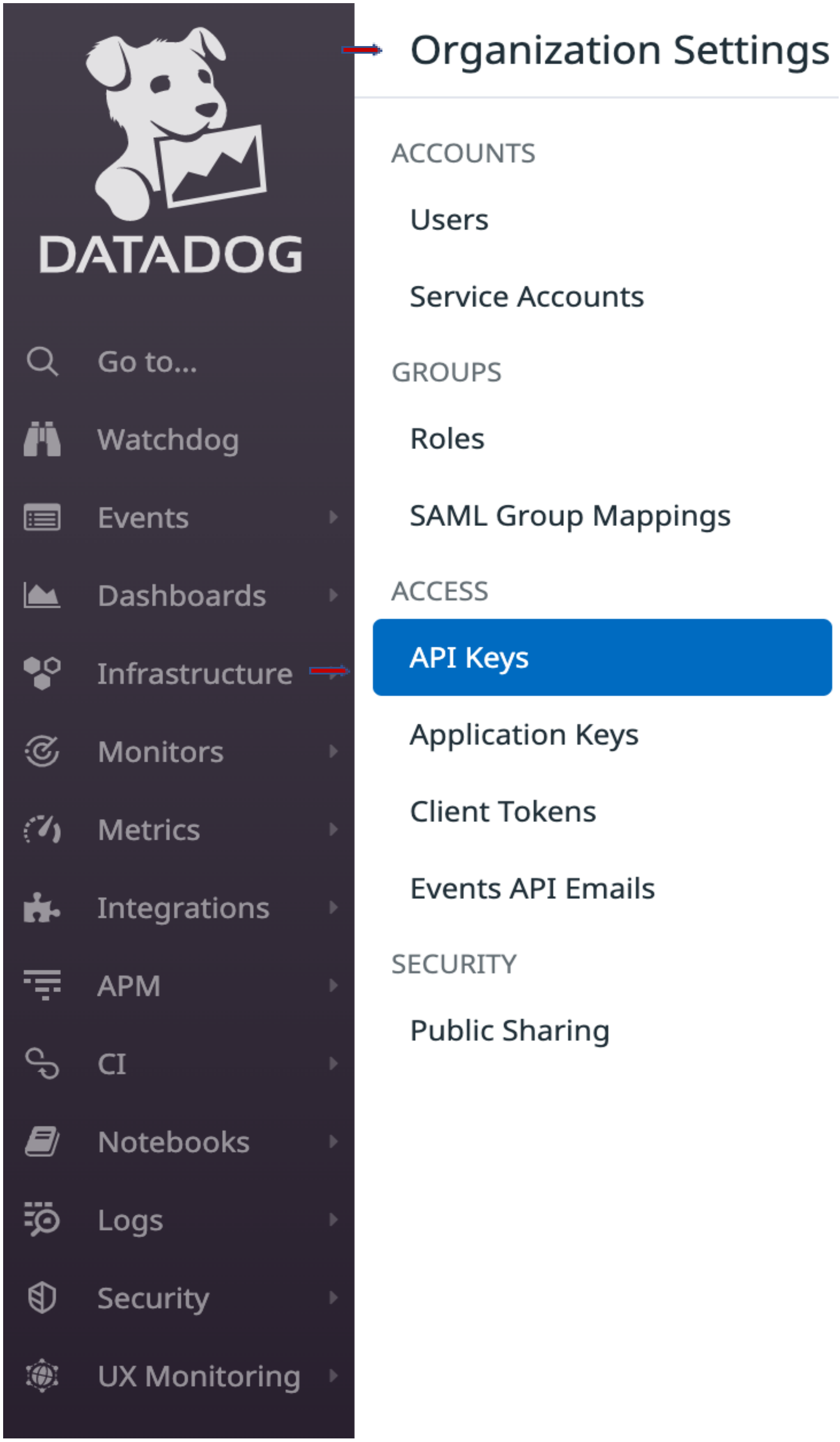
If you have an existing Datadog account, the API keys can be seen or generated by accessing Organization Settings in DataDog web console

For the Beyond Identity SIEM event collection , please create a new API. Please follow the below steps

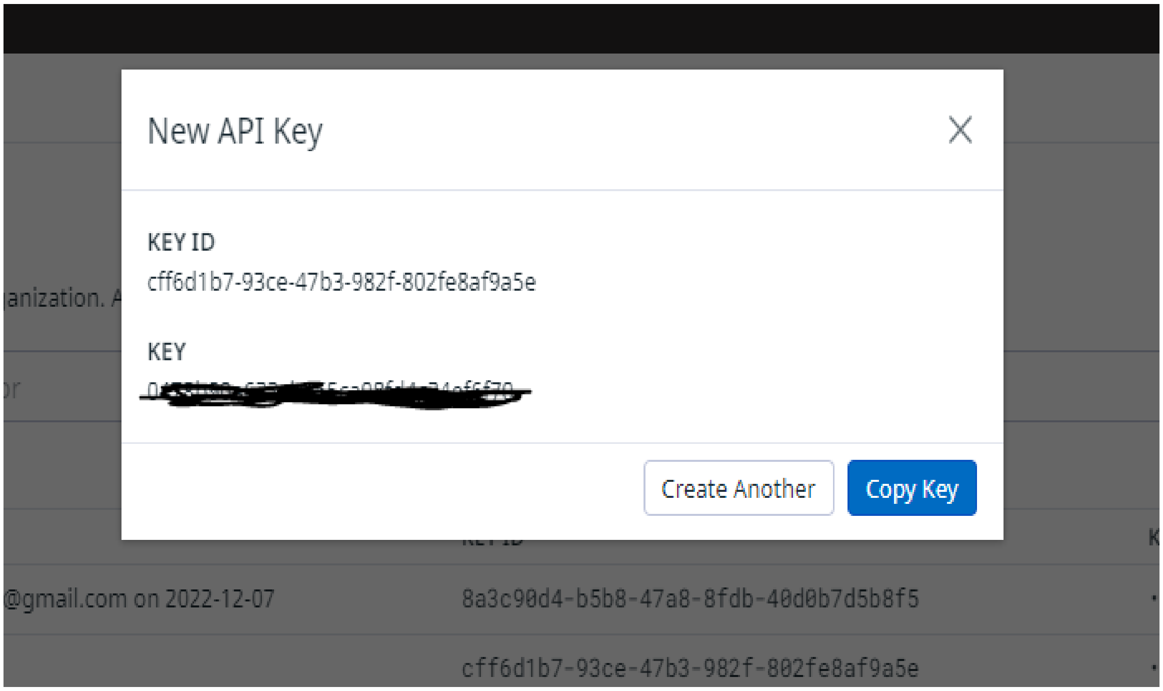
Navigate to your Account Profile and choose Organization Settings



Click on API Keys and choose add a new key by giving a name



Please copy the value of the newly created key which will be used in the next step for the SIEM integration in the Beyond Identity console



KEY ID
cff6d1b7-93ce-47b3-982f-802fe8af9a5e

KEY
[redacted]

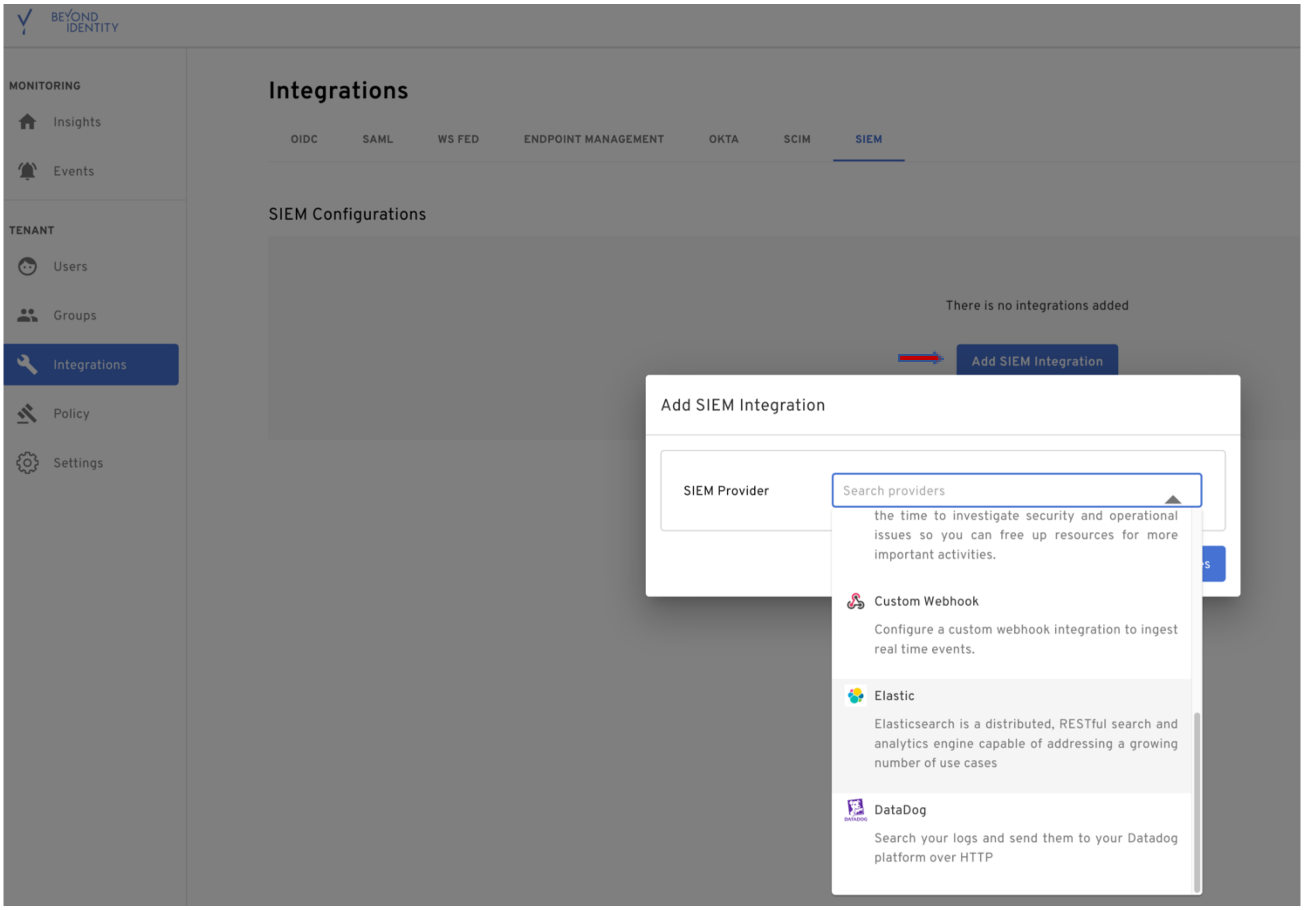
anization. A

@gmail.com on 2022-12-07 8a3c90d4-b5b8-47a8-8fdb-40d0b7d5b8f5

cff6d1b7-93ce-47b3-982f-802fe8af9a5e

3 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”. Under “SIEM Configurations”, click on “Add SIEM integration”. In “SIEM Provider” drop down, choose DataDog



There is no integrations added

the time to investigate security and operational issues so you can free up resources for more important activities.

Custom Webhook

Configure a custom webhook integration to ingest real time events.

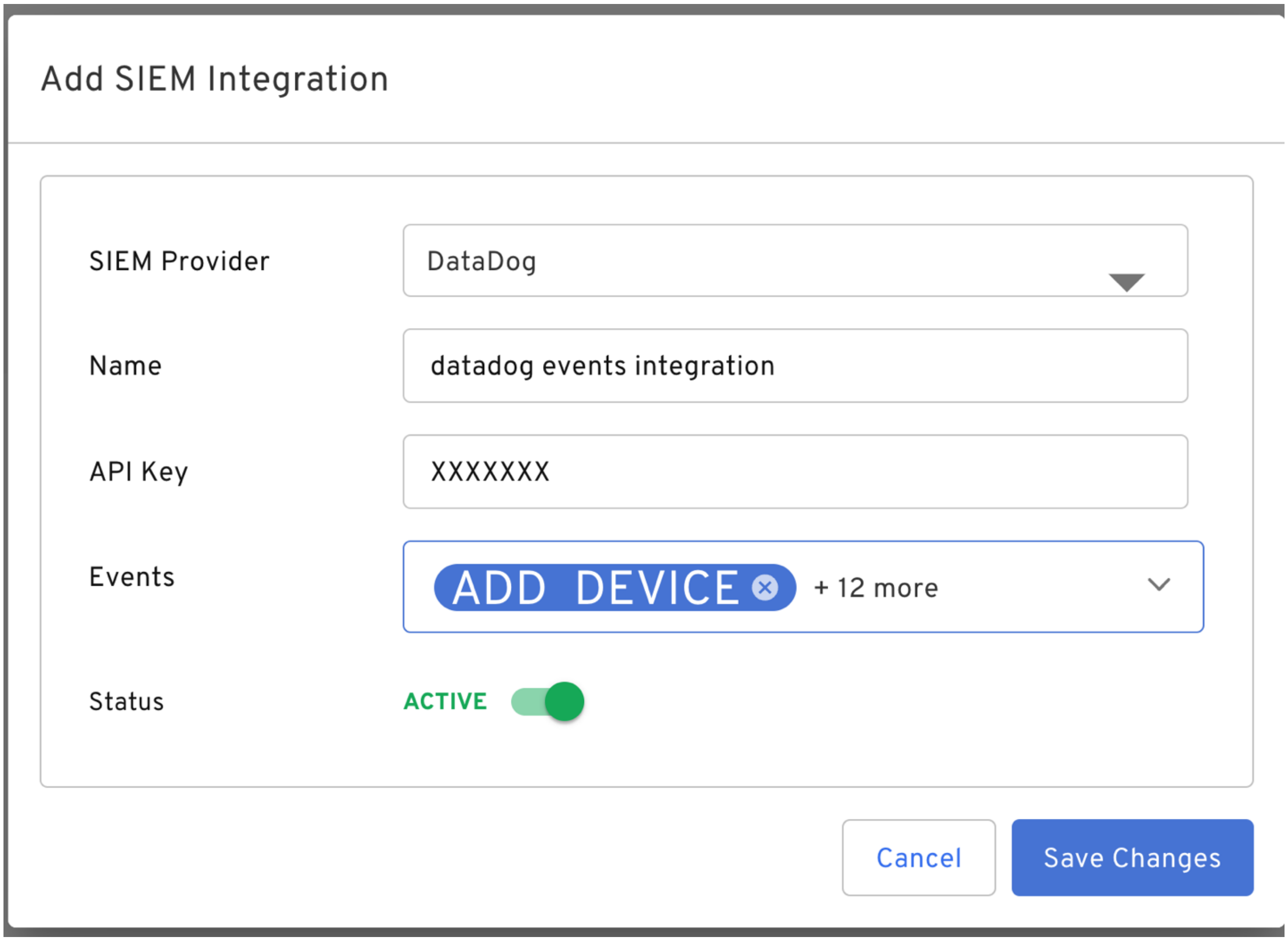
Elastic

Elasticsearch is a distributed, RESTful search and analytics engine capable of addressing a growing number of use cases

DataDog

Search your logs and send them to your Datadog platform over HTTP

The API key is obtained from DataDog deployment. Provide a name for the configuration. From the events drop down, “select all” events or one the events you are interested in.



Add SIEM Integration

SIEM Provider: DataDog

Name: datadog events integration

API Key: XXXXXXX

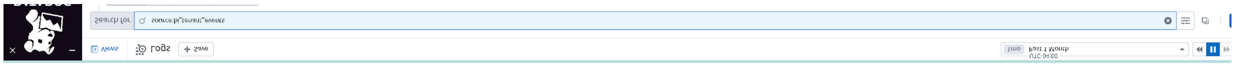
Events: ADD DEVICE + 12 more

Status: ACTIVE

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

4 Verification in Datadog

- Access your Datadog URL
- Select Logs in the left pane
- Use “source=beyond-identity” as the search pattern



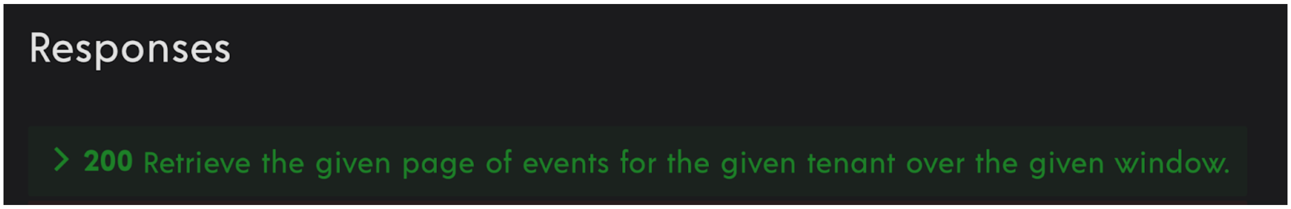
Search for: source:bi_tenant_events

5 Appendix A

How to get event types?

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

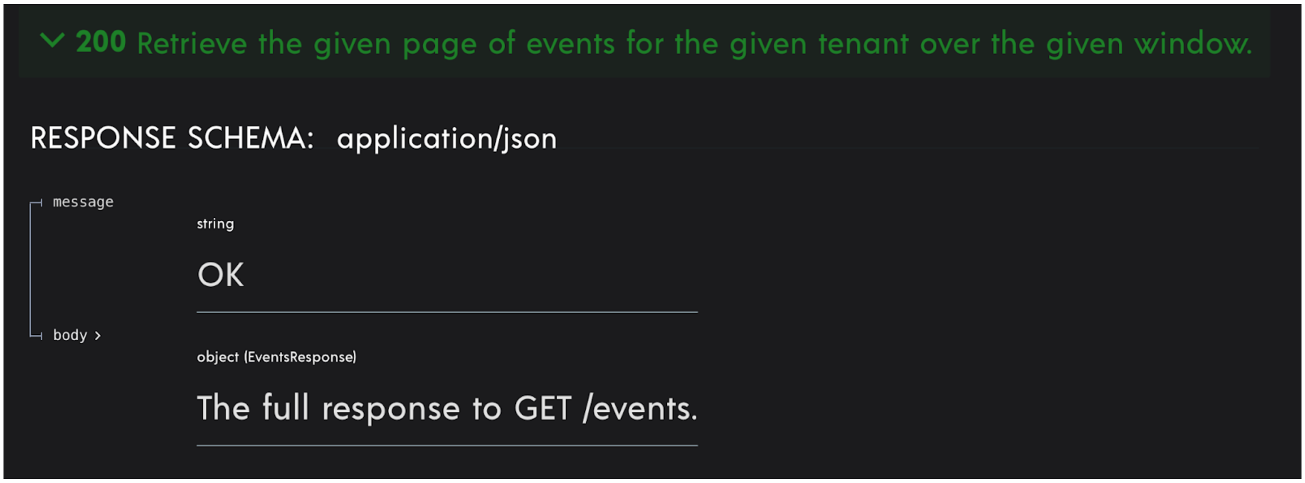
Scroll down



Responses

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

Click on arrow next to 200



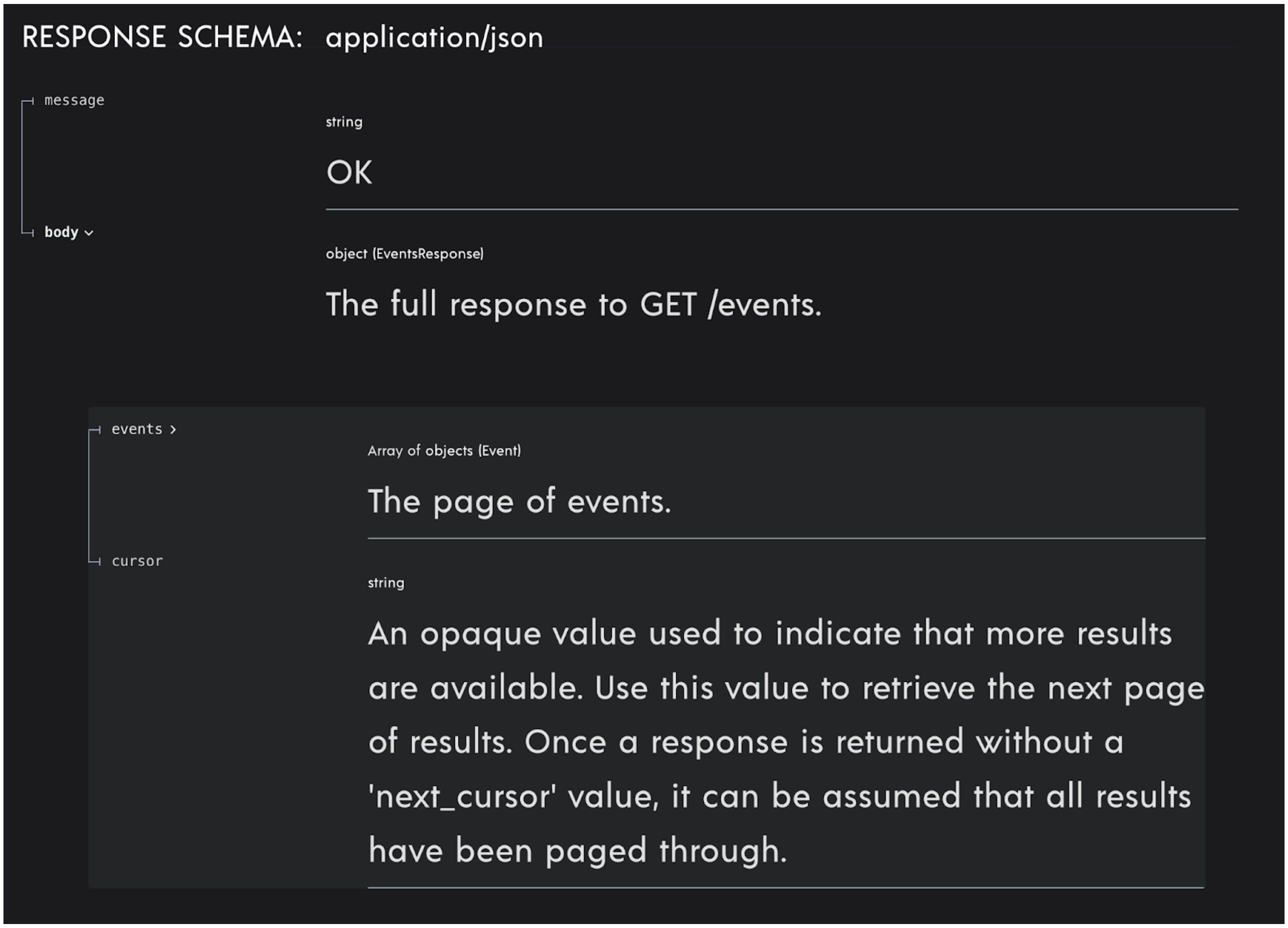
200 Retrieve the given page of events for the given tenant over the given window.

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)

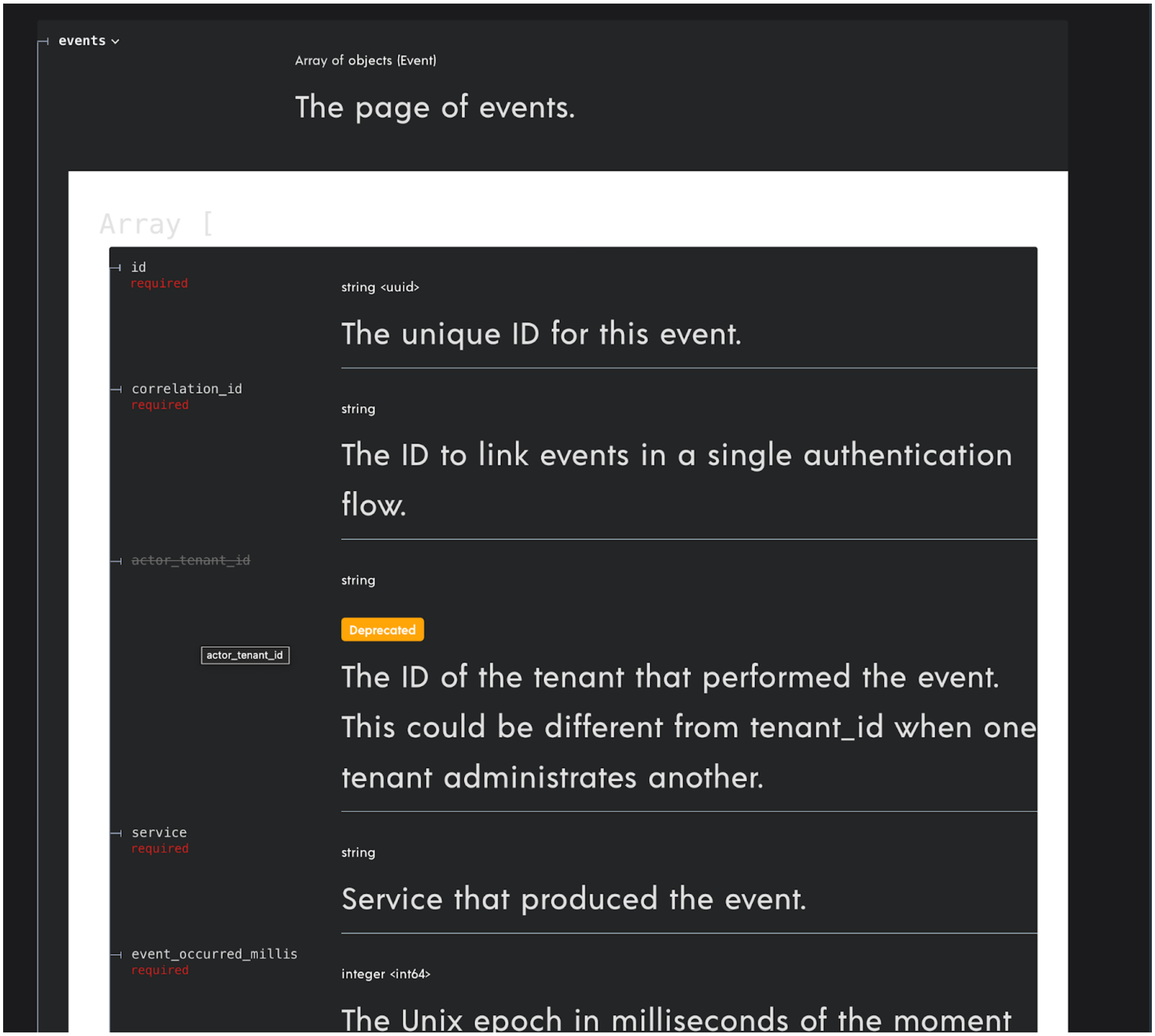
The page of events.

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~~

actor_tenant_id

string

Deprecated

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

service
required

string

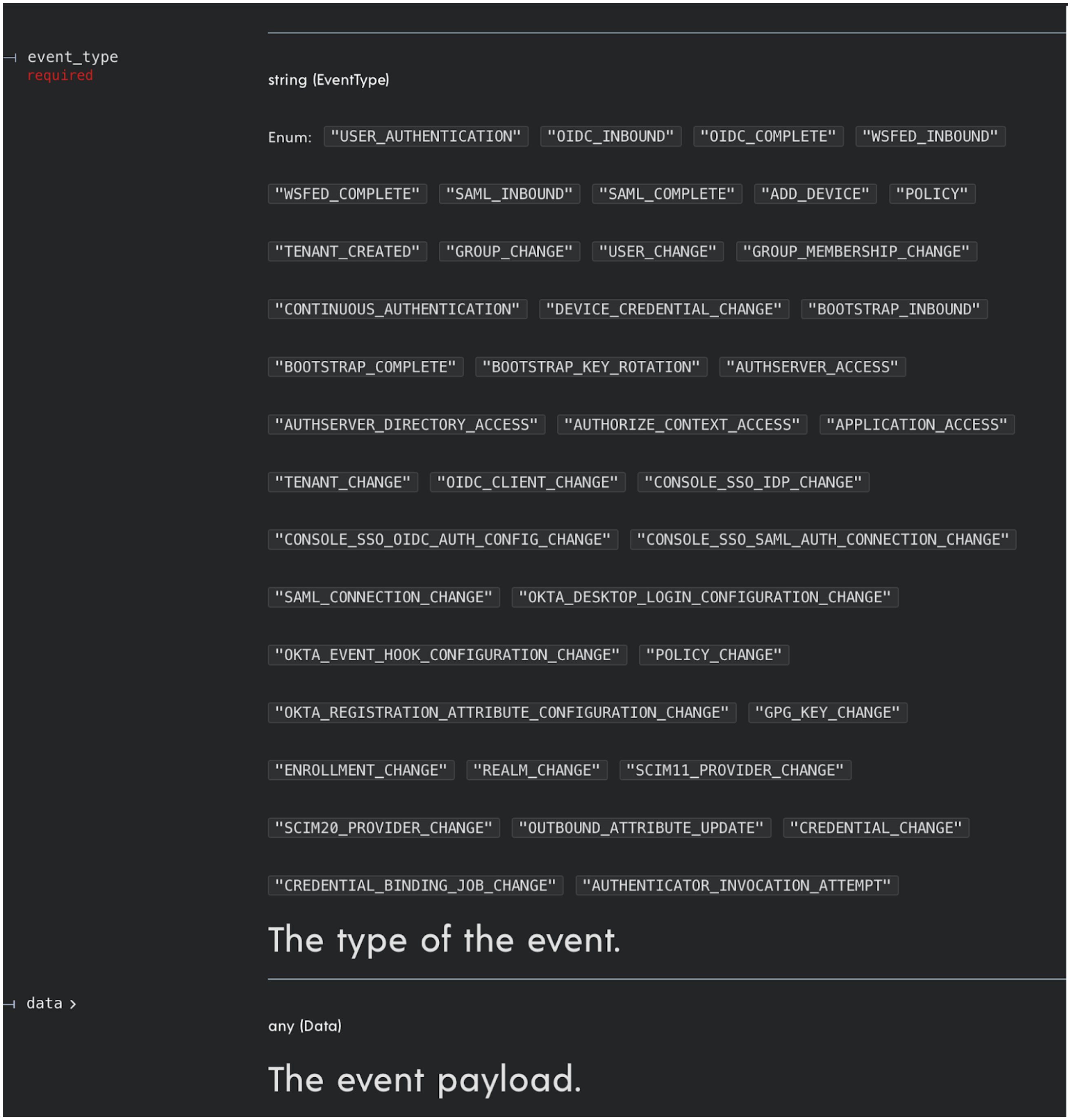
Service that produced the event.

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