

BEYOND IDENTITY EVENTS DATA INTEGRATION WITH ELASTIC – PUSH



1 Table of Contents

2	INTRODUCTION	2
2.1	ABOUT	2
2.2	PREREQUISITES	2
3	ELASTIC CONFIGURATION	2
3.1	CREATE ELASTIC DEPLOYMENT	3
3.2	INSTALL AGENT, ADD TO FLEET	5
3.3	CREATE AGENT POLICY / ADD AGENT	7
3.4	ADD HTTP LOGS INTEGRATION TO AGENT POLICY [PUSH]	10
3.5	PUSH TENANT EVENTS TO ELASTIC	12
4	BEYOND IDENTITY CONFIGURATION [NOT IN ADMIN CONSOLE YET!!]	12
5	VERIFICATION IN ELASTIC	13
6	APPENDIX A	16
7	APPENDIX B	17

2 Introduction

2.1 About

This guide provides instructions on how to:

- Integrate BI events data with Elastic. Elastic supports events push and events pull models

2.2 Prerequisites

Ensure that you have the following:

- You have a tenant configured for your organization and able to enroll users.
- You have an Elastic cloud account with admin privilege

BEYOND
IDENTITY

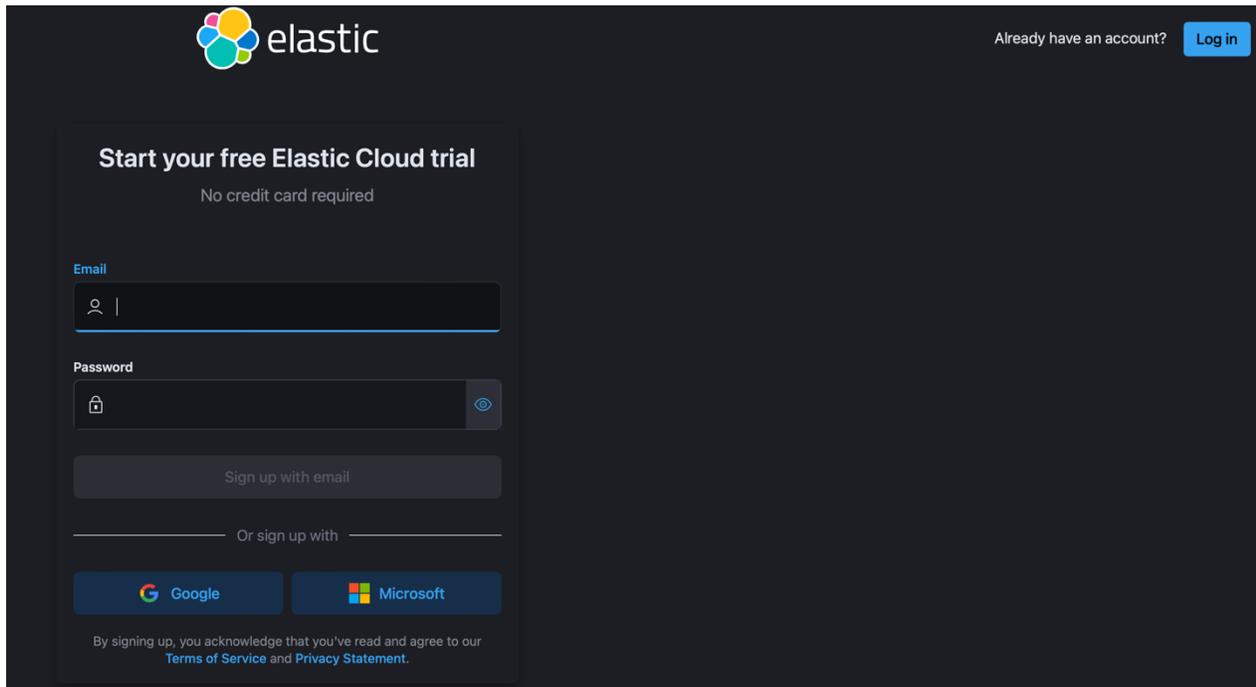
- The Firewall ports should be open to allow Beyond Identity[BI] to push events to your elastic deployment. Reach out to your BI contact for the ports details

3 Elastic configuration

- Create Elastic deployment
- Install Agent, Add to fleet
- Create Agent Policy / Add agent
- Add HTTP Logs Integration to agent policy [Push]
- Push tenant events to Elastic

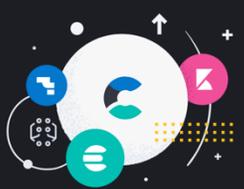
3.1 Create Elastic deployment

You need an Elastic account to create a deployment and configure push or pull. You can start free by accessing <https://cloud.elastic.co/registration> and sign up for a 14-day trial account



Once you the account is created, click on “Start your free trial”

Elasticsearch Service



Get started with Elasticsearch Service

Create your first deployment to manage an Elasticsearch cluster on the cloud platform of your choice. Add additional Elastic products to your deployment like Kibana, machine learning, or APM.

[Start your free trial](#)

Platform features

- ✓ Cloud hosting on AWS, GCP or Azure
- ✓ Logs, metrics, and APM in one place
- ✓ Includes machine learning, security, and more
- ✓ One-click upgrades with no downtime
- ✓ Same-day new version releases
- ✓ Monitored 24/7

Provide a Name for your deployment and click “Create deployment”.

Create your first deployment

A deployment includes Elasticsearch, Kibana, and other Elastic Stack features, allowing you to store, search, and analyze your data.

Name

 **GCP Iowa (us-central1)** [Edit settings](#)
Storage optimized, 8.3.2

[Create deployment](#)

After a few seconds, the deployment should be ready. Click on “Continue”



Your deployment is ready!



Continue

Save the deployment credentials

These root credentials are shown only once.
They provide super user access to your deployment. Keep them safe.

Username

elastic

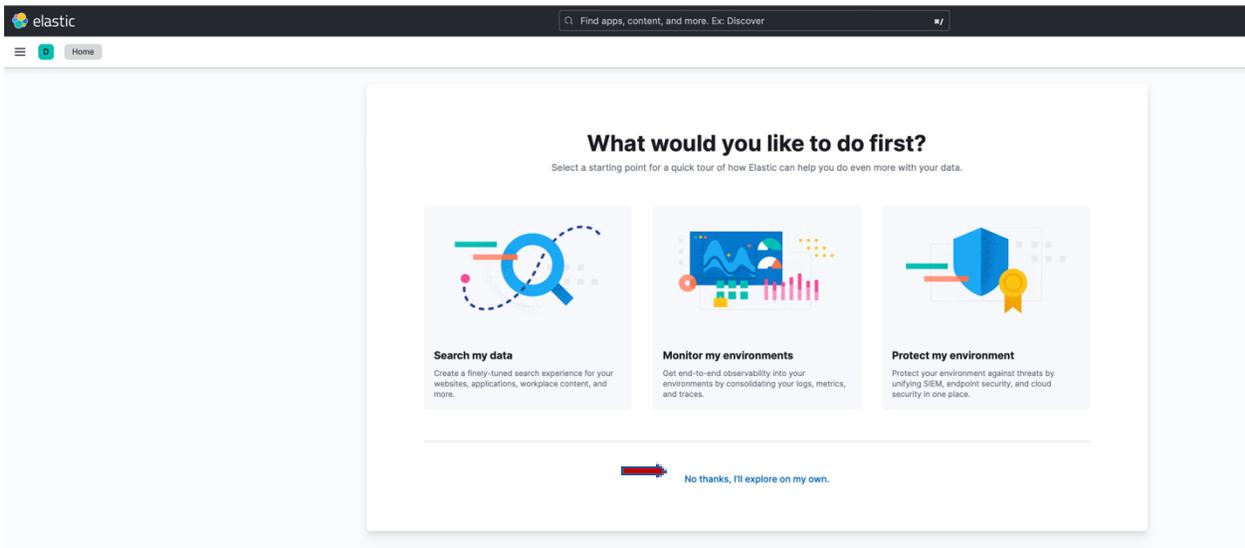
Password

6nfm0UcMGCLPtttrhrlKJvGm 

Download

Skip

3.2 Install Agent, Add to Fleet



elastic #/

Home

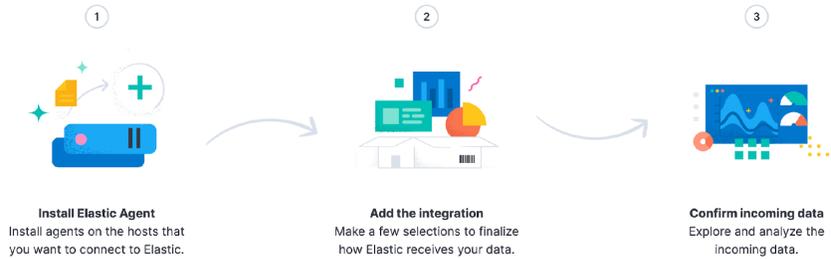
What would you like to do first?

Select a starting point for a quick tour of how Elastic can help you do even more with your data.

- Search my data**
Create a finely-tuned search experience for your websites, applications, workplace content, and more.
- Monitor my environments**
Get end-to-end observability into your environments by consolidating your logs, metrics, and traces.
- Protect my environment**
Protect your environment against threats by unifying SIEM, endpoint security, and cloud security in one place.

 No thanks, I'll explore on my own.

Ready to add your first integration?



[Learn more about installing Elastic Agent](#)

Go back

Install Elastic Agent

Set up Custom HTTP Endpoint Logs integration



These steps configure and enroll the Elastic Agent in Fleet to automatically deploy updates and centrally manage the agent. As an alternative to Fleet, advanced users can run agents in [standalone mode](#).

1 Install Elastic Agent on your host

Select the appropriate platform and run commands to install, enroll, and start Elastic Agent. Reuse commands to set up agents on more than one host. For aarch64, see our [downloads page](#). For additional guidance, see our [installation docs](#).

Linux Tar Mac Windows RPM DEB Kubernetes

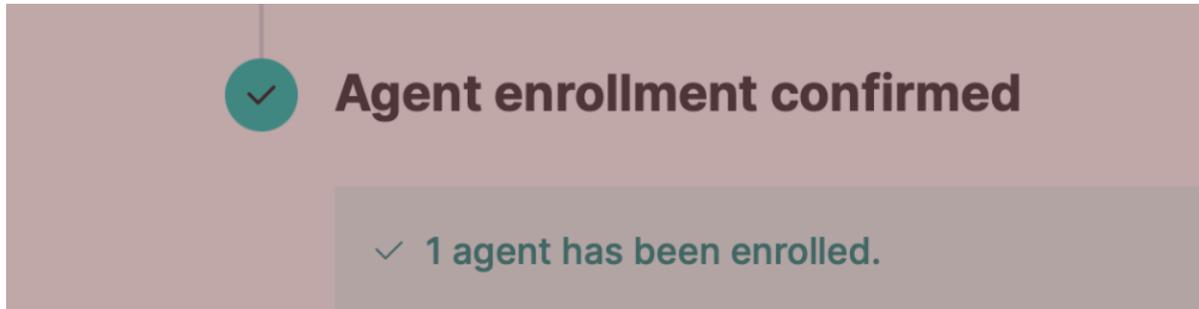
```
curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.4.2-linux-x86_64.tar.gz
tar xzvf elastic-agent-8.4.2-linux-x86_64.tar.gz
cd elastic-agent-8.4.2-linux-x86_64
sudo ./elastic-agent install --url=https://6970251b59b24d29b2f9405773a46f1.fleet.us-cen
```

Copy to clipboard

2 Confirm agent enrollment

After the agent starts up, the Elastic Stack listens for the agent and confirms the enrollment in Fleet. If you're having trouble connecting, check out the [troubleshooting guide](#).

Choose the agent platform as per your choice for example a host running in AWS EC2. Once the agent is successfully installed, the custom agent enrollment will display “agent has been enrolled”



You will be able to see the agent listed under Fleet, under Elastic web console=>Management=>Fleet

3.3 Create Agent Policy / Add agent

Agents are added to an agent policy and then integrations are attached to the policy. A policy is a collection of inputs and settings that defines the data to be collected by an Elastic Agent. Each Elastic Agent can only be enrolled in a single policy.

Within an Elastic Agent policy is a set of individual integration policies. These integration policies define the settings for each input type. The available settings in an integration depend on the version of the integration in use.

custom HTTP Endpoint Log integration is used for setting up a HTTP listener to post BI data events.
custom HTTPJSON input integration is used to ingest data from BI tenant events API endpoint[<https://dataexport-public.byndid.com/v1/events?ordering=desc>] to pull data.

Navigate to Fleet under Management, and choose “Agent Policies” Tab. Click on “create agent policy”

The screenshot shows the Elastic Fleet management interface. The left sidebar is expanded to show the 'Management' section, with 'Fleet' highlighted and a red arrow pointing to it. The main content area displays the 'Fleet' page, which includes a search bar, a 'Create agent policy' button, and a table of agent policies.

Name	Description	Last updated on	Agents	Integrations	Actions
Agent Policy 2 rev. 1		Sep 24, 2022	0	1	...
Agent policy 1 rev. 10		Aug 11, 2022	1	4	...
Elastic Cloud agent po... rev. 5	Default agent policy for agents hosted on Elastic Cloud	Jul 29, 2022	1	2	...
My first agent policy rev. 1		Jul 26, 2022	1	0	...

Provide a name for the agent policy, for example “Agent Policy 1”. Uncheck “Collect system logs and metrics”. Under “Advanced option”, uncheck “collect agent logs” and “collect agent metrics”. Click “Create agent policy”

Create agent policy



Agent policies are used to manage settings across a group of agents. You can add integrations to your agent policy to specify what data your agents collect. When you edit an agent policy, you can use Fleet to deploy updates to a specified group of agents.

Name

Collect system logs and metrics ⓘ

Advanced options

Description

Add a description of how this policy will be used.

Default namespace

Namespaces are a user-configurable arbitrary grouping that makes it easier to search for data and manage user permissions. A policy namespace is used to name its integration's data streams. [Learn more](#).

Agent monitoring

Collecting monitoring logs and metrics will also create an Elastic Agent integration. Monitoring data will be written to the default namespace specified above.

Collect agent logs ⓘ

Collect agent metrics ⓘ

Unenrollment timeout

An optional timeout in seconds. If provided, an agent will automatically unenroll after being gone for this period of time.

Output for integrations

Select which output to use for data from integrations.

Cancel



Create agent policy

3.4 Add HTTP Logs Integration to agent policy [Push]

Navigate to Management=>Fleet. Click on “Agent policies”.

The screenshot shows the Elastic Fleet management interface. The left sidebar contains navigation options: Home, Recently viewed, Observability, Security, and Management. Under Management, 'Fleet' is highlighted with a red arrow. The main content area shows the 'Fleet' overview with a table of agents. A red box highlights the 'Agent policies' tab in the top navigation bar.

Host	Status	Tags	Agent policy	Version	Last activity	Actions
67b1bb0c6896	Healthy		Elastic Cloud agent policy rev. 5	8.3.2	52 seconds ago	...
ip-172-50-0-130.us-west-2.compute.internal	Healthy		Agent policy 1 rev. 10	8.3.2	27 seconds ago	...
rriabsmac.local	Healthy		My first agent policy rev. 1	8.3.2	38 seconds ago	...

Click on “Add integrations”

The screenshot shows the Elastic Agent policy configuration page. The page title is 'Agent policy 1'. It shows a list of integrations with columns for Name, Integration, Namespace, and Actions. A red box highlights the 'Add Integration' button.

Name	Integration	Namespace	Actions
BL_pull_httpjson-1	Custom HTTPJSON input v1.3.1	default	...
elastic_agent-aws-ec2	Elastic Agent v1.3.3 Upgrade	default	...
http_endpoint-1	Custom HTTP Endpoint Logs v1.2.0	default	...
system-1	System v1.16.2 Upgrade	default	...

Type “HTTP” in the search box. In the search results, click “custom HTTP Endpoint Logs”

The screenshot shows the Elastic Integrations page. At the top, there is a search bar with the text "Find apps, content, and more. Ex: Discover". Below the search bar, there are three main integration cards: "Web crawler", "Elastic APM", and "Endpoint and Cloud Security". Below these cards, there is a list of categories on the left, including AWS, Azure, Cloud, Communications, Config management, Containers, Custom, Datastore, Elastic Stack, Enterprise search, File storage, and Geo. The search results for "HTTP" are displayed in the center, showing three cards: "Apache HTTP Server", "Custom API", and "Custom HTTP Endpoint Logs". A red arrow points to the search bar, and another red arrow points to the "Custom HTTP Endpoint Logs" card.

Click “Add Custom HTTP Endpoint Logs”

The screenshot shows the Elastic Custom HTTP Endpoint Logs page. At the top, there is a search bar with the text "Find apps, content, and more. Ex: Discover". Below the search bar, there are two main integration cards: "Web crawler" and "Elastic APM". Below these cards, there is a list of categories on the left, including AWS, Azure, Cloud, Communications, Config management, Containers, Custom, Datastore, Elastic Stack, Enterprise search, File storage, and Geo. The search results for "HTTP" are displayed in the center, showing three cards: "Apache HTTP Server", "Custom API", and "Custom HTTP Endpoint Logs". A red arrow points to the search bar, and another red arrow points to the "Custom HTTP Endpoint Logs" card. Below the search results, there is a section for "Custom HTTP Endpoint Logs" with a "Back to integrations" link and an "Add Custom HTTP Endpoint Logs" button. The page shows the "Custom HTTP Endpoint Log integration" details, including a description of the integration and a table of HTTP response codes and reasons.

Custom HTTP Endpoint Log integration

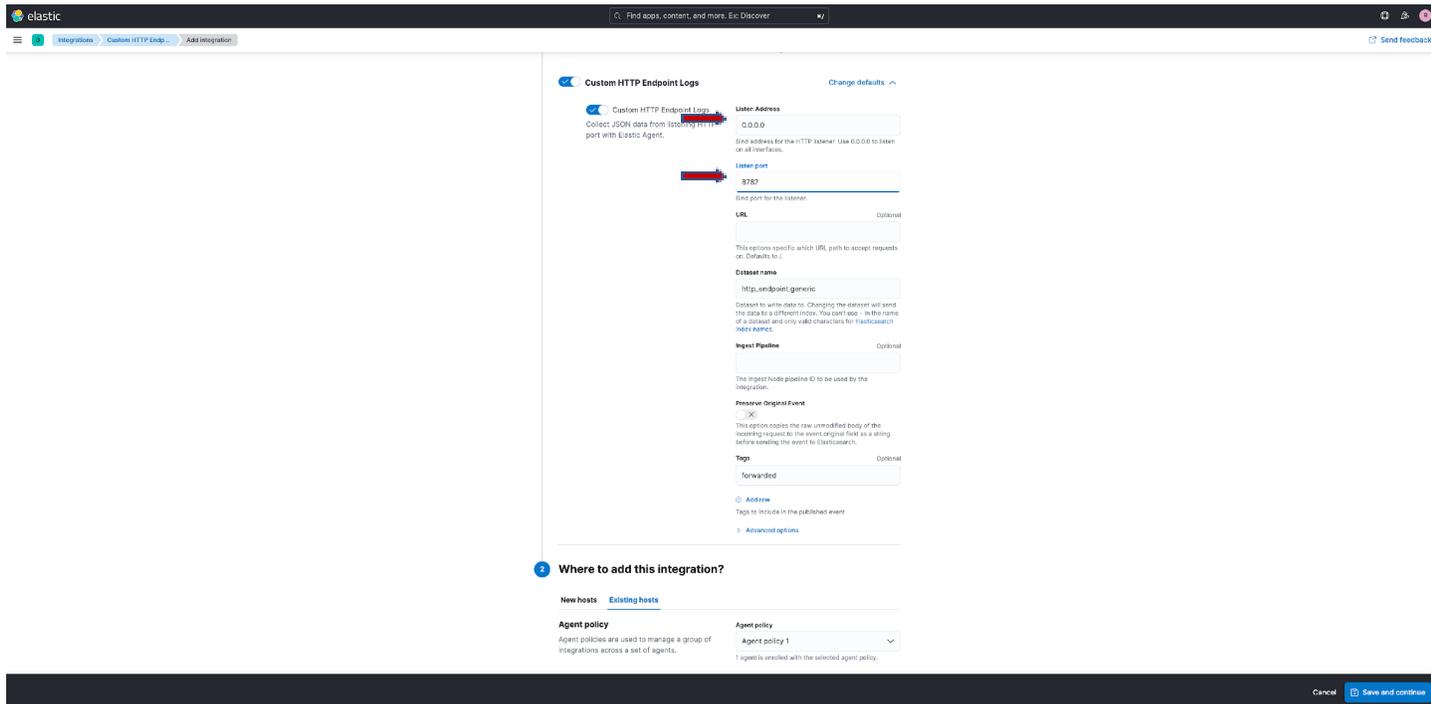
The custom HTTP Endpoint Log integration initializes a listening HTTP server that collects incoming HTTP POST requests containing a JSON body. The body must be either an object or an array of objects. Any other data types will result in an HTTP 400 (Bad Request) response. For arrays, one document is created for each object in the array.

These are the possible response codes from the server.

HTTP Response Code	Name	Reason
200	OK	Returned on success.
400	Bad Request	Returned if JSON body decoding fails.
401	Unauthorized	Returned when basic auth, secret header, or HMAC validation fails.
405	Method Not Allowed	Returned if methods other than POST are used.
406	Not Acceptable	Returned if the POST request does not contain a body.
415	Unsupported Media Type	Returned if the Content-Type is not application/json.
500	Internal Server Error	Returned if an I/O error occurs reading the request.

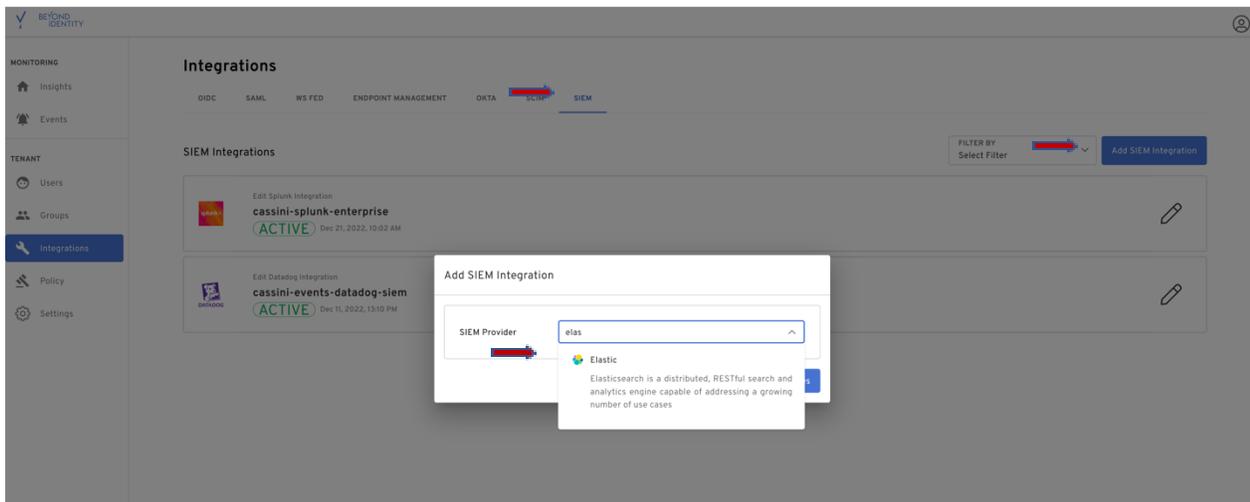
Custom ingest pipelines may be added by adding the name to the pipeline configuration option, creating custom ingest pipelines can be done either through the API or the [Ingest Node Pipeline UI](#).

Enter “0.0.0.0” for the Listen Address and a value for the listen port, for example 8787. Please note this port must be opened to Beyond Identity to post events. Leave the other settings to defaults. Under “Where to add this integration?”, choose the agent policy created in the section above “Agent Policy 1”



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”. Click on “Add SIEM Integration”



Choose “Elastic” from the drop down.

Add SIEM Integration

SIEM Provider	Elastic ▼
Name	BI tenant events elastic integration
Host	Elastic host name
Port	Elastic custom endpoint HTTP port
Authentication Method	NoAuth ▼
Events	CONTINUOUS AU... × + 4 more ▼
Status	ACTIVE <input checked="" type="checkbox"/>

Cancel

Save Changes

Provide a name for the configuration. From the events drop down, “select all” events or one the events you are interested in. Click on “Save Changes”

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

5 Verification in Elastic

- Access your Elastic URL
- Select “Discover” under “Analytics”

Manage this deployment

Home

Recently viewed

- user_name
- user_authentication_events
- 3. Login Failed Details

Analytics

Discover

- Dashboard
- Canvas
- Maps
- Machine Learning
- Graph
- Visualize Library

Enterprise Search

- Overview
- Elasticsearch
- App Search
- Workplace Search

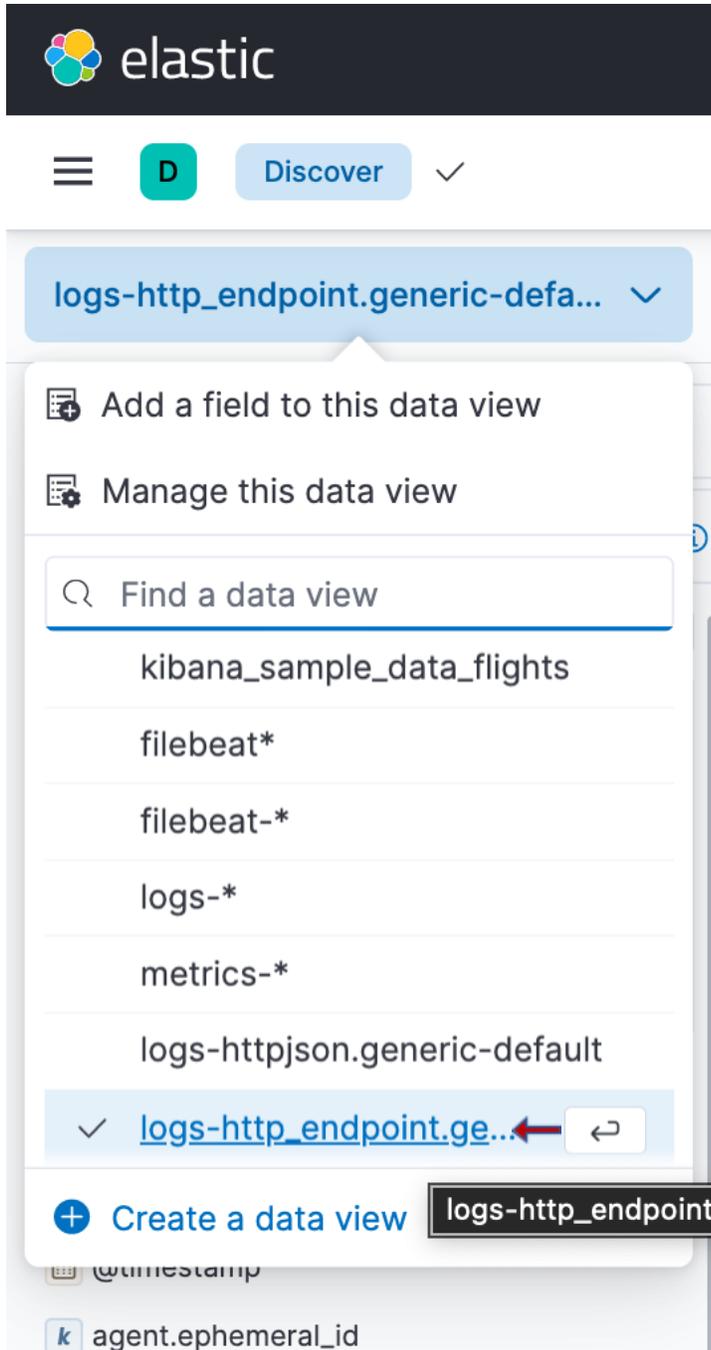
Observability

- Overview
- Alerts
- Cases
- Logs
- Metrics
- APM
- Uptime
- User Experience

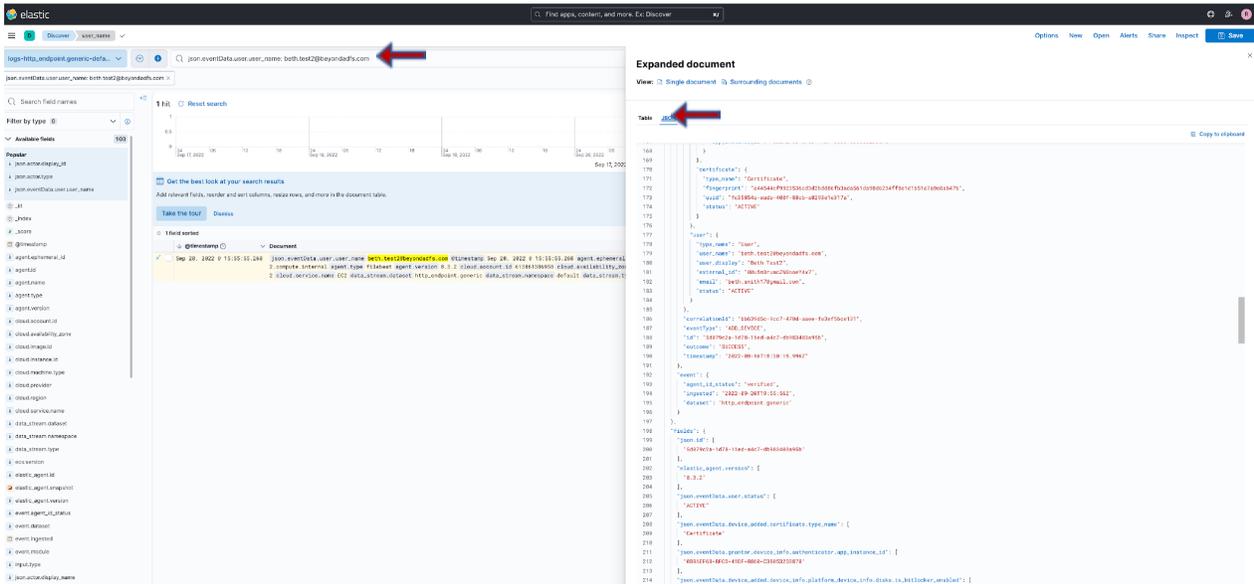
Security

- Dashboards
- Alerts
- Timelines
- Cases

Choose logs-http_endpoint.generic-default



Enter “json.eventData.user.user_name: USER_WHO_AUTHENTICATED_USING_BI” in the query box. Select the event in the results and click “JSON” on the right.

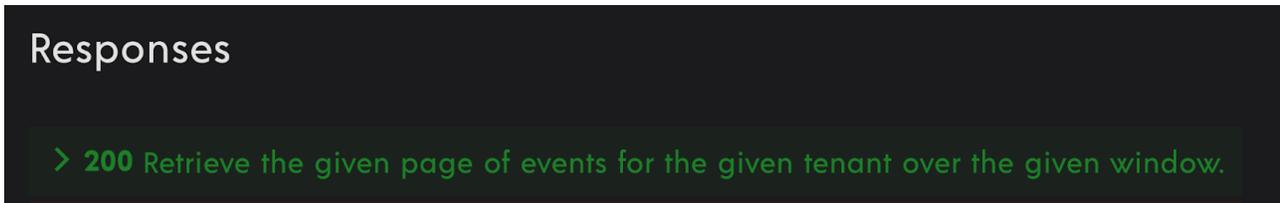


6 Appendix B

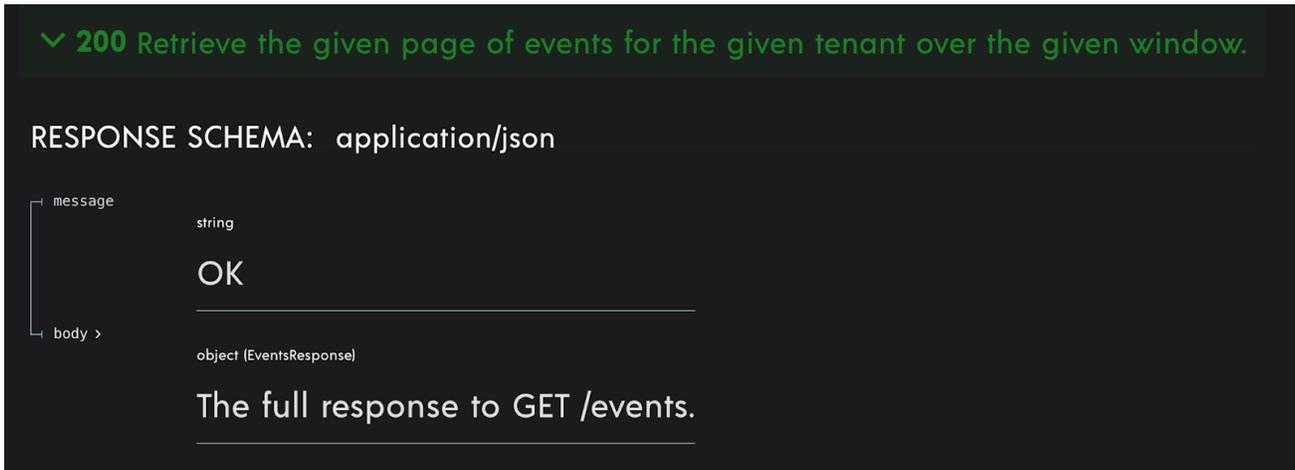
How to get event types?

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

Scroll down



Click on arrow next to 200



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	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