opentext™

# ArcSight Intelligence

Software Version: 24.1

## Developer's Guide for ArcSight Intelligence

Document Release Date: Jan 2024
Software Release Date: Jan 2024

# Legal Notices

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

# Copyright Notice



# Trademark Notices



# Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

https://www.microfocus.com/support-and-services/documentation

# Contents

# Introduction

This guide describes how to use the Intelligence REST API, which allows you to manage, develop, and interface with analytics data. This API also provides access to analytics results and related tuning parameters.

## Intended Audience

This Guide assumes that you are an experienced programmer and are familiar with REST APIs, web programming, and your organization's server environment, security infrastructure, and data sources.

You should also be familiar with the business needs of your organization.

## Construct API URLs

To call an endpoint in this API, use the fully-qualified domain name (FQDN) of ArcSight Intelligence, and append the base path (`/interset/api`) followed by the path listed in the Tuning API Reference and Analytics API Reference , For example, to call the `GET /tenants` endpoint, use the following URL with the GET method:

```
https://<FQDN of Intelligence>/interset/api/tenants
```

## Retrieve Paginated API Responses

Some endpoints return paginated results. These endpoints include a field called `scrollId` in their responses. To retrieve the next page of results from the same call, call the endpoint again with the same parameters, but this time pass the `scrollId` from the current response in the `scrollId` query parameter of the new API call.

For example, the response from the `GET /search/{tid}/{entityType}/topRisky` endpoint looks similar to the following:

```
{
  "requestTime": 29,
  "data": [
    {
      "entityHash": "bc23443bd21342fa8997e",
      "entityType": "user",
      "entityName": "Annie",
      "risk": 25,
```

```
      "riskChange": 0,
      "storyCount": 3,
      "lastActivity": 1453957200,
      "preDecayedRisk": 0,
      "decayedToTimestamp": 0,
      "mostSignificantAlert": null,
      "tags": [
        {
          "id": "9v3sdqdC2jdOFJCBuYcAPw",
          "name": "reviewed",
          "source": "user",
          "description": ""
        }
      ]
    },
  ],
  "totalHits": 25,
  "scrollId": "vabsjk5h24elkdasjfojdabhgjk32b5b",
  "cached": false
}
```

Note the returned `scrollId`. To get the next set of results, call the `GET /search/{tid}/{entityType}/topRisky` endpoint again, but pass the `scrollId` as a query parameter:

```
curl -X GET --header 'Accept: text/plain' \
   'https://<reporting_fqdn>/interset/api/search/<tenant_
ID>/files/topRisky?scrollid=vabsjk5h24elkdasjfojdabhgjk32b5b'
```

# Render Anomalies

For some of the search endpoints, you can specify a `markup` parameter. When `markup` is `false`, the returned anomalies contain only English text that can be directly displayed without further processing. When `markup` is `true`, the anomalies may contain markup tags in double curly braces, {{ and }}. The possible tags are as follows:

- **timestamp**

  The anomaly time.

  The timestamp corresponds to the start of the hour in which the anomaly occurs. For example:

  ```
  "...{{timestamp ms=\"1516748280000\" joda=\"h\" moment=\"h\"}} ..."
  ```

  The **timestamp** can include the following fields:

  - **ms**: the epoch (Unix) timestamp. Epoch timestamps are expressed in GMT (i.e., they don't contain time zone information). Usually this timestamp would be rendered in the

browser's time zone.

- **joda**: specifies the format to use when rendering with Joda-Time.
- **moment**: specifies the format to use when rendering with Moment.js or date-fns.

If the **moment** field isn't present, the Intelligence UI uses the format string "dddd".

- **entity**

  The entity that the text pertains to. For example:

```
 "... {{entity name=\"katherine.white\" hash=\"28044feb24be66c7\"
type=\"user\" risk=21 showRiskBall=false}} ..."
```

  The **entity** can include the following fields:

  - **name**: the name of the entity.
  - **hash**: an internal identifier for the entity that is used in other API calls.
  - **type**: identifies the kind of entity. One of: file, machine, project, server, user, volume, printer, share, resource, website, or ip.
  - **risk**: the current risk of the entity.
  - **showRiskBall**: specifies whether to show a visual indicator of the risk.

- **hover**

  Additional text to use for hovering.

```
"... the user {{#hover title=\"accessed in some way\"}} touched {{/hover}}
27 projects ..."
```

  This text provides a hint to the user interface that additional disclosure text is available. The text from the title field could be shown, for example, when the user hovers over the highlighted text.

# Use the API with the Swagger UI

You can use Swagger UI to familiarize yourself with the API. In the Swagger UI, you can see all the endpoints, their parameters, and sample responses.

**Note**: You must have the required permissions to call API endpoints. The required permissions vary from endpoint to endpoint. For more information, see "User Roles and Permissions" on the next page.

**To access the Swagger UI:**

1. In a web browser, log in to Intelligence as a user with the required permissions.
2. Click the gear icon on the top right corner of your screen, point to **API Documentation >**, then select the desired API in the drop-down list.
   Swagger for the selected API opens in a new browser window.
3. Click a category (such as **actions** or **tenants**) to expand it.
   The endpoints that are part of that category are listed.
4. Click an endpoint to show all its details. You can call an endpoint by clicking **Try it out!**, filling in the **Parameters** section (if required by the endpoint), and then clicking **Execute**.

## Example: Call an Endpoint

In this example, we will call the `info/build` endpoint.

1. In the Swagger UI, expand **info**, and then expand **GET /info/build**.
2. Scroll down to the **Response Messages** section, and then Click **Try it out!**.
3. The response is displayed in the **Response Body** section.

# User Roles and Permissions

You must have the required permissions to call API endpoints. The required permissions vary from endpoint to endpoint.

The following table lists the default roles, permissions, and the APIs the users have access to and can perform API operations.

Users must be created in Fusion and assigned relevant roles and permissions. For more information on creating users and roles, see the User's Guide for Fusion 1.5 in the ArcSight Platform.

| API | Required Permissions | Roles | Considerations |
|---|---|---|---|
| Tuning API | • Access Intelligence<br>• Tune Intelligence Analytics | • System Admin<br>• Admin<br>• Analyst | • Some endpoints require only the **Access Intelligence** permission.<br>• Some endpoints require only the **Tune Intelligence Analytics** permission.<br>• The Analyst role does not have access to end points that require the **Tune Intelligence Analytics** permission. |
| Analytics API | • Access Intelligence<br>• View Intelligence Raw Events | • System Admin<br>• Admin<br>• Analyst | • Some endpoints require only the **Access Intelligence** permission.<br>• Some endpoints require only the **View Intelligence Raw Events** permission.<br>• Some endpoints require both **Access Intelligence** and **View Intelligence Raw Events** permissions. |

# Tuning API Reference

Version: 24.1

BasePath: /interset/tuning

## Alert Templates

### POST /{tid}/alert_templates

#### Consumes

- application/json

#### Produces

- application/json

#### Path parameters

- **tid** (required)

  Tenant ID

#### Request body

AlertTemplate

#### Responses

`default`

successful operation

### DELETE /{tid}/alert_templates/{anomalyType}/{did}

### Consumes

- application/json

### Produces

- application/json

### Path parameters

- **tid** (required)
  Tenant ID
- **anomalyType** (required)
  Analytics Anomaly Type (i.e. 200)
- **did** (required)
  Data Identifier

### Responses

`default`

successful operation

## GET /{tid}/alert_templates/{anomalyType}/{did}

### Produces

- application/json

### Path parameters

- **tid** (required)
  Tenant ID
- **anomalyType** (required)
  Analytics Anomaly Type (i.e. 200)
- **did** (required)
  Data Identifier

## Return type

AlertTemplate

## Example data

Content-Type: application/json

```
{
  "genericSearchQuery" : "genericSearchQuery",
  "reconSearchQuery" : "reconSearchQuery",
  "unitName" : "unitName",
  "anomalyType" : "anomalyType",
  "reconStartTime" : "reconStartTime",
  "tid" : "tid",
  "templatesAlert" : "templatesAlert",
  "reconEndTime" : "reconEndTime",
  "unitType" : "unitType",
  "hasAggregatedIdentifiers" : true,
  "genericTimeRangeQuery" : "genericTimeRangeQuery",
  "datasource" : "datasource",
  "threatDescription" : "threatDescription",
  "familyName" : "familyName",
  "unitDescription" : "unitDescription",
  "contextType" : "contextType",
  "threatName" : "threatName",
  "templatesThreat" : "templatesThreat",
  "sqlSearchQuery" : "sqlSearchQuery",
  "templatesFamily" : "templatesFamily",
  "templatesTooltip" : "templatesTooltip",
  "bucketSize" : "bucketSize",
  "did" : 0,
  "templatesTeaser" : "templatesTeaser"
}
```

## Responses

```
200
```

successful operation

# PUT /{tid}/alert_templates/{anomalyType}/{did}

### Consumes

- application/json

### Produces

- application/json

### Path parameters

- **tid** (required)

  Tenant ID
- **anomalyType** (required)

  Analytics Anomaly Type (i.e. 200)
- **did** (required)

  Data Identifier

### Request body

AlertTemplate

### Responses

`default`

successful operation

# Anomaly Meta

## POST /{tid}/anomaly_meta

### Consumes

- application/json

### Produces

- application/json

### Path parameters

- **tid** (required)

  Tenant ID

### Request body

AnomalyMeta

### Responses

`default`

successful operation

## DELETE /{tid}/anomaly_meta/{anomalyType}

### Produces

- application/json

### Path parameters

- **tid** (required)

  Tenant ID
- **anomalyType** (required)

  Analytics Anomaly Type (i.e. 200)

### Responses

`default`

successful operation

## GET /{tid}/anomaly_meta/{anomalyType}

### Produces

- application/json

### Path parameters

- **tid** (required)

  Tenant ID
- **anomalyType** (required)

  Analytics Anomaly Type (i.e. 200)

### Return type

AnomalyMeta

### Example data

Content-Type: application/json

```
{
  "anomalyType" : 0,
  "timeBucket" : "timeBucket",
  "tid" : "tid"
}
```

### Responses

```
200
```

successful operation

## GET /{tid}/anomaly_meta

### Produces

- application/json

### Path parameters

- **tid** (required)

  Tenant ID

### Return type

array[AnomalyMeta]

### Example data

Content-Type: application/json

```
[ {
  "anomalyType" : 0,
  "timeBucket" : "timeBucket",
  "tid" : "tid"
}, {
  "anomalyType" : 0,
  "timeBucket" : "timeBucket",
  "tid" : "tid"
} ]
```

### Responses

```
200
```

successful operation

## PUT /{tid}/anomaly_meta/{anomalyType}

### Consumes

- application/json

### Produces

- application/json

### Path parameters

- **tid** (required)

  Tenant ID
- **anomalyType** (required)

  Analytics Anomaly Type (i.e. 200)

### Request body

AnomalyMeta

### Responses

`default`

successful operation

## Custom Anomalies

## GET /{tid}/byoa/{anomalyName}

### Produces

- application/json

### Path parameters

- **tid** (required)

  Tenant ID
- **anomalyName** (required)

  Anomaly Name

### Return type

array[AlertsMeta]

### Example data

Content-Type: application/json

```
[ {
  "alertType" : "alertType",
  "alertName" : "alertName",
  "anomalyType" : 6,
  "timeBucket" : "timeBucket",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
}, {
  "alertType" : "alertType",
  "alertName" : "alertName",
  "anomalyType" : 6,
  "timeBucket" : "timeBucket",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
} ]
```

### Responses

```
200
```

successful operation

## GET /{tid}/byoa

### Produces

- application/json

### Path parameters

- **tid** (required)

  Tenant ID

### Return type

array[AlertsMeta]

### Example data

Content-Type: application/json

```
[ {
  "alertType" : "alertType",
  "alertName" : "alertName",
  "anomalyType" : 6,
  "timeBucket" : "timeBucket",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
}, {
  "alertType" : "alertType",
  "alertName" : "alertName",
  "anomalyType" : 6,
  "timeBucket" : "timeBucket",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
} ]
```

### Responses

```
200
```

successful operation

## POST /{tid}/byoa/register

*Register Custom Anomaly.*

### Consumes

- application/json

### Produces

- application/json

### Path parameters

- **tid** (required)
  Tenant ID

### Request body

AlertsMetaSimple

### Responses

`default`

successful operation

## Custom Models

## GET /{tid}/byom/{ds}/{did}/{timeBucket}/{modelName}/export

### Produces

- text/xml

### Path parameters

- **tid** (required)
  Tenant ID
- **modelName** (required)
  Model Name
- **ds** (required)
  Data Source
- **did** (required)
  Data Identifier
- **timeBucket** (required)
  Time Bucket

### Responses

`default`

successful operation

## GET /{tid}/byom/{modelName}

### Produces

- application/json

### Path parameters

- **tid** (required)

  Tenant ID
- **modelName** (required)

  Model Name

### Return type

array[ByomMeta]

### Example data

Content-Type: application/json

```
[ {
  "secEntitytype" : "secEntitytype",
  "secEntityCol" : "secEntityCol",
  "modelName" : "modelName",
  "targetClass" : "targetClass",
  "primEntityCol" : "primEntityCol",
  "timeBucket" : "timeBucket",
  "primEntitytype" : "primEntitytype",
  "isActive" : true,
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
}, {
  "secEntitytype" : "secEntitytype",
```

```
  "secEntityCol" : "secEntityCol",
  "modelName" : "modelName",
  "targetClass" : "targetClass",
  "primEntityCol" : "primEntityCol",
  "timeBucket" : "timeBucket",
  "primEntitytype" : "primEntitytype",
  "isActive" : true,
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
} ]
```

### Responses

```
200
```

successful operation

## GET /{tid}/byom

### Produces

- application/json

### Path parameters

- **tid** (required)

  Tenant ID

### Return type

array[ByomMetaAnomalytype]

### Example data

Content-Type: application/json

```
[ {
  "secEntitytype" : "secEntitytype",
  "secEntityCol" : "secEntityCol",
  "modelName" : "modelName",
  "targetClass" : "targetClass",
```

```
  "anomalyType" : 6,
  "primEntityCol" : "primEntityCol",
  "timeBucket" : "timeBucket",
  "primEntitytype" : "primEntitytype",
  "isActive" : true,
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
}, {
  "secEntitytype" : "secEntitytype",
  "secEntityCol" : "secEntityCol",
  "modelName" : "modelName",
  "targetClass" : "targetClass",
  "anomalyType" : 6,
  "primEntityCol" : "primEntityCol",
  "timeBucket" : "timeBucket",
  "primEntitytype" : "primEntitytype",
  "isActive" : true,
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
} ]
```


### Responses

```
200
```

successful operation

## POST /{tid}/byom/register

*Register a new pmml model with metadata to the BYOM pipeline.*

### Consumes

- multipart/form-data

### Produces

- application/json

## Path parameters

- **tid** (required)
  Tenant ID

## Form parameters

- **file** (required)
  BYOM Custom Model (.pmml)
- **modelName** (required)
  Model Name
- **ds** (required)
  Data Source
- **did** (required)
  Data Identifier
- **timeBucket** (required)
  Time Bucket
- **primEntitytype** (required)
  Primary Entity Type
- **secEntitytype** (required)
  Secondary Entity Type
- **primEntityCol** (required)
  Primary Entity Column Name
- **secEntityCol** (required)
  Secondary Entity Column Name
- **isActive** (required)
  Model is active
- **targetClass** (required)
  Target Class

## Responses

```
default
```

successful operation

## PUT /{tid}/byom/{ds}/{did}/{timeBucket}/{modelName}

### Consumes

- multipart/form-data

### Produces

- application/json

### Path parameters

- **tid** (required)
  Tenant ID
- **modelName** (required)
  Model Name
- **ds** (required)
  Data Source
- **did** (required)
  Data Identifier
- **timeBucket** (required)
  Time Bucket

### Form parameters

- **isActive** (required)
  Model is active

### Responses

`default`

successful operation

# DID Tags

# POST /{tid}/did_tags

## Consumes

- application/json

## Produces

- application/json

## Path parameters

- **tid** (required)

  Tenant ID

## Request body

DidTag

## Responses

`default`

successful operation

# DELETE /{tid}/did_tags/{ds}/{did}/{type}/{identifier}/{tag}

## Produces

- application/json

## Path parameters

- **tid** (required)

  Tenant ID
- **ds** (required)

  Data Source

- **did** (required)

  Data Identifier
- **type** (required)

  Tag Type (i.e. 'did')
- **identifier** (required)

  Tag Key
- **tag** (required)

  Tag Value

### Responses

`default`

successful operation

## GET /{tid}/did_tags

### Produces

- application/json

### Path parameters

- **tid** (required)

  Tenant ID

### Return type

array[DidTag]

### Example data

Content-Type: application/json

```
[ {
  "identifier" : "identifier",
  "tag" : "tag",
  "type" : "type",
  "tid" : "tid",
```

```
  "did" : 0,
  "ds" : "ds"
}, {
  "identifier" : "identifier",
  "tag" : "tag",
  "type" : "type",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
} ]
```

### Responses

```
200
```

successful operation

## GET /{tid}/did_tags/{ds}

### Produces

- application/json

### Path parameters

- **tid** (required)

  Tenant ID
- **ds** (required)

  Data Source

### Return type

array[DidTag]

### Example data

Content-Type: application/json

```
[ {
  "identifier" : "identifier",
  "tag" : "tag",
```

```
  "type" : "type",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
}, {
  "identifier" : "identifier",
  "tag" : "tag",
  "type" : "type",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
} ]
```

### Responses

```
200
```

successful operation

## GET /{tid}/did_tags/{ds}/{did}

### Produces

- application/json

### Path parameters

- **tid** (required)

  Tenant ID
- **ds** (required)

  Data Source
- **did** (required)

  Data Identifier

### Return type

array[DidTag]

### Example data

Content-Type: application/json

```
[ {
  "identifier" : "identifier",
  "tag" : "tag",
  "type" : "type",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
}, {
  "identifier" : "identifier",
  "tag" : "tag",
  "type" : "type",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
} ]
```


### Responses

```
200
```

successful operation

## GET /{tid}/did_tags/{ds}/{did}/{type}

### Produces

- application/json

### Path parameters

- **tid** (required)

  Tenant ID
- **ds** (required)

  Data Source
- **did** (required)

  Data Identifier
- **type** (required)

  Tag Type (i.e. 'did')

### Return type

array[DidTag]

### Example data

Content-Type: application/json

```
[ {
  "identifier" : "identifier",
  "tag" : "tag",
  "type" : "type",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
}, {
  "identifier" : "identifier",
  "tag" : "tag",
  "type" : "type",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
} ]
```

### Responses

```
200
```

successful operation

## GET /{tid}/did_tags/{ds}/{did}/{type}/{identifier}/{tag}

### Produces

- application/json

### Path parameters

- **tid** (required)

  Tenant ID

- **ds** (required)

Data Source

- **did** (required)

  Data Identifier

- **type** (required)

  Tag Type (i.e. 'did')

- **identifier** (required)

  Tag Key

- **tag** (required)

  Tag Value

### Return type

DidTag

### Example data

Content-Type: application/json

```
{
  "identifier" : "identifier",
  "tag" : "tag",
  "type" : "type",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
}
```

### Responses

```
200
```

successful operation

## GET /{tid}/did_tags/{ds}/{did}/{type}/{identifier}

### Produces

- application/json

## Path parameters

- **tid** (required)

  Tenant ID
- **ds** (required)

  Data Source
- **did** (required)

  Data Identifier
- **type** (required)

  Tag Type (i.e. 'did')
- **identifier** (required)

  Tag Key

## Return type

array[DidTag]

## Example data

Content-Type: application/json

```
[ {
  "identifier" : "identifier",
  "tag" : "tag",
  "type" : "type",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
}, {
  "identifier" : "identifier",
  "tag" : "tag",
  "type" : "type",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
} ]
```

## Responses

```
200
```

successful operation

# PUT /{tid}/did_tags/{ds}/{did}/{type}/{identifier}/{tag}

## Consumes

- application/json

## Produces

- application/json

## Path parameters

- **tid** (required)

  Tenant ID
- **ds** (required)

  Data Source
- **did** (required)

  Data Identifier
- **type** (required)

  Tag Type (i.e. 'did')
- **identifier** (required)

  Tag Key
- **tag** (required)

  Tag Value

## Request body

DidTag

## Responses

`default`

successful operation

# Entity Mappings

## POST /{tid}/entity_mappings

### Consumes

- application/json

### Produces

- application/json

### Path parameters

- **tid** (required)
  Tenant ID

### Request body

EntityMapping

### Responses

`default`

successful operation

## DELETE /{tid}/entity_mappings/{ds}/{did}/{entityType}/{entityId}

### Produces

- application/json

### Path parameters

- **tid** (required)
  Tenant ID
- **ds** (required)
  Data Source
- **did** (required)
  Data Identifier
- **entityType** (required)
  Entity Type
- **entityId** (required)
  Entity ID

### Responses

`default`

successful operation

## GET /{tid}/entity_mappings/{ds}/{did}/{entityType}

### Produces

- application/json

### Path parameters

- **tid** (required)
  Tenant ID
- **ds** (required)
  Data Source
- **did** (required)
  Data Identifier
- **entityType** (required)
  Entity Type

### Return type

array[EntityMapping]

### Example data

Content-Type: application/json

```
[ {
  "mapping" : "mapping",
  "entityType" : "entityType",
  "entityId" : "entityId",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
}, {
  "mapping" : "mapping",
  "entityType" : "entityType",
  "entityId" : "entityId",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
} ]
```

### Responses

```
200
```

successful operation

## GET /{tid}/entity_mappings/{ds}/{did}

### Produces

- application/json

### Path parameters

- **tid** (required)

  Tenant ID

- **ds** (required)

Data Source

- **did** (required)

  Data Identifier

### Return type

array[EntityMapping]

### Example data

Content-Type: application/json

```
[ {
  "mapping" : "mapping",
  "entityType" : "entityType",
  "entityId" : "entityId",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
}, {
  "mapping" : "mapping",
  "entityType" : "entityType",
  "entityId" : "entityId",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
} ]
```

### Responses

```
200
```

successful operation

## GET /{tid}/entity_mappings/{ds}

### Produces

- application/json

### Path parameters

- **tid** (required)

  Tenant ID
- **ds** (required)

  Data Source

### Return type

array[EntityMapping]

### Example data

Content-Type: application/json

```
[ {
  "mapping" : "mapping",
  "entityType" : "entityType",
  "entityId" : "entityId",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
}, {
  "mapping" : "mapping",
  "entityType" : "entityType",
  "entityId" : "entityId",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
} ]
```

### Responses

```
200
```

successful operation

## GET /{tid}/entity_mappings

### Produces

- application/json

### Path parameters

- **tid** (required)

  Tenant ID

### Return type

array[EntityMapping]

### Example data

Content-Type: application/json

```
[ {
  "mapping" : "mapping",
  "entityType" : "entityType",
  "entityId" : "entityId",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
}, {
  "mapping" : "mapping",
  "entityType" : "entityType",
  "entityId" : "entityId",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
} ]
```

### Responses

```
200
```

successful operation

## GET /{tid}/entity_mappings/{ds}/{did}/{entityType}/{entityId}

## Produces

- application/json

## Path parameters

- **tid** (required)

  Tenant ID
- **ds** (required)

  Data Source
- **did** (required)

  Data Identifier
- **entityType** (required)

  Entity Type
- **entityId** (required)

  Entity ID

## Return type

EntityMapping

## Example data

Content-Type: application/json

```
{
  "mapping" : "mapping",
  "entityType" : "entityType",
  "entityId" : "entityId",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
}
```

## Responses

```
200
```

successful operation

## PUT /{tid}/entity_mappings/{ds}/{did}/{entityType}/{entityId}

### Consumes

- application/json

### Produces

- application/json

### Path parameters

- **tid** (required)

  Tenant ID
- **ds** (required)

  Data Source
- **did** (required)

  Data Identifier
- **entityType** (required)

  Entity Type
- **entityId** (required)

  Entity ID

### Request body

EntityMapping

### Responses

`default`

successful operation

# Entity Tags

## POST /{tid}/entity_tags

### Consumes

- application/json

### Produces

- application/json

### Path parameters

- **tid** (required)
  Tenant ID

### Request body

EntityTag

### Responses

`default`

successful operation

## DELETE /{tid}/entity_tags/{ds}/{did}/{type}/{identifier}/{tag}

### Produces

- application/json

### Path parameters

- **tid** (required)
  Tenant ID
- **ds** (required)
  Data Source
- **did** (required)
  Data Identifier

- **type** (required)

  Tag Type (i.e. 'did')
- **identifier** (required)

  Tag Key
- **tag** (required)

  Tag Value

### Responses

`default`

successful operation

## GET /{tid}/entity_tags

### Produces

- application/json

### Path parameters

- **tid** (required)

  Tenant ID

### Return type

array[EntityTag]

### Example data

Content-Type: application/json

```
[ {
  "identifier" : "identifier",
  "tag" : "tag",
  "type" : "type",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
}, {
```

```
  "identifier" : "identifier",
  "tag" : "tag",
  "type" : "type",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
} ]
```

### Responses

```
200
```

successful operation

## GET /{tid}/entity_tags/{ds}

### Produces

- application/json

### Path parameters

- **tid** (required)

  Tenant ID
- **ds** (required)

  Data Source

### Return type

array[EntityTag]

### Example data

Content-Type: application/json

```
[ {
  "identifier" : "identifier",
  "tag" : "tag",
  "type" : "type",
  "tid" : "tid",
  "did" : 0,
```

```
  "ds" : "ds"
}, {
  "identifier" : "identifier",
  "tag" : "tag",
  "type" : "type",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
} ]
```

### Responses

```
200
```

successful operation

## GET /{tid}/entity_tags/{ds}/{did}

### Produces

- application/json

### Path parameters

- **tid** (required)

  Tenant ID
- **ds** (required)

  Data Source
- **did** (required)

  Data Identifier

### Return type

array[EntityTag]

### Example data

Content-Type: application/json

```
[ {
  "identifier" : "identifier",
```

```
  "tag" : "tag",
  "type" : "type",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
}, {
  "identifier" : "identifier",
  "tag" : "tag",
  "type" : "type",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
} ]
```

### Responses

```
200
```

successful operation

## GET /{tid}/entity_tags/{ds}/{did}/{type}

### Produces

- application/json

### Path parameters

- **tid** (required)

  Tenant ID
- **ds** (required)

  Data Source
- **did** (required)

  Data Identifier
- **type** (required)

  Tag Type (i.e. 'did')

### Return type

array[EntityTag]

### Example data

Content-Type: application/json

```
[ {
  "identifier" : "identifier",
  "tag" : "tag",
  "type" : "type",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
}, {
  "identifier" : "identifier",
  "tag" : "tag",
  "type" : "type",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
} ]
```

### Responses

```
200
```

successful operation

## GET /{tid}/entity_tags/{ds}/{did}/{type}/{identifier}/{tag}

### Produces

- application/json

### Path parameters

- **tid** (required)

  Tenant ID
- **ds** (required)

  Data Source
- **did** (required)

  Data Identifier

- **type** (required)

  Tag Type (i.e. 'did')
- **identifier** (required)

  Tag Key
- **tag** (required)

  Tag Value

### Return type

EntityTag

### Example data

Content-Type: application/json

```
{
  "identifier" : "identifier",
  "tag" : "tag",
  "type" : "type",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
}
```

### Responses

```
200
```

successful operation

## GET /{tid}/entity_tags/{ds}/{did}/{type}/{identifier}

### Produces

- application/json

### Path parameters

- **tid** (required)

  Tenant ID

- **ds** (required)

  Data Source
- **did** (required)

  Data Identifier
- **type** (required)

  Tag Type (i.e. 'did')
- **identifier** (required)

  Tag Key

### Return type

array[EntityTag]

### Example data

Content-Type: application/json

```
[ {
  "identifier" : "identifier",
  "tag" : "tag",
  "type" : "type",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
}, {
  "identifier" : "identifier",
  "tag" : "tag",
  "type" : "type",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
} ]
```

### Responses

```
200
```

successful operation

## PUT /{tid}/entity_tags/{ds}/{did}/{type}/{identifier}/{tag}

### Consumes

- application/json

### Produces

- application/json

### Path parameters

- **tid** (required)

  Tenant ID
- **ds** (required)

  Data Source
- **did** (required)

  Data Identifier
- **type** (required)

  Tag Type (i.e. 'did')
- **identifier** (required)

  Tag Key
- **tag** (required)

  Tag Value

### Request body

EntityTag

### Responses

`default`

successful operation

# Example Anomalies

## GET /{tid}/alert_templates/example/{anomaly_type}

## Produces

- application/json

## Path parameters

- **tid** (required)

  Tenant ID
- **anomaly_type** (required)

  Analytics Anomaly Type (i.e. 200)

## Return type

ExampleAnomaly

## Example data

Content-Type: application/json


```
{
  "exampleEndTimestamp" : "exampleEndTimestamp",
  "exampleEntityType" : "exampleEntityType",
  "exampleEntityHash" : "exampleEntityHash",
  "exampleEntityName" : "exampleEntityName",
  "exampleRisk" : 6.027456183070403,
  "exampleProbability" : 1.4658129805029452,
  "exampleObserved" : 5.962133916683182,
  "exampleBaseline" : 5.637376656633329,
  "exampleIdHash" : "exampleIdHash",
  "tid" : "tid",
  "exampleTimestamp" : "exampleTimestamp",
  "exampleRelation" : "exampleRelation",
  "exampleIdName" : "exampleIdName",
  "exampleDid" : 0,
  "exampleAssociatedEntities" : "exampleAssociatedEntities",
  "exampleAnomalyType" : "exampleAnomalyType",
  "exampleIdType" : "exampleIdType"
}
```


## Responses

```
200
```

successful operation

# Field Mappings

## POST /{tid}/field_mappings

### Consumes

- application/json

### Produces

- application/json

### Path parameters

- **tid** (required)
  Tenant ID

### Request body

FieldMapping

### Responses

`default`

successful operation

## DELETE /{tid}/field_mappings/{ds}/{did}/{field}

### Produces

- application/json

### Path parameters

- **tid** (required)
  Tenant ID
- **ds** (required)
  Data Source
- **did** (required)
  Data Identifier
- **field** (required)
  Interset Field Name

### Responses

`default`

successful operation

## GET /{tid}/field_mappings/{ds}/{did}/{field}

### Produces

- application/json

### Path parameters

- **tid** (required)
  Tenant ID
- **ds** (required)
  Data Source
- **did** (required)
  Data Identifier
- **field** (required)
  Interset Field Name

### Return type

FieldMapping

### Example data

Content-Type: application/json

```
{
  "mappings" : "mappings",
  "field" : "field",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
}
```

### Responses

```
200
```

successful operation

## GET /{tid}/field_mappings

### Produces

- application/json

### Path parameters

- **tid** (required)

  Tenant ID

### Return type

array[FieldMapping]

### Example data

Content-Type: application/json

```
[ {
  "mappings" : "mappings",
  "field" : "field",
  "tid" : "tid",
  "did" : 0,
```

```
  "ds" : "ds"
}, {
  "mappings" : "mappings",
  "field" : "field",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
} ]
```

### Responses

```
200
```

successful operation

## GET /{tid}/field_mappings/{ds}

### Produces

- application/json

### Path parameters

- **tid** (required)

  Tenant ID
- **ds** (required)

  Data Source

### Return type

array[FieldMapping]

### Example data

Content-Type: application/json

```
[ {
  "mappings" : "mappings",
  "field" : "field",
  "tid" : "tid",
  "did" : 0,
```

```
  "ds" : "ds"
}, {
  "mappings" : "mappings",
  "field" : "field",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
} ]
```

### Responses

```
200
```

successful operation

## GET /{tid}/field_mappings/{ds}/{did}

### Produces

- application/json

### Path parameters

- **tid** (required)

  Tenant ID
- **ds** (required)

  Data Source
- **did** (required)

  Data Identifier

### Return type

array[FieldMapping]

### Example data

Content-Type: application/json

```
[ {
  "mappings" : "mappings",
  "field" : "field",
```

```
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
}, {
  "mappings" : "mappings",
  "field" : "field",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
} ]
```

### Responses

```
200
```

successful operation

## PUT /{tid}/field_mappings/{ds}/{did}/{field}

### Produces

- application/json

### Path parameters

- **tid** (required)

  Tenant ID
- **ds** (required)

  Data Source
- **did** (required)

  Data Identifier
- **field** (required)

  Interset Field Name

### Request body

FieldMapping

### Responses

`default`

successful operation

# Importance

## POST /{tid}/importance

### Consumes

- application/json

### Produces

- application/json

### Path parameters

- **tid** (required)
  Tenant ID

### Request body

Importance

### Responses

`default`

successful operation

## DELETE /{tid}/importance/{entityType}/{entityId}

### Produces

- application/json

### Path parameters

- **tid** (required)

  Tenant ID
- **entityType** (required)

  Entity Type
- **entityId** (required)

  Entity ID

### Responses

`default`

successful operation

## GET /{tid}/importance/{entityType}/{entityId}

### Produces

- application/json

### Path parameters

- **tid** (required)

  Tenant ID
- **entityType** (required)

  Entity Type
- **entityId** (required)

  Entity ID

### Return type

Importance

### Example data

Content-Type: application/json

```
{
  "score" : 0.8008281904610115,
  "entityType" : "entityType",
  "entityId" : "entityId",
  "tid" : "tid",
  "timestamp" : "2000-01-23T04:56:07.000+00:00"
}
```

### Responses

```
200
```

successful operation

## GET /{tid}/importance

### Produces

- application/json

### Path parameters

- **tid** (required)

  Tenant ID

### Return type

array[Importance]

### Example data

Content-Type: application/json

```
[ {
  "score" : 0.8008281904610115,
  "entityType" : "entityType",
  "entityId" : "entityId",
  "tid" : "tid",
```

```
  "timestamp" : "2000-01-23T04:56:07.000+00:00"
}, {
  "score" : 0.8008281904610115,
  "entityType" : "entityType",
  "entityId" : "entityId",
  "tid" : "tid",
  "timestamp" : "2000-01-23T04:56:07.000+00:00"
} ]
```

### Responses

```
200
```

successful operation

## GET /{tid}/importance/{entityType}

### Produces

- application/json

### Path parameters

- **tid** (required)

  Tenant ID
- **entityType** (required)

  Entity Type

### Return type

array[Importance]

### Example data

Content-Type: application/json

```
[ {
  "score" : 0.8008281904610115,
  "entityType" : "entityType",
  "entityId" : "entityId",
  "tid" : "tid",
```

```
  "timestamp" : "2000-01-23T04:56:07.000+00:00"
}, {
  "score" : 0.8008281904610115,
  "entityType" : "entityType",
  "entityId" : "entityId",
  "tid" : "tid",
  "timestamp" : "2000-01-23T04:56:07.000+00:00"
} ]
```


### Responses

```
200
```

successful operation

## PUT /{tid}/importance/{entityType}/{entityId}

### Consumes

- application/json

### Produces

- application/json

### Path parameters

- **tid** (required)

  Tenant ID
- **entityType** (required)

  Entity Type
- **entityId** (required)

  Entity ID

### Request body

Importance

### Responses

`default`

successful operation

# Parameters

## POST /{tid}/parameters

### Consumes

- application/json

### Produces

- application/json

### Path parameters

- **tid** (required)
  Tenant ID

### Request body

Parameter

### Responses

`default`

successful operation

## DELETE /{tid}/parameters/{name}

### Produces

- application/json

### Path parameters

- **tid** (required)

  Tenant ID
- **name** (required)

  Parameter Name

### Responses

`default`

successful operation

## GET /{tid}/parameters/{name}

### Produces

- application/json

### Path parameters

- **tid** (required)

  Tenant ID
- **name** (required)

  Parameter Name

### Return type

Parameter

### Example data

Content-Type: application/json

```
{
  "name" : "name",
  "value" : 0.8008281904610115,
  "tid" : "tid"
}
```

### Responses

```
200
```

successful operation

## GET /{tid}/parameters

### Produces

- application/json

### Path parameters

- **tid** (required)

  Tenant ID

### Return type

array[Parameter]

### Example data

Content-Type: application/json

```
[ {
  "name" : "name",
  "value" : 0.8008281904610115,
  "tid" : "tid"
}, {
  "name" : "name",
  "value" : 0.8008281904610115,
  "tid" : "tid"
} ]
```

### Responses

`200`

successful operation

## PUT /{tid}/parameters/{name}

### Consumes

- application/json

### Produces

- application/json

### Path parameters

- **tid** (required)
  Tenant ID
- **name** (required)
  Parameter Name

### Request body

Parameter

### Responses

`default`

successful operation

# Relation Tags

## POST /{tid}/relation_tags

### Consumes

- application/json

### Produces

- application/json

### Path parameters

- **tid** (required)
  Tenant ID

### Request body

RelationTag

### Responses

`default`

successful operation

## DELETE /{tid}/relation_tags/{ds}/{did}/{type}/{identifier}/{tag}

### Produces

- application/json

### Path parameters

- **tid** (required)
  Tenant ID
- **ds** (required)
  Data Source
- **did** (required)
  Data Identifier
- **type** (required)

Tag Type (i.e. 'did')

- **identifier** (required)

  Tag Key

- **tag** (required)

  Tag Value

### Responses

`default`

successful operation

## GET /{tid}/relation_tags

### Produces

- application/json

### Path parameters

- **tid** (required)

  Tenant ID

### Return type

array[RelationTag]

### Example data

Content-Type: application/json

```
[ {
  "identifier" : "identifier",
  "tag" : "tag",
  "type" : "type",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
}, {
  "identifier" : "identifier",
  "tag" : "tag",
```

```
  "type" : "type",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
} ]
```

### Responses

```
200
```

successful operation

## GET /{tid}/relation_tags/{ds}

### Produces

- application/json

### Path parameters

- **tid** (required)

  Tenant ID
- **ds** (required)

  Data Source

### Return type

array[RelationTag]

### Example data

Content-Type: application/json

```
[ {
  "identifier" : "identifier",
  "tag" : "tag",
  "type" : "type",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
}, {
```

```
  "identifier" : "identifier",
  "tag" : "tag",
  "type" : "type",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
} ]
```

### Responses

```
200
```

successful operation

## GET /{tid}/relation_tags/{ds}/{did}

### Produces

- application/json

### Path parameters

- **tid** (required)

  Tenant ID
- **ds** (required)

  Data Source
- **did** (required)

  Data Identifier

### Return type

array[RelationTag]

### Example data

Content-Type: application/json

```
[ {
  "identifier" : "identifier",
  "tag" : "tag",
  "type" : "type",
```

```
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
}, {
  "identifier" : "identifier",
  "tag" : "tag",
  "type" : "type",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
} ]
```

### Responses

```
200
```

successful operation

## GET /{tid}/relation_tags/{ds}/{did}/{type}

### Produces

- application/json

### Path parameters

- **tid** (required)

  Tenant ID
- **ds** (required)

  Data Source
- **did** (required)

  Data Identifier
- **type** (required)

  Tag Type (i.e. 'did')

### Return type

array[RelationTag]

### Example data

Content-Type: application/json

```
[ {
  "identifier" : "identifier",
  "tag" : "tag",
  "type" : "type",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
}, {
  "identifier" : "identifier",
  "tag" : "tag",
  "type" : "type",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
} ]
```

### Responses

```
200
```

successful operation

## GET /{tid}/relation_tags/{ds}/{did}/{type}/{identifier}/{tag}

### Produces

- application/json

### Path parameters

- **tid** (required)

  Tenant ID
- **ds** (required)

  Data Source
- **did** (required)

  Data Identifier

- **type** (required)

  Tag Type (i.e. 'did')
- **identifier** (required)

  Tag Key
- **tag** (required)

  Tag Value

### Return type

RelationTag

### Example data

Content-Type: application/json

```
{
  "identifier" : "identifier",
  "tag" : "tag",
  "type" : "type",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
}
```

### Responses

```
200
```

successful operation

## GET /{tid}/relation_tags/{ds}/{did}/{type}/{identifier}

### Produces

- application/json

### Path parameters

- **tid** (required)

  Tenant ID

- **ds** (required)

  Data Source
- **did** (required)

  Data Identifier
- **type** (required)

  Tag Type (i.e. 'did')
- **identifier** (required)

  Tag Key

### Return type

array[RelationTag]

### Example data

Content-Type: application/json

```
[ {
  "identifier" : "identifier",
  "tag" : "tag",
  "type" : "type",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
}, {
  "identifier" : "identifier",
  "tag" : "tag",
  "type" : "type",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
} ]
```

### Responses

```
200
```

successful operation

## PUT /{tid}/relation_tags/{ds}/{did}/{type}/{identifier}/{tag}

### Consumes

- application/json

### Produces

- application/json

### Path parameters

- **tid** (required)
  Tenant ID
- **ds** (required)
  Data Source
- **did** (required)
  Data Identifier
- **type** (required)
  Tag Type (i.e. 'did')
- **identifier** (required)
  Tag Key
- **tag** (required)
  Tag Value

### Request body

RelationTag

### Responses

`default`

successful operation

# Subqueries

## POST /{tid}/subqueries

### Consumes

- application/json

### Produces

- application/json

### Path parameters

- **tid** (required)
  Tenant ID

### Request body

Subquery

### Responses

`default`

successful operation

## DELETE /{tid}/subqueries/{ds}/{did}

### Consumes

- application/json

### Produces

- application/json

### Path parameters

- **tid** (required)
  Tenant ID
- **ds** (required)
  Data Source

- **did** (required)

  Data Identifier

### Responses

`default`

successful operation

## GET /{tid}/subqueries

### Produces

- application/json

### Path parameters

- **tid** (required)

  Tenant ID

### Return type

array[Subquery]

### Example data

Content-Type: application/json

```
[ {
  "subquery" : "subquery",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
}, {
  "subquery" : "subquery",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
} ]
```

### Responses

`200`

successful operation

## GET /{tid}/subqueries/{ds}

### Produces

- application/json

### Path parameters

- **tid** (required)

  Tenant ID
- **ds** (required)

  Data Source

### Return type

array[Subquery]

### Example data

Content-Type: application/json

```
[ {
  "subquery" : "subquery",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
}, {
  "subquery" : "subquery",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
} ]
```

### Responses

```
200
```

successful operation

# GET /{tid}/subqueries/{ds}/{did}

## Produces

- application/json

## Path parameters

- **tid** (required)

  Tenant ID
- **ds** (required)

  Data Source
- **did** (required)

  Data Identifier

## Return type

Subquery

## Example data

Content-Type: application/json

```
{
  "subquery" : "subquery",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
}
```

## Responses

```
200
```

successful operation

# PUT /{tid}/subqueries/{ds}/{did}

### Consumes

- application/json

### Produces

- application/json

### Path parameters

- **tid** (required)
  Tenant ID
- **ds** (required)
  Data Source
- **did** (required)
  Data Identifier

### Request body

Subquery

### Responses

`default`

successful operation

# Violations

## GET /{tid}/violations/{violationName}

### Produces

- application/json

### Path parameters

- **tid** (required)

  Tenant ID
- **violationName** (required)

  Alert Name

### Return type

array[AlertsMeta]

### Example data

Content-Type: application/json

```
[ {
  "alertType" : "alertType",
  "alertName" : "alertName",
  "anomalyType" : 6,
  "timeBucket" : "timeBucket",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
}, {
  "alertType" : "alertType",
  "alertName" : "alertName",
  "anomalyType" : 6,
  "timeBucket" : "timeBucket",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
} ]
```

### Responses

```
200
```

successful operation

## GET /{tid}/violations

### Produces

- application/json

### Path parameters

- **tid** (required)

  Tenant ID

### Return type

array[AlertsMeta]

### Example data

Content-Type: application/json

```
[ {
  "alertType" : "alertType",
  "alertName" : "alertName",
  "anomalyType" : 6,
  "timeBucket" : "timeBucket",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
}, {
  "alertType" : "alertType",
  "alertName" : "alertName",
  "anomalyType" : 6,
  "timeBucket" : "timeBucket",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
} ]
```

### Responses

```
200
```

successful operation

## POST /{tid}/violations/register

*Register Violation.*

### Consumes

- application/json

### Produces

- application/json

### Path parameters

- **tid** (required)
  Tenant ID

### Request body

AlertsMetaViolations

### Responses

`default`

successful operation

## Weights

## POST /{tid}/weights

### Consumes

- application/json

### Produces

- application/json

### Path parameters

- **tid** (required)
  Tenant ID

### Request body

Weight

### Responses

`default`

successful operation

## DELETE /{tid}/weights/{did}/{anomalyType}

### Produces

- application/json

### Path parameters

- **tid** (required)

  Tenant ID
- **did** (required)

  Data Identifier
- **anomalyType** (required)

  Analytics Anomaly Type (i.e. 200)

### Responses

`default`

successful operation

## GET /{tid}/weights/{did}/{anomalyType}

### Produces

- application/json

### Path parameters

- **tid** (required)

  Tenant ID
- **did** (required)

  Data Identifier
- **anomalyType** (required)

  Analytics Anomaly Type (i.e. 200)

### Return type

Weight

### Example data

Content-Type: application/json

```
{
  "anomalyType" : 6,
  "importance" : 5.637376656633329,
  "weight" : 1.4658129805029452,
  "probabilityThreshold" : 2.3021358869347655,
  "tid" : "tid",
  "did" : 0,
  "defaultWeight" : 5.962133916683182
}
```

### Responses

```
200
```

successful operation

## GET /{tid}/weights

### Produces

- application/json

### Path parameters

- **tid** (required)

  Tenant ID

### Return type

array[Weight]

### Example data

Content-Type: application/json


```
[ {
  "anomalyType" : 6,
  "importance" : 5.637376656633329,
  "weight" : 1.4658129805029452,
  "probabilityThreshold" : 2.3021358869347655,
  "tid" : "tid",
  "did" : 0,
  "defaultWeight" : 5.962133916683182
}, {
  "anomalyType" : 6,
  "importance" : 5.637376656633329,
  "weight" : 1.4658129805029452,
  "probabilityThreshold" : 2.3021358869347655,
  "tid" : "tid",
  "did" : 0,
  "defaultWeight" : 5.962133916683182
} ]
```


### Responses

```
200
```

successful operation

## GET /{tid}/weights/{did}

### Produces

- application/json

### Path parameters

- **tid** (required)

  Tenant ID
- **did** (required)

  Data Identifier

### Return type

array[Weight]

### Example data

Content-Type: application/json

```
[ {
  "anomalyType" : 6,
  "importance" : 5.637376656633329,
  "weight" : 1.4658129805029452,
  "probabilityThreshold" : 2.3021358869347655,
  "tid" : "tid",
  "did" : 0,
  "defaultWeight" : 5.962133916683182
}, {
  "anomalyType" : 6,
  "importance" : 5.637376656633329,
  "weight" : 1.4658129805029452,
  "probabilityThreshold" : 2.3021358869347655,
  "tid" : "tid",
  "did" : 0,
  "defaultWeight" : 5.962133916683182
} ]
```

### Responses

```
200
```

successful operation

## PUT /{tid}/weights/{did}/{anomalyType}

### Consumes

- application/json

### Produces

- application/json

### Path parameters

- **tid** (required)

  Tenant ID
- **did** (required)

  Data Identifier
- **anomalyType** (required)

  Analytics Anomaly Type (i.e. 200)

### Request body

Weight

### Responses

`default`

successful operation

# Models

## AlertTemplate

- **tid** -- String
- **did** -- Integer

  Format: int32
- **anomalyType** -- String

- **datasource** -- String
- **threatName** -- String
- **threatDescription** -- String
- **familyName** -- String
- **unitName** -- String
- **unitType** -- String
- **unitDescription** -- String
- **templatesTeaser** -- String
- **templatesAlert** -- String
- **templatesThreat** -- String
- **templatesFamily** -- String
- **templatesTooltip** -- String
- **reconSearchQuery** -- String
- **reconStartTime** -- String
- **reconEndTime** -- String
- **bucketSize** -- String
- **contextType** -- String
- **genericSearchQuery** -- String
- **genericTimeRangeQuery** -- String
- **sqlSearchQuery** -- String
- **hasAggregatedIdentifiers** -- Boolean

## AlertsMeta

- **tid** -- String
- **ds** -- String
- **did** -- Integer

Format: int32

- **alertType** -- String
- **alertName** -- String
- **timeBucket** -- String
- **anomalyType** -- Integer
  Format: int32

## AlertsMetaSimple

- **tid** -- String
- **ds** -- String
- **did** -- Integer
  Format: int32
- **alertName** -- String
- **timeBucket** -- String

## AlertsMetaViolations

- **tid** -- String
- **ds** -- String
- **did** -- Integer
  Format: int32
- **alertName** -- String
- **timeBucket** -- String
- **severity** -- String

## AnomalyMeta

- **tid** -- String
- **anomalyType** -- Integer
  Format: int32
- **timeBucket** -- String

## ByomMeta

- **tid** -- String
- **ds** -- String
- **did** -- Integer
  Format: int32
- **modelName** -- String
- **timeBucket** -- String
- **primEntitytype** -- String
- **secEntitytype** -- String
- **primEntityCol** -- String
- **secEntityCol** -- String
- **isActive** -- Boolean
- **targetClass** -- String

## ByomMetaAnomalytype

- **tid** -- String
- **ds** -- String
- **did** -- Integer
  Format: int32
- **modelName** -- String
- **timeBucket** -- String

- **primEntitytype** -- String
- **secEntitytype** -- String
- **primEntityCol** -- String
- **secEntityCol** -- String
- **isActive** -- Boolean
- **targetClass** -- String
- **anomalyType** -- Integer
  Format: int32

## DidTag

- **tid** -- String
- **ds** -- String
- **did** -- Integer
  Format: int32
- **type** -- String
- **identifier** -- String
- **tag** -- String

## EntityMapping

- **tid** -- String
- **ds** -- String
- **did** -- Integer
  Format: int32
- **entityType** -- String
- **entityId** -- String
- **mapping** -- String

## EntityTag

- **tid** -- String
- **ds** -- String
- **did** -- Integer
  Format: int32
- **type** -- String
- **identifier** -- String
- **tag** -- String

## ExampleAnomaly

- **tid** -- String
- **exampleAnomalyType** -- String
- **exampleDid** -- Integer
  Format: int32
- **exampleTimestamp** -- String
- **exampleRisk** -- Double
  Format: double
- **exampleProbability** -- Double
  Format: double
- **exampleObserved** -- Double
  Format: double
- **exampleBaseline** -- Double
  Format: double
- **exampleRelation** -- String
- **exampleEntityName** -- String
- **exampleEntityHash** -- String
- **exampleEntityType** -- String

- **exampleIdName** -- String
- **exampleIdHash** -- String
- **exampleIdType** -- String
- **exampleEndTimestamp** -- String
- **exampleAssociatedEntities** -- String

## FieldMapping

- **tid** -- String
- **ds** -- String
- **did** -- Integer
  Format: int32
- **field** -- String
- **mappings** -- String

## Importance

- **tid** -- String
- **entityType** -- String
- **entityId** -- String
- **score** -- Double
  Format: double
- **timestamp** -- Date
  Format: date-time

## Parameter

- **tid** -- String
- **name** -- String

- **value** -- Double
  Format: double

## RelationTag

- **tid** -- String
- **ds** -- String
- **did** -- Integer
  Format: int32
- **type** -- String
- **identifier** -- String
- **tag** -- String

## Subquery

- **tid** -- String
- **ds** -- String
- **did** -- Integer
  Format: int32
- **subquery** -- String

## Weight

- **tid** -- String
- **did** -- Integer
  Format: int32
- **anomalyType** -- Integer
  Format: int32
- **weight** -- Double

Format: double

- **defaultWeight** -- Double

  Format: double

- **importance** -- Double

  Format: double

- **probabilityThreshold** -- Double

  Format: double

# Analytics API Reference

Version: 24.1

BasePath: /interset/api

## actions

### POST /actions/login

*Log in*

Authenticates and creates a new session for the specified user identifier and password. Returns a JSON structure containing an access token and the token type.

#### Consumes

- application/json

#### Produces

- application/json

#### Request body

ApiCredentials

#### Return type

LoginResponse

### Example data

Content-Type: application/json

```
{
  "access_token" : "802BR4y-kajOPE4agOR_d4RaE-Ja",
  "token_type" : "Bearer"
}
```

### Responses

```
200
```

successful operation

## GET /actions/logoff

*Log off*

Ends the specified user session. Expects an Authorization header containing the string "<token_type>: <access_token>".The token_type is typically "Bearer".

### Consumes

- application/json

### Produces

- application/json

### Request headers

- **Authorization** (optional) -- String

### Return type

ApiAction

### Example data

Content-Type: application/json

```
{
  "success" : true,
  "detail" : "logged off"
}
```

### Responses

`200`

successful operation

## GET /actions/logoff/saml

*Log off (SAML)*

Expects an Authorization header containing the string "`<token_type>: <access_token>`". You can get both of these using the `/actions/login/saml` method. The token_type is typically `"Bearer"`.

This method redirects requests to the SAML logout URL.

### Consumes

- application/json

### Produces

- application/json

### Request headers

- **Authorization** (optional) -- String

### Query parameters

- **relayState** (optional)

### Responses

`default`

successful operation

# GET /actions/login/oauth2

*Login (OAuth2)*

Login API for OAuth2

## Consumes

- application/json

## Produces

- application/json

## Query parameters

- **relayState** (optional)

## Responses

`default`

successful operation

# GET /actions/login/oauth2/callback

*CallBack URI (OAuth2)*

This is callback handler which is registered with OAuth2 provider and this handler will be called with authcode and state info

## Consumes

- application/json

## Produces

- application/json

### Query parameters

- **code** (optional)
- **state** (optional)

### Responses

`default`

successful operation

## GET /actions/logoff/oauth2

*Log off (OAuth2)*

Revokes refresh token and invalidates all the sessions and cookies

### Consumes

- application/json

### Produces

- application/json

### Request headers

- **Authorization** (optional) -- String

### Query parameters

- **relayState** (optional)

### Responses

`default`

successful operation

## GET /actions/login/oauth2/renew

*Renew Token (OAuth2)*

Generates new access token using refresh token. Sets Interset Cookie and Authorization header with new access token

## Consumes

- application/json

## Produces

- application/json

## Request headers

- **Authorization** (optional) -- String

## Responses

```
default
```

successful operation

# GET /actions/login/saml

*Get SAML login page*

Returns an HTML document that loads a SAML login page and redirects the user to the requested path, if that path is valid.

## Example Response (Status 200)

```
<html><head></head><body><form id='TheForm'
action='https://company.okta.com/app/investigator/katex9fJY47c0Kh7ij90/sso/saml'
method='POST'><input type='hidden' id='SAMLRequest' name='SAMLRequest'
value='PD94bWwgdmhbWwycDbolj0iMS4wIiBlbmNvZGluZzlVyc2lvbKPHNJpBdXR0iVVRGLTgiPz4cXVl
c3QgQXNzZXJ0aW9uQ29uc3VtZXJTZXJ2aWNlVVJMPSJodHRwczovL3FhLWNvczcyLWNub2RlLmFk
LmludGVyc2V0LmNvbS9hcGkvYWN0aW9ucy9sb2dpbi9zYW1sL3NzbyIgSUQ9InphODkwYjg5My0z
ODFhLTQ3MWQtYTZkOS05NzVkN2EwNTllNmIiIElzc3VlSW5zdGFudD0iMjAxNy0wOS0yOVQxOToz
NTowMC4yMjlaIiBQcm90b2NvbEJpbmRpbmc9InVybjpvYXNpczpuYW1lczp0YzpTQU1MOjIuMDpi
aW5kaW5nczpIVFRQLVBPU1QiIFZlcnNpb249IjIuMCIgeG1sbnM6c2FtbDJwPSJ1cm46b2FzaXM6
bmFtZXM6dGM6U0FNTDoyLjA6cHJvdG9jb2wiPjxzYW1sMjpJc3N1ZXIgeG1sbnM6c2FtbDI9InVy
bjpvYXNpczpuYW1lczp0YzpTQU1MOjIuMDphc3NlcnRpb24iPkludmVzdGlnYXRvcjwvc2FtbDI6
SXNzdWVyPjxzYW1sMnA6TmFtZUlEUG9saWN5IEZvcm1hdD0idXJuOm9hc2lzOm5hbWVzOnRjOlNB
TUw6MS4xOm5hbWVpZC1mb3JtYXQ6dW5zcGVjaWZpZWQiLz48L3NhbWxwcDpBdXRoblJlcXVlc3Q+'/><input
```

```
type='hidden' id='RelayState' name='RelayState' value='/interset'/></form><script
type='text/javascript'>document.getElementById('TheForm').submit
();</script></body></html>
```

### Consumes

- application/json

### Produces

- application/json

### Query parameters

- **relayState** (optional)

  The path where the user should be redirected once authenticated.

### Responses

```
default
```

successful operation

## POST /actions/login/saml/sso

*Log in (SAML SSO)*

Expects an IDP generated SAML response. Processes a signed SAML response.

### Consumes

- application/x-www-form-urlencoded

### Produces

- application/json

### Form parameters

- **SAMLResponse** (optional)
- **RelayState** (optional)

  The path where the user should be redirected once authenticated.

### Responses

`default`

successful operation

# dashboards{tenantId}

## POST /dashboards/{tid}

*Add a dashboard*

Creates a new dashboard for the currently logged-in user.

### Example Request Body

```
{
  "doc":"{"title":"Overall Risk 2","layouts":[{"x":0,"y":0,"w":3,"h":16,"setting":
{"panelName":"MatrixVisualization"}}]}",
  "description":"This is my second dashboard",
  "name":"Overall Risk 2",
  "private":false
}
```

### Consumes

- application/json

### Produces

- application/json

### Path parameters

- **tid** (required)

  The tenant ID.

### Request body

ApiSimpleDashboard

### Return type

ApiDashboard

### Example data

Content-Type: application/json

```
{
  "private" : true,
  "lastModifiedDate" : "2000-01-23T04:56:07.000+00:00",
  "lastModifiedBy" : "lastModifiedBy",
  "name" : "name",
  "doc" : "doc",
  "description" : "description",
  "id" : 0,
  "creationDate" : "2000-01-23T04:56:07.000+00:00",
  "userId" : "userId",
  "tid" : "tid",
  "home" : true,
  "tags" : [ {
    "name" : "recon",
    "id" : "46b489f7f46588c6"
  }, {
    "name" : "recon",
    "id" : "46b489f7f46588c6"
  } ]
}
```

### Responses

```
200
```

successful operation

## PUT /dashboards/{tid}/tags/{id}

*Attach a tag to a dashboard*

Attaches a new tag

### Example Request Body

```
{
  "name": "newTag",
}
```

### Produces

- application/json

### Path parameters

- **tid** (required)

  The tenant ID.
- **id** (required)

  The dashboard ID.

### Request body

ApiSimpleDashboardTag

### Responses

`default`

successful operation

## DELETE /dashboards/{tid}/tags/{id}

*Detach tag from dashboard*

Removes specified tag from dashboard

### Produces

- application/json

### Path parameters

- **tid** (required)

  The tenant ID.

- **id** (required)

### Responses

```
default
```

successful operation

## GET /dashboards/{tid}/{id}

*Get a dashboard*

Returns the JSON representation of the dashboard with the specified ID.

### Example Response (Status 200)


```
{
  "doc":"{"title":"Overall Risk 2","layouts":[{"x":0,"y":0,"w":3,"h":16,"setting":
{"panelName":"MatrixVisualization"}}]}",
  "name":"Overall Risk 2",
  "description":"This is my second dashboard",
  "tid":"0",
  "userId":"admin",
  "id":78,
  "lastModifiedBy":"admin",
  "creationDate":"2018-11-22",
  "lastModifiedDate":"2018-11-22",
  "home":null,
  "private":false
}
```


### Produces

- application/json

### Path parameters

- **tid** (required)

  The tenant ID.
- **id** (required)

  The dashboard ID.

### Return type

ApiDashboard

### Example data

Content-Type: application/json

```
{
  "private" : true,
  "lastModifiedDate" : "2000-01-23T04:56:07.000+00:00",
  "lastModifiedBy" : "lastModifiedBy",
  "name" : "name",
  "doc" : "doc",
  "description" : "description",
  "id" : 0,
  "creationDate" : "2000-01-23T04:56:07.000+00:00",
  "userId" : "userId",
  "tid" : "tid",
  "home" : true,
  "tags" : [ {
    "name" : "recon",
    "id" : "46b489f7f46588c6"
  }, {
    "name" : "recon",
    "id" : "46b489f7f46588c6"
  } ]
}
```

### Responses

```
200
```

successful operation

## GET /dashboards/{tid}

*Get a list of dashboards*

Returns all public dashboards for the tenant, as well as the logged-in user's private dashboards.

## Example Response (Status 200)


```
[
   {
      "doc":null,
      "name":"Overall Risk 2",
      "description":"description":"This is my second dashboard",
      "tid":null,
      "userId":"admin",
      "id":78,
      "lastModifiedBy":"admin",
      "creationDate":"2018-11-22",
      "lastModifiedDate":"2018-11-22",
      "home":false,
      "tags":[
        {
          "name":"addedTag",
          "id":"4"
        }
      ],
      "private":false
   },
   {
      "doc":null,
      "name":"Breakdown Dashboard",
      "description":"description":"This is my breakdown dashboard",
      "tid":"0",
      "userId":"admin",
      "id":79,
      "lastModifiedBy":"admin",
      "creationDate":"2018-11-10",
      "lastModifiedDate":"2018-11-10",
      "home":true,
      "tags": [],
      "private":false
   }
]
```


## Produces

- application/json

## Path parameters

- **tid** (required)

  The tenant ID.

## Return type

array[ApiDashboard]

## Example data

Content-Type: application/json


```
[ {
  "private" : true,
  "lastModifiedDate" : "2000-01-23T04:56:07.000+00:00",
  "lastModifiedBy" : "lastModifiedBy",
  "name" : "name",
  "doc" : "doc",
  "description" : "description",
  "id" : 0,
  "creationDate" : "2000-01-23T04:56:07.000+00:00",
  "userId" : "userId",
  "tid" : "tid",
  "home" : true,
  "tags" : [ {
    "name" : "recon",
    "id" : "46b489f7f46588c6"
  }, {
    "name" : "recon",
    "id" : "46b489f7f46588c6"
  } ]
}, {
  "private" : true,
  "lastModifiedDate" : "2000-01-23T04:56:07.000+00:00",
  "lastModifiedBy" : "lastModifiedBy",
  "name" : "name",
  "doc" : "doc",
  "description" : "description",
  "id" : 0,
  "creationDate" : "2000-01-23T04:56:07.000+00:00",
  "userId" : "userId",
  "tid" : "tid",
  "home" : true,
  "tags" : [ {
    "name" : "recon",
    "id" : "46b489f7f46588c6"
  }, {
    "name" : "recon",
    "id" : "46b489f7f46588c6"
```

```
  } ]
} ]
```

## Responses

```
200
```

successful operation

# GET /dashboards/{tid}/home

*Get home dashboard*

Returns the JSON representation of the home dashboard for the logged-in user.

## Example Response (Status 200)

```
{
  "doc":"{"title":"Overall Risk 2","layouts":[{"x":0,"y":0,"w":3,"h":16,"setting":
{"panelName":"MatrixVisualization"}}]}",
  "name":"Overall Risk 2",
  "description":"This is my second dashboard",
  "tid":"0",
  "userId":"admin",
  "id":78,
  "lastModifiedBy":"admin",
  "creationDate":"2018-11-22",
  "lastModifiedDate":"2018-11-22",
  "home":null,
  "private":false
}
```

## Produces

- application/json

## Path parameters

- **tid** (required)

  The tenant ID.

## Responses

```
default
```

successful operation

# GET /dashboards/{tid}/tags

*Get a list of tags*

Gets all tags for the tenant

## Example Request Body

```
[
   {
      "name":"Aiden",
      "id":"4"
   },
   {
      "name": "Bryan",
      "id": "2"
   }]
```

## Produces

- application/json

## Path parameters

- **tid** (required)

  The tenant ID.

## Return type

array[ApiDashboardTag]

## Example data

Content-Type: application/json

```
[ {
  "name" : "recon",
  "id" : "46b489f7f46588c6"
}, {
  "name" : "recon",
  "id" : "46b489f7f46588c6"
} ]
```

### Responses

`200`

successful operation

## DELETE /dashboards/{tid}/{id}

*Delete a dashboard*

Deletes the dashboard with the specified ID. You must have the permissions required to delete the specified dashboard.

### Produces

- application/json

### Path parameters

- **tid** (required)

  The tenant ID.
- **id** (required)

### Responses

`default`

successful operation

## DELETE /dashboards/{tid}/home

*Reset home dashboard*

Resets the home dashboard for the currently logged-in user.

### Produces

- application/json

### Path parameters

- **tid** (required)

  The tenant ID.

### Responses

`default`

successful operation

## PUT /dashboards/{tid}/home/{id}

*Update home dashboard*

Sets the dashboard with the specified ID to be the home dashboard for the logged-in user.

### Produces

- application/json

### Path parameters

- **tid** (required)

  The tenant ID.
- **id** (required)

  The dashboard ID.

### Responses

`default`

successful operation

## PUT /dashboards/{tid}/{id}

*Update a dashboard*

Updates the dashboard with the specified ID. You must have the permissions required to update the specified dashboard.

## Example Request Body


```
{
  "doc":"{"title":"Overall Risk 2","layouts":[{"x":0,"y":0,"w":3,"h":16,"setting":
{"panelName":"MatrixVisualization"}}]}",
  "description":"This is my second dashboard",
  "name":"Overall Risk 2",
  "private":false
}
```


## Consumes

- application/json

## Produces

- application/json

## Path parameters

- **tid** (required)

  The tenant ID.
- **id** (required)

## Request body

ApiSimpleDashboard

## Return type

ApiDashboard

## Example data

Content-Type: application/json


```
{
  "private" : true,
  "lastModifiedDate" : "2000-01-23T04:56:07.000+00:00",
  "lastModifiedBy" : "lastModifiedBy",
  "name" : "name",
  "doc" : "doc",
  "description" : "description",
```

```
  "id" : 0,
  "creationDate" : "2000-01-23T04:56:07.000+00:00",
  "userId" : "userId",
  "tid" : "tid",
  "home" : true,
  "tags" : [ {
    "name" : "recon",
    "id" : "46b489f7f46588c6"
  }, {
    "name" : "recon",
    "id" : "46b489f7f46588c6"
  } ]
}
```

### Responses

```
200
```

successful operation

# events{tenantId}

## POST /events/{tid}/savedSearches

*Add a saved search*

Creates a new saved search for the currently logged-in user.

### Consumes

- application/json

### Produces

- application/json

### Path parameters

- **tid** (required)

  The tenant ID.

## Request body

ApiSavedSearches

## Return type

ApiSavedSearchesResponse

## Example data

Content-Type: application/json


```
{
  "docDraft" : {
    "integralNumber" : true,
    "double" : true,
    "valueNode" : true,
    "floatingPointNumber" : true,
    "bigInteger" : true,
    "nodeType" : "ARRAY",
    "float" : true,
    "int" : true,
    "long" : true,
    "textual" : true,
    "empty" : true,
    "missingNode" : true,
    "pojo" : true,
    "number" : true,
    "boolean" : true,
    "null" : true,
    "array" : true,
    "binary" : true,
    "containerNode" : true,
    "short" : true,
    "bigDecimal" : true,
    "object" : true
  },
  "columns" : {
    "integralNumber" : true,
    "double" : true,
    "valueNode" : true,
    "floatingPointNumber" : true,
    "bigInteger" : true,
    "nodeType" : "ARRAY",
    "float" : true,
    "int" : true,
```

```
    "long" : true,
    "textual" : true,
    "empty" : true,
    "missingNode" : true,
    "pojo" : true,
    "number" : true,
    "boolean" : true,
    "null" : true,
    "array" : true,
    "binary" : true,
    "containerNode" : true,
    "short" : true,
    "bigDecimal" : true,
    "object" : true
  },
  "name" : "name",
  "doc" : {
    "integralNumber" : true,
    "double" : true,
    "valueNode" : true,
    "floatingPointNumber" : true,
    "bigInteger" : true,
    "nodeType" : "ARRAY",
    "float" : true,
    "int" : true,
    "long" : true,
    "textual" : true,
    "empty" : true,
    "missingNode" : true,
    "pojo" : true,
    "number" : true,
    "boolean" : true,
    "null" : true,
    "array" : true,
    "binary" : true,
    "containerNode" : true,
    "short" : true,
    "bigDecimal" : true,
    "object" : true
  },
  "columnsDraft" : {
    "integralNumber" : true,
    "double" : true,
    "valueNode" : true,
    "floatingPointNumber" : true,
    "bigInteger" : true,
    "nodeType" : "ARRAY",
```

```
    "float" : true,
    "int" : true,
    "long" : true,
    "textual" : true,
    "empty" : true,
    "missingNode" : true,
    "pojo" : true,
    "number" : true,
    "boolean" : true,
    "null" : true,
    "array" : true,
    "binary" : true,
    "containerNode" : true,
    "short" : true,
    "bigDecimal" : true,
    "object" : true
  },
  "id" : 0
}
```

### Responses

```
200
```

successful operation

## GET /events/{tid}/savedSearches

*Get the saved searches for one user*

Return the saved searches for one user on a specific tenant.

### Produces

- application/json

### Path parameters

- **tid** (required)

  The tenant ID.

### Return type

array[ApiSavedSearchesResponse]

## Example data

Content-Type: application/json


```
[ {
  "docDraft" : {
    "integralNumber" : true,
    "double" : true,
    "valueNode" : true,
    "floatingPointNumber" : true,
    "bigInteger" : true,
    "nodeType" : "ARRAY",
    "float" : true,
    "int" : true,
    "long" : true,
    "textual" : true,
    "empty" : true,
    "missingNode" : true,
    "pojo" : true,
    "number" : true,
    "boolean" : true,
    "null" : true,
    "array" : true,
    "binary" : true,
    "containerNode" : true,
    "short" : true,
    "bigDecimal" : true,
    "object" : true
  },
  "columns" : {
    "integralNumber" : true,
    "double" : true,
    "valueNode" : true,
    "floatingPointNumber" : true,
    "bigInteger" : true,
    "nodeType" : "ARRAY",
    "float" : true,
    "int" : true,
    "long" : true,
    "textual" : true,
    "empty" : true,
    "missingNode" : true,
    "pojo" : true,
    "number" : true,
    "boolean" : true,
    "null" : true,
    "array" : true,
```

```
    "binary" : true,
    "containerNode" : true,
    "short" : true,
    "bigDecimal" : true,
    "object" : true
  },
  "name" : "name",
  "doc" : {
    "integralNumber" : true,
    "double" : true,
    "valueNode" : true,
    "floatingPointNumber" : true,
    "bigInteger" : true,
    "nodeType" : "ARRAY",
    "float" : true,
    "int" : true,
    "long" : true,
    "textual" : true,
    "empty" : true,
    "missingNode" : true,
    "pojo" : true,
    "number" : true,
    "boolean" : true,
    "null" : true,
    "array" : true,
    "binary" : true,
    "containerNode" : true,
    "short" : true,
    "bigDecimal" : true,
    "object" : true
  },
  "columnsDraft" : {
    "integralNumber" : true,
    "double" : true,
    "valueNode" : true,
    "floatingPointNumber" : true,
    "bigInteger" : true,
    "nodeType" : "ARRAY",
    "float" : true,
    "int" : true,
    "long" : true,
    "textual" : true,
    "empty" : true,
    "missingNode" : true,
    "pojo" : true,
    "number" : true,
    "boolean" : true,
```

```
    "null" : true,
    "array" : true,
    "binary" : true,
    "containerNode" : true,
    "short" : true,
    "bigDecimal" : true,
    "object" : true
  },
  "id" : 0
}, {
  "docDraft" : {
    "integralNumber" : true,
    "double" : true,
    "valueNode" : true,
    "floatingPointNumber" : true,
    "bigInteger" : true,
    "nodeType" : "ARRAY",
    "float" : true,
    "int" : true,
    "long" : true,
    "textual" : true,
    "empty" : true,
    "missingNode" : true,
    "pojo" : true,
    "number" : true,
    "boolean" : true,
    "null" : true,
    "array" : true,
    "binary" : true,
    "containerNode" : true,
    "short" : true,
    "bigDecimal" : true,
    "object" : true
  },
  "columns" : {
    "integralNumber" : true,
    "double" : true,
    "valueNode" : true,
    "floatingPointNumber" : true,
    "bigInteger" : true,
    "nodeType" : "ARRAY",
    "float" : true,
    "int" : true,
    "long" : true,
    "textual" : true,
    "empty" : true,
    "missingNode" : true,
```

```
    "pojo" : true,
    "number" : true,
    "boolean" : true,
    "null" : true,
    "array" : true,
    "binary" : true,
    "containerNode" : true,
    "short" : true,
    "bigDecimal" : true,
    "object" : true
  },
  "name" : "name",
  "doc" : {
    "integralNumber" : true,
    "double" : true,
    "valueNode" : true,
    "floatingPointNumber" : true,
    "bigInteger" : true,
    "nodeType" : "ARRAY",
    "float" : true,
    "int" : true,
    "long" : true,
    "textual" : true,
    "empty" : true,
    "missingNode" : true,
    "pojo" : true,
    "number" : true,
    "boolean" : true,
    "null" : true,
    "array" : true,
    "binary" : true,
    "containerNode" : true,
    "short" : true,
    "bigDecimal" : true,
    "object" : true
  },
  "columnsDraft" : {
    "integralNumber" : true,
    "double" : true,
    "valueNode" : true,
    "floatingPointNumber" : true,
    "bigInteger" : true,
    "nodeType" : "ARRAY",
    "float" : true,
    "int" : true,
    "long" : true,
    "textual" : true,
```

```
    "empty" : true,
    "missingNode" : true,
    "pojo" : true,
    "number" : true,
    "boolean" : true,
    "null" : true,
    "array" : true,
    "binary" : true,
    "containerNode" : true,
    "short" : true,
    "bigDecimal" : true,
    "object" : true
  },
  "id" : 0
} ]
```

### Responses

```
200
```

successful operation

## DELETE /events/{tid}/savedSearches/{id}

*Delete a saved search*

Deletes the saved search with the specified ID. You must have the permissions required to delete the specified saved search.

### Produces

- application/json

### Path parameters

- **tid** (required)

  The tenant ID.
- **id** (required)

### Responses

```
default
```

successful operation

# DELETE /events/{tid}/savedSearches/{id}/draft

*Removes a saved search draft*

Deletes the draft for the saved search with the specified ID.

## Produces

- application/json

## Path parameters

- **tid** (required)

  The tenant ID.
- **id** (required)

## Responses

`default`

successful operation

# PUT /events/{tid}/savedSearches/{id}

*Update a saved search*

Updates the saved search with the specified ID. You must have the permissions required to update the specified saved search.

## Consumes

- application/json

## Produces

- application/json

## Path parameters

- **tid** (required)

  The tenant ID.

- **id** (required)

## Request body

ApiSavedSearches

## Return type

ApiSavedSearchesResponse

## Example data

Content-Type: application/json


```
{
  "docDraft" : {
    "integralNumber" : true,
    "double" : true,
    "valueNode" : true,
    "floatingPointNumber" : true,
    "bigInteger" : true,
    "nodeType" : "ARRAY",
    "float" : true,
    "int" : true,
    "long" : true,
    "textual" : true,
    "empty" : true,
    "missingNode" : true,
    "pojo" : true,
    "number" : true,
    "boolean" : true,
    "null" : true,
    "array" : true,
    "binary" : true,
    "containerNode" : true,
    "short" : true,
    "bigDecimal" : true,
    "object" : true
  },
  "columns" : {
    "integralNumber" : true,
    "double" : true,
    "valueNode" : true,
    "floatingPointNumber" : true,
    "bigInteger" : true,
    "nodeType" : "ARRAY",
```

```
    "float" : true,
    "int" : true,
    "long" : true,
    "textual" : true,
    "empty" : true,
    "missingNode" : true,
    "pojo" : true,
    "number" : true,
    "boolean" : true,
    "null" : true,
    "array" : true,
    "binary" : true,
    "containerNode" : true,
    "short" : true,
    "bigDecimal" : true,
    "object" : true
  },
  "name" : "name",
  "doc" : {
    "integralNumber" : true,
    "double" : true,
    "valueNode" : true,
    "floatingPointNumber" : true,
    "bigInteger" : true,
    "nodeType" : "ARRAY",
    "float" : true,
    "int" : true,
    "long" : true,
    "textual" : true,
    "empty" : true,
    "missingNode" : true,
    "pojo" : true,
    "number" : true,
    "boolean" : true,
    "null" : true,
    "array" : true,
    "binary" : true,
    "containerNode" : true,
    "short" : true,
    "bigDecimal" : true,
    "object" : true
  },
  "columnsDraft" : {
    "integralNumber" : true,
    "double" : true,
    "valueNode" : true,
    "floatingPointNumber" : true,
```

```
    "bigInteger" : true,
    "nodeType" : "ARRAY",
    "float" : true,
    "int" : true,
    "long" : true,
    "textual" : true,
    "empty" : true,
    "missingNode" : true,
    "pojo" : true,
    "number" : true,
    "boolean" : true,
    "null" : true,
    "array" : true,
    "binary" : true,
    "containerNode" : true,
    "short" : true,
    "bigDecimal" : true,
    "object" : true
  },
  "id" : 0
}
```


### Responses

```
200
```

successful operation

## PUT /events/{tid}/savedSearches/{id}/draft

*Replace the draft for one saved search*

Updates the draft for the saved search with the specified ID.

### Consumes

- application/json

### Produces

- application/json

## Path parameters

- **tid** (required)

  The tenant ID.
- **id** (required)

## Request body

ApiSavedSearchesDraft

## Return type

ApiSavedSearchesDraft

## Example data

Content-Type: application/json


```
{
  "docDraft" : {
    "integralNumber" : true,
    "double" : true,
    "valueNode" : true,
    "floatingPointNumber" : true,
    "bigInteger" : true,
    "nodeType" : "ARRAY",
    "float" : true,
    "int" : true,
    "long" : true,
    "textual" : true,
    "empty" : true,
    "missingNode" : true,
    "pojo" : true,
    "number" : true,
    "boolean" : true,
    "null" : true,
    "array" : true,
    "binary" : true,
    "containerNode" : true,
    "short" : true,
    "bigDecimal" : true,
    "object" : true
  },
  "columnsDraft" : {
```

```
    "integralNumber" : true,
    "double" : true,
    "valueNode" : true,
    "floatingPointNumber" : true,
    "bigInteger" : true,
    "nodeType" : "ARRAY",
    "float" : true,
    "int" : true,
    "long" : true,
    "textual" : true,
    "empty" : true,
    "missingNode" : true,
    "pojo" : true,
    "number" : true,
    "boolean" : true,
    "null" : true,
    "array" : true,
    "binary" : true,
    "containerNode" : true,
    "short" : true,
    "bigDecimal" : true,
    "object" : true
  }
}
```

### Responses

```
200
```

successful operation

# info

## GET /info/auth

*Get authentication provider information*

Returns information about enabled authentication provider(s).

### Example Response (Status 200)

```
{
  "ldap": false,
```

```
  "saml": true,
  "local": false
}
```

### Produces

- application/json

### Responses

```
default
```

successful operation

## GET /info/analysedEntities/{tid}

*Get the number of entities that have been ingested and are available for analysis*

Returns the number of availed entities in the dataset.

### Example Response (Status 200)

### Filtering the results

The results can be filtered using the q parameter, which accepts a filter query (e.g., `entityType:users OR entityType:machines`):

- **entityType**: Allows filtering using the entityTypes (e.g., `entityType:users`)

### Produces

- application/json

### Path parameters

- **tid** (required)

  The tenant ID.

### Query parameters

- **q** (optional)

  Query filter.

### Responses

`default`

successful operation

## GET /info/deployment

*Get depolyment information*

Returns information about deployment type.

### Example Response (Status 200)

```
{
  "ldap": false,
  "saml": true,
  "local": false
}
```

### Produces

- application/json

### Responses

`default`

successful operation

## GET /info/session

*Get session information*

Returns information about the current session.

### Produces

- application/json

### Return type

SessionInfo

## Example data

Content-Type: application/json


```
{
  "extendedApi" : [ {
    "schema" : "schema",
    "prefix" : "prefix",
    "name" : "name",
    "description" : "description",
    "menu" : "menu",
    "permissionsByMethod" : {
      "key" : "ACCESS_INTELLIGENCE"
    }
  }, {
    "schema" : "schema",
    "prefix" : "prefix",
    "name" : "name",
    "description" : "description",
    "menu" : "menu",
    "permissionsByMethod" : {
      "key" : "ACCESS_INTELLIGENCE"
    }
  } ],
  "persistentSessions" : false,
  "permissions" : [ {
    "features" : "showTuning",
    "tenantName" : "Interset",
    "tenantId" : "0",
    "permission" : "ACCESS_INTELLIGENCE,VIEW_INTELLIGENCE_RAW_EVENTS",
    "userId" : "camilla"
  }, {
    "features" : "showTuning",
    "tenantName" : "Interset",
    "tenantId" : "0",
    "permission" : "ACCESS_INTELLIGENCE,VIEW_INTELLIGENCE_RAW_EVENTS",
    "userId" : "camilla"
  } ],
  "userDisplayName" : "Camilla Ferguson",
  "swaggerEndpoints" : {
    "key" : "swaggerEndpoints"
  },
  "analyticsTuningAvailable" : true,
  "disableTenantManagement" : false,
  "accessToken" : "FFvoDf8VkEKITR-L3z3xU_uKZxrT",
  "userId" : "camilla"
}
```

### Responses

`200`

successful operation

## GET /info/build

*Get version information*

Returns information about this Interset build.

### Example Response (Status 200)


```
{
  "Api-Current-Version": "6.3.0",
  "Build-Date": "2018-04-27T03:01:37Z",
  "Build-Number": "6.3.0.102",
  "Archiver-Version": "Plexus Archiver",
  "Built-By": "root",
  "Version": "6.3.0-SNAPSHOT",
  "Manifest-Version": "1.0",
  "Git-Commit": "b72836125ba95d855397b7fa63e50847f3fe255a",
  "Main-Class": "com.interset.reporting.InvestigatorApplication",
  "Git-Branch": "6.3.0",
  "Application": "com.interset.reporting",
  "Name": "reporting",
  "Created-By": "Apache Maven 3.3.9",
  "Build-Jdk": "1.8.0_92",
  "Api-Deprecated-Version": "5.9.0"
}
```


### Produces

- application/json

### Responses

`default`

successful operation

## rawEvents{tenantId}

# POST /rawEvents/{tid}/typeAhead

*Auto-complete event field by column*

## Produces

- application/json

## Path parameters

- **tid** (required)

  The tenant ID.

## Request body

RawEventsTypeaheadRequest

## Request headers

- **Interset-Version** (optional) -- String

  Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

## Query parameters

- **ts** (optional)

  Start time in seconds. If no value is provided, the start time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

- **te** (optional)

  End time in seconds. If no value is provided, the end time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

## Responses

`default`

successful operation

# GET /rawEvents/{tid}/csv

*Get raw data as CSV*

Download raw events in CSV format.

## Produces

- application/json

## Path parameters

- **tid** (required)

  The tenant ID.

## Query parameters

- **q** (optional)

  Accepts a Kibana-type query against the applicable raw data. For example, `(user:("camilla")) AND (project:("csrv/rel3/Auditor"))`.
- **ds** (optional)

  Comma separated list of datasources against which to query. Default includes all.
- **count** (optional)

  The maximum number of raw events to return.
- **tz** (optional)

  The timezone in which the results should be returned (e.g., +5:00, America/Montreal, EST).
- **ts** (optional)

  Start time in seconds. If no value is provided, the start time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.
- **te** (optional)

  End time in seconds. If no value is provided, the end time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

## Responses

`default`

successful operation

# GET /rawEvents/{tid}

*Get raw data as JSON*

Download raw events in JSON format.

## Produces

- application/json

## Path parameters

- **tid** (required)

  The tenant ID.

## Request headers

- **Interset-Version** (optional) -- String

  Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

## Query parameters

- **q** (optional)

  Accepts a Kibana-type query against the applicable raw data. For example, `(user:("camilla")) AND (project:("csrv/rel3/Auditor"))`.
- **ds** (optional)

  Comma separated list of datasources against which to query. Default includes all.
- **count** (optional)

  The maximum number of raw events to return.
- **includeFields** (optional)

  Should the fields be returned. If false, allFields and sortableFields will be omitted.
- **tz** (optional)

  The timezone in which the results should be returned (e.g., +5:00, America/Montreal, EST).
- **ts** (optional)

  Start time in seconds. If no value is provided, the start time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

- **te** (optional)

  End time in seconds. If no value is provided, the end time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

### Responses

`default`

successful operation

## POST /rawEvents/{tid}/graph

### Consumes

- application/json

### Produces

- application/json

### Path parameters

- **tid** (required)

  The tenant ID.

### Request body

RawEventsGraphRequest

### Request headers

- **Interset-Version** (optional) -- String

  Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

### Query parameters

- **tz** (optional)

  The timezone in which the results should be returned (e.g., +5:00, America/Montreal, EST).
- **ts** (optional)

  Start time in seconds. If no value is provided, the start time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.
- **te** (optional)

  End time in seconds. If no value is provided, the end time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

### Responses

`default`

successful operation

## POST /rawEvents/{tid}/resolve

*Get raw data as json or csv*

Retrieve raw events in csv or json.

### Consumes

- application/json

### Produces

- application/json

### Path parameters

- **tid** (required)

  The tenant ID.

### Request body

array[String]

### Request headers

- **Interset-Version** (optional) -- String

  Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

### Query parameters

- **format** (optional)

  The format of the response. Can be json or csv.

- **tz** (optional)

  The timezone in which the results should be returned (e.g., +5:00, America/Montreal, EST).

- **ts** (optional)

  Start time in seconds. If no value is provided, the start time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

- **te** (optional)

  End time in seconds. If no value is provided, the end time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

### Responses

`default`

successful operation

## GET /rawEvents/{tid}/resolve/{id}

*Get raw data as json or csv*

Retrieve raw events in csv or json.

### Consumes

- application/json

### Produces

- application/json

### Path parameters

- **tid** (required)

  The tenant ID.

- **id** (required)

  Event id

### Request headers

- **Interset-Version** (optional) -- String

  Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

### Query parameters

- **format** (optional)

  The format of the response. Can be json or csv.

- **tz** (optional)

  The timezone in which the results should be returned (e.g., +5:00, America/Montreal, EST).

- **ts** (optional)

  Start time in seconds. If no value is provided, the start time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

- **te** (optional)

  End time in seconds. If no value is provided, the end time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

### Responses

`default`

successful operation

## POST /rawEvents/{tid}/search

*Get an event stream that returns raw data as it's retrieved from backend storage*

Stream raw events

## Consumes

- application/json

## Produces

- text/event-stream

## Path parameters

- **tid** (required)

  The tenant ID.

## Request body

RawEventsRequest

## Request headers

- **Interset-Version** (optional) -- String

  Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

## Query parameters

- **count** (optional)

  The maximum number of raw events to return.
- **includeFields** (optional)

  Should the fields be returned. If false, allFields and sortableFields will be omitted.
- **tz** (optional)

  The timezone in which the results should be returned (e.g., +5:00, America/Montreal, EST).
- **scrollId** (optional)

  The `scrollId` from the previous request. Use this `scrollId` to get subsequent results.
- **ts** (optional)

  Start time in seconds. If no value is provided, the start time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.
- **te** (optional)

End time in seconds. If no value is provided, the end time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

### Responses

`default`

successful operation

# search{tenantId}

## GET /search/{tid}/{rollupLevel}/breakdown/risk

*Get risk breakdown for alerts/anomalies*

Gets the number of anomalies or alerts for each risk breakdown (low, medium, high, extreme).

### Example Response (Status 200)

```
{
  "requestTime": 29,
  "data": {
    "extreme": 38,
    "high": 433,
    "low": 231422,
    "medium": 2103
  },
  "cached": "false"
}
```

### Filtering the results

The results can be filtered using the `q` parameter, which accepts a filter query (e.g., `userid:a1cb99f133d83b44 AND risk:extreme`):

- **userid**: Allows filtering using the entityHash; use `serverid`, `projectid`, and so on, to filter on other types of scored entities.
- **user**: Allows filtering using the entityName; use `server`, `project`, and so on, to filter on other types of scored entities.
- **risk**: Allows filtering by risk level (low, medium, high, extreme).
- **anomalies**: Allows filtering by anomaly types (e.g., `anomalies:201,202`).

Although the operators AND and OR serve as separators between different filters, their respective values are currently ignored. Filters concerning the same `entityType` are automatically ORed, and those concerning different entities are ANDed.

## Produces

- application/json

## Path parameters

- **tid** (required)

  The tenant ID.

- **rollupLevel** (required)

  The level at which anomalies are combined. Aggregates combine similar alerts within the same time period across entities. Alerts combine similar anomalies within the same time period for a single entity.

## Request headers

- **Interset-Version** (optional) -- String

  Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

## Query parameters

- **minRisk** (optional)

  Minimum anomaly/alert risk. All anomalies/alerts below this threshold are excluded from the results.

- **maxRisk** (optional)

  Maximum anomaly/alert risk. All anomalies/alerts above this threshold are excluded from the results.

- **q** (optional)

  Query filter.

- **scType** (optional)

  Scaled contribution type. Always use `risk`; `contribution` is deprecated.

- **sc** (optional)

  Scaled contribution. Deprecated; use `minRisk`.

- **ts** (optional)

Start time in seconds. If no value is provided, the start time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

- **te** (optional)

  End time in seconds. If no value is provided, the end time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

### Responses

```
default
```

successful operation

## GET /search/{tid}/{rollupLevel}

*Get anomalies/alerts/aggregates for the selected level*

Returns anomalies, alerts, or aggregates for the selected rollup and for the specified tenant.

### Example Response (Status 200)


```
{
  "requestTime": 29,
  "data": [
    {
      "id": "",
      "alertId": "",
      "datasource": "repo",
      "timestamp": 1393567200,
      "risk": 13,
      "contribution": 10,
      "significance": 88,
      "templates": {
        "threat": "",
        "family": "",
        "teaser": "",
        "alert": "",
        "tooltip": ""
      },
      "anomalyTypes": [
        11
      ],
      "numAnomalies": 2,
      "category": "Repository",
```

```
      "bucketSize": "hourly",
      "rollupLevel": "alerts",
      "numChildren": 2,
      "parentId": "aggId1",
      "kibana": {
        "searchQuery": "",
        "indexName": ""
      },
      "contextAnomalyId": "",
      "contextType": "none",
      "tags": [
          {
            "id": "tagId1",
            "name": "foo",
            "source": "user",
            "createdAt": 1493453400000,
            "createdBy": "jp"
          },
          {
            "id": "tagId1",
            "name": "foo",
            "source": "user",
            "createdAt": 1493567200000,
            "createdBy": "sean"
          }
       ]
    },
  ],
  "totalHits": 25,
  "scrollId": "vabsjk5h24elkdasjfojdabhgjk32b5b",
  "cached": false
}
```


## Filtering the results

The results can be filtered using the `q` parameter, which accepts a filter query (e.g., `userid:a1cb99f133d83b44 AND risk:extreme`):

- **userid**: Allows filtering using the entityHash; use `serverid`, `projectid`, and so on, to filter on other types of scored entities.
- **user**: Allows filtering using the entityName; use `server`, `project`, and so on, to filter on other types of scored entities.
- **risk**: Allows filtering by risk level (low, medium, high, extreme).
- **anomalies**: Allows filtering by anomaly types (e.g., `anomalies:201,202`).

Although the operators AND and OR serve as separators between different filters, their respective values are currently ignored. Filters concerning the same `entityType` are automatically ORed, and those concerning different entities are ANDed.

## Produces

- application/json

## Path parameters

- **tid** (required)

  The tenant ID.

- **rollupLevel** (required)

  The level at which anomalies are combined. Aggregates combine similar alerts within the same time period across entities. Alerts combine similar anomalies within the same time period for a single entity.

## Request headers

- **Interset-Version** (optional) -- String

  Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

## Query parameters

- **count** (optional)

  count

- **sort** (optional)

  Method of sorting alerts.

- **sortOrder** (optional)

  Specifies the sort order of the results. Possible values are `desc` and `asc`.

- **riskSort** (optional)

  Risk sort order in which to return entities.

- **minRisk** (optional)

  Minimum anomaly/alert risk. All anomalies/alerts below this threshold are excluded from the results.

- **maxRisk** (optional)

  Maximum anomaly/alert risk. All anomalies/alerts above this threshold are excluded from the results.

- **q** (optional)

  Query filter.

- **markup** (optional)

  Indicates whether to include handlebar markup in alert text. When `false`, the returned anomalies contain only plain English text that can be displayed directly without further processing. When `true`, anomalies may contain markup tags in double curly braces, {{ and }}. For more information about rendering the returned anomalies, see the Introduction section of the developer guide.

- **scrollId** (optional)

  The `scrollId` from the previous request. Use this `scrollId` to get subsequent results.

- **scType** (optional)

  Scaled contribution type. Always use `risk`; `contribution` is deprecated.

- **sc** (optional)

  Scaled contribution. Deprecated; use `minRisk`.

- **ts** (optional)

  Start time in seconds. If no value is provided, the start time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

- **te** (optional)

  End time in seconds. If no value is provided, the end time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

### Responses

```
default
```

successful operation

## GET /search/{tid}/{rollupLevel}/count

*Get total count for rollup level*

Gets the total number of aggregates, alerts, or anomalies for the specified tenant and rollup level.

### Example Response (Status 200)

```
{
  "requestTime": 29,
  "data": {
```

```
    "count": 237086
  },
  "cached": "false"
}
```

## Filtering the results

The results can be filtered using the `q` parameter, which accepts a filter query (e.g., `userid:a1cb99f133d83b44 AND risk:extreme`):

- **userid**: Allows filtering using the entityHash; use `serverid`, `projectid`, and so on, to filter on other types of scored entities.
- **user**: Allows filtering using the entityName; use `server`, `project`, and so on, to filter on other types of scored entities.
- **risk**: Allows filtering by risk level (low, medium, high, extreme).
- **anomalies**: Allows filtering by anomaly types (e.g., `anomalies:201,202`).

Although the operators AND and OR serve as separators between different filters, their respective values are currently ignored. Filters concerning the same `entityType` are automatically ORed, and those concerning different entities are ANDed.

## Produces

- application/json

## Path parameters

- **tid** (required)

  The tenant ID.

- **rollupLevel** (required)

  The level at which anomalies are combined. Aggregates combine similar alerts within the same time period across entities. Alerts combine similar anomalies within the same time period for a single entity.

## Request headers

- **Interset-Version** (optional) -- String

  Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

### Query parameters

- **minRisk** (optional)

  Minimum anomaly/alert risk. All anomalies/alerts below this threshold are excluded from the results.

- **maxRisk** (optional)

  Maximum anomaly/alert risk. All anomalies/alerts above this threshold are excluded from the results.

- **q** (optional)

  Query filter.

- **scType** (optional)

  Scaled contribution type. Always use `risk`; `contribution` is deprecated.

- **sc** (optional)

  Scaled contribution. Deprecated; use `minRisk`.

- **ts** (optional)

  Start time in seconds. If no value is provided, the start time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

- **te** (optional)

  End time in seconds. If no value is provided, the end time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

### Responses

`default`

successful operation

## GET /search/{tid}/{rollupLevel}/{rollupId}

*Get anomaly/alert/aggregate for specified rollupId*

Returns the anomaly, alert, or aggregate with the specified rollup ID (anomaly ID, alert ID, aggregate ID).

## Example Response (Status 200)


```
{
  "requestTime": 29,
  "data": {
    "id": "ebea3079901fd4c1",
    "alertId": "ebea3079901fd4c1",
    "datasource": "repo",
    "timestamp": 1393453400,
    "risk": 8100,
    "contribution": 100,
    "significance": 88,
    "templates": {
      "threat": "",
      "family": "",
      "teaser": "",
      "alert": "",
      "tooltip": ""
    },
    "anomalyTypes": [
      11
    ],
    "numAnomalies": 2,
    "category": "Repository",
    "bucketSize": "hourly",
    "rollupLevel": "alerts",
    "numChildren": 2,
    "parentId": null,
    "kibana": {
      "searchQuery": "",
      "indexName": ""
    },
    "contextAnomalyId": "",
    "contextType": "none",
    "tags": [
        {
          "id": "tagId1",
          "name": "foo",
          "source": "user",
          "createdAt": 1493453400000,
          "createdBy": "jp"
        },
        {
          "id": "tagId1",
          "name": "foo",
          "source": "user",
          "createdAt": 1493567200000,
          "createdBy": "sean"
        }
     ]
```

```
  },
  "totalHits": 25,
  "cached": "false",
  "scrollId": "vabsjk5h24elkdasjfojdabhgjk32b5b"
}
```

## Filtering the results

The results can be filtered using the q parameter, which accepts a filter query (e.g., `userid:a1cb99f133d83b44 AND risk:extreme`):

- **userid**: Allows filtering using the entityHash; use `serverid`, `projectid`, and so on, to filter on other types of scored entities.
- **user**: Allows filtering using the entityName; use `server`, `project`, and so on, to filter on other types of scored entities.
- **risk**: Allows filtering by risk level (low, medium, high, extreme).
- **anomalies**: Allows filtering by anomaly types (e.g., `anomalies:201,202`).

Although the operators AND and OR serve as separators between different filters, their respective values are currently ignored. Filters concerning the same `entityType` are automatically ORed, and those concerning different entities are ANDed.

## Produces

- application/json

## Path parameters

- **tid** (required)

  The tenant ID.
- **rollupLevel** (required)

  The level at which anomalies are combined. Aggregates combine similar alerts within the same time period across entities. Alerts combine similar anomalies within the same time period for a single entity.
- **rollupId** (required)

  The ID of the aggregate, alert or anomaly to match.

## Request headers

- **Interset-Version** (optional) -- String

  Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

### Query parameters

- **markup** (optional)

  Indicates whether to include handlebar markup in alert text. When `false`, the returned anomalies contain only plain English text that can be displayed directly without further processing. When `true`, anomalies may contain markup tags in double curly braces, {{ and }}. For more information about rendering the returned anomalies, see the Introduction section of the developer guide.

- **riskSort** (optional)

  Which risk score should be associated with an entity.

### Responses

```
default
```

successful operation

## GET /search/{tid}/controllers/authentications

*Get authentication attempts*

Provides an overview of the number of successful and failed authentication attempts made against servers.

### Example Response (Status 200)

```
{
  "requestTime": 29,
  "data": {
    "failed": 4,
    "succeeded": 45
  },
  "cached": "false"
}
```

### Filtering the results

The results can be filtered using the q parameter, which accepts a filter query (e.g., `userid:a1cb99f133d83b44 AND risk:extreme`):

- **userid**: Allows filtering using the entityHash; use `serverid`, `projectid`, and so on, to filter on other types of scored entities.

- **user**: Allows filtering using the entityName; use `server`, `project`, and so on, to filter on other types of scored entities.
- **risk**: Allows filtering by risk level (low, medium, high, extreme).
- **anomalies**: Allows filtering by anomaly types (e.g., `anomalies:201,202`).

Although the operators AND and OR serve as separators between different filters, their respective values are currently ignored. Filters concerning the same `entityType` are automatically ORed, and those concerning different entities are ANDed.

## Produces

- application/json

## Path parameters

- **tid** (required)

  The tenant ID.

## Request headers

- **Interset-Version** (optional) -- String

  Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

## Query parameters

- **q** (optional)

  Query filter.
- **ts** (optional)

  Start time in seconds. If no value is provided, the start time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.
- **te** (optional)

  End time in seconds. If no value is provided, the end time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

## Responses

`default`

successful operation

# GET /search/{tid}/{rollupLevel}/{rollupId}/context

*Get context around an aggregate/alert/anomaly*

Returns the context and statistics for the specified anomaly, alert, or aggregate.

## Example Response (Status 200)


```
{
  "requestTime": 29,
  "data": {
    "values": [
      {
        "key": "probability",
        "value": 33.0,
        "type": "percentage",
        "description": "Anomalousness",
        "displayName": ""
      }
    ],
    "contextType": "rare",
    "threat": "Potential Internal Recon",
    "threatDescription": "When a user who rarely interacts with a certain volume type
then accesses it, this may represent suspicious activity.",
    "unit": "Anomaly Score",
    "unitDescription": ""Anomaly Score" represents how unusual it was for a user to
interact with a specific volume type, when that user rarely uses that volume type. The
anomaly is based on any use of a volume type by a user, compared to normal behavior.",
    "unitType": "Unknown",
    "bucketSize": "hourly"
  },
  "cached": "false"
}
```


## Filtering the results

The results can be filtered using the q parameter, which accepts a filter query (e.g., `userid:a1cb99f133d83b44 AND risk:extreme`):

- **userid**: Allows filtering using the entityHash; use `serverid`, `projectid`, and so on, to filter on other types of scored entities.
- **user**: Allows filtering using the entityName; use `server`, `project`, and so on, to filter on other types of scored entities.
- **risk**: Allows filtering by risk level (low, medium, high, extreme).
- **anomalies**: Allows filtering by anomaly types (e.g., `anomalies:201,202`).

Although the operators AND and OR serve as separators between different filters, their respective values are currently ignored. Filters concerning the same `entityType` are automatically ORed, and those concerning different entities are ANDed.

### Produces

- application/json

### Path parameters

- **tid** (required)

  The tenant ID.
- **rollupLevel** (required)

  The level at which anomalies are combined. Aggregates combine similar alerts within the same time period across entities. Alerts combine similar anomalies within the same time period for a single entity.
- **rollupId** (required)

  The ID of the aggregate, alert or anomaly to match.

### Request headers

- **Interset-Version** (optional) -- String

  Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

### Responses

```
default
```

successful operation

## GET /search/{tid}/{entityType}

*Get entities of a specific type*

Returns entities of the specified type sorted by entityName.

### Example Response (Status 200)

```
{
  "requestTime": 29,
```

```
  "data": [
    {
      "entityHash": "bc23443bd21342fa8997e",
      "entityType": "usr",
      "entityName": "Frank"
    },
    {
      "entityHash": "a89789b897e897d768ef8",
      "entityType": "usr",
      "entityName": "François"
    },
    {
      "entityHash": "9ba897e8978898e87fd76",
      "entityType": "usr",
      "entityName": "Joséphine"
    }
  ],
  "totalHits": 25,
  "scrollId": "vabsjk5h24elkdasjfojdabhgjk32b5b",
  "cached": false
}
```


## Produces

- application/json

## Path parameters

- **tid** (required)

  The tenant ID.

- **entityType** (required)

  The entity type, for example, user, volume, printer, website, etc.

## Request headers

- **Interset-Version** (optional) -- String

  Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

## Query parameters

- **count** (optional)

  The number of entities to return.

- **sortOrder** (optional)

Specifies the sort order of the results. Possible values are `desc` and `asc`.

- **scrollId** (optional)

  The `scrollId` from the previous request. Use this `scrollId` to get subsequent results.

### Responses

`default`

successful operation

## GET /search/{tid}/{entityType}/{entityHash}

*Get entity details*

Given an entity hash, returns the entity's name, type, bot score, tags and clusters.


```
{
  "requestTime": 29,
  "data": {
    "entityType": "user",
    "entityHash": "a1cb99f133d83b44",
    "entityName": "camilla",
    "botScore": 0.0007642867371433429,
    "tags": "[ BOT ]",
    "clusters": "[ KMEANS_2 ]"
  },
  "totalHits": 25,
  "scrollId": "vabsjk5h24elkdasjfojdabhgjk32b5b",
  "cached": false
}
```


### Produces

- application/json

### Path parameters

- **tid** (required)

  The tenant ID.

- **entityType** (required)

  The entity type, for example, user, volume, printer, website, etc.

- **entityHash** (required)

  Element hash (e.g., 393ff13c9b519ec2).

### Request headers

- **Interset-Version** (optional) -- String

  Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

### Responses

`default`

successful operation

## POST /search/{tid}/entityByName

*Get entity details by entity name*

Given an entity name and optionally an entity type, returns the entity's name, type, bot score, tags and clusters.


```
{
  "requestTime": 0,
  "data": {
    "entityType": "user",
    "entityHash": "c6b00f4cca9b3d9",
    "entityName": "jacquelyn.higdon",
    "botScore": 0.00032597667691905424,
    "tags": [],
    "clusters": [
      "KMEANS_5"
    ]
  },
  "cached": false
}
```


### Produces

- application/json

### Path parameters

- **tid** (required)

  The tenant ID.

### Request body

ApiEntityNameRequest

### Request headers

- **Interset-Version** (optional) -- String

  Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

### Responses

`default`

successful operation

## GET /search/{tid}/{entityType}/{entityHash}/risk

*Get the entity risk score*

Returns the current risk score for the specified entity for the specified time range. If the long format is requested, the entity's most significant alert is included in the response. The value of `riskChange` represents the change in risk over the past day. Note that the long format response and the risk change are populated only when the current risk score is requested for the entity.

### Example Response (Status 200)


```
{
  "requestTime": 29,
  "data": {
    "entityHash": "bc23443bd21342fa8997e",
    "entityType": "user",
    "entityName": "Annie",
    "risk": 25,
    "riskChange": -1,
    "lastActivity": 1453957200,
    "preDecayedRisk": 0,
    "decayedToTimestamp": 0,
    "mostSignificantAlert": {
      "id": "",
      "alertId": "",
      "datasource": "auth",
```

```
      "timestamp": 1459144000,
      "risk": 100,
      "contribution": 2,
      "significance": 100,
      "templates": {
        "threat": "",
        "family": "",
        "teaser": "",
        "alert": "",
        "tooltip": ""
      },
      "anomalyTypes": [],
      "numAnomalies": 3,
      "category": "Active Directory",
      "bucketSize": "hourly",
      "rollupLevel": "alerts",
      "numChildren": 3,
      "parentId": "aggId",
      "kibana": {
        "searchQuery": "",
        "indexName": ""
      },
      "contextAnomalyId": "",
      "contextType": "none"
    },
    "tags": [
      {
        "id": "9v3sdqdC2jdOFJCBuYcAPw",
        "name": "reviewed",
        "source": "user",
        "description": ""
      }
    ]
  },
  "cached": "false"
}
```


## Produces

- application/json

## Path parameters

- **tid** (required)

  The tenant ID.

- **entityType** (required)

  The entity type, for example, user, volume, printer, website, etc.

- **entityHash** (required)

  Element hash (e.g., 393ff13c9b519ec2).

## Request headers

- **Interset-Version** (optional) -- String

  Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

## Query parameters

- **sort** (optional)

  The risk to return for the entity.

- **format** (optional)

  The format of the response. When set to `long`, the top alert information for the entity is included in the response.

- **markup** (optional)

  Indicates whether to include handlebar markup in alert text. When `false`, the returned anomalies contain only plain English text that can be displayed directly without further processing. When `true`, anomalies may contain markup tags in double curly braces, {{ and }}. For more information about rendering the returned anomalies, see the Introduction section of the developer guide.

- **tz** (optional)

  The timezone in which the results should be returned (e.g., +5:00, America/Montreal, EST).

- **ts** (optional)

  Start time in seconds. If no value is provided, the start time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

- **te** (optional)

  End time in seconds. If no value is provided, the end time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

## Responses

`default`

successful operation

# GET /search/{tid}/{entityType}/{entityHash}/riskGraph

*Get the entity risk graph*

Returns a timeline of an entity's risk scores in a given time range. The risk returned in each time bucket represents the maximum risk for that entity within that bucket's time range.

## Example Response (Status 200)

The first array represents the start of each time bucket in seconds. Buckets with no risk are omitted. Each item in the second array represents the risk score for the bucket at the same index in the first array.


```
{
  "requestTime": 29,
  "data": [
    {
      "risk": 14,
      "timestamp": 1457982000
    },
    {
      "risk": 5,
      "timestamp": 1458003600
    },
    {
      "risk": 12,
      "timestamp": 1458046800
    }
  ],
  "cached": "false"
}
```


## Produces

- application/json

## Path parameters

- **tid** (required)

  The tenant ID.
- **entityType** (required)

  The entity type, for example, user, volume, printer, website, etc.
- **entityHash** (required)

  Element hash (e.g., 393ff13c9b519ec2).

## Request headers

- **Interset-Version** (optional) -- String

  Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

## Query parameters

- **count** (optional)

  The number of time buckets to return between `ts` and `te`. Each time bucket contains the entity's maximum risk in that time range.

- **interval** (optional)

  The bucket interval (supersedes the `count` parameter). Accepted values are: "day". Buckets are broken down based on the requested time zone.

- **tz** (optional)

  The timezone in which the results should be returned (e.g., +5:00, America/Montreal, EST).

- **ts** (optional)

  Start time in seconds. If no value is provided, the start time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

- **te** (optional)

  End time in seconds. If no value is provided, the end time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

## Responses

```
default
```

successful operation

# GET /search/{tid}/users/bots

*Get bot users*

Returns bot users ordered by descending bot score.

## Example Response (Status 200)


```
{
  "requestTime": 29,
  "data": [
    {
      "entityName": "anne@intserset.com",
      "entityHash": "aadfd74dc21710de",
      "entityType": "bot",
      "risk": 0.73,
      "tags": [
        {
          "id": "tagId0987",
          "name": "FORCEBOT",
          "source": "analytics",
          "description": ""
        },
        {
          "id": "tagId1244",
          "name": "BOT",
          "source": "analytics",
          "description": ""
        }
      ]
    }
  ],
  "cached": "false"
}
```


## Produces

- application/json

## Path parameters

- **tid** (required)

  The tenant ID.

## Request headers

- **Interset-Version** (optional) -- String

  Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

### Query parameters

- **count** (optional)

  The number of bots to return

### Responses

`default`

successful operation

## GET /search/{tid}/distribution/risk

*Get entity risk distribution*

Returns the number of entities associated with each risk level at the most current time in the dataset.

### Example Response (Status 200)

```
{
  "requestTime": 29,
  "data": {
    "risks": {
      "high": 0,
      "total": 370,
      "low": 370,
      "medium": 0,
      "extreme": 0
    },
    "entityTypes": ["projects", "users"],
    "name": "risk",
    "count": 4,
    "type": "current"
  },
  "cached": "false"
}
```

### Filtering the results

The results can be filtered using the `q` parameter, which accepts a filter query (e.g., `userid:a1cb99f133d83b44 AND risk:extreme`):

- **userid**: Allows filtering using the entityHash; use `serverid`, `projectid`, and so on, to filter on other types of scored entities.

- **user**: Allows filtering using the entityName; use `server`, `project`, and so on, to filter on other types of scored entities.
- **risk**: Allows filtering by risk level (low, medium, high, extreme).
- **anomalies**: Allows filtering by anomaly types (e.g., `anomalies:201,202`).

Although the operators AND and OR serve as separators between different filters, their respective values are currently ignored. Filters concerning the same `entityType` are automatically ORed, and those concerning different entities are ANDed.

## Produces

- application/json

## Path parameters

- **tid** (required)

  The tenant ID.

## Request headers

- **Interset-Version** (optional) -- String

  Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

## Query parameters

- **q** (optional)

  Query filter.
- **includeAssociatedEntities** (optional)

  If `false` and the `q` parameter filters for one or more entities and/or entity types, related entities of other entity types are not returned.
- **ts** (optional)

  Start time in seconds. If no value is provided, the start time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.
- **te** (optional)

  End time in seconds. If no value is provided, the end time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

### Responses

`default`

successful operation

## GET /search/{tid}/{entityType}/distribution/risk

*Get the entity risk distribution*

Provides an overview of how many entities of the specified type are associated with each risk level at the most current time in the dataset.

### Example Response (Status 200)


```
{
  "requestTime": 29,
  "data": {
    "risks": {
      "high": 0,
      "total": 370,
      "low": 370,
      "medium": 0,
      "extreme": 0
    },
    "entityTypes": ["projects"],
    "name": "risk",
    "count": 4,
    "type": "current"
  },
  "cached": "false"
}
```


### Filtering the results

The results can be filtered using the `q` parameter, which accepts a filter query (e.g., `userid:a1cb99f133d83b44 AND risk:extreme`):

- **userid**: Allows filtering using the entityHash; use `serverid`, `projectid`, and so on, to filter on other types of scored entities.
- **user**: Allows filtering using the entityName; use `server`, `project`, and so on, to filter on other types of scored entities.
- **risk**: Allows filtering by risk level (low, medium, high, extreme).
- **anomalies**: Allows filtering by anomaly types (e.g., `anomalies:201,202`).

Although the operators AND and OR serve as separators between different filters, their respective values are currently ignored. Filters concerning the same `entityType` are automatically ORed, and those concerning different entities are ANDed.

## Produces

- application/json

## Path parameters

- **tid** (required)

  The tenant ID.
- **entityType** (required)

  The entity type, for example, user, volume, printer, website, etc.

## Request headers

- **Interset-Version** (optional) -- String

  Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

## Query parameters

- **q** (optional)

  Query filter.
- **ts** (optional)

  Start time in seconds. If no value is provided, the start time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.
- **te** (optional)

  End time in seconds. If no value is provided, the end time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

## Responses

`default`

successful operation

# GET /search/{tid}/info

*Get tenant data overview*

Provides an overview of the tenant's data. Information includes scored entities and their counts, the total number of events analyzed, the anomalies discovered, and the time the tenant was last modified.

## Example Response (Status 200)


```
{
  "requestTime": 29,
  "data": {
    "timestart": 0,
    "timeend": 1488213317,
    "lastModified": 0,
    "totalDocs": 0,
    "totalScoredFiles": 0,
    "totalCurrentScoredFiles": 0,
    "totalScoredMachines": 0,
    "totalCurrentScoredMachines": 0,
    "totalScoredProjects": 0,
    "totalCurrentScoredProjects": 0,
    "totalScoredServers": 0,
    "totalCurrentScoredServers": 0,
    "totalScoredUsers": 0,
    "totalCurrentScoredUsers": 0,
    "totalScoredVolumes": 0,
    "totalCurrentScoredVolumes": 0,
    "totalScoredPrinters": 0,
    "totalCurrentScoredPrinters": 0,
    "totalScoredShares": 0,
    "totalCurrentScoredShares": 0,
    "totalScoredResources": 0,
    "totalCurrentScoredResources": 0,
    "totalScoredWebsites": 0,
    "totalCurrentScoredWebsites": 0,
    "totalScoredIps": 0,
    "totalCurrentScoredIps": 0,
    "totalAlerts": 0,
    "totalAnomalies": 0,
    "totalEvents": 0,
    "datasources": [
      "vpn",
      "auth",
      "netflow"
    ],
```

```
  "families": [],
  "threatTypes": ["Suspicious Activity", "Potential Account Misuse"],
  "uiMappings": {
    "volume": {
      "plural": "Volumes",
      "singular": "Volume",
      "query": "volume"
    },
    "server": {
      "plural": "Servers",
      "singular": "Server",
      "query": "server"
    },
    "website": {
      "plural": "Websites",
      "singular": "Website",
      "query": "website"
    },
    "file": {
      "plural": "Files",
      "singular": "File",
      "query": "file"
    },
    "resource": {
      "plural": "Resources",
      "singular": "Resource",
      "query": "resource"
    },
    "machine": {
      "plural": "Engines",
      "singular": "Engine",
      "query": "machine"
    },
    "ip": {
      "plural": "IP Addresses",
      "singular": "IP Address",
      "query": "ip"
    },
    "printer": {
      "plural": "Printers",
      "singular": "Printer",
      "query": "printer"
    },
    "project": {
      "plural": "Projects",
      "singular": "Project",
      "query": "project"
    },
    "share": {
      "plural": "Shares",
```

```
        "singular": "Share",
        "query": "share"
      },
      "user": {
        "plural": "Players",
        "singular": "Player",
        "query": "player"
      }
    },
    "features": [
      "awesomeFeature",
      "forAllFeature"
    ]
  },
  "cached": "false"
}
```

## Produces

- application/json

## Path parameters

- **tid** (required)

  The tenant ID.

## Request headers

- **Interset-Version** (optional) -- String

  Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

## Query parameters

- **ts** (optional)

  Start time in seconds. If no value is provided, the start time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

- **te** (optional)

  End time in seconds. If no value is provided, the end time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

## Responses

`default`

successful operation

# GET /search/{tid}/matrix/{type}

*Get anomaly matrix*

Returns a grid representation of the number of anomalies for each risk and time range. Parameters `tn` and `rn` can be used to control the number of datapoints returned.

## Example Response (Status 200)


```
{
  "requestTime": 29,
  "data": {
    "id": "6e129a48-e3cb-471c-90a4-e431f53301e5",
    "query": null,
    "axis": {
      "type": "timestamp",
      "min": 1440388800,
      "max": 1445540400,
      "count": 10
    },
    "dimensions": [
      {
        "maxvalue": 1640,
        "rows": 10,
        "axis": {
          "type": "risk",
          "min": 0,
          "max": 100,
          "count": 10
        },
        "totalhits": 21745,
        "data": [
          [
            1475,
            1475,
            1514,
            1640,
            1227,
            1024,
            733,
```

```
          765,
          782,
          583
        ],
        [
          305,
          305,
          338,
          308,
          244,
          611,
          255,
          205,
          496,
          157
        ],
        [
          25,
          25,
          127,
          22,
          20,
          247,
          94,
          25,
          125,
          19
        ],
        [
          500,
          500,
          408,
          400,
          400,
          530,
          400,
          500,
          579,
          381
        ],
        [
          0,
          0,
          51,
          0,
          0,
          76,
          0,
          0,
          0,
```

```
          0
        ],
        [
          0,
          0,
          12,
          0,
          0,
          0,
          0,
          0,
          0,
          0,
          0
        ],
        [
          50,
          50,
          40,
          40,
          40,
          116,
          40,
          50,
          50,
          38
        ],
        [
          0,
          0,
          0,
          0,
          0,
          0,
          0,
          0,
          0,
          0
        ],
        [
          50,
          50,
          37,
          40,
          40,
          40,
          40,
          50,
          50,
          38
        ],
```

```
          [
            100,
            100,
            80,
            80,
            80,
            92,
            80,
            100,
            100,
            76
          ]
        ]
      }
    ]
  },
  "cached": "false"
}
```


## Filtering the results

The results can be filtered using the `q` parameter, which accepts a filter query (e.g., `userid:a1cb99f133d83b44 AND risk:extreme`):

- **userid**: Allows filtering using the entityHash; use `serverid`, `projectid`, and so on, to filter on other types of scored entities.
- **user**: Allows filtering using the entityName; use `server`, `project`, and so on, to filter on other types of scored entities.
- **risk**: Allows filtering by risk level (low, medium, high, extreme).
- **anomalies**: Allows filtering by anomaly types (e.g., `anomalies:201,202`).

Although the operators AND and OR serve as separators between different filters, their respective values are currently ignored. Filters concerning the same `entityType` are automatically ORed, and those concerning different entities are ANDed.

## Produces

- application/json

## Path parameters

- **tid** (required)

  The tenant ID.
- **type** (required)

  The type of anomaly representation that should be graphed on the matrix.

### Request headers

- **Interset-Version** (optional) -- String

  Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

### Query parameters

- **rn** (optional)

  The number of risk rows to include in the matrix.
- **tn** (optional)

  The number of time buckets into which the time window should be split (matrix columns)
- **q** (optional)

  Query filter.
- **ts** (optional)

  Start time in seconds. If no value is provided, the start time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.
- **te** (optional)

  End time in seconds. If no value is provided, the end time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

### Responses

`default`

successful operation

## GET /search/{tid}/riskGraph/breakdown

*Population risk breakdown*

Returns a list of time buckets containing a breakdown of anomaly contribution to the population risk at each of those points in time. The risk can be included in the response by setting the query string parameter `includeRisk` to `true`. For performance reasons, we recommend that you call the `/riskGraph` endpoint if you are fetching only the risk.

A breakdown of contribution can be retrieved by:

- **risk**: Breakdown of anomaly risk levels that contributed to the current population risk
- **entityType**: Breakdown of the entityTypes involved in anomalies that contributed to the current population risk
- **threat/workingDays**: Breakdown of threat types involved in anomalies that contributed to the current population risk

## Example Response (Status 200)

Example of population risk breakdown by entity type:


```
{
  "requestTime": 29,
  "data": {
    "breakdown": [
      {
        "timestamp": 1479898800,
        "timestampStr": "2016-11-23T03:00:00-08:00[America/Los_Angeles]",
        "groupBy": "entityType",
        "values": {
          "projects": {
            "contribution": 23.0
          },
          "servers": {
            "contribution": 37.0
          },
          "files": {
            "contribution": 15.0
          },
          "users": {
            "contribution": 25.0
          }
        }
      },
    ],
    "categories": [
      "files",
      "machines",
      "projects",
      "servers",
      "users",
      "volumes",
      "printers",
      "shares",
      "resources",
      "websites",
      "ips"
    ]
  },
```

```
  "cached": "false"
}
```

## Filtering the results

The results can be filtered using the q parameter, which accepts a filter query (e.g., `userid:a1cb99f133d83b44 AND risk:extreme`):

- **userid**: Allows filtering using the entityHash; use `serverid`, `projectid`, and so on, to filter on other types of scored entities.
- **user**: Allows filtering using the entityName; use `server`, `project`, and so on, to filter on other types of scored entities.
- **risk**: Allows filtering by risk level (low, medium, high, extreme).
- **anomalies**: Allows filtering by anomaly types (e.g., `anomalies:201,202`).

Although the operators AND and OR serve as separators between different filters, their respective values are currently ignored. Filters concerning the same `entityType` are automatically ORed, and those concerning different entities are ANDed.

## Produces

- application/json

## Path parameters

- **tid** (required)

  The tenant ID.

## Request headers

- **Interset-Version** (optional) -- String

  Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

## Query parameters

- **count** (optional)

  If interval is set to day, the number of days to graph, working backwards from te; otherwise, the number of time buckets to return between ts and te. Each time bucket contains the entity's maximum risk in that time range. Maximum value of 100. The minimum bucket size is 1 hour.
- **interval** (optional)

Bucket interval (supersedes the count parameter). Accepted values are: "day". Buckets are broken down based on the requested timezone.

- **breakdownBy** (optional)

  Specifies how the risk contribution is broken down

- **includeRisk** (optional)

  When `true`, indicates that the risk for each bucket should be returned. The risk can be retrieved in parallel for the same buckets by using the /riskGraph endpoint with the same parameters.

- **tz** (optional)

  The timezone in which the results should be returned (e.g., +5:00, America/Montreal, EST).

- **q** (optional)

  Query filter.

- **ts** (optional)

  Start time in seconds. If no value is provided, the start time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

- **te** (optional)

  End time in seconds. If no value is provided, the end time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

### Responses

`default`

successful operation

## GET /search/{tid}/riskGraph

*Population risk graph*

Returns a list of time buckets containing the population risk at each of those points in time. The risk in each bucket represents a combination of the risk scores at that time for each entity not filtered out.

## Example Response (Status 200)


```
{
  "requestTime": 29,
  "data": {
    "breakdown": [
      {
        "timestamp": 1479898800,
        "timestampStr": "2016-11-23T03:00:00-08:00[America/Los_Angeles]",
        "risk": 32.0
        }
      },
      {
        "timestamp": 1479985200,
        "timestampStr": "2016-11-24T03:00:00-08:00[America/Los_Angeles]",
        "risk": 38.0
        }
      }
    ]  },
  "cached": "false"
}
```


## Filtering the results

The results can be filtered using the q parameter, which accepts a filter query (e.g., `userid:a1cb99f133d83b44 AND risk:extreme`):

- **userid**: Allows filtering using the entityHash; use `serverid`, `projectid`, and so on, to filter on other types of scored entities.
- **user**: Allows filtering using the entityName; use `server`, `project`, and so on, to filter on other types of scored entities.
- **risk**: Allows filtering by risk level (low, medium, high, extreme).
- **anomalies**: Allows filtering by anomaly types (e.g., `anomalies:201,202`).

Although the operators AND and OR serve as separators between different filters, their respective values are currently ignored. Filters concerning the same `entityType` are automatically ORed, and those concerning different entities are ANDed.

## Produces

- application/json

## Path parameters

- **tid** (required)

  The tenant ID.

## Request headers

- **Interset-Version** (optional) -- String

  Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

## Query parameters

- **count** (optional)

  Number of time buckets to return between ts and te. Each time bucket will contain the entity's maximum risk in that time range.

- **interval** (optional)

  Bucket interval (will supersede count parameter). Accepted values are: "day". Buckets will be broken down based on the requested timezone.

- **tz** (optional)

  The timezone in which the results should be returned (e.g., +5:00, America/Montreal, EST).

- **q** (optional)

  Query filter.

- **ts** (optional)

  Start time in seconds. If no value is provided, the start time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

- **te** (optional)

  End time in seconds. If no value is provided, the end time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

## Responses

`default`

successful operation

# GET /search/{tid}/riskyHours

*Get risky hours*

Returns a list of hours during which the specified entity had anomalies. Each hour is accompanied by the maximum risk of the entity at that time.

## Example Response (Status 200)


```
{
  "requestTime": 29,
  "data": [
    {
      "hour": 1357920900,
      "significance": 100.0
    },
    {
      "hour": 1357920900,
      "significance": 99.0
    },
    {
      "hour": 1357920900,
      "significance": 98.01
    },
    {
      "hour": 1357920900,
      "significance": 37.89
    }
  ],
  "cached": "false"
}
```


## Filtering the results

The results can be filtered using the `q` parameter, which accepts a filter query (e.g., `userid:a1cb99f133d83b44 AND risk:extreme`):

- **userid**: Allows filtering using the entityHash; use `serverid`, `projectid`, and so on, to filter on other types of scored entities.
- **user**: Allows filtering using the entityName; use `server`, `project`, and so on, to filter on other types of scored entities.
- **risk**: Allows filtering by risk level (low, medium, high, extreme).
- **anomalies**: Allows filtering by anomaly types (e.g., `anomalies:201,202`).

Although the operators AND and OR serve as separators between different filters, their respective values are currently ignored. Filters concerning the same `entityType` are automatically ORed, and those concerning different entities are ANDed.

## Produces

- application/json

## Path parameters

- **tid** (required)

  The tenant ID.

## Request headers

- **Interset-Version** (optional) -- String

  Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

## Query parameters

- **minRisk** (optional)

  Minimum anomaly/alert risk. All anomalies/alerts below this threshold are excluded from the results.

- **maxRisk** (optional)

  Maximum anomaly/alert risk. All anomalies/alerts above this threshold are excluded from the results.

- **q** (optional)

  Query filter.

- **ts** (optional)

  Start time in seconds. If no value is provided, the start time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

- **te** (optional)

  End time in seconds. If no value is provided, the end time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

### Responses

`default`

successful operation

## GET /search/{tid}/templates

*Get examples of rendered alert templates*

Returns an example showing how each anomaly type is rendered into a human-readable sentence using the templating engine. The response can be filtered to retrieve only anomalies of a single type or belonging to a specific datasource.

### Example Response (Status 200)


```
{
  "requestTime": 29,
  "data": [
    {
      "template": {
        "threat": "Suspicious Activity",
        "family": "Application/Protocol Use",
        "teaser": "7-8 PM Dec 20, 2012: Used EXPLORER rare for User.",
        "alert": "It was very unusual that {user1} used the application EXPLORER,
having only used that application 2 days.",
        "tooltip": ""
      },
      "category": "Endpoint",
      "threat": {
        "name": "Suspicious Activity",
        "description": "When a user who rarely uses an application then uses it, this
may represent suspicious activity."
      },
      "family": {
        "name": "Application/Protocol Use"
      },
      "anomalyType": 129,
      "datasource": "endpoint"
    }
  ],
  "cached": "false"
}
```

### Produces

- application/json

### Path parameters

- **tid** (required)

  The tenant ID.

### Request headers

- **Interset-Version** (optional) -- String

  Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

### Query parameters

- **ds** (optional)

  Data source
- **anomalyType** (optional)

  Anomaly type
- **markup** (optional)

  Indicates whether to include handlebar markup in alert text. When `false`, the returned anomalies contain only plain English text that can be displayed directly without further processing. When `true`, anomalies may contain markup tags in double curly braces, {{ and }}. For more information about rendering the returned anomalies, see the Introduction section of the developer guide.

### Responses

`default`

successful operation

## GET /search/{tid}/{entityType}/topAccessed

*Get the top accessed entities by entity type*

Returns a list of entities, ordered by the number of times they were accessed.

## Example Response (Status 200)

The keys represent the number of accesses, and their respective values represent the entities that recorded that number of accesses


```
{
  "requestTime": 29,
  "data": {
    "12": [
      {
        "entityHash": "bc23443bd21342fa8997e",
        "entityType": "server",
        "entityName": "server1"
      },
      {
        "entityHash": "a89789b897e897d768ef8",
        "entityType": "server",
        "entityName": "server2"
      }
    ],
    "8": [
      {
        "entityHash": "64d7794788a116f964733",
        "entityType": "server",
        "entityName": "server3"
      }
    ],
    "4": [
      {
        "entityHash": "af867786e09453b67457c",
        "entityType": "server",
        "entityName": "server4"
      }
    ]
  },
  "cached": "false"
}
```


## Filtering the results

The results can be filtered using the `q` parameter, which accepts a filter query (e.g., `userid:a1cb99f133d83b44 AND risk:extreme`):

- **userid**: Allows filtering using the entityHash; use `serverid`, `projectid`, and so on, to filter on other types of scored entities.
- **user**: Allows filtering using the entityName; use `server`, `project`, and so on, to filter on other types of scored entities.

- **risk**: Allows filtering by risk level (low, medium, high, extreme).
- **anomalies**: Allows filtering by anomaly types (e.g., `anomalies:201,202`).

Although the operators AND and OR serve as separators between different filters, their respective values are currently ignored. Filters concerning the same `entityType` are automatically ORed, and those concerning different entities are ANDed.

## Produces

- application/json

## Path parameters

- **tid** (required)

  The tenant ID.
- **entityType** (required)

  The entity type, for example, user, volume, printer, website, etc.

## Request headers

- **Interset-Version** (optional) -- String

  Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

## Query parameters

- **count** (optional)

  The number of top accessed entities to return
- **q** (optional)

  Query filter.
- **ts** (optional)

  Start time in seconds. If no value is provided, the start time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.
- **te** (optional)

  End time in seconds. If no value is provided, the end time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

## Responses

`default`

successful operation

# GET /search/{tid}/users/topExitProducers

*Get top producers of exit events*

Returns the users with the top number of events representing information exiting the system, for example, through a printer or USB.

## Example Response (Status 200)

The keys represent the number of exit events, and their respective values represent the entities that generated that number of exit events.


```
{
  "requestTime": 29,
  "data": {
    "12": [
      {
        "entityHash": "bc23443bd21342fa8997e",
        "entityType": "server",
        "entityName": "elavigne@interset.com"
      },
      {
        "entityHash": "a89789b897e897d768ef8",
        "entityType": "server",
        "entityName": "rwall@interset.com"
      }
    ],
    "8": [
      {
        "entityHash": "64d7794788a116f964733",
        "entityType": "server",
        "entityName": "mcyze@interset.com"
      }
    ],
    "4": [
      {
        "entityHash": "af867786e09453b67457c",
        "entityType": "server",
        "entityName": "jmahonin@interset.com"
      }
```

```
    ]
  },
  "cached": "false"
}
```

## Filtering the results

The results can be filtered using the `q` parameter, which accepts a filter query (e.g., `userid:a1cb99f133d83b44 AND risk:extreme`):

- **userid**: Allows filtering using the entityHash; use `serverid`, `projectid`, and so on, to filter on other types of scored entities.
- **user**: Allows filtering using the entityName; use `server`, `project`, and so on, to filter on other types of scored entities.
- **risk**: Allows filtering by risk level (low, medium, high, extreme).
- **anomalies**: Allows filtering by anomaly types (e.g., `anomalies:201,202`).

Although the operators AND and OR serve as separators between different filters, their respective values are currently ignored. Filters concerning the same `entityType` are automatically ORed, and those concerning different entities are ANDed.

## Produces

- application/json

## Path parameters

- **tid** (required)

  The tenant ID.

## Request headers

- **Interset-Version** (optional) -- String

  Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

## Query parameters

- **count** (optional)

  The number of top exit producers to return
- **q** (optional)

  Query filter.

- **ts** (optional)

  Start time in seconds. If no value is provided, the start time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

- **te** (optional)

  End time in seconds. If no value is provided, the end time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

### Responses

`default`

successful operation

## GET /search/{tid}/users/topFailedLogin

*Get top failed logins*

Returns the users with the top number of failed login attempts.

### Example Response (Status 200)


```
{
  "requestTime": 29,
  "data": [
    {
      "entityHash": "elavigne@interset.com",
      "entityName": "bc23443bd21342fa8997e",
      "totalSuccess": 25,
      "totalFailed": 33
    },
    {
      "entityHash": "rwall@interset.com",
      "entityName": "a89789b897e897d768ef8",
      "totalSuccess": 35,
      "totalFailed": 17
    },
    {
      "entityHash": "mcyze@interset.com",
      "entityName": "64d7794788a116f964733",
      "totalSuccess": 18,
      "totalFailed": 13
    }
```

```
  ],
  "cached": "false"
}
```

## Filtering the results

The results can be filtered using the `q` parameter, which accepts a filter query (e.g., `userid:a1cb99f133d83b44 AND risk:extreme`):

- **userid**: Allows filtering using the entityHash; use `serverid`, `projectid`, and so on, to filter on other types of scored entities.
- **user**: Allows filtering using the entityName; use `server`, `project`, and so on, to filter on other types of scored entities.
- **risk**: Allows filtering by risk level (low, medium, high, extreme).
- **anomalies**: Allows filtering by anomaly types (e.g., `anomalies:201,202`).

Although the operators AND and OR serve as separators between different filters, their respective values are currently ignored. Filters concerning the same `entityType` are automatically ORed, and those concerning different entities are ANDed.

## Produces

- application/json

## Path parameters

- **tid** (required)

  The tenant ID.

## Request headers

- **Interset-Version** (optional) -- String

  Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

## Query parameters

- **count** (optional)

  The number of top users with failed logins to return
- **q** (optional)

  Query filter.

- **ts** (optional)

  Start time in seconds. If no value is provided, the start time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

- **te** (optional)

  End time in seconds. If no value is provided, the end time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

### Responses

`default`

successful operation

## GET /search/{tid}/users/topScreenCaptures

*Get top producers of screen captures*

Returns the users with the top number of screen captures within the specified time period.

### Example Response (Status 200)

The keys represent the number of screen captures, and their respective values represent the entities that generated that number of screen captures.


```
{
  "requestTime": 29,
  "data": {
    "12": [
      {
        "entityHash": "bc23443bd21342fa8997e",
        "entityType": "server",
        "entityName": "elavigne@interset.com"
      },
      {
        "entityHash": "a89789b897e897d768ef8",
        "entityType": "server",
        "entityName": "rwall@interset.com"
      }
    ],
    "8": [
      {
        "entityHash": "64d7794788a116f964733",
```

```
        "entityType": "server",
        "entityName": "mcyze@interset.com"
      }
    ],
    "4": [
      {
        "entityHash": "af867786e09453b67457c",
        "entityType": "server",
        "entityName": "jmahonin@interset.com"
      }
    ]
  },
  "cached": "false"
}
```


## Filtering the results

The results can be filtered using the `q` parameter, which accepts a filter query (e.g., `userid:a1cb99f133d83b44 AND risk:extreme`):

- **userid**: Allows filtering using the entityHash; use `serverid`, `projectid`, and so on, to filter on other types of scored entities.
- **user**: Allows filtering using the entityName; use `server`, `project`, and so on, to filter on other types of scored entities.
- **risk**: Allows filtering by risk level (low, medium, high, extreme).
- **anomalies**: Allows filtering by anomaly types (e.g., `anomalies:201,202`).

Although the operators AND and OR serve as separators between different filters, their respective values are currently ignored. Filters concerning the same `entityType` are automatically ORed, and those concerning different entities are ANDed.

## Produces

- application/json

## Path parameters

- **tid** (required)

  The tenant ID.

## Request headers

- **Interset-Version** (optional) -- String

  Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

### Query parameters

- **count** (optional)

  The number of users to return.

- **q** (optional)

  Query filter.

- **ts** (optional)

  Start time in seconds. If no value is provided, the start time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

- **te** (optional)

  End time in seconds. If no value is provided, the end time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

### Responses

```
default
```

successful operation

## GET /search/{tid}/users/topViolationProducers

*Get top violation producers*

Returns the users that triggered the most violations within the specified time period.

### Example Response (Status 200)

The keys represent the number of violation events, and their respective values represent the entities that generated that number of violations.

```
{
  "requestTime": 29,
  "data": {
    "12": [
      {
        "entityHash": "bc23443bd21342fa8997e",
        "entityType": "server",
        "entityName": "elavigne@interset.com"
      },
```

```
      {
        "entityHash": "a89789b897e897d768ef8",
        "entityType": "server",
        "entityName": "rwall@interset.com"
      }
    ],
    "8": [
      {
        "entityHash": "64d7794788a116f964733",
        "entityType": "server",
        "entityName": "mcyze@interset.com"
      }
    ],
    "4": [
      {
        "entityHash": "af867786e09453b67457c",
        "entityType": "server",
        "entityName": "jmahonin@interset.com"
      }
    ]
  },
  "cached": "false"
}
```


## Filtering the results

The results can be filtered using the `q` parameter, which accepts a filter query (e.g., `userid:a1cb99f133d83b44 AND risk:extreme`):

- **userid**: Allows filtering using the entityHash; use `serverid`, `projectid`, and so on, to filter on other types of scored entities.
- **user**: Allows filtering using the entityName; use `server`, `project`, and so on, to filter on other types of scored entities.
- **risk**: Allows filtering by risk level (low, medium, high, extreme).
- **anomalies**: Allows filtering by anomaly types (e.g., `anomalies:201,202`).

Although the operators AND and OR serve as separators between different filters, their respective values are currently ignored. Filters concerning the same `entityType` are automatically ORed, and those concerning different entities are ANDed.

## Produces

- application/json

### Path parameters

- **tid** (required)

  The tenant ID.

### Request headers

- **Interset-Version** (optional) -- String

  Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

### Query parameters

- **count** (optional)

  The number of top violation producers to return.
- **q** (optional)

  Query filter.
- **ts** (optional)

  Start time in seconds. If no value is provided, the start time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.
- **te** (optional)

  End time in seconds. If no value is provided, the end time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

### Responses

```
default
```

successful operation

## GET /search/{tid}/typeAhead

*Auto-complete entity name for any entity type*

Returns entities across all entity types that have part of their name starting with the value provided in the text parameter.

## Example Response (Status 200)


```
{
  "requestTime": 29,
  "data": {
    "users": [
      {
        "entityHash": "bc23443bd21342fa8997e",
        "entityType": "user",
        "entityName": "user1",
        "risk": 100,
        "riskChange": 0,
        "lastActivity": 1453957200,
        "preDecayedRisk": 0,
        "decayedToTimestamp": 0,
        "mostSignificantAlert": null,
        "tags": []
      }
    ],
    "files": [
      {
        "entityHash": "a89789b897e897d768ef8",
        "entityType": "file",
        "entityName": "u-some-file",
        "risk": 100,
        "riskChange": 0,
        "lastActivity": 1453957200,
        "preDecayedRisk": 0,
        "decayedToTimestamp": 0,
        "mostSignificantAlert": null,
        "tags": []
      }
    ]
  },
  "cached": "false"
}
```


## Produces

- application/json

## Path parameters

- **tid** (required)

  The tenant ID.

### Request headers

- **Interset-Version** (optional) -- String

  Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

### Query parameters

- **count** (optional)

  The max number of entities to return per entity type

- **text** (required)

  The text to be used to match entity(ies) by name.

- **ts** (optional)

  Start time in seconds. If no value is provided, the start time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

- **te** (optional)

  End time in seconds. If no value is provided, the end time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

### Responses

`default`

successful operation

## GET /search/{tid}/users/{userHash}/workingHours/daily

*Get daily working hours per user*

Returns an array of expected activity for the specified user for each half hour of the day. The minute represents the beginning of the half hour period, and the expected value represents the level of activity expected for that half hour period. The expected values form a histogram and are not normalized to a particular scale.

## Example Response (Status 200)


```
{
  "requestTime": 29,
  "data": [
    {
      "minute": 0,
      "expected": 0.6
    },
    {
      "minute": 30,
      "expected": 0.78
    },
    {
      "minute": 60,
      "expected": 0.87
    },
    {
      "minute": 90,
      "expected": 0.9
    },
    {
      "minute": 120,
      "expected": 1.1
    }
  ],
  "cached": "false"
}
```


## Produces

- application/json

## Path parameters

- **tid** (required)

  The tenant ID.

- **userHash** (required)

  Element hash for a user entity (e.g., 393ff13c9b519ec2).

## Request headers

- **Interset-Version** (optional) -- String

  Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

## Responses

`default`

successful operation

# GET /search/{tid}/users/workingHours/weekly

*Get weekly working hours for the organization*

Returns an array of expected activity for the entire organization for each half hour of the week. The minute represents the beginning of the half hour period, and the expected value represents the level of activity expected for that half hour period. The expected values form a histogram and are not normalized to a particular scale.

## Example Response (Status 200)


```
{
  "requestTime": 29,
  "data": [
    {
      "minute": 150,
      "expected": 1.1
    },
    {
      "minute": 180,
      "expected": 1.2
    },
    {
      "minute": 210,
      "expected": 0.9
    },
    {
      "minute": 240,
      "expected": 0.5
    },
    {
      "minute": 270,
      "expected": 0.0
    }
  ],
  "cached": "false"
}
```

### Produces

- application/json

### Path parameters

- **tid** (required)

  The tenant ID.

### Request headers

- **Interset-Version** (optional) -- String

  Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

### Responses

`default`

successful operation

## GET /search/{tid}/users/workingHours/daily

*Get daily working hours for the organization*

Returns an array of expected activity for the entire organization for each half hour of the day. The minute represents the beginning of the half hour period, and the expected value represents the level of activity expected for that half hour period. The expected values form a histogram and are not normalized to a particular scale.

### Example Response (Status 200)

```
{
  "requestTime": 29,
  "data": [
    {
      "minute": 0,
      "expected": 0.6
    },
    {
      "minute": 30,
      "expected": 0.78
```

```
    },
    {
      "minute": 60,
      "expected": 0.87
    },
    {
      "minute": 90,
      "expected": 0.9
    },
    {
      "minute": 120,
      "expected": 1.1
    }
  ],
  "cached": "false"
}
```

### Produces

- application/json

### Path parameters

- **tid** (required)

  The tenant ID.

### Request headers

- **Interset-Version** (optional) -- String

  Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

### Responses

`default`

successful operation

## GET /search/{tid}/users/{userHash}/workingHours/weekly

*Get weekly working hours per user*

Returns an array of expected activity for the specified user for each half hour of the week. The minute represents the beginning of the half hour period, and the expected value represents

the level of activity expected for that half hour period. The expected values form a histogram and are not normalized to a particular scale.

## Example Response (Status 200)


```
{
  "requestTime": 29,
  "data": [
    {
      "minute": 150,
      "expected": 1.1
    },
    {
      "minute": 180,
      "expected": 1.2
    },
    {
      "minute": 210,
      "expected": 0.9
    },
    {
      "minute": 240,
      "expected": 0.5
    },
    {
      "minute": 270,
      "expected": 0.0
    }
  ],
  "cached": "false"
}
```


## Produces

- application/json

## Path parameters

- **tid** (required)

  The tenant ID.

- **userHash** (required)

  Element hash for a user entity (e.g., 393ff13c9b519ec2).

### Request headers

- **Interset-Version** (optional) -- String

  Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

### Responses

`default`

successful operation

## GET /search/{tid}/topRisky

*Get top risky entities*

Returns a list of all top risky entities.

### Example Response (Status 200)


```
{
  "requestTime": 29,
  "data": [
    {
      "entityHash": "bc23443bd21342fa8997e",
      "entityType": "user",
      "entityName": "Annie",
      "risk": 25,
      "riskChange": 0,
      "lastActivity": 1453957200,
      "preDecayedRisk": 0,
      "decayedToTimestamp": 0,
      "mostSignificantAlert": null,
      "tags": [
        {
          "id": "9v3sdqdC2jdOFJCBuYcAPw",
          "name": "reviewed",
          "source": "user",
          "description": ""
        }
      ]
    },
  ],
  "totalHits": 25,
  "scrollId": "vabsjk5h24elkdasjfojdabhgjk32b5b",
```

```
  "cached": false
}
```

## Filtering the results

The results can be filtered using the `q` parameter, which accepts a filter query (e.g., `userid:a1cb99f133d83b44 AND risk:extreme`):

- **userid**: Allows filtering using the entityHash; use `serverid`, `projectid`, and so on, to filter on other types of scored entities.
- **user**: Allows filtering using the entityName; use `server`, `project`, and so on, to filter on other types of scored entities.
- **risk**: Allows filtering by risk level (low, medium, high, extreme).
- **anomalies**: Allows filtering by anomaly types (e.g., `anomalies:201,202`).

Although the operators AND and OR serve as separators between different filters, their respective values are currently ignored. Filters concerning the same `entityType` are automatically ORed, and those concerning different entities are ANDed.

## Produces

- application/json

## Path parameters

- **tid** (required)

  The tenant ID.

## Request headers

- **Interset-Version** (optional) -- String

  Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

## Query parameters

- **sort** (optional)

  Risk sort order in which to return entities.
- **format** (optional)

  The format of the response. When set to `long`, the top alert information for the entity is included in the response.

- **q** (optional)

  Query filter.

- **includeAssociatedEntities** (optional)

  If `false` and the `q` parameter filters for one or more entities and/or entity types, related entities of other entity types are not returned.

- **markup** (optional)

  Indicates whether to include handlebar markup in alert text. When `false`, the returned anomalies contain only plain English text that can be displayed directly without further processing. When `true`, anomalies may contain markup tags in double curly braces, {{ and }}. For more information about rendering the returned anomalies, see the Introduction section of the developer guide.

- **tz** (optional)

  The timezone in which the results should be returned (e.g., +5:00, America/Montreal, EST).

- **count** (optional)

  Number of top risky entities to return

- **scrollId** (optional)

  The `scrollId` from the previous request. Use this `scrollId` to get subsequent results.

- **includeNonAnomalous** (optional)

  Set to true to include entities that never triggered anomalies

- **ts** (optional)

  Start time in seconds. If no value is provided, the start time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

- **te** (optional)

  End time in seconds. If no value is provided, the end time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

### Responses

`default`

successful operation

## GET /search/{tid}/{entityType}/topRisky

*Get top risky entities by type*

Returns a list of the top riskiest entities by type.

## Example Response (Status 200)


```
{
  "requestTime": 29,
  "data": [
    {
      "entityHash": "bc23443bd21342fa8997e",
      "entityType": "user",
      "entityName": "Annie",
      "risk": 25,
      "riskChange": 0,
      "lastActivity": 1453957200,
      "preDecayedRisk": 0,
      "decayedToTimestamp": 0,
      "mostSignificantAlert": null,
      "tags": [
        {
          "id": "9v3sdqdC2jdOFJCBuYcAPw",
          "name": "reviewed",
          "source": "user",
          "description": ""
        }
      ]
    },
  ],
  "totalHits": 25,
  "scrollId": "vabsjk5h24elkdasjfojdabhgjk32b5b",
  "cached": false
}
```


## Filtering the results

The results can be filtered using the `q` parameter, which accepts a filter query (e.g., `userid:a1cb99f133d83b44 AND risk:extreme`):

- **userid**: Allows filtering using the entityHash; use `serverid`, `projectid`, and so on, to filter on other types of scored entities.
- **user**: Allows filtering using the entityName; use `server`, `project`, and so on, to filter on other types of scored entities.
- **risk**: Allows filtering by risk level (low, medium, high, extreme).
- **anomalies**: Allows filtering by anomaly types (e.g., `anomalies:201,202`).

Although the operators AND and OR serve as separators between different filters, their respective values are currently ignored. Filters concerning the same `entityType` are automatically ORed, and those concerning different entities are ANDed.

## Produces

- application/json

## Path parameters

- **tid** (required)

  The tenant ID.
- **entityType** (required)

  The entity type, for example, user, volume, printer, website, etc.

## Request headers

- **Interset-Version** (optional) -- String

  Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

## Query parameters

- **sort** (optional)

  Risk sort order in which to return entities.
- **format** (optional)

  The format of the response. When set to `long`, the top alert information for the entity is included in the response.
- **q** (optional)

  Query filter.
- **markup** (optional)

  Indicates whether to include handlebar markup in alert text. When `false`, the returned anomalies contain only plain English text that can be displayed directly without further processing. When `true`, anomalies may contain markup tags in double curly braces, {{ and }}. For more information about rendering the returned anomalies, see the Introduction section of the developer guide.
- **tz** (optional)

  The timezone in which the results should be returned (e.g., +5:00, America/Montreal, EST).
- **count** (optional)

  The number of top risky entities to return
- **scrollId** (optional)

The `scrollId` from the previous request. Use this `scrollId` to get subsequent results.

- **includeNonAnomalous** (optional)

  Set to true to include entities that never triggered anomalies

- **ts** (optional)

  Start time in seconds. If no value is provided, the start time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

- **te** (optional)

  End time in seconds. If no value is provided, the end time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

### Responses

```
default
```

successful operation

## GET /search/{tid}/{rollupLevel}/{rollupId}/expand

*Get children of aggregate/alert/anomaly*

Returns the children of the specified rollup ID. If an aggregate ID is specified, this method returns the child alerts. If an alert ID is specified, the child anomalies are returned. Nothing is returned when an anomaly ID is specified because anomalies are the lowest level and have no children.

### Example Response (Status 200)


```
{
  "requestTime": 29,
  "data": [
    {
      "id": "ebea3079901fd4c1",
      "alertId": "ebea3079901fd4c1",
      "datasource": "repo",
      "timestamp": 1393453400,
      "risk": 8100,
      "contribution": 100,
      "significance": 88,
      "templates": {
        "threat": "",
```

```
        "family": "",
        "teaser": "",
        "alert": "",
        "tooltip": ""
      },
      "anomalyTypes": [
        11
      ],
      "numAnomalies": 2,
      "category": "Repository",
      "bucketSize": "hourly",
      "rollupLevel": "alerts",
      "numChildren": 2,
      "parentId": null,
      "kibana": {
        "searchQuery": "",
        "indexName": ""
      },
      "contextAnomalyId": "",
      "contextType": "none"
    }
  ],
  "totalHits": 25,
  "cached": false,
  "scrollId": "vabsjk5h24elkdasjfojdabhgjk32b5b"
}
```


## Filtering the results

The results can be filtered using the q parameter, which accepts a filter query (e.g., `userid:a1cb99f133d83b44 AND risk:extreme`):

- **userid**: Allows filtering using the entityHash; use `serverid`, `projectid`, and so on, to filter on other types of scored entities.
- **user**: Allows filtering using the entityName; use `server`, `project`, and so on, to filter on other types of scored entities.
- **risk**: Allows filtering by risk level (low, medium, high, extreme).
- **anomalies**: Allows filtering by anomaly types (e.g., `anomalies:201,202`).

Although the operators AND and OR serve as separators between different filters, their respective values are currently ignored. Filters concerning the same `entityType` are automatically ORed, and those concerning different entities are ANDed.

## Produces

- application/json

## Path parameters

- **tid** (required)

  The tenant ID.

- **rollupLevel** (required)

  The level at which anomalies are combined. Aggregates combine similar alerts within the same time period across entities. Alerts combine similar anomalies within the same time period for a single entity.

- **rollupId** (required)

  The ID of the aggregate, alert or anomaly to match.

## Request headers

- **Interset-Version** (optional) -- String

  Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

## Query parameters

- **minRisk** (optional)

  Minimum anomaly/alert risk. All anomalies/alerts below this threshold are excluded from the results.

- **maxRisk** (optional)

  Maximum anomaly/alert risk. All anomalies/alerts above this threshold are excluded from the results.

- **count** (optional)

- **q** (optional)

  Query filter.

- **markup** (optional)

  Indicates whether to include handlebar markup in alert text. When `false`, the returned anomalies contain only plain English text that can be displayed directly without further processing. When `true`, anomalies may contain markup tags in double curly braces, {{ and }}. For more information about rendering the returned anomalies, see the Introduction section of the developer guide.

- **scrollId** (optional)

  The `scrollId` from the previous request. Use this `scrollId` to get subsequent results.

- **sort** (optional)

  Method of sorting alerts.
- **sortOrder** (optional)

  Specifies the sort order of the results. Possible values are `desc` and `asc`.
- **riskSort** (optional)

  Risk sort order in which to return entities.
- **scType** (optional)

  Scaled contribution. Deprecated; use `minRisk`.
- **sc** (optional)

  Scaled contribution. Deprecated; use `minRisk`.

### Responses

`default`

successful operation

# search{tenantId}meta

## POST /search/{tid}/meta

*Create a meta resource*

Creates a new meta resource. Fields that must be added: `resourceType`, `destinationId`, `destinationType`, `content`, `contentType`

### Example Response (Status 200)


```
{
  "requestTime": 29,
  "data":
    {
      "id": "cb3c32ebc26d8463",
      "resourceType": "annotation",
      "sourceId": "abc@interset.com",
      "sourceType": "user",
      "destinationId": "b2d1bbfd2daa1fed",
      "destinationType": "entities",
      "content": "",
      "contentType": "html",
```

```
      "createdBy": "abc@interset.com"
      "created": 1541603226
      "timestamp": 1541725744
    },
  "cached": "false"
}
```

### Consumes

- application/json

### Produces

- application/json

### Path parameters

- **tid** (required)

  The tenant ID.

### Request body

ApiMetaRequest

### Request headers

- **Interset-Version** (optional) -- String

  Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

### Responses

```
default
```

successful operation

## DELETE /search/{tid}/meta/{metaId}

*Delete a meta resource*

Deletes the meta resource with the specified ID.

### Example Response (Status 200)

```
{
  "requestTime": 29,
  "data": {
    "message": "Meta resource with ID 6f327e088def9386 successfully deleted."
  },
  "cached": "false"
}
```

### Consumes

- application/json

### Produces

- application/json

### Path parameters

- **tid** (required)

  The tenant ID.
- **metaId** (required)

  The ID of the meta resource (e.g., cb3c32ebc26d8463).

### Request headers

- **Interset-Version** (optional) -- String

  Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

### Responses

`default`

successful operation

## GET /search/{tid}/meta/log

*Get all meta logs for a tenant with certain conditions.*

Get all meta logs for this tenant with the search conditions specified. Source type can be configured either by a user through the UI, or by Analytics. Currently supported destination types are alerts, anomalies and entities

## Example Response (Status 200)


```
{
  "requestTime": 29,
  "data": [
    {
      "id": "423c32ebc26d8bce",
      "resourceId": "null",
      "resourceType": "comment",
      "action": "create",
      "sourceId": "def@interset.com",
      "sourceType": "user",
      "destinationId": "8202835f7614404d",
      "destinationType": "alerts",
      "content": "This is my very first comment.",
      "contentType": "plaintext",
      "created": 1541603226
      "createdBy": "def@interset.com"
      "modifiedBy": null
      "timestamp": 1541603226
    },
    {
      "id": "cb3c32ebc26d8463",
      "resourceId": "423c32ebc26d8bce",
      "resourceType": "comment",
      "action": "update",
      "sourceId": "abc@interset.com",
      "sourceType": "user",
      "destinationId": "b2d1bbfd2daa1fed",
      "destinationType": "entities",
      "content": "This is my very first *edited* comment.",
      "contentType": "markdown",
      "created": 1541603226
      "createdBy": "abc@interset.com"
      "modifiedBy": "admin@interset.com"
      "timestamp": 1541725744
    },
  ],
  "cached": "false"
}
```


## Consumes

- application/json

## Produces

- application/json

## Path parameters

- **tid** (required)

  The tenant ID.

## Request headers

- **Interset-Version** (optional) -- String

  Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

## Query parameters

- **q** (optional)

  Query filter.
- **resourceId** (optional)

  A reference to the original resource if applicable (metaId, tagId, null)
- **resourceType** (optional)

  The type of the meta resource e.g. comment, annotation, tag, dashboard, visualization and so on.
- **action** (optional)

  The operation made on this meta resources. This API supports `add`, `update`, `delete`.
- **sourceId** (optional)

  The ID of the source. If the source type is `user`, then `createdBy` is the user's name.
- **sourceType** (optional)

  The type of the source. Currently supported: `user`, `analytics`
- **destinationId** (optional)

  The ID of the destination.
- **destinationType** (optional)

  The type of the source. Currently supported: `alerts`, `anomalies`, `entities`
- **content** (optional)

  The raw content of the object. This is a full text search. Larger than 128KB can significantly impact the search performance.

- **contentType** (optional)

  Currently supported: `markdown`, `plaintext`, `html`
- **createdBy** (optional)

  The name of the user that original created the resource - an informational field.
- **modifiedBy** (optional)

  The ID of the user that last modified the resource.

### Responses

`default`

successful operation

## GET /search/{tid}/meta/{metaId}

*Get the specified meta resource.*

Gets the meta resource with the specified ID.

### Example Response (Status 200)

```
{
  "requestTime": 29,
  "data":
    {
      "id": "cb3c32ebc26d8463",
      "resourceType": "annotation",
      "action": "update",
      "sourceId": "abc@interset.com",
      "sourceType": "user",
      "destinationId": "b2d1bbfd2daa1fed",
      "destinationType": "entities",
      "content": "",
      "contentType": "html",
      "created": 1541603226
      "createdBy": "abc@interset.com"
      "modifiedBy": "admin@interset.com"
      "timestamp": 1541725744
    },
  "cached": "false"
}
```

### Consumes

- application/json

### Produces

- application/json

### Path parameters

- **tid** (required)

  The tenant ID.
- **metaId** (required)

  The ID of the meta resource (e.g., cb3c32ebc26d8463).

### Request headers

- **Interset-Version** (optional) -- String

  Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

### Responses

```
default
```

successful operation

## GET /search/{tid}/meta

*Get all meta resources for a tenant with certain conditions.*

Get all meta resources for this tenant with the search conditions specified. Source type can be configured either by a user through the UI, or by Analytics. Currently supported destination types are alerts, anomalies and entities

### Example Response (Status 200)

```
{
  "requestTime": 29,
  "data": [
    {
```

```
      "id": "423c32ebc26d8bce",
      "resourceId": "null",
      "resourceType": "comment",
      "action": "create",
      "sourceId": "def@interset.com",
      "sourceType": "user",
      "destinationId": "8202835f7614404d",
      "destinationType": "alerts",
      "content": "This is my very first comment.",
      "contentType": "plaintext",
      "created": 1541603226
      "createdBy": "def@interset.com"
      "modifiedBy": null
      "timestamp": 1541603226
    },
    {
      "id": "cb3c32ebc26d8463",
      "resourceId": "423c32ebc26d8bce",
      "resourceType": "comment",
      "action": "update",
      "sourceId": "abc@interset.com",
      "sourceType": "user",
      "destinationId": "b2d1bbfd2daa1fed",
      "destinationType": "entities",
      "content": "This is my very first *edited* comment.",
      "contentType": "markdown",
      "created": 1541603226
      "createdBy": "abc@interset.com"
      "modifiedBy": "admin@interset.com"
      "timestamp": 1541725744
    },
  ],
  "cached": "false"
}
```


## Consumes

- application/json

## Produces

- application/json

## Path parameters

- **tid** (required)

  The tenant ID.

## Request headers

- **Interset-Version** (optional) -- String

  Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

## Query parameters

- **q** (optional)

  Query filter.
- **resourceType** (optional)

  The type of the meta resource e.g. comment, annotation, tag, dashboard, visualization and so on.
- **action** (optional)

  The operation made on this meta resources. This API supports `add`, `update`, `delete`.
- **sourceId** (optional)

  The ID of the source. If the source type is `user`, then `createdBy` is the user's name.
- **sourceType** (optional)

  The type of the source. Currently supported: `user`, `analytics`
- **destinationId** (optional)

  The ID of the destination.
- **destinationType** (optional)

  The type of the source. Currently supported: `alerts`, `anomalies`, `entities`
- **content** (optional)

  The raw content of the object. This is a full text search. Larger than 128KB can significantly impact the search performance.
- **contentType** (optional)

  Currently supported: `markdown`, `plaintext`, `html`
- **createdBy** (optional)

  The name of the user that original created the resource - an informational field.
- **modifiedBy** (optional)

  The ID of the user that last modified the resource.

## Responses

```
default
```

successful operation

## PUT /search/{tid}/meta/{metaId}

*Update a meta resource*

Update the specified a meta resource. Fields that can be updated: `resourceType`, `destinationId`, `destinationType`, `content`, `contentType`

### Example Response (Status 200)


```
    {
      "resourceType": "annotation",
      "id": "cb3c32ebc26d8463",
      "sourceId": "abc@interset.com",
      "sourceType": "user",
      "destinationId": "b2d1bbfd2daa1fed",
      "destinationType": "entities",
      "content": "",
      "contentType": "html",
      "createdBy": "abc@interset.com"
      "modifiedBy": "admin@interset.com"
      "created": 1541603226
      "timestamp": 1541725744
    },
  "cached": "false"
}
```


### Consumes

- application/json

### Produces

- application/json

### Path parameters

- **tid** (required)

  The tenant ID.
- **metaId** (required)

  The ID of the meta resource (e.g., cb3c32ebc26d8463).

### Request body

ApiMetaRequest

Changes the resource type, source, destination, content and modifiedBy for the specified meta resource.

### Request headers

- **Interset-Version** (optional) -- String

  Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

### Responses

`default`

successful operation

# search{tenantId}tags

## PUT /search/{tid}/tags/{tagId}/{tagElementType}/{elementHash}

*Add a tag to an element*

Adds a tag to an element such as an entity or an alert.

### Example Response (Status 200)

```
{
  "requestTime": 29,
  "data": {
    "message": "46b489f7f46588c6 successfully associated with 'entities' element
75c2599ddf50ea85"
  },
  "cached": "false"
}
```

### Consumes

- application/json

### Produces

- application/json

### Path parameters

- **tid** (required)

  The tenant ID.
- **tagId** (required)

  The ID of the tag (e.g., mQhWWuPFNqti-w-AlNWHdA).
- **elementHash** (required)

  Element hash (e.g., 393ff13c9b519ec2).
- **tagElementType** (required)

  The type of element with which the tag is associated.

### Request headers

- **Interset-Version** (optional) -- String

  Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

### Query parameters

- **retries** (optional)

  The number of times to retry the update operation if a conflict occurs.

### Responses

`default`

successful operation

## POST /search/{tid}/tags/{tagId}/{tagElementType}/add

*Add a tag to multiple elements*

Adds a tag to a list of elements of the same type.

## Example Response (Status 200)

```
{
  "requestTime": 29,
  "data": {
    "message": "46b489f7f46588c6 successfully associated with entities:
["75c2599ddf50ea85", "75c2599ddf50ea86"]"
  },
  "cached": "false"
}
```

## Consumes

- application/json

## Produces

- application/json

## Path parameters

- **tid** (required)

  The tenant ID.
- **tagId** (required)

  The ID of the tag (e.g., mQhWWuPFNqti-w-AlNWHdA).
- **tagElementType** (required)

  The type of element with which the tag is associated.

## Request body

ApiTagEntities

A list of element hashes.

## Request headers

- **Interset-Version** (optional) -- String

  Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

### Query parameters

- **retries** (optional)

  The number of times to retry the update operation if a conflict occurs.

### Responses

`default`

successful operation

## POST /search/{tid}/tags

*Create a tag*

Creates a new tag.

### Example Response (Status 200)

```
{
  "requestTime": 29,
  "data": {
    "name": "newTag",
    "description": "testing tags",
    "entities": [],
    "id": "6f327e088def9386",
    "created": "2017-12-01T00:16:56.016Z",
    "createdBy": "td5",
    "modified": "2017-12-01T00:16:56.016Z",
    "modifiedBy": "td5",
    "source": "user"
  },
  "cached": "false"
}
```

### Consumes

- application/json

### Produces

- application/json

### Path parameters

- **tid** (required)

  The tenant ID.

### Request body

TagBase

### Request headers

- **Interset-Version** (optional) -- String

  Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

### Responses

`default`

successful operation

## DELETE /search/{tid}/tags/{tagId}

*Delete a tag*

Deletes the tag with the specified ID.

### Example Response (Status 200)

```
{
  "requestTime": 29,
  "data": {
    "message": "Tag 6f327e088def9386 successfully deleted."
  },
  "cached": "false"
}
```

### Consumes

- application/json

### Produces

- application/json

### Path parameters

- **tid** (required)

  The tenant ID.
- **tagId** (required)

  The ID of the tag (e.g., mQhWWuPFNqti-w-AlNWHdA).

### Request headers

- **Interset-Version** (optional) -- String

  Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

### Query parameters

- **force** (optional)

  Force the action to be applied even in the presence of conflicts.

### Responses

```
default
```

successful operation

## GET /search/{tid}/tags/{tagId}/{tagElementType}

*Get elements associated with a particular tag*

Gets all elements that have the specified tag.

### Example Response (Status 200)

```
{
  "requestTime": 29,
  "data": [
    {
      "entityHash": "e6a4bb7b21cf495b",
```

```
      "entityType": "user",
      "entityName": "user1041@dev-win-10-conn"
    }
  ],
  "cached": "false"
}
```

## Consumes

- application/json

## Produces

- application/json

## Path parameters

- **tid** (required)

  The tenant ID.
- **tagId** (required)

  The ID of the tag (e.g., mQhWWuPFNqti-w-AlNWHdA).
- **tagElementType** (required)

  The type of element with which the tag is associated.

## Request headers

- **Interset-Version** (optional) -- String

  Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

## Query parameters

- **count** (optional)

  The number of tagged elements to return.
- **scrollId** (optional)

  The `scrollId` from the previous request. Use this `scrollId` to get subsequent results.

## Responses

```
default
```

successful operation

# GET /search/{tid}/tags/{tagId}

*Get the specified tag*

Gets the tag with the specified ID.

## Example Response (Status 200)


```
{
  "requestTime": 29,
  "data": {
    "name": "recon",
    "description": null,
    "entities": [],
    "id": "46b489f7f46588c6",
    "created": "2017-11-30T23:59:38.737Z",
    "createdBy": "td5",
    "modified": "2017-12-01T00:16:56.016Z",
    "modifiedBy": "td5",
    "source": "user"
  },
  "cached": "false"
}
```


## Consumes

- application/json

## Produces

- application/json

## Path parameters

- **tid** (required)

  The tenant ID.

- **tagId** (required)

  The ID of the tag (e.g., mQhWWuPFNqti-w-AlNWHdA).

## Request headers

- **Interset-Version** (optional) -- String

  Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

## Responses

`default`

successful operation

# GET /search/{tid}/tags/{boolOperator}/entities

*Get elements associated with tags*

Returns entities that match the specified tags.

## Example Response (Status 200)


```
{
  "requestTime": 29,
  "data": [
    {
      "entityHash": "75c2599ddf50ea85",
      "entityType": "user",
      "entityName": "user68@qa-win-7-conn.local"
    }
  ],
  "cached": "false"
}
```


## Consumes

- application/json

## Produces

- application/json

## Path parameters

- **tid** (required)

  The tenant ID.

- **boolOperator** (required)

  Indicates whether the returned entities must have any or all of the specified tags. Possible values are `any` (return entities with any of the specified tags) or `all` (return entities with all the specified tags).

### Request headers

- **Interset-Version** (optional) -- String

  Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

### Query parameters

- **tag** (optional)

  A list of tags, formatted as `tag=<tagID1>&tag=<tagID2>&tag=<tagID3>...`. In the UI, enter unquoted tag IDs in the textbox, one per line.
- **count** (optional)

  The number of tagged elements to return.
- **scrollId** (optional)

  The `scrollId` from the previous request. Use this `scrollId` to get subsequent results.

### Responses

`default`

successful operation

## GET /search/{tid}/tags

*Get all tags for a tenant*

Get all tags for this tenant. Tags can be configured either by a user through the UI, or by Analytics. The payload specifies the source of the tag.

### Example Response (Status 200)


```
{
  "requestTime": 29,
  "data": [
    {
      "name": "exfiltrate",
      "description": null,
      "entities": [],
      "id": "f2c23b9def498aeb",
      "created": "2017-11-30T23:58:55.529Z",
      "createdBy": "td5",
```

```
      "modified": "2017-12-01T00:16:56.016Z",
      "modifiedBy": "td5",
      "source": "user"
    },
    {
      "name": "recon",
      "description": null,
      "entities": [],
      "id": "46b489f7f46588c6",
      "created": "2017-11-30T23:59:38.737Z",
      "createdBy": "td5",
      "source": "user"
    }
  ],
  "cached": "false"
}
```


## Filtering the results

The results can be filtered using the q parameter, which accepts a filter query (e.g., `userid:a1cb99f133d83b44 AND risk:extreme`):

- **userid**: Allows filtering using the entityHash; use `serverid`, `projectid`, and so on, to filter on other types of scored entities.
- **user**: Allows filtering using the entityName; use `server`, `project`, and so on, to filter on other types of scored entities.
- **risk**: Allows filtering by risk level (low, medium, high, extreme).
- **anomalies**: Allows filtering by anomaly types (e.g., `anomalies:201,202`).

Although the operators AND and OR serve as separators between different filters, their respective values are currently ignored. Filters concerning the same `entityType` are automatically ORed, and those concerning different entities are ANDed.

## Consumes

- application/json

## Produces

- application/json

## Path parameters

- **tid** (required)

  The tenant ID.

### Request headers

- **Interset-Version** (optional) -- String

  Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

### Query parameters

- **source** (optional)

  Indicates how the tag was created (either by a user or by analytics).
- **q** (optional)

  Query filter.
- **typeahead** (optional)

  The text to be used to match tags by name.

### Responses

```
default
```

successful operation

## DELETE /search/{tid}/tags/{tagId}/{tagElementType}/{elementHash}

*Remove a tag from a single element*

Deletes a tag from an element such as an entity or an alert.

### Example Response (Status 200)

```
{
  "requestTime": 29,
  "data": {
    "message": "46b489f7f46588c6 successfully removed from 'entities' element
75c2599ddf50ea85"
  },
  "cached": "false"
}
```

### Consumes

- application/json

### Produces

- application/json

### Path parameters

- **tid** (required)

  The tenant ID.
- **tagId** (required)

  The ID of the tag (e.g., mQhWWuPFNqti-w-AlNWHdA).
- **elementHash** (required)

  The element hash (e.g., 393ff13c9b519ec2).
- **tagElementType** (required)

  The type of element with which the tag is associated.

### Request headers

- **Interset-Version** (optional) -- String

  Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

### Query parameters

- **retries** (optional)

  The number of times to retry the update operation if a conflict occurs.

### Responses

`default`

successful operation

## POST /search/{tid}/tags/{tagId}/{tagElementType}/remove

*Remove a tag from mulitple elements*

Deletes a tag from a list of elements of the same type.

## Example Response (Status 200)

```
{
  "requestTime": 29,
  "data": {
    "message": "46b489f7f46588c6 successfully removed from entities:
["75c2599ddf50ea85", "75c2599ddf50ea86"]"
  },  "cached": "false"
}
```

## Consumes

- application/json

## Produces

- application/json

## Path parameters

- **tid** (required)

  The tenant ID.
- **tagId** (required)

  The ID of the tag (e.g., mQhWWuPFNqti-w-AlNWHdA).
- **tagElementType** (required)

  The type of element with which the tag is associated.

## Request body

ApiTagEntities

A list of element hashes.

## Request headers

- **Interset-Version** (optional) -- String

  Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

## Query parameters

- **retries** (optional)

  The number of times to retry the update operation if a conflict occurs.

## Responses

`default`

successful operation

# POST /search/{tid}/tags/{tagId}/update

*Update a tag*

Changes the specified a tag.

## Example Response (Status 200)

```
{
  "requestTime": 29,
  "data": {
    "name": "changedTag",
    "description": "testing tags",
    "entities": [],
    "id": "6f327e088def9386",
    "created": "2017-12-01T00:16:56.016Z",
    "createdBy": "td5",
    "modified": "2017-12-01T00:16:56.016Z",
    "modifiedBy": "td5",
    "source": "user"
  },
  "cached": "false"
}
```

## Consumes

- application/json

## Produces

- application/json

### Path parameters

- **tid** (required)

  The tenant ID.
- **tagId** (required)

  The ID of the tag (e.g., mQhWWuPFNqti-w-AlNWHdA).

### Request body

TagBase

Changes the name, description, and the list of entity hashes for the specified tag.

### Request headers

- **Interset-Version** (optional) -- String

  Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

### Responses

`default`

successful operation

# tenants

## DELETE /tenants/{tid}

*Delete a tenant*

Delete the specified tenant.

### Produces

- application/json

### Path parameters

- **tid** (required)

### Responses

`default`

successful operation

## DELETE /tenants/{tid}/users/{userId}

*Delete a user*

Delete the specified user from the specified tenant. Permissions and sessions for the user are also deleted. If the user exists in another tenant, that user is not deleted.

### Produces

- application/json

### Path parameters

- **tid** (required)
- **userId** (required)

### Responses

`default`

successful operation

## GET /tenants/{tid}

*Get tenant details*

Get details for the specified tenant.

### Produces

- application/json

### Path parameters

- **tid** (required)

### Return type

Tenant

### Example data

Content-Type: application/json

```
{
  "created" : "2000-01-23T04:56:07.000+00:00",
  "tenantId" : "a3b",
  "name" : "Interset"
}
```

### Responses

```
200
```

successful operation

## GET /tenants/{tid}/users

*Get list of users for tenant*

Get the list of users for the specified tenant.

### Produces

- application/json

### Path parameters

- **tid** (required)

### Return type

array[ApiTenantUser]

### Example data

Content-Type: application/json

```
[ {
  "persistentSessions" : false,
```

```
  "password" : "password123",
  "role" : "admin",
  "permissions" : "[\"ACCESS_INTELLIGENCE\",\"VIEW_INTELLIGENCE_RAW_
EVENTS\"]",
  "created" : 0,
  "tenantId" : "0",
  "name" : "Camilla Ferguson",
  "isActive" : true,
  "userId" : "camilla",
  "local" : false
}, {
  "persistentSessions" : false,
  "password" : "password123",
  "role" : "admin",
  "permissions" : "[\"ACCESS_INTELLIGENCE\",\"VIEW_INTELLIGENCE_RAW_
EVENTS\"]",
  "created" : 0,
  "tenantId" : "0",
  "name" : "Camilla Ferguson",
  "isActive" : true,
  "userId" : "camilla",
  "local" : false
} ]
```


### Responses

```
200
```

successful operation

## GET /tenants

*Get the list of tenants*

Get the list of all tenants.

### Produces

- application/json

### Return type

array[Tenant]

### Example data

Content-Type: application/json

```
[ {
  "created" : "2000-01-23T04:56:07.000+00:00",
  "tenantId" : "a3b",
  "name" : "Interset"
}, {
  "created" : "2000-01-23T04:56:07.000+00:00",
  "tenantId" : "a3b",
  "name" : "Interset"
} ]
```

### Responses

```
200
```

successful operation

## GET /tenants/{tid}/users/{userId}

*Get user details for a tenant*

Get details about the specified user for the specified tenant.

### Produces

- application/json

### Path parameters

- **tid** (required)
- **userId** (required)

### Return type

ApiTenantUser

### Example data

Content-Type: application/json

```
{
  "persistentSessions" : false,
  "password" : "password123",
  "role" : "admin",
  "permissions" : "[\"ACCESS_INTELLIGENCE\",\"VIEW_INTELLIGENCE_RAW_
EVENTS\"]",
  "created" : 0,
  "tenantId" : "0",
  "name" : "Camilla Ferguson",
  "isActive" : true,
  "userId" : "camilla",
  "local" : false
}
```


### Responses

```
200
```

successful operation

## PUT /tenants/{tid}

*Update tenant details*

### Consumes

- application/json

### Produces

- application/json

### Path parameters

- **tid** (required)

### Request body

Tenant

### Return type

Tenant

### Example data

Content-Type: application/json

```
{
  "created" : "2000-01-23T04:56:07.000+00:00",
  "tenantId" : "a3b",
  "name" : "Interset"
}
```

### Responses

```
200
```

successful operation

## PUT /tenants

*Set details for multiple tenants*

### Consumes

- application/json

### Request body

array[Tenant]

### Responses

```
default
```

successful operation

## PUT /tenants/{tid}/users/{userId}

*Update user details*

Create or update the details of a user, or link a user to a tenant.

When you link an existing user to a tenant, the body of the request must contain only the `role`, `userId` and `tenantId` fields. Any update to the `name` and `password` fields must be made

against a tenant with which the user is already associated, unless it is a new user, in which case it can be created and linked to a tenant in the same request.

## Consumes

- application/json

## Produces

- application/json

## Path parameters

- **tid** (required)
- **userId** (required)

## Request body

ApiTenantUser

## Request headers

- **Interset-Version** (optional) -- String

  Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

## Return type

ApiTenantUser

## Example data

Content-Type: application/json


```
{
  "persistentSessions" : false,
  "password" : "password123",
  "role" : "admin",
  "permissions" : "[\"ACCESS_INTELLIGENCE\",\"VIEW_INTELLIGENCE_RAW_
EVENTS\"]",
  "created" : 0,
  "tenantId" : "0",
  "name" : "Camilla Ferguson",
```

```
  "isActive" : true,
  "userId" : "camilla",
  "local" : false
}
```

### Responses

```
200
```

successful operation

# theme

## DELETE /theme/{tid}

*Delete a custom theme*

### Produces

- application/json

### Path parameters

- **tid** (required)

### Responses

```
default
```

successful operation

## DELETE /theme

*Delete a default theme*

### Produces

- application/json

### Responses

`default`

successful operation

## GET /theme

*Get default theme*

Returns a map of the default theme information, or {} if none is set. You can set one default theme for your cluster.

Themes change the look and feel of applications by altering colors, text labels, and images.

### Example Response (Status 200)

```
{
  "loginGradient1": "linear-gradient(#b4bbc6 65%, #737b83)",
  "loginGradient2": "linear-gradient(#eda24e 65%, #e56443)",
  "accent": "#333333",
  "navBar": "rgb(68, 68, 68)",
  "font1": "hsl(0, 0%, 33%)",
  "font2": "hsl(0, 0%, 40%)",
  "font3": "hsl(0, 0%, 67%)",
  "bannerLabel": "Classified",
  "companyName": "Your Company",
  "footerLabel": "Effectively enhancing corporate synergy",
  "footerEnabled": "false",
  "loginLogo": "(optional - base64 encoded png, 100px height)",
  "navBarLogo": "(optional - base64 encoded png, 80px height)"
}
```

### Produces

- application/json

### Responses

`default`

successful operation

## GET /theme/{tid}

*Get a custom theme*

Returns a map of the custom theme information for the specified tenant, or {} if none is set.

Themes change the look and feel of applications by altering colors, text labels, and images.

## Example Response (Status 200)

```
{
  "loginGradient1": "linear-gradient(#b4bbc6 65%, #737b83)",
  "loginGradient2": "linear-gradient(#eda24e 65%, #e56443)",
  "accent": "#333333",
  "navBar": "rgb(68, 68, 68)",
  "font1": "hsl(0, 0%, 33%)",
  "font2": "hsl(0, 0%, 40%)",
  "font3": "hsl(0, 0%, 67%)",
  "bannerLabel": "Classified",
  "companyName": "Your Company",
  "footerLabel": "Effectively enhancing corporate synergy",
  "footerEnabled": "false",
  "loginLogo": "(optional - base64 encoded png, 100px height)",
  "navBarLogo": "(optional - base64 encoded png, 80px height)"
}
```

## Produces

- application/json

## Path parameters

- **tid** (required)

## Responses

```
default
```

successful operation

# PUT /theme

*Update default theme*

Sets the default theme. You can set one default theme for your cluster.

Themes change the look and feel of applications by altering colors, text labels, and images.

### Example Request Body

```
{
  "loginGradient1": "linear-gradient(#b4bbc6 65%, #737b83)",
  "loginGradient2": "linear-gradient(#eda24e 65%, #e56443)",
  "accent": "#333333",
  "navBar": "rgb(68, 68, 68)",
  "font1": "hsl(0, 0%, 33%)",
  "font2": "hsl(0, 0%, 40%)",
  "font3": "hsl(0, 0%, 67%)",
  "bannerLabel": "Classified",
  "companyName": "Your Company",
  "footerLabel": "Effectively enhancing corporate synergy",
  "footerEnabled": "false",
  "loginLogo": "(optional - base64 encoded png, 100px height)",
  "navBarLogo": "(optional - base64 encoded png, 80px height)"
}
```

### Consumes

- application/json

### Produces

- application/json

### Request body

ApiTheme

### Responses

```
default
```

successful operation

## PUT /theme/{tid}

*Update a custom theme*

Sets the custom theme for the specified tenant.

Themes change the look and feel of applications by altering colors, text labels, and images.

### Example Request Body

```
{
  "loginGradient1": "linear-gradient(#b4bbc6 65%, #737b83)",
  "loginGradient2": "linear-gradient(#eda24e 65%, #e56443)",
  "accent": "#333333",
  "navBar": "rgb(68, 68, 68)",
  "font1": "hsl(0, 0%, 33%)",
  "font2": "hsl(0, 0%, 40%)",
  "font3": "hsl(0, 0%, 67%)",
  "bannerLabel": "Classified",
  "companyName": "Your Company",
  "footerLabel": "Effectively enhancing corporate synergy",
  "footerEnabled": "false",
  "loginLogo": "(optional - base64 encoded png, 100px height)",
  "navBarLogo": "(optional - base64 encoded png, 80px height)"
}
```

### Consumes

- application/json

### Produces

- application/json

### Path parameters

- **tid** (required)

### Request body

ApiTheme

### Responses

```
default
```

successful operation

## url

# POST /url

*Create a hash for a URL*

Creates and returns a hash for the specified URL.

## Example Request Body

```
{
  "url": "http://localhost:3000/dashboard/0/entities?ts=-
2660400&te=133024&q=&dashboard=ts%3D-2660400%26te%3D133024%26q%3D"
}
```

## Example Response (Status 200)

```
{
  "hash": "89653e5d"
}
```

## Produces

- application/json

## Request body

ApiUrl

## Return type

ApiHash

## Example data

Content-Type: application/json

```
{
  "hash" : "hash"
}
```

## Responses

```
200
```

successful operation

## GET /url/{hash}

*Redirect to the URL for a hash*

Redirects the user interface to the URL associated with the specified hash.

### Produces

- application/json

### Path parameters

- **hash** (required)

  The URL's hash.

### Responses

`default`

successful operation

# users

## GET /users

*Get the list of users*

Gets the list of all users.

### Produces

- application/json

### Return type

array[Tenant]

### Example data

Content-Type: application/json

```
[ {
  "created" : "2000-01-23T04:56:07.000+00:00",
  "tenantId" : "a3b",
  "name" : "Interset"
}, {
  "created" : "2000-01-23T04:56:07.000+00:00",
  "tenantId" : "a3b",
  "name" : "Interset"
} ]
```

### Responses

```
200
```

successful operation

# Models

## ApiAction

- **success** -- Boolean
- **detail** -- String

## ApiCredentials

- **username** -- String
- **password** -- String

## ApiDashboard

- **doc** -- String
- **name** -- String
- **description** -- String
- **tid** -- String

- **userId** -- String
- **id** -- Integer
  Format: int32
- **lastModifiedBy** -- String
- **creationDate** -- Date
  Format: date-time
- **lastModifiedDate** -- Date
  Format: date-time
- **home** -- Boolean
- **tags** -- array[ApiDashboardTag]
- **private** -- Boolean

## ApiDashboardTag

- **name** -- String
  A name for the tag.
- **id** -- String
  Tag ID

## ApiEntityNameRequest

- **entityName** -- String
- **entityType** -- String

## ApiHash

- **hash** -- String

## ApiMetaRequest

- **resourceType***(Required)* -- String

  The type of the meta resource e.g. comment, annotation, tag, dashboard, visualization and so on.

  Enumeration:

  - comment
  - annotation
  - dashboard
  - tag
  - tuning
  - anomalySeen

- **destinationId***(Required)* -- String

  The ID of the destination.

- **destinationType***(Required)* -- String

  The type of the source. Currently supported

  Enumeration:

  - alerts
  - anomalies
  - entities

- **content***(Required)* -- String

  The raw content of the object. This is a full text search. Larger than 128KB can significantly impact the search performance.

- **contentType***(Required)* -- String

  Currently supported: `markdown`, `plaintext`, `html`

  Enumeration:

  - plaintext
  - markdown
  - json
  - html

## ApiSavedSearches

- **name** -- String
- **doc** -- JsonNode
- **columns** -- JsonNode

## ApiSavedSearchesDraft

- **docDraft** -- JsonNode
- **columnsDraft** -- JsonNode

## ApiSavedSearchesResponse

- **name** -- String
- **doc** -- JsonNode
- **columns** -- JsonNode
- **id** -- Integer
  Format: int32
- **docDraft** -- JsonNode
- **columnsDraft** -- JsonNode

## ApiSessionTenant

- **userId** -- String
  The user ID.
- **tenantId** -- String
  The tenant ID.
- **permission** -- array[String]
  The user's permissions for this tenant.
  Enumeration:
- **tenantName** -- String

The tenant name.

- **features** -- array[String]
  A list of UI configuration features.

## ApiSimpleDashboard

- **doc** -- String
- **name** -- String
- **description** -- String
- **private** -- Boolean

## ApiSimpleDashboardTag

- **name** -- String
  A name for the tag.

## ApiTagEntities

- **entities** -- array[String]

## ApiTenantUser

- **userId** -- String
  The user ID.
- **tenantId** -- String
  The tenant ID.
- **name** -- String
  The user's display name.
- **role** -- String
  The user's role for this tenant. The role determines the permissions for the user.

Enumeration:

- user
- admin
- root
- none

- **permissions** -- array[String]
  The user's permissions for this tenant.
  Enumeration:
- **isActive** -- Boolean
  When `false`, this user has been marked as inactive in an external authentication service.
- **password** -- String
- **created** -- Long
  The date in milliseconds when this user was created. Format: int64
- **persistentSessions** -- Boolean
  When set to `true`, sessions will not expire for this user.
- **local** -- Boolean
  When set to `true`, this user is local.

## ApiTheme

- **loginGradient1** -- String
- **loginGradient2** -- String
- **accent** -- String
- **navBar** -- String
- **font1** -- String
- **font2** -- String
- **font3** -- String
- **banner** -- String
- **bannerLabel** -- String
- **companyName** -- String

- **footerLabel** -- String
- **footerEnabled** -- Boolean
- **loginLogo** -- String
- **navBarLogo** -- String

## ApiUrl

- **url** -- String

## DbUser

- **userId** -- String
- **name** -- String
- **isActive** -- Boolean
- **passwordHash** -- String
- **passwordSalt** -- String
- **timestamp** -- Date
  Format: date-time
- **persistentSessions** -- Boolean
- **properties** -- map[String, String]

## JsonNode

- **valueNode** -- Boolean
- **containerNode** -- Boolean
- **missingNode** -- Boolean
- **nodeType** -- String

  Enumeration:

    - ARRAY
    - BINARY
    - BOOLEAN
    - MISSING
    - NULL
    - NUMBER
    - OBJECT
    - POJO
    - STRING
- **pojo** -- Boolean
- **number** -- Boolean
- **integralNumber** -- Boolean
- **floatingPointNumber** -- Boolean
- **short** -- Boolean
- **int** -- Boolean
- **long** -- Boolean
- **float** -- Boolean
- **double** -- Boolean
- **bigDecimal** -- Boolean
- **bigInteger** -- Boolean
- **textual** -- Boolean
- **boolean** -- Boolean
- **binary** -- Boolean
- **object** -- Boolean
- **array** -- Boolean
- **empty** -- Boolean
- **null** -- Boolean

## LoginResponse

- **access_token** -- String

  Access token.
- **token_type** -- String

  Token type (e.g., Basic, Bearer); usually Bearer.

## RawEventsGraphRequest

- **query** -- JsonNode
- **sortFields** -- array[SortField]
- **datasources** -- array[String]

  Enumeration:
- **ts** -- Long

  Format: int64
- **te** -- Long

  Format: int64
- **grouping** -- String
- **fields** -- array[String]

## RawEventsRequest

- **query** -- JsonNode
- **sortFields** -- array[SortField]
- **datasources** -- array[String]

  Enumeration:
- **ts** -- Long

  Format: int64
- **te** -- Long

Format: int64

## RawEventsTypeaheadRequest

- **query** -- JsonNode
- **sortFields** -- array[SortField]
- **datasources** -- array[String]

  Enumeration:
- **ts** -- Long

  Format: int64
- **te** -- Long

  Format: int64
- **count** -- Integer

  Format: int32
- **field** -- String
- **text** -- String
- **sort** -- String

  Enumeration:
  - asc
  - desc

## ServiceProxyInfo

- **schema** -- String
- **prefix** -- String
- **description** -- String
- **menu** -- String
- **permissionsByMethod** -- map[String, String]

  Enumeration:

- **name** -- String

## Session

- **user** -- DbUser
- **accessToken** -- String
- **expirationDate** -- Date
  Format: date-time
- **maxSessionAge** -- Integer
  Format: int32
- **permissionsPerTenant** -- map[String, array[String]]
  Enumeration:

## SessionInfo

- **userId** -- String
  The user ID.
- **userDisplayName** -- String
  The user's display name.
- **extendedApi** -- array[ServiceProxyInfo]
  The available proxied APIs.
- **persistentSessions** -- Boolean
  When set to `true`, sessions will not expire for this user.
- **disableTenantManagement** -- Boolean
  When set to `true`, multi-tenant support is disabled.
- **accessToken** -- String
  The current access token for this user
- **permissions** -- array[ApiSessionTenant]
- **analyticsTuningAvailable** -- Boolean
  Set to `true` to allow the tuning of analytics.
- **swaggerEndpoints** -- map[String, String]

Available Swagger Endpoints

## SortField

- **field** -- String
- **order** -- String

  Enumeration:
  - asc
  - desc

## TagBase

- **name** -- String

  A name for the tag.
- **description** -- String

  A description of the tag.
- **entities** -- array[String]

## Tenant

- **tenantId** -- String

  The tenant ID. Must be 1 to 3 alpha-numerical characters.
- **name** -- String

  The tenant name.
- **created** -- Date

  The tenant creation date. Format: date-time

# Exports API Reference

Version: 24.1

BasePath: /exports

The Exports API provides a mechanism for exporting reports that contain the information presented in the Intelligence user interface.

## Construct Exports API URLs

To call an endpoint in this API, use the fully-qualified domain name (FQDN) of Intelligence, and append the base path (`/exports`) followed by the path listed in the sections that follow. For example, to call the `GET /info/build` endpoint, use the following URL with the GET method:

```
https://<FQDN of Intelligence>/exports/info/build
```

## Exports API Endpoints

### GET /dashboard

*Get risk report*

Generates a detailed report of the organizational risk, including sections for Top Anomalies and Violations, Top Risky Users, Top Risky Projects, and so on.

#### Consumes

- application/json

#### Produces

- application/pdf

#### Query Parameters

- **tid**
  The tenant ID.
- **format**
  The format of the exported dashboard (`pdf`, `jpeg`, or `png`).

- **ts**
  Start time in seconds. If no value is provided, the start time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.
- **te**
  End time in seconds. If no value is provided, the end time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.
- **tz**
  The timezone in which the results should be returned (e.g., +5:00, America/Montreal, EST).

### Return type

String

### Responses

```
200 OK
```

Successful operation

## GET /info/build

*Get version information*

Returns information about this version of the Exports API.

### Example Response (Status 200)

```
{"Build-Number":"5.7.0.937"}
```

### Produces

application/json

### Responses

```
200 OK
```

Successful operation

# Publication Status

Released: Wednesday, January 10, 2024

## Support

### Contact Information

| | |
|---|---|
| **Phone** | A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information |
| **Support Web Site** | https://softwaresupport.softwaregrp.com/ |
| **ArcSight Product Documentation** | https://www.microfocus.com/documentation/arcsight/ |

# Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

**Feedback on Developer's Guide for ArcSight Intelligence (Intelligence 24.1)**

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to Documentation-Feedback@microfocus.com.

We appreciate your feedback!