Armis Centrix™

Armis API Guide - Version 2.1

November 9, 2023

Table of contents

Document version control

Version	Date	Change
1.4.0	October 2022	Added device tagging and custom property updates. Removed sections on users, ARP tables, and integrations.
1.5.0	November 2022	Added policy examples.
1.6.0	January 2023	Updated examples. Application retrieval from Armis.
1.7.0	February 2023	Updated formatting.
1.8.0	May 2023	Rearranged sections and edited text. Added note about *AQL* being renamed *ASQ*. Added note "The Python examples in this document do not include import requests." Added the following sections: "Dashboards", "Reports", "Vulnerability".
1.8.1	July 2023	Formatting
2.0	October 2023	Add additional sections such as ARP, Boundaries, Business applications, Certificate, Collectors, Device applications, Device boundaries, Device properties, Devices tags, Integrations, Roles, Search, and Sites. Additional examples, improved formatting.
2.1	November 9, 2023	Updates to examples in Basic instructions and best practices.

Armis API Integration Guide sections:

1 Overview

This guide describes the Armis API, which the Armis Centrix™ platform provides. You can use the Armis API to simplify the retrieval and uploading of data. This guide is intended to enable technical teams to quickly get up to speed with the Armis API and to realize proof of value as fast as possible.

Armis recommends using a tool such as Postman or Paw to quickly develop and test the Armis API. This will enable the developer to quickly debug requests to and responses from the API. These calls can then be implemented in your platform of choice.

For more information on the Armis Centrix™ platform, refer to the *Armis user guide*.

> **NOTE:** The name *Armis Query Language* (*AQL*) was changed to *Armis Standard Query* (*ASQ*). However, the API continues to use `aql` throughout.

2 Basic instructions and best practices

2.1 Obtaining your authorization token

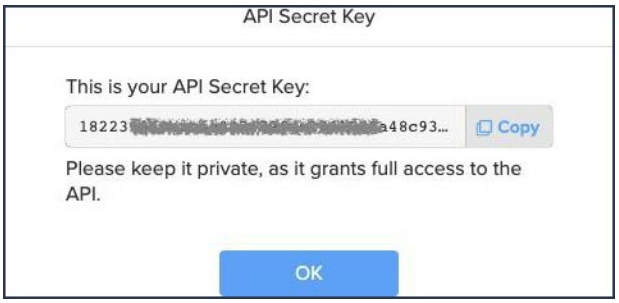
The authorization token is used for authentication of the Armis API.

To obtain your secret key from the Armis console:

- Go to **Settings** > **API Management**.

If the secret key has not already been created, do the following:

1. Click **Create** to create the secret key.
2. Click **Show** to access the secret key. The following dialog is displayed, from which you can copy your secret key.



3. Once you have obtained the secret key, perform a call to the Armis API to obtain the authentication token. This can be performed as a simple REST query.

> **NOTE:** The Python examples in this document do not include import requests.

The following are examples:

cURL

```
curl -X 'POST' \
  'https://<armis-instance>.armis.com/api/v1/access_token/' \
  -H 'accept: application/json' \
  -H 'Content-Type: application/x-www-form-urlencoded' \
  -d 'secret_key=353dfd76501e8650869b066b37463c7275122c39[redacted]'
```

2.1.1 Example

This will generate a response payload as follows in JSON format:

```
{
 "data": {
  "access_token": "e9a237ea027ff6096b1225b9c2a9bbe3ca[redacted]",
  "expiration_utc": "2021-06-14T22:30:45.373426+00:00"
 },
 "success": true
}
```

Here, the `access_token` is your authentication token to be used in subsequent Armis API calls.

> **NOTE:** The authentication token has a lifetime of 15 minutes, so if an API call fails, a new authentication token may need to be obtained. Check the return code of the API call. If the access token is invalid, the call will result in an HTTP status of *402 Unauthorized*, and the response payload will be as follows:

```
{
  "message": "Invalid access token.",
  "success": false
}
```

2.2 Simultaneous connections

Armis recommends no more than eight simultaneous connections to the Armis API.

2.3 Paging through large amounts of data

To page through large amounts of data, a simple modification to the Armis API REST calls is all that is required to implement this functionality. We will demonstrate this for device data, but the principle is the same for all REST calls to the Armis API.

2.4 Getting large device data sets

The following query shows how to get large amounts of device information from Armis Centrix™. Let's assume that we want to use a page size of 100, then our initial call to the API will look like this (to retrieve the first 100 devices):

cURL

```
curl "https://<armis-
instance>.armis.com/api/v1/search/?aql=in:device&length=100"
-H 'Authorization: <access-token>'
```

Python

```
response = requests.get(
url="https://<armis-instance>.armis.com/api/v1/search/",
            params={"aql": "in:devices ",
                    "length": "100"},
           headers={"Authorization": <access-token>})
```

2.4.1 Example: Retrieve the first 100 devices

The response will be a JSON array of devices similar to this:

```
{
   "data": {
     "count": 100,
     "next": 100,
     "prev": null,
     "results": [
      … (100 device entries)
      ],
     "total": 4415
   },
   "success": true
}
```

The key point here is that the "length=100" attribute is used to define the length of the "page" that you want to use.

However, we only retrieved the first 100 devices in the list. To get the next 100 devices in the list, we would then make the following call to the API:

cURL

```
curl "https://<armis-
instance>.armis.com/api/v1/search/?aql=in:device&length=100&from=100" -H
'Authorization: <access-token>'
```

Python

```
response = requests.get(
url="https://<armis-instance>.armis.com/api/v1/search/",
            params={"aql": "in:devices ",
                    "length": "100"},
                    "from": "100"},
            headers={"Authorization": <access-token>})
```

2.4.2 Example: Get the next 100 devices

The response will be a JSON array of devices similar to this:

```
{
        "data": {
           "count": 100,
           "next": 200,
           "prev": null,
           "results": [
             … (100 device entries)
             ],
           "total": 4415
        },
        "success": true
}
```

There are two key points to take away from this invocation. The first is that we have added the "from"="100" parameter to the API call. This indicates where to start the retrieval of the next set of devices, that is, where the next page starts. The second point to notice is that we have the "next": 200 value in the response from the API call. This indicates where to start the next API invocation with our chosen page size of 100.

The recommended procedure is to note the total number of device entries in Armis Centrix™ from the initial call to the API, then simply iterate through the appropriate number of pages (with your selected page size) until all of the device information has been retrieved.

> **NOTES:**
> - The Armis API has a maximum page size of 5,000.
> - Calculating the total number of records, which happens when the query is executed can take time. For time sensitive queries, filtering by time precludes iterating through all of the records in the result set and can significantly speed up query response.

2.5 Iterating through devices or alerts by time

In the case of finding devices or alerts over a specific time period, it is useful to specify the desired time frame and order the results accordingly.

2.5.1 Example

The following example illustrates how to get all devices seen over the last 7 days, and the results are ordered by the device ID. This is important because you do not want to miss any devices because the default sort order is by lastSeen, which can result in different results.

cURL

```
curl "https://<armis-
instance>.armis.com/api/v1/search/?aql=in:devices&timeFrame=7%20Days&
orderBy=id" -H 'Authorization: <access-token>'
```

Python

```
response = requests.get(    url="https://<armis-
instance>.armis.com/api/v1/search/",
       params={"aql": "in:devices ",
           "timeFrame": "7 Days",
           "orderBy": "id" },
       headers={"Authorization": <access-token>})
```

The response will be a JSON array of devices similar to this:

```
{
       "data": {
         "count": 10,
         "next": 10,
         "prev": null,
         "results": [
          … (n device entries ordered by the “id” field)
          ],
         "total": 4415
       },
       "success": true
}
```

> **NOTE:** Iterating over a set of results it is the recommended best practice to `orderBy` a fixed parameter (`deviceId` for example) in order to not to miss data between pages. This is because the default order is by `lastSeen`, so results can change.

2.6 Searching for devices or alerts by time

In the case of finding devices or alerts that have been either `lastSeen` (in the case of devices) or `time` (in the case of an alert), it is useful to specify the desired time frame in general using `before:YYYY-MM-DDTHH:MM:SS` and `after:YYYY-MM-DDTHH:MM:SS`.

For more information of searching for devices, see in:devices

2.6.1 Devices example

The following example shows how to get all devices seen on and after 2022-03-10.

> **NOTE:** The device search endpoint only supports the `after:` clause and is based on the **date** portion and is compared against the `lastSeen` value for the device.

The ASQ is: `in:devices after:2022-03-10`

cURL

```
curl "https://<armis-
instance>.armis.com/api/v1/search/?aql=in%3Adevices%20after%3A2022-03-10"
-H 'Authorization: <access-token>'
```

Python

```
response = requests.get(    url="https://<armis-
instance>.armis.com/api/v1/search/",
       params={"aql": "in:devices after:2022-03-10"},
       headers={"Authorization": <access-token>})
```

2.6.2 Example—Alerts by time

The following example illustrates how to get all alerts seen between the after: 2022-03- 11T14:00:00 and the before: 2022-03-16T14:00:00.

> **NOTE:** The alerts search endpoint supports both the `before:` and `after:` clauses and is based on the ***full datetime*** specified and is compared against the `time` value for the alert.

The ASQ is: `in:alerts after:2022-03-11T14:00:00 before:2022-03- 16T14:00:00`

cURL

```
curl "https://<armis-instance>.armis.com/api/v1/search/?aql=
in%3Aalerts%20after%3A2022-03-11T14%3A00%3A00%20before%3A2022-03-
16T14%3A00%3A00" -H 'Authorization: <access-token>'
```

Python

```
response = requests.get(    url="https://<armis-
instance>.armis.com/api/v1/search/",
       params={"aql": "in:alerts after:2022-03-11T14:00:00 before:2022-03-
16T14:00:00"},
       headers={"Authorization": <access-token>})
```

3 Access token

3.1 Returning a temporary access token

POST `/api/v1/access_token/`

3.1.1 URI parameters

Name	Type	Description
secret-key	string (formData)	Secret key.

3.1.2 Example

The response will be a JSON array of alerts similar to this:

```
{
  "data": {
    "access_token": "85c5eb5d4fb647bc91a1db46824aac3a83a86117…",
    "expiration_utc": "2023-10-11T09:49:00.818613+00:00"
  },
  "success": true
}
```

3.1.3 Responses

This API call has the following HTTP status codes:

Code	Description
200	OK.
400	Bad request, please check the arguments you passed.

4 Alerts

For more information about alerts, see the Armis user guide.

4.1 Updating alerts with the Armis Centrix™ status

PATCH `/api/v1/alerts/{alert_id}/`

To update a specific alert, the `alertId` is required. It is the unique numeric identifier of the alert in Armis Centrix™. Only individual alerts can be updated with this method and the update is performed using the HTTP PATCH call.

4.1.1 Permissions required

- **Alert** > **Manage** > **Resolve**
- **Alert** > **Manage** > **Suppress**

4.1.2 URI parameters

Name	Type	Description
alert_id * Required	(path)	The ID of the designated alert
status * Required	string (formData)	The status of the designated alert Available values : UNHANDLED, SUPPRESSED, RESOLVED

There are three states that can be attributed to an Armis alert:

- UNHANDLED
- SUPPRESSED
- RESOLVED

4.1.3 Example—Setting the alert status to “UNHANDLED”

cURL

```
curl -X "PATCH" "https://<armis-instance>.armis.com/api/v1/alerts/<alertId>/"
      -H 'Authorization: <access-token>'
      -H 'Content-Type: application/x-www-form-urlencoded'
      -d "status=UNHANDLED"
```

Python

```
response = requests.patch(
url="https://<armis-instance>.armis.com/api/v1/alerts/<alertId>/",
headers={"Authorization": <access-token>,
         "Content-Type": "application/x-www-form-urlencoded;
charset=utf-8"},
data = {"status": "UNHANDLED"})
```

If the call is successful, it will return the following:

```
{
   "success": true
}
```

If the alert was already in the UNHANDLED state, it will return the following:

```
{
    "message": "Nothing to change",
    "success": false
}
```

4.1.4 Example—Setting the alert status to “SUPPRESSED”

cURL

```
curl -X "PATCH" "https://<armis-instance>.armis.com/api/v1/alerts/<alertId>/"
       -H 'Authorization: <access-token>'
       -H 'Content-Type: application/x-www-form-urlencoded'
       -d "status=SUPPRESSED"
```

Python

```
response = requests.patch(url="https://<armis-
instance>.armis.com/api/v1/alerts/<alertId>/",
headers={"Authorization": <access-token>,
         "Content-Type": "application/x-www-form-urlencoded;
charset=utf-8"},
data = {"status": "SUPPRESSED"})
```

If the call is successful, it will return the following:

```
{
       "success": true
}
```

If the alert was already in the SUPPRESSED state, it will return the following:

```
{
        "message": "Nothing to change",
        "success": false
}
```

4.1.5 Example—Setting the alert status to “RESOLVED”

cURL

```
curl -X "PATCH" "https://<armis-instance>.armis.com/api/v1/alerts/<alertId>/"
       -H 'Authorization: <access-token>'
       -H 'Content-Type: application/x-www-form-urlencoded'
       -d "status=RESOLVED"
```

Python

```
response = requests.patch(
url="https://<armis-instance>.armis.com/api/v1/alerts/<alertId>/",
headers={"Authorization": <access-token>,
         "Content-Type": "application/x-www-form-urlencoded;
charset=utf-8"},
data = {"status": "RESOLVED"})
```

If the call is successful, it will return the following:

```
{
        "success": true
}
```

If the alert was already in the RESOLVED state, it will return the following:

```
{
        "message": "Nothing to change",
        "success": false
}
```

4.1.6 Response

This API call has the following HTTP status codes:

Code	Description
200	OK.
400	Nothing to change.
404	Unknown alert.

5 ARP

5.1 Uploading an ARP table

POST /api/v1/arp/

5.1.1 Permissions required

- **Device** > **Manage**

5.1.2 URI parameters

Name	Type	Description
arp * Required	file	CSV File encoded in UTF-8.
integrationGroupId	integer	Default value: 0
expiration * Required	number ($float)	Expiration for ARP table in days.

5.1.3 Example

To upload an ARP table into the Armis platform, the following example uses Python:

Python

```
arp_table_data = []

expiration = 1

arp_table_data.append(["10.100.100.1", "11:22:33:44:55:66"])

stream = io.StringIO()
writer = csv.writer(stream, skipinitialspace=True)
writer.writerow(["ip", "mac"])

i = 0
for i in range(len(arp_table_data)):
    writer.writerow(arp_table_data[i])
stream.seek(0)

response = requests.post(
url="https://<armis-instance>.armis.com/api/v1/arp/",
     params={"expiration": expiration},
     headers={"Authorization": <access-token>},
     files = {"arp": stream})
```

The response is a JSON array of devices similar to this (if successful):

```
{ "success": true }
```

5.1.4 Responses

This API call has the following HTTP status codes:

Code	Description
200	OK.
401	Authorization information is missing or invalid. **Name**—Authorization **Description**—The `access_token` obtained using the `/access_token/` endpoint. **Type**—string

6 Boundaries

6.1 Returning all boundaries information

GET `/api/v1/boundaries/`

Pagination is supported.

6.1.1 URI parameters

Name	Type	Description
from	integer (query)	Paging from.
length	integer (query)	Paging length.
affectedSites	(query)	Filter by affected sites. If omitted, all boundaries will be returned.
includeTotal	bool (query)	Return total count, default False.
fields	(query)	Fields to show. If omitted, returns a default subset of fields.

6.1.2 Example

The response will be a JSON array of devices similar to this:

```
{
  "data": {
    "boundaries": [
      {
        "affectedSites": "",
        "id": 3,
        "name": "Off Network",
        "ruleAql": null
      },
      {
        "affectedSites": "",
        "id": 4,
        "name": "network1",
        "ruleAql": {
          "and": [
            "category:Computers"
          ]
        }
      },
      {
        "affectedSites": "",
        "id": 6,
        "name": "new boundary - test when it fails",
        "ruleAql": {
          "and": [
            "type:\"Access Points\""
          ]
        }
      },
      {
        "affectedSites": "Meraki,switch",
        "id": 7,
        "name": "asdf",
        "ruleAql": {
          "and": [
            "name:rule1"
          ]
        }
      }
    ],
    "count": 4,
    "next": 7,
    "prev": 3
  },
  "success": true
}
```

6.1.3 Response parameters

Name	Type	Description
affectedSites	string	Specific sites affected by the boundary logic. E.g., Meraki, Switch, Site A, Site B.
id	integer	The ID assigned to the boundary.
name	string	The boundary's name. E.g., Corporate, Guest, Off Network.
ruleAql	JSON	The rule ASQ parameters.

6.1.4 Responses

This API call has the following HTTP status codes:

Code	Description
200	OK.
400	Bad request.
401	Authorization information is missing or invalid. **Name**—Authorization. **Description**—The `access_token` obtained using the `/access_token/` endpoint. **Type**—string.

6.2 Getting a boundary by ID

GET `/api/v1/boundaries/{boundary_id}/`

6.2.1 URI parameters

Name	Type	Description
boundary_id * Required	(path)	The boundary ID in the Armis system.
fields	(query)	Fields to show. If omitted, returns a default subset of fields.

6.2.2 Example


```
{
  "data": {
    "affectedSites": "",
    "id": 1,
    "name": "Corporate",
    "ruleAql": {
      "or": [
        "broadcastSsid:Sky,Arm",
        "lastConnectedSsid:Sky,Arm"
      ]
    }
  },
  "success": true
}
```


6.2.3 Response parameters

Name	Type	Description
affectedSites	string	Specific sites affected by the boundary logic. E.g., Meraki, Switch, Site A, Site B.
id	integer	The ID assigned to the boundary.
name	string	The boundary's name. E.g., Corporate, Guest, Off Network.
ruleAql	JSON	The rule ASQ parameters.

6.2.4 Responses

This API call has the following HTTP status codes:

Code	Description
200	OK.
400	Bad request, please check the arguments you passed.
401	Authorization information is missing or invalid. **Name**—Authorization. **Description**—The `access_token` obtained using the `/access_token/` endpoint. **Type**—string.
404	Unknown boundary.

6.3 Creating a new boundary

POST `/api/v1/boundaries/`

6.3.1 URI parameters

Name	Type	Description
site object	(body)	JSON describing the boundary.

6.3.2 Example

```
{
   "affectedSites": "siteA, siteB",
   "name": "my boundary name",
   "ruleAql": {
     "or": [
       "type:ACCESS_POINT"
     ]
   }
}
```

6.3.3 Responses

This API call has the following HTTP status codes:

Code	Description
201	Request accepted and sent for further processing.
400	Bad request.
401	Authorization information is missing or invalid. **Name**—Authorization. **Description**—The `access_token` obtained using the `/access_token/` endpoint. **Type**—string.

6.4 Deleting a boundary

DELETE `/api/v1/boundaries/{boundary_id}/`

6.4.1 URI parameters

Name	Type	Description
boundary_id * Required	(path)	The boundary ID in the Armis system.

6.4.2 Responses

This API call has the following HTTP status codes:

Code	Description
204	The entity deleted successfully.
400	Bad request, please check the arguments you passed.
401	Authorization information is missing or invalid. **Name**—Authorization. **Description**—The `access_token` obtained using the `/access_token/` endpoint. **Type**—string.
404	Unknown boundary.

6.5 Updating a boundary

PATCH `/api/v1/boundaries/{boundary_id}/`

6.5.1 URI parameters

Name	Type	Description
boundary_id * Required	(path)	The boundary ID in the Armis system.
site	object (body)	JSON describing the boundary.

6.5.2 Example

```
{
   "affectedSites": "siteA, siteB",
   "name": "my boundary name",
   "ruleAql": {
     "or": [
       "type:ACCESS_POINT"
     ]
   }
}
```

6.5.3 Responses

This API call has the following HTTP status codes:

Code	Description
200	OK.
400	Bad request, please check the arguments you passed.
401	Authorization information is missing or invalid. **Name**—Authorization. **Description**—The `access_token` obtained using the `/access_token/` endpoint. **Type**—string.
404	Unknown boundary.

7 Business applications

7.1 Bulk operation associating devices to business applications

POST `/api/v1/business-application-device-associations/_bulk/`

7.1.1 Permissions required

- **Business Applications** > **Manage** > **Upsert**

7.1.2 URI parameters

Name	Type	Description
body	array[object] (body)	

7.1.3 Example

```
[
  {
    "upsert": {
      "businessApplicationId": 0,
      "deviceId": 0
    }
  }
]
```

7.1.4 Responses

This API call has the following HTTP status codes:

Code	Description
207	Each item in the request has been processed on its own. Response indicates status of each individual item.
400	Bad request, please check the arguments you passed.
401	Authorization information is missing or invalid. **Name**—Authorization. **Description**—The `access_token` obtained using the `/access_token/` endpoint. **Type**—string.

7.2 Bulk operation on business applications

POST `/api/v1/business-applications/_bulk/`

7.3 Permissions required

- **Business Applications** > **Manage** > **Upsert**

7.3.1 URI parameters

Name	Type	Description
body	array[object]	

7.3.2 Example

```
[
  {
     "upsert": {
       "businessCriticality": "CRITICAL",
       "businessOwnerFullName": "Iorek B",
       "businessUnit": "",
       "description": "Database application to store our users",
       "environmentName": "Env1",
       "identifier": "aaa",
       "installationType": "SAAS",
       "name": "My_app",
       "source": "SERVICENOW",
       "type": "HOMEGROWN"
     }
  }
]
```

7.3.3 Responses

This API call has the following HTTP status codes:

Code	Description
207	Each item in the request has been processed on its own. Response indicates status of each individual item.
400	Bad request, please check the arguments you passed.
401	Authorization information is missing or invalid. **Name**—Authorization. **Description**—The `access_token` obtained using the `/access_token/` endpoint. **Type**—string.

7.4 Getting business application by ID

`GET /api/v1/business-applications/{business_application_id}/`

7.4.1 Permissions required

- **Business Applications** > **Read**

7.4.2 URI parameters

Name	Type	Description
business_application_id * Required	Type: (path)	Armis Business Application ID.

7.4.3 Example


```
{
  "data": [
    {
      "businessCriticality": "Critical",
      "businessOwner": "John",
      "businessUnit": null,
      "description": "Database application to store our users",
      "deviceIds": [
        2145,
        10,
        1,
        3,
        2
      ],
      "firstSeen": "2023-05-09T08:32:05.223649+00:00",
      "id": 6,
      "installationType": "SAAS",
      "lastSeen": "2023-10-15T20:51:59.585671+00:00",
      "name": "test business app",
      "operationalStatus": null,
      "type": "Homegrown"
    }
  ],
  "success": true
}
```

7.4.4 Response parameters

Name	Type	Description
businessCriticality	string	Describes how critical the business application is. Allowed values: Critical, High, Medium, Low. Mandatory.
businessOwner	string	Describes the Business Owner. Mandatory.
businessUnit	string	Describes the Business Unit.
description	string	A short description for the business application.
deviceIds	list	Device IDs.
firstSeen	timestamp	When the business application was first used.
id	integer	The ID assigned to the business application.
installationType	string	E.g., None, On-Premise, Cloud.
lastSeen	timestamp	When the business application was last used.
name	string	The name of the business application. Mandatory.
operationalStatus	string	Allowed values: Ready or Retired state
type	Enum	The application type. Allowed values: Commercial off the shelf, Homegrown

7.4.5 Responses

This API call has the following HTTP status codes:

Code	Description
200	OK.
401	Authorization information is missing or invalid. **Name**—Authorization. **Description**—The `access_token` obtained using the `/access_token/` endpoint. **Type**—string.
404	Unknown integration.

8 Certificate

8.1 Returning the tenant's root CA certificate (PEM file)

GET `/api/v1/certificates/root_ca/`

8.1.1 Permissions required

- **Settings**

8.1.2 URI parameters

None.

8.1.3 Responses

This API call has the following HTTP status codes:

Code	Description
200	OK.

9 Collectors

9.1 Returning existing collectors

GET /api/v1/collectors/

9.1.1 Permissions required

- **Settings** > **Collector** > **Read**

9.1.2 URI parameters

None.

9.1.3 Example


```
{
  "data": {
    "collectors": [
      {
        "clusterId": 0,
        "collectorNumber": 8100,
        "defaultGateway": "",
        "ipAddress": "",
        "lastSeen": "2023-10-17T14:28:13.360402+00:00",
        "macAddress": "",
        "name": "Armis Virtual Collector 8100",
        "status": "Active",
        "subnet": "",
        "type": "VM"
      }
    ],
    "count": 1,
    "next": null,
    "prev": null,
    "total": 1
  },
  "success": true
}
```


9.1.4 Responses

This API call has the following HTTP status codes:

Code	Description
200	OK.

9.2 Returning image URL collectors

GET /api/v1/collectors/_image/

9.2.1 Permissions required

- **Settings** > **Collector** > **Read**

9.2.2 URI parameters

None.

9.2.3 Responses

This API call has the following HTTP status codes:

Code	Description
200	OK.

9.3 Deleting a collector

DELETE /api/v1/collectors/{collector_id}/

9.3.1 Permissions required

- **Settings** > **Collector** > **Manage**

9.3.2 URI parameters

Name	Type	Description
collector_id * Required	(path)	Armis collector ID.

9.3.3 Responses

This API call has the following HTTP status codes:

Code	Description
200	OK.
400	Collector deletion error.
401	Unauthorized Collector ID.
404	Unknown Collector ID.

9.4 Getting collector by ID

`GET /api/v1/collectors/{collector_id}/`

9.4.1 Permissions required

- **Settings** > **Collector** > **Read**

9.4.2 URI parameters

Name	Type	Description
collector_id * Required	(path)	Armis collector ID.

9.4.3 Example


```
{
  "data": {
    "clusterId": 0,
    "collectorNumber": 8153,
    "defaultGateway": "",
    "ipAddress": "",
    "lastSeen": "2023-10-17T14:37:13.147483+00:00",
    "macAddress": "",
    "name": "Armis Virtual Collector 8153",
    "status": "Active",
    "subnet": "",
    "type": "VM"
  },
  "success": true
}
```


9.4.4 Responses

This API call has the following HTTP status codes:

Code	Description
200	OK.
400	Bad request, please check the arguments you passed.
401	Authorization information is missing or invalid. **Name**—Authorization. **Description**—The `access_token` obtained using the `/access_token/` endpoint. **Type**—string.
404	Unknown Collector.

9.5 Creating a new collector

POST `/api/v1/collectors/`

9.5.1 Permissions required

- **Settings** > **Collector** > **Manage**

9.5.2 URI parameters

Name	Type	Description
formData	(body)	

9.5.3 Example

```
{
   "deploymentType": "OVA",
   "name": "My Collector"
}
```

9.5.4 Responses

This API call has the following HTTP status codes:

Code	Description
200	OK.
400	Bad request, please check the arguments you passed.
401	Authorization information is missing or invalid. **Name**—Authorization. **Description**—The `access_token` obtained using the `/access_token/` endpoint. **Type**—string.

9.6 Updating the collector's name

PATCH `/api/v1/collectors/{collector_id}/`

9.6.1 Permissions required

- **Settings** > **Collector** > **Manage**

9.6.2 URI parameters

Name	Type	Description
collector_id * Required	(path)	Armis collector ID.
formData	(body)	

9.6.3 Example

```
{
   "deploymentType": "OVA",
   "name": "My Collector"
}
```

9.6.4 Responses

This API call has the following HTTP status codes:

Code	Description
200	OK.
400	Bad request, please check the arguments you passed.
401	Authorization information is missing or invalid. **Name**—Authorization. **Description**—The `access_token` obtained using the `/access_token/` endpoint. **Type**—string.
404	Unknown Collector.

10 Dashboards

The Dashboards API endpoints enable you to retrieve and create dashboards.

For more information about Armis dashboards, see Dashboards in the Armis user guide.

10.1 Getting existing dashboards

GET `/api/v1/dashboards/`

Retrieves existing dashboards and the type-value of each: `Main` or `VMS` (which relates to AVM).

10.1.1 URI parameters

Name	Type	Description
type	string (query)	The type of the dashboard.

10.1.2 Response

This API call has the following HTTP status code:

Code	Description
200	OK.

10.2 Getting an existing dashboard by ID

GET `/api/v1/dashboards/{dashboard_id}/`

Returns existing dashboard by the Armis dashboard ID.

10.2.1 URI parameters

Name	Type	Description
dashboard * Required	(path)	Armis dashboard ID.

10.2.2 Response

This API call has the following HTTP status codes:

Code	Description
200	OK.
400	Bad request, please check the arguments you passed.
401	Authorization information is missing or invalid. **Name**—Authorization. **Description**—The `access_token` obtained using the `/access_token/` endpoint. **Type**—string.
404	Dashboard not found.

10.3 Creating a new dashboard

POST `/api/v1/dashboards/`

10.3.1 URI parameters

Name	Type	Description
body *required	object (body)	

10.3.2 Example

```
{
  "dashboard": {
    "ownerId": 0,
    "title": "My Dashboard"
  },
  "dashlets": [
    {
      "dashlet": {
        "visualizationConfig": {
        "aggregateBy": "COUNT_DISTINCT_DEVICES",
        "groupBy": "DEVICE_TYPE",
        "type": "COLUMN"
      }
    },
    "searchString": "in:devices",
    "title": "My Dashlet"
    }
  ]
}
```

10.3.3 Response

This API call has the following HTTP status codes:

Code	Description
200	OK.
400	Bad request, please check the arguments you passed.

11 Devices

For more information about devices, see the Armis user guide.

11.1 Setting a tag on an Armis device

POST /api/v1/devices/{device_id}/tags/

11.1.1 Permissions required

- **Device** > **Manage** > **Tags**.

11.1.2 URI parameters

Name	Type	Description
device_id * Required	(path)	Armis device ID.
tags	object (body)	JSON with format {"tags": ["tag1", "tag2", ...]

11.1.3 Example

The following are examples of setting a tag on a device in Armis Centrix™:

cURL

```
curl -X “POST” "https://<armis-
instance>.armis.com/api/v1/devices/<deviceId>/tags/" -H 'Authorization:
 <access-token>' -d $'{
    "tags": [
      "foo",
      "bar"
    ]
}'
```

Python

```
response = requests.post(url=”https://<armis-
instance>.armis.com/api/v1/devices/<deviceId>/tags/",
      headers={"Authorization": <access-token>},
      data=json.dumps({
         "tags": [
             "foo",
             "bar"
          ]
    })
```

If successful, the response will be a JSON like this:

```
{
   "success": true
}
```

11.1.4 Responses

This API call has the following HTTP status codes:

Code	Description
200	OK.
400	Bad request, please check the arguments you passed.
401	Authorization information is missing or invalid.
404	Unknown device.

11.2 Removing a tag from an Armis device

DELETE /api/v1/devices/{device_id}/tags/

11.2.1 URI parameters

Name	Type	Description
device_id * Required	(path)	Armis device ID.
tags	object (body)	JSON with format {"tags": ["tag1", "tag2", ...]

11.2.2 Permissions Required

- **Device** > **Manage** > **Tags**

11.2.3 Example

The following are examples for removing a tag from a device in Armis Centrix™:

cURL

```
curl -X “DELETE” "https://<armis-
instance>.armis.com/api/v1/devices/<deviceId>/tags/"
-H 'Authorization: <access-token>' -d $'{
       "tags": [
               "foo"
       ]
}'
```

Python

```
response = requests.delete(url="https://<armis-
instance>.armis.com/api/v1/devices/<deviceId>/tags/",
                headers={"Authorization": <access-token>},
                data=json.dumps({
                        "tags": [
                                "foo"
                        ]
                })
```

If successful, the response will be a JSON like this:

```
{
    "success": true
}
```

11.2.4 Responses

This API call has the following HTTP status codes:

Code	Description
200	OK.
400	Bad request, please check the arguments you passed.
401	Authorization information is missing or invalid.
404	Unknown device.

11.3 Updating a custom property on an Armis device

POST `/api/v1/devices/custom-properties/_bulk/`

11.3.1 Permissions required

- **Device** > **Manage** > **Edit**

11.3.2 URI parameters

Name	Type	Description
body	arrray[object]	Upsert multiple custom properties for multiple devices in a single operation. This endpoint is highly recommended to be used when a large amount of custom properties should be updated.

11.3.3 Examples

The following are examples for updating custom properties on a device in the Armis Centrix™:

cURL

```
curl -X “POST” "https://<armis-
instance>.armis.com/api/v1/devices/custom-properties/_bulk/" -H
'Authorization: <access-token>' -d $'[
  {
     "upsert": {
       "type": “<Custom-Property-Name>”,
       "value": “<Custom-Property-Value>”,
       “deviceId”: <deviceId>
     }
  }
]'
```

Python

```
response = requests.post(url=”https://<armis-
instance>.armis.com/api/v1/devices/custom-properties/_bulk/",
         headers={"Authorization": <access-token>},
         data=json.dumps([
         {
             "upsert": {
                 "type": “<Custom-Property-Name>”,
                 "value": “<Custom-Property-Value>”,
                 “deviceId”: <deviceId>
             }
         }
        ])
```

If successful, the response will be a JSON like this:

```
[ {"result":{},"status":202}]
```

> **NOTE:** This is a bulk API, which allows for updating multiple devices with one API call. The updating or removing of custom properties is done by sending an array of data elements. Two operations are available: upsert and delete.

For example, to update the custom properties of two devices and remove one from a third, the data elements could look like:

```
[
  {
    "delete": {
      "deviceId": 1,
      "key": "location"
    },
    "upsert": {
      "deviceId": 1,
      "key": "location",
      "value": 123445
    }
  }
]
```

> **NOTE:** `Delete` removes the custom property from the specified device.

11.3.4 Responses

This API call has the following HTTP status code:

Code	Description
207	Each item in the request has been processed on its own. Response indicates status of each individual item.
400	Bad request, please check the arguments you passed.
401	Authorization information is missing or invalid. **Name**—Authorization. **Description**—The `access_token` obtained using the `/access_token/` endpoint. **Type**—string.

11.4 Adding applications to a device

`POST` `/api/v1/devices/{device_id}/applications/`

If the application exists it updates its last seen time.

11.4.1 Permissions required

- **Device** > **Manage** > **Edit**

11.4.2 URI parameters

Name	Type	Description
device_id * Required	(path)	Armis device ID.
applications	(body)	An array of applications.

11.4.3 Example

```
{
   "applications": [
      {
        "name": "Chrome",
        "version": "70.0.3538.77"
      },
      {
        "name": "YouTube"
      }
   ]
}
```

11.5 Updating one or more of the device's attributes

PATCH /api/v1/devices/{device_id}/

11.5.1 Permissions required

- **Device** > **Manage** > **Edit**

11.5.2 URI parameters

Name	Description
device_id * Required	Armis device ID. Type: (path)
device * Required	Armis device. Type: object (body)

11.5.3 Example

```
{
   "CATEGORY": "HANDHELD",
   "MODEL": "iPhone 6S",
   "NAME": "Mike's iPhone",
   "OS": "iOS",
   "OS_VERSION": "10.3.1",
   "SITE": "Boston",
   "TYPE": "MOBILE_PHONE"
}
```

11.5.4 Responses

This API call has the following HTTP status codes:

Code	Description
200	OK.
400	Bad request, please check the arguments you passed.
401	Authorization information is missing or invalid. **Name**—Authorization. **Description**—The `access_token` obtained using the `/access_token/` endpoint. **Type**—string.
404	Unknown device.

11.6 Uploading a CSV file with device data

POST `/api/v1/devices/csv/`

11.6.1 Permissions required

- **Device** > **Manage** > **Create**

11.6.2 URI parameters

Name	Type	Description
csv * Required	file	CSV File encoded in UTF-8 with the following columns: `device_id`, `mac`, `key`, `value`.

11.6.3 Responses

This API call has the following HTTP status codes:

Code	Description
200	OK.
401	Authorization information is missing or invalid. **Name**—Authorization. **Description**—The `access_token` obtained using the `/access_token/` endpoint. **Type**—string.

11.7 Returning supported keys

GET `/api/v1/devices/csv/`

11.7.1 Permissions required

- **Device** > **Read**

11.7.2 URI parameters

None.

11.7.3 Responses

This API call has the following HTTP status codes:

Code	Description
200	OK.
401	Authorization information is missing or invalid. **Name**—Authorization. **Description**—The `access_token` obtained using the `/access_token/` endpoint. **Type**—string.

11.8 Returning devices information for a given identifier

Indentifiers include IP address, MAC, Device ID, and Search.

GET `/api/v1/devices/`

11.8.1 Permissions required

- **Device** > **Read**

11.8.2 URI parameters

Name	Type	Description
id	integer (query)	The Armis device ID.
ip	string (query)	The IPv4 or IPv6 Address of the devices.
mac	string (query)	The MAC Address of the devices.
search	string (query)	The search string.
tag	string (query)	The tag of the devices.
fields	(query)	Fields to show. If omitted, returns a default subset of fields.
from	integer (query)	Paging from.
length	integer (query)	Paging length.

11.8.3 Responses

This API call has the following HTTP status codes:

Code	Description
200	OK.
400	Bad request. Missing identifier param, must provide one of `id`, `ip`, `mac`, `search`, or `tag`.
401	Authorization information is missing or invalid. **Name**—Authorization. **Description**—The `access_token` obtained using the `/access_token/` endpoint. **Type**—string.

12 Device applications

12.1 Bulk operation on device applications

POST `/api/v1/device-applications/_bulk/`

12.1.1 Permissions required

- **Device** > **Manage** > **Edit**

12.1.2 URI parameters

Name	Type	Description
body * Required	array[object] (body)	

12.1.3 Example

```
[
   {
      "upsert": {
        "deviceId": 1,
        "lastSeen": "2023-10-01T05:52:28",
        "name": "Chrome",
        "version": "80.0.3987.122"
      }
   }
]
```

12.1.4 Responses

This API call has the following HTTP status codes:

Code	Description
207	Each item in the request has been processed on its own. Response indicates status of each individual item.
400	Bad request, please check the arguments you passed.
401	Authorization information is missing or invalid. **Name**—Authorization. **Description**—The `access_token` obtained using the `/access_token/` endpoint. **Type**—string.

13 Device boundaries

13.1 Bulk operation on device boundaries

POST /api/v1/device-boundaries/_bulk/

13.1.1 Permissions required

- **Device** > **Manage** > **Edit**

13.1.2 URI parameters

Name	Type	Description
body * Required	array[object] (body)	

13.1.3 Example

```
[
   {
      "create": {
        "boundaryName": "Corporate",
        "deviceId": 1
      }
   },
   {
      "delete": {
        "boundaryName": "Guest",
        "deviceId": 2
      }
   }
]
```

13.1.4 Responses

This API call has the following HTTP status codes:

Code	Description
207	Each item in the request has been processed on its own. Response indicates status of each individual item.
400	Bad request, please check the arguments you passed.
401	Authorization information is missing or invalid. **Name**—Authorization. **Description**—The `access_token` obtained using the `/access_token/` endpoint. **Type**—string.

14 Device properties

14.1 Bulk operation on device properties

POST /api/v1/device-properties/_bulk/

14.1.1 Permissions required

- **Device** > **Manage** > **Edit**

14.1.2 URI parameters

Name	Type	Description
body	array[object] (body)	Upsert multiple properties for multiple devices in a single operation. This endpoint is highly recommended to be used when a large amount of properties should be updated.

14.1.3 Example

```
[
   {
      "upsert": {
        "description": "The port that is blocked on the device",
        "deviceId": 1,
        "lastSeen": "2023-10-01T05:52:28",
        "type": "SERIAL_NUMBER",
        "value": 123445
      }
   }
]
```

14.1.4 Responses

This API call has the following HTTP status codes:

Code	Description
207	Each item in the request has been processed on its own. Response indicates status of each individual item.
400	Bad request, please check the arguments you passed.
401	Authorization information is missing or invalid. **Name**—Authorization. **Description**—The `access_token` obtained using the `/access_token/` endpoint. **Type**—string.

15 Devices tags

15.1 Setting the status for a given set of tags and devices

POST `/api/v1/devices_tags/`

15.1.1 URI parameters

Name	Type	Description
device-tag state	object (body)	The device tag state to set.

15.1.2 Example

```
{
    "ips": [
       "1.1.1.1",
       "2.2.2.2"
    ],
    "macs": [
       "aa:aa:aa:aa:aa:aa",
       "bb:bb:bb:bb:bb:bb"
    ],
    "remove": false,
    "tags": [
       "foo",
       "bar"
    ]
}
```

15.1.3 Responses

This API call has the following HTTP status codes:

Code	Description
200	OK.
401	Authorization information is missing or invalid. **Name**—Authorization. **Description**—The `access_token` obtained using the `/access_token/` endpoint. **Type**—string.

16 Integrations

16.1 Returning existing integrations

GET `/api/v1/integrations/`

To get the current list of integrations configured in an Armis instance.

16.1.1 Permissions required

- **Settings** > **Integration** > **Read**

16.1.2 URI parameters

Name	Type	Description
from	integer (query)	Paging from.
length	integer (query)	Paging length.

16.1.3 Examples

The following REST queries are examples using CURL and Python:

cURL

```
curl "https://<armis-instance>.armis.com/api/v1/integrations/"
      -H 'Authorization: <access-token>'
```

Python

```
response = requests.get(
   url="https://<armis-instance>.armis.com/api/v1/integrations/",
   headers={"Authorization": <access-token>})
```

```
{
  "data": {
    "changeTime": 1687029687884,
    "creationTime": 1675263150366,
    "enforcementLists": [],
    "id": 1,
    "integrationState": "ACTIVE",
    "lastRunEnd": null,
    "name": "Workspace",
    "params": {
      "integration_schedule": {
        "allowed_time": {
          "days": [],
          "hours": []
        },
        "interval": {
          "amount": 8,
          "unit": "Hours"
        },
        "timezone": null
      },
      "mark_discovered_devices_as_managed": true,
      "workspace_one_auth_method": "oauth_auth_method",
      "workspace_one_aw_tenant_code": "********",
      "workspace_one_client_id": "868980e2dd70480b9b4689a21c79a607",
      "workspace_one_client_secret": "********",
      "workspace_one_host": "as1300.awmdm.com",
      "workspace_one_import_applications": true,
      "workspace_one_region": "emea"
    },
    "statistics": null,
    "type": "Workspace ONE"
  },
  "success": true
}
Response headers
```


16.1.4 Response parameters

Name	Type	Description
count	integer	The number of currently configured integrations.
changeTime	timestamp	A timestamp that indicates when the integration was last modified.
creationTime	timestamp	A timestamp that indicates when the integration was created.
icon	string	A string that describes the logo associated with the specific integration.
id	integer	The ID assigned to the integration.
name	string	The integration’s name.

Name	Type	Description
params	JSON	The relevant integration parameters. This parameter can be further nested
statistics	JSON	The various statistics related to the integration. This parameter can be further nested.
type	string	The integration type.

> **NOTE:** Passwords are not exposed in the integration details fetched by the API. They are replaced with asterisks.

16.1.5 Responses

This API call has the following HTTP status codes:

Code	Description
200	OK.

16.2 Getting the integration by ID

`GET /api/v1/integrations/{integration_id}/`

16.2.1 Permissions required

- **Settings** > **Integration** > **Read**

16.2.2 URI parameters

Name	Type	Description
integration_id * Required	(path)	Armis integration ID.

16.2.3 Example


```
{
  "data": {
    "changeTime": 1687029687884,
    "creationTime": 1675263150366,
    "enforcementLists": [],
    "id": 1,
    "integrationState": "ACTIVE",
    "lastRunEnd": null,
    "name": "Workspace",
    "params": {
      "integration_schedule": {
        "allowed_time": {
          "days": [],
          "hours": []
        },
        "interval": {
          "amount": 8,
          "unit": "Hours"
        },
        "timezone": null
      },
      "mark_discovered_devices_as_managed": true,
      "workspace_one_auth_method": "oauth_auth_method",
      "workspace_one_aw_tenant_code": "********",
      "workspace_one_client_id": "868980e2dd70480b9b4689a21c79a607",
      "workspace_one_client_secret": "********",
      "workspace_one_host": "as1300.awmdm.com",
      "workspace_one_import_applications": true,
      "workspace_one_region": "emea"
    },
    "statistics": null,
    "type": "Workspace ONE"
  },
  "success": true
}
```

16.2.4 Response parameters

Name	Type	Description
changeTime	timestamp	A timestamp that indicates when the integration was last modified.
creationTime	timestamp	A timestamp that indicates when the integration was created.
enforcementLists	string	Enforcements.
icon	string	A string that describes the logo associated with the specific integration.
id	integer	The ID assigned to the integration.
name	string	The integration's name.
params	JSON	The relevant integration parameters. This parameter can be further nested.
statistics	JSON	The various statistics related to the integration. This parameter can be further nested.
type	string	The integration type.

16.2.5 Responses

This API call has the following HTTP status codes:

Code	Description
200	OK.
401	Authorization information is missing or invalid. **Name**—Authorization. **Description**—The `access_token` obtained using the `/access_token/` endpoint. **Type**—string.
404	Unknown Integration.

16.3 Creating a new integration

POST `/api/v1/integrations/`

16.3.1 Permissions required

- **Settings** > **Integration** > **Manage**

16.3.2 URI parameters

Name	Type	Description
formData	(body)	

16.3.3 Example

```
{
   "name": "My Integration",|
   "params": {
      "sensor_id": "1",
      "sniff_interface": "eth1"
   },
   "type": "SWITCH"
}
```

16.3.4 Responses

This API call has the following HTTP status codes:

Code	Description
200	OK.
400	Custom invalid integration error.

16.4 Deleting an integration

DELETE /api/v1/integrations/{integration_id}/

16.4.1 Permissions required

- **Settings** > **Integration** > **Manage**

16.4.2 URI parameters

Name	Type	Description
integration_id * Required	(path)	Armis integration ID.

16.4.3 Responses

This API call has the following HTTP status codes:

Code	Description
200	OK.
400	Integration deletion error.
401	Unauthorized Integration ID.
404	Unknown Integration ID.

16.5 Updating the parameters of an integration by ID

PATCH `/api/v1/integrations/{integration_id}/`

16.5.1 Permissions required

- **Settings** > **Integration** > **Manage**

16.5.2 URI parameters

Name	Type	Description
integration_id * Required	(path)	Armis integration ID.
Body	(body)	

16.5.3 Example

```
{
   "params": {
      "ip_list": "1.2.3.4, 4.3.2.1"
   }
}
```

16.5.4 Responses

This API call has the following HTTP status codes:

Code	Description
200	OK.
400	Custom invalid integration parameter error.
401	User not authorized.
404	Integration not found.

17 Policies

For more information about policies, see the Armis user guide.

17.1 Getting all policies

GET /api/v1/policies/

17.1.1 Permissions required

- **Policy** > **Read**

17.1.2 URI parameters

Name	Type	Description
from	integer (query)	Paging from.
length	integer (query)	Paging length.

17.1.3 Example

The following are examples of retrieving all of the policies from Armis Centrix™:

cURL

```
curl "https://<armis-instance>.armis.com/api/v1/policies/" -H
'Authorization: <access-token>'
```

Python

```
response = requests.get(url="https://<armis-
instance>.armis.com/api/v1/policies/",headers={"Authorization": <access-
token>})
```

The response will be a JSON array of policies similar to this:


```
{
   "data": {
     "count": 10,
     "next": 10,
     "policies": [
       {
          "action": {
            "params": {
              "consolidation": {
                "amount": 1,
                "unit": "Minutes"
              },
              "description": "SIEM Test Policy based on DNS queries",
              "severity": "high",
              "type": "Security"
             },
             "type": "alert"
           },
           "id": "69",
           "isEnabled": false,
           "name": "SIEM Test",
           "rules": {
             "and": [
               "protocol:DNS"
             ]
       }
     },
     ….
     {...}
   ],
   "prev": null,
   "total": 48
 },
 "success": true
}
```


17.1.4 Response parameters

Name	Type	Description
action	JSON	The type of action and relevant action parameters: • type–(string). A policy action type (Tag, Untag, Alert, Enforce Devices etc.) • params–JSON. The parameters of the action type (may be nested).
id	integer	Armis policy ID.
isEnabled	boolean	The policy state (enabled/disabled).
name	string	The policy name.
rules	JSON	A recursive JSON with the format: {"and" / "or": [AQL string / rules JSON]} .

17.1.5 Responses

This API call has the following HTTP status codes:

Code	Description
200	OK

17.2 Getting policy by ID

GET `/api/v1/policies/{policy_id}/`

17.2.1 Permissions required

- **Policy** > **Read**

17.2.2 URI parameters

Name	Type	Description
policy_id * Required	(path)	The ID of the policy to query.

17.2.3 Response parameters

Name	Type	Description
action	JSON	The type of action and relevant action parameters: • type–(string). A policy action type (Tag, Untag, Alert, Enforce Devices etc.) • params–JSON. The parameters of the action type (may be nested).
id	integer	Armis policy ID.
isEnabled	boolean	Default—"false". The policy state (enabled/disabled).
name	string	The policy name.
rules	JSON	A recursive JSON with the format: {"and" / "or": [AQL string / rules JSON]} .

17.2.4 Responses

This API call has the following HTTP status codes:

Code	Description
200	OK
400	Custom invalid policy parameter error.
404	Unknown policy.

17.3 Creating a new policy

POST /api/v1/policies/

17.3.1 Permissions required

- **Policy** > **Manage**

17.3.2 URI parameters

Name	Type	Description
body	(body)	

17.3.3 Example

```
{
  "actions": [
    {
      "params": {
        "consolidation": {
          "amount": 1,
          "unit": "Days"
        },
        "severity": "high",
        "type": "Security or Network Performance"
      },
      "type": "alert"
    }
  ],
  "description": "Description (maximal length - 500)",
  "isEnabled": false,
  "labels": [
    "Security"
  ],
  "name": "My Policy",
  "ruleType": "Activity, IP Connection, Device or Vulnerability",
  "rules": {
    "and": [
      "protocol:BMS",
      {
        "or": [
          "content:(iPhone)",
          "content:(Android)"
        ]
      }
    ]
  }
}
```

17.3.4 Response parameters

Name	Type	Description
action	JSON	The type of action and relevant action parameters: • type–(string). A policy action type (Tag, Untag, Alert, Enforce Devices etc.) • params–JSON. The parameters of the action type (may be nested).
isEnabled	boolean	Optional. Default—"false". The policy state (enabled/disabled).
name	string	Mandatory. The policy name.
rules	JSON	Mandatory. A recursive JSON with the format: {"and" / "or": [AQL string / rules JSON]} .

17.3.5 Responses

This API call has the following HTTP status codes:

Code	Description
200	OK.
400	An invalid policy was provided.
409	Policy title already exists.

17.4 Deleting a policy by ID

DELETE /api/v1/policies/{policy_id}/

To delete a policy on Armis Centrix™, you only need to send the specific <Policy ID> of the policy.

17.4.1 Permissions required

- **Policy** > **Manage**

17.4.2 URI parameters

Name	Type	Description
policy_id * Required	(path)	The ID of the policy to query.

17.4.3 Example

The following are examples of deleting a policy on Armis Centrix™:

cURL

```
Curl -X "DELETE" "https://<armis-instance>.armis.com/api/v1/policies/<Policy
ID>/" -H 'Authorization:
<access-token>'
```

Python

```
response = requests.delete(url="https://<armis-
instance>.armis.com/api/v1/policies/<Policy ID>/",headers={"Authorization":
<access-token>})
```

If the call is successful, it will return the following:

```
{
   "success": true
}
```

If the alert was already in the RESOLVED state, it will return the following:

```
{
   "message": "Failed in deleting policy",
   "success": false
}
```

17.4.4 Responses

This API call has the following HTTP status codes:

Code	Description
200	OK.
400	Custom invalid policy parameter error.
404	Unknown policy.

17.4.5 Example—Creating an Activity policy

The following are examples of creating an Activity policy on Armis Centrix™:

cURL

```
curl -X "POST" "https://<armis-instance>.armis.com/api/v1/policies/" \
    -H 'Authorization: <access-token> \
    -H 'Content-Type: application/json' \
    -d $'{
          "labels": ["Security"],
          "actions": [
            {
              "type": "alert",
              "params": {
                "consolidation": {
                  "amount": 1,
                  "unit": "Days"
                },
                "type": "Security",
                "severity": "high"
             }
            }
          ],
          "isEnabled": true,
          "description": "My
          Description", "ruleType":
          "ACTIVITY",
          "name": "Test ACTIVITY Policy",
          "rules": {
            "and": [
              "protocol:BMS"
            ]
          }
      }'
```

Python

```
response = requests.post(
 url="https://<armis-instance>.armis.com/api/v1/devices/_bulk/",
 headers={"Authorization": <access-token>,
          "Content-Type": "application/json",},
            data=json.dumps({
                "labels": [
                    "Security"
                ],
                "actions": [
                    {
                        "type": "alert",
                        "params": {
                            "consolidation": {
                                "amount": 1,
                                "unit": "Days"
                            },
                            "type": "Security",
                            "severity": "high"
                        }
                    }
                ],
                "isEnabled": True,
                "description": "My Description",
                "ruleType": "ACTIVITY",
                "name": "Test ACTIVITY Policy",
                "rules": {
                    "and": [
                        "protocol:BMS"
                    ]
                 }
            })
     )
```

If successful, the response will be a JSON like this:

```
{
   "data": {
   "id": 274
   },
   "success": true
}
```

Where `274` is the ID of the new policy.

17.4.6 Example—Creating a Device policy

The following are examples of creating a Device policy on Armis Centrix™:

cURL

```
curl -X "POST" "https://<armis-instance>.armis.com/api/v1/policies/" \
    -H 'Authorization: <access-token> \
     -H 'Content-Type: application/json' \
     -d $'{
               "labels": [
                 "Security"
               ],
               "name": "Test DEVICE Policy",
               "ruleType": "DEVICE",
               "description": "My Description",
               "rules": {
                 "and": [ "macAddress:(00:00:11:11:22:22)
                 "
                 ]
               },
               "actions": [
                 {
                   "type": "alert",
                   "params": {
                     "consolidation": {
                       "amount": 1,
                       "unit": "Days"
                     },
                     "type": "Security",
                     "severity": "high"
                   }
                 }
             ],
             "isEnabled": true
      }'
```

Python

```
response = requests.post(
 url="https://<armis-instance>.armis.com/api/v1/devices/_bulk/",
 headers={"Authorization": <access-token>,
          "Content-Type": "application/json",},
            data=json.dumps({
                "labels": [
                    "Security"
                ],
                "name": "Test DEVICE Policy",
                "ruleType": "DEVICE",
                "description": "My Description",
                "rules": {
                    "and": [
          "macAddress:(00:00:11:11:22:22)"
             ]
          },
          "actions": [
            {
          "type": "alert",
          "params": {
                   "Consolidation" {
                   "amount": 1,
                   "unit": "Days"
              },
              "Type": "Security",
              "severity": "high"
                }
             }
          ],
          "isEnabled": True
        })
     )
```

If successful, the response will be a JSON like this:

```
{
   "data": {
     "id": 275
   },
   "success": true
}
```

Where `275` is the ID of the new policy.

17.4.7 Example—Creating an IP Connection policy

The following are examples of creating an IP Connection policy on Armis Centrix™:

cURL

```
curl -X "POST" "https://<armis-instance>.armis.com/api/v1/policies/" \
     -H 'Authorization: <access-token> \
     -H 'Content-Type: application/json' \|
     -d $'{
            "labels": [
              "Security"
            ],
            "name": "Test IP_CONNECTION Policy",
            "ruleType": "IP_CONNECTION",
            "description": "My Description",
            "rules": {
              "and": [
              "endpointB:(networkLocation:External)"
            ]
          },
          "actions": [
            {
              "type": "alert",
              "params": {
                "consolidation": {
                "amount": 1,
                "unit": "Days"
                },
                "type": "Security", "severity": "high"
              }
            }
          ],
          "isEnabled": true
       }'
```

Python

```
response = requests.post(
 url="https://<armis-instance>.armis.com/api/v1/devices/_bulk/",
 headers={"Authorization": <access-token>,
          "Content-Type": "application/json",},
            data=json.dumps({
                "labels": [ "Security" ],
                "name": "Test IP_CONNECTION Policy",
                "ruleType": "IP_CONNECTION",
                "description": "My Description",
                "rules": {
                    "and":
                      [ "endpointB:(networkLocation:External)" ]
                },
                "actions": [
                    {
                        "type": "alert",
                        "params": {
                            "consolidation": {
                                "amount": 1, "unit": "Days"
                            },
                            "type": "Security",
                            "severity": "high"
                        }
                     }
                ],
                "isEnabled": True
            })
        )
```

If successful, the response will be a JSON like this:

```
{
   "data": {
     "id": 276
   },
   "success": true
}
```

Where `276` is the ID of the new policy.

17.5 Updating a policy

PATCH `/api/v1/policies/{policy_id}/`

17.5.1 Permissions required

- **Policy** > **Manage**

17.5.2 URI parameters

Name	Type	Description
policy_id * Required	(path)	The ID of the policy to query.
Body	(body)	

To update a policy on Armis Centrix™, you only need to send the specific elements that are to be updated for the policy, which is denoted by the <Policy ID.

17.5.3 Examples

The following are examples of changing the status of a policy to be disabled:

cURL

```
curl -X "POST" "https://<armis-instance>.armis.com/api/v1/policies/<Policy
ID>/" \
      -H 'Authorization: <access-token> \
      -H 'Content-Type: application/json' \
      -d $'{ "isEnabled": false}'
```

Python

```
response = requests.post(
 url=
"https://<armis-instance>.armis.com/api/v1/policies/<Policy ID>/",
 headers={"Authorization": <access-token>,
          "Content-Type": "application/json",},
data=json.dumps({"isEnabled": false))
```

If the call is successful, it will return the following:

```
{
   "data": {
     "id": "<Policy ID>",
     "name": "Test Policy Name",
     "isEnabled": false,
     "rules": {
       "and": [
          "protocol:Bluetooth",
       {
            "or": [
              "content:(iPhone)",
              "content:(Android)"
            ]}]
},
     "action": {
       "params": {
         "consolidation": {
           "amount": 1,
           "unit": "Days"
         },
         "description": "New Test Policy",
         "severity": "high",
         "type": "Security"
       },
       "type": "alert"
     }
   },
   "success": true
}
```

The following is another example of changing the name of a policy:

cURL

```
curl -X "POST" "https://<armis-instance>.armis.com/api/v1/policies/<Policy
ID>/" \
       -H 'Authorization: <access-token> \
       -H 'Content-Type: application/json' \
       -d $'{ "name": "New Policy Name" }'
```

Python

```
response = requests.post(
   url=
"https://<armis-instance>.armis.com/api/v1/policies/<Policy ID>/",
 headers={"Authorization": <access-token>,
          "Content-Type": "application/json",},
data=json.dumps({"name": "New Policy Name"))
```

```
{
   "data": {
     "id": "<Policy ID>",
     "name": "New Policy Name",
     "isEnabled": false,
     "rules": {
       "and": [
         "protocol:Bluetooth",
       ]
     },
     "action": {
     "params": {
       "consolidation": {
         "amount": 1,
         "unit": "Days"
       },
       "description": "New Test Policy",
       "severity": "high",
       "type": "Security"
     },
     "type": "alert"
     }
   },
   "success": true
}
```

17.5.4 Response parameters

Name	Type	Description
action	JSON	The type of action and relevant action parameters: • type—(string). A policy action type (Tag, Untag, Alert, Enforce Devices etc.) • params—JSON. The parameters of the action type (may be nested).
id	integer	Armis policy ID.
isEnabled	boolean	Default—"false". The policy state (enabled/disabled).
name	string	The policy name.
rules	JSON	A recursive JSON with the format: {"and" / "or": [AQL string / rules JSON]} .

17.5.5 Responses

This API call has the following HTTP status codes:

Code	Description
200	OK.
400	An invalid policy was provided.
404	Unknown Policy.
409	Policy title already exists.

18 Reports

The Report API endpoints enable you to create, run, update, or delete a report on a tenant.

For more information about reports, see Reports in the Armis user guide.

The GET calls retrieve a list of existing reports previously configured on a tenant—to retrieve all reports or retrieve a specific report by its ID.

Additionally, if a report has been set on a tenant as a scheduled report, the API can also be used to obtain a link to download the report via a direct download URL. Upon download, the data within the report will reflect the last run cycle.

To get the report result as a file, do the following:

1. Get the file URL from the endpoint using the following request:
   `GET /api/v1/report-results/{report_id}/`
2. Download the report file from the URL that is specified in the request.

> **NOTE:** You can also download a report via an email link by sending a request to run the report (see Sending a request to run a report by ID).

The report file name has the following format:

`report_<UUID>.<extension>`

18.1 Creating a new report

POST `/api/v1/reports/`

> **NOTE:** It may be easier to start by generating a report in the Armis console, before automating the creation of reports using the API.

18.1.1 Permissions required

- **Report** > **Manage** > **Create**

18.1.2 URI parameters

Name	Type	Description
body	(body)	

18.1.3 Example

```
{
   "asq": "in:devices",
   "reportName": "test",
   "schedule": {
         "email": ["user@armis.com"],
         "repeatAmount": 2,
         "repeatUnit": "Days",
         "reportFileFormat": "csv",
         "timeOfDay": "15:00",
         "timezone": "Asia/Jerusalem",
         "weekdays": ["Monday"]
   }
}
```

18.1.4 Response

This API call has the following HTTP status codes:

Code	Description
201	Created. Body: `{"id": 123}`
400	In case of a failure to create the report. The data may indicate the reason for the failure. Body: `{ "message": "additional information", "success": false }`
401	Authorization information is missing or invalid. **Name**—Authorization. **Description**—The `access_token` obtained using the `/access_token/` endpoint. **Type**—string.
409	Report name already exists.

18.2 Updating a report

PATCH `/api/v1/reports/{report_id}/`

18.2.1 Permissions required

- **Report** > **Manage** > **Edit**

18.2.2 URI parameters

Name	Type	Description
report_id * Required	integer (path)	Patch report by ID.
body	(body)	

18.2.3 Example

```
{
   "asq": "in:devices",
   "reportName": "New Report Name",
   "schedule": {
         "email": ["user@armis.com"],
         "repeatAmount": 2,
         "repeatUnit": "Days",
         "reportFileFormat": "csv",
         "timeOfDay": "15:00",
         "timezone": "Asia/Jerusalem",
         "weekdays": ["Monday"]
   }
}
```

NOTES:

- To clear a field, pass it with an empty value, and ASQ will replace all existing rules.
- All fields are optional.
- Fields that are not provided will be ignored.

18.2.4 Response

This API call has the following HTTP status codes:

Code	Description
200	OK. Body: `{ "data": {"reportId": 123}, "success": true }`
400	Invalid weekday provided in report schedule.
401	Authorization information is missing or invalid. **Name**—Authorization. **Description**—The `access_token` obtained using the `/access_token/` endpoint. **Type**—string.
404	Report not found. Body: `{ "message": "additional information", "success": false }`

18.3 Deleting a report by ID

DELETE `/api/v1/reports/{report_id}/`

18.3.1 Permissions required

- **Report** > **Manage** > **Delete**

18.3.2 URI parameters

Name	Type	Description
report_id * Required	(path)	The ID of the report to query.

18.3.3 Response

This API call has the following HTTP status codes:

Code	Description
200	OK.
404	Report not found. The resource does not exist.

18.4 Getting report details by ID

GET /api/v1/reports/{report_id}/

18.4.1 Permissions required

- **Report** > **Read**

18.4.2 URI parameters

Name	Type	Description
report_id * Required	(path)	The ID of the report to query.

18.4.3 Example

```
{
  "asq": "in:devices timeFrame:\"1 Day\"",
  "reportName": "My Report",
  "schedule": {
    "email": [
      "test@armis.com"
    ],
    "repeatAmount": "2",
    "repeatUnit": "Days",
    "reportFileFormat": "csv",
    "timeOfDay": "15:00",
    "timezone": "Asia/Jerusalem",
    "weekdays": [
      "Monday"
    ]
  }
}
```

18.4.4 Response

This API call has the following HTTP status codes:

Code	Description
200	OK.

404	The report ID could not be found.
	Body:
	<pre>{
	"message": "additional information",
	"success": false
	}</pre>

18.5 Getting all report details

GET `/api/v1/reports/`

18.5.1 Permissions required

- **Report** > **Read**

18.5.2 URI parameters

None.

18.5.3 Response

This API call has the following HTTP status codes:

Code	Description

200	OK.
	Body:
	<pre>{
	"total": 282,
	"items":[
	{
	"asq": "in:devices",
	"creationTime": "2022-01-01T17:30",
	"id": 111,
	"isScheduled": true,
	"reportName": "ABC",
	"schedule": {
	"email": ["user@armis.com"],
	"repeatAmount": 2,
	"repeatUnit": "Days",
	"reportFileFormat": "csv",
	"timeOfDay": "15:00",
	"timezone": "Asia/Jerusalem",
	"weekdays": "Monday"
	}
	},
	...
	]
	}</pre>

401	Authorization information is missing or invalid. **Name**—Authorization. **Description**—The `access_token` obtained using the `/access_token/` endpoint. **Type**—string.

18.6 Getting the latest report by ID

GET `/api/v1/report-results/{report_id}/`

18.6.1 URI parameters

Name	Type	Description
report_id * Required	(path)	The ID of the report to query.

18.6.2 Response

This API call has the following HTTP status codes:

Code	Description
200	OK. Body: `{ "data": { "creationTime": "2023-01-01T10:10:10", "url": "https://{report download link}" } }`
400	Custom invalid report parameters error. The data may indicate the reason for the failure.
404	The Report ID could not be found. Body: `{ "message": "additional information", "success": false }`

18.7 Sending a request to run a report by ID

POST `/api/v1/reports/{report_id}/_run/`

Sends a request to run a report that has a schedule. The new report will be sent via email when ready, to the recipients defined in the report-schedule.

This request will have a rate limit of three reports every five hours, per report ID. A rate limit is required to avoid a single report running repeatedly and creating resource problems.

> **NOTES:**
> - To get the report ID, see Getting all report details.
> - The report or export link will be sent to you by email. It takes time, please be patient.

18.7.1 Permissions required

- **Report** > **Manage** > **Edit**

18.7.2 URI parameters

Name	Type	Description
report_id * Required	(path)	The ID of the report to query.

18.7.3 Response

This API call has the following HTTP status codes:

Code	Description
202	OK.
401	Unauthorized.
404	The report ID or report schedule could not be found.
429	Too Many Requests. The rate limit has been exceeded. Body: `{ "message": "additional information", "success": false }`

19 Roles

19.1 Getting details of all roles

GET `/api/v1/roles/`

19.1.1 Permissions required

- **Settings** > **Users And Roles** > **Read**

19.1.2 URI parameters

None.

19.1.3 Responses

This API call has the following HTTP status codes:

Code	Description
200	OK.
401	Authorization information is missing or invalid. **Name**—Authorization. **Description**—The `access_token` obtained using the `/access_token/` endpoint. **Type**—string.

19.2 Creating a new role

POST `/api/v1/roles/`

19.2.1 Permissions required

- **Settings** > **Users And Roles** > **Manage** > **Roles** > **Create**

19.2.2 URI parameters

Name	Type	Description
Body * Required	(body)	The role privileges. The set includes PII permissions (in advancedPermissions) and permissions per system entity. Each parameter and its nested options are Boolean. If a parent option is True, all its nested options must be True. If a nested option is False, its parent option cannot be True.

19.2.3 Example

```
{
  "name": "Custom Role",
  "permissions": {
    "advancedPermissions": {
      "all": true,
      "behavioral": {
        "all": true,
        "applicationName": {
          "all": true
        },
        "hostName": {
          "all": true
        },
        "serviceName": {
          "all": true
        }
      },
      "device": {
        "all": true,
        "deviceNames": {
          "all": true
        },
        "ipAddresses": {
          "all": true
        },
        "macAddresses": {
          "all": true
        },
        "phoneNumbers": {
          "all": true
        }
      }
    },
    "alert": {
      "all": true,
      "manage": {
        "all": true,
        "resolve": {
```

```
        "all": true
      },
      "suppress": {
        "all": true
      },
      "whitelistDevices": {
        "all": true
      }
    },
    "read": {
      "all": true
    }
  },
  "all": true,
  "business_applications": {
    "all": true,
    "manage": {
      "all": true,
      "delete": {
        "all": true
      },
      "upsert": {
        "all": true
      }
    },
    "read": {
      "all": true
    }
  },
  "device": {
    "all": true,
    "manage": {
      "all": true,
      "create": {
        "all": true
      },
      "edit": {
        "all": true
      },
      "enforce": {
        "all": true,
```

```
    },
    "read": {
      "all": true
    }
  },
  "risk_factor": {
    "all": true,
    "manage": {
      "all": true,
      "ignore": {
        "all": true
      },
      "resolve": {
        "all": true
      }
    },
    "read": {
      "all": true
    }
  },
  "settings": {
    "all": true,
    "auditLog": {
      "all": true
    },
    "boundary": {
      "all": true,
      "manage": {
        "all": true,
        "create": {
          "all": true
        },
        "delete": {
          "all": true
        },
        "edit": {
          "all": true
        }
      },
      "read": {
        "all": true
      }
    },
    "businessImpact": {
      "all": true,
      "manage": {
        "all": true
```

```
},
    "user": {
      "all": true,
      "read": {
        "all": true
      }
    },
    "vulnerability": {
      "all": true,
      "manage": {
        "all": true,
        "ignore": {
          "all": true
        },
        "resolve": {
          "all": true
        },
        "write": {
          "all": true
        }
      },
      "read": {
        "all": true
      }
    }
  }
}
```

19.2.4 Responses

This API call has the following HTTP status codes:

Code	Description
200	OK.
400	Bad request, please check the arguments you passed.
401	Authorization information is missing or invalid. **Name**—Authorization. **Description**—The `access_token` obtained using the `/access_token/` endpoint. **Type**—string.
404	Unknown role.

19.3 Deleting a role

DELETE `/api/v1/roles/{role_id}/`

19.3.1 Permissions required

- **Settings** > **Users And Roles** > **Manage** > **Roles** > **Delete**

19.3.2 URI parameters

Name	Type	Description
role_id * Required	(path)	The role ID in the Armis system.

19.3.3 Responses

This API call has the following HTTP status codes:

Code	Description
200	OK.
400	Bad request, please check the arguments you passed.
401	Authorization information is missing or invalid. **Name**—Authorization. **Description**—The `access_token` obtained using the `/access_token/` endpoint. **Type**—string.
404	Unknown role.

19.4 Get role details

GET `/api/v1/roles/{role_id}/`

19.4.1 Permissions required

- **Settings** > **Users And Roles** > **Read**

19.4.2 URI parameters

Name	Type	Description
role_id * Required	(path)	The role ID in the Armis system.

19.4.3 Responses

This API call has the following HTTP status codes:

Code	Description
200	OK.
404	Unknown role.

19.5 Update role privileges

PATCH `/api/v1/roles/{role_id}/`

Permissions required

- **Settings** > **Users And Roles** > **Manage** > **Roles** > **Edit**

19.5.1 URI parameters

Name	Type	Description
role_id * Required	(path)	The role ID in the Armis system.
body * Required	(body)	The role privileges. The set includes PII permissions (in advancedPermissions) and permissions per system entity. Each parameter and its nested options are Boolean. If a parent option is True, all its nested options must be True. If a nested option is False, its parent option cannot be True.

19.5.2 Example

```
{
  "name": "Custom Role",
  "permissions": {
    "advancedPermissions": {
      "all": true,
      "behavioral": {
        "all": true,
        "applicationName": {
          "all": true
        },
        "hostName": {
          "all": true
        },
        "serviceName": {
          "all": true
        }
      },
      "device": {
        "all": true,
        "deviceNames": {
          "all": true
        },
        "ipAddresses": {
          "all": true
        },
        "macAddresses": {
          "all": true
        },
        "phoneNumbers": {
          "all": true
        }
      }
    },
    "alert": {
      "all": true,
      "manage": {
        "all": true,
        "resolve": {
```

```
        "all": true
      },
      "suppress": {
        "all": true
      },
      "whitelistDevices": {
        "all": true
      }
    },
    "read": {
      "all": true
    }
  },
  "all": true,
  "business_applications": {
    "all": true,
    "manage": {
      "all": true,
      "delete": {
        "all": true
      },
      "upsert": {
        "all": true
      }
    },
    "read": {
      "all": true
    }
  },
  "device": {
    "all": true,
    "manage": {
      "all": true,
      "create": {
        "all": true
      },
      "edit": {
        "all": true
      },
      "enforce": {
        "all": true,
```

```
    },
    "read": {
      "all": true
    }
  },
  "risk_factor": {
    "all": true,
    "manage": {
      "all": true,
      "ignore": {
        "all": true
      },
      "resolve": {
        "all": true
      }
    },
    "read": {
      "all": true
    }
  },
  "settings": {
    "all": true,
    "auditLog": {
      "all": true
    },
    "boundary": {
      "all": true,
      "manage": {
        "all": true,
        "create": {
          "all": true
        },
        "delete": {
          "all": true
        },
        "edit": {
          "all": true
        }
      },
      "read": {
        "all": true
      }
    },
    "businessImpact": {
      "all": true,
      "manage": {
        "all": true
```

```
},
    "user": {
      "all": true,
      "read": {
        "all": true
      }
    },
    "vulnerability": {
      "all": true,
      "manage": {
        "all": true,
        "ignore": {
          "all": true
        },
        "resolve": {
          "all": true
        },
        "write": {
          "all": true
        }
      },
      "read": {
        "all": true
      }
    }
  }
}
```

19.5.3 Responses

This API call has the following HTTP status codes:

Code	Description
200	OK
400	Bad request, please check the arguments you passed.
401	Authorization information is missing or invalid. **Name**—Authorization. **Description**—The `access_token` obtained using the `/access_token/` endpoint. **Type**—string.
404	Unknown role.

20 Search

20.1 Return search result for given ASQ search string

GET `/api/v1/search/`

20.1.1 URI parameters

Name	Type	Description
aql *Required	string (query)	The AQL search string
fields	(query)	Fields to show. If omitted, returns a default subset of fields. See Searches types.
from	integer (query)	Paging from
length	integer (query)	Paging length
includeTotal	boolean (query)	If set to "false", the total count will not be calculated.
orderBy	string (query)	Sort order for results, values separated by commas. Default direction is ASC.
tz	string (query)	The time zone to run the query.

NOTES:

- Returned fields—All fields will be returned, except for nested entities which will be returned as a list of IDs.
- Optional filters—All filters available for the entity in the ASQ.

20.1.2 Responses

This API call has the following HTTP status codes:

Code	Description
200	OK.
400	Bad request. Missing `aql` parameter.
401	Authorization information is missing or invalid. **Name**—Authorization. **Description**—The `access_token` obtained using the `/access_token/` endpoint. **Type**—string.

20.1.3 orderBy function

Sorts the results fetched by the Search API by a variety of keywords in ascending or descending order:

`orderBy={keyword}:{sorting_order}`

The following keywords are available:

Type of search	orderBy keywords
in:activity	• protocol • sensor • time (default) • type
in:alerts	• severity • status • time • title • type **NOTE:** Most commonly, the `in:alerts` search is used to fetch unhandled alerts starting from the most up-to-date one. Therefore, by default, the search results are ordered first by status, and then by time, which is equivalent to `orderBy=status,time:desc`.
in:devices	• category • id • firstSeen

Type of search	orderBy keywords
	• ipAddress • lastSeen (default) • macAddress • manufacturer • model • brand • name • osFull • riskLevel • sensor • site • type • user **NOTE:** Applying the `osFull` keyword will order the search results by the operating system name (**`operatingSystem`**) and the operating system version number (`operatingSystemVersion`).
in:vulnerabilities	• affectedDevicesCount • attackComplexity • availabilityImpact • confidentialityImpact • exploitabilityScore • impactScore • integrityImpact • privilegesRequired • publishedDate (default) • score • severity • cveUid

NOTES:

- You can provide more than one keyword delimited by commas.
- By default, the values are sorted in ascending order. To apply descending order, append `:desc` to the keyword.

20.1.3.1 Examples

- To retrieve the complete device inventory, apply the `orderBy` parameter with a fixed property like **id** or **macAddress**. For instance, to fetch the list of devices by ID, use the **Pagination** method to specify a viable page length and the `orderBy=id` argument. Repeat the request while changing the pagination value until reaching the end of the device list. It is recommended to automate this operation with a script.
- The following command will fetch the first five devices with the smallest ID and sort them in ascending order:

  ```
  https://{org_name}.armis.com/api/v1/search/?aql=in:devices&
  length=5&orderBy=id
  ```

- This command will fetch the first five devices with the largest ID and sort them in descending order:

  ```
  https://{org_
  name}.armis.com/api/v1/search/?aql=in:devices&length=5&orderBy=id:desc
  ```

- The following command will order the first five fetched devices by the manufacturer name in descending order (from Z to A) and by the device ID in ascending order:

  ```
  https://{org_
  name}.armis.com/api/v1/search/?aql=in:devices&length=5&orderBy=manufact
  urer:desc,id
  ```

20.1.4 Searches types

The following types of searches are supported:

in:activity

in:alerts

in:applications

in:businessApplications

in:connections

in:devices

Document version control

in:operatingSystems

Document version control

in:services

in:traffic

in:users

in:vulnerabilities

20.1.4.1 in:activity

GET `https://{org_name}.armis.com/api/v1/search/?aql=in:activity {optional filters}`

20.1.4.1.1 Response parameters

Name	Type	Description
activityUUID	string	Activity ID.
content	string	Additional activity information.
connectionIds	list[integer]	List of connection IDs which are related to the activity.
deviceIds	list[integer]	List of devices IDs which are related to the activity.
protocol	string	Protocol used - Network, Wi-Fi etc.
sensor	JSON	Name of sensor that picked up the activity. **name** | sensor name
site	JSON	The sites where the sensor that picked up the connection is located. • location—The site location. • name—The site name.
sites	JSON	The sites where the sensor that picked up the connection is located. This parameter is used for multiple sites and replaces the `site` parameter. • location—The site location. • name—The site name.
title	string	Activity title.
type	string	Type of activity i.e., First connect, New Device, SSID Beacon Started, etc.
time	timestamp	Activity timestamp.

20.1.4.1.2 Example

GET `https://{org_name}.armis.com/api/v1/search/?aql=in:activity type:"Dns Query"`

```
{
  "data": {
    "results": [
      {
        "activityUUID": "sBEbYGsBAAAAAABkzx4s",
        "title": "e0553d490 performed DNS query to domain 'abc-ssl.xyz.com'",
        "content": "Resolved IPs: 152.101.26.236",
        "type": "Dns Query",
        "protocol": "Wifi",
         "sensor": {
          "name": "0c:8d:db:b2:61:3e"
        },
        "time": "2019-03-06T13:08:53.016075+00:0",
        "deviceIds": [1475,1498],
        "connectionIds": [1599, 9804]
      }
    ]
  },
  "success": true
}
```

20.1.4.2 in:alerts

GET https://{org_name}.armis.com/api/v1/search/?aql=in:alerts {optional filters}

20.1.4.2.1 Examples

The following are examples for retrieving all of the alerts from Armis Centrix™:

cURL

```
curl "https://<armis-instance>.armis.com/api/v1/search/?aql=in:alerts" -
H 'Authorization: <access-token>'
```

Python

```
response = requests.get(url="https://<armis-
instance>.armis.com/api/v1/search/",
       params={"aql": "in:alerts"},
       headers={"Authorization": <access-token>})
```

The response will be a JSON array of alerts similar to this:


```
{
   "data": {
        "count": 10,
        "next": 10,
        "prev": null,
        "results": [
          {
            "activityUUIDs": [
              "AHlSvXkBAAAAAE-7NRHb"
           ],
          "alertId": 7,
          "connectionIds": [
           37919,
            37925,
            37926
          ],
          "description": null,
          "deviceIds": [
            151,
            13
          ],
          "severity": "High",
          "status": "Unhandled",
          "time": "2021-05-30T08:19:03.543857+00:00",
          "title": "Krack attack detected",
          "type": "Anomaly Detection"
        },
        …
      ],
      "total": 24
   },
   "success": true
}
```


An example for Alerts Status that are Unhandled:

```
GET https://{org_name}.armis.com/api/v1/search/?aql=in:alerts
status:Unhandled
```

```
{
  "data": {
    "results": [
      {
        "alertId": 600,
        "title": "Restricted Device Connected to the Internet",
        "type": "SYSTEM_POLICY_VIOLATION",
        "time": "2019-03-06T13:08:53.016075+00:0",
        "severity": "Medium",
        "status": "Unhandled",
        "description": "System policy violation alert",
        "deviceIds": [1475,1498],
        "connectionIds": [1599,9804],
        "activityUUIDs": ["CyVdYGsBAAAAAABkjLed","mNVdYGsBAAAAAABkjLZe"]
      }
    ]
  },
  "success": true
}
```


Permissions required: **Alert** > **Read**

20.1.4.2.2 Response parameters

Name	Type	Description
alertId	integer	Armis alert ID.
activityUUIDs	list[string]	List of related activity IDs.
connectionIds	list[integer]	List of IDs of the connections related to the alert
description	string	User-defined alert description.
deviceIds	list[integer]	List of IDs of the devices related to the alert.
severity	string	Alert severity (Low/Medium/High).
status	string	Alert status i.e., `Unhandled`/`Resolved`.
title	string	Alert title.
type	string	Alert type, i.e., `System/User Policy Violation`, `Anomaly Detection`, etc.
time	timestamp	Alert timestamp.

20.1.4.3 in:applications

GET https://{org_name}.armis.com/api/v1/search/?aql=in:applications {optional filters}

20.1.4.3.1 Examples

The following are examples for retrieving all the applications from Armis Centrix™:

cURL

```
curl "https://<armis-instance>.armis.com/api/v1/search/?aql=in:applications"
-H 'Authorization: <access-token>'
```

Python

```
response = requests.get(url="https://<armis-
instance>.armis.com/api/v1/search/",
     params={"aql": "in:applications"},
     headers={"Authorization": <access-token>})
```

The response will be a JSON array of devices similar to this:

```
{
     "data": {
        "count": 10,
        "next": 10,
        "prev": null,
        "results": [
           {
               "devices": 502,
               "firstSeen": "2020-08-13T09:23:36.147000+00:00",
               "lastSeen": "2023-01-15T18:19:01+00:00",
               "name": "Audio MIDI Setup",
               "version": "3.5"
           },
          ...
        ],
        "total": 3200
    },
    "success": true
}
```

> **NOTE:** The total number of applications is the value for "total", in this case 3,200. However, the Armis API defaults to a page size of 10, so there will be only 10 application elements in the results array that is returned. To use a different page size, refer to Paging through large amounts of data.

Additional example for a7 day period and OpenSSH

GET https://{org_name}.armis.com/api/v1/search/?aql=in:applications timeFrame:"7 Days" name:OpenSSH

```
{
  "data": {
    "results": [
      {
        "devices": 6,
        "firstSeen": "2020-09-28T18:57:58.731657",
        "lastSeen": "2020-10-05T07:22:33.145168",
        "name": "OpenSSH",
        "version": "7.4p1"
      }
    ]
  },
  "success": true
}
```


20.1.4.3.2 Response parameters

Name	Type	Description
devices	integer	The number of devices that used the application.
firstSeen	timestamp	When the application was first used.
lastSeen	timestamp	When the application was last used.
name	string	Application name e.g., OpenSSH
version	string	The version of the application.

20.1.4.4 in:businessApplications

`GET https://{org_name}.armis.com/api/v1/search/?aql=in:businessApplications {optional filters}`

20.1.4.4.1 Response parameters

Name	Type	Description
businessCriticality	string	
businessOwner	string	
businessUnit	string	
description	string	
deviceIds	list	
firstSeen	timestamp	When the application was first used.

Name	Type	Description
id	integer	The ID assigned to the business application.
installationType	string	
lastSeen	timestamp	When the business application was last used.
name	string	
operationalStatus	string	
type	string	

20.1.4.4.2 Example

```
GET https://{org_name}.armis.com/api/v1/search/in:businessApplications
```

```
{
  "data": {
    "count": 2,
    "next": null,
    "prev": null,
    "results": [
      {
        "businessCriticality": "Critical",
        "businessOwner": "Iorek B",
        "businessUnit": null,
        "description": "Database application to store our users",
        "deviceIds": [
          2145
        ],
        "firstSeen": "2023-05-09T08:32:05.223649+00:00",
        "id": 6,
        "installationType": "SAAS",
        "lastSeen": "2023-05-09T08:32:05.223649+00:00",
        "name": "My_app",
        "operationalStatus": null,
        "type": "Homegrown"
      },
      {
        "businessCriticality": "Critical",
        "businessOwner": "Ariel B",
        "businessUnit": null,
        "description": "Demo of Business Application.",
        "deviceIds": [
          556,
          599,
          378,
          564,
          398,
          1771,
          929,
          1938,
          1099,
          6888
        ],
        "firstSeen": "2023-06-19T12:06:29.081237+00:00",
        "id": 14,
        "installationType": "SAAS",
        "lastSeen": "2023-06-19T12:06:29.081237+00:00",
        "name": "Business Application Demo",
        "operationalStatus": null,
        "type": "Homegrown"
      }
    ],
    "total": 2
  },
  "success": true
}
```

20.1.4.5 in:connections

GET https://{org_name}.armis.com/api/v1/search/?aql=in:connections {optional filters}

20.1.4.5.1 Example

GET https://{org_name}.armis.com/api/v1/search/?aql=in:connections timeFrame:"7 Days" protocol:Wi-Fi


```
{
  "data": {
    "results": [
      {
       "band": null,
        "channel": null,
        "dhcpAuthenticationDuration": null,
        "duration": null,
        "endTimestamp": "2020-10-05T07:52:18.760804",
        "id": 1408,
        "inboundTraffic": 1024,
        "outboundTraffic": 0,
        "protocol": "Wi-Fi",
        "radiusAuthenticationDuration": null,
        "risk": "Medium",
        "rssi": null,
        "sensor": {
          "name": "0c:8d:db:b2:64:66",
          "type": "Access Point"
        },
        "site": {
          "location": "NYU",
          "name": "NYU"
        },
        "snr": null,
        "sourceId": 169,
        "startTimestamp": "2020-10-05T07:52:18.760804",
        "targetId": 254,
        "title": "Connection between HPE8D8D1E0498F and Skynet",
        "totalAssociationDuration": null,
        "traffic": 1024,
        "wlanAssociationDuration": null
      }
    ]
  },
  "success": true
}
```

20.1.4.5.2 Response parameters

Name	Type	Description
band	string	The frequency at which the connection was established: 2.4GHZ or 5GHZ.
bssid	string	The BSSID of the access point or wireless router.
channel	integer	The channel at which connections were established.
duration	integer	Total duration of the connection.
endTimestamp	timestamp	When the connection was ended.
id	integer	The ID assigned to the connection.
inboundTraffic	integer	The volume of the inbound traffic.
outboundTraffic	integer	The volume of the outbound traffic.
protocol	string	Protocol used (Network, Wi-Fi, etc.)
risk	string	The risk associated with the specific connection.
rssi	integer	The level of the signal strength during the connection. RSSI stands for Received Signal Strength Indicator.
sensor	JSON	The sensor that picked up the connection. • name—The sensor name. • type—The sensor type.
site	JSON	The site where the sensor that picked up the connection is located. • location—The site location. • name—The site name.
sites	JSON	The sites where the sensor that picked up the connection is located. This parameter is used for multiple sites and replaces the `site` parameter. • location—The site location. • name—The site name.
snr	integer	The SNR (signal-to-noise) ratio expressed in decibels.

Name	Type	Description
sourceId	integer	The ID of the connection source.
ssid	integer	The SSID for the network.
startTimestamp	timestamp	When the connection was started.
targetId	integer	The ID of the connection target.
title	string	The title assigned to the connection by Armis.
traffic	integer	Total traffic that passed during the connection.

20.1.4.6 in:devices

GET https://{org_name}.armis.com/api/v1/search/?aql=in:devices {optional filters}

20.1.4.6.1 Examples

The following are examples of retrieving all the devices from Armis Centrix™:

cURL

```
curl "https://<armis-instance>.armiscom/api/v1/search/?aql=in:devices"
-H 'Authorization: <access-token>'
```

Python

```
response = requests.get(url="https://<armis-
instance>.armis.com/api/v1/search/",
       params={"aql": "in:devices"},
       headers={"Authorization": <access-token>})
```

The response will be a JSON array of devices similar to the following:

```
{
"data": {
 "count": 10,
 "next": 10,
 "prev": null,
 "results": [
    {
       "accessSwitch": null,
       "boundaries": "Off Network",
       "businessImpact": "Unassigned",
       "category": "Network Equipment",
       "customProperties": {},
       "dataSources": [
          {
            "firstSeen": "2022-04-25T14:56:00+00:00",
            "lastSeen": "2023-01-15T19:14:08+00:00",
            "name": "Meraki",
            "types": [
              "WLC"
            ]
          },
          {
            "firstSeen": "2023-01-09T07:36:32+00:00",
            "lastSeen": "2023-01-15T19:22:40+00:00",
            "name": "Aruba WLC",
            "types": [
              "WLC"
            ]
          }

        ],
        "firstSeen": "2020-01-12T09:35:28+00:00",
        "id": 303239,
        "ipAddress": "",
        "ipv6": null,
        "lastSeen": "2022-01-15T19:22:40+00:00",
        "macAddress": "E2:63:22:AC:70:96",
        "manufacturer": null,
        "model": null,
        "name": null,
        "operatingSystem": null,
        "operatingSystemVersion": null,
        "riskLevel": 1,
        "sensor": {
          "name": "a8:46:9d:1c:92:ea",
          "type": "Access Point"
        },
        "site": null,
        "tags": [
          "Access Point"
        ],
        "type": "Access Points",
```

```
    "userIds": [],
    "visibility": "Full"
  },
  {
    "accessSwitch": null,
    "boundaries": "Off Network",
    "businessImpact": "Unassigned",
    "category": "Network Equipment",
    "customProperties": {},
    "dataSources": [
      {
        "firstSeen": "2021-10-19T16:29:52+00:00",
        "lastSeen": "2022-01-15T19:14:08+00:00",
        "name": "Meraki",
        "types": [
          "WLC"
        ]
      },
      {
        "firstSeen": "2021-12-13T09:33:52+00:00",
        "lastSeen": "2021-01-15T19:14:08+00:00",
        "name": "Aruba WLC",
        "types": [
          "WLC"
        ]
      }
    ],
    "firstSeen": "2021-09-14T15:07:39+00:00",
    "id": 983,
    "ipAddress": "",
    "ipv6": null,
    "lastSeen": "2023-01-15T19:22:40+00:00",
    "macAddress": "44:48:C1:CD:C9:E0",
    "manufacturer": "Hewlett Packard",
    "model": "Hewlett device",
    "name": "i-a-instant",
    "operatingSystem": null,
    "operatingSystemVersion": null,
    "riskLevel": 2,
    "sensor": {
      "name": "d0:15:66:cf:f9:de",
      "type": "Access Point"
    },
    "site": null,
    "tags": [
      "SSID=i-A-Instant",
      "Off Network",
      "Access Point"
    ],
    "type": "Access Points",
    "userIds": [],
    "visibility": "Full"
  },
  ...
```

```
      ],
      "total": 4415
   },
   "success": true
}
```

NOTES:

- The total number of devices is the value for “total”, in this case 4415. However, the Armis API defaults to a page size of 10, so there will be only 10 device elements in the results array that is returned. To use a different page size, refer to Paging through large amounts of data.
- You can also add fields as parameters to get additional properties, for example:

  ```
  api/v1/search/?aql=in%3Adevices&fields=carbonBlackDefenseStatus&includeTotal=true
  ```

  The format of the properties needs to be the same as the ASQ format of the field.

20.1.4.6.2 Response parameters

Name	Type	Description
accessSwitch	string	
boundaries	string	
businessImpact	string	
category	string	The device category: computer, handheld, medical, and so on.
customProperties	JSON	
dataSources	list	
firstSeen	timestamp	When was the device first seen.
id	integer	Device ID.
ipAddress	string	Device IP address.
ipv6	string	Device IPv6 address.
lastSeen	timestamp	when was the device last seen
macAddress	string	Device MAC address.
manufacturer	string	Device manufacturer, represented in the Armis console as Brand.
model	string	Device model.
name	string	Device name.
names	string	
operatingSystem	string	device operating system

Name	Type	Description
operatingSystemVersion	string	device operating system version
purdueLevel	string	
riskLevel	string	Risk level assigned to the device: Low (1-3), Medium (4-7), or High (8-10).
sensor	JSON	Last sensor that saw the device • name: The sensor name.
site	JSON	Site to which the sensor belongs. • location: The site location. • name | site name
tags	list[string]	Attached device tags.
type	string	Device type
user	string	Device user.
userIds	list	
visibility	string	

20.1.4.7 in:operatingSystems

GET https://{org_name}.armis.com/api/v1/search/?aql=in:operatingSystems {optional filters}

20.1.4.7.1 Example

GET https://{org_name}.armis.com/api/v1/search/?aql=in:operatingSystems


```
{
  "data": {
    "count": 10,
    "next": 10,
    "prev": null,
    "results": [
      {
        "devices": 9,
        "firstSeen": "2023-02-13T12:04:26.626349+00:00",
        "lastSeen": "2023-10-12T08:20:14.149862+00:00",
        "name": "Amazon Linux",
        "version": "2"
      },
      {
        "devices": 2,
        "firstSeen": "2023-05-04T17:37:34.895874+00:00",
        "lastSeen": "2023-10-06T13:59:26+00:00",
        "name": "Amazon Linux",
        "version": "2023"
      },
      {
        "devices": 60,
        "firstSeen": "2023-02-12T16:10:35+00:00",
        "lastSeen": "2023-10-12T11:29:04+00:00",
        "name": "Android",
        "version": ""
      },
      {
        "devices": 2,
        "firstSeen": "2023-02-13T12:14:48.044508+00:00",
        "lastSeen": "2023-10-12T13:33:33.785147+00:00",
        "name": "ArubaOS",
        "version": ""
      }
    ],
    "total": 114
  },
  "success": true
}
```

20.1.4.7.2 Response parameters

Name	Type	Description
devices	integer	The number of devices that run the operating system.
firstSeen	timestamp	When the operating system was first seen.
lastSeen	timestamp	When the operating system was last seen.
name	string	The name of the operating system e.g., iOS, Android
version	string	The version of the operating system.

20.1.4.8 in:riskFactors

```
GET https://{org_name}.armis.com/api/v1/search/?aql=in:riskFactors
{optional filters}
```

20.1.4.8.1 Example

```
GET https://{org_name}.armis.com/api/v1/search/?aql=in:riskFactors
```

```
{
  "data": {
    "count": 10,
    "next": 10,
    "prev": null,
    "results": [
      {
        "category": "Behavioural",
        "description": "Policy Violation",
        "devices": 6123,
        "group": "Policies",
        "lastSeen": "2023-10-12T13:45:36+00:00",
        "score": "High",
        "status": "Open",
        "type": "Policy Violations"
      },
      {
        "category": "Profile",
        "description": "Device is accepting SMBv1 requests.",
        "devices": 10,
        "group": "Configuration",
        "lastSeen": "2023-10-12T13:34:36.618362+00:00",
        "score": "Medium",
        "status": "Open",
        "type": "SMBv1 Support"
      },
      {
        "category": "Behavioural",
        "description": "Policy Violation",
        "devices": 38,
        "group": "Policies",
        "lastSeen": "2023-10-12T13:32:48+00:00",
        "score": "Medium",
        "status": "Ignored",
        "type": "Policy Violations"
      },
      {
        "category": "Profile",
        "description": "Manufacturer 'VMware' detected",
        "devices": 801,
        "group": "Hardware",
        "lastSeen": "2023-10-12T11:20:39.254261+00:00",
        "score": "Low",
        "status": "Open",
        "type": "Manufacturer Reputation"
      },
      {
        "category": "Profile",
        "description": "Manufacturer 'Apple' detected",
        "devices": 4637,
        "group": "Hardware",
        "lastSeen": "2023-10-12T10:34:52.348939+00:00",
        "score": "Low",
        "status": "Open",
        "type": "Manufacturer Reputation"
```

```
      }
    ],
    "total": 223
  },
  "success": true
}
```

20.1.4.8.2 Response parameters

Name	Type	Description
category	string	The risk category e.g., Profile.
description	string	Description of a risk factor.
devices	integer	The number of devices on which the risk factor is detected.
group	string	E.g., Policies, Hardware
lastSeen	timestamp	When the risk factor was last detected.
score	string	The score assigned to the risk factor.
status	string	E.g., Open, Ignored.
type	string	The risk factor type.

20.1.4.9 in:services

GET `https://{org_name}.armis.com/api/v1/search/?aql=in:services {optional filters}`

20.1.4.9.1 Example

GET https://{org_name}.armis.com/api/v1/search/?aql=in:services timeFrame:"7 Days" name:(zoom)


```
{
  "data": {
    "results": [
      {
        "devices": 6,
        "firstSeen": "2020-09-28T19:00:00",
        "hosts": 1,
        "inboundTraffic": 123581783523,
        "jitterMS": 3.77868852459016,
        "lastSeen": "2020-10-04T10:00:00",
        "latency": null,
        "name": "Zoom:8801",
        "outboundTraffic": 59229109610,
        "packetLoss": 0.0879424661632147,
        "packetsCount": 308289341,
        "retransmitCount": 0,
        "traffic": 182810893133
        }
    ]
  },
  "success": true
}
```


20.1.4.9.2 Response parameters

Name	Type	Description
devices	integer	The number of devices that used a network service.
firstSeen	timestamp	When the operating system was first used.
hosts	integer	The number of service hosts.
inboundTraffic	integer	The volume of the inbound traffic.
jitterMS	integer	The deviation from true periodicity of a periodic signal (in milliseconds).
lastSeen	timestamp	When the service was last used.
latency	integer	The time it takes for a data packet to reach its destination (in milliseconds).

Name	Type	Description
name	string	The name of the port used by the service.
outboundTraffic	integer	The volume of the outbound traffic.
packetLoss	integer	The number of packets of data that did not reach their destination.
packetsCount	integer	The number of transmitted packets of data.
retransmitCount	integer	The number of times when packets were resent due to being lost or damaged.
traffic	integer	The total traffic volume.

20.1.4.10 in:traffic

GET https://{org_name}.armis.com/api/v1/search/?aql=in:traffic {optional filters}

20.1.4.10.1 Example

GET https://{org_name}.armis.com/api/v1/search/?aql=in:traffic timeFrame:"7 Days" sensors:"0c:8d:db:b2:61:3e"


```
{
  "data": {
    "results": [
      {
        "description": "Multicast DNS (mDNS)",
        "devices": 6,
        "firstSeen": "2020-09-28T19:00:00",
        "inboundTraffic": 0,
        "jitterMS": "N/A",
        "lastSeen": "2020-10-04T10:00:00",
        "latency": "N/A",
        "name": "mDNS",
        "outboundTraffic": 82819,
        "packetLoss": "N/A",
        "packetsCount": 220,
        "port": 5353,
        "retransmitCount": 0,
        "traffic": 82819
        }
    ]
  },
  "success": true
}
```


20.1.4.10.2 Response parameters

Name	Type	Description
description	string	The name of a protocol for which the network activity was analyzed.
devices	integer	The number of devices on which the network activity was analyzed.
firstSeen	timestamp	When the protocol was first used.
inboundTraffic	integer	The volume of the inbound traffic.
jitterMS	integer	The deviation from true periodicity of a periodic signal (in milliseconds).
latency	integer	The time it takes for a data packet to reach its destination (in milliseconds).
name	string	The name of the port used by the protocol.

Name	Type	Description
outboundTraffic	integer	The volume of the outbound traffic.
packetLoss	integer	The number of packets of data that did not reach their destination.
packetsCount	integer	The number of transmitted packets of data.
port	integer	The number of the port used by the protocol.
retransmitCount	integer	The number of times when packets were resent due to being lost or damaged.
traffic	integer	The total traffic volume.

20.1.4.11 in:users

GET https://{org_name}.armis.com/api/v1/search/?aql=in:users {optional filters}

20.1.4.11.1 Example

GET https://{org_name}.armis.com/api/v1/search/?aql=in:users


```
{
  "data": {
    "count": 1,
    "next": 9,
    "prev": 7,
    "results": [
      {
        "dataSources": [
          {
            "firstSeen": 1693985737554,
            "hideTimestamps": false,
            "icon": "iconIntegrationTypeDatasourceTrafficInspection",
            "id": 71426,
            "key": "TRAFFIC_INSPECTION",
            "lastSeen": 1695833231539,
            "name": "Traffic Inspection",
            "types": [
              "Traffic Inspection",
              "Data Analysis"
            ]
          }
        ],
        "deviceIds": [
          15037,
          14872
        ],
        "displayName": null,
        "email": null,
        "firstSeen": "2023-09-06T07:35:37.554610+00:00",
        "id": 197078,
        "lastSeen": "2023-09-27T16:47:11.539759+00:00",
        "lastUsedDevice": null,
        "name": "I-ALTIRIS$",
        "phone": null,
        "properties": {
          "domain": "ARMI"
        },
        "username": "I-ALTIRIS$"
      }
    ],
    "total": 5211
  },
  "success": true
}
```

20.1.4.11.2 Response parameters

Name	Type	Description
dataSources	list	This can include the following: firstSeen, hideTimestamps, icon, id, key, lastSeen, name, types.
deviceIds	list	List of devices IDs which are related to the user.
displayName	string	The users display name.
email	string	The users email address.
firstSeen	timestamp	When the user was first seen.
id	integer	The ID assigned to the user.
lastSeen	timestamp	When the user was last seen.
lastUsedDevice	string	The last device used.
name	string	The name.
phone	string	The phone number for the user.
properties	string	Additional properties
username	string	The username.

20.1.4.12 in:vulnerabilities

GET https://{org_name}.armis.com/api/v1/search/?aql=in:vulnerabilities {optional filters}}

20.1.4.12.1 Example

GET https://{org_name}.armis.com/api/v1/search/?aql=in:vulnerabilities


```
{
        "affectedDevicesCount": 1,
        "attackComplexity": "Low",
        "attackVector": "Not Defined",
        "availabilityImpact": "High",
        "confidentialityImpact": "None",
        "id": 1,
        "description": "An issue was discovered in certain Apple products.
         iOS before 11.3 is affected. The issue involves the \"Find My
iPhone\"
         component. It allows physically proximate attackers to bypass the
iCloud
         password requirement for disabling the \"Find My iPhone\" feature via
         vectors involving a backup restore.",
        "cveUid": "CVE-2018-4172",
        "exploitabilityScore": 0.9,
        "impactScore": 3.6,
        "integrityImpact": "None",
        "privilegesRequired": "None",
        "publishedDate": "2018-03-04T08:26:25.070341",
        "scope": "Unchanged",
        "score": 4.6,
        "severity": "High",
        "status": "Unresolved",
        "userInteraction": "None",
        "vulnerableEntities": [
       {
         "affectedDevicesCount": 1,
         "name": "iOS",
         "version": "11.3",
         "vendor": "Apple"
    }
  ]
}
```

20.1.4.12.2 Response parameters

Name	Type	Description
affectedDevicesCount	integer	The number of devices affected by the vulnerability.
attackComplexity	string	How complicated it is to exploit the discovered vulnerability: `None`, `Low`, `Medium`, `High`, or `Critical`.
attackVector	string	What access the attacker needs to exploit the vulnerability: `Network`, `Adjacent Network`, `Local` or `Physical`.
availabilityImpact	string	Level of impact to the data availability when the vulnerability is successfully exploited on a component: `None`, `Low`, `Medium`, `High`, or `Critical`.
confidentialityImpact	string	Level of impact to the data confidentiality when the vulnerability is successfully exploited on a component: `None`, `Low`, `Medium`, `High`, or `Critical`.
cveUid	string	ID of the corresponding entry in the CVE system.
cvssScore	string	The CVS score.
description	string	Vulnerability description.
exploitabilityScore	integer	Probability of the vulnerability to be exploited based on the current state of exploitation techniques or automated exploitation code.
id	integer	Armis vulnerability ID.
impactScore	integer	Numerical representation of the impact of a successful vulnerability exploit on your business: low (1-3), medium (4-7), or high (8-10).
integrityImpact	string	Level of impact to the data integrity when the vulnerability is successfully exploited on a component: None, Low, Medium, High, or Critical.
privilegesRequired	string	Level of privileges the attacker needs to exploit the vulnerability successfully: `None`, `Low`, `Medium`, `High`, or `Critical`.
publishedDate	timestamp	Date when the vulnerability was publicly exposed in the CVE system.
qualysScore	string	The Qualys score.

Name	Type	Description
scope	integer	Numerical representation of the vulnerability score calculated by adding exploitabilityScore to impactScore: low (1-3), medium (4-7), or high (8-10).
score	integer	Numerical representation of the vulnerability score calculated by adding exploitabilityScore to impactScore: low (1-3), medium (4-7), or high (8-10).
severity	string	Qualitative representation of the vulnerability severity: `None`, `Low`, `Medium`, `High`, or `Critical`.
status	string	Whether the vulnerability is Unresolved or Resolved. Resolved vulnerabilities will be fetched only by an explicit search for status:Resolved or for a specific id.
userInteraction	string	Whether the attacker can perpetrate the attack alone (None) or they must be assisted by another user (Required).
vulnerableEntities	list[JSON]	The entities (operating systems, applications, etc.) affected by the vulnerability • affectedDevicesCount | integer: Number of devices affected by the vulnerability • name—string: Name of the vulnerable entity. • version—string: Version of the vulnerable entity. • vendor—string: Vendor of the vulnerable entity.

21 Sites

21.1 Returning all sites information

GET `/api/v1/sites/`

21.1.1 URI parameters

Name	Type	Description
from	integer (query)	Paging from.
length	integer (query)	Paging from.
includeTotal	boolean (query)	Return total count, default False.
fields	(query)	Fields to show. If omitted, returns a default subset of fields.

21.1.2 Example


```
{
  "data": {
    "count": 10,
    "next": 10,
    "prev": 0,
    "sites": [
      {
        "id": "710",
        "integrationIds": [
          "27"
        ],
        "lat": 32.0852999,
        "lng": 34.7817676,
        "location": "Tel_a",
        "name": "Meraki",
        "networkEquipmentDeviceIds": [
          "258",
          "374"
        ]
      },
      {
        "id": "711",
        "integrationIds": [
          "25"
        ],
        "lat": 51.5072178,
        "lng": -0.1275862,
        "location": "London",
        "name": "switch"
      },
      {
        "id": "712",
        "name": "Jane"
      },

      {
        "id": "716",
        "location": "",
        "name": "efwwfe",
        "parentId": "713",
        "tier": "",
        "user": "john1@xyz.com"
      },
    ]
  },
  "success": true
}
```

21.1.3 Responses

This API call has the following HTTP status codes:

Code	Description
200	OK.
400	Bad request.
401	Authorization information is missing or invalid. **Name**—Authorization. **Description**—The `access_token` obtained using the `/access_token/` endpoint. **Type**—string.

21.2 Creating a new site

POST `/api/v1/sites/`

21.2.1 URI parameters

Name	Type	Description
site	object (body)	JSON describing the site.

21.2.2 Example

```
{
  "location": "my location",
  "name": "my site name",
  "parentSiteId": 1,
  "rule": {
    "or": [
      "type:ACCESS_POINT"
    ]
  },
  "tier": "tier A"
}
```

21.2.3 Responses

This API call has the following HTTP status codes:

Code	Description
201	OK.
400	Bad request.
401	Authorization information is missing or invalid. **Name**—Authorization. **Description**—The `access_token` obtained using the `/access_token/` endpoint. **Type**—string.

21.3 Deleting a site

`DELETE` `/api/v1/sites/{site_id}/`

21.3.1 URI parameters

Name	Type	Description
site_id * Required	(path)	The site ID in the Armis system.

21.3.2 Responses

This API call has the following HTTP status codes:

Code	Description
204	OK.
400	Bad request, please check the arguments you passed.
401	Authorization information is missing or invalid. **Name**—Authorization. **Description**—The `access_token` obtained using the `/access_token/` endpoint. **Type**—string.
404	Unknown site.

21.4 Getting a site by ID

GET `/api/v1/sites/{site_id}/`

21.4.1 URI parameters

Name	Type	Description
site_id * Required	(path)	The site ID in the Armis system.
fields	(query)	Fields to show. If omitted, returns a default subset of fields.

21.4.2 Example

```
{
  "data": {
    "id": "711",
    "integrationIds": [
      "25"
    ],
    "lat": 51.5072178,
    "lng": -0.1275862,
    "location": "London",
    "name": "switch"
  },
  "success": true
}
```

21.4.3 Responses

This API call has the following HTTP status codes:

Code	Description
200	OK.
400	Bad request, please check the arguments you passed.
401	Authorization information is missing or invalid. **Name**—Authorization. **Description**—The `access_token` obtained using the `/access_token/` endpoint. **Type**—string.
404	Unknown site.

21.5 Updating a site

PATCH `/api/v1/sites/{site_id}/`

21.5.1 URI parameters

Name	Type	Description
site_id * Required	(path)	The site ID in the Armis system.
site	object (body)	

21.5.2 Example

```
{
  "location": "my location",
  "name": "my site name",
  "parentSiteId": 1,
  "rule": {
    "or": [
      "type:ACCESS_POINT"
    ]
  },
  "tier": "tier A"
}
```

21.5.3 Responses

This API call has the following HTTP status codes:

Code	Description
200	OK.
400	Bad request, please check the arguments you passed.
401	Authorization information is missing or invalid. **Name**—Authorization. **Description**—The `access_token` obtained using the `/access_token/` endpoint. **Type**—string.
404	Unknown site.

21.6 Getting all integration IDs of the site

GET `/api/v1/sites/{site_id}/integrations-ids/`

21.6.1 URI parameters

Name	Type	Description
site_id * Required	(path)	The site ID in the Armis system.

21.6.2 Example

```
{
  "data": {
    "integrationIds": [
      27
    ]
  },
  "success": true
}
```

21.6.3 Responses

This API call has the following HTTP status codes:

Code	Description
204	The entity deleted successfully.
400	Bad request, please check the arguments you passed.
401	Authorization information is missing or invalid. **Name**—Authorization. **Description**—The `access_token` obtained using the `/access_token/` endpoint. **Type**—string.
404	Unknown site.

21.7 Adding a new integration ID to the site

POST `/api/v1/sites/{site_id}/integrations-ids/`

21.7.1 URI parameters

Name	Type	Description
site_id * Required	(path)	The site ID in the Armis system.
siteIntegrationId	object (body)	Site integration ID.

21.7.2 Example

```
{
  "integrationId": 1
}
```

21.7.3 Responses

This API call has the following HTTP status codes:

Code	Description
400	Bad request, please check the arguments you passed. **Example:** `{ "message": "string", "success": true }`

21.8 Deleting an integration ID from the site

DELETE `/api/v1/sites/{site_id}/integrations-ids/{integration_id}/`

21.8.1 URI parameters

Name	Type	Description
site_id	(path)	The site ID in the Armis system.
integration_id	integer (path)	The integration ID in the site to delete.

21.8.2 Responses

This API call has the following HTTP status codes:

Code	Description
204	The entity deleted successfully.
400	Bad request, please check the arguments you passed.
401	Authorization information is missing or invalid. **Name**—Authorization. **Description**—The `access_token` obtained using the `/access_token/` endpoint. **Type**—string.
404	Unknown site.

21.9 Getting all network equipment device IDs of the site

GET `/api/v1/sites/{site_id}/network-equipment/`

21.9.1 URI parameters

Name	Type	Description
site_id * Required	(path)	The site ID in the Armis system.

21.9.2 Example


```
{
  "data": {
    "networkEquipmentDeviceIds": [
      235,
      167,
      324,
      437,
      217,
      412,
      373,
      438,
      2801,
      159,
      292,
      413,
      354,
      230,
      223,
      161
    ]
  },
  "success": true
}
```


21.9.3 Responses

This API call has the following HTTP status codes:

Code	Description
204	The entity deleted successfully.
400	Bad request, please check the arguments you passed.
401	Authorization information is missing or invalid. **Name**—Authorization. **Description**—The `access_token` obtained using the `/access_token/` endpoint. **Type**—string.
404	Unknown site.

21.10 Adding a new network device ID to the site

POST `/api/v1/sites/{site_id}/network-equipment/`

21.10.1 URI parameters

Name	Type	Description
site_id * Required	(path)	The site Id in the Armis system.
networkEquipmentDeviceId	object (body)	Site network Equipment Device ID.

21.10.2 Example

```
{
  "networkEquipmentDeviceId": 1
}
```

21.10.3 Responses

This API call has the following HTTP status codes:

Code	Description
204	The entity deleted successfully.
400	Bad request, please check the arguments you passed.
401	Authorization information is missing or invalid. **Name**—Authorization. **Description**—The `access_token` obtained using the `/access_token/` endpoint. **Type**—string.
404	Unknown site.

21.11 Deleting a network device ID from the site

DELETE `/api/v1/sites/{site_id}/network-equipment/{network_equipment_id}/`

21.11.1 URI parameters

Name	Type	Description
site_id * Required	(path)	The site ID in the Armis system.
network_ equipment_id	integer (path)	

21.11.2 Responses

This API call has the following HTTP status codes:

Code	Description
204	The entity deleted successfully.
400	Bad request, please check the arguments you passed.
401	Authorization information is missing or invalid. **Name**—Authorization. **Description**—The `access_token` obtained using the `/access_token/` endpoint. **Type**—string.
404	Unknown site.

22 Users

22.1 Returning existing accounts

GET /api/v1/users/

22.1.1 Permissions required

- **Settings** > **Users And Roles** > **Read**

22.1.2 URI parameters

Name	Type	Description
fields	(query)	Fields to show, delimited by commas. If omitted, returns all fields.

22.1.3 Examples

cURL

```
curl "https://<armis-instance>.armis.com/api/v1/users/"
     -H 'Authorization: <access-token>'
```

Python

```
response =
requests.get(url="https://<armis-instance>.armis.com/api/v1/users/
",
headers={"Authorization": <access-token>})
```

```
{
   "data": {
     "users": [
       {
         "email": "jsmith@acme.com",
         "id": 1,
         "isActive": true,
         "location": null,
         "name": "Acme",
         "phone": null,
         "reportPermissions": "EXPORT",
         "role": "ADMIN",
         "roleAssignment": [
           {
             "name": [
               "Admin"
             ]
           }
         ],
         "title": "",
         "twoFactorAuthentication": false,
         "username": "acme"
       },
      ...
       { // Next user
      }
    ]
   },
   "success": true
}
```


22.1.4 Responses

This API call has the following HTTP status codes:

Code	Description
200	OK.

22.2 Creating a new account

POST `/api/v1/users/`

22.2.1 Permissions required

- **Settings** > **UsersAnd Roles** > **Manage** > **Users** > **Create**

22.2.2 URI parameters

Name	Type	Description
fields	(query)	Fields to show, delimited by commas. If omitted, returns all fields.
formData	(body)	

22.2.3 Example

```
{
  "dashboard_ids_to_clone": [
    "2",
    "6"
  ],
  "email": "jsmith@acme.com",
  "location": "New York, NY, USA",
  "name": "John Smith",
  "phone": "(478) 275-5945",
  "roleAssignment": [
    {
      "name": [
        "Reporter",
        "Viewer"
      ],
      "sites": [
        "Palo Alto",
        "Tel Aviv"
      ]
    }
  ],
  "title": "Security Analyst",
  "username": "jsmith"
}
```

22.2.4 Responses

This API call has the following HTTP status codes:

Code	Description
200	OK.
400	Unknown dashboard type.

22.3 Deleting a user

DELETE /api/v1/users/{user_id_or_email}/

22.3.1 Permissions required

- **Settings** > **Users And Roles** > **Manage** > **Users** > **Delete**

22.3.2 URI parameters

Name	Type	Description
user_id_or_email * Required	(path)	Armis user ID or email.

22.3.3 Responses

This API call has the following HTTP status codes:

Code	Description
200	OK
404	Unknown user.

22.4 Getting a user by ID or email

GET /api/v1/users/{user_id_or_email}/

22.4.1 Permissions required

- **Settings** > **Users And Roles** > **Read**

22.4.2 URI parameters

Name	Type	Description
user_id_or_email * Required	(path)	Armis user ID or email.
fields	(query)	Fields to show, delimited by commas. If omitted, returns all fields.

22.4.3 Responses

This API call has the following HTTP status codes:

Code	Description
200	OK
404	Unknown user.

22.5 Editing a user

PATCH /api/v1/users/{user_id_or_email}/

22.5.1 Permissions required

- **Settings** > **Users And Roles** > **Manage** > **Users** > **Edit**

22.5.2 URI parameters

Name	Type	Description
user_id_or_email * Required	(path)	Armis user ID or email.
fields	(query)	Fields to show, delimited by commas. If omitted, returns all fields.
formData	(body)	

22.5.3 Example

```
{
  "email": "jsmith@acme.com",
  "location": "New York, NY, USA",
  "name": "John Smith",
  "phone": "(478) 275-5945",
  "roleAssignment": [
    {
      "name": [
        "Reporter",
        "Viewer"
      ],
      "sites": [
        "Palo Alto",
        "Tel Aviv"
      ]
    }
  ],
  "title": "Security Analyst",
  "username": "jsmith"
}
```

22.5.4 Responses

This API call has the following HTTP status codes:

Code	Description
200	OK.
400	Invalid format of field `email`.
401	Authorization information is missing or invalid. **Name**—Authorization. **Description**—The `access_token` obtained using the `/access_token/` endpoint. **Type**—string.
404	Unknown user.

23 Vulnerability

The Vulnerability API endpoints enable you to do the following:

- Get CVE-on-asset matches according to CVE or device IDs.
- Set the status (Open, Ignored, Resolved) of CVE-on-asset matches according to CVE or device IDs.

For more information about vulnerabilities, see the Armis user guide and the *AVM User Guide*.

23.1 Getting CVE-on-asset matches according to CVE or device IDs

GET `/api/v1/vulnerability-match/`

23.1.1 Permissions required

- **Vulnerability** > **Read**

23.1.2 URI parameters

Name	Type	Description
device_ids	string (query)	A list of comma-separated Armis Device IDs.
vulnerability_ids	string (query)	A list of comma-separated Armis Vulnerability IDs.
from	integer (query)	Paging from
length	integer (query)	Paging length

23.1.3 Example

```
{
        "advisoryId": null,
        "avmRating": "MEDIUM",
        "confidenceLevel": "High",
        "cveUid": "CVE-2022-32845",
        "deviceId": 1736828,
        "firstDetected": "2022-12-27T15:39:15.787146+00:00",
        "lastDetected": "2022-12-27T15:39:15.787146+00:00",
        "matchCriteriaString": "OS:(iOS 14.4.2) ",
        "recommendedSteps": null,
        "remediationTypes": null,
        "status": "Resolved",
        "statusSource": "AUTO"
      },
      {
        "advisoryId": null,
        "avmRating": "MEDIUM",
        "confidenceLevel": "High",
        "cveUid": "CVE-2022-32845",
        "deviceId": 49,
        "firstDetected": "2022-11-02T07:41:24.918154+00:00",
        "lastDetected": "2023-01-02T18:58:47.402774+00:00",
        "matchCriteriaString": "OS:(macOS 12.2.1) ",
        "recommendedSteps": null,
        "remediationTypes": null,
        "status": "Resolved",
        "statusSource": "API"
      },
      {
        "advisoryId": null,
        "avmRating": "CRITICAL",
        "confidenceLevel": "High",
        "cveUid": "CVE-2020-1472",
        "deviceId": 1730667,
        "firstDetected": "2021-03-30T10:53:03.377466+00:00",
        "lastDetected": "2023-04-12T11:55:41.598613+00:00",
        "matchCriteriaString": "OS:(Fedora 33) ",
        "recommendedSteps": null,
        "remediationTypes": null,
        "status": "Open",
        "statusSource": "CONSOLE"
      },
      {
        "advisoryId": null,
        "avmRating": null,
        "confidenceLevel": "High",
        "cveUid": "CVE-2023-21427",
        "deviceId": 1734392,
        "firstDetected": "2023-04-23T11:58:49.227537+00:00",
        "lastDetected": "2023-04-23T11:58:49.227537+00:00",
        "matchCriteriaString": "OS:(Android 13.0) ",
        "recommendedSteps": null,
        "remediationTypes": null,
        "status": "Open",
        "statusSource": null
      }
```

23.1.4 Responses

This API call has the following HTTP status codes:

Code	Description
200	OK.
400	Bad request. Missing identifier parameter, must provide one of `device_ids`, `vulnerability_ids`.
401	Authorization information is missing or invalid. **Name**—Authorization. **Description**—The `access_token` obtained using the `/access_token/` endpoint. **Type**—string.
402	Not permitted.

23.2 Setting the status of CVE-on-asset matches according to CVE or device IDs

POST `/api/v1/vulnerability/set_status/`

23.2.1 URI parameters

Name	Type	Description
device_ids	string (formData)	A list of comma-separated Armis Device IDs.
vulnerability_ids	string (formData)	A list of comma-separated Armis Vulnerability IDs.
status * Required	string (formData)	The status of the designated vulnerability matches Available values : `OPEN`, `IGNORED`, `RESOLVED`

23.2.2 Responses

This API call has the following HTTP status codes:

Code	Description
200	OK.
400	Nothing to change.
401	Authorization information is missing or invalid. **Name**—Authorization. **Description**—The `access_token` obtained using the `/access_token/` endpoint. **Type**—string.
402	Not permitted.